

Active Directory Security Assessment

Protect Tier Zero and enhance security hygiene with Security Guardian

Cybersecurity threats are more sophisticated than ever. Identity platforms such as Microsoft Active Directory (AD) and Microsoft Entra ID are facing challenges in safeguarding digital infrastructure. Identity management is complex and fraught with misconfigurations and vulnerabilities; with 80 percent of breaches now involving the use of compromised identities, AD has become a prime target. The consequences of AD downtime are dire, with staggering costs reaching \$730K per hour, as reported by Forrester.

At Quest, we understand the dynamic and increasingly complex nature of Identity and Access Management (IAM) roles within today's intricate security landscape. Quest's Active Directory security assessment leverages the powerful capabilities of Security Guardian to deliver an evaluation of your AD environment and provide insight into the most actionable issues within it, so that you can stay ahead of sophisticated attacks.

How Does It Work?

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

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 Zero Objects:** Collaborating with your team, we will identify and catalog any custom Tier Zero 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 Security Guardian portal.

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

- **Tier Zero Objects Output:** All Tier Zero objects collected by the security assessment hybrid agent will be displayed, including the reasons why each object is considered Tier Zero. This list is exportable as a CSV file for your records.
- **Security Hygiene Items Output:** All identified issues are available within the Security Guardian 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.

The encrypted assessment data is only visible to you and will be deleted from the Security Guardian 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 Security Guardian 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 Security Guardian 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.

Benefits:

- Summarize AD security posture, including critical and high findings
- Identify and list Tier Zero objects
- Analyze key security hygiene items
- Obtain extensive findings in CSV format
- Review findings with Quest experts

About Quest

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Microsoft 365 migration and management, and cybersecurity resilience, Quest helps customers solve their next IT challenge now. Quest Software. Where next meets now.