



# Driving MSSPs' Growth with Flexible and Advanced FWaaS



The market is growing rapidly for resellers and service providers (SPs) that plan to offer Firewall-as-a-service (FWaaS) to organizations who want to get rid of firewall hardware appliances, simplify their IT infrastructure and stick to the rising use of cloud services. According to Gartner, by 2025, 30% of new distributed branch office firewalls deployments will switch to FWaaS, up from less than 5% in 2020 <sup>(1)</sup>.

FWaaS is the leading option that Managed Security Service Providers (MSSPs) could offer as the first line of defense against intrusions and advanced threats. FWaaS brings next-generation firewall (NGFW) capabilities, such as intrusion prevention, web filtering, anti-malware and application control, to protect all enterprise edges -data centers, branches, mobile users, and cloud infrastructure, while improving visibility and control, and ensuring consistent policies across the organization.

FWaaS enables MSSPs to deliver an all-in-one protection that combines cloud-based NGFW capabilities with 24/7 support, administration, and monitoring, insured by their in-house staff of security experts. Moreover, FWaaS provides their end-customers agility and flexibility by scaling out cost-effectively, adding or removing resources and capabilities when needed, at predictable and easy to calculate fees.

However, to succeed in this transition and seize this opportunity, prospective MSSPs need an affordable, integrated, scalable, and multitenant solution that enables them to rapidly deploy, configure, and manage a high volume of firewalls, through zero-touch provisioning, service automation and orchestration, and centralized management. Further, the solution has to allow on-demand licensing as a highly flexible option for both initial and subsequent deployments to adapt to the fast-changing business requirements.

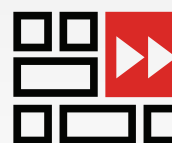
## How to catch-up the trend with Fortinet NGFW?

Fortinet's NGFW, FortiGate, provides the industry's highest performance, value, and flexibility, and delivers ultra-low latency using purpose-built security processor (SPU) technology, along with the most advanced threat-intelligence and threat-protection capabilities.

FortiGate is powered by the FortiOS™ operating system, the most widely deployed security operating system in the industry. Recently introduced FortiOS 7 expands the ability to deliver consistent security across hybrid deployment models and features the industry's first video filtering service to provide even more granular protection for organizations and users with new video-intense content consumption patterns driven by the increase in work-from-home.

# 30%

**of new distributed branch office firewalls deployments will switch to FWaaS by 2025 <sup>(1)</sup>**



**Fortinet is named a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls**

FortiGate is available in various form factors including hardware and virtual appliances, cloud-delivered, and Software-as-a-Service. This enables MSSPs to deliver high-performance FWaaS to their clients by either deploying FortiGate in their data centers in a mixed infrastructure of hardware and virtual appliances, or as a cloud-based service integrated with all major cloud providers and software-defined network (SDN) platforms, all integrated and managed from a common centralized management console.

FortiGate virtual appliances feature all of the security and networking services common to traditional hardware-based FortiGate appliances. They offer extensive flexibility through the support of a multitude of deployment methods across various private and public cloud, and allow both on-demand (PAYG) and bring-your-own-license (BYOL) licensing models, to fit any infrastructure requirement for rapid deployment capability whenever and wherever it is needed.

Lastly, FortiGate is independently tested and validated for best security effectiveness and performance. Fortinet is named a Leader in the 2020 Gartner Magic Quadrant for Network Firewalls, and for the second year in a row, Fortinet has been recognized as a Customers' Choice in the February 2021 Gartner Peer Insights 'Voice of the Customer: WAN Edge Infrastructure' in recognition of the reviews that customers have provided for our Secure SD-WAN solution. We believe this customer validation further highlights that Fortinet's simple, secure, and scalable platform approach resonates with customers across all industries.

### **Deploy FWaaS with Fortinet today, build many services tomorrow**

Leveraging the FortiGate-enabled FWaaS, MSSPs have the potential to deliver consistent security services and expand their portfolio with other value-added security services through the Fortinet Security Fabric, a broad, integrated and automated cybersecurity platform, with a rich open ecosystem, that spans the extended digital attack surface and cycle, enabling self-healing security and networking to protect devices, data, and applications. The Fortinet Security Fabric integrates solutions across the key cybersecurity domains-network, users and devices, and cloud – all administered with a single management console. It can be extended across organizations via seamless integration with diverse Fabric-Ready Partner solutions to secure and simplify their hybrid infrastructure on the journey to digital innovation.

This unified approach leverages prevention and detection of known and unknown attacks using continuous threat intelligence from AI-powered FortiGuard Security Services, deep analytics through FortiAnalyzer, secure against new zero-day and advanced threats with FortiSandbox, and harness FortiManager to easily manage and update the FortiGate and other security assets – hardware, virtual or both – from a single pane of glass.

As these security solutions are integrated, scalable and multi-tenant from the ground up, they enable MSSPs to reduce their capital expenditures (CAPEX) as well as optimize their operational expenses (OPEX), with a greatly reduced time to onboard customers. Moreover, they will allow MSSPs to recruit new clients, increase their footprint at existing ones, and improve operational efficiencies and customer value for a high level of revenue streams and margins.

**For MSSPs and SPs that want to take the leap and offer an efficient, scalable, and bespoke service, now is time to move forward and push the partnership with Fortinet a step further.**

(1) Gartner, Gartner Magic Quadrant for Network Firewalls, Rajpreet Kaur, et al., 9 November 2020.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Gartner, Gartner Peer Insights 'Voice of the Customer: WAN Edge Infrastructure, Peer Contributors, 5 February 2021.

Gartner Peer Insights Customers' Choice constitute the subjective opinions of individual end-user reviews, ratings, and data applied against a documented methodology; they neither represent the views of, nor constitute an endorsement by, Gartner or its affiliates.



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.