

Assure Digital Resilience Across Every Network

See, understand, and improve connected
experiences everywhere

Martin Kowalewski
Solution Engineer

February 5, 2026



Digitization Disrupts IT: Adapting to a New Reality

90%

of Board of Directors
see digital as an
integral part of
business strategies

80%

of CxOs consider
digital leadership
as part of their job

>50%

of Infrastructure and Operations
budget will be spent on unowned
technology by 2025

70%

of publicly reported
outages caused by
3rd party operators

Sources:

Gartner



IHS Markit

AI is increasing the pressures on performance assurance



Drowning in Data and Alerts

170,000+ alerts every hour, with expected 3x growth in AI



Speed is the Breaking Point

<50 millisecond latency needed for AI-agents

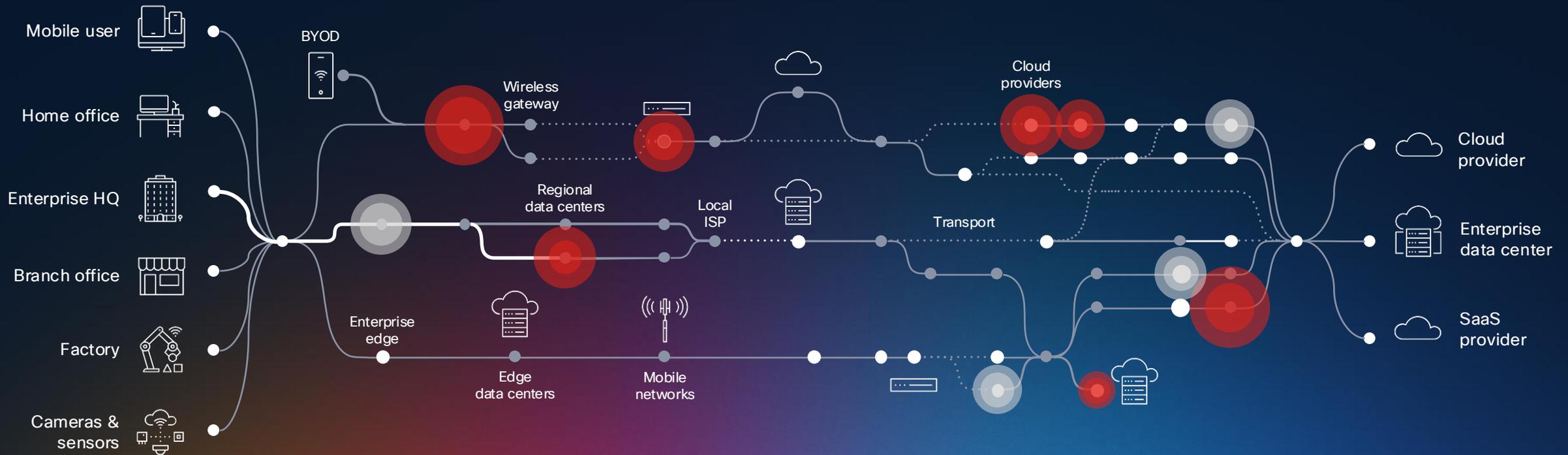


The Talent Gap Is Widening

64% of organizations will face IT skills shortage by 2026

Impacting brand, revenue and customer experience

Digital experiences span owned and unowned networks



Silos of people, tools and data increase complexity | AI-powered workflows introduce new demands



**Traditional operations
can't keep up**



From reactive troubleshooting to proactive operations



Baseline and Detect

Monitor end-to-end digital experience from critical vantage points



Localize and Diagnose

Visualize, localize, and diagnose across every network segment



Mitigate and Remediate

Closed-loop actions across digital domains and teams



Predict and Optimize

Forecast disruptions, optimize path, and plan connectivity and migrations



Assurance

Reactive monitoring

Cisco ThousandEyes Platform

Experience & Service Assurance



Digital experience

End user | Mobile
IIoT | VoIP



Proactive monitoring

Web | Network
BGP | DNS



Global visibility

On-Prem | Cisco
3rd party



Domain insights

Traffic | WAN
Internet | Cloud

AI-Powered Platform

Automation | Integrations | APIs



Path
visualization



Cross-layer
correlation



Anomaly detection &
alerting



Event summarization



Predictive
recommendations



Natural language
query

Eyes Everywhere

CLOUD AGENT



- 400+ ThousandEyes maintained POPs
- Global scale
- T1/2 DCs, Cloud and Broadband providers
- Outside-in visibility
- Public facing sites and APIs
- Customer experience

ENTERPRISE AGENT

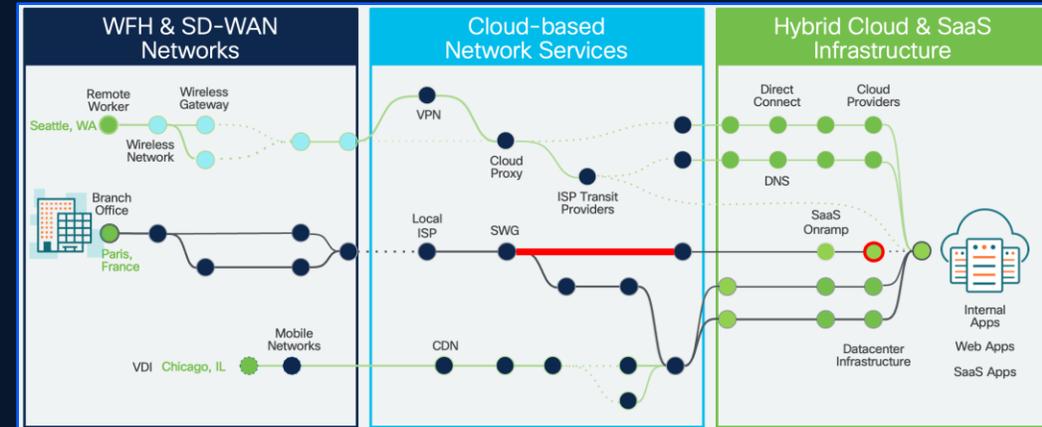
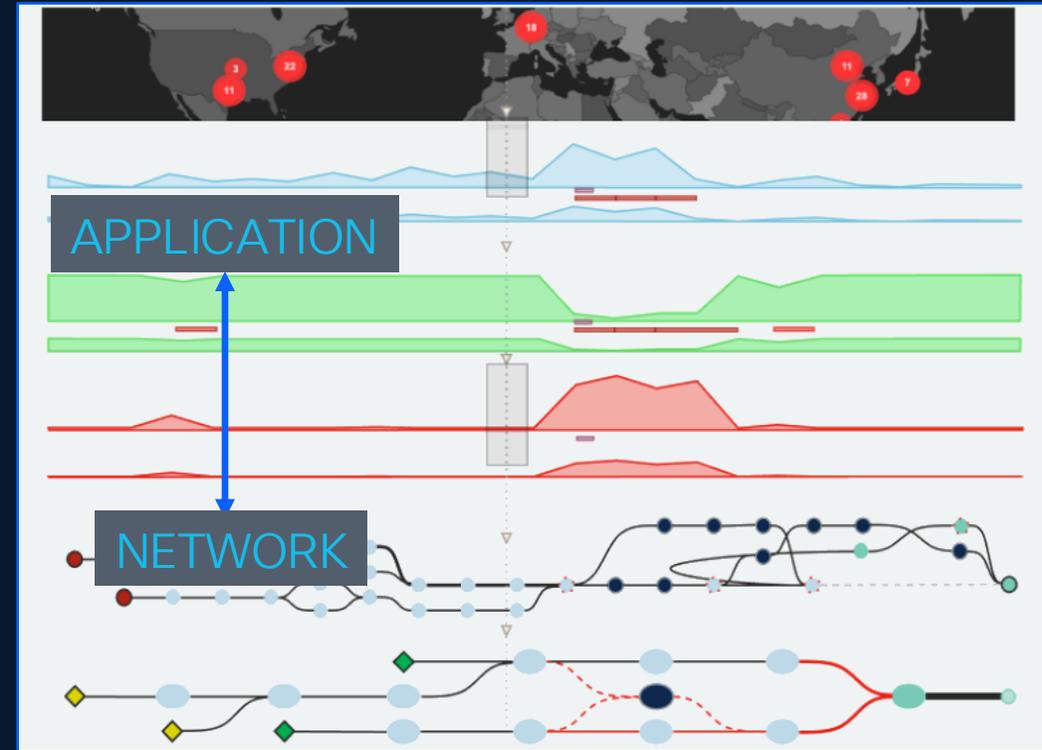


- Deployed in YOUR environment
- DCs, sites, offices, branches, stores...
- VMs, Servers, Containers, Cisco HW
- Inside-out, inside-inside
- Internal apps, SaaS, network
- Employee / network experience

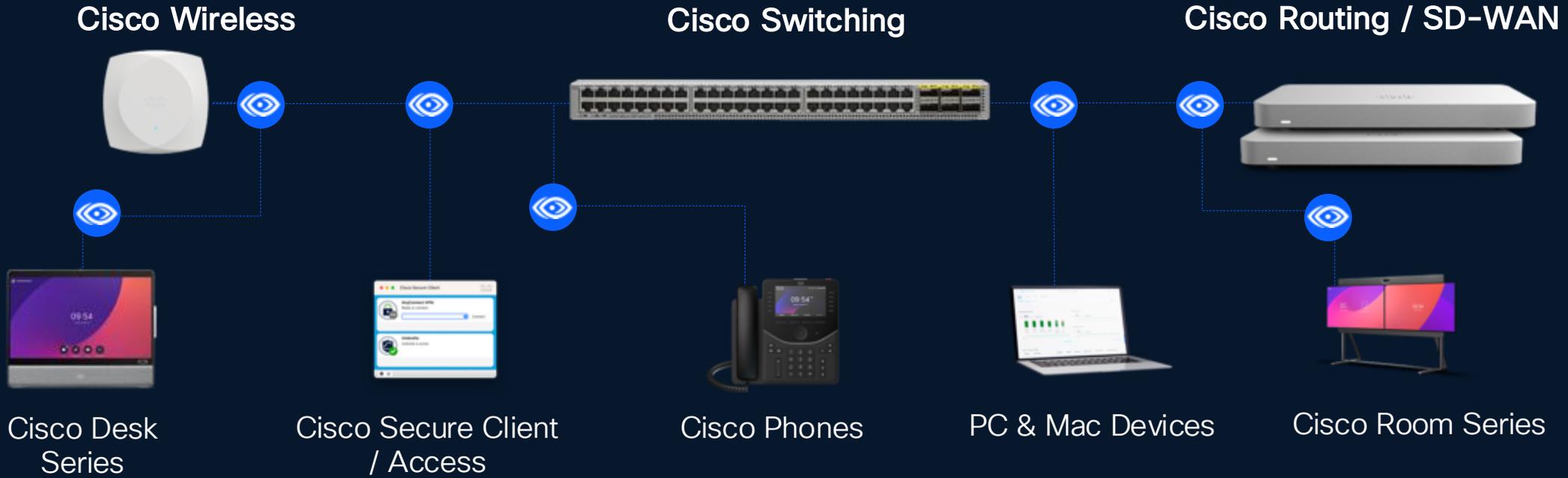
ENDPOINT AGENT



- Deployed on your employees' devices
- Home, office, anywhere...
- Laptops, RoomOS, Secure Access, Mobile
- Last mile visibility
- Internal/external apps, SaaS, network
- Wi-fi, VPN, ISP, any app



With Cisco, Assurance Is Built-In



AI-driven Intelligence + **splunk** > integration
a CISCO company

In Action

VISUALIZE

Application and service degradation immediately. Quickly identify the scope of the degradation.

UNDERSTAND

The fault domain instantly (i.e. Application vs. Network). Correlated hop by hop network performance across any network.

ACT

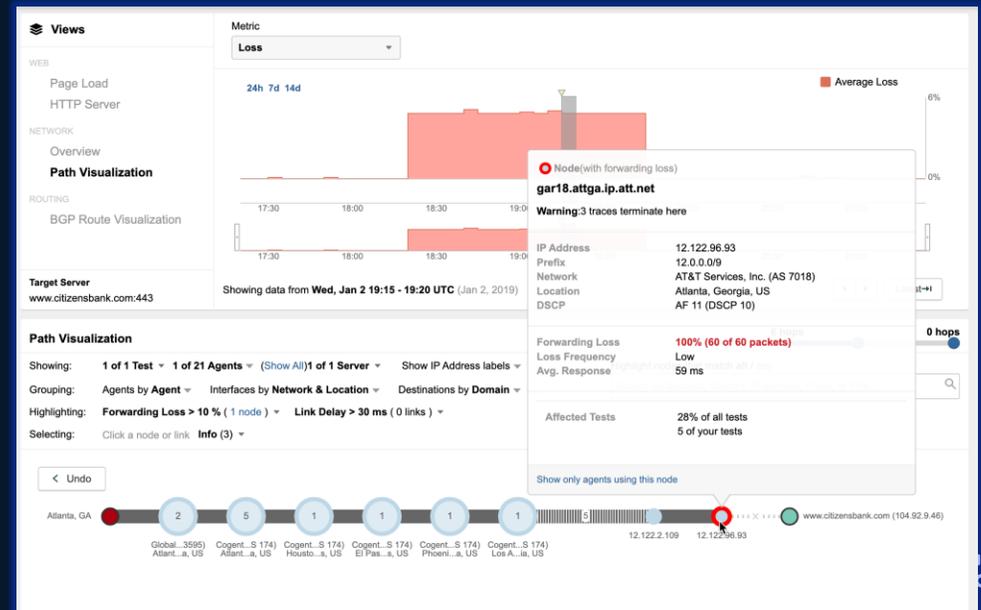
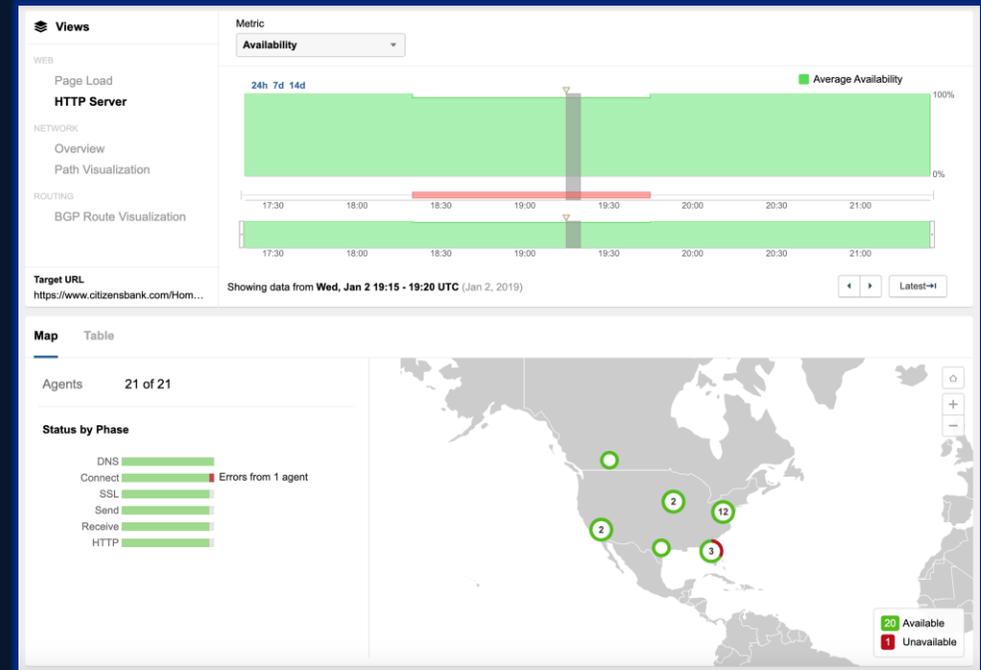
Quickly and easily share data with internal teams, or external providers to improved MTTR

Critical business service is unavailable for >90 minutes in ONE region of the US

Quickly identify impacted regions, and the suspected fault domain (network)

Correlated network packet loss to service disruption, pinpoint exactly where it's coming from.

Share data with external providers to accelerate time to remediation.



Cisco AI Assistant Integrated into ThousandEyes



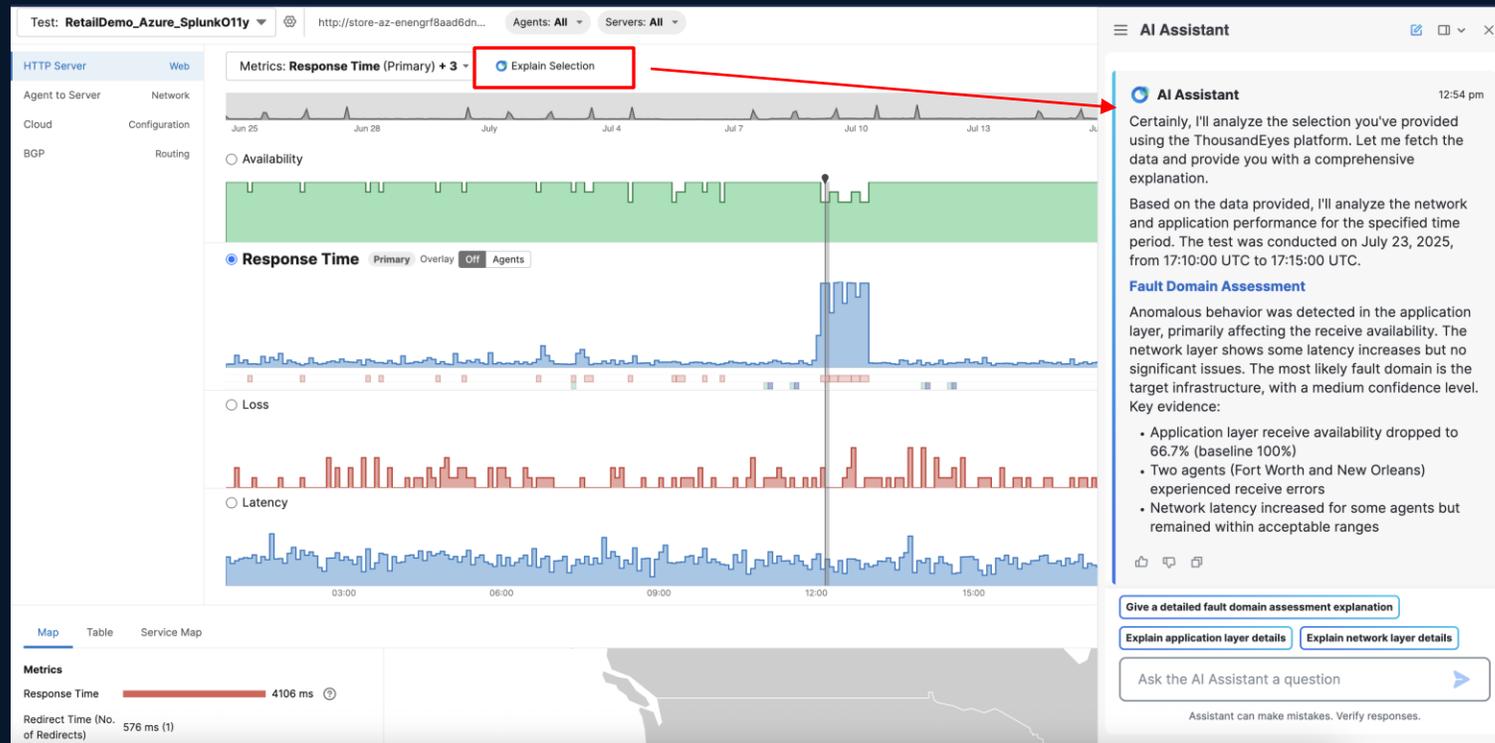
Unlock Assurance for all with everyday language empowering any user to operate like an expert



Instant explanations and guided troubleshooting, accelerate root cause analysis and resolution



Predict and minimize the impact of operational issues before they affect user experiences



ThousandEyes MCP Server (Released 1/30/26)

The Why

- AI assistants are increasingly being adopted as a troubleshooting interface for technical teams - integrating ThousandEyes data directly into these workflows reduces incident response time by simplifying access beyond the UI and APIs.
- The MCP Server solves this problem, meeting customers where they are, and making ThousandEyes data available directly within their AI assistants and agents.

The Value

- Conversational, AI-driven access to ThousandEyes data without context-switching.
- Aims to reduce Mean Time To Identification and Mean Time To Resolution by replacing manual navigation/correlation with natural language queries.
- The MCP server exposes ThousandEyes data using the standard MCP protocol, reducing integration complexity for MCP-compliant AI assistants like Claude

Sample Prompts

Q: Do I have any active alerts?

Are there any alerts active or cleared over the last 24 hours

Retrieving ThousandEyes alerts from past twenty-four hours >

I'll check for both active and cleared alerts over the last 24 hours for you.

Synthesized alert data and converted timestamps for clarity >

Based on my check of the last 24 hours, here's what I found:

Active Alerts: None currently active

Cleared Alerts: 1 alert cleared in the last 24 hours

Cleared Alert Details:

- **Test:** RetailDemo_AWS_SplunkO11y (HTTP Server test)
- **Alert Rule:** Response Time - Wait Time
- **Severity:** INFO
- **Condition:** Wait Time exceeded Medium sensitivity threshold and was \geq 1,500 ms
- **Duration:** 35 minutes (started Feb 4 at 11:05 PM, cleared at 11:40 PM)
- **Violation Count:** 3 violations during the alert period

The good news is there are no active alerts right now. The one cleared alert was a moderate response time issue on your RetailDemo AWS/Splunk O11y HTTP test that resolved itself after about 35 minutes yesterday evening.

Q: Please investigate the RetailDemo_AWS_SplunkO11y alert further??

Alert Summary

Target: <https://store.retailonlinestore.net/api/sales/summary/simappissue>

Duration: 35 minutes (Feb 4, 11:05 PM - 11:40 PM UTC)

Severity: INFO (Medium sensitivity threshold)

Root Cause Analysis

What Happened

The alert was triggered by extremely high **Wait Time** (server response time) on three specific agents:

Affected Agents (all AT&T West Coast):

- **Los Angeles, CA (AT&T):** 4,652.7ms wait time (normal: ~125ms) - **37x increase**
- **San Jose, CA (AT&T):** 4,177.5ms wait time (normal: ~136ms) - **31x increase**
- **Seattle, WA (AT&T):** 4,212.3ms wait time (normal: ~148ms) - **28x increase**

Key Findings

1. **Carrier-Specific Impact:** Only AT&T agents were affected. All other monitoring locations (Comcast, Verizon, Charter, Cox - 10 other agents) maintained normal response times throughout the incident.
2. **Geographic Pattern:** The issue only impacted AT&T's **West Coast** network. Other AT&T agents in Dallas, Chicago, New York and Ashburn showed no degradation.
3. **Network Layer Was Fine:** Network latency remained excellent (<1ms from affected agents), with no packet loss or connection issues detected. This rules out network-level

Q: Please provide a root cause analysis document for this issue?

Root Cause Analysis

RetailDemo AWS SplunkO11y Alert Investigation

February 5, 2026

Executive Summary

On February 4, 2026, an INFO-level alert was triggered on the RetailDemo_AWS_SplunkO11y HTTP Server test due to significantly elevated server response times (Wait Time) from AT&T network locations on the West Coast. The incident lasted 35 minutes and self-resolved without intervention. The issue was isolated to three specific monitoring agents in California and Washington, while all other monitoring locations maintained normal performance.

Incident Overview

Alert ID	661ac681-d381-4f76-b6be-bfb94372168f
Test Name	RetailDemo_AWS_SplunkO11y
Test Type	HTTP Server
Target URL	https://store.retailonlinestore.net/api/sales/summary/simappissue
Severity	INFO
Start Time	February 4, 2026 23:05:00 UTC
End Time	February 4, 2026 23:40:00 UTC
Duration	35 minutes
Alert Condition	Wait Time outside Medium sensitivity threshold AND Wait Time \geq 1,500 ms

Detailed Analysis

Affected Monitoring Agents

Three AT&T monitoring locations on the West Coast experienced severe performance degradation during the alert period:

Agent Location	Peak Wait Time	Normal Wait Time	Impact
Los Angeles, CA (AT&T)	4,652.7 ms	125.9 ms	37x

ThousandEyes Use Cases

Use Case

Value

Who (Teams)

What

1

EMPLOYEE DIGITAL EXPERIENCE



- Identify and fix end user problems faster, down to last mile
- Improved productivity
- Better WFH Experience

- Workforce Experience, Enduser Compute, Collaboration, Call Center
- HelpDesk, Operations, Monitoring

- WiFi
- VPN
- App monitoring
- Employee Last Mile

2

CLOUD/SAAS



- Visibility into infra you don't control
- Quickly identify WHERE problems are and the impact
- Ability to escalate with evidence for improved MTTR

- SaaS app owners
- Cloud infrastructure owners
- App teams with Hybrid apps
- HelpDesk, Operations, Monitoring

- Webex/MS Teams/Zoom
- MS O365
- Workday/SFDC/SAP
- AWS/Azure/GCP

3

ENTERPRISE NETWORK



- Visualize real-time/historical network paths for traditional and SDWAN networks (overlay/underlay)
- Correlated loss, latency and jitter with path and BGP change
- Hold ISPs and vendors accountable

- Network Operations/Engineering
- HelpDesk, Operations, Monitoring
- GNOC, NOC, GIS, Security

- Campus Branch WAN
- SDWAN/SASE
- ISP Health
- Hybrid Cloud
- Proxies and Internal Apps

4

CUSTOMER DIGITAL EXPERIENCE



- Quickly determine fault domain (app/network) when performance or availability problems happen
- Understand what impact external networks have on your end users
- Measure end user experience consistently from multiple locations

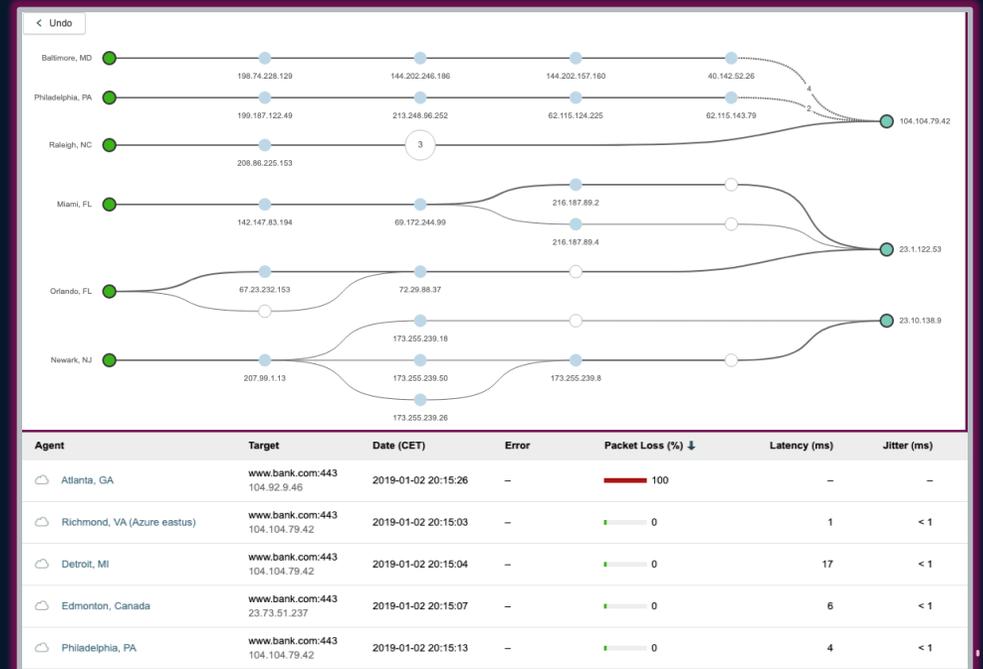
- Application Operations/Dev/Owners
- HelpDesk, Operations, Monitoring

- Customer facing apps
- APIs and 3rd Party Monitoring
- CDN
- BGP and DNS

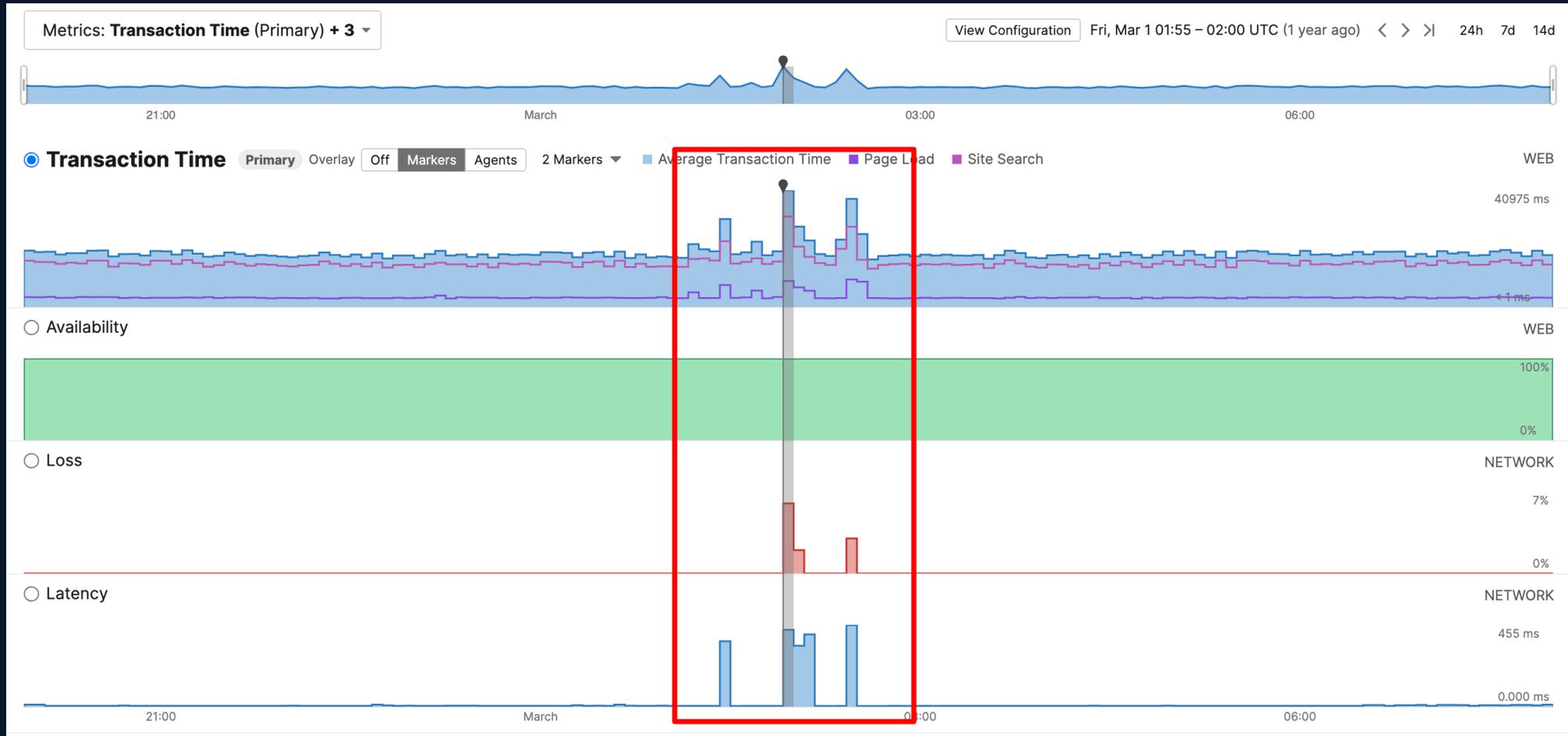
Customer Digital Experience with Splunk Synergies

ThousandEyes for CDX

- Synthetic application transaction tests (24/7)
- Easy to use and deploy (zero instrumentation, recorder)
- Hundreds of external points of presence
- Correlated network path visibility
- CDN, API, Cloud and external dependency visibility
- DNS/BGP Visibility and Correlation



ThousandEyes for CDX



A customer's primary revenue generating app was sporadically have slow downs. A ThousandEyes multi-step transaction test caught this and was able to correlate the increase in transaction time to network latency.

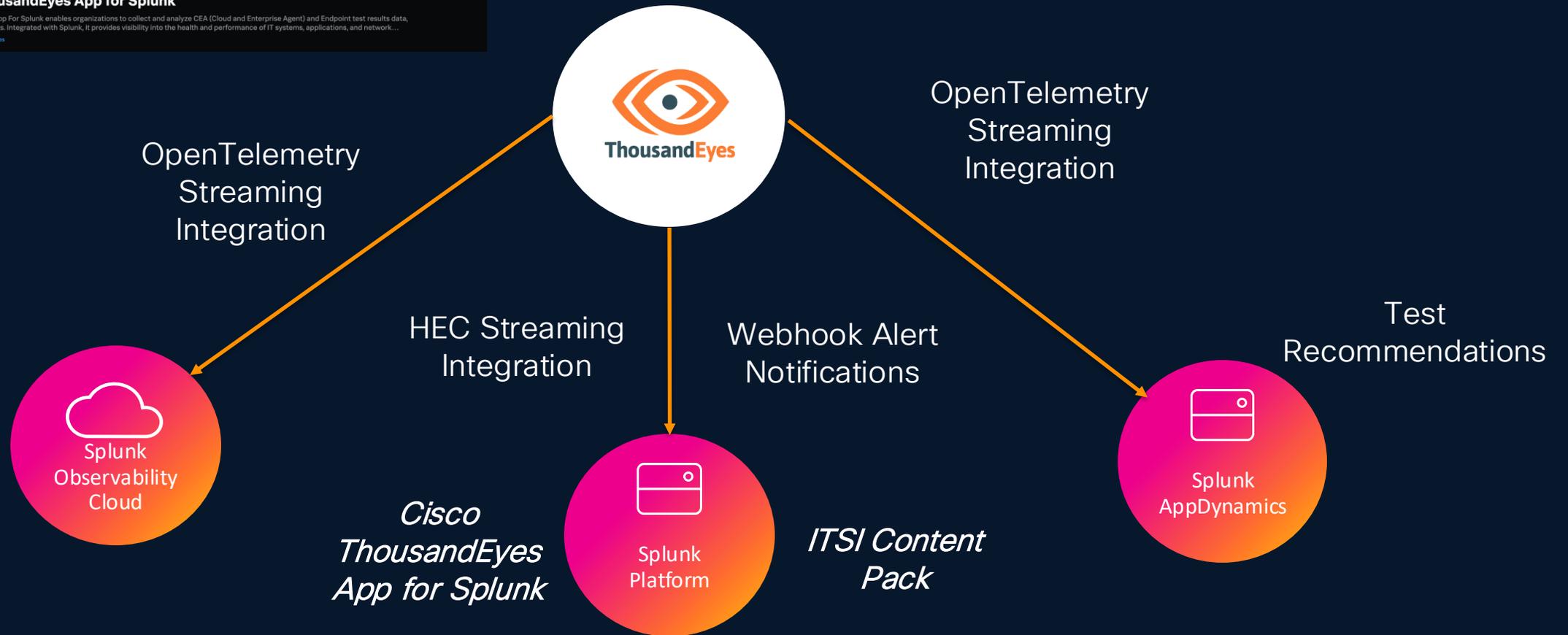
ThousandEyes for CDX



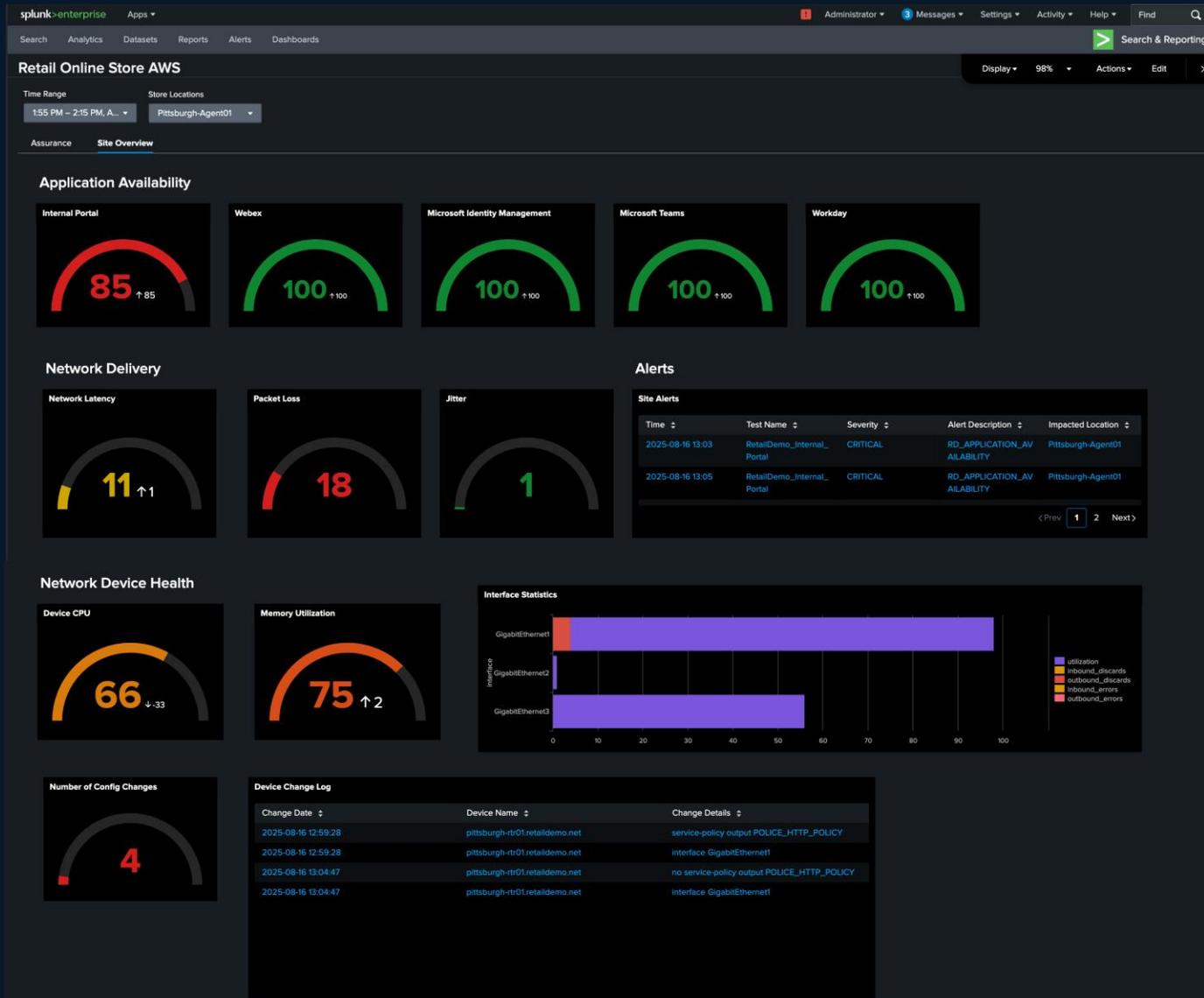
Here we can quickly see that the increase in network latency and therefore increase in transaction time is coming from the CDN provider.

ThousandEyes and Splunk

Integrate ThousandEyes with Splunk Platform and Splunk Observability



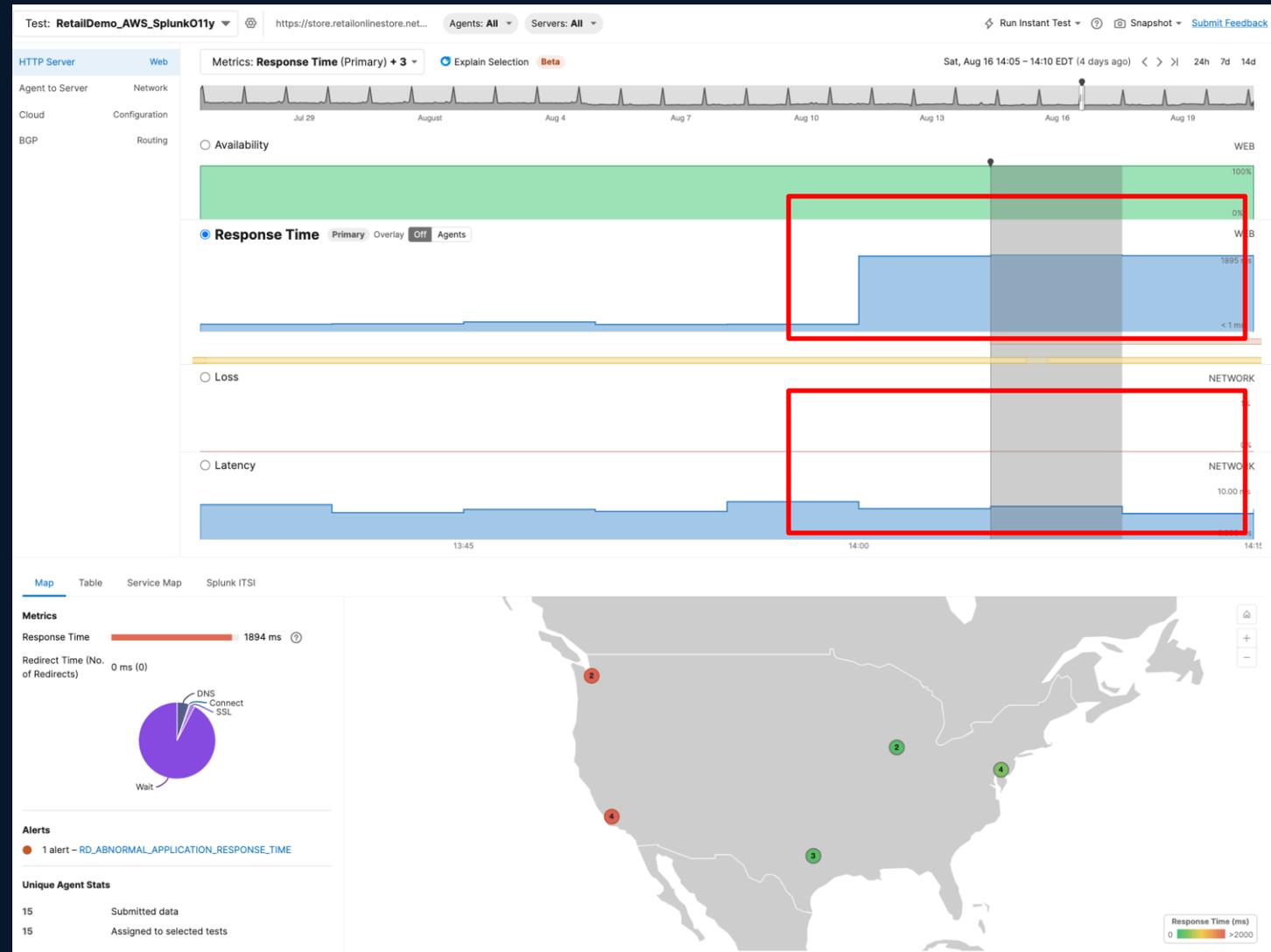
ThousandEyes and Splunk Platform



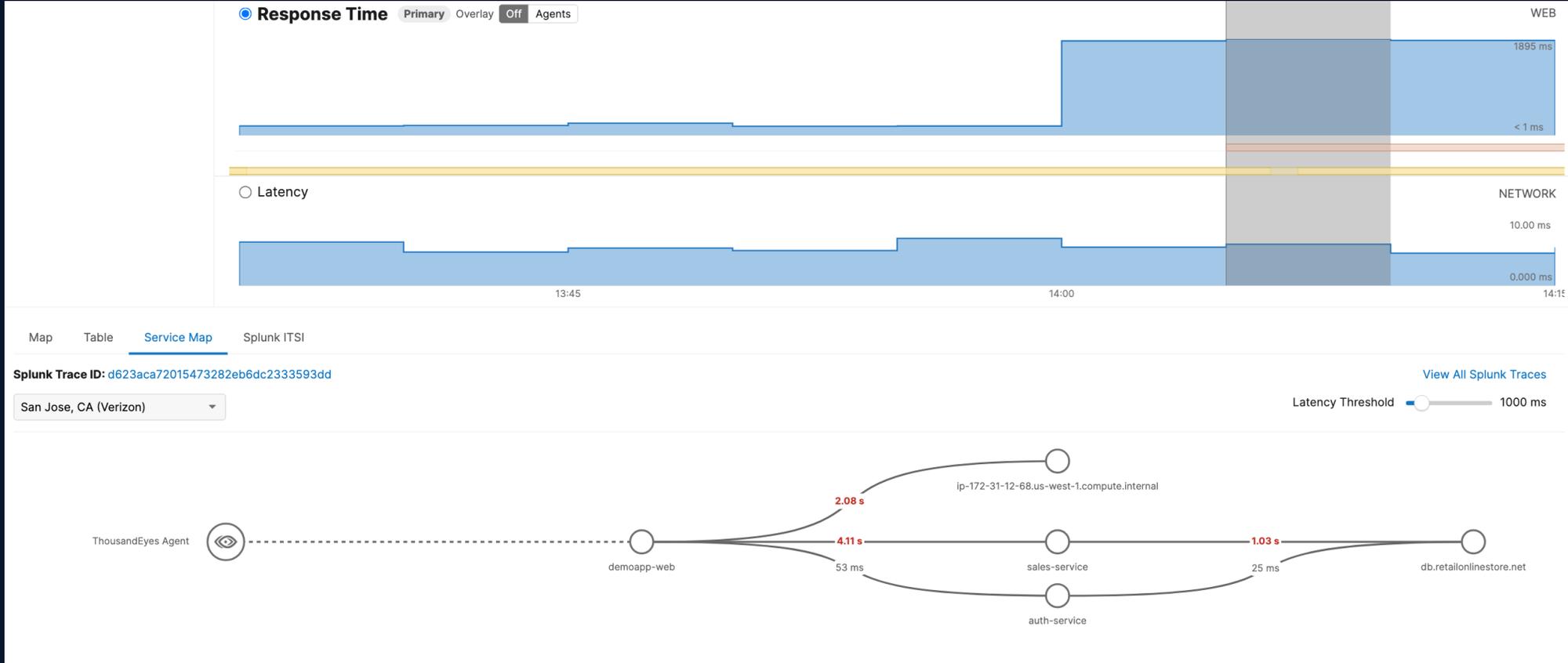
This is an example Retail store Dashboard leveraging ThousandEyes data using Open Telemetry, combined with Network Telemetry (SNMP / Syslog), and Observability Data for System Resources (CPU, Memory)

ThousandEyes with Splunk Observability Workflow

Here we see increases in application response time. ThousandEyes quickly shows that it does NOT appear to be network related.

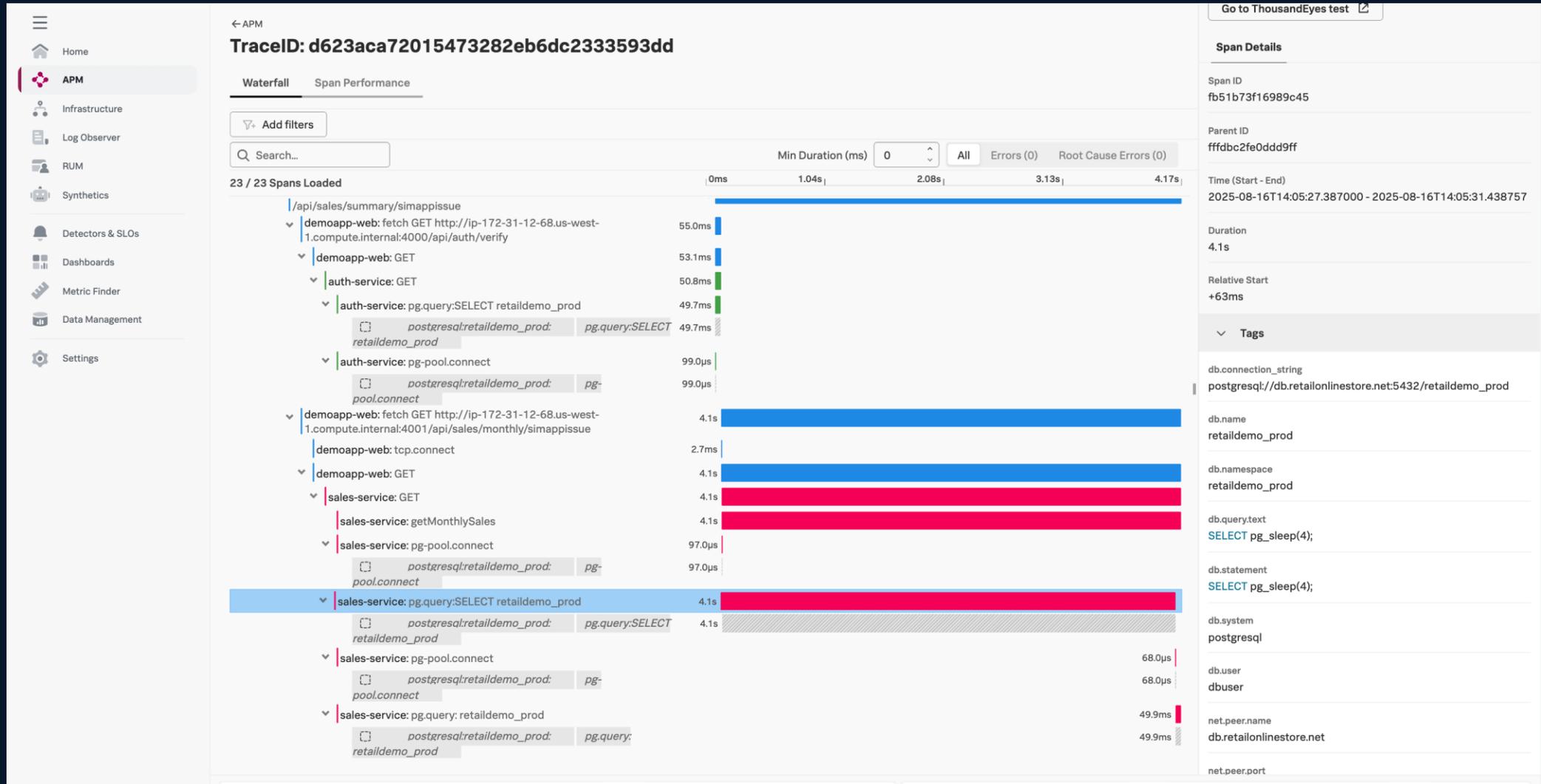


ThousandEyes with Application Dependencies (Observability)



The Splunk Observability Cloud service map provides the ability to diagnose backend application problems. We can quickly see high levels of inter-app latency. From here, we can launch in context to the Splunk Observability Cloud transaction trace.

Drill down to Application trace detail in Observability Cloud



The Trace shows us exactly where and why the application is slowing down.

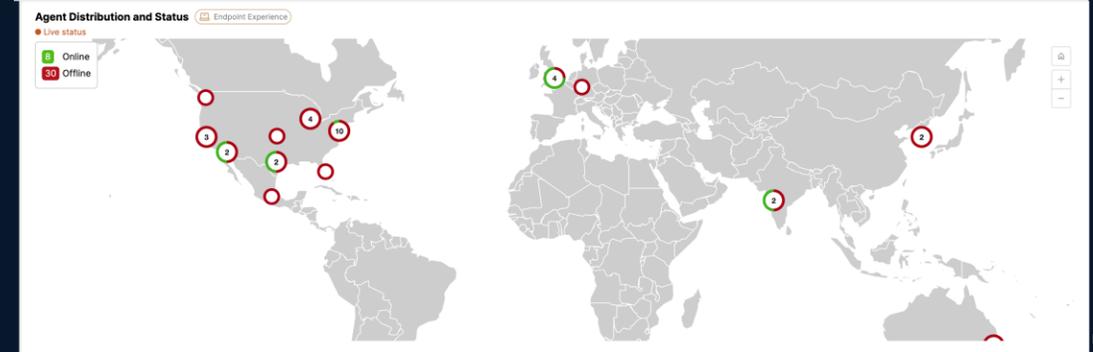
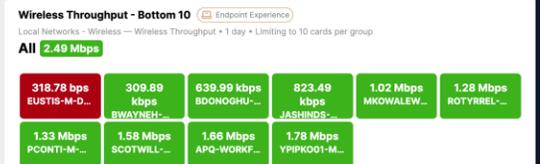
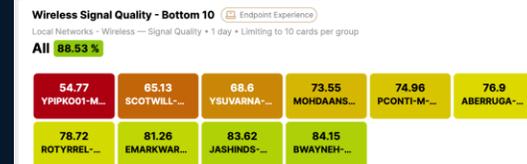
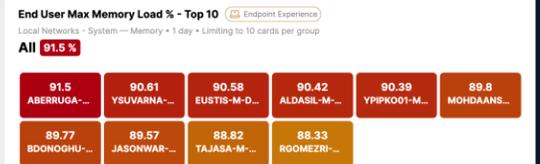
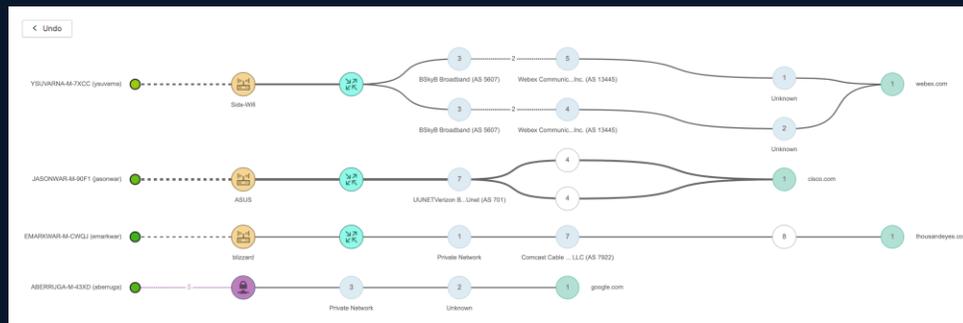
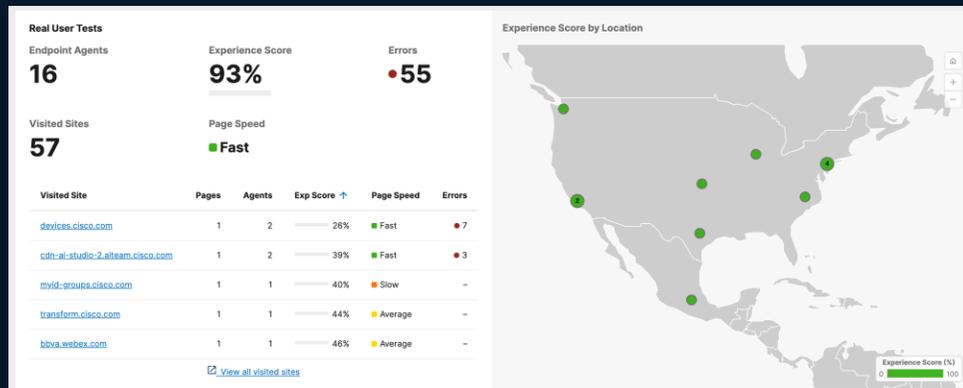
Employee Experience Cisco Synergies



CISCO
SECURE

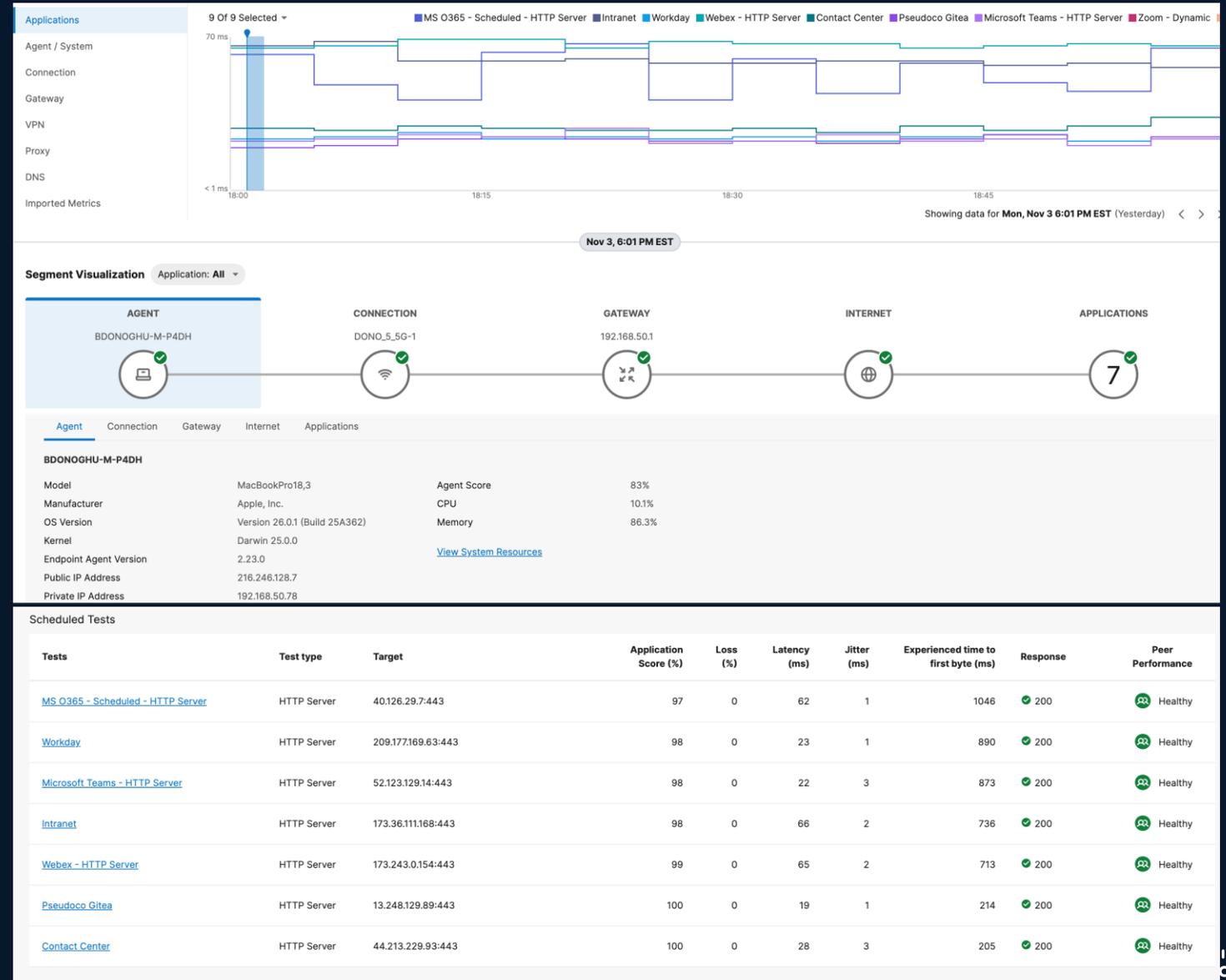
Understand Employee Experience Wherever They Are...

- App/Service Experience with correlated network visibility
- Last mile insights (WiFi, VPN, Proxy)
- Real User, Scheduled and Dynamic testing

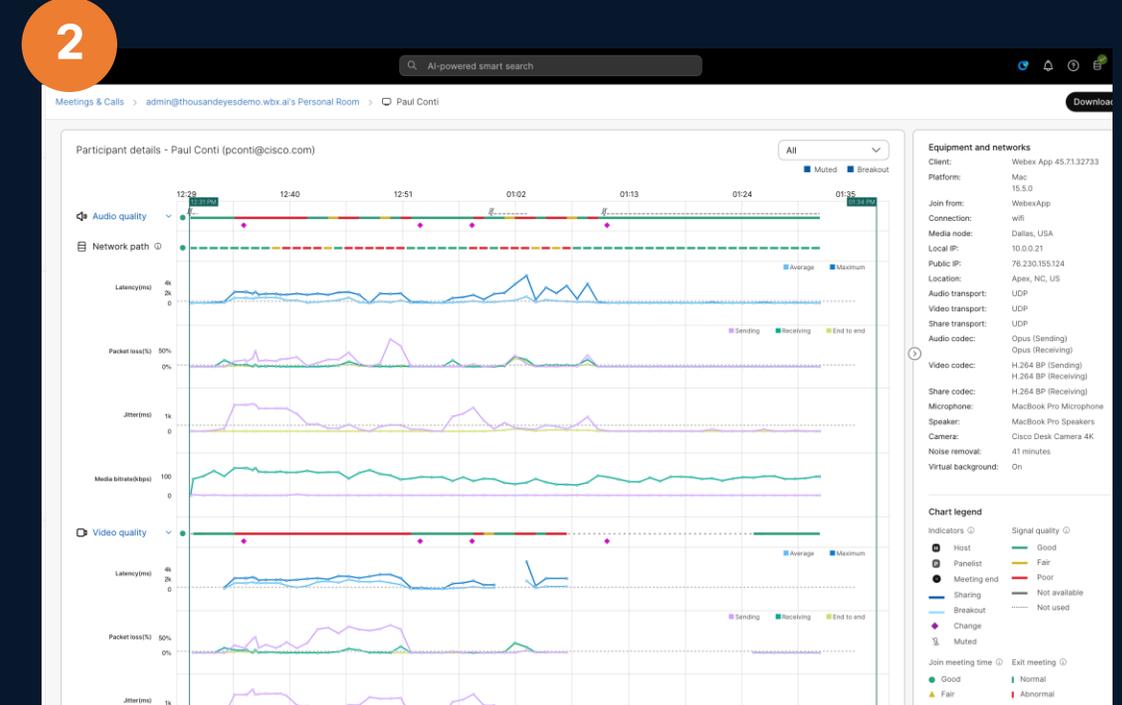
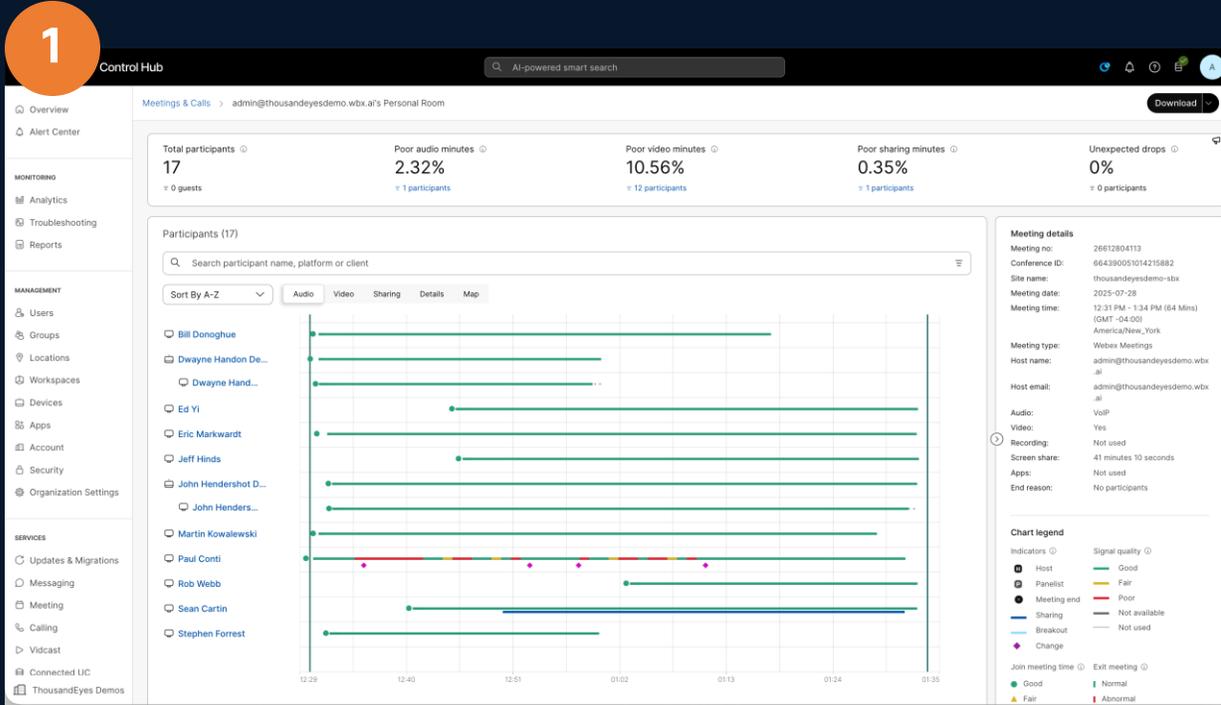


Endpoint - Agent View

- Holistically troubleshoot user experience in real-time or historically
- Proactive insights into service performance
- Simplistic segment visualization to quickly isolate the fault domain



ThousandEyes and Webex



Webex Control Hub shows the status of real-time or historical meetings. Here we can validate that Paul did not have a quality experience.

Control Hub shows us that during the meeting, Paul experienced poor audio and video, with elevated levels of packet loss, network latency and jitter.

ThousandEyes and Webex

3

Settings & Calls > admin@thousandeyesdemo.wbx.ai's Personal Room > Paul Conti

Participant details - Paul Conti (pconti@cisco.com)

Audio quality

Network path

Network path 12:50 - 12:51

We detected packet loss issue (loss rate > 10%), click each end point to view details.

Private Network 11 Unknown N...

Name	IP Address	Private IPv4	Loss	Latency	Jitter	Location
PCONTI-M-WTJ	172.20.10.12	172.20.10.12	40%	609ms	376ms	Cary, North Carolin...

Launch ThousandEyes dashboard Copy ThousandEyes URL

Media bitrate(kbps)

Video quality

Latency(ms)

Packet loss(%)

Jitter(ms)

Equipment and networks

Client: Webex App 45.71.32733
Platform: Mac 15.5.0
Join from: WebexApp
Connection: wifi
Media node: Dallas, USA
Local IP: 10.0.0.21
Public IP: 76.230.155.124
Location: Apex, NC, US
Audio transport: UDP
Video transport: UDP
Share transport: UDP
Audio codec: Opus (Sending)
Opus (Receiving)
Video codec: H.264 BP (Sending)
H.264 BP (Receiving)
Share codec: H.264 BP (Receiving)
Microphone: MacBook Pro Microphone
Speaker: MacBook Pro Speakers
Camera: Cisco Desk Camera 4K
Noise removal: 41 minutes
Virtual background: On

Chart legend

Indicators

- Host
- Panelist
- Meeting end
- Sharing
- Breakout
- Change
- Muted

Signal quality

- Good
- Fair
- Poor
- Not available
- Not used

Join meeting time

- Good
- Fair
- Normal
- Abnormal

With the ThousandEyes integration, Control Hub now has more insight into the health of the actual network path. We can quickly see WHERE the network disruption is coming from and launch in context to ThousandEyes.

ThousandEyes and Webex

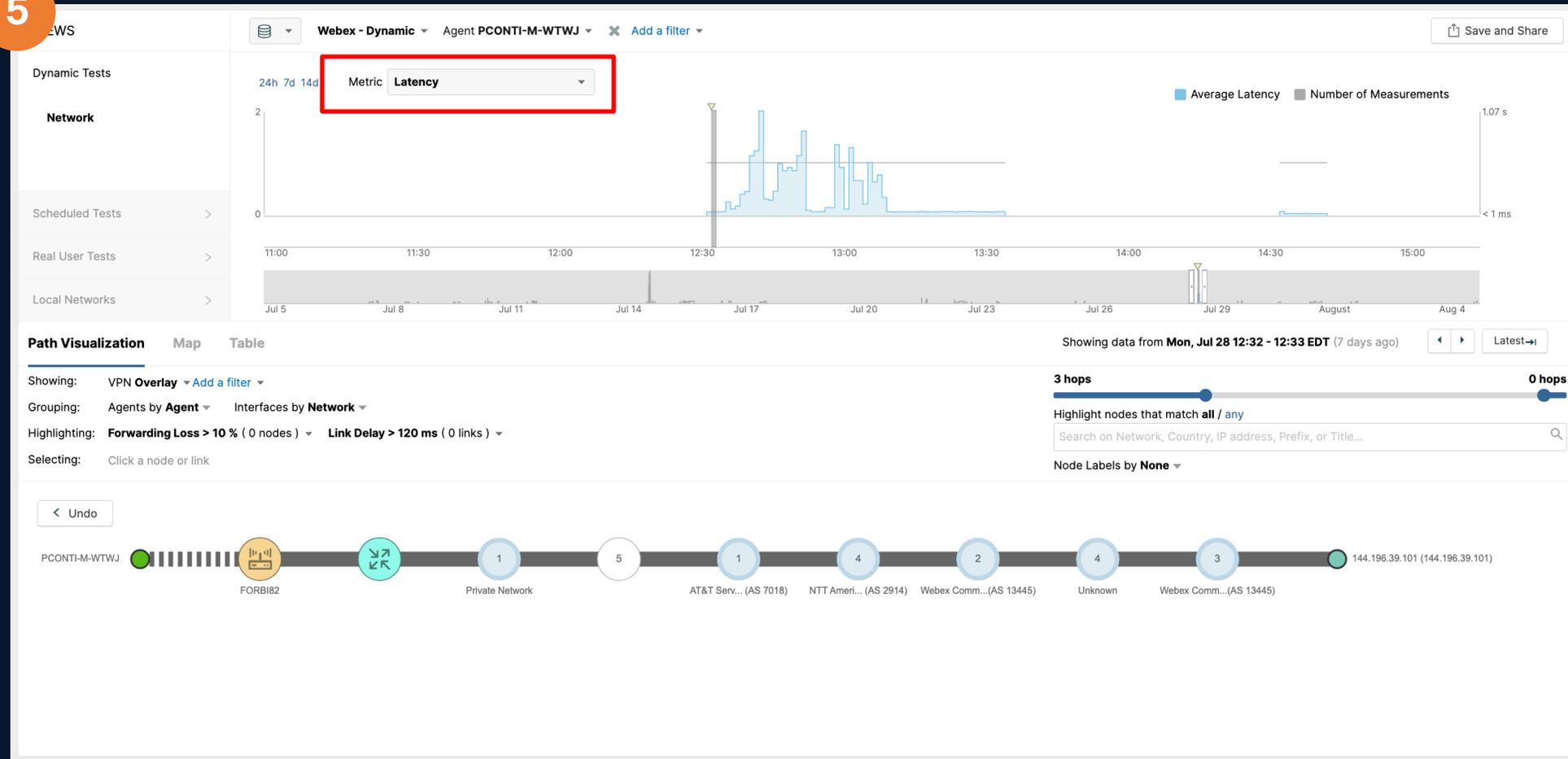
4



ThousandEyes shows us that for the meeting in question, the network latency and loss that is ultimately impacting Paul's experience is coming from his local network.

ThousandEyes and Webex

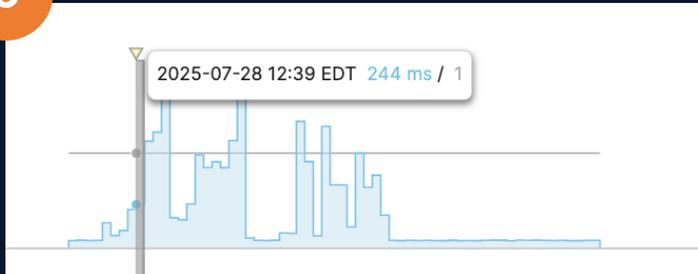
5



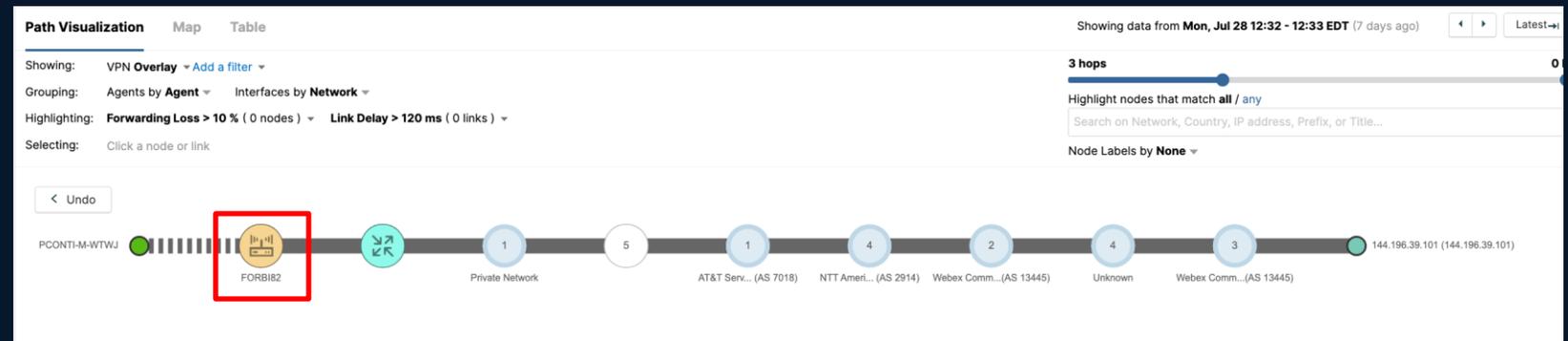
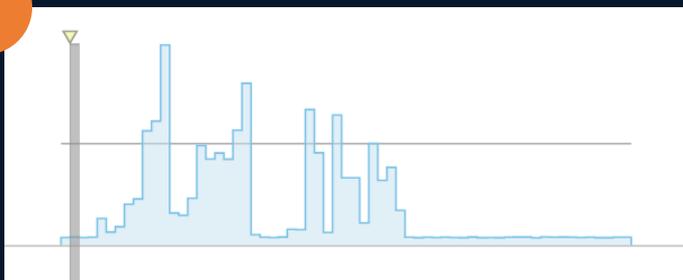
If we look BEFORE (or after) the elevation in latency and packet loss, we can see the network path is much different. Paul is connecting to a completely different network.

ThousandEyes and Webex

6



7



ThousandEyes sees that Paul bounces from his home wifi (good) to his iPhone (bad). This was the cause of his poor experience.

ThousandEyes and Secure Access

- Integrated ThousandEyes end-user experience/performance data into Secure Access Dashboard
- Validate VPN traffic and network performance to secure access env
- Package ThousandEyes agent with Secure Access config for simple deployment

The screenshot displays the Cisco Secure Access dashboard with the following sections:

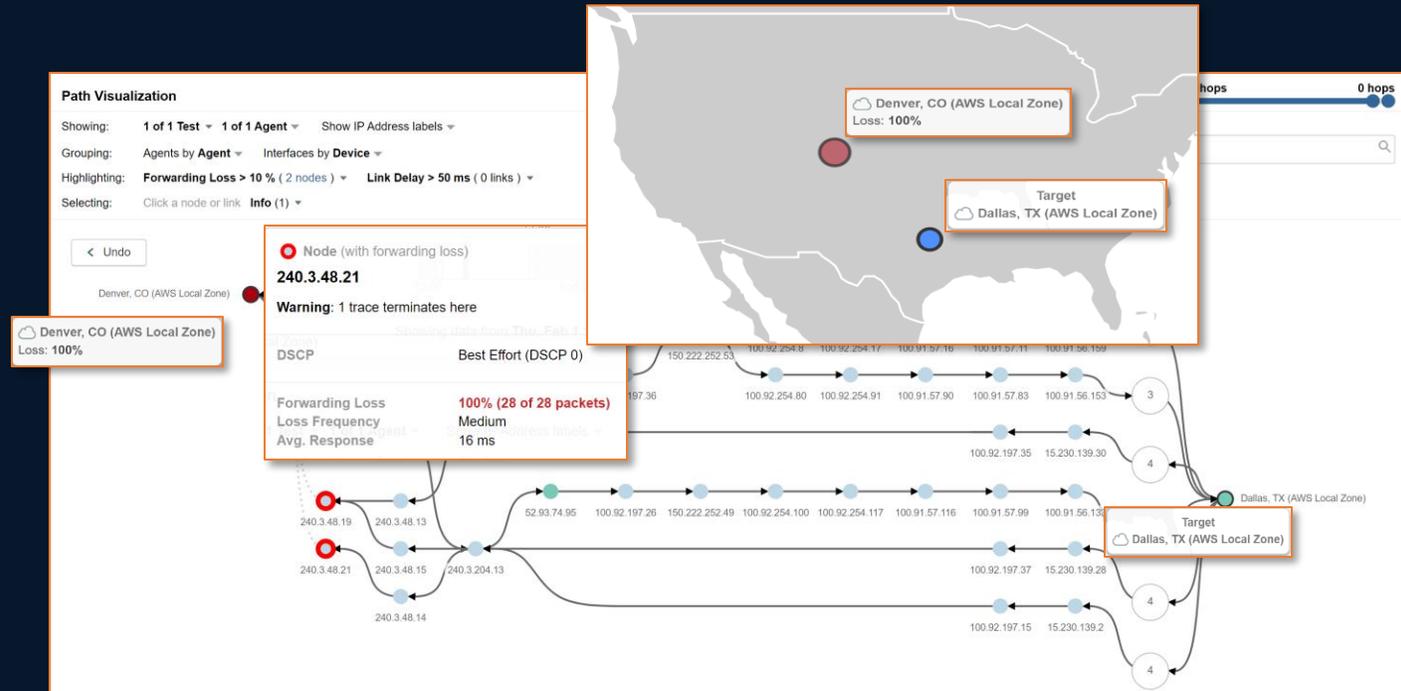
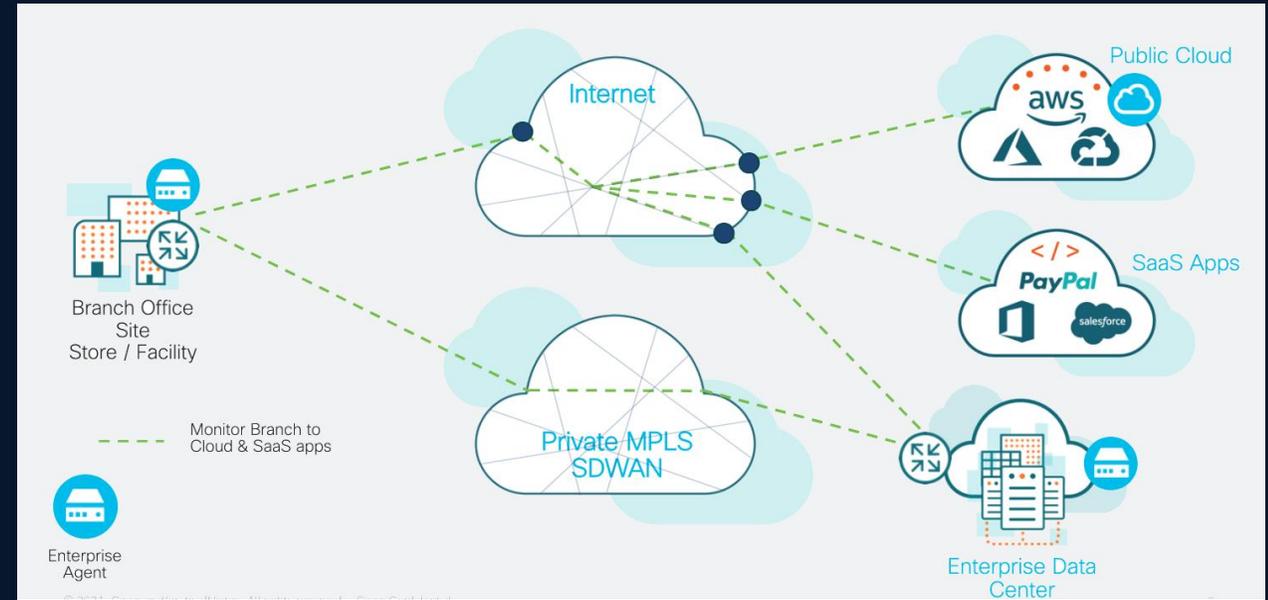
- Experience Insights:** Overview of user experience for SaaS applications in the US (Pacific Northwest). Applications shown include AWS (Reachable, 256ms), Azure (Reachable, 170ms), Bing (Reachable, 72ms), and Box (Reachable, 287ms).
- Endpoints summary:** 27 endpoints connected to Secure Access out of 196 registered.
- Endpoint map:** Geographic distribution of endpoints, showing a concentration in the United States.
- Endpoint health:** Metrics for WiFi Signal Quality (100%), CPU Usage (27.57%), and Memory Usage (84.89%).
- Segment visualization:** Network path from Agent to Internet to Applications.
- Scheduled Tests:**

Tests	Test type	Target	Application Score (%)	Loss (%)	Latency (ms)	Jitter (ms)	Experienced time to first byte (ms)	Response
insecureaccounting	HTTP Server	44.218.150.164:443	98	0	74	0	752	200
Google Search	HTTP Server	142.250.191.68:443	100	0	10	0	221	200
Cisco Secure Access (DO NOT EDIT)	Network	TCP 52.28.34.250:443	100	0	32	0	-	200
- Collaboration Application Summary:**
 - Webex Application Score:** 99.8% (High latency - more than 150 ms)
 - Latency:** 62.0 ms (High jitter - more than 30 ms)
 - Jitter:** 2.0 ms (High loss - more than 10%)
 - Loss:** 0.0%

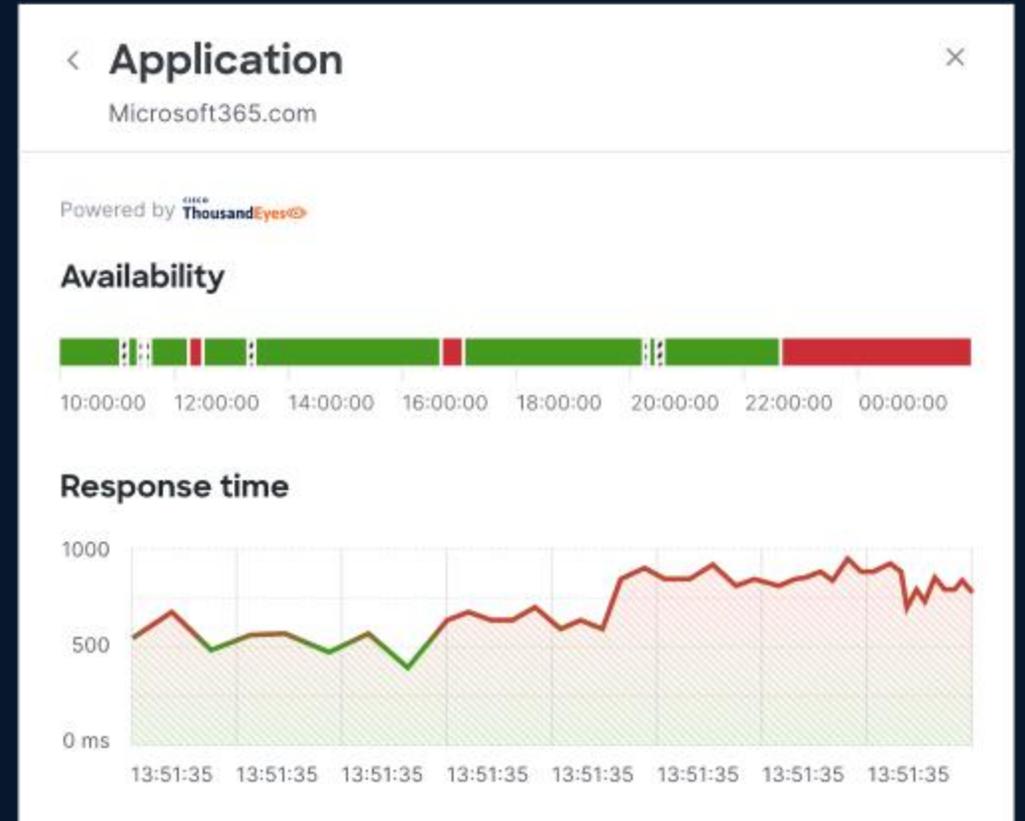
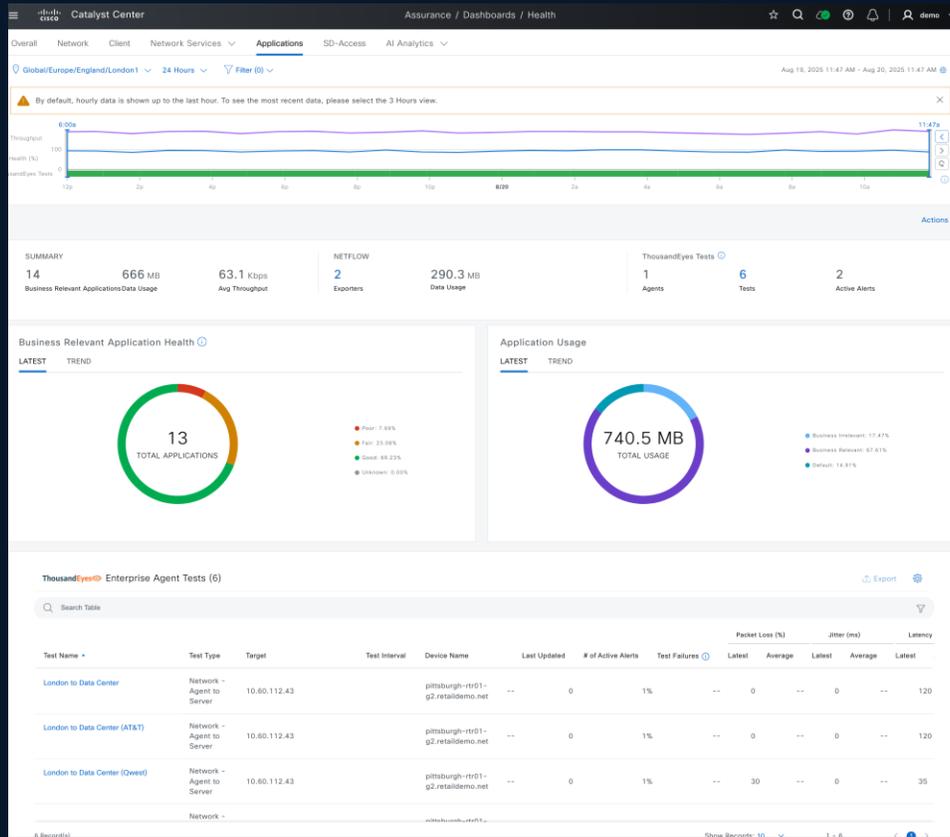
Enterprise Network Assurance

Network Visibility

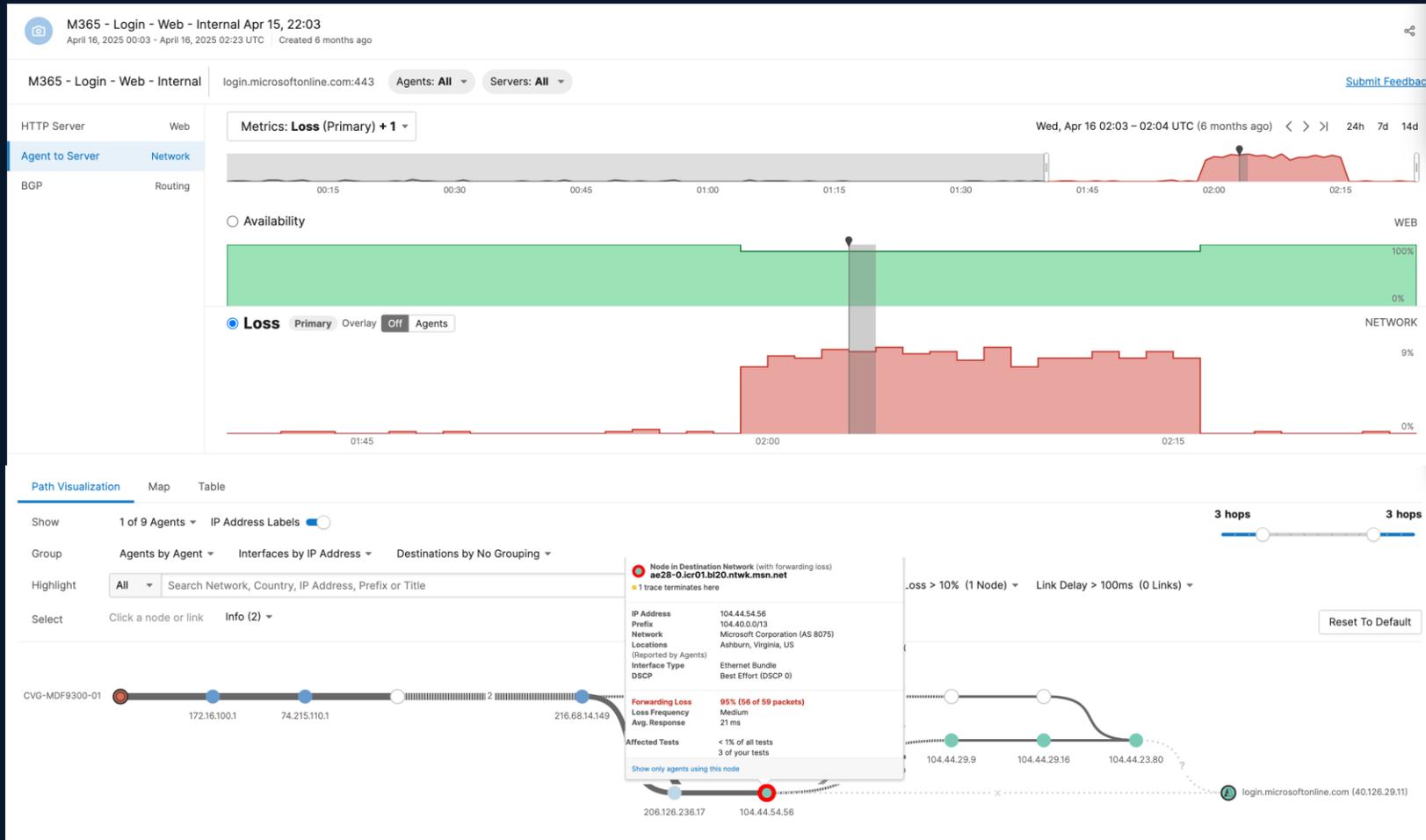
- Measure packet loss, latency and jitter across network paths, hop by hop visibility
- Validate change, understand historical traffic flows
- Measure and validate ISPs at DCs and Sites
- Site-to-site, SaaS and application performance, SDWAN (overlay/underlay)



Catalyst and Meraki Integrations



Cisco Networking



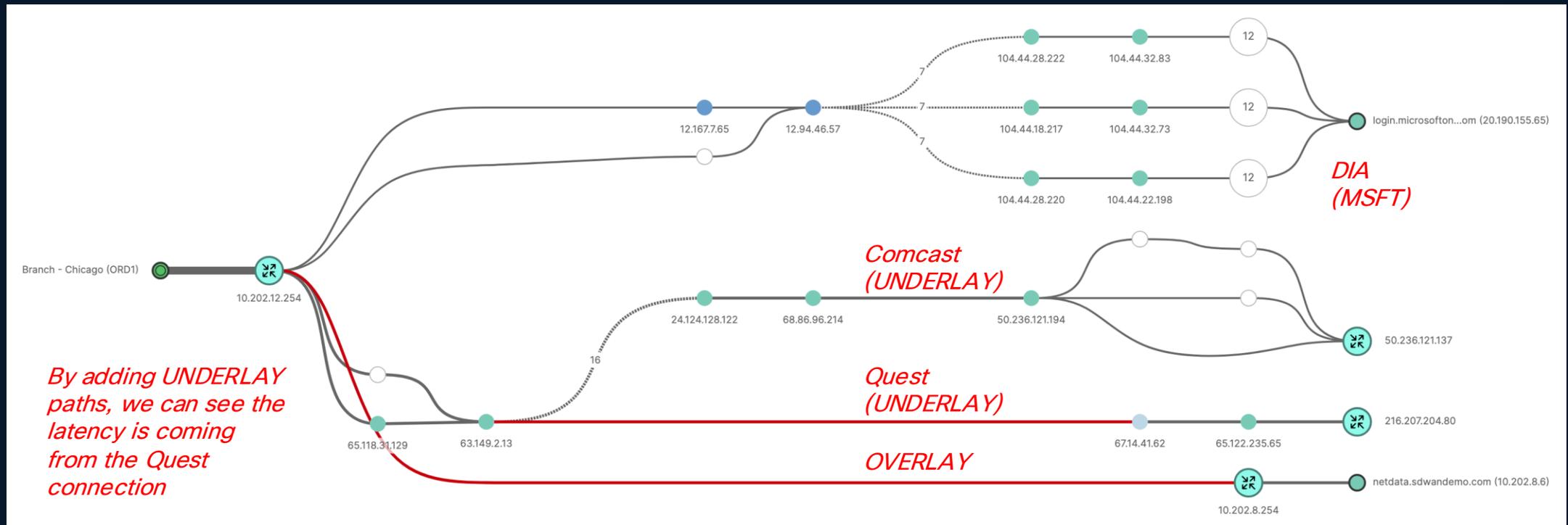
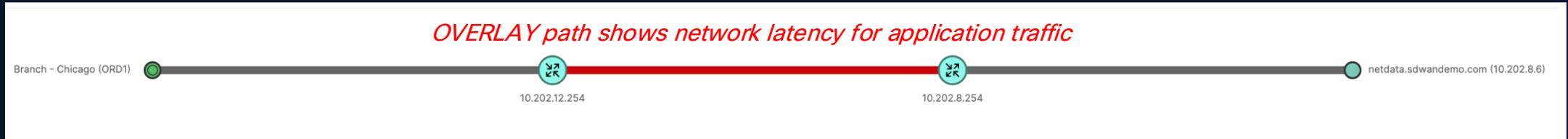
Here we see access to MS O365 was interrupted from a branch site. We are testing from a Cat9K and can quickly isolate the problem being one of a MSFT network issue. This data can be shared directly with MSFT to speed remediation.

SDWAN



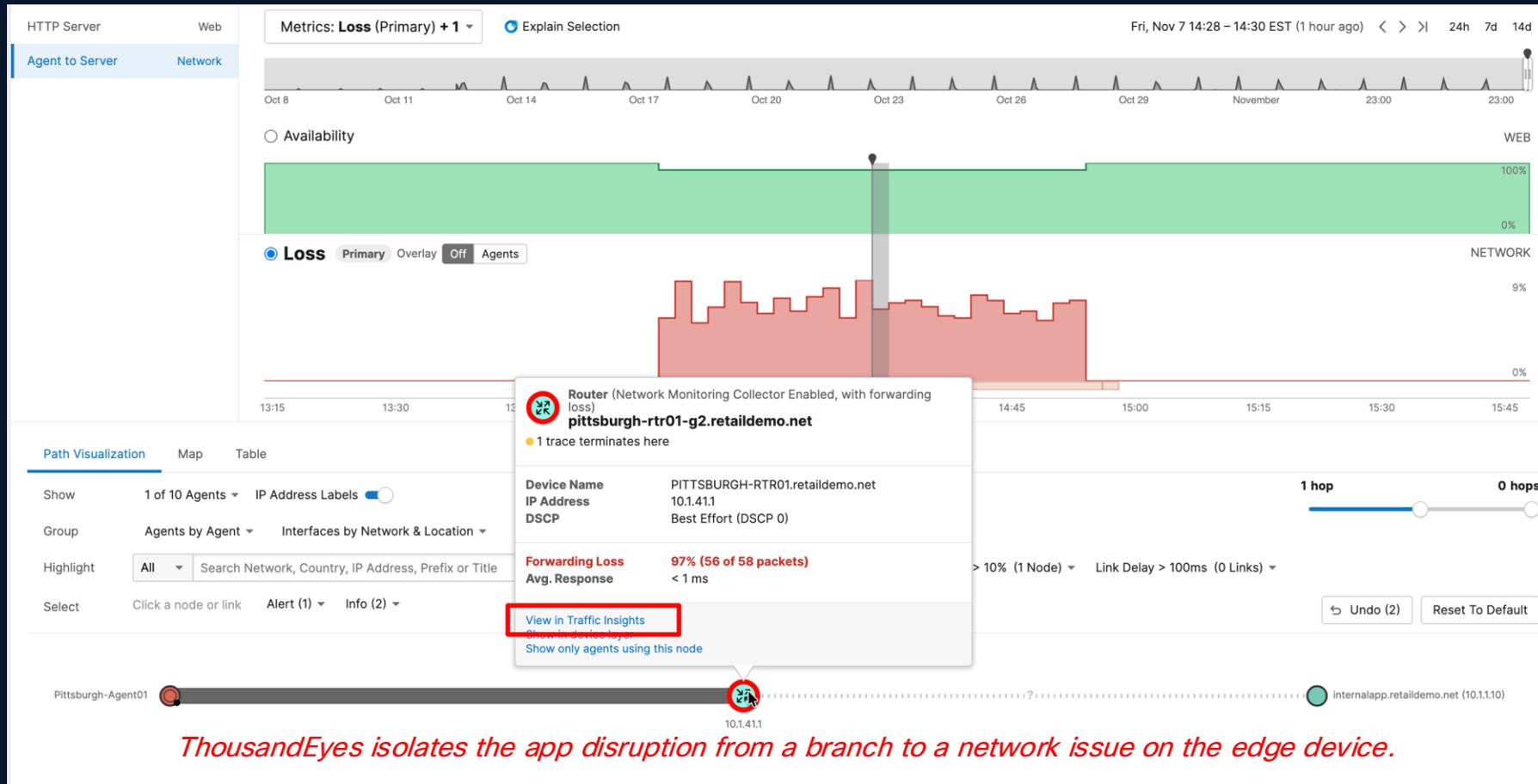
DC hosted application is accessed from branch sites via SDWAN. We can see periodic spikes in application page load time, additionally, spikes in network latency.

SDWAN



ThousandEyes gives you visibility into both UNDERLAY and OVERLAY paths, as well as DIA traffic to validate your deployment.

Traffic Insights

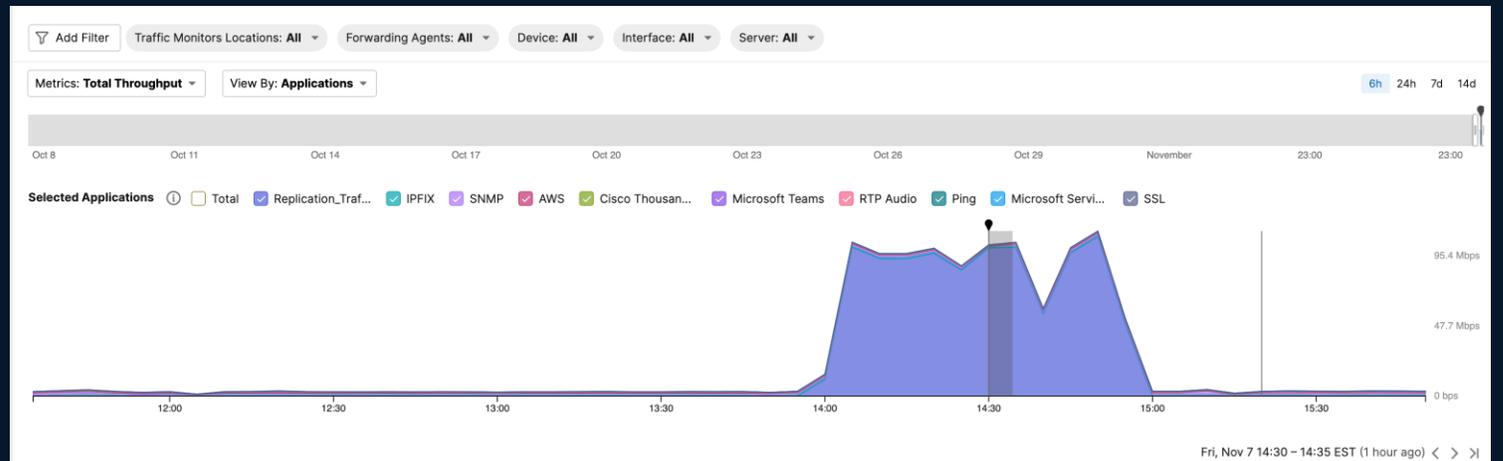
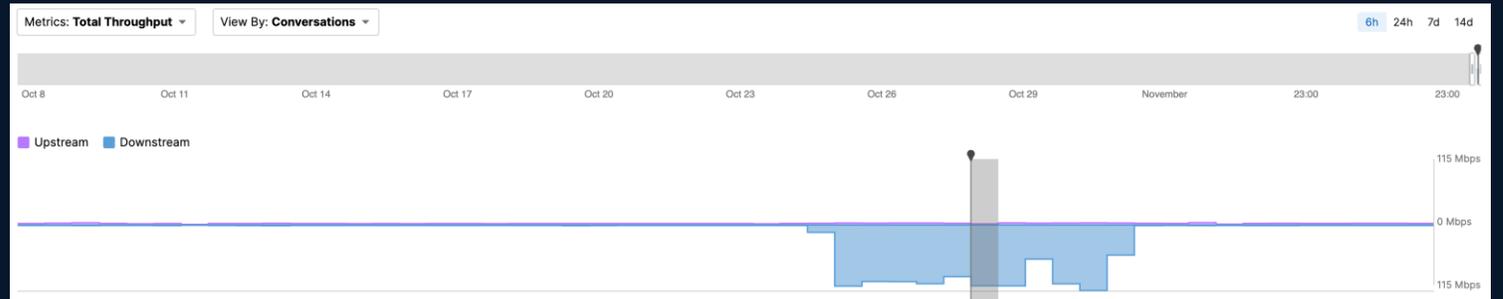


ThousandEyes detects an application outage from the Pittsburgh branch. We quickly isolate this to a network issue and identify that there is packet loss at the site edge device.

Traffic Insights

Traffic Insights gives an extra layer of visibility into YOUR network. ThousandEyes now collects network flow data (Netflow, IPFIX) and correlates that with application and network performance.

Not only can we point you to exactly where in your network the problem is coming from, but also why!



39 rows

Application	Total Throughput	Upstream Throughput	Downstream Throughput	CPS
<input checked="" type="checkbox"/> Replication_Traffic	100.6 Mbps / 97.8%	415.4 Kbps	100.2 Mbps	-
<input checked="" type="checkbox"/> IPFIX	1.0 Mbps / 1.0%	1.0 Mbps	0 bps	-
<input checked="" type="checkbox"/> AWS	330.6 Kbps / 0.3%	201.6 Kbps	129.0 Kbps	4.44
<input checked="" type="checkbox"/> Microsoft Teams	162.7 Kbps / 0.2%	49.6 Kbps	113.2 Kbps	3.43

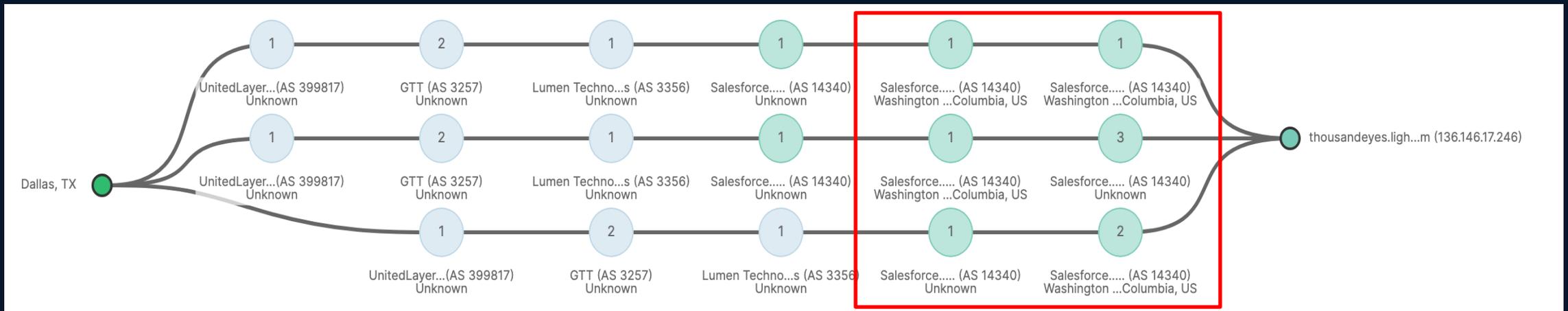
100/504 rows

Application	Client	Servers	Server Ports	Server Locations	Protocol	Devices	Client Interfaces	Server Interfaces	Total Throughput	CPS
<input checked="" type="checkbox"/> Replication_Traffic	10.1.41.7	10.1.1.10	10566	-	6	3	3	-	100.6 Mbps / 97.8%	-
<input checked="" type="checkbox"/> IPFIX	10.1.253.41	2	18089	-	17	3	3	-	134.4 Kbps / 0.1%	-
<input checked="" type="checkbox"/> IPFIX	10.1.253.31	2	18089	-	17	2	3	-	114.8 Kbps / 0.1%	-

CLOUD/SAAS Public Cloud Providers and SAAS Apps

ThousandEyes for Cloud and SaaS

- *CONTEXTUAL* Cloud-based infrastructure services, inventory and topology
- SaaS applications
- Hybrid App components living in the cloud (3rd party, API..etc)
- Visibility into provider network to isolate fault domain, and escalate with evidence



ThousandEyes Cloud Insights

Key Capabilities

1. Cloud Inventory

Automatically creates an inventory of all elements and services across the entire cloud infrastructure.

2. Cloud Path Enrichment and Topology Visualization

Auto discover cloud provider resources to understand every service dependency

3. Correlated Cloud Infrastructure Changes

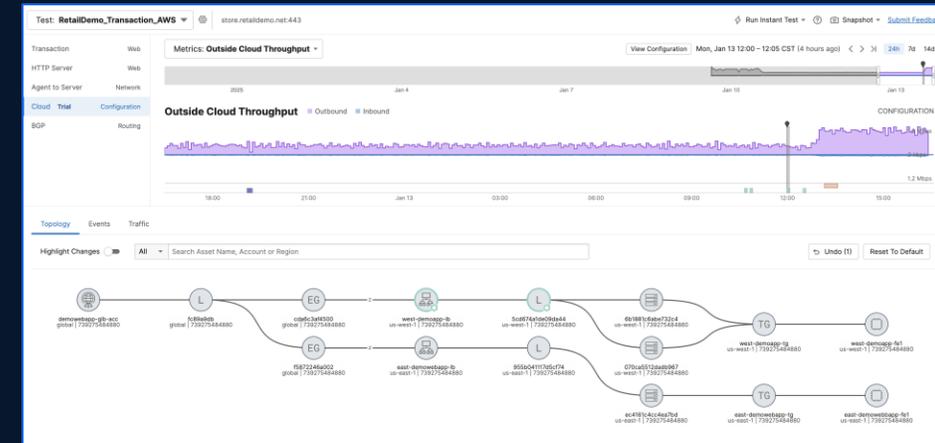
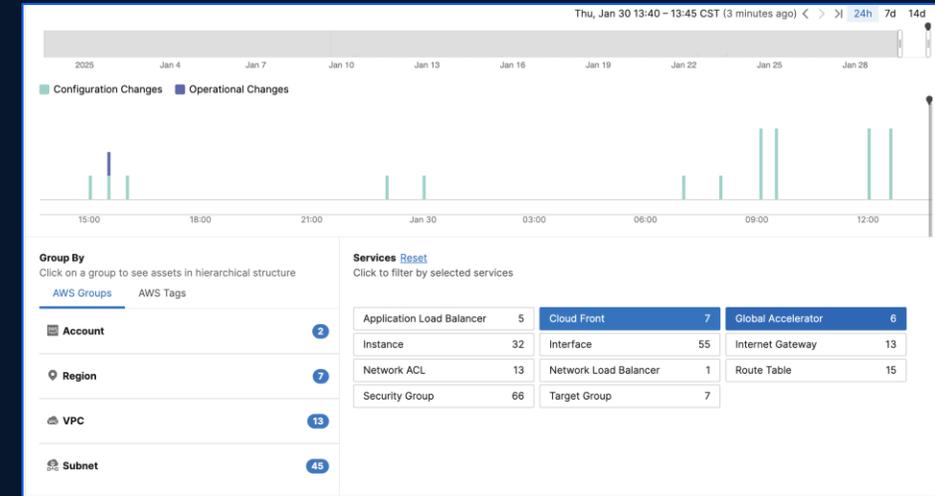
Append config changes and events to time-correlated views of experience so you can isolate root-cause faster

4. Cloud Traffic Views

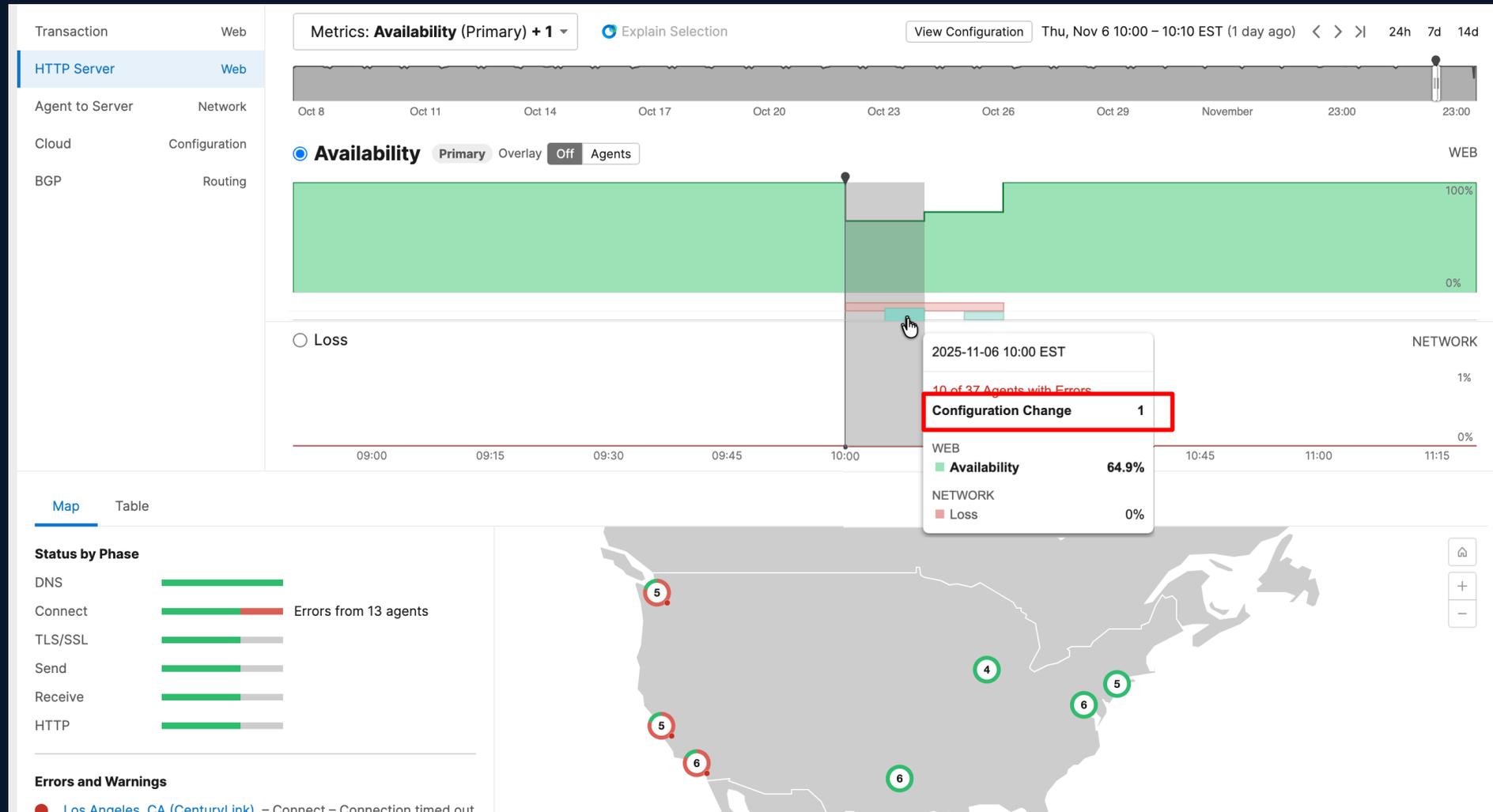
View traffic patterns so you can efficiently architect and troubleshoot your cloud network

Value

Deep visibility into public cloud infrastructure and service dependencies that impact digital experiences to dramatically reduce MTTR

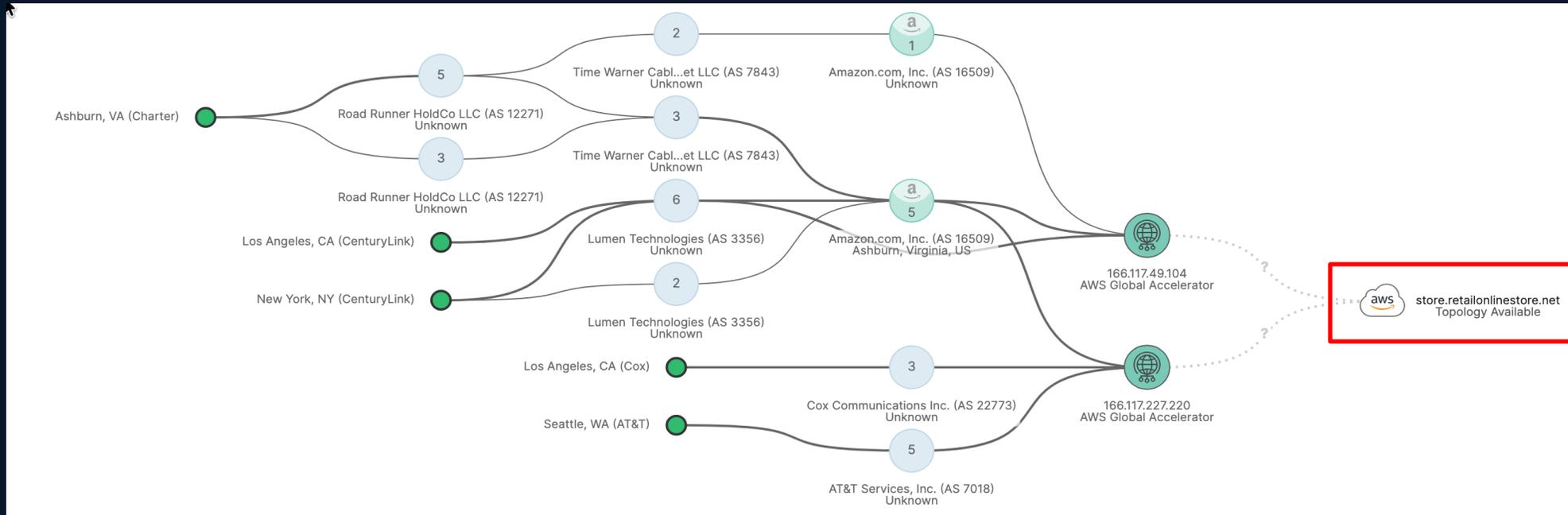


ThousandEyes for Cloud Hosted Apps



Critical customer facing application (hosted in AWS) has degraded availability impacting only the US West Coast. Does NOT appear to be a network issue.

ThousandEyes for Cloud Hosted Apps



Our path visualization validates there is no disruption to network delivery. With Cloud Insights, we can go deeper into the Cloud Service Topology.

ThousandEyes for Cloud Hosted Apps



Now we can see different cloud services leveraged by our application (security groups, load balancers, FW, compute..etc) and understand where changes are happening.

ThousandEyes for Cloud Hosted Apps

ork & App Synthetics

RetailDemo_Transaction_AWS

Thu, Nov 6 10:05 – 10:10 EST (1 day ago)

Oct 8 Oct 11

Highlight Changes All Search Asset Name, Entity ID, Account or Region

Service Configuration > Network and Security **New**

us-west-1

EG 96f06e625500 483411789967

eni-0...9c874d 483411789967

eni-0...51ac95 483411789967

SG Globa...rator 483411789967

SG Globa...rator 483411789967

Cloud Event Details

Time Thursday, November 6 2025, 10:05:00 EST

Asset Name uw1-retaildemo-web-lb-sg

Explore In AWS ↗

Contextual launch back to provider to remediate change.

Config Additional Details

```
15 ],
16 "toPort": -1
17 },
18 {
19 "fromPort": 22,
20 "ipProtocol": "tcp",
21 "ipRanges": [
22 {
23 "cidrIp": "104.15.131.179/32"
24 }
25 ],
26 "toPort": 22
27 },
28 {
29 "fromPort": 443,
30 "ipProtocol": "tcp",
31 "ipRanges": [
32 {
33 "cidrIp": "0.0.0.0/0"
34 }
35 ],
36 "toPort": 443
37 },
38 {
39 "fromPort": 3000,
40 "ipProtocol": "tcp",
41 "ipRanges": [
42 {
43 "cidrIp": "10.255.4.0/23",
44 "description": "UE2 Internal LB"
```

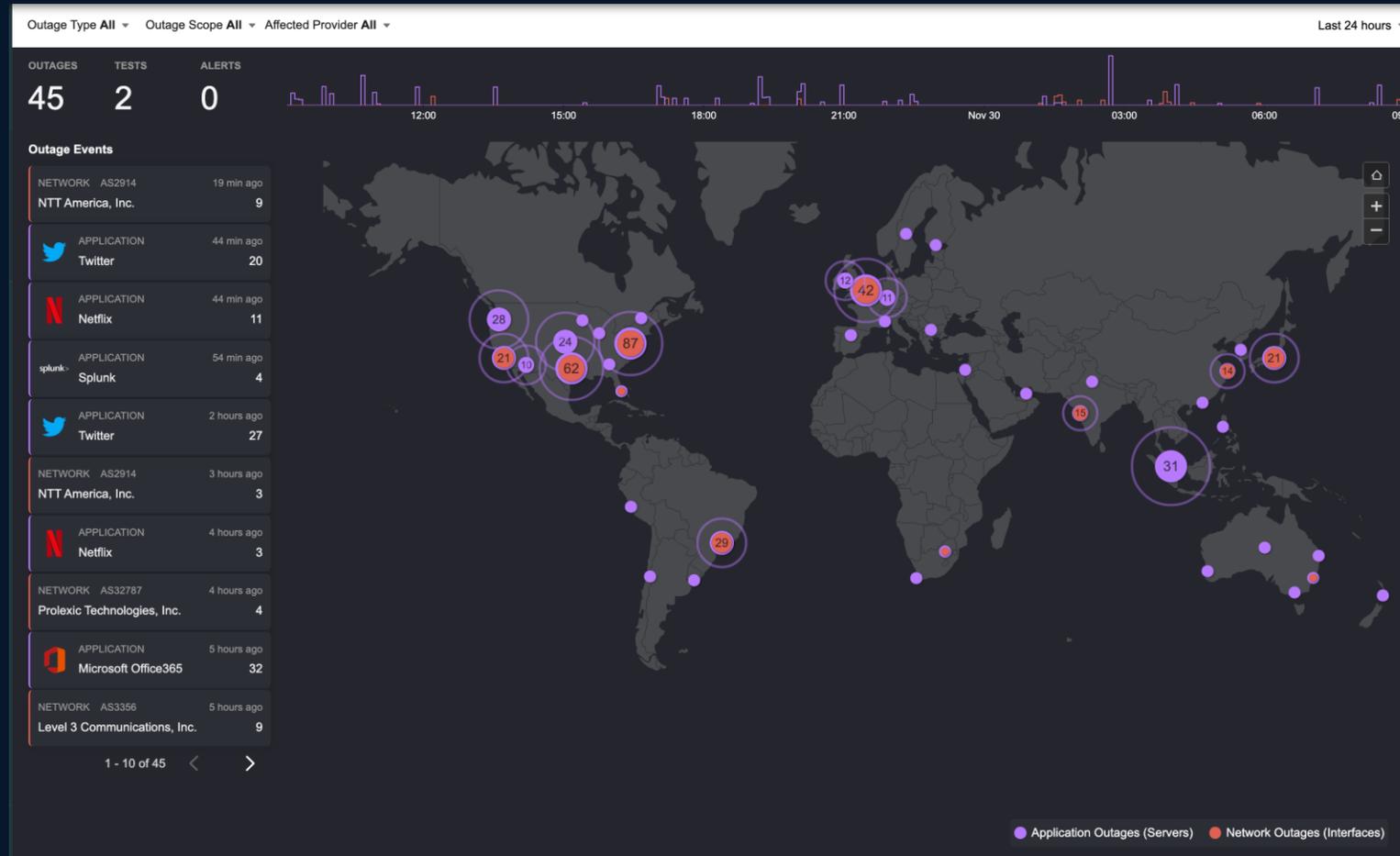
```
15 ],
16 "toPort": -1
17 },
18 {
19 "fromPort": 22,
20 "ipProtocol": "tcp",
21 "ipRanges": [
22 {
23 "cidrIp": "104.15.131.179/32"
24 }
25 ],
26 "toPort": 22
27 },
28 {
29 "fromPort": 443,
30 "ipProtocol": "tcp",
31 "ipRanges": [
32 {
33 "cidrIp": "209.214.0.0/15"
34 }
35 ],
36 "toPort": 443
37 },
38 {
39 "fromPort": 3000,
40 "ipProtocol": "tcp",
41 "ipRanges": [
42 {
43 "cidrIp": "10.255.4.0/23",
44 "description": "UE2 Internal LB"
```

Before and after service configuration view.

Cloud Insights gives you the ability to correlate application performance degradation directly with cloud provider service configuration changes. Dramatically reducing MTTR!

ThousandEyes Internet Insights

Global View
of SaaS App
Availability



Quickly identify
ISP outages
and impact

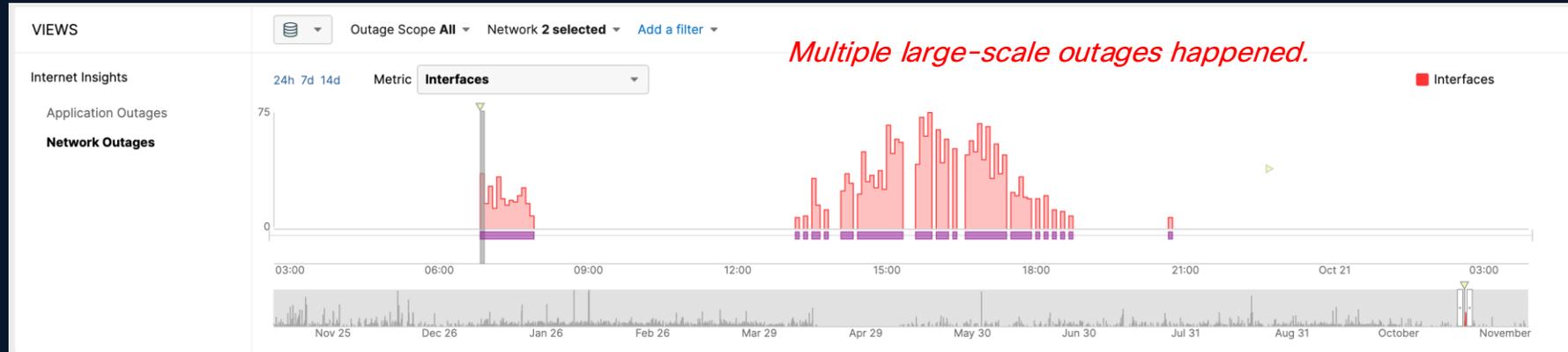
Rapid time to value

Faster incident response

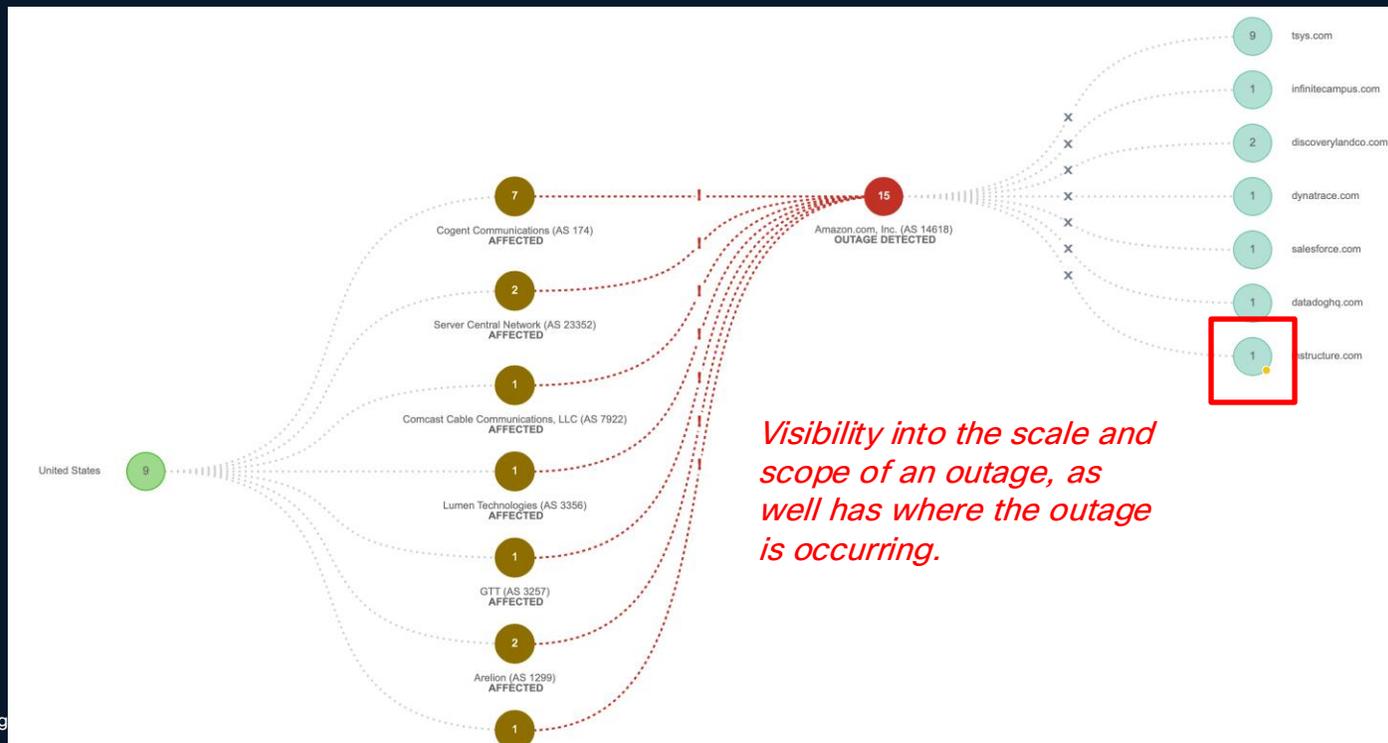
Provider-focused insights

Save Time and Resources

AWS Outage 10/20

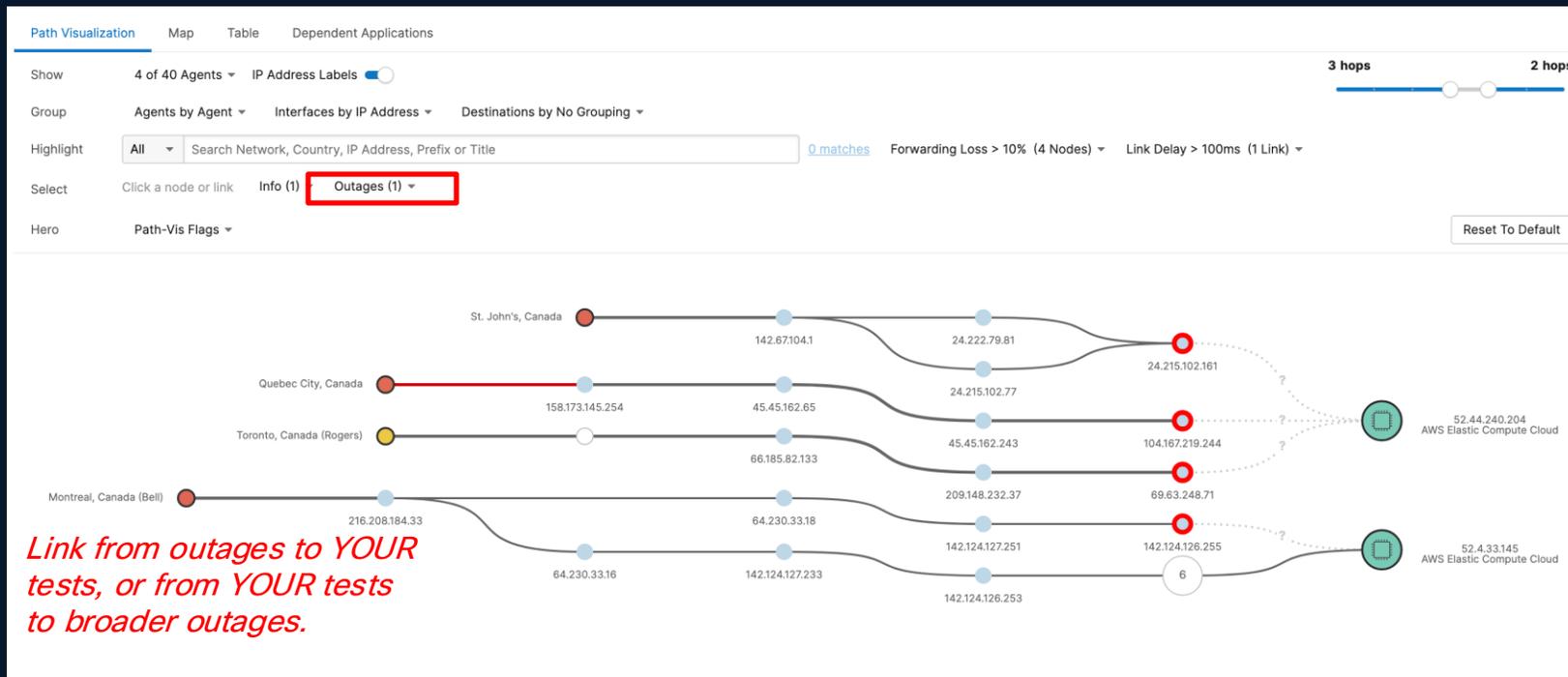


Stop wasting time with triage because a vendor has not posted that they are having an issue.



Internet Insights allows you to understand global ISP or SAAS outages based on real data. Even if YOU are not testing those services.

AWS Outage 10/20





“ThousandEyes helps you see beyond your environment, act with precision, and assure the performance of any connected experience—across owned and unowned networks.”

CISCO Connect !

Thank you

