



The bridge to possible

# New AppDynamics Innovations in Cloud and Security

Eugene Kim

Director of Global Product Marketing & Strategy, Cisco AppDynamics

Randy Birdsall

Director, Product Management, Cisco AppDynamics

# 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 until February 24, 2023.





# Agenda

- Industry Approaches to Observability
- What's New in AppDynamics Cloud
- What's New in Cisco Secure Application

# AppDynamics snapshot and strategy

AppDynamics drives business outcomes by putting application health in the context of your business, while providing unparalleled observability across tools, services and infrastructure on the backend.



## 1000's of happy customers

Across diverse industries such as:

- Finance
- Retail
- Healthcare
- Government
- And more...



## Supporting multiple deployments

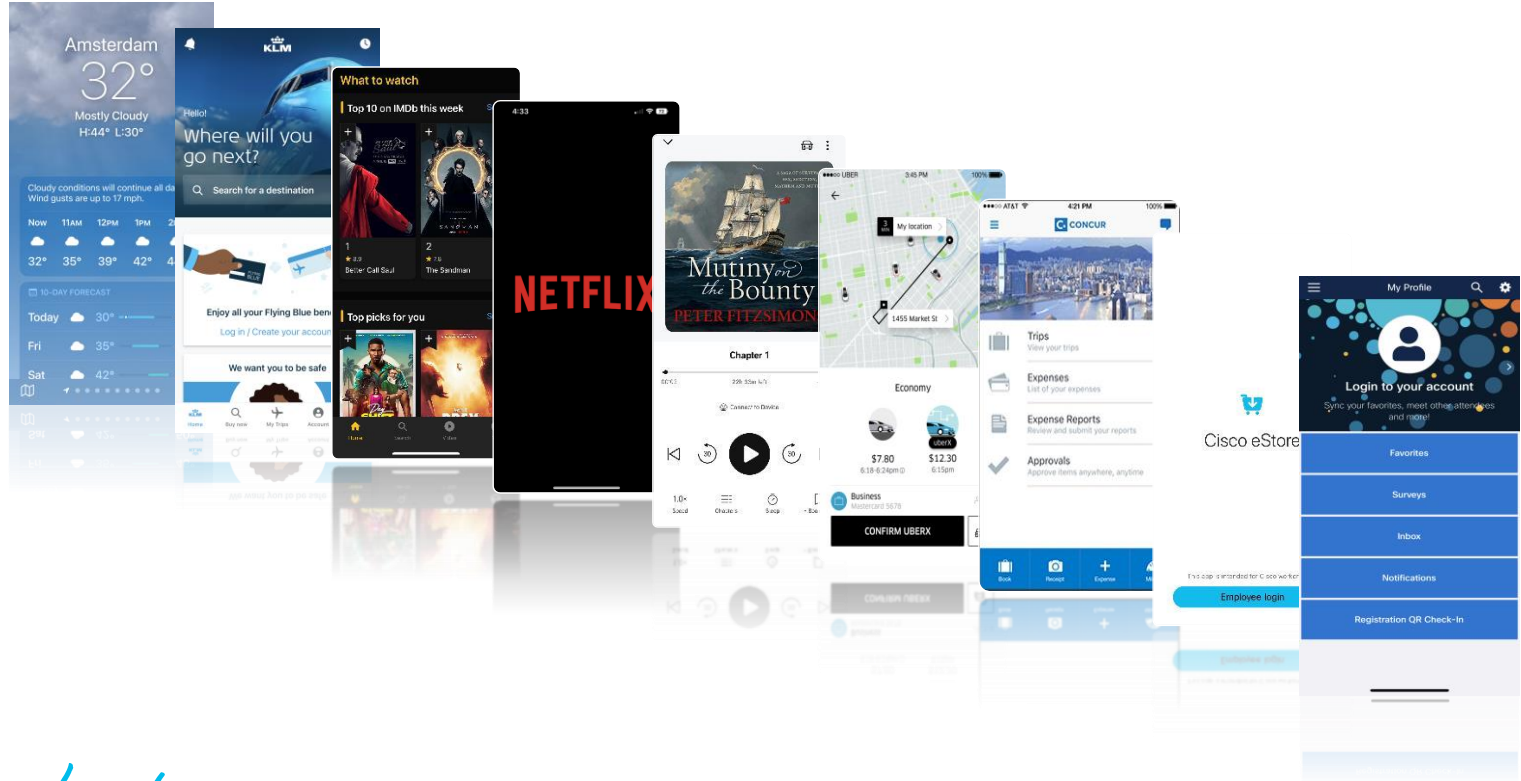
- AppDynamics (SaaS)
- AppDynamics (on-prem)
- AppDynamics GovAPM
- AppDynamics Cloud
- Secure Application



## Full-stack coverage

- Business
- User experience
- Applications
- Infrastructure
- Network
- Security

# On the way to Cisco Live



# Cloud-Native Observability challenges

Most offerings were designed years ago with a single purpose in mind and new use cases were bolted on



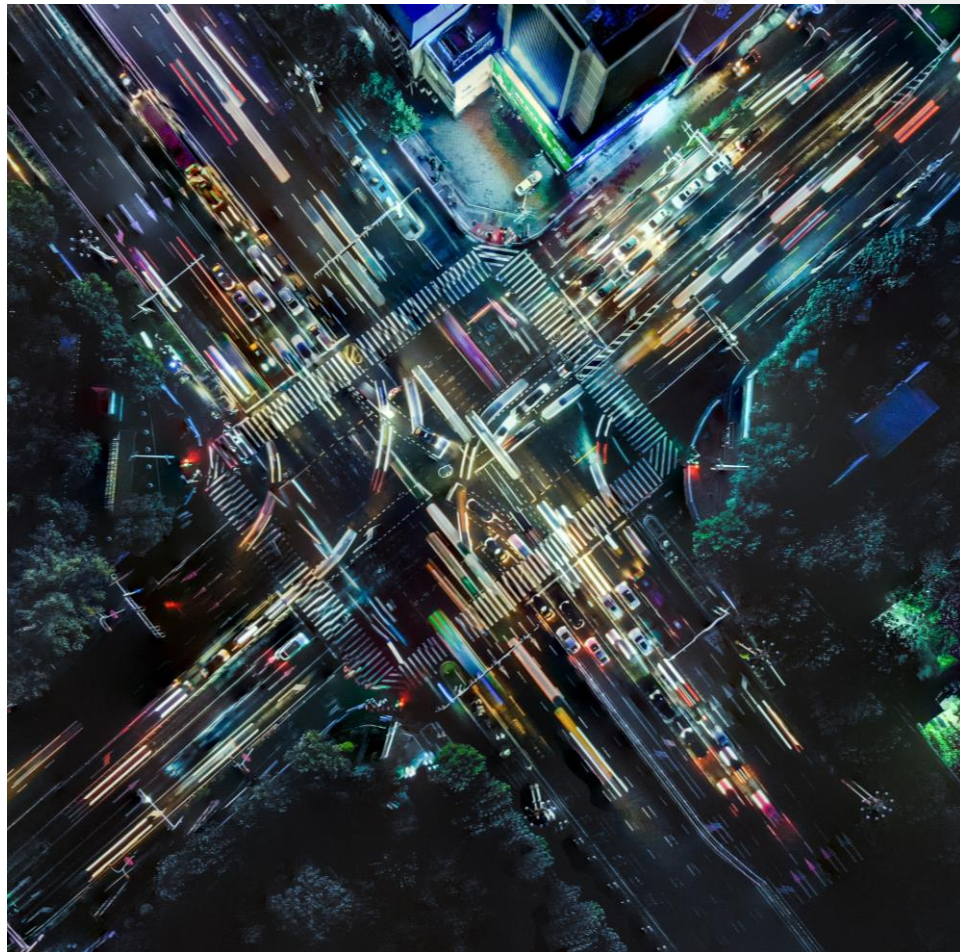
Disconnected silos of data and tab jumping



Incomplete visibility



Biased point of view based on legacy



# Cisco AppDynamics Cloud

Cloud-Native Observability built from the ground up

AppDynamics Cloud enables modern teams to eliminate siloes and navigate complex cloud-native relationships with a correlated view of all telemetry across their entire technology landscape

## Cloud-Native Visibility



**Full-Stack Observability Platform**  
foundation to see your entire cloud-native landscape and understand all relationships

## Cloud-Native Insights



**Business Context**  
cuts through the complexity of cloud-native operations and observe your app the way an end-user experiences it

## Cloud-Native Exploration



**Continuous-Context**  
quickly view and continuously analyze all the cloud-native observability dimensions to optimize for the business

RedHat OpenShift Support



Business Transaction  
Insights

Grafana Plug-ins



Continuous-Context Experience

Contextual Trace Visualization



# What's New in Cisco AppDynamics Cloud







# Contextual Trace Exploration

## Troubleshoot with business context

- Provide workload and interaction context to explore RCA performance issues
- Propagate Trace Attributes to enable correlations across domains
- Proactively discover bottlenecks and improve application performance

The screenshot displays the Cloud-Native Exploration interface, which is used for troubleshooting and performance analysis. The top section, titled 'Traces', shows a list of traces filtered by attributes. The filter applied is `attributes('service.name') IN ['orders-service', 'users-service'] && attributes('has_error') = true`. The table lists traces with columns for Origin, Number of spans, Duration, Status, Trace ID, and Actions. All listed traces are in an 'Error' status.

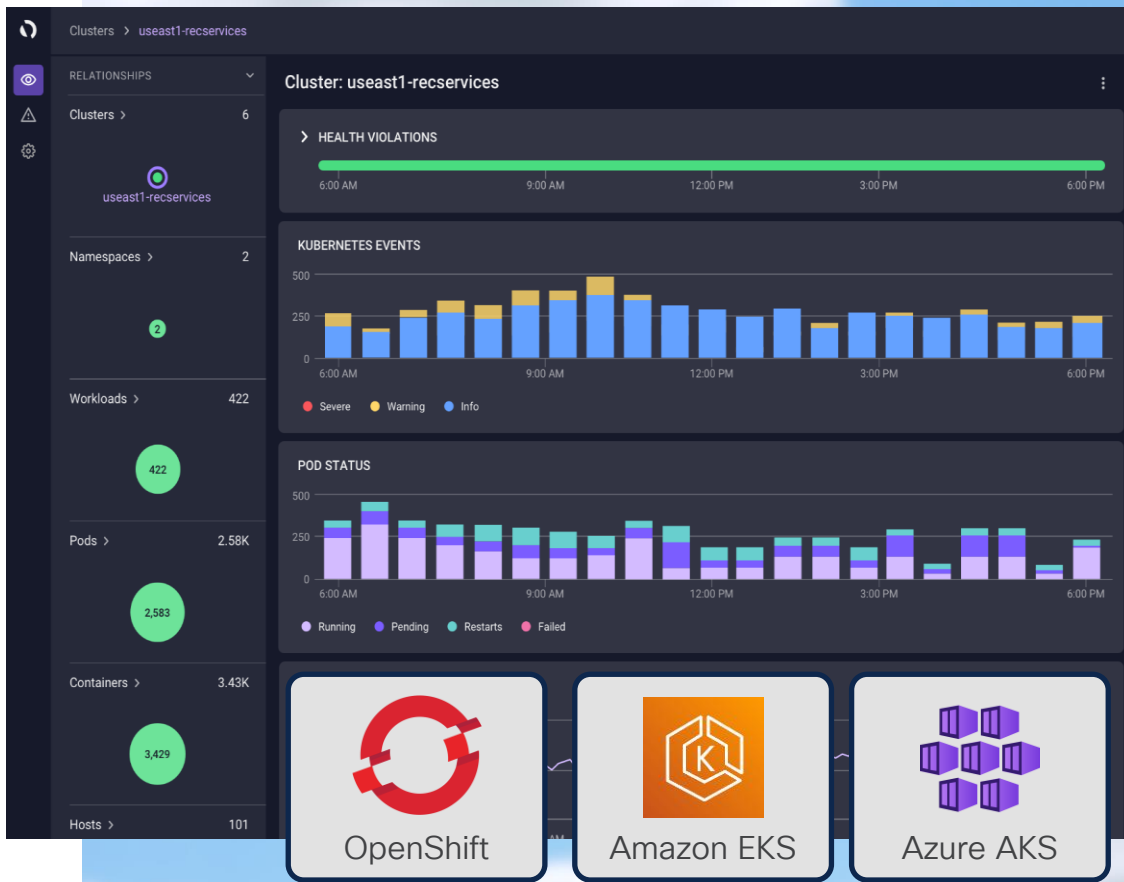
The bottom section, titled 'Trace\_ID', provides a detailed view of a specific trace. It includes a 'Service graph' showing the flow of the request through different services. Below the graph is the 'REQUEST FLOW' section, which shows a timeline of the request. The request starts with a `HTTP POST /purchase-order` to the `orders-service` (1.2s), followed by a `HTTP POST /user/verify` to the `users-service` (0.8s), and finally a `HTTP POST /verify-user` to the `auth0` service (0.6s). The total duration of the request is 1.2s.

On the right side of the 'Trace\_ID' view, there is a 'Trace Overview' panel. It shows the span overview for the `auth0/verify-user` span. The properties section includes the remote service (`auth0`), the operation (`/verify-user`), the duration (0.6s), the number of child spans (0), and the error code (`HTTP 504`).

# OpenShift Kubernetes visibility on AppD Cloud

Extend modern application observability from your clouds to on-prem

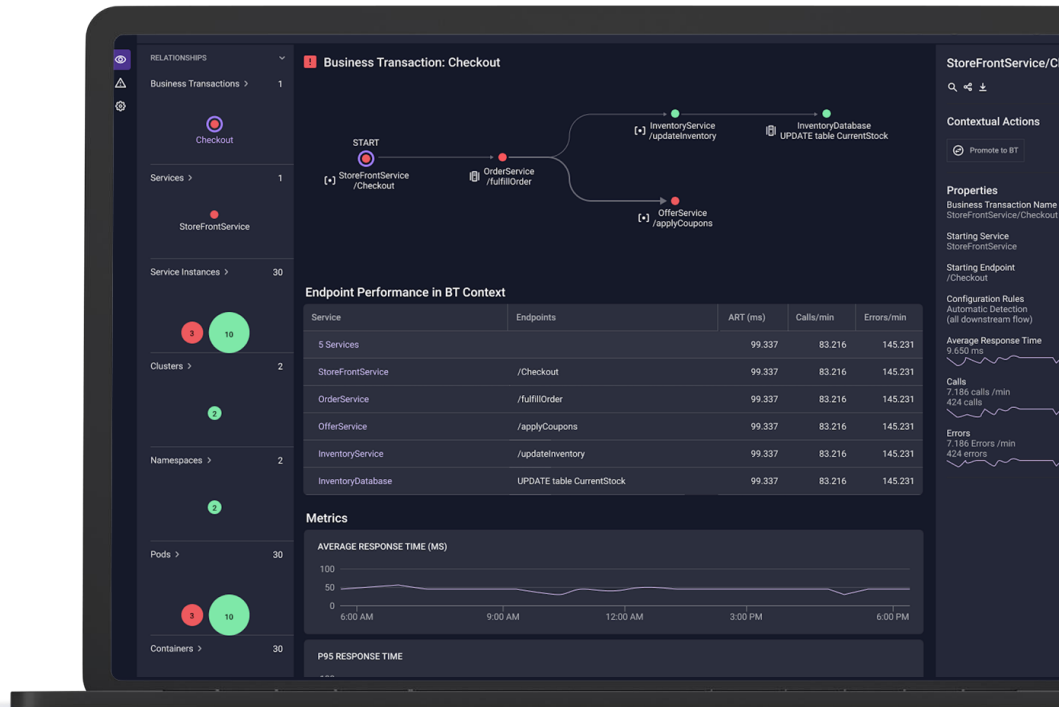
- Unify observability across clusters in public clouds, on-premises, or in hybrid clouds
- Power modern applications with the flexibility to obtain the best economics and performance
- Fully correlate Kubernetes infrastructure to app performance and business impacts



# Business Transactions Insights

Observe your Cloud-Native environment with the lens of the customer and business

- Be alerted to troubleshoot your most important customer experiences and business outcomes
- Auto-discover BT-i's for easier definition and faster setup
- Define new BT-i's for simpler transaction creation without coding
- Troubleshoot with continuous-context



# What's New in Cisco Secure Application



# Cisco Secure Application Business Risk Scoring for Applications

Unlike siloed security monitoring tools, Cisco Secure Application provides the business context needed to rapidly assess risk and align teams based on potential impact

## Business Context Mapping

Mapping vulnerabilities and attacks to common transactions like *'login, add-to-cart, and complete payment'* provides the business context to help you quickly understand the location and impact of threats.

+

## Vulnerability and Threat Intelligence

New threat intelligence feeds from Cisco Talos, Kenna, and Panoptica provides the threat context to understand the likelihood of threat exploits.

=

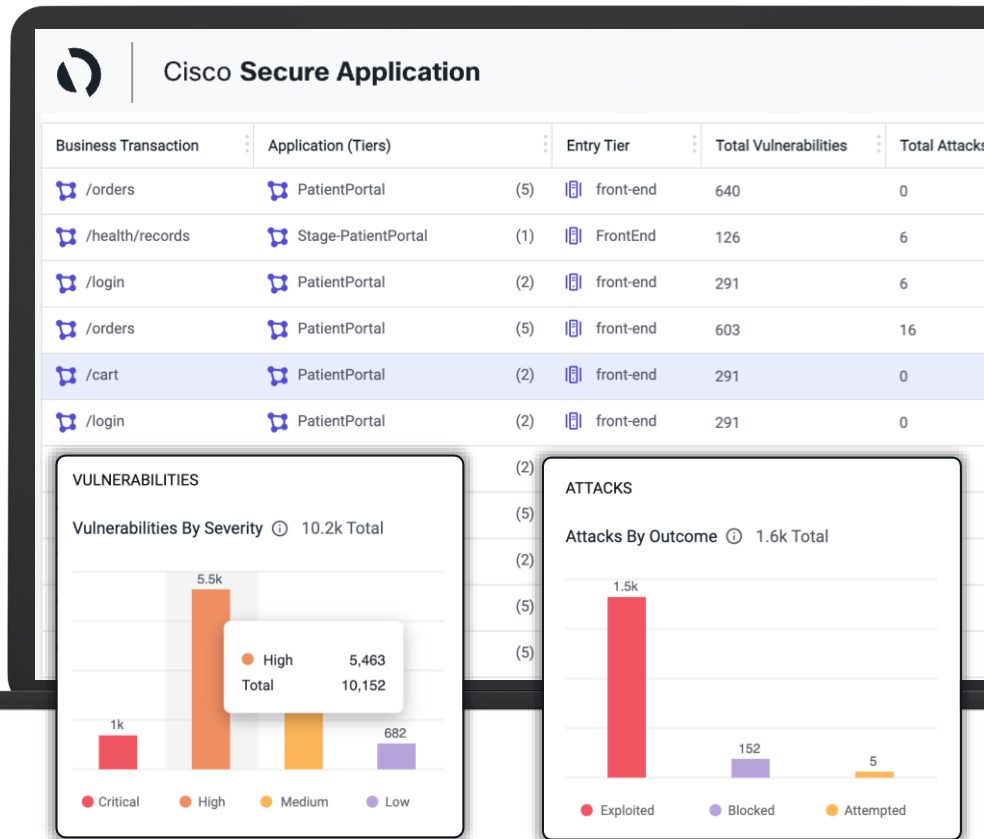
## Business Risk Scoring

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

# Correlate findings to Business Transactions

Give deeper biz context to guide prioritization

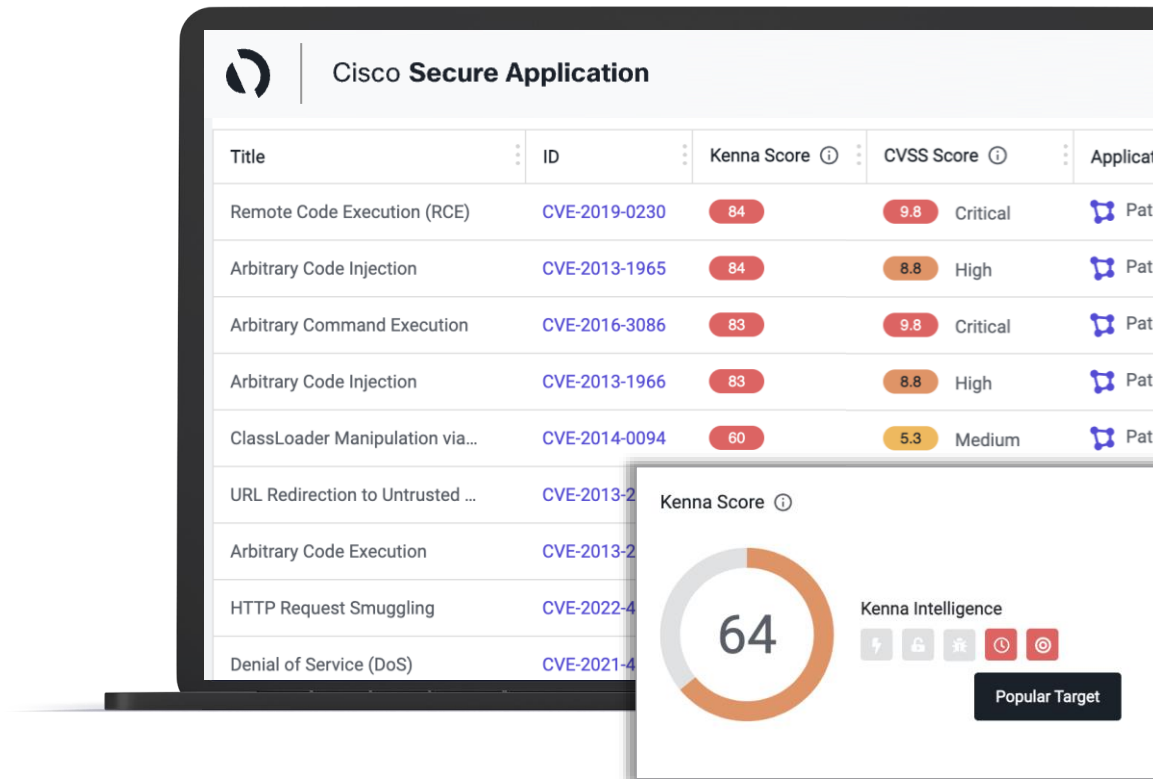
- Business context locates risk within critical transactions
- Exposing vulnerabilities across transactions gives complete view of risk
- Stack ranked risk prioritizes remediation and mitigation efforts



# Determine likelihood of exploit with Kenna

Use data science to identify real vulnerability risk

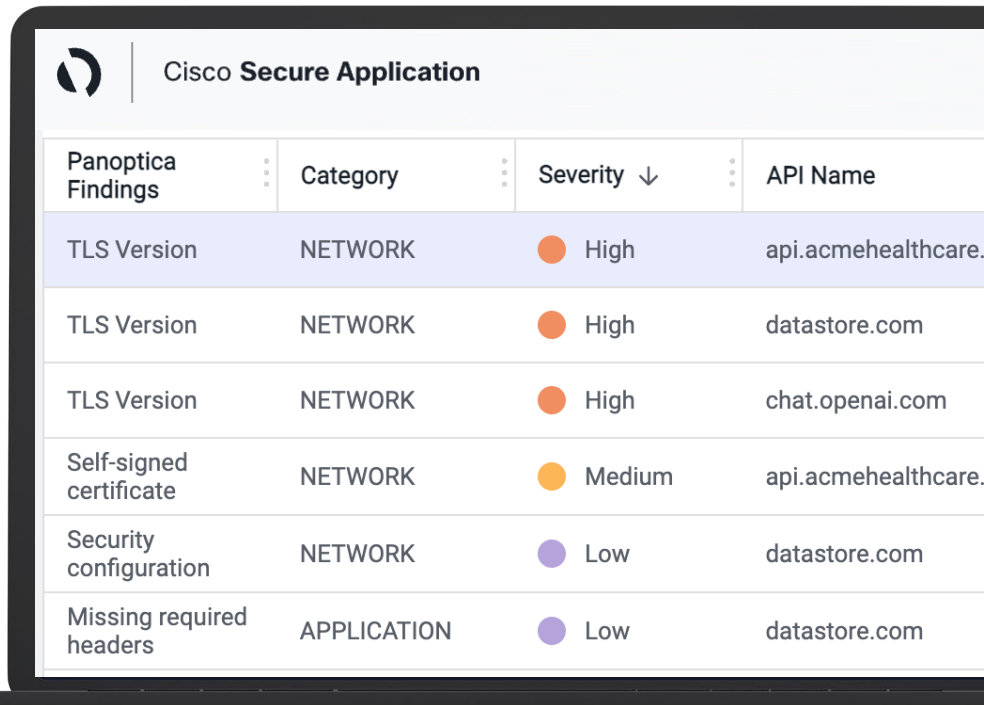
- Machine learning leveraging real-time and historical data to predict exploitation
- Leverage a better remediation methodology compared to CVSS
- Native backend integration maps Kenna scores to discovered vulns
- Combine findings into vuln and threat context for business risk scores



# 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



The image shows a screenshot of the Cisco Secure Application interface. At the top, there is a header with the Cisco logo and the text "Cisco Secure Application". Below the header is a table with four columns: "Panoptica Findings", "Category", "Severity ↓", and "API Name". The table contains six rows of data, each representing a finding. The first three rows are for "TLS Version" findings, all categorized as "NETWORK" with a "High" severity (indicated by an orange circle). The fourth row is for a "Self-signed certificate" finding, categorized as "NETWORK" with a "Medium" severity (indicated by a yellow circle). The fifth row is for a "Security configuration" finding, categorized as "NETWORK" with a "Low" severity (indicated by a purple circle). The sixth row is for a "Missing required headers" finding, categorized as "APPLICATION" with a "Low" severity (indicated by a purple circle).

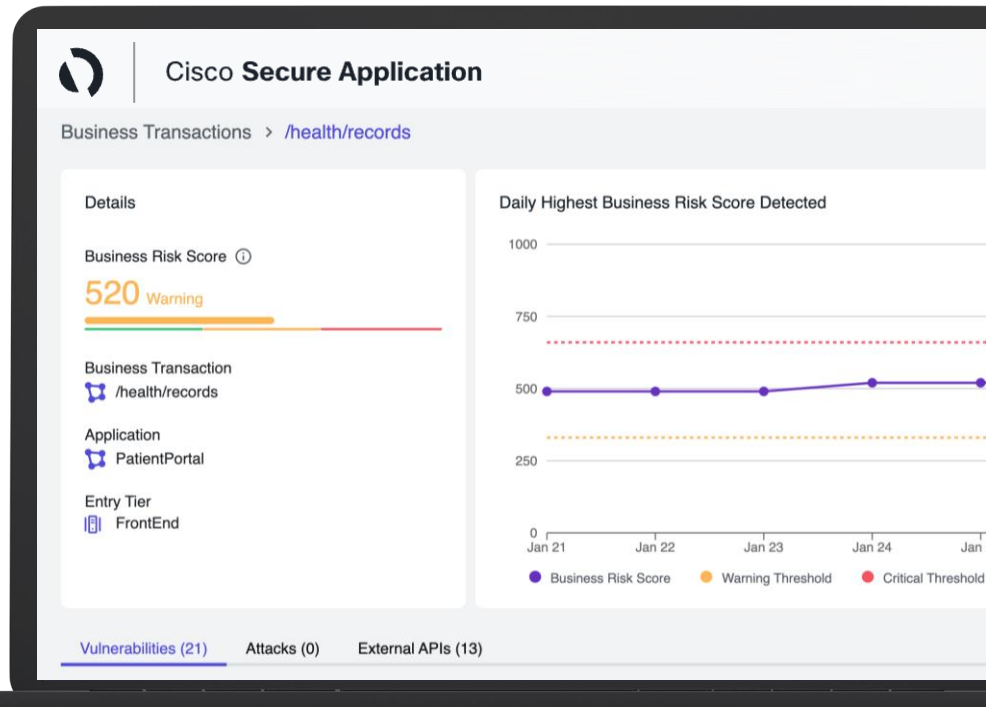
Panoptica Findings	Category	Severity ↓	API Name
TLS Version	NETWORK	High	api.acmehealthcare.
TLS Version	NETWORK	High	datastore.com
TLS Version	NETWORK	High	chat.openai.com
Self-signed certificate	NETWORK	Medium	api.acmehealthcare.
Security configuration	NETWORK	Low	datastore.com
Missing required headers	APPLICATION	Low	datastore.com



# 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, Snyk
- Continuously assess score reflect real-time risk
- Prioritize remediation and mitigation efforts by what matters to the biz



Deliver secure app  
performance together

Your Digital  
Business



AppDynamics



# Continue Your Education



Visit the Cisco Showcase for related demos.



Book your one-on-one Meet the Engineer meeting.



Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.



Visit the On-Demand Library for more sessions at [ciscolive.com/on-demand](https://ciscolive.com/on-demand).

# Complete your Session Survey

- Please complete your session survey after each session. Your feedback is important.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at <https://www.ciscolive.com/emea/learn/sessions/session-catalog.html>





The bridge to possible

# Thank you

CISCO *Live!*

# Are you playing the Cisco Live Game?

Scan the QR code and earn your  
**Cisco Theater** points here



CISCO *Live!*

