

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco & Splunk Unified Observability

Path to Digital Resilience

Diana Omuoyo
Sr Solutions Architect - Observability

Session ID: BRKAPP-1544

CISCO *Live!*

#CiscoLiveAPJC



Diana Omuoyo

Sr Solutions Architect - Observability
Sydney, Australia

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 November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP1544>



Today's session

Enterprise
Complexity

Unified
Observability

IT Service
Intelligence

Artificial
Intelligence

Data
Management

Q/A

Enterprise Complexity

Modernisation & Innovation



New technology is stacked on top of legacy systems, leaving a long tail of assets & tech debt

More workloads run on distributed hybrid systems, multi language microservices & with MELT telemetry foundation

Incremental Complexity

Iterative burst of dependencies, resources and data sources



More services to
monitor and secure



More tools and gaps
between systems



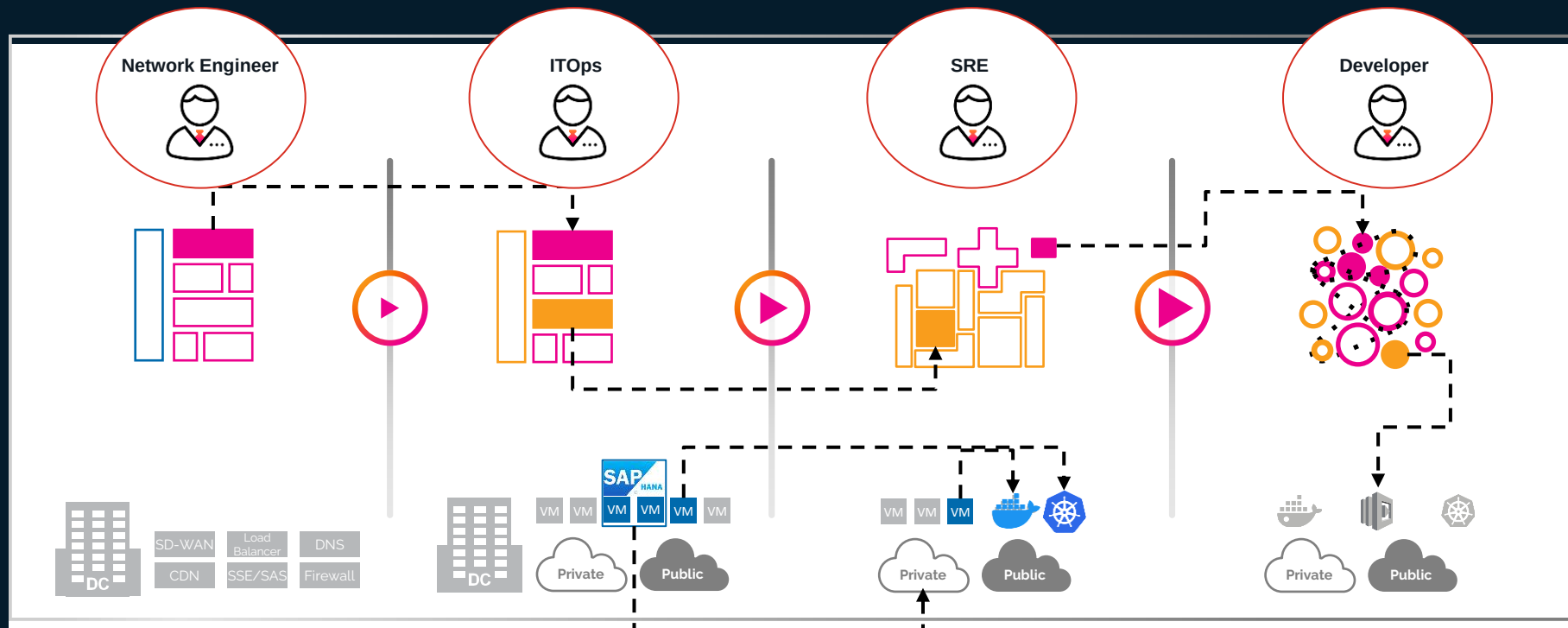
More data to analyse
and correlate



More points of failure &
unpredictability

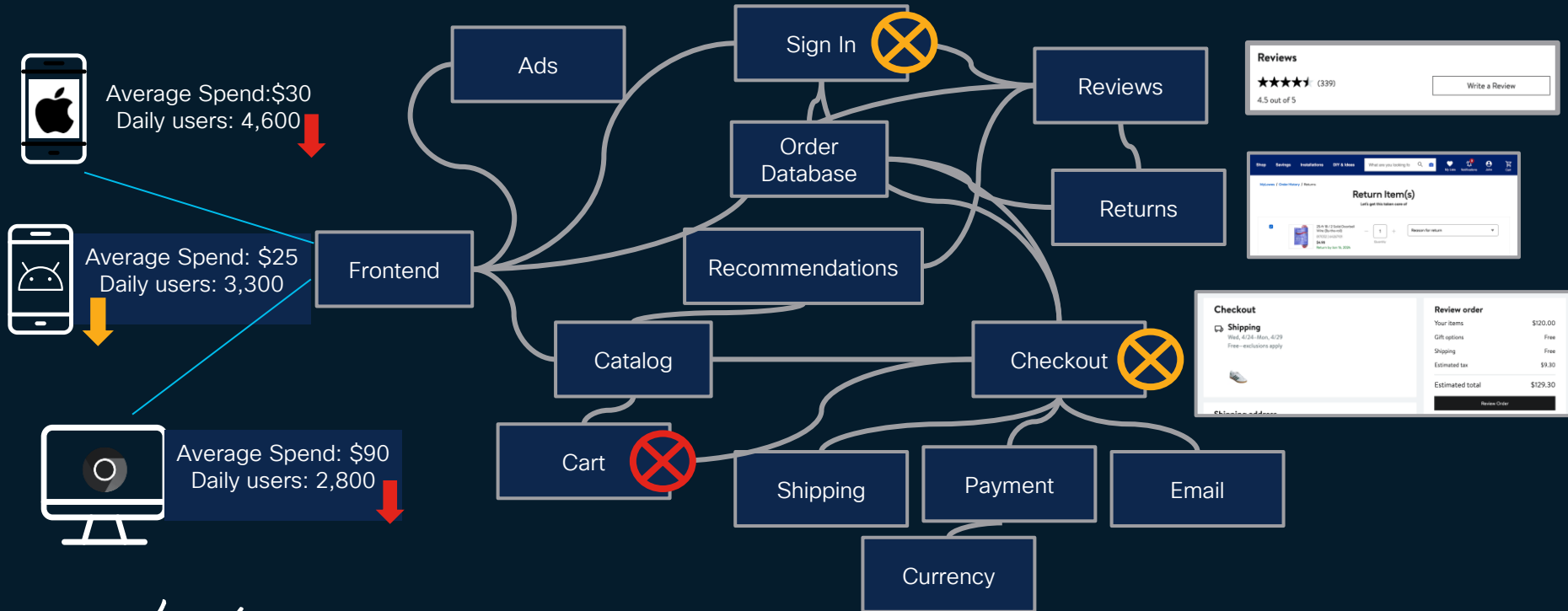
Siloed Domain Expertise

Disconnected visibility lead to blind spots for issues that span teams & services



Business Context Gets Lost

It's hard to triage performance problems based on business impact



Unified Observability

Integrated Solutions



Multi-Dimensional Observability

Solutions MUST cover multiple aspects of your business resilience strategy



Legacy | Modern
Applications



On-Prem | Hybrid |
Multi-Cloud



Enterprise Network &
Security

Splunk & Cisco are uniquely positioned to deliver **Observability** and **Security** capabilities across the entire enterprise and power the **future** of SOC and O11Y

Unified vision to reduce inefficiencies & the human toil of operating digital systems, by letting software do more of the heavy lifting

The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics
Events

Logs

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Logs

Metrics
Service Map

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Metrics
Anomalies

Logs & Other
Datasets
Unstructured / Structured

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

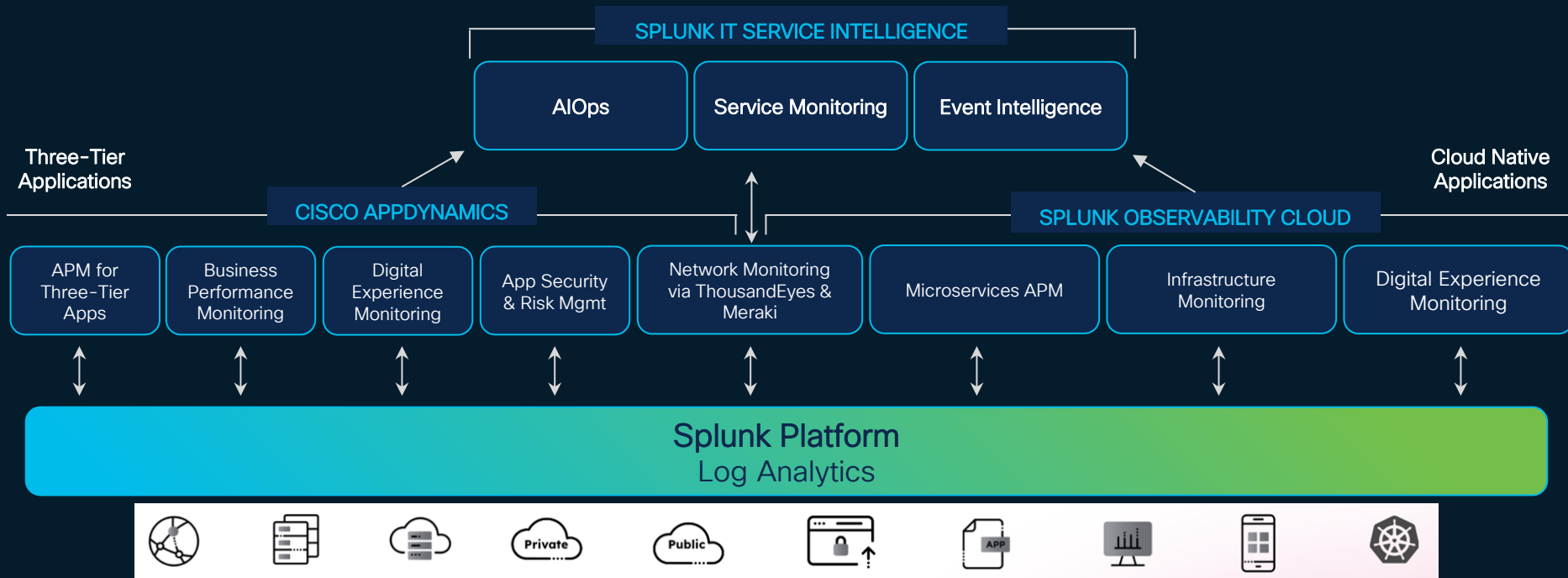
Metrics
Anomalies

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

Integrated E2E Observability

A view of the combined portfolio



The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

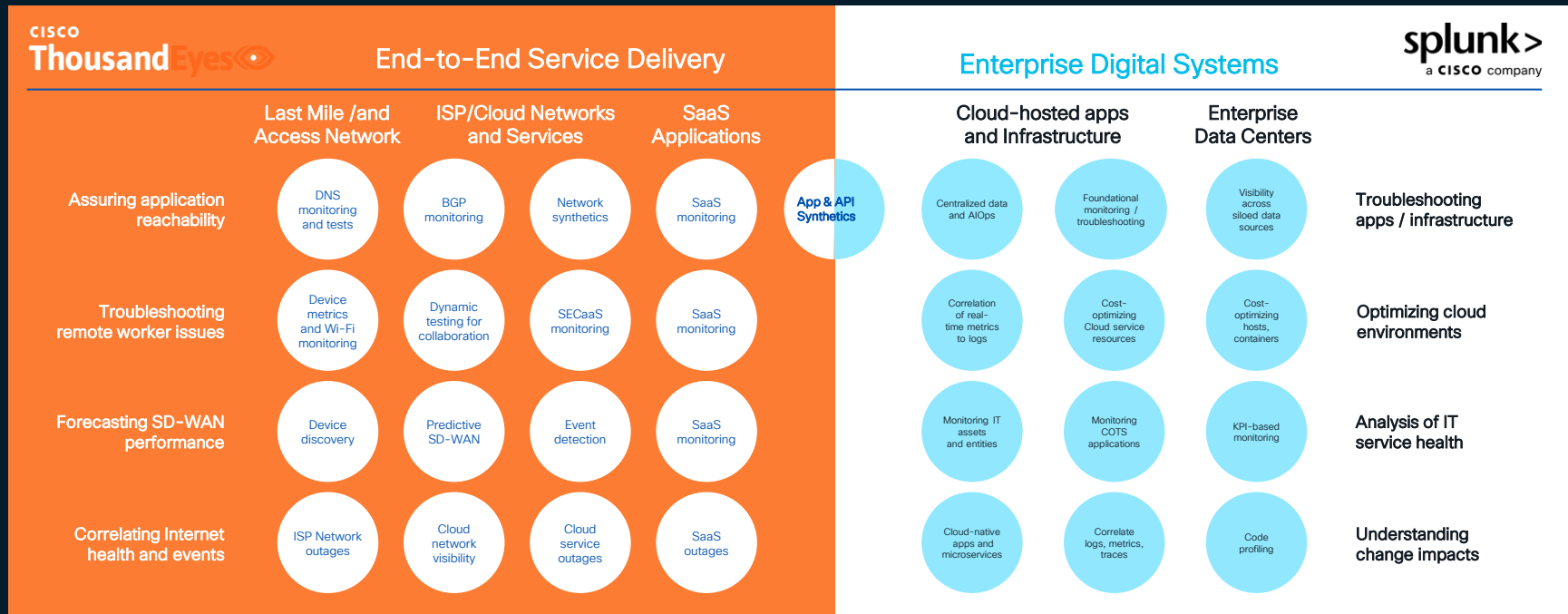
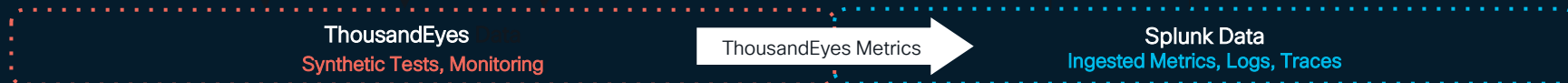
Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

Two Essential Solutions Driving Digital Resilience

	<div> Digital Experience Assurance (DXA)</div>	<div> a CISCO company Observability</div>
Distinct Purposes	Assuring digital experiences through end-to-end visibility into all networks and services that affect app performance and delivery	Making customer-controlled apps more resilient, performant and secure through visibility into app and infrastructure behavior
Distinct Personas	Network and ITOps teams	Application and Infrastructure teams
Complementary Use Cases	<ul style="list-style-type: none">• Assuring application reachability• Troubleshooting remote worker issues• Forecasting SD-WAN performance• Correlating Internet health and events	<ul style="list-style-type: none">• Troubleshooting apps and infrastructure• Optimizing cloud environments• Analysis of IT service health• Assessing change impacts on cloud-native apps

Visibility Across the Entire Digital Footprint



The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

Cisco & Splunk Security Portfolio

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

Network &
Endpoint
Monitoring

AppDynamics

Metrics & Traces
OnPrem / Traditional
Applications

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling |
100% traces

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Nexus Dashboard
Insights

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

Integrating Splunk & Cisco Security



Cisco Talos & CVM Intelligence

Native integration to give vulnerability insights,
Identify bad actors and expose 3rd party API
security issues

Security and IT teams



Hunt for Threats

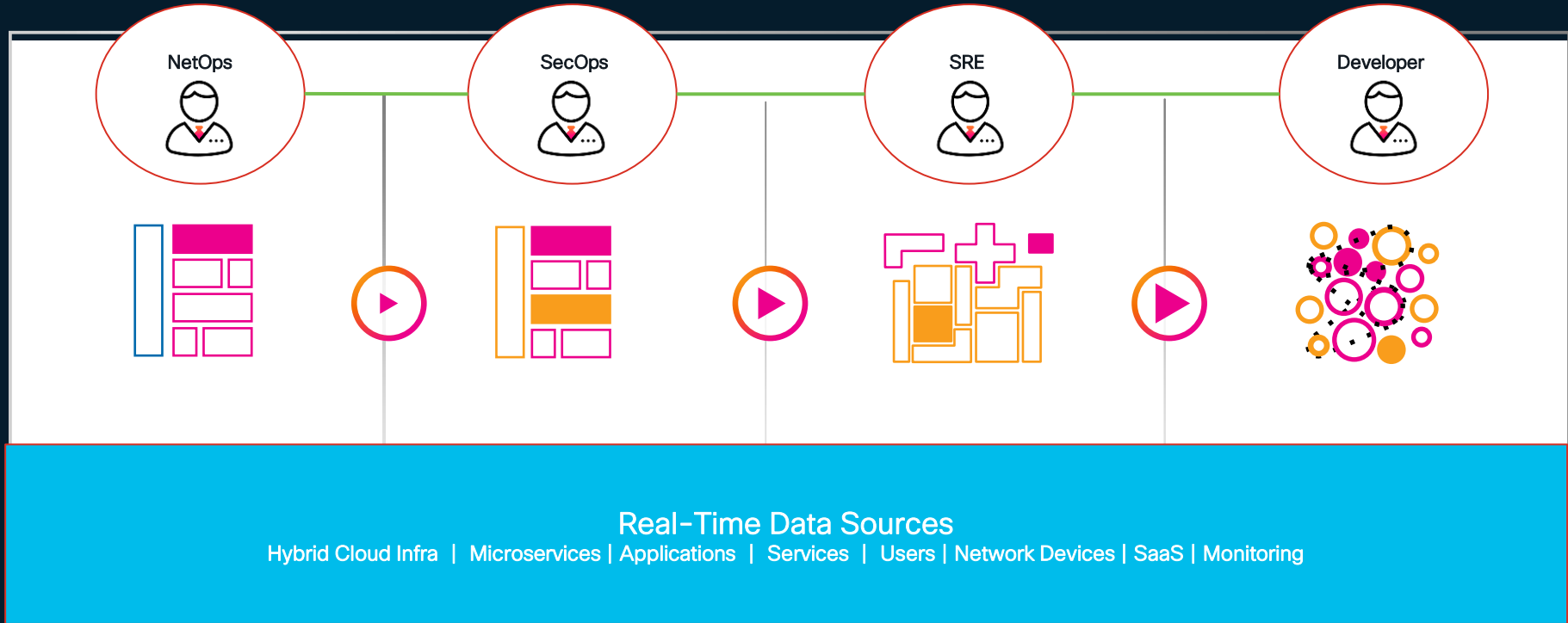
Give a more complete picture of an incident and
remediate with Splunk platform integration

Application and Security teams



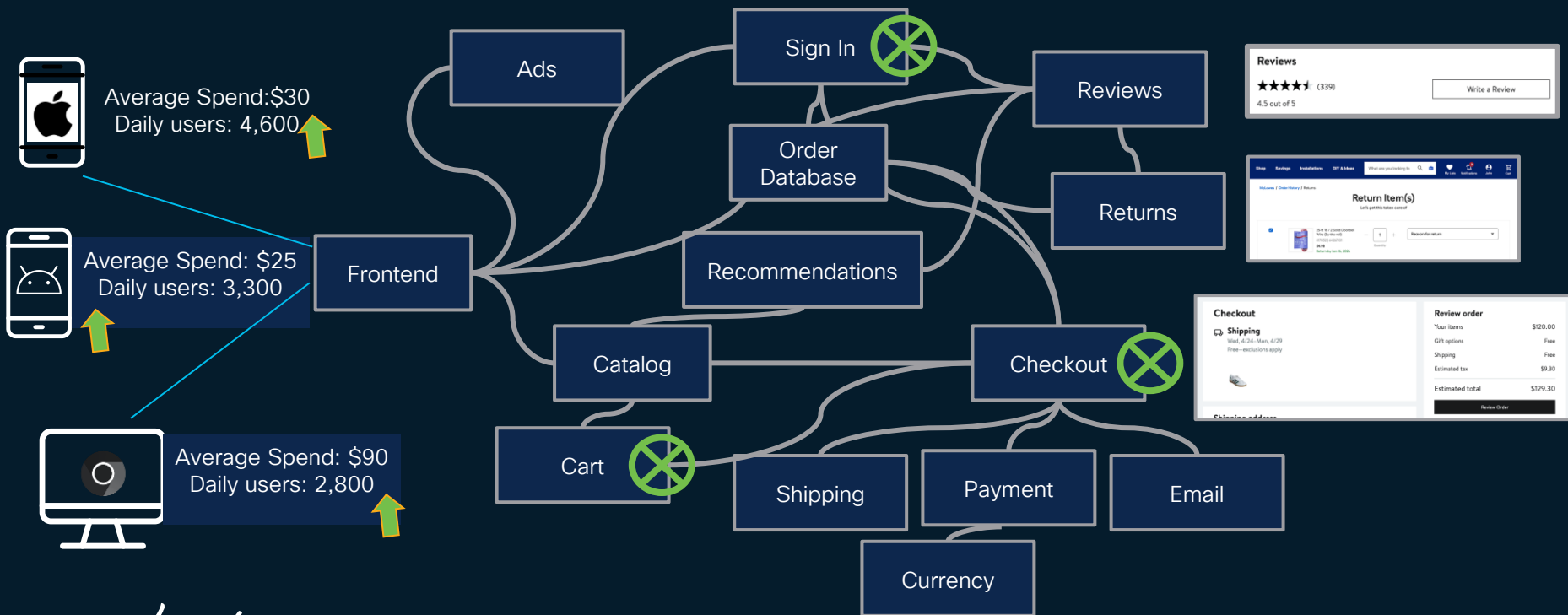
Unified | Correlated | Centralized Context

Ability to access insights into each platform and domain areas and all the dependencies



Contextual Visibility

Ability to pinpoint hot-spots and proactively address issues



The Most Complete Observability Solution

Splunk AIOps (IT Service Intelligence)

Executive Visibility | Proactive RCA | Event Management

SOAR

UBA

ES

Splunk Core Platform

3000+ OOTB Integrations | Schema on Read | Universal Data Ingestion

NO COST INTEGRATION

ThousandEyes

AppDynamics

Splunk Observability Cloud

RUM | APM | Infra Mon | Synthetic | K8s | Code profiling | 100% traces

Nexus Dashboard Insights

Network &
Endpoint
Monitoring

Metrics & Traces
OnPrem / Traditional
Applications

Metrics & Traces
Cloud Native Applications
Full Fidelity
Open Telemetry Native
High Resolution & Cardinality

Network
Monitoring

Logs & Other
Datasets
Unstructured / Structured

Metrics
Events

Logs

Logs

Metrics
Service Map

Metrics
Anomalies

Real-time Data Sources

Hybrid Cloud Infra | Microservices | Applications | Services | Users | Network Devices | SaaS | Monitoring

IT Service Intelligence

Business Service Monitoring & Analytics



IT Service Intelligence

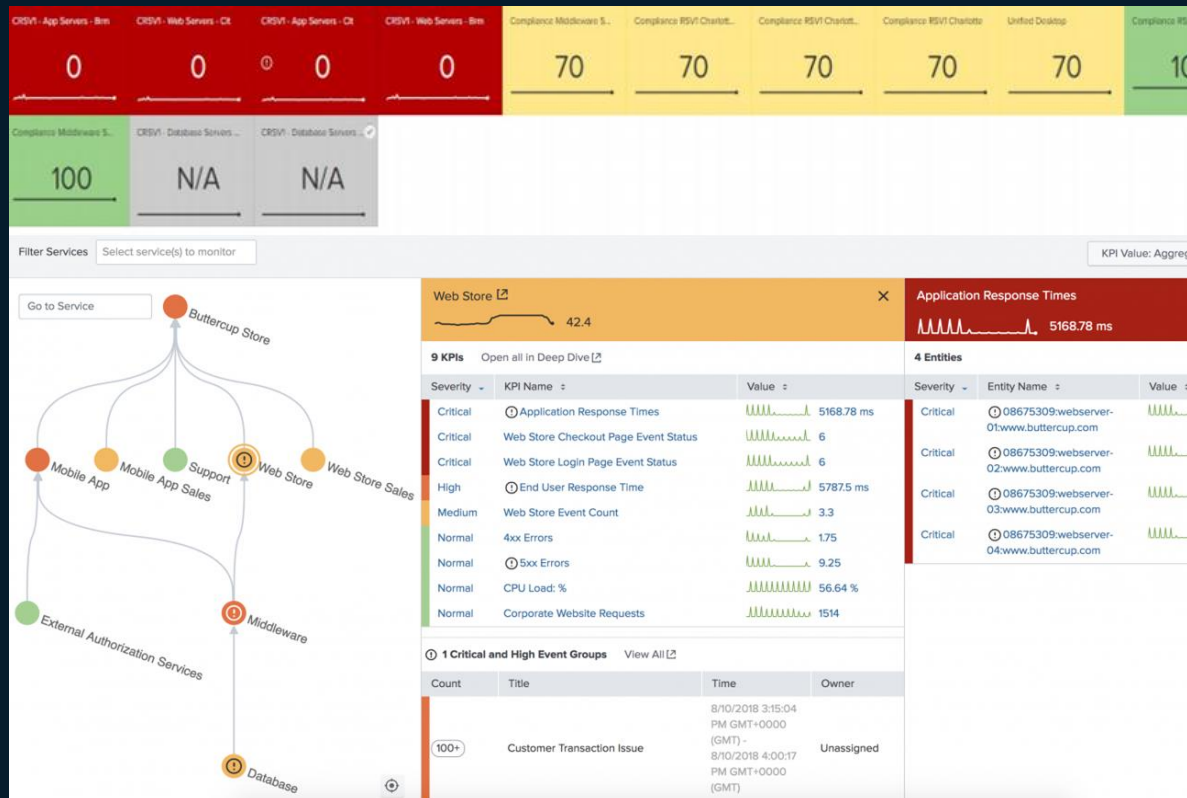
Core Use-Cases | Dimensions



End-2-End Business Visualisation

- Protect business performance
- Monitor service health
- Drill down into underlying dependencies

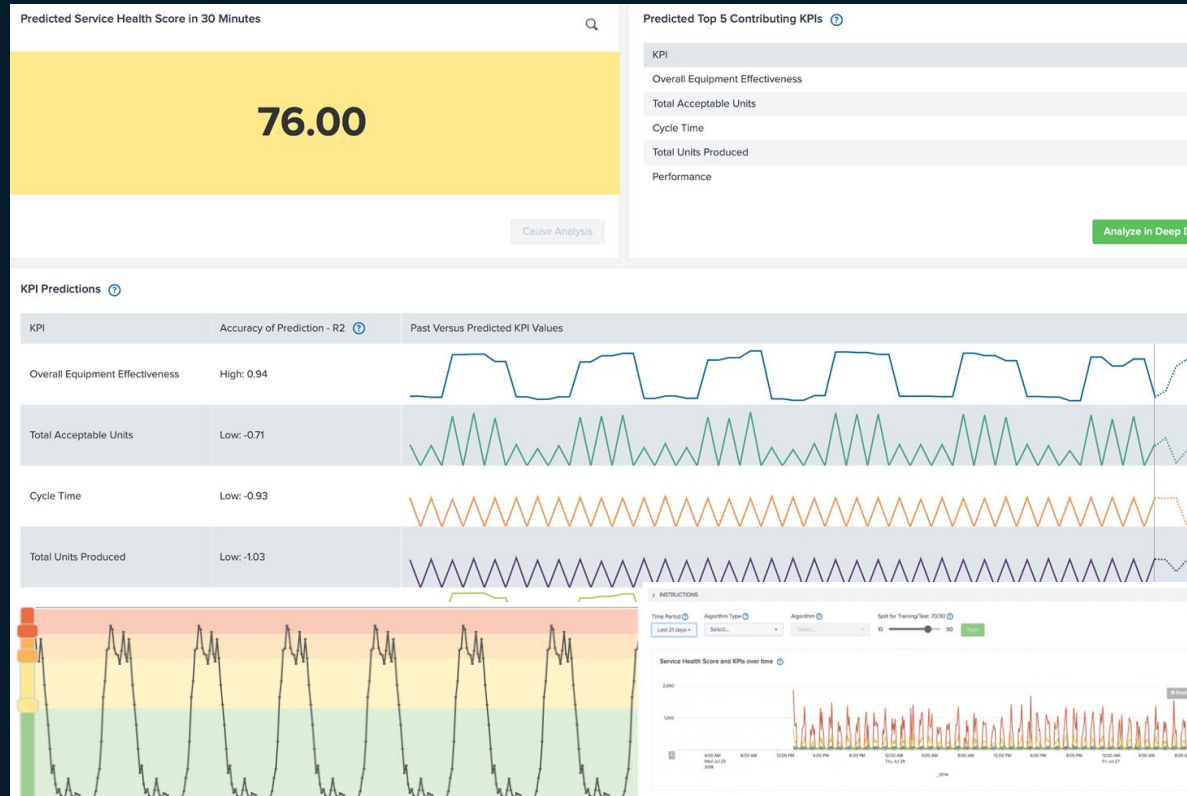
All from **one dashboard**.



ML & Predictive Analytics

- Anomaly detection
- Adaptive thresholding
- Predictive health scores

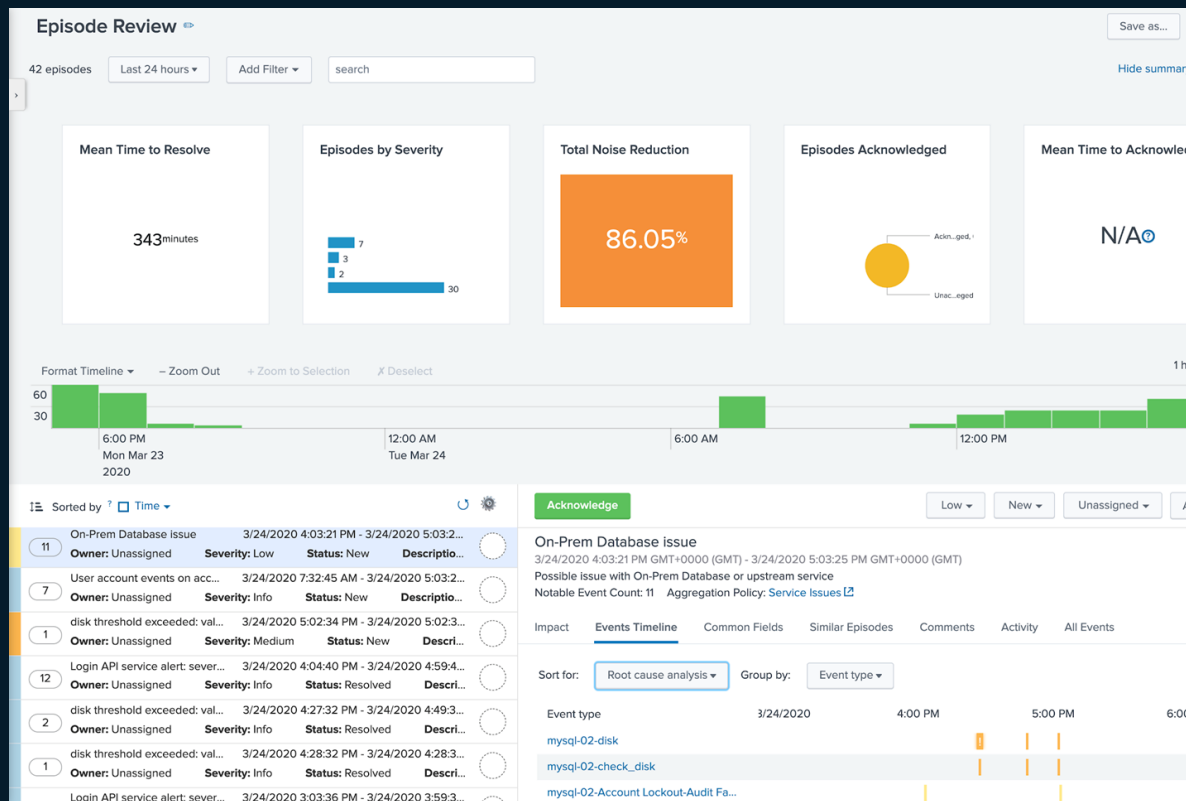
To monitor KPI data and prevent issues 30 min in advance.



Event Aggregation

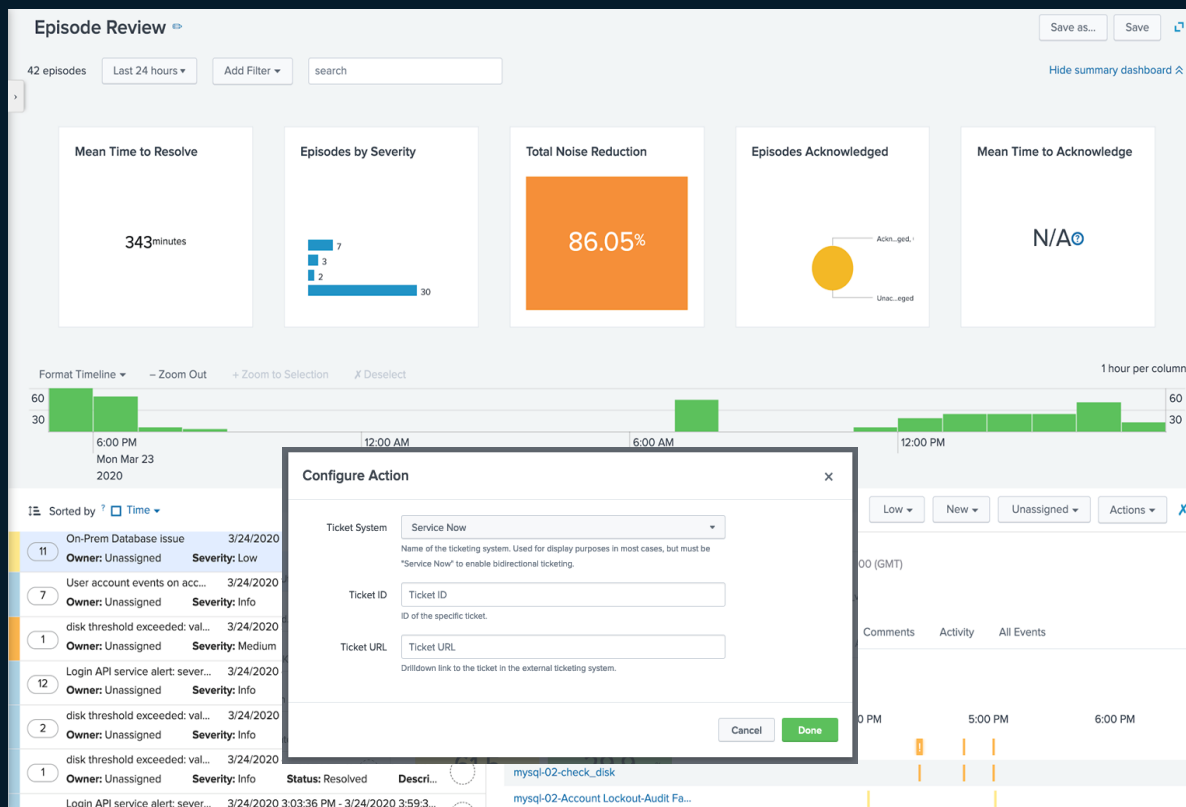
Machine learning policies automatically correlate and trigger alerts as data enters the system.

Immediate alert noise reduction.



Intelligent Incident Management

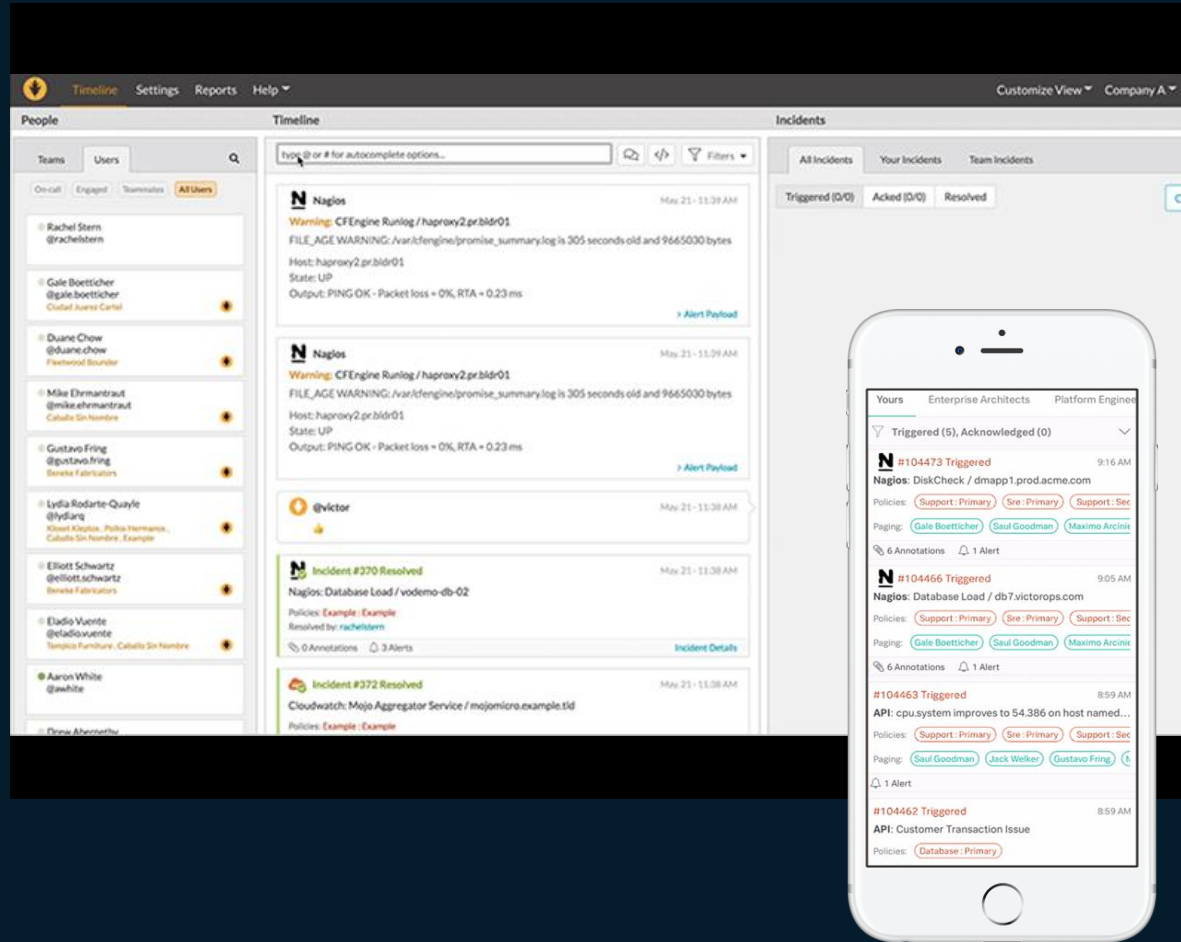
- Real-time event correlation
- Automated incident prioritisation
- integrations with IT service management (ITSM) tools



ITSM Integrations

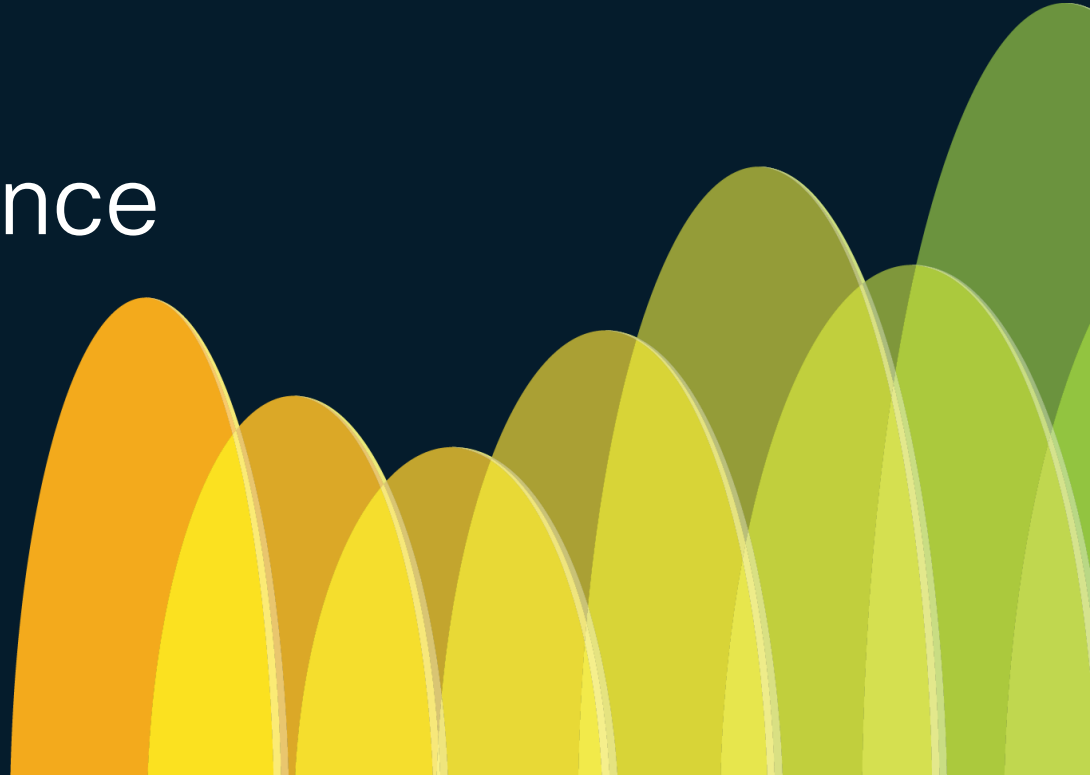
Integrations with service ticketing, on-call response and automated playbooks.

Focus urgent incidents first and reduce context-switching with a streamlined view for triage, investigation and response.



Artificial Intelligence

AI Assistant for Observability



Splunk & Cisco Philosophy on AI

Principles that drive the AI innovation



Domain and Splunk
Specific



Human in the Loop &
Trusted



Open & Extensible

Where are we investing?

Generative AI

Make sense of the signal to improve user productivity and outcomes.

Foundational AI

Find the signal from the noise in vast amounts of data.

Optimal Observability Unified AI

Combining predictive analytics & accelerated investigation



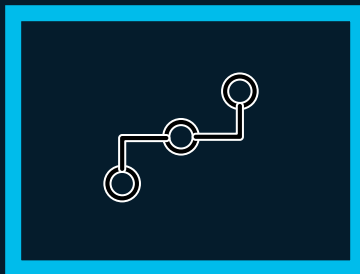
Generative AI Capabilities

Make Everyone an Expert

Reduce need for environment and tool expertise by simplifying content creation and investigation workflows

Detect & Predict

Real-time, streaming analysis to forecast trends and detect anomalies



Advanced Foundational AI

Correlate and Diagnose

Aggregate / analyze all data to direct investigation and identify root causes

Making Everyone an Observability Expert

Using powerful domain-specific LLMs, in-context, to power key workflows



Faster Insights and
Content

“Which K8s nodes have
memory utilisation more
than 90%?”



Chat with Your
Data

“List critical incidents
impacting checkout
service”

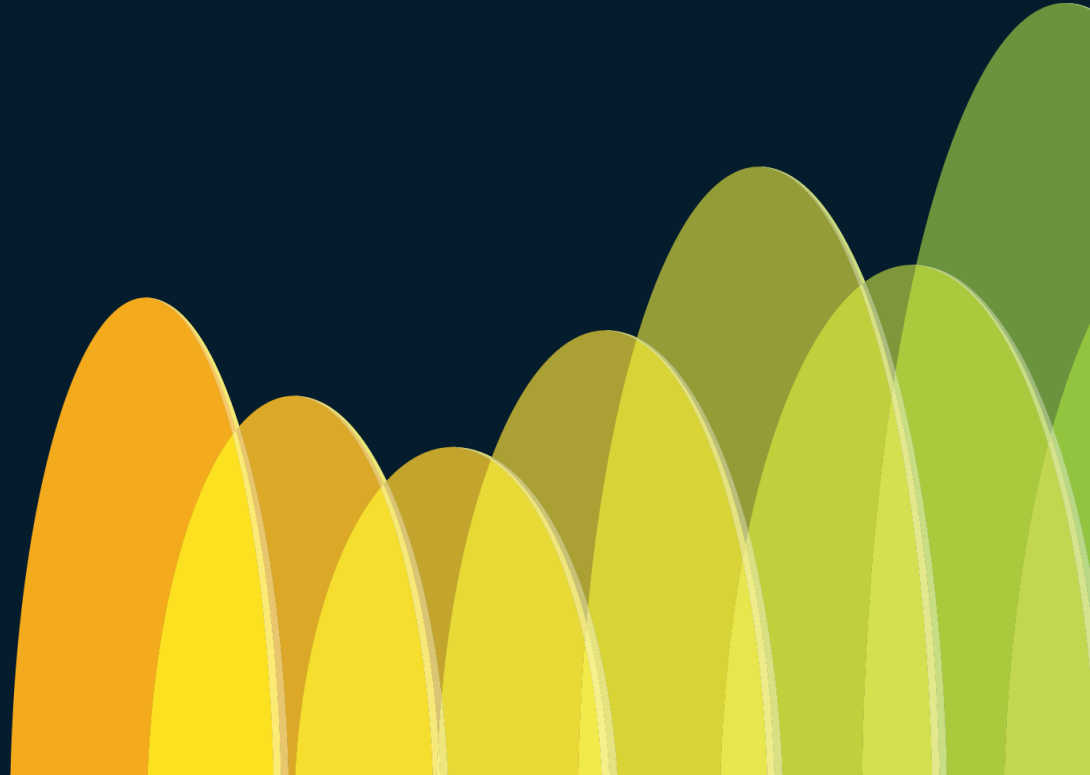


Assisted
Troubleshooting

“What is wrong with my
payment service?”

Data & Analytics

Managing Ingest, Processing,
Storage



GDI – Standardisation & Optimisation

Because data from every system may be different it's important to **standardise** & **simplify** ingestion engines & processes

Data Ingest - OpenTelemetry™

The standard for getting data into the Observability system

A **framework** featuring SDKs, a Collector, semantic conventions, etc.) for observability data



A **wire protocol** (OTLP); a library of components to receive, process, and export data in a flexible, open way

OpenTelemetry

Open Standard - Community - Adoption - Neutral - Traces, Metrics, Logs

Data Ingest - OpenTelemetry™

Splunk Enterprise vs. Splunk Observability - Know the journey



Universal / Heavy Forwarder
inputs.conf



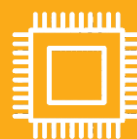
Heavy Forwarder / Indexer
props.conf | transforms.conf



Universal / Heavy Forwarder
outputs.conf



Receiver



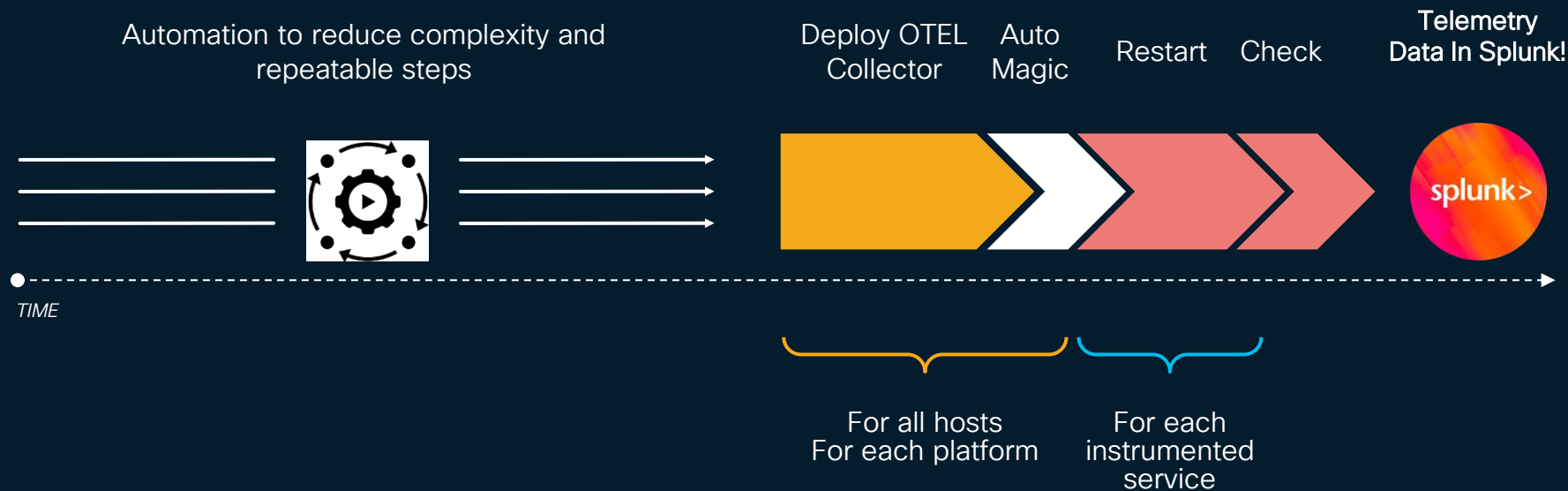
Processor



Exporter

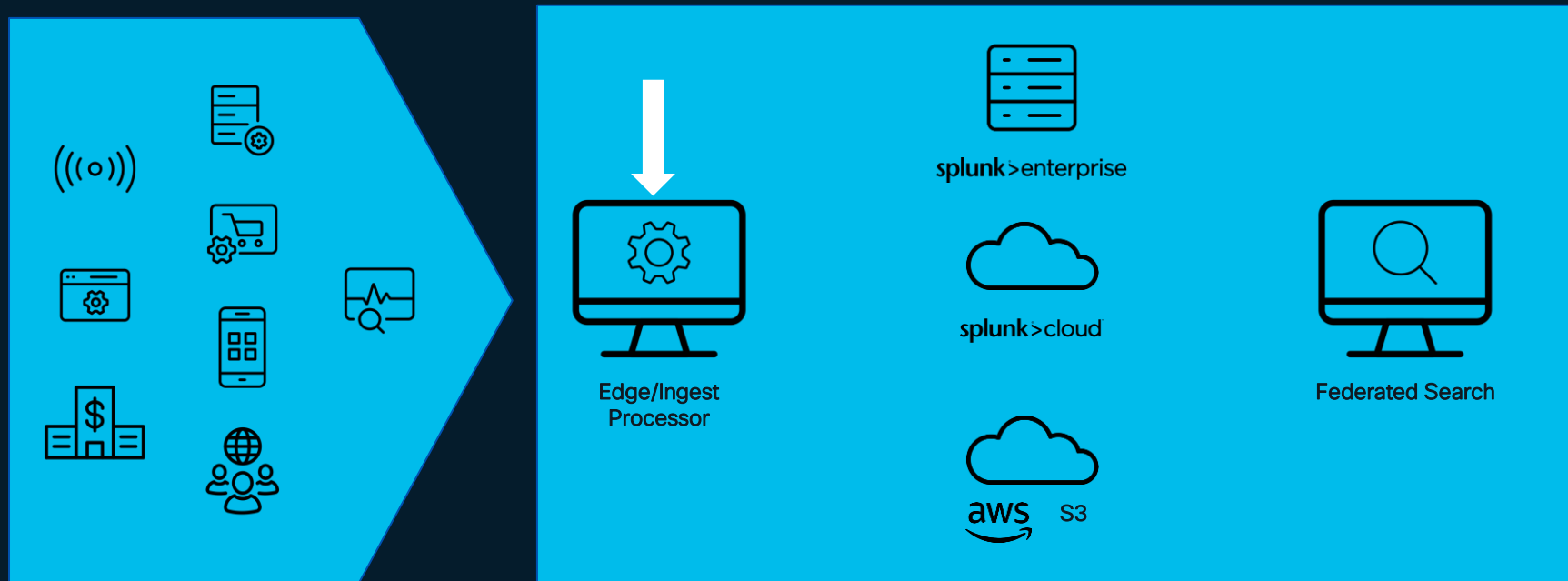
Data Ingest - OpenTelemetry™

Zero-Config Auto Instrumentation



Data Ingest – Pipeline Processing

Optimise existing data sources

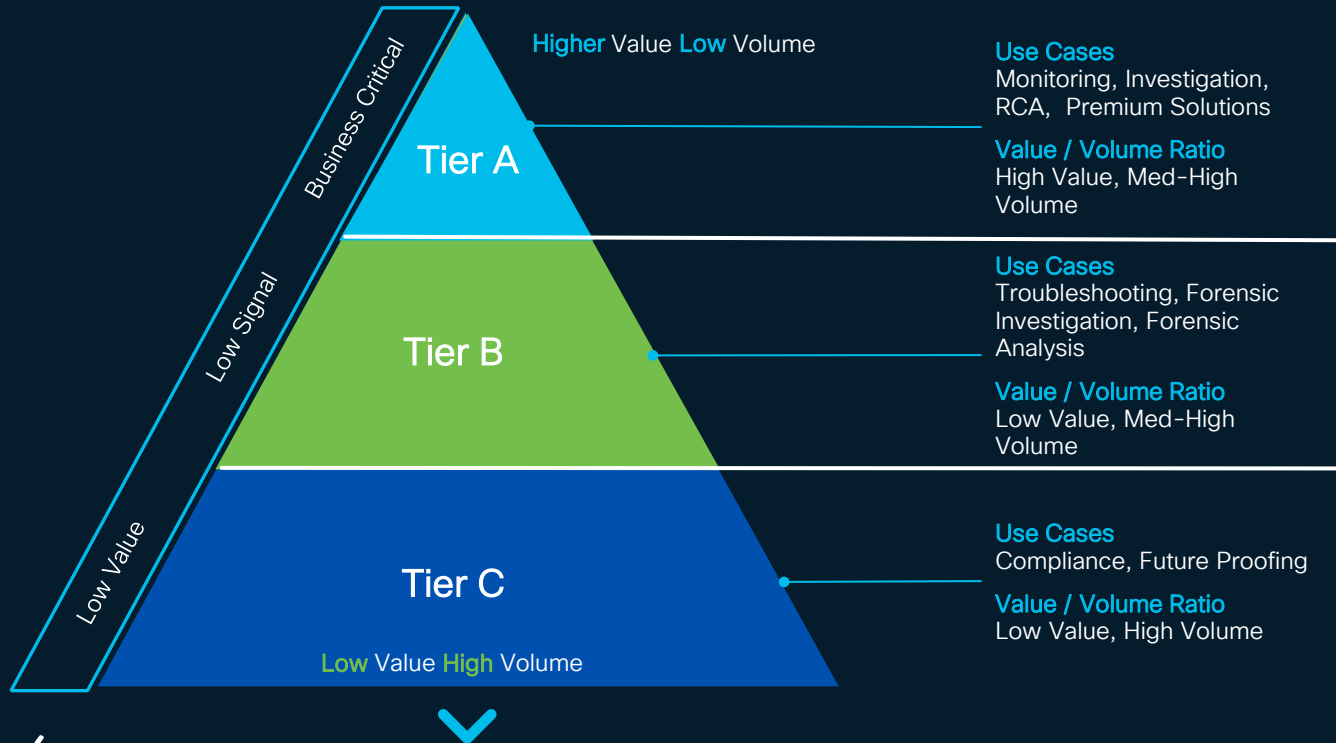


Data Storage & Cost Management

Know your data and key business
requirements, define critical use cases and
reduce costs

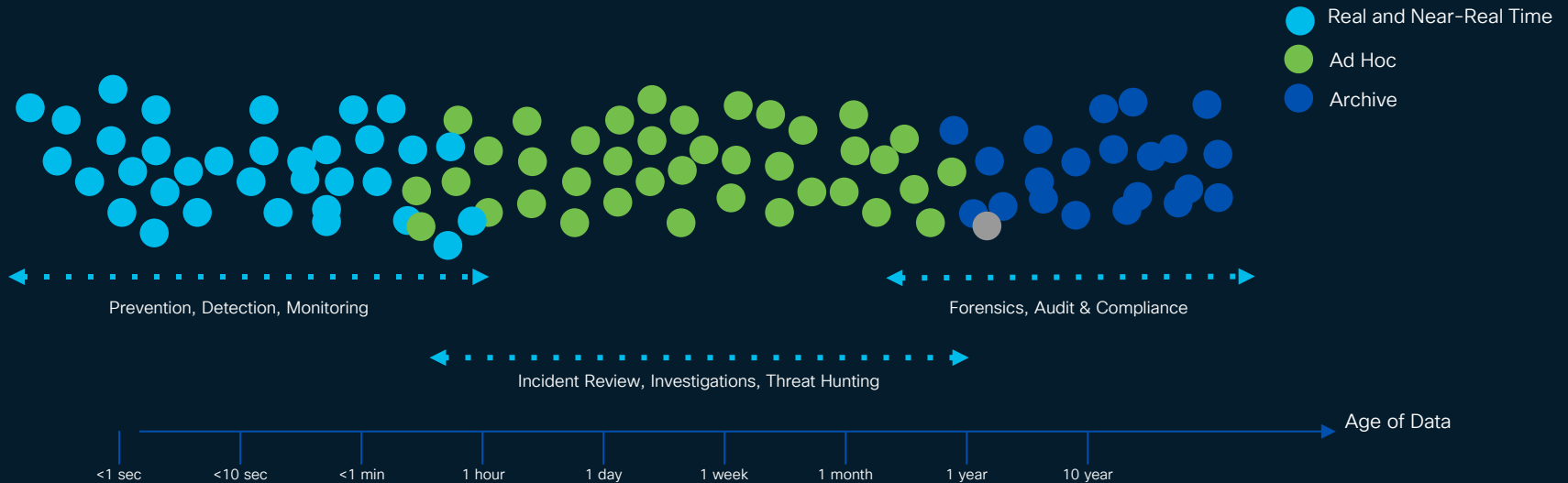
Data Tiering

Bringing a value-based approach to data strategy



Data Age and Applicability

Real Time vs Archive | Troubleshooting vs Analytics | Compliance



Questions



Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the **Cisco Stand Observability** 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

Contact me at: domuoyo@splunk.com



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC