Palo Alto Networks Calls on Cybersecurity Industry to Adopt ZTNA 2.0 -- Zero Trust with Zero Exceptions

May 11, 2022

First-gen ZTNA solutions have major gaps in security protection and can put organizations at significant risk

SANTA CLARA, Calif., May 11, 2022 /PRNewswire/ -- Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, today urged the industry to move to Zero Trust Network Access 2.0 (ZTNA 2.0) — the foundation for a new era of secure access. ZTNA was developed as a replacement for virtual private networks (VPNs) when it became clear that most VPNs did not adequately scale and were overly permissive, but the first-generation ZTNA products (ZTNA 1.0) are too trusting and can put customers at significant risk. ZTNA 2.0 solves these problems by removing implicit trust to help ensure organizations are properly secured.

"This is a critical time for cybersecurity. We are in an era of unprecedented cyberattacks, and the past two years have dramatically changed work — for many, work is now an activity, not a place. This means that securing employees and the applications they need is both harder and more important," said Nir Zuk, founder and chief technology officer at Palo Alto Networks. "Zero trust has been embraced as the solution — and it is absolutely the right approach! Unfortunately, not every solution with Zero Trust in its name can be trusted. ZTNA 1.0 — for example — falls short."

For modern organizations where hybrid work and distributed applications are the norm, ZTNA 1.0 has several limitations. It is overly permissive in granting access to applications because it can't control access to sub-applications or particular functions. Additionally, there is no monitoring of changes in user, application or device behavior, and it can't detect or prevent malware or lateral movement across connections. ZTNA 1.0 also cannot protect all enterprise data.

ZTNA 2.0-capable products, such as Palo Alto Networks Prisma® Access, help organizations meet the security challenges of modern applications, threats and the hybrid workforce. ZTNA 2.0 incorporates the following key principles:

- **Least-privileged access** — enables precise access control at the application and sub-application levels, independent of network constructs like IP addresses and port numbers.
- **Continuous trust verification** — after access to an application is granted, continuous trust assessment is ongoing based on changes in device posture, user behavior and application behavior.
- **Continuous security inspection** — uses deep and ongoing inspection of all application traffic, even for allowed connections to help prevent threats, including zero-day threats.
- **Protection of all data** — provides consistent control of data across all applications, including private applications and SaaS applications, with a single data loss prevention (DLP) policy.
- **Security for all applications** — consistently secures all types of applications used across the enterprise, including modern cloud native applications, legacy private applications and SaaS applications.

In a new report, John Grady, ESG senior analyst, said: "[F]irst-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." Grady also said, "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."

"Securing today's hybrid workforce, with an increase in cloud and mobile technologies and evolving requirements, can be complicated," said Jerry Chapman, engineering fellow, Optiv. "Rethinking Zero Trust is essential for modern, hybrid organizations to prevent threats. Together with Palo Alto Networks, we're advising our customers to incorporate ZTNA 2.0 principles like continuous review of identity and connection across their domains to stay secure."

New Prisma Access Capabilities
Palo Alto Networks Prisma Access is the industry's only solution that meets today's ZTNA 2.0 requirements. Prisma Access protects all application traffic with best-in-class capabilities while securing both access and data.

New additions to Prisma Access announced today add the following capabilities:

- **ZTNA connector** — simplifies the process of onboarding cloud native and traditional applications into the service, helping make ZTNA 2.0 easier to deploy and more secure.
- **The industry's only unified SASE product** — providing a common policy framework and data model for all SASE capabilities, managed from a single cloud management console.
- **Self-serve autonomous digital experience management (ADEM)** — helps proactively notify users of issues that require prompt attention and provides them with guidance on how to remediate.

Availability
Prisma Access is generally available today with full support for ZTNA 2.0. The new ZTNA connector, unified SASE, and self-service ADEM will be available in the next 90 days.

About Palo Alto Networks
Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration.

By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Prisma, and the Palo Alto Networks logo are registered trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.

Forward-Looking Statements

This release contains forward-looking statements that involve risks and uncertainties, including regarding the benefits or potential benefits to customers of our products. These forward-looking statements are not guarantees of future performance, and actual results, developments and business decisions may differ from those envisaged by such forward-looking statements. We identify the principal risks and uncertainties that affect our performance in our Annual Report on Form 10-K, filed on September 3, 2021, and our other filings with the U.S. Securities and Exchange Commission, which are available on our website at investors.paloaltonetworks.com and on the SEC's website at www.sec.gov. All forward-looking statements in this release are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-calls-on-cybersecurity-industry-to-adopt-ztna-2-0--zero-trust-with-zero-exceptions-301544625.html

SOURCE Palo Alto Networks, Inc.