5 costly Microsoft 365 protection gaps and how to close them

Protect data, identities and configurations as attacks move beyond the inbox.



Microsoft 365 is central to communication, collaboration and business operations. Microsoft provides a resilient cloud platform, but organizations remain responsible for their data, identities, access controls, configurations and compliance under the shared responsibility model.

The threat has also changed. Attackers increasingly target identity because a compromised account, session or application can provide trusted access without exploiting an endpoint. Password spraying remains widespread, while adversary-in-the-middle phishing, token theft, MFA fatigue and malicious OAuth consent can undermine traditional controls.

This makes Microsoft Entra ID part of the protection strategy, not just the sign-in layer. One identity incident can affect Microsoft 365 and every connected application that relies on Entra ID. These five gaps can turn a mistake or compromised identity into data loss, downtime and compliance exposure.



Microsoft's 2025 Digital Defense Report states that 38 million identity risk detections were analyzed on an average day and that 97% of identity attacks were password spray attacks.

Copyright © 2003-2026 Acronis International GmbH.

Identity compromise and control-plane attacks

The challenge: Stolen credentials are only one route into Microsoft 365. Attackers can capture session tokens through adversary-in-the-middle phishing, abuse a legitimate OAuth application, pressure users with repeated MFA prompts or persuade support staff to reset access. Once authenticated, they can read mail, change forwarding rules, access shared files, create persistence and move across connected services.

The protection gap: Availability and endpoint protection do not restore trust in a compromised tenant. Organizations need strong identity controls, phishing-resistant authentication where possible, monitoring for suspicious sign-ins and application consent, and tested recovery for affected users, groups, roles, policies and configurations.

Configuration drift and excessive privilege

The challenge: Microsoft 365 and Entra ID settings change constantly as users, applications, administrators and external collaborators are added or removed. Conditional Access exclusions, dormant accounts, broad admin roles, risky mailbox rules, legacy authentication and over-permissioned applications can create hidden attack paths. Manual reviews struggle to keep pace, particularly across multiple tenants or business units.

The protection gap: A secure baseline is not a one-time project. Organizations need continuous visibility into tenant posture, prioritized findings and repeatable remediation. Least-privilege access, controlled application consent, lifecycle management and regular review of privileged roles reduce the blast radius when an identity is compromised.

Accidental deletion, ransomware and insider actions

The challenge: Users, administrators, automation and malicious insiders can delete or alter mailboxes, files, sites, Teams content and identity objects. Ransomware and data-destruction attacks may use legitimate permissions, allowing damaging changes to look like authorized activity and propagate through synchronized services.

The protection gap: Native retention, versioning and recycle-bin features are valuable operational tools, but they are not a complete recovery strategy for every workload, object or incident. Recovery may be constrained by time limits, object support, configuration dependencies or the same administrative plane that was compromised. Independent, policy-based backup and regular recovery testing provide another route back to a known good state.



Copyright © 2003-2026 Acronis International GmbH.

Incomplete recovery of Entra ID

The challenge: Entra ID is the identity control plane for Microsoft 365 and many third-party, cloud and on-premises applications. Deleting or corrupting a user, group, role assignment, enterprise application or Conditional Access policy can interrupt access far beyond Microsoft 365. Restoring an account alone may not restore every relationship and configuration the business depends on.

The protection gap: Microsoft supports soft-delete recovery for selected Entra objects, generally for 30 days. Other objects can be hard deleted, and restored policies or named locations may require validation before they are safe to re-enable. A dedicated Entra ID backup strategy should capture critical objects, attributes and relationships, support granular comparison and restore, and be tested as part of business continuity planning.

Retention, compliance and AI-era data exposure

The challenge: Retention settings can be misconfigured, shortened or applied inconsistently. Legal holds and e-discovery requirements may span email, files, collaboration content and identity records. At the same time, Microsoft 365 Copilot and other AI tools can surface information users are already permitted to access, making overshared or poorly classified data easier to discover at scale.

The protection gap: Retention is not the same as backup, and compliance controls do not replace recoverability. Organizations need policies aligned to legal and business requirements, protected recovery points, auditable restore operations, and regular reviews of permissions, sharing and data exposure before AI adoption amplifies existing access problems.

Close the gaps with layered Microsoft 365 protection

No single control can prevent every identity-led attack or data-loss event. Our Microsoft 365 protection solution brings security, posture management and recovery together so your organization can reduce risk before an incident and recover when prevention is not enough.

Strengthen tenant security posture: Continuously identify risky settings, configuration drift, excessive privileges and gaps in security controls, with clear guidance for remediation.

Protect Microsoft 365 data: Back up Exchange Online, OneDrive, SharePoint and Teams data with flexible retention, search and granular recovery.

Protect the identity control plane: Back up critical Entra ID objects and configurations so users, groups, roles, policies and relationships can be recovered after accidental or malicious change.

Reduce phishing and account-compromise risk: Layer email and collaboration security with user awareness, strong authentication and monitoring for suspicious identity activity.

Support compliance and continuity: Use policy-based retention, auditable recovery and regular restore testing to help meet governance requirements and reduce operational downtime.

Simplify protection: Manage security posture, backup and recovery through a coordinated service instead of fragmented tools and manual processes.

Copyright © 2003-2026 Acronis International GmbH.

Protect your Microsoft 365 environment

Review your current Microsoft 365 security posture and recovery readiness. We can help you identify protection gaps, reduce identity risk and build a tested recovery plan for Microsoft 365 data and Entra ID.

Contact us to assess your Microsoft 365 protection gaps.



Source note: Microsoft Digital Defense Report 2025; Microsoft Learn guidance on shared responsibility, Microsoft 365 Backup and recovery from deletions in Microsoft Entra ID.

Acronis

Learn more at
acronis.com

Copyright © 2003–2026 Acronis International GmbH. All rights reserved. Acronis and the Acronis logo are trademarks of Acronis International GmbH in the United States and/or other countries. All other trademarks or registered trademarks are the property of their respective owners. Technical changes and Differences from the illustrations are reserved; errors are excepted. 2026-10