
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Secure Your Serverless Cloud Infrastructure

Ryan MacLennan
Technical Marketing Engineer
DEVNET-1075

Cisco Webex App

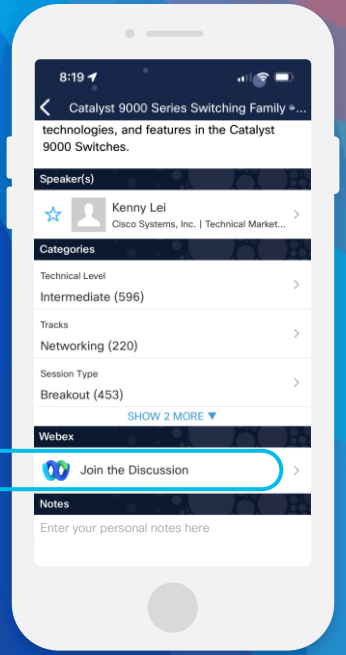
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 9, 2023.

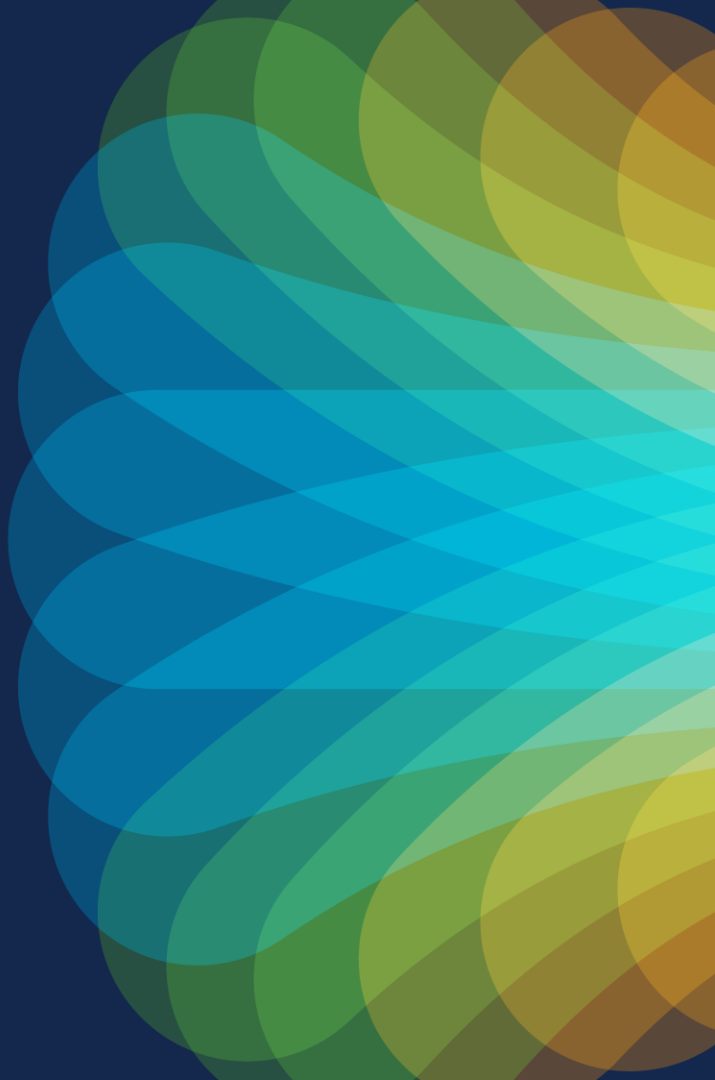


https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1075

Agenda

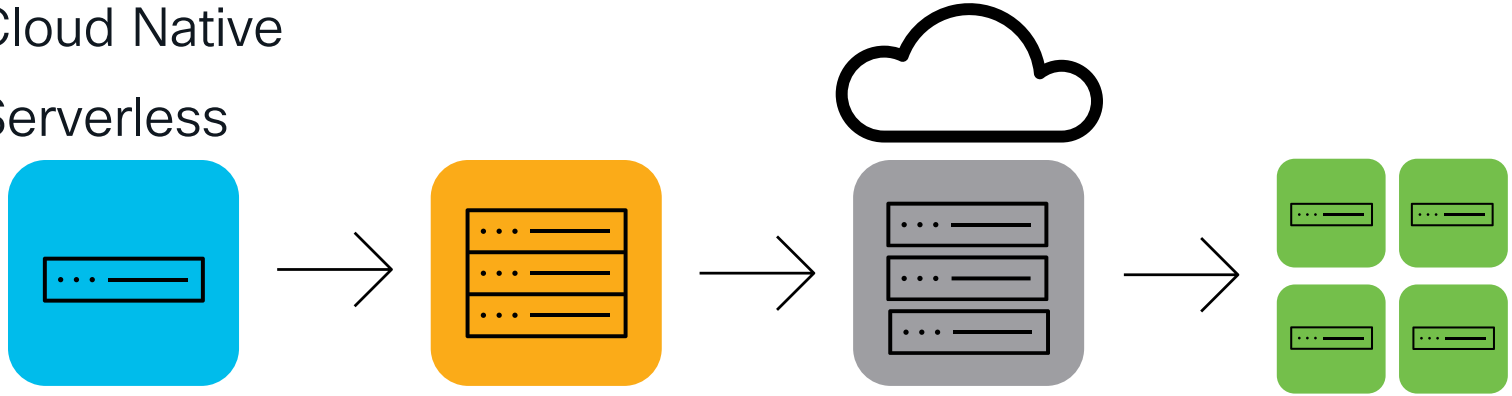
- Understanding Serverless
- Difficulty of Securing Serverless
- What Security Do You Need
- How We Fit
  - Panoptica
  - Radware Cloud WAF
  - Secure Cloud Insights/Analytics
  - AppDynamics

Understanding Serverless



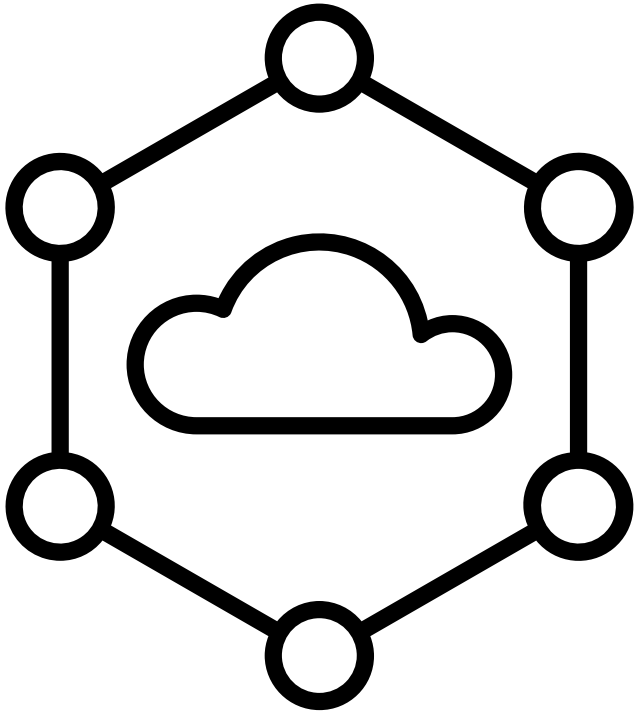
Evolution of Application Architectures

- Monolithic
- Service Oriented (Separation of concerns)
- Microservices
- Cloud Native
- Serverless



Serverless Is Multiple Services In One

- Backend as a Server (BaaS)
- Function as a Service (FaaS)
- Hosting
- Containers
- API Gateways



Why Talk About Serverless?

Companies using Serverless

*Regardless of cloud provider

Stack Overflow Questions

3+

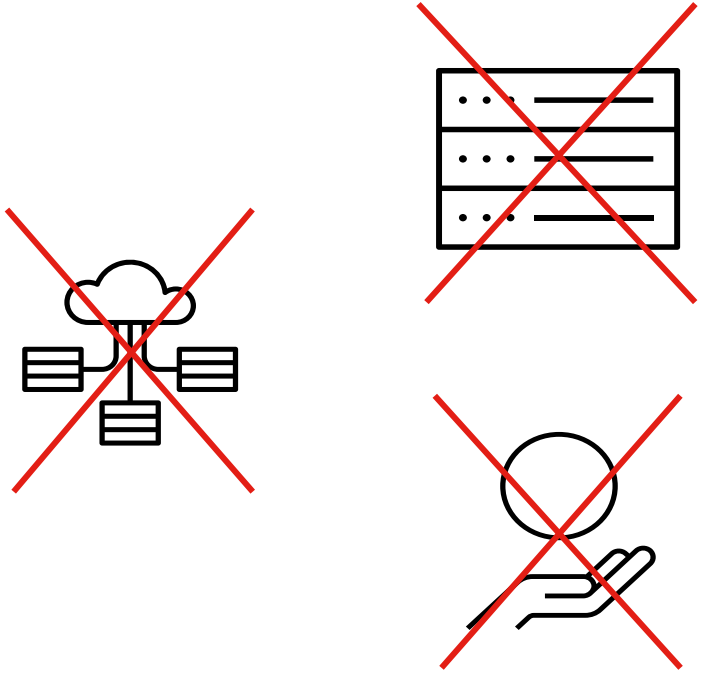
Languages

Used by 60% of large organizations

Difficulty of Securing Serverless

Traditional Security Does Not Apply

- No servers
- No networking
- No control



What Security Do You Need?

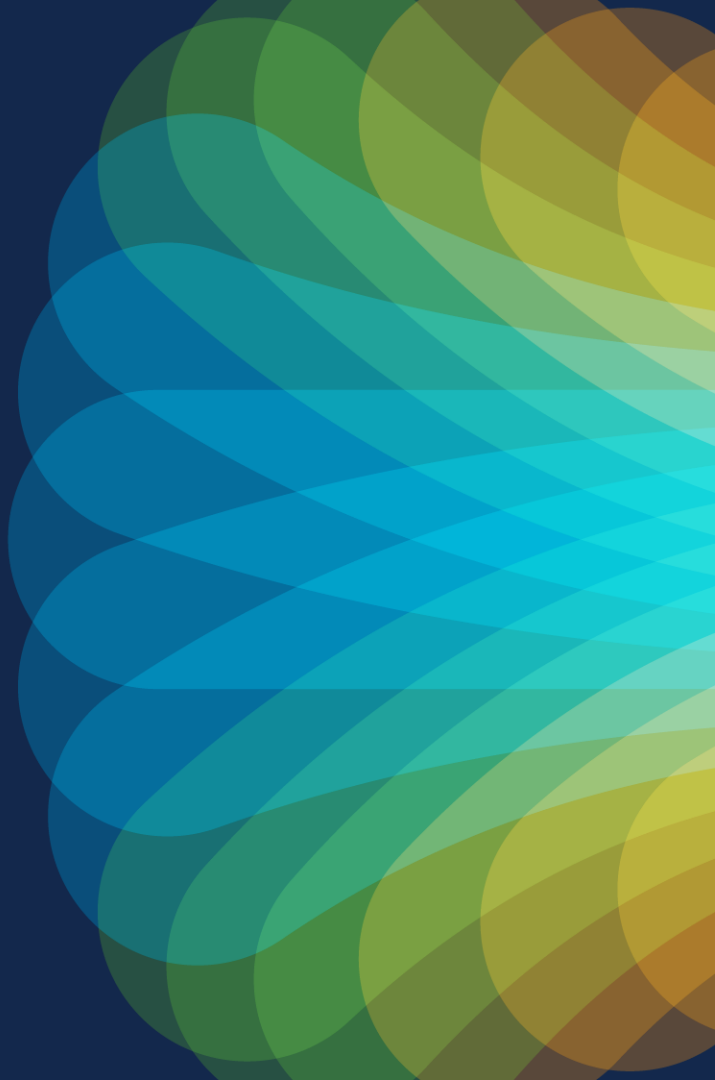
Three Components of Serverless Security

- Identity Access Management (IAM)
- Resource Management

- Continuous Integration/ Continuous Deployment (CI/CD)
- Code Vulnerabilities

- Distributed Denial of Service (DDoS)
- Bots
- Web Application Firewall (WAF)
- API Endpoints

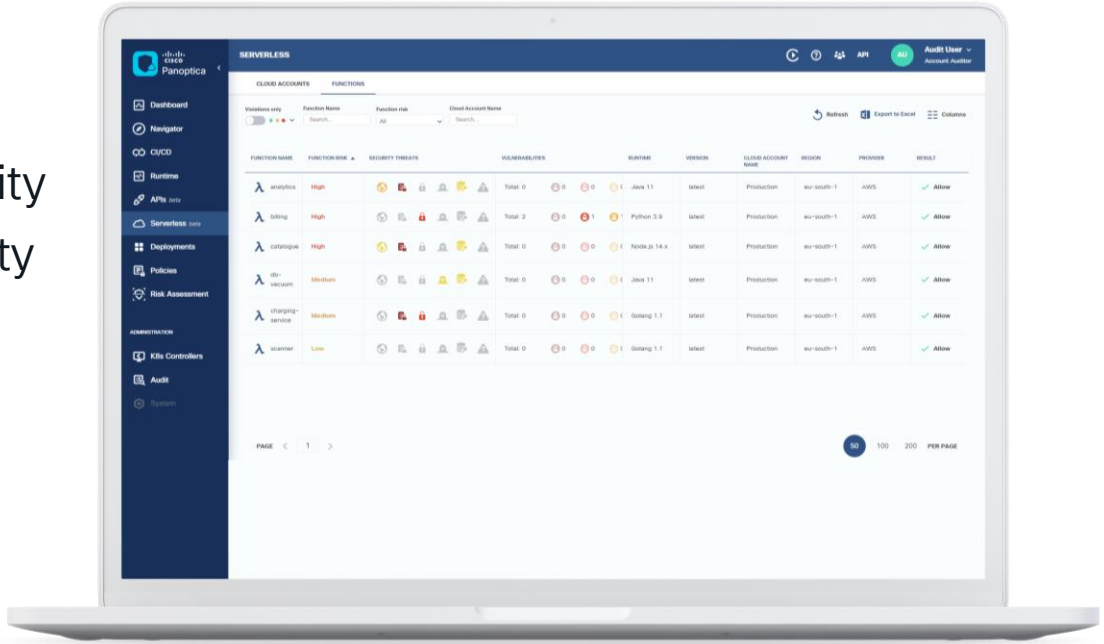
How We Fit



Panoptica

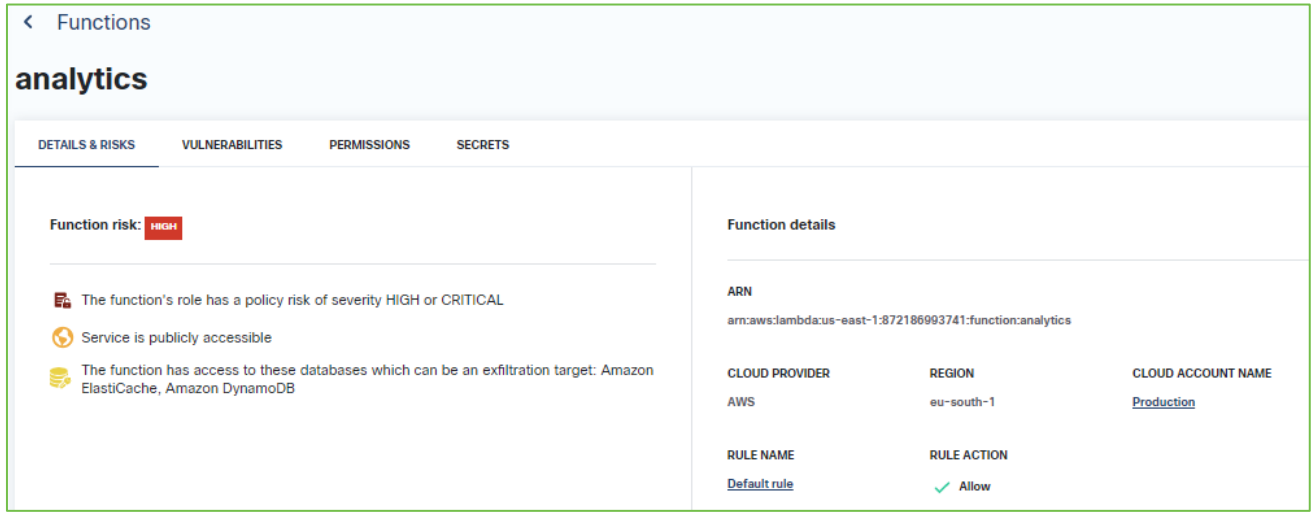
Panoptica Overview

- Cloud-Native Application Security, Simplified
- Features:
  - API Security
  - Cloud Function Security
  - CI/CD Pipeline Security



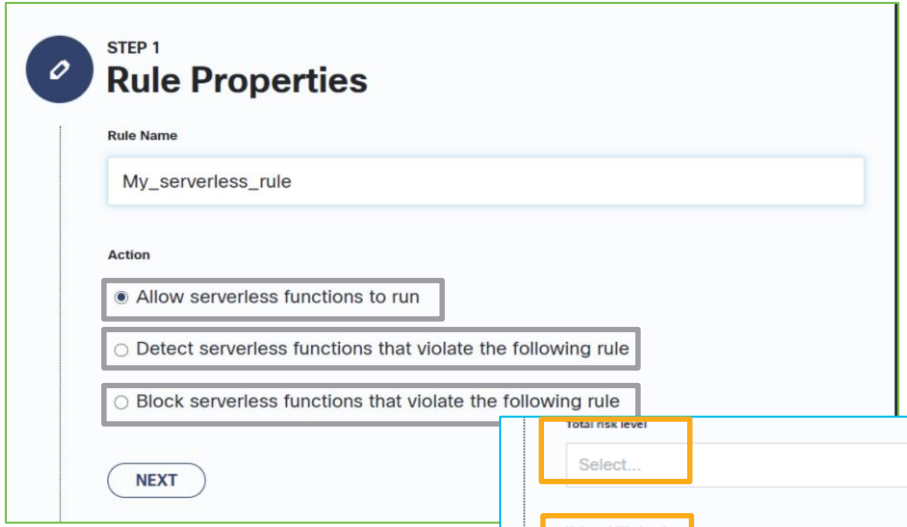
Panoptica Scans Functions For Threats & Vulnerabilities

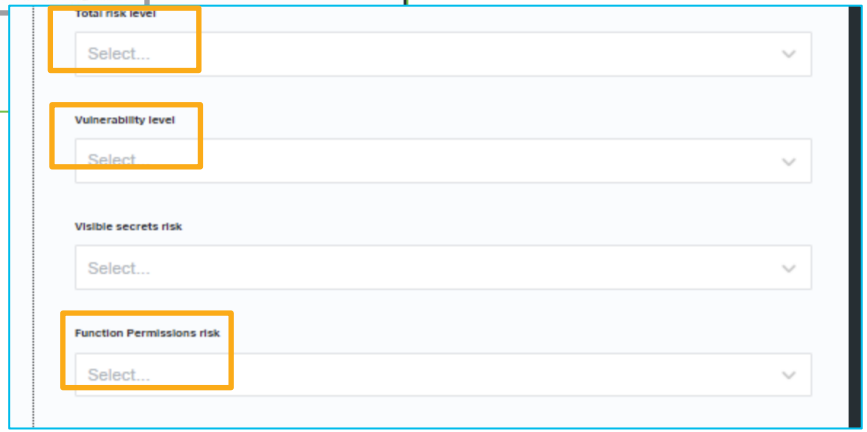
- Serverless is not scannable by regular vulnerability scanners
- Identifies and labels types of threats a serverless function has



Panoptica Has Access Controls For Cloud Functions

- ACLs can:
  - Allow
  - Detect
  - Block
- Based on:
  - Risk level
  - Vulnerability level
  - Permissions
  - Many more...



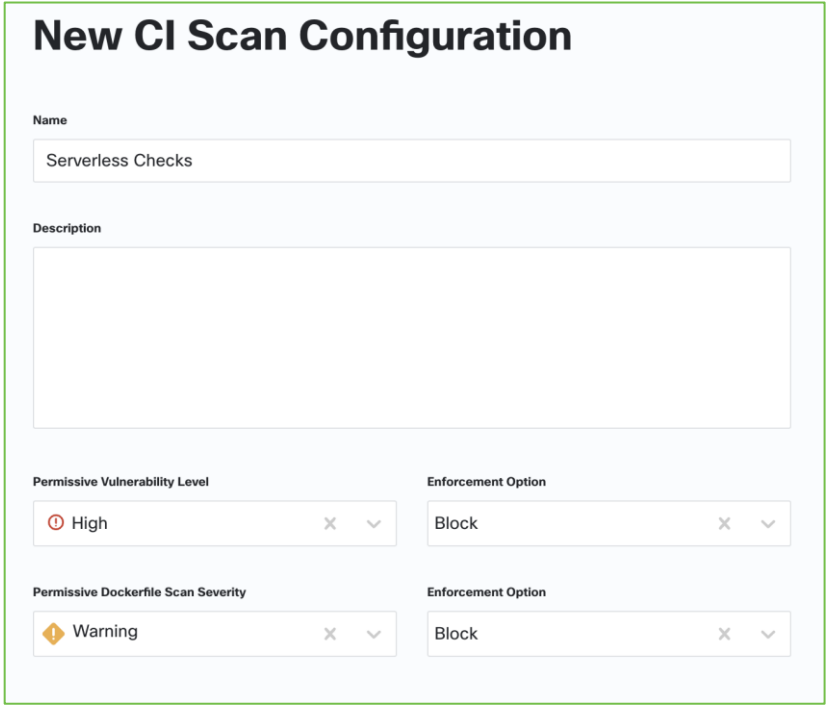


Panoptica Scans APIs for Security Posture

- Findings Can Include:
  - Network
  - Authentication
  - DNS
  - API Specifications
  - Many More…

Panoptica Scans Code for Vulnerabilities

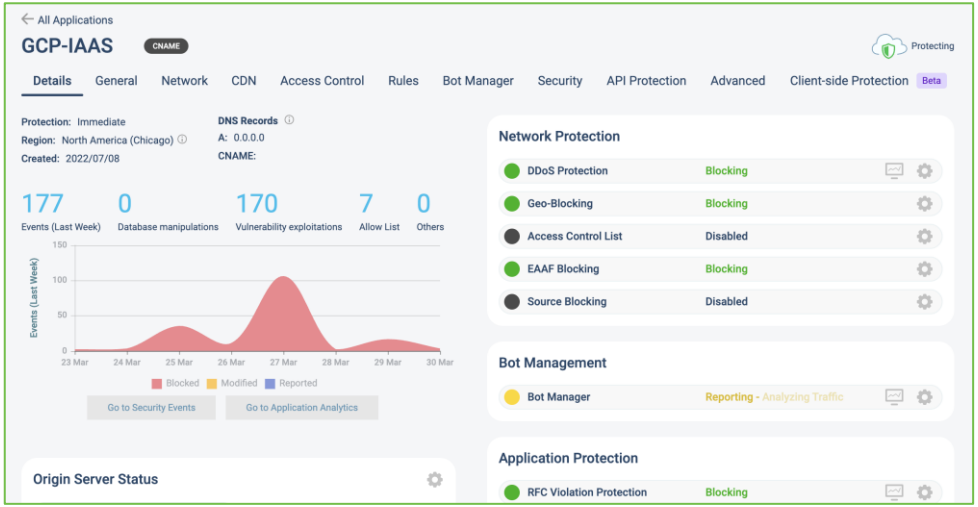
- Part of CI/CD pipeline
- Vulnerability scanning while building package
- Prevent unauthorized functions from being deployed



Radware Cloud WAF & DDoS

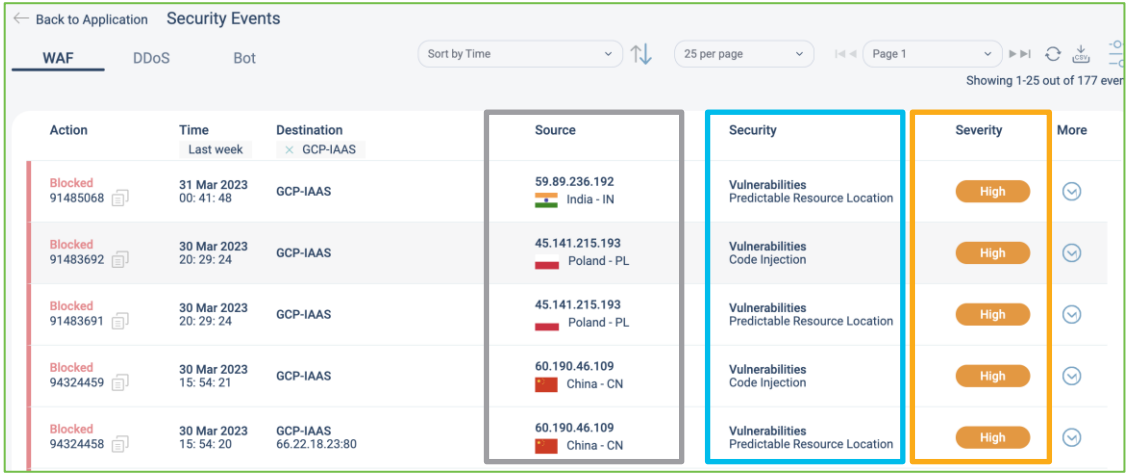
Radware Cloud WAF & DDoS Overview

- Provides multiple cloud-based services:
  - WAF
  - DDoS
  - Bot protection
  - API protection
  - Many more…



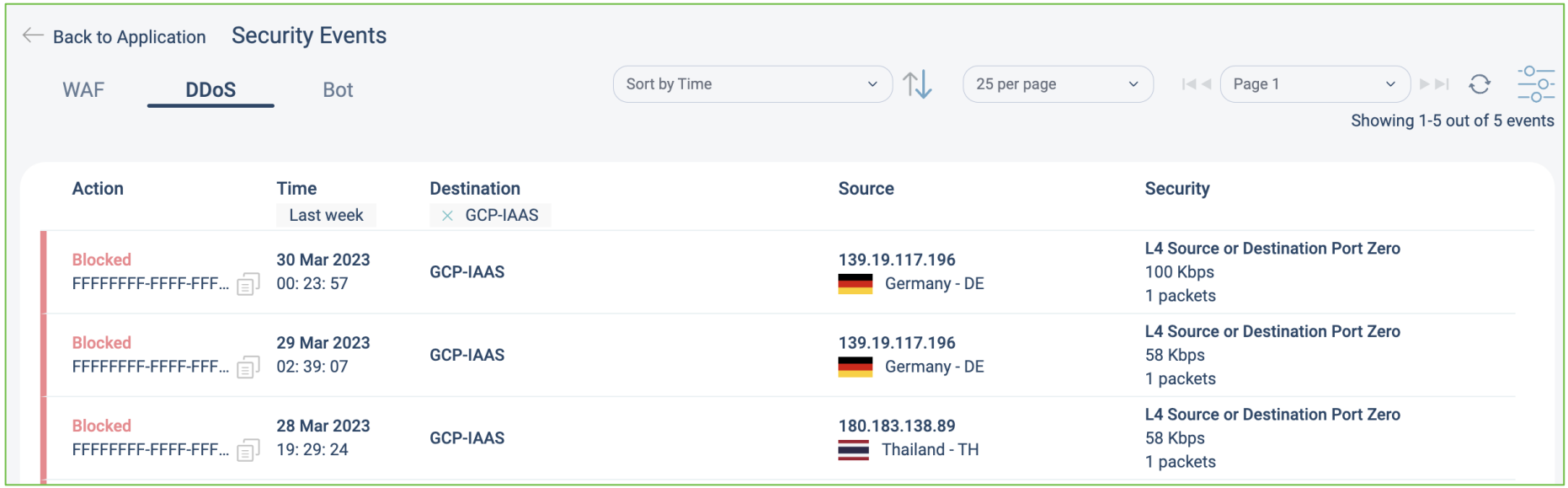
Radware is a Web Application Firewall

- Why it blocked a connection
- Where it came from
- The severity of the connection



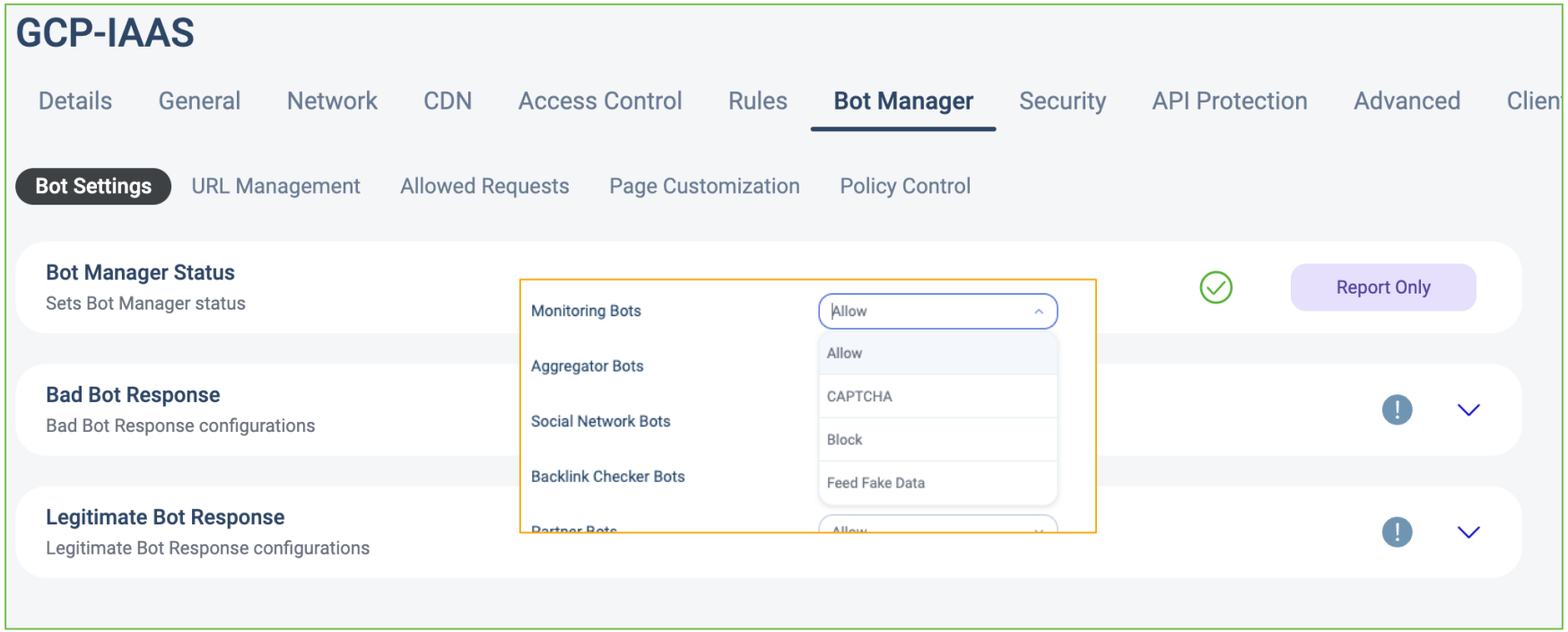
Radware Provides DDoS Protection

Prevents DDoS attempts from around the world



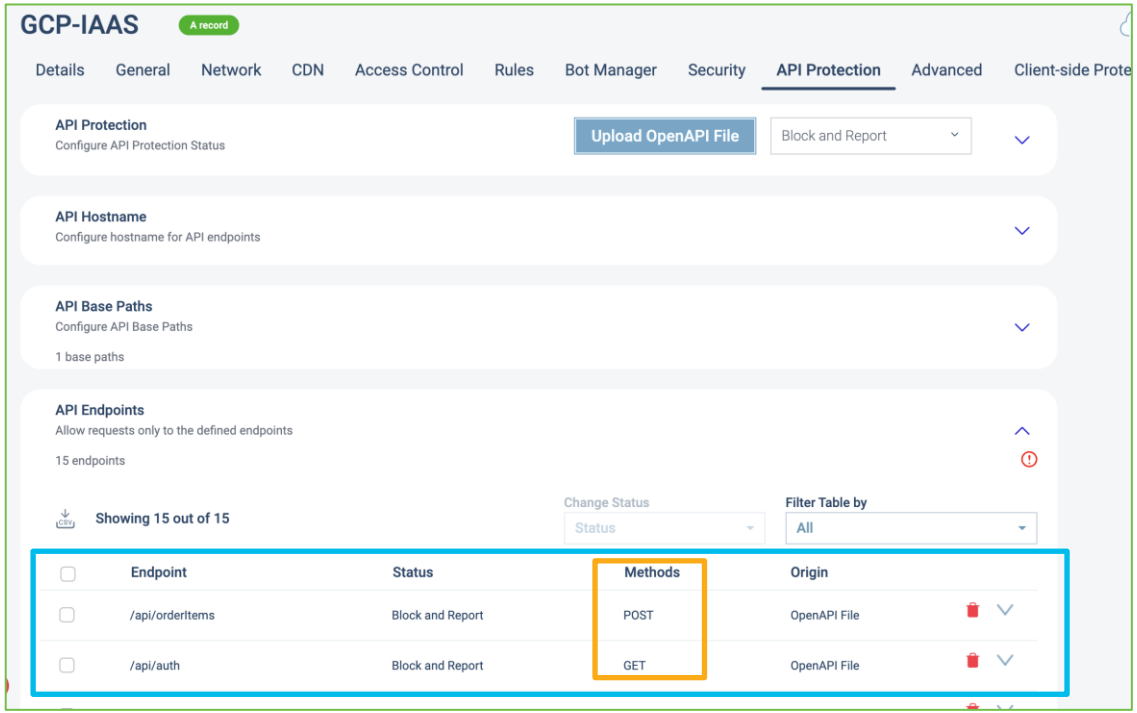
Radware Stops Bots

Can allow or deny bad bots or legitimate bots



Radware Scans Your APIs

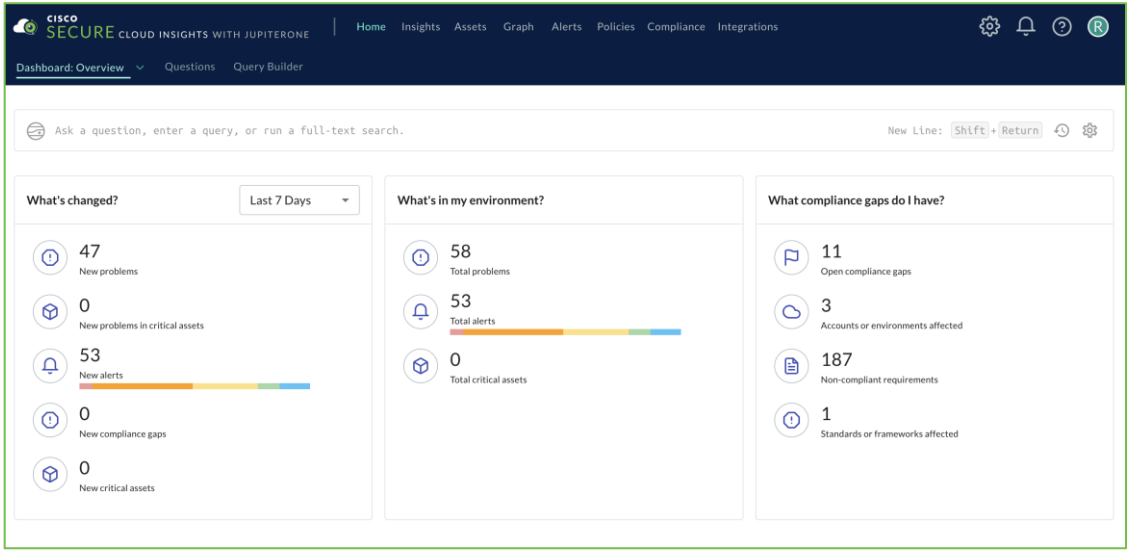
- Will discover APIs over time (including unknown API endpoints)
- Can prevent access to these endpoints
  - Or block specific request types



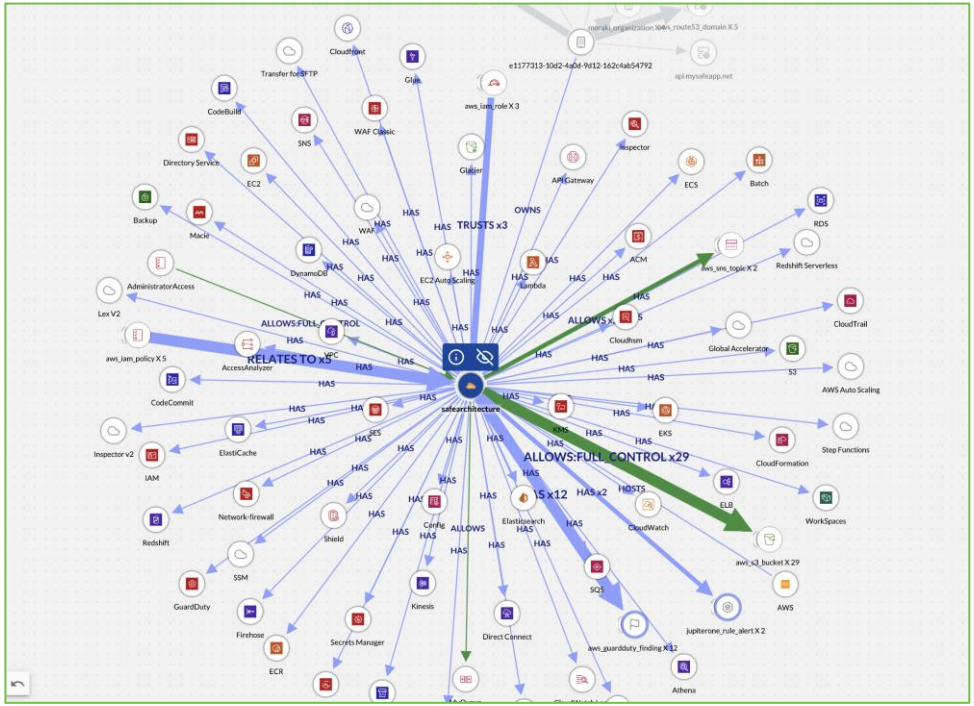
Secure Cloud Insights

SCI Overview

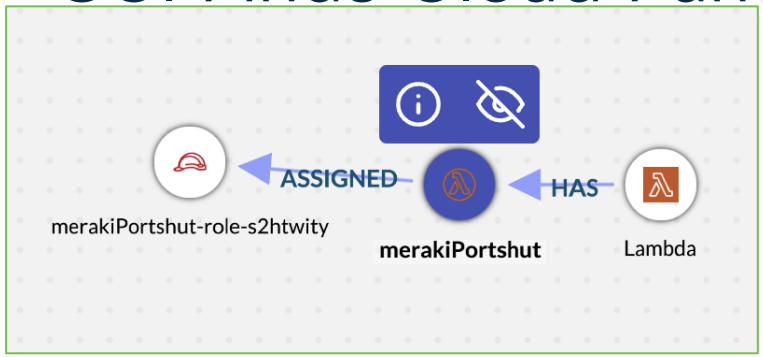
- Asset management
- Attack surface visualization
- Compliance

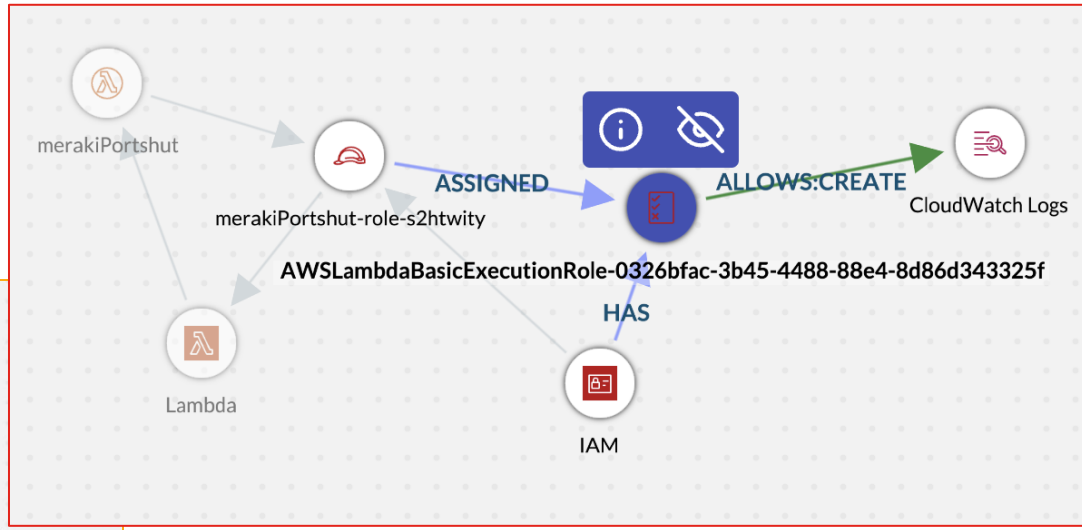


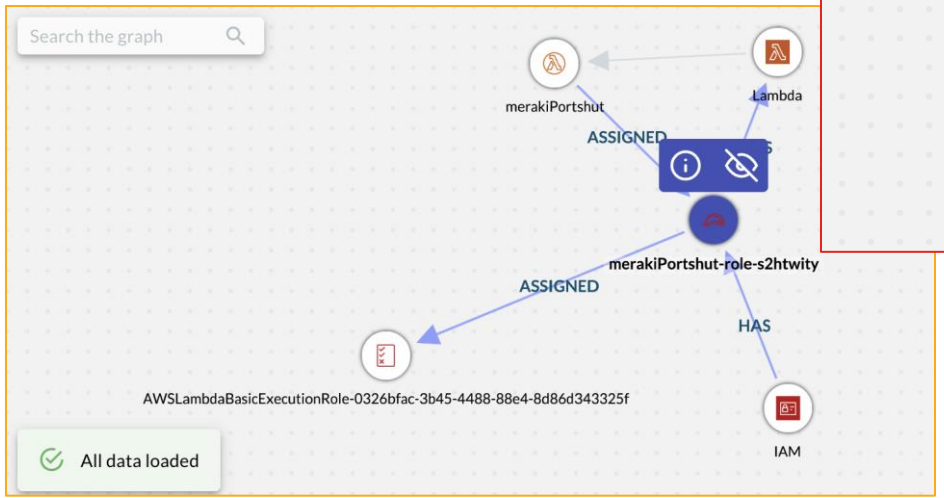
SCI Shows All Assets In The Cloud



SCI Finds Cloud Function Access to Resources

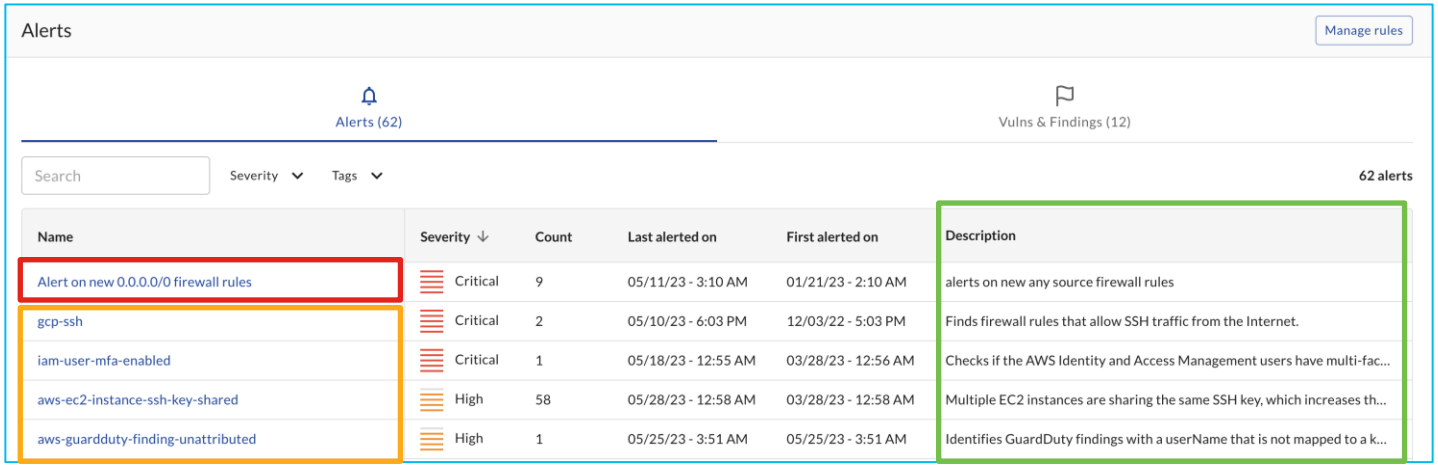






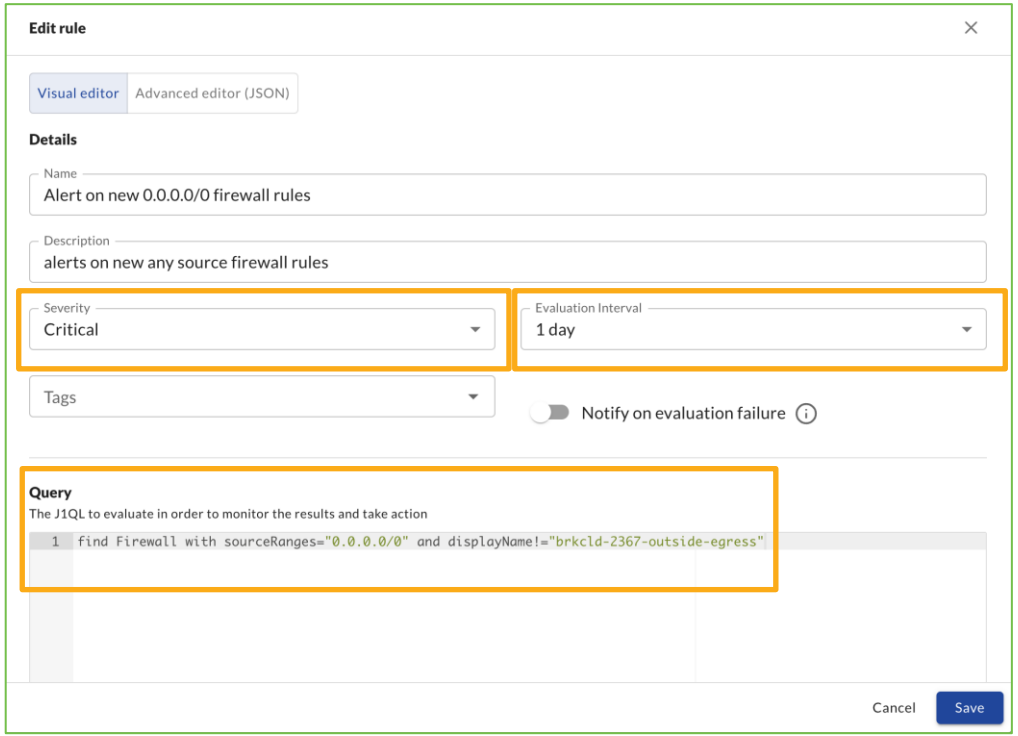
SCI Alerts are actionable

- SCI has built-in alerts it looks for
- Custom alert rules can be made
- They give exact cause making it easy to fix



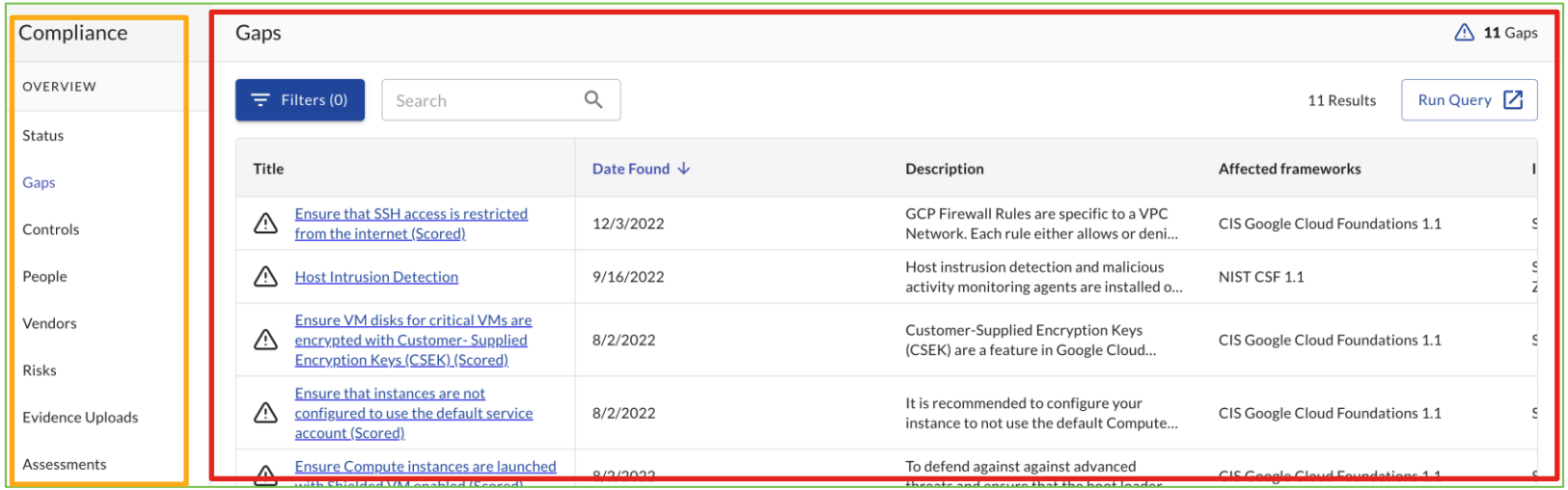
SCI Example of a Custom Rule

- How important the rule is
- When it should check
- The query SCI uses



SCI Monitors The Environment's Compliance

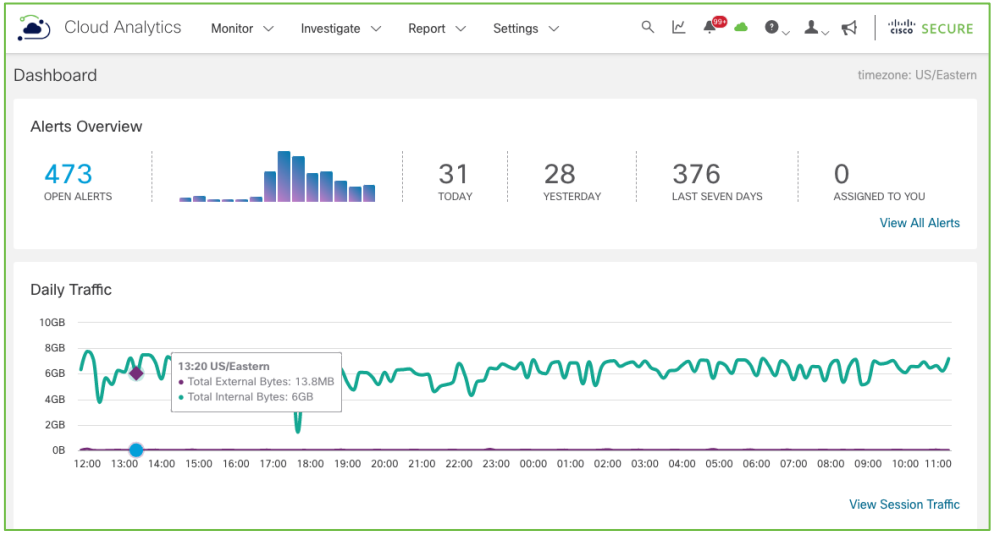
- Many sections of compliance within SCI
- Easy identification of what are issues



Secure Cloud Analytics

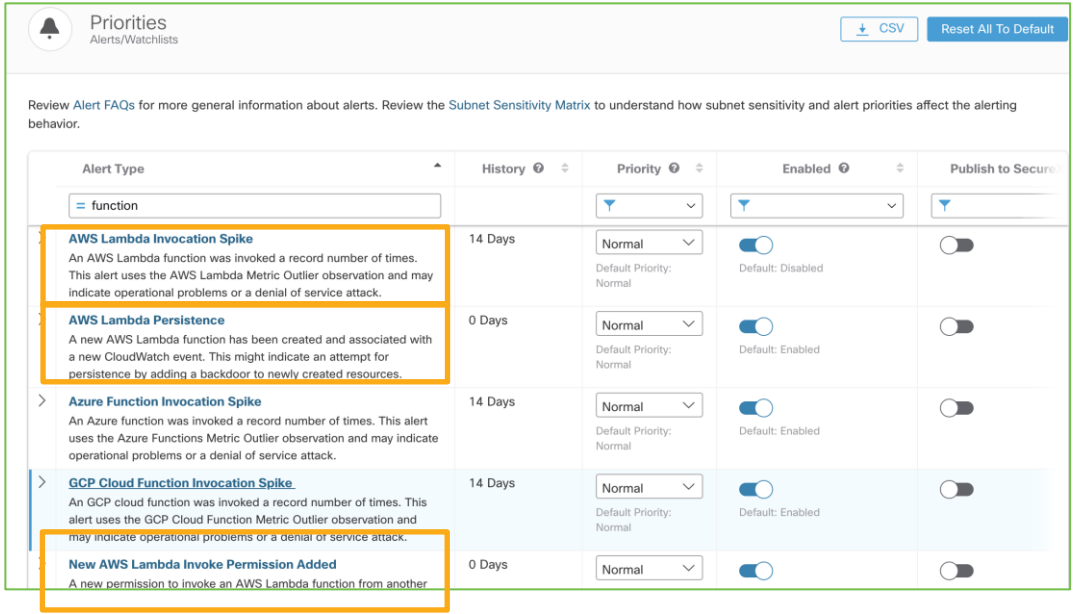
Secure Cloud Analytics Overview

- Comprehensive cloud analysis and alerts
- Monitors entire cloud infrastructure for anomalies
- Provides Cloud Function analysis
- Watches for unwanted traffic



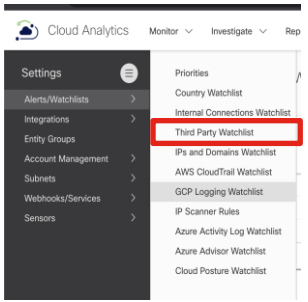
Secure Cloud Analytics Monitors Cloud Functions

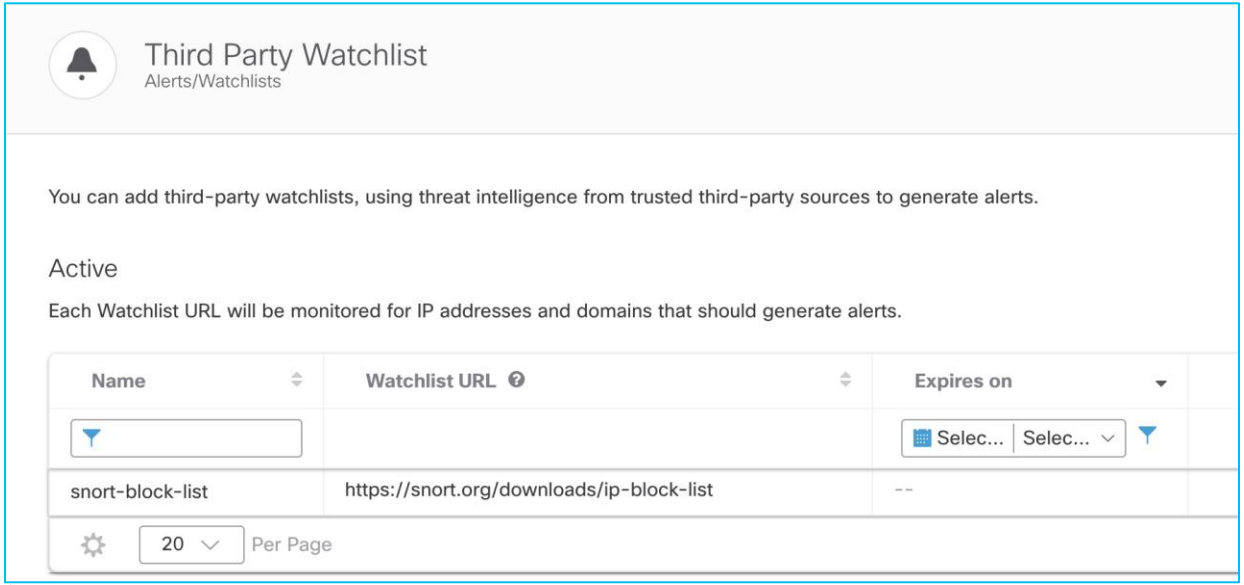
- Alerts on:
  - Abnormal amount of function runs
  - Attacker Persistence through a function
  - New permissions for account access



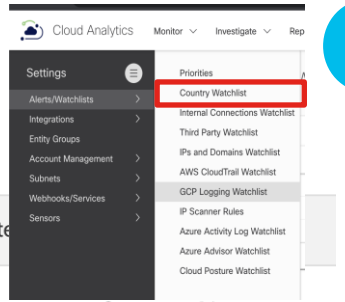
SCA Third Party Watchlist

- Upload custom domain/IP lists





SCA Country Watchlist



Country Watchlist
Alerts/Watchlists

The Country Watchlist is used to trigger several alerts, including the Remote Access (Geographic) alert, tl

Watched Status: Show all

Watched Status: Show selecte

Watched Status
Show all

Country Name

Watched Status
Show selected

Country Name

Select All | Unselect All

Select Filtered (3) | Unselect Filtered (3)

A
Afghanistan | Albania | Algeria | American Samoa
Antigua and Barbuda | Argentina | Armenia | Aruba

B

C
China

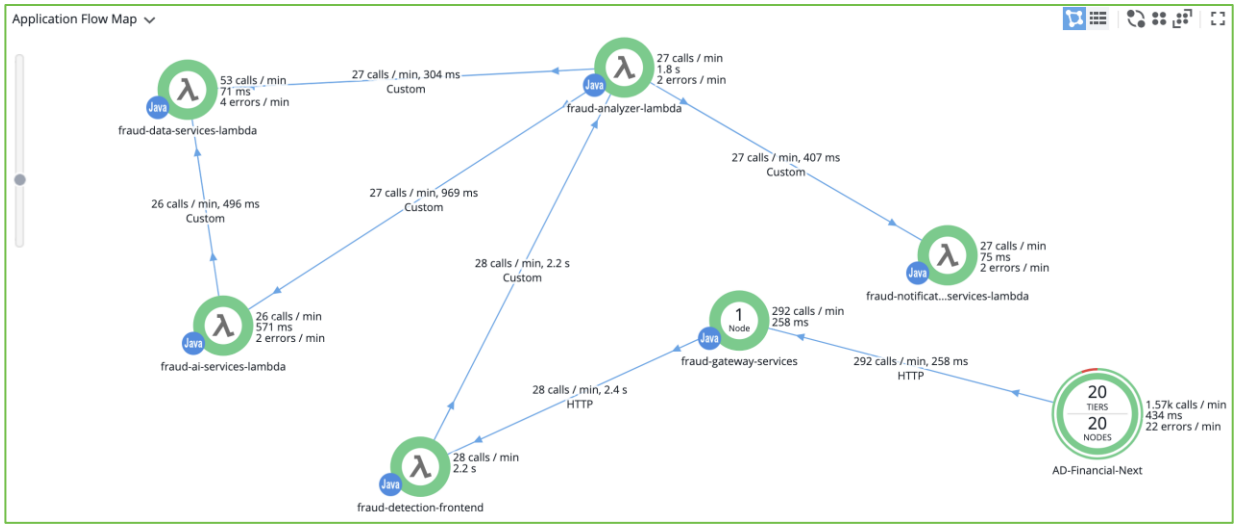
K
Korea (Democratic People's Republic of)

R
Russia

AppDynamics

AppDynamics Overview

- Provides:
  - Serverless application performance monitoring (APM)
  - Library monitoring
  - Attack monitoring



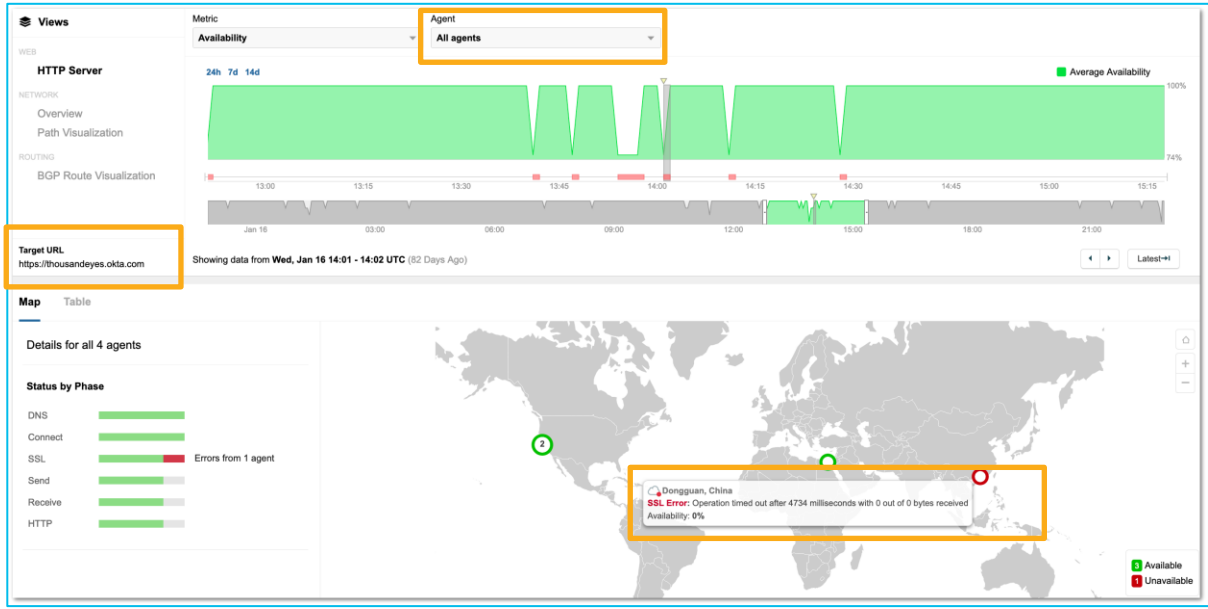
ThousandEyes

ThousandEyes Overview

- Provides internet & cloud visibility
- Service assurance
- Remote testing

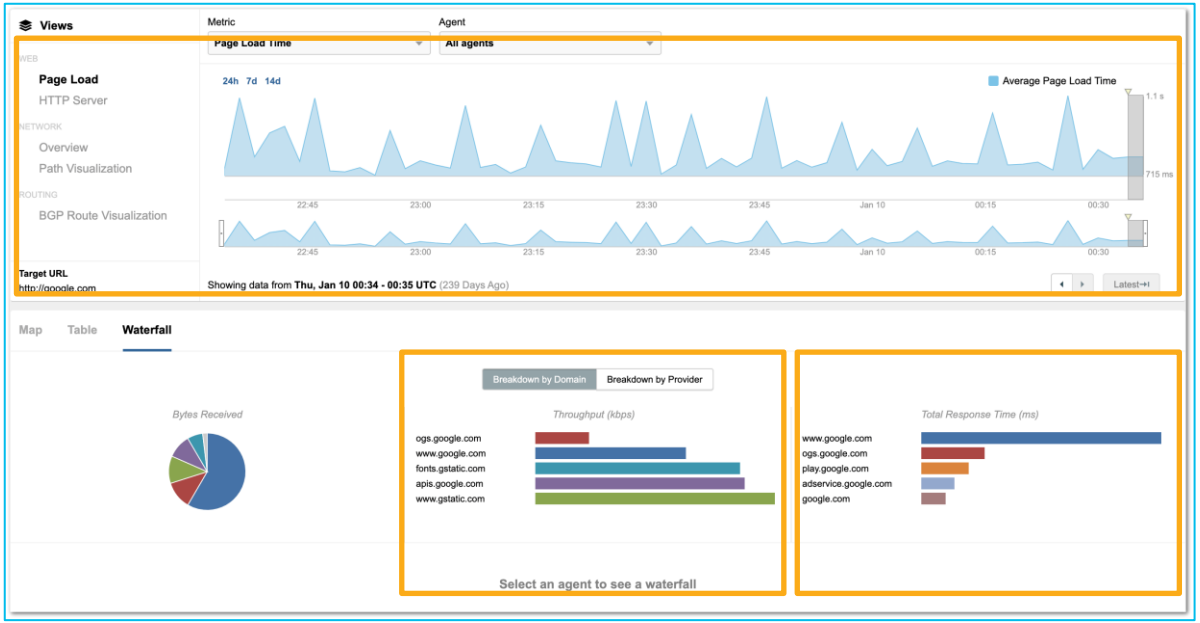
ThousandEyes HTTP Tests

- Can test any URL
- Runs from the cloud
  - Or anywhere an agent is
- Shows where an issue is
  - And why



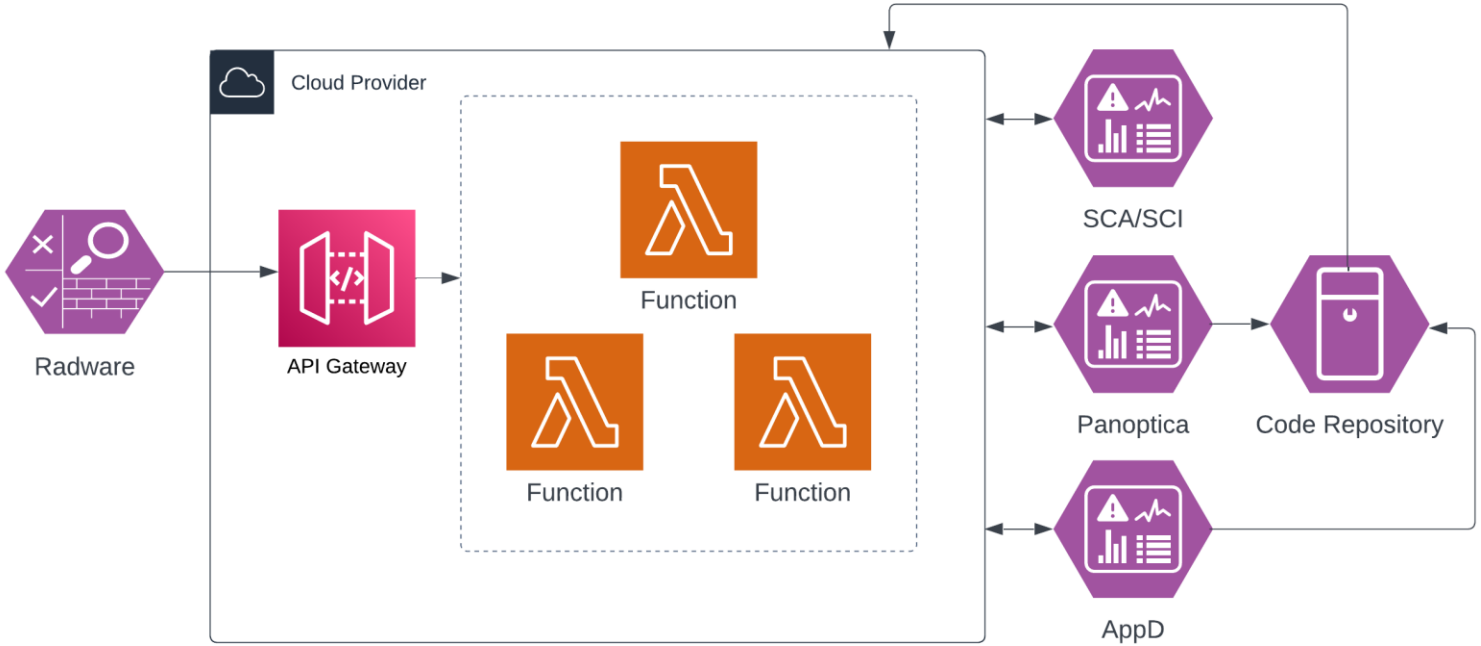
ThousandEyes Can Tests Page Loading Times

- Tests user experience
- Shows loading domains
- Shows page load blockers

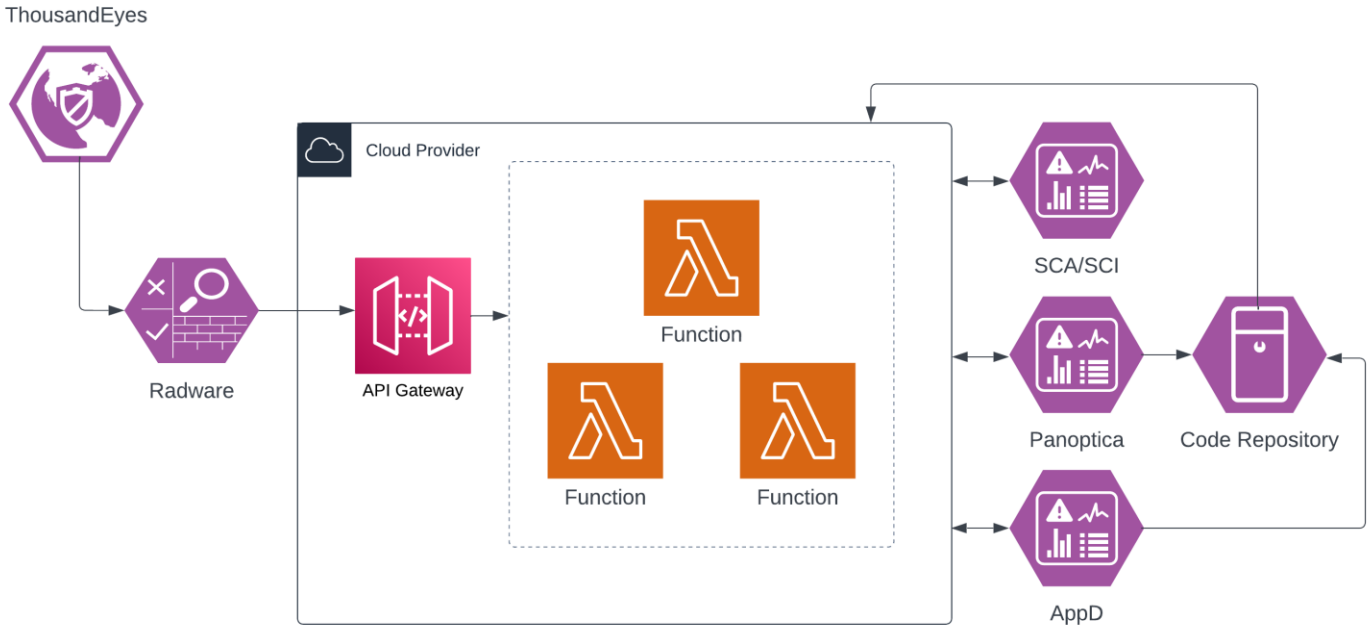


What It Looks Like

General Architecture Diagram



With ThousandEyes



Conclusion

- Using all these products is preferable
- One product cannot cover all the pillars
- Layers of security is the best policy

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

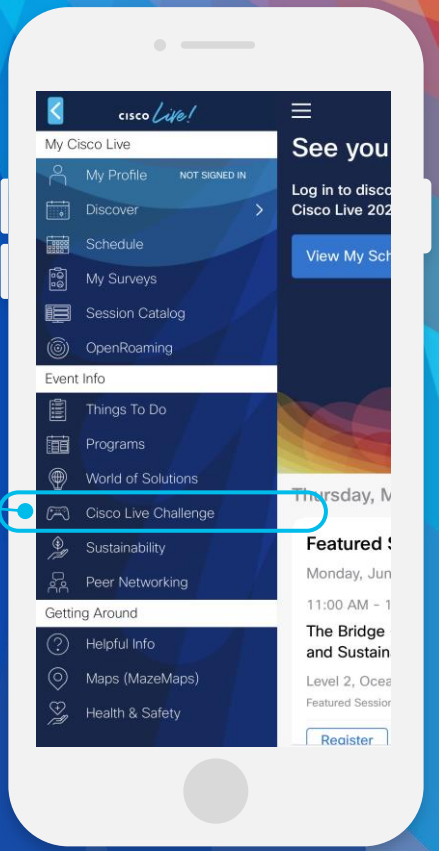
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:




cisco Live!
Let's go
#CiscoLive