Redefining Universal ZTNA: Securing the Future-proof Workplace

Securing the Future-proof Workplace

Never trust, always verify, enforce least privilege

Security leaders have long heard the steady drum beat of zero trust enthusiasts. It’s been one of the leading security frameworks recommended to organizations, and for good reason. Zero trust is often summarized as a “never trust, always verify, enforce least privilege” framework. In this context, the default assumption is that every attempt to access the network or an application could be a threat.

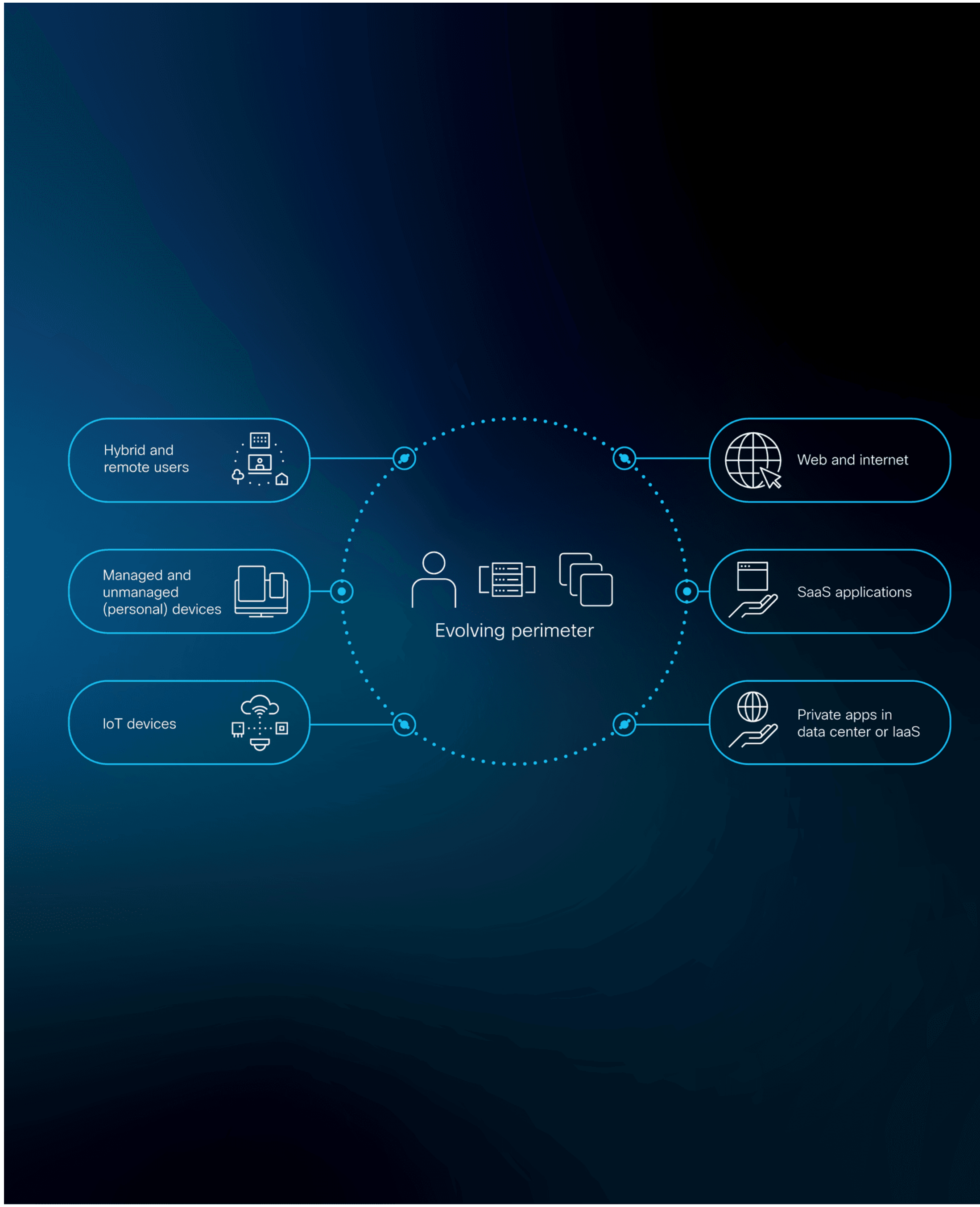
Remote users have traditionally gained access to enterprise resources through virtual private networks (VPNs), but the acceptance of hybrid working has made this unsustainable. For the last several years, Zero Trust Network Access (ZTNA) has become the norm for securing remote users as they access private applications. However, attempts by early-to-market zero trust vendors have often failed to live up to expectations. Instead of securing the modern workforce, some zero trust implementations have degraded application performance, hindered experiences, increased IT complexity and made enterprises less secure.

Cisco's Universal ZTNA

Cisco has turned zero trust on its head, using our deep understanding of the network to power a secure, in-office experience for all users across all locations, applications and devices. Our solution is delivered seamlessly through a single client, single console, AI-driven architecture, for fast and reliable (yet secure) application access to authorized users wherever resources reside. Ensuring a frictionless experience for remote users allows them to work productively wherever their business takes them – and without putting the organization at risk.

Universal ZTNA is only possible with a convergence of network and security for zero trust everywhere. Unlike ZTNA, which only protects remote user to private app access, Universal ZTNA covers all aspects of access for all users and IOT devices anywhere, accessing applications and resources everywhere, with flexible enforcement options.

▶ Watch more



Remote access, resilience, and user experience

The need for a fully-realized, modern zero trust network access approach has never been more clear.

82%

of organizations cite remote logins as a heightened threat vector

91%

of employees are using multiple networks to connect to work

85%

of employees access company platforms from unmanaged devices

According to the 2024 Cybersecurity Readiness Index, the five pillars of cybersecurity readiness include Identity Intelligence, Machine Trustworthiness, Network Resilience, Cloud Reinforcement and AI Fortification.

Zero trust is a key component in each of these areas, helping organizations increase cyber resilience in an increasingly risky world. Organizations that invest in each of these areas improve their ability to protect against today’s evolving threats. Zero trust is key to implementing these strategies.

The five pillars of cybersecurity readiness

Identity Intelligence

Machine Trustworthiness

Network Resilience

Cloud Reinforcement

AI Fortification

But if zero trust is hailed by security experts, why has delivering on zero trust in the real world been so limited and lackluster?

Remote Application Access is More Important than Ever →

SSE Solutions, Such as Standalone ZTNA, Fall Short →

Threat Actors Exploit Weak Identity Security →

Remote application access is more important than ever

The move to hybrid work has brought application performance for remote users to the forefront. VPNs were built when only a fraction of the workforce logged on from outside the network perimeter, and they aren’t designed to handle the increasing traffic of today’s remote workloads. Today’s users expect an in-office experience wherever they attempt to log in, and yet they often fail to get it. Poor performance drags down productivity and encourages users to try risky workarounds.

Cisco's Universal ZTNA accelerates least privilege access for all users across all locations, applications and devices without impacting the user experience. The best part? No action is required by the user. They simply log in and get to work and all the protection happens behind the scenes. Whether they’re at the office, at home or on the road, user experience remains the same – responsive, fast and intuitive.

SSE solutions, such as standalone ZTNA, fall short

Organizations are looking to move on from legacy VPN infrastructures and are in various stages of zero trust adoption. Unfortunately, legacy ZTNA solutions still aren't filling the gap due to their inability to cover all application types. As a result, IT teams are forced to install multiple clients and manage multiple access policies to accommodate the various ways users access applications. Users are just as confused – not knowing when they need to access an application through the VPN or whether it's safe to connect directly.

Cisco's solution is purpose-built to accelerate zero trust network access for any organization regardless of where they are in their zero trust journey. You can start moving applications – at a controlled pace – into the zero trust least privileged framework and continue to tighten controls little by little until you are completely covered. Cisco Secure Access is unique in that it offers both ZTNA and VPN in a single client and service offering allowing you to migrate along the zero trust journey at your own pace, whether on-premise or as a SaaS offering. Plus, with end-to-end visibility from ThousandEyes, you can troubleshoot performance issues faster.

Threat actors exploit weak identity security

Many legacy approaches rely on the concept of blind trust. Basically, once a threat actor gains access using a stolen credential, they essentially have free reign through the entire network and everything on it. After all, why hack in when you can just log in?

Cisco solves this problem by constantly assessing and verifying a user’s identity. This ensures entities attempting to connect to corporate resources are really who or what they say they are and ensures their requests and risky behaviors are being monitored as they navigate inside the network. These insights can trigger automatic actions if necessary or escalate issues to a human analyst.

Taking an Identity-Based Approach to Secure Application Access

A simple way of ensuring application access without putting the organization at risk

By taking an identity-first and context-aware approach to SSE, Cisco's Universal ZTNA powers a secure, in-office experience for all users across all locations, applications and devices. Our solution removes the obstacles enterprises face when implementing secure access for their hybrid workforce.

Compared to first-to-market SSE vendors who take a fragmented approach leading to a brittle architecture that lacks identity-awareness, Cisco uses modern architectures and protocols for zero trust network access that frustrates attackers and not users.

Identity Intelligence

Cisco Identity Intelligence is a unique system that constantly assesses and verifies a user’s identity, not based on a one-and-done login, but on the well-established patterns of behavior typically associated with those credentials.

Smart Authentication

Cisco enforces consistent zero trust network access for users and devices and dynamically adjusts based on trust level - across your entire ecosystem.

Everywhere Security

Cisco has taken the functions that lived in a box, defined them in software and reconstituted them into hundreds of millions of pieces and distributed them to points of presence throughout the Internet.

Identity-based approach to security

Identity is the new 'Spam'

Identity is the foundation of zero trust, making it a top target for attackers. Hardening the attack surface with zero trust capabilities means that identity can become the easiest path to compromise. Cisco's Universal ZTNA closes this blind trust between authentication and access by taking an identity-first and context-aware approach to Security Service Edge (SSE). Integrated Identity Intelligence gathers correlated identity information from all identity providers into Cisco Duo and Cisco Secure Access.

So, every time a user goes online, they establish their identity and create a trail of actions that can be analyzed to form a pattern of typical behavior. Cisco Identity Intelligence monitors a graphical database of those behaviors in real time, made up of all the different stores of identity the user creates – including actions, connections, locations, devices and applications. These insights are analyzed in real time and used to compile, change and monitor a user trust score that – when it reaches a certain threshold – can trigger security and access policy actions in real time.

Authentication of people and devices

In a world where attackers are increasingly successful at stealing legitimate users' credentials, how do you know people are who they say they are?

Smart authentication for users

Duo simplifies the user experience by providing security at the OS-level, allowing users to login once (using Mac TouchID or Windows Hello) to gain access to all their applications without re-authenticating – unless risk increases. Duo also provides modern, multi-layered defenses against the latest identity attacks such as MFA Interception and MFA Floods.

Smart authentication for devices

Automation and digital transformation mean that users aren't the only entities that need to connect to enterprise resources. Zero trust applies to device access policy as well – and an integrated approach is key. Cisco Identity Services Engine (ISE) automatically identifies and profiles devices and segments them from other parts of your network. This level of visibility and control allows IT teams to detect and block devices or sensors from accessing resources in unusual ways – a camera should not be talking to your printer or HR database, for example.

More Fabric than Fence

Extending security wherever you do business

Cisco delivers security as software distributed to global points of presence (PoPs) throughout the Internet. This hybrid architecture runs everywhere you do business today – in the public cloud, in our hosted data center for private cloud and soon to be available in on-premises campuses and branches. It’s optimized for connectivity, so all these disparate connections are executed in single pass with very low latency for high performance. This ensures a great experience for users across any device capable of accessing enterprise applications – including mobile devices.

Cisco built its SSE architecture just like the hyperscalers. We use the most modern and performant tech such as Vector Packet Processing (VPP), QUIC, and MASQUE – allowing our architecture to scale to cloud speeds. While other vendors have taken a bolted-on approach, Cisco’s solution addresses the unique requirements enterprises face when adopting zero trust.

Cisco's Universal ZTNA Changes the Game for Users and Administrators

Easily provide secure access without impacting the user experience

Cisco's Universal ZTNA provides secure application access for users without slowing them down. When their day begins, users start by logging into their computer – from home, the road or the office. They complete a phishing-resistant passwordless push, and Duo enables access to all applications they need. From there, that user will not need to use their phone again to do an interactive authentication. Instead, a single client manages the endpoint and application access behind the scenes. The user can safely open their email. They can safely browse the internet. And they can securely access private applications – either with Secure Application Access or through VPNaaS if an application is not compatible with the modern protocol.

The best part? No action is required by the user. They simply log in and get to work and all the protection happens behind the scenes. Whether they're at the office, at home or on the road, their experience accessing their apps remains the same – responsive, fast and intuitive.

For the administrator, provisioning new users for Cisco Secure Access is simple. Whether they're enabling remote employee access or a third-party contractor at the office, the process is straightforward and can been done across a distributed enterprise in a few hours. Implementing strong, phishing-resistant MFA that dynamically adjusts access to risk is also far faster and easier to set up with Cisco Duo than alternatives.

Next steps on your zero trust journey

A strong workplace security strategy means protecting users at moments of vulnerability, including their inbox, credentials, and access to applications and devices, as well as protection for devices that cannot have an agent, like cameras, printers, or unmanaged devices. Cisco’s User Protection Suite includes Universal ZTNA, as well as protection for email and endpoints to provide this holistic, layered approach.

Learn more about User Protection Suite

Ready to get started with Universal ZTNA?

Register for a workshop today.