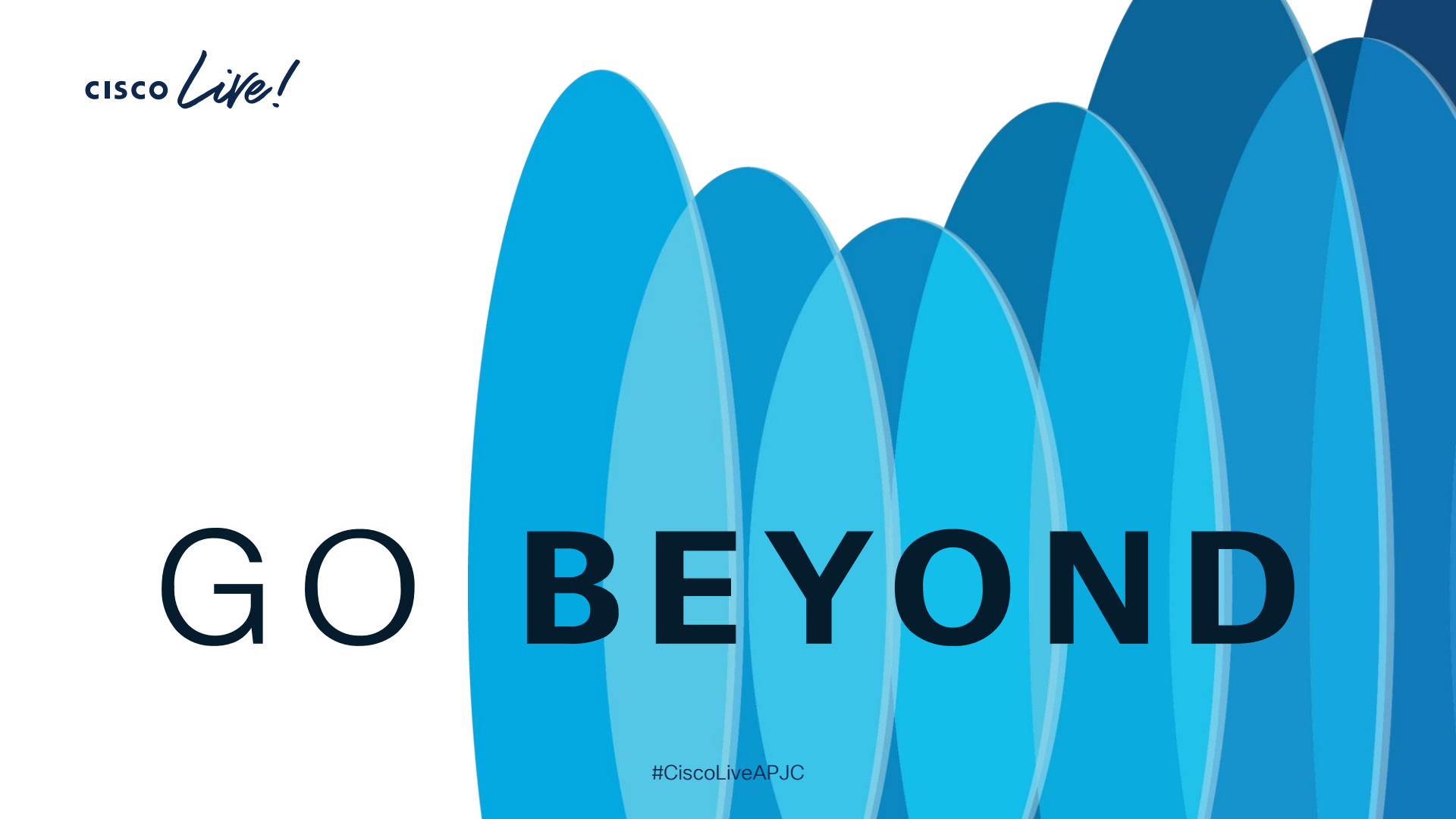

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Build Scalable Data-Driven Networks Using Splunk for Service Providers

Raman Jain – Principal Splunk Solution Architect

BRKSPG-2589

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/#BRKSPG-2589

cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Agenda

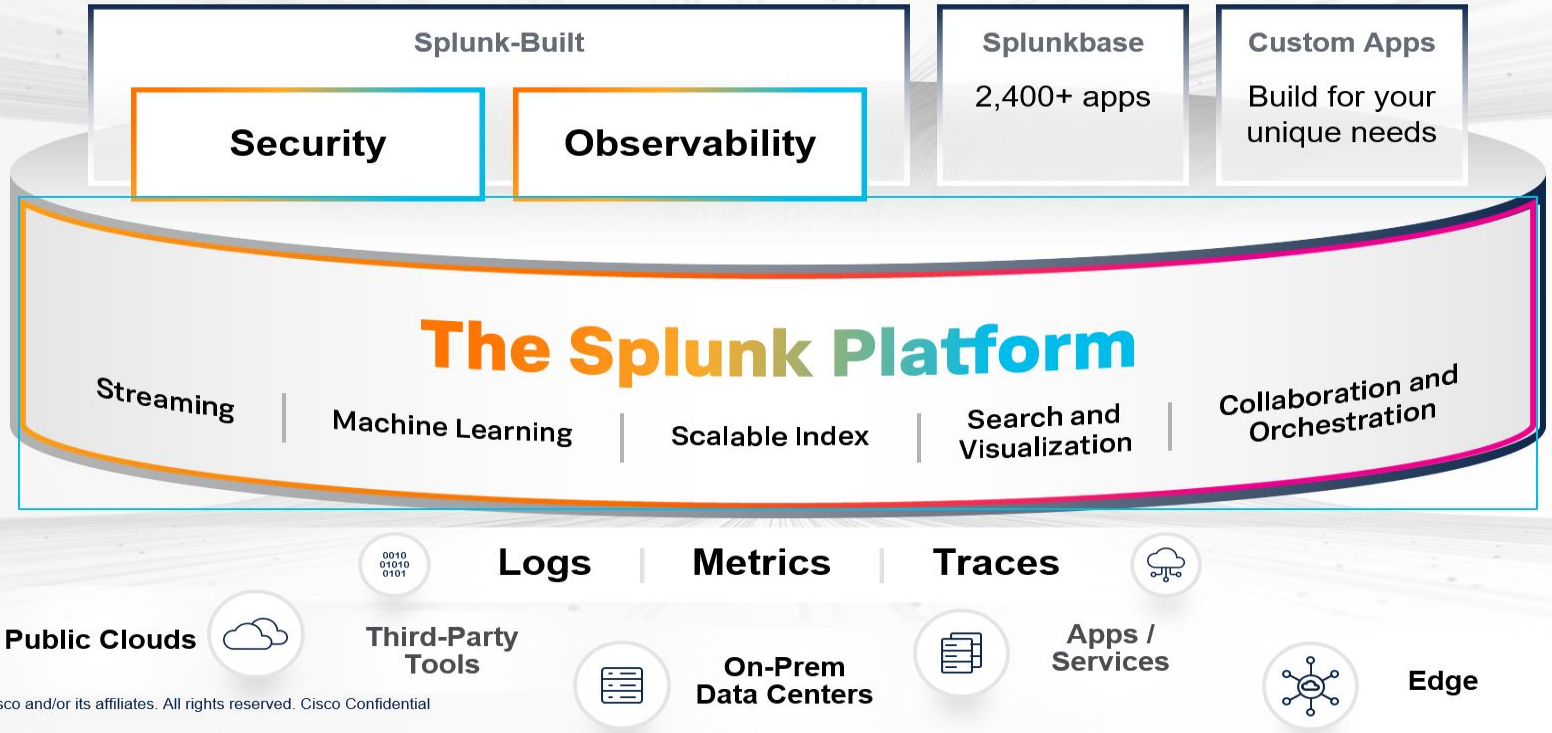
- Splunk scalable data platform
- Evolution of network monitoring
- Data-Driven networking use cases
- How service providers are using it – AI Driven Closed Loop Automation
- Takeaway - Splunk guide for CSPs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk Platform Recap

cisco Live!

Introducing Splunk Platform

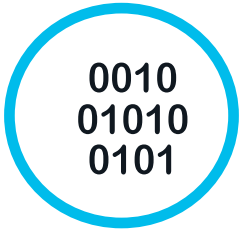


Cisco and/or its affiliates. All rights reserved. Cisco Confidential

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

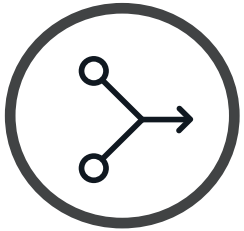
Scalable Index

What: Any and All Data



Index Any and All streaming, machine, and historical data

How: Point it at a Source



Point Splunk at a data source–tell it a bit about the source–that source becomes a data input

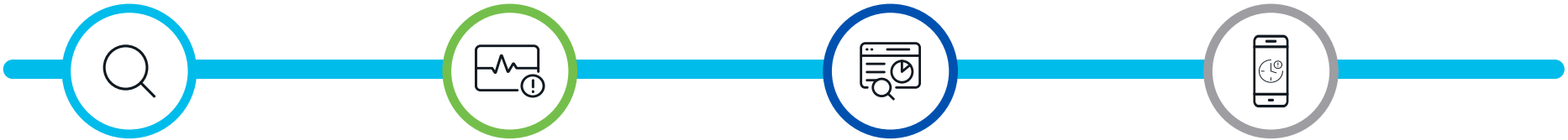
Then: Turn Source into Stream of Events

Splunk indexes the data stream and transforms it into a series of events–you can view and search those events right away

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Search and Visualisation

Use Search Process Language (SPL) to search and investigate your data across cloud or on prem deployments to find the needle in your haystack



✓Search Any Data Source

✓With Schema-on-the-Fly you can search any data source regardless of structure and across cloud or on prem deployment

✓Train and apply ML

✓Identify outliers, predict, classify, and forecast

✓Visualise and Save Dashboards

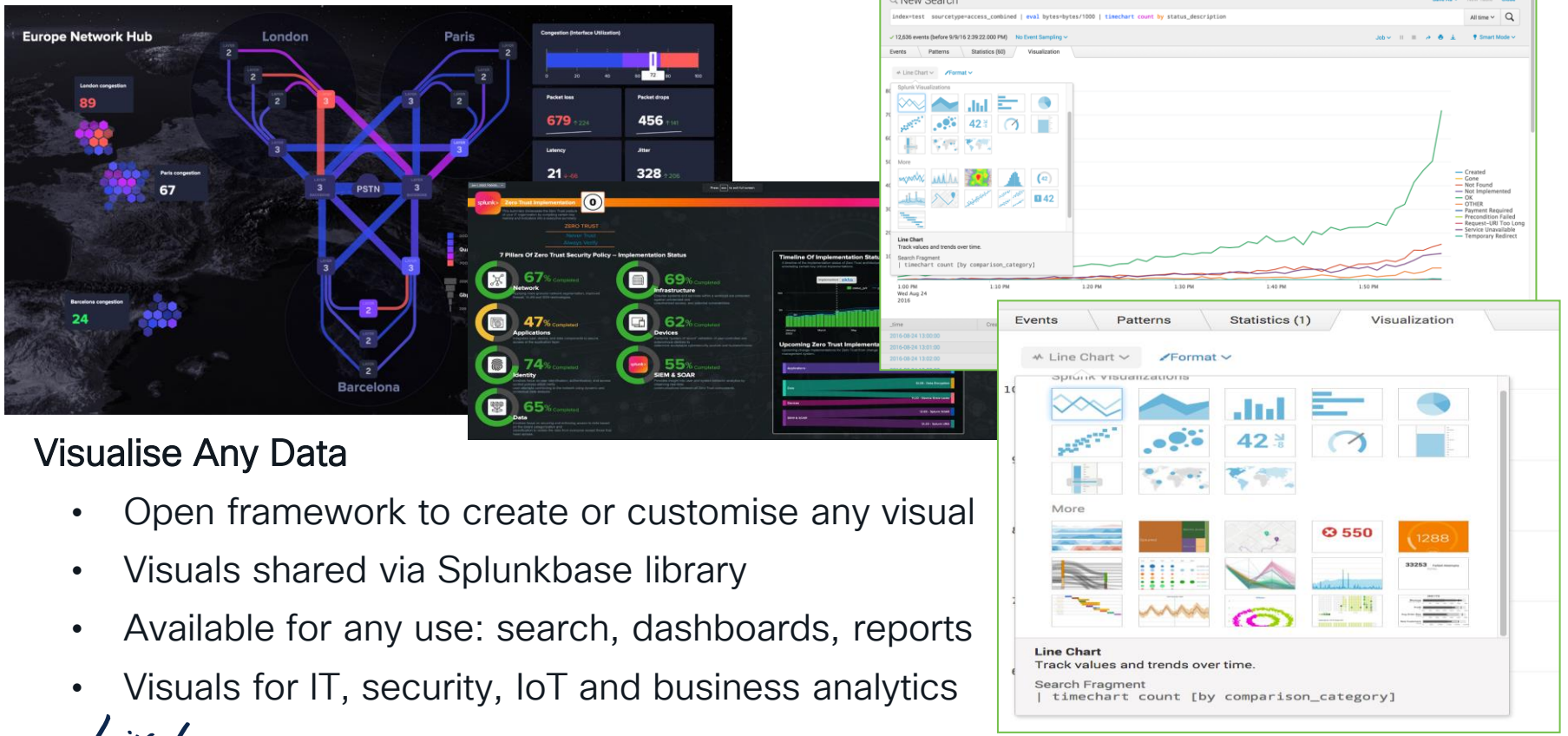
✓Add visualisations and save as dashboards

✓Create Ad Hoc Alerts & Automate

✓Create ad hoc alerts when you discover new issues or threats

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Reporting & Visualisations



Visualise Any Data

- Open framework to create or customise any visual
- Visuals shared via Splunkbase library
- Available for any use: search, dashboards, reports
- Visuals for IT, security, IoT and business analytics

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Industrial IoT Hub Data Integrations

- Complete Industrial IoT Solut Offering

1 IoT Hub Built-in Sensors

Light
High sensitivity light sensor

Temperature
(±0.2°C from 0°C to 90°C, IP67 rated membrane

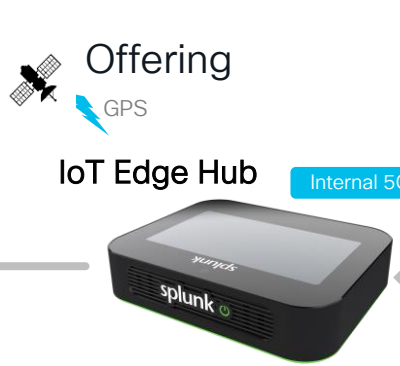
Humidity
(±2% from 0°C to 90°C)

Sound
Microphone - See Vesper VM1000 Spec Sheet

Vibration
3-Axis Accelerometer - See Bosch BMA456

Gyroscope
6-Axis Gyro & Accelerometer - See TDK ICM20600

Optional : Pressure, VOC w/ Gas Analysis
(300...1100 hPa) ± 0.12 hPa for Pressure, < 1s response with IAQ Score Output for Gas



3 Existing Industrial Control Systems

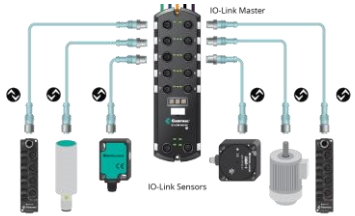
PLCs / RTUs
Programmable Logic Controls, Remote Terminal Units

OPC Servers
Industrial Control system statistical acquisition

SCADAs / HMIs
ICS control / management applications

Historians
Manufacturing statistical database

SPCs
Statistical Process Control applications

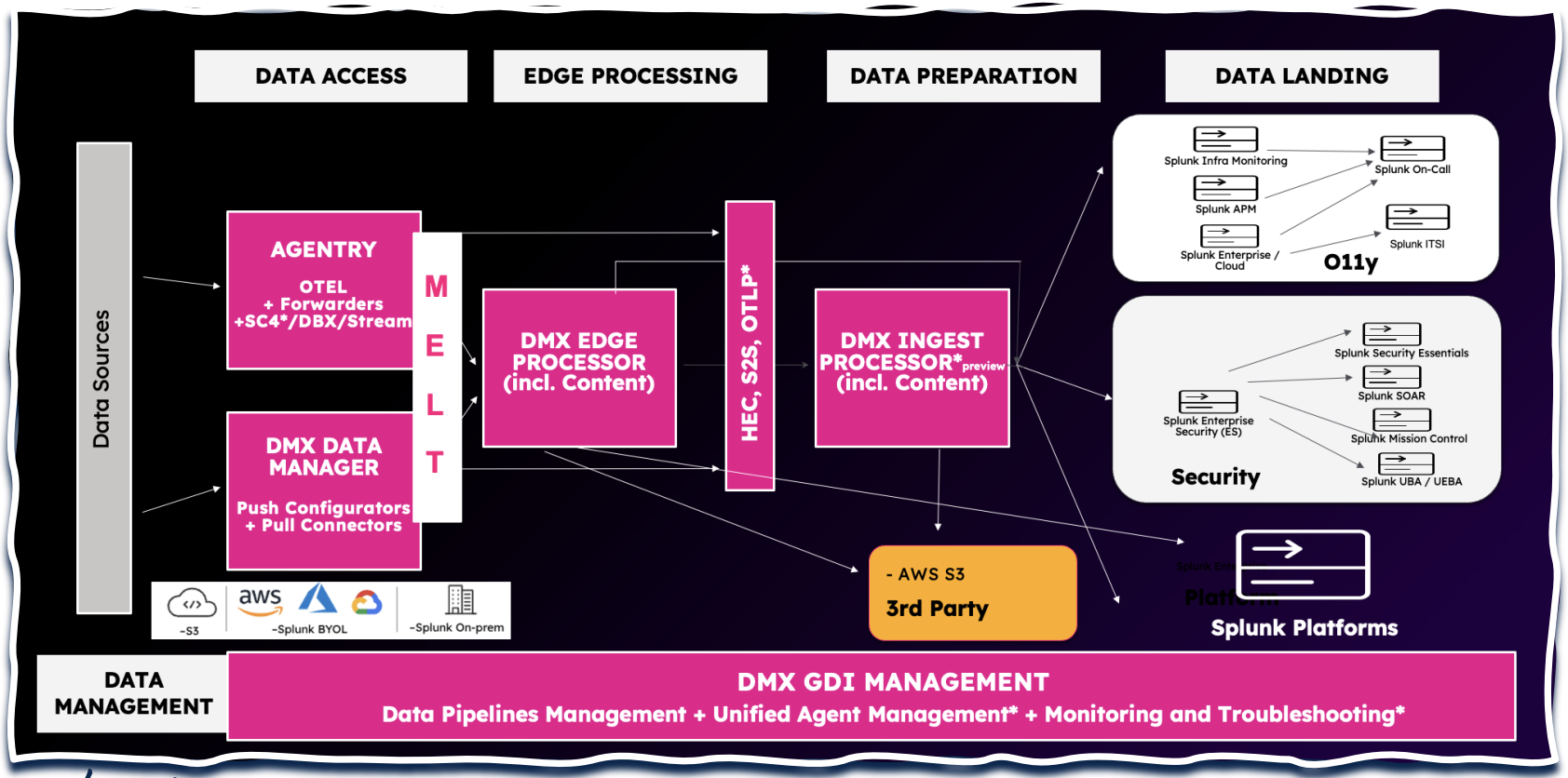


Wired Sensors

2 External Sensors

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

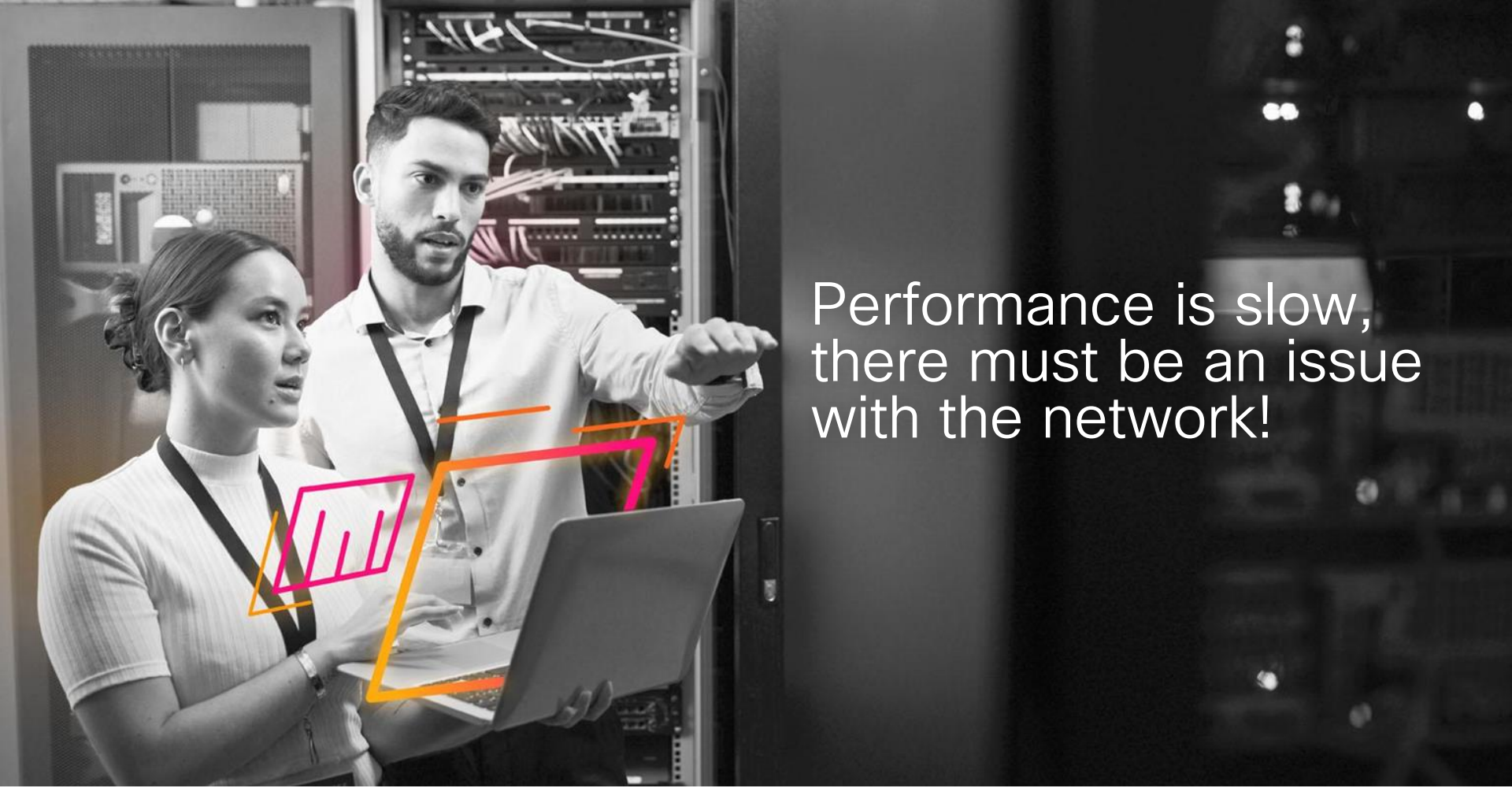
Splunk Data Management Experience



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolution of Network Monitoring

cisco Live!



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Lack of Visibility in the Networking Stack

38%* Inability to Identify Network Performance Issues

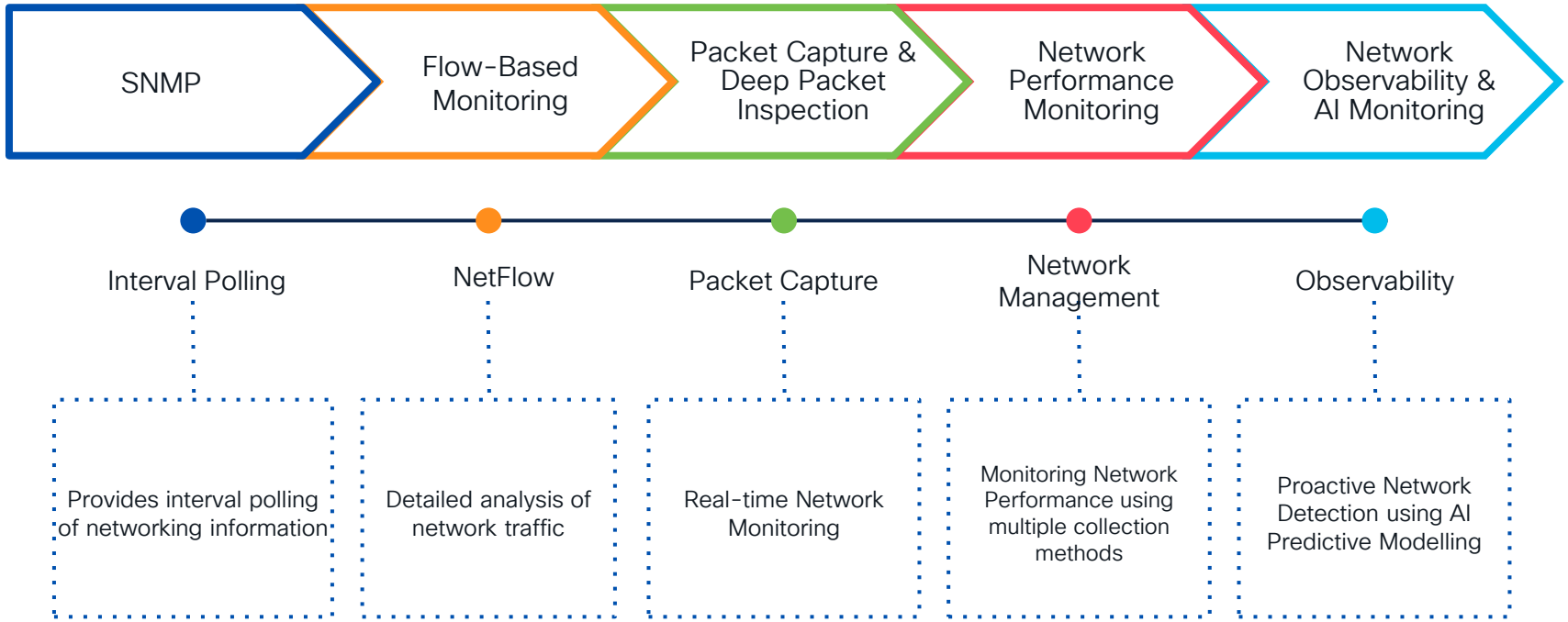
64% Administrators lack confidence in visibility of their security posture

6:10 Organisations lack confidence in the state of their security posture due to their visibility

Source: https://www.liveaction.com/resources/blog-post/2019-top-network-performance-challenges/

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Evolution of Network Monitoring



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

CSP NOC Maturity Model Example

Transforming from NOC to SOC (Service Operation Center)

CAPABILITY MATURITY MODEL

Predictive

Reactive

Unsupervised ML, Automation and Self Healing

Adaptive Thresholding and Advanced Correlation

Service Based Monitoring

Static Monitoring and Alerting

Search and Investigate

Example

AI-driven Adaptive Response

Streaming Telemetry

Closed-Loop Automation

Service Mapping

Service Monitoring w/ Cross-platform and cross-layer correlation

Transactional Records (e.g. xDRs, SIP,RTCP, Diameter, Flow), Registrations, Licensing)

Active Monitoring Service SLAs (e.g. Video, Voice, Data)

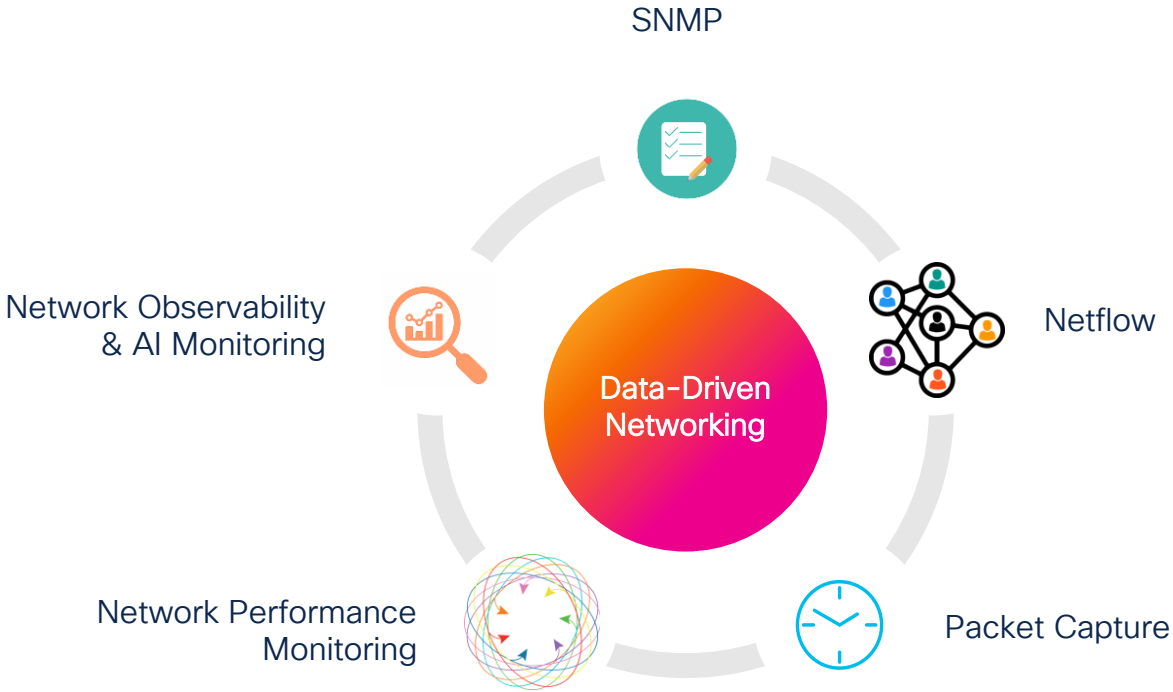
SNMP Traps
SNMP Polling
Syslog
Configs
Perf Counters

Platform Health Monitoring and Alerting

Auto-ticketing

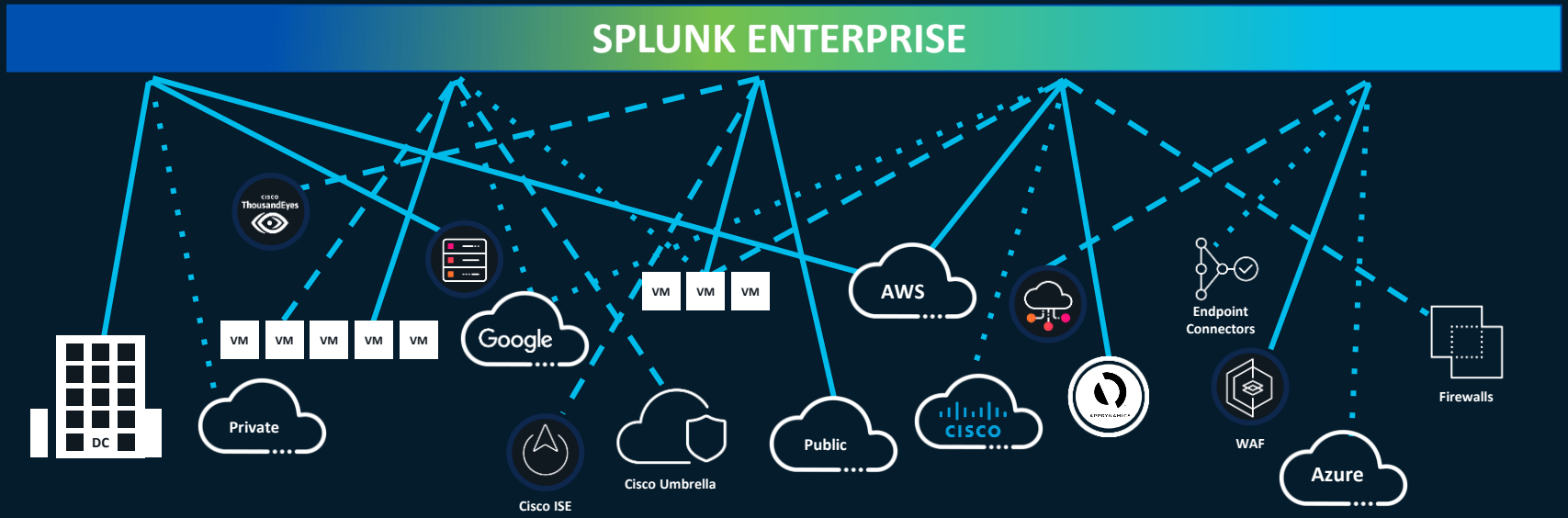
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Driven Network Monitoring



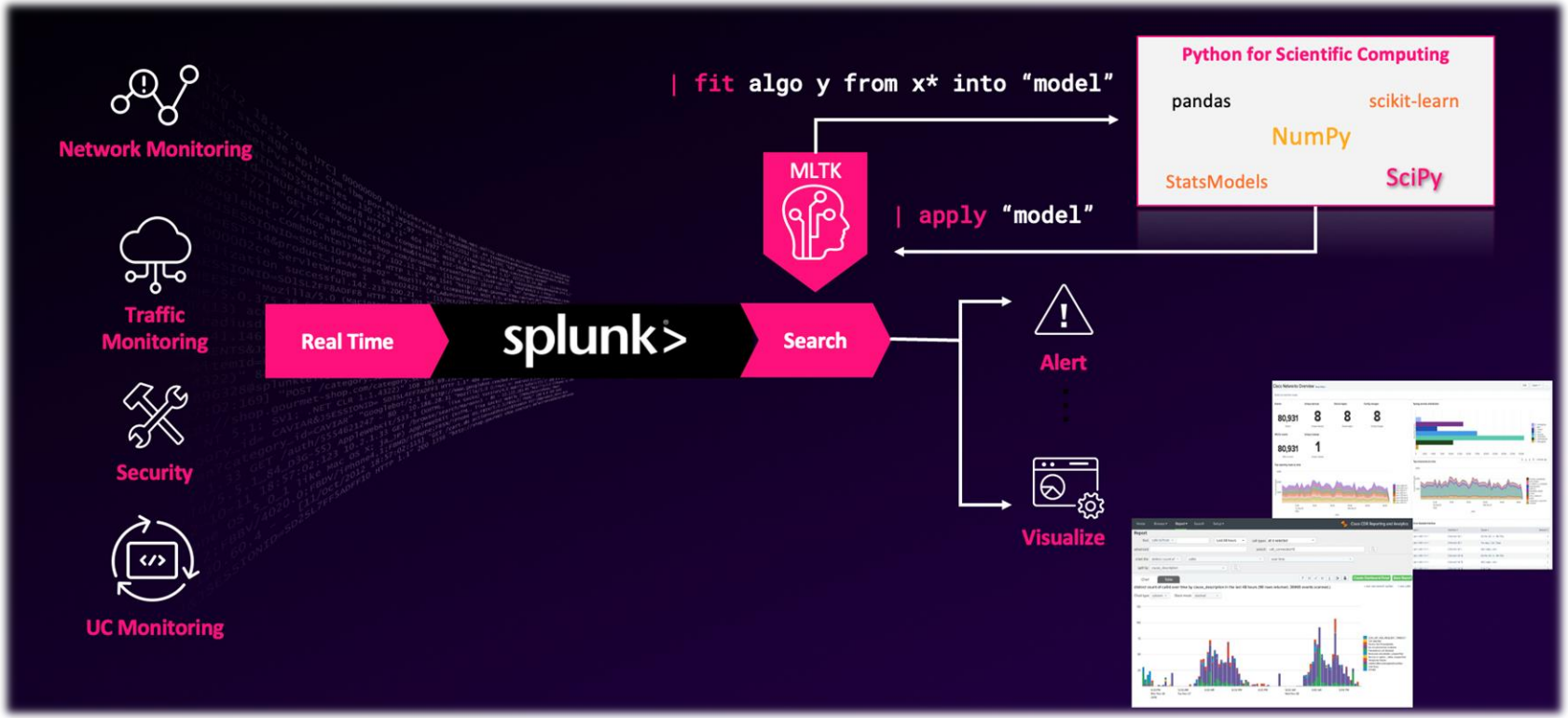
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data-Driven Network Monitoring for Faster Detection, Investigation and Response



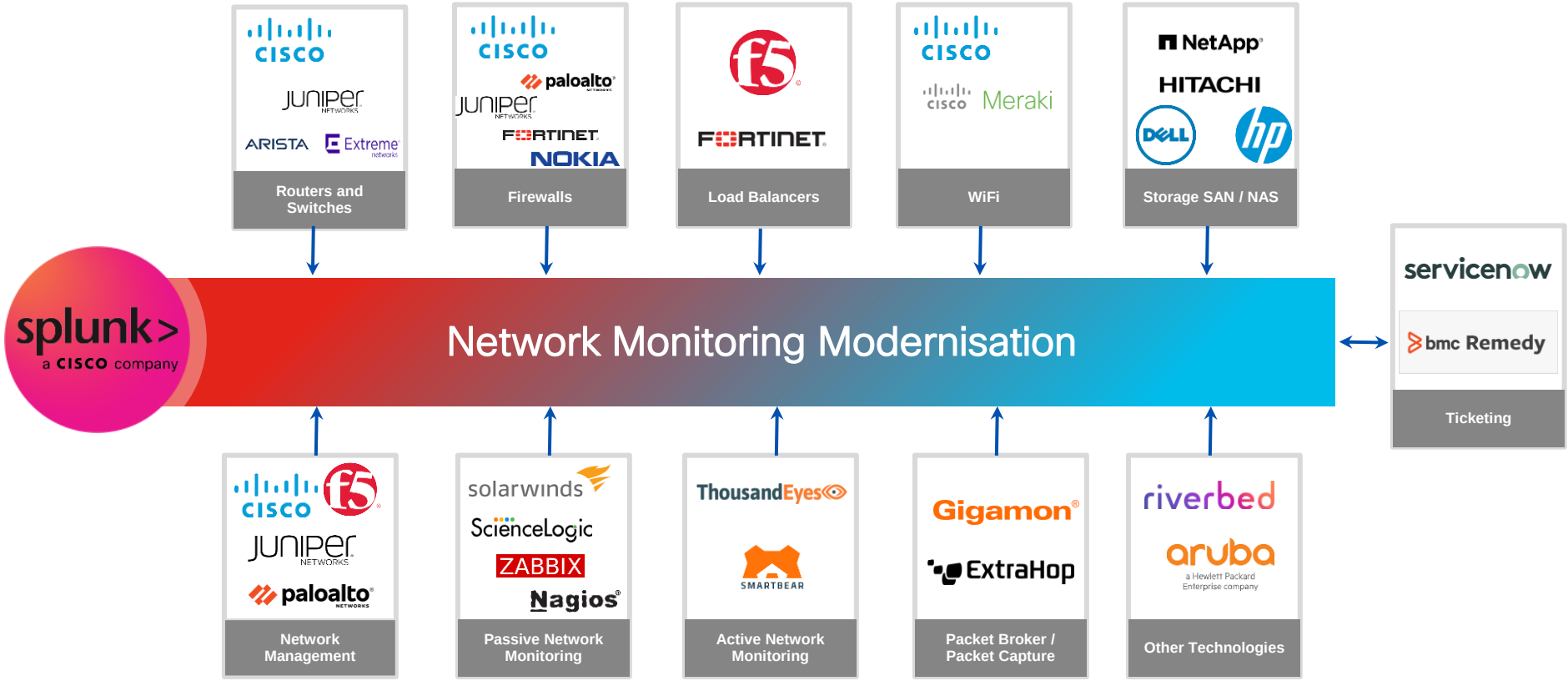
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data-Driven Networking Use Cases



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Monitoring – Data Sources



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

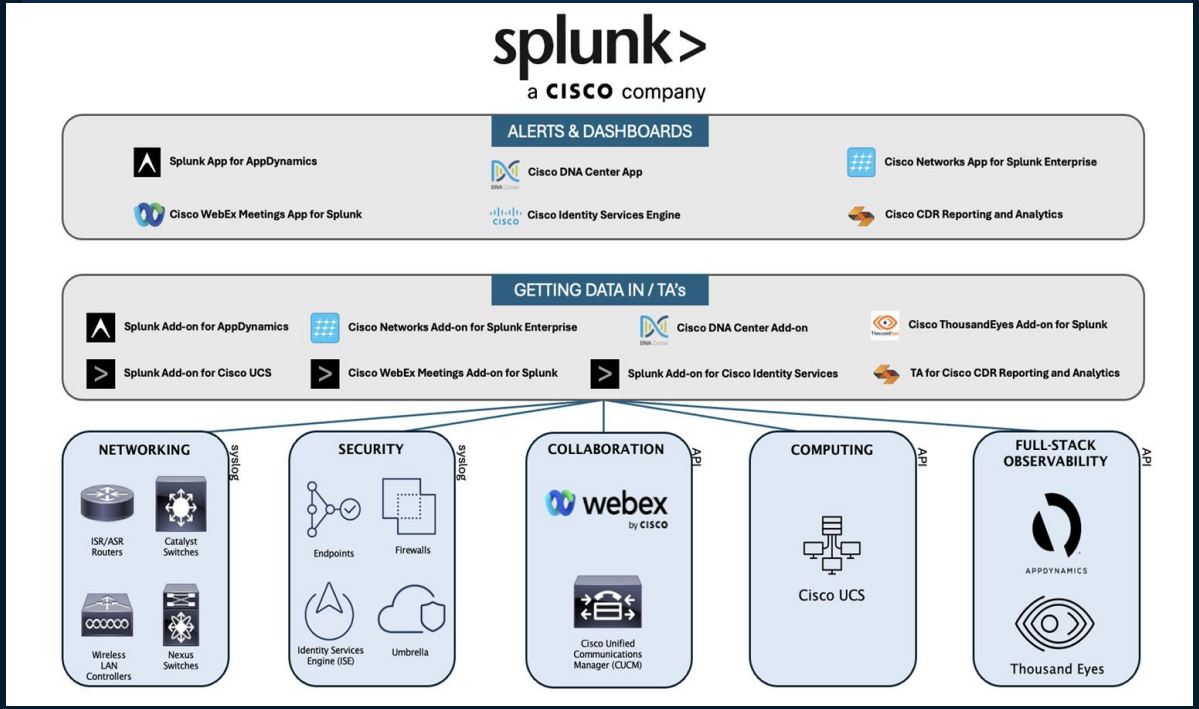
Cisco Network Framework w/Splunk

Method of Transport:

- Syslog (UDP / TCP)
- API (REST / XML)

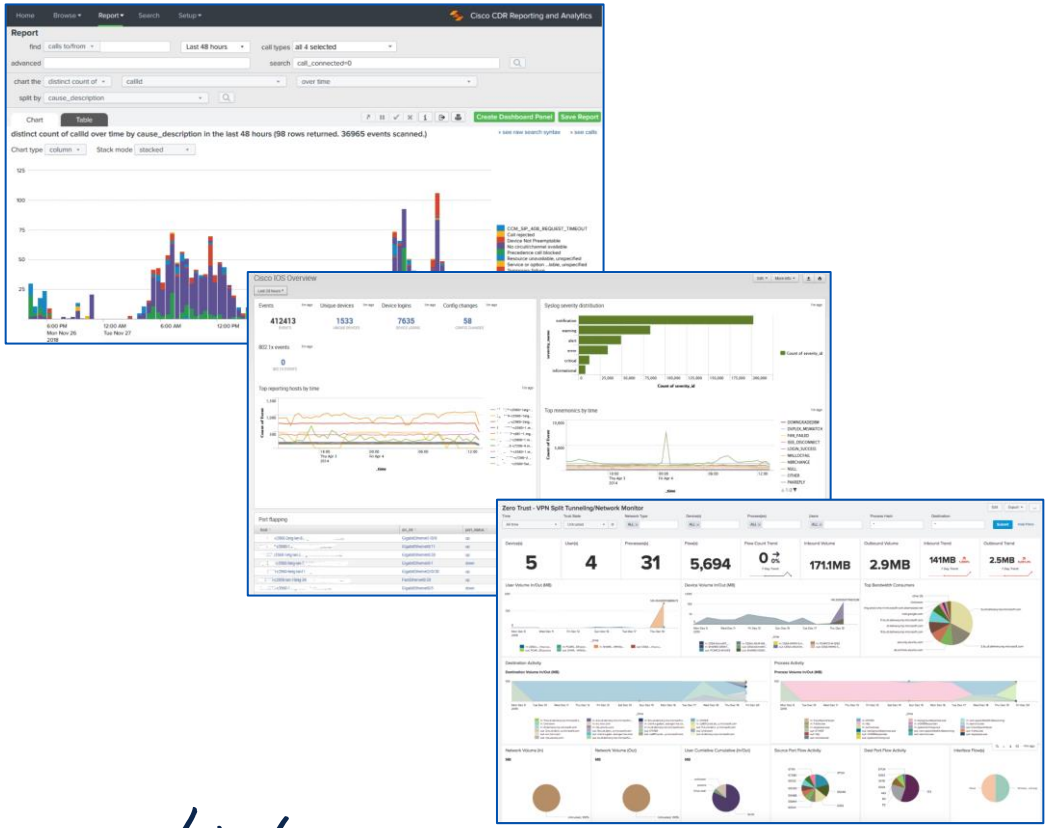
Integration Tools:

- Syslog Connect for Splunk
- Postman API
- NetConf & REST Conf API



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Network Monitoring Apps



Cisco and General Network Apps

- Cisco Networks App
- Cisco ThousandEyes Alerting App
- Cisco ThousandEyes Add-on for Splunk
- Cisco Catalyst SD-WAN App for Splunk
- Cisco Catalyst SD-WAN Add-on for Splunk
- Cisco UCM CDR Reporting & Analytics
- Cisco ACI App
- Cisco Nexus 9K App
- Cisco Identity Services
- Cisco UCS
- Cisco Endpoint Security Analytics (CESA)
- Cisco Network Assurance Engine (NAE)
- Splunk App for Stream
- Splunk Add-on for Infoblox
- Network Diagram Viz
- Splunk Connect for Syslog

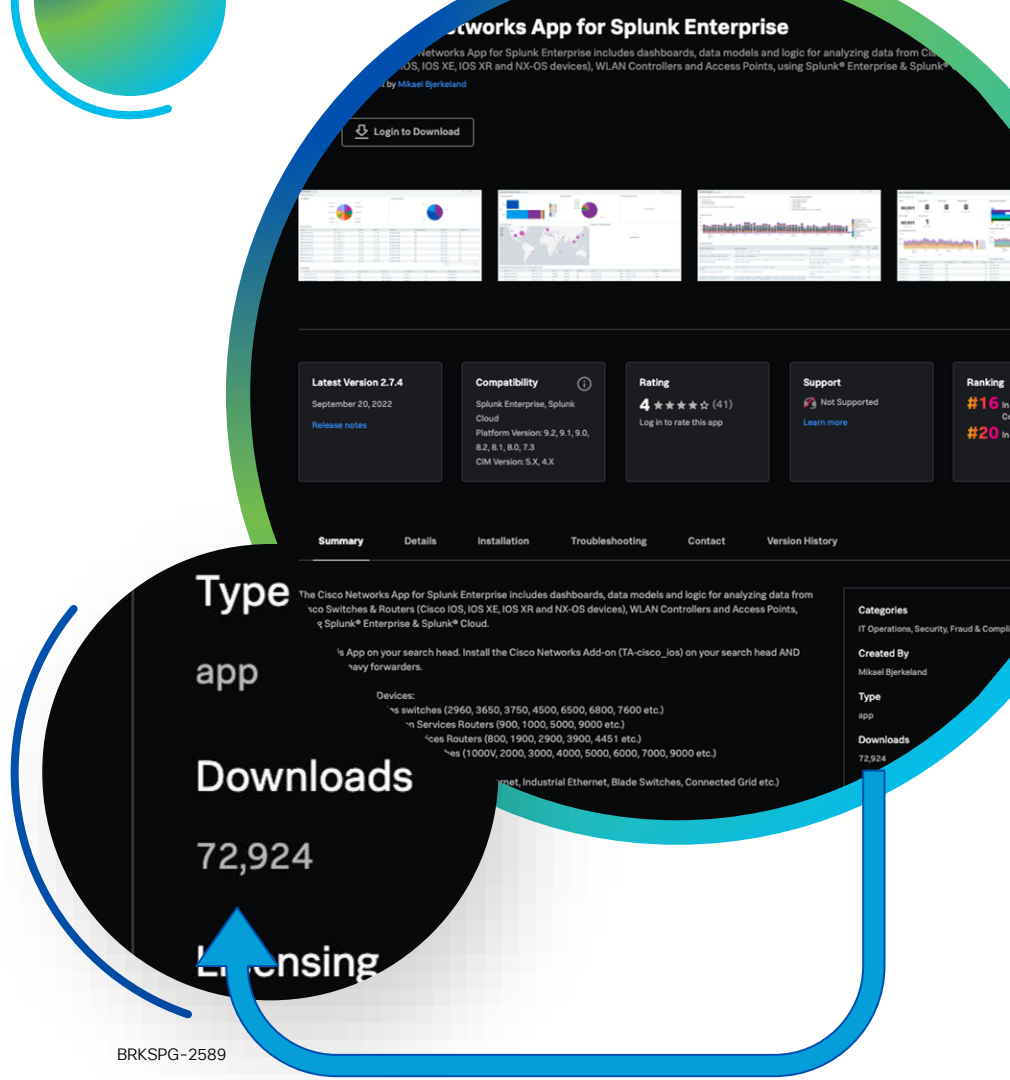
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Networks App for Splunk

[Splunkbase App]

Analyse data from Cisco Switches & Routers (**Cisco IOS, IOS XE, IOS XR and NX-OS devices**), WLAN Controllers and Access Points, using Splunk® Enterprise & Splunk® Cloud.

- Cisco Catalyst series switches (2960, 3650, 3750, 4500, 6500, 6800, 7600 etc.)
- Cisco ASR – Aggregation Services Routers (900, 1000, 5000, 9000 etc.)
- Cisco ISR – Integrated Services Routers (800, 1900, 2900, 3900, 4451 etc.)
- Cisco Nexus Data Center switches (1000V, 2000, 3000, 4000, 5000, 6000, 7000, 9000 etc.)
- Cisco Carrier Routing System
- Other Cisco IOS based devices (Metro Ethernet, Industrial Ethernet, Blade Switches, Connected Grid etc.)
- Cisco Access Points
- Cisco WLC – WLAN Controller

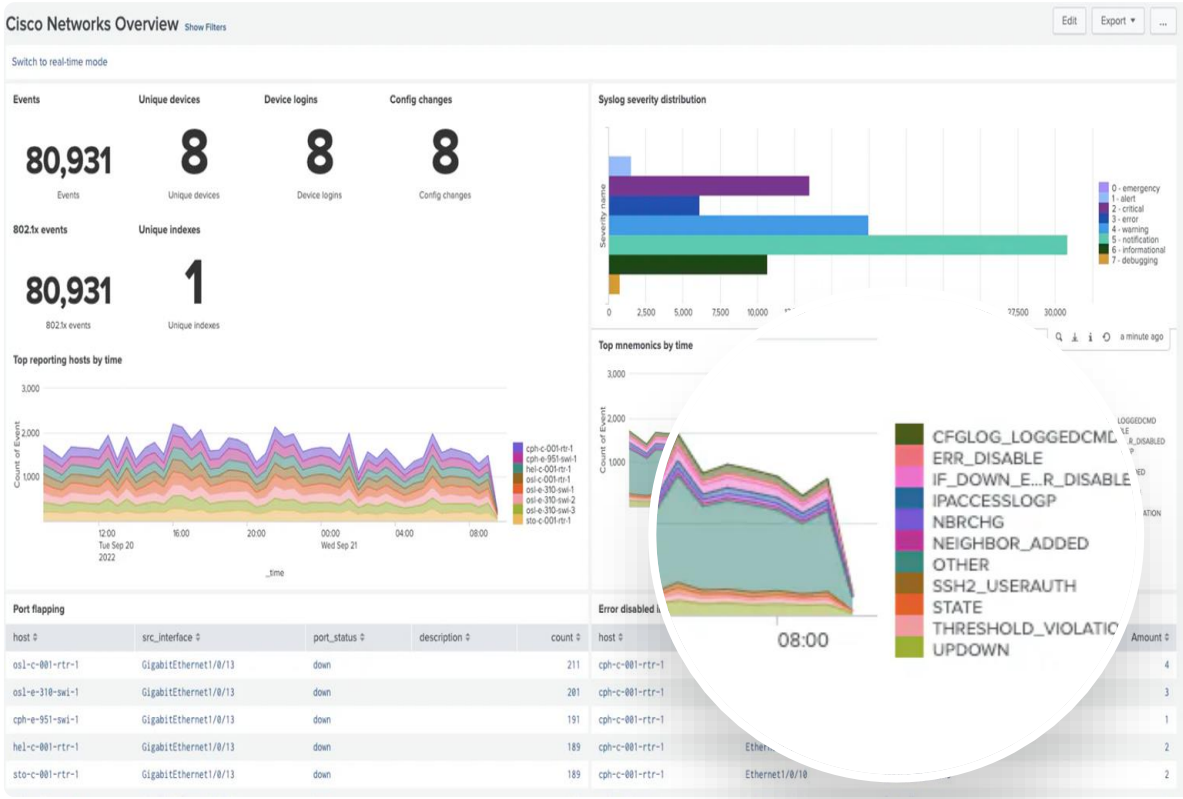


Cisco Networks Overview Application

Investigate faster

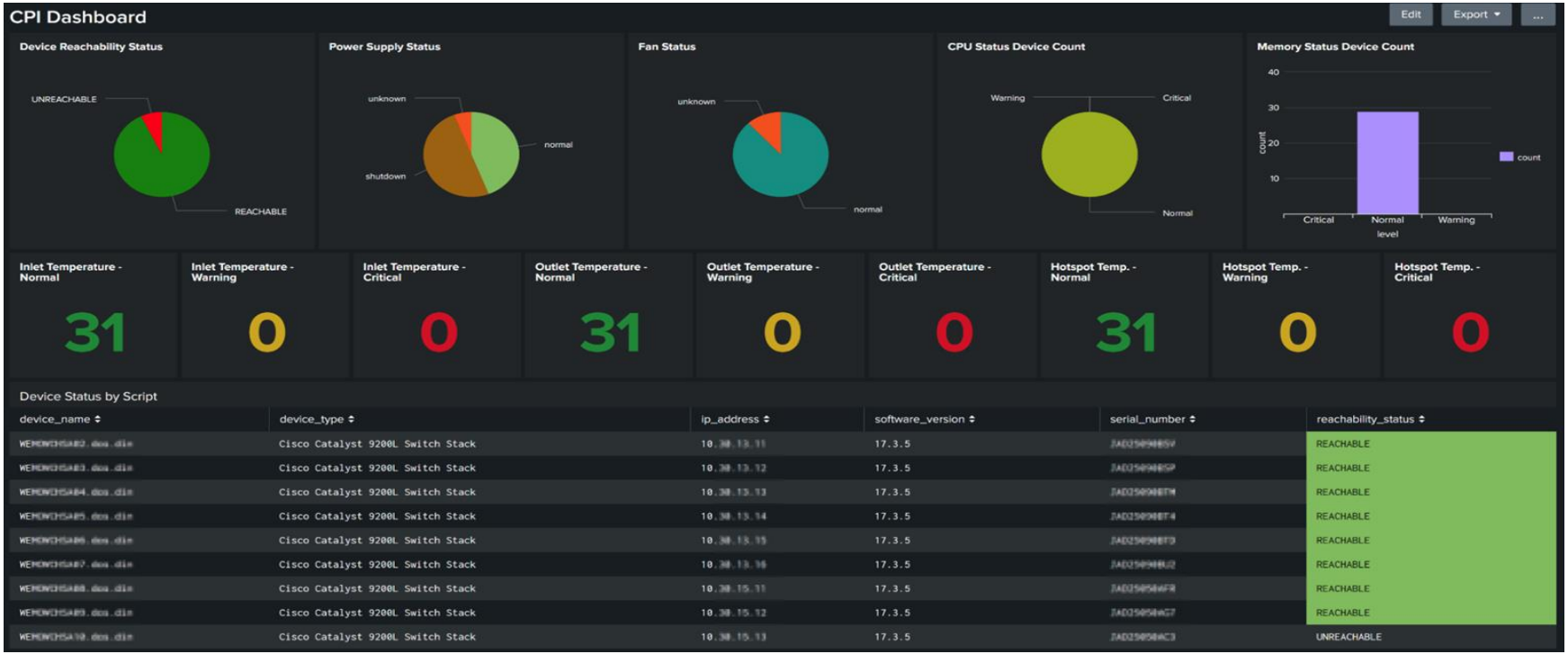
Save time while addressing threats more rapidly

Supported Technologies: Cisco IOS, IOS-XE, NX-OS, IOS XR devices, WLC



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

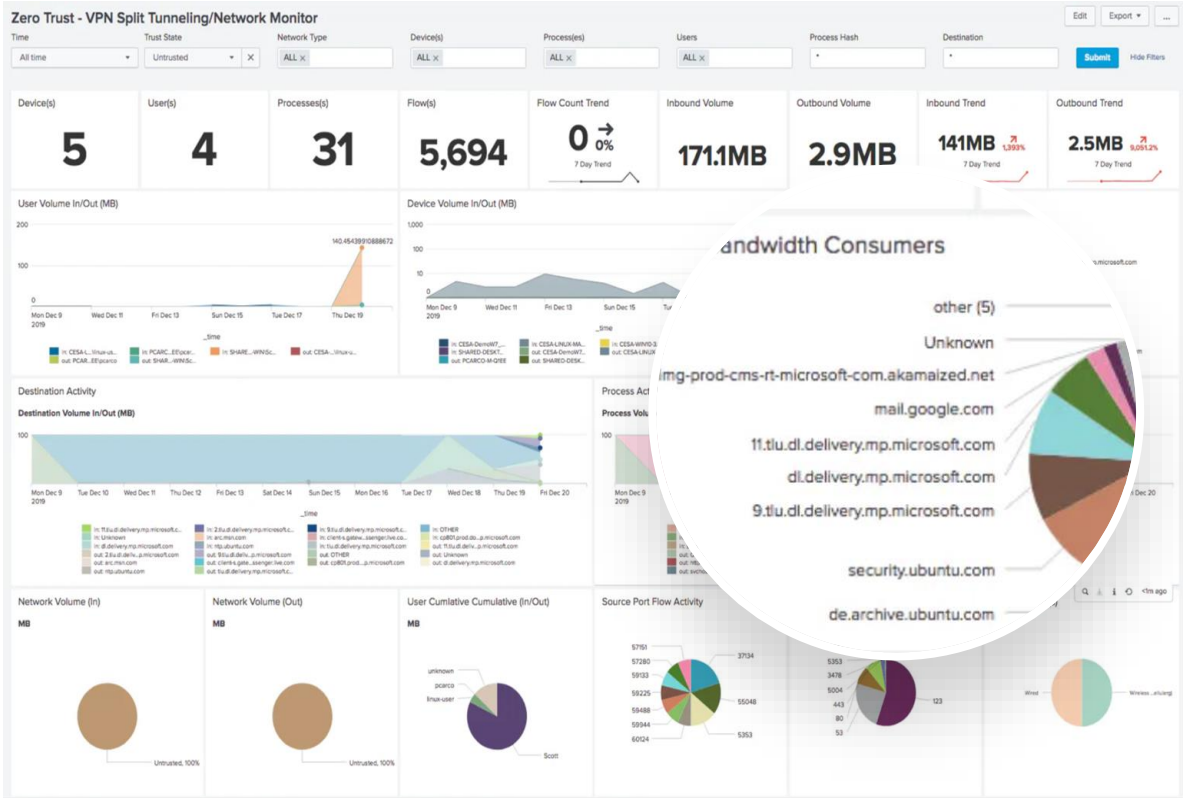
Cisco Prime Infrastructure Dashboard



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Endpoint Security Analytics (CESA)

- Improved visibility
- Correlation of user and endpoint behavior
- Faster detection into behavior on/off the network

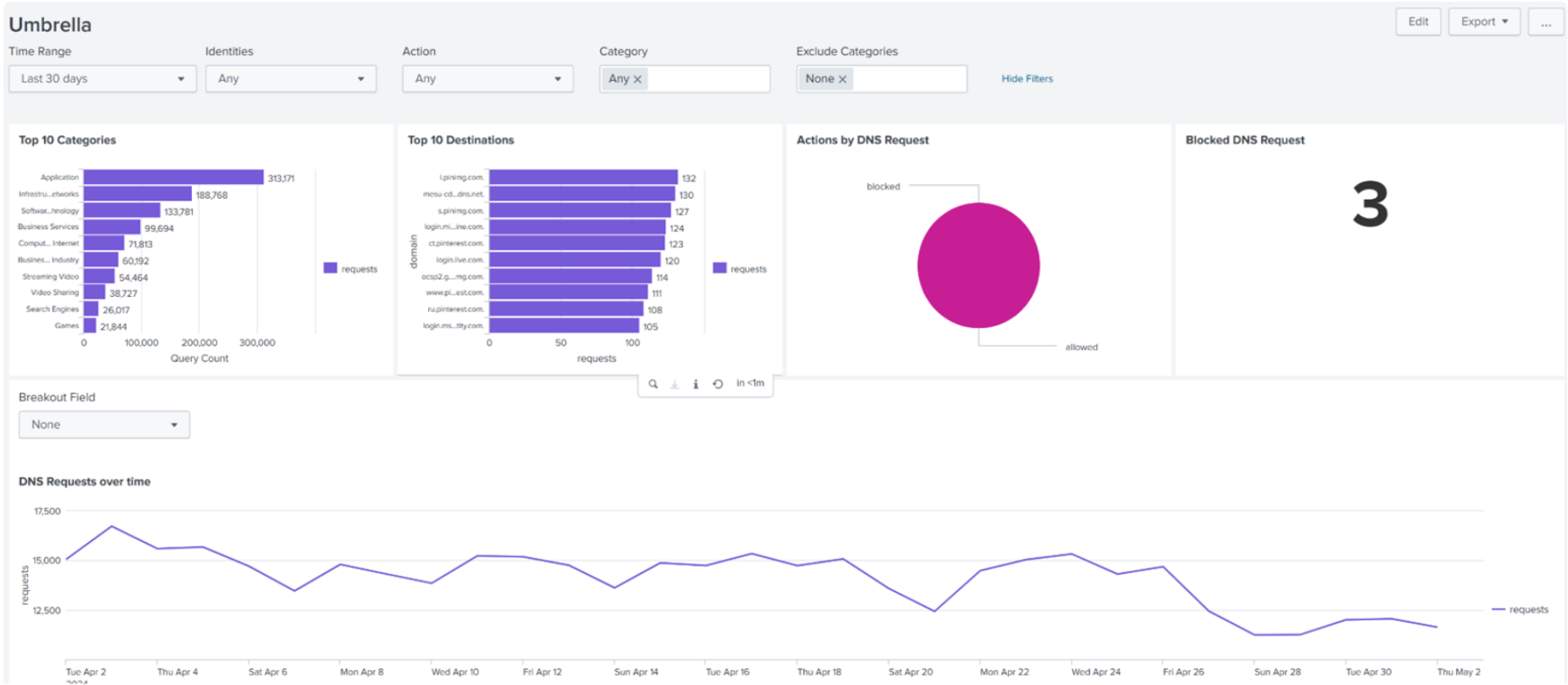


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Secure Networks Analytics Dashboard

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

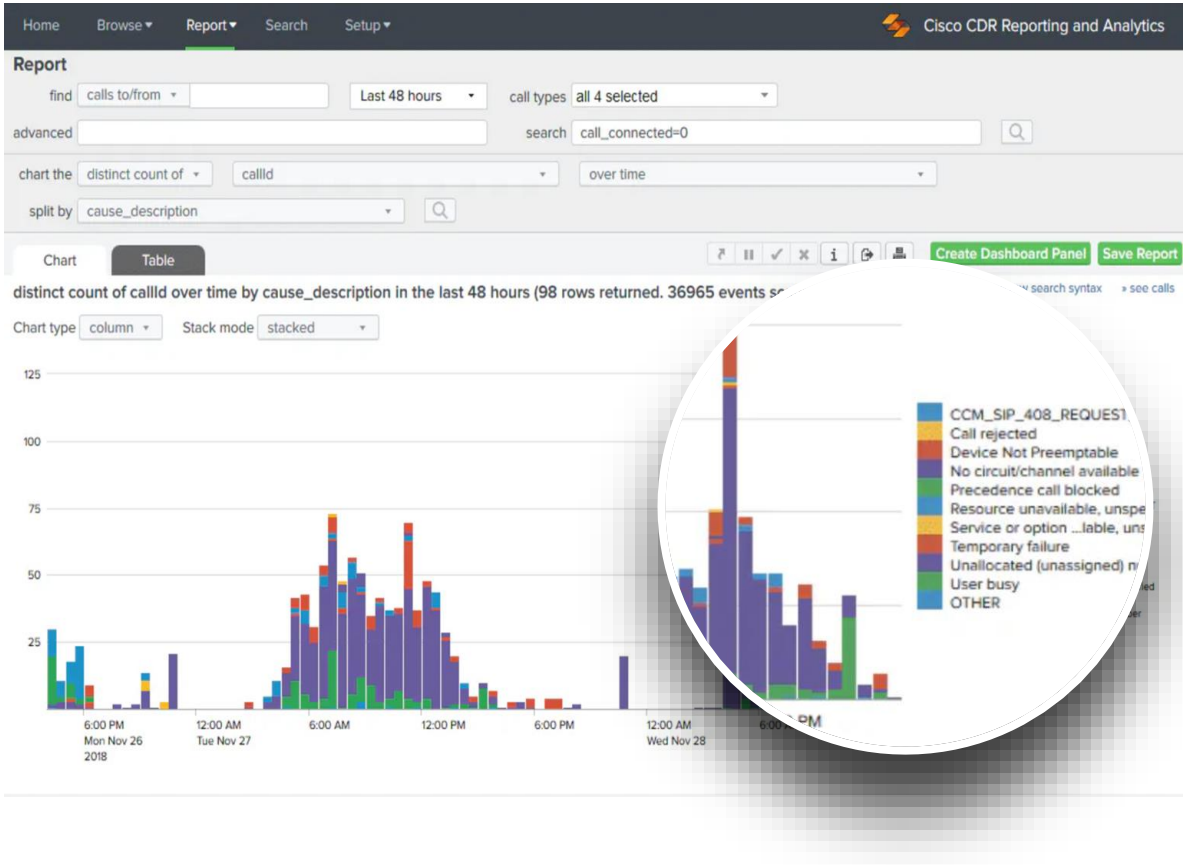
Cisco Umbrella Dashboard



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco UC Monitoring

- Monitor Call Quality
- Diagnose Issues with Call Quality Faster
- Improved Visibility into UC Performance & Potential Impacts



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Data Collection Examples

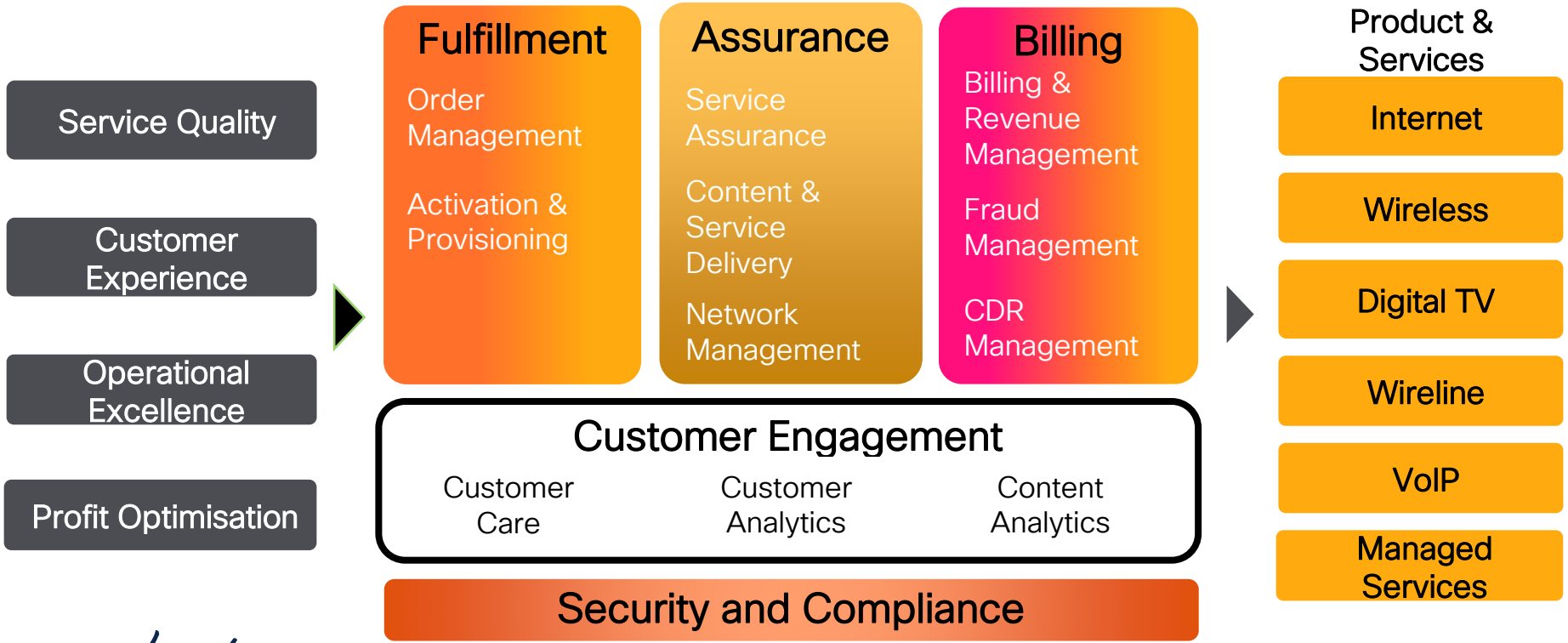
- Dedicated Syslog Server
  - Data Collection Guide
- Syslog Collection Application
  - Splunk Connect for Syslog
- Define Port Collections based on the Data Source

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

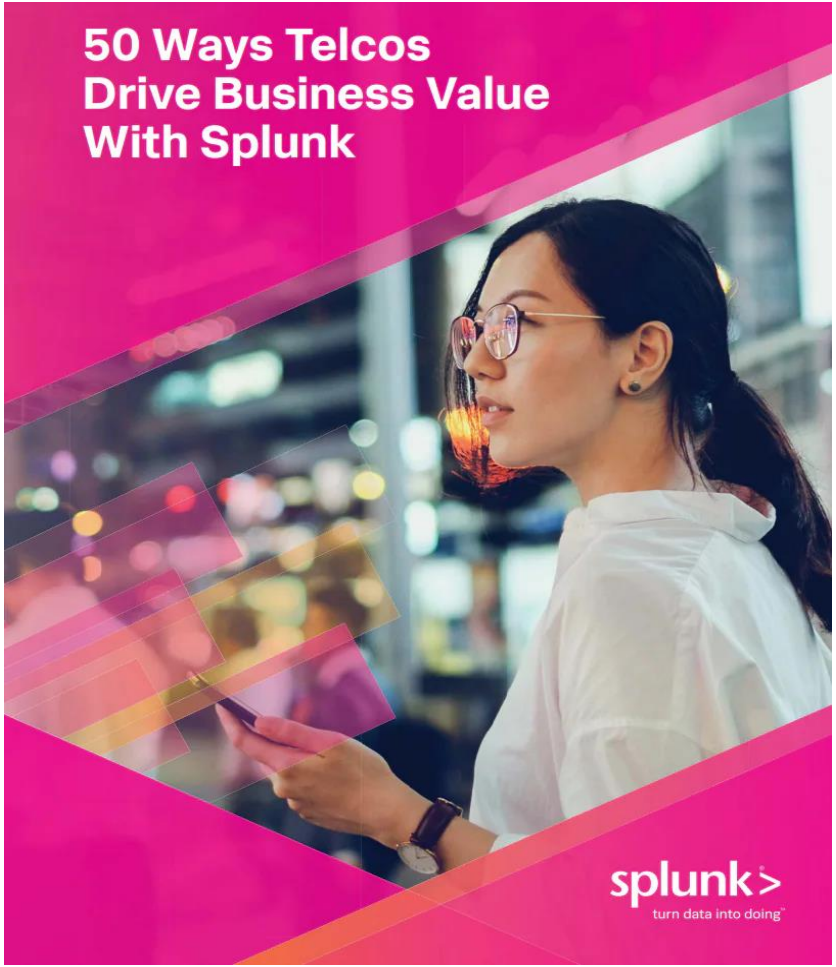
Additional Communication Service Providers Use Cases

Splunk Use Cases

Serving use cases in the following areas



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public



SERVICE ASSURANCE

- Order to Activation
- Contact Center Analytics
- CPE Monitoring
- Mobile Application Health
- Field Services Performance Optimization
- Emergency Services Monitoring
- Video Performance Monitoring
- Content Delivery Network Performance
- Enterprise Service Assurance
- Radio Access Network Monitoring
- IMS Core and VoLTE Monitoring
- Broadband Service Optimization

OPERATIONAL EXCELLENCE

- Enterprise Data Platform
- Enterprise Network Nerve Center
- Enterprise Security Nerve Center
- Managed Security Services
- Hybrid Cloud Monitoring
- Network Function Virtualization
- SDN and SD-WAN
- Core Network Monitoring
- Carrier Media Gateway Performance Monitoring
- DevOps Monitoring and Capacity Management
- Wireline Data Capture
- Network Access Monitoring
- Government Hosted Solutions

REVENUE ASSURANCE

- Churn Prediction
- Truck Dispatch Analytics
- Video Subscriber Analytics
- Reducing SLA Violations
- Real-Time Vulnerability Management
- Roaming Fraud Detection
- PBX/IP-PBX Fraud Mitigation
- Subscriber Fraud Protection
- Subscriber Endpoint Security
- Automated Compliance Reporting
- Data Center ICS Monitoring
- Outage Impact
- Voice/VoIP Revenue Assurance
- Prepaid Billing Account Analysis
- License Exhaustion Prediction
- Real-Time Service Reporting
- Least Cost Routing Optimization

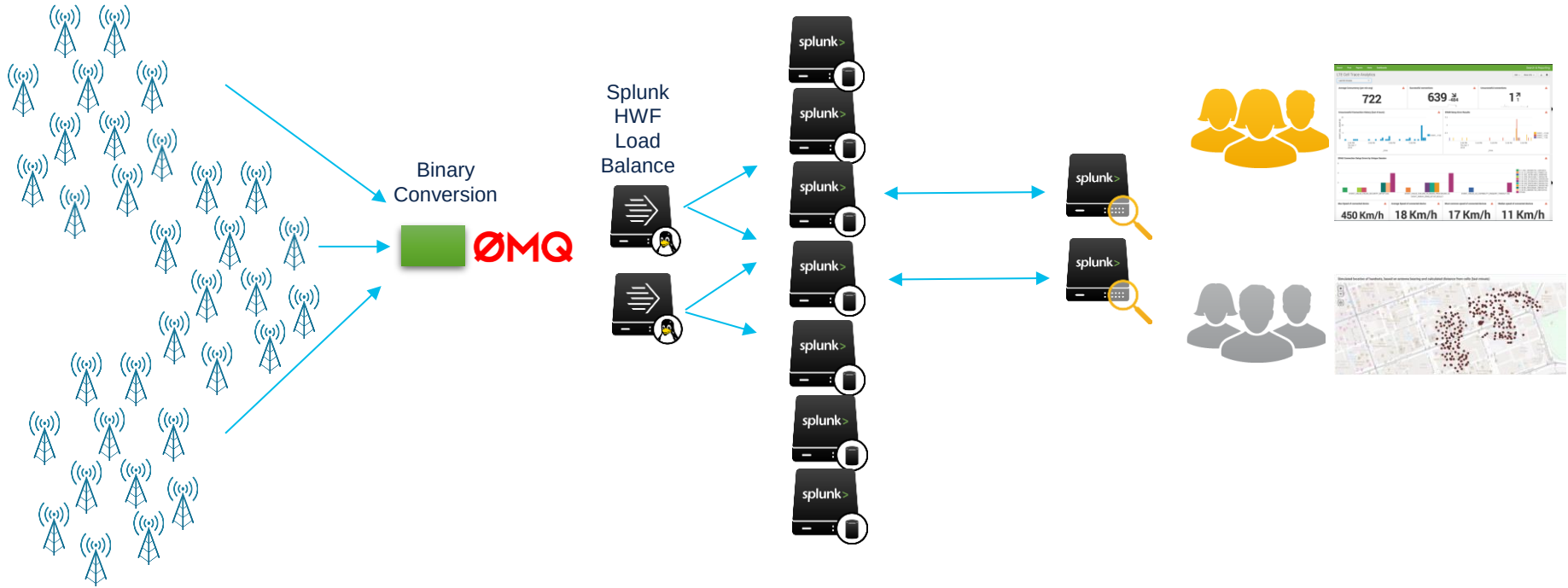
IMAGINE THE POSSIBILITIES

- Data Integrity with Blockchain
- Mobile Banking/Mobile Payments
- 5G Service Excellence
- Targeted Advertising with Small Cell
- Closed Loop Service Remediation
- Connected Experiences
- Customer 360
- Micro Weather Forecasting

Download eBook

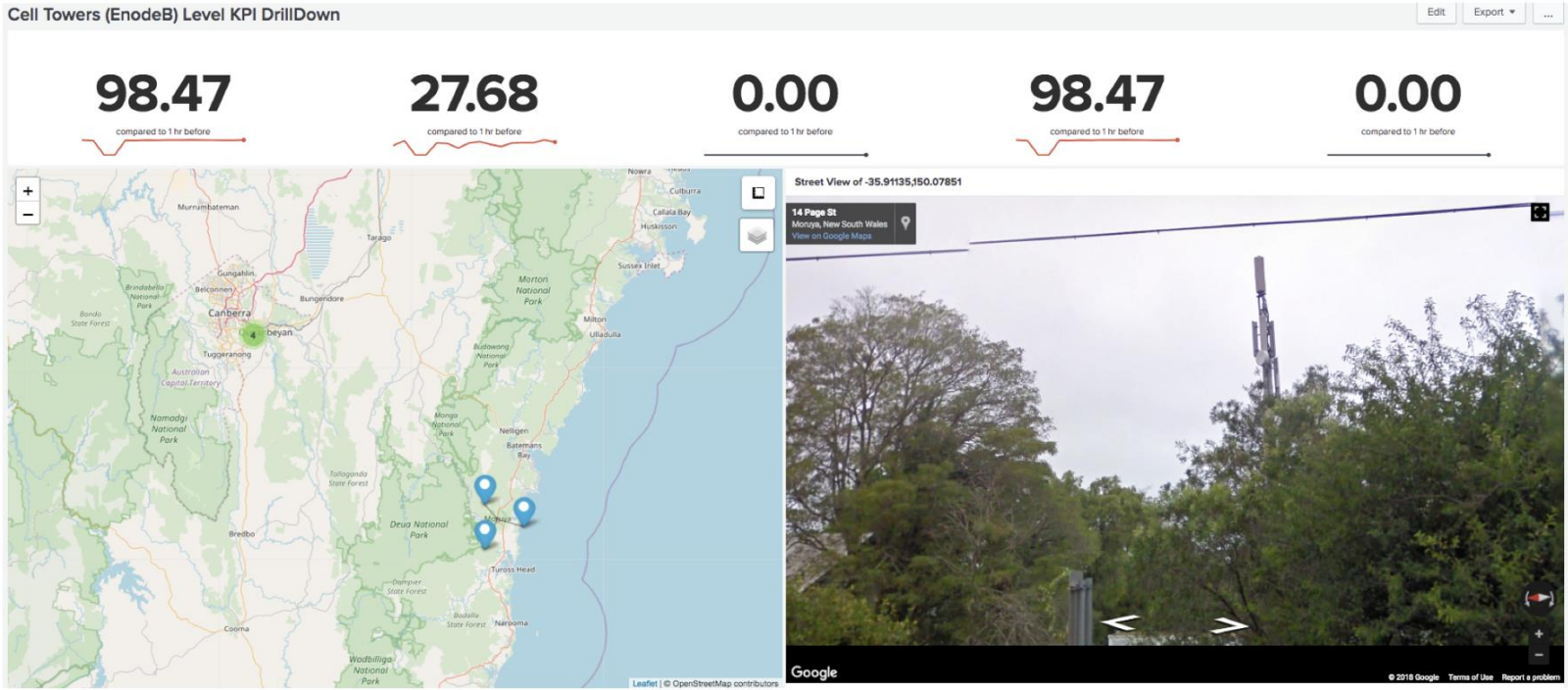
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

RAN Data Monitoring



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

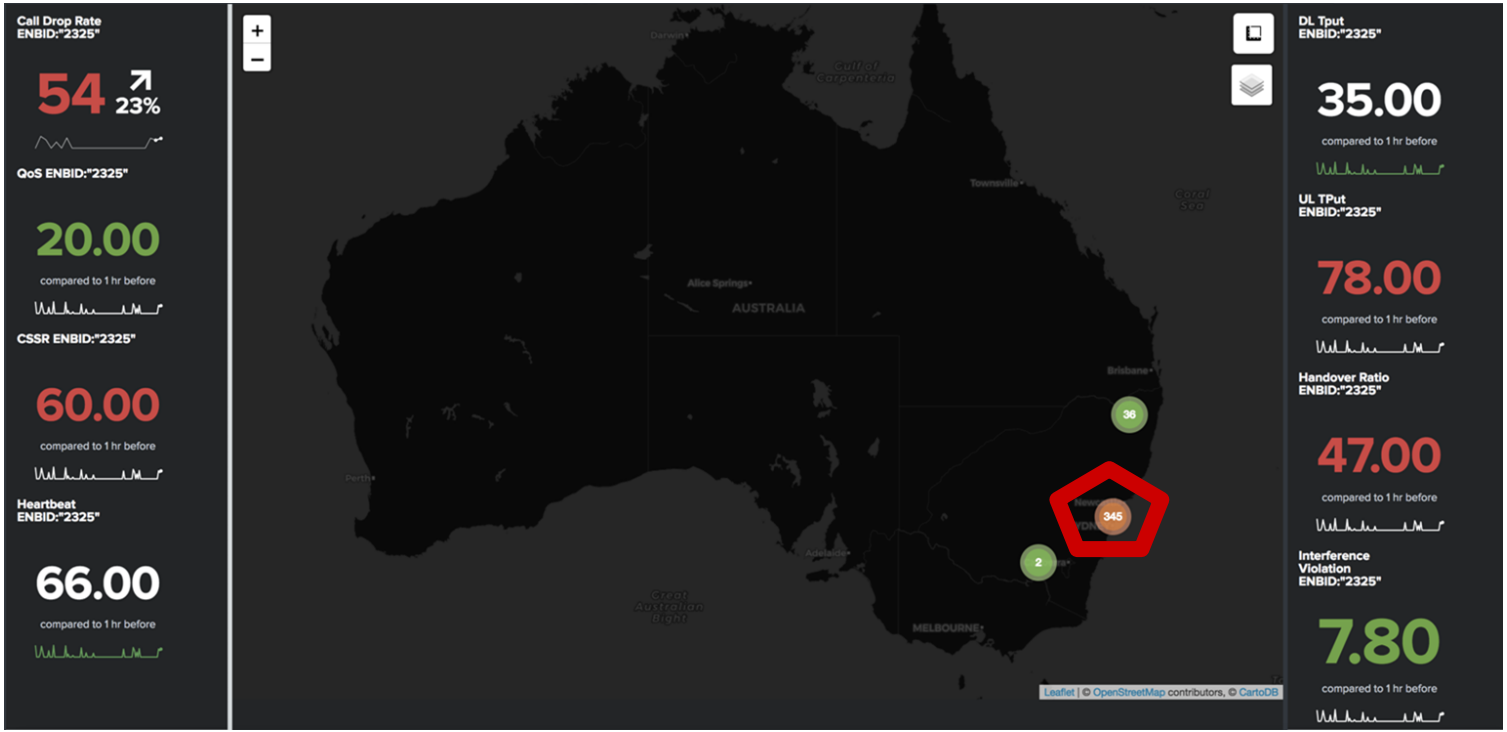
4G/5G KPIs Monitoring – Geo Based Visual



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Outage Impact Dashboard

Polygon contained impact consolidation

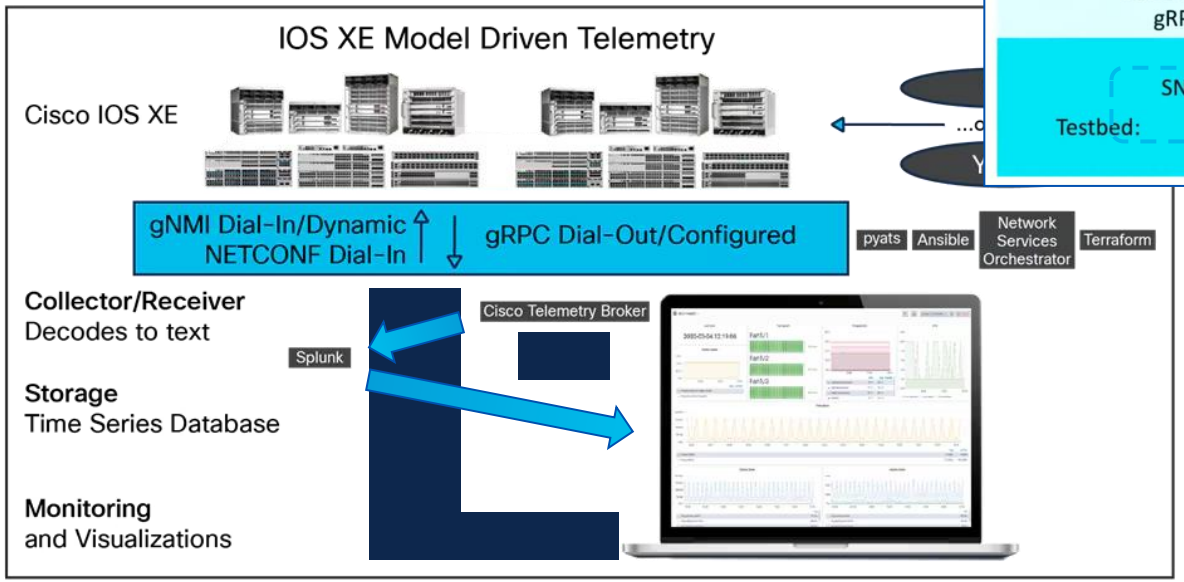


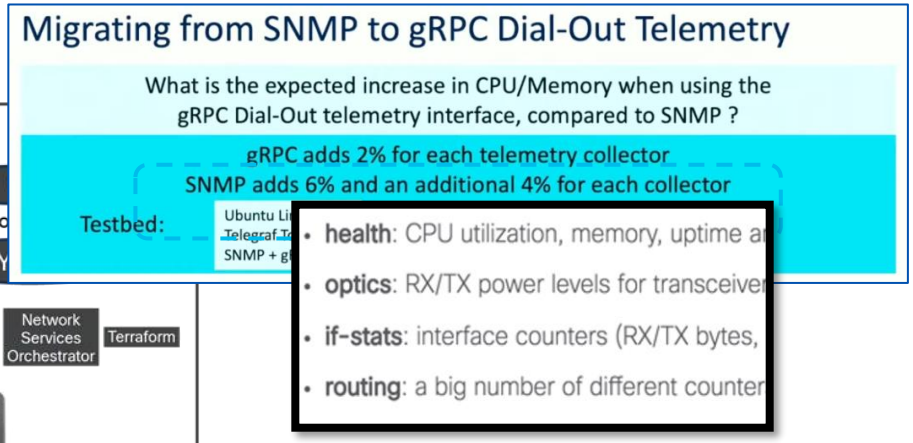
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where are CSPs heading?

“AI Driven Closed Loop Automation”

Model Driven / Streaming Telemetry





Key Points

- Alternative to SNMP
- Different from Open Telemetry
- OpenConfig project
- RFC 9232

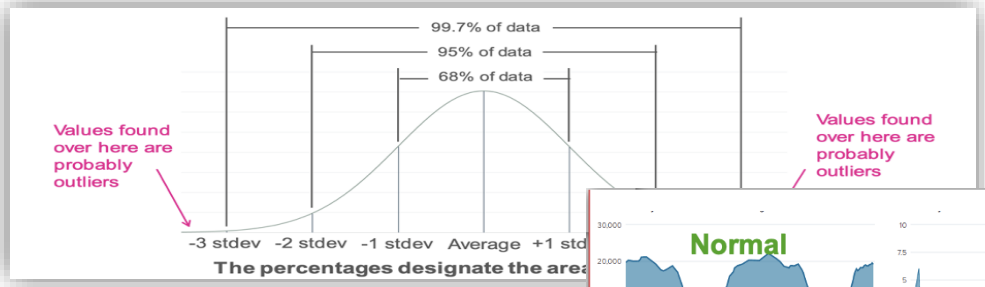
References:

Cisco Presentation on Benefits of Streaming Telemetry - Feb '24

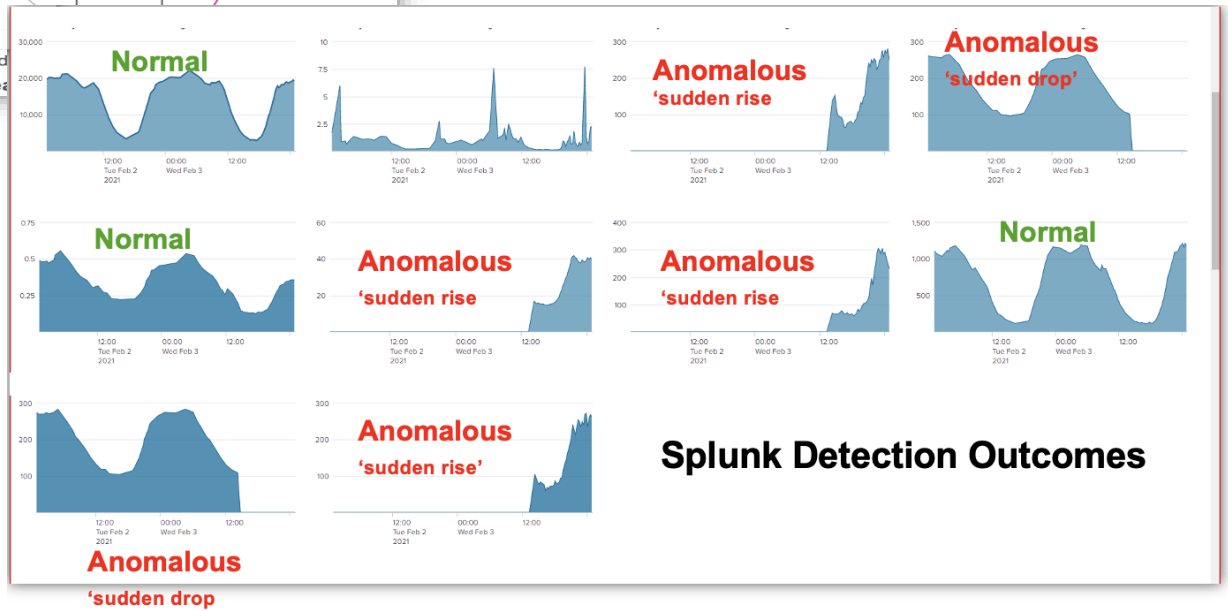
Cisco Catalyst 9300 Doc on sending Model-Driven Telemetry to Splunk and other tools

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Machine Learning – Detect Anomalies



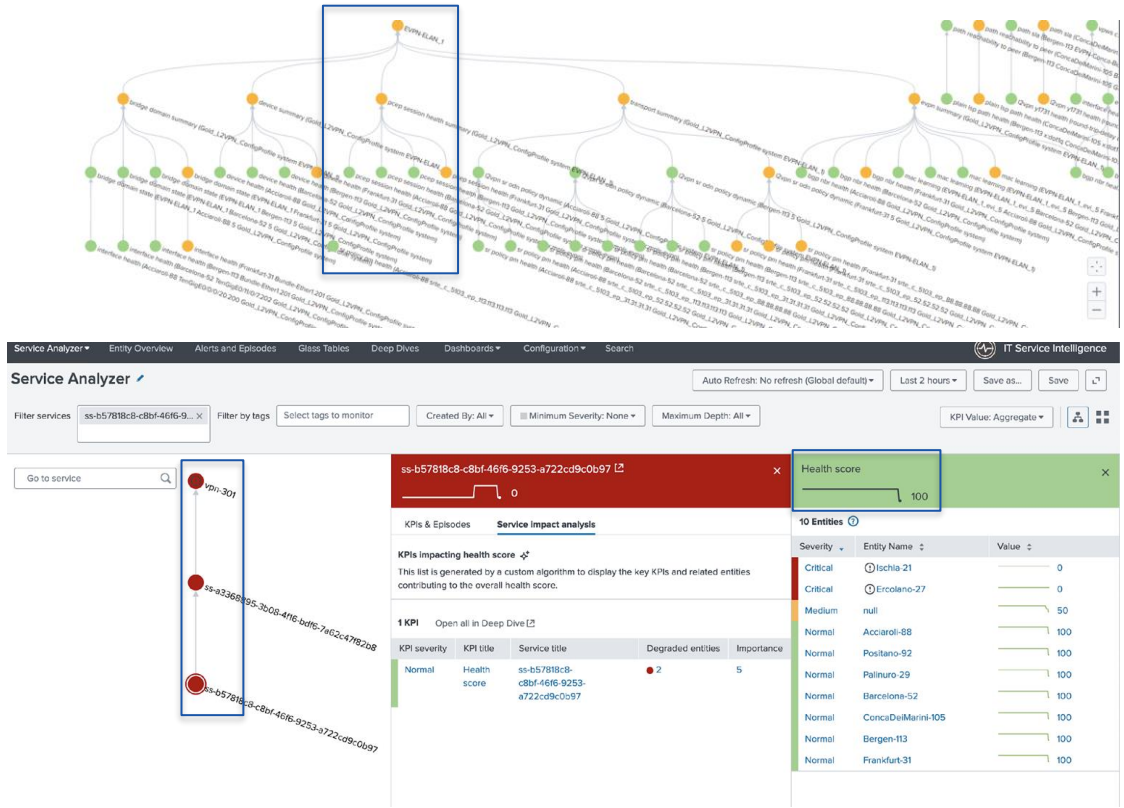
After few iterations, false positives stabilised within a range of 0.5 to 1%, which significantly reduced the number of alarms and improved detection and resolution time.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards AIOps for Autonomous Networks

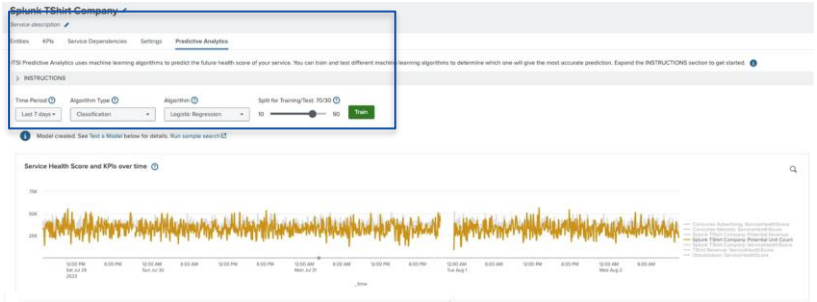
ITSI application → KPIs propagation across (sub)services and entities

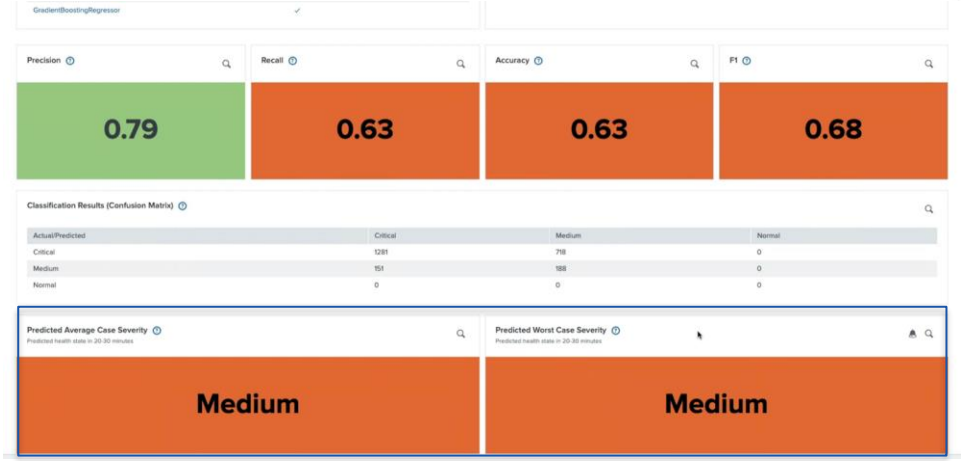


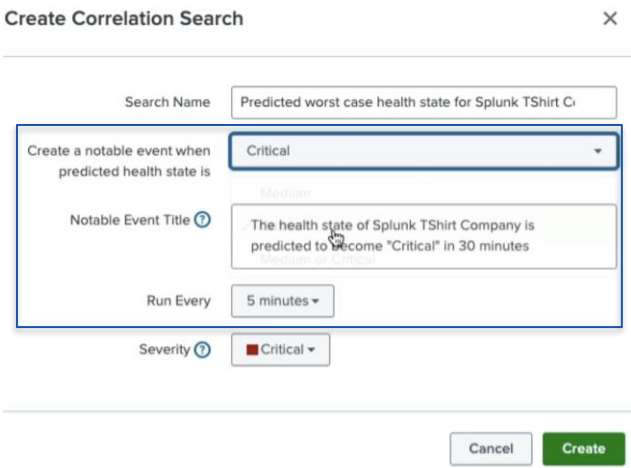
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards AIOps for Autonomous Networks

ITSI application → ***Predictive analytics** for service KPIs







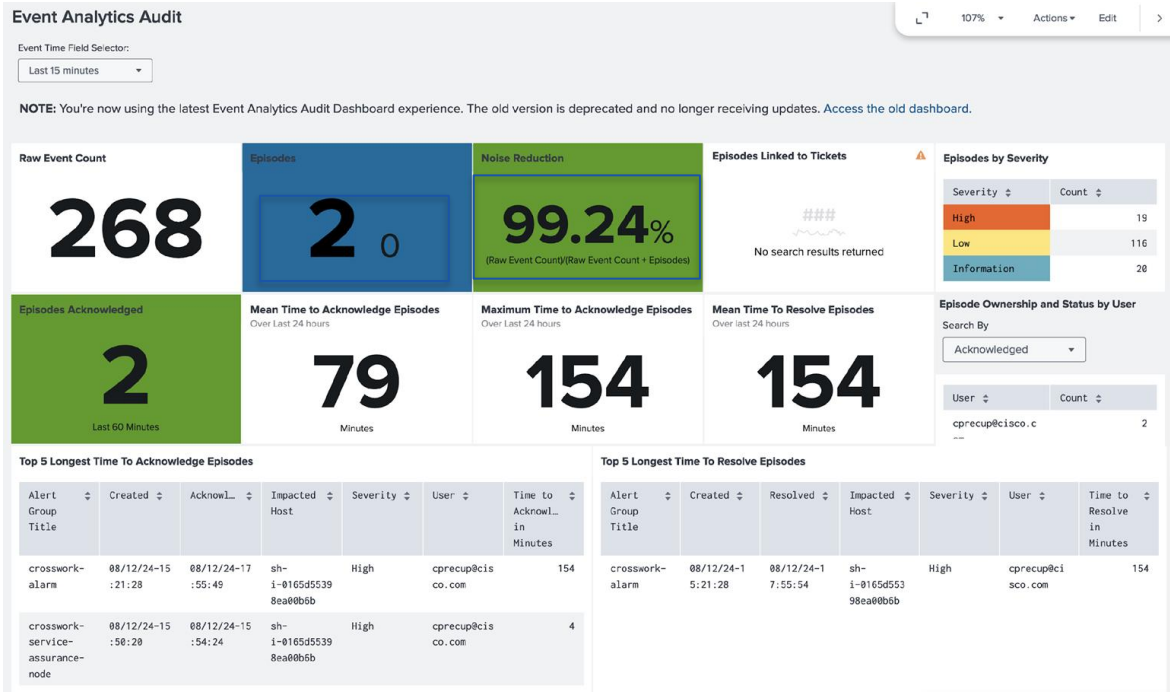
* Teset but not included in demo; suggested for later stage when key KPI is selected
https://lantern.splunk.com/Observability/Getting_Started/Working_with_machine_learning_in_ITSI

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Towards AIOps for Autonomous Networks

ITSI application → Events, Episodes and Correlation: **Smart Mode**

Smart Mode in IT Service Intelligence (ITSI) uses machine learning algorithms to **group notable events into episodes based on their similarities**.
Smart Mode compares event field values and **groups events that are related to each other**. It **reduces noise** and detects patterns in your events.



https://docs.splunk.com/Documentation/ITSI/4.19.0/EA/SmartMode

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Call to action

- Find out how many single-pane of glasses you currently have in your environment and identify how much time you spend reviewing each dashboard?
- Identify who's making decisions on your infrastructure. Do they have all of the information to make an informative decision and are their decisions effective?
- Create an enterprise logging infrastructure (syslog servers / netflow collectors.)
- Review at least 2-3 data sources for collection & identify the metrics you want to monitor.
- Develop alerts & reports to improve visibility & response.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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**.

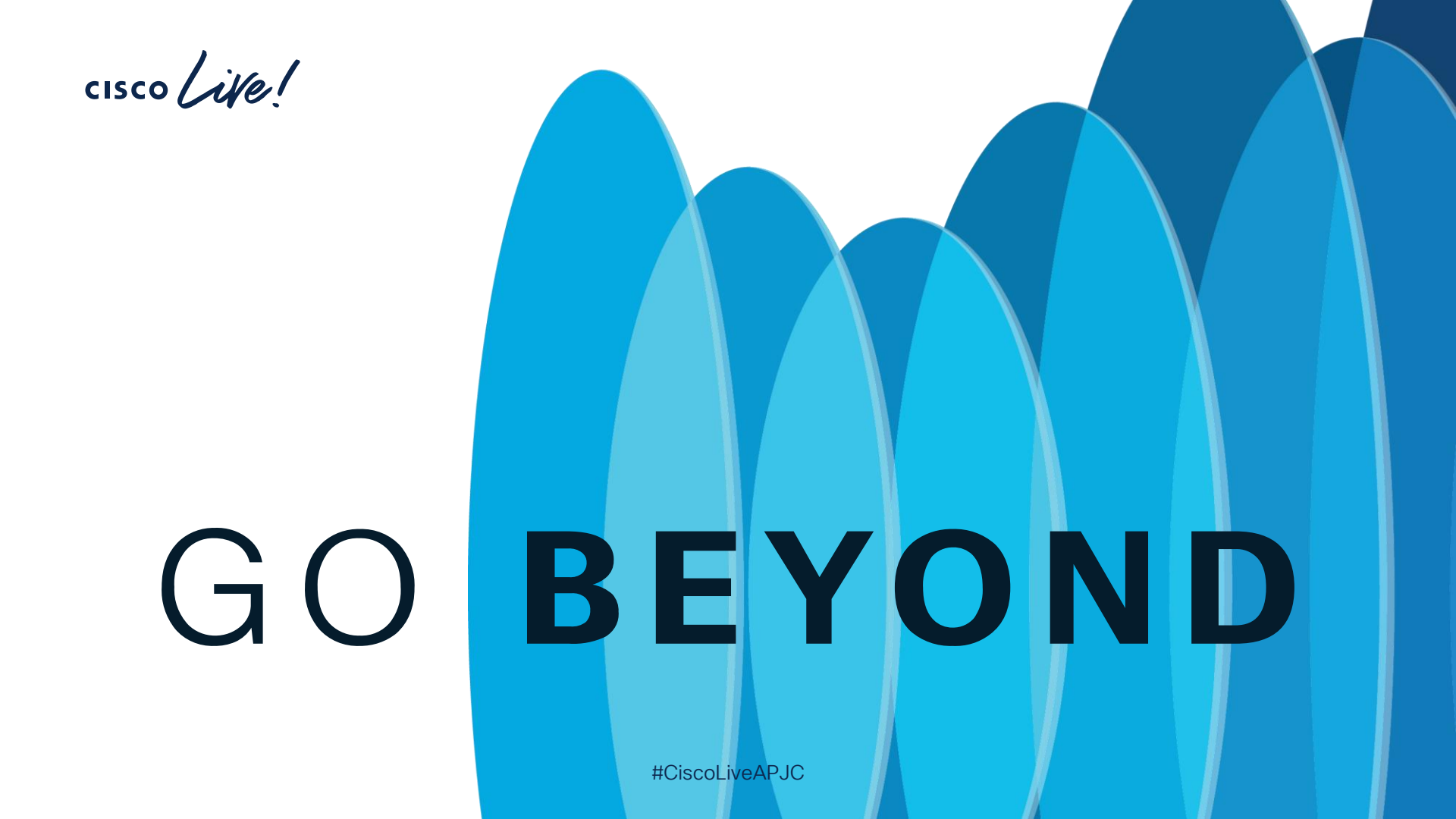
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC