DATA SHEET

Quest Security Guardian

Simplify and accelerate ITDR with a GenAI-powered hybrid AD security solution

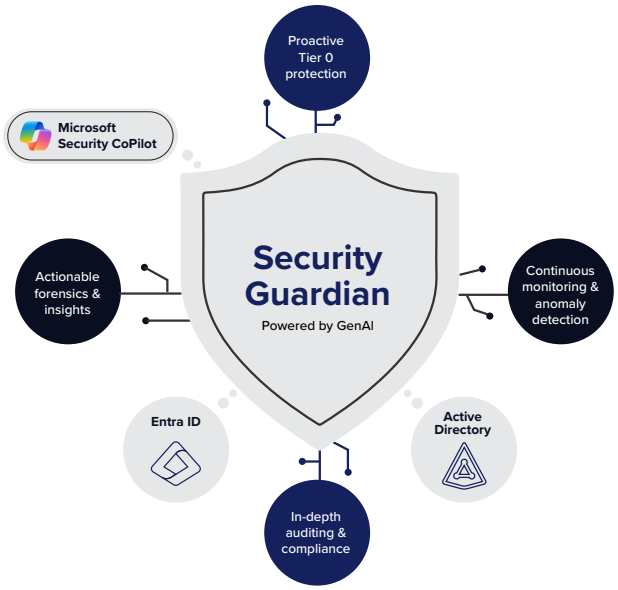
Powered by Generative AI and seamlessly integrated with Microsoft Security Copilot, Security Guardian accelerates hybrid AD threat detection, containment and response while minimizing downtime and exposure. From a unified workspace, it identifies and prioritizes high-risk misconfigurations and exposures and proactively safeguards critical objects to prevent threats before they escalate.

Simplify security and protect Tier 0 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).
- Leverage Generative AI intelligence to simplify and accelerate threat detection and response.

Benefits

- Reduce attack surface by assessing your hybrid AD against industry best practices
- Simplify AD and Entra ID security with total visibility, control and protection of critical assets
- Leverage Generative AI, Machine Learning and Microsoft Security CoPilot to identify anomalous behavior and accelerate threat response
- Stop attacks in real time by disrupting lateral movement and persistence techniques before they escalate
- Avoid alert fatigue and identify real threats by focusing on high-value alerts
- Weave together security signals, ensuring swift threat response



With 600 million identity attacks taking place daily, securing identity is essential for maintaining business continuity, particularly in hybrid environments with Active Directory and Entra ID. The consequences of failure are dire, with Forrester reporting AD downtime costing up to $730K per hour. Unfortunately, identity security is complex, and many organizations face a shortage of expertise and resources, making it even harder to efficiently detect and respond to threats across sprawling, misconfigured environments.

Security Guardian addresses these challenges with powerful Generative AI and Machine Learning capabilities that empower organizations to detect anomalous behaviors, reduce alert fatigue, and proactively protect critical assets. Integrated with Microsoft Security Copilot, it delivers intelligent, automated identity threat detection and response across hybrid AD.

Hybrid AD Security Assessment

Benchmark your current configurations against pre-defined industry best practices. Surface exposures and compromises that exist within the environment. Quickly mitigate these risks and reduce your attack surface..

Critical Asset Focus

Identify and prioritize Tier 0 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 0 list dynamically, so you're always aligned with your organization's evolving needs.

Proactive Threat Prevention

Activate dynamic, in-memory protection for Tier 0 assets, including sensitive GPOs, with the Shields Up capability. Contain incidents mid-flight by disrupting lateral movement and persistence techniques before they escalate, so you can protect critical systems in real time, not after damage is done. Get focused reports on object status, as well as the ability to effortlessly revert any unwanted changes to a previous, trusted state.

Automated Threat Detection

Leverage Generative AI and Machine Learning to detect unusual activity in Active Directory and Entra ID, such as spikes in account lockouts, failed sign-ins, permission changes and file renames. Continuously monitor hacker TTPs (Tactics, Techniques and Procedures) and audit changes. With one click, Security Guardian GenAI Intelligence translates data into business-relevant summaries, enabling security teams to streamline investigations and effectively communicate risk to executives and stakeholders.

Intelligent Incident Response

Quickly understand the who, what, where and when of threats by connecting anomalies and highlighting key security signals. Security Guardian's Generative AI delivers intelligent and contextual notifications, tailored remediation guidance and actionable recommendations designed for your environment, for faster, more confident risk mitigation. Seamlessly forward data collected to SIEM tools like Microsoft Sentinel and Splunk for integrated visibility and streamlined operations.

Microsoft Security Copilot Integration

Security Guardian integrates with Microsoft Security Copilot to provide comprehensive protection for your hybrid AD environment. By combining the strengths of both platforms, you gain a powerful solution that simplifies complex security threats, accelerates your response times, and empowers your security team to operate at peak efficiency.

Unified 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.

"Security Guardian is the best tool we could find available for identity threat hunting in Active Directory."

CISO, Large Media Company

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 →

Datasheet-MPM-SecurityGuardian-HO-99746