Mirazon

WHITEPAPER

From Defaults to Defense: Securing Your Microsoft 365 Tenant

Microsoft 365 Security Best Practices & Implementation

www.mirazon.com
(502) 240-0404
info@mirazon.com

More Than Email: Securing the Heart of Your Organization

Microsoft 365 is more than just email—it's the hub for your team's communication, collaboration, file storage, and device management. But with great power comes great responsibility. While Microsoft keeps the platform running and secure on the infrastructure side, **you're still responsible for protecting your data, identities, and access.**

That's where this guide comes in. We've distilled the most critical best practices for **security, identity management, collaboration governance, and data resiliency** into one approachable resource. Think of it as a roadmap for keeping your environment **safe, compliant, and resilient** without slowing your team down.

Inside, you'll find:

- How to understand and mitigate the **modern threat landscape.**
- Steps to lock down **identities and admin access.**
- Tips for securing **collaboration tools and sensitive data.**
- Guidance on **backup and resiliency** to protect against accidental deletion, ransomware, or other disasters.
- Actionable **next steps** to make real improvements in your tenant.

Whether you're an IT pro looking to tighten controls or a leader wanting confidence that your data is protected, this guide gives you the **practical, prioritized actions** you need—no fluff, no guesswork.

The Modern Threat Landscape

Microsoft 365 is the center of where your team emails, collaborates, stores files, and manages devices. It's powerful, but that also makes it a prime target for cyberthreats and attacks. While Microsoft handles the infrastructure, your team is still on the hook for securing identities, access, and data.

The shift to the cloud means attackers aren't just breaking into servers anymore—they're going after people. Credential theft, OAuth (Open Authorization) abuse, and lateral movement inside trusted apps are now the norm.

Data Theft

Unauthorized access and theft of sensitive business information via compromised accounts or malicious apps.

Emailed-Based Attacks

Phishing, business email compromise (BEC), and hijacked inboxes through malicious connectors or rules.

Ransomware & Data Destruction

Modern ransomware doesn't just lock files—it can delete, corrupt, and even wipe backups using stolen credentials.

Bottom line: The cloud gives your team flexibility—but it also gives attackers more ways in. Understanding the risks is just the first step. From there, it's about taking control of your environment, securing identities, setting smart access policies, and making sure your backup and recovery strategies are ironclad.

A few proactive steps today can save your team from hours of frustration, potential downtime, and costly data loss tomorrow.

Identity & Access Control (Microsoft Entra ID)

Microsoft Entra ID is the heart of Microsoft 365 security. If an identity gets compromised, attackers can move laterally and take over your entire tenant. That's why applying the **Principle of Least Privilege (PoLP)** here delivers the biggest security bang for your buck.

Security Defaults vs. Conditional Access

- **Security Defaults** – Think of this as your safety net. It provides baseline protections, including mandatory MFA for all users. It's all-or-nothing, and should stay enabled unless you're using Conditional Access. Learn More >>
- **Conditional Access** – This is the fine-tuned control panel. Require MFA only under certain conditions (like when logging in from an unmanaged device or a risky location), enforce compliant devices, or block logins from high-risk regions. Learn More >>
- **Pro Tip:** If nothing else, enable any form of MFA immediately. It's hands down the single most effective defense against automated credential attacks.

Administrative Account Management

- **No "Daily Drivers"** – Admin accounts are too powerful for routine tasks. Don't check email or browse the web with them. Always use separate sessions (incognito/private browsers help) to minimize risk.
- **Break-Glass Accounts** – Keep at least one emergency access account. Make it cloud-only, exclude it from Conditional Access to prevent lockouts, protect it with a strong password or FIDO2 key, and store it securely. Test it periodically so it's ready when you need it.
- **Privileged Identity Management (PIM)** – Use PIM for just-in-time access. Admin roles are only active when you need them and automatically expire afterward. Less time with power = less time for attackers to exploit it. Learn More >>

Session & Application Security

- **Idle Session Timeouts** – Automatically sign users out after periods of inactivity, especially on shared or unmanaged devices.
- **Admin Consent Workflow** – Require administrator approval for third-party app registrations. This blocks "consent phishing," which can quietly give apps persistent access without triggering MFA. Learn More >>

Bottom line: Your identities are your keys to the kingdom—treat them with care. Enforce MFA, manage admin accounts wisely, control sessions, and vet every third-party app. Small steps here prevent big headaches down the line.

Collaboration & Data Protection

Microsoft 365 runs on a **Shared Responsibility Model:** Microsoft locks down the infrastructure, but **you're still in charge of your data, who can access it, and how it's shared**. Neglecting governance here is one of the most common ways sensitive information slips out the door.

Governance for Teams & SharePoint

- **Review external sharing regularly** – Keep tabs on tenant- and site-level sharing policies to avoid accidental exposure.
- **Classify sites correctly** – Public or Private? Make sure each site matches its intended audience.
- **Expire guest access** – Configure automatic expiration so former collaborators don't retain indefinite access.

Misconfigured collaboration settings aren't just a risk—they're a target. Regularly reviewing these controls keeps your data in the right hands. Learn More >>

Email & Threat Protection

Microsoft Defender for Office 365 protects against phishing, malware, and business email compromise. Quick wins include:

- **Use Preset Security Policies** – Standard or Strict configurations apply Microsoft's recommended anti-spam and anti-phishing settings with zero guesswork.
- **Avoid over-customization too soon** – The built-in baselines are strong and battle-tested. Learn More >>

Audit Logging & Visibility

- **Enable the Unified Audit Log in Microsoft Purview** – Keep a searchable record of user and admin activity. Standard retention covers at least 90 days; longer retention is available with E5 or Audit Premium licenses.
- **Why it matters** – Audit visibility is critical for investigating incidents, answering compliance questions, and understanding what happened when things go sideways.

Bottom line: Collaboration and data protection are about smart guardrails, not roadblocks. Keep sharing in check, protect inboxes from attacks, and always have visibility into your environment. It's your best defense against human error and targeted attacks.

Resiliency & Backups

Here's a myth that needs busting: **Microsoft doesn't provide traditional backups for Microsoft 365**. While the platform is highly available and redundant, that only keeps the service running—it doesn't protect you from mistakes, ransomware, or accidental deletion.

High Availability vs. Backup

- **High Availability** – Keeps your services online and humming.
- **Backup** – Protects your data when things go wrong. **Microsoft does not guarantee recovery** from:
  - Accidental or malicious deletion
  - Ransomware or other malware encryption
  - Insider activity
  - Data corruption discovered after retention periods expire

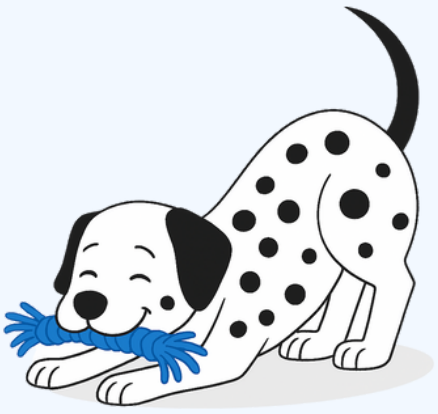
Retention policies and versioning are helpful, but **they are not a replacement for a dedicated backup solution**.

Backup Recommendations

- **Microsoft 365 Backup** – A native option for fast, in-ecosystem recovery.
- **Third-Party Solutions (e.g., Veeam)** – Offers additional features like immutable storage, air-gapped copies, and regulatory compliance.

When evaluating solutions, consider your **Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**—basically, how fast you need to recover and how much data loss you can tolerate.

Bottom line: High availability keeps your services running, but a backup keeps your data safe. Invest in a backup strategy today, and you'll thank yourself when mistakes—or worse—happen tomorrow.
Learn More >>



Next Steps for Your Organization

You've got the knowledge—now it's time to take action. Think of this as your practical roadmap to tighten security, protect data, and reduce risk across your Microsoft 365 environment. A few focused steps today can save hours, or even days, of headaches tomorrow.

#1) Check Your Scores

Start with Microsoft Secure Score and Compliance Score. These tools aren't just numbers—they're a prioritized, tenant-specific list of improvements that show you exactly where your environment is strong and where it needs attention. Treat it like a tailored "to-do list" for security and compliance.

#2) Audit Your Admins

Admins hold the keys to the kingdom, which makes them a top target for attackers. Regularly verify that every Global Admin:

- Uses a dedicated admin account (no "daily drivers" for email or browsing)
- Has multi-factor authentication strictly enforced
- Only has the roles necessary for their job responsibilities

Doing this reduces the blast radius if an account is ever compromised and ensures no one has unnecessary privileges lurking in your tenant.

#3) Evaluate Your Backup Strategy

Backups aren't just insurance—they're your lifeline. **Review your Recovery Time Objective (RTO)** and **Recovery Point Objective (RPO)**, and make sure your current solution—whether Microsoft 365 Backup or a trusted third-party provider—meets your recovery needs.

Consider scenarios like accidental deletion, ransomware, or insider errors, and ensure you can bounce back quickly without losing critical data.

Bottom line: Security, access, and backups aren't "set it and forget it." They're ongoing responsibilities that, when done right, turn Microsoft 365 from a potential risk into a resilient, reliable platform your team can trust. Regular checks, audits, and adjustments are the difference between reacting to incidents and staying ahead of them.

Let's Turn Best Practices Into Real Protection

Microsoft 365 is a powerful platform, but power comes with responsibility. Protecting identities, securing collaboration, and ensuring resilient backups aren't just IT tasks—they're essential steps to keep your organization running smoothly and your data safe.

You don't have to tackle it alone. Whether you need guidance on implementing best practices, auditing your environment, or setting up a bulletproof backup strategy, **our team is here to help**. Think of us as your trusted partner in making Microsoft 365 **safer, smarter, and stress-free**.

Take the insights from this guide, review your environment, and reach out if you need expert assistance. With a few strategic steps and the right support, you can turn Microsoft 365 into a platform that **works for your team—not against it**.

Next steps:

- Review your scores, admin accounts, and backup strategy
- Apply the best practices outlined in this guide
- Contact us for hands-on assistance, guidance, or a full Microsoft 365 security review

Your data, your users, and your peace of mind are worth it—and we're ready to help you get there.

Contact Us

Mirazon®

www.mirazon.com
(502) 240-0404
info@mirazon.com
1640 Lyndon Farm Ct., Suite 102
Louisville, KY 40223