NOVASYSTEM

CONTINUITY

StorageGuard

CONTINUITY

Founded in 2005, serving leading enterprises worldwide

How we help our customers:

- Securing Storage & Backup [StorageGuard]
- Govern and Manage IT Recoverability [RecoveryGuard]

SELECTED CUSTOMERS

UPS · State Street · citi · BPER: Banca · Liberty Mutual. · BNP PARIBAS · El Corte Inglés · verizon wireless · BANK OF OKLAHOMA · DHL · swisscom · USAA · Prudential

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

Il NIST (National Institute of Standards and Technology) che fissa gli standard di sicurezza per il Dipartimento di Stato USA ha incaricato il CTO di Continuity, Doron Pinhas, per redarre la guida di sicurezza delle infrastrutture di storage come co-autore.
Disponibile a questo link: https://csrc.nist.gov/publications/detail/sp/800-209/final

Topmost Critical ICT Assets

Storage systems

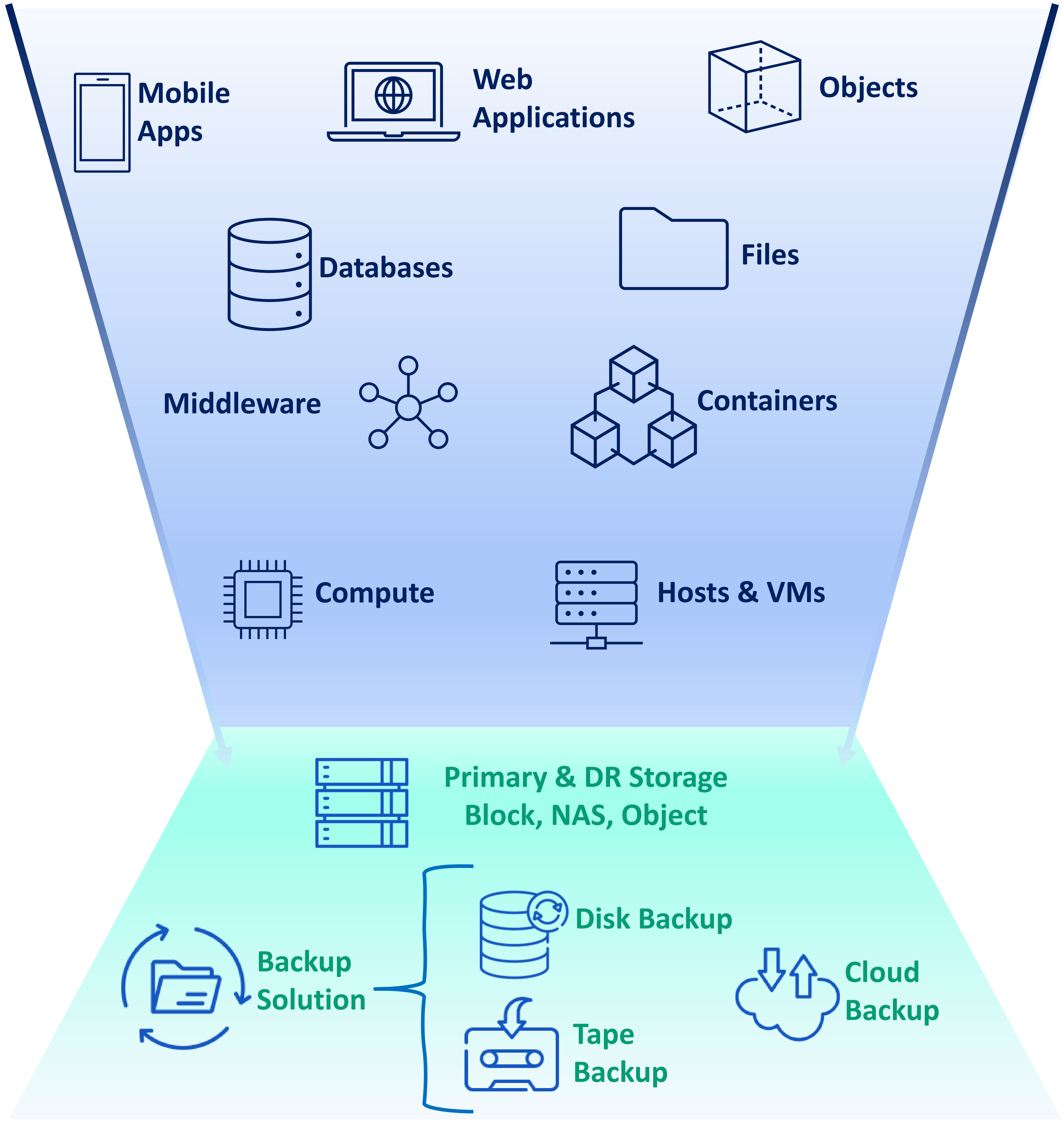
- Store nearly all **information assets**
- Store **data copies** for rapid recovery

Backup systems

- Create & store **data copies** for Cyber-Recovery and DR

Supporting **critical or important functions**

At the Heart of **Operational Resilience**



The State of Storage Security Report by Continuity

Over 6,300 security issues detected across hundreds of storage devices

On average, an enterprise storage device has 15 vulnerabilities or security misconfigurations

Out of these 15 vulnerabilities and misconfigurations, 3 are high or critical risks

THE GAP

Symantec
End-user devices
Mobile OS
tenable
End-user devices
Host OS
McAfee
Web Servers
Qualys.
Host OS
Web Servers
End-user devices
IMPERVA
DBMS

Storage & Backup

The Ultimate Line of Defense Against Cyberattacks

Why StorageGuard

"Perimeter defenses can no longer protect organizations' assets & data"

- NIST & MITRE, 2021 Cyber Resiliency Guide

Security Tool for Storage & Backup ICT Risk Management

"minimize the impact of ICT risk by deploying tools", DORA 2022/2554

How to meet Risk Management requirements for Storage & Backup ICT Assets?

How do you automate, validate, and enforce the Secure Configuration of your storage and backups?

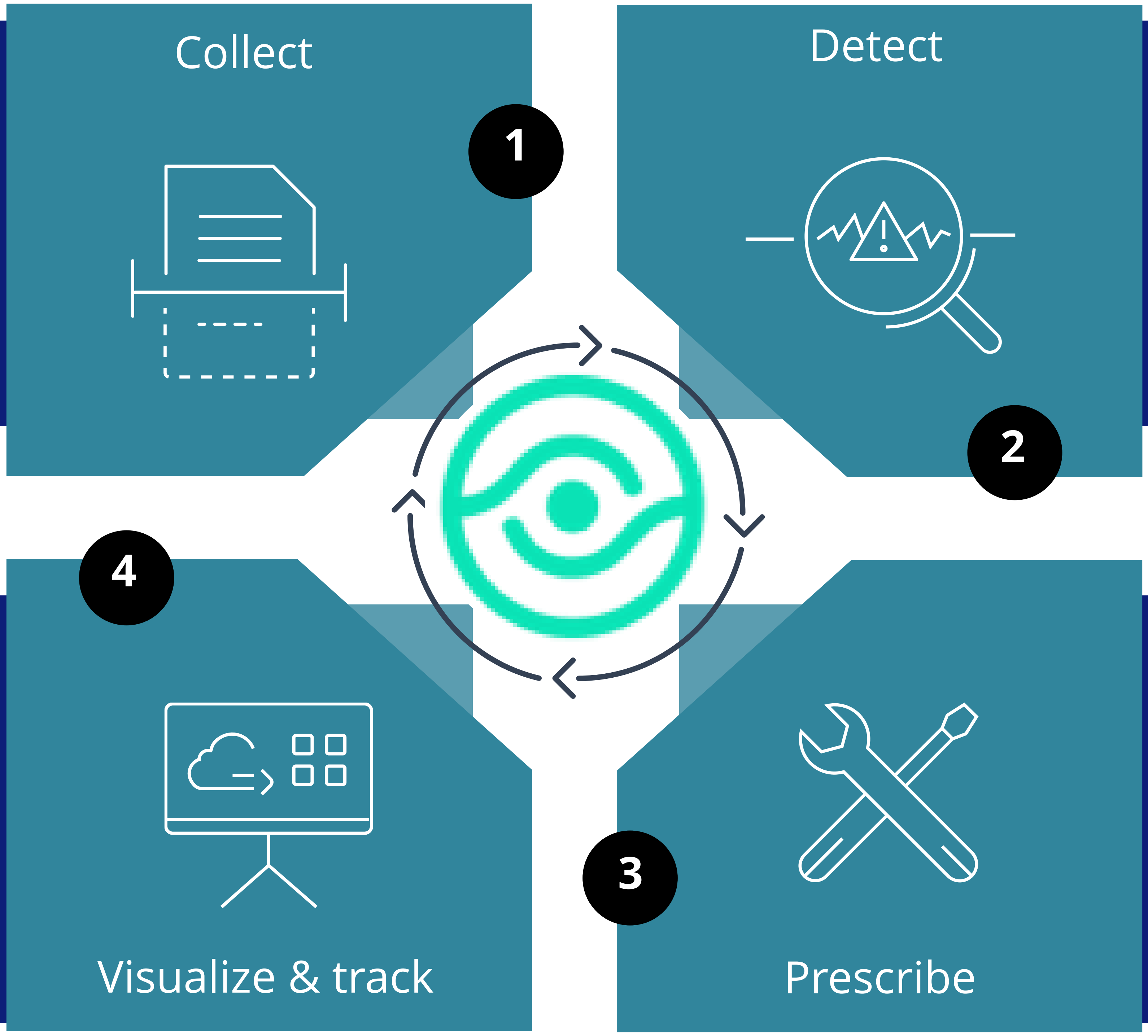
StorageGuard

Vulnerability Management and Secure Configuration 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, DORA and more.
- **Focus on storage and backup systems**
  - Block, object, IP storage, storage network, data protection systems
  - Storage & backup management, VSAN, NAS, SAN, File Shares and more
- **Custom checks**
  - Implement your own baseline checks

How It Works

- » Daily collection of configuration from all converged / storage / backup layers
- » Non-intrusive Read Only Credentials
- » Agentless
- » On-Prem



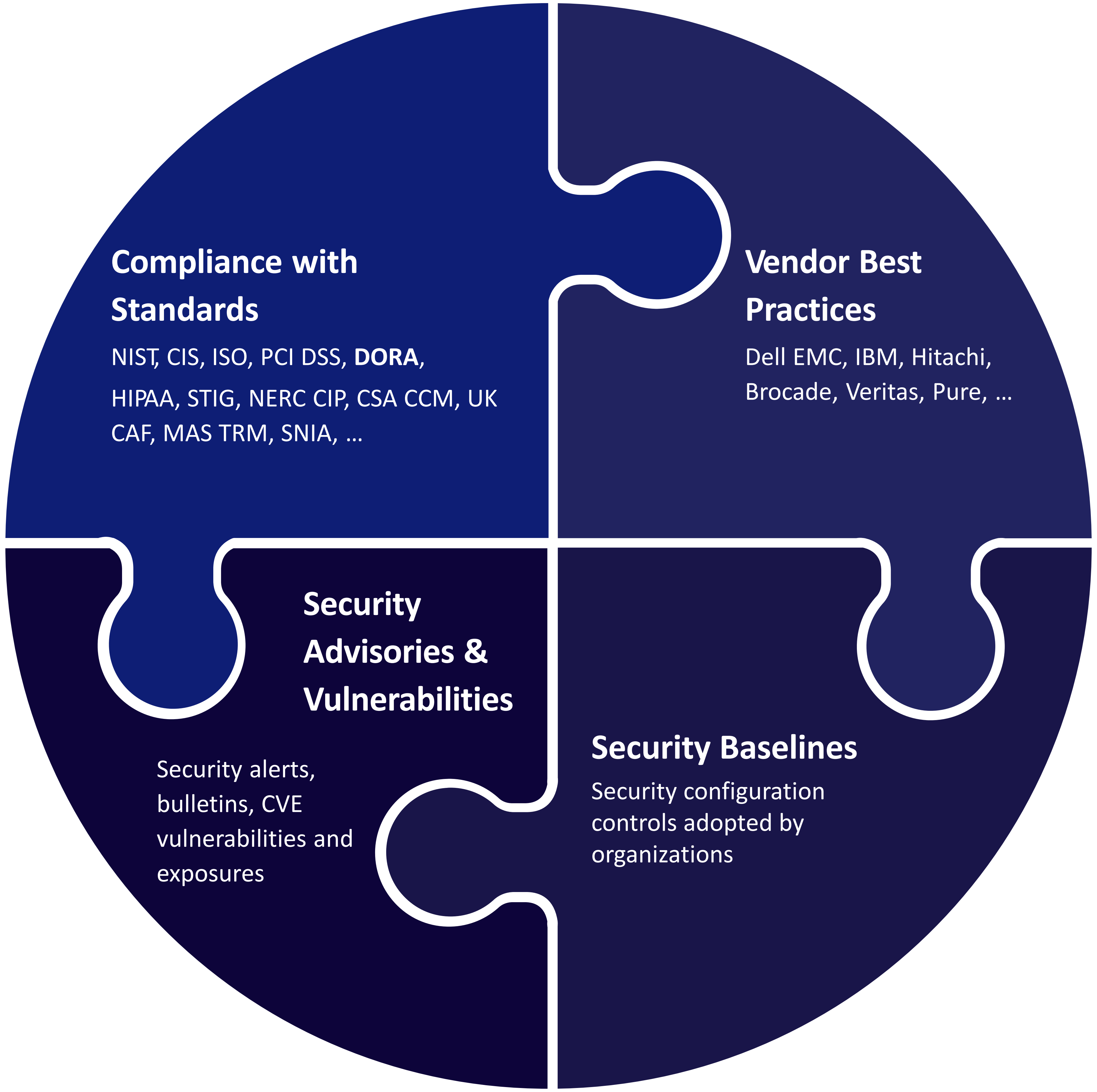
- » Analyzes configurations using a built-in risk detection engine
- » Detects security misconfigurations and vulnerabilities

- » Sends actionable alerts to appropriate teams
- » Suggests remedial steps
- » Integrates with existing management systems

- » Single-pane-of-glass for ensuring security of storage environment
- » Automatically reports on successful resolution of issues

StorageGuard Risk Knowledgebase

- Library of automated configuration checks
- Over 2500 built-in checks
- Regularly updated
- Based on four (4) primary categories



Compliance with Standards

NIST, CIS, ISO, PCI DSS, **DORA**, HIPAA, STIG, NERC CIP, CSA CCM, UK CAF, MAS TRM, SNIA, …

Vendor Best Practices

Dell EMC, IBM, Hitachi, Brocade, Veritas, Pure, …

Security Advisories & Vulnerabilities

Security alerts, bulletins, CVE vulnerabilities and exposures

Security Baselines

Security configuration controls adopted by organizations

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 Switches
- ○ Storage Management
- ○ Storage Virtualization
- ○ Data Protection Appliances
- ○ Object Storage
- ○ Storage Area Network (SAN)
- ○ Server-based Storage (VSAN)
- ○ Network Attached Systems (NAS)
- ○ Backup Systems
- ○ Software-Defined Storage
- ○ HCI
- ○ Cloud Storage

StorageGuard Support Matrix

SAN Arrays

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

Server-based SAN & HCI

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

File Storage & NAS

- NetApp FAS/AFF • cDOT • 7-mode • IBM N-Series
- Dell EMC Isilon • PowerScale • VNX/2 • Unity
- Cohesity SmartFiles • HNAS* • HPE StoreEasy* • Infinibox • Pure • Huawei* • Nasuni*

Object Storage

- Hitachi Content Platform (HCP) • Scality*
- Dell EMC ECS • Cloudian HyperStore*
- 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 • IDPA
- NetBackup • Commvault • HPE StoreOnce • Veeam • Cohesity • Rubrik • Networker*
- IBM Spectrum Protect (TSM)

Cloud Storage

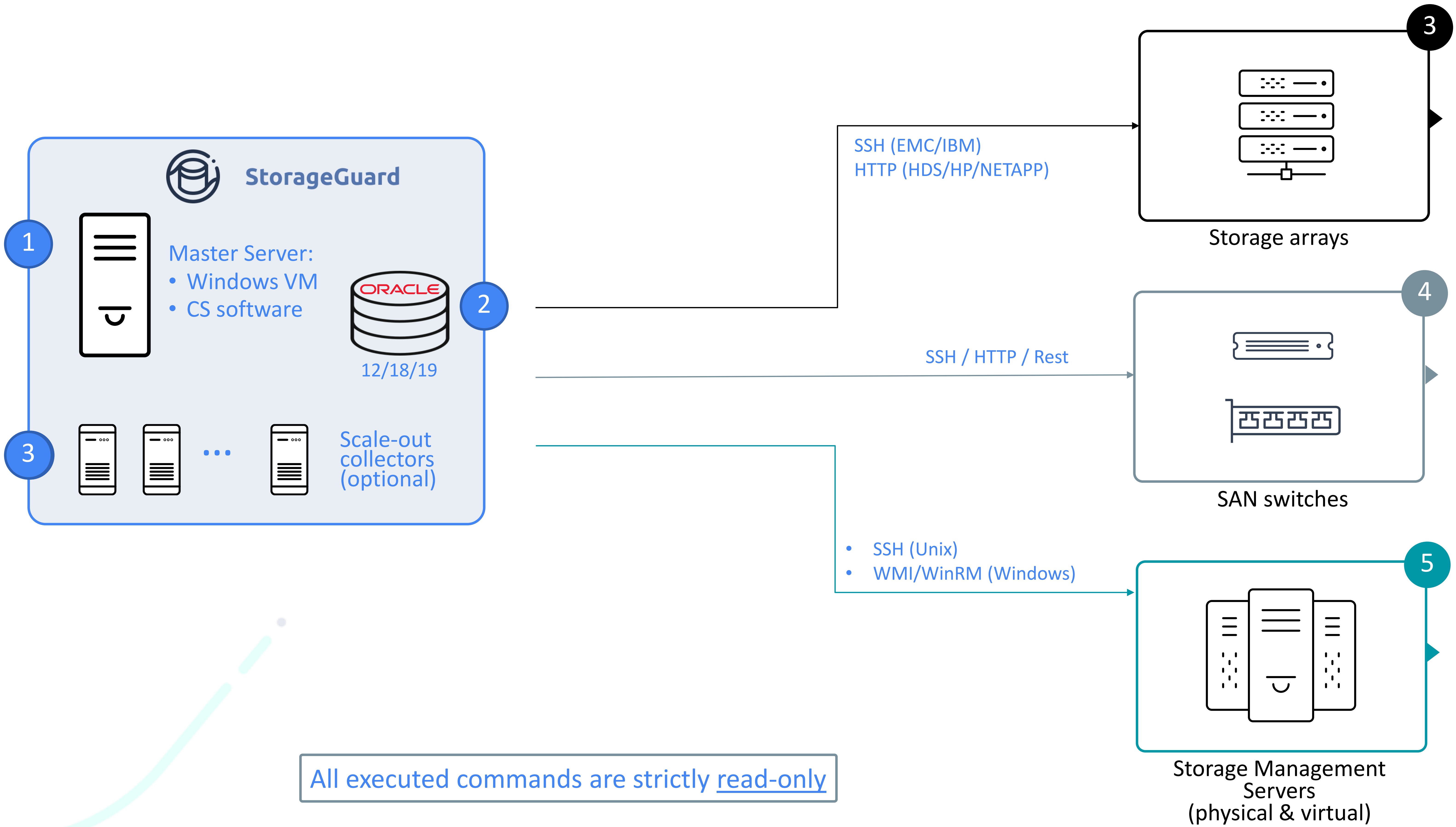
- Amazon Elastic Block Storage • S3 • Glacier
- Azure Blob / Disk Storage*
- Nasuni • Zadara*
- NetApp Cloud Volumes ONTAP

Storage Management

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

(*) roadmap items

StorageGuard On-Premises Architecture



StorageGuard

1 Master Server:
- Windows VM
- CS software

2 ORACLE 12/18/19

3 Scale-out collectors (optional)

SSH (EMC/IBM)
HTTP (HDS/HP/NETAPP)

SSH / HTTP / Rest

- SSH (Unix)
- WMI/WinRM (Windows)

3 Storage arrays

- SSH to CLI proxy (VMAX / XIV / 3PAR)
- SSH (V7000 / SVC / DataDomain / Isilon / RecoverPoint)
- HTTPS (Hitachi / VPLEX)
- ZAPI (NetApp)

4 SAN switches

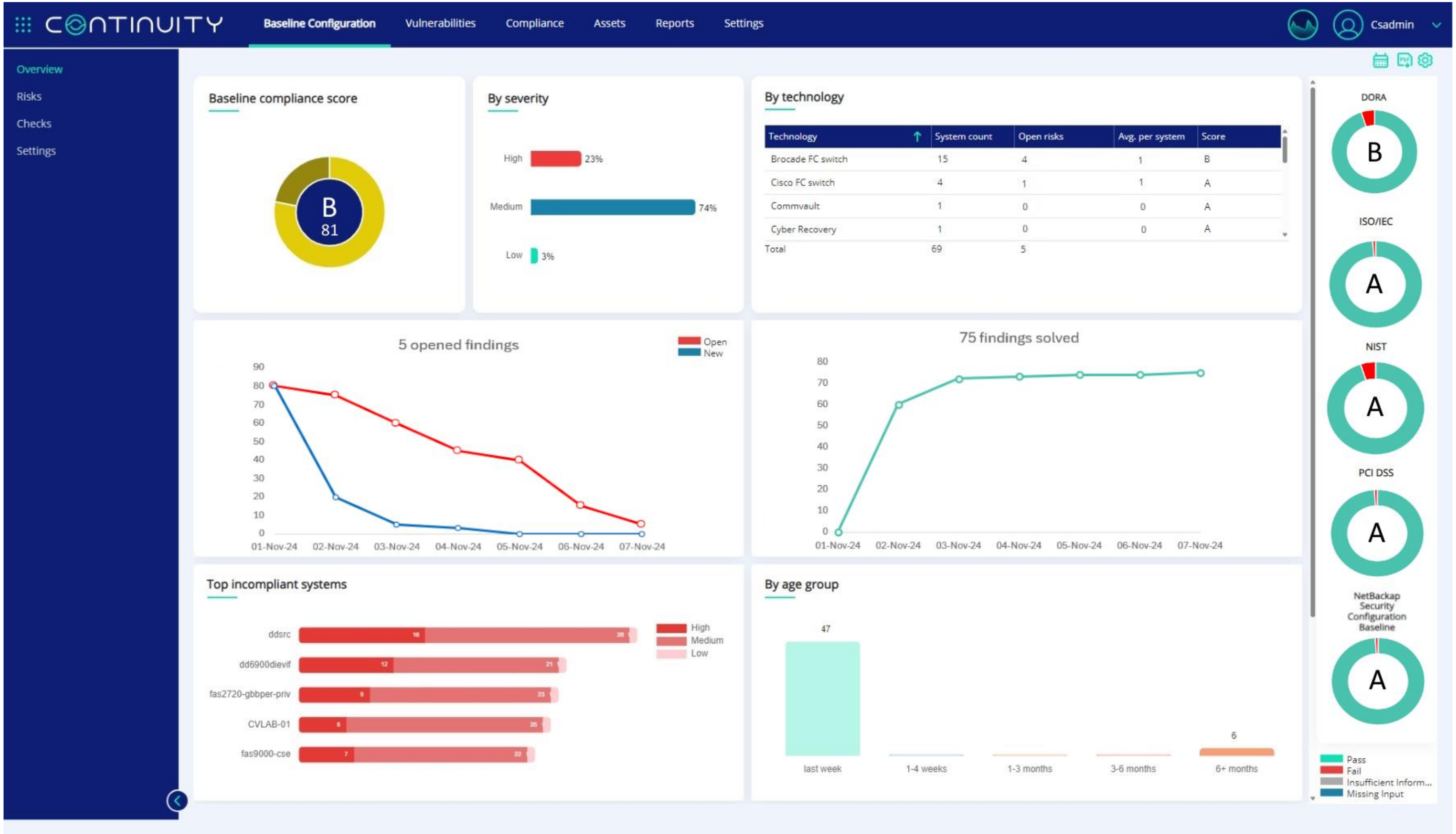
- Cisco MDS CLI
- HP vConnect CLI
- Brocade CLI
- BNA Rest API

5 Storage Management Servers (physical & virtual)

- OS and vendor commands / queries

All executed commands are strictly read-only

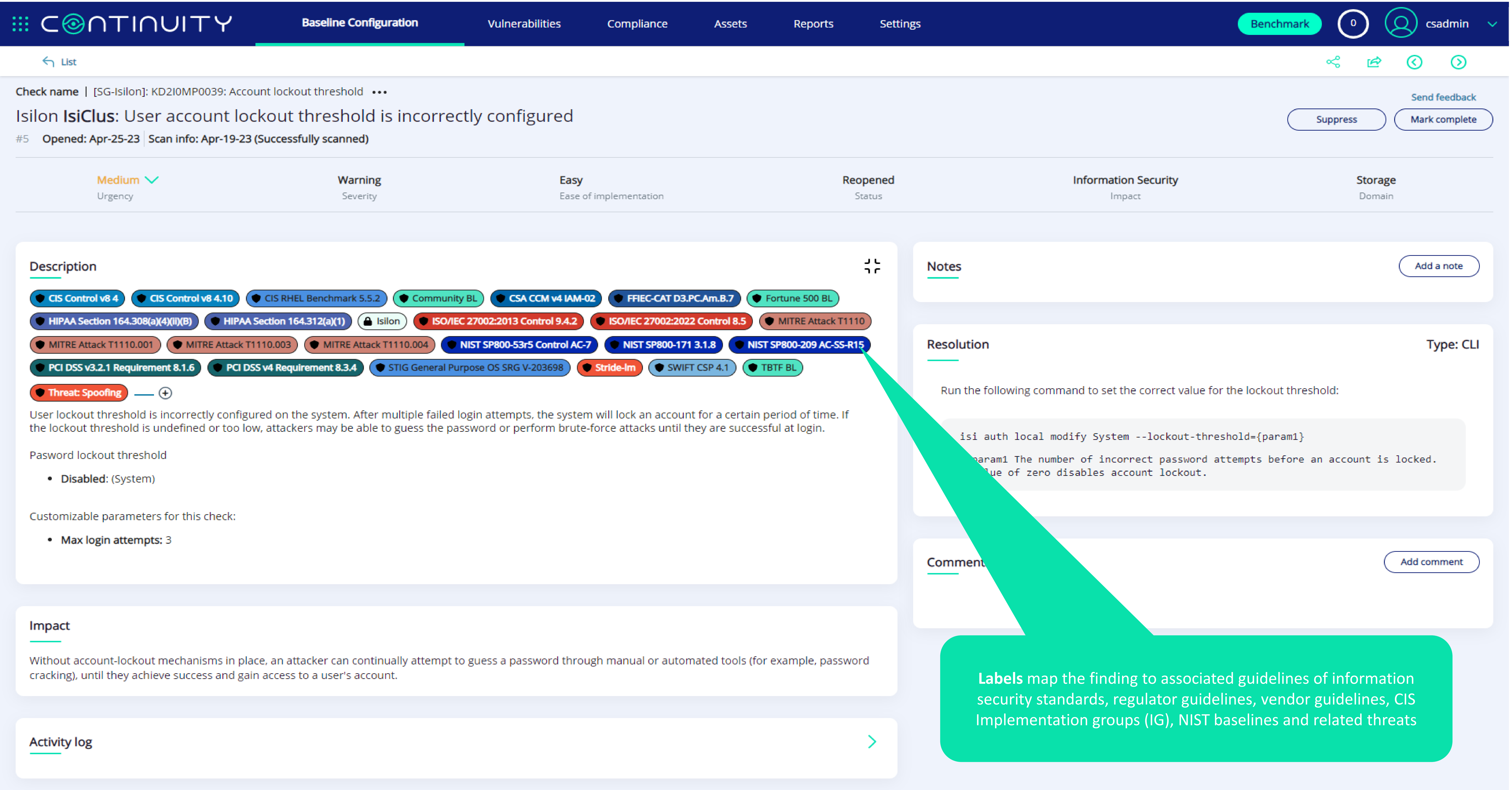
Dashboard di StorageGuard



By technology

Technology	System count	Open risks	Avg. per system	Score
Brocade FC switch	15	4	1	B
Cisco FC switch	4	1	1	A
Commvault	1	0	0	A
Cyber Recovery	1	0	0	A
Total	69	5		

Come StorageGuard presenta un rischio: Pericolosità, Descrizione, Impatto, Risoluzione



Check name | [SG-Isilon]: KD2I0MP0039: Account lockout threshold •••

Isilon **IsiClus:** User account lockout threshold is incorrectly configured

#5 Opened: Apr-25-23 | Scan info: Apr-19-23 (Successfully scanned)

Medium	Warning	Easy	Reopened	Information Security	Storage
Urgency	Severity	Ease of implementation	Status	Impact	Domain

Description

CIS Control v8 4 · CIS Control v8 4.10 · CIS RHEL Benchmark 5.5.2 · Community BL · CSA CCM v4 IAM-02 · FFIEC-CAT D3.PC.Am.B.7 · Fortune 500 BL · HIPAA Section 164.308(a)(4)(ii)(B) · HIPAA Section 164.312(a)(1) · Isilon · ISO/IEC 27002:2013 Control 9.4.2 · ISO/IEC 27002:2022 Control 8.5 · MITRE Attack T1110 · MITRE Attack T1110.001 · MITRE Attack T1110.003 · MITRE Attack T1110.004 · NIST SP800-53r5 Control AC-7 · NIST SP800-171 3.1.8 · NIST SP800-209 AC-SS-R15 · PCI DSS v3.2.1 Requirement 8.1.6 · PCI DSS v4 Requirement 8.3.4 · STIG General Purpose OS SRG V-203698 · Stride-Im · SWIFT CSP 4.1 · TBTF BL · Threat: Spoofing

User lockout threshold is incorrectly configured on the system. After multiple failed login attempts, the system will lock an account for a certain period of time. If the lockout threshold is undefined or too low, attackers may be able to guess the password or perform brute-force attacks until they are successful at login.

Pasword lockout threshold

- **Disabled:** (System)

Customizable parameters for this check:

- **Max login attempts:** 3

Impact

Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account.

Activity log

Notes

Resolution

Type: CLI

Run the following command to set the correct value for the lockout threshold:

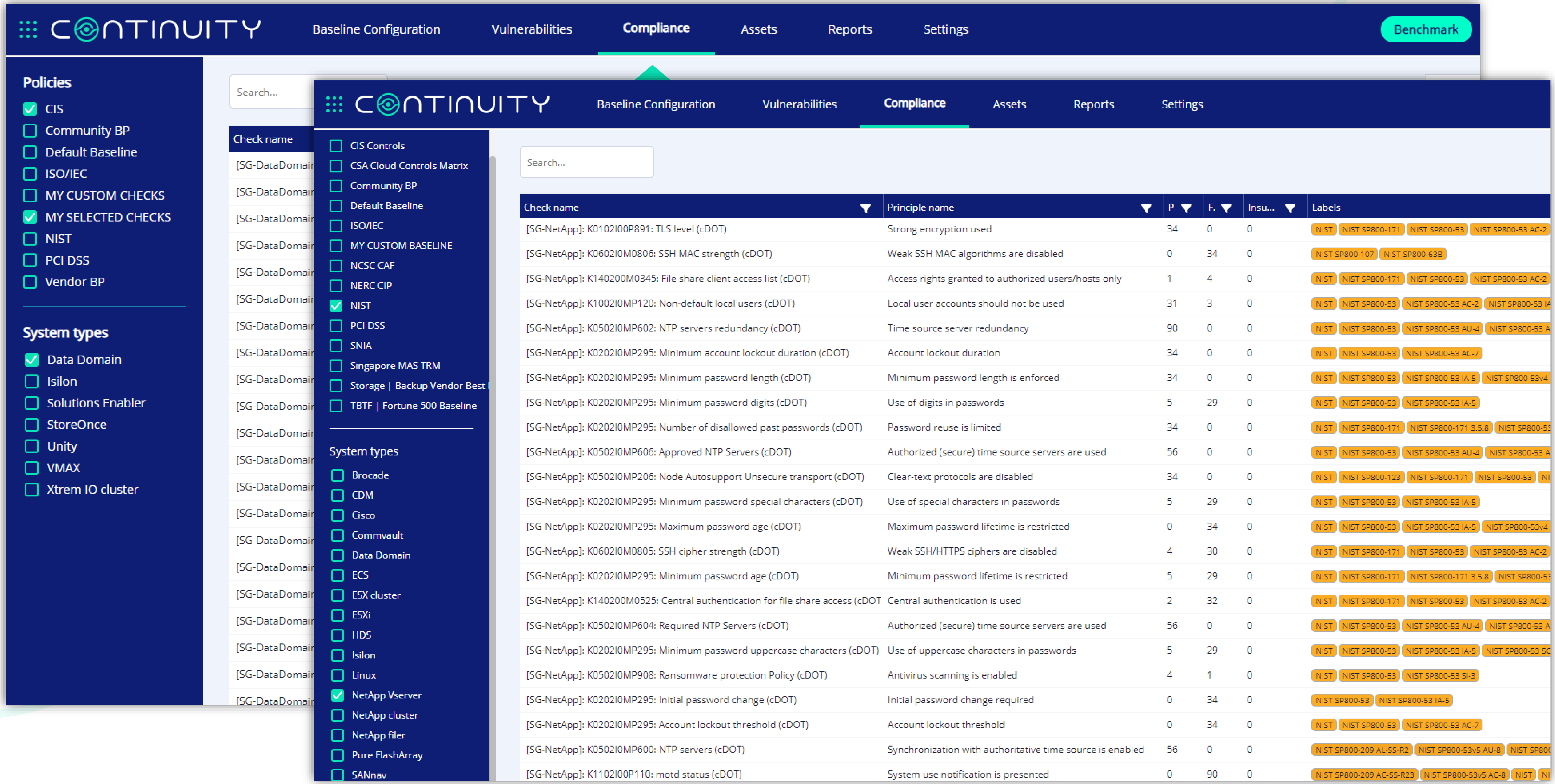
```
isi auth local modify System --lockout-threshold={param1}

param1 The number of incorrect password attempts before an account is locked.
lue of zero disables account lockout.
```

Comment

Labels map the finding to associated guidelines of information security standards, regulator guidelines, vendor guidelines, CIS Implementation groups (IG), NIST baselines and related threats

Strumento da utilizzare in sede di Audit



Policies

- ☑ CIS
- □ Community BP
- □ Default Baseline
- □ ISO/IEC
- □ MY CUSTOM CHECKS
- ☑ MY SELECTED CHECKS
- □ NIST
- □ PCI DSS
- □ Vendor BP

System types

- ☑ Data Domain
- □ Isilon
- □ Solutions Enabler
- □ StoreOnce
- □ Unity
- □ VMAX
- □ Xtrem IO cluster

Check name
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai
[SG-DataDomai

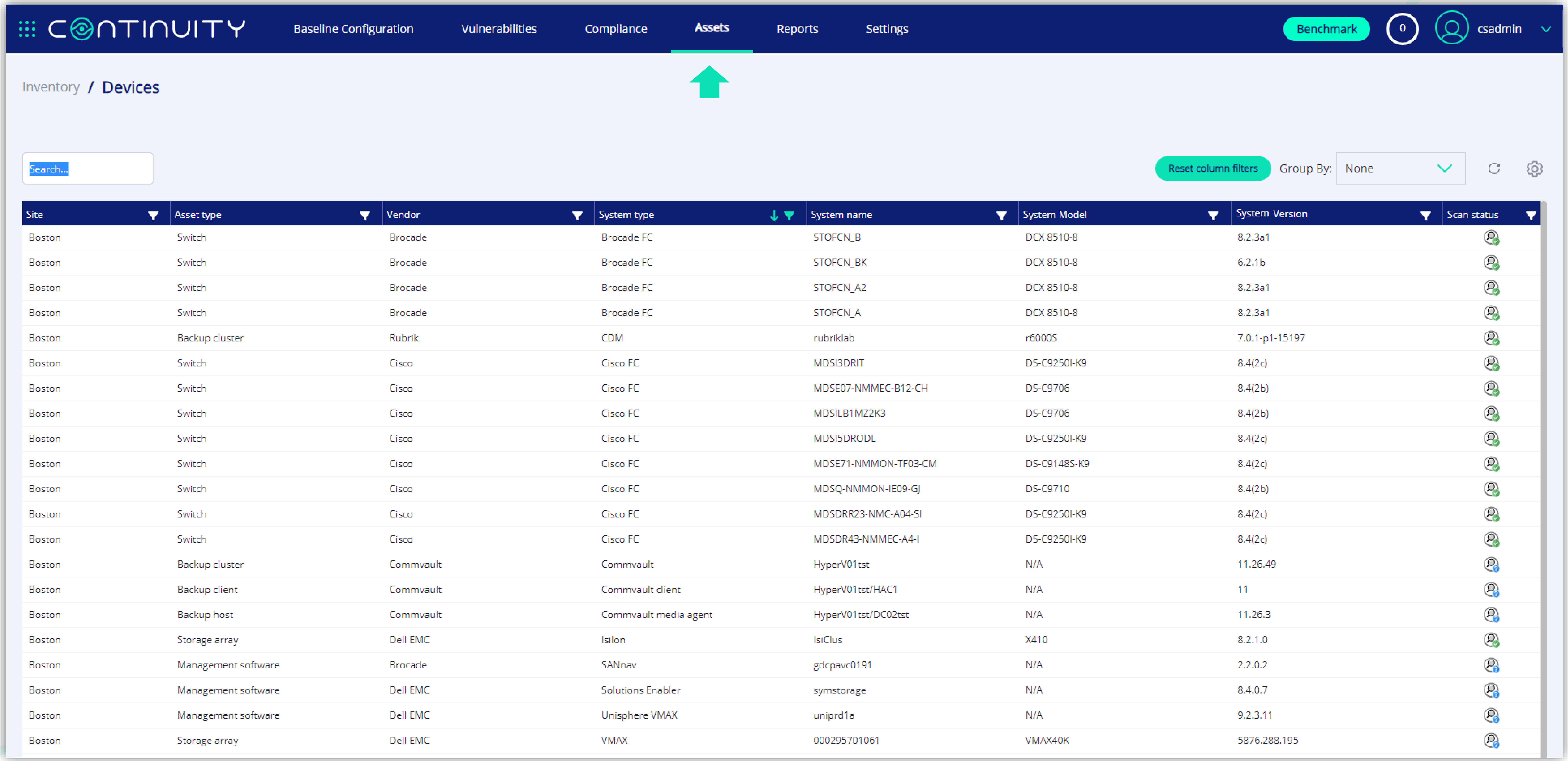
- □ CIS Controls
- □ CSA Cloud Controls Matrix
- □ Community BP
- □ Default Baseline
- □ ISO/IEC
- □ MY CUSTOM BASELINE
- □ NCSC CAF
- □ NERC CIP
- ☑ NIST
- □ PCI DSS
- □ SNIA
- □ Singapore MAS TRM
- □ Storage | Backup Vendor Best
- □ TBTF | Fortune 500 Baseline

System types

- □ Brocade
- □ CDM
- □ Cisco
- □ Commvault
- □ Data Domain
- □ ECS
- □ ESX cluster
- □ ESXi
- □ HDS
- □ Isilon
- □ Linux
- ☑ NetApp Vserver
- □ NetApp cluster
- □ NetApp filer
- □ Pure FlashArray
- □ SANnav

Check name	Principle name	P	F.	Insu...	Labels
[SG-NetApp]: K0102I00P891: TLS level (cDOT)	Strong encryption used	34	0	0	NIST NIST SP800-171 NIST SP800-53 NIST SP800-53 AC-2
[SG-NetApp]: K0602I0M0806: SSH MAC strength (cDOT)	Weak SSH MAC algorithms are disabled	0	34	0	NIST SP800-107 NIST SP800-63B
[SG-NetApp]: K140200M0345: File share client access list (cDOT)	Access rights granted to authorized users/hosts only	1	4	0	NIST NIST SP800-171 NIST SP800-53 NIST SP800-53 AC-2
[SG-NetApp]: K1002I0MP120: Non-default local users (cDOT)	Local user accounts should not be used	31	3	0	NIST NIST SP800-53 NIST SP800-53 AC-2 NIST SP800-53 IA
[SG-NetApp]: K0502I0MP602: NTP servers redundancy (cDOT)	Time source server redundancy	90	0	0	NIST NIST SP800-53 NIST SP800-53 AU-4 NIST SP800-53 A
[SG-NetApp]: K0202I0MP295: Minimum account lockout duration (cDOT)	Account lockout duration	34	0	0	NIST NIST SP800-53 NIST SP800-53 AC-7
[SG-NetApp]: K0202I0MP295: Minimum password length (cDOT)	Minimum password length is enforced	34	0	0	NIST NIST SP800-53 NIST SP800-53 IA-5 NIST SP800-53v4
[SG-NetApp]: K0202I0MP295: Minimum password digits (cDOT)	Use of digits in passwords	5	29	0	NIST NIST SP800-53 NIST SP800-53 IA-5
[SG-NetApp]: K0202I0MP295: Number of disallowed past passwords (cDOT)	Password reuse is limited	34	0	0	NIST NIST SP800-171 NIST SP800-171 3.5.8 NIST SP800-53
[SG-NetApp]: K0502I0MP606: Approved NTP Servers (cDOT)	Authorized (secure) time source servers are used	56	0	0	NIST NIST SP800-53 NIST SP800-53 AU-4 NIST SP800-53 A
[SG-NetApp]: K0502I0MP206: Node Autosupport Unsecure transport (cDOT)	Clear-text protocols are disabled	34	0	0	NIST NIST SP800-123 NIST SP800-171 NIST SP800-53 NI
[SG-NetApp]: K0202I0MP295: Minimum password special characters (cDOT)	Use of special characters in passwords	5	29	0	NIST NIST SP800-53 NIST SP800-53 IA-5
[SG-NetApp]: K0202I0MP295: Maximum password age (cDOT)	Maximum password lifetime is restricted	0	34	0	NIST NIST SP800-53 NIST SP800-53 IA-5 NIST SP800-53v4
[SG-NetApp]: K0602I0M0805: SSH cipher strength (cDOT)	Weak SSH/HTTPS ciphers are disabled	4	30	0	NIST NIST SP800-171 NIST SP800-53 NIST SP800-53 AC-2
[SG-NetApp]: K0202I0MP295: Minimum password age (cDOT)	Minimum password lifetime is restricted	5	29	0	NIST NIST SP800-171 NIST SP800-171 3.5.8 NIST SP800-53
[SG-NetApp]: K140200M0525: Central authentication for file share access (cDOT	Central authentication is used	2	32	0	NIST NIST SP800-171 NIST SP800-53 NIST SP800-53 AC-2
[SG-NetApp]: K0502I0MP604: Required NTP Servers (cDOT)	Authorized (secure) time source servers are used	56	0	0	NIST NIST SP800-53 NIST SP800-53 AU-4 NIST SP800-53 A
[SG-NetApp]: K0202I0MP295: Minimum password uppercase characters (cDOT)	Use of uppercase characters in passwords	5	29	0	NIST NIST SP800-53 NIST SP800-53 IA-5 NIST SP800-53 SC
[SG-NetApp]: K0502I0MP908: Ransomware protection Policy (cDOT)	Antivirus scanning is enabled	4	1	0	NIST NIST SP800-53 NIST SP800-53 SI-3
[SG-NetApp]: K0202I0MP295: Initial password change (cDOT)	Initial password change required	0	34	0	NIST SP800-53 NIST SP800-53 IA-5
[SG-NetApp]: K0202I0MP295: Account lockout threshold (cDOT)	Account lockout threshold	0	34	0	NIST NIST SP800-53 NIST SP800-53 AC-7
[SG-NetApp]: K0502I0MP600: NTP servers (cDOT)	Synchronization with authoritative time source is enabled	56	0	0	NIST SP800-209 AL-SS-R2 NIST SP800-53v5 AU-8 NIST SP800
[SG-NetApp]: K1102I00P110: motd status (cDOT)	System use notification is presented	0	90	0	NIST SP800-209 AC-SS-R23 NIST SP800-53v5 AC-8 NIST NI

Storage/Backup Asset Inventory



Site	Asset type	Vendor	System type	System name	System Model	System Version	Scan status
Boston	Switch	Brocade	Brocade FC	STOFCN_B	DCX 8510-8	8.2.3a1	✓
Boston	Switch	Brocade	Brocade FC	STOFCN_BK	DCX 8510-8	6.2.1b	✓
Boston	Switch	Brocade	Brocade FC	STOFCN_A2	DCX 8510-8	8.2.3a1	✓
Boston	Switch	Brocade	Brocade FC	STOFCN_A	DCX 8510-8	8.2.3a1	✓
Boston	Backup cluster	Rubrik	CDM	rubriklab	r6000S	7.0.1-p1-15197	✓
Boston	Switch	Cisco	Cisco FC	MDSI3DRIT	DS-C9250I-K9	8.4(2c)	✓
Boston	Switch	Cisco	Cisco FC	MDSE07-NMMEC-B12-CH	DS-C9706	8.4(2b)	✓
Boston	Switch	Cisco	Cisco FC	MDSILB1MZ2K3	DS-C9706	8.4(2b)	✓
Boston	Switch	Cisco	Cisco FC	MDSI5DRODL	DS-C9250I-K9	8.4(2c)	✓
Boston	Switch	Cisco	Cisco FC	MDSE71-NMMON-TF03-CM	DS-C9148S-K9	8.4(2c)	✓
Boston	Switch	Cisco	Cisco FC	MDSQ-NMMON-IE09-GJ	DS-C9710	8.4(2b)	✓
Boston	Switch	Cisco	Cisco FC	MDSDRR23-NMC-A04-SI	DS-C9250I-K9	8.4(2c)	✓
Boston	Switch	Cisco	Cisco FC	MDSDR43-NMMEC-A4-I	DS-C9250I-K9	8.4(2c)	✓
Boston	Backup cluster	Commvault	Commvault	HyperV01tst	N/A	11.26.49	?
Boston	Backup client	Commvault	Commvault client	HyperV01tst/HAC1	N/A	11	?
Boston	Backup host	Commvault	Commvault media agent	HyperV01tst/DC02tst	N/A	11.26.3	?
Boston	Storage array	Dell EMC	Isilon	IsiClus	X410	8.2.1.0	✓
Boston	Management software	Brocade	SANnav	gdcpavc0191	N/A	2.2.0.2	?
Boston	Management software	Dell EMC	Solutions Enabler	symstorage	N/A	8.4.0.7	?
Boston	Management software	Dell EMC	Unisphere VMAX	uniprd1a	N/A	9.2.3.11	?
Boston	Storage array	Dell EMC	VMAX	000295701061	VMAX40K	5876.288.195	?

NOVASYSTEM

CONTINUITY

Grazie