CLOUDFLARE

Improve Security with Zero Trust Network Access (ZTNA)

Legacy 'castle-and-moat' defenses are broken. ZTNA represents a modern and more secure approach for organizations to ensure the right person accesses the right application in the right context.

ZTNA technologies redraw the perimeter not around the corporate data center, but around individual users, apps, and devices to isolate them from facing attacks and from spreading harm.

The corporate perimeter is broken | Traditional security assumes that everyone inside the network perimeter should be trusted by default. The fatal flaw here is that once inside the network 'moat,' attackers are privileged to go anywhere inside the 'castle.' Today, remote work is the norm, and users need access to corporate applications from dispersed locations and devices. With the perimeter shifting infinitely outward, we can no longer assume that "inside means trusted."

Re-envisioning security perimeters with ZTNA | ZTNA technologies eliminate distinctions in trust and privilege between being 'on' versus 'off' the network. Unlike common remote-working offerings like VPNs, ZTNAs follow best practices in two meaningful ways. (1) ZTNAs adhere to the "never trust, always verify" principle: All requests are assumed risky by default, and the ZTNA verifies each request based on identity, policy adherence, and other context before granting access to any applications or data. (2) ZTNAs follow the 'least privilege' principle by only providing what users need in the moment, thereby minimizing the spread of any undetected harm laterally across the organization.

Architecturally, ZTNAs isolate apps and users from direct exposure to the internet, hiding the connection through encryption. For these logic-based boundaries, ZTNAs are also known as software-defined perimeters (or SDPs).

ZTNA reduces an organization's attack surface, and, like a bouncer at a nightclub, requires proof of identity for every user before granting access to an application.

What you can do with ZTNA

ZTNAs strengthen security, improve user experiences, and enable business success.

Improve visibility across your network

By logging each access request, ZTNA enables transparency into how information moves through your business, so you can manage threats more proactively.

Lower the risk of breaches

ZTNAs continuously monitor activity to prevent bad actors from entering and reduce the potential for costly and reputation-damaging breaches.

Prevent malware from spreading

The virtual perimeters created around users, apps, and devices make it harder for malware to propagate laterally and wreak havoc across your network.

Enable user productivity

Users avoid working with clunky, slow VPNs. Instead, ZTNAs deliver a faster, more seamless experience consistent with the SaaS applications they use daily.

Simplify access administration across business scenarios

ZTNAs offer granular and flexible controls to support diverse scenarios – whether onboarding contractors or integrating a recently acquired company.

Accelerate your cloud migration

Everything is migrating to the cloud. ZTNA-as-a-service offerings enable a more scalable approach to support your users and customers already are.

Sample use cases

Starter use cases	Advanced use cases
Improve remote employee access to internal applications without constraints of a VPN	Extend access to an acquired business during M&A process
Secure application access for contractors and other 3rd parties	Control access privileges for diverse supply chain partners
Authenticate within DevOps workflows	Expand bring-your-own-device programs securely

Learn more about ZTNA and how Cloudflare for Teams can support your zero trust ambitions

Gartner's 2020 Market Guide for Zero Trust Network Access

Understand how to evaluate zero trust offerings and why 90% of Gartner clients are seeking ZTNA-as-a-service offerings, like Cloudflare for Teams.

Omdia Market Radar: Zero Trust Access

Industry analyst Omdia named Cloudflare as a leading provider of zero trust access.

Set up Zero Trust Access (and ditch your VPN) in less than 45 minutes

In this live demo, see how radically simple zero trust deployment and adoption can be with products like Cloudflare for Teams.

Guide to Securing Contractor Application Access

Learn about the IT challenges of working with freelancers, contractors, and partners and how ZTNA provides a simpler, more secure way to collaborate externally.