

Quest Security Guardian

Stay ahead of cyberattacks targeting Active Directory with an AD security solution that spotlights what happened, what was exposed, and how to fix the problem.

Quest Security Guardian is an Active Directory security tool designed to reduce your attack surface. From a simplified, unified workspace, Security Guardian reduces alert fatigue by prioritizing your most exploitable vulnerabilities and Active Directory configurations that demand attention. The solution spotlights what happened, if you're exposed, and how to fix the problem.

Protect your critical Tier Zero assets with the ability to:

- Benchmark current Active Directory configuration against industry best practices
- Lock down critical objects, including GPOs, from misconfiguration and compromise
- Stay ahead of threats by continually monitoring for indicators of exposure (IOEs) and indicators of compromise (IOCs)

Securing identity is essential to maintain business continuity across your organization — especially Active Directory (AD). The consequences of AD downtime are dire, with costs reaching a staggering \$730K per hour, as reported by [Forrester Consulting](#). Plus, when you consider that 80 percent of breaches

now involve the use of compromised identities, AD has become a prime target. Quest Security Guardian will help you reduce your AD attack surface with simplicity and speed.

AD Security Assessment

Benchmark current Active Directory configuration against pre-defined industry best practices. You'll have full visibility into IOEs, IOCs and Tier Zero assets. This Active Directory security tool not only helps with threat mitigation, but also attack surface reduction.

Critical Asset Focus

Identify and prioritize Tier Zero assets effortlessly, ensuring that your most exploitable components receive the utmost attention. Gain full control over these critical assets, enabling you to modify the Tier Zero list dynamically, so you're always aligned with your organization's evolving needs.



Benefits:

- Reduce the attack surface by assessing your AD against industry best practices
- Simplify AD security with total visibility, control and protection of critical assets
- Mitigate AD configuration drift and stay one step ahead of attackers
- Avoid alert fatigue and identify real threats by focusing on high-value alerts
- Weave together IOC and IOE security signals, ensuring swift threat response

AD Threat Prevention

Secure critical AD objects from compromise and misconfiguration, including sensitive GPOs. This Active Directory security tool delivers focused reports on object status, giving you the context needed to take appropriate action.

AD Threat Detection

Stay on top of your threat mitigation goals by using this Active Directory security tool to continuously monitor for IOCs and configuration drifts, ensuring that you'll be well-prepared for a fast response to potential security incidents.

Fast Incident Response

Grasp the who, what, where, how and when of suspicious activities with intelligent and contextual notifications that will help reduce alert fatigue. Seamlessly forward IOEs and IOCs to your SIEM tools, such as Microsoft Sentinel and Splunk, for seamless integration and centralized visibility.

Unified AD Security Workspace

Focus on core operations with a friendly user interface that provides visibility into IOEs, IOCs and other security signals seamlessly.

“Rebuilding an AD object that was improperly modified could take hours, which would impact operation ... Quest object protection enables us to prevent such issues from arising in the first place.”

Alessandro Bottin, Global Infrastructure & Operation Manager, Prysmian Group

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.