Kaseya

datto

EBOOK

MSP buyer's guide to Microsoft Entra ID backup & identity resilience

Identity is the control plane. When it breaks, everything breaks.

Microsoft Entra ID (formerly Azure Active Directory) sits at the center of modern IT today, governing authentication, access and identity across Microsoft 365, SaaS apps and infrastructure. Every login request, every access approval, every privilege escalation flows through it. It's the front door and the security desk at the same time. And when it fails, users don't just lose access. Operations stop, apps go dark and business grinds to a halt.

However, here's the part many MSPs miss: identity protection is your responsibility, not Microsoft's.

Microsoft operates under a shared responsibility model, which means identity data protection and recovery are your responsibility, not theirs. So, when identity infrastructure fails for your clients, it lands squarely on your shoulders.

And if you're counting on Microsoft's native tools to bail you out — don't. They're built for availability and security, not backup or operational recovery. They offer limited retention and recovery capabilities, which are insufficient to protect your clients' critical identity data.

For MSPs, this creates a double-edged reality:

- A growing, often invisible risk spread across every client tenant
- And a clear opportunity to deliver high-value, high-margin identity resilience services

The question isn't whether your clients' identity infrastructures will be tested. It's whether they can recover when they are. That's exactly why this guide exists. We'll break down why Microsoft Entra ID needs purpose-built backup — and how to evaluate the right solution to protect your clients, meet SLAs and turn identity resilience into a competitive advantage.

Did you know?

Identity is now the primary attack vector. Microsoft tracks more than 4,000 identity attacks every second and analyzes 38 million identity risk detections daily.[1]

How to use this guide

Not all Entra ID protection solutions are built the same. To cut through the noise, focus on what actually matters for your business and your clients.

As you evaluate options, anchor your decisions around three outcomes:

- Eliminate single-cloud and identity control plane risks
- Meet SLAs with fast, reliable identity recovery
- Reduce the total cost of ownership (TCO) for identity recovery services

Everything in this guide is built to help you deliver on these.

Eliminate single-cloud and identity control plane risks

Microsoft Entra ID sits at the center of everything your clients do. Entra ID enables secure authentication, enforces conditional access and protects against unauthorized access with multifactor authentication (MFA), identity protection and single sign-on (SSO). It is also the bridge that connects users to Microsoft 365, Azure workloads, third-party SaaS applications and internal tools.

When it breaks, everything else stalls.

But if you think Microsoft's native capabilities have you covered when the identity infrastructure fails for your clients, that assumption is very risky.

By default, Entra ID retains deleted objects for 30 days in a soft-deleted state, after which they are permanently removed with no way to recover them. However, even this retention is limited to specific objects, such as users and groups, rather than the broader identity configurations that often drive access and security. It also does not account for more complex scenarios such as cascading misconfigurations, insider-driven changes or targeted attacks. These gaps make recovery unpredictable. Without a dedicated backup approach, restoring identity data can be time-consuming or, in some cases, impossible.

Microsoft's native capabilities are not designed to help you recover cleanly from an identity-related incident because:

- There is no traditional backup layer and no reliable way to restore identity to a specific point in time
- They lack complete recovery coverage for common failure scenarios such as misconfigurations, privilege changes, directory corruption or tenant-wide compromise
- Identity data remains within the same tenant and trust boundary, leaving no external fallback if that boundary is breached
- Both identity and recovery options can be affected at the same time if admin credentials are compromised

What MSPs should look for:

MSPs need a clear and reliable way to restore identity infrastructure and keep their clients operational when things go wrong. That means having the right capabilities in place to recover quickly, accurately and without added complexity.

Here are the key features to look for:

Purpose-built identity backup, not just logs or soft delete

A complete backup should capture the full identity layer, including users, groups, roles, directory configurations, applications, devices, administrative units, role assignments, organizational contacts, tenant settings, customer domains, conditional access policies, service principals and more. It should also maintain version history over time, so you can track changes and restore the exact state you need.

Point-in-time, quick recovery across identity objects

Recovery should not be guesswork. You should be able to rapidly restore identity to a known-good state before a misconfiguration or attack. This includes restoring individual objects, multiple object types or entire configurations without manually rebuilding identity structures.

Cross-tenant and cross-user recovery

Recovery should not be limited to the same environment. In active incidents, you need the flexibility to restore identities and configurations to alternate users or even clean tenants, ensuring continuity while the original environment is secured.

Independent backup control plane

Your backup system should be separate from the production identity system. It should operate with its own credentials and remain accessible even if the primary tenant is compromised. This separation ensures recovery remains possible during credential-based or tenant-level attacks.

Strong data encryption

Identity data must remain secure at all times. Look for solutions that use 256-bit AES encryption for data at rest and TLS encryption for data in transit to protect sensitive information throughout the backup and recovery process.

Meet SLAs for identity-driven operations and rapid recovery

Identity attacks rarely stay contained. What starts as a single compromised account can quickly escalate into a full-scale breach.

Picture this: An attacker gets in through a phishing email or stolen credentials. From there, they move quietly across the environment, access other systems, elevate privileges and create new accounts to stay persistent. By the time it's detected, access controls may already be altered, sensitive data may already be exposed and critical systems may be within reach.

In these scenarios, organizations are forced to lock down identity systems to contain the threat and investigate what happened.

This helps to:

- Stop the attacker's movement by cutting off access
- Preserve forensic evidence by freezing logs, permissions and configurations
- Prevent unintended admin changes that could overwrite critical data needed for investigation

But this containment comes at a cost.

When Entra ID is restricted or becomes inaccessible, the impact is immediate. Unlike a file or VM recovery, identity failures affect the entire organization at once. Users lose access to core services, applications become unavailable and day-to-day operations are disrupted. Teams are forced to rely on manual workarounds just to maintain continuity.

MSPs need a way to restore their clients' identity infrastructure quickly and get operations back on track without prolonged disruption. But Microsoft's native tools are not built to support that level of fast, complete recovery in these scenarios.

- They lack the ability to quickly roll back identity configurations to a previous state
- Recovery is limited and fragmented, with support mainly for deleted users within a fixed time window and select objects, not full environments
- There is no unified way to recover identity and user data together, leading to disconnected and time-consuming recovery efforts

What MSPs should look for

To meet SLAs in identity-driven environments, recovery cannot be slow, manual or uncertain. MSPs need capabilities that match the speed and scale of identity failures.

Here's what to prioritize:

Frequent backups to meet aggressive recovery point objectives (RPOs)
Identity changes constantly, and a single daily backup is not enough. Look for solutions that capture multiple backups throughout the day so you can recover from the most recent, known-good state.

Fast, granular recovery across identity objects
Recovery should give you flexibility, not limitations. You should be able to restore exactly what's needed — whether it's a single object, multiple object types or full configurations — without rebuilding identity structures from scratch.

Operationally simple recovery workflows
During an incident, complexity slows everything down. Recovery workflows should be straightforward and efficient, helping reduce time to resolution and get your clients back to normal operations faster.

Unified identity and mailbox recovery workflows
Recovering Entra ID users alone is not always enough to restore productivity. Mailboxes, permissions and user data may also require recovery to make users fully operational. Look for solutions that unify Microsoft 365 and Entra ID recovery in a single workflow, reducing manual effort, accelerating time-to-recovery and simplifying large-scale identity restoration during major incidents.

Reduce the total cost of ownership (TCO) for identity recovery services

Have you considered the hidden costs of “free” native tools?

Microsoft includes baseline identity capabilities, but “included” does not mean complete. There is no built-in backup for Entra ID. When something goes wrong, recovery becomes a manual effort. Admins have to step in, assess the damage and start rebuilding — and that effort adds up quickly. More hours spent on recovery mean higher labor costs. At the same time, downtime continues to affect your clients, resulting in lost productivity and potential revenue losses.

The recovery process itself is not straightforward.

- Rebuilding users, roles and permissions often has to be done manually, object by object
- Access across SaaS applications needs to be revalidated, adding another layer of effort and delay

For MSPs, this creates a ripple effect across operations and business.

- Service delivery becomes more expensive due to the time and effort involved
- Scaling becomes harder when every incident requires hands-on intervention
- The risk of missing SLAs increases, especially when recovery timelines are unpredictable

What looks like a cost-saving approach on the surface often leads to higher operational and financial impact over time.

What MSPs should look for

Controlling costs is not just about reducing spend — it is also about making recovery predictable, scalable and efficient across every client environment you manage.

Here's what to prioritize:

Predictable pricing model

Costs should not spike when things go wrong. Look for pricing that stays consistent and avoids variables tied to recovery effort, data movement or incident response. This ensures you can plan margins with confidence and avoid unexpected overhead during critical situations.

Cost-saving data lifecycle management

Not all data needs to stay active to remain valuable. For instance, the ability to retain inactive users without requiring active licenses helps reduce unnecessary costs while still preserving data for recovery, compliance or future use.

Operational efficiency at scale

As your client base grows, so should your ability to manage it without added complexity. Multitenant management is essential to oversee all clients from a single view. Automation and alerting help reduce manual effort and keep operations running smoothly. Minimal onboarding overhead ensures you can deploy protection quickly without long setup cycles.

Key questions to ask your vendor

The right solution should hold up when things break. These prompts will quickly reveal how prepared a vendor is for real-world identity failures.

How well is identity data protected from platform-level risks?
Identity backups should be stored independently of Microsoft Entra ID, ensuring they remain accessible even if the primary tenant is compromised. Another key factor to consider is whether the solution supports recovery from a full tenant-wide incident.

How complete and flexible are the recovery capabilities?
It is important to understand what identity objects are actually protected and how recovery works in practice. The solution should support restoring single objects, multiple object types or full configurations. It should also allow recovery into a different tenant when needed.

How well does the solution support SLA-driven recovery?
Backup frequency and recovery speed directly impact your ability to meet SLAs. Look for solutions that offer frequent backups and can restore identity at scale within tight timelines.

How practical is the solution for MSP operations and cost control?
The solution should offer predictable pricing and simplify operations across clients. It should support centralized multi-tenant management and provide ways to reduce costs for inactive users without losing access to their data.

Turn identity resilience into a scalable MSP growth engine

For MSPs looking to turn identity resilience into their next growth opportunity, Datto Backup for Microsoft Entra ID helps you back up, protect and restore Entra ID data with confidence. Notably, it delivers a unified recovery workflow across Entra ID and Microsoft 365, so identity configurations and user data can be restored together.

With Datto Backup for Microsoft Entra ID, you can:

Unlock new, high-value service offerings
Package identity protection as a revenue-generating service with Identity Backup as a Service (IBaaS). Expand your security and compliance portfolio and differentiate beyond standard Microsoft 365 backup.

Ensure reliable, frequent protection without manual effort
Automated, scheduled backups run throughout the day, capturing identity data at regular intervals without disruption. This ensures you always have recent restore points, helping you meet strict recovery objectives across clients.

Recover faster with flexible, real-world recovery options
Restore exactly what is needed, whether it is a single object, multiple object types or full configurations. Recovery is not limited to the same environment either. You can restore data to the original tenant or redirect it to a clean tenant during major incidents or rebuild scenarios.

Protect identity data outside the production risk zone
Backup data is stored independently from the production environment, ensuring it remains secure and accessible even if the primary tenant is compromised.

Simplify operations and scale without friction
Onboard clients in minutes and automate protection across tenants with a set-and-forget approach. Manage Entra ID and Microsoft 365 backups through a unified platform designed for multi-tenant MSP environments.

Accelerate recovery and reduce downtime impact
Restore identity configurations and user data in a single workflow, eliminating fragmented recovery processes and reducing time to full user productivity.

Optimize costs with MSP-first pricing
Benefit from simple per-user pricing with flexible license reassignment. Unlock volume-based discounts as you scale and reduce costs by preserving and restoring inactive user data without ongoing licensing overhead.

Strengthen compliance and long-term data retention
Support regulatory requirements with alignment to SOC 1, SOC 2, HIPAA and GDPR. Maintain infinite data retention to meet audit and compliance needs without added complexity.

Unlocking the next big opportunity in cyber resilience

Microsoft Entra ID sits at the center of modern IT environments today, powering authentication, access and control across everything your clients rely on. Unfortunately, that central role also makes it a prime target for attackers. Leaving it unprotected — or depending on native tools that are not built for backup and recovery — puts your clients just one incident away from widespread disruption, critical data exposure and costly, prolonged downtime.

For MSPs like you, this is a clear opportunity to step in with a stronger approach. Deliver identity resilience as a high-value service, help clients stay operational through incidents and build a consistent stream of recurring revenue in the process.

Ready to see how it works in action?

Source
1 https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/