CoreView

Recovering Data Is Easy — **Recovering Microsoft 365 Configurations Isn't.**

Executive Guide to M365 Tenant Configuration Recovery

Table of Contents

Introduction: The Invisible Threat Lurking in Every Microsoft 365 Tenant

If your Microsoft 365 tenant goes down, your business goes down.

In 2010, Office 365 was a fairly simple suite of office apps with email added on, but in 2025, Microsoft 365 is a different animal.

Services like Entra, Intune, Exchange, Defender, Teams, and SharePoint have thousands of configuration details that keep your business running – and running securely. If these are accidentally deleted, lost, or purposefully changed, your business can stop functioning. It's more than just data – tenant configurations are the entire blueprint for how your M365 environment operates.

> This is why it is mission critical to not only backup the data in your tenant, but also the configurations that enable your M365 tenant to operate securely.

Despite this, a widespread and dangerous misconception exists: that Microsoft's native backup solutions provide comprehensive protection for critical tenant configurations, settings, and policies.

This paper highlights the stark reality — **Microsoft does not back up or restore your tenant configurations**; this is your responsibility. As a result, businesses are exposed to a significant and frequently invisible cyber resilience and security risk. And while you will feel it if you experience a major disruption to your tenant and its configuration, it is very likely that you have no way to detect when seemingly minor configurations change (due to drift or some hidden malicious activity), and equally, no way to roll back configuration changes or drift or recover from much larger configuration tampering attacks.

You just don't know that you don't – and this is a major security blind spot and threat not only to your tenant resilience but also to your entire business.

Microsoft DOES NOT back up or restore your tenant configurations.

How Disaster Strikes: Four Ways Your M365 Tenant Can Fail Overnight

Without a comprehensive backup of your M365 tenant configurations, you are vulnerable to multiple, pervasive risks.

Risk Scenario 1: The Peril of Human Error

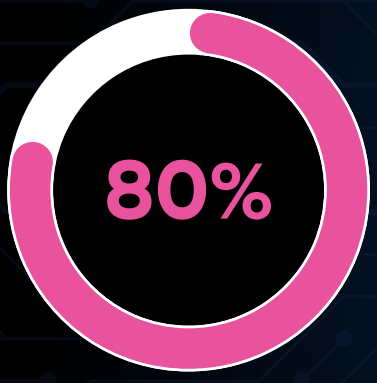
Your administrator accidentally deletes critical configurations. Even skilled administrators make mistakes.

> An example: a 100,000-person healthcare organization lost a critical email distribution group configuration when an admin accidentally deleted these painstakingly configured groups that made up the underlying email infrastructure for pushing out daily critical operational staff emails. Setting these email group configurations up again took days, during which the affected hospitals faced an operational nightmare.

These kinds of examples illustrate how easily one accidental change to a Conditional Access policy or the offboarding of the wrong user can cause immediate, widespread disruption. And it's not at all uncommon – **Gartner reports that misconfiguration-related issues cause 80% of all data security breaches, and predicts that in 2025, up to 99% of all cloud environment failures will be attributed to avoidable human error.**

These errors can be simple: an admin makes a direct change in a production environment rather than a test environment, or an incorrect user is offboarded, causing a critical policy to be deleted. The reliance on manual processes, particularly for user onboarding and offboarding, is a significant contributor to this risk.

The CoreView 2025 State of M365 Security report found that a concerning **30% of organizations still manually configure each new user, a process rife with opportunities for error and misconfiguration.** And manual, human effort is always a vector for human error.



Gartner reports that misconfiguration-related issues cause 80% of all data security breaches.

Risk Scenario 2: The Dangers of Malicious Activity or Insider Threats

Configuration tampering is a favorite tactic of attackers, allowing them to disable security controls and establish persistence quietly. In this kind of attack, a cyber criminal purposefully tampers with configurations.

> According to the 2025 CoreView State of Microsoft 365 Security report, there was a **79% increase in configuration tampering incidents since 2023**, with a surge in tampering with Defender, Intune, and Entra when gaining access to the tenant to reduce enterprise defenses and ensure re-entry if kicked out.

Organizations have no way to know which configurations were tampered with after an incident, forcing a full audit of all configurations before the tenant can be operated with confidence again. It's not just about changing existing configurations — attackers can also create new objects and configurations that lie in wait and serve their nefarious purposes.

This threat is not theoretical; **Microsoft's Digital Defense Report recorded over 176,000 incidents related to security setting tampering in a single month in 2024**. As described, this form of attack is often silent, as it involves subtle changes to critical controls. For example, attackers might alter a DLP policy to allow data exfiltration or disable audit logs to cover their tracks. Nation-state actors like Nobelium (Midnight Blizzard) have successfully exploited and created Entra Apps to elevate privileges and gain persistence in their target's tenants.

The Entra Apps Scanner finds the vulnerable apps Midnight Blizzard exploits. Download the free scanner now. →

Without a configuration backup, an attacker can silently alter settings – disabling MFA, changing DLP policies, or modifying audit logs — leaving no easy path to recovery. And not having visibility and an audit trail for M365 means you have no way of knowing how much tampering has happened – forcing you to review ALL configurations, which is basically like reconfiguring your tenant from scratch again.

One wrong change. That's all that's standing between you and your tenant going offline.

Risk Scenario 3: Total Tenant Takeover

In the most dramatic of disaster scenarios, an organization could face a total tenant takeover. In this scenario, an attacker gains full admin privileges AND uses this to lock out all users and admins and hold the tenant to ransom.

They demand payment. The organization is in panic mode and scrambles to review configurations of their secondary/dev tenant to see if they can start operating in that environment.

This review process could potentially take three weeks – and may not even yield complete or adequate results to operate without rebuilding a tenant from scratch.

Risk Scenario 4: The Unintentional Drift

While not as dramatic as hostile takeovers by cyber pirates, configuration drift is also a problem – an invisible, silent, cumulative collection of changes that occurs as multiple admins make small, uncoordinated alterations to configurations over time.

Drift has the potential to cause a range of consequences – from downtime to compliance violations to security breaches. This problem is exacerbated in complex environments with multiple tenants or many admins.

> Configuration drift without visibility into how things have changed makes it impossible to audit and report on your environment, leaving you in a state of not knowing what you don't know. Without a baseline backup and active monitoring, organizations are blind to this risk. And this is true in any of these risk scenarios.

Another important thing to keep in mind: *Even if your configuration has not changed, how would you know?*

Without an automated means to constantly monitor and easily restore baseline settings, you are blind to what has changed, and you would have to audit your entire tenant manually.

What is Configuration Drift?

Imagine your IT team sets up Microsoft 365 perfectly. You've set up all the right security settings, sharing rules, and access controls.

But over time...

- Users make changes
- New admins tweak settings
- Updates roll out
- Policies are forgotten

Suddenly, things aren't how you set them up (and you may not even realize it).

That's configuration drift.

It's when your Microsoft 365 environment slowly moves away from the secure, consistent state you intended, creating risks, inefficiencies, and surprises all along the way.

The fix?

You need tools that spot drift early, show you exactly what changed, and help you get back on track. That way, small issues don't become big problems.

The Hidden Weakness in Every Microsoft 365 Tenant: Overlooked, But Business-Critical

Imagine insuring every item in your home but neglecting to insure the house itself. If the house were destroyed, you would be able to replace your belongings but have nowhere to put them. This is the situation most organizations are in – ***without knowing it*** – with their Microsoft 365 tenants.

The Tenant as a Glass

Lack of configuration backup is not just a security and operational disaster-in-waiting – it reflects a fundamental misunderstanding of what Microsoft 365 is. It is not just an app your organization uses. It's rather like a glass of water: your Microsoft 365 tenant is the glass, and the water is your data.

Your **Microsoft 365 tenant** is the **glass**, and the **water** is your **data**.

Not all incidents threatening configurations are the same. On one end of the spectrum, minor tampering of key configurations could be an annoyance but not an existential threat to business. On the other end, you could face mass deletion of your identity infrastructure and security safeguards, which would be a potentially business-ending disaster.

If you face minor misconfigurations, such as a single user's permissions being accidentally changed, it could take hours to debug and resolve but is ultimately not an existential business crisis. It's a bit like having a chipped glass – usable, functional, and not a huge risk, even if it's not ideal.

Let's say instead a failed PowerShell script breaks a specific service for a limited number of users. This slows productivity and does cause a disruption to business, but it can still be recovered from, however inconvenient and time-consuming the outage ends up being. This is akin to a cracked glass. Still usable, but the risk to the glass's integrity is growing.

And finally, a total loss of tenant configurations would result in massive downtime, and for most organizations, the chaos of having no restoration plan or backups to rely on. This shattered-glass scenario occurs when core policies, such as authentication, mail flow, or access control, are corrupted, tampered with, or accidentally deleted, rendering the entire digital workspace unusable. And with the invisible problem of no configuration backups, including policies, permission settings, and user roles, organizations will struggle to return to baseline and lose not only configurations and customizations but time and resources.

> Ultimately, you don't want any of these scenarios – the more damage to your glass, the more risk to the water. In other words, if your configurations are not correct, then you do not have a safe environment in which to keep your data.

Tenant Configurations: Your Security Blueprint, Not a Checkbox

Tenant configurations are the digital blueprint of an organization's security posture and operational integrity. **Unlike data, they aren't backed up by default—even though they should be, since they define how data is protected, governed, and accessed.** Yet most enterprises run without M365 tenant configuration backups and are blind to the risk.

M365 configurations span over 10,000 unique policy elements across critical services, but Microsoft provides no native tenant-wide backup or rewind solution. These elements govern user access, compliance, and application behavior—everything essential to the smooth running of your business. **These include core business-critical functions:**

Security Settings

This category is the front line of defense. It includes Conditional Access policies that dictate who can access what from where, and multi-factor authentication (MFA) rules that prevent account takeover. When these settings are lost or tampered with, an attacker can bypass all perimeter controls.

Compliance Policies

For regulated industries, compliance is non-negotiable. Data Loss Prevention (DLP) policies prevent sensitive information from leaving the organization, while retention policies ensure data is preserved for legal and audit purposes. Without these, an organization is exposed to severe penalties and data privacy violations.

Identity Management

Over 95% of organizations experienced a cloud-related breach in the past 18 months, with 92% linked to insecure identities (2024 Cloud Security Alliance). User and group settings, admin roles, and app privileges in Entra ID (formerly Azure AD) form the core of identity security—if compromised, the framework collapses.

Collaboration Settings

Policies in Teams, SharePoint, and Exchange govern external sharing, guest access, and data flow. When these settings are missing or misconfigured, organizations risk uncontrolled data exposure, expanding the attack surface and opening the door to potential compromise.

.The integrity of these settings is the backbone of your Zero Trust architecture, your ability to enforce least privilege, and your compliance with industry regulations. Losing them is not a simple inconvenience; it is a fundamental loss of control over your entire digital workspace.

The Shared Responsibility Trap: Why Microsoft Can't Save You

According to the CoreView 2025 State of Microsoft 365 Security report, **49% of organizations mistakenly believe that Microsoft fully backs up their tenant configurations and will restore them after an incident**.

Reinforcing this idea, the Cloud Security Alliance's 2025 SaaS Security Survey cites the "overreliance on native control" as a major gap in enterprise security, as more than **69% of organizations state that they depend on the primary security controls within SaaS applications**. Blindly relying on M365 native controls, not knowing that such native controls do not exist for tenant configurations, is one such overreliance that is a lot more dangerous than anyone realizes.

A primary reason for this vulnerability is a widespread misconception. The truth lies in Microsoft's Shared Responsibility Model, which states that while Microsoft is responsible for the security of the cloud, the customer is responsible for security in the cloud. This means you are solely responsible for protecting your data and your tenant configuration settings.

> CoreView's CTO and Co-Founder, Ivan Fioravanti, provided a real-world example of a Teams channel that couldn't be restored due to a Microsoft-side bug. This incident exposed an uncomfortable truth: when Microsoft is the only controller, you are vulnerable not only to user errors but also to software bugs, policy gaps, and support bottlenecks. This is just one example of a way things can go wrong.

Microsoft's Digital Defense Report recorded over 176,000 incidents related to security setting tampering in a single month in 2024.

The True Cost of No Config Backups: Catastrophic Outages, Fines, and Failures

What happens if you do not have your tenant configuration backed up? From downtime/outages to non-compliance fines and penalties and audit failures to loss of Zero Trust posture to financial loss, a lack of configuration backups is a hidden business disaster – not just an inconvenience:

Exposure to Business Downtime

A compromised or misconfigured tenant can lock out the entire organization, disrupting authentication, email routing, and collaboration. Recovering from such an incident requires manually rebuilding the tenant, a process that can take days or weeks. In the event of a complete tenant takeover, most organizations will be unable to restore their environment, that is, put their "water into the new glass."

Making sure the new tenant is as close as possible to the original is painstaking and resource-intensive work, and your business experiences downtime during the whole process. Without an automated restore, a business is left vulnerable to further attacks during this long, arduous rebuild process.

Security Exposure

The absence of configurations can lead to immediate and widespread security compromises. Without MFA or DLP policies, an attacker can exfiltrate sensitive data with ease.

> The CoreView survey found that **58% of account compromises occur in environments still struggling with MFA adoption**, highlighting the critical gap between having a security control and enforcing it.

This is further underscored by Microsoft's own data, **which states that 99.9% of all account compromises happen on accounts without MFA**. Without a robust configuration backup, an organization cannot quickly restore the security policies needed to prevent such attacks.

99.9% of all account compromises happen on accounts without MFA.

Regulatory Fines and Audit Failures

M365 configurations are essential for demonstrating compliance with regulations and for being able to conduct audits. Without an immutable, restorable backup of these policies, an organization cannot prove its security posture or its ability to recover from a disaster. This exposes the business to significant regulatory fines, legal penalties, and failed audits.

For multinational organizations, especially those in highly regulated industries, the risk is even greater. Many companies operate in strict regulatory environments and have faced significant issues because of tenant issues.

> One financial firm failed an audit because they "had no meaningful way to restore your config after a disaster". Another firm with sensitive data they needed to segment for regulatory and protective IP purposes had no way to keep an admin in one country from being able to see all data.

Loss of Zero Trust Posture

Your Zero Trust architecture is built on the policies you define. The loss of these policies means an immediate reversion to a trust-all model, leaving your network open to lateral movement and privilege escalation.

The CoreView report confirms this, noting that **63% of tenants fail to implement least privilege effectively**. A configuration backup is the only way to quickly restore the fine-grained policies that enable least privilege and prevent an extreme blast radius during an incident.

Attackers don't just break systems — they exploit missing backups to keep them broken.

How to Bulletproof Your Microsoft 365 Tenant: Essential Resilience Steps

Protecting your Microsoft 365 tenant from misconfiguration, accidental changes, and malicious actions demands more than basic SaaS administration. Here are the essential steps for resilience:

Understand the Shared Responsibility Model

- **Accept Cloud Reality:** The first step is to acknowledge that the responsibility for tenant configuration resilience lies with you and your organization. Tenant-level configuration, access, and data resilience are in your hands, and Microsoft is not going to be able to help you. Microsoft secures the underlying infrastructure – you must secure your instance and everything in it. This is not just a technical problem; it's a strategic and cultural one.
- **Change Your Mindset:** An organizational mindset shift needs to happen – move from assuming native tools are sufficient and default settings are enough to actively taking ownership of your cloud security posture. This realistic perspective is essential for closing the hidden security gap and moving towards a proactive, resilient security model.

Assess and Document Your Baseline Tenant Configuration

- **Map Out Tenant Assets:** Identify all critical configuration areas—admin roles and permissions, security policies, conditional access, Exchange/SharePoint/Teams settings, compliance configurations, third-party integrations.
- **Perform a Configuration Audit:** Use tools like CoreView to generate a "configuration snapshot" of your current state. Document settings, policies, ownership, and exceptions

You cannot rely on Microsoft or your existing data backup solution to secure configuration backup.

Implement a Third-Party Configuration Backup Solution

- **Select a Trusted Solution:** Deploy a dedicated platform (e.g., CoreView) that automates configuration backups across all workloads (Exchange, Teams, OneDrive, SharePoint, Intune, etc.)
- **Verify Backup Coverage:** Ensure all security and service-related configurations are included, not just user data.
- **Schedule Regular Backups:** Automate configuration backups daily or as required by your change frequency.

It cannot be stated enough: you cannot rely on Microsoft or your existing data backup solution to secure configuration backup. CoreView found that only **18% of organizations manually back up configurations or rely on documentation** — a highly unreliable and error-prone process.

The CoreView 2025 State of Microsoft 365 Security report found that organizations with formal disaster recovery plans are **61% less likely to experience significant operational disruptions from misconfigurations**, proving that investing in the right tools makes a measurable difference.

Integrate Configuration Backup into Your Disaster Recovery Strategy

- **Tie Backups to Incident Response:** Align configuration backups with your incident response and cyber resilience framework.
- **Establish Monitoring for Configuration Drift:** Use change tracking and drift detection features to alert when configurations deviate from baseline or desired state.
- **Plan and Rehearse Restore Procedures:** Schedule regular “fire drills”. Restore configurations in test environments to ensure your team can recover quickly under pressure.

Organizations with formal change control processes in place report experiencing **72% fewer security incidents tied to misconfigurations**, highlighting the value of a disciplined and rehearsed approach to configuration backup.

Enforce Change Control and Governance

- **Adopt Formal Change Control Processes:** Require approval and logging for all configuration changes. Use workflow automation and audit trails.
- **Implement Role-Based/Function-Based Access Controls:** Restrict administrative privileges to only those who require them, and review roles regularly.
- **Use Delegated Administration:** Segment duties and limit the blast radius of any single admin account.

Monitor and Report on Configuration Health

- **Use Reporting Tools:** Continuously monitor configuration health using dashboards and reports. Prioritize alerts for high-risk changes.
- **Schedule Regular Reviews:** Present findings to executive stakeholders; update policies and procedures based on new threat vectors and lessons learned.

Educate Your Team

- **Conduct Regular Awareness Training:** Run workshops on configuration recovery, incident response and compliance requirements.
- **Update Playbooks:** Refine documentations, runbooks, and playbooks based on feedback from drills and actual incidents.

Test and Validate Your Resilience Continually

- **Simulate Real-World Scenarios:** Test how well backup and restore work against ransomware, insider attacks, and configuration errors.
- **Measure and Improve:** Analyze outcomes, identity gaps, and continually enhance your resilience strategy.

A key takeaway: Making your Microsoft 365 tenant resilient is an ongoing project that requires focus and discipline. By covering everything from baseline assessment through automated configuration backup, formal change control, regular drills to continuous monitoring, you can dramatically reduce operational risk and make your cloud collaboration environment resilient by design.

A configuration backup is the only way to quickly restore security policies and maintain resilience.

Don't Settle for Less: The Non-Negotiables in a Tenant Configuration Backup Solution

An effective tenant configuration solution should provide several non-negotiable essentials. Basic capabilities are critical for reliable restoration and business continuity while advanced requirements take on more importance for organization with complex compliance, governance, and security needs. Mature solutions should address both sets of needs for true tenant configuration management and resilience.

Basic Requirements for Tenant Configuration Backup and Restore

- **Complete Tenant-Wide Backup:** Securely archive all rules and policies across all M365 services, not just data. This must include granular details for every service, from Entra ID to Exchange Online.
- **Regular, Automated Snapshots:** Ensure continuous, automated backups with granular and full restore capabilities. This "rewind" functionality is crucial for rolling back to a previous, known-good state, whether it's for a single policy or the entire tenant.
- **Full Restore Capability:** Enable automated recovery that restores original configurations accurately and without delays. This capability is what transforms a manual, weeks-long rebuild process into a rapid, automated recovery.
- **Minimum Requirements for Coverage:** Ensure comprehensive coverage of security, compliance, identity, application, and delegation policies. Partial solutions do not cover everything required and therefore leave critical vulnerabilities exposed.

Advanced Requirements for Mature Tenant Configuration Management

- **Configuration Change Management:** Track, monitor, and maintain an auditable record of all configuration changes. This process supports ongoing change control and compliance efforts
- **Change Detection and Alerting:** Monitor continuously for configuration drift and alert administrators to unauthorized or mistaken changes in real-time. Regular audits help make the invisible problem of drift into a manageable, actionable process, ensuring you are always aware of your security posture.
- **Advanced Auditing and Reporting:** Provide detailed audit logs, historical reports, and change histories for governance, analysis, and compliance purposes.
- **Policy Versioning and Comparison:** Enable comparison between different versions of policies and configurations, supporting rollback and quick detection of anomalous changes.

Conclusion: M365 Is Your Business, Now Protect It like Your Bottom Line Depends On It

Global enterprises have become almost religious about safeguarding their critical data but very few recognize what kind of disaster they would face if they were to lose the tenant their data lives in. Laboring under the mistaken belief that their tenant configurations are backed up by Microsoft (or their data backup provider), most businesses fail to realize that in the event of a tenant failure – malicious or otherwise – they might be able to recover their carefully preserved data, but they would not have a tenant to restore it to.

Microsoft 365 is the backbone of your enterprise, but it is at risk without tenant configuration backup. The misconception that Microsoft has you covered is the biggest invisible threat to your cyber resilience, leaving your business one click away from a catastrophic failure. Mitigating this risk requires adopting a framework powered by a third-party configuration backup solution, making it a central pillar of any modern cyber resilience strategy. The goal is to address this existential configuration backup gap, which most organizations, despite investing heavily in cyber resilience, remain completely unaware of.

> CoreView was built to meet these specific challenges – helping you avoid these failures and protect your cyber resilience at the tenant level.

The invisible risk of lost or changed tenant configurations is one of the greatest threats facing your organization. But it's also one you can fully control.

Don't wait until an outage, compliance failure, or breach exposes this hidden vulnerability and costs your business time, money, and trust. By making tenant configuration backups a core part of your resilience strategy, you transform an invisible threat into a managed, recoverable risk.

Don't Leave Your Business Exposed to Silent Risk

Take the proactive step—secure your Microsoft 365 tenant configurations with CoreView today. Contact us to schedule a demo and turn invisible threats into managed, recoverable risks.

About CoreView

CoreView gives you cyber resilience that treats Microsoft 365 like the uniquely critical and sensitive environment it is. Whether you operate multiple tenants with on premise environments, or you're consolidating to a single tenant, CoreView gives you enterprise grade cyber resilience, simplifies and automates M365 administration, and detects wasted spend in your tenant. CoreView powers 4000+ organizations to secure, consolidate, and manage complex Microsoft 365 environments, including the largest Microsoft tenants globally.