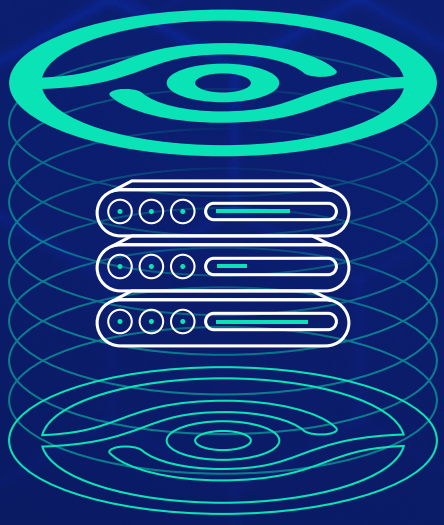
Storage & Data Protection Survey Results



2025 Priorities for Storage & IT Infrastructure Teams

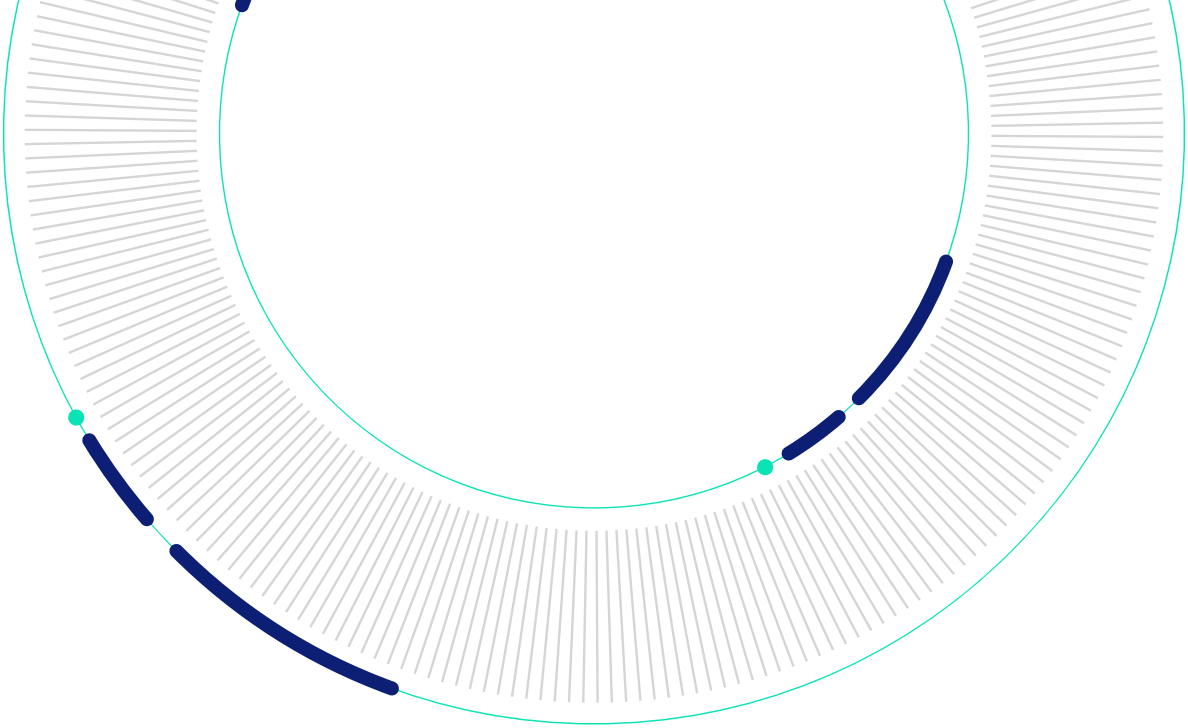
CONTINUITY

In a survey we ran throughout May-August 2024, we compiled feedback from Storage, Backup and IT Infrastructure leaders in Fortune 500 enterprises.

The purpose of this survey was to understand their plans and priorities for managing configuration of storage & backup environments, staying on top of configuration changes, deploying new cyber recovery capabilities, as well as navigating audit compliance requirements.

Key Findings

The top 4 **configuration** areas Storage teams are looking to improve are:	The top 4 **security & recoverability** areas Storage teams are looking to improve are:	The **standards that are internally mandated** for Storage, Data Protection and Backup Systems include:
1. **65%** - Detect hardware or software reaching end-of-support	1. **77%** - Backup and restore of system configuration	1. **49%** - NIST 800-53
2. **53%** - Detect deviation from ransomware protection best practices and vendor's hardening guidelines	2. **63%** - Data classification at the storage volume, pool or backup policy level	2. **44%** - PCI DSS
3. **53%** - On-demand configuration compliance evidence reporting	3. **58%** - Detect devices exposed to security advisories and alerts	3. **33%** - CIS
4. **44%** - Benchmark your security posture score against industry peers	4. **42%** - Detect immutability and isolation misconfigurations	4. **30%** - ISO/IEC 27000 series



Configuration

Detect hardware or software reaching end-of-support

As storage and backup systems reach end-of-support, vendors stop providing updates, patches, and technical support. This leaves your mission-critical systems vulnerable to security risks.

By proactively detecting and addressing end-of-support systems, you can ensure continuous security posture and data protection – while improving system reliability.

Detect deviation from ransomware protection best practices and vendor's hardening guidelines

As ransomware threats grow, organizations are increasingly looking at ways to secure their storage & backups, yet many still feel vulnerable.

Key strategies include implementing immutable backups, secure snapshots, anomaly detection, user behavior analysis, multi-factor authentication (MFA), two-person integrity controls, and secure time synchronization.

Additionally, it's crucial to rigorously follow vendor-recommended hardening guidelines, such as enforcing encrypted communications, account lockout policies, and the use of robust cipher suites and hashing algorithms, to ensure comprehensive protection.

On-demand configuration compliance evidence reporting

Many organizations still rely on manual processes to prove compliance during audits, recognizing the need for improvement.

Manual evidence gathering is cumbersome, time-consuming, and lacks repeatability. Automation can streamline compliance validation and evidence production, whether it's for data at-rest encryption or TLS configurations. By automating these tasks, organizations can operate at scale, efficiently manage diverse systems, and reduce dependence on individual team members, ultimately improving accuracy and consistency in compliance efforts.

Benchmark your security posture score against industry peers

Survey participants are keen on benchmarking their security posture against industry peers, probably because it provides a clear understanding of where they stand in terms of security maturity.

By comparing their scores, they can identify gaps, prioritize improvements, and justify investments in security initiatives. This benchmarking also fosters a competitive spirit, driving organizations to achieve higher standards, and offers reassurance that their practices align with or exceed industry norms, ultimately enhancing overall data protection and compliance.

Security & Recoverability

Backup and restore of system configuration

In conjunction with data backup, it is crucial to also regularly backup device and system configurations.

System configuration includes settings, policies, and operational parameters, and are critical to the proper functioning and performance of storage and backup infrastructure.

In the event of a system failure, corruption, or cyberattack, having a backup of these configurations ensures that the system can be quickly and accurately restored to its operational state; minimizing downtime and avoiding the complexities of manual reconfiguration.

This capability not only safeguards the integrity and reliability of the storage and backup environment but also supports business continuity by enabling swift recovery from unexpected disruptions.

Ensuring that configuration backups are part of a broader data protection strategy, and provides an additional layer of security to help organizations maintain seamless operations, even in the face of unforeseen challenges.

Data classification at the storage volume, pool or backup policy level

Data classification at the NFS share, SMB share, storage volume, storage pool, or backup policy level is crucial for enhancing data security and compliance within an organization.

By categorizing data based on its sensitivity—such as personally identifiable information (PII), protected health information (PHI), or social security numbers—organizations can apply appropriate access controls, encryption, and monitoring measures tailored to the level of risk associated with each data type.

This granular approach to data classification ensures that sensitive information is protected from unauthorized access or exposure, reducing the risk of data breaches and ensuring compliance with regulatory requirements such as GDPR, HIPAA, and others.

Furthermore, by integrating data classification into backup policies, organizations can prioritize the protection of critical data, ensuring that it is securely backed up and easily recoverable in the event of data loss.

This comprehensive strategy not only safeguards sensitive data across various storage and backup environments but also optimizes resource allocation and strengthens the overall security posture of the organization.

Detect devices exposed to security advisories and alerts

In recent months, multiple vulnerabilities in storage and backup solutions have been discovered and actively exploited. These include:

Veeam Backup & Replication:

- CVE-2022-26500 and CVE-2022-26501: These vulnerabilities allow remote, unauthenticated attackers to execute arbitrary code.
- CVE-2023-27532: This high-severity vulnerability allows attackers to bypass authentication and access sensitive data.

MinIO:

- CVE-2023-28432: This vulnerability allows attackers to return all environment variables, including sensitive information like root passwords
- CVE-2023-28434: An attacker can use crafted requests to bypass metadata bucket name checking and put an object into any bucket while processing PostPolicyBucket.

Veritas Backup Exec:

- CVE-2021-27876: This vulnerability allows unauthorized file access through the Backup Exec Agent.
- CVE-2021-27877: This involves improper authentication, potentially allowing attackers to access sensitive information.
- CVE-2021-27878: This vulnerability permits command execution, allowing attackers to run arbitrary commands on affected systems.

Oracle ZFS Storage Appliance:

- CVE-2020-14871: Easy-to-use, actively exploited vulnerability that allows unauthenticated attacker to compromise the system, causing high impacts to confidentiality, integrity, and availability.

It's only a matter of time until even more vulnerabilities are actively exploited by bad actors, putting petabytes of production data at risk, as well as backup copies. Here are some recent news headlines:

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

[Acronis Warns Of Critical-Severity Vulnerability Being Exploited In Their Storage And Cyber Protection Platform]

The security defect allows threat actors to execute arbitrary code remotely due to the use of default passwords, which could have dire consequences for the victims.

CSO

[Lockbit Variant Targets Backup Software – Which Is Supposed To Help You Recover From Ransomware]

Yet another new ransomware gang, EstateRansomware, is exploiting a Veeam vulnerability that was patched more than a year ago to drop file-encrypting malware, a LockBit variant, and extort payments from victims.

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

[Vulnerabilities Expose Brocade SAN Appliances & Switches to Hacking]

18 vulnerabilities were identified in Brocade storage appliances, including unauthenticated flaws allowing remote attackers to log in to vulnerable devices as root

Some storage & backup CVEs will be detected by existing Vulnerability Detection tools, particularly for small portions of the NAS space – but the vast majority of them would not.

Existing Vulnerability Scanners (e.g., Tenable, Rapid7, Qualys, etc.)	StorageGuard
• Focus on endpoints and network • Poor-to-no support for storage & backup • Passive (network) scan for storage & backup • Often requires an agent (cannot be installed on storage/backup system)	• Focus on storage and backup • Full coverage for storage & backup technologies • Continuously updated repository of storage & backup security best practices and vulnerabilities • Authenticated scan • API/CLI-based, unique to each storage and backup operating system, software • Configuration compliance • Deep understanding of storage and backup concepts – from LUN to backup policy • Agentless

Detect immutability and isolation misconfigurations

Immutability is an important capability; however, it can lead to a false sense of security if not implemented properly. 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.

One of the best practices by the backup vendors is to ensure immutable backups are configured with **retention lock** – a parameter that prevents their deletion for a minimum period of time. If retention lock is not configured, cybercriminals can breach the backups by modifying large amounts of data, thereby quickly filling up the backup pools which results in deletion of all existing backups to free up space.

Even when retention lock is enabled, care must be taken to make sure cybercriminals can't fool the backup systems to believe time is passing more quickly than intended. This is referred to as "time spoofing" attacks – where the attacker manipulates insufficiently secure time sync configuration to trick the backup systems into thinking that "X" years have passed.

To give you a helping hand, here's a list of do's & don'ts for your immutable backups:

Do's	Don'ts
1. Configure the immutability retention period	**1.** Many vendor solutions offer multiple flavors of immutable backup – some are softer than others. Weaker immutability mode enable users to alter, disable or remove the immutability option altogether – that of course defeats the purpose of immutability – you want to avoid these modes.
2. Use secure time synchronization	**2.** Don't use the same credentials to manage both primary storage and backup systems
3. Enable two-person rule on immutability related settings	**3.** Don't enable unrestricted remote access
4. Consider enabling anomaly detection	**4.** Don't enable unsecure protocols such as FTP, Telnet or plaintext HTTP
5. Secure underlying hardware components such as iDRAC, IPMI, BMC, iLO, etc.	**5.** Don't use unrestricted or vulnerable file shares
6. Enable local user MFA	**6.** Do not allow untrusted hosts to join the Backup domain
7. Limit number of sessions	**7.** Don't use default passwords
8. Account Login Threshold	
9. Restrict administrative access	
10. Create Security Officer	
11. Disable inactive users	
12. Harden your backup catalog / repository	

Industry & Security Standards

At the beginning of 2024, ISO released **ISO/IEC 27040:2024,** which provides recommendations for the security of storage & backup systems.

27040 provides detailed guidance for improving storage & backup security in three main areas: organizational, people, and technology controls. There are 220 discrete storage security recommendations, of which 70% are classified as “Guidance”, and 30% as “Requirements”.

NIST SP 800-209 – Security Guidelines for Storage Infrastructure is one of the most authoritative guidelines in the industry.

Co-authored by Continuity’s CTO, Doron Pinhas, the guide provides an overview of the evolution of storage technology, recent security threats, and the risks they pose.

It includes a comprehensive set of recommendations for the secure deployment, configuration, and operation of storage resources. These include data and confidentiality protection using encryption, isolation and restoration assurance.

The latest regulation to enter the scene in Europe is the **Digital Operational Resilience Act** (Regulation (EU) 2022/2554) – also known as **DORA.**

DORA

DORA is having a significant impact on the way financial institutions secure data storage and backup systems. The framework requires financial institutions to have a robust and resilient storage and backup system in place to protect their data from unauthorized access, loss, or corruption.

Without their data, preserved and secure, regulators know that businesses cannot be resilient faced with the current threat environment.

DORA requires financial institutions to:

- Have a documented data retention policy that specifies how long data should be stored and how it should be disposed of
- Implement appropriate technical and organizational measures to protect data storage and backup systems from unauthorized access, loss, or corruption of data
- Test and monitor their data storage and backup systems on a regular basis to ensure that they are working properly
- Ensure that data is protected from risks arising during its processing,, including poor administration, processing related risks and human error
- Ensure backup systems don’t jeopardize the security of the network and information systems

The Payment Card Industry Data Security Standard (PCI DSS) provides comprehensive requirements for protecting cardholder data, which includes guidelines related to storage and backup systems. Here are the key points PCI DSS makes regarding storage and backup systems:

Regular Testing and Monitoring (Requirement 11):	Access Control (Requirement 7 & 8):	Backup Security:
• **Vulnerability Scanning and Penetration Testing:** Regularly scan and test storage systems for vulnerabilities, and address any identified issues promptly.	• **Use Strong Authentication:** Implement multi-factor authentication for access to storage systems containing cardholder data, especially for remote access.	• **Secure Backup Data:** PCI DSS requires that backup data containing cardholder information be protected with the same level of security as the original data. This includes encryption, access control, and physical security measures.

By following these guidelines, organizations can ensure that their storage and backup systems are compliant with PCI DSS, thereby protecting cardholder data from unauthorized access and breaches.

CIS Controls

The CIS (Center for Internet Security) Controls emphasizes several key aspects in securing storage and backup systems

Data Protection (Control 13)

- **Ensure the Protection of Backups:** Backups should be encrypted and stored securely, with controls to prevent unauthorized access. Also, maintain an offline backup to protect against ransomware and other cyber threats that could compromise both primary and online backup systems.

Continuous Vulnerability Management (Control 7):

- **Conduct Regular Vulnerability Scans:** Regularly scan storage and backup systems for vulnerabilities and apply necessary patches or configurations to mitigate identified risks.

Account Monitoring and Control (Control 5)

- **Limit and Control the Use of Administrative Privileges:** Administrative access to storage and backup systems should be tightly controlled and monitored. This reduces the risk of unauthorized changes or access to critical systems and data.

Boundary Defense (Control 12):

- **Protect Backup Data from Unauthorized External Connections:** Ensure that backup systems are not directly accessible from the internet and are isolated from less secure parts of the network.

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers (Control 4)

- **Establish and Implement Secure Configurations for Backup Systems:** Ensure storage and backup systems are configured according to security best practices, including disabling unnecessary services and enforcing strong authentication mechanisms.

These guidelines are designed to protect critical data and ensure the resilience of storage and backup systems against cyber threats. By following these controls, organizations can minimize the risk of data loss and ensure that they can recover from incidents effectively.