FORTINET

EXCLUSIVE NETWORKS

WHITE PAPER

Why Fortinet For My MSSP?

Real-world Reasons Fortinet Dominates the MSSP Market

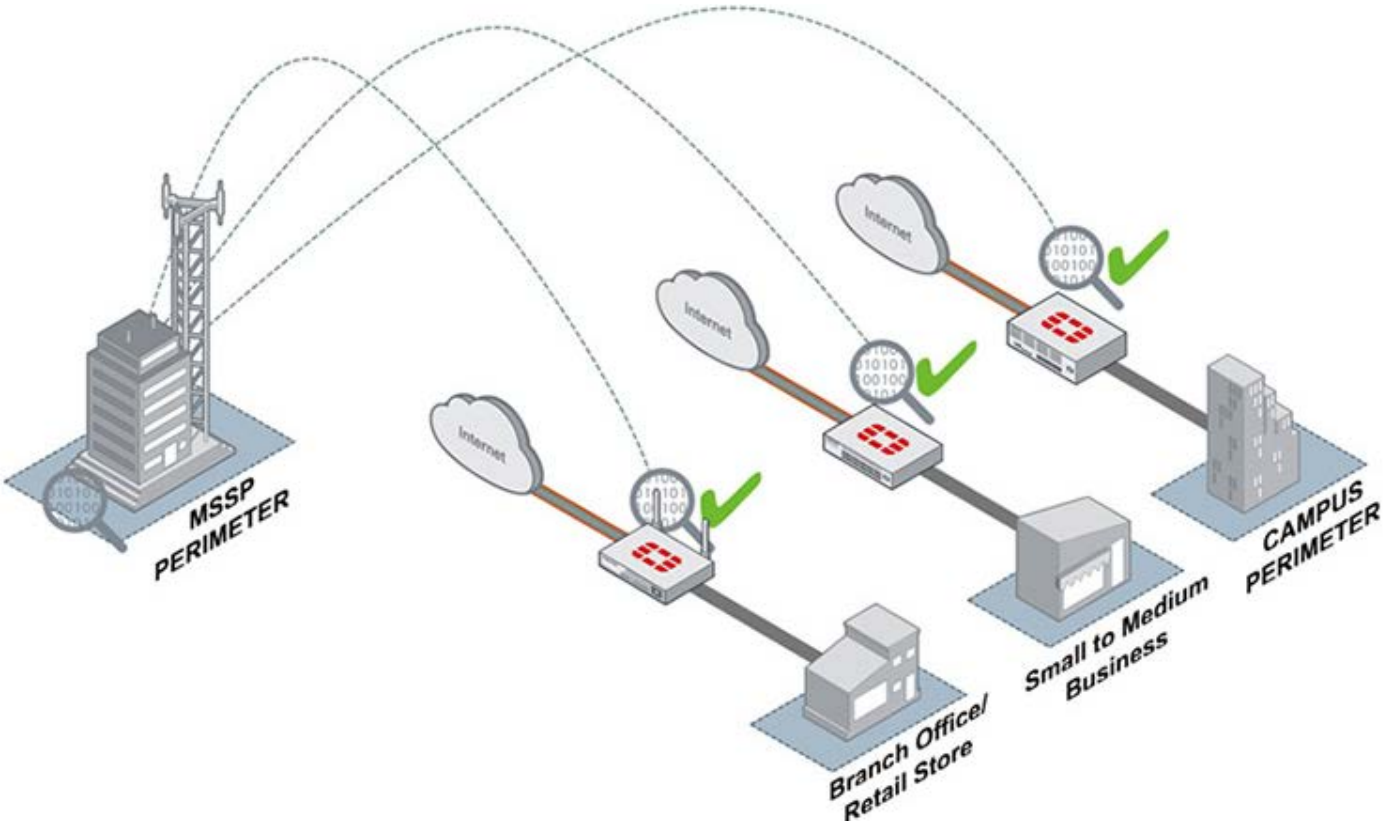
Introduction

Businesses worldwide are struggling to secure their networks against determined attackers that are commonly two steps ahead of the defenders. There is a perfect storm of challenges facing organizations wanting to expand into the new digital market without compromising their security or brands.

- Studies show that not only is the number of network attacks increasing, but the cost of being breached has also continued to rise per incident.
- Media attention on high-profile security breaches has also created a higher level of awareness among business leaders as to the risks and costs of security breaches to businesses.
- The depth and breadth of criminal and state-sponsored cyber criminals, who are often well-funded and are developing increasingly sophisticated attacks, are better understood by security buyers today than ever before.
- And at the same time, the security skills shortage continues to widen.

As a result, many CISOs are looking to migrate some or all of the risk out of their IT departments and into the hands of professionals such as managed security service providers (MSSPs).These MSSPs are expected to anticipate and secure networks against innovative and determined threat actors.

This responsibility comes with considerable challenges, including defending scores of customers while balancing security effectiveness against business profitability. As a result, today's MSSPs need tools that are highly scalable, support multitenant environments, and provide robust, single-pane-of-glass management and orchestration.



They also need reliable, high-performance, and cost-effective security that allows their networks to dynamically adapt to changing risk environments, and that can also scale to secure hundreds, thousands, or tens of thousands of customers at once, even when traffic spikes unexpectedly.

To make this happen, MSSPs must select a security vendor that not only ensures their own success as a service provider, but also the security of the customers they protect.

With hundreds of thousands of customer nodes under management, and billions of dollars of assets under their protection, the world's top MSSPs hold their firewalls to extremely high standards for reliability, functionality, and flexibility. So, when considering solutions to address their complex requirements, Fortinet stands above the crowd of security vendors by providing stable technology combined with specialized support built for carrier-class multi-tenancy and managed services.

Functions of the MSSP

At its core, an MSSP must provide two kinds of basic services: security device management and continuous monitoring. Customers with multiple locations and business-critical applications running across the network have stringent uptime requirements, so device management and monitoring are crucial to maintain business productivity.

Many service providers also add security analytics and threat-intelligence services to help mitigate new attacks, including actionable intelligence and a comprehensive view of the distributed security infrastructure. Going forward, these firms will likely differentiate themselves in new areas such as security analytics, threat intelligence, information portals, and customer service.

Many MSSPs will also want to provide security remediation, incident response, compliance services, or loss prevention to further differentiate them in the market. Securing thousands of customer locations, meeting service delivery service-level agreements (SLAs), and balancing profitability with engineering headcount and infrastructure are ongoing challenges facing MSSPs, so they need specialized security vendors that understand their business model and can help them meet customer requirements.

Why Top MSSPs Standardize on Fortinet

Frost & Sullivan recently recognized that "Fortinet has achieved a dominant position with MSSPs with its FortiGate line of high-performance firewalls." In their recent ranking of over 100 network security platforms, Fortinet scored "the highest possible ranking among North American MSSPs."

Fortinet covers critical aspects of an MSSP's business model like no other security manufacturer—offering the best in multitenancy, the most hardware flexibility, the highest performance through hardware acceleration, and the lowest TCO of any security vendor.

Why Fortinet For My MSSP?

Fortinet understands that the MSSP is a strategically differentiated channel partner, and for years has developed technology specifically suited to the MSSP business model. A foundational tenet of our strategy is to enhance our MSSP Partners' profitability.

Our unique channel enablement strategy creates a symbiotic relationship with MSSPs, as their customers rely on Fortinet products for network uptime and application availability, while Fortinet relies on the MSSP to win new customers with a blend of professional services and high-touch support that reduces our own cost of support.

Fortinet's MSSP innovative strategy can best be described in four key pillars or areas of influence: Vision, Technology, Economics, and Support. These areas capture many of Fortinet's differentiators for MSSPs, and help clarify the reasons for Fortinet's dominance in the space.

Vision

Fortinet's vision of security designed to operate as an integrated whole, while providing cost-effective performance and protection is key to its long-term position as a strategic business partner for network and managed security services providers.

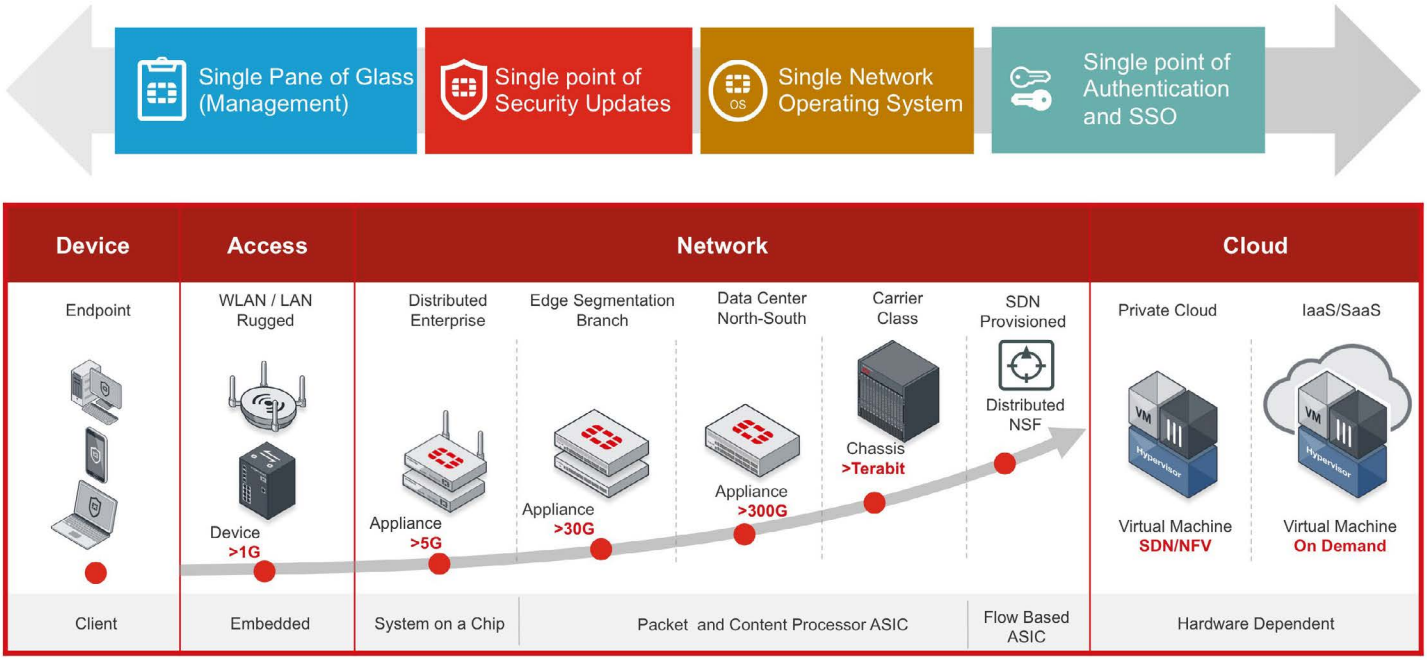
Fortinet's Strategic Visionary Investments

- Industry-leading MSSP partner program
- Global support from dedicated MSSP teams
- Enhanced technologies service development support
- Specialized team supporting best practices, customization, and automation
- Cloud-premium brand and broad support
- Software-defined network (SDN) and network functions virtualization (NFV) development partner

Fortinet's vision focuses on ongoing security innovation, advanced threat intelligence, delivering the fastest security platforms on the market, operating system (OS) portability to secure the cloud and Internet of Things (IoT), and leadership in SDN and NFV.

Fortinet's vision is actualized around our end-to-end security fabric that allows MSSPs to secure nearly any environment. This approach not only improves security, but also reduces operational costs and complexity for professional service organizations that are entrusted to secure their customers' networks.

Fortinet also leads the way in creating innovative security solutions with an integrated security approach for every business computing environment.



Many security vendors outsource hardware platforms, threat intelligence, or signature services to third parties. This is much less expensive than doing this work yourself. But Fortinet owns and operates all of our own technology, from the hardware to the software, and from subscriptions to threat intelligence. This ensures that MSSPs that deploy our gear are never unpleasantly surprised with unexpected changes in vendors or suppliers.

The value of Fortinet's vision is demonstrated through consistent industry recognition of the efficacy of our technology and threat intelligence by objective, third-party testing outfits like NSS Labs, ICSA, VB100, CVE, and AV Labs.

Threat Intelligence Made Actionable

The only way to mitigate risk in today's threat environment is with actionable threat intelligence, which is why the proprietary advanced threat intelligence and signature service from FortiGuard Labs comes standard on the FortiGate firewall. Our threat intelligence and signature service is recognized and certified as an industry leader for defense against a wide variety of threats, and trusted to secure some of the most sensitive networks in the world.

FortiGuard Labs threat intelligence is the best in the business, with 200+ security analysts and 2.5 million sensors worldwide that provide a crowdsourcing-style solution to risk mitigation, and over 90 distribution servers located worldwide to serve signature updates. We intercept 40 million threat events per minute, and simultaneously track over one million mobile viruses and 220+ botnets. Since the team's inception, they've discovered 197 zero-day threats in advance of their ability to compromise a customer's network—the most in the security industry. The result is higher catch rates and fewer security breaches in Fortinet defended networks.

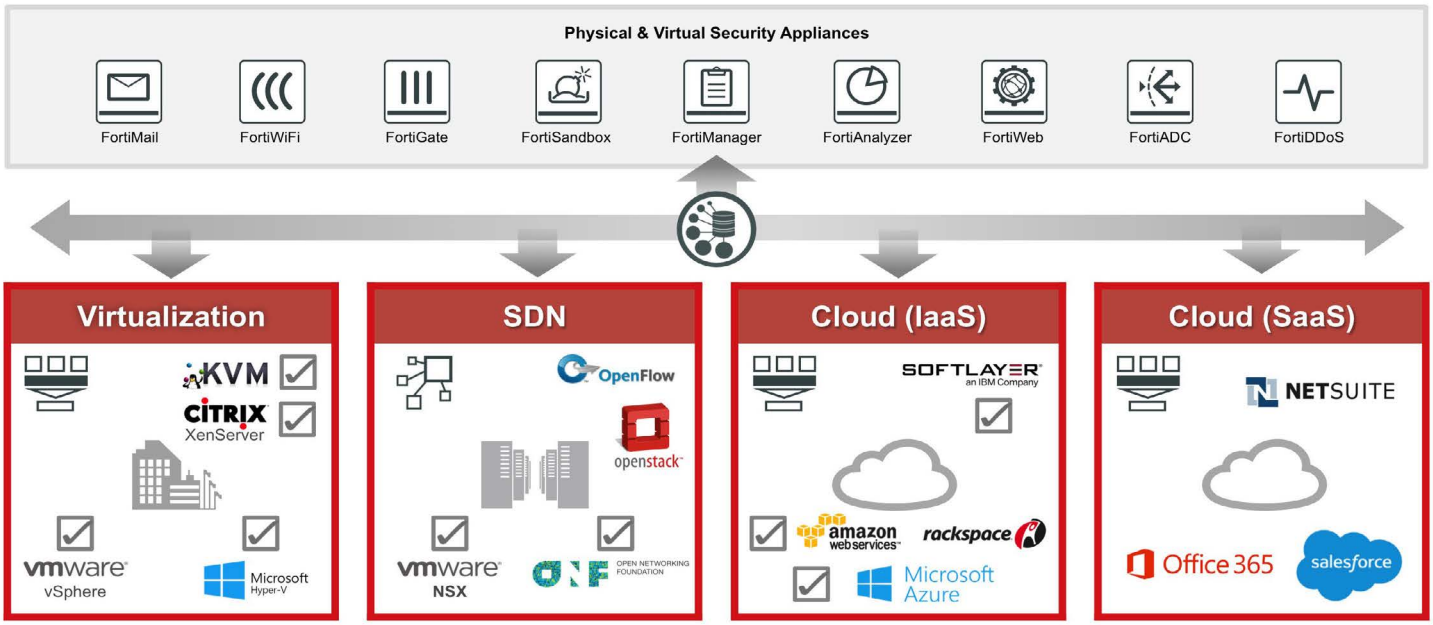
Strength in the Cloud—Securing the Ongoing Migration

According to Gartner, 73% of chief operating officers (CIOs) are budgeting for cloud migration in order to capitalize on the promises of 64% lower total cost of ownership (TCO) and a 68% efficiency increase in IT staff operations, along with 81% less downtime, and a whopping 560% five-year return on investment (ROI). This is why IDC predicts that 50% of workloads will move to the cloud by 2018.

From a security perspective, one of the challenges companies face is implementing a consistent security policy for data that moves between their on-premises and cloud environments. To address this challenge, we have partnered with major cloud service providers and virtualization vendors to ensure integrated defense across cloud workload migrations. This enables partners to use a single security platform for their customers' cloud and premises-based security requirements for consistent management, policy enforcement, and visibility.

Partnering closely with vendors like VMware, Microsoft, and Amazon, Fortinet develops integrated, next-generation security capabilities so service providers can stay on the leading edge of the technology and capitalize on "service injection" opportunities offered by SDN and NFV.

Fortinet's FortiGate firewall also supports all of the virtualization platforms and hypervisors, as well as leading open-source SDN protocols and advanced application programming interfaces (APIs) for orchestration and automation, to ensure the security of new, highly mobile workloads. Fortinet's web application firewall and database security solutions also provide the layered security needed to secure business applications in the cloud.



Technology

Ten out of 10 top global carrier MSSPs use Fortinet in some of the busiest, highest-performance networks in the world. Why is that?

There are several reasons:

Technical Dominance in MSSP Market

- Native multi-tenancy
- Customizable centralized management and reporting
- Extreme performance scalability and platform flexibility
- Ongoing advanced technology research and development

All of Fortinet's flagship security products support multi-tenant services and granular, delegated administration. This makes it easy for a service provider to host multiple customers on a single-security appliance or provide delegated administrative capacity and single-pane-of-glass management for the security infrastructure.

FortiGate firewalls also offer a broad suite of security controls that provide MSSPs with a full-featured platform to deliver advanced, adaptive security functionality to their customers. This allows the MSSP to deliver a wide variety of managed security services to match their customers' security requirements.

Performance Advantage—Slow is Broken

In the real world, network speeds are increasing exponentially, and MSSPs need security that can keep up with accelerating requirements.

Security performance has been a differentiator for Fortinet since our hardware-accelerated appliances first began shipping. This performance advantage is achieved through our ongoing investment in application-specific integrated circuits (ASICs), designed to process security and content inspection at speeds that off-the-shelf CPUs used by other vendors simply cannot match.

In fact, Ixia BreakingPoint recently recognized the FortiGate 5000 series chassis as the World's Fastest Firewall after rigorous real-world traffic testing. This is in addition to NSS Labs reports that detail FortiGate's low latency, high performance, and exceptional catch rates with a 99.8% security effectiveness score.

Additionally, Fortinet's platform flexibility allows service providers to deploy the same operating system and capabilities in any size environment, whether it's three point-of-sale (POS) machines, 300,000 workers accessing the Internet through a network firewall, or highly distributed users leveraging cloud-based applications.

Platform Flexibility—Deploy Anywhere

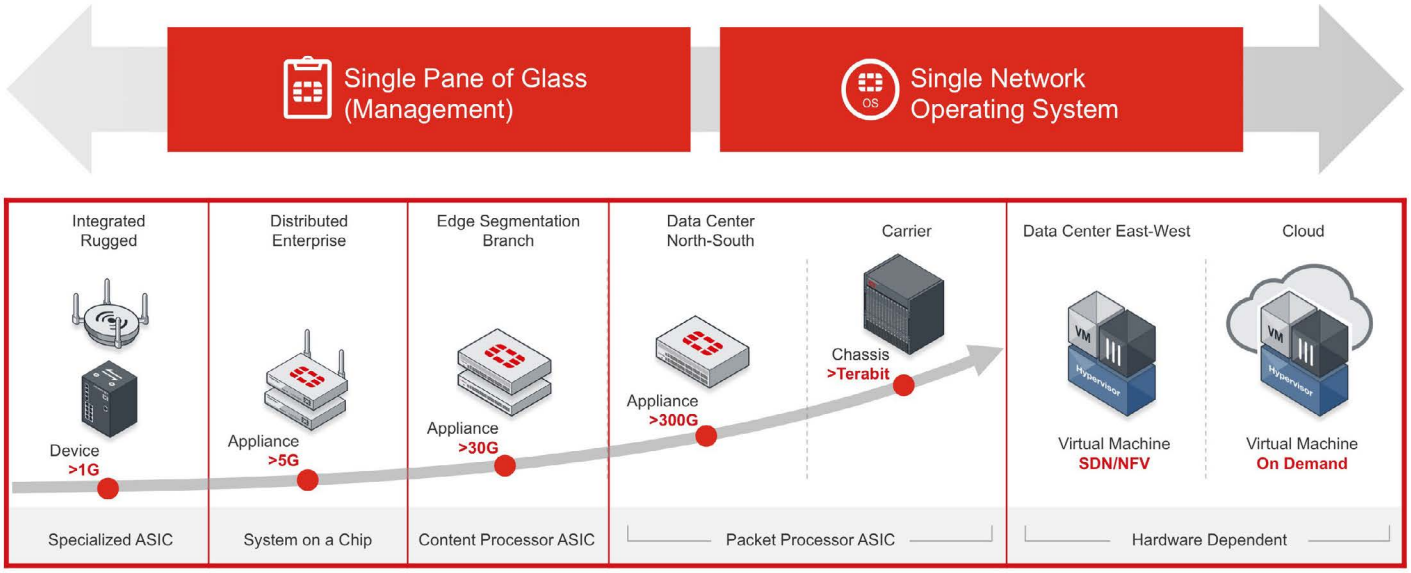
From the smallest devices to mid-sized and chassis-based systems, even virtual machine (VM) platforms, Fortinet offers the greatest flexibility in coverage, thereby allowing MSSPs to keep their operational costs down while keeping a close handle on hardware cost of goods sold (COGS).

FortiGate solutions also support virtual security domains (VDOMs), allowing MSSPs to leverage a single device to secure multiple customers. This is common among carriers, as larger FortiGate chassis are used to secure hundreds or thousands of customers on a single, high-availability security platform.

This native virtualization also meets the most rigorous security standards for the separation of traffic, and is used for highly secure government and carrier environments meeting Institute of Chartered Secretaries and Administrators (ICSA), Federal Information Processing Standards (FIPS), and Common Criteria standards for separation of customer traffic, while meeting all the security behaviors of a dedicated hardware device.

This allows the MSSP to deploy virtualized FortiGate appliances into some of the most stringent security environments, and is another reason FortiGate is the firewall of choice for MSSPs worldwide.

The Fortinet Security Fabric takes this functionality even further by allowing customers to tie their local Fortinet deployments to the cloud-based security provided by their MSSP. This allows them to create consistent policies between their on- and off-premises environments environments, and manage and orchestrate security through a common management interface. This allows threat intelligence to be shared dynamically between their local network and the cloud, and to impose threat intervention measures anywhere along the data path.



Centralized Management—Single Pane of Glass

For centralized management and reporting, Fortinet offers FortiManager and FortiAnalyzer, which provide fully featured, industrial-grade capabilities to deploy, manage, and report on thousands of devices.

Fortinet's powerful centralized management, with native support for multi-tenancy, and extensive customization options through API integration—along with advanced automation—ensure MSSPs remain efficient with their most expensive service delivery component: engineering time on task.

Fortinet centralized management supports a great deal of customization through APIs so that service providers can brand their management portals and offer co-administration and delegated administration.

One way to illustrate MSSP service value to the customer is through logging and reporting. FortiAnalyzer is designed to provide granular reporting on hundreds or even thousands of devices in a single set of reports, giving the customer a single-pane-of-glass view across their security deployment. These include:

- Logging of security events pulled from a variety of Fortinet security products
- Event management to highlight important activity and alerts based on pre-defined rules
- Simplified reporting across all FortiOS-enabled devices
- Drill-down functionality for detailed analysis

FortiManager provides key functionality and a conduit to customization and automation:

- Support for tens or thousands of devices
- Administrative domains for delegated admin and multi-tenancy
- Mass policy template deployments
- Large-scale firmware and FortiGuard updates
- Objects for common management functions

Emerging Models For Agile Service Delivery

In order to meet the demands of new networking paradigms being adopted by customers, many providers are looking to evolve their managed service offerings to align with the elastic and agile infrastructure and application delivery models, such as public clouds and Software-as-a-Service (SaaS), that many organizations are implementing.

The implementation of architectures such as NFV enables providers to build out network and security services as virtual network functions (VNF) on commoditized hardware, enabling a scale-out infrastructure that can efficiently and cost-effectively meet growing demand. At the same time, centralized network orchestration can automate service insertion and chaining to enable rapid deployment and delivery. Fortinet's extensible platform and validated integration efforts, not just with SDN but with NFV management and orchestration (MANO), enables the rapid deployment of new service models, such as virtual customer premises equipment (vCPE).

In addition, new pay-per-use (PPU) service models allow for services to be offered on demand or through self-service catalogs. But implementing these PPU services requires significant up-front operational expenditure (OPEX)-based infrastructure costs for providers. Fortinet's new platforms, such as our VM On-Demand program for providers, addresses this challenge by automating licensing, provisioning, metering, and billing with a turn-key deployment. This enables providers to rapidly stand up new on-demand service offerings and align costs with pay-as-you-go revenues.

Economics

MSSPs have distinct cost components to consider in their management accounting processes because they preside over a complex business model with profit margins as heavily dependent on operational efficiencies as they are on hardware and software costs.

Average revenue per unit (ARPU) is a key factor for MSSPs as they consider selecting security platforms for a managed security service. MSSPs are obviously looking for a higher ROI, as they will often own the security asset and depreciate it accordingly.

Fortinet delivers the highest ARPU in the industry due to multiple unified threat management (UTM) controls and high-performance hardware, allowing the MSSP to convert more services into revenue on a single device. Those aren't the only reasons:

- High-demand, revenue-generating controls
- Inclusive threat-intelligence service
- Native virtualization per device
- Enhanced technologies investment

This flexibility and functionality allows MSSPs to turn on more billable security services and secure more users behind one device than any other manufacturer.

MSSPs also gain healthy returns when they are able to cover broad customer sizing requirements with a single-security vendor. Training engineers on a single platform, as opposed to having to support multiple vendors, allows the MSSP to keep operational and training costs down.

Of course, operational expenses are the biggest cost component in any managed services practice because smart humans are expensive. The more time your engineers spend on configuration and management, the lower your profits. While effort is spent weighing hardware and software costs when considering a security vendor, remember that operational costs are usually the real margin killers.

This is why the Fortinet Developer Network was designed to develop solutions to help improve operational efficiencies, and create a community around automation and orchestration of security workloads. Here are a few examples:

FortiDeploy is an example of MSSP-specific tools built to improve operational efficiencies and keep costs down on mass deployments. This tool allows for the bootstrap deployment of FortiGate firewalls—thousands at once when needed—where the MSSP can provide a minimal configuration.

Once connected to the network, FortiDeploy will register the device, populate the new firewall into the proper customer administrative domain (ADOM), and push down a complete configuration. This process is fully automated, which saves the MSSP both time and money.

FortiUpgrade is another tool designed specifically for MSSPs to allow them to upgrade devices without manually stepping through each OS revision, which can be a time-consuming effort, and where skipping a step could turn your firewall into a paperweight. FortiUpgrade walks through this process automatically, ensuring that proper steps are taken in updating a device to the newest code, thereby saving time and money while

TCO is another important consideration, as this encompasses the direct and indirect costs of deploying and managing a security platform. Fortinet provides the lowest TCO for a variety of reasons:

- Scalable, centralized management and open-source APIs for automation
- Cost-effective hardware
- Simplified subscription and support
- OS uniformity across hardware and virtual platforms
- Non-user-based bundled pricing
- Special pricing models for OPEX
- Mass deployment and automation toolkits for improved operational efficiencies

Fortinet presents the lowest TCO and highest ARPU of any security manufacturer.

serving as a profit enhancer for the MSSP.

FortiPrivateCloud is a re-brandable, customer-facing interface that allows an MSSP customer to access logs and reports, as well as make changes to security policies as defined by the MSSP. This same service can cost hundreds of thousands of dollars and months of time to develop and maintain. But Fortinet makes it available as a private cloud-based service, sparing the MSSP the time and money needed to hire a coder to write up and integrate a customer portal for their offering.

Support

Fortinet's MSSP vision is global, with dedicated teams in each area of operation functioning under a worldwide standard for MSSP empowerment.

Fortinet MSSP specialists have backgrounds in managed security service provider operations, product development, and training that cross business development and engineering disciplines, and they understand the executive, operational, and sales aspects of the business.

This expert level of support, along with the specialized content and tools they create, dramatically shortens market delivery timeframes and product development cycles, and increases the likelihood of a positive product launch while improving go-to-market results.

Fortinet's MSSP teams also function as subject matter experts in an overlay organization that supports field sales, providing specialized support for partners with a mission of improving profit margins and operational efficiencies.

This specialized support comes in the form of product development, financial modeling, and engineering assistance, along with operational best practices documentation, market intelligence, and MSSP-specific sales collateral and go-to-market support.

The MSSP team also administers Fortinet's industry-leading MSSP Partner Program, which seeks to empower MSSPs to increase their margins while improving security effectiveness.

The main benefits of the MSSP Partner Program include:

- Programmatic discounts for OPEX MSS
- Exclusive engineering and marketing content
- Expert consultative support
- MSSP ecosystem

Selecting a security vendor in today's congested and confusing security market can be a real challenge. Fortinet has more experience and proven success in helping MSSPs build and deploy profitable managed security services than any other vendor in the industry. We have trained, professional teams ready to help you today.

Copyright © 2020 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.

November 13, 2020 1:26 AM

839519-0-0-EN

D:\Fortinet\Image Graphics\835741 - A definitive guide to MSSP Offerings\wp-why-fortinet-for-my-mssp-11132020