Data breaches cost the healthcare industry $355 per record, which is more than twice the average across all industries.¹ With the increased use of technology through IoT enabled devices and electronic health records, healthcare organizations have a heightened vulnerability to cyberattacks. IDC predicts that by 2018, ransomware attacks targeting the healthcare industry will double.² Organizations need enhanced visibility of their environment that allows them to take a proactive approach to cyber defense.

SAM Cybersecurity Assessment for Healthcare

A SAM Healthcare Cybersecurity Assessment takes a holistic look at your environment and helps you create a strong and cost-efficient foundation of security and privacy so you can focus on advancing innovation and care. In addition to helping ensure that you have the right processes in place to minimize cyber-risk, we'll also offer prescriptive guidance and best practices about cybersecurity in a digital world.

SAM Healthcare Cybersecurity Assessment benefits

• Save money by combatting cyberattacks and increasing efficiencies
• Minimize data loss, fraud, and employee downtime
• Securely manage software assets and promote reliable cybersecurity practices
• Build a resilient IT infrastructure that can quickly respond to threats
• Ensure that you have a secure and effective defense against attacks

In 2016, nearly 37% of spam emails had a ransomware attachment, up from 0.6% in 2015.¹

Next steps

Contact your Microsoft SAM Service Partner for more information.