How MSPs Protect Your Microsoft 365 Environment from Cyber Threats

Millions of users around the world benefit from the scalability, rich feature set and anytime/anywhere access provided by Microsoft 365. However, in any cloud environment, clear benefits come with added security risk. MSPs protect your Microsoft 365 environment by providing deep security expertise, cutting edge tools and other critical services.

While rich with possibility and promise, the cloud also brings new challenges. And guarding against cyber threats in the cloud requires a new set of skills and tools. Key cloud security threats include:

- **Misconfiguration** – Microsoft and other cloud providers offer a host of tools to manage risk and operate safely in the cloud. But security controls can prove complex, requiring significant knowledge of both the tools and the environment. Misconfiguring a single setting could expose your business to cyber attacks.
- **Lack of visibility** – With multiple clouds and hundreds or even thousands of connected devices, finding all the organization's data presents a challenge. And you cannot secure data if you do not know where it lives or who has access to it.
- **Expanded attack surface** – In addition to decreased visibility, a multi-cloud environment and numerous connected devices also mean more potential access points for hackers.
- **Overprovisioning** – Overprovisioning happens when users have more access than they need. Privileged accounts become prime targets for cyber criminals because they provide doorways

into the system and access to sensitive data. Limiting privileges to only the access users need to perform their jobs will help to contain potential damage.

- **API vulnerabilities** – Application programming interfaces (APIs) allow applications to interact with each other. For instance, the Pay with PayPal function in ecommerce uses an API. While APIs perform a vital function, they introduce additional security risks.

Highlight Security Risks

An MSP will conduct regular risk assessments and periodic penetration testing to identify weaknesses that hackers could exploit. Using these audits as a base, the organization can implement an informed security strategy and test its efficacy.

Provide 24/7 Security Monitoring

No CEO needs to receive a Monday morning call about a cyber attack that occurred over the weekend. Proactive 24/7 system monitoring, particularly when it involves machine learning, can identify and often address suspicious activity before a breach occurs. Security professionals need to be sure to collect the right data and analyze it properly.

A security-focused MSP will provide fully-managed incident detection and response that combines automated monitoring with human expert analysis. For instance, Security Information and Event Management (SIEM) systems deliver automated alerts. Trained engineers from the MSP then review and address those alerts using industry best practices.

Act as Trusted Advisors with Deep Microsoft Expertise

Microsoft 365 delivers a multi-faceted approach to security. The Microsoft Defender suite provides powerful tools for threat and vulnerability management. Microsoft Entra includes tools for identity governance, while Microsoft Intune streamlines endpoint management. On the privacy side, Microsoft Purview provides critical information governance tools.

These Microsoft services and other third-party tools allow organizations to find a critical balance between security and efficiency. But configuring the security controls properly requires significant cyber security expertise and deep Microsoft knowledge.

By partnering with the right MSP, companies gain critical access to trusted experts. For instance, the MSP can help standardize and automate security policies across multiple tenants. They can also assist your IT department with implementing MFA, zero trust, advanced email protection and other critical security tools.

Ensure Timely Patch Management

One critical element of cyber security includes keeping software, operating systems and firmware up-to-date. Vendors frequently release security patches to address known vulnerabilities. But organizations that neglect to install the patches leave their systems exposed.

With hundreds of applications and devices, including IoT devices, staying on top of security patches can prove challenging. An MSP protects your on-premises and cloud environments by implementing a comprehensive patch management strategy.

User Training

Whether on premises or in the cloud, end users represent both a potential weak link and a critical line of defense against attack. Make sure your workforce understands their roles in cloud security and that they know how to spot suspicious activity. An MSP like Messaging Architects' parent company, eMazzanti Technologies, can customize security awareness training to meet the needs of your organization.

MSPs Protect Your Microsoft 365 Environment

With deep expertise in Microsoft and cyber security, the consultants at Messaging Architects deliver the services you need to keep your Microsoft 365 environment safe. From risk assessments to continuous monitoring, epolicy review to email security, they will help you optimize your cloud environment.