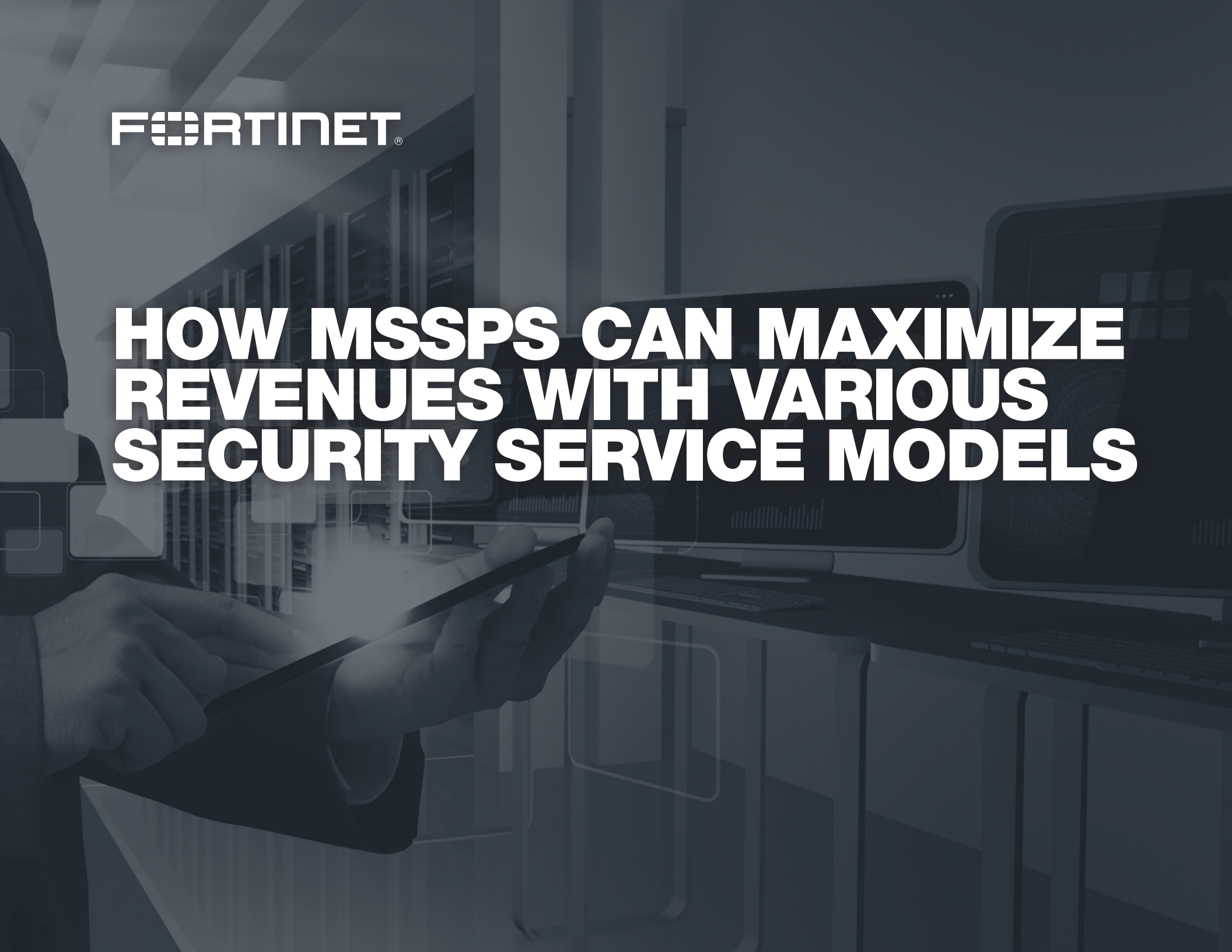

HOW MSSPS CAN MAXIMIZE REVENUES WITH VARIOUS SECURITY SERVICE MODELS

CONTENTS

INTRODUCTION

Businesses large and small are facing cyber attacks that are growing in number, sophistication, and cost. Due to the prevalence of high-profile security breaches, business leaders are increasingly making network security a top priority. Yet, their CISOs have an inadequate supply of high-level security skills to deal with the threats.

As a result, many organizations are looking to migrate some or all of the risk out of their IT departments and into the hands of managed security service providers (MSSPs). According to one estimate, the worldwide IT security services market will grow to $57.7 billion in 2018.[1] Another forecast pegs cumulative global spending on cybersecurity products and services from 2017 to 2021 at more than $1 trillion.[2]

If you are an MSSP product leader or executive, this burgeoning market represents both an unprecedented opportunity and a challenge. To win and retain business, you must demonstrate the ability to deliver security services more competently and less expensively than clients can achieve on their own. This eBook will show you how you can do so by optimizing and monetizing your security services.

[1] "Gartner: IT Security Spending to Reach $96 Billion in 2018," Dark Reading, December 2017.
[2] "Cybersecurity Market Report," Cybersecurity Ventures, May 2017.

01 MSSP DELIVERY MODELS

Companies that call themselves managed security service providers vary widely. Some originated as MSSPs. Others are managed service providers or cloud service providers that have seen the need to offer security as part of their IT service portfolio. Still others are security technology vendors that have identified a potential market for services that leverage their products.

Whatever path led your company to become an MSSP, it's an ongoing challenge to find the optimal breadth and depth of services that maximize revenues while minimizing operational costs. In this section, we will present several managed security service models. We'll discuss why you may want to transition from one model to the next and how you might go about it.

MODEL 1: ON-PREMISES SERVICES WITH A NOC

The core of managed security services focuses on threat prevention, using customer-sited or cloud-based next-generation firewalls (NGFWs). In support of these devices, many MSSPs offer multi-tenant network operations center (NOC) services where the staff provides 24-hour monitoring and device management.

If you have established a strong relationship with a leading firewall vendor, you will be able to stay at the cutting edge of threat prevention technology and best practices. As your clients' attack surfaces expand, however, you will find that threat prevention isn't enough. It is imperative to add threat detection and mitigation solutions to your security services arsenal to provide complete protection for your clients.

Because threat detection and mitigation involve an extensive range of advanced technologies, implementing these technologies all at once may not be practical. A stepwise introduction of increasingly sophisticated security capabilities will allow you to verify the profitability of each new service element before adding the next.

MODEL 2: ADVANCED SERVICES WITH A SECURITY FABRIC

A logical extension of core-managed security is to capitalize on the firewalls you already have, by adding web application security and sandboxing functions to those devices. Web application firewalling is now crucial, as the explosively growing universe of SaaS applications is one of the easiest targets for cyber crime. Meanwhile, sandboxing functionality can quarantine suspicious programs or code before they enter the network and test them in a safe environment.

Typically, these capabilities would be provided through additional customer premises equipment (CPE). However, in some cases, your firewalls may already include these functions. Simply turning on features of devices you're already running might enable you to achieve higher revenues per unit with no additional hardware investment.

A more forward-looking, and ultimately more profitable, approach would be to deploy web application security and sandboxing capabilities as centrally managed services in your NOC. This approach would allow you to deploy more streamlined devices on client premises (or none at all—see Model 3) while reducing your administrative burden.

More advanced MSSP services include:

- Web application security
- Sandboxing
- SIEM
- Centralized management with a customer portal option

If you also maintain a security operations center (SOC), you should consider adding more advanced management, analytics, and security incident and event management (SIEM) capabilities. These would provide both you and your clients greater visibility into the operation and effectiveness of the CPE or cloud-based firewalls.

Bear in mind that these security functions should not operate in isolation. Ideally, they will have built-in interfaces that will allow them to share information and be managed from a single pane of glass. This is especially important for the sandboxing and SIEM functions, which work to prevent attacks in one location from spreading through the client's enterprise.

This does not mean you need to procure all your security functions from one vendor; indeed, it would be difficult to find one vendor that offers every technology you need. If your managed security services architecture resembles a security fabric,[3] rather than a platform or a collection of point solutions, it will be easier to incorporate solutions from multiple vendors. In this manner, you can build a unified defense against a broad range of threats that may affect your clients' enterprises.

[3] "Why Fortinet for My MSSP? Real-world Reasons Fortinet Dominates the MSSP Market," Fortinet, December 2016.

MODEL 3: ON-DEMAND, INTEGRATED SERVICES

Once you are providing threat prevention, detection, and mitigation solutions through cloud-based services, the next step to greater competitive advantage lies in improving the agility of your cloud-based services through software-defined networking (SDN) and network functions virtualization (NFV). Instead of deploying physical CPE at client sites, you provision virtual CPE through the cloud.

By abstracting the administrative functions from the security functions, not only can you provision security services quickly from any location—which broadens your market reach and scale—but you can also enable clients to self-provision on demand. Taking this one step further, you can enable automatic provisioning of security services based on threat activity.

02 WHY A NETWORK SECURITY FABRIC IMPROVES MSSP

In describing Model 2 above, we mentioned the benefit of a security fabric architecture in incorporating products from multiple vendors. Eliminating vendor silos is important, but there's much more to the security fabric than that. Here, we will expand on the qualities of a fabric approach that can significantly improve your managed security services business.

IMPROVING EFFICIENCIES

As you evolve to meet escalating market demand, you will need to find ways to reduce your engineering hours. According to an informal study conducted by Fortinet's MSSP team, engineering costs account for 60% to 70% of a typical MSSP's cost of goods sold. A security fabric approach can help you improve staff efficiencies in several ways:

- **Centralized management and virtual CPE** reduce the number of physical devices at customer premises, significantly decreasing truck rolls for new client deployments, upgrades, or support. This structure also enables you to scale more cost-efficiently.
- **Integration between security functions** eliminates the need for engineers to transfer data from one device to another.
- **Customer self-service** management portals enable customers to generate reports (Model 2) and self-provision security functions (Model 3), which frees up your engineers for more value-added tasks.

MAINTAINING COMPETITIVE ADVANTAGE IN THREAT PROTECTION

As noted earlier, the general trend among MSSPs is to progress from threat prevention, using NGFWs, to advanced threat protection, which encompasses prevention, detection, and mitigation. To achieve and maintain competitive advantage in threat protection, you should keep an eye on the following three qualities of your security services architectures:

- **Breadth of protection.** How much visibility do security engineers have into threats and protection across the entire attack surface? Staying a step ahead of cyber criminals means employing multiple best-of-breed technologies and services, from email, web application, endpoint, and cloud security to sandboxing, SIEM, and analytics. Seek solutions that not only address the threats and attack vectors known today but also adapt to the changing threat landscape.
- **Integration** between security functions. You need to eliminate every silo to maximize your speed of threat response and mitigation and to reduce the risk of human error. Also, consider how threat intelligence services exchange information with your security fabric. It should appear as a seamless component of, not an adjunct to, your security technology.
- **Automation** of operation and analytics via a single pane of glass. Cyber criminals are leveraging artificial intelligence and automation to accelerate their discovery and exploitation of vulnerabilities. To protect your clients in today's threat landscape, you must augment your engineering expertise with automated threat response capabilities and advanced analytics to gain insights into evolving threats and attack vectors. Centralized, cloud-based control of threat detection and response makes it possible to scale your services without a correspondingly large investment in engineering staff.

FINDING NEW REVENUE OPPORTUNITIES

Whatever managed security services business model you currently employ, you have various opportunities to monetize the capabilities of your security technology assets.

Starting with your NGFWs, you can increase average revenue per unit by turning on functions that are already built into best-of-breed devices. For example, you can enable switch or access point security in the firewalls. Or you can enable clients to extend network security to the network edge with SD-WAN capabilities within the firewall. In this instance, you can generate additional revenue from a service that clients might have otherwise procured from their ISPs or non-security MSPs.

Customer self-service is another area that's ripe for monetization. For example, you may already offer some level of reporting. Using security analytics software that offers more in-depth or customizable reporting enables you to offer clients premium reports on the performance of their security solutions for an extra fee.

If you are aiming to increase revenues from your NOC or SOC services, you can show your growing clients how services such as advanced SIEM and analytics scale more cost-effectively when they are outsourced to a multi-tenant provider such as your company. You can also offer SIEM, sandboxing, and other functions as a service.[4] These services are more effective when used in conjunction with a compatible NGFW.

These are just a few of the opportunities for monetizing security technology. We encourage you to talk with your network security technology providers to expand this list.

[4] "Creating SIEM as a Service," Fortinet, 2017. "How to Create Sandbox-as-a-Service for MSSPs," Fortinet, 2015.

CONCLUSION

As your clients undertake digital transformation in an era of exploding cybersecurity threats, your opportunities as an MSSP will continue to grow. Staying competitive and profitable in this environment requires a technology and services roadmap based on integrated best-of-breed technologies that adapt to changing requirements. Hopefully, this eBook has provided a glimpse of this roadmap and how you can benefit from it. Check out the Fortinet MSSP content hub for more information about the security fabric approach and its applications for MSSPs.

www.fortinet.com

165050-0-A-EN