AWS Well-Architected

AWS Well-Architected Partner Solutions

New tools for automating Well-Architected Framework Reviews

Lauren Small
Well-Architected ISV Program Manager

AWS Well-Architected ISVs are:

Integrated with the AWS Well-Architected Tool

Validated through the AWS Competency

Designed to reduce time and resources to complete reviews and generate insights

Learn more: https://aws.amazon.com/well-architected-tool/partners/

Well-Architected Partner Solutions Webinar Series

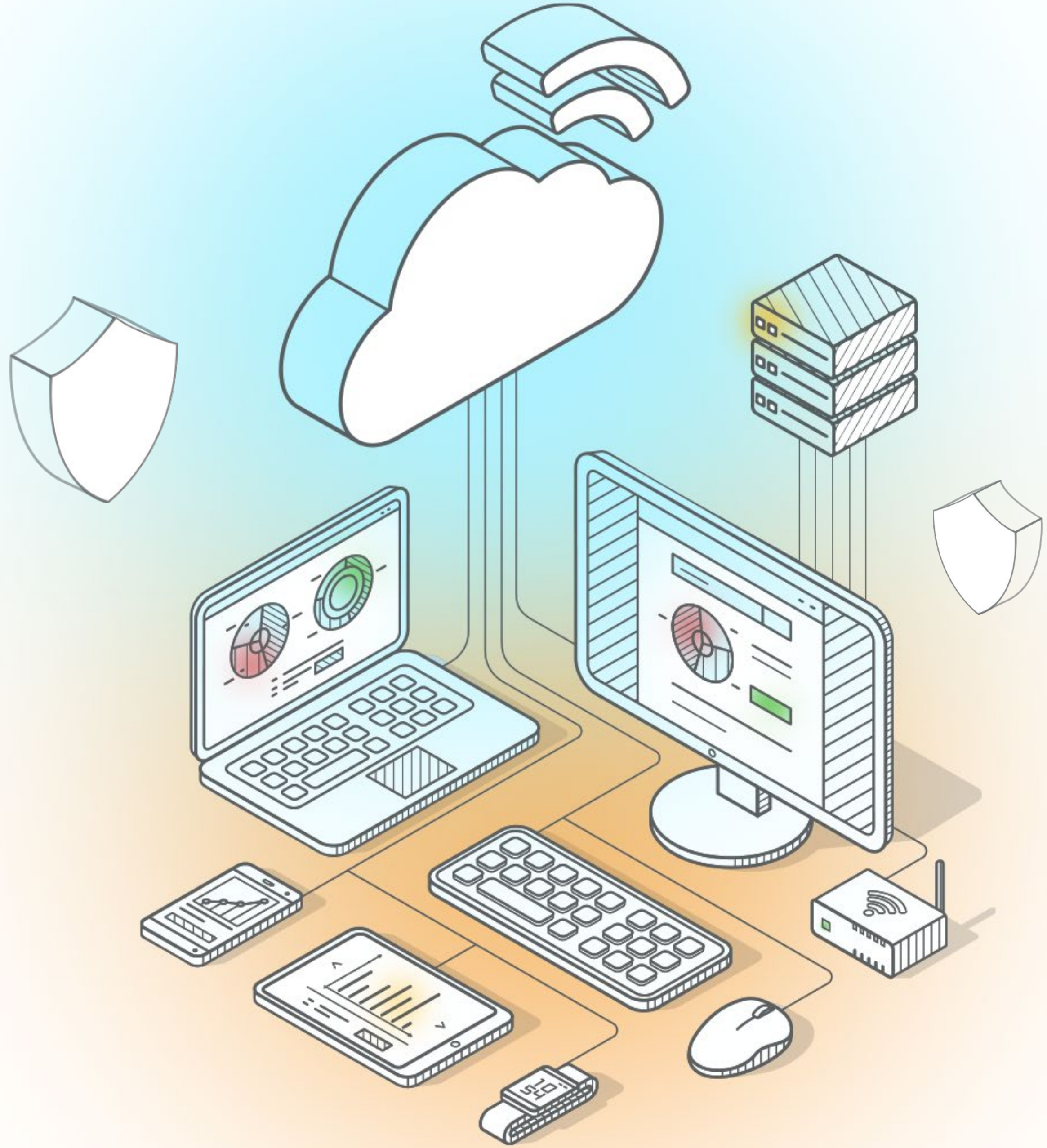
Date	Partner
On-demand	nOps
On-demand	CloudCheckr
On-demand	Turbot
On-demand	Trend Micro Cloud One-Conformity
» Now	Continuity Software

Access recordings of all webinars in this series at:
https://partners.awscloud.com/WAPPISVPartnerCastSeries_Registrationpage.html

CONTINUITY SOFTWARE

How to succeed with Cloud Storage Hardening

Continuity Software empowers the AWS Well-Architected Framework



What you'll learn in today's webinar

- » About us
- » Cloud Security: Reality Check
- » Securing Cloud Storage
- » Using Coral™ for Storage Security
- » 3 Steps to Success
- » Q&A

Our speakers

Yaniv Valik

VP Product

Continuity Software

Doron Youngerwood

VP Marketing

Continuity Software

About Continuity

- Two-fold mission
  - Validate data storage **security**
  - Validate data storage **recoverability**
- Scope
  - Public cloud
  - Private cloud + traditional on-prem workloads
- AWS Advanced Technology partner
- Listing available on the AWS Marketplace

Selected Customers

VISA
MIGDAL
ferrovial
Liberty Mutual.
BNP PARIBAS
BBVA
לאומי leumi
El Corte Inglés
swisscom
MetLife
MINISTRY OF GOVERNMENT ADMINISTRATION AND HOME AFFAIRS
中国平安 PING AN 保险 · 银行 · 投资
ups
Partner
Phoenix
NH Bank
KB KREDİ KAYIT BÜROSU
EL AL אל על
FIBI BANK
Industrial Bank of Korea

aws partner network

Advanced Technology Partner

aws marketplace

Marketplace seller

Reality check

Gartner

“By 2021, 50% of enterprises will unknowingly have some IaaS **storage services**… directly **exposed** to the public internet.”

“Through 2023, **99%** of cloud security failures will be the **customer’s fault.**”

Enterprises cannot tolerate data breaches or loss.

- Regulatory fines
- *“Capital One to pay $80 million fine after data breach”*
- Losing B2B business
- *"Texas Medicaid subcontractor dumped after data breach”*
- Losing B2C business
- *“Consumers are Abandoning Brands after Data Breaches”*

Quick Poll

CONTINUITY SOFTWARE

Storage security failures

EVERSOURCE

Eversource Energy

Customers' personal information was exposed on an unsecured cloud storage

April 21, 2021

Pfizer

A misconfigured Google Cloud database exposed information of hundreds of medical patients taking cancer drugs through a data leak.

October 20, 2020

Lion Air Airline

A breach that exposed data on millions of passengers is another example of the massive exposure that organizations face from leaving data in poorly secured cloud storage

Sep 19, 2019

mercato

Mercato

one of the company's cloud storage buckets, hosted on Amazon's cloud, was left open and unprotected.

April 14, 2021

PREMIER DIAGNOSTICS

Premier Diagnostics

... reported on the discovery of over 50,000 records stored on two publicly accessible AWS S3 buckets without password protection or authentication

March 15, 2021

NSW GOVERNMENT | Transport

Transport for NSW

Over 54,000 scanned NSW driver's licenses found in open cloud storage

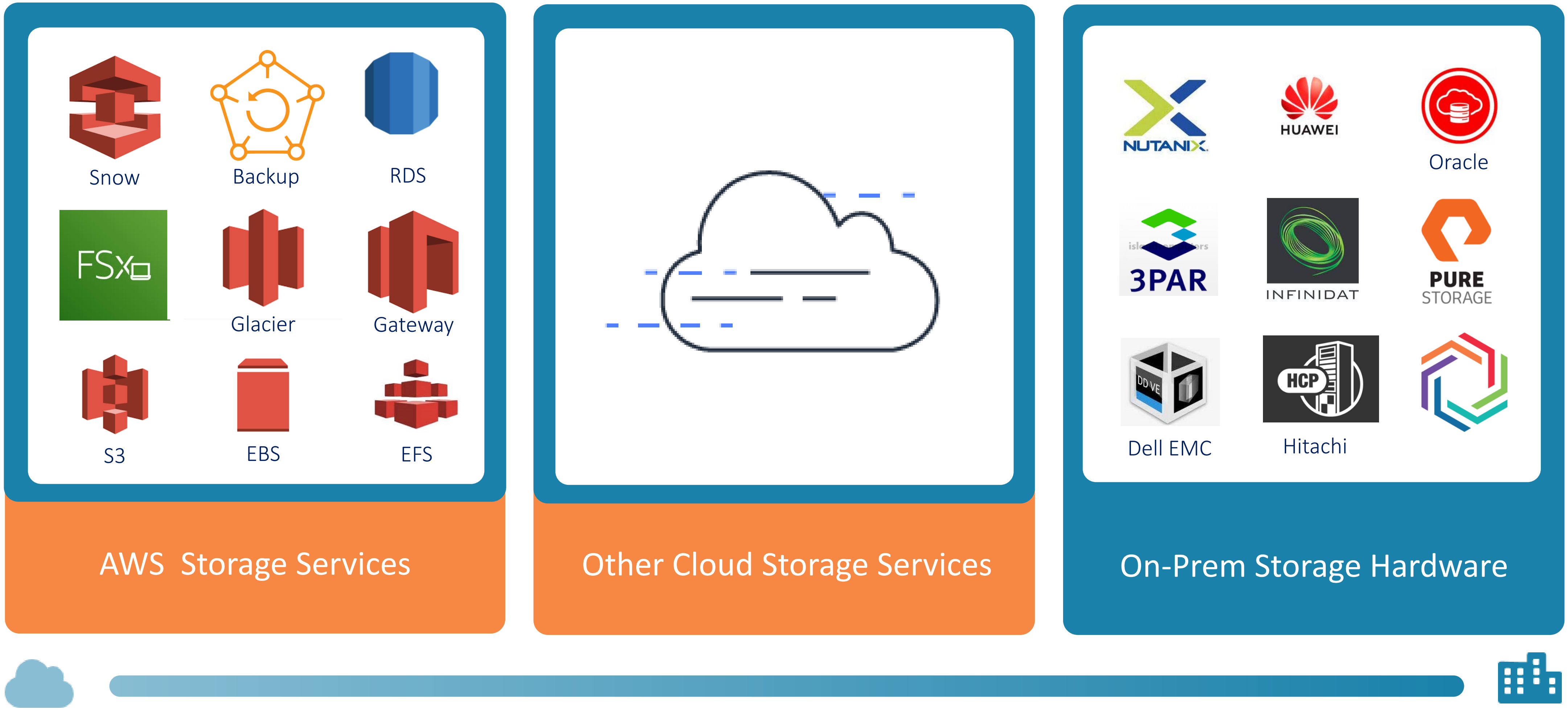
Aug 28, 2020

Netflix, TD Bank, Ford

Leaky AWS S3 Buckets Exposes Netflix, TD Bank, and Ford's Data...

June 28, 2019

Responsibility for storage security



Snow Backup RDS

FSx Glacier Gateway

S3 EBS EFS

AWS Storage Services

Other Cloud Storage Services

NUTANIX HUAWEI Oracle

3PAR INFINIDAT PURE STORAGE

Dell EMC Hitachi

On-Prem Storage Hardware

🟧 **Vendor** Responsibility 🟦 **Customer** Responsibility

Guidelines for storage security

AWS Well Architected Framework

Security pillar

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

NIST Security Guidelines for Storage Infrastructure

SP 800-209

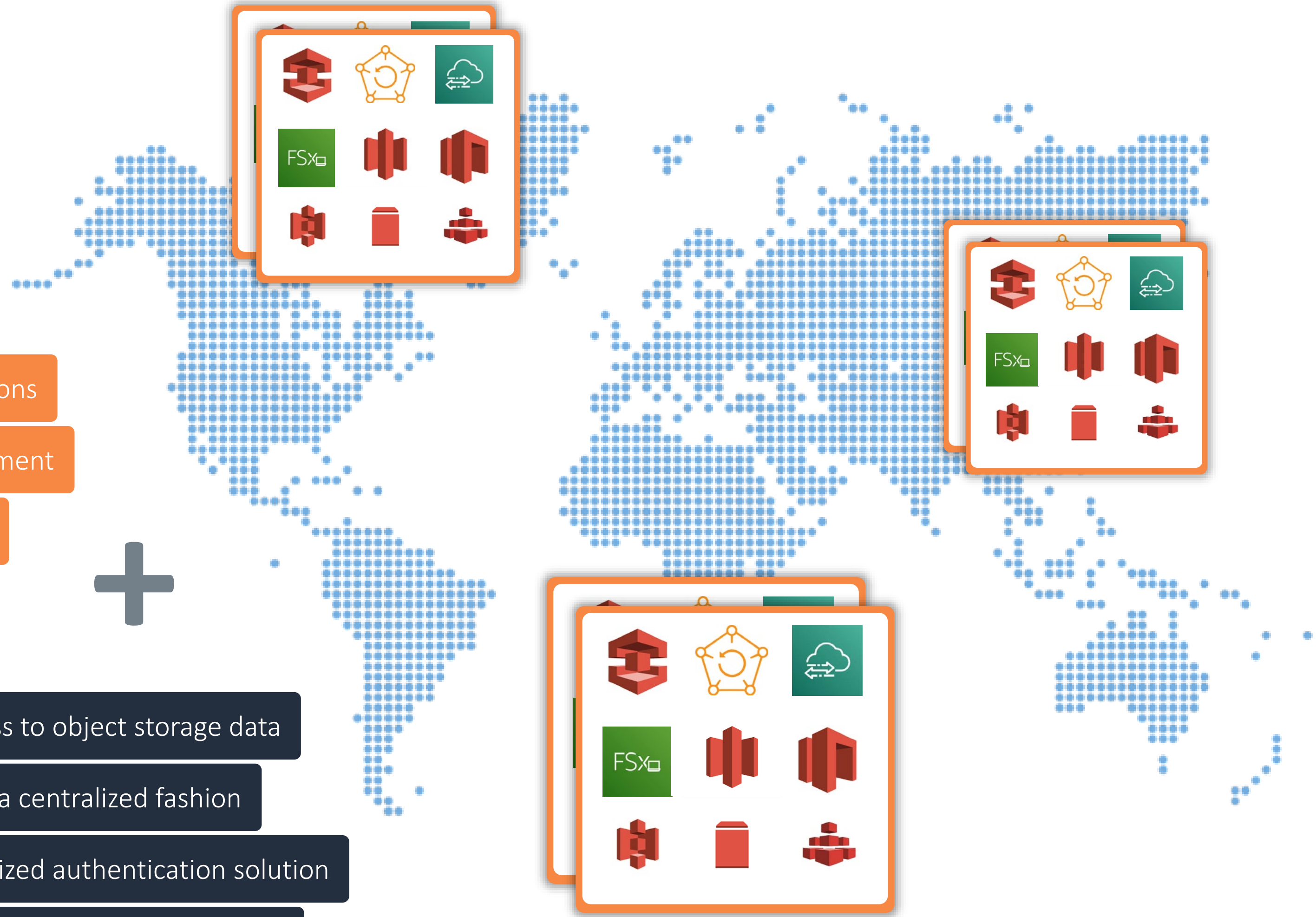
The challenge

- Enforce encryption at rest
- Authenticate network communications
- Implement secure key management
- Enforce encryption in transit
- Enforce access control

+

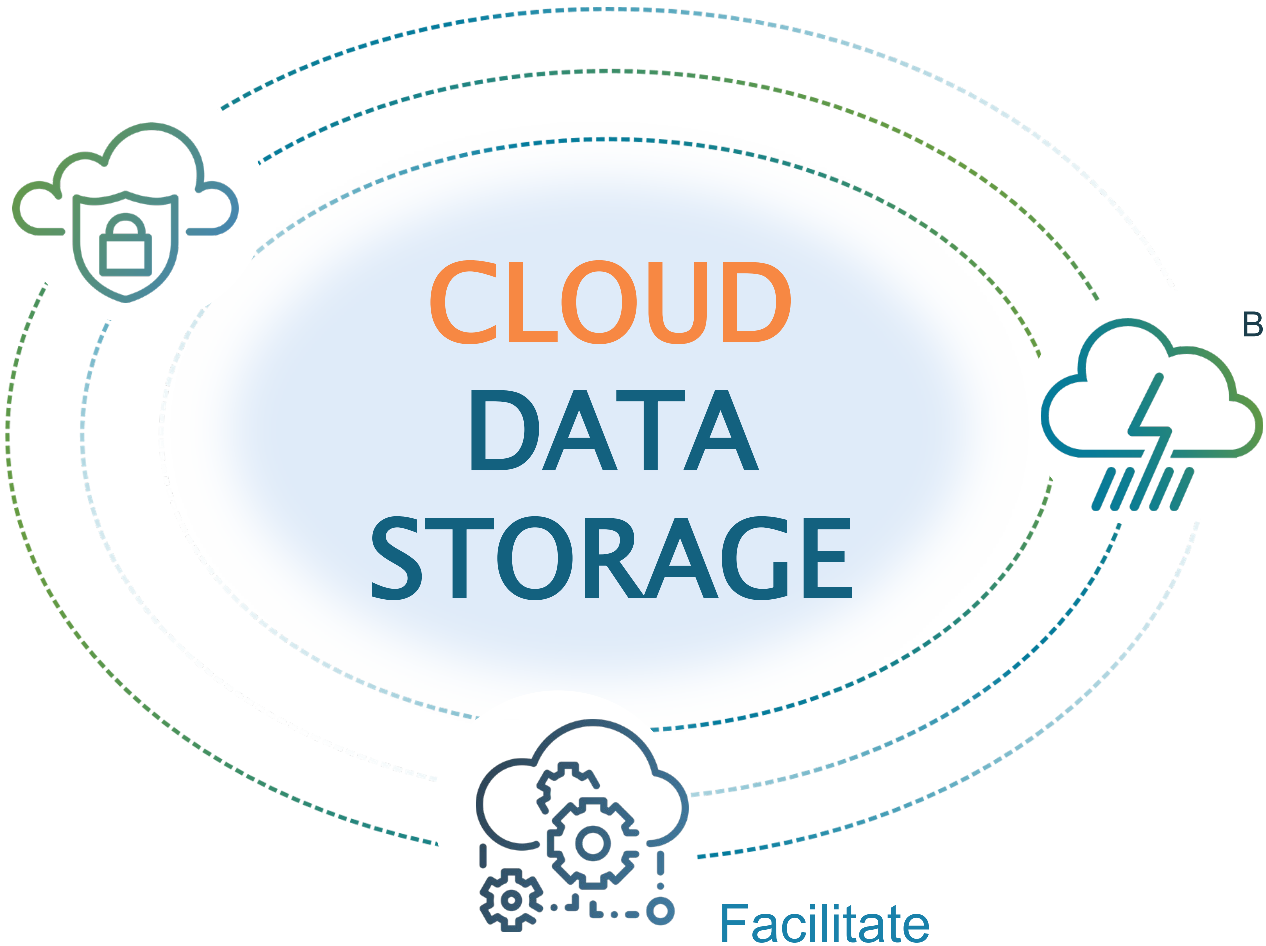
National Institute of Standards and Technology
U.S. Department of Commerce

- AC-SS-R30 – Restricting access to object storage data
- AL-SS-R3 – Collect logs in a centralized fashion
- AC-SS-R2 – A centralized authentication solution
- AC-SS-R34 –Granular permission assignment
- EN-SS-R6 – At-rest encryption of sensitive data



Securing data storage using Coral™

Continuous Compliance & Security Posture Validation



CLOUD DATA STORAGE

Prevent Security Failures

Before they impact business

Facilitate automatic healing

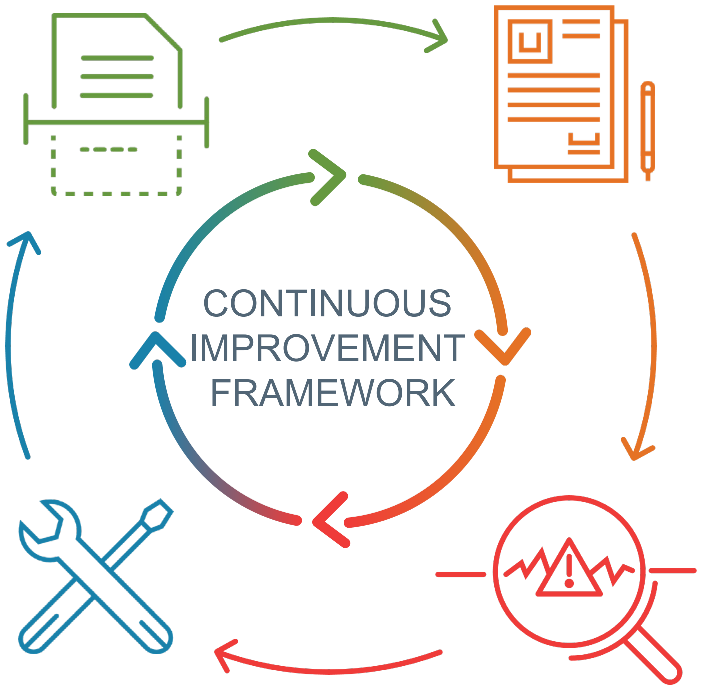
How it works

1 Scan

- » **Continuous / event driven data collection**
- » Non-intrusive and secure
- » API / agentless / agent options supported
- » AWS WA Tool integration

2 Analytics

- » **Hundreds of rules & vendor best-practices – deep / crowd knowledge driven**
- » Risk detection engine
- » Deep business impact
- » Custom rules and policies

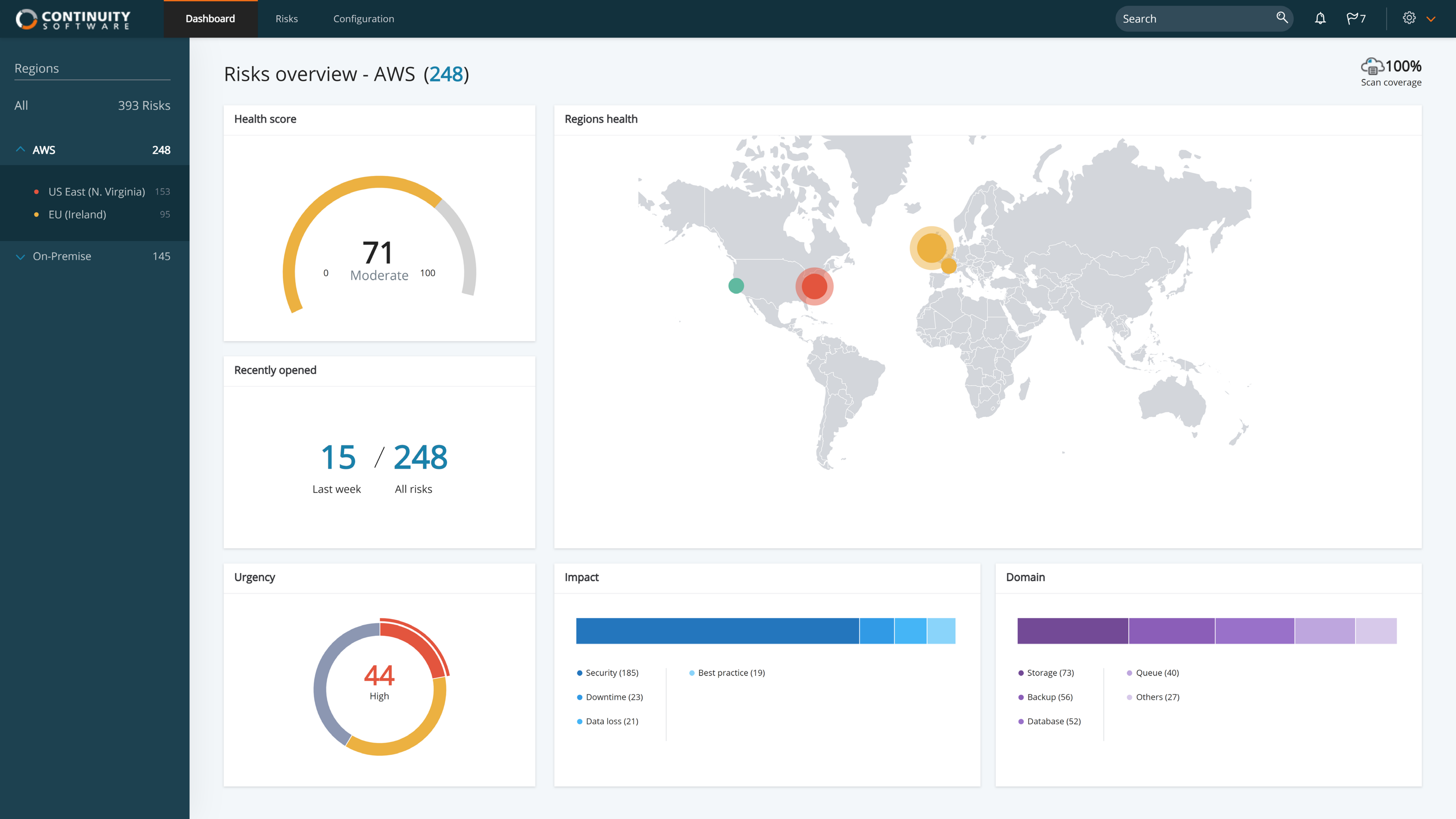


3 Remediate

- » **Actionable alerts and recommendations**
- » Remedial suggestions
- » Seamless integration with existing tools and workflows

4 Visualize

- » **Single-pane of glass for configuration quality, health & risk**
- » Risk & health scorecards
- » Reporting and Compliance tracking



Regions

All	393 Risks
AWS	248
● US East (N. Virginia)	153
● EU (Ireland)	95
On-Premise	145

Risks overview - AWS (248)

100%
Scan coverage

Health score

71
Moderate

Regions health

Recently opened

15 / 248
Last week · All risks

Urgency

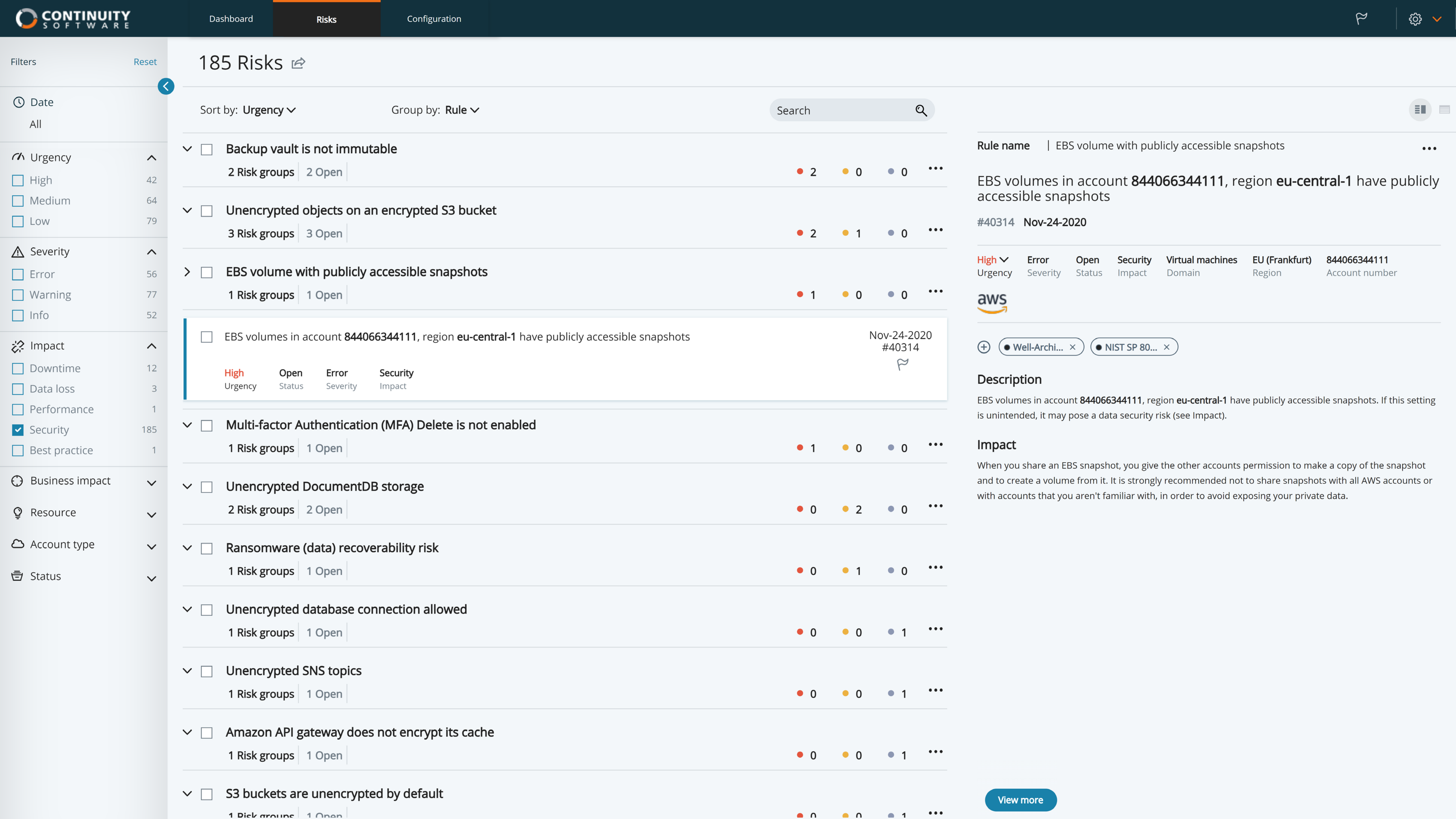
44
High

Impact

- Security (185)
- Downtime (23)
- Data loss (21)
- Best practice (19)

Domain

- Storage (73)
- Backup (56)
- Database (52)
- Queue (40)
- Others (27)



Filters Reset

185 Risks

Date
All

Urgency

□ High	42
□ Medium	64
□ Low	79

Severity

□ Error	56
□ Warning	77
□ Info	52

Impact

□ Downtime	12
□ Data loss	3
□ Performance	1
☑ Security	185
□ Best practice	1

Business impact

Resource

Account type

Status

Sort by: Urgency   Group by: Rule   Search

			●	●	●
□ Backup vault is not immutable	2 Risk groups	2 Open	2	0	0
□ Unencrypted objects on an encrypted S3 bucket	3 Risk groups	3 Open	2	1	0
□ EBS volume with publicly accessible snapshots	1 Risk groups	1 Open	1	0	0

□ EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots
Nov-24-2020
#40314

High	Open	Error	Security
Urgency	Status	Severity	Impact

			●	●	●
□ Multi-factor Authentication (MFA) Delete is not enabled	1 Risk groups	1 Open	1	0	0
□ Unencrypted DocumentDB storage	2 Risk groups	2 Open	0	2	0
□ Ransomware (data) recoverability risk	1 Risk groups	1 Open	0	1	0
□ Unencrypted database connection allowed	1 Risk groups	1 Open	0	0	1
□ Unencrypted SNS topics	1 Risk groups	1 Open	0	0	1
□ Amazon API gateway does not encrypt its cache	1 Risk groups	1 Open	0	0	1
□ S3 buckets are unencrypted by default	1 Risk groups	1 Open	0	0	1

Rule name | EBS volume with publicly accessible snapshots

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots

#40314 **Nov-24-2020**

High	Error	Open	Security	Virtual machines	EU (Frankfurt)	844066344111
Urgency	Severity	Status	Impact	Domain	Region	Account number

aws

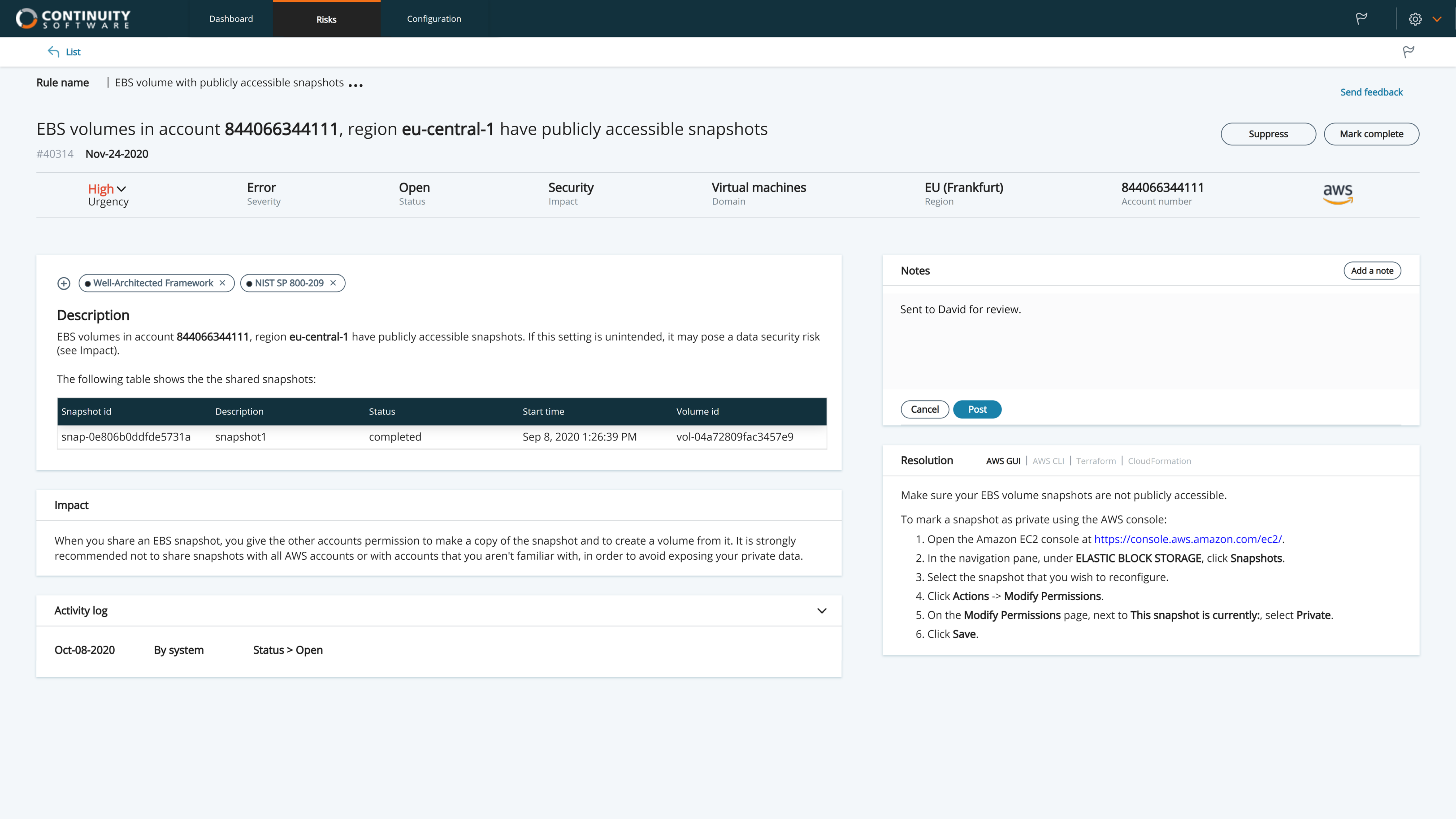
● Well-Archi... ✕ ● NIST SP 80... ✕

Description

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots. If this setting is unintended, it may pose a data security risk (see Impact).

Impact

When you share an EBS snapshot, you give the other accounts permission to make a copy of the snapshot and to create a volume from it. It is strongly recommended not to share snapshots with all AWS accounts or with accounts that you aren't familiar with, in order to avoid exposing your private data.



Rule name | EBS volume with publicly accessible snapshots ...

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots

#40314 Nov-24-2020

High Urgency	Error Severity	Open Status	Security Impact	Virtual machines Domain	EU (Frankfurt) Region	844066344111 Account number

● Well-Architected Framework × ● NIST SP 800-209 ×

Description

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots. If this setting is unintended, it may pose a data security risk (see Impact).

The following table shows the the shared snapshots:

Snapshot id	Description	Status	Start time	Volume id
snap-0e806b0ddfde5731a	snapshot1	completed	Sep 8, 2020 1:26:39 PM	vol-04a72809fac3457e9

Impact

When you share an EBS snapshot, you give the other accounts permission to make a copy of the snapshot and to create a volume from it. It is strongly recommended not to share snapshots with all AWS accounts or with accounts that you aren't familiar with, in order to avoid exposing your private data.

Activity log

Oct-08-2020 By system Status > Open

Notes

Sent to David for review.

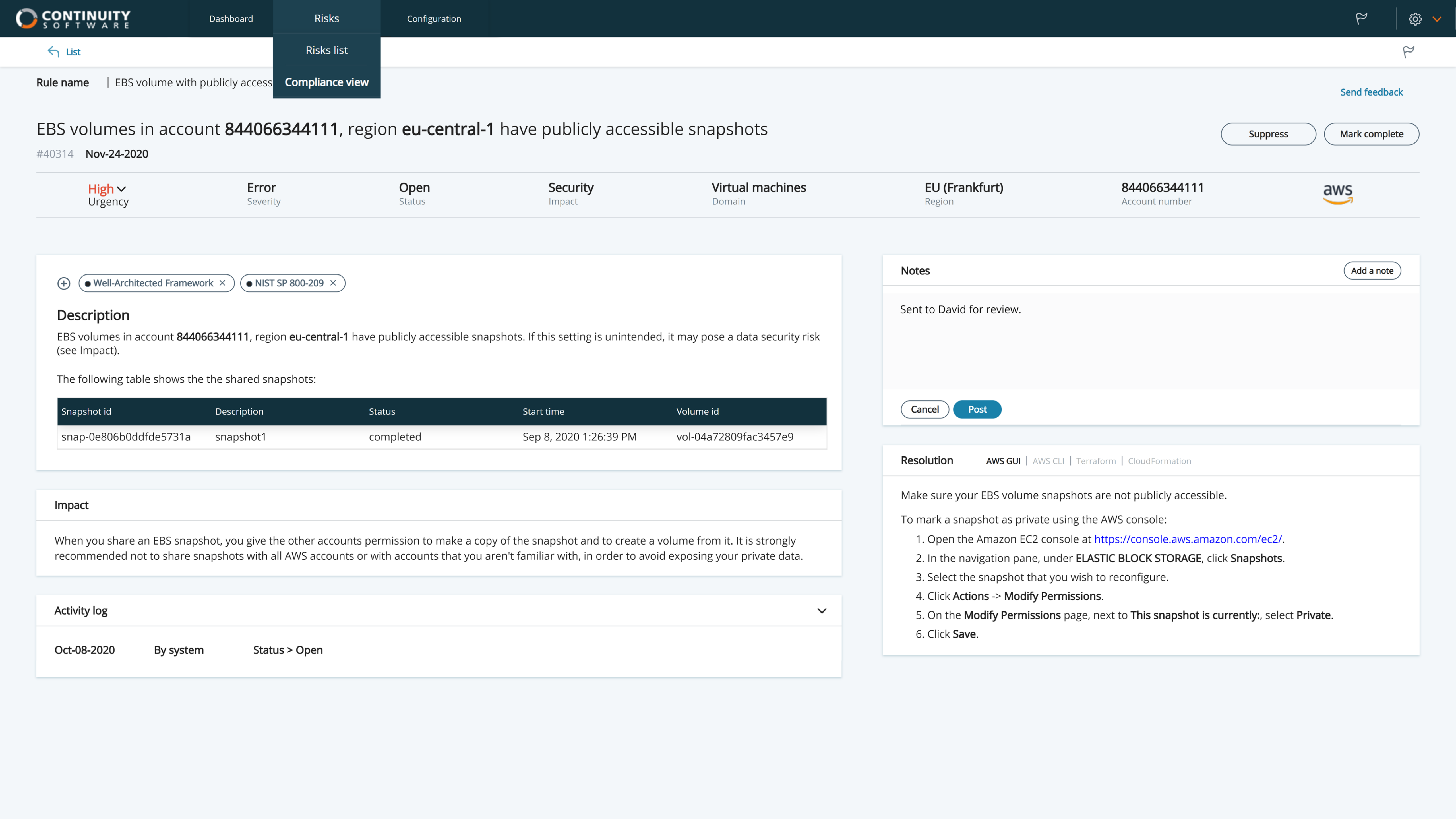
Resolution

AWS GUI | AWS CLI | Terraform | CloudFormation

Make sure your EBS volume snapshots are not publicly accessible.

To mark a snapshot as private using the AWS console:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **ELASTIC BLOCK STORAGE**, click **Snapshots**.
3. Select the snapshot that you wish to reconfigure.
4. Click **Actions** -> **Modify Permissions**.
5. On the **Modify Permissions** page, next to **This snapshot is currently:**, select **Private**.
6. Click **Save**.



Rule name | EBS volume with publicly access

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots

#40314 Nov-24-2020

High	Error	Open	Security	Virtual machines	EU (Frankfurt)	844066344111	aws
Urgency	Severity	Status	Impact	Domain	Region	Account number	

● Well-Architected Framework × ● NIST SP 800-209 ×

Description

EBS volumes in account **844066344111**, region **eu-central-1** have publicly accessible snapshots. If this setting is unintended, it may pose a data security risk (see Impact).

The following table shows the the shared snapshots:

Snapshot id	Description	Status	Start time	Volume id
snap-0e806b0ddfde5731a	snapshot1	completed	Sep 8, 2020 1:26:39 PM	vol-04a72809fac3457e9

Impact

When you share an EBS snapshot, you give the other accounts permission to make a copy of the snapshot and to create a volume from it. It is strongly recommended not to share snapshots with all AWS accounts or with accounts that you aren't familiar with, in order to avoid exposing your private data.

Activity log

Oct-08-2020	By system	Status > Open

Notes

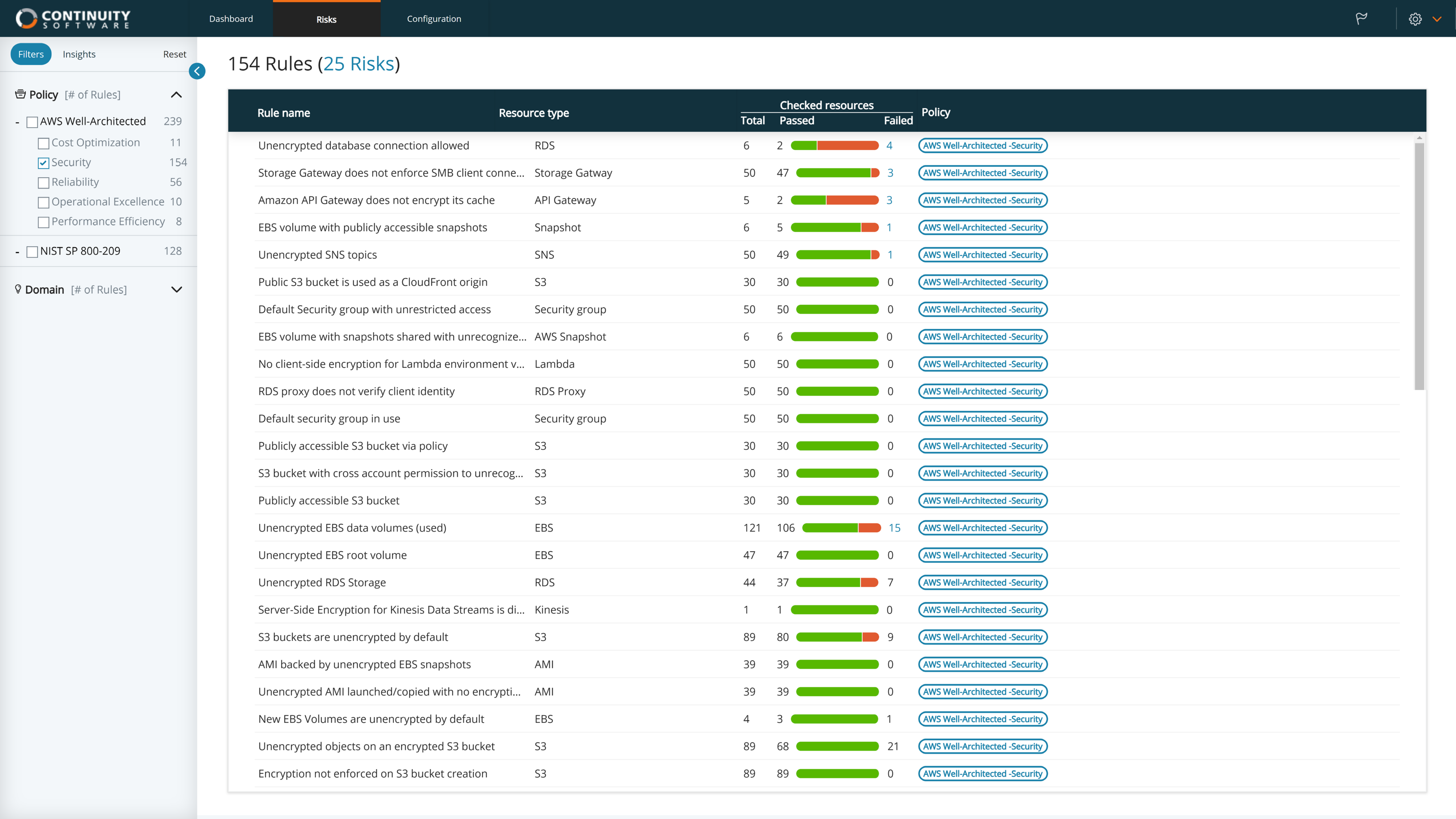
Sent to David for review.

Resolution

Make sure your EBS volume snapshots are not publicly accessible.

To mark a snapshot as private using the AWS console:

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, under **ELASTIC BLOCK STORAGE**, click **Snapshots**.
3. Select the snapshot that you wish to reconfigure.
4. Click **Actions** -> **Modify Permissions**.
5. On the **Modify Permissions** page, next to **This snapshot is currently:**, select **Private**.
6. Click **Save**.



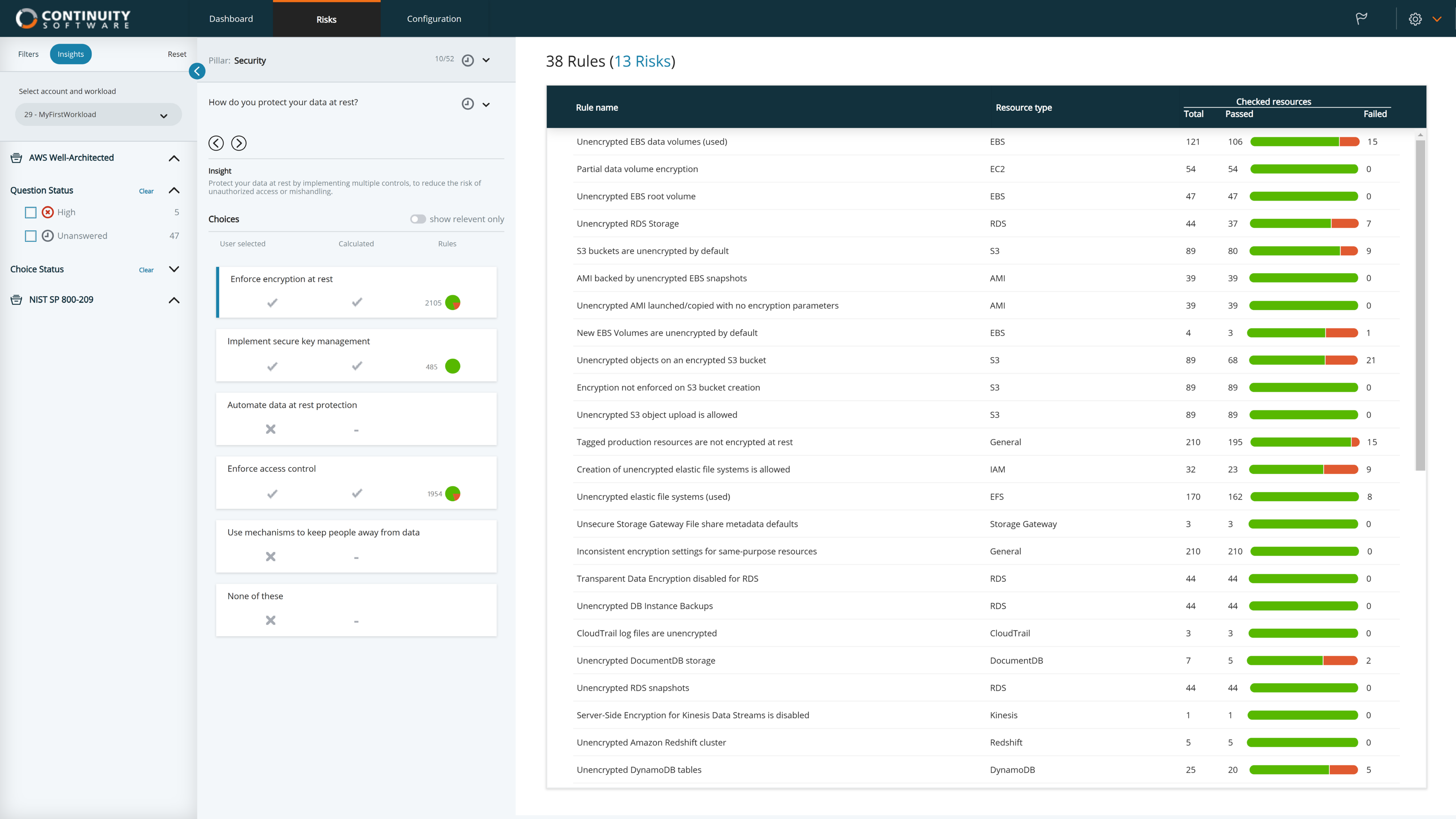
Policy [# of Rules]

- ☐ AWS Well-Architected 239
  - ☐ Cost Optimization 11
  - ☑ Security 154
  - ☐ Reliability 56
  - ☐ Operational Excellence 10
  - ☐ Performance Efficiency 8
- ☐ NIST SP 800-209 128

Domain [# of Rules]

154 Rules (25 Risks)

Rule name	Resource type	Checked resources			Policy
		Total	Passed	Failed	
Unencrypted database connection allowed	RDS	6	2	4	AWS Well-Architected -Security
Storage Gateway does not enforce SMB client conne...	Storage Gatway	50	47	3	AWS Well-Architected -Security
Amazon API Gateway does not encrypt its cache	API Gateway	5	2	3	AWS Well-Architected -Security
EBS volume with publicly accessible snapshots	Snapshot	6	5	1	AWS Well-Architected -Security
Unencrypted SNS topics	SNS	50	49	1	AWS Well-Architected -Security
Public S3 bucket is used as a CloudFront origin	S3	30	30	0	AWS Well-Architected -Security
Default Security group with unrestricted access	Security group	50	50	0	AWS Well-Architected -Security
EBS volume with snapshots shared with unrecognize...	AWS Snapshot	6	6	0	AWS Well-Architected -Security
No client-side encryption for Lambda environment v...	Lambda	50	50	0	AWS Well-Architected -Security
RDS proxy does not verify client identity	RDS Proxy	50	50	0	AWS Well-Architected -Security
Default security group in use	Security group	50	50	0	AWS Well-Architected -Security
Publicly accessible S3 bucket via policy	S3	30	30	0	AWS Well-Architected -Security
S3 bucket with cross account permission to unrecog...	S3	30	30	0	AWS Well-Architected -Security
Publicly accessible S3 bucket	S3	30	30	0	AWS Well-Architected -Security
Unencrypted EBS data volumes (used)	EBS	121	106	15	AWS Well-Architected -Security
Unencrypted EBS root volume	EBS	47	47	0	AWS Well-Architected -Security
Unencrypted RDS Storage	RDS	44	37	7	AWS Well-Architected -Security
Server-Side Encryption for Kinesis Data Streams is di...	Kinesis	1	1	0	AWS Well-Architected -Security
S3 buckets are unencrypted by default	S3	89	80	9	AWS Well-Architected -Security
AMI backed by unencrypted EBS snapshots	AMI	39	39	0	AWS Well-Architected -Security
Unencrypted AMI launched/copied with no encrypti...	AMI	39	39	0	AWS Well-Architected -Security
New EBS Volumes are unencrypted by default	EBS	4	3	1	AWS Well-Architected -Security
Unencrypted objects on an encrypted S3 bucket	S3	89	68	21	AWS Well-Architected -Security
Encryption not enforced on S3 bucket creation	S3	89	89	0	AWS Well-Architected -Security



Select account and workload

29 - MyFirstWorkload

AWS Well-Architected

Question Status Clear

□ High 5

□ Unanswered 47

Choice Status Clear

NIST SP 800-209

Pillar: Security 10/52

How do you protect your data at rest?

Insight

Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.

Choices show relevent only

	User selected	Calculated	Rules
Enforce encryption at rest	✓	✓	2105
Implement secure key management	✓	✓	485
Automate data at rest protection	✗	-	
Enforce access control	✓	✓	1954
Use mechanisms to keep people away from data	✗	-	
None of these	✗	-	

38 Rules (13 Risks)

Rule name	Resource type	Checked resources		
		Total	Passed	Failed
Unencrypted EBS data volumes (used)	EBS	121	106	15
Partial data volume encryption	EC2	54	54	0
Unencrypted EBS root volume	EBS	47	47	0
Unencrypted RDS Storage	RDS	44	37	7
S3 buckets are unencrypted by default	S3	89	80	9
AMI backed by unencrypted EBS snapshots	AMI	39	39	0
Unencrypted AMI launched/copied with no encryption parameters	AMI	39	39	0
New EBS Volumes are unencrypted by default	EBS	4	3	1
Unencrypted objects on an encrypted S3 bucket	S3	89	68	21
Encryption not enforced on S3 bucket creation	S3	89	89	0
Unencrypted S3 object upload is allowed	S3	89	89	0
Tagged production resources are not encrypted at rest	General	210	195	15
Creation of unencrypted elastic file systems is allowed	IAM	32	23	9
Unencrypted elastic file systems (used)	EFS	170	162	8
Unsecure Storage Gateway File share metadata defaults	Storage Gateway	3	3	0
Inconsistent encryption settings for same-purpose resources	General	210	210	0
Transparent Data Encryption disabled for RDS	RDS	44	44	0
Unencrypted DB Instance Backups	RDS	44	44	0
CloudTrail log files are unencrypted	CloudTrail	3	3	0
Unencrypted DocumentDB storage	DocumentDB	7	5	2
Unencrypted RDS snapshots	RDS	44	44	0
Server-Side Encryption for Kinesis Data Streams is disabled	Kinesis	1	1	0
Unencrypted Amazon Redshift cluster	Redshift	5	5	0
Unencrypted DynamoDB tables	DynamoDB	25	20	5

Questions to consider…

- Are you evaluating storage security on an ongoing basis?
- Do we have detailed plans and procedures for recovery from a successful attack on a storage or backup resources?
- Do we test such procedures?

3 Steps to Success

1

Build a plan to address knowledge gaps for storage security

2

Improve security program to address identified gap

3

Use automation to continually evaluate and prioritize risks

> You need to have governance and an active program to secure your storage management layer.

Marc Ashworth, CISO

FIRST BANK

> The hackers are after our data. In a bank, data is money. This is why I'm a big believer in securing storage.

Erdal Ozkaya, Former CISO

standard chartered

Try the Solution: Free Trial Offer

CONTINUITY SOFTWARE

Request access for a free Partner Trial of the solution »

Get in touch with Continuity: Contact Continuity Software now »

Access the solution brief »

AWS Well-Architected

Q&A

AWS Well-Architected

Thank you

Access recordings of all webinars in this series at:
https://partners.awscloud.com/WAPPISVPartnerCastSeries_Registrationpage.html