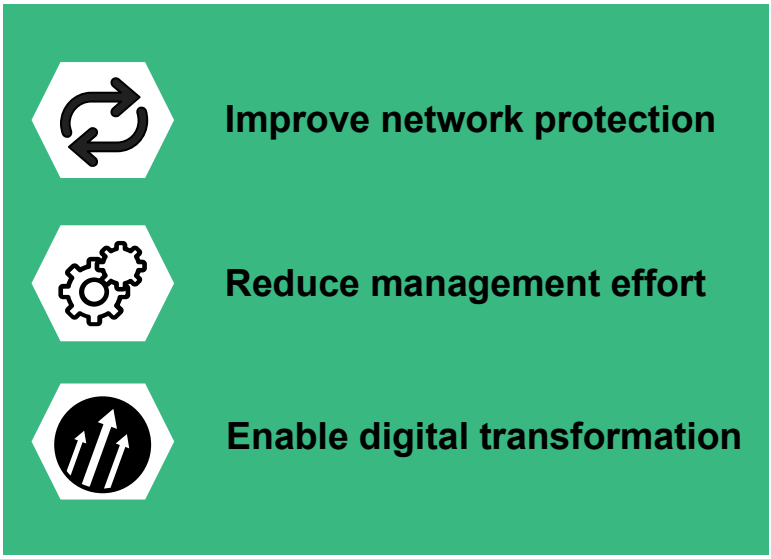
FORRESTER®

Easily Manage, Rapidly Secure Public And Private Cloud Deployments With VM-Series Virtual Firewalls

Forrester recently spoke with multiple Palo Alto Networks customers deploying a full stack of Palo Alto Networks security products and migrating away from multiprotocol label switching (MPLS) to the Palo Alto Networks Prisma SD-WAN solution. In these interviews for the subsequent Total Economic Impact™ (TEI) study, Forrester uncovered various benefits from customers in a range of Palo Alto Networks products.[1] This abstract focuses on interviewees' organizations that deployed VM-Series virtual firewalls as part of their transformation — and the benefits they recognized in their public and private cloud deployments.

Organizations are undergoing digital transformations to accommodate customers who expect services and solutions to be delivered faster than ever. To meet these needs, companies are expanding or migrating applications and data from traditional data centers to public cloud platforms and private clouds based on virtualized infrastructure. While the cloud allows organizations the flexibility to better serve customers without many of the operational costs or issues of a physical data center, these new environments open up a host of new security challenges.

VM-Series firewalls are the virtualized version of Palo Alto Networks' next-generation firewalls (NGFWs). VM-Series firewalls provide visibility and threat protection for apps, workloads, and data across both private and public clouds in a scalable and easy-to-manage manner. These virtual firewalls are designed to meet today's network security challenges — enabling security teams to control lateral, inbound, and outbound traffic in the public cloud as well as define and enforce segmentation and threat prevention policies in virtualized data centers.



Prior to investing in VM-Series firewalls, interviewees' organizations used a myriad of traditional firewalls and point solutions to secure their environments. Security and IT teams struggled to keep up with evolving business needs as their organizations lacked modern security technology.

The lack of a unified platform and next-generation firewall capabilities also left the organizations stuck in a cycle of devoting valuable resources to management, operations, and maintenance activities while work on new initiatives and enhancements fell to the wayside.

After the investment in the Palo Alto Networks network security solutions, 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 enhancing network security.

INVESTMENT DRIVERS

Interviewees described the following drivers for their investment in VM-Series firewalls:

- **Underperforming legacy solutions.** Interviewees said their organizations were utilizing legacy point solutions that failed to meet expectations for speed and performance. Previously deployed products were slow to upgrade and required significant capital investments to maintain necessary hardware and significant operational investments to keep the solutions running.
- **Decentralized and inefficient security tools.** Prior to deploying NGFWs, organizations used disparate solutions to cover on-premises and cloud infrastructure. This required multiple skill sets to perform simple tasks, and security teams struggled to enforce consistent policies and gain full visibility without a singular solution capable of protecting networks.
- **Protecting against increasingly sophisticated attacks and a desire for Layer 7 visibility and control.** As cybersecurity threats become more advanced, interviewees said their organizations sought more granular Layer 7 visibility into their networks and required application-level insight.

> **"The firewalls are top of the line. You can get speed to value very quickly, and the ability to increase your security posture while enabling the business is second to none."**
>
> *Network security manager, retail*

KEY FEATURES

VM-Series firewalls provide the following key features, which factored heavily into investment decisions:

- **Networkwide protection and visibility.** VM-Series firewalls provide visibility and control over inbound, outbound, and east-west network traffic across an organization's entire deployment. Security teams can define, enforce, and manage universal policies across a combination of public, private, and on-premises environments from a single console.
- **Stringent threat prevention and segmentation capabilities.** Palo Alto Networks provides next-generation protection in both public and private cloud deployments. VM-Series firewalls protect the public cloud by inspecting inbound and outbound traffic and using an integrated intrusion prevention system (IPS) and sandboxing to defend against known and unknown threats. In a virtualized private cloud, VM-Series firewalls provide segmentation and intrusion prevention to create trust zones to enforce security measures for east-west traffic and ensure regulatory compliance.
- **Automated and scalable network security.** Network security teams are tasked with the difficult mandate of securing ever-growing virtualized networks without impeding the speed of digital transformations. VM-Series firewalls scale automatically with cloud infrastructure ensuring consistent security in even the most dynamic environments. Tag-based policies enable network security teams to create policies that can be automatically applied to newly created workloads based on the native tags or labels used in a given cloud or virtual environment. As workloads are moved around the environment (e.g., VMs moved to another host for maintenance), their tag-based security

policies remain in place to ensure security without the need to manually adjust policies.

KEY RESULTS

Reduced management effort for IT teams. Virtualized firewalls require drastically less time and effort to operate and maintain than their hardware equivalents. Additionally, having one consistent toolset across public, private, and on-premises environments eliminates a significant amount of redundant work for network security teams.

- A CISO in the retail industry stated: "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."
- The network security manager for a retail firm explained: "You can completely change your firewalls in one push and in one commit. It is amazing."

Improved protection and reduced risk profile. Palo Alto Network's unified platform helped IT and SecOps professionals automate previously manual processes, define better rules for alerts, and improve visibility into network traffic. With a centralized and unified solution, organizations can implement the Zero Trust model that Palo Alto Networks technology supports.

- A CISO in the retail industry explained: "Because we put aggressive segmentation in place using data center firewalls and through continuous monitoring and continuously focusing on attacking any vulnerabilities, my team was able to reduce critical alerts by 80% in that part of our data center. We then moved to a different segment of the data center and repeated the process, ultimately cleaning up our entire environment."
- The deputy CISO for an entertainment firm detailed: "[We really value] feature capabilities like dynamic objects and dynamic groups and things like that. We've got our master blocklist loading from a mind-meld group that updates every 5 minutes. So, literally, our SOC can go out to a web page and add a site to a text file and all of our firewalls in the enterprise have that in their blocklist in 5 minutes."

Consolidated security toolset reducing hardware and software spend. Prior to investing in Palo Alto Networks, interviewees' organizations had a mix of on-premises and cloud solutions as well as some managed services. As networks grew in complexity, security teams were forced to implement point solutions to cover each new expansion of the network, often resulting in coverage gaps, confusing policies, and reducing visibility. VM-Series firewalls enabled organizations to retire point solutions and recognize software and hardware savings.

- One interviewee had accumulated 17 total solutions to provide adequate security for their network. After transitioning entirely to a Palo Alto Networks platform, including VM-Series, the organization drastically cut back on hardware and software spend. The interviewee explained, "Over the years, [we] have carved down our spend on products like that probably by at least $2 or $3 million a year."

Enabled next-generation security without inhibiting business agility. VM-Series firewalls can be deployed seamlessly into public or private cloud deployments. Having a consistent solution and set of policies across deployments creates a frictionless environment for development teams.

- The network security manager for a retail firm detailed: "By enabling faster change more securely, we're allowing the application teams to service the customers better, right? We are allowing the application teams to move faster, to push change faster and more securely."

TOTAL ECONOMIC IMPACT ANALYSIS OF PALO ALTO NETWORKS SECURITY PRODUCTS

This spotlight report about VM-Series virtual firewalls uses findings from "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 with experience using Palo Alto Networks security products at their organizations and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Reduced incidents by 12%, mean-time-to-resolution (MTTR) by 20%, and endpoint reimages by 45%.
- Reduced the likelihood of a data breach by 45%.
- Reallocated 7.8 FTEs due to enhanced security stack efficiency.

VM-Series virtual firewalls are a component of the solutions providing these benefits. For more information download the full study here.

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®