Zero Trust Access (ZTA)

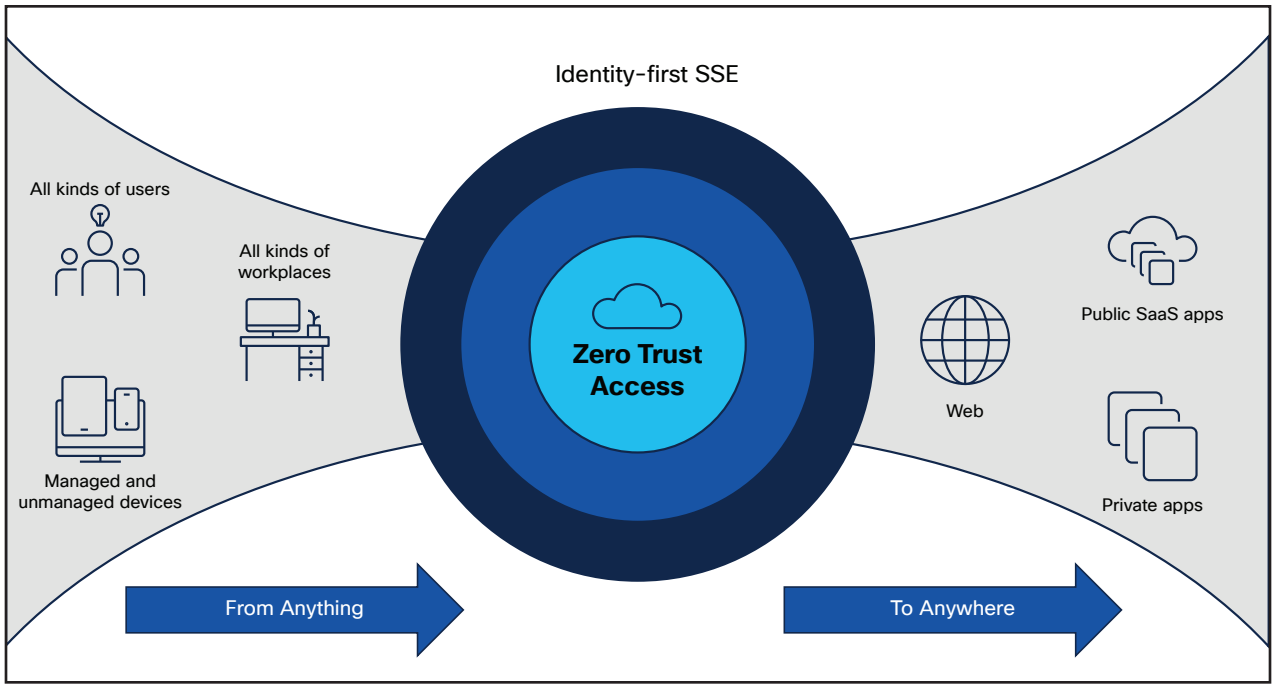
Today's distributed workforce requires secure access to a diverse set of applications and resources from any location, at any time. Your IT and security teams strive to protect users, workplaces, devices, and networks. Yet, the vast set of technologies used for zero trust adoption lack integration and are not designed to protect today's distributed environment. This tool sprawl increases complexity, inefficiency, and security gaps. While third-party Security Service Edge (SSE) products promise to streamline workflows and gain efficiencies, most fall short in security convergence and unified management.

And there is the concern of stronger security controls impeding user productivity. Your users expect an easy, fast, and reliable connection to the specific applications they require to do their jobs. You need security that's designed for this environment to boost user productivity, minimize risk, and employ zero trust principles to provide the right level of access.

By taking an identity-first approach to SSE, Cisco® Zero Trust Access (ZTA) powers a secure, in-office experience for all users, wherever they work and no matter where resources reside. It eases zero trust adoption for IT/security teams struggling to orchestrate disparate security solutions to secure their distributed workforce and workplace.

Benefits

- Better user experience with transparent, automatic secure connectivity for frictionless access to all applications—not some
- Simplified IT management via a single agent, single console, unified security policy set with end-to-end visibility from Digital Experience Monitoring (DEM)
- Fast user verification that gives trusted users longer access and fewer authentications
- Deep visibility into identity posture and access activity across diverse identity sources to protect against identity-based attacks
- Industry-leading security efficacy reduces organizational risk and sharpens resilience. It's security that frustrates attackers and not users



Cisco developed its purpose-built architecture for zero trust security using modern technology that readily scales to cloud speeds. Cisco Zero Trust Access brings together a verified set of cloud-based security services including:

Security Service Edge (SSE) from Cisco protects users, data, and devices as they securely access private applications, SaaS applications, and the internet, from on or off the corporate network. It provides seamless and secure access from anything to anywhere, so users enjoy a better experience, IT/security teams simplify operations, and the organization increases security via granular controls.

Cisco's SSE solution unifies multiple cloud-native capabilities such as Digital Experience Monitoring (DEM), Secure Web Gateway (SWG), Firewall as a Service (FWaaS), 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 Zero Trust Access solution offers multiple ways to enforce identity security for your workforce. It includes Multi-Factor Authentication (MFA), Single Sign-On (SSO), device security posture verification, and adaptive authentication. It ingests identity data from Cisco and third-party Identity Providers (IdP) and other sources such as Workday and Salesforce, analyzes the comprehensive identity-related activity across all accounts, devices, and IdPs, then assesses security posture and enhances enforcement points.

Organizations can move from determining whether to grant access to the 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. Cisco's Zero Trust Access includes integrated DEM capability to provide monitoring from the end user to the requested site and across the hops in between. Administrators gain details on endpoint activity including active/inactive users worldwide, connectivity metrics (throughput, bandwidth, latency), and application performance and reachability to help keep users working at top productivity.

Start where you are. Go at your own pace.

Cisco's Zero Trust Access is comprised of capabilities from Cisco Secure Access and Cisco Duo. 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

The Cisco Zero Trust Access solution accelerates zero trust adoption to protect all users, all locations, all apps, and all devices. Learn more about Cisco Zero Trust Access at https://www.cisco.com/go/zta.

C45-4703612-00 09/24