

TCO of Automating Network Firewall Virtualization

CALCULATING THE COST SAVINGS AND OTHER BENEFITS OF AUTOMATICALLY CONVERTING PHYSICAL NETWORK FIREWALLS TO VIRTUAL EQUIVALENTS

Current firewall architectures are complicated, do not scale and lock you in. That's why many organizations are looking at firewall virtualization. But it takes a lot of time, resources and specialized skills to build a virtualization platform that automatically converts physical to virtual firewalls and then efficiently maintains your virtual firewall environment.

With a turnkey platform that you subscribe to, you can save time and money by minimizing the need for DevOps while reducing project risk and speeding up time to deployment. You are also divorced from managing infrastructure and therefore save yourself the perennial headache of managing vendors and integration.

Let's look at the benefits of virtual firewalls versus physical ones and then the costs of various approaches.

BENEFITS OF VIRTUAL FIREWALLS WITH A TURNKEY PLATFORM VERSUS FIREWALL APPLIANCES

The benefits realized by using virtual firewalls with a turnkey platform that automates firewall virtualization are significant and outlined in the table below as they compare to the hardware-based firewalls.

Benefits	Firewall VMs Via Turnkey Platform	Firewalls Via Hardware Appliances
No need to tie up engineering resources. Customer or IT support can add firewall capacity for a new customer or user in minutes.	✓	✗
Zero-touch provisioning meaning no hardware to cable it's all software to call up new virtual firewalls, shuffle virtual firewalls, add firewall services and subscriptions to existing customer accounts.	✓	✗
No outdated appliances. Since VMs are a pooled firewall resource, MSSPs can fluidly replace VMs with new ones – always with the latest software version.	✓	✗
Zero downtime for any firewall during upgrades because upgrades are continuous.	✓	✗
Burst firewall capacity for customers can now be metered and charged for.	✓	✗
Cost-efficient pay-as-you-grow firewall capacity model so MSSPs never need to pay for more firewall capacity than customers are asking for today.	✓	✗
MSSP customers no longer need to share firewalls since each one gets dedicated virtual firewall with specific security services and subscriptions per their requirements.	✓	✗
No need to manage a whole variety of different firewall models and instead gets an elastic, pooled firewall resource consolidated around one platform.	✓	✗
Ends the process of having to do firewall refreshes every few years. Instead, just add what is needed, continuously, with all the latest upgrades/subscriptions included.	✓	✗
Infrastructure is evergreen as part of the subscription model so customers never have to deal with the infrastructure.	✓	✗

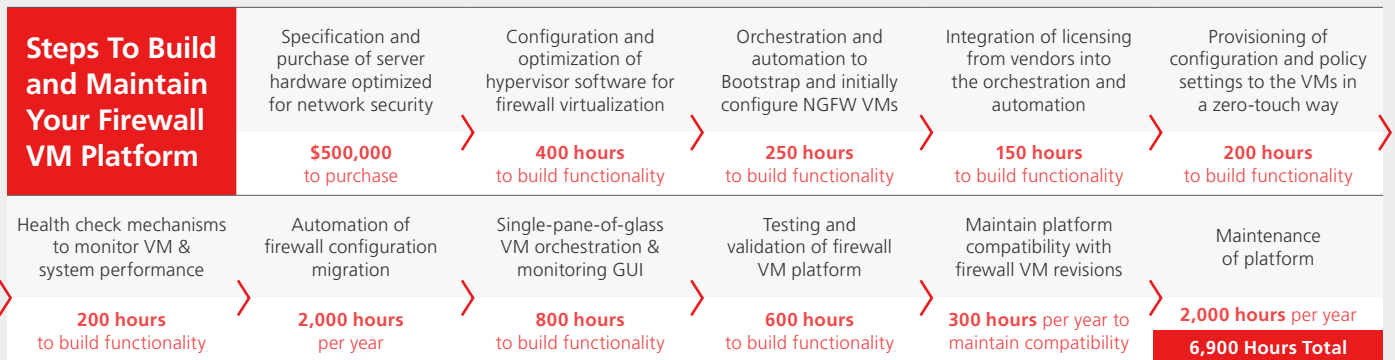
About Corsa Security

Corsa Security is the leader in scaling network security with the first turnkey network security virtualization platform that simplifies how large enterprises and service providers expand traffic inspection, increase threat protection and automate firewall virtualization, at much lower total cost of ownership (TCO). By tightly integrating virtualization with intelligent orchestration, Corsa Security streamlines deployment, management and migration of virtualized next generation firewalls (NGFW) for zero-touch network security operations. Customers subscribe to the Corsa Security services based on their current needs and then pay as they grow while never having to deal with the infrastructure. Learn how Corsa is revolutionizing network security at corsa.com.

THE SAVINGS ADD UP WITH AUTOMATED NETWORK FIREWALL VIRTUALIZATION

There are many steps and workflows needed in a system that automatically converts your physical firewalls to virtual equivalents and then orchestrates and manages them. Each step requires development from a team of experts in network engineering, security, systems integration and DevOps. And once the system is developed, on-going maintenance, upgrades, testing and validation are required which are a huge drain on resources.

To tackle all of this with a DIY approach can be a huge roadblock. With a turnkey platform, all of this is taken care of and you are able to instantly activate your new services built on virtualization.



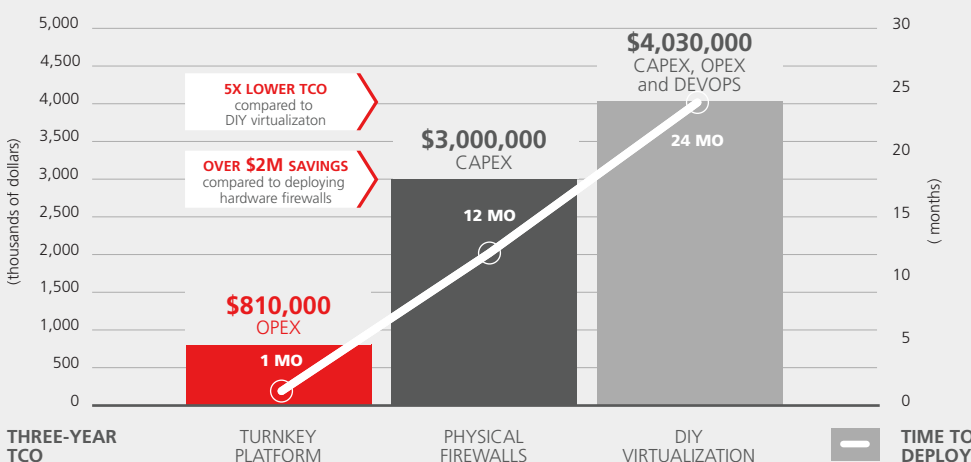
THREE-YEAR TCO ANALYSIS: PHYSICAL FIREWALLS VS AUTOMATED FIREWALL VIRTUALIZATION VS DIY FIREWALL VIRTUALIZATION

For our TCO scenario, we look at a network deployment that needs 50 firewalls and explore whether they should deploy physical or virtual ones and then whether virtualization can be done cheaper in-house. To go the hardware-based firewall route, they need to buy 50 physical firewalls with the appropriate license for 3 years plus 3 years of support. **This will cost \$3,000,000 CAPEX up-front and take over a year from conducting the RFP process to deploying the firewalls.**

If they want to go the virtual firewall work, and think they have the expertise in house to try it, we can use the table above to calculate the costs of the equipment plus the time spent by their team to build a virtualization platform. Based on our estimates, this will cost \$500,000 up-front for equipment plus between \$1,720,000 to \$2,150,000 in resources to build and deploy the platform. There will also be ongoing support and maintenance of \$345,000 to \$460,000 per year. **The total cost over 3 years will be \$3,255,000 to \$4,030,000 and it may take over 2 years to build the platform before you get started.**

To leverage a turnkey platform for automated firewall virtualization, like the Corsa Security platform, you will need to sign up for a monthly subscription but no longer need to worry about the CAPEX for hardware, pay-as-you-grow and have the flexibility of a common platform for different firewalls rather than being locked into the hardware you purchased in option 1. **The total cost of this route is \$810,000 OPEX over 3 years and you can be up in running in 30 days or less.**

5x lower TCO and 24X faster time to deployment



YOU CAN SAVE OVER 73% AND DEPLOY 12X FASTER if you subscribe to a turnkey platform compared to deploying hardware firewalls plus you eliminate up-front CAPEX.

BUT THIS IS NOTHING COMPARED TO THE 4-5X LOWER TCO AND 24X FASTER TIME TO DEPLOYMENT with a turnkey platform instead of DIY virtualization.