zscaler™

Next-Generation Zero Trust Network Access

The core tenets of next-generation ZTNA

Minimize the attack surface. Make applications invisible by establishing inside-out connections from application to user. IP addresses are never exposed to the internet, creating a "darknet" that is impossible to discover and exploit.

Eliminate lateral movement. Enforce least-privileged access by segmenting applications. Once a user is authorized, application access is granted on a one-to-one basis rather than full access to the network.

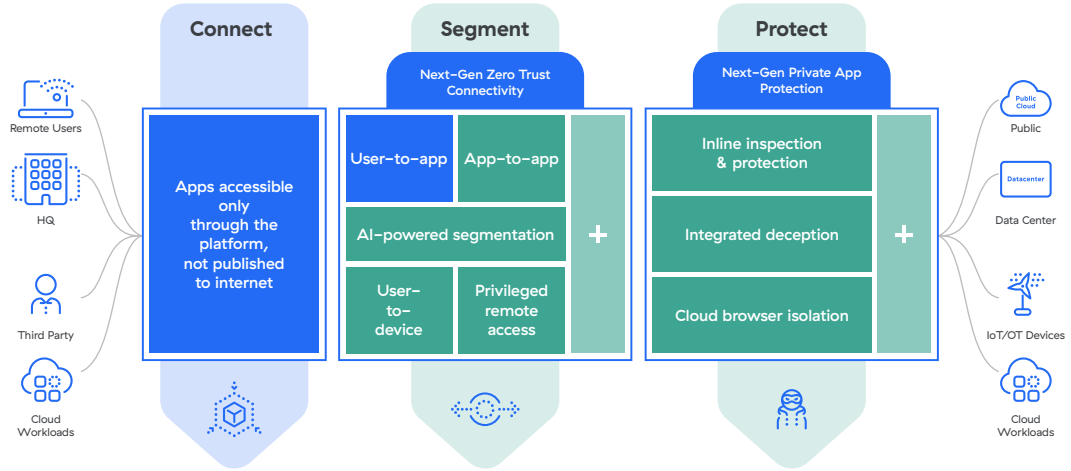
Stop compromised users and advanced attacks. Continuously monitor user and device behavior for abnormal activity with inline threat protections. Minimize the risk of active attacks and exploits targeted at applications.

The evolution of zero trust network access

With Zscaler Private Access™, Zscaler pioneered the first generation of zero trust network access (ZTNA) with a fundamentally different approach to application access. One that provides secure, flexible connectivity to private applications by hiding applications from the internet and connecting users directly to applications, not the corporate network, eliminating the need for remote access VPNs.

As organizations increasingly adopt zero trust to prevent breaches and enable secure hybrid work, ZTNA has evolved beyond its secure remote access roots to deliver a new generation of capabilities that protect against compromised users, detect the most sophisticated lateral movement attempts, and stop data loss. Built upon three core tenets, next-generation ZTNA connects, segments, and protects users, applications, workloads, and devices in a single, cloud-based platform.

Next-Generation ZTNA Capabilities



©2022 Zscaler, Inc. All rights reserved.

What is zero trust network access?

ZTNA is a set of technologies and functionalities that provide secure access to internal applications and eliminate excessive implicit trust inherent in other application access methods, such as legacy VPN. Like the software-defined perimeter (SDP) approach to controlling access, ZTNA creates secure, virtual boundaries between users and applications. Applications are made invisible and hidden from discovery, and least-privileged access is enforced by a trust broker that verifies identity, context, and policy.

By 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services, up from less than 10% at the end of 2021, according to Gartner.

Together, ZTNA, secure web gateway (SWG), and cloud access security broker (CASB) form the core technologies needed for a security service edge (SSE) platform that reduces risk, improves overall user experience, and replaces VPNs.

Learn more about next-gen ZTNA

Try our free 7-day test drive of Zscaler Private Access. This self-paced, online interactive demo lets you explore our zero trust service as both an admin and user.

Start Your 7-Day Test Drive →

Connect Minimize the attack surface	**Zero trust access** Hide or obfuscate all internal application IP addresses from the internet and remove all inbound connectivity for users and devices. Application access is brokered and orchestrated by the Zscaler Zero Trust Exchange™. **App discovery** Identify any unknown applications that your organization is using and who is accessing them so you can implement granular least-privileged access policies.
Segment Eliminate lateral movement	**AI-powered segmentation** Apply ML-based segmentation recommendations trained on millions of customer signals and application telemetry to minimize the internal attack surface. **User-to-app segmentation** Users are never connected to the internal network. Instead, they are connected directly to applications through a zero trust segment of one that creates a single microtunnel between the user and application. **App-to-app segmentation** Workloads in one public cloud securely communicate with another workload in any region of any cloud provider in hybrid and multi-cloud environments. **User-to-device segmentation** Securely connect remote workers and third parties to operational technology (OT) and industrial internet of things (IIoT) assets without bringing users directly onto the OT network. **Privileged remote access** Control privileged access to RDP and SSH systems with fully isolated remote desktop sessions that allow admins and third-party vendors to securely connect from unmanaged devices without the need for a client.
Protect Stop compromised users and advanced attackers	**Inline inspection and protection** Stop vulnerability-targeting attacks on private applications with inline detection and the blocking of malicious content embedded within user traffic. **Integrated deception** Deploy decoys and fake user paths throughout the environment for attackers to exploit without affecting business-critical applications. Any indicator of compromise cuts off access to private apps and shuts down active attackers in real time. **Integrated web isolation** Control sensitive data transmission to unmanaged devices by providing access to private applications through a secure isolated web browser.
Risk-based policy engine	Continuous validation of access based on the user's identity and on context, such as location, device, content, and application, minimizes trust granted.

zscaler™ | Experience your world, secured.™

Zscaler (NASDAQ: ZS) accelerates digital transformation so that customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange is the world's largest inline cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

©2022 Zscaler, Inc. All rights reserved. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, and ZPA™ are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com