paloalto NETWORKS | PRISMA® ACCESS

Secure remote access. Simplified.

Unified remote access security and the performance people love with Prisma® Access.

The workplace today is undeniably hybrid. The way people work and the enterprise infrastructures that support day-to-day business are highly distributed worldwide.

Hybrid work and infrastructures offer greater flexibility. They can enable workers to stay productive no matter if they're in the office, in the field, in transit, or at home. Hybrid infrastructures can allow organizations space to benefit from the agility, scalability, and resiliency of the cloud—at their own pace.

To power that flexibility, enterprises need network connectivity that's as flexible as the business models they support. They also need to secure those connections and safeguard the people, data, and other resources that interact across highly distributed organizations.

Many traditional connectivity approaches—like VPNs—fall short of delivering the performance, security, and ease of management that modern enterprises require. It's time for a better approach.

Hybrid work is here to stay despite return-to-office mandates.

In 2023

5 in 10
worked hybrid

3 in 10
worked exclusively remotely

2 in 10
worked entirely on-site

Source: Gallup, "The Future of the Office Has Arrived: It's Hybrid," October 2023.

An outdated security solution.

Virtual private networks, or VPNs, have been around for decades and are widely used to provide remote employees secure connectivity to organizational data and resources.

In the mid-1990s, when VPNs were invented, the need for remote connectivity looked very different than it does today. Only a small fraction of employee populations needed remote access since most of the work happened in the office. Productivity was tied to apps and data residing on-premises in data centers within each office. This is the outdated way of working that VPN security principles were built for and still operate on today.

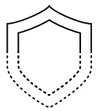
When the pandemic forced a rapid shift to remote work, VPN reliance increased exponentially, exposing its many limitations. Those limitations caused untold stress for IT and security professionals tasked with rapidly scaling secure access overnight. The stress of VPN limitations continue as workers move between remote and office locations.

Source: ESG, "Ten Considerations for Evaluating Zero Trust Network Access Solutions," September 2021.

A few of the more common constraints

Not easily managed or scaled

Setting up a new VPN requires investments in hardware, as well as the people to deploy and manage usage and maintenance. It's a mostly manual effort. When an organization needs to expand the reach of its VPN solution, it typically needs to invest in more resources, be it infrastructure or staff. There's a large cost, not just to procure and recruit more resources, but also in the time it takes to expand and maintain the VPN solution.



Limited security

Traditional VPN solutions protect access at the network perimeter. Once inside, users can move around unchecked to access all of the apps and data contained on the network. This is one reason why cyberattacks exploiting VPN vulnerabilities have exploded in frequency since the pandemic, as cybercriminals look to capitalize on the prevalence of remote and hybrid work.

Poor user experiences

VPN solutions are not always intuitive or easy to use. When connecting from home, employees may not have the technical expertise to successfully troubleshoot problems, leading to frustration. Employees will often experience slower connectivity when on VPNs, due to how traffic is routed and secured. That degraded experience can make employees reluctant to use VPNs, creating inconsistent security across the organization.

The bottom line

Using VPN solutions to meet the remote access needs of modern hybrid organizations can have material negative impacts, from increased security risks, to lost productivity, to higher costs to manage and scale.

Source: TechTarget, "Hackers targeting VPN vulnerabilities in ongoing attacks," April 2021.

Hybrid work makes network security more challenging.

59% find cybersecurity and management more difficult today.

41% see the increase in remote work as a factor making cybersecurity more challenging.

Source: ESG, "Ten Considerations for Evaluating Zero Trust Network Access Solutions," September 2021

A more secure approach.

Growing dissatisfaction with VPNs is leading enterprises to consider new remote connectivity approaches that are easier to deploy, high-performing and highly secure, and simpler to manage on an ongoing basis.

Chief among the alternatives is Zero Trust Network Access, or ZTNA, which has emerged as a leading method to securely connect employees to the apps and data they need to work, no matter where they are or how they connect.

An important advantage of ZTNA is that it moves companies away from providing wide-ranging network access through VPN. ZTNA enforces the core principles of Zero Trust:

- **Providing least-privilege access**, so that users are restricted to accessing only the specific apps and data they need to do their job, and no more.

- **Never trusting, always verifying**, meaning that every time a user requests access for an app, their identity and access rights are verified and they are continually checked, even after the initial verification.

With ZTNA, companies are in a better position to limit access in the event of a breach, reducing risk across the organization.

By 2025, Gartner predicts

70% of new remote access deployments will rely on ZTNA rather than on VPN services.

Source: Gartner Press Release, October 2022.

Transform your secure remote access.

Palo Alto Networks Prisma Access helps transform remote access and transcends the limitations of VPN. Providing high-performing secure remote access, Prisma Access not only reduces your exposure to threats, but also gives your people exceptional app experiences.

A cloud-delivered service, Prisma Access helps IT and security teams secure users, apps, and data at cloud scale, making it easier to expand access to as many employees as you need, at speed.

Turn hybrid and remote work into a competitive advantage with Prisma Access.

- **Solve for hybrid secure access and win over your workforce**. Deliver uncompromising security that doesn't get in the way of productivity. Your people will get the same great performance for on-premises, cloud, and SaaS-based applications, with secure direct-to-app connectivity and ongoing security inspection of traffic.

- **Dramatically reduce your exposure with granular, secure access**. Prisma Access uses the power of Zero Trust to focus security down to the individual user and application, reducing your attack surface.

- **Transform remote access management**. Manual access management will become a thing of the past. You'll be able to revolutionize how you safeguard and control remote access to critical systems and data through a solution designed to simplify and unify ongoing access management and operations.

Source: Forrester, "The Total Economic Impact™ Of Palo Alto Networks Prisma SASE," November 2023. Commissioned by Palo Alto Networks.

The **Prisma Access** difference

50% decreased likelihood of a data breach.

75% efficiency gains in managing secure access service edge (SASE) and making policy changes.

107% return on investment (ROI).

CUSTOMER SUCCESS

Better

Modernizing remote access at speed and scale.

Better, a digital-first homeownership company, wanted to modernize its approach to security across its network, endpoints, and security operations. Security is a big priority for the company, both for building trust with customers and for complying with state and federal regulations.

As part of its modernization vision, Better wanted to ensure secure online access for customers and employees. It had an existing VPN but wanted a cloud-based solution that would be easier to scale and manage–and more accessible for users to adopt, while offering greater data security.

Better was highly interested in Prisma Access, and began evaluating the solution with a proof of concept. During that time, the COVID pandemic ramped up. With help from Palo Alto Networks, the company was able to quickly and confidently pivot to remote work for its employees in just a few days.

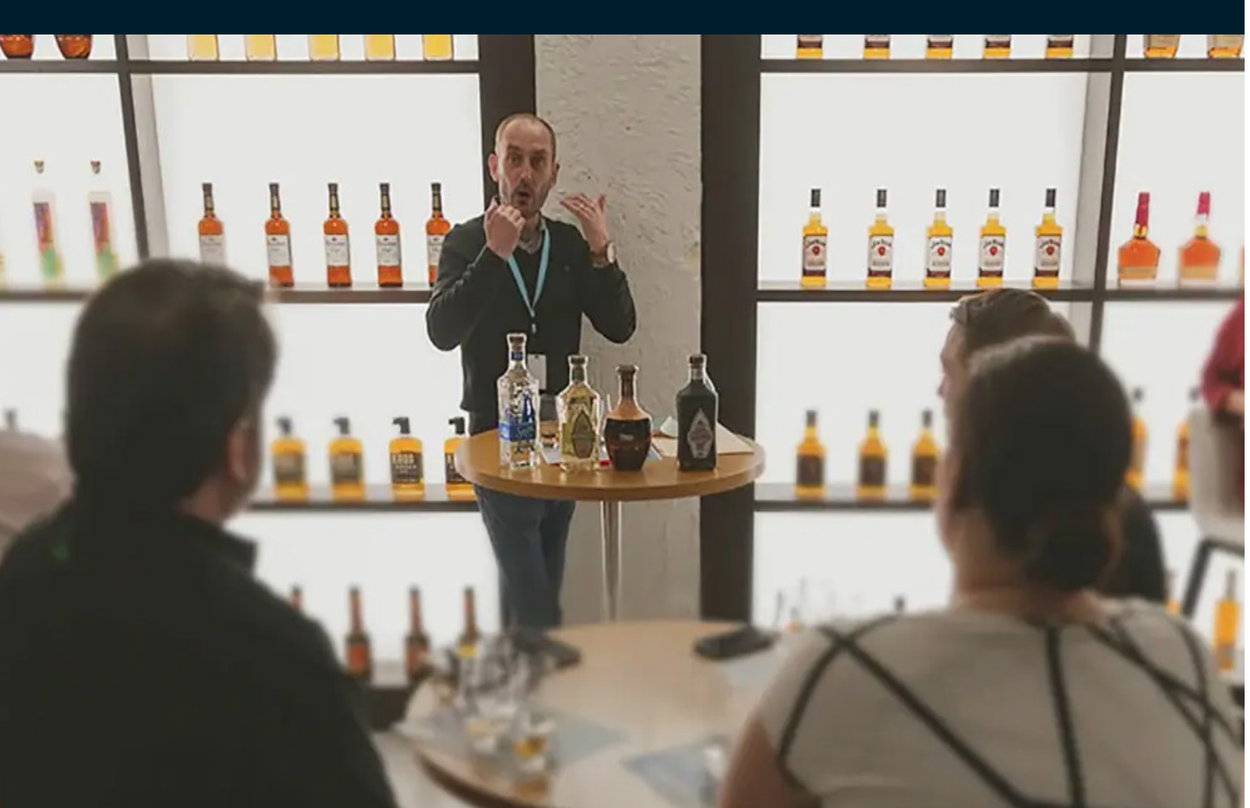
To read more about Better's security modernization journey, see the full story.

> "Prisma Access allowed us to securely deliver our software solutions internally to our employees anywhere in the world. That was a huge game changer."
>
> **- Ali Khan**, Chief Information Security Officer, Better

CUSTOMER SUCCESS

Beam SUNTORY

Improving security and performance.



The world's third-largest producer of distilled alcoholic beverages, Beam Suntory needed to take a new approach to security following a major security incident.

The company wanted to replace an aging networking and security estate that presented several challenges, from inconsistent protection, lack of scalability, losses of connectivity, and costly impacts to productivity.

While Beam Suntory initially approached its networking and security needs as two separate projects, the company realized it could combine its transformation efforts by adopting a SASE architecture.

With Prisma SASE, the company has significantly improved its security posture, network reliability, and performance. It's also simplified operations, making it easier to manage network and security components.

And when employees had to shift to remote work during the pandemic, Prisma SASE simplified that transition for the company. Rather than logging in through the data center, users could directly access the productivity tools they need in the cloud.

> "The product saved our lives and increased both the performance and the security level."
>
> **- Qun Wei**, Senior Network Architect, Beam Suntory

Next steps in your journey.

With Prisma Access, hybrid and remote work can turn into a competitive advantage. Give your people an exceptional experience while significantly reducing your exposure to risk and simplifying ongoing access management.

1

Learn more about how Prisma Access can deliver the secure remote access your people and IT teams will love.

2

Discover the superior ZTNA protection made possible by Prisma Access.

3

Talk to us and request a demo to see how you can transform secure remote access for your organization.

paloalto® NETWORKS | PRISMA® ACCESS