ANM
TECH DAY

Your VPN called. It's time to move on with Universal ZTNA.

Zero trust isn't a buzzword anymore. It's the architecture your users, devices, and data depend on.

Agenda

- Traditional Architecture
- SASE & Universal ZTNA
- SSE Vendor Comparison
- Cisco Secure Access
  - Architecture
  - Feature Deep Dive
- Challenges/Best Practices
- Key Takeaways
- Trivia Round
- References

Agustin Lozano

Solutions Architect, CCIE# 15915 (Routing/Switching & Security)

- 23+ years as a post-sales engineer troubleshooting, designing, implementing, & securing infrastructures across various industries throughout the country.
- ~5 years with ANM as pre-sales engineer assisting organizations position and adopt technologies
- Key focus areas: design & implementation of large scale, highly-available infrastructures, advanced routing, secured connectivity, & hardening attack surfaces.
- Passionate about working together to achieve desired outcomes.

Key Skills:

- Technology Research
- Outcome-Driven Solutions
- Technical Documentation
- Strategic Roadmap Planning
- Team Building

https://www.linkedin.com/in/agustin--lozano/

TECH DAY 2026

Traditional Architecture

The Problem with Traditional Networking & Security

Raise your hand if you're still running on-prem filtering today!

The Problem with Traditional

- Security services built around places.
- Remote Access VPN inherently grants access
- Inefficient backhaul traffic on-prem
- Limited by firewall horsepower for advanced features
- Lack of maintenance = insecure!
- Difficult to verify identity of users and devices
- Gaps in security protection & policy drift

Behavioral Shift Drove Architectural Change

- COVID changed work — not just 'remote", but at any hour & from any device.
- Majority of resources moving to SaaS/cloud, but not all
- Lack of granular end-to-end visibility to applications
- Even with 100% cloud architectures, still need a way to provide a unified access policy.

SOURCE

Cisco Talos
2024 Year in Review
Talos Incident Response

THE BLIND SPOTS SSE WAS BUILT TO FILL

Internet threats that bypass traditional security.

SHADOW SAAS

70K+

cloud apps in Cisco **App Discovery** — most orgs find 5× more than sanctioned.

CISCO SECURE ACCESS

LIVING OFF THE LAND

70%+

of Talos IR engagements involved **living-off-the-land techniques** — invisible to perimeter firewalls, caught by SSE inline inspection.

CISCO TALOS · 2024 YIR

TIME TO EXFIL

24hr

median time to **data exfiltration** after initial access — SSE's DLP + CASB catches this in-flight.

CISCO TALOS · 2024 YIR

60%

of Talos IR cases involved **identity-based attacks** — the #1 vector in 2024.

CISCO TALOS · 2024 YIR

47%

of malware delivered through **cloud & SaaS apps**, not traditional downloads.

NETSKOPE · 2024

26%

of users share data in **personal app instances** — #1 insider vector.

NETSKOPE · 2024

88%

of breaches caused by **human error** — accidental sharing, misdirected emails.

STANFORD / TESSIAN

WHY WE'RE STILL TALKING ABOUT THIS

Remote-Access VPN is now an attack surface, not a control.

SOURCES

Zscaler ThreatLabz
VPN Risk Report 2024 / 2025
Cisco Talos · 2024 Year in Review

This requires a new approach to networking and security...

ORG-LEVEL EXPOSURE

81%

of organizations are **extremely or very concerned** their VPN architecture will lead to a breach.

ZSCALER THREATLABZ · 2024

HIT LAST 12 MONTHS

56%

of organizations experienced one or more cyberattacks **via VPN vulnerabilities** in the last year.

THREATLABZ · 2025

NO SEGMENTATION

48%

of ransomware victims had **no network segmentation** — ZTNA eliminates flat-network lateral movement.

CISCO TALOS · 2024 YIR

65%

plan to adopt **zero trust** in the next 12 months.

THREATLABZ · 2025

#1

MFA misconfiguration or absence on remote access — the most common weakness across all Talos IR cases.

CISCO TALOS · 2024 YIR

60%

of Talos IR cases involved **identity-based attacks** — the #1 vector.

CISCO TALOS · 2024 YIR

45%

of attacked orgs reported **data exposure** as a direct VPN-incident outcome.

THREATLABZ · 2025

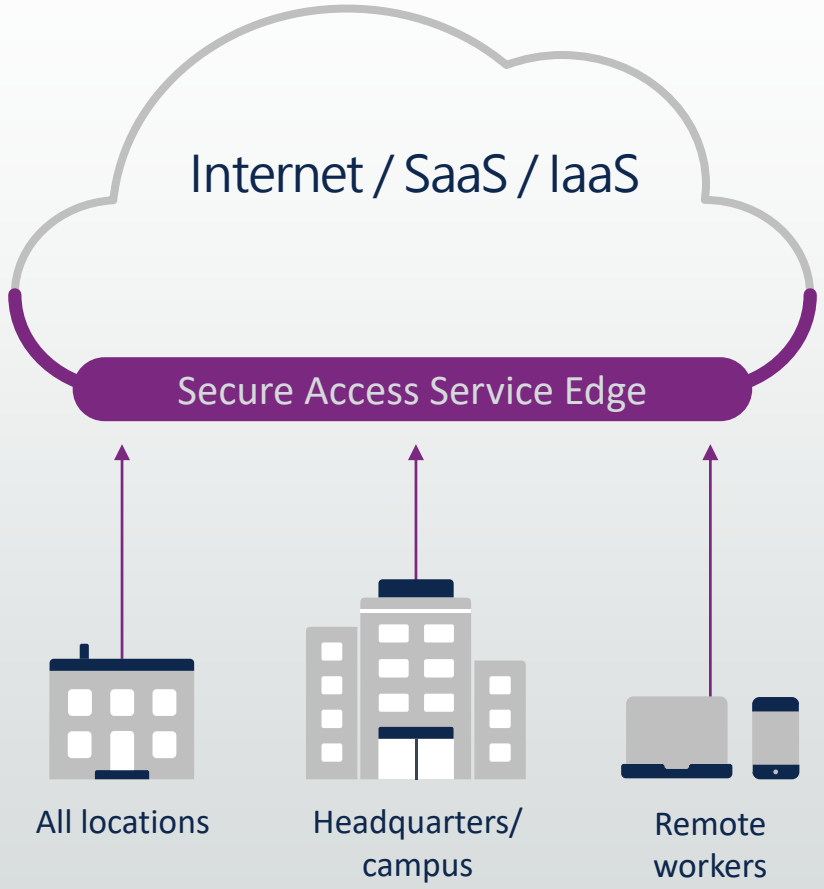
TECH DAY 2026

SASE & Universal ZTNA

Today's mobile & cloud-centric world

Drives the need for a Secure Access Service Edge (SASE) architecture

- **Connect users to the apps and data — in any environment, from anywhere**
- **Control access and enforce the right security protection consistently**
- **Combine networking and security functions in the cloud**



"The enterprise perimeter is no longer a location; it is a set of dynamic edge capabilities delivered when needed as a service from the cloud."

Gartner
The Future of Network Security is in the Cloud - Neil MacDonald, Lawrence Orans, Joe Skorupa, 2019

SOURCE

Gartner · August 2019 *The Future of Network Security Is in the Cloud*

Gartner SASE/SSE Authors

Who Defined Modern Secure Access

NEIL MACDONALD

THE ARCHITECT · SECURITY

DISTINGUISHED VP ANALYST

CONTRIBUTION

Convergence of **SWG, CASB, ZTNA & DLP** as a cloud-native platform.

LEGACY

Lead author of the **2019 SASE paper** and the **2021 roadmap** that introduced SSE.

JOE SKORUPA

THE NETWORKER · WAN

DISTINGUISHED VP ANALYST

CONTRIBUTION

The networking half — **SD-WAN & WAN edge** had to converge with security.

LEGACY

Co-author of the **2019 SASE paper** and the **WAN Edge Magic Quadrant** .

LAWRENCE ORANS

THE PRACTITIONER · SWG

VP ANALYST

CONTRIBUTION

17 yrs at Gartner. Lead author of the **SWG Magic Quadrant** .

LEGACY

Co-author of the **2019 SASE paper** that named the category.

JOHN WATTS

THE OPERATOR · ZTNA

VP ANALYST

CONTRIBUTION

Operationalized SSE — turned the category into the **SSE Magic Quadrant**.

LEGACY

Co-author of the **2021 SSE roadmap** ; lead author of every annual SSE MQ since 2022.

FOUNDATIONAL PAPERS · GARTNER RESEARCH

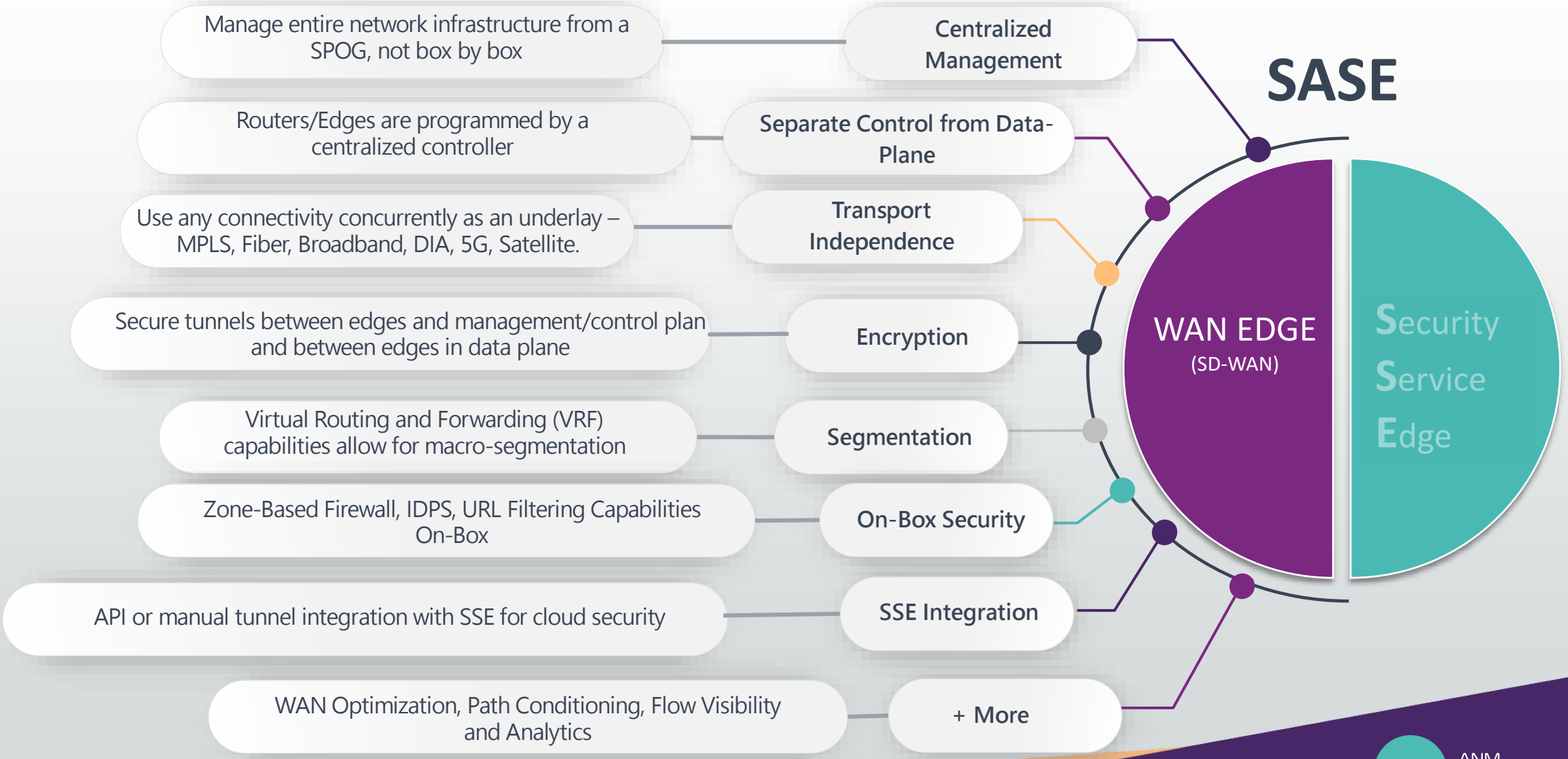
SASE — *The Future of Network Security Is in the Cloud* · MacDonald, Orans, Skorupa · **Aug 2019**

SSE — *2021 Strategic Roadmap for SASE Convergence* · MacDonald, Watts · **Mar 2021**

ANM TECH DAY

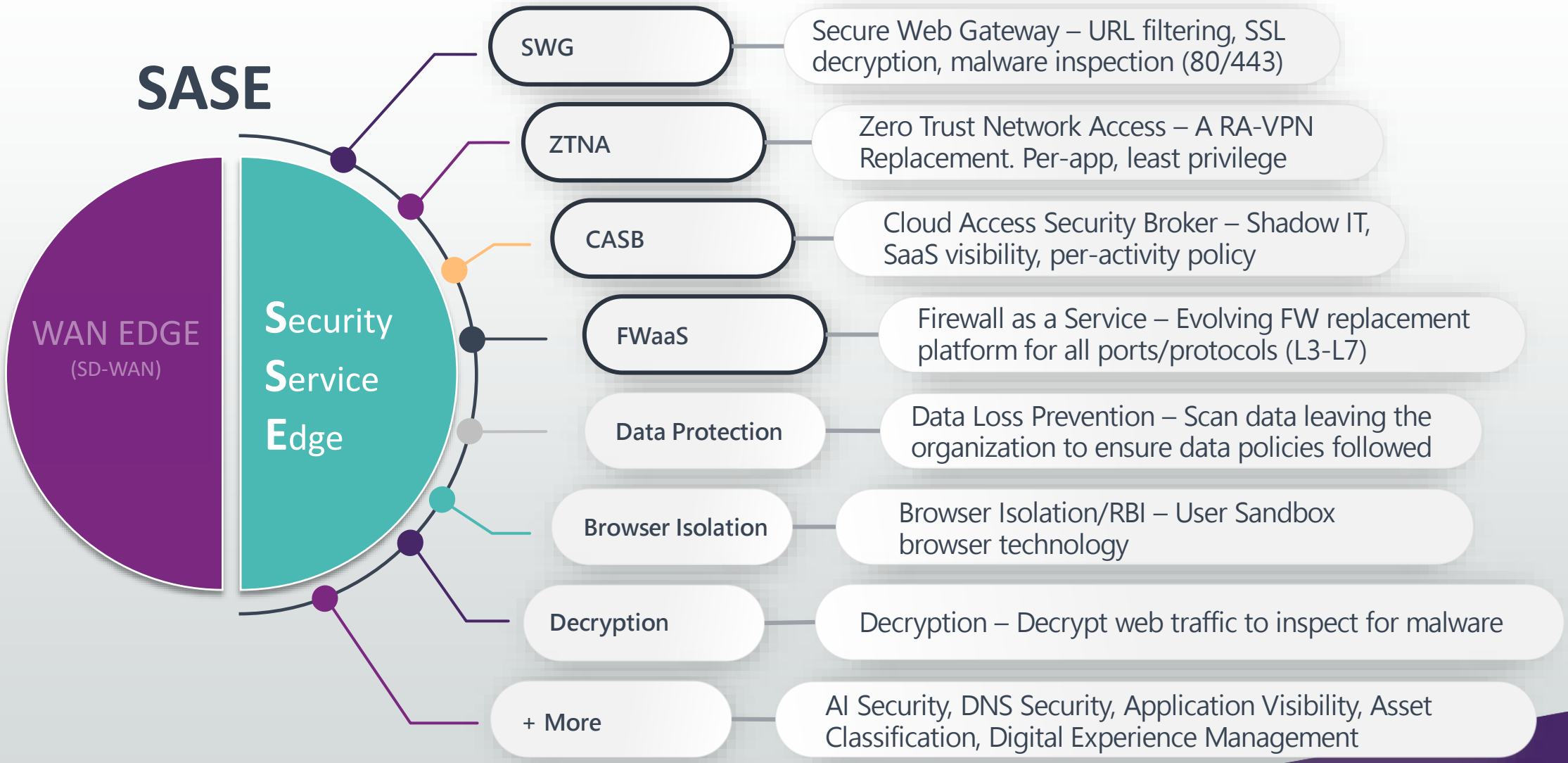
Secure Access Service Edge – WAN Edge

Networking



Secure Access Service Edge – Security Service Edge

Security



Security Service Edge (SSE) Benefits

Scale Up or Down Anytime
Cloud scales automatically, subscription based, no refresh cycles, no EoL equipment.

See Inside Encrypted Traffic
SSL decryption, DLP, Anti-malware, URL filtering for all users regardless of location or device.

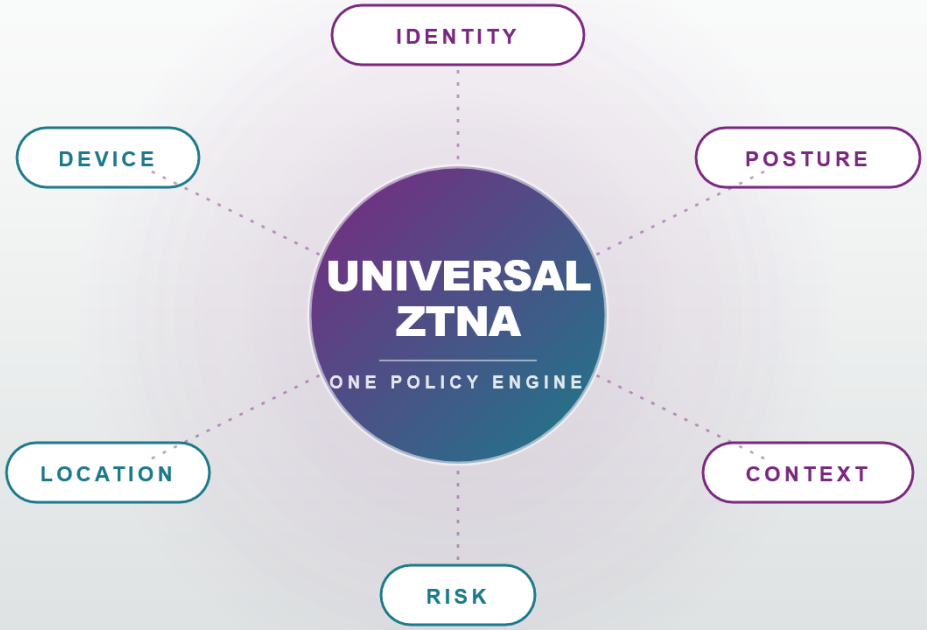
Eliminate VPN Attack Surface
Zero Trust: users connect to apps, not the network — eliminates lateral movement.

CASB / SWG / ZTNA / DLP / FWaaS
Single console, single policy engine, five products replaced with one. Visibility and control over SaaS usage, shadow IT discovery, data exfiltration prevention, cloud app risk scoring, etc.

Operations & Compliance
Third-party / vendor access | Secure AI tool governance | BYOD security | Compliance posture (HIPAA, FedRAMP, CMMC)

What makes it Universal ZTNA?

Identity-driven, continuously-evaluated, applied to every user, device, location, and resource, regardless of where they sit.



THE GARTNER TEST

One client, ZTNA + VPNaaS

A single endpoint agent must broker modern apps via ZTNA *and* tunnel legacy / non-IP apps via VPNaaS — under the same policy engine, with no second client to manage.

One trust verdict

Identity, posture, and risk signals produce **one trust verdict** applied uniformly to SaaS, internet, private DC apps, and on-prem branch/factory apps — not four separate enforcement decisions.

Agent + agentless + on-prem

Multiple enforcement modes — client agent for managed, browser-based for BYOD/3rd-party, on-prem firewall for LAN/branch, app connectors for IoT/OT — all governed by the same policy.

Continuous, adaptive trust

Trust is re-scored every session as posture, location, and behavioral signals change — access is revoked mid-session if risk rises, not granted once and forgotten.

TECH DAY 2026

SSE Vendor Comparison

SSE Competitor Strengths

Vendor-Independent Perspective — Every environment is unique, but some things are true

Founded 2007 / Launched SSE ~2021
Best-of-breed SSE, Enterprise-grade, Gartner Leader. Typically, more expensive to procure and support. Best for large enterprise & VPN replacement at scale. Emerging SASE solution.

Founded 2005 / Launched SSE ~2019
Continuous inline inspection of private app traffic; server-initiated traffic support (outbound); Threat-prevention at scale, App Acceleration. FW & SSE Unified Management via SCM.

Founded 2012 / Launched SSE ~2022
Data protection leader. Best-in-class CASB/DLP depth. Ideal for healthcare, finance, legal — where data exfiltration is the primary risk.

Founded 2003 / Launched SSE ~2021
Quality solution at a cost-effective price. Strong in K-12 — granular URL categories built for education. ZTNA included in base license.

Founded 1984 / Launched SSE 2023
Massive advantage if you have Umbrella, Cisco EA, or existing Cisco Security product investments. Transition to Universal ZTNA dramatically easier.

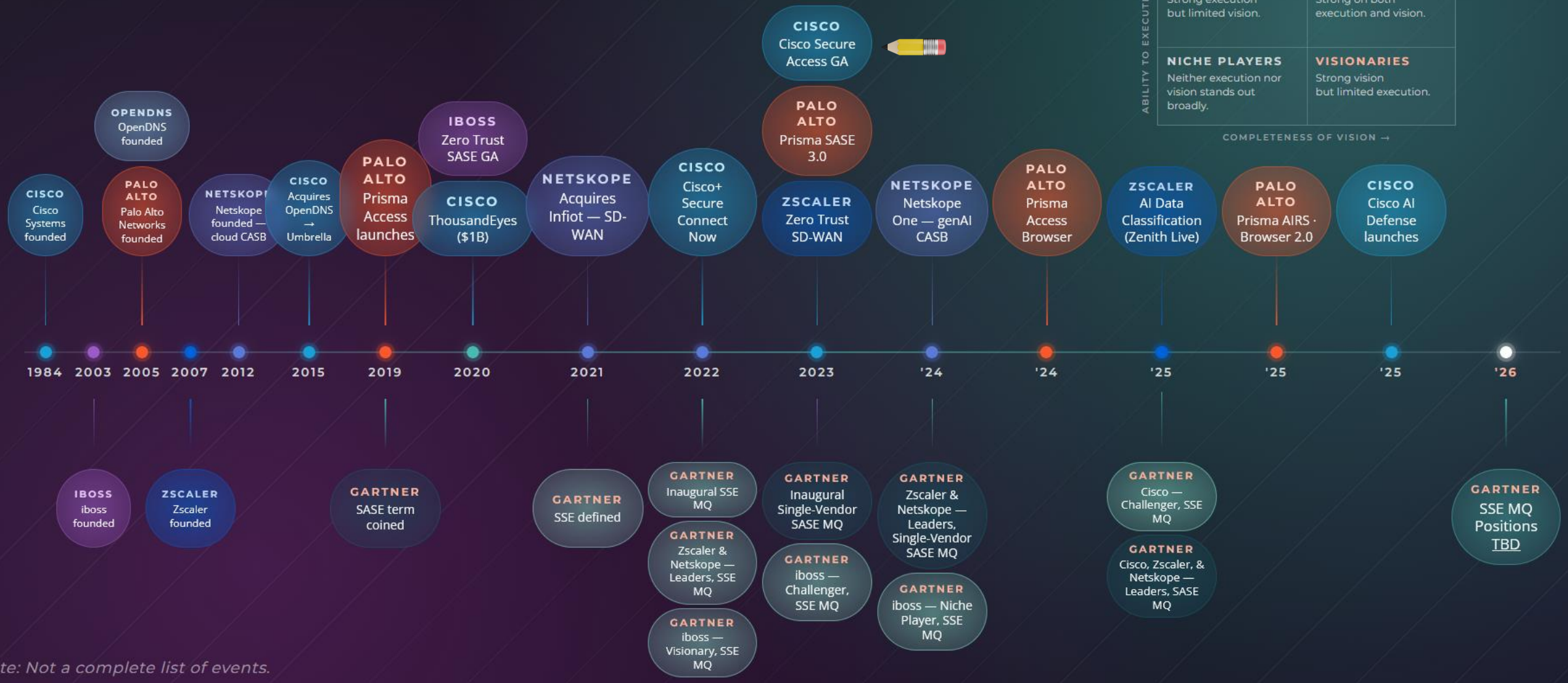
MARKET TIMELINE

SASE / SSE Evolution

From 1984 to today

Founding & SASE/SSE Milestones — Gartner, Cisco, Palo Alto, Zscaler, Netskope, iboss

LEGEND — CISCO · ZSCALER · NETSKOPE · PALO ALTO · IBOSS · GARTNER



Note: Not a complete list of events.

SIDE BY SIDE

ANM Focus SSE Solutions

SOURCES

Vendor data sheets · 2024 / 2025
Cisco · Zscaler · Netskope
Palo Alto Networks · iboss

CISCO

SECURE ACCESS

INTERNET ACCESS
Secure Internet Access

PRIVATE ACCESS
Secure Private Access

ZTNA MODEL
ZTNA 1.0 + hybrid VPNaaS

CLOUD FOOTPRINT
~50+ PoPs (AWS + Equinix + others)

DEM
ThousandEyes

THREAT INTEL
Talos

GOV/LEGAL (NIST SP 800-53)
FedRAMP Moderate

AI SECURITY
AI Defense + AI Access

ZSCALER

ZERO TRUST EXCHANGE

INTERNET ACCESS
Zscaler Internet Access

PRIVATE ACCESS
Zscaler Private Access

ZTNA MODEL
ZTNA 1.0

CLOUD FOOTPRINT
160+ PoPs (AWS + Equinix)

DEM
ZDX

THREAT INTEL
ThreatLabZ

GOV/LEGAL (NIST SP 800-53)
FedRAMP High

AI SECURITY
AI Security Suite · AI Guard

NETSKOPE

NETSKOPE ONE

INTERNET ACCESS
NG-SWG

PRIVATE ACCESS
Netskope Private Access

ZTNA MODEL
ZTNA 1.0 + Universal ZTNA

CLOUD FOOTPRINT
120+ DCs (NewEdge Private Cloud)

DEM
Netskope DEM

THREAT INTEL
Threat Labs

GOV/LEGAL (NIST SP 800-53)
FedRAMP High · IRAP

AI SECURITY
SkopeAI

PALO ALTO

PRISMA ACCESS

INTERNET ACCESS
Prisma Access

PRIVATE ACCESS
ZTNA Connector

ZTNA MODEL
ZTNA 2.0

CLOUD FOOTPRINT
100+ PoPs (AWS + GCP)

DEM
Autonomous DEM

THREAT INTEL
Unit 42

GOV/LEGAL (NIST SP 800-53)
FedRAMP High · IL5

AI SECURITY
Prisma AIRS

IBOSS

ZERO TRUST SASE

INTERNET ACCESS
Full stack

PRIVATE ACCESS
iboss ZTNA

ZTNA MODEL
ZTNA 1.0

CLOUD FOOTPRINT
100+ PoPs (AWS + Azure)

DEM
Native telemetry

THREAT INTEL
iboss Threat Research

GOV/LEGAL (NIST SP 800-53)
FedRAMP Moderate

AI SECURITY
AI CASB + AI SSPM

TECH DAY 2026

Cisco Secure Access

CISCO SSE PORTFOLIO

Cisco Umbrella & Secure Access

SOURCE

Cisco SSE Packages Comparison Guide · *Mar 2026*

Cisco Umbrella

FOUNDATIONAL

DNS-FIRST CLOUD SECURITY

Block malicious domains, phishing, and DNS exfiltration before traffic ever reaches your network.

PACKAGES

DNS Essentials

DNS-layer block, app discovery, category filtering.

DNS Advantage

+ Investigate (deep IP/ASN intel), partial URL/SWG.

SIG Essentials

+ Full SWG proxy, FWaaS L3/4, CASB, SD-WAN tunnels.

SIG Advantage

+ DLP (real-time/API), L7 firewall, SaaS malware scan.

BEST FIT

Orgs needing rapid DNS-layer protection, roaming user coverage.

Cisco Secure Access

CONVERGED

CLOUD-DELIVERED SSE · ZERO TRUST

ZTNA + SWG + CASB + FWaaS — plus VPNaaS, DLP, RBI, AI guardrails, DEM (ThousandEyes), Duo identity, and reserved IPs.

PACKAGES

DNS Defense

DNS-layer parity with Umbrella DNS.

SIA Essentials

Secure Internet Access — SWG, CASB, FWaaS L3/4.

SPA Essentials

Secure Private Access — ZTNA + VPNaaS, hybrid policy.

SIA Advantage

+ DLP, RBI, L7 FW, UEBA, ThousandEyes DEM, AI guardrails.

SPA Advantage

+ Clientless ZTNA, trust-level policy, Enterprise Browser, posture, full DEM.

BEST FIT

Orgs retiring VPN or standardizing on a unified zero-trust SSE fabric.

Architecture Overview

Any Endpoint, Any Destination, Policy Enforced in the Cloud

Endpoints/Destinations
- Managed, Unmanaged/BYOD, Mobile, Branch/SD-WAN
- Internet/SaaS, Private Apps, GenAI Apps, Partner APIs

Traffic Flow
- User/Device → Nearest Secure Access PoP → Destination
- Single-pass inspection for all services — all in one cloud gateway

Cloud Infrastructure
- 50+ global PoPs – AWS, Equinix, and others — US-based and international coverage

Security Cloud Control Plane
- Unified Management Console — single policy engine across all SSE functions
- Moving toward a "single-pane of glass"

How to Get Traffic to Secure Access

Cisco Secure Client Agent

Installs on endpoint, routes all traffic to nearest PoP automatically. Full SSL inspection, DLP, posture checks, ZTNA (preferred method)

IPsec/GRE Tunnel (On-Prem Devices / Branches)

Routers/firewalls tunnel all traffic to Secure Access PoP. Covers branches, IoT, and devices that can't run an agent.

Cisco/Meraki SD-WAN Integration

Native integration via API — No IPsec configuration. Seamless connectivity while other traffic goes direct

CASB API Integrations

Connects directly to Microsoft 365, Google Workspace, and other to scan data at rest. No traffic steering needed

PAC File / Explicit Proxy

Lightweight redirect, no full agent required. HTTP/HTTPS only. Unmanaged or partial rollouts.

TECH DAY 2026

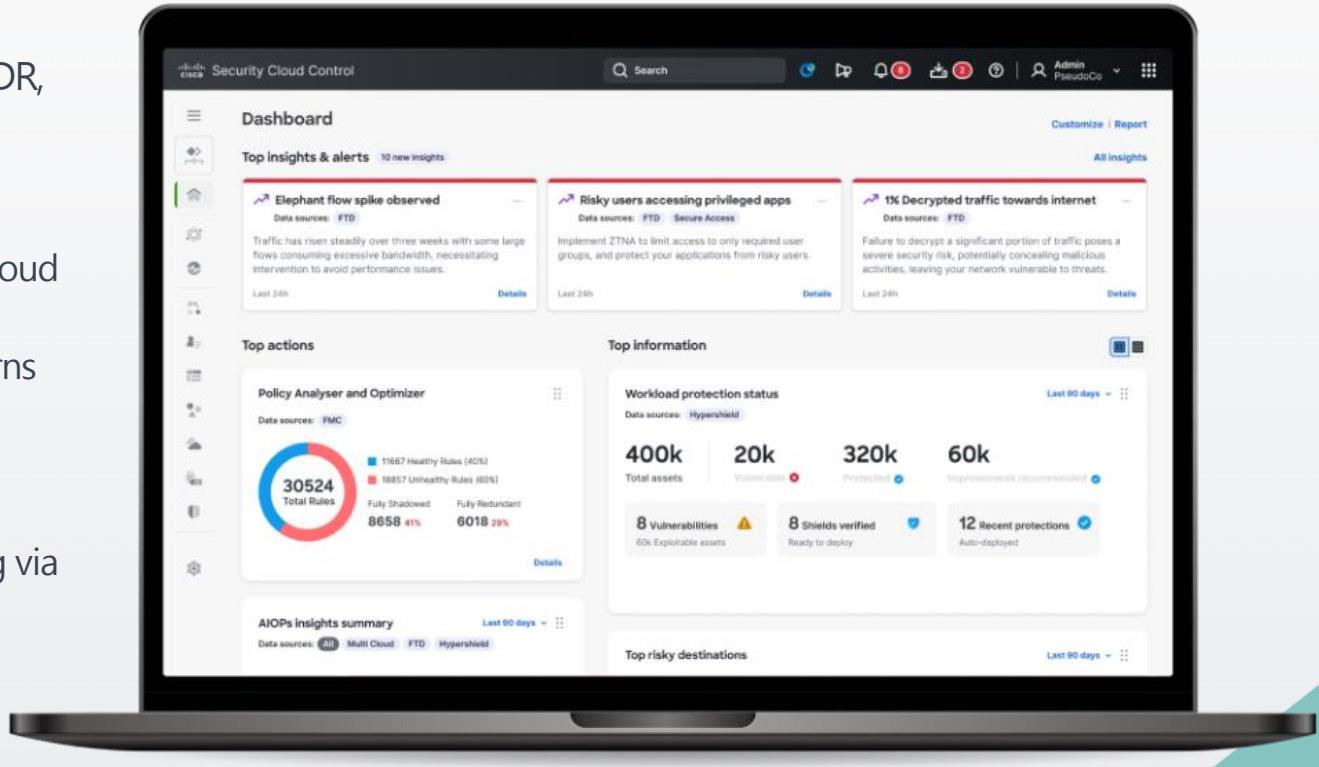
Cisco Secure Access Features

Cisco Security Cloud Control (SCC)

One AI-native console for Secure Access, Secure Firewall, Multicloud Defense, Hypershield, Catalyst SD-WAN, Secure Workload, and AI Defense — the successor to Cisco Defense Orchestrator.

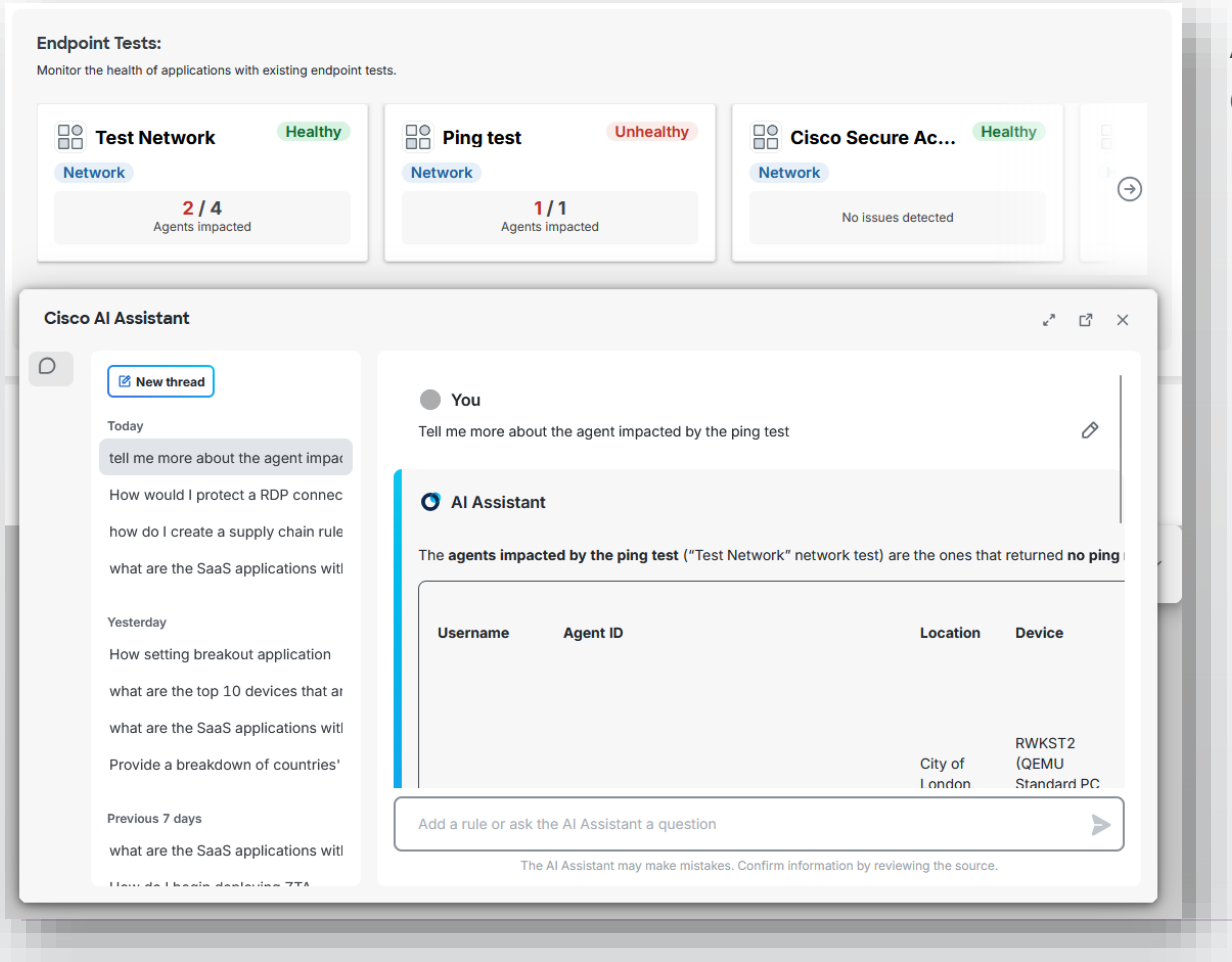
Cisco's unified management console for the Security Cloud. One interface for Secure Access, Secure Firewall, Multicloud Defense, XDR, and Duo, with a shared identity, SSO, and policy object model.

- **Products managed:** Secure Access, Secure Firewall (FTD/ASA), Multicloud Defense, XDR, Duo, Hypershield, Multifactor.
- **Identity:** Single SSO and unified roles — your IdP (SAML/OIDC) governs every Cisco Security product.
- **Policy:** Shared network, host, group, and user objects between Secure Access and Firewall policy.
- **AI Assistant:** Policy authoring, rule explain, event triage, and reporting via natural language.
- **APIs:** Open by default — REST + OpenAPI 3.0 for policy, tenants, and events; one SDK, every product.



Cisco AI Assistant for Secure Access

Natural-language copilot embedded in the Secure Access console — turns hours of policy work, troubleshooting, and reporting into a conversation.



AI Assistant for Security, embedded in the Secure Access console. Uses Cisco's security-trained LLMs grounded in tenant data to reason over policy, events, and configuration.

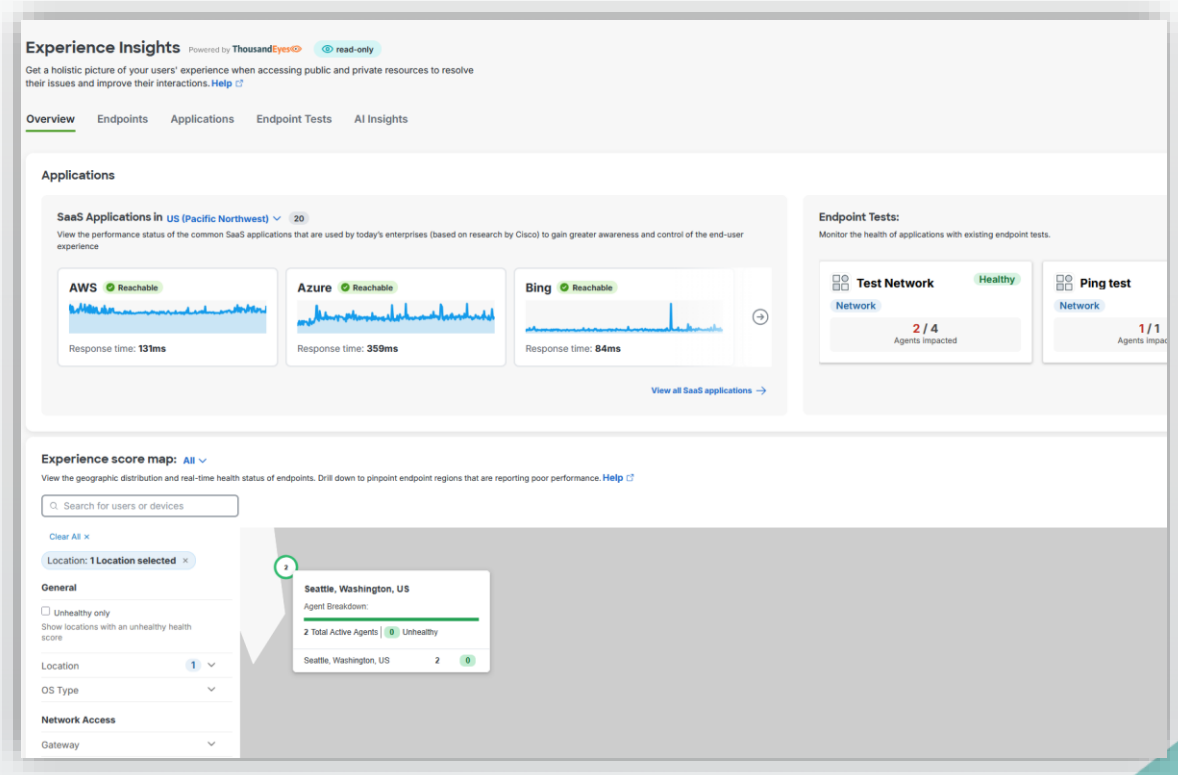
- **Policy authoring:** Generates draft access rules from natural-language intent.
- **Policy explanation:** Summarizes existing rules; flags shadowed, unused, or overlapping rules.
- **Event triage:** Explains block/allow decisions in plain language with the matched rule and signals.
- **Reporting:** Natural-language queries against Secure Access activity logs.
- **Privacy:** Tenant-scoped; customer data is not used to train foundation models.

Cisco Secure Access Experience Insights

ThousandEyes-powered DEM embedded directly in the Secure Access dashboard — device, network, and SaaS visibility for ITOps without leaving the SSE console.

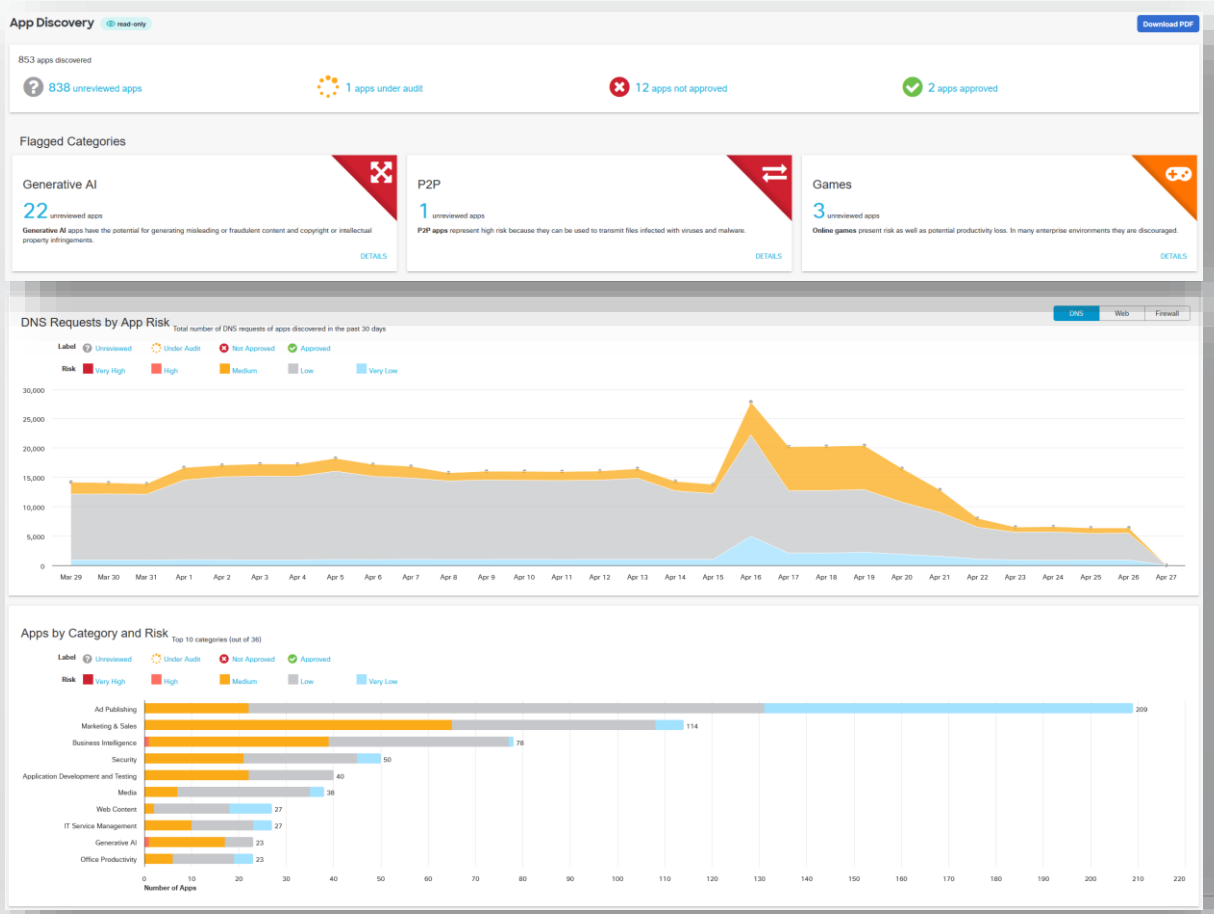
Digital-Experience Monitoring inside Secure Access. ThousandEyes endpoint agents on Cisco Secure Client measure the path from endpoint to SSE PoP to SaaS, surfacing where latency or loss is occurring.

- **Telemetry source:** ThousandEyes endpoint agents bundled with Cisco Secure Client.
- **Visibility:** Endpoint health, local Wi-Fi/LAN quality, hop-by-hop path to SSE PoP and to the application.
- **Apps monitored:** Microsoft 365, Google Workspace, Salesforce, Webex, and customer-defined SaaS targets.
- **Console:** Integrated in the Secure Access dashboard — shared with policy, users, and events.
- **Licensing:** Included with Secure Access — no separate ThousandEyes SKU required for the bundled agents.
- **Data retention:** 30 days of session and path metrics for trend analysis and root-cause review.



Cisco Secure Access App Discovery

See every SaaS and GenAI app your users touch — ranked by risk, mapped to users, and one click away from a policy decision.



Continuous SaaS and GenAI app inventory derived from Secure Access traffic. Identifies, scores, and attributes cloud apps to the users and groups consuming them.

- **Catalog:** 70,000+ cloud apps with risk scores and category metadata.
- **Attribution:** Apps mapped to users, groups, and source networks from Secure Access logs.
- **Risk scoring:** Vendor reputation, data-handling, compliance certifications, hosting region.
- **Tagging:** Sanctioned, tolerated, or unsanctioned tags drive policy decisions.
- **Action:** One-click policy creation to allow, block, or warn from the discovery view.

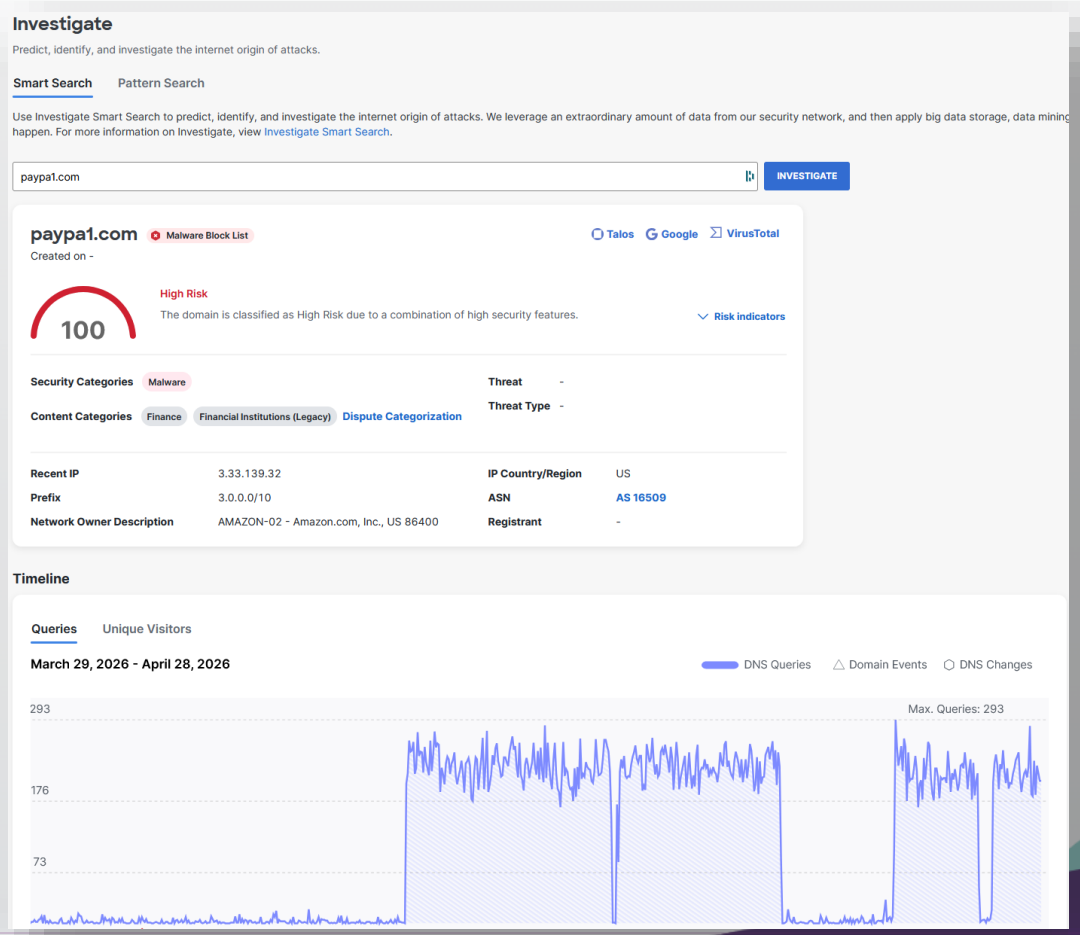
CISCO · THREAT INTELLIGENCE

Cisco Secure Access Investigate

A live map of the internet built from Cisco's global DNS — pivot any domain, IP, or hash into context, attribution, and connected infrastructure.

Investigation console for Secure Access, drawing on Umbrella's global recursive DNS data and Cisco Talos threat intelligence. Supports indicator pivoting and historical lookup for domains, IPs, URLs, ASNs, and file hashes.

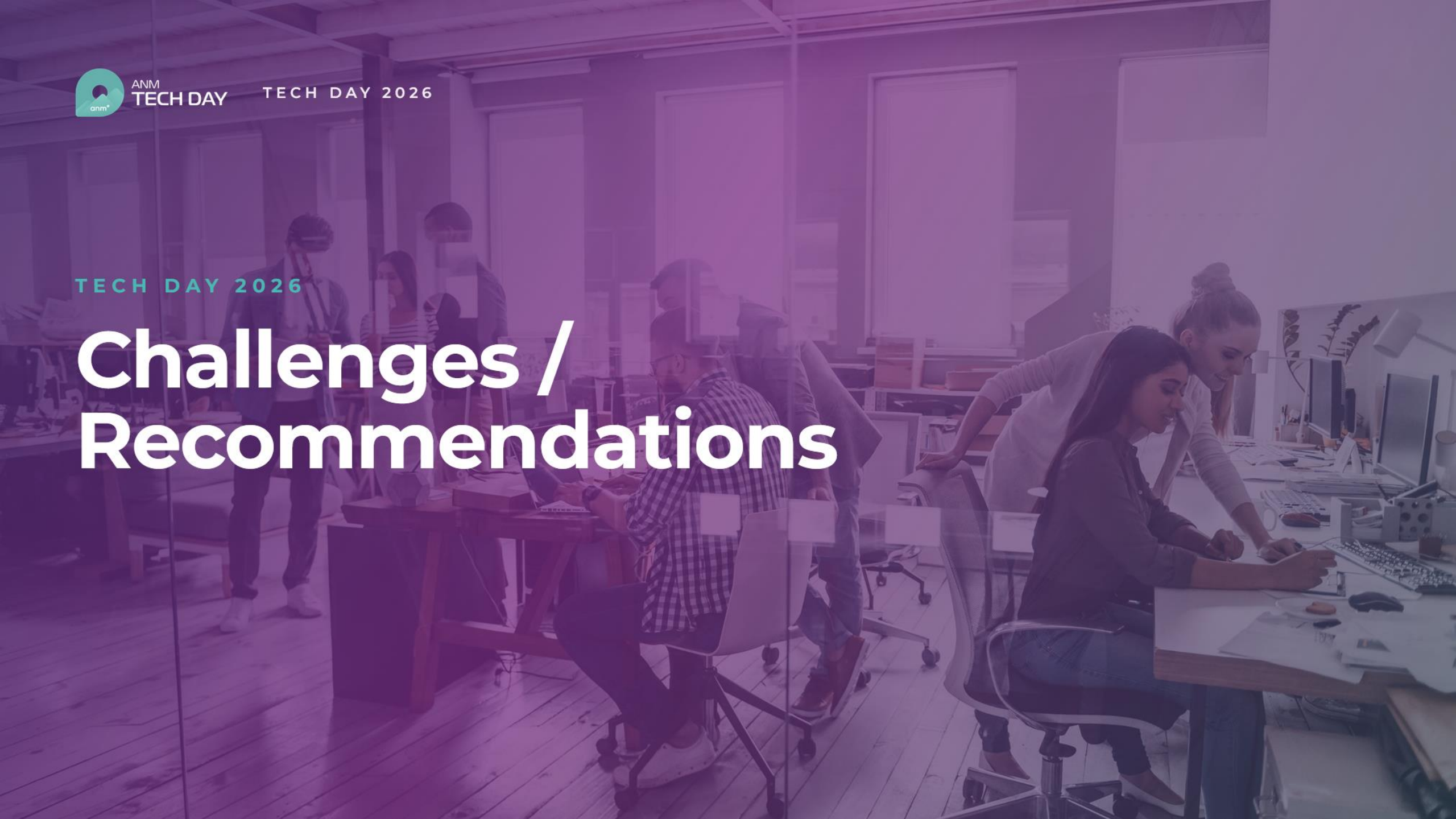
- **Data sources:** Umbrella DNS resolvers (600B+ daily requests), Talos threat feeds, BGP routing data.
- **Pivots:** Domain ↔ IP ↔ ASN ↔ WHOIS ↔ file hash ↔ co-occurrence ↔ passive DNS history.
- **Predictive intelligence:** Statistical and ML models score domains and IPs before they're weaponized.
- **API:** Investigate API for SOAR, XDR, and custom enrichment workflows.
- **Integration:** Results link directly to Secure Access policy actions and event records.



ANM TECH DAY

TECH DAY 2026

Challenges / Recommendations



Challenges

Real-world friction points worth knowing before you start

- Cisco Secure Access is an evolving platform — new features are added incrementally; speed of rollout = temporary gaps in control
- SSL decryption is a must to get real value — selective decryption available but some traffic cannot be decrypted (pinned certs, certain finance/medical apps)
- Public IP provisioning — Included with SIA Advantage & SPA Advantage; requires manual request through Cisco (historically long wait times)
- Network infrastructure overhead — IPsec tunnels from on-prem (maintenance windows).

Best Practice Recommendations

- The Firewall is not dead — Evaluate security strategy, refresh and resize.
- Lead with identity — Clean the IDP, kill stale groups; implement MFA
- Document App Requirements — critical step often skipped
- Don’ t just lift and shift, rethink policy and focus on business use cases
- Implement DEM Day One — Visibility is key to end user experience
- Crawl, Walk, Run – Start with DNS, Internet security → SSL/CASB/DLP → VPN Replacement/private apps.
- Take advantage of Security EAs — especially customers on multi-year agreements; price fluctuations are real!
- Lab it up first & Try Before You Buy — Cisco dCloud & POV

How Can ANM Help?

Vendor-independent guidance — we evaluate what's right for your environment, not just what's easiest to sell

Solution Deep Dive

Personalized review of features, licensing, and EA options with your ANM Solutions Architect. Build Roadmap & ZTA Workshops.

SSE Solution Evaluation

Vendor-independent assessment of which SSE solution fits your environment, budget, and use cases — Cisco Secure Access, Palo Alto, Zscaler, Netskope, iboss

POV Engagement Support

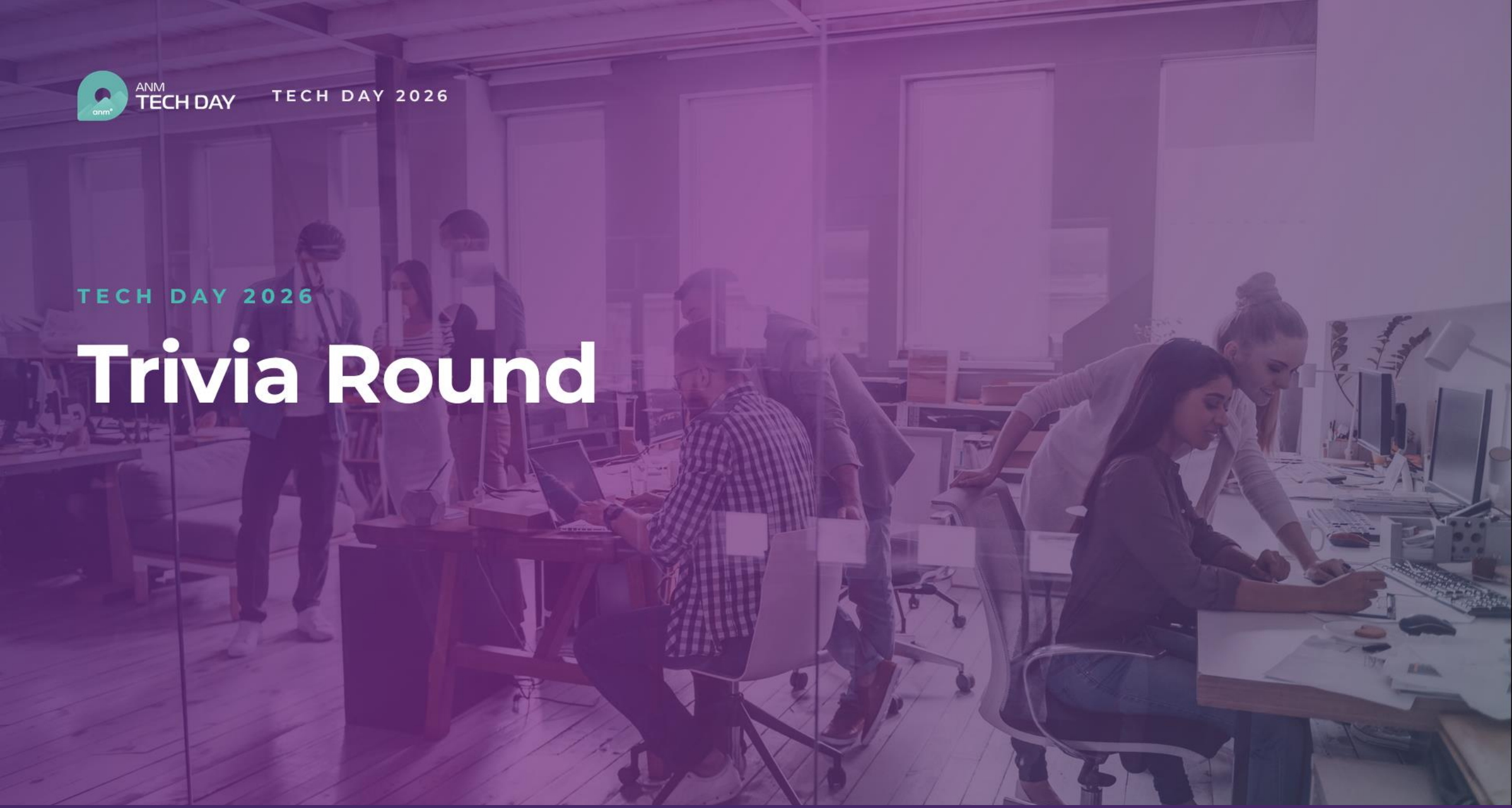
Bring ANM in during your POV to ensure pilot runs successfully.

Professional Services

End-to-end planning, design, testing, implementation, validation, documentation, knowledge transfer, project management

Key Takeaways

- SSE is not optional anymore. The question has become which vendor, when, and how?
- The end goal is Universal ZTNA. This requires a multi-layered approach (on-prem & cloud).
- Cisco newest to SSE the market, but the Cisco ecosystem provides native integrations that no other competitor can.
- Secure Access is a compelling and clear path forward for existing Umbrella Customer. Cisco focused environments should utilize EAs and Cisco Promotions to adopt SSE.



TECH DAY 2026

Trivia Round

Question 1

What does the acronym SSE stand for?

Question 1

What does the acronym SSE stand for?

Security Service Edge

Question 2

What year was Cisco Secure Access released?

Question 2

What year was Cisco Secure Access released?

2023

Question 3

Who was the primary author for both Gartner foundational papers on SASE and SSE?

Question 3

Who was the primary author for both Gartner foundational papers on SASE and SSE?

Neil MacDonald

Question 4

Which organization is the primary provider of threat intelligence for Secure Access?

Question 4

Which organization is the primary provider of threat intelligence for Secure Access?

Talos

Question 5

How many PoPs does Cisco Secure Access have?

Question 5

How many PoPs does Cisco Secure Access have?

50+

Question 6

What was the mean time to data exfiltration after initial access according to Cisco Talos?

Question 6

What was the mean time to data exfiltration after initial access according to Cisco Talos?

24 Hours

Question 7

According to Cisco Talos, what was the percentage of cyber-attacks attributed to VPN vulnerabilities?

Question 7

According to Cisco Talos, what was the percentage of cyber-attacks attributed to VPN vulnerabilities?

56%

Question 8

How many applications can Cisco Secure Access App Discovery feature catalog?

Question 8

How many applications can Cisco Secure Access App Discovery feature catalog?

70,000+

Question 9

What is the Digital-Experience Monitoring (DEM) solution inside of Cisco Secure Access?

Question 9

What is the Digital-Experience Monitoring (DEM) solution inside of Cisco Secure Access?

ThousandEyes

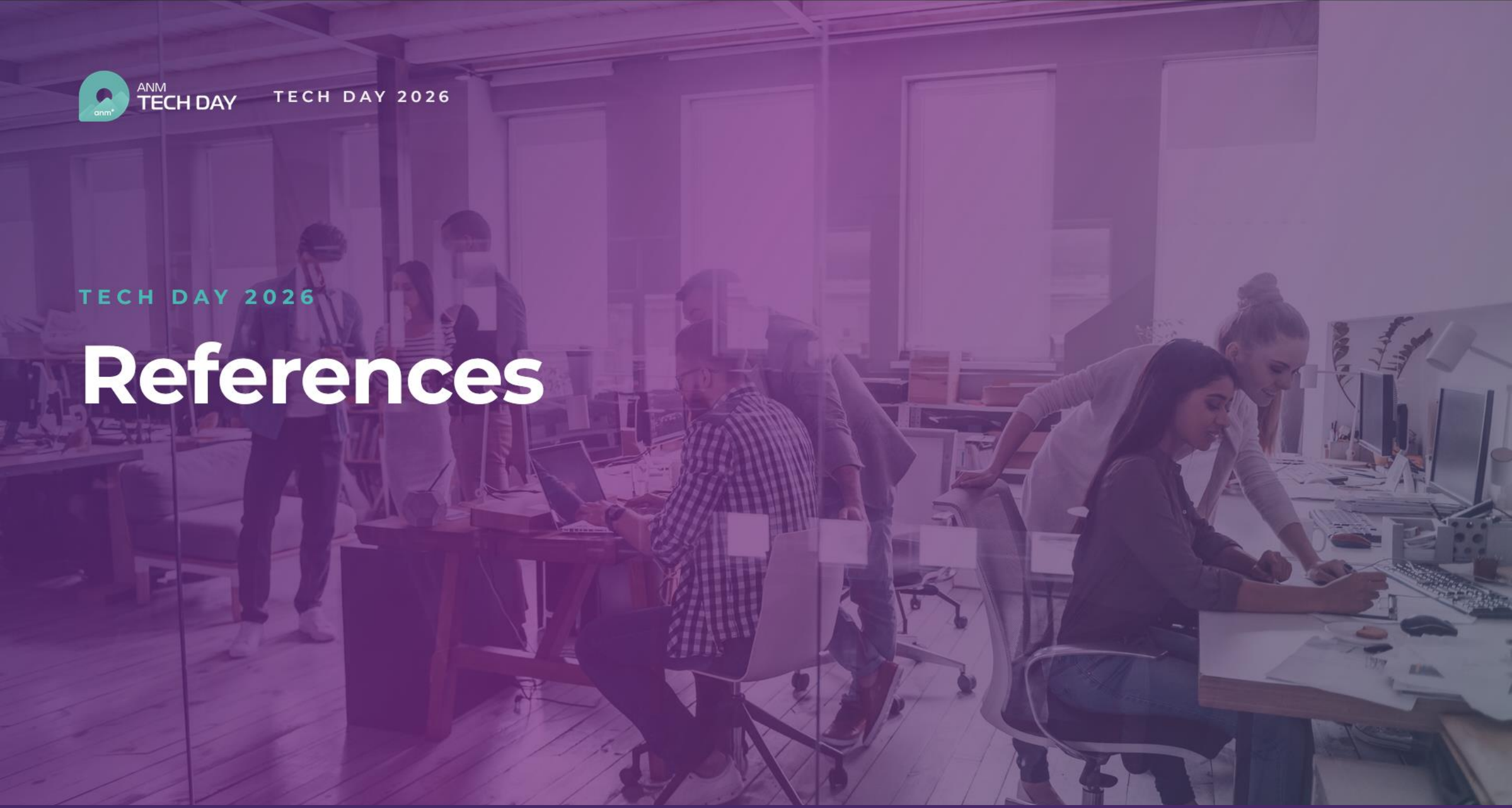
Question 10

What is the AI-native cloud console that manages Cisco Secure Access?

Question 10

What is the AI-native cloud console that manages Cisco Secure Access?

Security Cloud Control



TECH DAY 2026

References

References

Cited sources, analyst research, and vendor product pages

GARTNER — ANALYST RESEARCH

- The Future of Network Security Is in the Cloud (SASE, 2019)
- 2021 Strategic Roadmap for SASE Convergence (SSE, 2021)
- Magic Quadrant for Security Service Edge (2025)
- Magic Quadrant for SASE Platforms (2025)
- Gartner Peer Insights — SSE Market Reviews
- Peer Insights — Cisco Secure Access Reviews

CISCO — SECURE ACCESS PLATFORM & TALOS RESEARCH

- Cisco Secure Access — Product Page
- Cisco Secure Access Data Sheet
- Secure Access At-a-Glance
- Secure Access Ordering Guide
- Cisco Secure Access Offer Description
- Cisco Secure Access Help
- Configuration Examples & TechNotes
- Secure Access Regions & Export Compliance
- Products Supported by Security Cloud Control
- Security Cloud Control At-a-Glance
- Security Cloud Control Data Sheet
- Cisco AI Assistant for Security
- Cisco Talos — 2024 Year in Review

COMPETITIVE VENDORS — PRODUCT PAGES

Zscaler — Zero Trust Exchange & ThreatLabz

- Zero Trust Exchange Platform
- Zscaler in the Gartner SSE Magic Quadrant
- ThreatLabz — VPN Risk Report 2024 / 2025

Palo Alto Networks — Prisma Access

- Prisma Access Product Page
- Prisma Access Datasheet

Netskope — Netskope One SSE & Threat Labs

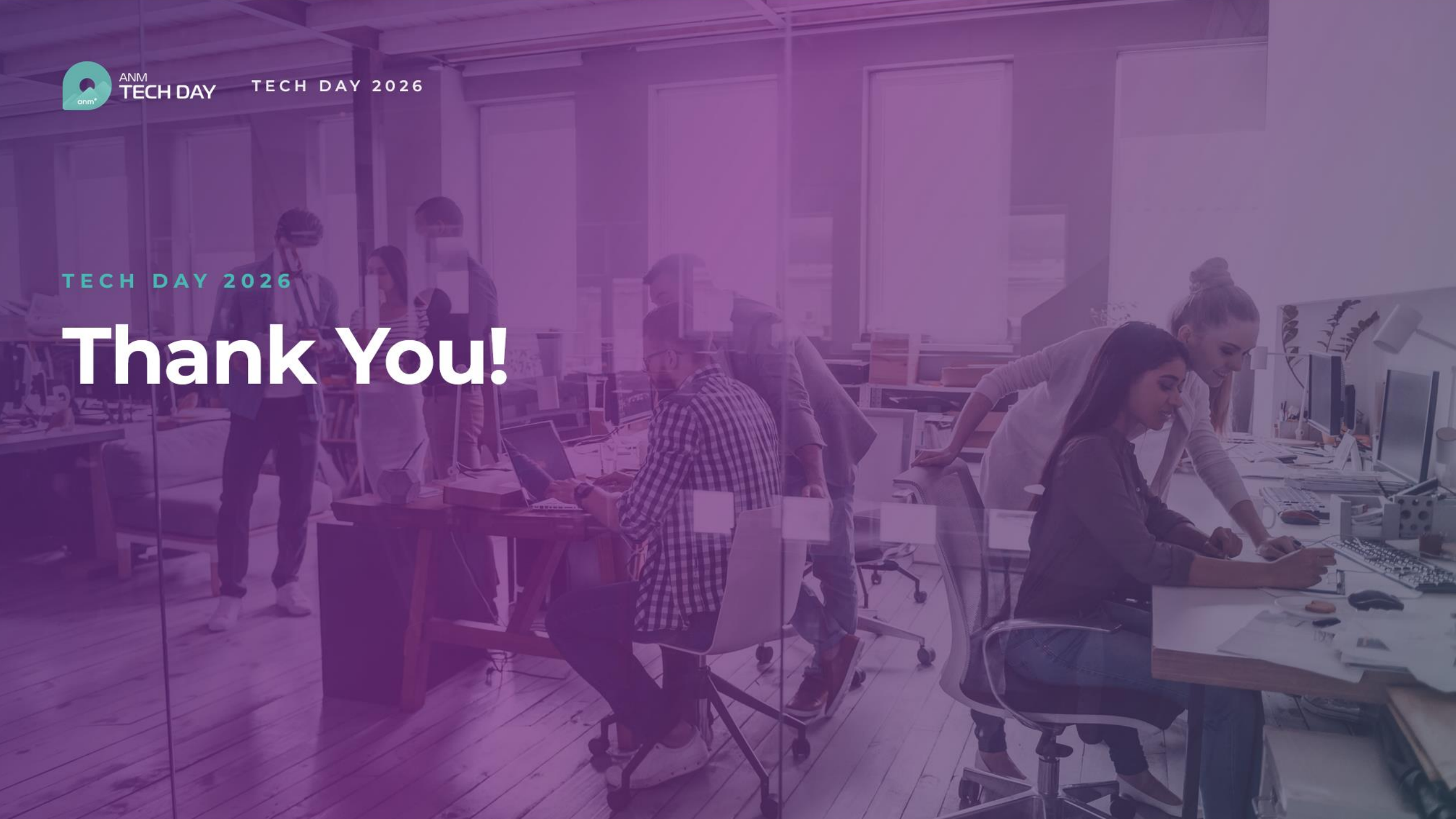
- Netskope One Security Service Edge
- Netskope in the Gartner SSE Magic Quadrant
- Netskope Threat Labs — Cloud & Threat Report

iboss — Zero Trust SASE / SSE

- iboss Zero Trust SASE Platform
- iboss Zero Trust Overview

Additional Research

- Stanford / Tessian — Psychology of Human Error



TECH DAY 2026

Thank You!