CONTINUITY

StorageGuard

Jasmin Hami, Head of Security Channels
jasminh@continuitysoftware.com

> “Ransomware attacks are targeting organizations’ network-attached storage (NAS) and backup storage devices.”

SecurityIntelligence

> “2021 will see a major emphasis in developing more comprehensive storage system security”

Forbes

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

- Refenced in Gartner's new report on Cyberstorage, the first such report on this topic.

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)

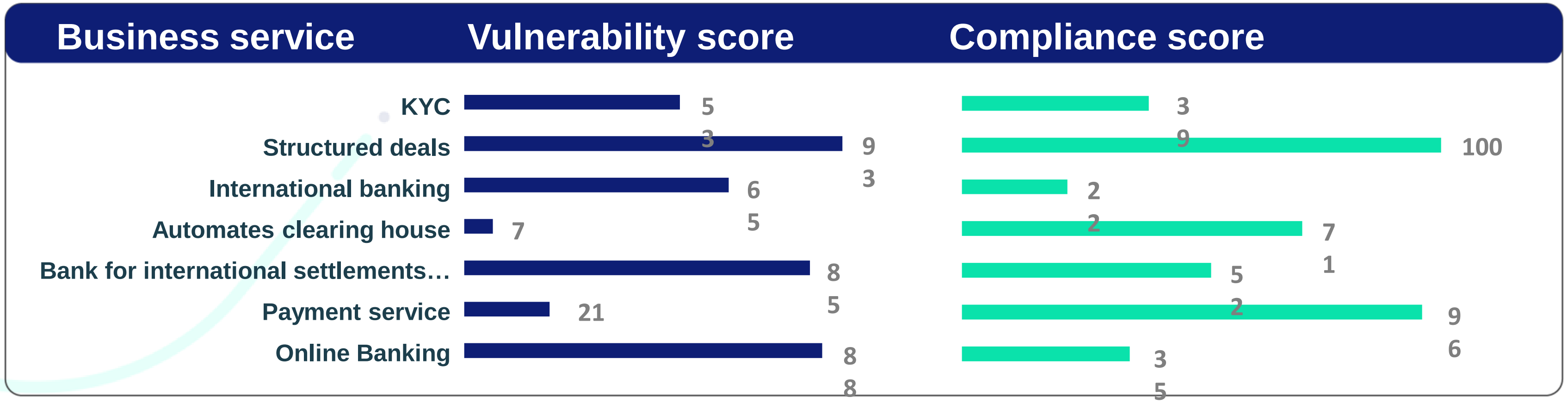
- Manual analysis is not feasible
- Failure to meet auditor deadlines for remediating the gap

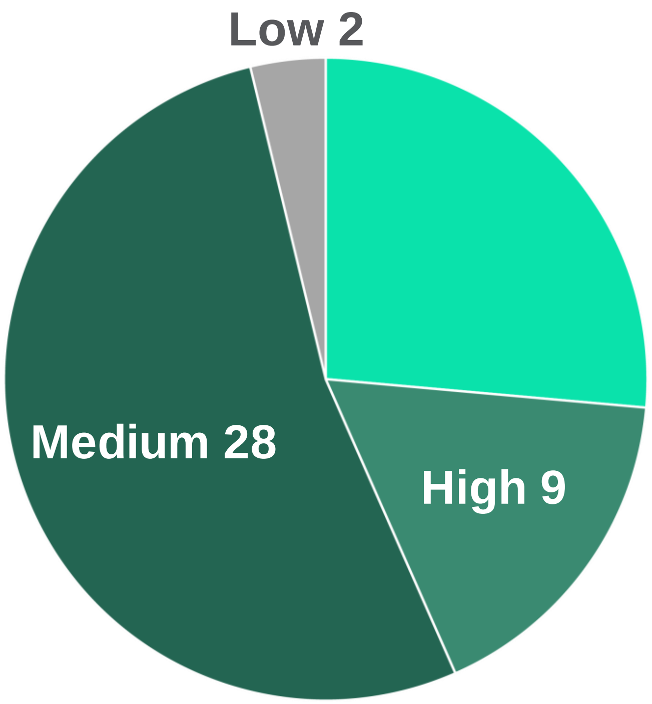
CHALLENGE

- 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





NIST Special Publication 800-209

Security Guidelines for Storage Infrastructure

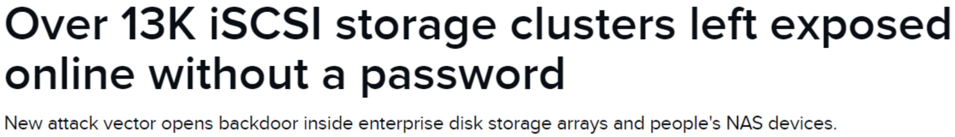
Ramaswamy Chandramouli
Doron Pinhas

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

FROM THE NEWS

New ransomware attacks target your **NAS** devices

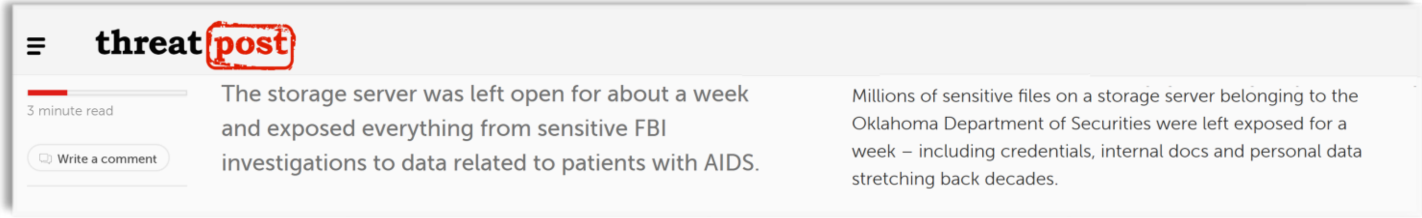


Over 13K iSCSI storage clusters left exposed online without a password

New attack vector opens backdoor inside enterprise disk storage arrays and people's NAS devices.

threatpost | Cloud Security / Malware / Vulnerabilities / InfoSec Insiders / Podcasts

Linux Variant of REvil Ransomware Targets VMware's ESXi, NAS Devices



threatpost

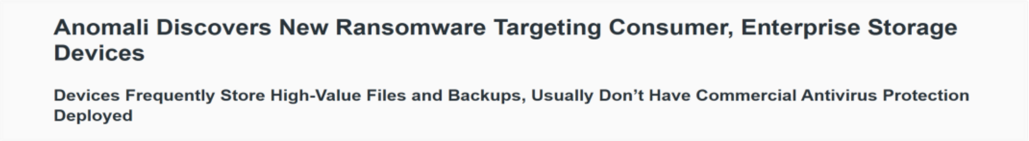
3 minute read

Write a comment

The storage server was left open for about a week and exposed everything from sensitive FBI investigations to data related to patients with AIDS.

Millions of sensitive files on a storage server belonging to the Oklahoma Department of Securities were left exposed for a week – including credentials, internal docs and personal data stretching back decades.

***OCIE risk alert:** "Misconfigured **security** settings on a **storage** device could result in unauthorized access to information"*



Anomali Discovers New Ransomware Targeting Consumer, Enterprise Storage Devices

Devices Frequently Store High-Value Files and Backups, Usually Don't Have Commercial Antivirus Protection Deployed

RISK ALERT

OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS

May 23, 2019

Safeguarding Customer Records and Information in Network Storage –

During recent examinations, the Office of Compliance Inspections and Examinations ("OCIE")' identified security risks associated with the storage of electronic customer records and information by broker-dealers and investment advisers in various network storage solutions, including those leveraging cloud-based storage.[1] Although the majority of these network storage solutions offered encryption, password protection, and other security features designed to prevent unauthorized access, examiners observed that firms did not always use the available security features. Weak or misconfigured security settings on a network storage device could result in unauthorized access to information stored on the device.

SECURITY

Why Enterprise Ransomware Attacks Are on the Rise

While ransomware attacks on consumers have declined, enterprise ransomware attacks have seen a more than 300% increase in the last year.

Brien Posey | Jun 24, 2019

threatpost

Previous article | Next article

LenovoEMC Storage Gear Leaks Sensitive Financial Data

Author:

Tom Spring

July 16, 2019 / 3:59 pm

Gartner: "*Harden the components of enterprise **backup** and **recovery** infrastructure against attacks… routinely examining backup application, **storage** and network access…. safeguard backup **storage** media and accessibility*"

Smarter With Gartner

6 Ways to Defend Against a Ransomware Attack

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

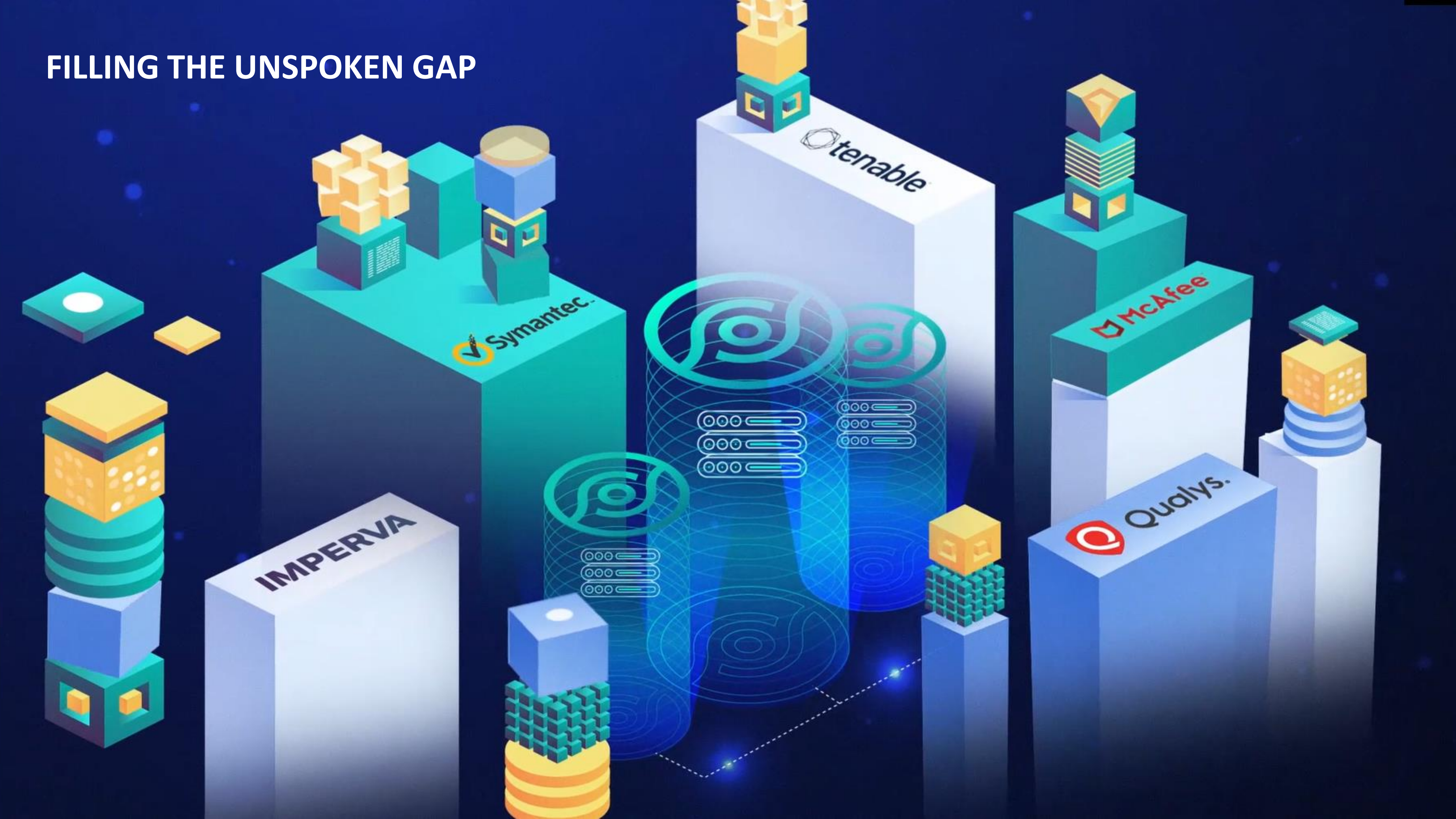
On average, an enterprise storage device has 15 vulnerabilities or security misconfigurations

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

THE UNSPOKEN GAP

A compromised storage system will lead to multi-system failure

FILLING THE UNSPOKEN GAP

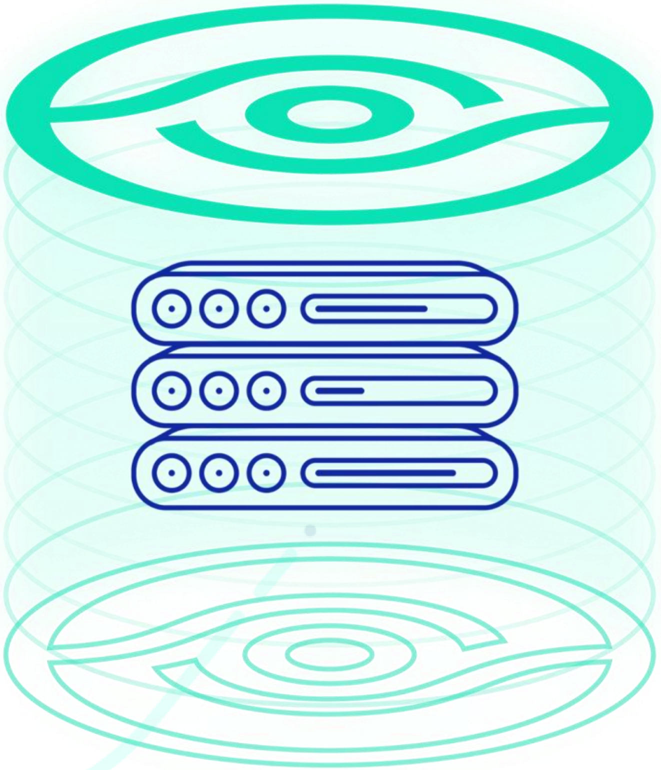


IS IT TIME FOR STORAGE SECURITY

	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 (e.g., 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

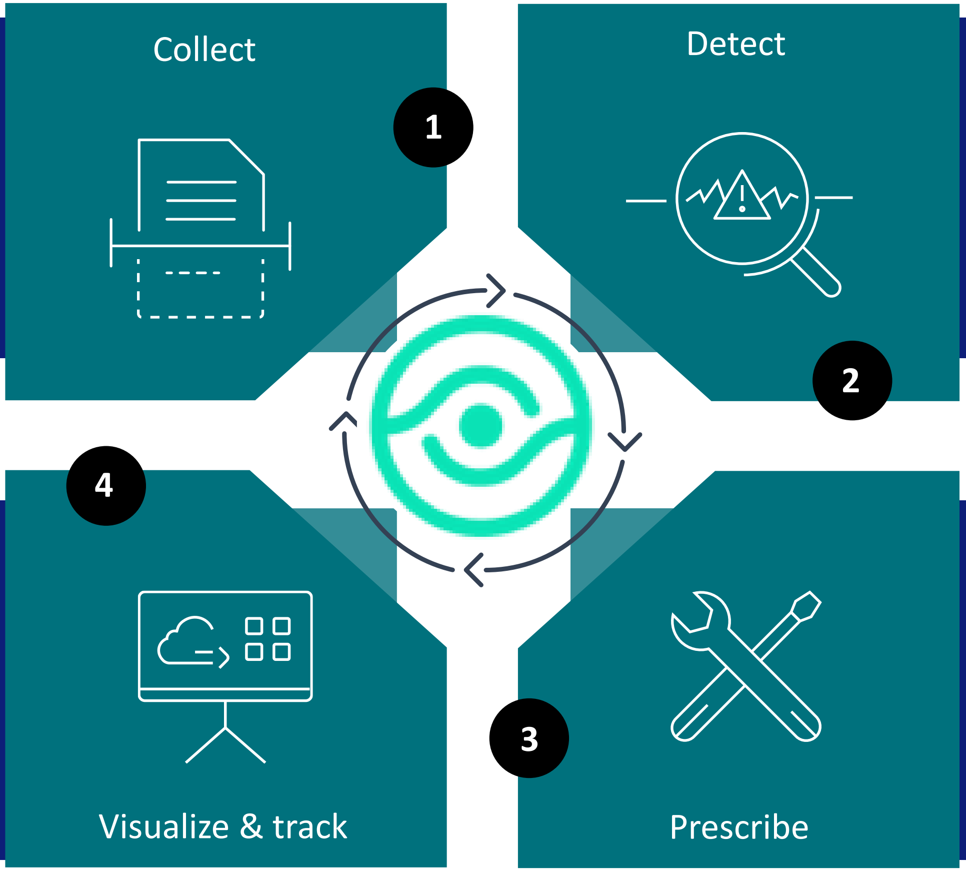
- Vendor best practices, community-driven baseline requirements
- Ransomware protection, vulnerabilities and compliance checks
- Configuration checks for Administrative Access, Authentication, Authorization, Audit Log, Data access, Services and Protocols, Isolation, ISO27001, CIS, NIST and more.

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

HOW IT WORKS

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

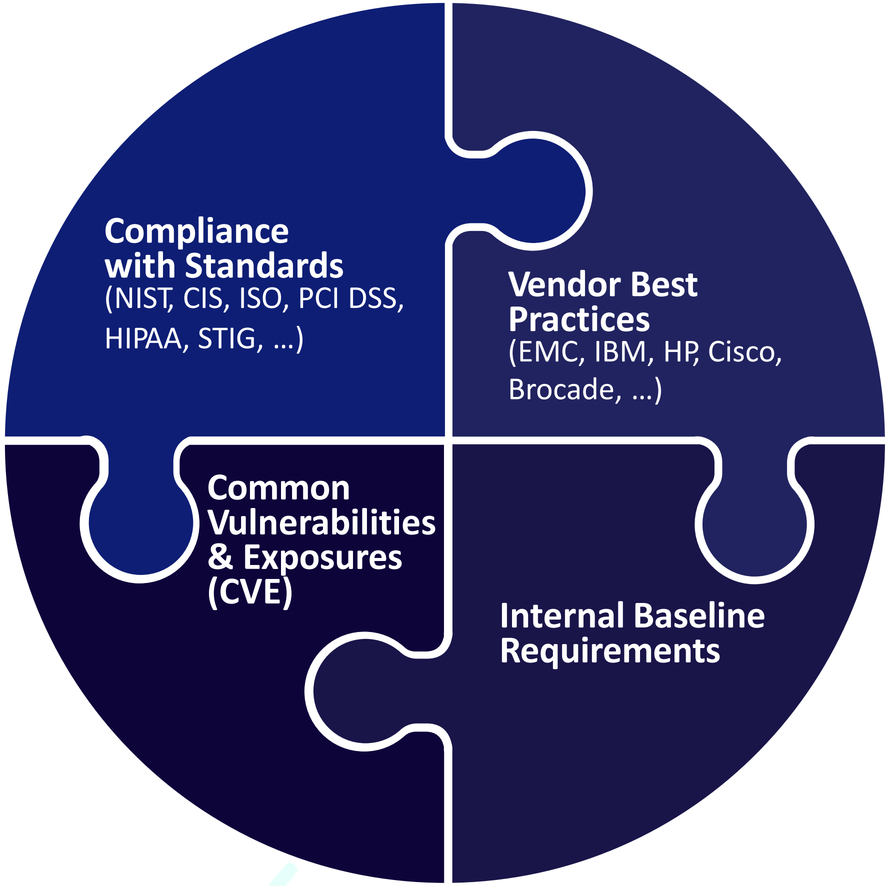


- » Analyzes configurations using a built-in risk detection engine
- » Detects security misconfigurations and vulnerabilities

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

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

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
- 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*

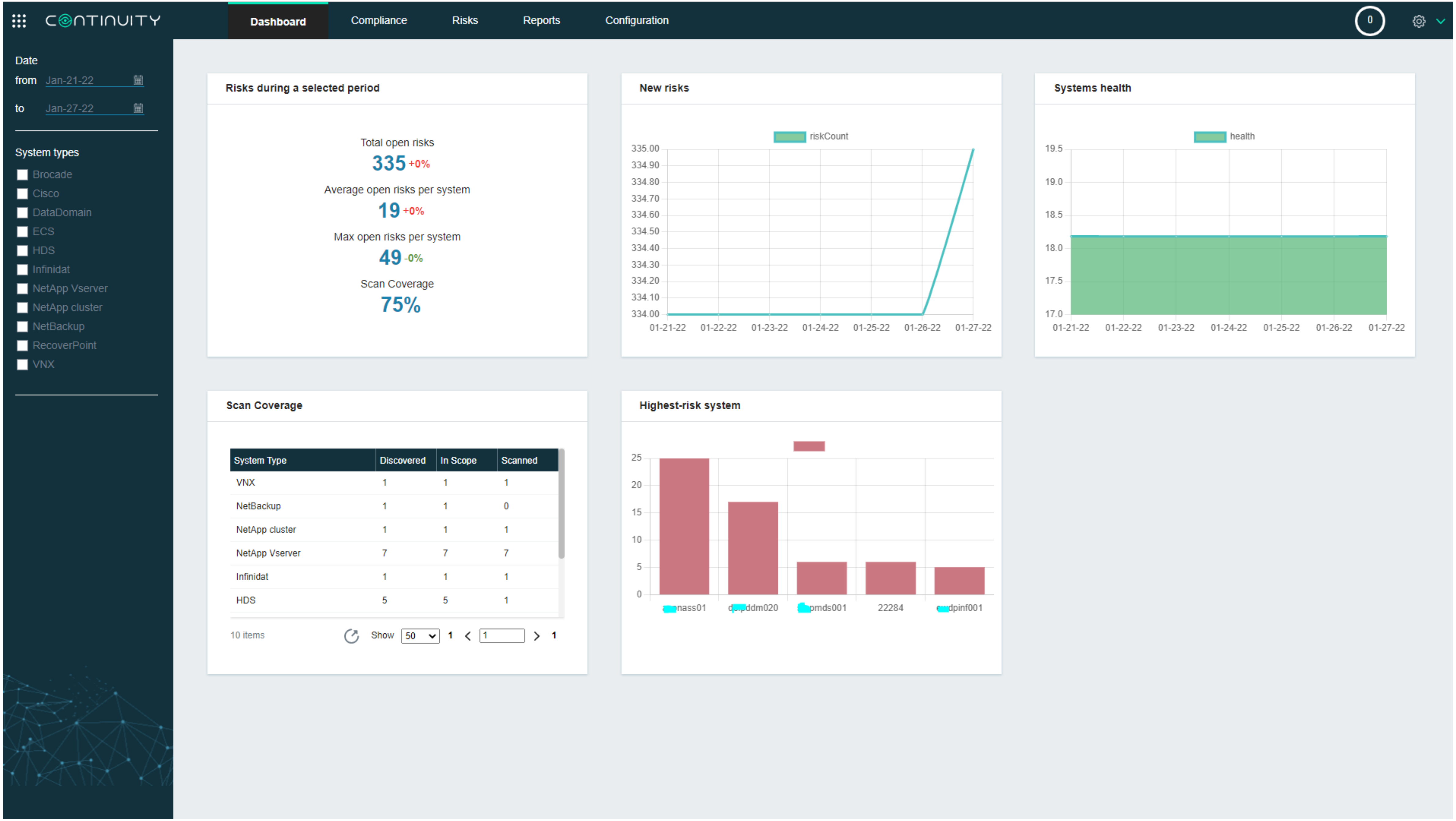
- Amazon Elastic Block Storage • S3 • Glacier
- Azure Blob / Disk Storage
- Nasuni • Zadara
- NetApp Cloud Volumes ONTAP

Storage Management

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

(*) roadmap items

CONTINUITY



Date

from Jan-21-22

to Jan-27-22

System types

- □ Brocade
- □ Cisco
- □ DataDomain
- □ ECS
- □ HDS
- □ Infinidat
- □ NetApp Vserver
- □ NetApp cluster
- □ NetBackup
- □ RecoverPoint
- □ VNX

Risks during a selected period

Total open risks
335 +0%

Average open risks per system
19 +0%

Max open risks per system
49 -0%

Scan Coverage
75%

New risks

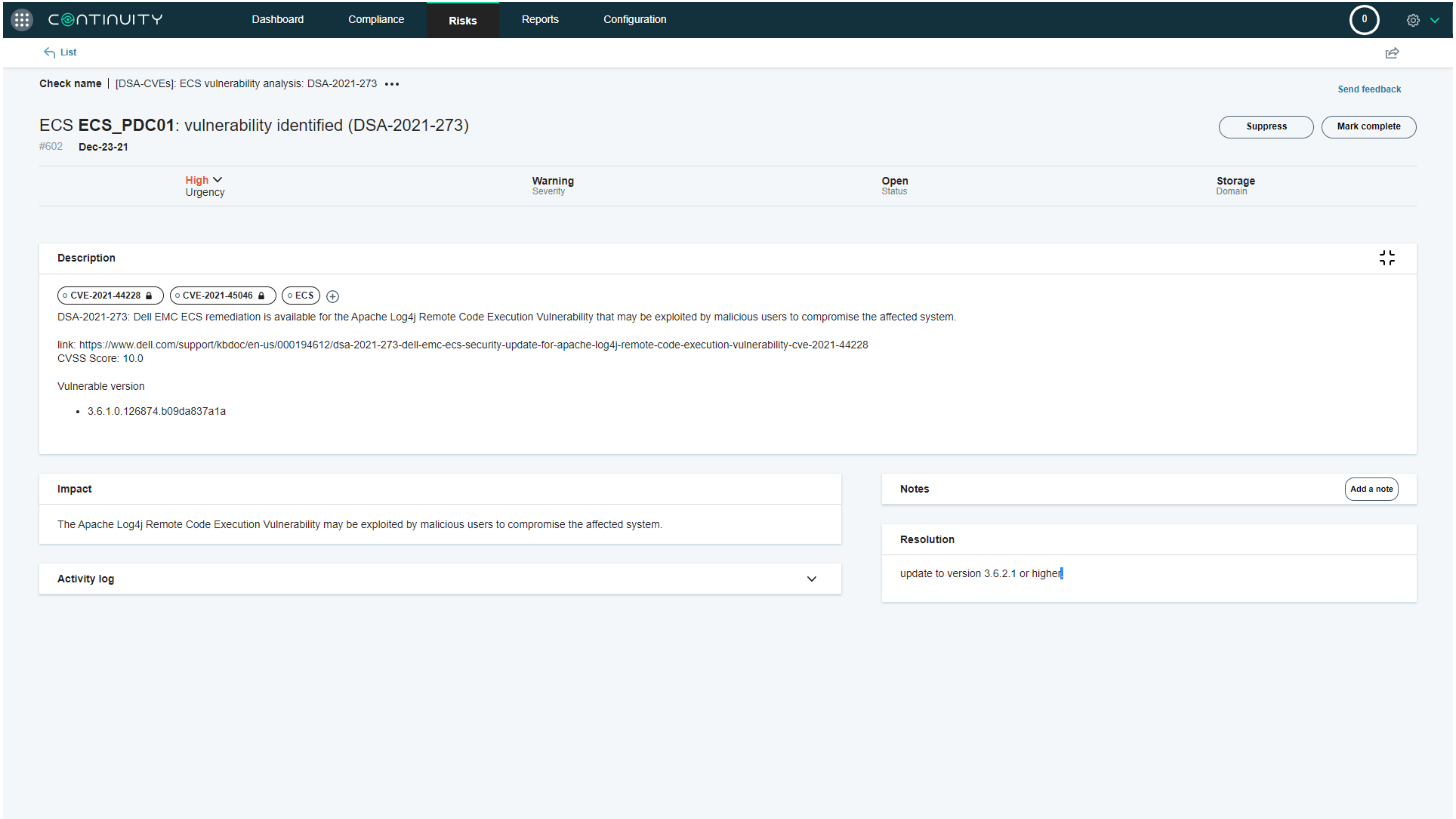
Systems health

Scan Coverage

System Type	Discovered	In Scope	Scanned
VNX	1	1	1
NetBackup	1	1	0
NetApp cluster	1	1	1
NetApp Vserver	7	7	7
Infinidat	1	1	1
HDS	5	5	1

10 items Show 50 1 < 1 > 1

Highest-risk system



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

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

#602 **Dec-23-21**

High Urgency	Warning Severity	Open Status	Storage 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

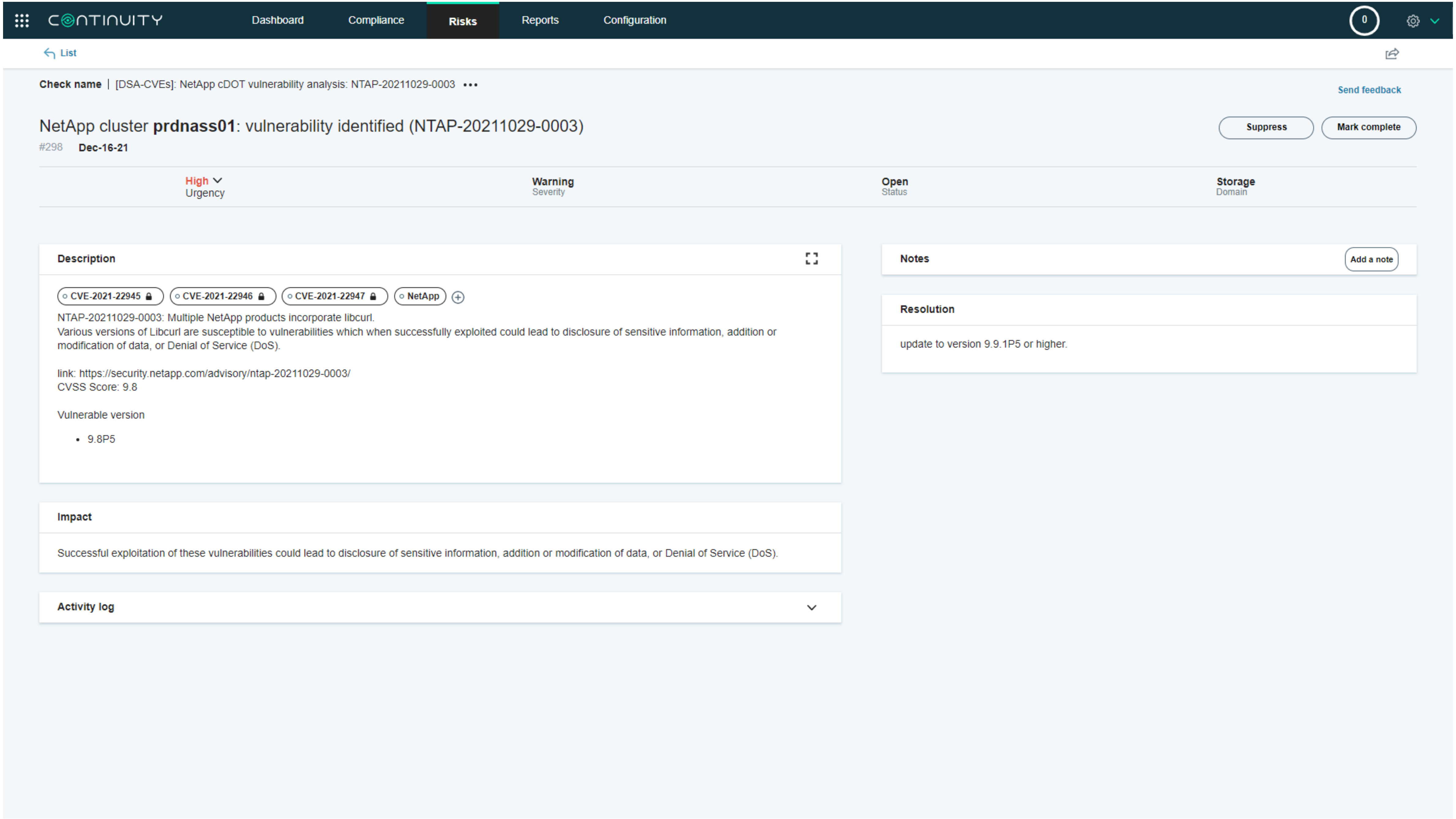
The Apache Log4j Remote Code Execution Vulnerability may be exploited by malicious users to compromise the affected system.

Activity log

Notes

Resolution

update to version 3.6.2.1 or higher



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

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

#298 **Dec-16-21**

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

Notes

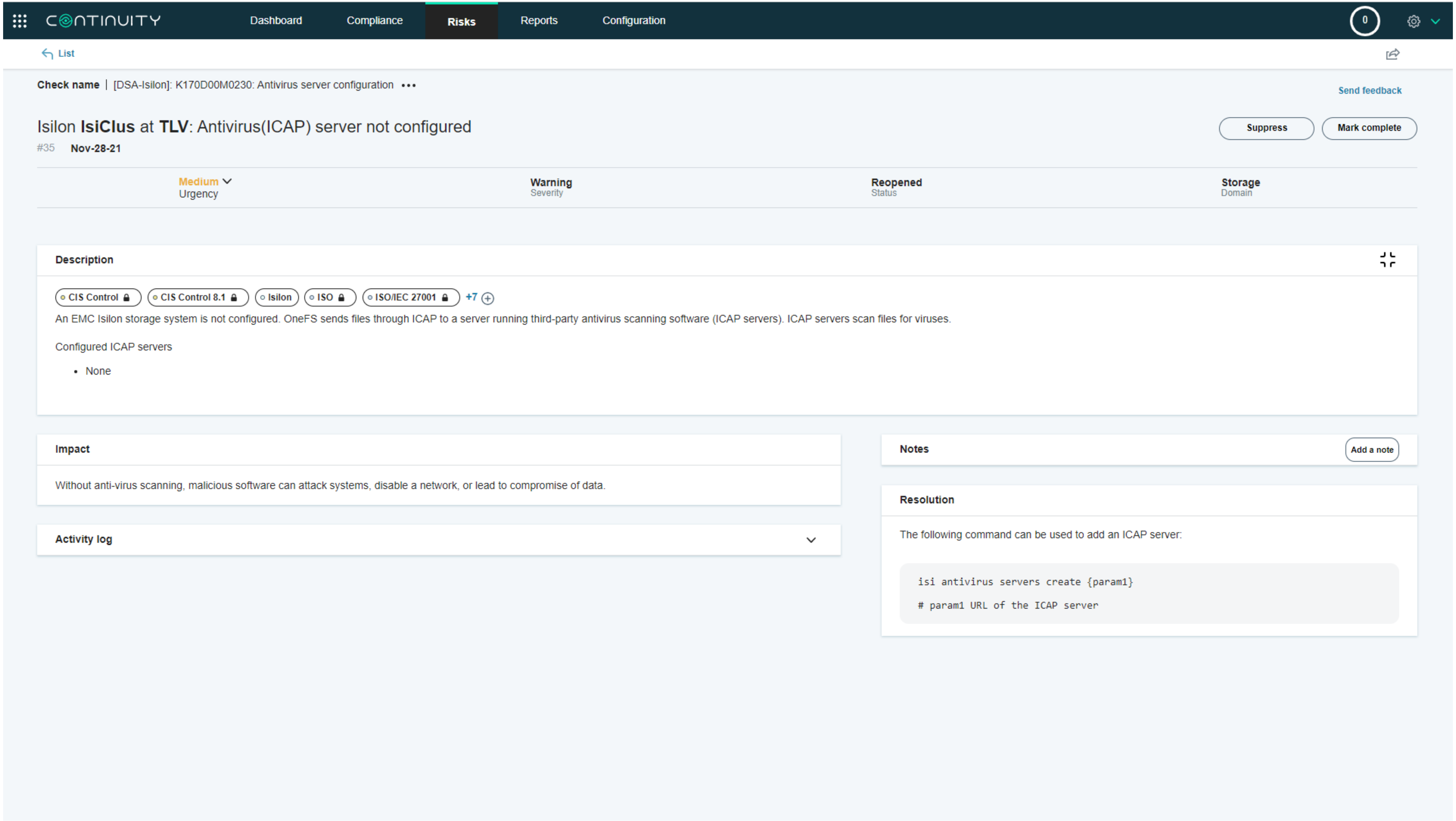
Resolution

update to version 9.9.1P5 or higher.

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



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

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

#35 **Nov-28-21**

Medium Urgency	Warning Severity	Reopened Status	Storage 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

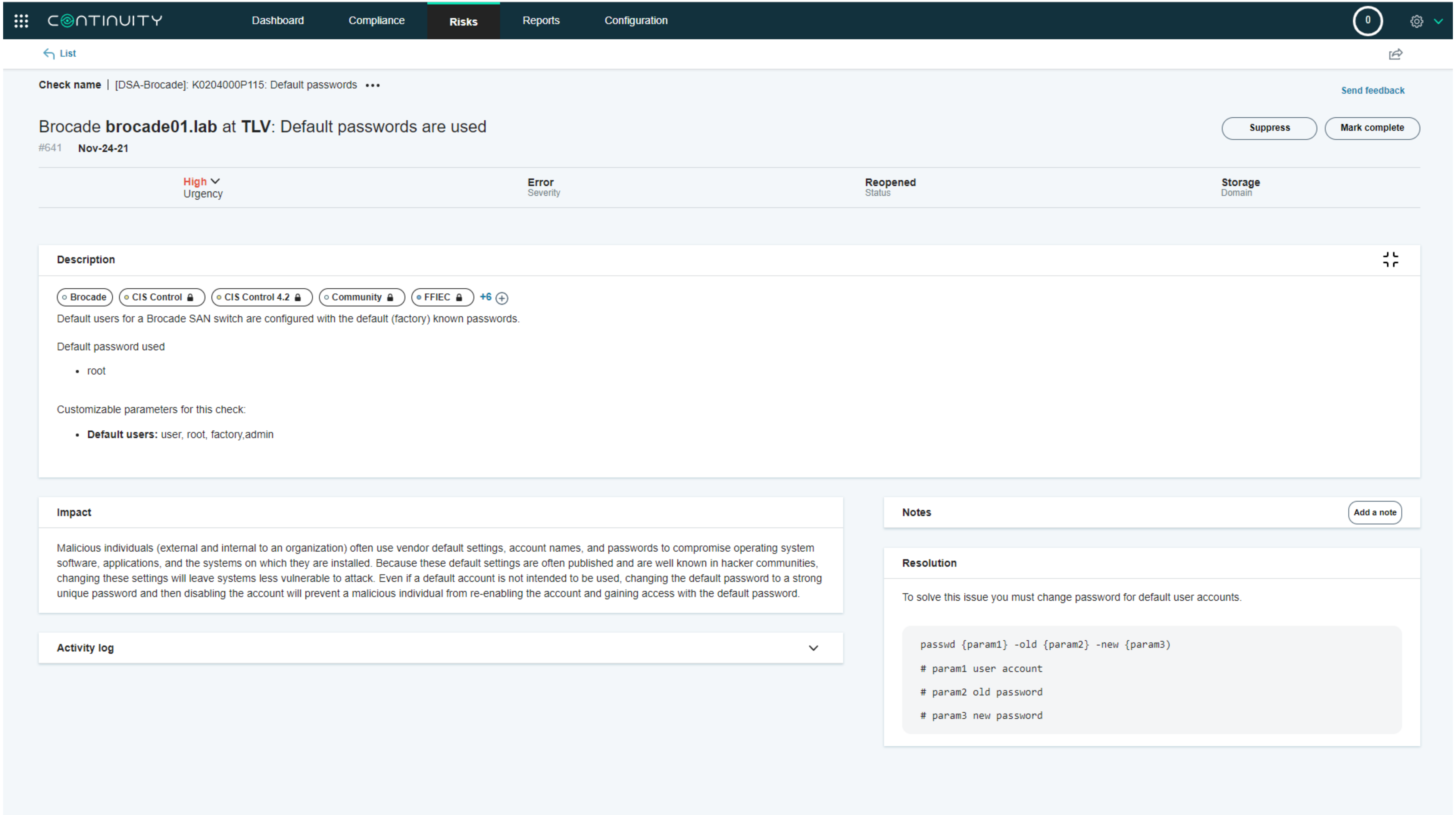
Notes

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 •••

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

#641 **Nov-24-21**

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.

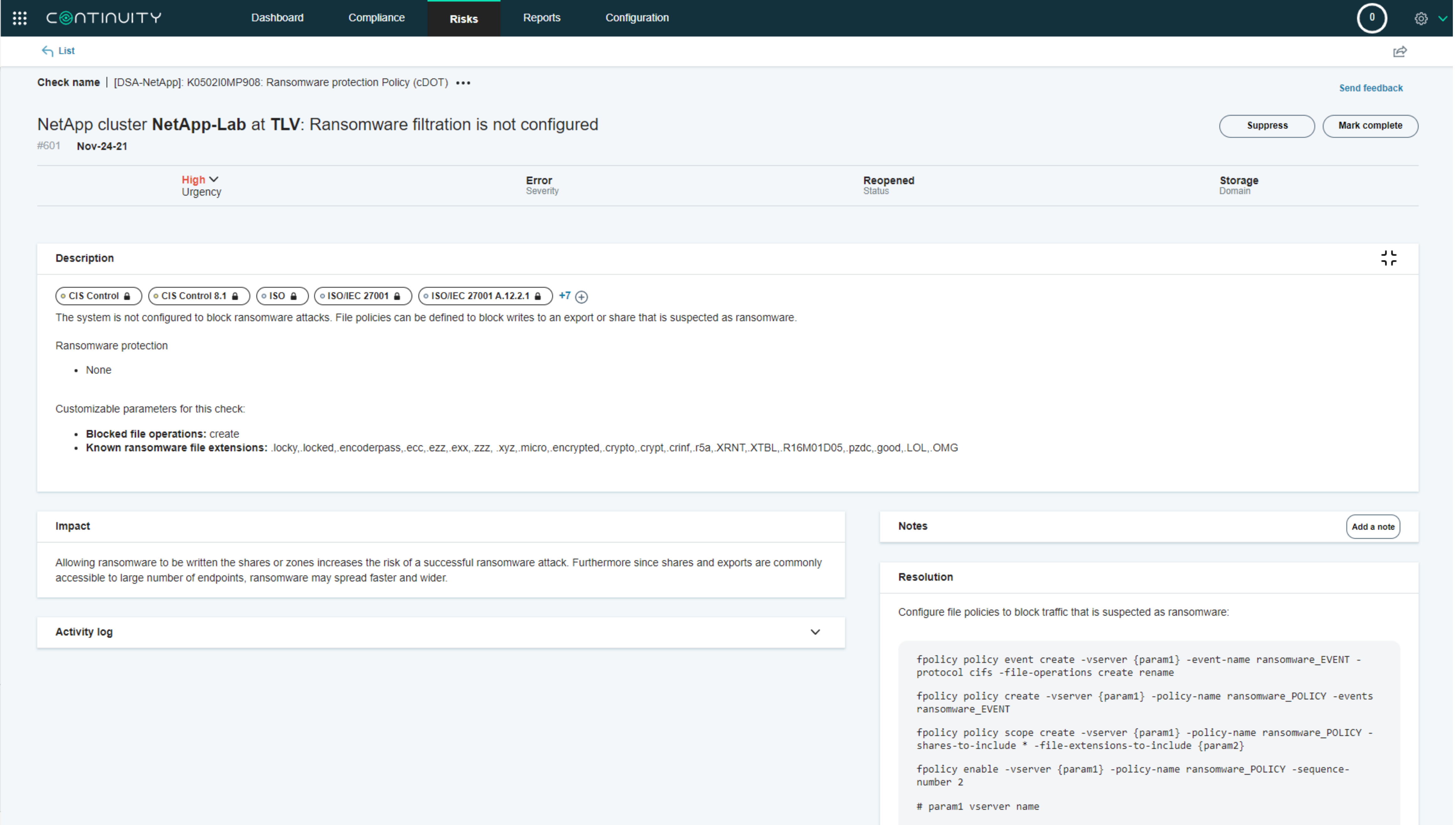
Activity log

Notes

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) •••

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

#601 **Nov-24-21**

High Urgency	**Error** Severity	**Reopened** Status	**Storage** 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

Resolution

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

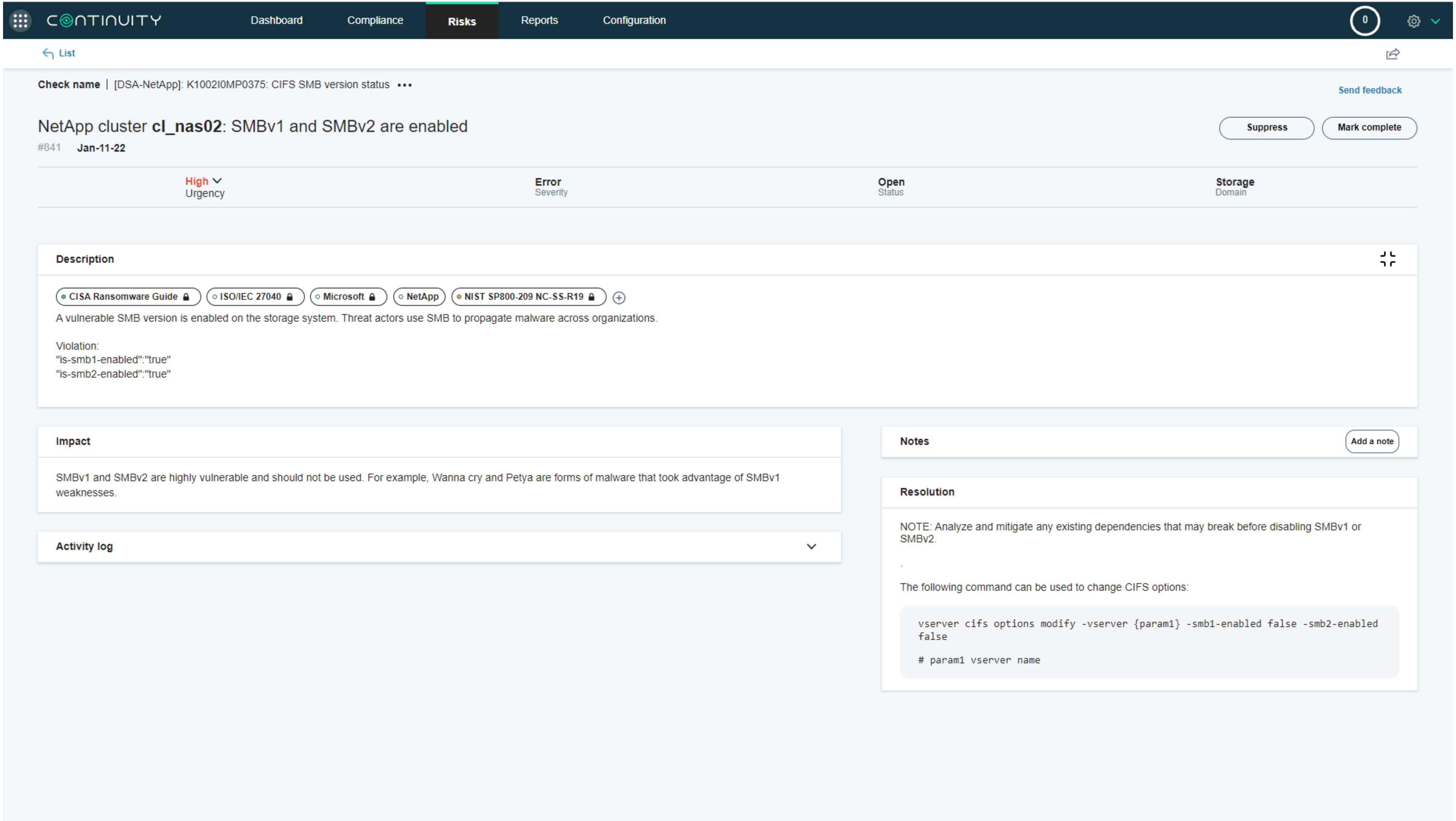
```
fpolicy policy event create -vserver {param1} -event-name ransomware_EVENT -
protocol cifs -file-operations create rename

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 •••

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

#841 **Jan-11-22**

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

Resolution

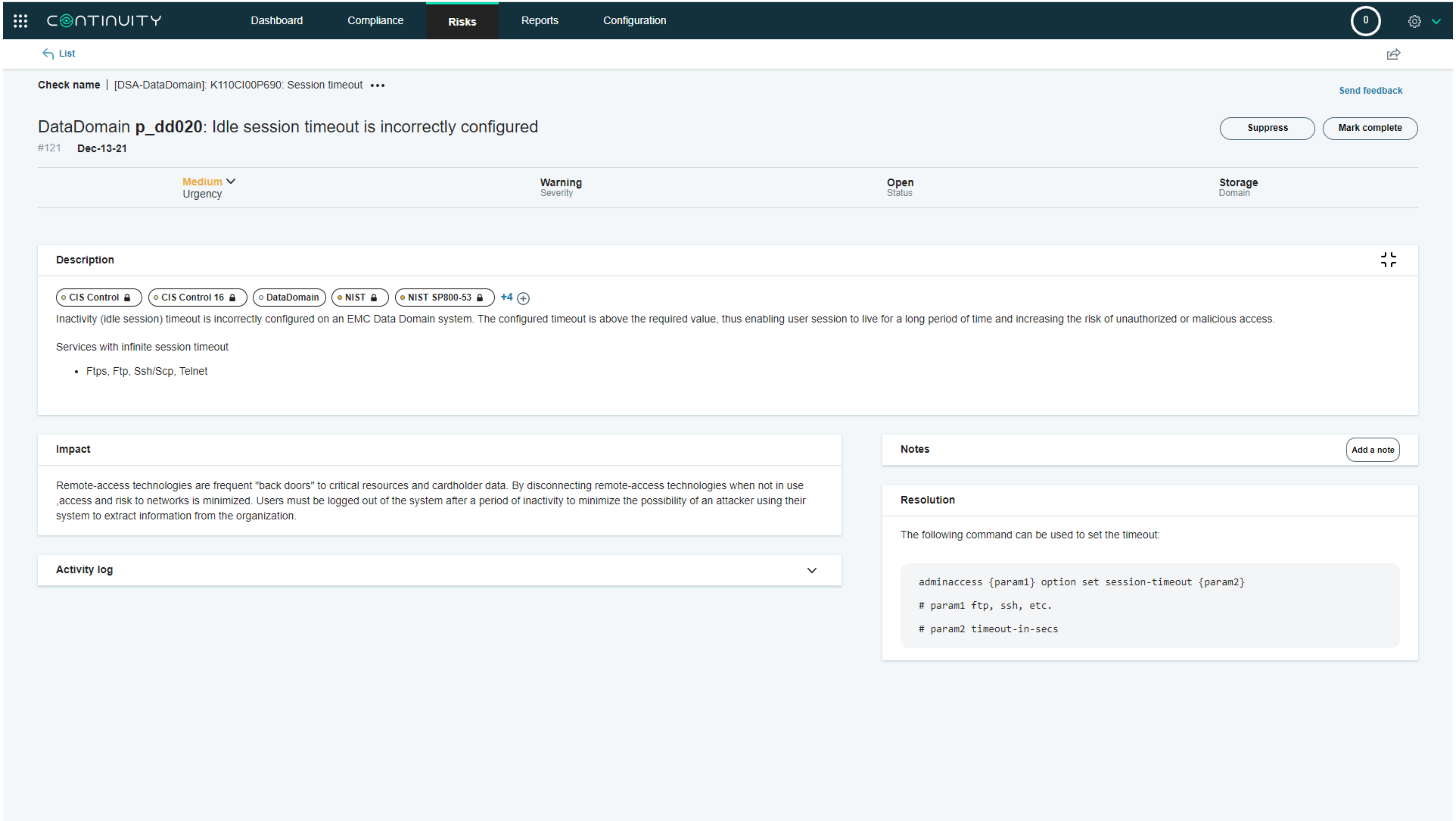
NOTE: Analyze and mitigate any existing dependencies that may break before disabling SMBv1 or SMBv2.

.

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 •••

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

#121 **Dec-13-21**

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

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
```

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

CONTINUITY