Zero Trust Everywhere – Cisco's Universal ZTNA

In today's dynamic digital landscape, organizations are tasked with delivering seamless, secure access to applications and data across a hybrid, multi-device world. The rise of remote work, IoT, and AI applications has made it increasingly challenging to implement least privilege access consistently every time a user-or device-connects to an application. Enter Cisco's Universal ZTNA, an evolutionary approach that redefines secure access for the modern era.

Understanding the need for Universal ZTNA

The traditional network perimeter is a thing of the past. Users-whether employees, partners, or contractors-connect from virtually anywhere, using a diverse array of devices. This shift has exposed critical gaps in traditional security models, such as legacy VPNs and reverse proxies, which fail to provide the flexibility and security that modern enterprises demand.

Cisco's approach: Universal ZTNA

Cisco's Universal ZTNA is a comprehensive solution enabling every user and device to securely connect to any application, anywhere, ensuring a consistent experience. It unifies identity-first zero trust access for modern and legacy apps, IoT/OT devices, and complex network environments, combining industry-leading performance, policy assurance, and end-to-end visibility to eliminate complexity and protect critical assets. Plus, our solution supports flexible enforcement, in the cloud or on-premises, so sensitive data is protected, and governance objectives met.

Key challenges

- **Consistent access control:** Ensuring least-privileged access across remote, branch, and campus environments is essential yet complex.
- **Device management:** Managing both managed and unmanaged devices, including IoT and OT systems, is crucial but challenging, often leaving the attack surface exposed.
- **Shadow AI risks:** Mitigating use of unauthorized AI applications within the organization has become a pressing concern with the rise of Shadow AI.
- **Performance expectations:** Delivering secure access without compromising performance, especially on low-bandwidth networks, is a major hurdle.
- **Privacy mandates:** Controlling where highly sensitive data is stored – at scale, across your global environment – is a policy management headache yet a governance must-have.

Our approach helps teams **modernize application access** with ZTNA and VPN-as-a-Service in a consistent way, **extend identity context** to include users and things, and **build operational resilience** through end-to-end digital experience monitoring and policy assurance.

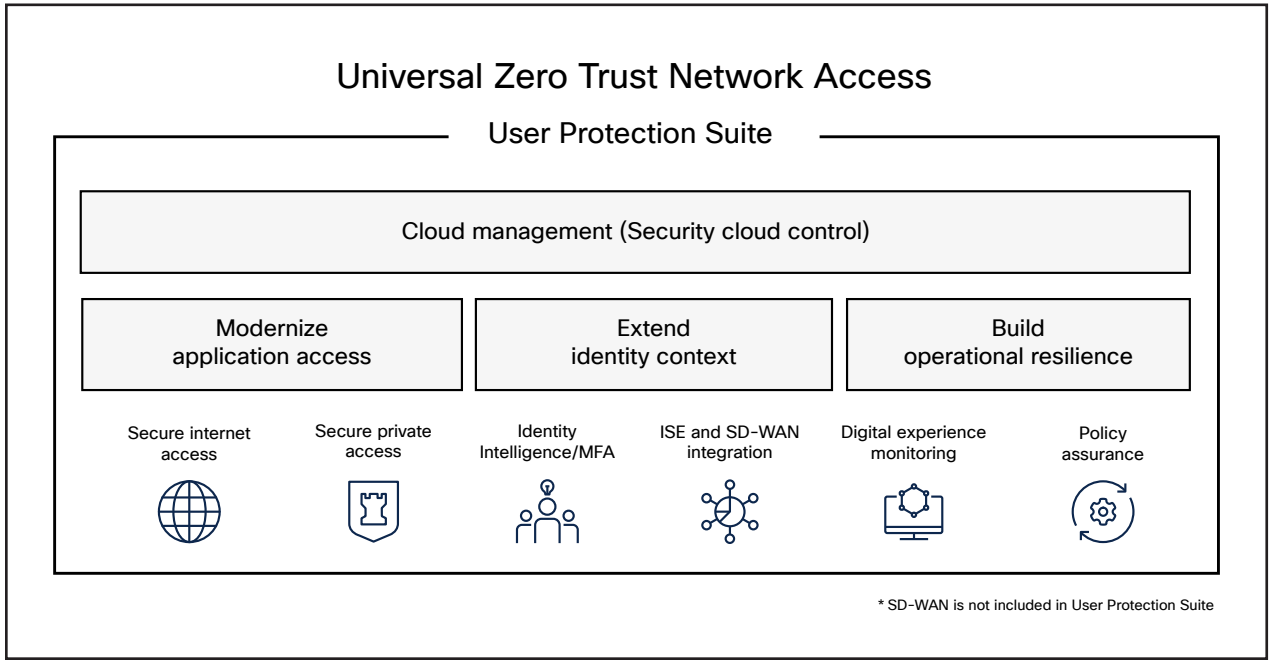

Figure 1. User Protection Suite eases our customers' journey to Universal Zero Trust Network Access

For example, via close collaboration with Google, Cisco's Universal ZTNA solution integrates with Chrome Enterprise, offering high-performance private application access with robust security controls. This collaboration enhances security and user experience on both managed and unmanaged devices, particularly benefiting third-party/contractor access and VDI migration.

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.

Key features of Cisco's Universal ZTNA

- **Access for all users, always-on:** Combining Secure Internet Access and Secure Private Access, Cisco provides a seamless and consistent experience for all users, whether remote or on-site, eliminating complex workflows and ensuring intuitive, always-available secure access.
- **User and device identity integration:** With integrated MFA and cross-platform identity intelligence, Cisco simplifies authentication and access verification by integrating user and device trust, extending beyond users to IoT, and enhancing security across distributed networks.
- **Resilient and consistent experience:** With end-to-end Digital Experience Monitoring and Policy Assurance, Cisco can help teams achieve a consistent and predictable in-office experience for users from any location, reducing risky workarounds and supporting secure AI usage.

Zero friction. Zero AI worries. Zero downtime.

Cisco's expertise in networking and security convergence positions it uniquely to deliver on the promise of Universal ZTNA. As a leader in SD-WAN, NAC, and zero trust segmentation, Cisco provides a single policy, client, and architecture adaptable to organizational needs.

Key differentiators:

- **Networking expertise:** Foundational skills in SD-WAN, VPN, and firewalls ensure seamless zero trust policy integration across hybrid environments.
- **Hybrid private access:** Consistent zero trust policy enforcement for remote, branch, and campus users across cloud and on-premises environments from a single management tool.
- **Shadow AI management:** Detects and manages use of unauthorized AI applications to prevent data leakage and ensure compliance.
- **Comprehensive application support:** Seamless handling of modern, legacy, SaaS, and private apps without disruptions.
- **Dynamic risk-based access:** Continuously adjusts access based on user behavior, device posture, and network conditions.

Start where you are. Go at your own pace.

Cisco's Universal ZTNA is comprised of capabilities from Cisco Secure Access, Cisco Duo, Cisco Identity Services Engine (ISE) and Cisco ThousandEyes. 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 Secure Access
- Cisco SASE
- Cisco Identity Services Engine
- Cisco Duo
- Cisco User Protection Suite

Cisco's Universal ZTNA represents a transformative leap in secure network access, empowering organizations to embrace a truly universal approach to zero trust. Learn more at https://www.cisco.com/go/zta.

To register for a Universal ZTNA workshop, please visit: https://cloudsecurity.cisco.com/cisco-universal-ztna-workshop.

C45-4703612-01 03/25