FORRESTER®

Executive Summary:

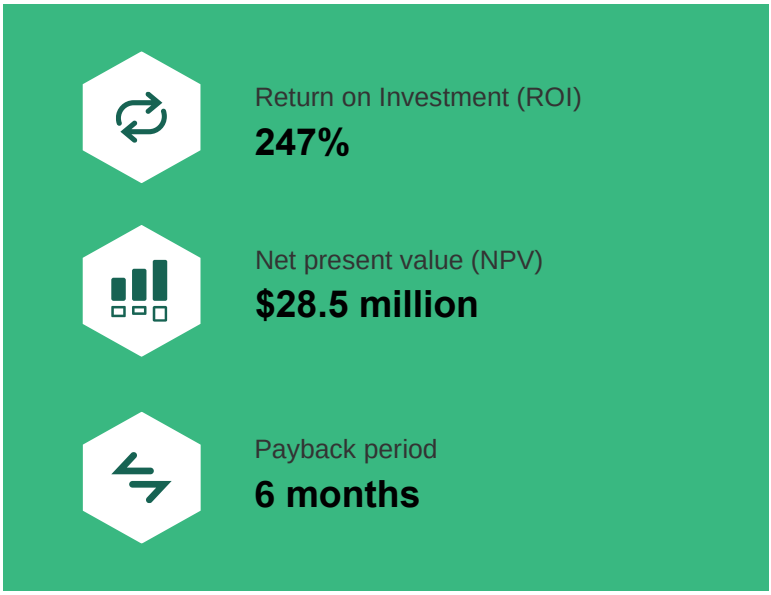
The Total Economic Impact™ Of Palo Alto Networks For Network Security And SD-WAN

Palo Alto Networks commissioned Forrester Consulting to conduct an objective Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises realize when deploying Palo Alto Networks for network security and SD-WAN. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Palo Alto Networks' products on their organizations. These products include Next-Generation Firewalls (NGFWs), Palo Alto Networks Prisma SD-WAN, and Cloud-Delivered Security Services covering Intrusion Prevention (IPS), Secure Web Gateway (SWG) and URL Filtering, Malware Analysis or Sandboxing, DNS security, and Internet-of-Things (IoT) security.

Palo Alto Networks network security and SD-WAN solutions span across major security controls, helping organizations centralize management, maintain optimum connectivity, and extend security policies and controls to every user, application, and device.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed nine customers and surveyed 133 customers with experience using Palo Alto Networks solutions. For the purposes of this study, Forrester aggregated the experiences of the interviewed and surveyed customers and combined the results into a single composite organization.

Prior to deploying Palo Alto Networks for network security needs, the customers leveraged traditional firewalls with multiple point solutions to secure their environments. This was a byproduct of digital transformation efforts. The organizations lacked modern security technology and efficiency as security and IT teams tried to keep up with evolving business needs. Digital transformation initiatives pushed more data, applications, and processes to the cloud while other core business functions remained on-premises.



After the investment in the Palo Alto Networks network security solution, the customers had a common platform that fed into a centralized tool: Palo Alto Networks' security management solution, Panorama. This significantly reduced investigational effort and freed up valuable resources to focus on enhancements and securing more of the network. The interviewees' organizations deployed some or all these network security and SD-WAN solutions from Palo Alto Networks.

Key results from the investment are highlighted by: efficiency gains for IT, security, and network operations teams, business end users, and in-store workers; a significantly reduced likelihood of a data breach; reduced costs associated with licensing and

managing legacy point-solution infrastructure; increased security coverage, and improvements to both IoT Security, Zero Trust and SD-WAN capabilities.

KEY RESULTS

Risk-adjusted present value (PV) quantified benefits include:

Data breach risk reduction

- **Decreased likelihood of a data breach by 45% after three years.** With Palo Alto Networks, the organizations were able to decrease security gaps, increase visibility, enact a Zero Trust security model, and apply consistent security policies across the entire organization. Cloud-Delivered Security Services supplemented the existing SecOps team, adding 24/7 support and notably prevention for vulnerabilities and all known and unknown threats.

Security & IT operations efficiency

- **SOC teams were able to reduce the number of advanced investigations by 35%, improve MTTR by 20%, and cut the number of devices that require re-imaging by half**, **all resulting in $5.1 million saved over three years.** Deploying Palo Alto Networks security solutions significantly improved visibility into the organizations' networks and introduced automation capabilities that drove down the number of critical alerts, including false positives, over time. Additionally, the organizations were able to reduce MTTR because analysts now had the data they needed at their fingertips. As a result, there were fewer malware infections and other issues with endpoint devices, reducing the workload for the IT operations team.

Reduced security stack management effort

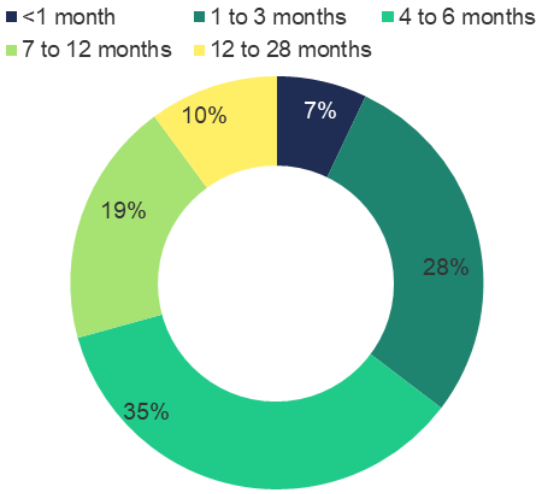
50%

End-user productivity improvement

- **Improved end-user productivity with fewer incidents and investigations, totaling $865,226 over three years.** With Palo Alto Networks security solutions, end users spend less time interacting with the security and IT operations teams, and they spend more time focusing on their primary roles and driving value for their organizations.

"What is the estimated time it took your organization to achieve steady state security posture with NGFW versus point solutions?"

(Displaying top 5 results only)



Base: 83 Palo Alto Networks users who noted "reduced organizational cybersecurity risk" as a benefit
Source: A commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, October 2020

Achieve steady-state security posture within 6-months of switching to Palo Alto Networks

70% of customers

READ THE FULL STUDY HERE

Security Infrastructure cost reduction and avoidance

- **Avoided and rationalized security infrastructure, saving $9.9 million over three years.** The organizations removed legacy security systems and products after deploying Palo Alto Networks. With as many as 17 vendors in their security stacks prior to investing, simplifying the environment and reducing the number of vendors was a priority, and the Palo Alto Networks solution provided superior coverage with less overhead. Some of the technologies that were supplanted by Palo Alto Networks Cloud-Delivered Security Services include intrusion prevention (IPS/IDS), secure web gateway (SWG), web proxy, VPN malware analysis (e.g., sandboxing), DNS, and software-as-a-service (SaaS) application security.

Security stack management efficiency from common platform

- **Reallocated roughly 50% full-time security professionals to higher-value initiatives due to management efficiencies from a common platform, saving $1.9 million over three years.** Removing legacy vendors and consolidating to a common platform meant fewer people were required to perform the same tasks, allowing the organizations to reduce their management teams by roughly half. Additionally, the common platform allowed the organizations to quickly roll out updates, patches, and security policies to the entire platform from a centralized location, rather than updating each security device manually and across multiple vendors.

Time to achieve proper security posture

30% faster

IoT Security costs and risks reduction

- **Saved $1.4 million on IoT from reduced management effort and a reduction in the number of new IoT devices purchased.** With IoT Security, the organizations were able to identify and secure all their IoT devices from a central platform, quickly understand the health and location of each device, and maximize the value and utilization of each device with the enhanced reporting capabilities. This reduced new purchases by 10%.

Decreased likelihood of a data breach after 3 years

45%

Security posture attainment speed

- **Reduced time to achieve proper security posture by 30%, saving $812,860 over three years.** By leveraging Palo Alto Networks' NGFWs and Cloud-Delivered Security Services, the organizations were able to stand up their security solutions faster and reach steady state more quickly. This gave the security teams a head start on optimizing the solution and achieving Zero Trust standards compared to using point solutions.

WAN Hardware & connectivity cost reduction

- **Cut costs on WAN hardware and connectivity at remote sites by over 90%, representing $6.04 million over three years.** By migrating away from multiprotocol label switching (MPLS) to Prisma SD-WAN, the organizations were able to significantly reduce monthly operating costs at their sites while improving visibility and control of network traffic.

SD-WAN management efficiency

- **Reduced management effort by half for IT teams and improved efficiency of branch office and retail store workers by 12% with Prisma SD-WAN, saving $4.9 million over three years.** With an intuitive UI and purpose-built hardware, Prisma SD-WAN enabled centralized management of the SD-WAN for IT teams. Additionally, the improved bandwidth, network performance, and security controls allowed the organizations to deploy better technology to their remote workers, improving productivity and customer experience.

COMPOSITE ORGANIZATION

Based on the interviews and survey, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the nine companies that Forrester interviewed and the 133 companies that Forrester surveyed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization is a distributed enterprise with 50,000 employees and $7 billion in annual revenue. It has 400 sites including its headquarters, data center, cloud, branch office, and retail and manufacturing locations. The composite's security team responds to 1,200 incidents a week, or 62,400 in the first year, with each incident taking an average of 2 hours to resolve.

INVESTMENT DRIVERS

The surveyed and interviewed organizations struggled with common challenges, including:

- **Underperforming legacy point cybersecurity solutions.** Interviewees said their organizations were utilizing legacy point solutions that failed to meet expectations around speed, performance, customer support from the vendor, and a lack of alignment with Zero Trust strategies. Previously deployed products were slow to upgrade, and they cost significant capital investments to maintain necessary hardware and significant operational investments to keep the solutions running.
- **Segmented, decentralized security features and platforms.** Several interviewees said that before their organizations deployed various Palo Alto Networks NGFW variants and Cloud-Delivered Security Services to cover on-premises and cloud infrastructures, they were using disparate security solutions that required multiple skill sets to perform simple tasks. Security teams struggled with visibility across multiple technologies, they could not transfer intelligence fast enough, lacked a cohesive suite to monitor their networks, and could not quantify risk due to gaps across infrastructures.
- **Protecting against increasingly sophisticated attacks and a desire for Layer 7 visibility and control.** As cybersecurity threats become more advanced, interviewees said their organizations were seeking to upgrade their aging security infrastructures and to move away from on-premises point solutions. They sought more granular Layer 7 visibility into their networks and required application-level insight. Their legacy solutions could not provide the visibility, decryption or performance needed.

WHY PALO ALTO NETWORKS?

The organizations searched for a solution that could:

- **Unify security, policy and management across network and cloud under the same centralized platform.** A head of IT architecture in the technology manufacturing industry said: "I now have more consistent security policy across my entire infrastructure worldwide. I don't have different vendors with different policies and different updates. I've got security consistency

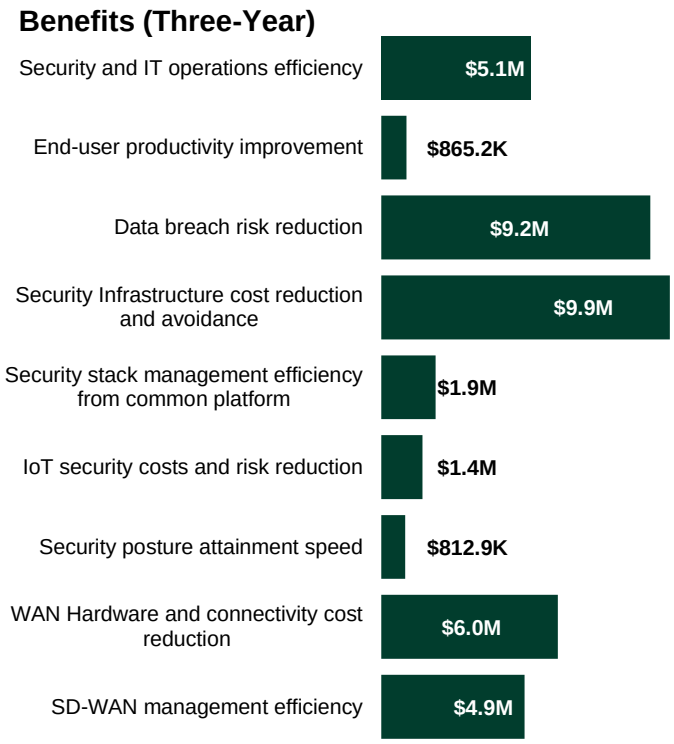
across all environments. It goes back to the singe pane of glass, but even without that, I've got a security policy that I know if I can define it once, I can run it everywhere."

- **Provide a single pane of glass and improved visibility during cloud transformation.** A CISO in the retail industry said they see the benefits of having an integrated and connected solution. They said "The beauty about this technology is that it all integrates with Panorama. In Panorama, we can control everything from one console. Instead of having 600 firewalls individually managed, I can start looking at my threat traffic through one console. That speaks for itself."
- **Integrate well with existing platforms to enable automation.** The Cloud-Delivered Security Services uses network effect to automate the analysis of a threat from one customer and prevent similar threats for all subscribed customers in seconds or less. A head of IT architecture in the computer manufacturing industry said: "We wanted out-of-box automation hooks. We didn't want to have to buy all of the products and then spend another million or so dollars developing automation on top of it. We wanted good integration with the existing platforms that we already have, and we needed to be able to expand into other areas that we haven't necessarily invested in yet."

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




FORRESTER®