



Enterprise Strategy Group | Getting to the bigger truth.™

ESG WHITE PAPER

The Evolution of ZTNA to Fully Support Zero Trust Strategies

By John Grady, ESG Senior Analyst

May 2022



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



Contents

Executive Summary	3
Access Challenges of the New Workplace	3
The Adoption of Zero Trust and ZTNA	5
Why a New Approach to ZTNA Is Necessary	7
Key Requirements for Supporting Enterprise-wide ZTNA	7
Palo Alto Networks' Prisma Access: Cloud-Delivered ZTNA 2.0	8
The Bigger Truth	9

Executive Summary

Zero trust network access (ZTNA) proved to be an important technology initiative during the pandemic, allowing organizations to empower remote workers by offering solutions that provided improvements in security, manageability, and scalability as opposed to using their existing virtual private networks alone. The transition to remote and hybrid work has had an ongoing and profound impact—not only on where we work, but also on how work gets done. Now, work is no longer a place we go, but more of an activity we perform. As businesses have adjusted to this new model of hybrid work, with users and applications being anywhere and everywhere, the teams responsible for IT, networking, and security are facing new challenges in the form of a massively increased attack surface due to direct-to-app connectivity.

Organizations have deployed ZTNA solutions as a way to try and get a handle on this trend by modernizing infrastructure to deliver needed networking and security capabilities in a cloud-delivered services edge—thus facilitating direct-to-app connectivity as close to the user and app as possible. However, first-generation/ZTNA 1.0 solutions fall short in many ways on delivering on the promise of true zero trust. In fact, they grant more access than is desired. What's more, once access is granted in ZTNA 1.0 solutions, the connection is implicitly trusted forever, allowing a handy exploit route for sophisticated threats and/or malicious actions and behavior.

It is time to embrace a new approach to ZTNA, one that has been designed from the ground up to meet the specific challenges of modern applications, threats, and a hybrid workforce. This white paper discusses why it is time for a new approach to ZTNA and describes the critical new capabilities that are required (such as truly applying the principles of least-privilege access and enabling continuous verification of trust), based on user activity, behavior, and enterprise-wide context—as well as security inspection to be able to effectively protect all applications and all data, everywhere. We explore the new approach to ZTNA that is now available in cloud-delivered Prisma Access solutions from Palo Alto Networks.

It is time to embrace a new approach to ZTNA, one that has been designed from the ground up to meet the specific challenges of modern applications, threats, and a hybrid workforce.

We also provide guidance on how decision makers can best leverage ZTNA 2.0 technology to reduce risk in the modern workplace.

Access Challenges of the New Workplace

The pandemic has proven that remote and hybrid work are not only feasible, but desired, for a large percentage of the workforce. What began as a response to a crisis has turned into an opportunity for organizations to be more efficient, productive, and responsive to the needs of their workers. However, the scale, scope, and speed of the transition to remote and hybrid work has also been a major challenge to IT, security, and networking teams. According to ESG research, 59% of decision makers said that cybersecurity has become more difficult over the last two years.¹

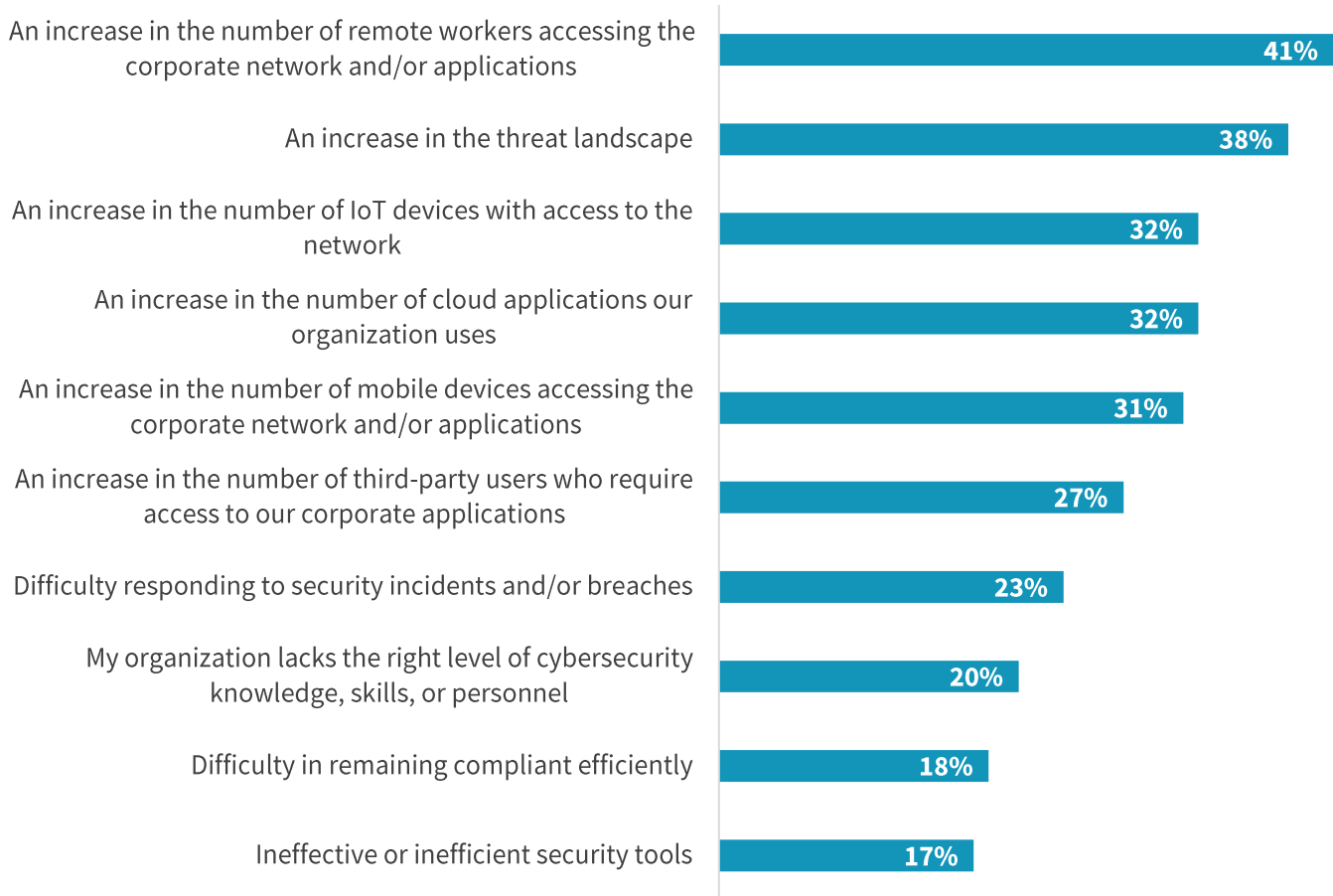
Respondents reported that the primary driver for additional cybersecurity difficulty was the increase in the number of remote workers accessing the corporate network and/or applications. Compounding the challenge of remote access, decision makers cited issues related to the changing threat landscape, the increase in the number of cloud applications used by their organizations, and the need to connect third-party users to corporate resources (see Figure 1).²

¹ Source: ESG Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

² Ibid.

Figure 1. Reasons Making Cybersecurity More Difficult

In your opinion, which of the following factors have been most responsible for making cybersecurity management and operations more difficult? (Percent of respondents, N=249, three responses accepted)

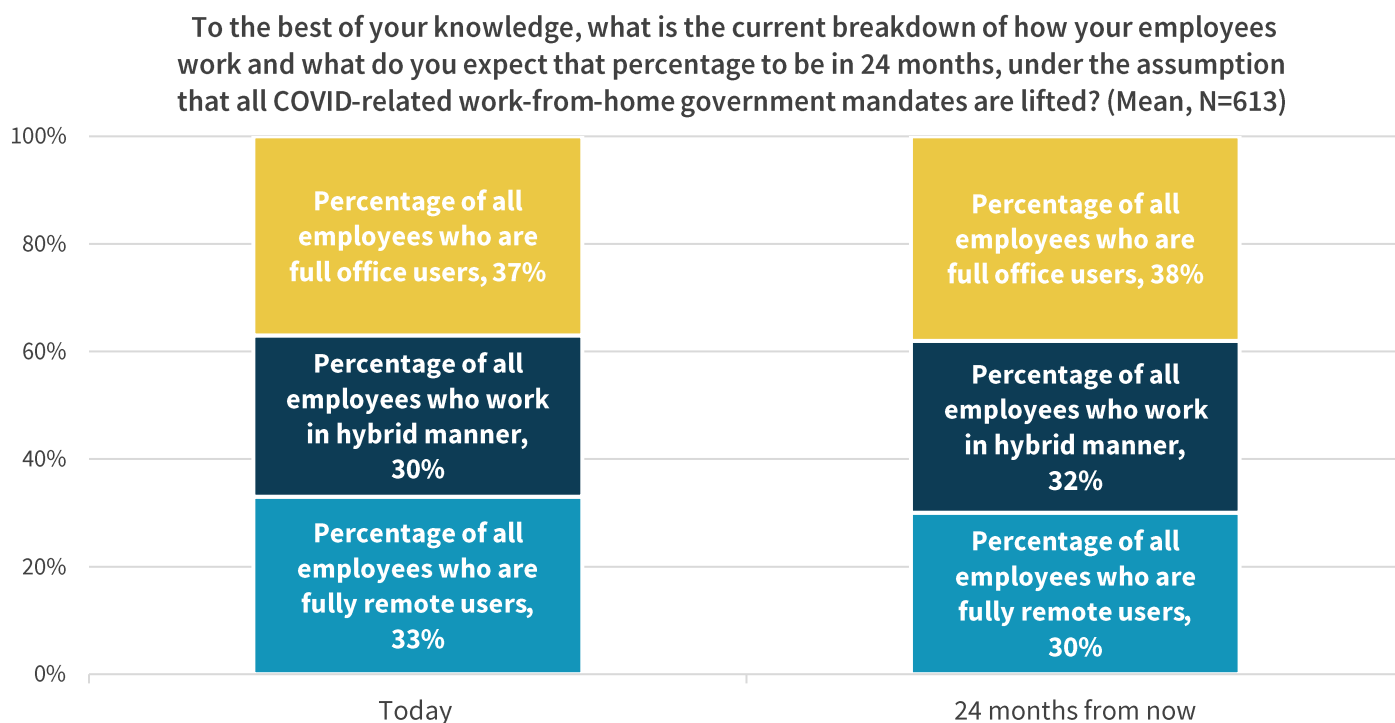


Source: ESG, a division of TechTarget, Inc.

The dynamics that catalyzed the shift to remote work may have changed, but the impact will be long-lasting. What began as a stopgap solution to a crisis has evolved into a new way of hybrid work that is now expected and, in many cases, demanded by employees. The idea of going back to the way things were before the pandemic is no longer realistic or viable. Research by ESG shows that more than 60% of employees today are working in a hybrid or fully remote environment. Tellingly, that percentage is only expected to change marginally over the next two years (see Figure 2).³

³Source: ESG Complete Survey Results, [2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased](#), December 2021.

Figure 2. The New Model of Work Will Be Mixed



Source: ESG, a division of TechTarget, Inc.

This new world of work has created challenges in consistently securing remote workers and providing access to the corporate network and business-critical applications. These challenges include a much larger attack surface and a shift from backhauling traffic to a data center via the corporate network to a model more driven by direct-to-app connectivity and edge computing.

At the same time, threat actors are increasingly sophisticated, with access to more funding and, in some cases, protections from state sponsors. To make matters even more challenging, attackers are focusing on exploiting gaps exposed by remote and hybrid workers and the inherent weaknesses in existing networking and security solutions. A new approach is needed, and it is needed now.

The Adoption of Zero Trust and ZTNA

Given the challenges in the market, it is clear that zero trust and ZTNA are essential elements of any approach to networking and security in the hybrid work world. Zero trust, when properly implemented, reduces threats of security breaches, simplifies policy management and enforcement, and creates additional assurances of protection for users, applications, and data. However, while the term “zero trust” has been around since 2010, actual deployments are still taking time to catch on. According to an ESG research survey, 54% of respondents stated that their organization’s zero trust initiative has been in place for less than two years.⁴

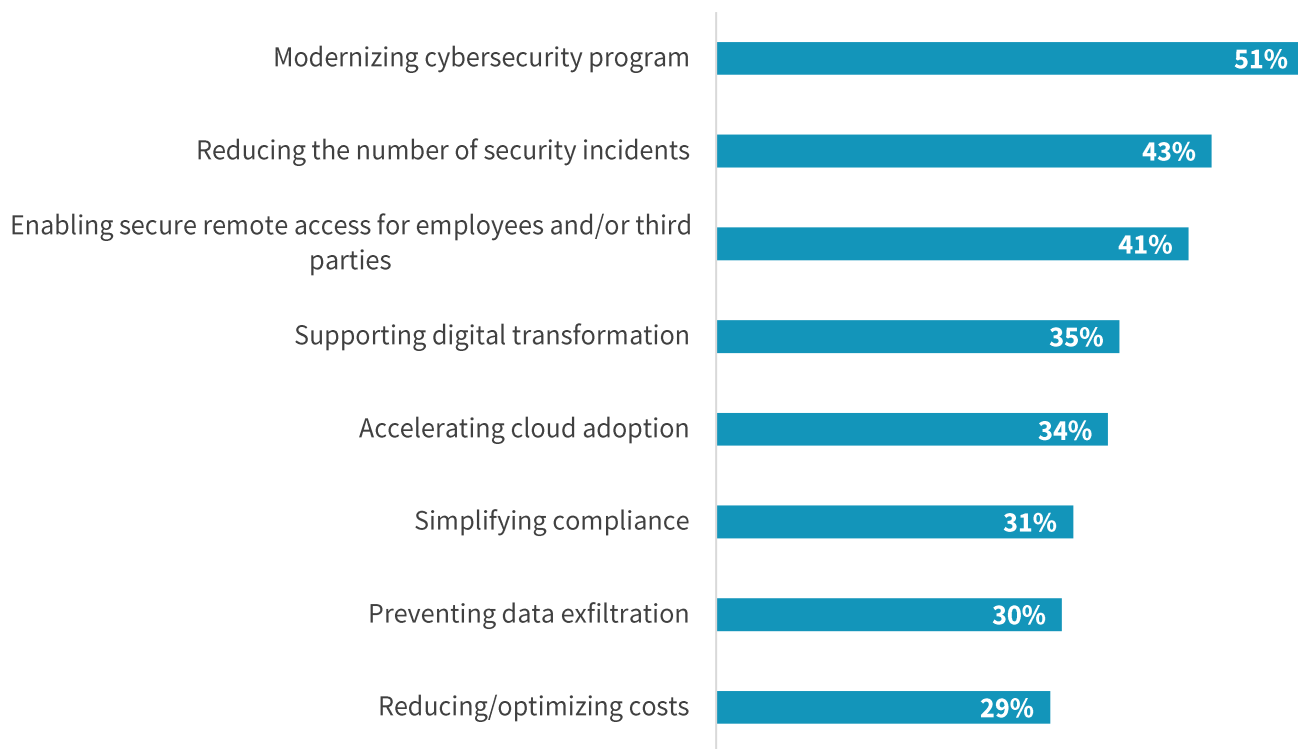
There are a variety of reasons why organizations are looking to implement zero trust strategies, including broad IT goals such as supporting digital transformation and accelerating cloud adoption. Two of the most common reasons are to support cybersecurity modernization and to enable secure remote access for employees and third parties (see Figure 3).⁵

⁴ Source: ESG Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

⁵ Ibid.

Figure 3. Zero Trust Drivers

Which of the following would you consider to be the top business drivers behind your organization’s adoption or consideration of a zero-trust strategy? (Percent of respondents, N=421, three responses accepted)



Source: ESG, a division of TechTarget, Inc.

The rapid expansion of remote work during the pandemic has been another catalyst for the heightened interest and expectations for zero trust. As organizations scaled remote workers quickly in response to the pandemic, many of the performance and operational drawbacks of VPNs for remote access became glaringly apparent. The drawbacks include a lack of scalability, a reliance on hardware-based technology, a need to backhaul traffic, and far too much access being granted.

These gaps created a groundswell of momentum, not just around zero trust as a framework, but specifically around zero trust network access as a viable and less risky alternative to VPNs. ESG research has found that 69% of organizations are using ZTNA and have moved away from VPN or are planning to move away from VPN.⁶ ZTNA provides distinct advantages over VPNs, including that:

- Users can only see the applications and services they are explicitly allowed to access.
- Applications are hidden from the public internet.
- In most cases, ZTNA solutions are delivered via the cloud.

⁶ Source: ESG Complete Survey Results, [2021 SASE Trends: Plans Coalesce But Convergence Will Be Phased](#), December 2021.

However, while existing ZTNA 1.0 solutions have been a necessary step forward from existing VPN appliances, the continued growth of remote and hybrid work and hybrid cloud, as well as the explosion of modern applications, is exposing gaps in the technology that need to be remedied.

Why a New Approach to ZTNA Is Necessary

Where do existing ZTNA 1.0 solutions fall short? The primary issues have to do with access controls, least-privilege access, lack of visibility, and an “allow and ignore” model that trusts but rarely verifies. This means that the full principles of zero trust are not being followed or enforced. Some of the specific weaknesses of ZTNA 1.0 approaches include:

1. **Least-privilege:** ZTNA 1.0 solutions are built to control access with coarse-grained access controls. This violates the principle of least privilege by treating applications as a network construct at layer 3-4 (IP and port). This affords users more access than is necessary. It also misses additional context around applications that can be helpful in verifying users or devices, including which applications are being used, time of day, location, and other factors.
2. **“Allow and ignore”:** Once access to an application is granted, that communication is implicitly trusted forever. This assumes that the user and the app will always behave in a trustworthy manner. “Allow and ignore” is not a strategy for today’s environment, nor for true zero trust, because breaches occur on allowed activity, which an “allow and ignore” model can’t prevent.
3. **No security inspections.** Today’s solutions assume traffic is secure, with no inspection and no ability to detect or prevent malware or lateral movement across connections once app access for a user is allowed. They grant access but do not incorporate visibility or control of the traffic, exposing the enterprise to increased risk of a data breach.
4. **Limited or even no data protection.** Current solutions provide little to no visibility nor any control over sensitive data. What’s more, organizations often rely on different solutions to secure sensitive data across private and SaaS or Internet applications, creating disparate and siloed approaches that add to complexity and expose organizations to the risk of data exfiltration from attackers or malicious insiders. Today’s enterprises need consistent control of data across all applications, with a single DLP policy.
5. **Separate platforms for cloud and on-premises applications:** ESG research shows that coverage for cloud and on-premises environments is the most important attribute for organizations in terms of the technologies supporting zero trust.⁷ Many existing ZTNA solutions are designed for either on-premises applications or cloud applications, but not both. A modern approach has to be all-inclusive and all-encompassing to reduce complexity as well as risk.

Key Requirements for Supporting Enterprise-wide ZTNA

To meet the challenges of the new workplace, ZTNA solutions need to close these gaps. Otherwise, organizations will be investing in solutions that don’t provide the level of security required in this era. In addition to concerns about increased and unnecessary risks, decision makers need to use solutions that factor in user experience, performance, and simplified manageability. Some of the key requirements for the next iteration of ZTNA, which take into account the challenges of hybrid work, hybrid cloud, and modern applications, include:

⁷ Source: ESG Survey Results, [The State of Zero Trust Security Strategies](#), May 2021.

- **Application centricity:** Focused on Layer 7, not just network-level policies and access. This allows users to fully realize the principle of least-privilege by operating at Layers 3-7, providing the most granular access control possible at both app and sub-app levels. This limits the risk of users having more access than necessary.
- **Continuous assessment based on behavior:** In a ZTNA 2.0 model, once access to an application is granted, trust is continuously assessed based on a variety of factors, including user activity, behavior, and enterprise-wide context. If suspicious activity is detected, or if data exfiltration is feared, access to an app can be revoked in real time.
- **Continuous security inspection.** Once the connection is established, continuous and ongoing inspection of all traffic, even for allowed connections, is required to prevent all threats, including zero-day threats. This is especially important in scenarios where legitimate user credentials are stolen and used to launch attacks against applications or infrastructure.
- **Protect all data.** With a ZTNA 2.0 model, organizations now have comprehensive and consistent visibility and control over sensitive data across all applications from a single management console and with a single policy. What's more, this new model allows enterprise DLP to be applied to all data, whether it is stored in on-prem legacy applications, public cloud applications, or SaaS.
- **Comprehensive application coverage:** All applications (public, private/on-premises, and cloud); all data access models (remote and hybrid); ultimately helps support a true zero trust architecture model, rather than remote-access specific. In addition, ZTNA 2.0 solutions should ensure that traffic is secure by performing deep and ongoing security inspections. This helps prevent all threats using machine learning, including the inline prevention of zero-day threats.

In addition to these five capabilities that address the weaknesses of existing ZTNA 1.0 solutions, decision makers should weigh additional criteria in choosing a solution that not only addresses today's challenges, but also meets future needs for reducing risk and supporting growth in the hybrid workplace. Specifically, when ZTNA is incorporated as part of a broader SASE platform, organizations can benefit from simplified, consistent management, which promotes operational efficiency and ensures consistent enforcement of policies and access rules for all applications and users across the environment. Further, this must be accomplished without impacting the user experience. As hybrid models take hold, the way users access the applications they use to do their jobs should not deviate widely based on where they happen to be located.

Palo Alto Networks' Prisma Access: Cloud-Delivered ZTNA 2.0

Palo Alto Networks has recently made enhancements to its Prisma Access solution to meet the remote access/zero trust needs of the hybrid work world. The solution is cloud-delivered and offers a true zero trust network access 2.0 experience. Key features and capabilities include:

- **Built to secure all users and applications, with fine-grained user-app and access controls.** Prisma Access allows organizations to fully realize least-privilege access from Layers 3 through 7, with controls at the app, sub-app, app function, and app activity levels. This applies to any user, any app, any location.
- **Continuous trust verification based on behavior.** If there is suspicious behavior or suspected data exfiltration, access to an app can be revoked in real time, minimizing risk and potential damage. This eliminates the "allow and ignore" approach of ZTNA 1.0 by assuring that trust is continuously assessed and verified.
- **Ensures traffic is secure with deep and ongoing security inspection.** Prisma Access provides single-pass traffic processing to inspect for all types of threats to deliver high performance and low latency. Machine learning

capabilities help to stop threats inline, without the use of signatures. As part of a broader platform, Prisma Access incorporates threat prevention, malware analysis, advanced URL filtering, DNS security, and other features.

- **Secures all the applications, all of the time, across all access models.** Prisma Access ZTNA 2.0 supports all users and applications used across the enterprise, including on-premises, public cloud, SaaS, legacy, and modern/cloud-native applications. Users can connect to Prisma Access ZTNA 2.0 with or without agents and be secured in the same consistent way.
- **Secures data everywhere.** Prisma Access secures both access and data everywhere with consistent control of data across all applications used in the enterprise and a single policy for data loss prevention. Prisma Access is built in the cloud to secure at cloud scale, leveraging the elastic scale and availability capabilities of leading hyperscale public clouds.
- **Unified management and consistent user experience.** Prisma Access is a unified platform that simplifies management and deployment for network and security teams while giving users a high-performance, consistent, and resilient experience across all applications, devices, and locations. The architectural model of Prisma Access supports five-nines uptime, 10ms security processing, and a performance SLA for software-as-a-service applications. Prisma Access also provides native Autonomous Digital Experience Management (ADEM) that provides proactive identification of problems with the ability to isolate and resolve issues before users even know about them.

The Bigger Truth

Organizations are under enormous pressure to empower remote and hybrid workers. Applications and users are everywhere, necessitating an architectural shift to direct-to-app connectivity, rather than backhauling all traffic to data centers. This transformation has a profound impact on how to secure the enterprise, particularly in an environment where cyber-threats are becoming more sophisticated and targeted at remote users.

While zero trust network access solutions have helped organizations temporarily adjust to the new world of work spurred by the pandemic, the continued growth and expansion of remote access and hybrid work has revealed gaps in the technology. These gaps must be addressed for organizations to feel confident in delivering the kind of flexible, productive, and secure hybrid work experience that employees are demanding.

As a long-time innovator in network security, endpoint security, zero trust, and remote access, Palo Alto Networks has identified the weaknesses in zero trust network access 1.0 solutions and has eliminated those gaps with the superior security of ZTNA 2.0 delivered in Prisma Access. This is the first ZTNA solution that offers true zero trust capabilities, including least-privilege access, continuous trust verification based on behavior, deep and ongoing security inspection, and consistent control of data across all applications. Prisma Access offers the additional advantages of a unified platform and management model to help ensure consistent high performance and user experience.



ePlus Security is a leading security technology advisor and integrator with a broad solutions portfolio, strong industry relationships and unmatched breadth of engineering talent and expertise. With a focus on customer experience, our security team designs and delivers outcome-focused, customized cyber security programs aimed at defining and mitigating business risk, identifying business challenges and creating safer digital environments.

www.eplus.com

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.


This publication is copyrighted by TechTarget, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com



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.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188