CONTINUITY

StorageGuard

StorageGuard

Security posture management for storage and data protection systems

The tactics being used by ransomware groups have changed. And it puts organizations' storage and data protection environments at major risk.

The attackers realize that an attack on the storage or data protection environment is the single biggest determining factor to show if the organization will pay the ransom.

ESSENTIALS

Ensure your storage and data protection systems are continuously hardened, to withstand ransomware and other cyberattacks

Eliminate manual security validation efforts, and continuously validate against your security baseline

Eliminate configuration drift – by tracking security configuration changes

Leverage remediation guidance to speed time-to-resolve

Meet IT audit requirements, providing evidence for compliance

Security hardening for storage and data protection systems

StorageGuard provides security hardening for all storage and data protection systems, to improve your security posture, enable cyber-resiliency, and meet IT audit requirements.

StorageGuard checks the security configuration of your storage and data protection systems - ensuring those systems are hardened, meet security best-practices, and comply with standards/baselines.

For the first time, get complete visibility of security risks across these mission-critical systems, and ensure compliance with security regulations and industry standards.

Discover

Continuously analyzes your storage & data protection systems, to automatically detect security misconfigurations and vulnerabilities, The built-in knowledgebase of checks covers:

- Security best-practices from Dell and other storage & backup vendors
- Standards (NIST, ISO, CIS, SNIA, PCI etc.) as applied to storage & backup
- Vulnerabilities (CVEs) in the storage & backup environment
- Commonly used security baselines

Prioritize

Prioritizes those risks in order of urgency and business impact.

Remediate

Provides clear security remediation commands and guidance, which can be integrated into your IT service management and SIEM workflows.

For every finding, StorageGuard provides detailed remediation commands for your team to quickly resolve the issue. This can also be integrated into your IT service management and SIEM workflows.

Improve your security posture

StorageGuard improves the ransomware-readiness and overall security posture of your storage and data protection systems. We reduce the effort required by IT operations and storage teams to develop and enforce security policies, prove compliance for audit, and chase down false positive CVE alerts raised by tools that aren't storage-aware.

Meet IT Audit requirements

StorageGuard provides broad storage and data protection system support, and an extremely wide knowledgebase of automated checks, built on industry standards (e.g., NIST, ISO, and CIS), regulatory frameworks (PCI/DSS), and Dell best practices. This makes it easy to audit and report on security misconfigurations and vulnerabilities across your entire storage and data protection infrastructure.

Fills a major gap

StorageGuard fills a critical gap in security posture management. Existing tools by the likes of Tenable's Nessus, Qualys and Rapid7 provide almost zero coverage for storage and backup systems.

CONTINUITY