Kaseya®

10 modern best practices to manage, secure and recover your Microsoft environment

Microsoft is mission-critical — and a target for cyberattacks

Microsoft 365 is the operating system of modern business. It has more than a million customers in the U.S. alone, and four out of every five Fortune 500 companies run on the platform.

For most organizations, Microsoft 365 is where email lives, where files are stored, where meetings happen and where work simply gets done. At the same time, rising server and storage costs are pushing more organizations to accelerate their move to Azure, deepening their integration with the Microsoft ecosystem.

That value comes with added risk. The same characteristics that make Microsoft indispensable — scale, centrality, and the sheer volume of sensitive data flowing through it — also make it one of the most attractive targets in the world for cyberattacks.

And as organizations adopt more Microsoft services, Microsoft has become a complex cloud environment, making it more difficult to maintain security policies and visibility.

Too often, Microsoft environments grow into a patchwork rather than a system. Security, infrastructure, identity, endpoint management, collaboration and cloud operations are managed through disconnected tools, teams and workflows. While Microsoft delivers powerful technology, IT teams consistently run into three recurring challenges:

- **Operational silos:** Users, devices, identities, licenses and endpoints are managed separately, making it difficult to enforce policy, automate routine administration or maintain unified visibility across the environment.
- **Identity-driven risk:** As Microsoft environments become more identity-centric, organizations face growing exposure to phishing, account compromise, unauthorized access and risky configuration changes across Microsoft 365, Entra ID and related services — making it harder for IT and security teams to catch threats before they escalate.
- **Over-reliance on native recovery:** Many organizations lean too heavily on Microsoft's built-in recovery tools, which keep backups inside the same tenant and credential ecosystem. That design increases the risk of ransomware attacks, tenant compromise, outages or accidental data loss, and it slows recovery exactly when speed matters most.

The new reality — you own the outcomes

Microsoft secures the platform. It does not secure your individual environment.

Microsoft is one of the largest and most respected technology companies in the world, and its engineers work around the clock to secure the infrastructure underneath Microsoft. But day-to-day security monitoring for individual end-user accounts? That responsibility isn't Microsoft's — it's yours.

This shift in responsibility, from the SaaS provider to the customer, is even written into Microsoft's own terms of service. Microsoft is not responsible for lost or stolen files, and its terms of use hold end users accountable for compromises within Microsoft 365. In practice, that means you can't outsource your organization's safety to your SaaS provider. That duty sits squarely on your shoulders.

Under this shared responsibility model, the customer owns:

- **Visibility and management:** Knowing what exists across users, devices and identities
- **Prevention and security:** Actively defending against phishing, compromise and misconfiguration
- **Recovery readiness:** Being able to restore data and operations on your own timeline, not Microsoft's

Nowhere is that gap more visible than in recovery. Microsoft's native capabilities are built for service availability and compliance, not for the operational recovery a real business continuity plan demands. Put side by side, the difference is clearer:

Native Microsoft Capabilities	Business Continuity Requirements
Retention	Recoverability
Redundancy	Operational resilience
Version history	Point-in-time recovery
Recycle bin	Granular recovery
Service availability	Business continuity
Cloud data storage	Isolated immutable backups & credentials
Shared responsibility	Shared responsibility

That distinction — between what's native and what's actually recoverable — is the thread running through everything that follows.

> The average cost of a data breach is now roughly $4.35 million globally, according to Microsoft. Preventing that check from ever needing to be written is one of the best investments an IT team can make.

10 best practices for managing, securing and recovering your Microsoft environment

Cybersecurity isn't as simple as it used to be. Attackers are finding more openings than ever and keeping Microsoft accounts safe requires the right combination of native controls and purpose-built tools layered on top. What follows are ten tips for managing, securing, and recovering your Microsoft environment, including some do's and don'ts, a few extra-credit strategies, and the tools that can help you stay ahead.

1 Start with the basics — and let Microsoft do some of the work

Microsoft doesn't cover your entire SaaS security posture, but it does give you a real head start. Several strong protections are already included in many Microsoft subscriptions. The trick is to turn them on and use them effectively.

Do

Take advantage of the security features Microsoft already offers. These won't be the end-all, be-all. You'll still want to layer additional protection on top. If the capability is already there, however, put it to work:

- **Defender:** Anti-malware, web protection and more
- **Purview:** Helps manage and categorize sensitive data
- **Secure Store:** An authorization service on SharePoint Server that provides credential storage and mapping

Don't

Forget about the most recent Microsoft patches.

- Keep end users current on the latest fixes to close doors for which attackers are actively looking
- Ignoring available patches leaves known vulnerabilities exposed

Bonus tip

The Kaseya Cloud Detection and Response solution makes it easy to implement and configure Microsoft's built-in security settings consistently for every end user — so the basics are enabled.

2 Centralize visibility across users, devices and identities

Your users, devices, identities, endpoints and applications are all connected, but managing them in separate tools creates blind spots, slows troubleshooting and increases risk.

Do

Create a single source of truth for your Microsoft environment by centrally documenting and maintaining visibility across:

- Users, identities, security groups and administrative accounts
- Microsoft 365 licenses and applications Workstations, laptops, servers, mobile devices and Cloud PCs
- On-premises infrastructure, virtual machines, network devices and printers

Don't

Manage Microsoft through disconnected tools and spreadsheets.

- New privileged accounts created without oversight
- Unauthorized device enrollments
- Security group and permission changes that go unnoticed
- Policy drift and configuration inconsistencies
- Stale accounts with lingering access
- Weak or outdated passwords and missing MFA enforcement
- Security and compliance gaps

The more visibility you have across your environment, the faster you can identify issues before they impact users. These operational silos make it harder to maintain control as your environment grows. This gives you a complete view of how users, devices, identities and permissions are connected, making it easier to identify issues before they impact users.

Bonus tip

Visibility isn't just about efficiency. It's the foundation of both security and recovery. If you don't know what exists in your environment, protecting or recovering it becomes exponentially harder.

Kaseya's IT service delivery solutions provide complete visibility and centralized management to your IT and Microsoft environments, helping you understand what exists, how everything is connected and the potential impact of every change because you can't secure what you can't see.

3 Standardize configurations before they become problems

When every department, site or administrator configures Microsoft 365 a little differently, what starts as flexibility quietly turns into technical debt.

Do

Establish consistent policies and configurations across your Microsoft 365 environment. Focus on:

- Security baselines
- Conditional access rules
- Device policies and compliance requirements
- User provisioning and offboarding processes
- Application permissions

Don't

Allow every department, site or administrator to configure settings differently.

- Security gaps open between inconsistent configurations
- Compliance issues become harder to track
- User confusion and increased support costs follow

When everyone follows the same standards, troubleshooting becomes faster and risk becomes easier to manage. This is where Conditional Access policies earn their keep. Build strong baseline policies to stop threat actors from getting in at all, then use tools to clone those proven policies across every client or business unit.

Bonus tip

Automate policy enforcement wherever possible. The less manual effort required, the more likely standards and compliance requirements remain consistent over time. Kaseya's endpoint management solution helps you enforce policies and governance wherever possible.

4 More MFA, fewer problems: But know its limits

Multi-Factor Authentication remains one of the most effective ways to prevent account compromise, but it isn't the silver bullet it once was. Treating it as a finish line rather than a starting point leaves a real gap.

Do

Enforce MFA for every user, and prioritize rollout for:

- Administrators
- Executives
- Finance teams
- Remote workers
- Third-party contractors

Don't

Assume passwords — or MFA alone — are enough.

- Passwords can be stolen, reused, phished, or purchased on the dark web
- Attackers increasingly use token theft to hijack an already-authenticated session, sidestepping MFA entirely
- MFA downgrade attacks are a real and growing technique

Passkeys can help defend against token theft, but they shouldn't be your only line of defense either. The stronger and more layered your identity protection is, the harder it becomes for attackers to gain and maintain access.

Bonus tip

Security awareness training and MFA are essential, but they can't stop every attack. If a session token is stolen, MFA can be bypassed.

*This makes **Kaseya's Cloud Detection and Response** essential for detecting and containing compromised accounts. Combined with **Kaseya's AI-powered email protection**, which provides real-time contextual guidance to help users identify suspicious emails, organizations can prevent more attacks before they become incidents.*

5 Monitor behavior, not just alerts

Attackers rarely announce themselves. Instead, they leave clues. The organizations that catch incidents early are the ones actively watching behavioral changes, not just waiting for static alerts.

Do

Continuously monitor user activity and environmental changes, including:

- Unusual login locations and impossible travel events
- Large-scale file downloads
- Suspicious sharing activity
- Permission changes
- New OAuth application approvals
- Malicious forwarding rules designed to quietly hide email

Don't

Wait for a user to report something suspicious.

- By the time a help desk ticket arrives, an attacker may have already accessed sensitive data
- They may have established persistence in the environment
- They may have already moved laterally across systems

Identifying anomalies early can prevent an incident from spreading. Reactive security leads to longer recovery times and greater business impact. The goal is to shrink the gap between compromise and detection to nearly zero.

Bonus tip

The goal is to have a proactive response and automated remediation whenever possible.

6 Protect data like it's already under attack

Customer information, financial records, intellectual property and employee data don't carry the same level of risk, but too many organizations treat them as if they did.

Do

Implement data protection controls around sensitive information using Microsoft's built-in tools for:

- Data classification
- Data Loss Prevention (DLP)
- Sensitivity labeling
- Information governance

Don't

Treat all data the same

- Without proper classification and monitoring, sensitive information can be shared, copied or exposed without anyone realizing it
- Customer information, financial records, intellectual property, and employee data carry different levels of risk

Understanding where sensitive data lives is the first step toward protecting it. Use the classification and DLP tools Microsoft already provides, and build monitoring on top, so exposure doesn't go unnoticed.

Bonus tip

The most damaging breaches aren't always caused by hackers. Misconfigured permissions and accidental sharing remain some of the biggest, and most preventable, causes of data exposure.

7 Backup doesn't equal recovery

Many organizations assume they're protected because Microsoft retains some data. Microsoft's native capabilities — retention policies, versioning, recycle bins and geo-redundancy — are valuable, but they weren't designed to provide comprehensive, operational recovery across the entire Microsoft estate.

Do

A complete recovery strategy covers more than just having copies of data. True resilience means being able to recover quickly, restore accurately, minimize downtime, maintain productivity and continue business operations through a disruption. That strategy should include:

- **Users and identities:** Restore deleted users and critical identity objects, recover from account compromise and preserve access to business-critical data
- **Exchange data:** Recover emails, folders, mailboxes, calendars, contacts or entire environments quickly, while retaining inactive user data cost-effectively to support long-term compliance
- **SharePoint data:** Restore sites, libraries, lists and documents, and protect against mass deletion and malicious changes
- **OneDrive data:** Restore employee files quickly, including after user departure or accidental deletion
- **Teams data:** Protect conversations, files and channels so teams don't lose the information they rely on every day

Don't

Don't mistake native retention for a complete recovery strategy. Microsoft's native capabilities are primarily designed for service availability, compliance and limited recovery scenarios. They may not fully address:

- Large-scale ransomware events
- Account compromise
- Insider threats
- Long-dormant data loss
- Bulk deletions
- Recovery needs that fall outside native retention windows
- Fast, granular restoration of business-critical information

Bonus tip

The real question isn't whether your data is backed up. It's how quickly you can get your business running again. A dedicated backup and recovery solution provides independent copies of Microsoft data, long-term retention flexibility, granular search and recovery, point-in-time restoration, faster recovery workflows, and recovery options that stay available even if Microsoft accounts or infrastructure are compromised.

8 Prepare for the worst day, not the best day

Every organization has backups. Far fewer have proven they can actually recover under pressure. Recovery planning should assume a disruption will happen and focus on how quickly normal operations can be restored.

Do

Create and test recovery plans regularly. Every organization should be prepared for:

- Ransomware attacks
- Account takeovers
- Accidental deletions
- Insider threats
- Service outages
- Third-party application failures
- Data corruption events

Don't

Wait until an emergency to validate your recovery process.

- Missing backups
- Incomplete recovery procedures
- Gaps in documentation
- Access issues
- Recovery delays that compound under pressure

Testing recovery procedures reveal weaknesses before an actual incident occurs. It helps answer the questions that matter most before you're under pressure to answer them: Can we find the data we need? How long will recovery take? Who owns which part of the process? What systems are most critical? Can we restore without disrupting users? Hope is not a disaster recovery strategy.

Bonus tip

Organizations that recover fastest aren't necessarily the ones with the most backups. They're the ones that have practiced recovery before they needed it.

9 Automate response wherever possible

Every minute matters during a security event. The faster a threat is contained, the smaller its blast radius. That's why automation, not manual triage, needs to be the first line of response.

Do

Reduce response times through automation. Many common incidents can trigger immediate action, such as:

- Alerting administrators
- Disabling compromised accounts
- Blocking risky sign-ins
- Escalating incidents
- Launching remediation workflows

Don't

Rely entirely on manual investigation and response.

- Security teams are already overwhelmed
- Manual processes create delays that attackers can exploit
- Every added minute of manual triage is an opportunity for an incident to spread

Bonus tip

The fastest response is often the one that happens before a human even notices there's a problem.

10 Secure the inbox before attackers reach your identities

Most Microsoft account compromise incidents begin the same way: with an email. As AI-generated phishing attacks become more convincing and scalable, attackers are increasingly using email to steal credentials, bypass traditional defenses and gain access to Microsoft environments.

Do

Layer AI-powered email security on top of Microsoft's native protections to help identify and stop:

- AI-generated phishing and social engineering attacks designed to evade traditional detection
- Credential harvesting attempts that target Microsoft 365 users and identities
- Business Email Compromise (BEC) and impersonation attacks
- Malicious links, QR codes and suspicious cloud-hosted content
- Threats that use brand impersonation, conversation hijacking and other tactics to appear legitimate

Don't

Treat email security and identity security as separate problems.

- Most account takeover attacks begin with a successful email-based compromise
- A suspicious email, risky sign-in, unusual mailbox activity or privilege escalation event may be related indicators of the same attack
- Investigating email threats and identity activity independently can delay detection and response

Bonus tip

The strongest Microsoft security strategies connect email protection, identity monitoring and threat detection. By correlating signals across the inbox, user accounts, and Microsoft 365 activity, organizations can identify threats earlier and respond before a compromised account becomes a larger security incident.

Purpose-built protection for your Microsoft environment

Microsoft gives your organization powerful tools to work, collaborate, and grow, but managing, securing, and recovering that environment is your responsibility, not Microsoft's. Closing the gap between what Microsoft provides natively and what true resilience requires means centralizing visibility, standardizing configuration, layering identity protection beyond MFA, continuously monitoring behavior and building a recovery strategy that stands on its own — independent of the tenant it protects.

Kaseya brings these capabilities together on one platform purpose-built for how Microsoft environments need to be protected: centralized visibility and policy enforcement, cloud detection and response for identity-based threats, email security that goes beyond native filtering and independent, granular backup and recovery for Exchange, SharePoint, OneDrive and Teams.

See how Kaseya can help you manage, secure, and recover your Microsoft environment.

Start the conversation today

Kaseya®

Kaseya is the leading global provider of AI-powered IT management and cybersecurity software. Kaseya delivers a unified technology platform to manage infrastructure, secure endpoints, back up critical data, and streamline operations for more than 40,000 MSP and SMB customers around the globe. To learn more, visit www.kaseya.com.

kaseya.com