Let's go

The bridge to possible

Business Risk Observability for Traditional and Modern Applications

Application Security with Business Context

Kashyap Merchant, Director, Product Management, Cisco

BRKSEC-2405

Cisco Webex App

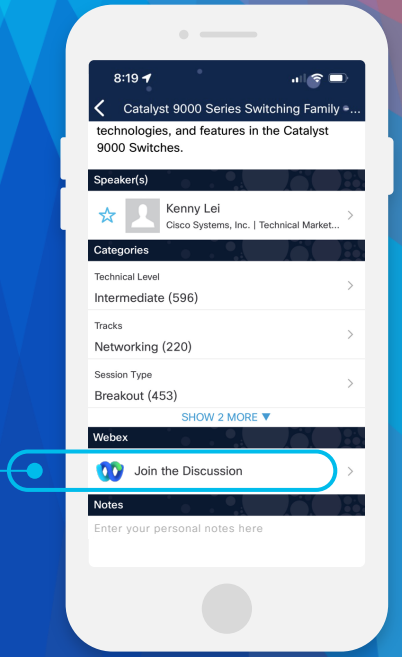
Questions?

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-2405

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

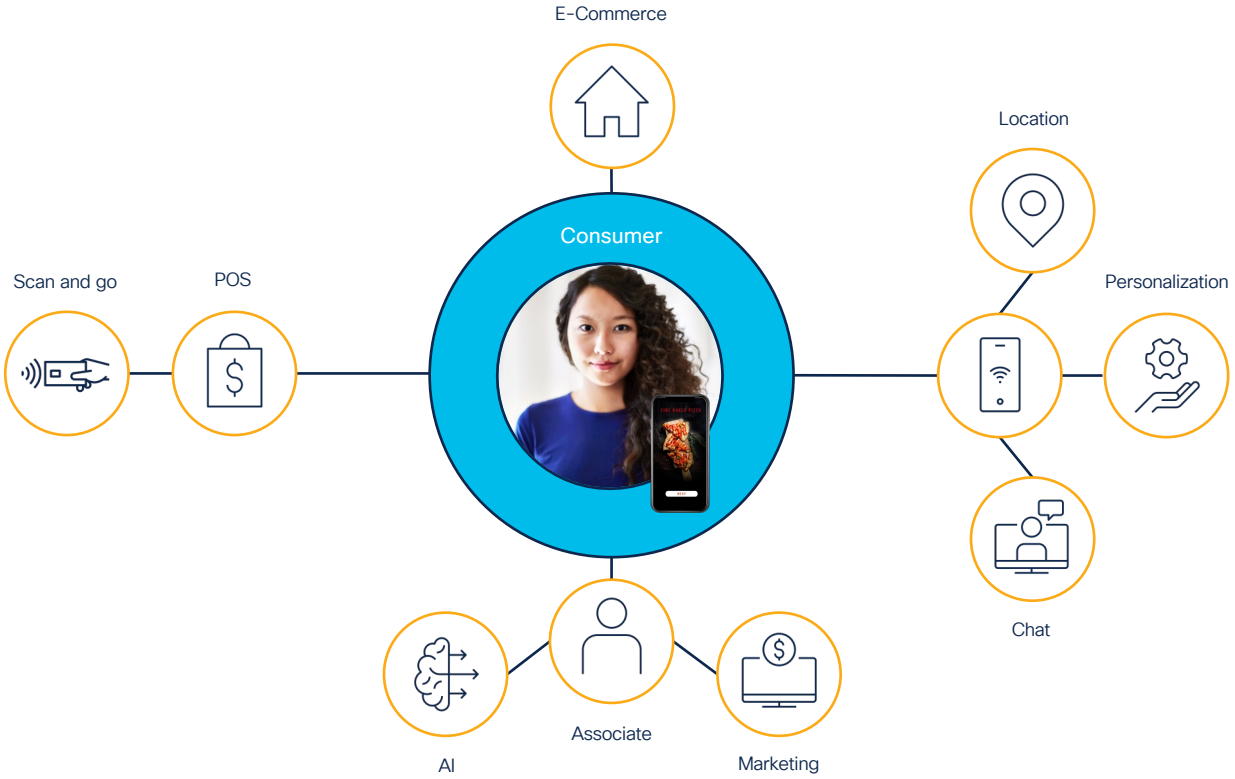
A little about me...

Agenda

- Securing the new digital world
- Foundational concepts of applications
- Application security for hybrid applications
- Security insights for cloud native applications

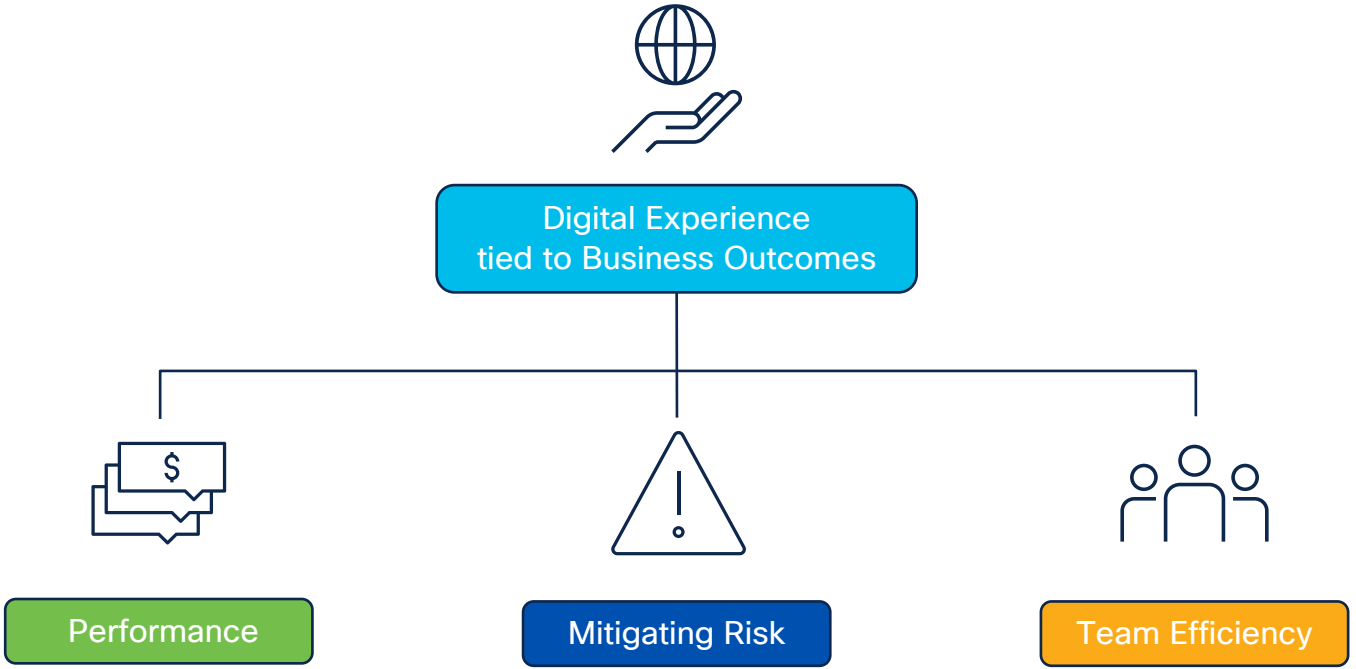
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

We will in an evolving and expanding digital world



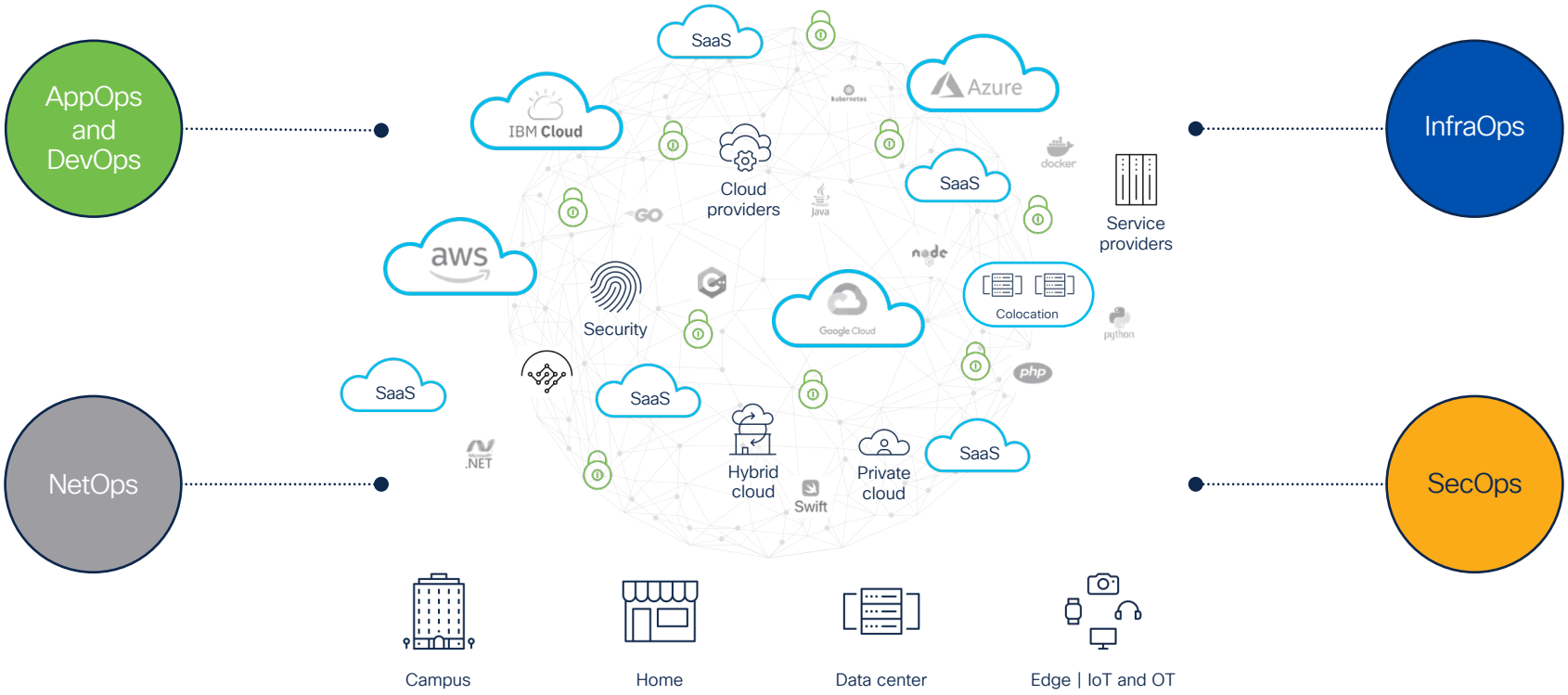
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where digital experience is the new business KPI



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

But applications are built in complex environment



There is no **business context**

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

Which leads to

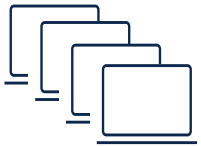
56% Use more than 10 application observability/monitoring tool

60% Say most observability tools serve narrow requirements and fail to enable a complete view

74% Struggle with data collection and correlation

Complexity

Data overload



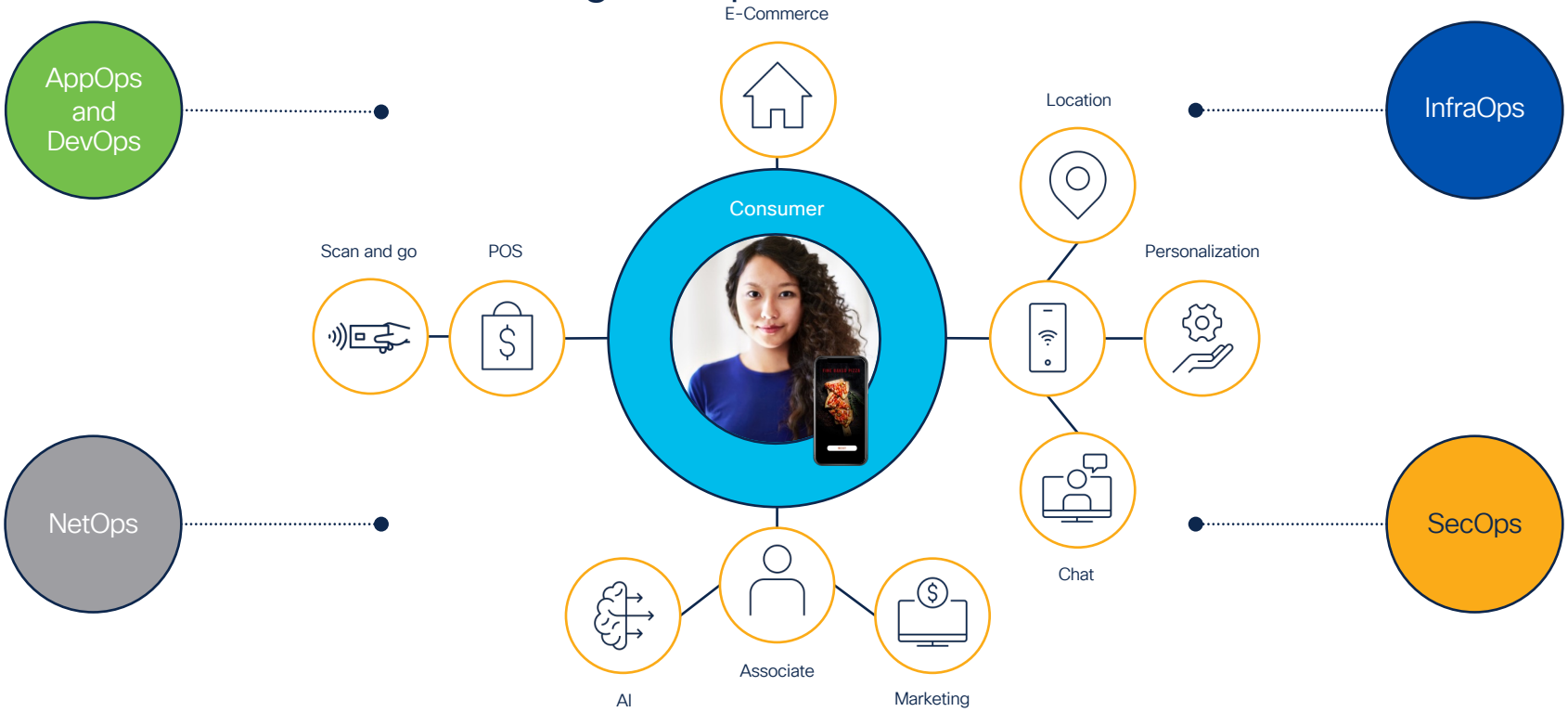
Tool sprawl

Friction between teams

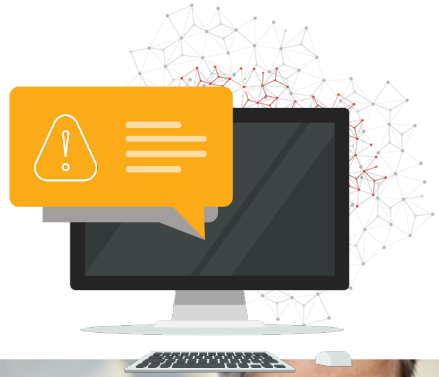
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

So, teams need to see the full stack of available data

Shared context across the digital experience



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



Focused on vulnerabilities & threats

App Team

Security Team

Focused on velocity & user experience

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

The stakes are different for security

$6-10 Trillion

Global Impact of Cybercrime

Cost siphoned from beneficial investment to combat Cybercrime

Source: Cybersecurity Ventures, 2021-2025 Estimate

800%

Increase in Nation-State initiated Cyber attacks

Since start of Russia-Ukraine War

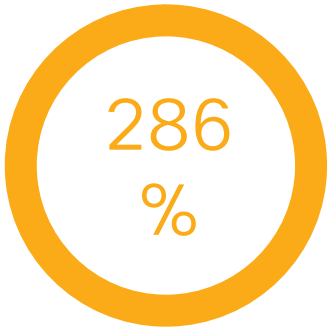
Source: The Register, Cyberattack Escalation, March 2022

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

Explosion of threats in microservices security

Companies with a Kubernetes security incident in last 12 months

Source: RedHat, 2022



API attacks increase, will be most frequent attack vector

Source: Gartner, 2022

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

Customer pain is real and similar to ITOps problems

$9.44M

Cost to Contain a Breach in the US

Average cost to contain a breach with 38% of this cost from lost business

Source: Ponemon Institute, 2022

277 days

¾ of a year to detect breach occurred!

Average time to identify and contain a data breach

Source: Ponemon Institute, 2022

Breaches with data exfiltrated in the first 24-hours

Source: Cisco Security, 2020

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

Our Agents of Transformation

ITOps / DevOps

“Allison”

“I want to help secure our apps, but not at the expense user experience or availability.”

SecOps

“Zane”

“I need visibility and control everywhere to protect our business, which leads to alert avalanches.”

AppSec

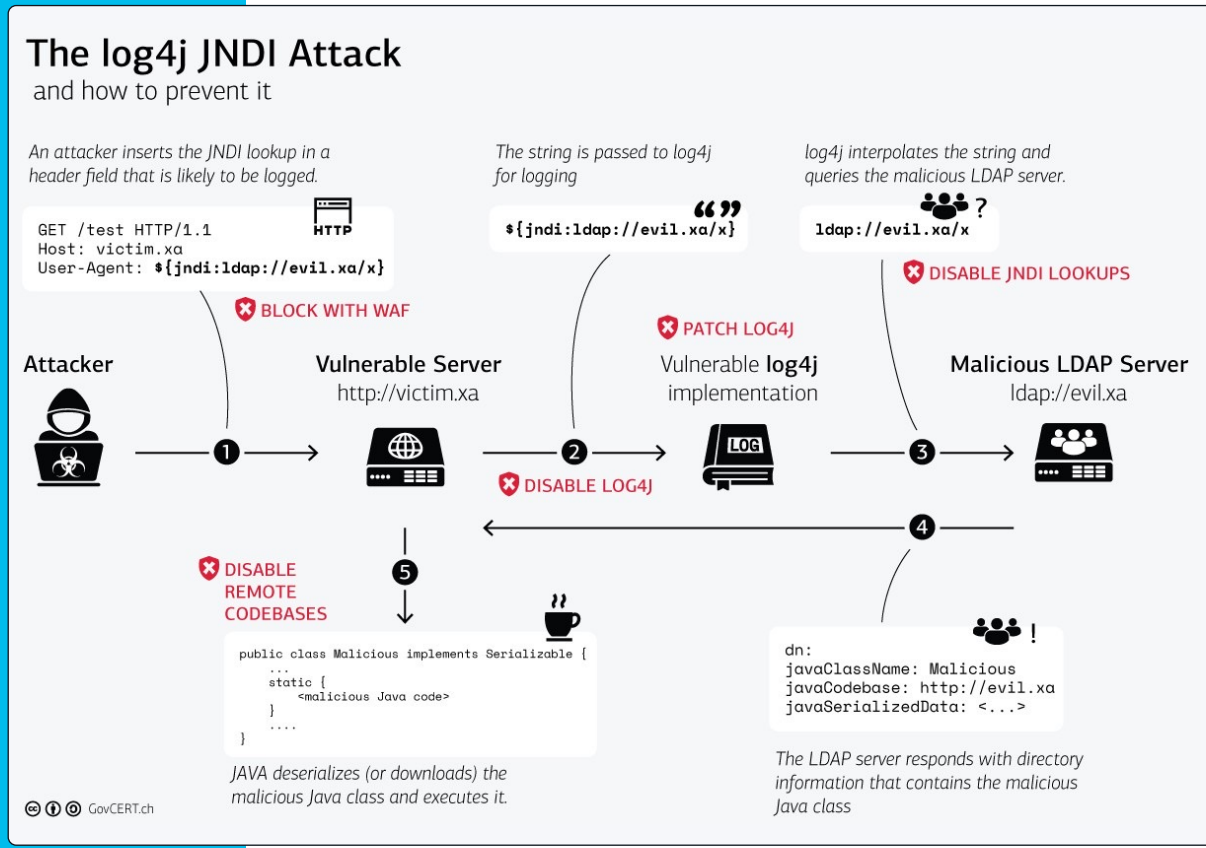
“Aarya”

“I uncover security bugs as soon as I can, but dev can’t fix them all, so I try to pick what matters most.”

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

Business can't afford App and Sec silos

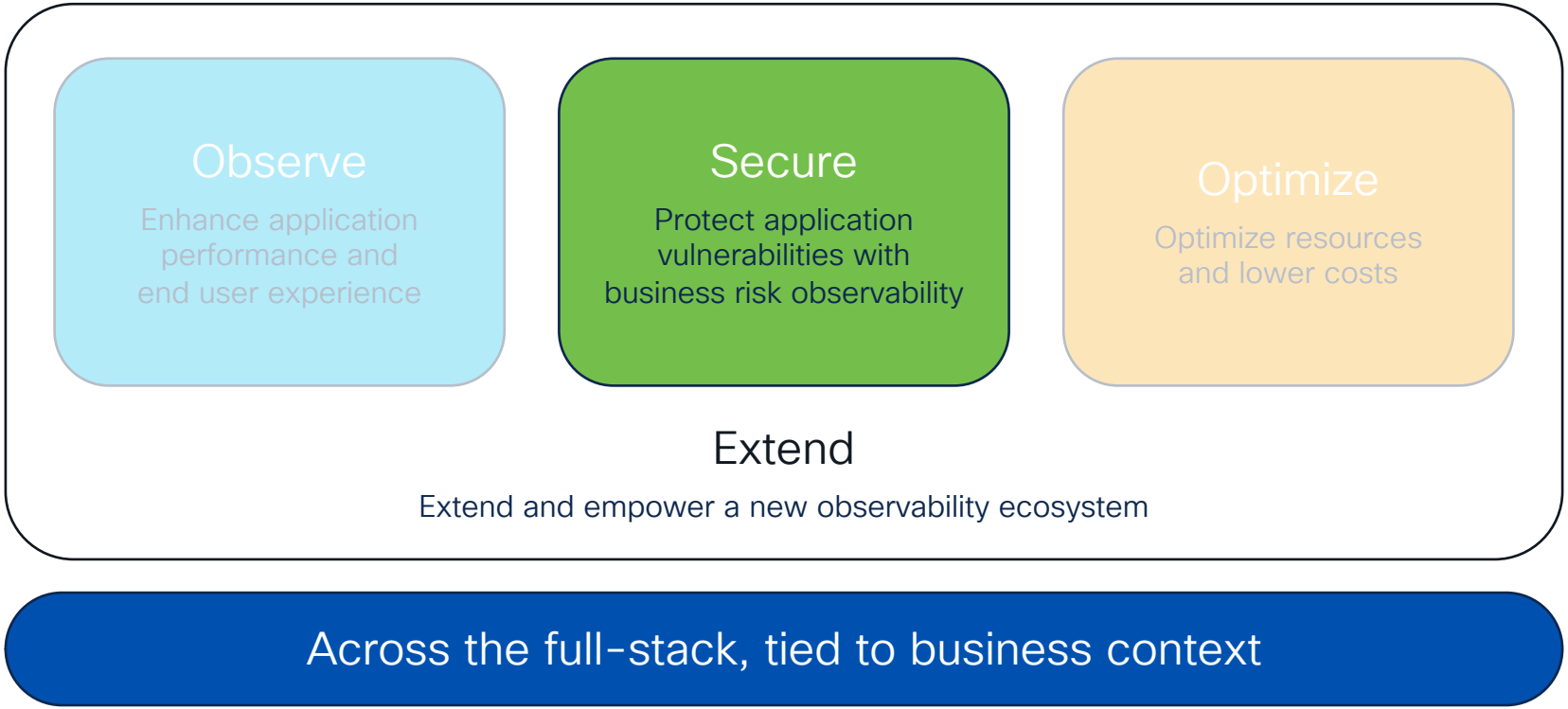
Without both teams joining the fight, issues like the log4j JNDI vulnerability can't be protected against in a timely fashion



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

How can Cisco help?

How Cisco Full-Stack Observability can help?



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

Applications require a new security approach

Empowering the digital enterprise to operate with speed and security

New applications		Require new protections
Run anywhere		CLOSER to the application
Change constantly		CONTINUOUSLY automates security
Are unique		ADAPTIVE for the application

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

Business Risk Observability

Full-Stack Observability – Secure

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.

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

Foundational concepts

Runtime Environments

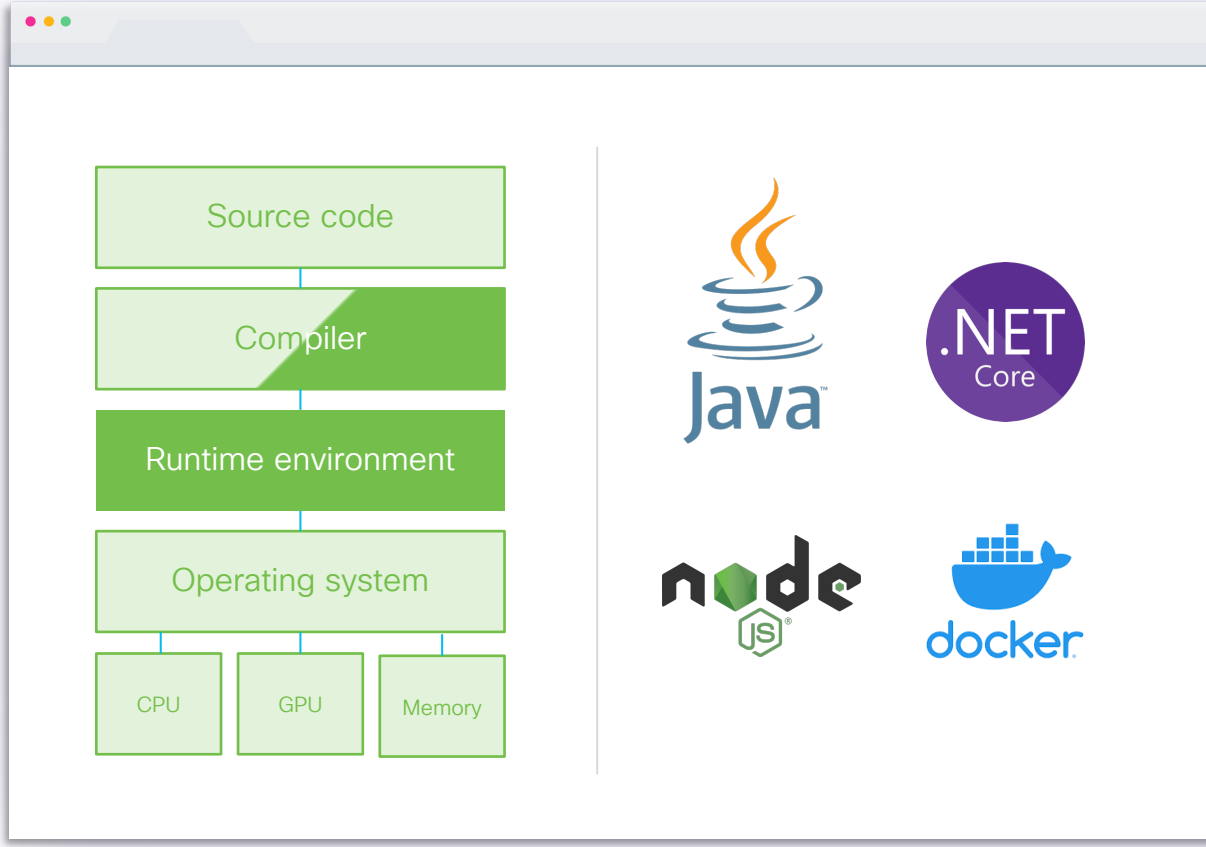
Everything needed to run the code

Enables portability
Write once and run everywhere*

Interfaces with the host OS
Obfuscate OS-specific APIs

Manage application memory
No need to handle the complexity in your code

Loads dependencies
Finds and makes third-party code accessible



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

Containers and Kubernetes

Accelerant to microservice architectures

Enables agile application processes

Continuous development, integration, and deployment

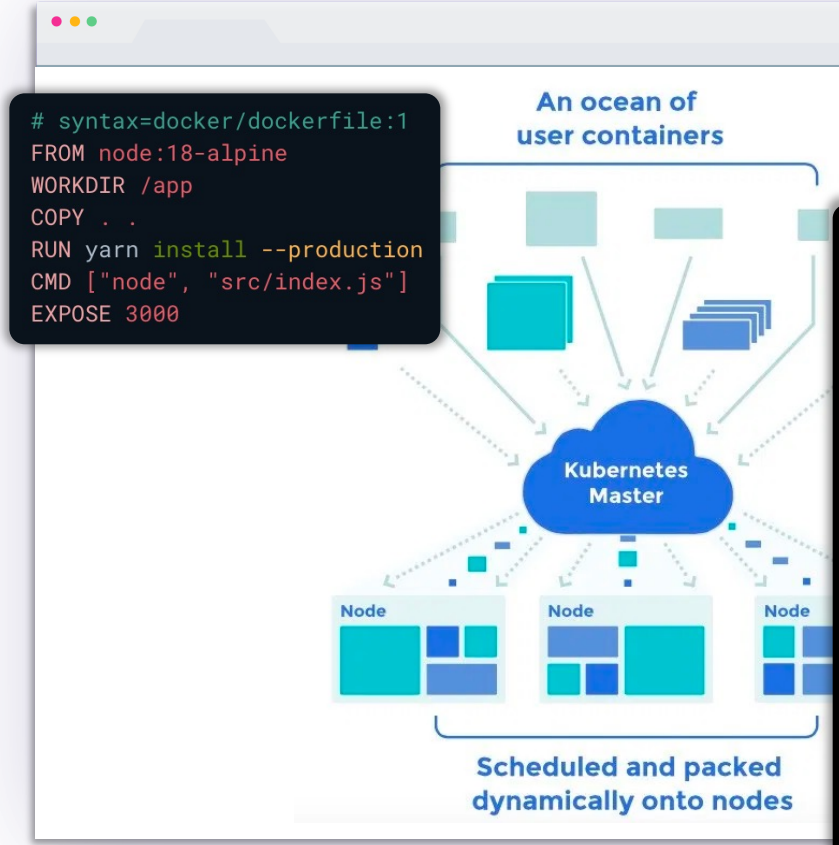
Resilient distributed systems

Service discovery and load-balancing and automated scaling and failover

Consistent deployments

Declarative configuration keeps environments running as expected

```
# syntax=docker/dockerfile:1
FROM node:18-alpine
WORKDIR /app
COPY . .
RUN yarn install --production
CMD ["node", "src/index.js"]
EXPOSE 3000
```




```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: nginx-deployment
  labels:
    app: nginx
spec:
  replicas: 3
  selector:
    matchLabels:
      app: nginx
  template:
    metadata:
      labels:
        app: nginx
    spec:
      containers:
      - name: nginx
        image: nginx:1.14
        ports:
        - containerPort:
```


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

Libraries

Build applications quicker with more consistency

Reusable building blocks for common functions

Teams standardize on OSS and internally-distributed libraries

Let the experts build your app for you

Focused and experienced teams often build a better solution

Static or shared libraries

Compile the library into the application or dynamically load it

```java
import org.apache.log4j.Logger;

public class HelloWorld {

   private static final Logger log = Logger.getLogger(HelloWorld.class);

   public static void main(String[] args) {
      log.info("Hello World!");
   }
}
```

```javascript
const express = require('express')
const app = express()

app.get('/', (req, res) => {
  res.send('Hello World!')
})

app.listen(8080)
```


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

Vulnerability Management

Common Vulnerabilities and Exposures (CVE)

Program identifies, defines, and catalogs publicly disclosed Cybersecurity Vulnerabilities

Common Vulnerability Scoring System (CVSS)

Severity	Base Score Range
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

- Consistent assessment across industry
- Static scoring without manual adjustments
- Does not measure risk—measures technical severity
- Not a predictor of exploitation

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

Instrumentation

Painlessly get deep insight and alter applications

Observe and measure

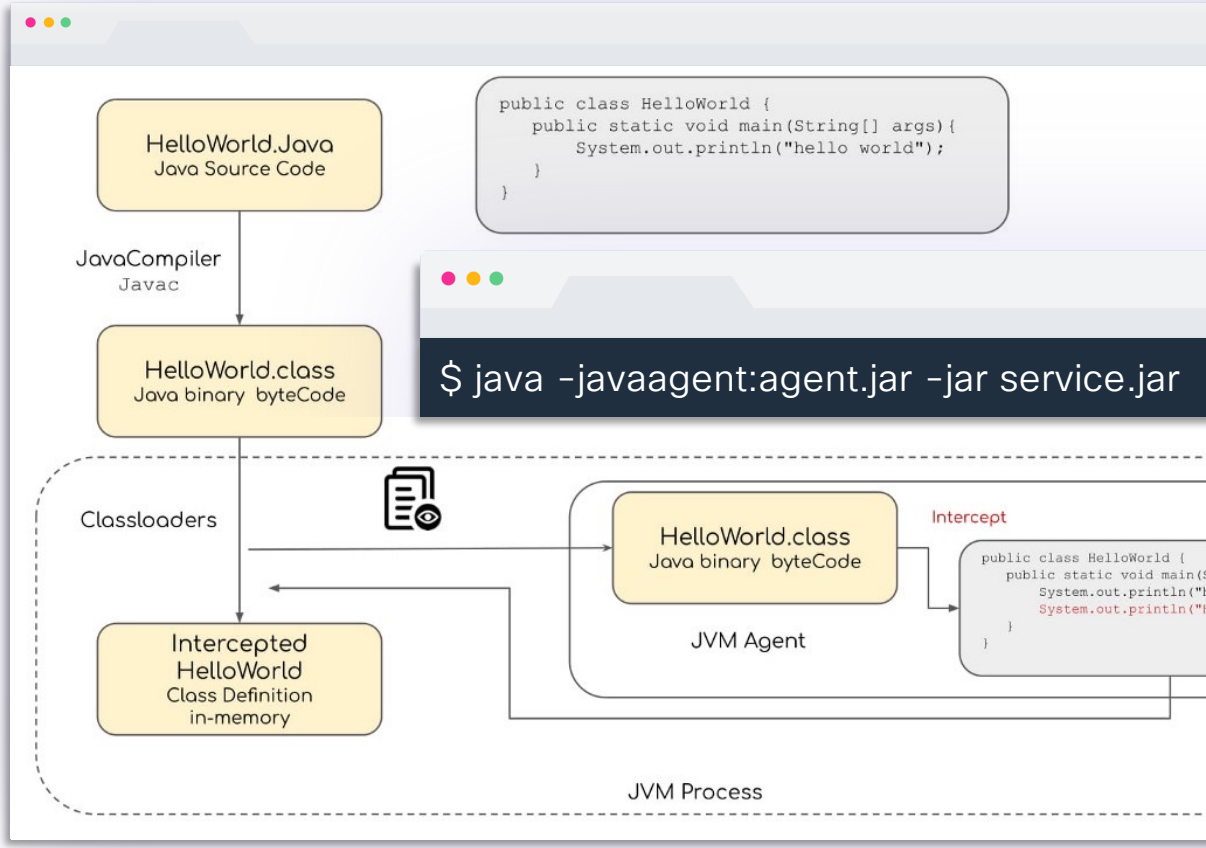
Ops gets insight into black box operation

Modify behavior

Ops can add capabilities to enhance or protect

Leave source code untouched

Devs don't need to get involved



Source: Balakrishnan Sathiyakugan

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

Stack Traces

Understand the path through an application when debugging

Triggered for explicit or unexpected error conditions
Give guidance to incorrect use of the application

Sequence of functions called during execution
Understand how execution arrived at the error

Correlate runtime to source
File and line of code from source guides Devs

```
1.  public class StackTrace {
2.
3.    public static void main(String[] args) {
4.      a();
5.    }
6.
7.    static void a() {
8.      b();
9.    }
10.
11.   static void b() {
12.     c();
13.   }
14.
15.   static void c() {
16.     Thread.dumpStack();
17.   }
18.
19. }
```

```
$ javac StackTrace.java
$ java StackTrace
java.lang.Exception: Stack trace
    at java.lang.Thread.dumpStack(Thread.java:132
    at StackTrace.c(StackTrace.java:16)
    at StackTrace.b(StackTrace.java:12)
    at StackTrace.a(StackTrace.java:8)
    at StackTrace.main(StackTrace.java:4)
```


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

OpenTelemetry

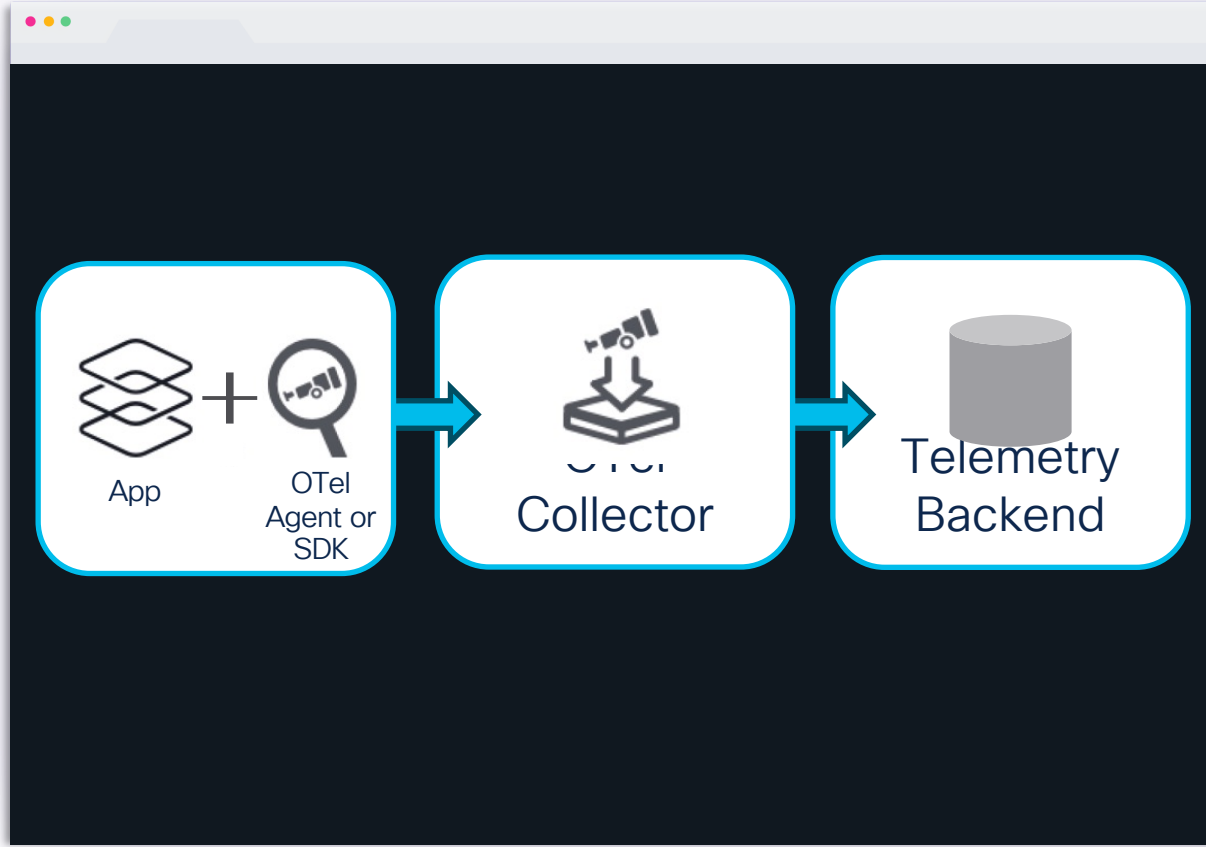
Vendor-agnostic telemetry for any stage in Observability journey

Instrumentation library per language
Support for both automatic and manual instrumentation

End-to-end implementation
Generate, emit, collect, process and export telemetry data

Full control of your data
Ability to send data to multiple destinations

Open-standard semantic conventions
Ensure vendor-agnostic data collection



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

Application Performance Monitoring

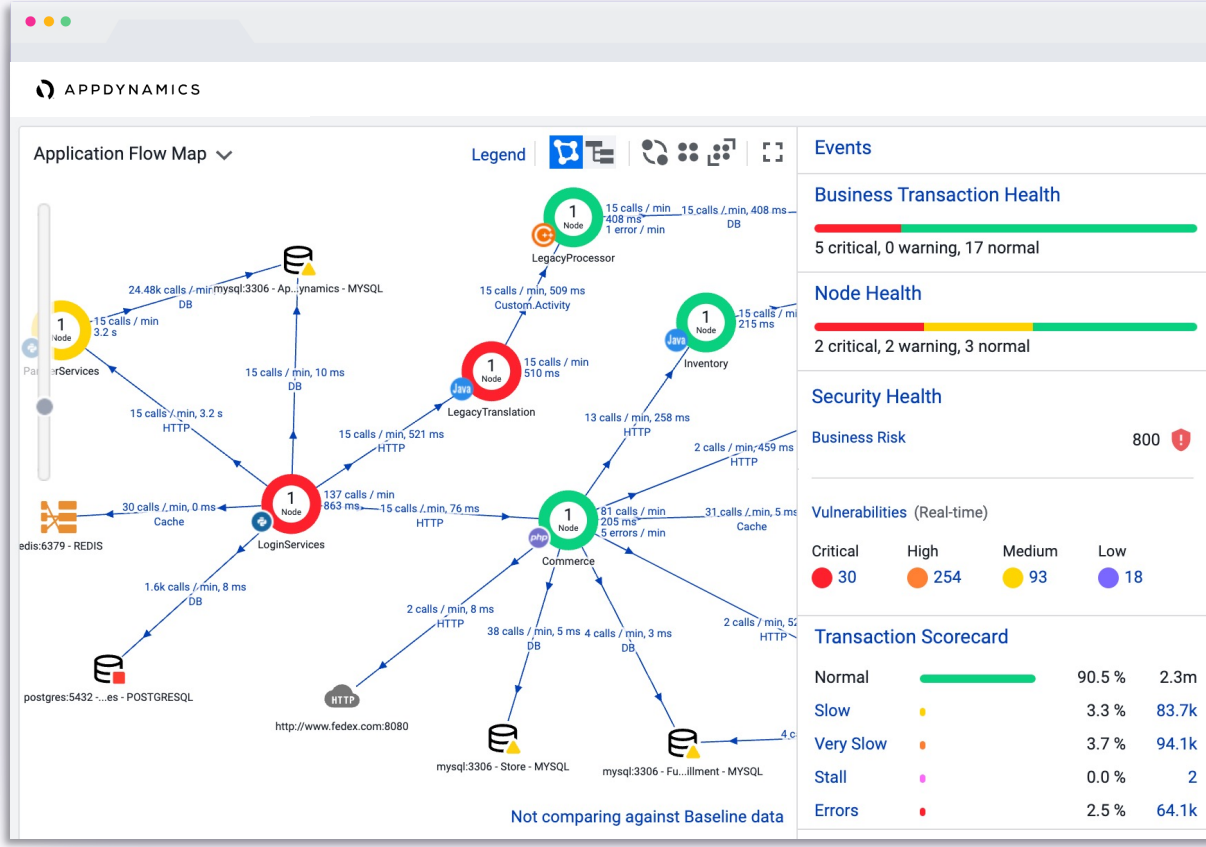
Real-time insights to app and business performance

Data Collection
Agents monitor performance of your code, runtime, and behavior

Auto-Discovery and Mapping
Map flow of all traffic across apps

Business Transaction Monitoring
Observe end-to-end critical user experiences across apps

Anomaly Detection and Root Cause Diagnostics
Automatically identify problems and track them to the source



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

End-to-end Tracing

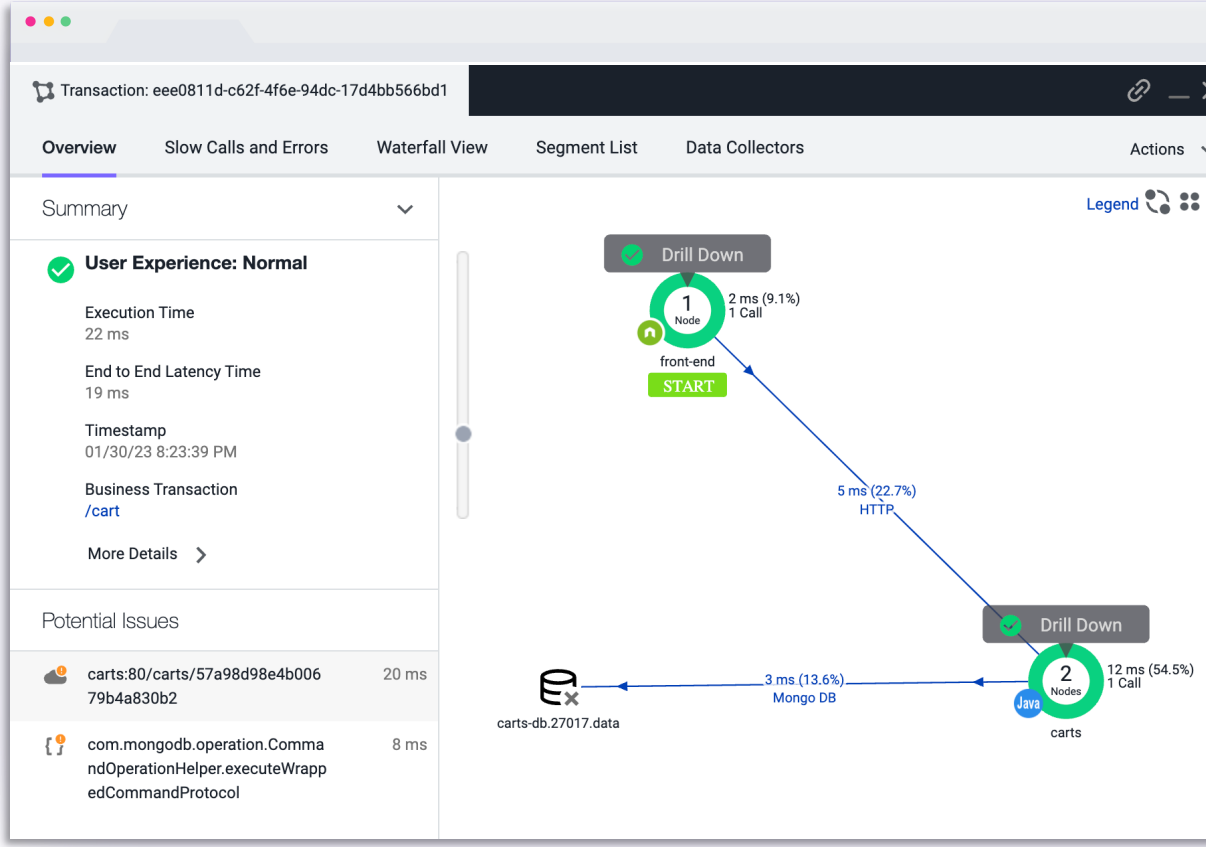
Complete view of an experience

Business-oriented observability
Measure what matters to your users and the business

Accurate reflection of performance
All dependencies considered when identifying problem spots

Capture business metrics
Enable analytics using the data within a transaction

Foundational to business insights
Measure business performance and risk



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

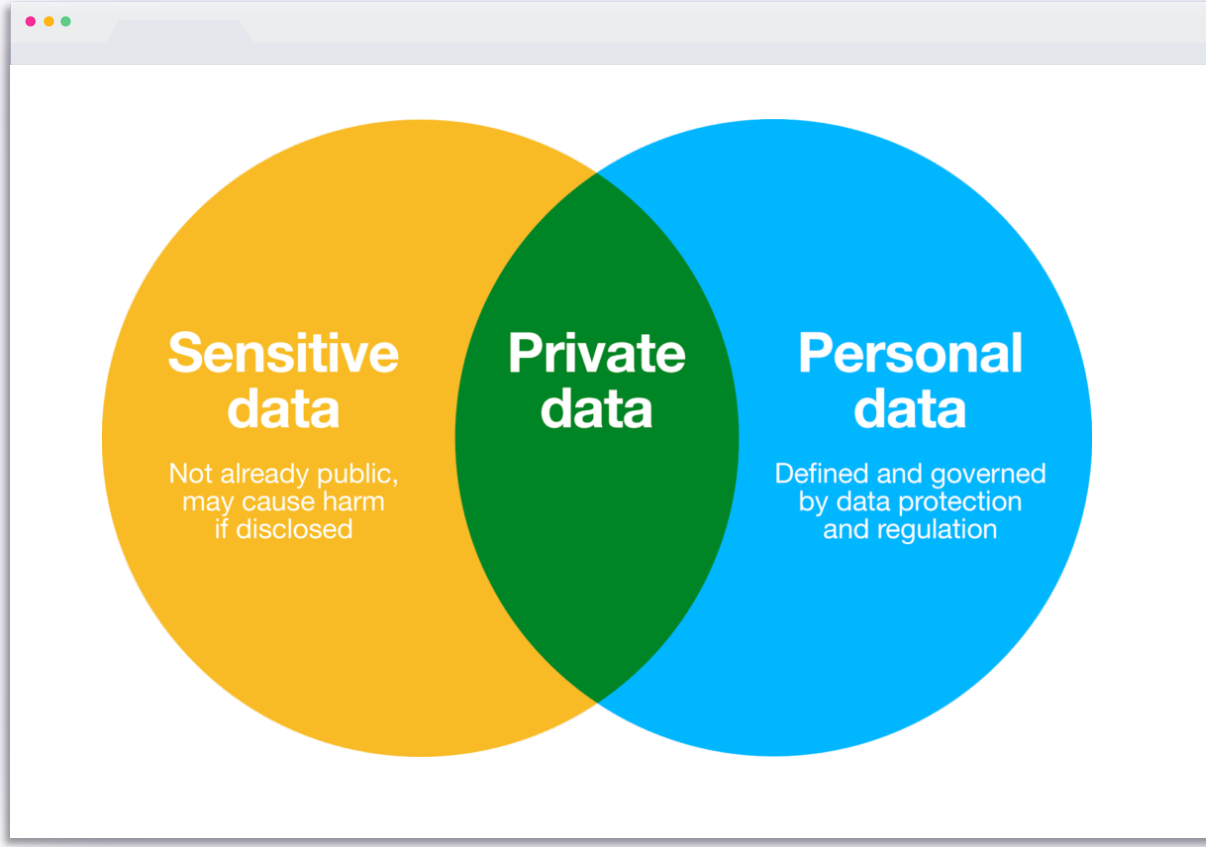
Data handling

Regulatory and ethical implications

Personal, Sensitive, Private
Classification is the first step to protect data

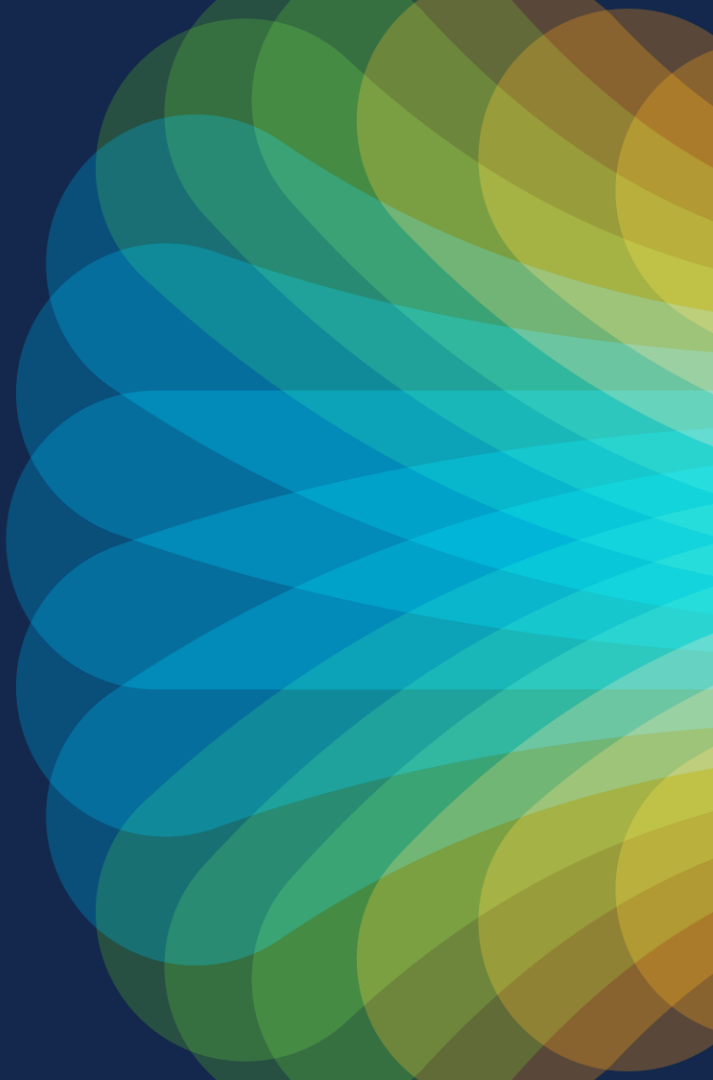
Data leakage
Unintentional data loss usually due to misconfiguration or unclean code

Data breach
Security incident that results in data loss



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

Application Security for Hybrid Applications

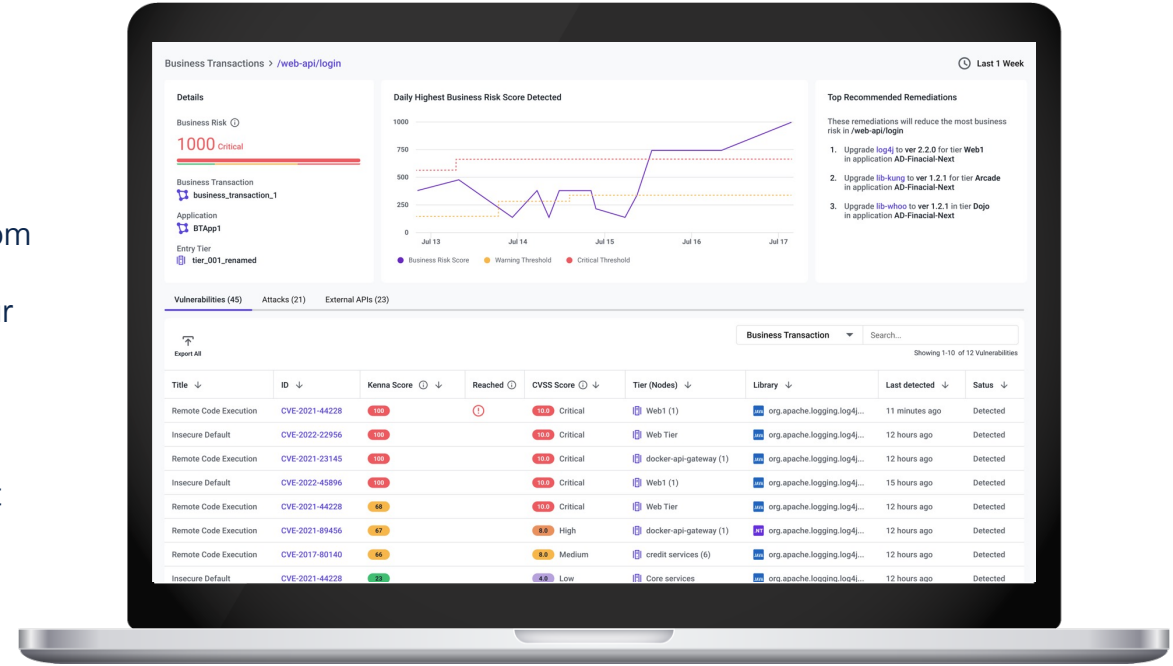


cisco Live!

Application security

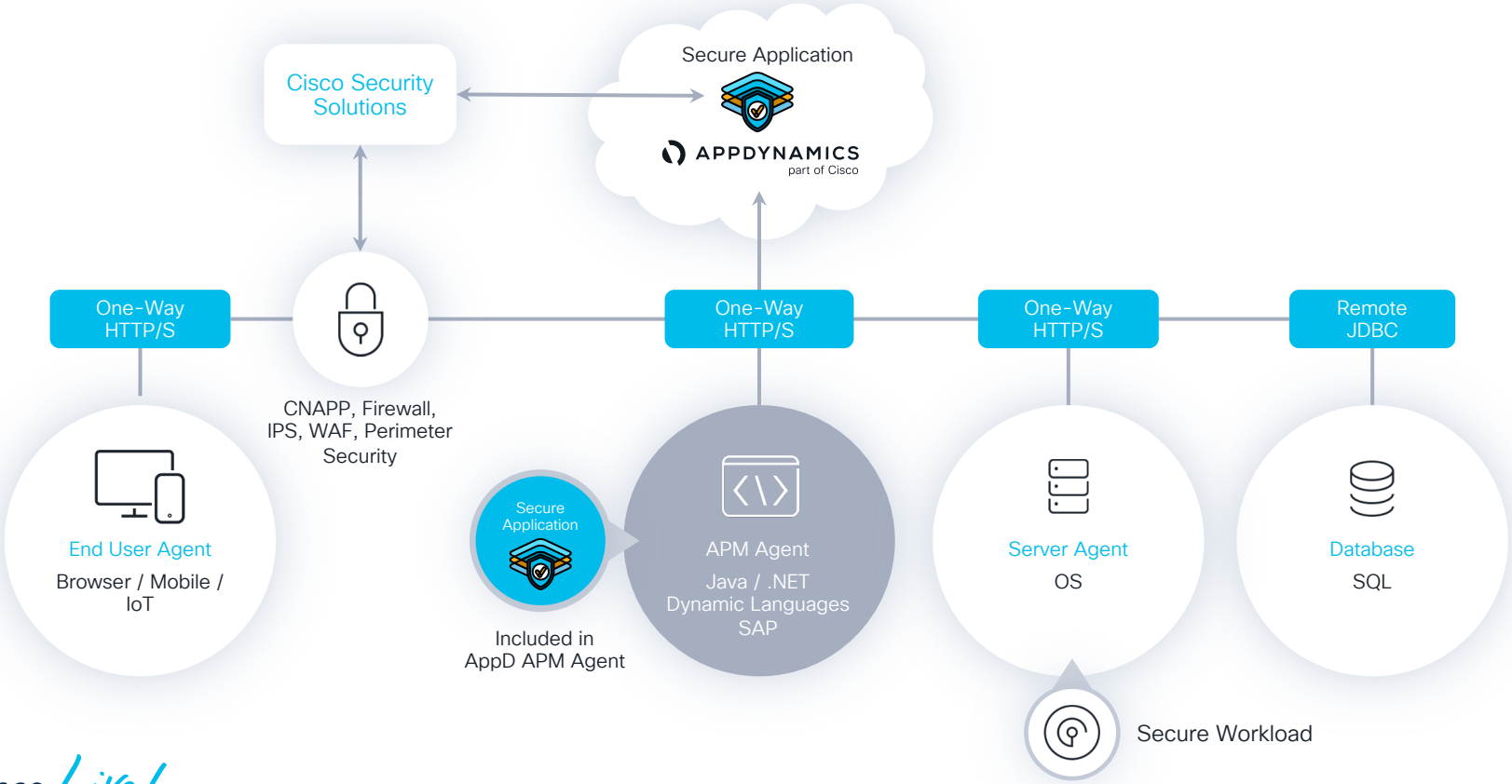
Business risk observability for hybrid application

- Locate how and where an attack occurs with business transaction mapping
- Leverage security intelligence from Cisco Talos, Kenna and Panoptica to quickly uncover your current security posture
- Combine threat and vulnerability intelligence with business impact and runtime behavior to provide a business risk score



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

AppDynamics Agent Architecture



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

Cisco Secure Application

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)

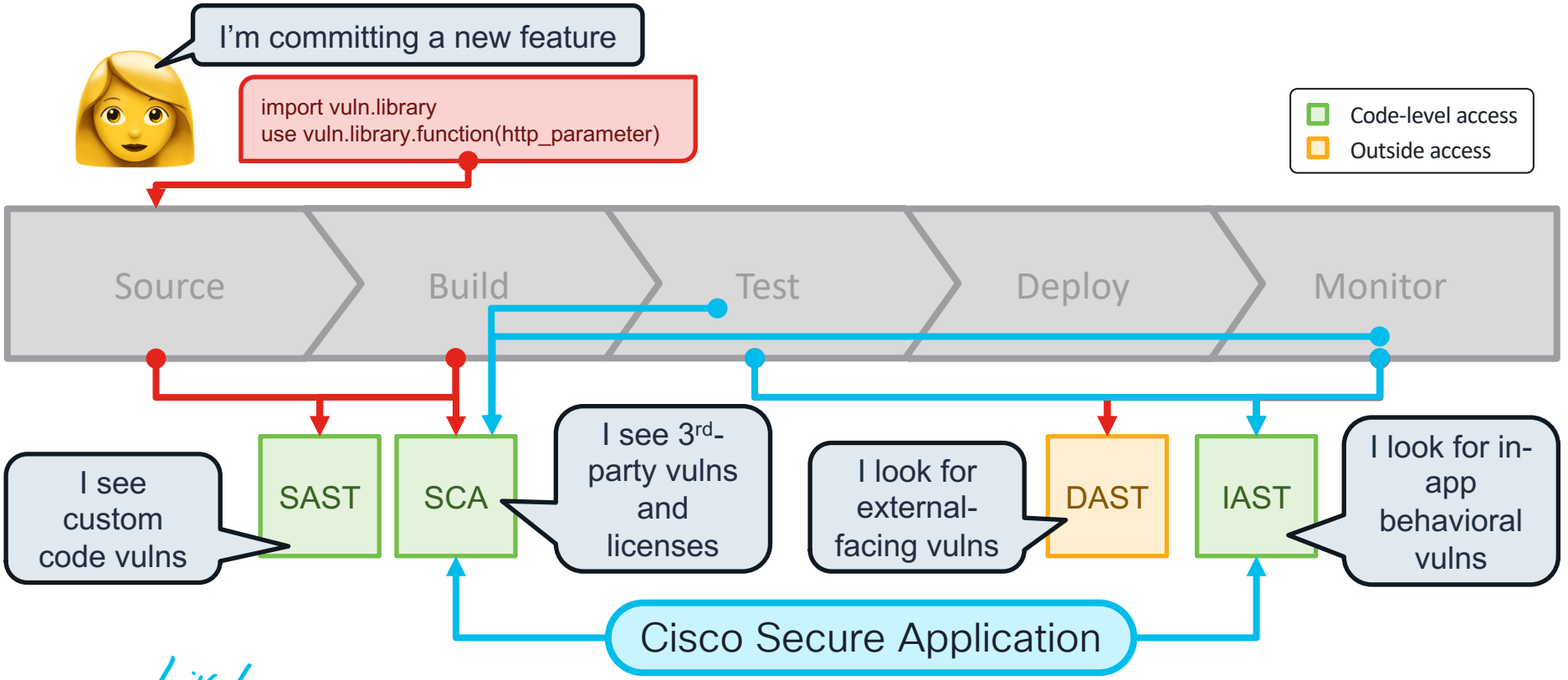
Block Attacks

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

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

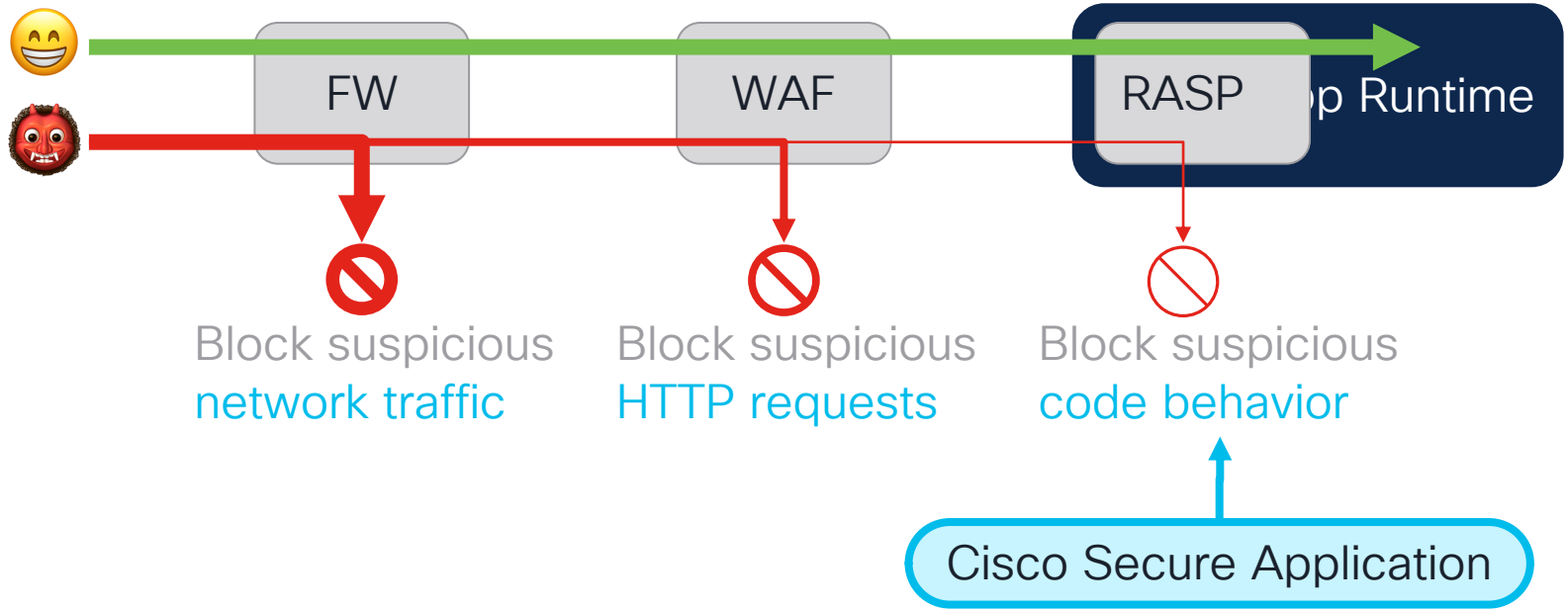
”But I’ve already got _____”

The role of application security testing in the pipeline



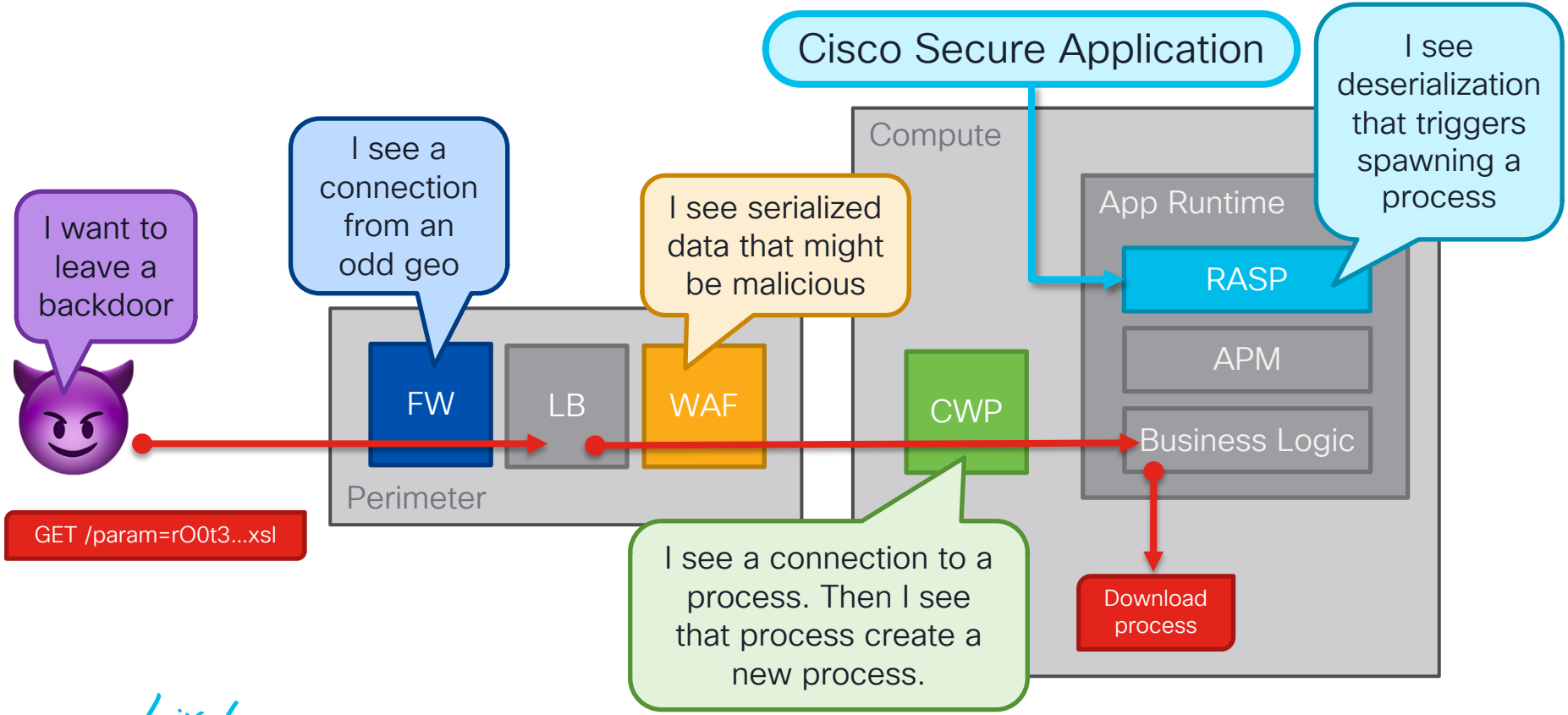
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Defense-in-depth reduces risk & load on the app



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

What an attack looks like to the runtime sec stack

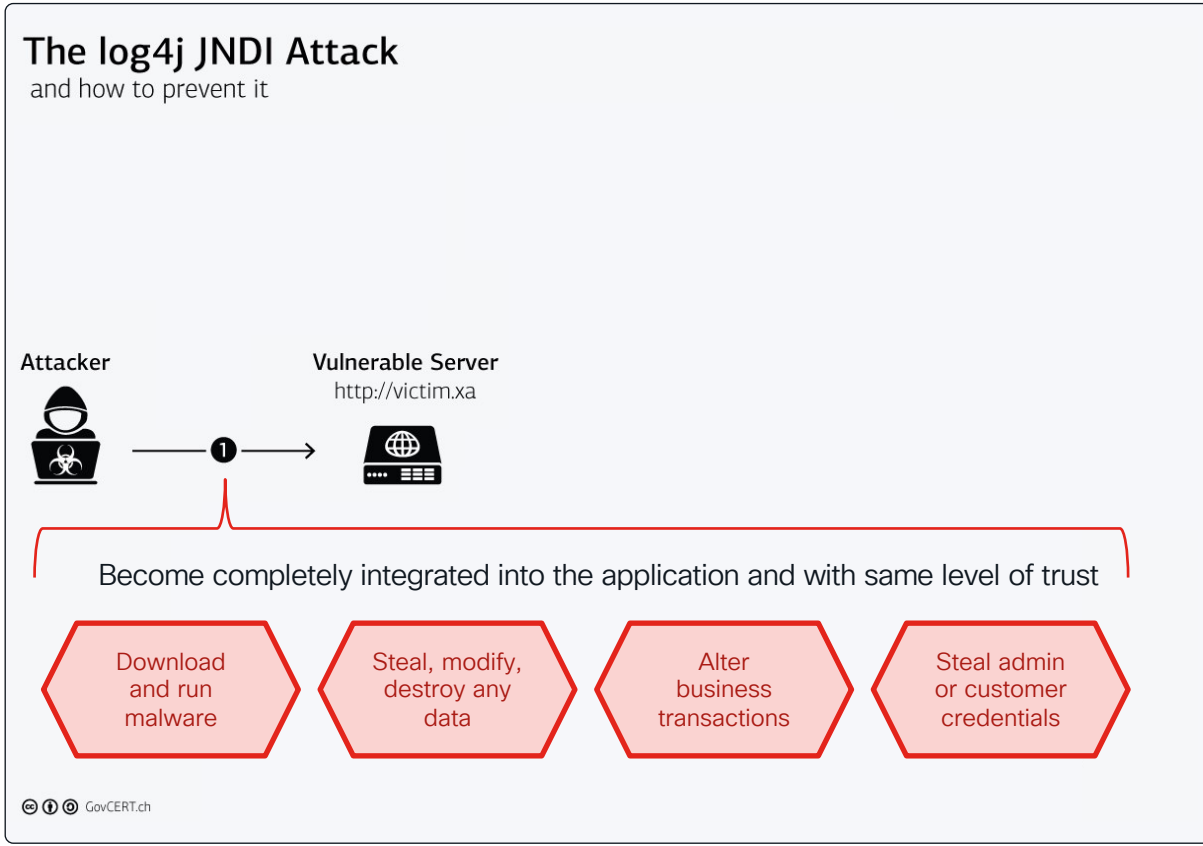


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Real-world usage

Log4shell Explained
(CVE-2021-44228)

Arbitrary code execution in Log4j, a popular Java logging framework

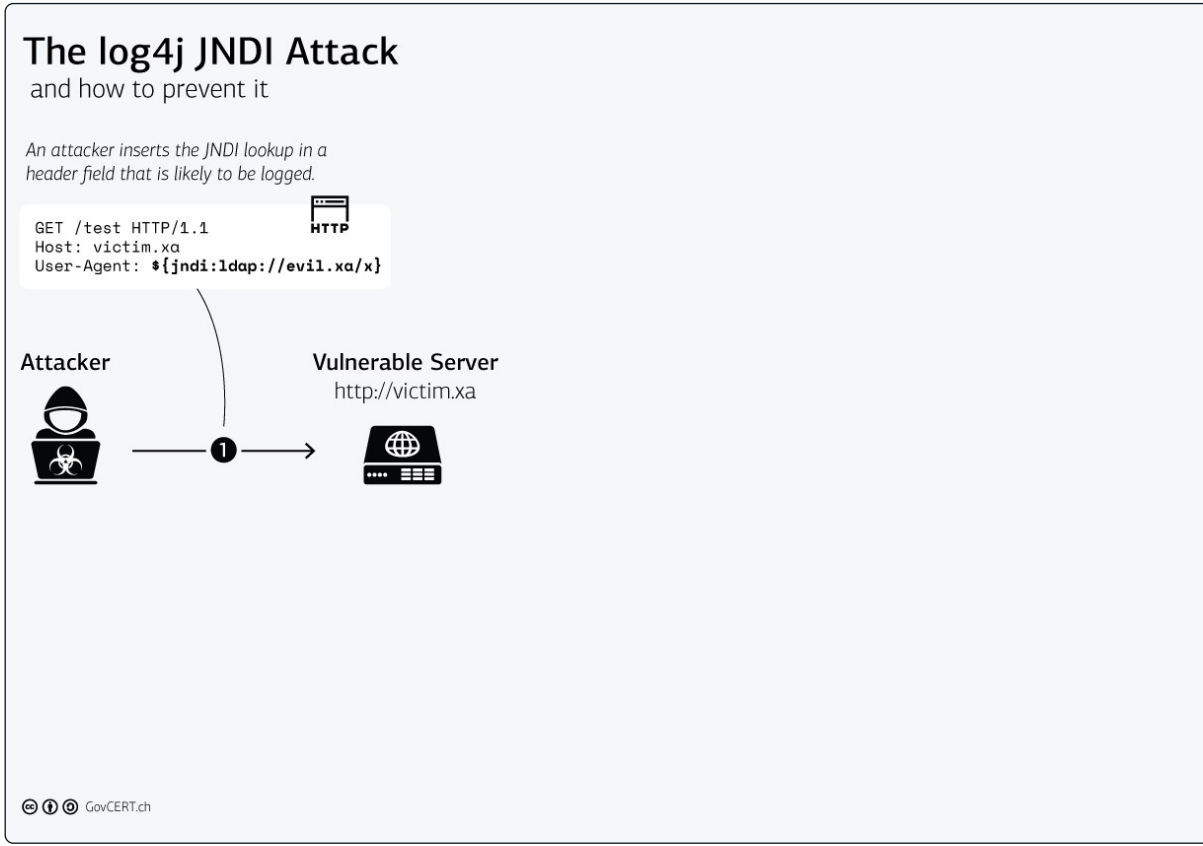


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Log4shell Explained
(CVE-2021-44228)

Arbitrary code execution in Log4j, a popular Java logging framework

Attacker delivers JNDI lookup string
Can be done remotely or locally



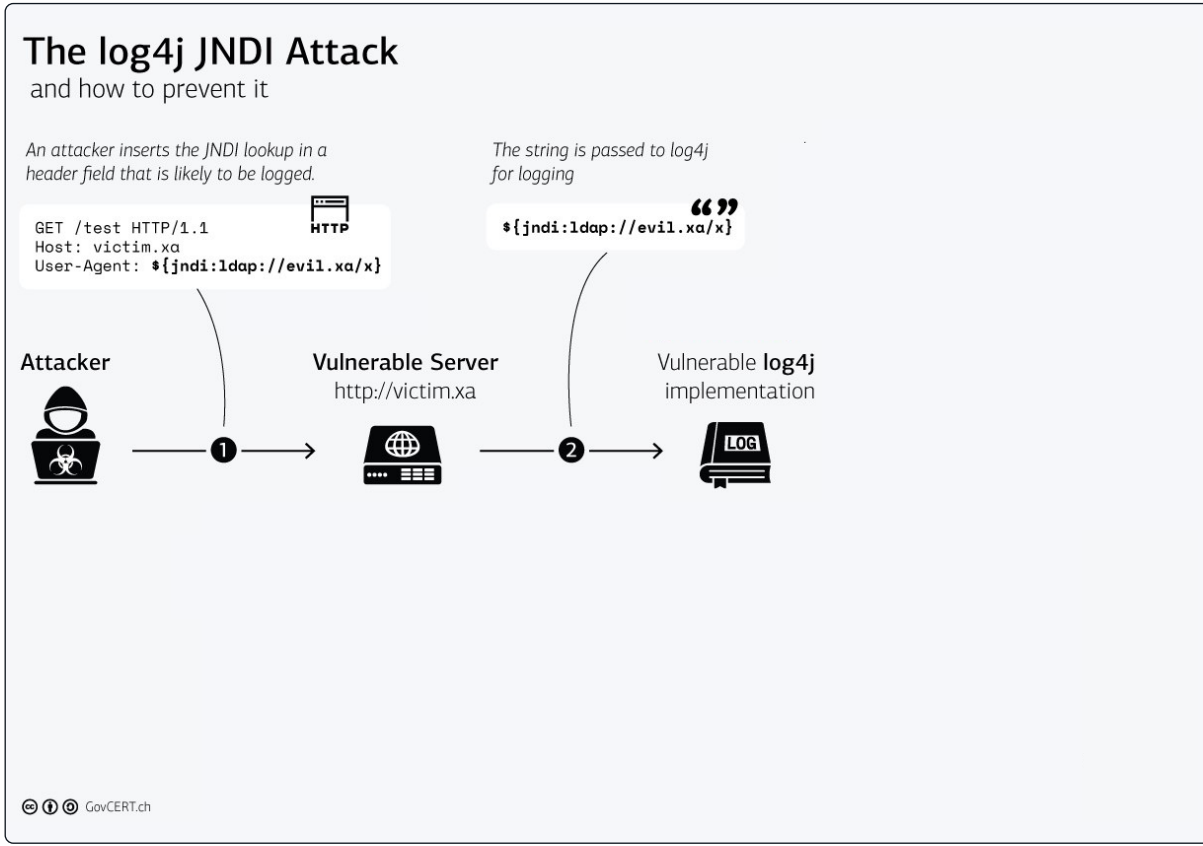
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Log4shell Explained (CVE-2021-44228)

Arbitrary code execution in Log4j, a popular Java logging framework

Attacker delivers JNDI lookup string
Can be done remotely or locally

String sent to log4j library
App must log the string



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

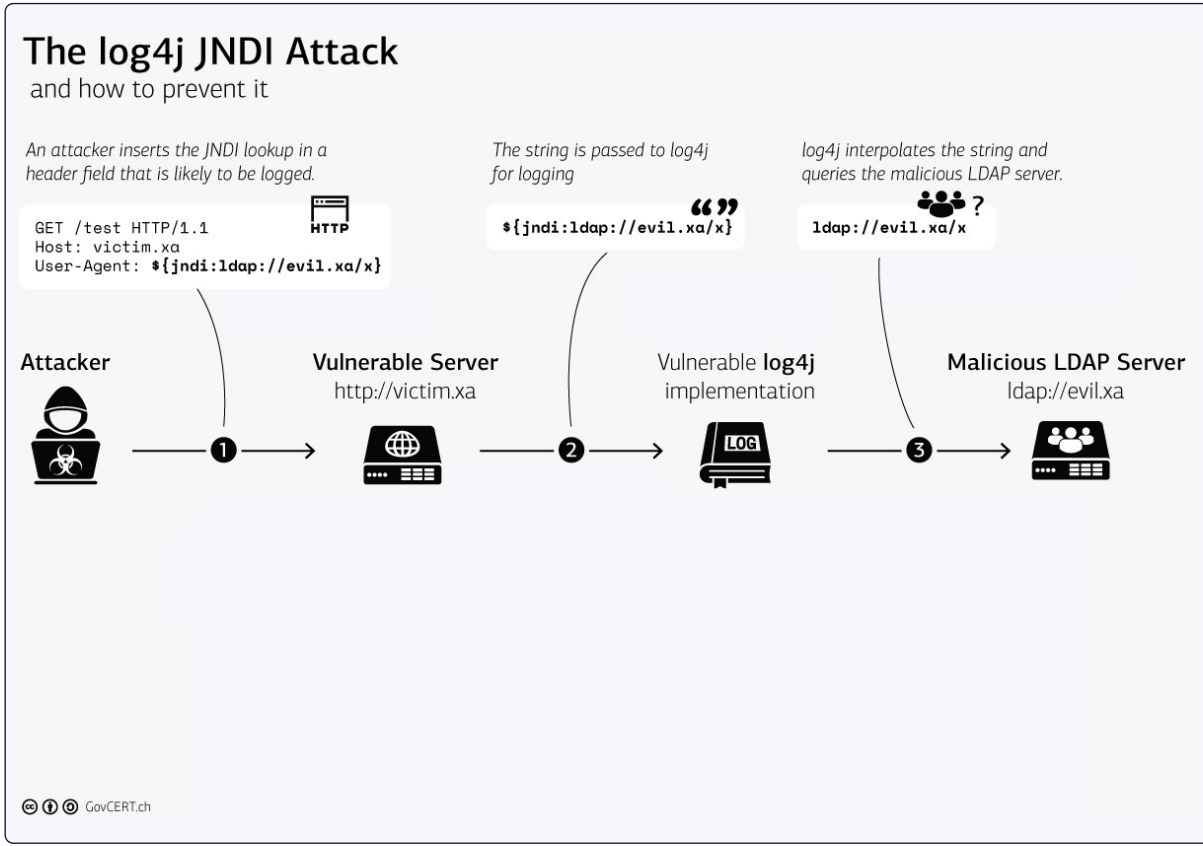
Log4shell Explained
(CVE-2021-44228)

Arbitrary code execution in Log4j, a popular Java logging framework

Attacker delivers JNDI lookup string
Can be done remotely or locally

String sent to log4j library
App must log the string

Log4j replaces string from a malicious server
App needs access to remote LDAP



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

Log4shell Explained
(CVE-2021-44228)

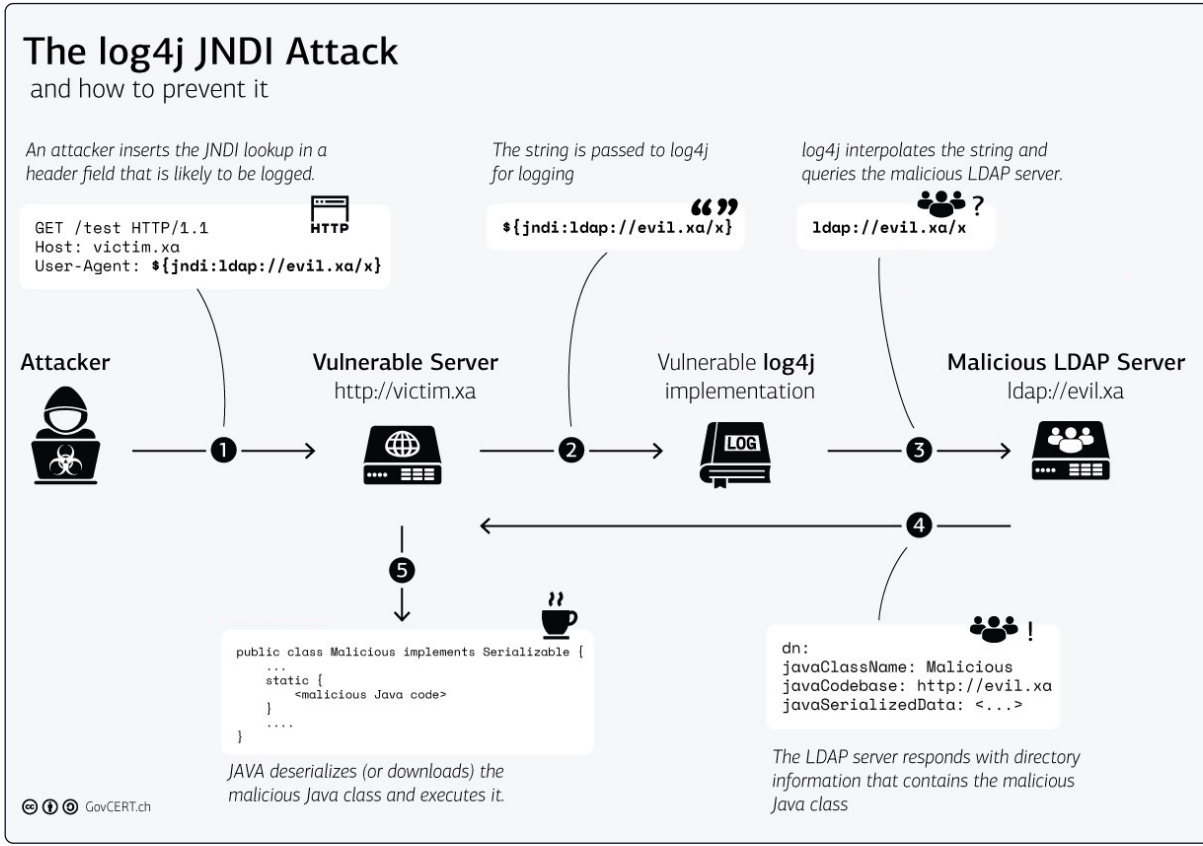
Arbitrary code execution in Log4j, a popular Java logging framework

Attacker delivers JNDI lookup string
Can be done remotely or locally

String sent to log4j library
App must log the string

Log4j replaces string from a malicious server
App needs access to remote LDAP

Server provides malicious code
Gives complete control of the application and access to host OS



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

Log4shell Explained
(CVE-2021-44228)

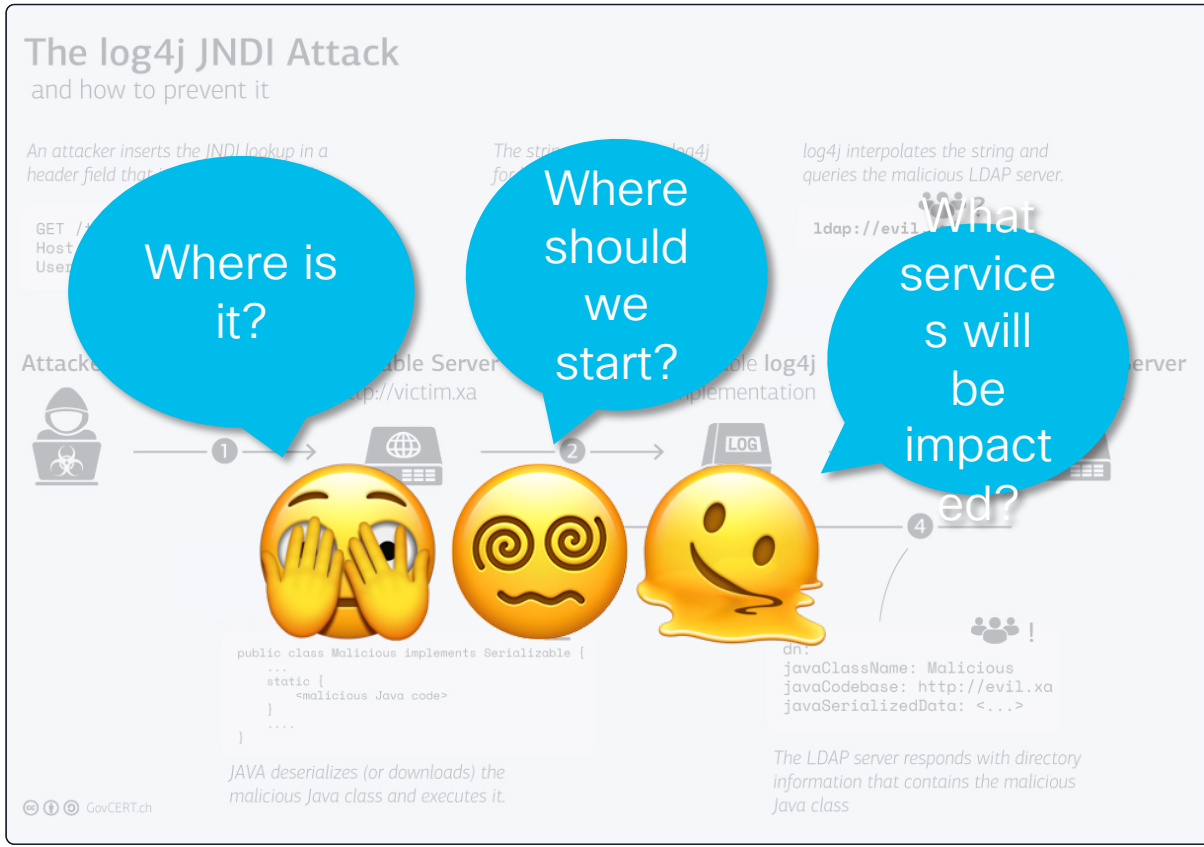
Arbitrary code execution in Log4j, a popular Java logging framework

Attacker delivers JNDI lookup string
Can be done remotely or locally

String sent to log4j library
App must log the string

Log4j replaces string from a malicious server
App needs access to remote LDAP

Server provides malicious code
Gives complete control of the application and access to host OS



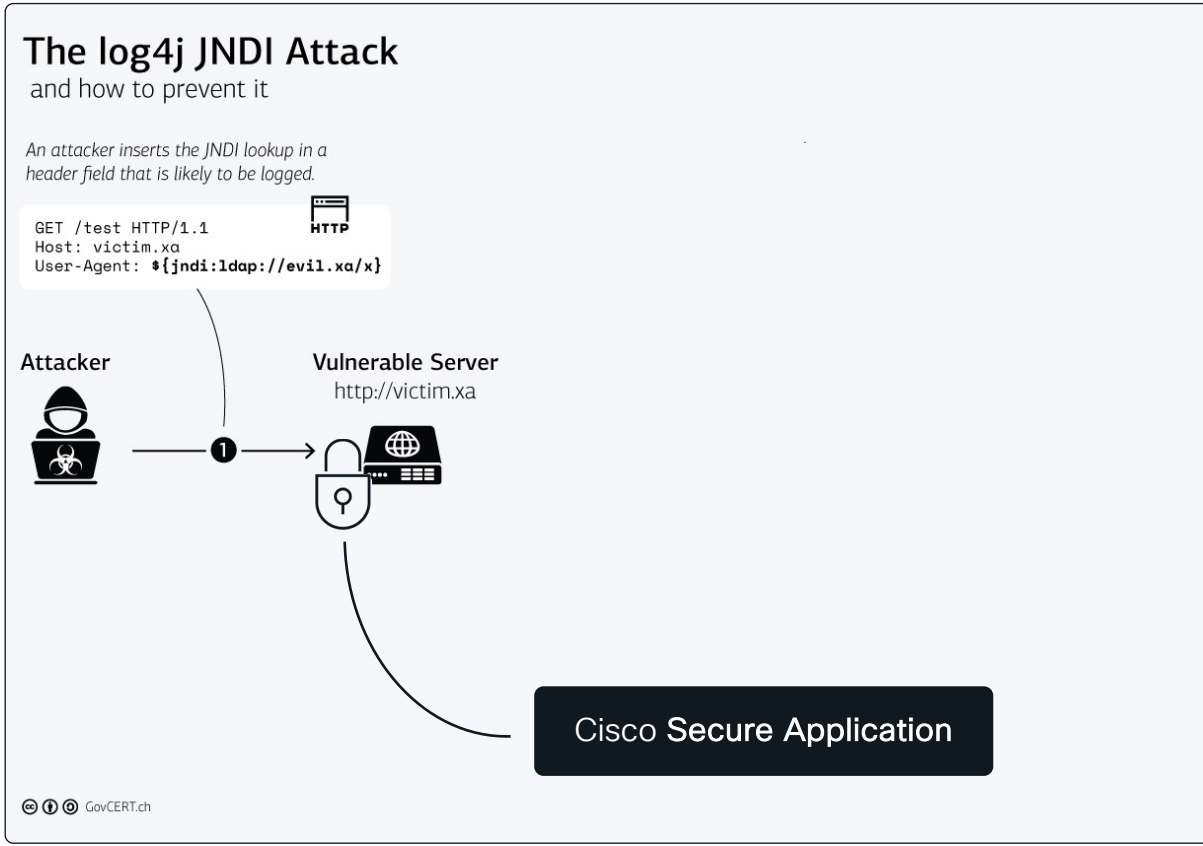
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Application Protects Against Log4Shell

Identify the risk and protect against exploits

Instrument apps with no code changes

Utilize existing workflow of dev and ops



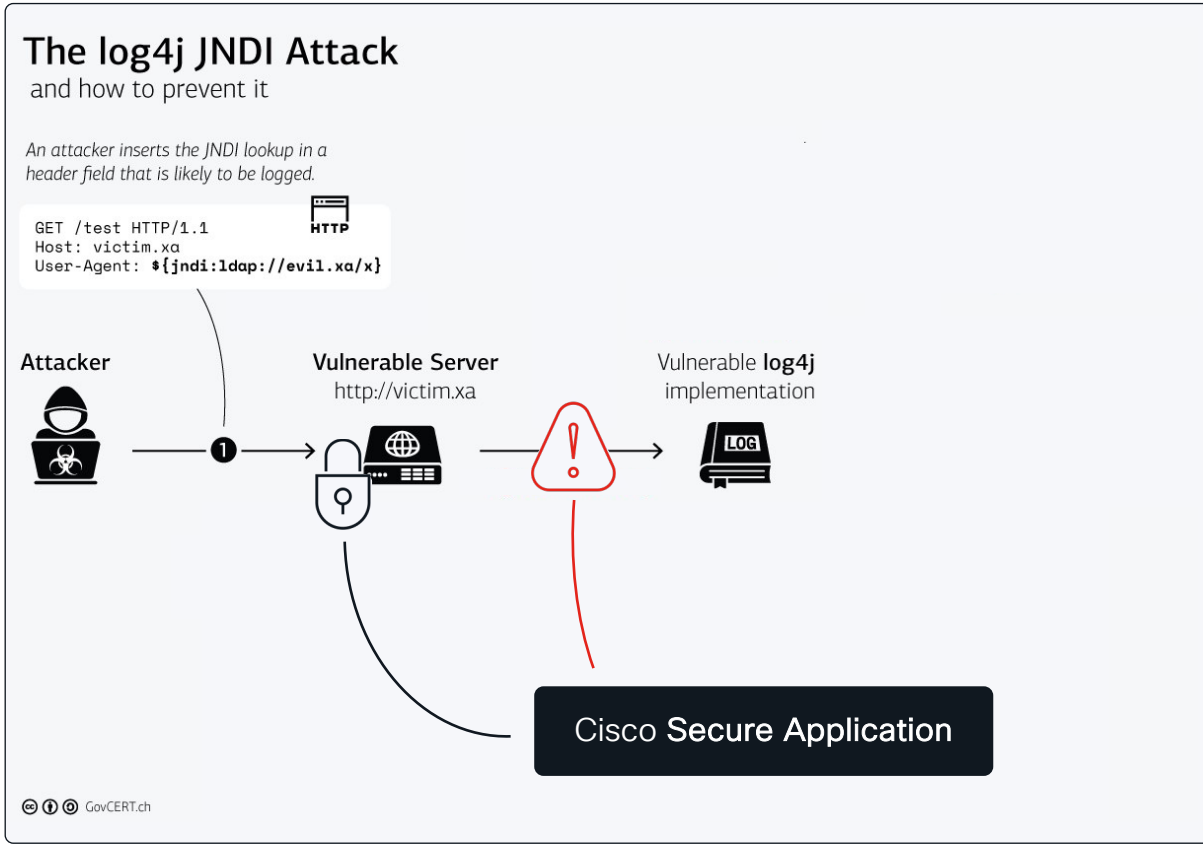
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Secure Application Protects Against Log4Shell

Identify the risk and protect against exploits

Instrument apps with no code changes
Utilize existing workflow of dev and ops

Detect vuln library usage in Business Transactions
Identify if the library is loaded and vuln code is reachable



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

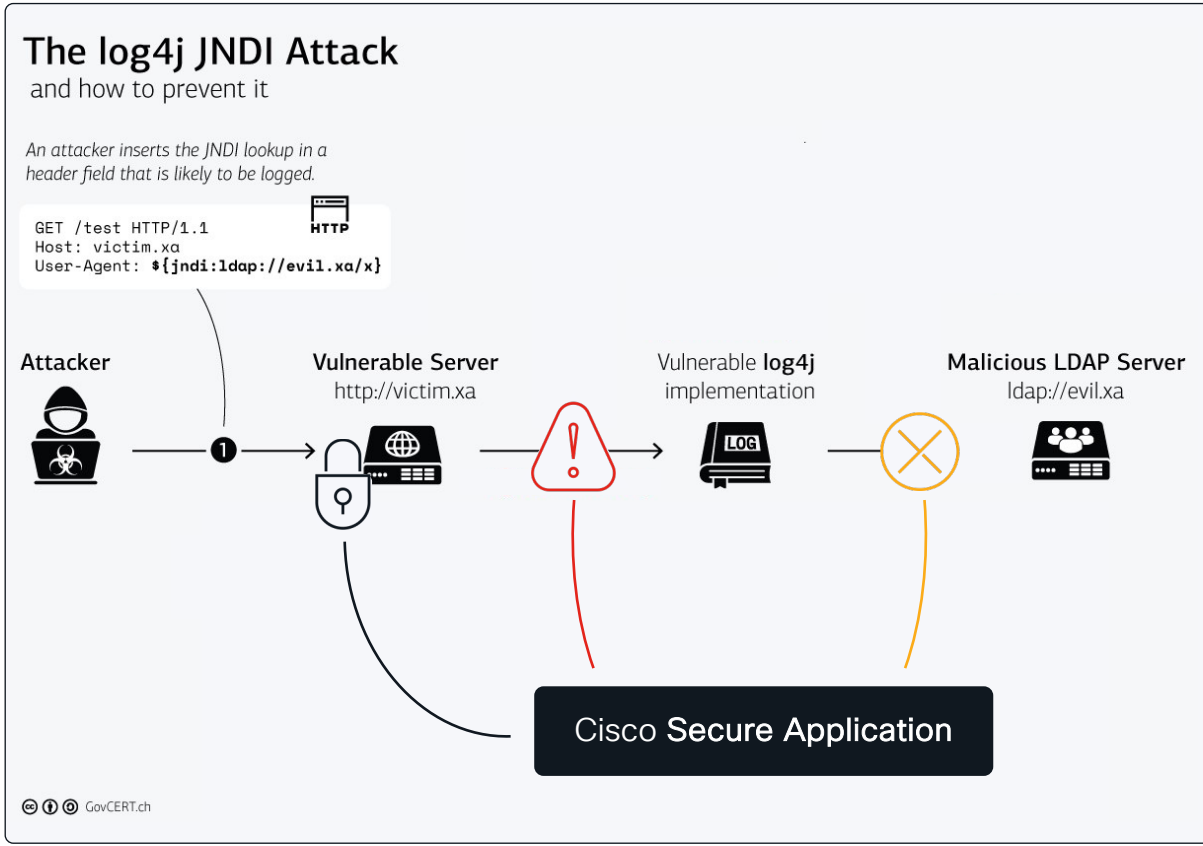
Secure Application Protects Against Log4Shell

Identify the risk and protect against exploits

Instrument apps with no code changes
Utilize existing workflow of dev and ops

Detect vuln library usage in Business Transactions
Identify if the library is loaded and vuln code is reachable

Block network access
Stop LDAP lookup for JNDI vuln code



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

Secure Application Protects Against Log4Shell

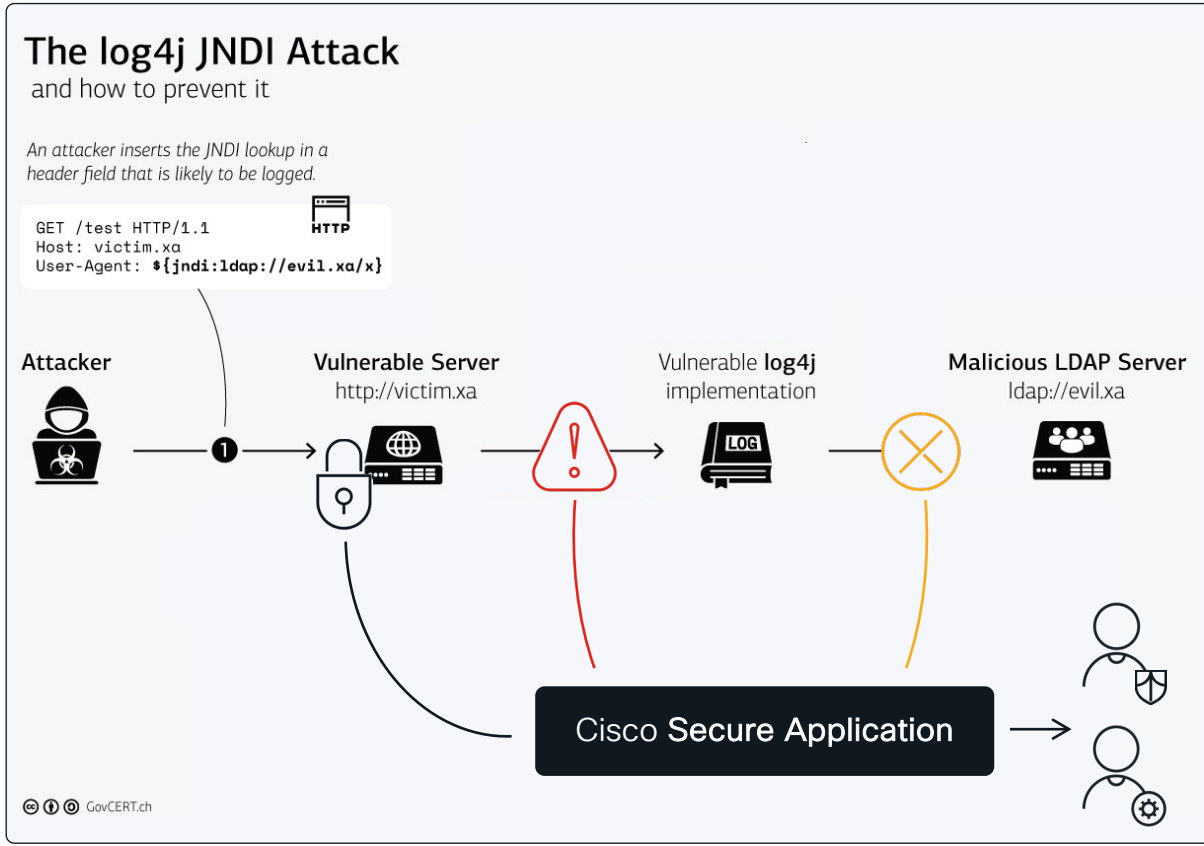
Identify the risk and protect against exploits

Instrument apps with no code changes
Utilize existing workflow of dev and ops

Detect vuln library usage in Business Transactions
Identify if the library is loaded and vuln code is reachable

Block network access
Stop LDAP lookup for JNDI vuln code

Alert sec and app teams
Insights provided with app and biz context



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

Dive into the details

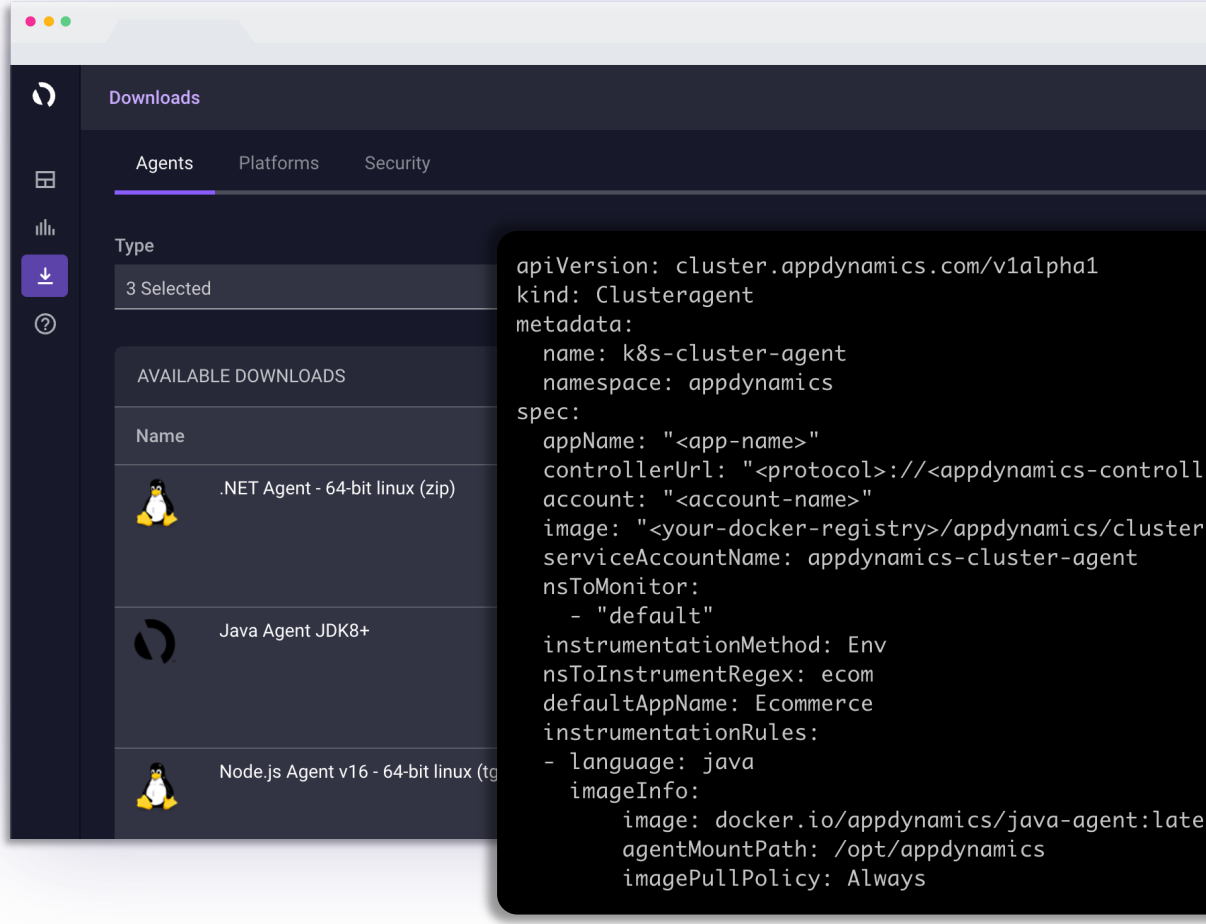
Supported Runtimes

Security integrated into our existing APM agents

Auto-instrument services
VMs and containers in Kubernetes

Vulnerable library detection
Java, .NET, Node.js

Attack detection and runtime protections
Java, .NET



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

Built with a performance mindset

Java and .NET

Disk

< 4MB install
< 15MB daily

Memory

< 4-6MB heap

CPU

< 1%
< 5% spikes

Latency

< 4-6ms per transaction
< 10ms spikes

Instrumentation

12 – 30 classes

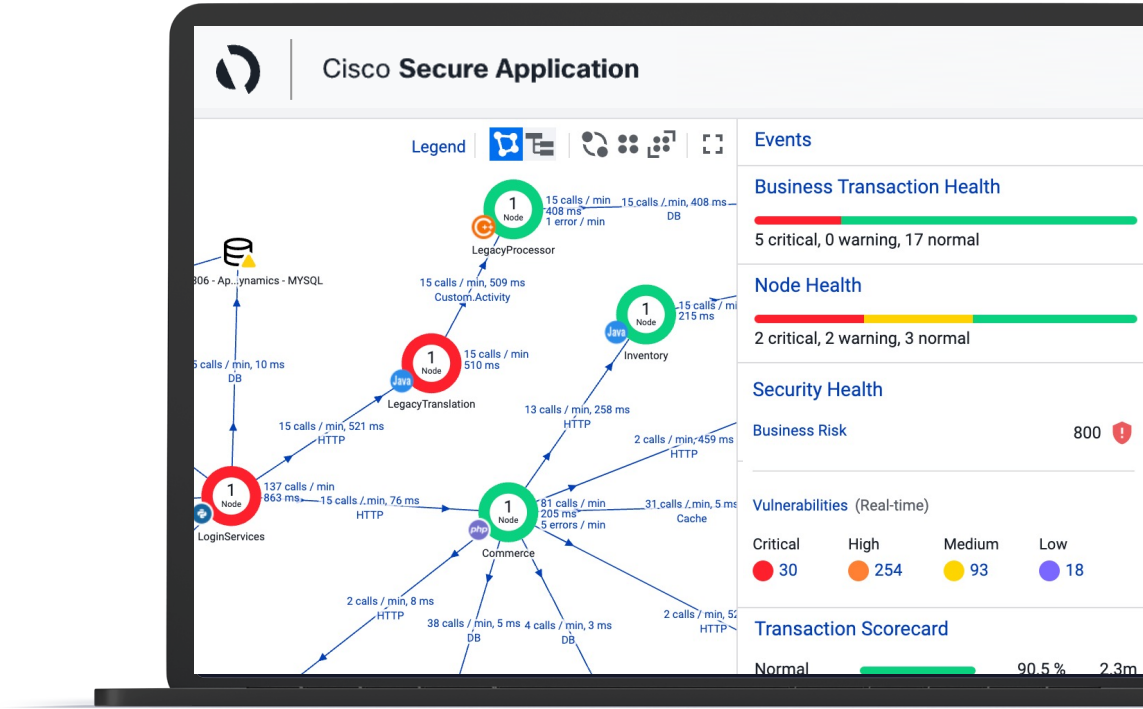
Vulnerable library detection Node.js has negligible resource utilization

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

Correlate findings to Business Transactions

Give deeper context to guide prioritization

- Automatically detect vulnerabilities and threats using existing AppDynamics agents
- Correlate findings to application entities and transactions
- Block attacks with code-level policy
- Business context locates risk within critical transactions



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

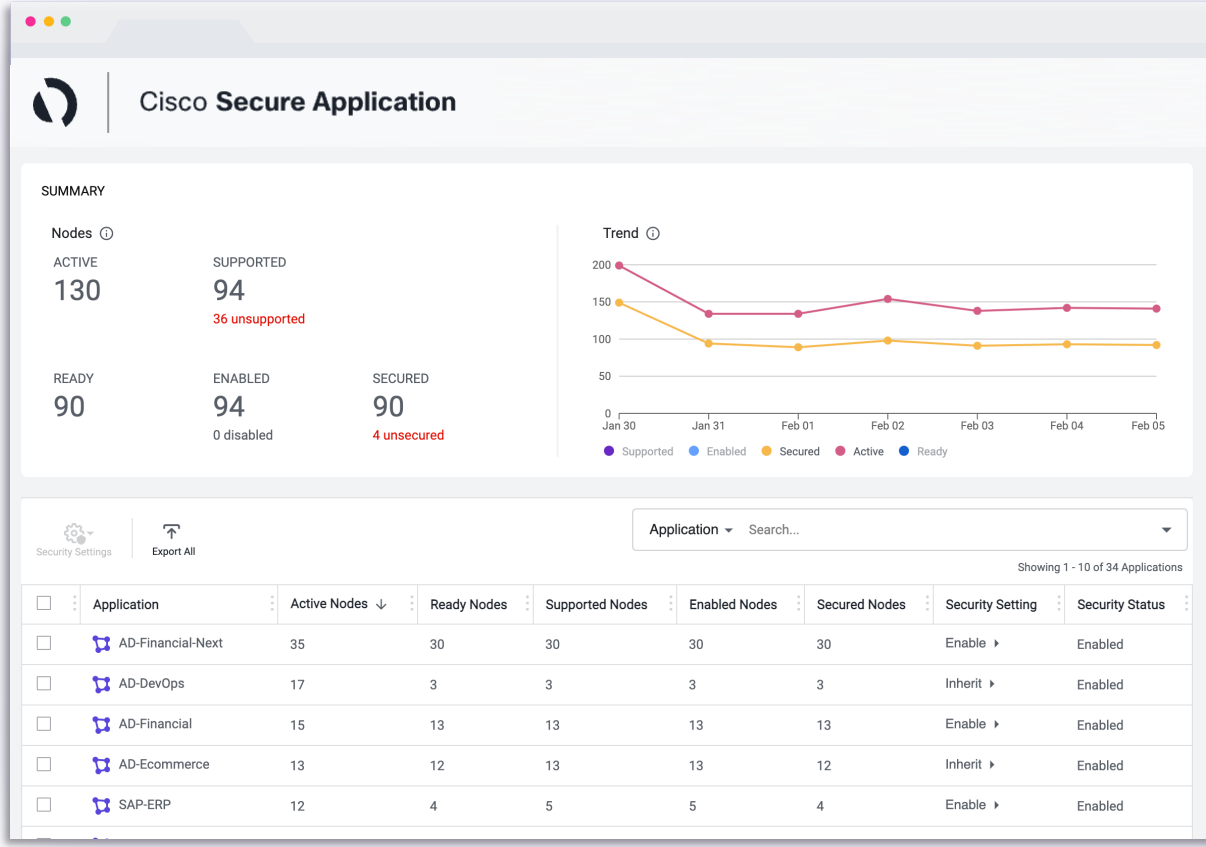
Seamless Onboarding

Get insights within minutes

No configuration required
Just enable security and your presented with valuable data

Flexible controls
Be precise or press the easy button

Diagnostics
Ensure your roll-out is moving smoothly and identify onboarding problems



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

Cisco Security integrations

Extended detection and response to boost productivity

Use Kenna, Talos, and Panoptica Intel

Native integration to get detailed vuln insights, identify bad actors, and expose 3rd-party API security issues

Hunt for threats in SecureX

Give a more complete picture of an incident

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

Identify Open-Source Risk

Know what third-party code your apps are using

Libraries usage

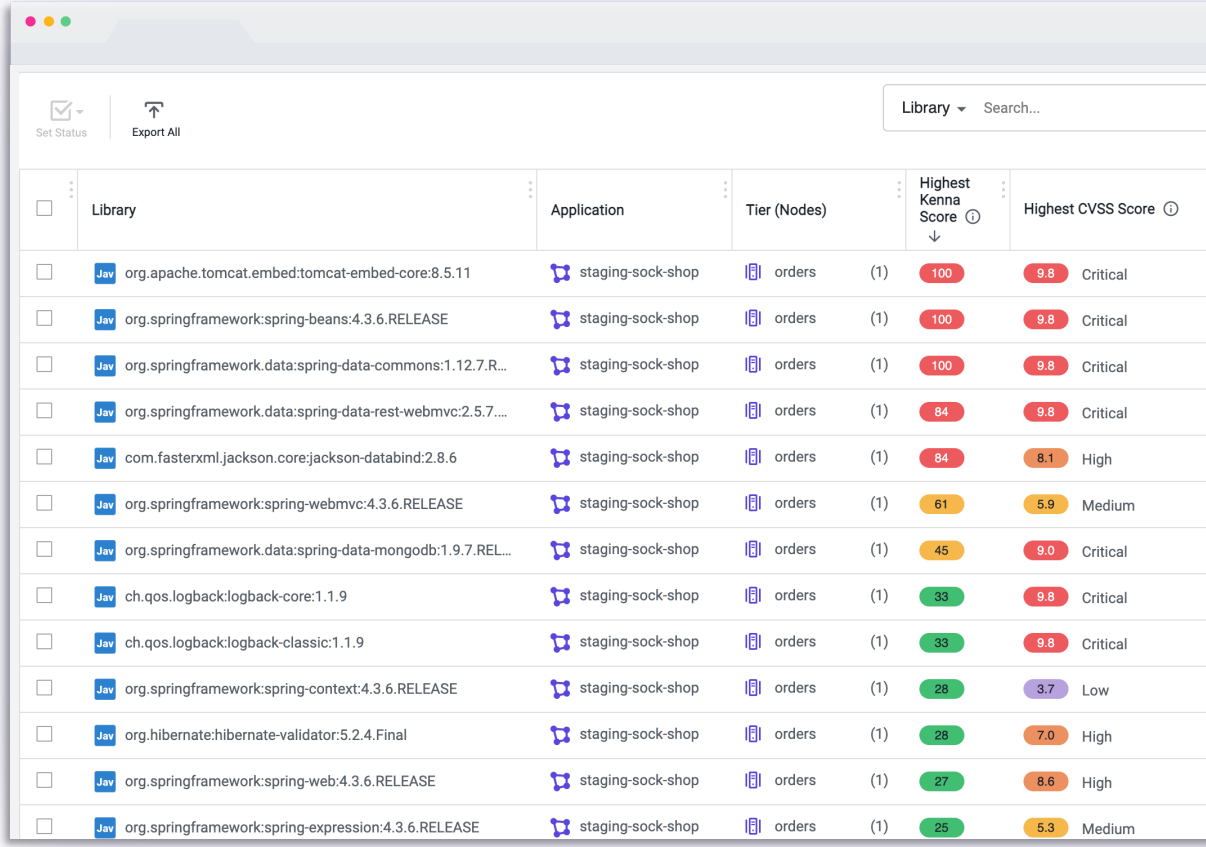
See anytime a library is loaded by your apps

Constant monitoring

Know where vulnerabilities are right after they're disclosed

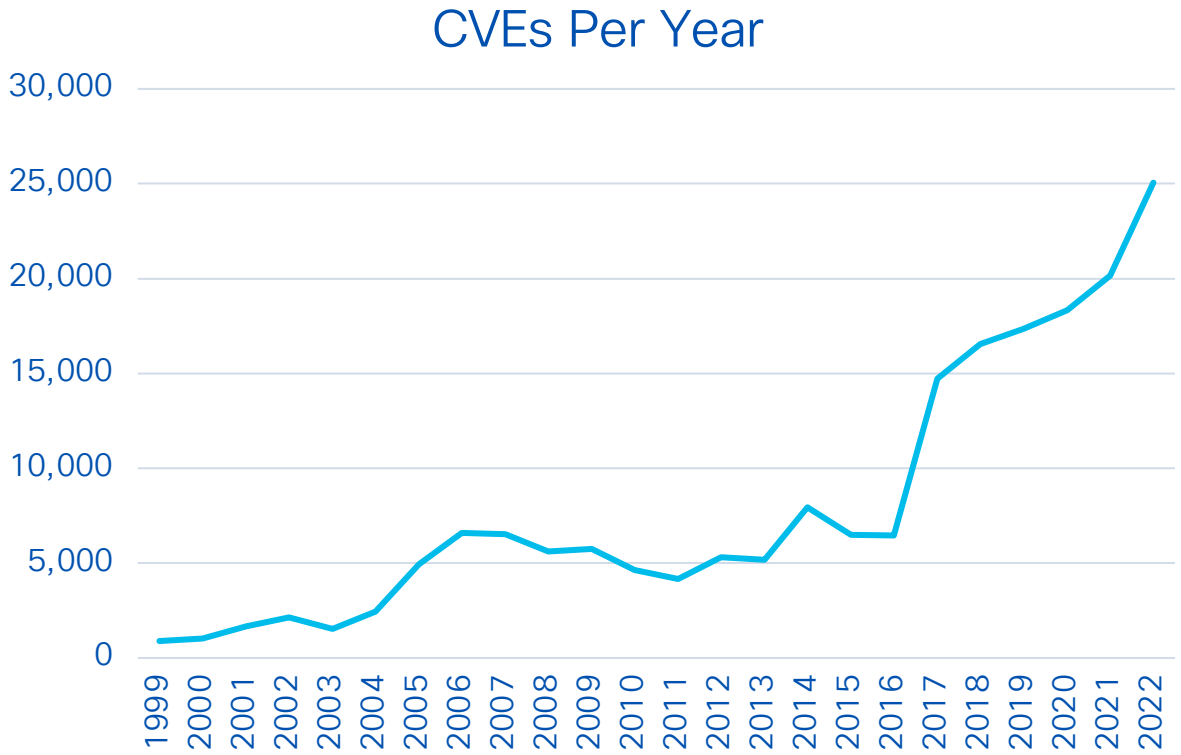
Remediation guidance

Get fixes out quicker tailored to your environment



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

Rate of Vulnerability Disclosure



CVEs from NVD
190,359

Average CVEs Published Per Day
68

2022
25,059
24% Y/Y

2023 Q1
17% Q/Q

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

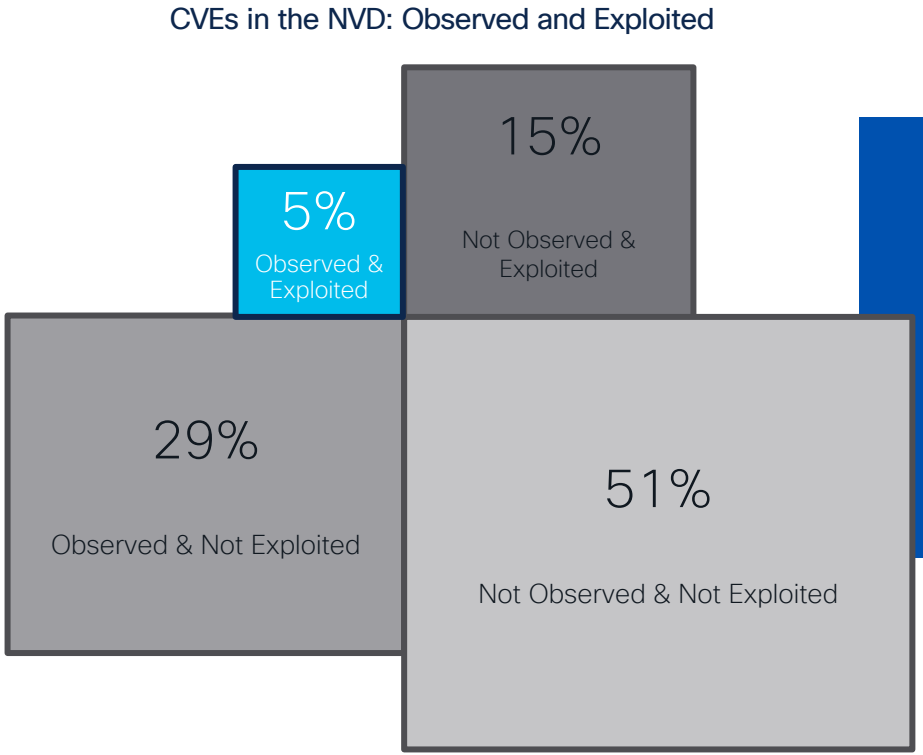
Our research shows us that...

- There were an average of 68 new software vulnerabilities published every day in 2022
- 95% of IT assets have at least one highly exploitable vulnerability.
- Organizations are remediating around 1 in 10 vulnerabilities in any month.
- Twitter mentions to prioritize software fixes are 2X as effective at reducing organizational exploitation as CVSS.

Source: Prioritization to Prediction, Volume 8, The Cyentia Institute & Kenna Security

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

Which vulnerabilities are truly risky?



Roughly 5% of CVEs in the NVD are *observed* in enterprises and *exploited* in the wild.

These are the ones you want to prioritize for remediation.

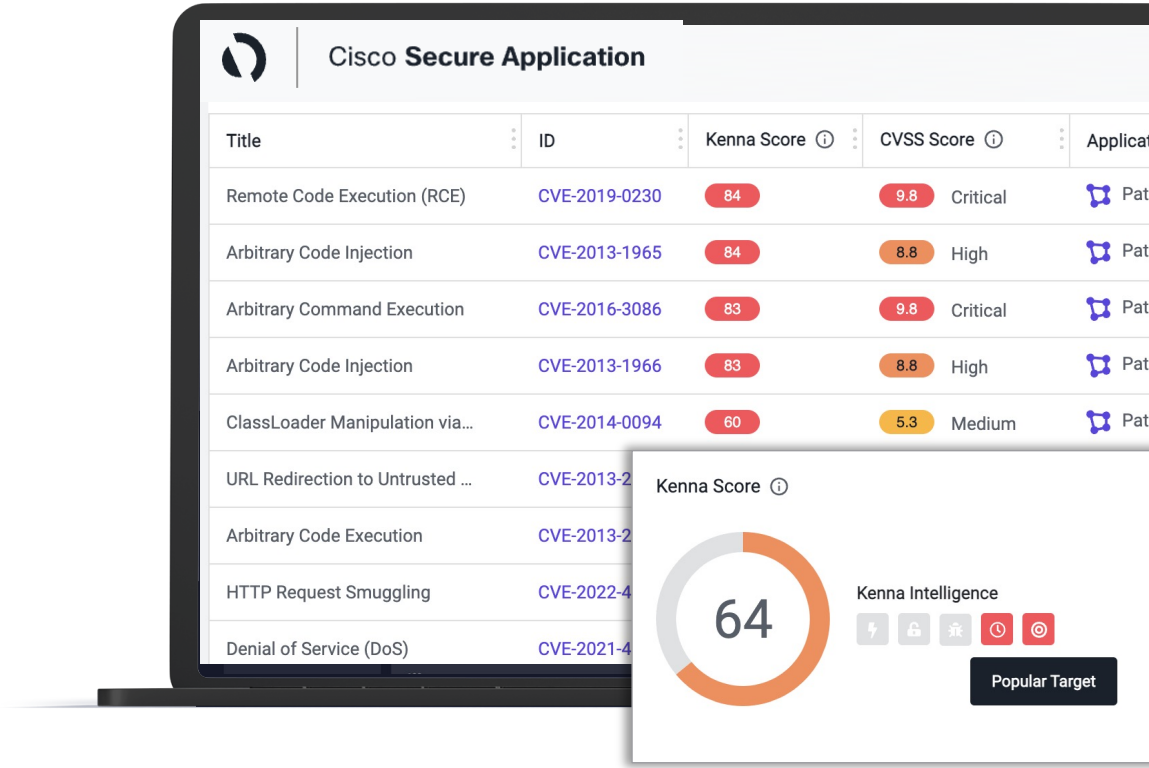
Source: Prioritization to Prediction, Volume 5, Kenna Security & The Cyentia Institute

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

Determine likelihood of exploit with 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



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

Cisco Kenna cuts through the noise

Kenna looks at various categories of vulnerability data to understand what happens to a CVE during all stages of its life, from the assignment of a CVE to the unlikely event of an exploitation in the wild.

Volume & velocity data is different than a "Yes/No" data point. It tells you: *In the past 24 hours, 7240 machines have been exploited using a CVE.*

Data Categories

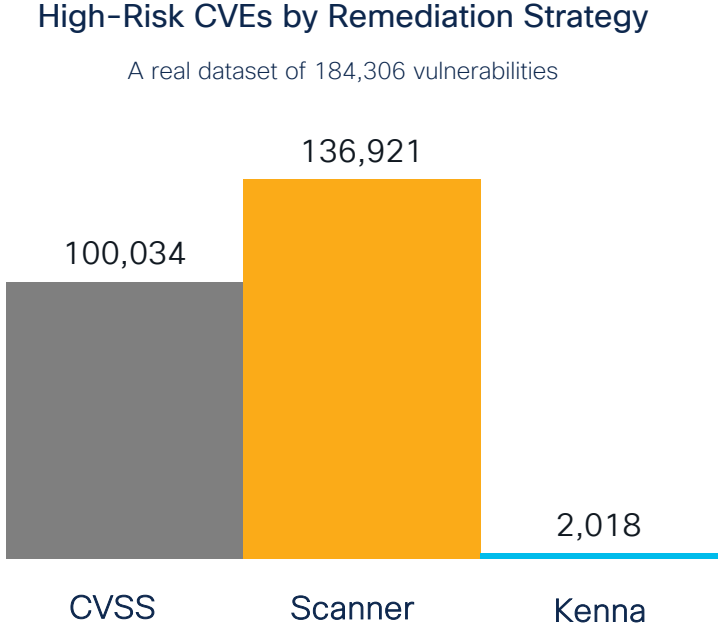
MITRE & NVD Vulnerability Scoring Early Warning Chatter	Exploit Databases Malware Analysis	Threat Actors Malware Families	Volume & Velocity of Exploitation in the Wild

Kenna Machine Learning Model-Based Risk Scoring

This incorporates the prediction of exploitation publication and exploitation event (94% accuracy)

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

High-risk remediation strategies



1.09% of these CVEs are considered high-risk by Kenna

- ✓ 134,903 fewer vulnerabilities to remediate compared to the scanner
- ✓ 98,016 fewer vulnerabilities to remediate compared to CVSS

Missed high-risk vulns

111 CVEs found high by Kenna but not found high by scanner

51 CVEs found high by Kenna but not found high by CVSS

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

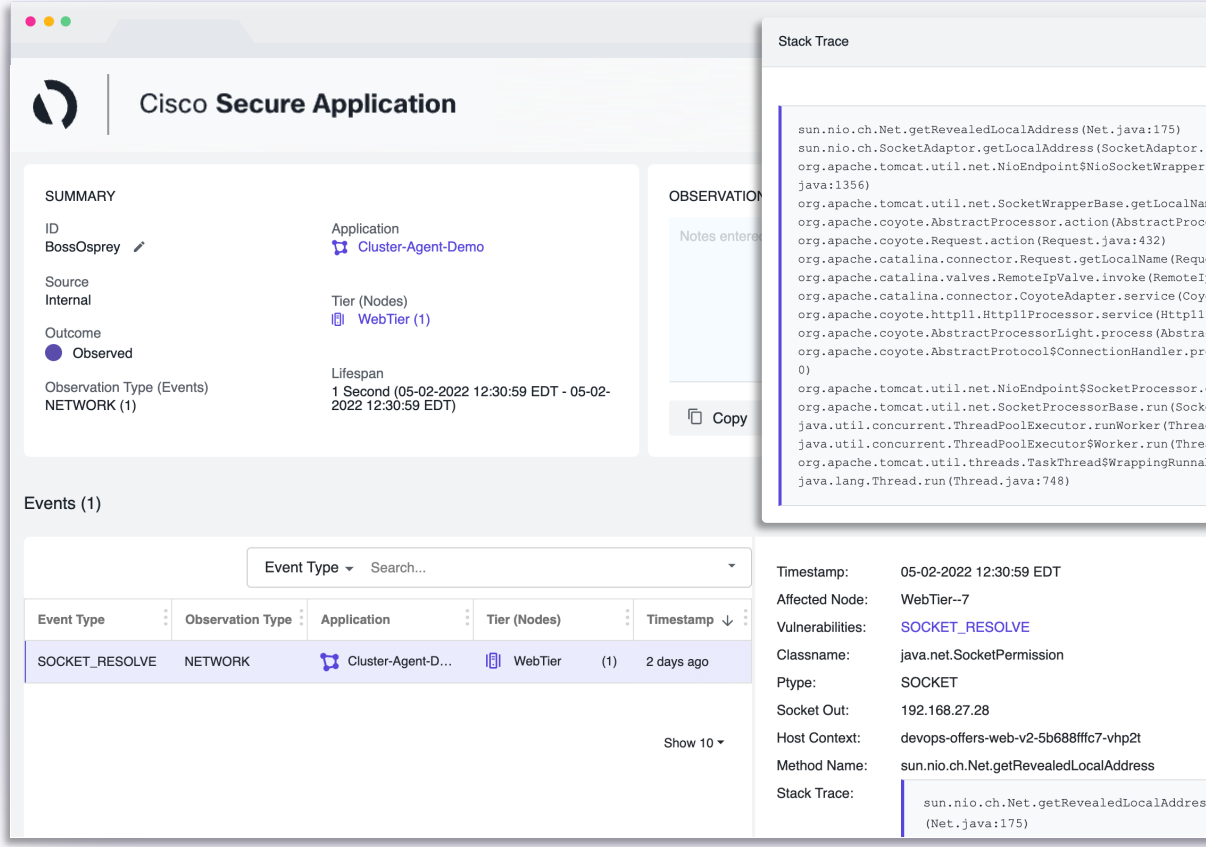
Runtime Monitoring

Observe access to resources and critical behaviors

Automatically instrumented
Nothing to configure for collection to start

Safe for production
Imperceptible impact on performance

Controlled with policy
Tailor what is monitored to your environments' needs



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

Monitored Runtime Events

Java and .NET

Command execution

HTTP transactions

Filesystem access

Method invocation

Socket activity

SQL DB access

Class deserialization

Exceptions

.NET currently supports Command Execution

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

Attack Detection

Find threats in monitored runtime events

Analyze runtime events

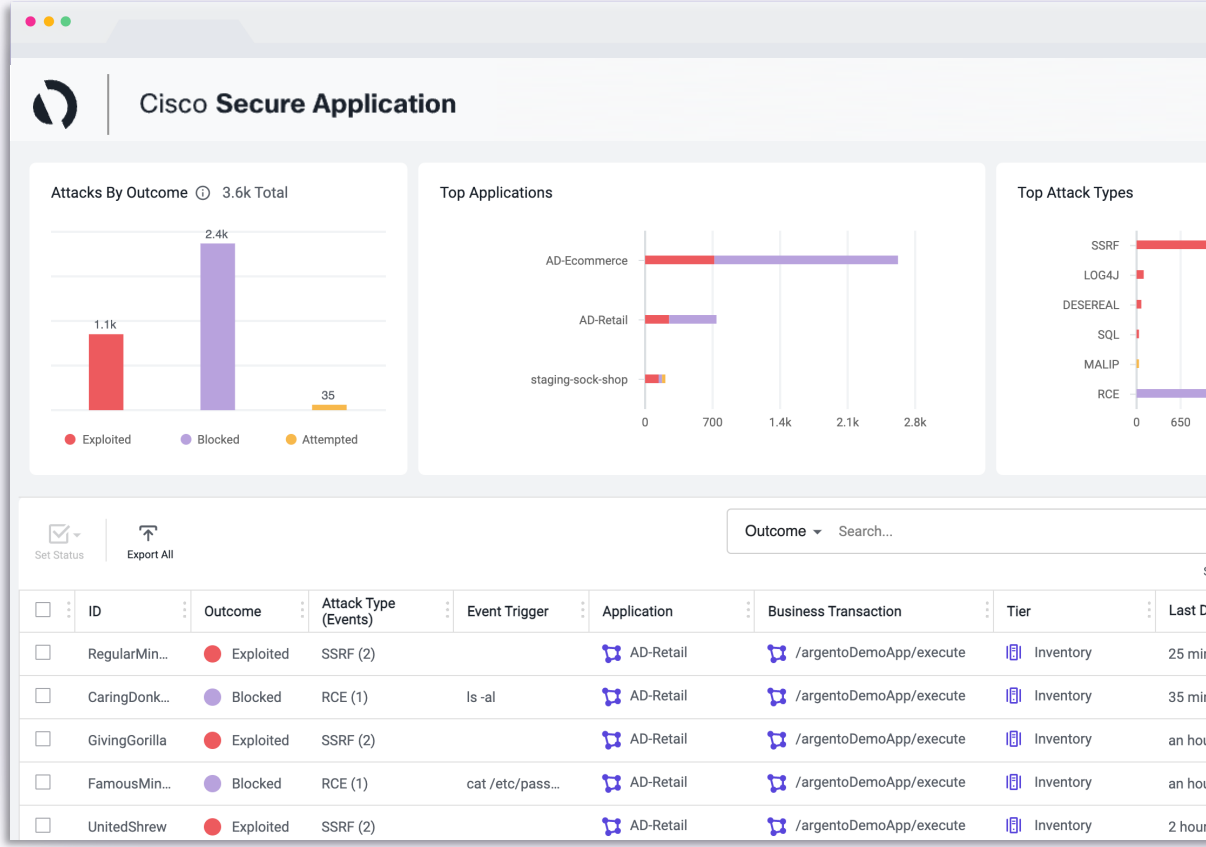
Parse and process application behaviors against our detection engine

Expose attack trigger

Identify and expose what is of most interest from the event

Correlate vulnerable code

Show when known vulnerability was exploited in the attack



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

Vulnerable Behavior Detection

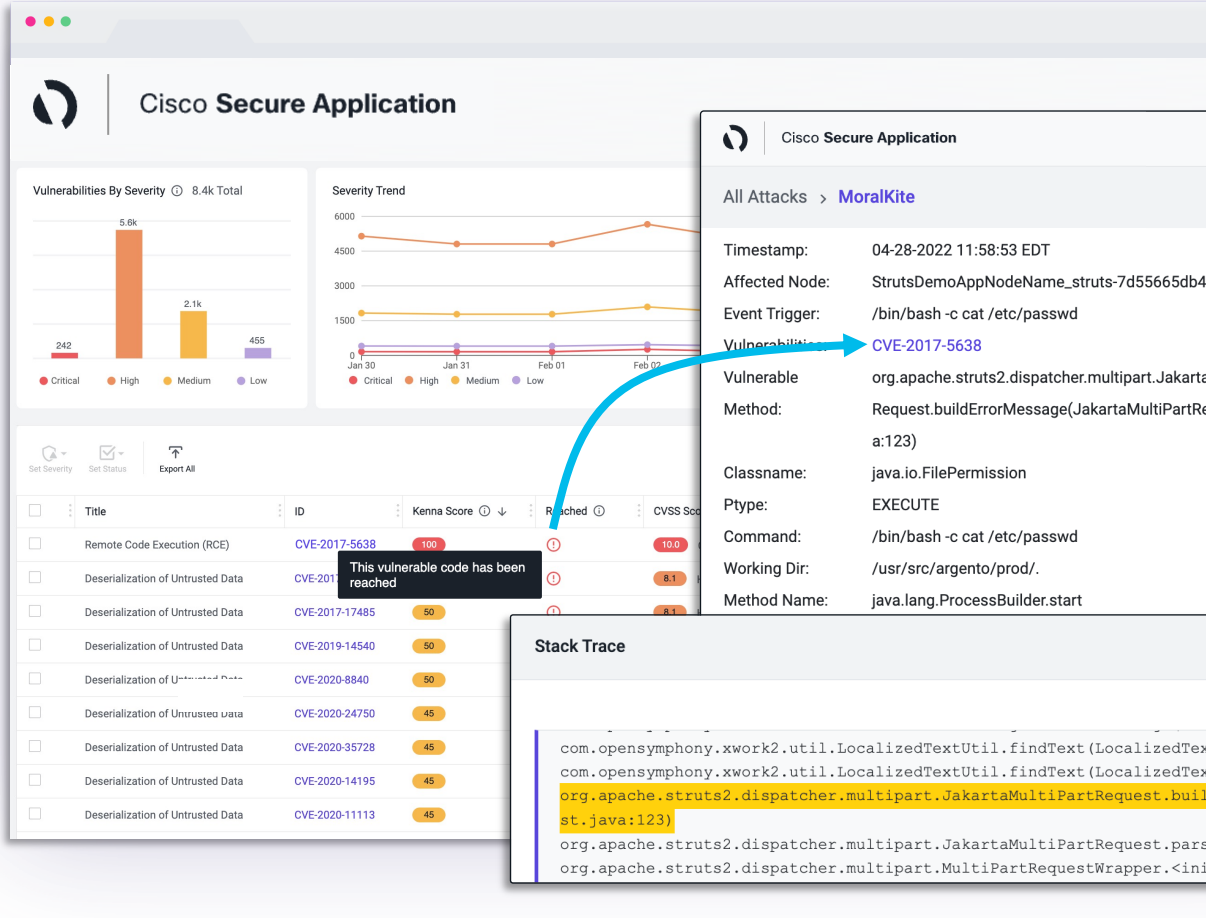
Identify when vulnerable code has been reached

Monitor vuln method usage

Remediate the libraries that introduce the biggest risk

Identify risky runtime events

Investigate and remediate call paths to vulnerable code

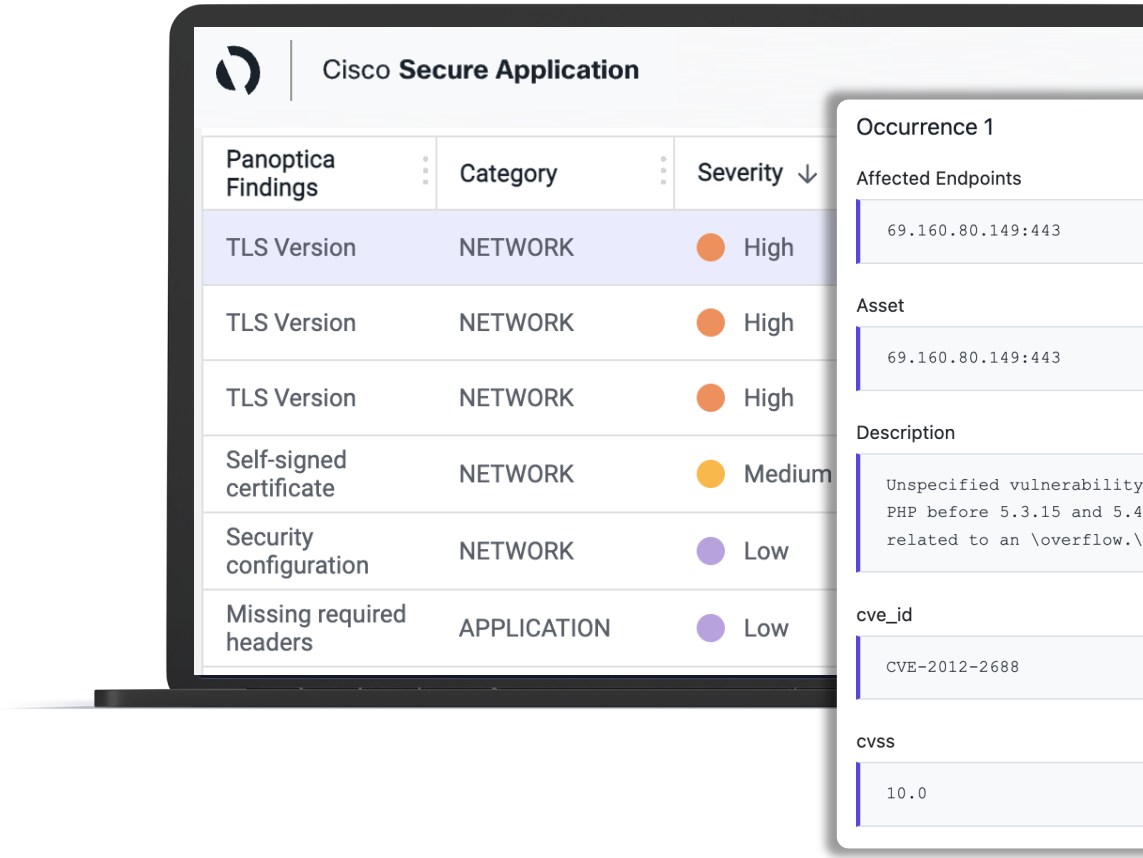


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

API Security Insights from Panoptica

Identify risk introduced by 3rd-party APIs

- Automatic discovery of API dependencies
- Determine security posture of APIs
- Native backend integration requiring no configuration
- Findings combined into application context for business risk scoring



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

Runtime Protection

Reduce alert fatigue and provide more targeted protections

Control runtime behavior

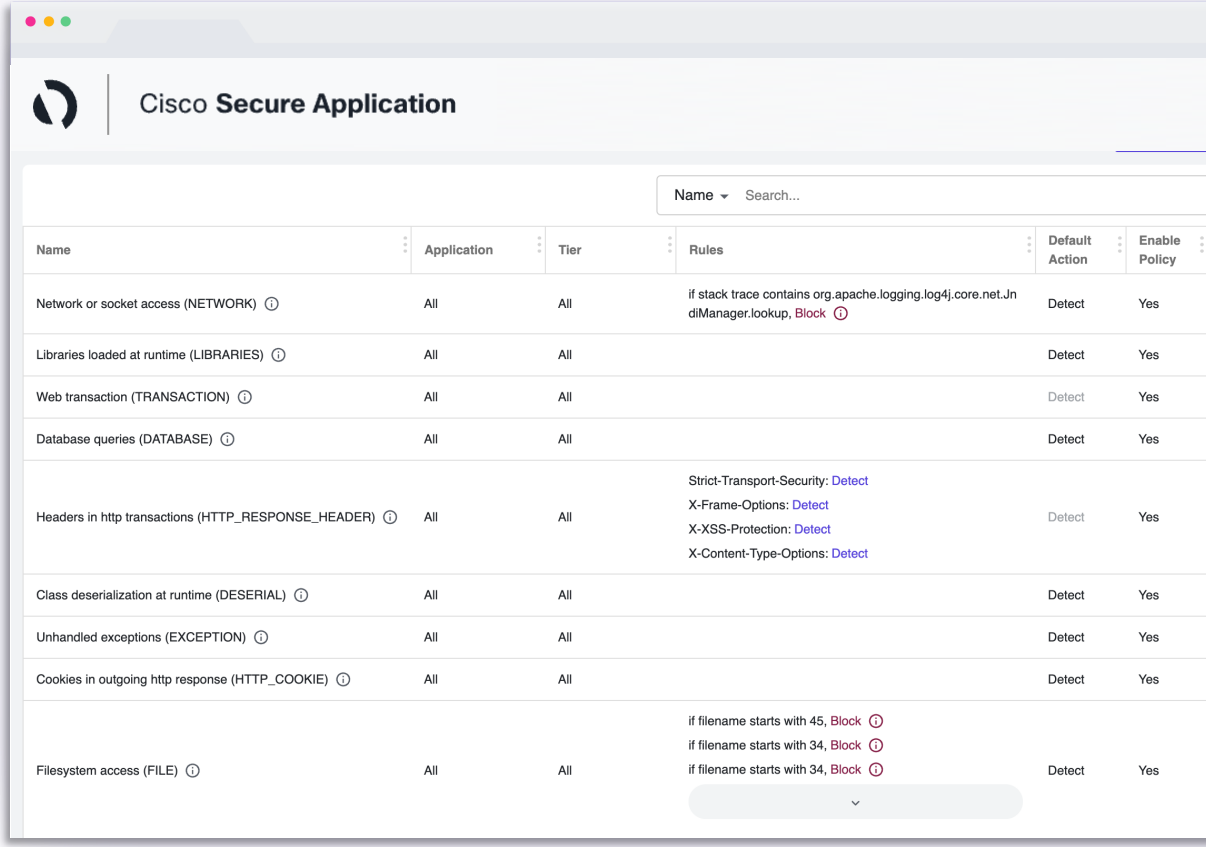
Without having to touch any code

Use stack traces & behavior

Buy devs time with targeted protection

Block access to sensitive resources

Enforce compliance across applications



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

Vulnerability Patching

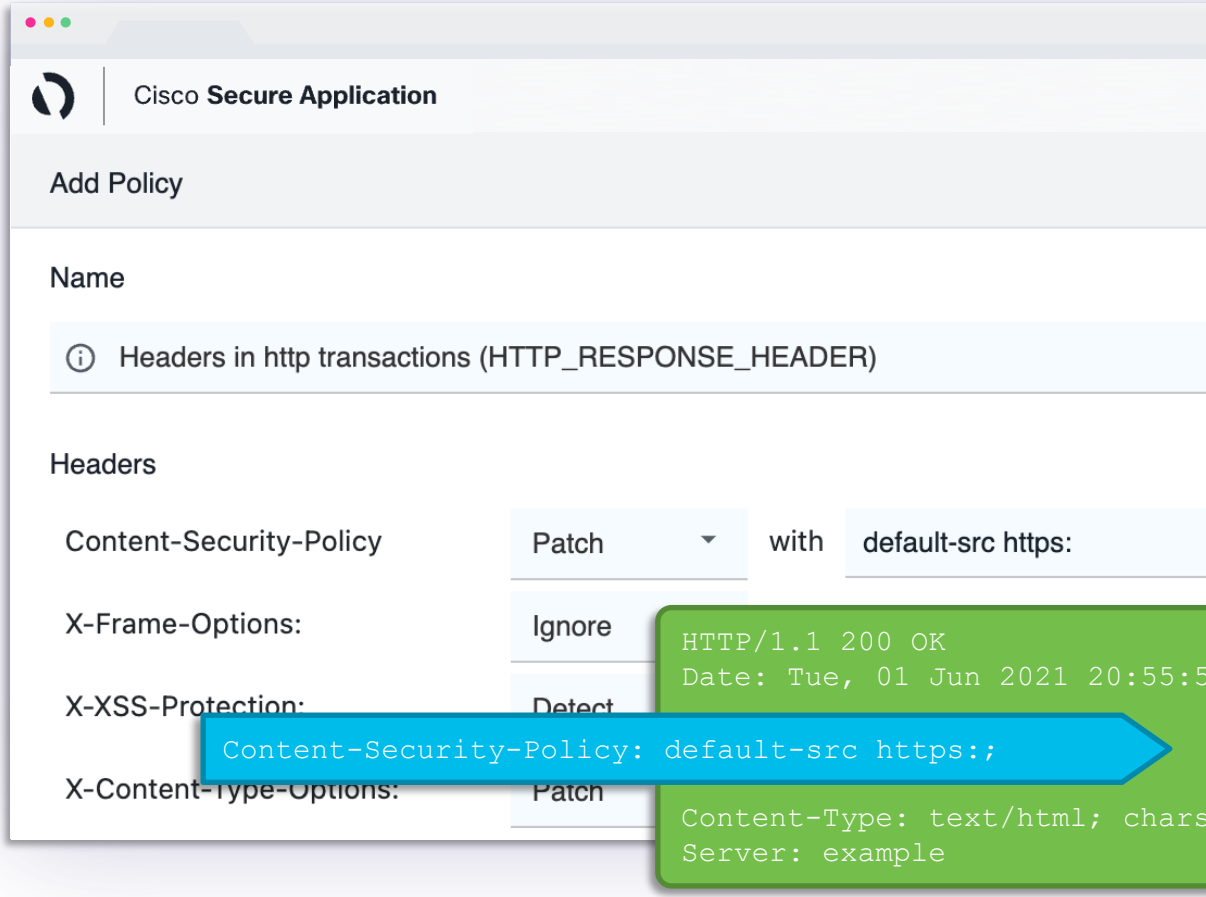
Protect against vulnerabilities without writing any code

Block use of vulnerable functions

Buy time for teams to investigate and remediate

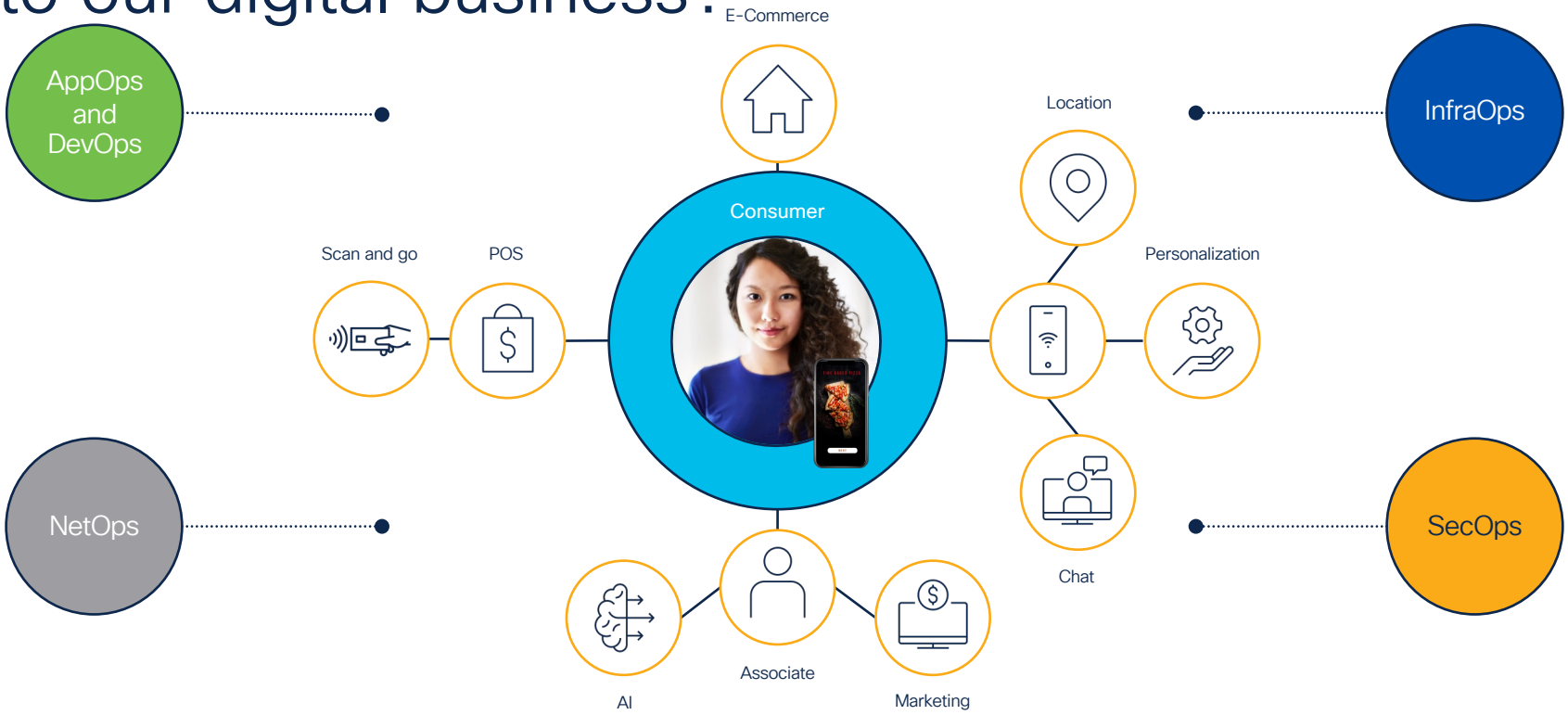
Add HTTP security headers

Devs don't need to modify legacy apps



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

Where should we focus our energy to reduce risk to our digital business?

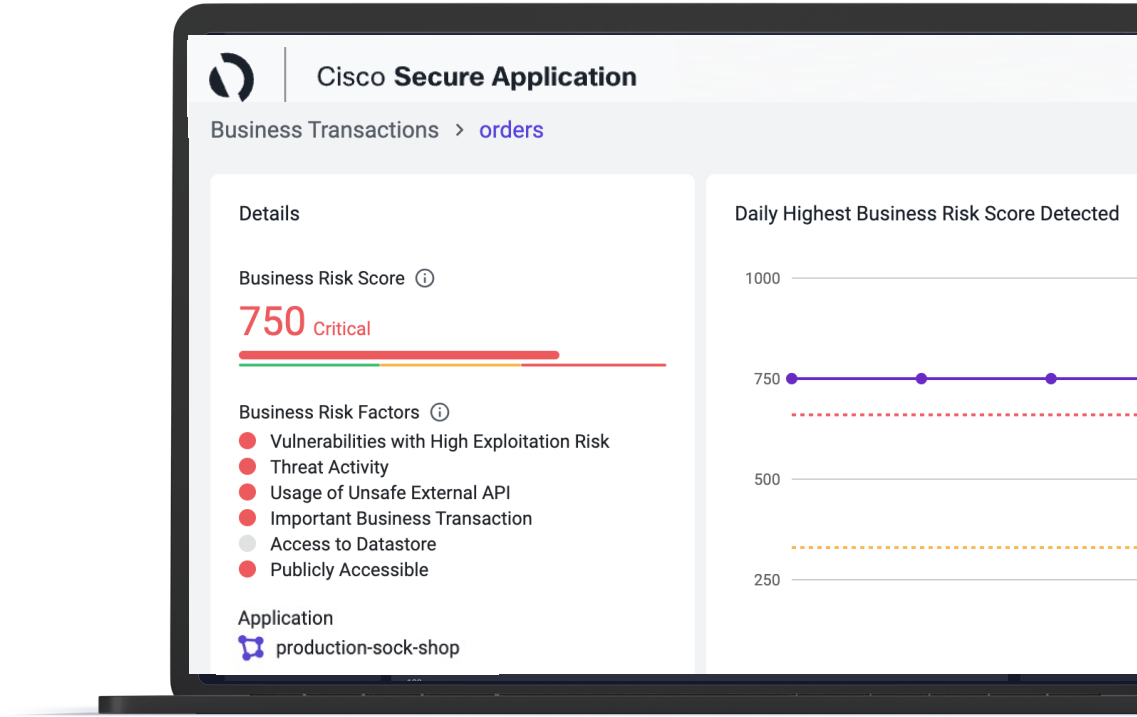


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Risk scoring with business-context

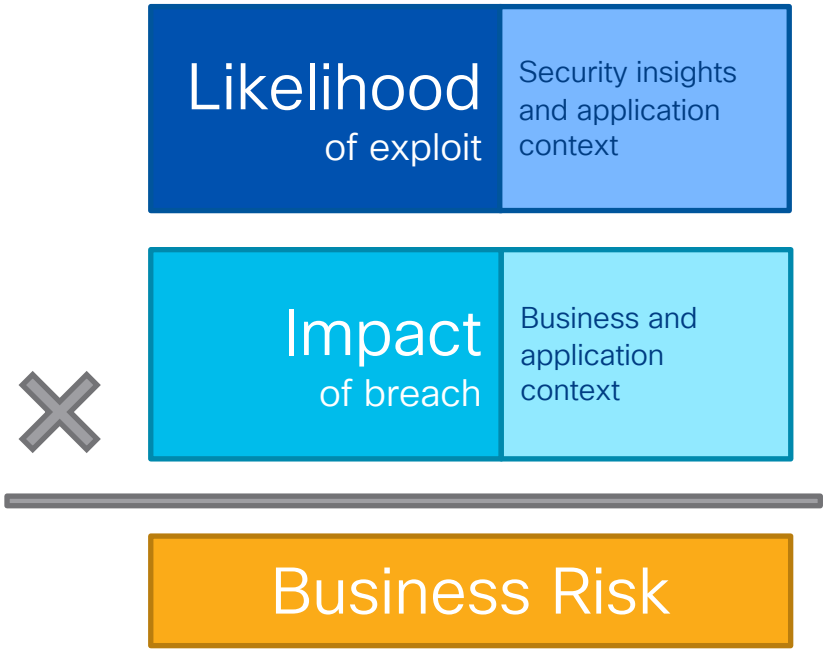
Tailored prioritization based on likelihood and impact

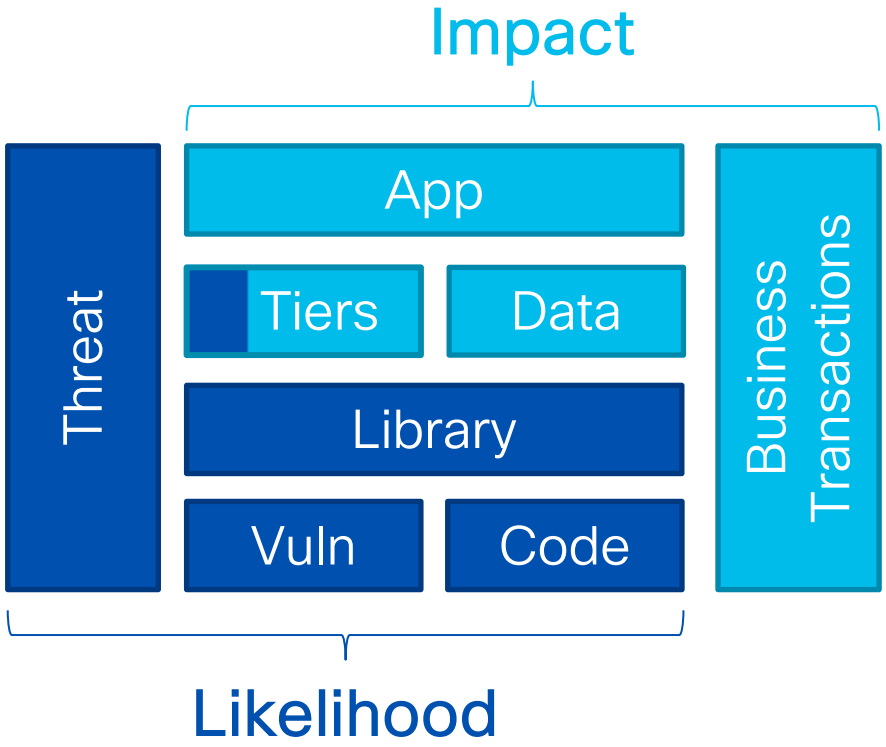
- Builds a customer-specific view of security risk
- Leverage findings and intel from Cisco Kenna, Panoptica, Talos
- Continuously assess score reflect real-time risk
- Prioritize remediation and mitigation efforts by what matters to the biz



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

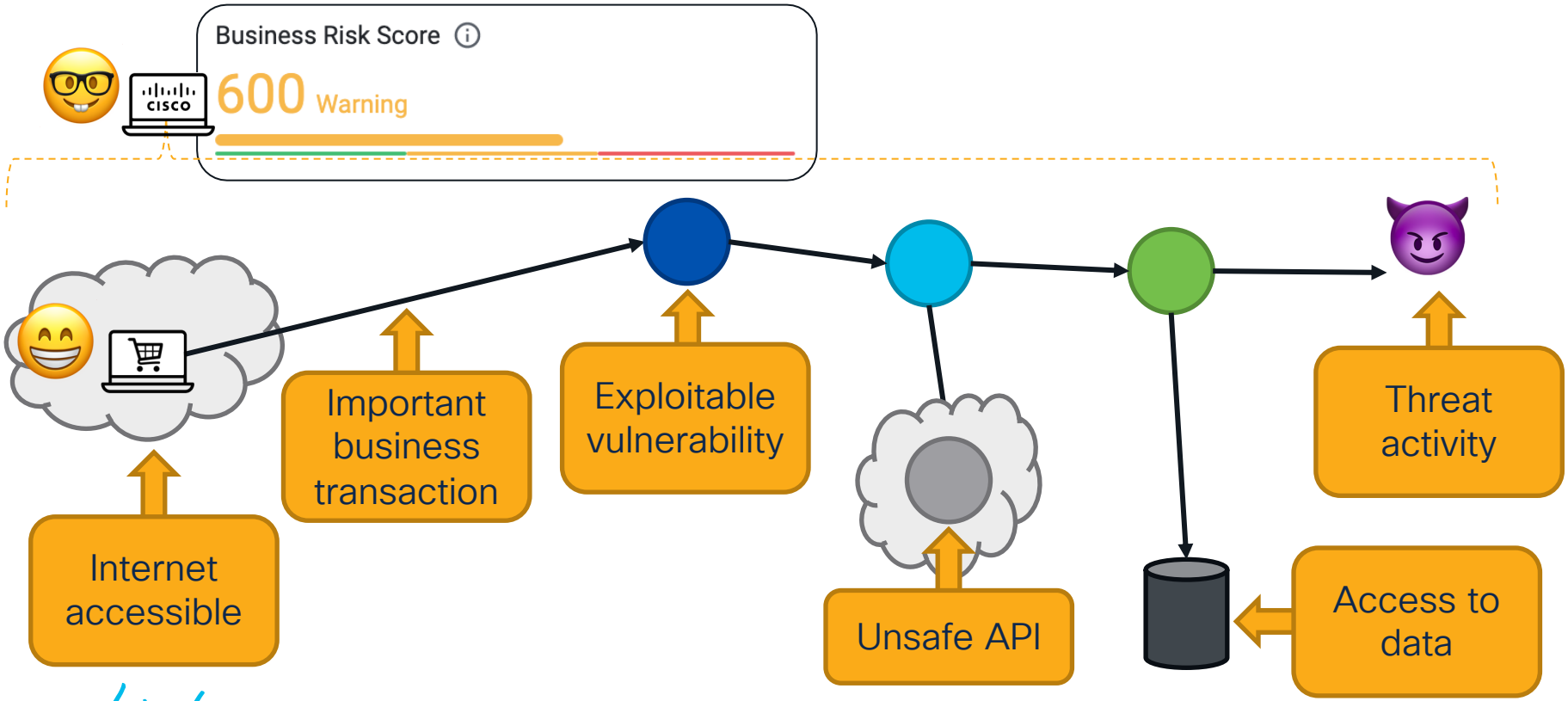
Calculating Business Risk





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

Components of Business Risk Assessment



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

Business Risk Demo
for Hybrid Applications

cisco Live!

Integrating insights into workflows

Get alerts to the people and the tools that trigger action

Trigger external API endpoints

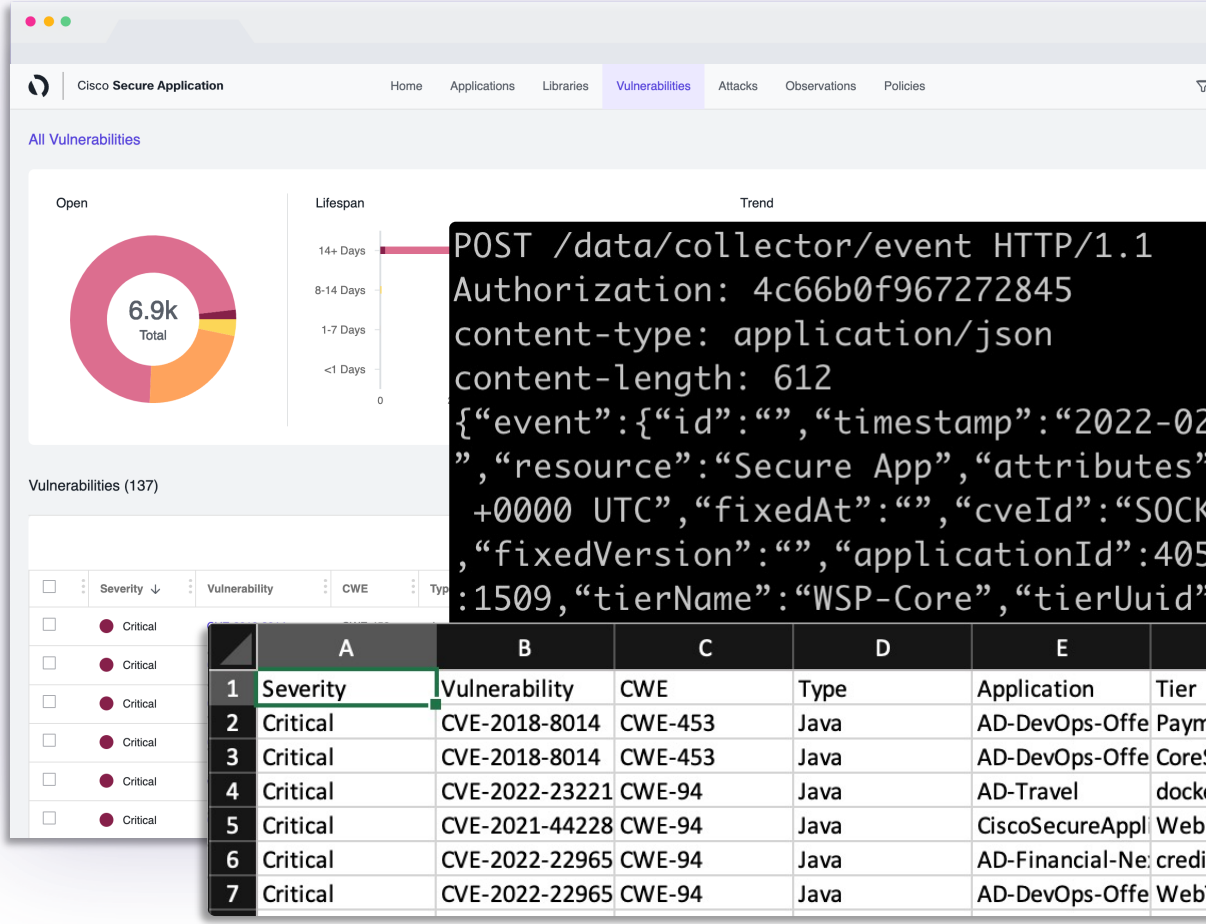
Pass alerts to workflow tools via HTTP REST APIs

Export reports

Extract data directly from filtered lists throughout the UI

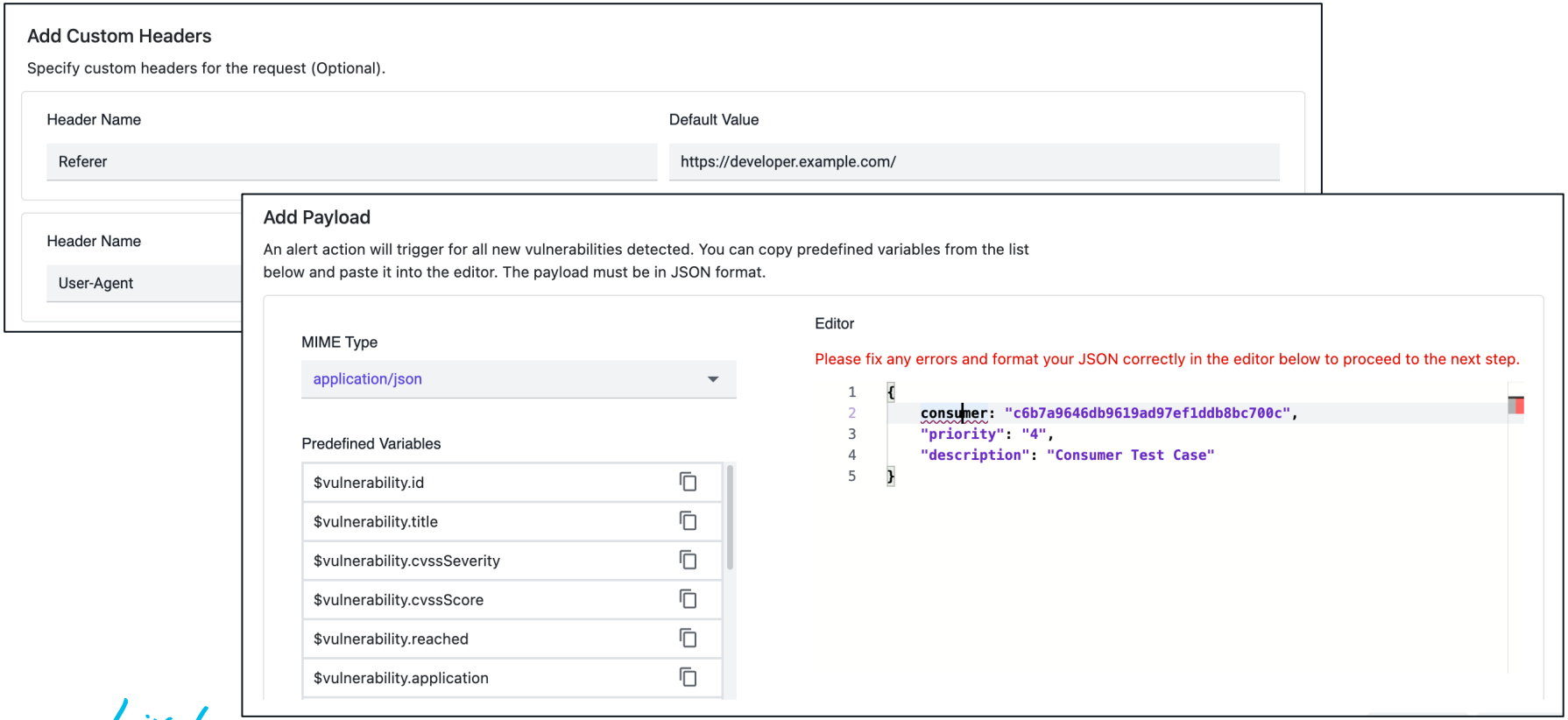
SIEM integration

Send all detections to Splunk



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

HTTP Alerting Configuration

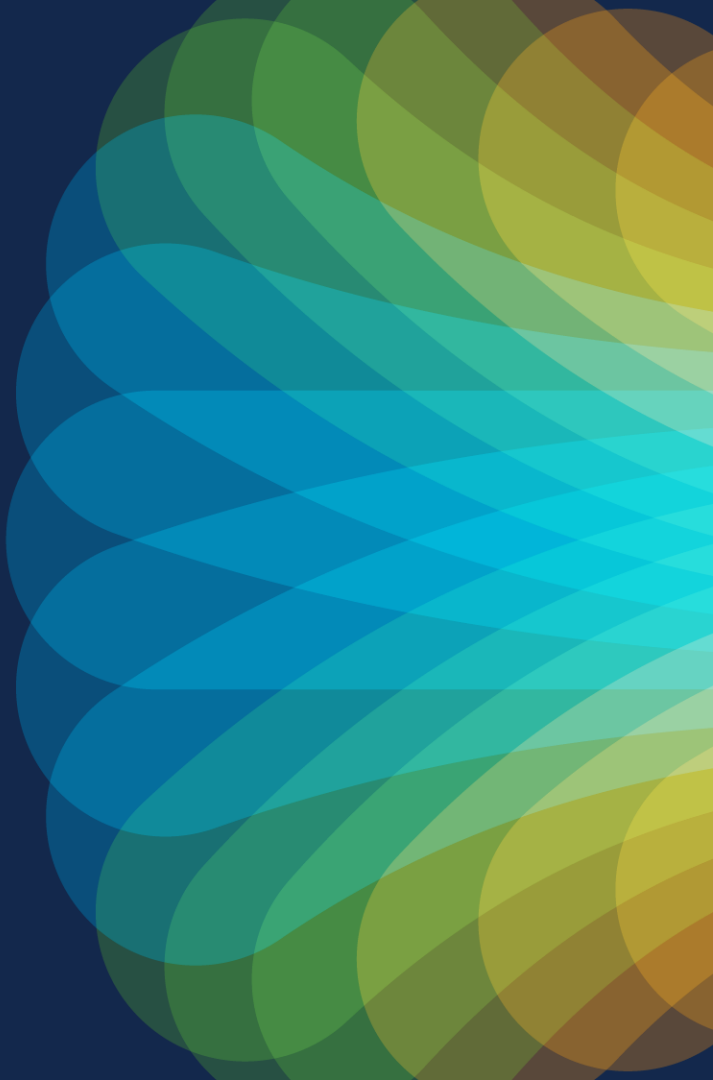


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Business Risk Observability Use Case

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

Application Security for Cloud Native Applications



cisco Live!

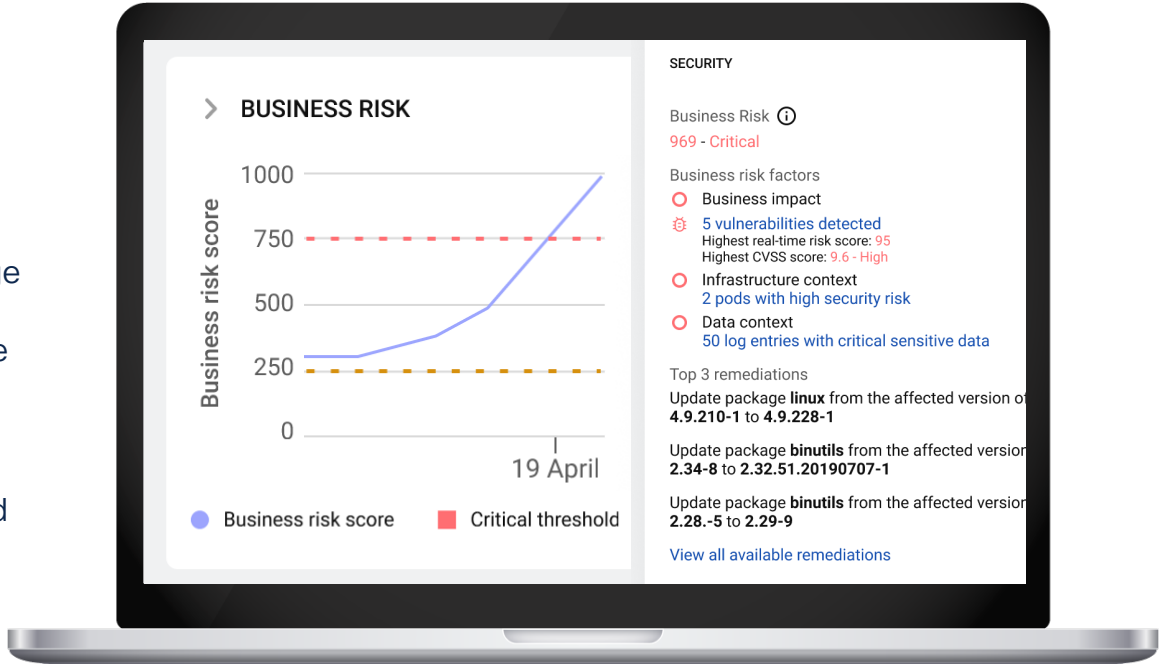
Cisco Secure Application

Business risk observability for cloud native applications

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

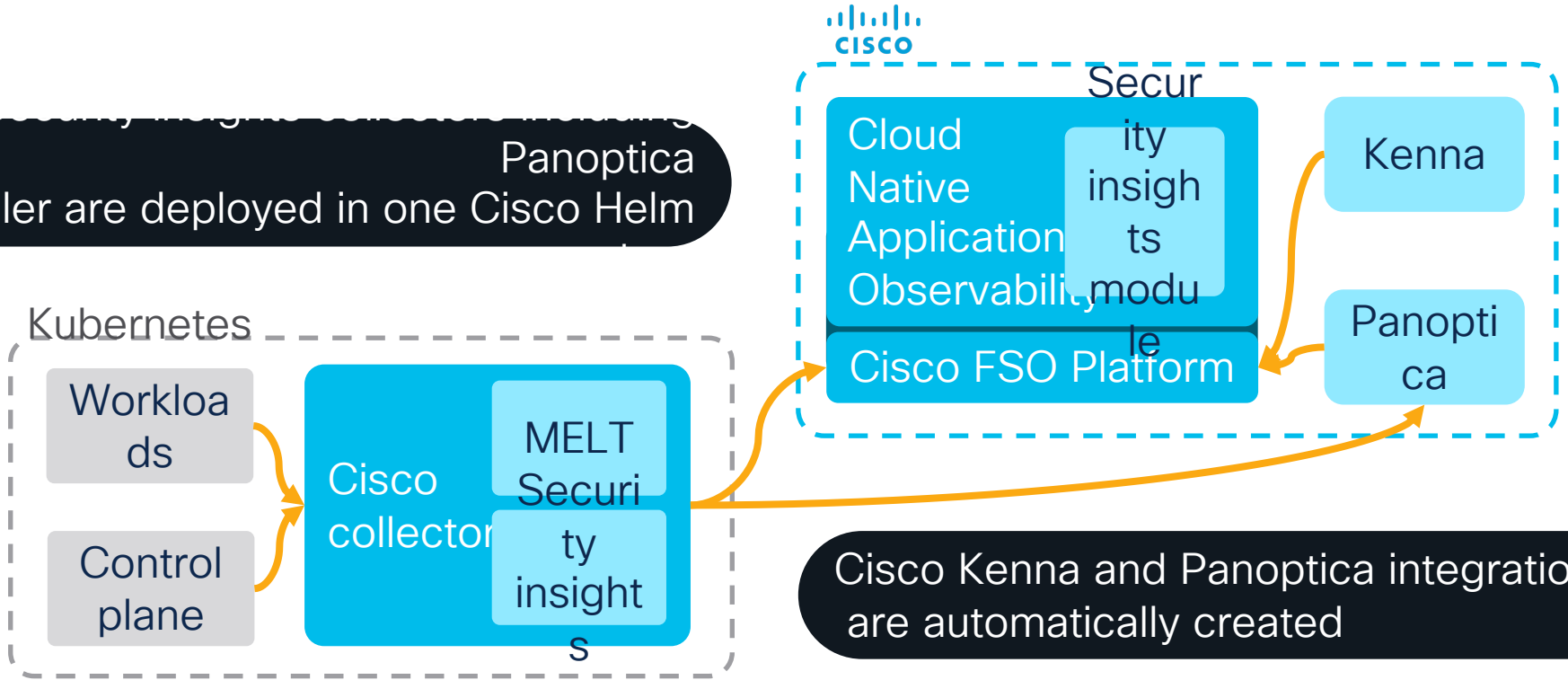
Combine threat and vulnerability intelligence from Cisco Kenna and Panoptica with business impact and runtime behavior to provide a business risk score



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

Security insights module architecture

Panoptica
ntroller are deployed in one Cisco Helm



Cisco Kenna and Panoptica integrations are automatically created

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

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

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

Foundational Capabilities

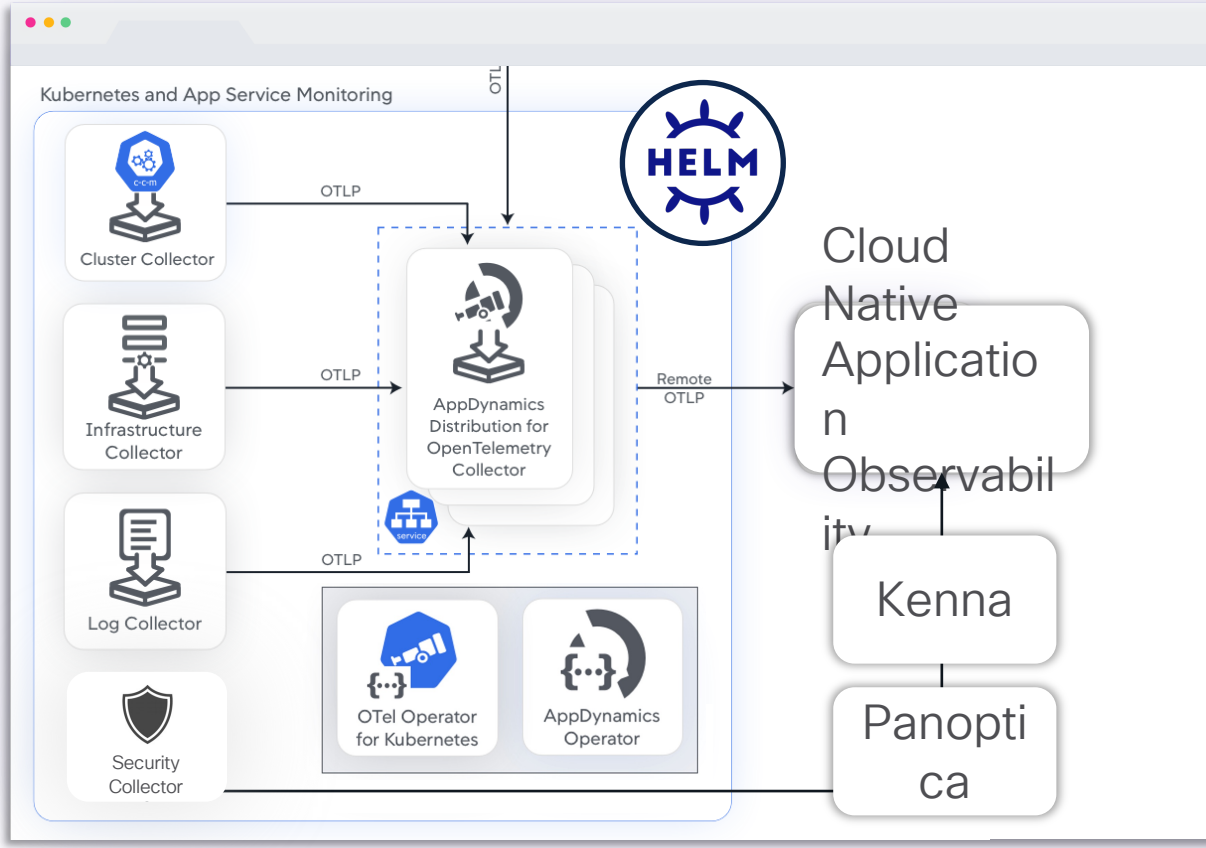
Seamless Onboarding

Get insights within minutes

Integrated collector deployment
Install a single Helm chart for all Observability data to be collected

No configuration required
Just subscribe to the security module and your presented with valuable data

No additional licensing
Kenna and Panoptica don't require any licenses



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

Application Metadata

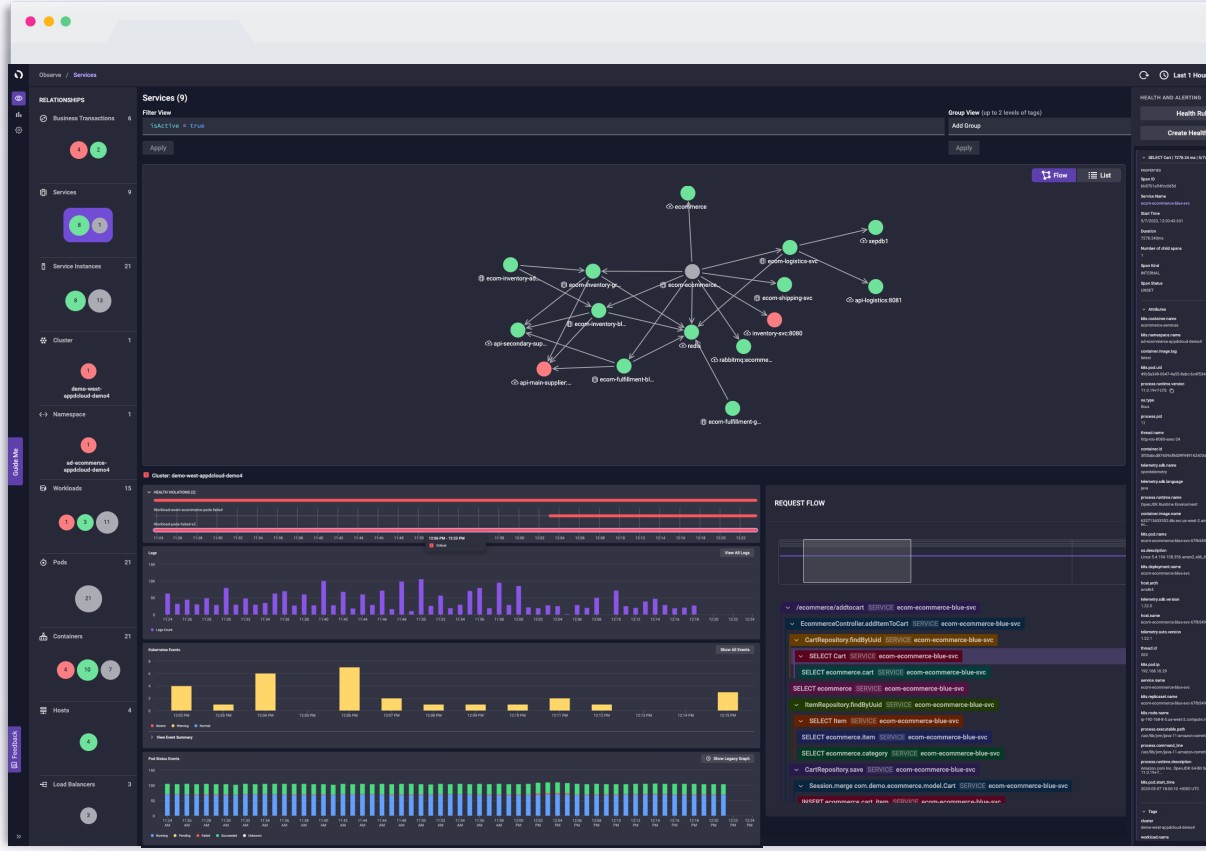
Give context to security insights

Leverage infrastructure and service entity identification

No one needs to prepopulate security tooling

Automatically correlate security insights to app entities

Immediate understanding between sec and app teams



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

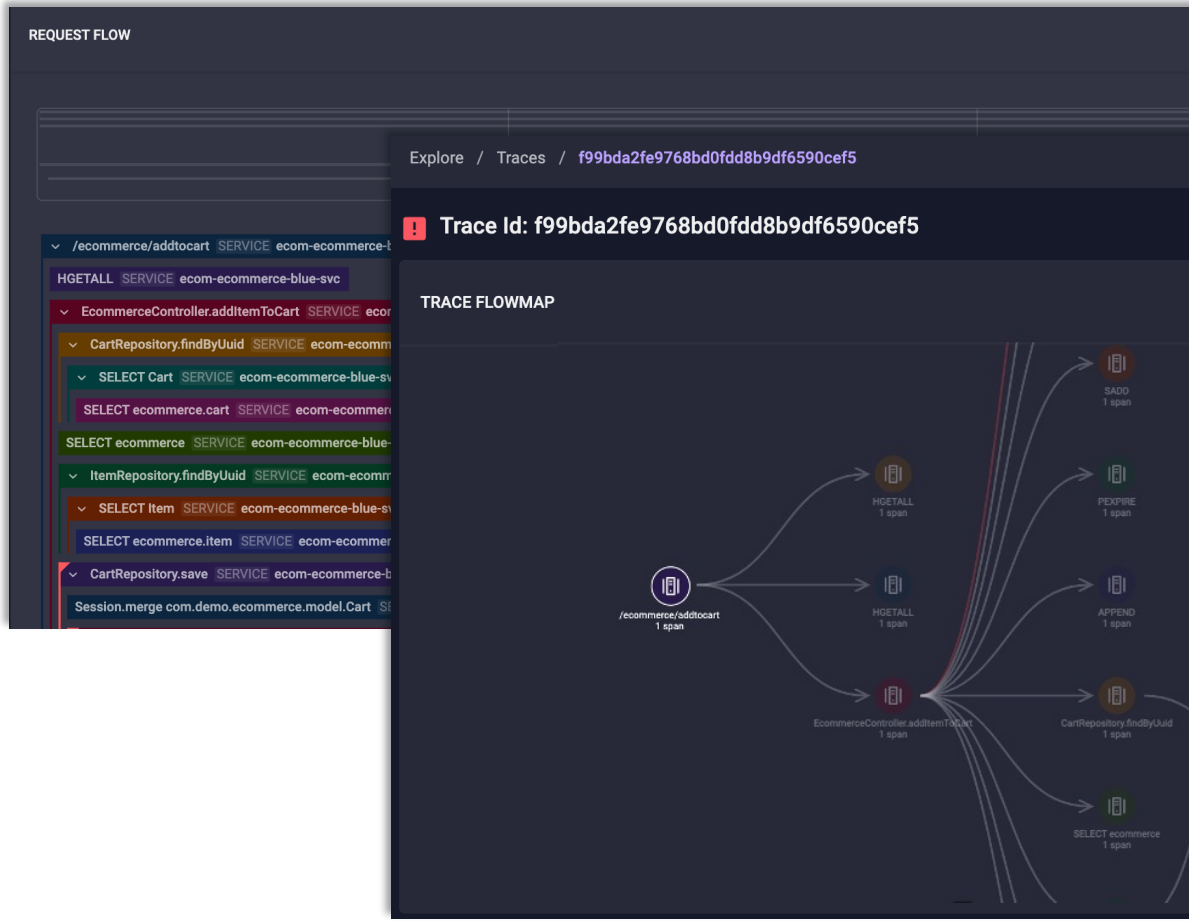
Trace Exploration

Troubleshoot at the most granular level with spans

Search Traces & Spans
by cross-domain & advanced criteria

Navigate across application
and infrastructure domains

Proactively discover bottlenecks
and improve application performance



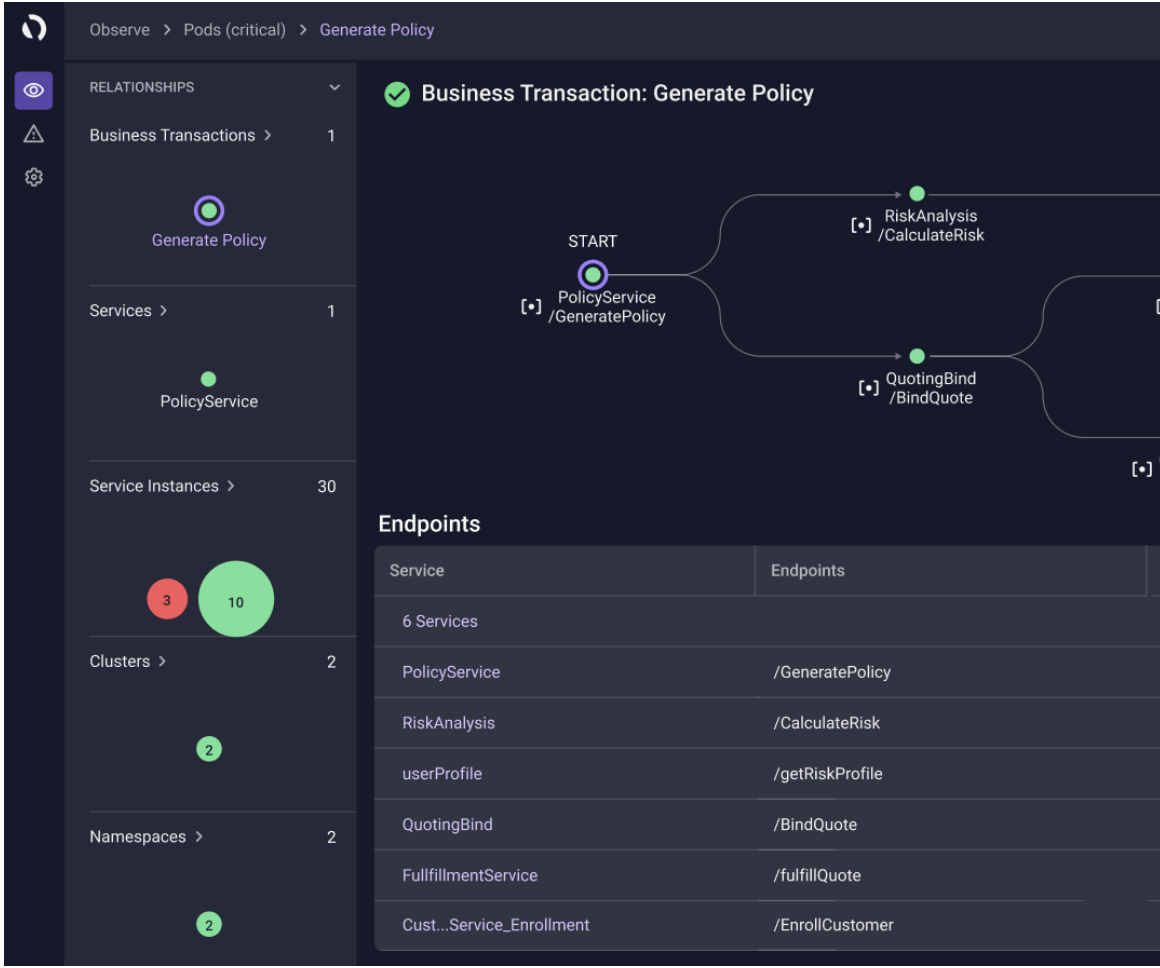
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Auto-Defined Business Transactions

Troubleshoot your most business-critical issues

Jumpstart your Business Centric Observability

with automatically defined business transactions leveraging predictive detection



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

Cross M.E.L.T. correlation

Find root cause in minutes with automated traces to logs correlation

Correlated Errors in Spans

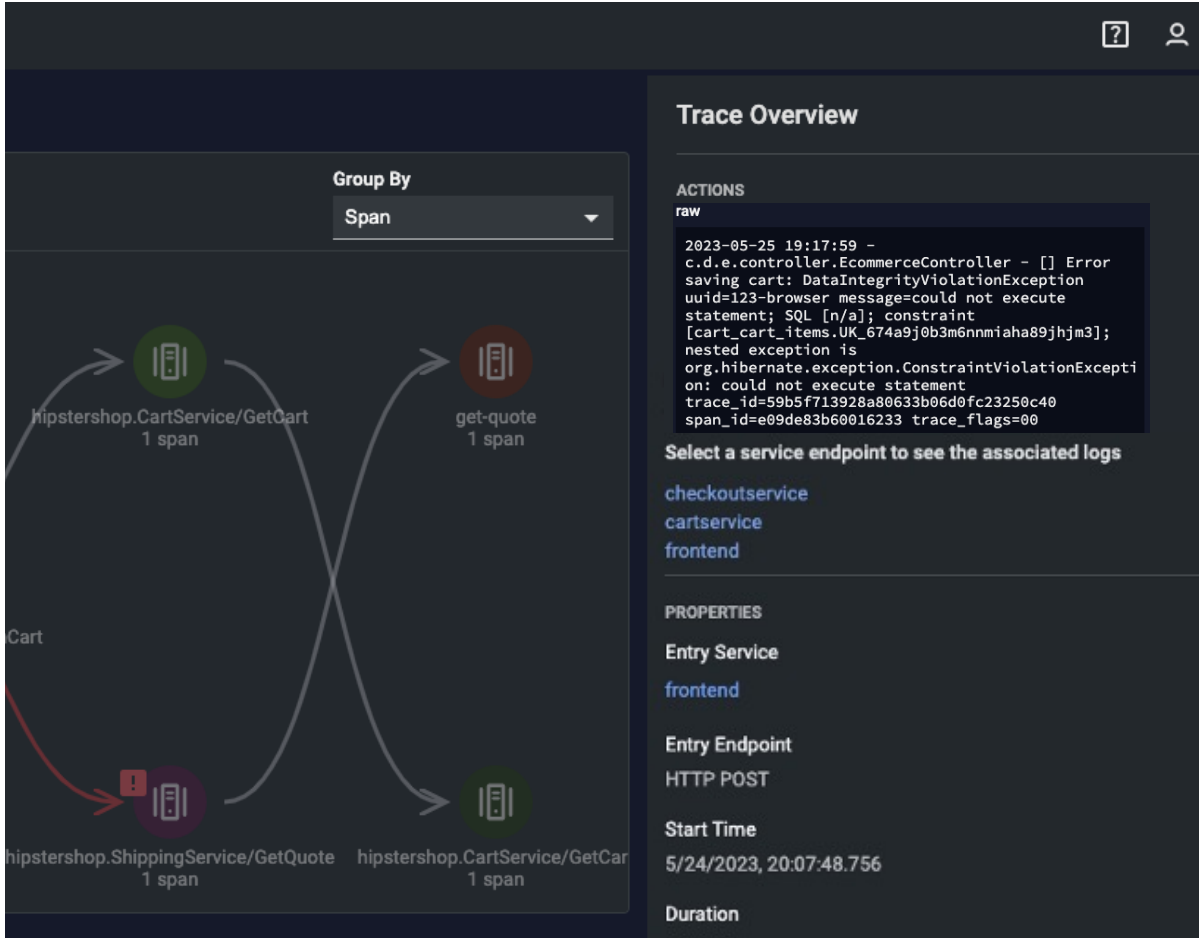
Surface log messages in context to reduce MTTR

Time to Value

with out of box correlation between traces and logs using Span IDs

Time to Value

with out of box correlation between traces and logs using Span IDs



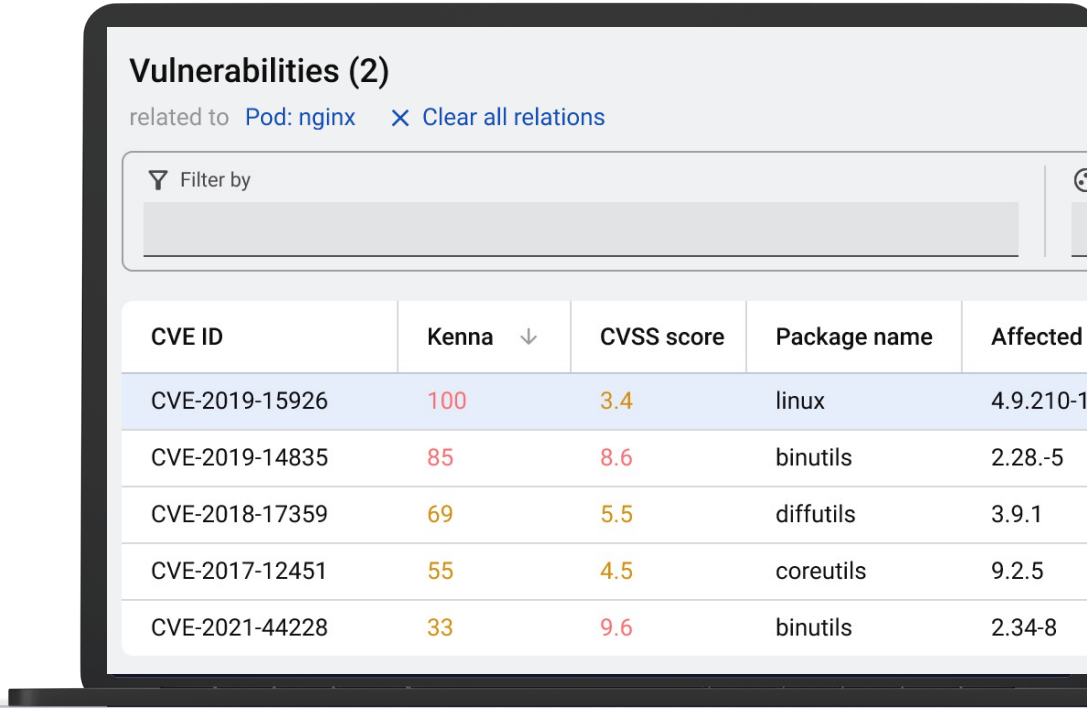
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security Capabilities

Identify Open-Source Risk

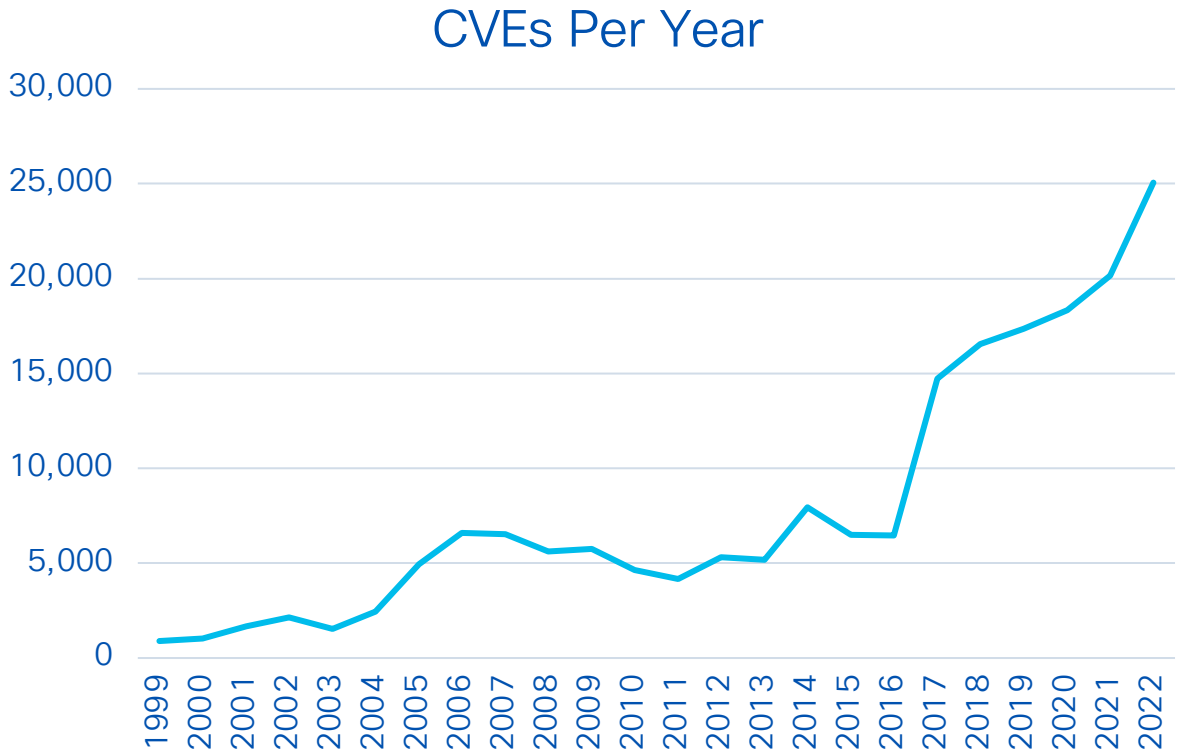
Know what vulnerable third-party code your apps are using

- Runtime container image scanning in Kubernetes from Panoptica
- Constant monitoring to detect vulnerabilities are right after they're disclosed
- Remediation guidance to get fixes out quicker tailored to your environment



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

Rate of Vulnerability Disclosure



CVEs from NVD
190,359

Average CVEs Published Per Day
68

2022
25,059
24% Y/Y

2023 Q1
17% Q/Q

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

Our research shows us that...

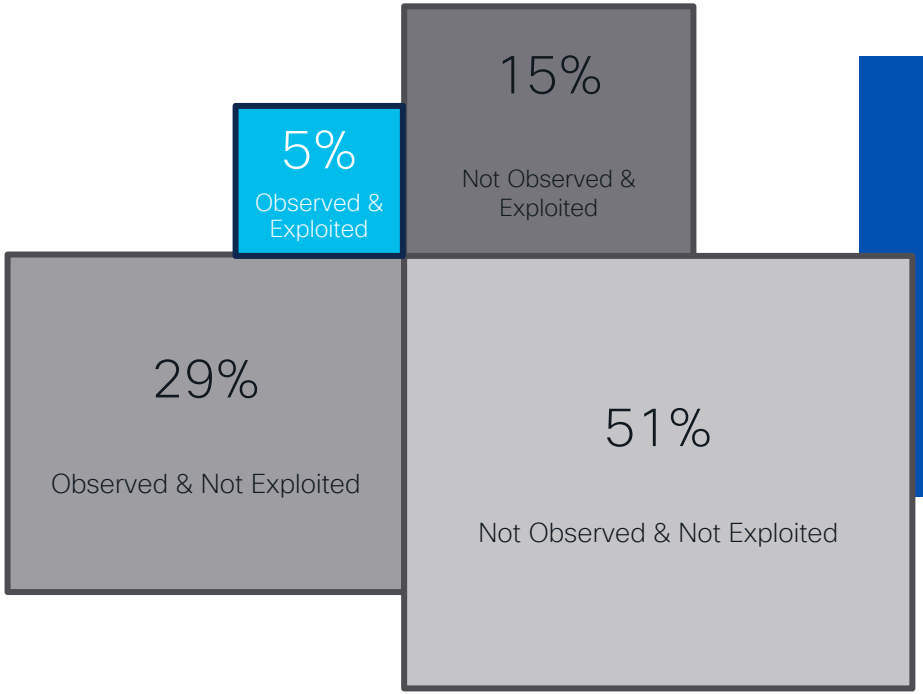
- There were an average of 68 new software vulnerabilities published every day in 2022
- 95% of IT assets have at least one highly exploitable vulnerability.
- Organizations are remediating around 1 in 10 vulnerabilities in any month.
- Twitter mentions to prioritize software fixes are 2X as effective at reducing organizational exploitation as CVSS.

Source: Prioritization to Prediction, Volume 8, The Cyentia Institute & Kenna Security

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

Which vulnerabilities are truly risky?

CVEs in the NVD: Observed and Exploited



Roughly 5% of CVEs in the NVD are *observed* in enterprises and *exploited* in the wild.

These are the ones you want to prioritize for remediation.

Source: Prioritization to Prediction, Volume 5, Kenna Security & The Cyentia Institute

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

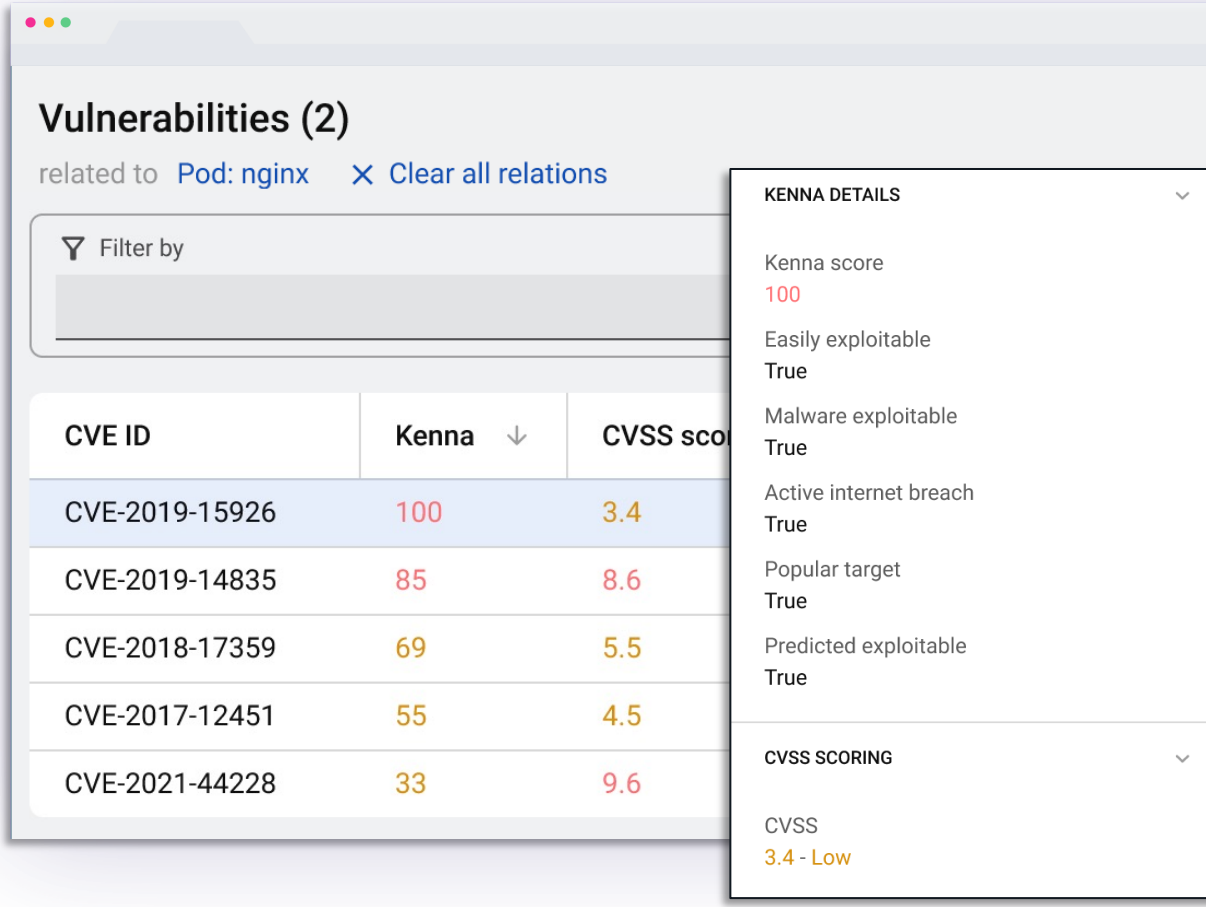
Determine likelihood of exploit

Use data science to identify real vulnerability risk

Leverage Kenna vulnerability intelligence
Native backend integration maps Kenna scores to discovered vulns

Better coverage in less time
Identify incorrect remediation prioritization

Factor in business risk
Combine findings into vuln and threat context for business risk scores



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

Cisco Kenna cuts through the noise

Kenna looks at various categories of vulnerability data to understand what happens to a CVE during all stages of its life, from the assignment of a CVE to the unlikely event of an exploitation in the wild.

Volume & velocity data is different than a "Yes/No" data point. It tells you: *In the past 24 hours, 7240 machines have been exploited using a CVE.*

Data Categories

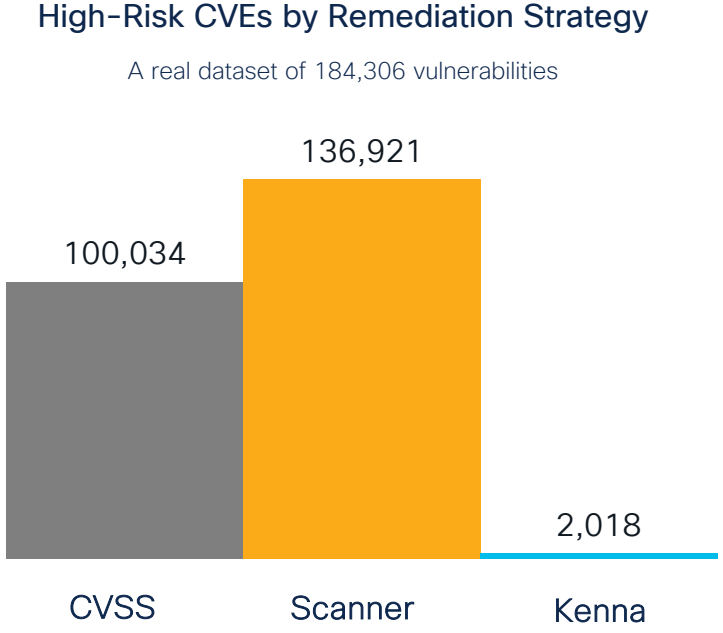
MITRE & NVD Vulnerability Scoring Early Warning Chatter	Exploit Databases Malware Analysis	Threat Actors Malware Families	Volume & Velocity of Exploitation in the Wild

Kenna Machine Learning Model-Based Risk Scoring

This incorporates the prediction of exploitation publication and exploitation event (94% accuracy)

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

High-risk remediation strategies



1.09% of these CVEs are considered high-risk by Kenna

- ✓ 134,903 fewer vulnerabilities to remediate compared to the scanner
- ✓ 98,016 fewer vulnerabilities to remediate compared to CVSS

Missed high-risk vulns

111 CVEs found high by Kenna but not found high by scanner

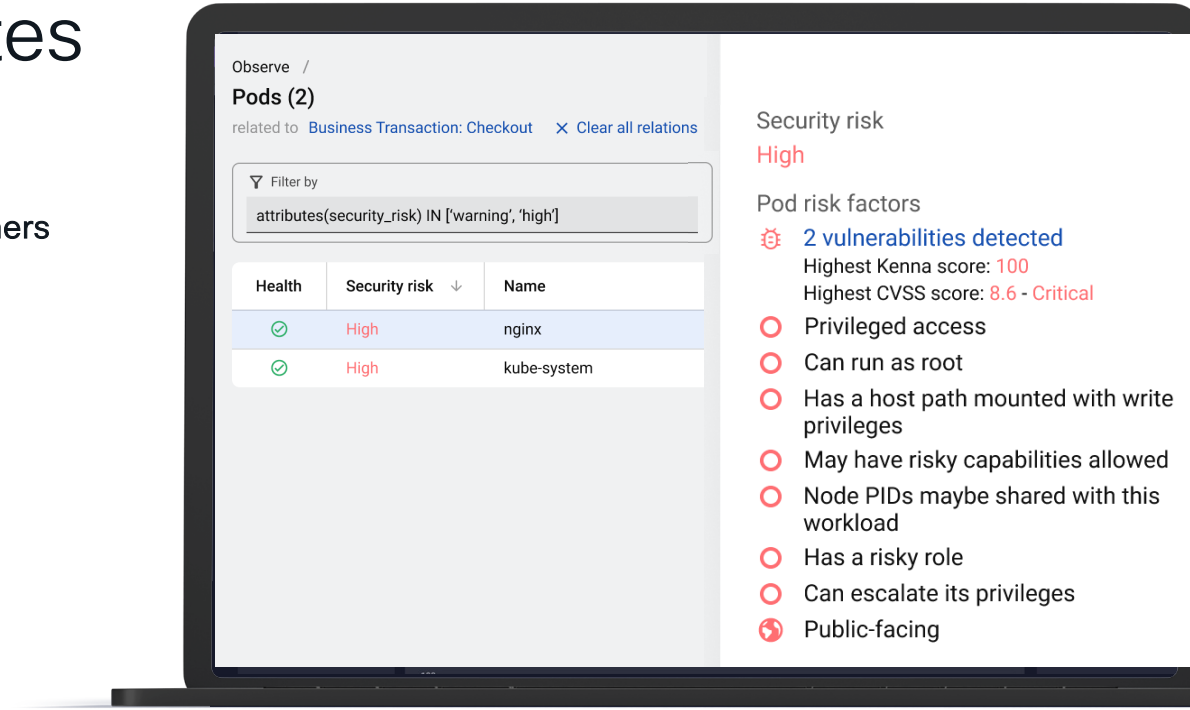
51 CVEs found high by Kenna but not found high by CVSS

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

Uncover Kubernetes security posture

Identify risk introduced by K8s & Containers

- Native backend integration with Panoptica
- Infrastructure risk cross-corelated with application entities
- Findings combined into application context for business risk scoring

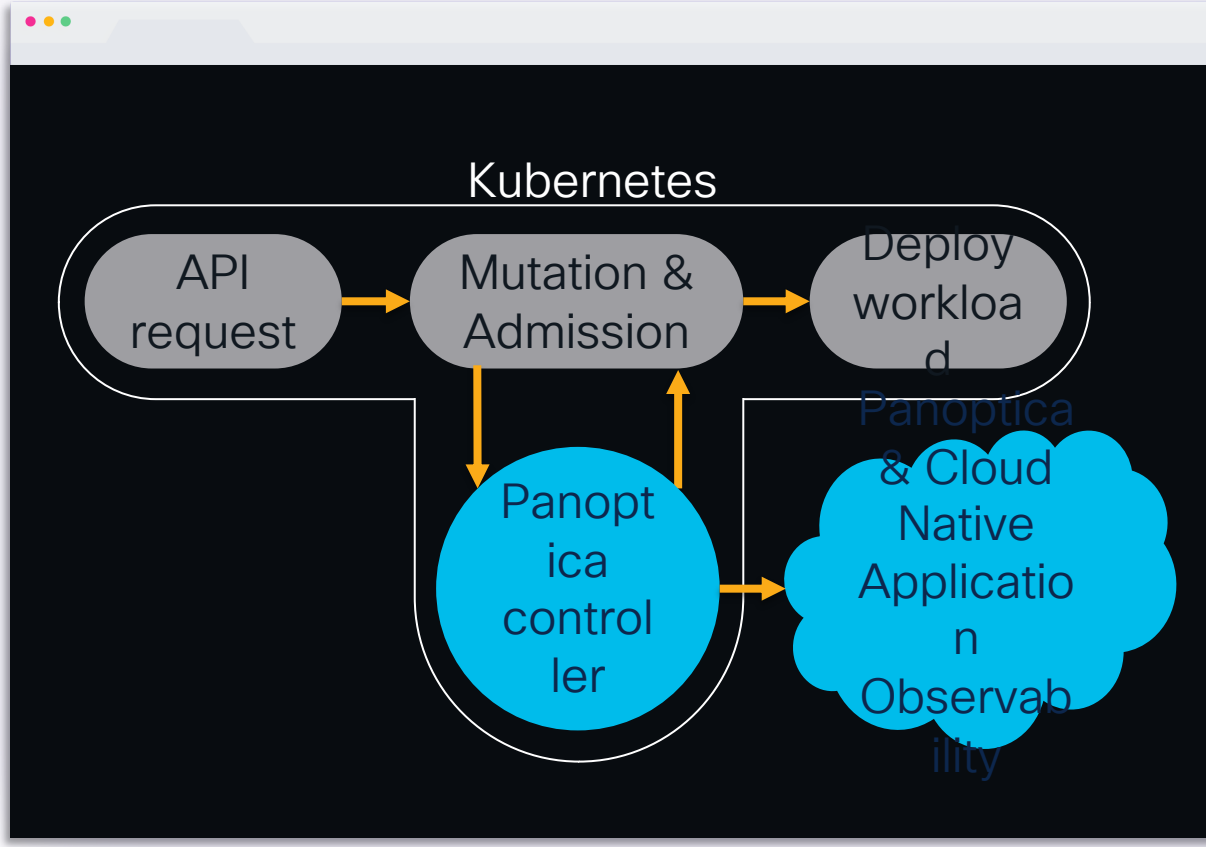


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Security insights runtime

Scalable real-time visibility and controls

- API integration provides agentless deployment
- Deploys as standard Kubernetes workload
- Scale using native Kubernetes constructs



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

Workload security posture

Panoptica catches dangerous configs

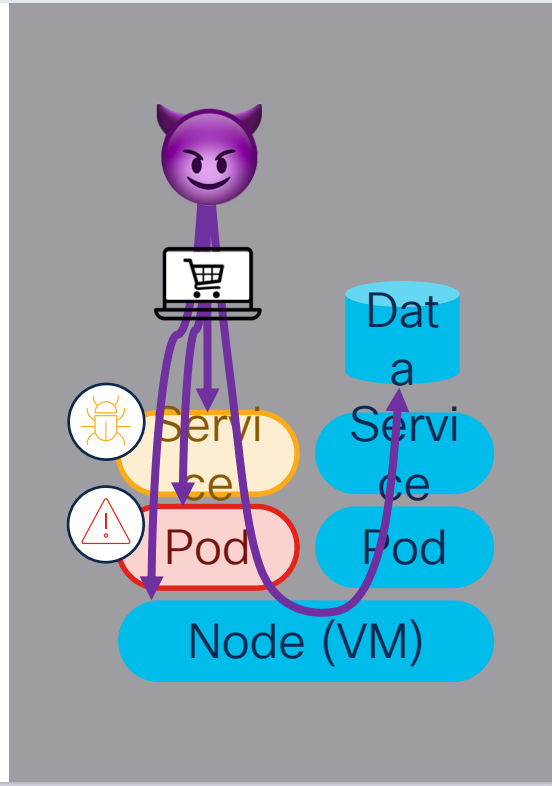
- Detect config risk for Kubernetes pods
- Identify accessibility outside of the cluster
- Weak posture leads to increased blast radius from vulnerabilities

Security risk

High

Pod risk factors

- 2 vulnerabilities detected
  - Highest Kenna score: 100
  - Highest CVSS score: 8.6 - Critical
- Privileged access
- Can run as root
- Has a host path mounted with write privileges
- May have risky capabilities allowed
- Node PIDs maybe shared with this workload
- Has a risky role
- Can escalate its privileges
- Public-facing

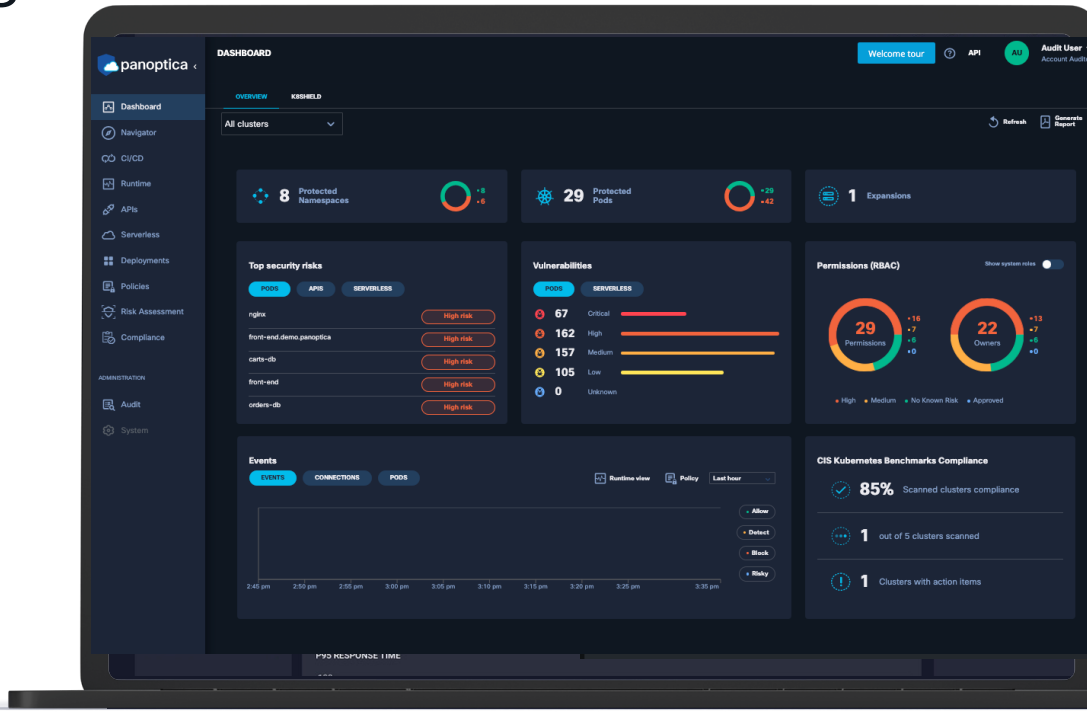


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Additional capabilities within Panoptica

Insight into Kubernetes, image vulnerabilities, RBAC and MITRE ATT&CK

- Service-mesh, mutating webhook, and CD plugins to perform vulnerability assessment and deployment policies
- Image scanning for VMs, containers and serverless functions; and SBOM/SLSA
- K8s vulnerabilities categorized by MITRE ATT&CK with remediation strategies
- Service mesh to obtain connection telemetry and enforce connection policies
- RBAC control to assess who can access what



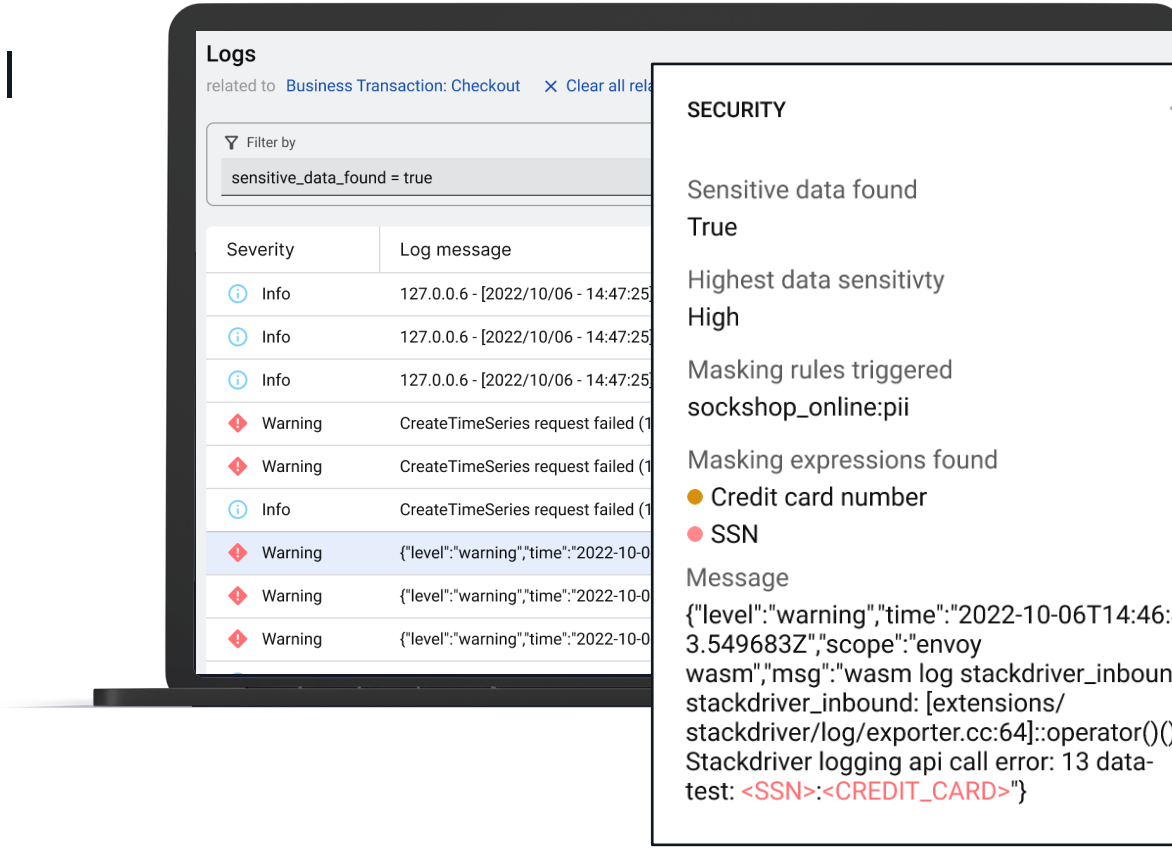
And many more use cases in Cloud Native Application Protectio

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

Detect and redact sensitive and personal data

Maintain compliance and protect customer data

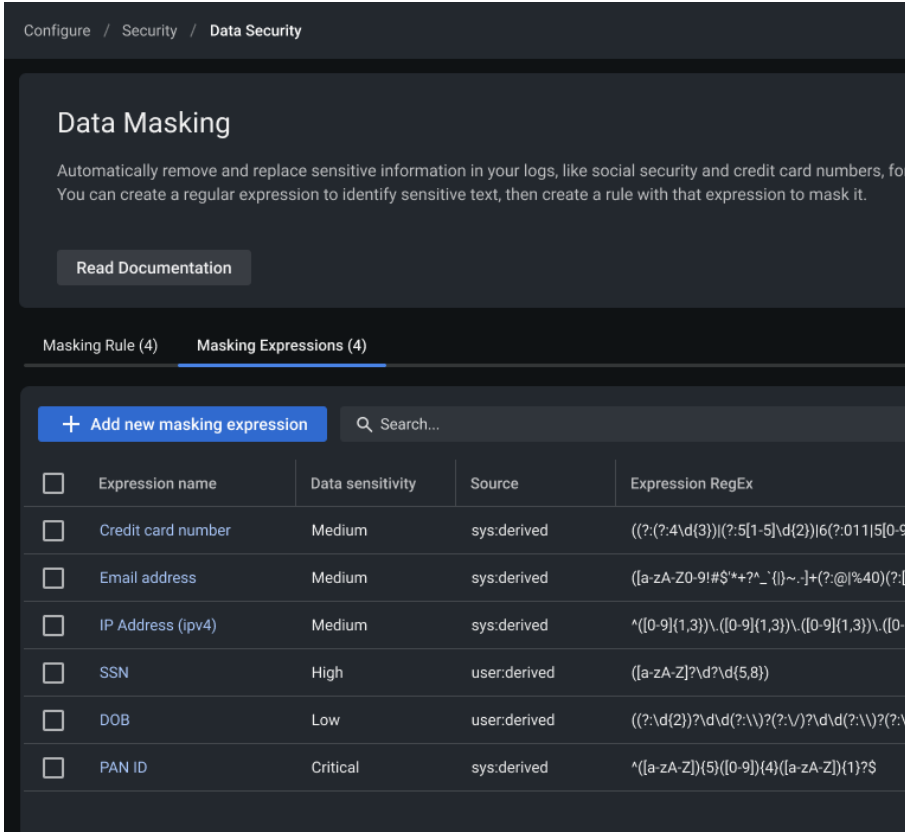
- PII leakage insights mapped to source entities to clamp down leakage
- Leverage prepackaged PII detection expressions to enable faster protection
- Build custom policies and expressions to detect and redact any data
- Combine findings into vuln and threat context for business risk scores



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

Data Expressions

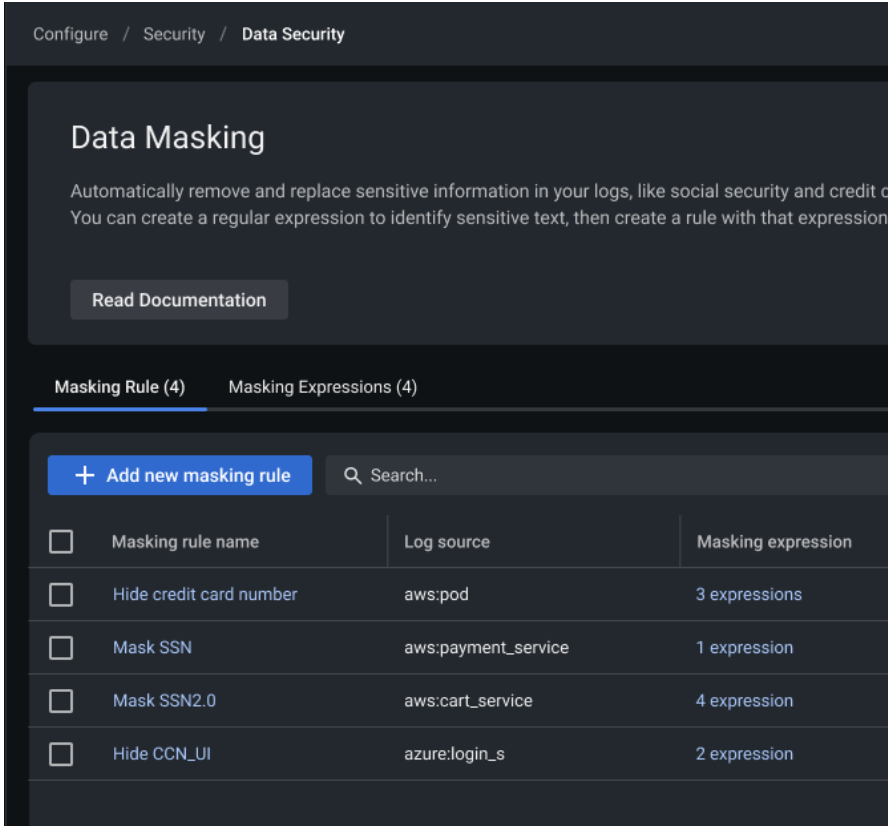
- Predefined expressions for common sensitive data types
- Create custom expressions using Regex
- Data is redacted
- Set sensitivity level of data based on your business



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

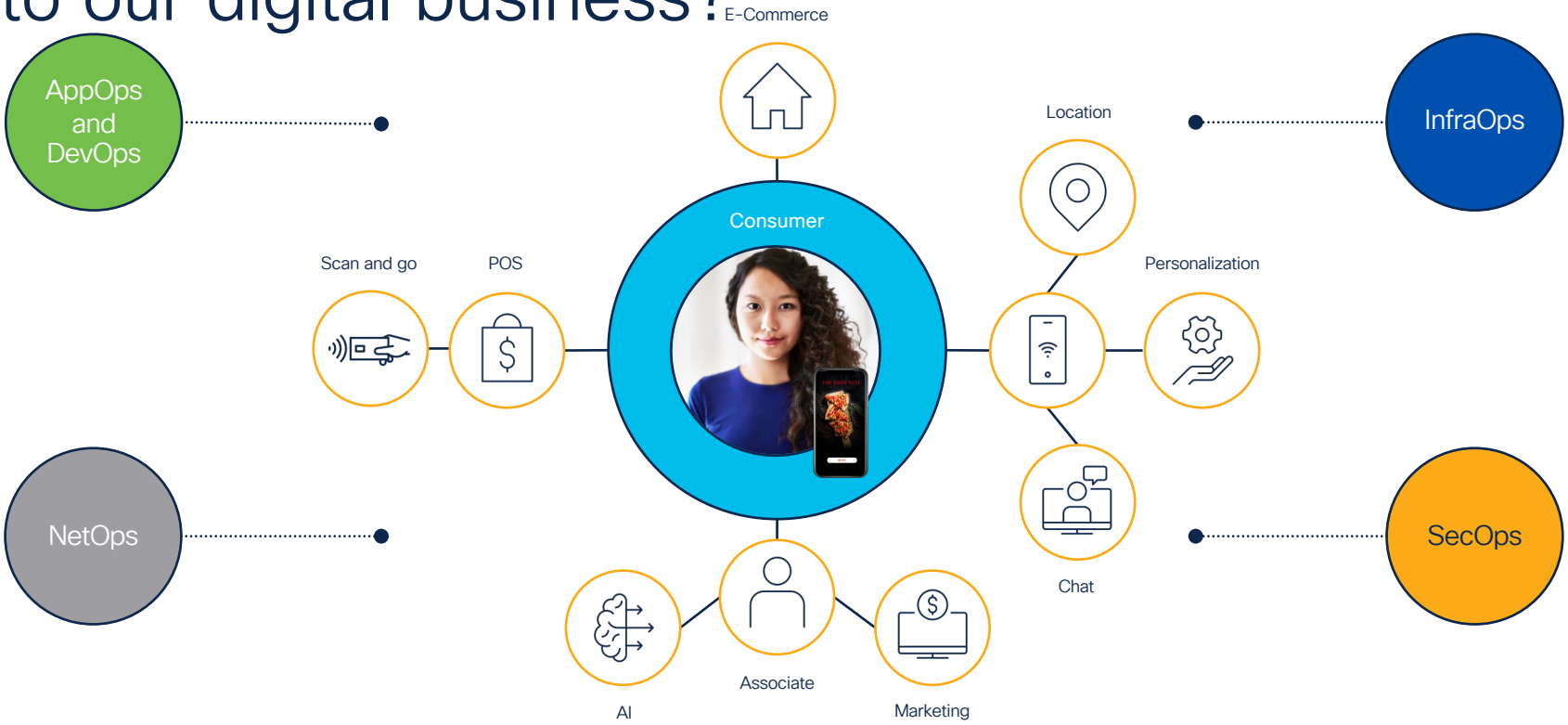
Data Rules

- Apply to targeted sources of data using tags and entities
- Map to one or more expressions
- Supports infra and service logs, but will expand to other telemetry
- Processed at ingest before data is stored



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

Where should we focus our energy to reduce risk to our digital business?

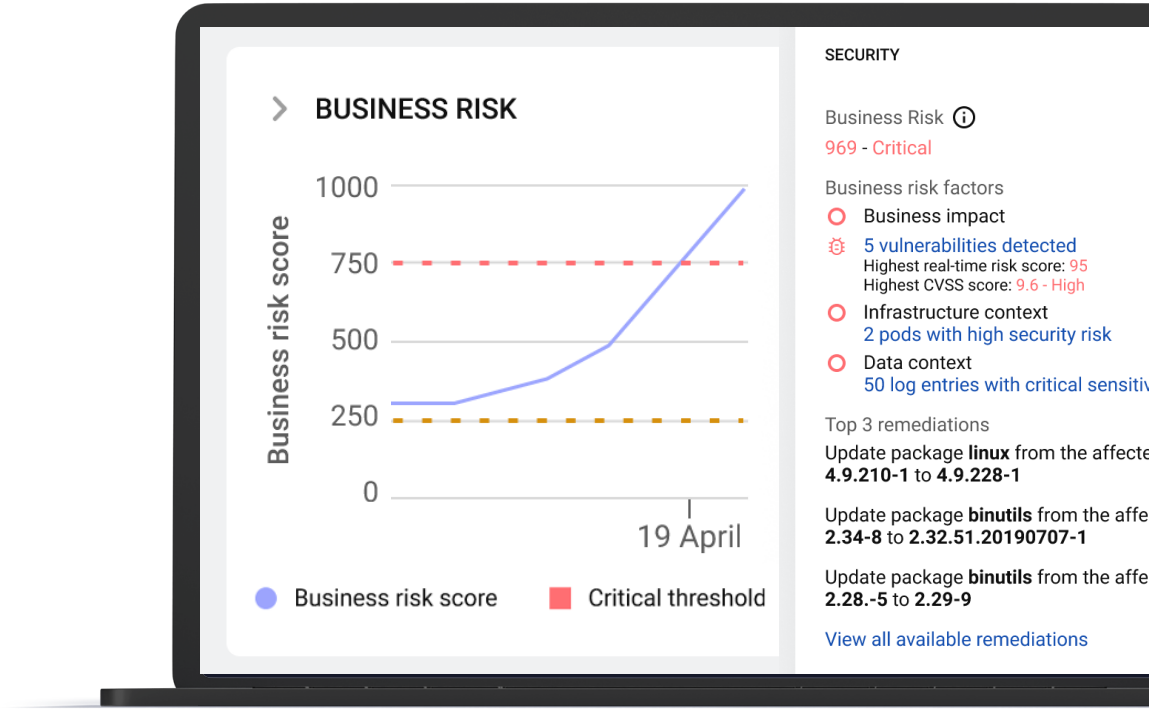


© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

Business Risk Score
Risk scoring with business-context

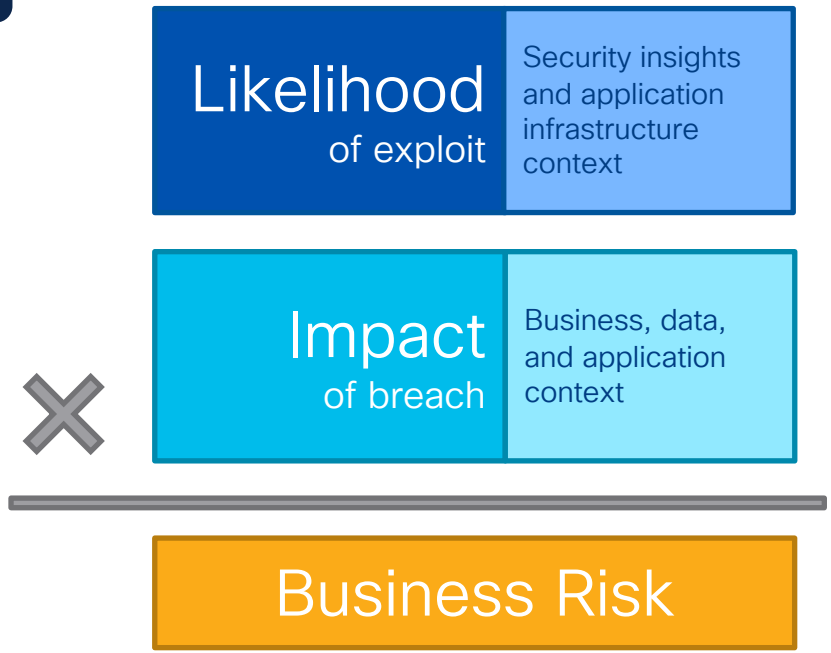
Tailored prioritization based on likelihood and impact

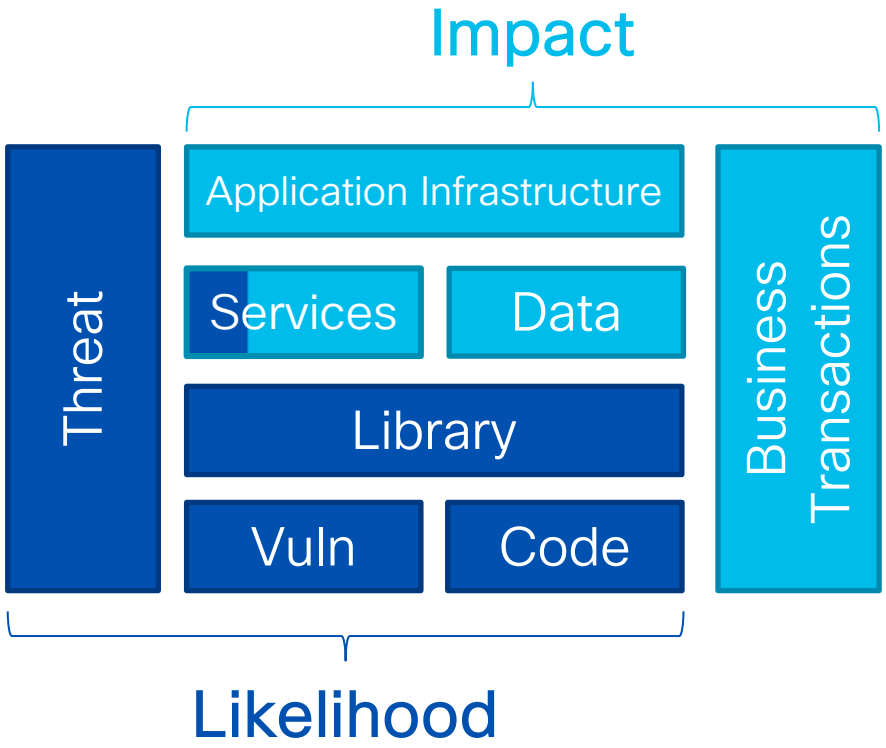
- Builds a customer-specific view of security risk
- Leverage findings and intel from Cisco Kenna and Panoptica
- Continuously assess score reflect real-time risk
- Prioritize remediation and mitigation efforts by what matters to the biz



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

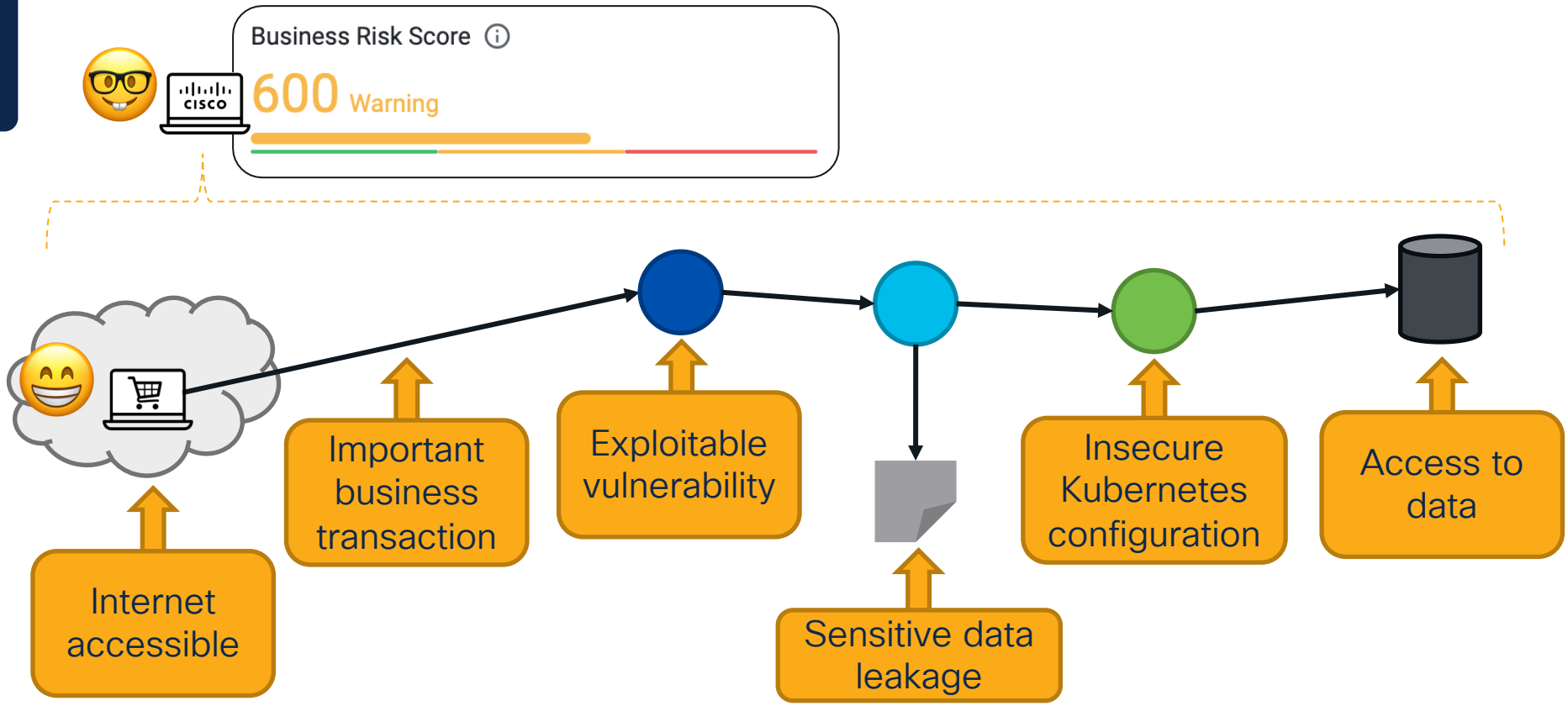
Calculating Business Risk





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

Components of Business Risk assessment



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

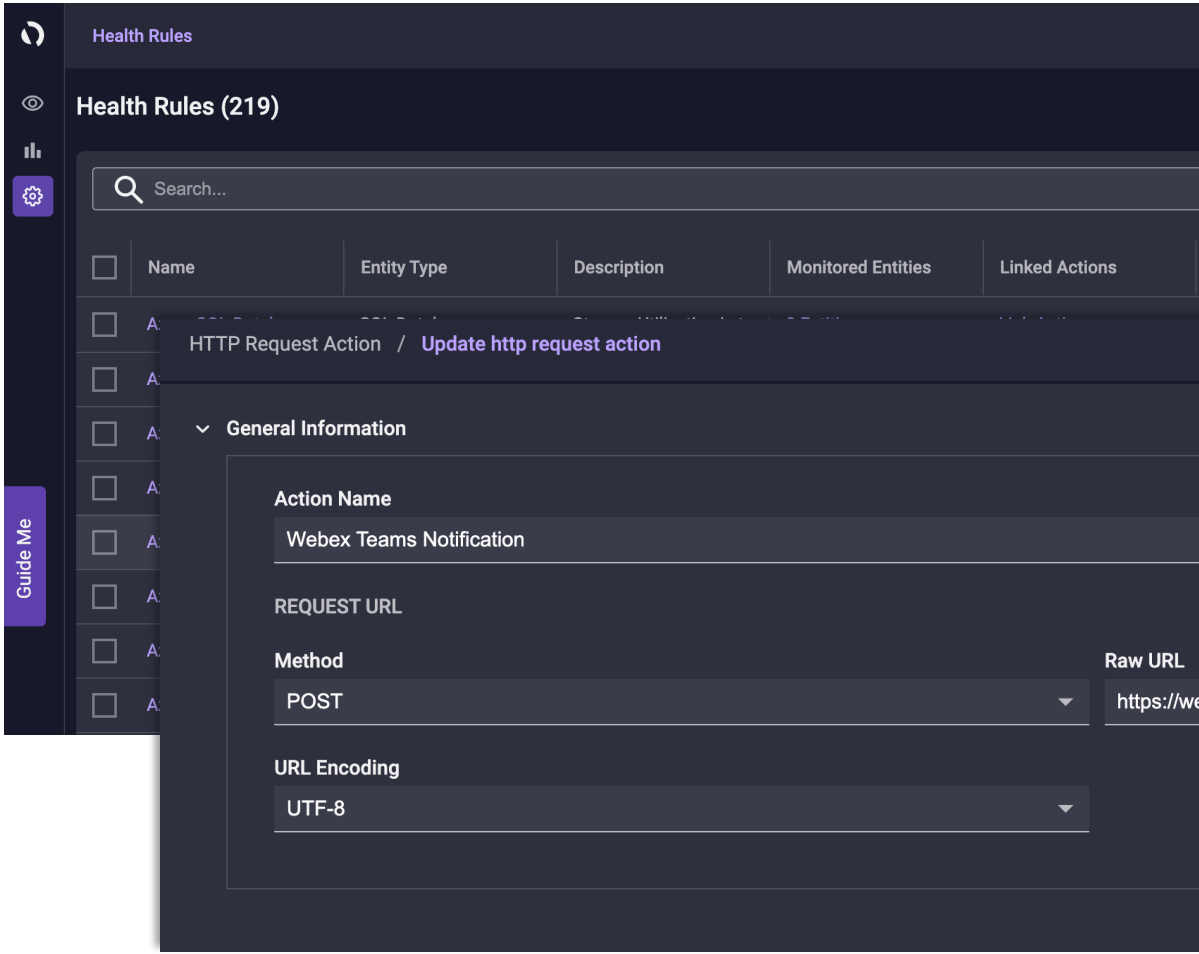
Correlated Alerts & Actions

Health Rules to monitor the key KPIs and take actions as required

Out of the box performance Health Rules based on Metrics Baselines and Thresholds

Custom Health Rules based on security metrics

Create HTTP Actions to integrate and share information with external systems



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

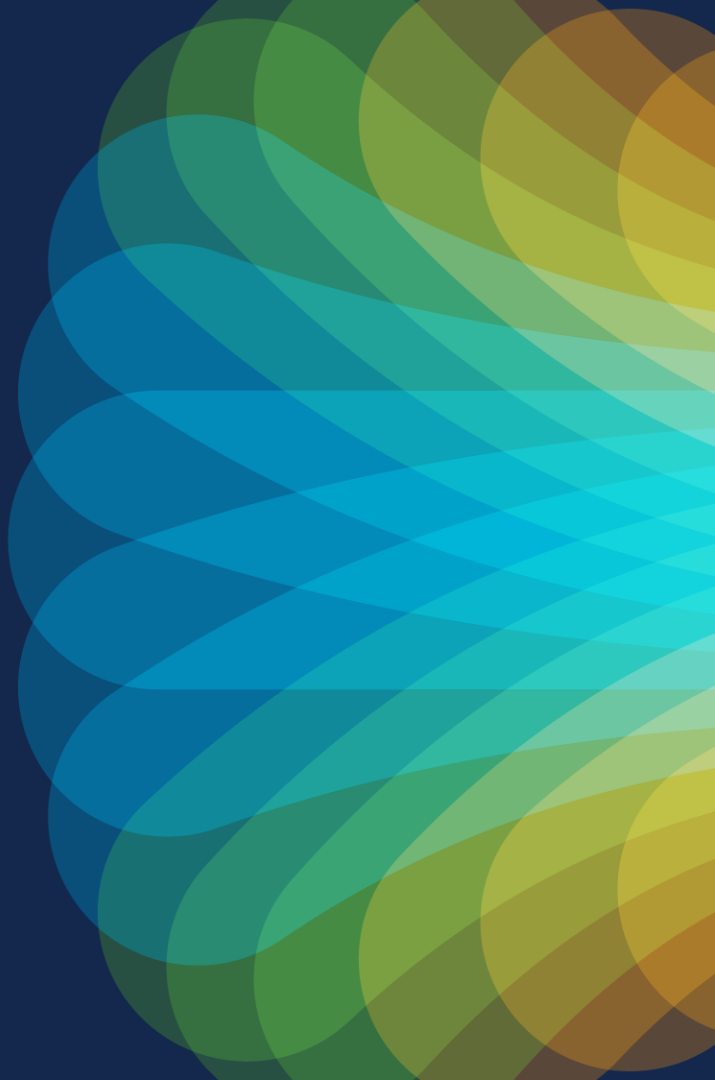
Business Risk Observability Use Case

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

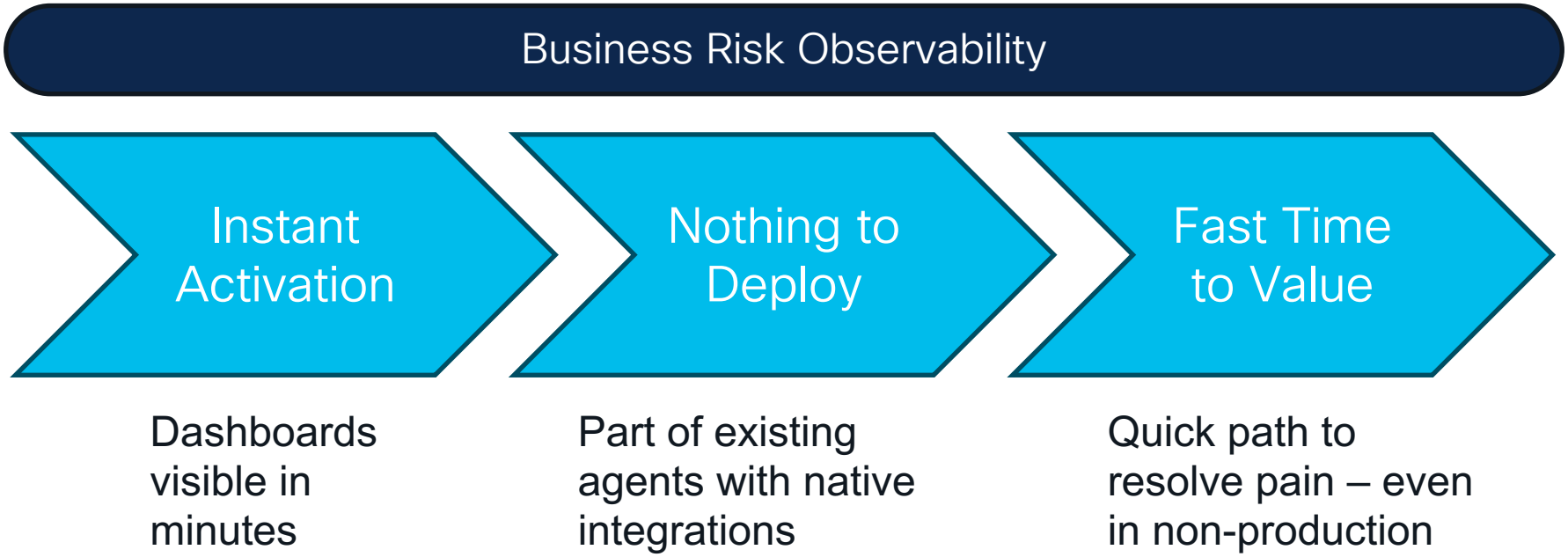
Business Risk Demo
for Cloud Native Applications

cisco Live!

Give me the goods



Zero Friction Enablement



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

Buzz on the street

2021 CyberSecurity Breakthrough Awards

Overall Web Security Solution of the Year

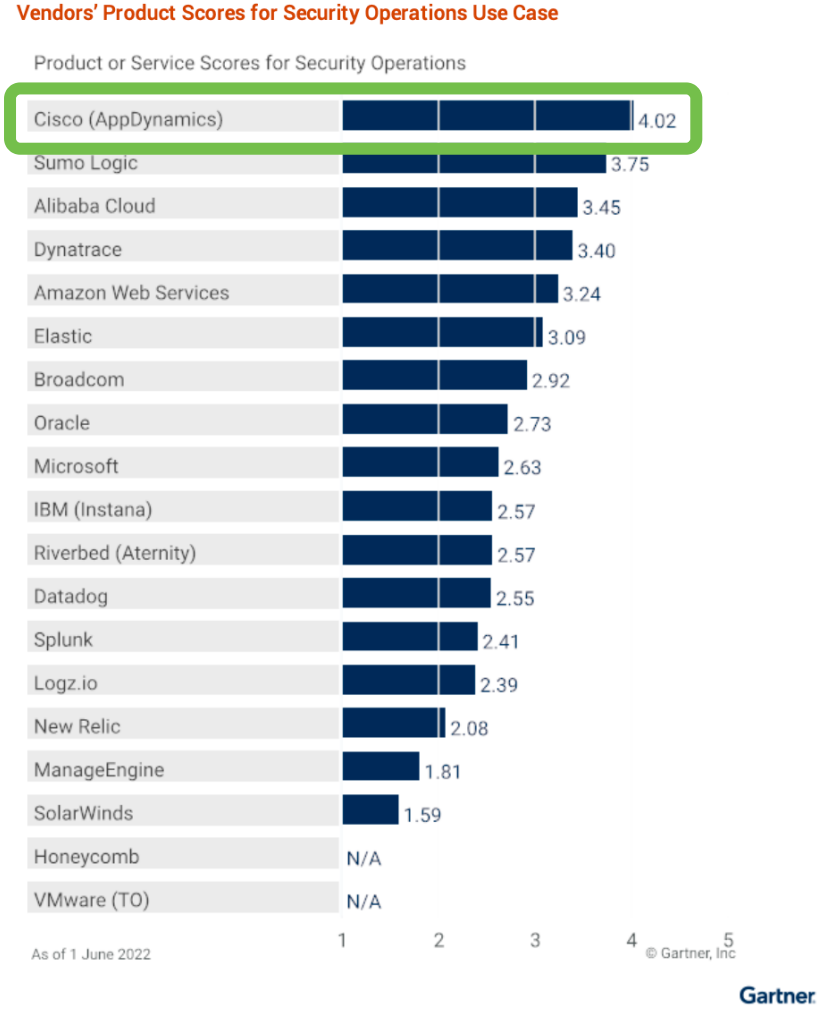
2022 CyberSecurity Excellence Award

Application Security Product of the Year

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

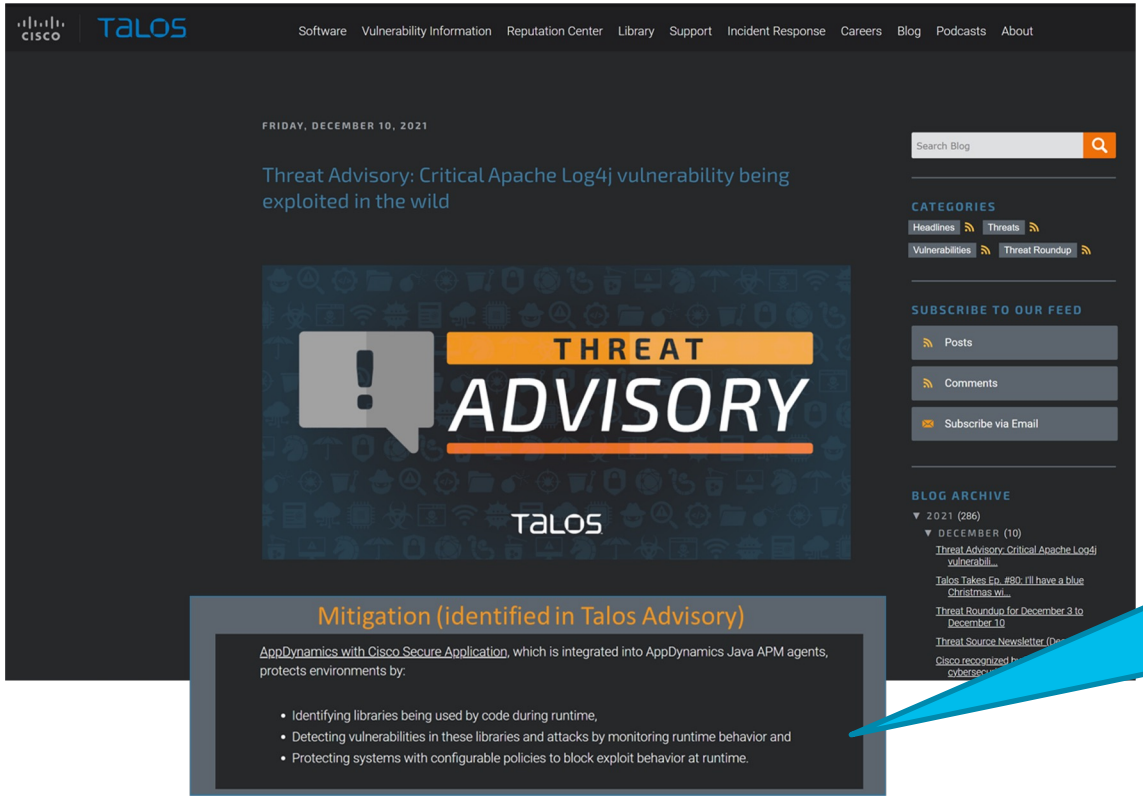
Security is a AppDynamics strength – Gartner

Cisco AppDynamics was ranked #1 by a wide margin in the Gartner 2022 Critical Capabilities report for Security Operations use cases.



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

Award Winning Power on Display

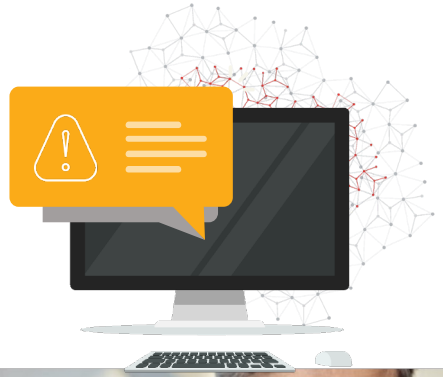


Log4j Vulnerability Mitigation Currently Applies to both CVE-2021-44228 and CVE-2021-45046.

"After days of working around the clock, my team and I can finally get some sleep!"

Director, AppOps @ Travel/Hospitality Customer
December 20, 2021

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



Focused on vulnerabilities & threats

App Team

Security Team

Focused on velocity & user experience

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

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

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

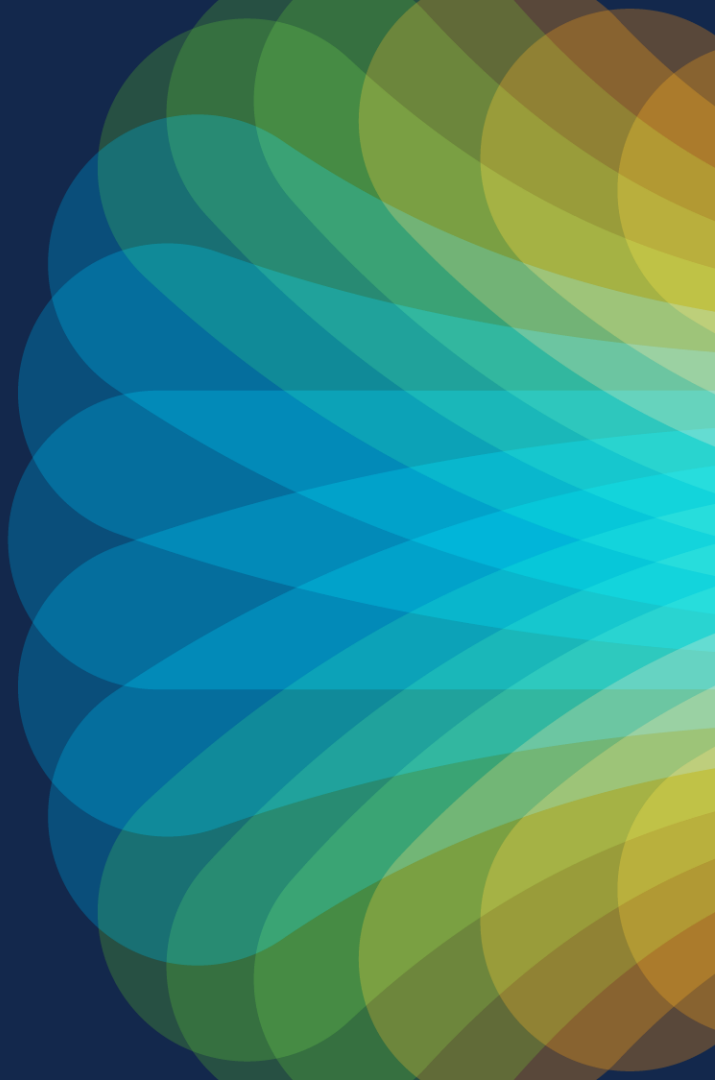
Continue your education

- 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

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

The bridge to possible

Thank you



Let's go