FORRESTER®

TEI Spotlight:

Palo Alto Networks Helps Financial Institutions Reduce Business Risk While Improving Network And Security Efficiency

This spotlight will focus on financial services and insurance (FSI) organizations' use of Palo Alto Networks network security and secure access service edge (SASE) offerings along with the value it delivers to the financial institutions. It also expands upon a Forrester Consulting Total Economic Impact study where nine customers were interviewed and 133 were surveyed on their experience using Palo Alto Networks solutions.[1]

To gain further FSI organizations' insights for this spotlight, Forrester interviewed an additional three decision-makers at various financial institutions, with roles such as head of infrastructure at an investment management firm, CIO at a credit union, and chief information security officer (CISO) at a regional bank. Their perspectives will shed further light on efficiency gains for internal and external groups, increased security coverage, risk reduction and improvements to both Zero Trust and software-defined wide-area network (SD-WAN) capabilities.

KEY CUSTOMER BENEFITS

Reduction in security incidents needing advanced investigations

35%

Decreased likelihood of a data breach after 3 years

45%

INVESTMENT DRIVERS

Some of the driving factors that encouraged financial institutions to improve their network and security infrastructure include:

- **Cybercriminals often target the FSI industry with sophisticated attacks.** Over the years, cybersecurity threats have been increasingly more sophisticated and advanced. This pushed organizations to seek upgrades to their often-aging security infrastructures and move away from on-premises solutions. Interviewed decision-makers noted that the increasing threat in the cybersecurity space was a big driver to their decision to improve their organizations' security networks and infrastructure. The head of infrastructure at an investment management company said: "The overall financial services market is a target for both sophisticated cyber criminals as well as nation states. Financial services and insurance companies are often sizable targets in terms of attacks, reputation, impact on the market, impact on the global economy, etc."
- **Internal drive for digital transformation.** Interviewees highlighted an internal push to incorporate more digital aspects into their business. Many initiated digital transformations in all parts of the organization, including security.

READ THE FULL TEI STUDY HERE

This motivation was further exacerbated by catalyst events such as COVID-19, which forced most organizations to introduce more flexible, remote work environments driven by digital solutions. Interviewed decision-makers deployed Prisma Access and noted the improved scalability to be a crucial piece in keeping business running when forced to shift to remote work. The CISO at a regional bank shared, "We wanted to be a digital first organization, which involves investing in IT and new systems, new capabilities."

- **Continuous push to consolidate infrastructure and improve operational efficiency.** Interviewees noted wanting to have an integrated and connected solution to give them a single pane of glass into their system. They also used this effort to improve their operational efficiency in their security and network organization. These are two pieces that organizations increasingly look for, especially as it becomes harder to hire for security operations and network operations positions. The CISO at a regional bank said: "Ten years ago, people bought tools that would meet specific needs, but weren't talking to each other. We were looking for ways to consolidate all security services under a single vendor."
- **The need for infrastructure modernization due to MPLS becoming increasingly cost prohibitive**. The costs for multiprotocol label switching (MPLS) networks were far more expensive than leveraging a public internet connection and the networks themselves were significantly slower. As businesses became more digital, leveraging more data, public cloud, and internet-based resources, the demand for bandwidth and direct internet access at each site continued to grow. Infrastructure modernization will take much of that MPLS expense out of the equation, where investment into the Prisma SD-WAN solution allows optimized end-user experiences across the wide area network circuits.

WHY PALO ALTO NETWORKS

Financial institutions shared the following key reasons for ultimately investing in Palo Alto Networks:

- **Holistic approach and largest network.** Interviewed decision-makers highlighted how Palo Alto Networks has the better and more comprehensive features compared to similar vendors in the market. The CIO at a credit union shared: "For our infrastructure modernization, we wanted to find a partner that was worth the investment. Palo Alto Networks had the most holistic approach, the largest network, and the people made all the difference."
- **Recognition for Sales and Customer Success teams.** Interviewees really emphasized the Sales and Customer Success teams of Palo Alto Networks as a key differentiator. The head of infrastructure at an investment management firm said: "The level of support from Palo Alto Networks from the executive and engineering standpoint is probably much better than any vendor that I have dealt with in my career. Its engagement and sponsorship on any issue we might face is why our firm continues to stay with Palo Alto Networks."
- **Scalability and flexibility of solution.** Interviewed decision-makers shared that the fact that Palo Alto Networks is scalable and can be customized according to their organizational needs was another key factor over the alternatives. The CISO at a regional bank noted: "We wanted a virtual firewall system that can plug into our system, without having to completely overhaul all traffic. [We wanted to be able] to pick

and choose what network traffic needed to come back and what needed to go straight out."

> **"What makes Palo Alto a good investment is not necessarily just the technology. The technology is fantastic, but it is the customer service and dedication to seeing its customers succeed that is truly a differentiator."**
>
> *CISO, regional bank*

KEY RESULTS

With these investment drivers and reasons for selecting Palo Alto Networks, interviewed decision-makers moved forward with their deployments. Key benefits include:

Efficient security stack management. Interviewees noted their organizations benefitting from having a centralized management dashboard and a single pane of glass, which simplified their efforts to secure their environment. Reducing the number of vendors in their environment means reducing the number of different skill sets required to manage and maintain their systems. Additionally, the unified platform and single source of truth via Panorama gives organizations much better visibility into network traffic, allowing them to seamlessly apply updates, patches, and policy rules across the environments with less effort.

- The head of infrastructure at an investment management firm said: "We were going from 10s of firewalls to 200+ firewalls. Managing it in a way that we were managing it before was just going to be impractical. With Palo Alto Networks, this only translated to us adding 1-2 additional team members, rather than the 10+ people we would have had to add if we used a different solution."
- The CISO at a regional bank shared: "By consolidating everything into Palo Alto Networks, we put all our eggs in one basket and see if it actually helps us because that's one basket to protect. In the security space, the more complex your environment gets, the harder it is to protect. One small mistake is going to be detrimental to the company."

Peace of mind from improvements in security posture. Interviewed decision-makers noted that with Palo Alto Networks, their organizations' security teams can easily identify and close any gaps in their security system. The fidelity of the information shared between systems is key in effective automated prevention of breaches and pivotal to administrators being able to apply the proper policies across the numerous devices on and off the corporate network and in the cloud.

Palo Alto Networks brings cloud architecture, remote location access, and software-as-a-service (SaaS) applications into the security posture of the corporate network, specifically with Prisma Access. As a result, there are no longer disparate policies, systems, controls, and protection gaps that often expose sites as the initial infection point or root cause of a breach before traversing east-west to reach objectives.

- The CIO at a credit union shared: "One way I know we have improved since using Palo Alto Networks can be seen in our audit results. Our periodical audits on our infrastructure have consistently returned with no concerns, whereas that was not the case in the prior environment."
- The head of infrastructure at an investment management firm said: "We are in a much better security posture than we were a few years ago due to Palo Alto Networks. We have a much more simplified rule base. We have better segmentation than we ever had. We have a better firewall-to-admin ratio than we ever had. We have better visibility into the network so our mean time to resolution (MTTR), our incident

calls, our availability, all trends in the right direction."

Ensure robust disaster recovery strategy and business continuity. In addition to the peace of mind around their security posture, interviewed decision-makers also noted that the fact that Palo Alto Networks' solution was cloud-based allows their organizations to ensure their infrastructure and business operation can remain functioning in the event of any disaster or disruption.

- The head of infrastructure at an investment management firm noted: "One of my greatest achievements was being able to get everyone at my company home at the beginning of the pandemic and not have any issues, impacts, or service level disruption. This is a huge testament to our technology selection, which includes Palo Alto Networks. From an MTTR perspective, we saw a 67% reduction."
- The CISO at a regional bank said, "Yes, there are some significant operational costs to having a strong security network and infrastructure, but that's a drop in the bucket to what the cost would be to recover from a ransomware payment, for example."
- The CIO at a credit union shared: "We have seen definite improvements from having the right architecture technical resources onboard to take advantage of the better context and filtration capability of next-generation firewall (NGFW) logs. Overall, we've had a ballpark estimate of 20% improvements in both MTTI (Mean Time to Identify) and MTTR.

Reduced risk allows core business to focus on revenue generating activities. By reducing the overall risk of their business environment, interviewees shared that this allows their organizations to focus on revenue-generating activities. Additionally, the improved operational efficiency means that they no longer have to allocate as many resources into their security infrastructure as they need prior to Palo Alto Networks, and thus can reallocate those same resources into more productive work elsewhere in the organization.

- The CIO at a credit union said: "Our environment is less risky due to Palo Alto Networks technology. Increased visibility, proactive Palo Alto Networks updates, and improved logging/reporting are all evidence of reduced risk."
- The CISO at a regional bank explained: "People in security are often thought of as call centers. I don't mind that being the case. It's the cost of doing business and I play an important role in reducing risks. Having the right security posture means the business can focus on increasing revenues."
- A senior VP in the financial services industry explained, "We don't have to worry about uptime and availability now as Palo Alto Networks guarantees a great uptime SLA as part of the service."

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: Prisma Access
- TEI Spotlight: Prisma SD-WAN
- TEI Spotlight: Cloud-Delivered Security Services

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of Palo Alto Networks For Network Security And SD-WAN," a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, January 2021.

STUDY FINDINGS

Forrester interviewed nine decision-makers and surveyed 133 organizations with experience using Palo Alto Networks products and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Reduced number of security incidents requiring manual investigation by 35% and MTTR by 20%.
- Decreased likelihood of a data breach by 45% after three years.
- Reallocated roughly 50% full-time security professionals to higher-value initiatives due to management efficiencies from a common platform.
- Reduced time to achieve proper security posture by 30%.

Return on investment (ROI)

247%

Net present value (NPV)

$28.5M

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®