CoreView

2025 CoreView State of Microsoft 365 Security

A comprehensive analysis of 250+ IT and security leaders reveals the hidden gaps in your security

Table of contents

Organizations believing they have *'advanced'* security are experiencing the **same compromise rates** as those with **basic implementations**.

Executive summary: Finding your hidden security gaps

There's a growing disconnect between perceived security maturity and actual protection levels

60% of organizations rate their Microsoft 365 security as "established" or "advanced." Yet,

60%

of those same organizations have experienced account compromise attacks.

Our survey of over 250 IT and security leaders across enterprise and mid-market organizations reveals a startling disconnect between perceived security maturity and actual protection levels.

If you're responsible for Microsoft 365 security, this report contains findings that might keep you awake tonight.

Organizations with formal disaster recovery plans are

61% less likely

to experience significant operational **disruptions from misconfiguration**

The survey reveals six distinct pain points creating unprecedented risk exposure

The tenant dilemma

Everyone wants one tenant, but few can stomach the risks.

1

Too many Entra privileges

Global admin usage is down, but application privileges are exploding.

2

Backups – more than just data

Everyone has their data backed up, few will have a tenant to restore it in.

3

Excessive privilege

Few organizations are capable of removing excessive access.

4

Configuration tampering

No one is noticing configuration tampering, but then again, no one is looking.

5

Zero assurance in Zero Trust

Few can confirm that their Zero-Trust investments are working.

6

Microsoft 365 environments: Survey respondents' landscape

What organizations believe vs. what Microsoft 365 actually protects

Before diving into the biggest pain points and security threats organizations face, let's frame the discussion with a snapshot of the responding organizations, their survey responses and how their realities shape the M365 challenges they face.

Across the board, **survey results reveal that organizations appear to be blissfully unaware of exactly how much or little Microsoft protects them in crisis situations**, what can be done to mitigate the security oversights in the M365 ecosystem, and what solutions exist to build resilience and efficiency into their M365 environment. There also seems to be a significant disconnect between how advanced organizations perceive their security posture to be versus the reality.

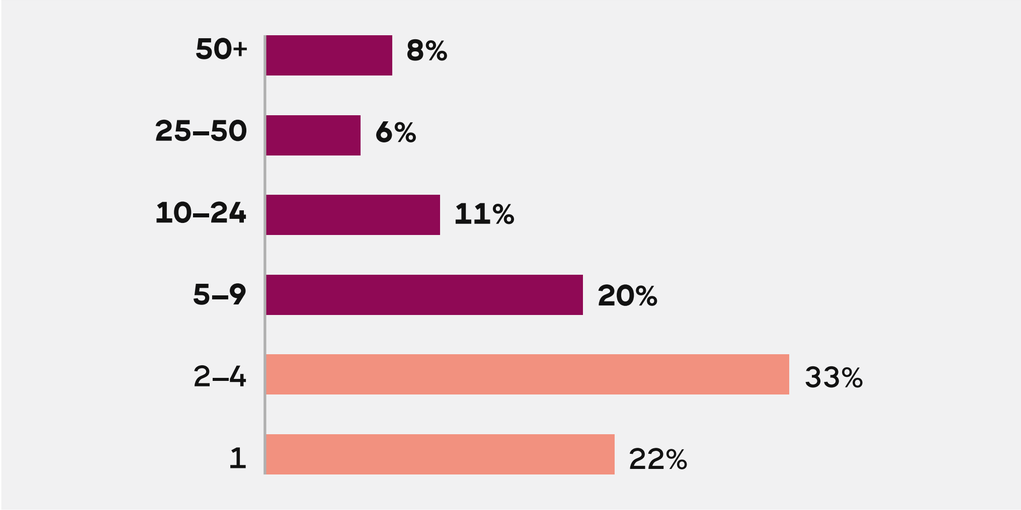
Some of the key results from the survey bring this disconnect to the surface.

49%

of organizations mistakenly believe Microsoft backs up their configurations — *but it doesn't.*

FIGURE 1

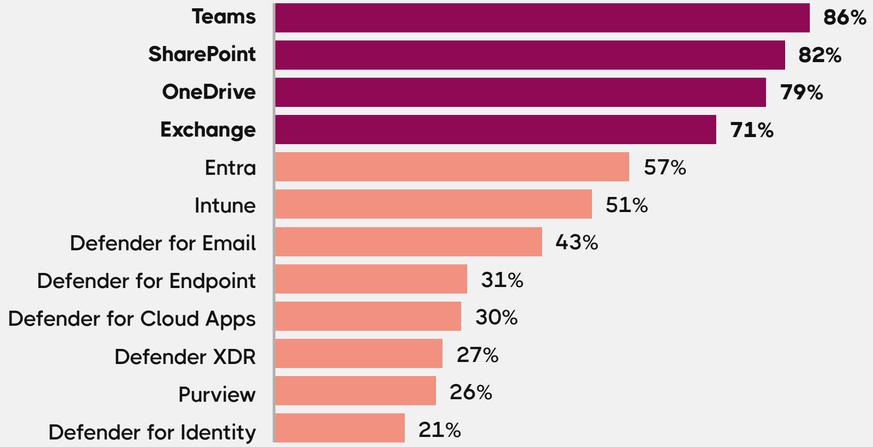
Responses to **"How many Microsoft tenants do you manage?"**



A majority of organizations manage multiple tenants — **78% operate more than one, and 45% manage more than five**. This complexity introduces greater risk and makes unified governance more difficult.

FIGURE 2

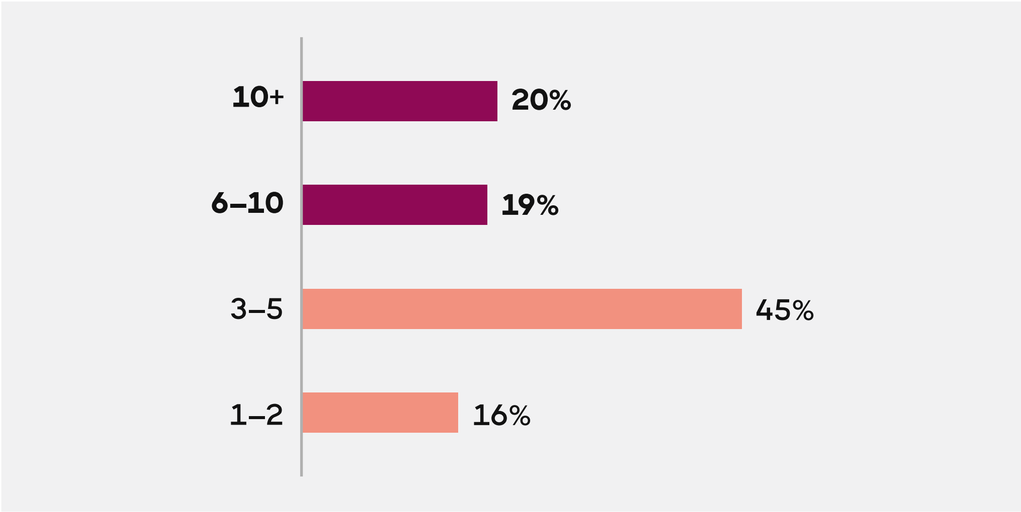
Responses to **"Which of the following Microsoft services are you using?"**



These tenants run diverse workloads. Over half run more than six services, i.e., software that runs continuously in the background. The three most common are **Microsoft Teams (86%)**, **SharePoint (82%)**, and **OneDrive (79%)**. **Exchange runs on 71%**. These four represent services that support the Microsoft 365 productivity ecosystem. The other services are more systemic in nature, e.g., Entra, Intune, Defender, and Purview, the latter two of which are for security.

FIGURE 3

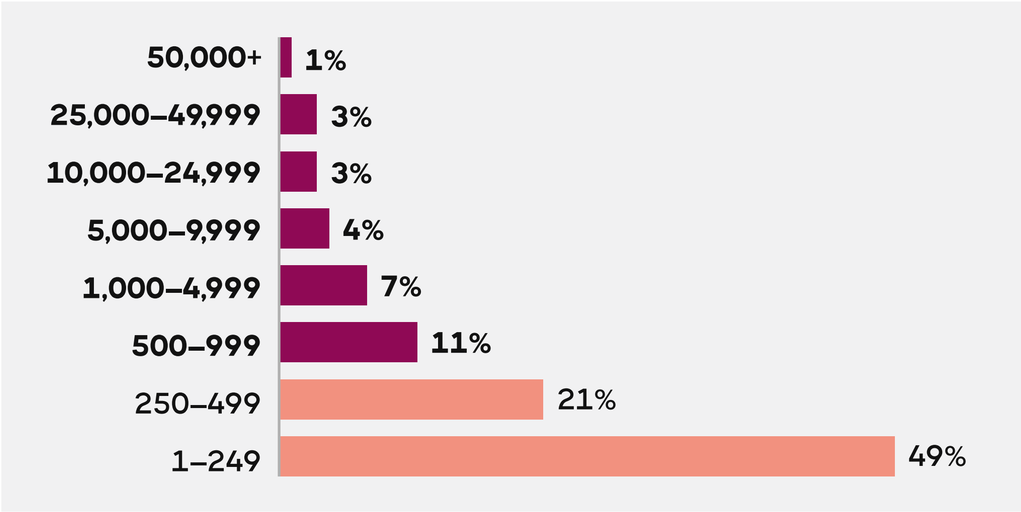
Responses to **"How many global admins do you have?"**



The global admin headcount remains relatively high, with **39% of organizations reporting more than six**. Microsoft recommends limiting the number of global admins to four or five at most to reduce risk.

FIGURE 4

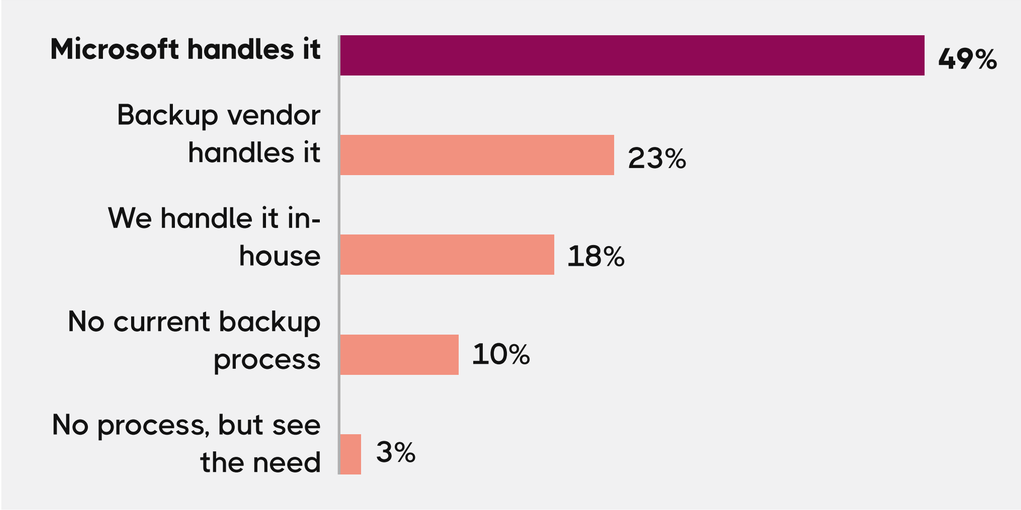
Responses to **"How many of your Entra or integrated apps use read-write permissions?"**



While global admin account numbers are down, the number of Entra apps with read-write permissions — another major risk — is higher than ever and still growing. **29% of organizations report having over 500 Entra apps with read-write access.** That's a red flag, as these apps can hold just as much power — and do just as much damage — as global admin accounts.

FIGURE 5

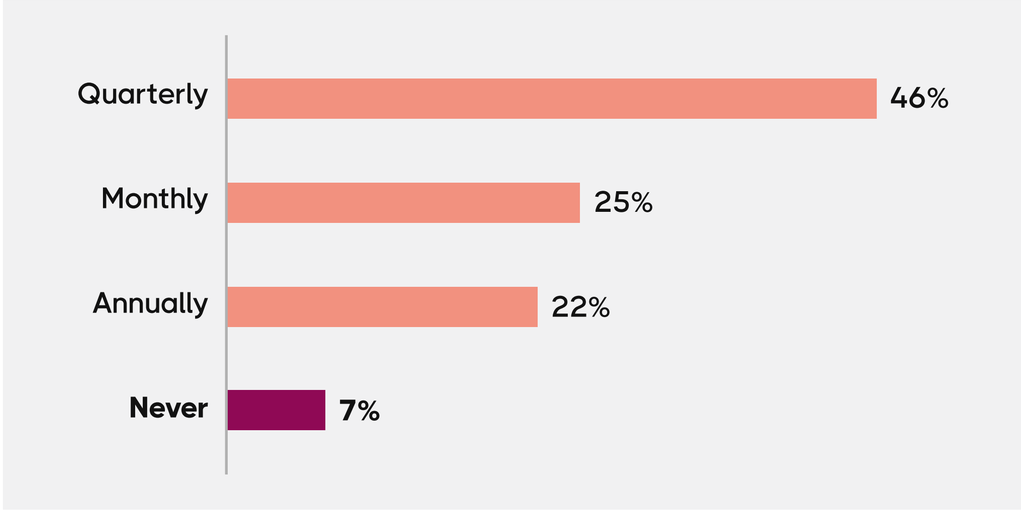
Responses to **"Do you have your Microsoft 365 configurations backed up?"**



Global organizations know the importance of backing up their data and report doing so assiduously. Yet, the same organizations suffer from the dangerous misconception that their tenant configurations are also backed up — which is, unfortunately, not the case. **Almost half of respondents believe Microsoft backs up configurations (they do not)**, and another near-quarter believe their data backup vendor does it (also not the case). This is a glaring blind spot and becomes a serious problem when organizations face a disaster recovery scenario.

FIGURE 6

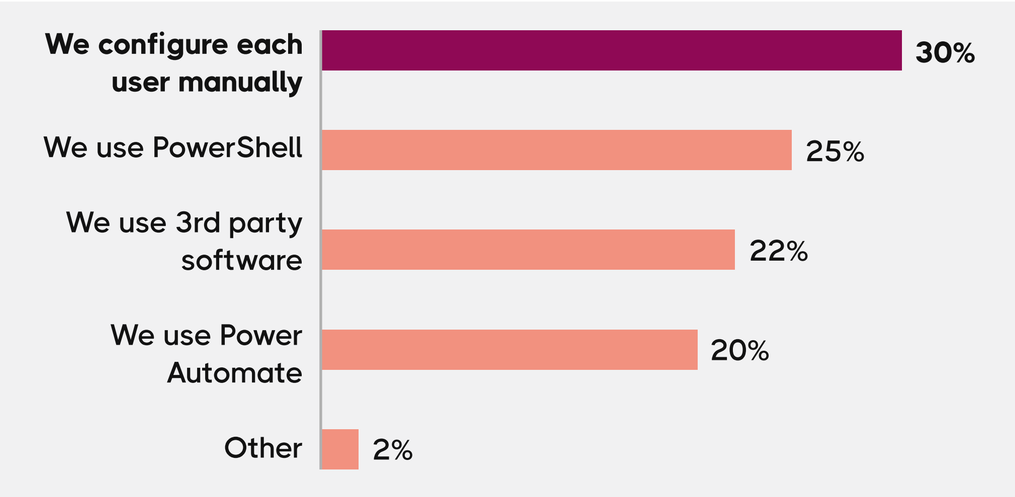
Responses to **"How often do you perform user access reviews?"**



Most organizations report performing user access reviews infrequently. Only 46% conduct them quarterly, while 25% do so monthly, and 22% annually. A concerning **7% never perform them at all**, creating significant risk exposure.

FIGURE 7

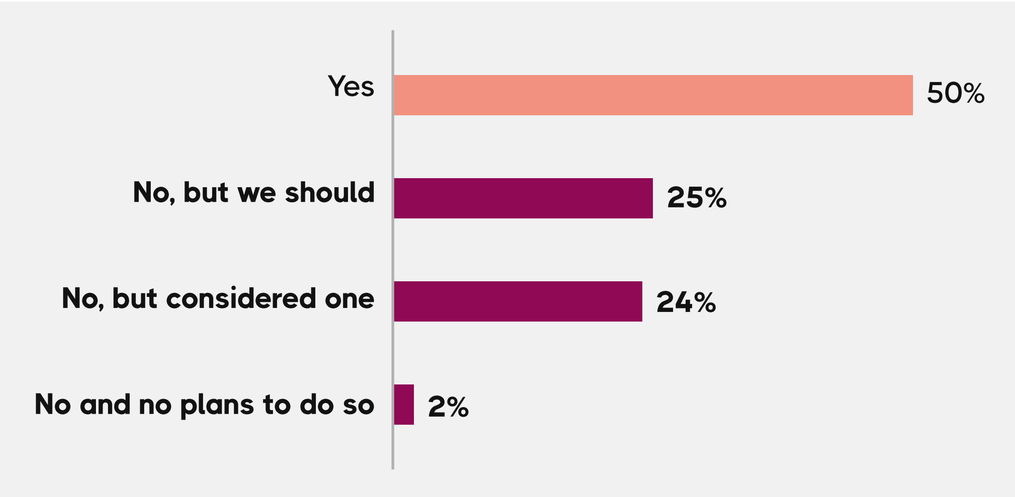
Responses to **"What is your process for onboarding and offboarding Microsoft 365 users?"**



Many organizations still rely on manual processes, with **30% configuring each user manually**. Only 20% use automation tools like Power Automate, while others use PowerShell (25%) or third-party tools (22%) — highlighting inefficiencies and risk during user lifecycle events.

FIGURE 8

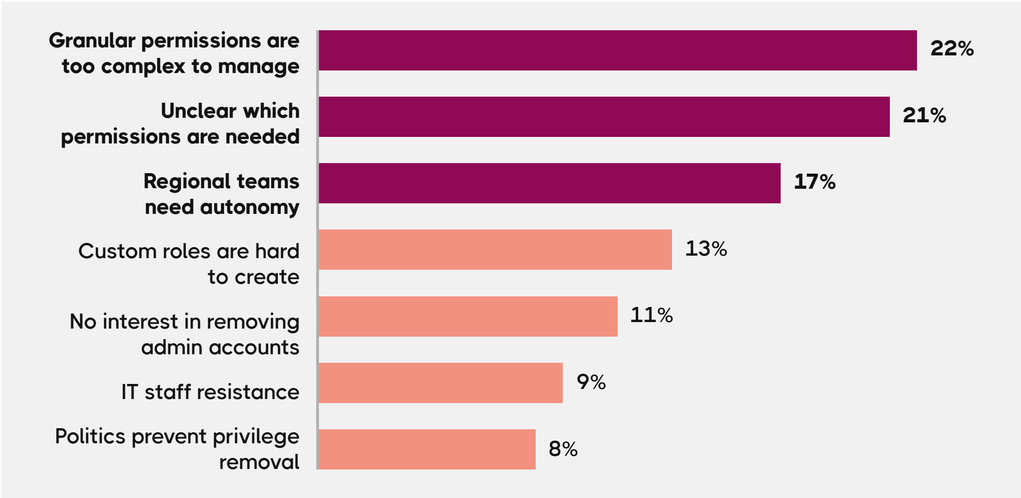
Responses to **"Do you have a privileged access management system deployed?"**



Only 50% of organizations have deployed a privileged access management (PAM) system. Another **25% say they should have one**, and **2% have no plans to deploy one** — leaving many exposed to unnecessary access risks.

FIGURE 9

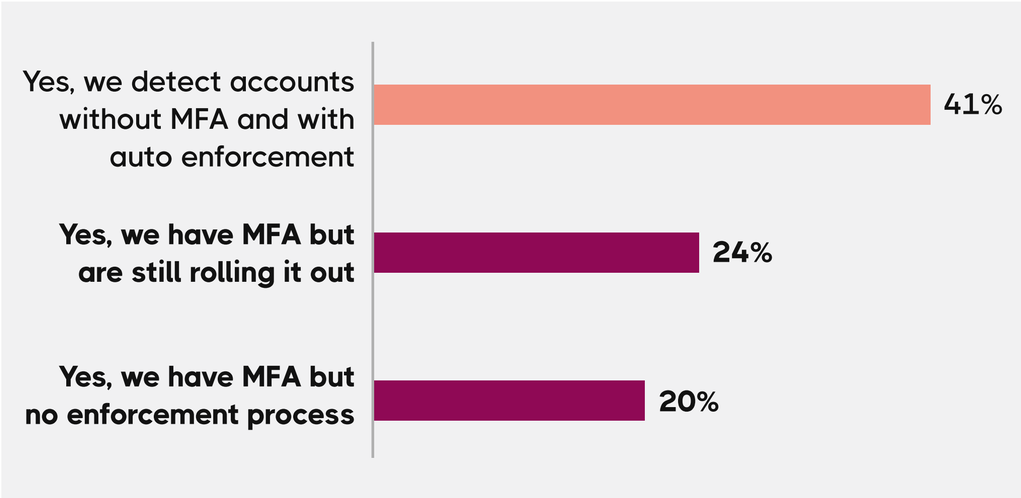
Responses to **"What's preventing you from reducing Microsoft 365 admin access?"**



The biggest barriers to managing and reducing privileged access are operational. The top challenges include the **overhead of managing granular permissions (22%)**, **uncertainty around which permissions are needed (21%)**, and **the need for regional team autonomy (17%)**.

FIGURE 10

Responses to **"Do you have MFA/Zero Trust implemented for Microsoft 365 user and admin access?"**



Identity and access management — complex as it is — reveals its most obvious gap through a general lack of multifactor authentication (MFA) enforcement across surveyed organizations. While over 90% have implemented some form of MFA, only 41% have automated detection and enforcement. **20% have MFA but no enforcement process**, and **24% are still rolling it out**. Another **9.7% have no MFA at all**.

Given this data, the confidence organizations express in their security maturity is difficult to justify

The Microsoft 365 attack surface is wide and unpredictable. Risks can come from any direction—whether it's the complexity of managing multiple tenants, the explosion of Entra apps with broad permissions, or inconsistent enforcement of security controls like MFA. These issues are often worsened by limited visibility, manual oversight, and a lack of cohesive governance.

Even small missteps—like an unmonitored configuration change or an overlooked admin role—can quietly introduce serious vulnerabilities. And without the right tools and processes in place, organizations may not even know these risks exist until it's too late.

Let's take a deeper look at six key threats based on these survey findings.

29%

of organizations have over 500 Entra apps with read-write permissions — as powerful and risky as global admin rights.

Six key threats to your Microsoft 365 environment

The tenant dilemma:

Everyone wants one tenant, but few can stomach the risks

78% **of organizations manage multiple Microsoft 365 tenants—a complexity nightmare that's crushing IT teams.**

Many valid reasons exist for maintaining multi-tenant architectures. It's often a strategic choice—not a technical limitation. **Organizational**, **geographic**, and **security factors** frequently drive the separation, such as:

Organizational structure alignment	Separate business units or subsidiaries often maintain their own tenants to preserve operational autonomy **(47%)**
Geographical and jurisdictional requirements	**35%** of multi-tenant organizations cite data sovereignty and compliance with regional regulations as a driver
Merger and acquisition history	Previously independent organizations bring their existing Microsoft 365 environments, creating multi-tenant landscapes
Security isolation	**34.8%** of multi-tenant organizations maintain separate tenants to enforce separation of duties and least privilege principles

Regardless of alignment, multi-tenant management brings complexity and risk—often beyond what organizations are prepared for. **Key technical and business challenges include:**

Operational overhead

71% cite increased management burden as the primary challenge.

Excessive costs

60% report higher licensing and administrative expenses.

Inconsistent configurations

60% struggle to maintain uniform security settings across tenants.

Identity management complexity

55% face difficulties with user authentication and access control.

Data silos

48% report challenges sharing information across tenant boundaries.

Why organizations can't consolidate

Until recently, using multiple tenants was the only way to enforce least privilege and separation in Microsoft 365. Organizations with complex needs—like data separation or residency—adopted this model by necessity.

Today, many consider consolidation to regain control, but the complexities involved are daunting. In the end, the choice often reflects what organizations think is possible—not what actually suits their business. Most don't want to manage multiple tenants—they just don't realize they have a choice.

The mathematics of complexity

Organizations with 10 or more tenants are 2.3 times more likely to report significant operational overhead than those with just 2–4. Each tenant adds its own configurations, licensing costs, admin burden, cross-tenant access risks, and contributes to identity and privilege sprawl.

79%

of IT leaders found segregation problems to be a roadblock to operating a single tenant, but the costs and risks led most organizations to at least consider merging tenants.

Too many Entra privileges:

Global admin usage down, application privileges exploding

The good news

Organizations are getting global admin proliferation under control. Just **20% report having 10+ global admins**, with **61% maintaining five or fewer**—close to Microsoft's best-practice recommendation of "fewer than five" total.

The dangerous trend

While global admin counts are down, a new risk is rising: 51% of organizations have 250+ Entra apps with read-write permissions—and 18% report over 1,000. Even among those limiting global admins to five or fewer, 43% still allow 250+ apps with these powerful permissions.

Yet most organizations lack strong oversight: **16% have no process at all**, **33% rely on manual reviews**, and only a minority use built-in **(29%)** or third-party **(22%)** tools to manage app permissions.

The permissions you dread

The fragmented approach to managing app permissions creates a perfect security storm. With just a few read-write permissions, an Entra app quickly becomes as powerful as a global administrator. These represent thousands of privileged access points direct into your tenant—creating massive attack surface expansion.

51%

of organizations report having 250+ Entra applications with read-write permissions.

Backups – more than just data:

Everyone has their data backed up, few will have a tenant to restore it in

The backup blind spot

If your Microsoft 365 tenant configurations were compromised tomorrow, how would you restore them?

While **96%** say their data is backed up or will be soon, many overlook configuration backup entirely:

47%
rely on Microsoft's built-in tools **(which back up data—not configurations)**

25%
use third-party backup vendors

18%
manually back up configurations or rely on documentation

10%
have no clear strategy at all

Configurations matter

This reveals a critical misunderstanding—configurations are vital to reliability, performance, and security, but most organizations lack proper safeguards.

49%

of survey respondents incorrectly believe Microsoft fully backs up tenant configurations and will restore them after an incident. *This is categorically false.*

Misconfiguration is a hidden risk

Configuration management is inconsistent, with many organizations lacking a clear approach to managing critical Microsoft 365 settings.

36%
follow best practices with dev/test/prod tenants

27%
say this is too much internal effort

22%
make changes directly in production

16%
have no process at all

In total, **65%** of organizations are managing Microsoft 365 configurations without following best practices—leaving them exposed to avoidable risk and operational disruption.

Lost configuration, lost control

Even more concerning, tenant configurations span critical areas like user access, compliance, and app settings. If configurations are lost without a backup, recovering them isn't just tedious—it can lead to downtime, operational disruption, and serious security exposure.

The business impact

Organizations with formal disaster recovery plans are **58% less likely to experience significant operational disruptions from misconfigurations**. And with formal change control processes in place, they see **72% fewer security incidents** tied to misconfigurations.

Without configuration backup, you might restore your data—but won't have a tenant to restore it to.

72%

fewer security incidents are reported by organizations that implement formal change control processes for configuration management.

Excessive privilege:

Few are capable of removing excessive access

Attack surface mathematics

Organizations with **10 or more global admin accounts** are **3.8x more likely** to experience frequent account compromise incidents than those with fewer admins.

Current global admin distribution:

45%
have 3–5 global admin accounts

19%
have 6–9 accounts

20%
have 10+ accounts **(high risk)**

16%
limit access to 1–2 accounts **(Microsoft recommended)**

Mind the PAM gap

Organizations that deploy privileged access management (PAM) solutions experience **64% fewer security incidents** related to admin account misuse.

Current PAM adoption status:

50%
have PAM deployed **(reduced risk)**

24%
are considering implementation

25%
acknowledge they should implement PAM

2%
have no plans to implement **(high risk)**

The Microsoft reality check

Microsoft recently reported that **63% of tenants** fail to implement least privilege. Our survey shows that **89% of IT leaders** want to remove admin accounts—but can't, largely due to Microsoft's complexity. Deep-rooted issues like poor user lifecycle processes, security immaturity, and internal resistance all contribute to the challenge.

Microsoft complicates least privilege

Microsoft 365 was never designed with least privilege in mind. A single admin role can impact the entire tenant—like a SharePoint admin managing settings across all sites. Administrative Units offer limited segmentation, mostly in Entra and Teams, while core services like Exchange and Intune remain exposed.

That's why **79%** of respondents say lack of segregation is the biggest barrier to tenant consolidation. A more granular approach to access control could reduce risk, streamline lifecycle management, and enable unification.

What's blocking PAM adoption

Organizations that deploy PAM solutions experience **64% fewer security incidents** tied to admin account misuse. Yet major barriers remain:

62% cite complexity and overhead

25% – administrative overhead

23% – unclear permission requirements

14% – difficulty creating custom roles

38% cite autonomy concerns and resistance

19% – regional teams need access and autonomy

10% – faced resistance from IT staff to removing accounts

9% – political issues prevent the removal of accounts

63%

of tenants fail to implement least privilege effectively.

The ROI of privileged access management is clear. Organizations with PAM in place experience **64% fewer security incidents** related to admin misuse. Automating user lifecycle management further reduces incidents by **68%**, while conducting monthly access reviews (instead of annual) cuts account compromise rates by **57%**. And those using dedicated access tools are **2.7x more likely** to perform these reviews regularly—maximizing both security and operational efficiency.

Configuration tampering:

No one is noticing configuration tampering, but then no one is looking

The invisible problem

Microsoft's Digital Defense Report 2024 documented **176,000 instances of configuration tampering** in May 2024 alone. Independent analyses show a **79% increase** in configuration tampering since 2023.

The detection disconnect

Despite this surge, **48% of survey respondents** claim little to no configuration tampering in their environments. The gap is clear: *you can't detect what you're not monitoring.*

79%

increase in configuration tampering incidents since 2023.

The monitoring reality

Only **45%** of organizations use tools to detect configuration tampering:

32%
rely solely on Microsoft's built-in tools

22%
use third-party monitoring solutions

26%
combine both

20%
report limited or no ability to detect changes

Why this matters

Organizations using **third-party monitoring tools** are **2.1x more likely** to detect security setting tampering compared to those relying solely on Microsoft's built-in capabilities. That difference matters. These attacks are rarely loud or obvious—often involving quiet changes to DLP policies, loosening cross-tenant access, or selectively disabling audit logs.

Silent changes, serious risk

These actions might appear harmless at first, but they open the door to persistent, hard-to-detect threats. Once attackers establish a foothold by modifying these controls, they can maintain prolonged access, avoid detection, and exfiltrate sensitive data without triggering alarms.

What makes this even more dangerous is the false sense of security many organizations have. Without proactive, purpose-built monitoring in place, these threats fly under the radar—silently degrading security posture over time.

The 10,000 configuration challenge

Microsoft 365 spans **more than 10,000 individual configuration elements** across critical services like Entra, Defender, Intune, Purview, Exchange, and others. These configurations define how users are authenticated, how data is protected, how apps behave, and how security policies are enforced across the tenant.

Many organizations lack the visibility and tools to track changes across Microsoft 365's vast configuration surface. This creates thousands of blind spots—each a potential vulnerability. Manual reviews are unrealistic and unsustainable in today's fast-changing environments.

Too much to manage manually

Without automation and alerting in place, teams are forced into reactive mode, often discovering misconfigurations only after an incident occurs. That's why configuration oversight is no longer a "nice to have"—it's a foundational pillar of security, compliance, and resilience in the Microsoft cloud.

48%

of organizations report little to no configuration tampering — highlighting a major detection gap.

Zero assurance in Zero Trust:

Few can confirm their investments are working

The attack reality

68% of organizations report that attackers attempt to access Microsoft 365 **weekly, daily, or constantly**. It's no surprise—M365 contains crown jewels:

Entra
controls cloud access

SharePoint & OneDrive
hold sensitive data

Exchange & Teams
manage all communication

The MFA implementation paradox

While **90%** have implemented MFA in some form, only **41%** have automated detection and enforcement—leaving **59% without real assurance**.

The Microsoft math

Microsoft reports that **99.9% of account compromises** happen on accounts without MFA. That means organizations could prevent **999 out of every 1,000 attacks**—but most aren't realizing this benefit.

59% **of organizations lack automated MFA enforcement—leaving them without real assurance that MFA is working.**

The effectiveness gap

Organizations with **automated MFA detection and enforcement** experience **53% fewer account compromise incidents** compared to those with only partial implementation.

More concerning: environments with MFA but no enforcement process experience compromise rates nearly identical to those without MFA. The highest rate of account compromises—**58.3%**—occurs in environments still struggling with MFA adoption.

This underscores a dangerous false sense of security—**having MFA is not the same as enforcing it**. Without automation, many organizations mistakenly assume they're protected while remaining highly vulnerable to targeted attacks.

The detailed breakdown

Despite widespread MFA adoption, maturity levels vary significantly—and only a minority have enforcement fully in place:

41%

MFA with automated enforcement **(optimal)**

21%

Still rolling out MFA

5%

Struggling with user adoption

10%

No MFA at all

These numbers reveal a critical gap between implementation and effectiveness. Without enforcement, MFA offers little real protection—leaving the majority of environments exposed despite appearing secure on paper.

58%

of account compromises occur in environments still struggling with MFA adoption—highlighting the critical gap between implementation and effective protection.

Other factors to take into account

Excessive app permissions widen the potential attack surface

The extensive ecosystem of integrated applications represents a rapidly expanding attack surface that most organizations cannot properly govern.

The scale of risk

18%
manage over 1,000 Entra apps with permissions

25%
manage 100–999 apps

36%
manage 10–99 apps

21%
manage fewer than 10 apps

No matter the size, every organization must prioritize visibility and control over their app ecosystem.

Read-write sprawl

12%
report over 1,000 apps with read-write Entra permissions

19%
report 100–999 apps with read-write permissions

42%
report 10–99 apps with read-write permissions

27%
report fewer than 10 apps with read-write permissions

Read-write access poses a significant risk and must be continuously monitored and governed.

The governance crisis

App permission management approaches reveal dangerous gaps:

16%

have no process for detecting and securing apps with powerful permissions

33%

rely on manual periodic reviews **(prone to human error)**

29%

use Microsoft's built-in tools for monitoring

22%

employ third-party tools for comprehensive monitoring

The business risk

Organizations without formal app permission management are **3.2x more likely** to experience security incidents related to third-party app integrations.

In **12%** of environments, over 1,000 apps have read-write access—yet only **22%** use third-party tools to monitor them. Most rely on manual reviews or Microsoft's native tools, which can't keep pace with the scale or complexity.

Without proactive oversight, excessive permissions become a gateway for data leaks, privilege abuse, and persistent threats.

Visibility isn't optional—it's essential for protecting your environment.

3.2x

more likely to experience security incidents—organizations without formal app permission management face heightened risk from third-party integrations, excessive permissions, and limited visibility.

Configuration management as hidden vulnerability

Configuration management represents the most critical gap in organizational security maturity, and for many organizations, it is invisible or impossible to govern.

The problem scale

44% of organizations experience security or operational issues due to misconfigurations at least "sometimes," yet most lack systematic governance approaches.

72%

fewer security incidents—formal change control turns misconfiguration risk into a manageable, governed process.

Configuration change maturity distribution

Approaches to managing configuration changes vary widely—and the level of maturity directly impacts risk exposure. Here's how organizations are currently approaching it:

No formal process

13% **(extremely high risk)**

Manual documentation and communication

28% **(high risk, error-prone)**

Ticketing system tracking

42% **(moderate risk, reactive)**

Formal change control with approvals

18% **(best practice)**

The ROI of configuration governance

Organizations with formal change control processes experience **72% fewer security incidents related to misconfigurations**. They're also **58% less likely** to suffer significant disruptions from Microsoft 365 updates—reducing both risk exposure and operational downtime.

Beyond reducing incidents, formal governance helps IT teams proactively plan for platform changes, improve collaboration across teams, and maintain compliance with internal and external standards.

By shifting from reactive to proactive configuration management, organizations can increase uptime, reduce costs tied to manual remediation, and boost confidence in their overall security posture.

Microsoft update impact

Unexpected Microsoft 365 updates cause operational disruptions:

3%
report issues "Very frequently"

9%
experience problems "Often"

39%
face issues "Sometimes"

41%
report "Rare" issues

9%
claim never experiencing significant issues

13%

of organizations have no formal configuration process—leaving them extremely vulnerable to misconfigurations and outages.

User lifecycle management and access risk

User lifecycle management maturity varies dramatically across organizations, creating persistent security risks.

Process maturity levels

29%

configure users manually **(high risk)**

36%

use basic automation tools **(moderate risk)**

26%

have implemented workflow automation **(good)**

9%

have fully automated user lifecycle management **(optimal)**

The security impact

Organizations with **fully automated user lifecycle management** experience **68% fewer security incidents related to lingering access rights**.

By streamlining provisioning and deprovisioning, automation reduces human error, eliminates delays, and ensures consistent access control across systems. This significantly lowers the risk of orphaned accounts, privilege creep, and unauthorized access.

68% **fewer security incidents—automated lifecycle management reduces lingering access risks.**

Access review frequency

47%
perform quarterly user access reviews

25%
perform monthly reviews **(optimal)**

22%
perform annual reviews **(insufficient)**

7%
never perform access reviews **(extremely high risk)**

The monthly review advantage

Organizations performing monthly access reviews experience **57% fewer** account compromise incidents compared to those performing annual reviews.

Access review barriers

32%
struggle with resource constraints

27%
face difficulty getting responses from staff

25%
lack adequate tooling for efficient reviews

17%
cite complexity of their access model

Organizations with dedicated access management tools are **2.7x more likely** to perform monthly access reviews.

47%

of organizations still rely on quarterly or less frequent access reviews—leaving extended access risks unchecked.

Industry and organizational size impact

Security maturity differs by industry and organization size—driven by complexity and varying levels of threat exposure.

Enterprise vs. mid-market security maturity

Enterprise organizations **(10,000+ employees)** show higher baseline security but face complexity penalties.

Enterprise advantages

28%

rate security as "Advanced"
(vs. 11% mid-market)

91%

have implemented MFA
(vs. 87% mid-market)

72%

have privileged access management
(vs. 43% mid-market)

Enterprise complexity challenges

38%

manage 10+ tenants **(vs. 11% mid-market)**

18%

have 10+ global admin accounts
(vs. 17% mid-market)

Enterprises face significantly higher operational overhead due to managing complex multi-tenant environments.

Strength meets complexity

Enterprises benefit from stronger security foundations, but that advantage is often offset by the operational complexity of managing large-scale, multi-tenant environments.

Industry-specific risk profiles

Financial services and healthcare show high maturity—paired with high threat exposure.

23% **(Financial services)**
rate their security as "advanced"
(vs. 15% average)

70% **(Financial services)**
have privileged access management deployed

23% **(Financial services)**
experience account compromise rates above average

15% **(Healthcare)**
experience account compromise rates above average

Manufacturing and education

Manufacturing and education show low security maturity, leaving them more exposed to configuration-based attacks.

7% **(Manufacturing)**
rate their security as "advanced"

6% **(Education)**
rate their security as "advanced"

39% **(Manufacturing)**
report automated MFA enforcement
(below the 41% average)

Both industries face heightened vulnerability due to limited maturity and slow adoption of foundational security practices.

72%

of enterprises have privileged access management—compared to just 43% of mid-market organizations—highlighting a major gap in protection for smaller environments.

Governance and compliance as a strategic imperative

Governance and compliance have become core priorities as organizations look to reduce risk, control sprawl, and meet rising regulatory demands.

Sprawl management priorities

Organizations identify key drivers for Microsoft 365 governance:

51%
need to keep attack surface lean

47%
aim to reduce security overhead

46%
seek to remove dangerous access points

46%
want to reduce management overhead

39%
focus on productivity improvements

41%
want to drive down storage costs

Compliance driver variations

Industry-specific regulations significantly impact governance approaches:

Financial services organizations
2.3x more likely to prioritize access control governance

Healthcare organizations
1.8x more likely to focus on data classification

Technology companies
1.5x more likely to prioritize automation

Organizations prioritize Microsoft 365 governance to reduce risk, cut overhead, and improve productivity. Compliance needs vary—financial services focus on access control, healthcare on data classification, and tech on automation.

Enterprise governance integration

Current state of Microsoft 365 governance:

23%
have fully integrated Microsoft 365 into enterprise governance frameworks

38%
have partial integration

31%
maintain separate governance processes

7%
lack formal governance entirely

Why it matters

Organizations with integrated frameworks experience **53% fewer** security and compliance incidents compared to those with siloed or absent governance. Integration ensures alignment across teams, streamlines auditing processes, and enables faster, more coordinated responses to threats and regulatory changes.

However, achieving full integration isn't without challenges. Many organizations struggle with legacy systems and inconsistent governance models. Limited executive buy-in, lack of unified tooling across platforms, and resistance to change—especially in decentralized IT environments—often stall progress and prevent organizations from realizing the full benefits of enterprise-wide governance.

Fully integrating Microsoft 365 governance drives consistency, reduces risk, and improves agility across your digital environment.

53%

fewer security and compliance incidents—organizations with integrated Microsoft 365 governance dramatically reduce risk exposure.

Cost pressures and resource strain on security efforts

Cost pressures, skills gaps, and training challenges continue to limit organizations' ability to secure Microsoft 365 effectively.

Budget impact on security

Cost efficiency concerns significantly influence security decision-making. Many organizations are actively seeking ways to reduce Microsoft 365 licensing costs, and in doing so, are closely tying cost optimization to security requirements.

As costs continue to rise, several organizations report growing concern, with budget constraints often forcing difficult trade-offs that affect security readiness.

Training challenges and user adoption barriers

Organizations continue to struggle with training staff on complex security features. The rapid pace of change in Microsoft 365 and ongoing interface complexity make adoption difficult. Many teams emphasize the need for better, more accessible training resources to support secure implementation.

Skills gap crisis

A lack of dedicated Azure, Microsoft 365, and Entra experts poses a major challenge for many teams. Hiring freezes further complicate the situation by preventing organizations from acquiring the necessary security expertise.

As a result, teams often admit they "stumble along as best we can" and rely heavily on tools to identify potential gaps. On top of that, the complexity of user interfaces and the constant evolution of the platform make it even harder for staff to keep up.

60%

of multi-tenant organizations report excessive licensing costs.

Perception gaps and the cost of inaction

Many organizations overestimate their security maturity—creating blind spots that lead to underinvestment, operational risk, and costly consequences.

Self-assessment distribution

Organizations were asked to self-assess their security maturity, revealing a wide range of perceived readiness levels.

Advanced - 15%

Comprehensive controls with continuous improvement

Established - 50%

Well-defined controls with regular reviews

Developing - 32%

Basic controls with some gaps

Initial - 3%

Minimal controls

The most concerning finding is the massive disconnect between self-assessed security maturity and actual practices.

The reality check

Despite high self-assessments, many organizations fall short in practice. **30% of those rating themselves as "advanced" or "established"** still report account compromises each year. **45% experience security issues caused by misconfigurations**, and **9% of organizations labeled as "advanced" don't have privileged access management in place**.

This perception gap creates dangerous blind spots that can lead to underinvestment in security due to an inflated sense of maturity.

30%

of 'secure' organizations still suffer account compromises.

Immediate financial impact

The financial cost of inaction is steep. Multi-tenant organizations face a **2.3x increase in administrative burden**, and **60% report excessive licensing costs**—both of which add ongoing strain to IT teams.

Even more critically, **account compromises cost an average of $4.45 million per incident** (IBM, 2023), highlighting the real financial risk of weak or misaligned security strategies.

Hidden business costs

Beyond the visible financial toll, organizations face deeper operational risks. Misconfigurations cause recurring disruptions that slow down essential processes and consume valuable resources. Inconsistent multi-tenant setups complicate audits and increase the likelihood of compliance failures.

The absence of reliable configuration backups puts business continuity in jeopardy. And with every security incident, trust among customers and stakeholders erodes—damaging reputation, relationships, and long-term growth potential.

The path forward

Many organizations overestimate their security maturity, creating blind spots that lead to risk, inefficiency, and rising costs. Closing the gap between perception and reality—with stronger governance, visibility, and accountability—is essential for reducing exposure and building long-term security resilience.

60%

of multi-tenant organizations report excessive licensing costs—highlighting the financial strain that comes with fragmented environments.

Critical actions for IT leaders

Based on these findings, **IT leaders should immediately** assess their organizations across these dimensions:

Adopt a unified multi-tenant governance framework

a. Establish consistent security baselines across all tenants

b. Implement centralized monitoring and management tools

c. Develop cross-tenant governance policies and processes

d. Consider tenant consolidation where appropriate

e. Maintain comprehensive documentation of tenant architectures and inter-relationship

Secure the application integration ecosystem

a. Implement comprehensive monitoring for app permissions

b. Regularly audit and review third-party app integrations

c. Enforce least privilege principles for integrated applications

d. Develop formal approval processes for new application integrations

e. Implement lifecycle management for integrated applications

Implement configuration management as a first-class security control

a. Establish formal change control processes for Microsoft 365 configurations

b. Implement independent backup of configurations beyond Microsoft's built-in capabilities

c. Deploy monitoring tools to detect unauthorized configuration changes

d. Conduct regular configuration audits against security baselines

Strengthen identity security beyond basic MFA

a. Implement automated MFA detection and enforcement

b. Deploy privileged access management solutions

c. Reduce the number of global admin accounts

d. Implement risk-based authentication

e. Conduct regular access reviews, particularly for privileged accounts

Automate user lifecycle management

a. Implement automated onboarding and offboarding workflows

b. Integrate Microsoft 365 identity management with HR systems

c. Implement regular attestation processes for access rights

d. Develop role-based access models with clear ownership

e. Monitor for orphaned accounts and excessive permissions

Conclusion:
Bring your security perceptions in line with your security reality

Bring your security perceptions in line with security reality

When "advanced" security isn't enough

Microsoft 365 security has reached a critical inflection point. While organizations have invested heavily in cloud security, fundamental architectural and operational challenges are introducing new categories of risk—ones that traditional approaches are not designed to address.

The data reveals a stark reality: **organizations that believe they have "advanced" security are experiencing compromise rates nearly identical to those with only basic implementations**. This perception gap isn't just a matter of measurement—it reflects a deeper misunderstanding of where real risks lie in today's Microsoft 365 environments.

The mathematical reality

The data is clear: **999 out of 1,000 account attacks could be prevented with proper MFA**. Organizations that implement **formal change control processes** experience **72% fewer configuration-related incidents**, while privileged access management reduces admin-related incidents by **64%**.

Meanwhile, automated configuration monitoring improves tampering detection rates by **2.1x**—proving that strategic, technical controls can drastically improve security outcomes.

These figures highlight a clear truth: real security gains come from operational discipline, not just tools. Organizations that invest in structured processes like access governance and automation experience fewer incidents and faster response times.

The complexity challenge

Microsoft 365's architectural limitations continue to force organizations into difficult trade-offs between security and operational efficiency. The **79% of organizations** that cite segregation issues as barriers to tenant consolidation aren't making poor decisions—they're reacting rationally to structural platform limitations that require careful navigation.

These limitations don't just complicate architecture—they also slow down incident response, fragment policy enforcement, and increase administrative overhead.

Without unified visibility and control, security teams are left stitching together siloed data and struggling to enforce consistent policies across environments. The result is an operating model that's reactive, inefficient, and vulnerable to misconfiguration and oversight.

The urgency

With **68% of organizations under constant attack** and Microsoft detecting **176,000 instances of configuration tampering each month**, the window for addressing these systemic vulnerabilities is rapidly closing.

Organizations that act now—by implementing structured approaches to configuration governance, privilege management, and multi-tenant security—will build long-term competitive advantages. Those that cling to traditional approaches risk becoming the next breach headline.

The choice is stark: **invest in systematic solutions today, or be forced to explain tomorrow why "advanced" wasn't enough**.

Want to take these stats to the next level? Contact us.

64%

reduction in admin-related incidents with proper privileged access management—proving that targeted controls can significantly reduce one of the most critical risk areas in Microsoft 365.

Appendix:
About the survey

Overview

This report is based on a comprehensive survey of 269 IT and security professionals responsible for Microsoft 365 environments, conducted in April-May 2025. The survey captured responses from senior decision-makers across diverse industries and organization sizes, providing a representative view of current Microsoft 365 security practices and challenges.

Respondent roles

- IT Directors: 32% (87 respondents)
- Security/Compliance Directors: 17% (45 respondents)
- IT Managers: 17% (45 respondents)
- VP/SVP level: 15% (40 respondents)
- CIOs: 10% (26 respondents)
- Other technical roles: 10% (27 respondents)

Organization size:

- Mid-market (1,000-9,999 employees): 65% (175 respondents)
- Enterprise (10,000+ employees): 33% (89 respondents)
- Small (under 1,000 employees): 2% (5 respondents)

Industry distribution:

- Technology/Software: 19% (50 respondents)
- Healthcare: 18% (49 respondents)
- Finance/Banking: 16% (44 respondents)
- Manufacturing: 15% (41 respondents)
- SLED (State, Local, Education): 12% (33 respondents)
- Other industries: 19% (52 respondents)

CoreView

Want to take these stats to the next level?

Contact us →

www.coreview.com


CoreView