The StorageGuard Bible Sales Playbook

CONTINUITY

ELEVATOR PITCH

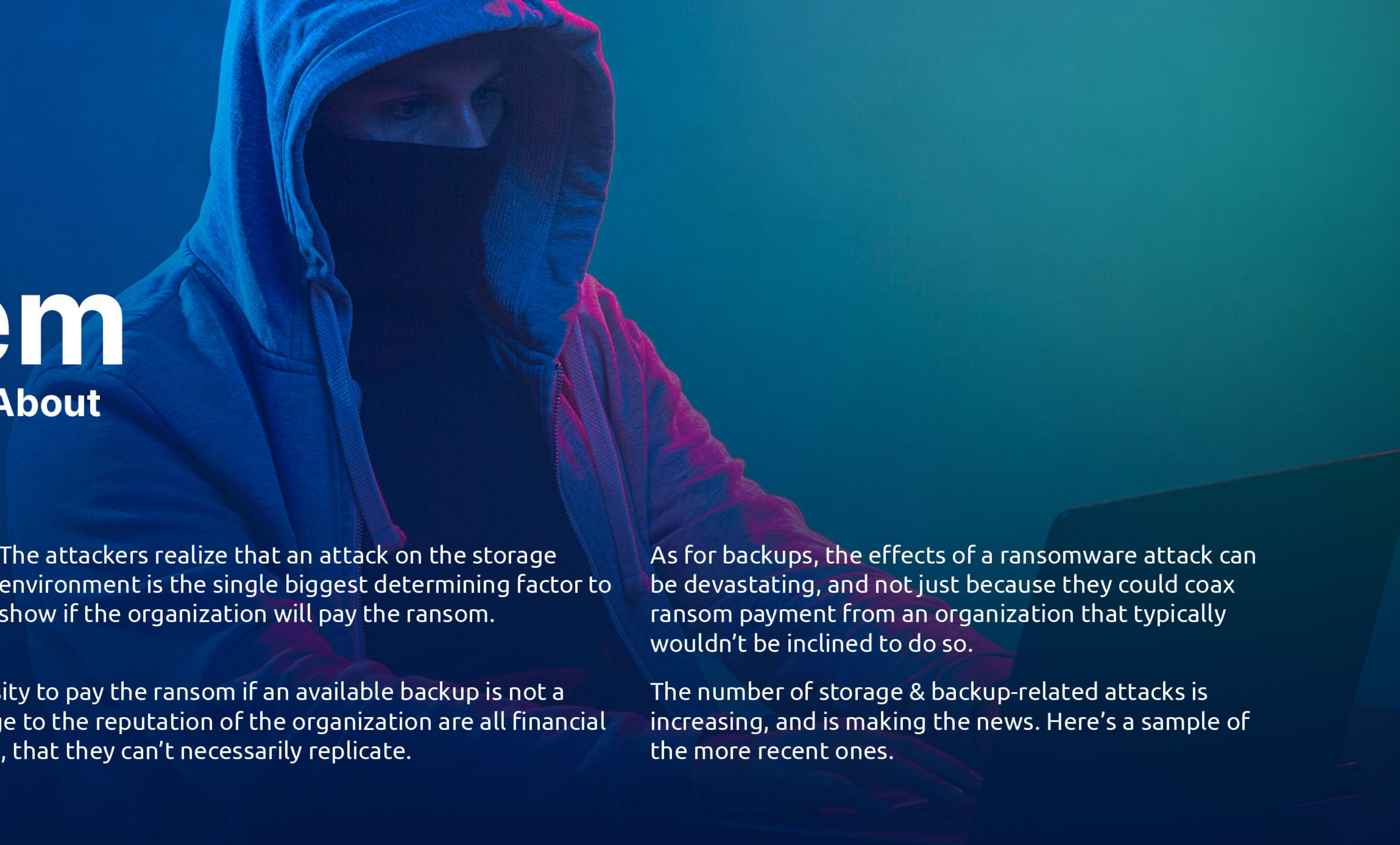
New ransomware groups are targeting storage and backup systems (e.g., Conti, Hive and REvil). However, storage & backup are currently the only infrastructure layers NOT COVERED by traditional vulnerability management solutions.

This is a glaring blind spot, since the working assumption should be that some attacks will succeed. When that happens, storage and backups are **your last line of defense**.

Continuity brings the industry's ONLY vulnerability management solution for storage & backup systems, helping you protect your most valuable data, and ensuring data recoverability in case of a breach.

For the first time, get complete visibility of security risks across your storage & backup systems, automatically prioritized in order of business impact, and with clear remediation guidelines.

Now's the time to get the peace of mind that your storage & backup systems can withstand a ransomware attack.



The Problem

Why Should Your Customers Care About Storage & Backup Security?

The tactics being used by sophisticated attackers have changed. And it puts larger organizations with legacy storage and backup environments at major risk.

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

The damage to an organization goes far beyond the necessity to pay the ransom if an available backup is not a possibility. Loss of revenue, business disruption and damage to the reputation of the organization are all financial burdens. Organizations stand to lose valuable data, as well, that they can't necessarily replicate.

As for backups, the effects of a ransomware attack can be devastating, and not just because they could coax ransom payment from an organization that typically wouldn't be inclined to do so.

The number of storage & backup-related attacks is increasing, and is making the news. Here's a sample of the more recent ones.

threatpost

The Conti ransomware gang has developed novel tactics to demolish backups

Conti bases its negotiation strategies on the premise that the majority of targets who pay the ransom are "motivated primarily by the need to restore their data."

According to Palo Alto Networks; "it's one of the most ruthless of the dozens of ransomware gangs that we follow."

security affairs

A new variant of the eCh0raix ransomware is able to target Network-Attached Storage (NAS) devices

NAS servers are a privileged target for hackers because they normally store large amounts of data.

The ransomware was targeting poorly protected or vulnerable NAS servers, threat actors exploited known vulnerabilities or carried out brute-force attacks.

threatpost

Cybercriminals behind a string of high-profile ransomware attacks, including one extorting $11 million from JBS Foods, have ported their malware code to the Linux operating system. The unusual move is **an attempt to target network attached storage (NAS) devices** that run on the Linux operating system (OS).

REvil is also targeting NAS devices as another storage platform with the potential to highly impact the affected companies.

BLEEPING COMPUTER

The ransomware gang, Hive, is known to seek out and delete any backups to prevent them from being used by the victim to recover their data.

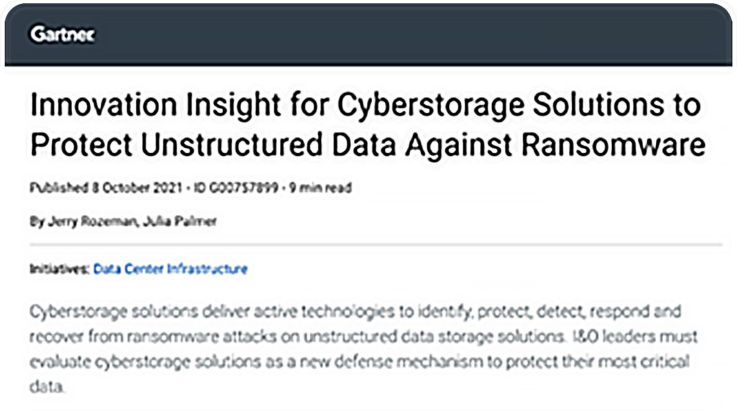
SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Western Digital had updated its SanDisk SecureAccess product to address vulnerabilities that can be exploited to gain access to user data through brute force and dictionary attacks.

BLEEPING COMPUTER

Synology warns of malware infecting NAS devices with ransomware

The NAS maker urges all system admins and customers to change weak administrative credentials on their systems, to enable account protection and auto block, and to set up multi-factor authentication where possible.



Gartner

Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware

Published 8 October 2021 · ID G00757899 · 9 min read

By Jerry Rozeman, Julia Palmer

Initiatives: Data Center Infrastructure

Cyberstorage solutions deliver active technologies to identify, protect, detect, respond and recover from ransomware attacks on unstructured data storage solutions. I&O leaders must evaluate cyberstorage solutions as a new defense mechanism to protect their most critical data.

In addition, Gartner published their first report on the topic of 'cyberstorage'.

"While storage infrastructure can be one of the most-impacted solutions attacked by ransomware, it initially receives limited attention by security and storage leaders."

Gartner Recommendation: "Harden your existing unstructured data storage solution by leveraging storage vulnerability management tools and following vendors best practices."

You can read Gartner's report here: **Innovation Insight for Cyberstorage Solutions to Protect Unstructured Data Against Ransomware**

The Solution

How Does StorageGuard Help?

Now that your clients recognize the problem, you can provide them with the reassurance that StorageGuard will help them harden their storage & backup systems, to withstand ransomware and other attacks targeting your data.

Existing vulnerability management tools (e.g., Nessus, Qualys, Rapid7) do a good job of scanning the Host OS, Network and Web – but offer virtually no support for Storage Arrays, Storage Network, Data Protection, Backup Systems and Storage Management.

This is where StorageGuard helps.

Discovers

Continuously scans your storage & backup systems, to automatically detect security misconfigurations and vulnerabilities.

Prioritizes

Prioritizes and categorizes risks in order of urgency, severity, and business impact.

Recommends

Provides remediation guidance and commands – with an option for facilitating automatic remediation.

StorageGuard contains a vast and continuously updated knowledge base of automated checks, covering:

• Security best-practices from the storage & backup vendors • Standards (NIST, ISO, CIS, SNIA, etc.) as applied to storage & backup • Vulnerabilities (CVEs) for the storage & backup environments • Commonly used security baselines

In addition, your clients can use StorageGuard to create custom checks and policies.

StorageGuard also integrates with your clients' GRC, ITSM and SIEM tools, to help them streamline their vulnerability remediation workflows.

The Benefit

What Does It Mean For Your Customers?

Visibility

Get a full view of the security risks in your storage & backup systems

Prioritization

Act upon your most urgent vulnerabilities, where you're most at risk

Protection

Ensure all your storage & backup systems can withstand an attack

Automation

Free up your time by eliminating manual security validation efforts

Compliance

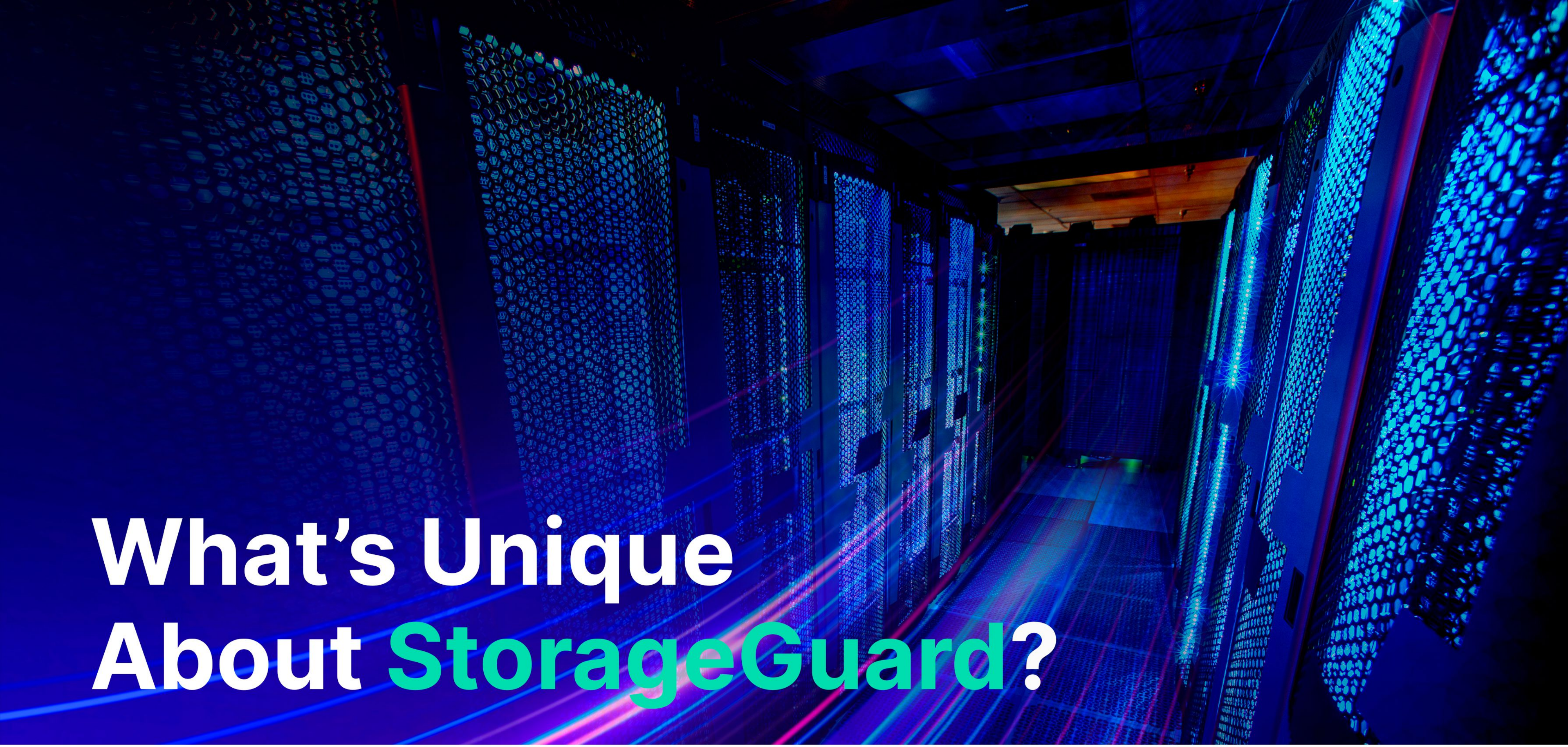
Guarantee storage & backup systems are compliant with security regulations and standards

The Competition

How Is StorageGuard Different From Existing Vulnerability Management Solutions?

StorageGuard does not compete with the vulnerability management vendors in the market. It actually complements them, to ensure your clients' most valuable data is protected.

	StorageGuard	Qualys
Markets	• Vulnerability Assessment • Security Posture Management • Data storage security	• Vulnerability Assessment • Web Application security
Focus Area	**Data Storage and Backup**	**Host and Desktops**
Main Scanned Platform Types	• Storage OS • Storage / Backup Software • Network (Storage)	• Host / Mobile OS, DBMS • Host Software • Network (Ethernet)
Coverage for Enterprise Storage	>88%	<9%
Storage Vulnerability Knowledgebase	Up to date / Continuously updated	Poor / Outdated / Rarely updated
Storage Configuration Hardening Checks	>1000	<100
Configuration Change Tracking	Yes	<100
Scan Frequency for Enterprise Storage	User-defined Daily (default) / Every X hours / Weekly Monthly / User-defined / Ad-hoc	User-defined Typically, infrequent (every X months)
Analysis method	**Storage-Aware scan** • Storage-savvy analysis including review of LUNs, volumes zoning, masking, etc. • Specialized Storage vulnerability and configuration hardening analysis • Storage access control analysis • Storage software analysis • Storage CLI / API / Config files	**Generic Web / Linux / Network** • Generic Web App / Linux Vulnerability detection • Generic network checks
API	**REST, SQL**	**REST**
Policy & Compliance	YES	YES
Integration	YES	YES



What's Unique About StorageGuard?

01 StorageGuard is the ONLY solution that can scan storage & backup systems for security vulnerabilities & misconfigurations.

02 StorageGuard contains the most comprehensive Knowledge Base of security risks & best practices for enterprise storage & backup environments

03 Continuity is the co-author of the NIST Special Publication: 'Security Guidelines for Storage Infrastructure'. This is the most authoritative guidebook on the topic of securing storage & backup systems.

Buyer Personas

Who To Sell To?

Job Function	What They Care About (Pain Points)	How StorageGuard Helps (Benefits)
Chief Information Security Officer (CISO) VP Information Security	• Identifying major security blind spots (unknown unknowns) • Protecting my data and my business – and also my reputation • Ensuring data recoverability (in case of a breach) • Access to information that helps them clearly communicate an accurate picture of their security posture to non-technical senior stakeholders • Showing business value	• Reassurance and peace of mind that their storage & backup systems can withstand ransomware and other attacks targeting their data • Be proactive: Act upon their most urgent vulnerabilities, where they're most at risk • Guarantee storage & backup systems are compliant with security regulations and standards • Ensure data recoverability in case of a breach
Head of Infrastructure Storage & Backup Manager	• Availability (consistent end-user experience) • Making sure data is available and protected -- replicated and backed up, providing appropriate access controls and processes, and ensuring regulatory compliance. • Secure (keep track of storage configuration changes, and automate validation & enforcement of storage security best practices) • Ensuring enterprise data is stored cost-effectively	• Identify and resolve storage security issues • Prove adherence to their security configuration standards / baseline • Eliminates security risks for all their storage systems

Questions To Start A Conversation With Your Clients

Do you scan your OS and network for vulnerabilities and misconfigurations?

Who in your organization is responsible for ensuring your backups are hardened?

How do you assess data recoverability in the event of a cyberattack?

Do you also currently scan your storage & backup environment? If not, are you interested in doing so?

How do you manage and prioritize storage security risks? Are these done manually?

How do you verify that your storage & backup systems are configured in a compliant manner? And aligned with the relevant security regulations?

How do you identify and resolve storage & backup security issues?

How do you keep track of storage & backup configuration changes?

Objection Handling

01 “Our storage is too deep to reach, and too obscure to attack”

It's much easier to get into the storage layer than you think! Social engineering tactics can fool even the most experienced storage admin, and all it takes is a click on a fictitious link in an email, to dump malware onto the network. From here, the road to directly controlling the storage device is nice and easy for the attacker.

02 “I have backups, so what could possibly go wrong?”

Backup copies can definitely save the day, when something goes wrong. But if attackers get access to the storage system, they can easily wipe out those snapshots and backups.

In fact, the same admin credentials that were used to access the production servers can also be used to get to the replicas. And this means that attackers can also delete the replicas – just as soon as they finish with the production storage.

Even immutable storage can be ‘poisoned’, enabling attackers to change the configuration of backup clients, and gradually replace stored data with junk data.

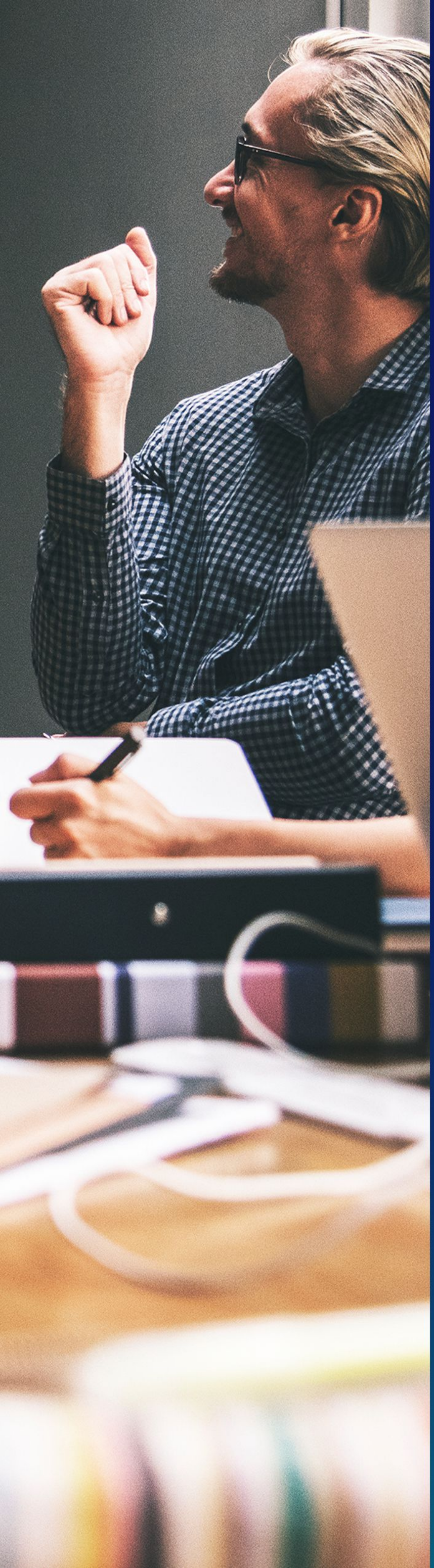
03 “We already have a vulnerability scanning tool. I got it covered!”

While existing vulnerability management solutions scan everything from the operating system to the network, they offer almost no coverage for storage, storage management, or backup systems. I encourage you to double-check with your existing vulnerability management vendor, to ensure they have broad coverage of your storage & backup systems.

If they don’t, then look for a vendor that understands storage & backup, and can help you fill this gap.

04 “If my data is encrypted, why do I need to secure my storage?”

Data encryption won’t prevent attackers from hacking into an organization's storage systems. And once inside, attackers can delete petabytes of data volumes – whether they’re encrypted or not.



FAQS

We have our network and OS covered. Why do we need storage security?

Perimeter-based defense is not enough to protect against threats. The storage system is where all data is kept. Your existing vulnerability scanning solutions cover everything today, except for your storage, backup and storage management systems.
When a hacker gets control of a desktop, the damage is minimal. But when a hacker gets control of the storage systems, they have access to ALL THE DATA! This includes backup, copies, recovery copies, and production Data. They can delete it, corrupt it, or sell it.

What are the possible impacts of an unsecured storage system?

Attackers with access to a storage system could delete data volumes, encrypt data volumes, make data volumes inaccessible, corrupt / delete data recovery volumes and snapshots. A single storage array serves hundreds of database and application servers, thus a compromised storage system would cripple at least dozens business services and applications.

Why is Storage Security essential for Ransomware protection? (and why now)

There has been a major shift in the threat landscape, with the emergence of ransomware-as-a-service. The first step taken by threat actors is to knock out an enterprise's ability to recover from an infection, by exploiting vulnerabilities in storage and storage management configurations.

A hacked storage system is the equivalent of hacking two hundred servers!

This greatly improves the incentive for enterprises to pay the ransom, after the critical data is exfiltrated and then encrypted. And it has significant implications for CISOs and Heads of Storage and requires a drastically different approach to cybersecurity.

Storage also plays a critical role in the ability to recover from a cyberattack, since storage is where replicas, snapshots and backups are kept.

What kind of checks does StorageGuard perform?

Automatically identifying storage security misconfigurations and vulnerabilities. Our checks repository is constantly updated with security recommendations based on the following publications

- *Vendor Security guides and articles: Dell EMC, IBM, Hitachi, NetApp, INFINIBOX, Brocade, HPE, Pure and others*
- *Information Security standards: NIST, ISO/IEC, PCI DSS, CIS Control, FFIEC and more*
- *Security advisories, bulletins and CVEs (MITRE / vendors)*
- *Community feedback – security configuration baseline suggestions by users*

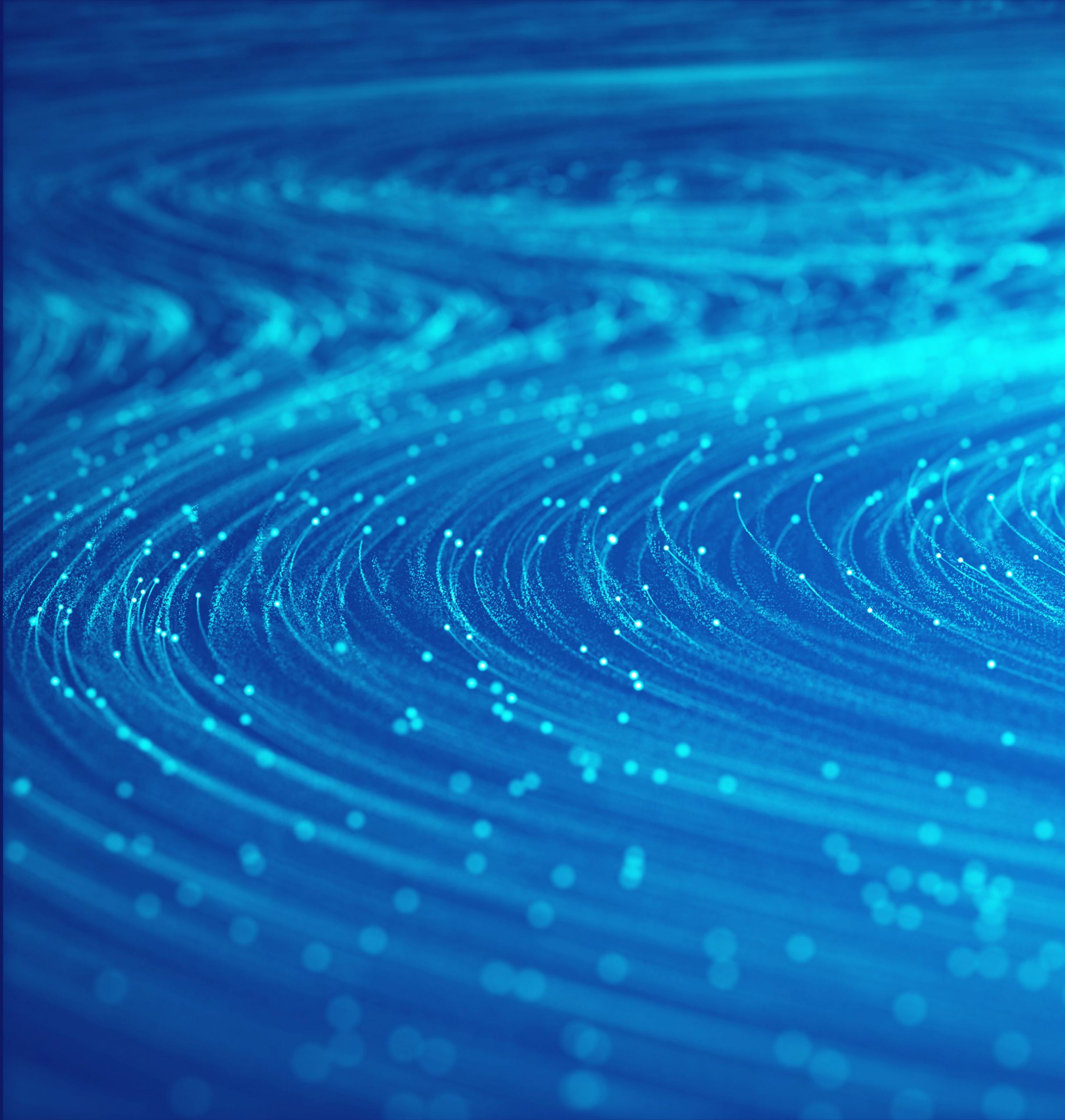
The checks cover a wide range of areas: authentication, authorization, administrative access, malware protection, services and protocols, interfaces and ports, anti-ransomware, SAN access control, encryption, audit logging, NAS access control, object access control and more.

Which storage systems and devices does StorageGuard support?

StorageGuard supports storage arrays, storage networking, data protection appliances, storage virtualization, storage management, storage software and plugins.

How is securing storage different than securing servers?

- *Different network model (SAN vs TCP)*
- *Different access control features (zoning, masking)*
- *Scanning agents cannot be installed on the majority of storage systems (closed systems / appliances)*
- *Some of the systems run non-standard operating systems*
- *Some of the systems are only accessible through vendor-specific commands / programs (CLI/API)*
- *Difficulty to identify the attack surface; including all hosts installed with storage CLI/API kit*
- *Lack of storage security expertise within IS/IT*
- *Poor support by existing Security Vulnerability Scanning solutions – in terms of coverage and depth*



WWW.CONTINUITYSOFTWARE.COM