360° Cyber Resilience for Entra ID

Protect, secure, and recover your critical cloud-based identity infrastructure

With over 600 million daily identity attacks targeting Microsoft environments—and ransomware groups like *Storm-0501* now weaponizing cloud-based identity compromise—organizations face unprecedented risk. Traditional fragmented approaches that protect Microsoft 365 data while overlooking identity leave critical gaps that attackers exploit. Organizations must consider comprehensive protection of their Microsoft 365 apps alongside the critical identity infrastructure such as Entra ID.

When identities break, business breaks. For many organizations, email, applications, authentication, conditional access, automation, and security controls all depend on Entra ID. Yet many organizations still rely on Microsoft's limited native recovery, creating operational and compliance exposure no security team can afford. In fact, Gartner forecasts that 75% of enterprises will treat SaaS backup as mission critical by 2028, up from just 15% in 2024—driven partially by the rise in identity-led attacks and tightening regulatory requirements.

Key Benefits

- Unified protection for M365, Entra ID, and MBS data
- Immutable, isolated identity backups attackers cannot alter
- Compliance-ready long-term retention and audit trails
- Granular, fast recovery of users, groups, applications, policies, and relationships
- Clean, verified recovery points that prevent reinfection and restore trust

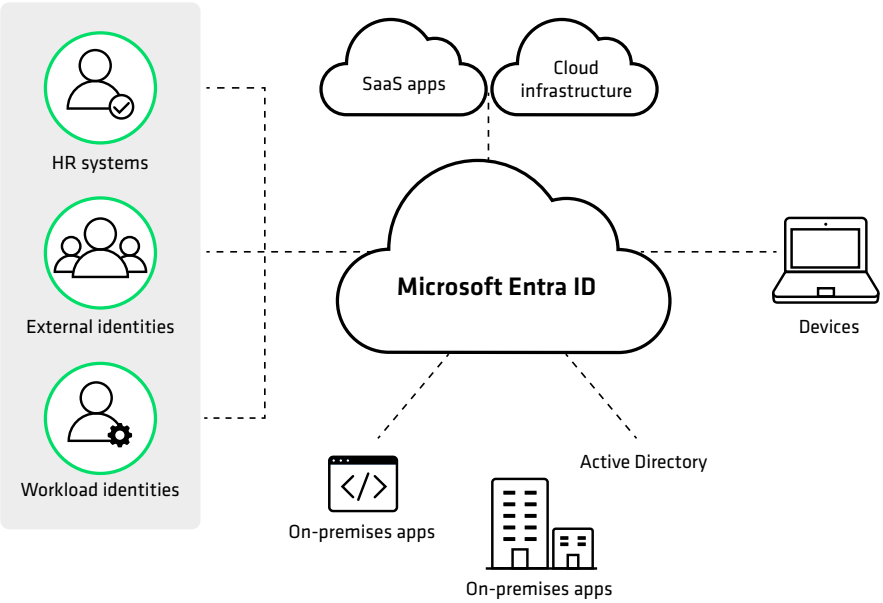

Figure 1: Entra ID is a critical part of the enterprise IT infrastructure. It manages access for employees, workloads, and third-party vendors to a variety of applications, devices, and beyond.

The challenge

Identity is an essential and highly targeted part of an organization's IT ecosystem. With the majority of attacks leveraging Active Directory or Entra ID—and identity-related breaches averaging $4.5M per incident—an effective cyber resilience strategy hinges on whether organizations can protect and rapidly restore their identity infrastructure.

Entra ID is a highly complex workload and cannot simply be rebuilt. Without clean copies of users, groups, service principals, roles, and policies, recovery becomes slow, error-prone, and incomplete—extending outages and amplifying the blast radius of cyber events. Attackers know this and target identity systems like Entra ID to maximize disruption. Without effective identity protection, security, and recovery organizations face sever impacts that directly halt operations:

- **Permanent loss of access when attackers delete or alter identity objects**
  Critical accounts—including admins and service principals—can be removed or modified, preventing authentication and blocking recovery efforts.
- **Irreversible damage from malicious hard-deletes**
  Once objects are purged, Microsoft's native protections don't provide a path to restore identities essential for daily operations and automation.
- **Collapse of security posture when Conditional Access policies are changed or wiped**
  Attackers can disable MFA, weaken controls, and create persistence paths—with no native rollback or version history to restore from.
- **Extended outages due to loss of identity relationships across users, groups, apps, and roles**
  Even recreated accounts cannot function without the relationships that govern access, permissions, and integration across cloud services.

It's important to note that Microsoft provides continuity and availability for their solutions, and not the necessary capabilities to achieve true cyber resilience in the face of today's threats. Without comprehensive protection of Entra ID, identity compromise can become extended business downtime and undeniable risk.

The solution

Cohesity delivers 360° cyber resilience for Entra ID across the entire attack lifecycle—from proactive protection to rapid, clean recovery—in one platform that unifies both Microsoft 365 and Entra ID protection. The platform provides comprehensive coverage for all critical Entra ID objects. This ensures organizations can restore complete identity-driven business processes with all data, relationships, and configurations intact, rather than piecing together disconnected components that no longer function.

Critical Entra ID objects protected by Cohesity

- Users
- Groups
- Applications
- Service Principals
- Devices
- Role Assignments
- Admin Unites
- Conditional Access Policies
- Contacts

Protected data will reside in Cohesity's tenants—not in Microsoft's or the customer's – so identity data is isolated in Cohesity's immutable, durable, isolated storage that cannot be altered or encrypted by attackers, preventing tampering, ransomware spread, and identity poisoning. And with no retention limits, organizations can preserve Entra ID backups for as long as operational, governance, or compliance needs demand—ensuring long-term cyber resilience expanding native Microsoft capabilities.

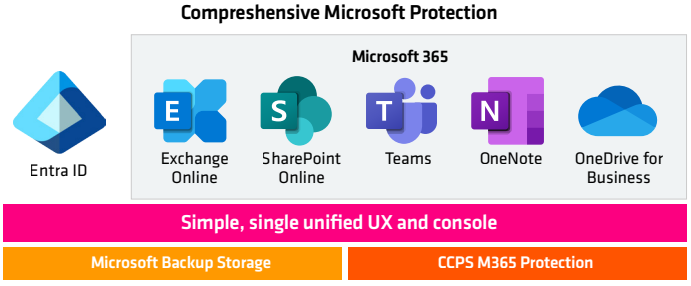

Figure 2: Cohesity brings comprehensive cyber resilience for all your critical Microsoft 365 apps and Entra ID with protection, security, and recovery capabilities integrated with Microsoft 365 Backup Storage.

For hybrid identity scenarios

Many organizations use a hybrid identity model with both on-premises Active Directory and cloud-based Entra ID. Because these systems are usually synced or federated, securing both is essential. If only one is protected or recoverable, your overall identity posture is still at risk. In hybrid environments where identities are synced from Active Directory to Entra ID, Cohesity's solution works alongside your existing AD protection strategy. After your AD recovery solution restores Active Directory objects and Entra Connect synchronizes them to Entra ID, Cohesity completes the identity recovery process by restoring Entra ID-specific attributes, ensuring your cloud identity infrastructure is fully operational.

To learn more about Cohesity's approach to Active Directory protection, recovery, and security, explore Cohesity Identity Resilience here.

Organizations rely on Cohesity for end-to-end Entra ID protection

Proactive Protection	Active Protection	Reactive Protection
✔ Continuous identity data protection across users, groups, roles, apps, and policies ✔ Immutable, isolated backup copies to safeguard against ransomware and insider threats ✔ Long-term retention & governance controls for compliance (beyond Microsoft's 30-day recycle bin) ✔ Policy-based protection to automatically secure new identity objects created in Entra ID **Outcome:** Reduce risk of identity compromise, misconfiguration fallout, and compliance violations before they occur.	✔ Guaranteed clean recovery point even if threat actors poison identity objects ✔ Granular object-level restore (e.g., users, groups, service principals, etc.) ✔ Maintain continuity of access to mission-critical cloud services during identity disruption **Outcome**: Contain identity-based attacks and misconfigurations, preserve access continuity, and avoid operational shutdown	✔ Rapid restore of Entra ID identities and directory structure ✔ Hybrid restore workflows for AD-synced environments—restore cloud and on-prem identities cohesively ✔ Forensic audit trail to validate clean recovery and prove compliance ✔ Restore to known-good last-state to avoid re-injecting compromised identity objects **Outcome**: Dramatically reduce downtime and business interruption after an identity attack or accidental deletion

Cohesity delivers the cyber resilience your Microsoft environments demand. By unifying protection, security, and recovery from before and after an attack across Microsoft 365 and Entra ID, Cohesity ensures that organizations can withstand identity-based attacks and recover with confidence.

Ready to see how Cohesity protects, secures, and recovers Entra ID? Contact Cohesity today to learn more.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

3000183-001-EN 12-2025