DATA SHEET

Hybrid Active Directory Security Assessment

Protect hybrid identity and accelerate threat response with Quest

With hundreds of millions of identity attacks taking place daily, securing identity is essential for maintaining business continuity, particularly in hybrid Active Directory and Entra ID environments. The consequences of failure are dire, with Forrester reporting AD downtime costing up to $730K per hour.

At Quest, we understand the dynamic and increasingly complex nature of identity within today's evolving security landscape. Quest's Active Directory security assessment leverages the powerful capabilities of Identity Defense to deliver an evaluation of your hybrid AD environments and provide insight into the most actionable issues within them, so that you can stay ahead of sophisticated attacks.

How Does It Work?

The hybrid AD security assessment provides a two-week license of Identity Defense and support from Quest pre-sales to install the on-premises hybrid collection agent in any environments scoped for inclusion in the assessment.

Benefits

- Summarize identity security posture, including critical and high findings
- Identify and list Tier 0 objects
- Analyze key security hygiene items
- Export AI summary of findings
- Compare how common your vulnerabilities are next to similar sized organizations
- Review findings with Quest experts

Setup Process

Quest pre-sales will participate in an initial meeting to assist with:

- **Environment and Hybrid Agent Setup** — Our experts will guide you through the process of setting up your environment and installing the hybrid agent. The first data collection will establish a baseline for the assessment.
- **Identification of Custom Tier 0 Objects** — Collaborating with your team, we will identify and catalog any custom Tier 0 objects within your environment. These objects are critical to your security posture and must be accurately assessed.

Assessment Results

Assessment results are available within the Quest Identity Defense portal.

The assessment results provide a deep dive into your identity security, highlighting critical areas of concern and offering actionable insights. The results include two key elements

- **Tier 0 Objects Output** — All Tier 0 objects collected by the security assessment hybrid agent will be displayed, including the reasons why each object is considered Tier 0. This list is exportable as a CSV file for your records.
- **Security Hygiene Items Output** — All identified issues are available within the Identity Defense portal. Details for each issue include all affected objects, the reason why the issue is problematic, and the activities that are needed to remediate the issue.
- **Entra ID and AD Workload Identity Analysis** — Inventories of Entra ID Service Principals and Active Directory Service accounts are available within the portal and can be easily exported.
- **Summary Report** — Exportable summary of all identity vulnerabilities detected by Identity Defense summarized in a report.

The encrypted assessment data is only visible to you and will be deleted from the Identity Defense portal shortly after the two-week license expires. Quest pre-sales will walk you through the assessment results over a screen share to answer questions and provide context around your assessment.

Requirements

The Identity Defense Hybrid Agent is the only on-premises component needed. In order to install the component, the following is required:

- **Windows PC with Internet Access** — The Identity Defense Hybrid Agent requires a Windows PC with internet access to run. This does not need to be a server, as the collection process is a one-time event.
- **Administrative Collection Account** — An account with local administrative rights to the Windows PC and domain user rights to each domain the agent will collect data from is required. This account does not need to be dedicated solely to this task.
- For environments with multiple domains or forests that do not have trusts with each other, multiple hybrid agents may need to be deployed.

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 →