COHESITY

core6

[* * * *]

StorageGuard

Keep Your Cohesity Environment
Continuously Hardened

StorageGuard

Continuous security configuration validation for Cohesity and your entire storage and backup estate, so your recovery layer stays hardened and compliant.

Cohesity gives enterprises a comprehensive set of features to keep data secure. While StorageGuard, by Core6, ensures the infrastructure underneath that data is continuously hardened.

That matters more every day: AI-driven threats have shrunk the exposure window from months to seconds, so periodic checks can no longer keep up.

StorageGuard detects misconfigurations, vulnerabilities and configuration drift across Cohesity components and across your heterogeneous storage and backup systems around them.

Together, Cohesity and Core6 help enterprises protect both their data and the systems that hold it.

The challenge: secure data depends on securely configured infrastructure

Comprehensive protection of storage and backup needs two things working together:

Intact content	Hardened infrastructure
Primary and backup data must stay free of malware, using antivirus, file analysis, anomaly detection and similar tools.	The storage and backup systems holding that data must be configured securely and be free of known vulnerabilities, verified through configuration compliance and authenticated scanning, not only network vulnerability scans.

Your backup system can be configured correctly on day 1 and still be exposed on day 2. Knowledge gaps and configuration drift create non-compliance and openings that cybercriminals can exploit, putting every piece of primary and backup data on that system at risk.

Enterprises also face strict requirements set by security standards such as NIST, ISO, DORA, and PCI, and must prove they meet them.

> The question for every Cohesity customer: how do you know that DataPlatform, DataProtect, Helios, SmartFiles, agents, connectors and the other components in your environment are configured to security best practices, and free of vulnerabilities?

The solution: StorageGuard for Cohesity environments

StorageGuard is an enterprise-grade security posture management solution built to help organizations securely configure their complete backup and storage estates.

It scans Cohesity components and the systems around them, compares what it finds to security best practices, vendor guidance and industry standards, and shows exactly where the environment has drifted, and which security features are deployed and which are not.

KEY CAPABILITIES

- **Misconfiguration detection.** Finds security misconfigurations and best practice violations
- **Vulnerability detection.** Surfaces security advisories and vulnerabilities affecting storage and backup systems
- **Compliance checks.** Detects non-compliance with industry standards such as NIST, ISO, DORA and PCI

One Security Lifecycle Center for the whole estate

Most customers run Cohesity alongside other storage and backup platforms. For those heterogeneous estates, StorageGuard acts as a Security Lifecycle Center: one place to assess, score, track and remediate the security posture of your entire backup and storage estate, not just one vendor's slice of it.



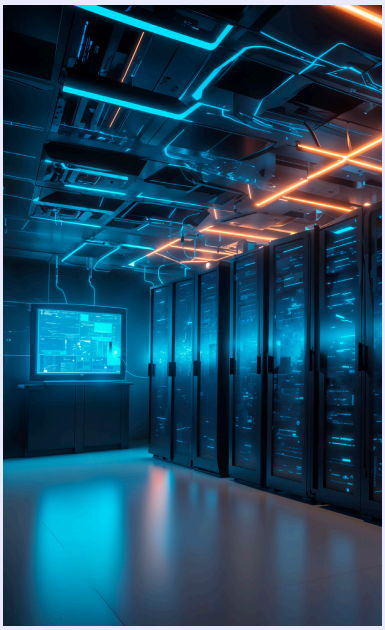
Coverage across your Cohesity and heterogeneous estate

StorageGuard checks that each layer of the environment is configured to security best practices and is not vulnerable.

Layer	What StorageGuard assesses
Cohesity platform	DataPlatform, DataProtect, Helios, SmartFiles, agents, connectors and other components
NetBackup	Master, media, agent and appliance components
Backup destinations	The storage systems that receive backups
Primary storage	The systems being backed up, from vendors such as Dell, NetApp, Hitachi Vantara, IBM, Everpure, HPE, VAST Data, and more

Benefits

- **Full visibility.** See every storage and backup vendor, model and version in the estate, and the findings against each one, in a single view
- **Smaller attack surface.** Catch misconfigurations, vulnerabilities and drift before they can be exploited
- **Audit-ready compliance.** Measure adherence to NIST, ISO, PCI and internal policies, with scores and evidence security and audit teams can use
- **Faster remediation.** Push findings into ITSM so the right team owns each fix and progress is tracked to closure, or use StorageGuard's "Fix it" auto-remediation to resolve findings automatically
- **One lifecycle across vendors.** Apply the same security posture process to Cohesity and to every other storage and backup platform in the environment



www.core6.com/Cohesity