FORRESTER®

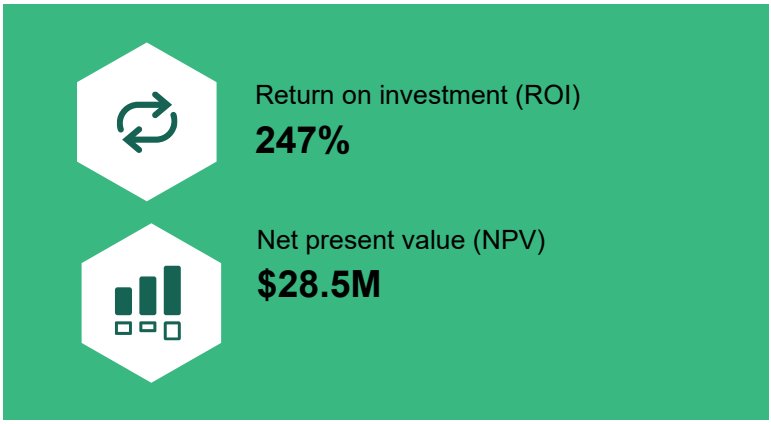
TEI Spotlight:

Provide Secure Remote Access And Gain Peace Of Mind With Palo Alto Networks Prisma Access

Forrester recently spoke with multiple Palo Alto Networks customers regarding their investment in Prisma Access as part of a Total Economic Impact™ (TEI) study.[1] Through these interviews, Forrester uncovered various benefits from customers' adoption of Prisma Access, a cloud-delivered network security solution that is part of Palo Alto Networks secure access services edge (SASE) platform. Prisma Access is primarily used to connect and secure access for remote users, branch offices/locations, and other remote networks.

As more applications, servers and services are delivered from the cloud and remote work becomes a global norm, organizations are reevaluating whether legacy point solutions can adequately scale and provide secure, reliable access for their users and locations. Workers typically rely on remote access VPN or similar services to access critical data or perform critical, time-sensitive tasks, which means the secure access experience for users can have a real impact to an organization's bottom-line. Additionally, with the increasing complexity and sophistication of cyber-attacks, it is critically important that organizations are able to centralize and leverage log data from all of their services to close gaps in security posture, and detect and mitigate any potential threats to network security.

Palo Alto Networks provides an integrated platform to address organizations broad networking and security needs. Specifically, Prisma Access, a cloud-native solution, provides consistent network security services and access to all types of cloud applications for remote users and to remote sites and locations. With Prisma Access, organizations no longer need to rely on multiple point and on-premises solutions, reducing both cost and complexity while improving overall security posture.



To better understand the benefits, costs, and risks associated with Prisma Access, Palo Alto Networks commissioned Forrester Consulting to interview 10 customers, survey an additional 133 customers, and conduct a Total Economic Impact™ (TEI) study. For this Prisma Access spotlight, Forrester leveraged data from nine interviewed organizations, all with experience using Prisma Access to provide secure remote access to critical applications and services to globally a distributed organization.

This abstract will focus on these interviewed organizations use of Prisma Access and its value to their organizations.

Reduce likelihood of a data breach

45%

INVESTMENT DRIVERS

Organizations described the following drivers for their investment in Prisma Access from Palo Alto Networks:

- **Provide a secure, reliable connection to anyone from anywhere.** Legacy solutions such as on-prem VPNs or web proxy services did not provide the visibility that organizations needed to confidently secure their networks and were notoriously unreliable with users complaining of frequent disconnects and access issues. A senior VP in the financial services industry explained "With our previous remote access solution, our users would often complain about slow speeds, especially if they were traveling internationally. We also don't have to worry about uptime and availability now as Palo Alto Networks guarantees a great uptime SLA as part of the service."

> **"That's one of the benefits of Prisma Access, we don't touch it at all. We don't have to spend all the time patching and monitoring the portals and the gateways"**
>
> *Director of network and monitoring services, education*

- **Scaling to meet increasing demand for remote access pre and post pandemic.** Even before COVID-19 forced most organizations to enable more flexible, remote work, organizations were struggling to scale their legacy solutions to meet increasing demand for remote access. Interviewed organizations made the decision to deploy Prisma Access prior to the COVID-19 pandemic and noted that the improved scalability has been a crucial piece of keeping business running while shifting to a more remote workforce. A senior VP in the financial services industry explained "Prisma Access has enabled our users to access the applications and data they need, in a secure way, regardless of where they are. This has been critical throughout the pandemic, where our organization moved to 100% remote work. There is no way our previous remote access solution could have effectively scaled to support that shift in remote workers."

  Additionally, organizations want all users to leverage Prisma Access to ensure they are protected from threats, especially when accessing apps or data from risky locations. A director of network and monitoring services in the education industry said: "We have two primary use cases that we supported for the VPN and now support with Prisma Access. One is to provide secure remote access to users who are remote and need to access secure applications on the campus network. The other use case is to provide a secure internet connection to our users while they are on an insecure network. Users often log in from public hotspots, hotels, coffee shops, etc. so we encourage all users to leverage these services to secure their own devices."

- **Improve performance while reducing maintenance and support.** The primary issue that organizations faced with legacy solutions were reliability and performance. Users complained of frequent disconnections and slow speeds, clogging up help-desk resources and having a negative impact to productivity and user experience. In addition to user-related issues, legacy solutions required frequent updates, patches and monitoring to ensure the network remains secure and functioning properly. A director of network and monitoring services in the education industry said "We did have problems [with a legacy VPN solution] in terms of just having to reboot the VPN server and having to monitor it. For three years, it was constant babysitting on the server side for my team. That's one of the benefits of Prisma Access, we don't have to touch it at all. We don't have to spend all our time patching and monitoring it."

WHY PALO ALTO NETWORKS PRISMA ACCESS?

Organizations shared the following key reasons for ultimately investing in Prisma Access:

- **Cloud-delivered and scalable solution.** A director of network and monitoring services in the education industry said "We used to receive a lot of complaints about slow speeds from our users with our legacy solution, especially from international users, because we provide a full tunnel VPN. With Prisma Access, we like that the solution allows us to stay full tunnel, but the gateways can actually handle the traffic that was going to the internet. That was one of the big drivers and when we did our proof-of-concept, we had users and faculty test the solution from around the globe to help with our evaluation and received great feedback."
- **Improved performance, reliability and security.** A senior VP in the financial services industry said, "Security investment is often justified by how much it can reduce risk, and Prisma Access definitely reduces risk for us. But it is also one of the rare security products that can enable your organization to be more productive and improve the efficiency of our users."
- **Increase in organizational security with integration with the rest of the Palo Alto Networks ecosystem.** A director of network and monitoring services in education said "We like that Prisma Access is integrated into all of our internal logging mechanisms like our SIEM and help desk system. Our legacy solution was very limited in terms of logs and integrations but with Palo Alto Networks and Prisma Access we have better visibility and can see where the traffic on our networks is coming from."

KEY RESULTS

Prisma Access played a role in some key quantified benefits from the larger TEI study on the Palo Alto Networks network security portfolio. Key benefits and Prisma Access's impact on the greater solution set included:

$9.2 million in savings enabled by a 45% data breach risk reduction. While not solely responsible, Prisma Access played a key role in reducing the likelihood and impact of a security breach for organizations.

- **Reduce likelihood of a data breach.** With Prisma Access, all users are leveraging a secure gateway to access critical networks and applications, protecting both the network and the end-user device from malware and internet-based attacks while connected.
- **Reduce impact of a security breach.** All security logs are easily integrated with existing security SIEM solutions and other Palo Alto Networks security solutions, improving visibility and detection capabilities and allowing security teams to identify and remediate any threats more quickly.

Avoided and rationalized security infrastructure saving $9.9 million. Prisma Access was able to help organizations rationalize their legacy security infrastructure, removing redundant technologies like VPN services and on-premises infrastructure.

- **Save costs, reduce complexity and improve security performance.** With Prisma Access, organizations were able to remove a redundant point solution, reducing complexity of their environment, removing a vendor, and patching any gaps in coverage.

READ THE FULL STUDY HERE

Security stack management efficiencies reduce workloads by almost 50%, saving $1.9 million. By adopting Prisma Access, organizations are no longer responsible for maintaining legacy solutions, reducing labor costs and allowing organizations to reallocate valuable resources to higher-value tasks.

- **Reduced maintenance with improved performance makes happy users.** Organizations reported that with Prisma Access, they were not longer constantly patching and monitoring portals and gateways. End users reported improved performance in terms of connectivity and speed, and had fewer issues installing and running Prisma Access.

Reduce time to achieve proper security posture by 30%. With Prisma Access, organizations can apply consistent security policies and controls to all incoming traffic, reducing deployment and fine-tuning efforts compared to a point-product approach.

- **Centrally managed from a single-pane-of-glass, Panorama.** Prisma Access integrates with Palo Alto Networks other security products, including their security management solution Panorama. With Panorama, organizations can manage all security policy and monitor services from a central location with each application or service having a similar look-and-feel, cutting down on training times and improving the experience for security and IT teams. Additionally, Prisma Access provides a dedicated cloud-based management console for customers who don't use Panorama.

ADDITIONAL RESOURCES

Forrester developed additional resources to dive deeper into the impact and benefits of the specific solutions included in this study. More information and access to these additional resources can be found here:

- The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN
- Executive Summary: TEI™ of Palo Alto Networks for Network Security and SD-WAN
- TEI Spotlight: CloudGenix SD-WAN
- TEI Spotlight: Cloud-Delivered Security Services

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full report "The Total Economic ImpactTM of Palo Alto Networks For Network Security And SD-WAN", commissioned by Palo Alto Networks and delivered by Forrester Consulting.

STUDY FINDINGS

Forrester interviewed 10 and surveyed 133 organizations with experience using Prisma Access from Palo Alto Networks along with their other Cloud-Delivered Security Services, SD-WAN and NGFWs, and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Security stack infrastructure cost avoidance and management efficiencies totaling $11.7 million.
- Efficiency gains for Security, IT operations, and end users totaling $6.0 million.
- Reduced risk of a data breach saving $9.2 million.
- Read the study for additional benefits and details.

Return on investment (ROI)

247%

Net present value (NPV)

$28.5 million

Appendix A: Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.


FORRESTER®