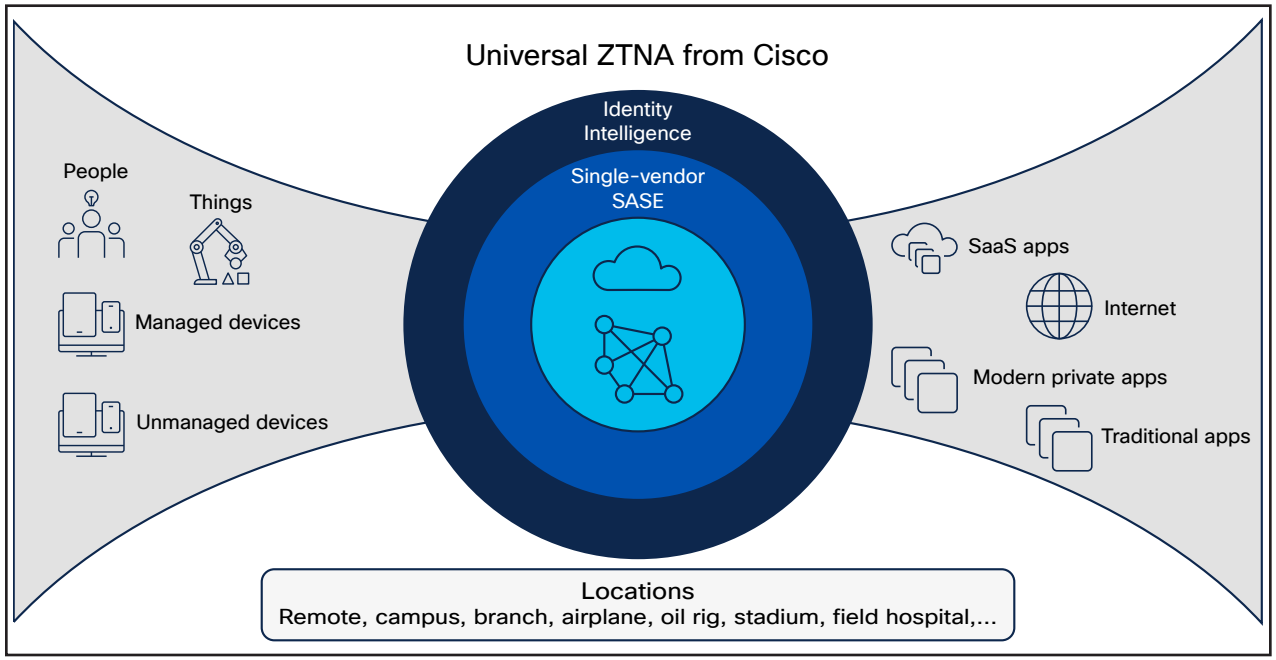
Zero Trust Everywhere: Cisco's Universal ZTNA

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. Cisco's Universal ZTNA redefines secure access for the modern era.

Benefits overview

Cisco's Universal ZTNA enables every user and device to securely connect to any application, anywhere, ensuring a consistent experience. The solution 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 protect critical assets. It supports flexible enforcement to safeguard sensitive data and meet governance objectives.



Universal ZTNA from Cisco: A day in the life

What does it mean to achieve Universal Zero Trust Network Access? It means securing every user–employees, contractors, partners–and every device, whether managed or unmanaged. It means protecting every application, modern or traditional, and covering every location, from oil rigs to airplanes, offices to homes.

For example, when a user or thing (e.g., IoT devices) attempts to access a resource, Universal ZTNA ensures that their (its) request is scrutinized through multiple layers of verification. This means authenticating user and device identities, assessing their security posture, and continuously monitoring and correlating activity – across the identity ecosystem - to detect threats that may require a change in access policy.

How it works: Key features

- **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 experience for users from any location, reducing risky workarounds and supporting secure AI usage.

After all, identity is at the heart of zero trust. Any Universal ZTNA solution in name must be able to use identity context to drive a dynamic access policy – and that includes the identities of things as well as users.

Key use cases: How to accelerate zero trust outcomes

Modernizing Application Access: Customers seek to consistently enforce least privilege access for all users and applications, regardless of location. Cisco's approach simplifies this with a unified solution supporting both legacy and next-gen apps, for a consistent experience everywhere.

Securing AI Access: Mitigate the risks associated with use of unauthorized AI applications by providing detailed visibility and control over Shadow AI– with guardrails for safety, security, privacy, and data protection.

Protecting Identities: Identity is central to zero trust. By integrating multi-factor authentication with identity intelligence, Cisco bridges the blind trust between authentication and access.

Extending Identity Context: Expanding identity context across IT and IoT devices allows for adaptive access policies that adjust to risks, ensuring a consistent experience across branch, campus, and home networks.

Building Operational Resilience: Cisco combines end-to-end visibility with a highly performant architecture, empowering organizations to confidently implement policy changes. This ensures high availability and reliable security connectivity in distributed environments.

Deploying a SASE Architecture: Choosing Cisco Secure Access and Catalyst SD-WAN for single vendor SASE creates consistent experiences for users and unified control for IT - zero trust that spans users, apps, devices, and networks. Everywhere.

Meeting Privacy Mandates: Cisco Secure Access simplifies compliance with privacy mandates by offering granular control over data storage and access. It allows organizations to enforce data governance policies across global environments, ensuring sensitive data is stored appropriately and securely, in compliance with regulations.

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.

Zero friction. Zero AI worries. Zero downtime.

Cisco's expertise in networking and security convergence uniquely positions it to deliver Universal ZTNA. As a leader in SD-WAN, NAC, and zero trust segmentation, Cisco offers a single policy, client, and adaptable architecture to meet customers where they are and take them where they need to go.

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 across remote, branch, and campus users from a single management tool - enhances user experience and eases compliance for highly sensitive applications.
- **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.
- **Policy assurance:** AI-driven policy validation using synthetic traffic reduces misconfigurations and prevents downtime.

C22-4715900-01 03/25