SentinelOne

DATA SHEET

Threat Detection for NetApp

AI-Powered Cloud Data Security

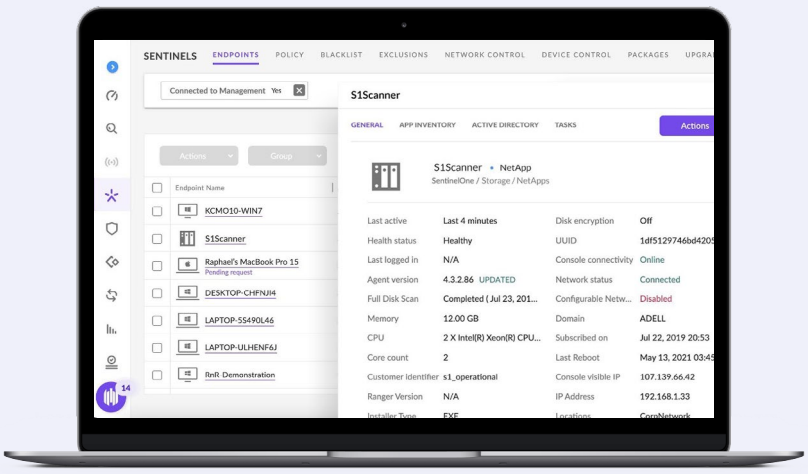
Network-attached storage devices contain volumes of data vital to your business. With ready access available to so many users, protecting your NetApp All-Flash Arrays from malware is critical to operational security.

Modern cyber attacks readily evade signature-based AV, thereby requiring modern cyber defenses to detect and thwart such attacks. Such protection must not come at the expense of performance, so that your business users have a seamless experience when accessing the files they need to work effectively.

Part of the Singularity Cloud Data Security product line, Threat Detection for NetApp is a new cloud data security solution from SentinelOne that is laser-focused on protecting your organization from file-based threats. By bringing SentinelOne's proprietary cybersecurity defenses directly to NetApp storage, customers can conveniently manage storage security in the same SentinelOne Management Console they use for user endpoints, cloud workload protection, and more. In-line file scanning delivers verdicts in milliseconds.

Prevent the spread of malware. Protect your NetApp All-Flash Arrays. Protect your business.

Conveniently manage NetApp All-Flash Arrays security within the SentinelOne Management Console



HIGH PERFORMANCE, LOW LATENCY PROTECTION FOR NETAPP ARRAYS

KEY FEATURES

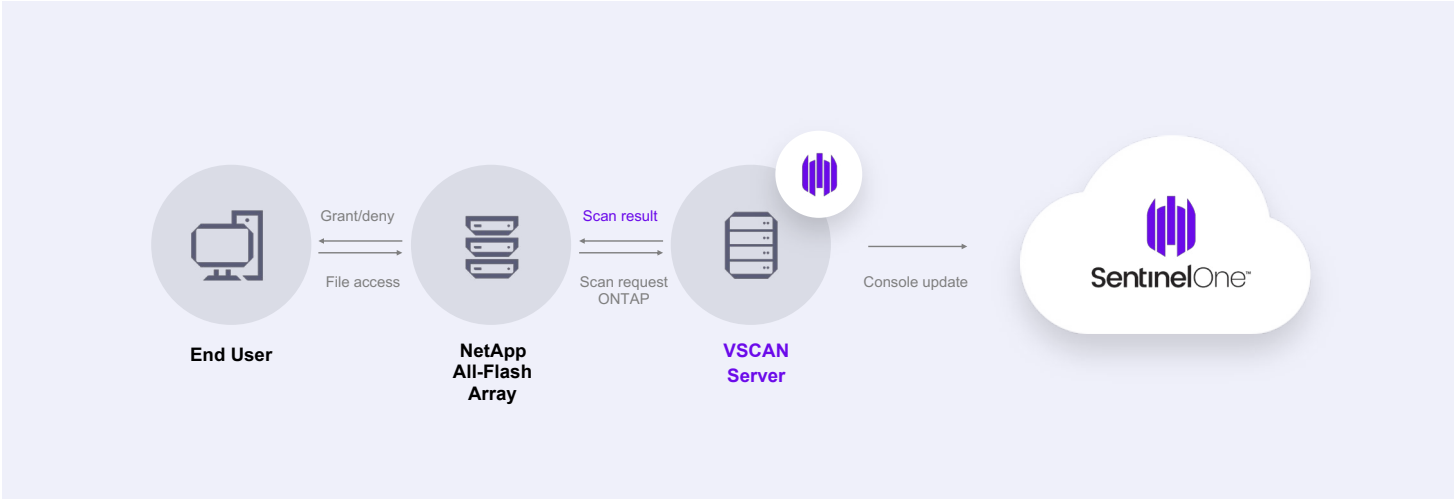
+ In-line file scanning via SentinelOne's advanced ML and Cloud Intelligence Engines
+ File quarantine / unquarantine
+ File exclusions and user block list
+ File fetch of quarantined and encrypted threats
+ Threat metadata, including endpoint from which the threat originated
+ Configurable policy-based response automation
+ A single console for user endpoints, cloud workloads, IoT, and storage
+ Supported by NetApp

Gartner peerinsights™

"Great customer service, even better product.

★★★★★

SENIOR DIRECTOR, IT
Healthcare



Key Capabilities

- **Multi-layered protection** against file-born malware and zero-day attacks via the SentinelOne advanced ML and Cloud Intelligence Engines.
- **Scalable storage protection** with load balancing for optimized performance across multiple All-Flash Arrays.
- **In-line file scanning** that delivers a verdict in milliseconds, for a seamless user experience that does not sacrifice security.
- **Automated quarantine** and encryption of malicious files prevents the spread of malware.
- **File fetch**, together with threat metadata to streamline threat analysis. Includes details on the originating endpoint, even if it is unmanaged or outside the organization.
- **Convenient unquarantine** for admins directly in the console
- **File exclusions and user block lists** simplify management

KEY BENEFITS

+ Easy configuration, available as 100% SaaS
+ Detect malware & zero-days in milliseconds
+ Prevent file storage from spreading malware
+ Streamline threat file analysis
+ Unquarantine files as needed
+ One security management console spans storage, endpoint, CWPP, and more

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2022 Magic Quadrant for Endpoint Protection Platforms

MITRE ENGENUITY

Record Breaking ATT&CK Evaluation

- 100% Protection. 100% Detection
- Top Analytic Coverage, 3 Years Running
- 100% Real-time with Zero Delays

Gartner Peer Insights

96% of Gartner Peer Insights™

EDR Reviewers Recommend SentinelOne Singularity

FedRAMP · TEVORA PCI DSS Attestation HIPAA Attestation · AICPA SOC · STAR LEVEL ONE · VB100 VIRUS · SE Labs BEST Innovator WINNER 2021 · AAA · Trusted Cloud Provider CSA

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.

sentinelone.com

sales@sentinelone.com
+ 1 855 868 3733