



The bridge to possible

Full-stack Observability (FSO)

Focused on New Features and Strategy

Martin Divis, TSA, Cisco Systems, Central Theatre

BRKAPP-2624

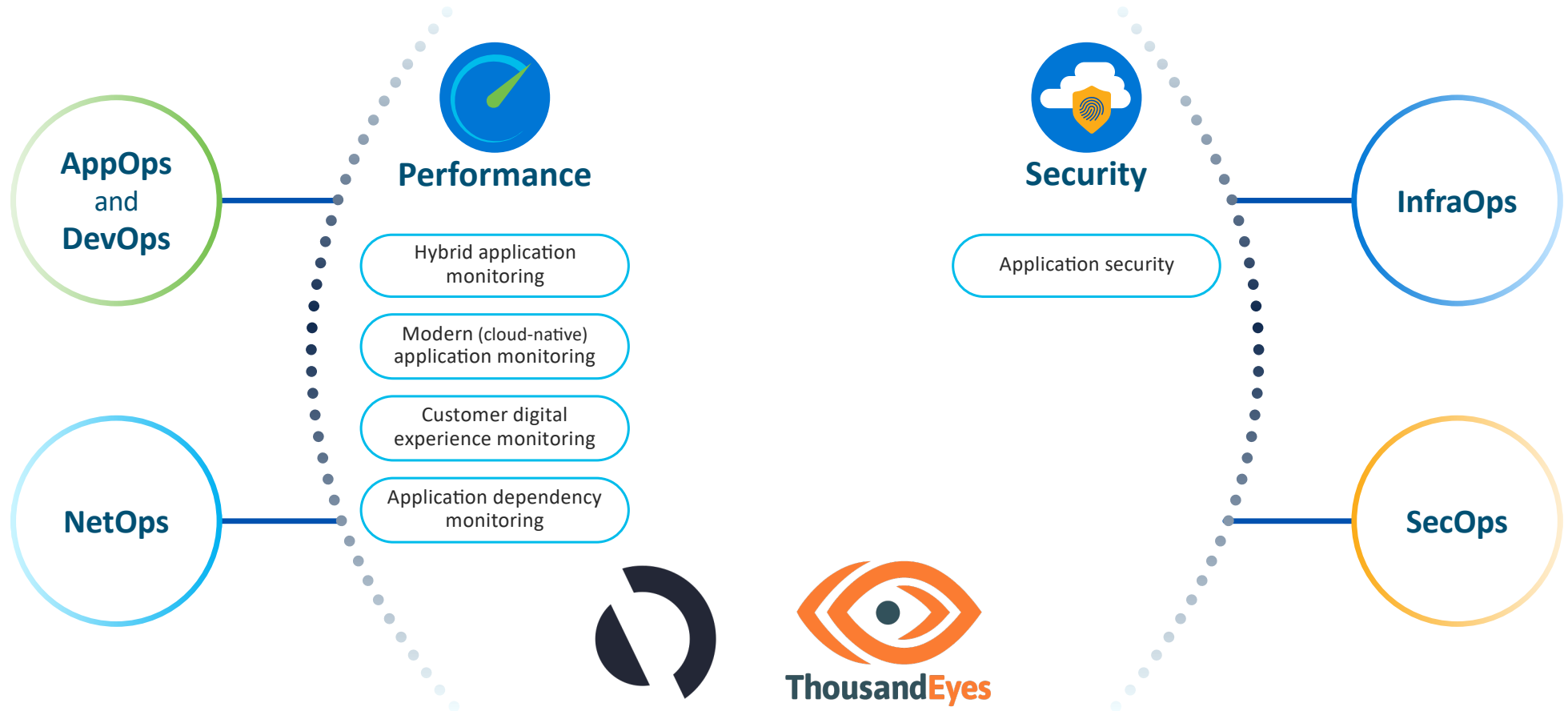


Agenda

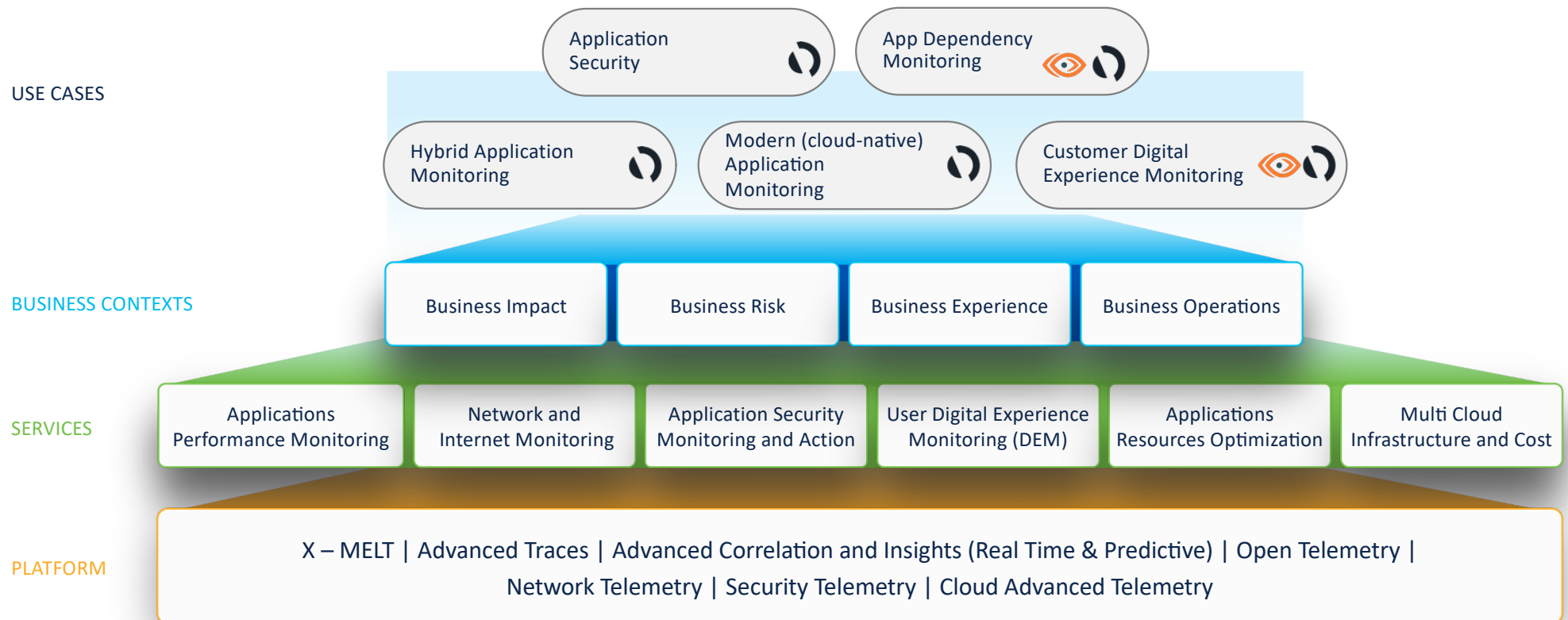
- Introduction to Cisco FSO
- AppDynamics cSaaS – Secure Application solution
- AppDynamics and ThousandEyes integration
- AppDynamics Cloud introduction

Full-Stack Observability

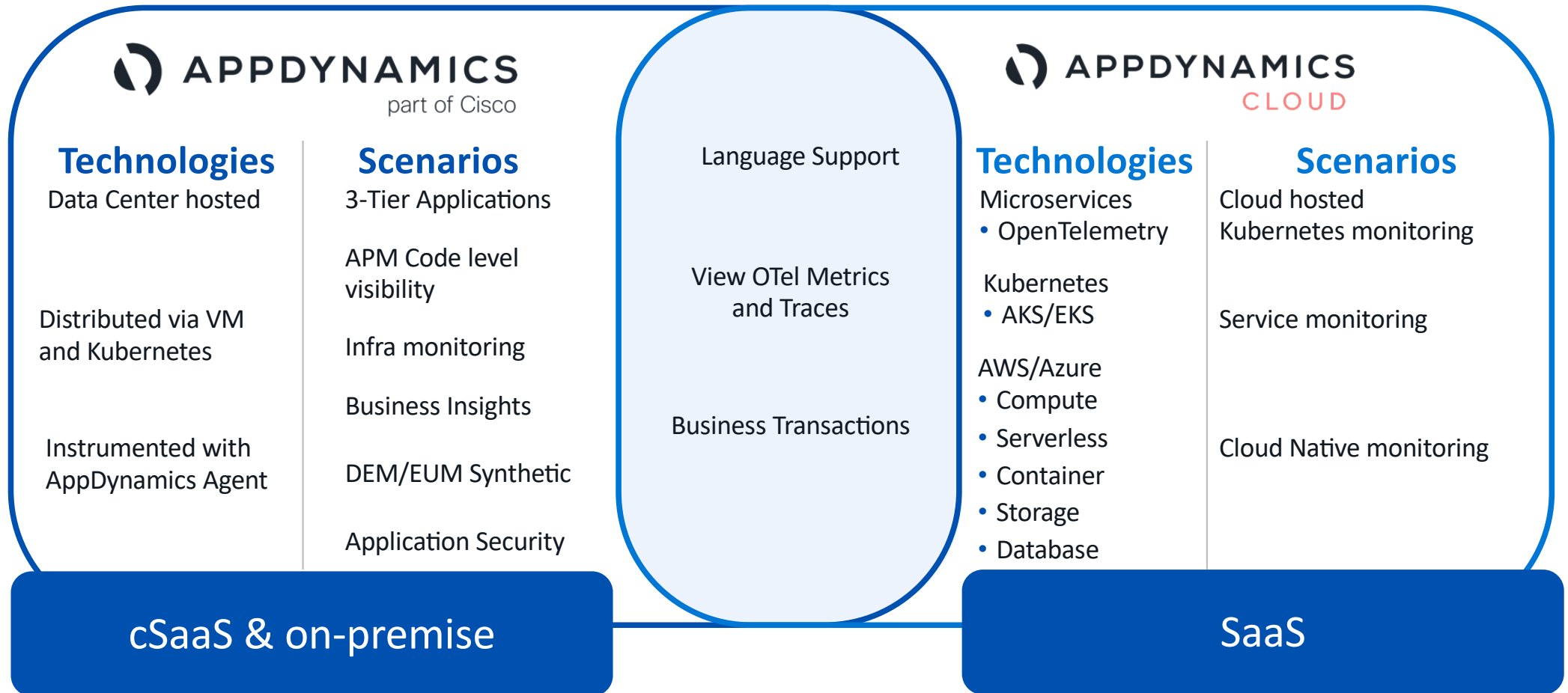
Business context – customer use cases



Cisco full-stack observability architecture foundation



AppDynamics and AppDynamics Cloud



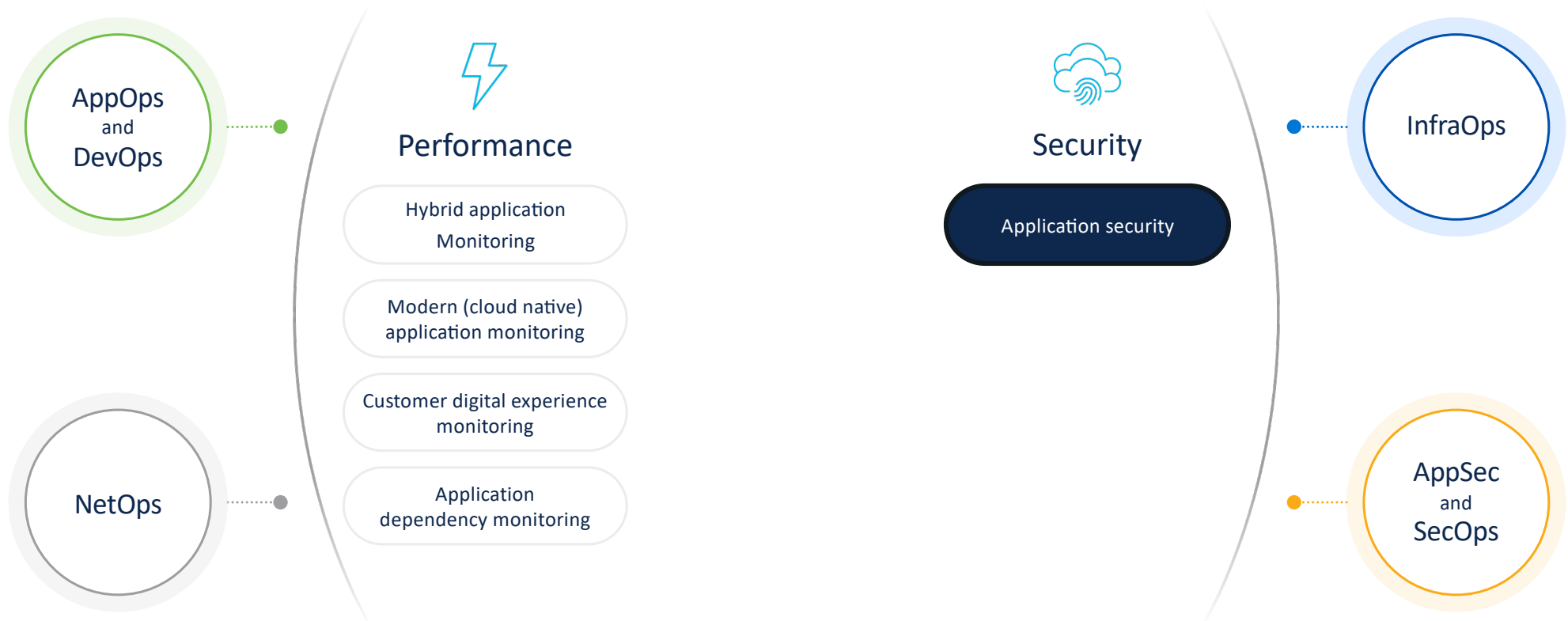
AppDynamics cSaaS Secure Application

Integration of Kenna and Panoptica

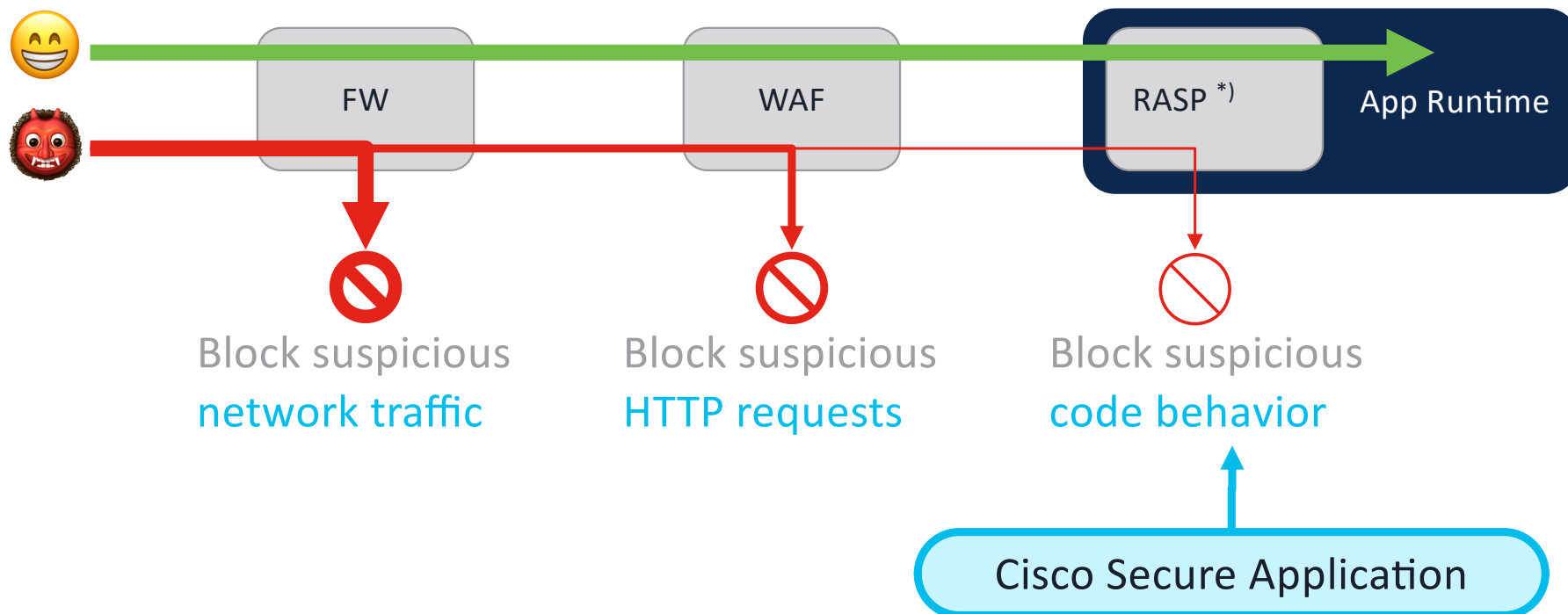


Cisco Full-Stack Observability

With business context – customer use cases



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



*) RASP = Runtime Application Self-Protection

Add application security controls



Sec

Can I add a security tool to your apps?

No.



App

Vulnerability scanning



Sec

I'm scanning our websites on Tues.

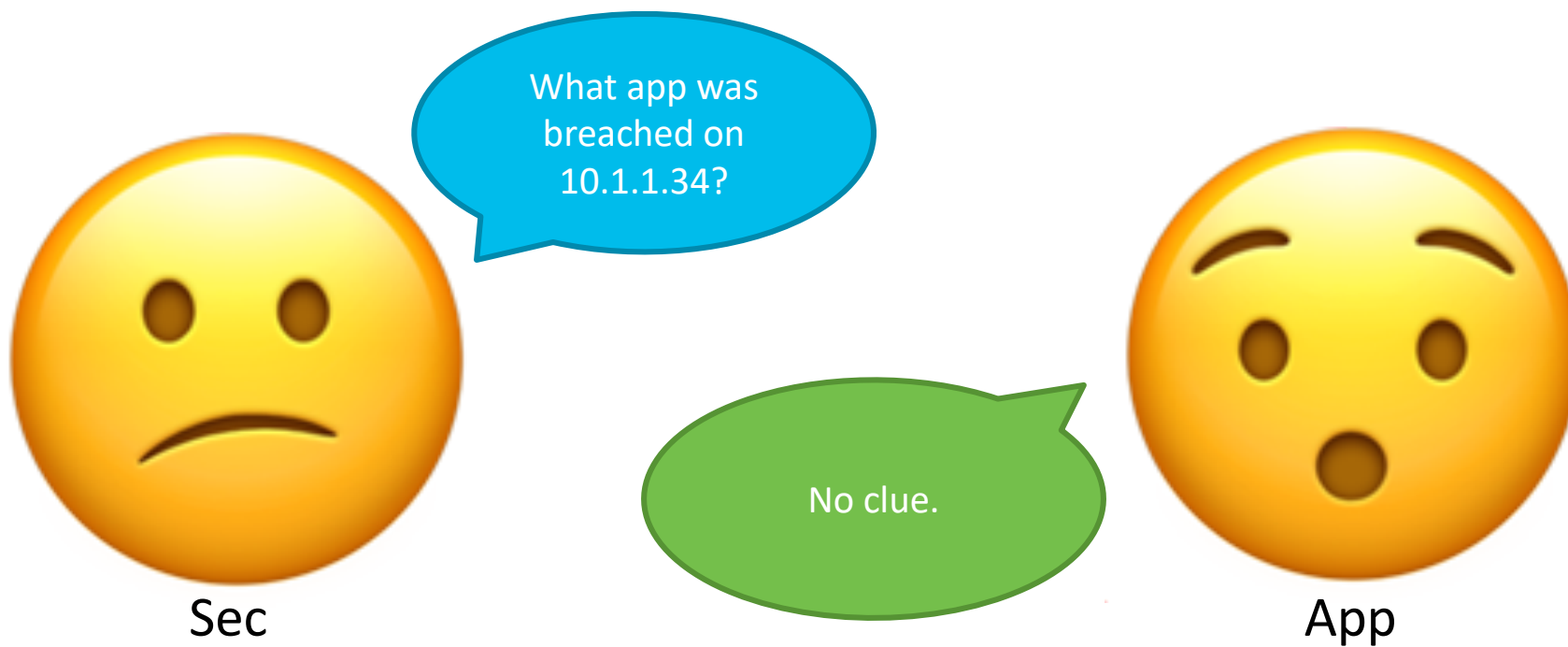


We deploy on Weds.



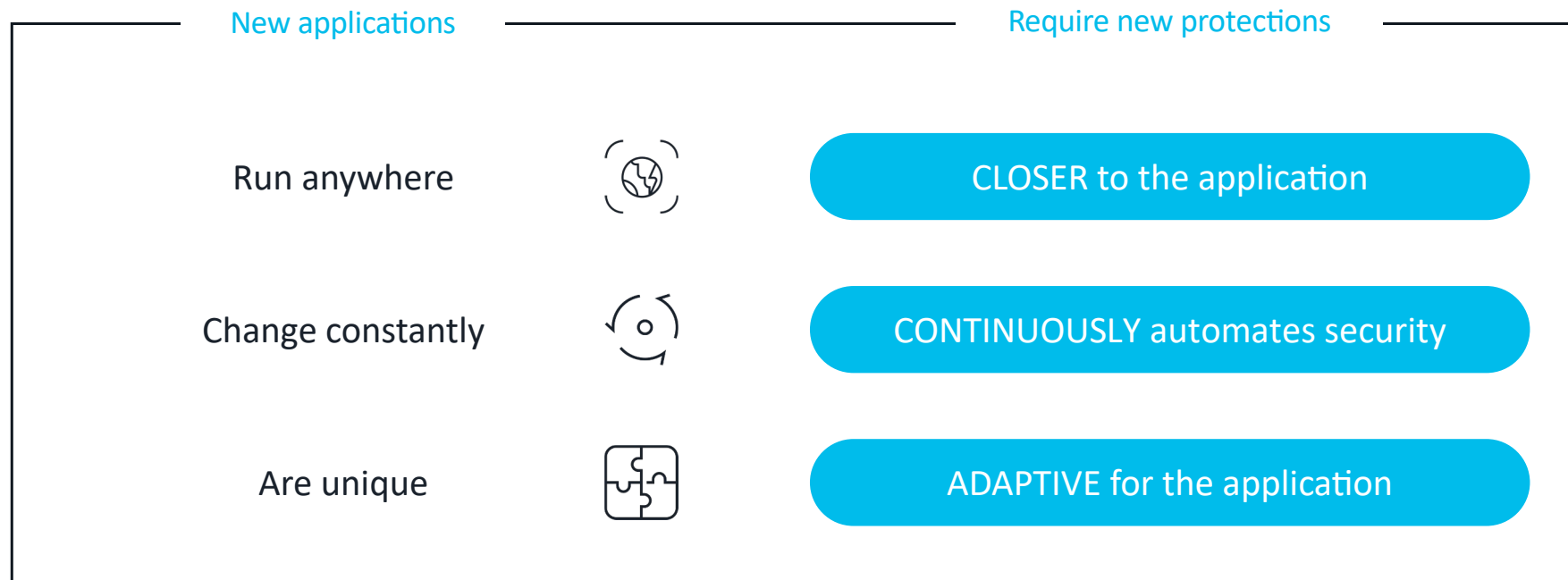
App

Incident investigation



Applications require a new security approach

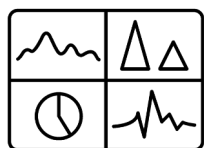
Empowering the digital enterprise to operate with speed and security



Secure Application Use Cases at Runtime

Fast to deploy, immediate time to value, and performant for all environments

Detect Vulnerabilities



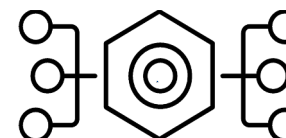
Common Vulnerabilities and Exceptions with Code Level correlation

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

Security insights provided with Application and Business context

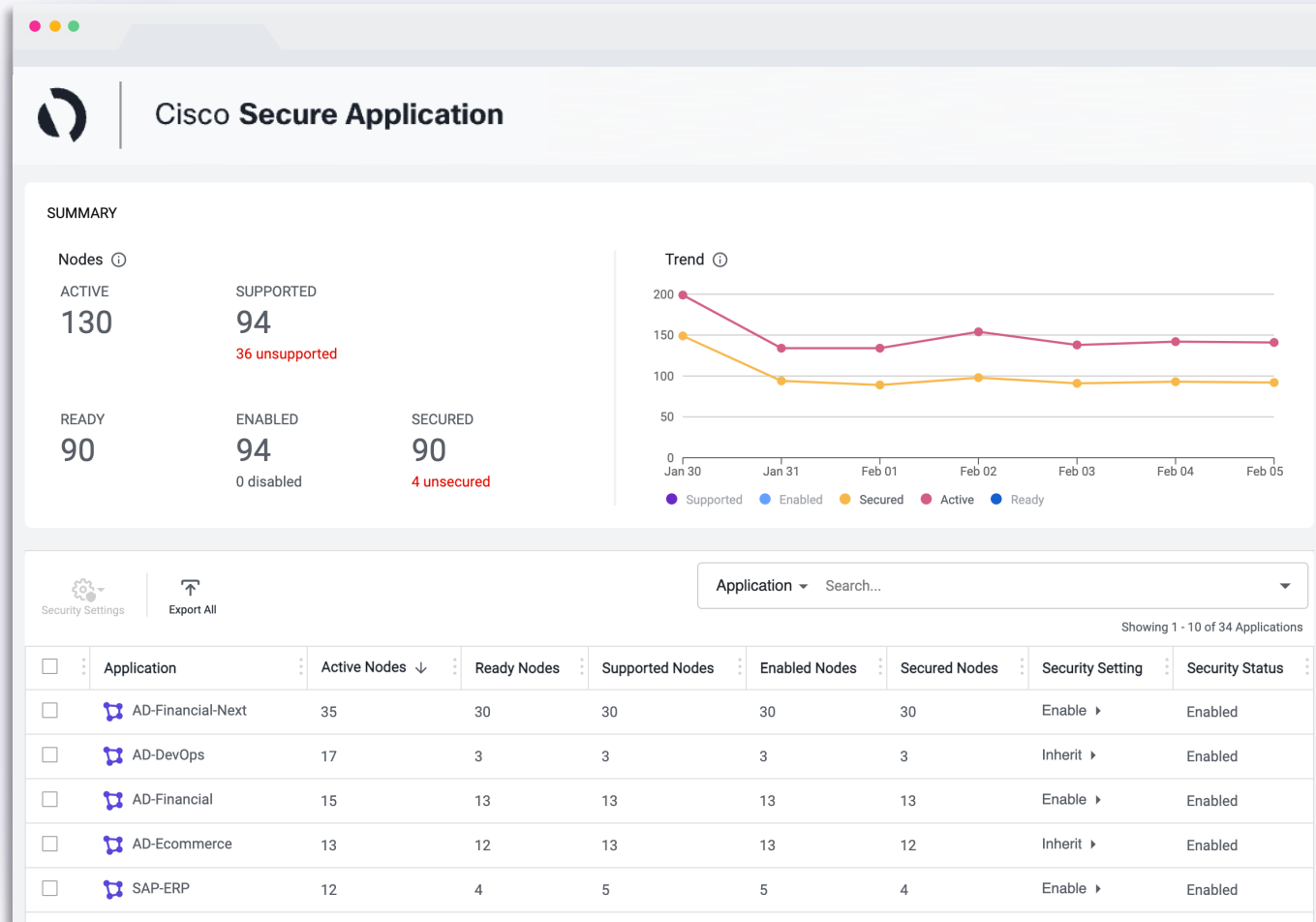
Seamless Onboarding

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



Vulnerability Detection

SAST

static application security testing

Proactive scanning

Source, Build

Inside access

Custom code

SCA

software composition analysis

Proactive scanning

Source, Build, Run

Inside access

Open-source code

DAST

dynamic application security testing

Proactive scanning

Test, Run

Outside access

All code

IAST

interactive application security testing

Reactive scanning

Test, Run

Inside access

All code



Secure Application

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

Vulnerability reports



Sec

Here's the 1000 vulnerabilities I mentioned.

Thanks?!



App

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

Cisco Secure Application

Timestamp: 05-02-2022 09:30:45 EDT
Affected Node: node-20
Event Trigger: 178.175.1.244
Vulnerabilities: [CVE-2021-44228](#)
Entry Point: https://localhost:8088/app/execute?upload=http://178.175.1.244
Client IP: 189.203.158.82 [Investigate in SecureX](#)
Socket Address: 178.175.1.244 Matches Talos Security Intelligence block list
Network Flow: 127.0.0.1:40758 → 127.0.0.1:8088
Judgement: Suspicious [Talos]
Classname: java.net.SocketPermission
Socket Out: 178.175.1.244:443
Method Name: sun.net.www.http.HttpClient.openServer
Api Server External: true
Stack Trace: java.lang.SecurityManager.checkConnect (SecurityManager.java:1051)
sun.net.www.http.HttpClient.openServer (HttpClient.java:51)

Panoptica
Cloud-Native Application Security, Simplified

KENNA
Security

Identify Open-Source Risk

Know what third-party code your apps are actually using

Libraries usage

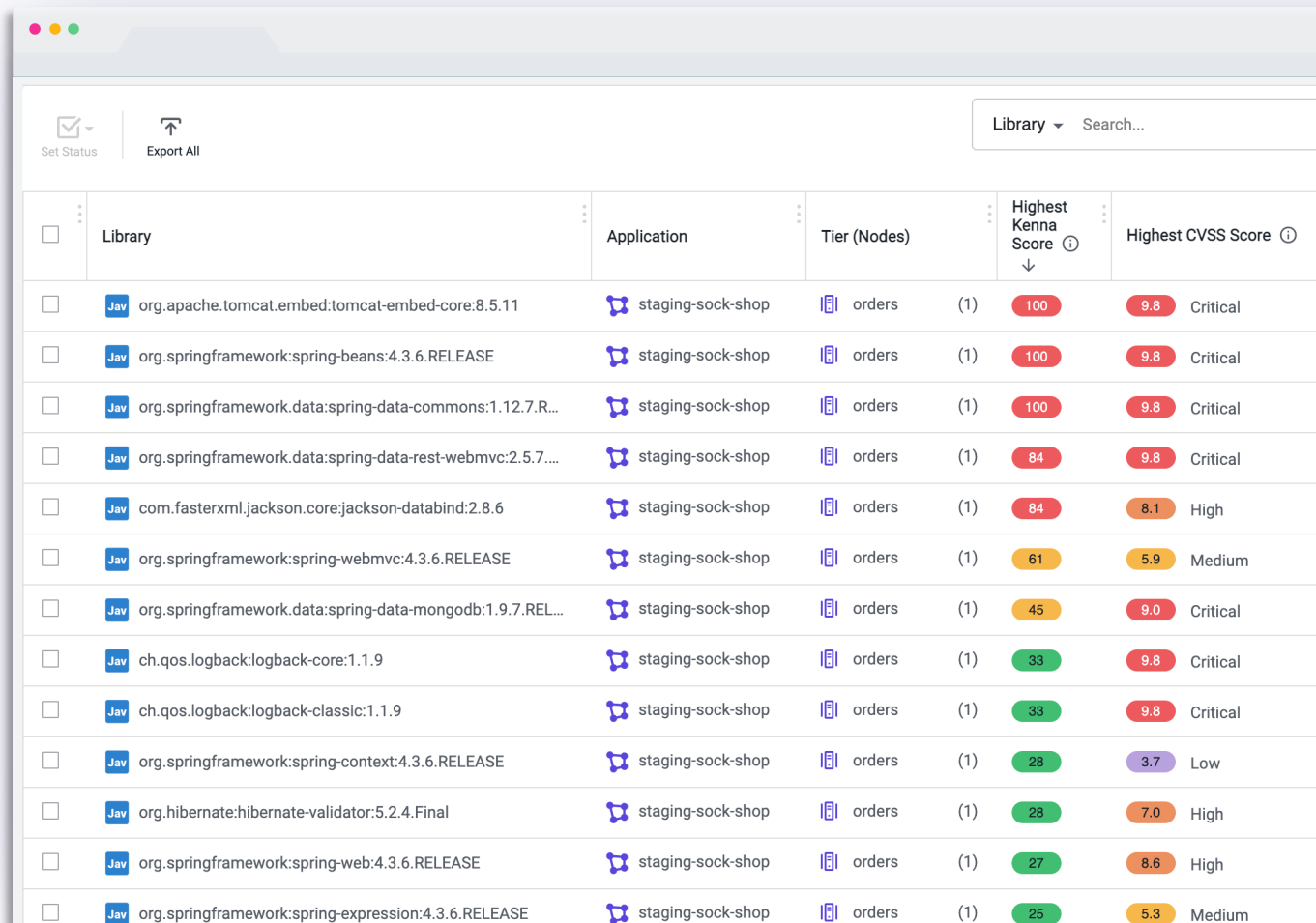
See anytime a library is loaded by your apps

Constant monitoring

Know where vulnerabilities are right after they're disclosed

Remediation guidance

Get fixes out quicker tailored to your environment



<input type="checkbox"/>	Library	Application	Tier (Nodes)	Highest Kenna Score	Highest CVSS Score
<input type="checkbox"/>	org.apache.tomcat.embed:tomcat-embed-core:8.5.11	staging-sock-shop	orders (1)	100	9.8 Critical
<input type="checkbox"/>	org.springframework:spring-beans:4.3.6.RELEASE	staging-sock-shop	orders (1)	100	9.8 Critical
<input type="checkbox"/>	org.springframework.data:spring-data-commons:1.12.7.R...	staging-sock-shop	orders (1)	100	9.8 Critical
<input type="checkbox"/>	org.springframework.data:spring-data-rest-webmvc:2.5.7...	staging-sock-shop	orders (1)	84	9.8 Critical
<input type="checkbox"/>	com.fasterxml.jackson.core:jackson-databind:2.8.6	staging-sock-shop	orders (1)	84	8.1 High
<input type="checkbox"/>	org.springframework:spring-webmvc:4.3.6.RELEASE	staging-sock-shop	orders (1)	61	5.9 Medium
<input type="checkbox"/>	org.springframework.data:spring-data-mongodb:1.9.7.REL...	staging-sock-shop	orders (1)	45	9.0 Critical
<input type="checkbox"/>	ch.qos.logback:logback-core:1.1.9	staging-sock-shop	orders (1)	33	9.8 Critical
<input type="checkbox"/>	ch.qos.logback:logback-classic:1.1.9	staging-sock-shop	orders (1)	33	9.8 Critical
<input type="checkbox"/>	org.springframework:spring-context:4.3.6.RELEASE	staging-sock-shop	orders (1)	28	3.7 Low
<input type="checkbox"/>	org.hibernate:hibernate-validator:5.2.4.Final	staging-sock-shop	orders (1)	28	7.0 High
<input type="checkbox"/>	org.springframework:spring-web:4.3.6.RELEASE	staging-sock-shop	orders (1)	27	8.6 High
<input type="checkbox"/>	org.springframework:spring-expression:4.3.6.RELEASE	staging-sock-shop	orders (1)	25	5.3 Medium

API Security Insights

Identify risk introduced by 3rd-party APIs

Discover API usage

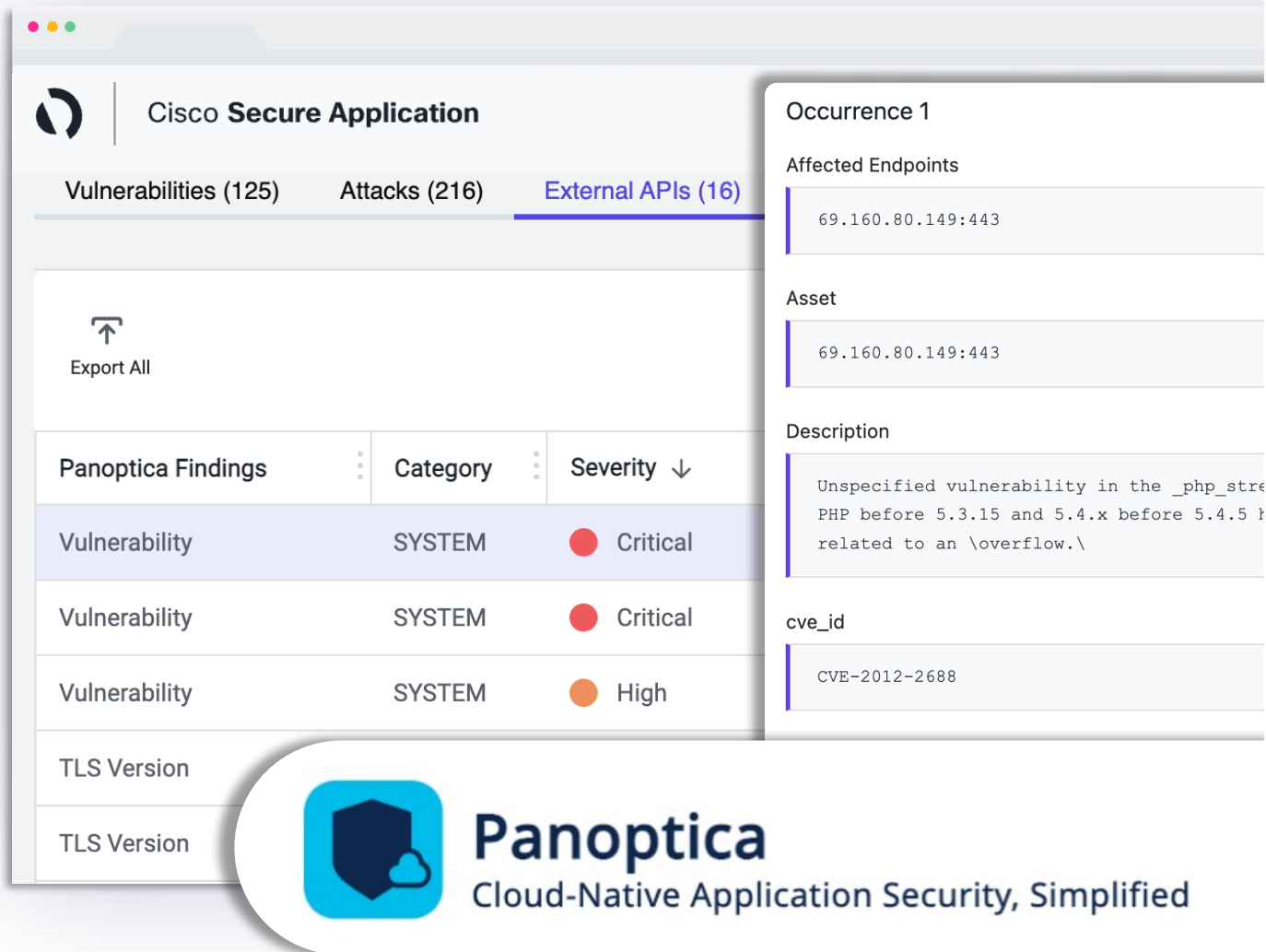
Automatically detect when services rely on 3rd-party APIs

Leverage Panoptica API intelligence

Native backend integration provides security findings

Factor in business risk

Combine findings into application context for business risk scoring



The screenshot displays the Cisco Secure Application interface. At the top, there are navigation tabs for 'Vulnerabilities (125)', 'Attacks (216)', and 'External APIs (16)'. Below these is an 'Export All' button. A table lists findings with columns for 'Panoptica Findings', 'Category', and 'Severity'. The table contains three rows of 'Vulnerability' findings, all categorized as 'SYSTEM'. The first two are 'Critical' (red dot) and the third is 'High' (orange dot). A right-hand sidebar shows details for 'Occurrence 1', including 'Affected Endpoints' (69.160.80.149:443), 'Asset' (69.160.80.149:443), and a 'Description' of an unspecified vulnerability in the _php_stre PHP before 5.3.15 and 5.4.x before 5.4.5 related to an overflow. The 'cve_id' is listed as CVE-2012-2688. At the bottom, the Panoptica logo and tagline 'Cloud-Native Application Security, Simplified' are visible.

Panoptica Findings	Category	Severity
Vulnerability	SYSTEM	Critical
Vulnerability	SYSTEM	Critical
Vulnerability	SYSTEM	High

Panoptica
Cloud-Native Application Security, Simplified

AppDynamics cSaaS ThousandEyes Integration

Extending the End User Monitoring



User Experience Monitoring

Real User Monitoring

- Monitors real users experience with an application
- Correlation to backend side of application processing
- Statistics on demography, OS versions etc.
- Web application monitoring
 - Simple web applications
 - Single-page applications (React, Angular, Vue,..)
- Mobile applications
 - Android - Java, Kotlin, Flutter
 - Apple IOS – Swift, Flutter

User Experience Monitoring

Synthetic Monitoring

- Emulation of user-actions for web applications
- Both AppDynamics and ThousandEyes – which to take? It depends...

AppDynamics Synthetic Monitoring	ThousandEyes
Cloud (a few of) and private systems with browser emulators	Cloud (a lot of) and private systems with browser emulators (agents)
Integral part of end user monitoring	Deployable on network devices
Programmed in Python	Programmed in Javascript
API monitoring	API monitoring, also from user endpoints
Can take screenshots	Monitoring of 3rd party and SaaS applications
Correlation to backend business transaction monitoring	Network path analysis
Support for CI/CD pipelines	Network services availability monitoring (DNS, BGP)
	Integration with AppDynamics
	Internet Insights

TE Onboarding in AppDynamics

End User Experience

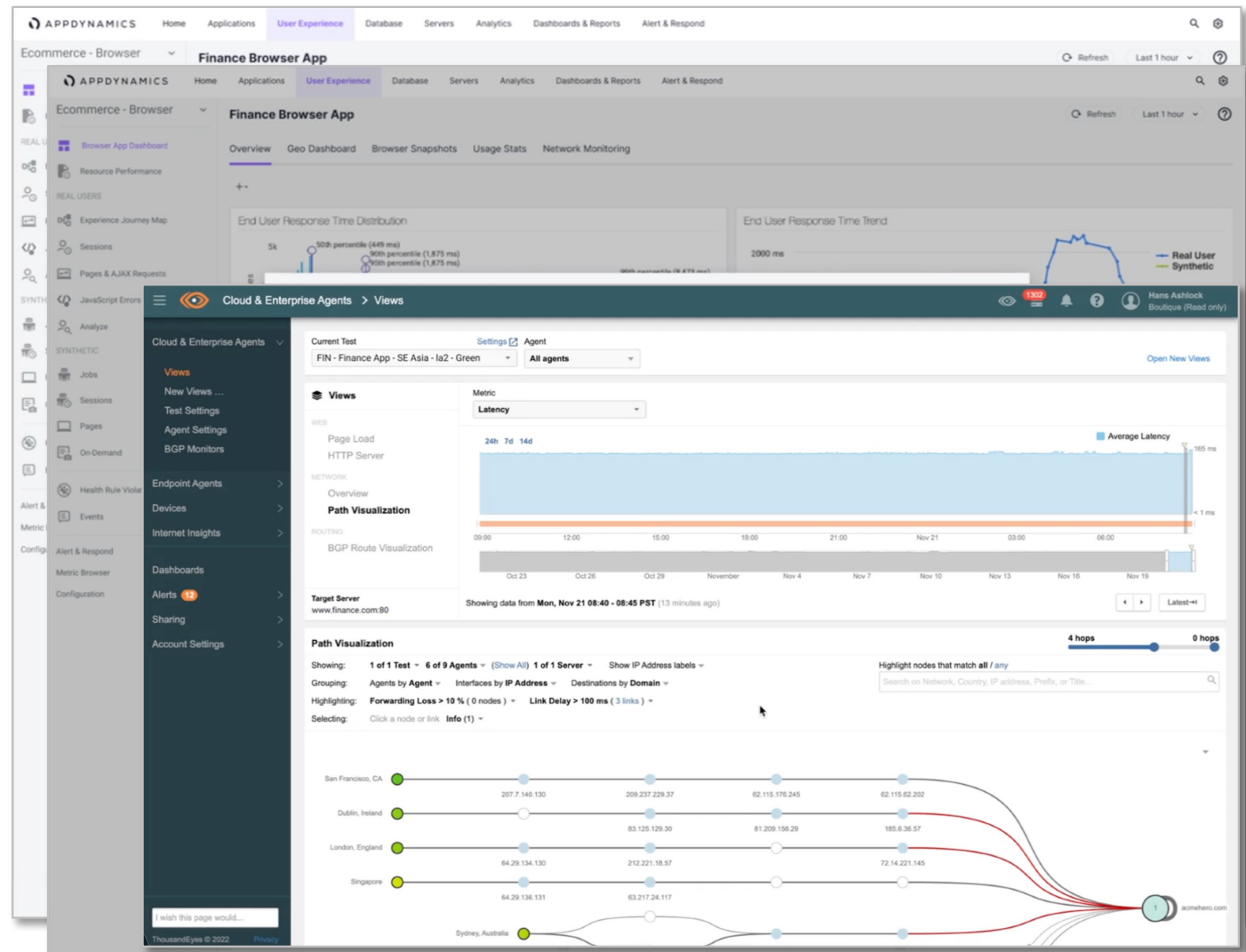
- Easy wizard based onboarding
- Backend-to-backend integration
- Bind TE tests based on domains in EUM

The screenshot displays the AppDynamics User Experience dashboard. The main interface includes a navigation bar with 'APPDYNAMICS' and various menu items like 'Home', 'Applications', 'User Experience', 'Database', 'Servers', 'Analytics', 'Dashboards & Reports', and 'Alert & Respond'. Below the navigation, there are tabs for 'Browser Apps', 'Mobile Apps', 'Connected Devices', and 'API Monitoring'. A table lists various applications with columns for 'Name', 'Requests', 'Requests per Minute', 'Errors', 'Error Rate', 'Response Time (ms)', 'Synthetic Availability', 'Synthetic Response Time (ms)', and 'Monitoring Enabled'. Overlaid on this is a 'Synchronise with ThousandEyes' dialog box. The dialog features the AppDynamics logo on the left and the ThousandEyes logo on the right, connected by a double-headed arrow. A large green checkmark is centered above the text: 'Success! ThousandEyes tests Matched to 32 domains in 7 apps'. A 'Continue' button is at the bottom of the dialog. In the background, another 'Synchronise with ThousandEyes' dialog is visible, and a 'Next: Sync' button is located in the bottom right corner of the main interface.

AppDynamics EUM dashboard

Single Pane of Glass

- Visual correlation of EUM and TE metrics
- Interactive TE widgets
- Easy handoff to TE



AppDynamics in ThousandEyes

Easy integration

- Backend-to-backend integration
- Create TE tests based on EUM domains

The screenshot shows the ThousandEyes interface with the AppDynamics Integration section. The main dashboard displays a grid of test results for various AppDynamics services. The services and their results are as follows:

Service	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7
Application Health	Good	Good	Bad	Good	Good	Good	Bad
Application Services Health	Degraded	Bad	Bad	Good	Degraded	Degraded	Good
HTTP Server Availability	100	98.97	0	100	99.9	99.9	65.16
Network Loss	0	0	9.8	0.1	0.2	0	2.16
Network Latency	12	23	234	23	24	24	65.16
Network Jitter	0	0	12.7	0	12.7	0	5.16

The interface also shows a list of tests with columns for Test Name, Test Type, Alert Status, and Threshold (50%) Current Values. The tests listed include:

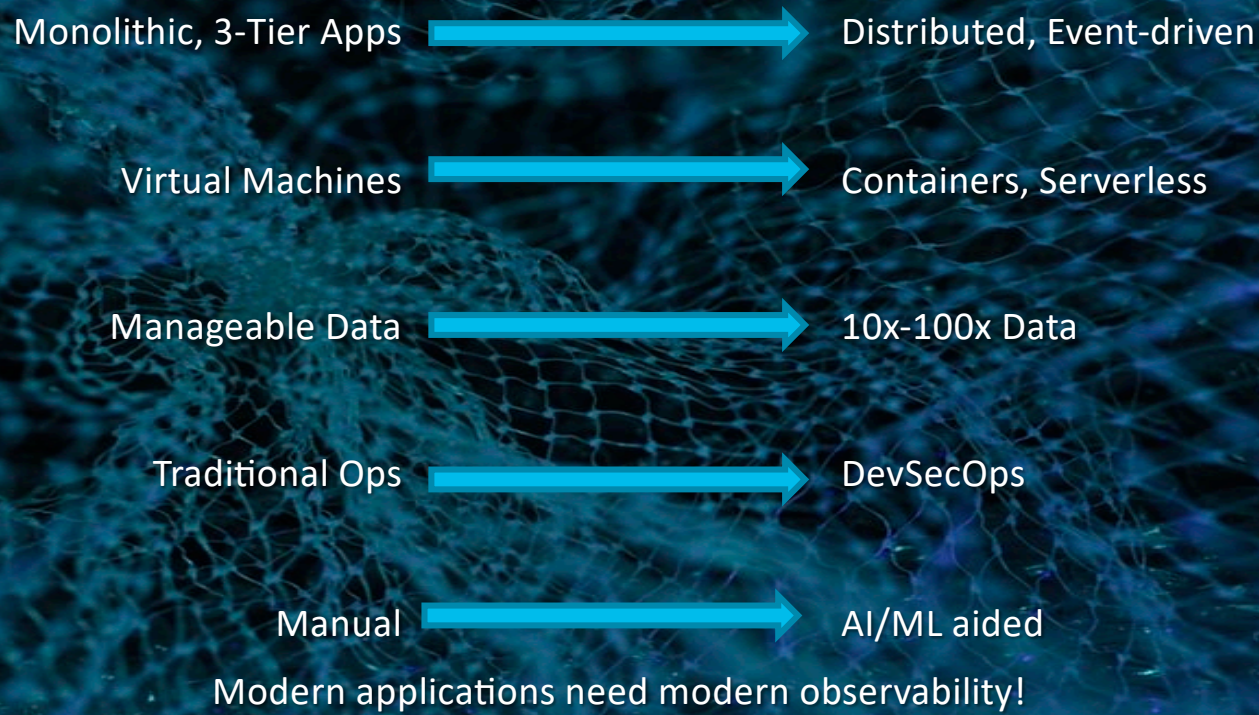
- FIN - Finance Dev - SE Asia
- FIN - Finance Dev API
- FIN - Finance Dev Payment
- FIN - Finance Dev Auth
- FIN - Finance Dev Auth2
- FIN - Finance Dev AMS
- FIN - Finance Dev Chat
- FIN - Finance Dev non-prod
- FIN - Finance Dev permsbs
- FIN - Finance Dev McAfee
- FIN - Finance Dev confuent-tim
- FIN - Finance Dev Sendgrid
- fonts.googleapis.com

AppDynamics Cloud

Introduction



The application world has changed



FSO Platform

Single platform for Cisco and 3rd party FSO applications

Multi-product integration platform

Ingestion and storage for compute, networking, security, public and hybrid clouds

Cross-MELT troubleshooting

Anomaly detection and root cause analysis services across metrics, events, logs and traces

Multiple sources → Single entity

MELT from multiple collectors are combined for a single entity view for multi-dimensional visibility

Extensibility

Cross-MELT | Advanced Traces | Advanced Correlation and Insights
(Real time/ Predictive)

Open Telemetry | Network / Security / Cloud advanced telemetry

Cross-MELT AD Troubleshooting

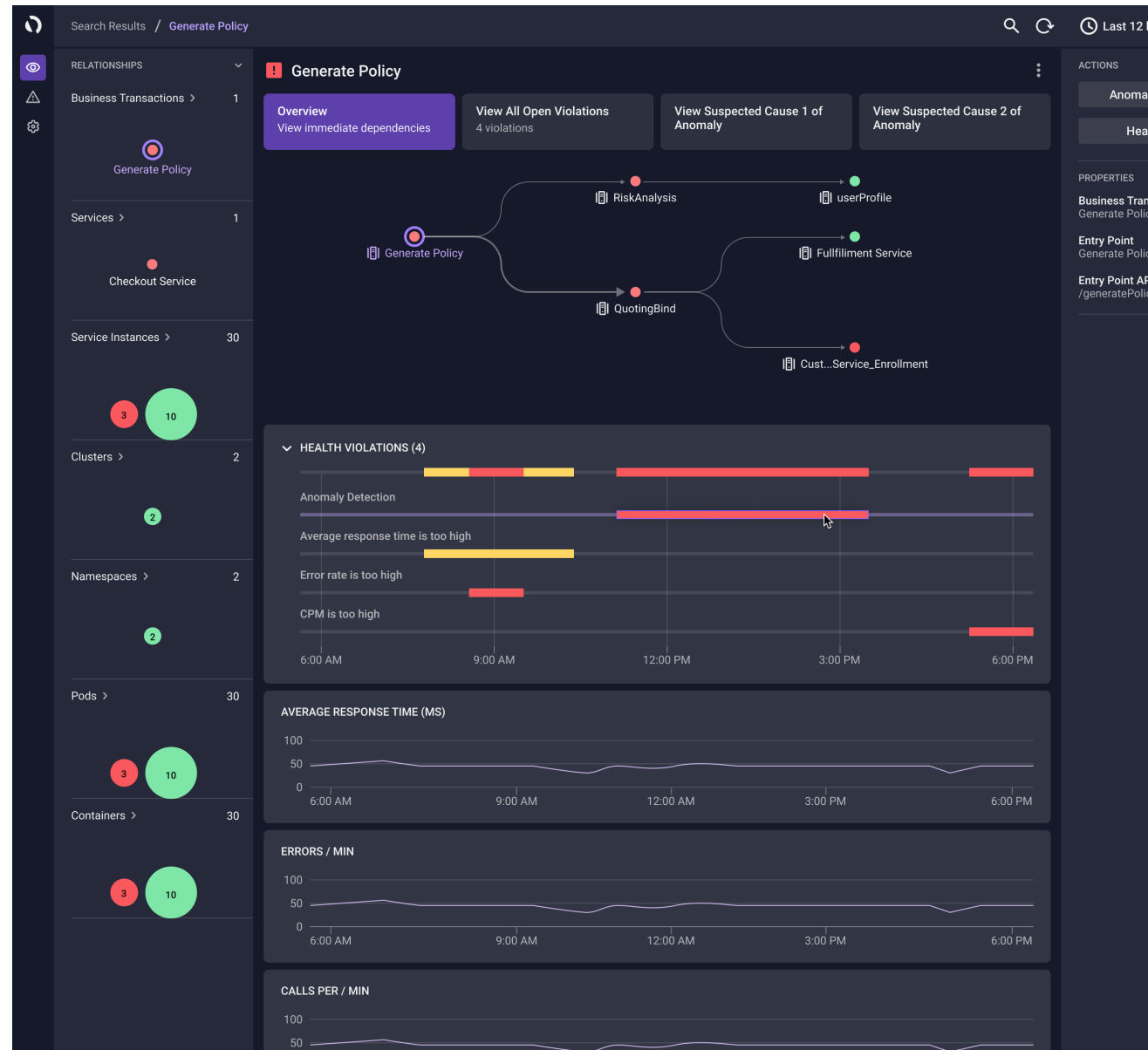
Leverage AI to reduce mean
time to resolution (MTTR)

Detect Cross-Domain Anomalies Alert
across K8s, services & cloud metrics

Anomaly Detection for BTs
Identify issues aligned to business objects

Correlate Alerts
Reduce alert noise for related issues using
topology and time

Cross-Domain RCA
Extend root cause from service layer to
infrastructure layer



The power of AppDynamics Cloud

1

Purpose Built Platform for
cloud-native Observability
AWS & Azure & Openshift OnPrem

2

Contextual awareness from any
telemetry source

3

Resolve issues faster with AI
model-driven remediation

Public Cloud Visibility

Troubleshoot public cloud
infra and correlate to APM

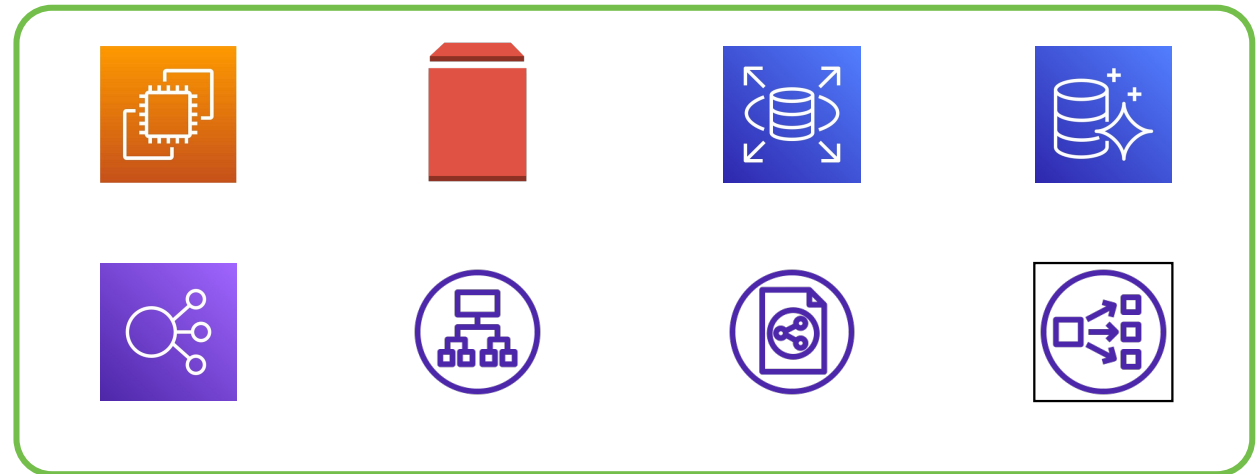
Expanding services coverage for
greater breadth

Cloud service log collection for
agentless access to S3 buckets
and CloudWatch log groups

Correlated metric and log analysis
to uncover root cause



Available NOW



By January

Feb-Apr



Public Cloud Visibility

Troubleshoot public cloud infra
and correlate to APM

Expanding services coverage for
greater breadth

Cloud service log collection for
agentless access Azure Monitor log
groups

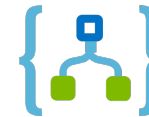
Correlated metric and log analysis to
uncover root cause



Available NOW



Feb-Apr



May-Nov

App Gateway | Container | Table Storage | API Manager

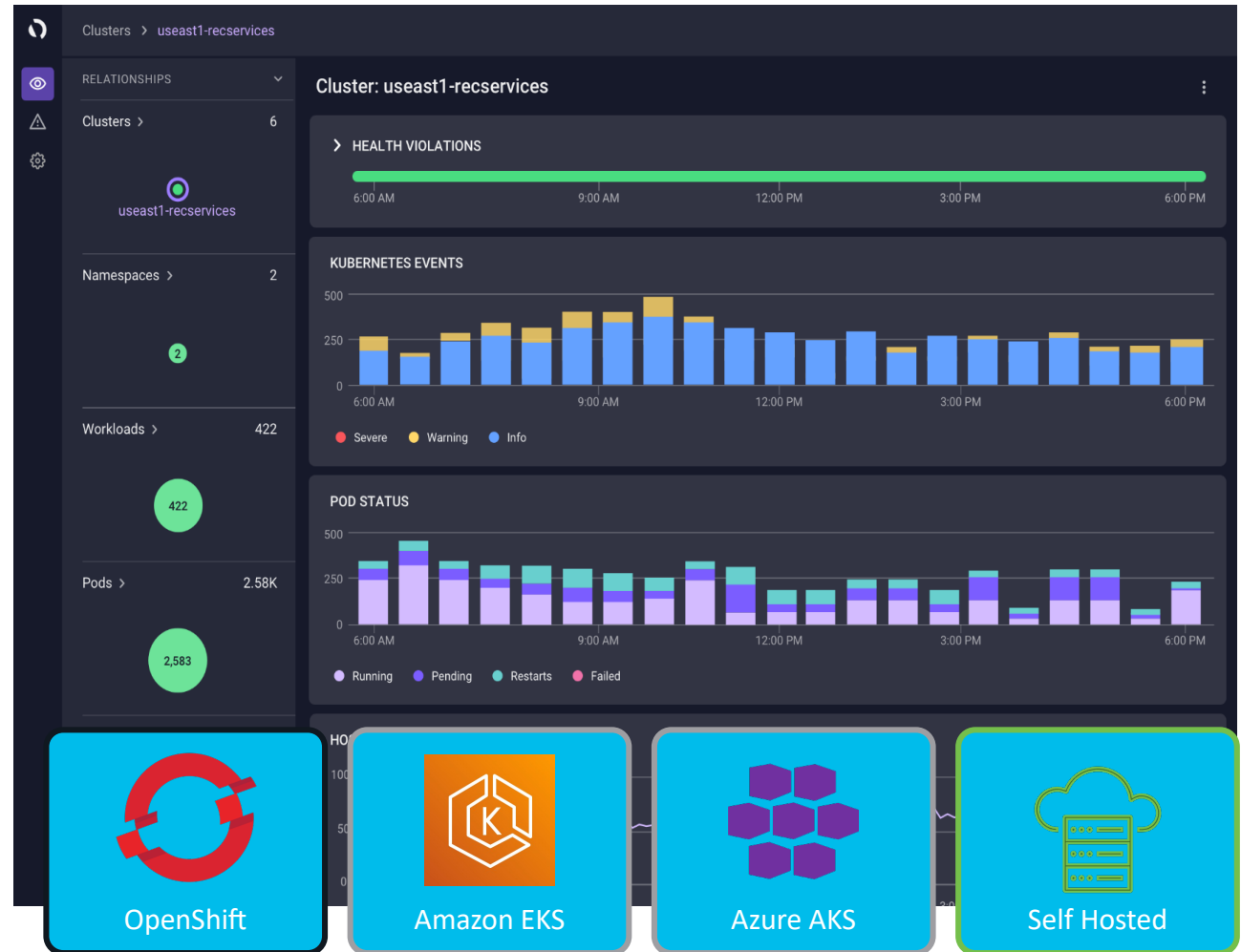
OpenShift Kubernetes

Unify observability across clusters
both on-premise and in the cloud

Self-managed k8s support extends to
most common enterprise container
platforms

Easy to deploy on large clusters with
OOTB health rules for fast start

Just released!



*AWS EKS and Azure AKS support added in November



The bridge to possible

Thank you

