Zero Trust Access by Cisco

Powering a secure, in-office experience, for an anywhere workplace

All kinds of...

Users
(and devices)

Places
(and networks)

Apps
(and data)

Overview

Today's modern workforce is highly distributed, with users working at home, in the office, and places in between and beyond. Protecting distributed employees who need to access resources in private and public data centers requires reliable and secure access plus deep visibility into how identities gain access—to verify that users and devices are trusted and should have access. Most global enterprises struggle with this. Concerns about stronger security potentially impeding user productivity and increased IT complexity from security tool proliferation contribute to this struggle.

By taking an identity-first approach to SSE, Zero Trust Access by Cisco powers a secure, in-office experience for all users, wherever they work and no matter where resources reside. It eases the transition to zero trust by delivering a consistent and frictionless user experience that boosts productivity, simplified administration that streamlines IT operations, and highly resilient security for all.

By taking an identity-first approach to SSE, Zero Trust Access by Cisco provides comprehensive coverage and a seamless experience securing all users, all locations, all applications, and all devices, helping enterprises accelerate their journey to zero trust.

"By centralizing telemetry and data, we're streamlining incident management, eliminating the need for multiple teams to analyze networking and security data, and sidestepping complex tasks like IP—user mapping. We've seen reductions in mean time to troubleshoot by up to 25%."

Rich West, Principal Engineer,
Cisco Security and Trust Organization

Benefits

Elevate user productivity.

- An in-office experience for everyone from everywhere
- Transparent, automatic connectivity via either Zero Trust Network Access (ZTNA) or VPN-as-a-Service (VPNaaS)
- Fast user verification that gives trusted users longer access and fewer authentications

Streamline IT administration.

- End-to-end visibility with digital experience monitoring (DEM)
- Smooth migration from on-premises VPN to ZTNA via transparent use of VPNaaS
- Simplified IT management via unified agent, single console, consistent security policy

Increase security and resilience.

- Application access control over all ports and protocols
- User trust score with increased visibility into identity posture and access activity
- Better user experience reduces the number of frustrated/distracted users who can be easy targets for identity-based attacks.
- Advanced, AI-assisted threat detection from Cisco Talos

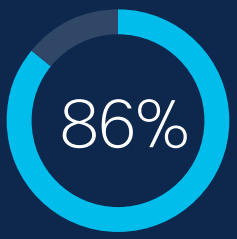
Trends and challenges

Your organization is trying to secure all kinds of users and diverse devices, connecting from anywhere to applications of varying architectures, across data centers and public clouds. Yet, your workers expect easy, fast, and reliable connections.

Most SSE solutions cannot deliver on the promise of easy, secure access for all. That's why zero trust projects are stalling. Although 86% of organizations have started adopting zero trust security, only 32% have achieved maturity in one (of four) pillars and virtually none have achieved maturity in all four pillars.[1] Many existing SSE solutions touting 'zero trust' aren't designed for this and are creating frustration for users and IT/security teams.

Users typically find it harder to connect to applications when working remotely than when in the office. There are more authentication obstacles, VPNs to fire up, and connectivity is often unreliable.

IT teams are juggling far too many technologies, and the tool sprawl aggravates complexity, inefficiency, and security gaps. While SSE does promise to streamline workflows and gain efficiencies, most SSE solutions fall short in security convergence and unified management.



Nearly all organizations have started on some aspect of zero trust (at least one pillar)

Have reached maturity across all CISA pillars... meaning that 98% have not.

Key Challenges

- Poor user experience
- Diverse set of assets to protect
- Too many technologies to manage

[1] Cisco's Security Outcomes for Zero Trust report, January 2024

How it works: Key features and components

Cisco developed its purpose-built architecture for zero trust security just like the hyperscalers, using modern and performant technology that readily scales to cloud speeds. Cisco's Zero Trust Access brings together a verified set of cloud-based security services including:

Cisco Security Service Edge (SSE)

SSE from Cisco combines a unique level of user simplicity and IT efficiency for frictionless access to all applications (not some). Using a cloud-centric approach for enforcing security policies, grounded in zero trust, it protects users, data, and devices as they securely access private applications, SaaS applications, and the internet, from on or off the corporate network. Users enjoy a better experience, IT/security teams simplify operations, and the organization increases security.

Cisco's SSE solution unifies multiple cloud-native capabilities such as secure web gateway (SWG), cloud firewall, cloud access security broker (CASB), zero trust network access (ZTNA), data loss prevention (DLP), remote browser isolation (RBI), DNS-layer security, and more.

Cisco Identity Security

Cisco's solution offers multiple ways to enforce identity security for your workforce. Examples include:

- Phishing-resistant MFA to verify users truly are who they say they are
- Device posture checks and the ability to block unwanted access with a trusted endpoint policy
- Passwordless SSO to reduce password usage and thus shrink the attack surface
- Risk-based authentication that adapts access dynamically based on user or device behavior
- Wi-fi profile analysis and session trust analysis to bring visibility and control to risk remediation during an established session

But it doesn't end there.

Cisco Identity Security can ingest identity data from Cisco and third-party identity providers (IdP) and sources such as Workday and Salesforce, analyze identity activity across all accounts, devices, and IdPs, then assess security posture and enhance enforcement points. For example, if a third-party identity source

detects risk, Cisco Duo can increase authentication requirements.

In short, organizations can move from determining whether to grant access to the vastly more important question—should they grant access.

Digital experience monitoring (DEM)

When rolling out zero trust access for your distributed workforce, your IT team needs to monitor the health and performance of users, applications, and network connectivity. Zero Trust Access by Cisco includes integrated DEM capability (based on ThousandEyes) to provide this monitoring – from the end user to the requested site and across the hops in between. Administrators gain details on endpoint activity including:

- Active and inactive users worldwide
- Connectivity metrics such as throughput rates, bandwidth utilization, latency, jitter, and packet loss on each network segment
- Application performance and reachability for private applications and over 20 SaaS applications

This helps to keep hybrid and remote users working at top productivity.

Start where you are. Go at your own pace.

Zero Trust Access by Cisco is comprised of capabilities from Cisco Secure Access, Cisco Duo, and Cisco Identity Intelligence. However, you can start where your need is greatest and evolve at your own pace. Depending upon your situation, you might begin with any of these products:

- Cisco User Protection Suite
- Cisco Duo
- Cisco Secure Access

What makes Zero Trust Access by Cisco unique?

Differentiated for user experience

- ✓ Lower latency, more reliable connectivity via the next-generation QUIC/MASQUE architecture
- ✓ Higher throughput via performant technology such as Vector Packet Processing (VPP)
- ✓ Native mobile support via OS integrations with QUIC
- ✓ Passwordless login that brokers trust at the OS level and passes trust forward (e.g. different browser, different application), without the need to be network or domain joined
- ✓ Continuous background posture and security checking, only prompting reauthentication if risk increases

Unique for IT/security administration

- ✓ Integrated DEM to quickly identify bottlenecks, speed troubleshooting, accelerate remediation
- ✓ Single, unified client for remote access services and a suite of modular security services
- ✓ AI Assistant accelerates policy creation and simplifies management
- ✓ Ability to safely use generative AI tools
- ✓ User trust score, distilled from cross-platform activity, for use in security policy and decisions

Unmatched for security efficacy

- ✓ Deep visibility into identity posture and access activity across diverse identity sources
- ✓ DNS-layer security blocks most threats before they reach into the security stack
- ✓ Cross-platform detection of identity-related activity, using broad context and integration with enforcement

Platform approach

Most SSE solutions emerged from point solution vendors (e.g. CASB, NGFW, or SWG) who bolted on additional capabilities, an approach that can impact user productivity, lower security efficacy, and leave gaps for identity-based attacks. Contrary to this, Zero Trust Access by Cisco offers a unique platform approach that brings together:

- ✓ Verified set of cloud-based security services including SSE and a unified client to secure access
- ✓ Identity intelligence to continually verify identity at every access decision
- ✓ Ability to detect and respond to threats before they spread, with generative AI and machine learning

In short, a comprehensive architecture for applying zero trust security across the pillars of identity, access, and response

> "We wanted to approach security as one integrated ecosystem to ensure defense-in-depth. And the vendor with the most cohesive security platform was Cisco."
>
> **Network Security Architect, Banking**

Use cases

Access	Secure access for users and things, from anywhere to resources everywhere, while delivering a consistent, seamless, and low-latency user experience. Granular controls enable the right access to the right resource.
Identity	Gain smart access and authentication for users and things, with access dynamically adjusted based on user or device behavior. Deep visibility across identity sources enables correlation of identity data, detection of attack patterns, and powerful remediation.
Resilience	Achieve a highly resilient security infrastructure that withstands or recovers quickly from difficulties via resilient connectivity, robust and multilayer security, and deep visibility to keep the user experience performant and productive.

Cisco advantage (why Cisco?)

Zero Trust Access by Cisco safely connects users anywhere to applications everywhere for a consistent, simple, frictionless user experience. It eases zero trust adoption for IT and security teams struggling to orchestrate disparate security solutions for securing their highly distributed workforce. Industry-leading security efficacy increases resilience and reduces organizational risk.

It's security that frustrates attackers and not users.

Learn More

Learn more by visiting https://www.cisco.com/go/zta or contact your Cisco sales representative.