

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright, multi-colored sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Unleashing the power of ThousandEyes collective intelligence to troubleshoot outages

Mike Hicks
@apnoau
BRKAPP-2360

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

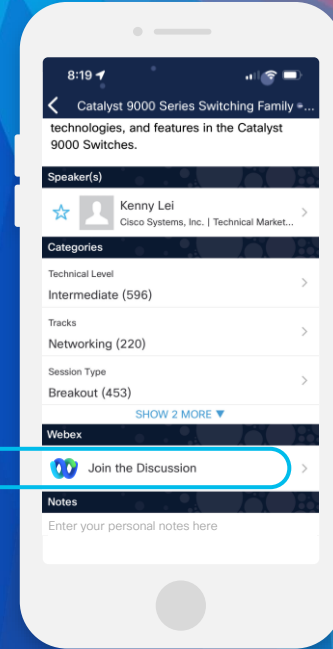
Questions?

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 December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP-2360>

Who is Mike Hicks?



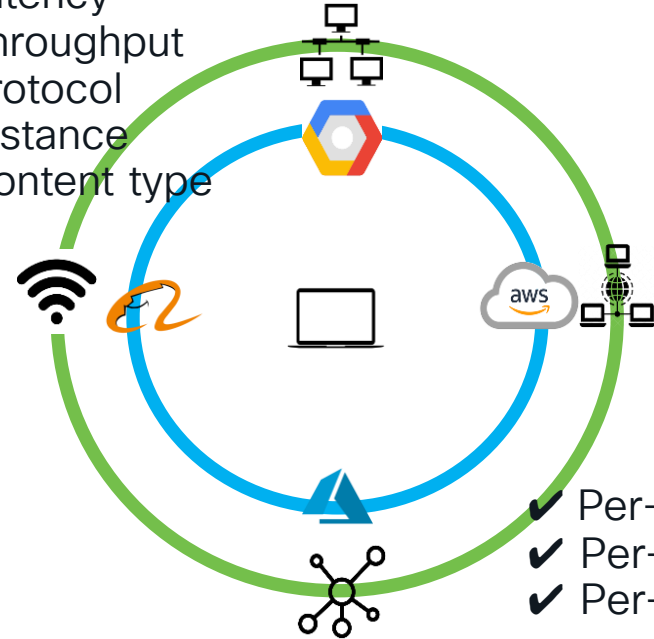
- Over 30 years of experience in network and application performance.
- Worked with infrastructure vendors on application profiling and management.
- Author of "Managing Distributed Applications: Troubleshooting in a Heterogeneous Environment" (Prentice Hall 2000) and "Optimizing Applications on Cisco Networks" (Cisco Press 2004).



The View From The Network

- Many causes of poor end-user performance are in the network.
- Network architecture, type of client, client network, type of content being delivered, status of the server serving the content, can all contribute.
- Applications have varying performance characteristics when delivered over different kinds of networks.
- Contextual and complete awareness of heterogeneous network environment is required

- ✓ Latency
- ✓ Throughput
- ✓ Protocol
- ✓ Distance
- ✓ Content type



- ✓ Per-Application
- ✓ Per-location
- ✓ Per-network

Unavoidable scale and complexity of today's service delivery

Digital experience is not monolithic

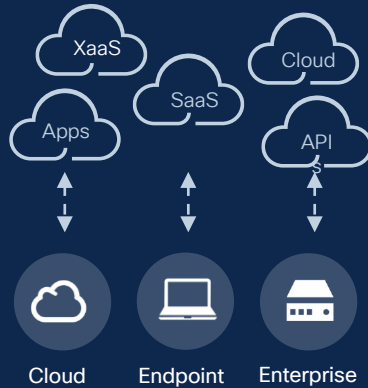
You don't own (by design) most dependencies

Fixing what you own isn't good enough

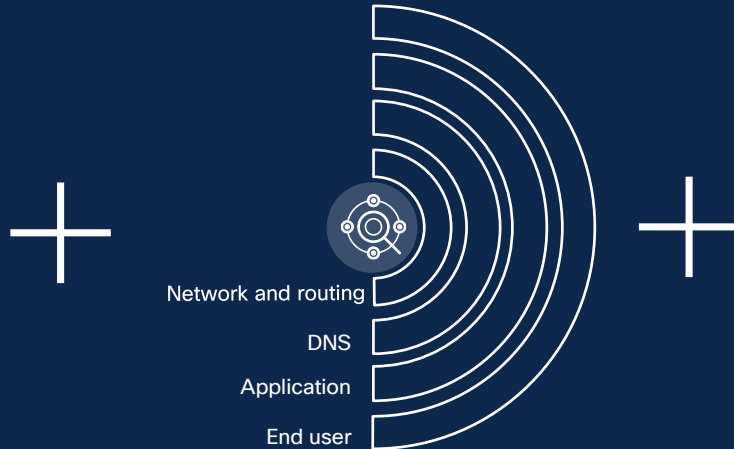


Applying Collective intelligence

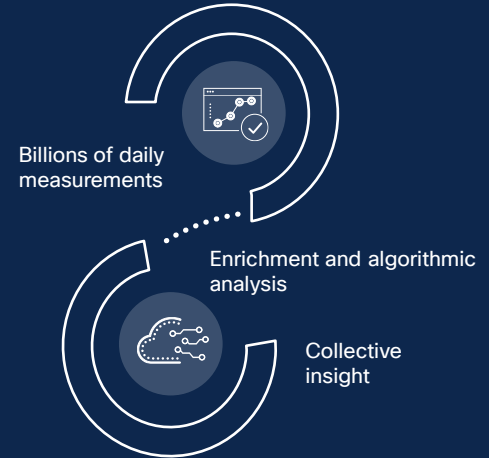
1000s of Global
Vantage Points



X-layer Telemetry



Global Collective
Insight



End-to-end **command** of service delivery

SITUATIONAL AWARENESS

Are regional ISPs spoofing our DNS records?

CUSTOMER SUPPORT

Is an Internet outage preventing users from reaching our service?

NETWORK SECURITY

Are SASE routing policies working as we expect?

RISK AND COMPLIANCE

Is our traffic getting routed out of region?

SERVICE RECOVERY

Did we successfully cut over to our DDoS mitigation service?

REVENUE PROTECTION

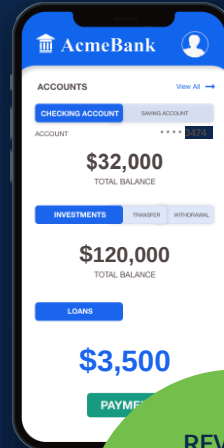
Is the payment gateway down or just unreachable?

WORKFORCE PRODUCTIVITY

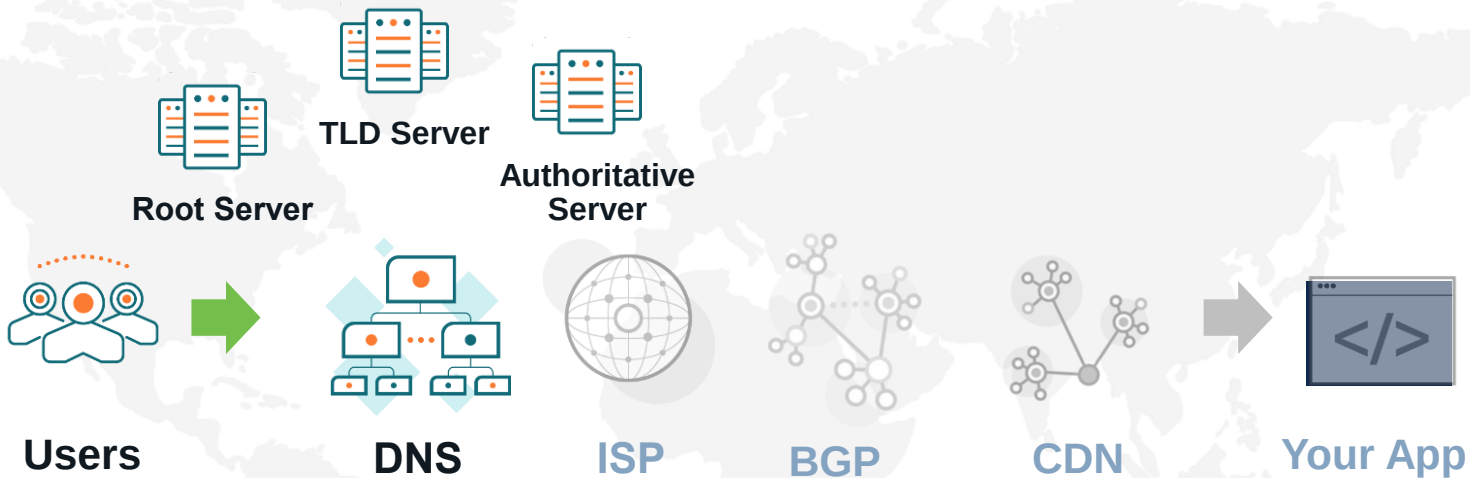
Will our Salesforce dev updates degrade performance for some global users?

SERVICE PLANNING

Which cloud regions should we choose?



Step 1: DNS – Where are We Going?



Step 2: How do We Get There?



Step 3: CDNs - Do We Have to Travel So Far?



Protocols on Protocols

- Simple and convenient experiences are easy to take for granted.
- A complex web of technologies that power those experiences.
- Understand the impact of the network on the application
- And application on the network



Anatomy of an outage

- Understanding different types of internet outages is important to mitigate their impact
- Outages can vary in blast radius, be planned or unplanned, and have varying MTTR
- Network outages depend on where the problem occurs, with transit network incidents impacting multiple providers

Symptoms

Packet loss: **High**

Latency: **Increased**

Path Length: **Hops increased**

Route: **Suboptimal, misdirected**

Access: **Initial**

Network connectivity: **Degraded**

Prefixes: **Unaffected**

Device Layer: **Unaffected**

Cause

BGP Hijack



Who to involve

Responsible: **ISP, NetOps**

Accountable: **NetOps**

Consulted: **SecOps**

Inform: **Executives**

Actions To take

Re-advertise BGP route using alternate prefix

Update and propagate DNS records with revised IP mappings



Packet loss: **High**

Latency: **Increased**

Path Length: **Hops increased**

Route: **Suboptimal**

Access: **Initial**

Network connectivity: **Degraded**

Prefixes: **Affected**

Device Layer: **Unaffected**

BGP Route Leak

Responsible: **ISP**

Accountable: **NetOps**

Consulted: **SecOps**

Inform: **Executives**

Contact your ISP with evidence
(e.g. ThousandEyes Share Link)

Re-advertise preferred routes
using more specific prefixes

Symptoms

Packet loss: **Total**

Latency: **Max**

Path Length: **Hops fluctuate**

Route: **Unstable** (with periodic stabilization)

Access: **Inaccessible**

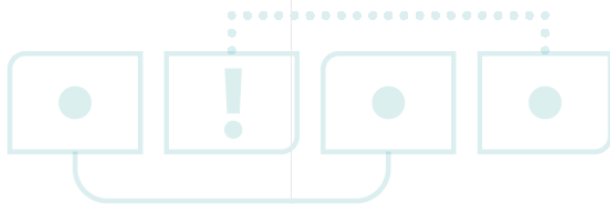
Network connectivity: **Degraded**

Prefixes: **Unaffected**

Device Layer: **Unaffected**

Cause

BGP Route Flap



Who to involve

Responsible: **ISP, NetOps**

Accountable: **NetOps**

Consulted: **Network Architects**

Inform: **Executives**

Actions To take

Wait for the routing table to stabilize through the use of route dampening and route aggregation

Re-advertise route prefixes under a different prefix or via another network



Packet loss: **Very high**

Latency: **High**

Path Length: **Hops increased**

Route: **Suboptimal**

Access: **Inaccessible**

Network connectivity: **Unavailable**

Prefixes: **Unaffected**

Device Layer: **Locked**

DDoS Attack

Responsible: **ITOps, ISP, DDoS Mitigation Provider**

Accountable: **SecOps**

Consulted: **NetOps**

Inform: **Executives**

Divert traffic to a DDoS mitigation service

Re-advertise DNS with revised IP mapping



Packet loss: **Some**

Latency: **High**

Path Length: **Hops increased**

Route: **Misdirected**

Access: **Accessible**

Network connectivity: **Degraded**

Prefixes: **Unaffected**

Device Layer: **Unaffected**

DNS Hijacking & Poisoning



Responsible: **ITOps**

Accountable: **System Admins**

Consulted: **NetOps**

Inform: **SecOps**

Flush DNS, readvertise DNS

Instigate [DNSSEC across your domains](#)

Readvertise DNS name under an alternative prefix

Diversify CDN providers

Consider configuring several case-sensitive recursive DNS entries to limit/prevent future DNS hijackings

Quarantine and assess damage (i.e., loss of data) to mitigate follow-on attack



Packet loss: **Total**

Latency: **High**

Path Length: **Hops increased**

Route: **Suboptimal**

Access: **Inaccessible (at times)**

Network connectivity: **Unavailable**

Prefixes: **Unaffected**

Device Layer: **Unaffected**

**ISP Infrastructure
(Outage)**

Responsible: **ISP**

Accountable: **NetOps**

Consulted: **Network Architects**

Inform: **Executives, Comms**

Revert to a backup circuit if that capability is available

Inform your ISP with evidence (i.e., a ThousandEyes Share Link)

Automate the fail-over process as a best practice

Assess ISP service during and after the outage to determine future mitigation options



Packet loss: **Total**

Latency: **High**

Path Length: **Hops increased**

Route: **Suboptimal**

Access: **Accessible (generally)**

Network connectivity: **Degraded**

Prefixes: **Unaffected**

Device Layer: **Unaffected**

**Cloud Provider Network
(Outage)**



Responsible: **Cloud provider**

Accountable: **DevOps**

Consulted: **NetOps**

Inform: **Executives, Comms**

Assess wherein the digital service delivery chain the outage is occurring

Have DevOps mitigate through reconfiguration

Contact cloud provider to notify them of the fault domain



Packet loss: **High**

Latency: **High**

Path Length: **Hops minimally affected**

Route: **Inaccessible**

Access: **Inaccessible**

Network connectivity: **Degraded**

Prefixes: **Unaffected**

Device Layer: **Degraded**

**Operator Error/
Configuration Error
on Infrastructure**

Responsible: **NetOps, DevOps**

Accountable: **ITOps**

Consulted: **Network Architects**

Inform: **Helpdesk, Executives,
Comms**

Identify fault domain

Correlate with change control/release schedule

Rollback change

Analyze cause

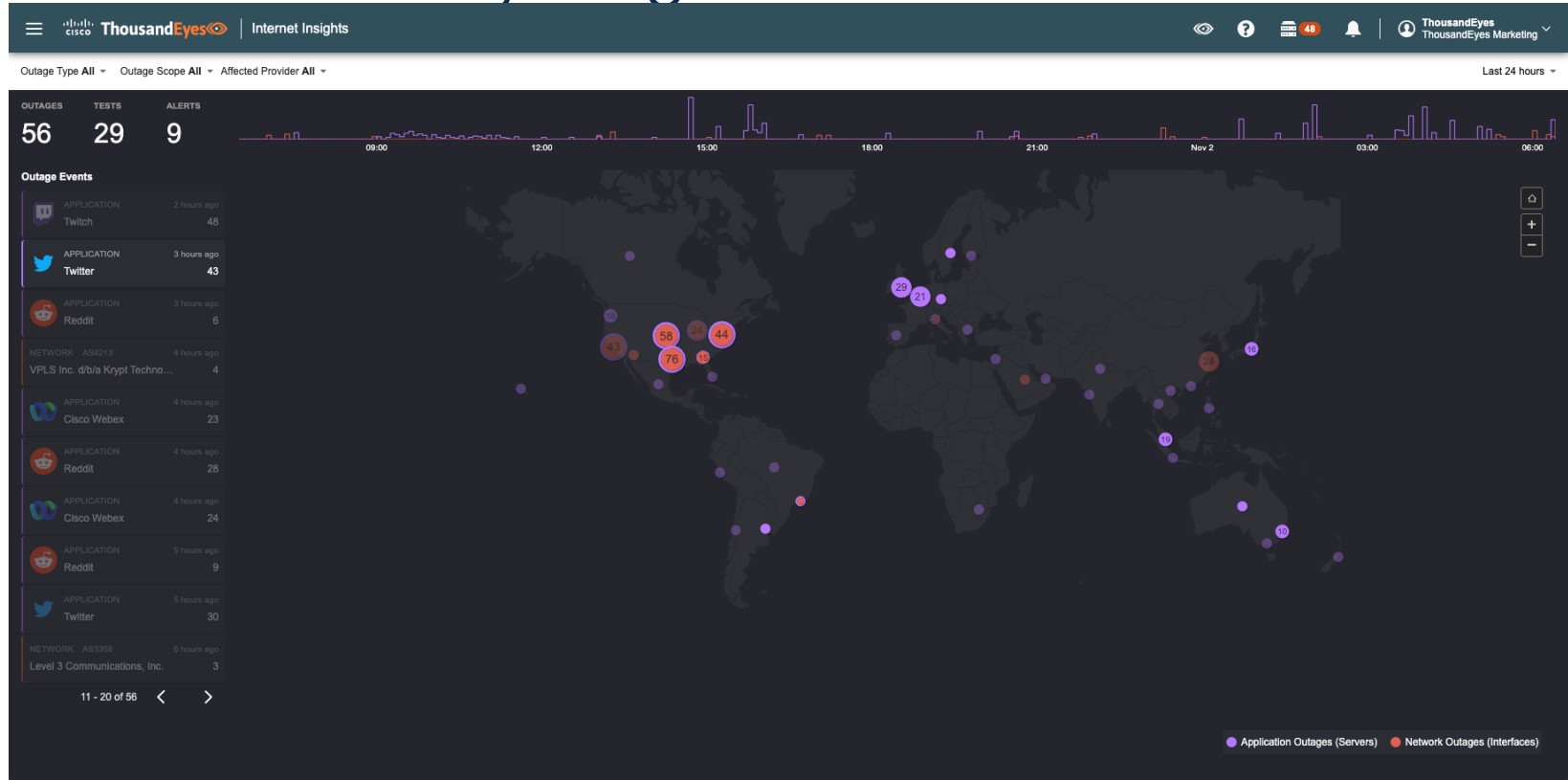
Implement fix



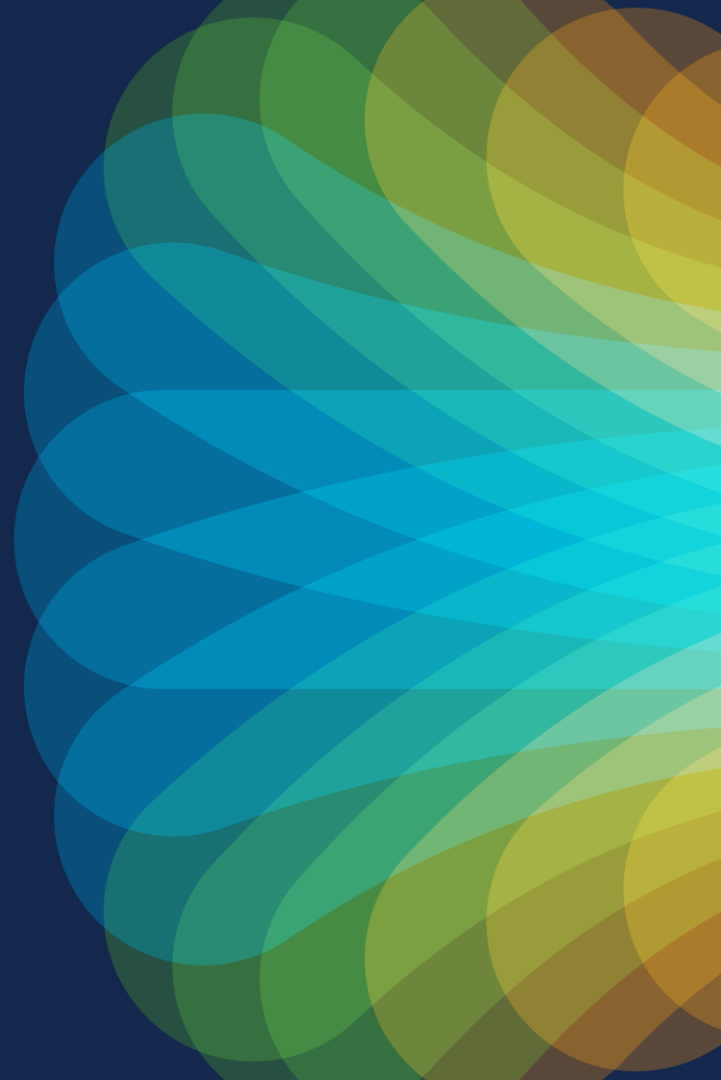
*“If we could first know where we are,
and whither we are tending, we
could then better judge what to do,
and how to do it.”*

Abraham Lincoln

Context is everything



Outages



But it's working for me?

Current Status by Service			✓ No Issues	🔧 Maintenance
Login/SSO No issues	✓	Connections No issues		
Messaging No issues	✓	Files No issues		
Notifications No issues	✓	Huddles No issues		
Search No issues				
Workspace/Org Adm No issues				
Canvases No issues				

End users may experience 403 forbidden error

Status

RESOLVED

Category

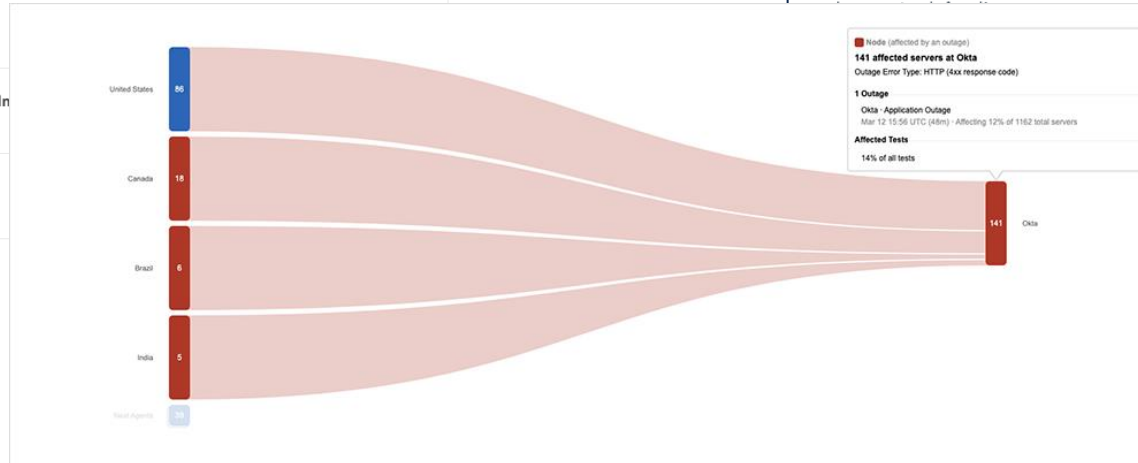
Service Degradation

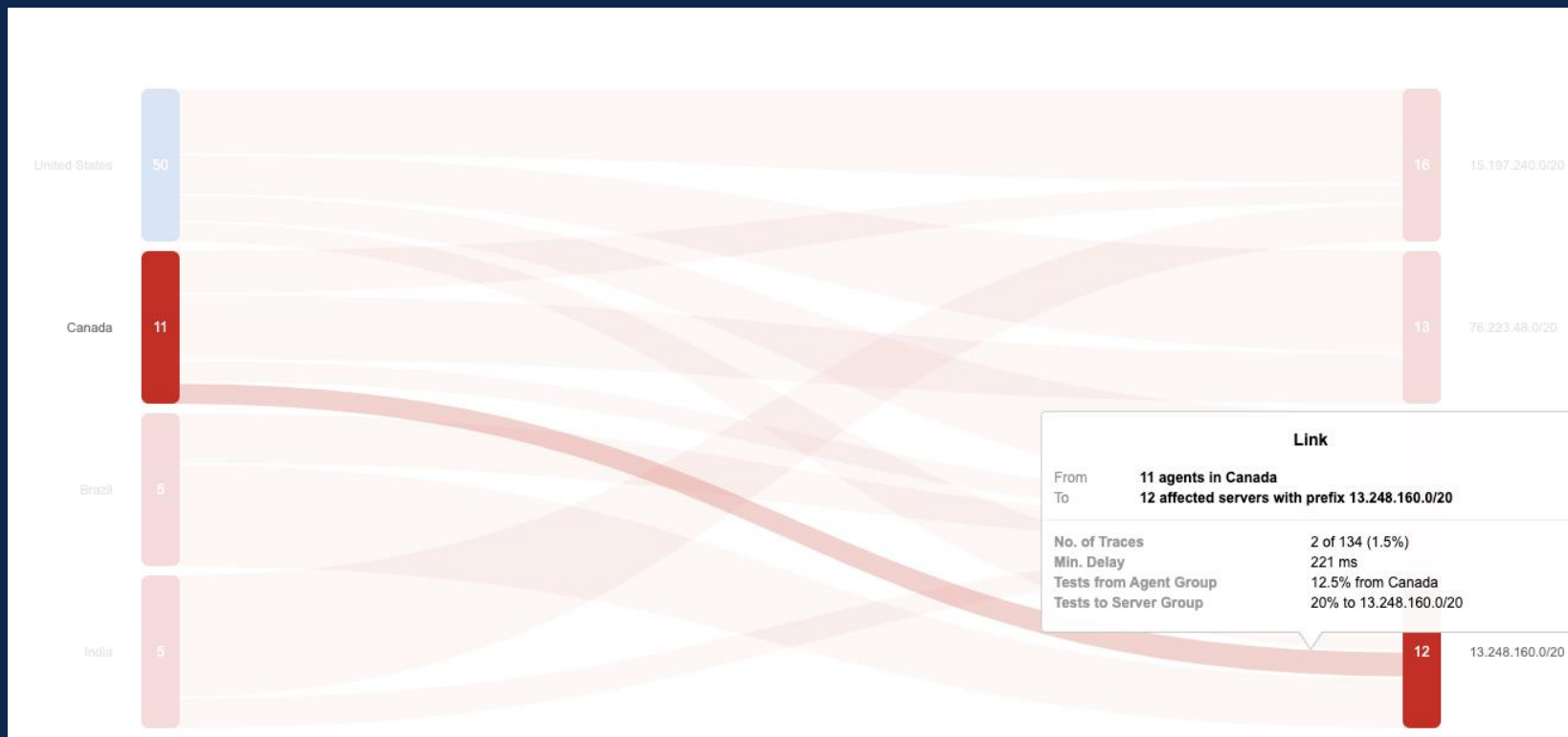
Impacted Cell(s)

OK1 Cell (US), OK2 Cell (US), OK3 Cell (US), OK4 Cell (US)

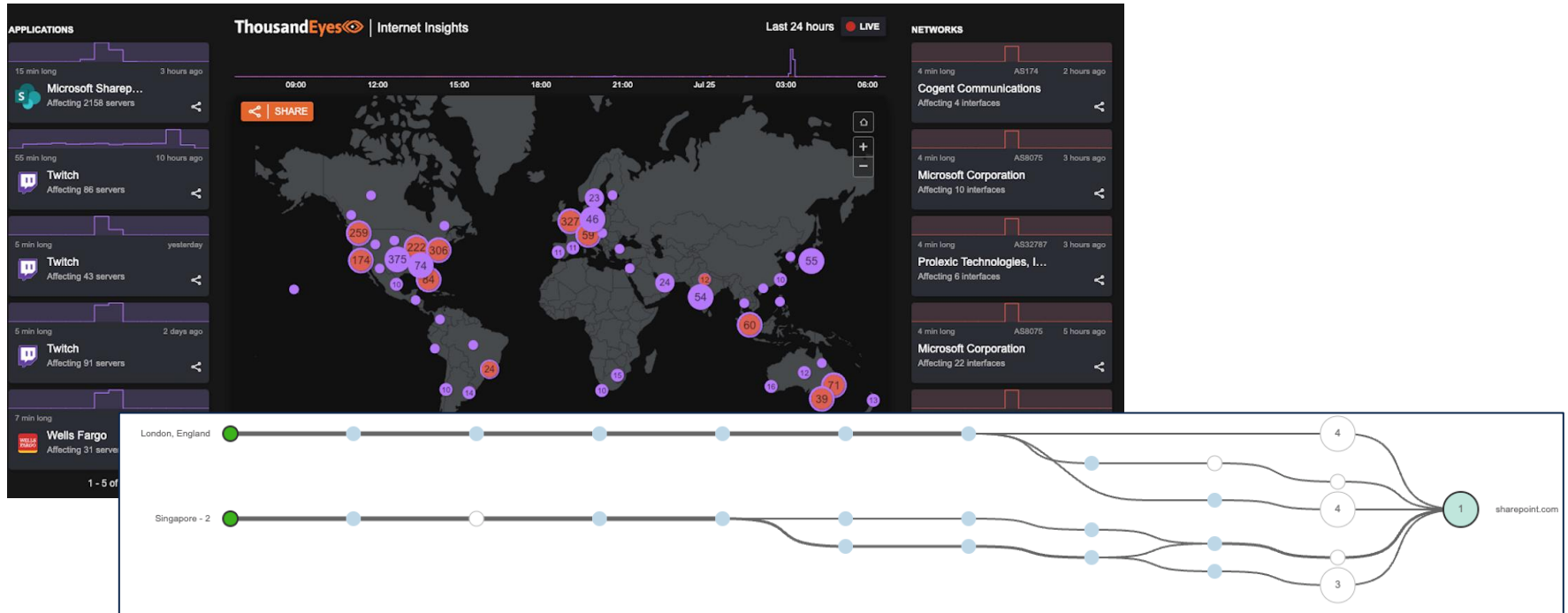
Impacted Services(s)

Okta Services: Core Platform

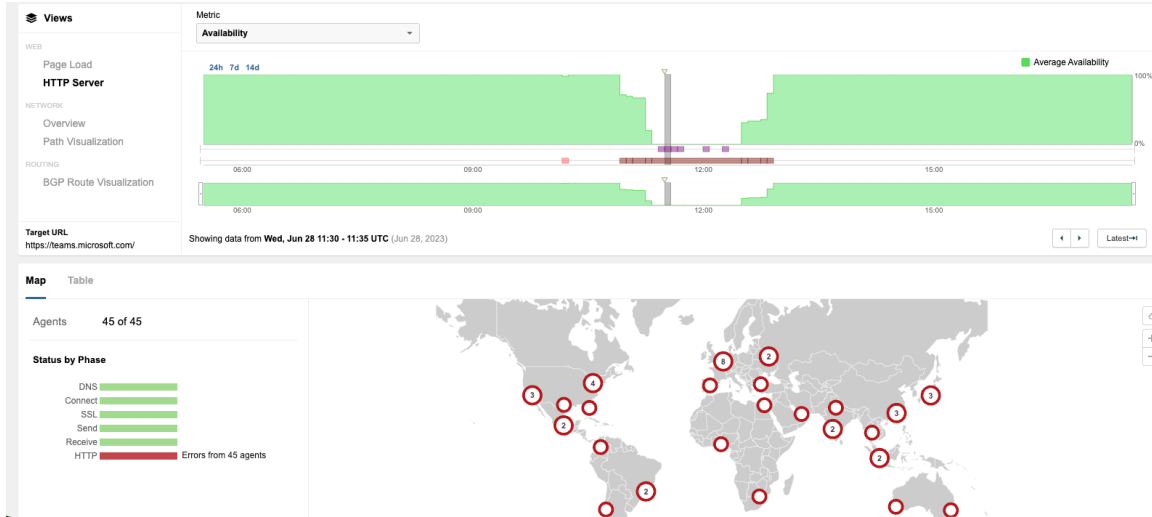
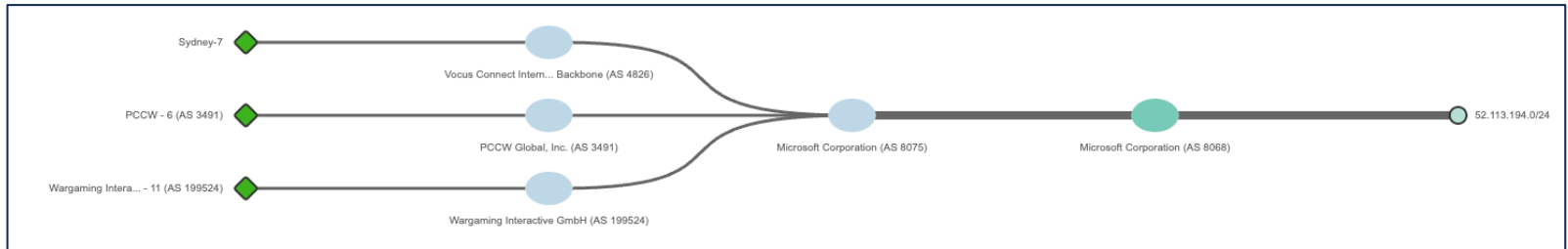


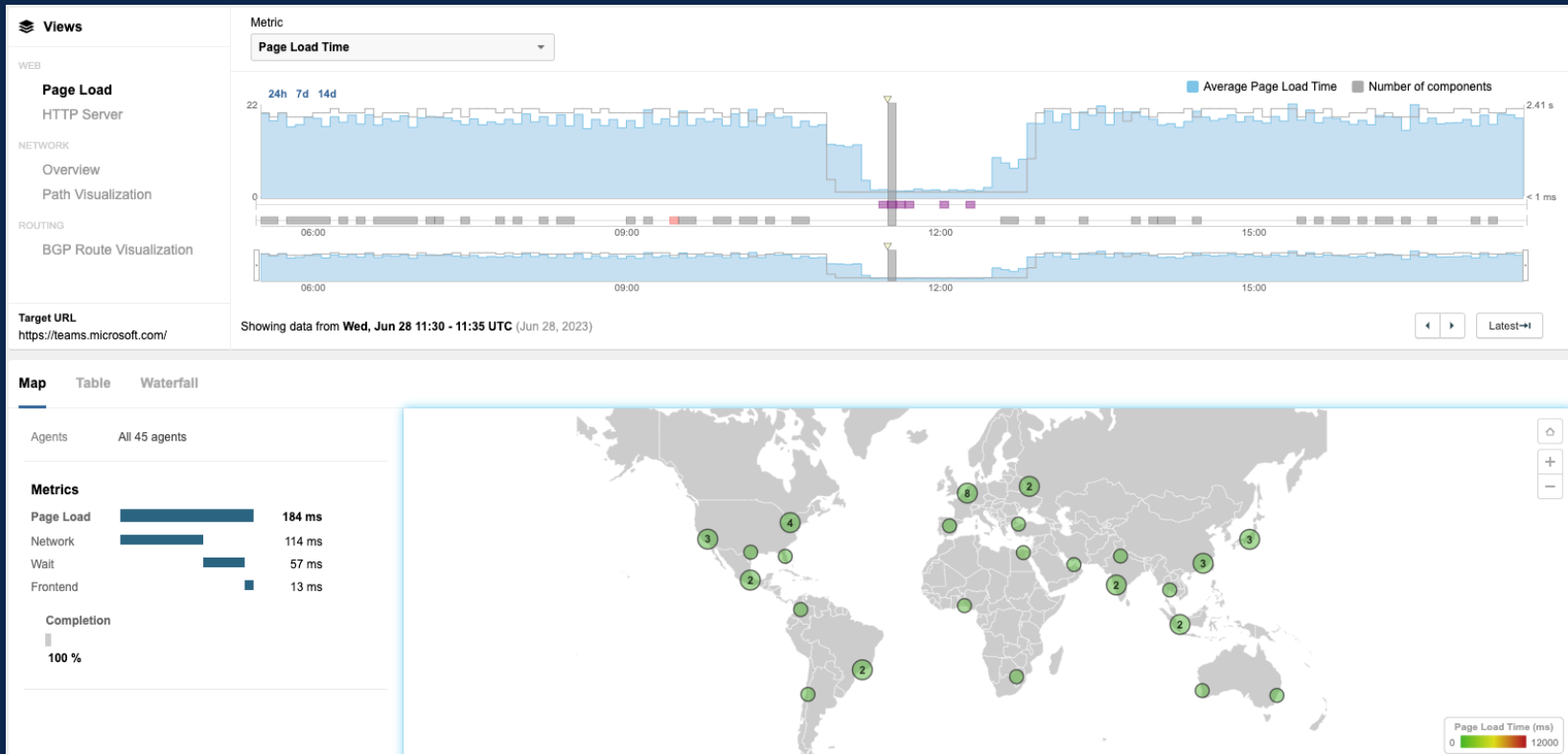


Network or Application?

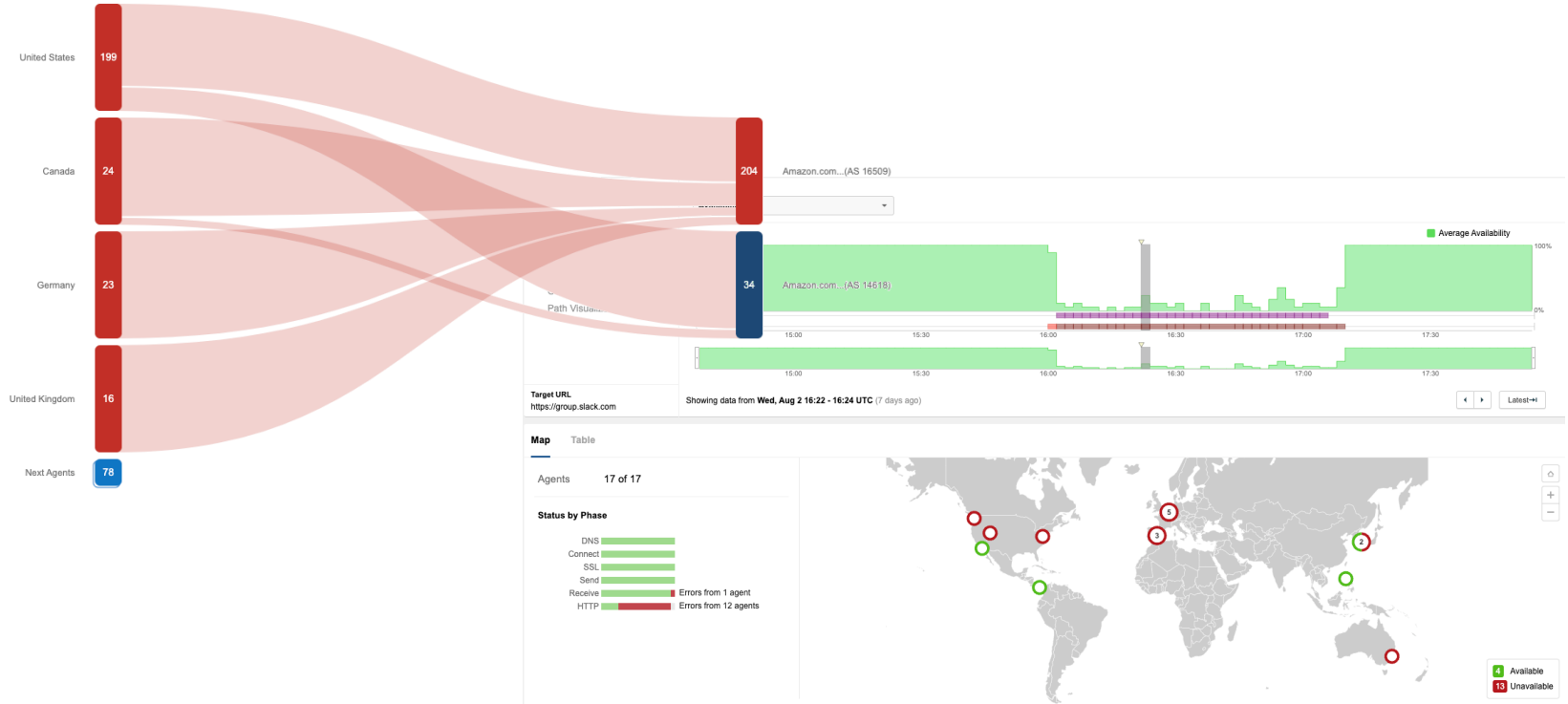


When is a door not a door?

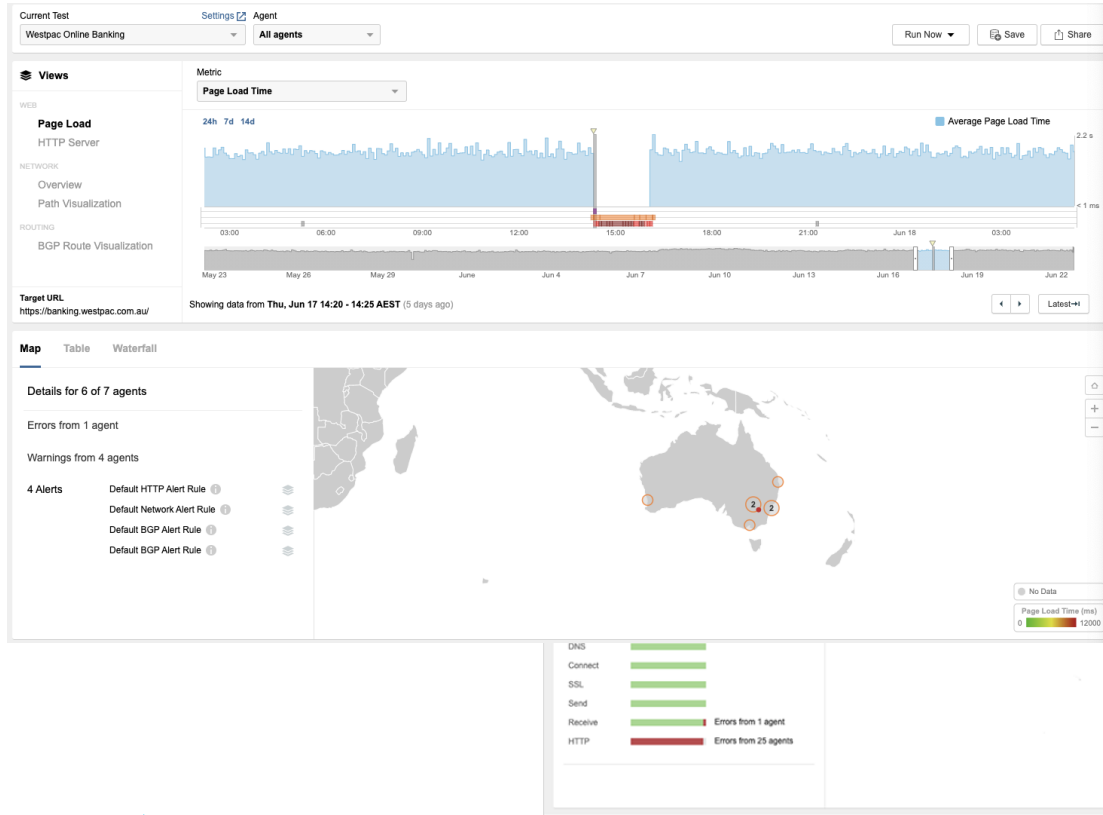


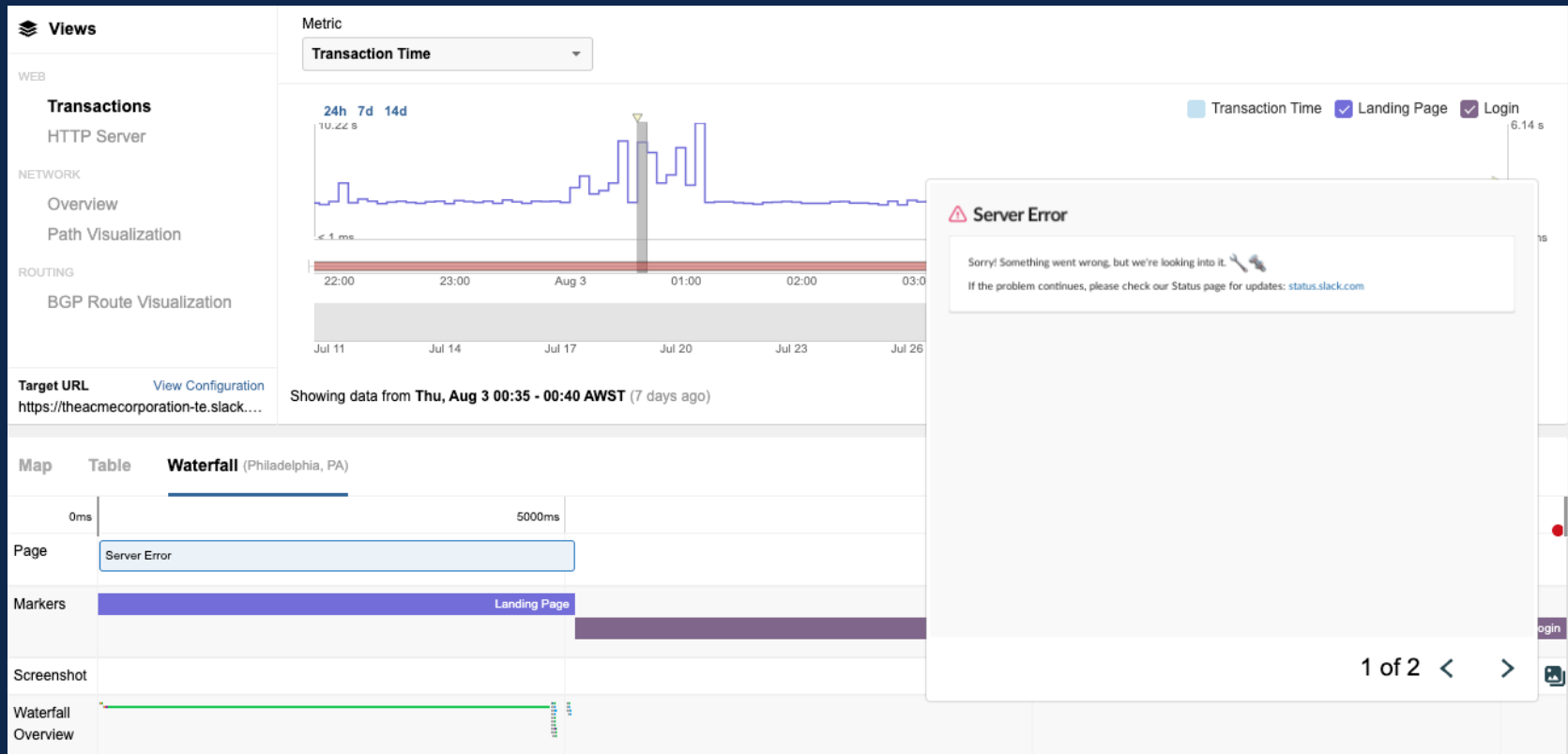


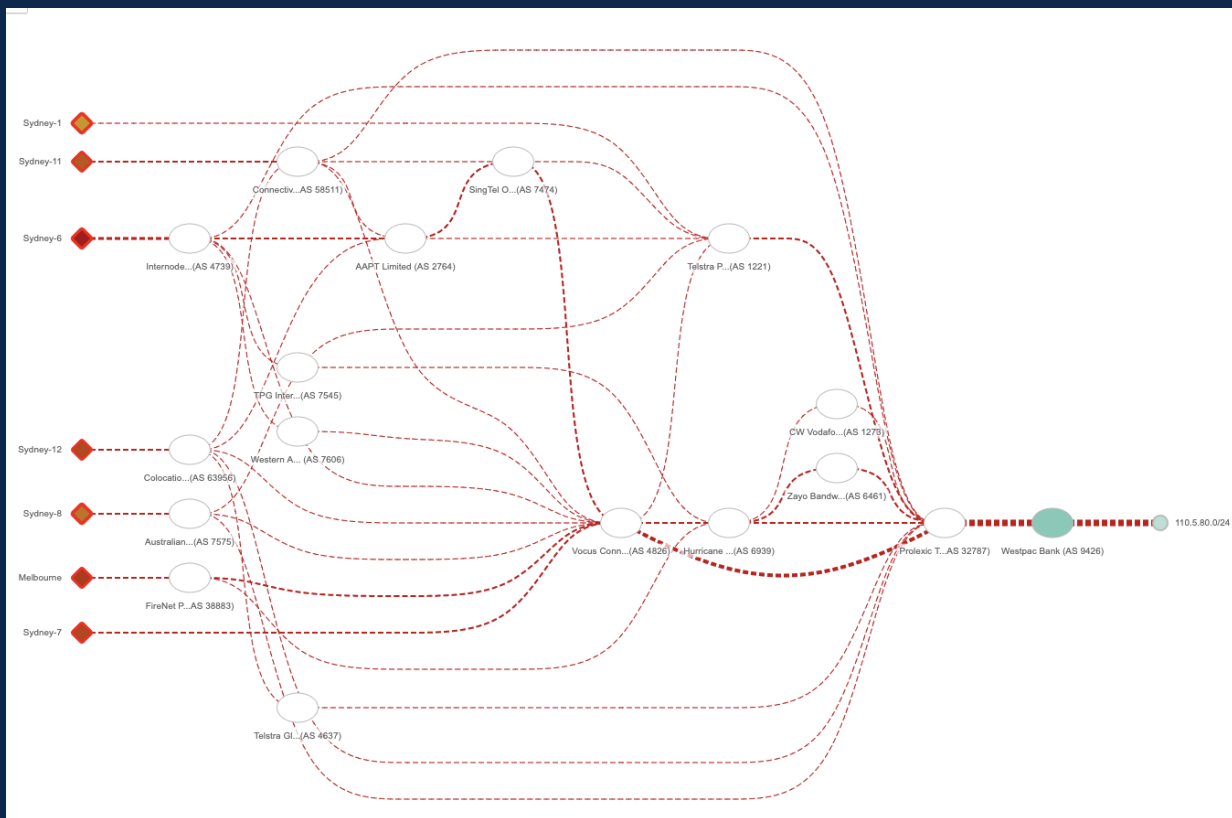
Its not me its you? – Backend Functional Failure



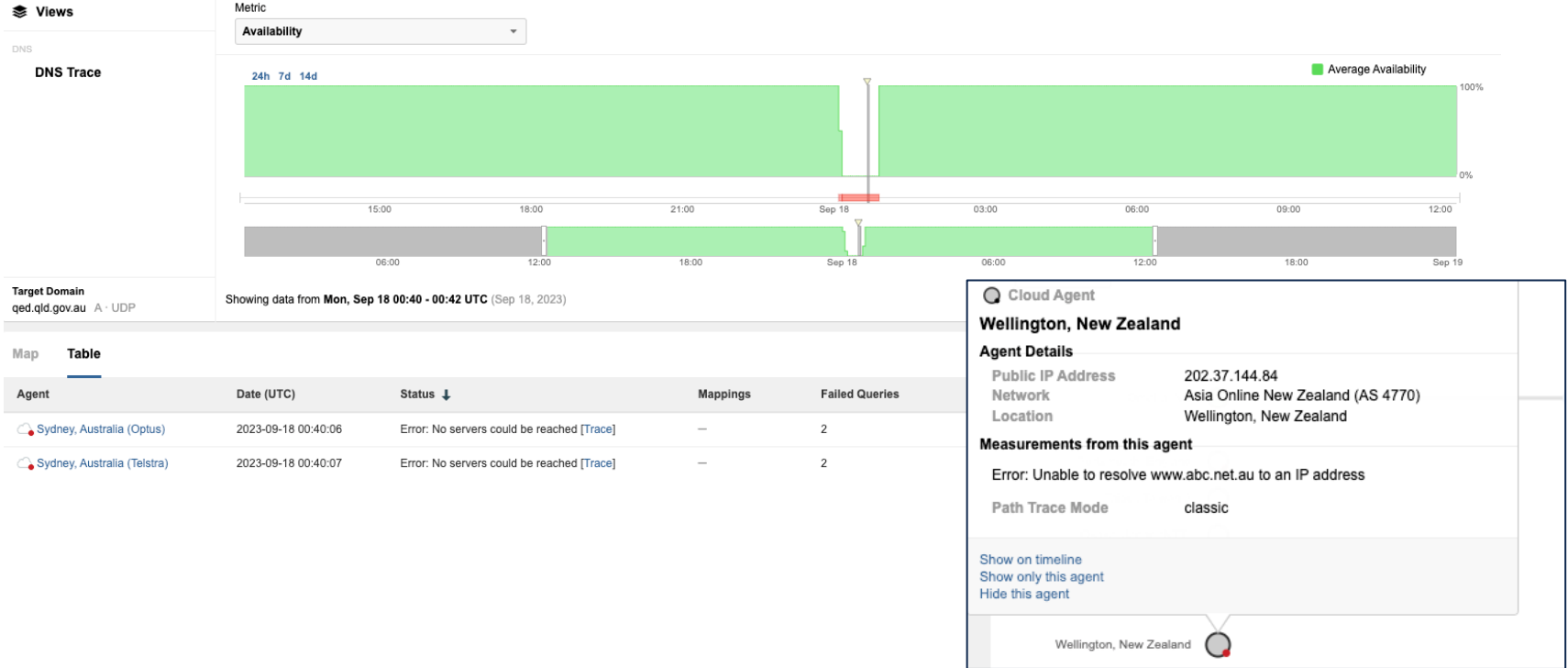
Network Service Outage

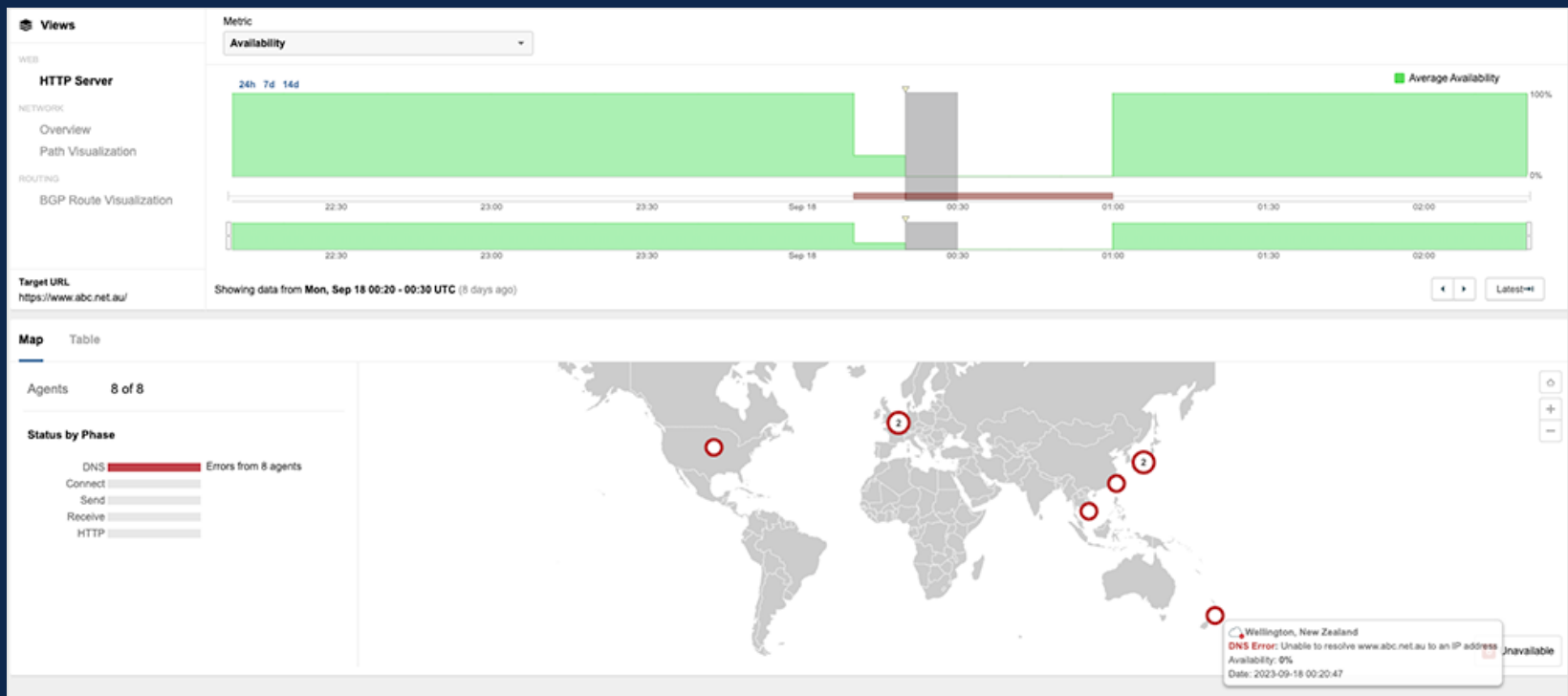




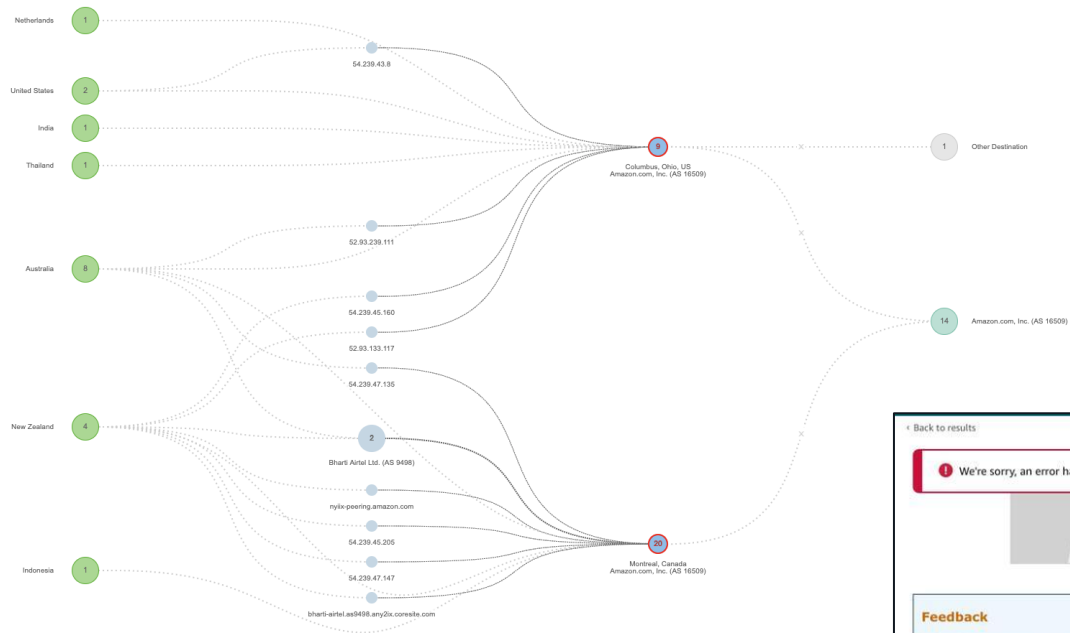
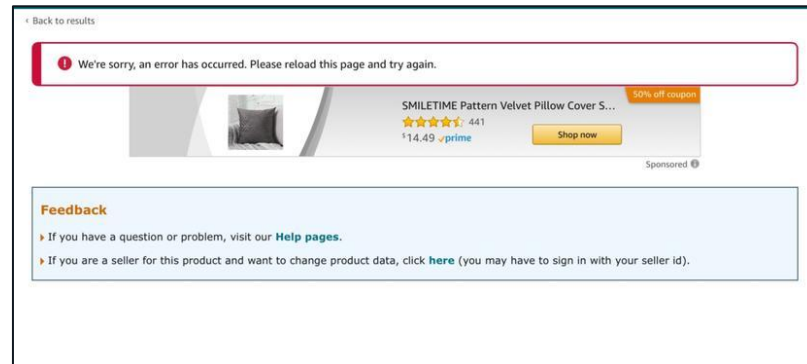


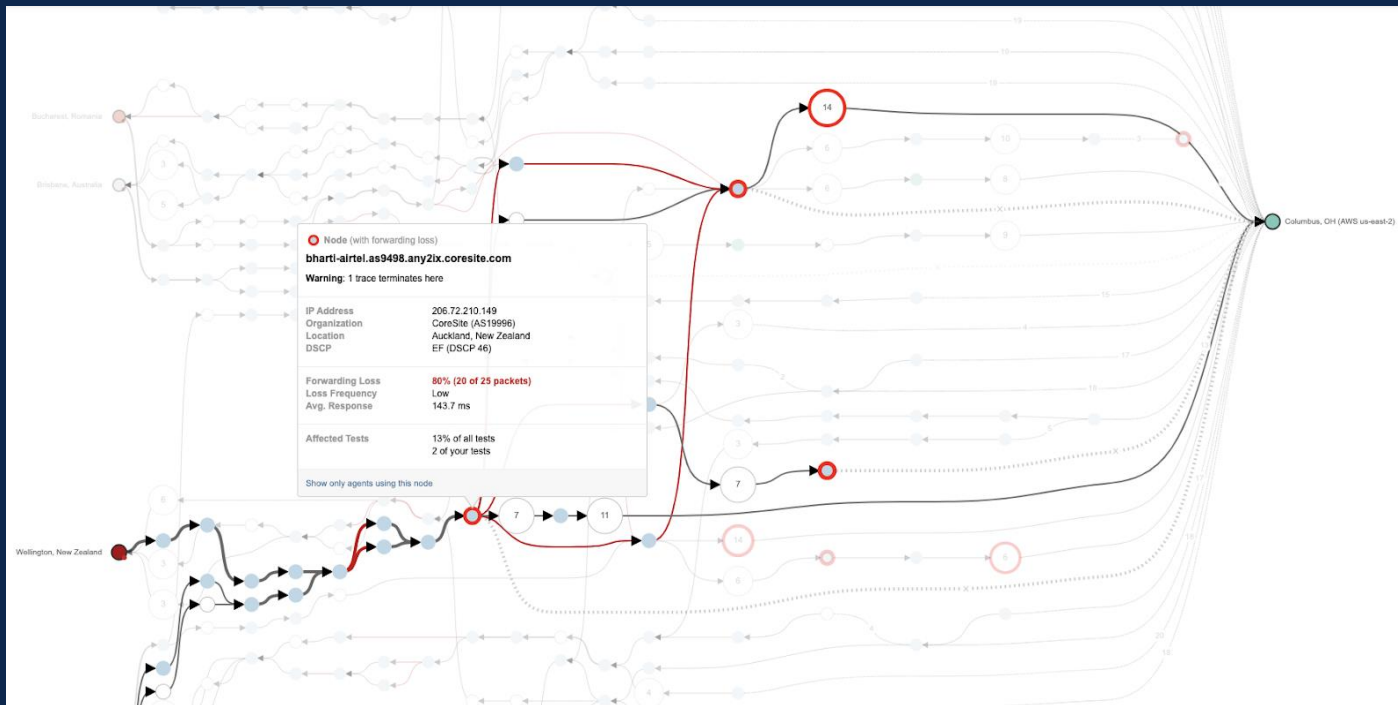
It could be DNS ?





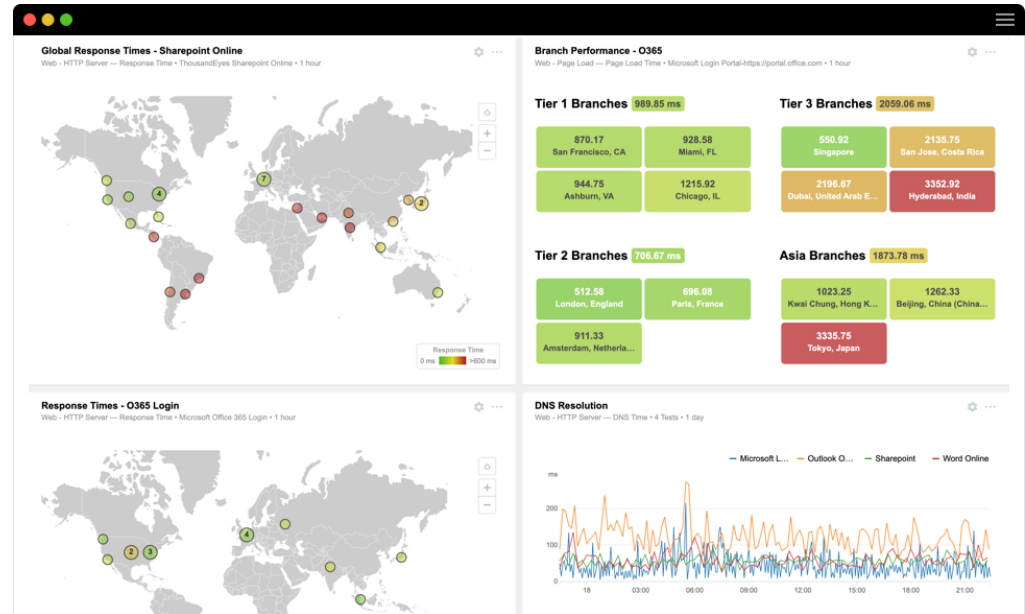
The Butterfly Effect – why should I care?





Presenting empirical evidence

- Describe what you see
- Show behavioral patterns
- Intuitive representation
- Common format



Take aways

- Understanding how your application works is important for quickly identifying failures and making improvements.
- Just because your application is working doesn't mean it's functioning optimally.
- Knowing how all parts of the service work together is crucial for ongoing design and future optimizations.
- Improved visibility and operational optimizations can prevent outages and minimize their impact.
- Tracking different categories of outages and degradations over time can be helpful.

Internet outages and research. Available 24x7.

ThousandEyes Internet Intelligence

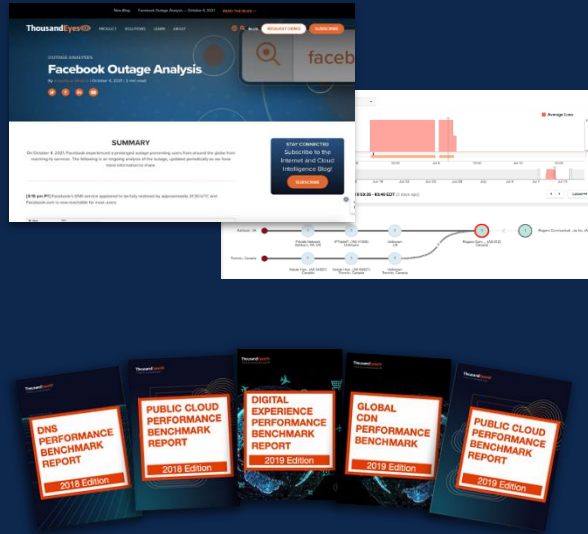
Subscribe to our blog



Follow us on



www.thousandeyes.com/outages
www.thousandeyes.com/blog
www.thousandeyes.com/research



CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt.



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert 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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of colorful rays in shades of blue, green, and yellow, creating a sunburst effect.

cisco *Live!*

Let's go

#CiscoLiveAPJC