

Five Steps to Launch an Automated FWaaS

How to automate the virtualization
of network firewalls with increased
speed, agility, and simplicity



It is not uncommon for an enterprise to operate their firewall in a **suboptimal manner** and not take full advantage of application-level inspection and filtering capabilities. That's because current firewall architectures are **complicated and expensive**, require **continual monitoring** and lock you in to an **inflexible hardware platform**.

This is why enterprises no longer want to own and manage their own physical firewalls, which gives MSSPs an opportunity to expand their business by offering an **automated Firewall as a Service (FWaaS)** that replaces the enterprise's physical firewalls with **managed virtual firewalls**.

Managed Security Services market size is projected to grow from

31.6
billion (USD)

in 2020 to



46.4
billion (USD)

by 2025, at a
Compound Annual Growth Rate (CAGR) of 8%¹

¹ Managed Security Services Market by Type (Managed IAM, Antivirus/Antimalware, SIEM, and UTM), Deployment Mode, Organization Size, Vertical (BFSI, Government, Retail, Healthcare, Telecom, Utilities, and Manufacturing), and Region – Global Forecast to 2025”, published by MarketsandMarkets™

FIVE STEPS TO LAUNCH AN AUTOMATED FWaaS

1 2 3 4 5

EMBRACE
VIRTUALIZATION

DEPLOY A
TURNKEY PLATFORM

SIMPLIFY
YOUR DEVOPS

SCALE THE
SERVICE

INCREASE YOUR
PROFITABILITY

EMBRACE VIRTUALIZATION

To keep pace with growing and ever changing cyber attacks, enterprises are learning from the data centers. Instead of trying to manage physical network firewalls, they want to benefit from virtualization to make their network threat protection more flexible and agile to meet these changing demands. A virtualized FWaaS eliminates the need for ongoing hardware refreshes to scale network firewalls, instead giving enterprises an automated, self-service system with pay-as-you-grow capacity. For the MSSP, your team has more time available to focus on high-value, long-term security service innovations that add value for your enterprise customers.

“

When you adopt **virtualization** to replace physical firewalls, you have a platform that is **more flexible** and can **quickly address new requirements**, both now and in the future.

”

DEPLOY A TURNKEY PLATFORM

But virtualization can be hard. That's why it's important to find a turnkey virtualization platform that is built on a Secure Access Secure Edge (SASE) framework to converge network and security functions into a unified cloud-centric service. When the platform operates as "just-in-time" infrastructure, automating firewall virtualization is simple and quick; it can be done in minutes and if resources become scarce, you are alerted by the system. All it takes is the click of a button to add more firewalls, while the underlying infrastructure remains invisible to your customers. The additional resources are ready for use in minutes as opposed to the days or weeks it takes to set up hardware appliances.

“

By 2024, Gartner expects at least **40% of enterprises** will have **explicit strategies to adopt SASE**, a merger of network and security capabilities into a unified whole.

”

SIMPLIFY YOUR DEVOPS

Many who want to virtualize their firewall architectures are stymied by the time and effort required. There are multiple steps involved to build-your-own virtual firewall platform. These include: configuration and optimization of hypervisor software; bootstrap and initially configure NGFW VMs; integration of licensing from firewall vendors; health check mechanisms; and much more. Not to mention the fact that you need to maintain and upgrade this platform. But you can automate the virtualization of physical firewalls with a turnkey platform that takes care of all of these steps so a customer support team can deploy the service and you simplify your DevOps.

“

One of the greatest benefits of automation is **simplicity**. It allows you to **focus** on what sets you apart as a business rather than getting bogged down with menial and repetitive tasks. You gain **increased agility** as well as **costs savings**.

”

SCALE THE SERVICE

When the virtual FWaaS platform supports multi-tenancy, you can offer specific services and capacity to individual customers in minutes and quickly scale your service offerings. The platform needs to integrate with monitoring, billing, CRM, CMDB, and inventory tools so your team continues to use the same processes as they always have except that it's even simpler. And when one of your customers need more firewalls or capacity, you can add virtual firewalls in the increments that suit their traffic patterns with the click of a button. There is no more upsizing of hardware firewalls or ongoing hardware refreshes to keep up with network security demands.

“

According to Gartner, firewalls are typically on a **five-year refresh cycle**. For each refresh, organizations need to evaluate everything from throughput capacity to required features and deployment criteria to configuration options.

”

INCREASE YOUR PROFITABILITY

Enterprises want to outsource their firewalls to MSSPs offering virtualized FWaaS to improve their network security. To compete in a crowded space, MSSPs offering FWaaS need a SASE framework that unlocks operational efficiencies to deliver top rate service velocity. With a turnkey virtualization platform that automates the migration of physical firewalls to virtual, you are not only offering a service that your customers are demanding but doing so in a new way that will clearly impact your bottom line too. By eliminating the need for DevOps skills, offering a low cost of entry and pay-as-you-grow model, MSSPs can reduce their network operations expenses resulting in a more profitable service.

WITH A TURNKEY PLATFORM AND PAY-AS-YOU-GROW MODEL YOU GET:



Greatly reduced up-front costs



A future-proof SASE framework



Accelerated ROI



Spin up new services quickly

There is an amazing opportunity to help your enterprise customers replace their physical firewalls, which they no longer want to own or manage, with virtual firewalls. **But you need to automate firewall virtualization through intelligent orchestration for zero-touch network operations.**

A turnkey platform built on a SASE framework quickly and easily lets you launch an automated FWaaS that will not only grow your company, but frees up your team to focus on strategic priorities and other new service innovations.

**AUTOMATE YOUR FWaaS
WITH INCREASED SPEED,
AGILITY, AND SIMPLICITY**

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
or email info@corsa.com

TS-CDD0018-000, Rev 001