

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Observability Convergence

Cisco + Splunk & Panel Discussion

Russ Atkin, Global Service Creation Lead, Managed Observability
@ruatkin
BRKAPP-2043

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/#BRKAPP-2043>





Agenda

- Observability Convergence
- Evolution to a SNOC
- Why O11y is Important
- Cisco+Splunk
- Panel Discussion

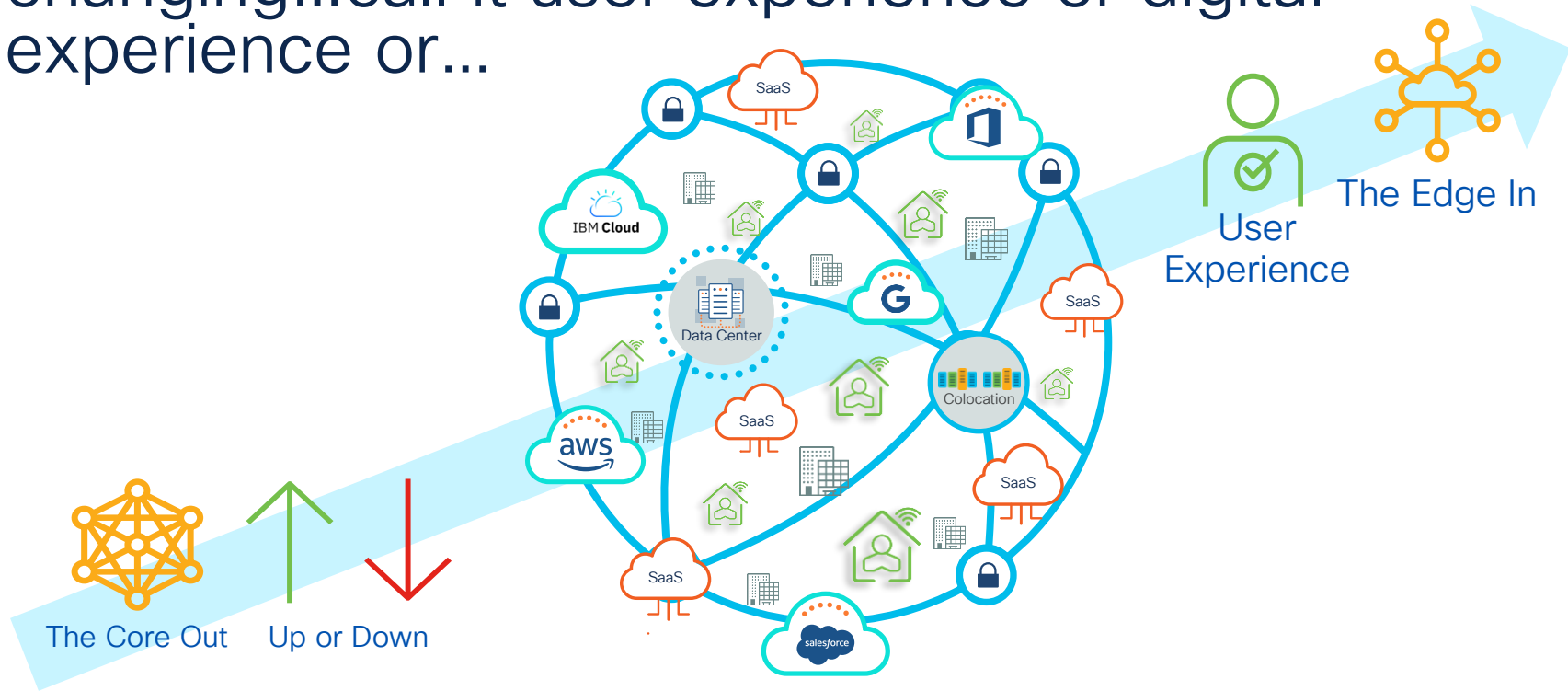
Our objective is to consider the art of the possible for O11y (Observability) Convergence.

- What are the challenges?
- What are the opportunities?
- How can Cisco+Splunk address these?
- How are MSPs and Customers managing this convergence?

Our intent is to spur conversation and collaboration on what good looks like.

Your feedback and comments are welcome and encouraged!

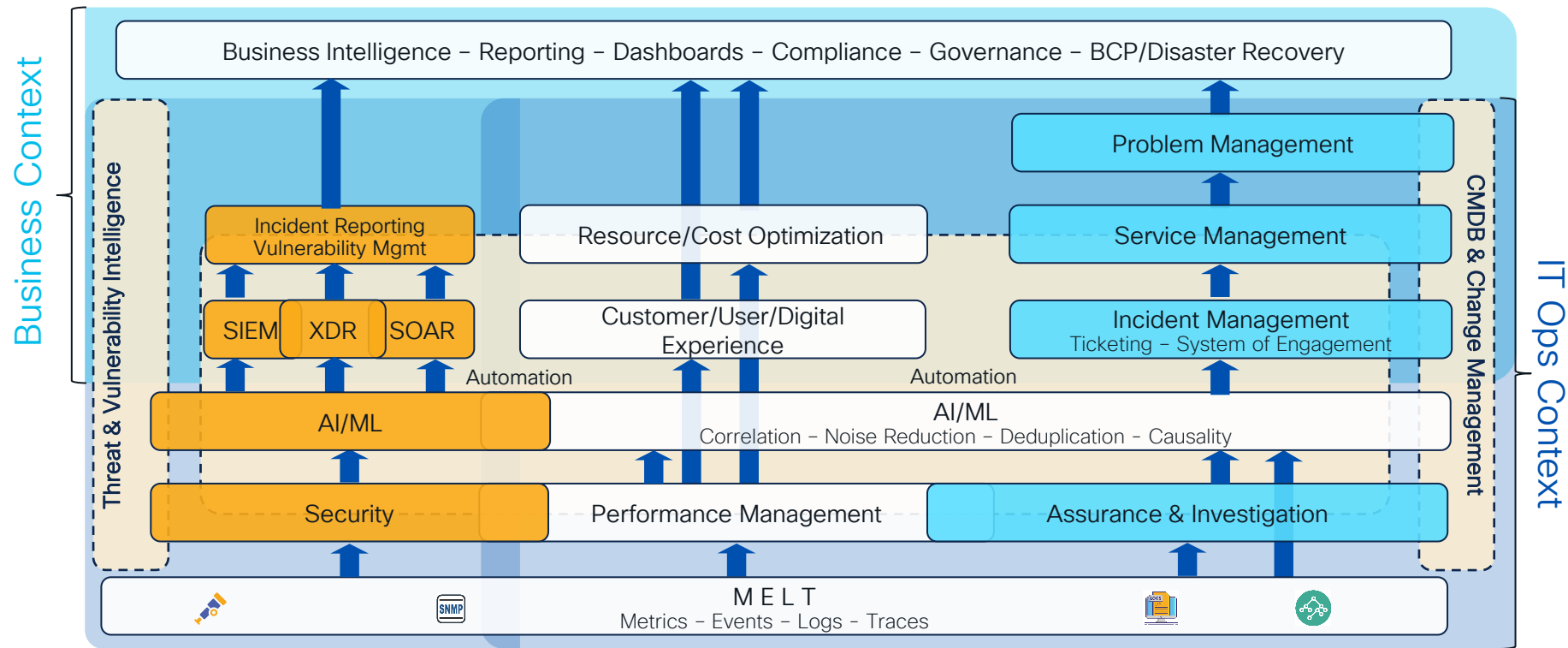
The way we manage our IT environment is changing...call it user experience or digital experience or...



Challenges

- Technology is converging however our Ops Teams are siloed and Root Cause becomes more difficult...
- Applications are everywhere
- Users are everywhere
- Customers want to engage via apps/web/in-person

Functional Architecture (ITOps, NetOps, DevOps, SecOps)



Tom Chan

Director Network
Solutions & Security

OPTUS

CISCO *Live!*



The Evolution of Enterprise Networking

Increased Complexity & Reach

- Cloud adoption
- Internet-based networking
- Hybrid work
- IoT growth

Security as a Core Service

- Firewalls as networking devices
- SD-WAN as firewalls
- SSE/SASE
- Zero Trust

Worlds are
converging,
and there are
no boundaries!

What are our customer's requesting?

Strong preference for a single managed provider

Expect faster incident response times

Desire for a unified approach with streamlined policy creation and orchestration

Need for greater visibility, policy enforcement, and stronger security posture

Impact on us as an MSP

Requirement for a single control plane

Need for operational efficiency, automation and get smarter

Importance of Secure By Design

Importance of Secure By Design

What Optus is doing

Single control plane for networking and security

Leveraging common tool sets, observability, intel feeds and data analytics

End to end inclusion of secure networking requirements

End to end inclusion of secure networking requirements

The Optus Integrated NOC and SOC

Heritage & Trust

- Large federal and state government agencies
- Banks
- Airlines
- Educational institutions

NOC + SOC

=

ASOC

GSOC

Integrated tools

- Splunk
- Talos
- Splunk Analytics
- Thousand Eyes
- Identity Services Engine

This enables us to provide managed secure networking,
tailored to **modern needs** and **future threats**

Customer benefits



Holistic IT Monitoring
and Management



Improved
Customer Experience



Compliance and
Data Protection



Cost Efficiency



Simplified Reporting
and Transparency



Incident Correlation and
Contextual Awareness



Enhanced security

Francesco Sbaraglia

SRE Tech Lead ANZ &
O11y Expert



CISCO *Live!*



Accenture Splunk Business Group

Accenture is the only Global Splunk Partner at scale, implementing some of the largest deployments in the world, driving joint innovation with Splunk

3300+ Joint Engagements	800+ Joint Clients	19+ Countries	8+ Years Partnership
-----------------------------------	------------------------------	-------------------------	--------------------------------



ASPBG Global Practice Use Cases

Observability	Security	DevOps	Business Ops
Multi-Cloud Monitoring	Advanced Threat Detection	Real-Time Observability with Monitoring and Diagnostics	Business Process Mining
Application Lifecycle Analytics	Insider Threats	Distributed Tracing	Customer Experience Optimization
Application Release Analytics	Incident Investigation and Forensics	Collaborative Investigation and Troubleshooting	Incident Management
Container Monitoring	SOC Automation	SDKs for GO, Python, JavaScript	Digital Marketing Optimization
Infrastructure Monitoring	Compliance	Intelligent DevOps	Predictive Analytics
E2E Monitoring	ICS Security	SRE Observability	SAP Monitoring

Accenture Splunk Partnership:

- Zeta Sponsor
- Global System Integration Partner of the year 2022/2023
- Rising Star of the Year 2024
- 9000+ Splunk Trained Globally
- 200+ Splunk Trained ANZ/APAJ





Challenges in modern Observability



Lack of Deep Visibility

- Fragmented tooling and data siloes
- High volume of alerts and noise
- Correlating metrics across distributed systems



Security and Performance Trade-Offs

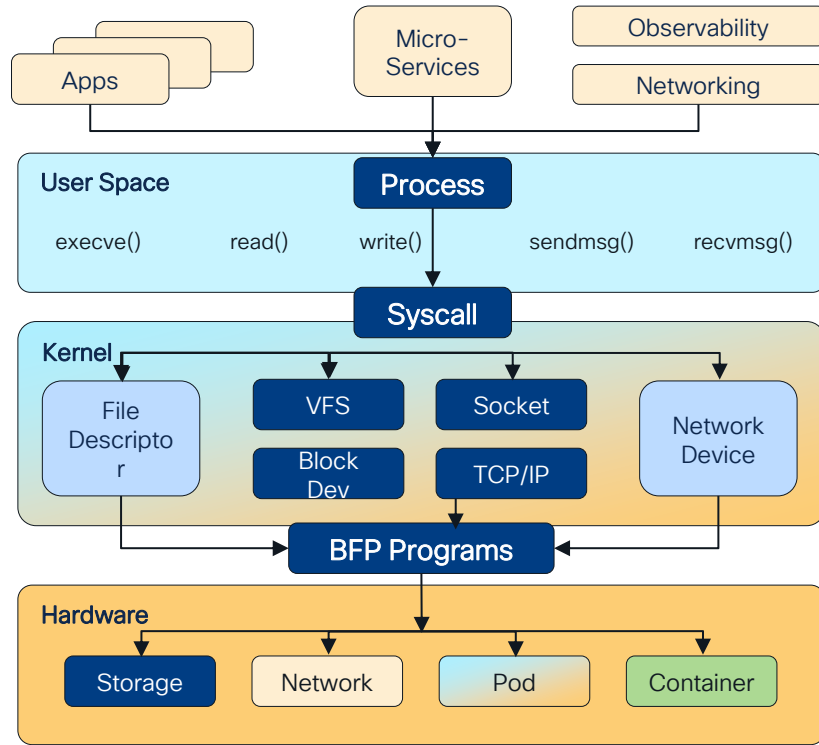
- Identifying and isolating performance bottlenecks
- Scalability in Large, distributed Networks
- Balancing Security and performance monitoring



Rising Complexity of AI Workloads

- Scaling AI Infrastructure
- Real-time Observability of LLM and RAG architecture
- Data Management and workflow complexity

Introducing eBPF



What is eBPF?

„eBPF, which stands for extended Berkeley Packet Filter, is an extraordinary technology with origins in the Linux Kernel, that can run sandboxed programs in a privileged context.”

Source: <https://ebpf.io/what-is-ebpf/>

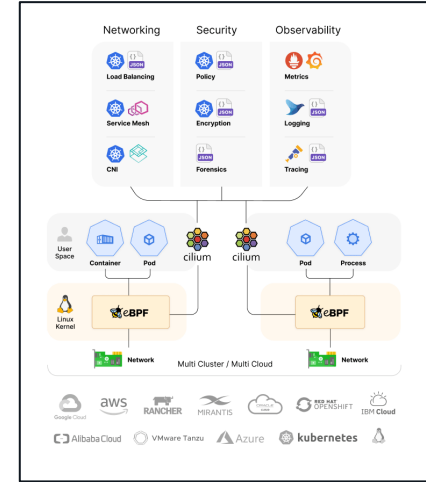
„... achieving passive observability service instrumentation and bring eBPF data into Splunk...”



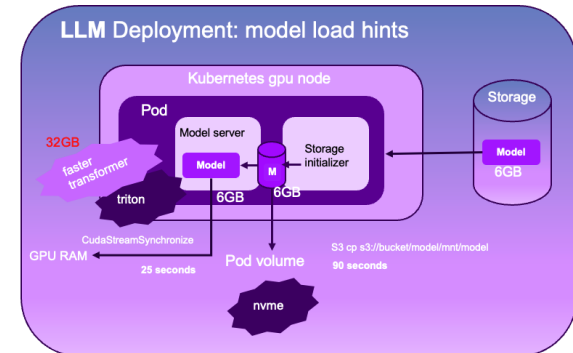
E2E Full Visibility across workloads

Modern Observability building blocks using Cisco and Splunk technologies

- **Full Visibility** via Cisco Hypershield. Cisco just acquired Isovalent, creator of Cilium. Cilium is based on eBPF. It is a unique new mechanism for observing, connecting and protecting multi cloud, sovereign-cloud and cloud-native workloads.
- **Hardware acceleration:** It takes advantage of DPUs (server Data Process Unit) and other HW accelerators in servers and other network infrastructure.
- **Optimized for AI:** Partnership with GPU-vendor to co-create security-specific AI models.



Source: isovalent.com

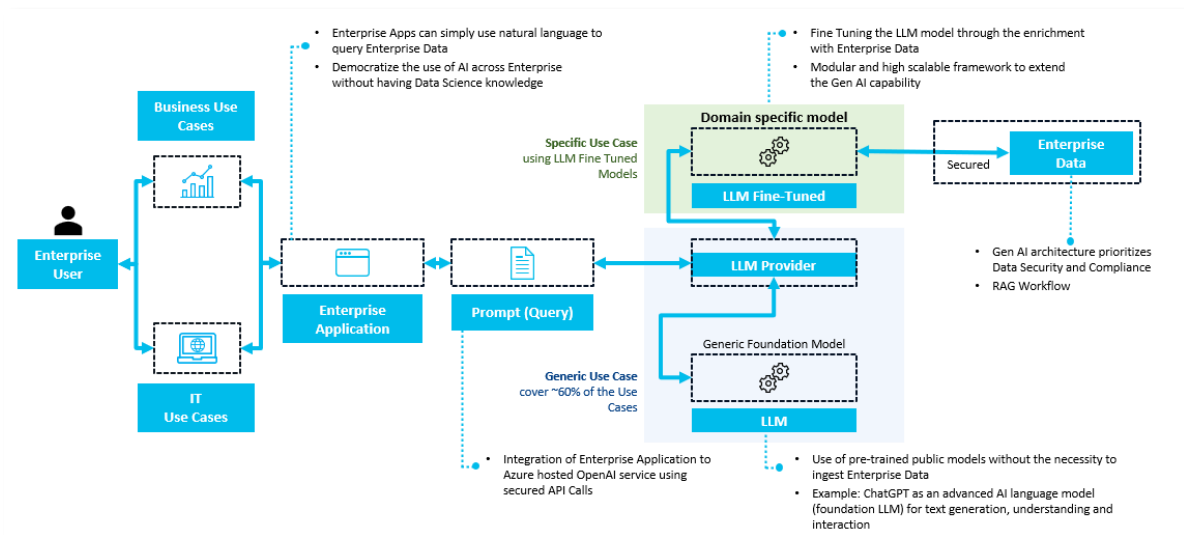


Future of Observability

Key Insights

- AI and Observability converge
 - Splunk Observability** for AI workload:
 - Trace your RAG pipeline
 - Trace Llama-Index-based RAG pipeline
 - Trace Prompt and Completions
 - Cisco Nexus Hyperfabric AI**
- Unified, Deep Observability
- Building resilience in Distributed Cloud-Native Systems
- Embedding AI/GenAI in Root-Cause-Identification

LLMOps Model Architecture



Matt Gillies
Cisco Fellow & Chief
Architect

Chris Crocco
Director, Observability
Technical Interlock

CISCO *Live!*



Digital resilience can:



Identify early signals
of disruption

Leverage real-time data
and insights



Prevent or reduce
impact

Enable mission-critical
service delivery



Continue to deliver
a good user experience

Provide uninterrupted
customer service,
minimize financial
losses, and prevent
reputational damage

Customers require proactive intelligence, predictive recommendations,
and automated remediation.

Digital resilience can:



Identify early signals
of disruption

Leverage real-time data
and insights



Prevent or reduce
impact

Enable mission-critical
service delivery



Continue to deliver
a good user experience

Provide uninterrupted
customer service,
minimize financial
losses, and prevent
reputational damage

Customers require proactive intelligence, predictive recommendations,
and automated remediation.

The path to greater resilience

Security
SecOps

Observability
ITOps,
Engineering

Foundational Visibility

See across hybrid
environments

Search and
investigate

Troubleshoot with
log analytics

Prioritized Actions

Understand risk
and performance

Expand monitoring,
alerting and
response

Understand
service health

Proactive Response

Get ahead of
issues

Deliver situational
awareness and
automation

Help ensure reliability
of consumer-facing
web applications

Optimized Experiences

Delight customers
and build trust

Achieve real-time
risk insights

Deliver exceptional
digital customer
experiences

Digital Resilience at Enterprise Scale

Managing network data with Splunk

Data Sources

Traditional Monitoring



Syslog



SNMP

Streaming Data



Netflow



Telemetry

Microservice and Cloud



Data Collection/Management



Technical Add-Ons (TAs)



OpenTelemetry (OTel)



Splunk API Endpoints

Splunk Platform



Performance Monitoring



Incident Management



AI Analytics and Insights

What's OpenTelemetry?

Standardizing data collection

OpenTelemetry is robust, portable telemetry as a built-in feature of cloud-native software.

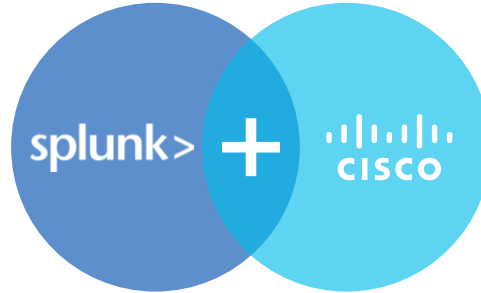


- The standard for getting data into an observability system
- A framework (featuring SDKs, a collector, semantic conventions, etc.) for observability data
- A wire protocol (OTLP); a library of components to receive, process, and export data in a flexible, open way

Easy onboarding of the data you need



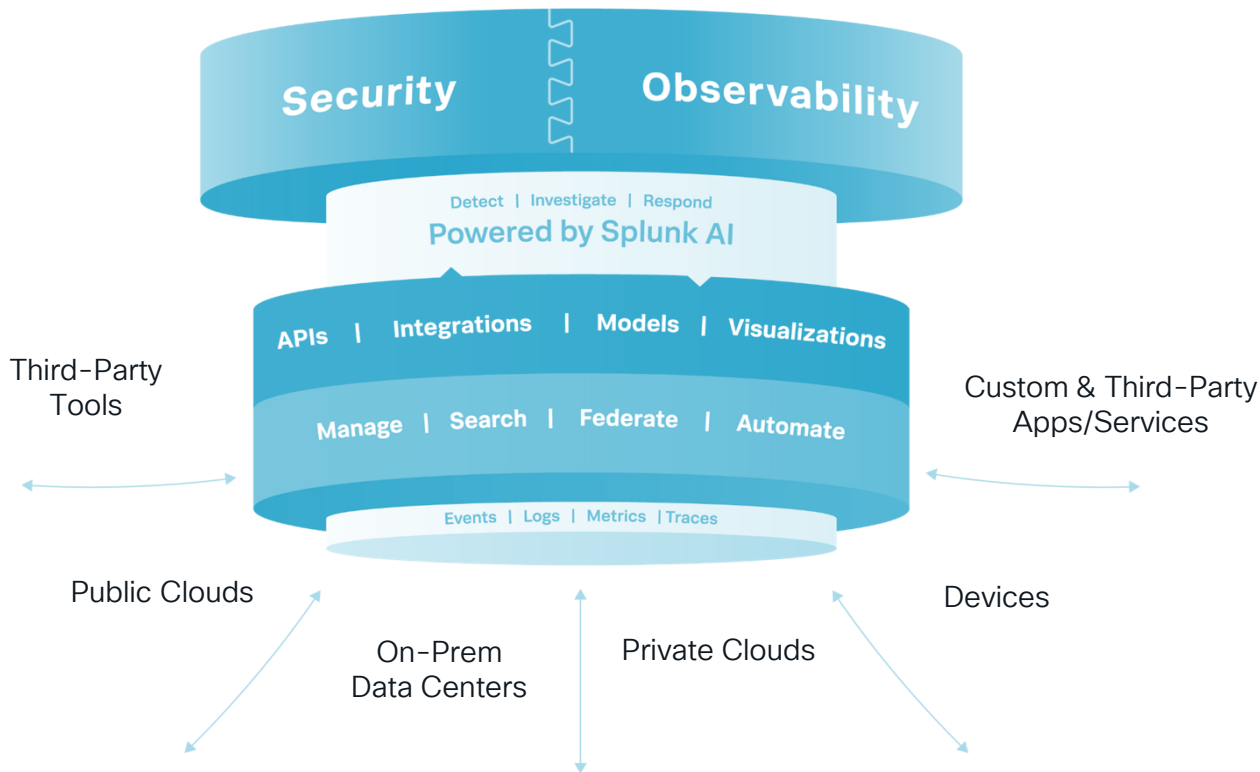
Open standards-based agent for metrics, traces, logs, and more for more control and greater ROI of infrastructure and application data



Splunk TAs

Normalization and optimization of data for specific technologies, data types and use cases, optimized for easy access and action on well-known data sources

Make your organization more resilient with Splunk



Full-Stack end-to-end

Seamlessly integrated UX,
context and workflows

Synthetics

Infrastructure
Monitoring

APM

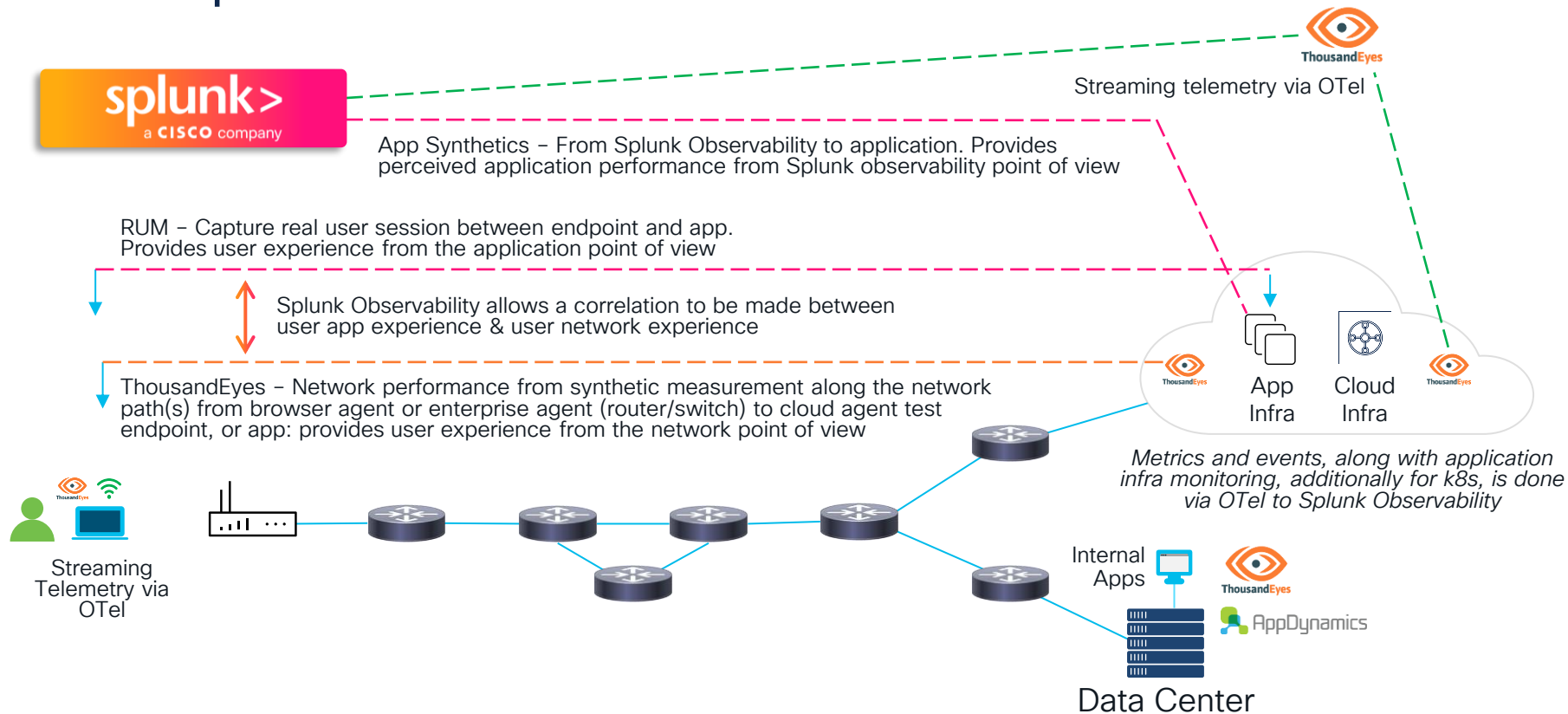
On-Call

RUM

Log Observer

IT Service Intelligence

End-to-end application observability for the enterprise



(Demo) - Cisco Live Melbourne

Auto Refresh: 10 minutes ▾ Last 4 hours ▾ Save as... Save L7

Filter services Corporate IT x

Filter by tags Select tags to monitor

Minimum Severity None ▾

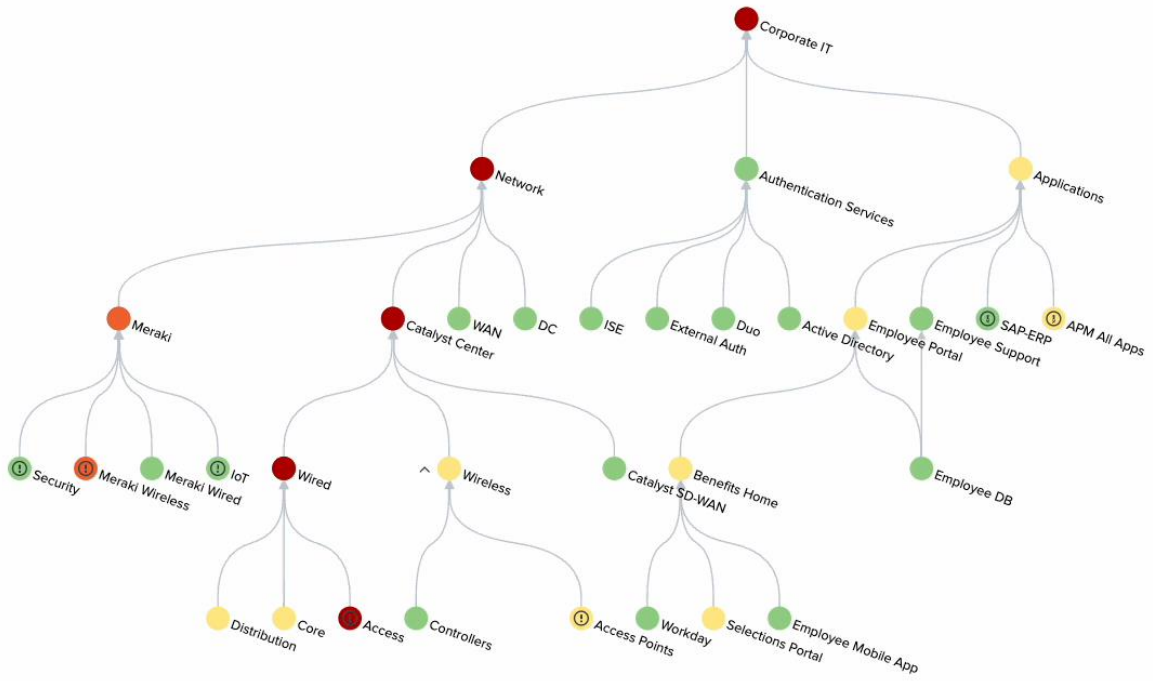
Filter by Service Depth

Maximum Depth: All ▾

KPI Value: Aggregate ▾

⌵ ⌵

Go to service 🔍

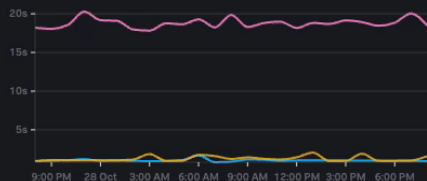




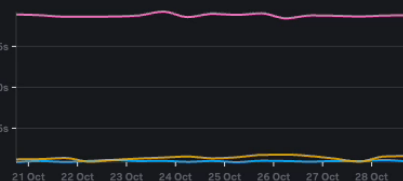
✓ Every 5 minutes from 1 location. <https://employeebenefitsdemo.splunko11y.com> Last run today at 8:33:15 PM

[Edit test](#)[Create Detector](#)

Last day



Last 8 days



Last 30 days



Uptime Trends



Availability

Performance KPIs

MDT -06:00
-8h

Segment By

Location

Filter

AWS - N. Virginia

(1)

Search Metrics

Run duration, First TCP connect...

(2)

Result

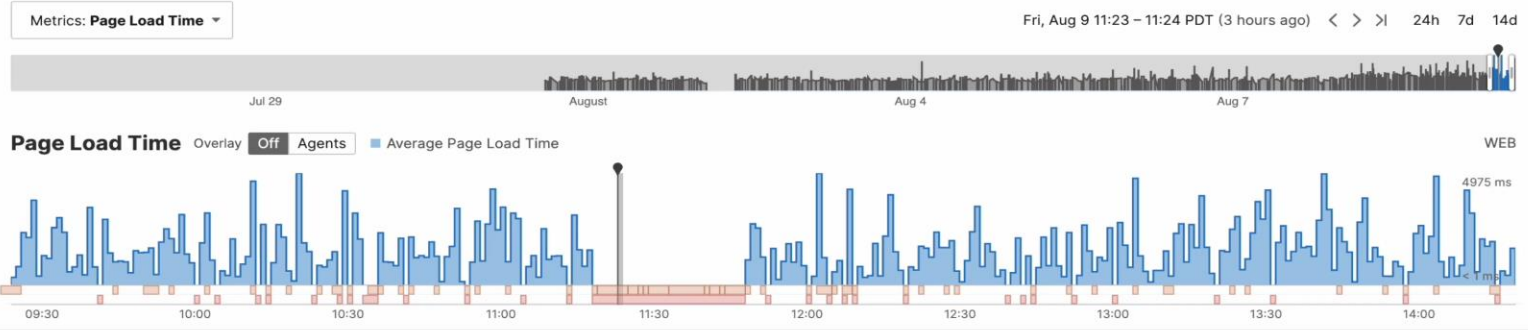
All



Run duration - AWS - N. ... 18.67s
First TCP connect time - ... 69.30



- Page Load** **Web**
- HTTP Server **Web**
- Agent to Server **Network**



Map Table Waterfall **Select an Agent**

Agent **PseudoCo Brunch**

Page Title **http://192.168.100.2/test1.html**

Chromium **118 (1 Agent)**

Version

Page Breakdown 1 resource (0 kB)

Domain	Provider	Type
--------	----------	------

Metrics



(Demo) - Buttercup Retail

Auto Refresh: 10 minutes

Last 4 hours

Save as...

Save



Filter services Buttercup Retail

Filter by tags Select tags to monitor

Minimum Severity None

Filter by Service Depth

Maximum Depth: All

KPI Value: Aggregate



Go to service



Panel Discussion

Matt Gillies
Cisco Fellow &
Chief Architect



Chris Crocco
Director,
Observability
Technical Interlock



Tom Chan
Director Network
Solutions & Security



Francesco Sbaraglia
SRE Tech Lead ANZ,
Olly Expert & Author



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 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



Thank you

CISCO *Live!*

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC