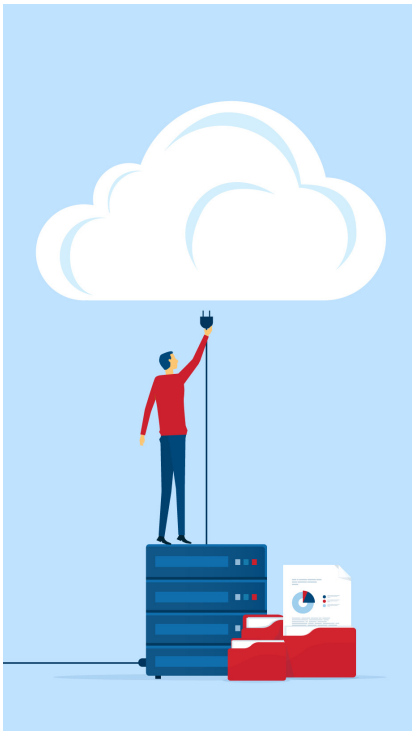
AVALONCyber

Why You May Need a Microsoft 365 Best Practices Security Assessment



Microsoft 365 (previously Office 365) offers a wealth of tools, including Teams, SharePoint, OneDrive, PowerPoint, Excel, and more, that help your team work and collaborate easily and efficiently from anywhere in the world. And, since the platform is cloud-based, your business has access to all these resources, yet doesn't have to host the infrastructure.

But, regarding security, keep in mind that Microsoft 365 is a shared security model. Microsoft does provide security features that can be enabled and configured by your IT team, such as encrypted email, data loss prevention, and advanced threat analytics (ATA). However, you are responsible for assessing your security posture to decide which of these services and controls you need to administer. How? By having a Microsoft 365 best practices security assessment conducted.

Microsoft 365 is a **shared security model...**

You are responsible for **assessing your security posture** to **decide which services and controls** you need to administer.

Here's How Avalon Cyber Assesses Your Microsoft 365 Security Controls

Our Objectives:

To assess the security settings and policies you currently have in place and identify where improvements can be made to protect your instance and sensitive and business-critical data.

Avalon Cyber meets these objectives by completing the following:

- Comparing your current settings and configurations to known best practices, such as those of the Center for Internet Security (CIS), the National Institute of Standards and Technology (NIST), and the Cybersecurity and Infrastructure Security Agency (CISA), as well as Microsoft's standard security/settings best practices
- Outlining our findings in a detailed report identifying whether the settings you have in place passes, fails, or is in a warning state based on industry best practices
- Providing strategic recommendations to address any settings and configuration shortcomings and rationales regarding why certain settings can pose a risk

AVALONCyber

Why You May Need a Microsoft 365 Best Practices Security Assessment

Don't miss out on more free content from Team Avalon!

Join the Avalon mailing list to receive useful case studies, industry insights, handy tips, and more delivered straight to your inbox.

Sign up to receive exclusive content!

Our Methodology:

For assessing areas of potential risk within Microsoft 365, we combine manual review and automation to verify all relevant settings through authenticated view-only admin access. We utilize the standards mentioned above (CIS, NIST, etc.) and test the following products, applications, and frameworks:

- Azure Directory
- Security & Compliance
- Microsoft 365
- Exchange
- Teams
- SharePoint

Microsoft 365 offers many advantages for your team, but like any other software or platform, is not without its challenges. Engaging a trained and knowledgeable cybersecurity team to perform an assessment is an easy way to help identify areas of risk within the cloud that require attention.

To learn more or to schedule a Microsoft 365 best practices security assessment, contact the experts at Avalon Cyber today.

AVALONCyber

QUESTIONS?

For more information on any of our services, please contact:

Rebecca Rudell
Marketing Manager
rebecca.rudell@teamavalon.com