THE STATE OF STORAGE & BACKUP SECURITY REPORT 2023

CONTINUITY

Assessing The Security Risks Of Enterprise Storage & Backup Systems

Continuing the tradition we started in 2021, Continuity is now publishing the 2023 research report that provides an analysis of the security risks of enterprise storage and backup systems.

We compiled anonymized inputs from a large number of storage and backup risk assessments in 2022, to provide a unique insight into the state of storage and backup security. The analyzed data covers multiple storage and backup vendors and models including Dell EMC, IBM, Hitachi Vantara, NetApp, Veritas, Commvault, Cisco, Brocade (Broadcom), and others.

Continuity's automated risk detection engines check for thousands of possible security misconfigurations and vulnerabilities at the storage and backup systems 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 and backup.

Key Findings

9,996
9,996 discrete security issues were analyzed.

14
An enterprise storage & backup device has on average 14 vulnerabilities

3
Out of 14 vulnerabilities, 3 are high or critical risk

245 environments assessed, with 8,589 storage & backup devices, of which 702 were selected for analysis (*)

The 5 most common types of risks include:

01 Insecure network settings

02 Unaddressed CVEs

03 Access rights issues (over exposure)

04 Insecure user management and authentication

05 Insufficient logging & auditing

Note (*): To prevent any bias, device selection was performed by the organizations who participated in the risk assessments (and not Continuity). Each organization was asked to choose a representative sample from each of their environments.

The research scope has significantly increased compared to the last report (by more than 65%). **It includes 245 different organizational environments.**

Just over 60% of organizations were from the Banking sector. The remaining industries included Healthcare, IT Services, Media, Shipping Carriers, Financial Services, and Telecommunications.

702 enterprise storage & backup devices were analyzed (an increase of 66% from last year), and a total of 9,996 discrete security issues (e.g., vulnerabilities and security misconfigurations) were detected, spanning more than 270 security principles that were not adequately followed. Most frequent, and other significant findings are discussed in more detail below.

On average, an enterprise storage & backup device **has 14 security risks**, out of which 3 were of high or critical risk rating (i.e., could present significant compromise if exploited). While this finding was similar in the previous report, there was a change in the types of issues detected, as further discussed below).

Similar to the previous report , weak correlation was observed between geographic location and storage & backup security maturity. This means that similar issue frequency and severity were observed in all environments regardless of their geographic location.

We didn't detect any significant correlation between security maturity and industry segment. Although it is commonly accepted that certain industries, like financial services, tend to have more mature security strategies, this report shows that the entire field of storage & backup security across all industries is still overlooked. While this was similar to the last report, it is still very surprising, given the severity of recent-years data-targeted attacks, and the amount of time the industry had to develop more robust security measures.

Top five security risks found in this year's analysis:

01 Insecure network settings

02 Unaddressed CVEs

03 Access rights issues (over-exposure)

04 Insecure user management and authentication

05 Insufficient or incorrect logging and auditing

In addition to the five most common risks, other risks that appeared less frequently but were classified as high priority, included:

06 Vulnerabilities in software supply-chain management

07 Incorrect configuration or non-use of anti-ransomware features, including immutability

08 Undocumented and insecure API / CLI

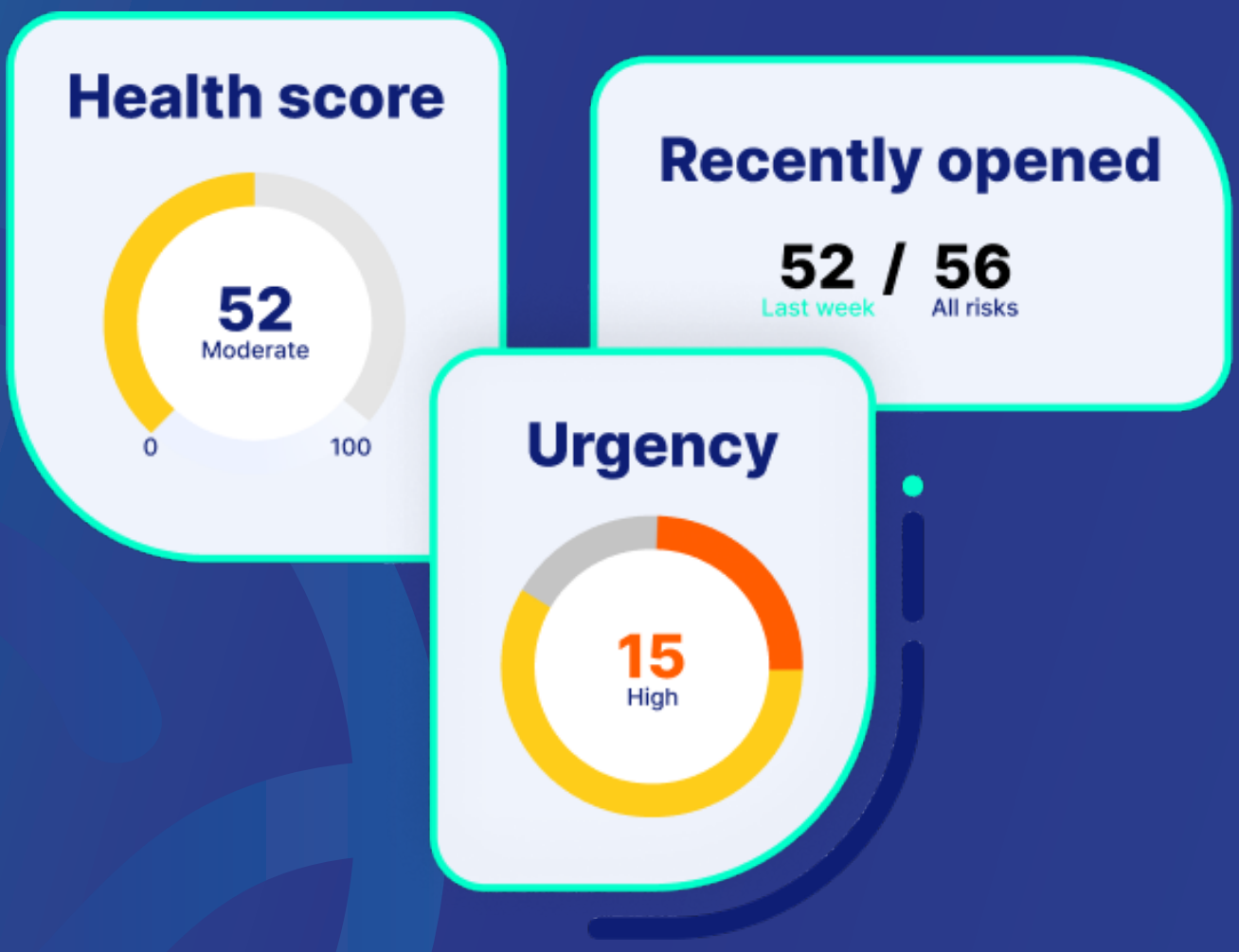
Recommendations

The state of enterprise storage & backup 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.

Determine if knowledge gaps exist in terms of storage & backup security, and build a plan to address them

Improve security program to address identified gap

Proactively address risks by using an automated solution that continually validates the security posture of your storage and backup systems



Observations

Backup & Data Protection Systems

We did not see a significant difference in the number of security misconfigurations or unresolved CVEs in backup environments compared to storage systems; both suffer equally from a lack of hardening.

In the past two years, online backups were frequently targeted as part of ransomware attacks. This led to data being deleted or made otherwise unusable to prevent recovery of now-encrypted primary data. Our recommendation is to maintain an immutable, preferably offline copy of backups and test them regularly to ensure viability.

Immutability

In our analysis, we detected an increase in the number of storage and backup environments with immutable data copy technology. This is an important capability; however, it can lead to a false sense of security if not implemented properly, and unfortunately, we did detect a significant number of misconfiguration issues specific to these features.

When misconfigured, it is possible to delete supposedly immutable data (for example, by manipulating time/date settings on the storage device to bypass retention enforcement mechanisms). Even when configured correctly, an attacker with access to the data source can poison an immutable data store over time, corrupting it such that it becomes useless when needed for recovery.

Ransomware

Unpatched vulnerabilities are the main points of attack for most ransomware, a recent example being the ESXiArgs ransomware variant that exploited a two-year-old CVE in unpatched VMware clusters[1]. This gap in simple CVE remediation can undermine any other ransomware-focused defense.

[1] Hackers exploiting two-year-old VMware flaw to launch large-scale ransomware campaign | TechCrunch

Observations

Russia-Ukraine Conflict

State-sponsored hacking groups associated with the Russian government were implicated in numerous cyberattacks going back to the 2017 NotPetya malware outbreak across Europe, Asia and beyond. These types of attacks have continued during the Russia-Ukraine conflict, targeting Ukraine, the United States, Finland, and other nations.

A Microsoft Digital Security Unit report on the Russia-Ukraine conflict identified no fewer than eight malware families leveraged by Russia-aligned cybercriminals[2] , most of which are designed for data encryption, destruction, or exfiltration. The same report called for heightened vigilance against further state-sponsored attacks against NATO countries, other states supporting Ukraine, and their constituent organizations or businesses.

Nation-state actors may use novel tools, but their avenues of attack often fall along familiar lines like spear-phishing that can be mitigated by standard cyber security protocols laid out by NIST, ISO, and others. Note that adoption of these protocols is quickly becoming a prerequisite for cyber insurance coverage, discussed in further detail below.

Compliance & Cyber Insurance

Cyber insurance has become a hot commodity in the past three years, spurred by events like the Colonial Pipeline ransomware attack. Direct written cyber insurance premiums rose by 74% in 2021[3] and according to a recent survey of insurance agents and brokers, 81% reported "a top client concern was cyber risk"[4].

Storage and backup vendors are getting into the picture as well, offering warranties that data protected by their ransomware defense solutions can be recovered in case of an attack. The fine print on these guarantees typically lays out very detailed requirements including an active support contract, using the latest versions of software, etc. Note that potential payouts are often limited, making such warranties useless for larger enterprises.

Due to the increased liability exposure, insurers are implementing stricter baselines for coverage; these include improved basic authentication and authorization controls like multifactor authentication and least privilege access models, adherence to NIST guidelines, separation of storage & backup network access and admin roles from other IT functions, and third-party audits.

Shared Responsibility Model

Storage and backup vendors ship their systems with a minimal base-level of security configuration, one that is often insufficient for use in a production environment, and provide separate guidance for further hardening by the end user. It is the end-user responsibility to develop their own security baseline following current industry best practices, determine how best to implement a configuration adhering to that baseline, and then ensure that configuration is enforced continuously over time – not just at initial deployment.

Roles & Responsibilities: IT Infrastructure vs. Security

We have noted a repeated pattern of division between IT infrastructure and security teams, whereby security teams develop security policies and procedures that infrastructure teams are tasked with implementing, sometimes with minimal direction.

Often, security teams are not aware of cyber resiliency capabilities offered by storage and backup systems, while infrastructure teams are more focused on day-to-day operations and less concerned with reducing the potential for cyberattacks.

This division is underlined by our findings, which show the use of insecure protocols and unpatched CVEs continue to be the top security risks. These issues are among the most basic aspects of a strong data security posture. An opportunity now exists to increase the level of security literacy among the teams who manage data storage and backup, while improving the storage-specific knowledge and toolsets available to security teams.

[2] Special Report: Ukraine – April 27, 2022, Microsoft Digital Security Unit
[3] 2022 Cyber Supplement Report for 2021 Data, National Association of Insurance Commissioners
[4] Q3 Property / Casualty Market Survey 2022 – Council of Insurance Agents and Brokers

Background

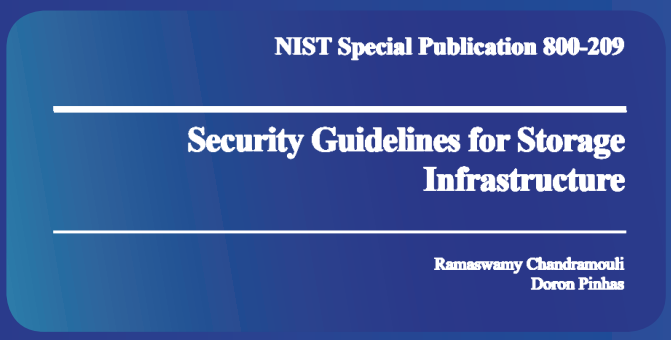
Of the three main IT infrastructure categories: Compute, Network, and Storage – the later potentially holds the greatest value, from both the security and business perspectives. Indeed, while compromise or loss of compute or network infrastructure could be highly disruptive - resulting in downtime - 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 network[5]. Acomprehensive storage & backup security practice should cover the entire lifecycle of data[6].

With a growing industry and government attention to data storage & backup security, resources are now available to guide organizations on building a secure storage management practice, including NIST SP-800-209 'Security Guidelines for Storage Infrastructure', ISO 27040 (to be published at the end of 2023), and a series of educational storage security papers by SNIA.


NIST Special Publication 800-209

Security Guidelines for Storage Infrastructure

Ramaswamy Chandramouli
Doron Pinhas

Given the growing evidence that new forms of malware and ransomwares 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 of storage & backup security, to gauge the overall market maturity and to identify if common areas of weakness or oversight exist.

Encouraged by enthusiastic interest in our first issue published in 2021, we are pleased to provide an updated analysis of the state of the storage and backup security. This year we've expanded our analysis scope, and highlighted the major trends in 2023, and the differences between this report and the previous one.

It is our hope that these reports could help organizations increase awareness to this important area, help identify gaps in existing plans, and provide insights based on community data.

[5] While many of the principles involved in securing storage and backup 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 and backup. These include proper design, implementation and testing of data protection and recovery, securing storage protocols and storage networking, and data immutability features.

[6] 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 Security Risks

01

Insecure Network Settings

Storage protocols span both traditional networking[7](IP over Ethernet and WAN) and dedicated (Fibre-Channel) storage networking[8]. It is critical to secure storage and backup network settings both during session establishment, and while exchanging data. However, in too many cases, and in most storage and backup 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 (Allowing cleartext HTTP sessions, using unsecure SNMP community strings, etc.)

Business Impact

Cybercriminals can use such configuration mistakes to retrieve configuration information and stored data, and in many cases, can also tamper with (e.g., modify, destroy, lock) the data itself, including the copies used to protect the data.

Recommendations

Close knowledge gaps refer to resources such as NIST 800-209 and SNIA to get familiar with storage and backup network security concepts, risks, and best practices

Define internal requirements to adapt industry recommendations to business requirements

Identify and remediate gaps between requirements and actual settings

Build an effective, ongoing process to continually evaluate the storage and backup security posture

[7] Mostly used for file and object storage, with a steadily growing use for block storage
[8] Encompassing FC switches, FC protocols, and FC network management protocols

02

Unidentified And Unaddressed Vulnerabilities

There are a number of software components used for storage and backup systems that get updated from time to time, including:

Storage arrays, backup appliances, fibre-channel storage switches - all have operating systems (often proprietary, or highly specialized and restricted versions of commercial or open-source operating systems)

IO Controller (such as HBAs, FCoE, NVMEoF adapters) have dedicated firmware

Management software suites

API servers (e.g., storage connectors for virtual environments)

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 recommended.

Common vulnerability management tools used by organizations **do not detect the majority of storage and backup CVEs** (but rather focus on server OS, traditional network, and software products). This is why a large percentage of storage and backup devices are exposed.

198 different CVEs were identified in the environments covered in this research (of course, thousands are documented), with an alarming 28% of the devices analyzed being exposed.

Business Impact

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

Recommendations

Improve proactive CVE identification use storage-specific tools to scan storage and backup environments for CVEs, instead of server-specific vulnerability management tools that cannot identify storage and backup platforms appropriately

Reduce remediation time for important vulnerabilities identify and patch CVEs with critical and high CVSS scores as quickly as possible, using all relevant tools (in-house scans, vendor security announcements, etc.)

03

Access Rights Issues (Over-Exposure)

Access control to storage & backup, 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, file-level and device-level ACLs)

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.

Business Impact

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

Recommendations

Implement appropriate least-privilege access models both for data access (file/LUN/object etc.) as well as management and control planes

Audit and correct exposures on a frequent basis, in an automated (and thus easily repeatable) way

04

Insecure User Management And Authentication

Storage and backup systems 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 level as they are for compute and network elements. These include:

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)

Business Impact

Incorrect and insecure configuration can allow cybercriminals to take full control over storage and backup systems, and enable them to exfiltrate and destroy the data – and its copies.

Recommendations

Lock and rename or delete factory default users, where possible

Eliminate the use of local user accounts use centralized authentication mechanisms such as Active Directory or LDAP

Separate responsibilities and access roles for primary data copies and secondary data copies e.g. storage admins should not have admin access to backups, while data vault administrators should not have admin access to production systems

Enable multifactor authentication

05

Insufficient Or Incorrect Logging And Auditing

Logging and auditing are fundamental requirements of any security practice – including storage. All administrative activities and security configuration should be logged. For sensitive information, storage access should also be logged.

Thorough logging involves the correct configuration of logged-events, the configuration of approved, redundant central logging servers, correct timekeeping and more. 15% of production storage devices were not logged at all, and a significant number of those that were logged were susceptible to manipulation.

Business Impact

Improper logging can help cybercriminals mask malicious activities and interfere with the ability of central security tools to detect anomalies. In particular, any backup configuration change and data retrieval should be logged, as they are often the pre-cursors of data theft, and backup-poisoning attacks.

Recommendations

Log to external repositories configure redundant logging targets for each device

Configure external timekeeping Use at least two NTP sources

Ensure granular logging at a minimum, log all authentication failures, all administrative / security configuration events, and all storage access events for critical or sensitive data. Carefully log backup configuration changes, and data restores

In addition to the five most common risks, other risks that appeared less frequently but were classified as high priority, included:

06

Vulnerabilities In Software Supply-Chain Management

As already discussed, updates to storage & backup systems are regularly issued. For some organizations these updates, as well as transfer of support information, are performed with designated vendor support environments outside of the organization premises.

Although there are established policies to prevent connection to vendor-support environments, such connections were still found enabled and active in some organizations.
In any case, there is a set of minimal safeguards that need to be observed for software updates (manual or automated). These include proper signing, end-to-end encryption when obtaining binaries, proper authentication and IP filtering, etc.

In several environments, configuration issues were detected that could allow unapproved images to be deployed, or enable cybercriminals to tamper with data transfer and support sessions.

Business Impact

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

Recommendations

Implement whitelists disallow access to all but specifically approved and verified sources / IP addresses for software and firmware updates

Use only secure transmission methods only allow downloads or remote support efforts over secured connections from hosts with verified certificates

Verify packages use md5sum or other hash checking to verify a software package prior to installation

Do not allow externally-initiated support connections require that any connection to a third party, e.g., remote support and software download, originate from within your network

07

Incorrect Use Of Ransomware-Protection Features

Modern storage and backup systems provide advanced ransomware detection and prevention capabilities, as well as 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.

Business Impact

With limited or no protection from ransomware, cybercriminals can easily circumvent or disable protection mechanisms.

Recommendations

Implement and follow vendor best practice for ransomware-defense features including data immutability enabling identification and blocking of known attack indications (e.g., known ransomware file-suffixes), etc.

Be aware of potential impact while implementations differ, immutability features typically increase overall storage consumption with trickle-down effects on replication and performance

Immutability considerations pay attention to relevant vendor best practices, such as enabling retention lock, hardening time-server configuration, and enabling MFA

08

Undocumented And Insecure API / CLI

There are a surprising number of ways storage and backup systems 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 it can provide (e.g., which actions are allowed, including creation, destruction, mapping, copying, and more), which components could be controlled, filtering to which IPs, and more.

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

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

Business Impact

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

Recommendations

Document all approved control points disable any other method of access

Allow administrative connections from only designated hosts jump boxes, management VLANs, etc.

Implement least-privileged access models where possible, strictly scope allowed API calls by role

Summary and Recommendations

It appears that the state of enterprise storage & backup 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 and backup 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 and backup 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 the security of our storage & backup infrastructure on an ongoing basis?

Do we have detailed plans and 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, and similar ones do not, and cannot occur in our environment?

If needed, 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 & backup security, and building a plan to address them

Improving security program to address identified gap

Proactively address risks, by using an automated solution that continually validates the security posture of your storage and backup systems

Finally, we encourage you to learn more about storage & backup security.
A good start could be:

Read the NIST SP-800-209 Security Guidelines for Storage Infrastructure - co-authored by Continuity.

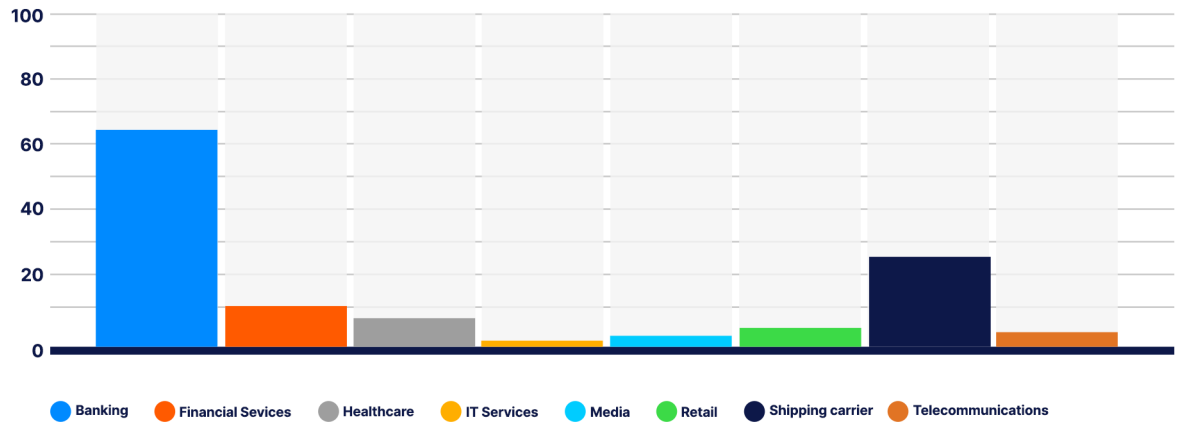
There's also a selection of practical guides on www.continuitysoftware.com

Methodology

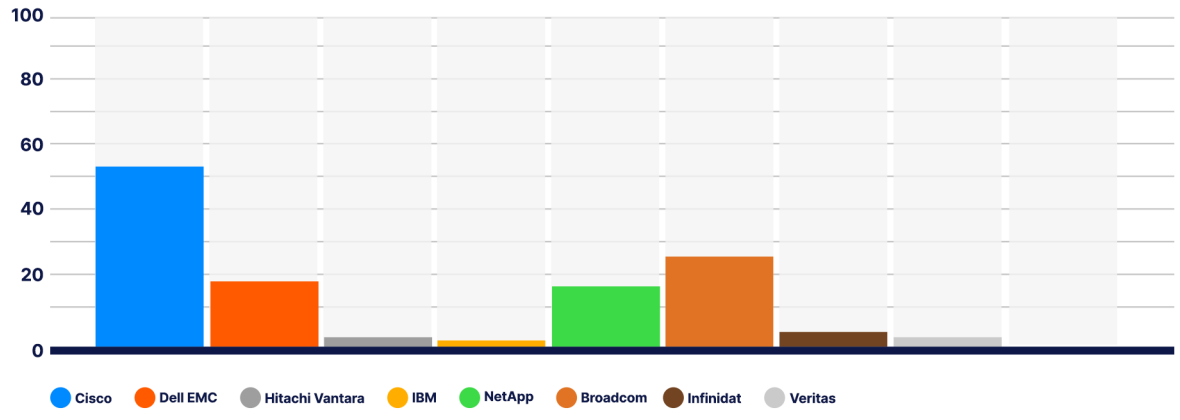
Continuity has 17 years of expertise in evaluating and validating the configuration of storage and backup systems. Our product, StorageGuard is a dedicated security posture management solution for storage and backup systems, scanning these critical systems for security misconfigurations and vulnerabilities, while auto-remediating many of those risks.

For this research, we compiled anonymized inputs from 245 customer environments, providing a unique cross-industry insight into the state of storage and backup security:

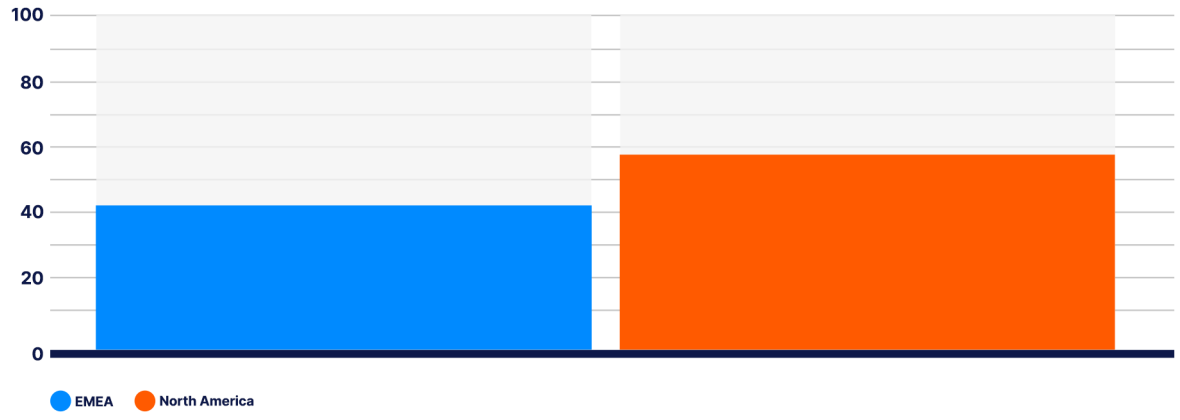
Demographics by industry



Demographics by storage & backup vendor



Demographics by geography



The data in this report was collected and analyzed from configuration data across multiple storage and backup vendors and models, including Dell EMC, IBM, Hitachi Vantara, Commvault, Cisco, Brocade (Broadcom), NetApp, Veritas (NetBackup), and others.

The analysis covered 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, backup software, backup appliances, and other storage devices.

Our automated risk detection engines check for thousands of possible security misconfigurations and vulnerabilities at the storage and backup system level that pose a security threat to enterprises' data. These security risks 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 and 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, 9,996 discrete security risks were reviewed, allowing us to uncover recurring patterns and important considerations many organizations fail to get right when managing the security posture of their storage and backup systems.

CONTINUITY

www.continuitysoftware.com