ZTNA 2.0: The New Standard for Securing Access

Secure the Hybrid Workforce in a World Where Work Is an Activity, Not a Place

Table of Contents

Introduction

The past two years have dramatically changed all aspects of how and where we now work. Initiatives that were already underway, such as working remotely and cloud transformation, were suddenly and deliberately accelerated to accommodate our new realities. We now work in a world where work is no longer a place we go. Instead, it's something we do.

As a result, the attack surface has increased exponentially, with many architectures now supporting direct-to-app connections versus backhauling traffic to data centers.

What's more, legacy remote access architectures further complicate the situation by providing too much access with little to no threat or vulnerability detection, leaving privileged resources vulnerable to user account compromise.

At the same time, we are seeing a dramatic increase in the volume and sophistication of cyberattacks. Ransomware operators have been especially busy during the pandemic, realizing lucrative returns from their exploits.

It's clear the legacy approaches for secure remote access and out-of-date architectures—like the initial iteration of Zero Trust Network Access (ZTNA)—are not able to handle the onslaught of new and increasingly sophisticated attacks across our exploding attack surfaces.

Apps Are Everywhere

80% of organizations have a hybrid cloud strategy.[1]

The average organization uses 110 SaaS apps.[2]

The Five Limitations of ZTNA 1.0

First-generation ZTNA solutions—we'll call them ZTNA 1.0—were introduced almost a decade ago, back when the threat landscape, corporate networks, and how and where people worked were vastly different. Today, ZTNA 1.0 solutions no longer align with the new world of work, and malicious actors are diligently finding ways to exploit the limitations of these ZTNA 1.0 approaches.

Before we explore the gaps that exist now, let's look at what ZTNA 1.0 was built to protect.

ZTNA 1.0 was designed to protect organizations by limiting their exposure and reducing their attack surface. It works as an access broker to facilitate connectivity to an application. When a user requests access to an application, the access broker determines whether the user should have permission to access an application. Once the permission is verified, the access broker grants access, and the connection is established.

And that's it. The broker is no longer in the picture, and the user is now given complete access to the application without any additional monitoring from the security system.

This is the architectural model of ZTNA 1.0. This model isn't just problematic in the context of today's threat landscape—it's dangerous. Here's a look at five reasons sticking with ZTNA 1.0 may cause more harm than good when it comes to battling today's cybersecurity threats.

Users Are Everywhere

76% of employees want to continue working from home at least part of the time.[3]

1. Violates the Principle of Least Privilege

The first issue with the ZTNA 1.0 model is it violates the principle of least privilege. When you hear the term Zero Trust, it implies that nothing is inherently trusted. The intent is to ensure least privilege by connecting a user to an application and nothing else.

In fact, all vendors offering ZTNA 1.0 solutions talk a pretty good game about this very principle, arguing against giving access to broad network segments by granting access to applications. However, the reality with existing ZTNA 1.0 solutions is that application access is managed at Layer 3 and Layer 4 of the OSI model—the network and transport layers—using only IP address and TCP/UDP port constructs.

A network is not the same as an application, yet ZTNA 1.0 solutions rely on network-level access controls to provide users application-level access. Unfortunately, relying on policy at Layer 3 and Layer 4 creates a number of problems. For example, if an app uses dynamic ports or IP addresses, you must grant access to broad ranges of IPs and ports, exposing more surface area than necessary. Access cannot be restricted at the sub-app level or app function level either; access can only be granted to entire apps.

Ransomware Made a Big Impact in 2021

518% increase in ransomware attacks from 2020.[4]

171% increase in ransom paid by organizations in the US, Canada and Europe from 2020.[5]

1. *Flexera 2021 State of the Cloud Report*, March 9, 2021, Flexera, https://www.flexera.com/about-us/press-center/flexera-releases-2021-state-of-the-cloud-report.
2. "Average number of software as a service (SaaS) applications used by organizations worldwide from 2015 to 2021," Statista, February 16, 2022, https://www.statista.com/statistics/1233538/average-number-saas-apps-yearly/.
3. *The State of Hybrid Workforce Security 2021*, Palo Alto Networks, August 15, 2021, https://start.paloaltonetworks.com/state-of-hybrid-workforce-security-2021.
4. *Unit 42 Ransomware Threat Report*, Unit 42, March 24, 2022, https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html.
5. Ibid.

And any malware that listens on the same allowed IP addresses and port numbers can freely communicate and spread laterally. The bottom line is that ZTNA 1.0 grants far too much access than is actually required, violating the principle of least privilege.

2. Follows the "Allow-and-Ignore" Model

The second issue with ZTNA 1.0 solutions is their reliance on the allow-and-ignore model. This model is very risky.

Why is the allow-and-ignore model risky? Once the access broker establishes the connection between the user and the application they are trying to access, that connection is trusted for the duration of that session, and all user and device behavior for that session goes unchecked.

Assuming trust can be verified only once and not checked again is a recipe for disaster. A lot can happen after trust is verified. User and application behavior can change, and applications can be compromised.

Security breaches can't happen unless someone or something is allowed in to wreak havoc and cause harm, and many modern cybersecurity threats only piggyback on allowed activity to avoid triggering alarms.

3. No Security Inspection

In addition to trusting whatever gets access to the network, ZTNA 1.0 solutions don't inspect application traffic either. Once a connection is established, ZTNA 1.0 trusts that active session implicitly, therefore performing no additional traffic inspection. If the device is compromised and malware is introduced into the session, there is no means for a ZTNA 1.0 solution to detect any malicious or other compromised traffic and respond accordingly. This turns ZTNA 1.0 into a "security-through-obscurity-only" approach that further puts organizations, their users, apps, and data at risk of malware, compromised devices, and malicious traffic.

4. No Data Protection

ZTNA 1.0 solutions don't provide data protection—especially the data within private applications. This leaves most of the organization's traffic vulnerable to data exfiltration from malicious insiders or external attackers and requires completely different data loss prevention (DLP) solutions to protect sensitive data in SaaS applications. ZTNA 1.0 introduces more complexity and risk as it requires organizations to use multiple point products to secure data everywhere.

5. Inability to Secure All Apps

ZTNA 1.0 solutions don't provide coverage for all applications. They don't support cloud-based apps or other apps that use dynamic ports or server-initiated applications—like support help desk apps that employ server-initiated connections to remote devices. ZTNA 1.0 solutions don't support SaaS apps either.

Modern cloud native apps are comprised of many containers of microservices, often using dynamic IP addresses and port numbers—a recipe for disaster. ZTNA 1.0 access control becomes completely ineffective in these sorts of environments, as it requires access to be opened up for broad ranges of IPs and ports, defeating the point of Zero Trust.

As more and more organizations continue on their cloud journey and run their businesses on cloud native applications, ZTNA 1.0 becomes obsolete.

The Advent of ZTNA 2.0

We've seen the digital transformations organizations have underway to run efficiently and provide employees access to all the tools they need—no matter where they choose to work.

This transformation manifests itself most visibly in how employees now access these tools, connecting directly to the applications they need to get their work done. And it shouldn't matter whether the employee is at home, on the road, or in an office; the expectation is that each employee will be given access to the applications they need to perform their work without increasing the organization's attack surface.

This transformation requires a paradigm shift in cybersecurity. This paradigm shift is ZTNA 2.0.

The Five Tenets of ZTNA 2.0

There are five key tenets of ZTNA 2.0.

1. ZTNA 2.0 uses the most stringent enforcement of the principle of least privilege, providing access control from the network layer—Layer 3—all the way to the application layer—Layer 7.
2. ZTNA 2.0 delivers continuous trust verification. When a user's behavior changes, an application's behavior changes, or device posture changes, there has to be a continuous assessment of the trust level granted and the ability to react—in real time—to any and all changes.
3. ZTNA 2.0 delivers continuous security inspection for all traffic to protect against all threats and threat vectors.
4. ZTNA 2.0 protects all data, and it does this consistently across all application data, from the data within applications running on legacy mainframes all the way up to the data stored in modern, cloud native and collaboration applications.
5. ZTNA 2.0 protects and secures all applications across the entire organization, including Private apps, cloud apps and SaaS.

These five key capabilities overcome the limitations of ZTNA 1.0 solutions and provide better security outcomes to support the digital transformation, and hybrid workforce needs facing organizations today. Let's take an in-depth look at each tenet.

1. Least-Privileged Access

At Palo Alto Networks, we invented App-ID™, User-ID™ and Device-ID™—all of which deliver rich context and a more granular approach to allowing access to applications. But it's not a "one-and-done" situation with ZTNA 2.0. We don't just check the user ID and how it has interacted with the FQDN or IP ports and call it a day.

ZTNA 2.0 requires App-ID capabilities to be stateful. This means we continuously gather information about the transmission control protocol (TCP) session, the application handshakes, the application behavior, the stateful protocols, and more. At the same time, User-ID and Device-ID controls continuously gather information about users and the device.

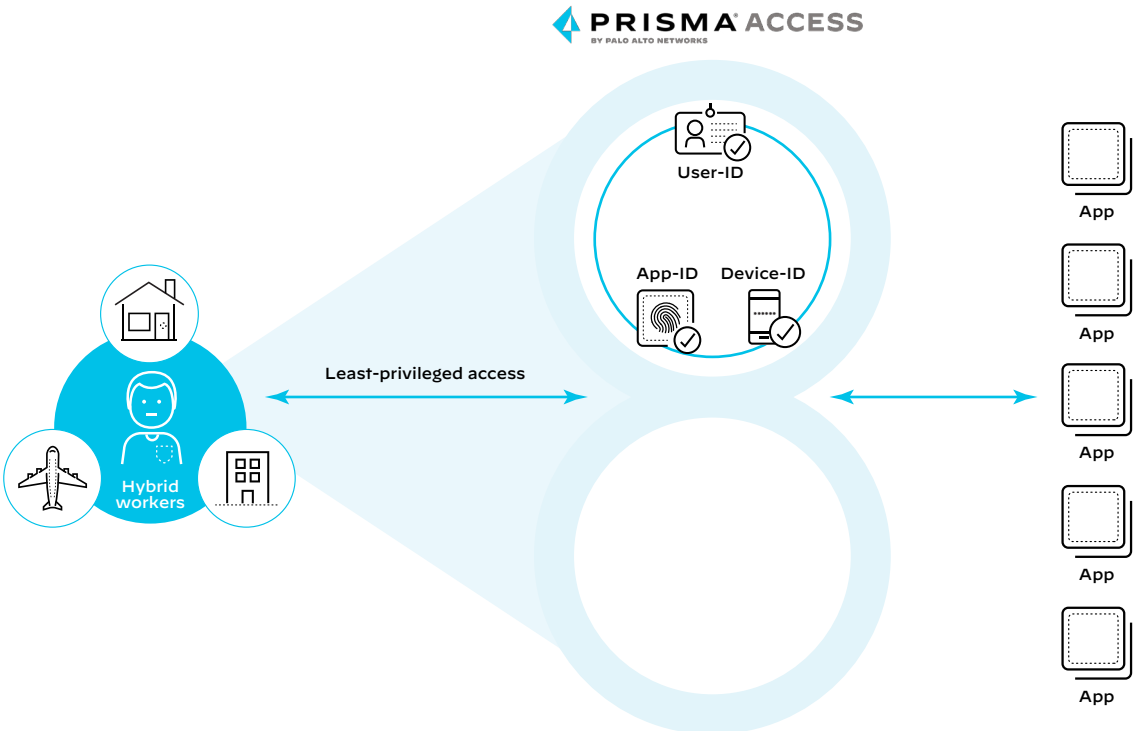

Figure 1: Palo Alto Networks uses App-ID, User-ID and Device-ID to facilitate comprehensive least-privileged access

When you combine App-ID, User-ID and Device-ID access controls, you move beyond simple point-in-time trust assurances and gain an environment that now provides rich contextual information for making better decisions. Organizations can enable access for any user on any device to the specific application they request and continuously gather additional context to react to changes in real time.

2. Continuous Trust Verification

Prisma Access provides continuous trust verification even after access to the app has been granted. Continuous trust verification capabilities continuously monitor and verify device posture or any changes to it, along with user and application behaviors, to respond in real time.

The core principle of Zero Trust is to remove implicit trust. However, without continuous trust verification, the system assumes that the user and the app will behave in a trustworthy manner forever once a connection is established. However, we know a lot can happen after trust is verified, including user and application behavior change or compromise.

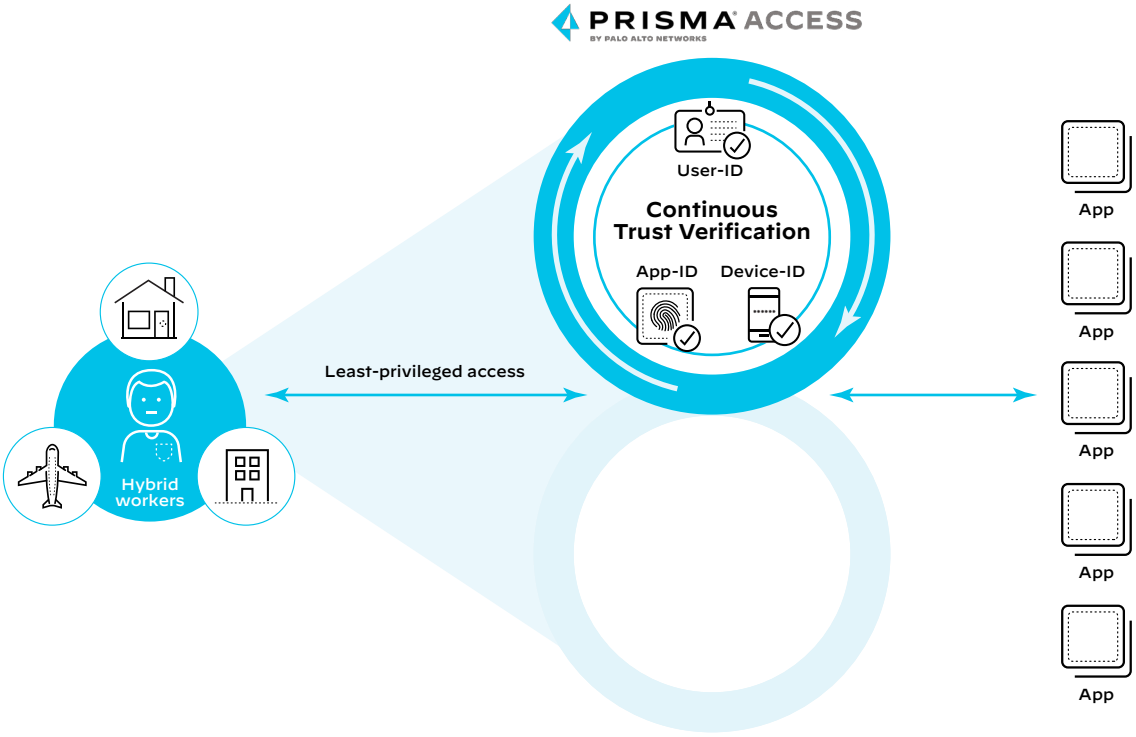

Figure 2: Continuous trust verification continuously monitors device posture, application behavior, and user behavior even after users gain application access

3. Continuous Security Inspection

Prisma Access provides continuous security inspection withWildFire®, Advanced URL Filtering, Threat Prevention, SaaS Security, DNS security and more. We also perform deep and ongoing security inspection that includes allowed connections and zero-day threat monitoring. With our AI and ML-powered threat prevention technologies, we stop 95% of zero-day threats inline. This means you don't need a first victim or have to wait for signatures to be updated to be protected—your environment is instantly protected.

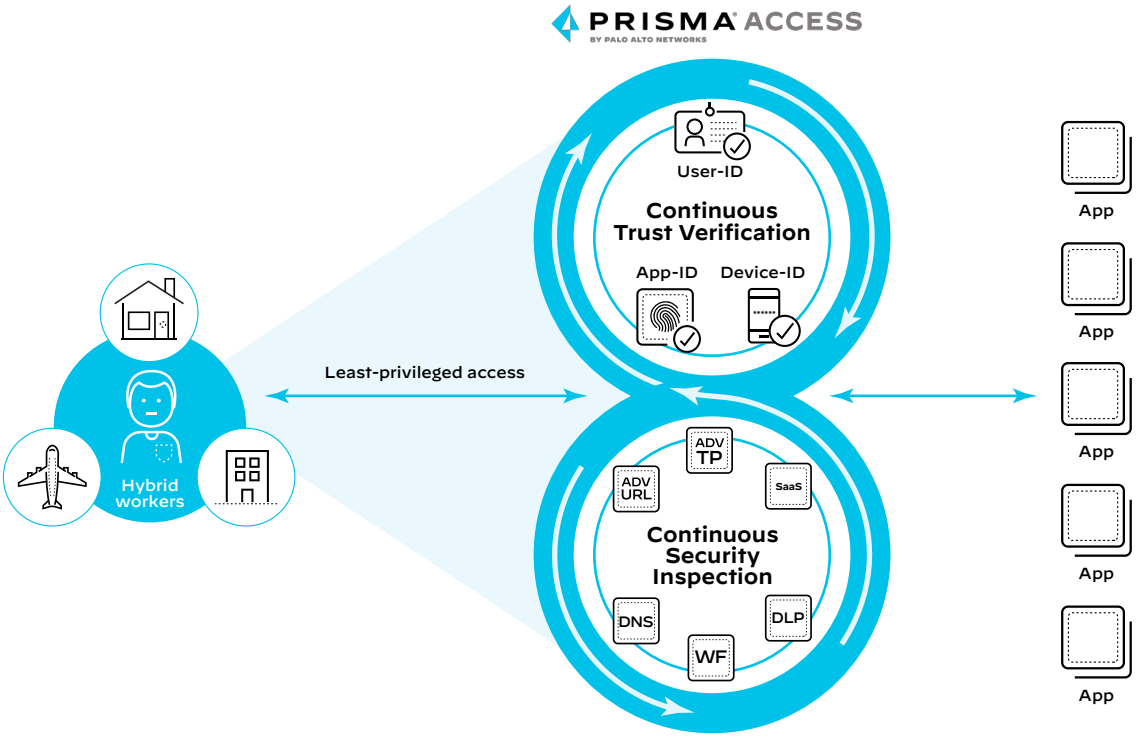

Figure 3: Continous security inspection is always monitoring to prevent and protect your environment from threats

4. Consistent Protection for All Data

Prisma Access applies advanced DLP capabilities consistently to all application data. This means we provide the same DLP policy to the data within private apps and SaaS apps, eliminating the need to guess which apps are protected and what data is secure. Organizations realize strong data protection and security policies across their apps from a single solution.

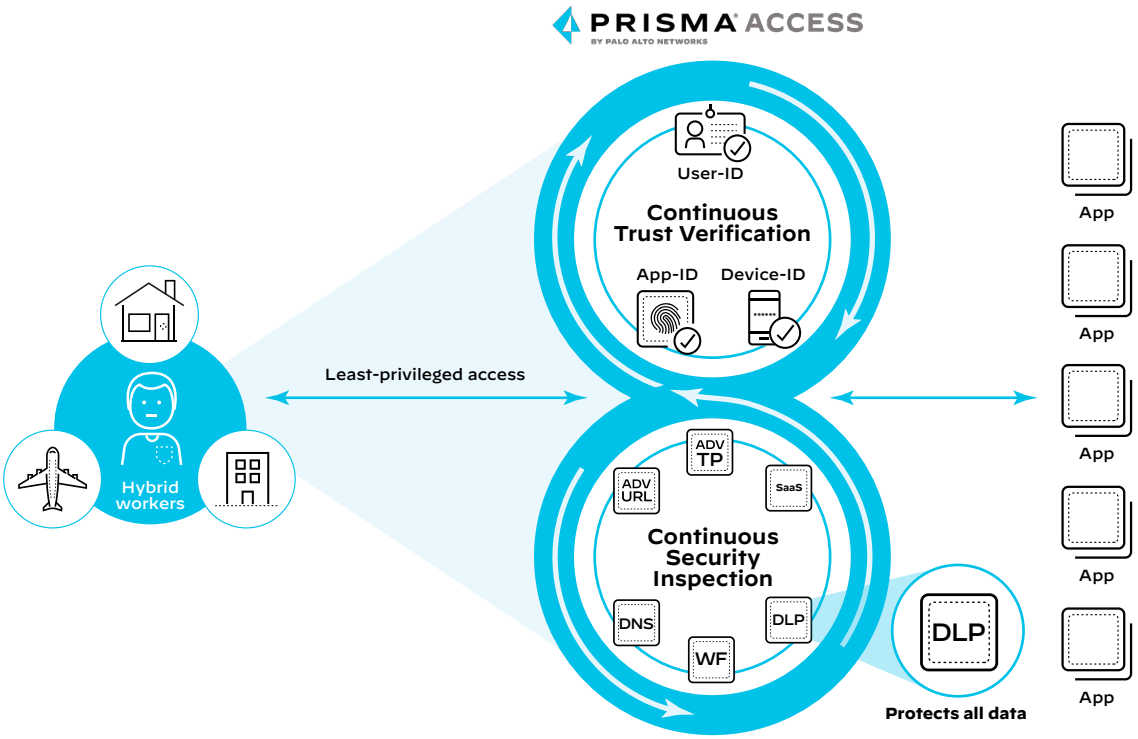

Figure 4: Consistent data protection applies the same strong data protection and security policies across your environment

5. Consistent Security for All Apps

Prisma Access provides consistent security for apps all across your organization. It can be a modern cloud native microservices-based application that doesn't get restricted by IPs and ports, a SaaS app, a traditional private app or legacy app.

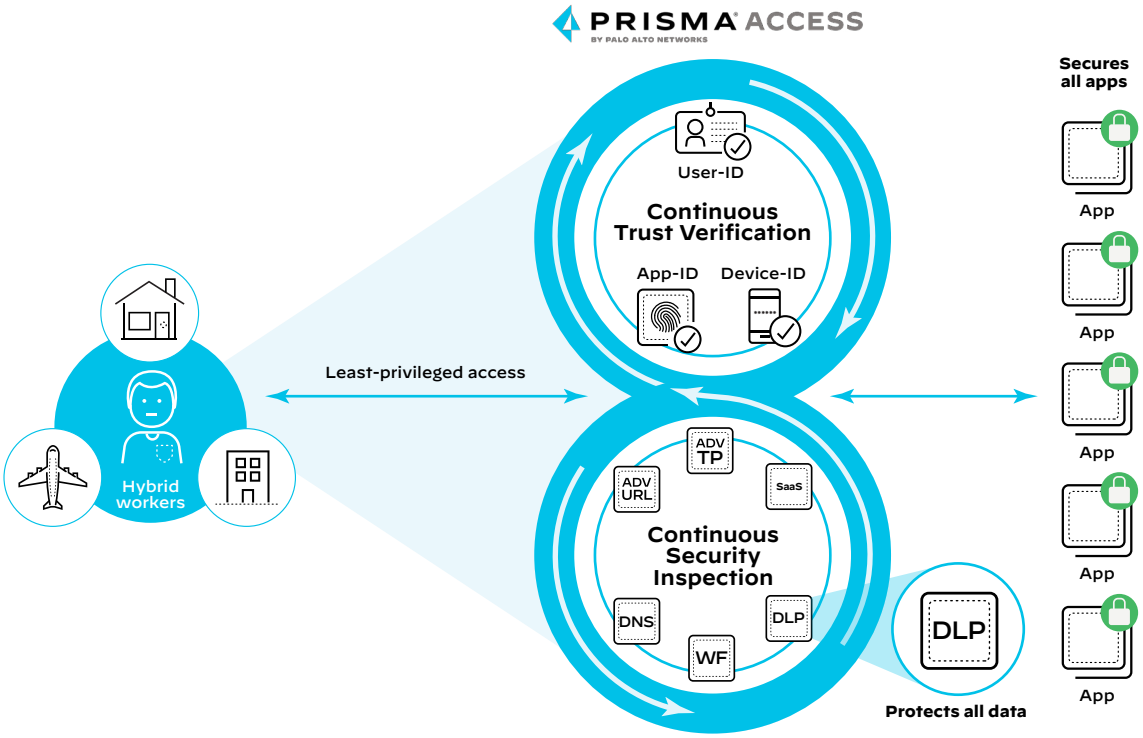

Figure 5: It doesn't matter if your apps are legacy, private, or cloud native—we provide consistent security for all of them

Prisma Access: The ZTNA 2.0 Engine

Prisma® Access provides the industry's only cloud-delivered ZTNA 2.0 solution designed around an easy-to-use, unified security product that delivers the best user experience. Overcoming the shortcomings of legacy solutions, only Prisma Access consolidates best-of-breed capabilities, such as ZTNA 2.0, SWG, Next-Gen CASB, FWaaS, DLP, and more, into a cloud native global services edge that:

- Securely connects all users and all apps with **fine-grained access controls** to dramatically reduce the attack surface
- Provides behavior-based **continuous trust verification** after users connect
- Provides **deep and ongoing security inspection** to ensure all traffic is secure without compromising performance or user experience
- Provides consistent visibility with a single DLP policy to **secure both access and data**
- **Secures all apps, all the time**, including premises-based, internet-based, legacy, SaaS, and modern/cloud native apps from a single product

The unique architecture of Prisma Access is built in the cloud to secure at cloud scale with true multitenancy while ensuring all customers are isolated from each other.

Leveraging the elastic scale of the largest cloud providers in the world along with access to dedicated premium fiber networks, Prisma Access delivers industry-leading SLAs for security processing as well as app performance.

What's more, the native Autonomous Digital Experience Management capabilities provide proactive identification and resolution of potential problems before a user even knows about them. These capabilities guarantee the **best possible performance and user experience**.

Three ZTNA 2.0 Starting Points for Your Organization

Getting started with ZTNA 2.0 should not be difficult, overwhelming, or come with compromises. It boils down to alignment—mapping needs to the key concerns or challenges most organizations face to solve their challenges without requiring a massive architectural shift or business disruption.

Here are the three key projects where you can begin implementing ZTNA 2.0 into your organization today:

- **VPN replacement project**. Move away from on-premises VPN concentrators and poor performing backhauling architectures, inefficient network paths, and expensive-to-manage infrastructure.
- ***SWG replacement project***. Move away from premises-based and legacy proxy architectures to a modern, cloud-based approach to secure users accessing web and internet tools.
- **Advanced SaaS app security or Next-Gen CASB project**. Modernize security for and regain control over the explosion of SaaS applications, limit exposure, provide better protection for sensitive data, and get a handle on shadow IT.

Starting Point 1: VPN Replacement Project

Replace legacy remote access outdated VPN technologies that deliver network access to the remote and hybrid workforce with a more modern ZTNA 2.0 solution that overcomes performance bottlenecks and simplifies management.

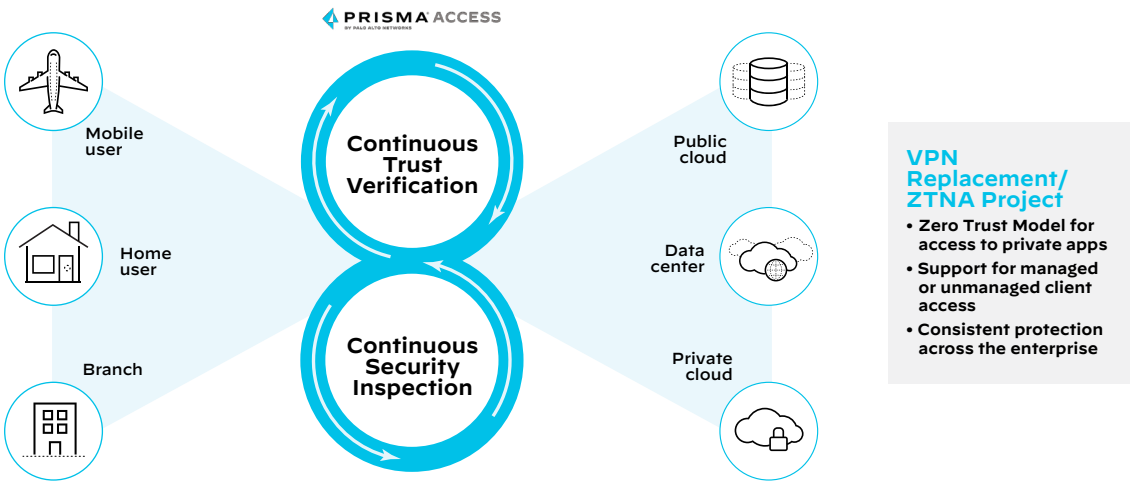

Figure 6: ZTNA 2.0 removes the challenges VPN brings to securing remote and hybrid workforces

VPN replacement initiatives are driven by a number of factors:

- Applications moving to a true hybrid model—taking advantage of on-premises, cloud, and multi-cloud environments. Legacy VPN technology that trombones or backhauls traffic to a premises "concentrator" doesn't scale or deliver the best possible user experience in this new model.
- Changes in enterprise app access requirements. Traditionally, employees used managed devices to complete work-related tasks. However, more and more unmanaged devices have made their way onto corporate networks and can access corporate applications.
- Organizations looking for consistent and universal protection and security model for all apps, not just web or legacy applications.

While there are a number of solutions that can address some of those needs, only ZTNA 2.0 with Prisma Access helps transform networking and security to support both managed and unmanaged devices while delivering consistent security protection across the entire organization.

Replaced VPN to Secure Thousands of Employees Worldwide

With Prisma Access, this customer is able to connect all 350,000 users across 158 countries consistently while also providing secure direct-to-internet connectivity for the hundreds of branch offices across the globe. What's more, Prisma Access ensures consistent and secure access to all apps, including legacy apps, across 30+ data centers and cloud locations.

- The primary driver for this Fortune 100 consulting services company was to retire their aging, multivendor unscalable VPN solution connecting their remote employees and sites to corporate resources.
- Because of the hodge-podge nature of the VPN solution, they were struggling to attain consistent visibility and security across the sheer volume of employees and locations around the globe.
- Employee satisfaction with the previous solution mix was very low, as employees experienced slow connectivity, unreliable performance, and inconsistent experience from site to site and location to location.

Starting Point 2: SWG Replacement

Many organizations are looking for ways to improve their employee experience when accessing web applications. Rather than dealing with the latency that comes with backhauling web traffic to corporate data centers before delivering the requested content to wherever an employee is located, the cloud SWG capabilities within Prisma Access remove the latency and improve the security capabilities.

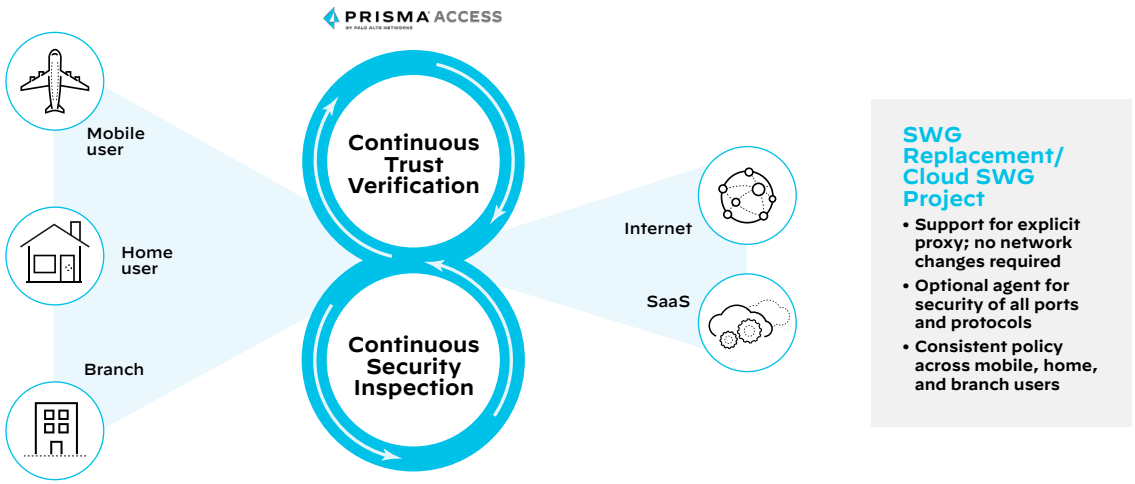

Figure 7: ZTNA 2.0 with Prisma Access removes the latency frustrations experienced with traditional SWG implementations

Prisma Access future proofs the ZTNA 2.0 journey. At any point, an organization can choose to deploy agents to secure all ports, protocols, and applications. Prisma Access:

- Offers multiple connect methods to implement SWG for all hybrid users and branch offices—explicit proxy, agent, or clientless
- Makes it easy for organizations to move from legacy proxy to cloud-enabled secure access without making any network changes by simply updating their existing PAC files
- Integrates with Prisma SD-WAN to provide a seamless way to onboard to Prisma Access and offers consistency of security for all branch locations

Migrated from On-Premises to Cloud-Native Security

As more of the tools and apps employees needed to do their work were migrating to the cloud, existing solutions couldn't offer a seamless experience and match expectations, which caused poor overall user satisfaction with the current solutions.

This Fortune 100 pharmaceutical company wanted to reduce its multivendor, on-premises hardware deployments and modernize its infrastructure by deploying cloud-delivered security.

They chose Prisma Access to easily migrate all 100,000 users within three months without re-architecting their network, leveraging the explicit proxy capabilities of Prisma Access.

Their new cloud native solution consolidated and eliminated their on-premises proxy hardware and allowed them to realize an improved security posture across all users and locations. What's more, they also deployed the native autonomous digital experience management (ADEM) capabilities of Prisma Access to ensure exceptional user experiences for all hybrid workers.

Starting Point 3: Advanced SaaS App Security Project

The Next-Gen CASB capabilities within Prisma Access ensure complete coverage, securing all apps, whether on-premises or in the cloud. Organizations get full visibility into "shadow IT" and easy-to-use workflows to safely enable SaaS app usage to keep your business ahead of the SaaS application explosion.

Prisma Access offers the industry's broadest coverage for API-based protection of sanctioned SaaS and collaboration apps.

With advanced DLP for both private and public apps, Prisma Access Next-Gen CASB seamlessly extends consistent data protection across SaaS, network, branch offices and hybrid workforces. It also offers end-user self-remediation and incident response management.

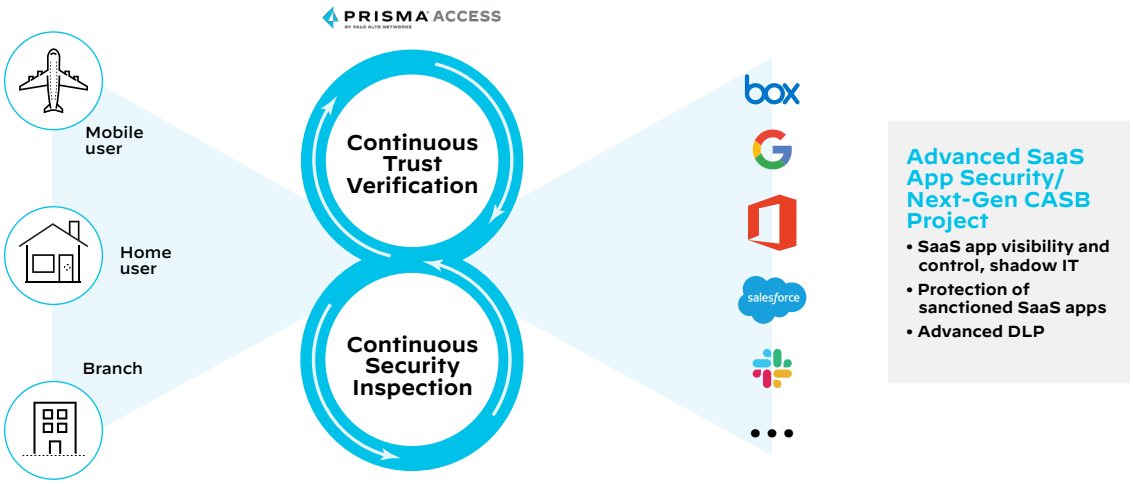

Figure 8: Next-Gen CASB capabilities within Prisma Access secure all apps, whether on-premises or in the cloud

Advanced SaaS App Visibility, Control, & Data Security

A global automotive technology leader, with more than 180,000 people across 124 manufacturing facilities, 12 major technical centers worldwide, and a presence in 44 countries, was relying on more apps in the cloud. They needed better visibility and granular control of known and unknown SaaS applications; consolidated management from the multiple vendors and products they were working with; and threat inspection.

They were also looking for simple policy creation and deployment without leveraging proxy or agents and desired to eliminate the need to synchronize risks, policies, and goals across a separate layer of the stack. Next-Gen CASB capabilities within Prisma Access enabled the organization to eliminate the requirement to update/configure agents for inline inspection and protect unmanaged endpoints.

Conclusion

With the five big challenges of the ZTNA 1.0 approach, you may be wondering, "How did ZTNA 1.0 even make it to the market?" It was a good solution to the cybersecurity challenges organizations faced years ago. However, the threat landscape has become more sophisticated and evolved, and the attack surface has exploded as a result of the hybrid network environments that have more people working outside controlled corporate environments, turning work into an activity, not a place.

ZTNA 2.0 ushers in a new era of secure access in a world where work is an activity, not a place. And Prisma Access is the industry's only ZTNA 2.0 security solution delivered in a simple, unified product, purpose-built to help you achieve ZTNA 2.0 success.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com