RESEARCH
Influence and insight
through social media

July 2022

Hybrid Work Drives the Need for ZTNA 2.0

WHITE PAPER

Prepared by
Zeus Kerravala

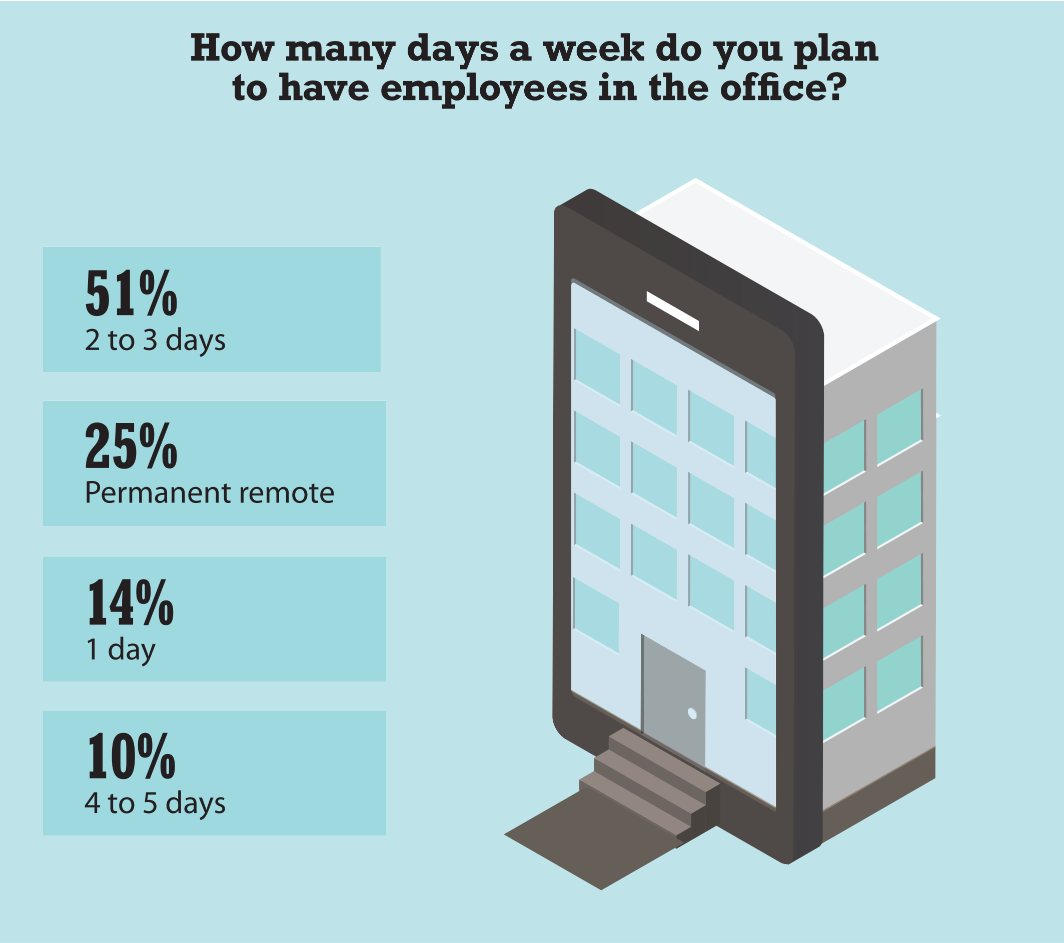
ZK Research
A Division of
Kerravala Consulting

INTRODUCTION: HYBRID WORK IS NOW THE NORM

The COVID-19 pandemic has had a profound effect on the world. Businesses have compressed into months digitization plans that they had envisioned would take years. Employees who had been tied to one location can now work from anywhere (WFA), and that trend will persist for the foreseeable future. Results from the ZK Research 2022 Work-from-Anywhere Study show that while only 22% of employees regularly worked remotely before the pandemic, 51% will work from home two to three days per week, and another 14% will do so one day per week (Exhibit 1). This indicates that the future of work is hybrid.

In addition, many companies don't expect to have employees back in the office full time ever again. Salesforce's president and chief people officer, Brent Hyder, told MarketWatch that the company will revamp its offices to eliminate a "sea of desks" and expects that 65% of its 54,000 employees will come into the office only one to three days per week (up from 40% pre-pandemic). Other companies, such as Microsoft and Google, are also embracing the hybrid work trend.

Exhibit 1: The Future of Work Is Hybrid



ZK Research 2022 Work-from-Anywhere Study

ABOUT THE AUTHOR

Zeus Kerravala is the founder and principal analyst with ZK Research. Kerravala provides tactical advice and strategic guidance to help his clients in both the current business climate and the long term. He delivers research and insight to the following constituents: end-user IT and network managers; vendors of IT hardware, software and services; and members of the financial community looking to invest in the companies that he covers.

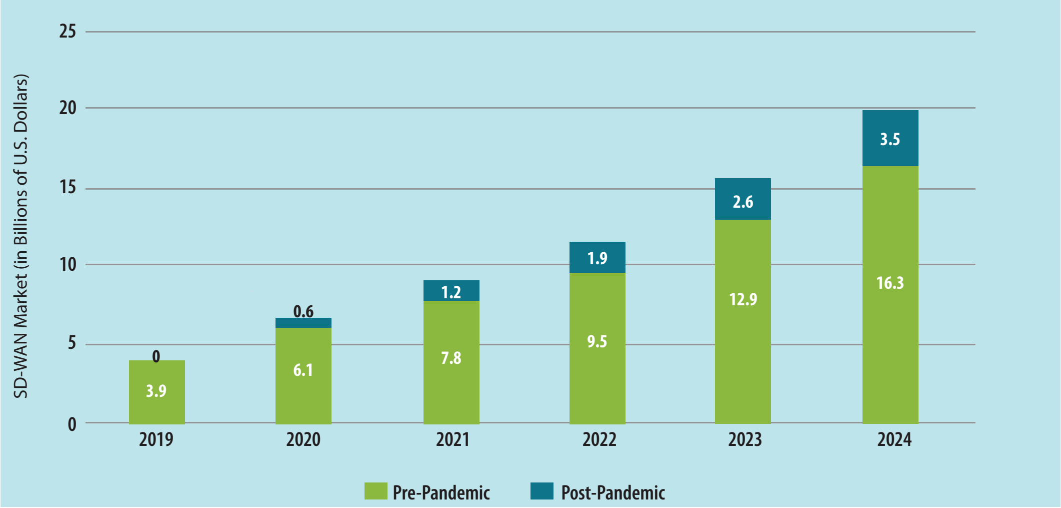
It's been well documented in many media publications how hybrid work has changed the way people do their jobs, particularly those who need to collaborate with others. What hasn't been as widely understood is the impact to corporate IT. Hybrid work has fundamentally changed the technology businesses use and the way it's deployed. For example:

Cloud adoption accelerates and the cloud model evolves. Clouds are shifting away from a centralized model to a distributed one where workloads and applications can span private clouds, public clouds and edge locations. Cloud services are location-independent, making them ideal for hybrid work. The ZK Research 2022 Work-from-Anywhere Study found that 64% of companies have increased their spend on public clouds, while 58% have boosted their budgets for private clouds.

Remote access needs change. Businesses need to be prepared for scenarios where most users work remotely for an indefinite period. Virtual private networks (VPNs) acted as a "Band-Aid" solution, allowing people to connect remotely. However, because of security issues, such as open network access and performance problems caused by backhauling network traffic, VPNs are not a good long-term solution. Businesses will look to augment connectivity with software-defined wide-area network (SD-WAN) and secure access service edge (SASE) solutions to connect and secure remote workers. Exhibit 2 shows the boost SD-WAN will see due to the pandemic.

IT has less direct control over infrastructure. A decade ago, corporate IT teams determined what endpoint and apps workers used, where and when resources could be accessed,

Exhibit 2: SD-WAN Spend Accelerates



ZK Research 2021 SD-WAN Forecast

and how employees connect, and the network was private. Today, control is largely gone as shadow IT has taken over software-as-a-service (SaaS) purchasing, SD-WAN has introduced public broadband and hybrid work has pushed the enterprise edge to the home. IT's formerly tightly controlled environment has given way to a chaotic, unpredictable one.

Of all the domains within IT, it's arguable that the one most impacted is security. Cyber engineers need to protect a dynamic, distributed and ephemeral attack surface. This has made traditional security constructs necessary but no longer sufficient. VPNs have been the standard for decades, but they lack the performance and security requirements of most workers. Therefore, it's time for access to evolve to a zero-trust model. However, first-generation zero-trust network access (ZTNA) solutions were basic network access tools with a few features bolted on. Today's businesses need a paradigm shift in zero trust, or ZTNA 2.0, to secure the modern hybrid workforce.

Today's businesses need a paradigm shift in zero trust, or ZTNA 2.0, to secure the modern hybrid workforce.

SECTION II: ZTNA 1.0 SOLUTIONS LEAVE COMPANIES OPEN TO BREACHES

ZTNA has drawn tremendous interest over the past several years because it improves security by shrinking the attack surface. IP networks were designed with openness in mind, so any connected endpoint can connect with any other. This is why the internet works as seamlessly and as fast as it does. The problem is that once a network is breached, the threat actor has access to every company resource and can often "hide" in the environment for months, causing significant damage to companies.

The thesis behind ZTNA is to shift to a least-privilege model where no endpoint can communicate with any other unless explicitly allowed. This minimizes the attack surface so if a breach occurs, the threat actor will only have access to a few or perhaps no other systems, limiting the "blast radius" of the breach. Although this was the original concept behind ZTNA, first-generation solutions have one or more of the following limitations:

Violate the principle of least privilege: Least privilege is at the core of ZTNA, but it can't be achieved with network solutions. Even when vendors claim to understand applications or application-level access control, most equate applications to network constructs such as IP address, port number and fully qualified domain names (FQNDs). This might seem reasonable, as the internet is built using these constructs, but there are three significant problems:

- **The attack surface is not optimized.** Most applications use dynamic ports and IP addresses. Consequently, ZTNA solutions need to grant access to a wide range of ports and addresses, and this leaves a much broader attack surface exposed than should be necessary.
- **Access can only be restricted at the application level.** ZTNA 1.0 solutions only have visibility at the application level, meaning they can't control access to apps. In some cases, it may be beneficial to restrict access to specific functions. To do this, the ZTNA solution would need to control access at the sub-application level.

- **The environment is subject to lateral malware movement.** Malware often listens on the same port number and/or IP address that allowed applications do. This lets malware access the environment and then move laterally across the business.

Assume trust once access is granted: One significant flaw in ZTNA 1.0 solutions is that once access is granted to a user or application, that communication is implicitly trusted in perpetuity with the assumption that the user or app will act in a trustworthy manner. All breaches occur when access is allowed. So, when behavior becomes suspicious, access must be revoked. The "allow and ignore" construct of ZTNA 1.0 cannot prevent this.

Lack continuous security inspection: ZTNA 1.0 was designed to be an access control mechanism, with no ability to detect or prevent malware or lateral movement across connections once a user is allowed app access. This is essentially security through obscurity, which assumes all allowed traffic is free from malware as well as other threats or vulnerabilities.

Have no data protection: Existing ZTNA solutions have no visibility or control of data. This exposes the enterprise to the risk of data exfiltration from attackers or malicious insiders. The latter is often ignored by businesses, but it is a significant source of data loss. The Verizon 2021 Data Breach Investigations Report found that between 2018 and 2020, there was a 47% increase in the frequency of incidents involving insider threats, and those breaches accounted for 22% of all security incidents.

Are unable to secure all applications: Existing ZTNA solutions can only address the subset of private applications that use static ports. Also, they cannot properly secure microservices-based cloud-native apps or apps that use dynamic ports such as voice and video apps, or server initiatives apps like help desk and patching systems. Lastly, current ZTNA solutions completely ignore SaaS apps, which now represent most enterprise apps and continue to grow. The ZK Research 2021 Global UC Forecast shows that cloud UC, which includes voice and video, will grow at a 21% CAGR though 2026 (Exhibit 3). This is one of the fastest-growing application segments, and it has exposed a significant hole in ZTNA 1.0.

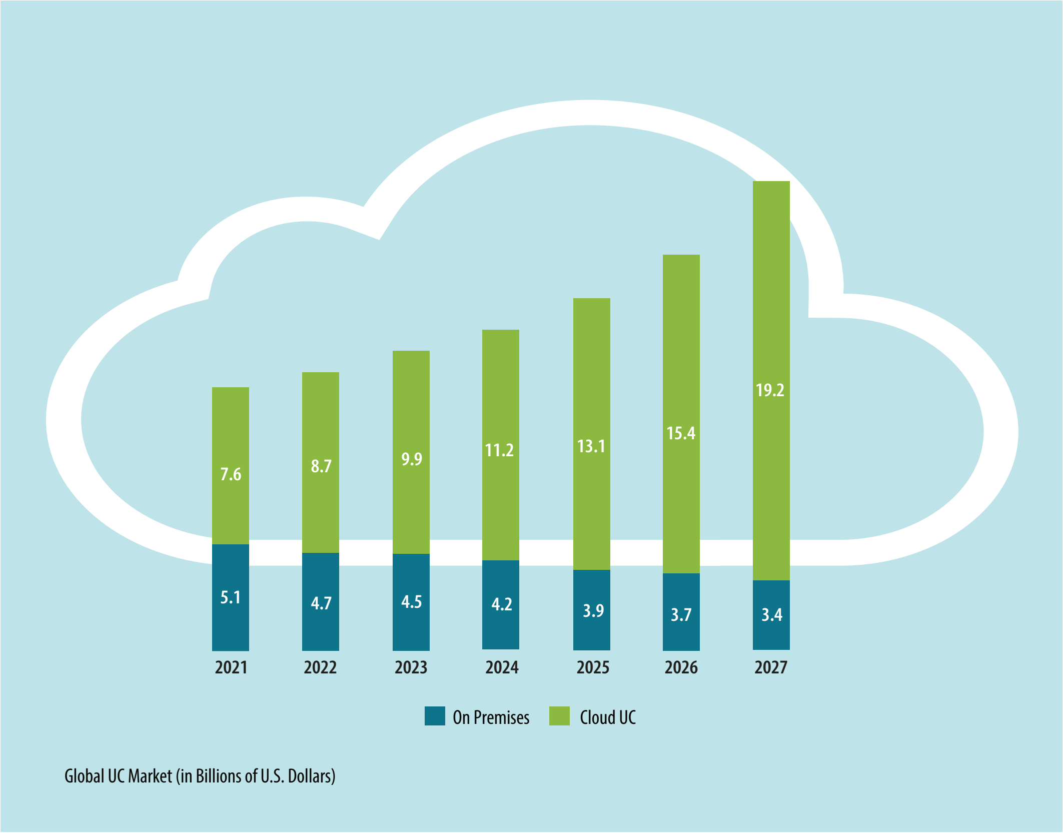
Although the promise of ZTNA has been well understood, 1.0 solutions cannot deliver the necessary features to protect the business.

Although the promise of ZTNA has been well understood, 1.0 solutions cannot deliver the necessary features to protect the business. Hybrid work has changed the way people work, the applications that workers use and how the environment is accessed. It's time for ZTNA to evolve.

SECTION III: DEFINING ZTNA 2.0

ZTNA 2.0 is a complete rethink of how access is managed. First-generation solutions were upgraded VPN products, but second-generation products are built from the ground up to ensure least

Exhibit 3: Cloud Communications Grows with Hybrid Work



ZK Research 2022 Global UC Forecast

privilege can be maintained across the extended enterprise, all the time. The following principles are fundamental to ZTNA 2.0:

Operates at the application layer: ZTNA 2.0 shifts the focus of the technology from the network (Layer 3) to the application (Layer 7), which enables the full potential of zero trust to be unleashed. This ensures granular access control can be applied at the application and even sub-application level independent of network configurations, helping organizations to fully realize the principle of least privilege. If a user moves location or network changes are made, these are transparent to ZTNA, ensuring least privilege is always being maintained.

Maintains continuous trust verification: As indicated in the previous section, continuous trust is difficult, if not impossible, to maintain. Once a user is granted access to an application, trust is implied—which can cause breaches to go undetected. ZTNA 2.0 must continually assess trust based on changes in device posture, user behavior and app activity, and then revoke access on anything anomalous. For example, if a user logs in from across the globe only minutes after accessing an application locally, that indicates the credentials were stolen. Alternatively, if an application starts running on a new port, that likely indicates it was hijacked.

Continuously inspects security: ZTNA 2.0 solutions should continuously perform deep packet inspection of all traffic, even for connections that have previously been allowed. This can help quickly find and stop both breaches and zero-day threats. Continuous security is the best form of defense when a legitimate user's credentials are stolen and used to launch attacks against applications or infrastructure.

ZTNA 2.0 offers consistent control of data across every application used in the enterprise.

Delivers comprehensive data protection: ZTNA 2.0 offers consistent control of data across every application used in the enterprise, including on-premises applications and SaaS apps—the latter of which are invisible to first-generation ZTNA. This can all be done with a single data loss prevention (DLP) policy, which dramatically simplifies operations.

Provides complete application security: With ZTNA 2.0, all applications across the business are secured, including legacy applications, SaaS applications, private apps and modernized, cloud-native ones. It's important to note this also includes apps that utilize dynamic ports and ones that leverage server-initiated connections.

SECTION IV: PALO ALTO NETWORKS IS A COMPLETE ZTNA 2.0 PROVIDER

Silicon Valley–based Palo Alto Networks is the security industry's market leader, and it has the broadest and deepest product portfolio of all vendors. The company's Prisma Access product has been a de facto standard for securing and connecting remote workers for years. Palo Alto was one of the early-to-market ZTNA vendors and is a leader in Forrester's most recent ZTNA New Wave report.

Recently, the company introduced the industry's first ZTNA 2.0 solution on Prisma Access, which is designed to protect the hybrid workforce while providing a great user experience via a simple and unified security product. Although many security vendors offer "cloud" security, most are built on older technology that went through a "lift and shift." Palo Alto offers a fully modernized, cloud-native set of security services that include secure web gateway (SWG), next-generation cloud access security broker (NG-CASB), firewall as a service (FWaaS) and DLP in a cloud-native global services edge. Prisma Access has a common policy framework that enables single-pane-of-glass management, which is ideally suited to secure today's hybrid workforce without compromising performance.

Palo Alto's Prisma Access meets the criteria outlined in Section III in the following ways:

Ensures least privilege access: Prisma Access operates at Layers 3 to 7 of the Open Systems Interconnection (OSI) stack, spanning from the network through applications. Palo Alto uses patented App-ID technology to accurately control access at the app and the sub-app level, which includes the ability to control specific functions such as upload/download.

Delivers continuous trust verification: Palo Alto's solution constantly assesses trust and verification through the following three patented processes:

- **User-ID** provides deep visibility into users and continuously monitors user behavior for suspicious activity.
- **Device-ID** offers visibility into the posture of devices, giving the ability to revoke access if a device falls out of compliance with company policy.
- **App-ID** ensures traffic running over specific ports consists of the appropriate applications. For example, traffic flowing over Port 443 is secure web.

Provides continuous security inspection: Prisma Access has a machine learning (ML)–powered engine to stop 95% of threats inline without using signatures. The ML-powered capabilities combined with Palo Alto's cloud security services block more than 224 billion threats per day for customers. For the threats that cannot be stopped with inline protection, Prisma Access uses single-pass traffic processing for other cloud-delivered security services, including the following:

- **Threat Prevention** prevents exploits, command-and-control, and other network attacks across all apps and protocols.
- **WildFire** is a massive malware analysis ecosystem that provides fast signature delivery.
- **Advanced URL Filtering** is web security that prevents 24% more phishing than all other vendors.
- **DNS Security** thwarts all major Domain Name System (DNS)–layer attack types.

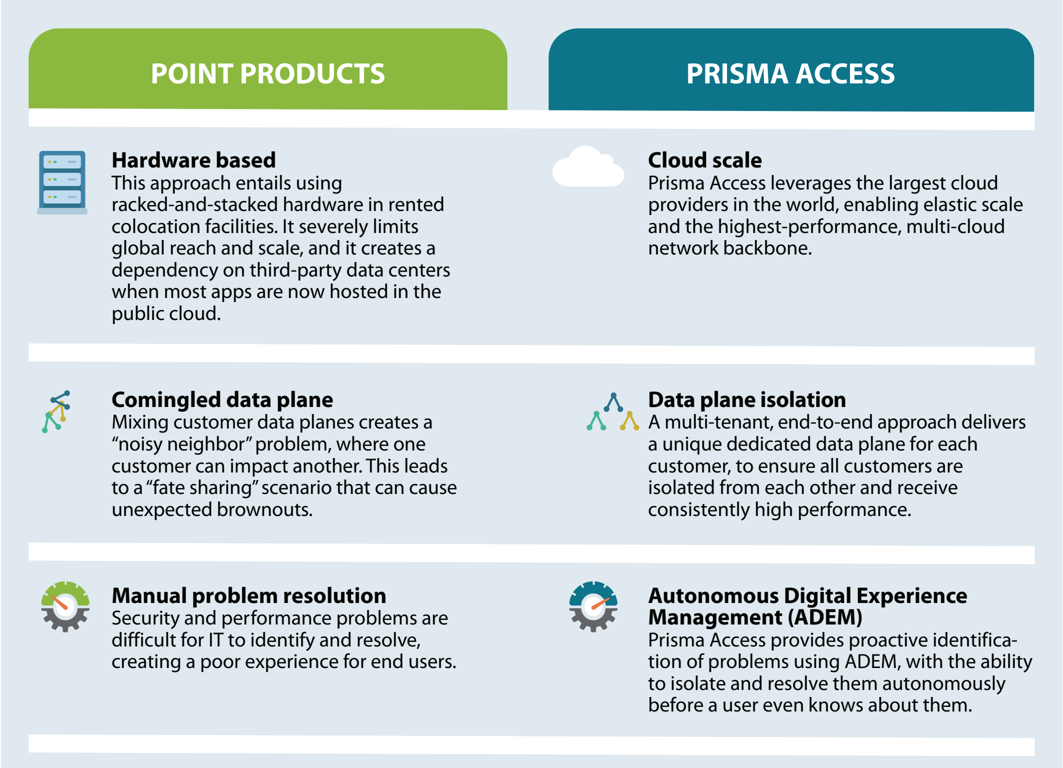
Protects all data: Unlike ZTNA 1.0 solutions, which have no visibility into data exfiltration or loss, Prisma Access supports Palo Alto's enterprise DLP, which provides consistent visibility of data access across the enterprise. From a single management console, customers can apply consistent DLP to all data—whether it is stored in on-premises legacy apps, public cloud apps or SaaS—all with a single policy.

Secures all applications: Prisma Access utilizes a single, unified product to protect all users and applications across the company, regardless of whether the user connects to the product via an agent or without one. This includes on-premises, public cloud, SaaS, legacy and modern/cloud-native apps.

Prisma Access utilizes a single, unified product to protect all users and applications across the company.

Also, Prisma Access was designed with the best-in-class user experience in mind, and Palo Alto backs this up with aggressive service-level agreements (SLAs) featuring five-nines of uptime and less

Exhibit 4: Cloud-Native Architecture of Prisma Access Modernizes ZTNA



POINT PRODUCTS	PRISMA ACCESS
Hardware based This approach entails using racked-and-stacked hardware in rented colocation facilities. It severely limits global reach and scale, and it creates a dependency on third-party data centers when most apps are now hosted in the public cloud.	**Cloud scale** Prisma Access leverages the largest cloud providers in the world, enabling elastic scale and the highest-performance, multi-cloud network backbone.
Comingled data plane Mixing customer data planes creates a "noisy neighbor" problem, where one customer can impact another. This leads to a "fate sharing" scenario that can cause unexpected brownouts.	**Data plane isolation** A multi-tenant, end-to-end approach delivers a unique dedicated data plane for each customer, to ensure all customers are isolated from each other and receive consistently high performance.
Manual problem resolution Security and performance problems are difficult for IT to identify and resolve, creating a poor experience for end users.	**Autonomous Digital Experience Management (ADEM)** Prisma Access provides proactive identification of problems using ADEM, with the ability to isolate and resolve them autonomously before a user even knows about them.

Palo Alto Networks and ZK Research, 2022

than 10 ms security processing. ZK Research believes Palo Alto Networks is the only ZTNA 2.0 vendor with a performance SLA for third-party SaaS applications.

Although a security team could attempt to build a ZTNA 2.0 solution using point products that went through a lift and shift to make them cloud residents, that model has some significant gaps compared to Palo Alto's cloud-native Prisma Access. Exhibit 4 highlights the main differences in these two approaches.

SECTION V: CONCLUSION AND RECOMMENDATIONS

Hybrid work is here to stay and has forever changed the way we work. It's also changing the way businesses need to secure and connect workers. Legacy VPN and first-generation ZTNA products were sufficient as a stopgap to get users up and running, but now it's time for companies to consider the long-term impact of hybrid work.

Access must evolve, and ZTNA 2.0 is the path forward. Legacy solutions were sufficient a decade ago, but they were never designed for a world that is both dynamic and distributed. ZTNA 2.0 was built from the ground up for cloud-first, distributed companies—which include almost all businesses today. Therefore, ZTNA 2.0 is now an imperative. As companies look to evolve to ZTNA 2.0, ZK Research offers the following recommendations:

Rethink security in the era of hybrid work. The traditional security model of buying point products was sufficient in the past because IT controlled every aspect of working—from the apps and devices people used, to the network and even how they accessed the network. With hybrid work, apps have moved to the cloud, devices are now mobile and people are working at home. This dictates that security move from point product to a platform where it is enforced end to end. Palo Alto's Prisma Access is a good example of such a platform.

Start with the biggest security pain point. All businesses should be looking at ZTNA 2.0, but the starting point will be different based on the individual company. ZK Research has identified three initiatives that can help organizations move to ZTNA:

- Securing private app access as a VPN replacement
- Securing internet and SaaS access as an SWG replacement
- Implementing advanced SaaS app security as a CASB and DLP replacement

Choose a cloud-native security partner. Dozens of security vendors claim to offer security via the cloud. Therefore, it's important for customers to understand that not all versions of cloud are created equal, and that "cloud" does not always mean "cloud native." Customers must do their due diligence and ensure the vendor is running a modernized, cloud-native platform, as this will lead to faster innovation and better resiliency.

CONTACT
zeus@zkresearch.com
Cell: 301-775-7447
Office: 978-252-5314