FORRESTER®

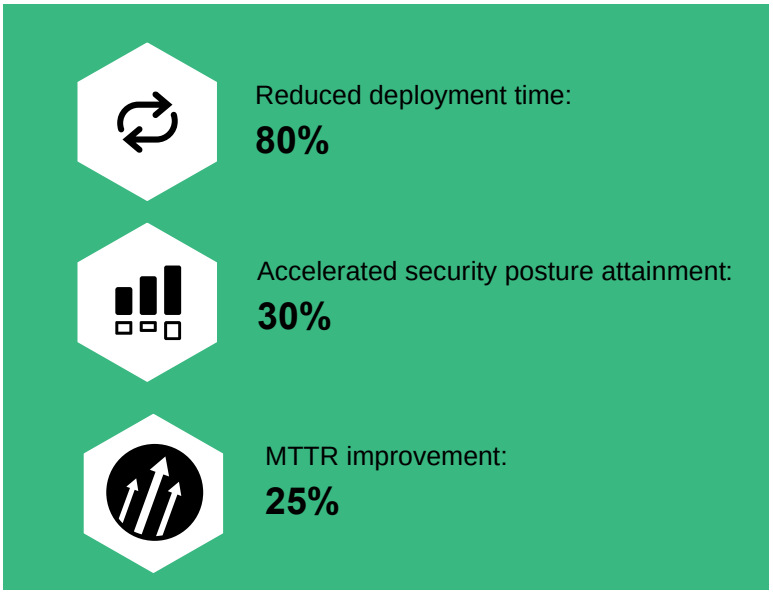
Palo Alto Networks VM-Series Virtual Firewalls Offer Advanced Technology To Address Hybrid Cloud Security

The COVID-19 pandemic has accelerated an already prevalent trend: Enterprise cloud usage is increasing. As companies expand into hybrid cloud deployments, security teams face new challenges, including the need to secure data paths to multiple clouds. Palo Alto Networks VM-Series Virtual Firewalls bring the dependability of firewalls to cloud security, and it offers enterprises flexibility and agility in their solution.

To better understand the benefits, costs, and risks associated with Palo Alto Networks VM-Series Virtual Firewalls, Palo Alto Networks commissioned Forrester Consulting to interview eight decision-makers and survey an additional 132 decision-makers who have experience using the solution and conduct a Total Economic Impact™ (TEI) study.[1]

This abstract will focus on the technology behind the VM-Series virtual firewalls and its value to the interviewees' organizations.

Prior to using VM-Series virtual firewalls, the interviewees' organizations primarily relied on hardware firewalls with point solutions. However, as they took on larger digital transformation projects and moved towards virtualization across the enterprise — consolidating network and security infrastructures and public clouds — they found that legacy firewalls lacked the flexibility that teams required. They investigated relying on the native security capabilities of cloud service providers, but they found them lacking the proficiency that a mature security provider like Palo Alto Networks can provide. Furthermore, the interviewees used a combination of public and private clouds, and they did not want to introduce more complexity to their security stacks.



After investing in VM-Series virtual firewalls, the interviewees' organizations addressed the security challenges of their hybrid-cloud and multicloud environments. Their security teams could easily deploy advanced security controls and define, enforce, and manage consistent security policies from a single console. With improved visibility, they gained precise control of inbound, outbound, and east-west traffic, which ensured that attack surfaces were greatly reduced. The form factor of the VM-Series also afforded the interviewees the flexibility to automate firewall deployment and provisioning and to scale with demand. This reduced deployment times and eliminated overprovisioning costs.

READ THE FULL STUDY HERE

INVESTMENT DRIVERS

The interviewees' organizations outlined the following drivers for their investment in VM-Series virtual firewalls:

- **Underperforming legacy point solutions.** The interviewees said prior legacy point solutions failed to meet expectations around speed, performance, and customer support from vendors. Previously deployed products were slow to upgrade and required significant internal effort to deploy and to maintain.
- **Decentralized security platforms and capabilities.** Prior to using VM-Series firewalls, the interviewees' organizations struggled to manage decentralized security tools, and that led to gaps in visibility and redundant work. For example, organizations that used multiple clouds would have to write and push multiple versions of the same policies when using native tools.
- **Organizational cloud migration mandates.** Many of the organizations operated in environments with strict timelines to achieve cloud migrations. These organizations needed security solutions that could be quickly deployed and that ensured they had proper visibility to adequately protect their new cloud deployments.

> **"We came at [our decision to invest in Palo Alto Networks] from a financial perspective, a security perspective, and operational overhead efficiency savings perspective, and from a feature-set [perspective] too. When you put [Palo Alto Networks] side-by-side with a lot of other vendors, there was really no comparison dollar per dollar."**
>
> — EVP of engineering, IT services

WHY PALO ALTO NETWORKS

The interviewees' organizations evaluated multiple solutions before eventually deciding to invest in VM-Series virtual firewalls. Key capabilities that factored into the investments included:

- **Layer 7 visibility.** VM-Series firewalls offer application visibility across all ports and provide pertinent data for making policy decisions. The global head of IT engineering in the beverage industry noted, "One of the things that Palo Alto brings to the table from a security standpoint is that it is more focused, and the DNA is around identity and being able to refresh security in real time."
- **Application segmentation.** Organizations can use VM-Series firewalls to protect network segments and control application communications. This is bolstered by advanced threat prevention to identify and block lateral network threats.
- **Advanced security with CDSS.** Palo Alto Networks security subscriptions can be enabled on the VM-Series without requiring the installation or deployment of additional sensors or appliances. This allows organizations to recognize the additional protection benefits of services such as advanced intrusion prevention systems (IPS), domain name system (DNS) security, URL filtering, and zero-day threat prevention and sandboxing, all without additional overhead.
- **User-based policies.** VM-Series firewalls natively provide user-based policies, and they are integrated with a wide range of user identity data platforms. This enables dynamic, user-based access control policies in addition to application-based policies.
- **Centralized management for consistent policies and simplified management.** VM-Series firewalls can be managed centrally

through Panorama, which ensures policy consistency across multiple cloud and on-premises deployments. Panorama also alleviates the need for operators to manage their network security postures from multiple, disparate consoles.

- **Automated deployment and policy updates.** Organizations can leverage VM-Series capabilities to integrate security into application development workflows including automatic provisioning, automated policy updates, use of native cloud provider templates, and cloud-native scalability.

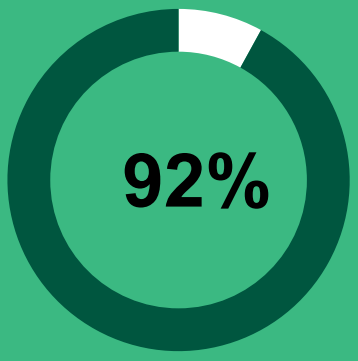
KEY RESULTS

The interviewees' organizations experienced significant benefits because of their investments in Palo Alto Networks VM-Series virtual firewalls. The efficiencies and time-savings outlined below were consistently driven by the offering's competitive technology, including:

Reduced time and effort required to deploy and maintain firewalls. The technology behind VM-Series virtual firewalls allows users to spend 90% less time on deployment, and it improved network and security team efficiencies by 80% over traditional firewalls.

- **Deployment time savings.** In the virtual form factor, it takes significantly less time to deploy VM-Series firewalls than traditional legacy firewalls, which often includes the hardware being shipped, installed, and tuned. The global head of engineering at a beverage organization described the arduous experience of deploying a legacy solution, saying, "When you include the cost of shipping the physical components, the delays in getting that equipment shipped out there, and then racking, that is a pretty large amount of time wasted before you can bring the firewall up and running."
- **Management and maintenance savings.** Palo Alto Networks Panorama provides centralized network security management. Panorama was a key time saver for organizations that had used native cloud service provider solutions in the past, allowing organizations to maintain a single set of policies across clouds, centralize patching, and make upgrades. An EVP of engineering for an IT services firm described Panorama's benefits, noting: "When you're deploying security services and running a firewall, security is the top priority. Right? So, the amount of man hours required to update individual firewalls is just untenable with multiple solutions. In the past, when we would deploy something, we would spend 2 to 3 hours per firewall, and that was just to get it going and get it deployed to get all the networks and everything set up. That did not include any rule sets, any refinements of the rules, or any of that. Now, we've got that [timeframe] down to less than 10 minutes."

Survey respondents said VM-Series virtual firewalls improved management, admin, and operation efforts on cybersecurity.



Faster security posture attainment. By leveraging Palo Alto Networks' next-generation firewalls (NGFWs) and cloud-delivered security services, the interviewees' organizations were able to reduce the time needed to achieve proper security posture by 30%.

- **Palo Alto Networks' consistent technology, unified platform, and advanced management capabilities allowed interviewees to get their organizations to a steady state more quickly.** They deploy their security stacks faster, reduce their implementation efforts, and allow security teams to start fine-tuning sooner than if they leveraged point solutions. Interviewees were also able to integrate all components on a common platform, making deployments faster and freeing up resources to fine-tune the solution, implement automated workflows, and otherwise improve efficiency for security, IT, and business users.

Improved security operations and IT operations efficiency. Reduced the number of security incidents requiring manual investigation by 19% and decreased the mean-time-to-resolution (MTTR) by 25%.

- **VM-Series virtual firewalls allowed teams to automate previously manual processes, provided improved visibility into network traffic, and offered log tracing and analysis capabilities.** With better visibility and data, teams were able to resolve problems faster and saw fewer security issues that impacted devices. The network engineer for a communications infrastructure firm said: "It's easier to manage. The logging from the cloud coming through the network to [Palo Alto Networks'] logging servers just gives it so much visibility into what's happening in the cloud. We go into Panorama, enter the configuration that they need, and then we push it out. So, the time savings on that versus somebody going to each firewall and actually having to enter that information is tremendous. And the time that it takes to do that is minutes. So, there's definite time savings for security to be able to act on something we are seeing from the logging information."

MTTR reduced by

25%

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of Palo Alto Networks VM-Series Virtual Firewalls," a commissioned study conducted by Forrester Consulting on behalf of Palo Alto Networks, September 2021.

STUDY FINDINGS

Forrester interviewed eight decision-makers and surveyed 132 decision-makers at organizations with experience using the VM-Series virtual firewalls and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits include:

- Reduced time required to deploy firewalls by 90%, and improved network and security team efficiencies by 80%.
- Reduced time to achieve proper security posture by 30%.
- Reduced number of security incidents by 18% and decreased MTTR by 25%.

Return on investment (ROI)
115%

Net present value (NPV)
$1.83M

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®