Quest Security Guardian

Stay ahead of cyberattacks with a hybrid AD security solution that spotlights what happened, what was exposed, and how to fix the problem.

Quest Security Guardian is a Hybrid Active Directory security solution designed to significantly reduce your attack surface. From a streamlined, unified workspace, Security Guardian alleviates alert fatigue by prioritizing the vulnerabilities and configurations that pose the greatest risk to your organization. Powered by Azure AI and Deep Machine Learning (ML), and now seamlessly integrated with Microsoft Copilot for Security, Security Guardian not only spotlights what happened, if you're exposed, and how to remediate, but it also accelerates identity threat responses, simplifies complex security and empowers your team with advanced AI expertise.

Protect your critical Tier Zero assets with the ability to:

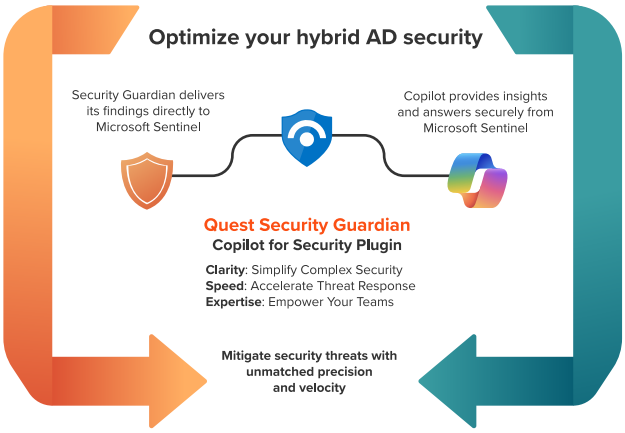
- Benchmark your current Active Directory configuration against industry-leading security hygiene practices.
- Lock down critical objects, such as GPOs, from misconfiguration and compromise.
- Continuously monitor anomalous user activities and emerging hacker tactics, techniques, and procedures (TTPs) with Machine Learning.

- Leverage cross-product AI insights from Microsoft Copilot for Security to simplify and accelerate threat detection and response.

Securing identity, particularly in hybrid environments with Active Directory and Entra ID, is crucial for maintaining business continuity. Forrester reports downtime costs as high as $730K per hour, and with 80% of breaches involving compromised identities, these systems have become prime targets. Security Guardian mitigates these risks by using Machine Learning to establish behavioral baselines, detecting unusual patterns like spikes in account lockouts, failed sign-ins, and permission changes. Through integration with Microsoft Copilot for Security,

Benefits:

- **Reduce attack surface by assessing your hybrid AD against industry best practices**
- **Simplify AD and Entra IDsecurity with total visibility, control and protection of critical assets**
- **Leverage Microsoft Copilot, AI and Machine Learning to identify anomalous behavior and accelerate threat response**
- **Mitigate hybrid 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 security signals, ensuring swift threat response**



it extends detection and response capabilities, providing seamless protection across your hybrid AD environment.

Hybrid AD Security Assessment

Benchmark current hybrid Active Directory configuration against pre-defined industry best practices. You'll have full visibility into vulnerabilities, hacker tactics, techniques and procedures (TTPS) and Tier Zero assets. This hybrid AD 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.

Hybrid AD Threat Prevention

Secure critical AD and Entra ID objects from compromise and misconfiguration, including sensitive Group Policy Objects (GPOs). Get focused reports on object status, as well as the ability to effortlessly revert any unwanted changes to a previous, trusted state.

Hybrid AD Threat Detection

Leverage AI and Machine Learning to automatically detect anomalous behaviors within Active Directory and Entra ID, such as unusual spikes in account lockouts, failed sign-ins, permission changes, and file renames. By identifying these anomalies early, Security Guardian helps you stay on top of threat mitigation goals and predict potential compromises before they escalate. Continuously monitor for hacker TTPs (Tactics, Techniques, and Procedures) and configuration drifts, ensuring faster response times and reduced false positives.

> **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.**
>
> *Allessandro Bottin, Global Infrastructure & Operation Manager, Prysmian Group*

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 security signals to your SIEM tools, such as Microsoft Sentinel and Splunk, for seamless integration and centralized visibility.

Unified Hybrid AD Security Workspace

Remove the complexity from AD and Entra ID security by focusing on core operations with a friendly user interface that provides visibility into exposures, vulnerabilities and other security signals seamlessly.

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.