

DATA SHEET

Quest Identity Insights

See Every Identity Access Chain
Human | Non-human | Agentic

Organizations can already spot accounts that look stale, over-privileged or misconfigured. What they cannot tell is whether those identities are still in use, where, and what breaks if they change. So nothing changes — service accounts, privileged identities, old credentials and legacy authentication sit untouched for years, not for lack of findings but for lack of evidence to act safely.

Machine identities outnumber human identities 109 to 1, up from 82 to 1 a year earlier. This growing population includes service accounts, workload identities, automation and AI agents that may lack clear ownership, lifecycle controls or a recognizable login pattern. In Quest-led assessments, up to 60% of identities hold active privileges and access relationships with no observable activity. A last-logon attribute will not settle it: accounts get used in ways that never update the signals Active Directory and Entra ID rely on, so an identity can look dormant while holding privileged access and live dependencies.

Benefits

- Shrink the identity attack surface by uncovering dormant access and excessive privilege
- Prioritize remediation using observed activity and access chain evidence
- Reduce service account privileges with less risk of operational disruption
- Accelerate Zero Trust, legacy authentication reduction and identity modernization programs
- Cut manual log analysis with one shared view of identity activity and exposure
- Strengthen audit, compliance and cyber insurance readiness with defensible evidence
- SOC 2 Type II audited

Why Now

- **October 2026 is a critical milestone.** Microsoft will strengthen default NTLMv1 restrictions, increasing the risk of disruption for organizations that do not know where the protocol remains in use. Identity Insights reads authentication evidence at the endpoint, helping teams map dependencies before making changes.
- **Agentic identity is already here.** AI agents and automation act on behalf of other identities, creating delegated chains that entitlement views cannot explain. Visibility has to come before governance.
- **Modernization is already underway.** AD modernization, Entra transition, legacy-authentication reduction and M&A all stall on the same question: which identities and authentication relationships are actually live?
- **The category is brand new.** Gartner established Identity Visibility and Intelligence Platforms (IVIP) as a new category in July 2025. With market penetration still below 5%, organizations that act now can address identity blind spots before the category becomes mainstream.

What Quest Identity Insights Is

Quest Identity Insights is an identity visibility and intelligence solution for hybrid Active Directory and Entra ID environments, with deep Active Directory context and Entra ID visibility across the estate. It reveals observed identity relationships and access-chain patterns across human, non-human and supported agentic identities, showing how identities are actually used, authenticated and connected. This helps teams see where identity relationships create exposure, which risks warrant action and what is safe to change.

What an Access Chain Is

Every identity can begin a chain of activity that reaches critical systems and data. These chains can form through direct relationships (roles, groups, delegated permissions), inherited relationships (nested groups, policies, accumulated access) and delegated activity (workloads, automation, APIs and supported agentic identities). Governance helps define what access should exist; Identity Insights reveals the observed relationships and transitions that show how access is used, and how activity and relationships combine to create exposure.

Core Capabilities

- **Continuous identity visibility and intelligence.** Maintain an ongoing view of human, non-human and supported agentic identities across Active Directory and Entra ID. By combining identity inventory and configuration context with observed activity, teams can understand not only how identities are configured, but how they are used.
- **Observed access-chain intelligence.** Uncover identity relationships and transition patterns that may create exposure. An interactive graph view lets teams select identities and resources, explore incoming and outgoing connections, apply filters, and examine authentication methods, access methods, timestamps and repeated observations.
- **Behavior-informed identity analysis.** Identify usage-based dormancy, mixed-use accounts, observed NTLM activity and identities used outside their intended purpose. Connecting observed behavior with the accounts and systems involved helps teams distinguish meaningful exposure from configuration-only findings and plan authentication modernization.

- **Impact-based risk prioritization.** Understand the potential risk impact of identities and observed transitions. Impact Scores and escalation categories help teams identify higher-impact identities, privilege and impact escalation patterns, and relationships that warrant further investigation.
- **Identity exposure and drift management.** Understand how identity activity, access relationships and risk impact change over time. Dashboards, filters, trends and graph views help teams identify emerging exposure, changing dependencies and apparently inactive identities that continue to retain privileges or access relationships.
- **Evidence for informed action.** Bring identity context, observed activity and system dependencies together to support service-account cleanup, credential rotation, access reduction and authentication modernization. Teams can better evaluate operational impact and make identity changes with greater confidence.

Part of Quest Security Management Platform

Aligned to the NIST Cybersecurity Framework (CSF) 2.0 and Gartner's ITDR model, Quest Identity Insights combines identity context with observed activity and access chain evidence to reveal how identities are actually used, authenticated and connected. This helps organizations understand where identity exposure is forming and act with greater confidence. Quest Identity Defense adds identity security posture across Active Directory and Entra ID by identifying critical identity assets, Tier Zero and workload identities, then protects, detects and responds to identity threats. Quest Identity Recovery extends the platform with recovery for hybrid AD and Entra ID, while Quest migration capabilities support identity modernization.

"We use Quest to gain greater visibility into our identity environment. The insights it provides help us better understand identity-related risk and make more informed security decisions. As identity environments become increasingly complex, having clear visibility into potential exposures is critical. We're excited to see these capabilities become part of Quest's broader identity security and cyber resilience strategy."

Jeromy Lease | Director Cybersecurity, SSR Mining Inc.

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 →

© 2026 Quest Software Inc. I ALL RIGHTS RESERVED.
Quest, Quest Software, 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-Quest Identity Insights-HO-105678