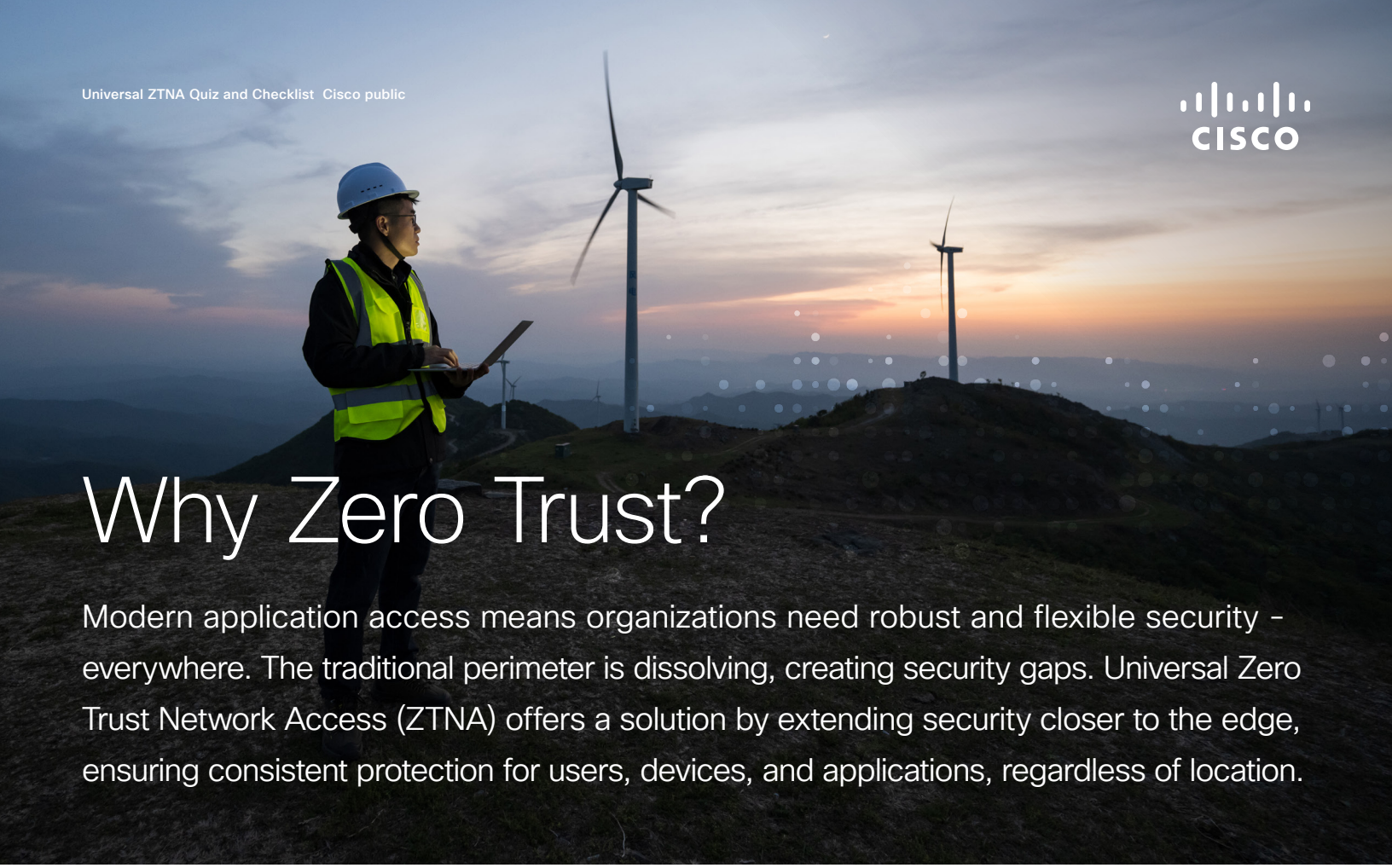

Why Zero Trust?

Modern application access means organizations need robust and flexible security – everywhere. The traditional perimeter is dissolving, creating security gaps. Universal Zero Trust Network Access (ZTNA) offers a solution by extending security closer to the edge, ensuring consistent protection for users, devices, and applications, regardless of location.

Is Traditional ZTNA Enough? Take this Quiz To Find Out

If any of the following items apply to your organization, you may need more than traditional ZTNA:

- ✓ We don't know how to start with ZTNA. My team is worried about the risks of using traditional VPN for access but is also afraid of disruptions from implementing cloud-based ZTNA.
- ✓ We struggle to maintain consistent security for our users working from remote, on-campus, and branch office locations.
- ✓ Our IT and security teams must manage separate access policies (across multiple platforms) for legacy VPN-dependent applications and modern ZTNA-aware apps, leading to inefficiencies and gaps in coverage.
- ✓ Contractors, partners, and BYOD users complicate security enforcement. Many of our solutions require agent-based models that are impractical for unmanaged devices.
- ✓ Misconfigured access policies have led to security gaps, outages, and compliance violations, placing a heavy burden on our IT team.
- ✓ Our IoT/OT devices are tough to manage and monitor since an agent-based approach won't work.
- ✓ When remote and mobile workers are in environments like airplanes, factories, and rural areas, they often face poor performance because traditional TCP/IP-based solutions falter.
- ✓ We can't keep sensitive app data from flowing through a cloud PoP while enforcing zero trust policies and providing a common, streamlined user experience.
- ✓ It's a struggle to get strong identity protection in place because of coverage gaps and user pushback about authentication friction.

Evolving to Universal ZTNA: A Ten-Step Checklist

Use this checklist to guide your organization toward Universal ZTNA:

1. **Identify connectivity challenges.** Recognize common issues such as reliance on VPNs, inconsistent security across locations, and latency due to POP-only architectures.
2. **Address security complexities.** Tackle siloed policies for legacy and modern apps, manage BYOD and unmanaged devices, and mitigate risks from misconfigured policies. Enhance IoT/OT support and strengthen identity security.
3. **Enable secure, reliable access.** Ensure every user, device, and application can connect securely from any location over any network. Focus on delivering low-latency access to enhance productivity.
4. **Assess identity posture.** Discover and evaluate your entire identity population including accounts that may be at risk or may pose a risk to your organization.
5. **Unify application support.** Support legacy VPN-dependent, modern ZTNA-aware, and SaaS applications with a single, multi-purpose client and policy engine.
6. **Enable agentless access.** Benefit from partnerships with Google Chrome Enterprise, Apple, and Samsung to support unmanaged devices and optimize the mobile experience.
7. **Leverage intelligent access decisions.** Use Cisco Identity Intelligence and Identity Services Engine for granular identity management and IoT/OT device security.
8. **Apply unified policy and flexible enforcement.** Implement unified policy with proactive policy assurance and flexible enforcement.
9. **Accelerate zero trust maturity.** Deliver consistent security across all users, devices, and locations with flexible adoption. Optimize security and performance, enforce least privilege controls, and manage third-party AI applications.
10. **Reap the benefits.** Increase user productivity with high-performance, consistent experiences. Control GenAI app usage and enforce data protection, accelerating zero trust maturity with a single-vendor solution.

Why Cisco for Universal ZTNA?

Cisco simplifies zero trust access and policy management with a single-vendor approach, accelerating your journey to zero trust maturity. Cisco redefines Universal ZTNA by using identity context to drive dynamic access policy for users and devices aka “things.” Cisco provides the tools needed to deploy and manage zero trust for the modern, hybrid workforce in a way that frustrates attackers and not users.

Summary

Universal ZTNA is crucial for modern security, addressing the limitations of traditional VPNs and ZTNA solutions. Cisco’s approach offers a comprehensive, integrated solution that enhances security, simplifies IT management, and improves the user experience.

Next steps

Download the full Universal ZTNA Handbook: Explore additional details about our Universal ZTNA solution.

Register for a Universal ZTNA Workshop: Work directly with a Cisco security specialist to see firsthand how Cisco’s Universal ZTNA is better for users, easier for IT, and safer for everyone.

Visit our Universal ZTNA Web Page: Learn more about Cisco’s Universal ZTNA solution and how it can accelerate your journey to zero trust.