Maximizing AI Potential: Best Practices for Leveraging Cisco and Splunk Data

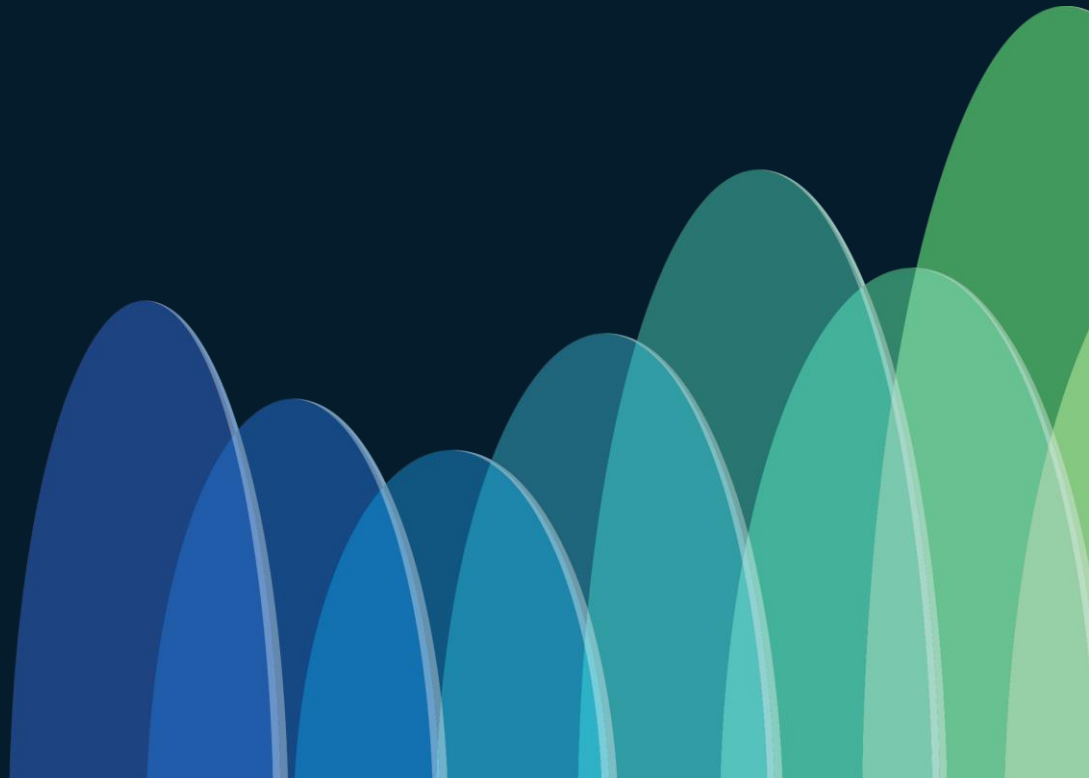
Faisal Azizullah, Principal Architect CX Engineering
@faisalazizulla
David Stanford, Sr. Director CX CTO
@dastanfo

CISCOU-2029

Agenda

- Introduction
- Why AI in Networking?
- The Role of Data
- Use-Cases & Best Practices
- Challenges and Solutions
- Success Story
- Conclusion

Introduction



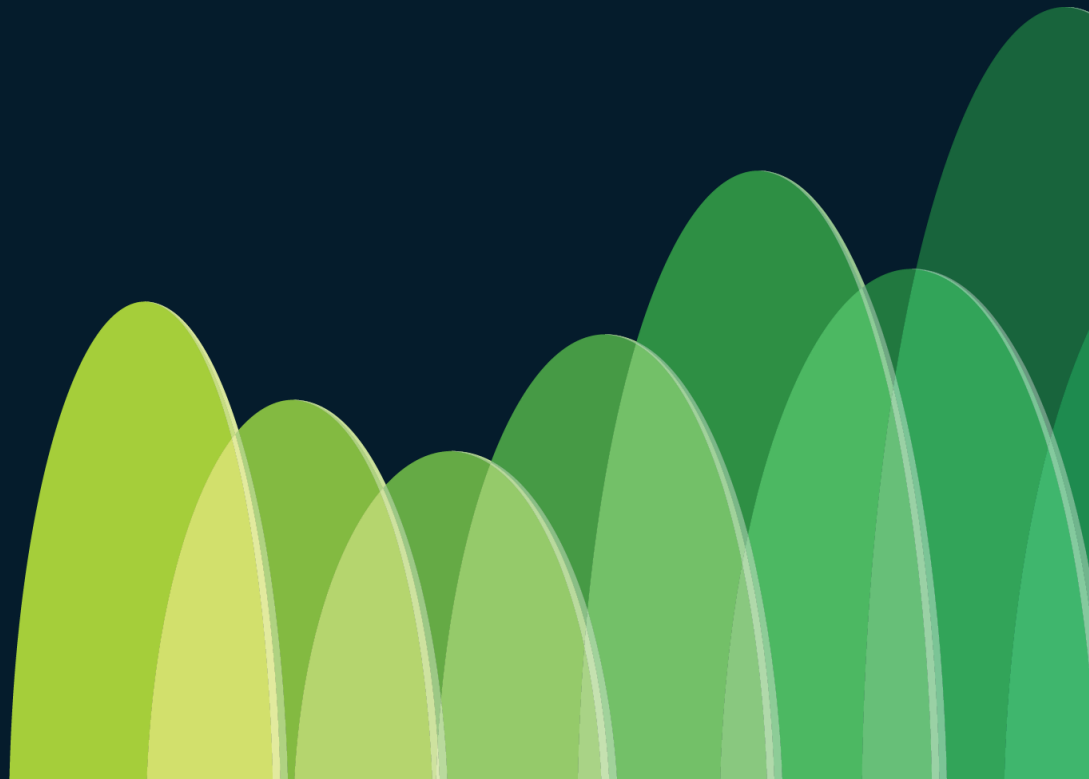
Introduction

- Faisal Azizullah – Principal Architect
- David Stanford – Sr. Director

This session will show you how to maximize AI capabilities by leveraging Cisco telemetry and Splunk's observability data.

Data is key to all use-cases and the focus we have here will be on Networking, how we integrate, and some of the challenges and solutions.

Why AI in Networking?



cisco Live!

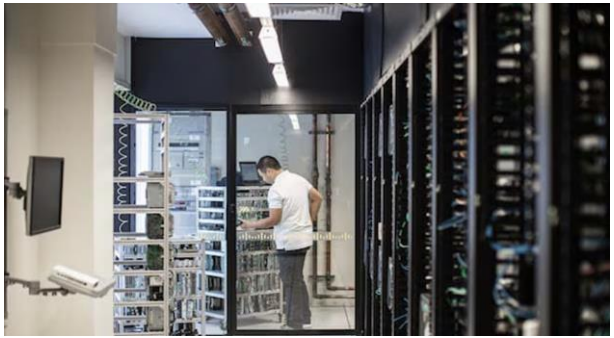
AI and Networking

Modern networks are becoming increasingly complex and the demand for real-time insights and automation has never been higher.

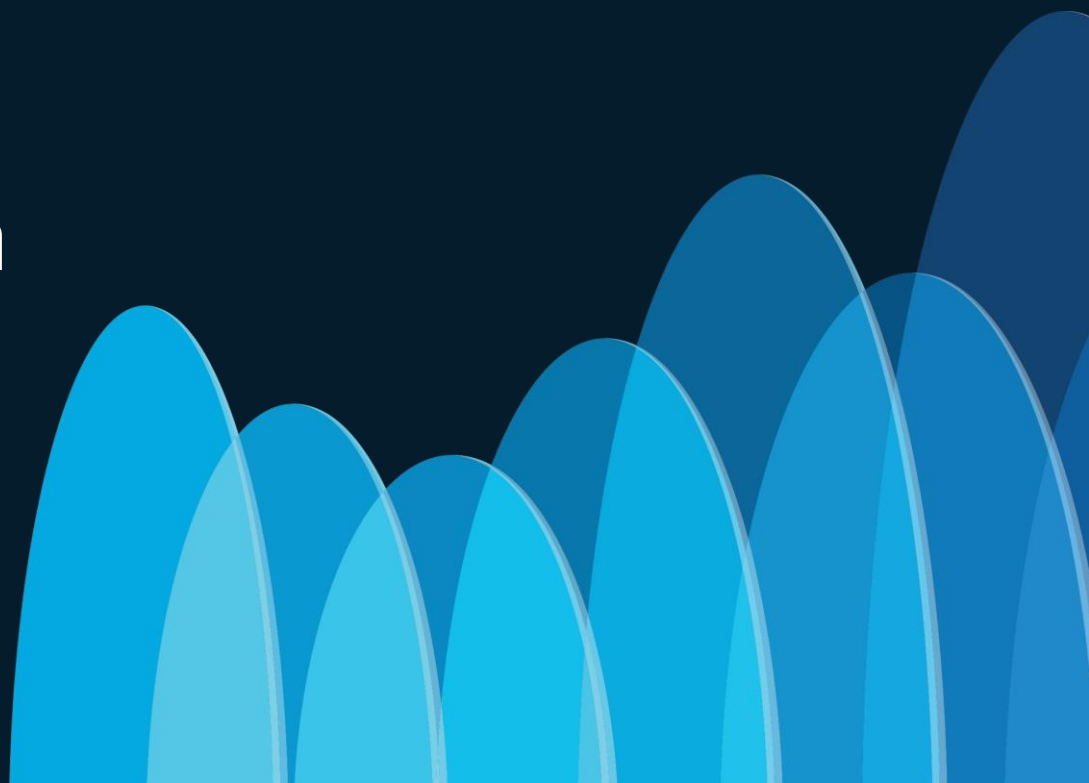
- Billions of devices connected with unique features and at the same time vulnerabilities
- Hybrid Architectures with Dynamic workloads and advanced applications
- Increase Security Challenges

AI provides us with opportunities including:

- Predictive Maintenance.
- Network Optimization.
- Enhanced Security



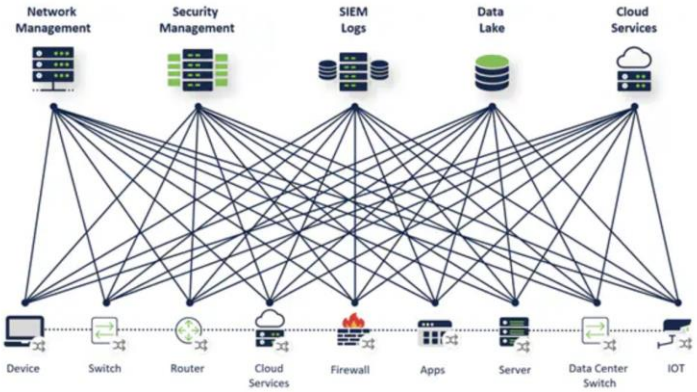
The Role of Data



Cisco Data

Cisco has numerous key data sources including:

- Cisco Catalyst Center telemetry
- ThousandEyes monitoring
- Meraki Cloud Insights
- Security analytics from Cisco XDR



These sources provide benefits including:

- Granular network visibility
- Proactive incident management
- Proactive Security
- Automation and AI

Splunk Data

Splunk’s Observability Suite provides data including:

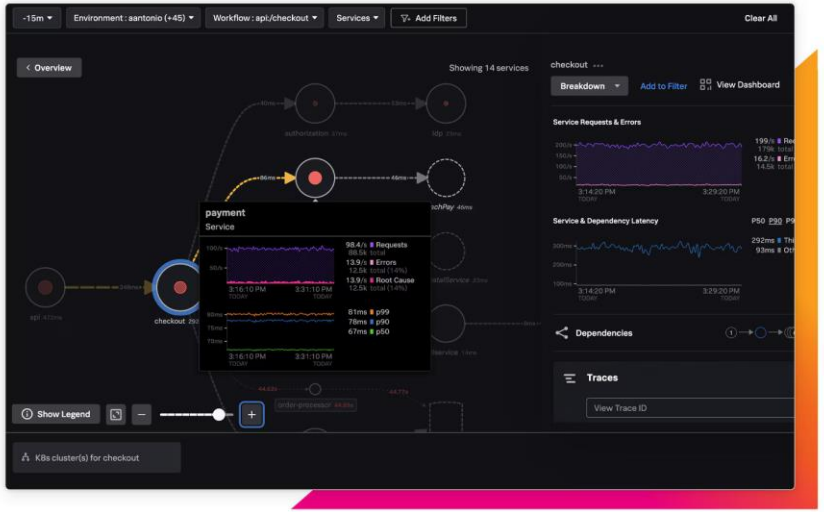
Application
- Metrics, Logs, and Traces

Infrastructure
- Host, Container, and Cloud Metrics

Network
- Traffic, Flow, and Connectivity

Security and Compliance
- Audit Logs and Threat Detection

Machine Learning and Analytics
- Anomaly Detection and Predictive Analytics

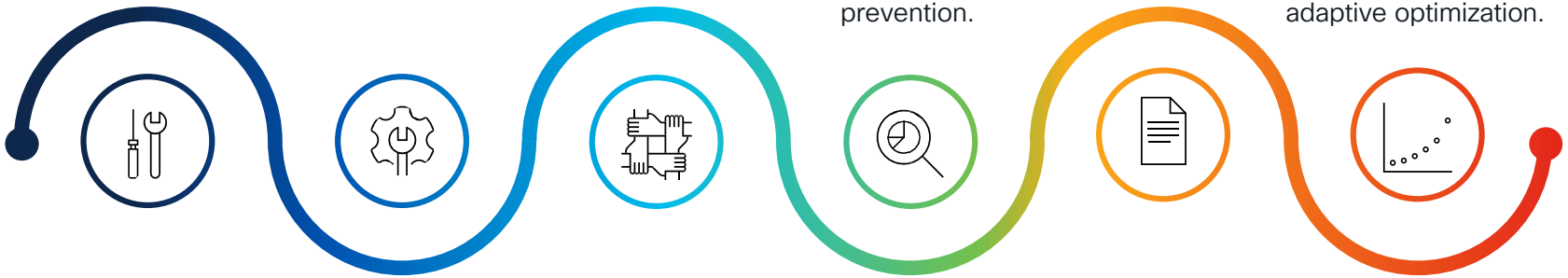


AI-Driven Telemetry Workflow for Predictive Networking

Data Ingestion & Processing
Aggregates, normalizes, and enriches telemetry data for AI-driven analysis.

Predictive Insights & Automation
Generates actionable recommendations for performance optimization, security, and fault prevention.

Automated Response (Agentic Framework)
AI-driven agents dynamically implement network changes, ensuring self-healing and adaptive optimization.



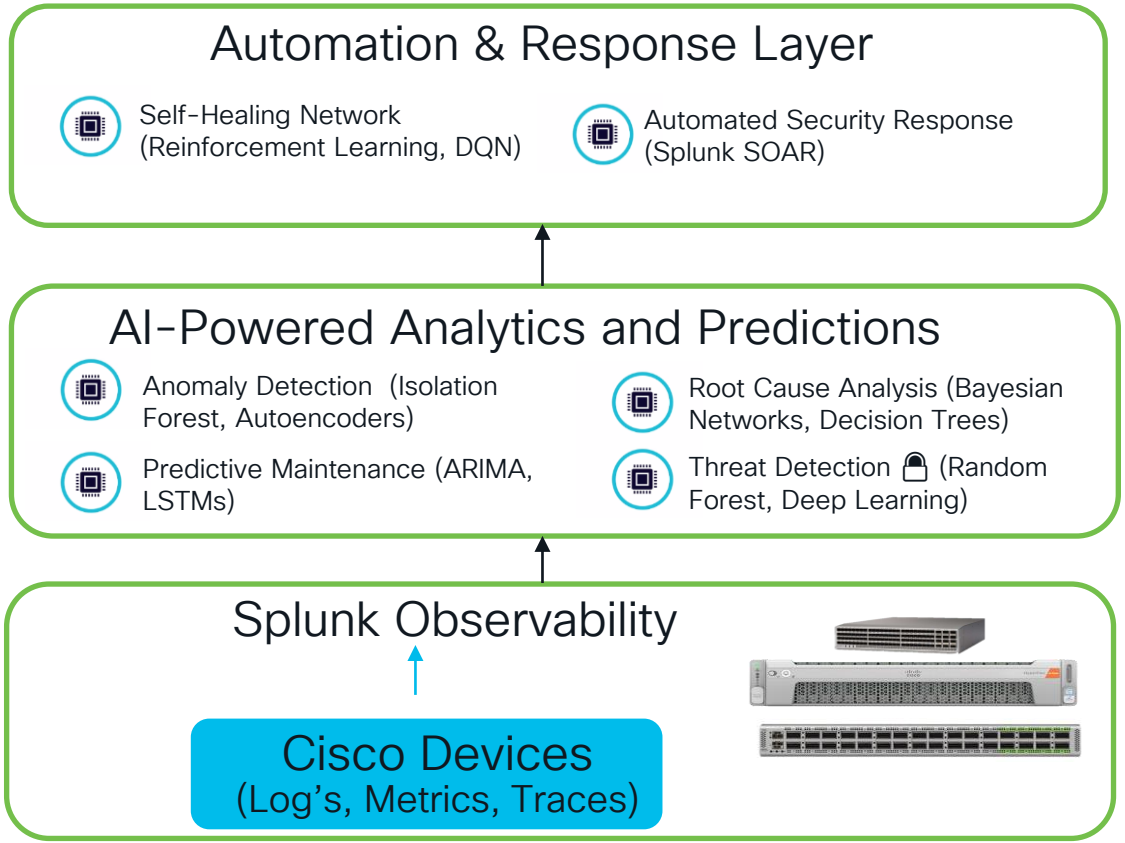
Telemetry Data Collection
Captures real-time network data from Cisco devices, including logs, metrics, and traffic patterns.

AI-Powered Analysis & Anomaly Detection
Uses machine learning models to identify patterns, detect anomalies, and predict potential failures.

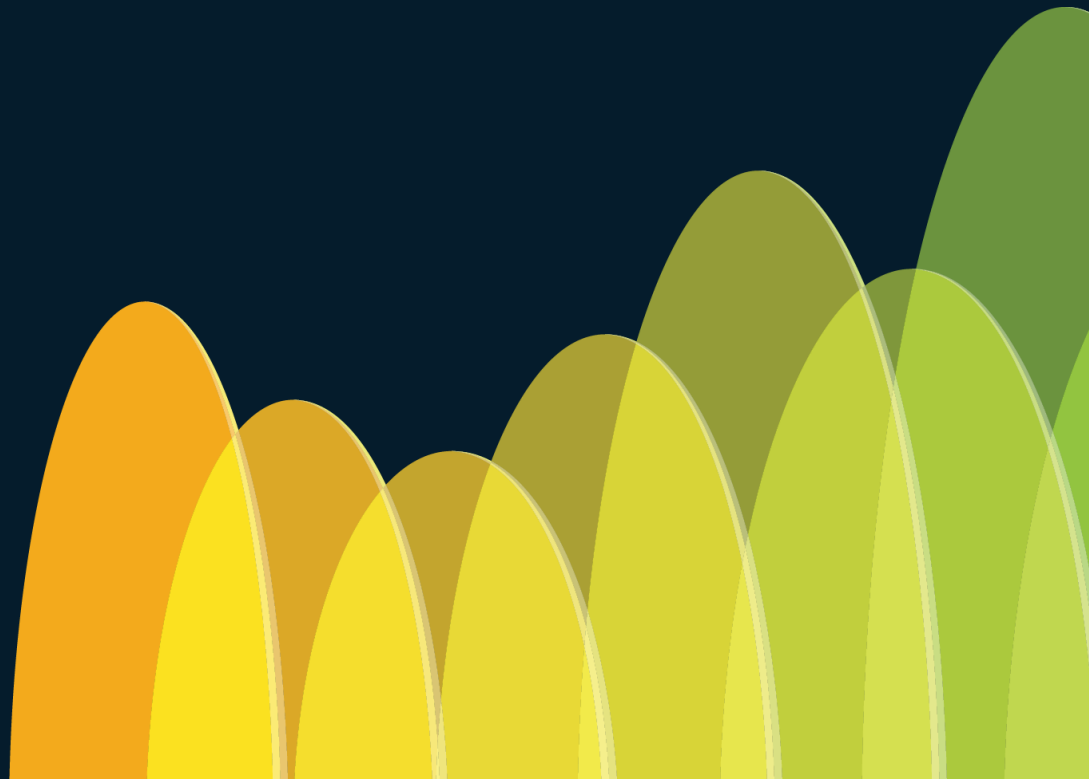
Actionable Response & Optimization
Automates policy adjustments, traffic shaping, and incident responses based on AI insights.

cisco Live!

AI-Powered Networking with Telemetry



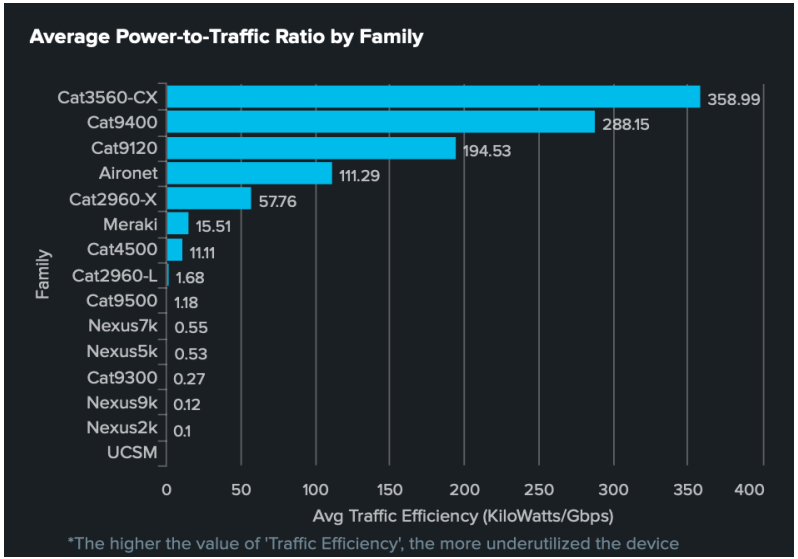
Use-Cases & Best Practices



cisco Live!

Use Case 1 – Predictive Maintenance

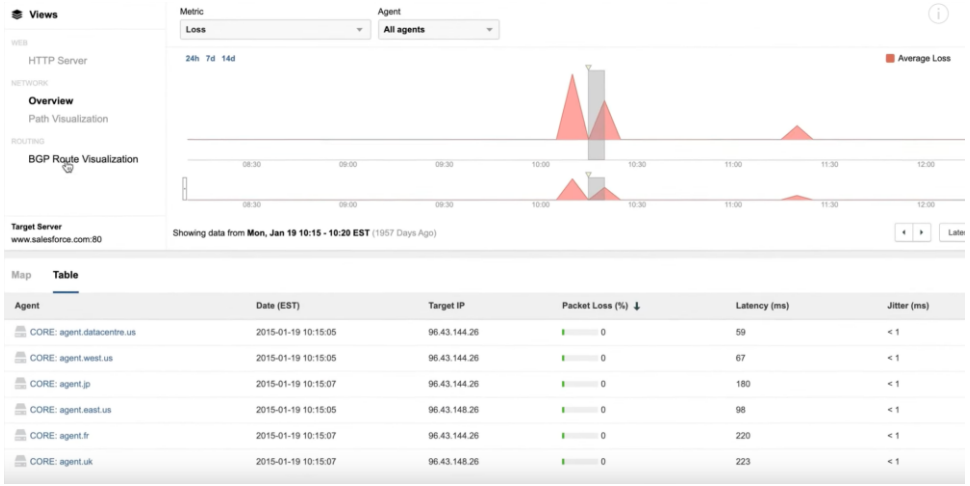
Predictive Maintenance Leveraging Cisco's device health data and Splunk's logs to predict failures.



- Identify the specific devices or systems that require predictive maintenance (e.g., routers, switches, or access points).
- Set measurable goals such as reducing downtime, preventing failures, or improving network reliability.

Use Case 2 – Network Optimization

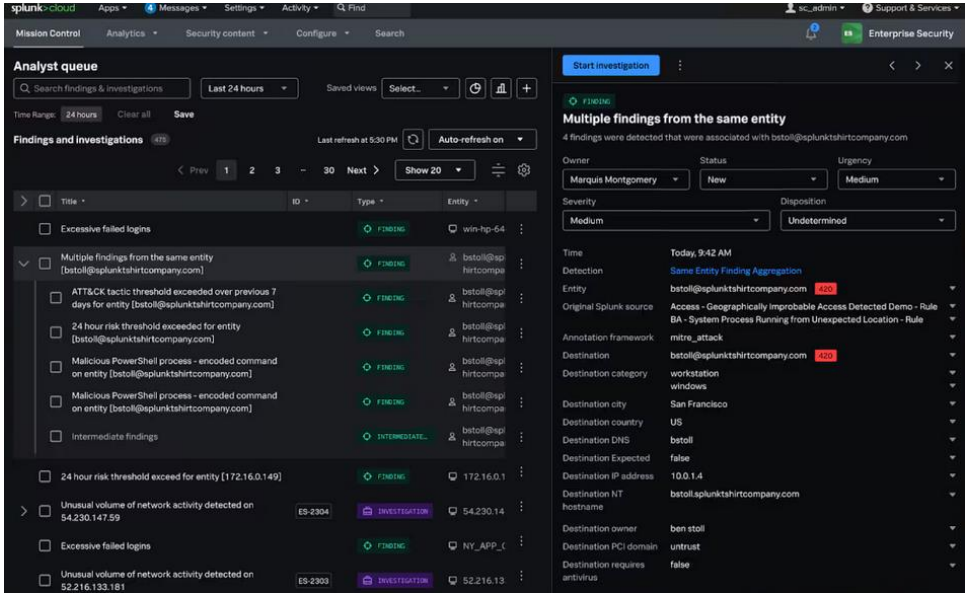
Network Optimization using AI models to optimize network traffic flows and reduce congestion.



- Reduce network congestion and improve traffic flows
- Minimize latency, balance loads across links, or maximize throughput
- Identify areas for optimization (e.g., data centers, branch offices, or WAN links).

Use Case 3 – Security Incident Detection

Security Incident Detection combining threat intelligence from Cisco with Splunk's anomaly detection



- Enhance security by proactively detecting and responding to threats
- Focus on specific use cases like phishing detection, malware identification, or insider threats
- Identify key security tools and data sources (e.g., Cisco SecureX and Splunk)

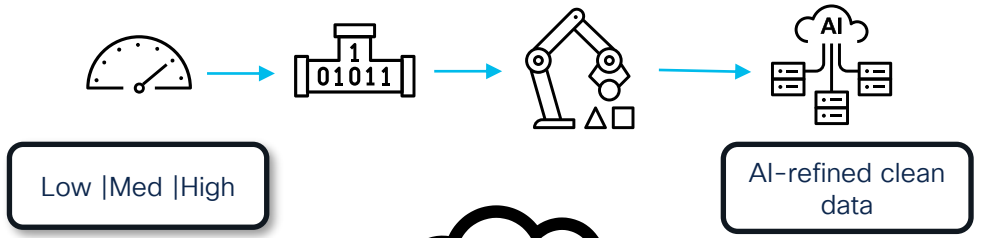
Technical Architecture Recap

Data Flow:

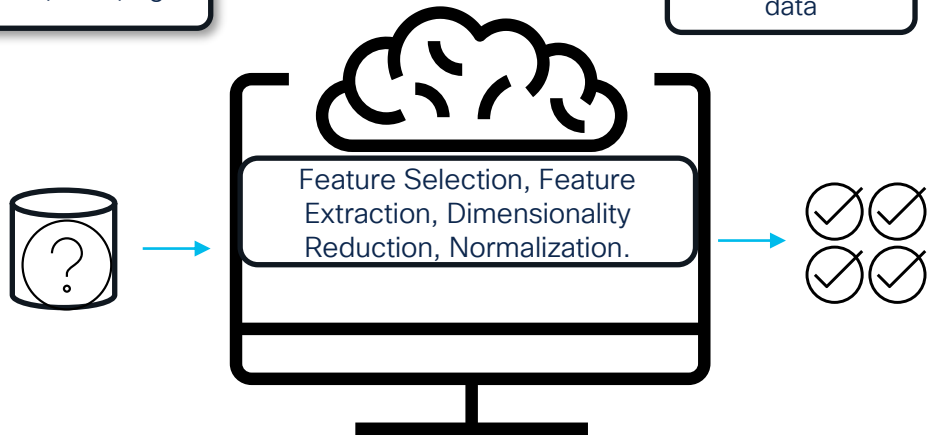
1) Data ingestion from Cisco devices
2) Data aggregation and correlation in Splunk.
3) AI model training using combined datasets.
4) Real-time predictions and automated actions.

AI Model Design Considerations

Data Quality



Feature Engineering



Model Evaluation

Best Practices for Implementation

Start Small

- Focus on a specific use case.

Automate Data Pipelines

- Use APIs and connectors.

Monitor and Improve Models

- Regularly update models based on new data

Challenges and Solutions

Challenges and Solutions

Challenge: Data Silos

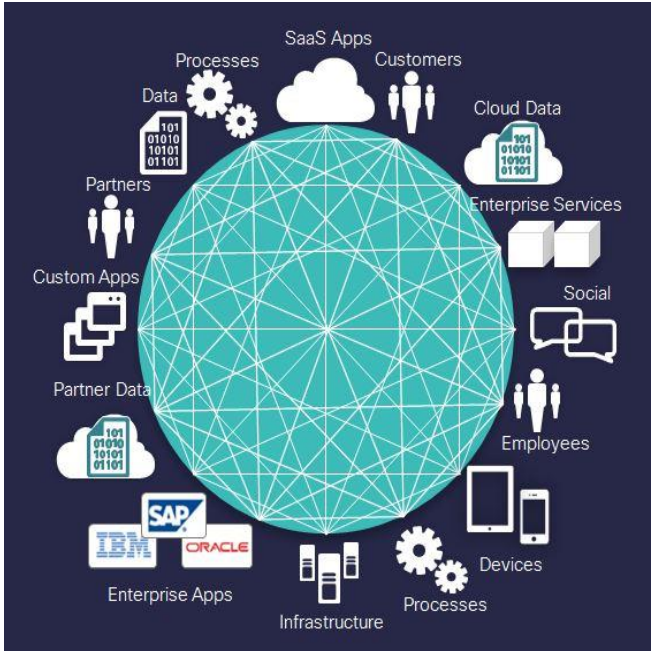
Solution: Use Splunk for data aggregation.

Challenge: Model Drift

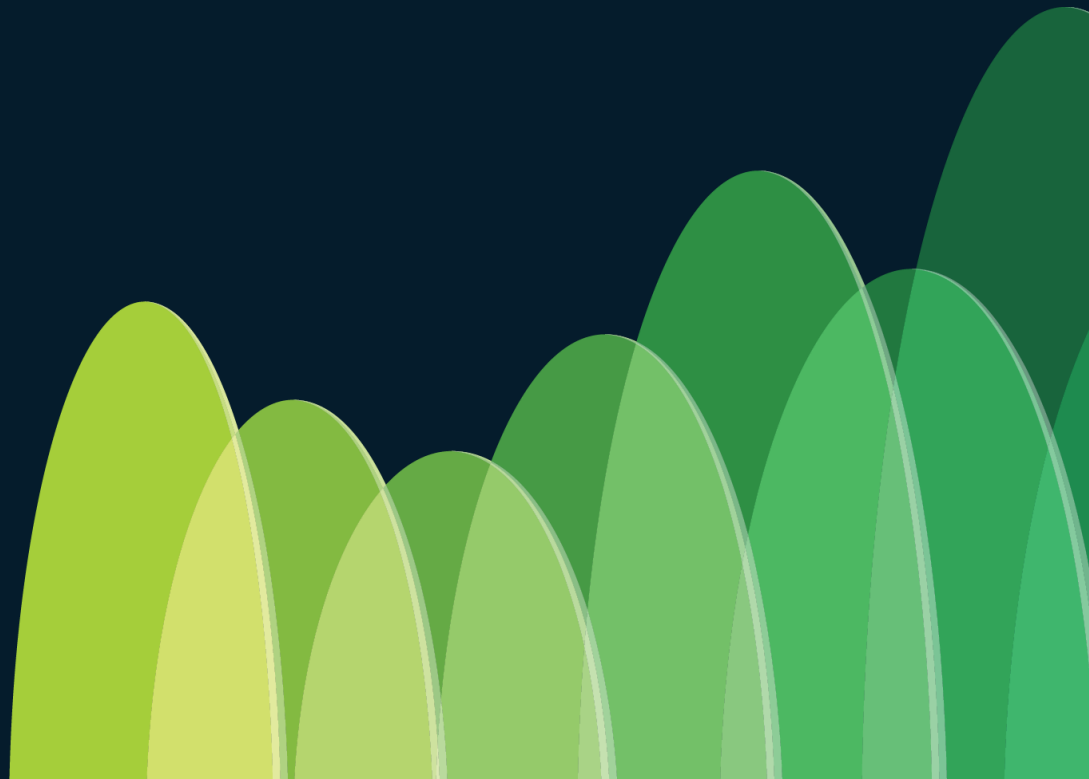
Solution: Continuous model monitoring.

Challenge: Security & Privacy

Solution: Implement role-based access controls.



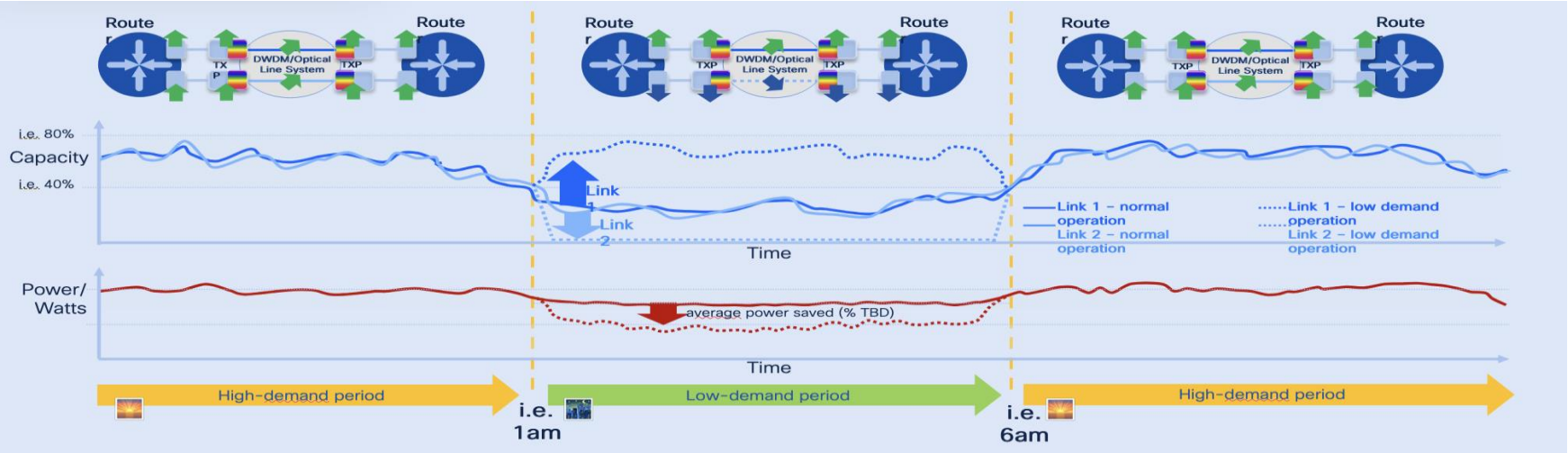
Success Story



Success Story

Case Study: SP Customer Challenge: Power and Cost

- Solution: Integrated Cisco and Splunk data to predict network utilization and enable power savings
- Outcome: Reduced power utilization and energy costs



Webex App

Questions?

Use the Webex app to chat with the speaker after the session

How

1. Find this session in the Cisco Events 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 February 28, 2025.

Fill Out Your Session Surveys

Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)

All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the ‘Participant Dashboard’

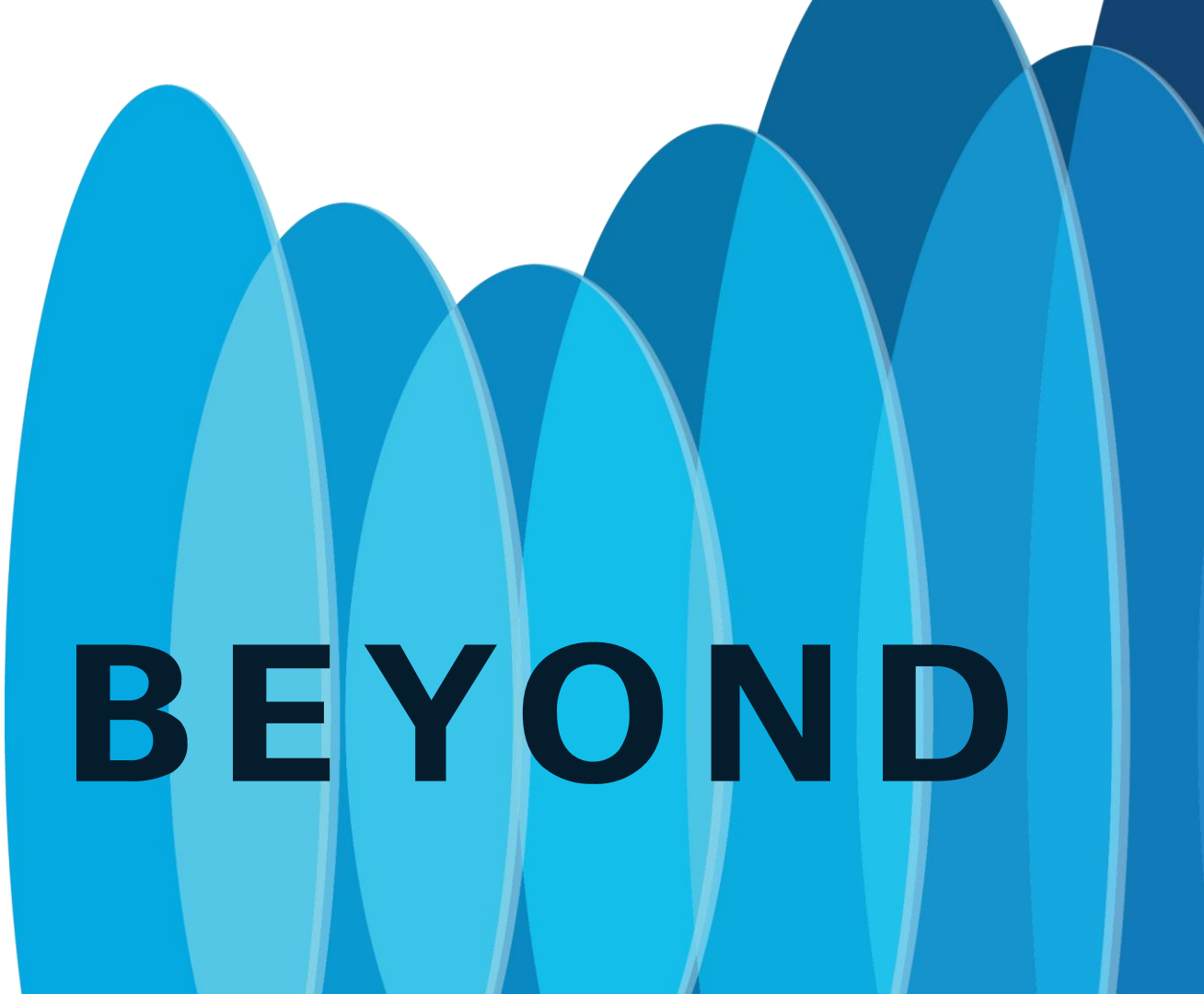
Content Catalog

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND