About this Playbook

This playbook is intended for the business and technical leadership of Microsoft partners that are interested in adding a security-focused practice to their business.

Objectives

The goal of this playbook is to help accelerate or optimize a security-focused practice and understand the practice opportunity, not to re-write the existing body of detailed guidance on how to perform any given recommendation. Instead, this playbook will direct partners to the best resources to build or grow a practice.

For the business side, this playbook provides valuable resources for driving new revenue opportunities, developing strategies for marketing, selling, and lead capture, as well as building deeper and longer term engagements with customers through potential new service offerings like managed services.

For the technical side, the playbook offers guidance on a number of topics that range from the technical skills needed, to resources available to accelerate learning, as well as an explanation of some of the key opportunities for technical delivery to focus on.

How this playbook was made

This playbook is part of a series of guidance written by Microsoft Partner, Solliance, in conjunction with the Microsoft One Commercial Partner group and 14 other successful partners that have volunteered time to provide input and best practices to share with the rest of the partner community.

To validate the guidance provided in this playbooks, Microsoft worked with MDC Research to conduct a survey of 484 global partners. In this survey, insights were gathered on a range of topics, including how partners hire, compensate and train resources; their business model, revenue and profitability; what practices and services they offer; and what skillsets they have in place to support their offers. The results of this survey are provided in-line with the guidance found within this playbook.

This playbook is focused on security with elements of compliance included, but it is not intended to be a comprehensive compliance guide.

<table>
<thead>
<tr>
<th>CONTRIBUTING PARTNERS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Accenture</td>
<td>KPMG</td>
</tr>
<tr>
<td>Atea</td>
<td>Performanta</td>
</tr>
<tr>
<td>BT</td>
<td>ResourceiT</td>
</tr>
<tr>
<td>Dimension Data</td>
<td>Slalom</td>
</tr>
<tr>
<td>Extra Mile Marketing</td>
<td>SoftwareOne</td>
</tr>
<tr>
<td>Ernst &amp; Young</td>
<td>VBC</td>
</tr>
<tr>
<td>Hanu Software</td>
<td>Wortell</td>
</tr>
</tbody>
</table>

aka.ms/practiceplaybooks
Using the playbook effectively

Quickly read through the playbook to become familiar with the layout and content. Each section includes an executive summary and key actions for that specific topic. Review these summaries first to decide which areas to focus on. Go over the content several times, if needed, then share with the team.

TO GET THE MOST VALUE OUT OF THIS PLAYBOOK:

☑ Get the team together and discuss which pieces of the strategy each person is responsible for
☑ Share the playbook with sales, marketing, support, technical, and managed services teams
☑ Leverage the resources available from Microsoft to help maximize profitability
☑ Share feedback on how we can improve this and other playbooks by emailing playbookfeedback@microsoft.com
# Table of Contents

About this Playbook: 2  
Table of Contents: 4  
The Security Opportunity: 5  
Partner Practice Development Framework: 8  
**Define the Strategy**: 9  
Executive Summary: 10  
Define the Practice Focus: 11  
Understanding the Security Practice: 12  
Define and Design the Solution Offer: 22  
Understanding Project Based Services: 23  
Deploy Microsoft Intune: 34  
Deploy Advanced Threat Analytics: 35  
Deploy Azure Sentinel: 36  
Deploy Information Protection: 37  
Deploy Azure Information Protection: 39  
Understanding Managed Services: 48  
Accelerate the Managed Service Model: 52  
Understanding Intellectual Property: 75  
Define Vertical Offerings: 78  
Define the Pricing Strategy: 79  
Identify Partnership Opportunities: 85  
Define Engagement Process: 87  
Implementation Process: 88  
Stay Informed on Security & Compliance: 89  
Identify Potential Customers: 93  
Join the Microsoft Partner Network: 94  
Identify Solution Marketplace Platform: 97  
**Hire & Train**: 98  
Executive Summary: 99  
Hire, Build, and Train The Team: 101  
Job Descriptions: 104  
Recruiting Resources: 111  
Training & Readiness: 112  
Competencies and Certifications: 117  
**Operationalize**: 118  
Executive Summary: 119  
Implement a Solution Delivery Process: 120  
Claim Internal Use Benefits: 121  
Manage and Support an Azure Deployment: 130  
Support Ticket Setup and Tracking: 132  
Integrate Into a Marketplace: 133  
Implement Intellectual Property Offerings: 134  
Setup Social Offerings: 135  
Create Engagement Checklists & Templates: 136  
**Go to Market and Close Deals**: 137  
Executive Summary: 138  
Marketing to the Security Buyer: 139  
Consultative Selling and Technical Pre-Sales: 141  
Architecture Design Session (ADS): 147  
Implement Proof of Concepts: 149  
Go-to-Market and Close Deals Guide: 150  
**Optimize and Grow**: 151  
Executive Summary: 152  
Understanding Customer Lifetime Value: 153  
Guide: Optimize and Grow: 155  
Security Playbook Summary: 156  

© 2020 Microsoft. All rights reserved.
The Security Opportunity

As companies embrace the opportunities presented by cloud and mobile computing to connect with customers and optimize operations, they take on new risks. One of the biggest challenges in digital transformation is ensuring security, privacy, and compliance.

PROTECTING AGAINST EVOLVING CYBERSECURITY THREATS

In today’s world, it’s clear that increasing trust and managing security is a struggle for many organizations. But as these statistics point out, the importance of improving security comprehensively has become even more evident:

- **250%**
  - Increase in phishing emails between January and December 2018.¹

- **279 Days**
  - Average time to identify and contain a breach.²

- **$133.8 Billion**
  - Forecasted global spending on security solutions by 2022.³

Traditional IT boundaries are disappearing and organizations now need to protect data on employee-owned mobile devices and SaaS applications not operated by the IT team. If they do not adapt their approach to security, companies face the risk of significant financial loss, damage to customer satisfaction, and market reputation. This presents an opportunity to help companies manage security concerns in an ever-evolving technology world that’s constantly under threat.

COMPLIANCE REGULATIONS PRESENT NEW OPPORTUNITIES

The General Data Protection Regulation (GDPR) brought about significant changes on organizations all over the world regarding how they manage and protect personal data. Since May, 2018, GDPR has imposed new rules on organizations that offer goods and services to people who reside in the European Union (EU), or that collect and analyze data tied to EU residents, no matter where they are located.

Partners have multiple opportunities to monetize on GDPR. First, customers will need consultants to support them on their journey to GDPR compliance, which may start with assisting customers in identifying the personal data they store, where it is stored, how it is stored, and how it needs to be protected. Second, partners can conduct gap assessments and make recommendations on technology, people, and processes that customers need to comply with GDPR. And third, partners can play a major role in helping customers build and maintain detection and notification systems for data breaches.

**SOURCES:**

- ¹ Trends in Cybersecurity: Top 10 insights from the Microsoft Security Intelligence Report
- ² 2019 Cost of Data Breach Report
- ³ IDC Worldwide Semiannual Security Spending Guide

aka.ms/practiceplaybooks
# Microsoft Security Solutions

Partners can help customers protect against breaches, detect breaches, and respond to breaches with a comprehensive security solution. The overarching security environment of the enterprise includes a mix of solutions provided by many different vendors. This playbook focuses coverage on Microsoft products and services that play a critical role in securing this environment.

## + Identity and Access Management

| Safeguard and manage identity | Azure Key Vault  
| Detect and respond to identity-based threats | Azure Active Directory  
| Protect against password attacks | Azure Active Directory  

## + Information Protection

| Manage cloud application usage | Microsoft Cloud App Security  
| Protect against data leakage | Azure Information Protection  
| Protect against malware and phishing attacks | Azure Information Protection  
| Respond to security incidents | Office 365 Advanced Threat Protection  

## + Threat Protection

| Protect against malware attacks | Windows Defender  
| Manage mobile devices and applications | Windows Defender Device Guard  
| Respond to malware attacks | UEFI Secure Boot and the Trusted Boot Process  

## + Security Management

| Detect and respond to threats | Azure Sentinel  
| Protect against threats | Azure Security Center  
| Gain visibility into security health | Azure Advisor  

## = Comprehensive Security Solution
Microsoft’s intelligent cloud offers smart, adaptive security solutions that does not hamper productivity, starting with a user authentication experience accessible from any device and threat detection tools that communicate with each other across the entire digital footprint and automate detection, investigation, and remediation.

**ZERO TRUST**
Cloud applications and the mobile workforce have redefined the security perimeter, and Microsoft has shared its guiding principles with its [Zero Trust security model](#), designed to more effectively adapt to the complexity of the modern workplace, by protecting people, devices, apps, and data wherever they’re located. In a Zero Trust model, every access request is strongly authenticated, authorized within policy constraints and inspected for anomalies before granting access. Partners are encouraged to use this model to build Zero Trust into their customers’ organizations.

Source: [Zero Trust reference architecture](#)
Partner Practice Development Framework

The partner practice development framework defines how to take a practice from concept to growth in five stages. It is the foundation of this playbook, and each phase of the framework is covered in a dedicated chapter.

- **Define Strategy**
  Define your offer, benchmark your practice, and identify required resources.

- **Hire & Train**
  Hire talent, train resources, and complete certifications.

- **Operationalize**
  Prepare for launch with systems, tools, and processes in place.

- **Go to Market & Close Deals**
  Execute your sales and marketing strategy to find your first customers and close deals with winning proposals.

- **Optimize & Grow**
  Collect feedback, identify expansion opportunities, optimize your practice, grow partnerships, and refine your offer.
Define the Strategy

Security

aka.ms/practiceplaybooks
Executive Summary

Now that everyone understands the opportunity, it is time to build a strategy and determine which parts of a Security practice an organization will pursue.

We begin by providing an overview of the areas of expertise within the security practice: identity and access management, threat protection, information protection, and security management. A practice may have expertise in just one of these areas, across multiple, or all areas. For each area, we provide details about the nature of the business opportunity and the key Microsoft products and services leveraged in delivering solutions that capitalize on the opportunity.

Then we will guide everyone through the process of defining an offer and its value proposition. Simply stated, this is what partners will sell and why customers will want to buy it. Along the way we will review the four cloud business models (reselling, project services, managed services, and intellectual property), their respective profitability, and how partners can assess the profitability of their own practice. For project services, managed services, and intellectual property, we provide guidance on what other successful partners are selling, and recommendations on what to include in project services (e.g., delivering Secure Score workshops and providing planning and deployment services), managed services (e.g., providing managed security monitoring and remediation services), and intellectual property (e.g., packaging a practice and offering integrated security dashboards) offerings.

We will drill into how to price an offer base, including what pricing strategy to use to drive adoption of the offer, and how to minimize risk by establishing up-front fees and payment terms. The ultimate goal is to help partners build a solid business plan that addresses their team, marketing, sales, and financial aspects.

Then we dive deeper into sales to help define a pre-sales and post-sales engagement process, and how to compensate sales executives.

We will give a tour of the Microsoft Partner Network, the programs to leverage to grow a practice, how to earn competencies that yield additional benefits, and how to maximize the benefits from the program.

After that, we provide a head start in how to identify potential customers when starting a practice, as well as potential service offerings.

We’ll conclude this section by helping partners understand support — how to support customers, Microsoft’s support offerings, and the support-related benefits partners get from establishing competencies in the Microsoft Partner Network.

Top 4 things to do

Measure twice and cut once. Here are the top 4 things partners should absolutely do when defining a Security strategy.

- Define focus and value proposition
- Understand the security opportunity
- Define and design the solution offer
- Define a pricing strategy
Define the Practice Focus

Through a security practice, partners can help keep customers productive and secure — and their company data protected — on their favorite apps and devices with Microsoft solutions.

**IDENTITY AND ACCESS MANAGEMENT**

Help customers protect their identities and data. Use behavioral analysis to provide actionable insights and ensure that customers have a sound approach to manage users and groups, as well as secure access to on-premise and cloud apps.

**THREAT PROTECTION**

Build a practice that helps customers proactively guard against threats, identify breaches and threats using advanced analytics, and automate the response to threats enterprise-wide.

**INFORMATION PROTECTION**

Manage and protect corporate apps and data. Provide customers with mobile device management, mobile app management, and PC management capabilities. Enable employees with access from virtually anywhere on almost any device, while helping to keep corporate information secure and compliant.

**SECURITY MANAGEMENT**

Help customers manage the security of their enterprise-wide assets with centralized tooling, and help them establish a security operations center from which to monitor and manage.
Understanding the Security Practice

By developing a security practice, partners can help turn the potentially dizzying array of services, licensing options, and overlapping featuresets into a cohesive, comprehensive, and understandable security solution that enables customers to manage their security, protect their assets, and respond to security incidents.

The Identity & Access Management Opportunity

According to the Verizon 2019 Data Breach Investigations Report, 52% of all breaches featured hacking and 71% of breaches were financially motivated. Phishing attacks, the practice of sending fraudulent emails to get individuals to reveal personal information, are continuing to prove successful. In the same report, it was found that 32% of breaches involved phishing. The impact of phishing should not be lost as it represents the start of a negative chain of events: phishing is used to gain a foothold using malware, in which the stolen credentials are leveraged to increase the scope of the breach. The opportunity to help customers here should be plain — equip customers to better manage their identity and access controls, and stop breaches before they escalate in severity.
Consider using the following Microsoft products and services to develop solutions for a security practice focused on identity and access management:

| SAFEGUARD AND MANAGE IDENTITY | Azure Key Vault  
  | Azure Active Directory |
| DETECT AND RESPOND TO IDENTITY-BASED THREATS | Azure Active Directory  
  | Microsoft Cloud App Security  
  | Microsoft Advanced Threat Analytics |
| PROTECT AGAINST PASSWORD ATTACKS | Windows Hello for Business  
  | Windows Defender Credential Guard  
  | Multi-Factor Authentication for Office 365  
  | Azure Multi-Factor Authentication |
The Information Protection Opportunity

According to the 2019 Ponemon Institute Cost of a Data Breach study, the cost incurred for each lost or stolen record of sensitive data is now at $150, with the total consolidated cost of a data breach at $3.92 million. Meanwhile, according to the PWC Global State of Information Security Survey, the sources of security incidents perpetrated by current employees remains high, and that from business partners continues to rise. Additionally, 87% of organizations surveyed believe they do not yet have the sufficient budget to provide the levels of cybersecurity they desire, according to the EY Global Information Security Survey. All of this combines to create the demand for partners to improve their customers’ defense with information protection.

Consider using the following Microsoft products and services to develop solutions for a security practice focused on information protection:

| MANAGE CLOUD APPLICATION USAGE | Microsoft Cloud App Security |
| PROTECT AGAINST DATA LEAKAGE | Azure Information Protection  
Data Loss Prevention for Office 365  
Customer Lockbox for Office 365  
Windows Information Protection  
SQL Server/Azure SQL DB Transparent Data Encryption  
Azure Storage Service Encryption |
| PROTECT AGAINST MALWARE AND PHISHING ATTACKS | Office 365 Advanced Threat Protection |
| RESPOND TO SECURITY INCIDENTS | Office 365 Advanced Discovery  
Office 365 Advanced Data Governance |
The Threat Protection Opportunity

According to EY Global Information Security Survey, 22% of the organizations surveyed saw phishing as the top threat and 20% identified malware as their top threat. Additionally, these organizations identified zero-day attacks and targeted cyber attacks to steal financial information, disrupt or deface the organization, or steal intellectual property or data. Yet, in the same survey, only 35% of respondents said they have a threat intelligence program. In the Verizon 2019 Data Breach Investigation Report, the data confirms that the threats are still very real.

The threat protection opportunity is about enabling customers to remain constantly aware of the current threat landscape and identifying attackers — and the attacks they are using — before they cause damage.

Consider using the following Microsoft products and services to develop solutions for a security practice focused on threat protection:

| PROTECT AGAINST MALWARE ATTACKS | Windows Defender  
| Device Guard  
| UEFI Secure Boot and the Trusted Boot Process |
| MANAGE MOBILE DEVICES AND APPLICATIONS | Enterprise Mobility + Security  
| Mobile Device Management for Office 365  
| Microsoft Intune |
| RESPOND TO MALWARE ATTACKS | Microsoft Defender Advanced Threat Protection  
| Office 365 Advanced Threat Protection  
| Microsoft Intelligent Security Graph |

aka.ms/practiceplaybooks
The Security Management Opportunity

To proactively manage security, organizations should consider implementing a security operations center (SOC). This is a centralized unit designed to address organizational and technical security levels where staff monitors the site using advanced data processing technology. The cornerstone capability underpinning any such effort is a set of centralized tools for monitoring and management. Very few organizations today claim they have a mature security management posture, according to EY’s 2018-2019 Global Information Security Survey.

Consider using the following Microsoft products and services to develop solutions for a security practice focused on security management:

| DETECT AND RESPOND TO THREATS | Azure Sentinel  
| Azure Security Center  
| Azure Advisor  
| Microsoft Defender Advanced Threat Protection |
| PROTECT AGAINST THREATS | Microsoft Azure  
| Windows Server  
| Azure SQL Database Threat Detection  
| Microsoft Defender Advanced Threat Protection |
| GAIN VISIBILITY INTO SECURITY HEALTH | Azure Sentinel  
| Azure Security Center  
| Azure Network Watcher  
| Azure Monitor  
| Microsoft 365 Secure Score  
| Office 365 Advanced Threat Protection  
| Office 365 Threat Intelligence  
| Microsoft Cloud App Security |
Security Suites

One way to help customers make sense of the options and simplify their licensing is to guide them to an appropriate suite.

According to a 2016 study of 130 security partners conducted for Microsoft by MDC, a significant portion of security partners are in the early phases of selling security services. This represents an opportunity in the market for new entrants, and a growth opportunity for established participants.
Enterprise Mobility + Security (EM+S)

EM+S provides an identity-driven security solution that offers a holistic approach to the security challenges in this mobile-first, cloud-first era. It bundles five products to deliver a device-management and virtual identity management suite. The suite is offered in two tiers, EM+S E3 and EM+S E5 that offer the suite of services for a single per user price. Customers with EM+S E3 can also purchase the Identity & Threat Protection offering and Information Protection & Compliance offering simplifying the path to M365 E5, delivering cost savings over purchasing standalones.

**AZURE ACTIVE DIRECTORY PREMIUM**

Azure Active Directory Premium provides the single sign-on capability for the entire enterprise targeting resources both in the cloud and on-premises. At the E3 level, EM+S includes AAD Premium P1 which provides the secure single sign-on to cloud and on-premises apps, along with multi-factor authentication support (requiring further authentication via phone call, text message or mobile app verification), conditional access (based on group membership, geographic location and device state), and advanced security reporting. With the Identity & Threat Protection offering and at the EM+S E5 level, AAD Premium P2 is included that builds on AAD Premium P1 by adding more advanced protection for users (such as conditional access based on sign-in or user risk) and support for privileged identities (which enables on-demand, “just in time” privilege escalation for administrative access).

**MICROSOFT INTUNE**

Microsoft Intune is included for both EM+S E3 and E5 to provide mobile device and app management capabilities to protect corporate apps and data on any device — even when users bring their own personal devices.

**AZURE INFORMATION PROTECTION PREMIUM**

Azure Information Protection Premium enables control over the access to files and emails across cloud and on-premises, and is provided at two levels in EM+S. Within EM+S E3, Azure Information Protection Premium P1 is provided and includes support for file and email encryption and cloud based tracking of files. The Identity & Threat Protection Offering and EM+S E5 provides Azure Information Protection Premium P2, which layers on automated, intelligent classification and encryption for files and emails.

**MICROSOFT CLOUD APP SECURITY**

Microsoft Cloud App Security brings the security capabilities traditionally available to on-premises systems to SaaS cloud applications like DropBox, Office 365, G Suite, and Salesforce, and enables deeper visibility, comprehensive controls, and enhanced protection against cloud security issues. Cloud App Security is included in the Identity & Threat Protection offering and with EM+S E5.

**ADVANCED THREAT ANALYTICS**

Advanced Threat Analytics is an on-premises platform that helps protect the enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior. It is available in both EM+S E3 and E5.
## Microsoft 365 Enterprise Plan Overview

<table>
<thead>
<tr>
<th>Category</th>
<th>M365 F1</th>
<th>M365 E3&lt;sup&gt;1&lt;/sup&gt;</th>
<th>M365 E5&lt;sup&gt;1&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Productivity &amp; Collaboration</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office client apps (Word, Excel, PowerPoint, OneNote, Access)</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Microsoft Teams, Skye for Business Online, Office Mobile apps, email &amp; calendar (Outlook, Exchange), social &amp; internet (SharePoint, Yammer)</td>
<td></td>
<td>2</td>
<td>●</td>
</tr>
<tr>
<td><strong>Device &amp; App Management</strong></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Microsoft Intune, Windows AutoPilot, Fine Tuned User Experience, and Windows Analytics Device Health</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Microsoft Advanced Threat Analytics, Windows Defender Antivirus, Device Guard&lt;sup&gt;3&lt;/sup&gt;, Azure Active Directory Premium Plan 1, Windows Hello, Credential Guard and Direct Access, Windows Information Protection &amp; BitLocker, Azure Information Protection Plan 1</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Office 365 Data Loss Prevention</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Information Protection &amp; Compliance (O365 Advanced Compliance, Azure Information Protection Plan 2)</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td><strong>Voice</strong></td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Audio Conferencing, Phone System</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td><strong>Analytics</strong></td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>MyAnalytics</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Delve</td>
<td></td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Power BI Pro</td>
<td></td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>

<sup>1</sup>Productivity Server Rights – SharePoint, Exchange and Skype for Business productivity server rights for M365 E3 & E5 customers (Hybrid Rights unavailable in CSP Channel).

<sup>2</sup>Use of Office Mobile apps limited to devices with integrated screens 10.1" diagonally or less. Skype for Business Basic client only. 2GB Inbox, no voicemail. Meetings are join only, 1:1 audio/video calls are supported, no desktop or app sharing. Cannot be site administrators, no site mailbox, no personal site, cannot create forms.

<sup>3</sup>Not available on Windows 10 Enterprise E3 in S mode.
Microsoft 365

Microsoft 365 is a complete, intelligent solution to empower employees to be creative and work together, securely.

<table>
<thead>
<tr>
<th>Microsoft 365 Enterprise</th>
<th>Microsoft 365 Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Available as Microsoft 365 E3 and Microsoft 365 E5 offerings</td>
<td>• Designed for small and midsize businesses with up to 300 users</td>
</tr>
</tbody>
</table>

MICROSOFT 365 AND THE INTELLIGENT CLOUD HELP CUSTOMERS

- Protect, detect, and respond to today’s modern security landscape, which presents new risks and opportunities
- Drive digital transformation that includes everyone, from the executive office to the frontline worker

As a fully integrated, end-to-end solution, Microsoft 365 provides unique customer value, which in turn creates amazing new partner opportunities.

ENGAGE CUSTOMERS IN STRATEGIC CONVERSATIONS

Microsoft 365 will enable partners to engage customers in strategic conversations around:

- Advanced Security
- Compliance & GDPR
- Collaboration & Cloud Voice
- Microsoft 365 powered device
- Firstline Workers

Leverage Microsoft 365 to spark dialogue with customers about the growing threat of cyber attacks, the enterprise need for the advanced security in Microsoft 365, and the importance of protecting privacy, especially in context of compliance regulations. Discuss collaboration and what the teams of today need to get work done together, what modern desktop and devices have to offer businesses, and how Microsoft 365 helps to empower firstline workers.

GROW BUSINESS WITH MICROSOFT 365

- **Grow with Managed Services.** Modernize the customer’s environment leading with security
- **Differentiate offerings.** Offer advanced enterprise services based on intelligence capabilities of Microsoft 365
- **Increase deal size.** Elevate the customer conversation by leveraging the broad value of Microsoft 365

NEW REVENUE AND SERVICE DELIVERY OPPORTUNITIES

Digital transformation is fundamentally changing the way companies use technology to empower employees, optimize operations, transform products, and engage customers. Partners and their customers no longer think about solutions as individual workloads, but as a coordinated multi-year journey to achieve business objectives. According to research by Forrester¹, Microsoft 365 is central to customers' digital transformation initiatives, and with Microsoft 365, partners stand to make:

- Nearly $1500 in revenue per user²
- Over $700 in margin per user²

¹ A commissioned study conducted by Forrester Consulting on behalf of Microsoft.

² Over three years based on a 5,000 seat deployment.
Leverage New Ways to Upsell Microsoft 365 E5

<table>
<thead>
<tr>
<th>Category</th>
<th>O365 ATP Plan 2(^1)</th>
<th>O365 Advanced Compliance</th>
<th>Azure Information Protection Plan 2</th>
<th>M365 E5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsoft Cloud App Security(^2)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure Active Directory Plan 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Azure Advanced Threat Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Defender Advanced Threat Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^1\) Consolidates O365 Threat Intelligence and O365 ATP Plan 1 value

\(^2\) Consolidates O365 CAS and MCAS value
Define and Design the Solution Offer

Understand the Cloud Business Models

It’s key to understand that not all revenue streams are equal.

THERE ARE FOUR WAYS TO MAKE MONEY SELLING CLOUD:
- Resale
- Project Services
- Managed Services
- Packaged IP

Partners that focus almost entirely on product revenue have the biggest barrier, and typically see margins in the range of 5–20%. This is because the margins for this revenue line are tied to vendor incentives. These partners are subject to changes in strategy and the desire to fund programs, and have the least control over their own destiny.

Project services typically drive a range of approximately 35% gross margin, but this has been under pressure for some time. This is a result of little differentiation in the channel, which has caused billable price points to hold steady over the past five or more years, while increasing salary and benefit costs of consultants and inflation have eroded profitability.

As a result, aggressive and entrepreneurial members of the channel have adapted and gone after the higher margin opportunities of managed services, which generate on average 45% gross margin and packaged IP, which often exceeds 70%.

It’s these partners who are setting themselves up to be rewarded. The mergers and acquisition space is quite active. The partners who have gravitated toward the recurring revenue lines and realizing healthy growth are being presented with much higher valuations. This can have a dramatic increase in the cash event of the company and overall shareholder value — far higher than what a traditional partner focused on product and billable services can realize.

A business plan is a critical asset that can help partners envision and think through the details of their practice, identify gaps that need to be addressed, and explain the fundamentals of their practice to others. Leverage the Cloud Business Plan guide for details, profitability scenario overviews, business plan templates, and financial models.

Read on to understand what types of project services, managed services, and intellectual property partners should consider in a security practice.
Understanding Project Based Services

Building a new practice is a daunting challenge. It is not that different from starting a business from scratch. Just like any business venture, it’s important to start with a vision of what the business will do, what problems it will solve, and how it will make money.

Let’s start off with the premise that there are four categories of offerings that we’ll work from: project based services, managed services, intellectual property, and vertical solutions.

In the Microsoft Cloud Practice Development Study, 484 partners that identified as having a security practice were asked what project services they offer within their practice. The results are below. Consider this data when designing project based offerings.

<table>
<thead>
<tr>
<th>PROJECT BASED OFFERINGS</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Migration Planning</td>
<td>64%</td>
</tr>
<tr>
<td>Configuration</td>
<td>63%</td>
</tr>
<tr>
<td>Help-Desk Support</td>
<td>52%</td>
</tr>
<tr>
<td>Data Loss Prevention &amp; Systems Integration</td>
<td>51%</td>
</tr>
<tr>
<td>Patch Management</td>
<td>50%</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>48%</td>
</tr>
<tr>
<td>Office Client Deployment</td>
<td>48%</td>
</tr>
<tr>
<td>Deployment Services</td>
<td>46%</td>
</tr>
<tr>
<td>Data Migration Management</td>
<td>43%</td>
</tr>
<tr>
<td>Enable Multi-Factor Authentication</td>
<td>43%</td>
</tr>
<tr>
<td>Identity and Access Control Enablement</td>
<td>42%</td>
</tr>
<tr>
<td>Cloud Readiness Assessment</td>
<td>42%</td>
</tr>
<tr>
<td>Solution Support &amp; Training</td>
<td>42%</td>
</tr>
<tr>
<td>Health Checks</td>
<td>41%</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>40%</td>
</tr>
<tr>
<td>Proof of Concept</td>
<td>38%</td>
</tr>
<tr>
<td>Auding, Security &amp; Compliance Assessments</td>
<td>37%</td>
</tr>
<tr>
<td>Activity and Log Audit Management</td>
<td>37%</td>
</tr>
<tr>
<td>Cloud Solution Costing &amp; Spend Optimization</td>
<td>35%</td>
</tr>
<tr>
<td>Solution Configuration &amp; Customization</td>
<td>35%</td>
</tr>
<tr>
<td>Policy Recommendation &amp; Improvement</td>
<td>33%</td>
</tr>
<tr>
<td>Password Complexity Management</td>
<td>32%</td>
</tr>
<tr>
<td>User Monitoring</td>
<td>31%</td>
</tr>
<tr>
<td>Threat Detection &amp; Migration Enablement</td>
<td>30%</td>
</tr>
<tr>
<td>Cyber Security Risk Assessment</td>
<td>29%</td>
</tr>
<tr>
<td>Information Protection Configuration</td>
<td>29%</td>
</tr>
<tr>
<td>Solution Analysis Scope &amp; Design</td>
<td>28%</td>
</tr>
<tr>
<td>User Enablement</td>
<td>28%</td>
</tr>
<tr>
<td>Security &amp; Compliance Enablement</td>
<td>27%</td>
</tr>
<tr>
<td>User Training &amp; Customer Self Portal &amp; Mentoring</td>
<td>24%</td>
</tr>
<tr>
<td>Data Leakage Prevention</td>
<td>23%</td>
</tr>
<tr>
<td>Device Procurement &amp; Deployment</td>
<td>23%</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>23%</td>
</tr>
<tr>
<td>Custom Application Development</td>
<td>22%</td>
</tr>
<tr>
<td>Incidence Response Management</td>
<td>21%</td>
</tr>
<tr>
<td>Data Classification &amp; Data Governance</td>
<td>19%</td>
</tr>
<tr>
<td>Training on Azure or Microsoft Security Products</td>
<td>19%</td>
</tr>
<tr>
<td>Security-Penetration Testing</td>
<td>18%</td>
</tr>
</tbody>
</table>
REVENUE

<table>
<thead>
<tr>
<th>Revenue Category</th>
<th>Total Median (n=464)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$48,946</td>
</tr>
</tbody>
</table>

BY CUSTOMER FOCUS

<table>
<thead>
<tr>
<th>Customer Focus</th>
<th>Total Median (n=464)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMB (n=401)</td>
<td>$45,569</td>
</tr>
<tr>
<td>Enterprise (n=63)</td>
<td>$541,965</td>
</tr>
</tbody>
</table>

When creating project services, research with partners emphasized the importance of targeting the enterprise customer to attain significantly higher per-project revenue.

Source: Microsoft Cloud Practice Development Study, MDC Research, June 2017.

PROJECT SERVICES BY REGION

<table>
<thead>
<tr>
<th>Project Services by Region</th>
<th>Total n=484</th>
<th>APAC n=24*</th>
<th>Canada n=18*</th>
<th>CEE n=27*</th>
<th>Germany n=36</th>
<th>LATAM n=41</th>
<th>MEA n=32</th>
<th>UK n=43</th>
<th>US n=119</th>
<th>WE n=103</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Migration Planning</td>
<td>64%</td>
<td>63%</td>
<td>72%</td>
<td>41%</td>
<td>81%</td>
<td>49%</td>
<td>69%</td>
<td>72%</td>
<td>72%</td>
<td>57%</td>
</tr>
<tr>
<td>Configuration</td>
<td>63%</td>
<td>58%</td>
<td>67%</td>
<td>56%</td>
<td>78%</td>
<td>59%</td>
<td>63%</td>
<td>53%</td>
<td>70%</td>
<td>66%</td>
</tr>
<tr>
<td>Help-Desk Support</td>
<td>52%</td>
<td>58%</td>
<td>61%</td>
<td>37%</td>
<td>50%</td>
<td>22%</td>
<td>66%</td>
<td>58%</td>
<td>65%</td>
<td>51%</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>51%</td>
<td>54%</td>
<td>44%</td>
<td>59%</td>
<td>47%</td>
<td>56%</td>
<td>63%</td>
<td>47%</td>
<td>55%</td>
<td>51%</td>
</tr>
<tr>
<td>Systems Integration</td>
<td>51%</td>
<td>58%</td>
<td>61%</td>
<td>48%</td>
<td>64%</td>
<td>34%</td>
<td>44%</td>
<td>47%</td>
<td>58%</td>
<td>49%</td>
</tr>
<tr>
<td>Patch Management</td>
<td>50%</td>
<td>54%</td>
<td>56%</td>
<td>41%</td>
<td>61%</td>
<td>27%</td>
<td>53%</td>
<td>56%</td>
<td>63%</td>
<td>45%</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>48%</td>
<td>58%</td>
<td>39%</td>
<td>41%</td>
<td>56%</td>
<td>41%</td>
<td>59%</td>
<td>42%</td>
<td>46%</td>
<td>51%</td>
</tr>
<tr>
<td>Office Client Deployment</td>
<td>48%</td>
<td>46%</td>
<td>44%</td>
<td>33%</td>
<td>47%</td>
<td>46%</td>
<td>63%</td>
<td>51%</td>
<td>53%</td>
<td>45%</td>
</tr>
<tr>
<td>Deployment Services</td>
<td>46%</td>
<td>54%</td>
<td>61%</td>
<td>26%</td>
<td>58%</td>
<td>39%</td>
<td>44%</td>
<td>56%</td>
<td>52%</td>
<td>34%</td>
</tr>
<tr>
<td>Data Migration Management</td>
<td>43%</td>
<td>50%</td>
<td>50%</td>
<td>26%</td>
<td>47%</td>
<td>32%</td>
<td>47%</td>
<td>49%</td>
<td>54%</td>
<td>36%</td>
</tr>
<tr>
<td>Enable Multi-Factor</td>
<td>43%</td>
<td>42%</td>
<td>61%</td>
<td>19%</td>
<td>58%</td>
<td>27%</td>
<td>34%</td>
<td>53%</td>
<td>57%</td>
<td>34%</td>
</tr>
<tr>
<td>Authentication</td>
<td>42%</td>
<td>42%</td>
<td>56%</td>
<td>19%</td>
<td>50%</td>
<td>27%</td>
<td>38%</td>
<td>44%</td>
<td>48%</td>
<td>47%</td>
</tr>
<tr>
<td>Identity and Access</td>
<td>42%</td>
<td>42%</td>
<td>56%</td>
<td>19%</td>
<td>50%</td>
<td>27%</td>
<td>38%</td>
<td>44%</td>
<td>48%</td>
<td>47%</td>
</tr>
<tr>
<td>Control Enablement</td>
<td>42%</td>
<td>42%</td>
<td>56%</td>
<td>19%</td>
<td>50%</td>
<td>27%</td>
<td>38%</td>
<td>44%</td>
<td>48%</td>
<td>47%</td>
</tr>
<tr>
<td>Cloud Readiness Assessment</td>
<td>42%</td>
<td>50%</td>
<td>56%</td>
<td>15%</td>
<td>58%</td>
<td>22%</td>
<td>38%</td>
<td>60%</td>
<td>55%</td>
<td>29%</td>
</tr>
<tr>
<td>Solution Support &amp; Training</td>
<td>42%</td>
<td>42%</td>
<td>50%</td>
<td>33%</td>
<td>22%</td>
<td>29%</td>
<td>50%</td>
<td>33%</td>
<td>52%</td>
<td>41%</td>
</tr>
<tr>
<td>Health Checks</td>
<td>41%</td>
<td>50%</td>
<td>39%</td>
<td>37%</td>
<td>44%</td>
<td>24%</td>
<td>31%</td>
<td>67%</td>
<td>52%</td>
<td>32%</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>40%</td>
<td>42%</td>
<td>39%</td>
<td>11%</td>
<td>58%</td>
<td>12%</td>
<td>31%</td>
<td>53%</td>
<td>55%</td>
<td>38%</td>
</tr>
<tr>
<td>Proof of Concept</td>
<td>38%</td>
<td>42%</td>
<td>33%</td>
<td>19%</td>
<td>61%</td>
<td>37%</td>
<td>38%</td>
<td>26%</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Auditing, Security</td>
<td>37%</td>
<td>38%</td>
<td>33%</td>
<td>33%</td>
<td>28%</td>
<td>37%</td>
<td>38%</td>
<td>51%</td>
<td>39%</td>
<td>39%</td>
</tr>
<tr>
<td>&amp; Compliance Assessments</td>
<td>37%</td>
<td>29%</td>
<td>33%</td>
<td>37%</td>
<td>28%</td>
<td>37%</td>
<td>44%</td>
<td>35%</td>
<td>44%</td>
<td>32%</td>
</tr>
<tr>
<td>Activity and Log Audit</td>
<td>37%</td>
<td>29%</td>
<td>33%</td>
<td>37%</td>
<td>28%</td>
<td>37%</td>
<td>44%</td>
<td>35%</td>
<td>44%</td>
<td>32%</td>
</tr>
<tr>
<td>Management</td>
<td>35%</td>
<td>42%</td>
<td>39%</td>
<td>26%</td>
<td>28%</td>
<td>24%</td>
<td>38%</td>
<td>37%</td>
<td>53%</td>
<td>21%</td>
</tr>
</tbody>
</table>

aka.ms/practiceplaybooks
### DEFINE THE STRATEGY

<table>
<thead>
<tr>
<th>Category</th>
<th>35%</th>
<th>42%</th>
<th>44%</th>
<th>26%</th>
<th>31%</th>
<th>27%</th>
<th>31%</th>
<th>33%</th>
<th>45%</th>
<th>26%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Configuration/Customization</td>
<td>33%</td>
<td>38%</td>
<td>61%</td>
<td>26%</td>
<td>33%</td>
<td>12%</td>
<td>41%</td>
<td>26%</td>
<td>41%</td>
<td>32%</td>
</tr>
<tr>
<td>Policy Recommendation and Improvement</td>
<td>32%</td>
<td>33%</td>
<td>28%</td>
<td>22%</td>
<td>19%</td>
<td>20%</td>
<td>31%</td>
<td>49%</td>
<td>46%</td>
<td>27%</td>
</tr>
<tr>
<td>Password Complexity Management</td>
<td>31%</td>
<td>29%</td>
<td>11%</td>
<td>19%</td>
<td>28%</td>
<td>24%</td>
<td>31%</td>
<td>42%</td>
<td>43%</td>
<td>27%</td>
</tr>
<tr>
<td>Security and Compliance Assessment</td>
<td>31%</td>
<td>29%</td>
<td>39%</td>
<td>26%</td>
<td>19%</td>
<td>22%</td>
<td>22%</td>
<td>30%</td>
<td>46%</td>
<td>25%</td>
</tr>
<tr>
<td>Thin Detection &amp; Mitigation Enablement</td>
<td>30%</td>
<td>33%</td>
<td>17%</td>
<td>15%</td>
<td>31%</td>
<td>7%</td>
<td>31%</td>
<td>44%</td>
<td>43%</td>
<td>26%</td>
</tr>
<tr>
<td>Cyber Security Risk Assessment</td>
<td>29%</td>
<td>38%</td>
<td>22%</td>
<td>19%</td>
<td>22%</td>
<td>22%</td>
<td>19%</td>
<td>42%</td>
<td>42%</td>
<td>23%</td>
</tr>
<tr>
<td>Information Protection Configuration</td>
<td>28%</td>
<td>46%</td>
<td>22%</td>
<td>15%</td>
<td>17%</td>
<td>20%</td>
<td>28%</td>
<td>19%</td>
<td>45%</td>
<td>24%</td>
</tr>
<tr>
<td>Security and Compliance Enablement</td>
<td>28%</td>
<td>46%</td>
<td>39%</td>
<td>22%</td>
<td>17%</td>
<td>16%</td>
<td>35%</td>
<td>34%</td>
<td>22%</td>
<td></td>
</tr>
<tr>
<td>User Training and Customer Self-Serve Portal</td>
<td>27%</td>
<td>21%</td>
<td>6%</td>
<td>11%</td>
<td>33%</td>
<td>22%</td>
<td>22%</td>
<td>40%</td>
<td>35%</td>
<td>23%</td>
</tr>
<tr>
<td>Mentoring</td>
<td>24%</td>
<td>21%</td>
<td>39%</td>
<td>19%</td>
<td>14%</td>
<td>7%</td>
<td>25%</td>
<td>16%</td>
<td>42%</td>
<td>17%</td>
</tr>
<tr>
<td>Data Leakage Prevention</td>
<td>24%</td>
<td>25%</td>
<td>28%</td>
<td>19%</td>
<td>22%</td>
<td>20%</td>
<td>22%</td>
<td>26%</td>
<td>32%</td>
<td>19%</td>
</tr>
<tr>
<td>Device Procurement and Deployment</td>
<td>23%</td>
<td>33%</td>
<td>56%</td>
<td>11%</td>
<td>31%</td>
<td>5%</td>
<td>22%</td>
<td>23%</td>
<td>35%</td>
<td>9%</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>23%</td>
<td>21%</td>
<td>17%</td>
<td>22%</td>
<td>19%</td>
<td>15%</td>
<td>19%</td>
<td>33%</td>
<td>32%</td>
<td>18%</td>
</tr>
<tr>
<td>Custom Application Development</td>
<td>22%</td>
<td>29%</td>
<td>33%</td>
<td>30%</td>
<td>22%</td>
<td>10%</td>
<td>13%</td>
<td>12%</td>
<td>29%</td>
<td>22%</td>
</tr>
<tr>
<td>Incidence Response Management</td>
<td>21%</td>
<td>33%</td>
<td>33%</td>
<td>11%</td>
<td>11%</td>
<td>12%</td>
<td>16%</td>
<td>19%</td>
<td>31%</td>
<td>19%</td>
</tr>
<tr>
<td>Data Classification and Data Governance</td>
<td>19%</td>
<td>21%</td>
<td>28%</td>
<td>7%</td>
<td>14%</td>
<td>15%</td>
<td>22%</td>
<td>19%</td>
<td>28%</td>
<td>14%</td>
</tr>
<tr>
<td>Training on Azure or Microsoft Security Services</td>
<td>19%</td>
<td>8%</td>
<td>17%</td>
<td>7%</td>
<td>17%</td>
<td>15%</td>
<td>19%</td>
<td>14%</td>
<td>29%</td>
<td>16%</td>
</tr>
<tr>
<td>Security-Penetration Testing</td>
<td>18%</td>
<td>8%</td>
<td>0%</td>
<td>15%</td>
<td>19%</td>
<td>15%</td>
<td>16%</td>
<td>16%</td>
<td>29%</td>
<td>14%</td>
</tr>
<tr>
<td>Productivity Cloud App Usage Management</td>
<td>17%</td>
<td>17%</td>
<td>11%</td>
<td>15%</td>
<td>14%</td>
<td>12%</td>
<td>22%</td>
<td>12%</td>
<td>28%</td>
<td>9%</td>
</tr>
<tr>
<td>Security Operations Center Management</td>
<td>13%</td>
<td>8%</td>
<td>6%</td>
<td>11%</td>
<td>11%</td>
<td>7%</td>
<td>16%</td>
<td>12%</td>
<td>18%</td>
<td>12%</td>
</tr>
</tbody>
</table>

Source: Microsoft Cloud Practice Development Study, MDC Research, June 2017

aka.ms/practiceplaybooks
Deliver A Workshop

Delivering a workshop that provides assessments, training, or planning services is a great project services approach to launching a new customer engagement.

**ENTERPRISE MOBILITY STRATEGY & PLANNING WORKSHOP**

Most customers today have already started taking the cloud seriously. However, not every customer is savvy enough to build a robust cloud strategy. From the enterprise mobility perspective, many don’t have granular visibility into what data employees are storing on their devices, if corporate data is being used on unknown and unmanaged SaaS applications, or how to protect their files and data from being accidently or deliberately distributed. Others, while aware of these challenges, don’t know where to start and are unsure of how ready their staff, systems, tools, and processes are for true enterprise mobility.

This is why most managed services engagements and significant enterprise mobility projects begin with an enterprise mobility assessment. Microsoft has created the Microsoft Security Assessment for partners to deliver this assessment in a workshop form. This one-day workshop is designed to help enterprise customers envision and plan Microsoft’s solutions for mobilizing, managing, and securing enterprise mobility.

Solution architects can use the workshop during a pre-sales effort to scope and size an engagement to help the customer achieve their mobility goals.

---

**AT THE END OF THE WORKSHOP:**

- The customer will have a vision of how Enterprise Mobility can help their organization realize their mobility goals and drive business impact.
- The partner will have sufficient knowledge to write a proposal for a mobility engagement (e.g., Enterprise Mobility Suite Pilot, Dynamic Identity Framework, Universal Application Development).

**TARGET CUSTOMERS FOR THIS OFFERING INCLUDE:**

- Customers not yet convinced that EMS is right (e.g., BDMs are not engaged).
- Customers who own licenses but have no deployment plan.
MICROSOFT SECURE SCORE WORKSHOP

The Microsoft Security Assessment includes the Microsoft Secure Score workshop which is a structured engagement that uses the Microsoft Secure Score tool to evaluate and prioritize the tenant security settings of an organization.

Microsoft Secure Score provides a numerical summary of a customer’s security posture within Office 365 based on system configurations, user behavior, and other security-related measurements. It is not an absolute measurement of how likely a system or data will be breached; rather, it represents the extent to which security controls available in Office 365 have been adopted that can help offset the risk of being breached.

The Microsoft Secure Score workshop can help partners create and present to customers a customized, prioritized, and actionable roadmap based on the recommendations from the Microsoft Secure Score tool. The agenda typically consists of an up to two-hour, remote kick-off meeting followed by a two-day, on-site assessment workshop.

The artifacts within the Microsoft Security Assessment are intended to be customized so that the engagement is aligned to a partner organization’s own value proposition, workflows, delivery methodologies, related work streams, and offerings. The outcome of the Microsoft Security Assessment is to assist with the development of a roadmap of actionable customer recommendations used to drive additional project-based work. Alternately, it can be used to inform a repeatable lifecycle of security management tasks within a managed service offering.

Leverage the Microsoft Security Assessment, available at: https://aka.ms/M365securityassessment.

aka.ms/practiceplaybooks
“Our biggest success basically is that we introduce or we analyze our customers’ security level by implementing or by taking them through a secure score analysis, and based on that, doing all different sorts of recommendations.”

DANNY BURLAGE, Founder & CTO Wortell
Enable and Support Deployment

Offer a set of project services that revolves around enabling customer use of security products and cloud services, and deployment support.

ENABLE HYBRID IDENTITY

Managing identity is just as important in the public cloud as it is on premises. To help with this, Azure supports several different cloud identity technologies:

- Run Windows Server Active Directory (commonly called AD) in the cloud using virtual machines created with Azure Virtual Machine. This approach makes sense when using Azure to extend an on-premises datacenter into the cloud.
- Use Azure Active Directory to give users single sign-on to Software as a Service (SaaS) applications. Microsoft’s Office 365 uses this technology, for example. Applications running on Azure or other cloud platforms can also use it.
- Applications running in the cloud or on-premises can use Azure Active Directory Access Control to let users log in using identities from Facebook, Google, Microsoft, and other identity providers.

SOME OF THE KEY CUSTOMER CHALLENGES AND QUESTIONS PARTNERS MAY FACE ARE:

- Is Azure Active Directory secure?
- Is it safe to deploy Active Directory in an Azure Virtual Machine?
- How can I enable single-sign-on with my existing Windows Server Active Directory domains and my resources in Azure?
- Can I enable single-sign-on with other cloud-based SaaS services?
- Do I need to deploy Active Directory Federation Services?
HOW AZURE ACTIVE DIRECTORY CAN HELP

<table>
<thead>
<tr>
<th>USER ACCESS MANAGEMENT</th>
<th>USER TAGGING &amp; CHANGE MANAGEMENT</th>
<th>SINGLE-SIGN-ON</th>
<th>MULTI-FACTOR AUTHENTICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>This is a simple but important aspect of ID management that gives admins the power to identify and control the state of users logged in to the network. MSPs, on their customers’ behalf, can add or delete users, query or filter users, set access policies, and enforce strong authentication when users access resources. This can be done using CSP Partner Center and Azure Portal.</td>
<td>This allows the use of Azure tags and to manage the logging of all user activity on Azure. Maintain multiple Azure subscriptions, as well as role-based access, for individual users for specific subscriptions and specific Azure resources.</td>
<td>This enables customer to have access to their resources by using a single set of user credentials and a unified authentication method across Azure, hosted infrastructure, on-prem infrastructure and other SaaS apps. Free customers from multiple authentication processes for accessing different apps.</td>
<td>A method of ID authentication that requires more than one verification process (e.g., phone verification), adding a valuable second layer of security to signing in and completing any transactions. MSPs can provide improved application security with Microsoft Azure Active Directory Multi-Factor Authentication (MFA).</td>
</tr>
</tbody>
</table>

Enabling hybrid identity is a foundational step in for many organizations’ digital transformation.

RESOURCES:

- [What is Azure Active Directory](#)
- [Deploying a Hybrid Identity Solution](#)
- [How to Deploy ADFS in Azure](#)
- [Azure AD Domain Services](#)
PROVIDE PLANNING & DEPLOYMENT SERVICES FOR PROTECTING IDENTITIES WITH WINDOWS HELLO FOR BUSINESS & CREDENTIAL GUARD

Passwords are a burden on users and a liability to the enterprise. Enable enterprise customers to modernize authentication by helping them plan and deploy Windows Hello for Business.

Users forget their passwords. Moreover, a Security Week survey found that 75% of individuals use only three or four passwords across all of their accounts. This means users will tend to use the same password for authentication against both personal and corporate assets, making corporate assets as easy to compromise as the personal asset having the weakest security.

Once authenticated on a device, without any additional measures, the tokens that device uses to authenticate with other enterprise assets can be compromised and reused, effectively giving an attacker the privileges of the user without knowing the password.
Multifactor authentication is the right approach, but as it is deployed today presents an additional burden on users, so its use is only applied to specific assets that require more stringent security instead of being applied universally.

Windows Hello for Business provides users a natural approach to multi-factor authentication and in a way in which they will never forget their password because the user’s own biometrics (via facial recognition or fingerprints) and device (via a certificate issued to the device during setup) combined constitute the password. The user simply sits within view of the device camera or presses the fingerprint reader on the device. The way Windows Hello is deployed yields breach-, theft-, and phishing-proof identities that can be used to provide single sign-on to resources on-premises, on the web, and to devices by authorizing against user identities stored in Azure Active Directory.
AUGMENT CREDENTIAL PROTECTION WITH CREDENTIAL GUARD

Credential Guard prevents attackers from being able to retrieve credentials from operating system memory by maintaining them in a virtualized environment that is only accessible by privileged system software, and is not directly accessible by privileged users. Credential Guard works to protect derived credentials used at logon time including NTLM hashes (one way functions) and Kerberos credentials (usernames and passwords, long-lived keys and ticket-granting ticket session keys). Unauthorized access to these secrets can lead to credential theft attacks, such as Pass-the-Hash or Pass-The-Ticket. Credential Guard protects against these types of attacks.

Partners should guide their customers to combine Credential Guard with Windows Hello for Business and Windows Server 2016 for comprehensive credential protection. Use of Windows Hello ensures that there are no usernames or passwords to phish and protects private keys from extraction, and Credential Guard protects derived credentials after logon. On Windows Server 2016 domains, Credential Guard also protects the private key of domain joined devices and authentication policies can require users to sign on from specific domain joined devices which are protected with Credential Guard. Should Credential Guard be disabled, the result is a denial of service instead of a security breach as privileged users cannot logon and sensitive users remain protected.
Deploy Microsoft Intune

Microsoft Intune is a cloud-based enterprise mobility management (EMM) service that helps enable a mobile workforce to be productive when using their personal devices — all while keeping corporate data protected.

Intune provides mobile device management, mobile application management, and PC management capabilities from the cloud.

MOBILE DEVICE MANAGEMENT

Intune helps provide secure management of personal and corporate-owned devices across the most popular platforms, including Windows, Windows Phone, iOS, and Android. Users can be given the ability to enroll their own devices for management, as well as install corporate applications from the self-service company portal. In the case of large-scale device deployments, it is possible to simplify enrollment using Apple Configurator or an Intune service account. With Intune’s resource access policies, users can be restricted from accessing corporate resources on an unenrolled or noncompliant device. Device settings can be applied that can enable remote actions such as passcode reset, device lock, data encryption, or full wipe of a lost or stolen device.

MOBILE APPLICATION MANAGEMENT

Microsoft Intune enables control of corporate data at the app level without having to lock down the entire device. This is commonly an issue with employees using their own personal devices who feel IT is intruding on their device when locking it down. With Intune, manageability and data protection is built directly into the Office mobile apps employees are most familiar with, helping prevent leakage of company data by restricting actions such as copy, cut, paste, and save between Intune-managed apps and personal apps. Intune provides the flexibility to extend these capabilities to existing line-of-business apps with the Intune App Wrapping Tool and offers secure content viewing using the Intune Managed Browser, PDF Viewer, AV Player, and Image Viewer apps. Administrators also have the ability to deny specific applications or URL addresses from being accessed on a mobile device, and can push required apps automatically during enrollment. To further protect corporate information, wipe managed apps and related data on devices that are unenrolled can be selectively wiped, no longer compliant, lost, stolen, or retired from use.

aka.ms/practiceplaybooks
Deploy Advanced Threat Analytics

From detecting known malicious attacks to uncovering abnormal activity with machine learning and behavioral analytics, identify advanced persistent threats to the enterprise quickly — and take action swiftly — with Microsoft Advanced Threat Analytics.

WHAT IS ADVANCED THREAT ANALYTICS?

Advanced Threat Analytics (ATA) is an on-premises platform that can help protect an enterprise from advanced targeted attacks by automatically analyzing, learning, and identifying normal and abnormal entity (user, devices, and resources) behavior. It addresses the following:

**MALICIOUS ATTACKS**

ATA detects known malicious attacks almost as instantly as they occur.
- Pass-the-Ticket (PtT)
- Pass-the-Hash (PtH)
- Overpass-the-Hash
- Forged PAC (MS14-068)
- Golden Ticket
- Malicious replications
- Reconnaissance
- Brute Force
- Remote execution
- Malicious DPAPI

**ABNORMAL BEHAVIOR**

Behavioral analytics leverage machine learning to uncover questionable activities and abnormal behavior.
- Anomalous logins
- Unknown threats
- Password sharing
- Lateral movement

**SECURITY ISSUES & RISKS**

ATA identifies known security issues using world-class security research.
- Broken trust
- Weak protocols
- Known protocol vulnerabilities

HOW IS ATA UNIQUE?

The constant reporting of traditional security tools and sifting through them to locate the important and relevant alerts can get overwhelming. ATA provides a timeline view of events. The attack timeline is a clear, efficient, and convenient feed that surfaces the right things on a timeline, giving the power of perspective on the who, what, when, and how. ATA also provides recommendations for investigation and remediation for each suspicious activity.

For a complete list of the detections and their descriptions, please see [What Suspicious Activities can ATA Detect?](aka.ms/practiceplaybooks)

HOW IS ATA DEPLOYED?

ATA can be deployed either as an out-of-band solution by utilizing port mirroring without affecting the existing environment. ATA can also be deployed directly on the domain controllers without the added overhead of additional servers. Once deployed, ATA automatically starts analyzing and detecting suspicious activities.
Deploy Azure Sentinel

For security information and event management in the cloud.

Performing security operations for digitally transforming customers can be complex and costly as these operations typically have hybrid or multi-cloud environments. Existing enterprise-level security information and event management systems (SIEMs) can’t keep pace at cloud scale. Security operations teams are inundated with threat alerts, resulting in a high volume of time-wasting false positives and uninvestigated alerts.

Azure Sentinel is the first SIEM+SOAR (Security information and event management + Security Orchestration and Automated response) solution built into a public cloud platform to deliver intelligent security analytics across the enterprise and automatic scalability to meet ever evolving needs.

With native integration of machine learning, and User and Entity Behavioral Analysis (UEBA) models, Azure Sentinel can help detect threats quickly and reduce the noise and alert fatigue by up to 90%.

A BIRD’S-EYE VIEW ACROSS THE ENTIRE DIGITAL ESTATE

Azure Sentinel is a software-as-a-service solution for SIEM and security orchestration and automated response (SOAR). It uses Azure Monitor which is built on a proven and scalable log analytics database that ingests more than 10 petabytes every day and provides a very fast query engine that can sort through millions of records in seconds. With built-in connectors for collecting data, Azure Sentinel ingests security data from a wide range of data sources including Azure, SaaS applications including Office 365, networks, and on-premises systems, Linux, Windows, Amazon Web Services (AWS), other Microsoft services, and hardware.

It features native integration of Microsoft signals and support for industry standard log formats, SYSLOG, CEF, event forwarding, and API ingestion. It also allows partners to enrich signals and filter out false positives using known malicious IP addresses derived from the context of the trillions of diverse signals in the intelligent security graph. Azure Sentinel can also leverage Microsoft’s Graph Security API to integrate existing threat intelligence sources and tools.

Key benefits for partners and their customers include:

- Cloud-native with no infrastructure set-up and maintenance
- Intelligence from decades of Microsoft security experience
- Machine learning to make threat detection, analysis and response smarter and faster
- Integrated security orchestration and automation (SOAR) capabilities
- Real world investigation and remediation playbooks built by analysts in Microsoft’s SOC
- Ingest Microsoft 365 data for free, and analyze and draw correlations to deepen threat intelligence
- Rapidly spot anomalies without a mountain of false positives and respond to the real threats in minutes, not days

With an expected shortfall of 3.5M security professionals by 2021, partners will need a solution that empowers existing SecOps team to see the threats clearer and eliminate the distractions.

USE AZURE LIGHTHOUSE TO MANAGE SENTINEL WORKSPACES ACROSS MULTIPLE TENANTS

Azure Lighthouse provides capability for cross-tenancy management of Azure services for Managed Service Providers (MSPs) and organizations with multiple Azure tenants, all from a single Azure portal. Azure Lighthouse can be used to investigate an attack that targets several customers at once.

aka.ms/practiceplaybooks
Deploy Information Protection

With BitLocker and Windows Information Protection.

Information security starts with device protection, meaning a solution is needed that can protect data while it is at rest, even if the device is lost or stolen. Windows includes BitLocker for this scenario. BitLocker is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker achieves this by encrypting all user files and system files on the operating system drive, including the swap files and hibernation files, and checking the integrity of early boot components and boot configuration data.

**THE FOLLOWING REQUIREMENTS ARE FUNDAMENTAL TO INFORMATION PROTECTION:**

- Provide the means to identify personal versus corporate data, such that corporate data can be contained and securely wiped on demand.
- Provide the ability to prevent business data from leaking in an unauthorized way. For instance, with a solution that can prevent data from being copied from corporate documents into non-corporate locations.
- Ensure that business data can be securely shared with others within and outside of their organization.
**Windows Information Protection** (WIP) includes the functionality necessary to identify personal and business information, determine which apps have access to it, and provide the basic controls necessary to determine what users are able to do with business data, for example by imposing copy and paste restrictions. WIP is designed to work with the Office 365 and Azure Rights Management, which can help protect business data when it leaves the device or when it is shared with others, such as via printing restrictions or limiting email forwarding. WIP is enabled enterprise-wide by turning on policies in Microsoft Intune or System Center Configuration Manager. WIP is fully integrated within the experience users are already familiar with, and they can continue to use the apps that they, or IT, choose to access protected content. WIP does not require users to use special folders, change modes, use alternate apps or move into secure zones or partitions. Instead, the solution works completely behind the scenes and helps protect data wherever it lives on the device. It can continue the protection when data is copied to removable storage devices such as a thumb drives. The deployment and configuration of BitLocker and WIP represent important project services opportunities for partners.

To streamline the process of discovering, classifying, and labeling sensitive data in a customer’s database environment, **SQL Information Protection** offers a set of advanced services, aimed at protecting not just the database, but controlling access to the data within. Sensitive data can include anything from business, financial, healthcare, and personally identifiable information (PII), and SQL Information Protection can play a role in data-centric security scenarios such as auditing and alerting on anomalous access.
Deploy Azure Information Protection

Resources

- Overview of Azure Information Protection
- Data Classification for Azure
- Azure Information Protection Data Sheet
- See how Azure Information Protection Protects Company Data

Deploy Azure Information Protection

Azure Information Protection is a cloud-based solution that helps an organization classify, label, and protect its documents and emails. This can be done automatically by administrators who define rules and conditions, manually by users, or a combination in which users are given recommendations.

CLASSIFICATION AND LABELING

Classify data based on source, context, and content at the time of creation or modification, either automatically or manually. Once classified, a persistent label is embedded in the data and actions such as visual marking and encryption can be taken based on the classification and label.

PROTECTION AND USE RIGHTS

Protect sensitive data by encrypting it and allowing only authorized users access to the data. The protection is persistent to ensure data is protected at all times, regardless of where it’s stored or with whom it is shared.

TRACKING AND REPORTING

Track activities on shared files and revoke access if they encounter unexpected activities. The solution provides rich logs and reporting that can be leveraged for compliance and regulatory purposes.

SOME OF THE KEY CUSTOMER CHALLENGES AND QUESTIONS

- How should I classify data?
- How does Azure Information Protection help protect sensitive data?
- How can we securely collaborate inside and outside of our organization?
THREAT PROTECTION

Users can track activities on shared files and revoke access if they encounter unexpected activities. The solution provides rich logs and reporting that can be leveraged for compliance and regulatory purposes.
DEFINE THE STRATEGY

DEPLOY MICROSOFT CLOUD APP SECURITY

Bring the security capabilities traditionally available to on-premises systems to SaaS cloud applications like Dropbox, Office 365, G Suite and Salesforce, and get deeper visibility, comprehensive controls, and enhanced protection against cloud security issues.

SOME OF THE KEY CUSTOMER CHALLENGES AND QUESTIONS

- How do I identify applications in use by employees?
- How do I ensure that sensitive data is protected?
- How do I track access to shared files and compliance issues?

How Cloud App Security Helps

APP DISCOVERY

Discover all the cloud apps in a network, gain visibility into Shadow IT, and assess risk without installing agents. All information is gathered directly from the network firewalls and proxies by a log collector that runs on that network and receives logs over Syslog or FTP, and uploads them to Cloud App Security.
DATA CONTROL

Protect sensitive data by encrypting it and allowing only authorized users access to the data. The protection is persistent to ensure data is protected at all times, regardless of where it’s stored or with whom it’s shared. This is performed via the integrated app connectors to SaaS cloud application APIs. The following table illustrates the security capabilities available with each supported cloud application.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Office 365</th>
<th>Box</th>
<th>Okta</th>
<th>G Suite</th>
<th>Service Now</th>
<th>Salesforce</th>
<th>Dropbox</th>
<th>AWS</th>
</tr>
</thead>
<tbody>
<tr>
<td>List accounts</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Group</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Privileges</td>
<td>✓</td>
<td>✓</td>
<td>Not supported by provider</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>User governance</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Coming soon</td>
<td>Coming soon</td>
<td>Coming soon</td>
<td></td>
</tr>
<tr>
<td>Log on activity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>User activity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Administrative activity</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Partial</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Periodic file scan</td>
<td>✓</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Near-realtime file scan</td>
<td>✓</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Sharing control</td>
<td>✓</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantine</td>
<td>✓</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>View app permissions</td>
<td>✓</td>
<td>Not supported by provider</td>
<td>Not applicable</td>
<td>✓</td>
<td>✓</td>
<td>Not supported by provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Revoke app permissions</td>
<td>✓</td>
<td>Not applicable</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cloud App Security is available as a part of the Identity & Threat Protection offering for customers with the Windows 10 Enterprise E3 plan and as a part of EM+S E5. Learn more at [https://www.microsoft.com/cloud-platform/cloud-app-security](https://www.microsoft.com/cloud-platform/cloud-app-security).
Plan a Proof of Concept

One of the key services in the project services arsenal is the Proof of Concept (PoC).

PROOF OF CONCEPT HIGH LEVEL FLOW

Define Scope

Why Perform a Proof of Concept?

Proof of concepts (PoC) serve several purposes. One of the primary aims is to overcome customer objections by demonstrating that the solution will solve the problem it’s being designed for. The PoC also can serve as evidence that a practice can use for future engagements with the same customer or with new customers. Many times, the output of a PoC can be added to a practice’s intellectual property list for demonstrations, or used to accelerate future solutions. Proof of concepts are one of the key tools when trying to displace the competition by rapidly showing value and hopefully a quick return on investment.

POC Execution

First, get a commitment to move ahead following a successful PoC (which should be clearly defined in the success criteria), and identify the technical resources needed for the PoC. This will include the technical implementation team, as well as project management for tracking the progress of the engagement. Beyond identification of resources, ensure all members of the team and the customer’s technical team (if they are participating) are clear on responsibilities. During the PoC it is important that the initial design follows best practices and is designed for production (just scaled down) from the beginning. Communication is critical, so ensure that the progress of the PoC is communicated to all stakeholders on a regular basis.

Define Scope

A proper PoC is defined with a clear and concrete scope and success criteria. Conduct an application design session (ADS) to align business and technical requirements and set clear goals. This should include:

- Identify workloads and features to demonstrate.
- Determine what will be provided and which objections need to be overcome.
- Clearly demarcate responsibilities and set up organization.
- Set up subscriptions, define payment, and perform cost estimates of the PoC.
- Agree on the next step if success criteria are met.

Next Step

At the end of the PoC, create a report that explains the overall status of the PoC and any issues identified during the PoC. The report should elaborate on the pros and cons of the delivery and clearly explain the value prop of moving forward with a real implementation to the stakeholders along with expected production costs over time. Assuming the stakeholders agree to move forward, put a plan into place to deploy the PoC into production while ensuring that the PoC is designed for production usage.
Implement a Secure Solution in Azure

If a project services offering calls for implementation on or deployment into Microsoft Azure, delivering a secure solution should be a critical piece of the value the project delivers. So, what are the security-related services and features that should be considered?

The table below provides a summary of select, important security-related services (with features of a service explicitly called out when that is more relevant) grouped into these major security categories: storage, networking, compute, database, identity and access management, and security management and monitoring. Within each category is a selection of services or resources to use, the security objective to accomplish, and what Azure services or features should be leveraged to meet that security objective. This list is constantly evolving and is more comprehensive than what can be covered in this playbook. For the most up-to-date and comprehensive treatment, see https://docs.microsoft.com/azure/security/azure-security-services-technologies.

**STORAGE**

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Azure Storage</strong></td>
<td>Encrypt data at rest</td>
<td>• Service Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Client Side Encryption</td>
</tr>
<tr>
<td></td>
<td>Protect data in transit</td>
<td>• File Shares with SMB 3.0 Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TLS protocol</td>
</tr>
<tr>
<td></td>
<td>Control data access</td>
<td>• Account Keys</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shared Access Signatures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Stored Access Policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cross Origin Resource Sharing (CORS)</td>
</tr>
<tr>
<td></td>
<td>Audit usage</td>
<td>• Storage Analytics</td>
</tr>
<tr>
<td><strong>Azure Data Lake Store</strong></td>
<td>Encrypt data at rest</td>
<td>• Block encryption</td>
</tr>
<tr>
<td></td>
<td>Protect data in transit</td>
<td>• TLS protocol</td>
</tr>
<tr>
<td></td>
<td>Control data access</td>
<td>• Access control lists</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td></td>
<td>Audit usage</td>
<td>• Audit logs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Diagnostic logs</td>
</tr>
</tbody>
</table>
### NETWORKING

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
</table>
| **Virtual Networks**| Secure the virtual network perimeter  | • Network Security Groups  
|                     |                                       | • Azure Application Gateway                           |
|                     | Secure hybrid connectivity             | • Azure VPN Gateway  
|                     |                                       | • Azure ExpressRoute  
|                     |                                       | • Azure Application Proxy                              |
|                     | Audit usage                            | • Azure Network Watcher  
|                     |                                       | • Log analytics for Network Security Groups            |

### COMPUTE

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
</table>
| **Virtual Machines** | Secure Virtual machines             | • Azure Disk Encryption  
|                      |                                     | • Microsoft Antimalware  
|                      |                                     | • Diagnostic logs                                           |
| **Cloud Services**   | Secure cloud services               | • Microsoft Antimalware  
|                      |                                     | • Diagnostic logs                                           |
| **App Services**     | Secure app services                 | • Enforce HTTPS  
|                      |                                     | • TLS mutual authentication                              |
|                      |                                     | • Diagnostic logs                                           |

### DATABASE

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
</table>
| **Azure SQL Database** | Encrypt data at rest              | • Transparent data encryption  
|                     |                                     | • Column level encryption                                  |
|                     |                                     | • Always encrypted                                          |
|                     | Protect data in transit             | • TDS over TLS protocol                                  |
|                     | Control data access                 | • SQL Authentication  
|                     |                                     | • Azure Active Directory Authentication                  |
|                     |                                     | • Dynamic Data Masking                                    |
|                     |                                     | • Row Level Security                                      |
|                     |                                     | • Role Membership & Object Level Permissions              |
|                     |                                     | • Firewall                                                |
|                     |                                     | • Virtual network service endpoints                       |
|                     | Audit usage                         | • SQL Database Usage                                      |
|                     | Detect threats                      | • SQL Database Threat Detection                           |
### Identity & Access Management

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
</table>
| Azure Services | Control management plane access to Azure Services | • Azure Resource Manager  
                  • Role Based Access Control |
|              | Manage identity | • Azure Active Directory  
                  • Azure Active Directory B2C  
                  • Azure Active Directory Domain Services |
|              | Store secrets & encryption keys | • Azure Key Vault |
|              | Audit usage | • SQL Database Usage |
|              | Protect identities | • Azure Multi-Factor Authentication |

### Security Management & Monitoring

<table>
<thead>
<tr>
<th>If using...</th>
<th>And want to...</th>
<th>Then consider...</th>
</tr>
</thead>
</table>
| Azure Services | Manage and monitor security of Azure resources | • Azure Security Center  
                  • Azure Monitor  
                  • Azure Sentinel |
|              | Manage and audit logs | • Log Analytics  
                  • Azure Log Integration |

### The Microsoft Azure IP Advantage

Microsoft Azure IP Advantage program represents the industry’s most comprehensive protection against intellectual property (IP) risks. The Microsoft Azure IP Advantage program includes the following benefits:

- Best-in-industry intellectual property protection with uncapped indemnification coverage will now also cover any open source technology that powers Microsoft Azure services, such as Hadoop used for Azure HD Insight.
- Makes 10,000 Microsoft patents available to customers that use Azure services for the sole purpose of enabling them to better defend themselves against patent lawsuits against their services that run on top of Azure. These patents are broadly representative of Microsoft’s overall patent portfolio and are the result of years of cutting-edge innovation by our best engineers around the world.
- Microsoft is pledging to Azure customers that if Microsoft transfers patents in the future to non-practicing entities, they can never be asserted against them.

With these changes, Microsoft now offers our customers industry-leading protection against intellectual property risk in the cloud. Learn more at [aka.ms/AzureIPAdvantage](https://aka.ms/AzureIPAdvantage).
Nothing produces more ‘aha!’ moments than when a customer first sees advanced threat protection block malicious emails that normally would have gone into their inbox.

BRUCE WARD
Vice President of Business Strategy,
Peters & Associates
Understanding Managed Services

With managed services, partners can help their customers on a regular basis by offering white-glove services. As a managed service provider (MSP), offerings can span from planning and enablement, to day-to-day operations and support.

Managed services is not a new business model. For more than 20 years, large enterprises have relied on service providers to manage their IT assets. Whether they are called an outsourcer, an RMM provider, or a managed IT provider, service providers have been managing their customers’ workloads — either in their own data centers or those operated by their customers. Cloud, however, requires a new method of management because of its focus on scale, elasticity, and automation. For CIOs, cloud represents a paradigm shift in the way they think about embracing IT. DevOps has completely changed the way applications are developed and maintained. The hyper-scale nature of cloud provides a completely new meaning to scalability, elasticity and resiliency — and has redefined how applications are architected and delivered. The pay-as-you-go model provides a fail-fast, agile method of app development. Device and data proliferation means customers want to — and can — do so much more with their IT assets, with cloud providing the computing resources to do so. Because of cloud, CIOs are demanding a new way to think about data governance and security. A cloud MSP is someone who helps their customer transition to (and embrace) this paradigm shift in technology — by guiding them in all aspects of their cloud journey. From consulting to migrations, to operations management, cloud MSPs show customers all the benefits that come with cloud adoption.

<table>
<thead>
<tr>
<th>PLANNING</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Assess the customer’s IT environment and determine risks and policies that are viable security opportunities</td>
</tr>
<tr>
<td>• Deliver ongoing Security Assessments utilizing Secure Score</td>
</tr>
<tr>
<td>• Offer customers a roadmap based on their Secure Score mitigation or recommendations</td>
</tr>
<tr>
<td>• Provide TCO and ROI analysis for moving their security to the cloud</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ENABLEMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Migrate workloads to Azure and Office 365</td>
</tr>
<tr>
<td>• Remediate security gaps found in the Security Assessment Workshop</td>
</tr>
<tr>
<td>• Address security needs across enterprise, including on-premises</td>
</tr>
<tr>
<td>• Optimize security workloads for apps running across on-premises and in Azure and Office 365 cloud environments</td>
</tr>
<tr>
<td>• Optimize advanced security workloads</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUPPORT OPERATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Offer further support while delivering on SLAs and uptime guarantees</td>
</tr>
<tr>
<td>• Operate and monitor the customer’s Azure, Office 365, and hybrid cloud environments</td>
</tr>
<tr>
<td>• Provide customers with governance over their cloud strategy by managing their policies</td>
</tr>
</tbody>
</table>
Managed Services Offerings

The project services discussed earlier are all potential offerings in a managed services offering. Beyond those, an MSP can offer a much broader set of long-term support and consulting offerings.

In the Microsoft Cloud Practice Development Study, 484 partners that identified as having a security practice were asked which managed services they offered within their practices. The results are below. Consider this data when designing managed services-based offerings.

### MANAGED SERVICES

<table>
<thead>
<tr>
<th>Managed Services by Region</th>
<th>Total n=484</th>
<th>APAC n=24*</th>
<th>Canada n=18*</th>
<th>CEE n=27*</th>
<th>Germany n=36</th>
<th>LATAM n=41</th>
<th>MEA n=32</th>
<th>UK n=43</th>
<th>US n=119</th>
<th>WE n=103</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration</td>
<td>54%</td>
<td>42%</td>
<td>44%</td>
<td>52%</td>
<td>39%</td>
<td>54%</td>
<td>59%</td>
<td>56%</td>
<td>58%</td>
<td>58%</td>
</tr>
<tr>
<td>Help-Desk Support</td>
<td>52%</td>
<td>50%</td>
<td>50%</td>
<td>33%</td>
<td>53%</td>
<td>37%</td>
<td>47%</td>
<td>65%</td>
<td>63%</td>
<td>50%</td>
</tr>
<tr>
<td>Desktop &amp; Device Management &amp; Support</td>
<td>47%</td>
<td>50%</td>
<td>44%</td>
<td>41%</td>
<td>36%</td>
<td>29%</td>
<td>72%</td>
<td>56%</td>
<td>55%</td>
<td>41%</td>
</tr>
<tr>
<td>Patch Management</td>
<td>45%</td>
<td>58%</td>
<td>39%</td>
<td>30%</td>
<td>47%</td>
<td>29%</td>
<td>41%</td>
<td>63%</td>
<td>56%</td>
<td>41%</td>
</tr>
<tr>
<td>Active Directory Federation &amp; Management</td>
<td>45%</td>
<td>33%</td>
<td>50%</td>
<td>37%</td>
<td>53%</td>
<td>49%</td>
<td>53%</td>
<td>35%</td>
<td>43%</td>
<td>48%</td>
</tr>
<tr>
<td>Domain Management</td>
<td>44%</td>
<td>50%</td>
<td>39%</td>
<td>44%</td>
<td>33%</td>
<td>37%</td>
<td>47%</td>
<td>53%</td>
<td>57%</td>
<td>36%</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>44%</td>
<td>38%</td>
<td>28%</td>
<td>39%</td>
<td>59%</td>
<td>59%</td>
<td>47%</td>
<td>42%</td>
<td>47%</td>
<td>45%</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>43%</td>
<td>38%</td>
<td>33%</td>
<td>33%</td>
<td>47%</td>
<td>37%</td>
<td>31%</td>
<td>49%</td>
<td>55%</td>
<td>44%</td>
</tr>
<tr>
<td>Enable Multi-Factor Authentication</td>
<td>39%</td>
<td>38%</td>
<td>50%</td>
<td>26%</td>
<td>42%</td>
<td>29%</td>
<td>34%</td>
<td>51%</td>
<td>49%</td>
<td>34%</td>
</tr>
<tr>
<td>Advanced Threat Protection</td>
<td>38%</td>
<td>42%</td>
<td>33%</td>
<td>33%</td>
<td>42%</td>
<td>29%</td>
<td>53%</td>
<td>30%</td>
<td>34%</td>
<td>43%</td>
</tr>
<tr>
<td>New Accounts Added &amp; Removed</td>
<td>37%</td>
<td>50%</td>
<td>39%</td>
<td>30%</td>
<td>28%</td>
<td>12%</td>
<td>44%</td>
<td>58%</td>
<td>51%</td>
<td>25%</td>
</tr>
<tr>
<td>User Rights &amp; Account Management</td>
<td>36%</td>
<td>33%</td>
<td>39%</td>
<td>30%</td>
<td>25%</td>
<td>24%</td>
<td>34%</td>
<td>47%</td>
<td>50%</td>
<td>27%</td>
</tr>
<tr>
<td>Hybrid Environment Support</td>
<td>34%</td>
<td>33%</td>
<td>56%</td>
<td>22%</td>
<td>33%</td>
<td>22%</td>
<td>34%</td>
<td>33%</td>
<td>45%</td>
<td>32%</td>
</tr>
<tr>
<td>Microsoft Support</td>
<td>34%</td>
<td>38%</td>
<td>44%</td>
<td>26%</td>
<td>25%</td>
<td>17%</td>
<td>34%</td>
<td>47%</td>
<td>51%</td>
<td>23%</td>
</tr>
<tr>
<td>Identity &amp; Access Control Management</td>
<td>33%</td>
<td>38%</td>
<td>56%</td>
<td>15%</td>
<td>36%</td>
<td>27%</td>
<td>28%</td>
<td>35%</td>
<td>41%</td>
<td>30%</td>
</tr>
<tr>
<td>Data Migration Management</td>
<td>33%</td>
<td>33%</td>
<td>50%</td>
<td>30%</td>
<td>25%</td>
<td>34%</td>
<td>31%</td>
<td>33%</td>
<td>43%</td>
<td>27%</td>
</tr>
<tr>
<td>Password Complexity Management</td>
<td>33%</td>
<td>33%</td>
<td>28%</td>
<td>26%</td>
<td>14%</td>
<td>20%</td>
<td>38%</td>
<td>49%</td>
<td>47%</td>
<td>31%</td>
</tr>
<tr>
<td>Reactive Help Desk Support</td>
<td>33%</td>
<td>38%</td>
<td>33%</td>
<td>11%</td>
<td>22%</td>
<td>17%</td>
<td>31%</td>
<td>51%</td>
<td>50%</td>
<td>26%</td>
</tr>
<tr>
<td>Activity and Log Audit Management</td>
<td>32%</td>
<td>33%</td>
<td>30%</td>
<td>33%</td>
<td>28%</td>
<td>29%</td>
<td>31%</td>
<td>28%</td>
<td>35%</td>
<td>31%</td>
</tr>
<tr>
<td>Mobile Device Management</td>
<td>30%</td>
<td>33%</td>
<td>39%</td>
<td>11%</td>
<td>31%</td>
<td>10%</td>
<td>31%</td>
<td>44%</td>
<td>41%</td>
<td>28%</td>
</tr>
<tr>
<td>Performance Monitoring and Reporting</td>
<td>30%</td>
<td>25%</td>
<td>28%</td>
<td>26%</td>
<td>36%</td>
<td>22%</td>
<td>31%</td>
<td>35%</td>
<td>42%</td>
<td>22%</td>
</tr>
<tr>
<td>Single Sign-On Management</td>
<td>30%</td>
<td>21%</td>
<td>39%</td>
<td>19%</td>
<td>31%</td>
<td>20%</td>
<td>22%</td>
<td>26%</td>
<td>40%</td>
<td>30%</td>
</tr>
<tr>
<td>Threat Detection, Monitoring &amp; Mitigation</td>
<td>28%</td>
<td>29%</td>
<td>28%</td>
<td>19%</td>
<td>25%</td>
<td>15%</td>
<td>38%</td>
<td>26%</td>
<td>42%</td>
<td>21%</td>
</tr>
</tbody>
</table>

aka.ms/practiceplaybooks
<table>
<thead>
<tr>
<th>Service</th>
<th>28%</th>
<th>21%</th>
<th>39%</th>
<th>30%</th>
<th>11%</th>
<th>27%</th>
<th>19%</th>
<th>35%</th>
<th>44%</th>
<th>19%</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Recommendation and Improvement</td>
<td>26%</td>
<td>33%</td>
<td>22%</td>
<td>11%</td>
<td>28%</td>
<td>10%</td>
<td>25%</td>
<td>37%</td>
<td>37%</td>
<td>23%</td>
</tr>
<tr>
<td>Auditing, Security &amp; Compliance Assessments</td>
<td>26%</td>
<td>25%</td>
<td>22%</td>
<td>19%</td>
<td>8%</td>
<td>29%</td>
<td>22%</td>
<td>23%</td>
<td>37%</td>
<td>24%</td>
</tr>
<tr>
<td>Security Management &amp; Identity Protection</td>
<td>25%</td>
<td>42%</td>
<td>28%</td>
<td>19%</td>
<td>14%</td>
<td>20%</td>
<td>19%</td>
<td>30%</td>
<td>34%</td>
<td>20%</td>
</tr>
<tr>
<td>Managed Access to Email Groups</td>
<td>24%</td>
<td>25%</td>
<td>22%</td>
<td>15%</td>
<td>14%</td>
<td>20%</td>
<td>41%</td>
<td>35%</td>
<td>34%</td>
<td>15%</td>
</tr>
<tr>
<td>Reporting and Analytics</td>
<td>23%</td>
<td>29%</td>
<td>50%</td>
<td>26%</td>
<td>25%</td>
<td>15%</td>
<td>19%</td>
<td>23%</td>
<td>33%</td>
<td>13%</td>
</tr>
<tr>
<td>Cyber Security Risk Assessment</td>
<td>23%</td>
<td>25%</td>
<td>17%</td>
<td>11%</td>
<td>8%</td>
<td>17%</td>
<td>9%</td>
<td>26%</td>
<td>39%</td>
<td>17%</td>
</tr>
<tr>
<td>Information Protection Management</td>
<td>21%</td>
<td>13%</td>
<td>22%</td>
<td>19%</td>
<td>17%</td>
<td>12%</td>
<td>25%</td>
<td>28%</td>
<td>33%</td>
<td>14%</td>
</tr>
<tr>
<td>Application Lifecycle Management &amp; Support</td>
<td>19%</td>
<td>17%</td>
<td>11%</td>
<td>15%</td>
<td>14%</td>
<td>20%</td>
<td>16%</td>
<td>14%</td>
<td>27%</td>
<td>16%</td>
</tr>
<tr>
<td>Data Leakage Prevention</td>
<td>19%</td>
<td>13%</td>
<td>6%</td>
<td>22%</td>
<td>6%</td>
<td>20%</td>
<td>31%</td>
<td>21%</td>
<td>24%</td>
<td>16%</td>
</tr>
<tr>
<td>Auditing, Security &amp; Compliance Enablement</td>
<td>18%</td>
<td>13%</td>
<td>11%</td>
<td>7%</td>
<td>6%</td>
<td>17%</td>
<td>16%</td>
<td>21%</td>
<td>31%</td>
<td>17%</td>
</tr>
<tr>
<td>Incidence Response Management</td>
<td>18%</td>
<td>17%</td>
<td>17%</td>
<td>7%</td>
<td>8%</td>
<td>12%</td>
<td>16%</td>
<td>23%</td>
<td>32%</td>
<td>13%</td>
</tr>
<tr>
<td>Penetration Testing</td>
<td>18%</td>
<td>13%</td>
<td>6%</td>
<td>15%</td>
<td>17%</td>
<td>17%</td>
<td>16%</td>
<td>28%</td>
<td>24%</td>
<td>15%</td>
</tr>
<tr>
<td>Reports and Dashboard Maintenance</td>
<td>18%</td>
<td>21%</td>
<td>39%</td>
<td>11%</td>
<td>11%</td>
<td>10%</td>
<td>25%</td>
<td>14%</td>
<td>29%</td>
<td>8%</td>
</tr>
<tr>
<td>Identity as a Service</td>
<td>14%</td>
<td>0%</td>
<td>17%</td>
<td>15%</td>
<td>11%</td>
<td>22%</td>
<td>9%</td>
<td>16%</td>
<td>18%</td>
<td>12%</td>
</tr>
<tr>
<td>Data Classification and Data Governance</td>
<td>13%</td>
<td>4%</td>
<td>17%</td>
<td>7%</td>
<td>11%</td>
<td>12%</td>
<td>16%</td>
<td>12%</td>
<td>21%</td>
<td>7%</td>
</tr>
<tr>
<td>Productivity Cloud App Usage Management</td>
<td>11%</td>
<td>13%</td>
<td>22%</td>
<td>11%</td>
<td>0%</td>
<td>2%</td>
<td>13%</td>
<td>9%</td>
<td>20%</td>
<td>6%</td>
</tr>
<tr>
<td>Security Operations Center Management</td>
<td>10%</td>
<td>13%</td>
<td>0%</td>
<td>11%</td>
<td>0%</td>
<td>10%</td>
<td>16%</td>
<td>7%</td>
<td>18%</td>
<td>6%</td>
</tr>
<tr>
<td>CISO or Security Analyst as a Service</td>
<td>9%</td>
<td>17%</td>
<td>6%</td>
<td>7%</td>
<td>6%</td>
<td>7%</td>
<td>9%</td>
<td>5%</td>
<td>15%</td>
<td>7%</td>
</tr>
</tbody>
</table>

We do not offer any of these managed services

|          | 8% | 8% | 6% | 15% | 17% | 5% | 6% | 2% | 8% | 8% |

**REVENUE**

<table>
<thead>
<tr>
<th>Total Median (n=445)</th>
<th>$46,355</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BY CUSTOMER FOCUS</strong></td>
<td></td>
</tr>
<tr>
<td>SMB (n=386)</td>
<td>$43,274</td>
</tr>
<tr>
<td>Enterprise (n=59)</td>
<td>$489,815</td>
</tr>
</tbody>
</table>

When creating managed services, research with partners emphasized the importance of targeting the enterprise customer to attain significantly higher managed revenues.

Source: Microsoft Cloud Practice Development Study, MDC Research, June 2017.

aka.ms/practiceplaybooks
Going from Project Services to Managed Services

Build a practice from providing project services such as assessments and deployments to ongoing managed security services and operational support. This will help create annuity income streams with higher professional services margins.

Separate security managed services teams from traditional IT managed services teams to land new clients

Separate security services teams can help build a new solution message for an organization. Most partners have a single or integrated team offering their managed services and security services.

A small share of partners are beginning to recognize opportunities to land clients that traditionally would not engage them for traditional managed IT services using security service offerings. Spinning off a separate security services team has allowed them to generate a differentiated offering that positions them as experts in the security service space.

Few have separated managed services and security services teams; challenges integrating security into managed services teams center around education.

Because most partners are using the same staff to market and sell their security services business as their traditional IT and managed services business, the greatest challenge is ensuring their staff has the right marketing/sales resources and solution knowledge to support a security services conversation.

Compared to many IT offerings today, security services require more intensive education of clients about the risks and solutions available.

Keep in mind that client conversations and education about security and security services are increasing with C-level or non-technical BDMs, so a different level of information is required to support that interaction.

aka.ms/practiceplaybooks
Accelerate the Managed Service Model

Resources

The Microsoft Cloud Solution Provider (CSP) program enables partners to directly manage their entire Microsoft cloud customer lifecycle.

Partners in the CSP program utilize in-product tools to directly provision, manage, and support their customer subscriptions. Partners can easily package their own tools, products, and services, and combine them into one monthly or annual customer bill.

CSP DIRECT

The CSP Direct model is great for partners who have the infrastructure in place to do it all. If a partner business meets these requirements, they can enroll today.

CSP DIRECT REQUIREMENT CHECKLIST

- Services business model
- Customer support infrastructure
- Customer billing and invoicing capabilities
- Ability to scale

KEY SERVICES FOR THIS OFFERING

- Be the first point of contact for a customers’ needs
- Own and control the billing cycle
- Sell integrated offers and services — one sales motion to drive services, attach, and upsell
- Receive in-product tools to directly provision, manage, and support customers

CSP INDIRECT

Spend more time with customers and provide specialized service offerings. For partners not interested in building an infrastructure to provide customer support and billing, get started as an Indirect Provider.

aka.ms/practiceplaybooks
Security as a Managed Service

The current digital security landscape for businesses can accurately be described in one word: complicated. More numerous and advanced threats, more nebulous and complex compliance requirements, more difficult and intricate infrastructure to secure. Simply put, keeping data, workloads, and users secure is more than a full-time job — and organizations are having trouble keeping up. The graphic below illustrates the myriad offerings and postures taken by security companies, highlighting the fragmented nature of the market. However, this harsh environment represents a significant opportunity for partners looking to offer security as a managed service.

For even the most adept IT and incident response teams, effectively handling patching, malware threats, and intrusion detection can be too difficult to manage without help. MSPs can offer their services to ensure enterprise clients are secured. But in this age where we hear about security breaches almost daily, how can partners help their customers stay ahead of the game, and avoid becoming a statistic?

KEY CUSTOMER CHALLENGES AND QUESTIONS

1. They lack the tools and expertise to effectively get ahead of security threats and compliance risks
2. They are unable to identify, assess, and mitigate security risks
3. They are able to detect threats, but are unable to correctly respond in a timely fashion
4. They are unfamiliar with security best practices and the overall threat landscape
5. They are confused with the myriad offerings out there

EXAMPLE OF A SECURITY MANAGED SERVICES OFFERING

<table>
<thead>
<tr>
<th>Basic</th>
<th>Pro</th>
<th>Premium</th>
</tr>
</thead>
<tbody>
<tr>
<td>$ per user per month</td>
<td>$5 per user per month</td>
<td>$55 per user per month</td>
</tr>
<tr>
<td>with Office 365</td>
<td>with Office 365 and Office 365 Advanced Security &amp; Compliance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Plan and deploy Office 365 capabilities</td>
<td>• Monitor the following services:</td>
</tr>
<tr>
<td></td>
<td>• Provide end-user training</td>
<td>• $25 app usage</td>
</tr>
<tr>
<td></td>
<td>• Email and data migration to cloud</td>
<td>• Top targeted users</td>
</tr>
<tr>
<td></td>
<td>• Deliver end user support and incident</td>
<td>• Unusual signs-likes</td>
</tr>
<tr>
<td></td>
<td>management</td>
<td>• Potential threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Sensitive Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>sharing to external users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Manage customers security policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>including secure score reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Support data classification policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Pro and basic benefits</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
IDENTITY IS FUNDAMENTAL

When considering a managed services offering for a security practice, notice how it helps build a deeper customer relationship. Partners start, metaphorically, by securing the customer’s front door by providing identity-driven security. With identity in place, the offer can evolve to securing content (protecting content, managing content creation, transit, and consumption) and securing devices (both workplace-issued devices and staff personal devices).

SECURE THE FRONT DOOR

Just like for a house, the front door is where it is decided who to let in. Now, apply that to a customers’ data and digital assets. Customers want to be able to answer YES to the following:

- Do they know who is accessing their data?
- Can they grant access to data based on risk in real time?
- Can they quickly find and react to a breach?

To get to YES, a solution is needed that adapts in a changing environment and learns what is normal credential use from what looks questionable. This occurs when risk-based policies are implemented that are driven by machine learning. The addition of machine learning adds intelligence that lets the system monitor and identify brute force attacks, infected devices, configuration vulnerabilities, leaked credentials, suspicious sign-in activities, sign-ins from atypical locations, or multiple sign-ins from geographically distant locations in less time than the travel would take. The system detects those types of risk events and assigns a risk level that indicates how strongly an event indicates a compromised identity. With risk level assigned to the risk event detected, risk-based policies can be executed for the detected threat in question. A Multi-Factor Authentication (MFA) challenge could be issued that

aka.ms/practiceplaybooks
blocks risky logins or changes credentials known to have been compromised.

If this sounds like science fiction, consider this example, which uses machine learning to assign a risk score to a user (e.g., base on intelligence like XYZ), which in turn, is evaluated by a condition that when the risk is determined to be high, the system will mitigate the risk by issuing an MFA challenge. Within Azure Active Directory, the **Identity Protection** feature can detect the potential vulnerability affecting an organization identity by assigning it a risk level. Automated responses can be configured to detected suspicious actions by their level of risk of compromise using **Conditional Access**. For example, block access, or allow access but require Multi-Factor Authentication or a password change. A report of the users flagged for risk, the number of risk events triggered, and the status of any remediation actions taken can be reviewed at a later time. Action can be taken to close any listed risk events manually, which can help the machine learning algorithm to improve the classification of similar events in the future.

As an added layer of security, utilize **Privileged Identity Management** to ensure privileged users (e.g., those with administrator level credentials) must first escalate their user role to admin (refered to as activating the role). Role activation may require approval by other users in the organization and the admin role only applies for a limited window of time.

**EXAMPLE COMPONENTS OF AN IDENTITY OFFER**

Consider the following table which provides an example approach to selling identity-driven security.

<table>
<thead>
<tr>
<th>Secure the Front Door</th>
<th>Capabilities</th>
<th>Enabling Technologies</th>
<th>UP-SELL / CROSS-SELL</th>
</tr>
</thead>
</table>
| **Identity Driven Security** | 1. Risk-based Conditional Access and Multi-Factor Authentication  
2. Advanced security reporting  
3. Identify threats on-premises  
4. Identify high-risk usage of cloud apps, user behavior, detect abnormal downloads, prevent threat | Azure Active Directory Premium P2  
Azure Active Directory Premium P1 (included in P2)  
Cloud App Security | No Prerequisites. Every Organization needs to secure their front door.  
Best Position with:  
1. Business Premium  
2. E3  
3. E5  
4. Azure Deals |
SECURE CONTENT

Now that the front door is secured, it is time to focus on securing the contents of the house. Securing content means being able to take a series of steps against the content:

- Define policies, templates and rules for content
- Define exceptions
- Define content classification labels
- Detect the SaaS apps that are in use and assigning them a security risk rating
- Define data copy and usage rules for apps on devices
- Control sharing of data based on identity
- Detect data and users violating content policies
- Take action to maintain the security of content

EXAMPLE COMPONENTS WITHIN A CONTENT PROTECTION OFFER

The following table provides an example approach to selling content protection.
**SECURE DEVICES**

Devices represent other doors into data and digital assets, and need to be secured accordingly. Similar to the example used in “Secure the Front Door,” the process for securing devices also includes intelligent access management. Conditional Access can be used to restrict access based on the device platform (e.g., iOS, Android) whether or not it is enrolled into the mobile device management solution provided by Microsoft Intune. Constraints also can be applied on a per-mobile app basis using the mobile application management capabilities of Microsoft Intune.

![Manage Devices Table]

**EXAMPLE COMPONENTS WITH A DEVICE PROTECTION OFFER**

The following table provides an example approach to selling device protection.
DELIVER A GREAT EMPLOYEE EXPERIENCE

It’s no secret that ease-of-use and security are often at odds. In helping secure customers, it is important to also deliver a great experience for the users who will be affected by the security solution deployed. Turn security into an improved experience for a customer’s users by enabling capabilities like single sign-on, self-service password reset, and the ability to securely use their own personal devices without IT intrusion.

EXAMPLE COMPONENTS OF A GREAT EMPLOYEE EXPERIENCE OFFER

The following table provides an example approach to a great experience while delivering tight security.

<table>
<thead>
<tr>
<th>Great Employee Experience</th>
<th>Capabilities</th>
<th>Enabling Technologies</th>
<th>Up-sell/Cross-sell</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Single Sign-On</td>
<td>Azure Active Directory Premium P1</td>
<td>No Prerequisites, up-sell with any Office 365 offer</td>
</tr>
<tr>
<td></td>
<td>2. Self Service</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Advanced Multi-Factor Authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4. App Proxy without the need of VPN</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Productivity without Compromise</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SECURE & MONITOR THE CUSTOMER’S OFFICE 365 ENVIRONMENT WITH MICROSOFT CLOUD APP SECURITY ADVANCED SECURITY MANAGEMENT CAPABILITIES

Microsoft Cloud App Security advanced security management capabilities provide enhanced visibility and control over Office 365. It increases the security of Office 365 environments by providing:

THREAT DETECTION

Microsoft Cloud App Security enables identification of high-risk user activities and abnormal usage (e.g., impossible travel, logon from unknown or risk IP address, mass downloads by a single user), security incidents, and threats. It provides insights into potential breaches by identifying anomalies in an Office 365 environment, applies behavioral analytics to help assess risk, and leverages Microsoft’s Threat Intelligence to identify known attack pattern activities originating from risky sources.

ENHANCED CONTROLS

aka.ms/practiceplaybooks
Microsoft Cloud App Security provides both out of the box and customizable policies, and provides visibility into violations of those policies as well as supports a response that includes the ability trigger email or SMS text message alerts and automatic remediation (such as by user suspension). Additionally, it enables partners to assess the risk from SaaS apps that have permissions into Office 365 data and to remove their rights from a central location.

DISCOVERY & INSIGHT

Azure Service Management (ASM) enables a view into Office 365 usage via an easy to understand dashboard that helps keep tabs on shadow IT by enabling the discovery of more than 1,000 SaaS applications in use on a network.
THE PARTNER OPPORTUNITY

Office 365 is the most widely-used productivity suite. For many organizations Office 365 is the main portal through which employees access company resources: email, calendars, documents and the company directory. The core opportunity for partners is to help customers understand the importance of leveraging ASM to secure their Office 365 environment, helping them with deployment, tuning and providing training. A managed service offering built around providing on-going monitoring services on behalf of the customer that bundles Office 365, ASM and the monitoring services fees into a single monthly fee represents an opportunity for partners to capture more profitable and recurring revenue.
ENABLE THREAT ALERTING AND REMIDATION WITH MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

Threat intelligence and response capabilities in Microsoft Defender Advanced Threat Protection allows partners to take increased control over an Office 365 deployment by enabling full visibility into what threats are in the environment, which users are compromised and what data is at risk. Additionally, Threat Intelligence provides remediation capabilities for suspicious content.

By collecting rich threat signals from SharePoint, Exchange, OneDrive for Business, Skype for Business and Azure Active Directory, Threat Intelligence keeps organizations abreast of phishing, malware and suspicious activity. This threat data is enriched by correlation with security signals from across Microsoft, global targeting data, and actor profiles which give detailed background on threats present in the environment and those actively circulating globally.

Threat analytics provide information into mitigated and potential attacks, as well as investigation tools that allow organizations to explore attack campaigns, people and data. Threat Intelligence provides the tools to organize incident response with task oriented workflows, attack alerts, detailed forensics and remediation workflows.
Threat explorer lets organizations to interactively navigate a timeline view of threats and get more details on detected threats.

For a given threat, administrators are able to drill into the threat to get documentation on the threat, the users affected by that threat and the technical details of the threat (such as threats often associated with the selected threat).

Additionally Microsoft Defender Advanced Threat Protection integrates with Windows Defender Advanced Threat Protection — when threats are detected on individual devices these signals are shared with Microsoft Defender Advanced Threat Protection so it can take appropriate action to protect other users and devices from the detected threat. For example, if a suspicious activity was detected by Windows Defender Advanced Threat Protection that resulted from opening an email with Outlook, this signal is shared with Microsoft Defender Advanced Threat Protection which automatically blocks all emails having a similar attachment.

THE PARTNER OPPORTUNITY

Microsoft Defender Advanced Threat Protection is included in the Office 365 Enterprise E5 plan and is also available with the Identity & Threat Protection offering for customers with the Windows 10 Enterprise E3 plan.

This enables partners to provide a managed services offer that includes Office 365 with Microsoft Defender Advanced Threat Protection to provide additional value by including monitoring and remediation services that utilize threat intelligence for a consolidated monthly fee per user. Those services could include a risk assessment analysis, mobile device or messaging protection, or even using AI and machine learning to prevent or contain attacks.
ENABLE POST BREACH DEFENSES AS A SERVICE WITH MICROSOFT DEFENDER ADVANCED THREAT PROTECTION

Traditional threat detection focuses on the datacenter and firewall, but device endpoints are often the weak link in the system. Microsoft Defender Advanced Threat Protection layers on to Windows 10 devices a monitoring service to help detect advanced attacks and remediate them.

BUILT INTO WINDOWS

Microsoft Defender Advanced Threat Protection is agentless, that is to say there is no additional deployment or infrastructure besides Windows 10. It stays continuously up-to-date.

STATE OF THE ART BEHAVIORAL DETECTION

Provides signature-less, intelligent, behavioral, machine learning and past attack detections based on Microsoft’s unparalleled optics and security experts.

SOPHISTICATED ANALYTICAL ENGINE

Makes it easy to understand the scope of a breach, surfacing data across endpoints with 6 months of stored log history, presented in a way that enables partners to quickly understand the evolution of a breach and analyze the result.

UNIQUE THREAT INTELLIGENCE KNOWLEDGEBASE

The cloud based knowledgebase provides unparalleled threat optics across the world’s largest device database to provide detailed actor profiles. Enhanced by 24x7 threat intelligence from both Microsoft and the community of security researchers, as well as third party threat intelligence data.

THE PARTNER OPPORTUNITY

Microsoft Defender Advanced Threat Protection is available with the Identity & Threat Protection offering for customers with the Windows 10 Enterprise E3 plan and with the Windows 10 Enterprise E5 plan. For partners in the Cloud Solution Provider program, this creates multiple opportunities:

- Increase revenue: Drive customers to upgrade from the Windows 10 Enterprise E3 to E5 plan and double Windows 10 license subscription revenue, and the profits that are associated with it.
- Managed service: Provide expert monitoring and remediation using Microsoft Defender Advanced Threat Protection as a value-add, managed service to customers. By combining the subscription price of the Identity & Threat Protection or E5 plan with the price for the monitoring service, partners can deliver a packaged offer that provides both for one monthly fee to customers.

aka.ms/practiceplaybooks
Customers are asking for more intelligence and insights into threats – it’s something they need and have been asking for constantly. Threat intelligence dashboard is going to be very valuable and will really enhance the solutions we offer.

ETHAN MCCONNELL
Vice President of Olive & Goose
Compliance as a Managed Service

The adherence to regulatory standards, government regulations, and other industry requirements represents a challenge most customers don’t want to face alone — and presents an opportunity for a long-term relationship with partners.

Partners can help customers on many different levels. They can provide services that help them to prepare and pre-check for audit, provide compliance auditing services, and help a customer define or implement their compliance strategy.

Partners also can help customers meet general compliance requirements by:

- Ensuring they are aware of how Customer Lockbox can help them meet compliance obligations for controlling data access by Microsoft support engineers.
- Enabling them with full audit tracking to monitor and investigate events related to their data.
- Reduce their cost and risk with in-place intelligent advanced eDiscovery.
- Empower them to efficiently perform risk assessment with Office 365 Service Assurance.
- Prevent, detect, and contain internal risks with the insider risk management feature in Microsoft 365.
- Manage their data retention with Office 365 Advanced Data Governance.

In any combination, these make up core components of any compliance-related managed services offer. However, there is an even more critical opportunity on the horizon that motivates building a compliance managed services offering — one that is predicted to create a $3.5 billion market opportunity for security and storage vendors according to IDC.

THE GENERAL DATA PROTECTION REGULATION (GDPR)

In May 2018, a European privacy law, the General Data Protection Regulation (GDPR) took effect imposing new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents. The GDPR applies regardless of location.

It gives EU residents more control over their “personal data” (which is precisely defined by the GDPR). The GDPR also seeks to ensure personal data is protected no matter where it is sent, processed, or stored.

The GDPR contains many requirements about the collection, storage and use personal information. This means not only how to identify and secure the personal data in organizational systems, but also how to accommodate new transparency requirements, detect and report personal data breaches, and train privacy personnel and employees. The table below shows the considerations and provisions that must be made to remain compliant with this far reaching regulation:
Failure to comply with the GDPR could prove costly, as companies that do not meet the requirements and obligations could face substantial fines and reputational harm. Companies can be fined up to €20m or 4% of annual global turnover, whichever is greater, for failure to meet certain requirements of the GDPR. Additional individual remedies could increase risk if there is a failure to adhere to the GDPR requirements.

The Partner Opportunity

GDPR applies to companies that trade products or services with European customers or in European market, creating the potential for a global impact. Resulting from this wide-spread impact, there will be a serious resource shortfall of Privacy Professionals — a perfect opportunity for partners to pick up the slack.

GDPR policies require privacy-by-design and by-default, and brings with it inherent operational complexity. Partners can become privacy consultants or implementers to support the customer GDPR journey.

The significant fines imposed for non-compliance could put many companies out of business. This means customers should be motivated to achieve compliance. With those motivators in mind, here are 4 opportunities for partners:
To plan accordingly, here are five Microsoft-recommended steps to provide effective services to customers:

| GLOBAL MANDATE | The large number of firms doing business in the Europe market or with European customers are tackling privacy rules. Microsoft Cloud services and a partner’s GDPR-related services can be critical to compliance. |
| PRIVACY-BY-DESIGN | Partners can work closely with security leaders to provide GDPR assessments and determine how Microsoft Cloud services and partner services can enable customers to meet privacy-by-design requirements. |
| DATA BREACH NOTIFICATION | With 72-hour data breach notification, partners can utilize Microsoft Cloud services to become an incident response (IR) orchestrator through managed services or professional services. |
| DATA PRIVACY OFFICER (DPO) | The demand for DPOs is creating a serious shortfall of privacy skills. Partners can consider providing DPO as a service to customers. |
| EVIDENCE OF RISK MITIGATION | Per GDPR policy, organizations must demonstrate that they have implemented appropriate measures to mitigate privacy risks. Partners and customers can use Microsoft Cloud services to build evidence of mitigation strategies and controls. |

### Five Key Reasons

Why should partners utilize Microsoft Solutions for GDPR

1. Microsoft was the first major cloud services provider to [pledge GDPR compliance](#).
2. Microsoft has been an industry leader on Model Clauses, HIPAA, ISO 27018, and is taking a similar lead on GDPR compliance.
3. Microsoft offers the most comprehensive set of compliance capabilities of any major cloud service provider and has the best baseline to build from.
4. Microsoft provides a single stack solution — all pieces work well together.
5. Microsoft’s speed of solution innovation is high (according to MDC Partner Research’s Microsoft and Office 365 Security Solution Selling Qualitative Research Findings, December 2016) and will continue as it enables partners and customers to meet their compliance needs.

---

2. Study: GDPR’s global reach to require at least 75,000 DPOs worldwide, Rita Heimes, CIPP/US, Sam Pfeifle, November 9, 2016.
TAKE A PLATFORM APPROACH

Rather than track the controls required by individual standards or regulations on a case-by-case basis, a best practice is to identify an overall set of controls and capabilities to meet these requirements. Likewise, rather than assessing individual technologies and solutions against a comprehensive regulation such as the GDPR, taking a platform view—such as one encompassing Windows, Microsoft SQL Server, SharePoint, Exchange, Office 365, Azure, and Dynamics 365—can provide a clearer path to ensure a customer complies not only with the GDPR, but also with other requirements important to the customer as well.

THE PROCESS FOR SUPPORTING CUSTOMERS WITH GDPR COMPLIANCE

The following illustration summarizes a step-by-step process that can be used as a foundation helping customers towards GDPR compliance.

Process to support your customers

1. Discover
   Identify what personal data they have and where it resides.

2. Manage
   Govern how personal data is used and accessed.

3. Protect
   Establish security controls to prevent, detect, and respond to vulnerabilities & data breaches.

4. Report
   Keep required documentation, manage data requests and breach notifications.

aka.ms/practiceplaybooks
Microsoft’s Journey to GDPR Compliance e-Book

To help partners with their GDPR efforts, Microsoft has published the Journey to GDPR Compliance e-Book.

This e-book provides an overview of Microsoft’s own journey to GDPR compliance—including how they approached privacy regulations, the organizational structure of the Microsoft Privacy team, their GDPR approach, and learnings from implementation workstreams.

This e-book was developed through interviews of privacy-accountable leaders across Microsoft’s major horizontals and verticals, resulting in a comprehensive and transparent overview of the Microsoft approach to not only the GDPR, but privacy in general.
**NEXT STEPS FOR PARTNERS**

Follow this checklist:

- ✔ Determine if GDPR compliance is needed. If so, act now!
- ✔ Reassure customers that Microsoft Cloud services are compliant with the GDPR, and share with them the [GDPR Frequently Asked Questions](#) that succinctly describes common questions about Microsoft’s commitments to GDPR.
- ✔ Learn more about the GDPR and Microsoft Security offerings using the [Trust Center](#).
- ✔ Identify offerings and go-to-market strategy using Microsoft Cloud and leverage the [GDPR Sales Kit](#).
- ✔ Review the [Beginning your GDPR Journey](#) whitepaper.
- ✔ Pilot services and offerings with a few customers before going broad.
Support as a Managed Service

It should go without saying that one of the most important functions of a managed service practice is supporting a customer once their applications and data are firmly in the cloud or a hybrid deployment.

No matter how well a cloud or hybrid environment is planned, provisioned, operated or monitored, problems will arise, and those problems will need to be remediated. It’s the MSP’s job to offer support to customers to deal with outages, breaches, inefficiencies, and disaster scenarios. MSPs need to consider the level of support that makes sense for their practice — in terms of resources and revenue — as well as what makes sense to the customers they serve.

KEY CUSTOMER CHALLENGES

- They lack the expertise and resources to troubleshoot problems.
- They are unable to determine the root cause of performance issues and glitches.
- They have no knowledge of how to remediate problems when they correctly identify them.
- They do not want to spend time and resources fixing problems.

KEY SERVICES FOR THIS OFFERING

- **User Support:** Provide support for frequently asked questions, setup and usage, best practices, questions around billing and invoicing, break-fix support for developers, architecture design, and solution design support for architects.
- **System Support:** Provide customers with information on any service interruption, and relay expectations on when the system will be back online.
- **Product Support Support:** Provide support when the Microsoft product is not working as expected or the service stops working. Escalate to Microsoft when the issue cannot be resolved with existing documentation and/or training.
- **Extended Support Support Hours:** Many customers need the ability for 24/7 support support, but cannot justify the overhead internally.
- **Account Management:** Offering an account manager that is responsible for reporting service consumption and ultimately minimizing time to resolution is a service that can be offered at a premium.
- **Dedicated Support:** The value add of a dedicated support team cannot be understated. Engineering resources that already know the customers’ environment, including the business and technical reasons for how a solution was implemented can add a tremendous value over the lifetime of an agreement.

Adding managed support services to an offering increases a partner’s value and profitability. Learn more in this article: Four ways owning the customer life cycle makes you more profitable.
Cloud Monitoring Services

Back in the 2000s, Managed Services was synonymous with Remote Management & Monitoring (RMM).

In the cloud world, the tools and requirements have evolved, but the problem statement hasn’t fundamentally changed. How do I monitor the health and performance of my IT infrastructure? There is no easy answer to this and customers expect their service providers to solve it for them. Most mid-market and enterprise organizations simply do not have the time, resources, or dedicated staff required to monitor every aspect of IT, and this is where MSPs add the most value. While Azure offers many monitoring capabilities built within the platform, there is still a place for partners who (a) provide additional, deeper monitoring tooling (b) triage the false positives from the real alerts (c) proactively act upon the alerts before any measurable loss in performance.

KEY CUSTOMER CHALLENGES

- I don’t have the time or resources to monitor all my hosted and internal IT assets.
- I need a single pane of glass view that tells me how all my apps and VMs are performing, at any point in time.
- I find it challenging to diagnose the root cause of breakdowns or outages.
- How do I respond to so many alerts? How do I differentiate the false positives from the concerning ones?

KEY SERVICES FOR THIS OFFERING

<table>
<thead>
<tr>
<th>SYSTEM HEALTH MONITORING</th>
<th>LOG ANALYTICS AND ALERTING</th>
<th>DATABASE MONITORING</th>
<th>APP PERFORMANCE MONITORING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete monitoring of VMs, CPU utilization, memory usage, storage IOPs, and OS performance. Includes monitoring of application performance and operation health, and dashboards and reports on system health.</td>
<td>Every client, device, and user accessing a network produces data that is logged. Analyzing those logs can offer deep insight into performance, security, resource consumption, and a number of other meaningful metrics.</td>
<td>A view into the customer’s database that helps MSPs ensure high availability of database servers. The process involves keeping logs of size, connection time and users of databases, analyzing use trends, and leveraging data to proactively remediate issues.</td>
<td>End-to-end tracking of all aspects of an application (or webpage). App monitoring involves watching every part — from shopping carts to registration pages — of a customer’s app(s) for performance issues in an effort to provide the best user experience possible.</td>
</tr>
</tbody>
</table>

RESOURCES

- Azure Advisor
- Azure Application Insights
- Azure Diagnostics
- Azure Monitor Log Analytics
- System Center
- Automation

THIRD-PARTY RESOURCES

- App Dynamics
- Nagios
- New Relic
- Science Logic
- Splunk
- Logic Monitor

aka.ms/practiceplaybooks
Hybrid Device Management: Manage PCs, Servers and Devices

With the increasing demand to support bring-your-own-device (BYOD) scenarios, organizations are faced with the challenge of finding the right balance between allowing their employees to choose which devices they use, while making sure those devices have access to the right set of applications and meet corporate data protection and compliance requirements.

**KEY CUSTOMER CHALLENGES (USER)**
- Demand their own choice of devices and apps
- Expect anywhere connectivity and productivity

**KEY CUSTOMER CHALLENGES (IT)**
- Needs to maintain compliance and data protection
- Must avoid the complexity and cost associated with many discrete management infrastructures

**KEY SERVICES FOR THIS OFFERING**

Microsoft’s solution builds on market-leading client management by combining System Center Configuration Manager with Microsoft Intune to provide organizations with a comprehensive, cross-platform, and user-centric way to deploy applications and manage users’ devices, whether they are corporate-connected or cloud-based.

With Configuration Manager and Intune, organizations can enable their employees to choose devices, unify management infrastructure, and simplify IT administration. IT can deliver and manage consistent application experiences for employees based on their corporate identity, network connectivity, and device type, helping maintain productivity as employees use various devices throughout their day. Through a single infrastructure and administrative console, IT can manage PCs, servers, mobile devices, endpoint protection, and virtual machines across various platforms, including Windows, Linux/Unix, Mac OS X, iOS, and Android.

Simplified server and client deployment, streamlined updates, and consolidated reporting enable IT staff to easily manage mobile, physical, and virtual client environments, reducing costs and increasing efficiency through comprehensive application and device management. Unified security, including System Center Endpoint Protection, protects corporate information and helps partners better manage risk by deploying software updates and antimalware definitions to PCs, as well as enabling selective wipe of mobile devices. New improvements — such as the support of latest Windows 10 features, Windows in-place upgrade, more frequent and easier updates, unified end-user portal, and on-premises MDM — make deploying and managing Windows easier than ever.

**RESOURCES**

- Managing Corporate Devices
- Choose between Microsoft Intune Standalone and Hybrid Mobile Device Management with System Center Configuration Manager

aka.ms/practiceplaybooks
Understanding Intellectual Property

The idea of coming up with “productized” IP may sound daunting, but many partners find that they already had IP, and it just wasn’t packaged that way. The custom solution that was successful for one client could be beneficial to many customers who are trying to solve the same problem.

Review successful projects to see if there are repeatable elements that can be productized. Repeatable elements can be about a partner’s unique vertical or process best practices, or even focus on common customer pain points. Start small. The IP can be a simple template or just a few lines of code that automates a function in a way the market typically needs. Productizing IP and creating repeatable processes has been a very successful strategy for many partners. Some partners are achieving gross margins in excess of 70% by productizing IP and selling it to their customers on a recurring revenue basis. Productizing IP helps create stickiness with customers and opens up opportunities to sell solutions through the partner channel.

For partners who don’t want to create their own IP, they can also look to the partner ecosystem for incremental solutions that can be bundled with Microsoft’s offerings to round out the total solution. There are multiple opportunities for building intellectual property that can be used to expedite engagements, or even as an entire engagement. With the ability to create fully automated solutions, partners can challenge their creative side to offer up solutions that can save their customers money, as well as add a striking differentiator amongst peers. In the Microsoft Cloud Practice Development Study, 484 partners that identified as having an security practice were asked which intellectual property offerings they provide within their practice. The results are below.

Consider this data when designing intellectual property offerings.

<table>
<thead>
<tr>
<th>SECURITY INTELLLECTUAL PROPERTY BY REGION</th>
<th>Total n=484</th>
<th>APAC n=24*</th>
<th>Canada n=18*</th>
<th>CEE n=27*</th>
<th>Germany n=36</th>
<th>LATAM n=41</th>
<th>MEA n=32</th>
<th>UK n=43</th>
<th>US n=119</th>
<th>WE n=103</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity &amp; access control solutions</td>
<td>33%</td>
<td>38%</td>
<td>28%</td>
<td>37%</td>
<td>36%</td>
<td>39%</td>
<td>44%</td>
<td>21%</td>
<td>31%</td>
<td>30%</td>
</tr>
<tr>
<td>Information Protection Solutions</td>
<td>27%</td>
<td>21%</td>
<td>28%</td>
<td>37%</td>
<td>19%</td>
<td>34%</td>
<td>50%</td>
<td>23%</td>
<td>25%</td>
<td>19%</td>
</tr>
<tr>
<td>Mobility Solutions</td>
<td>26%</td>
<td>25%</td>
<td>33%</td>
<td>15%</td>
<td>36%</td>
<td>17%</td>
<td>38%</td>
<td>26%</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>Threat detection, monitoring and mitigation solutions</td>
<td>24%</td>
<td>29%</td>
<td>22%</td>
<td>15%</td>
<td>33%</td>
<td>15%</td>
<td>41%</td>
<td>21%</td>
<td>24%</td>
<td>22%</td>
</tr>
<tr>
<td>Auditing solutions</td>
<td>22%</td>
<td>17%</td>
<td>17%</td>
<td>30%</td>
<td>14%</td>
<td>34%</td>
<td>22%</td>
<td>19%</td>
<td>18%</td>
<td>24%</td>
</tr>
<tr>
<td>Customer Self-Serve Portals</td>
<td>21%</td>
<td>13%</td>
<td>33%</td>
<td>22%</td>
<td>17%</td>
<td>22%</td>
<td>34%</td>
<td>19%</td>
<td>20%</td>
<td>18%</td>
</tr>
<tr>
<td>Pre-Configured Dashboards</td>
<td>14%</td>
<td>17%</td>
<td>22%</td>
<td>15%</td>
<td>8%</td>
<td>22%</td>
<td>25%</td>
<td>9%</td>
<td>17%</td>
<td>9%</td>
</tr>
<tr>
<td>Turnkey BI Portals</td>
<td>6%</td>
<td>4%</td>
<td>17%</td>
<td>4%</td>
<td>3%</td>
<td>10%</td>
<td>9%</td>
<td>5%</td>
<td>7%</td>
<td>4%</td>
</tr>
<tr>
<td>We do not offer any of these intellectual property services</td>
<td>36%</td>
<td>42%</td>
<td>33%</td>
<td>33%</td>
<td>36%</td>
<td>32%</td>
<td>16%</td>
<td>49%</td>
<td>43%</td>
<td>36%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REVENUE</th>
<th>Total Median (n=309)</th>
<th>$41,091</th>
</tr>
</thead>
<tbody>
<tr>
<td>BY CUSTOMER FOCUS</td>
<td>SMB (n=269)</td>
<td>$38,211</td>
</tr>
<tr>
<td></td>
<td>Enterprise (n=40)</td>
<td>$472,222</td>
</tr>
</tbody>
</table>

When targeting intellectual property offerings, research with partners emphasized the importance of targeting the enterprise customer to attain significantly higher managed revenues.

Source: Microsoft Cloud Practice Development Study, MDC Research, June 2017.

aka.ms/practiceplaybooks
Creating Intellectual Property in the Security Practice

Making money in the cloud usually requires partners to partially retain IP to drive annuity. Annuity is a key strategic component to a cloud practice.

INTEGRATE SECURITY APIs TO DELIVER HIGH-VALUE INTELLECTUAL PROPERTY

Consider providing customized solutions that provide experiences for customers integrating the Microsoft Graph API (which provides access to data about emails, security events, users, files, and groups), the Office 365 Service Communications API (for reporting on service status), the Office 365 Management Activity API (to retrieve information about user, admin, system, and policy actions and events from Office 365 and Azure AD activity logs), the Microsoft 365 Secure Score API (for monitoring and reporting a secure score), the Azure Billing API (to monitor usage of Azure resources), and the Azure REST API (for integrating data from and managing Azure services). Use these APIs together to create solutions that provide integrated visualization, customized monitoring, and remediation workflows, and handle vertical-specific workloads.

PACKAGE THE PROCESS

Another way partners are creating IP in security practices is by packaging their assessments, documents, and processes into proprietary, reusable components that only they own and can deliver. For example, package a service around security monitoring that relies on the ongoing application and review of Secure Score.
Don’t be an ostrich. Cloud makes software your competitive advantage. We have packaged repeatable projects that are focused around rapidly demonstrating value within the cloud and identifying the big transformational opportunities.

ALEX BROWN
CEO, 10th Magnitude
Define Vertical Offerings

Resources

Delivering datacenter level networking expertise is critical to an enterprise hybrid cloud offering.

➔ Maximize profitability with vertical solutions
➔ Cloud Partner Strategy 2.0 Going Vertical

Consider Verticalizing the Security Offer

It is recommended that partners specialize by vertical, functional process, or technology.

EXAMPLES OF THESE TYPES OF SPECIALIZATION

- Vertical specialization: manufacturing, banking, retail
- Functional process specialization: accounting, human resources, marketing campaign management
- Technology specialization: systems management, analytics, enterprise resource planning

Think about it this way; if there is lack of differentiation in the market owing to approaches like verticalization, then price becomes the primary differentiator between one partner and the competition. This can erode margins and trap a partner in a business they can’t afford to invest in as prices race to the bottom in order to win customers.

It is important to become the established expert in selected areas. Focus on a specific technology or become known as an early adopter and technology leader. But the real value comes from IP or expertise in an industry, vertical, or business process. The combination of adding IP to a vertical or business process expertise makes that advantage even more powerful.

Research with partners suggests mastering one specialization before adding additional ones. It is easy to be distracted by saying “yes” to every request and diversifying into too many offerings. But in the long run, it is better to say “no” to projects outside an organization’s focus area. Partners have shown benefit from having a strict focus on one key solution and expanding one vertical at a time.
Define the Pricing Strategy

Pricing security offering is no longer determined simply by cost plus margin.

Review this four-step approach to determine how to best price cloud-based security solutions.

Step 1: Evaluate the Customer Value of the Offer

Pricing a product or offering is different in today’s marketplace. Increasingly it is about return on value (ROV) — the added benefits (e.g., better per-unit price, improved service characteristics) customer get by being loyal customers (e.g., buying contracts with longer durations, making upfront payments, etc.). Customers will only pay as much as the value they estimate they will get from the offering.

Three value categories may be considered.

- **Direct value** is the value that a partner can measure in the customer accounting books, and it can be either incremental revenues or cost reductions. For example, selling an E-Commerce solution to a retailer may lead the partner to reach new customers and generate more revenues. Or, selling a Device as a Service, may lead the customer to end his contract with maintenance company and result into immediate and tangible savings.

- **Indirect value** is the value that is real and tangible but can hardly be seen in the customer company books. For example, by subscribing to Microsoft Dynamics CRM, a customer’s sales team may increase its productivity by 20% although it may not result in immediate incremental revenues.

- **Operating value** suggests better results on key performance indicators defined by the customers such as reputation, employee retention rate, or product quality.

Estimating the value of an offer for the customer will enable a partner to set a price range that should ideally be appreciated as a great return for his business.
Step 2: Select a Relevant Price Unit

As usage becomes the currency of the Cloud era, a **price per user** is increasingly popular and applied for many solutions. Yet, it may not be applicable for all solutions where user is not the main variable. We may select a **price per application** instead, or a **price per group of indicator** for a BI solution or even a **price per result**. Whatever unit is chosen it should suggest a sense of freedom for the customer likewise subscribers of mobile phone plans do not feel constrained by the number of calls they can make anymore.
Step 3: Define Price and the Variation Model

STANDARD PRICING

Pricing is the consequence of the product and aligns to the accepted industry/application standard. Think of this as reference pricing; as in customers have seen similar products sold for this amount, so partners price their offer so that it is similar. What’s the standard price for a mobile phone app? $0.99. If a partner charges more, he is breaking from the industry accepted, standard pricing. This is an old way to look at pricing. Buyers today will accept this model, but they do not prefer it and it provides minimal help in getting the partner offer purchased.

VIRTUOUS PRICING

Virtuous pricing is about using the price as a sales weapon. The goal of virtuous pricing is to create a virtuous sales cycle within customers, where each sale encourages the next sale within the customer organization. It fosters product adoption and proliferation. Let’s begin with a counter example of what is not virtuous pricing — a fixed price per user. Here, a partner has a simple pricing structure (which is important), but there is nothing to encourage more aggressive purchasing by the customer.

Enter digressive pricing, which drops the per-unit price with the purchase of more units. Customers get a discount per unit price the more they buy. This can help create a virtuous sales cycle within the customer because now the customer is looking for way to bring their cost per unit (e.g., user) down.

For example, assume one line of business has already purchased 19 users at $49 per user. Now, there are discussions within another line of business within the same customer organization to purchase a similar product from a competitor or buy from the current partner. The existing customer is incentivized to lobby on the existing partner’s behalf because if the other line of business purchases that partner’s product, their cost per user will drop to $39 per user. And the cycle can continue as each new group evaluates the solution offering.

There is a way to adjust digressive pricing slightly to make it significantly more profitable — step pricing. This method sets the price for each step as the top number of users in the range. Building on the example from digressive pricing, let’s say that the customer purchased 15 users. They would pay for the equivalent of 19 users since that is the price for this range of units.

Why is this more profitable? Because the customer is effectively paying for the 4 users they are not using (yet) — which goes straight into the partner’s profits. What’s more, the virtuous sales cycle has been amplified because the customer wants to get as close to the maximum number of users for the step as possible in order to get the lowest possible cost per unit.

VIRTUOUS PRICING

<table>
<thead>
<tr>
<th>Pricing Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed pricing</td>
<td>Regardless of the number of users</td>
<td>$495/user</td>
</tr>
<tr>
<td>Digressive pricing</td>
<td>From 10 to 19 users $495/user</td>
<td>More attractive</td>
</tr>
<tr>
<td></td>
<td>From 20 to 49 users $395/user</td>
<td></td>
</tr>
<tr>
<td></td>
<td>From 50 to 100 users $295/user</td>
<td></td>
</tr>
<tr>
<td>Step pricing</td>
<td>More profitable</td>
<td>$295*100=29500$ (*Theoretical User Price (T.U.P))</td>
</tr>
</tbody>
</table>

©2019 Lemon Operations
Step 4: Evaluate Creative Pricing Models

**FLAT RATING** is one of the most powerful business pricing strategies. Flat rating pricings is leveraged by banks, insurance, etc., every time a customer pays premiums. While it can have varying levels of sophistication (banks and insurance firms use sophisticated versions of this based on significant work by their actuaries), the model can be described and implemented in a simple fashion. The basic idea is that a partner provides a certain quantity of value for a set cost that all customers pay. Some customers may come close to (or even exceed) using the full value of what they pay for, while the rest are nowhere close. A well-crafted model identifies the average consumption across all customers, and creates a situation where more than 80% of the customers are using less than what they are paying for (and ideally less than the average consumption) and fewer than 20% are using more. Set the price above the average consumption. By doing so, the 80% of clients who use less than what they pay for drive the profit. The further they are below the average consumption, the more profit they generate. For the 20% who use more than they pay for, the partner might take a loss on them individually. However, in the aggregate, the long tail more than covers the cost of heavy consumers, and these heavy consumers are likely to be a partner’s biggest champions. So, there are tangential benefits to supporting their cost. Models built around flat rate pricing have shown between 1.5 and 3 times as much profit as traditional models.

![FLAT RATING Diagram](https://example.com/flattagram.png)
Another consideration of pricing strategy is whether to charge customers an upfront fee.

Reasons for doing so include providing some working capital to get resources going in the early days of a practice, mitigate the risk that a customer abandons a project without any payment and ensure the customer is as invested in a project. It can also serve to minimize financial impact to a practice when the customer has requested longer payment terms.

In a survey of 1,136 Azure partners, only about half charged an upfront fee for project or managed services. When an upfront fee was requested, it was typically less than 25% of the total project or managed services fee.
PAYMENT TERMS

The final consideration for pricing strategy is the payment terms. This is defined as the duration of time between when the customer is invoiced for service rendered and when payment is received from the customer.

Payment terms are measured in days; for example 10 days, 15 days, 30 days or 90 days. These are usually expressed as NET 10, NET 15, NET 30 or NET 90 payment terms. In addition, partners might consider offering the customer a discount for prompt payment on the shortest payment option. For example NET 2/10/30 is used to describe terms where a 2% discount is provided for payment received within 10 days of invoicing, otherwise the full invoice amount is due in 30 days.

The Microsoft Cloud Practice Development Study found that the most common payment terms used was NET 30, and that for SMB customers shorter payment terms were preferred.

PRICING COMMUNICATION

Price is rarely mentioned on service provider websites. The sales copy speaks of partnerships and the price is often revealed only after speaking to a sales representative. In an offer-based strategy, this will not work. In the business of cloud, price is always disclosed up front. Because price is part of the value proposition and solution offer, pricing is something partners can be proud to share. Partners are in a race against themselves and the competition. Show pricing early, removing any customer concerns.
Identify Partnership Opportunities

Partner to Partner

Facilitate growth opportunities and fill solution and talent gaps through partnerships

Learning how to develop successful partnerships with others in the Microsoft partner ecosystem can drive efficiencies, revenue and profits. Digital transformation is changing the way partners approach their marketplaces. It requires the delivery of integrated solutions to address unique customer needs, the capacity to scale and reduce the cost of selling into new markets.

Partnering together successfully starts with defining a partner’s value as a business and goals. That means answering questions such as: What’s the mission statement regarding partnerships? How will partners benefit from and monetize the solutions? What gaps are in the offerings that could be filled by strategic partners? What steps are necessary to engage with partners in a structured way?

PARTNER-TO-PARTNER SUCCESS FORMULA

To help partners capture these opportunities, Microsoft has collected the strategies, best practices, and resources for successful partner-to-partner (P2P) collaboration. The partnering success formula is a three-stage framework for establishing and managing effective partnerships:

- **Ready** – At this stage partners are laying the groundwork for P2P success, defining the value of a partner and their own value as a strategic partner. Partners need to assess their investment, value chain, solution and talent gaps, and go-to-market partnering plan.
- **Connect** – Identify and win strategic partners, go to market together and effectively manage the partnership. Get more granular on how to sell and close deals, with an understanding of how to will review the business.
- **Grow** – Maximizing the partner opportunity means constantly pushing for better results and seeking new and better partnerships to drive deeper penetration in the existing customer base and expand the customer base with joint offerings and investments. Partners are executing joint marketing strategies to expand market reach, generate leads, and increase customer loyalty and retention.

See the full partnering success formula in the Power of Partnership Guide: [https://aka.ms/p2pguide](https://aka.ms/p2pguide).

aka.ms/practiceplaybooks
THE ISV + CHANNEL-BASED MSP COMBINATION

With a little help from a channel-based MSP, an ISV partner can earn greater reach for its IP solutions. Likewise, a partnership with an ISV can lead to an expanded partner channel for channel-based MSPs. Some partner combinations meld together well to create success. To help find the right mix, here’s a partner recipe for success we know works.

ACCELERATING DIGITAL TRANSFORMATION

The pace of change impacts how partners work together and add value. New business models, subscription pricing, and resource gaps make partnering essential to scale and respond to these conditions. Microsoft has linked up its network of partners, making it possible to access the greater partner ecosystem, reduce the cost of selling, increase efficiency and solution delivery, and drive profits.

See the Power of Partnership Guide: (https://aka.ms/p2pguide) for more details.
Define Engagement Process

Pre-Sales, Post Sales, and Support

Define the technical effort required before the sale (pre-sales), after the sale (post-sales), and in support of the sale. Understand the technical pre-sales and post-sales requirements for a solution offer.

**PRE-SALES**

The technical effort required to make the sale involves:

- Discussing the customer requirements and address their objections.
- Developing technical pitch decks.
- Providing a technical demo. This demo may be generic or may need customization to the better meet the requirements of the customer. The goal of the technical demo is to inspire confidence in the partner’s ability to deliver the desired solution by demonstrating they have “already done something like it before.”

**POST-SALES**

For guidance with sales efforts, consider the learning paths available in the [Microsoft Partner Network Training Center](https://aka.ms/PracticePlaybooks).

Leverage these presentations which can be used for technical briefings or sales pitches:

- **SMB Security Practice Go-to-Market**
- **Enterprise Security Practice Go-to-Market**
- **GDPR Go-to-Market**

Partners should customize each presentation to explain how their unique offering makes the overall solution a true differentiator.

Leverage [Partner Technical Services](https://aka.ms/PracticePlaybooks) available from Microsoft to help build technical capabilities faster to accelerate sales, deployments, and app development.
Implementation Process

The process partners follow in delivering their solutions to customers is just as important as the technologies used to deliver it.

When it comes to delivering solutions for a security practice, consider that the processes a partner defines become an important part of his intellectual property.

As a starting point, consider the following four phases for a security practice:

- **Assessment**: Raise the customer’s awareness of their security environment, risks, threats, and opportunities for improvement.
- **Consultation**: Work with the customer to provide process and technology recommendations.
- **Implementation**: As a service provider, help the customer’s implementation in one of three ways: Be the expert guiding their resource to do the work based on recommendations; Be the extra “pair of hands” helping them with their implementation; or be their implementation partner, balancing guidance and hands-on work.
- **Ongoing support**: Provide managed services that give the customer ongoing access to support and expertise, while receiving perpetual revenue. An important security service related to this is incident response — being the expert on call to help a customer resolve a security incident.

aka.ms/practiceplaybooks
Stay Informed on Security and Compliance Matters

The Microsoft Trust Center and Office 365 Security and Compliance Center are two resources to be familiar with when defining a Security practice strategy.

Microsoft Trust Center

Microsoft Trust Center is a resource for learning how Microsoft implements and support security, privacy, compliance, transparency in its cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud initiative and provides support and resources for the legal and compliance community.

THE TRUST CENTER SITE PROVIDES:

- In-depth information about security, privacy, and compliance offerings, policies, features, and practices across Microsoft cloud products.
- Recommended resources, a curated list of the most applicable and widely-used resources for each topic.
- Information specific to key organizational roles, including business managers, tenant admins or data security teams, risk assessment and privacy officers, and legal compliance teams.
- Direct guidance and support, including options for contacting Microsoft.
Office 365 Security & Compliance Center

The Office 365 Security & Compliance Center is the one-stop portal for protecting data in Office 365. Use it to help address data protection or compliance needs, or to audit user activity in an organization. Use the Office 365 Security & Compliance Center to manage compliance for all of an entire organization’s data across Office 365 and manage eDiscovery searches and holds, access for mobile devices, and more.

THE SECURITY & COMPLIANCE CENTER INCLUDES CAPABILITIES FOR:

- **Alerts**: View and manage alerts for an Office 365 organization, including Advanced Security Management alerts.
- **Permissions**: Grant permissions to people who perform compliance tasks like device management, data loss prevention, eDiscovery, and retention.
- **Threat management**: Manage mobile devices and set up data loss prevention for an organization. Help protect inbound and outbound messages from malicious software and spam. Manage which apps have access to Office 365.
- **Data governance**: Import email from other systems. Enable archive mailboxes or set policies for retaining email and other content within an organization.
- **Search & investigation**: Search for content and review user activity. Use eDiscovery to manage cases and set up supervisory review policies to help capture communication for review.
- **Report**: Use a variety of reports to help understand how the organization is using Office 365, including reports related to auditing, device management, Supervisory review, and data loss prevention. View user activity reports such as sign-ins for SharePoint Online, Exchange Online, and Azure Active Directory.
- **Service assurance**: View details about how Microsoft keeps Office 365 customer data safe, and how Office 365 helps customers meet industry compliance requirements.
Calculate Azure Practice Costs

A practice relies on Azure services to deliver customer success, so understanding the Azure related expenses incurred in delivering a customer solution is critical.

In research of 1,136 Azure partners, enterprise-focused partners spent a median of $8,107 in Azure for research and development annually; whereas SMB-focused partners spent a median of $1,933 annually.

![Annual Azure Consumption](source: Microsoft Cloud MDC Research, November 2016)

Use the Azure Pricing Calculator to estimate Azure costs and be sure to check the resources list for pricing on the various services within EMS. Partners can build an estimate online and export it to Excel for further refinement and analysis. This tool also gives the retail rates (also known as the Pay-As-You-Go option) for Azure services, so treat it like the “high end” of a consumption estimate.

Become familiar with the discounted pricing and Azure credits:

- **Graduated Pricing:** Services like Azure Storage have tiered pricing based upon the volume used. For example, in November 2019, if partner used less than 50 TB per month it would cost $0.0184 per GB per month, but if he used significantly more it could drop to $0.017 per GB per month.

- **Enterprise Agreement:** By making a three-year monetary commitment, Azure services are available at a discount off retail rates. To learn more, see Enterprise Agreements.

- **Azure Credits:** Microsoft Partners can receive Azure credits as a part of their benefit. For example, partners with the Silver Cloud Platform Competency receive $500 USD per month in Azure credits; those with Gold Cloud Platform Competency receive $1,200 USD per month in Azure credits.

It can be helpful to identify items which are used elastically versus items that have a fixed monthly cost. Significant savings can be achieved via elastic use of resources because they can be turned off (or paused) when not in use.

**FOR EXAMPLE**

- **Elastic:** SQL Data Warehouse is used only during month-end calculations; it can be paused the rest of the month. Another example of elastic use is to leverage auto-scale capabilities of the resource, such as auto-scaling the number of App Services instances down in the evenings and back up during the workday.

- **Fixed:** Azure App Service can hosting a website in a Web App. This App Service needs to run 24x7 because visitors will arrive at all hours.

Finally, for those who don’t understand how much of a given resource will used, consider building a scaled down proof-of-concept to get a first estimate.
AZURE COST MANAGEMENT

In addition to the Azure Pricing Calculator, partners can also use Azure Cost Management that is natively available thru the Azure Portal. This service helps partners monitor cloud spend, drive organizational accountability, and optimize cloud efficiency. Through a series of dashboards, partners can get an idea of how their organization is using Azure resources and where their budget dollars are going.

Azure Cost Management gives a high-level overview of usage metrics breaking them down by services and assets, as well as forecasts of cloud spend.

RESOURCES

➔ Azure Pricing Calculator
➔ Enterprise Agreements
➔ Azure Active Directory Pricing
➔ Azure Information Protection Pricing
➔ Microsoft Intune Pricing
➔ Advanced Threat Analytics Pricing
Identify Potential Customers

Build a prospect hit list

To build a list of prospects that could potentially turn into customers, create an awareness campaign to draw attention to security practice service offerings and uses previous customer success to earn additional business with customers and the industry at large.

Use these awareness activities to help generate new customers:

**WEBINARS AND PODCASTS**
A great way to transfer knowledge, establish expertise, and pique the interest of potential customers.

**REFERRALS**
Ask for referrals in email and phone calls when talking with existing customers, partners, and vendors who might know someone who is ready for the services.

**WHITE PAPERS**
These are a great way to build credibility with decision makers. Technical staff often expect a white paper to help them understand underlying architecture and technology of the solutions.

**NEWS ARTICLES**
Leverage public relation efforts to drive publicity around the technology, things being done in the market, and other topics of current interest.

**SOCIAL MEDIA**
Social media such as Twitter, LinkedIn, etc., is a place to build awareness, reputation, and customer satisfaction — and gain new customers.

Also, consider offering services as a pilot project to prospects. With a pilot project, the customer receives two important values. First, they get to better understand how the project goals will be successful. Second, they have a production-grade starting point for their larger efforts.

It is important to keep the distinction between proof-of-concept (PoC) and pilot clear. A PoC should never be considered for direct deployment into production; whereas a pilot should be constructed with a production release in mind.
Join the Microsoft Partner Network

Partnering with Microsoft

The Microsoft Partner Network is the start of a journey. One of the first steps to partnering with Microsoft for an Azure practice is to join the Microsoft Partner Network if not already a member. As a partner, resources like training, whitepapers, and marketing material described in this playbook are accessible. It’s also where users can be set up to gain Microsoft Partner competencies and access to partner benefits.

TO BECOME A MICROSOFT PARTNER

The Microsoft Partner Network provides three types of memberships. Each type provides a set of benefits to help partners grow their business. As partners achieve goals, they can participate in the program at the level that suits their unique needs, so they can access more benefits and develop a relationship with Microsoft and other Microsoft Partners.

- **Network Member**: Receive a set of no-cost introductory benefits to help save time and money. New partners can use these resources to help build their business and discover next steps.
- **Microsoft Action Pack Subscription (MAPS)**: This affordable yearly subscription is for businesses looking to begin, build, and grow their Microsoft practice in the cloud-first, mobile-first world through a wide range of software and benefits.
- **Competency**: Get rewarded for success with increased support, software, and training.

**TAKE THE NEXT STEP WITH A COMPETENCY**

As a competency partner, both gold and silver competencies can be earned in one or more areas. A silver competency can help businesses demonstrate expertise or a gold competency can showcase the business's best-in-class capabilities within a Microsoft solution area. Later in this playbook we'll review the competencies relevant for launching a successful security practice.

**CLOUD ENABLEMENT DESK**

The goal of the Cloud Enablement Desk is to assist partners in obtaining their first Silver Cloud Competency. Partners will be assigned a Cloud Program Specialist (CPS) for up to six months on their way to obtaining their first Silver Cloud Competency.

The Cloud Enablement Desk program requirements include:

- Partner must have a MPN ID.
- Partner must agree to and sign Conditions of Satisfaction that state partner is actively trying to achieve Silver Cloud Competency status and include the name of the primary contact person.
- Partner cannot have an existing Microsoft account management relationship.
Identify Sales Incentives

Compensation for sales executives is an area all partners grapple with. Without the right mix in compensation, it’s difficult to attract and retain the best people, and drive the offers deliver the best long-term value. Our research revealed three core principles of sales compensation.

**REWARD A SALES ACTION**

This means rewarding an array of sales activities, not just the final close. Sometimes this can be challenging. The reward does not have to be big, but there must be something to reward the right sales behavior that will lead to the final sale.

**THE LEVEL OF INCENTIVE VERSUS REQUIRED SELLING EFFORT**

Not all sales are created equal. Sometimes a renewal, for instance, can be much easier than acquiring a new customer. Consideration must be given to effort put in when setting up a compensation model. Reward the right behavior that get the right result. Don’t over-compensate for routine activities that require less effort and expertise. Consider how much of the sales process can be done by lower-level sales staff versus the sales executive. This is also a way to keep sales compensation costs manageable.

aka.ms/practiceplaybooks
SIMPLE ENOUGH TO BE UNDERSTOOD AND DRIVE ACTIONS

Always keep it simple. Sales people are brought on for their ability to communicate, engage and educate customers, and the always-important act of closing. Don’t overly complicate the sales actions required in order to be compensated. Drive the behavior that leads to closing business. Reward that behavior and get reps to see it through to the close of business.

Remember that everyone is a seller in most companies. It’s important to train all employees in appropriate sales techniques. Everyone should be on the lookout for existing customer opportunities as well as new ones. Teach them the signs and how to react. Reward everyone in the company for positive sales behavior.

SALES COMPENSATION VARIABLES

When deciding how to calculate the compensation for sales incentives, consider the variables that help describe the magnitude of the benefit of the sale to the company and the effort required to close the sale. Examples include:

- **Expected duration**: How long is the contract for? Longer contracts are more lucrative to the company and should have higher valued incentives.
- **Expected number of units**: How much of the service is purchased? Higher quantity purchases deliver more value to the company and should have higher valued incentives.
- **Feature options**: Some features are more profitable to the company than others. Consider incentivizing the higher profit margin features with higher valued incentives to drive sales.

POSITIONING THE OFFER VIA INCENTIVES

Depending on the maturity of the practice, partners may have to create different incentives to encourage the selling of the offer. The above diagram illustrates a decision-making process partners can follow to fine tune their incentives based on how the offer’s incentives compete with other company incentives.

aka.ms/practiceplaybooks
Identify Solution Marketplace Platform

Resources

Azure Marketplace

Azure Marketplace is an online store that enables ecosystem partners to offer their solutions to enterprises and Azure customers around the world. Within a single, unified platform, customers can easily search, purchase, and deploy solutions on Azure with just a few clicks.

Azure Marketplace is the source for thousands of software applications and services certified by Microsoft to run on Azure. Azure Marketplace supports offers that include virtual machines, developer services, and solution templates.

Azure Marketplace gives partner solutions exposure through the marketplace page and the listings integrated with the Azure Portal. For example, HDInsight Applications are integrated into the steps users take to deploy an HDInsight cluster (so users could layer an application atop their HDInsight cluster), but are also available via the Marketplace blade of the Azure Portal.

The process of getting a solution listed in the Azure Marketplace is referred to as getting Microsoft Azure Certified. This comes with benefits, many of which include select benefits from the MPN Silver Cloud Competency.

CERTIFY APPLICATIONS AND SERVICES

Solutions sold in the Azure Marketplace must be Microsoft Azure Certified. This provides assurance to customers that the offers have been tested for usability, readiness, and compatibility with Azure.

- Access broad-reaching Microsoft marketing channels, and receive co-marketing assistance and promotion outside of a Azure Marketplace listing.
- Leverage technical and business planning support to help maximize ROI.
- Utilize a self-service portal that contains ready-to-use marketing resources to enhance communications and messaging.
- Take advantage of resources, such as the Sales Accelerator Toolkit and credits for display, and search advertising to help drive customer adoption.
Hire & Train
Security

aka.ms/practiceplaybooks
Executive Summary

Now that the various services partners can pursue to set up or build a security practice have been reviewed, it’s time look at what is necessary to build and train a team to deliver these services.

First, let’s define the roles needed for this practice and the skills they should bring to the table. If it’s necessary to need to hire to fill gaps, there are detailed job descriptions that can be used, as well as ideas on where to look for resources, the factors to consider in a candidate’s skillset, and what to expect to pay by role and region.

A big focus of this section is the critical piece of ensuring all practice resources are trained and continue to receive ongoing training. We cover not just the technical training, but also sales and marketing training.

Finally, review the specific Microsoft certifications technical resources should be working towards, both for their own professional development and to help partner organizations earn Microsoft Partner Network competencies.

Top 5 things to do

Make sure to nail down these tasks before moving to the next section.

- Define the members and roles required
- Identify capability and skills gaps
- Decide which skills to hire and train
- Hire to fill gaps
- Train and certify technical roles
Create a Hiring Plan

Human resources are a critical asset to any services-based practice. Starting a new practice requires an evaluation of existing team members (if any) and then make the decision on whether to hire new employees or bring existing team up to speed.

The following sections describe the recommended resources across sales, technical and support functions that will likely be needed. In many practices that are just getting started, partners may not be able to fill all roles with individual professionals. In this situation one person will likely be required to fulfill the duties of multiple roles.

Partner Skillsets

Referrals and LinkedIn are top sources for identifying skilled labor. Once a candidate is identified, work history, cultural fit, and years of experience become the important considerations.

Roles associated with cloud practices typically have at least 3 years of experience. Furthermore, most companies engage in at least annual ongoing staff learning efforts like conferences/events and online training. A median of 8.5% of technical resource time is spent on training.

RESOURCES

- Recruit, Hire, Onboard and Retain Talent Playbook
- Microsoft Digital Transformation eBook 3: Empower Employees

aka.ms/practiceplaybooks
Hire, Build, and Train The Team

Sales Resources

Even the best products need a sales strategy to gain maximum market traction. Consider hiring for the following sales positions for broad reach.

The **Solution Sales Manager** (SSM) is a senior leader within the enterprise sales organization. The SSM leads, develops, and manages a team of high-performing sales and technical pre-sales/post-sales resources to drive solution opportunity revenue and market share by leveraging the Microsoft Security and Cloud offerings to meet their customers’ Mission Critical Tier1 security needs. Ten or more years of sales experience is required for this position. Qualifications include people management, business development, competitive selling, and the ability to thrive in complex, ambiguous, and dynamic environments.

The **Cloud Solutions Sales Manager** is a solution sales leadership role that is responsible for delivering sustainable new business growth across segments; providing thought-leadership; and driving customer acceleration to cloud and security across the enterprise sales and marketing teams. The Solution Sales Manager is a great sales coach and leader, has a challenger mentality, is savvy in sales leadership practice, and contributes with vision and flawless execution of solution sales across workloads and solution areas.

The **Technical Sales Manager** (TSM) is a senior leader within the enterprise sales organization. A TSM drives revenue and market share by leading a team of technical sellers that provide customers with insights and solutions. The Technical Sales Manager will manage, coach, and lead a team of solution architects and tech sales professionals to uncover and support the business and IT goals of customers by driving the technical decision and providing business value with the Microsoft platform, thus securing long-term sustainable growth. A computer science degree or related field is required for this role. Additional qualifications include strategic insight, project management, analytical problem solving, customer/partner relationship building, and exceptional product and technical expertise.

Technical Resources

(Architecture, Infrastructure, and Development)

These roles form the heart of a security solution. Hiring the right people can turn a vision into reality.

A **Cloud Architect** (CA) drives customer initiatives in collaboration with customers. The CA is a technical, customer-facing role that is accountable for the end-to-end customer cloud deployment experience. CAs own the technical customer engagement, including architectural design sessions, specific implementation projects and/or proofs of concepts. The ideal candidate will have experience in customer-facing roles and success leading deep technical architecture and application design discussions with senior customer executives to drive cloud deployment. A computer science or related engineering degree is required.

The **Mobility Solution Engineer** is responsible for the design, implementation, integration, support and monitoring of enterprise mobility solutions. The ideal candidate should have a diverse understanding of the current state of security best practices, including identity and access control, mobile technology, and mobile best practices throughout a variety of industries. In addition, this individual must have working knowledge of mobile development standards, can identify a landscape of mobile vendors (MDM, MADPs, etc.), and be familiar with the deployment of mobile applications across platforms. The candidate must have prior experience formulating, planning, and implementing a mobile strategy, including formulating policies for “bring your own device” (BYOD) policy and remote access. The candidate should have outstanding technical and analytical skills to outline why a
mobile strategy is needed, and how to identify and prioritize applications, data, and devices to manage.

The **Identity Solution Engineer** is responsible for the design, implementation, integration, support, and monitoring of enterprise identity and access control solutions. The ideal candidate should have a diverse understanding of the current state of security best practices, including identity and access control, mobile technology, and best practices throughout a variety of industries. In addition, this individual must have a strong knowledge of identity standards and protocols, as well as a deep skillset with Windows Server Active Directory and industry security solutions.

**Management**

Consider the following management positions if development effort will involve eight or more technical staff. In smaller teams, senior-level employees sometimes take on management duties along with their other responsibilities, removing the need for dedicated managers.

The **Product Manager** (or Product Management team) establishes and sustains the business case for the project and plays a key role in identifying and setting priorities across the target audience. This includes ensuring that business expectations are clearly articulated and understood by the project team, and that the functional specifications respond to business priorities.

Product Management owns the vision statement for the project. The vision statement is an informal document that communicates the expectations and assumptions on which the project is based.

Product Management is also responsible for high-level project communications such as business projections, project costing, and contract negotiation. Product Management communicates the high-level milestones to the target audience and other team members.

The **Program Manager** or Program Management team “owns” the specification for an application’s features and functionality and coordinates the day-to-day communication required to develop and deliver the application effectively and consistently within organizational standards.

Program Management has a key communication and coordination role. With input from other team leads, Program Management assists Product Management in articulating the vision for the project. Using this vision, Program Management drafts the initial version of the functional specification and is considered the keeper of the functional specification. Program Management is responsible for all activities associated with analysis, specification, and architecture. Program Management is also responsible for defining how the project will interoperate with external standards, maintaining external technical coordination and communication, and managing the master schedule.

**Support Resources**

A lot of effort goes on behind the scenes, or in positions that involve post-sales customer engagement. To ensure long-term success of projects, consider hiring some of these support roles.

A **Customer Success Manager** is passionate about engaging customers and helping them expand their use cases. They have excellent relational skills, and can create win/win environments for all parties they work with. In their day-to-day responsibilities, they own the overall relationship with assigned clients by increasing adoption and ensuring retention and satisfaction. They make a large impact on enterprise security business by establishing a trusted and strategic advisor relationship with each assigned client, driving continued value of the products and services. The Customer Success Manager will help drive sales by working to identify or develop upsell opportunities. Additionally, they will advocate customer needs and issues cross-departmentally and program manage account escalations. Qualifications include prior experience in customer success or equivalent history of increasing customer satisfaction, adoption, and retention.
A **Quality Assurance (QA) / Test Technician** is thorough and detail-oriented, and should work well with established processes. The primary goal of this role is to help avoid defects in the final product or solution. This person will be involved throughout the development process and use their intuition to problem solve and identify technical, procedural, and usability concerns. They must take meticulous notes, be organized about recording process steps, and work well with others since they will be coordinating with technical and management teams to ensure that the correct measures are put into place to align the final product with the initial goal.

An **Information Security Analyst** assesses and provides security advice on cloud infrastructure, including network, service, and application components. This role conducts risk assessments and architectural reviews, provides cybersecurity subject matter expertise, and assists in the building and design of secure solutions. Additional duties may include network and application penetration testing, and support for cyber security investigations, as well as on-call response for cyber security incidents. A computer science or related engineering degree is required, or the equivalent combination of education, professional training, or work experience.

A **User Support Specialist** assists customers who are having technical issues with the product, or who need help realizing the full benefit of the solution to help them deliver their cloud-based workloads. They will likely be in a position to help customers navigate the operational challenges of cloud computing, so thoroughly training them on both the product — and the infrastructure on which it is built — is paramount to their success, and ultimately, the customers’ satisfaction. Qualifications include technical support experience and great communication and interpersonal skills (soft skills). Experience with cloud technologies is a major plus.

A **Data Protection Officer** assesses and advises across the company group for data protection and privacy matters related to security. This role is a subject matter expert in the handling of personal data, and ensures there are policy and compliance processes to comply with local data protection legislation. Expert knowledge of global and national data protection law and practices, as well as the General Data Protection Regulation (GDPR) is a requirement, as well as the ability to fulfil the tasks referred to in Article 39 of the GDPR. Experience in conduction data privacy compliance, reviews, and audits is beneficial.
Job Descriptions

The following tables provide detailed job descriptions that can be utilized to hire the key technical resources. All technical skills, non-technical skills, certifications, and technologies listed are potential items a candidate should have, but no candidate will have all the items listed.

### Cloud Administrator

A Cloud Administrator manages cloud tenants. They should be the interface with the support engineers and the cloud provider support. They deploy cloud applications based on deployment templates and DevOps processes and have deeper technical knowledge of the various cloud technologies (Networking, IaaS, PaaS, Security) than a support engineer. Cloud Administrators also manage the license assignments for cloud users across your various SaaS applications.

- **Top Qualities:** Problem Solving (69%), Highly Organized (41%), Integrity (28%)
- **Previous Roles:** IT Administrator (67%), Network Engineer (45%)
- **Certifications:** MCSA, MCSE (38%), MCITP (14%), Cisco Certified Network Associate (CCNA) (10%), Cisco Certified Network Professional (CCNP) (9%)

<table>
<thead>
<tr>
<th>Technical Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep understanding of cloud computing technologies, business drivers, and emerging computing trends.</td>
</tr>
<tr>
<td>Strong foundation in system administration, including performing backups, upgrading and patching, performance tuning, monitoring, alerting, deployments, and disaster recovery.</td>
</tr>
<tr>
<td>Understanding of infrastructure design, including public and private cloud, networking, virtualization, identity, security and storage.</td>
</tr>
<tr>
<td>Experience deploying &amp; managing the infrastructure for databases (e.g. SQL Server, Oracle, Maria, Cassandra).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Non-Technical Skills</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proven track record of building deep technical relationships business leaders, creating rich technical documentation, and following industry standards.</td>
</tr>
<tr>
<td>Background in software license management.</td>
</tr>
<tr>
<td>Analytical and process oriented, with a proven track record of driving decisions collaboratively, resolving conflicts and ensuring follow through.</td>
</tr>
<tr>
<td>Problem solving mentality leveraging internal and/or external resources.</td>
</tr>
<tr>
<td>Exceptional verbal and written communication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory, Ansible, AWS, Azure, CentOS, Chef, Citrix, Confluence, Docker, Excel, firewalls, Jira, Microsoft Project, MySQL, Node.js, Office 365, PostgreSQL, Puppet, ServiceNow, SharePoint, SQL Server, Visio, VMware</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Programming/Scripting Languages</th>
</tr>
</thead>
<tbody>
<tr>
<td>C#, Java, JavaScript, Perl, PowerShell, Python, Ruby, SQL</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux, Windows</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Certifications</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://aka.ms/azureadmin">Microsoft Certified: Azure Administrator Associate</a>, MCSA Cloud Platform, MCSE Cloud Platform and Infrastructure, CompTIA Security+, AWS Certified DevOps Administrator, Google Cloud Certified Professional Cloud Architect</td>
</tr>
<tr>
<td>Exam priority: <a href="https://aka.ms/azureadmin">Microsoft Azure Administrator AZ-103</a>, <a href="https://aka.ms/azureadmin">Microsoft Azure Administrator AZ-104</a>, <a href="https://aka.ms/azureadmin">Implementing Infrastructure Solutions 70-533</a> (retired), <a href="https://aka.ms/azureadmin">Microsoft Azure Infrastructure and Deployment AZ-100</a> (retired) and <a href="https://aka.ms/azureadmin">Microsoft Azure Integration and Security AZ-101</a> (retired) or <a href="https://aka.ms/azureadmin">Microsoft Azure Administrator Certification Transition AZ-102</a> (retired)</td>
</tr>
</tbody>
</table>
## Project Experience Types/Qualities

- 3+ years of implementing and maintaining cloud monitoring systems and monitoring cloud services for errors and issues.
- 5+ years of setting up and deploying large software packages to cloud systems.
- 3+ years migrating on-premises environments to cloud, virtual network deployments, and cloud security implementations using best practices.
- 3+ years of setting up and maintaining hybrid backup and restore systems.
- 5+ years of experience with scripting and DevOps for cloud.

---

## Compliance Officer (Data Protection Officer)

Compliance Officers, or Data Protection Officers, are responsible for ensuring that data is kept safe and secured throughout your various technology solutions. They work with internal and external data processors to ensure that legal regulations are followed. These individuals are to work with legal bodies and the internal and external legal teams when litigations via lawsuits are involved. They work hand in hand with your Security Architects and Analysts to discover, remediate and resolve compliance issues and unauthorized data breaches.

- **Top Qualities:** Highly Organized (48%), Integrity (45%), Written communication (36%)
- **Previous Roles:** Security Architect (31%), Technical Program Manager (26%), Solution Architect (24%)
- **Certifications:** Certified Information Systems Security Professional (CISSP) (16%), Certified Information Systems Auditor (CISA) (12%), Certified Information Security Manager (CISM) (10%)

---

## Technical Skills

- Solid understanding of modern cyber security methodologies and protocols.
- Experience with tools for conducting port scans, network scans, fingerprinting and vulnerability scans.
- Experience with tools for conducting enumeration of target environment and configuration.
- Strong understanding of cloud computing technologies.

---

## Non-Technical Skills

- Proven track record of maintaining regulatory compliance and a high degree of understanding around regulatory requirements, such as GDPR, HIPPA, and PCI.
- Proven track record of successfully working with auditors, both internal and external.
- Proven track record of driving decisions collaboratively, resolving conflicts & ensuring follow through.
- Presentation skills with a high degree of comfort with both large and small audiences.
- Problem solving mentality leveraging internal and/or external resources.
- Awareness of current laws and governing agencies that may affect regulatory compliance.
- Exceptional verbal and written communication.

---

## Technologies

- Access, Excel, SharePoint, Word
- **Programming/Scripting Languages:** None
- **Platforms:** Westlaw

---

## Certifications

- Certified Information Systems Security Officer (CISSO)
- Certified Cloud Security Officer (CCSO)
- Certified Chief Information Security Officer (CISO)
- Certified Security Leadership Officer (CSLO)
Project Experience Types/Qualities

• 5+ years of experience with understanding regulations and laws governing compliance and maintaining an up-to-date awareness of security issues.
• 5-10 years of experience working with local, state and federal investigations and auditors.
• 7+ years of implementing policies, standards and guidelines around security, risk management, and providing security recommendations.
• Experience with the prosecution of bad actors a plus.

Identity Solution Engineer

Identity Solution Engineers (ISE) are responsible for securing your organizational identities. This includes the integration with internal and external applications. They should be familiar with identity management platforms such as Active Directory, Active Directory Federated Services (ADFS), and Azure Active Directory. They are responsible for configuring trusts and federation and understanding the various standard authentication protocols like OpenID and OAuth. They are also responsible with what and how profile information is exposed to applications.

• Top Qualities: Problem Solving (65%), Integrity (35%), Highly Organized (33%)
• Previous Roles: IT Administrator (54%), Support Engineer (40%), Network Engineer (33%), Developer (15%)
• Certifications: Certified Identity Management Professional (CIMP), Certified Identity Security Technologist (CIST)

Technical Skills

• Solid understanding of modern authentication protocols and a background in cyber security.
• Deep understanding of cloud computing technologies, business drivers, and emerging computing trends.
• Experience with Windows Server Active Directory and other LDAP-based directory services.
• Experience with Azure AD and Azure Infrastructure as a Service (Virtual Machines, Virtual Networks).
• Integration and migration experience with Skype for Business, Exchange, SharePoint, and Office 365.
• Experience with Windows, Linux, iOS, Android, Blackberry.
• Experienced troubleshooter, analyzing log files, network traffic, permissions issues, identifying problems with performance and scale.
• Developer experience with .NET, Java, HTML, CSS, JavaScript.

Non-Technical Skills

• Proven track record of driving decisions collaboratively, resolving conflicts, and ensuring follow through.
• Presentation skills with a high degree of comfort with both large and small audiences.
• Problem-solving mentality leveraging internal and/or external resources.
• Exceptional verbal and written communication.
• Basic understanding and knowledge of PCI and SOX regulatory standards.

Technologies

• Access, Active Directory, ADFS, Auth0, AWS, Azure, Citrix, Excel, firewalls, MySQL, Node.js, Office 365, Okta, Oracle, Oracle Identity Management, Ping Identity, PostgreSQL, Power BI, Radius, SharePoint, Skype, SQL Server, SSAS, SSIS, SSRS, Apache Tomcat, VMware
• Programming/Scripting Languages: C#, C++, Java, JavaScript, Perl, PHP, PowerShell, Python, Ruby, SQL
• Platforms: Linux, Windows
Certifications
- Exam priorities: Microsoft Azure Administrator AZ-103, Microsoft Azure Administrator AZ-104, Microsoft Azure Architect Technologies AZ-300, AZ-303; Microsoft Azure Architect Design AZ-301, AZ-304; Identity with Window Server 2016; Implementing Infrastructure Solutions 70-533 (retired); Microsoft Azure Infrastructure and Deployment AZ-100 (retired) and Microsoft Azure Integration and Security AZ-101 (retired) or Microsoft Azure Administrator Certification Transition AZ-102 (retired).

Project Experience Types/Qualities
- 3–5+ years senior (tier 3) level support with identity management as part of responsibilities.
- 5–8 years of experience with identity architecture and management.
- 3–5 years deploying, migrating, or managing an Office 365 environment.

Security Analyst
An Information Security Analyst assesses and provides security advice on your cloud infrastructure, including network, service, and application components. This role conducts risk assessments, architectural reviews, provides cyber security subject matter expertise, and assists in the building and design of secure solutions. Additional duties may include network and application penetration testing, and support for cyber security investigations as well as on-call response for cyber security incidents. A computer science or related engineering degree is required, or the equivalent combination of education, professional training, or work experience.

- Top Qualities: Problem Solving (69%), Integrity (49%), Verbal Communication Skills (34%), Highly Organized (34%)
- Previous Roles: IT Administrator (66%), Solution Architect (37%), Developer (19%))
- Certifications: Certified Cloud Security Professional (CCSP) (22%), Certified Ethical Hacker (CEH) (19%), Cisco Certified Network Professional (CCNP) (17%). Certified Information Systems Security Professional (CISSP) (17%)

Technical Skills
- Solid understanding of modern authentication protocols and a background in cyber security.
- Deep understanding of cloud computing technologies.
- Experience with Windows, Linux, iOS, Android.
- Experience in network security: TCP/IP, DNS, proxies, firewall configuration, intrusion detection and prevention systems, IPSec and TLS/SSL.
- Experience with cryptography: symmetric and asymmetric cryptography, hashing.
- Experience with tools for conducting port scans, network scans, fingerprinting and vulnerability scans.
- Experience with tools for conducting enumeration of target environment and configuration.
- Experience with tools used for system hacking (e.g., password cracking), malware creation/deployment, network traffic sniffers, session hijacking, denial of service and SQL injection.

Non-Technical Skills
- Proven track record of conducting vulnerability assessments and delivering clear, actionable reports.
- Problem-solving mentality leveraging internal and/or external resources.
- Exceptional written communication and strong verbal communication skills.
- Awareness of current laws that may affect penetration testing and analysis, and in conducting test that stay within the law.
- Experience with non-technical attacks and social engineering.

Technologies
- Access, Active Directory, ASP.NET, AWS, Azure, Burp Suite, Chef, Excel, firewalls, HP Fortify, Db2, Jira, Metasploit, Microsoft IIS, MySQL, Nessus, Nmap, Node.js, Oracle, PaaS, Microsoft Project, Puppet, Radius, ServiceNow, Sharepoint, sniffers, Oracle Solaris, SQL Server, Sybase, Visio, VMware, WSDL
- Programming/Scripting Languages: C#, C++, Java, JavaScript, Perl, PowerShell, Python, Ruby
- Platforms: Linux, Windows
**Certifications**

- Relevant security certifications, such as Microsoft Certified: Azure Security Engineer Associate (AZ-500), CISSP, Certified Ethical Hacker, AWS Certified Security, Certified Penetration Testing Consultant (CPTC), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Certified Penetration Testing Engineer (CPTE), Licensed Penetration Tester (LPT), GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Cisco CyberSecurity Specialist, Offensive Security Certified Expert (OSCE)

**Project Experience Types/Qualities**

- 5+ years of experience implementing and validating security postures, performing vulnerability assessments and remediations, implementing intrusion detection and prevention system, and performing cloud-based security audits.
- 5-10 years of working with security testing frameworks such as OWASP.
- 8-10 years of experience with identity audit log review strategies, and SIEM tool implementation and configuration.
- 3+ years of experience in legal investigations working with state and federal authorities.
- 5+ years of successful prevention of phishing and social engineering campaigns.

**Security Architect**

A Security Architect is the first line of defense in the prevention of hackers, malware, viruses and other malicious activities. They are responsible for setting up policies, procedures and guidelines for system access and ensuring that your SIEM systems are monitoring all business-critical applications. Security Architects must be familiar with all levels of the application and network communications. It is their job to implement encryption at rest, encryption in transit and ensure proper access and data loss prevention controls are in place. They interact with your Compliance Officer and Legal team to provide technical guidance on security incidents.

- **Top Qualities:** Problem Solving (70%), Integrity (43%), Confidence (32%)
- **Previous Roles:** IT Administrator (57%), Security Analyst (45%), Developer (11%)
- **Certifications:** Certified Information Systems Security Professional (CISSP) (32%), Certified Information Security Manager (CISM) (28%), Certified Cloud Security Professional (CCSP) (19%)

**Hard Skills: Technical**

- Solid understanding of modern authentication protocols and a background in cyber security.
- Deep understanding of cloud computing technologies and network architectures.
- Experience with Windows, Linux, iOS, Android.
- Deep experience in network security: TCP/IP, DNS, proxies, firewall configuration, intrusion detection and prevention systems, IPsec and TLS/SSL.
- Solid understanding of cryptography: symmetric and asymmetric cryptography, hashing.
- Strong experience with tools for conducting port scans, network scans, fingerprinting and vulnerability scans.
- Deep experience with tools used for system hacking (e.g., password cracking), malware creation/deployment, network traffic sniffers, session hijacking, denial of service and SQL injection.

**Hard Skills: Non-Technical**

- Proven track record of conducting vulnerability assessments and delivering clear, actionable reports.
- Problem-solving mentality leveraging internal and/or external resources.
- Exceptional written communication and strong verbal communication skills.
- Awareness of current laws that may affect penetration testing and analysis, and in conducting test that stay within the law.
- Experience with non-technical attacks and social engineering.

**Technologies**

Active Directory, Azure, Chef, Excel, firewalls, Jira, Metasploit, Nessus, Oracle, Oracle Solaris, VMware

**Programming/Scripting Languages:** C, C#, C++, Java, JavaScript, Perl, PHP, PowerShell, Python, Ruby

**Platforms:** Linux, Windows

aka.ms/practiceplaybooks
**Certifications**

Relevant security certifications, such as Microsoft Certified: Azure Security Engineer Associate (AZ-500), CISSP, Certified Ethical Hacker, AWS Certified Security, Certified Penetration Testing Consultant (CPTC), GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), Certified Penetration Testing Engineer (CPTE), Licensed Penetration Tester (LPT), GIAC Penetration Tester (GPEN), GIAC Web Application Penetration Tester (GWAPT), Cisco CyberSecurity Specialist, Offensive Security Certified Expert (OSCE).

**Project Experience**

**Types/Qualities**

- 7+ years of experience implementing and validating security postures, performing vulnerability assessments and remediations, implementing intrusion detection and prevention system, and performing cloud-based security audits.
- 5-10 years of working with security testing frameworks such as OWASP.
- 8-10 years of experience with identity audit log review strategies, and SIEM tool implementation and configuration.
- 5+ years of experience in legal investigations working with state and federal authorities.
- 7+ years of successful prevention of phishing and social engineering campaigns.
- 7+ years of knowledge about network and application vulnerabilities.

**Solution Architect**

A Solution Architect (CA) drives Azure-based customer initiatives in collaboration with customers and participates in both pre and post-sales (e.g., deployment) efforts. The CA is a technical, customer facing role that is accountable for the end-to-end customer cloud deployment experience. CAs own the Azure technical customer engagement including architectural design sessions, specific implementation projects and/or proofs of concept, and deployment. The ideal candidate has experience in customer facing roles and success leading deep technical architecture and application design discussions with senior customer executives to drive cloud deployment. Five or more years of architecture, design implementation and/or support of distributed applications designed to run in the cloud or across hybrid cloud and on-premises environments. Experience in consultative sales, design and deployment of projects strongly preferred. A computer science or related engineering degree is required.

- **Top Qualities**: Problem Solving (41%), Creativity (21%), Attitude (20%)
- **Previous Roles**: Developer (42%), Support Engineer (25%), Network Engineer (22%), No previous role (22%)
- **Certifications**: MCSA Cloud Platform Solutions Associate (24%), MCSE Cloud Platform and Infrastructure (21%), MCSA Linux on Azure Solutions Associate (8%)

**Technical Skills**

- Deep understanding of cloud computing technologies, business drivers, and emerging computing trends.
- Solid understanding of cloud virtualization, storage and networking.
- Understanding of cloud governance technologies for cost management and control.
- Understanding of common database technologies such as SQL Database/Server, Oracle, MySQL.
- Deep technical experience in enterprise mobile, identity and access control, & security solutions.
- Working knowledge with AGILE development, SCRUM and Application Lifecycle Management (ALM) with one or more of the following programming languages: PowerShell, Bash, .NET, C++, Java, JSON, PHP, Perl, Python, Ruby on Rails, HTML, CSS, JavaScript, Responsive Web Design.
- Solid understanding of modern DevOps practices, including automation, continuous delivery, continuous deployment, and continuous integration methodologies.
- Deep understanding of cloud-based Business Continuity and Disaster Recovery practices.
### Non-Technical Skills
- Building customer/partner relationships.
- Proven track record of building deep technical relationships with senior executives and growing cloud consumption share in large or highly strategic accounts.
- Proven track record of driving decisions collaboratively, resolving conflicts & ensuring follow through.
- Presentation skills with a high degree of comfort with both large and small audiences.
- Prior work experience in a consulting/architecture position within a software & services company.
- Problem-solving mentality leveraging internal and/or external resources.
- Exceptional verbal and written communication.

### Technologies

**Programming/Scripting Languages:** C#, C++, Apache Hive, Perl, PHP, Pig, PowerShell, Ruby, Ruby on Rails, Scala, SQL, T-SQL

### Certifications
- Exam priorities: Implementing Infrastructure Solutions 70-533 (retired), Microsoft Azure Infrastructure and Deployment AZ-100 (retired) and Microsoft Azure Integration and Security AZ-101 (retired) or Microsoft Azure Administrator Certification Transition AZ-102 (retired); Architecting Azure Solutions 70-535 (retired), Microsoft Azure Architect Technologies AZ-300, AZ-303; Microsoft Azure Architect Design AZ-301, AZ-304.

### Project Experience
- 5-8 years of experience designing and delivering cloud solutions on an enterprise scale.
- 5+ years of experience with creating pilots, prototypes, and proof-of-concepts to provide validation of specific scenarios.
- 4-6 years of experience providing cloud solutions, including hybrid solutions on-premises or in the cloud, lift-and-shift initiatives, migrations and upgrades.
Recruiting Resources

Top 10 Sources to Find Skilled Labor and What to Look For

Sourcing skilled labor can be a challenge. In the Microsoft Hiring and Onboarding Playbook Study, referrals (63%), website (57%) and LinkedIn (56%) were reported as the top approaches for generating leads.

<table>
<thead>
<tr>
<th>TOP CANDIDATE LEAD SOURCES</th>
<th>TOTAL (n=275)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Referrals from employees or partnerships</td>
<td>63%</td>
</tr>
<tr>
<td>Posting on website</td>
<td>57%</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>56%</td>
</tr>
<tr>
<td>Social media</td>
<td>42%</td>
</tr>
<tr>
<td>Former employees</td>
<td>36%</td>
</tr>
<tr>
<td>University recruiting</td>
<td>36%</td>
</tr>
<tr>
<td>Local technical communities</td>
<td>35%</td>
</tr>
<tr>
<td>Recruit from competitors</td>
<td>23%</td>
</tr>
<tr>
<td>Meetups</td>
<td>16%</td>
</tr>
<tr>
<td>Recruitment agency</td>
<td>4%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: Microsoft Hiring and Onboarding Playbook Study, MDC Research, June 2018

Now, what are the most important factors to look for in a potential hire’s skillset? In the Microsoft Cloud Practice Development Study, we asked the Azure partners this question. What they told us was that the top three most important factors were work history, cultural fit, and years of experience.

<table>
<thead>
<tr>
<th></th>
<th>TOTAL (n=1136)</th>
<th>SMB (n=886)</th>
<th>ENTERPRISE (n=250)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Work history</td>
<td>69%</td>
<td>68%</td>
<td>74%</td>
</tr>
<tr>
<td>Cultural fit</td>
<td>43%</td>
<td>40%</td>
<td>53%</td>
</tr>
<tr>
<td>Years of experience</td>
<td>42%</td>
<td>41%</td>
<td>47%</td>
</tr>
<tr>
<td>Professional certifications</td>
<td>32%</td>
<td>34%</td>
<td>22%</td>
</tr>
<tr>
<td>Referrals</td>
<td>28%</td>
<td>29%</td>
<td>26%</td>
</tr>
<tr>
<td>Professional training received</td>
<td>20%</td>
<td>21%</td>
<td>16%</td>
</tr>
<tr>
<td>Reputation through community</td>
<td>16%</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>Formal education</td>
<td>13%</td>
<td>14%</td>
<td>11%</td>
</tr>
<tr>
<td>Contract to hire</td>
<td>13%</td>
<td>13%</td>
<td>13%</td>
</tr>
<tr>
<td>Publications</td>
<td>3%</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Awards received</td>
<td>2%</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Attitude</td>
<td>0%</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Other</td>
<td>4%</td>
<td>4%</td>
<td>4%</td>
</tr>
</tbody>
</table>


aka.ms/practiceplaybooks
Training & Readiness

Follow a learning curriculum to build the skills the organization needs most to stay relevant. Fill a skills gap or improve the team’s skill surface area with sales and technical training.

Suggested resources to help onboard employees for training success are available in this section. This includes a range of online learning resources for self-paced learning, as well as options for instructor-led training for rapid technology adoption.

In our research, we found that most partners staff are trained using on-demand and self-study, with a smaller percentage using a mix of on-demand and instructor-led training.

![Cloud Technology Technical Staff Training Strategy](chart)

Source: Microsoft Azure Migration eBook, MDC Research, January 2018

**MICROSOFT AZURE TRAINING RESOURCES**

Use the following resources as part of Azure onboarding for new and existing staff.

- **Azure Training and Certification** provides free online training options including online courses, learning paths, hands-on labs as well as resources to help find learning partners who can help partners achieve their skills development goals using Microsoft Azure services.
- **Microsoft Learn** offers free on-demand role-based learning paths designed to prepare technical roles to deliver Azure services and solutions.
General Technical Training

Whether partners need to fill a skills gap or are looking to improve their team’s skill surface area, technical training is critical to success.

In our research, we found conferences and paid online training are the most common learning mechanisms.

MPN PARTNER TRAINING CENTER

The MPN Partner Training Center provides a centralized interface with training opportunities and certification options organized by role, products, competencies, certifications, and job role.

MICROSOFT 365 SECURITY TRAINING

The Microsoft 365 Security Track offers online curated training for individual certifications and partner competencies, including and advanced partner workshop and M365 Administration Certification prep.

AZURE SECURITY COMPASS ON GITHUB

Microsoft’s Cybersecurity Solutions Group has a GitHub page on Azure Security Compass with download files including presentations, best practices, videos, and tracking worksheets.

MICROSOFT CONFERENCE RECORDINGS

For those who missed the annual live event, the Microsoft Inspire and Microsoft Ignite conferences provide many of its sessions as on-demand recordings — no conference pass required.

PARTNER COMMUNITY EVENTS, CALLS & WEBINARS

The Microsoft Partner Enablement Blog maintains a schedule of trainings available to partners. Visit often and plan a training calendar.

SMART PARTNER MARKETING

Leverage the Microsoft Smart Partner Marketing site as a starting point for training marketing resources.

Source: Microsoft Cloud Practice Development Study, MDC Research, November 2016

aka.ms/practiceplaybooks
Additional Resources

Microsoft Learning Partners are available worldwide to deliver training for Microsoft Azure via live instructor-led courses. This can be scheduled as a dedicated delivery at a specific location or virtually using remote learning technologies. Many courses are scheduled as open-enrollment courses, which doesn’t require scheduling a dedicated class.

- **Pluralsight** is a key Microsoft partner that offers Azure training. Gain the know-how through these free online courses, delivered in partnership with Pluralsight.
- **Opsgility** is a key Microsoft partner that offers Azure training. Find more than 70 online classes focused on Azure with full learning paths for Azure certification. Opsgility also offers a full set of instructor-led Azure trainings that focus on architects, developers, DevOps, operations, sales and decision makers.
- **O’Reilly Safari** provides subscription access to more than 40,000 books, videos, and interactive tutorials from over 200 of the world’s best publishers, including O’Reilly, Pearson, Harvard Business Review, and Packt. It also offers live online training courses led by instructors from O’Reilly’s network of tech innovators and expert practitioners.
#1 challenge for the cloud adoption is access to talent. Building a learning culture inside the organization is the success mantra for keeping our azure rockstars up-to-date on the ever improving azure platform.

ANIL SINGH
CEO, Hanu Software
Increase Readiness and Marketability with Learning Paths and Assessments, Competencies & Certifications

There are numerous assessments and certifications employees should consider as motivation for advancing their skills, creating proof points for the organization’s practice and achieving Microsoft Partner Network competencies.

PARTNER TRAINING CENTER

The MPN Partner Training Center that provides a simplified experience that offers new role-based learning paths with curated training recommendations based on technical role, skill level, and solutions being developed.
Competencies and Certifications
Build and verify technical expertise

Competencies

A Microsoft Partner Network competency demonstrates to customers a company’s expertise in a specific product or solution. Among the first steps to achieving a competency is to meet technical skills requirements. One of the next steps is for partners to ensure they align the technical team to the MPN competency for their practice.

The competencies most applicable to the security practice are:

- Security
- Cloud Productivity
- Small and Midmarket Cloud Solutions
- Enterprise Mobility Management
- Cloud Platform Competency

Each competency has a Gold or Silver level that define specific requirements and provide differentiated benefits. Partners can always find the latest competency requirements and benefits available on the Microsoft Partner Network competencies portal.

Certifications

Certification is a way to demonstrate to customers that partner organization has the skills to create solutions that enable the design and implementation of secure solutions. Security certifications are industry-aligned to meet specific job roles and market needs. They don’t just assess what individual know, but also their ability to apply what they know to solve real business challenges.

- Browse role-based Security Engineer certifications
- Browse role-based Azure Developer certifications
- Browse role-based Azure Administrator certifications
- Browse role-based Azure Architect certifications
- Browse role-based Azure Data Engineer certifications
Operationalize

Security

aka.ms/practiceplaybooks
Executive Summary

In the previous section, we reviewed how partners should hire, train, and equip their staff. In this section, we will review the steps to operationalize their practice.

We walk through the options for leveraging internal use benefits that provide complimentary software licenses and subscriptions for use within an organization, as well as how to deepen relationships with customer by re-selling Security products as an overall package along with custom software, creating a new revenue stream for a security practice.

This section also provides guidance on how to operate a business, from the infrastructure considerations of sales and marketing operations to the key contracts partners will want to put in place.

Whether they’re building products, providing managed services, or performing project work for customers, their success may be impacted by their ability to manage their customer records, their projects, and their support trouble tickets. We provide guidance on what tools and systems they should consider implementing.

Top 5 things to do

Get a practice off ground by putting a plan into action. These are the things to get the momentum going.

- Leverage internal use benefits
- Prepare key contracts
- Setup support process and systems
- Setup social offerings
- Standardize engagements using checklists
Implement a Solution Delivery Process

The process partners follow in delivering their solution to customers is just as important as the technologies they use to deliver it.

When it comes to delivering solutions for their Security practice, incorporate the processes that best fit the needs of the partner organization and its team.

**Scrum Process**

The Scrum process works great for tracking product backlog items (PBIs) and bugs on the Kanban board, or break PBIs and bugs down into tasks on a task board. This process supports the Scrum methodology as defined by the Scrum organization. Tasks in this process support tracking remaining work only.

**Agile Process**

Choose Agile when using Agile planning methods, including Scrum, and tracks development and test activities separately. This process works great for tracking user stories and bugs on the Kanban board, or track bugs and tasks on the task board. Learn more about Agile methodologies at the Agile Alliance. Tasks support tracking Original Estimate, Remaining Work, and Completed Work.

---

**CREATE REPEATABLE PROCESSES**

Repeatable processes make for profitable practices. Use the following example checklist to use when executing a new engagement.

- Hold initial requirements meeting
- Identify product owner/manager(s)
- Follow-up meeting to clarify and establish next steps
- Discuss MVP (minimal viable product) criteria
- Establish development process (Agile, Scrum, etc.)
- Identify milestones and tasks; share with customer
- Provide cost estimates for development, cloud services, and ongoing maintenance/support
- Address customer objections to proposed technology and services
- Acquire data (or sample of data) for initial data assessment and proof of concept development.
- Host project artifacts (issues, code, etc.) to share with internal team and customer (e.g. Visual Studio Team Services)
- Follow up with customer and provide status/demos on a regular basis (e.g. 2 week sprint)
- Coordinate a final handoff to customer
- Conduct project debrief with customer
- Organize internal project post-mortem
- Customer conducts acceptance test
Claim Internal Use Benefits

AZURE CREDITS
Providing access to Azure for technology professionals is one of the key first steps to preparing for a successful Security practice. Microsoft provides several ways for an organization to gain access to Microsoft Azure for development of new services, testing workloads, delivering services, or learning in general. Members of the Microsoft Action Pack program receive $100 monthly Azure credits.

Microsoft Partners with the Cloud Productivity Competency get Azure credits as a part of the Visual Studio subscription’s core benefit (see the next section on Visual Studio).

Microsoft Partners with a Cloud Platform Competency at the Silver or Gold level get even more — $6,000 per year and $12,000 per year respectively.

OFFICE 365 BENEFITS
Microsoft Partner Network core benefits include access to the Microsoft Office 365 Demo tenant that can be used to sell Microsoft Office 365, Power BI Pro, Microsoft Dynamics CRM Online and Project Online. Partners also get 25 seats of Office 365 E3 at the silver competency level or 100 seats of Office 365 E3 at the gold level.

As a Microsoft Partner with the Small & Midmarket Cloud Solutions competency, in addition to core benefits, partners get 10 seats of Office 365 E3 at the silver level and 25 seats of Office 365 at the gold level.

As a Microsoft Partner with the Cloud Productivity or Communications Competency, partners get 25 seats to Office 365 E5 and 100 seats with the Gold competency.

aka.ms/practiceplaybooks

VISUAL STUDIO
Each Visual Studio subscription has a set amount of Azure credits built in that the subscriber can use. The credit amount varies depending on the type of subscription purchased. The rate partners will pay does not include any licensing costs — even virtual machines with SQL Server, SharePoint Server, or other software that is normally billed at a higher rate.

Providing technical resources access to Azure is just as important as providing them a computer.

<table>
<thead>
<tr>
<th>$50 AZURE CREDIT</th>
<th>$100 AZURE CREDIT</th>
<th>$150 AZURE CREDIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Visual Studio Professional – annual</td>
<td>• MSDN Platforms</td>
<td>• Visual Studio Enterprise – annual</td>
</tr>
<tr>
<td>• Visual Studio Professional with MSDN</td>
<td></td>
<td>• Visual Studio Enterprise with MSDN</td>
</tr>
<tr>
<td>• Visual Studio Test Professional with MSDN</td>
<td></td>
<td>• Visual Studio Enterprise with MSDN (BizSpark)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Visual Studio</td>
</tr>
</tbody>
</table>

aka.ms/practiceplaybooks
Ways to Purchase Azure

There are several options

**ENTERPRISE AGREEMENTS**

An option for getting access to technical professionals is to purchase an Enterprise Agreement (EA). This arrangement is ideal for larger organizations that require the ability to create subscriptions for different departments, and even implement charge-back based on the department. Azure subscriptions within an EA agreement are managed through the Azure EA portal and allow for delegated administration and the ability to set quotas at the department or subscription level. For more information on how to get started with purchasing an enterprise agreement for Azure usage or adding Azure to an existing EA, visit: https://azure.microsoft.com/pricing/enterprise-agreement/.

**PAY AS YOU GO AND TRIAL ACCOUNTS**

Create a free trial with Azure and allow it to convert to a pay-as-you-go subscription. An Azure free trial is valid for 30 days and allows up to $200 in Azure credits. After the initial 30 days, any Azure usage is billed directly to a credit card. Start a free trial by browsing http://azure.microsoft.com and clicking the free trial link.

**OPEN LICENSE**

Purchase Azure through a reseller using the Microsoft Open License Program. Open Value is the recommended program for small to midsize organizations with five or more desktop PCs who want to simplify license management, manage software costs, and get better control over their investment. It also includes Software Assurance, providing access to valuable benefits such as training, deployment planning, software upgrades, and product support to help boost the productivity of an entire organization. For more information on the Microsoft Open Licensing program, visit: https://www.microsoft.com/licensing/licensing-programs/open-license.aspx.

**CSP SANDBOX**

Make sure to take advantage of the CSP sandbox capability. Every Microsoft Partner onboarded in CSP has access to $200 worth of test accounts for every subscription they provision.
Key Contracts and Tools for a Practice

Practices need to use a set of legal documents to ensure compliance and deliverables, and an implementation process, to track the progress of a project both in terms of progress against a project plan and project budget, as well as protect IP.

**KEY CONTRACTS**

Leverage the [Key Contracts for Your Practice guide](https://aka.ms/practiceplaybooks), to learn more about developing service level agreements, master services agreements, a statement of work, and a mutual non-disclosure agreement.

**MICROSOFT PROJECT ONLINE**

[Microsoft Project Online](https://aka.ms/practiceplaybooks) is a flexible online solution for project portfolio management (PPM) and everyday work. Delivered through Office 365, Project Online provides powerful project management capabilities for planning, prioritizing, and managing projects and project portfolio investments — from almost anywhere on almost any device. Project Online can be used by administrators, portfolio managers and viewers, project and resource managers, and team leads and members.

**AZURE DEVOPS**

[Azure DevOps](https://aka.ms/practiceplaybooks) provides various tools for tasks like running agile teams, providing support for Kanban boards, handling work item backlogs, scrum boards, source control, continuous integration and release management. Source control functionality provides Git support, which enables integration with GitHub if such integration is desired.

While Azure DevOps will help manage the technical aspects of a project, cost-containment requires a different set of tools.

**MICROSOFT DYNAMICS 365 FOR PROJECT SERVICE AUTOMATION**

[Microsoft Dynamics 365 for Project Service Automation](https://aka.ms/practiceplaybooks) provides users with the capabilities required for setting up a project organization, engaging with customers, project scheduling and costing, managing and approving time and expenses, and closing projects. It is specially targeted to address the needs of a Project Services based practices, as it is designed for professionals who manage projects and the associated customer engagement process end to end.

**GITHUB**

[GitHub](https://aka.ms/practiceplaybooks) provides the hosted environment for the AI implementation team to version control and share their source code, notebooks and other artifacts both privately (e.g., internally to a team) and publicly (e.g., an open source project) and collaborate on development projects.
Collaboration Tools and File Sharing

Collaborating with customers through the lifecycle of a project or the duration of a managed services agreement is critical. There are several services that can help to share project plans or set up lists for shared data.

**JUPYTER NOTEBOOKS**

[Jupyter Notebooks](https://jupyter.org) is an open source web app that enables teams to share live code and collaborate on data wrangling, data understanding, data preparation, model training and model evaluation and reporting. They also provide convenient mechanism to share results (in the form of notebooks that include rich text, tabular data and charts) with customers and other stakeholders in a read-only fashion.

**MICROSOFT TEAMS**

[Microsoft Teams](https://www.microsoft.com/en-us/microsoft-teams) is the latest collaboration tool from Microsoft and is designed to make content, tools, people, and conversations available in a single location.

**YAMMER**

[Yammer](https://yammer.microsoft.com) is an enterprise social network collaboration offering to help teams collaborate and share files with each other.

**ONEDRIVE FOR BUSINESS**

[OneDrive for Business](https://www.microsoft.com/en-us/oneway) is an enterprise file sharing service that is designed for automatic synchronization of files between a computer and the cloud. OneDrive makes it easy to share files with a customers.

**SURFACE HUB**

[Microsoft Surface Hub](https://www.microsoft.com/en-us/surface/hub) is a Teams integrated collaborations device, or “meeting room in a box.” In addition to the built-in team experiences like Teams, Microsoft Office, and Whiteboard, Microsoft Surface Hub is customizable with a wide array of applications. Universal apps built for Windows 10 shine on Microsoft Surface Hub and scale to the large screen. Connect apps from a personal device and drive them from Microsoft Surface Hub.
Use CRM to grow a business

CRM solutions streamline processes and increase profitability in sales, marketing, and service divisions.

A strong CRM solution is a multifaceted platform where everything crucial to developing, improving, and retaining customer relationships is stored. Without the support of an integrated CRM solution, partners can miss growth opportunities and lose revenue because they’re not maximizing business relationships. Imagine misplacing customer contact information, only to learn that the delay pushed a client into the arms of a competitor. Or, picture the top two salespeople in an organization pursuing the same prospect, resulting in an annoyed potential customer and some unfriendly, in-house competition. Without a centralized program where people can log and track customer interactions, a business falls behind schedule and out of touch.

THE FUNDAMENTALS OF CUSTOMER RELATIONSHIP MANAGEMENT

CRM tools make the customer-facing functions of business easier. They help:

- Centralize customer information
- Automate marketing interactions
- Provide business intelligence
- Facilitate communications
- Track sales opportunities
- Analyze data
- Enable responsive customer service

Running a successful business is no simple task. When marketing campaigns, data analysis, meetings, customer care, and more, all happen simultaneously, organizations need a powerful CRM solution to bring all these functions together in one place.

Sales professional will work with the following types of records:

ACCOUNTS: Account records contain information about the companies with whom business is conducted.

CONTACTS: Contact records contain information about the known people with whom one works. Usually, multiple contacts are associated with one account. Contacts could include people responsible for making purchasing decisions or paying invoices, support technicians, or anyone that works at the company.

LEADS: Leads are potential sales, and a seller and his company can get leads from many different sources. For example, generate sales leads from marketing campaigns, inquiries from a website, mailing lists, social media posts, or in person at a trade convention.

OPPORTUNITIES: When qualify a lead, it becomes an opportunity, or a deal that is ready to close.

Microsoft Dynamics 365 can be customized so that records relevant to a specific field and the way an organization does business, including sales, customer service, field service, project service automation, and marketing.
Define Customer Support Program & Process

Support Overview

It has been said that an unhappy customer represents an opportunity to make a customer for life. Studies have found when a customer gets to the point of a complaint, they are very emotionally engaged. Turn a negative to a positive and potentially create a customer for life.

When it comes to support, there are two questions to consider. First, how can partners support customers when they have engaged them for project services, managed services, or to utilize their intellectual property, and second, where can partners go for Azure support from Microsoft for a solution they are building, or to get assistance on behalf of their customer?

THE ITEMS TO WORK THROUGH INCLUDE

- Defining a support model
- Provisioning support infrastructure
- Defining and implementing an escalation process
- Selecting and enabling support options for Azure

We cover each of these topics in the pages that follow.

RESOURCES

➔ Azure Support for Customers

aka.ms/practiceplaybooks
Supporting Customers

Let’s begin with the first scenario – direct support for customers. It should go without saying that one of the most important functions for an Security managed services practice will be supporting customers once their applications and data are firmly in the cloud or sitting in a hybrid deployment. No matter how well a cloud or hybrid environment is planned, provisioned, operated, or monitored, problems will arise — and those problems will need to be remediated. It’s the role of the managed services provider (MSP) to offer support to customers to deal with outages, breaches, inefficiencies, and disaster scenarios. MSPs need to consider the level of support that makes sense for their practice — in terms of resources and revenue — as well as what makes sense to the customers they serve.

SUPPORT MODEL

What is the best way to package and sell support? The typical options are to provide support either on a retainer basis (where the customer pays a monthly fee for up to a certain number of “use it or lose it” support hours) or per incident (where the customer pays a fee every time they utilize the support service). Managed services providers must also define their support availability so customers have a realistic expectation of when they can access the service.

ESCALATION PROCESS

How does a customer get help at the right technical level? For the support process to make economic sense, avoid having the most skilled and most expensive resources (e.g., architects, senior developers, data scientists, etc.) answer every support call. For a particular solution offering, consider implementing a tiered support offering of junior-level resources that are equipped to handle common issues. These resources should be equipped to escalate a customer support case to a more senior-level resource once the common issues have been ruled out. The provider will need to decide how many levels of tiered support to offer, but two to three tiers is most common. When defining an escalation process, do not forget about the basics. For example, how do customers contact support in the first place? This could be a dedicated support telephone number, forum or chat room, Twitter handle, email address, etc.

Support infrastructure: How will customer support requests be managed and tracked to closure? Many MSPs offer premium support offerings such as a Technical Account Manager who is responsible for tracking, reporting, and escalating an issue.
Support Options from Microsoft

How to receive support for implementation efforts or on behalf of customer

SIGNATURE CLOUD SUPPORT

Microsoft Signature Cloud Support is provided as benefit to Silver and Gold partners. It primarily provides support for issues occurring in Azure subscriptions a partner owns or on which they are a co-admin. It is not intended for use in supporting issues in subscriptions owned by their customers.

MICROSOFT ADVANCED SUPPORT FOR PARTNERS

Microsoft Advanced Support for Partners is the ideal solution for partners who are growing their cloud business. Not quite ready for Premier Support, but need a higher level of service than the Microsoft Partner Network core benefits provide? The Advanced Support program delivers the right level of support to meet partners in the middle while their business grows. With Advanced Support for Partners, partners get cloud support at an accessible price point, which helps them be a great ally to customers and grow their business faster. The program includes valuable proactive and reactive services delivered by experienced Services Account Managers and Partner Technical Consultants. Advanced Support for partners enables partners to provide support on behalf of their end customers, in addition to providing support on subscriptions they own directly. Microsoft Advanced Support for Partners addresses the specific needs of Cloud Solutions Providers (CSPs), born-in-the-cloud partners, and all other partners selling Microsoft cloud services.

MICROSOFT PREMIER SUPPORT FOR PARTNERS

Microsoft Premier Support for Partners delivers a managed support offering for partners and their customers — proactive support services for developing, deploying, and supporting Microsoft technology whether on-premises, hybrid, or in the cloud. As the only partner program with complete, end-to-end managed support across the full Microsoft platform, Premier Support for Partners also provides a powerful marketing tool to gain competitive advantage in the marketplace.

Microsoft offers a range of paid Azure support plan options for customers from developers starting their journey in the cloud to enterprises deploying business-critical, strategic applications on Microsoft Azure. These options are available in tiers — Premier, Professional Direct, Standard and Developer Support Plans — that are available for purchase directly for those who are not Microsoft Partners. In addition to these paid plans, Azure offers core support, which is free and provides support via forums, and help with account billing or management questions.

SUBMITTING AZURE SUPPORT REQUESTS

Support requests need to be submitted using the Azure Portal. First, log in to the subscription for which support is required. Next, submit a support request. Once submitted, partners can manage the incident from the Azure Portal.
Partner Advisory Hours

Partner advisory hours are used as currency for technical presales and advisory services offered by the Microsoft Partner Technical Services team.

As part of a Microsoft Partner Network membership, organizations receive partner advisory hours for attaining a Microsoft competency and subscribing to Microsoft Action Pack (MAPs).

<table>
<thead>
<tr>
<th>NETWORK MEMBER</th>
<th>MAPS</th>
<th>SILVER</th>
<th>GOLD</th>
</tr>
</thead>
</table>
| 0 hours        | Access + Advisory  
Unlimited remote technical training  
5 partner advisory hours for technical presales, development and deployment consultations | Access + Advisory  
Unlimited remote technical training  
Unlimited technical presales assistance for Cloud deals  
20 partner advisory hours for development and deployment consultations | Access + Advisory  
Unlimited remote technical training  
Unlimited technical presales assistance for Cloud deals  
50 partner advisory hours for development and deployment consultations |

SUPPORT OPTIONS

<table>
<thead>
<tr>
<th>PARTNER-FACING OPTIONS</th>
<th>RESPONSE TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Cloud Support</td>
<td>Less than 2 hours</td>
</tr>
<tr>
<td>Microsoft Advanced Support for Partners</td>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>Microsoft Premier Support for Partners</td>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>Partner advisory hours</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CUSTOMER-FACING OPTIONS</th>
<th>RESPONSE TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Premier</td>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>Professional-Direct</td>
<td>Less than 1 hour</td>
</tr>
<tr>
<td>Standard</td>
<td>Less than 2 hours</td>
</tr>
<tr>
<td>Developer</td>
<td>Less than 8 hours</td>
</tr>
<tr>
<td>Core</td>
<td>N/A</td>
</tr>
</tbody>
</table>

RESOURCES

→ Partner Technical Services

aka.ms/practiceplaybooks
Manage and Support an Azure Deployment

Support Resources

Supporting an Azure deployment involves transitioning from deployment focus to ongoing health and occasional troubleshooting. Microsoft Azure offers several services to help manage and monitor workloads running in Azure, as well as documentation for troubleshooting practice services.

**AZURE SECURITY CENTER**

Security Center helps prevent, detect, and respond to threats with increased visibility into and control over the security of Azure resources. It provides integrated security monitoring and policy management across Azure subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions. Azure Security Center should be part of any managed service practice to assist with monitoring and support.
Security Center delivers easy-to-use and effective threat prevention, detection, and response capabilities that are built in to Azure. Some of its key capabilities are:

- Monitor the security state of Azure resources
- Defines policies for Azure subscriptions and resource groups based on a company’s security requirements, the types of applications used, and the sensitivity of data
- Uses policy-driven security recommendations to guide service owners through implementing needed controls
- Rapidly deploy security services and appliances from Microsoft and partners
- Automatically collect and analyze security data from Azure resources, the network, and partner solutions like antimalware programs and firewalls
- Leverages global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds
- Apply advanced analytics, including machine learning and behavioral analysis
- Provides prioritized security incidents/alerts
- Offers insights into the source of the attack and impacted resources
- Suggests ways to stop the current attack and help prevent future attacks

Azure Security Center enables partners to offer cloud security posture management (CSPM) and cloud workload protection platform (CWPP) as services. For instance, Microsoft partner BUI is a dedicated cyber security facility that leverages Azure Sentinel to offer threat detection, investigation and response in its [BUI Cyber SoC service](https://aka.ms/BUICyberSoC). BUI offers the service in three packages (Bronze/Gold/Silver) and bills monthly on a consumption model and uses our Tier One Microsoft CSP.

To help customers understand the benefits of adopting ASC, consider performing a proof-of-concept to validate specific scenarios. This [how-to article](https://aka.ms/AzureASCPlaybookHowTo) walks through the steps of performing an Security Center proof-of-concept.

### AZURE ADVISOR

Azure Advisor analyzes an organization’s resource configuration and usage telemetry to detect risks and potential issues. It then draws on Azure best practices to recommend solutions that will reduce cost and improve the security, performance, and reliability of applications.

### AZURE MONITOR

For those who are not offering Azure Monitor in its entirety as part of a core offering, using Log Analytics for support and monitoring can be a huge time saver. Log Analytics can help collect and analyze data generated by resources in cloud and on-premises environments. It gives real-time insights using integrated search and custom dashboards to readily analyze millions of records across all workloads and servers regardless of their physical location.

### ENGAGING MICROSOFT SUPPORT

Partners who are Cloud Solution Providers (CSPs) or have sold support as part of their managed services solution, they are the front-line support for their customer. At some point, they may need to contact Microsoft to escalate an issue. Microsoft offers several options via forum support or paid options as discussed in the “Support options from Microsoft” section of this playbook.

### RESOURCES

- [Azure Security Center Overview](https://aka.ms/AzureASCPlaybookHowTo)
- [Azure Advisor](https://aka.ms/AzureASCPlaybookHowTo)
- [Azure Forum Support Resources](https://aka.ms/AzureASCPlaybookHowTo)
- [Log Analytics](https://aka.ms/AzureASCPlaybookHowTo)
- [Partner Support Resources](https://aka.ms/AzureASCPlaybookHowTo)
Support Ticket Setup and Tracking

Customer Support

Setting up tickets, tracking issue resolution, and managing customer success are fundamentals of a practice.

Providing support to customers is a non-trivial, omni-channel effort. Consider using Azure Machine Learning to monitor the performance of production deployed models. We suggest implementing Microsoft Dynamics 365 for Customer Service to quickly set up and start managing overall customer support efforts.

MICROSOFT DYNAMICS 365 FOR CUSTOMER SERVICE

Microsoft Dynamics 365 for Customer Service is designed to manage the efforts of customer support teams. It provides licensed users with access to core customer service capabilities for a significantly lower price than comparable offerings from other vendors, including enterprise case management, Interactive Service Hub, Unified Service Desk, SLAs and Entitlements, and other service group management functionality.

CREATE CONSISTENCY AND LOYALTY

Provide the seamless service customers expect by meeting them where they are with the information they need, every time.

- Give customers great service on their channel of choice.
- Make help easy by providing relevant, personalized service.
- Proactively address issues by detecting customers' intent and social sentiment.

MAKE THE AGENTS' JOBS EASIER

Give agents complete information — in a single customer service software app — to make smart decisions and provide great service.

- Reveal customers' case histories, preferences, and feedback.
- Provide guidance on entitlements and service-level agreements.
- Display it all in a single interface tailored to their job and skillset.

GET AN ADAPTIVE ENGINE

Respond quickly to customer and market changes within an agile, cloud-based environment that has digital intelligence built in.

- Adapt and customize easily using configuration, not code.
- Extend functionality through a single interface.
- Rely on advanced analytics and a trusted cloud platform.

aka.ms/practiceplaybooks
Integrate Into a Marketplace

Resources

- How to Publish an Offer in the Azure Marketplace
- AppSource Review Guidelines
- Get Listed on PowerBI.com

Increase visibility

Once partners identify and select the marketplace to target for promoting or selling their services, they can follow these steps.

Each marketplace is different in its approach to performing the integration, but an organization will likely need to go through the following:

CREATE THE COMMERCIALS

This involves partners providing information about their company and the descriptions about the product or service they will list. In some cases, partners may need to wait to be approved and onboarded before they can proceed.

PACKAGE AND INTEGRATE

In this technical step, partners will work with the marketplace APIs to integrate their offering. At this stage, partners typically are able to test the marketplace offering and make sure everything works as expected and looks correct.

SUBMIT FOR APPROVAL

Once integration is complete, partners will need to submit their integrated package for review before it is made publicly available. Partners may need to iterate on this step to make sure the package is compliant with the marketplace requirements.

SHARE

A marketplace can help increase a partner’s visibility. But without additional effort to call attention to the company’s listing, a customer’s ability to find the partner in the most popular marketplaces may be like finding the proverbial needle in a haystack. Make sure to publicize this offer, list it on the company’s website, and ensure that existing customers are aware so they can help point others to it.
Implement Intellectual Property Offerings
Implementing IP in a Security Offerings

Consider these tips to start productizing IP and go to market.

**DEFINE THE SOLUTION**
When we ask partners how they determined what IP they were going to build, we often get the same answer, which is that they realized most of their customers were asking for the same thing or something very similar. And rather than continuing to do high-cost custom work for every customer, they decided to productize what their customers were asking for. They bring together sales, marketing, technical, and delivery teams to brainstorm and define what their solution will look like.

**DETERMINE WHAT WILL DIFFERENTIATE THE SOLUTION FROM OTHERS IN THE MARKET**
It is important that partners think about their differentiation strategy. What is going to make their solution better than similar solutions in the industry?

**MAINTAIN RIGHTS TO THE IP**
As partners make the transition from project or custom services to packaged IP, it is critical they revise their customer agreements so the partner can maintain the IP rights to the solutions.

**ESTABLISH A RECURRING REVENUE MODEL**
The beauty of deploying IP in the cloud is that partners can light up the recurring revenue model, which will have a positive impact on the valuation of their business and even help cash flows in the future.

**CONSIDER A CHANNEL STRATEGY**
One of the advantages of productizing IP is that it opens up a lot of doors to sell the solution through channel partners.
Setup Social Offerings

Blogging, Meetups, and More!

Contributing to the technical community can help increase credibility for a practice. It has the side benefit of strengthening the technical acumen of a delivery team by having them focus on a specific subject for a public-facing deliverable. Below are some suggested options to get started.

**BLOGGING**

Technical blogging is a great way to increase the skills of a technical team, as well as increase the stature of an organization in the community at large. Blog posts should be well thought out and simple to digest. Visual aids such as diagrams or nicely formatted source code snippets go a long way towards readability.

**MEETUPS AND USER GROUPS**

Speaking at user groups is another valuable tool to increase the skills of team members. Similar to blog posts, it’s great practice for honing vital communication skills, as well as a great opportunity to dig deeper into a specific subject related to the practice.

**GLOBAL AZURE BOOTCAMP**

Each user group will organize their own one-day deep dive class on Azure the way they see fit. The result is that thousands of people get to learn about Azure and join online under the social hashtag #GlobalAzure! This is a great opportunity to attend, participate as a speaker (reach out to the local organizer to see how to help) or host an event. For more information, visit [http://global.azurebootcamp.net/](http://global.azurebootcamp.net/).

**WEBINARS**

Webinars are another resource to extend teams skills. Similar in scope to speaking at a meetup or user group, the webinar allows a much broader reach as attendees from all over the globe can attend.

**MICROSOFT MVP COMMUNITY**

For more than two decades, the Microsoft MVP Award is our way of showing appreciation to outstanding community leaders. The contributions MVPs make to the community, ranging from speaking engagements and social media posts to writing books and helping others in online communities, have incredible impact. Among other benefits, MVPs get early access to Microsoft products and direct communication channels with product teams, and are invited to the Global MVP Summit, an exclusive annual event hosted in Microsoft’s global HQ in Redmond. They also have a very close relationship with the local Microsoft teams in their area, who are there to support and empower MVPs to address needs and opportunities in the local ecosystem.

Contributing to the Azure community not only helps the reputation of a practice, but it can also hone much-needed skills for a delivery team.
Create Engagement Checklists & Templates

Standardize Customer Engagement

Repeatability processes make for profitable practices. Use the following example to kickstart a checklist for executing a new engagement.

- Conduct initial requirements meeting.
- Identify product owner/manager(s).
- Conduct follow-up meeting to clarify and establish next steps.
- Discuss minimal viable product (MVP) criteria.
- Establish development process (Agile, Scrum, etc.).
- Identify milestones and tasks; share with customer.
- Provide cost estimates for development, cloud services, and ongoing maintenance/support.
- Address customer objections to proposed technology and services.
- Acquire data (or sample of data) for initial data assessment and proof of concept development.
- Host project artifacts (issues, code, etc.) to share with internal team and customer (e.g., Visual Studio Team Services).
- Follow up with customer and provide status/demos on a regular basis (e.g., two-week sprint).
- Conduct a final handoff to customer.
- Conduct project debrief with customer.
- Conduct internal project post-mortem.
- Customer conducts acceptance tests.
Executive Summary

In previous sections, we covered topics from how to build a practice by selecting products or services to specialize in, to building and training a team to help turn great ideas into reality, to bringing a special offering to market and finding and keeping great customers. So, what’s left to do? In this section, we’ll discover strategies to compel potential customers that may be sitting on the fence to take action, from creating a good value proposition to building marketing and sales materials.

It has been said that current customers are the best customers. What makes customers the best? What do they have in common? And how can partners find more like them? We’ll start by building foundational marketing materials such as marketing personas, points of differentiation, value propositions, and customer business needs.

Next, we’ll look at how to put these materials to work. We’ll go through the different ways partners can attract new customers and look at best practices. We’ll discuss why integrated marketing campaigns work the best, and the tools needed to run them, such as a CRM system and marketing automation.

But marketing is only half of the story. The sales team is the other half. Don’t forget how the two work together and what marketing can do to support sales. The job of the marketing team is to build out not only customer facing materials, but also compelling materials that can be used to train and arm the sales team.

The sales end of the bargain is to close the sale. One way to do this is by writing a winning proposal. Another way is to build a proof of concept or prototype of a product or service offering, which could help a prospect understand the offer, or solidify their vision of what is possible.

Microsoft is committed to helping partners business grow, and provides both co-selling and co-marketing opportunities.

Finally, don’t miss the Microsoft resources available to help build marketing materials and campaigns, as well as resources to help close the deal.

Top 5 things to do

Add value to the practice and turn prospective customers into lasting ones. These are the activities partners should do to go to market and get deals done.

- Identify customer’s business needs
- Write a compelling value proposition
- Leverage marketing to find customers
- Build marketing and sales materials
- Collaborate with partners
Marketing to the Security Buyer

Plan the customer’s journey to buying

The cloud changes the partner business model. Buyers buy differently than in the past. With all the information on the internet, buyers tend to research and self-educate long before they engage with sales people. By the time they do engage with sales, they’ve already made some decisions.

And, while cloud buyers are often eager to move to a SaaS model, with predictable monthly pricing, there are still concerns about the security of the cloud, and therefore, a partner’s cloud services. Businesses are seeking out more advanced security solutions including threat management, vulnerability management, firewalls, and anti-malware.

CONSIDER THE FOLLOWING

- In 2016, there were 4,000 ransomware attacks daily*
- The average cost of a data breach is $3.92 million**

* 2017 FBI report “Ransomware Prevention and Response for CISOs”
** 2019 Ponemon Institute Cost of a Data Breach Report

DOs and DON’Ts for Marketing to the Security Buyer

**DO** target existing customers with envisioning sessions and PoCs before marketing to win new customers

**DO** engage the CISO early to remove security blockers

**DO** help them envision the possibilities enabled by whiteboarding the security story

**DO** describe the benefits in terms of the business needs

**DO** emphasize intelligence as differentiator, Microsoft Intelligent Security Graph draws upon insights from billions of emails analyzed, user authentications, device protection, and web pages.

**DO** provide realistic benefits based on previous experience with the solution

**DO** be prepared to answer key customer concerns and challenger questions

**DON’T** compartmentalize security, have the all-up security discussion that emphasizes Microsoft’s end-to-end security built into the platform

**DON’T** overpromise the capabilities of security

RESOURCES

➤ Go to Market Guide
➤ The Microsoft Digital Transformation Series – Part 2: Engaging Customers

aka.ms/practiceplaybooks
Buyer Engagement

Buyers buy differently than in the past. With all the information on the internet, buyers tend to research and self-educate long before they engage with sales people. By the time they do engage with sales, they’ve already made some decisions.

To help illustrate this, just think about the way a buyer might go about buying a new car. Before going to the car dealership, the buyer will likely read about various car models on the internet, read reviews, and make some decisions. When the buyer is ready to visit a dealership, they already know what they want and how much they are willing to pay for that car. This poses a challenge for sellers. How can they get prospects to engage with them earlier in the process? Through marketing.

Another way partner businesses are changing is that when selling cloud-based solutions, they can gain recurring revenue streams. Recurring revenues provide business stability and confidence for business owners and managers, allowing them to make business decisions that may not be as easy when revenues are irregular and lumpy. While these recurring revenues are smaller on a per-transaction basis than buyers’ large capital expenditures, they adjust for this. They need a higher volume of transactions.

To support that, a higher volume of high quality sales leads are needed (through modern marketing techniques) to create larger sales pipelines. Clients who are buying on a recurring basis represent great opportunities for partners to upsell and cross-sell additional products and services.

Marketing is not an option anymore. Marketing helps educate, identify, and engage with prospects earlier in the sales process. By identifying prospects who indicate interest in products and services via their behavior (website visits, clicks, downloads, etc.), marketing can deliver high-quality leads.

Inbound marketing techniques such as search engine optimization and pay-per-click advertising make it easy for prospects to find partners. Outbound marketing techniques, such as e-mail and telemarketing, enable partners to tell prospects about their company’s solutions.

Marketing is the toolset that addresses all these changes. Marketing today is digital and has the power to reach more people. Again, it’s not to say that more traditional, non-digital marketing is ineffective. But to be found by brand new prospective buyers, organizations need to employ digital marketing techniques. Modern marketing is focused on the prospects’ and clients’ views of the world.
Consultative Selling and Technical Pre-Sales

Discovering the Art of the Possible

From the very start of an engagement with a prospect, partners should be aware of the need for technical pre-sales assistance. Many times, they are dealing with business decision makers during the buying cycle. In that case, they are less likely to have a need for technical assistance. However, more than ever before, technical staff are a part of decision making with security practices as they help envision a solution to solve a customer need.

The technical pre-sales staff should be very experienced users of a company’s products and services. These employees need training or experience as a user of those products. Former support employees often make good technical pre-sales staff. The technical pre-sales staff is in place to explain technology, how it works, how it meets a business need and to answer any other questions. They should excel at the more complex issues that come from prospects, and be focused on pre-sales, working together with sales and marketing, who address the business benefits. One without the other cannot be effective. The sales staff needs to speak to business decision makers and envision the art of the possible, with security solutions this often occurs jointly with technical expertise.

Examples of technical probing questions to ask during pre-sales conversations supporting an Security practice:

- What are the challenges you are looking to solve?
- Are you looking to improve communication, learn from your data (such as predicting future events)?
- Do you have the data to help you approach these challenges? In what formats?
- Is the data generated and captured with your system or is it external and provided by 3rd parties?
- What application development and technologies are within your existing team’s comfort zone? Do you have any data scientists on the team?
- What application platforms would you like to target? Web, mobile, desktop, IoT, etc.
- Are there any compliance or regulatory requirements that pertain to the handling of data?
- How does data enter the system and how it is ultimately consumed?
- Is Office on-premises or delivered as Office 365?
- Does your company allow workers to bring their own devices?
- How are corporate and personal devices managed today? Is corporate data being loaded on to personal devices?
- How do you ensure that internal documents are protected and not sent out to your competition?
- How do you ensure that if an employee leaves that corporate data does not leave on their personal devices?
- How do you manage user experience and security for SaaS applications?
- Does your IT/Helpdesk have problems or heavy cost with password resets?

BEST PRACTICES – CONSULTATIVE SELLING:

Rather than just promoting an existing product, the salesperson focuses on the customer’s problems and addresses the issue with appropriate offerings (products and services). The problem resolution is what constitutes a “solution”.

The best reps combine solution selling with insights. To gain credibility in the eyes of the buyer, the solutions sales rep must introduce content and data that adds value to the sales call.

Ask good questions. The successful solutions seller remains sensitive to the buyer’s needs and asks important questions at the right moment.

Listen actively. Solution selling requires considerable understanding of the buyer’s needs, which will only come from listening attentively. Solution sellers should actively listen as the buyer details their organizational needs, taking notes and asking considerate questions in the process.
**Offer guidance.** Solution sellers must guide the buyer towards the solution being offered. This guidance comes as the solution seller adopts something of a teaching role, helping the buyer to overcome business challenges by utilizing their deep knowledge of industry pain points and trends.

**Sales Kits**

The [Security Sales Kit](https://aka.ms/practiceplaybooks) and the [GDPR Sales Kit](https://aka.ms/practiceplaybooks) were both created by Microsoft and are freely available to partners. They are designed to save time with go to market activities. Each contains customizable marketing assets to help partners drive leads, build offer awareness, and close Security and GDPR related deals:

- Customer leave-behinds and flyers to set the stage and increase awareness
- Digital campaign to drive demand
- Customer email template to reach out to customers and highlight the offer
- Customer presentation that can be tailored with unique solutions and CTA
- Sample Statement of Work

---

**RESOURCES**

- [Azure Pre-Sales Resources](https://aka.ms/practiceplaybooks)
- [Engagement Offerings](https://aka.ms/practiceplaybooks)

---

1. **Get prepared**
   - **Get to know GDPR** Use the GDPR Foundations Training to get educated about the GDPR.
   - **Customer Journey** Map out the steps organizations need to take to prepare for and stay compliant with the GDPR.

2. **Drive leads**
   - **Is your customer ready?** Create a diagram that highlights the impact on organizations.
   - **Customer Email** Create an email campaign to drive interest and increase awareness.
   - **Digital Campaign** Connect with current and potential customers using social media and LinkedIn.

3. **Build awareness**
   - **Day in the Life of a DPO** Explore the day-to-day challenges of privacy and data protection officers.
   - **Customer Quiz** Survey current and potential customers to assess their knowledge of GDPR.
   - **Customer Presentation** Create a presentation that educates customers on the benefits of GDPR compliance.

4. **Close deals**
   - **Offer Flyer** Create a flyer that highlights the benefits and features of your solution.
   - **Sample SOW** Use this template to create a Statement of Work for a customer.
The Office 365 Advanced Security Sales Formula

To get to the sale tipping point for Office 365 advanced security features, it is important that partners know and understand how to showcase the customer value and benefits.

Most effective advanced security sales start early and with an assessment. Sales cycles can be long, so start as early as possible. Ensure the right partner solution specialists are fully engaged as part of the end-to-end sales process. Security workloads are complex; be sure to leverage the most strategic sellers and consultants as part of a wider team.
<table>
<thead>
<tr>
<th><strong>GO TO MARKET &amp; CLOSE DEALS</strong></th>
<th><strong>RESOURCES FOR USE DURING SELLING</strong></th>
<th><strong>STEPS FOR SELLING TO CUSTOMER</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare</strong></td>
<td>Know the product, programs, tools, training and research to get ready.</td>
<td>Discuss with customers their security needs, identify how best to deliver a Security Assessment Workshop.</td>
</tr>
<tr>
<td><strong>Select + Qualify Lead</strong></td>
<td>Target the right industry verticals to maximize effort. Explore customers who have existing Exchange Online deployments or EMS customers. Have a CISO discussion to drive engagement and possible security assessment workshop.</td>
<td>Understand the customer landscape and define positioning of the advanced security workload post Security Assessment Workshop.</td>
</tr>
<tr>
<td><strong>Develop Strategy</strong></td>
<td>Learn the <a href="#">Digital Transformation vision</a> presentation and the advanced security and Secure Score demos.</td>
<td>Create Security Assessment Workshop strategy, publish security offerings, baseline offering strategy, land with customers.</td>
</tr>
<tr>
<td><strong>Present Value</strong></td>
<td>Utilize customer evidence and <a href="#">success stories</a> to showcase customers leveraging Office 365 Advanced Security.</td>
<td>Showcase the value of Office 365 advanced security through proof points and demos.</td>
</tr>
<tr>
<td><strong>Prove Value</strong></td>
<td>Show economic value and value of security assessments by leveraging Secure Score.</td>
<td>Use customer evidence to demonstrate the ROI and business impact.</td>
</tr>
<tr>
<td><strong>Drive Adoption</strong></td>
<td>Drive advanced security workloads by realizing the benefits identified in the security assessment workshop and bringing customer security environments up to the customer desired level.</td>
<td>Build security into the Customer Success Plan and help customers realize the value of security identified in the Security Assessment Workshop.</td>
</tr>
</tbody>
</table>
Every Office 365 engagement that we’re a part of has a component of security discussion or deployment and implementation with a customer... our primary focus is making sure the customer is doing well, and that approach has worked well for us. We make sure their security and compliance needs are met, while also helping them save money.

ETHAN MCCONNELL
Vice President, Olive & Goose
Microsoft Technology Centers

The Microsoft Technology Center (MTC) can help partners find the right solutions to transform their customer’s business in a mobile-first, cloud-first world.

With more than 40 locations around the globe, the MTCs bring together the right resources to help partners accelerate their customer’s digital transformation.

- **People:** The MTC staff is comprised of experts in Microsoft solutions. Their tenure in the industry ensures they will quickly guide partners to find solutions to meet their technology challenges.

- **Partners:** The MTCs have formed alliances with industry leaders who provide comprehensive resources, including hardware, software, and services to explore during engagements.

- **Place:** The MTC environment provides rich interactive and immersive experiences to learn first-hand how Microsoft and partner technologies can help take on the most difficult challenges.

Start digital transformation by experiencing the Microsoft cloud at one of the 40+ centers around the globe.

The MTC can help partners close sales with these engagement offerings:

- **Strategy Briefing:** This one-day briefing starts by examining the current IT environment and business objectives. Then it moves into the Envisioning Center, where partners can see Microsoft solutions in action through powerful demos and scenarios customized to meet their needs. The day includes mutual discovery, tailored product and technology drill-downs, and expert presentations. It culminates with the delivery of a clear and actionable picture of how Microsoft and partner technologies can help partners reach their business goals.

- **Architecture Design Session:** This custom session focuses on business objectives and aligns them with specific applications of Microsoft software to help not only meet specific goals, but also capitalize on them. Architectural guidance, consultation on preferred practices, and risk analysis to chief technology officers, architects, and senior development team members are included in the session.

- **Proof-of-Concept:** In this multi week, in-depth workshop, Microsoft architects work closely with key members of a partner’s technical staff to transfer knowledge and prove out customized solutions. This workshop may also include detailed demos and training sessions. The partner team will have a private, secure, and fully loaded development suite that’s preconfigured prior to their arrival.

- **Workshops:** Attend a custom briefing that includes a facilitated, hands-on environment where partners and their colleagues can experience the vision of Microsoft’s platform and solutions firsthand.

**RESOURCES**

⇒ [https://www.microsoft.com/mtc/offerings](https://www.microsoft.com/mtc/offerings)
Architecture Design Session (ADS)

Engage in a working design session with customers

This intensive, two-day session delivers in-depth technical information on integrating data from across the customer’s entire organization and delivering it in an analysis-ready form. Presentations, demonstrations, and whiteboard discussions are customized to address the customer’s needs. In many cases, the design session is used to identify candidate proofs of concept. Here are some potential topics that are covered during an architecture design session:

- **Server topology**: To plan and deploy the customer’s business productivity solution, it’s necessary to understand the required server topology.
- **Integration platform**: The Azure services work seamlessly together and can also be integrated with third-party and LOB applications. The ADS will endeavor to fit diverse systems together.
- **Social computing**: Companies need to leverage their employees’ ability to make business connections and create, share, and evaluate content in a natural way.
- **Secure framework**: Companies can create experiences that are both user-based and role-based. Choose from a range of options for restricting sensitive information, and deliver the most relevant experience while meeting industry standards and enterprise security requirements.
- **Virtualization and cloud computing**: Extending the customer’s enterprise by leveraging cloud resources or virtualization reduces the cost of hardware and additional resources.

**PRIMARY AUDIENCE**

- Architects
- Developers
- Test and quality assurance (QA) engineers
- Technical staff

**Phases of a successful ADS**

**BEFORE THE ARCHITECTURE DESIGN SESSION**

Before performing the architecture design session, it is important to conduct a simple session with the customer to establish the scenario. This session is oftentimes referred to as ideation or opportunity definition. The goal is to establish the five Ws (who, what, when, where, and why) of their needs, which can be used as a guide for the ADS, streamlining the brainstorming process, and informing the agenda and milestone goals a partner brings to the session.

- **Schedule a time for the design session**: This is normally 1–2 days.
- **Schedule a location**: Ensure there are whiteboards and a projector.
- **Schedule resources**: This could include experts from the team and a cross-cutting panel of technical and business stakeholders from the customer.
- **Build an agenda**: Establish milestone goals in advance so that the ADS doesn’t get consumed discussing a single topic.
- **Prepare preliminary documentation and architectural diagrams**: Even if it’s only the basic building blocks, come prepared with something that can be modified during or after the session.
- **Perform a security assessment**: Prior to the ADS, perform a security assessment (such as by using Secure Score) to baseline the customer’s current security situation and identify preliminary opportunities for improvement.

**DURING THE ARCHITECTURE DESIGN SESSION**

Begin by reviewing requirements with the customer. During the design session, whiteboard the requirements and proposed solutions, and arrive at a consensus for each major topic. During this time, be sure to capture photos of the whiteboard so as not to lose notes. There are typically the following phases during an architecture design session: discovery, envisioning, and planning.
DISCOVERY
- Customer background and business technology strategy
- Project background and its drivers/aims
- Functional and non-functional requirements
- Usage scenarios
- Technology landscape

ENVISIONING
- Key functions and capabilities
- Components of the solution
- External connections and integration points
- Security considerations
- Abilities considerations
- Map requirements and scenarios to components

PLANNING
- Establish proof points
- Exclusions, risks, and issues
- Pre-requisites
- Deliverables
- Resources
- Escalation, communication, and long-term plans

AFTER THE ARCHITECTURE DESIGN SESSION
During the ADS, a high-level architecture framework and conceptual design for a solution that addresses their organization's business goals and technical requirements will be planned. In addition to a summary of the engagement, partners will deliver information about:

- Special areas of concern to the customer's organization, such as security, compliance, and compatibility.
- Deployment scenarios that map to established deployment and practices and that cite specific examples where applicable.
- Familiarity with the Microsoft technologies proposed for the solution, in addition to any trade-offs among the differing technology options.
- The capabilities of the partner's solution to deliver business performance on premises or in the cloud.

The outcome should be polished architecture diagrams that can be reviewed and signed off on by the customer. If one or more proof of concepts are desired, provide a plan and a timeline to deliver.
Implement Proof of Concepts

Resources

Proof of Concepts

The ability to quickly provision infrastructure and managed services makes it easier to stand up a proof of concept and demonstration for key stakeholders.

The acceptance criteria for a proof of concept should be chosen early, with short but clearly defined milestones that lead the way to a successful proof of concept. Some common best practices of an Azure PoC include:

- Start small by identifying the minimum problem to be solved — and focus on it.
- Look for high-value but low-risk opportunities when getting started.
- Take advantage of the platform. Azure can replicate some of the best technology in the datacenter, but it can also do much more. Consider PaaS services that can accelerate milestones and lower the overall burden from manageability and support.
- Treat each PoC as a continuous learning and improvement process. As Azure skills improve, so will the PoC approach.
- After proving the concept, test it for performance, security, usability, and supportability.
- If additional support is needed in building out a PoC, leverage the partner Technical Presales Assistance from a Microsoft expert.

ESTABLISH EVALUATION CRITERIA

Ideally, an Azure solution offers some key benefits over deploying the same solution on-premises. Establish goals early on and measure them throughout the PoC. Some common goals customers may ask for include:

- How easy is it to scale up or down?
- Does it offer the service to users in different regions?
- How can I monitor and support the solution if it fails?
- How do I know my data is secure?

COMMON PROOF OF CONCEPTS FOR SECURITY

- Chalk talk to workshop training to orientate customer to EM+S capabilities
- Synchronize Windows Server AD with Azure AD using Azure AD Connect
- Configure devices for security, patching, and policy with Microsoft Intune
- Configure a demonstration of Azure Information Protection
- Configure self-service password reset with Azure AD
- Configure multi-factor authentication with Azure AD
- Configure single sign-on with SaaS applications
- Deploy Advanced Threat Analytics (ATA)
- Deploy Advanced Threat Protection (ATP)
Go-to-Market and Close Deals Guide

Leverage the Microsoft resources available in the Go-to-Market and Close Deals guide.

Help plan the customer’s buying journey by understanding how to market to the cloud buyer. Align marketing goals with business goals, and develop marketing for each phase of the sales journey. Understand marketing tactics, sales assets, resources, and best practices.
Optimize and Grow

Security

aka.ms/practiceplaybooks
Executive Summary

So far we’ve covered strategies for building a security practice, finding and keeping customers providing them with ongoing support.

In this section, we’ll focus on how to optimize a practice, strengthen relationship with customers, and evaluate performance to continue to delight prospects and customers.

Are customers delighted by the services and products provided? Delighted and not just satisfied? In this section, partners will learn why customer lifetime value is so important, and how to create more customers for life. We’ll share how to get to know customers better by following their journey with secret shopping and analysis. We’ll also explore the use of a “land and expand” strategy and see how getting to know customers better can lead to incremental opportunities to provide additional services.

Discover ways to keep solutions top of mind for prospects and customers through nurture marketing, and how to grow and improve lead generation practice through a well-planned referral marketing program. Learn how to make the most of the renewal process, and how to get ahead of deadlines.

In addition, we’ll offer guidance on how to grow a business by identifying the best customer personas and creating “look-alike” prospects, deepening expertise in key verticals and marketing that expertise, and collaborating with other partners to offer customers a more comprehensive level of service and support.

We will end by discussing how important it is to create advocates for a company. This includes turning a customer into a fan and collecting testimonials to create case studies that can be used in future marketing campaigns. Map a customer’s experience and ask for feedback to ensure satisfied customers become delighted customers who will become advocates.

Top 5 things to do

Learn from customers and experience to optimize a practice, and expand to new markets through strategic partnerships. These are the things to do to optimize and grow a practice.

- Gather feedback from customers
- Nurture existing customers
- Turn customers into advocates
- Generate referrals with marketing
- Nurture strategic partnerships
Understanding Customer Lifetime Value

Customer lifetime value (CLV) is the revenue from a customer over the lifetime of the relationship.

As most businesses have experienced within the tech industry, a lifelong customer is of far greater value than any one-off transaction. It's no longer enough for companies to invest their time and resources into the generation of single purchases. Especially in the cloud world, it is critical for businesses to develop relationships and solutions that engage a customer for life.

CLV allows businesses to step back and look at not just one sale, not just one customer, but the customer base as a whole. It’s about defining the economic value of each customer within that base and using that metric to make data-based decisions. If partners don’t know what a client is worth, they don’t know what they should spend to get or keep one.

Knowing the CLV helps partners make critical business decisions about sales, marketing, product development, and customer support. For example:

- **Marketing**: What should acquisition costs be?
- **Sales**: What types of customers should sales reps spend the most time on trying to acquire?
- **Product**: How can I tailor my products and services to my best customers?

- **Customer Support**: How much can I afford to spend to provide customer service to my customers?

CLV is also a good way to guide and reward a sales team. Pay them more for bringing in customers with high potential lifetime value. By measuring and monitoring cloud customer CLV, partners can:

- Gain insight into the customers’ cloud consumption and usage.
- Qualify for MPN cloud competencies that will help partners grow their business.
- Help customers reach their desired business outcomes.
- Leverage insight for cross-sell/upsell and proactively engage customers for extension opportunities.

By increasing customer adoption rates, partners can increase CLV, particularly with cloud customers. The more employees who use the service or solution, the more likely partners are to increase CLV. Here are some ways to improve adoption:

**What is needed to be successful?**

Key attributes of a successful adoption approach

<table>
<thead>
<tr>
<th>Define a vision &amp; identify business scenarios</th>
<th>Prioritize solution &amp; create an adoption plan</th>
<th>Commit resources &amp; execute an adoption plan</th>
<th>Measure, share success, &amp; iterate</th>
</tr>
</thead>
<tbody>
<tr>
<td>A deep understanding of the business goals, as well as people challenges and needs to achieve them.</td>
<td>A solution that people love and that helps them achieve business goals and get things done more effectively.</td>
<td>A strategy to drive adoption including communications, readiness, and community.</td>
<td>A benchmark, KPIs, and success stories to help demonstrate success internally, improve, &amp; expand.</td>
</tr>
</tbody>
</table>
While it’s important to define and track metrics, there are some simple things that be done to increase CLV.

Customer strategy must be built on a culture of customer success and tracking customer satisfaction. Critical success factors, when it comes to CLV, are:

- Being sensitive to customers’ emotions.
- Maintaining good communication.
- Listening to customer pain points.
- Understanding that there are multiple layers to any one concern.
- Doing business with an understanding and empathy for where the customer is coming from.

NEXT STEPS

- Identify customer lifetime value of the five best customers.
- Identify average customer lifetime value along with a Microsoft contact.
- Identify actions to increase average customer lifetime value.

Explore the CLV modeling tool available on the MPN portal to get started.
Guide: Optimize and Grow

Leverage the Microsoft resources available in the Optimize and Grow guide.

Understand details on building customer lifetime value, executing nurture marketing efforts, optimizing and growing from feedback, refining customer value proposition, growing partnerships, and measuring results.
Security Playbook Summary

Thank you for taking the time to review this playbook. We hope you have gained new insight on how to successfully grow your security practice by taking advantage of unique offerings from Microsoft, engaging with your customers, and forming strategic partnerships.

Our goal, when creating this playbook, was to organize resources and provide insight that can be used to quickly accelerate or optimize a security practice. To this end, we laid out the practice's opportunity, then provided relevant information on business strategies and technical topics to capitalize on the opportunity, within five sections that can be reviewed in order, or individually at any time.

In the first section, Define the Strategy, we offered guidance on how to define the strategy upon which the practice will be built. The key actions were: identify the unique value proposition, define and price the offer, build a business plan, leverage the Microsoft Partner Network, and plan support options.

In the second section, Hire & Train, we focused on the importance of hiring the right team, and then providing appropriate and ongoing training and certifications.

In the third section, Operationalize, we suggested putting a plan into action. Leverage internal use benefits to get Microsoft licenses and subscriptions, create key contracts, setup a support process, setup social offerings and organize an engagement process into checklists.

The fourth section, Go to Market & Close Deals, emphasized getting a practice off the ground by defining the sales process, building materials to support sales and marketing, finding new customers, and then nurturing and investing in them to build lasting relationships. We also provided resources to help in the sales process including the pitch and negotiation.

The final section, Optimize & Grow, stressed the importance of learning from customers and experience in providing solutions to them to optimize a practice and expand to new vertical markets through strategic partnerships. The top five actions provided for in this section were: Gather feedback from customers, learn from project successes and failures, create case studies and a marketing plan to expand into new vertical markets, maximize efficiency and profit to fuel growth, and establish and nurture strategic partnerships.

FEEDBACK

Share feedback on how we can improve this and other playbooks by emailing playbookfeedback@microsoft.com