Barracuda Networks case study

Barracuda Networks utilizes Microsoft Azure Graph Security API to build cloud security platform management program

Cloud deployment velocity
As companies quickly execute cloud deployments, they can inadvertently miss key security configurations and best practices.

Microsoft Azure telemetry
Barracuda Networks employed Microsoft Azure Graph Security API in creating a robust cloud security platform management program.

Full-stack security
Barracuda’s Cloud Security Guardian addresses control, management, data planes, and the challenges that are beyond traditional solutions.

Microsoft Partner Network

© 2019 Microsoft Corporation. All rights reserved. This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft and Microsoft Azure are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.
Barracuda's mission and relationship with Microsoft

Barracuda believes every business deserves access to cloud-engineered, enterprise-grade security solutions that are easy to buy, deploy, and use. The company protects email, data, networks, and applications with innovative solutions that grow and adapt with each customer's journey. More than 150,000 organizations worldwide trust Barracuda to protect them—in areas they may not even know they are at risk—so they can focus on taking their business to the next level.

Barracuda and Microsoft have a long history of collaboration. Barracuda is a globally managed Apps & Infrastructure partner, a Gold Cloud Platform partner, and more. Barracuda was named Partner of the Year in 2016.

The impetus for Cloud Security Guardian

In deploying thousands of security reference architectures, Barracuda learned that as companies adopt and consume more Azure, they encounter new security challenges. While building a solution for these challenges, Barracuda looked for ways to identify telemetry in Azure and found that Azure Graph Security API would deliver real-time bidirectional alerts and permit Barracuda to build a robust cloud security platform management program on top.

Barracuda also adopted a suite of policies using CIS Benchmarks, PCI DSS, and HIPAA that could be automatically deployed and would enable easy remediation of any violations. Barracuda also incorporated telemetry and management for its own perimeter security (Barracuda CloudGen Firewall and CloudGen WAF). In close collaboration with Microsoft, Barracuda included management for Barracuda CloudGen Firewalls as well as Azure Firewall. Barracuda demonstrated this functionality at Ignite 2018.

Cloud Security Guardian addresses the security challenges companies face that are beyond traditional solutions by combining known best practices, robust alert data from Azure Graph Security API, and the ability to remediate policy violations in an automated fashion. Cloud Security Guardian essentially removes the burden of understanding security from individuals configuring and deploying cloud services. This removes a blocker from developers, and it frees up security professionals, as they can now rely on interactive mapping, automated remediation, and robust reports to ensure their infrastructure complies with the latest security standards. Cloud Security Guardian also eases the regulatory burden of ensuring cloud infrastructures conform to regulatory guidelines, since it provides the reporting and visibility needed to demonstrate infrastructure compliance.

“The Azure Graph Security API was perfect for our needs. Ultimately, we were able to create a solution that not only leveraged Azure services but provided data back to them as well—hence the orchestration for Azure Firewall. This is a great example of how Microsoft’s ‘build with’ motion delivers groundbreaking customer solutions.”

- Nicole Napiltonia, VP of Business Development and Alliances, Barracuda Networks

© 2019 Microsoft Corporation. All rights reserved. This case study is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft and Microsoft Azure are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are property of their respective owners.