The CISO's Guide: From VPN Replacement to Comprehensive ZTNA

How Zscaler Private Access (ZPA) ensures secure access from anywhere

WHITEPAPER

Table of Contents

SECTION 1

The Situation

Modern work can't be contained by perimeter-era security

Work no longer happens in a single office or on a single network. While this evolution has made companies more flexible and responsive, attackers have adapted more quickly than most security architectures, creating a gap between existing solutions and evolving threats.

As users, apps, and infrastructure continue to spread across offices, homes, clouds, and SaaS apps, traditional network-based controls simply can't keep pace. Today's enterprises need zero trust approaches that protect every connection—not just remote VPN users.

Distributed work isn't the only thing impacting the landscape. A 2024 IBM security report highlights a significant shift toward AI, indicating that cybersecurity may now be interdependent with AI capabilities, as noted by Wes Gyure, Executive Director of IBM Security Product Management.

Google confirms that adversaries are fully embracing AI, utilizing it not as an exception but a standard practice to make criminal operations faster and more effective. The use of agentic AI in particular creates a new class of threats that require approaches that are secure by design.

Threats are evolving rapidly in a distributed, AI-driven world

The security landscape has shifted from occasional, predictable events to continuous, fast-moving campaigns that target every gap in a hybrid enterprise. Attackers now blend traditional techniques with AI to automate reconnaissance, accelerate exploitation, and create highly convincing lures at scale. Security operations centers (SOCs) designed for a slower-paced world are trying to grapple with a new reality:

- **Threats are broader and more frequent**, spanning credential stuffing, phishing, ransomware, supply chain compromise, and exploitation of internet-exposed services.
- **Attackers are using AI** to generate and refine brute-force attacks, craft tailored phishing and vishing campaigns, and rapidly test new evasion techniques.
- **Attackers rapidly exploit vulnerabilities like zero days and misconfigurations**, giving them a short but powerful window to move laterally and exfiltrate data before defenses catch up.
- **Visibility gaps grow with hybrid work**, as users, devices, and apps operate across unmanaged networks and multiple clouds, making consistent enforcement difficult

> "Attackers will increasingly leverage AI for automated reconnaissance, intelligent password spraying, and rapid exploit development, allowing them to compromise VPNs at scale."
>
> **DEEPEN DESAI**
> CSO, Zscaler
> [Zscaler ThreatLabz 2025 Report]

Legacy VPNs and network-centric access are no match for today's needs

Traditional remote access solutions were designed for a small number of users connecting back to a central corporate network, not for the hybrid, app-centric, work-anywhere world. As organizations scaled remote and third-party access, they made do by layering on more VPNs and network controls. This patchwork approach brought some additional protections but also increased complexity, risk, and user frustration.

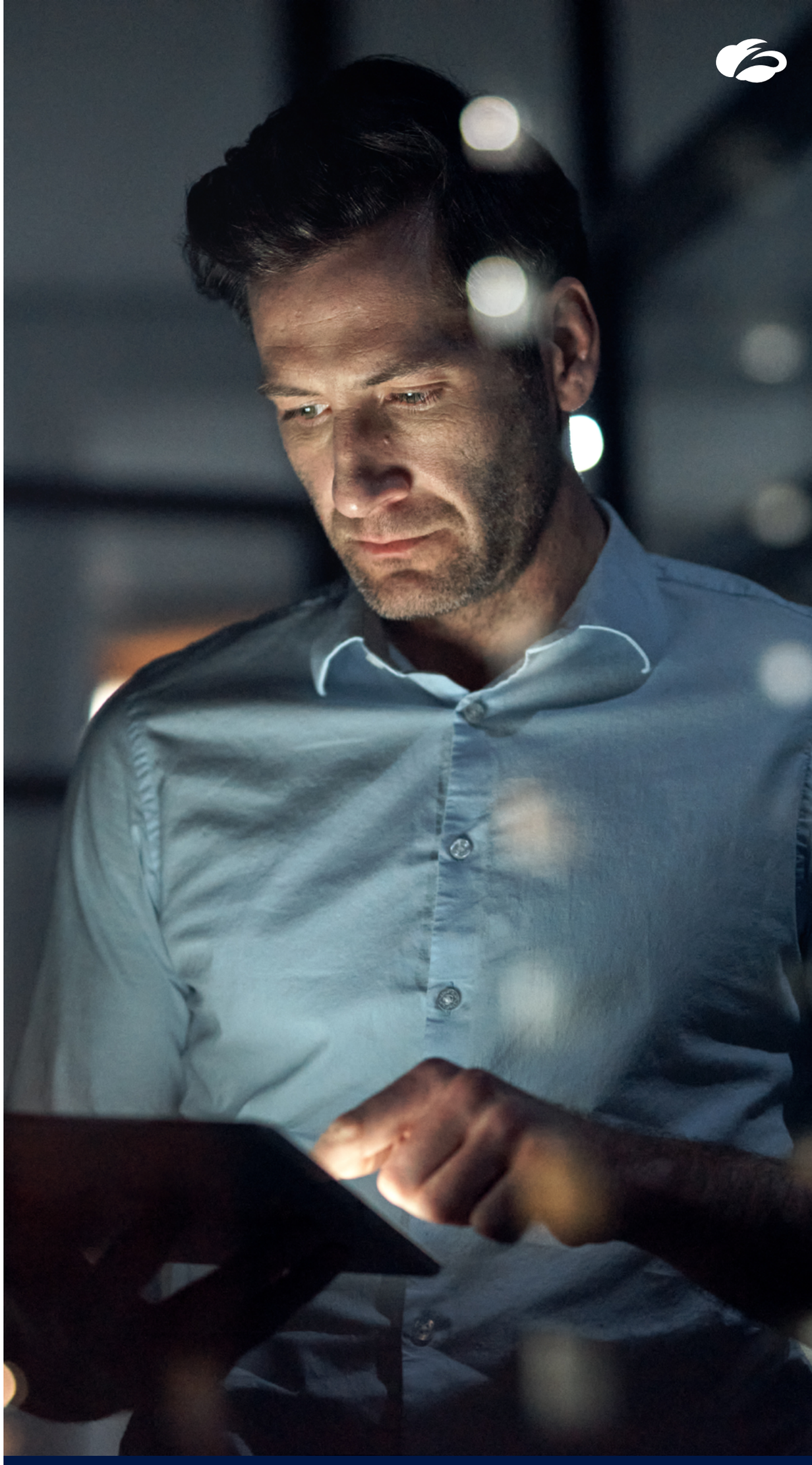
Today, the dangers and burdens of these legacy systems has never been more clear:

- **VPNs expose the network by design**, publishing gateways to the public internet and granting broad network-level access once users authenticate. This makes corporate assets discoverable by attackers, and continuously expands the overall attack surface.

- **Flat, IP-based access enables lateral movement**, allowing attackers to move from one compromised credential or device across multiple internal systems when segmentation is weak or inconsistent.

- **User experience suffers with backhauled traffic**, as VPNs route connections through central choke points, causing latency, congestion, and frequent drops when usage spikes. This is not only frustrating for end users, but can directly impact productivity and other business goals.

- **Operational overhead steadily increases**, with teams managing multiple VPN appliances, licenses, and policies, along with ongoing patching and troubleshooting for an aging access model. Overwhelm means important things inevitably get missed.



92% of 600+ IT and security professionals surveyed worry that unpatched VPN flaws directly lead to ransomware incidents, highlighting how difficult it is to continuously patch VPNs in time.

[Zscaler ThreatLabz 2025 VPN Risk Report]

A zero trust model for every user, everywhere

Hybrid work, aggressive threats, and fragmented infrastructure are exposing the limits of network-centric security. Security leaders need an access model that protects users and applications without slowing the business down—no matter where people work or where apps live.

In the zero trust model:

- **Security starts at the application**, not the network, so users reach only what they are explicitly allowed to use, instead of broad, flat environments.
- **Decisions are based on identity and context**, continuously evaluating user, device posture, location, and behavior rather than trusting anything just because it is on the network.
- **Direct, reliable access to applications is seamless**—from the office, at home, or on the road—without slow backhauling, frequent reauthentication, or clunky workarounds.
- **One unified way to manage access**, replacing fragmented policies and point solutions with a single, coherent model that spans data centers, multiple clouds, and SaaS for employees, contractors, and partners.

IBM suggests that identity is becoming the new security perimeter, forcing enterprises to continue their shift to an identity-first strategy:

> "When done right, this will be a welcome relief to security professionals, taming the chaos and risk caused by a proliferation of multi-cloud environments and scattered identity solutions."
>
> **WES GYURE**
> Executive Director, IBM Security Product Management

SECTION 2

The Zscaler Solution

Secure access for a distributed, AI-powered world

Zscaler Private Access™ (ZPA) takes a strategic approach to secure access by directly connecting authenticated users to specific applications, which minimizes the attack surface and ensures fast, consistent performance.

Organizations using ZPA experience a 55% reduction in the risk of breaches.

[The Total Economic Impact™ Of Zscaler Private Access (ZPA)]

Making direct connections to applications

What sets ZPA apart from traditional security models is the ability to establish direct, secure connections between users and applications—bypassing the network entirely. Because Zscaler never connects users to the network, attackers have far less access to it, creating a fundamental shift crucial for reducing vulnerabilities.

Our unique approach delivers a number of benefits for security teams:

- **Minimizing the attack surface significantly reduces infiltration risks** by preventing direct network access.
- **Focusing on least-privileged access effectively narrows user access** to only the applications necessary for their roles.
- **Creating direct connections to applications enhances user experiences** by ensuring faster access and improved performance.
- **Adapting the security posture keeps defenses strong and flexible** as ZPA continuously evaluates user context and device posture.

Extending ZPA for comprehensive coverage across the enterprise

While many organizations initially adopt ZPA as a VPN replacement for remote workers, its capabilities extend far beyond remote access. ZPA is a powerful solution that can secure users, workloads, and apps everywhere.

- **Streamlined secure access for branch locations** eliminates reliance on complicated legacy systems, simplifying connectivity for branch offices.
- **Enhanced security for third parties** allows contractors and partners to securely connect to necessary resources without exposing sensitive corporate networks.
- **AI-driven security framework for unified protection** uses Autonomous user-to-app segmentation and context-aware policies to establish a unified security posture that effectively meets diverse security needs.

SECTION 3

Beyond Remote Access

Expanding the potential of Zscaler Private Access

ZPA serves as a universal zero trust access platform that transforms security practices across the enterprise. Remote access should be the first use case, but not the only one.

Extending ZPA to users in every location

ZPA can provide a seamless experience for every user, no matter where they're located. The core principles of zero trust and least privilege access can be effectively applied throughout the organization.

- **Universal access for all users** means on-site employees, contractors, and partners can benefit from the same app-level, least-privilege access as remote users.
- **Common policies and controls** supported by autonomous, user-to-app segmentation ensure that security measures are consistent across the organization, simplifying management and compliance.
- **Decoupling access from physical networks** allows businesses to cover data centers, branch locations, and cloud applications under a single logical access plane.
- **Enhancing flexibility and efficiency** in operations enables organizations to better meet the demands of a dynamic work environment.

"Regardless of where users are, they're receiving the same exact security and policies that on-premises users have."

DAN HAN
CISO, Commonwealth University

Decommissioning legacy complexity

As organizations expand their ZPA deployments, they gain another benefit: the ability to simplify network designs and gradually retire outdated solutions. As a result, management and security operations become simpler, less obscure, and more effective.

- **Retiring legacy VPNs** reduces reliance on internal firewalls for segmentation and improves agility.
- **Simplifying network designs** becomes easier when routing user–to–app flows through ZPA rather than maintaining complex site–to–site VPN meshes.
- **Reducing operational overhead** decreases the number of licenses and appliances required, leading to cost savings and streamlined operations.
- **Migrating away from virtual desktop infrastructure (VDI)** improves the user experience on unmanaged devices and enables superior performance through secure agentless, browser–based access.

By embracing ZPA across the entire organization, companies can enhance their security posture, reduce complexity, and equip every user with fast, secure access to the resources they need.

SECTION 4

Why ZPA?

Secure, scalable, zero trust access

Zscaler Private Access provides advantages for both IT and security teams, as well as end users. It enables secure, seamless, and scalable zero trust access in on-premises, remote, or hybrid environments. By adopting ZPA, organizations enhance their security posture, improve user experiences, and streamline operations—all while improving agility and productivity.

Achieving zero trust segmentation at scale

ZPA empowers teams to implement effective zero trust segmentation, which plays a crucial role in reducing the attack surface and preventing lateral threat movement.

- **Minimizes the attack surface** by hiding private applications from direct discovery, which removes inbound connectivity and keeps the network invisible to the internet.
- **Automates app discovery and segmentation** through AI-powered features that help security teams catalog private applications and create granular user-to-app policies.
- **Prevents lateral movement** by ensuring that connections are made on a one-to-one basis so users are never connected to the network itself.
- **Reduces risks effectively** as threats are unable to breach the network due to the least-privileged access approach used by ZPA.

Enabling better user experiences

With ZPA, users gain fast, seamless access to the specific applications they need, which eliminates frustrating delays and improves overall satisfaction.

- **Offers direct connections** to the closest ZPA service edge before reaching the application, preventing latency caused by backhauling through central VPN gateways.
- **Delivers faster access** to applications through its extensive network of more than 160 globally distributed points of presence (PoPs).
- **Provides a consistent experience** for users whether they're in the office, at home, or on mobile devices, avoiding reliance on clunky solutions like VDI or RDP.
- **Secures user connections** without exposing internal systems to untrusted devices, thus reducing vulnerabilities associated with older remote access methods.

Simplifying Network / IT operations

ZPA streamlines operational complexities by centralizing policy enforcement and reducing the number of disparate tools that teams need to manage.

- **Consolidates security solutions** onto a single unified platform, allowing teams to simplify their infrastructure and reduce management overhead.
- **Implements consistent access** policies that are defined once based on identity, device posture, application, and risk, ensuring enforcement across all environments.
- **Enhances troubleshooting and incident response** with centralized logging and native integrations with SIEM and identity providers, easing the workload for network and security teams.
- **Reduces help desk tickets and outages** compared to traditional VPNs and firewalls, leading to a more efficient operational environment.

By addressing the vulnerabilities associated with conventional VPNs and delivering secure, seamless and scalable zero trust access, Zscaler enhances security, performance, and operational efficiency, making it an ideal solution for the modern enterprise.

"Zscaler fast-tracked our digital transformation, allowing us to modernize both our security infrastructure and our workplace, transforming the way we work daily...We are more productive, efficient, and secure than we have ever been."

STEPHEN BAILEY
Vice President of Information Technology,
Cache Creek Casino Resort

SECTION 5

Stronger Security, Stronger Business

Gain a competitive edge with ZPA

As ZPA enhances security and streamlines operations for organizations, it also strengthens their core business. A Forrester Total Economic Impact™ (TEI) Study found that ZPA delivers a return on investment (ROI) of 289%. Let's explore three ways ZPA gives businesses a competitive edge.

1. REDUCING ENTERPRISE RISK AND BREACH IMPACT

ZPA minimizes risks to the enterprise and lessens the impact of potential breaches.

- **By enforcing user-to-app segmentation and full content inspection**, ZPA effectively contains compromised accounts, limits the spread of ransomware, and safeguards sensitive data in transit.
- **Creating a secure environment fosters confidence**, minimizing the chances of reputation-damaging incidents that can disrupt operations.

2. SUPPORTING COMPLIANCE AND GOVERNANCE

ZPA is ideal for organizations looking to stay compliant while improving governance practices.

- **By implementing granular, identity-based access controls**, ZPA helps organizations align with frameworks like NIST's zero trust guidance and meet industry regulations that require least privilege and strong segmentation.
- **Enforcing consistent policies across various locations and environments** simplifies demonstrating control effectiveness to auditors and regulators, making compliance simple and straightforward.

3. ACCELERATING BUSINESS INITIATIVES

ZPA accelerates key business initiatives, supporting smoother transitions and faster processes.

- **Enabling faster onboarding of new users and systems** means security won't stand in the way of strategic programs like cloud migration or mergers and acquisitions.
- **Reducing operational complexity and minimizing access outages** allows IT and security teams to focus on higher-value transformation projects instead of getting bogged down in day-to-day challenges.

With ZPA, organizations can transform their security landscape while driving business growth, making Zscaler an essential ally in today's hybrid world.

> "Zscaler gives us full visibility into our environment, whereas before, we had less than 50% visibility."
>
> **RICK RINEWALT**
> CTO, Upland Software

SECTION 6

Additional ZPA Use Cases

More ways to use ZPA

The versatility of ZPA lets organizations enhance security and efficiency across all access points, streamlining operations in numerous areas with tailored solutions that meet specific needs.

In-office and on-premises access: Allow users on the corporate LAN to access data center and cloud applications with the same zero trust controls as remote users, eliminating outdated trusted network assumptions.

Third-party and contractor access: Enable secure, time-bound access for vendors, partners, and contractors without requiring VPN clients, exposing only specific applications through browser-based or isolated sessions.

Privileged admin and operations workflows: Provide secure, audited access to management interfaces, servers, and network devices without exposing RDP, SSH, or VNC to the internet, ensuring privileged access governance requirements are met.

BYOD/Unmanaged devices: Keep BYOD and unmanaged devices isolated from sensitive applications, protecting data from unauthorized actions like copying or downloading.

Merger and acquisition integrations: Grant acquired employees swift access to target applications without complex network integration, maintaining separate networks while providing unified, least-privileged access.

Modernizing data center and cloud app access: Replace jump hosts, bastion servers, and site-to-site VPNs with direct, policy-based access to applications in private and multicloud environments while continuously identifying new or shadow IT applications to bring under consistent zero trust policies.

"Zscaler AI-Powered App Segmentation enabled integration with [acquired company] Eldor 75% faster. In just days, BorgWarner engineers were collaborating with teams from Eldor."

MARK WILLIAMS
IT Director, Global Network Engineering, BorgWarner

SECTION 7

Wrap Up

Zero trust access everywhere, for everyone

Zscaler Private Access helps organizations make multiple improvements in a short time—enhancing their security posture, defending against evolving cyberthreats, and increasing operational efficiency. By shifting from network-centric to app-centric access models, Zscaler equips organizations to defend and grow in the fast-paced, hybrid landscape.

By extending ZPA beyond remote workers to encompass all users and key third parties, organizations can retire outdated VPNs, simplify their networks, and standardize on one zero trust access platform. In turn, they can strengthen their security posture, boost business resilience, and ensure better user experiences at scale.

Ultimately, consolidating legacy complexity into a unified foundation isn't just an upgrade; it's a strategic leap forward, paving the way for a more secure and agile future.

Take the ZPA product tour.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform 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 SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

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

zscaler™

Zero Trust Everywhere