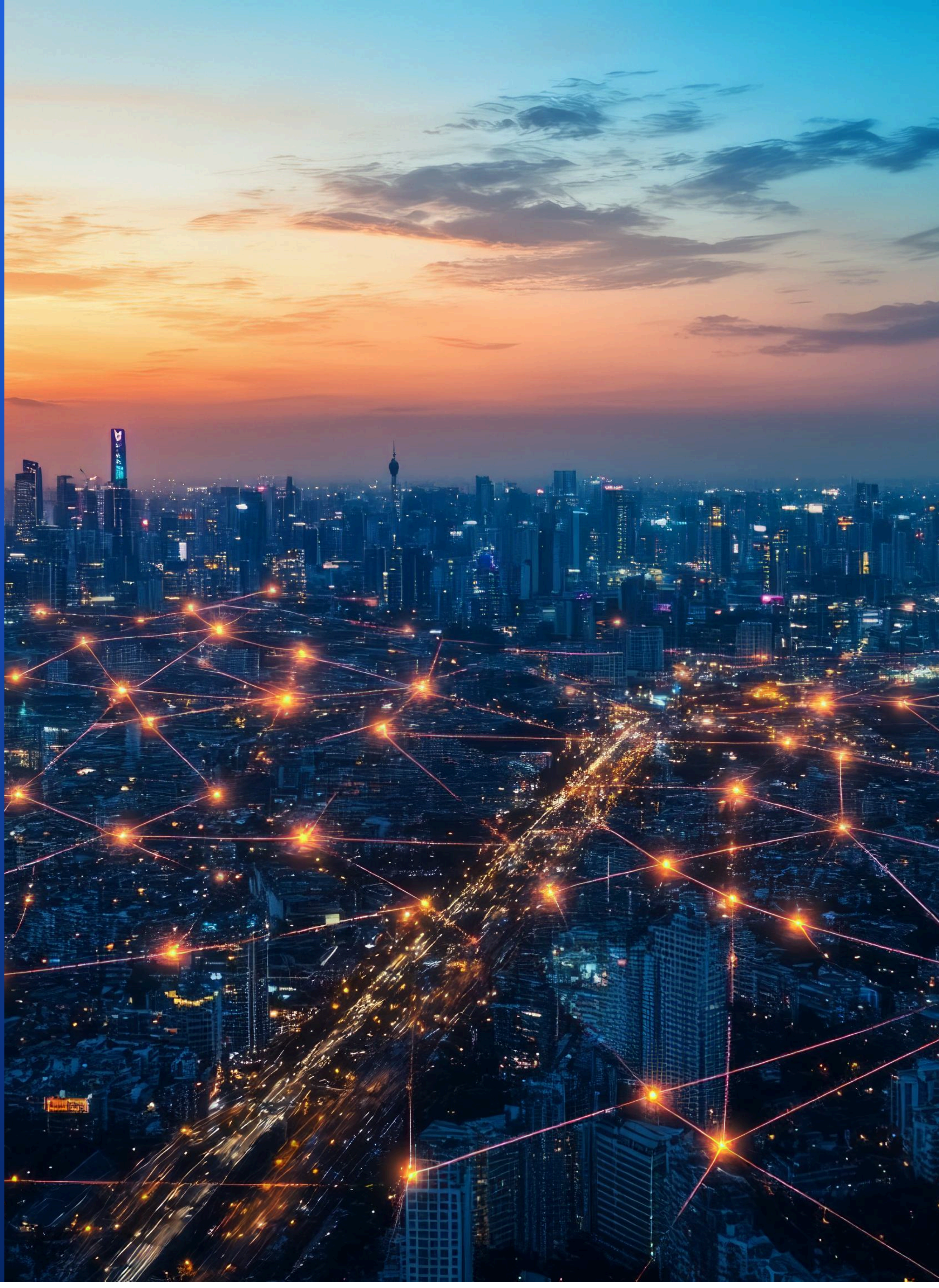
zscaler™

ZTNA: REDEFINING SECURE ACCESS FOR THE MODERN ERA



Zero Trust Network Access (ZTNA) is no longer optional—it is a critical necessity for secure application access. Legacy VPNs, originally designed for perimeter-based security, are no longer sufficient to meet the demands of modern IT environments. They create broad network access, increasing the risk of lateral movement, data breaches, and operational inefficiencies.

Cybersecurity and Infrastructure Security Agency (CISA) strongly recommends transitioning away from legacy solutions like VPNs, citing their inability to address modern security challenges and evolving threats. Embracing a zero trust architecture is crucial for organizations to secure access, protect data, and safeguard critical systems in today's dynamic environments.

ZTNA eliminates implicit trust, providing seamless, least-privileged access to applications without exposing the network. By adopting a zero trust model, organizations can reduce attack surfaces, enhance security, and improve operational efficiency.

VPN vulnerabilities continue to be a threat to app security

The Zscaler ThreatLabz 2025 VPN Risk Report found that 92% of the organizations expressed concerns about being targeted by ransomware due to unpatched VPN vulnerabilities.[1] VPNs were designed for perimeter-based security models that are now obsolete. Their broad network-level access enables attackers to infiltrate, move laterally, and exfiltrate sensitive data.

Key challenges:

1. Increased risk in security breaches

Once authenticated, users receive broad network access, increasing attack risks to infiltrate systems, spread across networks, and compromise sensitive data.

2. Operational shortcomings

VPNs route traffic through centralized networks, degrading SaaS and cloud app performance.

3. High IT effort

Managing legacy access solutions requires constant patching and troubleshooting, straining IT teams.

4. Increased costs

The infrastructure, licensing, and maintenance of outdated access methods are costly, and breaches lead to further financial loss and long-term reputational damage.

Complexities of securing access for all users

Providing secure access for diverse user groups in a hybrid and remote workforce presents significant challenges. Remote employees often struggle with performance and productivity issues when accessing private applications securely. BYOD and third-party users, such as contractors, partners, or vendors, require tailored access policies to protect private apps from potential vulnerabilities introduced by unmanaged devices or external entities. Unrestricted access granted to third-party users can lead to sensitive data exposure or security breaches. Additionally, users who need regular access to OT/IT assets face unique challenges in maintaining production uptime and avoiding disruptions caused by equipment or process failures, all while ensuring the security of critical systems. Balancing these diverse needs without compromising security requires a robust and adaptive approach.

[1] Zscaler ThreatLabz 2025 VPN Risk Report with Cybersecurity Insiders. https://www.zscaler.com/campaign/threatlabz-vpn-risk-report

93%

According to Zscaler ThreatLabz 2025 VPN Risk Report, 93% of organizations expressed apprehension about third parties serving as a potential backdoor into their network through VPN access.[1]

Top VPN vulnerabilities in 2024

Throughout 2024, major VPN vulnerabilities enabled attackers to access customer data, exploit stolen credentials, and infiltrate internal tools, prompting CISA to issue emergency directives.

WHAT HAPPENED?

Quarter 1–2024

Hackers used the stolen credentials of a former employee to breach a mobile tracking company's internal tools.

Quarter 2–2024

A known VPN vulnerability allowed attackers to infiltrate a U.S. ticket sales entertainment company and steal vast customer data.

Quarter 3–2024

At a global telecommunication company attackers exploited VPN vulnerabilities, accessing nearly all phone records of current and former customers.

WHAT'S THE IMPACT?

Expanded attack surface enabled lateral movement, exposing highly sensitive data.

Customer data is exfiltrated, leading to potential fraud, legal issues, and loss of trust.

Internal tools are weaponized, increasing the risk of further data breaches and reputation damage.

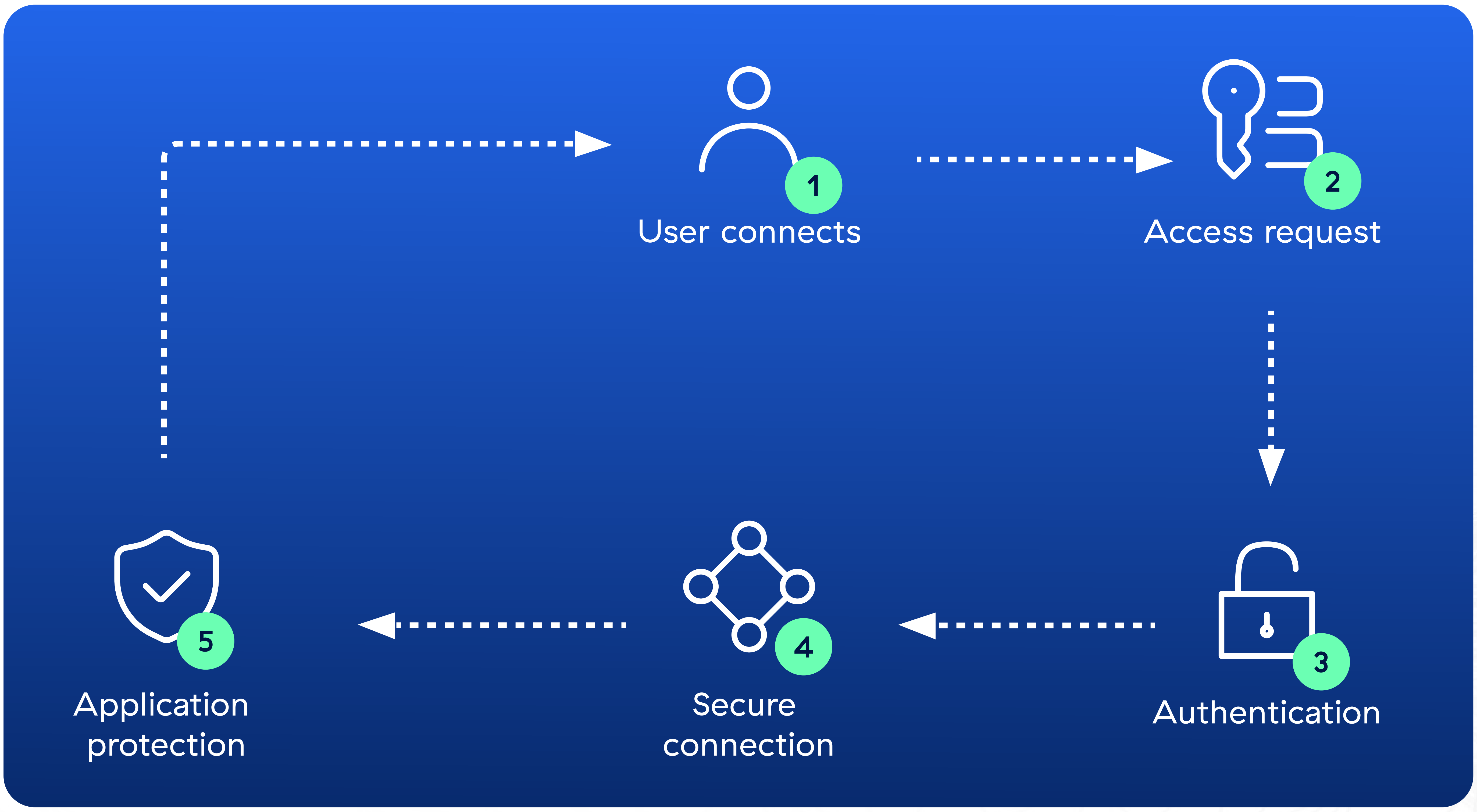
The shift towards zero trust: Securing modern access needs

Traditional access solutions fail to meet the needs of hybrid work, third-party access, and evolving threats. ZTNA eliminates broad, implicit trust by granting precise, need-based access and continuously verifying user trust. This ensures seamless, secure access while reducing the attack surface.

[1] Zscaler ThreatLabz 2025 VPN Risk Report with Cybersecurity Insiders. https://www.zscaler.com/campaign/threatlabz-vpn-risk-report

ZTNA in action

ZTNA continuously verifies identity, security posture, and context before granting access only to applications the user is authorized to access. By keeping applications hidden from unauthorized users, ZTNA eliminates attack vectors before they can be exploited.



ZTNA delivers:

- Low-latency, seamless application access for third-parties, contractors, and vendors regardless of their location
- Elimination of costly VPN infrastructure, reducing operational costs
- Simplified management with centralized policies and automation
- Scalable, secure access across hybrid and multi-cloud environments

70%

[We saved] approximately 70% on hardware, updates, and licensing costs versus our VPN system.[2]

Steffen Erler, Dir., IT Security and Network Services, Baker & Baker

[2] Baker & Baker Case Study. https://www.zscaler.com/customers/baker-baker

Why ZTNA fits the modern security landscape

Why ZTNA is trending

In a survey of over 2,200 IT and business leaders from large enterprises, almost half of respondents (46%) said that their organization was in the process of moving to a zero-trust model. Additionally, 43% reported already adopting zero-trust principles.[3] So, what's driving this massive shift?

1. Third-party access:

Secure, application-specific access for contractors, vendors, and external partners. ZTNA reduces exposure to risks by eliminating network-level access.

2. Browser-based access:

Clientless solutions simplify deployment and ensure secure access for unmanaged devices, supporting BYOD users and third parties.

3. Hybrid work models:

Traditional VPNs, designed for remote access only, fail to address the needs of in-office and hybrid employees. ZTNA bridges this gap, providing secure, scalable access to applications regardless of location.

ZTNA use cases

With zero trust solutions, organizations can ensure secure and seamless connectivity for any user from any location using any device. Here are some compelling use cases where ZTNA truly shines.

1. Remote workforce enablement

- Secure access to applications for employees working remotely without exposing the network to potential threats.
- Ensure consistent user experiences with low-latency connectivity, regardless of geographic location.

2. Hybrid workforce enablement

- Support employees transitioning between in-office and remote environments with seamless access to on-premise and cloud-based applications.

[3] Grand View Research. Zero Trust Security Market Size & Trends. https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

3. Third-party access

- Protect sensitive resources by granting granular, application-specific access to external contractors or vendors.
- Eliminate the risk of network-level access that VPNs traditionally expose.

4. BYOD (bring your own device) management

- Enable secure access from unmanaged personal devices without compromising the organization's security posture.
- Provide clientless, browser-based connectivity to avoid dependency on hardware.

5. Privileged access for IT admins and developers

- Enforce least-privilege policies for privileged remote access (PRA) users, ensuring administrators and developers only access what they need for critical tasks.
- Prevent lateral movement within the network, even in the event of compromised credentials.

6. Multi-cloud and SaaS security

- Ensure secure and scalable application access across multiple cloud platforms, including AWS, Azure, and Google Cloud, without requiring separate VPN setups for each environment.

7. Zero-day threat protection

- Mitigate risks from emerging threats targeting application vulnerabilities or misconfigurations.

Why organizations must act now

Urgency of ZTNA deployment

Leaving your systems exposed to outdated VPNs is like leaving your front door wide open for cybercriminals. There are just too many weaknesses that attackers are actively exploiting. By implementing zero trust principles now, you're not just patching holes. You're gaining a strategic advantage—an architecture that is both scalable and resilient and a robust defense against cyber threats.

Key considerations for deployment

Strategic implementation is crucial to ensuring a smooth transition and maximizing the benefits of ZTNA. As you plan your deployment, start with high-risk areas (remote access and third-party) and ensure alignment among stakeholders with broader zero trust strategies.

Focus on mission-critical tasks and implement ZTNA for the most sensitive and essential workloads to immediately mitigate risks and protect core business operations.

Zscaler Private Access: Taking ZTNA to the next level

Zscaler Private Access (ZPA) is a cloud-native solution that delivers zero trust access for all users with direct connectivity to private applications while minimizing the attack surface by hiding apps behind the Zero Trust Exchange™, eliminating lateral movement using AI-powered user-to-app segmentation, and protecting against sophisticated attacks with integrated traffic inspection, application and data protection.

Key use cases a robust ZTNA solution should address to ensure secure and seamless access in today's dynamic environments include:

01 **Secure remote work:**
Provides seamless, low-latency access to applications without exposing the network.

02 **Empower in-office and hybrid users:**
Supports employees transitioning between in-office and remote environments with seamless access to SaaS, on-premise, and cloud-based applications.

03 **Secure BYOD and third-party access:**
Enables granular, application-specific access for contractors, vendors, and unmanaged devices through clientless, browser-based connectivity, minimizing risk without requiring an agent.

04 **Privileged access management:**
Enforces least-privilege policies for IT administrators and developers to secure critical resources.

05 **Microsegmentation:**
Delivers user-to-app segmentation, simplifying policy deployment and eliminating lateral threat movement.

ZPA bridges zero trust strategies with real-world enterprise demands by providing:

- **Security:** Precise, dynamic access control through AI-powered segmentation minimizes the attack surface and prevents lateral movement, reducing the risk of breaches. It also protects against web and identity threats with private appprotection.
- **Scalability:** As a cloud-native platform, ZPA offers the scalability needed to support growing business demands without complex infrastructure.
- **Efficiency:** ZPA simplifies operations by consolidating security functions and centralizing policy management, reducing the need for multiple-point products and decreasing configuration complexity. Additionally, ZPA also accelerates the integration of network environments during an M&A from months to weeks.

ACCORDING TO A FORRESTER TEI STUDY OF ZSCALER PRIVATE ACCESS, CUSTOMERS REALIZED:[4]

Return on investment (ROI)

289%

Reduced IT and administrative burden

Up to

75%

Annual infrastructure cost savings

Up to

$1.75M

Reduction in risk of security breaches

55%

[4] The Forrester Total Economic Impact™ Study of Zscaler Private Access. https://www.zscaler.com/campaign/forrester-tei-zscaler-private-access-report

Conclusion: ZTNA is the foundation for secure, modern access

The modern workplace is complex, with remote and in-office employees, third-party users, and evolving cyber threats. Traditional access solutions can no longer keep up. Organizations require a security model that meets today's demands while anticipating future challenges.

ZTNA represents a fundamental shift in security—one that ensures scalable, resilient, and secure access for modern workforces. As part of Zscaler Zero Trust Exchange™, ZPA is a cloud-native solution that extends fast, secure, and reliable private app access for all users from any device or location. From secure healthcare access to streamlined financial workflows and protected IoT connectivity in manufacturing, ZPA is the backbone of secure, modern access.

↗ Take the next step toward a more secure, agile, and resilient future. Learn more about ZPA and schedule a zero trust demo.

Forrester Consulting interviewed customers and combined the results into a single composite organization to understand the 3-year total economic impact of replacing VPNs with ZPA.

"The Total Economic Impact™ Of Zscaler Private Access (ZPA)," December 2024 a commissioned study conducted by Forrester Consulting on behalf of Zscaler.

zscaler™ | Experience your world, secured.™

About Zscaler 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. To learn more, visit www.zscaler.com.

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

zscaler.com