

The background features a vibrant, abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, cyan, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

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 *Live!*

#CiscoLiveAPJC

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
 - 21 years in security industry, 18 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



Cisco Webex App

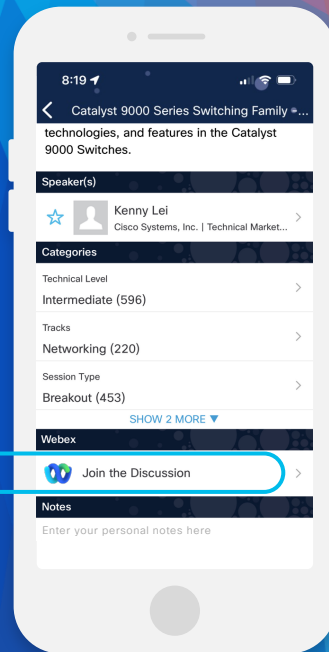
Questions?

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 December 22, 2023.

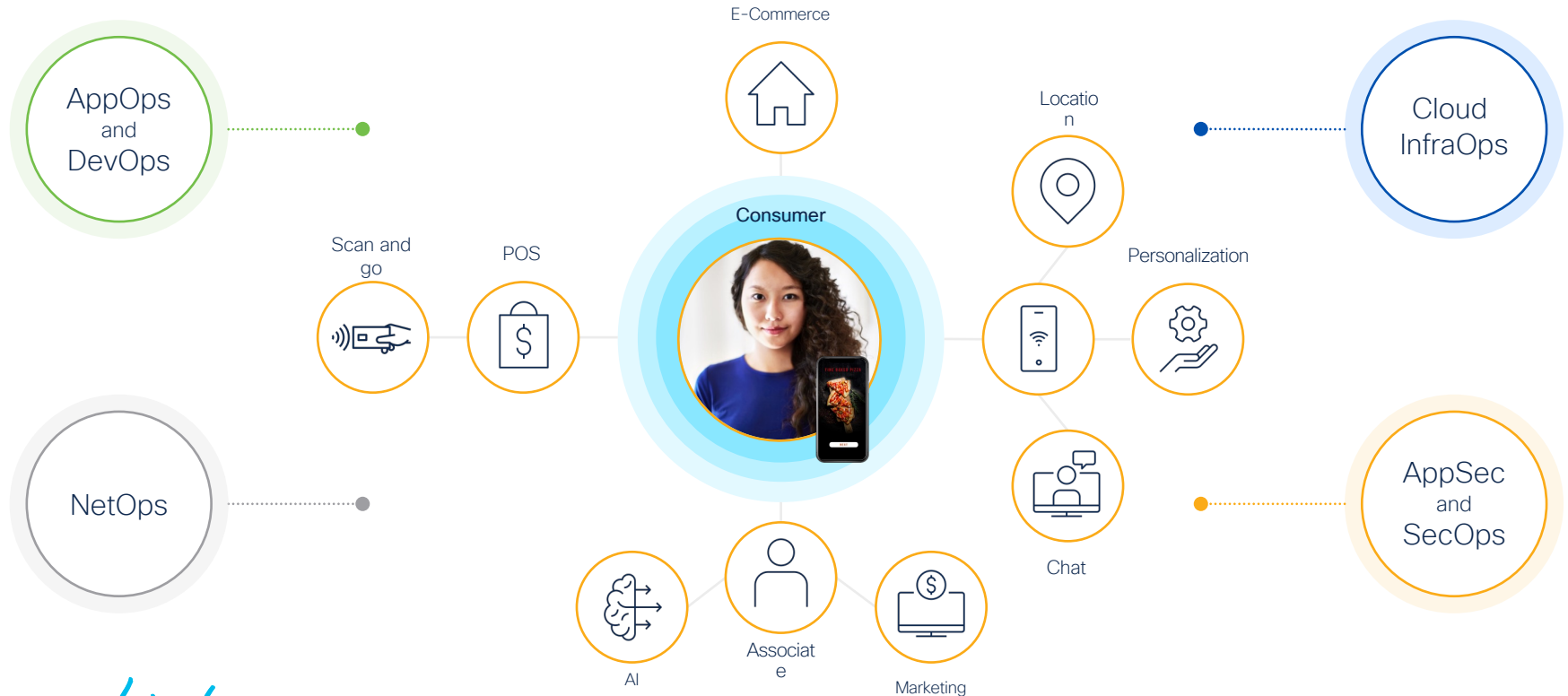


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1139>

Agenda

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

Navigating the new world order isn't easy



Infrastructure
is changing

Welcome to the Multi-Cloud Era

Numbers to remember

94% are still wasting money in the cloud

56%

Boosted cloud spending in the last year, despite macroeconomic uncertainty

92%

*Of highly cloud mature organizations say **multi-cloud** is working, or is expected to within a year*

53%

*Of high-maturity organizations are using **multi-cloud** to save money*

#1

*Rank of **security** as a multi-cloud success factor*

#1

*Rank of **skills shortages** as a multi-cloud barrier*

74%

Of high-maturity companies say multi-cloud helps them attract, motivate, and retain talent

92%

*Of organizations are adopting, standardizing, or scaling **platform teams***

Applications are changing

Applications are critical to modern businesses

Applications are the New Lifeline of Modern Businesses



500M

Apps will be developed over the next three years¹

More Applications are Being Born in the Cloud

30%

of custom enterprise applications will run in a container environment by 2024 (up from <10% in 2020)²

90%

of new apps will be developed as cloud-native applications by 2025³

Security challenges for cloud-native applications



Blurring boundaries between Dev and Security teams



DevSecOps must **manually stitch 10+** disparate tools

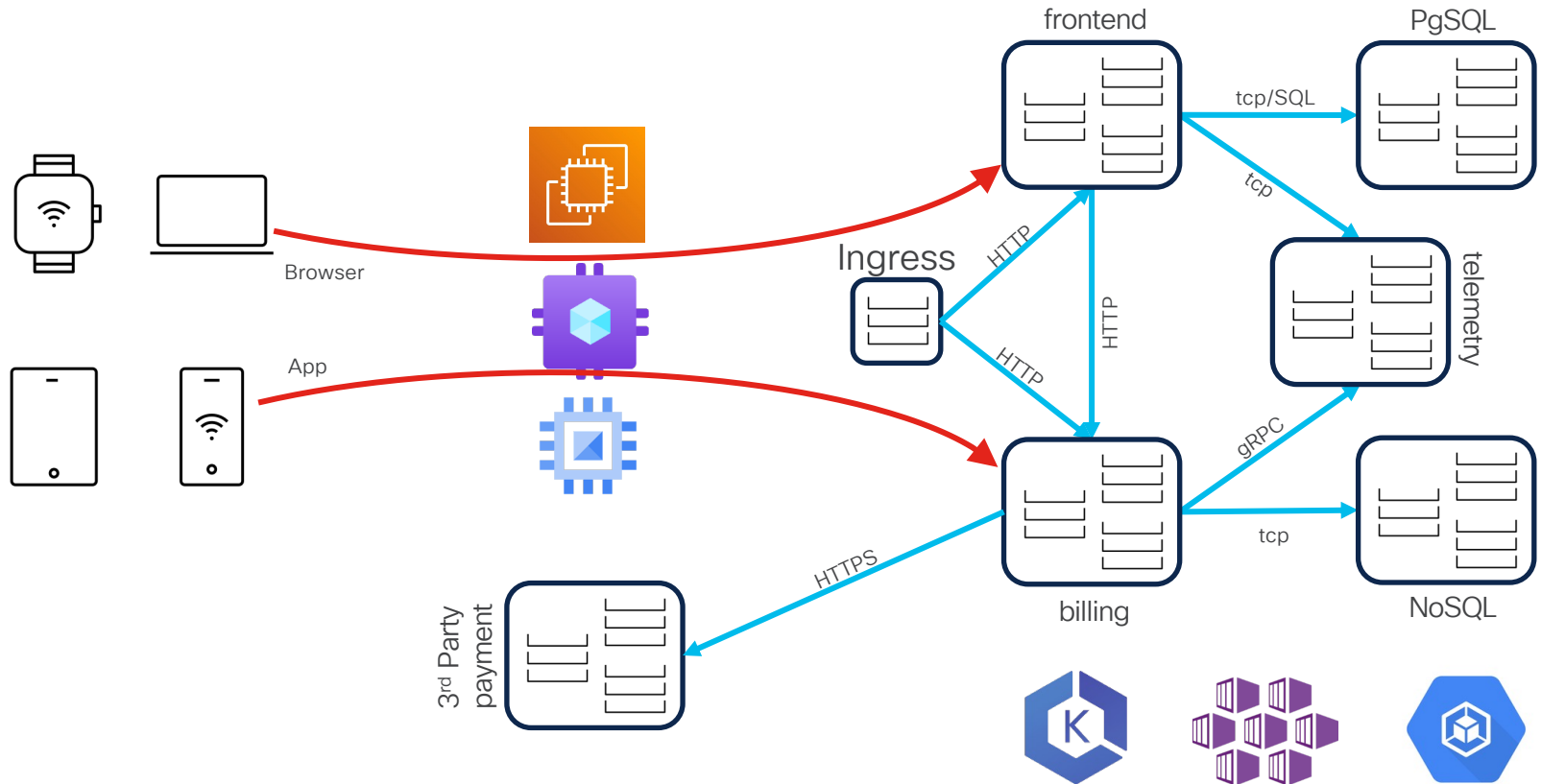


Increased threats & increased Reg & Compliance requirements



Legacy tools are **not enough to secure** cloud native apps

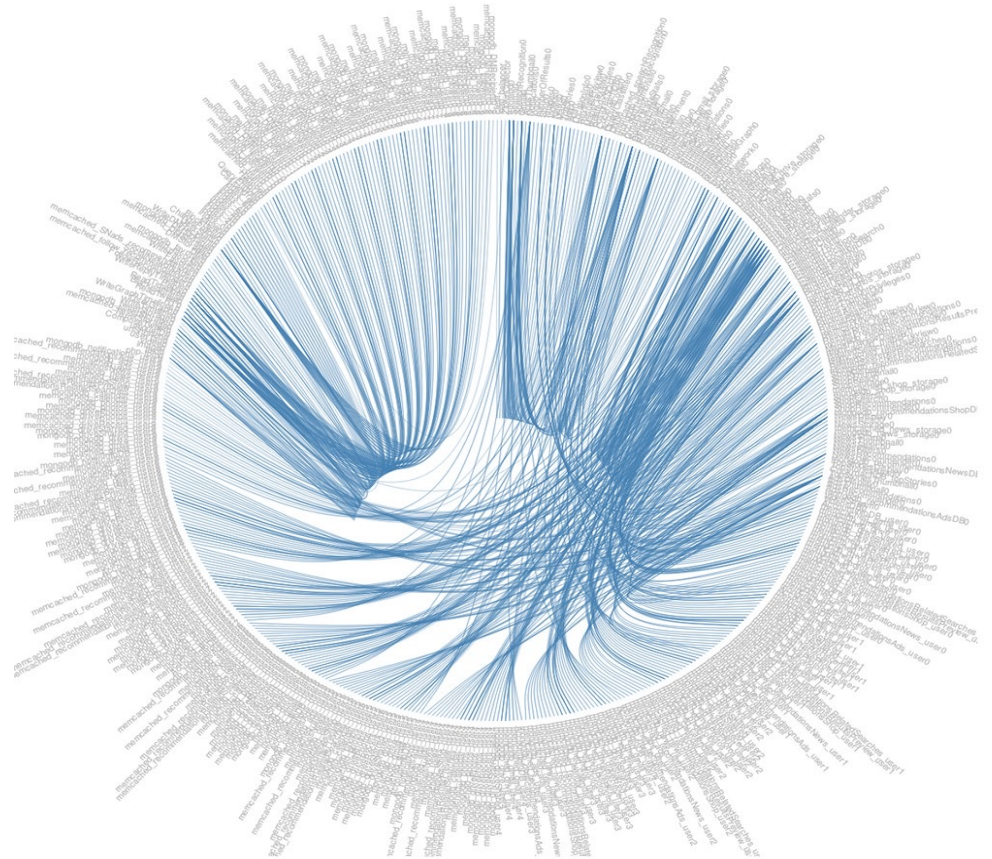
Simple Modern Application



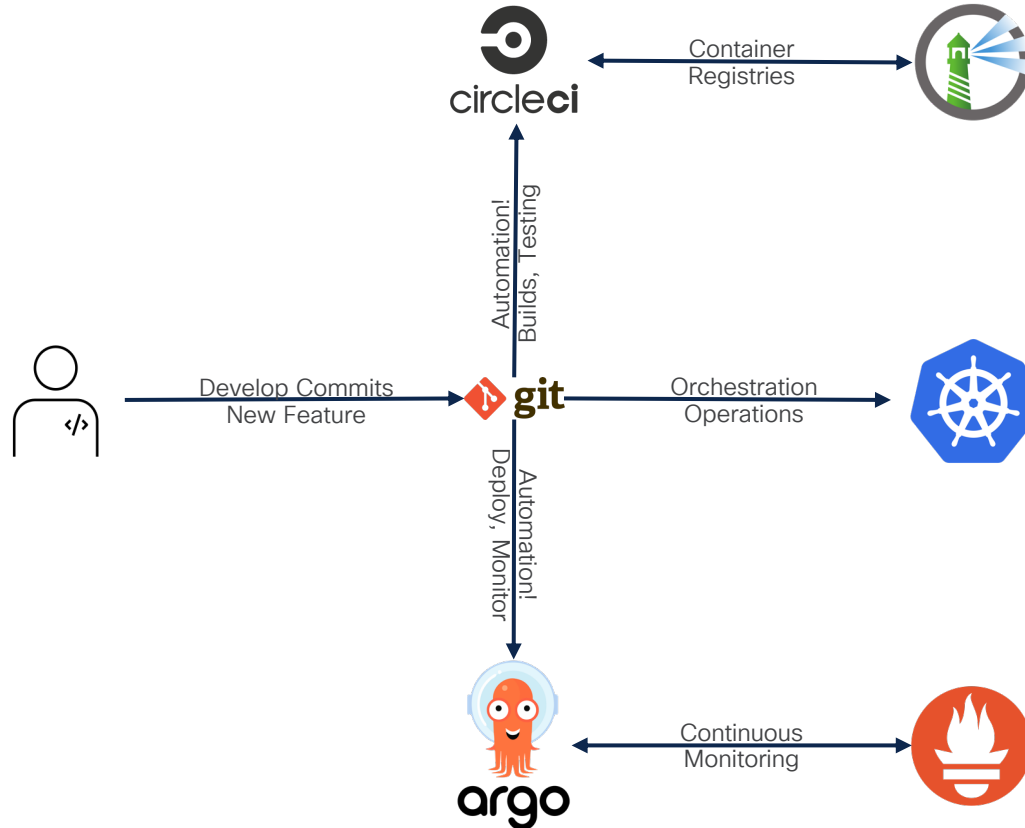
The reality

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

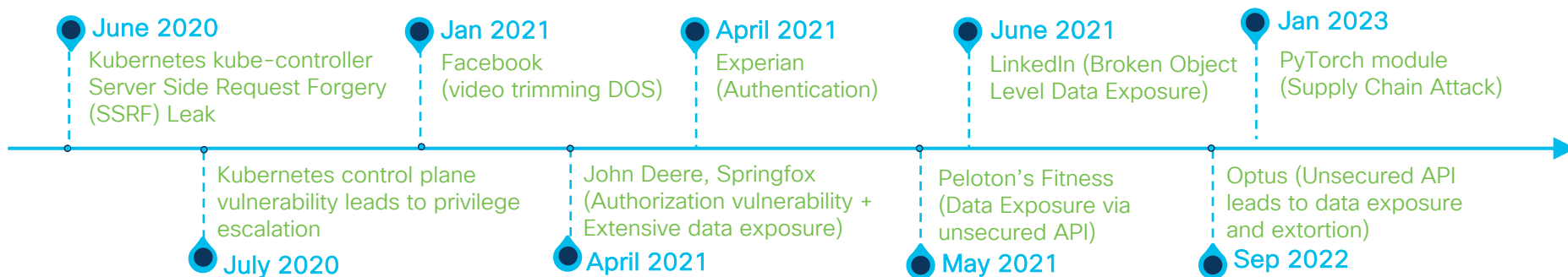
- Decoupled
- Dynamic
- Scalable



Application development workflows have evolved



Recent exploits of new attack surfaces



Explosion of threat vectors in microservices security

API attacks will become the most-frequent attack vector, causing data breaches for enterprise web applications.

- Gartner, 2022

93%

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

Reference Redhat 2022 <https://www.redhat.com/en/blog/state-kubernetes-security-2022-1>

\$4.35 million

Average cost of a data breach in 2022

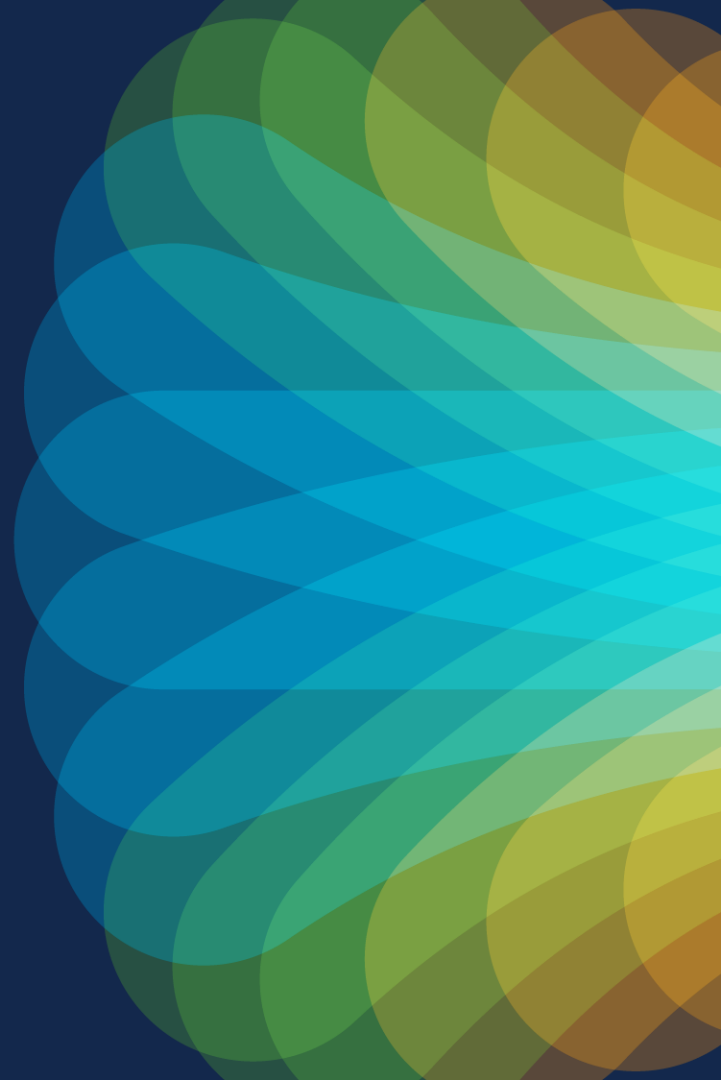
Reference IBM 2022 <https://www.ibm.com/downloads/cas/3R8N1DZ1>

286% API attack increase

Every quarter

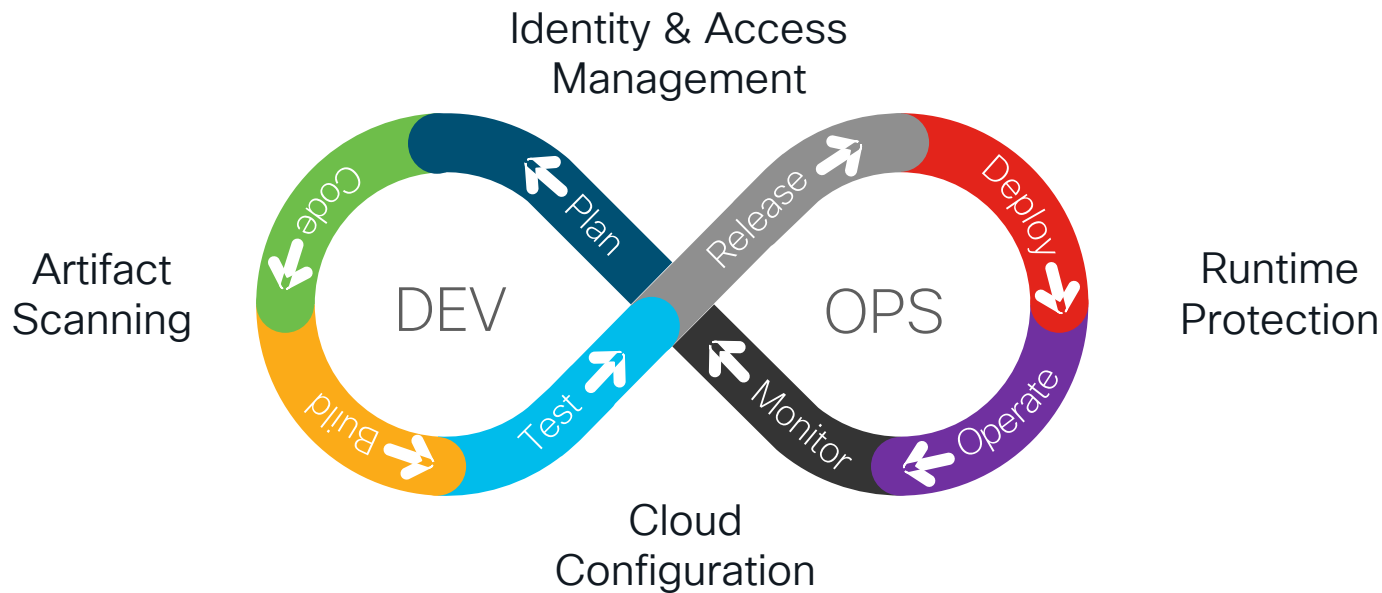
Reference Forbes 2022 <https://www.forbes.com/sites/forbestechcouncil/2022/07/25/how-to-address-growing-api-security-vulnerabilities-in-2022/?sh=33a064495a9e>

So where does
that leave
security teams?





Protecting Apps from Development to Runtime



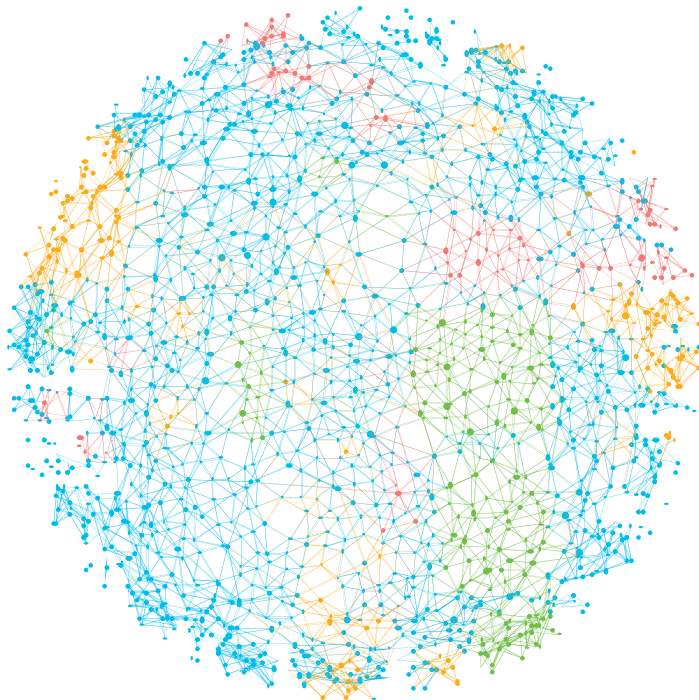
Example: Cloud Native Application Security Challenges

Securing Containers, K8s & APIs

K8s, Container images & runtimes

Key Questions:

- Are my images **immutable** throughout the application lifecycle (i.e., no drift?)
- Do I have proper **RBAC** and **pod security** measures in place?
- Do I have **visibility** of all my images and how they interact with other services?



Cloud Native applications rely extensively on internal and external APIs

Key Questions:

- Are **my** APIs vulnerable?
- Do I **depend** on vulnerable APIs?
- Do I have **indirect dependencies** on vulnerable APIs?
- Can an attacker get to my **data**?

Cloud Native security must be **automated** within existing processes

An example set of capabilities

Cloud Detection & Response



Application runtime



- Application code security testing
- Application runtime governance and protections



Containerization technologies



Istio



- Protecting containerization technologies and environments
- Risk and compliance

Workload & Cloud infrastructure



- Dynamic, context aware micro and macro segmentation and access control for zero trust
- Threat prevention for public clouds

Cisco Capability Mapping

Cisco XDR



Application runtime



- Cisco Secure App with AppD
- Cisco Panoptica



Istio



Containerization technologies

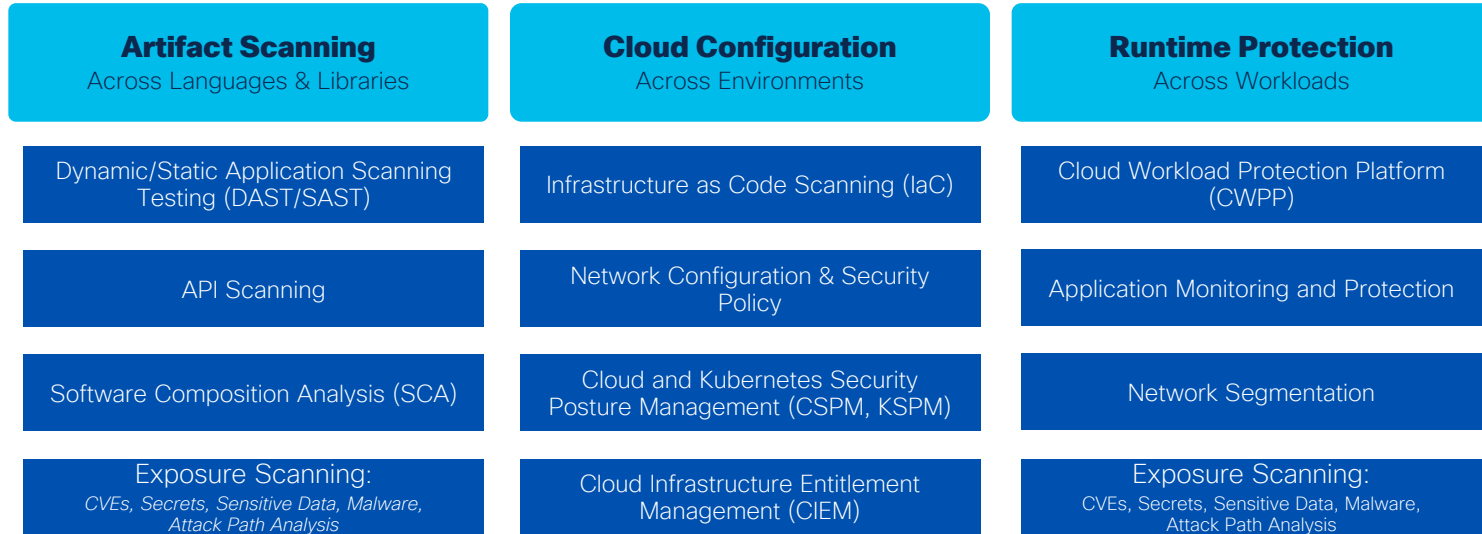
- Cisco Panoptica
- Cisco Secure Workload
- Cisco Full Stack Observability

Workload & Cloud infrastructure



- Cisco Panoptica
- Cisco Secure Workload
- Cisco Secure Firewall
- Cisco Multi-Cloud Defense

Gartner's View of Cloud and Application Security



Missing Pieces to the Puzzle

Full-Stack Observability with Business Context

Artifact Scanning

Across Languages & Libraries

Dynamic/Static Application Scanning
Testing (DAST/SAST)

API Scanning

Software Composition Analysis (SCA)

Exposure Scanning:

*CVEs, Secrets, Sensitive Data, Malware,
Attack Path Analysis*

Cloud Configuration

Across Environments

Infrastructure as Code Scanning (IaC)

Network Configuration & Security
Policy

Cloud and Kubernetes Security
Posture Management (CSPM, KSPM)

Cloud Infrastructure Entitlement
Management (CIEM)

Runtime Protection

Across Workloads

Cloud Workload Protection Platform
(CWPP)

Application Monitoring and Protection

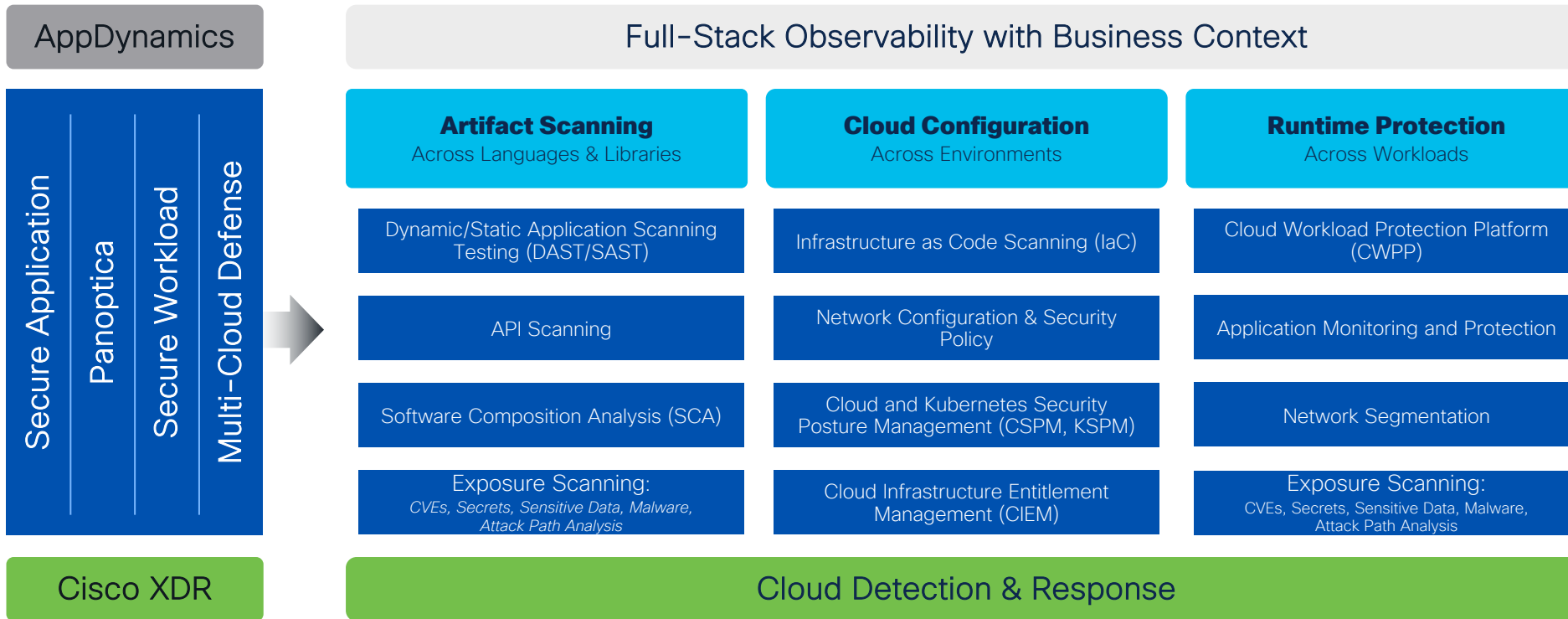
Network Segmentation

Exposure Scanning:

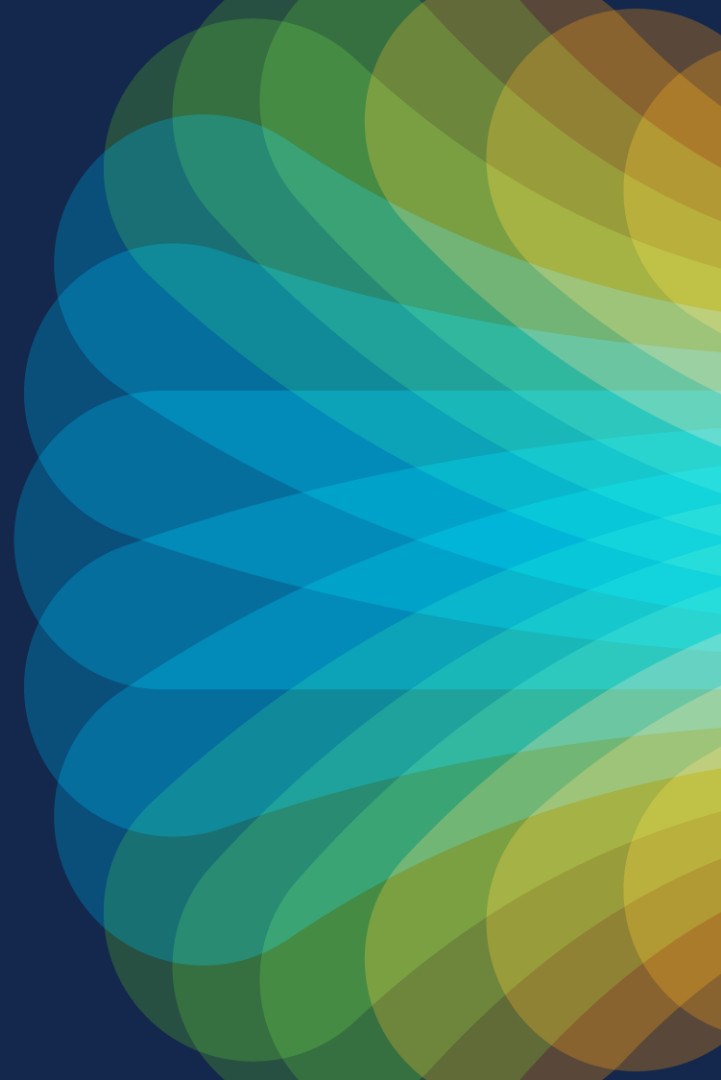
*CVEs, Secrets, Sensitive Data, Malware,
Attack Path Analysis*

Cloud Detection & Response

Cisco's Cloud and Application Security Focus



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

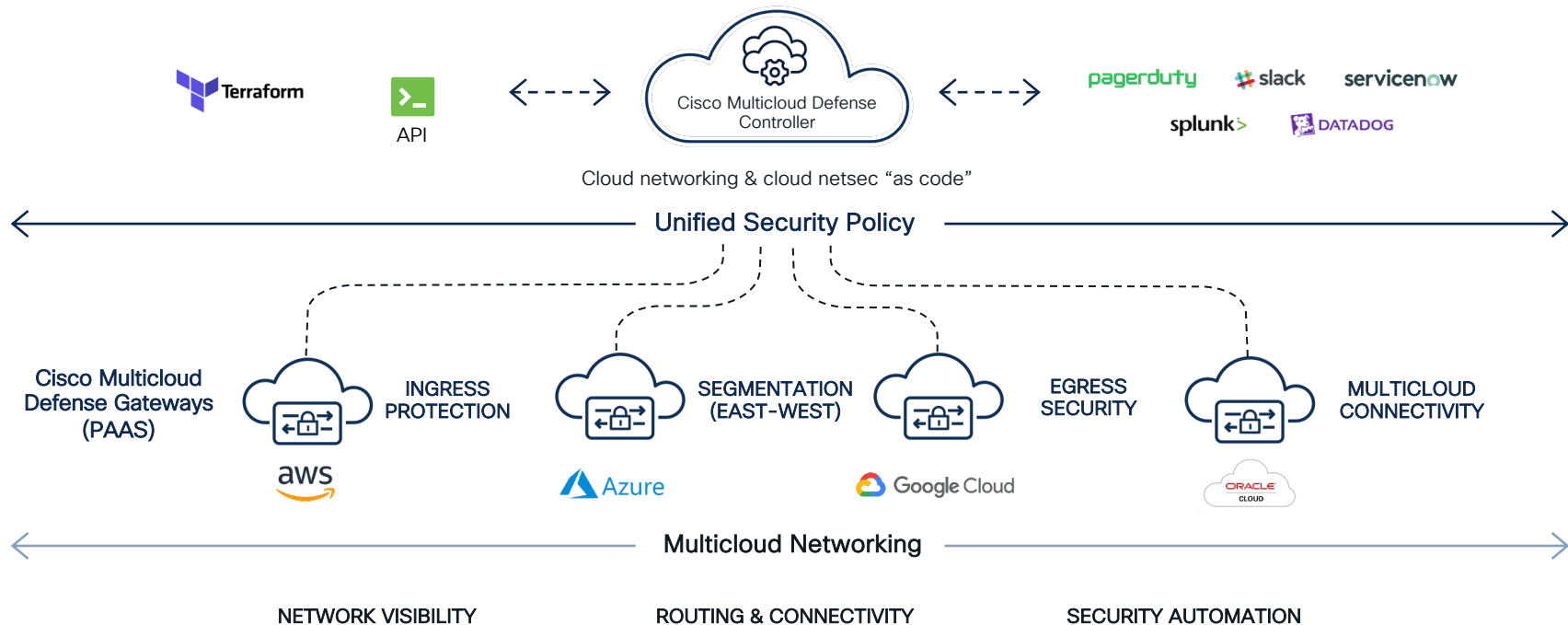


Threats

Addressing the Basics for Public Cloud Transition

Cisco Multicloud Defense

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



Multicloud Defense Gateways



Ingress Gateway

- ✓ Reverse Proxy
- ✓ TLS decrypt
- ✓ WAF – L7 DoS
- ✓ IDS / IPS
- ✓ Antivirus
- ✓ Geo IP
- ✓ Malicious IP



Egress Gateway

Egress

- ✓ URL filtering
- ✓ Forward proxy
- ✓ TLS decrypt
- ✓ FQDN filtering*
- ✓ FQDN-based firewall policy
- ✓ DLP
- ✓ IDS / IPS
- ✓ Antivirus

East/West

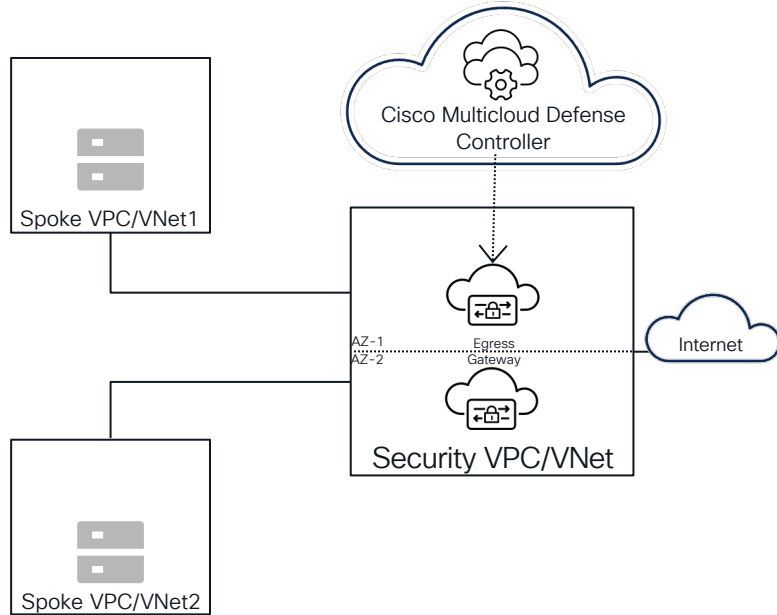
- ✓ FQDN filtering
- ✓ IPS / IDS
- ✓ Antivirus
- ✓ Micro-segmentation
- ✓ FQDN-based firewall policy
- ✓ TLS decrypt

* No TLS decryption is needed

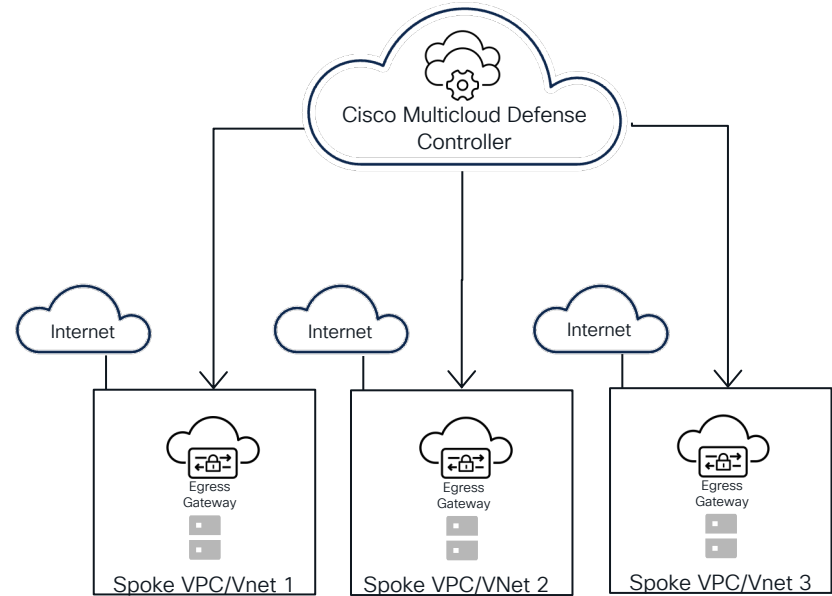
Forwarding mode is available on Multicloud Defense Gateway

Deployment Models

Centralized 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	<ul style="list-style-type: none">• Supply Chain Vulnerabilities• Library Exploits (Log4Shell)• Compliance	<ul style="list-style-type: none">• Zero Days• C2, Ransomware• Compliance	<ul style="list-style-type: none">• Zero Trust / Least Privilege• Data Protection• Compliance
Security Controls	<ul style="list-style-type: none">✓ WAF✓ IDS / IPS✓ Geo IP✓ Malicious IP✓ Antivirus	<ul style="list-style-type: none">✓ FQDN Filtering✓ URL Filtering✓ DLP✓ IPS / IDS✓ Antivirus	<ul style="list-style-type: none">✓ Cloud-native Identity✓ IPS / IDS✓ Antivirus

Hide Menu

Dashboard

Multicloud Defense New

Inventory

Configuration

Policies >

Objects

VPN >

Events & Monitoring

Analytics >

Change Log

Jobs

Tools & Services >

Settings >

Welcome to Cisco Defense Orchestrator

Quick Actions

Multicloud Defense

Get started

Connect a cloud account

Gain visibility and control of what's happening in your cloud environments while ensuring they are managed securely.

[Learn more](#)



Connect Cloud Accounts

Connect a cloud account with the Multi-Cloud Controller



Enable Traffic Visibility

Enable traffic visibility on specific VPCs to allow for more insight into the traffic in and out of your account



Secure Account

Setup a Service VPC and Multi-Cloud gateway to secure your account

Inventory & Objects

+ Onboard

Connectivity States



Configuration States

1 Synced



0 Not Synced



0 Conflict Detected



Object Issues

Object status	Number of objects
All Objects	3
Inconsistent	0
Duplicate	0
Unused	0

No Active Jobs



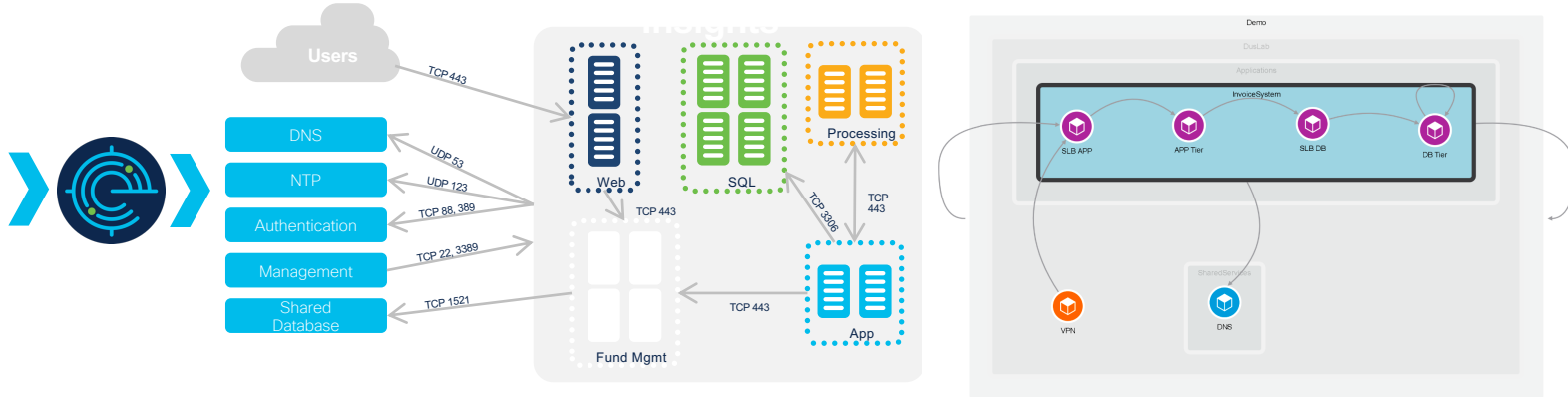
Show desktop

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 Policies 13 Catch All DENY Grouped Ungrouped

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

The Policy Puzzle

Arriving at layers of policy

Host Operating System



Kubernetes Nodes



Virtual Desktops



Cloud Security Groups



Load Balancers/
Ingress Controllers



Firewalls



Policy Domains

Multiple **teams** and organizations

Multiple **environments** and clouds

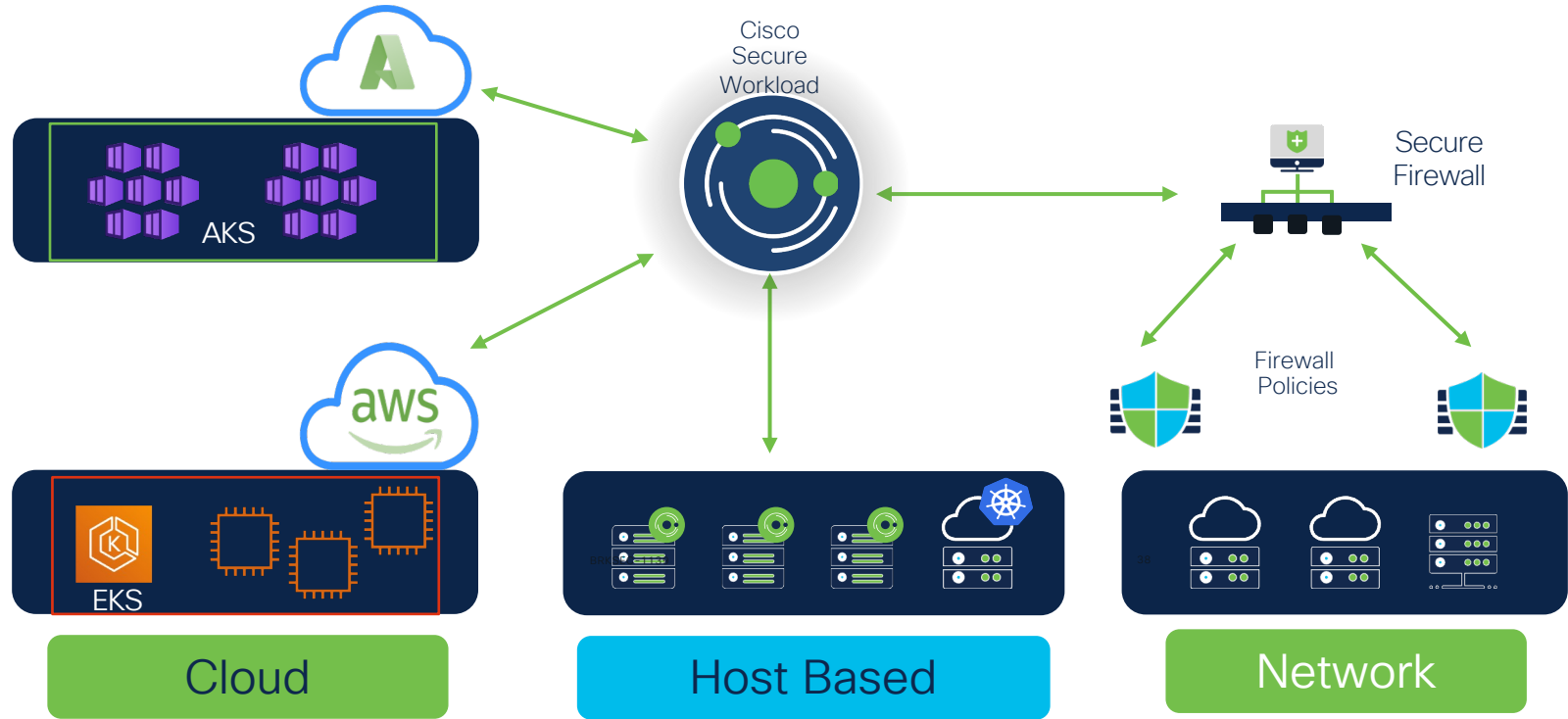
Each have **segmentation** methods and tools



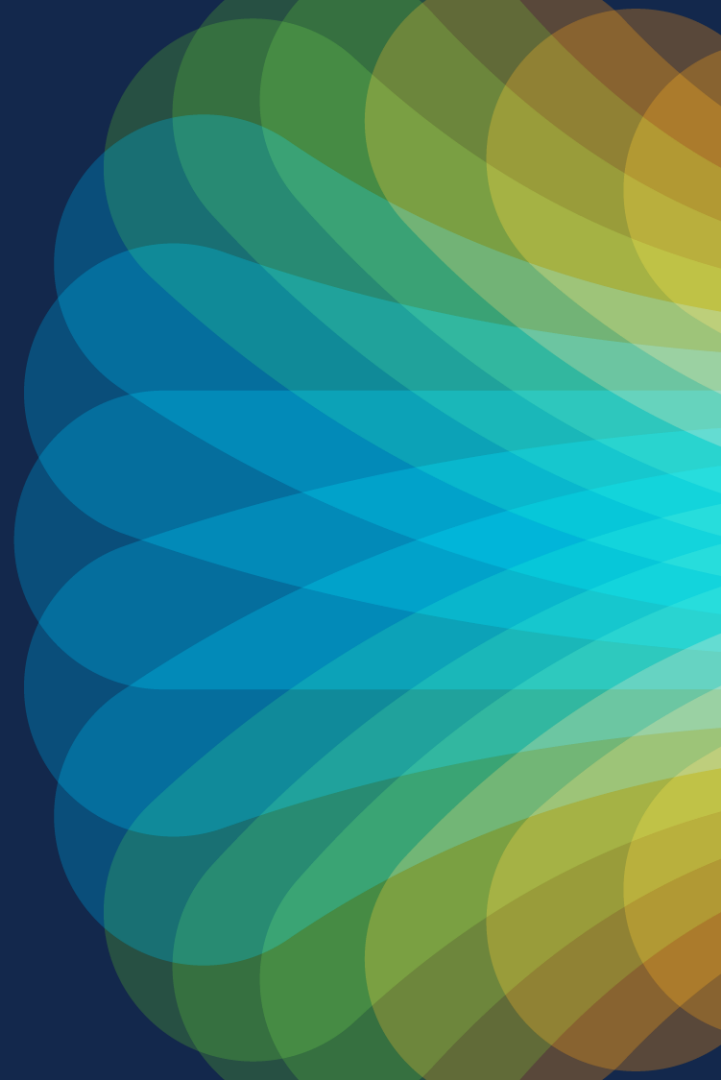
Inconsistent and siloed islands of policy controls across network & apps

Enforce Policy with Cisco Secure Workload

Unified Policy across Host, Network and Cloud

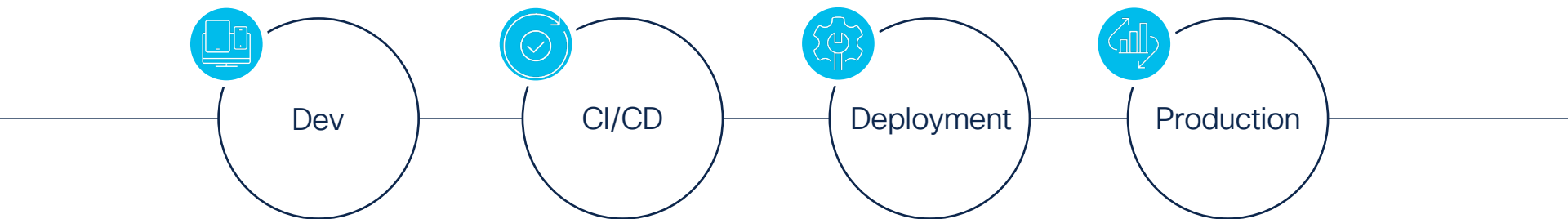


Securing Cloud Native Technologies



Enabling security across the full app stack

From Dev to Runtime



Shift Left
Security

Application
Composition

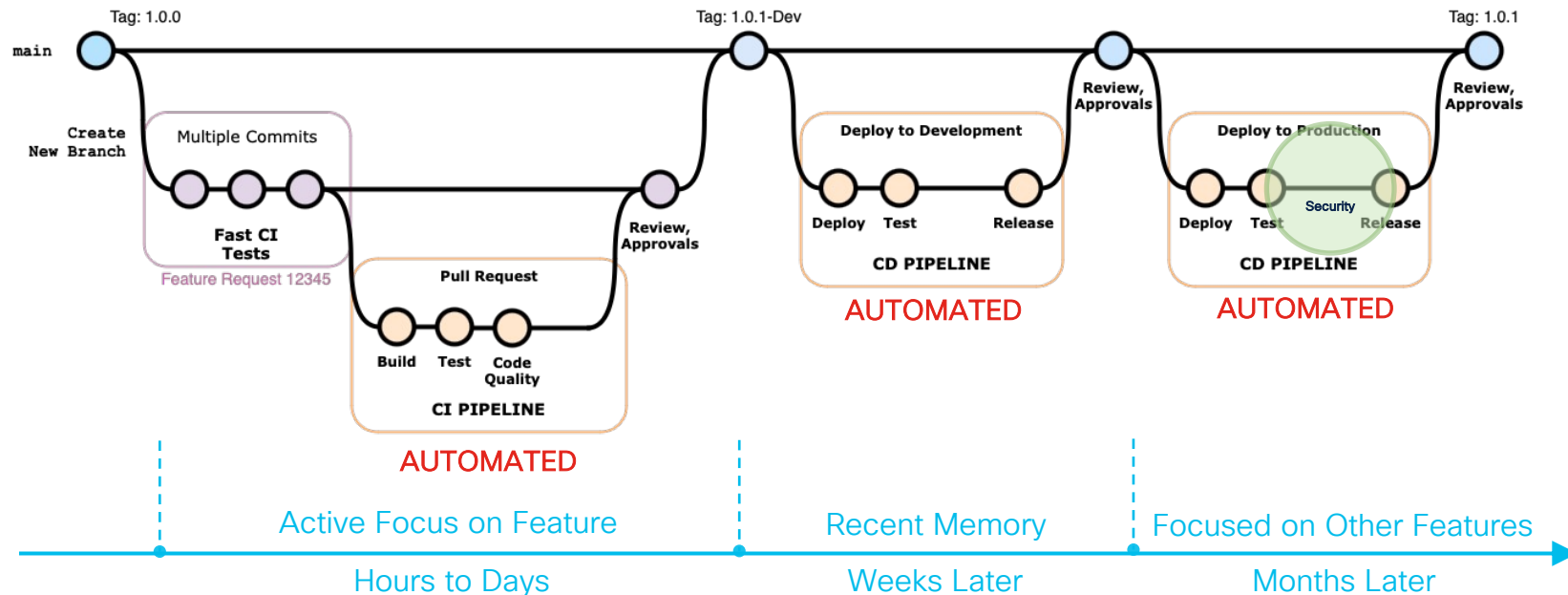
Connection and
API Assessment

Policy Control
Governance

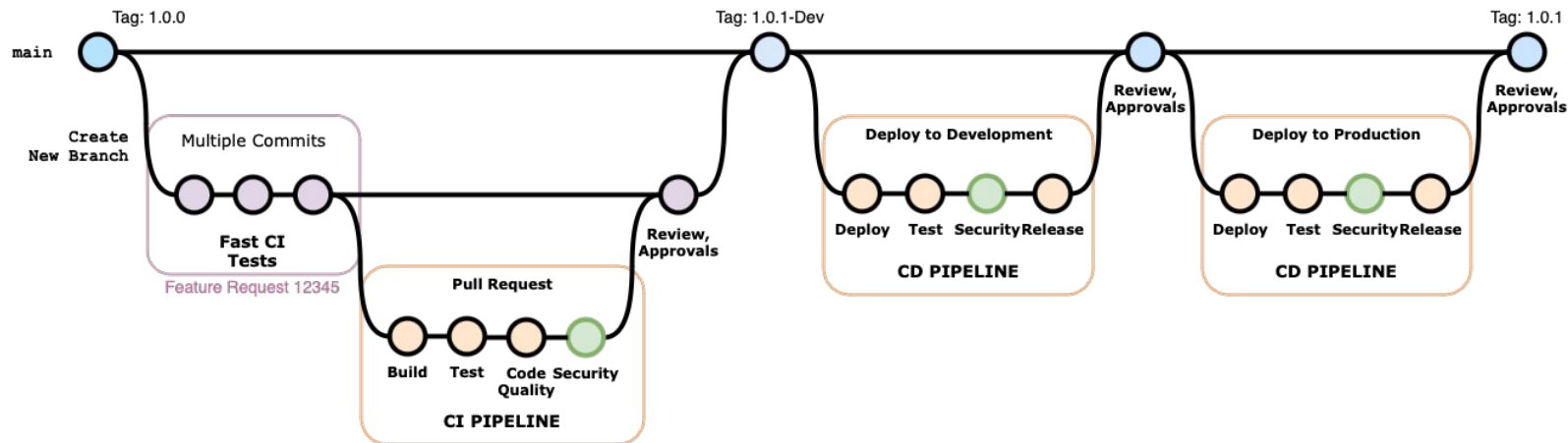


FAAS

Cloud Native Development Drives Velocity



Integrating Security in the Pipeline



Apply Security Before *Any* Integration

Apply Security Before *Every* Deployment

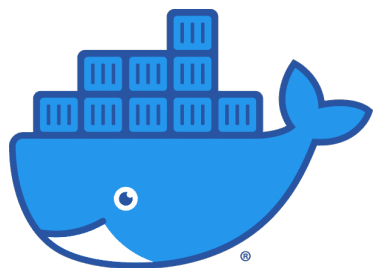
Shifting Security to the Left

Continuous Integration Actionable Security

PACKAGE NAME	PACKAGE VERSION	FIXED IN VERSION	VULNERABILITY	SEVERITY
python3.10	3.10.6-1~22.04.1	3.10.6-1~22.04.2	CVE-2022-37454	MEDIUM
python3.10	3.10.6-1~22.04.1	3.10.6-1~22.04.2	CVE-2022-45061	MEDIUM
python3.10-minimal	3.10.6-1~22.04.1	3.10.6-1~22.04.2	CVE-2022-37454	MEDIUM
python3.10-minimal	3.10.6-1~22.04.1	3.10.6-1~22.04.2	CVE-2022-45061	MEDIUM
zlib1g	1:1.2.11.dfsg-2ubuntu9.1	1:1.2.11.dfsg-2ubuntu9.2	CVE-2022-37434	MEDIUM
libssl3	3.0.2-0ubuntu1.6	3.0.2-0ubuntu1.7	CVE-2022-3602	HIGH
libssl3	3.0.2-0ubuntu1.6	3.0.2-0ubuntu1.7	CVE-2022-3786	HIGH
openssl	3.0.2-0ubuntu1	3.0.2-0ubuntu1.7	CVE-2022-3602	HIGH
openssl	3.0.2-0ubuntu1	3.0.2-0ubuntu1.7	CVE-2022-3786	HIGH
Total vulnerabilities: 54 (0 Critical, 4 High, 19 Medium, 31 Low, 0 Unknown)				
2022-12-12T22:08:32.854754Z info There is no .dockleignore file				
INFO - CIS-DI-0005: Enable Content trust for Docker				
* export DOCKER_CONTENT_TRUST=1 before docker pull/build				
INFO - CIS-DI-0006: Add HEALTHCHECK instruction to the container image				
* not found HEALTHCHECK statement				
INFO - CIS-DI-0008: Confirm safety of setuid/setgid files				
* setuid file: urwxr-xr-x usr/bin/chfn				
* setuid file: urwxr-xr-x usr/bin/chsh				
* setuid file: urwxr-xr-x usr/bin/su				
* setuid file: urwxr-xr-x usr/bin/gpasswd				
* setgid file: grwxr-xr-x usr/bin/chage				
* setuid file: urwxr-xr-x usr/bin/umount				
* setgid file: grwxr-xr-x usr/bin/expiry				
* setgid file: grwxr-xr-x usr/sbin/pam_extrausers_chkpwd				
* setgid file: grwxr-xr-x usr/sbin/unix_chkpwd				
* setuid file: urwxr-xr-x usr/bin/newgrp				
* setuid file: urwxr-xr-x usr/bin/mount				
* setgid file: grwxr-xr-x usr/bin/wall				
* setuid file: urwxr-xr-x usr/bin/passwd				

Developer Persona
Pipeline Report

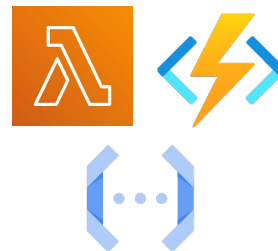
Cloud Native Technologies to Secure



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

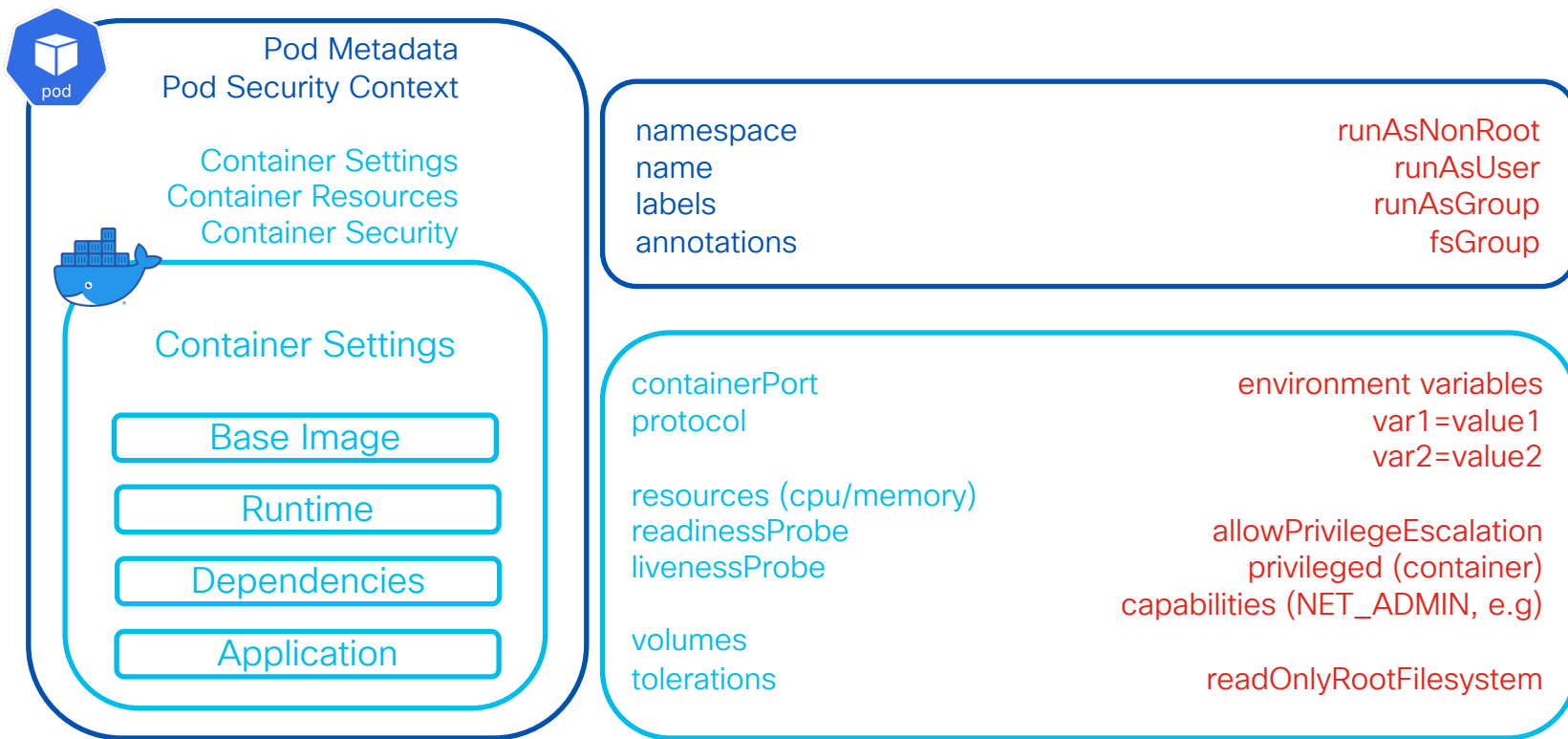
Application

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

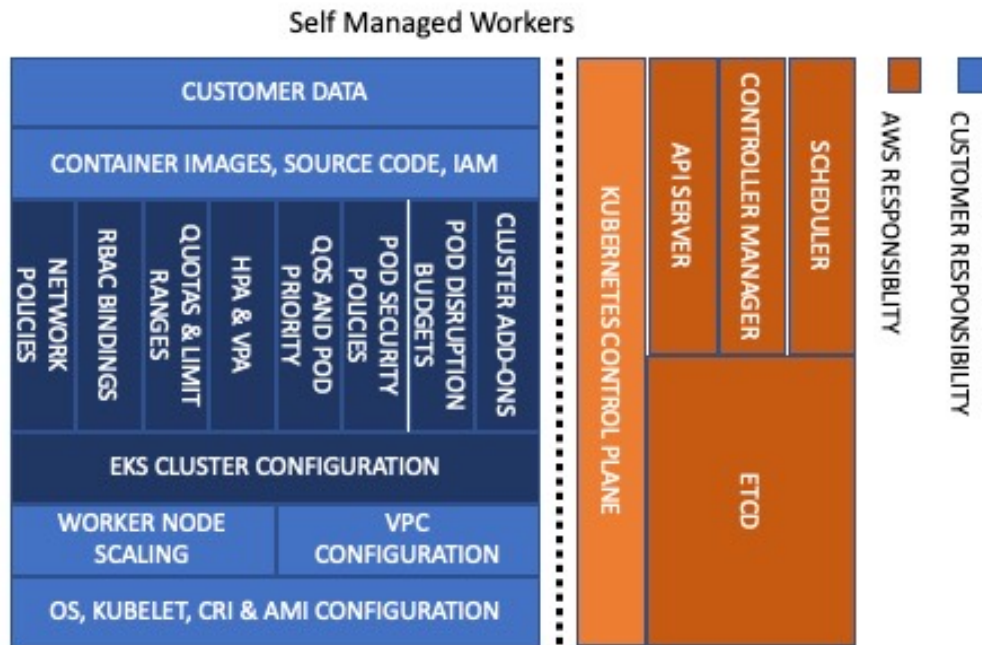
CIS Kubernetes Benchmarks

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

CIS Docker Benchmarks

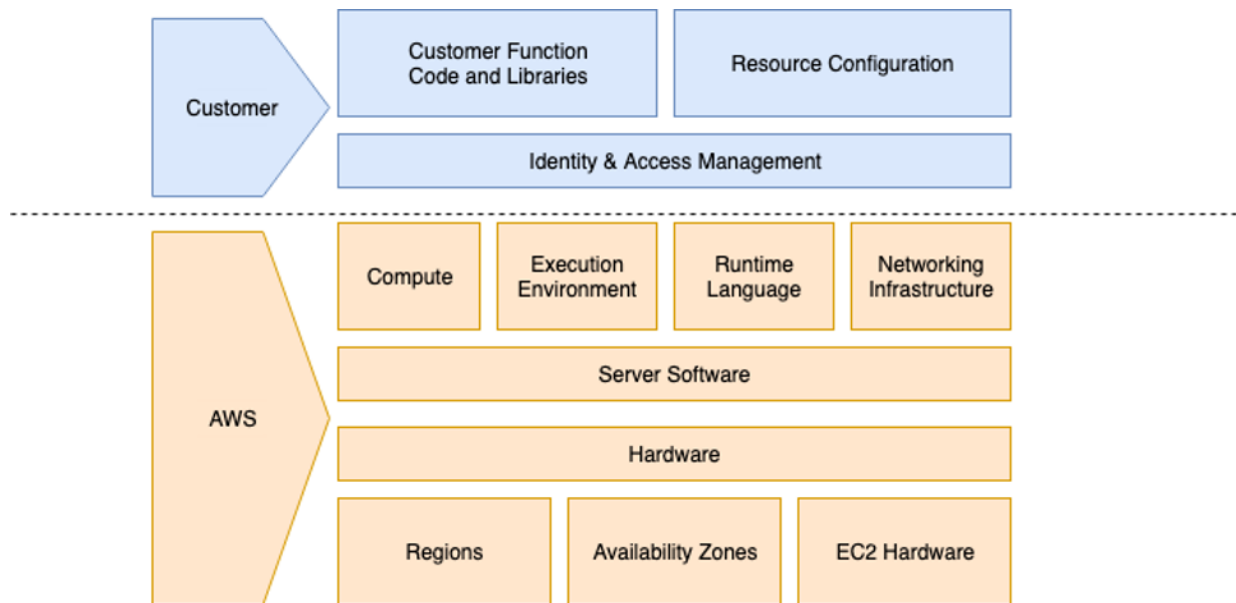
<https://www.cisecurity.org/benchmark/docker>

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

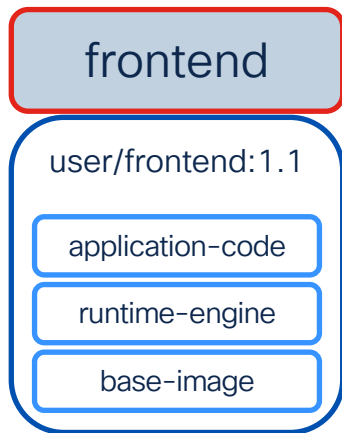
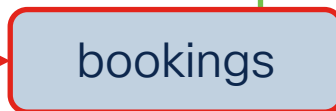
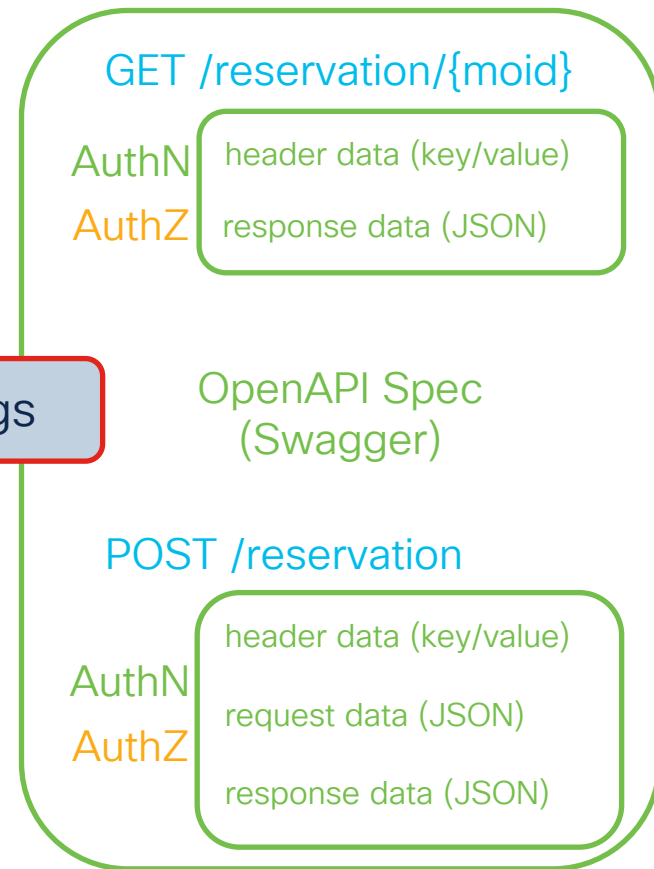


Source: AWS Shared Responsibility Model for Serverless

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

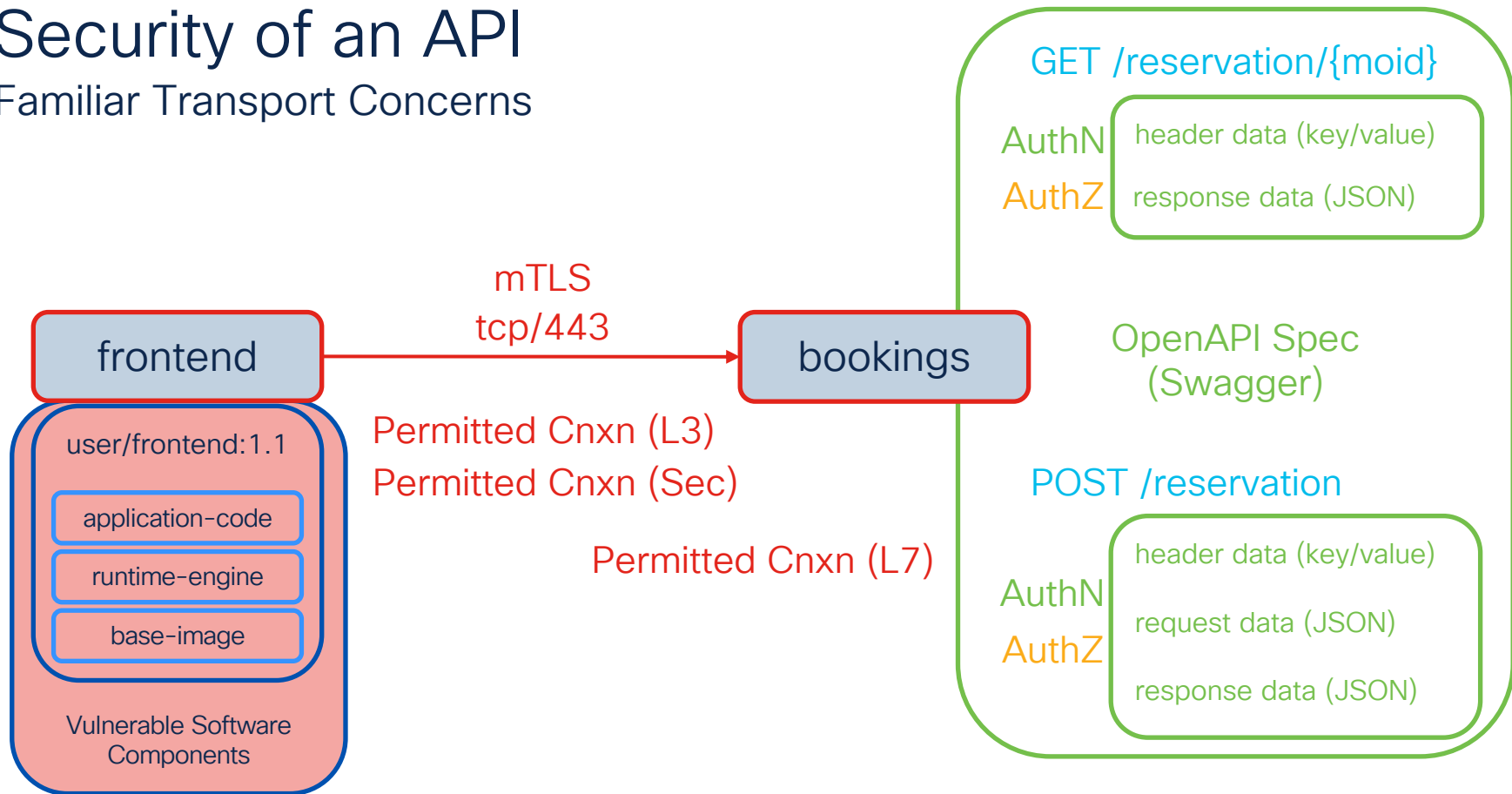
Anatomy of an API

(Application Programming Interface)



Security of an API

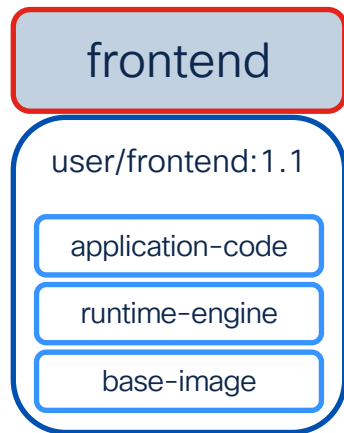
Familiar Transport Concerns



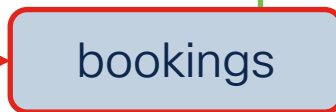
Security of an API

Application Layer (L7) Concerns

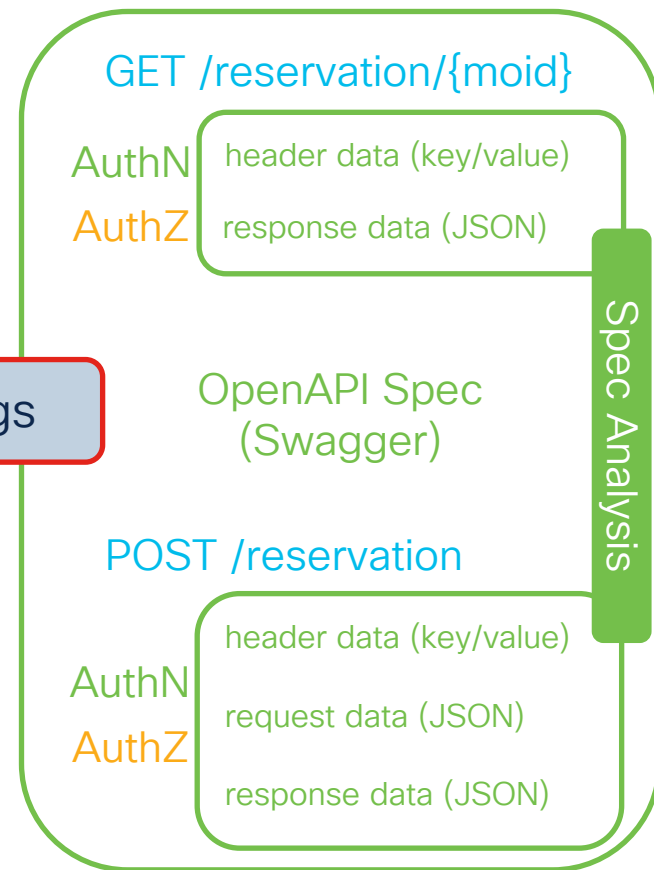
Broken Object Level AuthZ



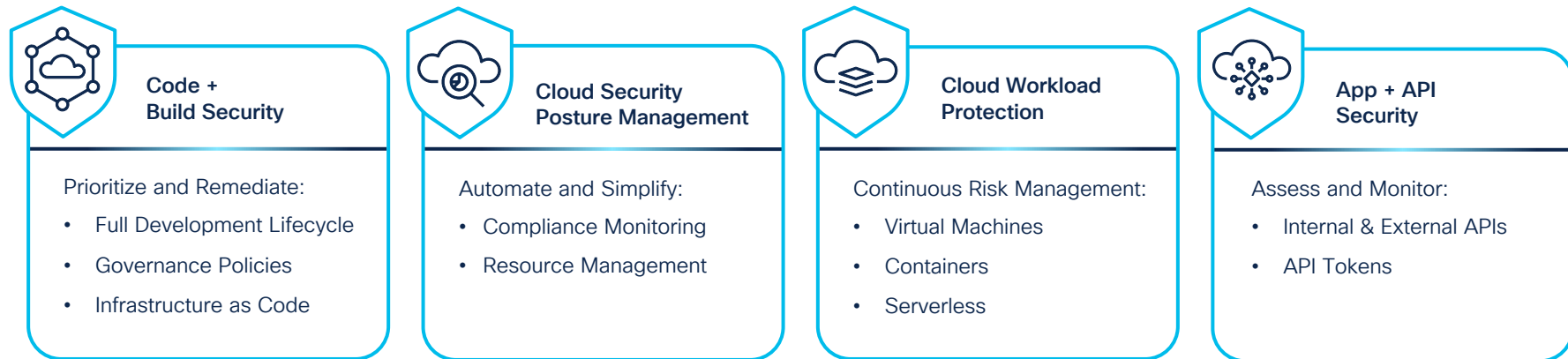
AuthN Token

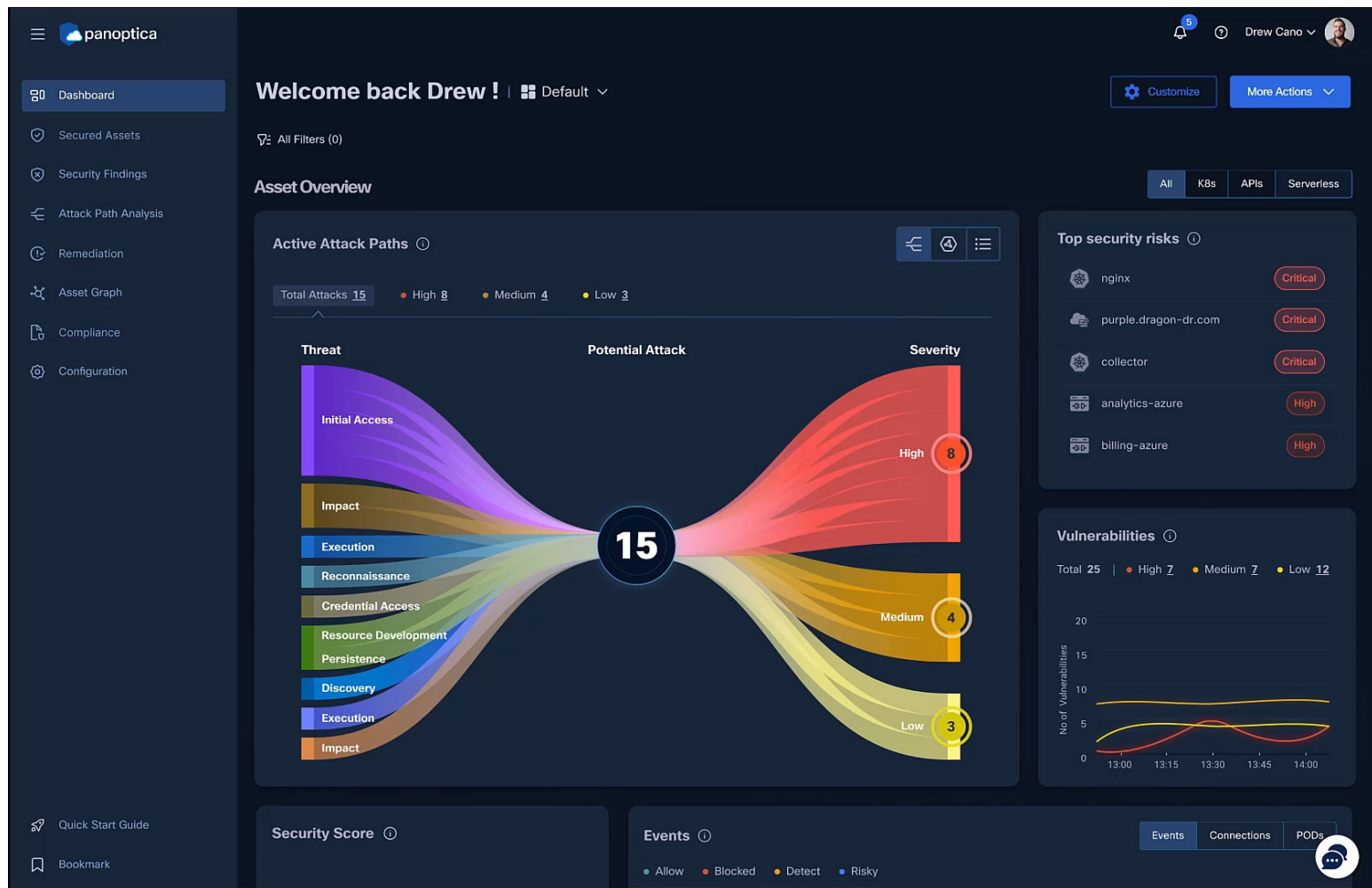


Broken Function Level AuthZ



Panoptica—Comprehensive Code to Cloud Security





Securing Application Runtimes

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

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

What is achievable in App Runtime

Software Composition Analysis (SCA) & Runtime App Self Protection (RASP)

Security insights enriched with Application and Business context to **Establish Visibility**

Continually
Detect
Vulnerabilities in
Libraries



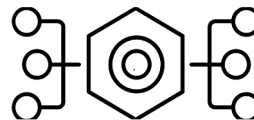
Common
Vulnerabilities and
Exceptions with Code
Level correlation

Enhanced Attack
detection via stack
traces



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

Respond by
Blocking Attacks



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

Enforce Policy through runtime instrumentation

Cisco Secure Application via AppDynamics Agent

Security insights provided with Application and Business context

Business Risk Observability

Detect Vulnerabilities



Common Vulnerabilities and Exceptions with Code Level correlation

Detect Attacks



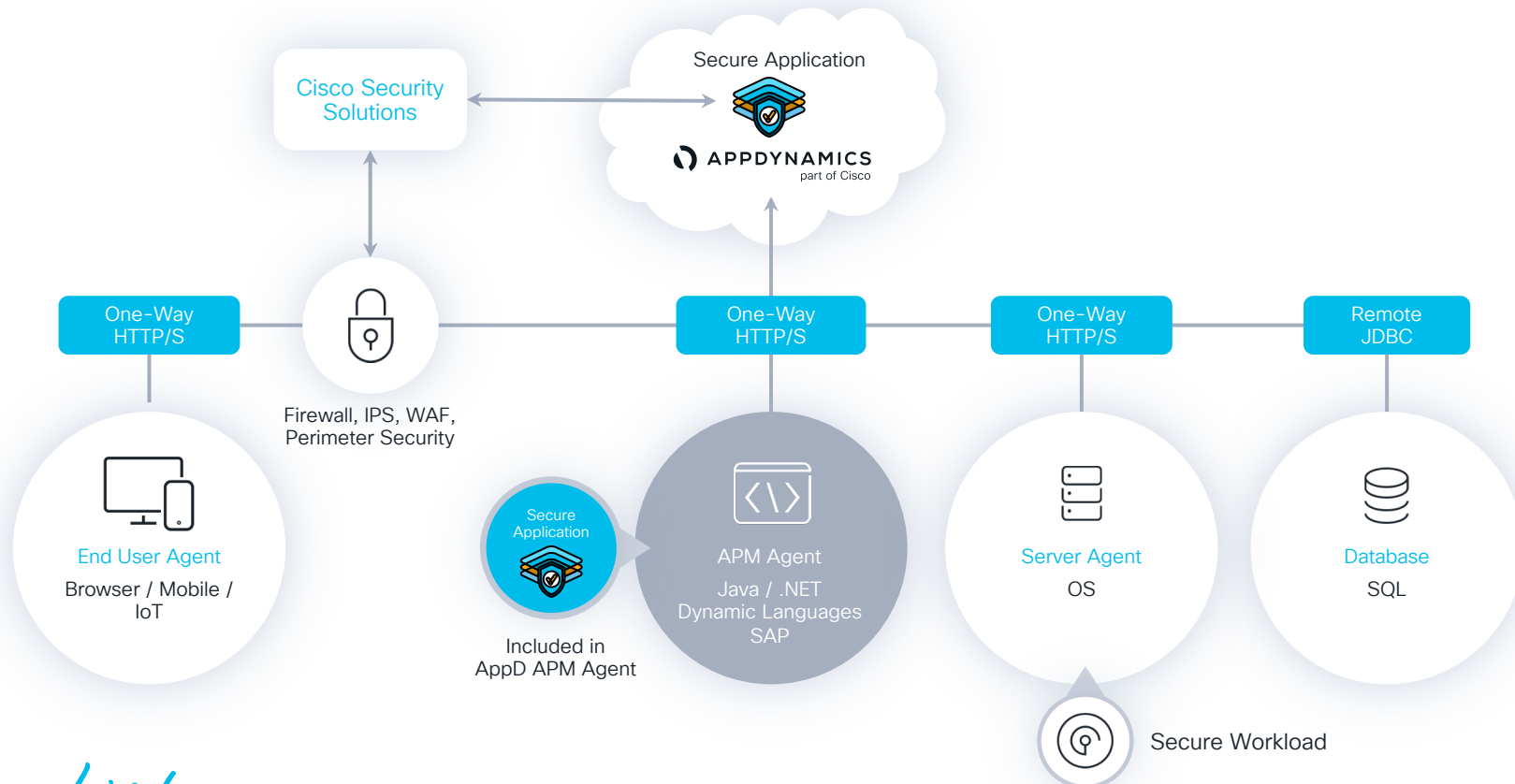
Spot CVE correlated runtime exploits and Zero Day attacks (like Log4j)

Block Attacks

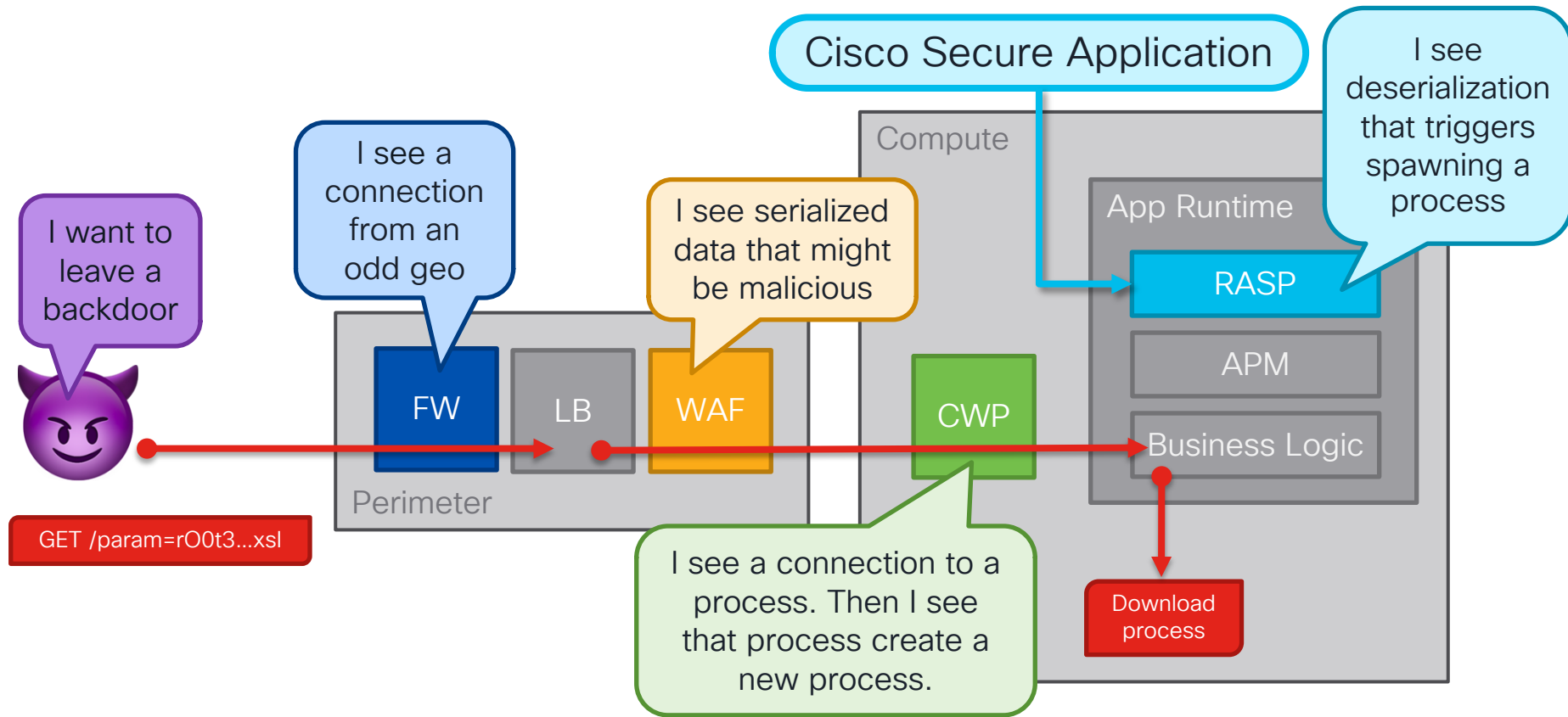


Policy level blocking that stops bad actors... even if vulnerabilities exist

AppDynamics Agent Architecture



What an attack looks like to the runtime sec stack



staging-sock-shop

Application Dashboard

Business Transactions

Service Endpoints

Tiers & Nodes

Servers

Containers

Database Calls

Remote Services

Troubleshoot

More

Alert & Respond

Metric Browser

Configuration

staging-sock-shop



Baseline...

last 1 hour



Dashboard

Network Dashboard

Events

Top Business Transactions

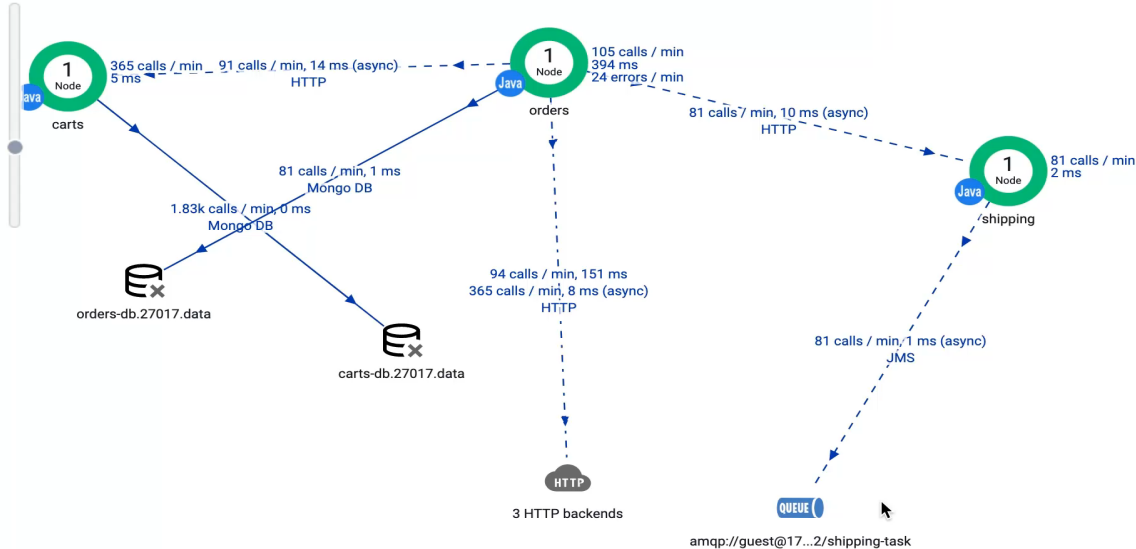
Transaction Snapshots

Transaction Score

Actions

Application Flow Map

Legend



Events

No Events in selected time range

Business Transaction Health

0 critical, 0 warning, 7 normal

Node Health

0 critical, 0 warning, 3 normal

Server Health

Security Health

Business Risk

800

Vulnerabilities (Real-time)

Critical 30 High 254 Medium 93 Low 18

Attacks (Last 1 Hour)

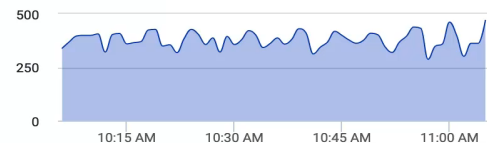
Exploited 4 Blocked 1 Attempted 1

Transaction Scorecard

Normal 93.3 % 21.2k

Not comparing against Baseline data

Load 22.7k calls 379 calls / min



Response Time (ms) 113 ms average



Errors 6.4% 1.45k errors 24 errors / min



Cisco Secure Application for cloud native apps

Business risk insights via Full Stack Observability – agentless approach



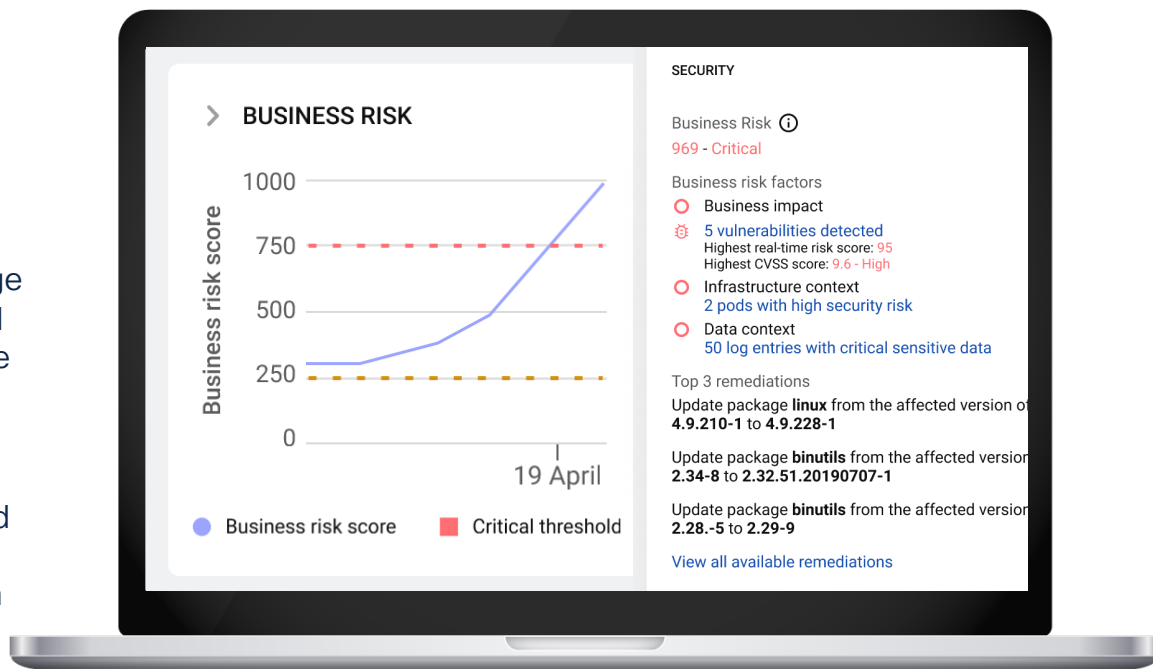
Locate and highlight threats and vulnerabilities across k8s and containers, securing deployment of modern applications on k8s



Detect and protect against leakage of sensitive data with pre-defined expressions to ensure compliance

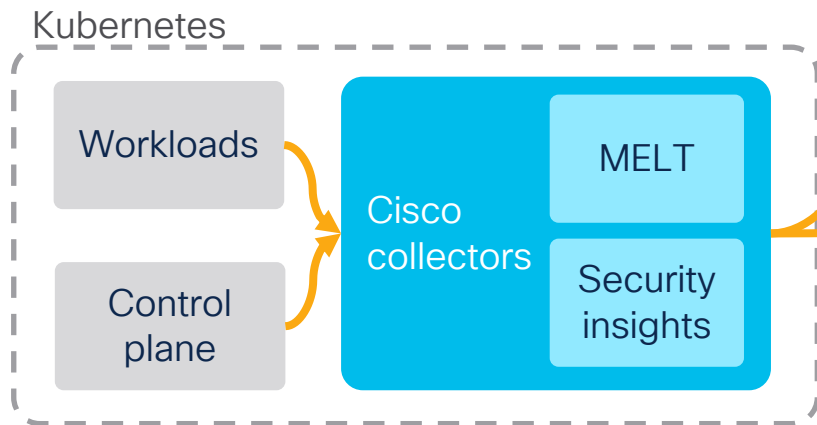
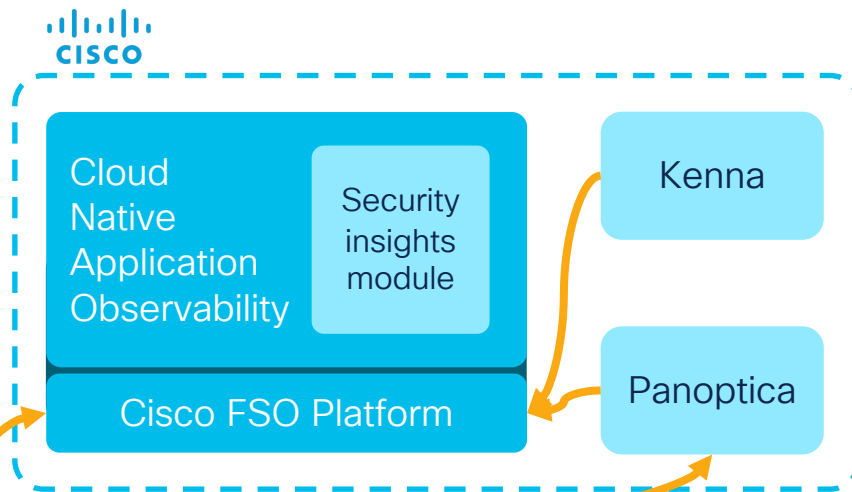


Combine threat and vulnerability intelligence from Cisco Kenna and Panoptica with business impact and runtime behavior to provide a business risk score



Security insights module architecture

Security insights collectors including Panoptica Controller are deployed in one Cisco Helm chart



Cisco Kenna and Panoptica integrations are automatically created

Security insights module

Correlated with Application and Business context

Business Risk Observability

Detect Vulnerabilities



Runtime container vulnerability detection with remediation guidance

Infrastructure Posture



Find configuration issues and vulnerabilities in Kubernetes configurations

Sensitive Data Redaction



Automatically detect and redact data leakage to maintain compliance

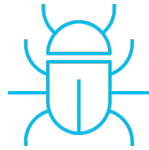


Summary

Cloud Native Apps introduce more security complexity



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	

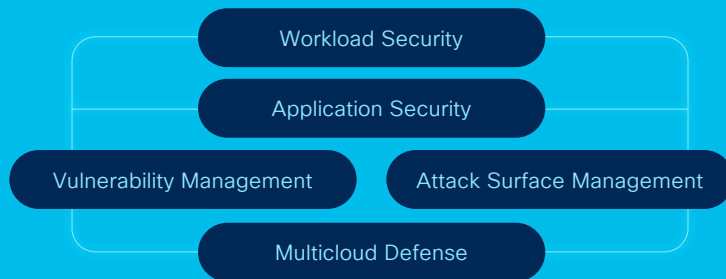
Sleep Peacefully



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

Introducing security only Cisco can deliver

Cisco Cloud Protection Suite



* Global General Availability Coming Soon



Cisco
Multicloud
Defense



Cisco
Vulnerability
Management



Cisco Secure
Workload



Cisco Attack
Surface
Management



Cisco Cloud
Application
Security

Related Sessions

- Securing Cloud Native Applications with Panoptica - BRKETI-2511
- Business Risk Observability for Traditional and Modern Applications- BRKSEC-2405
- How to Build a Secure Multi-Cloud Environment with Cisco Secure Workload & Multicloud Defense - BRKSEC-1773

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase 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



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#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

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



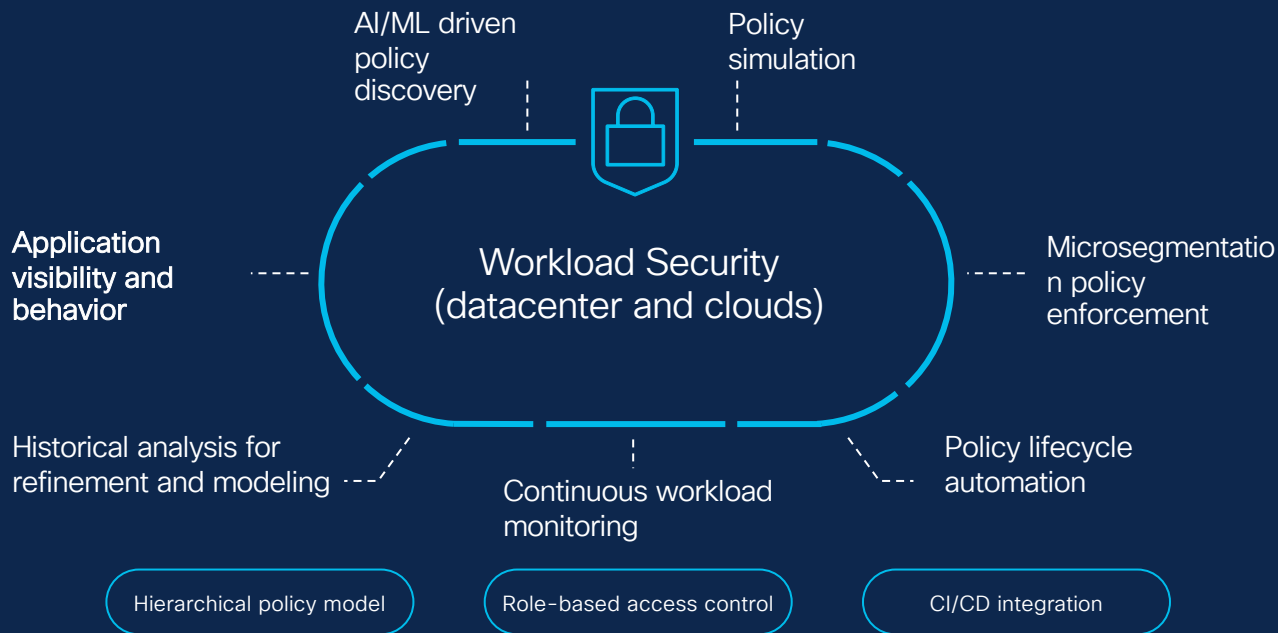
Data-driven vulnerability prioritization

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

Cisco Secure Workload



Stop lateral movement

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

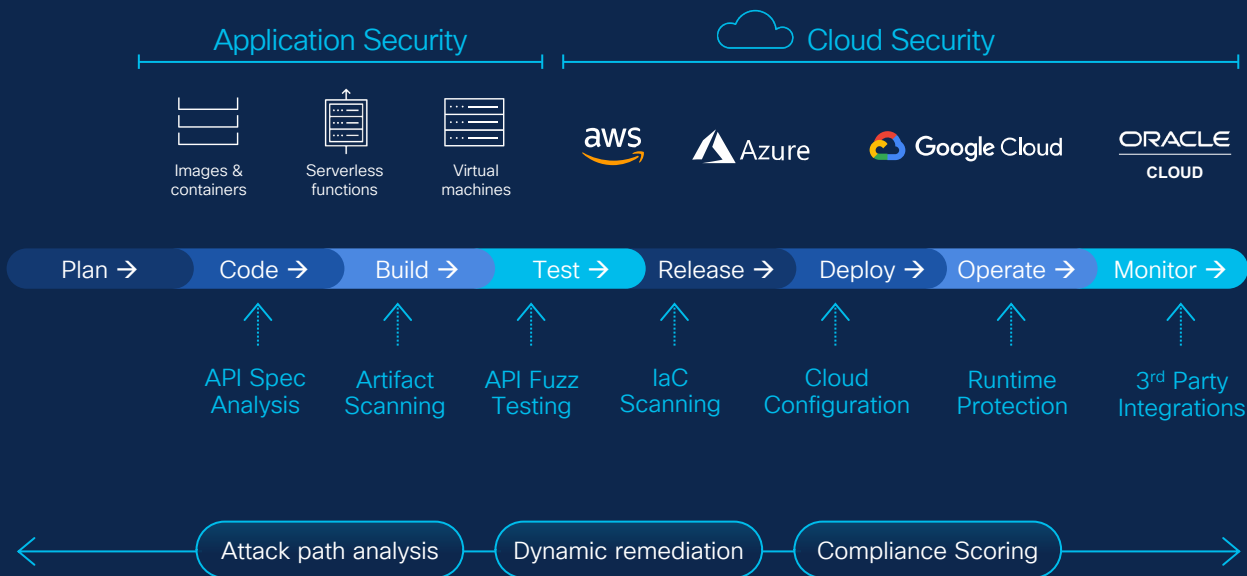
Quickly improve security posture

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

