WHITE PAPER

Why Branch Evolution Demands Zero Trust Network Access

Cybercriminals and their tactics are more sophisticated than ever, and security breaches continue to skyrocket. 65% of attacks originate from exposure of user data by applications, cloud/internet services and IoT devices, 98% of which are unencrypted. That's why zero trust security that is natively integrated with an SD-WAN solution may be an enterprises' best line of defense in protecting people, apps and things.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

sdxcentral®

Introduction

Continuous digital transformation is critical for the modern enterprise to remain competitive, meet customer needs and demands, increase efficiencies and provide cutting edge products. But when it comes to security, the advent of hybrid work, increasingly distributed devices and users and an explosion of Internet of Things (IoT) has significantly broadened the attack surface.

The simple fact is that in today's modern enterprise, everything is at risk — from data to credentials to devices to networks. The branch of yesterday simply doesn't accommodate the type of security architectures that are imperative to protecting employees, diverse and distributed apps and a rapid increase in IoT devices.

Enterprises must take deliberate, strategic steps to secure their branches, users and things. How? With a zero trust approach that ensures least privileged access integrated directly into SD-WAN through a secure access service edge (SASE) solution.

Let's dive into the evolving threat landscape, challenges with legacy solutions and why zero trust must be an imperative.

Cyberattacks at a Frenzied Pace

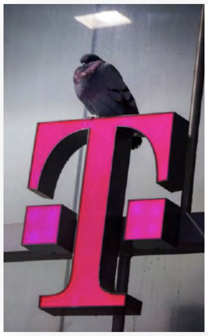
High-profile security breaches make the news every day (and, increasingly, multiple times a day). Enterprises large and small, healthcare systems, financial and educational institutions, the ever-expanding software supply chain and more are constantly under barrage.

Recent examples include:

A social engineering attack on Uber in September, 2022 in which a teenage hacker gained access to the company's privilege access management services and several systems including AWS, Duo, GSuite, Slack, VMware and Windows;

In the beginning of January, it was revealed that a bank of email addresses belonging to roughly 200 million Twitter users was being sold on the dark web for as low as $2. This followed reports that Twitter user data was continuously bought and sold on the dark web throughout 2022;

Specific to IoT, in March 2021 hackers breached a database containing security camera feeds collected by startup Verkada, Inc. This database contained live feeds from 150,000 surveillance cameras inside hospitals, organizations, police departments, prisons and schools. Tesla and Cloudflare were among the companies exposed.



Cell phone giant T-Mobile has been hit multiple times over the last year. The company just reported in April that it was breached for the second time in 2023. The stolen information varied from customer to customer, but could have included full name, contact information, account number and associated phone numbers, account PIN, social security number, government ID, date of birth and balance due.

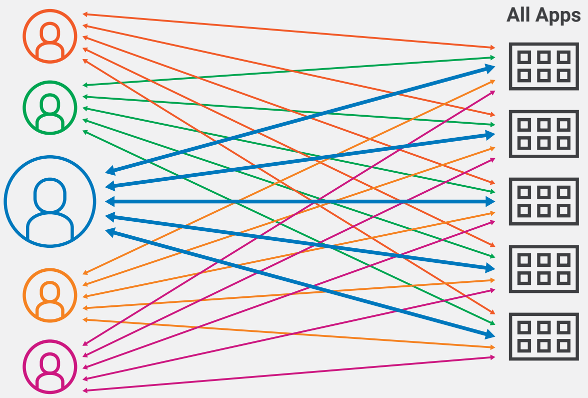
And that's just to name a few.

Cyberattacks and ransomware attacks are rampant: Threat actors are constantly seeking to steal data, intellectual property (IP) and personally identifiable information (PII) to either directly exploit them or demand ransom. Alarmingly, in fact, more than 80% of U.S. companies indicate their systems have been successfully hacked in an attempt to steal, change or make public important data.

Some other stark statistics:

- The average cost of a data breach now sits at $4.35 million.
- 82% of data breaches involved the human element, including social attacks, error and misuse.
- In 2022, 71% of companies worldwide were affected by ransomware, and roughly 72% paid the ransom.

Further exacerbating the situation is the dramatic growth in IoT devices. Their number is forecast to almost triple to more than 29 billion in 2030. Overall, market research firm IoT Analytics predicts there will be approximately 27 billion connected IoT devices throughout enterprises by 2025. To put that in perspective: In just a few years, there will be more than four times more devices connecting to enterprise networks than users.



Bigger Attack Surface= More Attacks

92%

of technology executives said that their companies experienced a cyber attack over the past 12 months.

(Forrester, 2021)

A New Threat, A New Security Tool

76

The average number of security tools in an organization. (+19% over the past two years, from 64 to 76)

(Panaseer, 2022)

Figure 1. The Attack Surface Has Exploded

Undoubtedly, devices have enabled and further accelerated digital transformation. But at the same time, they have clearly exposed enterprises and their various branches to new threats. An IoT Threat Report by Palo Alto Networks Unit 42 found that:

- **57%** of IoT devices are highly vulnerable
- **98%** of all connected device traffic is unencrypted
- **83%** of connected devices run an unsupported OS

This trend combined with the fact that more and more applications are being widely distributed across branch locations and hybrid networks along with the rapid adoption of all things cloud means vulnerabilities will continue to be exploited — only at a much more frequent pace.

Too Many Tools, Not Enough Visibility

Cybersecurity is also evolving rapidly as the enterprise attack surface has increased — spurred largely by the almost overnight shift to remote work during the COVID-19 pandemic…and the fact that the hybrid work model looks like it's here to stay. After all, recent studies show that 74% of U.S. companies are using or plan to implement a permanent hybrid work model.

It's not just an enterprise-specific problem, either. The software supply chain, largely composed of vulnerable open-source code, has also experienced an increasingly growing attack surface.

At the same time, threat actors are growing more sophisticated, exploiting every entry point they can. They are also commoditizing ransomware tools — known as ransomware-as-a-service (RaaS) — that allow novices without coding or hacking skills to access RaaS kits for as low as $100.

The challenge businesses face is their security tools have traditionally been too basic. Enterprises grapple to secure a broad set of locations, users and apps, and have reactively installed a range of disparate point-products — from monitoring tools to alert mechanisms to sandbox environments — based on a basic understanding of what they have and what they can secure.

According to security posture management company Panaseer, large enterprises now have an average of 76 security tools deployed in their environments. At the same time, 82% of security leaders have been surprised by a security event, incident or breach which evaded a control they thought was in place.

This underscores the fact that enterprise leaders often have a lack of visibility or knowledge as to what is going on in their network, let alone how they might secure it end-to-end.

Further complicating this situation is the fact that these disparate tools often live in corporate data centers, which necessitates the need to backhaul data from a branch or remote location to the data center, thus impacting performance and user experience.

However, today apps are everywhere and branches are everywhere, so sending everything to the data center doesn't scale, nor does it make sense from a traffic optimization perspective. Yes, in a standalone data center, security teams can install firewalls — one or multiple — but that gets expensive and unwieldy when an enterprise has multiple branches in different states, regions or countries. It also blurs visibility; enterprises have a difficult time making sense of where things are going and wrangling thousands or millions of data points to derive critical analytics.

Instead, a distributed network should, naturally, have distributed security with global scale, interconnectivity and full accessibility. With users connecting from anywhere and everywhere, all endpoints should have a next-generation level of security.

Most importantly, enterprises can't just infer from past experiences that they have visibility into their users, devices and patterns. In today's world, there are so many unknowns about whether a user is actually who they say they are, what and where they're connecting from and what exactly they're accessing.

Enter Zero Trust — and Accelerating to Zero Trust 2.0

As the old proverb goes, enterprises today must "trust, but verify" every digital transaction. A modern approach to zero trust turns this on its head — verify, then trust; verify again, then trust (and so on).

The term "zero trust" was coined in 2010 by Forrester Research analyst John Kindervag, who based it on the assumption that risk is an inherent factor both inside and outside a network.

While many enterprise leaders have undoubtedly heard of the term and the concept, more breaches and the shift to hybrid work makes zero trust an imperative for both IT staff and executives.

Early iterations of zero trust were simplistic and basic — users were typically verified just once, or maybe occasionally after that, then left to do what they would on a device or network.

But today's modern enterprises must take that a step further through constant, continuous trust verification based on least privileged access. Every single access request must be thoroughly validated and inspected and the appropriate security policy applied, then dually and triply authenticated, constantly throughout the entire connection.

Consider this zero trust network access (ZTNA) 2.0.

Think of the concept of zero trust 2.0 as a 21st century, post-9/11 airport: When a traveler enters the facility, they first go through a metal detector; then through the baggage check/boarding pass line; then through security to their gate; then finally onto the plane. At every single one of these points, they are stopped and must provide credentials.

With zero trust 1.0, comparatively, that same traveler might go to the same airport the next day and be allowed to skip all those checkpoints because they were verified and allowed through once before.

When combined, zero trust network access and SASE — which integrates software-defined wide area network (SD-WAN) with network security solutions into a single, cloud-delivered service — can prove a formidable line of defense and supplement several other key features including:

- Elastic networking, a centralized controller-based architecture that simplifies connectivity through automatic network topology updates and access list changes through zero-routing operations.
- Direct app-to-app architecture to all applications — including SaaS, cloud, internet and private — to ensure performance.
- Automation of complex IT operations through artificial intelligence (AI)/machine learning (ML).

Selecting the Right Tool

Still, zero trust must be integrated correctly. According to Gartner, 60% of organizations will embrace zero trust as a starting point for security by 2025, but more than half will fail to realize the benefits.

To ensure success, the right zero trust tool must provide integrated and cloud-delivered security services to branch offices, no matter where they are located.

Security must be granular — what's known as Layer 7, which is considered to be the highest level of security at the application level, because information is evaluated based on the actual application being used. This enforces true least-privilege access and ensures that only the right people get access to the right information and assets, and only at the time and place they truly need them.

Optimal tools must also provide visibility into all assets, including rapidly growing IoT devices, to ensure that the right controls and policies are applied to the entire network.

Just as importantly, tools should include robust AI, ML and automation capabilities to simplify the process and to provide valuable data, analytics and insight that can be actioned on in real time and inform future policies and protocols.

The Prisma SD-WAN Advantage

Palo Alto Networks' Prisma SD-WAN simplifies operations by merging networking and security into a single service and enabling zero trust access with a single click.

Users and their SD-WAN device are automatically connected to the closest available Prisma Access node, and the system automatically discovers and secures apps. This takes place continually across the branch landscape, with hundreds to tens of thousands of devices connected to the closest nodes

Least privileged access is enabled via continuous security inspection and continuous trust verification of user, app and device IDs. This protects all users and consistently secures all applications across enterprises, including modern, cloud native, legacy private and SaaS apps. It is globally available — branches have the same kind of trust and security regardless of where they are located or from where (and how) their users are connecting.

Prisma SD-WAN offers layer 7 visibility, highly distributed security and continuous trust verification and traffic inspection. Security, performance and visibility are extended to all devices — including IoT, regardless of manufacturer or operating system. Furthermore, AI/ML capabilities automate processes and policies, continuously monitor the network, detect attempted or successful breaches and recommend best practices.

Business Benefits of Integrated SD-WAN/SASE

With Prisma SD-WAN, enterprises get three distinct benefits:

- “Best of breed” security for people, apps and things
- A unified, centrally managed tool that simplifies day-to-day operations
- A better user experience: The system always connects users to the closest proximity node, whether they’re in San Francisco or Australia (or beyond)

This is all enabled via several different elements, including:

- Sub-app access control. Prisma SD-WAN can identify, prioritize and traffic engineer numerous business-critical, SaaS and cloud applications.
- Active-active app access. The platform creates fully automated, proprietary overlay tunnels to Prisma Access that allow it to be used in active-active and active standby connections.
- Simplified integration with API-based CloudBlade architecture with zero service disruption. This provides automated connectivity to Prisma Access’s global presence at scale.
- Rotating security keys. Encrypted overlay tunnels are periodically rotated and renewed from the cloud controller, providing better security for branch-to-cloud app traffic.
- Unified management. Prisma SASE and Prisma Access can be accessed in a unified console and managed from the same interface. This helps provide visibility into the threat landscape, security alerts and critical network events.
- A single unified data lake for all data /metrics including networking, security and experience. This allows the platform to seamlessly correlate data, cross-reference user and application identification and glean security insights.

With Prisma SD-WAN, everything sits under one umbrella. Operations are simplified across a secured, highly visible network. One-click deployment protects users, apps, the network and IoT. AI/ML and automation constantly scan for suspicious activity and provide critical business insights.

Your Branch Has Changed. Your SD-WAN Should, Too

Today’s modern enterprise — and that of the future — must be integrated, connected, visible and digital-first.

And above all, it must be secure.

Considering the ever-evolving threat landscape, today’s enterprises can’t afford to do anything but enforce zero trust — and on a continual basis — for people, apps and things. This is particularly effective when combined with SD-WAN and SASE via an integrated, end-to-end solution.

Learn more about how Prisma SD-WAN can secure your branch of the future — today.

PRISMA® SD-WAN
BY PALO ALTO NETWORKS

About Prisma SD-WAN

Palo Alto Networks Prisma SASE powers the branch of the future that is hybrid, digitized and secure with next-generation SD-WAN. Unlike the Gen-1 SD-WAN solution, it provides flexible and resilient connectivity on any WAN and application SLAs. Furthermore, it provides Zero Trust security for users, apps and IoT devices, and automates Day 2 operations with AIOps. As a result, businesses can seamlessly deliver exceptional user experience, secures their network holistically (incl IoT), and simplify complex IT operations.

www.paloaltonetworks.com/sase/sd-wan

sdxcentral®

About SDxCentral

SDxCentral is a B2B media and martech company. On the media side, we leverage our expertise to empower IT professionals to make better decisions for their organizations while advancing their careers. Our content educates and informs cloud, networking, and security professionals working in operations, development, and leadership within large enterprises and service providers. On the martech side we use buyer engagements to understand and predict intent, connecting our clients with engaged IT professionals. Combined with data-driven custom content, our martech solutions enable industry professionals from corporate marketing to product marketing and sales to influence IT buyers and turn them into customers.

www.sdxcentral.com