CONTINUITY

StorageGuard

ABOUT US

Founded in 2005,
helping enterprises with:

- Proactively preventing outages and data loss incidents on critical IT
- Ensuring the security of data storage systems

SELECTED CUSTOMERS

JPMorganChase	ups	Bank of America	MetLife
swisscom	Liberty Mutual.	BNP PARIBAS	citi
MINISTRY OF SECURITY AND PUBLIC ADMINISTRATION	verizonwireless	ferrovial	El Corte Inglés
STAPLES	BANK OF OKLAHOMA	MassMutual	BBVA

SUCCESS STORY - LEADING BANK

THE CUSTOMER

- An American multinational bank and financial services company*

CHALLENGE (CONTINUED)

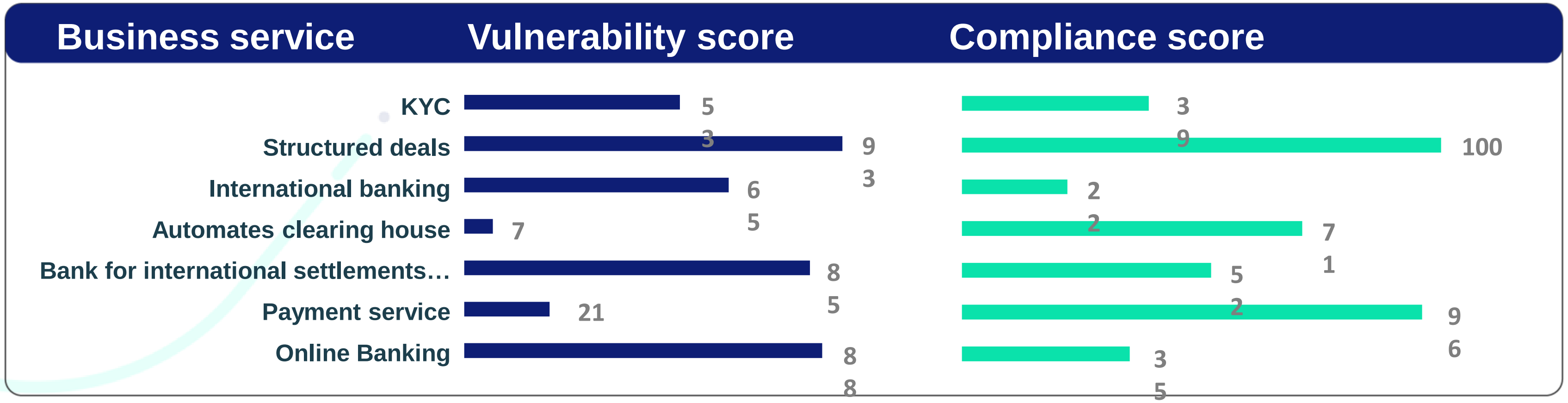
- Manual analysis is not feasible
- Failure to meet auditor deadlines for remediating the gap

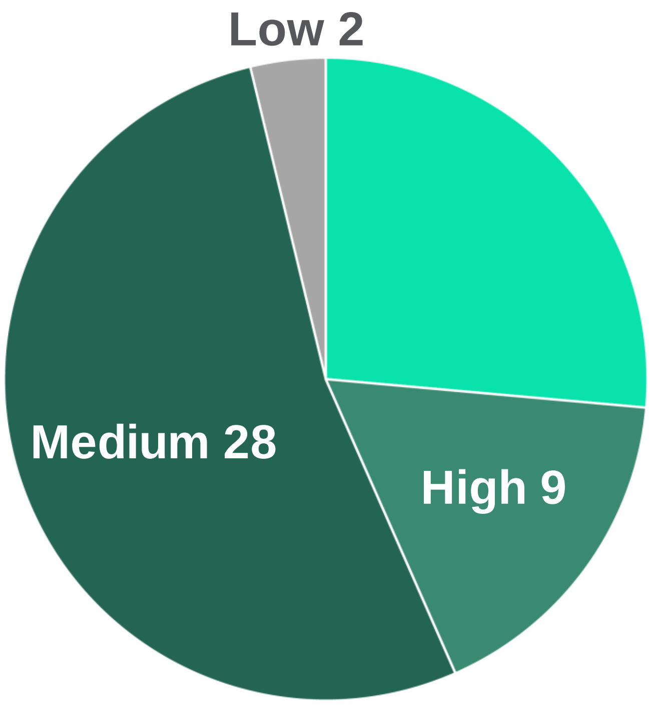
CHALLENGE

- No repeatable and trackable method to assess the security of business-critical data enterprise storage systems
- Ransomware concern

SOLUTION BY CONTINUITY SOFTWARE

- Continuous scanning and analysis of the bank IT systems worldwide
- Overall health and compliance reports



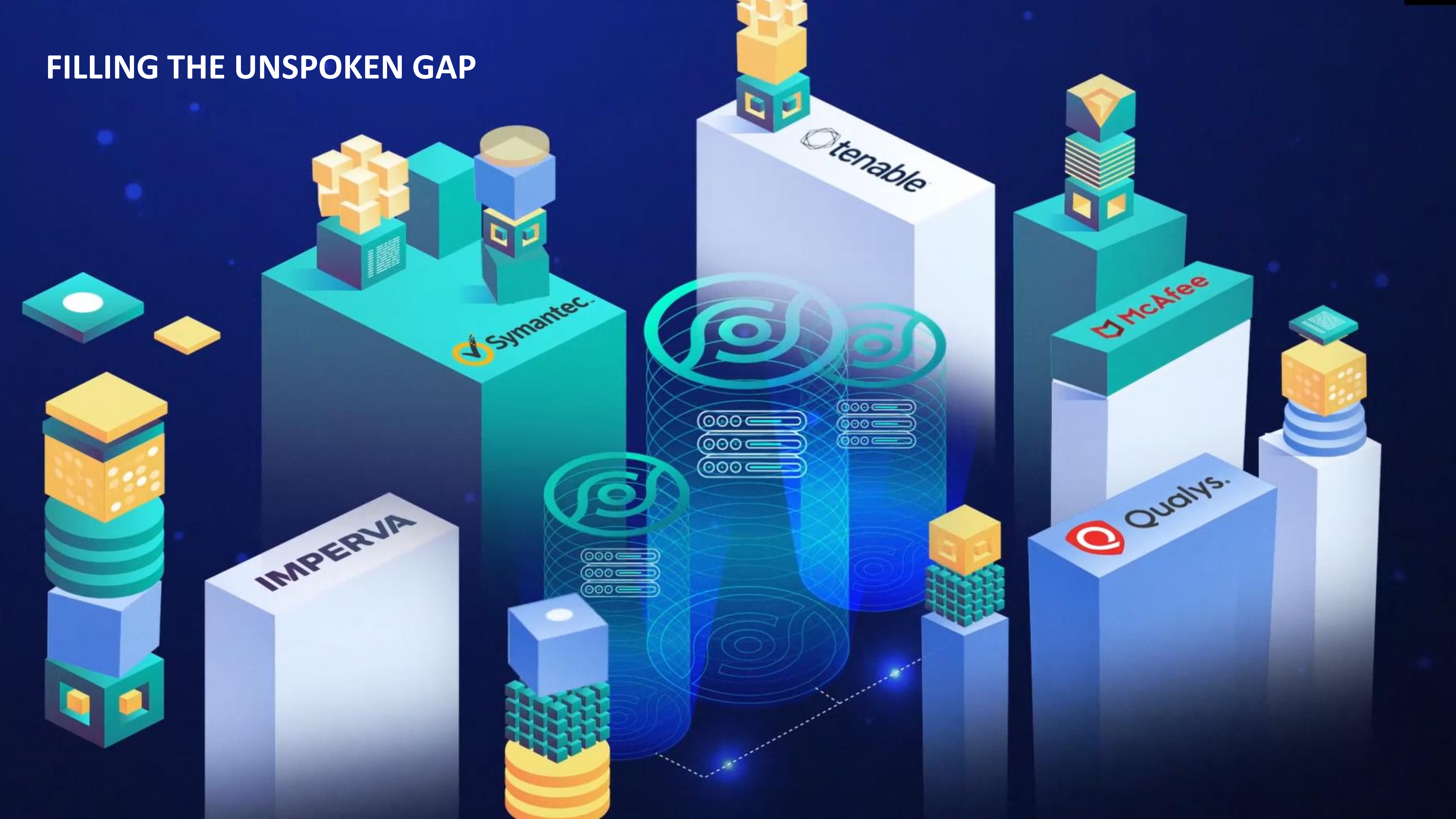


CONTINUITY

THE UNSPOKEN GAP

A compromised storage system will lead to multi-system failure

FILLING THE UNSPOKEN GAP

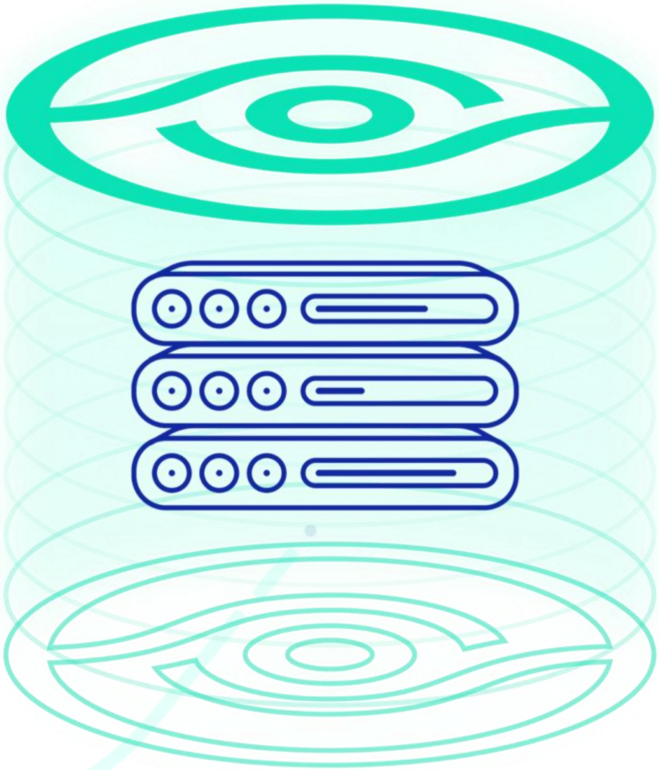


IS IT TIME FOR STORAGE SECURITY

	Commonly-held Assumption	Reality
Data	Data is already secured at multiple layers (OS, Database, Network…)	Storage & Backup is where 100% of your data lives!
Attack Surface	Small and deep inside the perimeter/datacenter	Large, vulnerable, and reachable
Threat Level	Most attacks target users, end-points, servers	Number of attacks on storage is small but growing; however, impact can be devastating
Ransomware	Most ransomware encrypts data on end-points/servers; securing storage can't stop that	Storage & Backup is the last line of defense against any ransomware attack -- secure data copies & backups essential for recovery!
Existing Tools	Lots of tools already in place for vulnerability scanning (eg, Rapid7, Nessus, Qualys)	Existing tools offer almost zero coverage for storage, storage management, and backup

THE SOLUTION - STORAGEGUARD

Validation of security configurations and vulnerability management for storage & backup systems



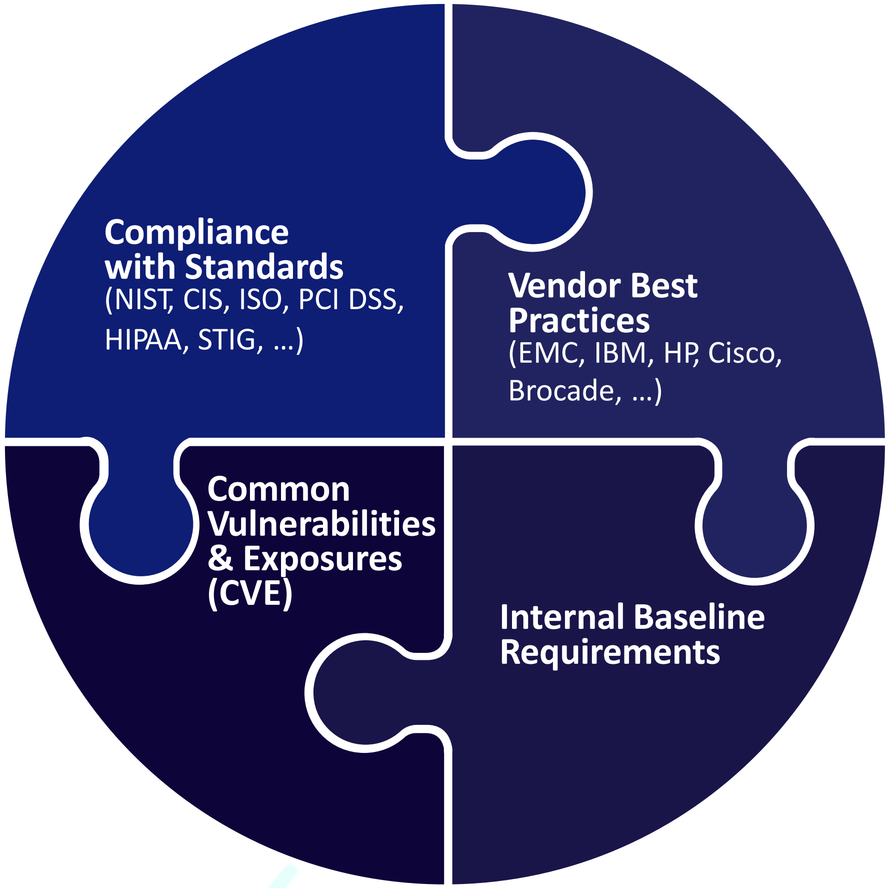
Built-in risk knowledgebase of security configuration best practices

- Vendor best practices, community-driven baseline requirements
- Ransomware protection, vulnerabilities and compliance checks
- Configuration checks for Administrative Access, Authentication, Authorization, Audit Log, Data access, Services and Protocols, Isolation, ISO27001, CIS, NIST and more.

Focus on converged and storage systems

- Block, object, Cloud, IP storage, storage network, data protection systems,
- Storage management systems, Virtual SAN, NAS/SAN, File System and more

THE RISK KNOWLEDGEBASE SOURCES


Compliance with Standards
(NIST, CIS, ISO, PCI DSS, HIPAA, STIG, …)
Vendor Best Practices
(EMC, IBM, HP, Cisco, Brocade, …)
Common Vulnerabilities & Exposures (CVE)
Internal Baseline Requirements

Four main sources, including:

- Automatic checks based on standard, interpreted for each device type
- Automatic checks for comprehensive and ongoingly updated vendor best practices
- Automatic checks for storage system vulnerabilities
- Automatic checks for community-driven security baseline configurations

THE RISK KNOWLEDGEBASE CATEGORIES

Authentication

- AD / LDAP, Vaulting, Radius
- Kerberos, MFA
- Login & passwd requirements

Authorization

- Role configuration
- Restricted Admin access
- Default accounts / passwords

SAN / NAS

- Zoning and masking
- CIFS and NFS access
- Port config

Vendor best practices

- Dell EMC, IBM, HP,
- Hitachi
- Cisco, Brocade, NetApp

Infinidat, Amazon, more.

Administrative access

- Management systems / Apps
- CLI /API/SMI-S servers
- Automatic logoff, sessions

Encryption

- At rest / In transit
- Encryption level, FIPS, Hashes
- Admin / User access, SSL/TLS

Vulnerabilities

- Storage CVE detection
- Approved versions

Leading standards

- ISO 27001, NIST, CIS SANS
- NYDFS, SEC, FFIEC, HIPAA
- FIPS, PCI DSS and more.

Audit log

- Central Logging
- Log Retention
- Log Config and Immutability

Services / Protocols

- Telnet, FTP, RSH, SSH, Rlogin
- NFS, CIFS (SMB)
- SNMP, NDMP, SMTP

Ransomware protection

- Vendor / industry best practices
- Protection policies

And more…

- Antivirus settings
- Time synchronization
- And more…

COVERAGE

- Block Storage Arrays
- Storage Network Switches
- Storage Management Applications / Servers
- Storage Virtualization Systems
- Data Protection Appliances
- Object Storage
- Storage Area Network (SAN)
- Server-based SAN (Virtual SAN)
- Network Attached Storage (NAS)
- Backup Systems
- Cloud storage*
- Converged / Blade / Hypervisor*

STORAGEGUARD SUPPORT MATRIX

SAN Arrays

- Dell EMC Symmetrix • VMAX • PowerMAX
- Dell EMC XtremIO • PowerStore* • IDPA
- Dell EMC VNX • VNX2 • Unity
- NetApp FAS/AFF • cDOT • 7-mode • filer
- Hitachi VSP/USP • AMS • HUS • G-Series
- IBM DS • XIV • IBM SVC • V7000/5000 • Storwize • A9000/R • V9000 • FlashSystem • Spectrum Virtualize • Spectrum Accelerate • N-Series
- HPE XP • 3PAR • Nimble*
- Infinidat InfiniBox
- Pure*

Server-based SAN & HCI

- Dell EMC PowerFlex (ScaleIO / vxflex OS)
- VMware VSAN*
- Nutanix*

File Storage & NAS

- NetApp FAS/AFF • cDOT • 7-mode
- Dell EMC Isilon • PowerScale • VNX/2 • Unity
- IBM N-Series • Hitachi NAS* • HPE StoreEasy* • Infinibox

Object Storage

- Hitachi Content Platform (HCP)
- Dell EMC Elastic Cloud Storage (ECS)
- IBM Object Storage* • NetApp StorageGRID*

Storage Network

- Brocade directors / switches • OEM versions
- Cisco MDS • Nexus • OEM versions
- HP VirtualConnect / FlexFabric

Storage Appliance

- IBM Spectrum Scale* • Hadoop Appliance*
- Oracle ZFS* • Oracle Exadata storage*

Storage Virtualization

- Dell EMC VPLEX
- IBM SAN Volume Controller • Spectrum Virtualize
- NetApp FlexArray*

Data Protection

- Dell EMC RecoverPoint • Dell EMC Data Domain • Dell EMC PowerProtect DD • Dell EMC Avamar
- NetBackup • Commvault* • HP StoreOnce • Veeam* • Cohesity* • Rubrik*
- IBM Spectrum Protect (Tivoli Storage Manager)*

Cloud Storage*

- Amazon Elastic Block Storage • S3 • Glacier
- Azure Blob / Disk Storage
- Nasuni • Zadara
- NetApp Cloud Volumes ONTAP

Storage Management

Dell EMC • IBM • HPE • Hitachi Vantara • NetApp • Infinidat • More.

(*) roadmap items

NIST Special Publication 800-209

Security Guidelines for Storage Infrastructure

Ramaswamy Chandramouli
Doron Pinhas

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-209

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

BENEFITS OF USING STORAGEGUARD

Ensure storage systems are hardened and can withstand ransomware and other cyber-attacks

Protection & Compliance

- Eliminate manual security validation efforts
- Obtain valuable remediation guidance
- Meet IT Audit requirements: providing evidence for compliance
- Eliminate configuration drift: tracking security configuration changes

Visibility & Prioritization

- Reporting and dashboarding of remediation status and risk reduction trends
- Routinely updated risk knowledgebase
- Easily customizable with required additional security checks

STORAGEGUARD RISK ASSESSMENT

A one-time scan of up to 25 storage systems

- Complete and actionable findings report
- Performed by Continuity’s Professional Services team
- Requires minimal customer effort
- Full risk report completed within 1 week

CONTINUITY

CONTINUITY