The Anatomy of SASE

Build for Speed, Security and Success!

Ernest Pronk – SDWAN/SASE Lead

October 2022

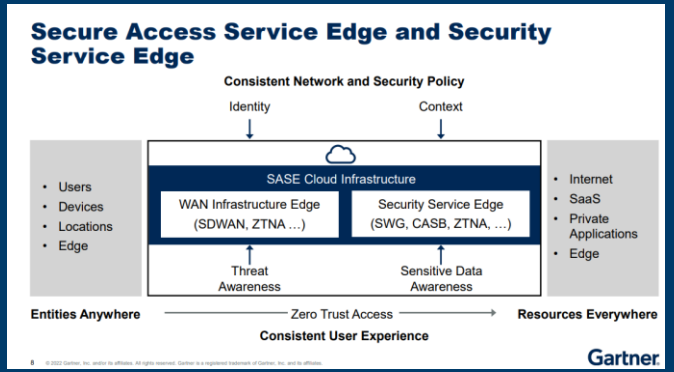
Where is SASE coming from?
A long-term industry strategy

Need: Reduce complexity and improve performance from everywhere
Result: Convergence of connectivity, security, and identity

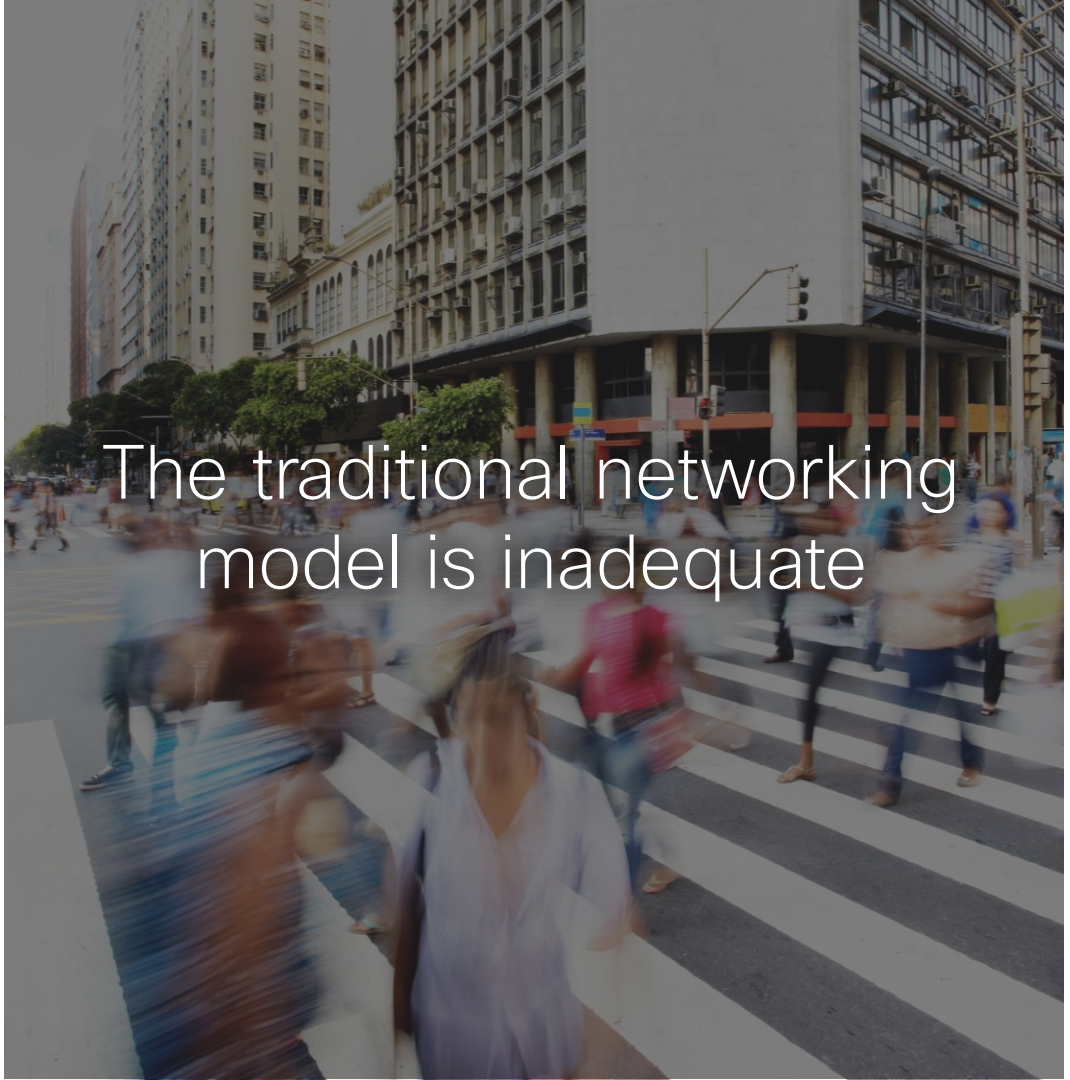
There are many names for this multi-function approach…

Gartner	Secure Access Service Edge (SASE) Secure Internet Gateway (SIG)
FORRESTER®	Zero Trust Edge
ESG Enterprise Strategy Group	Elastic Cloud Gateway

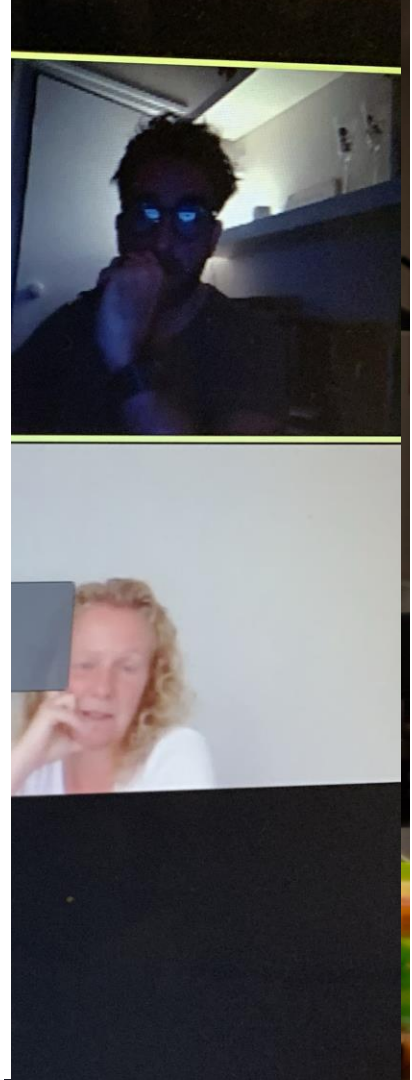
…but full agreement on the move to cloud-native aggregation



Gartner 2019
SASE Hype Cycle for Enterprise Networking, Andrew Lerner, 2019



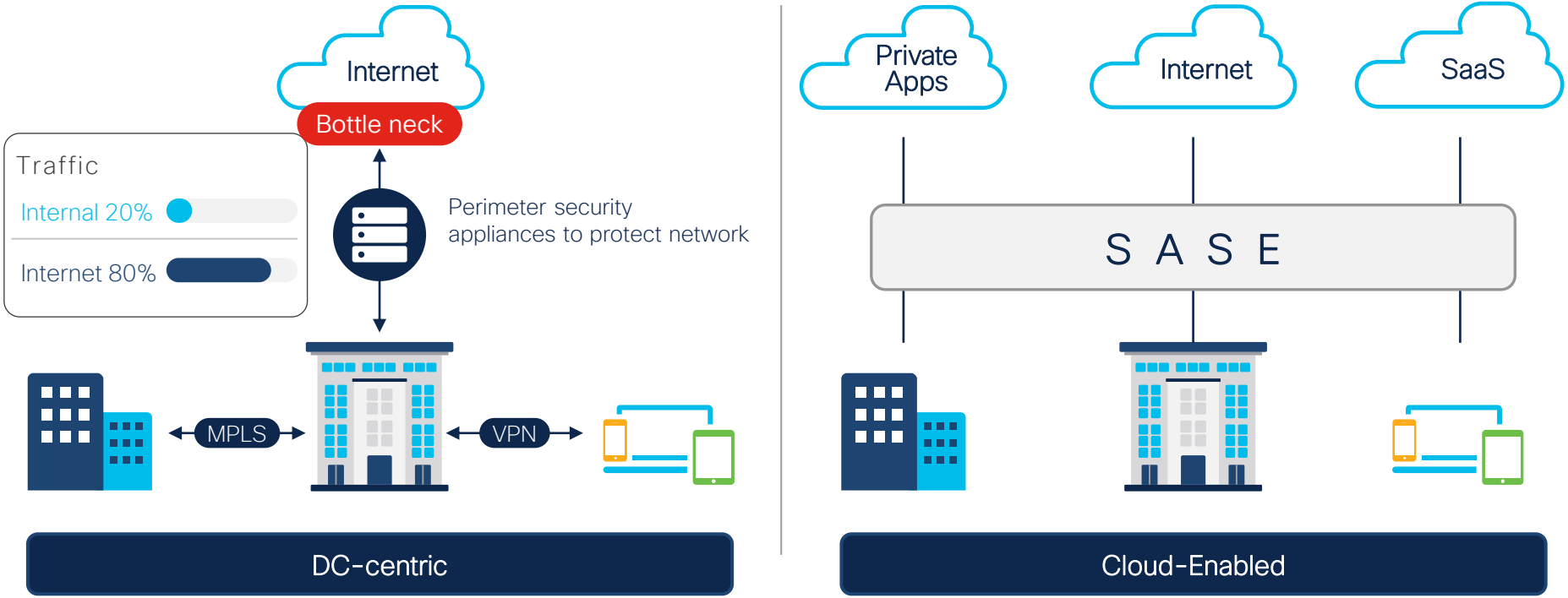
The traditional networking model is inadequate




HITACHI
Inspire the Next

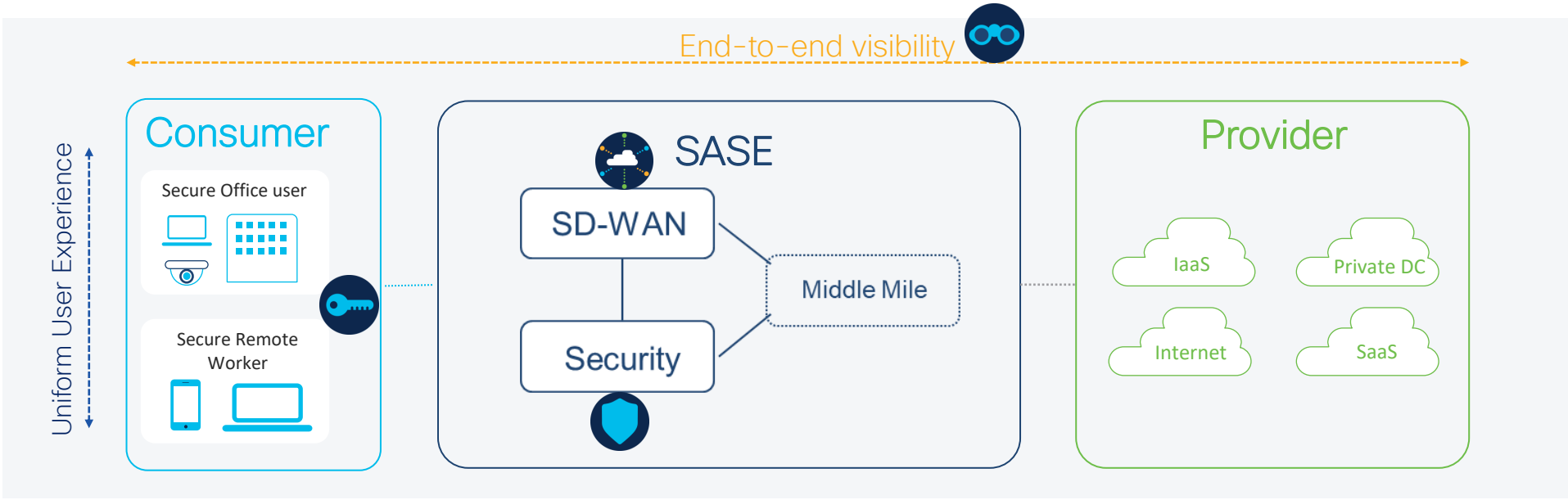
Network transformation

Transition from a DC-centric topology to one that's cloud ready



The Anatomy
Cisco SASE Architecture

Cisco SASE Architecture



Reduce cost

Improve OpEx with circuit consolidation and consolidation of UI touchpoints

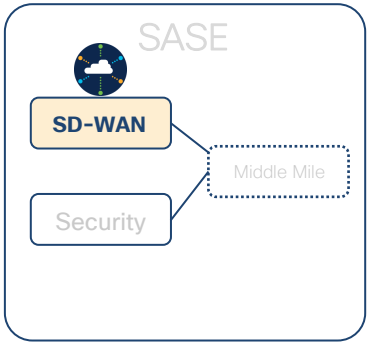
Improve user experience

Bring services closer to user and leverage middle-mile partnerships + password-less authentication to optimize connections

Minimize risk

Decryption & inspection addressing data loss, leveraging a true zero-trust approach across the IT perimeter

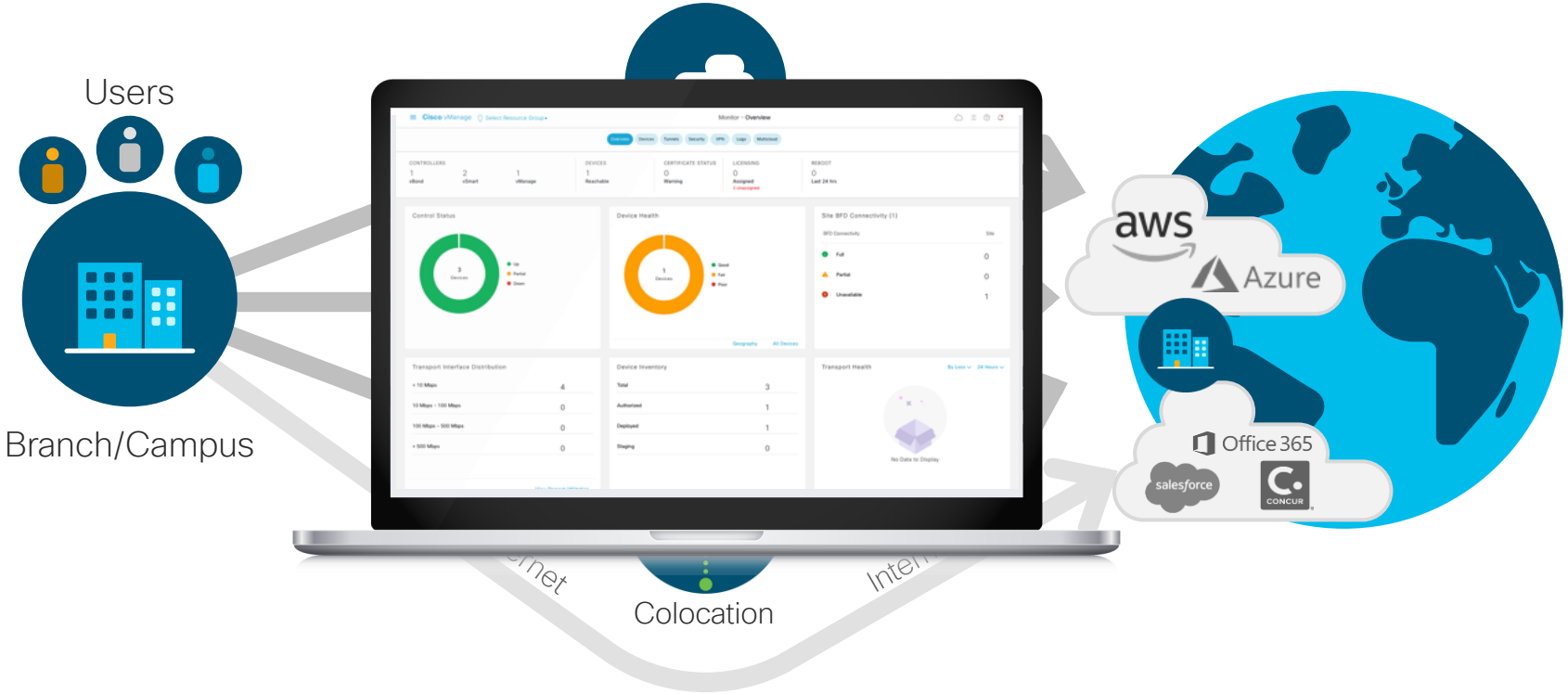
SASE building block #1



SD-WAN

Automation and Cloud-Based orchestration	Software Defined Cloud Internet and Multicloud access	Middle mile optimization	Integrated security and macro/micro segmentation	Dynamic performance routing	Analytics, SaaS Telemetry, Smart thresholds
✓	✓	✓	✓	✓	✓
Zero touch onboarding and provisioning	Single pane of glass cloud networking orchestration	Flexible and programmable cloud interconnect options	Integrated security and network policy controls	Predictable app performance and user experience	Proactive network assurance and network operations

SD-WAN Technics



Best Path Selection, Greater visibility and Manageability

Multicloud access – Software Defined Cloud Interconnect

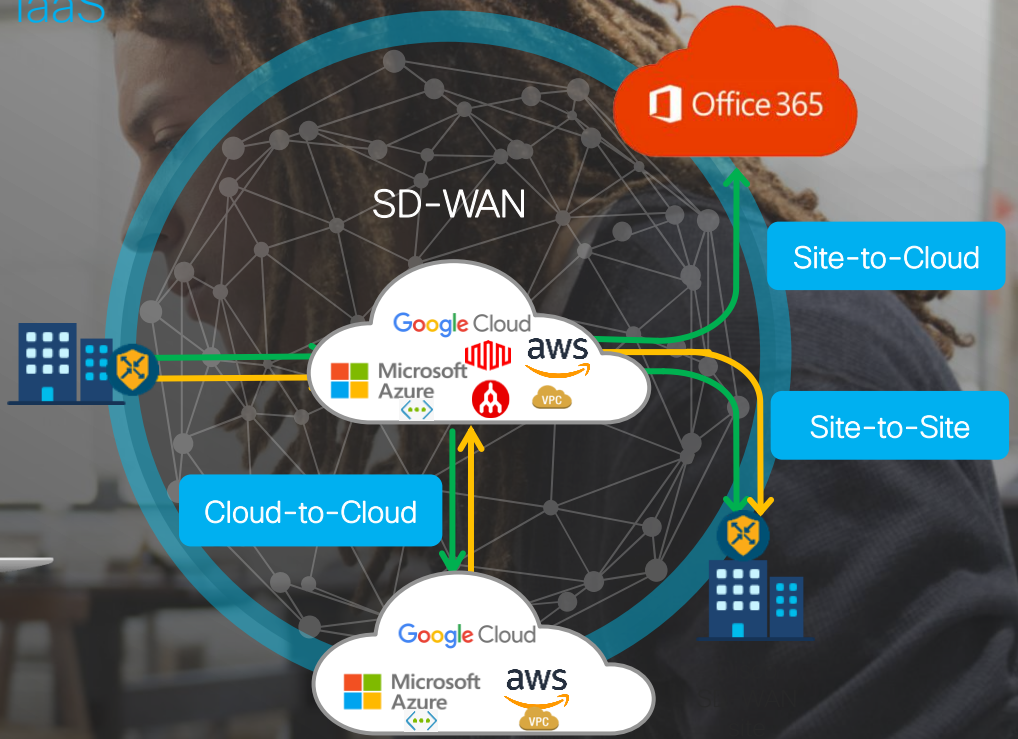
Extending SD-WAN Fabric to IaaS

On-demand connectivity
Reduce time from months to minutes for multicloud connectivity. PAYG model

Highly available backbone
Worldwide connections: 20+ countries, 5 continents, 100's of data centers, up to 99.999% availability

Single management
Automate the connections through vManage

Latency optimized
Remove congestion risk by sending packets through a private backbone



Multicloud for Microsoft 365

Dynamic URL/IP Categorization

- Distinct URLs for different Applications.
- URLs can be mapped to different traffic precedence and Service-Area.
- Microsoft 365 traffic divided into 3 categories based on sensitivity.
- Optimize, Allow and Default.

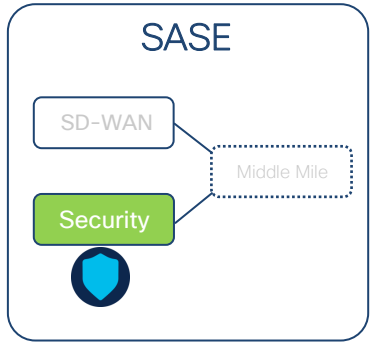
Microsoft Informed Routing

- End-to-end telemetry using Application Infused Path Feedback (AIPF) for Exchange Service Area.
- Import and Export telemetry from/to Microsoft for best path selection.

Microsoft Informed Routing for Teams and SharePoint

- End-to-end telemetry using Application Infused Path Feedback (AIPF) for Teams and SharePoint Service Areas.
- Import and Export telemetry from/to Microsoft for best path selection.

SASE building block #2



SSE (Cloud delivered security)

DNS-layer security	Cloud-delivered firewall	Secure web gateway	Cloud App & Data Security (CASB & DLP)	Remote Access	Interactive threat intel	SecureX Platform
✓	✓	✓	✓	✓	✓	✓
Stop threats before traffic reaches the network	L7 security across all sites to stop non-web-based threats	Full URL visibility/control to enforce policy block advance threats	Discover, report and control cloud application use	Cloud-delivered Secure Remote Access	Real-time threat context expediting incident investigation and response	Visibility across the entire security stack, with automated actions

Often used, not often monitored

90%

Of malware use
DNS in attacks

68%

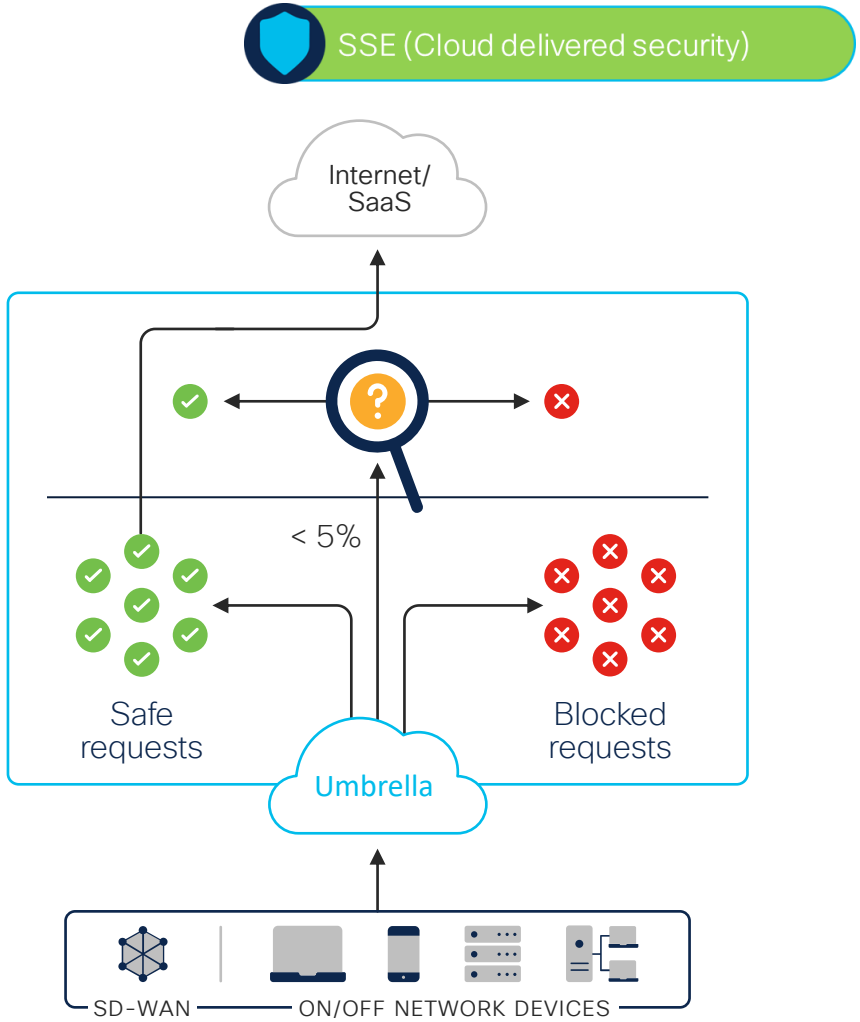
Of organizations
don't monitor their DNS

Source: Cisco Security Research Report

DNS-layer security

First line of defense

- Deploy enterprise wide in minutes
- Block domains associated with malware, phishing, command and control callbacks anywhere
- Stop threats at the earliest point and contain malware if already inside
- Accelerate threat response with an integrated security platform
- Amazing user experience – faster internet access; only proxy risky domains

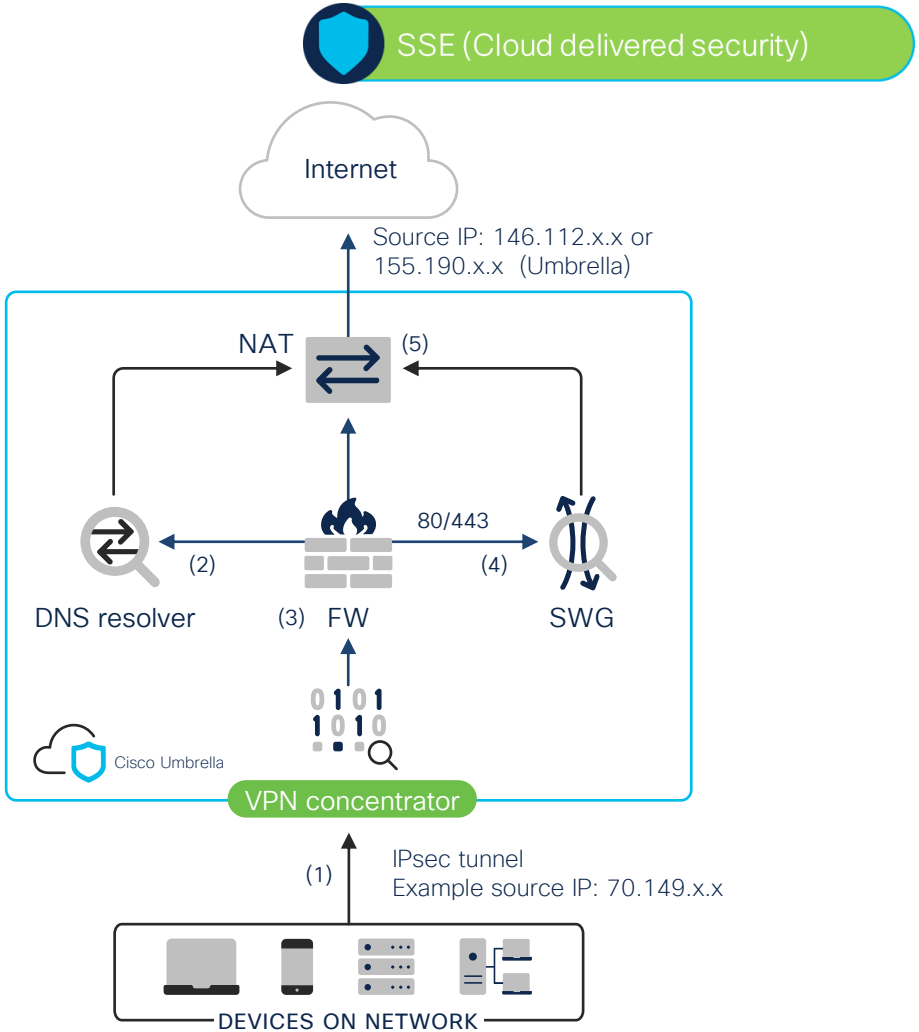


Application flow

DNS, SWG, and CDFW rules

1. Forward traffic via IPSEC tunnel to the cloud.
2. Apply DNS security policy.
3. CDFW inspects traffic (layer 3, 4, 7 and IPS). Web traffic not blocked by CDFW is sent to SWG.
4. SWG does its policy inspection (DLP or RBI is applied).
5. 'Allowed' traffic egresses through NAT.

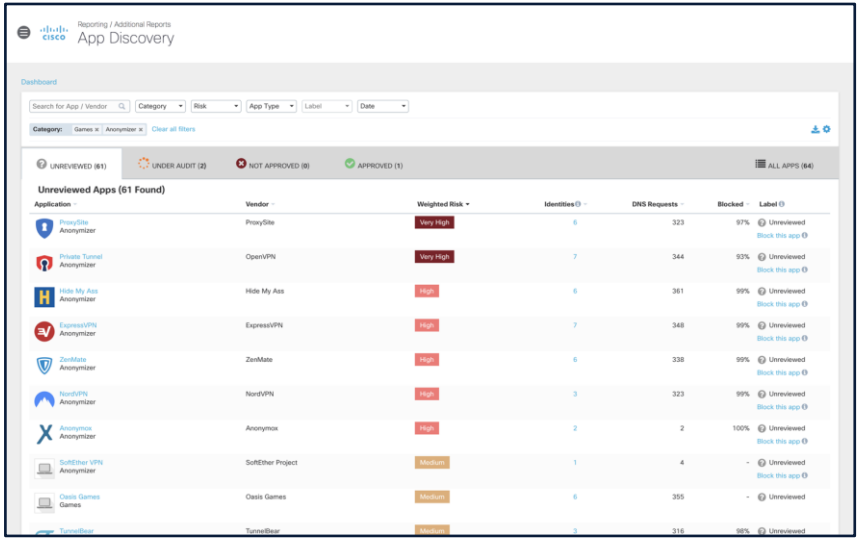
Traffic is logged at each stage.



CASB – App discovery and controls

Visibility into shadow IT and control of cloud apps

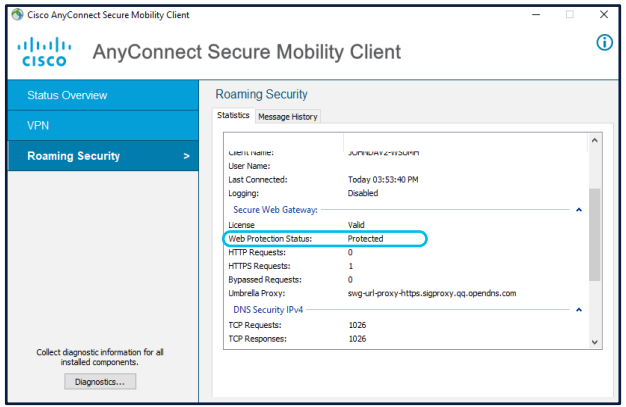
- Full list of cloud apps in use
- Reports by category and risk level
- Number of users and amount of incoming and outgoing traffic
- Blocking of high-risk categories or individual apps



SSE (Cloud delivered security)

Secure Client

- Secure client can be used across an entire enterprise
- Both Umbrella DNS and Secure Web Gateway services can co-exist
- Protect assets on or off network
- Simple and consistent user attribution
- Choice of fail open or fail closed



Supports Windows and Mac desktops

Talos: the largest threat intelligence organization on the planet

- 400+ full-time threat researchers and data scientists
- 5 billion reputation requests, 2 billion malware samples seen daily
- 5 billion category responses, 200 million IPs & URLs blocked daily.

We see more so you can block more and respond faster to threats.

SASE building block #3

End-to-end visibility

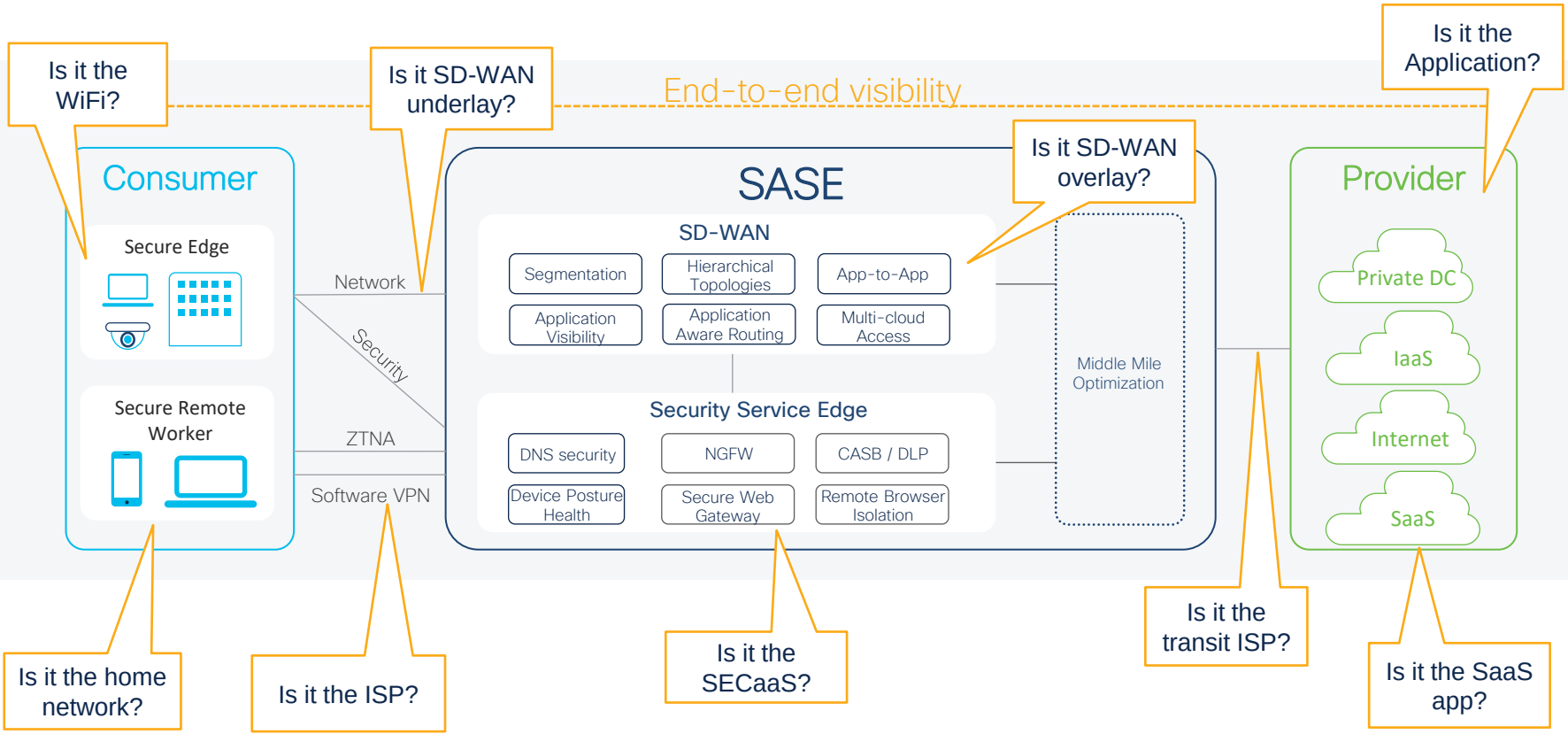
Visibility end-to-end

App performance	Path visualization	Internet and WAN health	BGP route monitoring	Remote worker experience
✓	✓	✓	✓	✓
Isolate app issues from network issues	Pinpoint issues down to a service provider, location and interface	Internet is your new WAN. Monitor its performance	Ensure Internet routing issues don't affect your users and services	Business apps must be available when employees work from home

Correlated insights to take action

Visibility from every user, to any application, over any network.

A holistic view



Visibility end-to-end

Predictive network assurance for digital experience

Forecasts conditions

Identifies expected issues based on predictive analysis

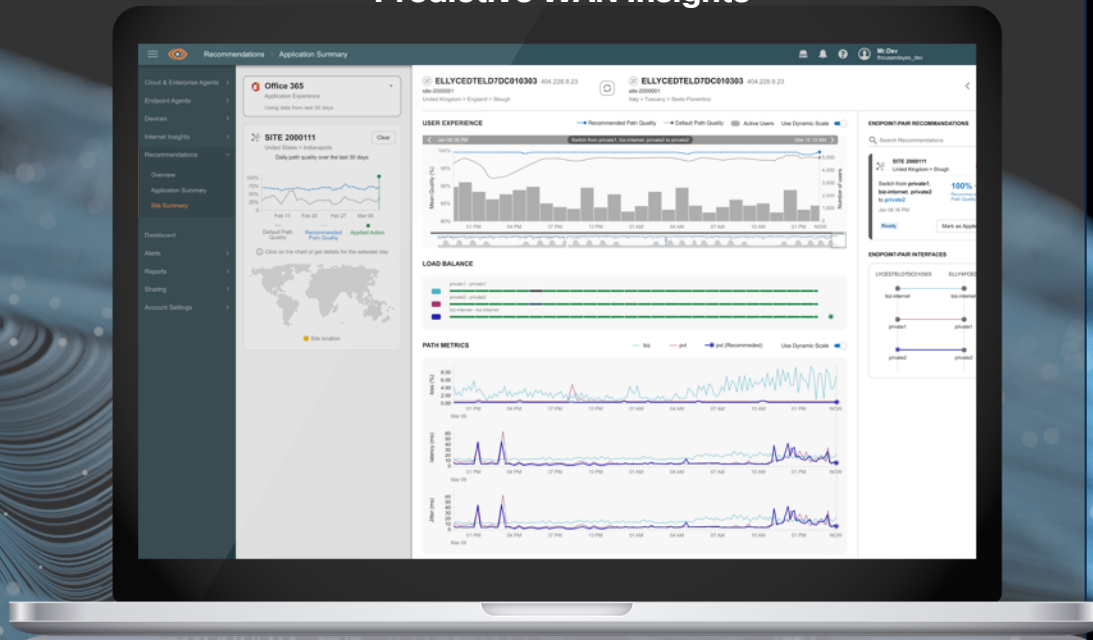
Recommends actions

Provides specific steps to improve application experience

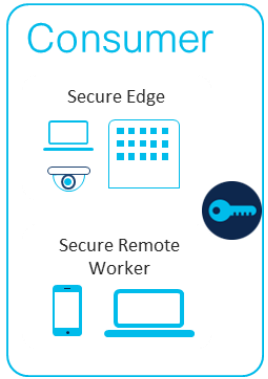
Improves experience

Sustained improvement over a longer period of time—promotes continuous improvement

Predictive WAN Insights



SASE building block #4



Zero Trust

Adaptive MFA	Device posture and health	Least privileged access	Continuous verification	Behavior analytics
✓	✓	✓	✓	✓
Ensure users are who they say they are	Assess and enforce the endpoint for health prior to login	Zero Trust – ensure security and posture at EVERY application login	Every login gets continued security analysis	Detect and report on anomalous, unusual and suspect login/access activity

Every user. Every device. Every application.

It's segmentation

It's ZTNA

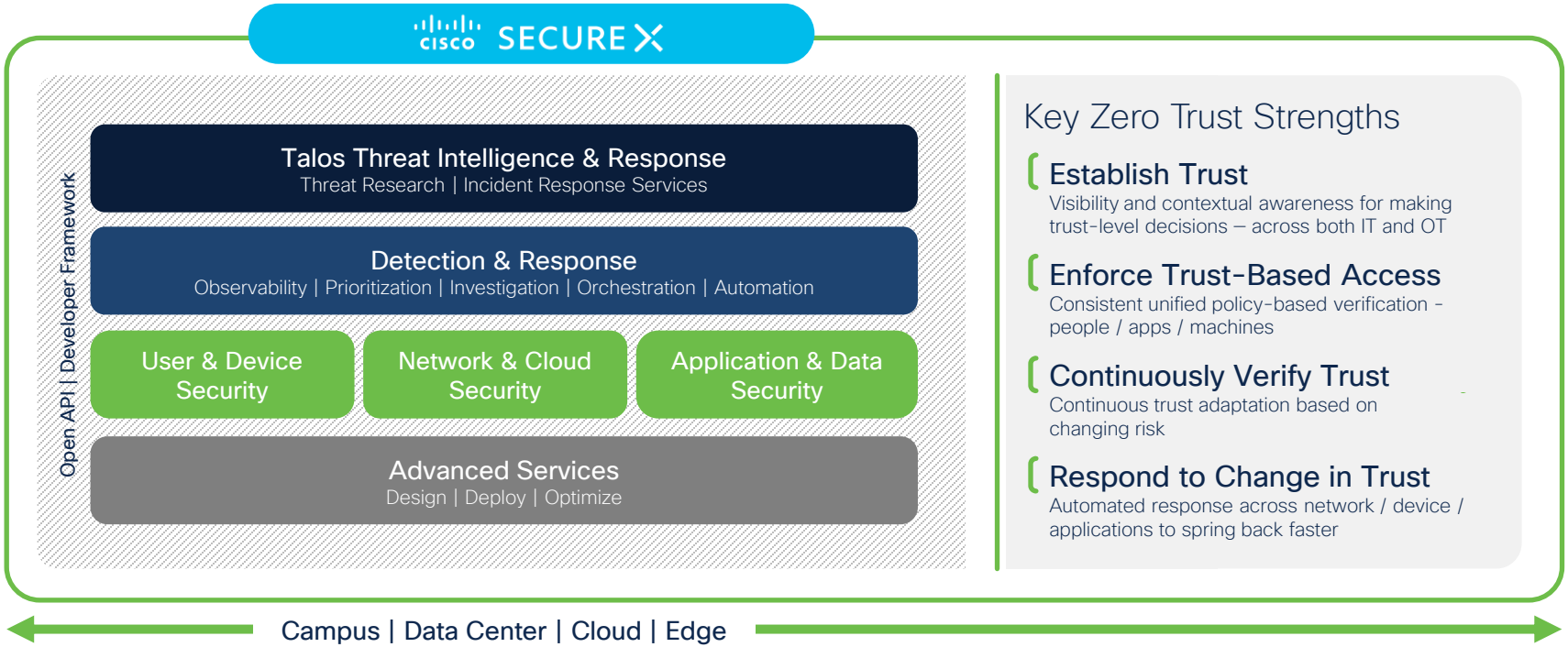
It's endpoint security

Zero Trust means different things to different people

It's firewall

It's identity

Delivering Zero Trust to meet where you are

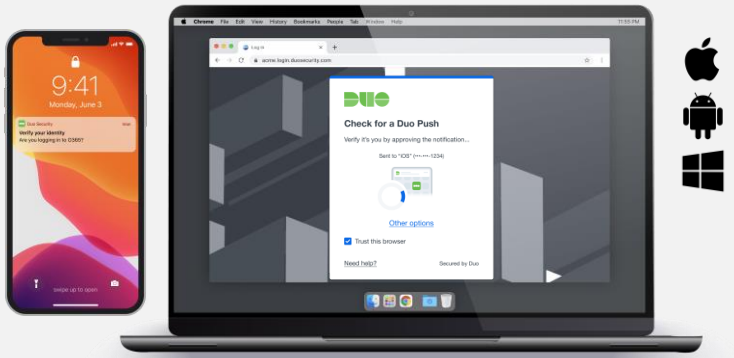


Zero Trust

Establish trust

Remote user trying to access a *cloud app* from their device

1. User starts authentication
2. User is verified, device posture is checked, device trust is validated
3. User gains the right access and session



Strong Security

- **Enable broadest MFA options** – push, calls, SMS, biometrics, wearables, passwordless, tokens, and more
- **Establish device trust** – device risk level, compliance, management and compromise status
- **Set adaptive policies** – global, app, and group-level access to hundreds of apps based on verified business need

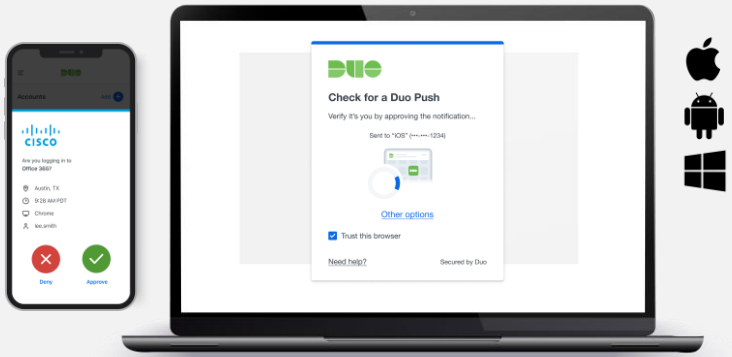
High Productivity

- **Remove user friction** – authenticate in seconds, fewest number of clicks
- **Adopt in just days –** SaaS deployment, users enroll in a few easy steps
- **Reduce help desk tickets** – user self-enrollment, self-service to update and reset devices

Zero Trust

Enforce trust-based access

Remote user trying to access a *private application* without VPN



1. User requires access to private app from managed or unmanaged device
2. User can directly access app using any browser (without any remote access software)
3. User gets access only to the app (and nothing more)

Strong Security

- **Establish explicit trust** – default closed access model with access on a per-app basis
- **Secure highly used and high-risk protocols –** RDP and SSH
- **Secure BYOD** – device posture assessment for unmanaged devices

High Productivity

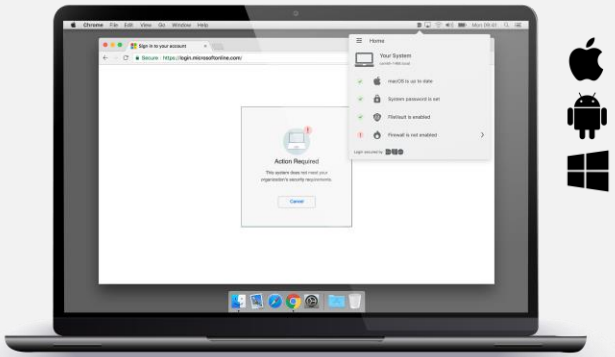
- **Provide frictionless, consistent access** – for any application, using any browser
- **Reduce latency** – scalable, VPN-less access to applications
- **Support hybrid environments** – cloud and on-premises implementation options, instant access to apps anywhere, single-sign-on (SSO) integration

Zero Trust

Continuously verify trust

Remote user and device behavior impacts trust levels

1. User is already authenticated and using an app
2. Firewall is disabled; trust is lost, app access is revoked
3. User prompted to re-enable firewall to regain access; event is captured



Strong Security

- **Share signals to quickly detect change in risk** – device posture, disabled security features, vulnerabilities, etc.
- **Leverage contextual awareness** – GeoIP, Wi-Fi fingerprint, authentication history, etc.
- **Control user sessions** – integration with Cisco and third-party apps such as Webex and Box

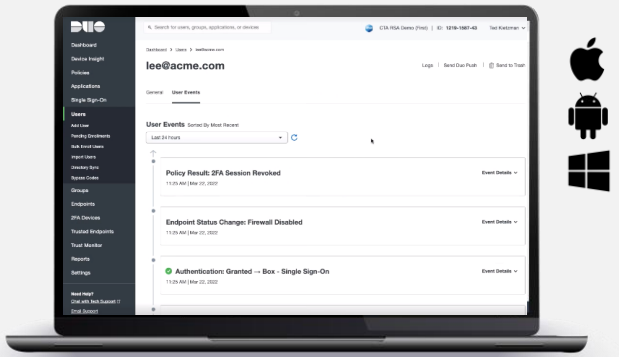
High Productivity

- **Work without interruption** – session extension for high trust
- **Improve IT efficiency** – automatic access revocation
- **Expedite restoration of access** – user self-service remediation

Respond to change in trust

User's device potentially compromised

1. Firewall is disabled; trust is lost, app access is revoked
2. Analyst immediately investigates to detect potential breach in progress
3. Analyst finds a malware alert on the device; device access is blocked



Strong Security

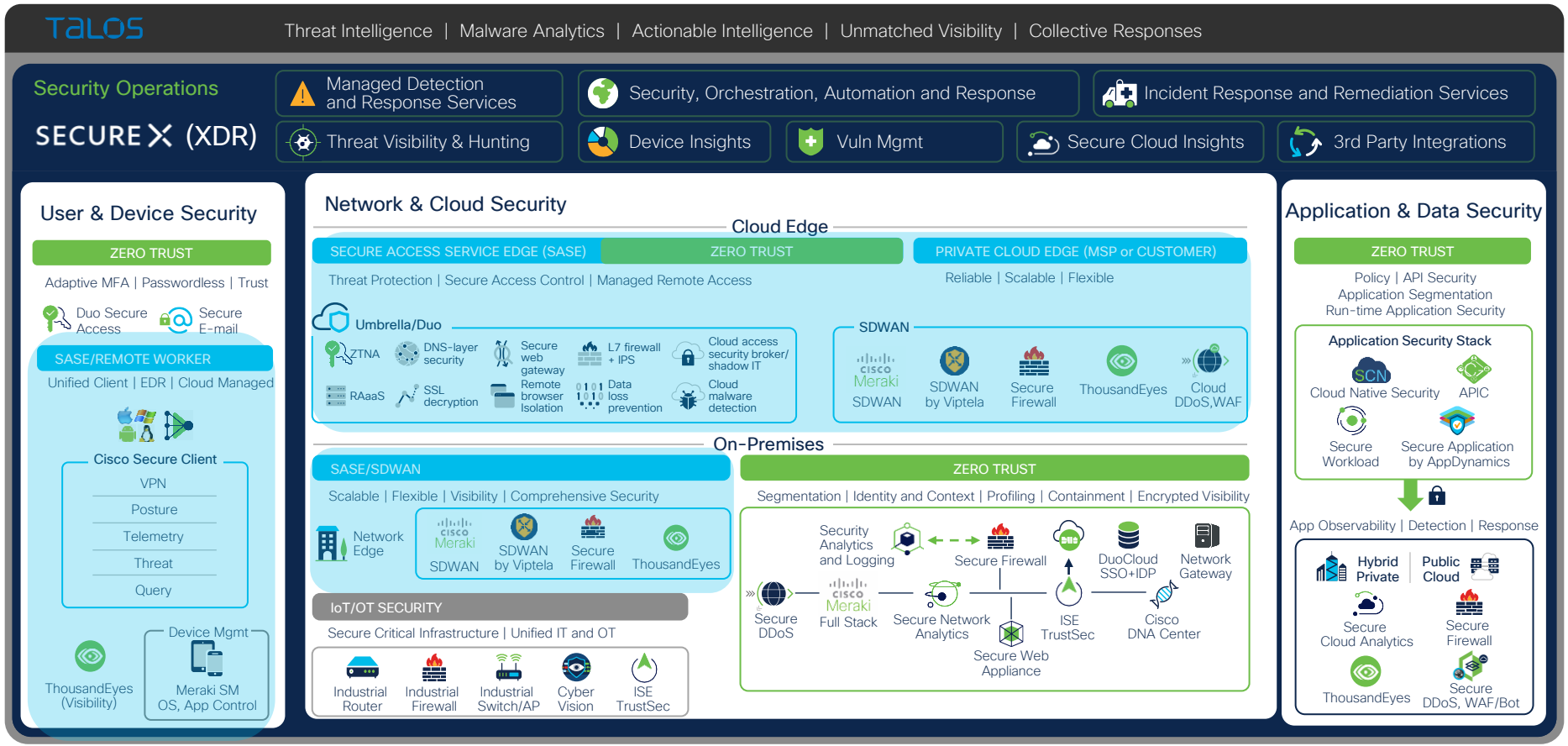
- **Detect breaches early** – immediate notification of changes in trust, integrated threat intelligence
- **Quickly pinpoint incident scope and origin** – forensic analysis, file and device trajectory
- **Prevent data theft and lateral movement** – device isolation

High Productivity

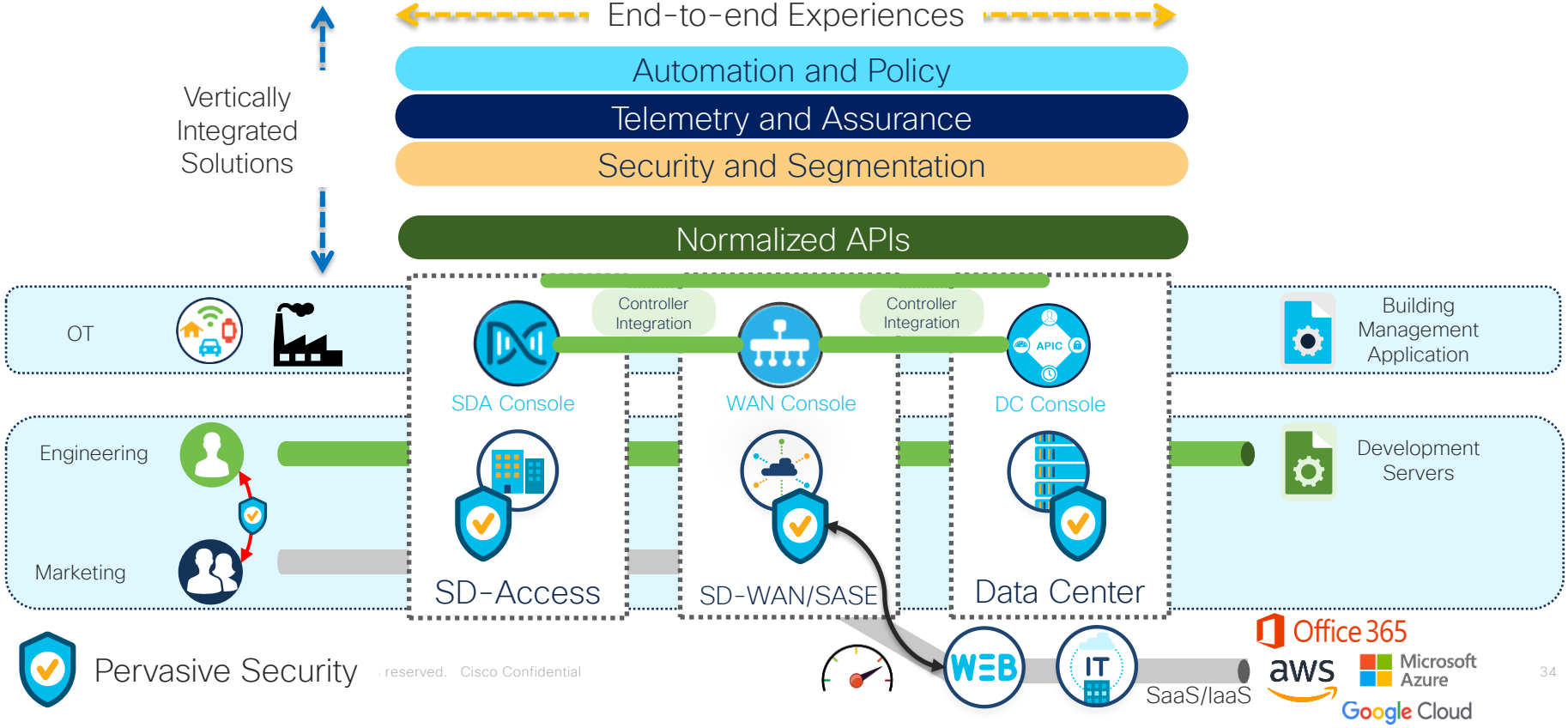
- **Work without interruption** – BYOD support
- **Accelerate threat response** – unified visibility, aggregation and correlation of data across entire environment
- **Accomplish more with current teams –** playbooks, workflows, and playbook-driven automation

CISCO SECURE

Security Reference Architecture

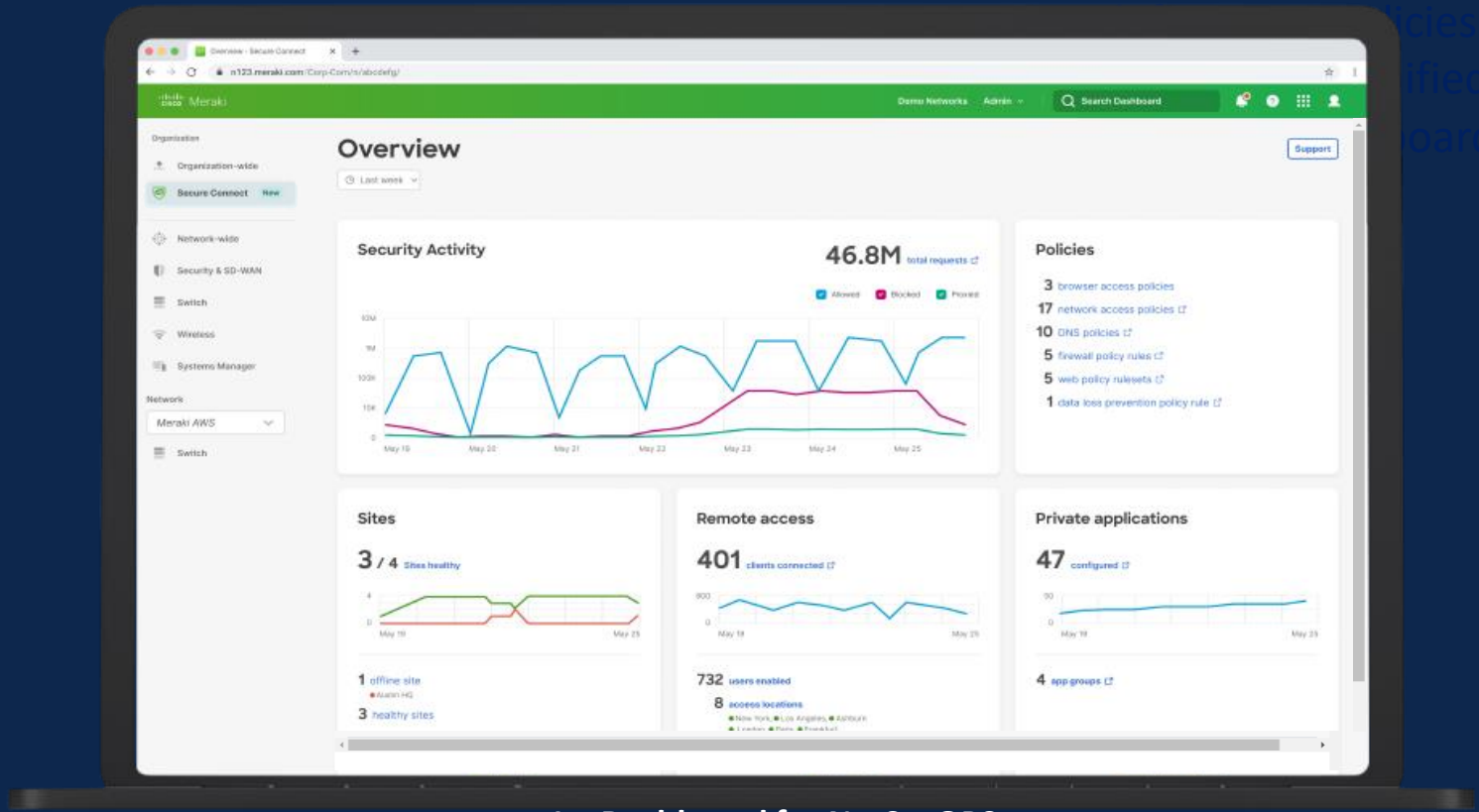


The Secure Productivity Experience Delivered




Integrated Dashboard

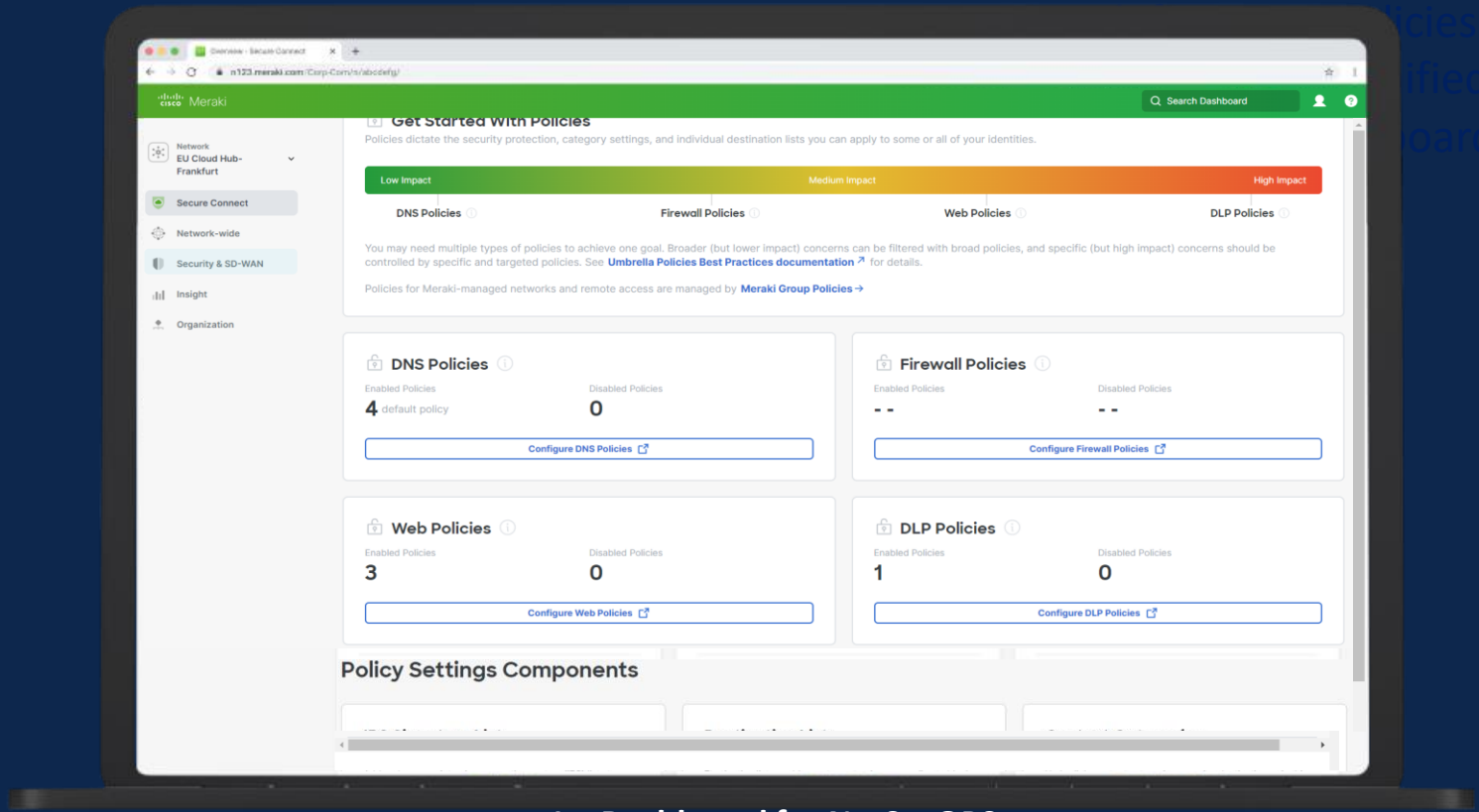
Dashboard Overview



1 x Dashboard for NetSecOPS

No upfront investment or set-up is required.

Dashboard Security

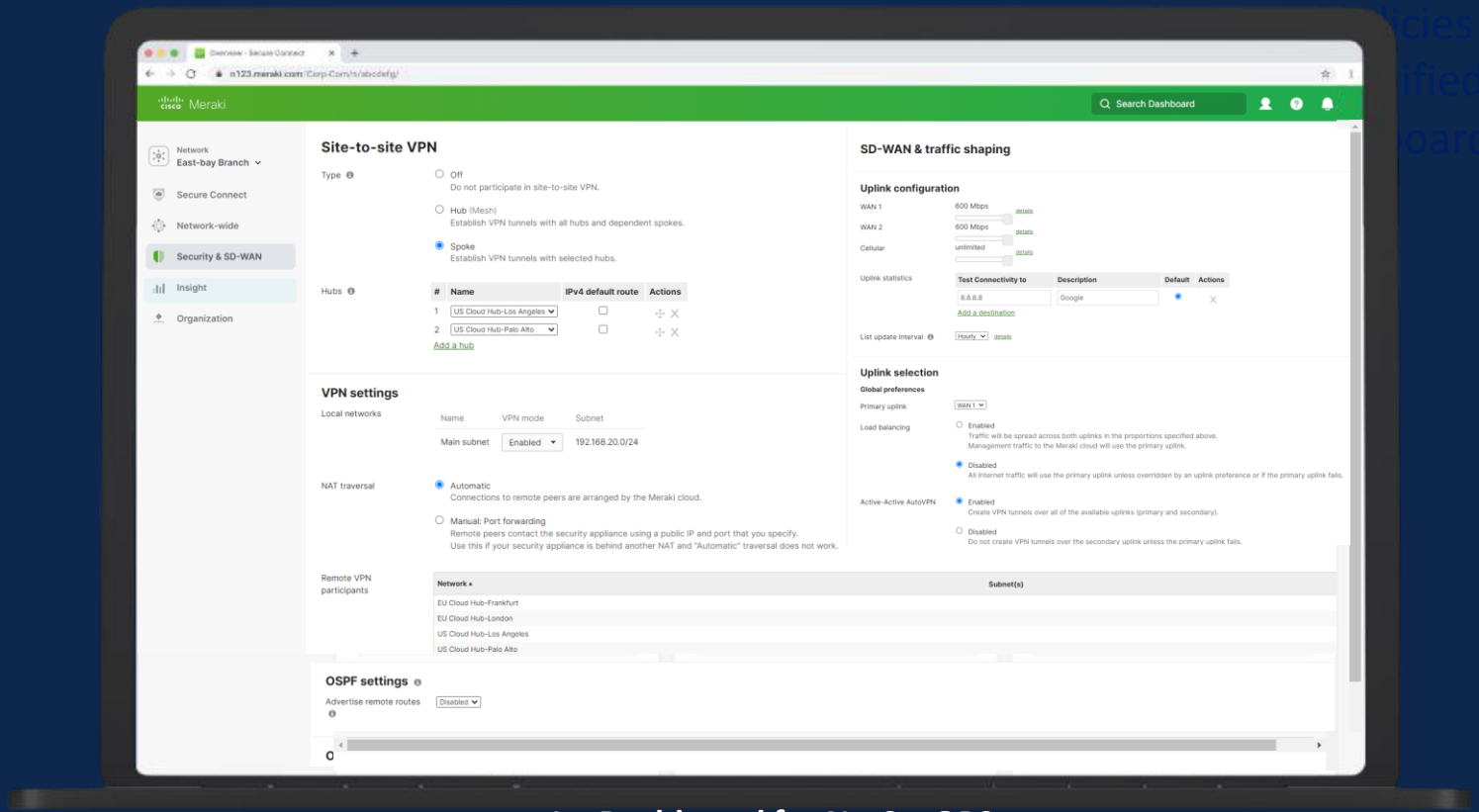


1 x Dashboard for NetSecOPS

No upfront investment or set-up is required.

Dashboard SD-WAN

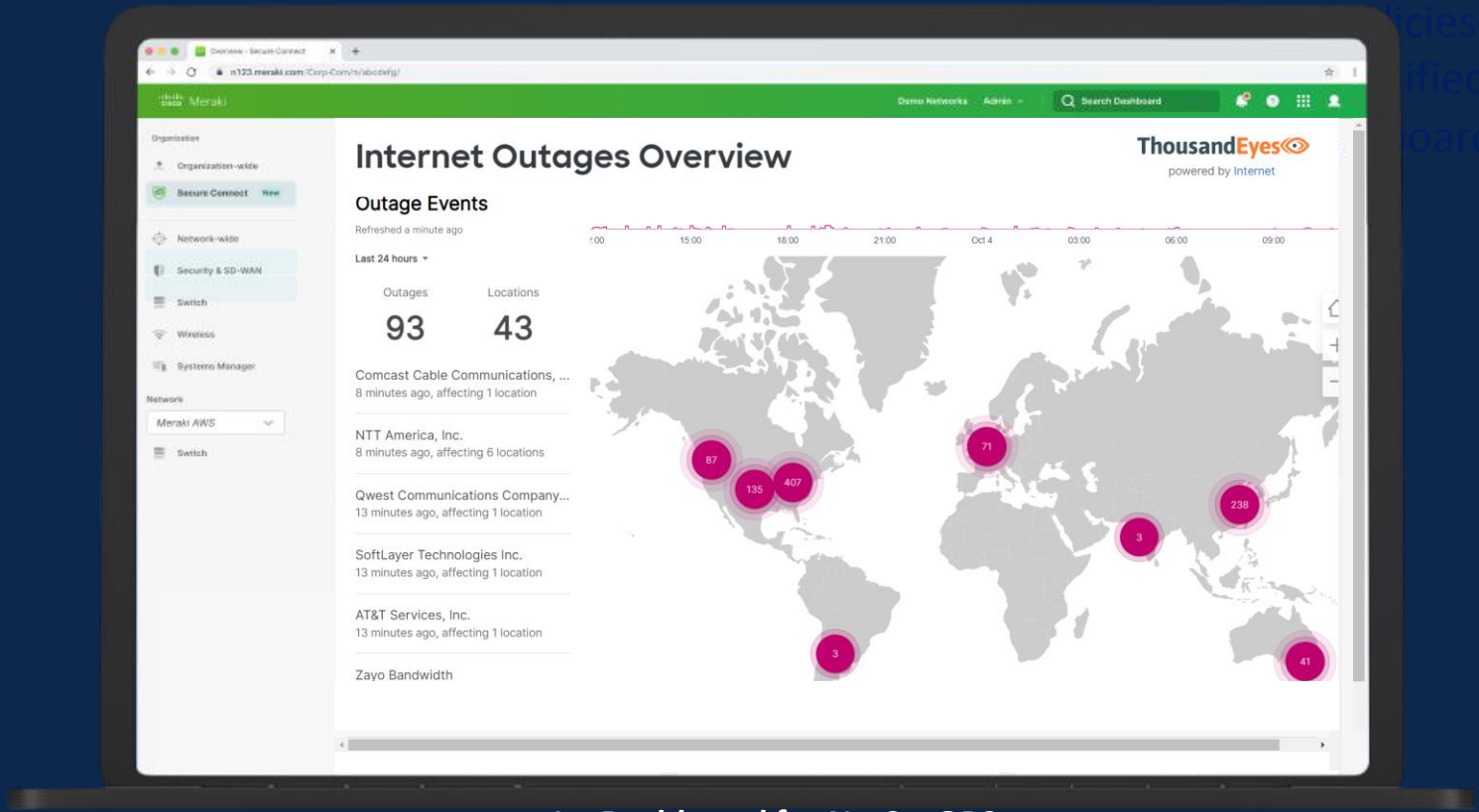
Activate Connectivity and Security at lightning speed, icies once — ified cloud- oard.



1 x Dashboard for NetSecOPS

No upfront investment or set-up is required.

Dashboard Visibility



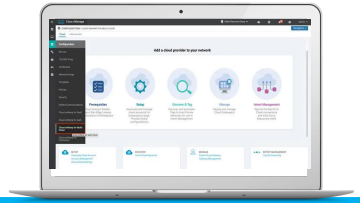
1 x Dashboard for NetSecOPS

No upfront investment or set-up is required.

Customer benefits

Hybrid Worker

- Anywhere, Anything connectivity with an optimal user experience and security.



NetSecOps

- 1 x Dashboard to configure Networking and Security policies and have visibility end-to-end
- Multicloud Access/SDCI; rapid deployments to build connectivity

CIO/CISO

- General cost reduction; MPLS vs Internet, SASE as a subscription service Capex vs Opex. Hardware reduction in DC, energy/rackspace reduction
- Sustainability; further lower carbon footprint by consuming services from the Cloud, FTE reduction

Cisco's journey

We've made our $50B global company a test-bed for Zero Trust

"It's not often that you can say you are improving security while also improving the user experience, but that's what we have achieved with this rollout."

– **Josephina Fernandez**
Director, Security Architecture & Research, Cisco

170,000+ devices secured
5.76 million health checks/month
86,000 devices/month remediated

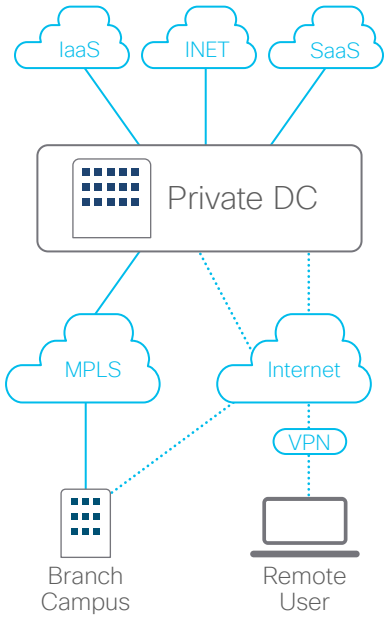
100,000+ users onboarded
Only < 1% contacting helpdesk

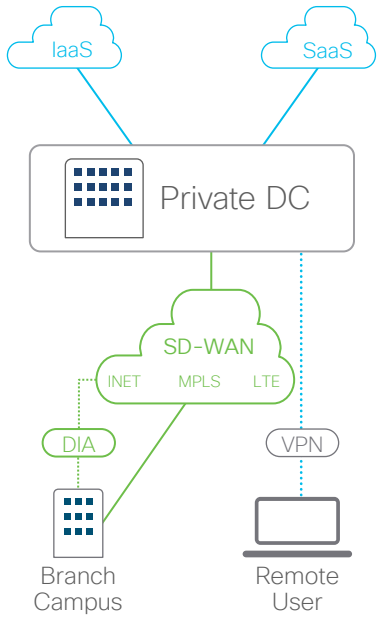
410,000+ fewer VPN auths/month
Users no longer need the VPN for access to more than 100 applications (on-premises and SaaS)

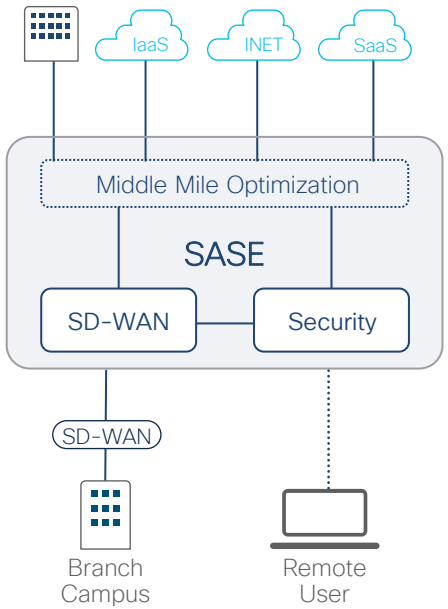
5-month deployment timeline
From defining requirements in July to enterprise-wide rollout of 98 countries in December

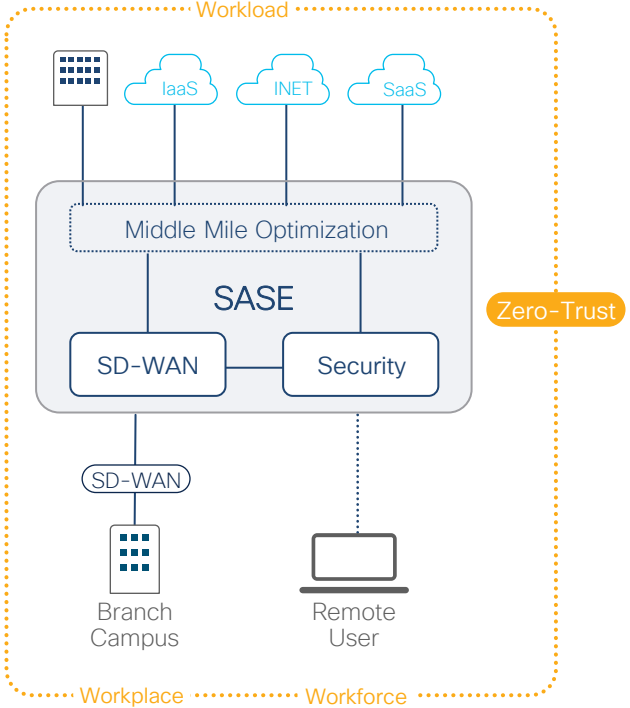
SASE is a Journey

DC-centric topology → Move to SD-WAN and DIA → Private DC to cloud-enabled and consolidating services → Wrap in Zero-Trust









Want to learn more about Cisco SASE?

cisco.com/go/sase

Ernest Pronk

Cisco | SD-WAN - SASE Specialist | Helping customers to optimize and secure their Hybrid Workforce experience.

Amsterdam, North Holland, Netherlands · Contact info

Contact Info

Your Profile
linkedin.com/in/ernestpronk

Website
cisco.com (Company)

Email
epronk@cisco.com