



THE STATE OF **STORAGE SECURITY** REPORT

ASSESSING THE VULNERABILITIES OF ENTERPRISE STORAGE

In the first of its kind, Continuity has published a new research report that provides an analysis of the vulnerabilities and misconfigurations of enterprise storage systems.

We compiled anonymized inputs from a large number of storage risk assessments, to provide a unique insight into the state of storage security. The analyzed data covers multiple storage vendors and models including Dell EMC, IBM, Hitachi Data Systems, Cisco, Brocade, NetApp, and others.

Continuity's automated risk detection engines check for thousands of possible misconfigurations and vulnerabilities at the storage system level that pose a security threat to enterprises' data.

In preparation of this report, thousands of discrete security misconfigurations were reviewed, allowing us to uncover recurring patterns and important security considerations many organizations fail to get right when managing storage.

KEY FINDINGS



6,300 discrete security issues detected



An enterprise storage device has 15 vulnerabilities



Out of 15 vulnerabilities, 3 are high or critical risk

THE MOST COMMON TYPES OF VULNERABILITIES INCLUDE

- Use of vulnerable protocols / protocol settings
- Unaddressed CVEs
- Access rights issues (over exposure)
- Insecure user management and authentication
- Insufficient logging

- 423 high-end storage devices were analyzed, and a total of more than 6,300 discrete security issues (e.g., vulnerabilities, misconfigurations) were detected, spanning more than 170 security principles that were not adequately followed (most frequent, and other high significance findings are discussed in more detail below).

- On average, an enterprise storage device has around 15 security vulnerabilities, out of which 3 were of high or critical risk rating (i.e., could present significant compromise if exploited).
- There was weak correlation between geographic location and storage security maturity (meaning, similar issue frequency and severity were observed in all environments regardless of their geographic location).
- Additional noteworthy findings were observed. Though far less frequent than the top 5, each could lead to substantial data compromise if exploited (see further details in the next section). These include:

Incorrect use of ransomware-protection features

Undocumented & insecure API / CLI

Vulnerabilities & oversight in storage software supply-chain management

RECOMMENDATIONS

The state of enterprise storage security is significantly lagging behind that of compute & network security.

This is a significant gap that should be addressed as soon as possible; with growing sophistication of data-centric attacks, and with tightened regulations, the business implications of ineffective resolution could rapidly increase.

- Determine if knowledge gaps exist in terms of storage security, and build a plan to address them
- Review your existing security program to determine how effectively it addresses storage and storage networking technologies – in particular, the key gaps identified in this report, and build a plan to close any identified gaps
- Consider the use of automation to continually evaluate the status of storage infrastructure security, in order to proactively address risks

These recommendations are covered in more detail throughout the report.

BACKGROUND ●

Of the three main IT infrastructure categories: Compute, Network, and Storage – the later potentially holds the greatest value, from both the security and business perspectives. Indeed, while compromise or loss of compute or network infrastructure could be highly disruptive - resulting in downtime - one imposed on storage presents a completely different threat.

If damage to data is sufficiently extensive, most organizations could sustain a devastating injury. Consider the position of a large bank if a coordinated attack succeeds in compromising current and long-term customer financial records (e.g., attacking both primary storage and its protective copies, such as snapshots, backup, and archived copies).

It is therefore evident that the storage layer should be secured and hardened to a similar if not greater extent than that employed for compute and network¹. A comprehensive storage security practice should cover the entire lifecycle of data².

With a growing industry and government attention to data storage security, resources are now available to guide organizations on building a secure storage management practice, including NIST SP-800-209 - published in 2020, ISO 27041 – published in 2015, and a series of educational storage security papers by SNIA.

Given the growing evidence, starting late 2019 and throughout 2020, that new forms of malware and ransoms are specifically targeting storage and backup systems, we came to realize it would be valuable to research and compile an industry benchmark for the state storage security, to gauge the overall market maturity and to identify if common areas of weakness or oversight exist.

The results of this research are included in this report. It is our hope that the findings could help organizations increase awareness to this important area, help identify gaps in existing plans, and provide insights based on community data.



¹ While many of the principles involved in securing storage are similar in nature to those used for compute and network infrastructure (e.g., authentication and authorization, access control, vulnerability management, etc.), certain aspects are unique to storage. These include proper design, implementation and testing of data protection and recovery, securing storage protocols and storage networking, and data immutability features.

² Encompassing secure design, enforcement of security principles during all deployment and maintenance phases, comprehensive testing, and ongoing auditing, vulnerability assessment and anomaly detection.

DETAILED INFORMATION ABOUT KEY VULNERABILITIES

Use of vulnerable protocols / protocol settings

Insufficient logging

Unaddressed CVEs

Incorrect use of ransomware-protection features

Access rights issues (over exposure)

Undocumented and insecure API / CLI

Insecure user management & authentication

Vulnerabilities & oversight in storage software supply-chain management

USE OF VULNERABLE PROTOCOLS / PROTOCOL SETTINGS

Storage protocols span both traditional networking³ (IP over Ethernet and WAN) and dedicated Fibre-Channel storage networking⁴. It is critical to secure those protocols both during session establishment, and while exchanging data. However, in a far too-high number of cases, and in most environments, it is still common to find configuration gaps such as:

- Not disabling legacy versions of storage protocols, or even worse, defaulting to their use (e.g., SMBv1, NFSv3)
- Use of no-longer recommended cypher suites (e.g., allowing TLS 1.0 and 1.1, not disabling SSL 2.0 and 3.0) – some of which must be disabled to comply with regulatory frameworks (e.g., PCI DSS)
- Not enforcing data encryption for critical data feeds (e.g., management transport, replication transport, backup transport)
- And many others (e.g., allowing cleartext HTTP sessions, using unsecure SNMP community strings, etc.)



Significance of the findings:



Incorrect access right management, can at best lead to data exposure, and at worst to compromise of the data itself and its copies, and in some cases, of the operating systems of the hosts that use the storage.

³ Mostly used for file and object storage, with a steadily growing (yet still far behind) use for block-storage

⁴ Encompassing FC switches, FC protocols, and FC network management protocols

UNADDRESSED CVES

There is a variety of software components used for Storage devices, and storage networking, that get updated from time to time, including:

- Device Operating systems (Proprietary, or highly specialized and restricted versions of commercial or open-source operating systems) – for storage arrays and network switches
- API servers (e.g., storage connectors for virtual environments)
- Controller firmware
- Management software suites
- And other

Vulnerabilities are discovered on an ongoing basis for such devices, and Common Vulnerability and Exposure (CVE) records are accordingly published. In most cases, a fix in the form of an upgrade, or configuration change is suggested. Common vulnerability management tools used by organizations and enterprises do not detect many storage CVEs (but rather focus on server OS, traditional network gear, software products), and there's a rather large percentage of storage devices (close to 20%) that are exposed.

MORE THAN 70 DIFFERENT CVES WERE DETECTED IN THE ENVIRONMENTS COVERED IN THIS RESEARCH (OF COURSE, MANY MORE EXIST).

Significance of the findings:



Each CVEs details the possible exposures and outcomes it presents – and these span a rather wide range. Among the risks identified in environments that were included in this research were the ability to exfiltrate files, initiate denial-of-service attacks, and even take ownership of files and block devices.



ACCESS RIGHTS ISSUES (OVER-EXPOSURE)

Access control to storage, includes several different configuration levels:



- Access to storage elements - such as block devices, network shares, or even individual files and objects should be mapped only to designated components (e.g., individual hosts or applications). This is done both at the device level (e.g., share configuration, LUN mapping) and using network filtering techniques (e.g., IP filters, SAN zoning and Masking)
- Level of access to the data itself (e.g., read, write, modify permissions and ownership, ACLs)
- Which elements and what users and roles are allowed access to advanced storage capabilities (e.g., management, control, replication, snapshot management)



A large number of devices were affected by improper configuration, including unrestricted access to shared storage, unrecommended zoning and masking configuration, ability to reach storage elements from external networks, and more.

Significance of the findings:



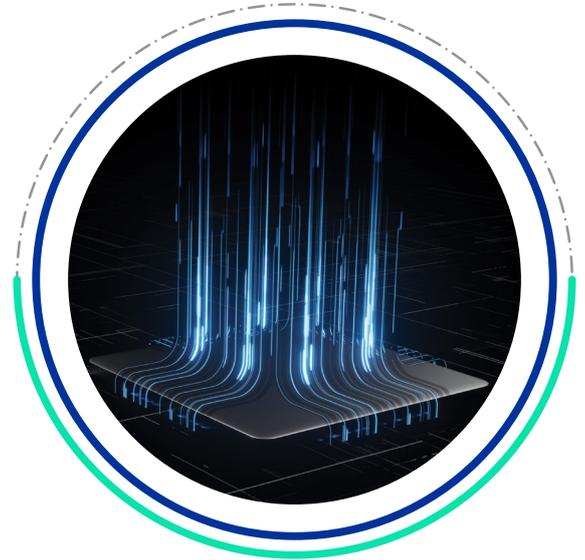
Incorrect access right management, can at best lead to data exposure, and at worst to compromise of the data itself and its copies, and in some cases, of the operating systems of the hosts that use the storage

INSECURE USER MANAGEMENT & AUTHENTICATION

Storage devices are managed using users and roles, and in many cases, access to the data itself is also regulated using similar means. There are basic recommendations for user management and authentication that are, for a variety of reasons, not kept for storage devices at the same rigor allied for compute & network elements.

THESE INCLUDES:

- Unrecommended use of local users (as opposed to approved central user management protocols) for routine operations – in far too many cases, default factory accounts were still in use
- Use of non-individual admin accounts
- Not enforcing session management restrictions
- Improper separation of duties (e.g., same roles used to manage data and its protection mechanisms – such as snapshots and backups)



Significance of the findings:



Incorrect and insecure configuration can allow adversaries to take full control over the storage device, up to, and including exfiltration and destruction of the data and its copies.

INSUFFICIENT OR INCORRECT LOGGING & AUDITING

Logging and auditing is a fundamental requirement of any sound security practice – including storage. All administrative activities and security configuration should be logged, and for sensitive information, it is also recommended that storage access should also be logged. Proper logging involves the correct configuration of logging (including level of detail, event types) – the configuration of approved, redundant central logging servers, correct timekeeping and more. A large percentage of production storage devices (around 15%) were not logged at all, and a substantial additional percentage of those that were logged was susceptible to manipulation.

Significance of the findings:



Improper logging can help adversaries mask malicious activities, and interfere with the ability of central security tools to detect anomalies.

INCORRECT USE OF RANSOMWARE-PROTECTION FEATURES

Modern storage devices become more sophisticated, and offer advanced ransomware detection and prevention capabilities, as well as advanced capabilities for locking retained copies, protecting critical data from tampering and deletion, and certain forms of air-gapping. These features are often overlooked – and even when used, many configurations did not meet vendor best-practices.

Significance of the findings:



Limited or no protection from ransomware, adversaries can easily circumvent or disable protection mechanisms.

UNDOCUMENTED & INSECURE API / CLI



There is a surprising number of ways storage devices can be manipulated and managed:

- Using device APIs
- Using management hosts and API gateways
- In-band – using storage protocols
- Using dedicated host agents
- Using storage agents on virtual infrastructure

Most of those control methods can be further managed to define what access level each can provide (e.g., which actions are allowed -including creation, destruction, mapping, copying, and more), what components could be controlled, filtering as to which IPs, devices and objects can connect and more.

It is of an utmost importance to approve and document all allowed connections, limit their access level and scope to the minimum, and to actively block any other connection.

In around 10% of the environments undocumented API entry points were found, whose purpose could not be accounted for, and in around 20% of the environment approved mechanisms were not properly hardened and limited.

Significance of the findings:



Undocumented and insecure API and CLI access paths can provide an adversary with a backdoor to control storage devices, exfiltrate data, and tamer with storage content and its backups.

VULNERABILITIES AND OVERSIGHT IN STORAGE SOFTWARE SUPPLY-CHAIN MANAGEMENT

As already discussed, storage device updates are regularly issued. In certain organizations these updates, as well as transfer of support information is performed with designated vendor support environments outside of the customer premises. In other organizations, even though it's an established policy to not allow connection to vendor support environments – such connections were still found enabled and active.

In any case, there's a set of minimal safeguards that need to be observed in regards to software updates (manual or automated) – including proper signing, proper end-to-end encryption when obtaining binaries, proper authentication and IP filtering, etc.



In several of the environments, configuration issues were detected that can allow unapproved images to be deployed, or can allow an adversary to intercept and tamper with data transfer and support sessions.

Significance of the findings:



Improper control and enforcement of software supply-chain paths can allow adversaries to tamper with the storage OS, and thereby gain full control over the devices, the data, and its protective copies.

SUMMARY & RECOMMENDATIONS

It appears that the state of enterprise storage security is significantly lagging behind that of compute and network security. This is a significant gap that should be addressed as soon as possible; with growing sophistication of data-centric attacks, and with tightened regulations, the business implications of ineffective resolution could rapidly increase.

On the bright side, industry awareness of storage security is growing, and new resources and guidance are available to help organizations build an effective program to address the gap.

It is recommended to evaluate existing internal security processes to determine if they cover storage infrastructure to a sufficient degree. Some of the questions that could help clarify the level of maturity of storage security planning are:

Do our security policies cover specific storage, storage networking, and backup risks?

Are we evaluating storage infrastructure security on an ongoing basis?

Do we have detailed plans & procedures for recovery from a successful attack on a storage or backup system? Do we test such procedures?

How confident are we that the key findings highlighted in this report, & similar ones do not, and can not occur in our environment?

If needed, third parties and vendors could be consulted, or invited to be involved in such evaluation. Based on the findings, we'd recommend:

- Determining if knowledge gaps exist in terms of storage security, and building a plan to address them
- Improving security program to address identified gap
- Considering the use of automation to continually evaluate the status of storage infrastructure security, in order to proactively address risks



FINALLY, WE ENCOURAGE THE READERS TO LEARN MORE ABOUT STORAGE SECURITY.
A GOOD START COULD BE:

Read the NIST Guide for Storage Security – co-authored by Continuity.

There's also a selection of practical guides on

www.continuitysoftware.com

NEXT STEPS

This is the first of its kind storage security analysis. It is our hope and intention to periodically publish follow-up reports, and to continually expand the sample base, improve the metrics, and include additional information that is of interest to our readers, and the industry. To this end, we would love to get your feedback on the level of detail you expect in future surveys, and your thoughts as to what additional areas you think we could cover.

Of course, we'd also be pleased to offer our services to help you evaluate and assess your storage infrastructure.

marketing@continuitysoftware.com

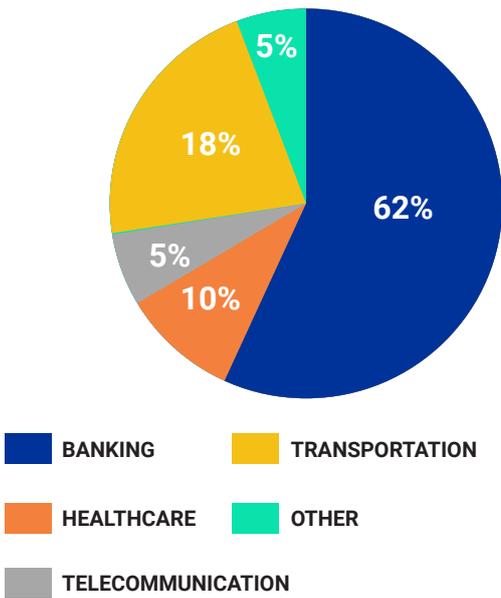


METHODOLOGY

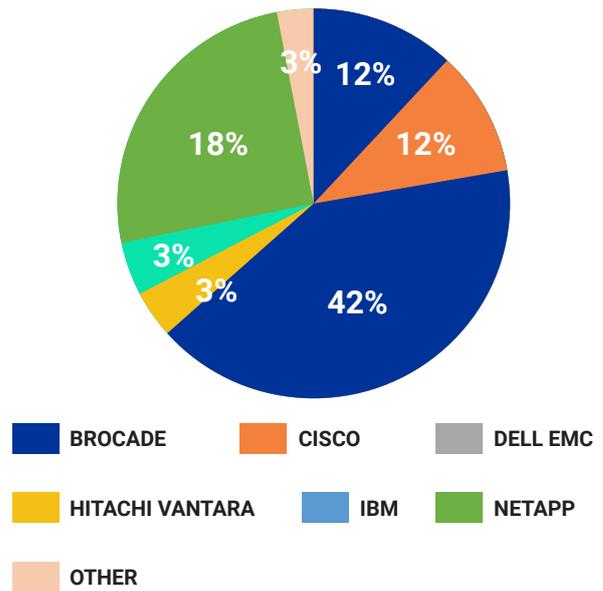
Continuity has more than 15 years of expertise in evaluating and validating the configuration of storage systems – using advanced software tools. While our software can be integrated into existing SIEM implementations, continually scan the organizational storage for vulnerabilities, and facilitate auto-healing – we also offer organizations with a one-time storage security assessment.

We have compiled anonymized inputs from over 20 customer environments, that provide a unique cross-industry insight into the state of storage security:

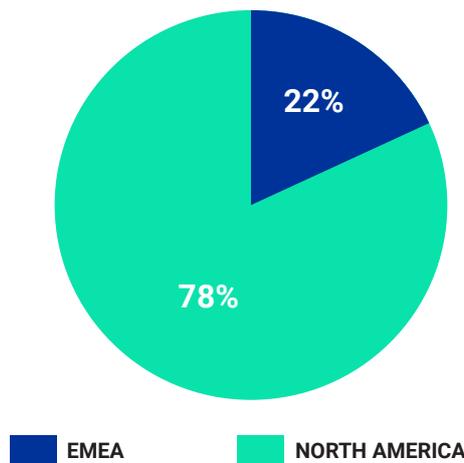
DEMOGRAPHICS - BY INDUSTRY



DEMOGRAPHICS - BY STORAGE VENDOR



DEMOGRAPHICS - BY GEOGRAPHIC LOCATION



The data in this report was collected and analyzed from configuration data across multiple storage vendors and models including Dell EMC , IBM, Hitachi Data Systems, Cisco, Brocade, NetApp, and others.

⁵ Including multiple product families, including: Symmetrix, DataDomain, Isilon, XtremIO, and VPLEX

The analysis covered in the configuration of block, object and IP storage systems, SAN / NAS, storage management servers, storage appliances, virtual SAN, storage network switches, data protection appliances, storage virtualization systems and other storage devices.

Our automated risk detection engines check for thousands of possible misconfigurations and vulnerabilities at the storage system level that pose a security threat to enterprises' data. These misconfigurations fit into 4 main categories:

Violations of vendor security configuration guidelines

Violation of compliance framework requirements (CIS, NIST, PCI DSS and others)

Identified storage Common Vulnerabilities & Exposures (CVEs)

Deviation from community-driven best practices (gathered and generalized from dozens of enterprise internal security baselines for storage – representing shared community insights)

Each finding is tagged with a security risk index (1-5), and is tracked with a wide array of tags, that allow for detailed assessment, aggregation, and drill down. These tags include:

- Demographics: Industry, country & region, organization size (# of devices, # of employees, ...)
- Device tags: vendor, model, model, capacity, firmware level, ...
- Security principle (e.g., authentication, authorization, logging, encryption, least-privileges, and their sub-categories)
- Security frameworks (compliance framework, organization baselines)
- And more

In preparation of this report, more than 6,000 discrete security misconfigurations were reviewed, allowing us to uncover recurring patterns and important security considerations many organizations fail to get right when managing storage.



C@NTINUITY