

Unified Observability from Splunk

CISCO Live !

Eliminate data silos and streamline workflows

Diana Omuoyo
Global Technical Observability Strategist,
Cisco

Session ID: BRKOBS-2546

Cisco Webex App

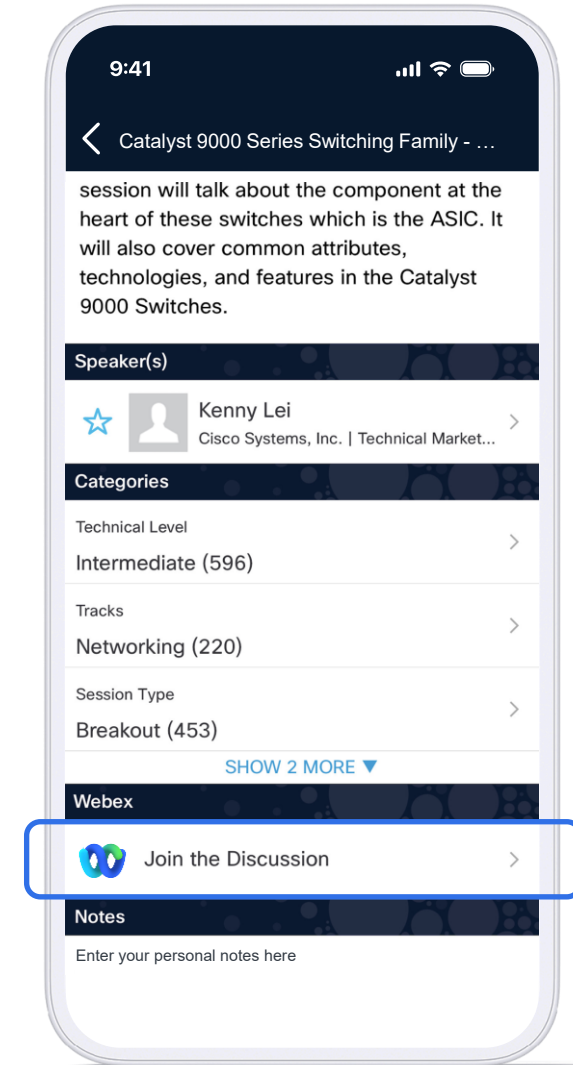
Questions?

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 14 November 2025.



<https://cislive.ciscoevents.com/cislivebot/#BRKOBS-2546>

Diana Omuoyo

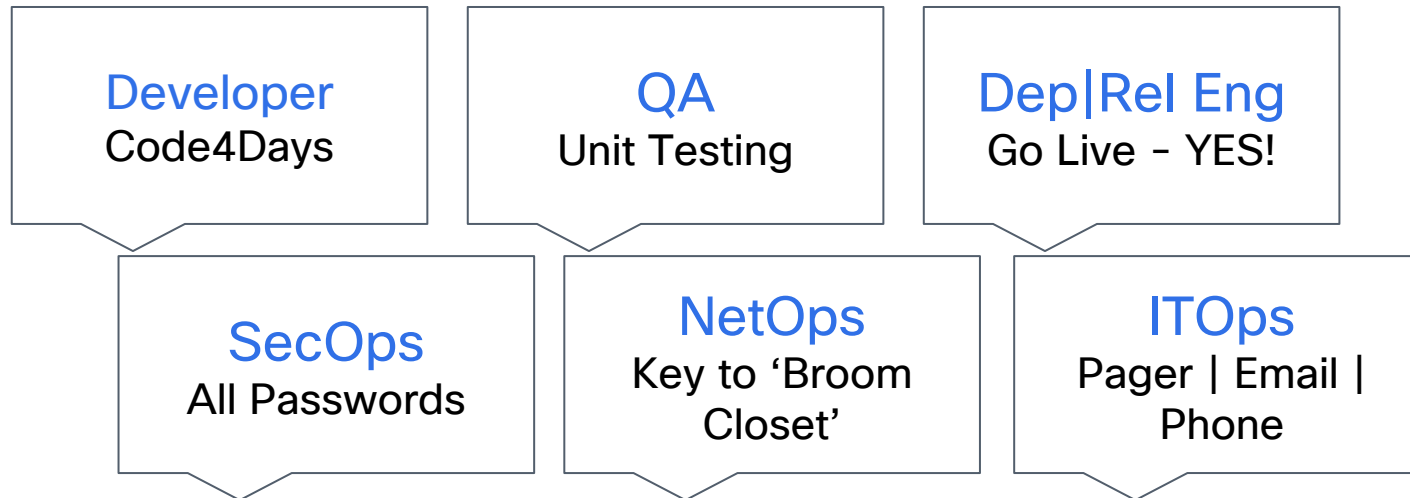
Global Technical Observability Specialist

Passion for tech – people,
ideas and possibilities



Then....

Full Stack Developer

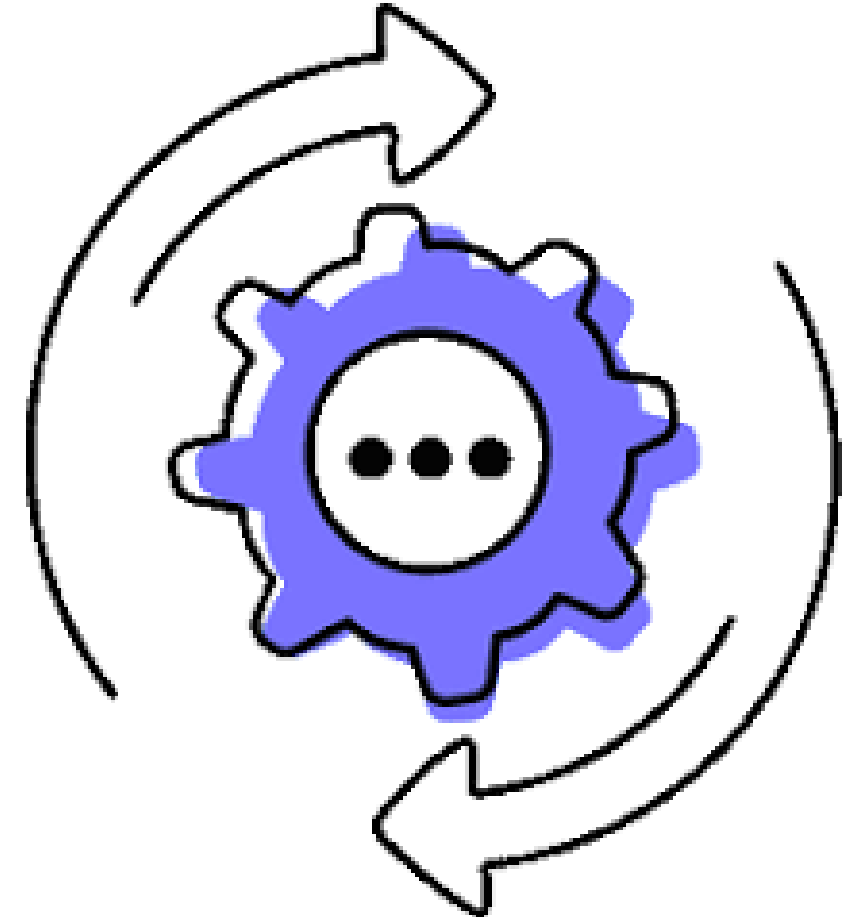


Best Part

Simplified Triage
| MTTx

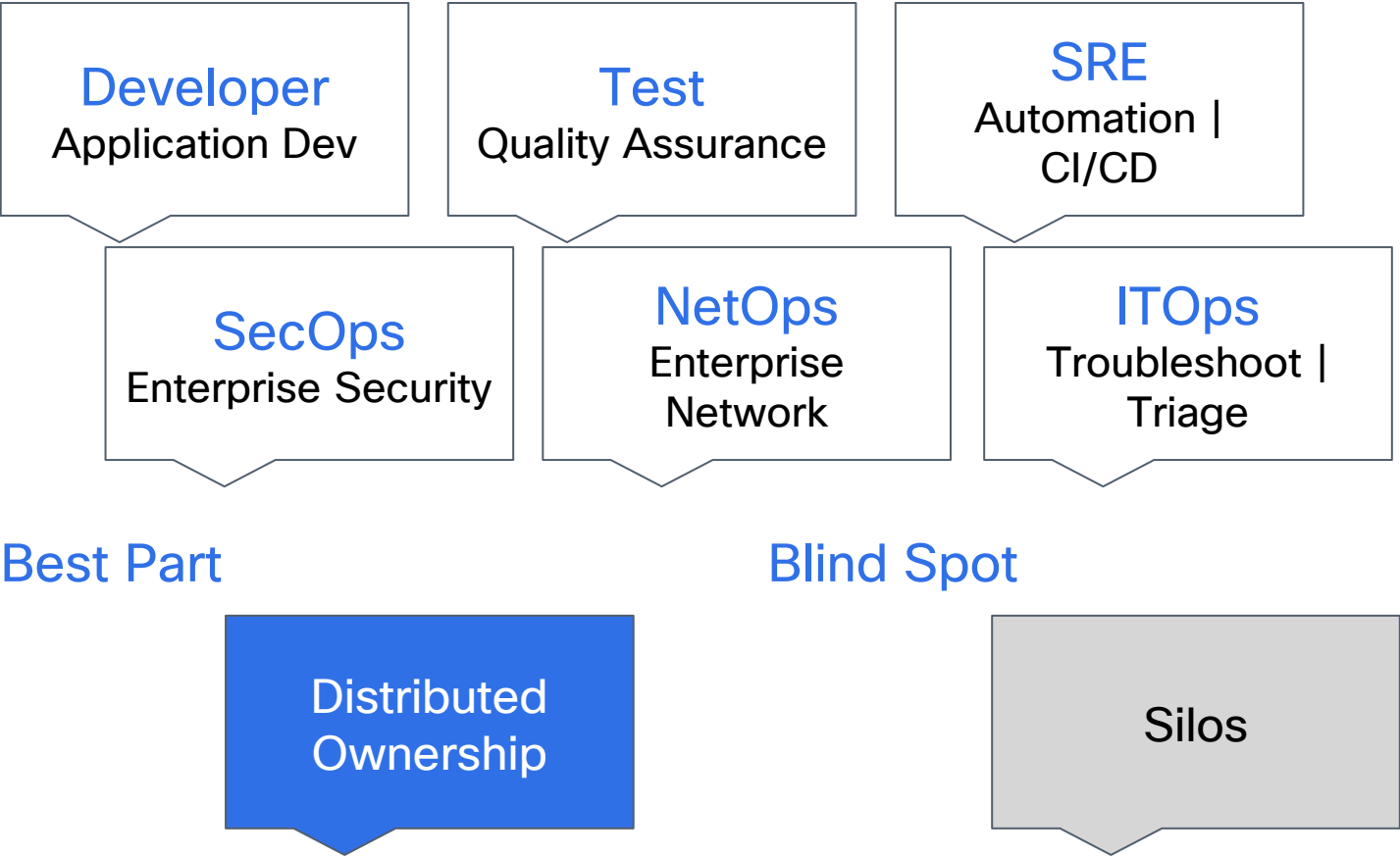
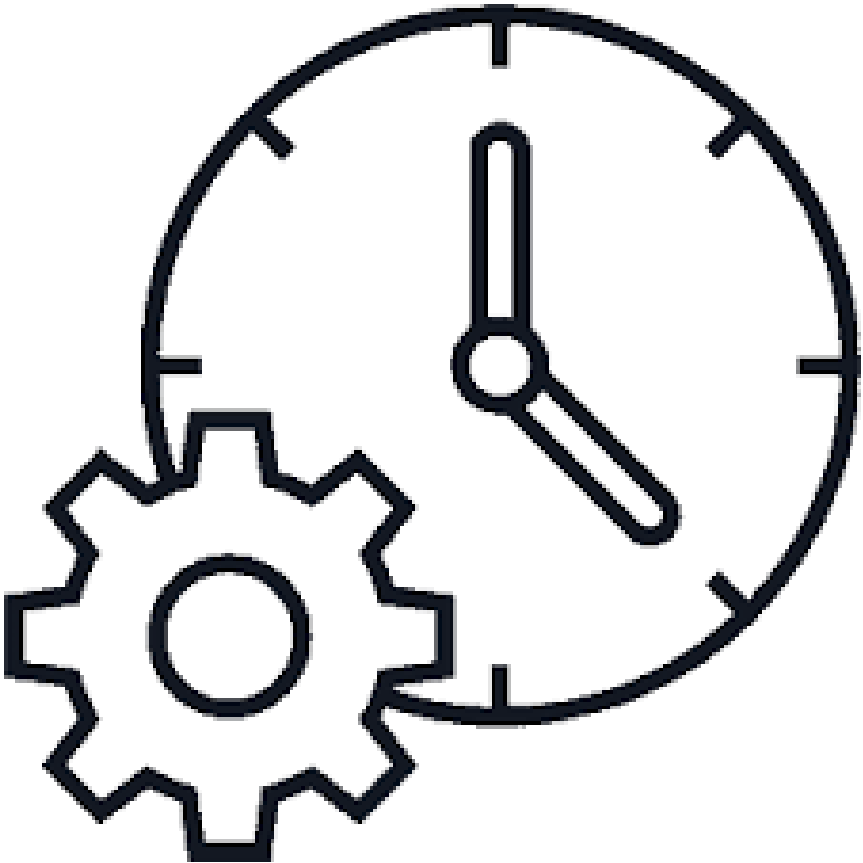
Blind Spot

Single Point of
Failure

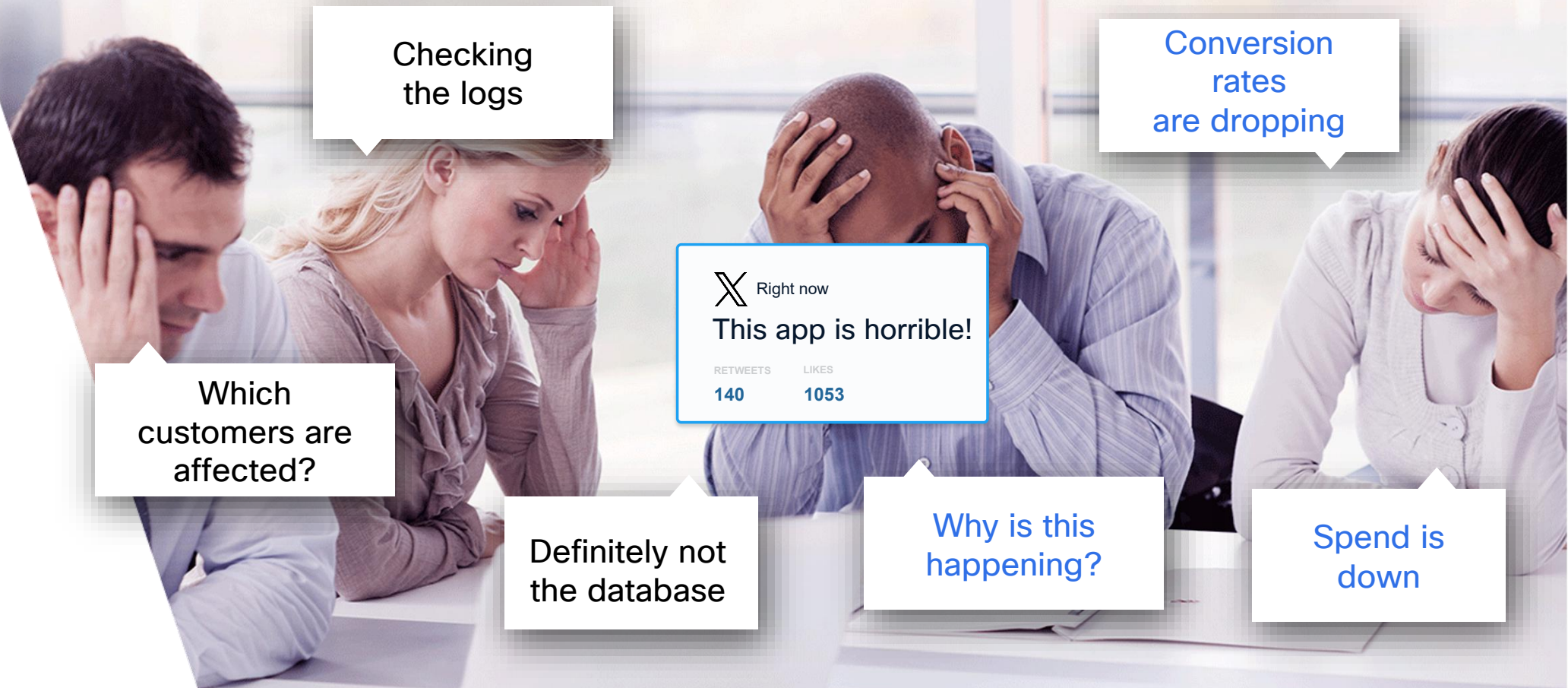


Now....

Dedicated Teams | Domain SMEs



Siloed teams solving complex problems



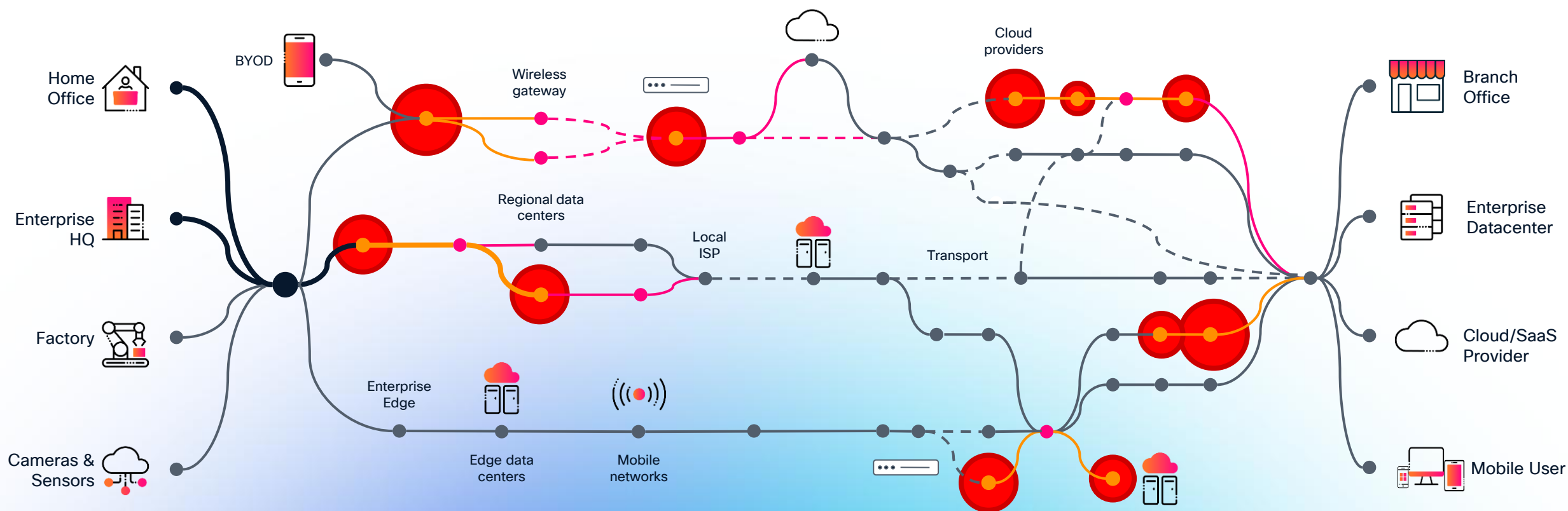
ITOps Team

Customers

Business

Challenge: Chaos & disorder

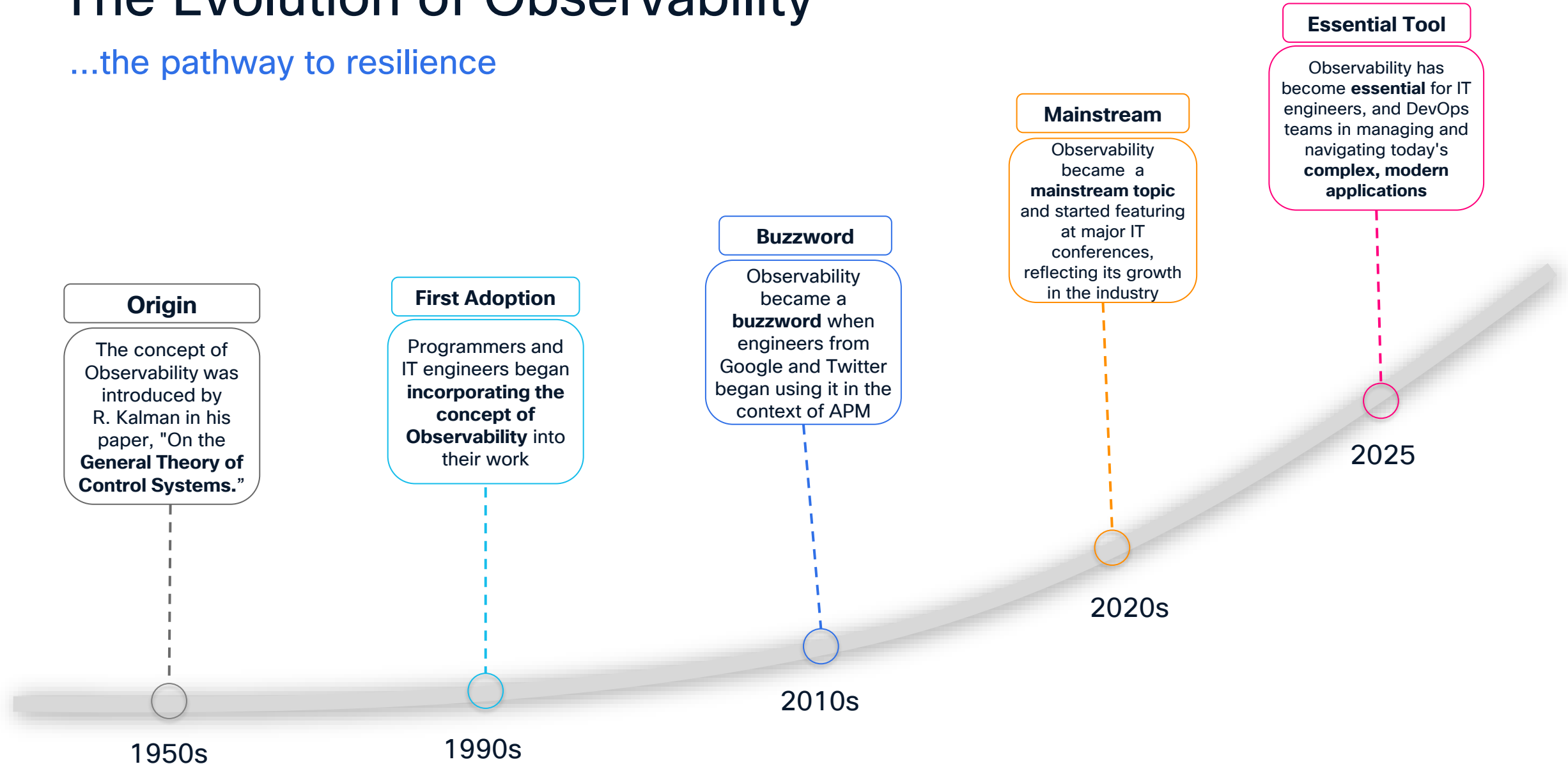
..yesterday's approaches to monitoring don't support today's reality



Strategic Observability

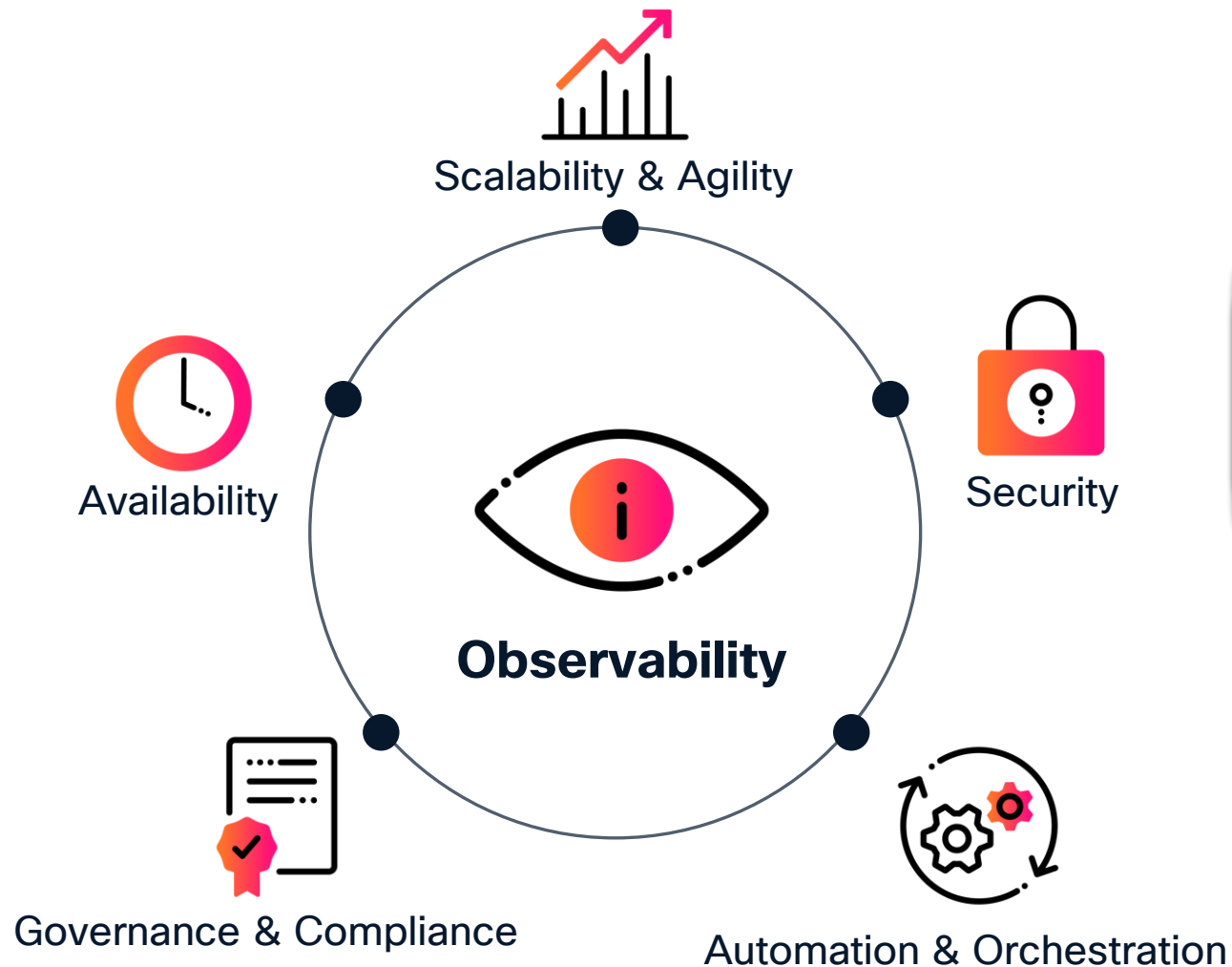
The Evolution of Observability

...the pathway to resilience



Task: Effective response & planning

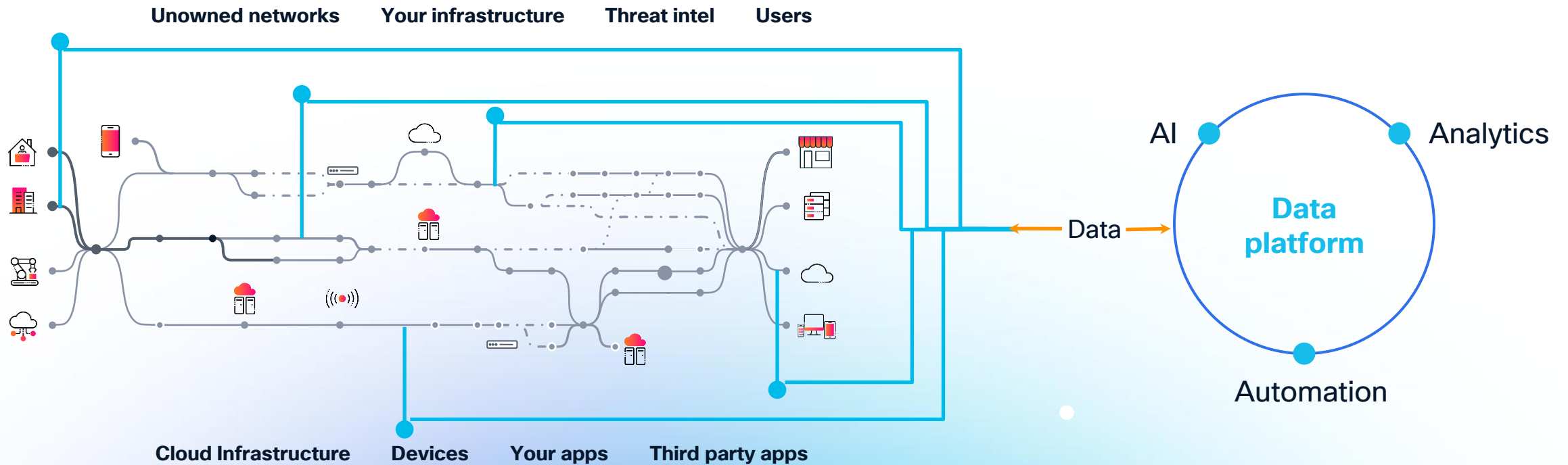
...key pillars of resilience



Ensure infrastructure **aligns with corporate policies, regulations, and risk frameworks**. Tracks configuration drift, access control, and audit readiness.

Goal: Single source of truth

...by unifying data across your observability practice



Security

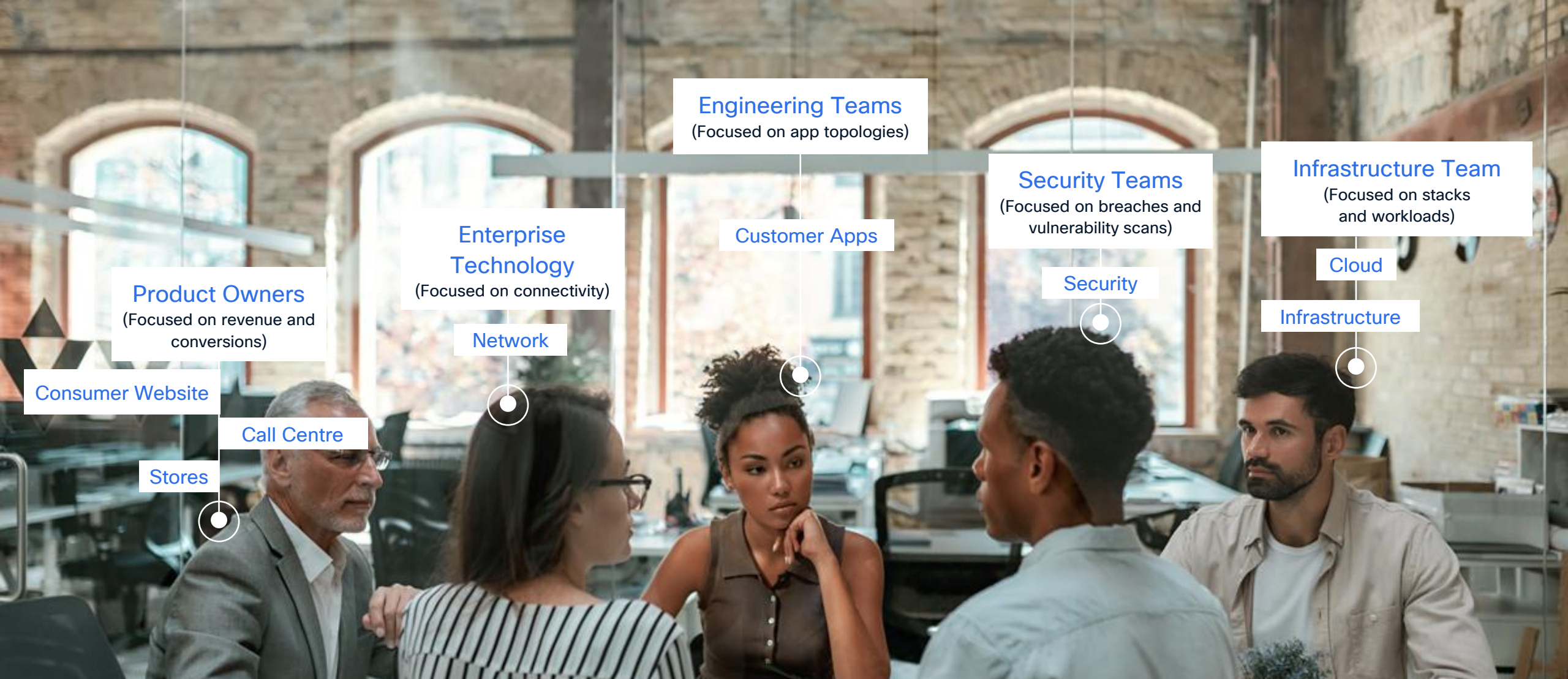
Comprehensive threat detection, investigation & response for orgs of any size & maturity

Assurance

Seamless connectivity across cloud, internet and enterprise networks

Observability

Prevent downtime and optimize experiences with visibility and insights across digital systems



Shifting the conversation to align **technical priorities** with **business outcomes**

Redefine complexity & risk

..understand relationships and dependencies in our environments

Enable the ability to:

- Anticipate
- Withstand
- Recover
- Adapt

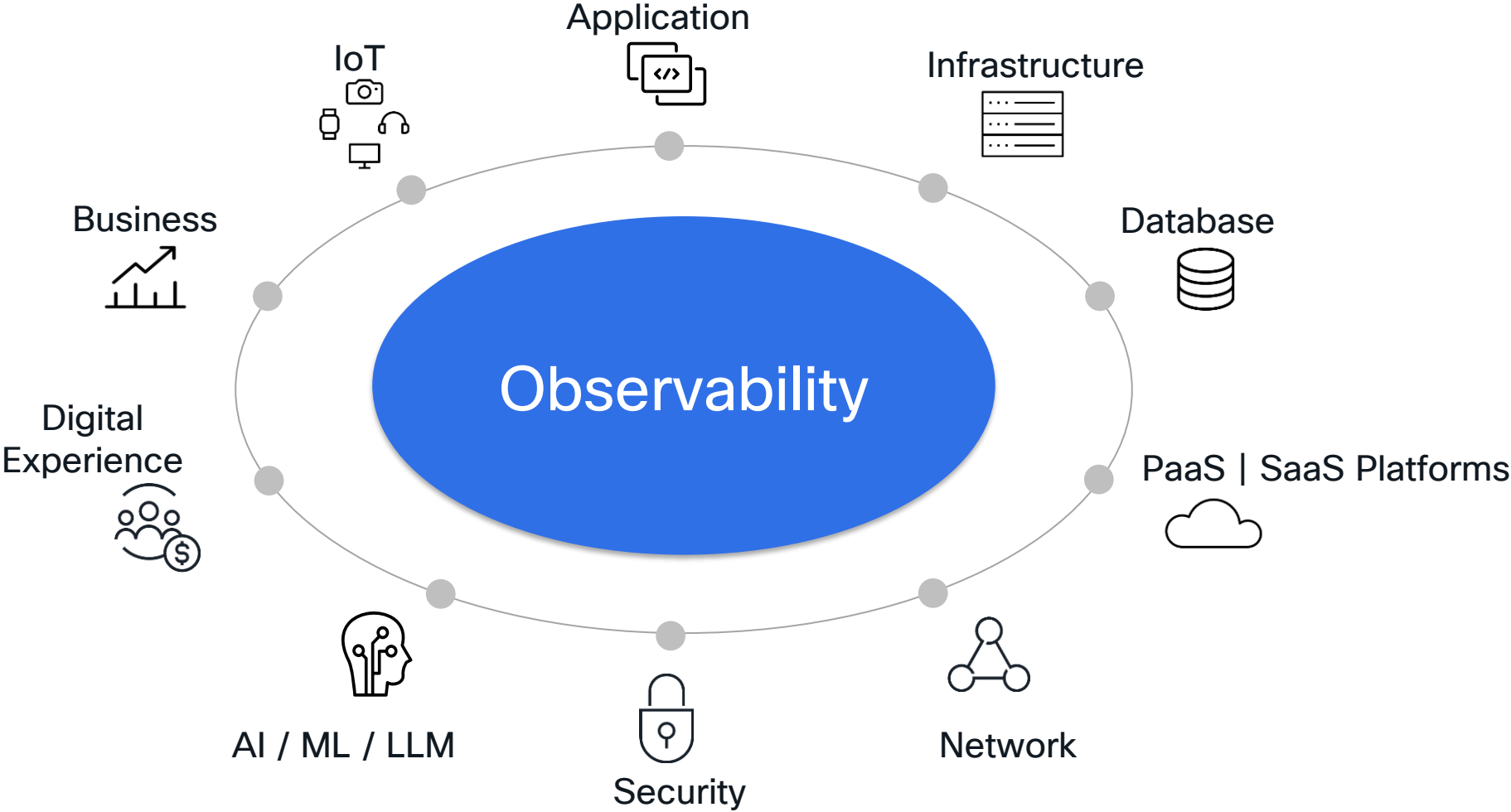
Why it matters

- Protects **brand reputation** and **customer trust**.
- Ensures **compliance** with regulations.
- Minimizes **downtime** and **financial loss**.
- Enables **innovation** without unnecessary risk.



Data Convergence

Exploring key observability domain areas





Bringing Splunk to your data

Building your Observability Practice with Splunk

Troubleshooting & Root Cause Analysis

AI-powered detection, diagnosis and response for performance problems across your apps and infrastructure.

Monitoring Critical Business Processes

See the impact of performance problems on business processes (checkout flows, order fulfillment, loan processing, etc.) and KPIs.

Understanding Critical User Journeys

See every step users are taking and improve their experiences on your web and mobile apps.

Performance Optimization for Apps & Infrastructure

Proactively improve the reliability of apps and infrastructure to prevent future problems.

Optimizing Observability Costs

Manage growing telemetry volumes more efficiently to reduce spend and avoid costly overages.

Detect & Prioritize App Security Vulnerabilities

Detect vulnerabilities and attacks in your application code, and prioritize response based on likely business risk.

Correlate network domains

Assure network service health by unifying visibility and reducing alert noise across network domains.

Pinpointing network impact on app performance

Troubleshoot app performance problems with dependencies on owned and unowned networks.

Monitoring AI applications & infrastructure

Monitor the health and performance of your AI application stack, including Agents, LLMs, and AI infrastructure.

Building your Observability Practice with Splunk

The power of a truly integrated solution

Splunk
ITSI

Cisco
ThousandEyes

Tests data exported in OpenTelemetry format
Deep-links from O11y Cloud to ThousandEyes

New!

Technology Add-on (TA)

Application running on
top of Splunk Platform

ITSI content packs (CP)

Log Observer Connect

AppD: Test results available in dashboards and EUM
TE: Tests recommendations, service dependency
and alert notification

Log Observer Connect for AppDynamics

Technology Add-On (TA)

Splunk Platform

Splunk O11y
Cloud

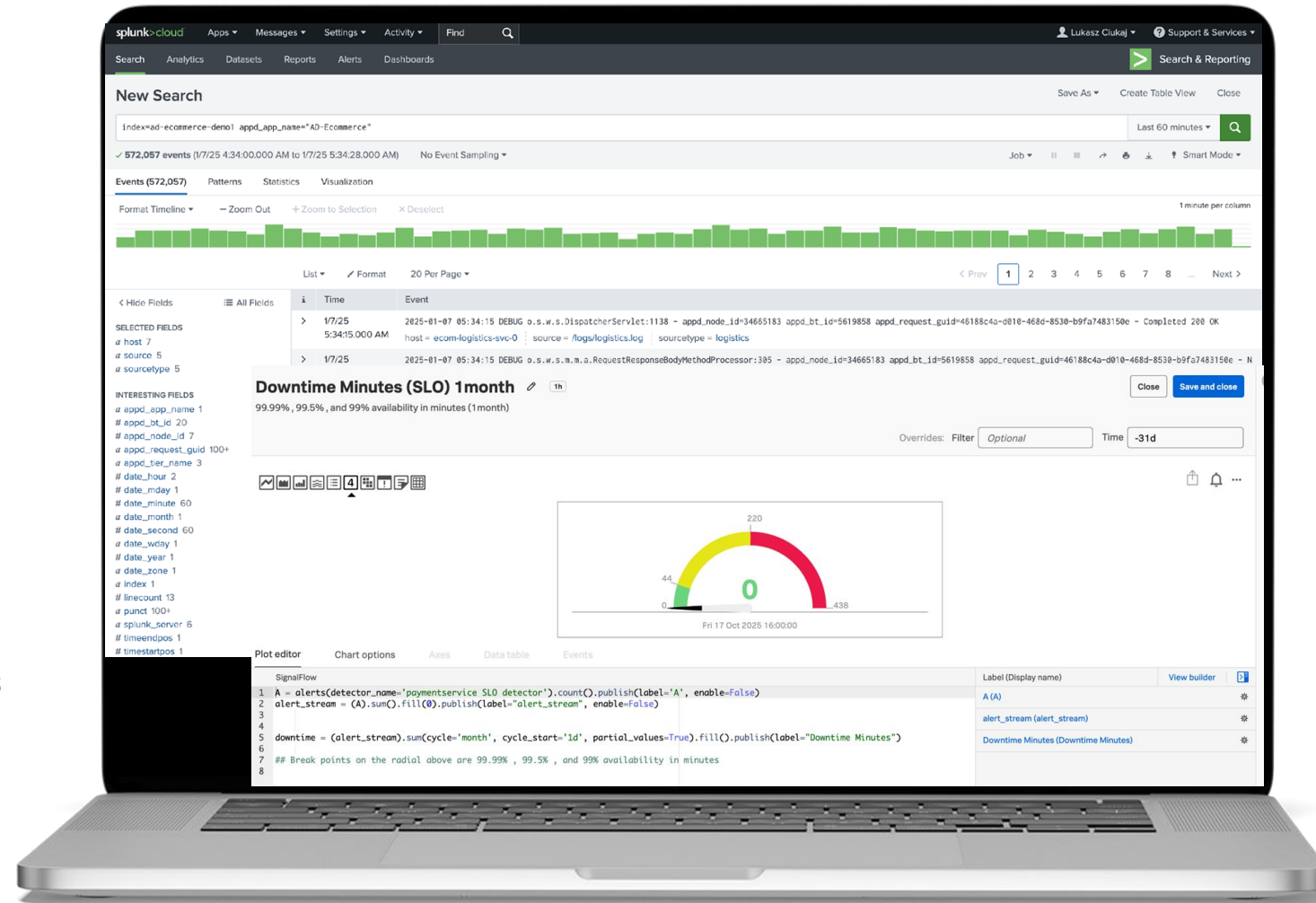
Splunk
AppDynamics

...digital ecosystem observability



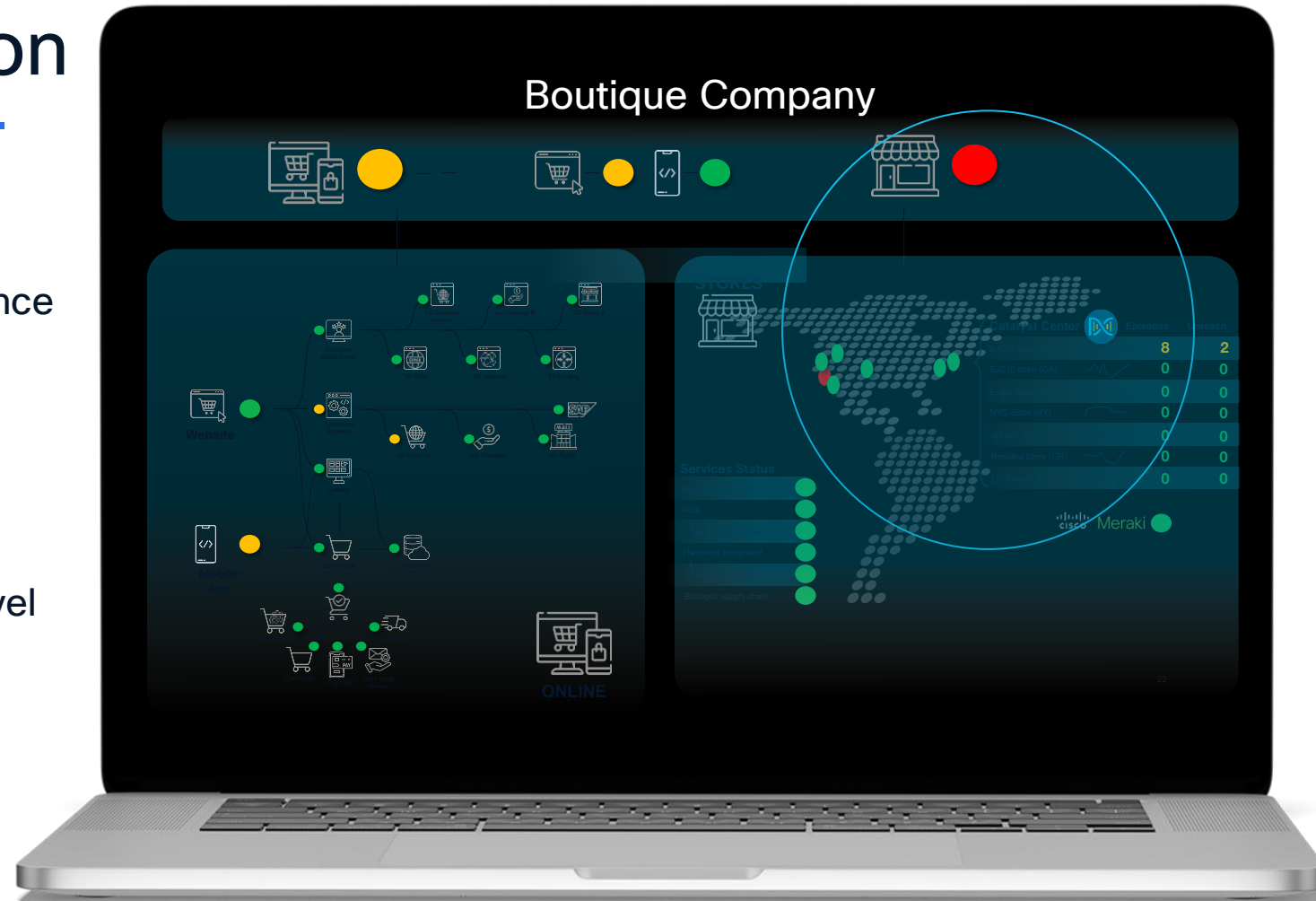
Powerful machine data aggregation, search, reporting and alerting

- Flexible data onboarding
- Full-fidelity investigation
- Real-time alerting
- Build custom apps
- SaaS or self-managed
- Standardize Observability Practices Across Teams (OpenTelemetry native)



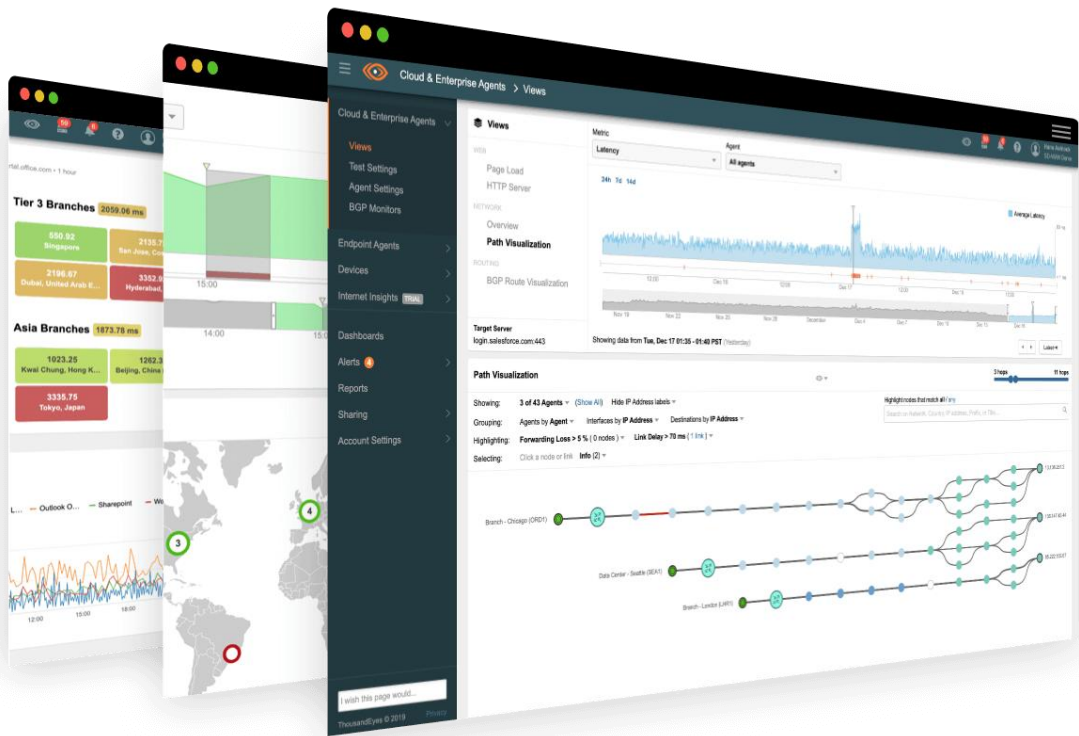
Optimize hybrid application performance with end-2-end insights

- End-to-end visibility from end-user experience to back-end code & infra
- Insight into cross-application dependencies
- Visualize the business impact of application performance issues
- Monitor SAP performance down to code-level insights



Digital experience framework

...enhancing Observability with Assurance through a big data source



Customer

Your Apps

Deliver stellar digital experiences to users

Workforce

Your People

Keep workers connected and enjoying seamless app performance

Enterprise

Your Infrastructure

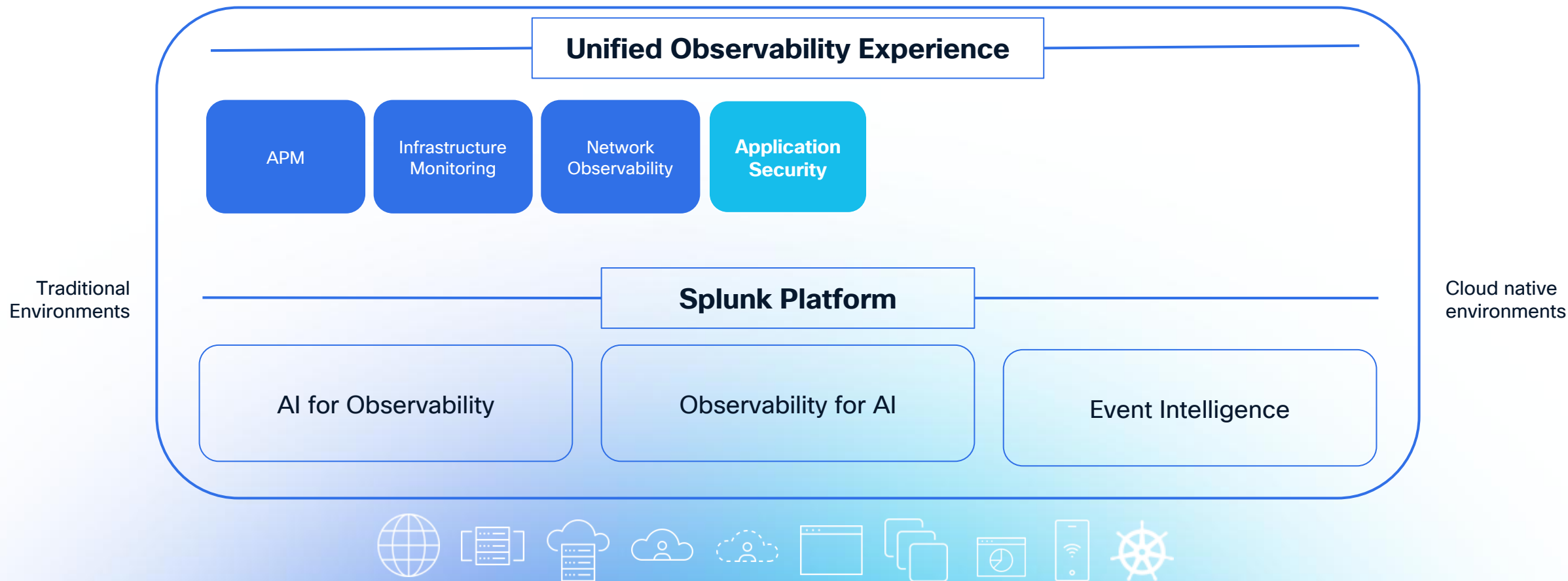
Optimize and sustain the flow of your digital supply chain

Demo Placeholder

TE & O11Y

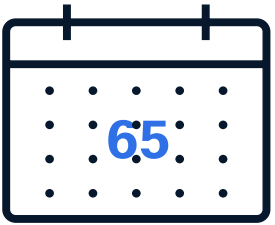
Building your Observability Practice with Splunk

Security Insights

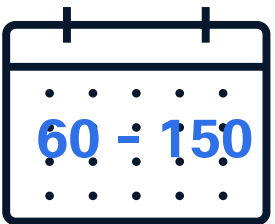


Prioritize remediation based on business impact

...bridging observability & security



days to resolve critical vulnerabilities



days to remediate known vulnerabilities

What matters....

- Severity
- Complexity of the fix
- Organizational practices

Detect & remediate vulnerabilities & exploits

...digital security

Risk & Impact-Based Prioritization



Detect Vulnerabilities



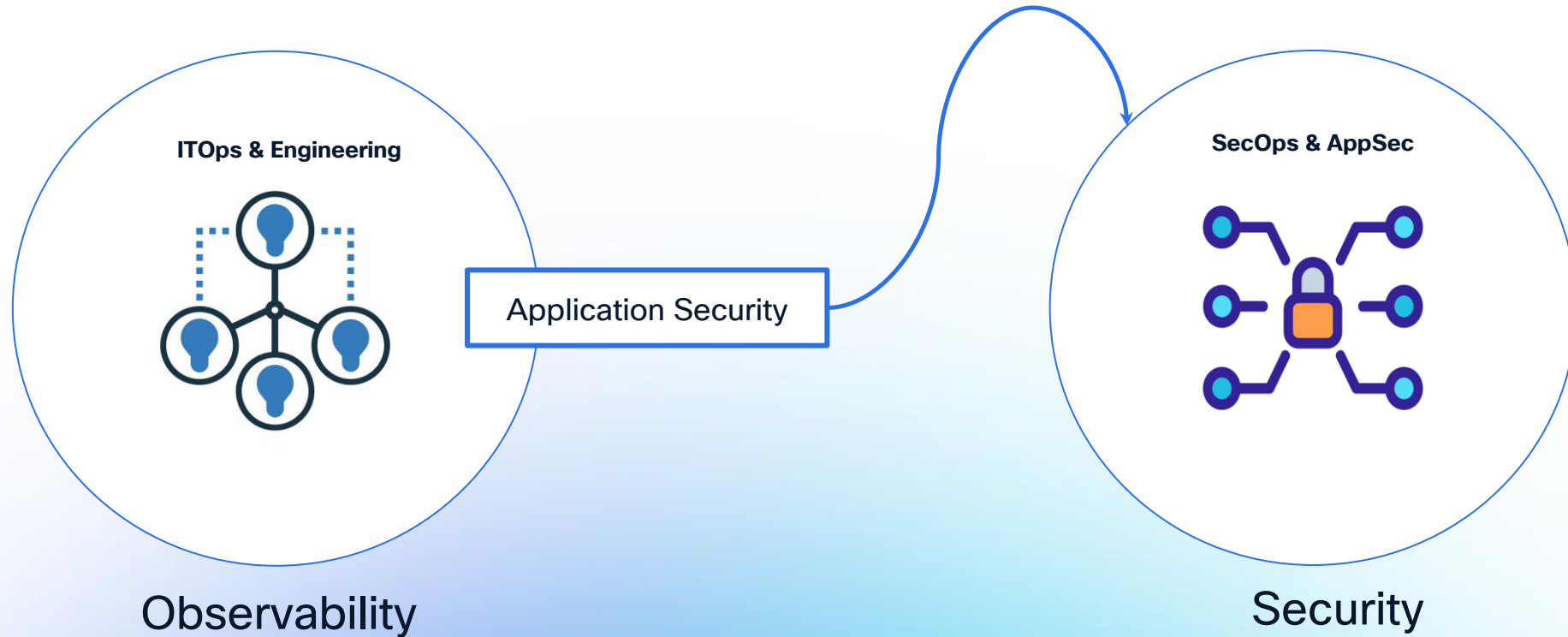
Detect Threats



Block Threats

Bridging application and security teams

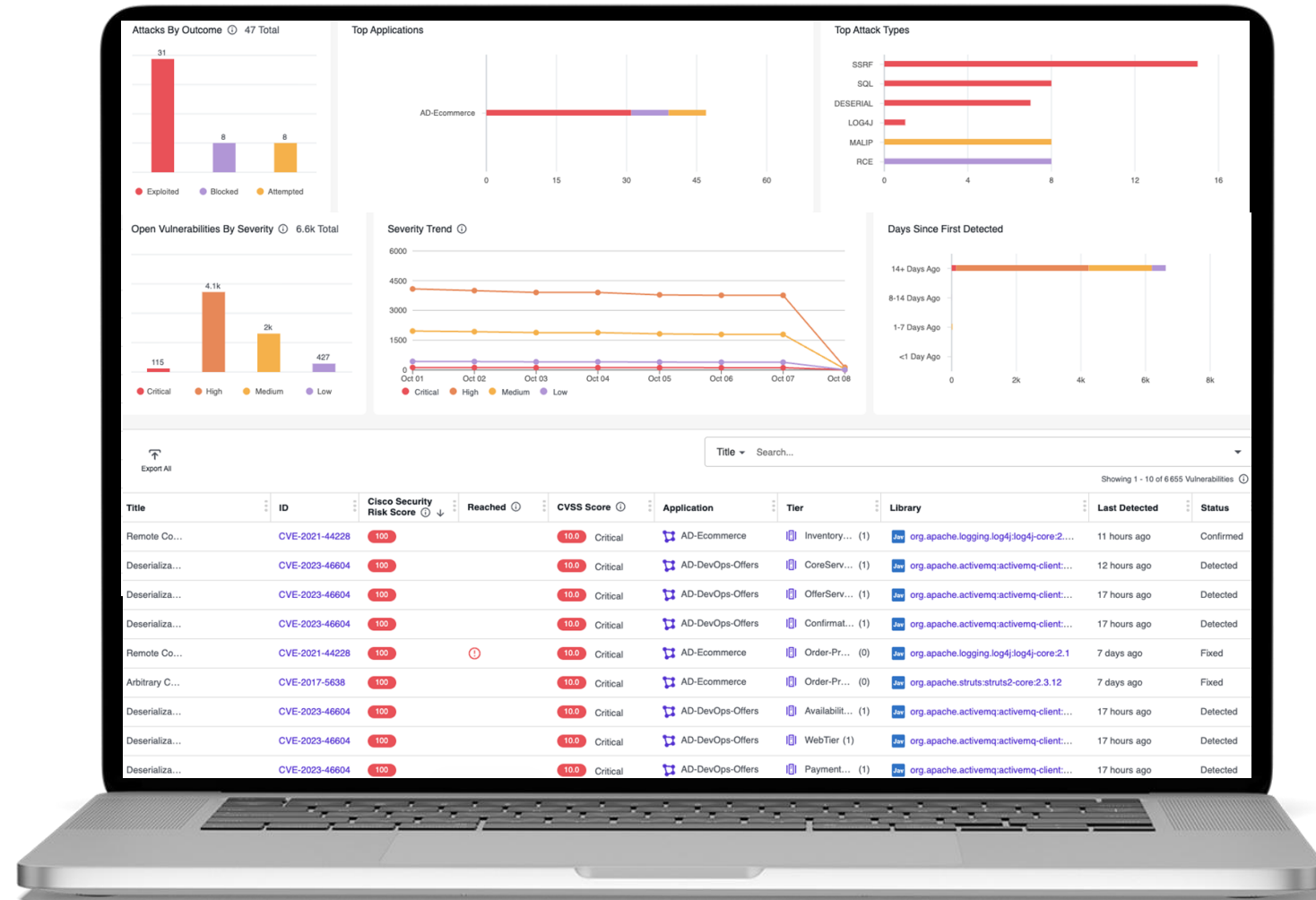
...bridging observability and security



Bridging application and security teams

...increase agility through cross team information sharing to speed MTTR

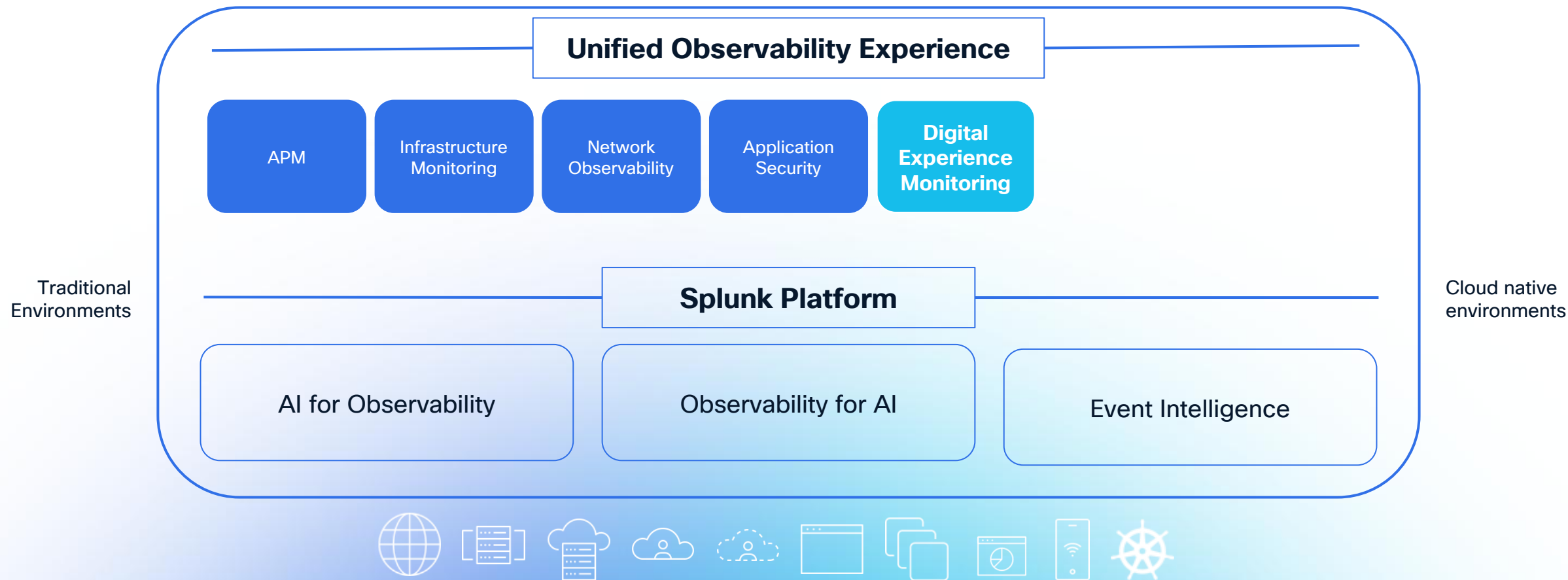
- Seamless integration with Splunk Enterprise Security so SecOps can leverage application and risk context
- Share critical exploit, application, and vulnerability details to align teams
- Enable SecOps to prioritize security incidents based on actual risk rather than generic threat indicators



Demo Placeholder

Building your Observability Practice with Splunk

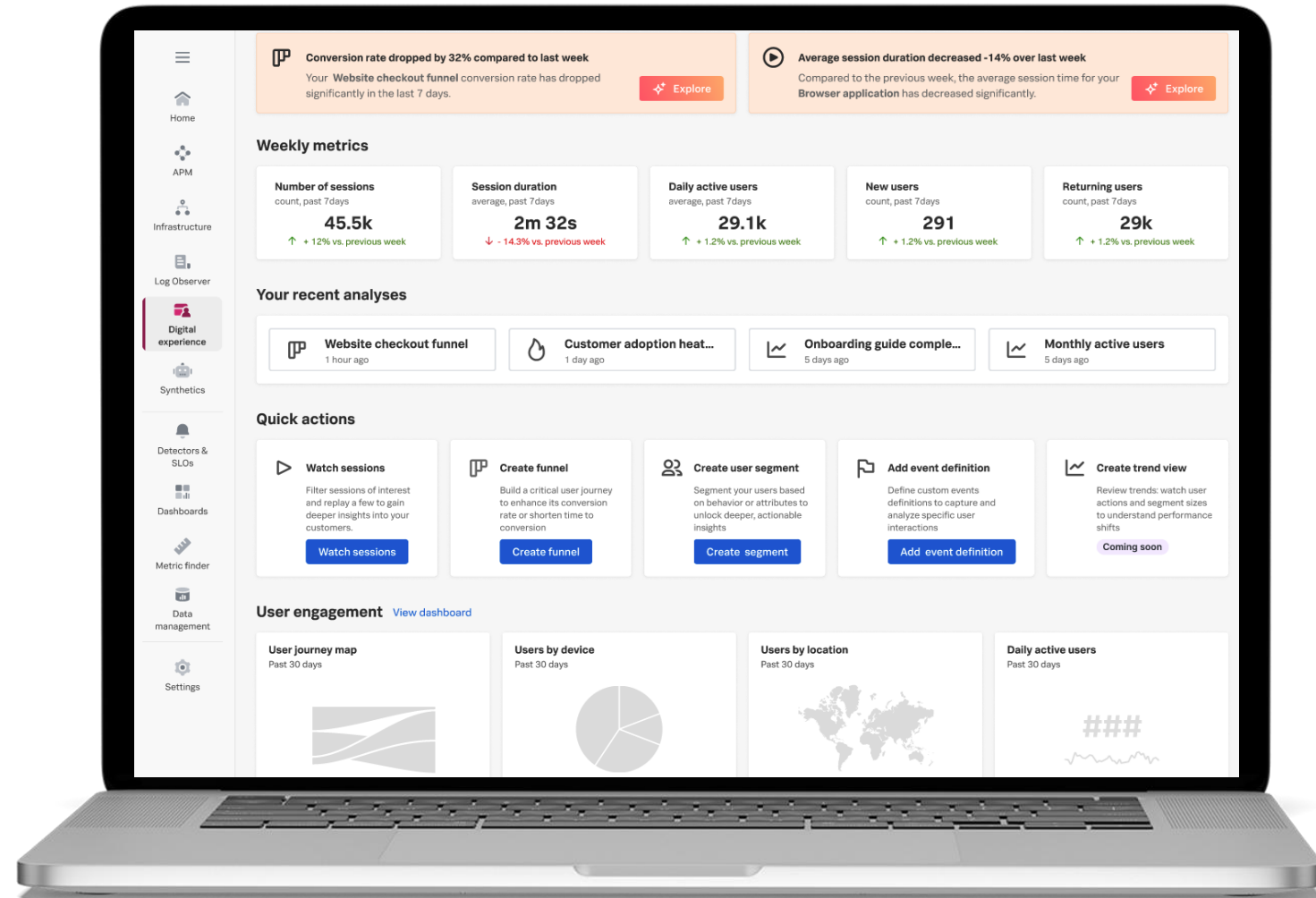
...digital experience monitoring



Digital Experience Analysis

Digital Experience Analytics is the process of understanding customer behavior, intent and sentiment across all digital domains and generating actionable insights for digital product teams.

—Gartner



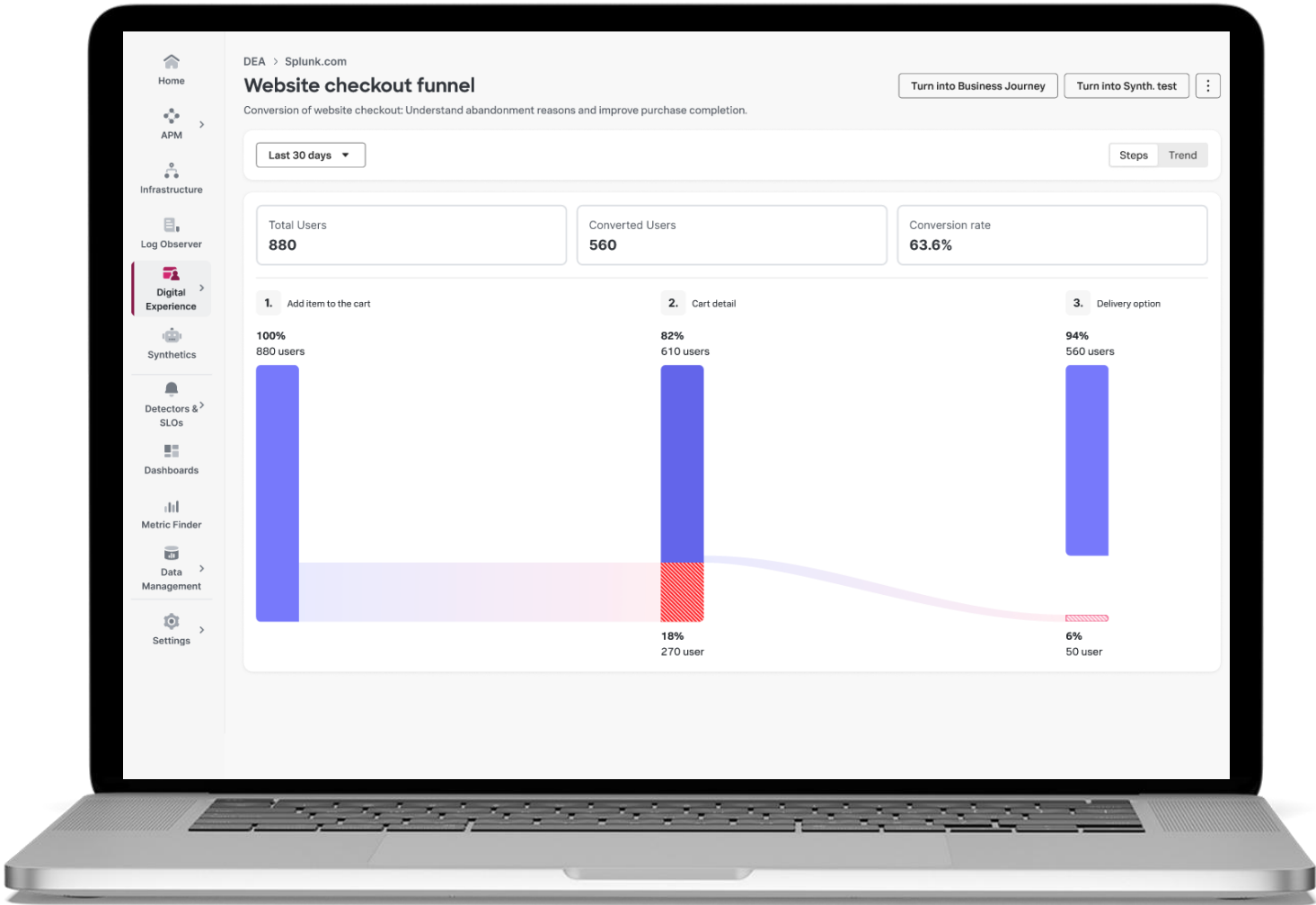
Conversion Funnels

Conversion funnels help you understand the conversion rates of essential user journeys.

Q Search...

User ↕	Session Start ↓	Session Replay ↕	Platform ↕
907...327	9/18/25, 1:05 PM	▶ Replay	Windows Chrome
62d...5e9	9/17/25, 1:18 PM	▶ Replay	Mac OS X Chrome

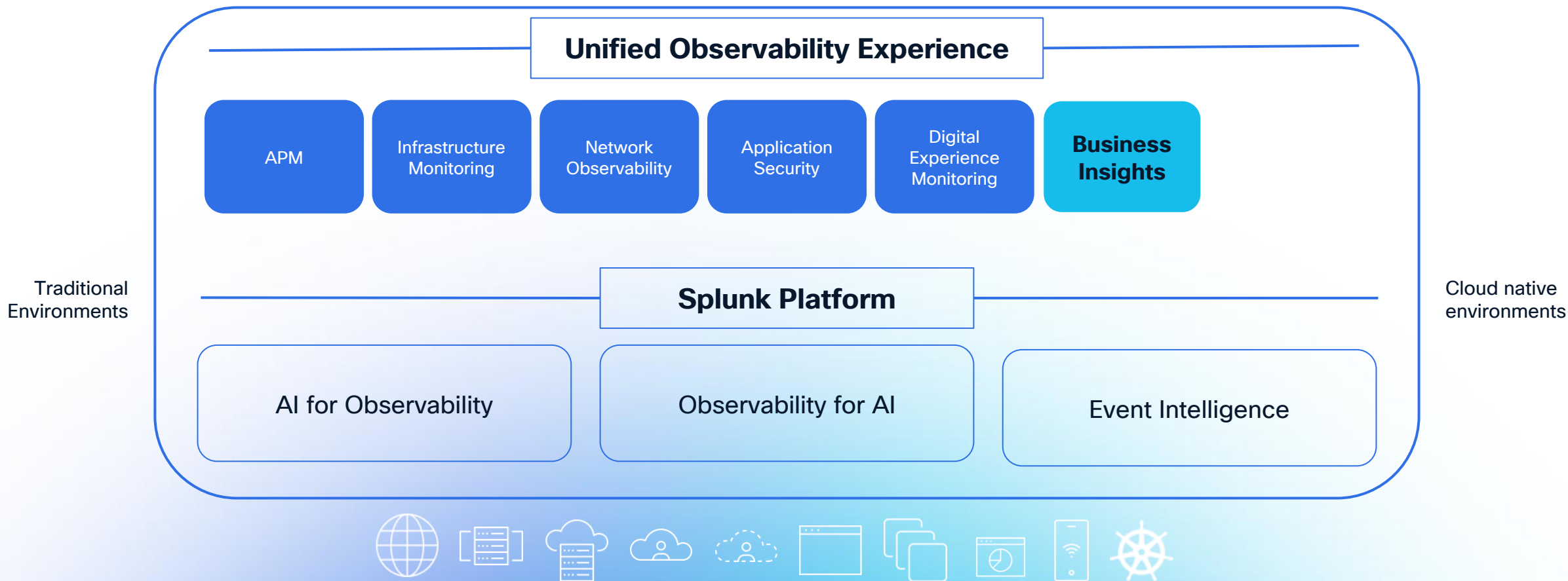
Use filtered sessions to replay and analyze significant drop-offs and determine their causes.



Demo Placeholder

Building your Observability Practice with Splunk

...business performance & insights



Contextualized data to understand your business

..digital business insights

- From executive dashboards to the line of code
- Curated journeys for critical business processes
- KPI-based monitoring to improve service health
- Track unlimited custom metrics without penalties
- Gain complete understanding across every environment
- AI-powered detection & investigation of business impacting issues



Business Service Intelligence

KPI-driven, predictive analytics solution for digital services

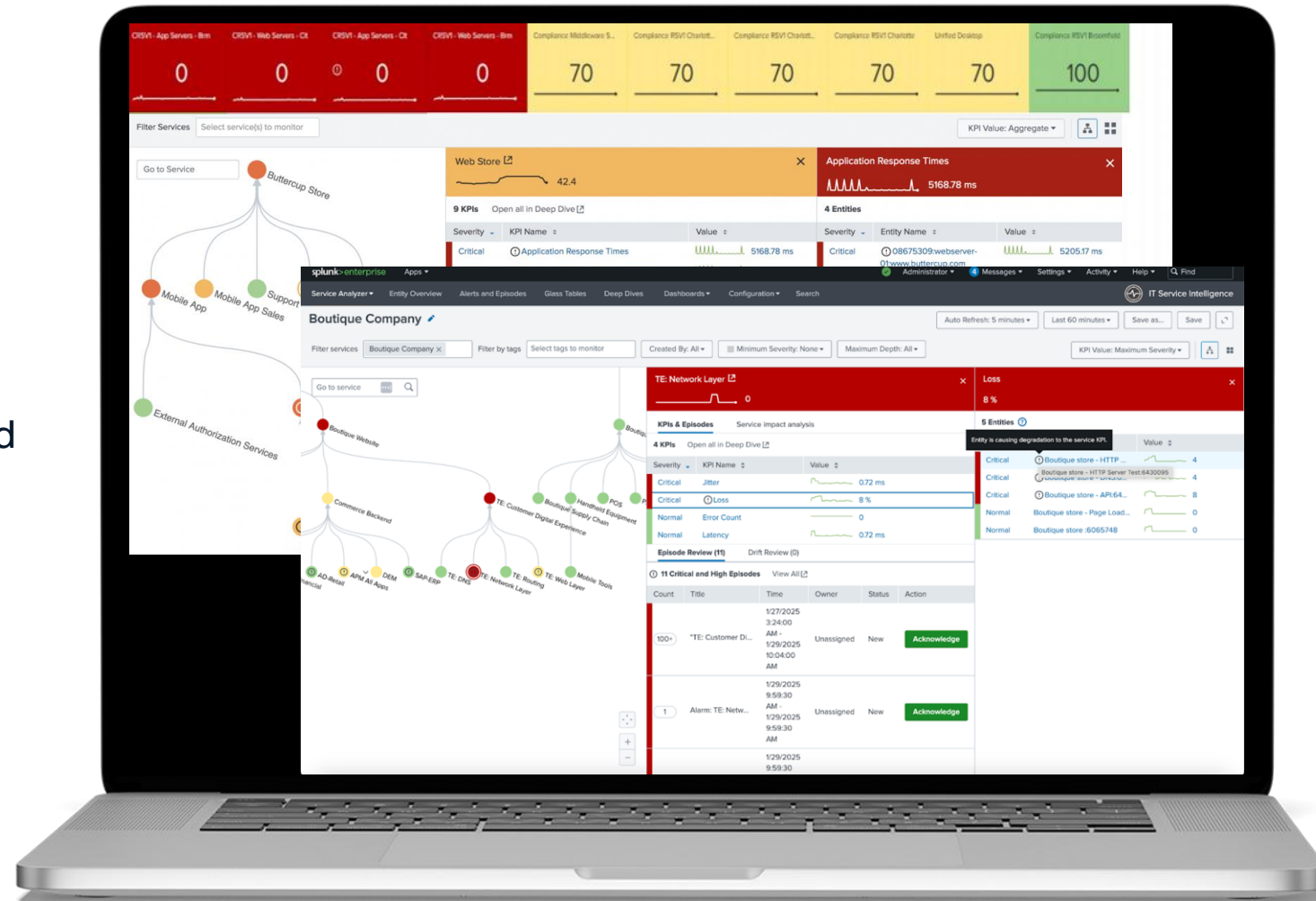
- Complete business visibility
- Intelligent incident management
- Machine learning & predictive analytics



Complete Business Visibility

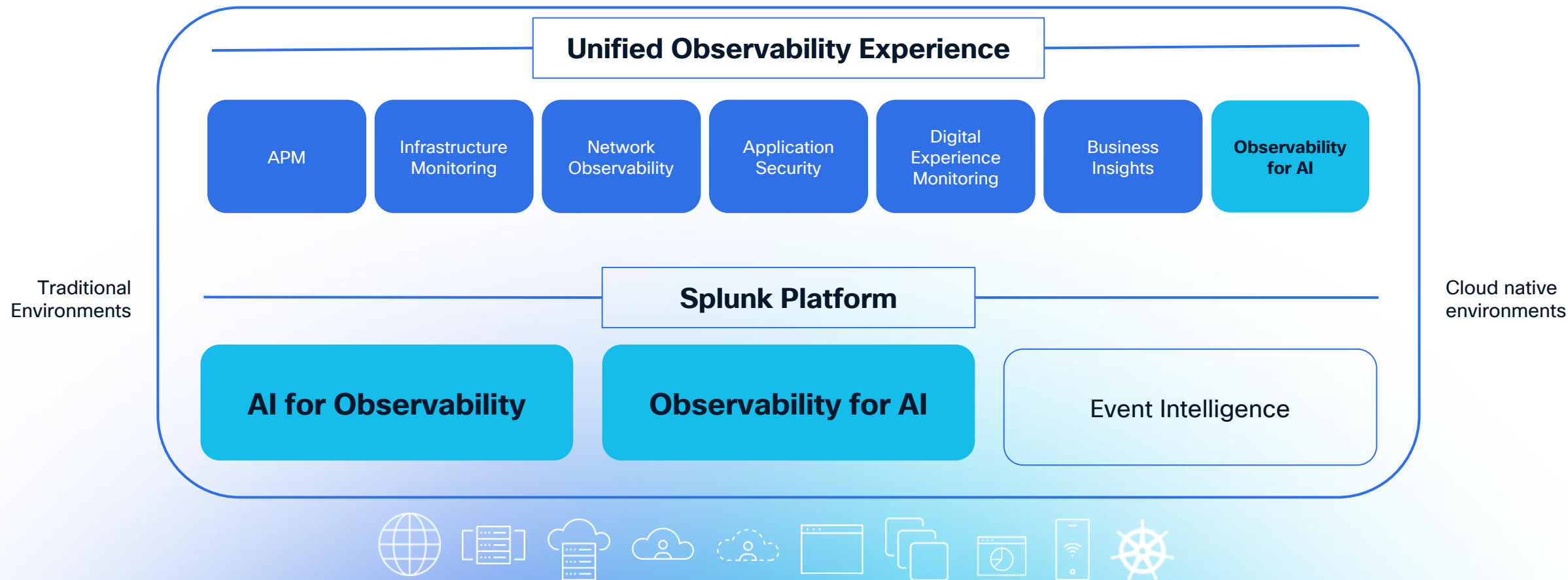
- Protect business performance, monitor service health, and drill down into underlying infrastructure, all from one dashboard
- Identify a problem, isolate domain, understand impact radius, accelerate root cause analysis

“Is the end user experiencing slow application page load due to network latency or a code issue?”



Building your Observability Practice with Splunk

Embedded AI|ML & AIOps



AI is rewriting the rules

**Apps can now be written
with little human
involvement**

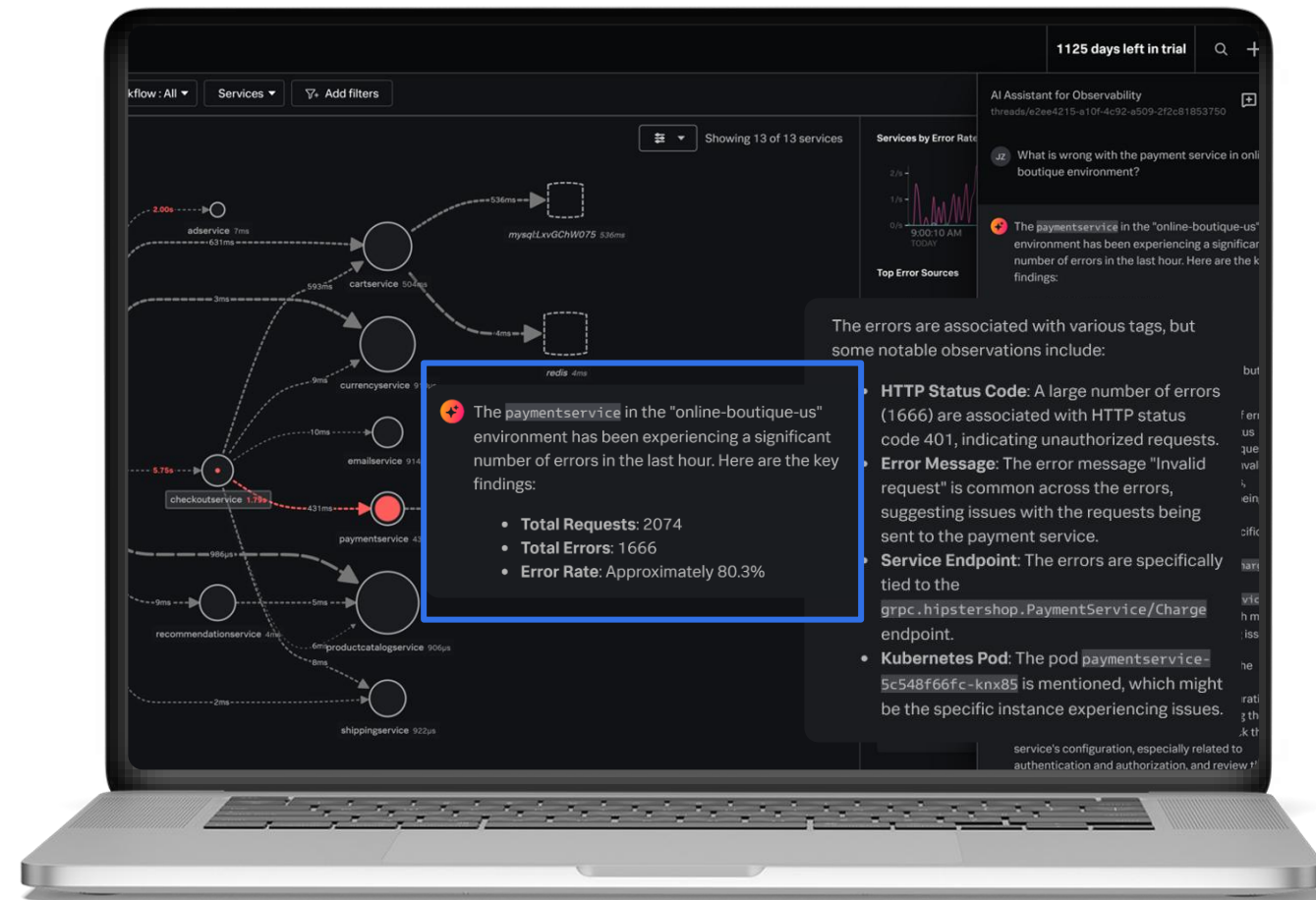
**AI agents perform basic
troubleshooting and
fixes autonomously**

**AI apps require
new forms
of telemetry**

AI Assistant in Observability Cloud

Find and fix issues faster using natural language.

- Surface key insights by chatting with your data
- Accelerate investigations and day-to-day monitoring tasks
- Get context and support as you troubleshoot



Easily **extract insights** & accelerate investigations using **natural language**



Faster and simplified investigations to reduce downtime



AI insights across your stack for better decision making



Higher productivity and flattened learning curve

Observability AI has evolved... Again

Fix and prevent
with AI agents

Observe AI agents
and infrastructure

Unify observability
and show business
impact

Introducing agentic observability

...three key innovation areas



Unified observability that surfaces business impact

Instrument and monitor three-tier and microservices environments in one solution, with deeper business context.



Fix & prevent problems using AI agents

Agentic AI to assist setup, and detect, identify root causes and fix problems before they turn into business-impacting incidents.

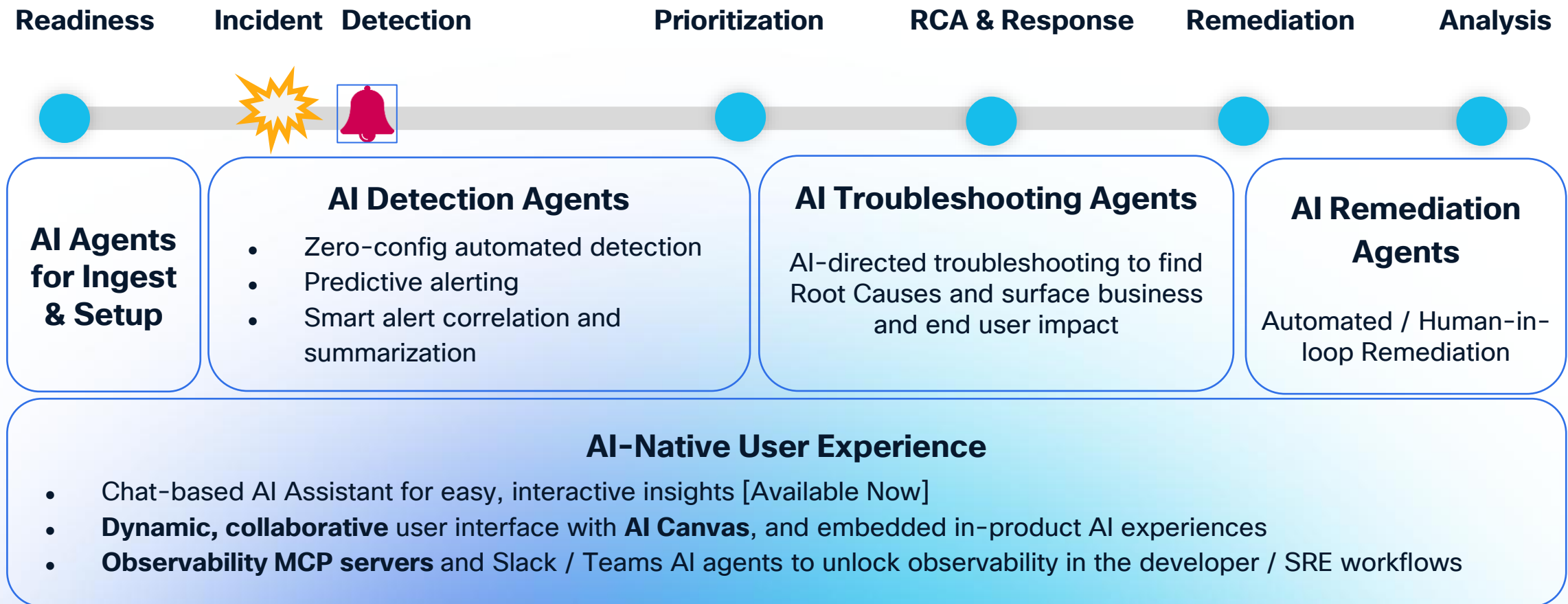


Observe AI agents & infrastructure

Monitor the health, performance, quality, and cost of the entire AI application stack, including agents, LLMs, and AI infrastructure.

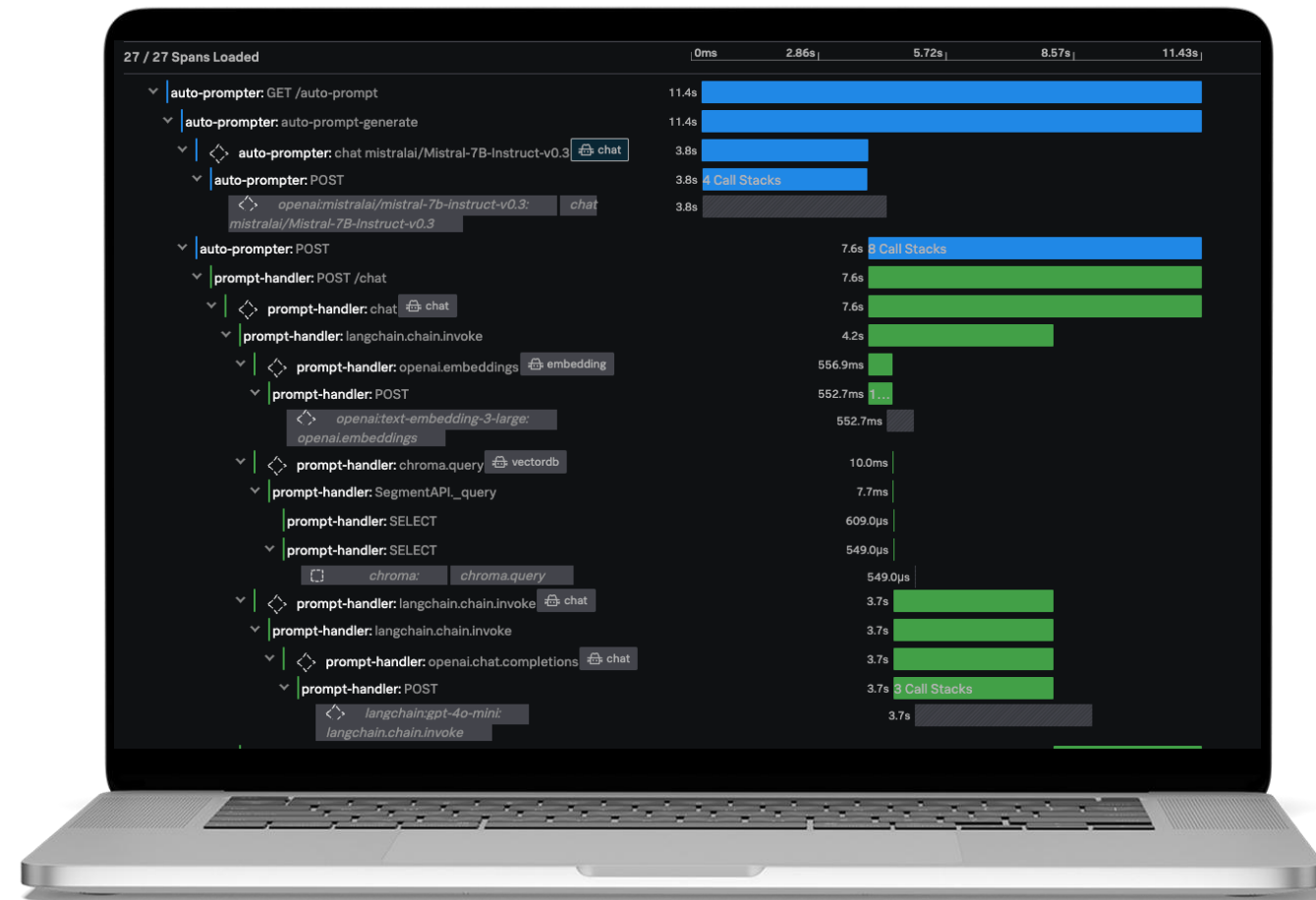
Minimize & prevent incidents with agentic AI

...agents deployed across every stage of the incident response lifecycle



Observe AI agents

Ensure the quality, accuracy, and security of **LLMs** and **agentic apps** to minimize bias, inaccuracies, hallucinations, and costs and performance risks

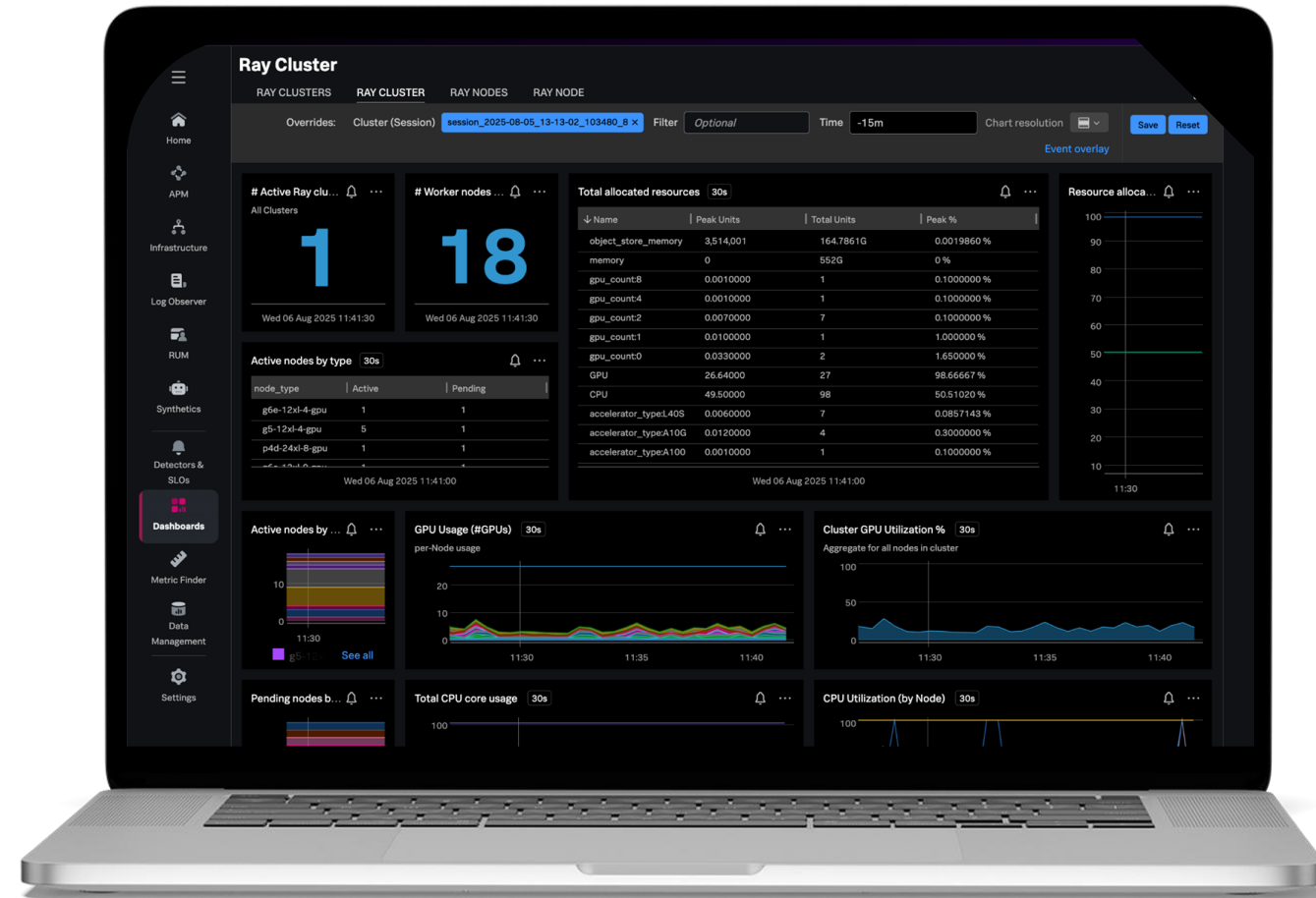


TRAVELPORT

PROGRESSIVE

Observe AI infrastructure

Monitor the health and consumption of **GPUs**, **vector databases**, **orchestration frameworks** & **agent platforms** to control costs & ensure reliability

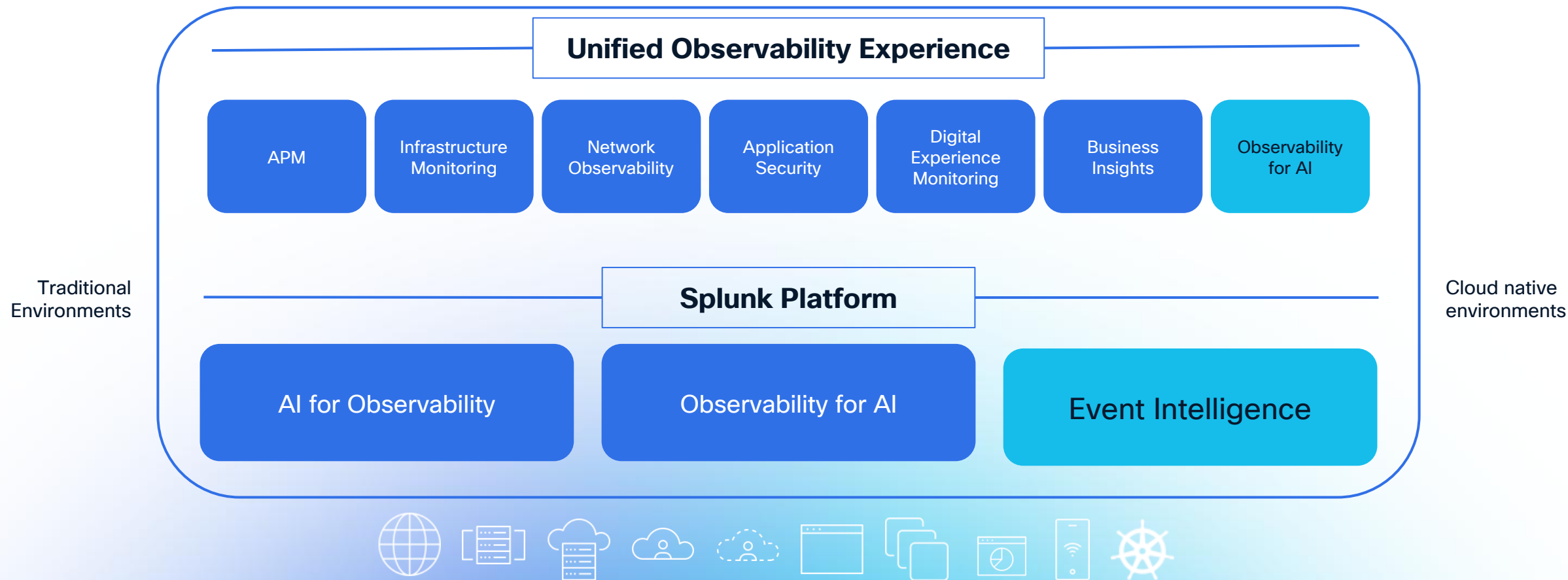


TRAVELPORT

PROGRESSIVE

Building your Observability Practice with Splunk

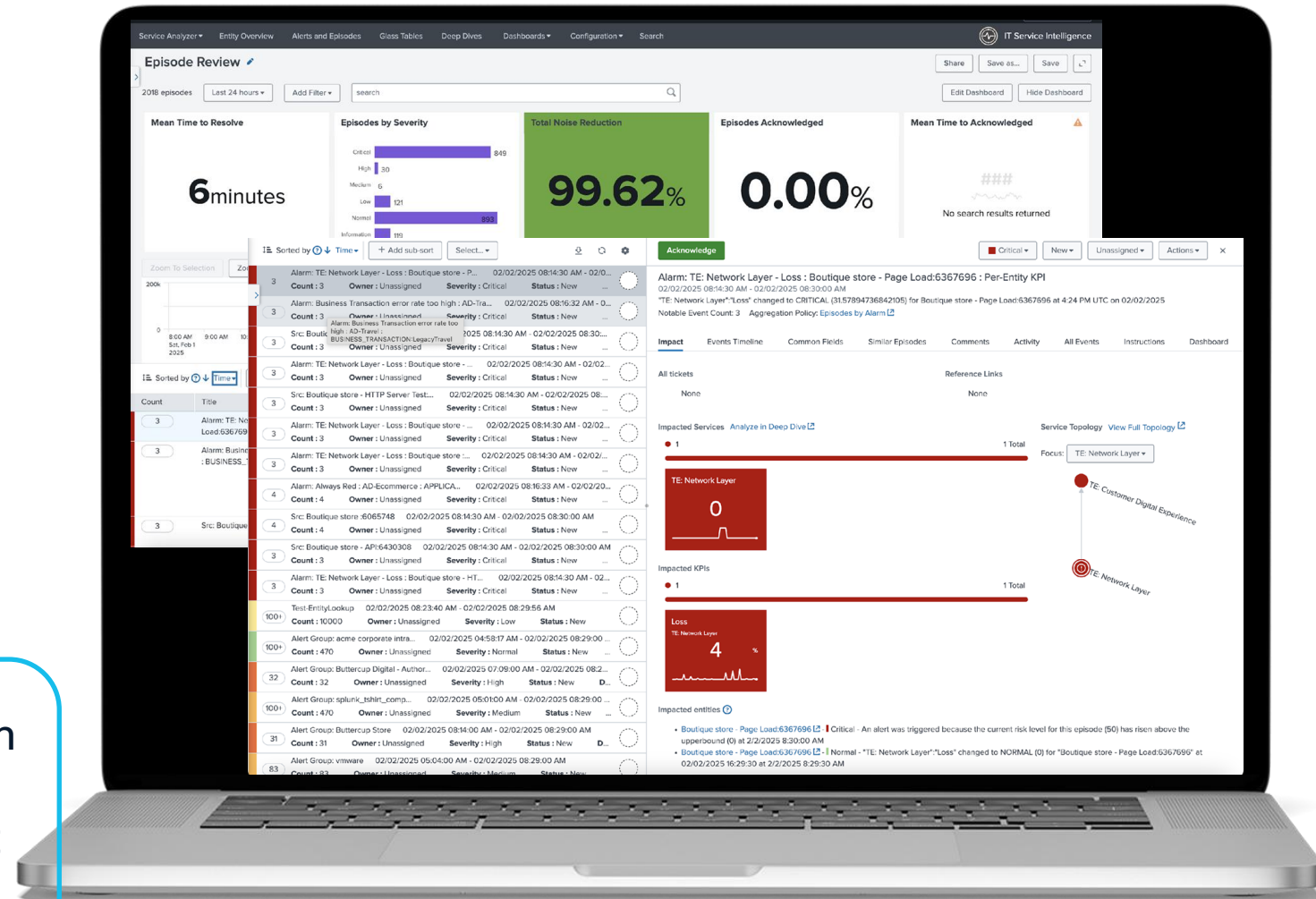
Embedded AI|ML & AIOps



Intelligent Incident Management

- Accelerate MTTR using real-time event correlation, automated incident prioritization, and integrations with IT service management (ITSM) tools
- Group related alerts from network devices, system infrastructure, & applications in cause-symptom relationship for a single actionable incident

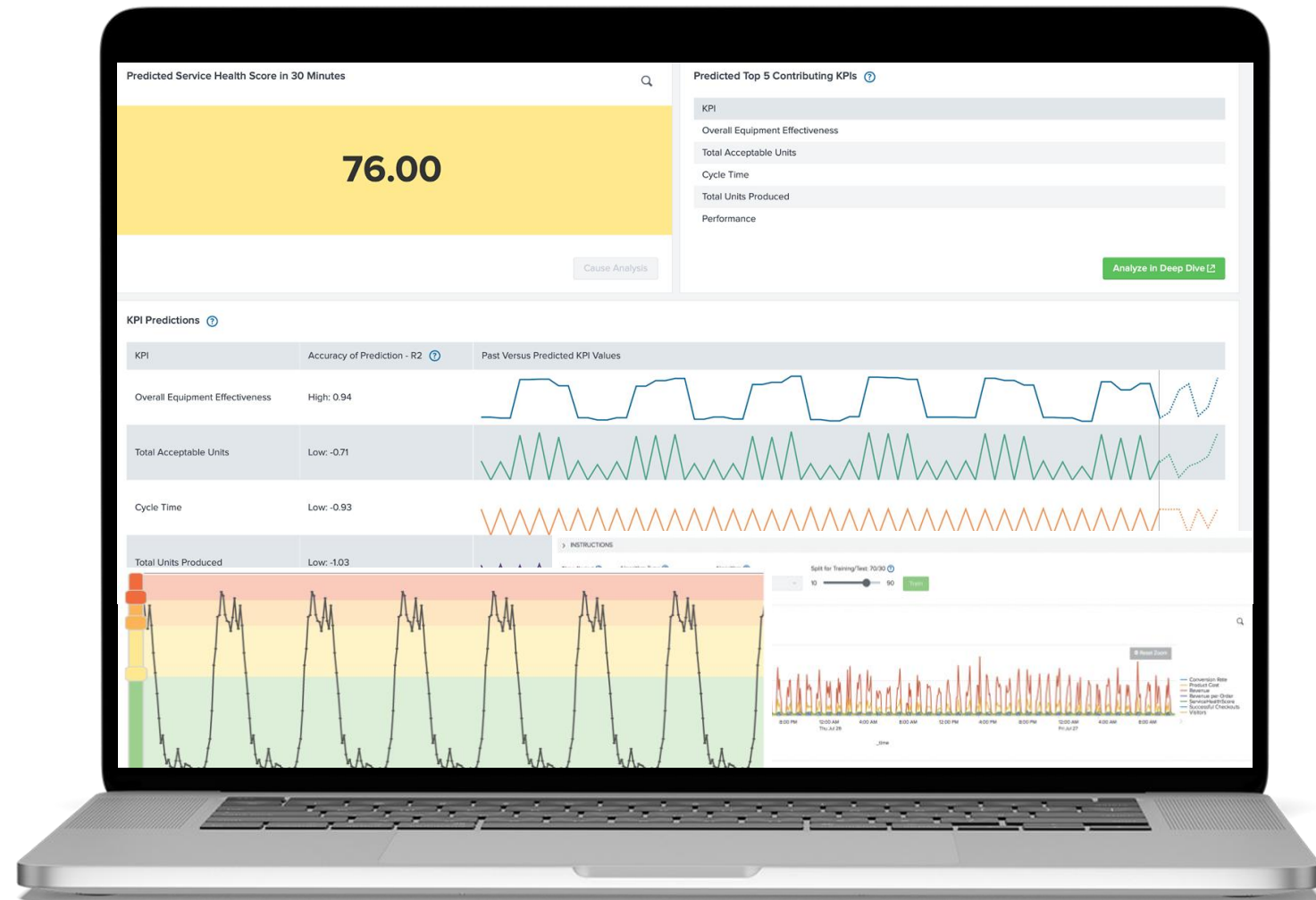
“Are all the alerts related to slow application response, database connection timeouts, page loading time related to packet loss at network layer?”



Predictive Incident Prevention

- Detect anomalies in KPI trends over time to identify a non-normal behavior using dynamic baselines
- Predict an incident 30 mins in advance via predictive service health analytics

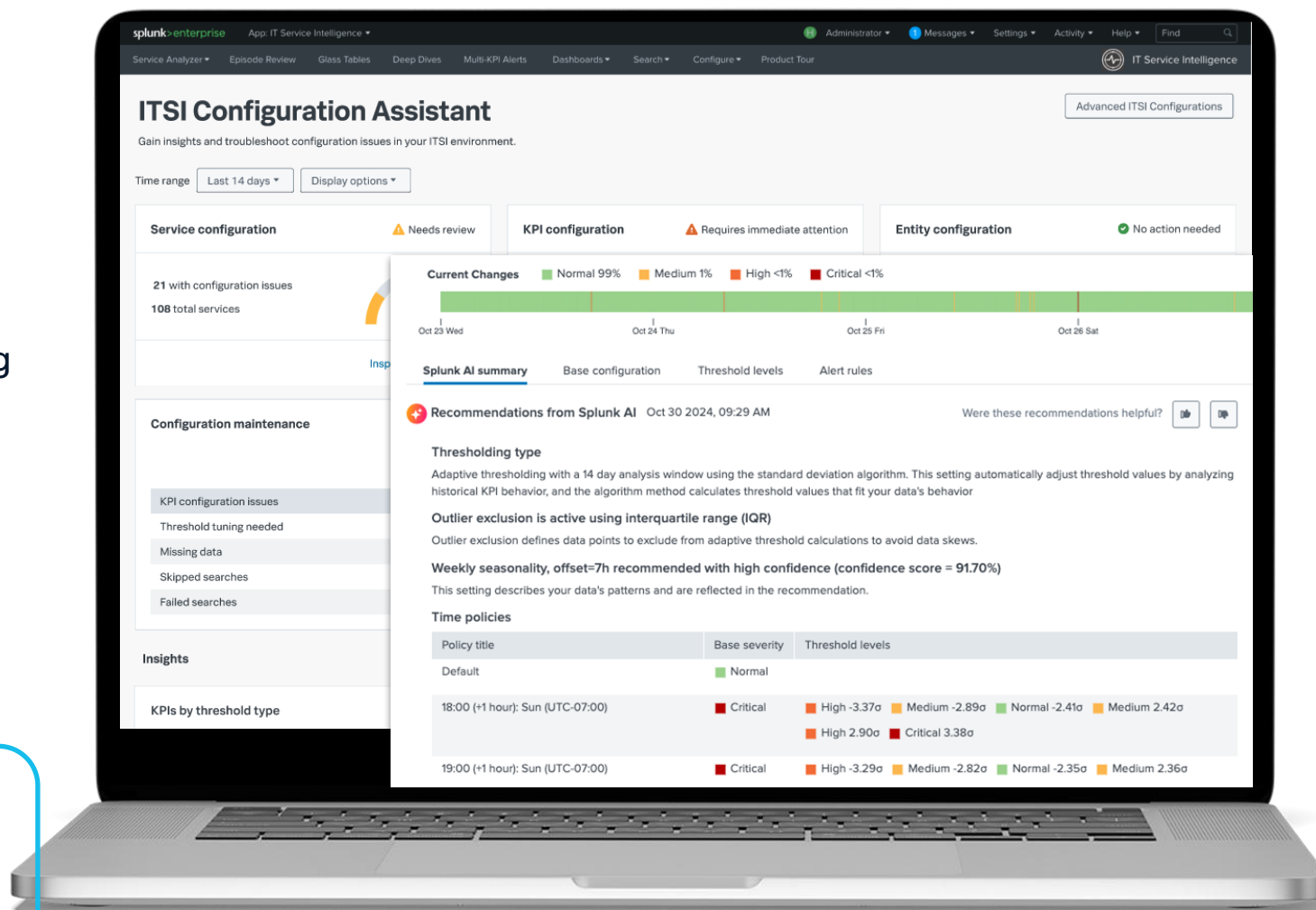
“Is there a possible outage about to happen in the data center given the downwards trend of network throughout?”



Prescriptive Guidance with AI/ML

- **ML-Assisted Thresholds** for OOTB guided approach to set up and identify anomalies on KPIs
- **Drift Detection** to proactively detect long trending anomalies as signals of performance degradation
- **Configuration Assistant** to signal when to optimize thresholds
- Ability to automate training and saving of ML-Assisted thresholds

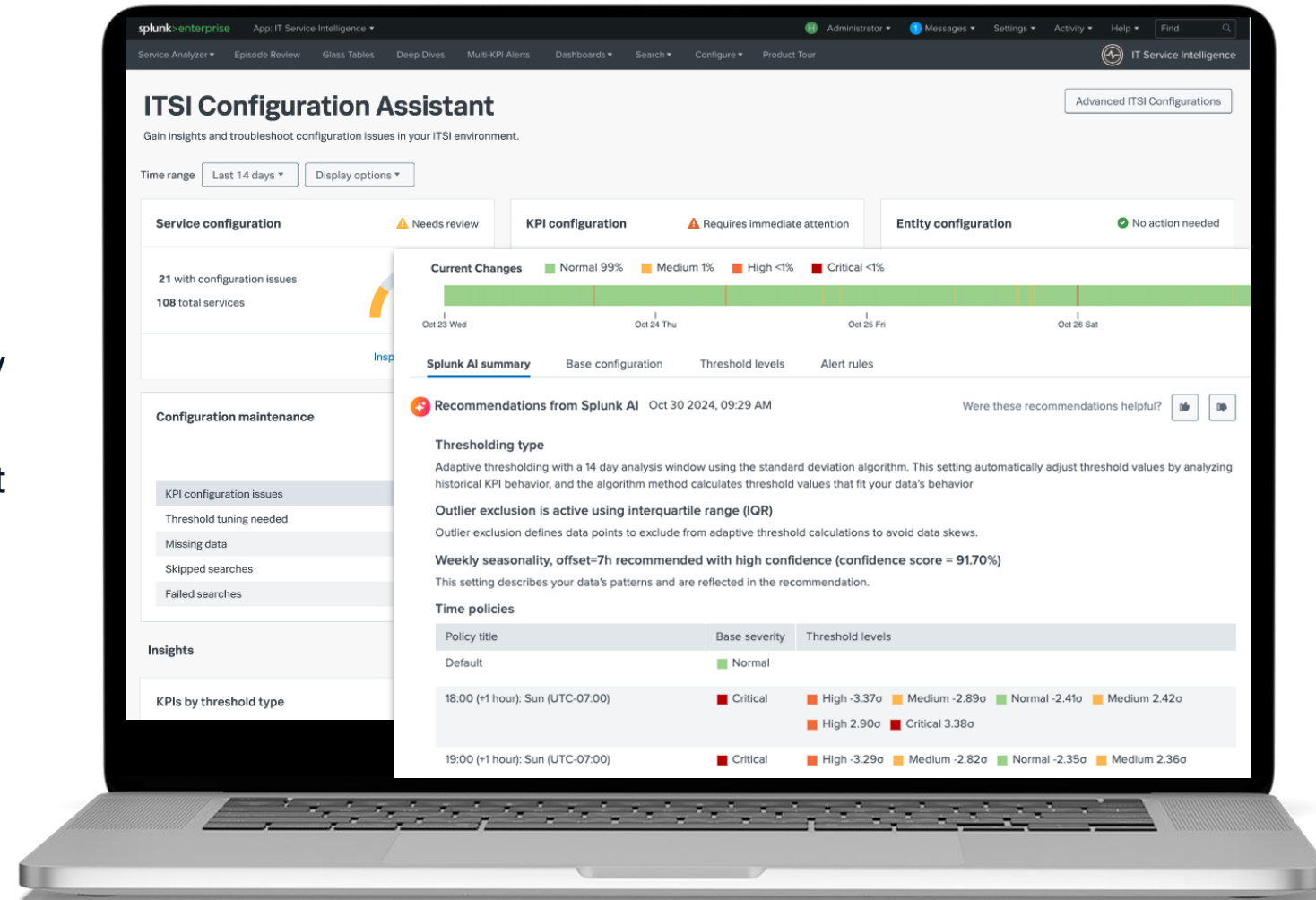
Recommendation based thresholds for network performance monitoring; proactive alerting for slow latency increase over a long period of time



End-to-end AI-driven Incident Management

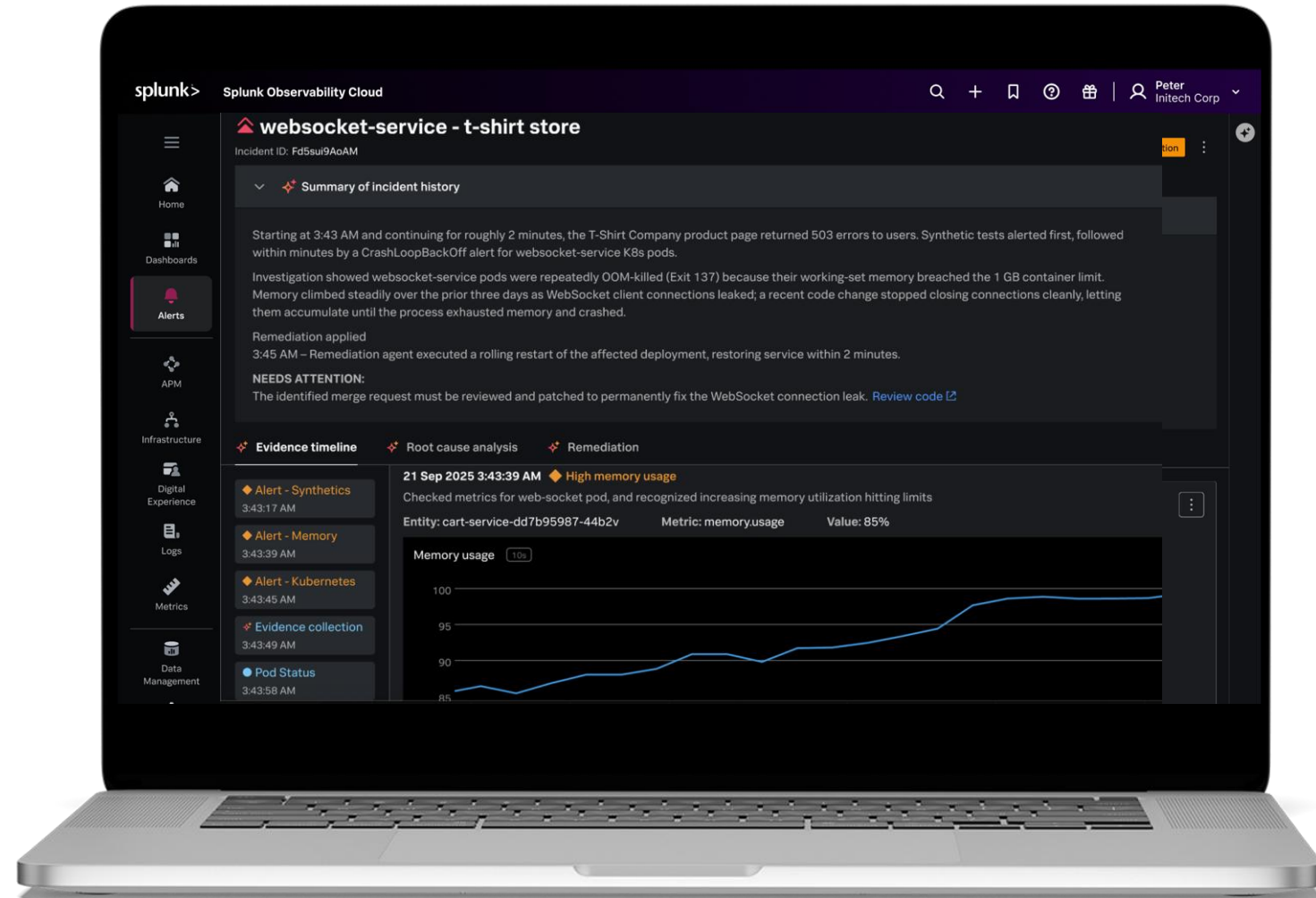
- Incident Creation – Event iQ correlates alerts into actionable episodes that update dynamically as the situation develops:
- Automated and tunable alert grouping policy generation incl. field prioritization
- Ability for extract important values from alert data with ML-based tagging

Automated alert grouping for domains across networks, infrastructure, and applications



Fix & prevent problems using AI agents

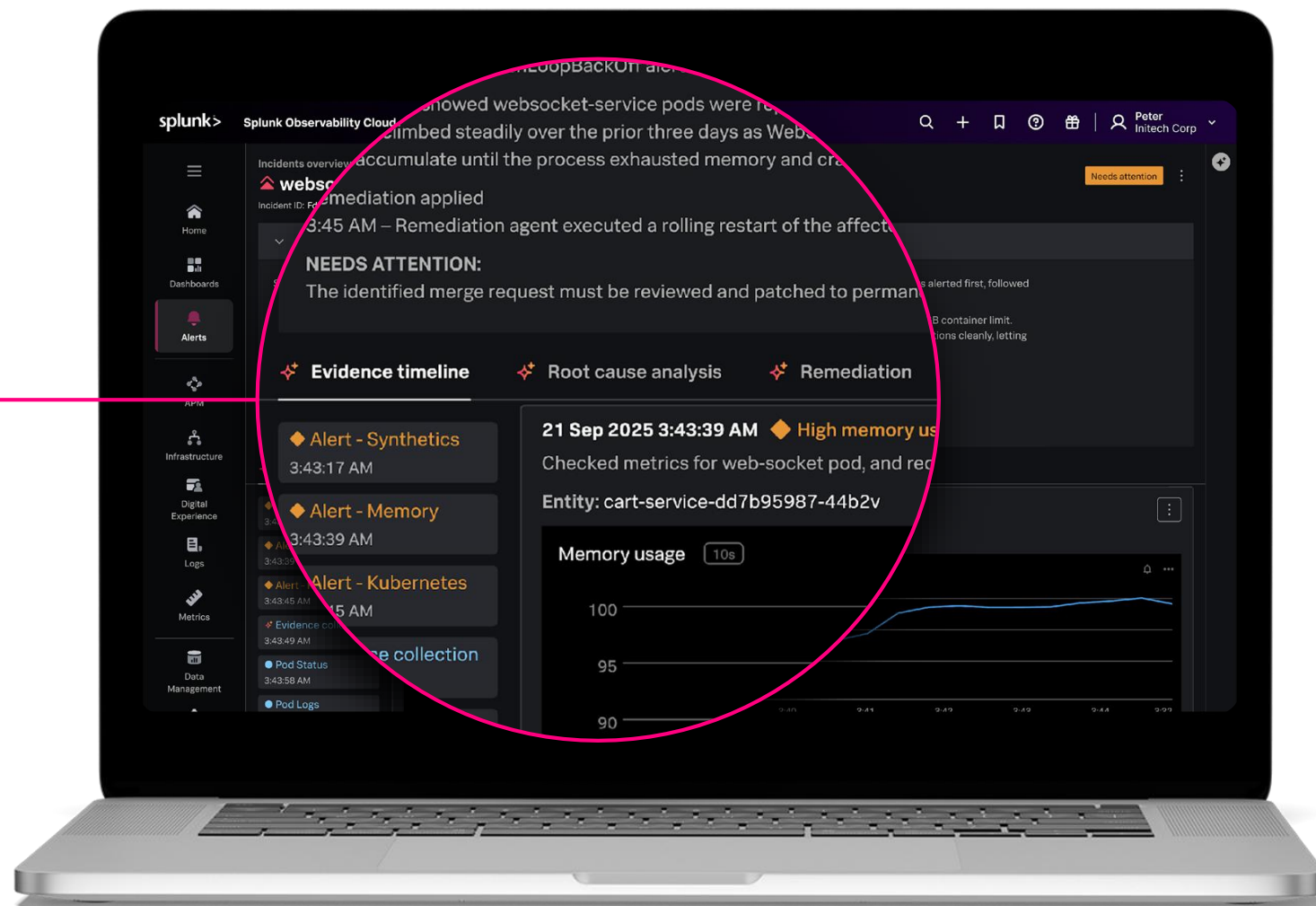
- AI-generated RCA in-context, to reduce MTTI
- AI-directed alert correlation and summarization to reduce alert noise
- AI agents to prevent problems by optimizing data collection and alert configuration
- AI agents to automate every stage of the incident response lifecycle

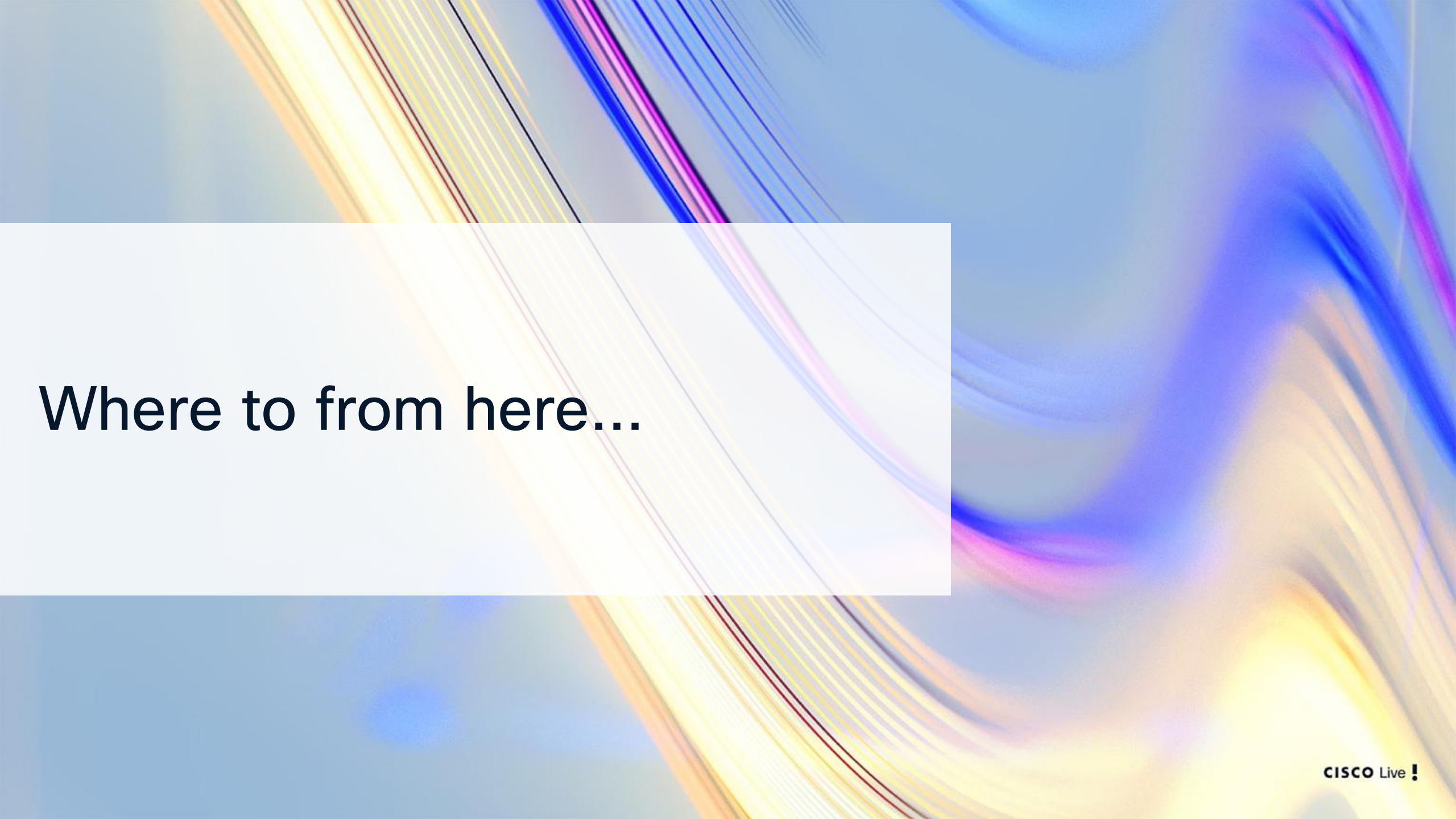


AI Troubleshooting Agents

Fix issues faster with
automated Root Cause
Analysis

Makes everyone an expert





Where to from here...

Top 5 things to start with

...quick Wins (Easy Wins to Build Momentum)

Identify High-Impact Use Case

- Tie it to real business impact (e.g. cart conversion, check-in failures)

Instrument Golden Signals

- Latency, Traffic, Errors, Saturation – start with one critical service

Centralize Dashboards

- Bring in key metrics (infra + app + network) into a single pane of glass

Create an Incident Playbook

- Define roles, escalation, and response steps for one high-priority incident type

Host a Blameless Postmortem

- Use observability data to show what happened & capture lessons learned

“Embrace a life of curiosity & never stop learning”

Complete your session evaluations



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



Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live Events app.

Continue your education



Visit the Cisco Stand 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 www.CiscoLive.com/on-demand

Thank you

CISCO Live !

