



# Extend your network security to where you need it.

Simplify secure remote access with a unified platform from Palo Alto Networks.





---

For decades, protecting the corporate network centered on hardware solutions residing in physical locations like data centers. Palo Alto Networks was born to address this security need through its Next-Generation Firewalls (NGFWs), offering protection for networks within headquarters, across campuses, and at office locations.

Yet, the demands on corporate networks haven't remained static over time. In the last few years, the rapid shift to remote and hybrid work has surfaced new security challenges for enterprise organizations.

Work is no longer a place and can be carried out anywhere. Organizations need a flexible and scalable approach to secure users and apps that extends the same level of protection established on-premises to anywhere.







## As work styles evolve, so must network security.

Hybrid work is prevalent today. Many return-to-office mandates don't require five full days in the office, still allowing employees to work remotely part of the time.

When employees work from home or any other remote location, organizations must contend with more variables to be secure. There are new risks to be considered, for example:

- If an employee is using their own device at home, how secure is it?
- Can organizations verify that the person logging in from home is indeed their employee?
- Should the employee have the same level of access at home?
- What kinds of apps will the employee need to access throughout the day?

**Preference for hybrid work remained strong in 2023.**

**5 in 10** worked hybrid

**3 in 10** worked exclusively remotely

**2 in 10** worked entirely on-site



# The challenge

For many organizations, adapting to these realities is not easy. Some of the more common problems include:

## OVERLY COMPLEX MANAGEMENT

While organizations may have robust protections in place for the office environment, they likely need to onboard new solutions to address security for distributed users, apps, and data. However, new tools don't always integrate well with existing security solutions. That can result in greater management complexity for IT and security teams, who end up using multiple dashboards for a full security picture.

## CUMBERSOME WORKAROUNDS

Alternatively, network teams might rely on existing hardware firewalls to secure remote work. This approach typically involves backhauling internet, cloud, or SaaS traffic through those firewalls. Users are now protected, but there's often a cost to the performance of the network itself. Connections become slower and applications take longer to respond.

## INCONSISTENT SECURITY

When organizations rely on multiple point products to secure users, it's more difficult to enforce consistent levels of security across the business. It takes a lot more time to manage access, set policies, and review logs and reports for all users, apps, and security postures across the organization. It's also easier to make unintentional errors.







**Unify your network security posture.**

Next-Gen Firewalls



Prisma® Access

---

## **A simpler, better approach.**

Securing the shift to hybrid work doesn't have to mean greater management complexity or degraded performance for your employees. IT teams shouldn't have to choose between enforcing your company's security standards or enabling great remote user experiences.

An easier path is available with Palo Alto Networks. Now it's possible to extend the network security posture established with NGFWs with Prisma® Access, a cloud-delivered service optimized to protect distributed users and apps.

Prisma Access seamlessly integrates with Palo Alto Networks NGFWs. Easily retain the same security policies already in place and extend them to wherever employees are, dramatically simplifying security management.



## When you add Prisma Access to your network security portfolio, you gain:

### ▶ TRUSTED SECURITY

Companies can count on best-in-class security everywhere from Palo Alto Networks, a vendor they already know and trust. By leveraging the de facto standard for secure access, organizations will be able to deliver it to all users and apps through a globally distributed, highly scalable, cloud-delivered service. Prisma Access enables fine-grained, least-privileged access control, reducing organizations' attack surface while providing deep and ongoing AI-powered security inspections for real-time protection.

### ▶ STREAMLINED OPERATIONS

Drive efficiencies and consistency through a familiar, unified management environment. With a unified management approach, dramatically simplify enforcement of consistent security policies across on-premises, cloud, and distributed environments. Also, because employees will be using familiar interfaces and integrated solutions, they can accelerate operational tasks.

### ▶ EXCEPTIONAL VALUE

Extract more value from a consolidated approach to network security. Because Prisma Access seamlessly integrates with existing Palo Alto Networks security environments, IT and security teams can immediately be productive in protecting your distributed users, apps, and devices. Both employees and IT teams will save time and be able to focus on their most important priorities.

## 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



# Driving digital innovation with a modern network security platform.



Sumitovant Biopharma, a patient-first, technology-driven biopharmaceutical company, embraced digital transformation to achieve its goals of getting research-supported drugs to market faster and improving patient lives.

When it came to network security, the company chose Palo Alto Networks as its partner. Palo Alto Networks Next-Generation Firewalls and GlobalProtect® network security client allowed the IT team to get users online securely.

When the pandemic hit, Sumitovant explored other options to connect workers as they worked from home. The IT team selected Prisma Access to replace its VPN and provide least-privileged secure connectivity for their workforce.

Read the [full story](#).

**“The Network Security Platform allows us to focus on what’s really important, which is moving into the future with modern technologies and not managing mundane day-to-day security tasks that should be automated.”**

**Trevor Cardwell**  
Senior Cloud and Network Architect  
Sumitovant Biopharma





# Adopting a no-compromise security posture.

Imagination Technologies Group, a semiconductor company, had an aging cybersecurity infrastructure that struggled to keep pace with business growth. The company launched a “Cyber Transformation Program” to help transform its cybersecurity capabilities.

Imagination selected Palo Alto Networks to help it secure across its network, endpoints, and clouds, and realize a modern, “no compromise” security strategy, including:

- NGFWs, together with Cloud-Delivered Security Services (CDSS), were deployed to every site to instantly prevent new threats, automate processes, and extend visibility into all applications, users, and devices, including IoT.
- Cortex XSIAM was added to deliver automated end-to-end threat management wherever threats originate.
- Prisma Access provides always-on, secure remote access for over 1,000 users regardless of location.
- Unit 42® Managed Threat Hunting provides 24/7 threat hunting anywhere in the environment, across managed and unmanaged devices and remote users.

Read the [full story](#).

**“This is frictionless, no-compromise security at its very best. Everything connects seamlessly with Palo Alto Networks—the technologies, the people, and the future roadmap.”**

**Paul Alexander**  
Director of IT Operations  
Imagination Technologies Group



# Get started today.

Achieve a consistent security posture wherever work gets done with the combination of Next-Generation Firewalls and Prisma Access.

Provide a more seamless experience for employees while simplifying network security management.

Expand on the exceptional value of existing Palo Alto Networks investments with an integrated approach and a familiar, easy-to-use interface.

Learn more about how [Prisma Access](#) can extend network security.

[Talk to us](#) and request a demo to see it in action.





