Cisco Tech Day

Denver

March 3, 2026

Network Observability with Cisco & Splunk

Cisco Tech Day
Denver

Chris Crocco

Director – Observability Technical Interlock, Splunk/Cisco

Agenda

01 **The reality of Modern Enterprise Networks**

02 **The challenges faced by network teams**

03 **Why traditional monitoring falls short**

04 **Cisco Integrated Assurance Architecture**

05 **Maturing monitoring to observability**

06 **Real world examples**

07 Demo

08 Questions

The reality of
Modern Enterprise Networks

Modern networks are growing in complexity & demand

More network dependencies lives outside the enterprise walls than ever before (SaaS, Cloud, etc.)

More sophisticated threats to manage across distributed and dynamic edge (SASE, SD-WAN)

More Edge computing and IoT devices proliferating network traffic and telemetry (flows, metrics, logs)

More noise and alert fatigue across multi-vendor environments and multi-AI agent architectures

cisco

Challenges of Hybrid Environments

Lack of Visibility

Unable to determine if degradations or downtime are due to owned or unowned networks

Complex Toolset

Multiple domain controllers and monitoring tools makes unified observability difficult

Poor MTTx

Detecting degradations, defining root cause and remediating issues is manual, siloed and error-prone

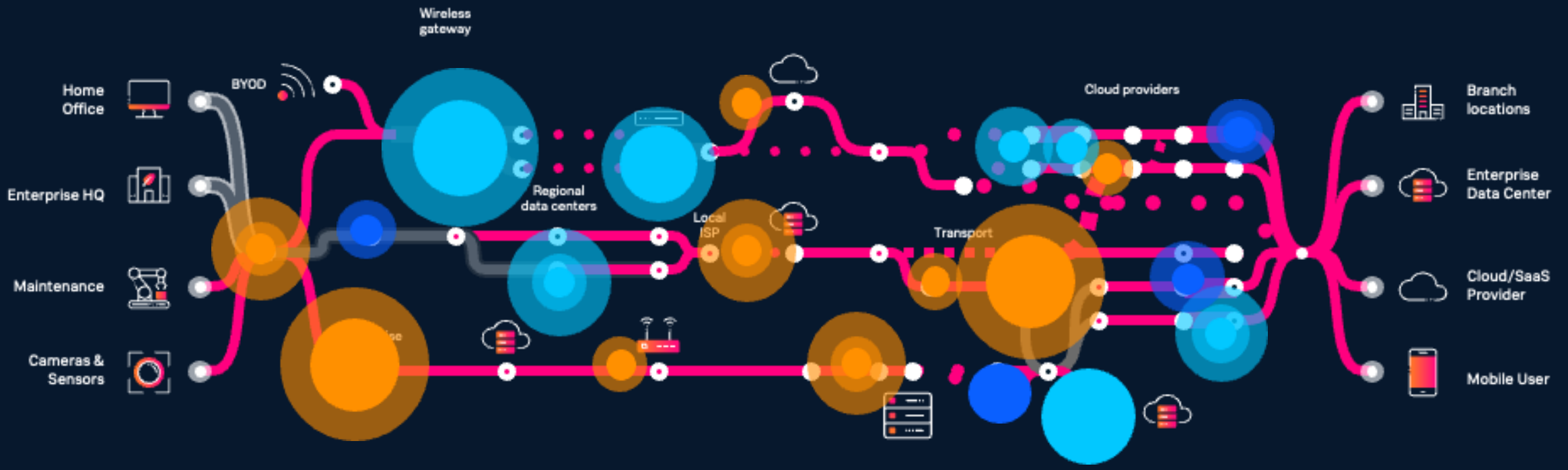
Scale Difficulties

Gathering data across different controllers, regions, and clouds can be difficult and inconsistent

cisco

Challenges we face as network teams

Complexity creates risk

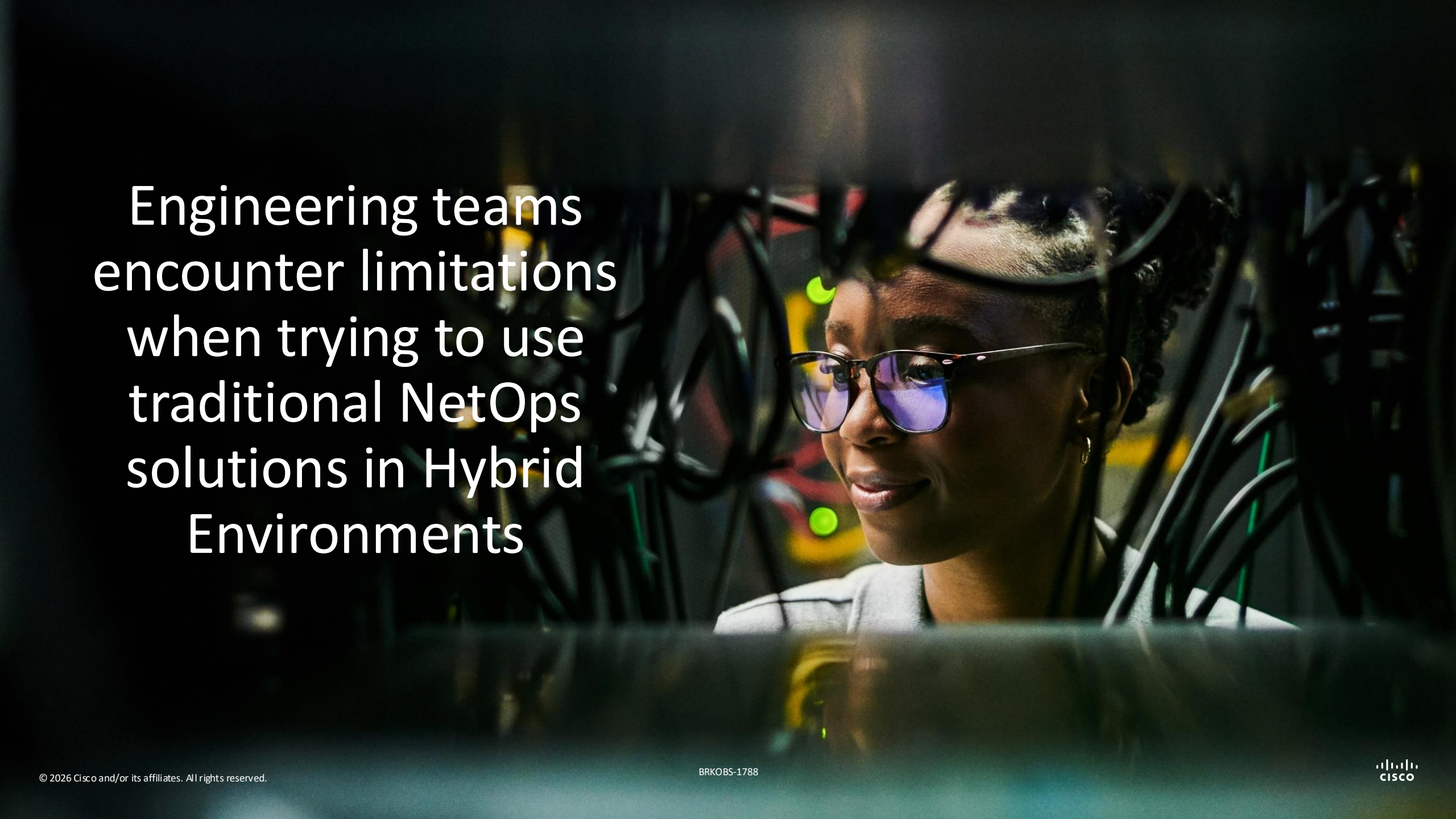


Human-caused issues

Hardware issues

External Networks

Engineering teams encounter limitations when trying to use traditional NetOps solutions in Hybrid Environments



cisco

Limitations of traditional Network Operations

- Device-centric monitoring misses user experience
- Internal telemetry ignores internet paths
- Logs without service context lack meaning
- War rooms driven by opinion, not evidence

Maintaining silos exacerbates operational challenges

Increased Noise-to-Signal

No context between business impact, alert correlation or external dependencies has application, network and security teams pointing fingers at each other

Data Fatigue is real

Every device, application, and client is emitting data, and the volume is growing faster than most teams can respond with existing controllers.

Focus on reaction over experience

Processes and tooling are focused on reacting to incidents after they occur (Up/Down) instead of proactive network performance

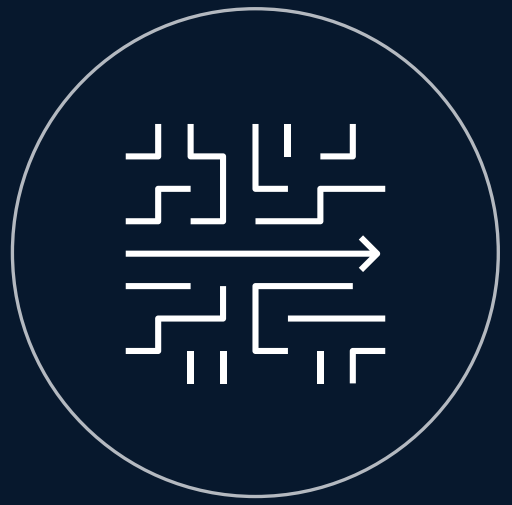
Persistence of silos within the network

Point solutions and vendor-provided monitoring lacks end to end context, resulting in no single, constant source of truth

Most teams aren’t struggling to detect issues — they’re struggling to **explain them quickly and** accurately.

Silos | Visibility | Action

Building blocks for Network Observability



Telemetry Data

- **Logs** (connection attempts, routing updates, etc.)
- **Flow data** (NetFlow, sFlow, IPFIX)
- **Metrics** (bandwidth usage, packet loss, latency)
- **Traces** (End-to-end records of request paths through the network

Instrumentation

- **Agents and Probes (Devices, endpoints, CSPs)**
- **Model-Driven Telemetry (Pushed from the device)**
- **SNMP (Polling AND traps)**
- **Streaming Telemetry (Structured device-level data)**

Data Correlation and Analytics

- **Multi-source analytics**
- **Schema-on-the-fly queries**
- **Actions from insights**
- **Data tiering and aggregation**

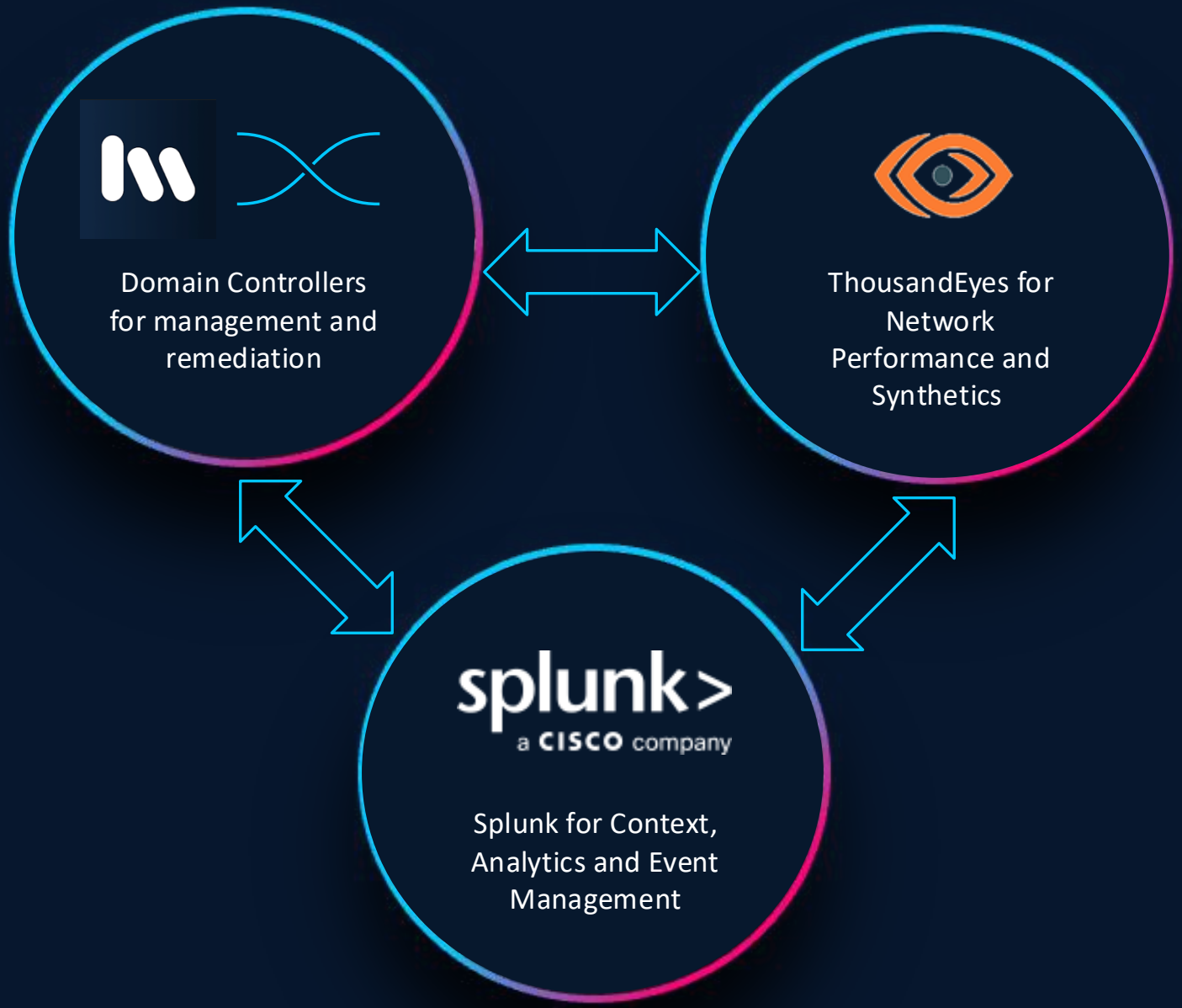
Alerts and Dashboards

- **Dashboards (pre-configured and customizable)**
- **Actionable notifications and output from alerts**
- **Topological views for specific data types**

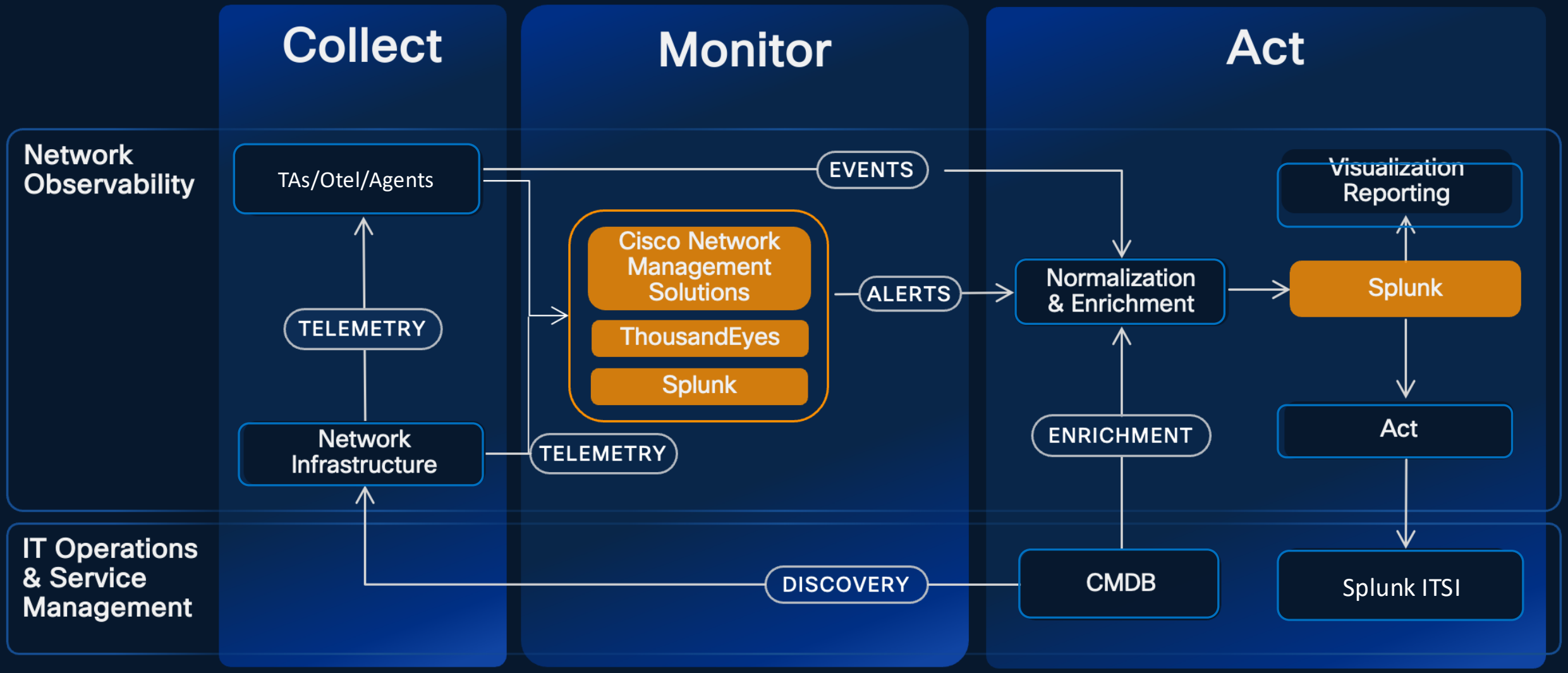
cisco

How Cisco solves Network Observability

Complimentary Network-specific solutions from one vendor



Three Pillars of Network Observability



Managing network data with Splunk

Data Sources

Traditional Monitoring

Syslog

SNMP

Streaming Data

Netflow

Telemetry

Microservice and Cloud

gRPC

Data Collection/Management

Technical Add-Ons (TAs)

OpenTelemetry (OTel)

Splunk API Endpoints

Splunk Platform

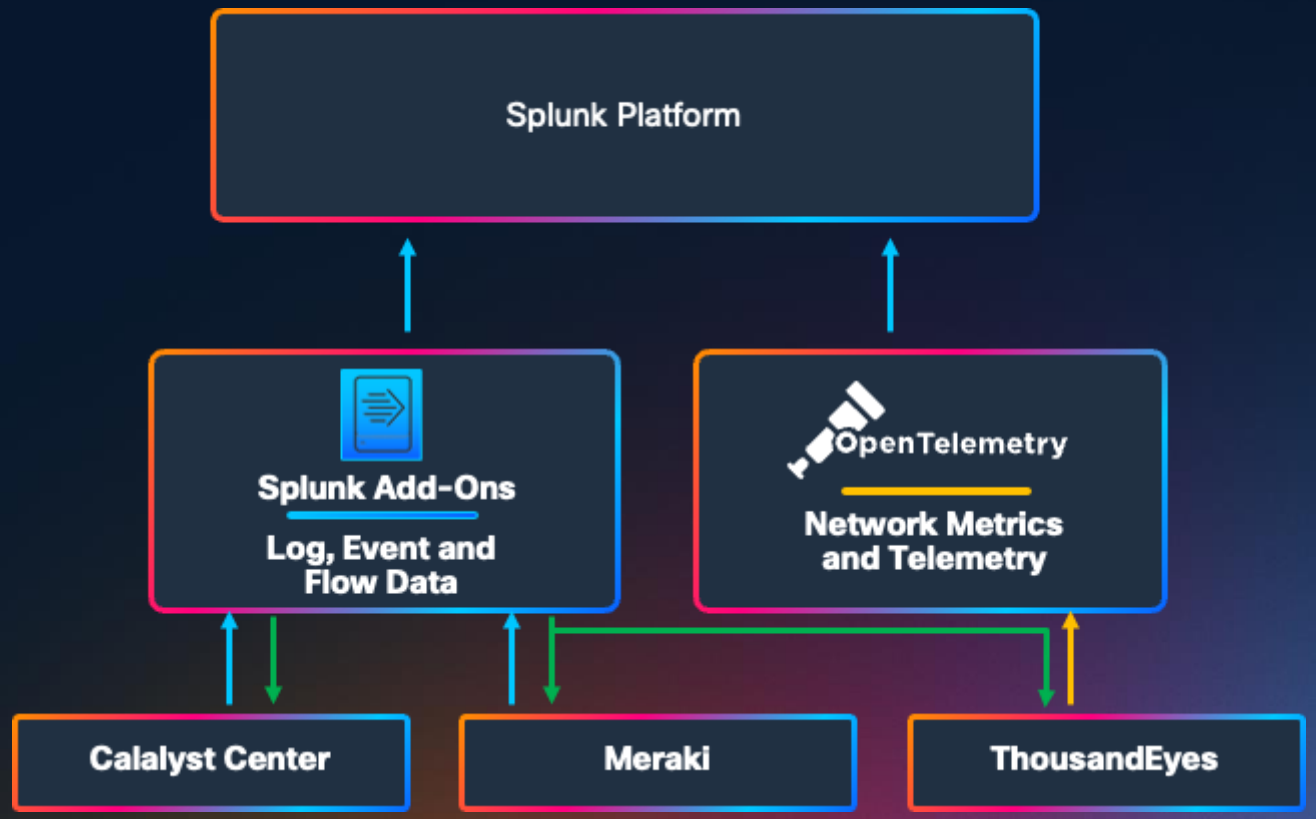
Performance Monitoring

Incident Management

AI Analytics and Insights

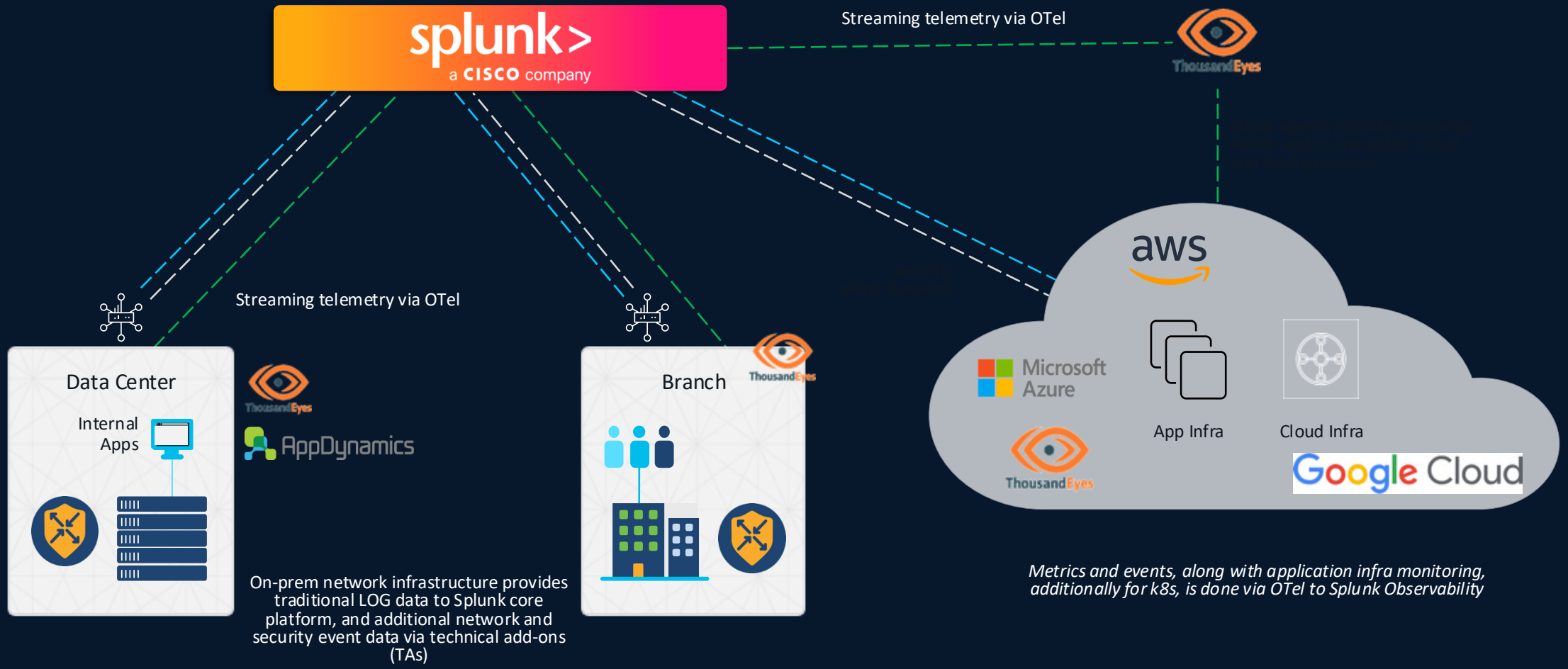
cisco

Centralizing the data you need

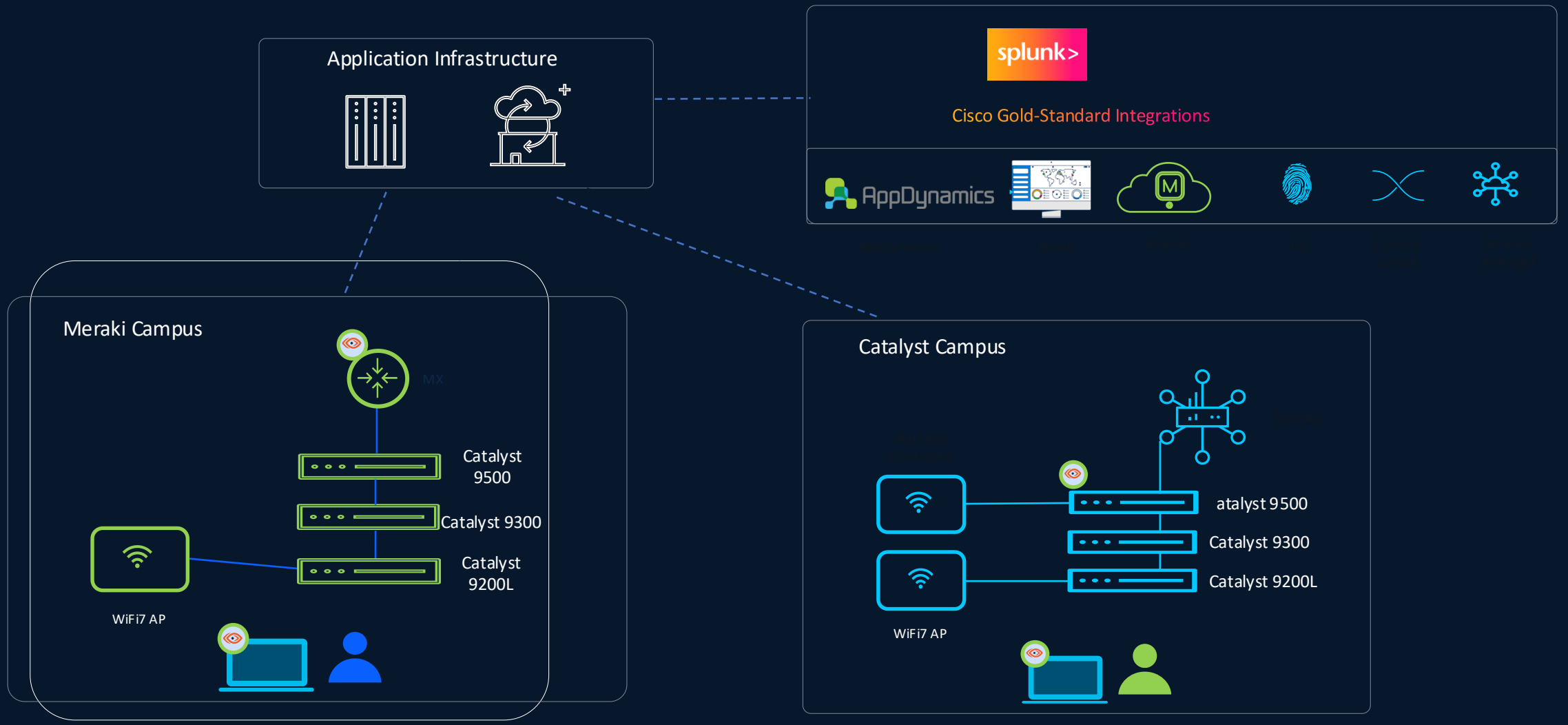


- Consolidated visibility across Meraki, ThousandEyes and other Domain Controllers
- Cross-domain correlation, analytics, and AI insights
- Unified visualization and alerting
- Single vendor support across network, synthetics and observability solutions
- Extensible with other Cisco Enterprise Network Splunk integrations

End-to-end application observability for the enterprise



Expanding Observability to Enterprise Networks

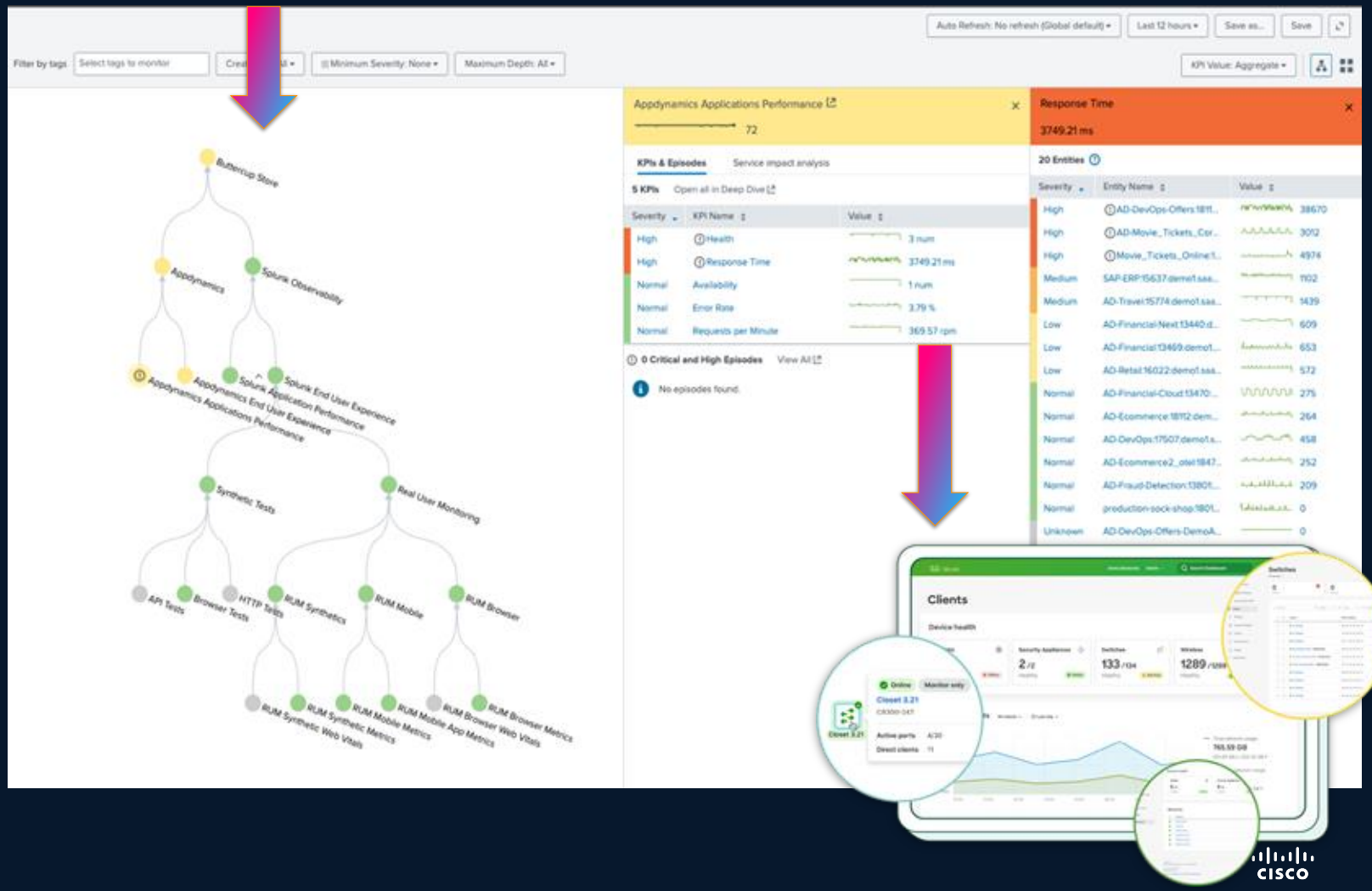


GA

Splunk ITSI & Cisco Enterprise Networking

Enterprise Network Monitoring for branch & campus to quickly pinpoint site & device issues in Cisco networks

- Integrations with Catalyst Center and Meraki
- Cross-domain correlation for reduced alert noise and domain isolation
- Out-of-the-box topology to measure the health of a location (e.g. retail store) and isolate problematic devices
- Device alert import, normalization, deduplication, and correlation logic
- Insights for problem troubleshooting (e.g. recent configuration changes)
- In-context guidance into Catalyst Center & M



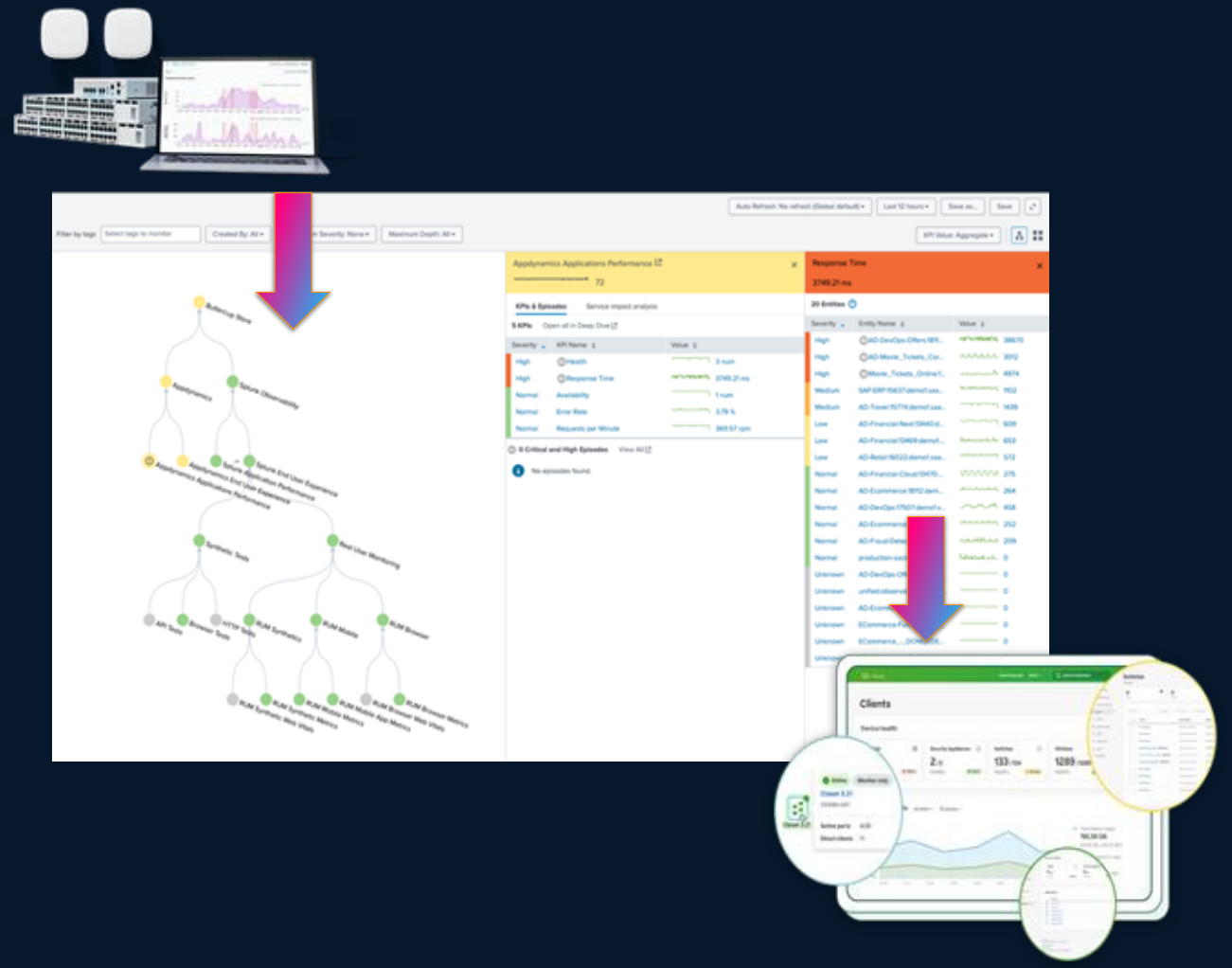
Let's see it in action!

Real World Examples

Network Engineering & Architecture

Scenario: Hybrid WAN and Cloud Connectivity rollout

- Catalyst Center provides deterministic core and WAN behavior
- **Meraki Accelerates Branch Deployment**
- **ThousandEyes validates paths pre and post change**
- Splunk ITSI tracks performance and configuration impact

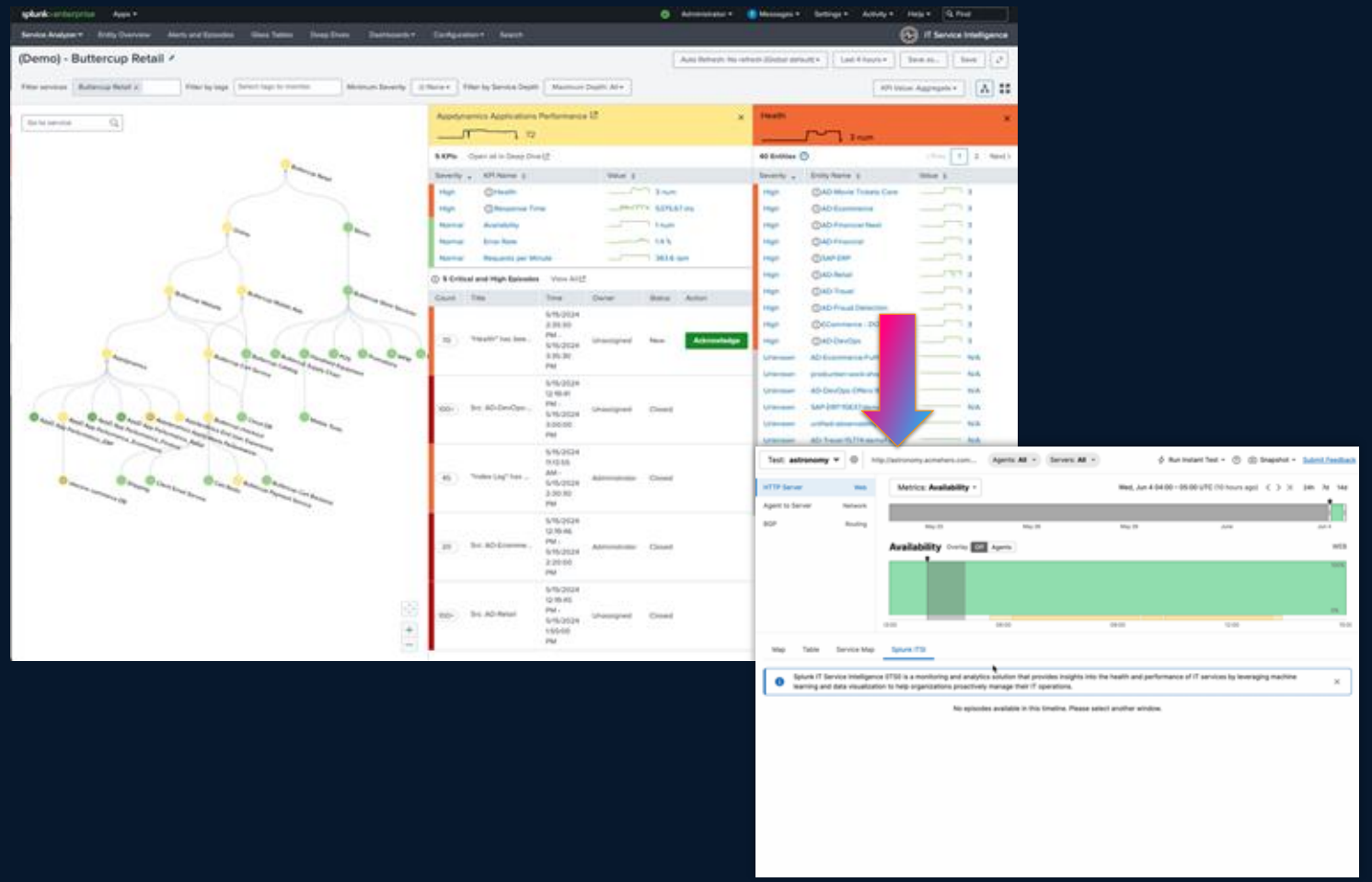


Outcome: Predictable deployments and measurable outcomes

NOC & Operations Leadership

Scenario: Widespread performance degradation across regions

- **Device Telemetry Consolidated in Splunk**
- **Splunk ITSI App correlates events into Service Impacting Issues**
- **ThousandEyes identifies ISP-Level Latency**
- **Streaming Telemetry (Structured device-level data)**



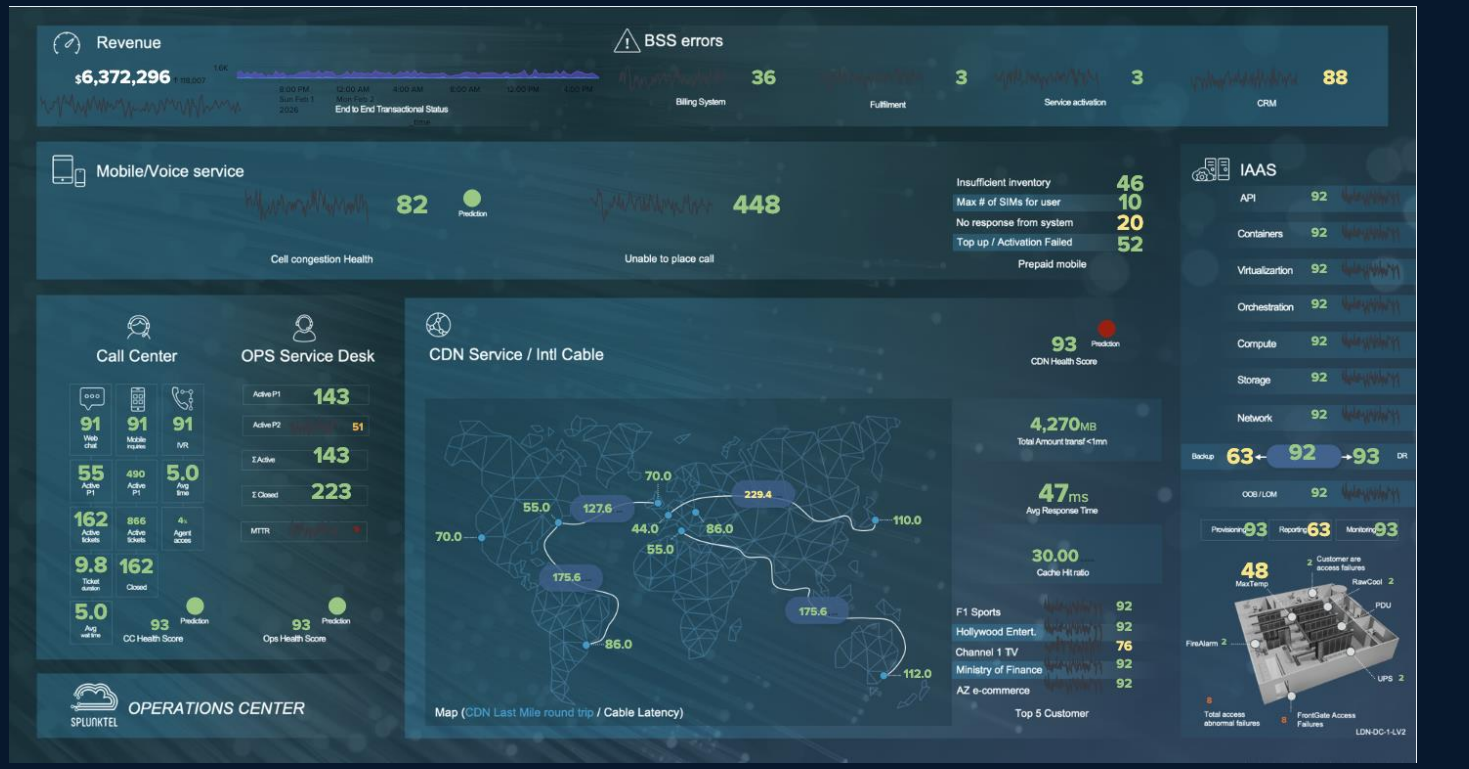
Outcome: Faster MTTR with minimal escalation

Service Reliability & Executive Escalations

Scenario: Intermittent SaaS degradation reported by employees

- **ThousandEyes exposes cloud routing instability**
- **Splunk correlates user experience and error logs**
- **Splunk ITSI quantifies business impact**
- **Network teams validate internal health**

Outcome: Clear accountability and informed escalation



If you remember nothing else from this session...

Observability and Monitoring are not the same

True network observability allows for contextual insights into network performance at any time, not just when things are breaking

Network Observability requires cross-domain visibility

Unifying your analytics, visualization, alerting and storage across domain controllers reduces MTTx, streamlines processes, and provides your teams with a consistent and complete observability solution

Splunk provides these solutions today

Splunk integrates with Cisco, and non-Cisco network data to provide a rich and complete Network Observability solution aligned to best practices

cisco

Cisco on Cisco stories

Cisco IT modernizes network observability strategy to automate 99.998% of 4M daily alerts

“Now that we have this unprecedented network visibility, we can proactively solve issues before users are impacted — making us a stronger, more resilient organization."

Manny Garcia
Distinguished Engineer
Cisco IT

Get the full story

How to get started

Meraki Add-On for Splunk

https://splunkbase.splunk.com/app/5580

ThousandEyes Add-On for Splunk

https://splunkbase.splunk.com/app/7719

Splunk App for Enterprise Networks

https://splunkbase.splunk.com/app/7539

Questions

Thank you to our sponsors!

World Wide Technology, Inc.

PRESIDIO®

CROSSCONNECT ENGINEERING

CompuNet

Qumulo

e+

anm

ONSTAK

Where Technology Means More®

NUTANIX

wyebot™


CISCO