DATA SHEET

Quest Security Management Platform

Modern, secure, and resilient identity for the AI era

The Quest Security Management Platform is the industry's first unified, AI-powered platform for identity threat detection and response (ITDR) and secure identity modernization. It protects Active Directory (AD) and Entra ID, securing human and non-human identities across the identity lifecycle.

The platform unifies identity defense, recovery and migration, applying consistent security controls across daily operations and high-risk moments of change, such as migration, AI adoption and M&A. With Quest, organizations achieve a 44% improvement in identity mean time to response (MTTR) and up to 90% faster identity recovery.

What security leaders are facing

Identity is now the primary attack surface, yet most security teams rely on endpoint-centric detection tools and backup and data protection platforms that were not designed for AD or Entra ID. Identity recovery capabilities recently added to these platforms are often limited to basic restore, making it difficult to prove clean recovery or restore identity trust after an attack.

Over 80% of attacks are malware-free, as attackers abuse valid privileges. Security teams receive alerts but lack the ability to prevent identity changes or stop attacks at the directory layer. AI accelerates these attacks and multiplies non-human identities, increasing exposure faster than controls can adapt. Compounding this: migrations and modernization often occur outside established security controls, further expanding privilege and attack surface.

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 pending

Negative business consequences

Identity compromise leads to longer outages, slower recovery, and higher ransomware impact with multimillion-dollar losses. Security teams face alert fatigue without the ability to contain identity attacks, and fragmented tools fail to deliver measurable identity resilience. The downstream effects include audit findings, regulatory exposure, and lost executive confidence.

What you can do with the Quest Security Management Platform

Quest delivers a single, AI-powered platform that enables you to actively prevent and contain identity-based attacks, quickly recover and restore identity trust, and secure migrations throughout the lifecycle. By unifying identity defense, recovery, and modernization, the Quest Security Management Platform ensures that identity security does not pause before, during, and after change.

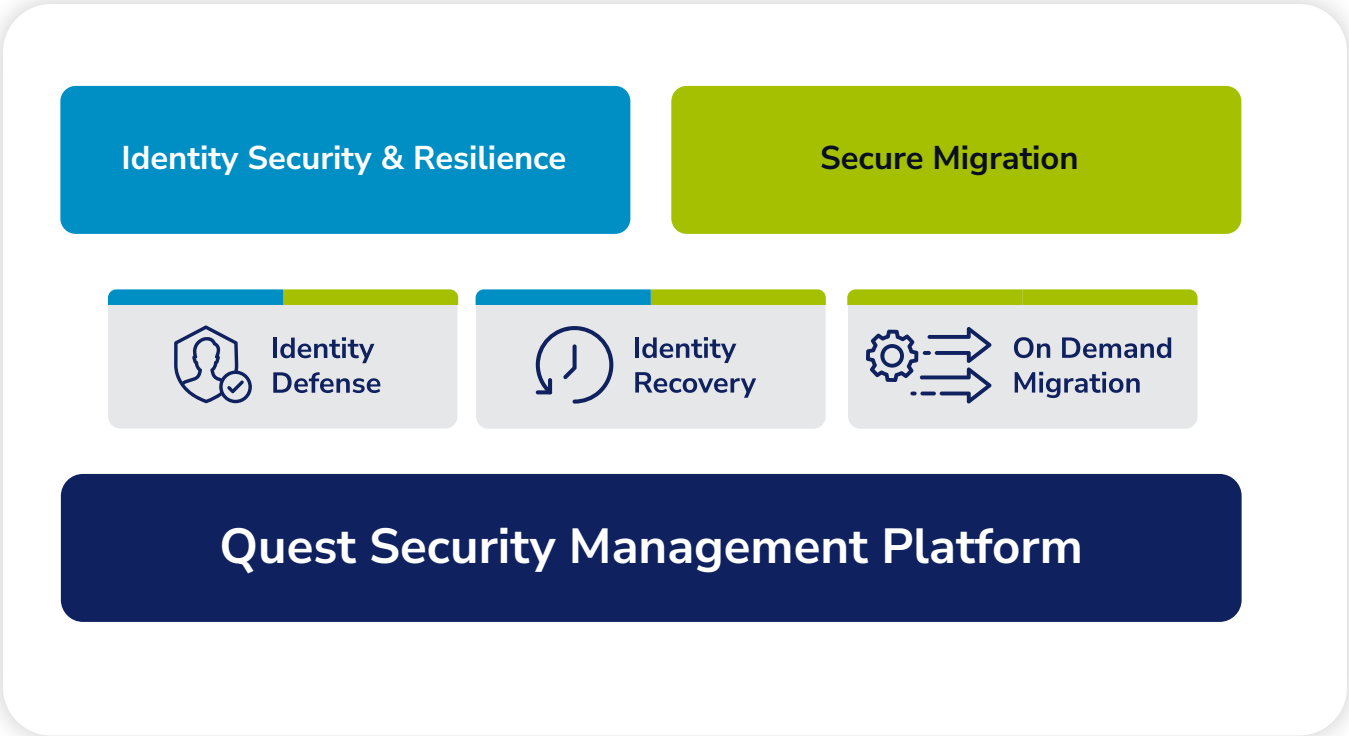
> "Quest Identity Defense is the best tool we could find available for identity threat hunting."
>
> CISO | Large Media Company

ISO 27001 CERTIFIED by schellman

ISO 27701 CERTIFIED by schellman

ISO 27017 by schellman

ISO 27018 by schellman



Key capabilities

- **Proactive identity defense** — Blocks identity-based attacks at the identity control plane, not just at the alert layer. Tier 0 protections and unique Shields Up containment freeze changes to crown-jewel identity assets during active incidents, disrupting attacker persistence and lateral movement before damage spreads. GPO governance extends protection by enforcing controlled, auditable policy changes with versioning and rapid rollback, preventing attackers from exploiting Group Policy.
- **Deep identity visibility** — Provides security-grade visibility into human and non-human hybrid identity activity spanning AD and Entra ID that traditional EDR tools miss – revealing the who, what, when, where, and originating workstation behind every change. Human-readable audit trails surface risky or malicious changes earlier in the attack chain, reducing dwell time and improving MTTR by 44%.
- **Attack-tested identity recovery** — Delivers proven, automated recovery of hybrid AD and Entra ID to a known-good, trusted state without reintroducing malicious 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, lowering disaster impact, outage duration, and cost per incident.
- **Security-first modernization** — Extends ITDR into identity modernization, where risk peaks. Quest treats migration as a security-critical event, enforcing Tier 0 protection, auditing, and recovery readiness so organizations can modernize without sacrificing resilience.
- **Unified ITDR** — Operationalizes Gartner's expanded ITDR framework across prevention, detection, response, and recovery through a single control plane – not a collection of point tools – aligned to NIST CSF 2.0.

25+ year Microsoft partnership

- Microsoft 365 Certified
- Microsoft Intelligent Security Association (MISA) membership
- Available on Azure Marketplace
- Integrates with Microsoft Security Copilot and Microsoft Sentinel
- Complements Microsoft Defender for Identity

"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.

Explore our solutions →

Datasheet-Security-Mgmt-Platform-HO-102709