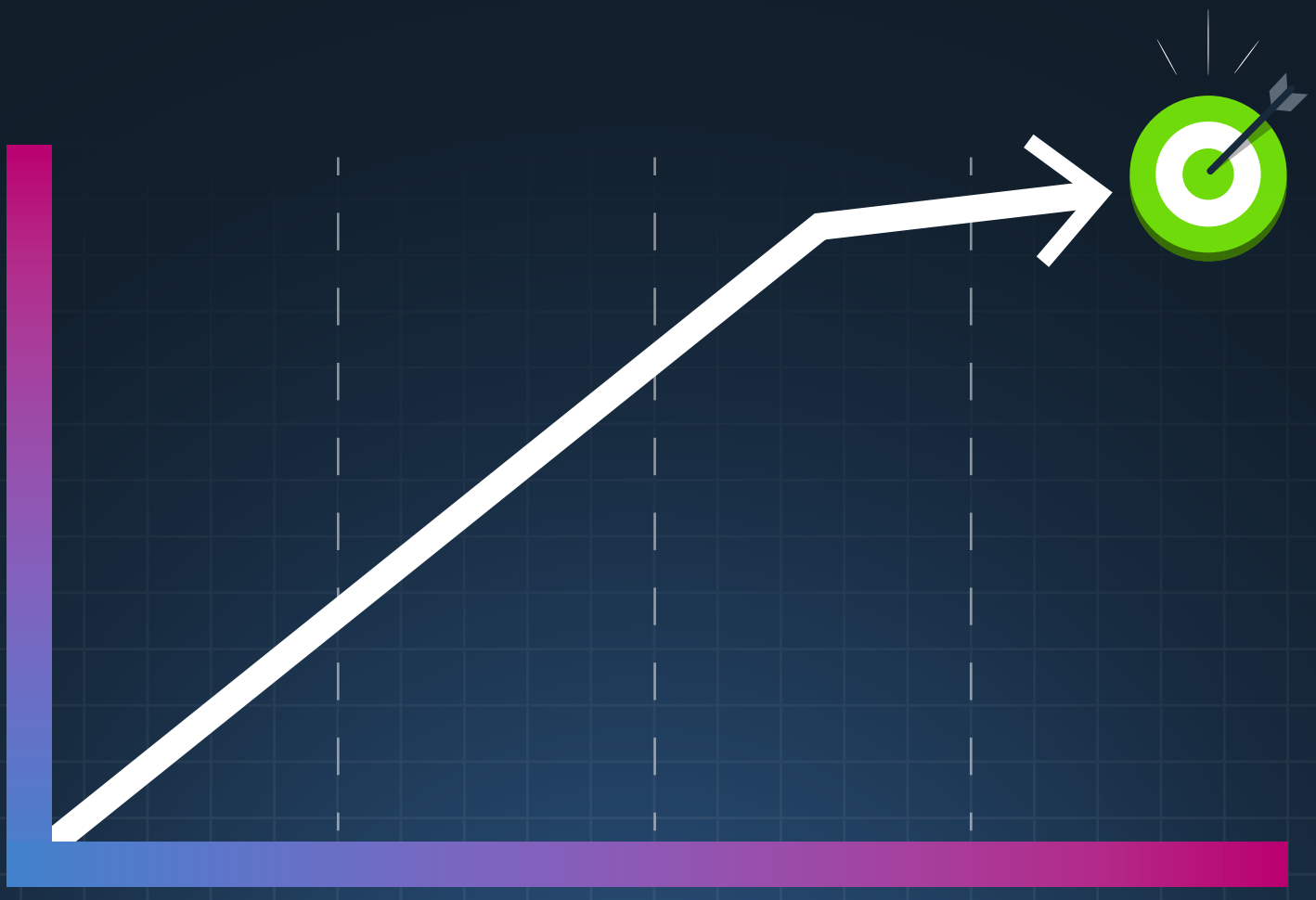
CoreView

Microsoft 365 Cyber Resilience Maturity Model:

A Step-by-step Framework to Harden Your Tenant



Cyber Resilience for Microsoft 365 – Who Cares?

You're busy. So why should Cyber Resilience for Microsoft 365 demand your attention?

It goes without saying that the global pandemic put the final nail in the coffin for traditional office-based work. But even since we started to prioritize getting back to the office, every human interaction now has a digital counterpart.

If you can't reference your emails, search through your Teams chats, or dial in Bob who couldn't make it in due to a family issue, you're not going to get very far.

Even in our physical workspace we are relying on our digital workspace, and for 80% of the Fortune 500, that digital workspace is Microsoft 365.

This means that if your Microsoft 365 tenant is breached, you don't just have a cyber attack to worry about, but also the risk of your digital workspace facing operational downtime.

And when your digital workspace isn't working, your business isn't working.

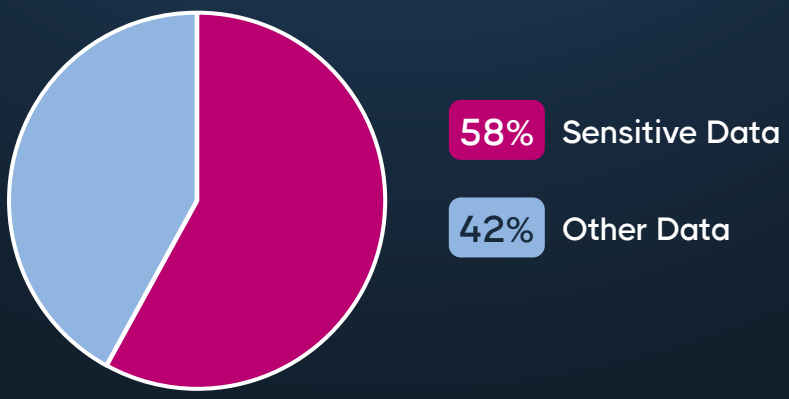
The Data on Tenant Compromise

Given that the average Microsoft 365 tenant contains 58% of an organization's sensitive cloud data and arguably has the most powerful privileged accounts a business has, it is a prime target for cybercriminals.

While the major data breach analysis reports still don't offer a breakdown based on SaaS environments, industry surveys have revealed that Microsoft 365 tenants are still facing a constant barrage of attacks.

Sensitive Cloud Data in Microsoft 365

With **58%** of an organization's sensitive cloud data stored within, Microsoft 365 tenants are prime targets for cybercriminals.



Nation state attackers like Nobelium (Midnight Blizzard) and Hafnium have consistently prioritized attacks on Microsoft 365 tenants, to the point that CISA is now mandating all federal agencies to implement secure configurations across all Microsoft 365 tenants by June 20th 2025.[1]

Outside of the public sector, a Vectra survey[2] of over 1,000 security professionals found that 71% of Microsoft 365 deployments had suffered an average of seven successful account takeovers.

For most Microsoft 365 organizations, it is no longer a question of if their tenant will be breached, it is a question of when (and how often).

And once inside your environment, it takes an attacker an average of 16 hours to reach your Directory (Entra/AD).[3]

Essentially, once your tenant is breached, there is a ticking clock until the attacker gets to the crown jewels.

So, what does this mean?

It would be perfect if someone could promise that your tenant won't ever be compromised, but we all know that in 2025 this is a fantasy.

Instead, we need to use resilience to reduce the impact of a breach when it happens.

Time is Ticking

Once inside your environment, it takes an attacker an average of **16 hours** to reach your Directory (Entra/AD).

In a short timeframe, attackers can exploit pathways to domain admin access, significantly increase the risk of data breaches, and escalate their privileges.

What is Cyber Resilience for Microsoft 365?

NIST defines Cyber Resilience as:

> *"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."* [4]

Let's break this down into its four constituents and look at what this may involve for Microsoft 365.

Anticipate

Whereas traditional security builds defenses based on an existing understanding of best practices, cyber resilience implores security teams to look ahead and anticipate emerging threats and trends.

This is challenging. No one can successfully predict the future. However, you can ensure you partner with vendors and service providers who react quickly to the threat landscape. And you can implement an internal process to review emerging threats frequently and adapt your internal standards appropriately.

Implementing such a process is a strong starting point, but it should also include a practical way to make changes quickly. For example, if you identify a requirement that your existing toolset cannot deliver, you will be able to adapt faster if you have an extensible platform.

Because of this, it is important that the vendors you partner with for Microsoft 365 security and cyber resilience have an extensible platform that will allow you to respond to changing requirements quickly.

The Four Pillars of Cyber Resilience in Microsoft 365

1. Anticipate
Look ahead to emerging threats.

2. Withstand
Implement robust security measures.

3. Recover
Restore configurations and services.

4. Adapt
Learn and evolve from experiences.

Withstand

It is common sense to suggest that every organization should implement strong access-level security for its tenants, such as email filtering, zero-trust authentication, and cloud access control. However, withstanding an attack means implementing robust security measures to minimize the impact when someone successfully outwits or bypasses these controls.

To minimize the impact when your tenant is breached, you will want to make it as difficult as possible for cybercriminals to move laterally, elevate their privileges, persist in your tenant, and reach their final objective.

At a high level, we can recommend the following initiatives:

Enforce Least Privilege

- Create custom admin roles with "just enough" access instead of using the native admin roles provided by Entra
- Monitor and manage Entra Apps privileges
- Ensure all users have their permissions properly configured and are not accidentally over-privileged

Enforce Secure Configuration

- Ensure all tenant configurations and policy details are configured according to best practice
- Monitor all configurations and get alerted when they drift from your ideal baseline
- Implement configuration change management to ensure that configuration changes are properly tested and that you do not deploy dangerous configurations

Collaboration Monitoring

- Monitor external, guest, and anonymous users within your tenant and detect/remediate high-risk scenarios
- Monitor your tenant for dangerous sharing and high-risk external sharing
- Monitor exchange for suspicious mailboxes and high-risk mail configurations

Lifecycle Management and Governance

- Implement a rigorous user onboarding process to ensure that all Microsoft 365 users are properly configured without unnecessary or accidental privileges
- Detect unused objects and users and deprovision them on an ongoing basis
- Perform ongoing access reviews for users in Microsoft 365 to ensure that unused privileges/access is removed
- Enforce comprehensive user offboarding as soon as a user no longer needs access to your tenant

Recover

Since the first days of Office 365, the scale of the offering has ballooned to include over 40+ workloads, including services like Entra, Intune, Defender, and Teams—all of which are mission critical for business operations.

These services come with configurations. *A lot of them.*

There are now over 10,000 unique policy elements across Microsoft 365's many configuration types, with many of these designed to have multiple variations (e.g., multiple user groups or conditional access policies).

This means **the day-to-day operation of a Microsoft 365 tenant may rely on hundreds of thousands (or in some cases millions) of unique configurations.**

With this complexity, it is now critical that organizations keep their Microsoft 365 tenant configurations backed up, ready to be restored in the event of a disaster.

With this said, here are some key areas to prioritize in your cyber resilience recovery strategy:

Comprehensive Configuration Backup

Microsoft does not keep your tenant configurations backed up for a disaster.

Needing to manually reconfigure your tenant is not just a time issue, it is also a security one. Without rigorous controls in place from day one, your tenant will be vulnerable to attacks. Restoring your tenant ensures rolling out strong security baselines across configurations for these applications:

- Entra
- Intune
- Defender
- Purview
- Teams
- SharePoint
- Exchange
- Microsoft Admin Center

Roll Back and Restore Configurations

Configuration backup is critical for big disasters, but your ability to recover is only as good as your ability to restore configurations into production tenant:

- The ability to roll back to a previous configuration state
- The ability to restore configurations in a disaster

Secure Admin Delegation for Secure Recovery

Ensure you can delegate admins with “just enough” access to perform key tasks during the recovery process.

Streamlined Management for Faster Recovery

- Consider using an enhanced management layer for Microsoft 365 to simplify and speed up critical administration during the recovery process
- Democratize, automate, and simplify complex tasks to minimize unwanted mistakes during the recovery process

Adapt

The final element in the NIST definition of cyber resilience is the ability to adapt and continuously improve your tenant security based on what you learn from past incidents.

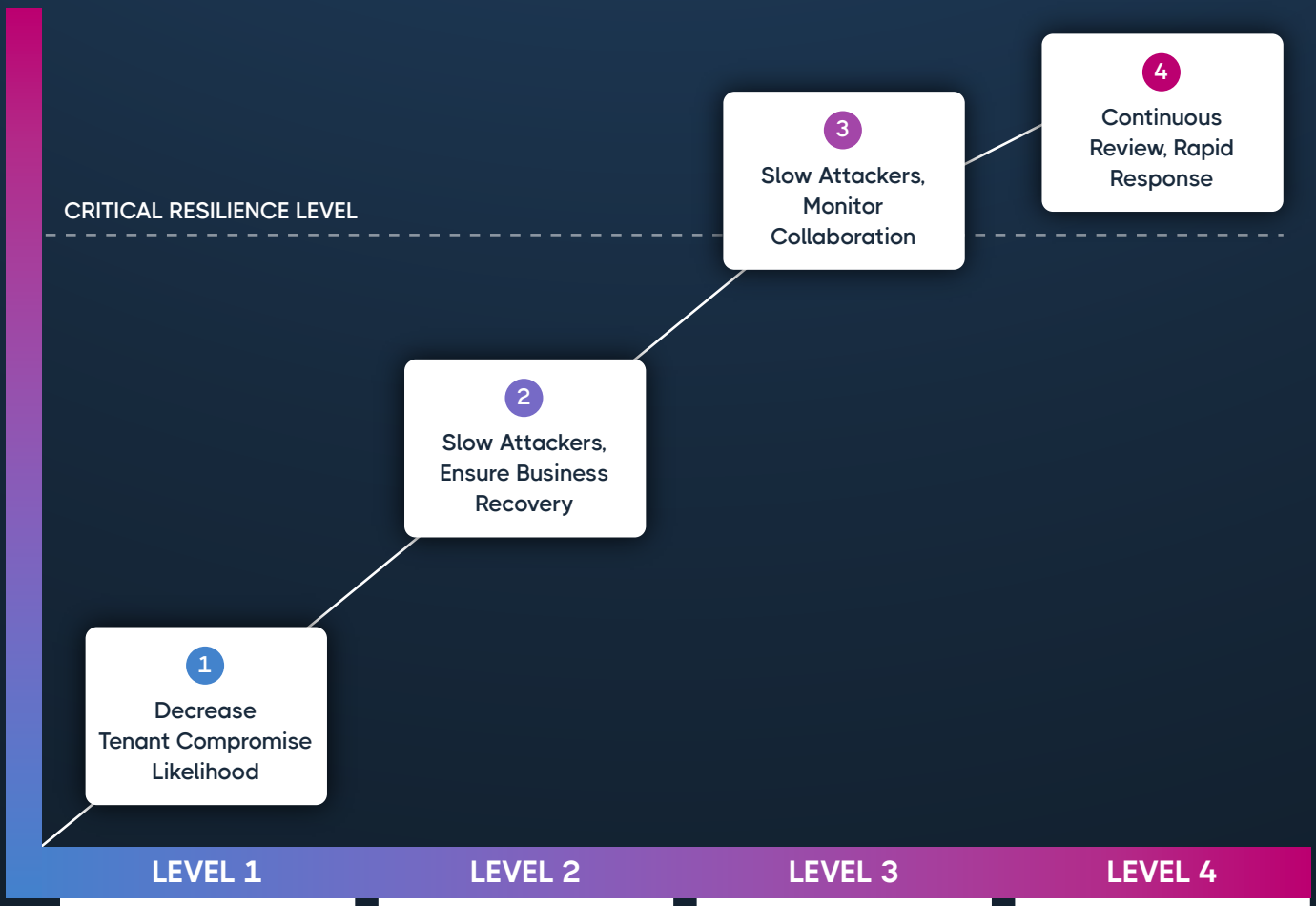
To ensure you can do this, it is critical to ensure you are working with platforms that are extensible and allow you to adapt them to your unique requirements.

Extensible Reporting and Automation

- Review your Microsoft 365 security toolset and identify where you can customize (and where you cannot)
- Invest in platforms and/or skills that enable you to create custom reports and visibility based on your requirements
- Invest in platforms and/or skills that enable you to create custom automations and remediations based on your requirements.

There are now over **10,000** unique policy elements across Microsoft 365’s many configuration types, with many of these designed to have multiple variations (e.g., multiple user groups or conditional access policies).

The Cyber Resilience Maturity Model for Microsoft 365



LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
ACCESS SECURITY & DATA BACKUP	**CONFIGURATION & BACKUP**	**LEAST PRIVILEGE & COLLABORATION**	**GOVERNANCE & AUTOMATION**
• Zero-Trust Auth • Privileged Access • Email Filtering • Cloud Access Control • Data Backup	• Config Backup • Deploy Secure Configs • Detect Drift • Enforce Change • Test M365 Updates	• Least Privilege Roles • Entra Apps • External Users • High-Risk Sharing • Suspicious Mailboxes	• Lifecycle Management • User Access Reviews • Enhanced Admin UI/UX • Secure Task Automation • Rapid Extensibility

The Cyber Resilience Maturity Model for Microsoft 365

Level 1: Access Security and Data Backup

OUTCOMES: REDUCE THE LIKELIHOOD OF INITIAL COMPROMISE

Implementing Basic Cyber Hygiene

Implementing the controls associated with Level 1 will help you enforce strong user access, email filtering, and data access controls for your tenant, driving down the risk of an initial breach.

For the sake of this model, it is assumed that most organizations have some of the basics in place here. However, as we'll see in Level 2, there are some additional layers of resilience that are required to ensure that your tenant perimeter is properly secured.

Privileged Access Management vs. Least Privilege

This is also an important place to note the contrast between Privileged Access Management and truly enforcing Least Privilege (something we will cover in Level 3).

Traditional Privileged Access Management (PAM) tools vault privileged accounts and then enforce strong authentication and monitoring for them. This, however, is distinct from truly enforcing least privileged access. **In the context of Microsoft 365, true least privileged access requires you to give each administrator "just enough" access to perform their role. Doing this with the 80 native Microsoft admin roles is not possible as these roles are not designed to fit one-to-one with your organization's operational needs.**

Therefore, **achieving *true* least privileged access requires the ability to quickly create roles that have "just enough" access—something that traditional PAM tools are unable to do.**

With that said, starting with privileged access management, zero-trust authentication, email filtering, and other basic cyber-hygiene practices are a critical foundation for a well-built Microsoft 365 cyber resilience strategy. We will see how we build on this foundation with Levels 2-4.

Achieving true least privilege access requires quickly creating roles with **"just enough"** access—something traditional PAM tools cannot provide.

Level 2: Configuration and Backup

OUTCOMES: REDUCE THE IMPACT OF TENANT COMPROMISE

The controls associated with Level 2 are designed to significantly reduce the impact of a tenant breach when it occurs. Let's run through each control.

Backup Microsoft 365 Configurations

Microsoft does not back up your tenant configurations.

This means that if your configurations are changed or a disaster partially (or totally) destroys your configurations, you have no way to quickly rebuild and restore business operations.

As we will see further below, it is not uncommon for cybercriminals to change configurations as they push through your tenant to their target destination. And it's also possible that a ransomware attack could encrypt your tenant entirely, potentially requiring you to move to a new tenant.

In these scenarios, **having your configurations backed up and ready to be rolled back or restored will enable you to weather difficult storms.**

It is especially important to note that during the reconfiguration/recovery process, a business is especially vulnerable to further attacks. Because of this, being able to deploy your best practice Intune, Entra, Defender, and Purview policies from day one will not only save you time but will also improve your resilience against further compromise.

Microsoft 365 does not back up your configurations, but Gartner recommends CoreView as a vendor that can deliver this—along with many of the other cyber resilience requirements listed below.[5]

Deploy Secure Configurations

How do you practically ensure all your configurations are what they should be?

With over 10,000 configuration and policy elements, Microsoft 365 is almost impossible to configure properly. Even the best teams in the world will make mistakes.

Following an analysis of many successful cyberattacks on Microsoft 365 tenants, the Microsoft Incident Response team recommended that organizations:

> *"Adhere to security configuration baselines and best practices when deploying and maintaining identity systems, such AD and Azure AD infrastructure."*
>
> **– Microsoft Digital Defense Report 2023**[6]

Baselines act as an independent source of truth and (with some good tooling and automation) can streamline the configuration process, especially for multi-tenant environments.

Detect Configuration Drift

Research shows[7] that cybercriminals are big fans of MITRE technique T-1562 – Impair Defences:

> *"Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior."*
>
> **– MITRE ATT&CK framework**[8]

In the context of Microsoft 365, the best way to impair defenses is by tampering with Entra, Intune, Purview, and Defender configurations.

And research from Sophos X-OPs shows that attackers have been doubling down on disabling Microsoft Defender as they work through the tenant. Their research shows that use of this technique nearly doubled between 2021 and 2023.[9]

Microsoft's most recent Digital Defense report also highlights this issue:

> *"In May 2024, Microsoft Defender XDR recorded over 176,000 incidents related to security setting tampering."* [10]

Thankfully, the guidance from Microsoft (see "Deploy Secure Configurations") continues to have value here. By using configuration baselines, you not only streamline the configuration process, but with the right automation and tooling, you can also detect when your configurations deviate from the baseline.

Using software like CoreView Configuration Manager will enable you to detect when configurations change in Microsoft 365, allowing you to quickly respond to this common attack technique.

Enforce Configuration Change Management

It is also important to plan for security gaps accidentally created by busy admins.

With so much to do, it's not unusual for administrators to accidentally misconfigure something. Sometimes, the impact of this will be sudden and obvious (e.g., a disastrous change to your company's conditional access policy), but it can also be silent and deadly—not revealing itself until it's too late.

To prevent such misconfigurations, Microsoft recommends that:

> *"Alterations to the intended configuration of a Microsoft Entra tenant are subject to robust configuration change management."*
>
> **– Microsoft Learn – Preventing Misconfigurations**[11]

Delivering change management in this context requires you to create dev and test environments where you can test new configurations before deploying them into production.

This sounds simple enough, but doing this requires you to create separate tenants, each of which must maintain consistent configurations. **If configurations vary between your test and production tenants, the legitimacy of the testing process will be undermined.**

This further highlights the need to deploy secure configurations to multiple tenants to achieve full cyber resiliency.

Detect and Test New Microsoft 365 Updates

This final control is critical to ensure you remain in control of your tenant security.

One of the biggest trade-offs of moving to the cloud is that you are no longer in control of when and how you deploy updates to your Microsoft infrastructure.

This matters. On premises, organizations prefer to test the impact of new updates in a contained environment before rolling them out across their infrastructure. However, in the cloud you lose this privilege—and potentially with severe consequences.

In one incident, a global brand had its production tenant compromised just 60 minutes after a new Microsoft 365 update was auto-deployed, changing some seemingly innocuous security configurations in their environment. This was despite months of careful configuration of Microsoft's native security capabilities.

Such a case study highlights the need to take back control of the update process.

Therefore, it is **recommended that organizations implement an alerting process to detect new updates and create a mechanism to test the new updates within a contained environment.** This is not possible with Microsoft's native updates, but it is with a tool like CoreView Configuration Manager.

Retaining Control Over Microsoft 365 Updates

Level 3: Least Privilege and Collaboration

OUTCOMES: REMOVE COMMON PRIVILEGE ESCALATION PATHWAYS

With your configurations now tamper-proof, Level 3 looks to remove escalation vectors that cybercriminals love to exploit.

True Least Privilege Admin Roles

We all know it by now: doing security properly means managing privileges.

However, there is an astonishing delta between traditional privileged access (emphasis on "access"!) management and true least privilege.

PAM tools focus on the access part: let's get our most powerful accounts, store them in an encrypted vault, enforce strong zero-trust authentication on the front end, and monitor and audit their usage.

This is a brilliant start, but all this does is implement layers of security around the bomb, rather than reducing the bomb's explosive power.

When it comes to successfully weathering a cyber attack, we need to look at Microsoft's admin powers from both angles: managing access to them and reducing them to the bare minimum required.

Where possible, organizations should avoid using the big permissive accounts that Microsoft offers in favour of customized admin roles. **The problem is that creating custom roles in Entra is not only complex and confusing, but it also still leads to a classic trade-off between security and operations.**

Using a delegation management tool like CoreView allows you to create "just enough" access for admins in a few clicks. This is great for productivity and enabling less experienced, less trusted admins to self-serve. But, the big win here is security: if such an admin is compromised, the scope of the powers available to the attacker is significantly lessened.

Wherein some tenants the pathways to privilege are plentiful, they will be barren and riddled with limitations in yours.

When it comes to successfully weathering a cyber attack, we need to look at **Microsoft's admin powers** from both angles: managing access to them and reducing them to the bare minimum required.

Entra App Management

In 2024, Microsoft announced that its own tenants had been successfully breached by the nation-state group Nobelium (Midnight Blizzard).

The culprit? Well, like every attack, there were multiple points of failure, but one technique the attackers relied on was to find, exploit, and create Entra Apps.

Microsoft recommends that a tenant have no more than four global admins, and yet, Entra Apps (which can quickly accrue enough permissions to be considered a global admin equivalent) have no such guidance applied to them.

In the Midnight Blizzard attack, the cybercriminals used an existing app to elevate from Microsoft's dev tenant into their production tenant. Then, they used these newly gained powers to create even more privileged Entra Apps for persistence.

The big takeaway here? If Microsoft is struggling to maintain oversight of their own Entra Apps then there is probably a need for proactive reporting.

Best practice here requires building out visibility to show where your apps are and what permissions they have, highlighting those that are high-risk.

Any applications with readwrite.all level permissions should go through a security review, and any applications that are not being used should be immediately deprovisioned.

Introducing these reviews into your existing processes will ensure that you continue removing pathways to escalation for attackers.

Furthermore, where possible, you should apply conditional access policies for your Entra Apps to avoid potential misuse.

External User and Collaboration Security

Microsoft 365 makes cross-tenant collaboration easy.

The Teams and SharePoint infrastructure ensures that you can easily communicate, work with, and share files with external guests and anonymous users.

However, this also opens up an attack vector that is increasingly being exploited.

Research from Mimecast has found that 94% of organizations are reporting attacks in these collaboration environments, and, of course, why wouldn't they?

Most people implicitly trust users in these cross-tenant spaces, making them a perfect target for cyber attacks.

Because of this, it is vital to implement some foundational policies for these spaces. (For example, you should ensure that Defender's advanced threat protection is properly configured to prevent phishing links from causing harm.) Another important area of concern is to ensure that you continuously discover guest, external, and anonymous users in your collaboration environments and respond appropriately.

Where external users are not active, they should be immediately removed, and where they are active in sensitive environments, alerts and remediations should be triggered.

Detect High-Risk Files and Sharing

Following on from the previous point, it is also important to identify sharing links that are blurring your tenant boundaries.

Files and pages being shared externally create a web of access between your tenant and other tenants or environments you have no control over.

Where possible, it is recommended that you apply strict controls on external sharing and, where it is required, set expiration dates.

Detect Suspicious Mailboxes

Finally, it is important to monitor your mailboxes for suspicious settings.

Cybercriminals sometimes set up mail forwarding and obscure mailbox-rules to ensure that they retain visibility of sensitive communications if they are kicked from the tenant.

It is highly recommended that you implement an ongoing review of your email environment to find mailboxes with auto-forwarding, disabled audit logging, sharing configurations, and mailboxes with unblocked credentials.

Level 4: Governance and Automation

OUTCOMES: CONTAIN ATTACK SURFACES AND ENABLE RAPID RESPONSE

By the time you come to Level 4, you have put layers of resilience into your tenant to slow attackers down to a crawl. The next step is to implement governance and automation to keep your attack surface lean and your response time fast.

Sprawl and Lifecycle Management

One of the consequences of adoption in Microsoft 365 is that, over time, you accrue more and more accounts and objects, massively expanding your attack surface and impinging on your ability for oversight and security.

A study from Gartner found that Microsoft's native capabilities available in their E5 license gives you only 33% of the capabilities required to combat sprawl.

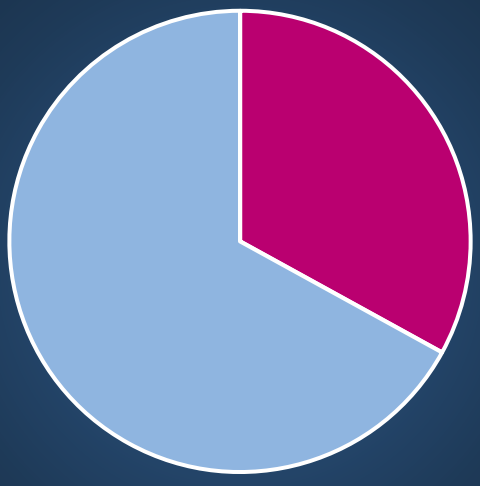
Since this research, Microsoft has added some additional capabilities, but these are locked away in higher-tiered packages like Entra ID P1 and P2.

The implication of this is that true sprawl and lifecycle management will require enhanced capabilities that go beyond the Microsoft 365 license. These include the ability to detect when users, Entra apps, objects, and licenses are no longer being used and the ability to correctly provision new users and rapidly deprovision and review user privileges throughout the lifecycle.

If you can deliver these capabilities, the combined impact will be huge on your total standing privileges and the attack surface available for cybercriminals to exploit.

Gartner Study Insight: Microsoft 365 E5 License Capabilities

Microsoft E5 license provides only **33%** of required capabilities to combat sprawl.



User Access Reviews

A major component of the previous section that deserves its own dedicated focus is access reviews. **Access reviews are designed to ensure that users and admins who are given access are periodically reviewed to determine whether they still need the permissions and privileges assigned to them.**

This process not only helps with compliance but also ensures that unused permissions and privileges are able to be removed by IT on an ongoing basis.

This is not an easy process without supporting technology. Entra ID Governance (available as part of the enhanced Entra ID P2 license) allows organizations to delegate access reviews to end users. For those who don't want to sign up for the whole package, software like CoreView has powerful access review capabilities without the baggage.

Enhanced Audit and Reporting

When responding to an attack—or recovering from one, there is nothing worse than not being able to find what you want.

Microsoft 365 has many incredible qualities. But its many configurations and management types being split across so many different interfaces is not one of them. For large, well-resourced IT teams, this will be a frustration that you could potentially overcome with the sheer volume of administrators. But for most businesses, this complexity has a real-world impact.

IT admins frequently highlight the constant updates to Microsoft 365's many interfaces as a big pain. It's one thing to try and remember the intricacies of 18+ admin UIs, it's another to constantly re-learn them due to ongoing updates.

UI complexity isn't just annoying, it significantly impacts your ability to respond during a crisis.

To ensure best practice recovery and response during an incident, it is recommended to create enhanced reporting, dashboards, and audit trails so that you can quickly triage and respond to events.

Access reviews are designed to ensure that users and admins who are given access are periodically reviewed to determine whether they still need the **permissions** and **privileges** assigned to them.

Secure Task Automation

One of the best ways to prevent misconfigurations and admin errors from occurring is to use task automation. When admins and helpdesk staff are overwhelmed with repetitive tasks, it is more likely that mistakes will occur, leading to gaps in your tenant that can be exploited.

Because of this, **it is highly recommended that you use task automation for repetitive tasks like user onboarding and offboarding.**

PowerShell is a go-to for many organizations. However, these highly privileged scripts can increase your attack surface when not carefully managed. And, due to ongoing updates and changes, scripts can sometimes break.

Using Power-Automate or other advanced task automation software like CoreView can ensure your admins avoid making mistakes while also offering a more mature solution than scripting.

Rapid Extensibility

Finally, one of the most underappreciated elements of responding to attacks is quickly being able to adapt your environment as threats change.

If your existing tool set doesn't give you the ability to quickly customise new reports and automations based on your requirements, your ability to adapt is slowed down.

Using PowerShell, Excel, and Power BI to try and create rigorous custom reports can sometimes take days or weeks of finetuning—plenty of time for cybercriminals to achieve what they want.

Having a platform that enables fast custom reporting and remediations means you are better equipped to stay in control when you are under pressure.

Key Resources for Enhancing Cyber Resilience

To enhance your organization's cyber resilience and effectively manage your Microsoft 365 environment, consider the following resources designed to help you strengthen your security posture and stay ahead of potential threats:

Admin Permissions Scanner for Microsoft 365

Identify accounts with excessive permissions and reduce exposure to minimize the risk of data breaches. See how →

Anatomy of a Microsoft 365 Attack

Stay updated on the latest attack tactics from cybercriminals to strengthen your organization's defenses against evolving threats. See how →

Building an Effective Cyber Resilience Strategy with CoreView

CoreView enables security best practices, governance automation, and compliance in Microsoft 365. See how →

About CoreView

CoreView is the Global Leader in Effortless Microsoft 365 Security, Governance, and Administration. Offering an end-to-end solution that stretches across the whole M365 ecosystem; from your tenant level configurations, right up to your most critical workloads.

Created by M365 experts, for M365 experts, CoreView makes best practice for M365 effortless by simplifying, unifying, and enhancing the M365 admin experience. CoreView empowers 1500 M365 organizations to turn the tide on endless tasks, deliver best practice security, and drive ROI.

[1] https://www.cisa.gov/resources-tools/services/bod-25-01-implementing-secure-practices-cloud-services-required-configurations

[2] https://www.vectra.ai/about/news/global-survey-finds-71-of-cloud-users-suffered-up-to-seven-malicious-account-takeovers-in-last-year

[3] https://news.sophos.com/en-us/2023/08/23/active-adversary-for-tech-leaders/

[4] https://csrc.nist.gov/glossary/term/cyber_resiliency

[5] https://www.gartner.com/document-reader/document/6091427?ref=lib

[6] https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023

[7] https://www.picussecurity.com/resource/report/red-report-2024

[8] https://attack.mitre.org/techniques/T1562/

[9] https://news.sophos.com/en-us/2023/08/23/active-adversary-for-tech-leaders/

[10] https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#section-master-oc526b

[11] https://learn.microsoft.com/en-us/entra/architecture/recover-from-misconfigurations