Enterprise Strategy Group™ by TechTarget

WHITE PAPER

Making Sense of a Quickly Evolving ZTNA Market

By John Grady, Principal Analyst
Enterprise Strategy Group

February 2023

Contents

Executive Summary

Enterprise environments are fundamentally different than they were just a few years ago, and providing consistent, secure application access across a range of users and devices is a key responsibility for security teams. VPNs were not designed with the modern enterprise in mind, so the use of zero trust network access (ZTNA) tools has increased dramatically as security teams seek to revamp their secure access model. To date, this has been focused mostly on remote access, which misses the broader shift toward comprehensive zero trust architectures. To support this more comprehensive approach, ZTNA tools should provide universal coverage, secure application segmentation, and advanced security. Zscaler Private Access delivers these capabilities and helps security teams reduce their attack surface, minimize lateral movement, and ensure a consistent user experience across the environment.

Zero trust network access tools should provide universal coverage, secure application segmentation, and advanced security.

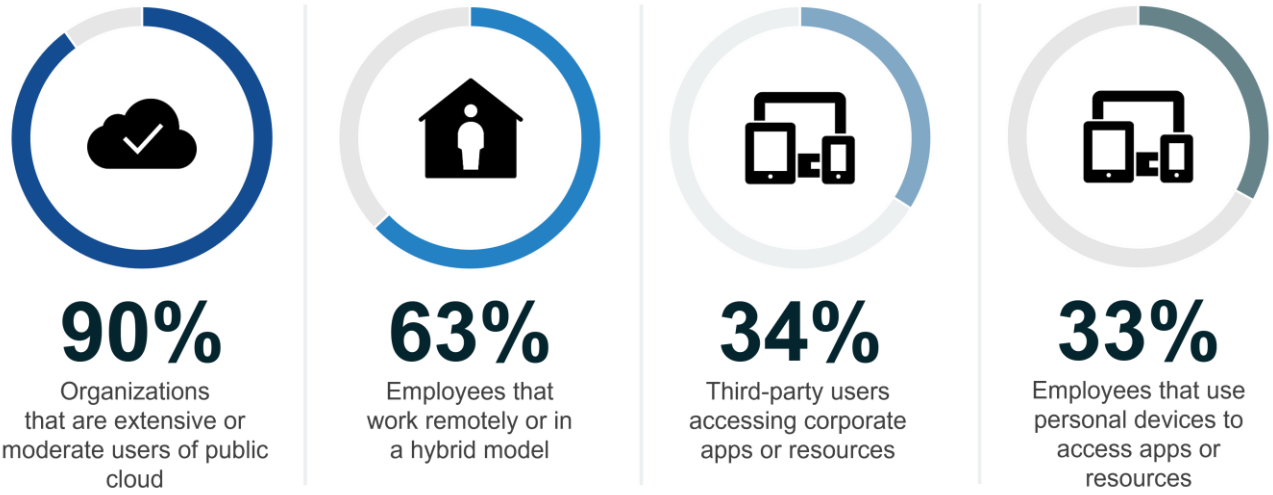
Improving Secure Access for Today's Enterprise

Many organizations have squeezed a decade's worth of digital transformation into the last two years. The use of cloud, nature of work, and role of applications have all evolved at an exceptionally rapid pace (see Figure 1).[1] Specifically:

- The migration of resources to the cloud has been occurring for years, but the need to improve agility and resiliency has accelerated this transition, with research from TechTarget's Enterprise Strategy Group (ESG) finding that 94% of organizations are now extensive or moderate users of public cloud services.
- At the same time, the users accessing those resources are more distributed and diverse than ever. The shift to remote work is well known, but this has gradually given way to a hybrid model in which employees work from a corporate office on a regular basis at least one day per week. According to ESG research, 63% of employees now work either remotely or in a hybrid manner.
- Further complicating this picture is the prevalence of third parties and unmanaged devices in the corporate IT ecosystem. The need to connect contractors, partners, suppliers, affiliates, and other third parties to corporate resources has increased as applications have become central to a variety of business processes. This trend is directly connected to the use of unmanaged, personal devices, which extends to employees as well. ESG research has found that 34% of the users accessing corporate applications or resources are third parties, with one-third of employees using personal devices.

[1] Source: Enterprise Strategy Group Complete Survey Results, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, December 2021.

Figure 1. The Changing Enterprise IT Ecosystem



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Traditional Remote Access Models Fall Short

These changes demand that secure access models be modernized. Historically, cybersecurity strategies have been predicated on a well-defined, static perimeter where everything inside is considered trusted and everything outside untrusted. VPNs have typically been the tool of choice to connect users outside of corporate locations back to the corporate network in order to access applications and other resources. However, VPNs come with three main drawbacks, namely:

1. **Weak security.** VPNs provide broad access to the network and offer no inherent security features. This prevents security teams from centrally limiting what users are able to do once they connect. Additionally, VPNs are often subject to vulnerabilities that attackers exploit to gain entry and launch an attack on the broader environment.
2. **Poor user experience.** With applications and users now more likely to be outside of the perimeter than within, the practice of backhauling traffic to on-premises locations only to be routed back to the cloud no longer makes sense and often introduces latency, which can impact application performance. Further, requiring users to manually decide whether a policy requires them to connect to a VPN and, if so, decide which gateway they should use can be burdensome and further negates the user experience.
3. **Little scalability.** VPNs are typically deployed as appliances, which take effort to install and have a defined ceiling for capacity. This means that if usage requirements change, new appliances must be deployed, costing an organization both time and money. The need for agents also prevents organizations from providing access to third parties in a simple, straightforward manner.

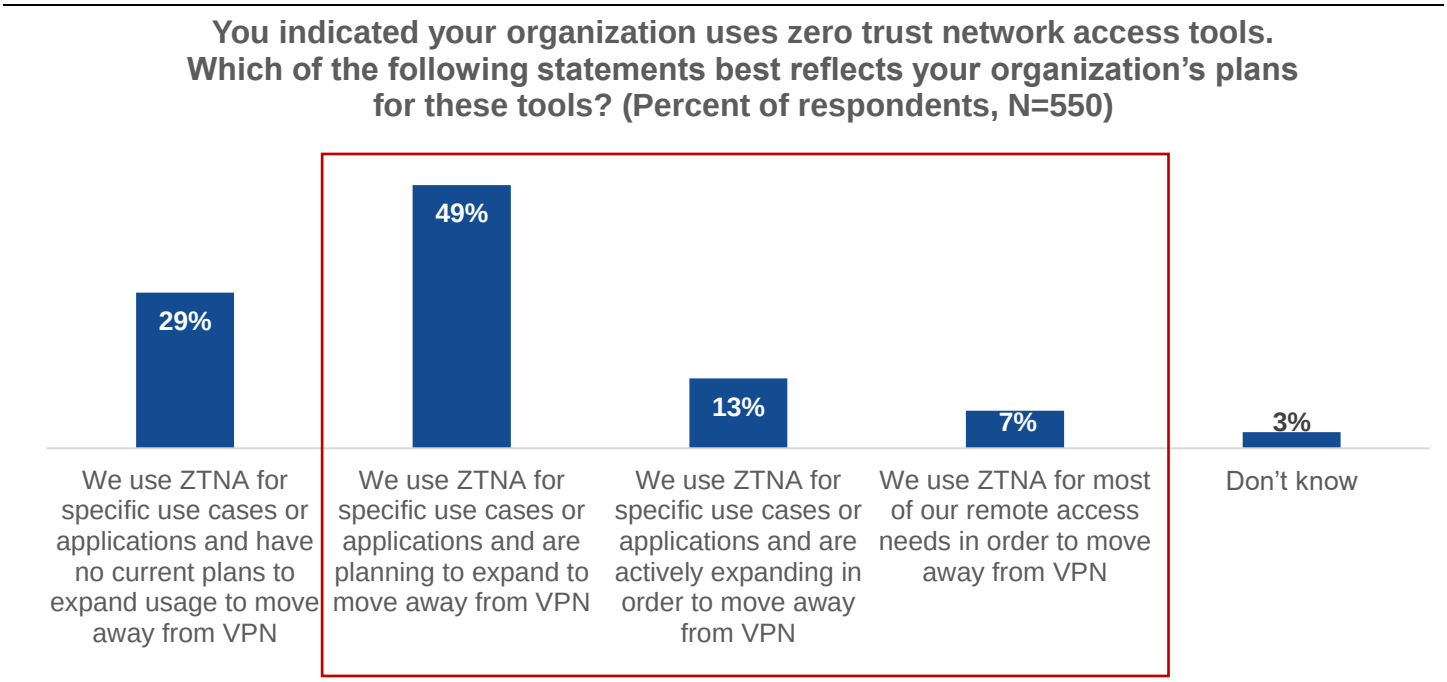
ZTNA Emerges as a VPN Replacement

ZTNA solutions have garnered immense interest in the market to specifically address these issues. ZTNA tools create an identity- and context-based logical access boundary around an application or set of applications, hiding them from public view and restricting access to a set of named entities via a trust broker.

69% of organizations are moving forward with, or are interested in, replacing their VPNs with ZTNA tools.

As the name denotes, these tools support zero trust tenets by enforcing least privilege policies and incorporating additional context, such as the location of the user, time of day, or device type and posture, into the decision to determine whether to allow or block a connection. Agentless options provide flexibility to support specific use cases such as BYOD and third-party access, and the fact that ZTNA is typically cloud-delivered helps improve scalability and agility. As a result, Enterprise Strategy Group research has found that 69% of organizations are moving forward with, or are interested in, replacing their VPNs with ZTNA tools (see Figure 2).[2]

Figure 2. Interest in VPN Replacement Is Strong



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Next Evolution of ZTNA

Yet, while most ZTNA tools provide clear and distinct advantages over legacy VPNs, not all address the challenges security teams face in comprehensively securing access to and protecting applications in modern distributed environments. In fact, Enterprise Strategy Group research has found that, while 41% of organizations said enabling secure remote access for employees and third parties was a top driver for their zero trust initiative, more than half

[2] Ibid.

(51%) pointed to a broader modernization of their cybersecurity program as the impetus for such a project.[3] Ultimately, tools supporting this broader type of approach require a more substantial set of features and capabilities compared to those focused solely on the remote access use case.

Ultimately, tools supporting a broader zero trust approach require a more substantial set of features and capabilities compared to those focused solely on the remote access use case.

To date, ZTNA has been overly focused on remote access and web applications. While this was a clear pain point in the early days of ZTNA, the shift from fully remote to hybrid work requires a more unified model that provides consistency regardless of where the user is connecting from. While cloud-only tools were ideal for connecting remote users to applications either in the cloud or on-premises, they introduce a sort of inverse backhauling model when users in offices have to access on-premises resources and are routed through the cloud to do so. Also, while web applications have become pervasive, many organizations support access to resources over RDP, SSH, or other protocols. Furthermore, the convergence of IT and OT systems, combined with the increased use of connected devices in industrial environments, has introduced another access vector security teams must account for.

An additional consideration is the protection of the application itself. ZTNA took a significant step forward in protecting applications when compared to VPN, but it often fails to holistically address the issue. For example, it is common for ZTNA solutions to establish a connection between a user and application and then step out of the way rather than continuing to scan the traffic for security threats. This can open the door for attackers or malicious insiders to upload malware or otherwise exploit the application. From a segmentation perspective, most ZTNA tools provide basic separation to support least privilege policies and ensure users only have access to resources they are entitled to. However, when legitimate users are compromised, this does not prevent attackers from moving laterally and accessing other resources the impacted user has access to.

Key Requirements for ZTNA Tools Moving Forward

To overcome these issues, ZTNA must take major steps forward to more comprehensively support a zero trust access model, reduce enterprise risk, and deliver continuous, effective security. With this in mind, security teams should look for ZTNA tools that provide universal coverage, secure application segmentation, and advanced security.

Universal Coverage

Security teams now require "ZTNA Anywhere" for both remote and in-office workers. To support this, solutions must be cloud-centric, but not cloud-only. While a globally distributed, highly performant network is absolutely foundational for ZTNA, tools should also provide on-premises "private edge" options to avoid having to route traffic to the cloud in order to secure access between office users and data center applications. Supporting this fact, Enterprise Strategy Group research has found that 31% of research respondents say coverage for cloud and on-premises environments is one of the most important attributes for technologies supporting zero trust.[4]

Additionally, tools should provide connectivity for a variety of access scenarios to help organizations move beyond simply replacing their VPN. This includes support for:

- Providing straightforward, agentless access for remote employees, third parties, and BYOD users.

[3] Source: Enterprise Strategy Group Research Report, *The State of Zero-trust Security Strategies*, April 2021.
[4] Ibid.

- Controlling access to resources for privileged IT users.
- Extending ZTNA to industrial IoT and OT environments for internal and third-party users.

Together, these aspects form the concept of universal ZTNA, which can help organizations secure access across a variety of locations and scenarios, and plays a key part in creating a positive and consistent user and management experience. Users are able to natively access the application or resource without having to connect to specific gateways. Traffic to cloud applications is routed directly through the closest, most logical PoP, with redundant options available in nearby proximity, while on-premises traffic remains on-premises. Finally, administrators are able to centrally define policies one time and then consistently apply them throughout the environment.

Secure Application Segmentation

By definition, ZTNA tools help protect applications by removing the need to expose them to the internet and establishing brokered, one-to-one connections between resources and users. Many ZTNA tools do support these concepts on some level to reduce the attack surface.

However, ZTNA tools should go further and extend segmentation mechanisms across workloads and devices to more effectively prevent lateral movement of threats inside a cloud or data center environment. As a result of digital transformation, modern environments are dynamic and constantly expanding their digital estates outside their traditional borders. ZTNA tools that automatically discover applications and provide risk-based policy recommendations can help minimize lateral movement. In fact, Enterprise Strategy Group research has found that, when asked for the most important capabilities in tools supporting zero trust, 29% of organizations cited risk assessment capabilities, while 25% mentioned the automation of policy creation or management.[5]

Advanced Security

Secure access and ZTNA should not be operated in a silo and must be part of a larger, integrated platform focused on protecting distributed users and applications. Specifically, this means being part of a broader secure access service edge (SASE) or security service edge (SSE) platform. For many, ZTNA is not just a part, but a foundational aspect, of these architectures, with 58% of Enterprise Strategy Group (ESG) research respondents that have begun to implement SASE indicating that ZTNA was a starting point for their project.[6]

58% of Enterprise Strategy Group (ESG) research respondents that have begun to implement SASE indicate that ZTNA was a starting point for their project.

As part of this approach, continuous security inspection to detect threats and sensitive data loss is needed. Attackers often utilize stolen credentials to gain initial access and move laterally, making it critical for ZTNA tools to remain in line of traffic and continuously monitor the session at the application level to identify signs of malicious activity. Tools that operate at the network level can have difficulty controlling lateral or east/west movement. Conversely, ZTNA acts as a shield between private applications and compromised users and inspects entity to resource traffic to mitigate common types of application attacks, such as cross-site scripting, remote code execution, and SQL injection.

Data protection is also a key component of SASE and SSE, and thus, it is an important consideration for ZTNA. ESG research has found that 38% of organizations say that incorporating more data-centric security policies will be an initial SASE use case.[7] ZTNA tools that incorporate browser isolation technology can help organizations secure access to corporate applications and data from unmanaged devices to address third-party and BYOD access

[5] Ibid.
[6] Source: Enterprise Strategy Group Complete Survey Results, *2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased*, December 2021.
[7] Ibid.

scenarios. Agentless approaches (both browser and portal-based) are typically used to minimize user friction, but secure browser isolation is necessary to prevent risky devices from infecting internal applications and networks. By allowing only isolated access in a secured environment separate from the device and network, the user (if actually an attacker) is prevented from directly connecting or interacting with the application, and thus cannot upload malware to the application or download data to an untrusted device or location.

Zero Trust Benefits

While most organizations would prefer stronger security, only some are willing to sacrifice user productivity to do so. In fact, one of the misconceptions about zero trust is that it can adversely impact the user experience or productivity. But in reality, more than one-third (36%) of those organizations that have moved forward with a zero trust initiative have reported better employee productivity thanks to zero trust. Even more tellingly, 77% of Enterprise Strategy Group research respondents that have begun a zero trust initiative have seen at least one security benefit (such as reducing the number of incidents, improving SOC efficiency, simplifying compliance, and reducing the number of data breaches) *and* one business benefit (becoming more agile, becoming more adaptive, increasing employee productivity, user satisfaction, and reducing security costs).[8] By using ZTNA tools that meet the requirements discussed above, security teams can help expand their organization's zero trust strategy and deliver these benefits to their company.

77% of Enterprise Strategy Group research respondents that have begun a zero trust initiative have seen at least one security and business benefit.

Figure 3. Benefits Seen from Zero Trust Adoption

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

[8] Source: Enterprise Strategy Group Survey Results, *The State of Zero Trust Security Strategies*, May 2021.

Zscaler Private Access Delivers Universal ZTNA

Zscaler was among the first security companies to recognize the need for cloud-delivered security services and has helped push the industry in this direction over the last decade. Zscaler Private Access is the vendor's ZTNA solution and is a cloud-native service built on a holistic SSE platform. The solution delivers universal zero trust connectivity for hybrid workforces, secure zero trust segmentation, and inline threat and data protection to help security teams reduce their attack surface; minimize the lateral movement of threats, and ensure users have consistent and performant access to the resources they need to be productive.

Zscaler Private Access is optimized to provide the same access experience for remote and in-office workers. It offers clientless access for users to connect to not only web applications, but other private applications, workloads, and IoT/OT devices as well. In a standard deployment, most users would connect through Zscaler's Public Service Edges, which are full-featured private application access brokers that manage connections, enforce policies, and provide integrated security. Public Service Edges are hosted by Zscaler in more than 150 globally distributed edge locations to ensure the shortest path between users and their destination, minimize latency, and provide a strong user experience.

Private Service Edges provide similar connections as Public Service Edges but are hosted locally by the customer in their data center. This deployment model allows seamless zero trust controls on-premises, which is useful to reduce application latency when the application and user are in the same location or when sessions need to be controlled within regions or sites. This option also provides a layer of business continuity if a catastrophic event takes place that disrupts internet connectivity and shuts down access to critical applications.

Zscaler Private Access provides advanced connectivity, segmentation, and security capabilities. Specifically:

- **Universal connectivity** with unified client and clientless access methods to address a wide range of scenarios including remote work, on-campus access, third-party users, and BYOD.
- **Zero trust segmentation** provides granular control of user-to-app, user-to-device, and workload-to-workload communications to minimize the lateral spread of an attack. Application discovery automatically identifies internal applications as they are used and helps security teams define their attack surface and go on to create more granular access control policies. AI/ML segmentation automatically recommends application segments to simplify policy building and minimize lateral movement. The solution extends segmentation even further and applies zero trust more broadly to application workloads across cloud environments with Zscaler Private Access for Workloads.
- **AppProtection** provides high-performance, inline inspection of the application payload to identify threats and block known application security risks such as the OWASP Top 10 and emerging zero-day vulnerabilities. Typically, these types of web application firewall (WAF) capabilities have been deployed in front of public, customer facing applications, which leaves private applications unprotected. By embedding application protection directly in its ZTNA solution, Zscaler helps organizations prevent the disruption of critical applications that are core to the enterprise.
- **Browser Isolation** provides air-gapped, clientless access to applications for employees and third parties using BYOD, ensuring unmanaged endpoints with vulnerabilities or malware infections do not compromise the network or applications. It addresses more sophisticated use cases that require data exfiltration controls for clipboard sharing, printing, uploads, and downloads. This further helps to mitigate cyber-attacks and data leaks and provides a level of security few ZTNA tools can offer.
- **Privileged Remote Access** provides employees and third parties who administer or operate internal systems and equipment with secure, privileged access by establishing privileged sessions using protocols such as RDP, SSH, and VNC. This provides a higher level of control, reducing the attack surface of privileged users and mitigating the risk of escalation.

- **Deception** is perhaps the most innovative aspect of Zscaler Private Access. By deploying decoy applications, deception identifies lateral movement and can shut down access to internal resources before attackers are ever able to access them. One of the benefits of this deception approach is the nearly unquestionable degree of confidence with which the technology identifies malicious actors.

Ultimately, Zscaler Private Access seeks to provide a better user experience that "just works." Access is continuous regardless of changes to network connectivity and is consistently fast whether remote or in office. Integrated digital experience monitoring (DEM) provides visibility into performance across the environment to help administrators quickly identify whether performance issues are related to network connectivity, application performance, the user device, or other factors, reducing calls to the help desk and network teams.

Conclusion

ZTNA is a good example of a technology that benefited from a perfect storm of multiple market conditions. While the security deficiencies of VPNs had been known for years, the overnight shift to remote work during the pandemic cast a spotlight on the scalability inadequacies as well. By providing stronger security and flexibility through the cloud, ZTNA offered organizations a VPN alternative that had not been available before.

Fast forward to today, and the ZTNA market is quickly evolving and the number of vendors offering ZTNA capabilities is continually increasing. ZTNA also addresses a much broader set of use cases than VPN replacement for remote work: secure access for users on-campus, third-party access and BYOD, privileged users, active threats, and overall security transformation are all examples where ZTNA can significantly move the needle. But only if the solution has the right capabilities.

As a result, the industry must move beyond the phase of contrasting these tools against past approaches and begin comparing ZTNA solutions against one another to assess which solutions are best equipped to support broader security transformation initiatives and expanding use cases over time. This requires:

- Universal coverage to help organizations secure access across a variety of locations and scenarios and ensure a positive and consistent user and management experience.
- Secure application segmentation to more effectively prevent the lateral movement of threats inside a cloud or data center environment.
- Advanced security inclusive of application protection, data protection, and isolation to continuously inspect traffic and prevent threats and data leakage.

ZTNA has something to offer organizations of all types, sizes, and stages of digital maturation. Across the board, ZTNA provides better scalability, security, and performance compared to traditional VPN approaches. However, by considering a solution that offers these capabilities such as Zscaler Private Access, security teams better protect and support their organizations both now and in the future.

About Enterprise Strategy Group
Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community. © TechTarget 2023.

contact@esg-global.com
www.esg-global.com