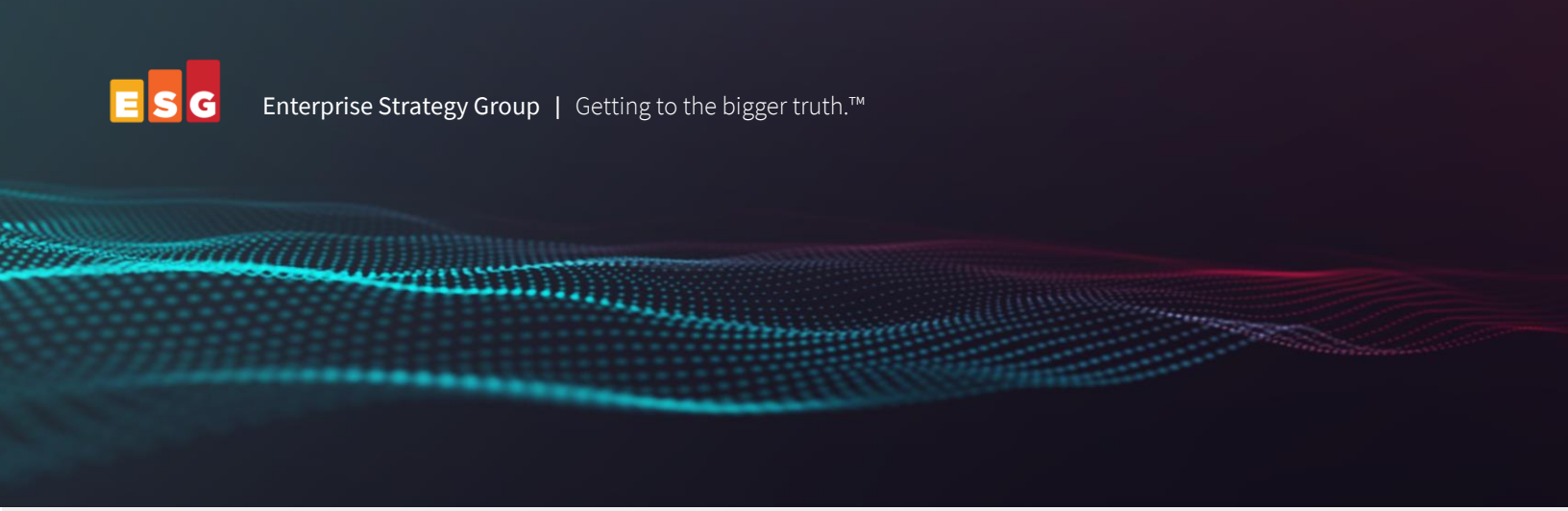


ESG WHITE PAPER

Ten Considerations for Evaluating Zero Trust Network Access Solutions

By John Grady, ESG Senior Analyst

August 2021

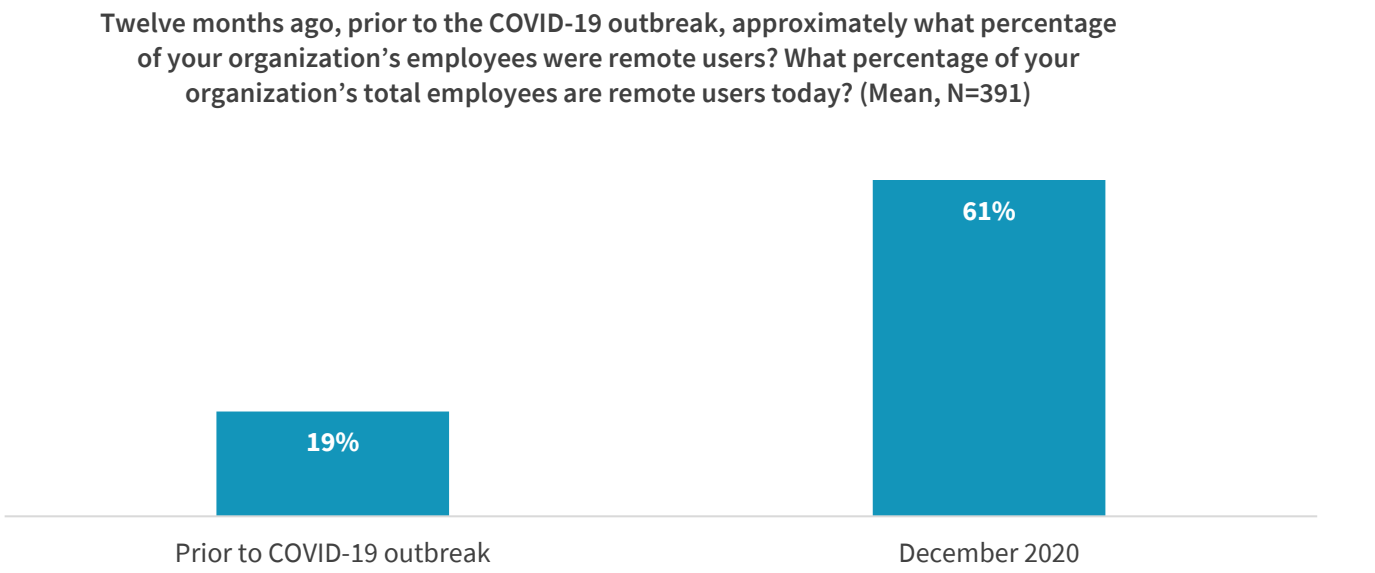
This ESG White Paper was commissioned by Palo Alto Networks and is distributed under license from ESG.

Contents

The Changing Nature of Remote Access

Even before the pandemic, the lines between office and home life had begun to blur. In 2019, ESG research found that employees spent an average of six hours per week doing work-related tasks outside of office hours, with 68% of respondents indicating that this occurred multiple times per week.[1] Most commonly, this involved something simple, such as checking email, though some employees regularly worked outside of the office, necessitating remote access to corporate applications and resources. However, the scale of this dynamic fundamentally changed due to the COVID-19 pandemic. In fact, ESG research has found that an average of 61% of employees now work remotely, more than three times the number prior to the pandemic (see Figure 1).[2]

Figure 1. Average Percentage of Remote Workers

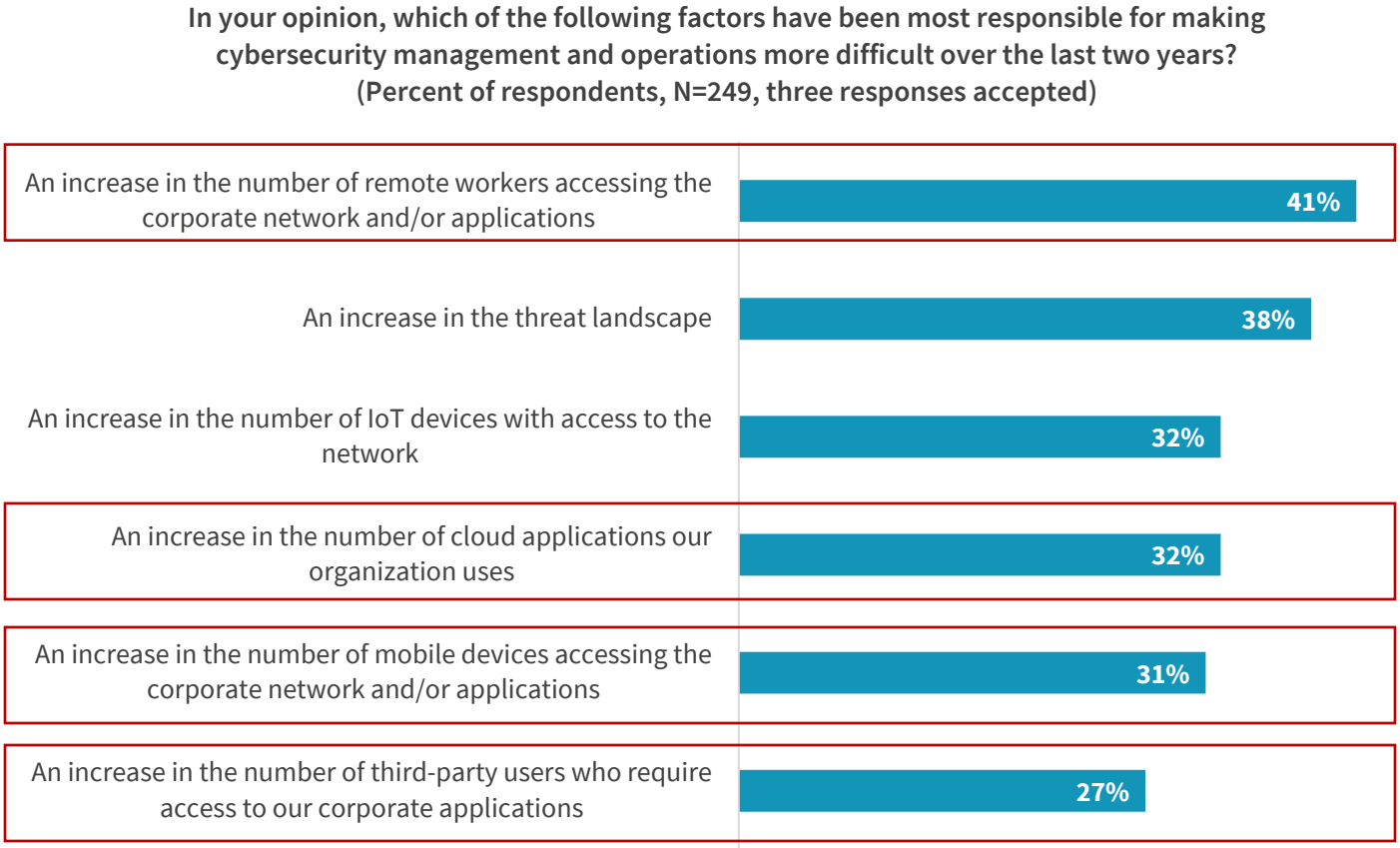


Source: Enterprise Strategy Group

These trends are critically important, as the exodus of employees from corporate locations coupled with the increasing use of cloud-based resources are among the biggest drivers of cybersecurity complexity today. Overall, 59% of ESG research respondents indicate that cybersecurity is more difficult today than it was just two years ago. Historically, the changing threat landscape, both in terms of volume and complexity, has been the most common driver of these difficulties. However, a staggering 41% of respondents indicated that the increase in remote workers was among the factors most responsible for making cybersecurity and management more difficult over the last two years. Further, four of the top six reasons are directly related to securing user access to corporate resources, including the number of cloud applications supported, the number of devices used, and the necessity of providing third-party access (see Figure 2).

[1] Source: ESG Research Report, *2019 Digital Work Survey,* December 2019.
[2] Source: ESG Master Survey Results, *The State of Zero Trust Security Strategies,* May 2021. All ESG research references and charts in this white paper have been taken from this master survey results set, unless otherwise indicated.

Figure 2. Top Six Reasons Cybersecurity Has Become More Difficult



Source: Enterprise Strategy Group

Where Legacy Approaches Fall Short and the Shift to Zero Trust Network Access

Historically, organizations have provided users with remote access to corporate resources by connecting them to the broader enterprise network. This has often been accomplished through VPNs, with ESG research finding that 67% of organizations currently use VPNs to provide access to remote users. This model typically requires an endpoint agent on the user's device and a VPN appliance on the corporate network.

When most applications resided inside a data center and only a handful of users were accessing enterprise resources remotely and from corporate-owned devices, this approach was somewhat manageable, if not ideal. However, the inversion of the access model, with both users and applications now residing outside of traditional corporate locations coupled with device sprawl, has made this approach untenable. Some of the specific limitations of a VPN approach to remote access in this new model include:

- Poor security. VPNs are visible on the public internet. When vulnerabilities in these tools are discovered, this visibility is used by attackers to gain entry into the corporate network. Further, VPNs connect users to the network rather than specific applications, allowing users to have broader visibility and access to corporate resources than they should otherwise have. Compromised credentials provide an attacker with access to an entire swath of resources, enabling reconnaissance and lateral movement. Finally, VPN encryption cloaks malicious insider and outside behavior from most security inspection, allowing an attacker to remain undetected for an extended period of time.

- Lack of scalability. Because VPNs are typically deployed as appliances, increasing capacity can be difficult. This issue was highlighted during the pandemic when organizations with networks architected to support a workforce that was minimally remote had to acquire, provision, and configure additional hardware appliances to support a work-from-home model. Further, the need for VPN agents on endpoints complicates certain remote access use cases, including employee-owned devices, third-party access, and mergers and acquisitions.
- Siloed management. Remote access VPNs are typically deployed as siloed tools, requiring dedicated policy management. Further, they only support broad, network-level visibility rather than application- or user-based reporting. Both these issues have only been highlighted as security tool sprawl continues to increase and granular visibility is increasingly required to understand what is happening on the network.

Enter Zero Trust Network Access

As enterprise architectures have become more distributed, interest in zero trust strategies has exploded. However, confusion with regard to zero trust has risen even as the term has become ubiquitous. Zero trust should be viewed as a strategy or framework on which a security program can be built.

It relies on technology but is more oriented toward weaving principles, such as never inherently trusting a connection, least-privilege, and continuous assessment, throughout an organization's security policies. Yet one of the clearest areas where the concept of zero trust strategies overlaps directly into technology is with zero trust network access (ZTNA).

ZTNA, sometimes called software-defined perimeter, facilitates one-to-one connections between users and applications, isolating application access from the broader network using least-privilege principles and continually assessing the trustworthiness of the connection. Users can only see the applications and services they are explicitly allowed to access, preventing malicious insiders or compromised accounts from being used for reconnaissance and lateral movement. Additionally, applications are hidden from the public internet, preventing attackers from exploiting corporate resources. ZTNA solutions are often delivered via the cloud, providing scalability as users are added. And while many ZTNA solutions require agents, some support an agentless model, making them better served to provide secure access to third parties.

Based on the inclusion of least-privilege and continuous assessment, it should come as no surprise that many organizations find ZTNA highly effective in supporting zero trust strategies. In fact, 29% of ESG research respondents indicated that zero trust network access is the most effective tool at supporting a zero trust initiative, the highest percentage provided by respondents for any tool.

Key Zero Trust Principles:

Never trust, always verify: Historically, security has been predicated on a defined perimeter to delineate the trusted (anything inside) versus the untrusted (everything outside). Zero trust strategies aim to remove the assumption of trust based on location, identity, or any other criteria and ensure that all entities and connections are thoroughly validated and authenticated.

Least-privilege: The principle of least-privilege states that users, applications, and devices should only be given the minimal level of access required to perform their job or function. Least-privilege is a critical component of zero trust strategies to ensure that lateral movement is limited in the event of a breach.

Continuous assessment: In addition to incorporating strong authentication mechanisms to validate the initial level of trust, zero trust strategies require the ongoing monitoring of device health, user activity, data access, and a variety of other factors. This ensures that if the risk level of the user, application, or device changes, appropriate action can be taken.

This has impacted how organizations are considering deploying ZTNA in their environments, which has evolved over the last 18 months. Initially, ZTNA deployments would focus on specific use cases: enabling secure access to only cloud applications, providing contractors access to corporate applications, or supporting merger and acquisition strategies. However, today, many organizations are looking at ZTNA with an eye toward full VPN replacement. While the initial deployment is still typically for a targeted use case, there are often more formal plans from the outset to expand usage quickly and reduce the reliance on VPN. Specifically, ESG research has found that 51% of organizations surveyed are using or plan to use ZTNA for the full-scale replacement of existing remote access VPN solutions within the next two years.[3]

ZTNA is often targeted toward a specific use case such as enabling secure access to cloud applications, providing contractors access to corporate applications, or supporting mergers and acquisitions. Yet increasingly, there are formal plans to quickly broaden ZTNA usage and shift away from VPN.

RFP Checklist: Ten Things Organizations Should Look for When Considering ZTNA Solutions

As organizations move forward with long-term planning to ensure application-focused, secure access for a highly distributed workforce and application environment, IT leaders should add the following items to their RFP checklist.

Zero trust network access solutions should:

1. Focus on least-privilege and zero trust. While it may seem as though all tools positioned as zero trust network access would inherently support zero trust principles, including least-privilege, that is not always the case. ZTNA is not simply moving VPN to the cloud, but fundamentally changing the way users remotely access corporate resources. ZTNA tools must take a default deny posture and ensure access is provided only to a specific application or resource and not the broader network segment. Further, this access should not be granted until proper authentication has occurred. Additionally, authentication should be based on a variety of factors, including identity, device, and deeper context of the request, such as time and geolocation.

2. Continuously assess and monitor connections. Just as importantly, even after the initial connection is initiated, the session should be continually assessed. If the risk level changes due to the health of the device or activity of the user, the session may need to be reauthorized, the level of access may be reduced (to read-only for example), or the connection may be terminated.

3. Provide granular visibility and reporting. ZTNA solutions facilitating access on an application-by-application basis provide a deeper level of visibility than traditional VPN solutions. Rather than reporting on IP addresses and higher-level network access, ZTNA solutions should report on groups and users as well as the specific applications they are accessing. This enables administrators to investigate issues and troubleshoot problems much more quickly and efficiently.

4. Support both agent-based and agentless deployments. An agent-based ZTNA approach is required for access to some types of applications and for better visibility into the health and posture of the user's device prior to authenticating. Yet agentless models can provide an attractive alternative to support third-party access and

[3] Source: ESG Master Survey Results, *Transitioning Network Security Controls to the Cloud.* July 2020.

prevent agent sprawl in cases where that may be a concern. The flexibility to support both models allows organizations to expand ZTNA deployments to additional use cases over time.

5. Enable access to different types of applications. Many applications are shifting to the cloud, yet a number continue to remain in on-premises data centers for one reason or another. Similarly, many applications are web-based, but others rely on SSH, RDP, or other non-web protocols. ZTNA solutions should provide access across a variety of different application locations and types. When combined with the support for both agent and agentless approaches, broad application coverage can provide organizations a path towards full VPN replacement.

6. Be built on a scalable and reliable platform. ZTNA solutions delivered via the cloud require a global infrastructure to ensure minimal latency for users accessing corporate resources. One of the key issues with VPN is the need to backhaul traffic to a central point, which can affect performance and negatively impact the user experience and productivity. If ZTNA traffic must be routed to data centers in other countries or regions, only to circle back to the region of origin, the same issues can occur. With application access as critical to business productivity as it is today, a global distributed infrastructure to ensure minimal latency and provide redundancy, coupled with service level agreements (SLA) guaranteeing at least five nines uptime, is critical to ensure users can quickly access the resources they require to do their jobs at all times.

7. Include a broad ecosystem of identity integrations. Many organizations now use a variety of identity providers across their on-premises and cloud environments. This creates complexity, but consolidating providers is often not possible. As a result, ZTNA solutions should offer integrations with a wide range of identity vendors to simplify deployment and help reduce complexity.

8. Ensure consistent user experiences. Today, security solutions must not only protect but also enable the business. Solutions must be easy for users to navigate and not impact their productivity. With many organizations planning for a shift toward hybrid work, ensuring consistency for users wherever they are and whatever resource they are accessing is critical. There may be small differences based on the type of the device being used or additional authentication mechanisms depending on the level of risk. However, the core method of how users access the applications they use to do their jobs should not deviate widely based on where they are.

9. Incorporate integrations with broader zero trust or SASE platforms. The goal of ZTNA is to prevent attacks from occurring by limiting access. Yet the reality is that threats can and do slip through. So, while ZTNA may be undertaken as a standalone project, it is increasingly part of a broader initiative to incorporate additional context and capabilities through the integration with threat prevention and DLP tools. This is often accomplished through secure access service edge (SASE). SASE architectures converge a variety of security and network capabilities in a cloud-delivered model to provide centralized management and consistent, distributed enforcement for users regardless of location. While SASE is a broad initiative incorporating a long list of capabilities, ZTNA has quickly become a critical component of the architecture. By including ZTNA in a SASE architecture, organizations can limit their threat surface, prevent threats that do bypass defenses from compromising systems, and ensure that attempts to exfiltrate data by attackers or malicious insiders are prevented.

10. Provide a consistent management experience. Similarly, security teams are too often overworked and understaffed. Finding solutions that support organizational efficiency to overcome these issues and ensure consistent security by avoiding human error is critical. This requires more than just functional integrations to support broader zero trust and SASE approaches, but a common management experience so that access rules are consistently applied with administrators having to replicate policies.

Palo Alto Networks' Prisma Access: Cloud-delivered Zero Trust Network Access

Palo Alto Networks delivers zero trust network access as part of its Prisma Access cloud-delivered security platform, which also includes firewall-as-a-service (FWaaS), cloud access security broker (CASB), secure web gateway (SWG), threat prevention, and other capabilities. Prisma Access integrates with Prisma SD-WAN to comprise Palo Alto's complete SASE solution. Through its Prisma Access platform, Palo Alto Networks provides a scalable zero trust network access solution that supports zero trust initiatives and offers a simple, unified management experience.

Scalability

Prisma Access is built on the combined infrastructure of Google Cloud Platform and Amazon Web Services, including Google's private global network. With more than 100 global points of presence, this network provides a scalable, resilient platform with 99.999% uptime and under 10 millisecond latency. Additionally, Prisma access supports both agent-based and agentless models. Organizations can use Palo Alto's GlobalProtect agent to establish an encrypted IPSec tunnel as well as collect information on the operating system, patch state, firewall status, and security software running on the device. Alternatively, an agentless approach can be supported through an SSL/TLS-enabled web browser.

Simple, Unified Management

As part of Prisma Access, ZTNA can be managed through one of two unified portals. Panorama is Palo Alto's on-premises option for centralized management of the vendor's next-generation firewalls, as well as Prisma Access. Alternatively, Prisma Access Cloud Management provides a cloud-based option for Prisma Access Management, helping to streamline configuration management, onboarding, and reporting.

Additionally, Prisma Access integrates with all major directory and identity stores, including Active Directory, Kerberos, LDAP, Okta, and OneLogin, among others. By synchronizing across these different providers and incorporating device and location context, Prisma Access can enforce different levels of authentication depending on the perceived risk of the connection. By leveraging user telemetry and AI/ML models, Prisma Access can automatically enforce risk-based access control, adapting user access before identity stores are even updated. For users connecting via the agentless approach, identity can be validated via CaptivePortal, client probing, MFA request, or NAC.

True Zero Trust

Prisma Access uses a default to deny posture and post-connect threat monitoring as part of its zero trust network access approach. Prisma Access decrypts and scans incoming traffic before authenticating and (if properly authenticated) re-encrypts and connects the user to the correct application or service. Traffic is scanned for threats using traditional anti-malware and intrusion prevention technologies, file execution through its WildFire malware analysis engine, and AI/ML-based detection to detect signatureless attacks and protect against zero day exploits. Data loss prevention can also be added through an additional license to scan traffic for signs of data exfiltration. All this scanning occurs both at the initial time of connection, and through the session, providing continuous protection and assessment.

The Bigger Truth

The pervasiveness of remote work, coupled with the increasing use of applications by not only employees, but third parties as well, have highlighted the shortcomings of traditional secure remote access solutions such as VPN. Many organizations have shifted from viewing the lack of scalability and inherently poor security offered by VPNs as simply an inconvenience to a critical issue they must address. As a result, ZTNA has quickly risen from an emerging, use-case-driven deployment to a core component of security modernization plans and zero trust initiatives.

Due to this, organizations exploring ZTNA tools should consider not only the standalone capabilities offered, but how the solution fits into and supports a broader SASE and zero trust platform. Palo Alto Networks' zero trust network access capabilities, offered through its Prisma Access platform, provide organizations a scalable, resilient solution that supports tactical remote access needs in the short term and a strategic approach to SASE over time through its native integrations with a broad set of security capabilities.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.


www.esg-global.com


contact@esg-global.com


508.482.0188