QUISITIVE

Spyglass™ Cloud Security Assessment for Healthcare

Safeguard your records and ensure compliance with our comprehensive security assessment and vulnerability analysis

Healthcare continues to be a prime focal point for data breaches, consistently topping the industries list. The financial toll of these breaches is unparalleled, averaging **$10.93 million**,[1] and has surged for the 13th consecutive year. Yet, the average healthcare organization **only dedicates 4-7% of IT budget** for cybersecurity.[2]

Quisitive's **Spyglass Cloud Security Assessment for Healthcare** is a complete evaluation tailored specifically to healthcare organizations, focusing on safeguarding critical records such as patient data, electronic health records (EHRs), and sensitive healthcare information. Our assessment encompasses an in-depth analysis of your organization's cloud security posture, emphasizing key areas such as identity management, data protection, medical device security, application security, and access controls.

Quisitive's Spyglass Cloud Security Assessment has helped prevent billions of dollars lost in cybersecurity and data breach fallout.

This assessment is designed to evaluate and enhance the security of your healthcare environment, including Microsoft 365 and Azure platforms, along with endpoint devices used within your healthcare network. Our expert team provides a comprehensive analysis of your entire Microsoft cloud security infrastructure, identifying vulnerabilities and providing actionable recommendations for improvement. **It is also an effective way to prepare your organization for HIGHTRUST® certification.**

SPYGLASS CLOUD SECURITY ASSESSMENT

TYPICAL TIMEFRAME: 6 WEEKS

M365 Security Assessment

Microsoft 365 offers unparalleled opportunities for workforce enablement, but if M365 controls are not set or monitored properly, HIPAA compliance and security diligence is at risk.

Quisitive security experts inspect your M365 tools and identify security features and controls you may not realize you already own and should be using— providing you a new, meaningful view of your security landscape.

Azure Security Assessment

Azure provides healthcare organizations with the flexibility to innovate, develop, and implement solutions tailored to their specific requirements. Despite this, concerns about cloud security can hinder adoption. Our Azure Security Assessment addresses these by providing actionable insights into your organization's cloud security posture. We evaluate your Azure deployment to identify areas for improvement, ensuring a safe and secure environment for your healthcare data and operations.

Endpoint Management Workshop

The most common causes of data breaches in the healthcare industry are phishing, ransomware, and business email compromise attacks (BEC). The nature of healthcare demands that users be connected/productive from anywhere, on any device, without compromising IT security. Learn how to leverage intelligent security, risk-based controls, zero-touch provisioning, advanced analytics, device-level vulnerability analysis, and deep integration to the Microsoft products you already use.

Assessments or workshops can be done individually to meet your needs.

What you get:

- Comprehensive review of your current security and data compliance status
- Security findings briefing including immediate insight on risky activities detected within your environment
- Enablement of key Microsoft features and tools to help improve your security posture
- Security roadmap on next steps to ensure your environment is kept secure and compliant

Who is typically involved:

- CISO
- CTO
- Director
- Internal Auditor

Your involvement: 8 – 10 hours

Available As Needed

- App Security Assessment
- Data Security Assessment
- Dynamics Security Assessment
- On-Prem Security Assessment
- M365 Copilot Quickstart

1 https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/

2 https://www.getastra.com/blogM/security-audit/healthcare-data-breach-statistics/