StorageGuard™

FOR NETWORK-ATTACHED STORAGE (NAS) DEVICES

BACKGROUND

Organizations use network-attached storage (NAS) devices to centrally store petabytes of files, and share them over the network with groups of users within the organization.

In addition, backup devices often use NAS devices as targets for storage of backup sets (either writing to NAS shares or utilizing NAS-specific archiving features).

Whether for production data or for backup, NAS devices are specialized for file storage and access by their hardware, software and configuration, and are often manufactured as proprietary storage appliances.

Examples of leading Enterprise Storage devices offering NAS capability:

NetApp FAS	Dell EMC Unity	Dell EMC VNX
Dell EMC PowerScale	Hitachi NAS Platform (HNAS)	Dell EMC Isilon
Pure Storage FlashBlade NAS	HPE StoreEasy	Infinidat Infinibox
Dell EMC PowerProtect DD	HPE StoreOnce	Dell EMC Data Domain

CHALLENGES

Cyberattacks on NAS devices have become increasingly common.

Ransomware strains such as REvil and eCh0raix specifically target NAS devices and threaten to destroy petabytes of data kept within them.

Since NAS devices are connected to many endpoints, they also serve as fertile ground to spread malware like wildfire. Considering the size and critical nature of data stored on central NAS devices, most organizations cannot afford for them to be breached.

A compromised NAS device will lead to significant reputation loss and may not allow the organization to continue to function – without its central data storage system.

Furthermore – when NAS devices are also the targets for backup, successful attacks could not only compromise production data, but would also eliminate all possibility of recovery from a recent copy.

Subsequently, it is imperative to harden and continuously validate the security settings and vulnerabilities of all NAS devices.

Traditional vulnerability management tools focus on the host operating system and web applications. They don't protect storage devices - including NAS devices - from security misconfigurations and vulnerabilities, that can be exploited by malicious actors.

StorageGuard by Continuity is the ONLY solution that secures the data storage and backup layer: including block, SAN, NAS, Object, Backup and other types of data storage and backup systems.

By scanning NAS devices and automatically identifying NAS security misconfigurations and vulnerabilities, StorageGuard allows organizations to improve the security posture of NAS devices, thus significantly reducing the risk of a breach or malware.

StorageGuard also provides remediation guidelines for detected security configuration issues and vulnerabilities, to help you resolve them quickly and seamlessly.

StorageGuard uses a vast and continuously updated risk knowledgebase of thousands of security best practices, guidelines, recommendations, advisories and alerts from storage and backup vendors, industry security standards and the community of organizations.

WHAT'S IN IT FOR YOU

Ransomware preparedness

StorageGuard validates whether Anti Ransomware features such as file policies and immutable copies have been enabled and configured correctly and consistently.

File share & exports security

StorageGuard identifies security misconfigurations for SMB (CIFS) file shares and NFS exports such as unsecure share access lists, permissive share access rights.

In addition, StorageGuard also validates authentication settings, encryption and other aspects of the protocols used for file access.

Protocol security

StorageGuard validates that a variety of protocols used by NAS devices are properly hardened and secured. For example: that obsolete versions of file sharing protocols are disables, that NDMP – a backup management protocol is properly secured (or disabled – if not in use), that monitoring protocols, such as SNMP are properly hardened to prevent exploits, that block access protocols, that are sometimes also enabled on NAS (such as iSCSI, or even native Fibre-Channel) are properly hardened.

NAS management plane security

If malicious actors gain access to NAS management interfaces - whether through the NAS device command line, API or web interfaces, or through NAS management software deployed in the datacenter - they can delete, encrypt, shutdown or leak NAS data volumes.

StorageGuard checks how well-hardened the management plane is, including authentication, authorization, services, protocols, interfaces ports, administrative access points and more.

Vulnerability management

Like Host OS and applications, Storage Operating Environments (OE), firmware and software components suffer from vulnerabilities and exposures that can be exploited by attackers to bypass authentication, perform unauthorized actions, and wreak havoc in the NAS device and data stored on it.

StorageGuard includes the most comprehensive and up to date knowledgebase of security advisories, bulletin, alerts and CVEs for Storage and Backup components, and can automatically detect whether NAS devices are vulnerable and how.

Auditing and logging

Auditing configuration changes and security-related events in NAS devices is of the utmost importance. Often, proper auditing could provide an early notice that attacks are being initiated – days, or even weeks in advance.

StorageGuard provides comprehensive validation that different aspects of auditing are properly considered and correctly implemented. These include: access and failed access attempts, configuration changes, logging redundancy, etc.

Compliance with industry frameworks

Many industry-specific regulations (NIST, FFIEC, NERC CIP, PCI and others) provide general guidance that also applies to NAS devices. Existing auditing processes and frameworks often overlook these aspects.

Many organizations report that external auditors pay much closer attention today to inspecting NAS-related security aspects – such as implementing a strong security baseline and tight access control for both data and management planes.

Adherence to vendor specific security recommendations

Storage and backup vendors provide extensive security configuration guides and articles but do not necessarily ship the NAS devices with a secure configuration out of the factory, nor they provide comprehensive and easy-to-use tools for validating and hardening security settings.

StorageGuard has a built-in risk knowledge base that is continuously updated to automatically check for all vendor-provided security guidelines, allowing organizations to control and improve their NAS storage security posture.

Want to learn more?

Contact us

StorageGuard secures your storage and backup systems, to help you protect your data.
It scans data storage, storage management, and backup systems for vulnerabilities and misconfigurations. For the first time, organizations can have complete visibility of their storage and backup security blind spots, with the most urgent risks automatically prioritized.