SNIA STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Cyber Storage

A little less conversation, a little more action

Doron Pinhas

A SNIA Event

Agenda

- Storage and backup - the last line of defense
- Present-day data threats
- How do storage and backup fit in
- The state of the industry
- What can / should we do?
- Summary and further resources
- Q&A

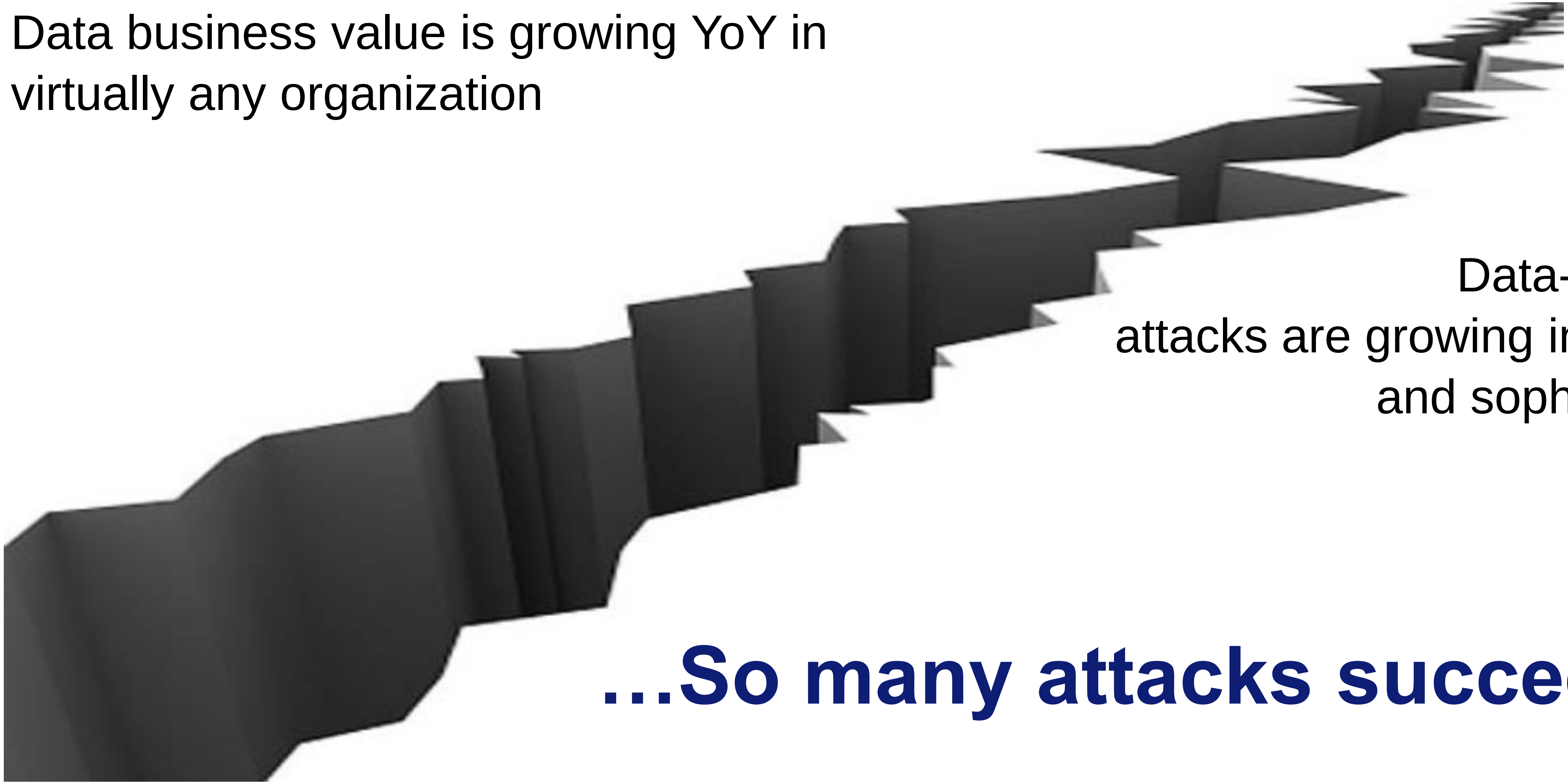
©2022 Storage Networking Industry Association. All Rights Reserved.

Storage and backup - the last line of defense

When data does get compromised…

The unspoken gap

Data business value is growing YoY in virtually any organization

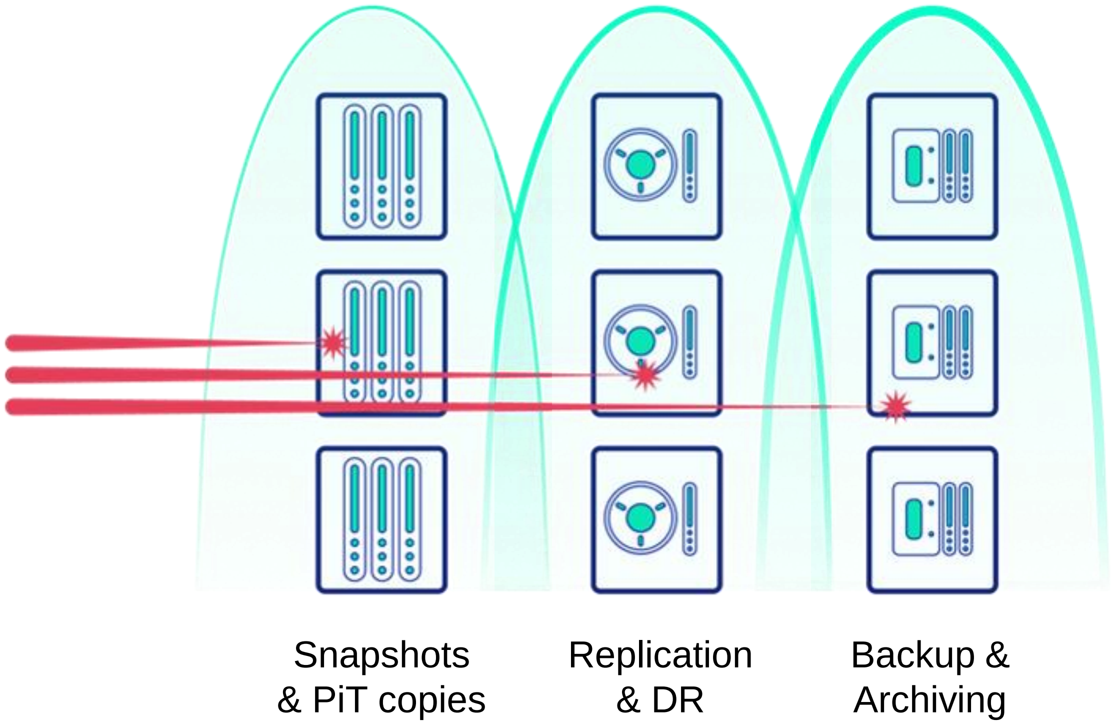


Data-centered
attacks are growing in number
and sophistication

…So many attacks succeed

Threat landscape is shifting – data is the prime target

- A successful attack is a question of “when”, not “if”
- Recovery of your data is **only possible** through the storage and backup layers



©2022 Storage Networking Industry Association. All Rights Reserved.

Present-day data threats

Bird’s-eye view

1) Data exfiltration

- Motivations: monetary, political, …
- Direct damaged: ransom, extortion, damage to public image, regulatory fines
- Harvesting of the data could yield secondary damages:
  - Access to privileged financial records or your users, customers, and ecosystem
  - Influence decisions, public opinions, market sentiments
  - Compromise or neutralize assets

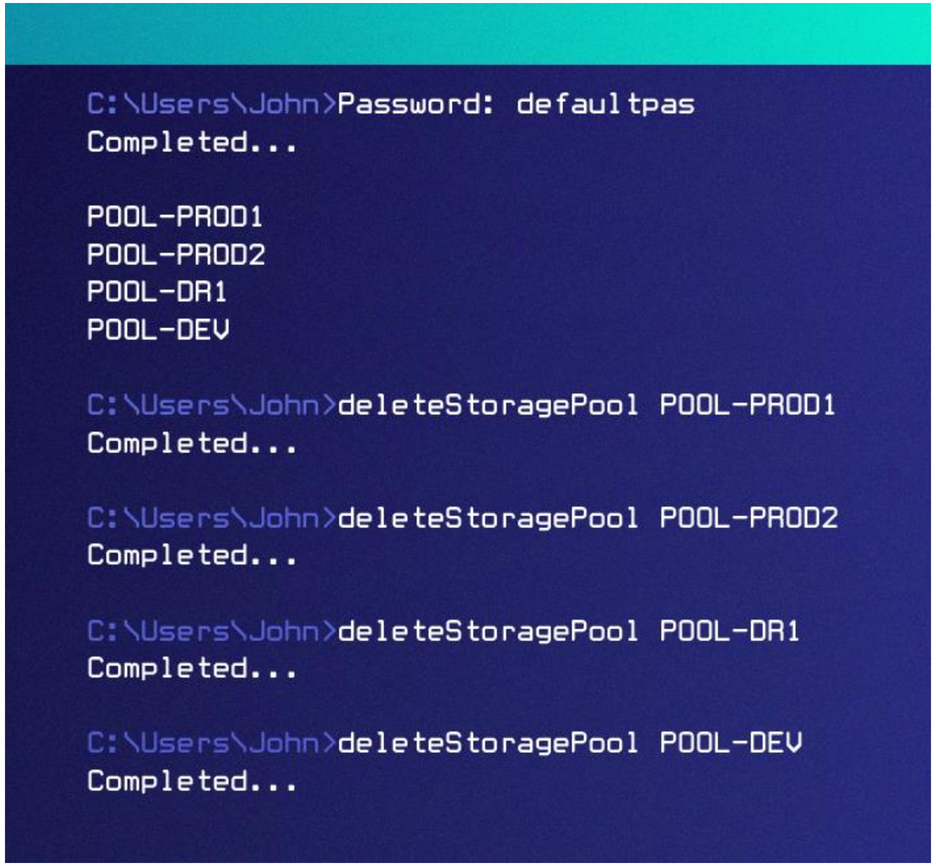
The data is corrupted

The only available files are more than 90 days old

©2022 Storage Networking Industry Association. All Rights Reserved.

2) Ransomware and data destruction

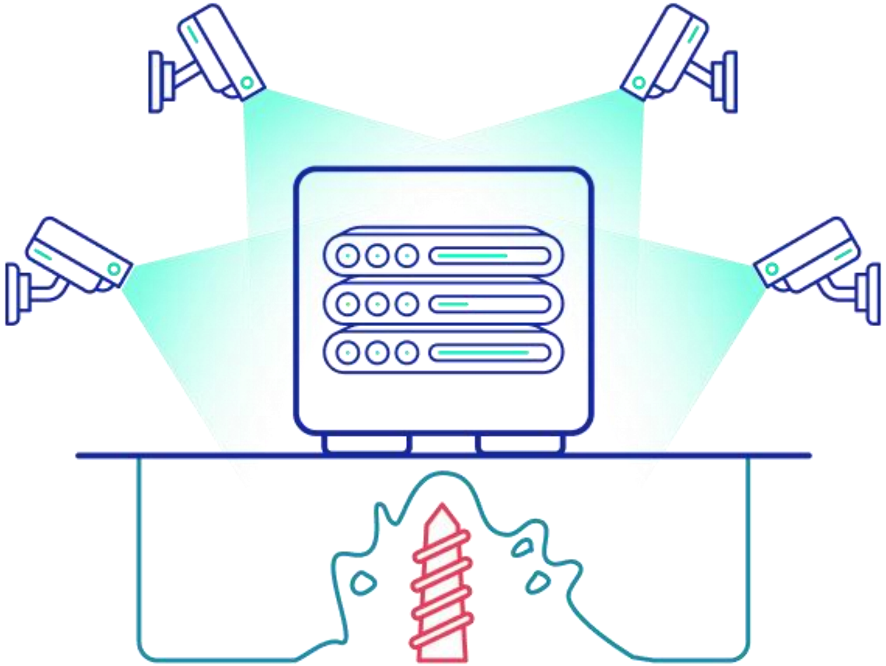
- For ransom or sabotage
- Emerging as the new norm:
  - Prevent restoration by attacking backup
  - “Double extortion”
    - Also use exfiltration to threat leaking sensitive data if ransom is not paid



```
C:\Users\John>Password: defaultpas
Completed...

POOL-PROD1
POOL-PROD2
POOL-DR1
POOL-DEV

C:\Users\John>deleteStoragePool POOL-PROD1
Completed...

C:\Users\John>deleteStoragePool POOL-PROD2
Completed...

C:\Users\John>deleteStoragePool POOL-DR1
Completed...

C:\Users\John>deleteStoragePool POOL-DEV
Completed...
```

3) Data alteration

- Modify sensitive records
  - To gain access to funds, commit fraud
  - To do, or threat doing harm (people, organizations, resources, nation-states, …)
  - To influence your ecosystem
    - Using your organization’s trust and supply-chain dependencies to attack others



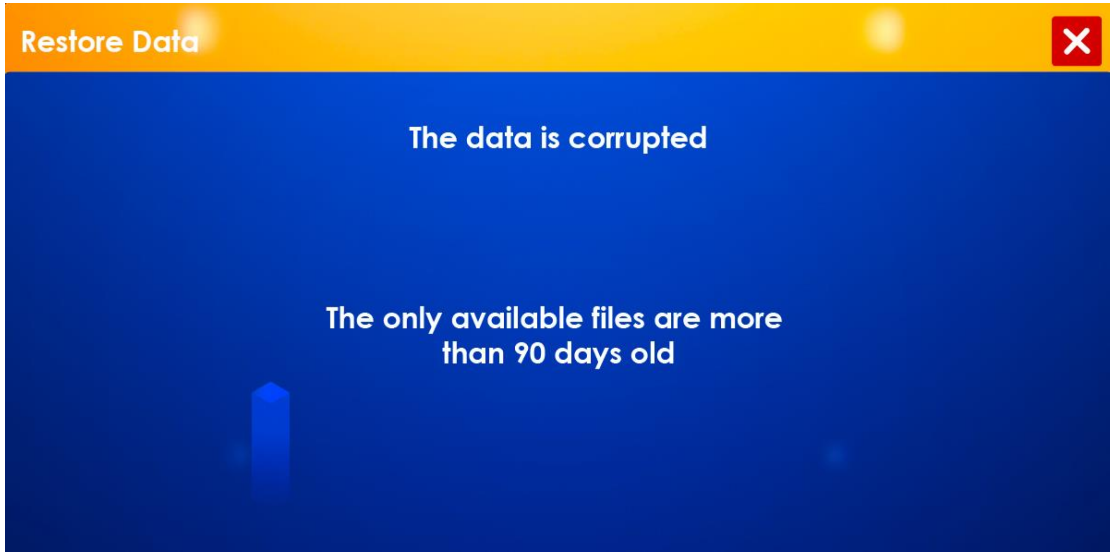
©2022 Storage Networking Industry Association. All Rights Reserved.

How do storage and backup fit in?

Insecure storage & backup
=
adversary's treasure trove

1) Data exfiltration

- Untracked copies all over – often in insecure environments
- When storage and backup are not hardened:
  - Data can be exfiltrated “out-of-band”
    - Raising no alarms
  - They can become part of the kill chain
    - E.g., alter an existing backup job to include desired data, and ship it to an insecure cloud account

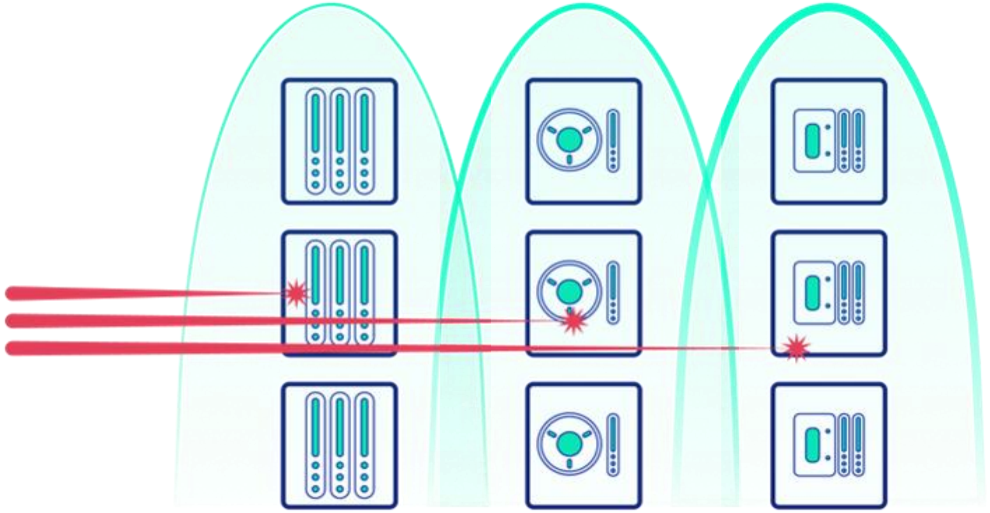


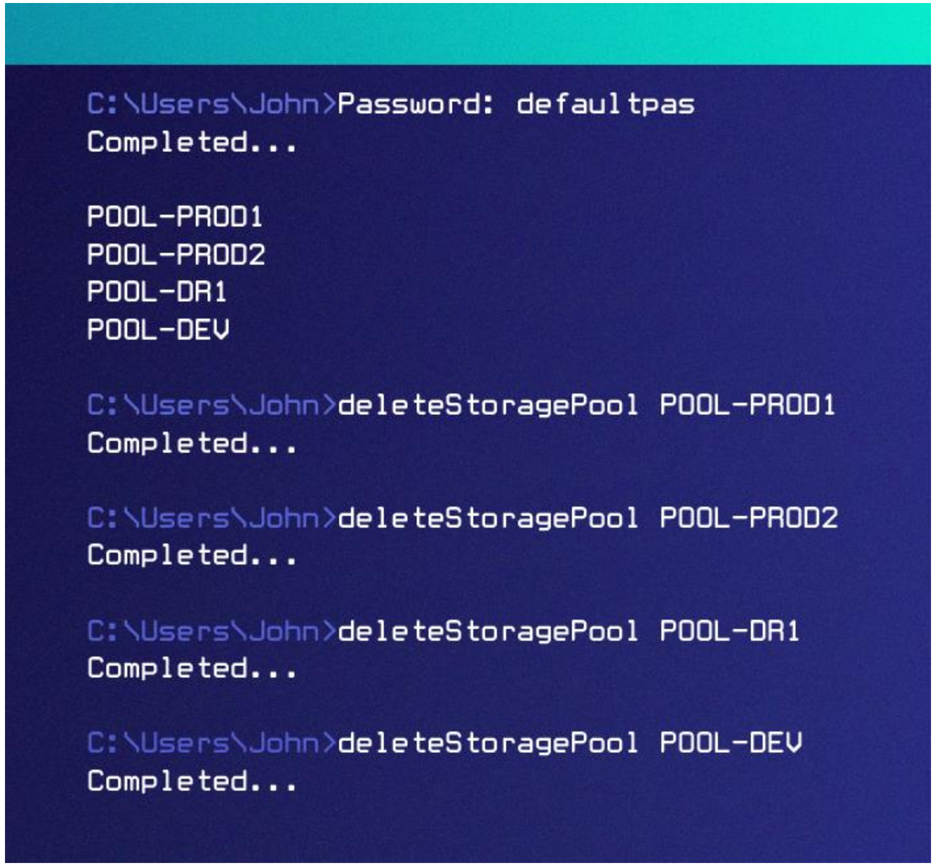
The data is corrupted

The only available files are more than 90 days old

2) Ransomware and data destruction

- As mentioned, adversaries go after your backups!

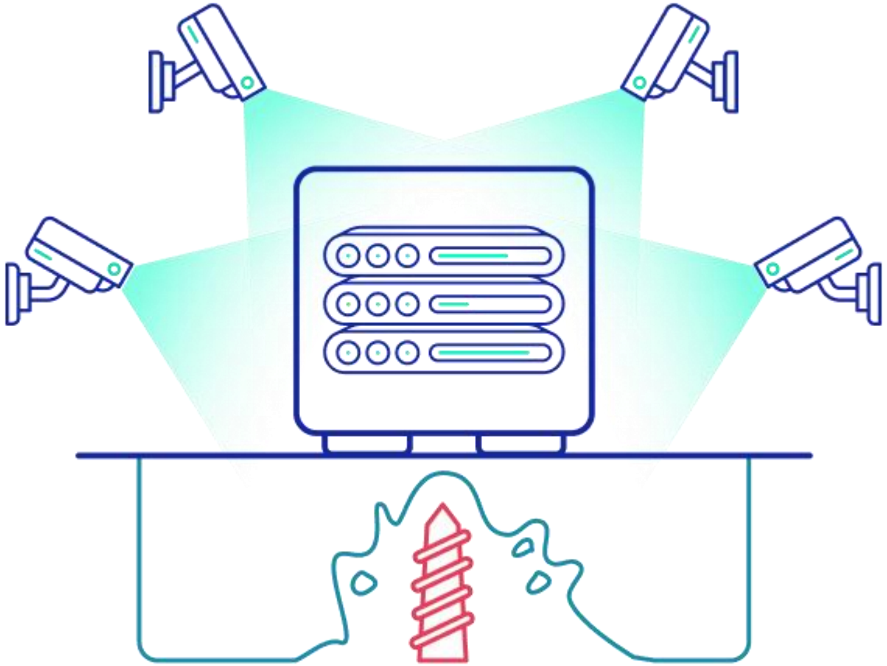




```
C:\Users\John>Password: defaultpas
Completed...

POOL-PROD1
POOL-PROD2
POOL-DR1
POOL-DEV

C:\Users\John>deleteStoragePool POOL-PROD1
Completed...

C:\Users\John>deleteStoragePool POOL-PROD2
Completed...

C:\Users\John>deleteStoragePool POOL-DR1
Completed...

C:\Users\John>deleteStoragePool POOL-DEV
Completed...
```

3) Data alteration

- Not a current focus of hackers, but can easily change
- Without proper hardening of storage & backup
  - Adversaries can exploit infrastructure to gain direct access to data
  - Bypassing existing security layers, leaving little or no trace



Conclusions and observations

- Storage and backup systems:
  - Are the only layer of IT not covered by Vulnerability Management solutions
  - Often left out of Incident Response Plans
  - Must be hardened

The state of the industry

Results from a 2021 survey

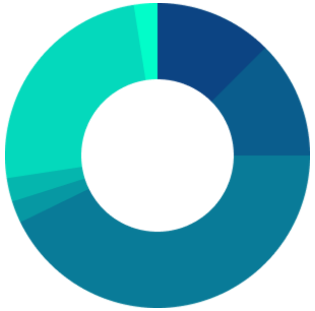
6,300
security issues detected

An enterprise storage device has **15** vulnerabilities

Out of **15** vulnerabilities, **3** are high or critical risk

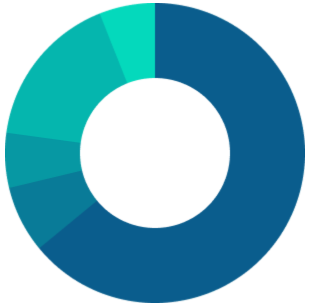
Demographics

Storage Vendor



12%	Brocade
12%	Cisco
42%	Dell EMC
3%	Hitachi Vantara
3%	IBM
25%	NetApp
3%	Other

Industry



62%	Banking
10%	Healthcare
5%	Telecommunication
18%	Transportation
5%	Other

6,300

security issues detected

An enterprise storage device has 15 vulnerabilities

Out of 15 vulnerabilities, 3 are high or critical risk

most frequent issues

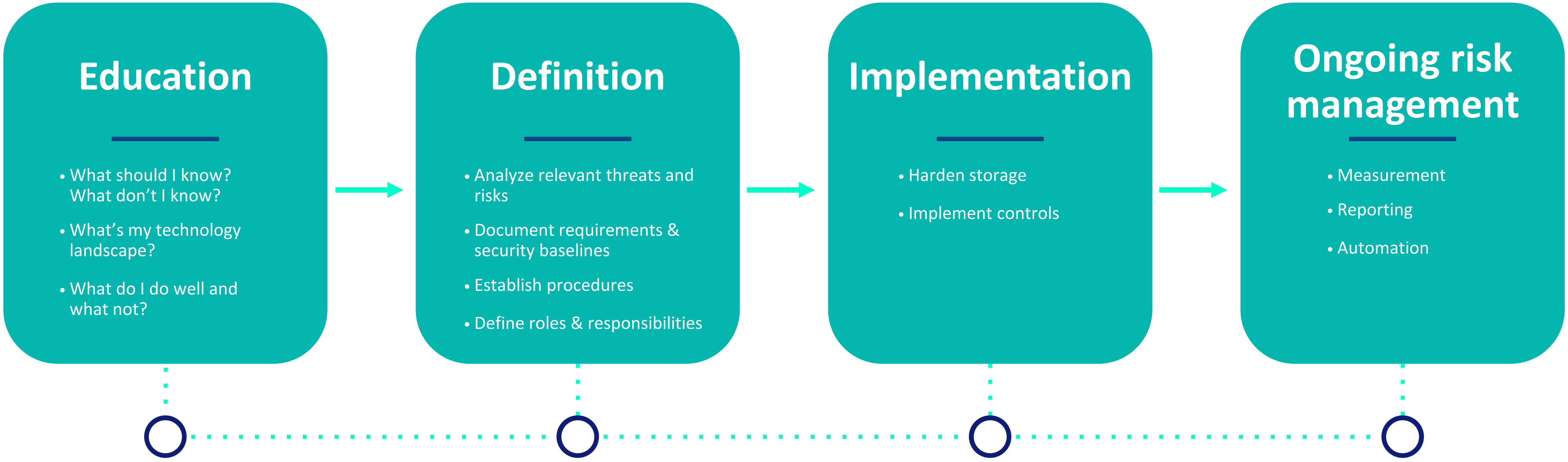
1. Use of vulnerable protocols / protocol settings
2. Unaddressed CVEs
3. Access rights issues (over exposure)
4. Insecure user management and authentication
5. Insufficient logging

most "lethal" issues

1. Incorrect use of ransomware-protection features
2. Undocumented and insecure API / CLI
3. Vulnerabilities and oversight in storage software supply-chain management

What should you do now?

Developing a Program for Storage & Backup Security



Education

- What should I know? What don't I know?
- What's my technology landscape?
- What do I do well and what not?

Definition

- Analyze relevant threats and risks
- Document requirements & security baselines
- Establish procedures
- Define roles & responsibilities

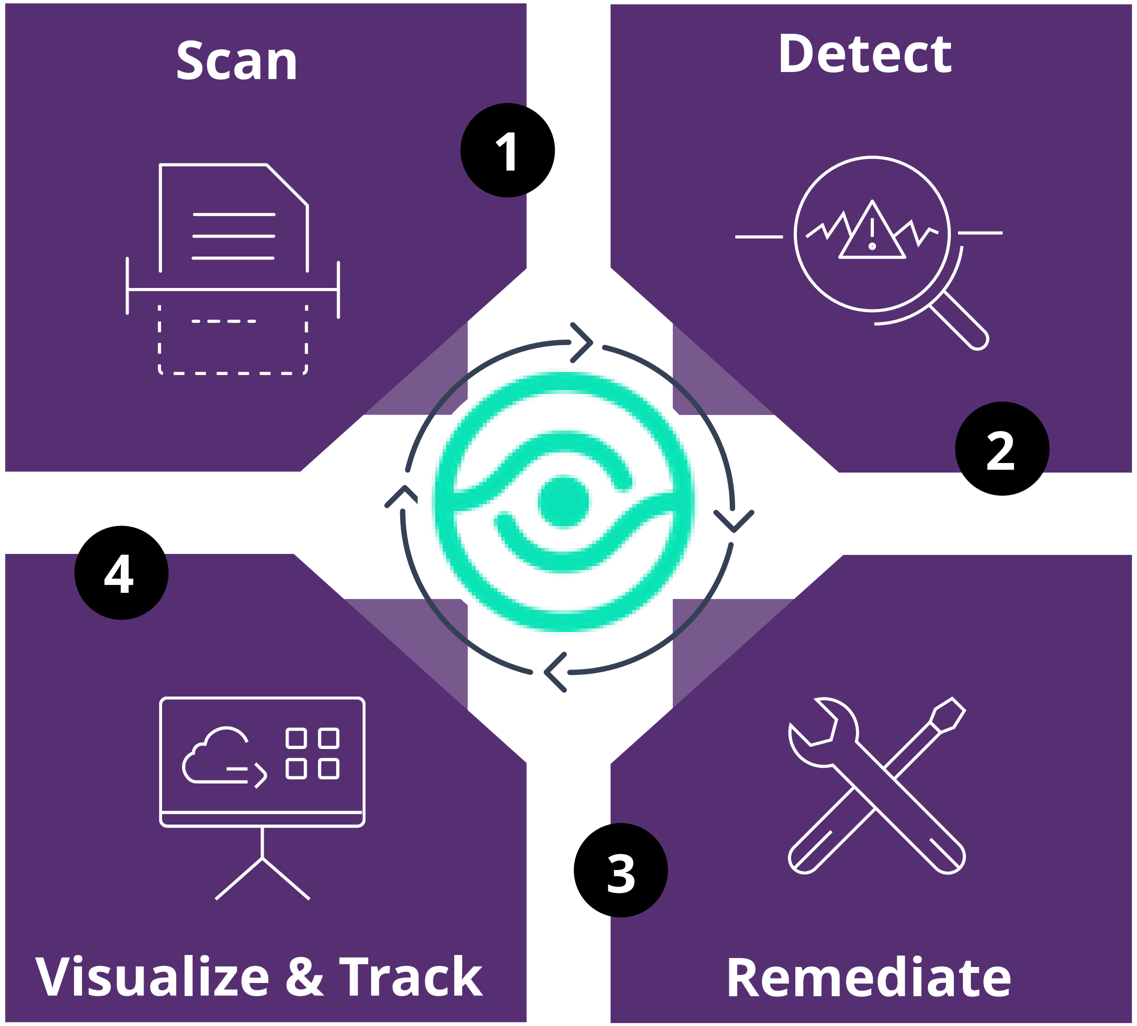
Implementation

- Harden storage
- Implement controls

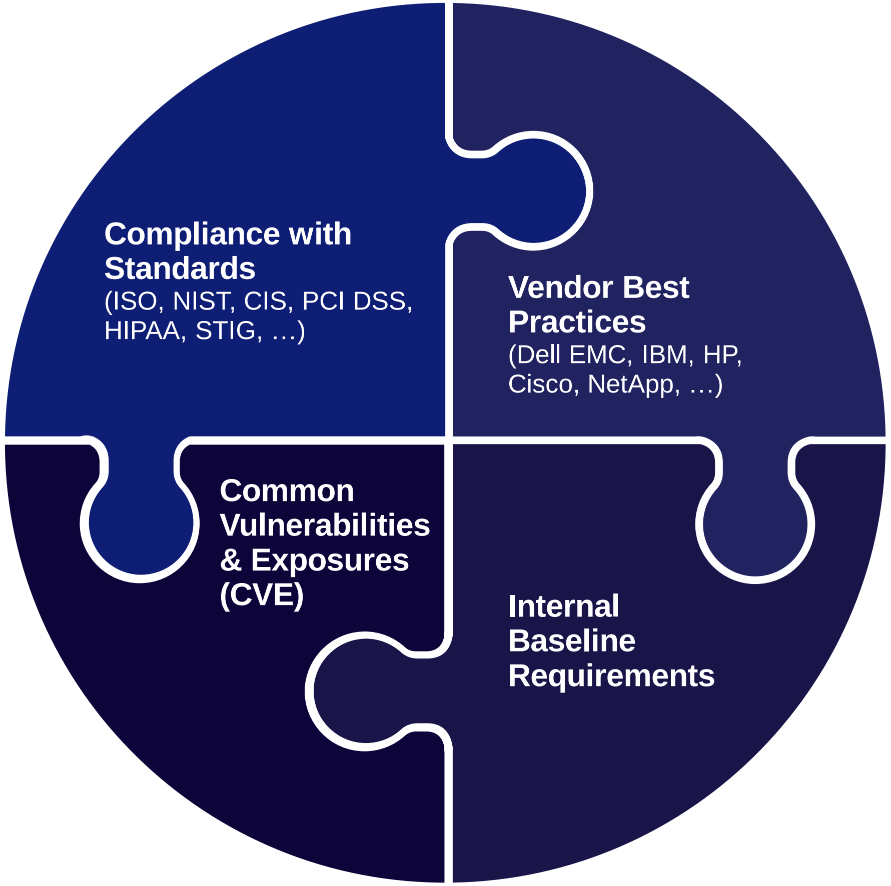
Ongoing risk management

- Measurement
- Reporting
- Automation

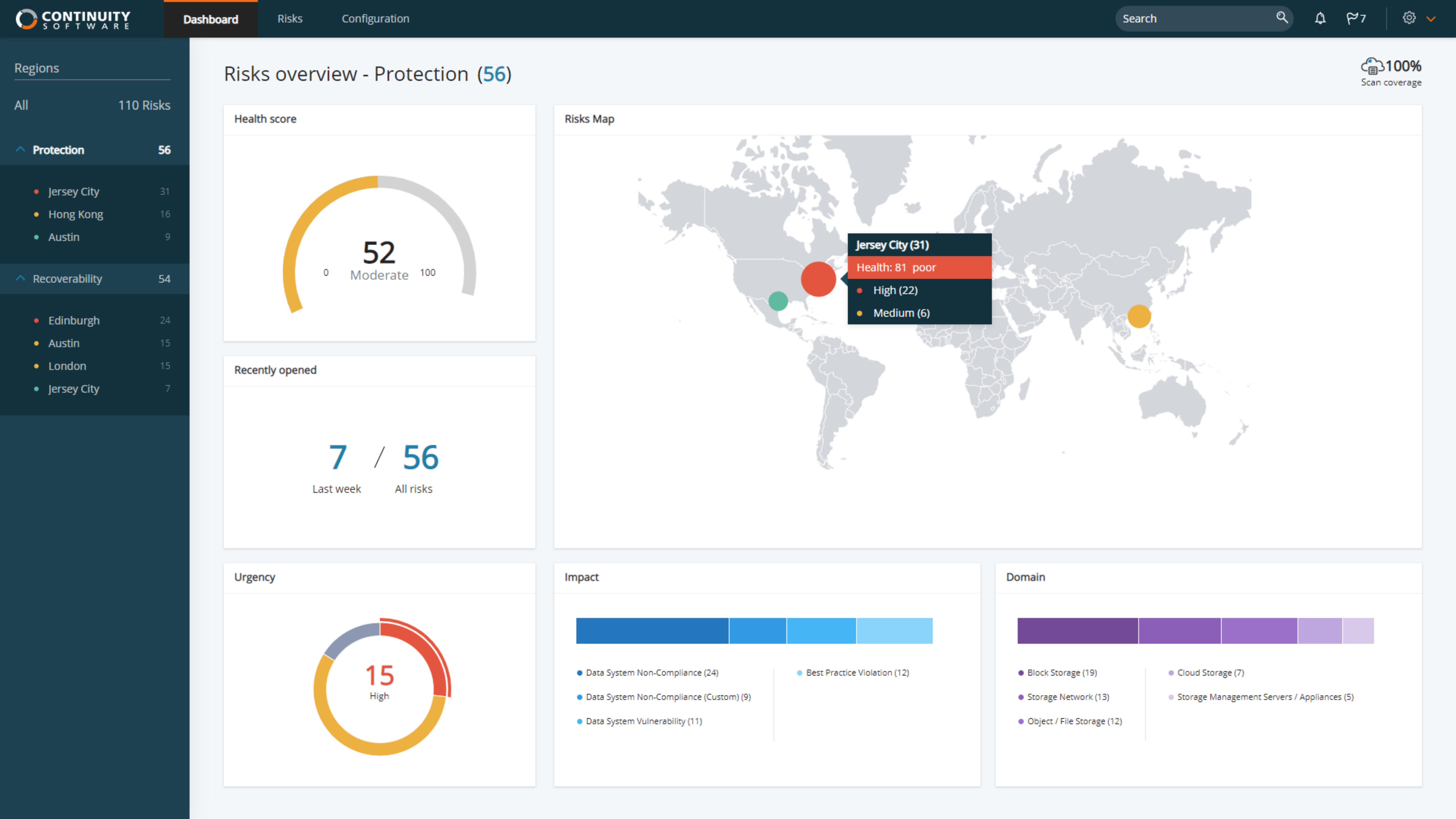
Introducing StorageGuard



The StorageGuard Knowledge Base


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

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



Regions

All	110 Risks
Protection	56
● Jersey City	31
● Hong Kong	16
● Austin	9
Recoverability	54
● Edinburgh	24
● Austin	15
● London	15
● Jersey City	7

Risks overview - Protection (56)

100%
Scan coverage

Health score

Risks Map

Jersey City (31)
Health: 81 poor
● High (22)
● Medium (6)

Recently opened

7 / 56
Last week All risks

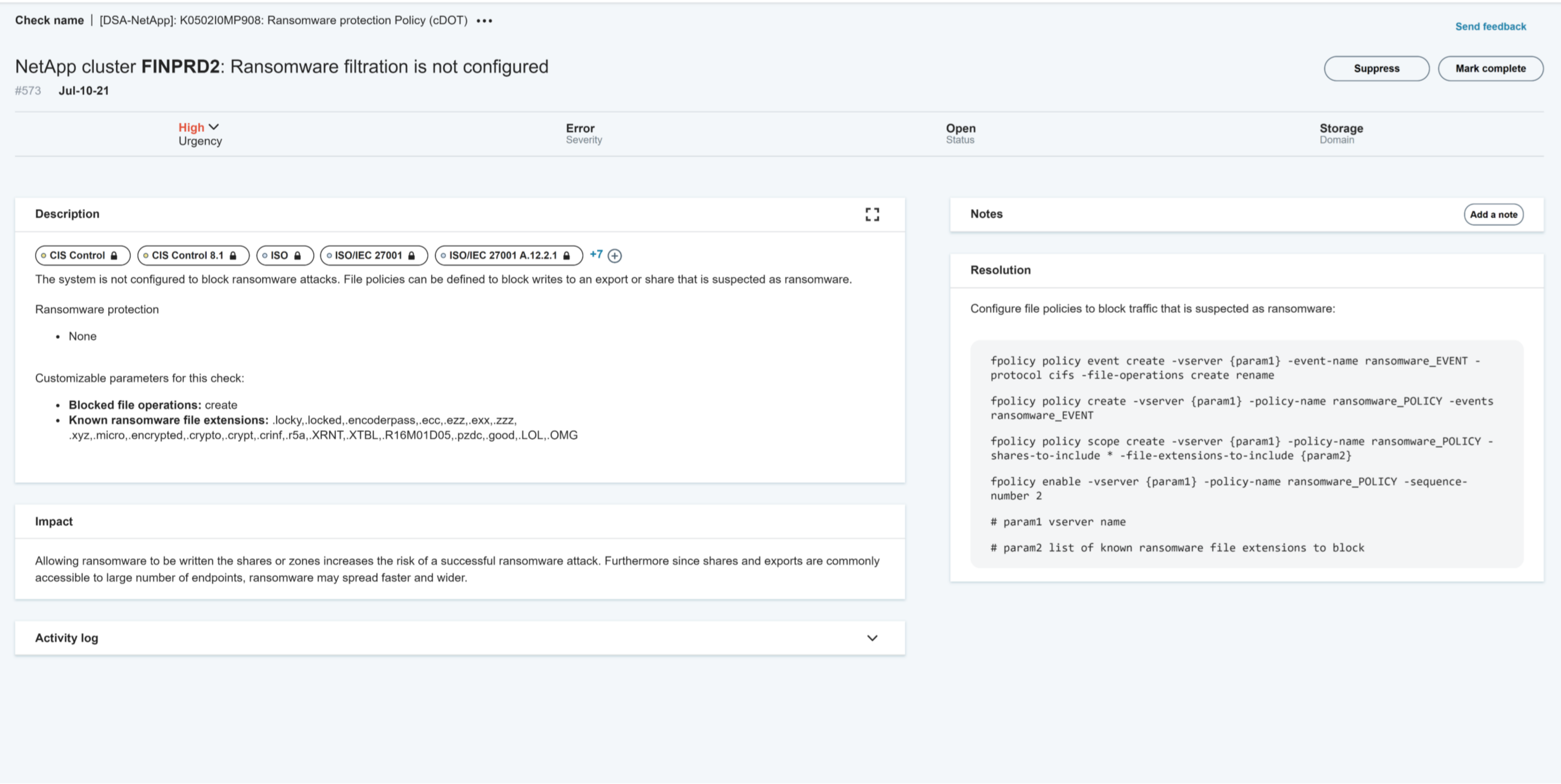
Urgency

Impact

- ● Data System Non-Compliance (24)
- ● Data System Non-Compliance (Custom) (9)
- ● Data System Vulnerability (11)
- ● Best Practice Violation (12)

Domain

- ● Block Storage (19)
- ● Storage Network (13)
- ● Object / File Storage (12)
- ● Cloud Storage (7)
- ● Storage Management Servers / Appliances (5)



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

NetApp cluster **FINPRD2**: Ransomware filtration is not configured

#573 **Jul-10-21**

High	**Error**	**Open**	**Storage**
Urgency	Severity	Status	Domain

Description

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.

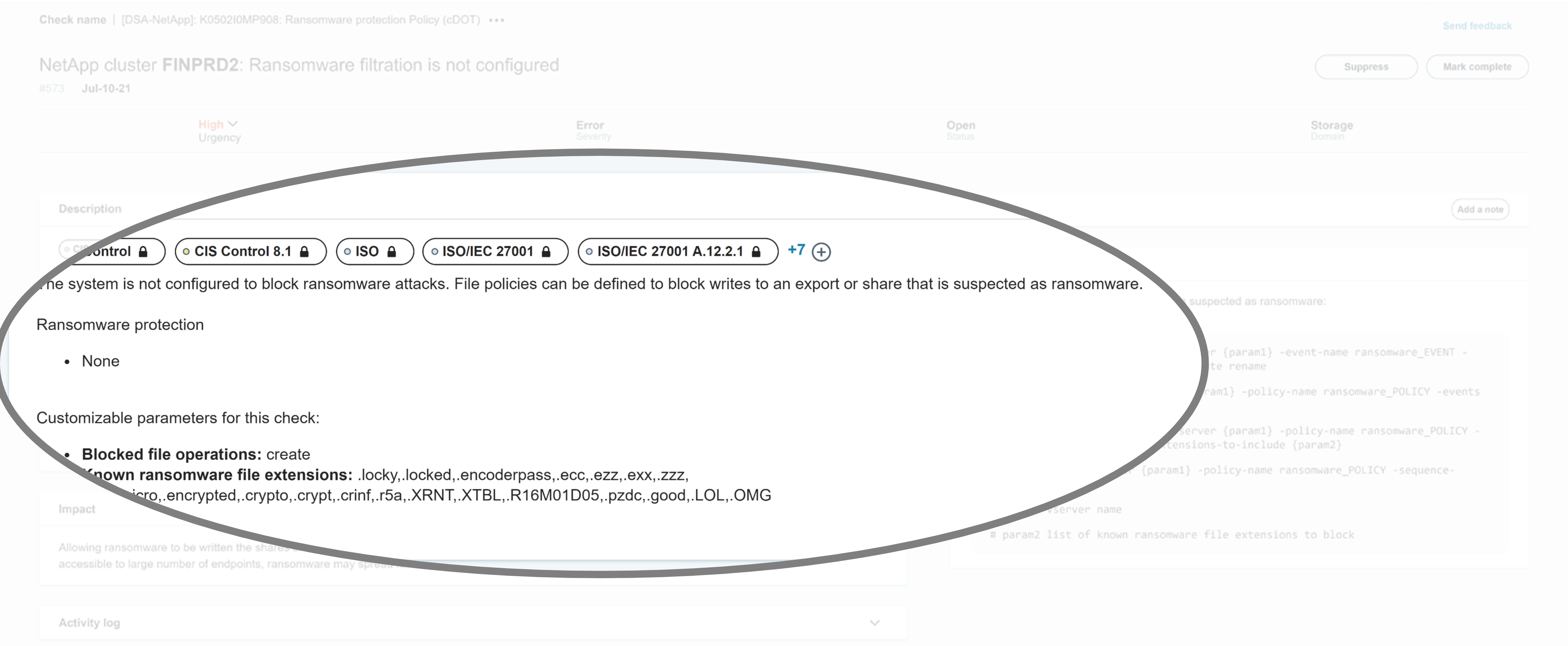
Activity log

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

# param2 list of known ransomware file extensions to block
```



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

NetApp cluster **FINPRD2**: Ransomware filtration is not configured

#573 Jul-10-21

High Urgency	Error Severity	Open 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:

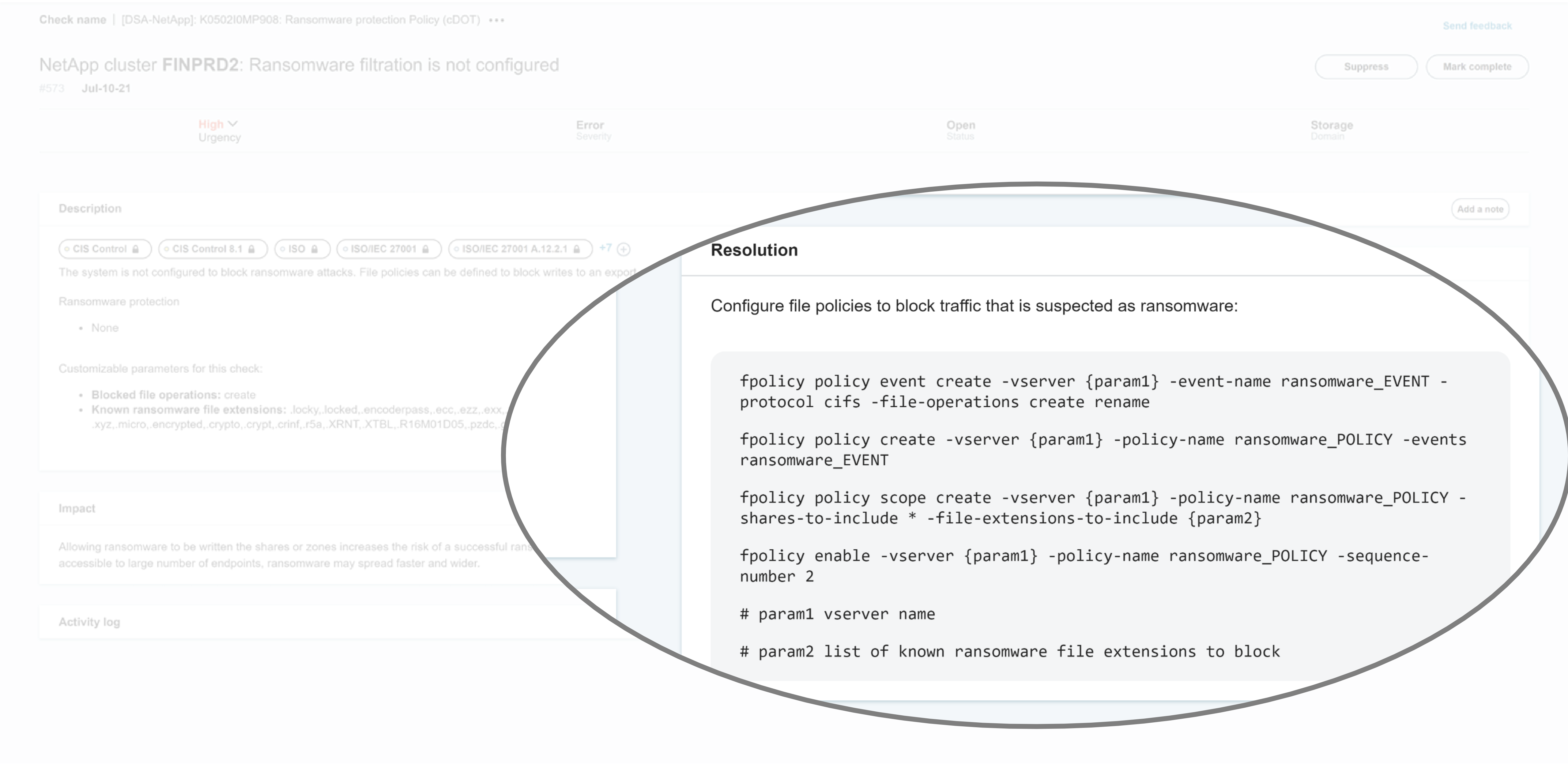
- **Blocked file operations:** create
- **Known ransomware file extensions:** .locky,.locked,.encoderpass,.ecc,.ezz,.exx,.zzz,
  ...icro,.encrypted,.crypto,.crypt,.crinf,.r5a,.XRNT,.XTBL,.R16M01D05,.pzdc,.good,.LOL,.OMG

suspected as ransomware:

```
r {param1} -event-name ransomware_EVENT -
te rename

ram1} -policy-name ransomware_POLICY -events

server {param1} -policy-name ransomware_POLICY -
tensions-to-include {param2}

r {param1} -policy-name ransomware_POLICY -sequence-

vserver name

# param2 list of known ransomware file extensions to block
```

Impact

Allowing ransomware to be written the shares ...
accessible to large number of endpoints, ransomware may spread ...



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

NetApp cluster **FINPRD2**: Ransomware filtration is not configured

#573 **Jul-10-21**

High Urgency | Error Severity | Open Status | Storage Domain

Description

The system is not configured to block ransomware attacks. File policies can be defined to block writes to an export

Ransomware protection

- None

Customizable parameters for this check:

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

Impact

Allowing ransomware to be written the shares or zones increases the risk of a successful rans accessible to large number of endpoints, ransomware may spread faster and wider.

Activity log

Resolution

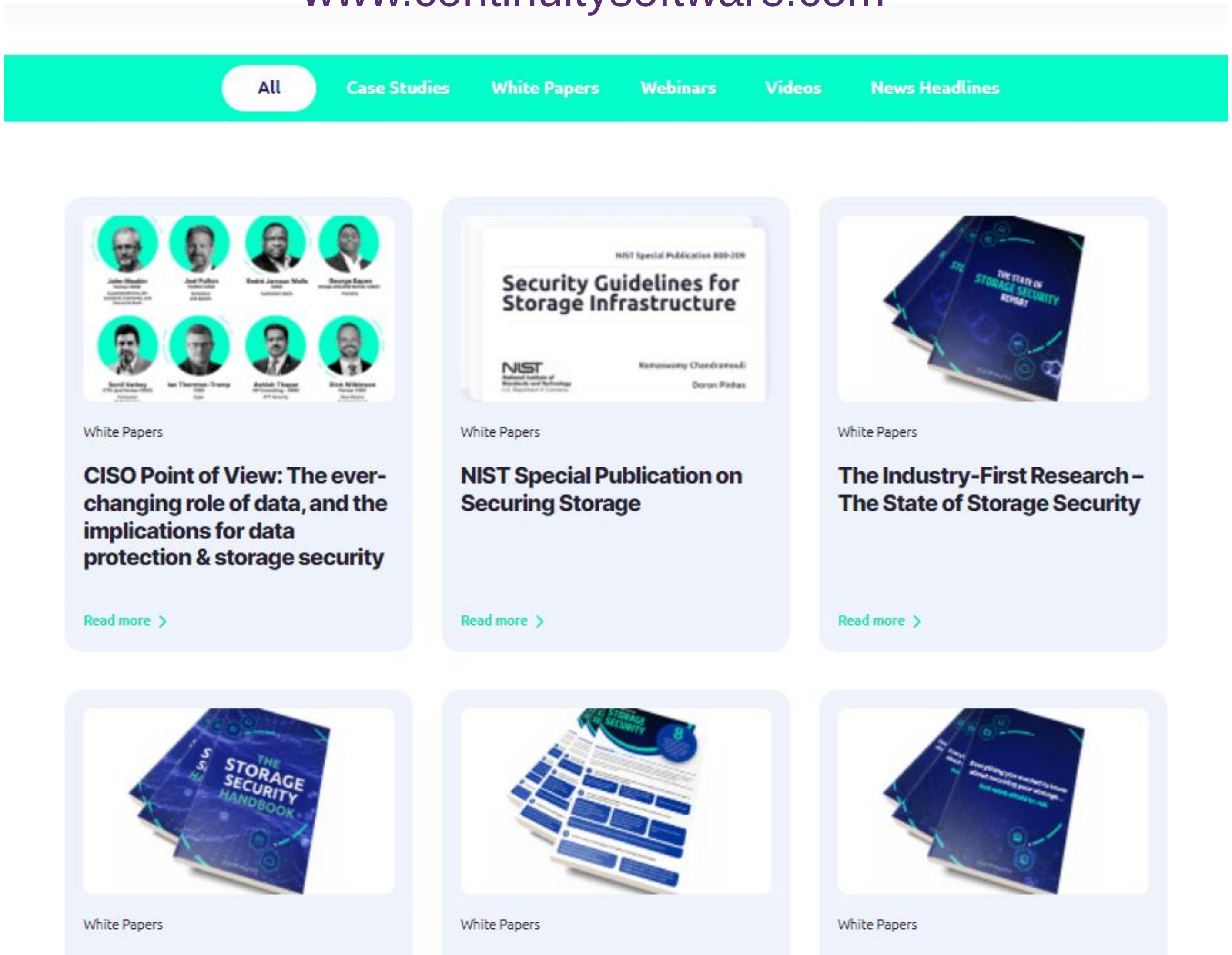
Configure file policies to block traffic that is suspected as ransomware:

```
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

# param2 list of known ransomware file extensions to block
```

SNIA. STORAGE
SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Summary and further resources

www.continuitysoftware.com


All
Case Studies
White Papers
Webinars
Videos
News Headlines
NIST Special Publication 800-209
Security Guidelines for Storage Infrastructure
NIST
Ramaswamy Chandramouli
Doron Pinhas
The State of Storage Security Report
The Storage Security Handbook
Read more
Read more
Read more

White Papers

CISO Point of View: The ever-changing role of data, and the implications for data protection & storage security

White Papers

NIST Special Publication on Securing Storage

White Papers

The Industry-First Research – The State of Storage Security

White Papers

White Papers

White Papers

Sign up for a free trial

A limited scan of 3 storage / backup systems

Receive a report identifying security risks, prioritized by risk level, and with resolution guidance

Q&A

SNIA® STORAGE SECURITY SUMMIT
Wednesday, May 11, 2022 • Virtual

Please take a moment to rate this session.

Your feedback is important to us.