# Active Directory Security Assessment

## Overview

The purpose of the **Active Directory Security Assessment** Services Offering is to detect current threats, identify misconfiguration, and recommend remediation activities for managing risks to AD and Entra ID. Based on a collaborative planning session, Quest experts will install security tools in your environment to identify vulnerabilities. Data gathered by the tools and corresponding staff interviews will be analyzed to produce an assessment and recommendations for immediate implementation.

As part of the engagement, the Quest team will conduct a workshop to review the security findings, highlight prioritized vulnerabilities, and discuss potential remediation steps where applicable. In addition, Quest will provide guidance for how your staff can repeat the assessment after recommendations have been implemented.

## Approach and Activities

The following phases are included in the scope of the **Active Directory Security Assessment** Service offering:

### Install and Configure Security Tools

- Quest Identity Defense
- Quest Change Auditor

### Data Collection and Analysis

- Once configured, the security tools will gather data for two (2) to five (5) days. During this time the Quest team will interview your resources to collect information related to administration of Active Directory, including: privileged access management, disaster recovery planning, tier zero or control plane segmentation, Group Policy administration, and delegated administration.
- Quest Identity Defense and Quest Change Auditor evaluate both on-premises Active Directory and Entra ID environments.
- Quest will document the current AD and Entra ID security state and recommendations. You will be provided a prioritized list of key threats along with recommended remediation actions in a Security Findings Report.

### Security Findings Workshop

Quest will schedule up to two (2) workshop sessions (up to four (4) hours each) with you to review the following:

- Contents of the Security Findings Report, including prioritized vulnerabilities and risks identified, with discussion of potential remediation steps where applicable.
- Interactive review of recommended remediation actions, including implementation guidance and priority sequencing.
- Demonstration of security tools to conduct future security assessments.

## Prerequisites and Assumptions

As part of the offering, you agree to cooperate with Quest in its delivery of the Services and to the following responsibilities:

- Scope of the engagement is limited to a single Active Directory Forest and Entra ID tenant.
- Remediation of identified misconfiguration or vulnerabilities is not within scope of this engagement. Should evidence of an active compromise be discovered, the engagement will be suspended while you remediate the breach. Incident response and risk remediation services can be purchased under separate contracts.
- Ensure that the existing infrastructure configuration of their environment is sufficient to support the products to be implemented, based on published product documentation. This includes hardware, service accounts, database, and permissions.
- Commit a technical resource on a full-time basis to provide Quest with the assistance required.
- Provide project team members with suitable business expertise, technical expertise, and decision-making authority to ensure efficient project progress.
- You will provide current account provisioning and deprovisioning workflow including accounts with elevated privileges.
- Ensure that required network connectivity is in place between the servers with Quest software deployed, Quest SaaS platform and all domain controllers, servers, and in scope Entra ID tenants.

| SKU | |
|---|---|
| **BBC-QOD-PP** | Active Directory Hybrid Security Assessment |