

See Everything, Solve Anything:

Advanced Network Intelligence with ThousandEyes



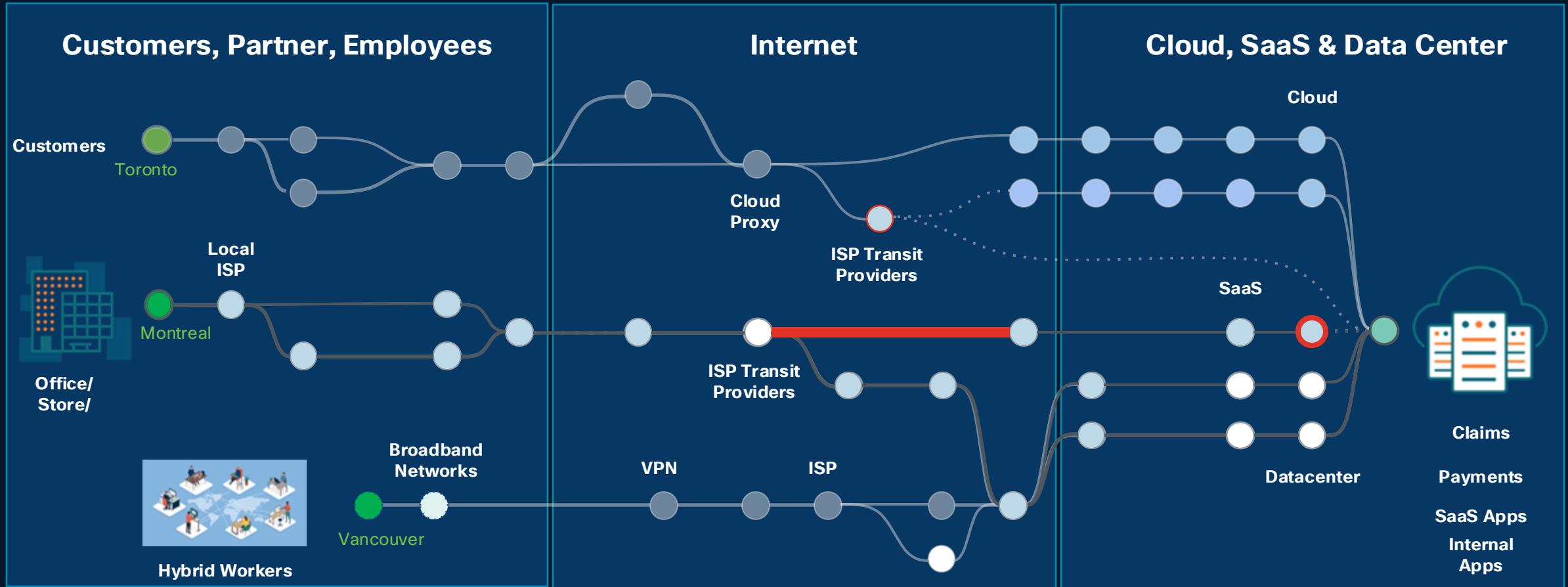
Vineeth Somanchi

ThousandEyes Solutions Engineer

Agenda

1. What is ThousandEyes
2. Cloud Assurance
3. AI Event Detection and Assistant
4. Splunk Integrations

Challenges ThousandEyes Helps Solve



Distributed workforce using

No visibility into unowned ISP infrastructure

No visibility into Cloud and SaaS provider networks

Integrated with Cisco's Environment

LAN/WAN



Catalyst Switching
Catalyst Routing
Meraki MX
Nexus Switching
Industrial Ethernet (IE) Switching
Industrial Routing (IR)

SSE/SASE



Monitor Endpoint connectivity to cloud proxy and VPN

Collaboration



Monitor video devices & IP phone connectivity to collaboration services

Observability



Extensible data enables cross-domain root cause analysis

How It Works



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



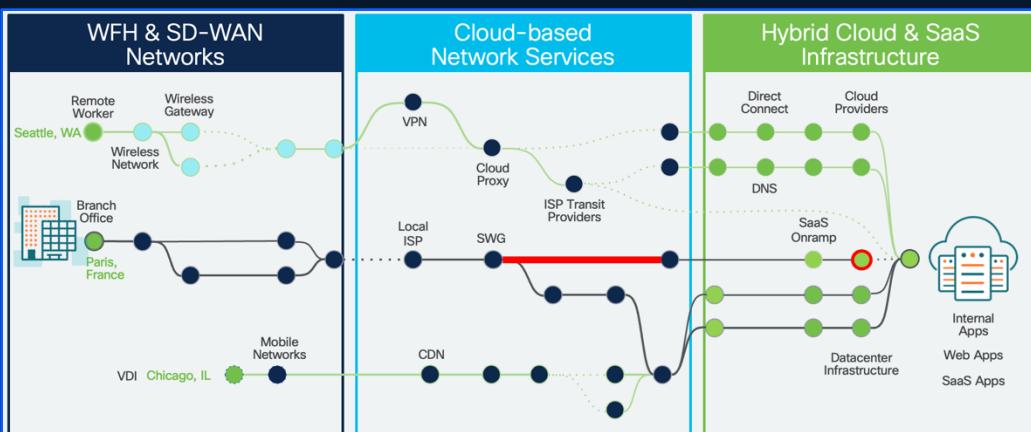
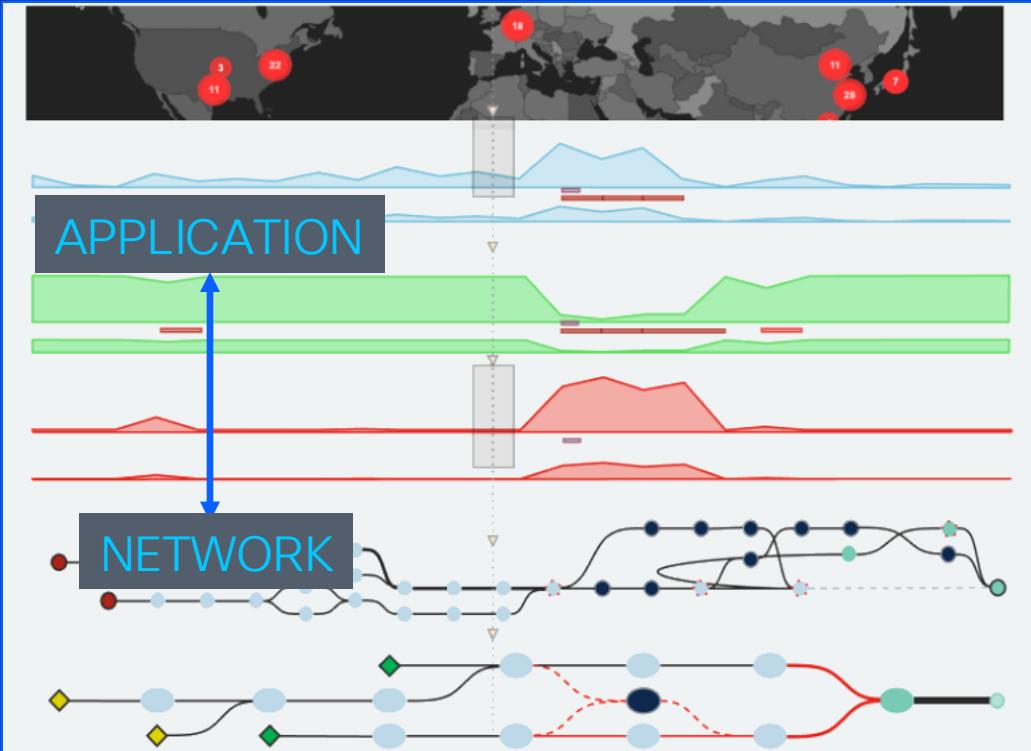
ENTERPRISE AGENT

- 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



Introducing Cisco ThousandEyes Mobile Endpoint Agent for Android

- Extends ThousandEyes Endpoint Experience to help assure mobile-enabled use cases
- Supported on Android 11+ devices, including Zebra scanners
- Lightweight agent for end-to-end visibility and optimal battery life
- Scheduled synthetic tests run at rapid intervals continuously monitor end-to-end connectivity
- Collects and reports on device and wireless metrics



Zebra Scanner Support

Cisco is a member of Zebra's Alliance Partner program

VALIDATED

Cisco

Cisco ThousandEyes Mobile Endpoint Agent

Successfully Tested
Validated with **Zebra**

Version **1.X**

Mobile Computers:

TC15	HC20/HC25	TC53e-RFID
TC22/TC27	HC50/HC55	WT5400
TC53/58	MC3400/MC3450	WT6400
TC77/TC78	MC9400/MC9450	WT6300
ET40/ET45	EC50/EC55	VC8300
ET60/ET65	EM45	PS30

July 2025

Completed by the Zebra Global Enablement Center

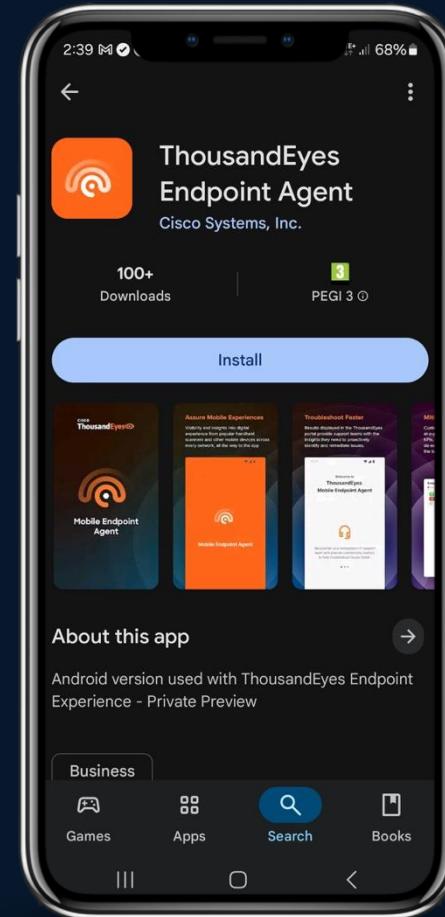
Nayeem

Nayeem Al Tamzid Bhuiyan
Application/System Engineer
Global Enablement Center (GEC)

A hexagonal badge with the Zebra logo in the center. The word "VALIDATED" is printed in white on a blue horizontal bar at the bottom of the badge.

Agent Requirements and Installation

- Current app version on Play Store: 1.2.6
- Supported OS: Android 11 and later
- Installation via Play Store or MDM
 - Play Store - via QR code and activation link
 - MDM (Mobile Device Management)
 - Microsoft Intune
 - Omnistar Workspace ONE
 - SOTI
 - Meraki SM



Mobile Endpoint Agent for Android - Technical Use Cases

Features

Application & Device Performance

HTTP Testing

Network Testing

Device Health (Battery, Memory)

Android 11+ (Zebra)

Connection Stability

Internet Connection Stability (Gateway & Wireless Profile)

Mobile Connectivity (3G/4G/5G/LTE)

Mobile Telemetry (RSSI, RSRP, RSRQ, SINR)

Network Core Diagnostics

VPN Secure Internet Connectivity

Agent-to-Server (ICMP)

Monitoring Availability

Continuous

Testing Capacity

4 concurrent tests

Data Retention

14 days Essentials
30 days Advantage

Core Capabilities

Path Visualizations, Maps, Dashboards, Snapshots and Alerts

Deployment

Intune, SOTI, Meraki SM, WorkspaceOne, Google Play Store

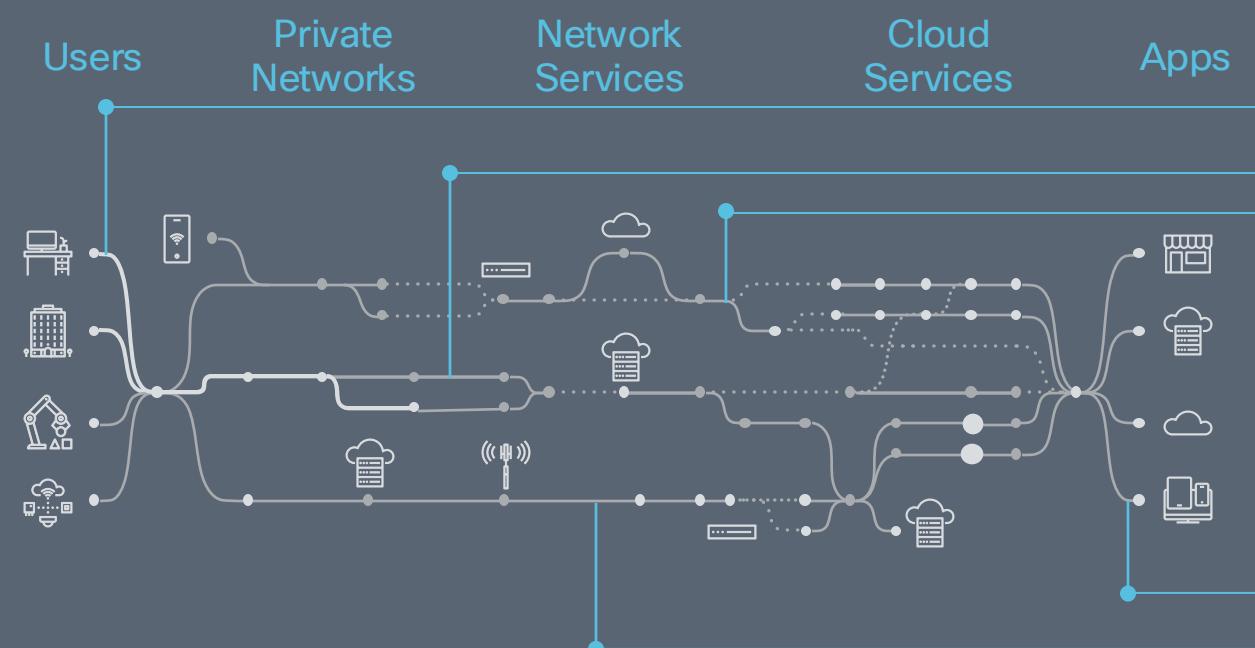
Cloud Assurance

Applications Are Moving to Multiple Clouds



Cloud-native monitoring tools provide siloed data

Incomplete End-to-End View



Complete experience needs data sources from the complete user journey

Cloud-native tools



Invocations

CPU

Disk I/O

Memory

Cloud Resources

DB Load

Network Traffic

Latency

Request count

Isolated Logs and Metrics

Core Use Cases

End-to-End Assurance for Cloud



Inventory

Multi-cloud, multi-account, multi-region cloud inventory for configuration and operational event correlation with synthetics



Application

Monitoring CDN and internet-facing applications and APIs gaining visibility across the entire delivery chain and service dependencies



Hybrid Cloud

Monitor the Direct link, service components, network services offered across and correlate them to cloud events.



Cloud Network

Understand the Hub and spoke architecture of your Cloud networks, correlate with cloud events and traffic analysis.

Cloud Inventory Monitoring

Finding Resources across Cloud Providers, Accounts & Regions

App Down?

Where is this resource?

Infer from billing

Search each region?



$$200 \text{ Accounts} \times 17 \text{ Regions} = 3400$$

Finding Resources | Infosec incident

Search for resources using:

- Name
- Tags
- ARN
- IP addresses

Where is this
resource?

Search each
region?



For example: 200 Accounts x 17
Regions = 3400 possible combinations

Cloud Inventory



Centralize cloud resources
across Cloud Providers,
Accounts & Regions

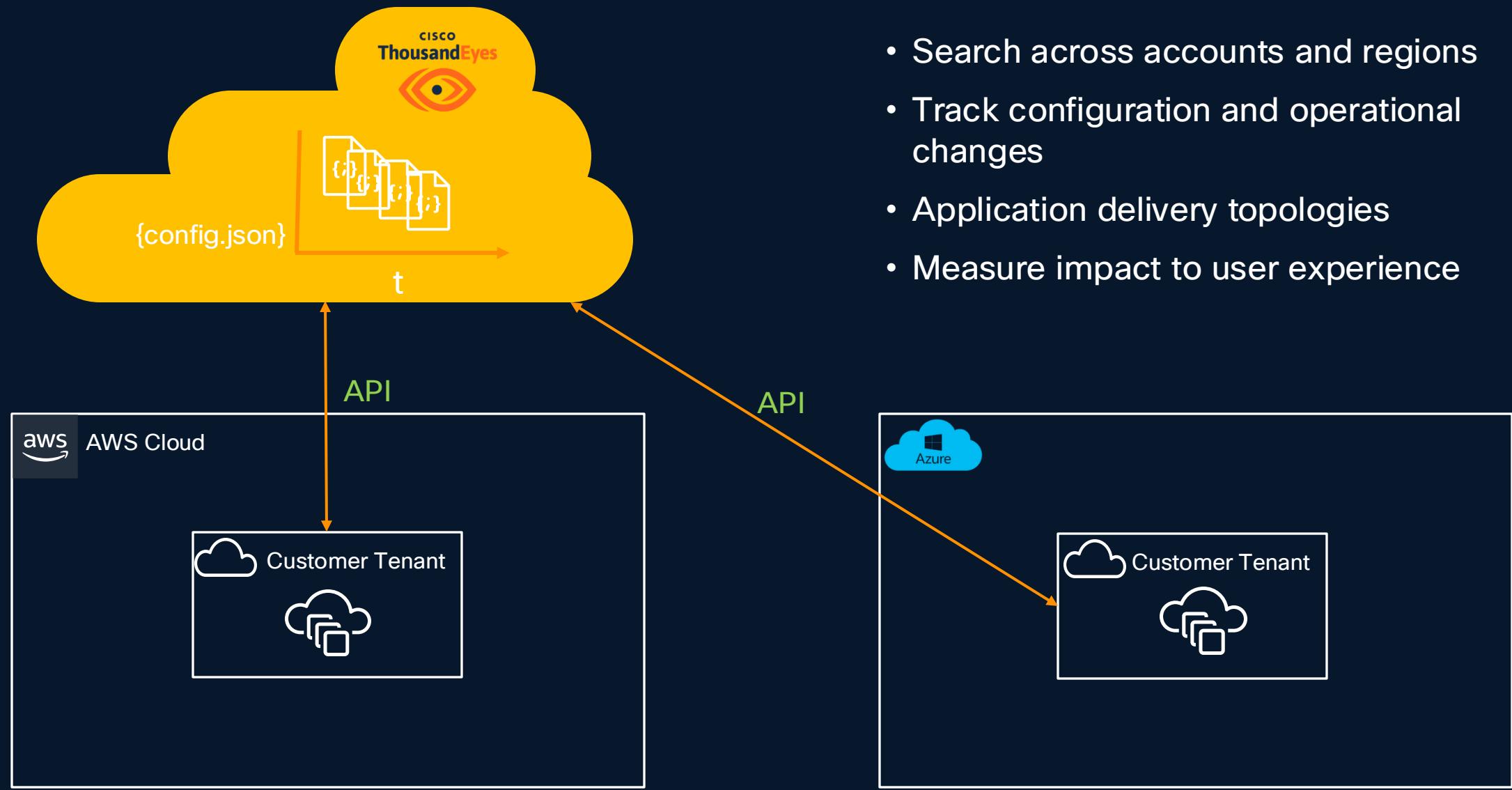


Track Configuration &
Operational Changes



Correlate events to service
impacting problems

Multi-Cloud Inventory Solution



Can you trace the outcome back to a particular configuration change event?

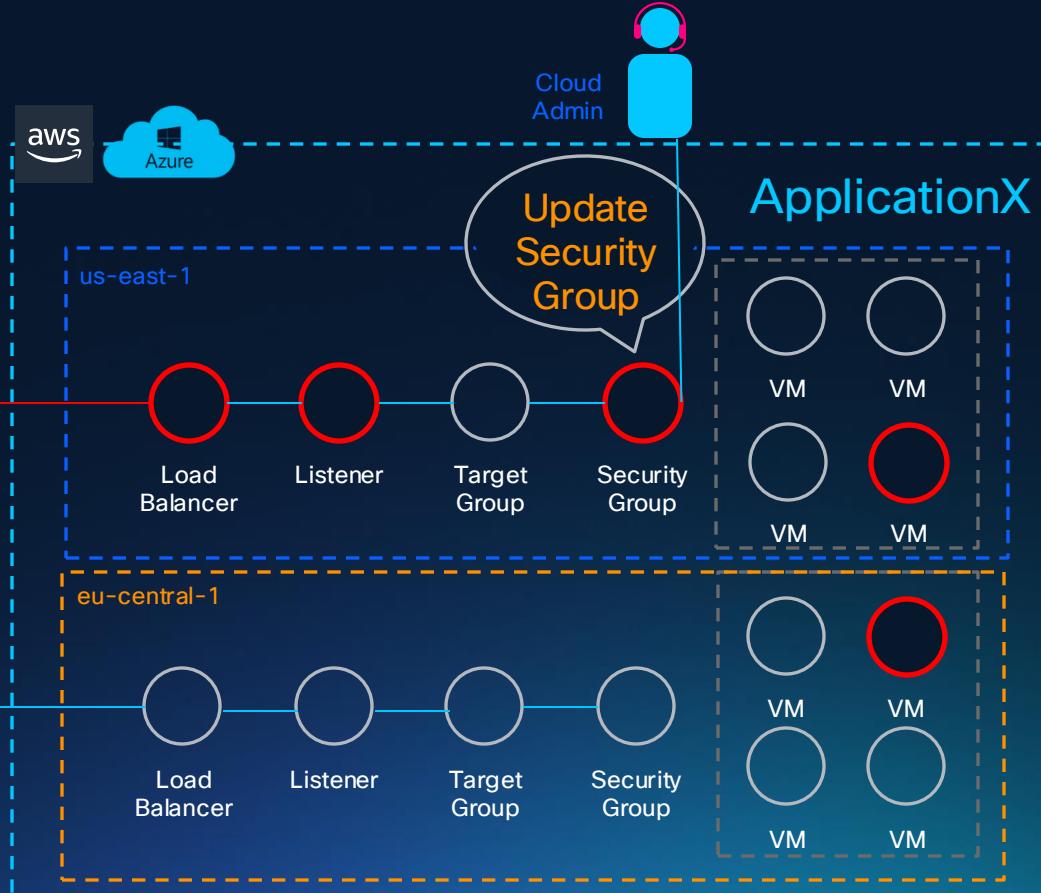
Can't reach the app!



US East Coast Users



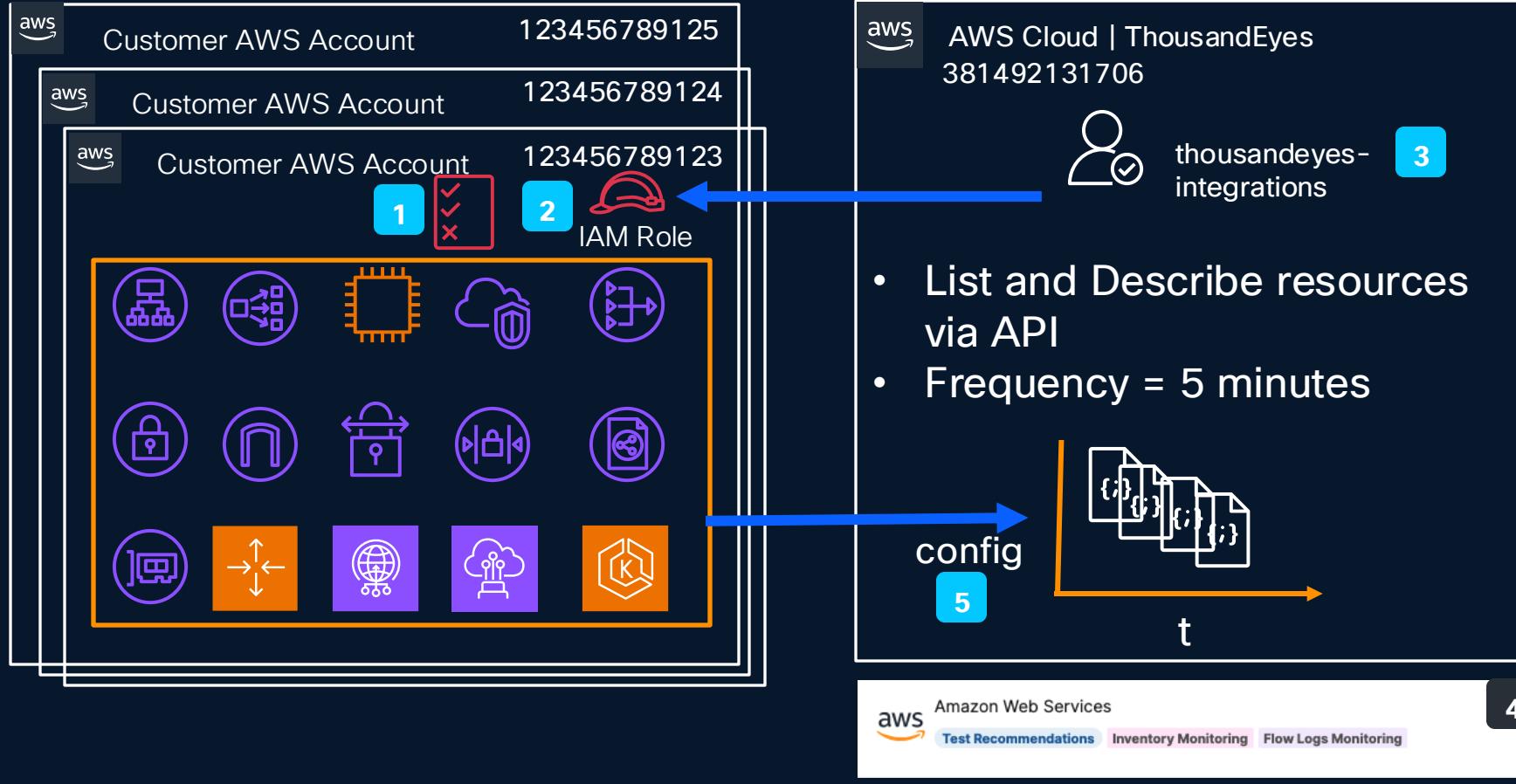
EU Central Users



Example of disruptive changes

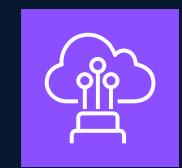
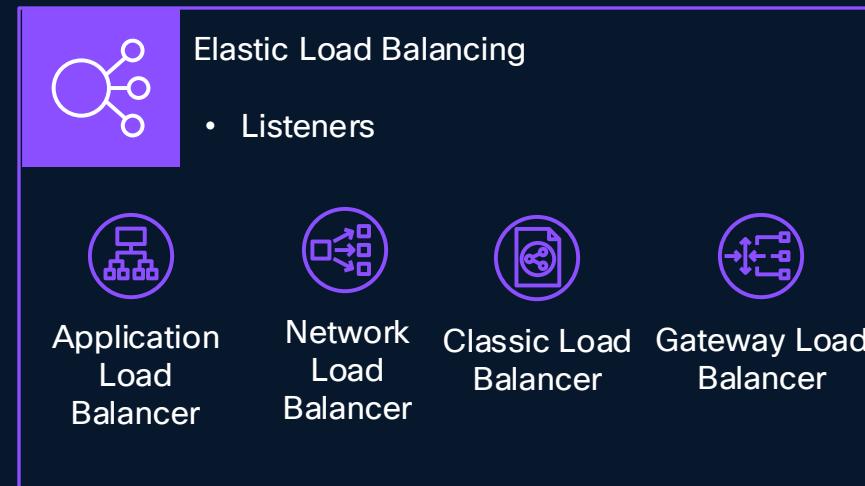
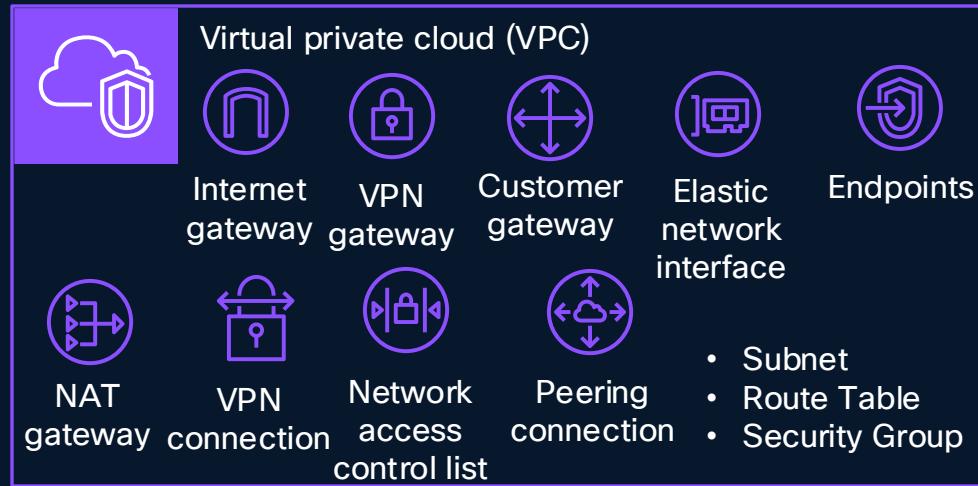
- LB Listener config blocking traffic
- Route table misconfiguration increasing latency
- NAT GW deletion – resulting in outbound loss from private subnets
- TGW route table resulting in cross-VPC communication failures.
- Faulty Load Balancer Health Check resulting in transaction errors
- SSL Certificate update resulting in SSL handshake failures
- DNS record updates resulting in resolution failure
- Direct Connect configuration update resulting in connectivity problems

Inventory Monitoring Integration Components

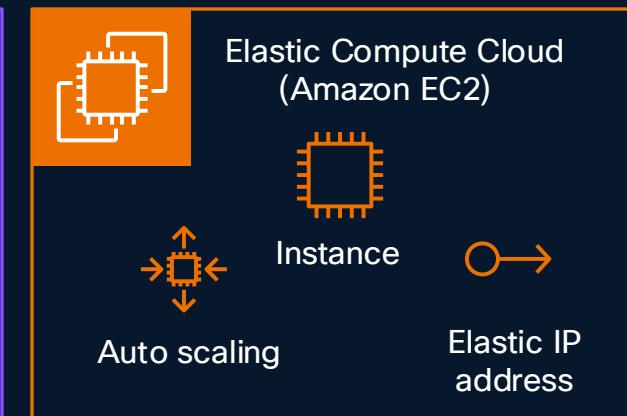
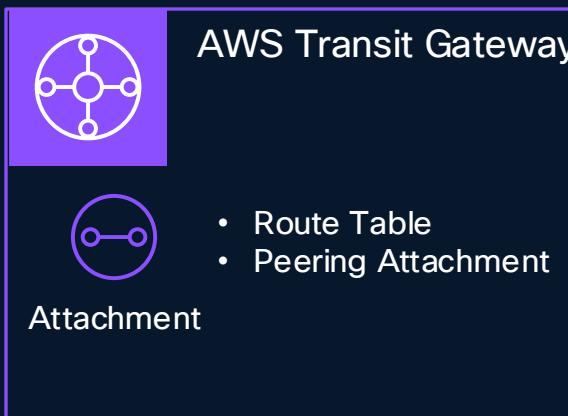


- 1 Create IAM Policies with read permissions to resources
- 2 Create IAM Role and attach permission policies to it
- 3 Allow the thousandeyes-integrations user on the trust policy
- 4 Create a new AWS InventoryIntegration in app.thousandeyes.com
- 5 Wait a few minutes while resource discovery finds all resources and adds them to inventory

Inventory Monitoring Supported AWS Services

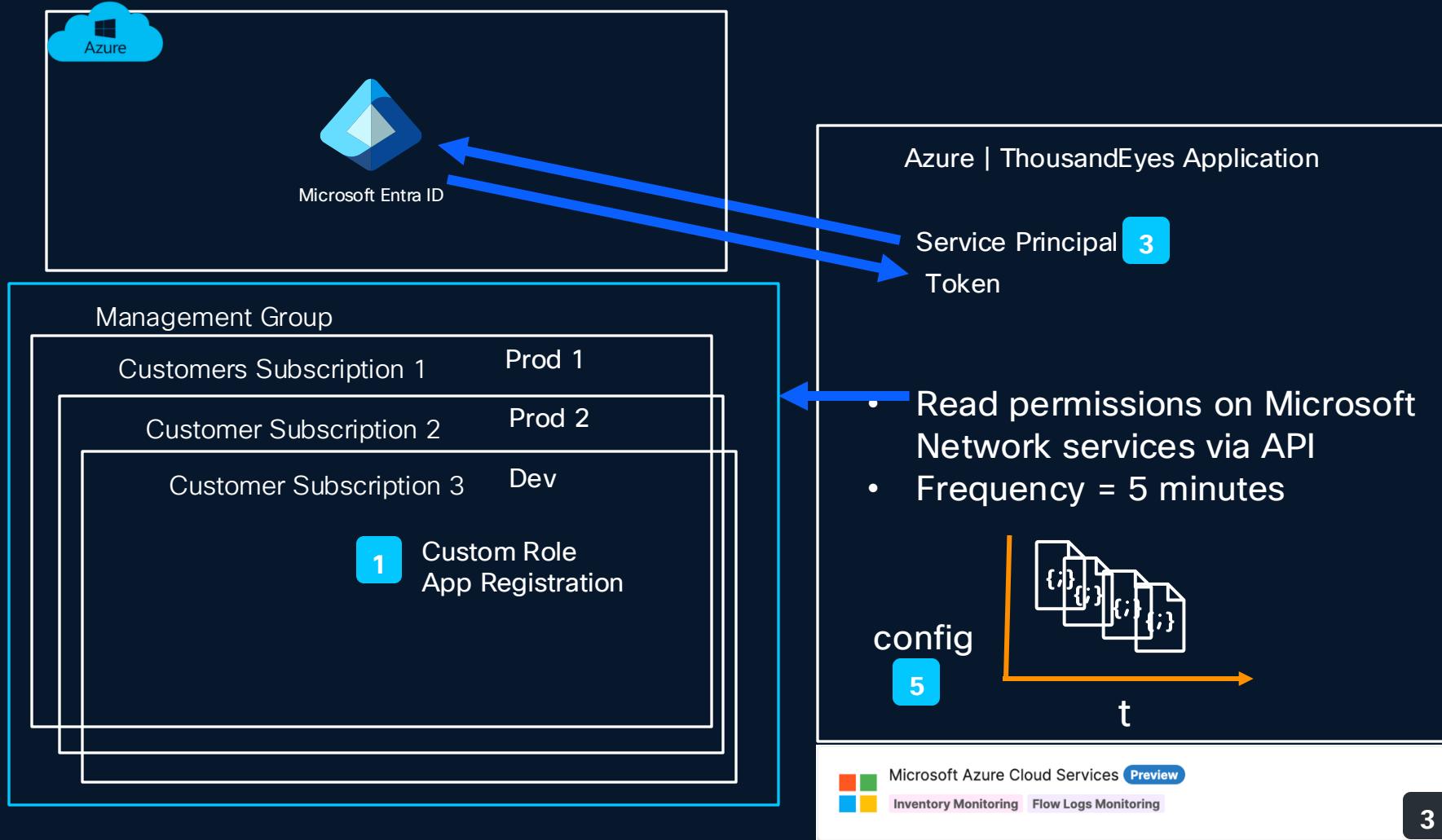


AWS Direct Connect



Elastic Kubernetes Service (Amazon EKS)

Inventory Monitoring Integration Components



- 1 Create custom role and app registration
- 2 Create a Service Principal with the role & subscriptions to be onboarded as scopes
- 3 Create a new AWS InventoryIntegration in app.thousandeyes.com
- 4
- 5 Wait a few minutes while resource discovery finds all resources and adds them to inventory

Inventory Monitoring Supported Azure Services

Networking



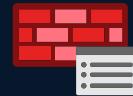
Application-Gateways



Network-Interfaces



Front-Door



Azure-Firewall-Policy



Virtual-Networks



ExpressRoute-Circuits



Connections



Subnet



Bastions



Route-Tables



Public-IP-Addresses



Network-Security-Groups



Load-Balancers



Virtual-WAN-Hub



NAT

Compute



VM-Scale-Sets

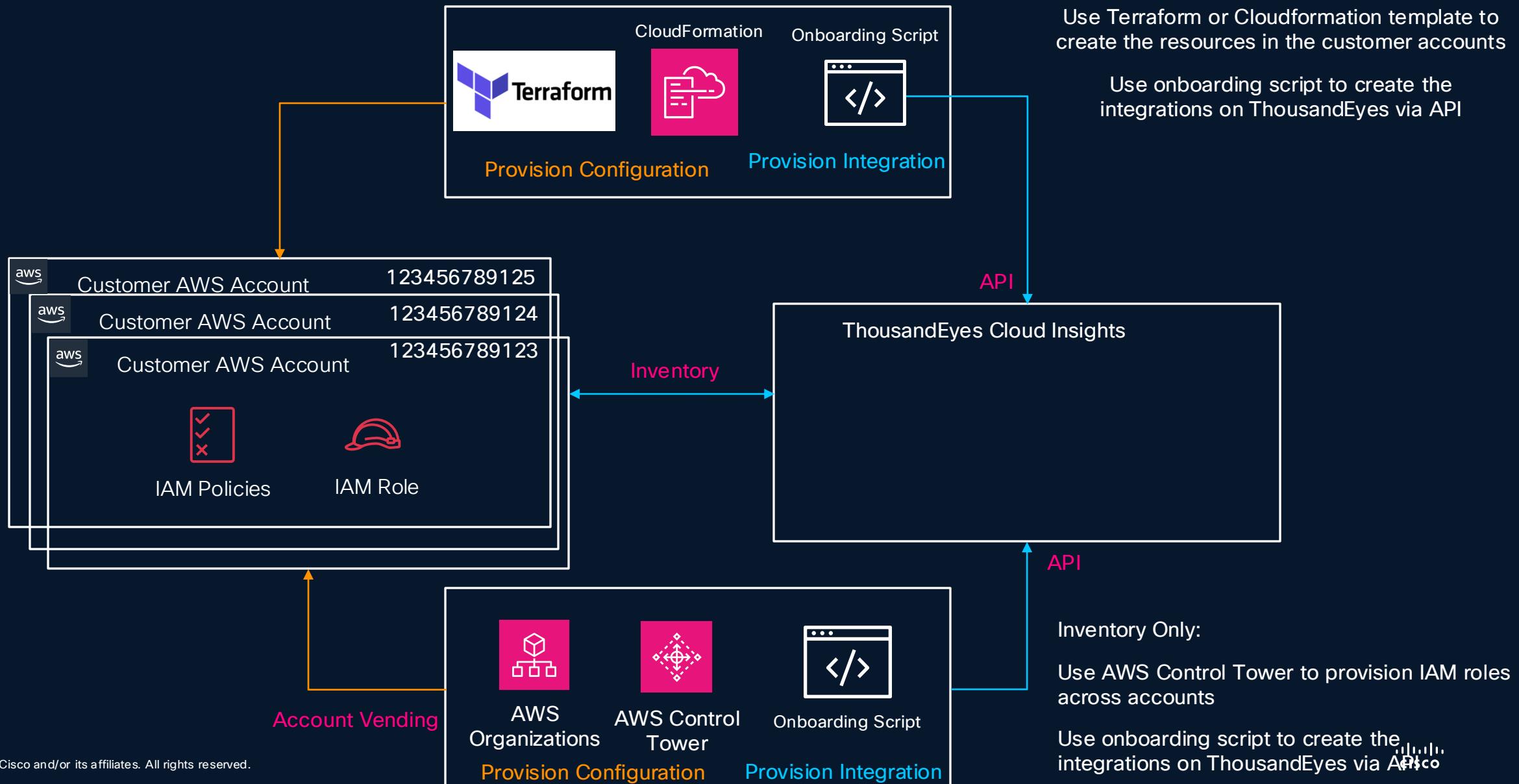


Virtual-Machine

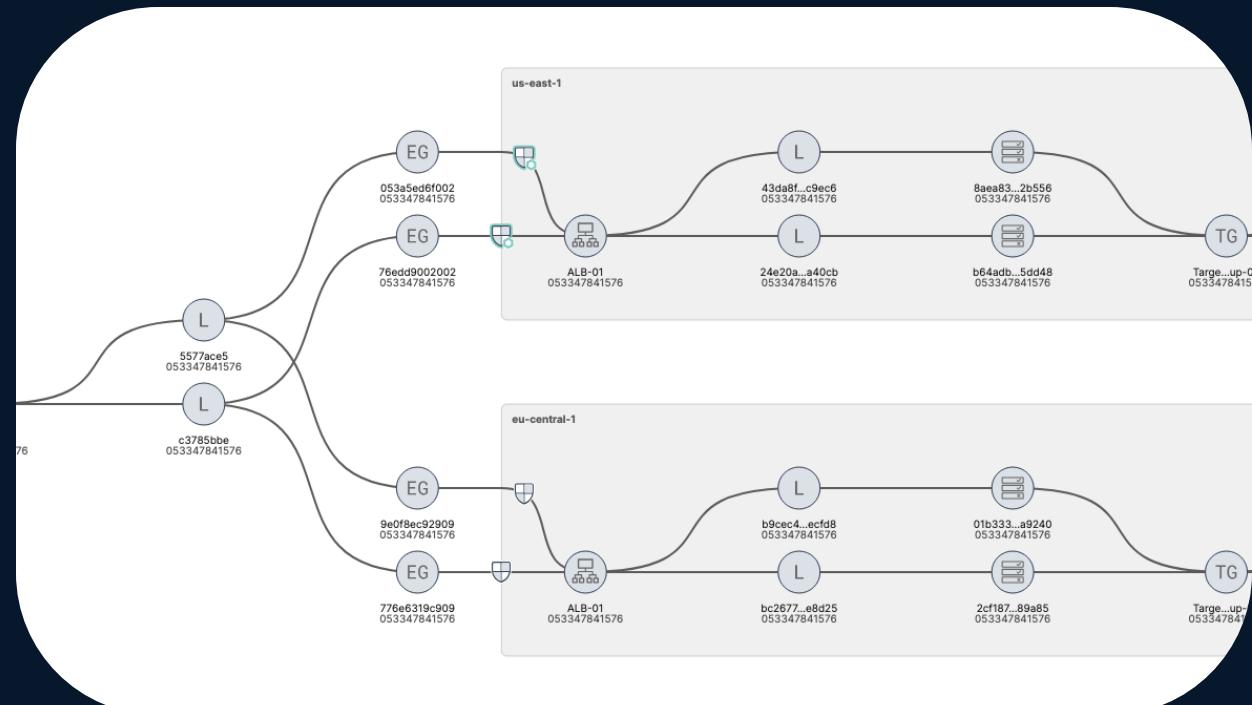
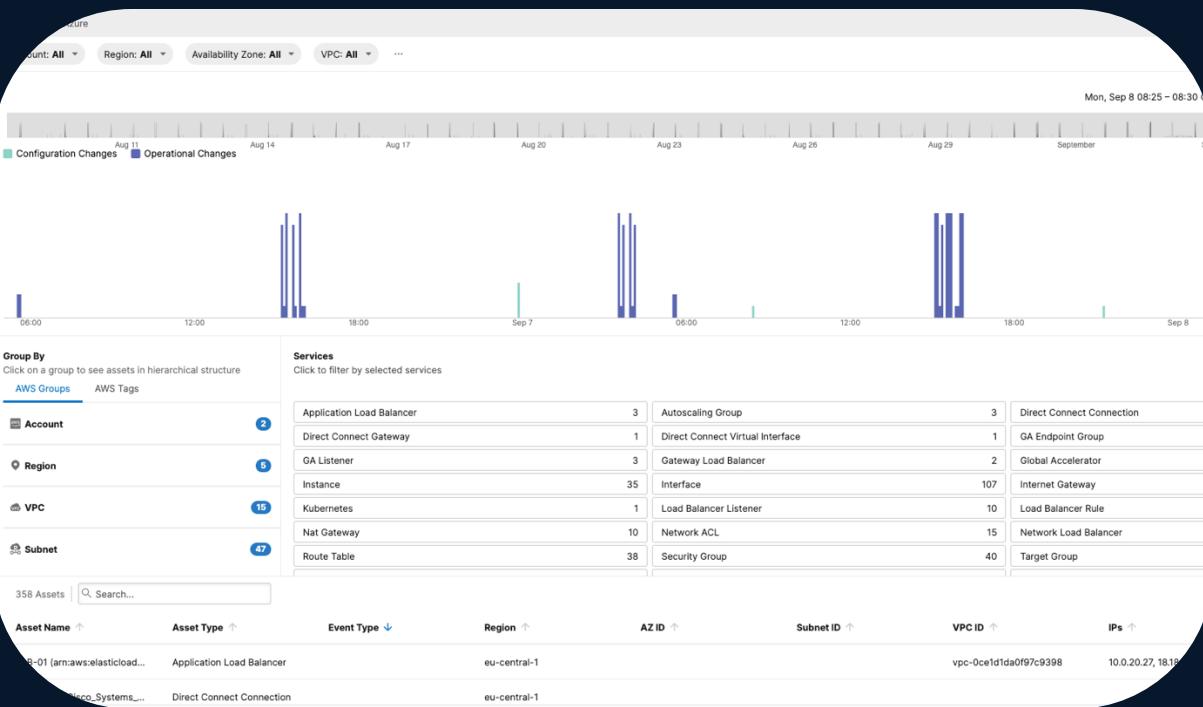


Kubernetes-Services

Multi-Account Onboarding

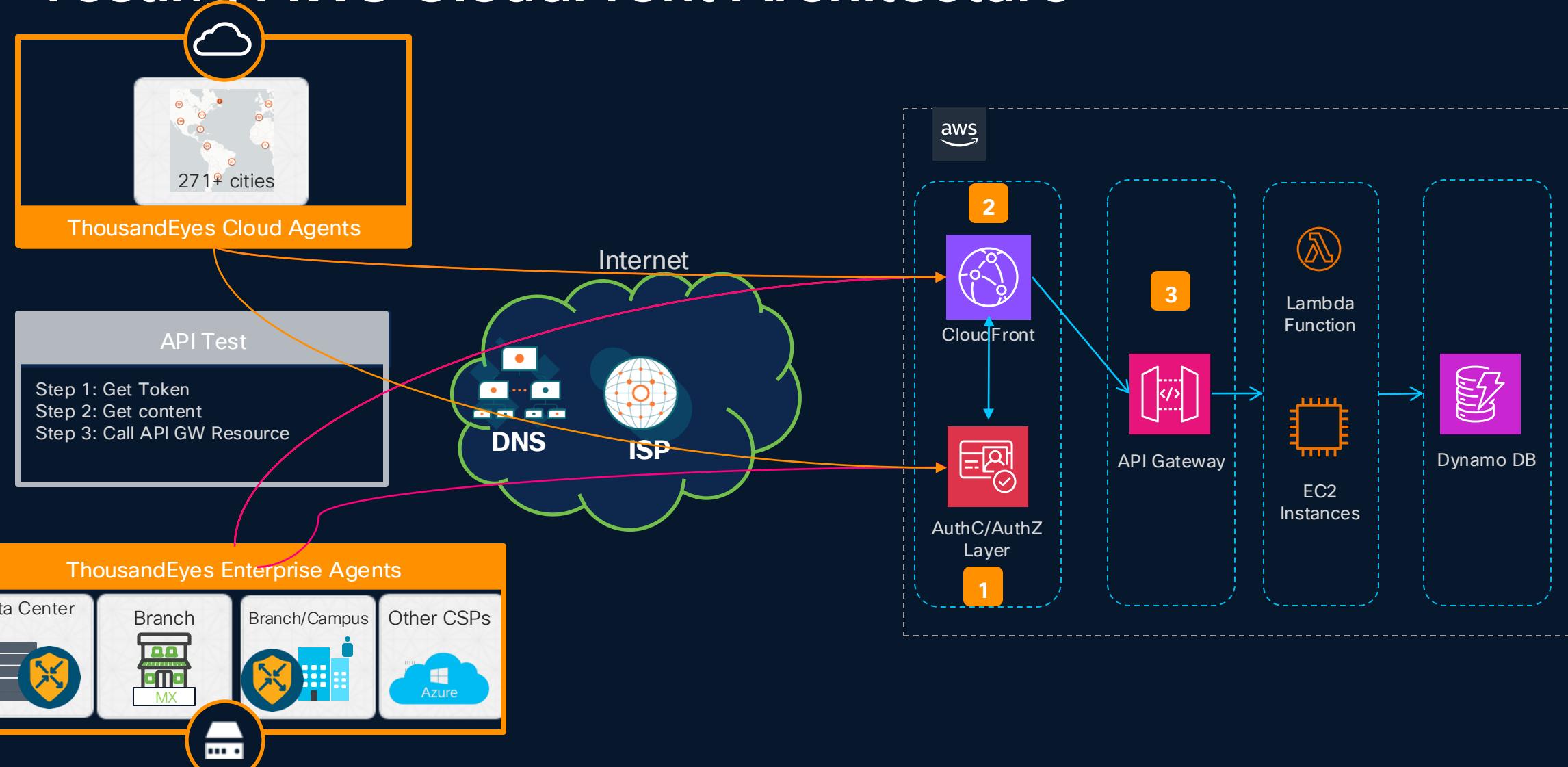


Multi-Account Inventory and Service Configurations

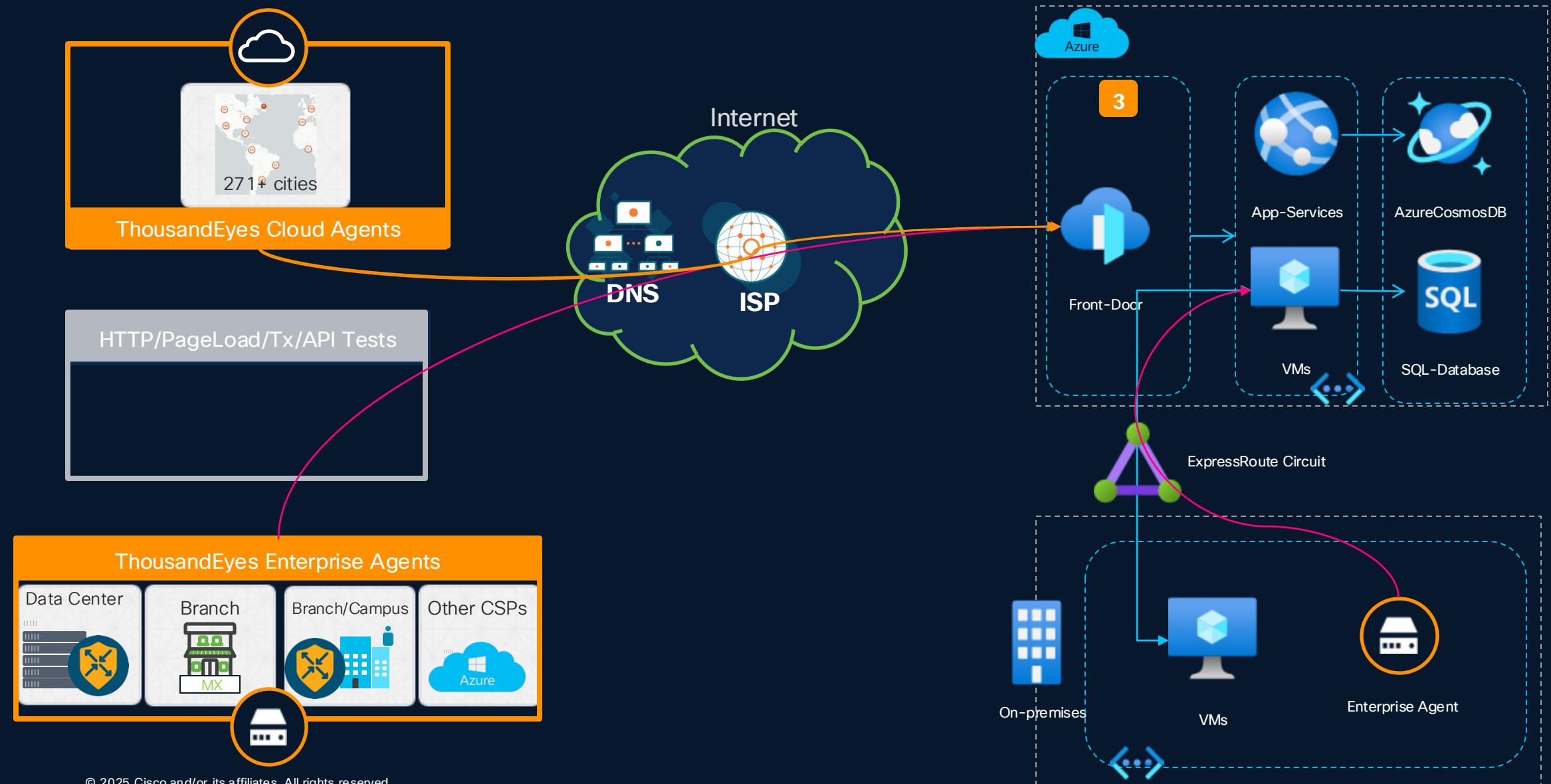


Monitoring Content Delivery Network Services

Testing AWS CloudFront Architecture

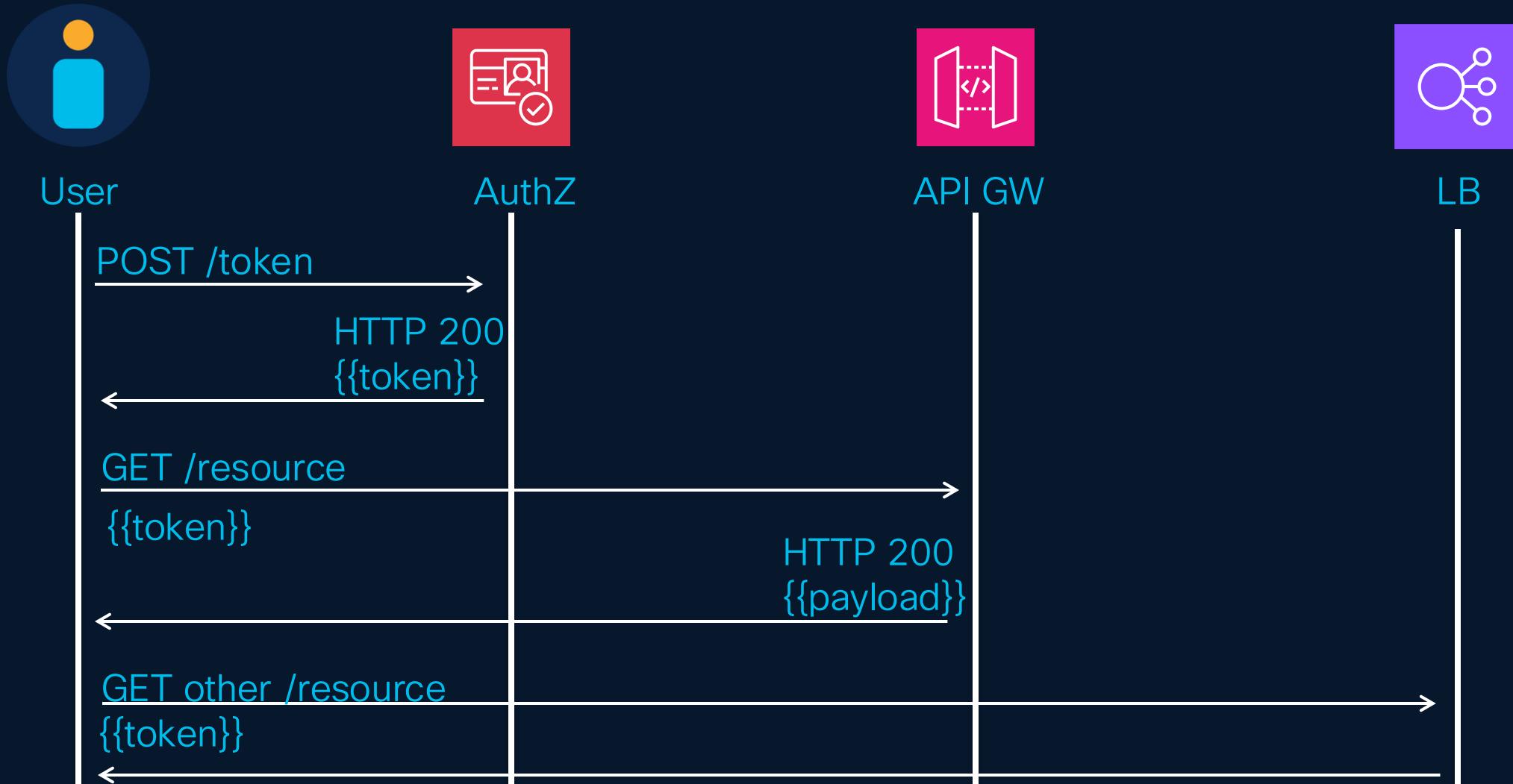


Testing Azure Frontdoor Architecture



API Monitoring

API Workflow



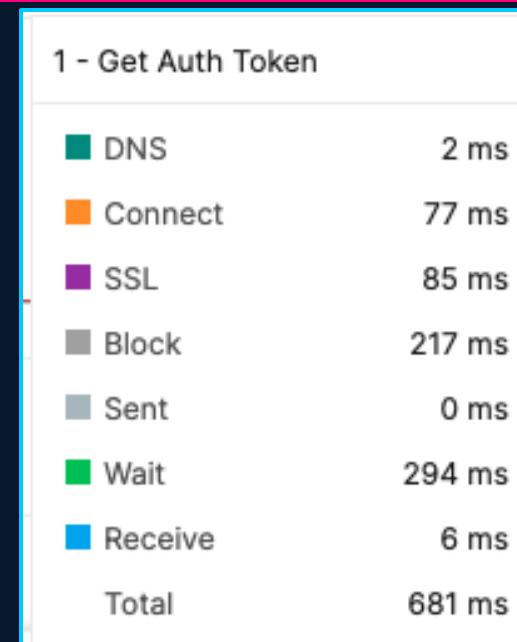
Service Configuration Topology & Event Correlation

Map Table **Details** Brooklyn, NY ▾ Dependent Applications

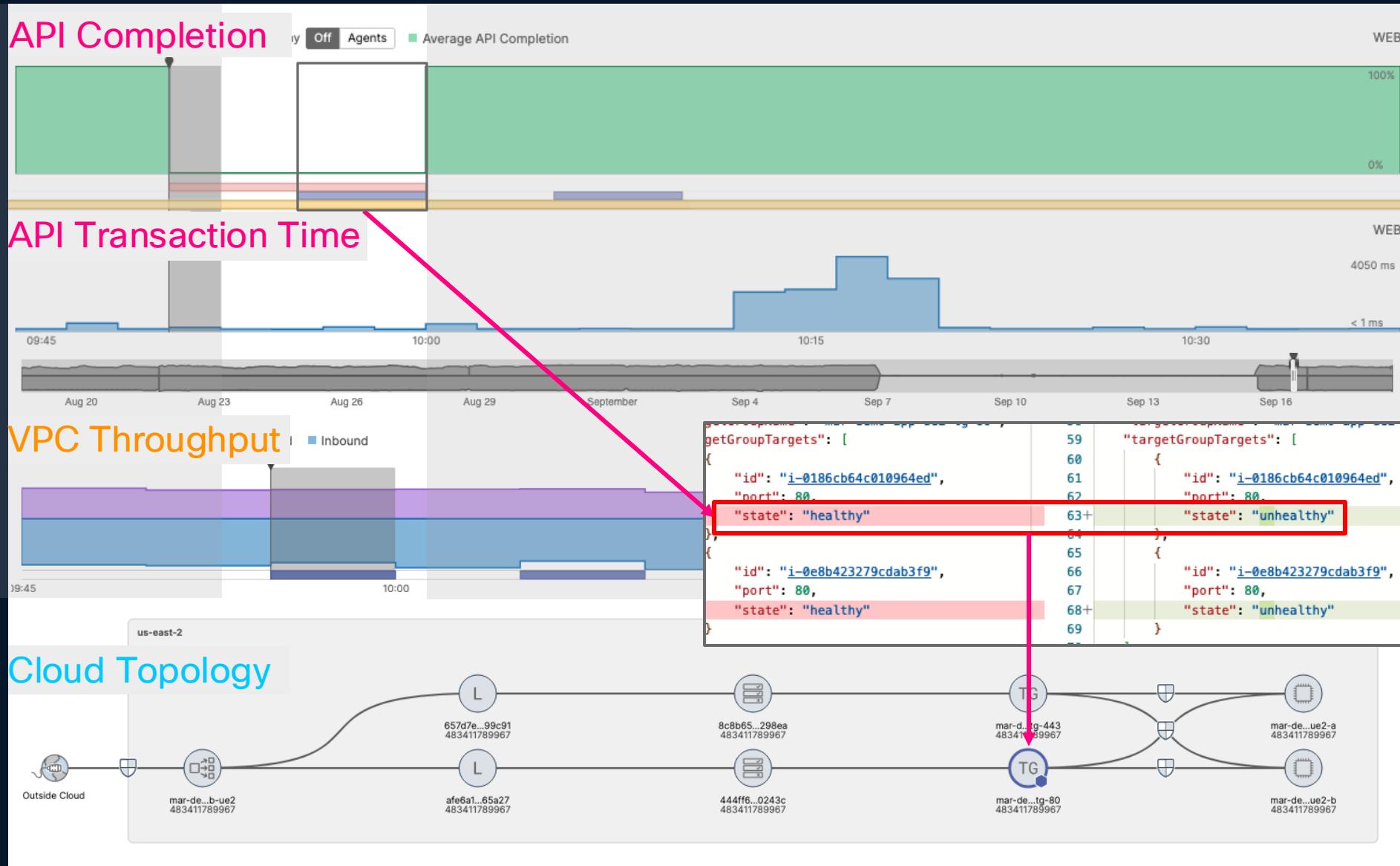
API Steps

1: Get Auth Token https://thousandeyesapi.auth.us-west-1.amazoncognito.com/oauth2/token? POST	Response Code 200	Assertions -	API Call Time 681 ms	Processing Time 67 ms
2: API GW GET https://6ch0m9o4yi.execute-api.us-west-2.amazonaws.com/prod	Response Code 200	Assertions 1 of 1 passed	API Call Time 261 ms	Processing Time 4 ms

- Identify bottlenecks in the application workflow from step-by-step metrics
- Assertions help verify responses
- Correlate API metrics to end-to-end data points: DNS, Network, BGP and more



API Tests: Event Correlation Across Layers



Application

Errors

API Step

- Response Code
- Assertions
- API Call Time
- Processing Time

Flow Logs

Ingress Throughput

Egress Throughput

Rejected Throughput

Connection Rate

Cloud

Configuration changes

Operational Changes

Topology

Flow Log Analysis

VPC Flow Logs

Search...

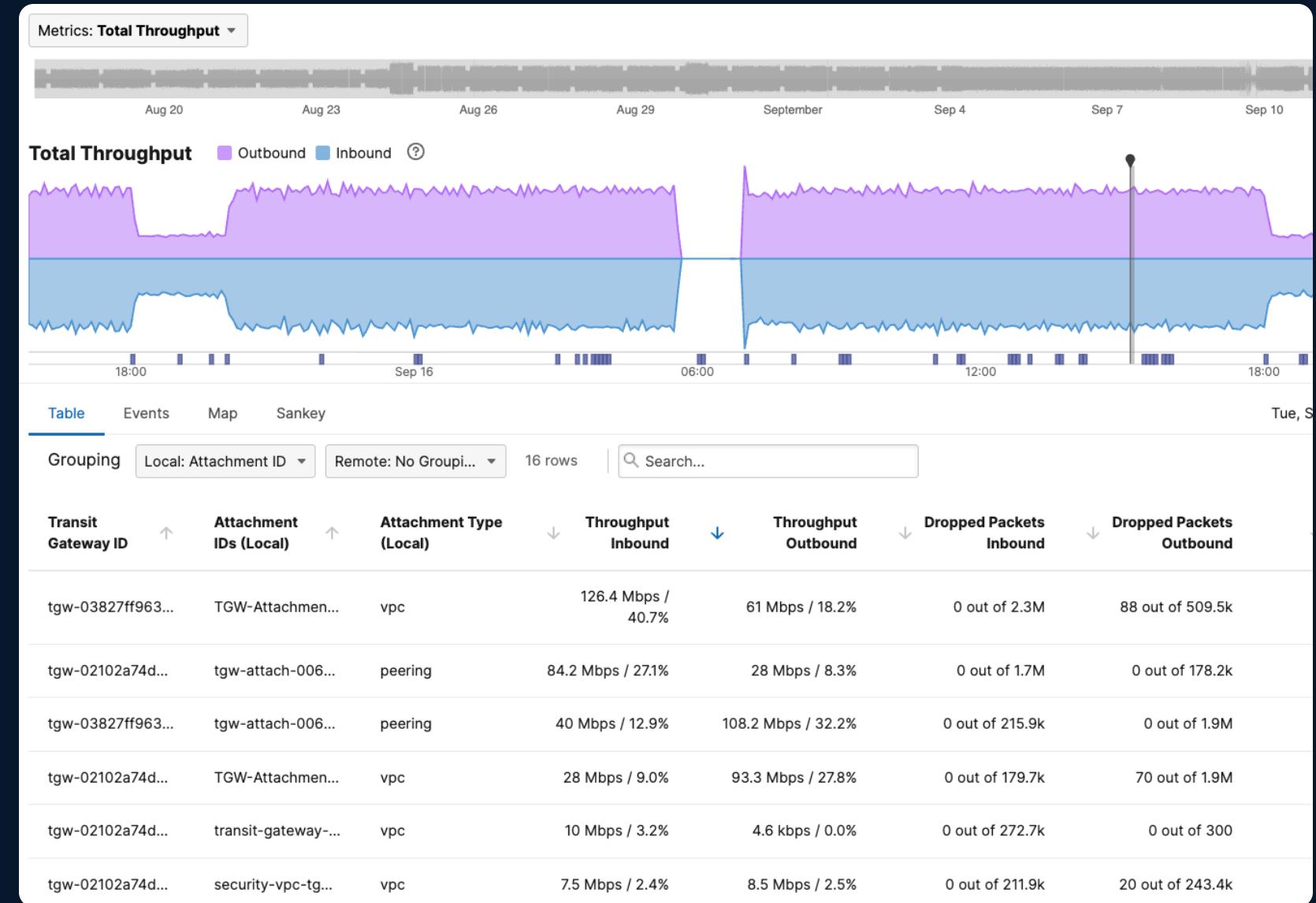
Transit Gateway

- Transit Gateway ID
- Transit Gateway Account
- Transit Gateway Region

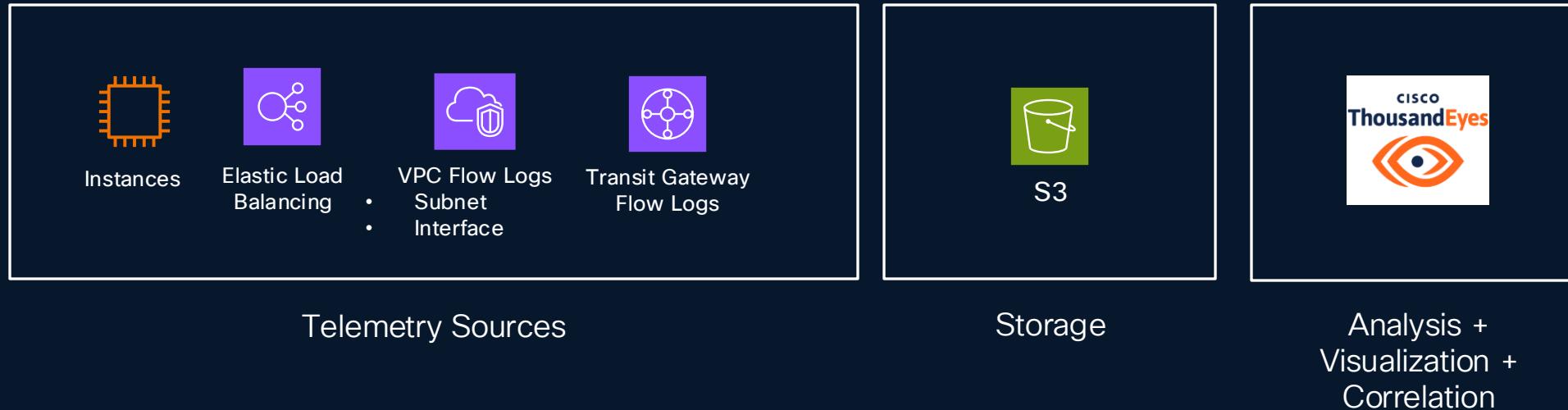
Transit Gateway Attachment

- Attachment Type
- Attachment AZ
- Attachment VPC
- Attachment Subnet
- Attachment ID**
- Attachment Interface
- Attachment VPC Account

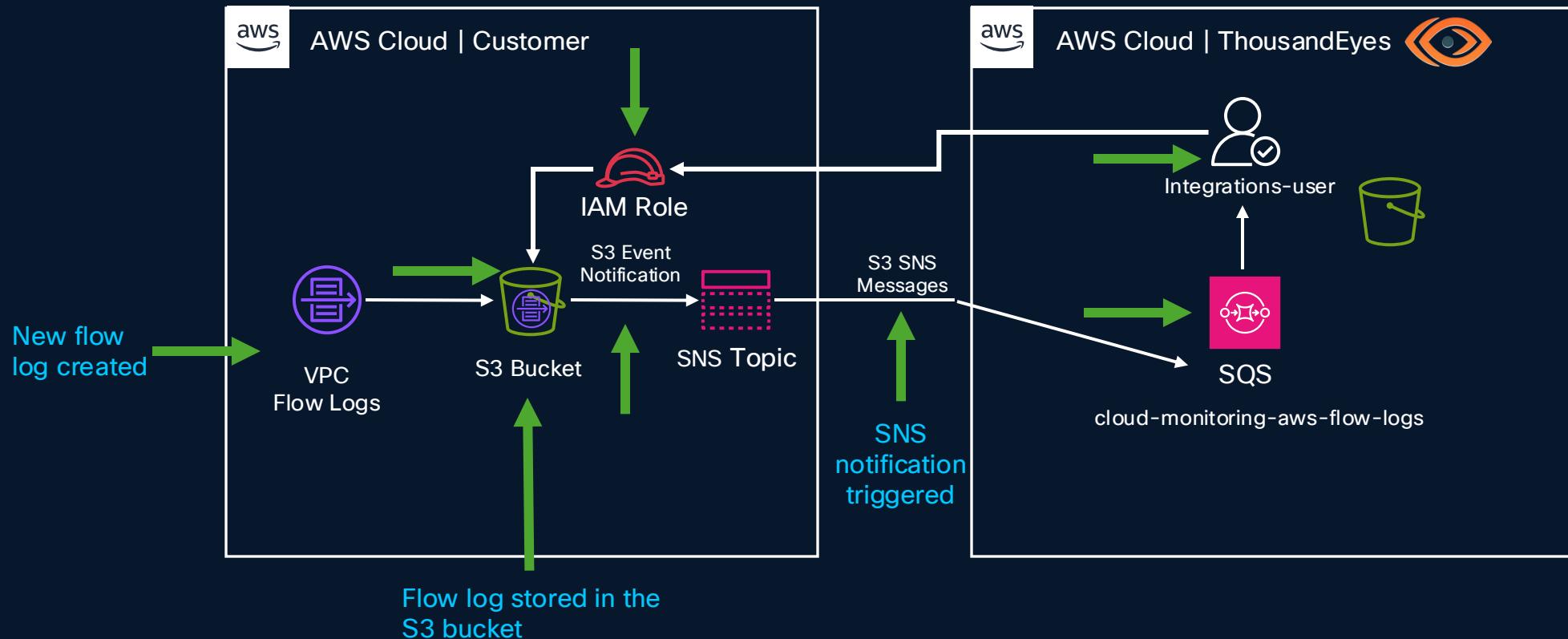
Local: Attachment ID Remote: No Group... 16 rows



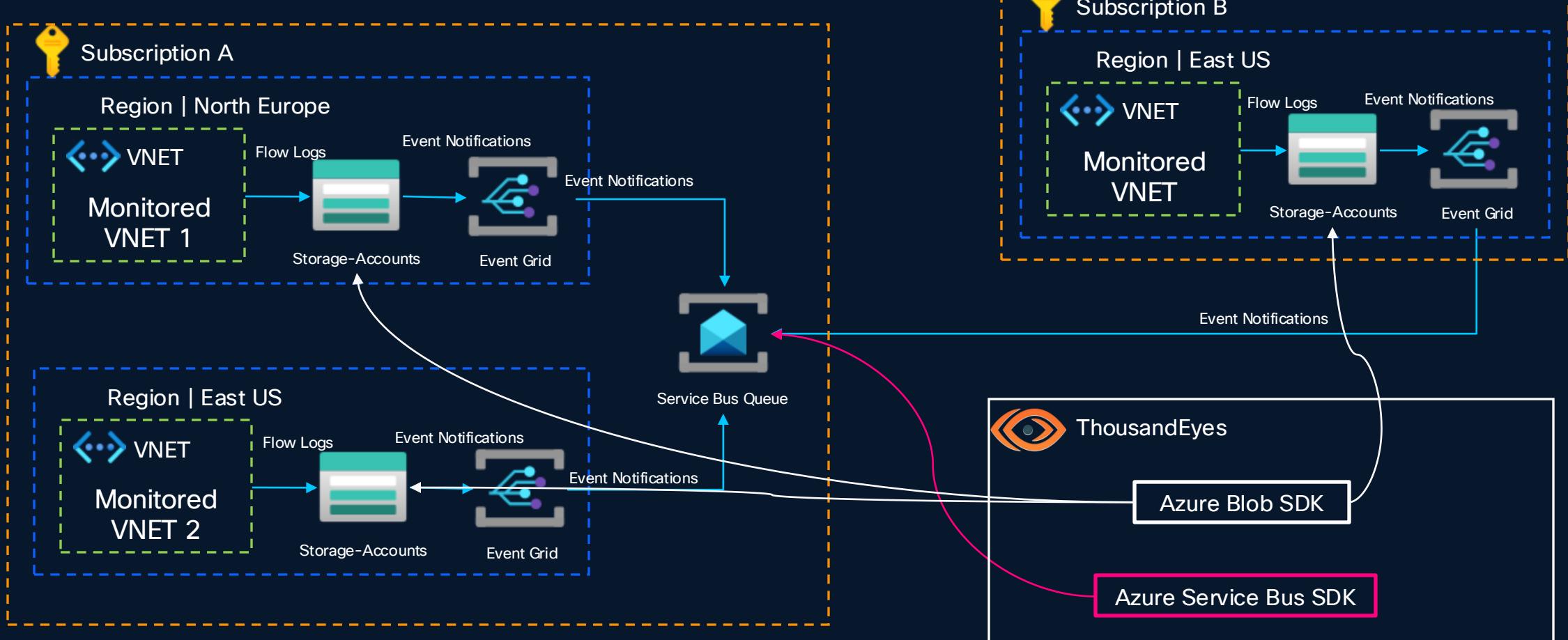
VPC Flow Logs Components



VPC Flow Log Integration Components



VNET Flow Log Integration Components



Support Synthetic Testing

Service Type	AWS	Azure	GCP (Planned Cisco Live US 2026)
CDN	CloudFront	Front Door	Cloud CDN
Global Networking	Global Accelerator	Front Door / Traffic Manager	Network Service Tiers
Load Balancing	Network Load Balancer Application Load Balancer	Load Balancer Application Load Balancer	Cloud Load Balancing
Hybrid network	Direct Connect	Express Routes	Cloud Interconnect

AI Innovations

Event Detection

- ML-based engine that auto-detects and correlates anomalies in synthetic tests and raises “events” when metrics deviate from learned baselines
- Classifies problem domain (local network, network path, network outage, proxy, server)
- Uses Cisco AI Assistant (LLMs) to summarize each event and its recurrences in plain language
- Events feed alert rules, webhooks, and dashboards so NOC/SRE teams can plug AI-detected issues into existing incident workflows

The image shows two screenshots of the Cisco Event Detection interface. The top screenshot displays the 'Server Issue' event details. It includes a summary box, a map showing 'Affected Agents' in North America and Europe with a total of 10 issues detected, and a table of 'Affected Items' for 'HTTP Server' tests. The bottom screenshot displays the 'Proxy Issue detected' event details, showing a map of South Africa with 1 issue detected, and a table of 'Affected Items' for 'HTTP Server' tests.

Server Issue

Summarize Event | AI-generated
November 13, 2025 15:20 (America/Los_Angeles)
Significant number of issues detected with
to HTTP Receive Timeout

Event Type	Server Issue
Duration	4m
10 Agents Affected	1 Test Affected

Affected Items

Test Name	Test Target	Test Type	Affected Agents	Account Group
HTTP Server	HTTP Server	HTTP Server	10	1

Proxy Issue detected

Affecting Proxy

Proxy Issue Details
Significant trouble testing through
Proxy:

Event Impact	Start Date (UTC)	Affected Agents
High	February 26, 2024 08:20	7
	Duration: 08:20-08:24 (4m)	Unique Tests: 9

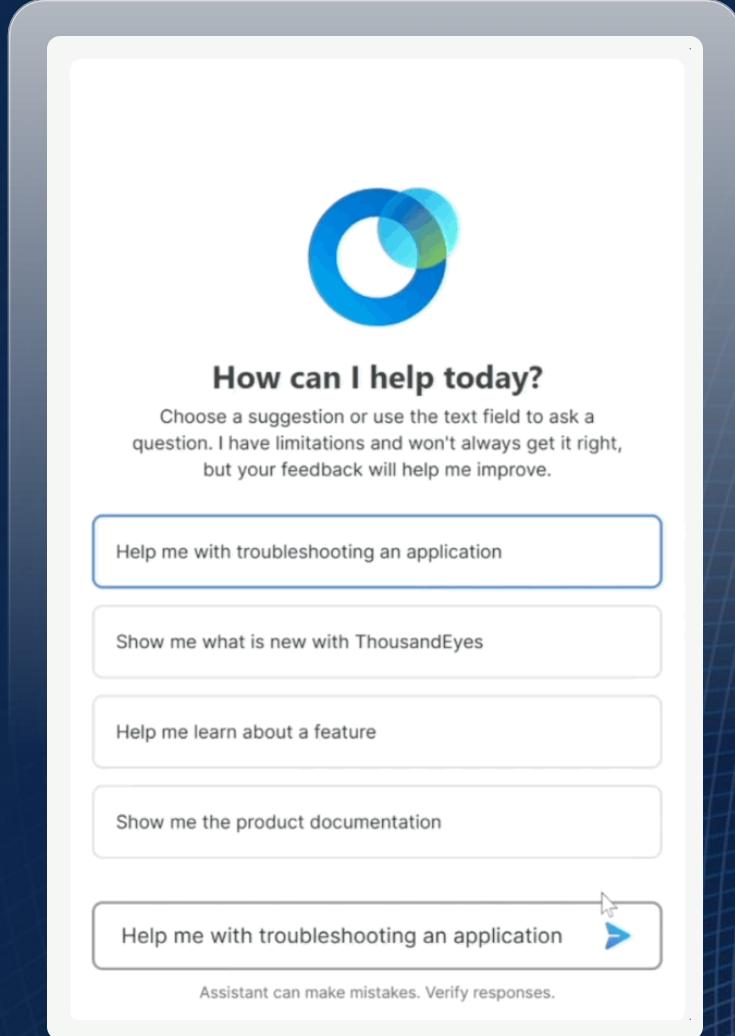
Affected Items

Test Name	Test Target	Test Type	Affected Agents	Account Group
HTTP Server	HTTP Server	HTTP Server	2	1
HTTP Server	HTTP Server	HTTP Server	2	1
HTTP Server	HTTP Server	HTTP Server	1	1
HTTP Server	HTTP Server	HTTP Server	1	1
HTTP Server	HTTP Server	HTTP Server	1	1

Cisco AI Assistant

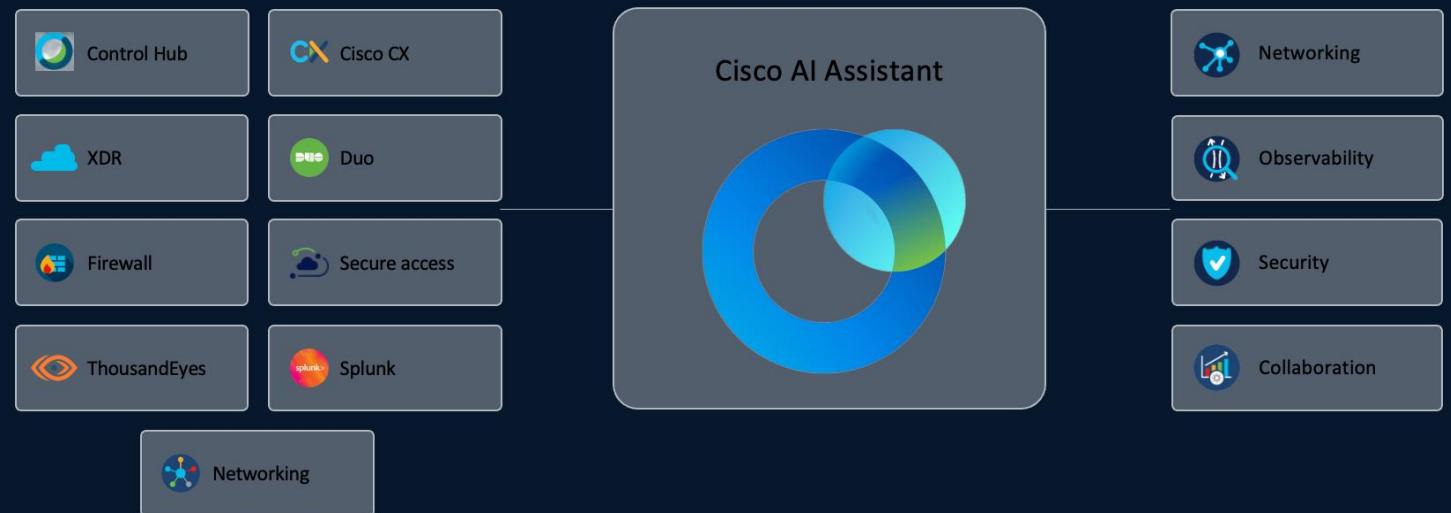
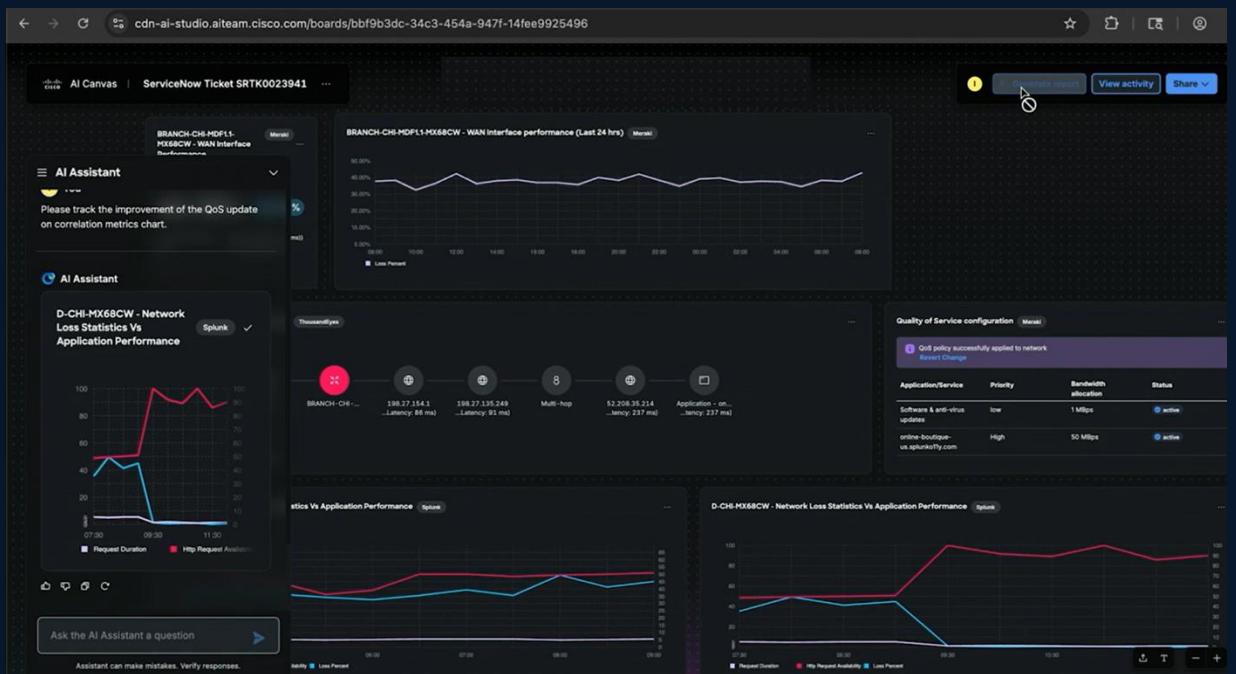
Transformative GenAI innovations unlock expertise for every user, advancing Assurance across owned and unowned network

- **Troubleshooting skill:** Accelerate root cause analysis and resolution with guided troubleshooting workflows that span Internet outages, organization-wide events, and alerts
- **Views explanations:** Pinpoint issues in seconds with AI-generated explanations of in-product views and visualizations
- **Test analysis:** Continuously analyze test settings and results at scale to ensure coverage of critical services that fuel your digital experiences
- **Documentation skill:** Summarize product knowledge and expertise from the leader in Internet intelligence in real-time to demystify Assurance



AI Canvas

- AI Canvas is a **generative UI** shared workspace that sits on top of Cisco's Deep Network Model and AI Assistant to unify NetOps/SecOps/AppOps views
- Ingests real-time telemetry from tools like ThousandEyes, Meraki, and Splunk to auto-build incident-specific, time-aligned dashboards
- Uses AgenticOps multi-agent workflows to correlate issues and propose remediation

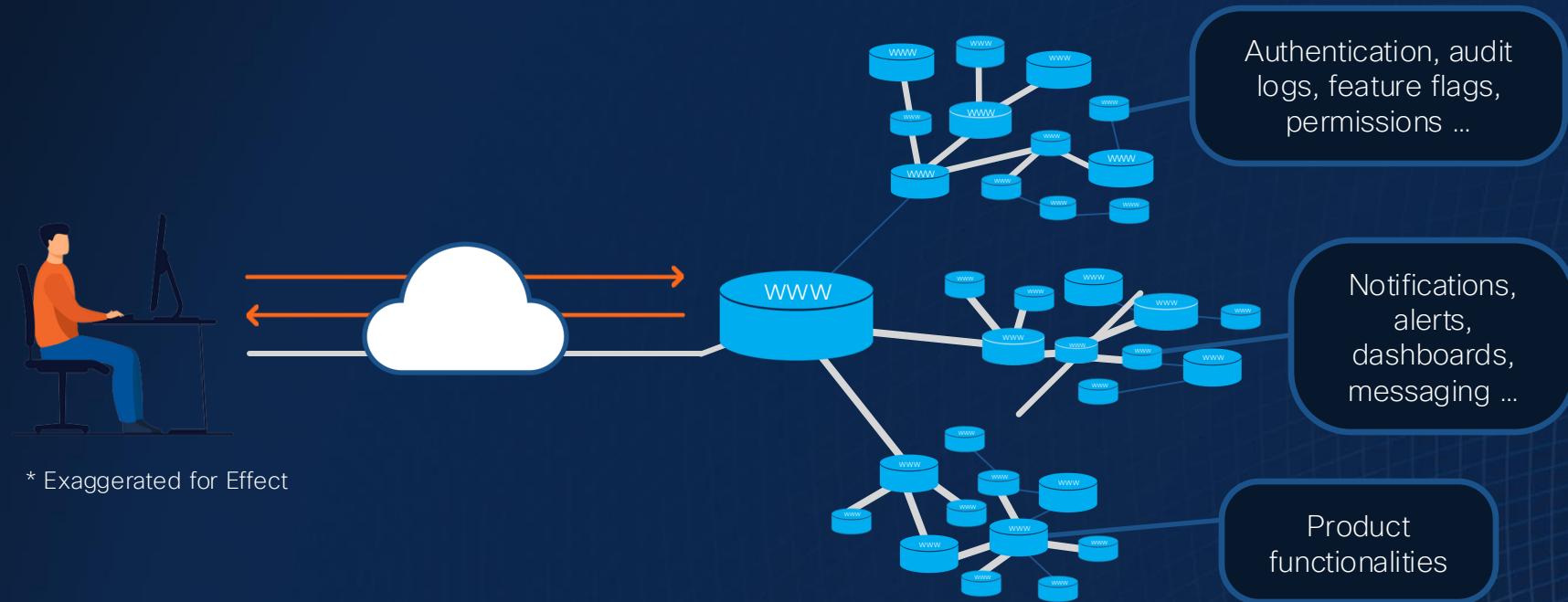


Splunk Integrations

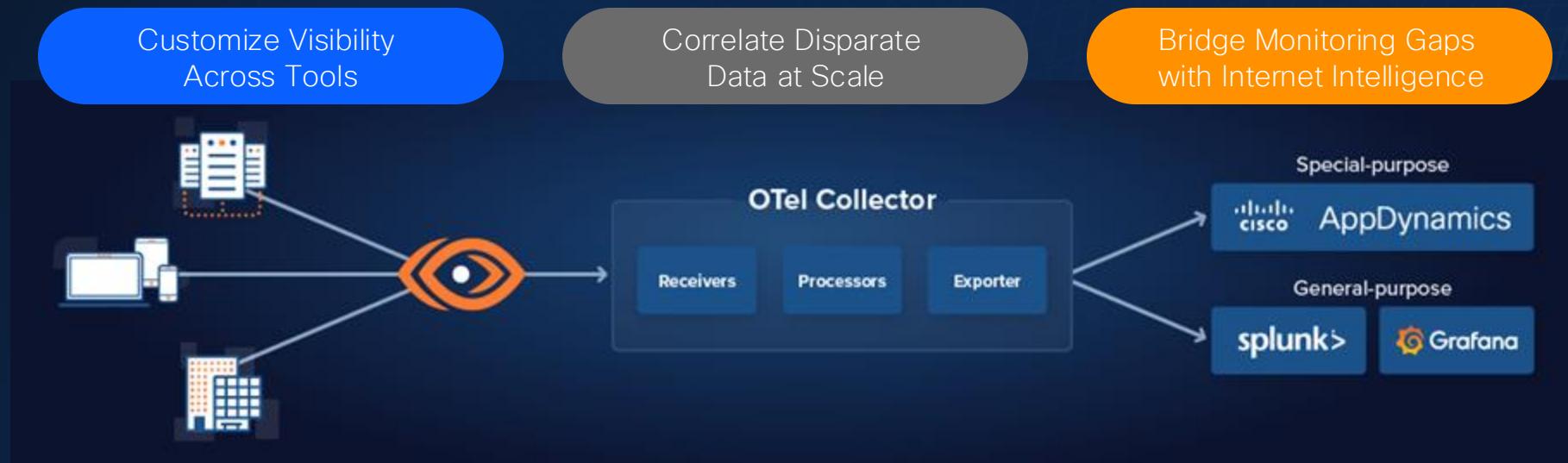
Evolution of Application Architectures



Evolution of Application Architectures

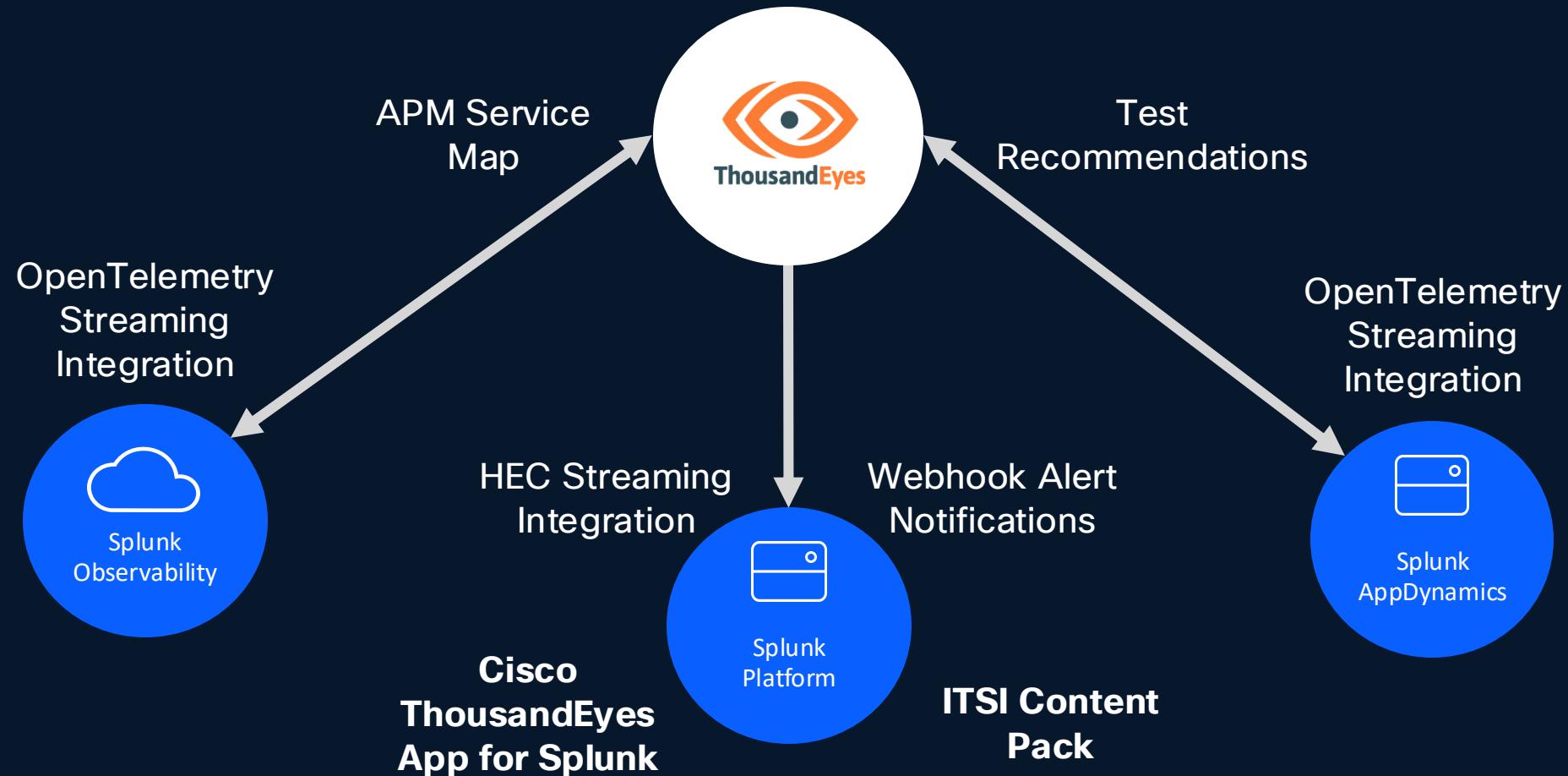
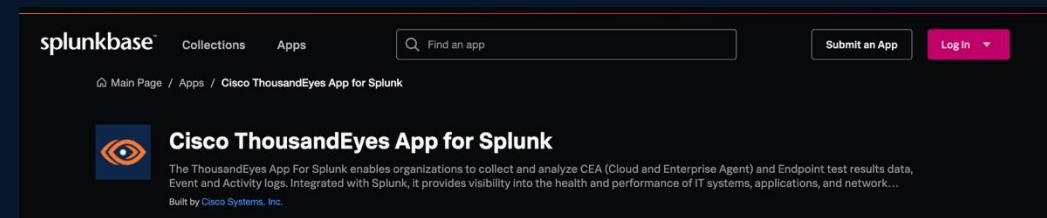


OpenTelemetry



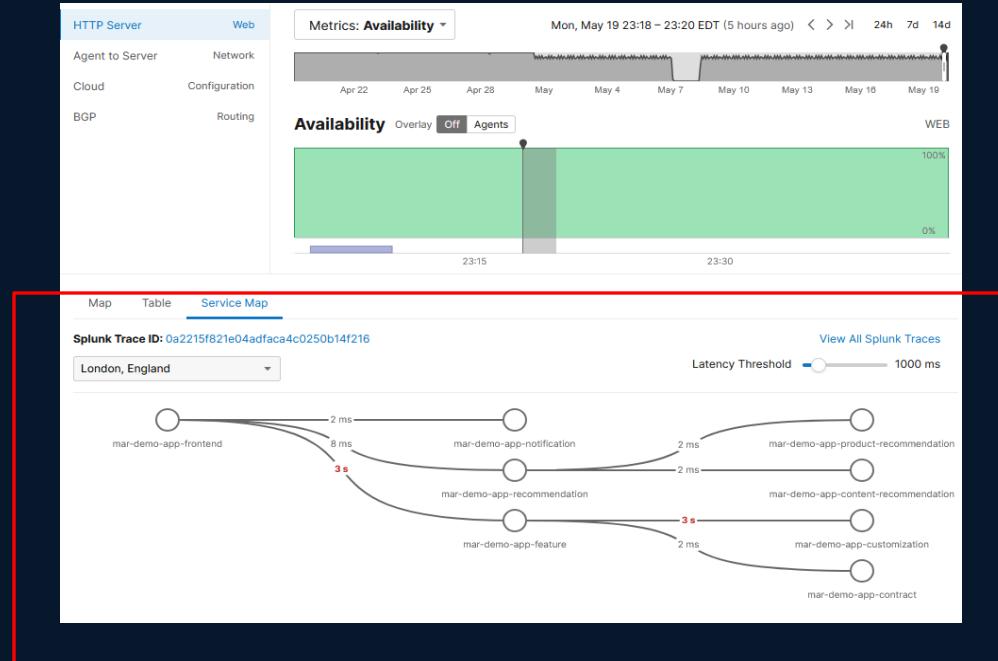
Splunk + ThousandEyes

Contextual Data Sharing and Enrichment

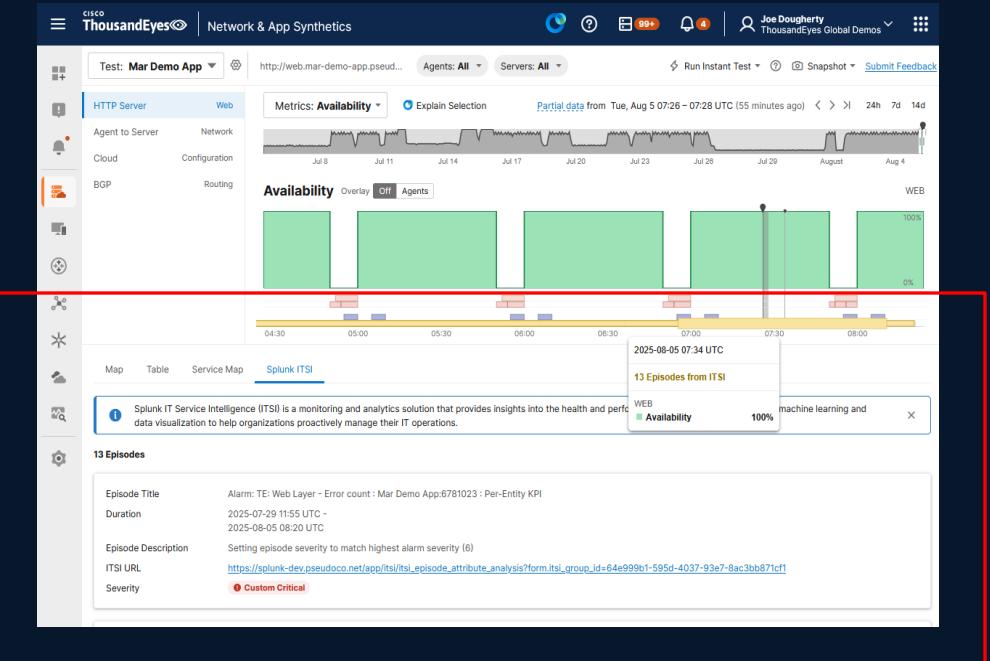


Splunk + ThousandEyes

Contextual Data Sharing and Enrichment

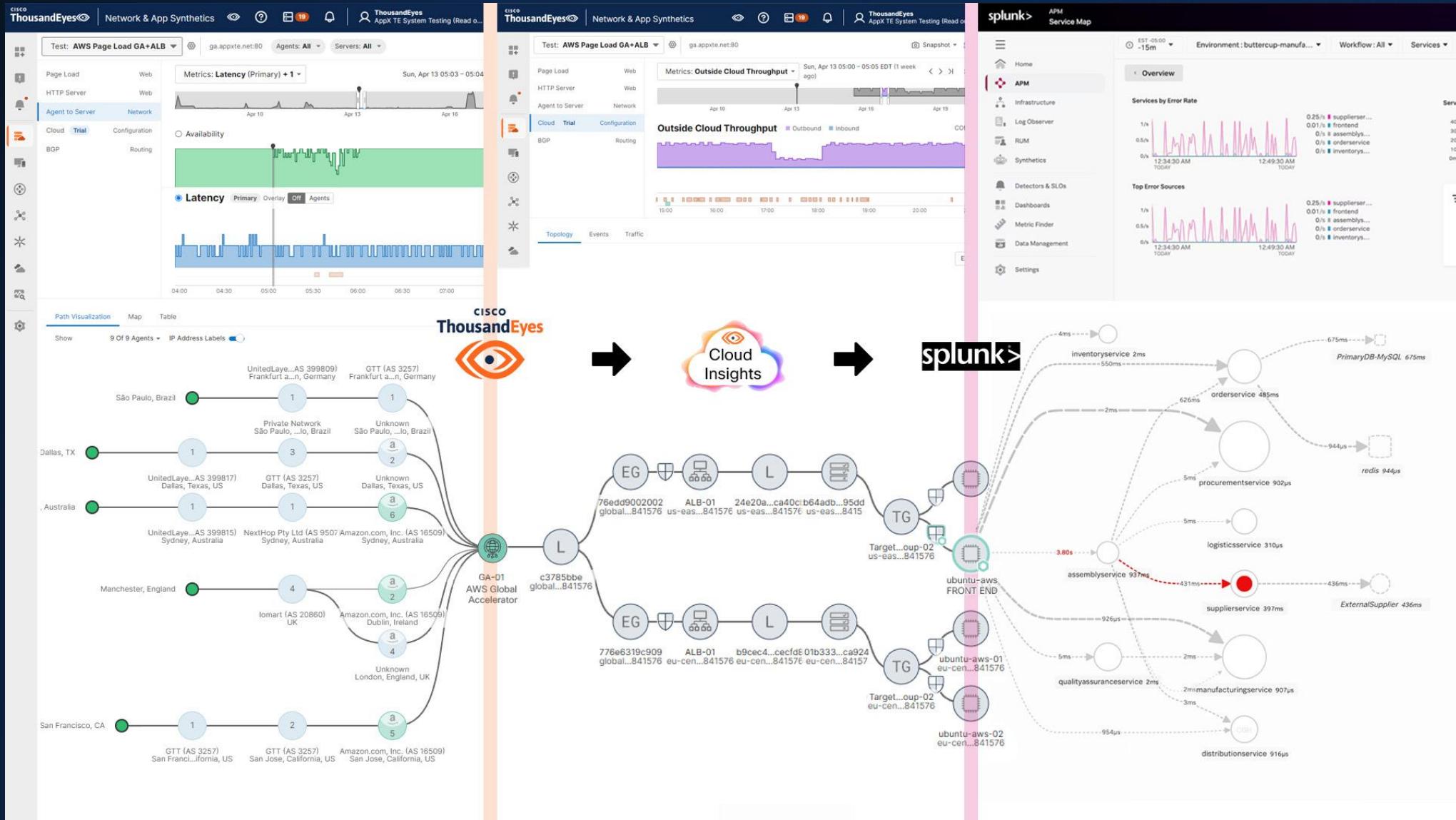


Splunk Service Dependency Map in ThousandEyes



Splunk ITSI Event Context data in ThousandEyes

End-to-End Visibility



IT Service Intelligence: Top-Down Business Visibility

From Reactive to Proactive Starts with Intelligence



Baseline and detect

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

See across environments

Troubleshoot mission-critical apps and infrastructure



Localize and diagnose

Visualize, localize, and diagnose across every network segment

Guided insights

Prioritize issues based on business impact



Mitigate and remediate

Closed-loop actions across digital domains and teams

Proactive response

Prevent outages & accelerate MTTR with guided root cause analysis



Predict and optimize

Forecast disruptions, optimize path, and plan connectivity and migrations

Unified workflows

Standardize observability practices across teams

CISCO Engage !

Thank you!

