Check Point®
SOFTWARE TECHNOLOGIES LTD

CHECK POINT
CloudGuard™

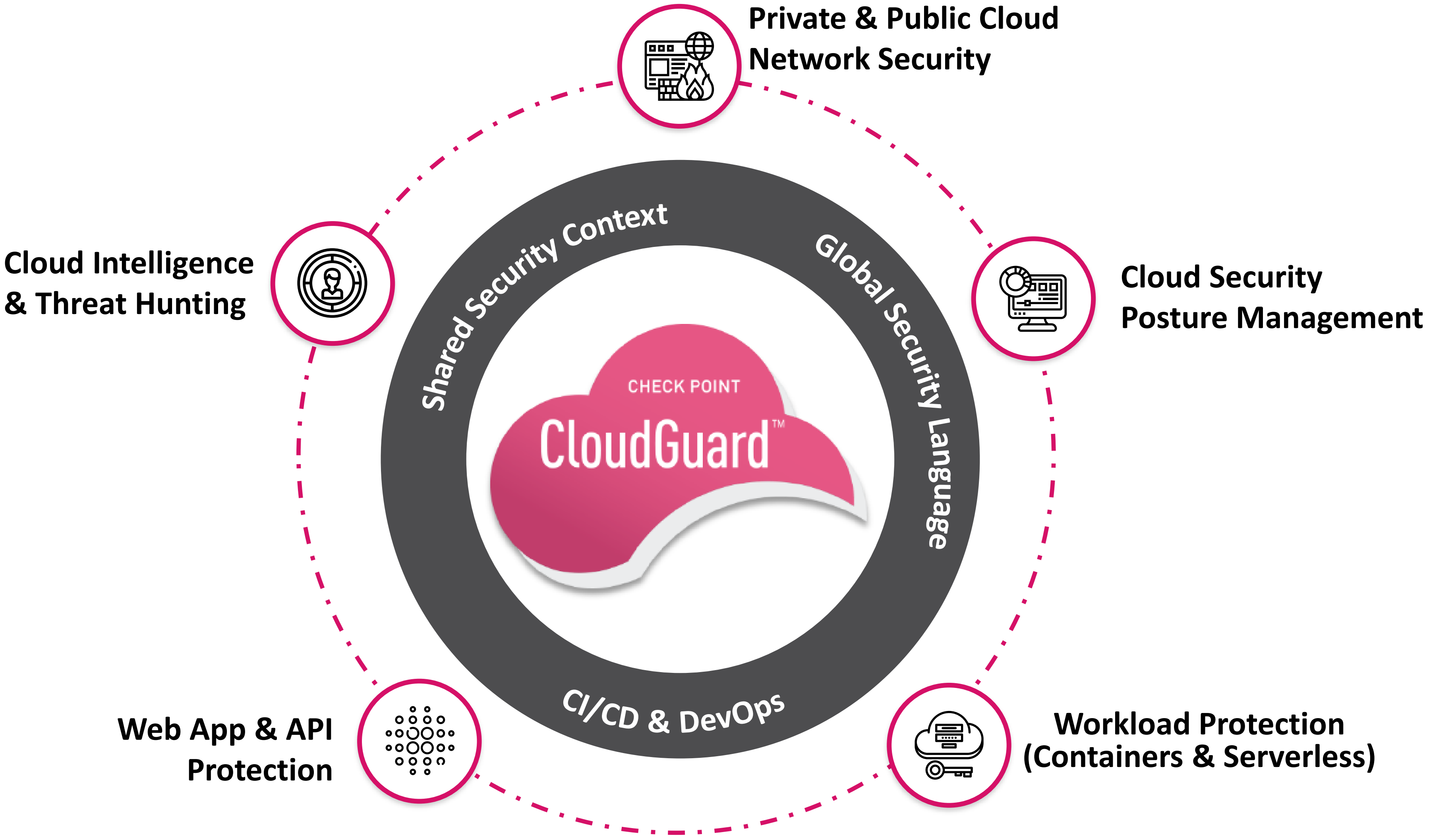
UNIFIED CLOUD-NATIVE SECURITY

CLOUD WITH CONFIDENCE WITH CHECK POINT

- UNIFIED
- SECURITY
- AUTOMATED
- EVERYWHERE

CHECK POINT CloudGuard™

UNIFIED MULTI CLOUD SECURITY

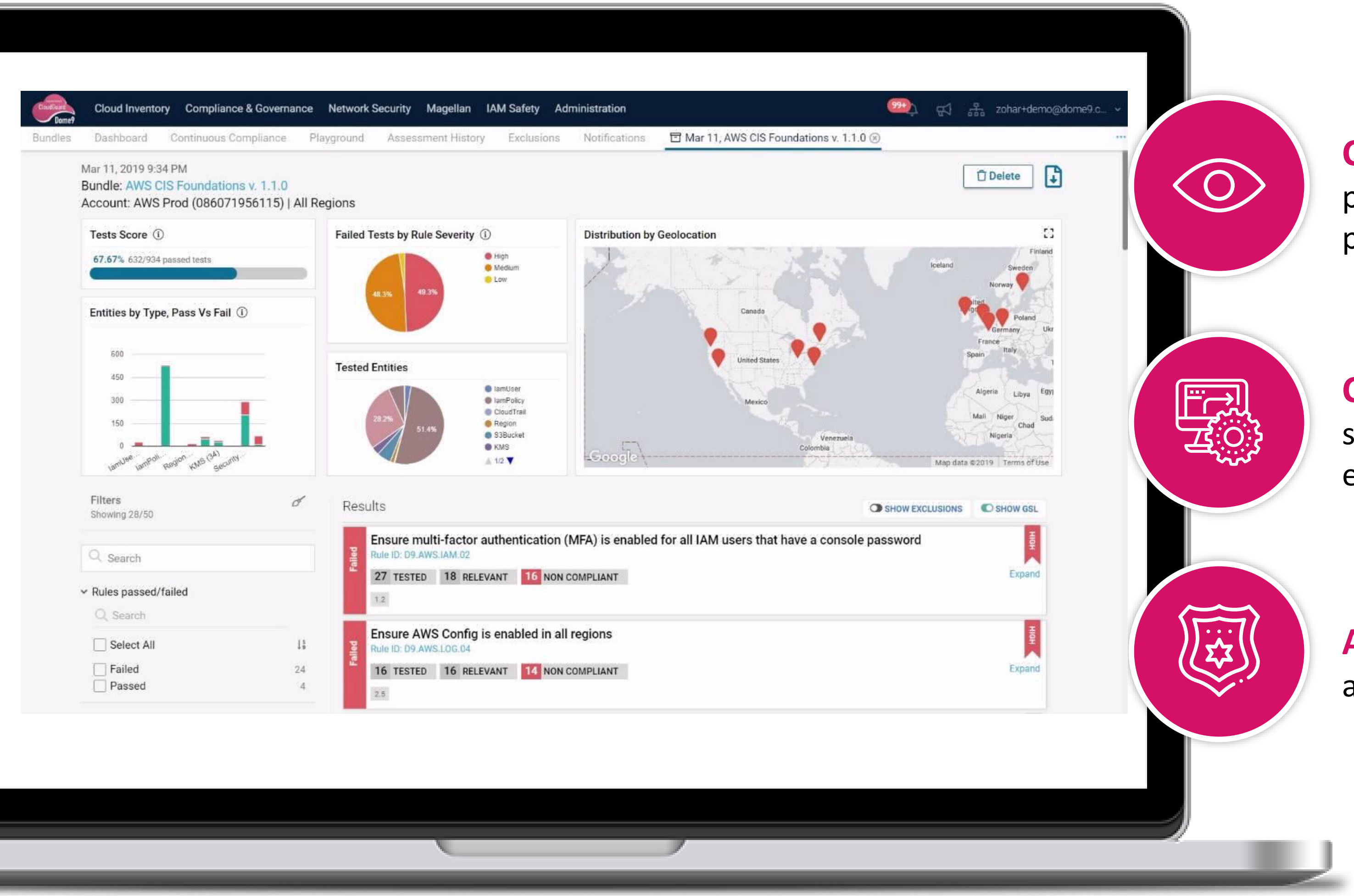


Private & Public Cloud Network Security
Cloud Intelligence & Threat Hunting
Cloud Security Posture Management
Shared Security Context
Global Security Language
CHECK POINT
CloudGuard™
CI/CD & DevOps
Web App & API Protection
Workload Protection (Containers & Serverless)

Check Point
SOFTWARE TECHNOLOGIES

Cloud Security Posture Management

Security, governance and compliance automation for public clouds and Kubernetes environments.



Mar 11, 2019 9:34 PM
Bundle: AWS CIS Foundations v. 1.1.0
Account: AWS Prod (086071956115) | All Regions

Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password
Rule ID: D9.AWS.IAM.02
27 TESTED 18 RELEVANT 16 NON COMPLIANT
1.2

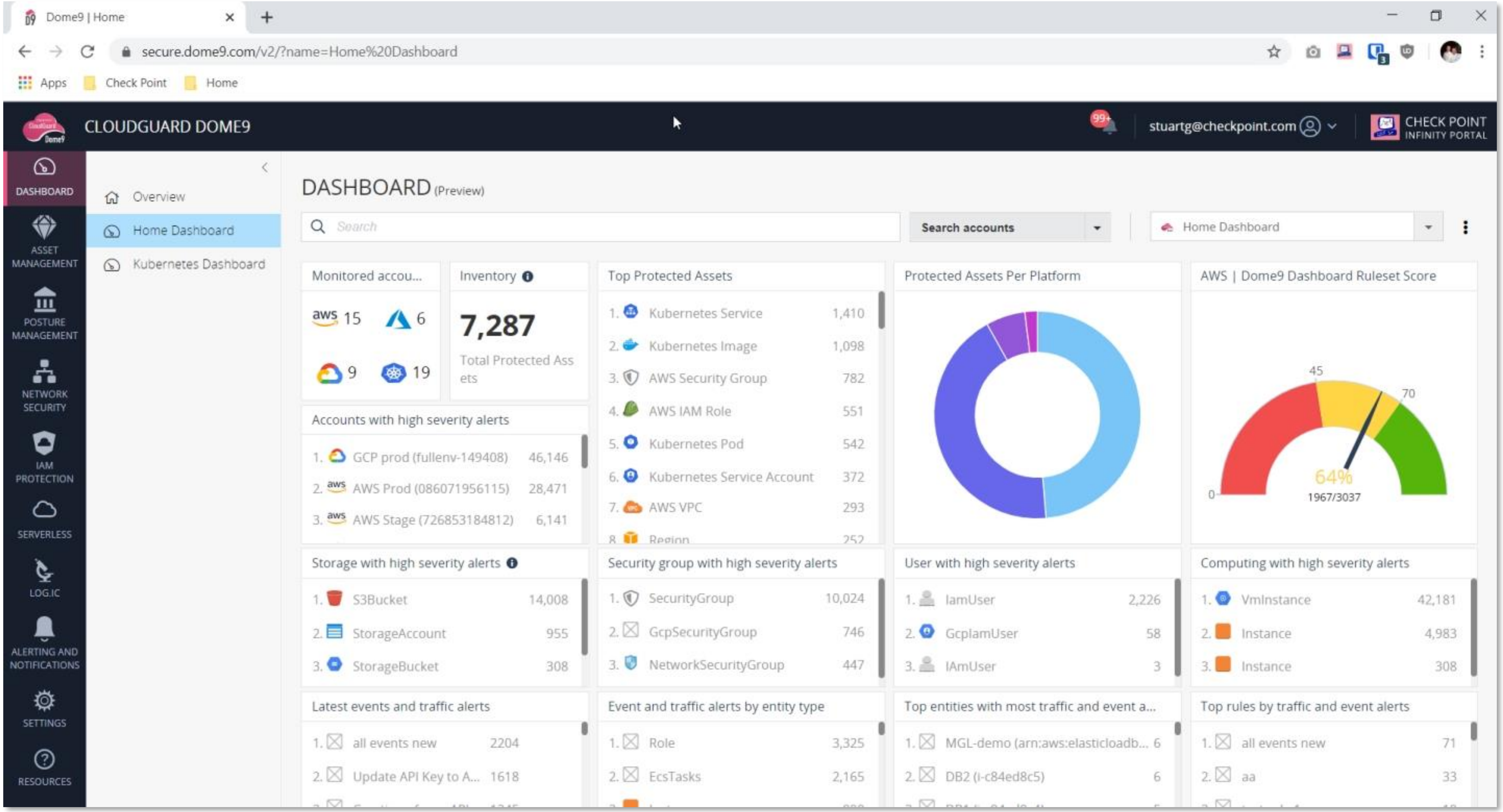
Ensure AWS Config is enabled in all regions
Rule ID: D9.AWS.LOG.04
16 TESTED 16 RELEVANT 14 NON COMPLIANT
2.5

Complete visibility into all assets, workloads and security policies across virtual networks, regions, and accounts on public clouds & K8S.

Continuous enforcement of regulatory compliance standards and security best practices, with flexible rules engine and auto-remediation.

Active protection against vulnerabilities, identity theft, data loss, and accidental or unauthorized changes.

Check Point
SOFTWARE TECHNOLOGIES



DASHBOARD (Preview)

Monitored accou...

aws 15 · 6 · 9 · 19

Inventory

7,287
Total Protected Assets

Top Protected Assets	
1. Kubernetes Service	1,410
2. Kubernetes Image	1,098
3. AWS Security Group	782
4. AWS IAM Role	551
5. Kubernetes Pod	542
6. Kubernetes Service Account	372
7. AWS VPC	293
8. Region	252

Protected Assets Per Platform

AWS | Dome9 Dashboard Ruleset Score

Accounts with high severity alerts	
1. GCP prod (fullenv-149408)	46,146
2. AWS Prod (086071956115)	28,471
3. AWS Stage (726853184812)	6,141

Storage with high severity alerts	
1. S3Bucket	14,008
2. StorageAccount	955
3. StorageBucket	308

Security group with high severity alerts	
1. SecurityGroup	10,024
2. GcpSecurityGroup	746
3. NetworkSecurityGroup	447

User with high severity alerts	
1. IamUser	2,226
2. GcpIamUser	58
3. IAmUser	3

Computing with high severity alerts	
1. VmInstance	42,181
2. Instance	4,983
3. Instance	308

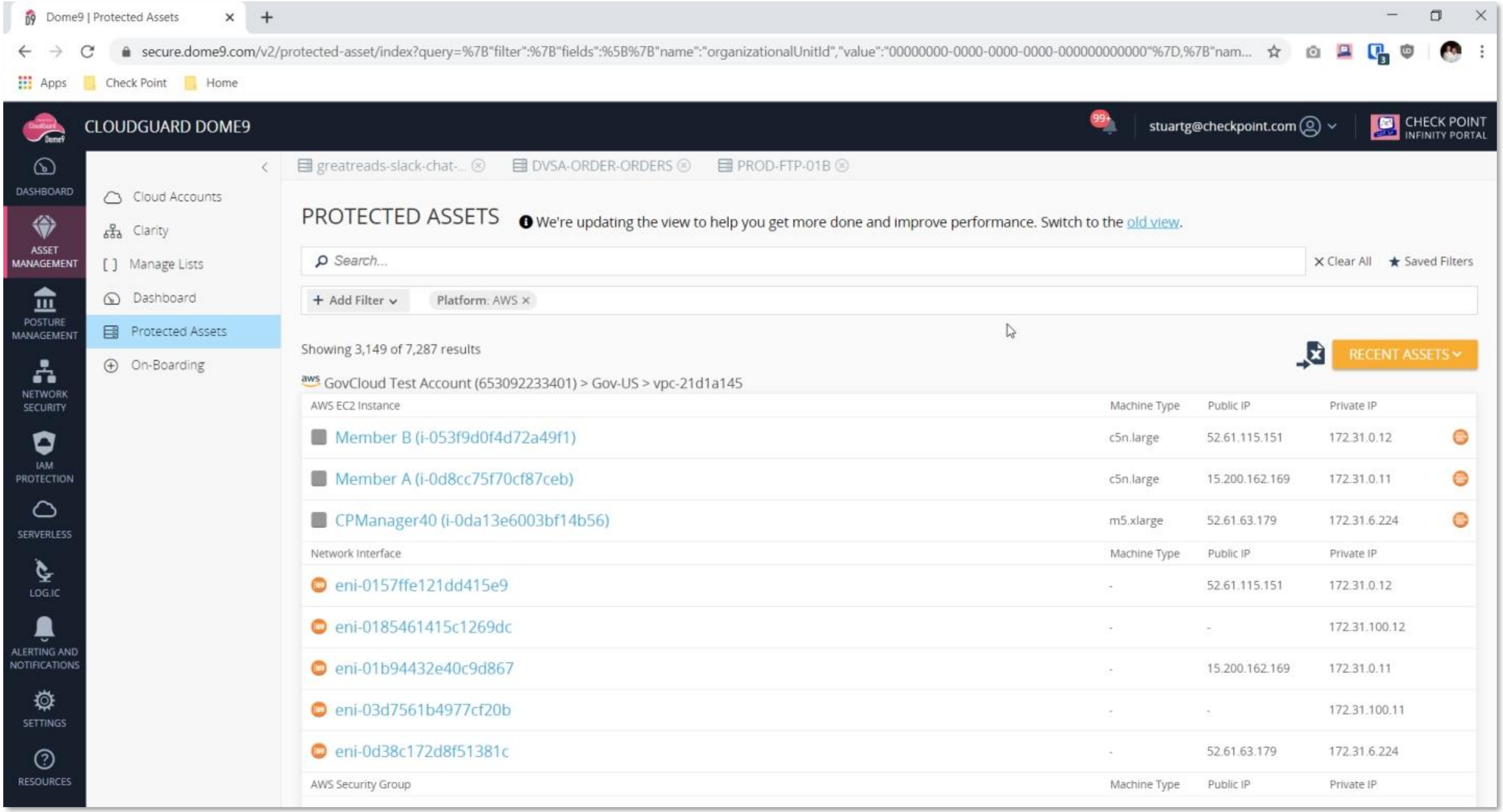
Latest events and traffic alerts	
1. all events new	2204
2. Update API Key to A...	1618

Event and traffic alerts by entity type	
1. Role	3,325
2. EcsTasks	2,165

Top entities with most traffic and event a...	
1. MGL-demo (arn:aws:elasticloadb...	6
2. DB2 (i-c84ed8c5)	6

Top rules by traffic and event alerts	
1. all events new	71
2. aa	33

Check Point
SOFTWARE TECHNOLOGIES



PROTECTED ASSETS

We're updating the view to help you get more done and improve performance. Switch to the old view.

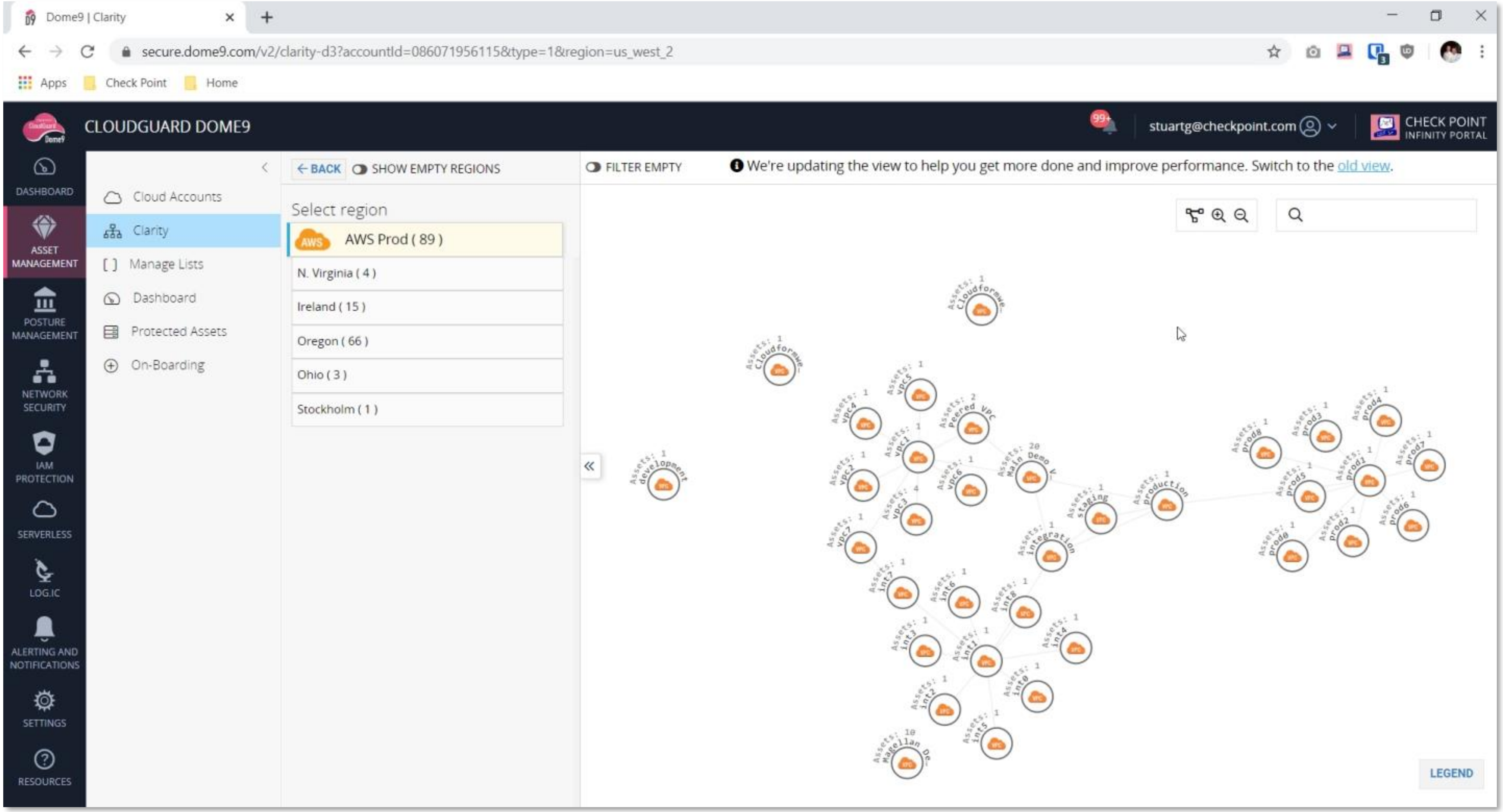
Showing 3,149 of 7,287 results

aws GovCloud Test Account (653092233401) > Gov-US > vpc-21d1a145

AWS EC2 Instance	Machine Type	Public IP	Private IP
Member B (i-053f9d0f4d72a49f1)	c5n.large	52.61.115.151	172.31.0.12
Member A (i-0d8cc75f70cf87ceb)	c5n.large	15.200.162.169	172.31.0.11
CPManager40 (i-0da13e6003bf14b56)	m5.xlarge	52.61.63.179	172.31.6.224
Network Interface	**Machine Type**	**Public IP**	**Private IP**
eni-0157ffe121dd415e9	-	52.61.115.151	172.31.0.12
eni-0185461415c1269dc	-	-	172.31.100.12
eni-01b94432e40c9d867	-	15.200.162.169	172.31.0.11
eni-03d7561b4977cf20b	-	-	172.31.100.11
eni-0d38c172d8f51381c	-	52.61.63.179	172.31.6.224
AWS Security Group	**Machine Type**	**Public IP**	**Private IP**

Check Point
SOFTWARE TECHNOLOGIES

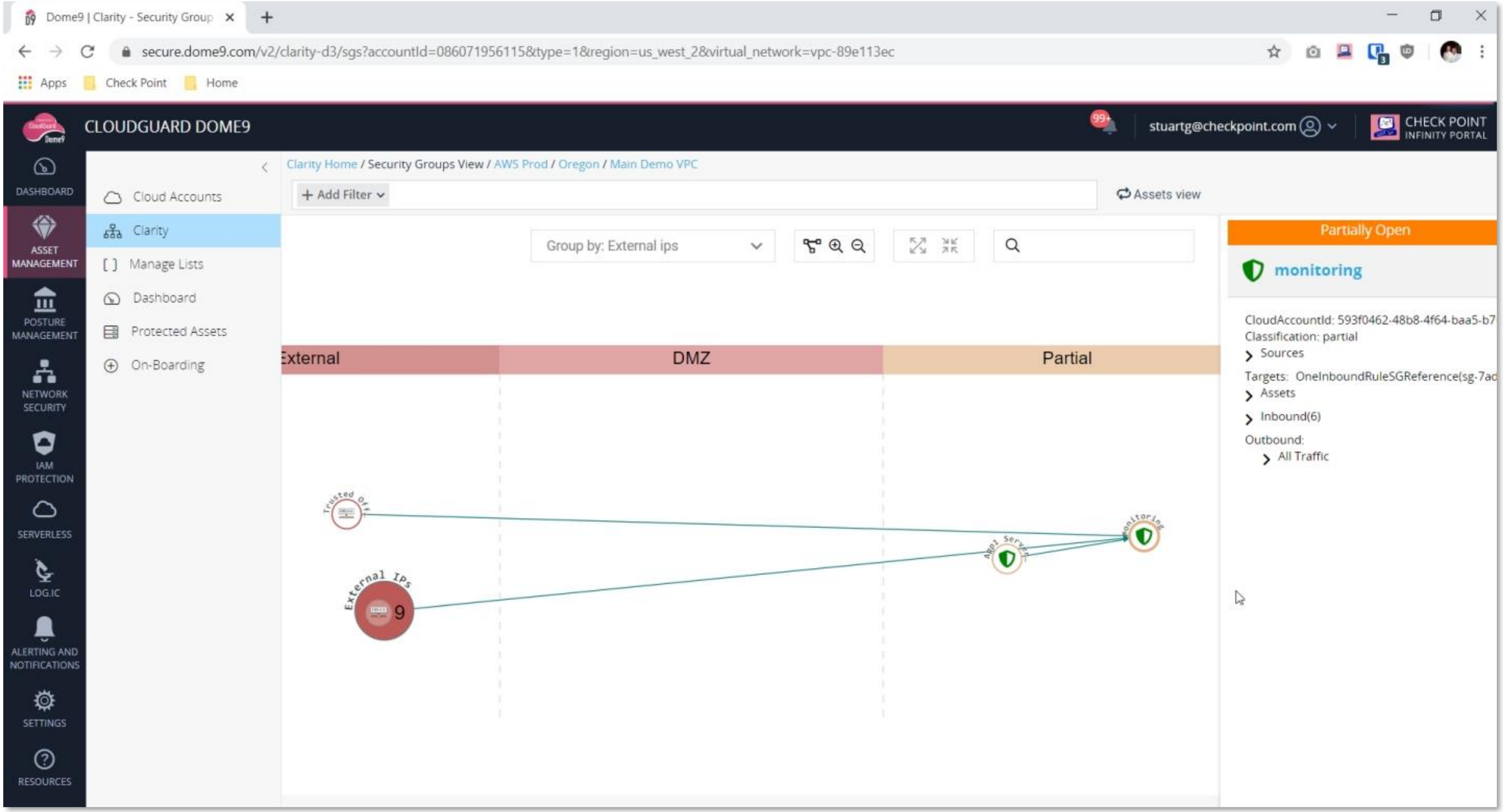
©2020 Check Point Software Technologies Ltd.



We're updating the view to help you get more done and improve performance. Switch to the old view.

Select region

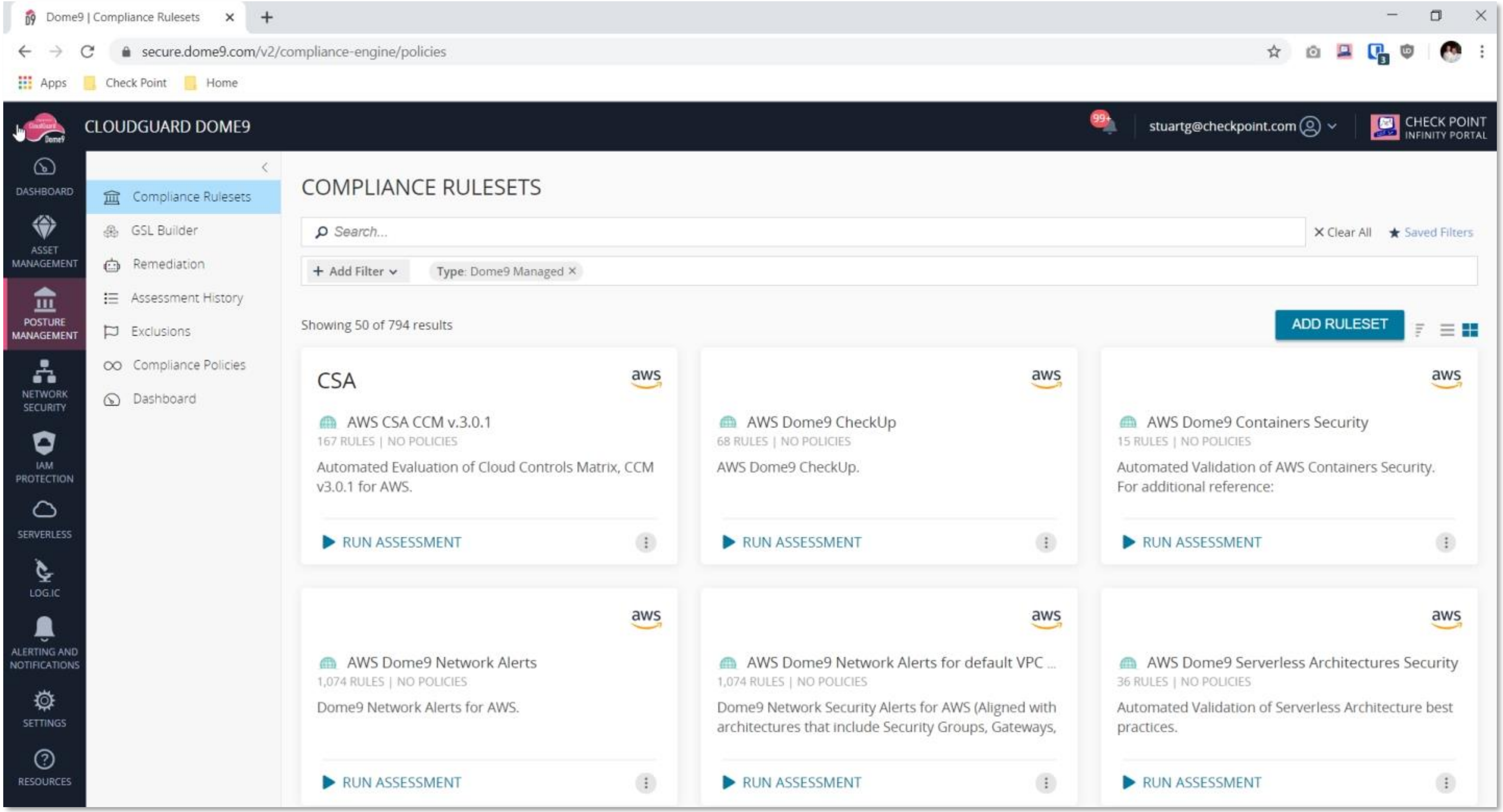
- AWS Prod (89)
- N. Virginia (4)
- Ireland (15)
- Oregon (66)
- Ohio (3)
- Stockholm (1)



Partially Open

monitoring

CloudAccountId: 593f0462-48b8-4f64-baa5-b7
Classification: partial
› Sources
Targets: OneInboundRuleSGReference(sg-7ad
› Assets
› Inbound(6)
Outbound:
› All Traffic



COMPLIANCE RULESETS

Type: Dome9 Managed

Showing 50 of 794 results

CSA

AWS CSA CCM v.3.0.1
167 RULES | NO POLICIES
Automated Evaluation of Cloud Controls Matrix, CCM v3.0.1 for AWS.

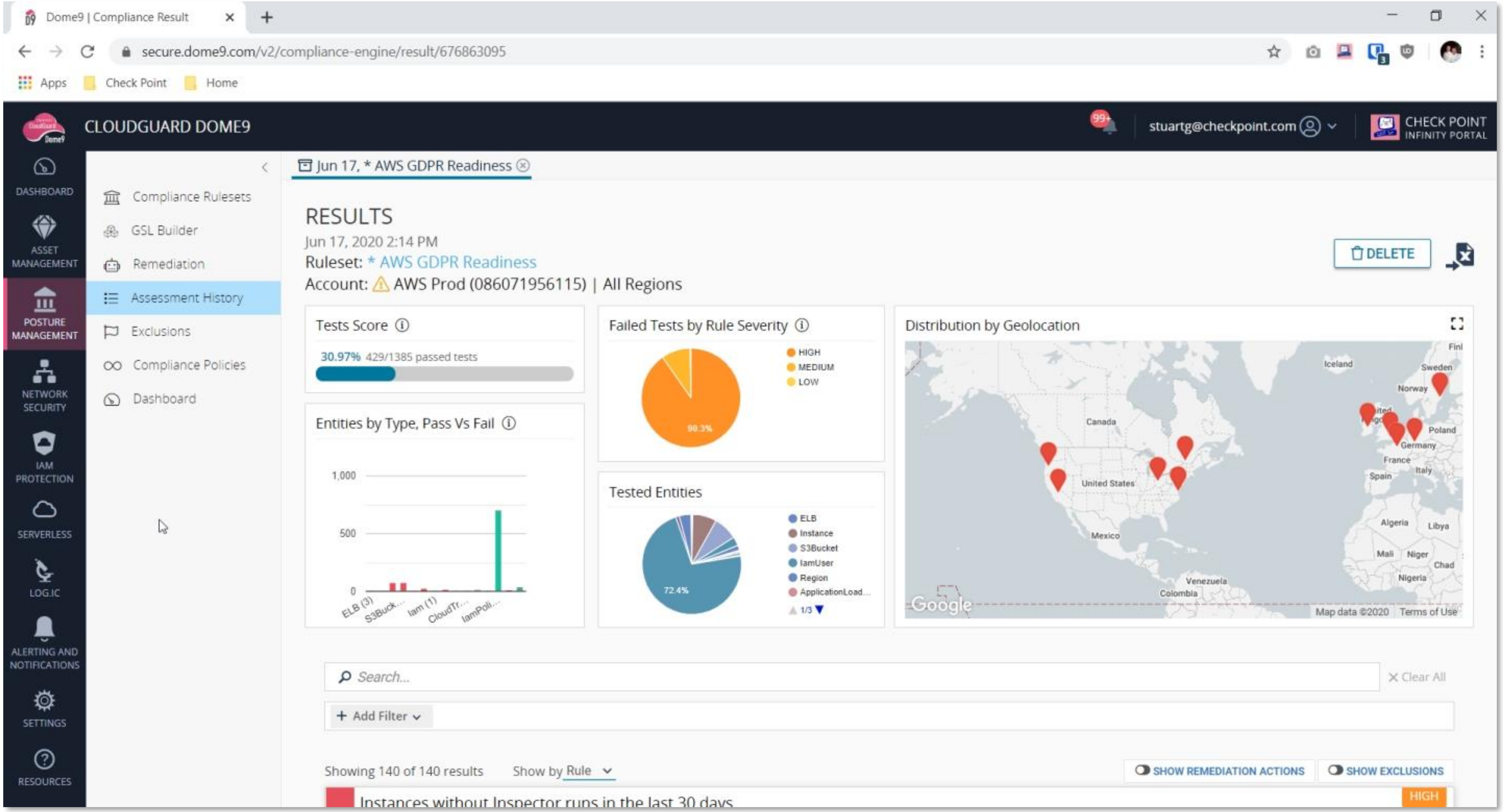
AWS Dome9 CheckUp
68 RULES | NO POLICIES
AWS Dome9 CheckUp.

AWS Dome9 Containers Security
15 RULES | NO POLICIES
Automated Validation of AWS Containers Security. For additional reference:

AWS Dome9 Network Alerts
1,074 RULES | NO POLICIES
Dome9 Network Alerts for AWS.

AWS Dome9 Network Alerts for default VPC ...
1,074 RULES | NO POLICIES
Dome9 Network Security Alerts for AWS (Aligned with architectures that include Security Groups, Gateways,

AWS Dome9 Serverless Architectures Security
36 RULES | NO POLICIES
Automated Validation of Serverless Architecture best practices.



RESULTS

Jun 17, 2020 2:14 PM

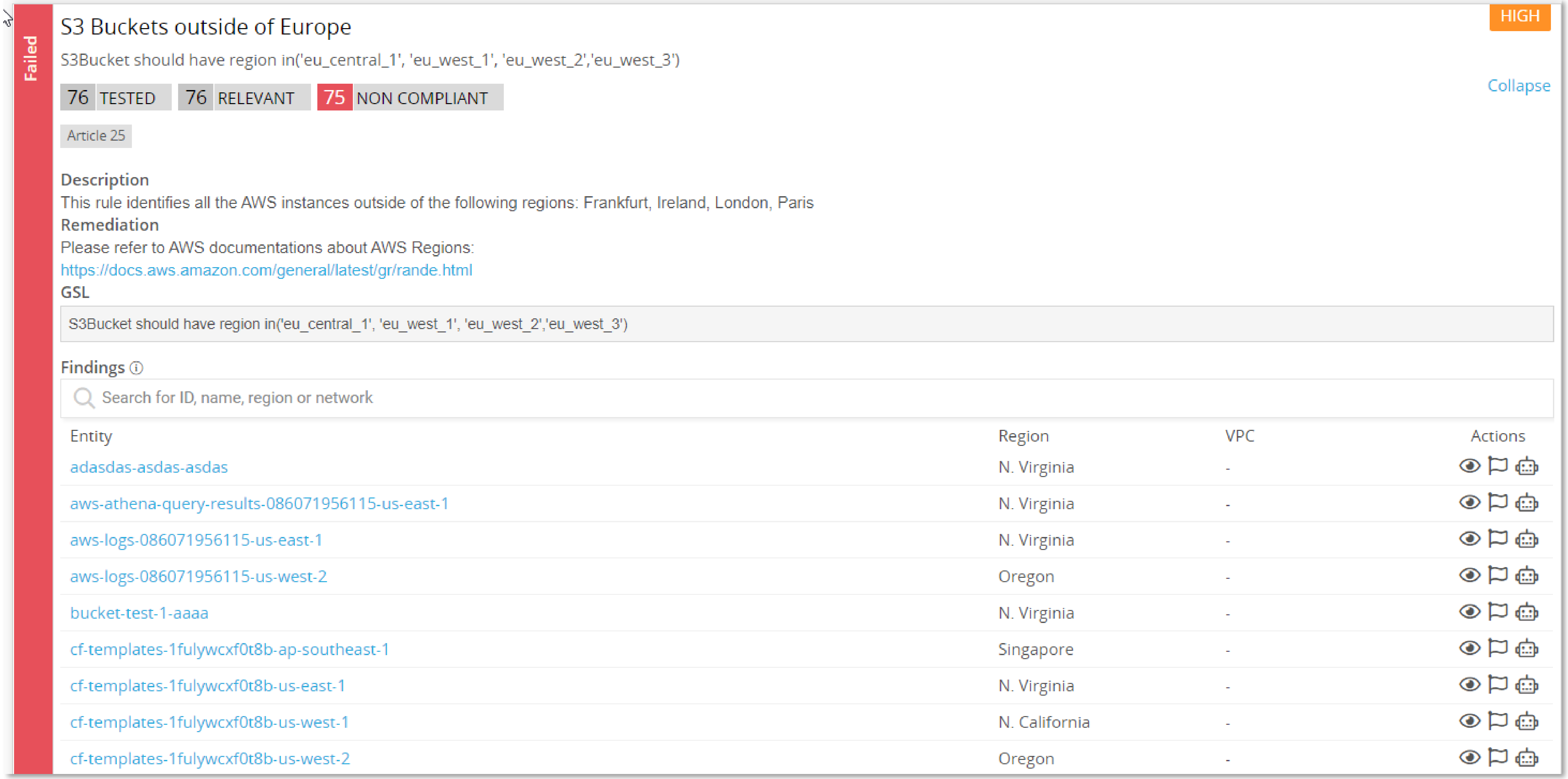
Ruleset: * AWS GDPR Readiness

Account: ⚠ AWS Prod (086071956115) | All Regions

Tests Score: 30.97% 429/1385 passed tests

Showing 140 of 140 results

Instances without Inspector runs in the last 30 days HIGH



Failed

S3 Buckets outside of Europe

HIGH

S3Bucket should have region in('eu_central_1', 'eu_west_1', 'eu_west_2','eu_west_3')

76 TESTED 76 RELEVANT 75 NON COMPLIANT

Collapse

Article 25

Description

This rule identifies all the AWS instances outside of the following regions: Frankfurt, Ireland, London, Paris

Remediation

Please refer to AWS documentations about AWS Regions:

https://docs.aws.amazon.com/general/latest/gr/rande.html

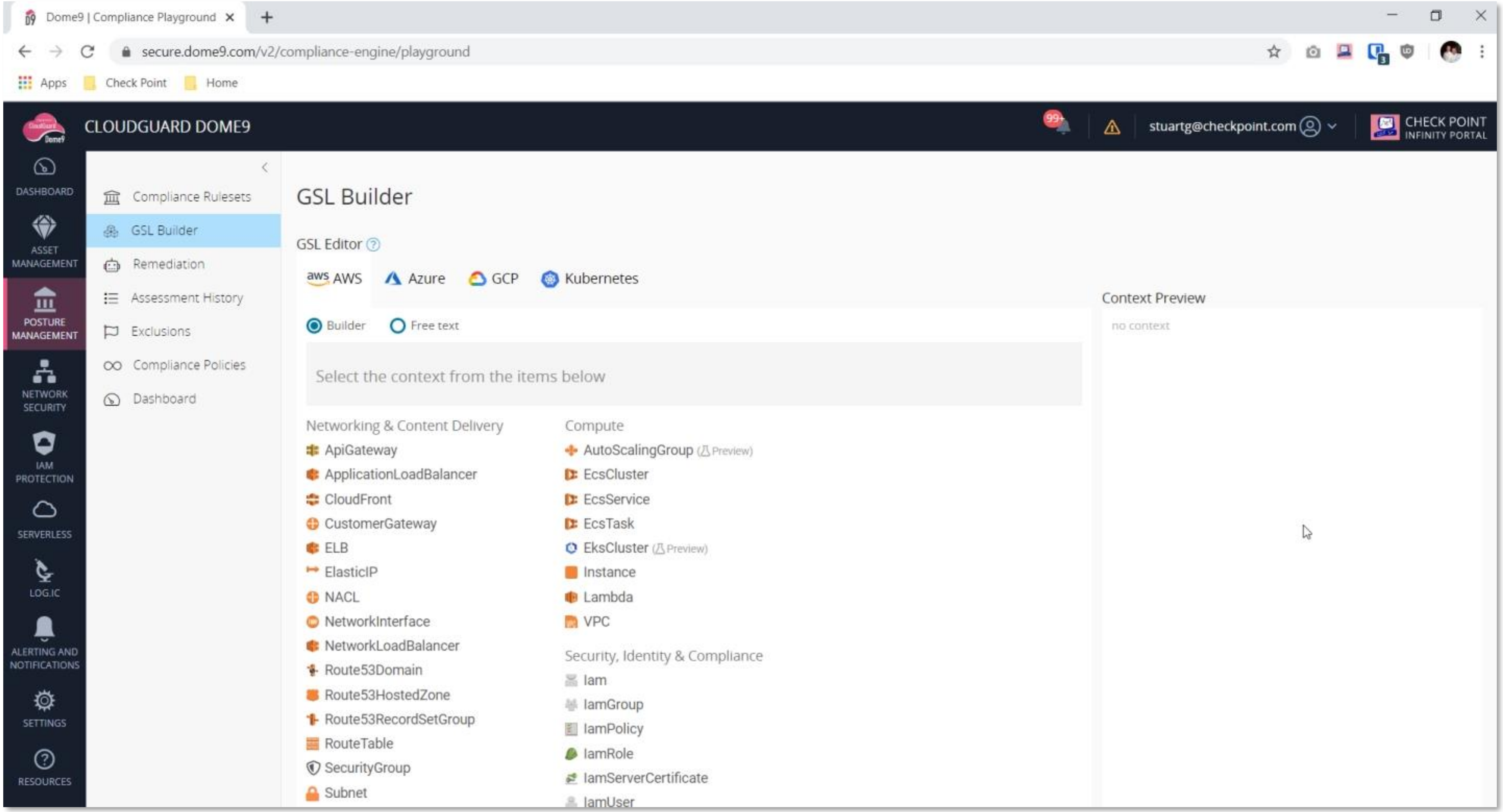
GSL

```
S3Bucket should have region in('eu_central_1', 'eu_west_1', 'eu_west_2','eu_west_3')
```

Findings ⓘ

Search for ID, name, region or network

Entity	Region	VPC	Actions
adasdas-asdas-asdas	N. Virginia	-	👁 ⚐ 🤖
aws-athena-query-results-086071956115-us-east-1	N. Virginia	-	👁 ⚐ 🤖
aws-logs-086071956115-us-east-1	N. Virginia	-	👁 ⚐ 🤖
aws-logs-086071956115-us-west-2	Oregon	-	👁 ⚐ 🤖
bucket-test-1-aaaa	N. Virginia	-	👁 ⚐ 🤖
cf-templates-1fulywcxf0t8b-ap-southeast-1	Singapore	-	👁 ⚐ 🤖
cf-templates-1fulywcxf0t8b-us-east-1	N. Virginia	-	👁 ⚐ 🤖
cf-templates-1fulywcxf0t8b-us-west-1	N. California	-	👁 ⚐ 🤖
cf-templates-1fulywcxf0t8b-us-west-2	Oregon	-	👁 ⚐ 🤖



Dome9 | Compliance Playground

secure.dome9.com/v2/compliance-engine/playground

Apps | Check Point | Home

CLOUDGUARD DOME9

stuartg@checkpoint.com

CHECK POINT INFINITY PORTAL

DASHBOARD
ASSET MANAGEMENT
POSTURE MANAGEMENT
NETWORK SECURITY
IAM PROTECTION
SERVERLESS
LOG.IC
ALERTING AND NOTIFICATIONS
SETTINGS
RESOURCES

- Compliance Rulesets
- GSL Builder
- Remediation
- Assessment History
- Exclusions
- Compliance Policies
- Dashboard

GSL Builder

GSL Editor

AWS | Azure | GCP | Kubernetes

● Builder ○ Free text

Select the context from the items below

Networking & Content Delivery
- ApiGateway
- ApplicationLoadBalancer
- CloudFront
- CustomerGateway
- ELB
- ElasticIP
- NACL
- NetworkInterface
- NetworkLoadBalancer
- Route53Domain
- Route53HostedZone
- Route53RecordSetGroup
- RouteTable
- SecurityGroup
- Subnet

Compute
- AutoScalingGroup (Preview)
- EcsCluster
- EcsService
- EcsTask
- EksCluster (Preview)
- Instance
- Lambda
- VPC

Security, Identity & Compliance
- Iam
- IamGroup
- IamPolicy
- IamRole
- IamServerCertificate
- IamUser

Context Preview

no context

Protect your Cloud Journey

Cloud Security Posture Management

Continuous Cloud Security Posture Management providing visibility, control & compliance across all assets and all clouds

Key capabilities:

- ✓ Gain visibility
- ✓ Customize policies
- ✓ Streamline and create ongoing process
- ✓ Evaluate results
- ✓ Take action

Security posture management

Continuous validation across compliance rules

Full visualization of cloud assets

Privileged Identity Protection

Everywhere:

aws Google Cloud Azure

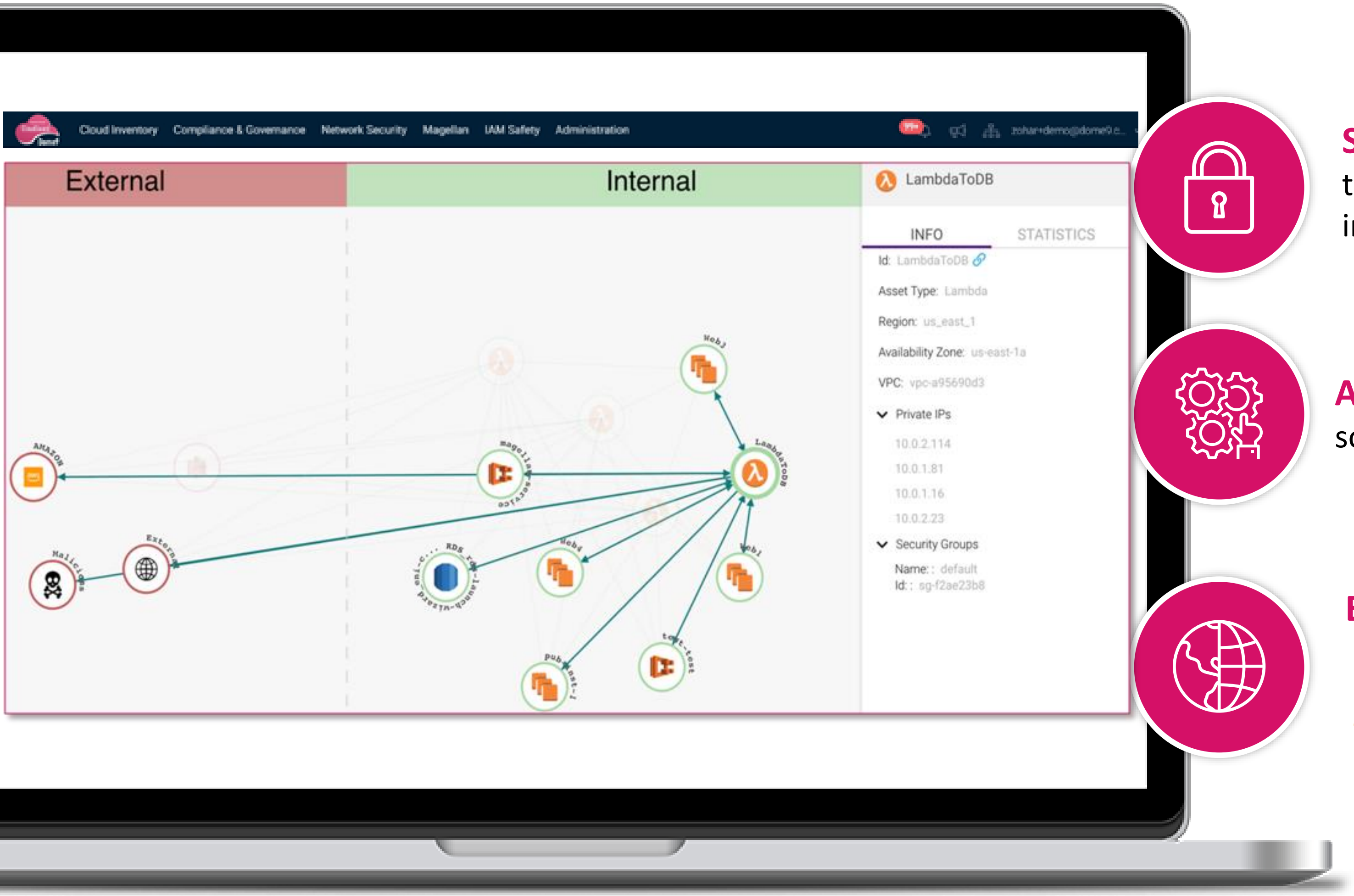
Trusted by:

cādence Omnyway TRADAIR datastream CONNEXION Centrify ZERO TRUST SECURITY

Check Point SOFTWARE TECHNOLOGIES

Cloud Intelligence & Threat Hunting

Transforming cloud big data to hi-definition intelligence and actionable security logic.



λ LambdaToDB

INFO | STATISTICS

Id: LambdaToDB

Asset Type: Lambda

Region: us_east_1

Availability Zone: us-east-1a

VPC: vpc-a95690d3

Private IPs

10.0.2.114
10.0.1.81
10.0.1.16
10.0.2.23

Security Groups

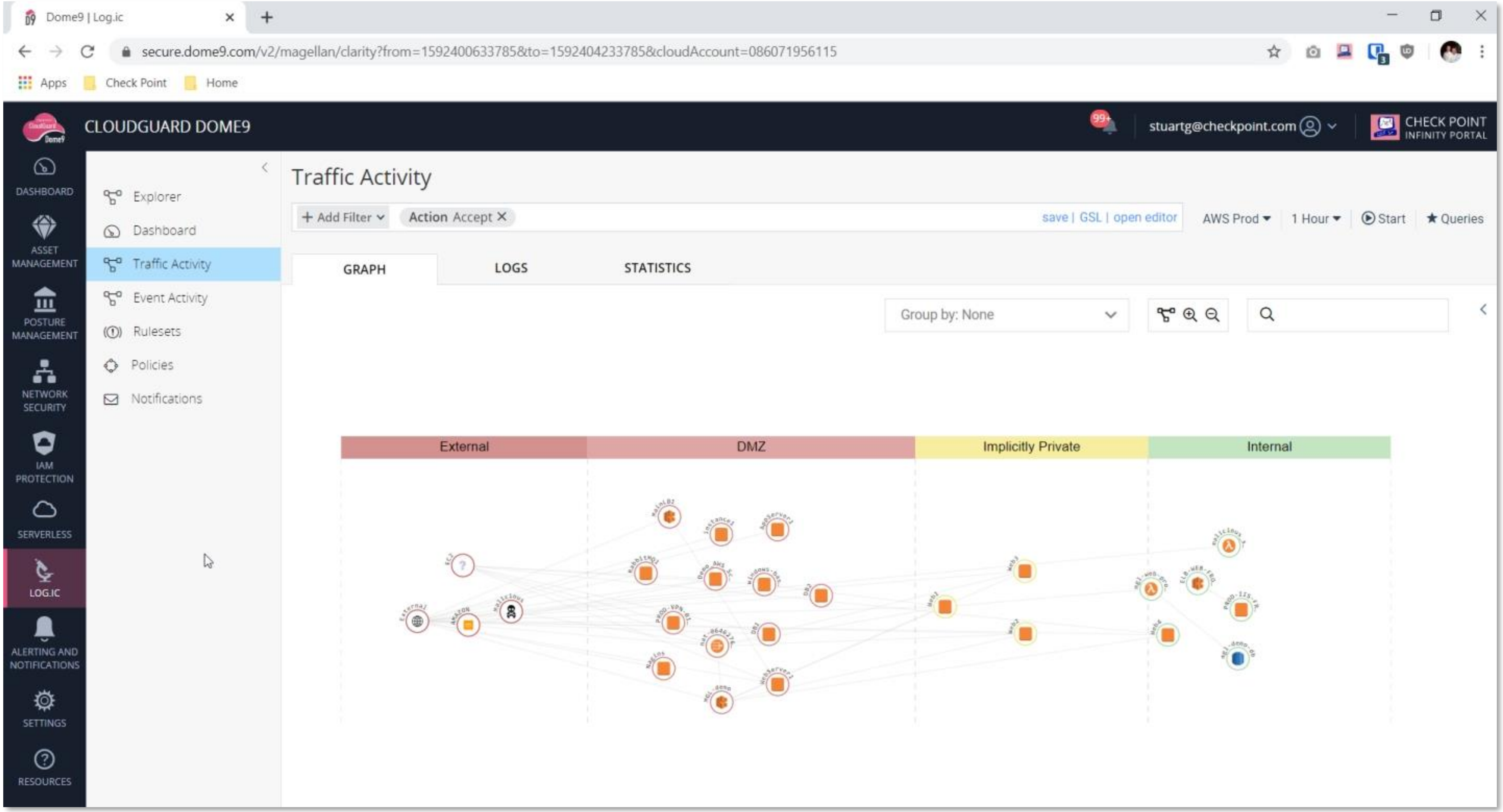
Name: : default
Id: : sg-f2ae23b8

Security: Detects application and network anomalies in real time, and quarantines threats utilizing the world's largest threat intelligence feed.

Automated: out of the box visibility and threat hunting with sophisticated learning algorithms and pre-built rules.

Everywhere:

aws Google Cloud Azure



secure.dome9.com/v2/magellan/clarity?from=1592400633785&to=1592404233785&cloudAccount=086071956115

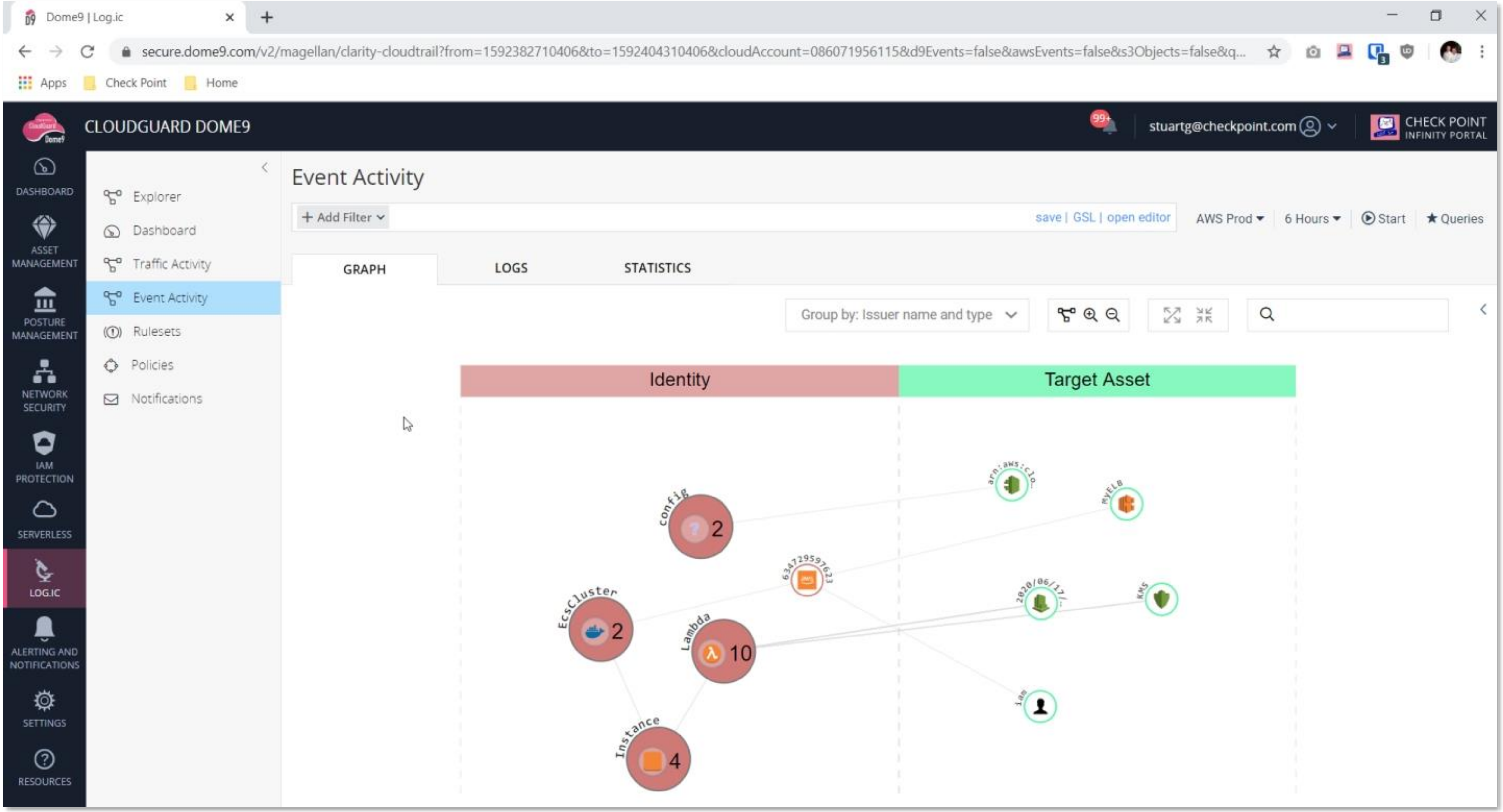
Traffic Activity

Action Accept ✕

AWS Prod

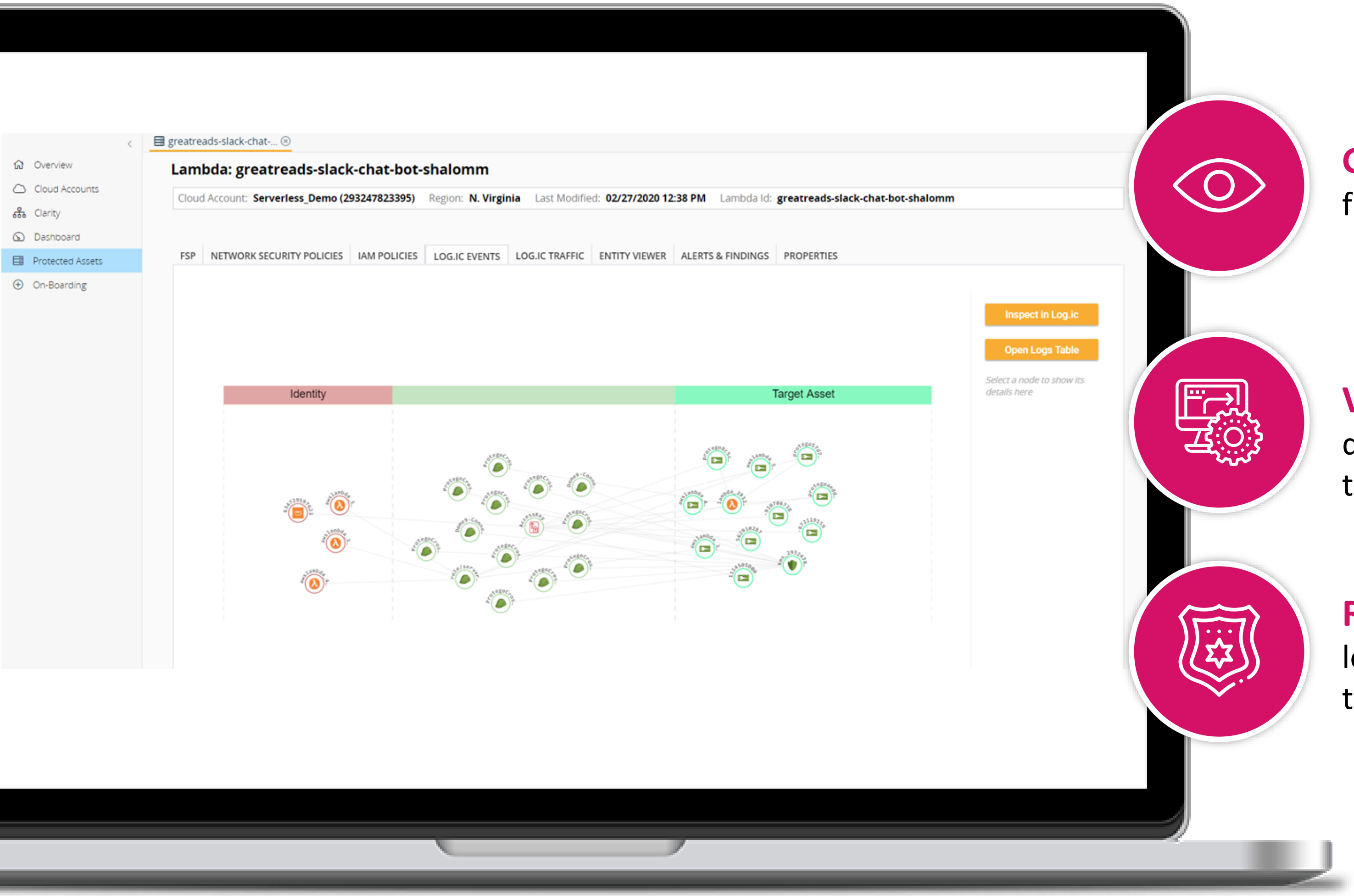
1 Hour

Group by: None


Dome9 | Log.ic
secure.dome9.com/v2/magellan/clarity-cloudtrail?from=1592382710406&to=1592404310406&cloudAccount=086071956115&d9Events=false&awsEvents=false&s3Objects=false&q...
Apps
Check Point
Home
CLOUDGUARD DOME9
99+
stuartg@checkpoint.com
CHECK POINT
INFINITY PORTAL
DASHBOARD
ASSET MANAGEMENT
POSTURE MANAGEMENT
NETWORK SECURITY
IAM PROTECTION
SERVERLESS
LOG.IC
ALERTING AND NOTIFICATIONS
SETTINGS
RESOURCES
Explorer
Dashboard
Traffic Activity
Event Activity
Rulesets
Policies
Notifications
Event Activity
+ Add Filter
save | GSL | open editor
AWS Prod
6 Hours
Start
★ Queries
GRAPH
LOGS
STATISTICS
Group by: Issuer name and type
Identity
Target Asset
config
2
634729597623
EcsCluster
2
Lambda
10
Instance
4
arn:aws:clo...
myELB
2020/06/17/...
KMS
iam

Cloud Workload Protection Platform

Automated security for cloud workloads, including Virtual machines, Containers & Functions



Lambda: greatreads-slack-chat-bot-shalomm

Cloud Account: Serverless_Demo (293247823395) Region: N. Virginia Last Modified: 02/27/2020 12:38 PM Lambda Id: greatreads-slack-chat-bot-shalomm

Select a node to show its details here

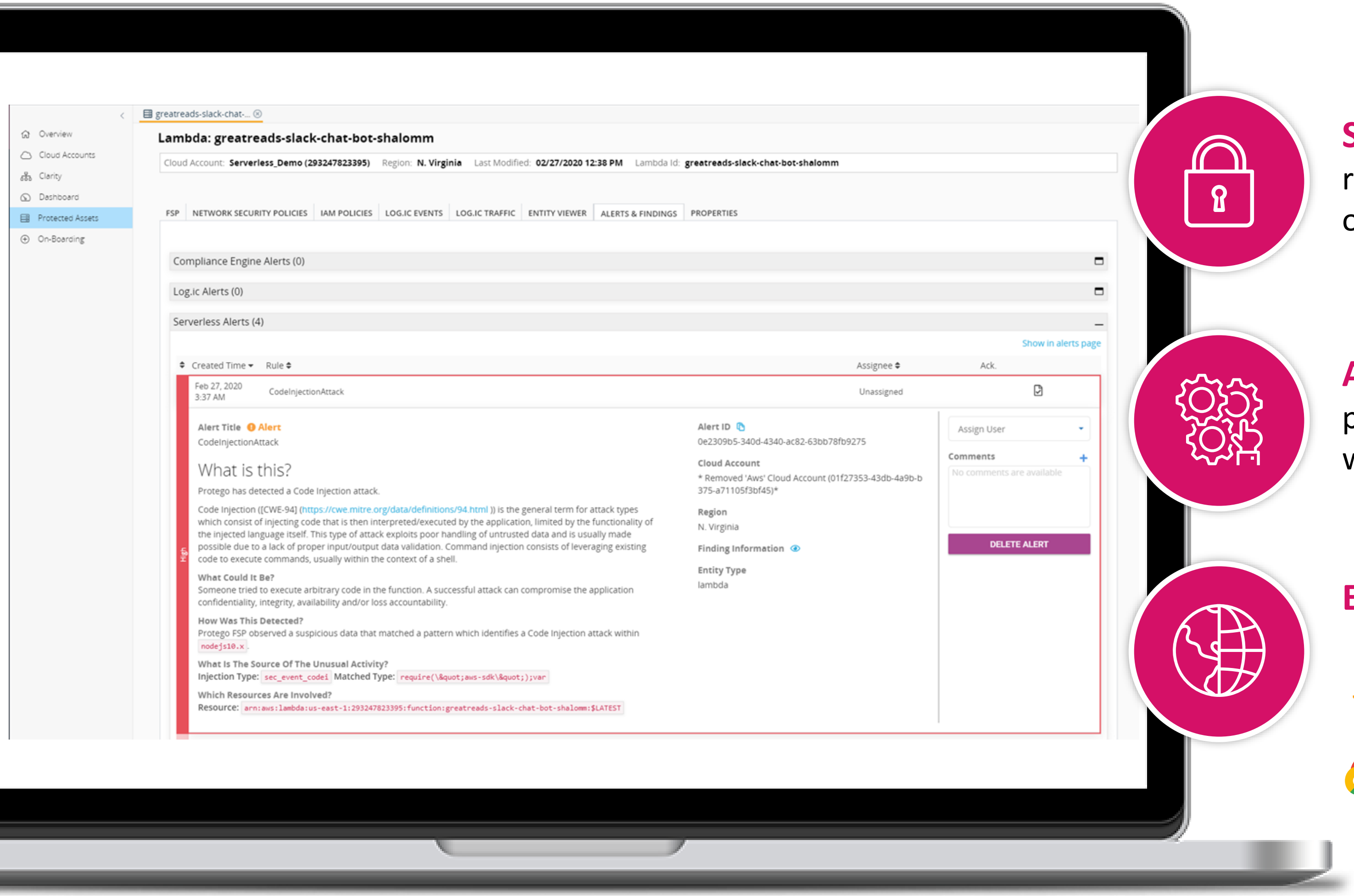
Governance: Define compliance rules and enforce guardrails from CI/CD to production.

Vulnerability Management: Scan code, images and cloud deployment templates to detect vulnerabilities and embedded threats.

Run time Protection: multi-layer cloud native protection leveraging pattern matching, whitelisting & blacklisting applied at the workload level.

Cloud Workload Protection Platform

Automated security for cloud workloads, including Virtual machines, Containers & Functions



Lambda: greatreads-slack-chat-bot-shalomm

Cloud Account: **Serverless_Demo (293247823395)** Region: **N. Virginia** Last Modified: **02/27/2020 12:38 PM** Lambda Id: **greatreads-slack-chat-bot-shalomm**

Compliance Engine Alerts (0)

Log.ic Alerts (0)

Serverless Alerts (4)

Created Time	Rule	Assignee	Ack.
Feb 27, 2020 3:37 AM	CodeInjectionAttack	Unassigned	

Alert Title Alert

CodeInjectionAttack

What is this?

Protego has detected a Code Injection attack.

Code Injection ([CWE-94] (https://cwe.mitre.org/data/definitions/94.html)) is the general term for attack types which consist of injecting code that is then interpreted/executed by the application, limited by the functionality of the injected language itself. This type of attack exploits poor handling of untrusted data and is usually made possible due to a lack of proper input/output data validation. Command injection consists of leveraging existing code to execute commands, usually within the context of a shell.

What Could It Be?
Someone tried to execute arbitrary code in the function. A successful attack can compromise the application confidentiality, integrity, availability and/or loss accountability.

How Was This Detected?
Protego FSP observed a suspicious data that matched a pattern which identifies a Code Injection attack within `nodejs10.x`.

What Is The Source Of The Unusual Activity?
Injection Type: `sec_event_codei` **Matched Type:** `require(\&quot;aws-sdk\&quot;);var`

Which Resources Are Involved?
Resource: `arn:aws:lambda:us-east-1:293247823395:function:greatreads-slack-chat-bot-shalomm:$LATEST`

Alert ID
0e2309b5-340d-4340-ac82-63bb78fb9275

Cloud Account
* Removed 'Aws' Cloud Account (01f27353-43db-4a9b-b375-a71105f3bf45)*

Region
N. Virginia

Finding Information

Entity Type
lambda

No comments are available

Security: Full context of the protected workload from code to run time delivers maximum security and accuracy with minimal overhead.

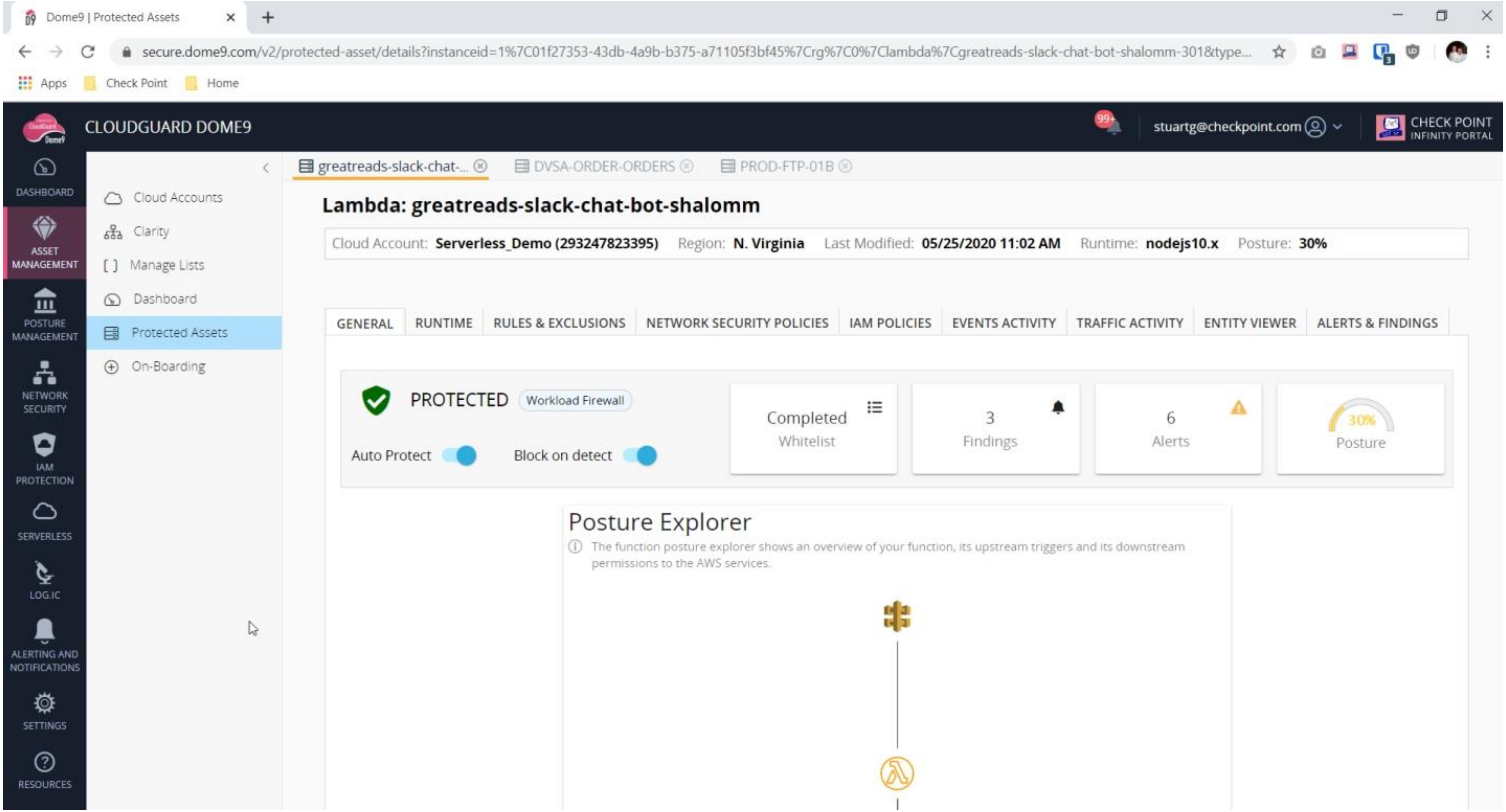
Automated: Driven by machine learning and code analysis, protection profiles are created and maintained automatically while adapting to application changes.

Everywhere:

aws Azure

Google Cloud

docker



Dome9 | Protected Assets

secure.dome9.com/v2/protected-asset/details?instanceid=1%7C01f27353-43db-4a9b-b375-a71105f3bf45%7Crg%7C0%7Clambda%7Cgreatreads-slack-chat-bot-shalomm-301&type...

Apps · Check Point · Home

CLOUDGUARD DOME9

stuartg@checkpoint.com

CHECK POINT INFINITY PORTAL

Lambda: greatreads-slack-chat-bot-shalomm

Cloud Account: **Serverless_Demo (293247823395)** Region: **N. Virginia** Last Modified: **05/25/2020 11:02 AM** Runtime: **nodejs10.x** Posture: **30%**

PROTECTED Workload Firewall

Auto Protect ● Block on detect ●

Completed Whitelist

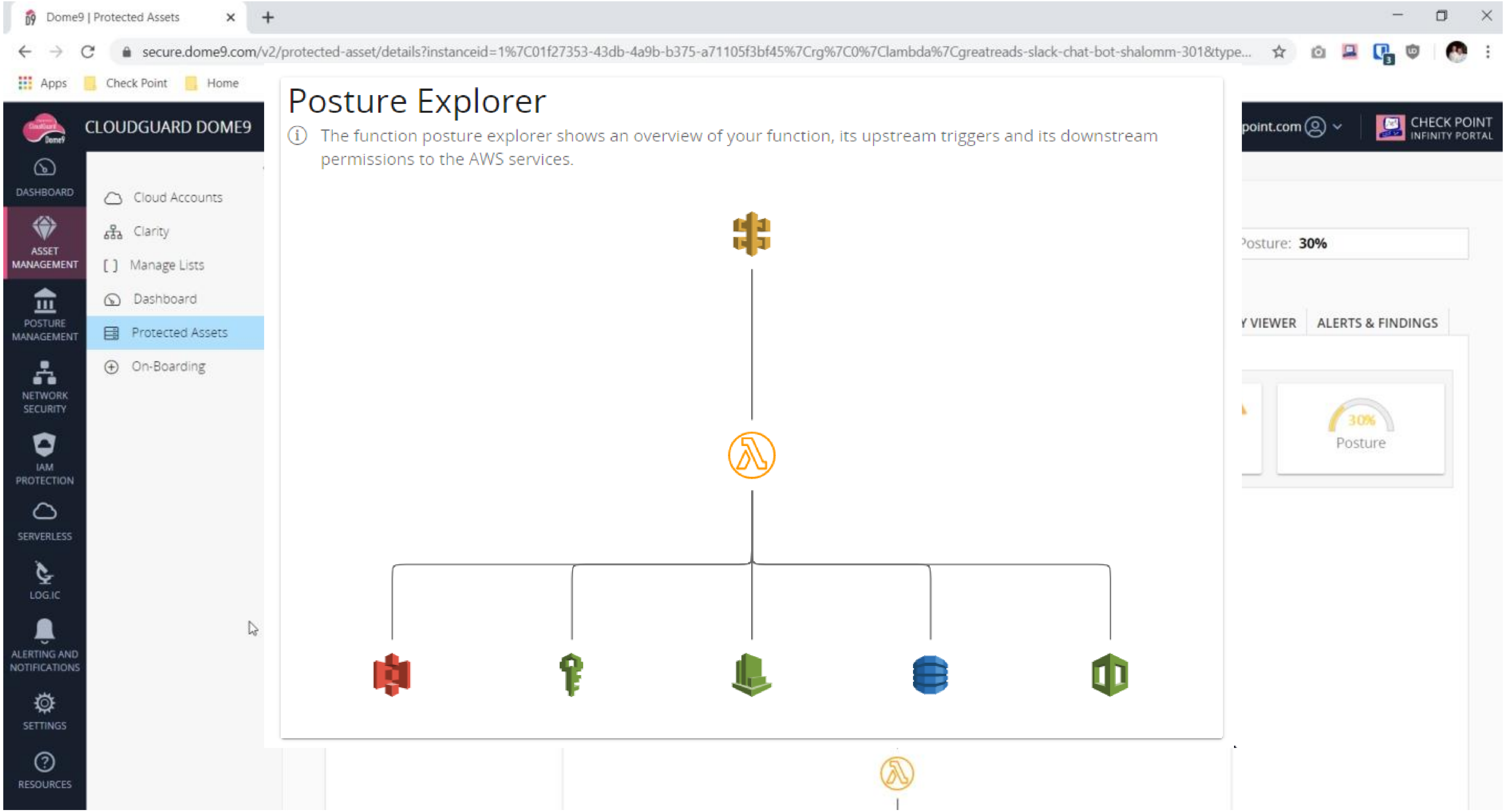
3 Findings

6 Alerts

30% Posture

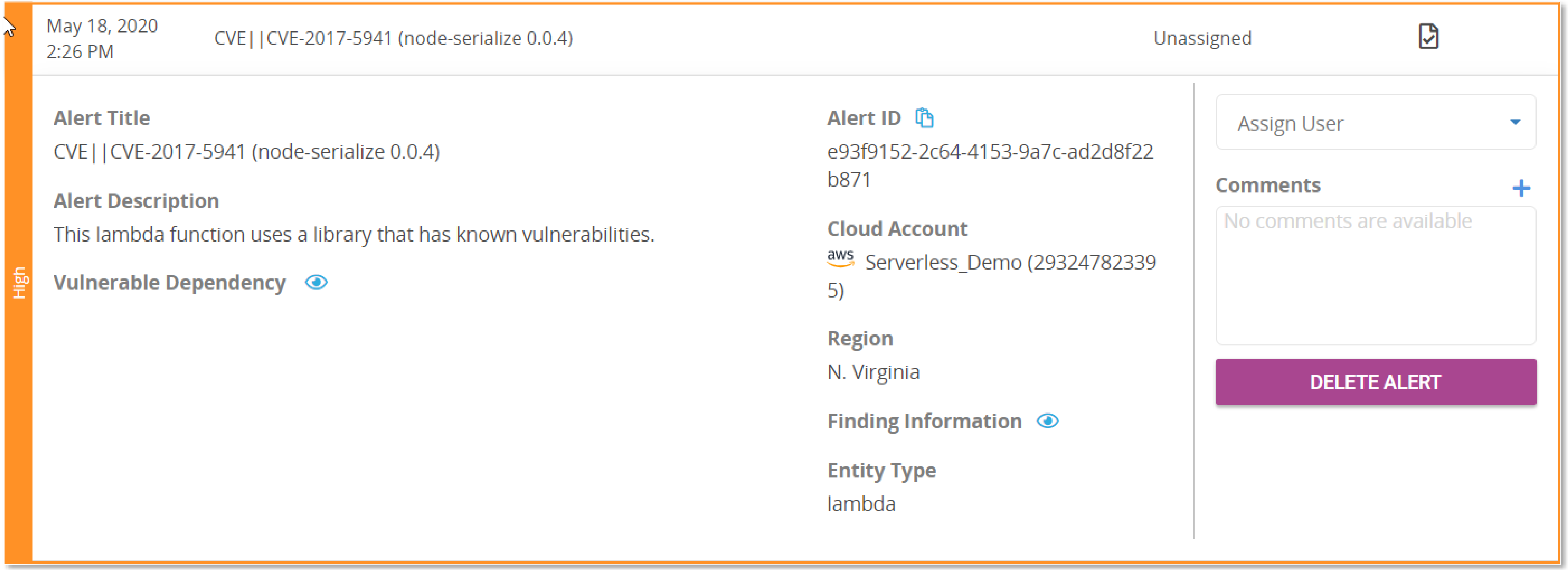
Posture Explorer

The function posture explorer shows an overview of your function, its upstream triggers and its downstream permissions to the AWS services.



Posture Explorer

ⓘ The function posture explorer shows an overview of your function, its upstream triggers and its downstream permissions to the AWS services.



May 18, 2020
2:26 PM

CVE||CVE-2017-5941 (node-serialize 0.0.4)

Unassigned

Alert Title
CVE||CVE-2017-5941 (node-serialize 0.0.4)

Alert Description
This lambda function uses a library that has known vulnerabilities.

Vulnerable Dependency

Alert ID
e93f9152-2c64-4153-9a7c-ad2d8f22b871

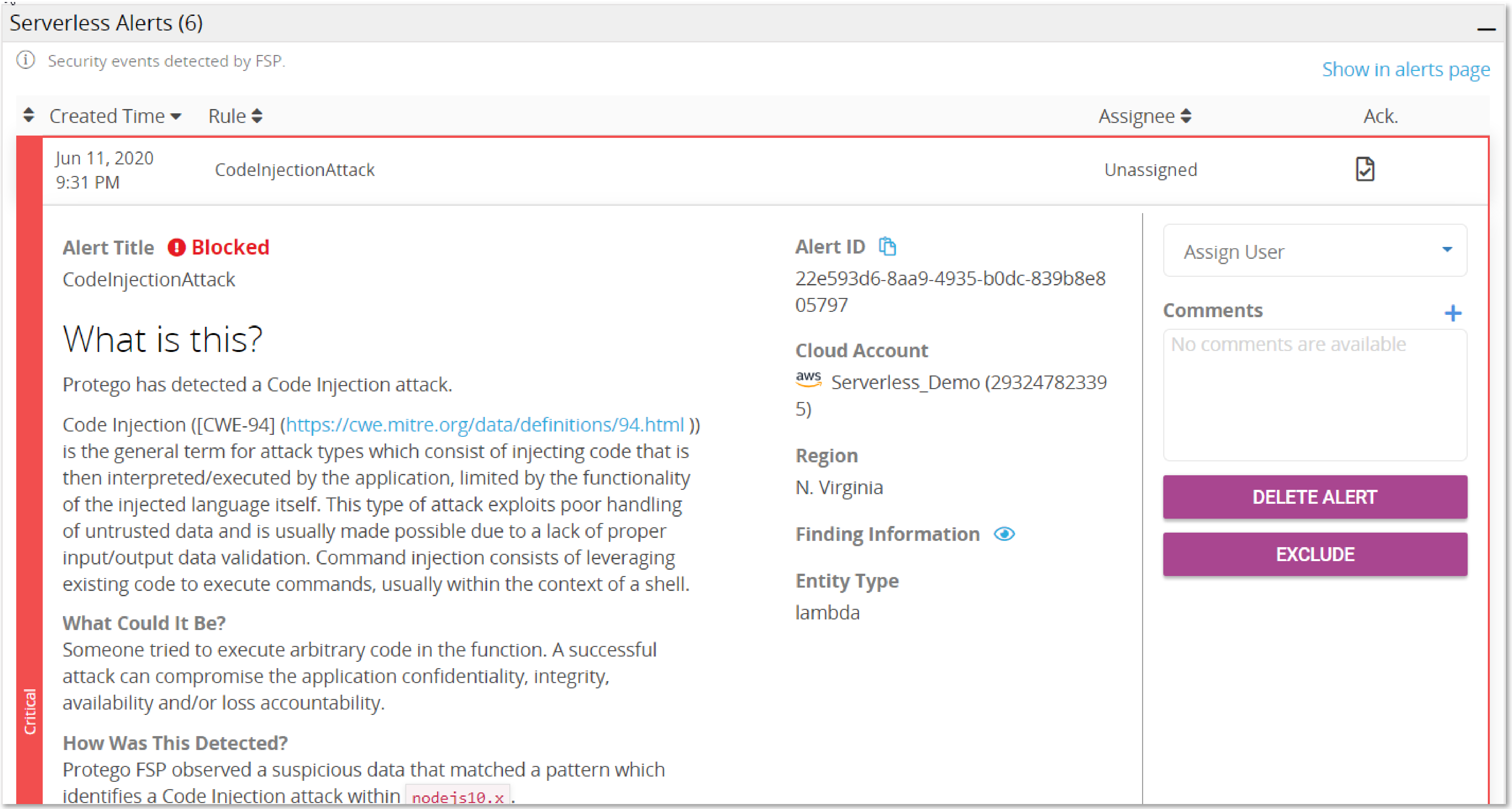
Cloud Account
aws Serverless_Demo (293247823395)

Region
N. Virginia

Finding Information

Entity Type
lambda

Comments
No comments are available



Serverless Alerts (6)

ⓘ Security events detected by FSP.

Show in alerts page

Created Time	Rule	Assignee	Ack.
Jun 11, 2020 9:31 PM	CodeInjectionAttack	Unassigned	

Critical

Alert Title **Blocked**

CodeInjectionAttack

What is this?

Protego has detected a Code Injection attack.

Code Injection ([CWE-94] (https://cwe.mitre.org/data/definitions/94.html)) is the general term for attack types which consist of injecting code that is then interpreted/executed by the application, limited by the functionality of the injected language itself. This type of attack exploits poor handling of untrusted data and is usually made possible due to a lack of proper input/output data validation. Command injection consists of leveraging existing code to execute commands, usually within the context of a shell.

What Could It Be?

Someone tried to execute arbitrary code in the function. A successful attack can compromise the application confidentiality, integrity, availability and/or loss accountability.

How Was This Detected?

Protego FSP observed a suspicious data that matched a pattern which identifies a Code Injection attack within `nodejs10.x`.

Alert ID

22e593d6-8aa9-4935-b0dc-839b8e805797

Cloud Account

aws Serverless_Demo (293247823395)

Region

N. Virginia

Finding Information

Entity Type

lambda

Assign User

Comments +

No comments are available

Protect your Cloud Journey

Workload Protection

Automated runtime protection for cloud workloads including serverless, containers, VMs, and other microservices

Key capabilities:

- ✓ Automated protection, development & runtime
- ✓ Automatic profiling of application behavior
- ✓ Zero trust boundaries
- ✓ No latency

Vulnerability scanning during CI/CD

Runtime protection

Detect over permissive functions

Auto-remediation

Everywhere:

aws Azure Google Cloud

docker

Trusted by:

Best Friends
Los Angeles

CHECK POINT
CloudGuard

Security

High Fidelity cloud security posture management and advanced cloud threat

Automated

From automated deployment to auto generated protection policies during CI/CD and in runtime

prevention

Everywhere

From CI/CD to production, from private to public clouds and across any workload

UNIFIED CLOUD NATIVE SECURITY PLATFORM

Check Point
SOFTWARE TECHNOLOGIES

Check Point®
SOFTWARE TECHNOLOGIES LTD

THANK YOU

QUESTIONS?