CONTINUITY

StorageGuard

About Us

Founded in 2005, serving leading enterprises worldwide

We help our customers to

- Prevent outages on their critical IT infrastructure
- Secure their Storage & Backup environment

SELECTED CUSTOMERS

Storage Security 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

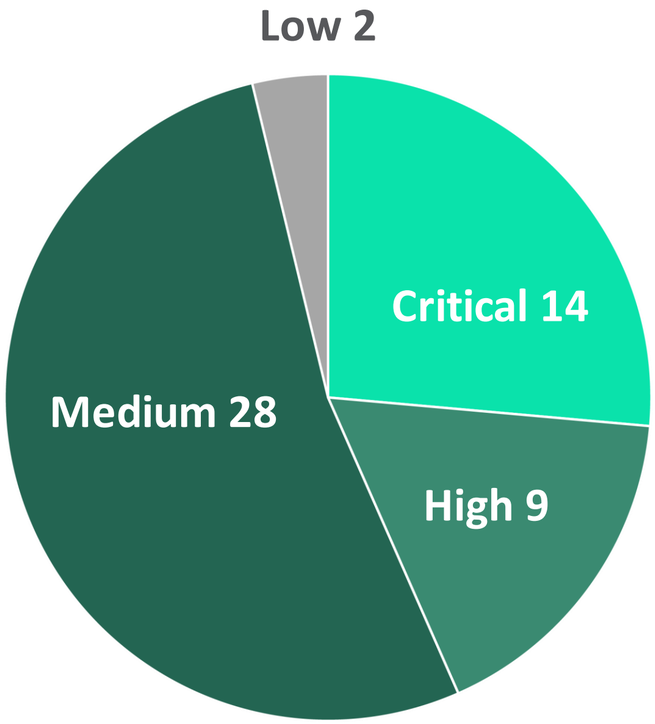
CHALLENGE

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

SOLUTION BY CONTINUITY

- Continuous scanning and analysis of the bank's storage and backup systems worldwide
- Automatic detection of security risks
- Overall health and compliance reports

Storage / Backup vendor	Vulnerability score	Configuration Compliance score
Dell EMC	53	39
Cohesity	93	100
IBM	65	22
Pure Storage	7	71
Rubrik	85	52
Hitachi Vantara	21	96
NetApp	88	35



CONTINUITY


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

The Gap

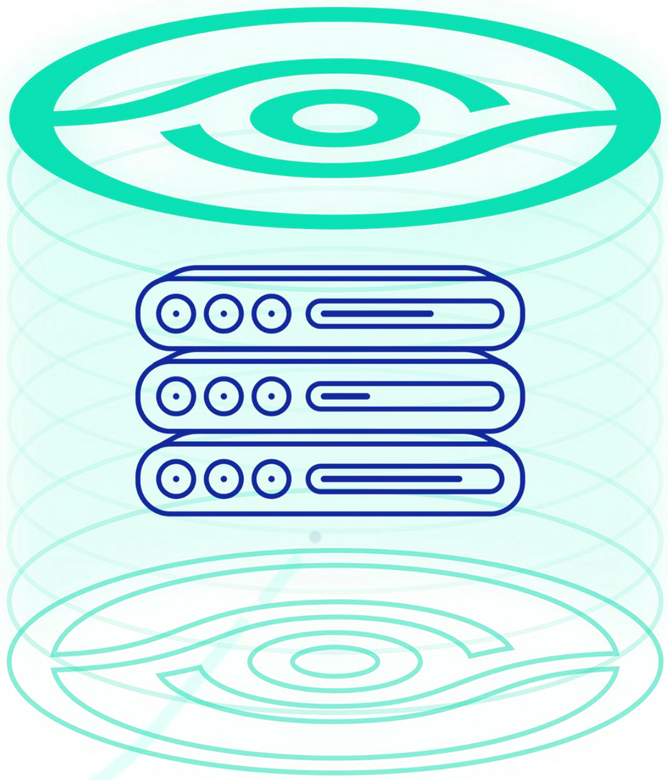

NETWORK
ENDPOINTS
SERVERS
DATABASES
COMPUTE
Storage & Backup
The Ultimate Line of Defense Against Cyberattacks
Block Storage
Storage Software
Storage Management
SAN
Storage Network
Backup Systems
Object Storage
Data Protection Systems
Storage Virtualization
Server-Based Storage
File Storage

Is it time for more Storage & Backup 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 (e.g., Rapid7, Nessus, Qualys)	Existing tools offer almost zero coverage for storage, storage management, and backup

The Solution – StorageGuard

Validation of security config and (“Security Baselines”) 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.

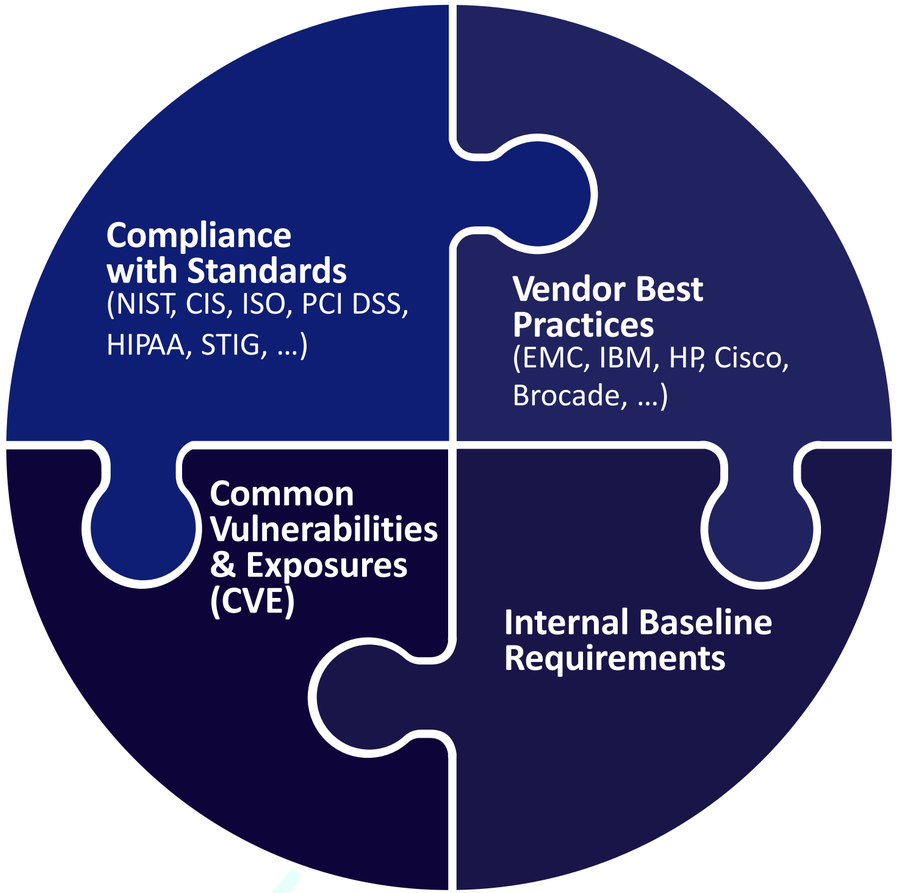
Focus on converged and storage systems

- Block, object, IP storage, storage network, data protection systems,
- Storage & backup management systems, Virtual SAN, NAS/SAN, file shares and more

How it works

- Fast on-prem deployment, agentless scan, zero impact on production

The Risk Knowledgebase Sources



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*

CONTINUITY

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 • XIV • IBM SVC • V7000/5000 • Storwize • A9000/R • V9000 • FlashSystem • 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)*
- 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 • Pure • Huawei*

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 • IDPA
- NetBackup • Commvault • HP StoreOnce • Veeam* • Cohesity • Rubrik • Networker*
- 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

CONTINUITY

Date
from Mar-05-21
to Mar-11-21

System types
- [x] 3PAR
- [x] Brocade
- [ ] Cisco
- [x] DataDomain
- [ ] ECS
- [ ] HCP
- [ ] HCP tenant
- [x] HDS
- [x] Infinidat
- [ ] Isilon
- [ ] Linux
- [ ] NetApp Vserver
- [x] NetApp cluster
- [ ] NetApp filer
- [ ] RecoverPoint
- [x] SVC
- [ ] ScaleIO system
- [x] Symmetrix
- [ ] VNX
- [ ] VPLEX cluster
- [ ] XIV
- [x] Xtrem IO cluster

Risks during a selected period

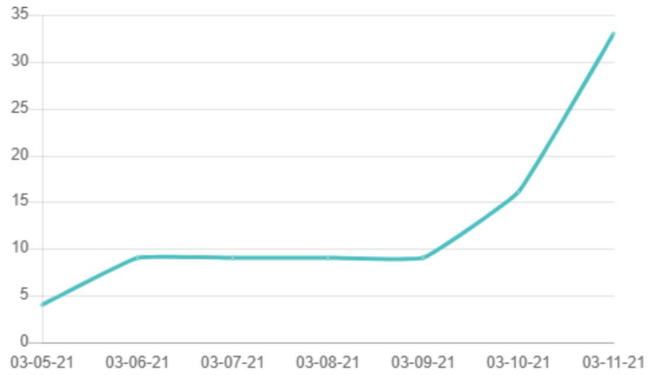
Total open risks
33 +72%

Average open risks per system
5 +31%

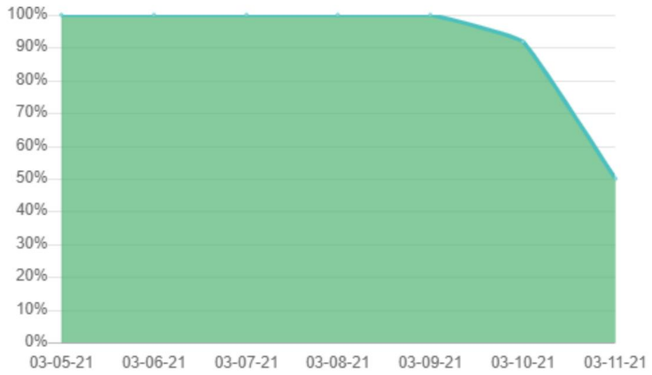
Max open risks per system
13 +12%

Scan Coverage
100%

New risks



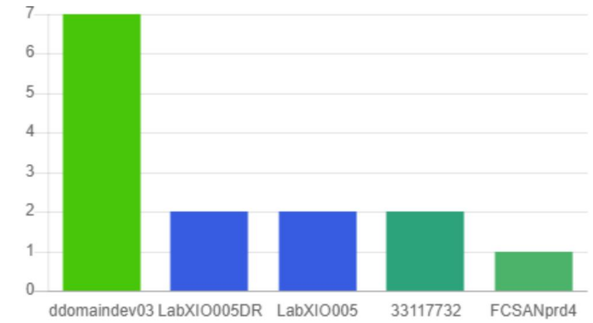
Systems health



Scan Coverage

System Type	Discovered	In Scope	Scanned
3PAR	2	1	1
Brocade	2	2	2
DataDomain	1	1	1
HDS	5	5	5
Infinidat	1	0	0
NetApp cluster	1	1	1
SVC	1	0	0
Symmetrix	1	0	0
Xtrem IO cluster	2	2	2

Highest-risk system



Check name | [DSA-CVEs]: ECS vulnerability analysis: DSA-2021-273 •••

Send feedback

ECS **ECS_PDC01**: vulnerability identified (DSA-2021-273)

#602 **Dec-23-21**

Suppress Mark complete

High	Warning	Open	Storage
Urgency	Severity	Status	Domain

Description

CVE-2021-44228 CVE-2021-45046 ECS

DSA-2021-273: Dell EMC ECS remediation is available for the Apache Log4j Remote Code Execution Vulnerability that may be exploited by malicious users to compromise the affected system.

link: https://www.dell.com/support/kbdoc/en-us/000194612/dsa-2021-273-dell-emc-ecs-security-update-for-apache-log4j-remote-code-execution-vulnerability-cve-2021-44228
CVSS Score: 10.0

Vulnerable version

- 3.6.1.0.126874.b09da837a1a

Impact

The Apache Log4j Remote Code Execution Vulnerability may be exploited by malicious users to compromise the affected system.

Activity log

Notes

Add a note

Resolution

update to version 3.6.2.1 or higher

Check name | [DSA-CVEs]: NetApp cDOT vulnerability analysis: NTAP-20211029-0003 •••

Send feedback

NetApp cluster **prdnass01**: vulnerability identified (NTAP-20211029-0003)

#298 **Dec-16-21**

Suppress | Mark complete

High Urgency	Warning Severity	Open Status	Storage Domain

Description

CVE-2021-22945 | CVE-2021-22946 | CVE-2021-22947 | NetApp

NTAP-20211029-0003: Multiple NetApp products incorporate libcurl.
Various versions of Libcurl are susceptible to vulnerabilities which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

link: https://security.netapp.com/advisory/ntap-20211029-0003/
CVSS Score: 9.8

Vulnerable version

- 9.8P5

Impact

Successful exploitation of these vulnerabilities could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS).

Activity log

Notes

Add a note

Resolution

update to version 9.9.1P5 or higher.

Check name | [DSA-Isilon]: K170D00M0230: Antivirus server configuration •••

Send feedback

Isilon **IsiClus** at **TLV**: Antivirus(ICAP) server not configured

#35 **Nov-28-21**

Suppress | Mark complete

Medium	Warning	Reopened	Storage
Urgency	Severity	Status	Domain

Description

CIS Control | CIS Control 8.1 | Isilon | ISO | ISO/IEC 27001 | +7

An EMC Isilon storage system is not configured. OneFS sends files through ICAP to a server running third-party antivirus scanning software (ICAP servers). ICAP servers scan files for viruses.

Configured ICAP servers

- None

Impact

Without anti-virus scanning, malicious software can attack systems, disable a network, or lead to compromise of data.

Activity log

Notes

Add a note

Resolution

The following command can be used to add an ICAP server:

```
isi antivirus servers create {param1}
# param1 URL of the ICAP server
```

Check name | [DSA-Brocade]: K0204000P115: Default passwords •••

Send feedback

Brocade **brocade01.lab** at **TLV**: Default passwords are used

#641 **Nov-24-21**

Suppress | Mark complete

High Urgency	Error Severity	Reopened Status	Storage Domain

Description

Brocade | CIS Control | CIS Control 4.2 | Community | FFIEC | +6

Default users for a Brocade SAN switch are configured with the default (factory) known passwords.

Default password used

- root

Customizable parameters for this check:

- **Default users:** user, root, factory,admin

Impact

Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.

Activity log

Notes

Add a note

Resolution

To solve this issue you must change password for default user accounts.

```
passwd {param1} -old {param2} -new {param3)
# param1 user account
# param2 old password
# param3 new password
```

Check name | [DSA-NetApp]: K0502I0MP908: Ransomware protection Policy (cDOT) •••

Send feedback

NetApp cluster **NetApp-Lab** at **TLV**: Ransomware filtration is not configured

#601 **Nov-24-21**

Suppress | Mark complete

High ⌄	Error	Reopened	Storage
Urgency	Severity	Status	Domain

Description

CIS Control | CIS Control 8.1 | ISO | ISO/IEC 27001 | ISO/IEC 27001 A.12.2.1 +7

The system is not configured to block ransomware attacks. File policies can be defined to block writes to an export or share that is suspected as ransomware.

Ransomware protection

- None

Customizable parameters for this check:

- **Blocked file operations:** create
- **Known ransomware file extensions:** .locky,.locked,.encoderpass,.ecc,.ezz,.exx,.zzz, .xyz,.micro,.encrypted,.crypto,.crypt,.crinf,.r5a,.XRNT,.XTBL,.R16M01D05,.pzdc,.good,.LOL,.OMG

Impact

Allowing ransomware to be written the shares or zones increases the risk of a successful ransomware attack. Furthermore since shares and exports are commonly accessible to large number of endpoints, ransomware may spread faster and wider.

Activity log

Notes

Add a note

Resolution

Configure file policies to block traffic that is suspected as ransomware:

```
fpolicy policy event create -vserver {param1} -event-name ransomware_EVENT -
protocol cifs -file-operations create rename

fpolicy policy create -vserver {param1} -policy-name ransomware_POLICY -events
ransomware_EVENT

fpolicy policy scope create -vserver {param1} -policy-name ransomware_POLICY -
shares-to-include * -file-extensions-to-include {param2}

fpolicy enable -vserver {param1} -policy-name ransomware_POLICY -sequence-
number 2

# param1 vserver name
```

Check name | [DSA-NetApp]: K1002I0MP0375: CIFS SMB version status •••

Send feedback

NetApp cluster **cl_nas02**: SMBv1 and SMBv2 are enabled

#841 **Jan-11-22**

Suppress | Mark complete

High	Error	Open	Storage
Urgency	Severity	Status	Domain

Description

CISA Ransomware Guide | ISO/IEC 27040 | Microsoft | NetApp | NIST SP800-209 NC-SS-R19

A vulnerable SMB version is enabled on the storage system. Threat actors use SMB to propagate malware across organizations.

Violation:
"is-smb1-enabled":"true"
"is-smb2-enabled":"true"

Impact

SMBv1 and SMBv2 are highly vulnerable and should not be used. For example, Wanna cry and Petya are forms of malware that took advantage of SMBv1 weaknesses.

Activity log

Notes

Add a note

Resolution

NOTE: Analyze and mitigate any existing dependencies that may break before disabling SMBv1 or SMBv2.

.

The following command can be used to change CIFS options:

```
vserver cifs options modify -vserver {param1} -smb1-enabled false -smb2-enabled
false

# param1 vserver name
```

Check name | [DSA-DataDomain]: K110CI00P690: Session timeout •••

Send feedback

DataDomain **p_dd020**: Idle session timeout is incorrectly configured

#121 **Dec-13-21**

Suppress | Mark complete

Medium Urgency	Warning Severity	Open Status	Storage Domain

Description

CIS Control | CIS Control 16 | DataDomain | NIST | NIST SP800-53 | +4

Inactivity (idle session) timeout is incorrectly configured on an EMC Data Domain system. The configured timeout is above the required value, thus enabling user session to live for a long period of time and increasing the risk of unauthorized or malicious access.

Services with infinite session timeout

- Ftps, Ftp, Ssh/Scp, Telnet

Impact

Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use ,access and risk to networks is minimized. Users must be logged out of the system after a period of inactivity to minimize the possibility of an attacker using their system to extract information from the organization.

Activity log

Notes

Add a note

Resolution

The following command can be used to set the timeout:

```
adminaccess {param1} option set session-timeout {param2}
# param1 ftp, ssh, etc.
# param2 timeout-in-secs
```

DataDomain **dd-prd02**: File retention lock option is disabled.

#15 **Opened: May-16-22**

Suppress Mark complete

High	Error	Open	Storage
Urgency	Severity	Status	Domain

Description

DataDomain FFIEC ISO/IEC 27040 SEC Rule 17a-4

Data Domain retention lock functionality ensures backup cannot be deleted during the retention period.

Retention Lock is status

- disabled

Impact

An attacker obtaining administrative access could delete backup copies and make recovery of data impossible.

ITSM systems

Activity log

Notes

Add a note

Resolution

Review backup software documentation for integration options with EMC Data Domain retention lock functionality.Use the following commands to configure retention lock:

```
mtree retention-lock set min-retention-period {param1} mtree {param2}
mtree retention-lock set max-retention-period {param3} mtree {param4}
system retention-lock compliance configure #reboots the system
# param1 min period (example: 1min, 1hr, 1day, 1mo, 1year)
# param2 mtree name
# param3 max period (example: 1min, 1hr, 1day, 1mo, 1year)
# param4 mtree name
```

Benefits of using StorageGuard

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

Protection & Compliance

- **Eliminate manual security validation efforts**
- Obtain valuable **remediation guidance** to speed-up time to resolve
- Meet **IT Audit requirements**: providing evidence for compliance
- Eliminate **configuration drift**: tracking **security configuration changes**
- **Continuously validate** against your chosen storage/backup security baseline

Visibility & Prioritization

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

CONTINUITY

StorageGuard POC

Learn how to achieve continuous storage/backup security, by running a StorageGuard POC

- A POC covers up to 9 scenarios:
  - Scan of 3 selected storage/backup systems
  - Detection of security risks
  - Remediation guidance
  - Auto-validation of remediated risks
  - Security baseline creation
  - Security baseline reporting and continuous validation
  - Compliance reporting
  - Integration and routing options
  - Custom checks
- Details: See StorageGuard POC Plan
- Duration: 5 joint work sessions (typically over a 2-week period)
- Conclusion: Presentation of POC Summary & Results to Senior Management

CONTINUITY


CONTINUITY