FORRESTER®

Palo Alto Networks VM-Series Virtual Firewalls Deliver Scalable Perimeter Security For Branch-Level Protection

Many organizations have embraced digital transformation at centralized data centers. Those with geographically dispersed locations and retail footprints are now recognizing the added benefit of creating software-defined branches. Palo Alto Networks VM-Series virtual Next-Generation Firewalls (NGFWs) provide powerful monitoring and segmentation capabilities to organizations' multicloud deployments, and in their virtual form factor are an ideal tool to extend segmentation and enable secure software-defined WAN (SD-WAN) connection at the branch level.

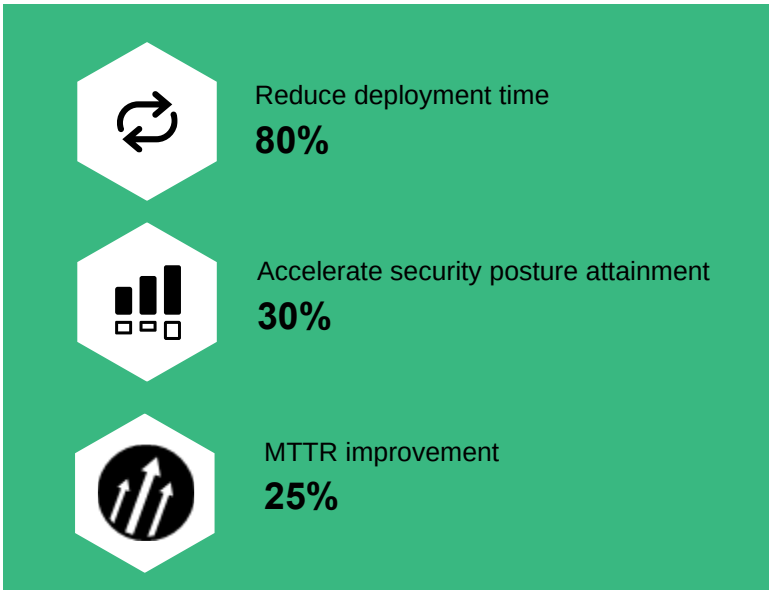
To better understand the benefits, costs, and risks associated with Palo Alto Networks VM-Series virtual NGFWs, Palo Alto Networks commissioned Forrester Consulting to interview eight decision-makers and survey 132 decision-makers who have experience using the solution and conduct a Total Economic Impact™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

This abstract will focus on two organizations using Palo Alto Networks VM-Series virtual firewalls for branch and perimeter security:

- A communications infrastructure firm using VM-Series firewalls to protect 80 branch locations across the United States.
- A beverage company using VM-Series firewalls to secure thousands of remote point-of-sale devices.

INVESTMENT DRIVERS

Decision-makers reported to Forrester that several factors led to these two organizations investing in Palo Alto Networks VM-Series firewalls:



- **Decentralized security tools with sluggish deployment.** Traditionally, organizations have deployed hardware firewalls at each branch location. This requires the organization to allocate space at each site and have technical resources on hand to deploy and manage the hardware. With legacy hardware, organizations need to wait for physical assets to be shipped and installed at branches. Travel times and the availability of technical resources could significantly delay installation and accelerating this process could prove costly.

  The communications infrastructure firm was opening new branch locations and adding them through acquisitions. It did not have enough resources or technical expertise to install and maintain physical hardware at multiple locations across the country simultaneously, nor did it wish

READ THE FULL STUDY HERE

to incur shipping costs for hardware. Delaying the opening of new branches or having acquired branches miss compliance requirements was out of the question.

- **Increasingly sophisticated attacks threatening security and a desire for layer 7 visibility and control.** As cybersecurity threats became more advanced, interviewees said their organizations sought more granular layer 7 visibility into their networks and required application-level insight.
- **Perimeter vulnerability.** Interviewed decision-makers said that their organizations lacked the resources and skills to enforce local segmentation between individual branches or points-of-sale and the rest of the network. The beverage firm's decision-maker said it had hundreds of remote point-of-sale terminals and lacked the adequate personnel to manually monitor traffic between them and the network. The organization explored using expensive specialized networking hardware, but this proved costly and prone to tampering or damage.

WHY PALO ALTO NETWORKS

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

- **Ease of deployment and maintenance in virtual form factor.** VM-Series firewalls can be deployed on existing servers, eliminating the process of shipping, installing, and maintaining physical hardware. Organizations can deploy with existing on-site resources, reducing overhead and accelerating deployment time.

> **"Our company said no [to] travel, so we wrote up instructions on how to install [VM-Series virtual firewalls] and found local people to do it. It's easier now and the roll out has been quick. We pretty much would have been standing still without going this route."**
>
> *Network engineer, communications infrastructure*

- **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. Organizations can manage branch security centrally with the same tools and policies for data center, private cloud, and public cloud networks.
- **Scalable solution to fit current needs.** With legacy firewall appliances, organizations would overprovision in anticipation of growing needs, leading to underutilized assets. VM-Series virtual NGFWs allow organizations to allocate and reallocate security based on immediate needs. The network engineer for the communications infrastructure firm explained: "The issue of redundancy has been simplified. Before we were buying two of everything to make sure we'd be covered."
- **Layer 7 visibility.** VM-Series firewalls offer application visibility across all ports, as well as applications, users, and devices, 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."

- **Advanced security with cloud-delivered security subscriptions.** Palo Alto Networks' cloud-delivered security subscriptions (CDSS) 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, advanced URL filtering, and zero-day threat prevention and sandboxing without additional overhead.

KEY RESULTS

The interviewed organizations experienced significant benefits because of their investment 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 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 NGFWs than traditional legacy firewalls that require hardware to be shipped, installed, and tuned. The interviewed global head of engineering at the 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."

  The interviewee from the communications infrastructure firm added: "There's also the time to spin up these devices and get them out in the field and the time involved in configuring all this equipment, so we're definitely saving that way. For example, with our old firewall, if you didn't size it correctly with an appliance, you would have to go out and purchase another appliance that was bigger. With [VM-Series NGFWs], you just put a different license in, and now you've got a firewall that's the right size."

- **Utilize existing skills and space.** VM-Series firewalls can be deployed on existing servers, reducing the need for shipping and storing additional hardware. Installation requires minimal work from on-site staff, as virtual machines can be preconfigured and tuned from central IT. The infrastructure communications firm installed VM-Series firewalls on existing white-box appliances and simply required on-site staff to install them, avoiding the need to send network or security specialists to remote locations. The interviewee explained: "We built base images that we knew we would need in every location. So, we've built base images that we could basically duplicate onto these generic appliances and send them out."

  The interviewee added**:** "I mean, a lot of times [before VM-Series] we subcontracted people to go out to the offices. A lot of times, you had to pay for travel if one of our engineers went up there. So, I would say maybe $5,000 per location just in installation cost. Getting the right people out there to do the job if [the location] had a router, and a switch, and firewall, and there are other devices that we were using as well. Getting somebody to connect all that up, we were probably [spending] around $5,000 [per] location for an office."

- **Centralized management and maintenance.** Using Panorama, organizations could monitor security and enforce a single policy model across on-premises deployments, private and public clouds, and branches. This strengthened their overall security posture and reduced management overhead. The interviewee from the communications infrastructure industry stated: "I could go to Panorama, which has our firewalls, [and] just type 'VM', and it tells me how many VM-Series Firewalls are throughout [our organization]. Again, those are made up of multiple types: cloud VMs [virtual machines], remote office VMs, and data centers."

Improved Security Operations and IT Operations efficiency. The implementation of the Palo Alto Networks VM-series firewalls reduced the number of security incidents requiring manual investigation by 19% and decreased the mean-time-to-resolution (MTTR) by 25%.

- **Improve visibility and reduce response times.** The network engineer for the 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 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 to do something like that. So, there's definite time savings for security to be able to act on something we are seeing from the logging information."

Enabled next-generation security without inhibiting business agility. VM-Series firewalls can be deployed quickly and seamlessly into a myriad of deployment types. With ease of deployment and confidence in protection, security teams can have branch locations operational and secure at a pace to meet ever-changing business demands.

- **Automate deployment processes.** The communications infrastructure interviewee stated: "Compared to a configured appliance, the VM is pretty fresh. I would say maybe a week timeframe, a week more to do the appliance than to actually do the VM. There's definitely a lot of time savings the way we're doing it. We have templates that we built for everything, and now, we actually have scripts that we write. You have your base image, you run your script, you type in the dynamic information that you need to configure it, and it basically runs within a day. You could have something ready to send out to an office."

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 8 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®