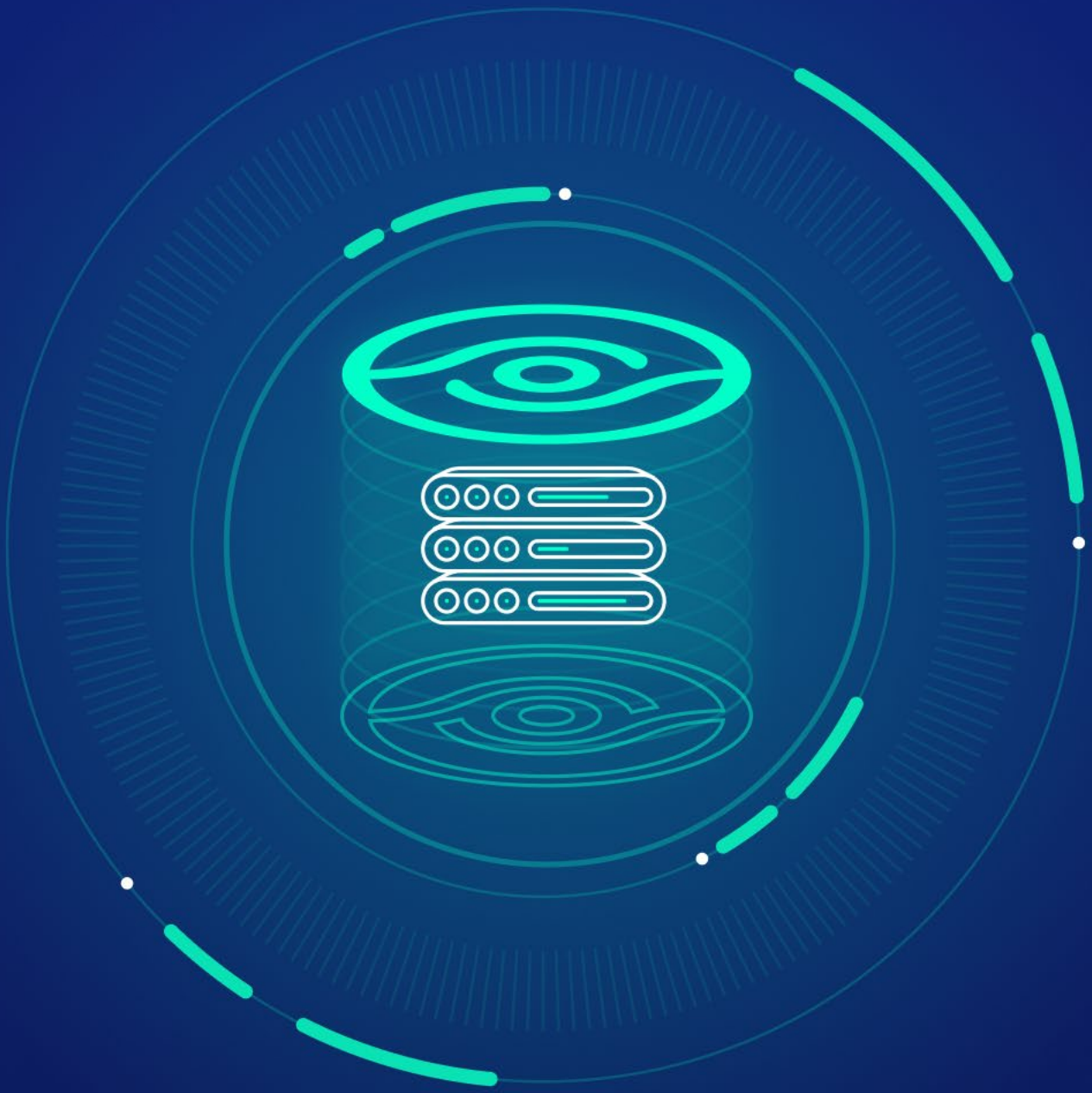


CONTINUITY

Storage and Backup Security

Risk Summary Report

Prepared for: XYZ Bank

Issued by: Continuity - StorageGuard™

February 2022

CONTINUITY

Table of Contents

Introduction

StorageGuard is an enterprise-grade solution, securing data storage and backup systems in any type of IT environment. The solution proactively checks for vulnerabilities, security misconfigurations and ransomware preparedness issues based on a vast and continuously updated knowledge base of security best practices from enterprise storage vendors, leading information security standards and the community. StorageGuard identifies violation of industry best practices, organizational security baseline requirements, ransomware guidelines and non-compliance with regulations that could impact the security posture of core storage and backup systems. It informs the relevant IT teams of violations and how to repair them in order to close the security gaps that put critical data systems at risk.

StorageGuard collects and analyzes configuration data from all enterprise storage and backup systems. A built-in security risk detection engine checks for thousands of possible misconfigurations and vulnerabilities at the storage system level that pose a security threat to your critical business data. This includes analyzing 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. StorageGuard identifies violations of vendor security configuration guidelines, organizational security baseline requirements (built-in and custom), community-driven best practices, compliance requirements (CIS, NIST, PCI DSS and more) and vulnerabilities. The StorageGuard Risk Signature Knowledgebase includes built-in automatic checks for authentication configuration, administrative access, storage access control, insecure protocols and services, ransomware protection guidelines, file shares security recommendations, NIST requirements, storage CVEs and many more.

Remediation of such risks will harden the data storage environment and protect critical business data from attacks. When a risk is discovered by StorageGuard, a detailed description and the suggested resolution are forwarded to the right IT teams for timely action. StorageGuard operation is agent-less, secure and non-intrusive. Such risks are the natural result of a large volume of ongoing changes within a highly complex technology environment. Given the nature of such environments, it is practically impossible to manually identify such issues. Automated, proactive discovery of these irregularities is critical to preventing data security risks and successfully completing Information Security audits.

Key Benefits of StorageGuard

- StorageGuard ensures core data storage infrastructure systems are hardened and can withstand ransomware and other attacks.
- StorageGuard detects security misconfigurations, vulnerabilities, security baseline violations and compliance issues.
- StorageGuard eliminates manual security validation efforts and provide continuous configuration validation at scale.
- StorageGuard provides valuable remediation guidance.
- StorageGuard assists with preparation for audit and with achieving and sustaining and providing evidence for compliance.
- StorageGuard tracks security configuration changes.
- StorageGuard is based on our mature enterprise-ready scan and analysis platform.
- StorageGuard is easy to deploy and operationalize as it uses an agent-less scan and has integration plugins for ITSM.
- StorageGuard can be easily customized to address additional baseline requirements.

Supported Storage and Backup Systems

StorageGuard supports a wide range of Storage and Backup systems from vendors such as Dell EMC, IBM, Hitachi, HPE, NetApp, Cohesity, Pure, Infinidat, Brocade, Cisco and more. Please visit https://www.continuitysoftware.com/storage-backup-vendor-list for the complete and up to date list of supported Storage and Backup Systems.

Executive Summary

Overview

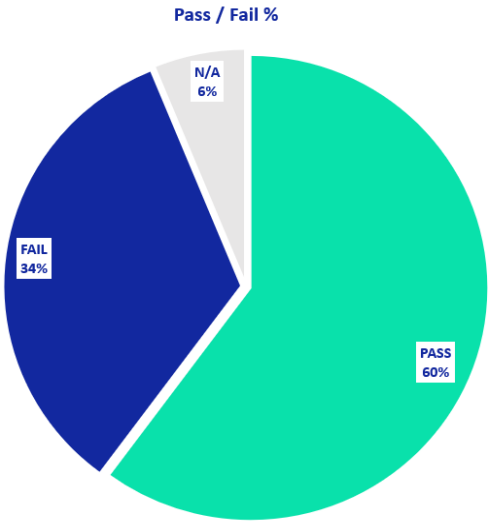
- A small subset of the environment was scanned and analyzed by StorageGuard.
- The one-time collection of configuration data was performed using the StorageGuard agentless scan technology, with no impact on scanned systems and without installing any software on the target systems.
- The scan scope included multiple vendors and models.

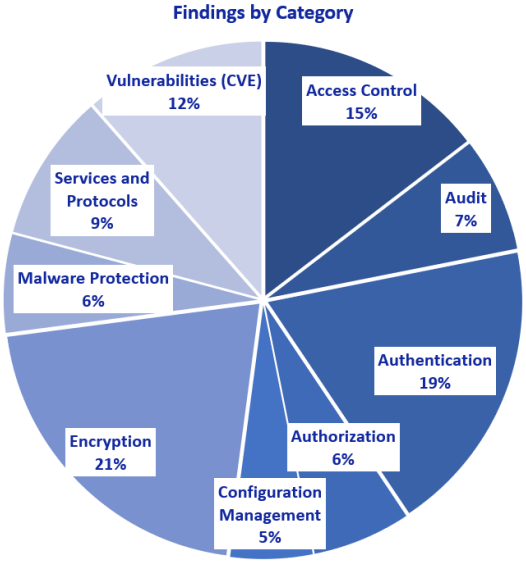
Findings

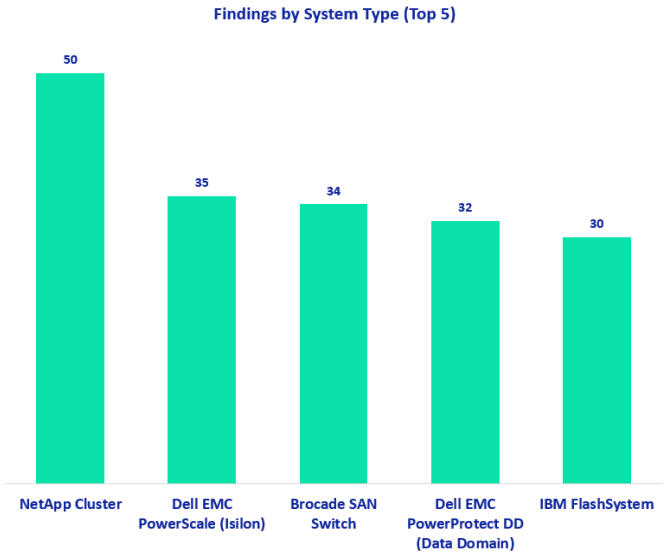
- A total of 416 risk types were detected.
- The data security configuration issues and vulnerabilities identified span all layers of the storage infrastructure, including file, block and object storage, storage network, backup and storage management systems.
- A detailed listing of 10 sample risks is included in this report.
- To run recurring scans and to view all risks, upgrade from the Trial version to a standard license.

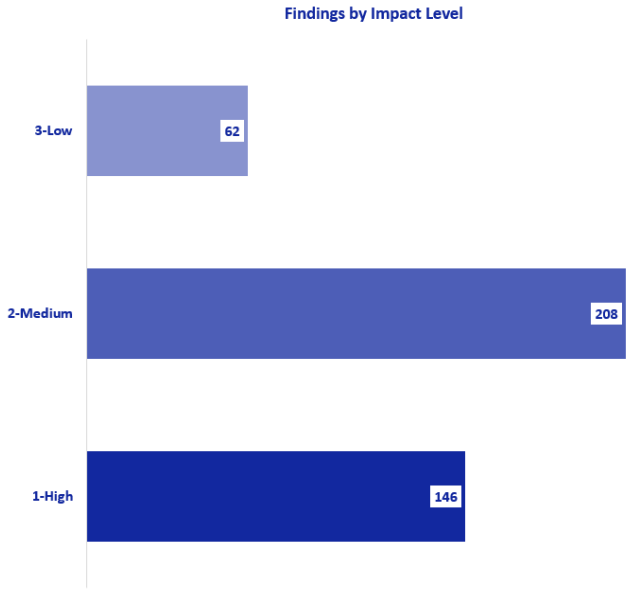
Conclusions

- Significant data security risks identified for the storage systems scanned.
- It is practically impossible to manually identify such risks manually and at scale - though simple to repair once found.
- Similar and other issues may be present in the un-scanned portion of the production environment.
- Running a recurring scan on all critical systems is highly recommended.









Key Takeaways

- Your organization is taking particular care to maintain the security posture of storage and backup systems; nevertheless, numerous significant issues were identified on the scanned systems that may be maliciously exploited by attackers, and mitigation of these issues is highly recommended.
- Consider enabling 2-factor authentication for sensitive systems such file storage and backup systems.
- Consider enabling ransomware prevention features on file and object storage systems such as ransomware file filtration policies and on-box anti-ransomware.
- As guided by CISA, disable unsecure file SMB protocol versions that have been exploited to launch ransomware and other attacks.
- Consider increasing cyber-recoverability assurance by setting up retention-locked non-erasable snapshots and backup copies.
- Multiple critical vulnerabilities found, including high CVSS score vulnerabilities that allow users to run commands as the root user; Update Storage OS and firmware to recommended and secure releases.
- Configure all systems to use TLSv1.2 (and above) as recommended by NIST, the NSA and other leading organizations, and avoid the vulnerable earlier (deprecated) versions.
- Remove or disable weak encryption and hash algorithms from all systems (MD5, SHA1, SSLv3, CBC, DES, etc.) that have been deprecated by NIST and other leading organizations.
- Restrict access to file shares to designated IP ranges and avoid granting access to all IP addresses.
- Consider implementing access lists for all storage systems / services to minimize the storage and backup management attack surface.
- Disable all cleartext protocols still in use in the network (HTTP, LDAP, SNMP, etc.).
- To protect against eavesdropping and data leakage, consider encrypting data in transit through various connections and protocols (CIFS, NFS, replication, remote support, etc.).
- Configure strict local user password policies on all storage and backup systems
- Enable and configure account lockout capabilities to prevent successful brute-force attacks on storage systems.
- Consider enabling storage area network authentication features for improved storage security.
- Apply a stronger cryptographic template on SAN switches.
- Consider whether to keep remote connection / access to vendor and/or cloud enabled.
- Consider enabling the hardened FIPS mode.
- Consider expanding the StorageGuard scan to all the storage and backup systems to identify other hidden risks that jeopardize critical and/or sensitive data systems.
- Consider running recurring scans to identify security configuration drifts and to automatically check your storage and backup systems against new security best practices and vulnerabilities, as these are published.

Pass/Fail by System Type

The following table lists the scanned system types, and the number of checks that have passed or failed:

System Type	Number of Scanned Systems	Pass	Fail	Not Applicable
Brocade SAN Switch	2	92	34	11
Cohesity DataPlatform	1	58	29	1
Dell EMC ECS	1	25	19	0
Dell EMC PowerMAX	2	23	18	0
Dell EMC PowerProtect DD (Data Domain)	2	34	32	0
Dell EMC PowerScale (Isilon)	2	72	35	4
Dell EMC Unity	2	21	18	0
Hitachi VSP	2	90	27	11
IBM FlashSystem	2	91	30	13
IBM Storwize V7000/SVC	2	40	22	1
Infinidat Infinibox	1	28	24	0
NetApp Cluster	3	96	50	15
Pure FlashArray	1	68	26	8
Veritas NetBackup	1	35	27	0
Hitachi Content Platform (HCP)	1	55	25	0
Total	25	828	416	64

Impact / Ease Matrix

The following matrix provides a quantitative summary of findings divided by impact and ease of implementation.

Guidelines for using this matrix:

- Table cells have unique identifiers: C1 to C9.
- In addition, each table cell contains a hyperlink with the following characteristics:
  - The hyperlink specifies the number of findings that meet the impact and ease of implementation criterions.
  - For instance, C6 indicates there are 36 findings with medium impact and high ease of implementation.
  - The hyperlink leads to the appropriate section within the "Risk in Detail" section.
- High ease of implementation indicates relatively low mitigation effort whereas low ease of implementation indicates high mitigation effort.
- Findings with high impact and high ease of implementation should be considered as "quick wins".
- Findings with low impact and low ease of implementation should be considered as "fill Ins".
- The matrix can be used to prioritize the process of review and mitigation of the findings.
  - For instance: C9 → C8 → C6 → C5 → C7 → C3 → C4 → C2 → C1

Impact \ Ease of Implementation	Low (Difficult)	Medium	High (Easy)
Low	C1 19	C2 19	C3 24
Medium	C4 25	C5 79	C6 104
High	C7 32	C8 48	C9 66