DATA SHEET

Quest Identity Security & Resilience

Unified Identity Threat Detection and Response (ITDR) for Microsoft Active Directory and Entra ID, aligned to NIST CSF 2.0 and Gartner's expanded ITDR definition.

Identity is the #1 attack surface. Some security teams can detect an issue. Few can decisively recover from one.

Identity is the primary attack surface, yet most security teams rely on endpoint-centric detection tools and backup platforms that were not designed for AD or Entra ID. As attackers abuse valid credentials and privileges – often without malware – teams receive alerts but lack the ability to prevent identity changes or stop attacks at the directory layer.

At the same time, more than 75% of organizations aren't testing disaster recovery plans often enough. AD and Entra ID recovery capabilities recently added to backup platforms are often limited to basic restore, making it difficult to prove clean recovery or restore identity trust after an attack.

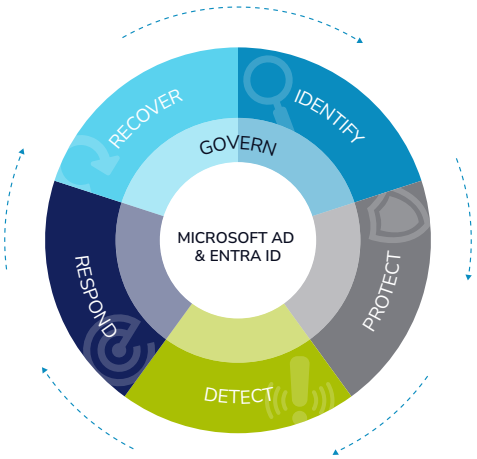
Compounding this: a shrinking pool of identity expertise, expanding hybrid environments, and machine identities now outnumber humans 109:1. Organizations also need to understand not only how identities are configured, but how they are actually used, authenticated, and connected across the environment so they can prioritize meaningful exposure before it becomes an incident.

The result is a fractured identity security model. Organizations get alerts without control, recovery without confidence, and no unified way to identify, prevent, contain, and recover from identity-based attacks. This is exactly why Gartner's expanded ITDR definition and NIST CSF 2.0 now emphasize identity security across the full lifecycle, not detection or restore alone.

Benefits

- 44% improvement in identity MTTR
- 90% faster identity recovery, with $19.7M in average downtime savings
- 24/7 recovery response services included at no extra cost
- Clear alignment to NIST CSF 2.0 and Gartner's ITDR framework
- Trusted by thousands, managing over 60B Entra ID objects and growing 30%+ annually
- 25+ years in Active Directory and 10+ years in Entra ID - more experience than any other vendor
- SOC 2 Type II audited; ISO 27001, 27017, 27018, 27701 certified
- FedRAMP High Authorization

FedRAMP® ISO 27001 CERTIFIED by schellman ISO 27701 CERTIFIED by schellman ISO 27017 CERTIFIED by schellman ISO 27018 CERTIFIED by schellman



Powered by Quest Security Management Platform

Unified ITDR platform aligned to NIST CSF 2.0 and Gartner

Quest Identity Security and Resilience is a unified ITDR solution for Active Directory and Entra ID. Built on decades of experience defending the most critical identity assets, Quest gives security teams control across the full identity attack lifecycle — actively preventing identity attacks, containing privilege abuse during live incidents, and restoring identity trust with attack-tested recovery automated up to 90% faster. Customers improve mean time to response by 44% while reducing downtime and operational risk.

Identify — Continuous identity risk assessment

Quest continuously assesses identity exposure across hybrid AD and Entra ID environments, spanning human, non-human, and supported agentic identities. Beyond identifying critical assets, Tier 0 exposure, privilege risk and misconfigurations, Quest reveals how identities are actually used, authenticated, and connected through observed access chains. This gives security teams a clearer view of where identity exposure is forming, helping them prioritize meaningful risk and reduce exposure before attackers exploit it.

Protect — Active threat prevention

Quest goes beyond alerting by enabling real prevention at the identity layer. Through deep architectural integration with Active Directory, security teams can block unauthorized changes to Tier 0 and other crown jewel assets, including GPOs. GPO governance extends protection by enforcing controlled, auditable policy changes with versioning and rapid rollback, preventing attackers from exploiting Group Policy. Freeze risky identities, preventing them from making changes, adding more flexibility and coverage.

Detect — Earlier, higher fidelity identity detection

Quest detects identity threats earlier in the attack chain by capturing rich audit data that endpoint and alert-only ITDR tools miss – revealing the who, what, when, where, and originating workstation behind every change. Quest's integrated AI-powered detection translates complex, technical findings into human-readable alerts that reduce investigation time and dependency on scarce AD expertise, delivering a 44% improvement in mean time to response (MTTR). A flexible API extends these insights across your existing security ecosystem and custom workflows.

Respond — Shields Up threat containment

In the event of a live security incident, Shields Up and agentic defense capabilities can autonomously execute predefined actions and automatically contain threats. Stop attacker movement and techniques in real time - including DCShadow-style attacks - limiting the blast radius before damage spreads.

Recover — Proven identity recovery at speed

Quest delivers proven, automated recovery of hybrid AD and Entra ID to a known-good, trusted state without reintroducing malicious changes or losing legitimate users and changes. This enables the world's most complex and regulated organizations to rapidly restore critical identity services after ransomware attacks, destructive cyber events, or operational failures. From granular object-level restores to full environment rebuilds, Quest enables up to 90% faster identity recovery with a near zero Recovery Point Objective, lowering business impact, outage duration, and cost per incident.

NIST CSF 2.0 Pillar	Quest capability	Identity Insights, Identity Defense & Identity Recovery	Identity Insights & Identity Defense	Identity Recovery Plus
Identify	Access-chain visibility across human, non-human, and agentic identities	✔	✔	
	Tier 0 and AD/Entra security posture management	✔	✔	
Protect	Threat prevention - Block changes to Tier 0 assets	✔	✔	
Detect	AI-powered threat detection	✔	✔	
	Hybrid identity auditing & visibility - human readable	✔	✔	
Respond	Autonomous threat response - Agentic AI Defense	✔	✔	
	Shields Up emergency containment	✔	✔	
Recover	AD disaster recovery - SaaS delivered	✔		✔
	Granular, object-level recovery - AD	✔		✔
	Granular, object-level recovery - Entra ID	✔		✔
	AD disaster recovery - On-prem delivered, enterprise-scale	✔		✔

"We have peace of mind that we can recover Active Directory … within hours, rather than the days it would have taken with our previous approach."

Head of Infrastructure | Global Manufacturer

About Quest Software

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

© 2026 Quest Software Inc.
ALL RIGHTS RESERVED.
Quest, and the Quest logo are trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks are properties of their respective owners.
Datasheet-ID-Security-and-Resilience-Solution-HO-102831

Explore our solutions →

Quest