

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Application Security in the Cloud Native world

Architecting a journey to cloud native application security

Jatin Sachdeva, Principal Security Architect
Cisco Global Security Architecture Team (GSAT)
BRKSEC-1139

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1139>





Agenda

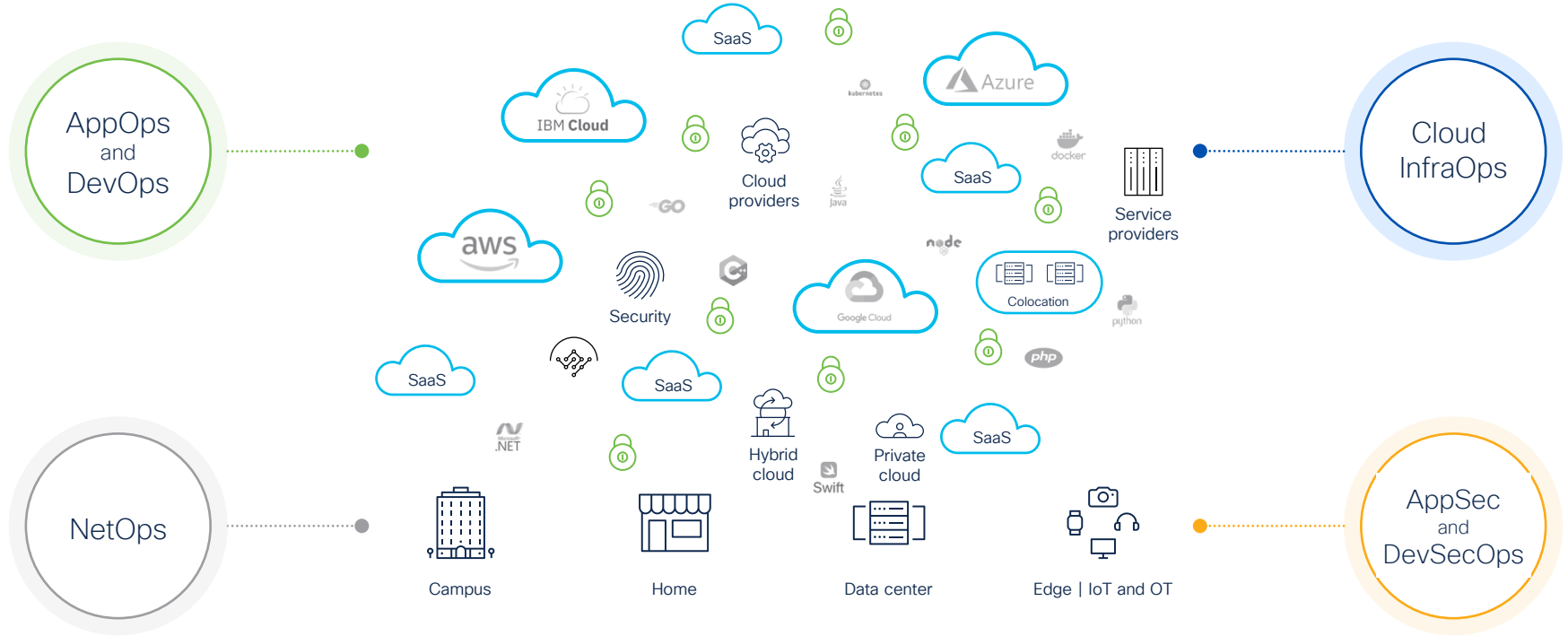
- Intro to Cloud Native Security
- Securing Public Cloud Infrastructure
- Securing Cloud Native Technologies
- Securing Application Runtimes
- Outro

About your speaker

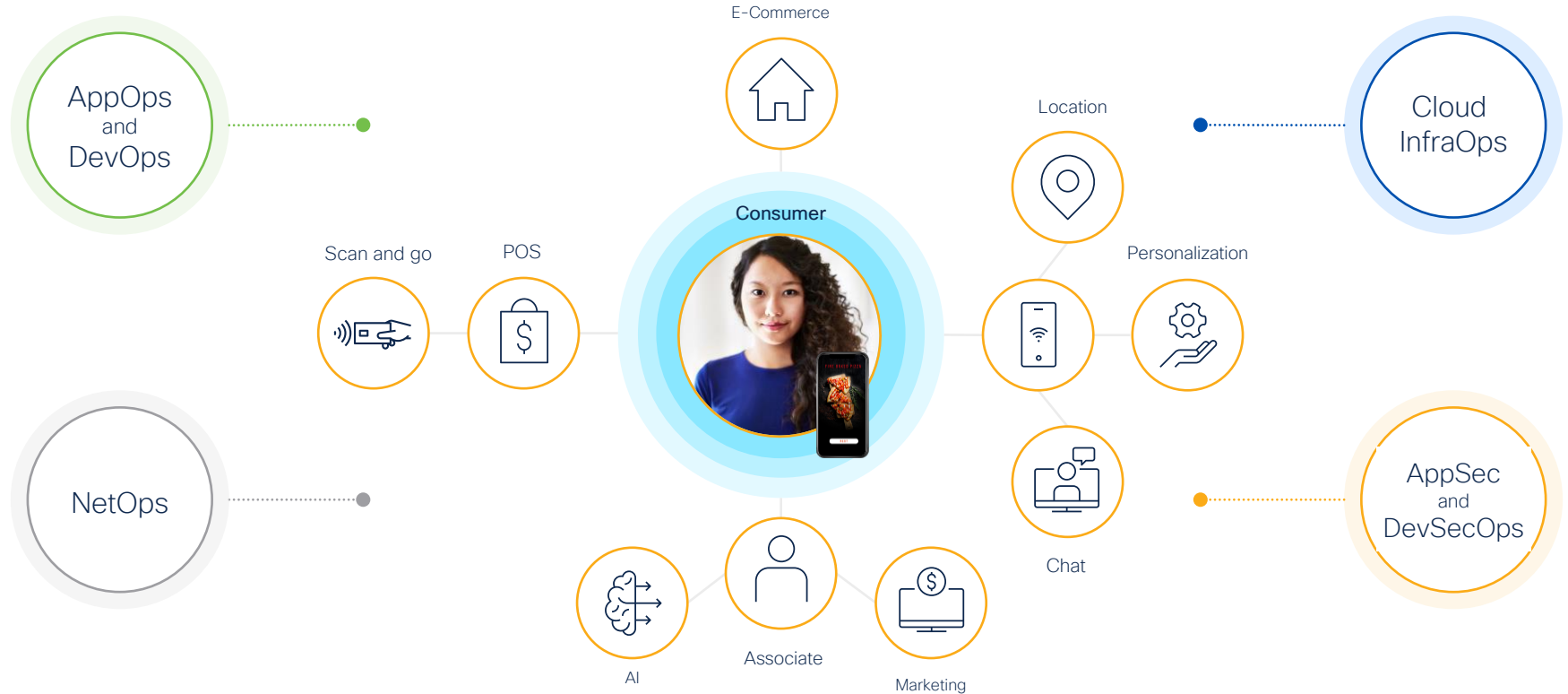
- Fun fact – I am Indian, but I am not into cricket or spicy food!
- Play
 - Live in Melbourne, Australia with my lovely family and this crazy fellow
 - Can nerd out on anything from tech and cars to fitness and nutrition!
- Work
 - 22 years in security industry, 19 in Cisco.
 - Knowledge seeker hence certs a plenty – CISSP, CISA, CEH, GWAPT, GSEC, GCIA, GCIH, GCSA, GPCS, SFCE
 - Prior to Cisco – security consulting, implementation and audit



Navigating the new world order isn't easy



Navigating the new world order isn't easy



Infrastructure & Applications are changing



A tale of cloud maturity

91%

are wasting money in the cloud

64%

are experiencing a shortage of skilled staff

Security is the **#1 factor** high-maturity organizations use to assess cloud **success** and the **#1 one benefit** they say they get from their cloud program.

86%

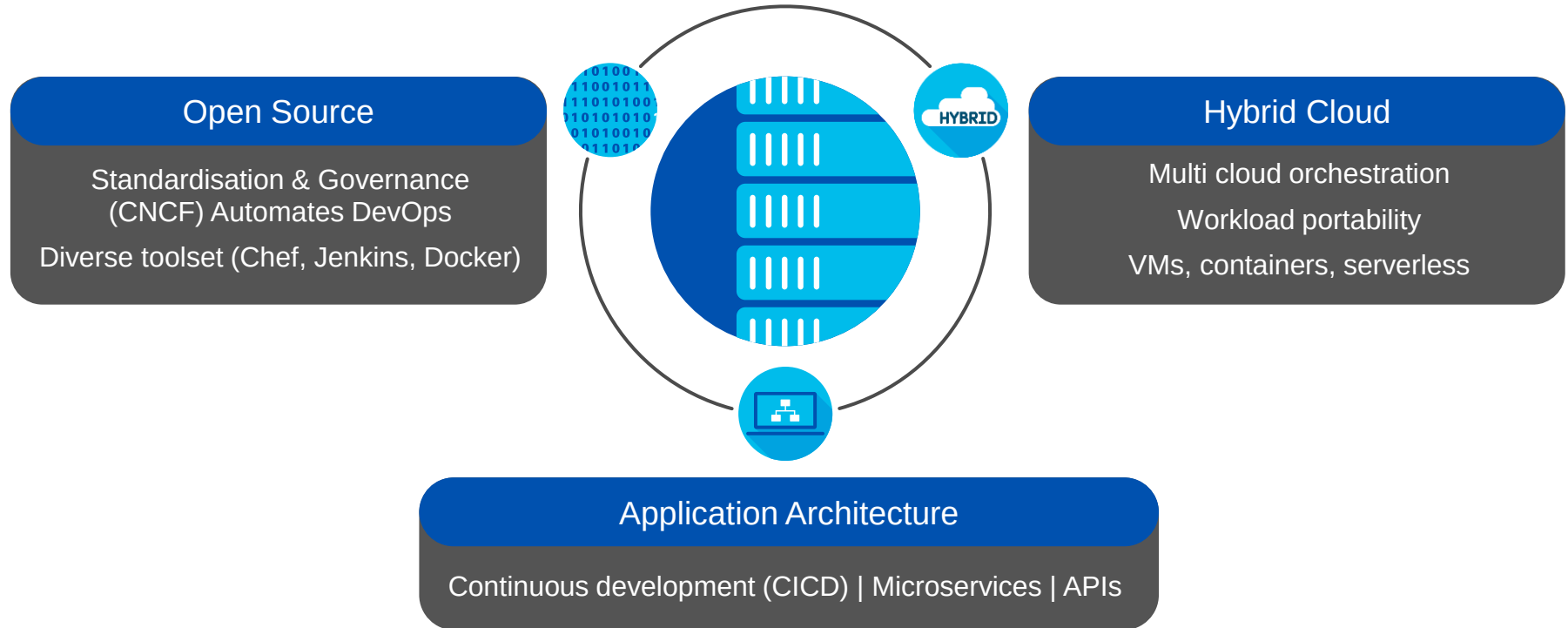
of high-maturity organizations are getting stronger security in the cloud

8%

of respondents qualify as highly cloud mature

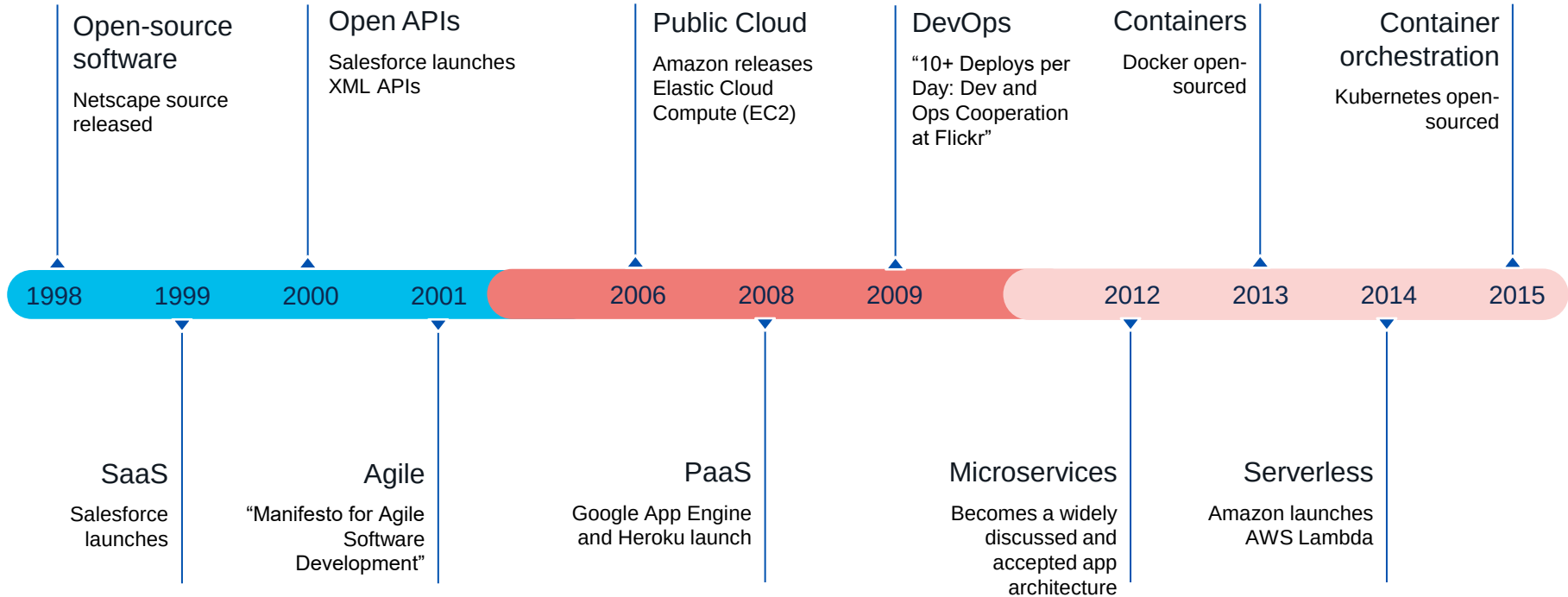
HashiCorp 2024 State of Cloud Strategy Survey

How are applications changing?

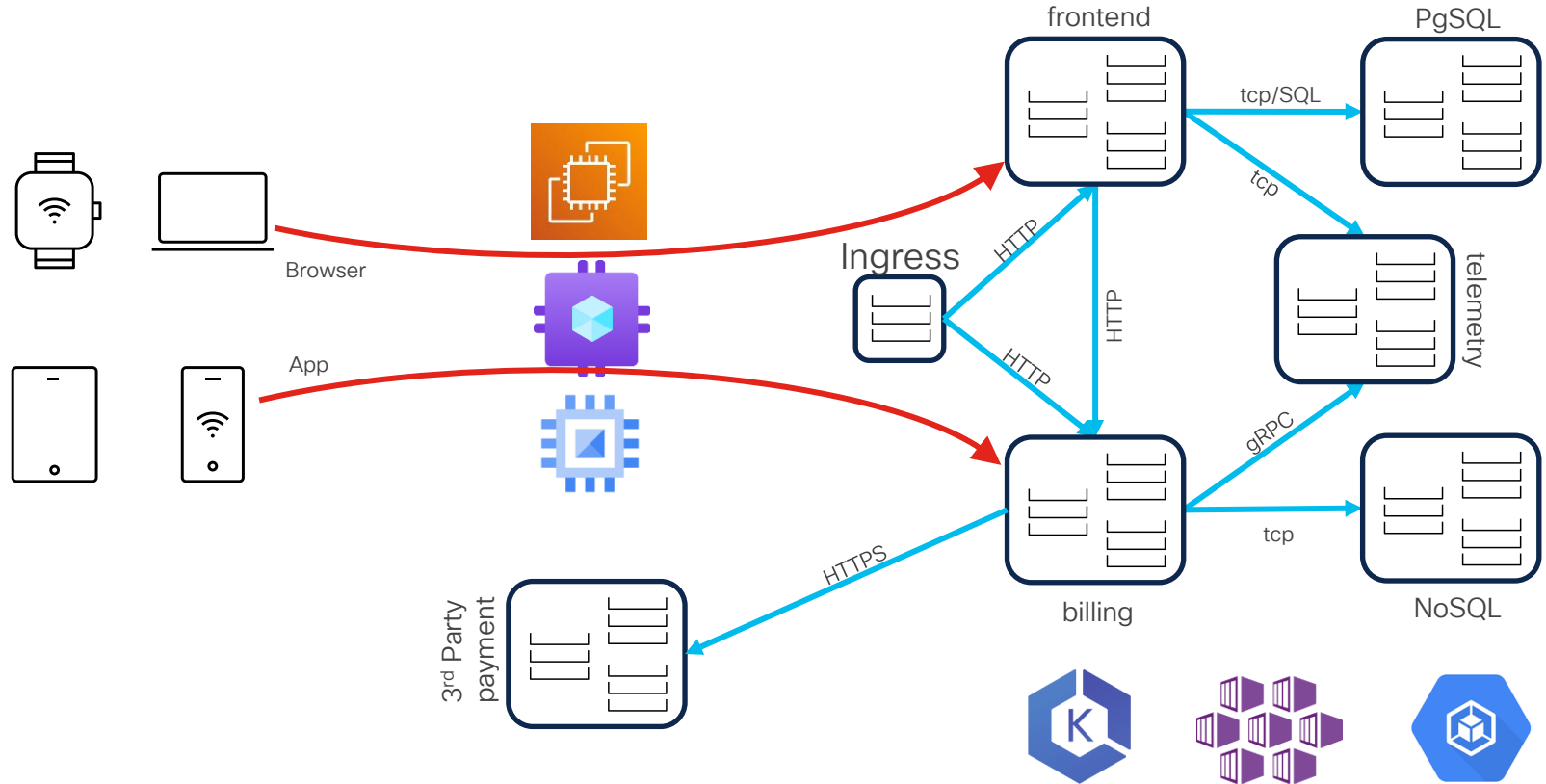


How did we get here?

From pets to cattle – the application infrastructure journey



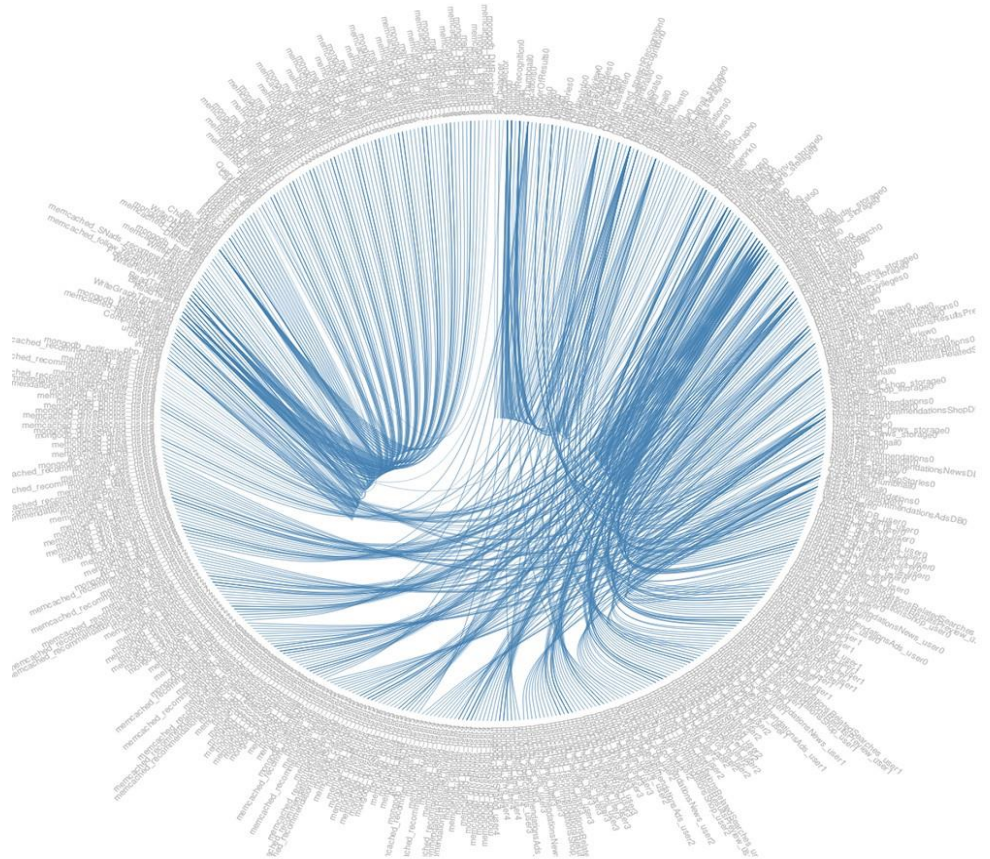
Simple modern application



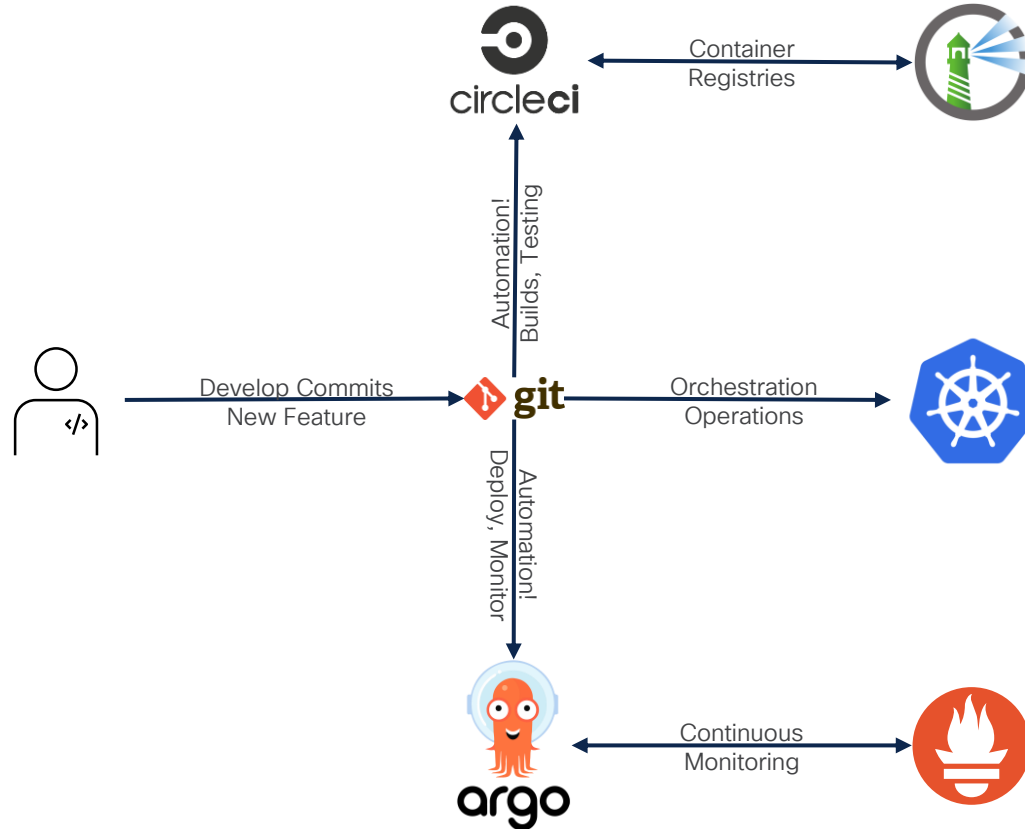
The reality

Deployed in Multi-cloud
using Microservices,
Serverless functions and
APIs

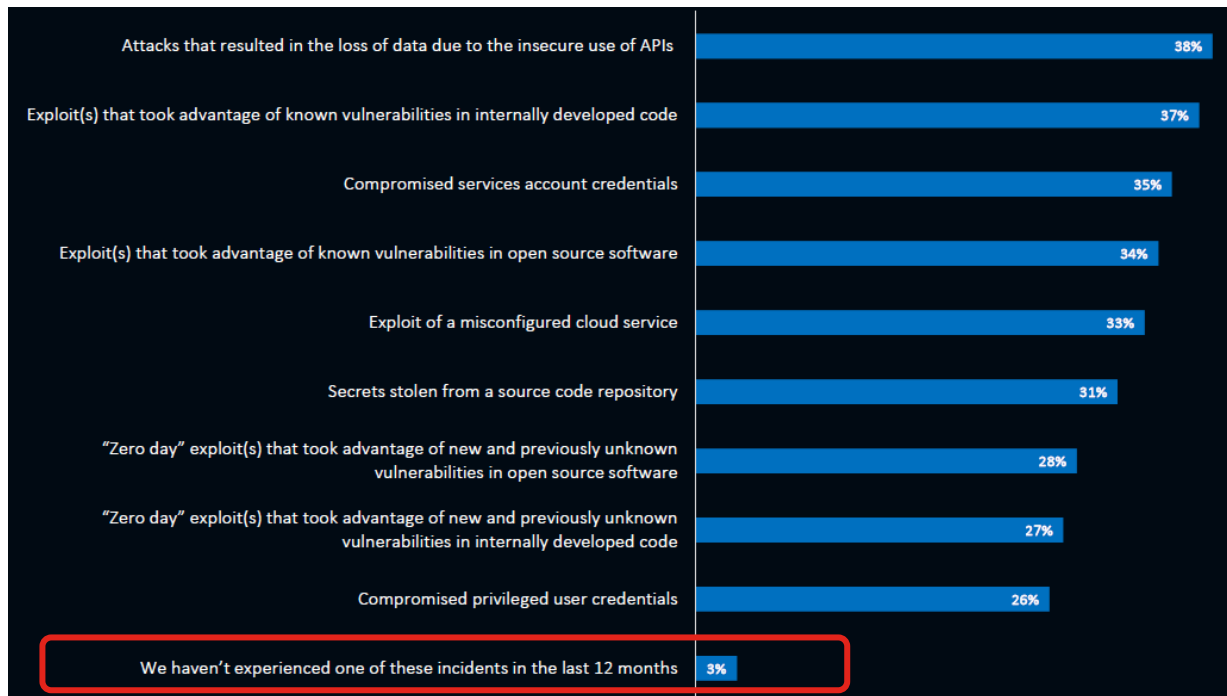
- Decoupled
- Dynamic
- Scalable



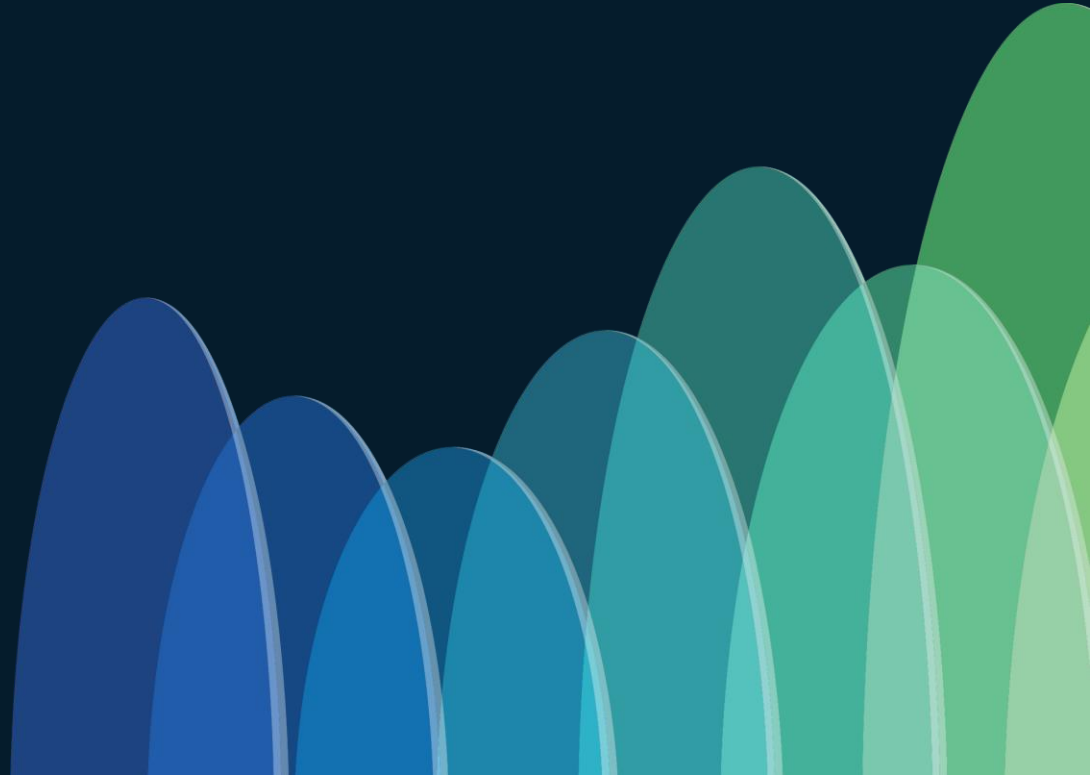
Application development workflows have evolved



Industry Survey: What Security Incidents Have You Experienced?

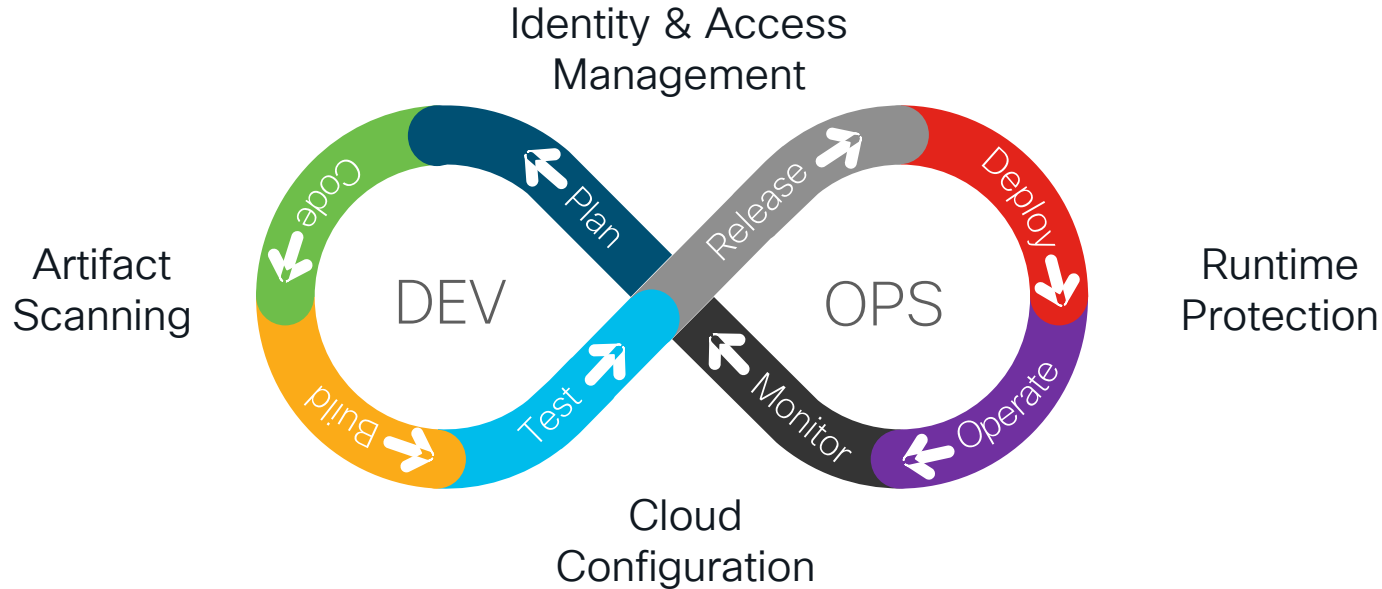


So where does
that leave
security teams?





Protecting Apps from Development to Runtime



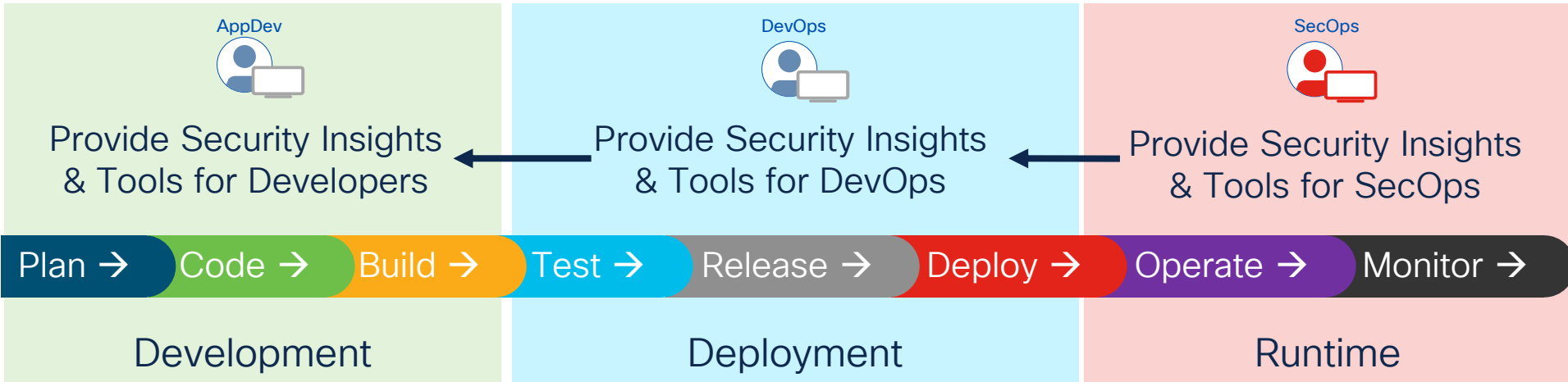
Protecting Apps from Development to Runtime



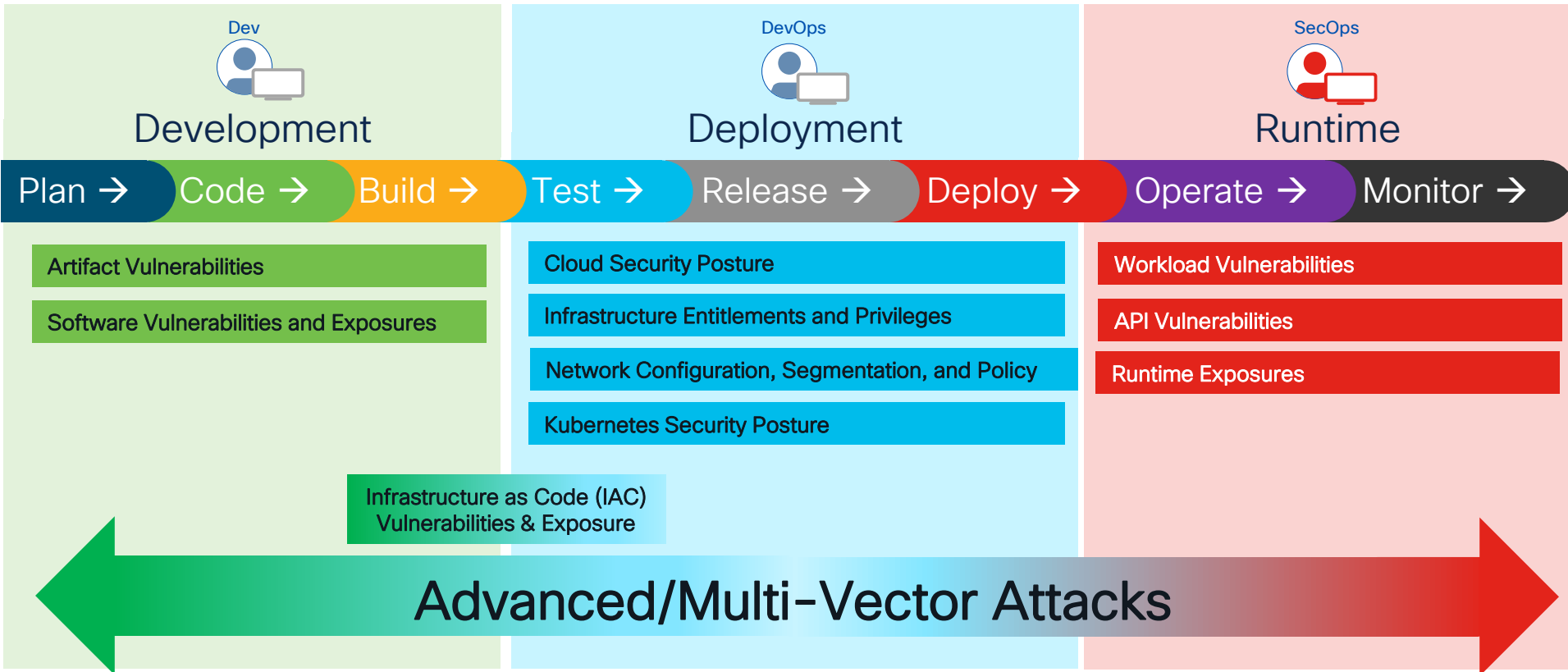
Security Commonly Remains an Afterthought



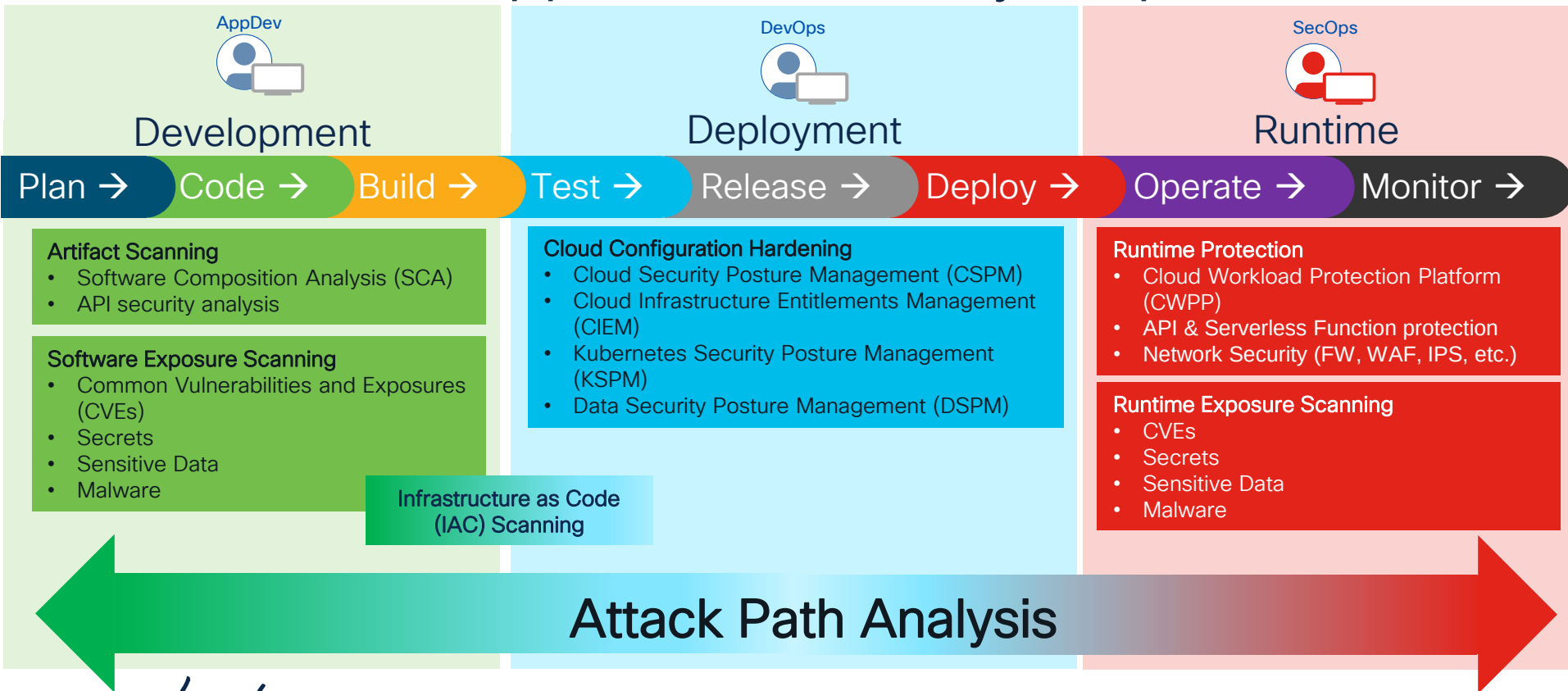
Shift-Left Goal for Cloud Native App Security



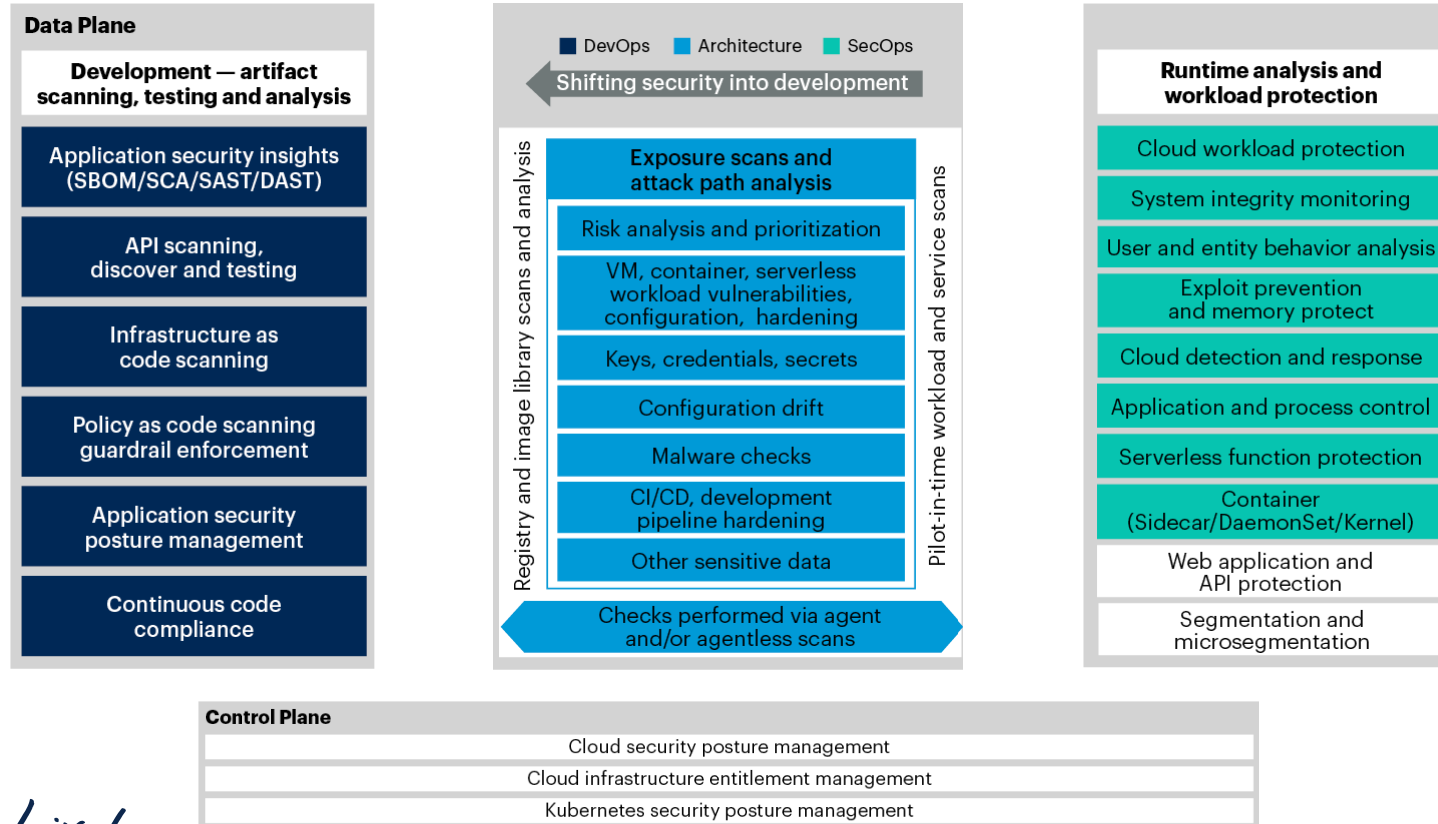
Cloud Native Application Security Vulnerabilities



Cloud Native Application Security Requirements



Gartner's View of Cloud and Application Security



Securing Public Cloud Infrastructure

Foundation to move up the application security stack

Adaptive Application Segmentation



As attributes and conditions change

Workload vulnerability and exploit detection



Behavior



Vulnerabilities



Exploits

Comprehensive visibility into multi-cloud activity



Consistent up-to-date view

Identify threats based on cloud infrastructure behavior



Behavior



Threats

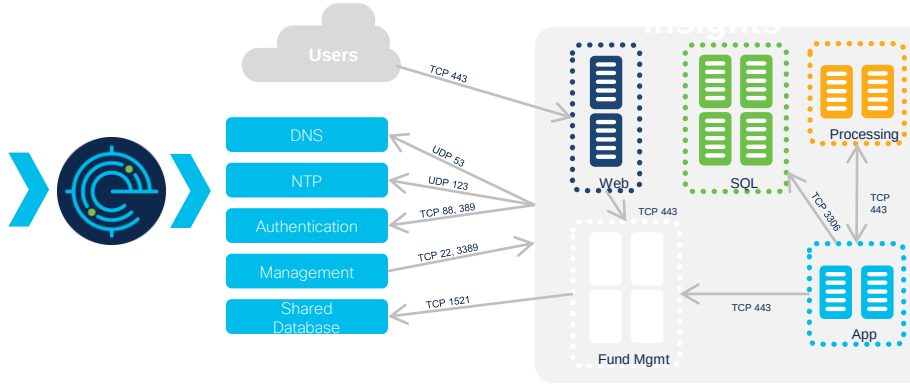
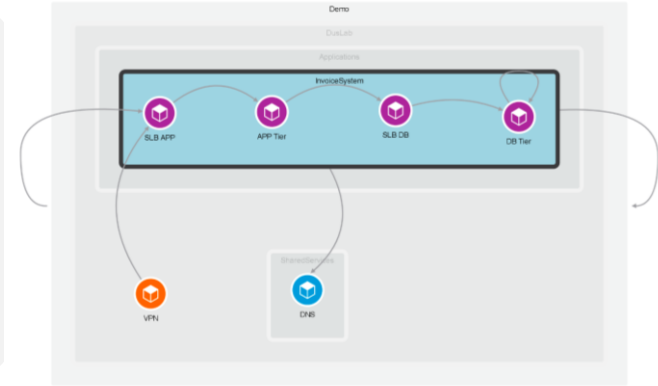
Addressing the Basics for Public Cloud Transition

Cloud Workload Protection done right

Automated discovery, clustering & policy generation with Cisco Secure Workload

Baseline workload protection posture

- Network communications
- Process behaviour
- Vulnerabilities
- Labels



Absolute and Default Policies13

Catch AllDENY

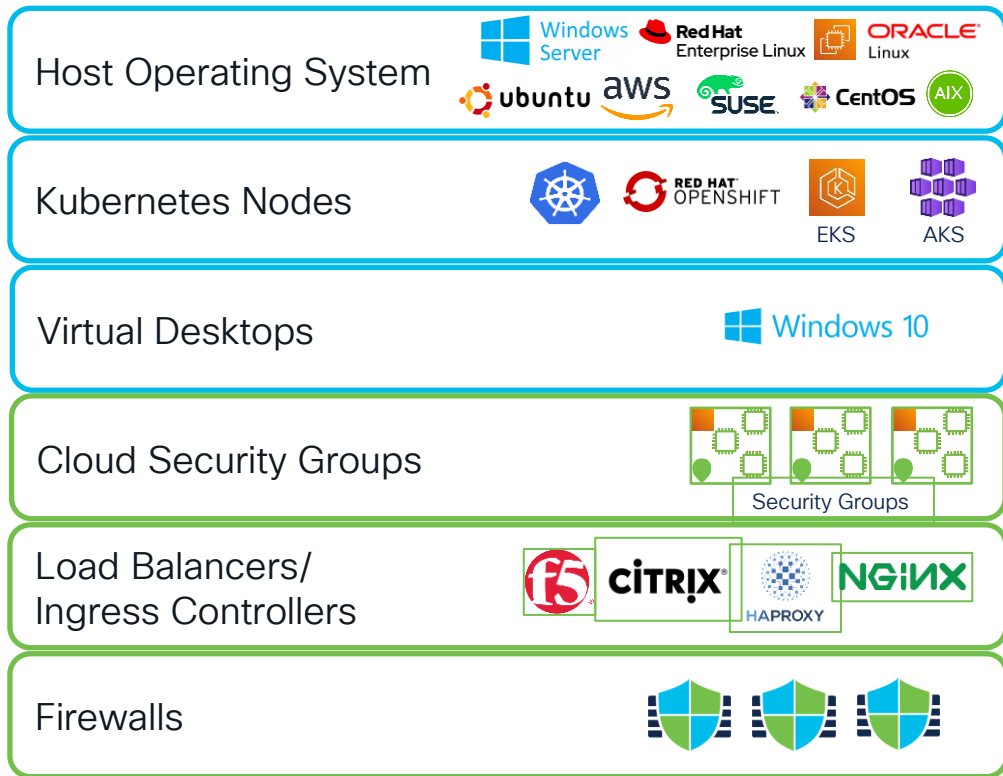
Grouped

Ungrouped

	Rank ↑↓	Priority ↑↓	Action ↑↓	Consumer ↓	Provider ↑↓	Protocols And Ports ↑↓	
	Absolute	100	<div><div></div>ALLOW</div>	<div><div></div>VPN</div>	<div><div></div>SLB APP</div>	TCP : 1936	<div><div></div><div></div></div>
	Default	100	<div><div></div>ALLOW</div>	<div><div></div>VPN</div>	<div><div></div>SLB APP</div>	TCP : 80 (HTTP)	<div><div></div><div></div></div>
	Default	100	<div><div></div>ALLOW</div>	<div><div></div>SLB DB</div>	<div><div></div>DB Tier</div>	TCP : 3306 (MySQL)	<div><div></div><div></div></div>
	Default	100	<div><div></div>ALLOW</div>	<div><div></div>SLB APP</div>	<div><div></div>APP Tier</div>	TCP : 8081	<div><div></div><div></div></div>
	Default	100	<div><div></div>ALLOW</div>	<div><div></div>Demo : DusLab : Applications : InvoiceSystem</div>	<div><div></div>Demo</div>	UDP : 123 (NTP) ...2 more	<div><div></div><div></div></div>
	Default	100	<div><div></div>ALLOW</div>	<div><div></div>Demo : DusLab : Applications : InvoiceSystem</div>	<div><div></div>Demo : DusLab : SharedServices : DNS</div>	UDP : 53 (DNS) ...1 more	<div><div></div><div></div></div>

The Policy Puzzle

Arriving at layers of policy



Policy Domains

Multiple **teams** and organizations

Multiple **environments** and clouds

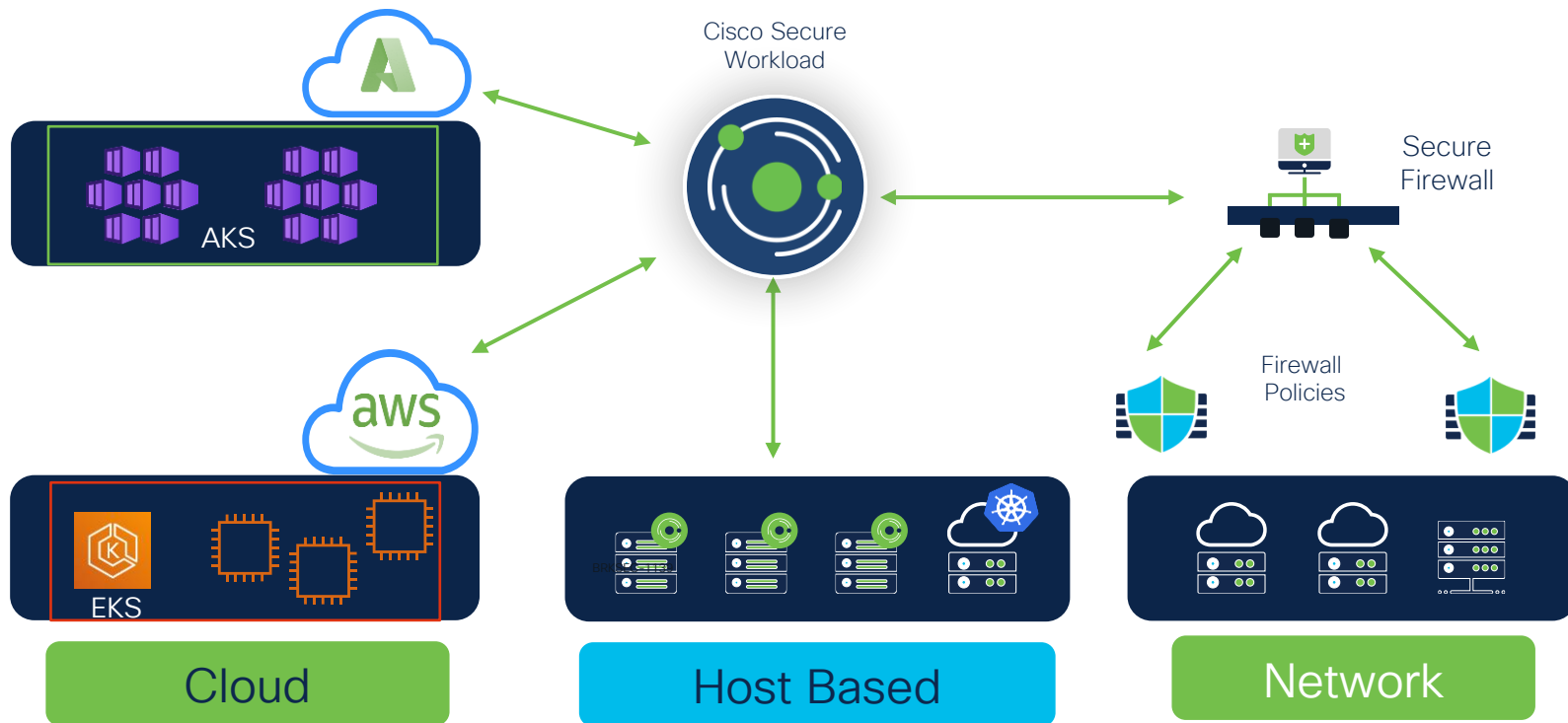
Each have **segmentation** methods and tools



Inconsistent and siloed islands of policy controls across network & apps

Enforce Policy with Cisco Secure Workload

Unified Policy across Host, Network and Cloud



Zoning & (Micro)Segmentation Demo

Instances (9) Info

Search

Instance state: **running** Clear filters

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 D
dev-storage-1	i-0fc7b1de63344f911	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-sql-1	i-0b063fd1cbeb0914d	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-web-1	i-0aa5be3edb1ef3226	Running	t2.micro	2/2 checks passed	No alarms	us-west-2c	-
dev-storage-2	i-050e049948215bbd5	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-213-2
dev-sql-2	i-04201f6c2fecfe88c	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-35-163-1
dev-web-2	i-0fd95bc88828304f1	Running	t2.micro	2/2 checks passed	No alarms	us-west-2b	ec2-34-209-1
aws-sapphire-prod-sql	i-0eee56c4a4238156f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
aws-sapphire-prod-web	i-07cf51cb82e99cf9b	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-
aws-sapphire-prod-nfs	i-05f7cda90d27d276f	Running	t2.micro	2/2 checks passed	No alarms	us-west-2a	-

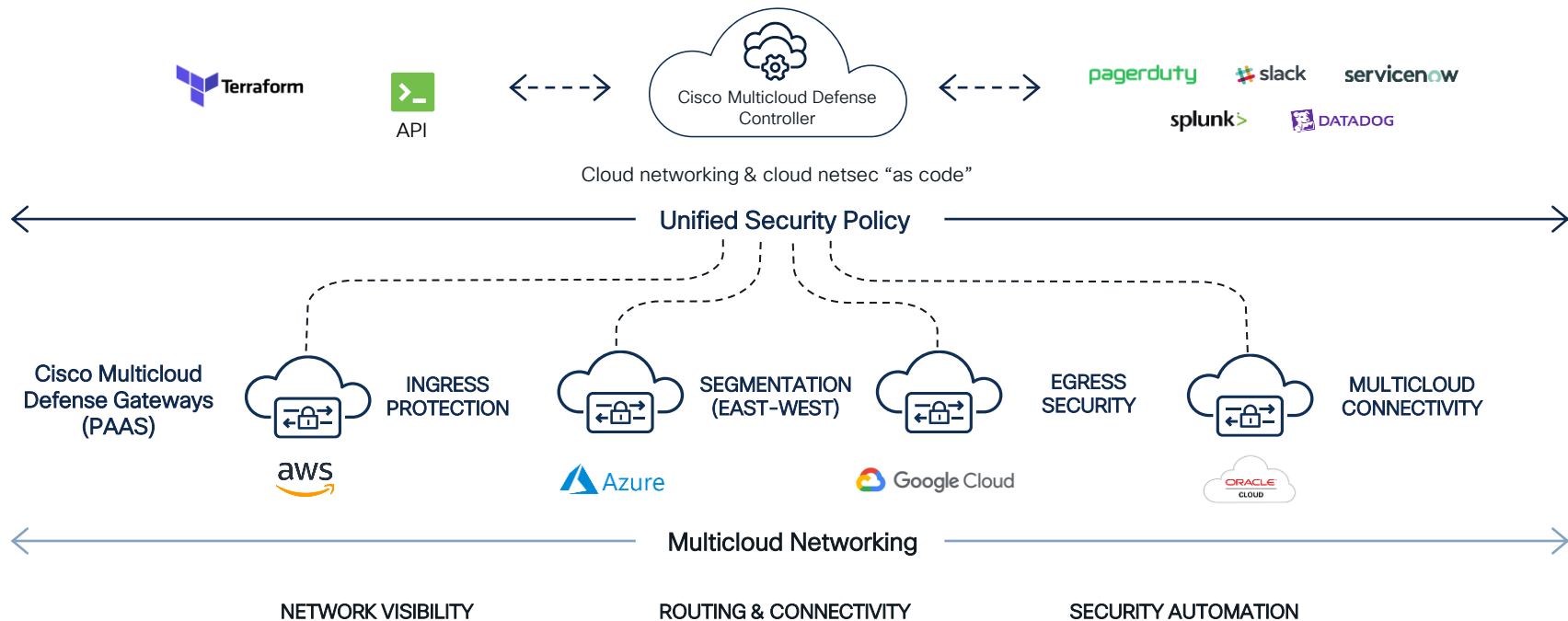
Select an instance

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

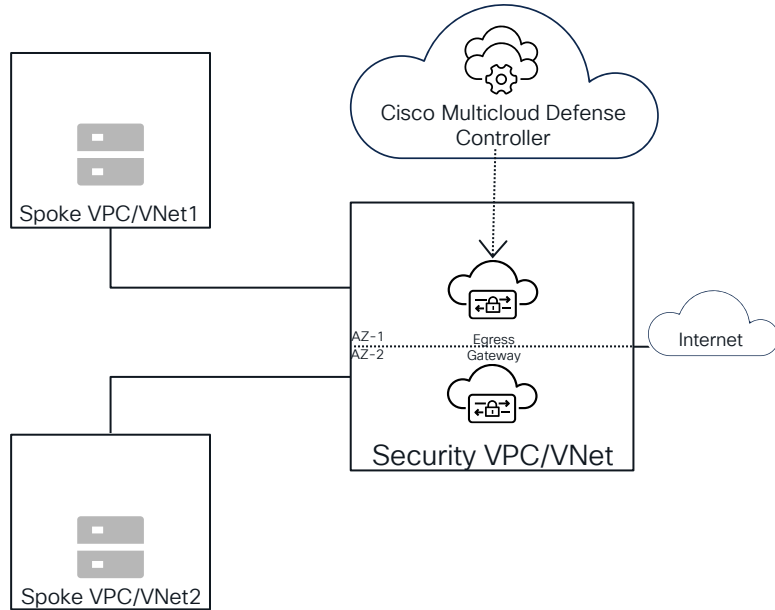
Cisco Multicloud Defense

Combining multicloud networking, automation, and cloud-native network security controls

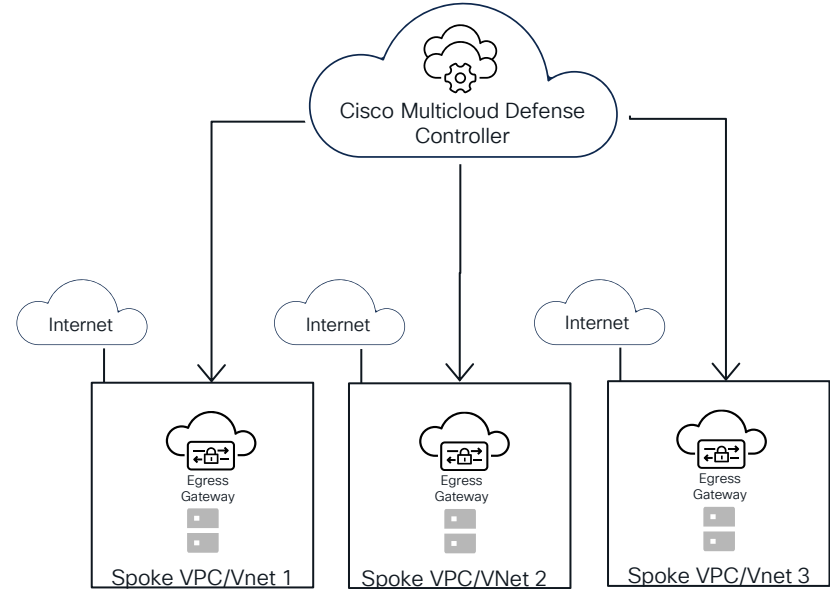


Deployment Models

Centralised Security Model



Distributed Security Model



Use cases



**Ingress
protection**



**Egress
security**



Segmentation

Why Critical?

**Stop inbound threats for web
and non-web apps**

**Block Command & Control,
Botnets, Data Exfiltration**

Mitigate Lateral Movement

Market Drivers

- Supply Chain Vulnerabilities
- Library Exploits (Log4Shell)
- Compliance

- Zero Days
- C2, Ransomware
- Compliance

- Zero Trust / Least Privilege
- Data Protection
- Compliance

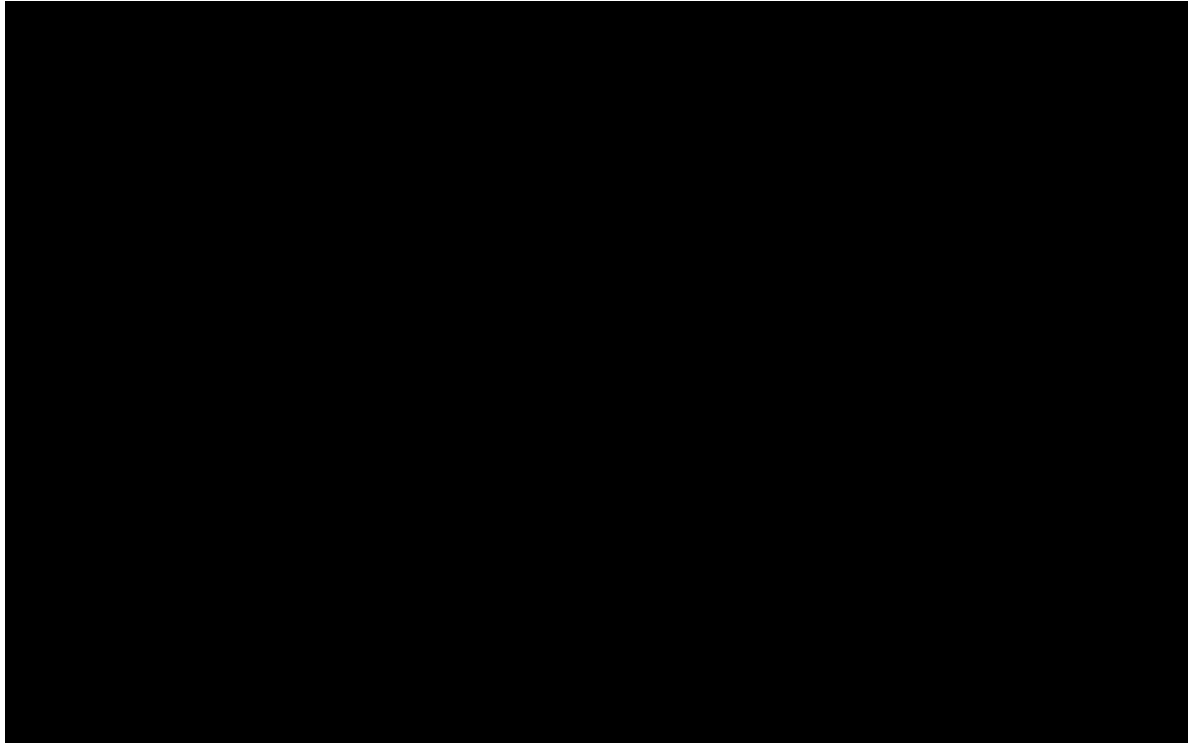
**Security
Controls**

- ✓ WAF
- ✓ IDS / IPS
- ✓ Geo IP
- ✓ Malicious IP
- ✓ Antivirus

- ✓ FQDN Filtering
- ✓ URL Filtering
- ✓ DLP
- ✓ IPS / IDS
- ✓ Antivirus

- ✓ Cloud-native Identity
- ✓ IPS / IDS
- ✓ Antivirus

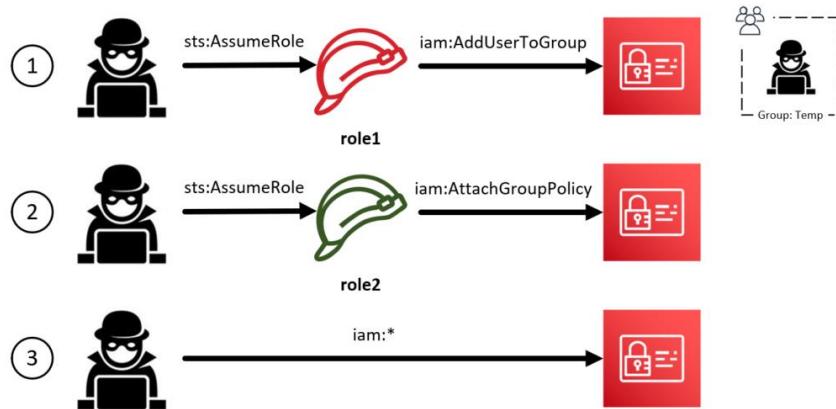
Firewalling in the Cloud demo



Are we safe with
zoning,
microsegmentation
& firewalling 😊

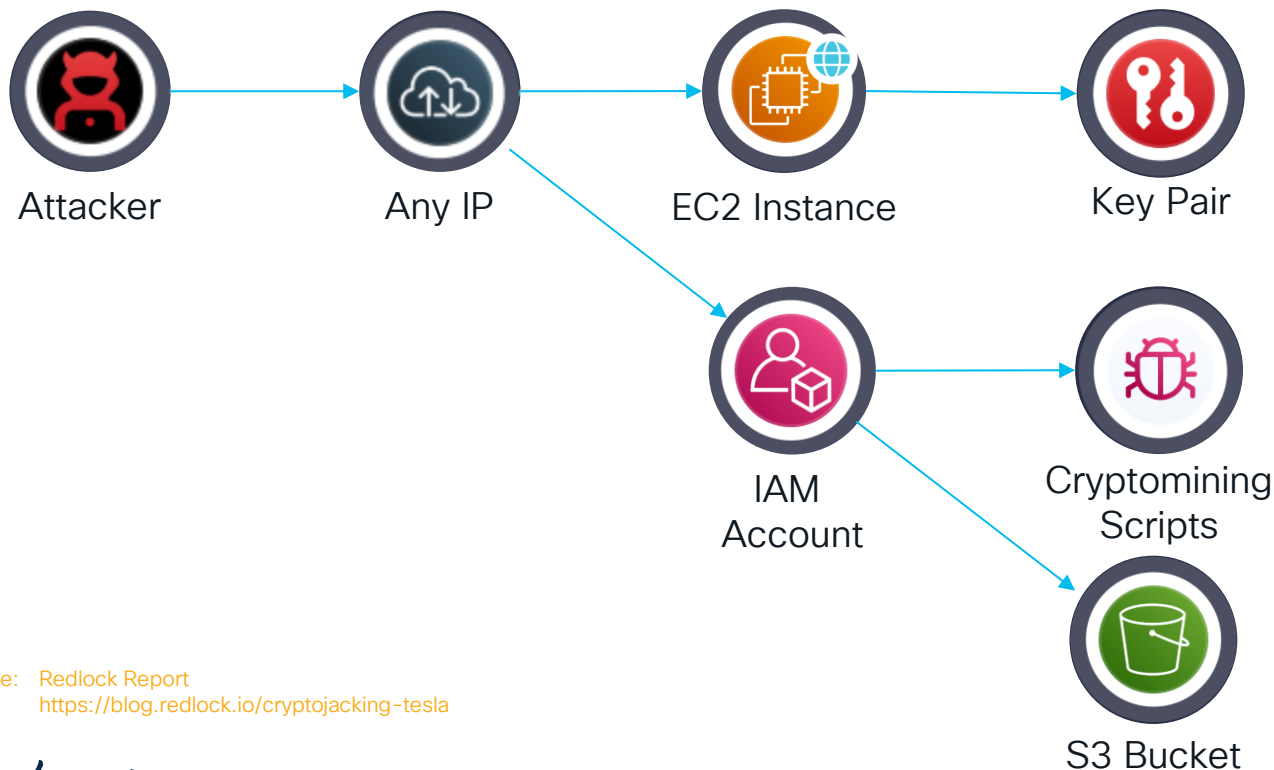


The Bigger Issue - Privilege Escalation



Source - <https://sra.io/blog/aws-iam-exploitation/>

Public Facing Assets, Embedded Secrets & more



Source: Redlock Report
<https://blog.redlock.io/cryptojacking-tesla>

How Serious is it?



139M

Number of
cryptojacking
attacks in 2022
(43% increase)



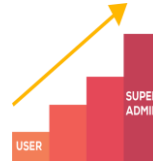
70%

of organizations
have a Kubernetes
API server that is
publicly accessible



99%

of cloud failures are
due to cloud
misconfigurations



80%

of security
breaches
involve
privileged
credentials



72%

of
organizations
have at least
one S3 bucket
that allows
public “read”
access



36%

of organizations
keep unencrypted
secrets and
personally
identifiable
information (PII) in
these cloud
services.

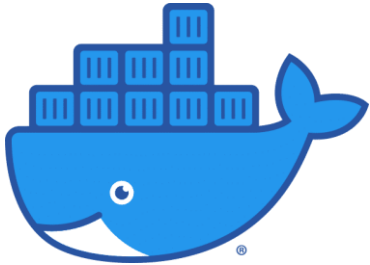
Sources: IBM/Ponemon Institute, Cost of a Data Breach Report 2023
Orca 2022 State of Public Cloud Security Report
Sonic Wall 2023 Cyber Threat Report
Gartner 2022 Report
Forrester

Cloud Security Posture Management Demo



Securing Cloud Native Technologies

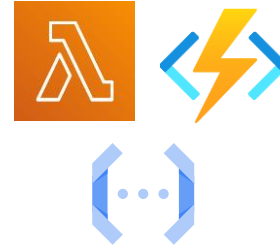
Cloud Native Technologies to Secure



Containers



Kubernetes



Serverless



API

Anatomy of a Container



USER moby ENV var1
EXPOSE 443/tcp ENV var2

Base Image

Runtime

Dependencies

Application

```
Dockerfile X
Dockerfile > ...
1  # BASE LAYER
2  FROM rockylinux:9.1.20221123 AS base
3
4  # RUNTIME LAYER
5  RUN dnf install -y python3 python3-pip python3-setuptools && \
6     dnf clean all
7
8  # DEPENDENCIES
9  RUN pip install wheel && pip install "fastapi[all]" "uvicorn[standard]"
10
11 # APPLICATION
12 WORKDIR /app
13 COPY ./src /app
14
15 RUN useradd -u 5678 appuser && chown -R appuser /app
16
17 # SETTINGS
18 USER appuser
19 EXPOSE 8080
20
21 ENV STORAGE_SVC storage-service
22 ENV STORAGE_PORT 8080
23 ENV ACCESS_KEY never_do_this_in_prod
24 ENV SECRET_KEY cross_the_streams_bad
25
26 CMD ["uvicorn", "--host", "0.0.0.0", "--port", "8080", "example:api"]
27
```

Software Bill of Materials

```
8 # DEPENDENCIES
9 RUN pip install wheel && pip install "fastapi[all]" "uvicorn[standard]"
```



Container Settings

Base Image

Runtime

Dependencies

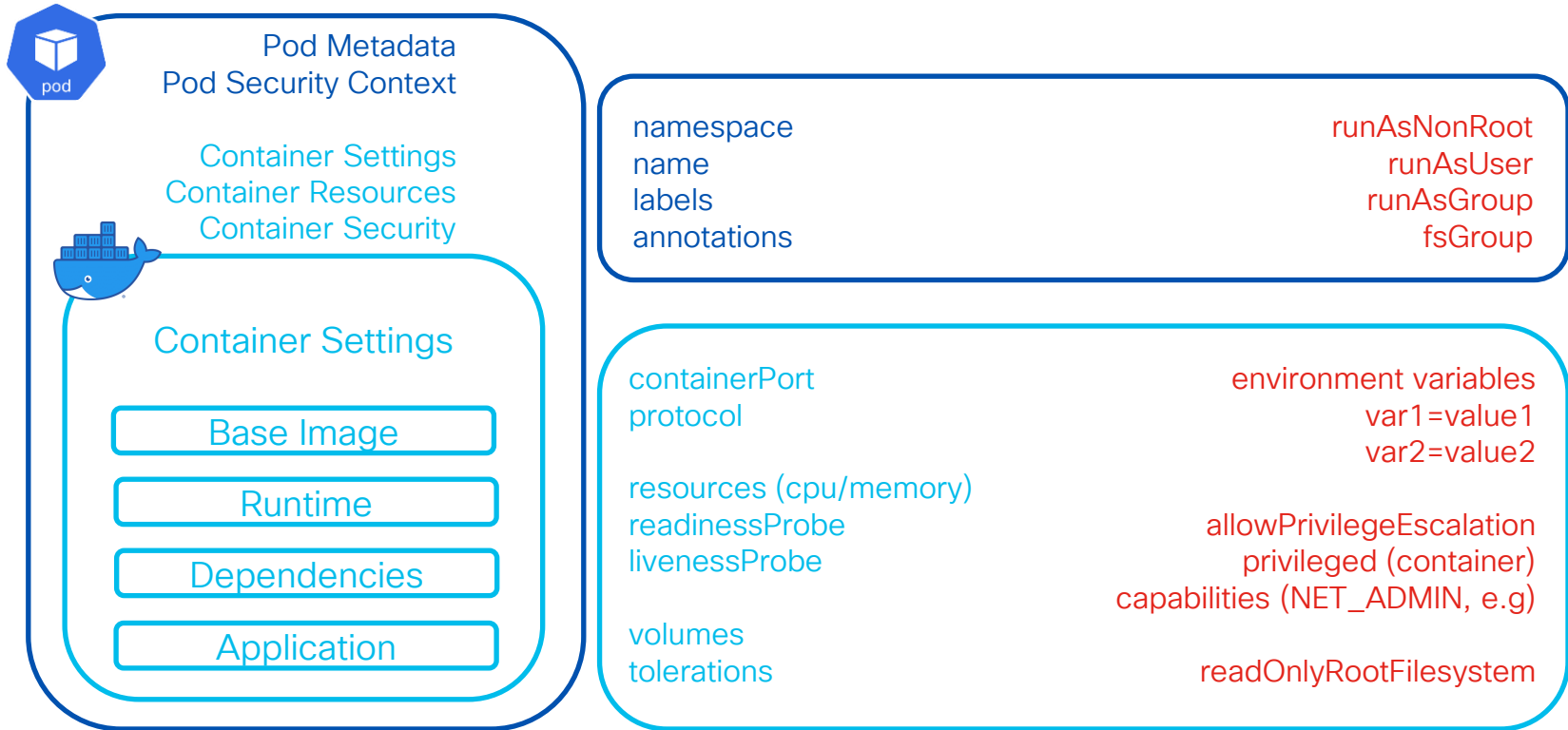
Application

identified.layer.dependencies.txt

identified.layer.dependencies.txt

1	Jinja2	3.1.2	python
2	MarkupSafe	2.1.1	python
3	PyYAML	6.0	python
4	anyio	3.6.2	python
5	certifi	2022.12.7	python
6	click	8.1.3	python
7	dnspython	2.2.1	python
8	email-validator	1.3.0	python
9	fastapi	0.88.0	python
10	h11	0.14.0	python
11	httpcore	0.16.3	python
12	httptools	0.5.0	python
13	httpx	0.23.3	python
14	idna	3.4	python
15	itsdangerous	2.1.2	python
16	orjson	3.8.4	python
17	pydantic	1.10.4	python
18	python-dotenv	0.21.0	python
19	python-multipart	0.0.5	python
20	rfc3986	1.5.0	python
21	six	1.16.0	python
22	sniffio	1.3.0	python
23	starlette	0.22.0	python
24	typing_extensions	4.4.0	python
25	ujson	5.6.0	python
26	uvicorn	0.20.0	python
27	uvloop	0.17.0	python
28	watchfiles	0.18.1	python
29	websockets	10.4	python
30	wheel	0.38.4	python

Anatomy of a Kubernetes Application



Leveraging Industry Best Practices



Pod Metadata
Pod Security Context

Container Settings
Container Resources
Container Security



Container Settings

Base Image

Runtime

Dependencies

Application

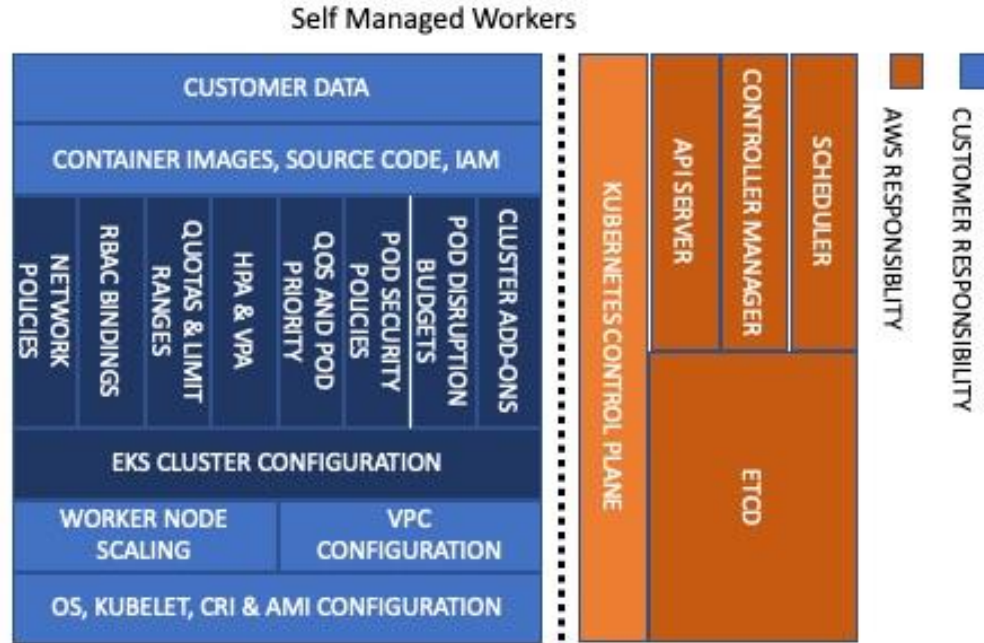
CIS Kubernetes Benchmarks

<https://www.cisecurity.org/benchmark/kubernetes>

CIS Docker Benchmarks

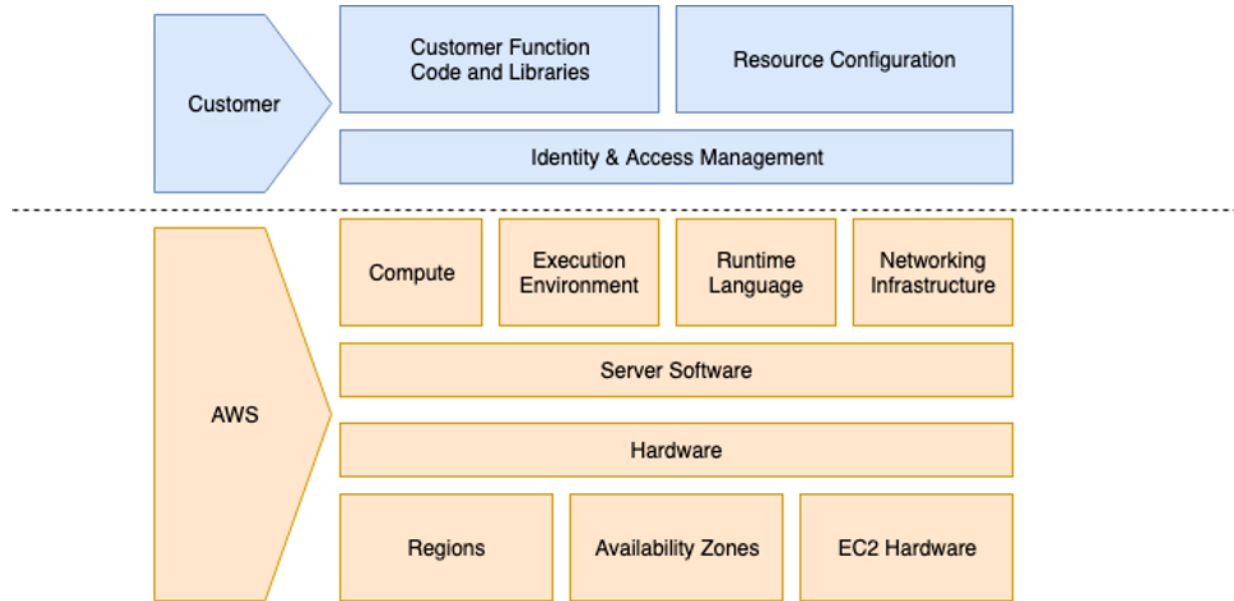
<https://www.cisecurity.org/benchmark/docker>

Shared Responsibility Model for Kubernetes



Source: AWS Shared Responsibility Model for EKS
<https://aws.github.io/aws-eks-best-practices/security/docs/index.html>

Serverless Doesn't Mean Secureless

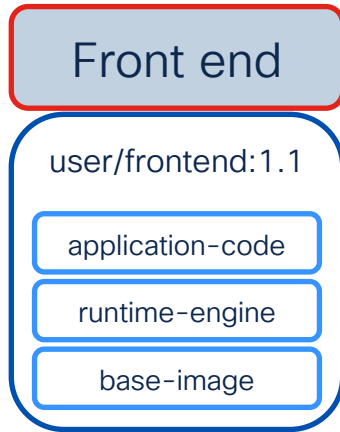
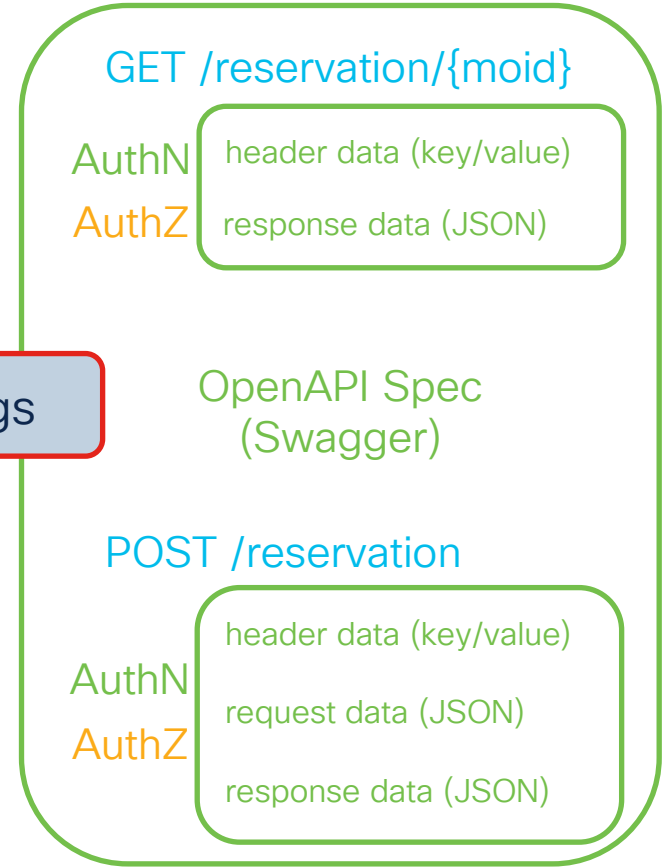


Source: AWS Shared Responsibility Model for Serverless

<https://docs.aws.amazon.com/whitepapers/latest/security-overview-aws-lambda/security-overview-aws-lambda.html>

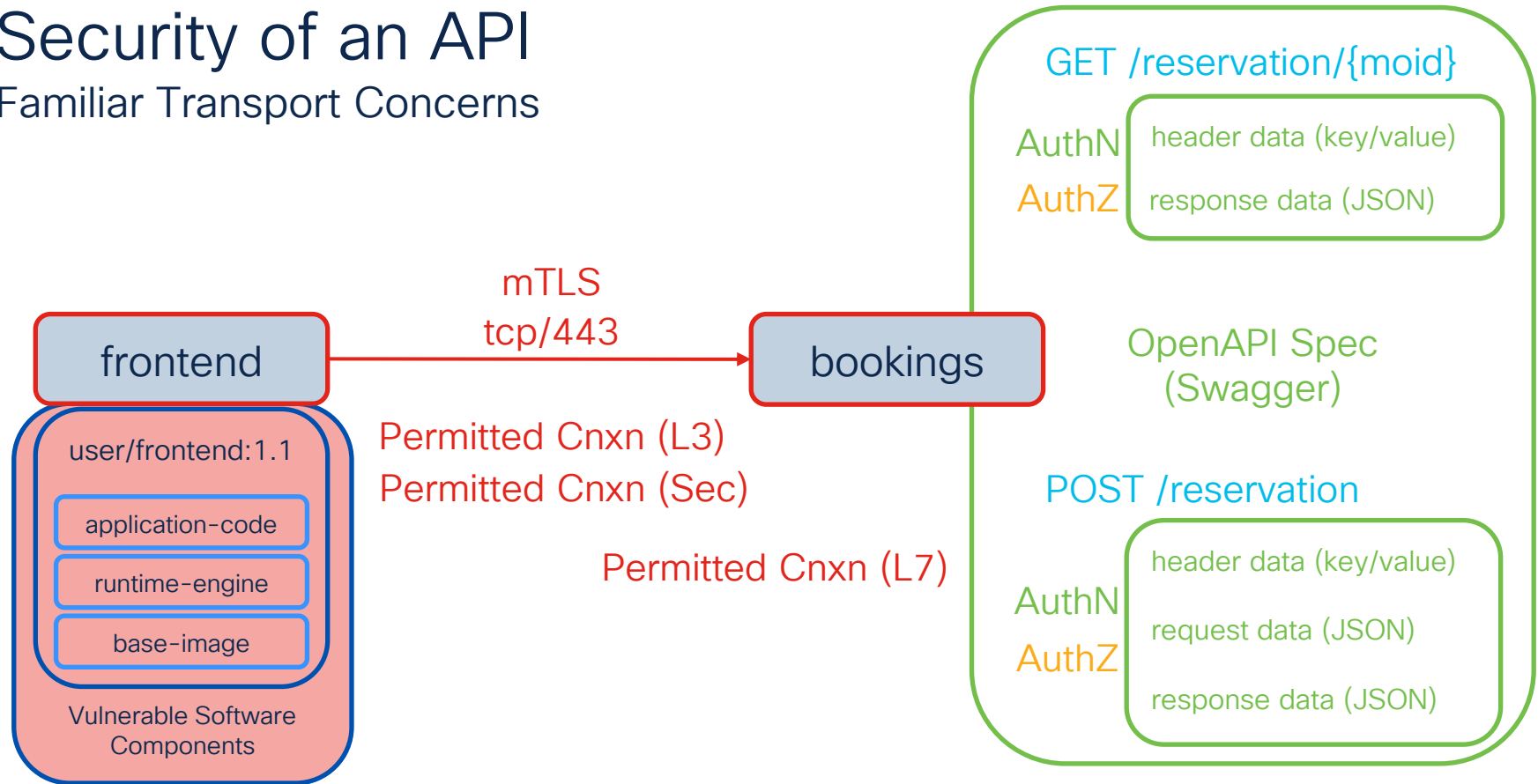
Anatomy of an API

(Application Programming Interface)



Security of an API

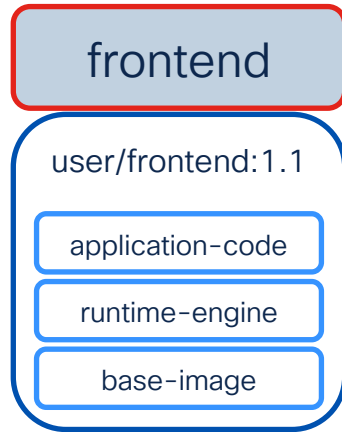
Familiar Transport Concerns



Security of an API

Application Layer (L7) Concerns

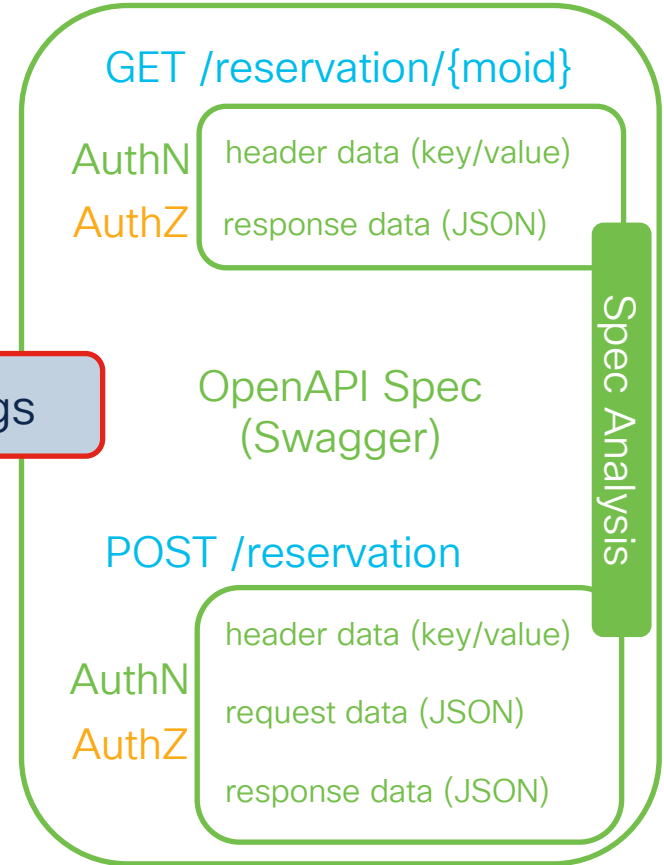
Broken Object Level AuthZ



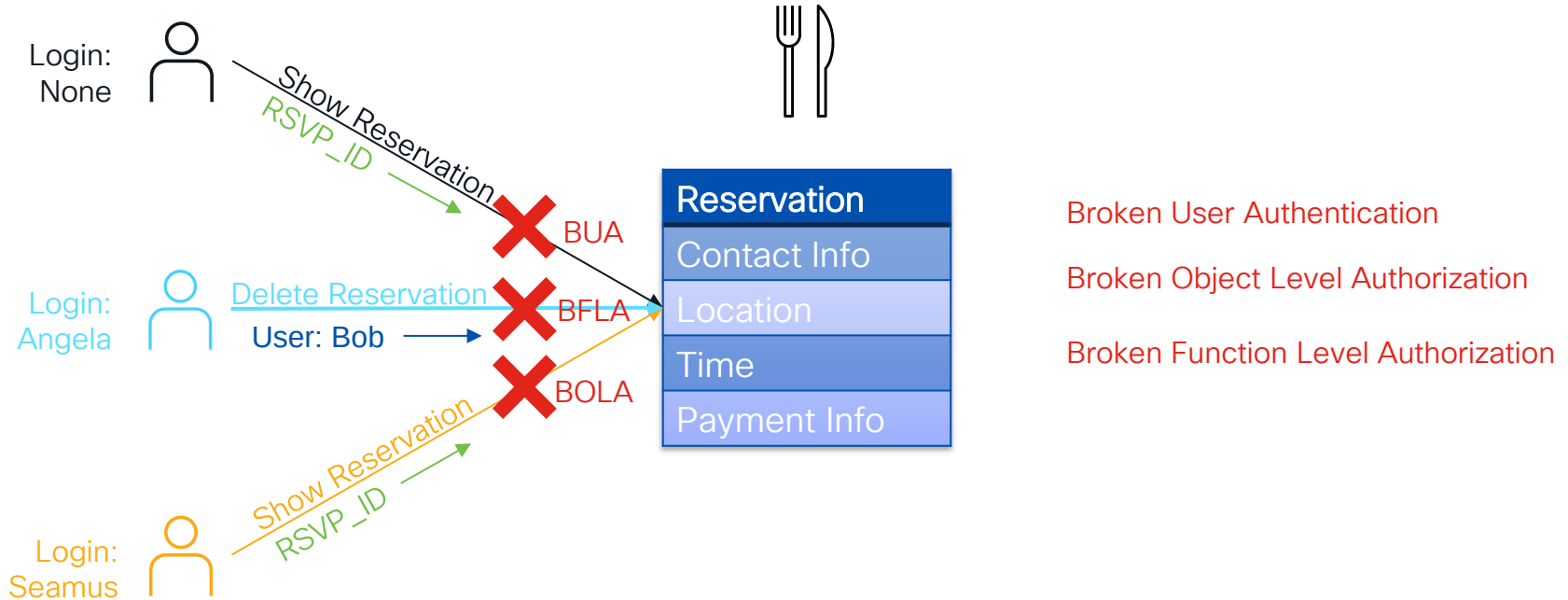
AuthN Token

bookings

Broken Function Level AuthZ



Broken Authentication and Authorization



How Bad is it?



78%

of identified attack paths use known vulnerabilities (CVEs) as an initial access attack vector



93%

of companies had a Kubernetes security incident in the last 12 months



#1

API attacks will become the most-frequent attack vector



286%

quarterly increase in API attacks in 2022



20%

of organizations have experienced a breach resulting from insecure APIs

Vulnerabilities Management & API Security Demo



Traditional Analysis

CVE list

- 1 => CVE1, CVE2
- 2 => CVE2, CVE3
- 3 => CVE4, CVE5
- ...



Container X
has CVEs



EC2 has
public SSH

EC2 has
admin S3
access

Container list

- A => 1
- B => 2
- C => 3
- ...



EC2 has
malware

API served
from container X

API list

- A
- B
- C
- ...



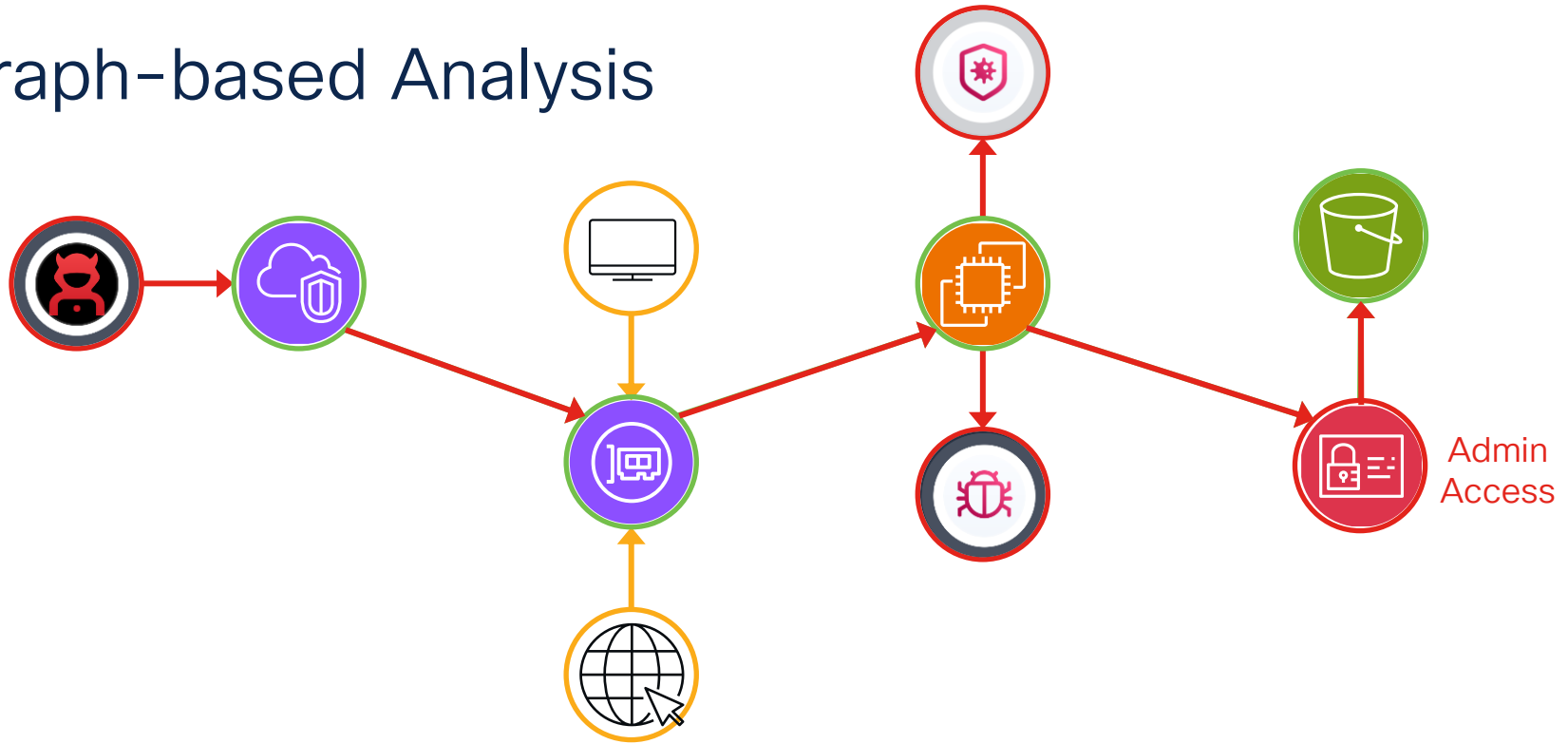
API has weak
authentication



Final List

- Result 1 => API A, Container 1, CVE1, CVE2
- Result 2 => API B, Container 2, CVE2, CVE3
- Result 3 => API C, Container 3, CVE4, CVE5
- ...

Graph-based Analysis



A well-architected single-vendor CNAPP offering should have the following characteristics ... Deep understanding of relationships between the elements of an application (VMs, containers, service functions and storage), security posture, permissions and connectivity, typically enabled by underlying graph database technology.

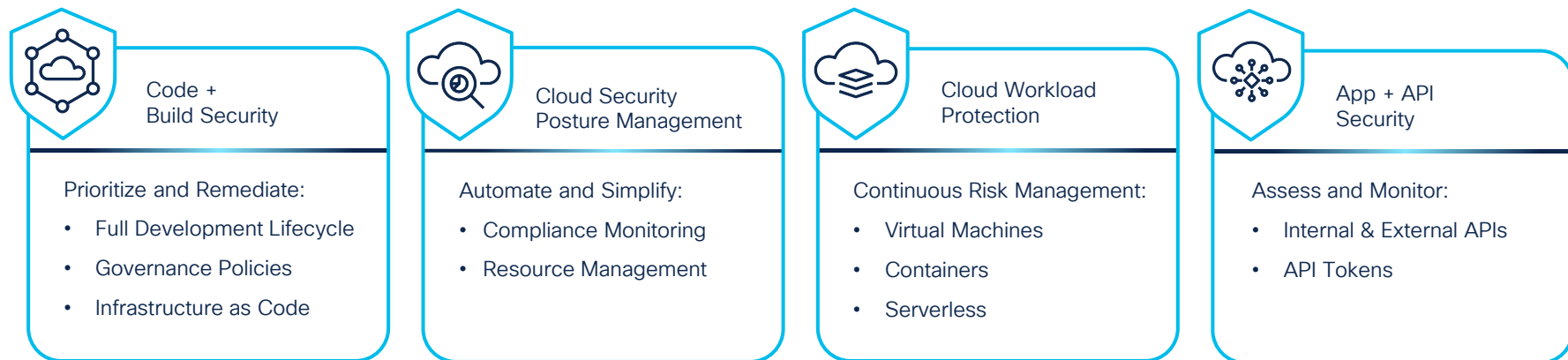
—Gartner

Attack Path Analysis Demo



Cisco Cloud Application Security (Panoptica)

Comprehensive Code to Cloud Security



Prioritize with precision.
Remediate the risks that matter—first.

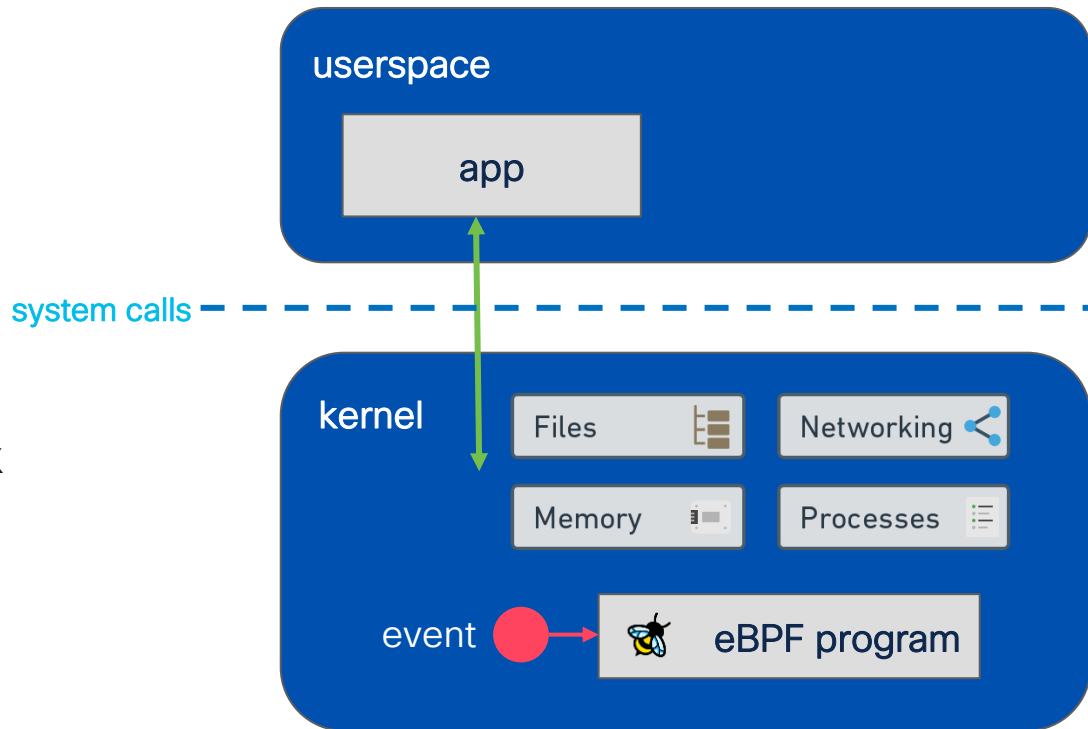
Open-Source Projects driving Cloud Native Visibility & Policy



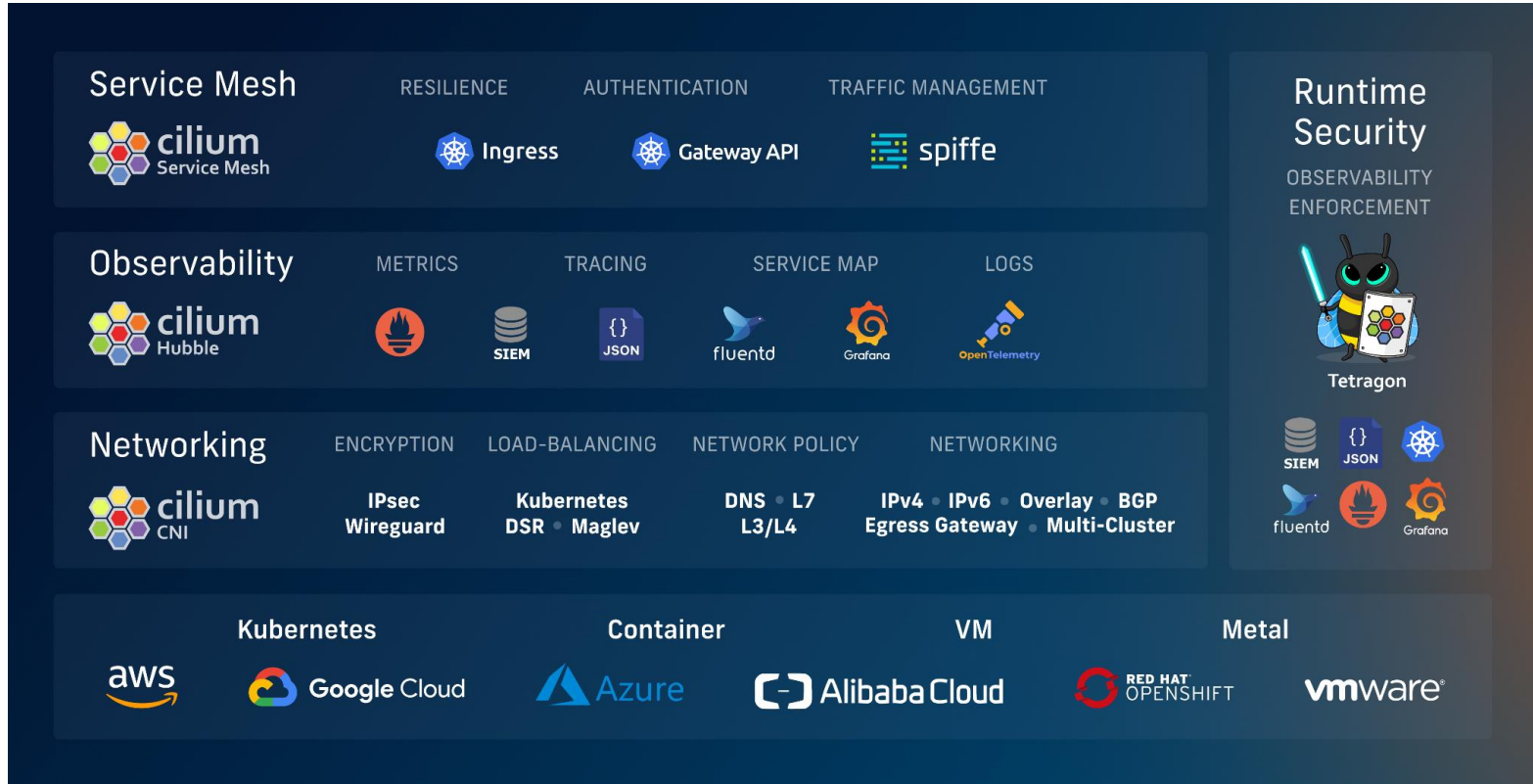


Makes the Linux kernel programmable in a secure and efficient way.

“What JavaScript is to the browser, eBPF is to the Linux Kernel”

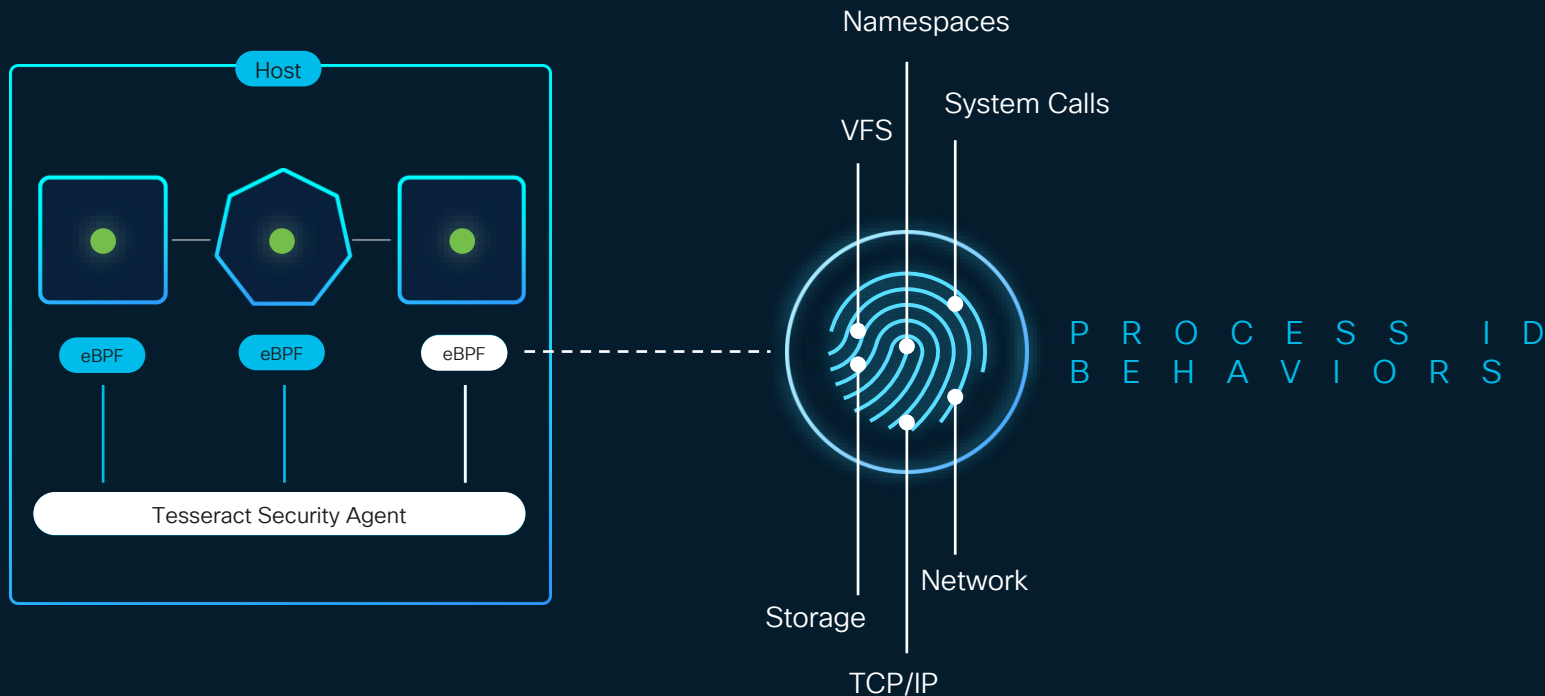


The Isovalent Overview



Deep visibility and enforcement in the workload

Built on Isovalent Tetragon



Introducing Cisco Hypershield Vision

Scalable hyper-distributed architecture

AI-Native

Built-in AI from inception.

Earns your trust, analysis-backed recommendations and interactions



Cloud-Native

Built on open source eBPF

eBPF powers default network for cloud-native workloads in hyperscalers

Hyper-Distributed

Distributed enforcement points across appliances, in the network, and the workload.

Managed as one system.

Cisco Hypershield



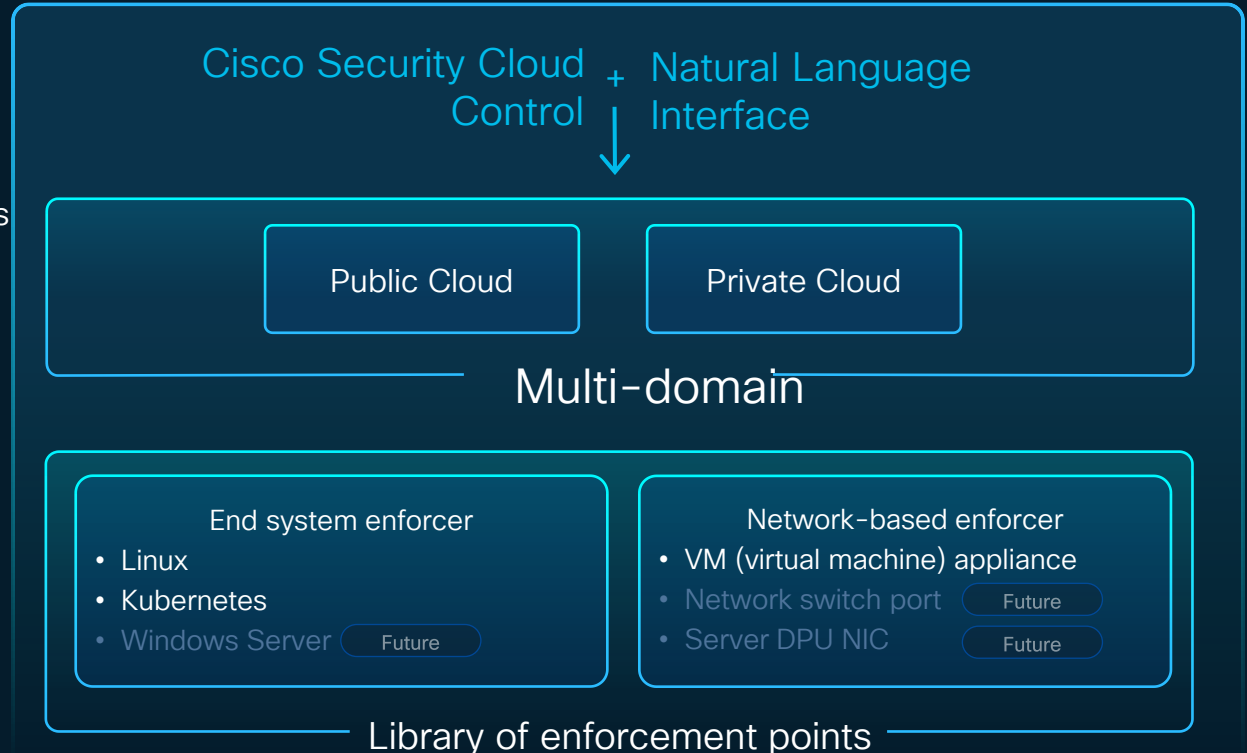
Manage globally, enforce locally

Includes

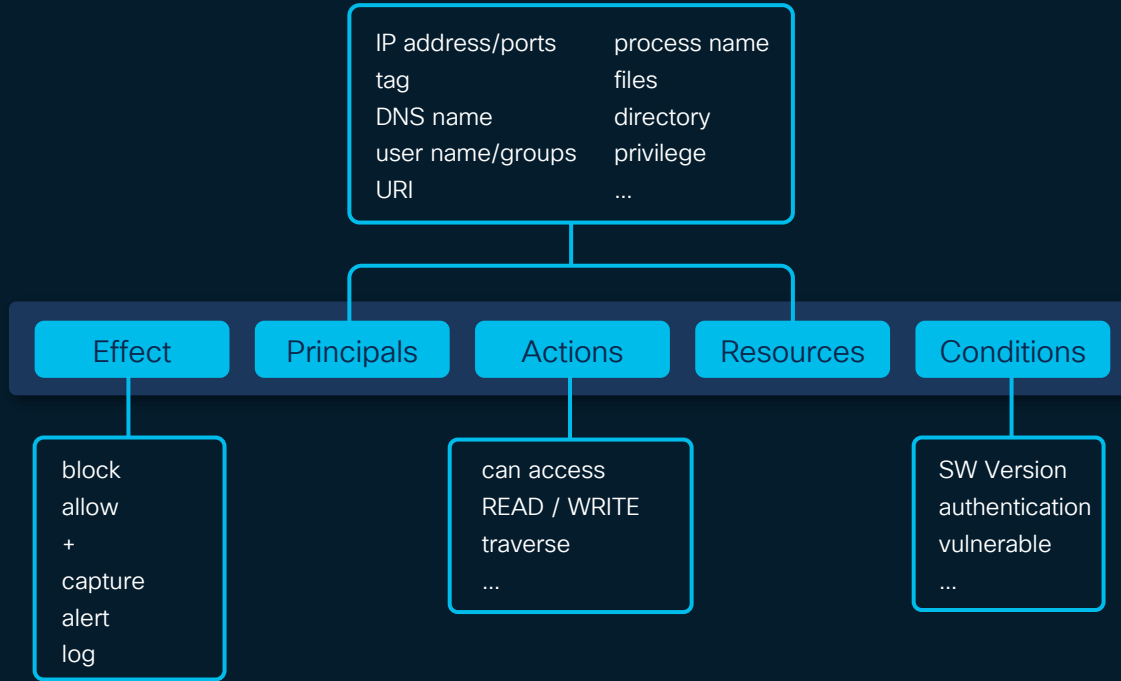
- Unified management
- Single global policy
- Intelligent placement of shields
- Integrations with cloud/app/infra metadata

Environments

- Kubernetes
- Cloud – Private/Public
- On-prem



Single policy covering network and workload



Hypershield Policy Construct

- Intent based
- Order independent
- Rule Auto-compilation
- Intelligent Rule Placement
- Single Global Policy
- Unified management

Hypershield AI can recommend PARC policies

✓ Distributed Exploit Shield | runc-exec...

✓ Verified

^

REMEDIATION 1

Recommended

...

The Distributed Exploit Shield blocks new container processes with a current working directory of "/" in the host namespace.

Reason

Remediates vulnerability CVE-2024-21626

Effect

Block and alert

Principal

/usr/local/sbin/runc

Action

sys_execve

Resource

*

Condition

when principal.version <= 1.1.11 or unknown
and action.cwd = "host_ns:/"

Deployed by 8,734 other customers

Deploy

View 3 alternative remediations

Archive

AI generated rule blocking a vulnerable container process:

Effect

Block & Alert

Principals

File path / executable

Actions

Execute Permit

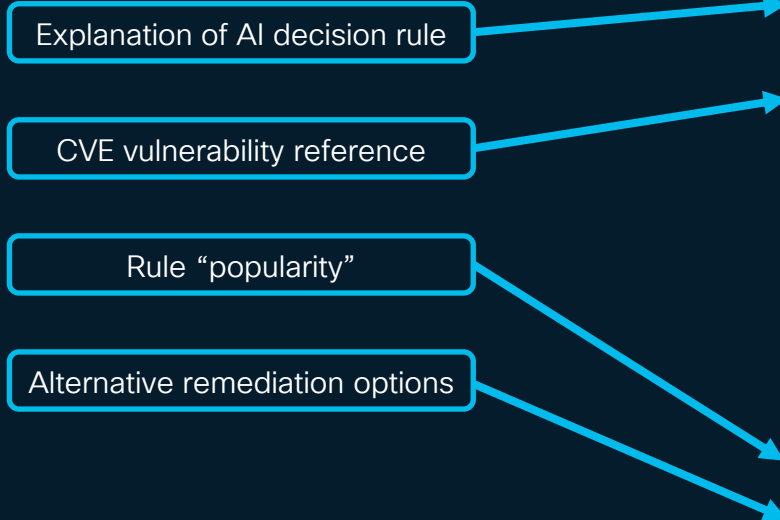
Resources

* (act on any resource)

Conditions

Minimum version & namespace

AI-Based Policy Engine – Earning Trust



Distributed Exploit Shield | runc-exec... Verified

REMEDIATION 1 Recommended

The Distributed Exploit Shield blocks new container processes with a current working directory of "/" in the host namespace.

Reason	Remediates vulnerability CVE-2024-21626
Effect	Block and alert
Principal	/usr/local/sbin/runc
Action	sys_execve
Resource	*
Condition	when principal.version <= 1.1.11 or unknown and action.cwd = "host_ns:/"

Deployed by 8,734 other customers

Changes can be validated on your live, production environment

Network-based enforcer's dual data plane: Earning your trust

Primary Data Plane

VERSION 2.0

VERSION 2.1

Shadow Data Plane

Self qualifying software updates

Primary Data Plane

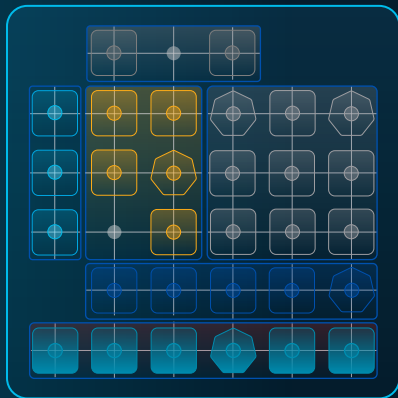
DEPLOYED POLICY

POLICY GROUP A

Shadow Data Plane

Policy verification, exploit protection test

Cisco Hypershield use cases



Autonomous Segmentation

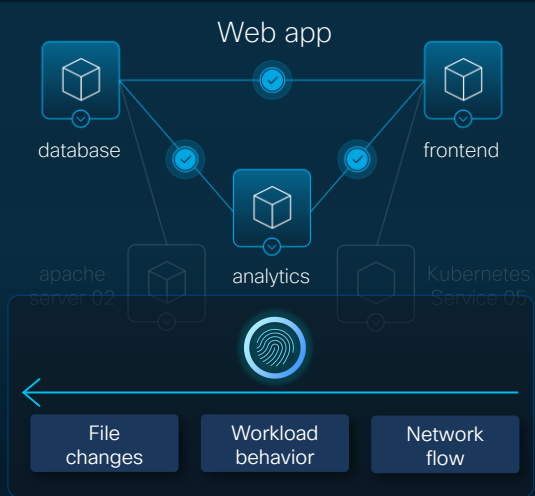
- Deep understanding of app behavior
- Comprehensive inputs for policy creation
- Constantly adapting to changing apps



Distributed Exploit Protection

- Mitigate known and unknown vulnerabilities
- Surgical mitigating controls
- Protection within minutes, while app keeps running

Segmentation that is effective and keeps up with changing applications

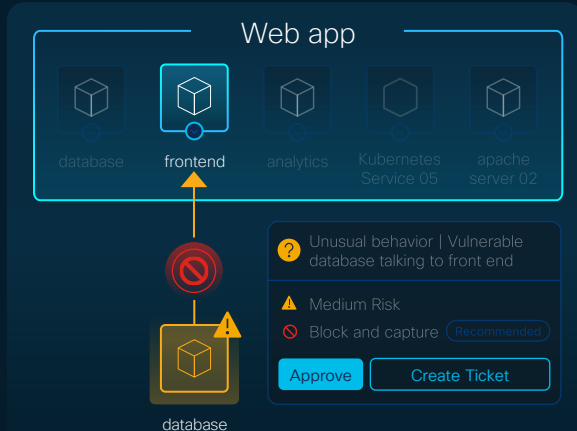


Complete understanding of changing app behavior from network to workload to pre-prod

Recommendations

- ✓ Permit web app frontend can access database ✓
- ✓ Permit web app frontend can access analytics ✓
- ✓ Permit web app analytics can access database ✓
- ✓ Default observe and permit web app policy group... ✓

Flexible segmentation rules that help avoid app fragility



Policies updated to stricter rules in response to suspicious events



Overview



Dashboard



AI Ops Insights



Inventory



Policies



Objects



Connectivity

Troubleshoot
and Logs

Security posture

Vulnerabilities

Recommendations 10

History

Q Search

All types

Recommendation

Number of actions

Security score impact

Action

Assigned to



> Remediate vulnerabilities from CVE-2024-21626

2

> Autonomous segmentation available for 1 application

2

Segmentation recommendation
for Finance app

Policy group

Policy changes

Object changes

Created by

Created on

Status

Confidence Score

Finance App group

3 added 1 edited

—

Hypershield

May 19 2024 07:21

Testing Completed

95%

Explain why this recommendation is needed

Show the effects of the recommendation

> Autonomous segmentation available for 2 zones

1

+ 16

Review

Nik



> Autonomous segmentation available for 32 workloads

1

+ 5

Review

Nik



> Autonomous segmentation available for 32 workloads

2

+ 3

Review

Nik



> Autonomous segmentation available for 5 applications

2

+ 2

Review

Nik



> Review 2 unusual behaviors

2

+ 1

Review

Nik





← Staging

Finance App group

Testing completed



Autonomous Segmentation policies were generated by Hypershield's AI and tested in your environment with live traffic.

[Explain how these policies were created](#)

Dashboard



AI Ops Insights



Inventory



Policies



Objects



Connectivity

Troubleshoot
and Logs

+ 0.02% CPU

+3 Allowed flows

-3 Denied flows

+80 policy hits

Primary dataplane

Currently deployed

Shadow dataplane

Testing completed

Testing complete

Confidence Score 95%

Tested for 3 hours starting on Jan 17, 2024 08:30 by Hypershield

[More options](#)[Retest](#)[Deploy](#)

Approval

Policy tested and verified in
shadow data plane



Dashboard



AI Ops Insights



Inventory



Policies



Objects



Connectivity

Troubleshoot
and Logs

Ask a question about the test results



Changes tested

3

policies added

1

policy edited

Policies

Objects

Operation	Policy Name	Change added by	Change added on	
> + Added	Default permit and observe finance app policy group	Hypershield	Apr 19 2024 07:21	...
> + Added	Block finance app frontend can access database	Hypershield	Apr 19 2024 07:21	...
> + Added	Block finance app frontend can access analytics	Hypershield	Apr 19 2024 07:21	...
✓ - Edited	Block finance app analytics can access database	Hypershield	Apr 19 2024 07:21	...

Policy update
recommendations

Effect	Principal	Action	Resource
Before Block and alert	Analytics	TCP	Server
Change		TCP UDP	Server → Database 2
After Block and alert	Analytics	TCP UDP	Database 2

Related enforcement points

Network Enforcement Points

3 to review

Search

Hide passed

Name	Differences to review	Confidence	Test result
Network Enforcement Point 5	3	92%	Review
Network Enforcement Point 6	1	92%	Review
Network Enforcement Point 7	1	91%	Review
Network Enforcement Point 1	0	98%	Passed
Network Enforcement Point 2	0	96%	Passed
Network Enforcement Point 3	0	95%	Passed
Network Enforcement Point 4	0	95%	Passed
Network Enforcement Point 3	0	95%	Passed
Network Enforcement Point 3	0	95%	Passed
Network Enforcement Point 3	0	95%	Passed
Network Enforcement Point 3	0	95%	Passed
Network Enforcement Point 3	0	95%	Passed

Test results

Name	Network Enforcement Point 5
Differences to review	3
Confidence	92%
Result	Review

Performance

Passed

CPU

CPU Min
3.50% Primary 3.70% 1% Shadow

CPU Average
3.50% Primary 3.70% 1% Shadow

CPU Max
3.50% Primary 3.70% 1% Shadow

Detailed test result journal for each enforcement point



Policies

Active

Drafts

History



Dashboard



AI Ops Insights



Inventory



Policies



Objects



Connectivity

Troubleshoot
and Logs

Finance App group successfully deployed and is now on the primary dataplane.

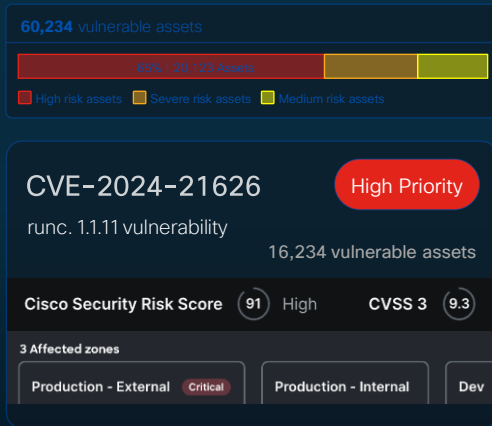
Would you like to notify Drew, Sam, and the SOC team in Webex? [Notify](#)

Search

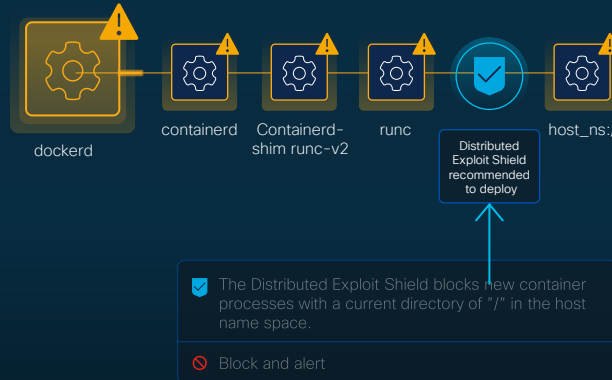
Name	Effect	Principal	Action	Resource	
Default permit and observe finance app policy group	✓ Permit	Finance ap	UTP	*	...
Block finance app frontend can access database	⊘ Block and alert	Frontend	TCP	Database	...
Block finance app frontend can access analytics	⊘ Block and alert	Frontend	UDP	Analytics	...
Block finance app analytics can access database	⊘ Block and alert	Analytics	UDP	Database2	...

Shadow data plane policy
moved into production - policy
active

Close the exploit gap against growing CVEs/CWEs with automated workflows



Complete view of the vulnerabilities, prioritised by severity and critical business flows

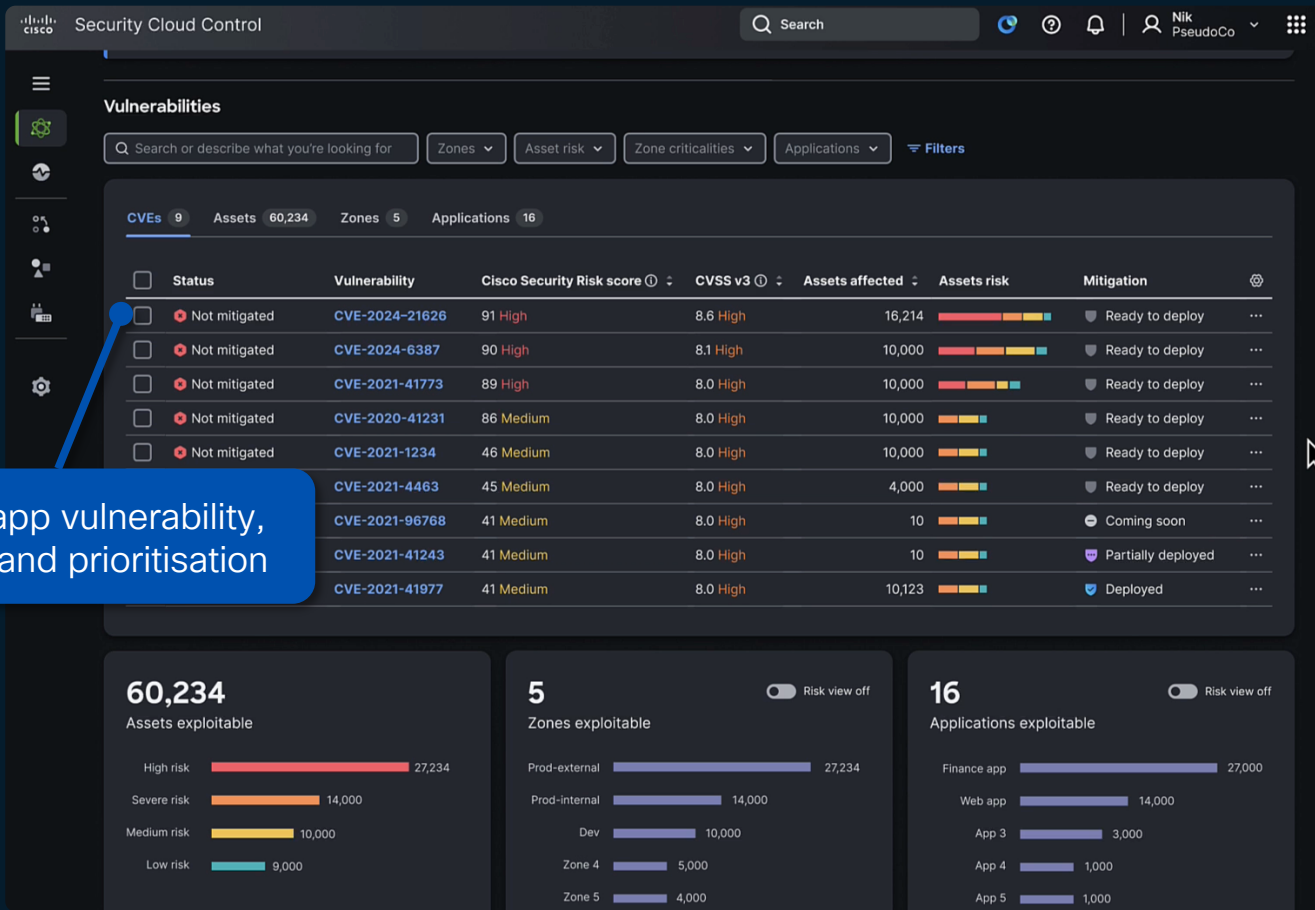


Surgical mitigating control in the path of the process that keeps application running



☒ The Distributed Exploit Shield was already tested in your environment

Tested against live production traffic to earn trust and increase confidence



Finance app vulnerability, severity, and prioritisation

Security Cloud Control

Search

Nik PseudoCo

CVE-2024-21626

Not mitigated

Description Talos Cisco Vulnerability Management

runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc 1.1.11 and earlier, due to an internal file descriptor leak, an attacker could cause a newly-spawned container process (from runc exec) to hav [See more](#)

[Summarize CVE](#)

Cisco Security Risk Score 91 High

CVSS v3 8.6 High

Mitigation

Distributed Exploit Shield Verified

The Distributed Exploit Shield mitigates vulnerability CVE-2024-21626 by blocking new container processes with a current working directory of "/" in the host namespace.

[Deploy](#)

Time Hypershield created	Confidence Score	Effectiveness Score	Assets shielded	Created on	Updated on
1 hour from known exploit	95%	100%	16,234	Jul 8 2024 08:34	—

Effect Forbid and alert

Principal `/usr/local/sbin/runc`

Action `sys_execve`

Resource *

Condition `principal.version <= 1.1.11 or unknown` and `action.cwd = "host_ns:/"`

[Explain mitigation](#)

Exploitable path

☐ View recommended Distributed Exploit Shield in path

```
graph LR; A[containerd] --> B[containerd-shim]; B --> C[runc]; C --> D[host_ns:/]; D --> E[host_ns:/];
```

CVE info

Compensating control recommendation

Exploit in execution path

Security Cloud Control Search

Distributed Exploit Shields will automatically be removed when they are no longer needed to shield the assets.

The Distributed Exploit Shield mitigates vulnerability **CVE-2024-21626** by blocking new container processes with a current working directory of `"/"` in the host namespace.

Time Hypershield created	Confidence Score	Assets shielded	Created on	Updated on
1 hour from known exploit	95%	16,234	Jul 8 2024 08:34	—

Deployed on	Deployed by
Jul 8 2024 09:34	Nik

Effect: **Forbid and alert**

Principal: `/usr/local/sbin/runc`

Action: `sys_execve`

Resource: `*`

Condition: `principal.version <= 1.111 or unknown` and `action.cwd = "host_ns:/"`

[Explain mitigation](#)

Exploitable path

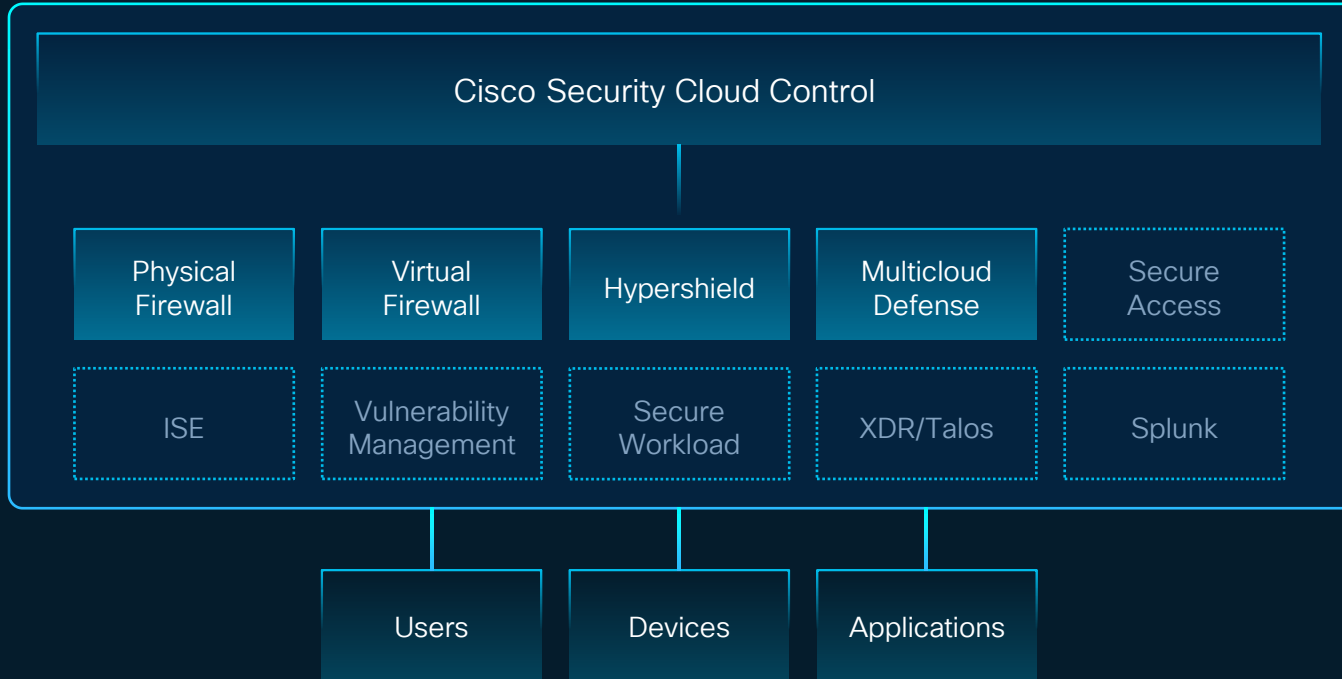
```
graph LR; dockerd[dockerd] --> containerd[containerd]; containerd --> shim[containerd-shim-runc-v2]; shim --> runc[runc]; runc --> host_ns[host_ns/];
```

Legend +

[View test results](#)

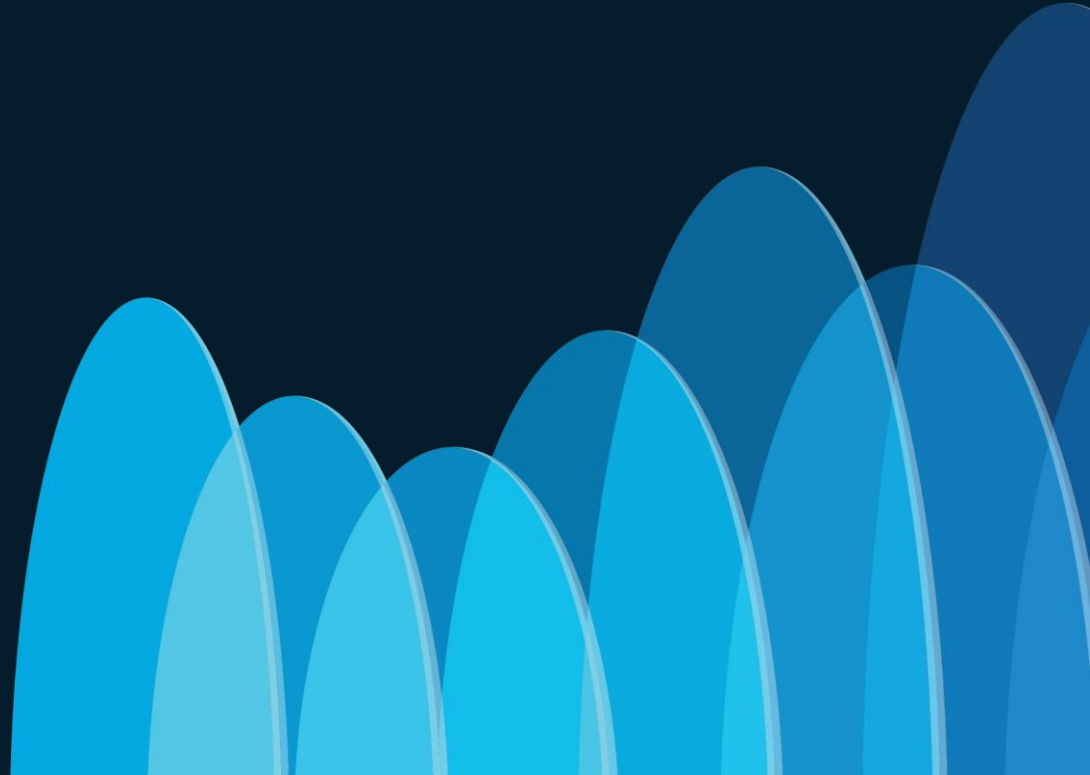
Threat (not workload) isolated

Security Cloud Control unifies security management



- Unified coordination of security solutions
- Consistent policy enforcement and object sharing
- Support for hybrid environments including on-premises

Application Detection & Response



Business Risk Observability

Security through Full-Stack Observability

Provide business context needed to rapidly assess risk and align teams based on potential impact

Business Context Mapping

Mapping vulnerabilities and attacks to common transactions provides the business context to help you quickly understand the location and impact of threats.

+

Vulnerability and Threat Intelligence

Threat intelligence feeds from multiple yet complementary sources provide the threat context to understand the likelihood of exploits.

=

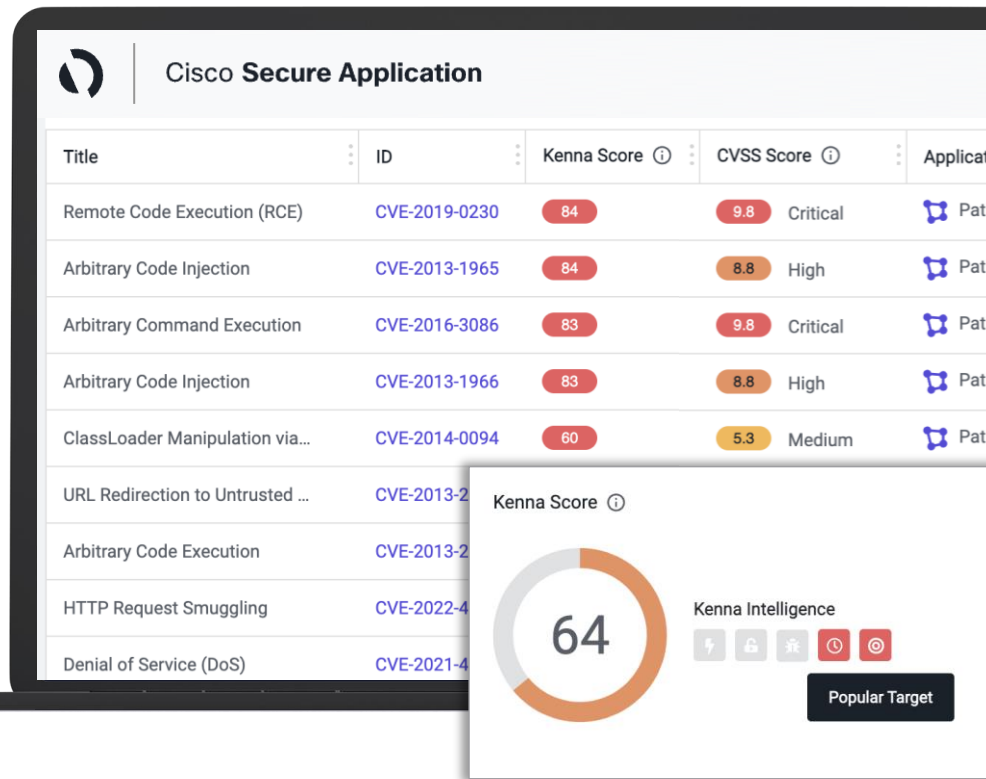
Business Risk Score & Remediation Guidance

Scoring composited from analysis of runtime behavior + business impact + intelligence provides complete business risk context to instantly assess and prioritise action across ITOps and Security teams.

Determine likelihood of exploit with Cisco Vulnerability Management (Kenna)

Use data science to identify real vulnerability risk

- Machine learning leveraging real-time and historical data to predict exploitation
- Leverage a better remediation methodology compared to CVSS
- Native backend integration maps Kenna scores to discovered vulns
- Combine findings into vuln and threat context for business risk scores



Cisco Secure Application via AppDynamics Agent

Security insights provided with Application and Business context

Business Risk Observability

Detect
Vulnerabilities in
Libraries



Common Vulnerabilities
and Exceptions with Code
Level correlation

Detect
Attacks via
Stack Traces



Spot CVE correlated
runtime exploits and Zero
Day attacks (like Log4j)

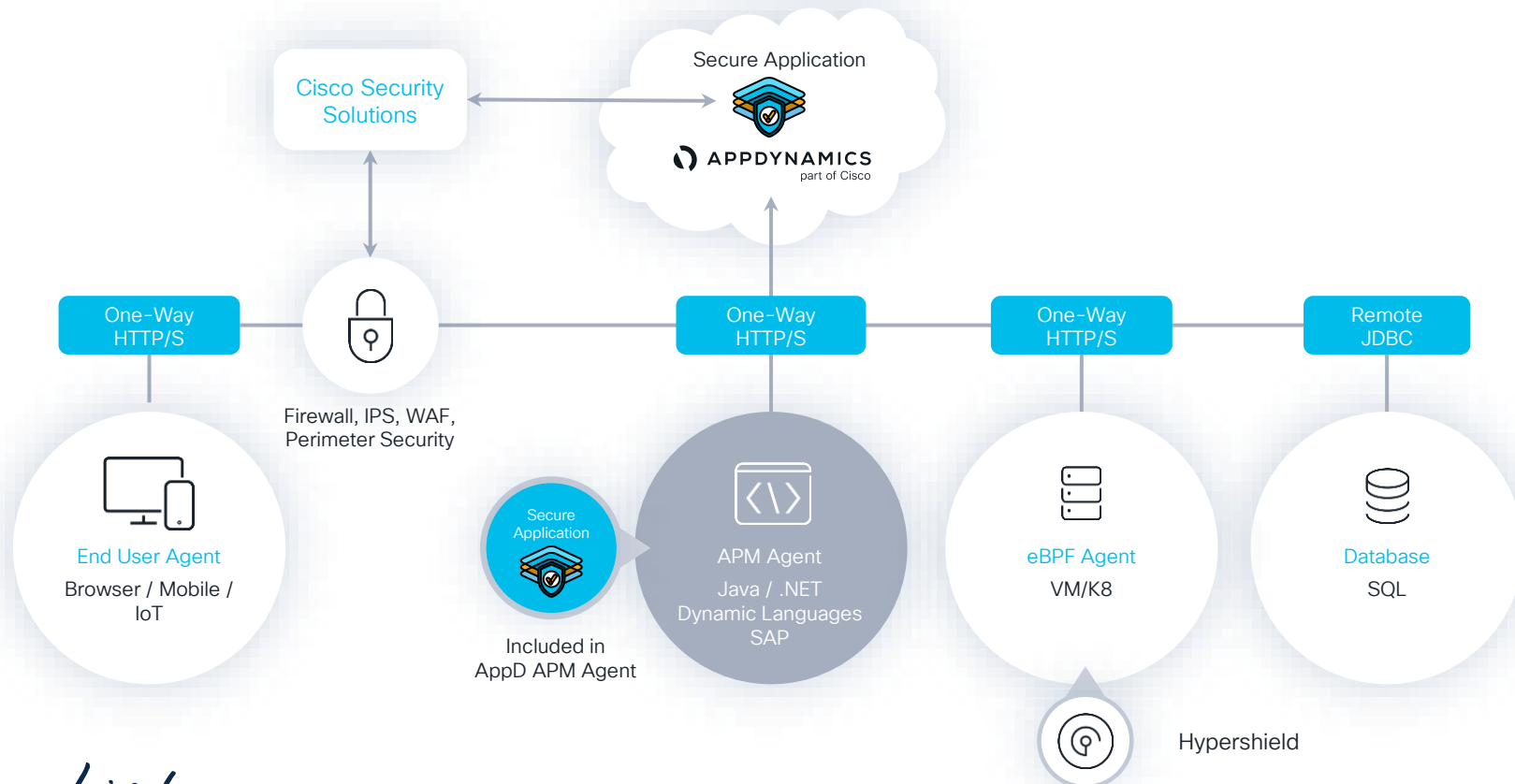
Block Attacks
via Byte Code
Instrumentation



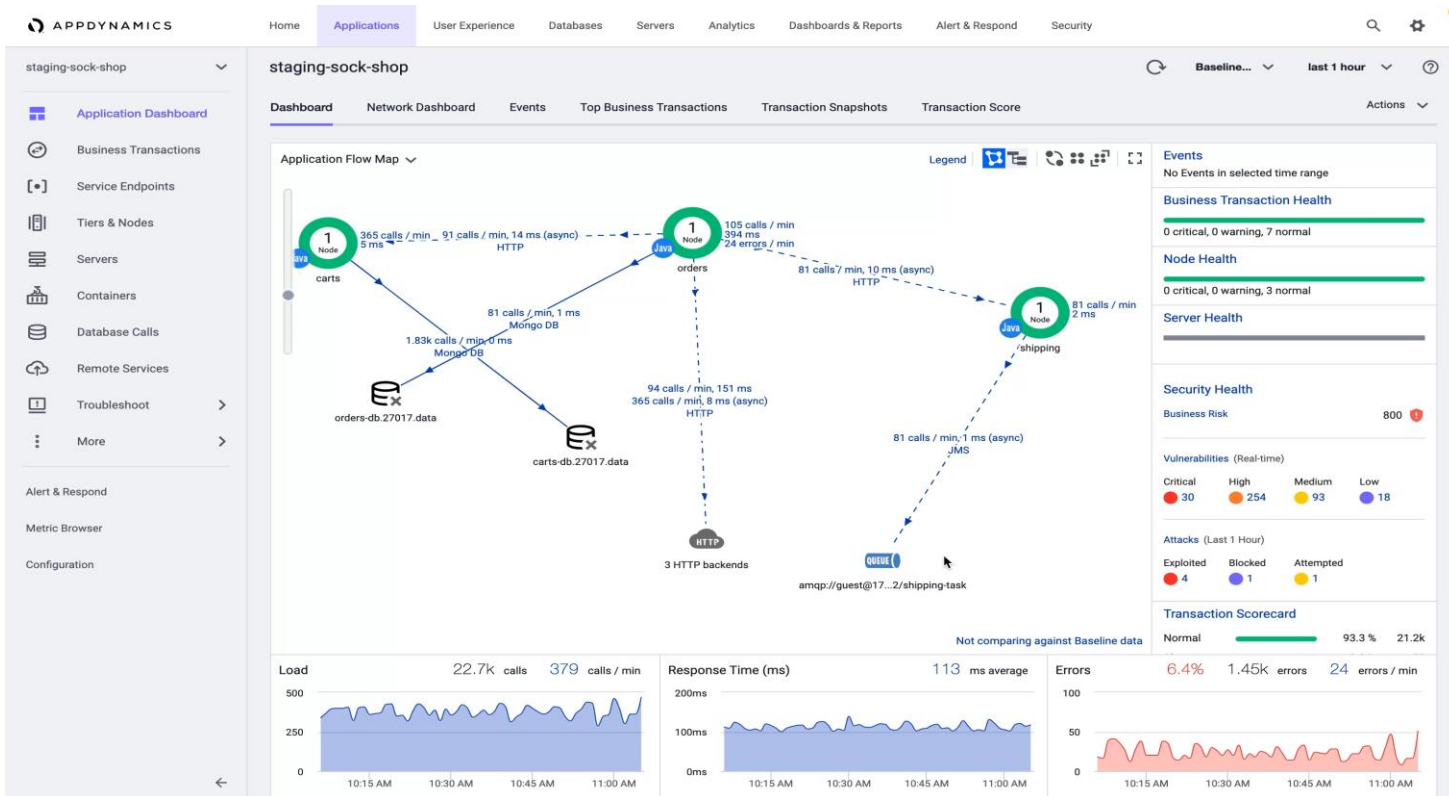
Policy level blocking that
stops bad actors... even if
vulnerabilities exist

Application Detection & Response

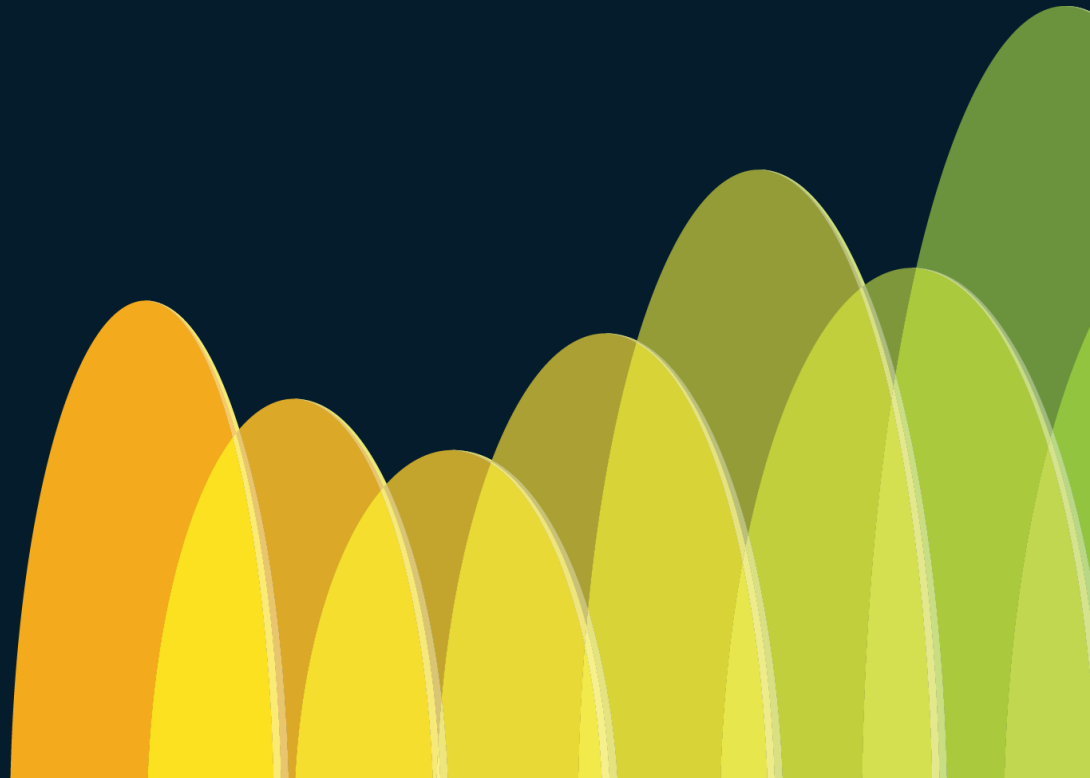
AppDynamics Agent Architecture



Cisco Secure Application Demo



Summary



Cloud Native Apps introduce more security **Complexity** but more **Opportunity** as well!



Traditional security tools don't meet the needs for cloud native app development



Kubernetes is not secure by default; massive proliferation of one-function tools



SecOps has to keep up with the speed of app development and have an integrated workflow

Bringing Worlds Together



Entry Point	 <p>Start from the left by integrating into dev toolchain</p>	 <p>Start from the right with runtime protection</p>
Stakeholders	CIO and the DevOps team	CISO and the security teams
Cisco Offerings	Vulnerability Management (Kenna), Cisco Secure Application for AppDynamics, Panoptica, Secure Workload, Multicloud Defense, Hypershield	

Sleep Peacefully



And not
worry about
hackers
taking a bite
out of your
data

Transitioning Securely to Cloud Native with Cisco

CSPM
CNAPP
CIEM
CWPP
KSPM
DSPM

- External Attack Surface
- Cloud Security Posture
- Segmentation
- Containers and K8s
- Vulnerability Management
- API security
- Serverless
- IAC and CI/CD pipeline
- Data Exposure
- CDR and Attack Path Analysis

Cisco
Vulnerability
Management
(Kenna)



Cloud Native
Application
Observability
(AppD)



Cisco Secure
Workload



Cisco
Hypershield



Cisco Cloud
Application
Security
(Panoptica)



Cisco
Multicloud
Defense



Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Lets bring joy to my family and make Australia proud



Related Sessions

- eBPF and Cilium – the foundations of modern application networking and security [BRKSEC-2169]
- How to build a secure modern Hybrid cloud Environment [BRKSEC-2444]
- Intelligent Security for the Hybrid Cloud and Multi-cloud [BRKSEC-2581]
- Cisco Hypershield: a New Era of AI-Native Security for Data Centers and Cloud – [BRKSEC-1501]
- Simplify Security Management – Unified cloud-based security management platform [BRKSEC-2112]

Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert 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



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC

Appendix: Capabilities Detail

Multicloud Defense



"This is way faster. Minutes versus what would take us 20 days with our current CheckPoint virtual appliances."

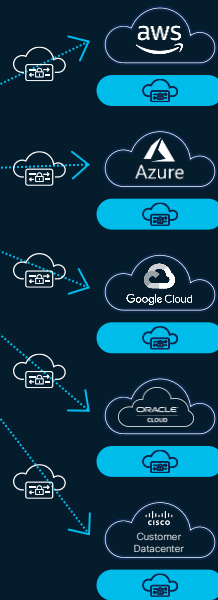
Global Cloud Architect
Global Food and Beverage Manufacturer



Controller

- Visibility into cloud assets
- Multidirectional protection
- Create, enforce, and manage policies
- Network routing and connectivity
- Automation and orchestration

One interface to manage and deploy policies across all clouds



Accelerate operations and reduce learning curves with one consistent experience

Dynamic policy

Firewall and IDS/IPS	Web Application Firewall
Data Loss Prevention	URL Filtering
FQDN Filtering	Antivirus

Gateway

- Stop inbound threats (ingress)
- Block data exfiltration (egress)
- Protect clouds and VPCs from lateral movement (east-west)

Automation and orchestration reduces manual processes and misconfigurations

Cisco Vulnerability Management



Remediation teams are able to focus their efforts on the most impactful actions that can significantly reduce risk, versus running on the vulnerability treadmill and not making any real progress."

Rohit Kohli,
Assistant Vice President,
Information Security
Genpact

Enterprise Data

From every available source across an organization's:

- Infrastructure
- Applications
- Internet of Things (IoT)

Global Threat Intel

- 19+ exploit and threat intel feeds
- 15+ billion security events
- 12.7+ billion managed vulnerabilities



Data-driven vulnerability prioritization

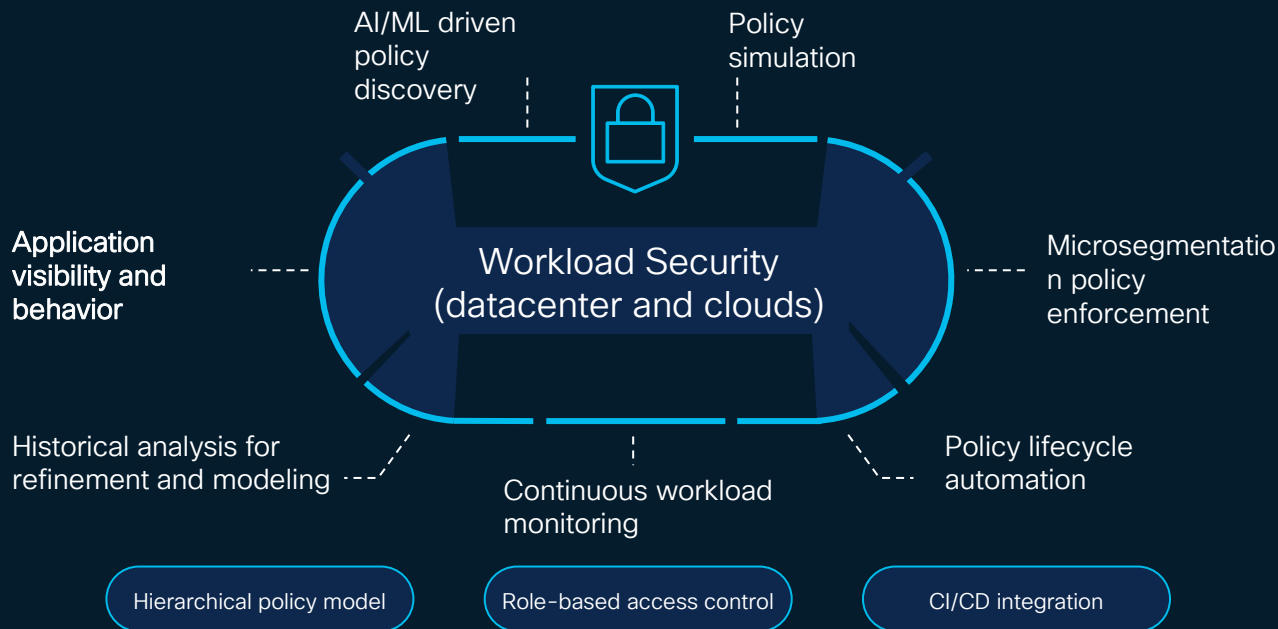
Powered by data science, machine learning, and patented predictive modeling

Reduce risk effectively by prioritizing the vulnerabilities that matter most

Accelerate remediation efforts through security & IT alignment

Centralize your vulnerability data in one location for a holistic view of risk across your environment

Cisco Secure Workload



Stop lateral movement

Zero trust microsegmentation protects application workloads across the data center and clouds from one solution

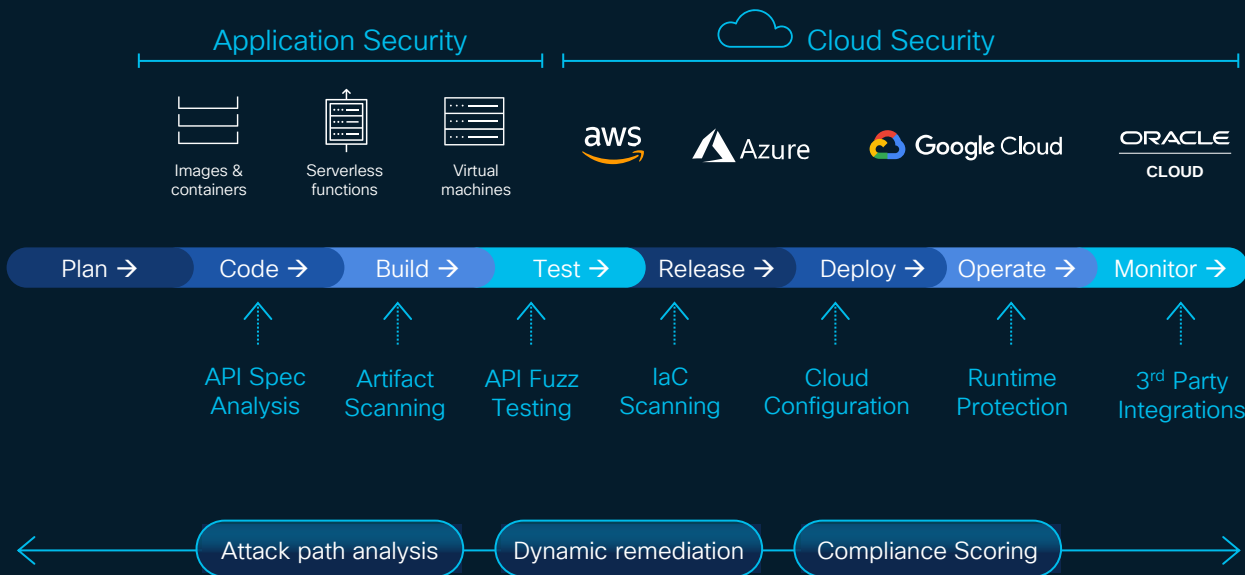
Quickly improve security posture

Understand application behavior and enact best-practice hardening policies such as blocking insecure app to app communications

AI/ML tackles tasks that are beyond human scale

Powerful AI/ML driven policy discovery recommends policies tailored to the unique environment and automation ensures consistency and accuracy

Cisco Cloud Application Security



Increased visibility & risk mitigation across cloud native applications from dev to runtime

Discover and protect all your cloud assets

Prioritize your risk remediations with precision using graph-based attack path analysis

Secure your API communications

Compliance scorecards for quick benchmarking to known standards for cloud, Kubernetes, containers

Cisco Attack Surface Management



We had a misconfiguration incident. One system was missing MFA enforcement for the users. The vendor responsible for the SaaS app credited \$9 million back to us after we demonstrated that it was fraud. If we had visibility on the users and their configuration on that system, we could have been aware of the risk or maybe prevented it.

Information Security Manager in the fintech industry

