MICROSOFT 365 SECURITY

It Takes a Village

It's hard to find an organization that isn't using Microsoft 365 in some way, shape, or form. It has become a staple of corporate enterprises and the capabilities it offers continue to expand. As new features are added, how are you accounting for security best practices?

SEVN-X offers comprehensive security reviews of Microsoft 365 that align with the Center for Internet Security (CIS) Benchmarks. Currently, this includes the following functional areas:

Accounts (Entra ID)
MFA? Conditional Access? Admin management? We review account-level and subscription-level settings to ensure security best practices are met.

Apps, Data, Email, Storage
Each of these areas have specific security controls that are not enabled by default (usually to support legacy clients and functionality).

Auditing
Investigation and "look-back" capabilities are critical to supporting security, legal, and audit requests. We ensure the proper logging and auditing is configured.

Mobile Device Management
Don't lose sleep worrying about end-user devices; Microsoft offers security controls for businesses to manage both organization and BYOD devices with Intune policies. We'll ensure they're configured with security in mind.

What do I get?

SEVN-X uses the latest published security standards from the CIS when conducting a Microsoft 365 assessment. We'll assess the environment with each control domain in mind, note areas of non-compliance or deficiency, and provide actionable remediation plans.

Sometimes the fix is a single line of PowerShell, other times, it's a policy or procedure change. We'll break it down and make it easy, so you can focus on remediation.

If you also use Azure for hosted infrastructure (IaaS, PaaS), we've got you covered there too.

Talk to us today for more information and to see if our Microsoft 365 security assessments are right for you.

info@sevnx.com

484.989.0911

ACHIEVE BETTER CYBERSECURITY