5 Easy Steps to Achieve Microsoft 365 Cyber Resilience

Contents

The Rise of Microsoft 365 Cyberattacks

Protecting Microsoft 365 data is an essential aspect of a modern cybersecurity strategy, as the suite's applications permeate the daily operations of countless small and medium businesses and operations. Microsoft 365 contains a wealth of sensitive information and critical business data — and is the reason more small and mid-sized organizations than ever are investing in third-party solutions or managed backup services to protect it.[1]

With the implementation of Microsoft 365 on the rise, the risks associated with losing Microsoft 365 data are becoming more stressful by the day. Data loss results in serious operational disruptions and can inflict significant financial damage due to downtime and lost productivity. In one report, IT leaders estimated the cost of downtime to be $1,467 per minute ($88,000 per hour)[2] — which, for a business of any size, would be a crushing blow — but for a small or medium business? That type of damage could be insurmountable. A proactive approach to securing Microsoft 365 data is more than an innovative idea — it is imperative to ensure businesses maintain continuity, uphold legal and regulatory responsibilities, and maintain customer trust.

[1] 2024 Data Protection Trends Report

[2] https://www.veeam.com/resources/wp-data-protection-trends-report.html?wpty

Cost associated with data loss

The cost of dowtime to be $1,467 per minute ($88,000 per hour)

Data loss results in serious operational disruptions and can inflict significant financial damage

Steps to Prepare for Attacks

1. Control Who Has Access

Multi-factor authentication (MFA), the principle of least privilege (PoLP), and a software restriction policy (SRP) are all cornerstones of effective cybersecurity practices and are integrally related to the concept of a zero-trust architecture. Zero trust is a security feature that organizations can use to identify and control the execution of software on specified hardware. For small and mid-sized organizations using Microsoft 365, implementing such can act as a critical defense mechanism for protecting the many devices for which they are responsible.

MFA is an essential security measure that requires users to provide two or more verification factors to gain access to digital resources, such as email accounts, business applications, and online services. There are many benefits of MFA, for example, MFA can defend against the consequences of common cyberattacks such as phishing.

The principle of least privilege can also significantly enhance the security posture of your Microsoft 365 environment. PoLP minimizes the suite's potential attack surface for cybercriminals. If a user's account is compromised, the attacker is limited to the access rights of that account, which ideally should be as restrictive as possible. This damage limitation creates a quarantine zone for any security breaches and is pivotal in controlling the spread of an attack within an organization.

SRPs are a security feature that organizations can use to identify and control the execution of software on specified hardware. For small and mid-sized organizations using Microsoft 365, implementing such can act as a critical defense mechanism for protecting the many devices for which they are responsible. By dictating which software can and cannot run on a system, SRPs effectively reduce the attack surface available to malicious actors.

2. Protect Your Backups

Bad actors target enterprises and small and medium businesses at the same rate, and they are almost always looking to attack your backups. Backups are extremely important for Microsoft 365 — especially when you consider Microsoft's Shared Responsibility Model.[3] Ransomware poses a significant threat to data integrity, as attackers aim to encrypt an organization's files and demand payment to release them. Nevertheless, threats to data aren't limited to malicious attacks. Data can also be jeopardized by accidental deletions or various other mishaps.

Implementing a regular backup routine means establishing a schedule that strikes a balance between the volume of data handled and the resources available for backup operations. This should include backing up all data stored within the Microsoft 365 suite. Immutability also plays a pivotal role in securing an organization's digital assets against alteration or deletion, whether by cyberthreats or human error. For small and mid-sized organizations using Microsoft 365, immutable backups stand as a shield against ransomware attacks, which target not only live operational data but also backup repositories. In fact, according to one survey, almost all ransomware attacks (93%) specifically target backups.[4] So ensuring that you can recover your own data without having to pay out the ransom is a critical step in the survival of your small or medium business.

[3] Shared Responsibility in the Cloud

[4] 2023 Ransomware Trends Report

3. Incident Response Plan

An incident response plan details the processes an organization must follow when faced with various cybersecurity incidents, serving as playbooks for identifying, containing, eradicating, and recovering from security threats, and ensuring all stakeholders are informed and prepared to act. For small and medium organizations using Microsoft 365, the foundation of a strong incident response plan includes identifying critical assets within the Microsoft 365 ecosystem.

Your organizations should identify where sensitive data is stored, then define potential threats and create a prioritized list of risks, alongside strategies for mitigating them. This includes the use of integrated monitoring and detection tools, immediate containment strategies, threat eradication, robust communication between parties, and the identification and recovery of any lost or compromised data.

4. Audit, Test, Monitors, and Logs

Regular audits and penetration testing are integral components of maintaining a resilient Microsoft 365 environment. These practices serve as proactive measures, enabling firms to identify and rectify problems before they can be exploited as attackers. Monitoring and logging also constitute a vital step in ensuring the security and integrity of any Microsoft 365 environment. By keeping a vigilant eye on system activities and maintaining comprehensive records of events, organizations can detect potential security incidents in real time, diagnose system issues, understand the scope of breaches, and improve overall security posture.

Effective audits, tests, monitoring, and logs should cast a wide net to detect a range of possible anomalies indicative of a security threat. Over time, the insights gleaned from these observations can provide organizations with the data necessary for making proactive policy changes and streamlining security updates.

5. Data Separation and Encryption

Privilege separation is a widely applicable and effective strategy used by organizations to enhance their security infrastructure and is highly applicable when integrating data-driven services like Microsoft 365. By keeping different sets of data apart and dividing networks into discrete segments, organizations significantly reduce the initial risk of security breaches and effectively quarantines outbreaks should they occur.

The use of privilege separation policies within Microsoft 365 allows organizations to maintain strict access rules. Methodical separation can be applied to all levels of an organization's hierarchy and provides a robust foundation for securing Microsoft 365 data and other digital assets. Encryption is another fundamental security measure that serves as a primary line of defense in the protection of sensitive information, ensuring that only authorized parties with the correct decryption key can access the original information, and applies to data regardless of its use, movement, or location.

As it pertains to Microsoft 365, encryption provides a layer of security that helps businesses safeguard their communications, documents, and other data — no matter where they reside within their cloud infrastructure. Effective encryption ultimately forms the bedrock upon which privacy and regulatory compliance are built. Solid encryption practices are pivotal in the safeguard of valuable data against ransomware and cyberthreats, thereby underpinning privacy, ensuring regulatory compliance, and supporting a secure, collaborative workspace.

Microsoft 365 Cyber Resilience Begins with Backup

As we consider the future landscape of data management and security, Backup as-a-Service (BaaS) has emerged as a preferred method for protecting SaaS apps like Microsoft 365. Integrating BaaS with a Microsoft 365 strategy aligns with the need for robust, scalable, and flexible data protection solutions — all critical components for ensuring organizational resilience.

Backup services allow small and medium businesses to outsource their backup needs to specialized providers, who offer end-to-end solutions that can automate backup processes, reduce the amount of necessary on-premises infrastructure, and provide top-tier security measures — all while providing them direct access and control over their data. For Microsoft 365 users, BaaS means enhanced data safety, operational efficiency, and peace of mind.

Veeam Data Cloud *for Microsoft 365*

Veeam Data Cloud *for Microsoft 365* enables radical resilience for Microsoft 365 data, with a modern twist. The industry's leading Microsoft 365 backup solution — Veeam Backup *for Microsoft 365* — is now delivered as a service.

Simplify your backup strategy with software, backup infrastructure, and unlimited storage in an all-in-one cloud service that allows you to leverage powerful data protection and security technology within a simple, seamless user experience.

Veeam Data Cloud *for Microsoft 365* is a backup service providing comprehensive data protection and data recovery for **Microsoft Exchange, SharePoint, OneDrive for Business and Teams**, giving you complete control of your Microsoft 365 environment.

With **Veeam Data Cloud *for Microsoft 365,*** you get:

- **Trusted, industry-leading technology:** The most comprehensive data protection solution with over a decade of continuous innovation built to scale.
- **Modern, secure, and intuitive platform:** Easily create backup jobs, complete restores, and gain Microsoft 365 insights from within a modern, web UI.
- **All-inclusive service:** Software, backup infrastructure, and unlimited storage bundled together with ongoing maintenance covered by the experts.

→ Request a demo of
Veeam Data Cloud *for Microsoft 365*

Be Prepared, Stay Informed

Your journey towards Microsoft 365 cyber resilience doesn't end here — it is just getting started. Expand your understanding, refine your strategies, and stay ahead of the curve in 2024. Let us help you transform challenges into opportunities by checking out our expanded collection of resources:

- 4 Benefits of Microsoft 365 Backup Services
- Game Changing M365 Backup Service: What Small Businesses Need to Know
- Microsoft 365 Recovery Best Practices

About Veeam Software

Veeam, the #1 global market leader in data resilience, believes businesses should control all their data whenever and wherever they need it. Veeam provides data resilience through data backup, data recovery, data freedom, data security, and data intelligence. Based in Seattle, Veeam protects over 550,000 customers worldwide who trust Veeam to keep their businesses running. Learn more at www.veeam.com or follow Veeam on LinkedIn @veeam-software and X @veeam.

→ Learn more: veeam.com