cisco Live!

ALL IN

#CiscoLive

cisco The bridge to possible

Container security and their APIs

Two sides of the Same Security Coin

Peter Bosch, Distinguished Engineer and CTO AppSec

BRKSEC-2080

Panoptica

Peter Bosch

Distinguished engineer at Cisco

- Mobile SDWAN/Invisible networking
- Virtualized professional media systems
- Virtualized mobile packet cores and GiLAN

CTO Application Security

- Cloud-native application security
- API security

Associate professor University of Twente

- Reliable and secure distributed system
- Looking for PhD students!

Cisco Webex app

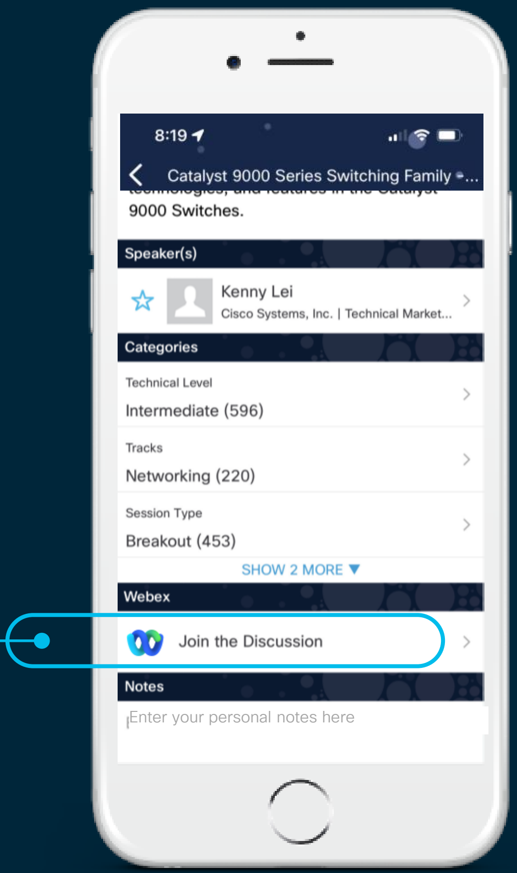
Questions?

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 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

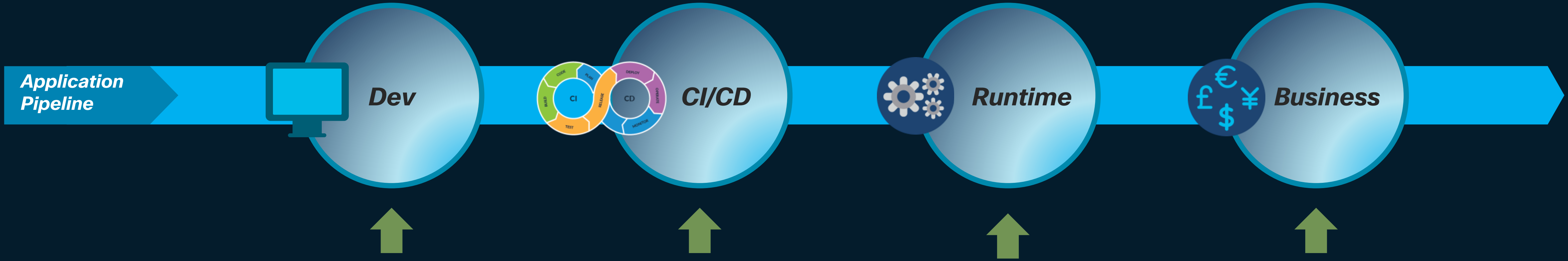
https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2080

cisco Live!

Agenda

- Panoptica, cloud-native application security
- A quick demo

Panoptica: Cisco application security

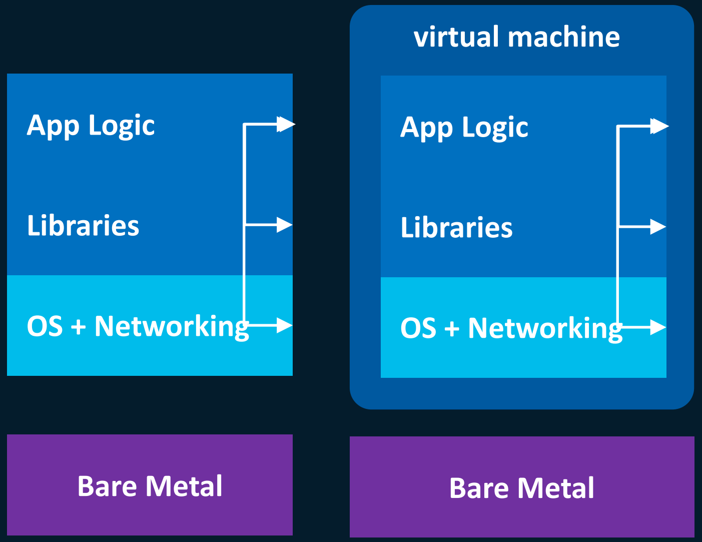


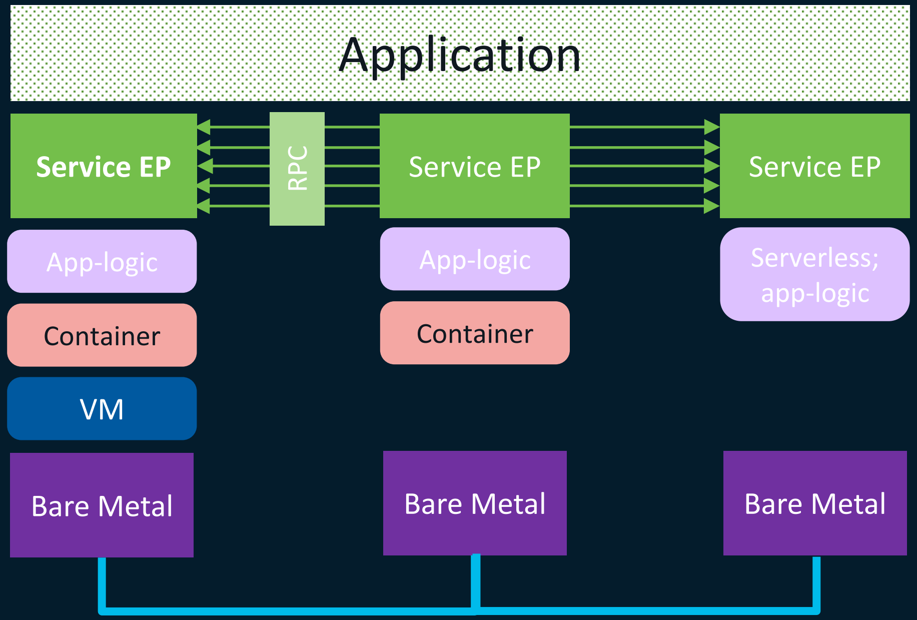
Instrument via Cloud Native Infra (Kubernetes, Service Mesh), In-app agent, DevOps toolchain plugins and API Gateway connectors

Cisco Secure Application secures the cloud native application ***in all its stages***, and for ***all components***: micro-services, functions, APIs and configurations

From monolithic

To composable, modern applications





The wide-open Internet is the runtime for all modern apps…

… but the new perimeter of apps and security is diffuse

1 How do I protect cloud native apps? I must rely on the app’s own defenses when running in the cloud!

2 Is the application’s configuration sound? What software am I really using for my application?

3 Do I build a barrier inside my cloud app? Can I rely on trusted communication?

4 Can I automatically manage applications that are vulnerable. Can these be repaired semi-automatically?

Introducing: Panoptica

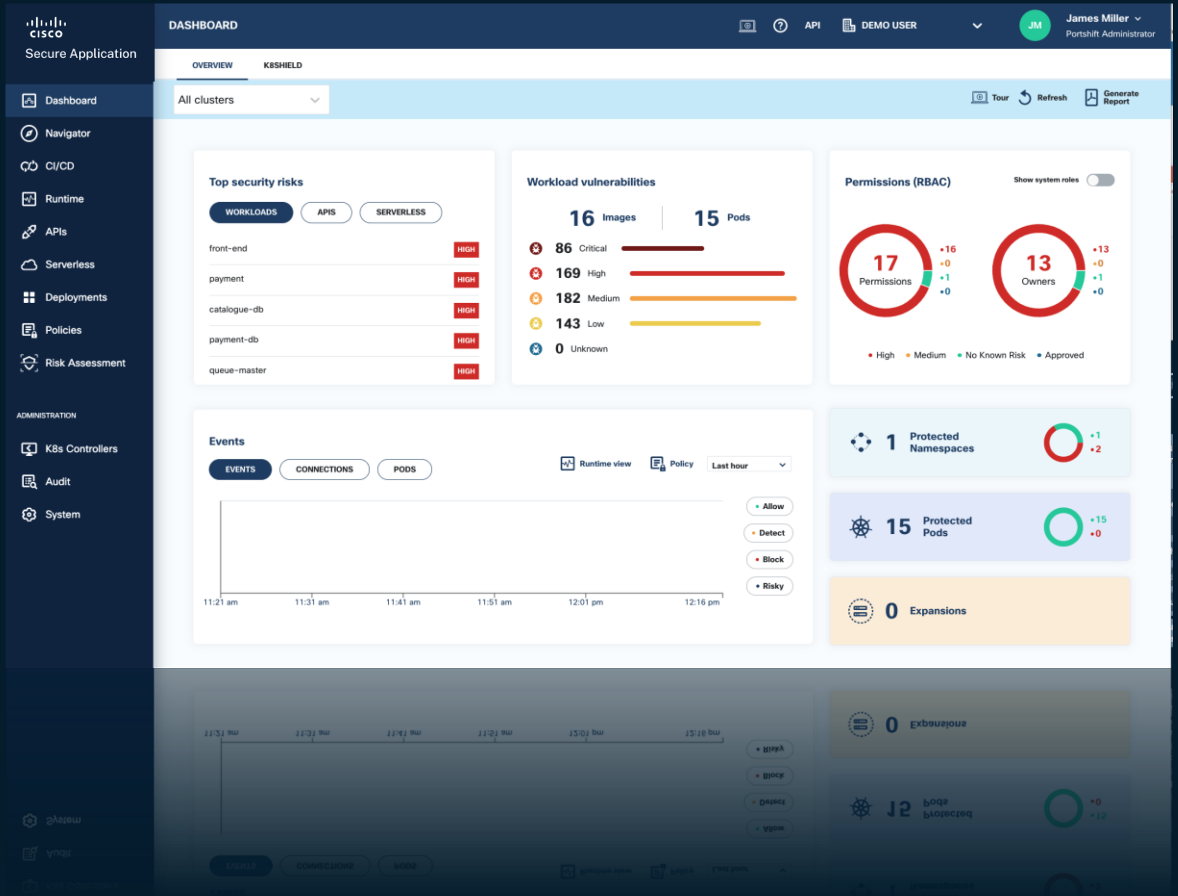
A single pane of glass for all things cloud-native app

Present all artefacts of the applications and its vulnerabilities

Control container, images, SBOM, supply chain, serverless and APIs

Manage the risks through a MITRE ATT&CK framework

Define and enforce security policies and compliance for the enterprise



Top security risks

front-end	HIGH
payment	HIGH
catalogue-db	HIGH
payment-db	HIGH
queue-master	HIGH

Workload vulnerabilities: 16 Images, 15 Pods

86	Critical
169	High
182	Medium
143	Low
0	Unknown

Permissions (RBAC): 17 Permissions (16, 0, 1, 0); 13 Owners (13, 0, 1, 0)

High · Medium · No Known Risk · Approved

1 Protected Namespaces (1, 2)

15 Protected Pods (15, 0)

0 Expansions

Panoptica key components

Cisco open sourced two innovative components of SecureApplication

KUBE Clarity

A Kubernetes runtime vulnerability scanner to capture and analyze container images and their risks

APIClarity

A cloud native visibility tool for APIs to capture, analyze and test API traffic and identify potential risks.

1 What software components are used in your application? What's their provenance?

2 What vulnerabilities are hidden in those software components? Will these impact the app's security?

3 Can I scan for these vulnerabilities automatically? With multiple tools? For different kinds of issues?

4 Multiply this across thousands of apps. Can I automate the analysis? Can I easily remediate?

Universal scan

Vulnerabilities scan for source code and containers images

Runtime scan

Scan K8s deployments providing an accurate snapshot of its risks

S-BoM creation

Creating a S-BOM for quick detection of risks and their relevance

Flexible

Scan entire app, use multiple scanners, alert of specific vulnerabilities and severities

Accurate

Uses multiple vulnerabilities feeds for effective and accurate discovery

KubeClarity

1 Are serverless functions vulnerable? Did serverless code functions degrade over time?

2 Are secrets embedded in the code? Are my functions overly permissive? Are my functions publicly exposed?

3 Does code provide direct access to data sources? What resources are used by the functions?

4 Can I deny bad serverless functions from firing? Can I scan for serverless vulnerabilities automatically?

Serverless scan

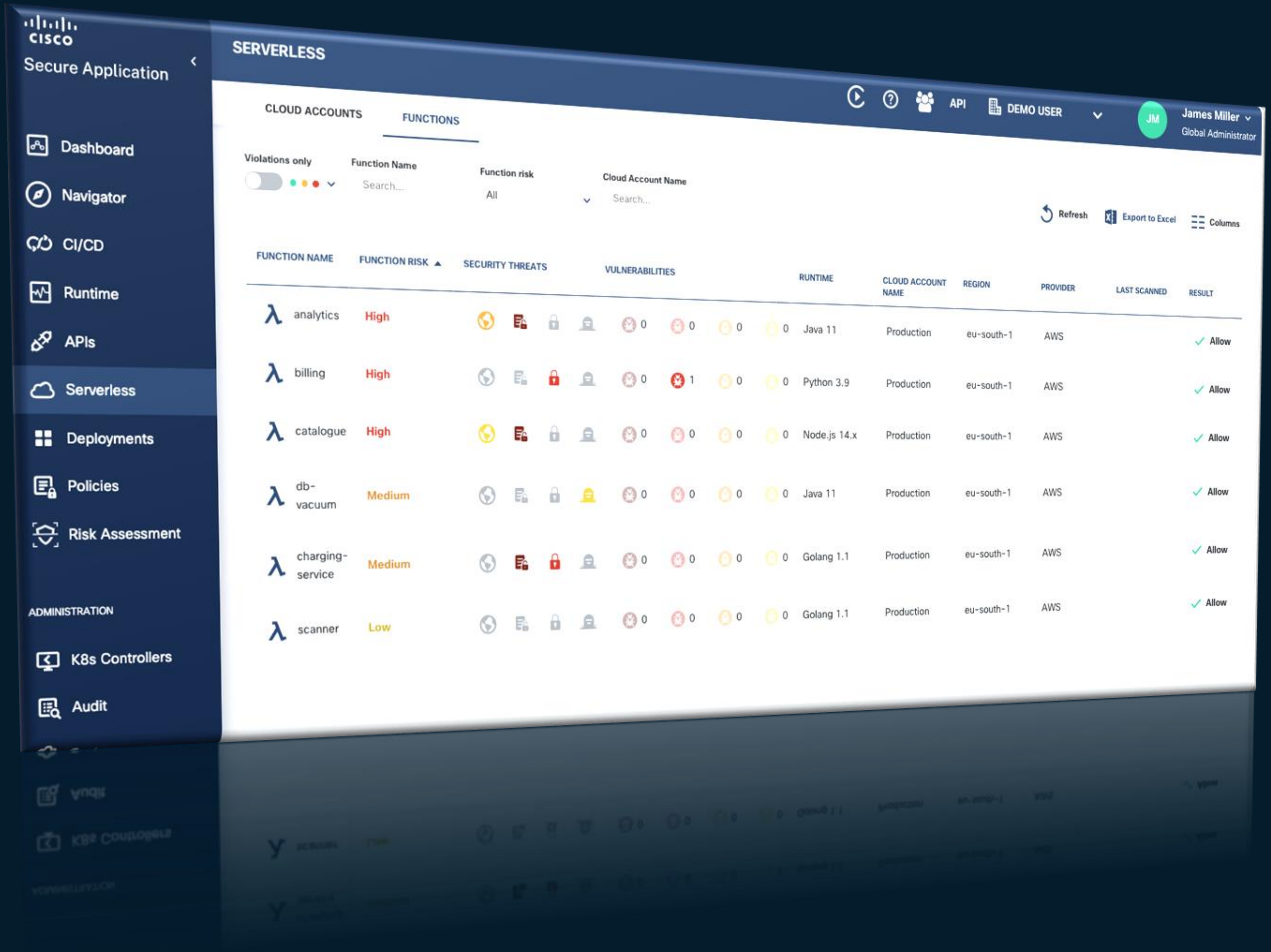
Scan for software and configuration issues in serverless functions in cloud systems

Policies

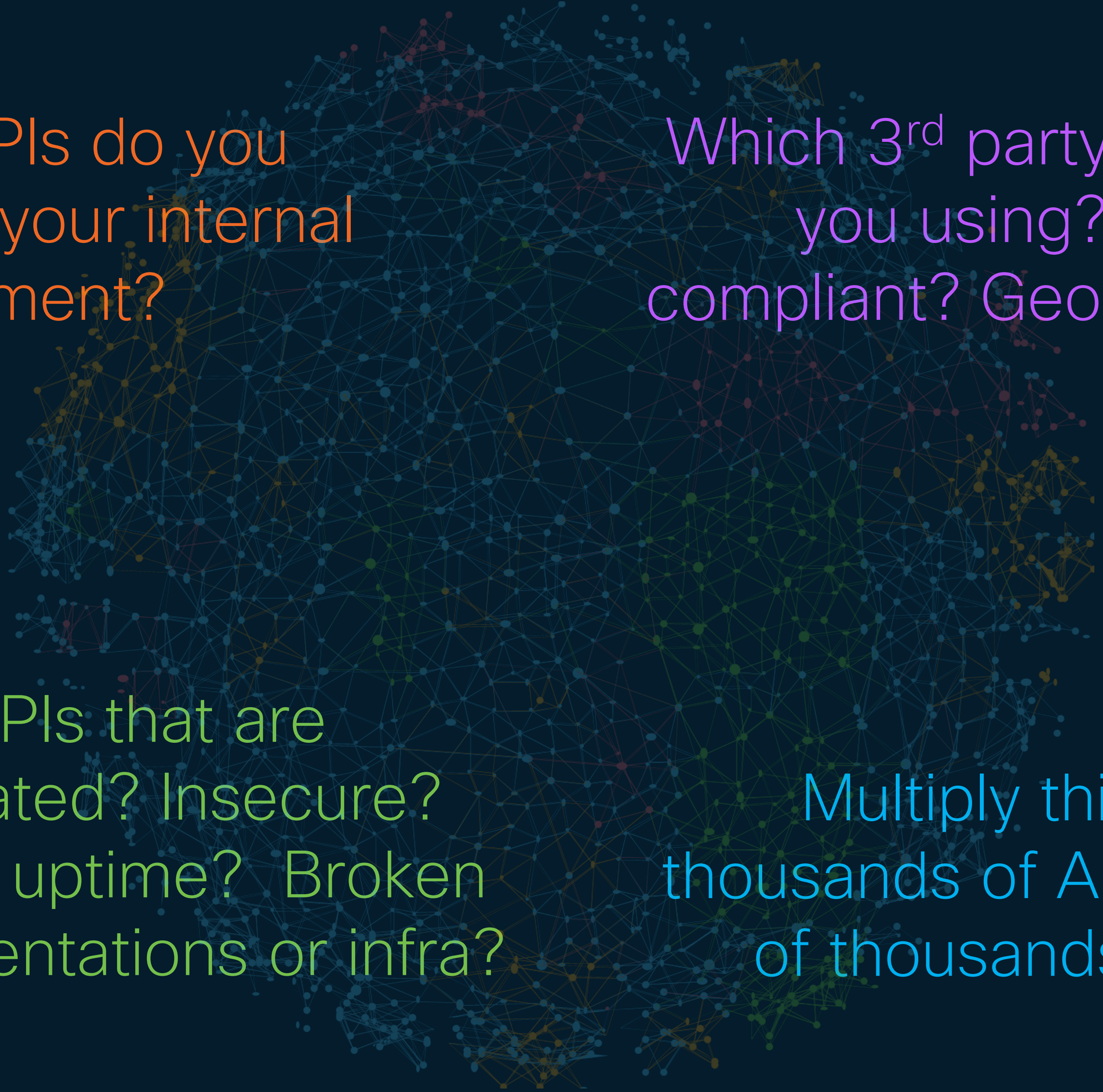
Define rules when to allow serverless functions to run and enforce such rules

Integrate

With cloud accounts to access serverless functions



FUNCTION NAME	FUNCTION RISK ▲	SECURITY THREATS	VULNERABILITIES				RUNTIME	CLOUD ACCOUNT NAME	REGION	PROVIDER	LAST SCANNED	RESULT
λ analytics	High		0	0	0	0	Java 11	Production	eu-south-1	AWS		✓ Allow
λ billing	High		0	1	0	0	Python 3.9	Production	eu-south-1	AWS		✓ Allow
λ catalogue	High		0	0	0	0	Node.js 14.x	Production	eu-south-1	AWS		✓ Allow
λ db-vacuum	Medium		0	0	0	0	Java 11	Production	eu-south-1	AWS		✓ Allow
λ charging-service	Medium		0	0	0	0	Golang 1.1	Production	eu-south-1	AWS		✓ Allow
λ scanner	Low		0	0	0	0	Golang 1.1	Production	eu-south-1	AWS		✓ Allow



1 What APIs do you have in your internal environment?

2 Which 3rd party APIs are you using? Are they compliant? Geo-fenced?

3 Using APIs that are deprecated? Insecure? Terrible uptime? Broken implementations or infra?

4 Multiply this across thousands of Apps, 10s of thousands of APIs

Frictionless

No code changes needed to your App

Automated

Constructs the OpenAPI spec by observing API traffic

Reconcile and Drift

Upload and review of OpenAPI specs, track deltas over time

Zombies & Shadows

Visibility of deprecated and undocumented API usage

Test

Fuzz and test the APIs to find vulnerabilities, authorization mistakes and more

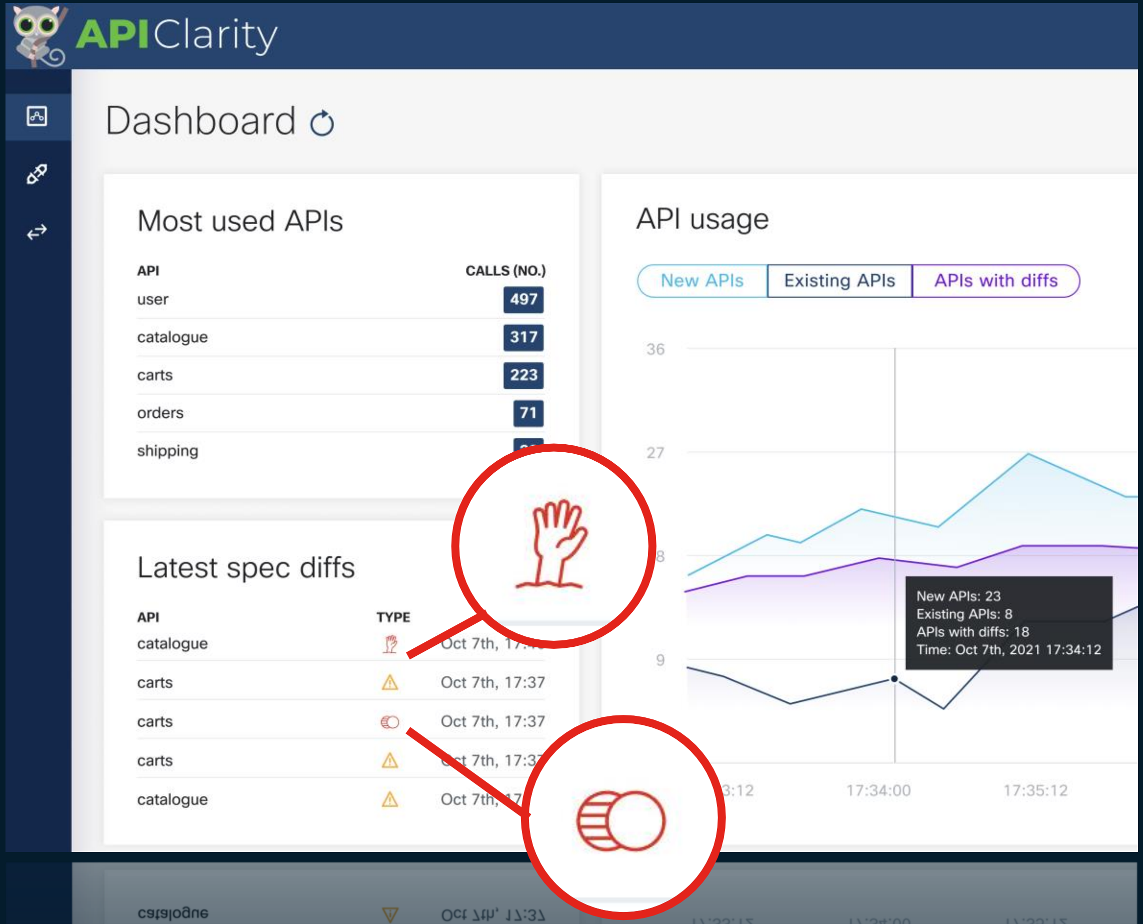
Visual

UI dashboard to audit and monitor the API findings

APIClarity

apiclarity.io

For Devs, SRE, and SecOps



Most used APIs

API	CALLS (NO.)
user	497
catalogue	317
carts	223
orders	71
shipping	[illegible]

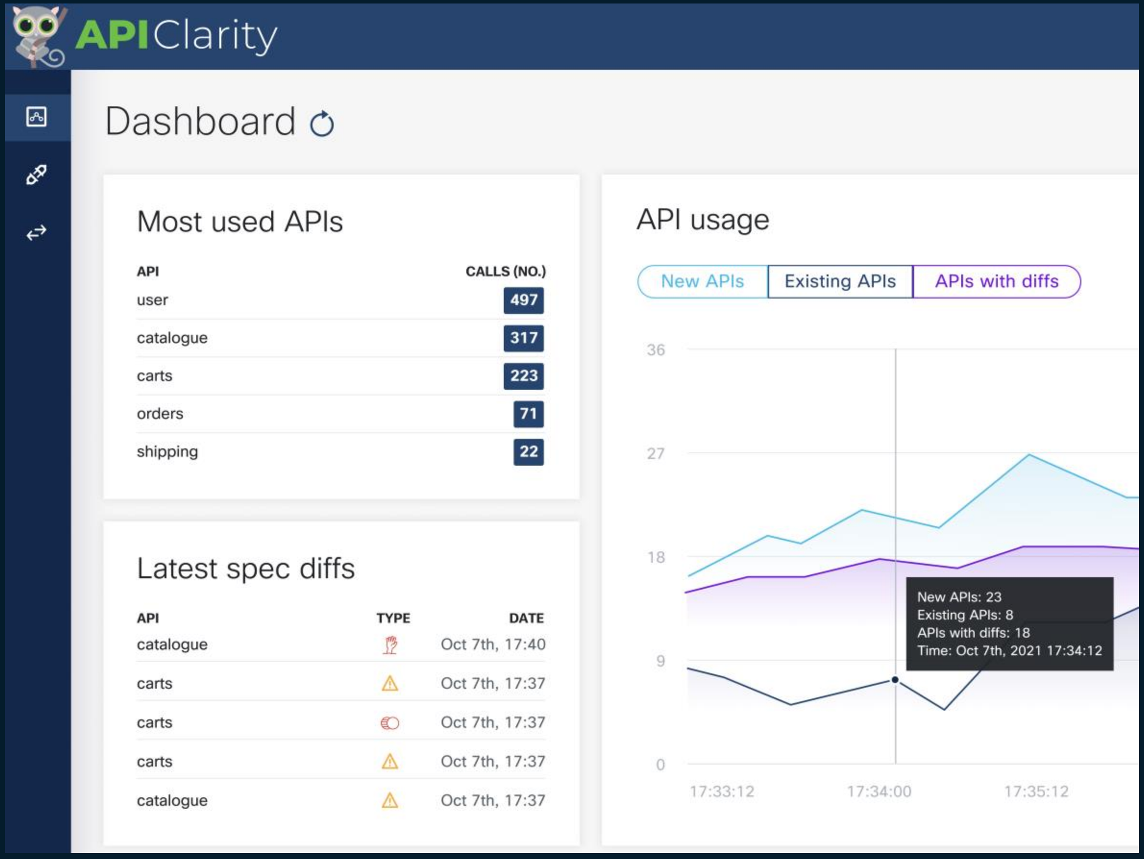
New APIs: 23
Existing APIs: 8
APIs with diffs: 18
Time: Oct 7th, 2021 17:34:12

Latest spec diffs

API	TYPE	
catalogue	✋	Oct 7th, 17:
carts	⚠	Oct 7th, 17:37
carts	◎	Oct 7th, 17:37
carts	⚠	t 7th, 17:3
catalogue	⚠	Oct 7th, 17

Having clarity on the API spec is the first step

For Devs, SRE, and SecOps



Dashboard

Most used APIs

API	CALLS (NO.)
user	497
catalogue	317
carts	223
orders	71
shipping	22

API usage

Latest spec diffs

API	TYPE	DATE
catalogue	✋	Oct 7th, 17:40
carts	⚠	Oct 7th, 17:37
carts	◎	Oct 7th, 17:37
carts	⚠	Oct 7th, 17:37
catalogue	⚠	Oct 7th, 17:37

Having clarity on the API spec is <u>just</u> the first step

Analyze spec for security issues and best practices

Run API fuzzing tests using the spec, test biz logic

Test application authorization logic

Generate Client and Server code

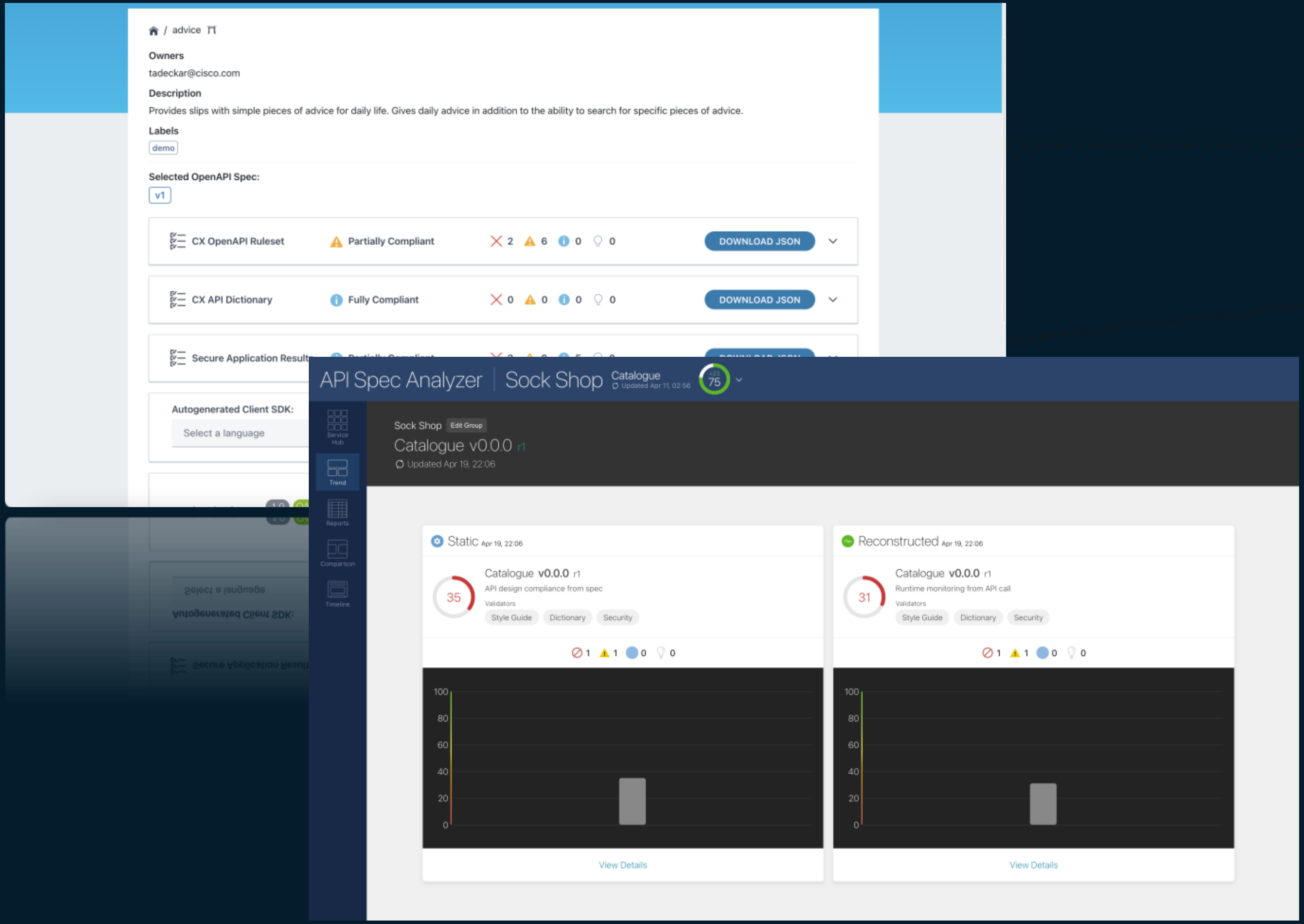
1 How do I protect and track apps from cradle to grave? Can I make a one-stop-shop for all my apps from build to run?

2 Are applications compliant with my company rules? How about the industry's rules? In build and run-time?

3 How do I track the daily chain of new app versions? How do I test for regression in apps and their APIs?

4 How do I automatically manage hundreds of applications? How do I address API risks while the app is running?

An API for an API



Owners

tadeckar@cisco.com

Description

Provides slips with simple pieces of advice for daily life. Gives daily advice in addition to the ability to search for specific pieces of advice.

Labels

demo

Selected OpenAPI Spec:

v1

CX OpenAPI Ruleset	Partially Compliant	2	6	0	0
CX API Dictionary	Fully Compliant	0	0	0	0
Secure Application Results					

Catalogue
Updated Apr 11, 02:56
75

Sock Shop

Catalogue v0.0.0 r1

Updated Apr 19, 22:06

Static Apr 19, 22:06

Catalogue v0.0.0 r1
API design compliance from spec
35
Validators
Style Guide · Dictionary · Security
1 · 1 · 0 · 0

Reconstructed Apr 19, 22:06

Catalogue v0.0.0 r1
Runtime monitoring from API call
31
Validators
Style Guide · Dictionary · Security
1 · 1 · 0 · 0

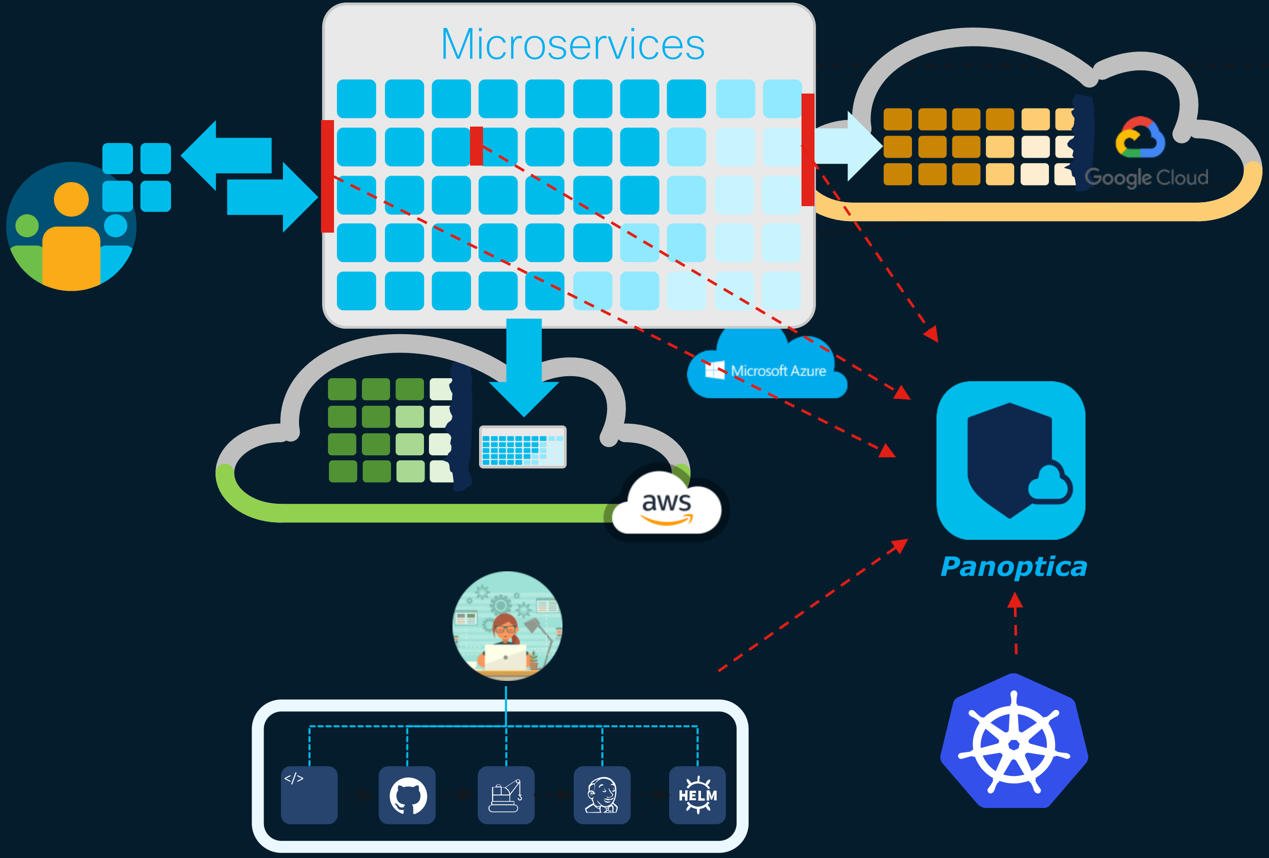
Analyze the app’s APIs before deployed; track APIs over time

Deploy apps automatically behind an API gateway and connect the app to the Internet

Test and fuzz the APIs daily to detect feature creep

Manage security vulnerabilities in the API and suspend, report or block the app

Panoptica's API security in a boring slide



Ingress/egress traffic visibility and enforcement

- Specification reconstruction and analysis
- 3rd party API classification and scoring, internal server security posture and scores and inventories

Token insertion with a vault for API use

API testing, scoring and analysis

- BOLA/BFLA, guessable ID and non-learned ID detection
- Fuzzing, application and service modeling and DASTing

Platforms

- Envoy, Kong, Tyk, Gloo (viz + enforcement)
- Virtual machines (through gateway) and containers
- Open-source

Interface Definition Languages

- OpenAPIv2/v3 and gRPC

Try API clarity and KubeClarity code on GitHub

github.com/apiclarity/apiclarity

github.com/cisco-open/kubei

Try Panoptica

eti.cisco.com/appsec

Become a Cisco Design Partner

www.ciscodesignpartners.com

Check out the Cisco Tech Blogs

https://techblog.cisco.com

Twitter: **@CiscoEmerge**

LinkedIn: Emerging Tech & Incubation

Web: **eti.cisco.com**

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- 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.

Cisco learning and certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

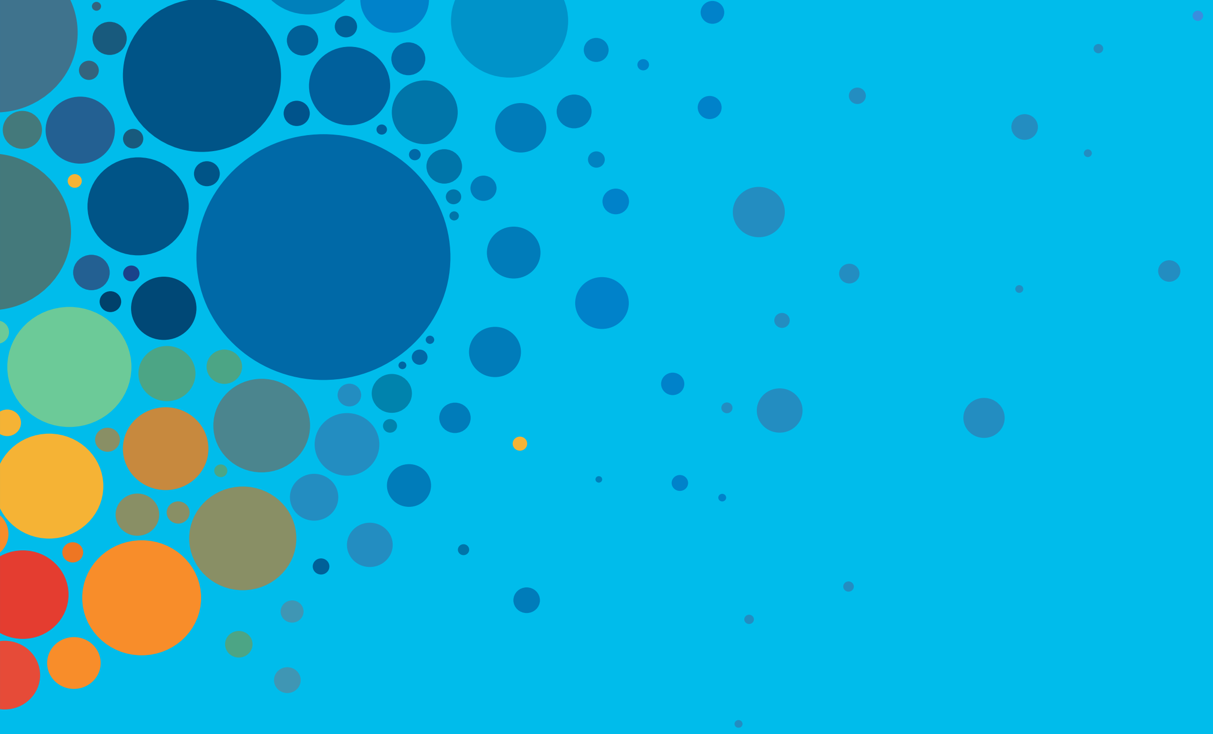
Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



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

cisco Live!

The bridge to possible

Thanks for all the fish

cisco Live!

#CiscoLive