CONTINUITY

StorageGuard
Pre-Sales Guide and FAQs
For Partners

For any questions or requests, please email JasminH@ContinuitySoftware.com (Head of Channels) and YanivV@ContinuitySoftware.com (Product Management)

Last updated: August 2022

CONTINUITY

Contents

CONTINUITY

-- VALUE PROPOSITION --

How to describe StorageGuard in a sentence?

StorageGuard scans and detects security misconfigurations and vulnerabilities for mission-critical Storage and Backup systems, enabling organizations to harden Storage and Backup Systems to withstand ransomware and other forms of cyberattacks.

How to describe StorageGuard in a single paragraph?

The increase in ransomware and other cyberattacks on internal network systems has made organizations realize that internal high-value IT assets must be protected. Storage and Backup systems retain all mission-critical data including recovery and backup data copies, effectively serving as the final line of defense against ransomware and other forms of cyberattack. StorageGuard scans and detects security misconfigurations and vulnerabilities for mission-critical Storage and Backup systems, enabling organizations to harden Storage and Backup Systems to withstand ransomware and other forms of cyberattacks.

How to describe StorageGuard in several paragraphs?

The increase in ransomware and other cyberattacks on internal network systems has made organizations realize that internal high-value IT assets must be protected. Storage and Backup systems retain all mission-critical data including recovery and backup data copies, effectively serving as the final line of defense against ransomware and other forms of cyberattack.
StorageGuard is the only solution that provides continuous validation for storage and backup security - including Block storage, SAN, NAS, Object Storage, VSAN, Data Protection appliances, Backup Software and other types of data storage and backup systems.
StorageGuard scans and automatically detects security configuration issues and vulnerabilities for Storage and Backup systems, using a vast repository of thousands of automatic checks. The repository is continuously updated based on vendor security best practice guides, industry standards (NIST, CIS, SNIA, ISO, PCI, and others), community-driven baseline guidelines, security advisories, CVEs, and other sources. The automatic configuration checks cover wide range of security categories such as authentication, authorization, administrative access, malware protection, services and protocols, interfaces and ports, anti-ransomware, access control, encryption, audit logging and more.
While various solutions help organizations to secure hosts and web applications, StorageGuard is the only comprehensive solution for validating the security of Storage and Backup systems from vendors such as Dell EMC, IBM, Hitachi, NetApp, Pure, Infinidat, HPE, Cohesity, Commvault, Brocade, Cisco, and others.

CONTINUITY

-- THE SECURITY GAP –

What is the problem solved by StorageGuard?

Organizations **fail to harden and secure Storage and Backup** systems due to a knowledge gap, due to the uniqueness and complexity of the Storage / Backup solutions and due to the lack of automated repeatable scanning. **Storage and Backup systems contain significant vulnerabilities and security misconfigurations**, and do not adhere to industry information security standards and best practices.
The increased rate of ransomware and other attacks on internal IT systems lead to a **paradigm shift – perimeter protection is no longer sufficient, and high-value internal IT assets like Active Directory, Storage and Backup must be strictly secure at all times.**
The implications of non-secure Storage and backup are:

1. Petabytes of data (of hundreds of applications) exposed to cyberattacks.
2. Compromised storage and backup will affect the organization ability to recover from ransomware and other cyberattacks.

Why is it important to secure Storage?

Storage systems are central data systems that retain petabytes of data. If compromised, enormous amount of production data will be affected; a compromised storage system is the equivalent of breaching hundreds of database servers. In addition, storage systems are the final line of defense against ransomware and other cyberattacks; if compromised, valid snapshot and replica data copies will not be available for the cyber-recovery process. Without StorageGuard, your storage systems are likely to include security misconfigurations and vulnerabilities that can be exploited by attackers to compromise production and recovery systems and data on them.

Why is it important to secure Backup?

Backup systems are the final line of defense against ransomware and other cyberattacks; if compromised, valid snapshot and backup data copies will not be available for the cyber-recovery process. Without StorageGuard, your backup systems are likely to include security misconfigurations and vulnerabilities that can be exploited by attackers to compromise recovery systems and data on them.

How does StorageGuard help with Ransomware protection?

StorageGuard does not detect or block ransomware. Among the rest, StorageGuard verifies that native features, capabilities, and options for ransomware preparedness are enabled and configured according to best practices, including -

- StorageGuard validates that data volumes, exports and shares are configured with restricted access and privileges, and according to security best practices.
- StorageGuard validates NFS, SMB/CIFS and general NAS security best practices.
- StorageGuard verifies that Ransomware protection best practices published by storage and backup vendors are implemented.
- StorageGuard verifies that Anti-ransomware features are enabled and configured correctly (ransomware detection, ransomware isolation, anomaly detection, User behavioral analysis, AV scanning and more)

- StorageGuard verifies that the Storage management plane is highly secured, to prevent attackers from gaining Storage administrative access and compromising data volumes, exports, shares, luns, objects and other data elements.
- StorageGuard verifies that snapshots, replicas, images, and backup sets which are required for recovery from Ransomware - are secure, immutable isolated and generally protected.
- StorageGuard verifies that Backup systems are hardened and isolated.

CONTINUITY

-- STORAGEGUARD POC –

What does a StorageGuard POC include?

The Customer and Continuity have agreed to conduct a proof-of-concept ("POC") of StorageGuard in the Customer's environment. StorageGuard is the leading solution for validating the security of storage and backup systems. This POC shall exercise StorageGuard in an agreed set of scenarios and use cases to verify that the solution helps ensure security hardening – effectively and continuously – in the Customer's specific environment and relative to the Customer's own security needs.

- The POC is subject to the POC License Agreement available here: www.continuitysoftware.com/POC_License_Agreement

What is the definition of a storage / backup system for POC / pricing purposes?

The POC is free of charge and covers up to 3 storage / backup systems according to the definition below:

A 'Storage/Backup System' means any one of the following:	**Examples:**
1. Storage array or appliance (block, file, object)	Dell EMC VMAX; NetApp cluster
2. SAN switch	Brocade switch or director
3. Each 4 nodes in a CI/HCI cluster	Nutanix cluster, VMware VSAN cluster
4. Data protection appliance	Dell EMC RecoverPoint
5. Backup master server	NetBackup master server
6. Backup media server	NetBackup media server
7. Backup node	Node in a Rubrik cluster

What is the duration and method of the POC?

The POC shall be performed remotely via WebEx (or other screen-sharing utility acceptable to the Customer).
The estimated number of sessions required from kick-off to completion is 5.
The POC could be completed in as little as 2 weeks.

Which scenarios and use cases does the POC cover?

This POC shall exercise StorageGuard in the following scenarios and use cases:

#	Scenarios / Use Case	Details	Success Criteria
1	Scan of selected storage/backup systems	The following 3 systems shall be scanned: • TBD1 • TBD2 • TBD3	Fast, non-intrusive, no impact on scanned systems
2	Detection of security risks	Review and discussion of selected risks detected by the scan.	Detection of a range of risks or various types and severity levels, including

			at least 5 high-priority risks.
3	Remediation guidance	Review of the detailed remediation guidance provided for each of the selected risks detected. For up to 3 risks, Customer may choose to run the remediation commands provided, so as the resolve each risk.	Remediation guidance and commands are clear and detailed, explaining the nature and impact of each, and speeding time to resolution.
4	Auto-validation of remediated risks	If Customer has remediated selected 3 risks as suggested above, an additional scan shall be executed to auto-validate the resolution status of each risk.	All resolved/unresolved risks are correctly identified as such.
5	Security baseline creation	Review of the Customer's existing security baseline (if available) for storage/backup, followed by a demonstration of how to model that baseline as a Custom Security Policy (or set of Policies) in StorageGuard, drawing on the built-in knowledgebase of checks. If the Customer does not already have an established security baseline, such a baseline shall be proposed from StorageGuard's built-in knowledgebase.	The Customer's security baseline is readily modelled in StorageGuard, in a straightforward manner, with the vast majority of required checks available in the built-in knowledgebase.
6	Security baseline reporting and continuous validation	Once a sample/demo security baseline has been defined, reports will be created and run to validate alignment with that baseline. Options to run the scan and reports on a daily, weekly, or other frequency will be reviewed.	The reports and periodic scans provide the required visibility to ensure continuous alignment with the Customer's security baseline.
7	Compliance reporting [Optional]	Optional (if requested by Customer): Additional reports shall be executed to evidence compliance with specific security or regulatory standards (e.g., NIST, CIS, PCI etc).	The reports meet the Customer's compliance reporting needs, relative to storage/backup.
8	Integration and routing options	Review and discussion of the range of available integration and routing options, including direct routing of risks and reports by StorageGuard, built-in integration with ServiceNow, REST API integration, and other mechanisms.	Available integration and routing options meet the workflow needs of the Customer.
9	Custom checks	Demonstration of how to create custom checks, to augment the built-in knowledge, based on Customer-specific requirements.	A sample custom check was created and executed successfully.

POC summary presentation

Continuity shall prepare a presentation summarizing the results of the POC. Continuity and the Customer's POC team shall present the results to the Customer's Senior Management. For the purpose of preparing the presentation, the Customer shall provide Continuity with a StorageGuard Support Pack, auto generated by the product, and consisting of StorageGuard outputs and logs.

What are the technical requirements for a StorageGuard POC?

Installation requirements -
The StorageGuard software is installed on a customer-provided Windows virtual machine.

VM requirements:

- VM OS: 64-bit Windows Server 2012/2016/2019.
- English Edition and Locale.
- Local administrative rights required for the installation.
- Specs: 4vCPUs (2 sockets – recommended), 32GB RAM, 120GB Disk.
- Located on a local network that can access the scan targets / Open FW rules if needed.

We'd be glad to provide you with a pre-installed StorageGuard VM (OVA) that can be easily imported into your VMware environment – if preferred.

Scan requirements –
StorageGuard performs data collection using an agentless scan, by connecting remotely with valid credentials over standard protocols (SSH, HTTPS) and running read-only vendor-specific API calls and commands. refer to StorageGuard-Scan-Requirements for guidelines for specific storage and backup systems.

Where can I find the StorageGuard support matrix?

StorageGuard compatibility vendor list can be found here.

CONTINUITY

-- STORAGEGUARD FUNCTIONALITY –

What types of checks are performed by StorageGuard?

StorageGuard checks the security of Storage and Backup systems at three levels: the management plane, the data plane, and the recovery plane.

StorageGuard performs checks for the configurations of storage and backup systems in various areas such as authentication, authorization, encryption audit logging, administrative access, services and protocols, interfaces and ports, storage network (SAN), ransomware protection, time synchronization, data access and more.
StorageGuard also detects when Storage and Backup systems are exposed to security advisories, security bulletins, security alerts and CVEs.

Our checks repository is constantly updated with security recommendations based on the following publications –

- Vendor security configuration guidelines from Dell EMC, IBM, Hitachi, NetApp, INFINIBOX, Brocade, Cisco, HPE, Pure, Commvault, and many more.
- Guidelines of leading information Security standards: NIST, ISO/IEC, PCI DSS, CIS Control, FFIEC, SNIA and more
- Published Security advisories, alerts, bulletins, and CVEs (MITRE / vendors)
- Community feedback – security configuration baseline suggestions by users
- Recommendations by our Security research team

StorageGuard provides the ability to detect and track changes to the storage security configuration on a daily basis, thereby helping to identify unplanned or incorrect changes that may put storage and backup systems at risk.

How is the StorageGuard knowledgebase being updated?

Option 1 – Automatic – StorageGuard connects and securely downloads SG updates

Option 2 – Manual (default) – The StorageGuard administrator subscribes to receive notification re updates and can manually download and apply them to StorageGuard in a few simple steps.

Where can I find sizing guidelines for StorageGuard?

In our online Help Center as well as in our Documentation.

How does StorageGuard scan?

StorageGuard uses an agentless-scan and collects the configuration data from Storage and Backup systems by running read-only API and CLI commands on a user-defined schedule.
StorageGuard collectors can be used to collect configurations of storage and backup systems located in remote distant sites, which are then shipped and analyzed by the master StorageGuard server.
See also: What is the footprint / impact of a StorageGuard scan?

What is the footprint / impact of a StorageGuard scan?

The scan of a Storage or Backup system lasts between 30 seconds to several minutes. During the scan, StorageGuard runs read-only vendor commands and/or API requests. The read-only commands/API requests are executed serially (one at a time). The scan has negligible impact on the storage/backup CPU.
Only system configuration data is collected; no business data is collected.
Customer may initially scan the lab environment, and only then proceed to production.

What types of Credentials are supported for scanning?

The following types of credential sets can be configured for scanning:

- Local user account
- AD/LDAP account
- Key-based authentication
- Rotating password
- Password vault (Cyber-Ark, Cloakware)
- Kerberos

You may use the same user account for all systems, a different user account per system (or anything in between) – maximum flexibility.

Where can I find information regarding the Scan Requirements?

There's a section dedicated to StorageGuard Scan Requirements in the Knowledgebase category of our online Help Center. Also, you can find the Scan Requirements document in the Documentation section.

What kind of information is collected by StorageGuard?

StorageGuard collects configuration information of Storage and Backup systems such as model, version, updates, services, features, interfaces, ports, protocols, images, volumes, pools, luns, replication, exports, user roles, groups, zones, logging, policies, security, and general options.
No business data is collected.

Is StorageGuard a secure application?

Continuity serves the largest banks worldwide for many years and as such we're committed to high security standards. Our company completes successful the most rigorous third-party risk assessments from leading financial firms, and we conduct regularly external audits, penetration tests and vulnerability scans for our company facilities, IT network and for our software solutions.
As for StorageGuard –

- The StorageGuard web interface uses HTTPS only. TLS 1.2 is used for master-collector communication (in large multi geography) deployments.
- The target storage and backup systems are scanned with valid read-only credentials and over secure channels (SSH, HTTPS).
- The product leverages standard read-only vendor API and CLI commands. Our various integration plugins also support secure communication (Email, LDAPS, REST API, ITSM and more).
- Cached login credentials are strongly encrypted with a unique, per-customer AES encryption key, and further hashed with MD5. Not accessible from the UI. Shielded by DB credentials.

- StorageGuard collects configuration data for Storage and Backup systems. StorageGuard does **not** collect any business data (credit cards, social security numbers, etc.).

Is StorageGuard a SaaS solution?

No, StorageGuard is installed on-premises.

Does StorageGuard requires access to cloud or external connections?

StorageGuard is installed on-premises and by default does not require access to cloud or external connections. If Automatic update is enabled (optional), StorageGuard must be allowed to access a secure download location for risk knowledgebase updates.

Does StorageGuard requires an agent?

No. StorageGuard scans without agent, by leveraging credentials and connecting remotely to scanned storage and backup systems.

How often do you update the repository of best practice checks?

Our team works diligently to update our knowledgebase with new vulnerabilities of high or critical impact within 2 business days, and vulnerabilities of medium or low impact within 10 business days.

How do you prioritize findings?

Vulnerabilities are reported along with their CVSS score and impact levels.
Secure configuration issues are prioritized based on team's expertise and while considering the prioritization assigned the applicable best practice source (NIST, STIG, ISO, etc.).

Can StorageGuard be integrated with ITSM / Security monitoring solutions?

Yes, StorageGuard includes:

- Built-in specific (customizable) plugins for ServiceNow, HPE ServiceDesk and other management systems.
- General XML plugin that can be customized and configured to integrate with other systems.
- Rich REST API library for automation, integration, and reporting.
- Database API for reporting.

Our Support team will be glad to guide you as you integrate StorageGuard to your security and ITSM systems.
You may also engage with our Professional Services team if you're seeking assistance with tailor-made custom integration.

Does StorageGuard also fixes the detected findings?

No, however StorageGuard provides remediation guidelines for its findings, including the commands or APIs that can be used to resolve the reported vulnerability or misconfiguration. The remediation guidelines can also be accessed through API and integrated into configuration management solutions such as Chef and Ansible for automated remediation.
We are planning to also add a "Fix now" option for findings which we will require the user to provide read-write credentials (that will not be saved). StorageGuard scans with read-only credentials.

Can I create my own configuration checks for Storage and Backup?

Yes, StorageGuard enables users to easily create custom configuration collection and custom checks. In addition, our Professional Services team will be glad to assist with creating custom checks.

Is it possible to tune the checks performed by StorageGuard?

Yes, in several ways:

- Users can control which security principles and checks are analyzed – as part of defining a policy.
- StorageGuard Checks have customizable parameters that can be modified by users according to the organization's security requirements (e.g., idle session timeout, TLS level, etc.).
- When viewing findings, users can suppress individual findings or whole checks.
- Users can modify the urgency level for detected findings.

Can you help me to configure a policy to automatically check my baseline? What can be done about missing checks?

Yes. Our Professional Services team will be glad to guide your through the definition of a StorageGuard security policy, and make sure it includes all you baseline requirements.

For missing checks, you have the following options –

- Speak to us! We will gladly consider developing and adding them to the repository of automatic checks.
- Define a custom check.
- Work with our Professional Services team to define a custom check.

IS CLI access required?

As a general rule, we prefer using REST API (or other HTTPS-based API) over SSH for data collection. However, we found that in some cases the REST API of storage/backup system provides significantly less information than the CLI (SSH), especially when it comes to security configuration.
Since our goal is to perform a comprehensive secure configuration and vulnerability analysis, in some cases we do use CLI over SSH.
As you may see from the summary table, some systems are accessed through SSH while others through HTTPS.

System Type	Connection Protocol	Collection method	Note
Brocade FC Switch	SSH	CLI	
Cisco FC Switch	SSH	CLI	
Clustered Data ONTAP (cDOT)	HTTPS	API	
Data ONTAP 7-Mode	HTTPS	API	
Dell EMC VNX	SSH	CLI	
Dell EMC Unity	HTTPS	API	Through Unisphere

Dell EMC ECS	HTTPS	API	
Dell EMC Data Domain (Power Protect DD)	SSH	CLI	
Dell EMC PowerScale (Isilon)	SSH	CLI	
Dell EMC PowerMax, VMAX and Symmetrix	SSH	CLI	Through Solutions Enabler (SYMCLI)
Dell EMC XtremIO	HTTPS	API	
Dell EMC VPLEX	HTTPS, SSH	API, CLI	
Dell EMC RecoverPoint	SSH	CLI	
Dell EMC Avamar	SSH	CLI	Through MCCLI
Hitachi VSP	HTTPS	API	Through HCS
HPE XP	HTTPS	API	Through CommandCenter
Hitachi Content Platform (HCP)	HTTPS	API	
Veritas NetBackup	HTTPS	API	Through the master server
IBM FlashSystem	SSH	CLI	
Infinidat InfiniBox	HTTPS	API	
PureStorage FlashArray	HTTPS	API	
HPE StoreOnce	HTTPS	API	
Cohesity DataPlatform	HTTPS	API	

I don’t like using Oracle; do you support other databases for your SG application?

We will enable to deploy StorageGuard with a Postgres database in the future – roadmap.
Meanwhile it is possible to use an Oracle Trial or Oracle Express (Free) for the POC.

-- STORAGEGUARD DEPLOYMENT & ARCHITECTURE --

How long does it take to install StorageGuard?

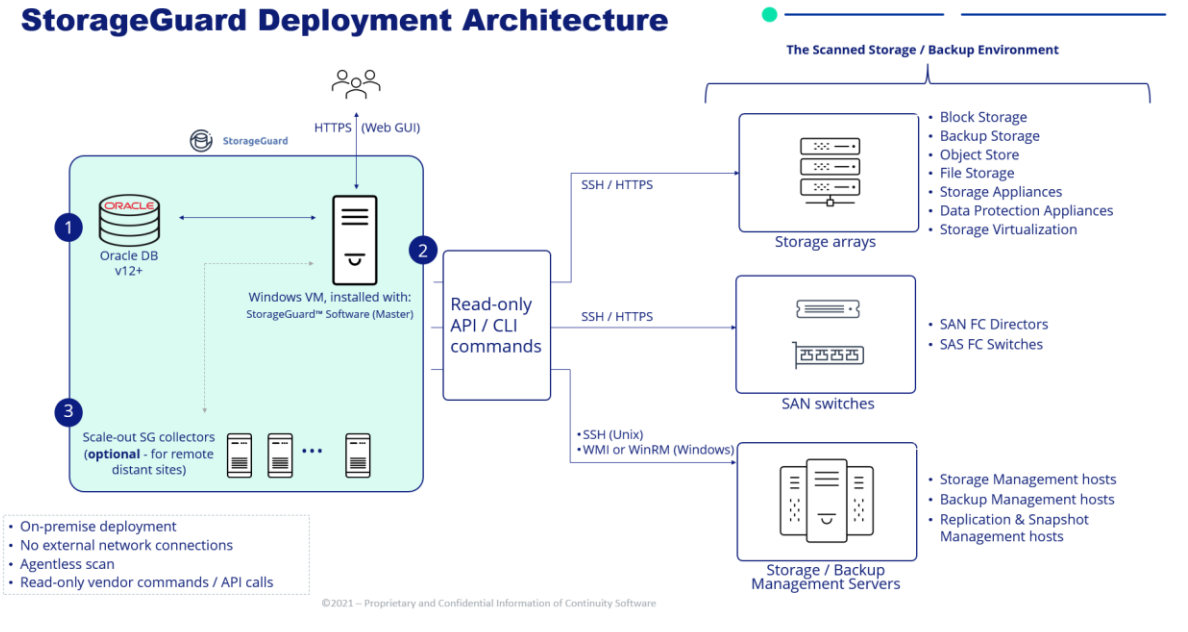
StorageGuard can be installed on a designated Windows virtual machine within 30 minutes. An OVF is available for customers who prefer to import a pre-installed StorageGuard virtual machine. Following the installation, you may enter scan credentials to storage and backup systems and immediately see results.

How is StorageGuard deployed?

StorageGuard is very easy to deploy –
StorageGuard is deployed on premises, either by installing the software on a Windows virtual machine or by importing a VMware OVF file.
Once you enter the scan credentials for Storage and Backup systems, you can immediately begin to analyze the security posture of the designated systems, review findings and remediation guidelines.
If your organization has multiple datacenters, you may deploy StorageGuard collector virtual machines in remote sites. The collectors will scan local Storage and Backup systems and communicate with the master StorageGuard server to provide you with a complete view of your security posture.

Do you have an Architecture diagram for StorageGuard?

Yes, below:



-- ADDRESSING OBJECTIONS –

Why do I need continuous validation? Can't I just do it once?

Storage and Backup configurations change on a regular basis, resulting in vulnerabilities and misconfigurations that can be exploited by attackers –

- Changes to port zoning, file shares, LUNs, access rights, backup policies, administrative accesses and other configuration items can adversely affect the security posture of your storage and backup systems.
- Upgrades, updates and hotfixes to Storage OE, Storage firmware, Storage Software components and Backup software often result in hardened security settings being reverted to non-secure values, without the awareness of the organization.
- new vulnerabilities are discovered and published frequently, and it is difficult to keep track and validate that storage and backup systems are not exposed to them.
- New security guidelines are published regularly by organizations such as CISA, NIST, CIS, ISO and others.

Without regularly validating the security posture of Storage and Backup systems, vulnerabilities and misconfiguration exist for sufficient periods of time to allow attackers to exploit them.

Last, continuous validation enables organizations to embrace a process for gradually improving the security of storage and backup systems and expanding the security baseline.

What could go wrong if I don't harden my Storage?

If storage systems are not strictly secure, attackers may be able to delete, corrupt, encrypt, alter, leak or make unavailable the data volumes kept with these systems. Such attacks have a destructive potential, impacting petabytes of data and hundreds of applications.
Other than centrally storing production data, storage arrays also retain the snapshots, replicas and backup images that serve as the final line of defense against disaster recovery and cyberattacks. In the event storage systems are compromised, the organization may not be able to restore data and dependent services to an operational state.

What could go wrong if I don't harden my Backup?

If backup data or backup data management are not strictly secure, attackers may be able to delete or corrupt backup as part of a cyberattack, leaving an organization no choice but to succumb to malicious actor's demand or worse – without a feasible option to restore data and dependent services to an operational state.

-- STORAGEGUARD AND REGULATORY GUIDELINES / STANDARDS --

StorageGuard and the MAS TRM Guidelines

A document outlining how StorageGuard assist organizations to adhere to the Singapore TRM guidelines is available upon request.

How does StorageGuard help with the NIS Directive?

Yes, StorageGuard helps with the NIS directive goal because is aligns critical data storage systems to common best practices and standards.
StorageGuard helps achieving "higher level of security" as requested by NIS directive.
StorageGuard helps organizations to "take appropriate and proportionate technical measures to manage risks posed to the security of network cand information systems"
StorageGuard helps with the NIS directive to have the following security measures:

- Security of systems
- Business continuity management
- Monitoring, auditing, testing Compliance with international standards

StorageGuard helps ensure that "electronic security designed to protect their systems from misuse or unauthorized access..." are in place.
StorageGuard helps with the goal of "lost data is close to zero"

How does StorageGuard help with the NERC (Energy)?

Many of the StorageGuard checks are validating guidelines specified by NERC standards – such as CIP-003, CIP-007, CIP-009, CIP-010, CIP-011 and more.

How does StorageGuard help with MITRE Att&ack Framework?

StorageGuard has excellent coverage for the Mitre Enterprise Att&ck framework – for Storage and Backup systems.
StorageGuard checks that storage and backup systems are configured according to Mitre's hardening and risk mitigation guidelines for known attack techniques – such as Privilege escalation, Discovery, Credential Access, Exfiltration and more.
StorageGuard also has excellent coverage for NIST guidelines – often the Mitre and NIST frameworks go hand in hand; and Continuity also took part in defining the NIST security best practices for storage – see XYZ.

How does StorageGuard help with the ISO standards?

StorageGuard helps automatically verifying that Storage and Backup systems adhere to ISO/IEC 27001, ISO/IEC 27040, and others. The findings of StorageGuard contain references to specific ISO guidelines, and PASS/FAIL summary reports can be generated.

How does StorageGuard help with NIST?

StorageGuard helps automatically verifying that Storage and Backup systems adhere to NIST SP800-53, NIST SP800-63, NIST SP800-209 and many others. The findings of StorageGuard contain references to specific NIST guidelines, and PASS/FAIL summary reports can be generated.

How does StorageGuard help with PCI?

StorageGuard helps automatically verifying that the configuration of Storage and Backup systems adhere to PCI DSS guidelines. The findings of StorageGuard contain references to specific PCI DSS guidelines, and PASS/FAIL summary reports can be generated. StorageGuard does not analyze business data for PII.

-- INDUSTRY REFERRING TO SECURING STORAGE & BACKUP --

Does Gartner say anything about Storage and Backup Security?

Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware | October 2021

- "While storage infrastructure can be one of the most-impacted solutions attacked by ransomware, it initially receives limited attention by security and storage leaders."
- "Although numerous solutions are available for endpoint protection, centralized storage lacks active protection against malicious attacks."
- Gartner Recommendation: "Harden your existing unstructured data storage solution by leveraging storage vulnerability management tools and following vendors best practices."
- "In October 2020, the National Institute of Standards and Technology (NIST) released Special Publication (SP) 800-209, Security Guidelines for Storage Infrastructure, which includes comprehensive security recommendations for storage infrastructures." – Co-authored by Continuity
- Gartner named **Continuity StorageGuard** as one of the Cyberstorage Solutions to Protect Unstructured Data Against Ransomware
- Continuity Named Vendor in Gartner® Hype Cycle™ for Storage & Data Protection Technologies - https://www.einnews.com/pr_news/580021945/continuity-named-vendor-in-gartner-hype-cycle-for-storage-data-protection-technologies

6 ways to defend against Ransomware | Nov 2020

"Harden the components of enterprise backup and recovery infrastructure against attacks… routinely examining backup application, storage and network access…. safeguard backup storage media and accessibility"

Other publications (non-Gartner)

Security Intelligence: "Ransomware attacks are targeting organizations' network-attached storage (NAS) and backup storage devices."

Forbes: "2021 will see a major emphasis in developing more comprehensive storage system security"

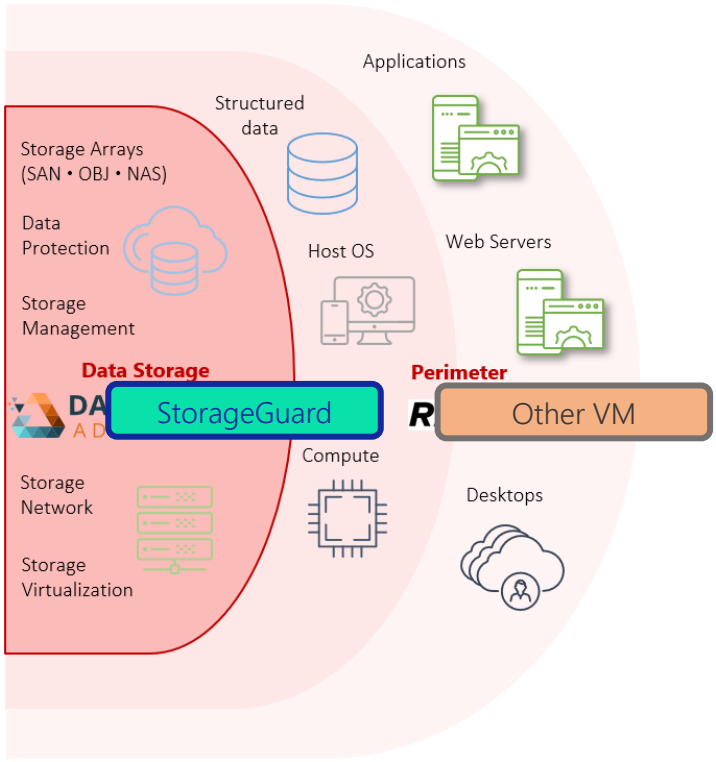
-- COMPETITION --

Do I need StorageGuard if I'm already using vulnerability management (VM) solutions?

VM solutions are focused on analyzing vulnerabilities for endpoints such as web applications, desktops, laptops, and hosts.
StorageGuard is focused on analyzing vulnerabilities and secure configuration issues for data storage and backup systems such as block storage, object storage, NAS, SAN, data protection appliances, backup solutions, storage management and more.
VMs such as Tenable/Qualys and StorageGuard are complementary and do not overlap.

	StorageGuard	VM Solution
Markets	▪ Vulnerability Scanning ▪ Security Posture Management ▪ Cyber-Storage and Backup Security	▪ Vulnerability Scanning ▪ Security Posture Management ▪ Application security
Main Features	▪ Security configuration assessment ▪ Vulnerability scanning ▪ Policy and Compliance (Audit) ▪ Threat detection[1]	▪ Security configuration assessment ▪ Vulnerability scanning ▪ Policy and Compliance (Audit)
Scalability	Enterprise-scale (distributed collection)	Enterprise-scale (distributed collection)
Focus Area	▪ Data Storage & Backup	▪ Endpoints and Web applications
Supported Platform Types	▪ Data and Backup Storage Systems ▪ Storage Software ▪ Backup Solutions ▪ Network (Storage)	▪ Host / Mobile OS, DBMS ▪ Host Software ▪ Web Application ▪ Network (Ethernet)

[1] roadmap



How is StorageGuard compared to native Storage/Backup security validation capabilities?

While Storage vendors provide excellent tools to manage availability and performance of storage systems, they do not do the same for the security of storage systems –

- Some storage vendors publish security best practice guides; however, implementation and monitoring of security features and configurations is entirely the responsibility of the IT/IS organization.
- Many storage systems are shipped with default non-secure settings and customers are required to enable and correctly configure various settings to secure their storage. [Side note, not sure if to include: Because historically and even today storage systems are benchmarked based on performance, storage vendors are by nature not enthusiastic about enabling security features, which occasionally may have certain performance implications.]
- There are no tools from the vendors to automatically scan and validate security configurations such as authentication config, access control settings, ransomware preparedness config, administrative access, encryption, and other security configuration categories.
- In addition, when it comes to CVEs, vendors publish security advisories from time to time, but do not provide automatic scan and detection.
- [not sure if need to add] Last, the technical teams of the storage vendors often do not have expertise in security and are often geared toward performance due to business and historical reasons.

How is StorageGuard different or better than Qualys / Rapid7 / Nessus?

Refer to Do I need StorageGuard if I'm already using vulnerability management (VM) solutions?
And the following data table:

	VM	SG
Support Matrix	The support matrix of Qualys, Rapid7, Nessus and other VM solutions is focused on web application and endpoints and includes nearly no coverage for Storage and Backup.	The support matrix of StorageGuard is focused on Storage and Backup systems, and includes support for nearly all Enterprise Storage and Backup system from Dell EMC, IBM, NetApp, Hitachi, HPE, Cohesity, Pure and other vendors
Data collection	Generic network / Linux scan	Specific, in-depth security configuration data collection for each Storage and Backup system, using the vendor's native API and CLI.
Secure configuration and configuration compliance	Nearly no coverage for Storage and Backup.	The most comprehensive and continuously updated repository of security configuration best practices for Storage and Backup
Security advisories and CVEs	Nearly no coverage for Storage and Backup.	The most comprehensive and continuously updated repository of security advisories and CVEs for Storage and Backup

If I use Disk Encryption, do I still need StorageGuard?

In a nutshell –

- The practice of Data Encryption helps ensure no one can read your data if a storage disk is lost, misplaced, or stolen.
- The practice of Storage Security helps ensure attackers cannot compromise central data storage systems by exploiting vulnerabilities, misconfigurations, or weak security settings, or by deploying malware.

Tell me more about the StorageGuard support pack

There's no automatic sending of data by the software.
The support bundle is available for your review.
The support bundle is manually transferred to us securely as a protected file.
The support bundle is only accessible to select few involved in the risk assessment.
The support bundle is kept in an isolated secure environment and on encrypted disks.
The support bundle is securely erased after the delivery of the risk assessment report.
The support bundle does not contain any business data.

StorageGuard vs Malware Protection

Malware protection solutions verify that files are not infected with viruses or other malicious code. StorageGuard verifies that the Storage and Backup IT infrastructure is hardened and configured according to security best practices for least privilege, encryption, logging, administrative access and more.

StorageGuard vs Dell EMC Storage Resource Manager

Dell EMC SRM is a solution for capacity management, free space monitoring, storage utilization and trends, performance, and availability management.

StorageGuard is a solution for storage and backup security posture management. StorageGuard scans and automatically identifies secure configuration issues and vulnerabilities for Storage and Backup (Dell EMC and other vendors) – using a continuously updated knowledgebase of security configuration best practices and vulnerabilities. StorageGuard validates the configuration of authentication, authorization, ransomware preparedness, encryption, protocols and services, audit logging, administrative access, and other areas.

There's no overlap between the solutions and there are complementary.

StorageGuard vs StealthAudit

- The two solutions are complimentary. There is no overlap in functionality or coverage areas.
- StorageGuard automatically scans detects on a daily basis security misconfigurations and vulnerabilities at the Storage and Backup infrastructure levels (management, data and data recovery planes). Cent
- StealthAudit is an Access & Data Governance solution operating the file and AD account levels

	StorageGuard	**StealthAudit**
Description	StorageGuard is a secure configuration and vulnerability scanning solution focused on **Data Storage and Backup Systems,** enabling organizations to continuously validate storage and backup systems are configured according to security best practices, standards, and organizational baselines, and are not vulnerable.	StealthAudit is a reporting and governance solutions focused on **File Systems and Active Directory**, analyzing file access rights and user permissions.
Focus Area	• Enterprise Storage and Backup Systems (Where petabytes of production data is stored as well as snapshots, replications and backup data for cyber-recovery)	• File / File System, AD

Supported Systems	• Dell EMC Symmetrix • VMAX • PowerMAX • Dell EMC XtremIO • PowerStore • IDPA • Dell EMC VNX • VNX2 • Unity • NetApp FAS/AFF • cDOT • 7-mode • filer • Hitachi VSP/USP • AMS • HUS • G-Series • IBM DS • XIV • Storwize • A9000/R • V9000 • FlashSystem • Spectrum Accelerate • N-Series • HPE XP • 3PAR • Primera • Infinidat InfiniBox • Pure • VMware VSAN • Dell EMC Isilon • PowerScale • Hitachi Content Platform (HCP) • Dell EMC Elastic Cloud Storage (ECS) • Brocade directors / switches • Cisco FC MDS • Nexus • Dell EMC VPLEX • IBM SAN Volume Controller • Spectrum Virtualize • Dell EMC RecoverPoint • Dell EMC Data Domain • Dell EMC PowerProtect DD • Dell EMC Avamar • PowerVault ME • NetBackup • Commvault • HP StoreOnce • Cohesity • Rubrik	• File systems • Sharepoint • Onedrive for business • Active directory • Azure active directory • Exchange • Exchange Online • Dropbox • Box • AWS s3 • SQL • Azure sql • Oracle • Windows • Unix & Linux

StorageGuard vs Varonis (and equivalent – Stealthbits etc.)

Varonis is about mapping and analyzing file-level permissions and vulnerabilities. It is a File Analysis Software.
StorageGuard is about mapping and analyzing the security and vulnerabilities of storage systems. StorageGuard belongs to the world of vulnerability scanning and security posture management software solutions.
A file (e.g., a doc file, a xls file etc.) can be stored on a file system on a desktop, server, or NAS storage system.

A storage system is device used to save, send, or manage data storage such as a SAN storage array, Storage Management software or Storage network switch.
Files eventually are stored within storage devices. If you break into a storage device, you can delete, alter, or block all files stored within the device.
StorageGuard looks at the entire range of storage devices (SAN, Object, Storage Network, Storage Management, Storage Virtualization, VSAN, Data Protection Systems and NAS), and verify these devices are secure and configured in a way that would make hard for an attacker to penetrate.
StorageGuard analyzes the configuration of the devices – settings such as authentication, authorization, protocols (NDMP, SNMP, HTTP, FTP, …), ports, encryption, access lists, ransomware protection features, SAN/NAS security. StorageGuard does not analyze the security of the files within the file system.
Thus, Varonis and StorageGuard are complementary solutions that do not compete with each other.

StorageGuard vs Dell PowerProtect Cyber Recovery

Dell PowerProtect Cyber Recovery and StorageGuard are entirely different solutions and complementary to each other.

	Dell PowerProtect Cyber Recovery	**StorageGuard**
	Backup Storage, Cyber Storage	Configuration Hardening and Vulnerability Management
What does it do?	Provides isolated immutable data copies with machine learning to identify signs of corruption due to ransomware	Enables organizations to harden Storage and Backup systems by scanning them for security misconfigurations and vulnerabilities using a knowledgebase of security best practices, standards and vulnerabilities
Scope	Dell EMC Data Domain	Dell EMC VMAX, Isilon, … Hitachi VSP, HCP, … IBM Flash, … Pure, Infinidat, … NetBackup, Cohesity, … HPE, … Brocade, Cisco, …

Among the rest, **StorageGuard** scans **Dell PowerProtect Cyber Recovery systems**.
StorageGuard verifies **Dell PowerProtect Cyber Recovery systems** are configured according to (1) Dell's Security Configuration and Hardening Guides for PowerProtect Cyber Recovery (2) Storage and Backup security best practices (3) Industry standards (4) Community-driven security best practices.
StorageGuard also verifies that **Dell PowerProtect Cyber Recovery system** software and components are not vulnerable to known security advisories, alerts, bulletins, or CVEs.
StorageGuard tracks configuration changes for **Dell PowerProtect Cyber Recovery systems**
StorageGuard verifies compliance of **Dell PowerProtect Cyber Recovery systems** with Standards and with Security Baselines.

-- STORAGE CYBER ATTACKS --

Are there any known attacks on Storage and Backup?

Hackers frequently target MSSP backup systems as door openers to cyberattacks & malware campaigns, Darktrace research finds.
MSSPs Among Hardest Hit by Cyberattacks Targeting Backup Vulnerabilities - MSSP Alert
"Cybercriminals behind a string of high-profile ransomware attacks…The unusual move is an attempt to target …network attached storage (NAS) devices"
Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices | Threatpost
"most commonly exploited….Intel SA-00191….Specific Intel firmware is susceptible to security vulnerabilities that may allow hackers to disclose sensitive information, escalate privileges and launch DoS (Denial of Service) attacks…. **NetApp** suite of products… are at risk"
https://resources.infosecinstitute.com/topic/32-hardware-and-firmware-vulnerabilities/
New attack vector opens backdoor inside enterprise disk **storage** arrays and people's **NAS** devices.
Over 13K iSCSI storage clusters left exposed online without a password | ZDNet
"The NCSC has seen numerous incidents where ransomware has not only encrypted the original data on-disk, but also network **storage** drives holding data **backups"**
Cognizant Hacked, Customers Affected, Maze Ransomware Named (techmonitor.ai)
"… hackers were able to gain privileged access to…. File **storage** services"
US says cyber hack poses 'grave risk' to critical infrastructure | Financial Times (ft.com)
"LNK files in his company's network attached **storage** (**NAS**) … sign of a rogue AutoIT worm… a hacker could use that program to get a hold of the company's intellectual property and hold it for ransom."
What Happens When A Company Gets Hacked? | Built In
"…the malicious actor was able to partially compromise our infrastructure, and gain access to document **storage**"
Security Incident on November 13, 2020 (liquid.com)
"…a '*nix' version is being made available that could target **NAS** devices and VMware ESXi virtualization hosts alongside the already supported Windows hosts."
Babuk Locker (cyberint.com)
"… the attacker released information pertaining to the victim's **NAS** servers and then released a supposed finance-related folder…. hundreds of gigabytes of data"
Pay2Key Ransomware Joins the Threat Landscape - Security Boulevard
OCIE Alert: "Weak or misconfigured security settings on a network **storage** device could result in unauthorized access to information stored on the device."
https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf

https://cyware.com/news/your-nas-devices-are-under-threat-from-ransomware-say-researchers-21cee063
"Previously, encryption ransomware targeting NAS was hardly evident in the wild, and this year alone we have already detected a number of new ransomware families focused solely on NAS. This trend is unlikely to fade, as this attack vector proves to be very profitable for the attackers, especially due to the users being completely unprepared for them as they consider this technology highly reliable," said Fedor Sinitsyn, security researcher at Kaspersky.
https://www.mcafee.com/enterprise/en-us/threat-center/threat-landscape-dashboard/ransomware-details.megalocker-ransomware.html
MegaLocker – Ransomware. The ransomware targets NAS storage devices and Samba servers and append either ".crypted" or ".NamPoHyu" to infected files. The malware is known to encrypt remote Samba servers but instead of encrypting locally on the victim's server the ransomware runs the encryption process at a remote location.

https://securityintelligence.com/news/ransomware-attacks-targeting-organizations-backup-data-storage/
A quarterly threat report found that ransomware attacks are targeting organizations' network-attached storage (NAS) and backup storage devices.
https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Network%20Storage.pdf
Misconfigured network storage solutions. In some cases, firms did not adequately configure the security settings on their network storage solution to protect against unauthorized access. In addition, some firms did not have policies and procedures addressing the security configuration of their network storage solution. Often, misconfigured settings resulted from a lack of effective oversight when the storage solution was initially implemented.
Inadequate oversight of vendor-provided network storage solutions. In some cases, firms did not ensure, through policies, procedures, contractual provisions, or otherwise, that the security settings on vendor-provided network storage solutions were configured in accordance with the firm's standards.
https://www.globenewswire.com/news-release/2019/07/10/1880925/0/en/Anomali-Discovers-New-Ransomware-Targeting-Consumer-Enterprise-Storage-Devices.html
Anomali, a leader in threat intelligence, today published its latest research blog. It details a new type of ransomware identified by the Anomali Threat Research Team. Designated as "eCh0raix," it is targeting QNAP Network Attached Storage (NAS) device
https://www.anomali.com/blog/threat-actors-utilizing-ech0raix-ransomware-change-nas-targeting
Synology Inc., a Taiwan-based Network Attached Storage (NAS) company, posted an advisory on safeguarding internet-connected Synology NAS devices from Ransomware attacks
https://krebsonsecurity.com/2020/02/zyxel-fixes-0day-in-network-storage-devices/
Networking hardware vendor Zyxel today released an update to fix a critical flaw in many of its network attached storage (NAS) devices that can be used to remotely commandeer them