ThousandEyes
part of Cisco

Digital Assurance

Forrest Burchell
Leader, Solutions Engineering

Table of Contents

1. Solution Overview
2. Cloud Insights
3. Demo
4. Traffic Insights
5. Demo

ThousandEyes

Solution Overview

When something goes wrong…

Service Desk

Customer or employee opens support ticket

Endpoint Team

All devices are showing green.

Network Team

Everything’s fine!

Cloud Ops / Infra Team

IaaS vendor says they’re good.

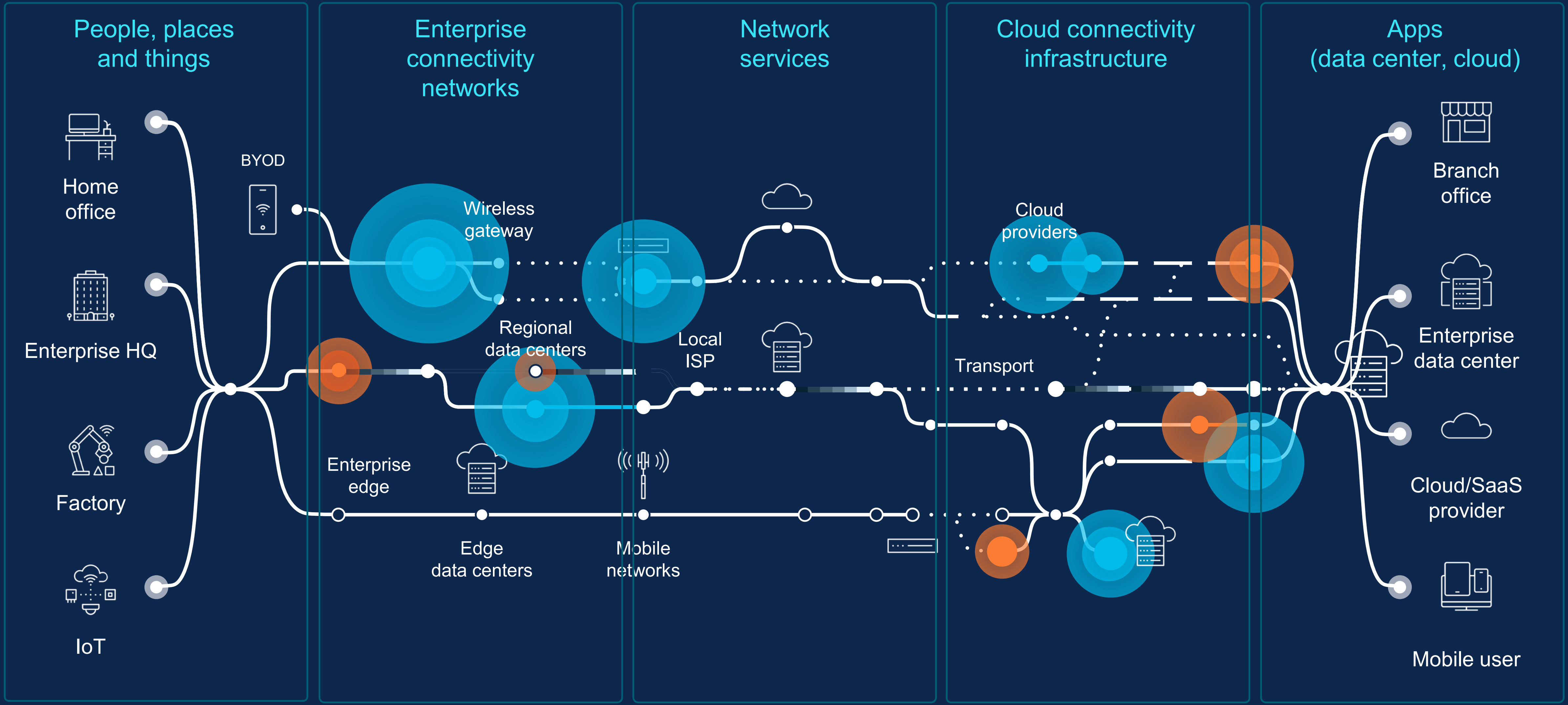
App Team

No issues here.

“War Room”

Multiple teams. Of course, no finger pointing.

Assuring Your Network is an End-to-End Challenge



How ThousandEyes Collects Data

Enterprise

Lightweight agent deployed to customer sites and data center locations.

Cloud

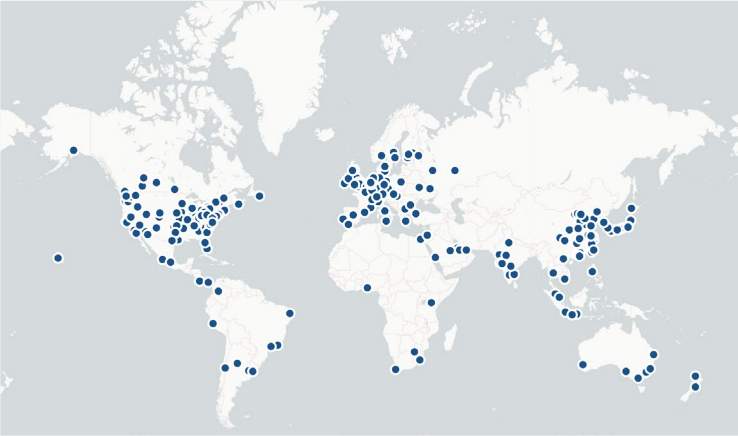
No installation required. > 400 POPs. Tier 1, 2 and 3 ISPs, broadband service providers and Cloud DCs.

Endpoint

Pushed to end user laptop or desktop for last mile visibility.

Flexible Deployment Options

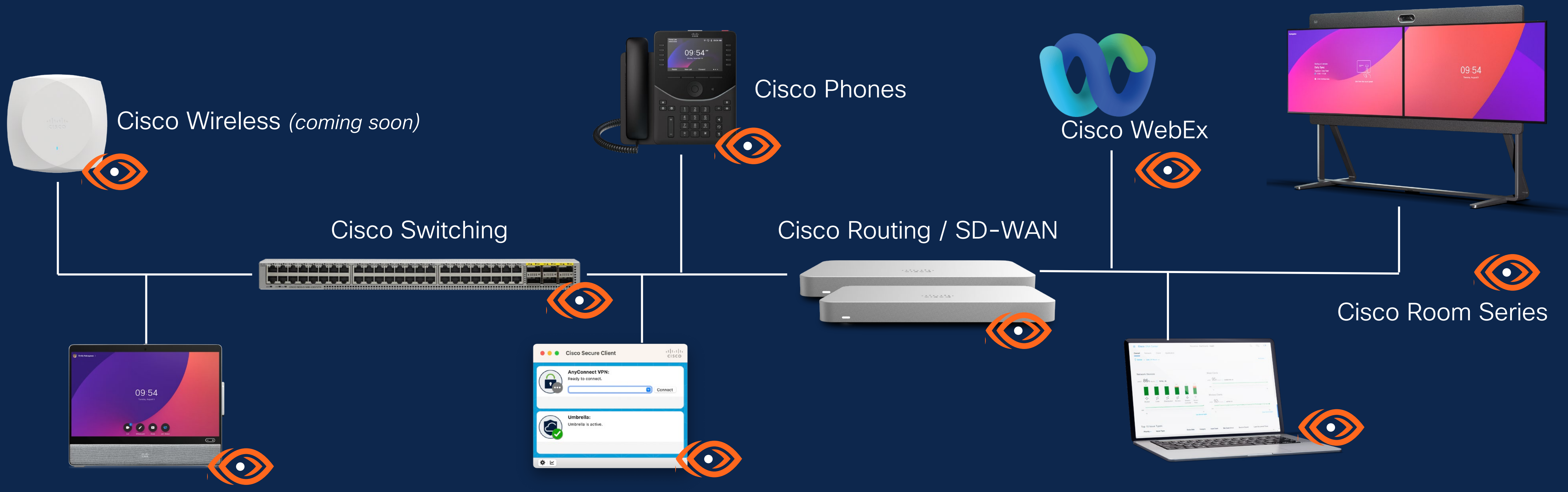
- OVA / Virtual Machine
- Linux Server
- Intel NUC / rPi
- Cisco Routing and Switching
- Docker
- AWS / Azure / GCP



End User Visibility

- Real user (browser) telemetry
- Automated session testing
- 24/7 scheduled testing

With Cisco, Assurance is built-in



Cisco Wireless *(coming soon)*

Cisco Phones

Cisco WebEx

Cisco Switching

Cisco Routing / SD-WAN

Cisco Room Series

Cisco Secure Client

AnyConnect VPN:
Ready to connect.

Umbrella:
Umbrella is active.

Cisco Desk Series

Cisco Secure Client / Access

PC & Mac Devices

Drives closed-loop operations + splunk> a cisco company integration

Correlated Application and Network Visibility

Internet Insights

- Detection of global network outages
- Identification of affected domains

App Experience

- Transaction scripting, page load
- Waterfall

HTTP/DNS/RTP Server

- HTTP Availability, response time, throughput

Network Metrics

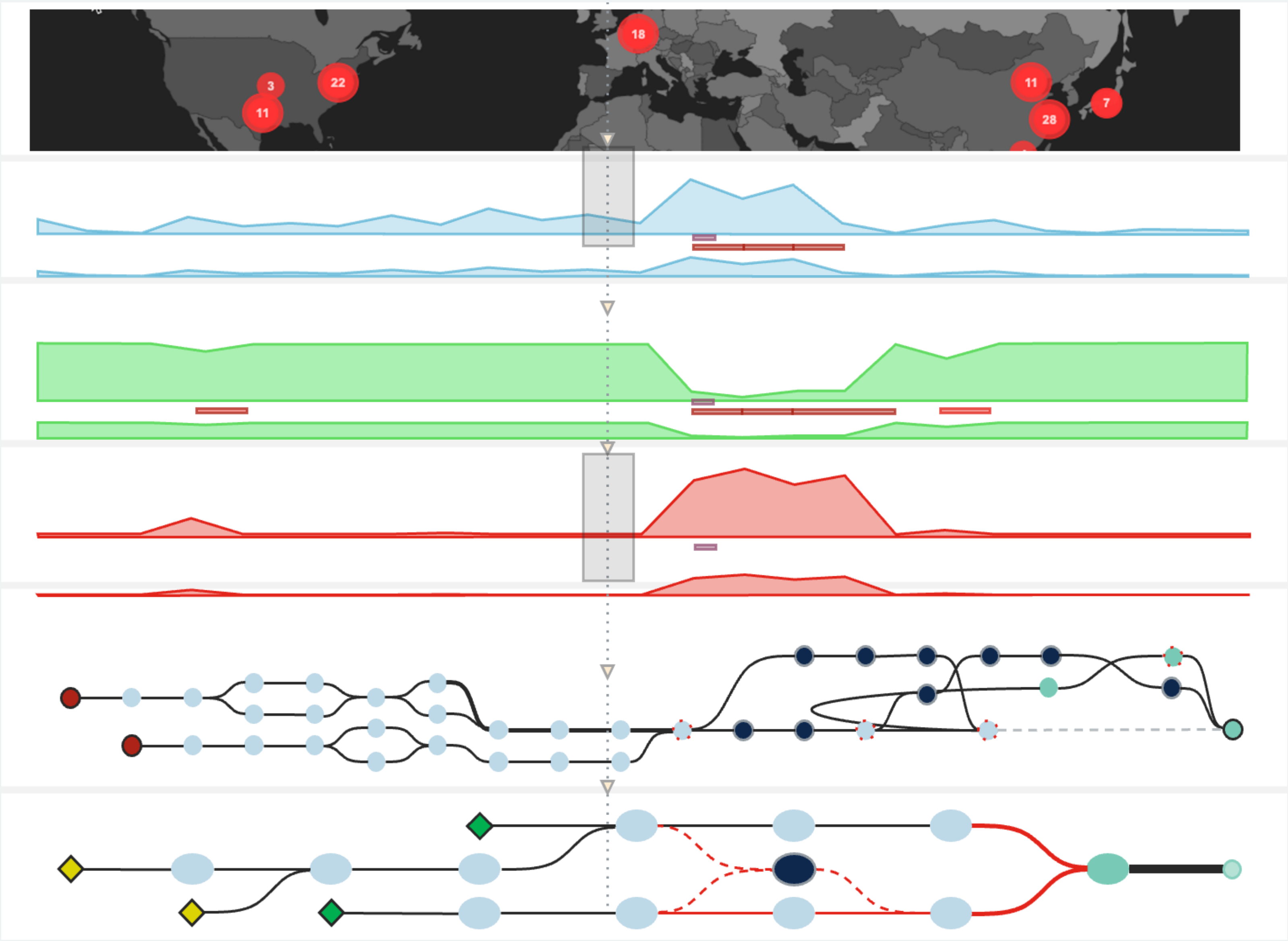
- Packet Loss, Latency, Jitter

Path Visualization

- Hop-by-hop; multi-point; bidirectional
- Metrics and data per hop
- Integrated Outage Detection

BGP Monitoring

- Reachability, path changes, updates

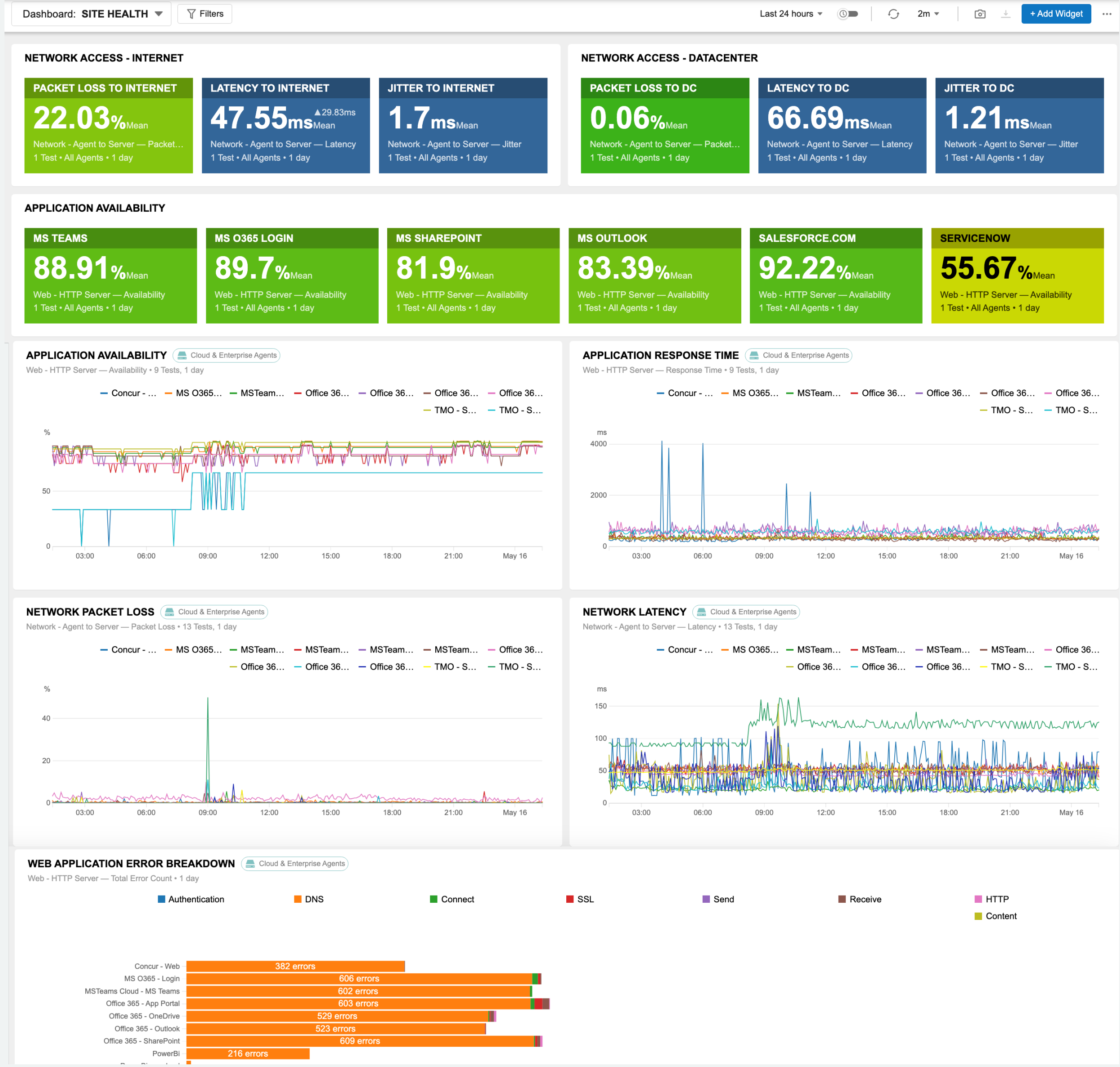


ThousandEyes Dashboards

Role-based views, widget driven, easily customized

Seamlessly drill down into specific test data

Save views as reports/pdfs, share dashboard views with sharelinks



Dashboard: **SITE HEALTH**

NETWORK ACCESS - INTERNET

PACKET LOSS TO INTERNET
22.03% Mean
Network - Agent to Server — Packet…
1 Test • All Agents • 1 day

LATENCY TO INTERNET
47.55ms Mean ▲29.83ms
Network - Agent to Server — Latency
1 Test • All Agents • 1 day

JITTER TO INTERNET
1.7ms Mean
Network - Agent to Server — Jitter
1 Test • All Agents • 1 day

NETWORK ACCESS - DATACENTER

PACKET LOSS TO DC
0.06% Mean
Network - Agent to Server — Packet…
1 Test • All Agents • 1 day

LATENCY TO DC
66.69ms Mean
Network - Agent to Server — Latency
1 Test • All Agents • 1 day

JITTER TO DC
1.21ms Mean
Network - Agent to Server — Jitter
1 Test • All Agents • 1 day

APPLICATION AVAILABILITY

MS TEAMS
88.91% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

MS O365 LOGIN
89.7% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

MS SHAREPOINT
81.9% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

MS OUTLOOK
83.39% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

SALESFORCE.COM
92.22% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

SERVICENOW
55.67% Mean
Web - HTTP Server — Availability
1 Test • All Agents • 1 day

APPLICATION AVAILABILITY Cloud & Enterprise Agents
Web - HTTP Server — Availability • 9 Tests, 1 day

APPLICATION RESPONSE TIME Cloud & Enterprise Agents
Web - HTTP Server — Response Time • 9 Tests, 1 day

NETWORK PACKET LOSS Cloud & Enterprise Agents
Network - Agent to Server — Packet Loss • 13 Tests, 1 day

NETWORK LATENCY Cloud & Enterprise Agents
Network - Agent to Server — Latency • 13 Tests, 1 day

WEB APPLICATION ERROR BREAKDOWN Cloud & Enterprise Agents
Web - HTTP Server — Total Error Count • 1 day

Context driven – change context with filters focus on the data you need – on dashboard for multiple data sets

Set time context that allows you to quickly adjust scope

Integrate – export widgets as iframes to embed in other platforms

Automation and Integration

- Out-of-box integration with popular automation, ITSM and notification solutions
- Flexible and configurable alert integration
- Easy data integration into 3rd party and custom analytic and reporting solutions using the OpenTelemetry connector
- Flexible, powerful REST APIs (developer.thousandeyes.com)

splunk>
slack
PagerDuty
servicenow
puppet
Progress Chef
CISCO
DNA Center
SALTSTACK
ANSIBLE
APPDYNAMICS
part of Cisco
Microsoft Teams

ThousandEyes

Cloud Insights

Cloud: A Dominant Pillar in Digitization

From a technology disruptor to a required component for competitiveness that enables businesses and individuals to scale, collaborate, and innovate

+90%

Of organizations use the public cloud.

Source: Spacelift stats

73%

Of organizations embrace hybrid cloud environments.

Source: Flexera

2nd

Top challenge

Is operational complexity using multiple cloud environments.

Source: Cisco

Organizations must balance the greater flexibility and breadth of technology options offered by different cloud strategies against operational complexity.

Cloud Networking Architectures

Cloud providers' network strategies can drastically impact performance and operations once user traffic enters their environment.

Cloud networks are highly virtualized

Traditional monitoring tools provide limited visibility into a cloud providers network.

Cloud networks are highly dynamic

Cloud platform configuration changes and automation make them a moving target due to the ephemeral nature of cloud resources.

Cloud networks span cross multiple accounts

Managing multiple accounts across cloud providers is challenging due to the complexity of managing access control, and resource allocation across different accounts.

Today's approaches are not enough to close the Visibility Gap

Create homegrown solutions

1 Leverage **internal tools for traffic mapping between instances and identify gaps in security group rules.**

2 Create network connectivity checkers that confirm if networking issues are impacting services

3 Adopting a “shared VPC model” to understand if a set of services are operational post migration

Use cloud provider tools

1 Collect metrics and logs and create alerts to monitor performance and troubleshoot instances

2 Record resource activity including API calls, administrative actions, and data access

3 Discover resources and configurations and receive notifications of resource creation, modification or deletion

To succeed I&O teams need 360-degree visibility across multi-cloud environments enriched with the context of owned and unowned networks

ThousandEyes Cloud Insights

Navigate and explore the assets deployed in your cloud environment

Topology Visualization

Auto discover cloud provider resources to understand every service dependency

Infrastructure Changes

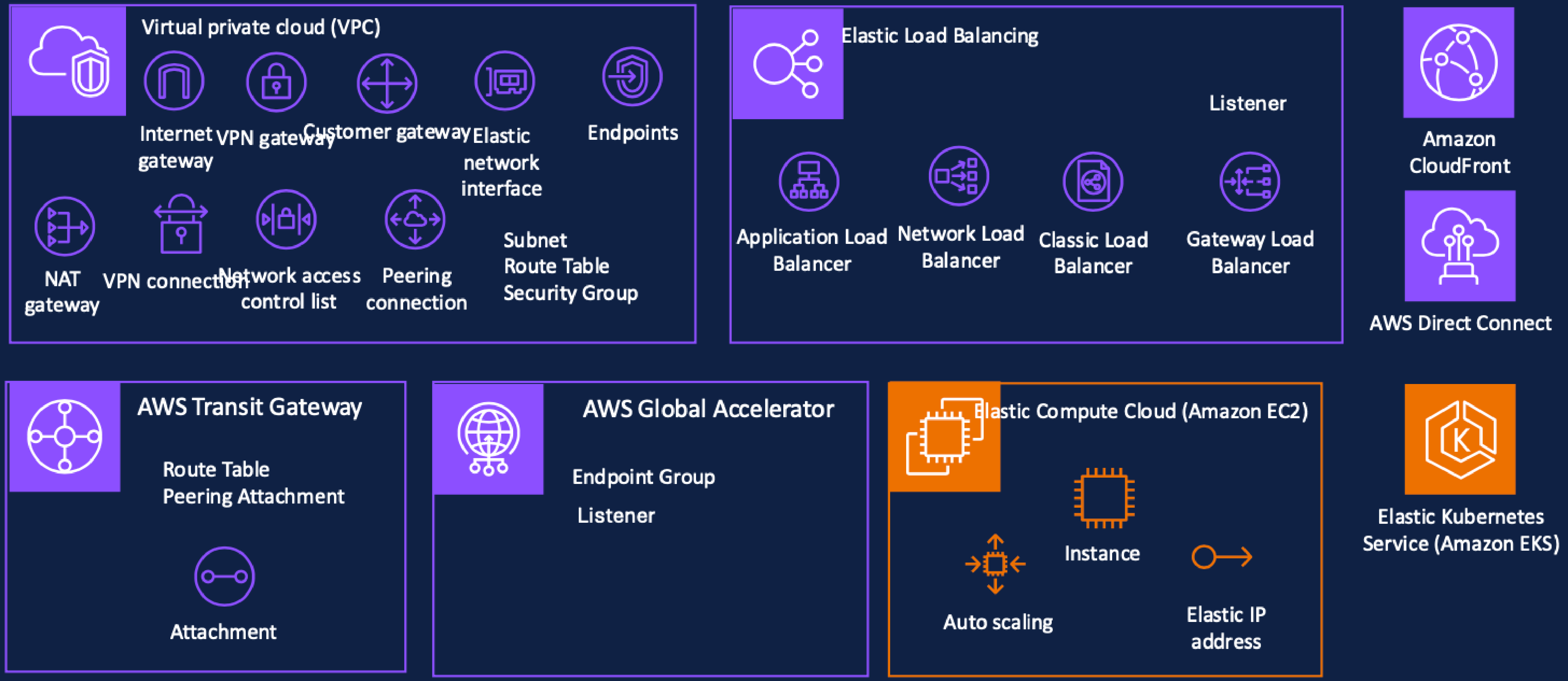
Correlate network performance issues within the cloud environment with configuration changes

Traffic Views

View traffic patterns to efficiently architect and troubleshoot your cloud network

Inventory Monitoring Supported AWS Services

Inventory Monitoring & Topology



Virtual private cloud (VPC)

Internet gateway

VPN gateway

Customer gateway

Elastic network interface

Endpoints

NAT gateway

VPN connection

Network access control list

Peering connection

Subnet
Route Table
Security Group

Elastic Load Balancing

Listener

Application Load Balancer

Network Load Balancer

Classic Load Balancer

Gateway Load Balancer

Amazon CloudFront

AWS Direct Connect

AWS Transit Gateway

Route Table
Peering Attachment

Attachment

AWS Global Accelerator

Endpoint Group

Listener

Elastic Compute Cloud (Amazon EC2)

Instance

Auto scaling

Elastic IP address

Elastic Kubernetes Service (Amazon EKS)

ThousandEyes

Use Cases

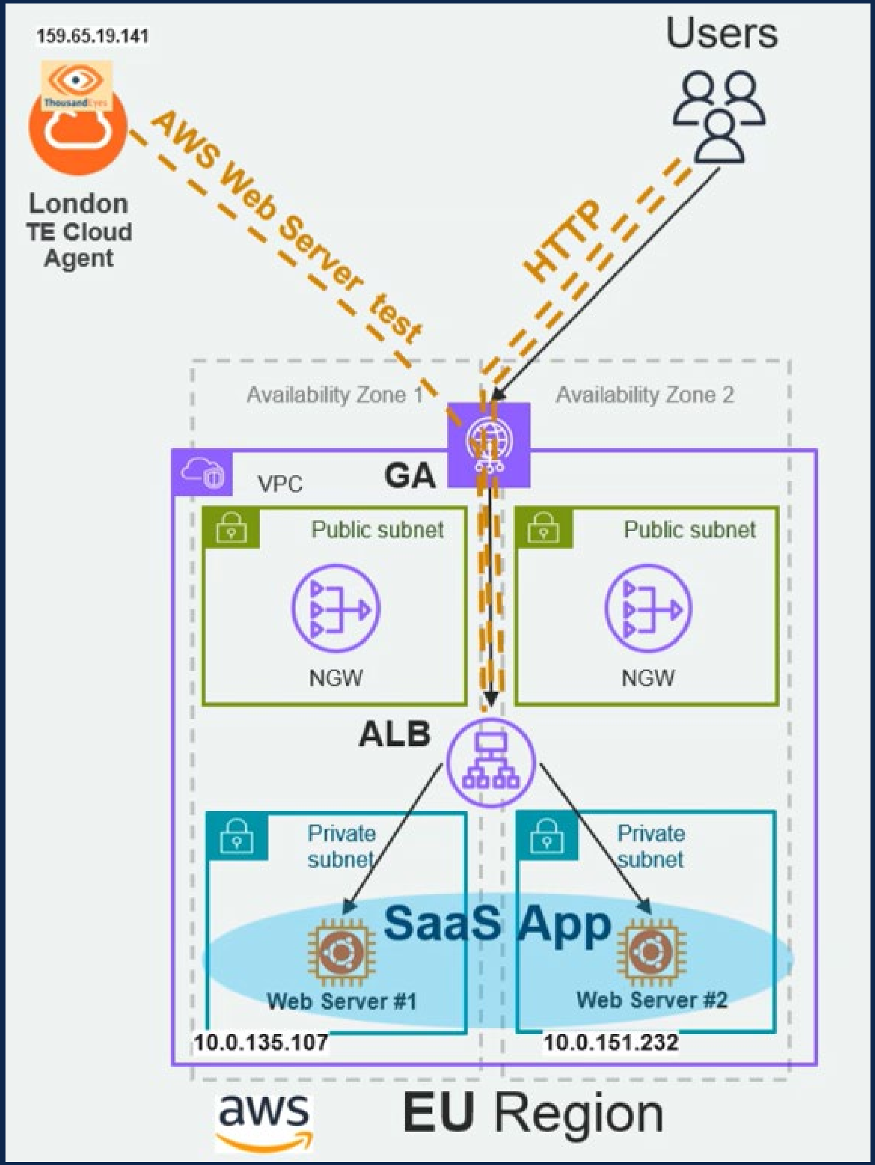
Use case: Ensure digital experience to critical apps

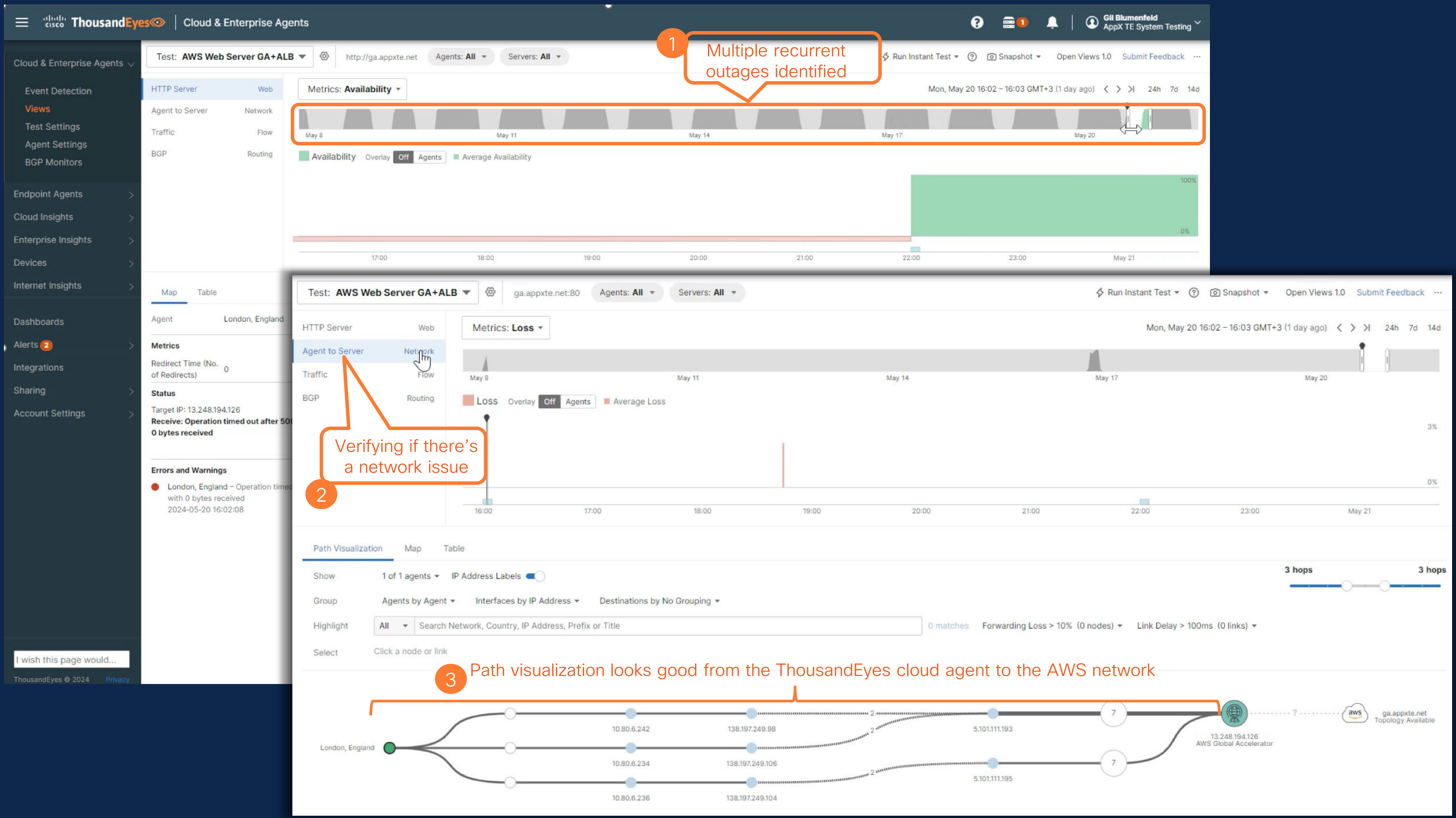
Situation:

1 Cloud providers, like all organizations, experience performance issues. Whether intermittent or sustained, can have a meaningful impact.

2 A distributed workforce connects from different locations and different networks, not controlled by IT, to the SaaS applications they need.

3 I&O teams are responsible of architecting and ensuring the user experience and reachability to the app considering the interdependencies of the Internet and the topology within the cloud.





Test: AWS Web Server GA+ALB

http://ga.appxte.net

Agents: All

Servers: All

Metrics: Availability

Mon, May 20 16:02 – 16:03 GMT+3 (1 day ago)

Agent London, England

Metrics

Redirect Time (No. of Redirects) 0

Status

Target IP: 13.248.194.126

Receive: Operation timed out after 50

0 bytes received

Errors and Warnings

London, England – Operation timed with 0 bytes received

2024-05-20 16:02:08

Test: AWS Web Server GA+ALB

ga.appxte.net:80

Agents: All

Servers: All

Metrics: Loss

Mon, May 20 16:02 – 16:03 GMT+3 (1 day ago)

Show: 1 of 1 agents; IP Address Labels

Group: Agents by Agent; Interfaces by IP Address; Destinations by No Grouping

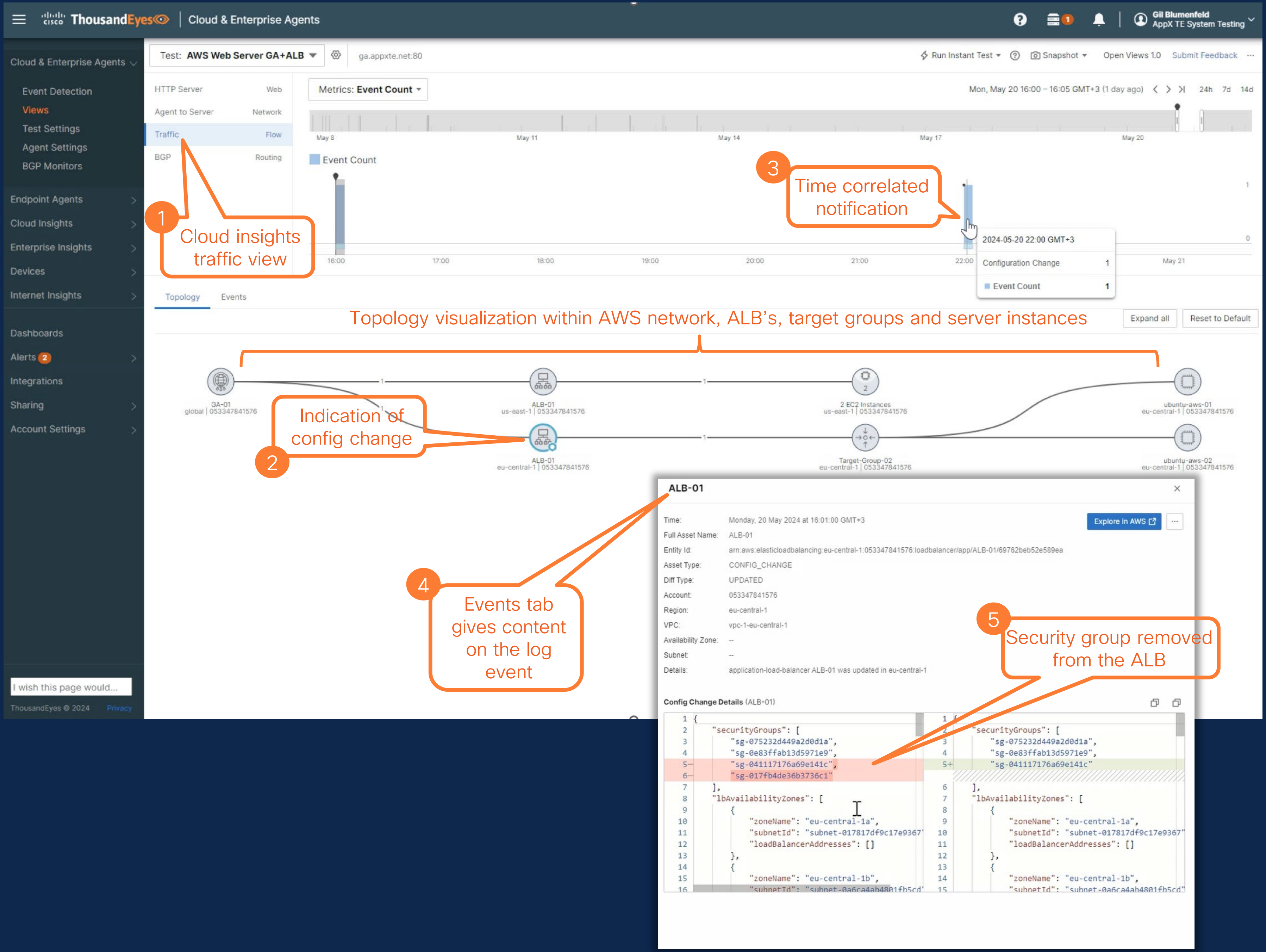
Highlight: All; Search Network, Country, IP Address, Prefix or Title; 0 matches; Forwarding Loss > 10% (0 nodes); Link Delay > 100ms (0 links)

Select: Click a node or link

1 Multiple recurrent outages identified

2 Verifying if there's a network issue

3 Path visualization looks good from the ThousandEyes cloud agent to the AWS network



ALB-01

Time: Monday, 20 May 2024 at 16:01:00 GMT+3

Full Asset Name: ALB-01

Entity Id: arn:aws:elasticloadbalancing:eu-central-1:053347841576:loadbalancer/app/ALB-01/69762beb52e589ea

Asset Type: CONFIG_CHANGE

Diff Type: UPDATED

Account: 053347841576

Region: eu-central-1

VPC: vpc-1-eu-central-1

Availability Zone: --

Subnet: --

Details: application-load-balancer ALB-01 was updated in eu-central-1

Config Change Details (ALB-01)

```
{
    "securityGroups": [
        "sg-075232d449a2d0d1a",
        "sg-0e83ffab13d5971e9",
-       "sg-041117176a69e141c",
-       "sg-017fb4de36b3736c1"
    ],
    "lbAvailabilityZones": [
        {
            "zoneName": "eu-central-1a",
            "subnetId": "subnet-017817df9c17e9367"
            "loadBalancerAddresses": []
        },
        {
            "zoneName": "eu-central-1b",
            "subnetId": "subnet-0a6ca4ab4801fb5cd'
```

```
{
    "securityGroups": [
        "sg-075232d449a2d0d1a",
        "sg-0e83ffab13d5971e9",
+       "sg-041117176a69e141c"
    ],
    "lbAvailabilityZones": [
        {
            "zoneName": "eu-central-1a",
            "subnetId": "subnet-017817df9c17e9367"
            "loadBalancerAddresses": []
        },
        {
            "zoneName": "eu-central-1b",
            "subnetId": "subnet-0a6ca4ab4801fb5cd"
```

1 Cloud insights traffic view

2 Indication of config change

3 Time correlated notification

Topology visualization within AWS network, ALB's, target groups and server instances

4 Events tab gives content on the log event

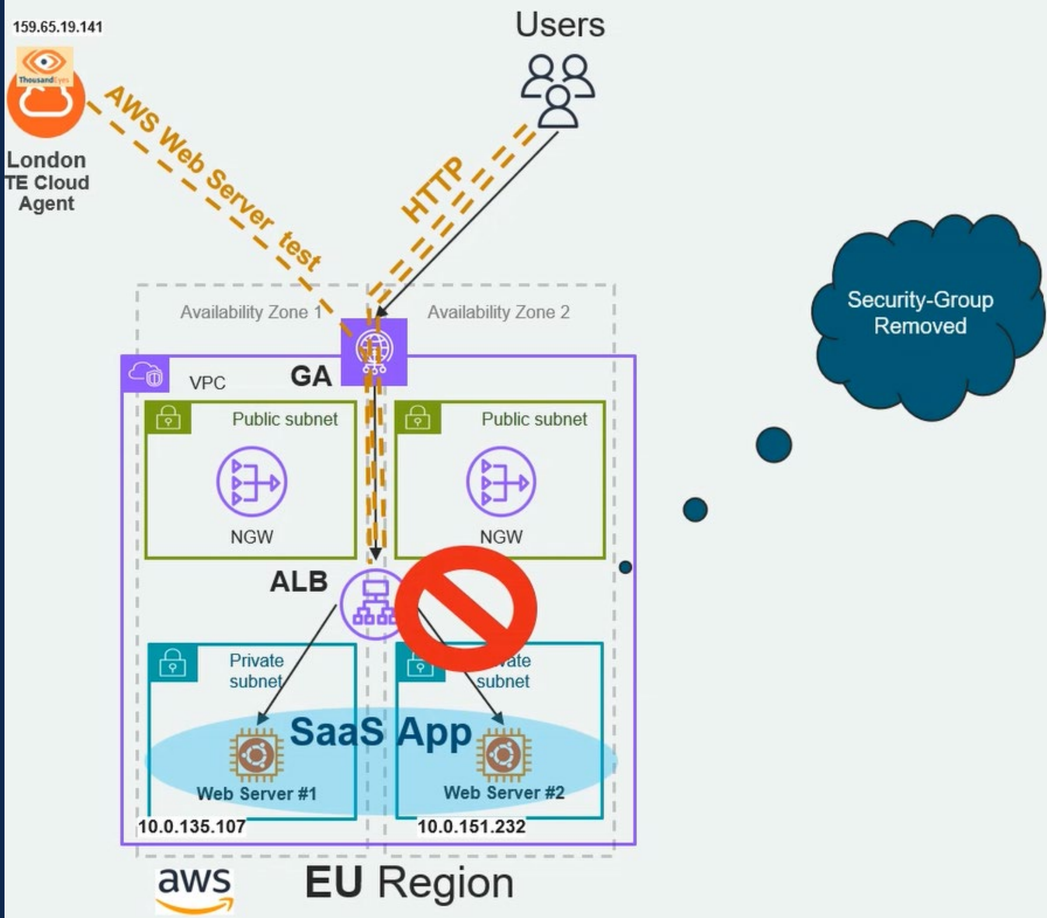
5 Security group removed from the ALB

Summary

1 Visibility within the cloud topology in the context of the end-to-end path from the user to the app, is key.

2 Taking a proactive approach emulating users' interaction with critical applications can prevent business disruptions and employee productivity issues.

3 Identifying the problem domain, whether the network, the application, or anything in between, helps I&O teams ensure business continuity.



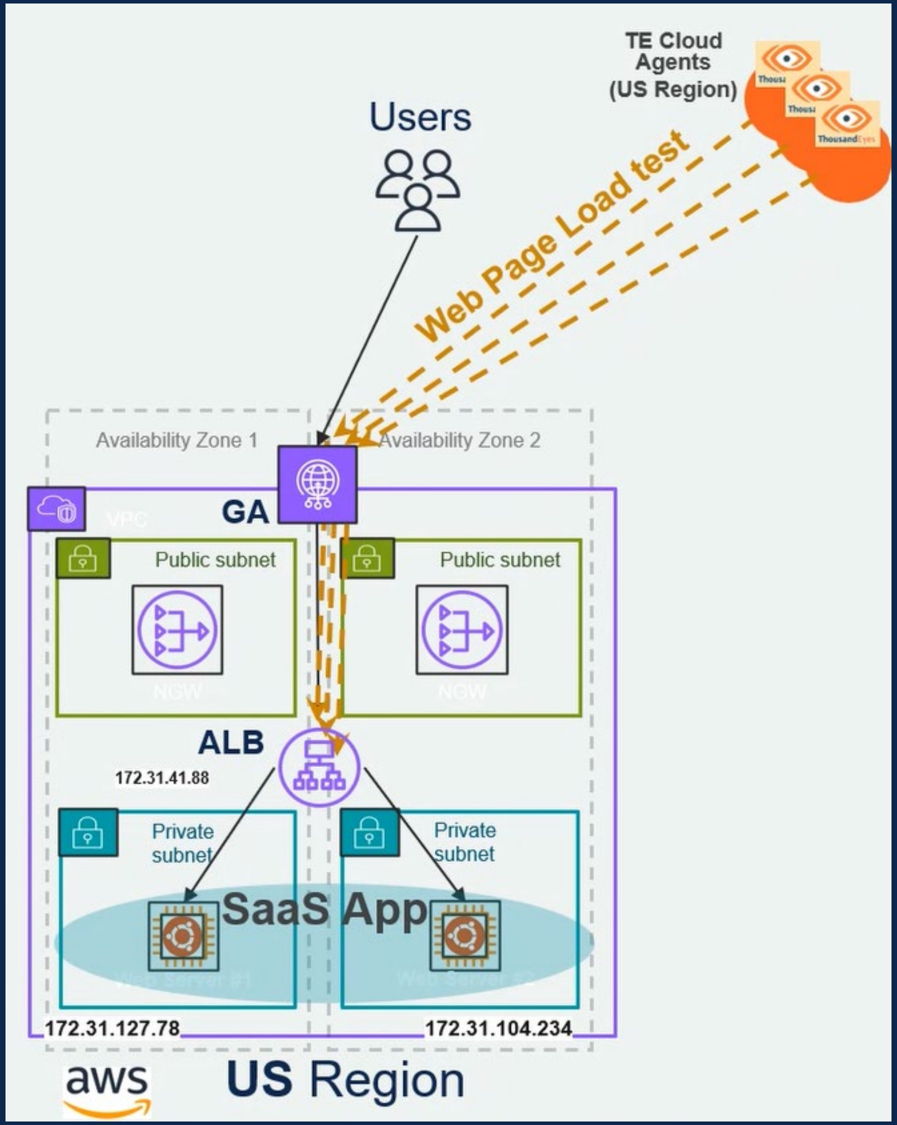
Use case: Poor digital experience due to malicious traffic

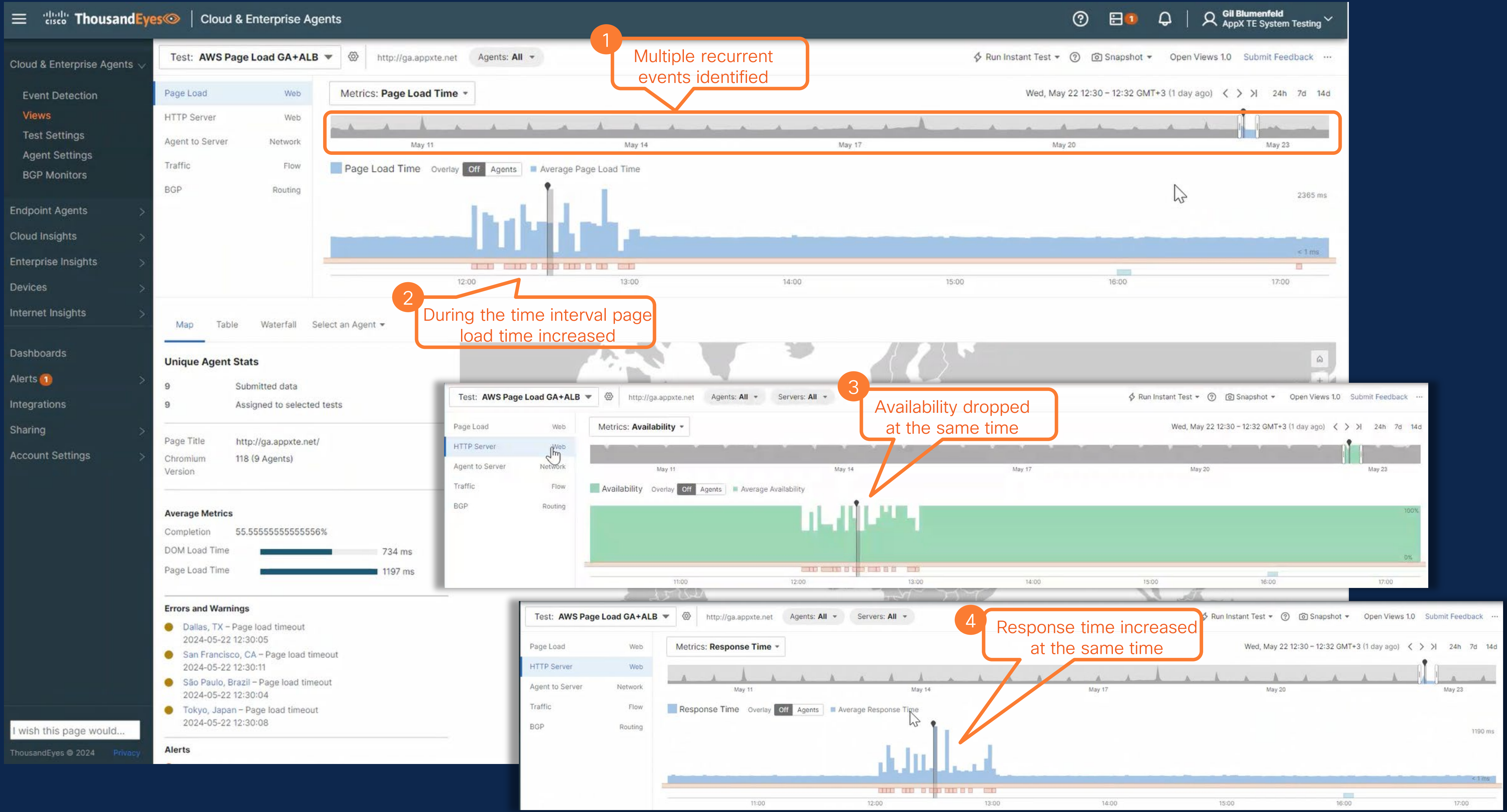
Situation:

1 While security is a top priority for cloud providers, malicious traffic may be targeting an app hosted in more than one region.

2 Baselining the end user experience with the application can help identify if there's degradation leading to poor performance.

3 IT requires the proper tools to quickly identify the problem domain and minimize time to problem resolution.





1 Multiple recurrent events identified

2 During the time interval page load time increased

3 Availability dropped at the same time

4 Response time increased at the same time

Test: AWS Page Load GA+ALB

http://ga.appxte.net

Agents: All

Metrics: Page Load Time

Wed, May 22 12:30 – 12:32 GMT+3 (1 day ago)

Unique Agent Stats

9 Submitted data

9 Assigned to selected tests

Page Title http://ga.appxte.net/

Chromium Version 118 (9 Agents)

Average Metrics

Completion 55.55555555555556%

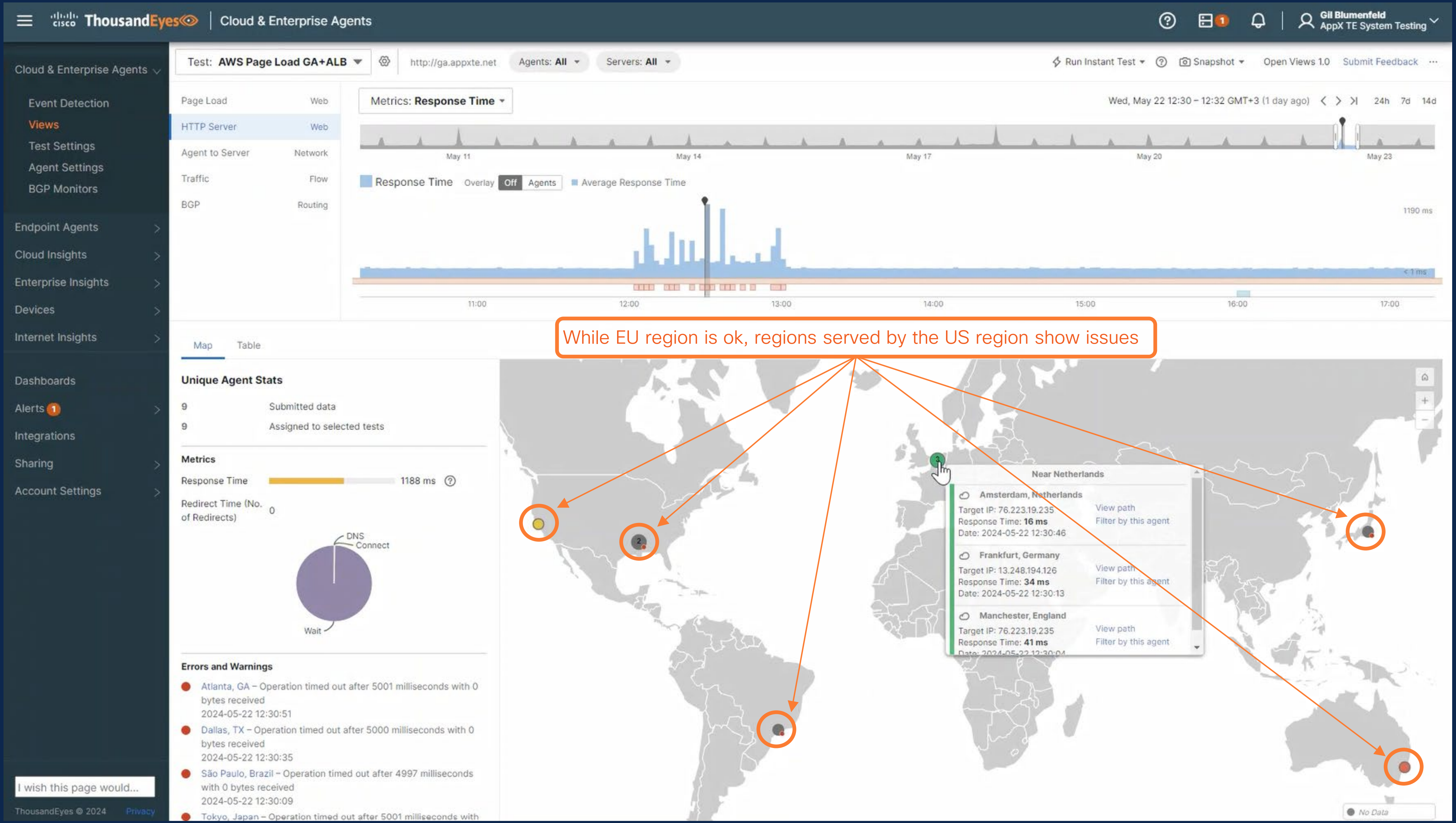
DOM Load Time 734 ms

Page Load Time 1197 ms

Errors and Warnings

- Dallas, TX – Page load timeout 2024-05-22 12:30:05
- San Francisco, CA – Page load timeout 2024-05-22 12:30:11
- São Paulo, Brazil – Page load timeout 2024-05-22 12:30:04
- Tokyo, Japan – Page load timeout 2024-05-22 12:30:08

Alerts



Test: **AWS Page Load GA+ALB**

http://ga.appxte.net

Agents: **All**

Servers: **All**

Metrics: **Response Time**

Unique Agent Stats

9	Submitted data
9	Assigned to selected tests

Metrics

Response Time	1188 ms
Redirect Time (No. of Redirects)	0

Errors and Warnings

- Atlanta, GA – Operation timed out after 5001 milliseconds with 0 bytes received
  2024-05-22 12:30:51
- Dallas, TX – Operation timed out after 5000 milliseconds with 0 bytes received
  2024-05-22 12:30:35
- São Paulo, Brazil – Operation timed out after 4997 milliseconds with 0 bytes received
  2024-05-22 12:30:09
- Tokyo, Japan – Operation timed out after 5001 milliseconds with

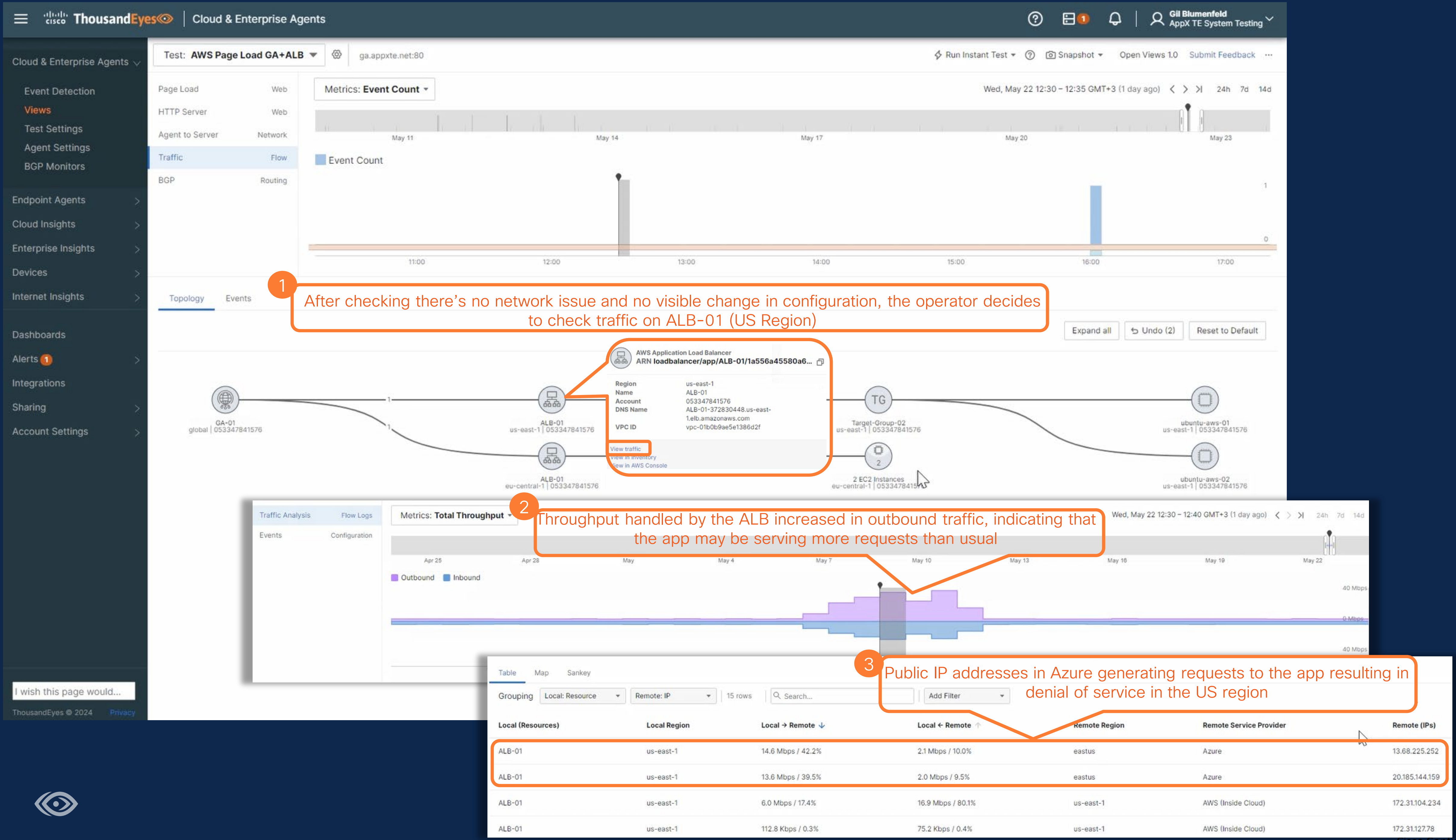
Near Netherlands

Amsterdam, Netherlands
Target IP: 76.223.19.235
Response Time: **16 ms**
Date: 2024-05-22 12:30:46
View path
Filter by this agent

Frankfurt, Germany
Target IP: 13.248.194.126
Response Time: **34 ms**
Date: 2024-05-22 12:30:13
View path
Filter by this agent

Manchester, England
Target IP: 76.223.19.235
Response Time: **41 ms**
Date: 2024-05-22 12:30:04
View path
Filter by this agent

While EU region is ok, regions served by the US region show issues



AWS Application Load Balancer
ARN loadbalancer/app/ALB-01/1a556a45580a6...

Region us-east-1
Name ALB-01
Account 053347841576
DNS Name ALB-01-372830448.us-east-1.elb.amazonaws.com
VPC ID vpc-01b0b9ae5e1386d2f

View traffic
View in Inventory
View in AWS Console

1 After checking there's no network issue and no visible change in configuration, the operator decides to check traffic on ALB-01 (US Region)

2 Throughput handled by the ALB increased in outbound traffic, indicating that the app may be serving more requests than usual

3 Public IP addresses in Azure generating requests to the app resulting in denial of service in the US region

Grouping: Local: Resource | Remote: IP | 15 rows | Search...

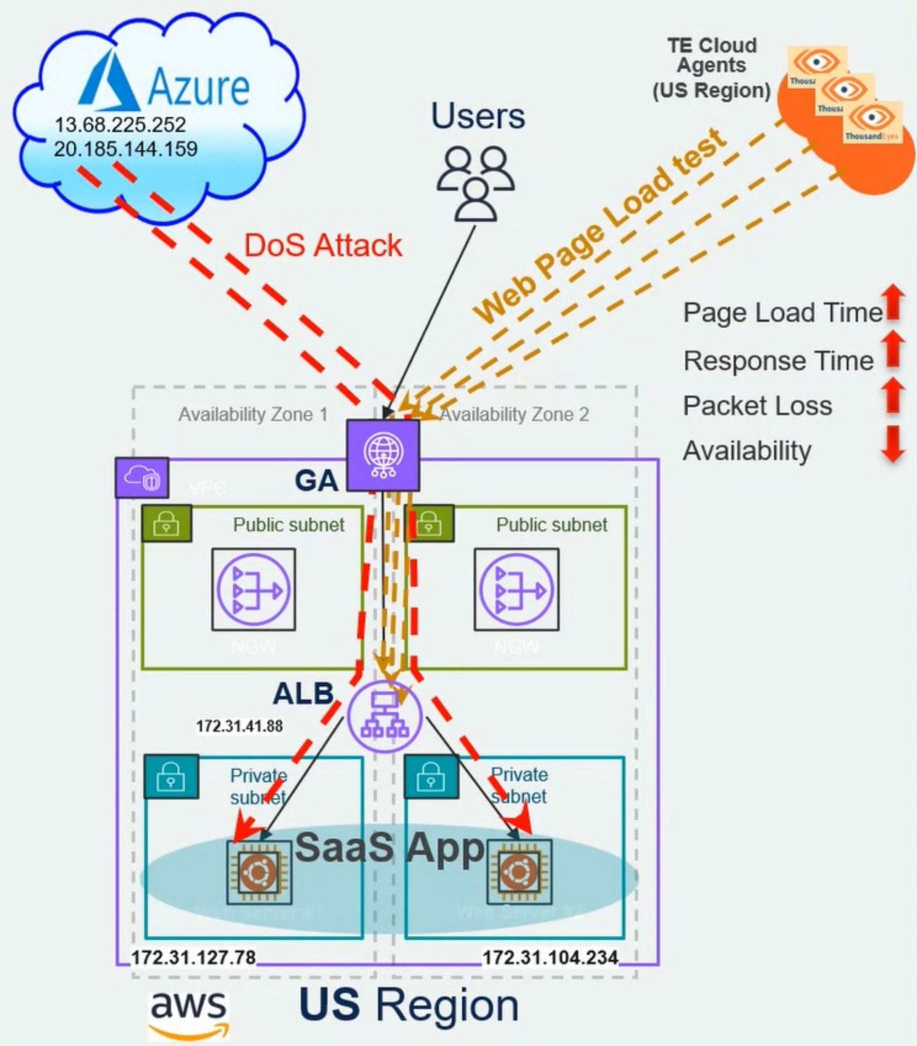
Local (Resources)	Local Region	Local → Remote	Local ← Remote	Remote Region	Remote Service Provider	Remote (IPs)
ALB-01	us-east-1	14.6 Mbps / 42.2%	2.1 Mbps / 10.0%	eastus	Azure	13.68.225.252
ALB-01	us-east-1	13.6 Mbps / 39.5%	2.0 Mbps / 9.5%	eastus	Azure	20.185.144.159
ALB-01	us-east-1	6.0 Mbps / 17.4%	16.9 Mbps / 80.1%	us-east-1	AWS (Inside Cloud)	172.31.104.234
ALB-01	us-east-1	112.8 Kbps / 0.3%	75.2 Kbps / 0.4%	us-east-1	AWS (Inside Cloud)	172.31.127.78

Summary

1 Continuously monitor the app performance helps quickly identify when there’s degradation causing a poor user experience.

2 The correlation on the application and network layers helps narrow the troubleshooting process to investigate further within the cloud.

3 The ability to see the cloud service dependencies and local resources within the AWS network, at the IP address level, helps identify external sources affecting app performance.



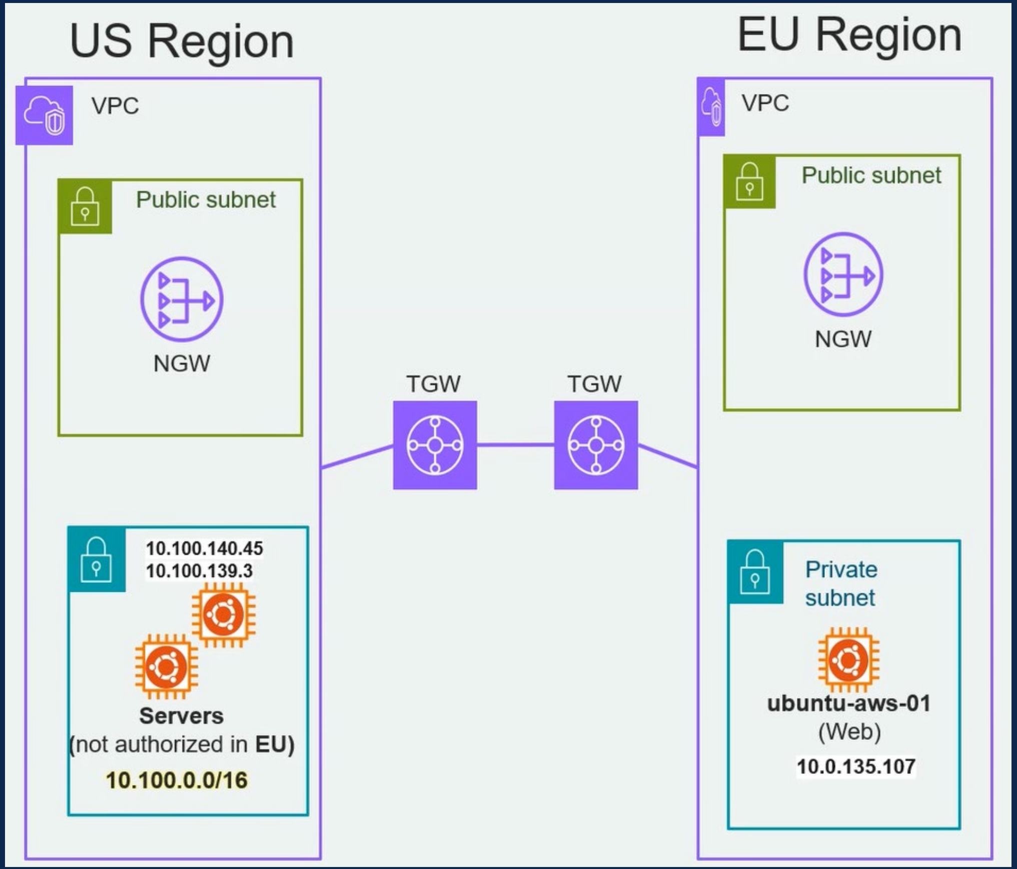
Use case: Cloud traffic visibility and analysis

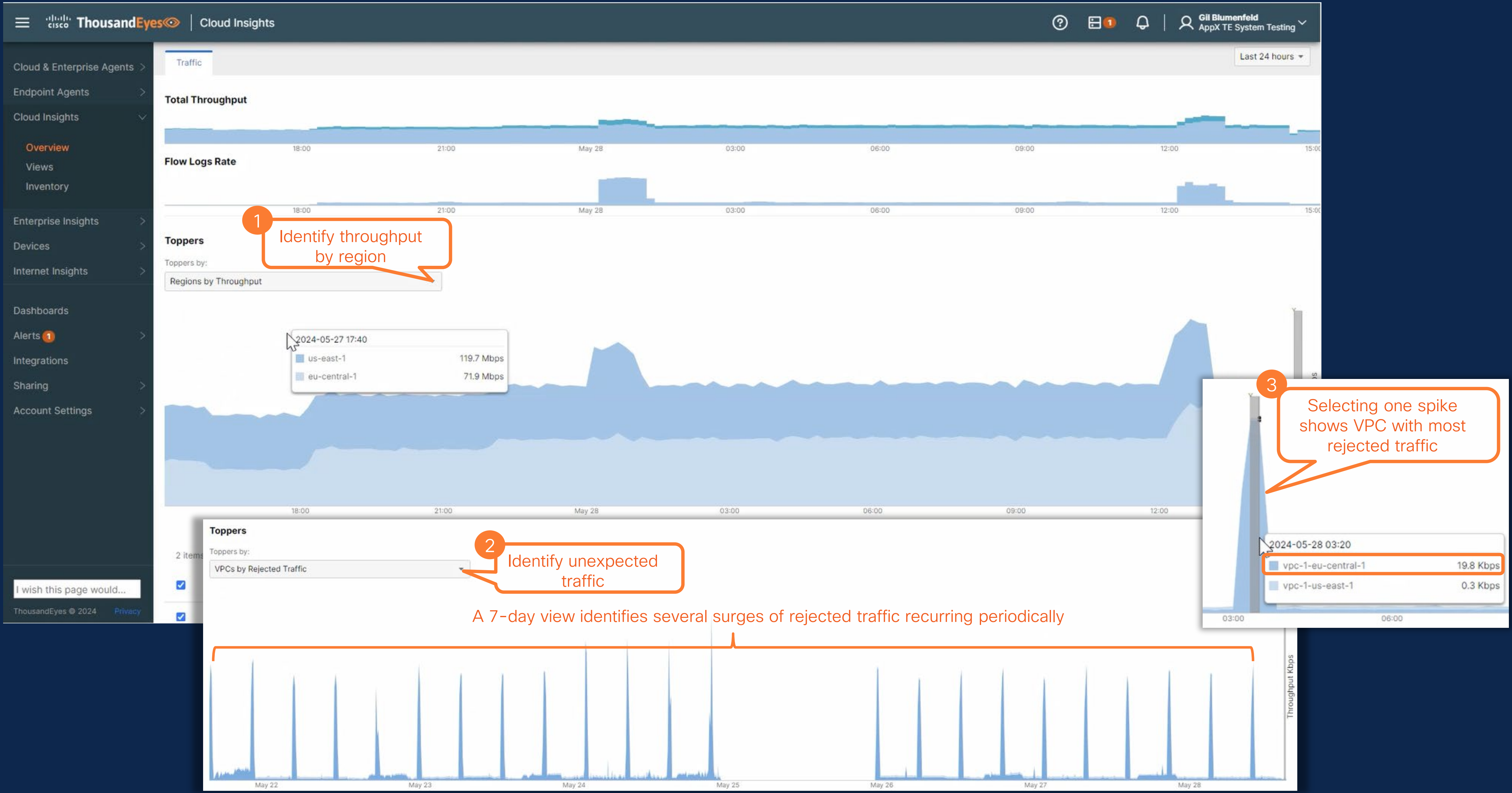
Scenario:

1. Organizations with global presence can leverage transit gateways to centralize network connectivity, improve performance and security.

2. Inbound and outbound traffic can be very dynamic and sometimes, inbound rules are configured to restrict access to specific IP subnets.

3. IT teams need to continuously check if there's any traffic, potentially rejected by security groups, from unexpected sources inside the cloud network.





Toppers

Toppers by: Regions by Throughput

2024-05-27 17:40
- us-east-1 119.7 Mbps
- eu-central-1 71.9 Mbps

Toppers

Toppers by: VPCs by Rejected Traffic

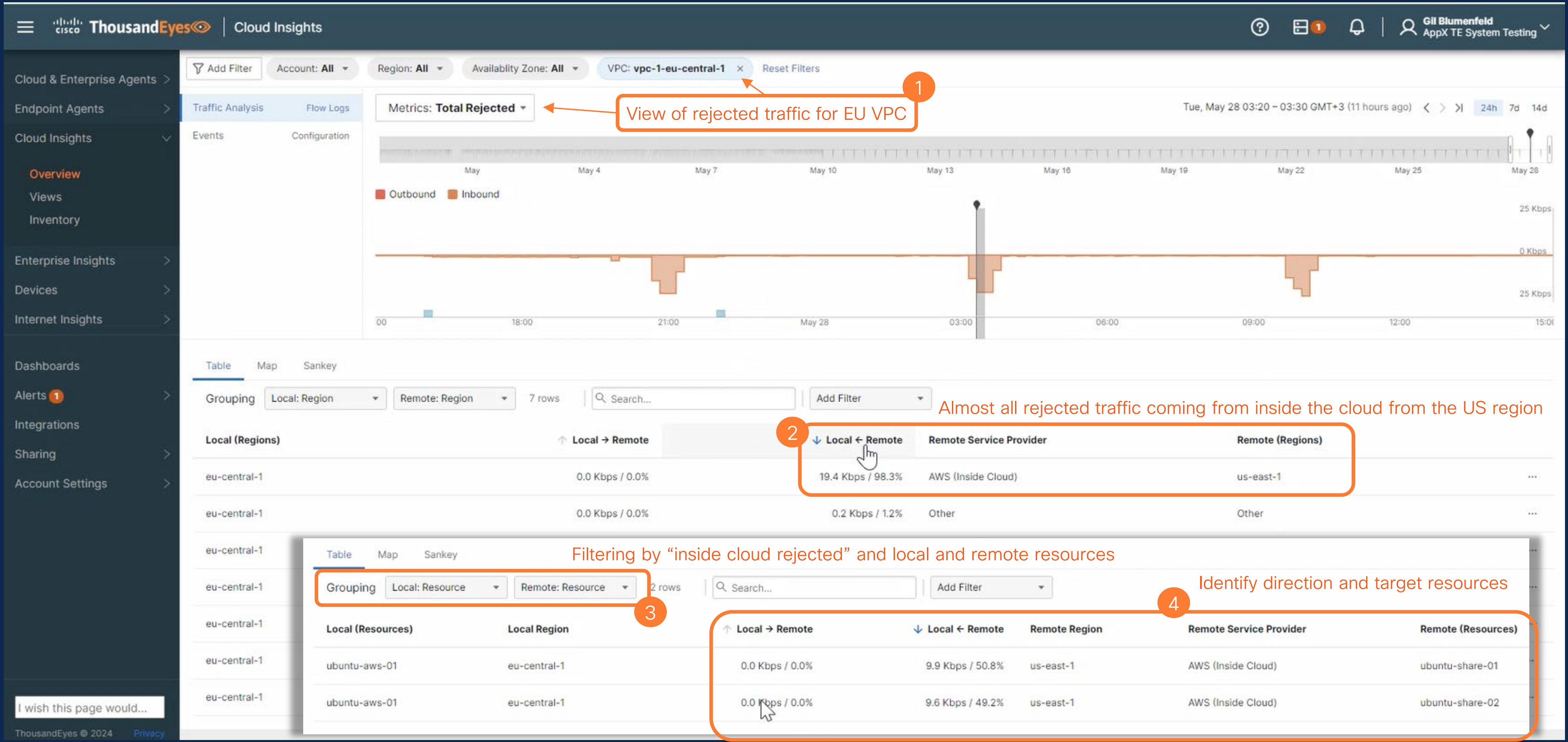
2024-05-28 03:20
- vpc-1-eu-central-1 19.8 Kbps
- vpc-1-us-east-1 0.3 Kbps

1 Identify throughput by region

2 Identify unexpected traffic

3 Selecting one spike shows VPC with most rejected traffic

A 7-day view identifies several surges of rejected traffic recurring periodically



Add Filter | Account: All | Region: All | Availablity Zone: All | VPC: vpc-1-eu-central-1 × | Reset Filters

Metrics: Total Rejected

Tue, May 28 03:20 – 03:30 GMT+3 (11 hours ago) | 24h | 7d | 14d

1 View of rejected traffic for EU VPC

Grouping: Local: Region | Remote: Region | 7 rows | Search... | Add Filter

2 Almost all rejected traffic coming from inside the cloud from the US region

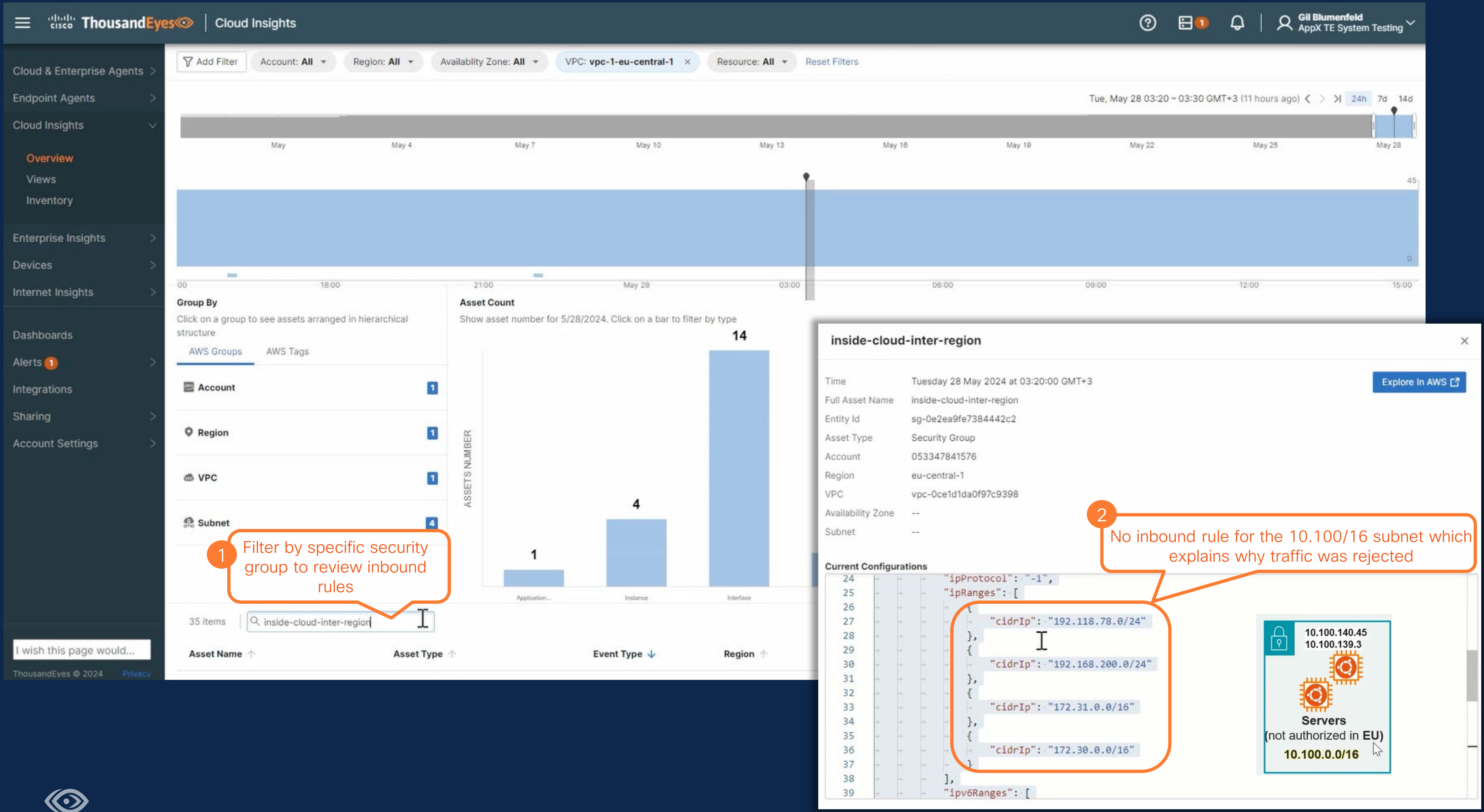
Local (Regions)	Local → Remote	Local ← Remote	Remote Service Provider	Remote (Regions)
eu-central-1	0.0 Kbps / 0.0%	19.4 Kbps / 98.3%	AWS (Inside Cloud)	us-east-1
eu-central-1	0.0 Kbps / 0.0%	0.2 Kbps / 1.2%	Other	Other
eu-central-1				
eu-central-1				
eu-central-1				
eu-central-1				
eu-central-1				

Filtering by "inside cloud rejected" and local and remote resources

3 Grouping: Local: Resource | Remote: Resource | 2 rows | Search... | Add Filter

4 Identify direction and target resources

Local (Resources)	Local Region	Local → Remote	Local ← Remote	Remote Region	Remote Service Provider	Remote (Resources)
ubuntu-aws-01	eu-central-1	0.0 Kbps / 0.0%	9.9 Kbps / 50.8%	us-east-1	AWS (Inside Cloud)	ubuntu-share-01
ubuntu-aws-01	eu-central-1	0.0 Kbps / 0.0%	9.6 Kbps / 49.2%	us-east-1	AWS (Inside Cloud)	ubuntu-share-02



inside-cloud-inter-region

Time	Tuesday 28 May 2024 at 03:20:00 GMT+3
Full Asset Name	inside-cloud-inter-region
Entity Id	sg-0e2ea9fe7384442c2
Asset Type	Security Group
Account	053347841576
Region	eu-central-1
VPC	vpc-0ce1d1da0f97c9398
Availability Zone	--
Subnet	--

Current Configurations

```
            "ipProtocol": "-1",
            "ipRanges": [
              {
                "cidrIp": "192.118.78.0/24"
              },
              {
                "cidrIp": "192.168.200.0/24"
              },
              {
                "cidrIp": "172.31.0.0/16"
              },
              {
                "cidrIp": "172.30.0.0/16"
              }
            ],
            "ipv6Ranges": [
```

1 Filter by specific security group to review inbound rules

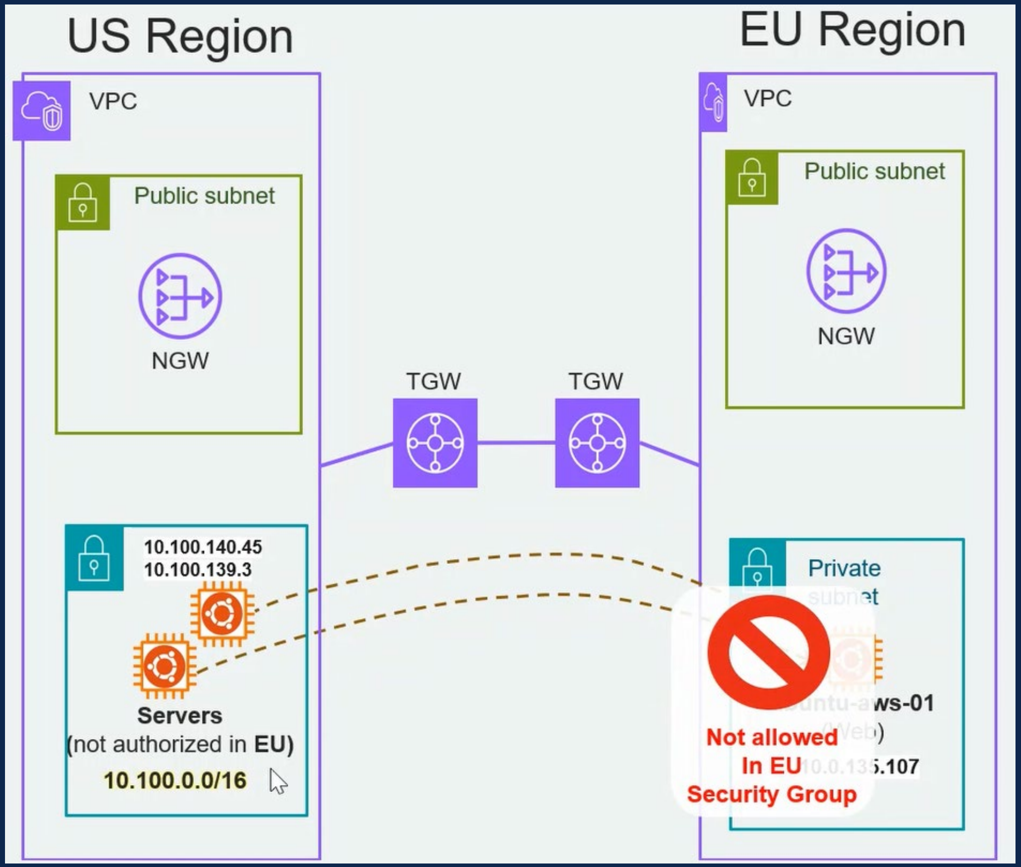
2 No inbound rule for the 10.100/16 subnet which explains why traffic was rejected

Summary

1 Creating Security Groups are crucial to maintaining a secure environment. I&O teams need to detect unauthorized traffic from the inside or outside of the cloud.

2 Assuring the user experience requires getting detailed traffic analysis and toppers view can help understand who are the main actors and their impact in the cloud network.

3 Finding abnormal and recurrent traffic spikes and AWS config causing rejects, with evidence, helps you better collaborate with your AWS support team and minimize MTTR.



A Holistic Approach to Cloud Monitoring

Organizations need to understand how cloud providers operate their networks and factor their performance and behaviors into their cloud management strategy

Put the full digital experience in context

Virtual Automatic correlation of cloud provider configurations and traffic with digital experience data

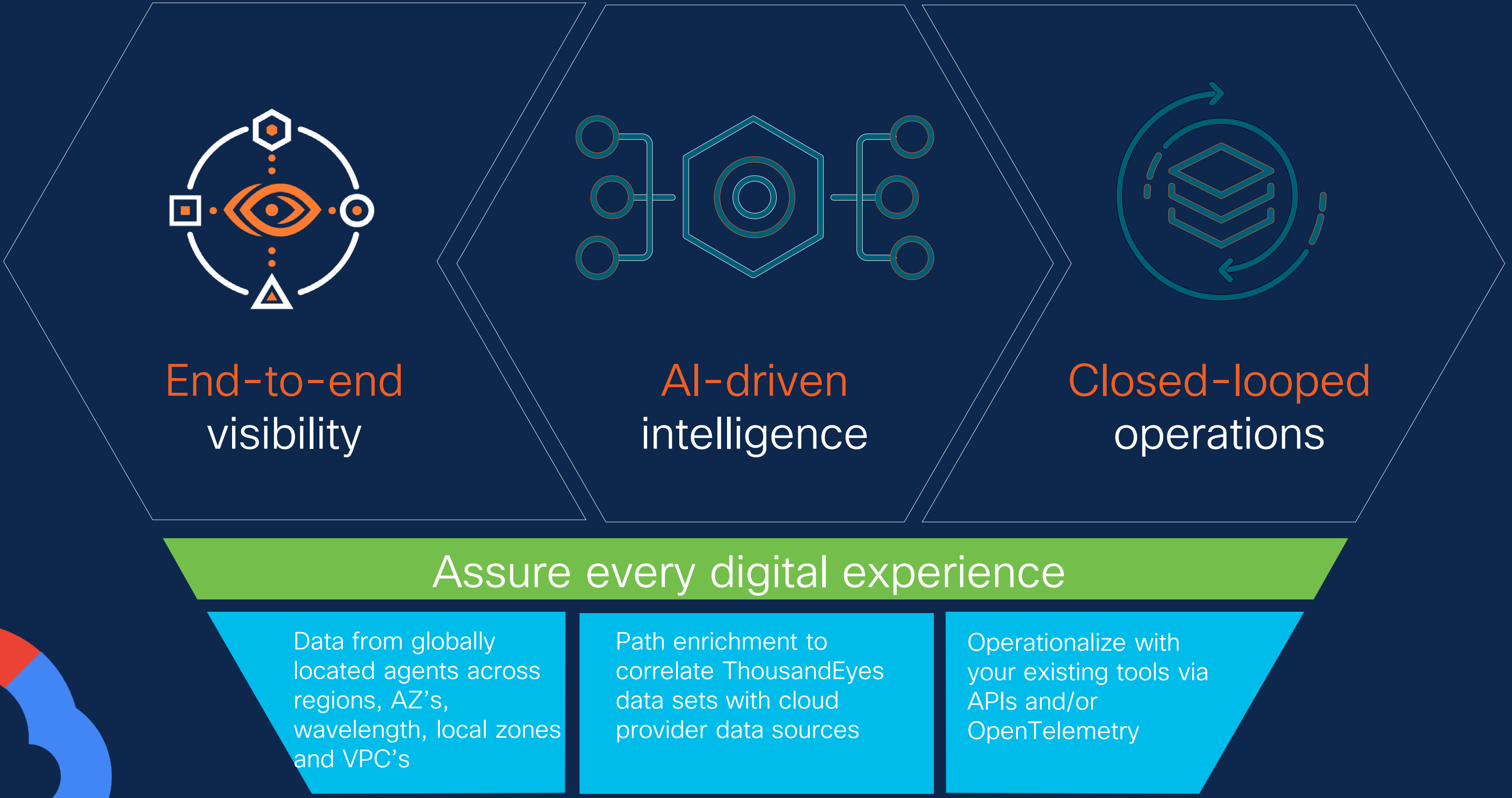
Centralized view across all owned and unowned environments

Deep visibility into on-premises deployments, public cloud providers, and the Internet, with a single view of resources across providers

See cloud networks like your own

See 3rd party cloud infrastructure like an extension of your environment and overlay performance metrics from multiple public cloud environments for centralized visibility and troubleshooting .

One Platform for your Multicloud Environments



End-to-end visibility

AI-driven intelligence

Closed-looped operations

Assure every digital experience

Data from globally located agents across regions, AZ's, wavelength, local zones and VPC's

Path enrichment to correlate ThousandEyes data sets with cloud provider data sources

Operationalize with your existing tools via APIs and/or OpenTelemetry

ThousandEyes

DEMO

ThousandEyes

Traffic Insights

NetOps today relies on multiple tools/solutions

Inefficient troubleshooting workflows = slower time to identify/remediate

- Time lost manually correlating disparate datasets
- Difficult to identify root cause at the node level
- Don’t know which users are impacted and where
- Can’t tell which apps are degrading experience

Today's Monitoring – More Complementary than Cohesive

Disparities in data and usage reduce efficiency, accuracy

	Passive (NetFlow, SNMP)	Active (Synthetics)
Used with	• Networks within your control	• Networks within and outside your control
Measures	• Network/node utilization • Traffic characteristics/patterns	• End-to-end performance • Symptoms (loss, latency, etc.)
When data is analyzed	• After collection / flow termination	• Near real-time
Typical use cases	• Infrastructure troubleshooting • Traffic engineering • Trend analysis • Capacity planning	• End-to-end troubleshooting • Monitoring 3rd-party networks/services • Proactive incident detection • Before/during/after analytics

Cisco ThousandEyes Traffic Insights

Rapidly attribute degraded network performance to specific traffic flows

Boost efficiency through automated correlation

Dramatically reduce time and effort to determine root cause

View flow data in the context of synthetics to quickly see which traffic is impacting experience

Quickly identify issues across your network

Flexible views make it easy to understand and interpret usage

Filtering and dashboards to format and view data exactly the way you want

Scale visibility through simplified deployment

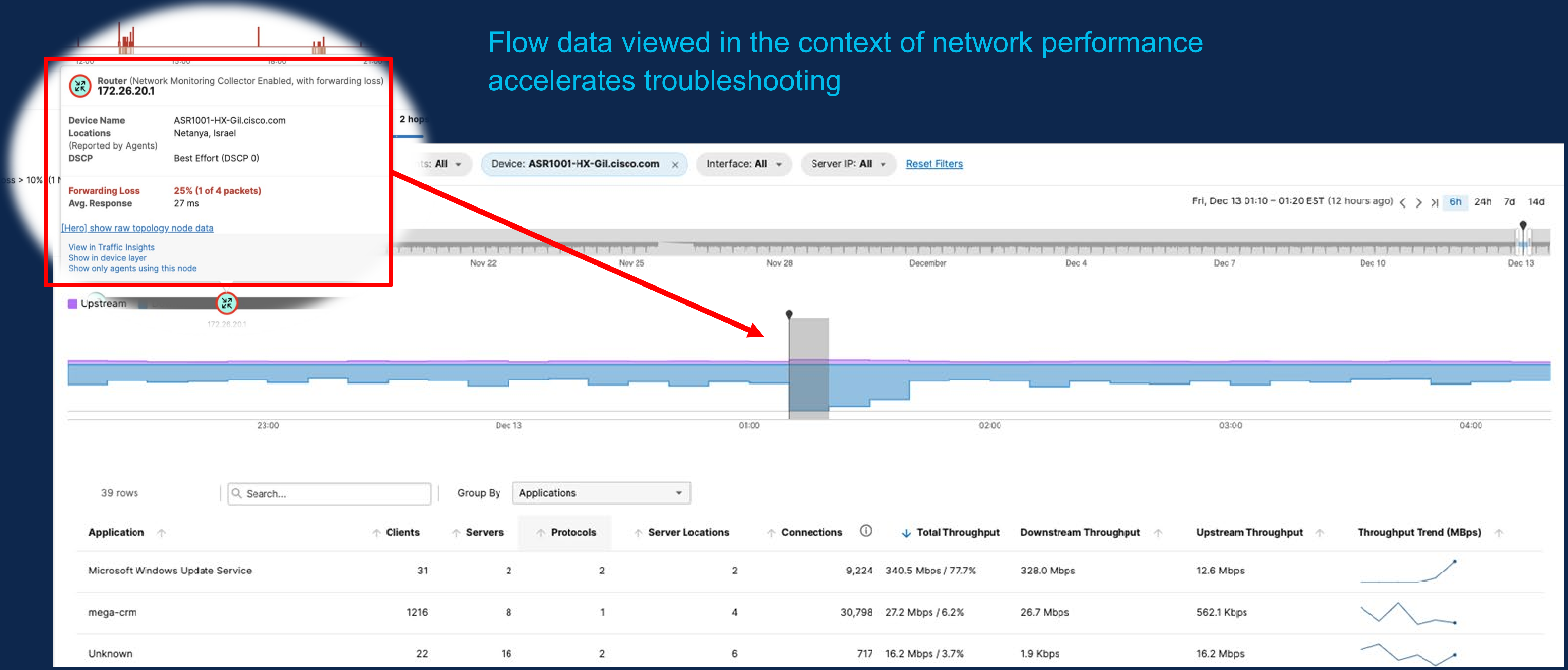
Centralized onboarding makes it simple to activate more locations

ThousandEyes Enterprise Agents with integrated NetFlow, IPFIX for broader more granular visibility

Traffic Insights Changes the Game for NetOps

Quickly resolve degraded experiences through detailed visibility into network traffic

Flow data viewed in the context of network performance accelerates troubleshooting



Router (Network Monitoring Collector Enabled, with forwarding loss)
172.26.20.1

Device Name ASR1001-HX-Gil.cisco.com
Locations Netanya, Israel
(Reported by Agents)
DSCP Best Effort (DSCP 0)

Forwarding Loss **25% (1 of 4 packets)**
Avg. Response 27 ms

[Hero] show raw topology node data

View in Traffic Insights
Show in device layer
Show only agents using this node

ts: **All** ▾ | Device: **ASR1001-HX-Gil.cisco.com** × | Interface: **All** ▾ | Server IP: **All** ▾ | Reset Filters

Fri, Dec 13 01:10 – 01:20 EST (12 hours ago) ‹ › ›| 6h 24h 7d 14d

39 rows | Search... | Group By Applications ▾

Application ↑	↑ Clients	↑ Servers	↑ Protocols	↑ Server Locations	↑ Connections ⓘ	↓ Total Throughput	Downstream Throughput ↑	Upstream Throughput ↑	Throughput Trend (MBps) ↑
Microsoft Windows Update Service	31	2	2	2	9,224	340.5 Mbps / 77.7%	328.0 Mbps	12.6 Mbps	
mega-crm	1216	8	1	4	30,798	27.2 Mbps / 6.2%	26.7 Mbps	562.1 Kbps	
Unknown	22	16	2	6	717	16.2 Mbps / 3.7%	1.9 Kbps	16.2 Mbps	

Powerful Views, Seamless Integration

Traffic Insights combines power with flexibility

Intuitive User Interface

Access views directly or via path visualization

- Assess performance over 30-day window for before / during / after analysis
- Filter / group data to quickly zero in on root cause

Customizable Alerts

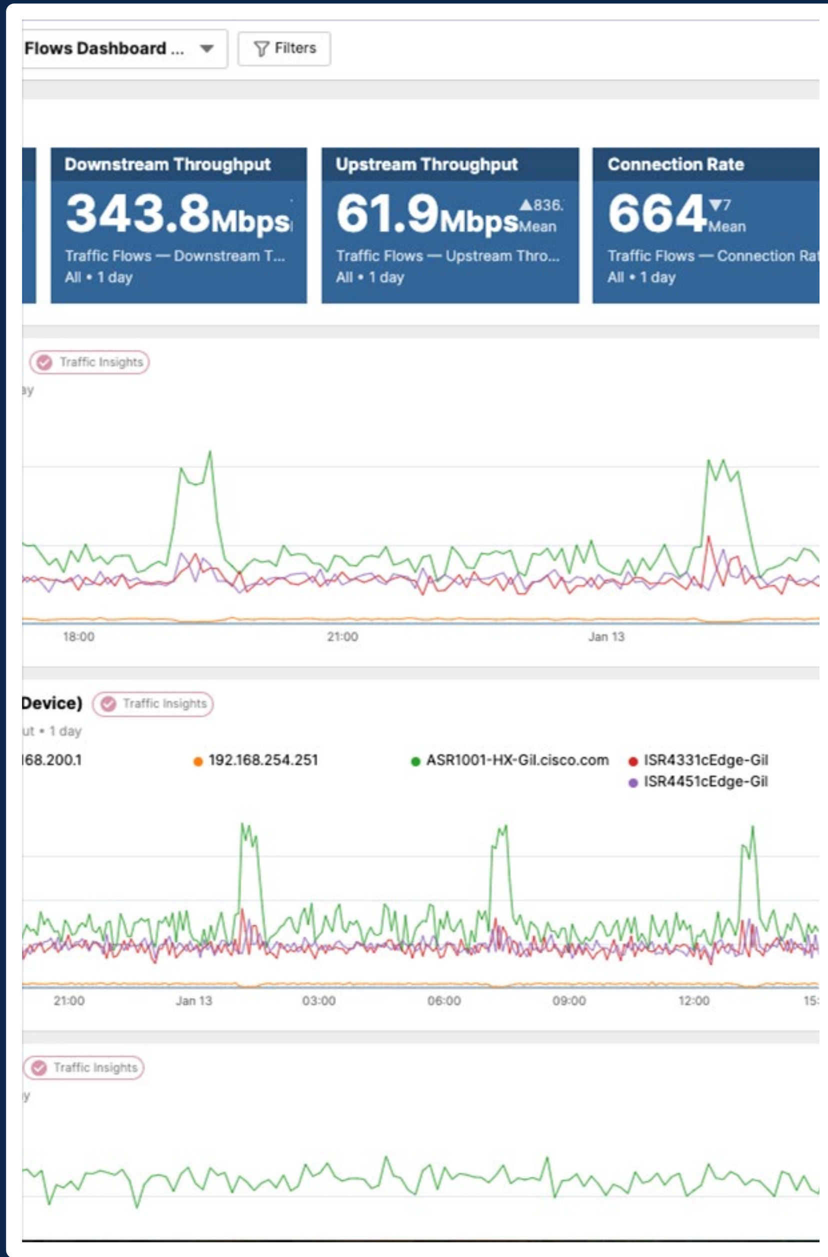
Respond immediately when traffic levels spike

- Leverage flow-specific thresholds
- Integrate with ITSM via built-in integrations or custom webhooks

Custom Dashboards and Reporting

Understand trends, anticipate issues

- View usage data according to user preference
- Pre-configured or customizable widgets



Scalable Visibility Across the Enterprise

Activate Traffic Insights at any location with an Enterprise Agent

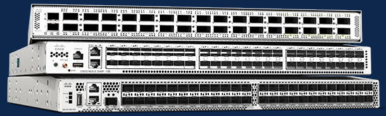
Flexible deployment options

- Physical or virtual appliance
- Native Linux
- Docker container
- Cisco Networking – branch, campus, datacenter

Simple, straightforward activation

NetFlow and IPFIX collection & forwarding

Compatible with external collectors


Nexus 9000 Switches

Catalyst 9000 Switches

Catalyst 8000 Routers

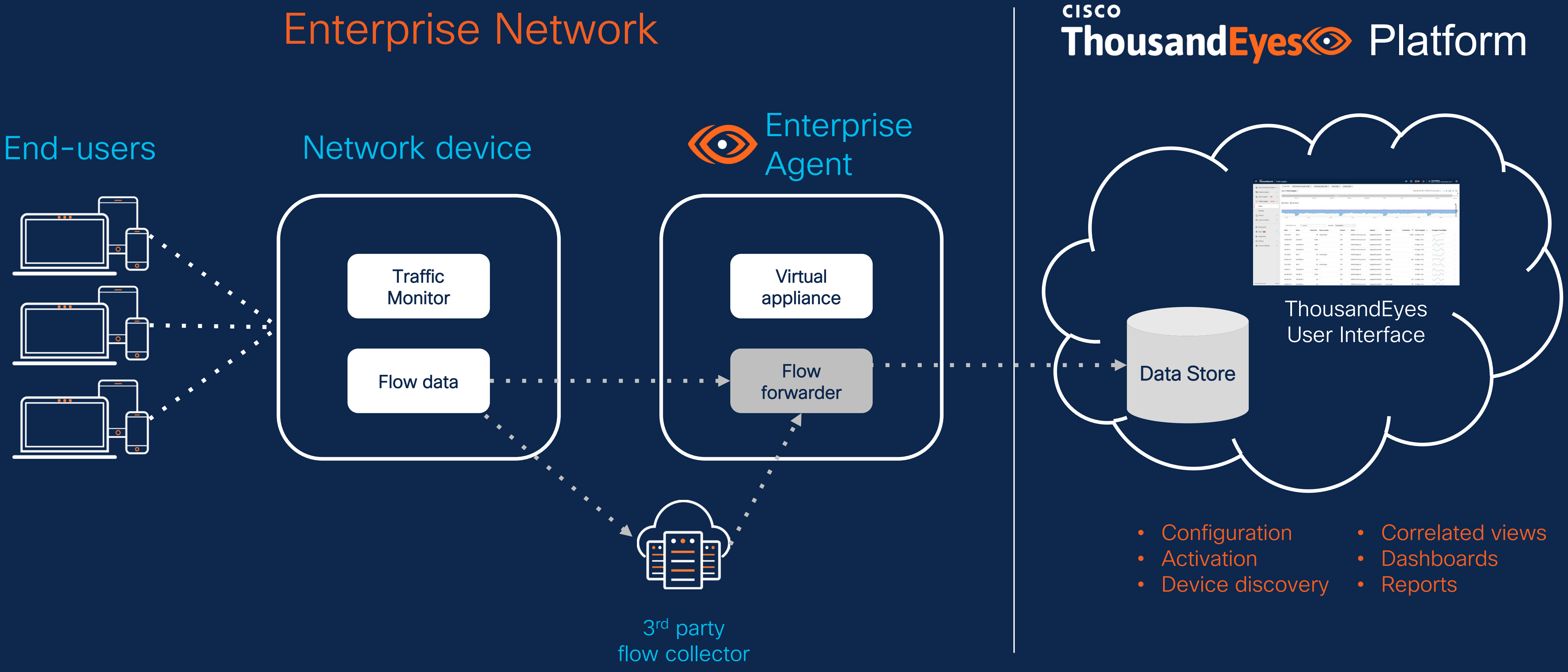
ISR 4000 Series

ASR 1000 Series

ISR 1000 Series

Meraki MX

A Unique Solution to a Complex Problem



Enterprise Network

cisco ThousandEyes Platform

End-users

Network device

Traffic Monitor

Flow data

Enterprise Agent

Virtual appliance

Flow forwarder

3rd party flow collector

Data Store

ThousandEyes User Interface

- Configuration
- Activation
- Device discovery

- Correlated views
- Dashboards
- Reports

ThousandEyes

DEMO

ThousandEyes

part of Cisco