NGFW AS A SERVICE: PREPARING TO OFFER OPEX SERVICE

EXECUTIVE SUMMARY

Adding managed security service provider (MSSP) offerings to a reseller portfolio requires a great deal of analysis, strategizing, and due diligence. A successful transition requires well-researched, deliberative decisions about the business model and service offerings. The market is growing rapidly for service providers that offer a next-generation firewall (NGFW) as a service—firms that own and operate the customer's security hardware and software for a predetermined monthly fee over a contracted period of time. Many firms find that operating as a security provider increases customer value and retention, making revenue streams and margins more predictable, so the transition is well worth the effort.

WHITE PAPER

GROWING DEMAND FOR MANAGED SECURITY SERVICES

Managed security services are taking off. The sector is projected to experience a compound annual growth rate (CAGR) of 14.5% for the next four years, reaching more than $45 billion by 2022.[1] One reason is that every year, more companies shift toward the model of security as a utility, delivered like power or water by specialized organizations consumed as a monthly fee.

This trend is driven by the growing complexity of securing corporate networks. As networks evolve to include technologies such as Internet of Things (IoT) and wireless access for personal devices, the corporate attack surface expands, intensifying the burden on the IT security team. The resulting security infrastructure and processes must protect more devices and applications than ever before against advanced and rapidly evolving threats.

At the same time, many organizations struggle to maintain the expertise on staff to effectively secure their infrastructure. By outsourcing tasks to a security provider, a company will dramatically reduce the complexity of security responsibilities that fall on internal personnel, while saving the time and cost of recruiting security staff from a severely limited labor pool.

Migrating risk from the organization's IT department to firms that specialize in cybersecurity is seen as a way to improve the organization's security posture. Security provider staff have a depth and breadth of experience that enables them to make more informed technology selection and security policy decisions. Moreover, they have the skills to make better use of the technologies they select.

Customers of all sizes are looking to MSSPs to simplify the complexity of cybersecurity, mitigate their need to select and support multiple security vendors, remedy the cybersecurity skills shortage, and convert cybersecurity expenditures into a predictable and strategic endeavor.

One of the MSSP model's biggest benefits for customers is the smoothing out of corporate expenditures on cybersecurity. Relying on a security provider moves spending on security systems out of the traditional capital expenditures (CAPEX) bucket and into operational expenditures (OPEX). This makes costs predictable and eliminates spikes in spending anytime a firewall or other device needs to be upgraded or new attack methods arise requiring new security measures. In addition, spending on services receives favorable tax treatment, compared with hardware that involves depreciation and amortization over a period of years.

These are some of the key reasons for the trend toward OPEX-managed security services, in which security is consumed by the customer for a monthly fee that includes hardware, software, engineering, and ongoing management. Not only does this service model provide important deliverables to the customer, but it also offers the service provider a way to maintain high margins, improve customer stickiness, and add greater value than selling a firewall to the customer and managing it with a separate monthly fee.

CYBERSECURITY SKILLS SHORTAGE

14.5% CAGR, reaching **$45 billion** by 2022[2]

(Source: MSSP Alert)

Just as the MSSP model gives customers **predictability in their security spending**, it also **builds reliable revenue streams** for the service provider.

BENEFITS FOR SERVICE PROVIDERS

For the prospective service provider, operating as an MSSP requires a much different business model than selling security products does. The MSSP sector offers simplification of the complexity of cybersecurity, converting security acquisitions into a monthly fee. Competitive differentiation revolves around providing top-quality service over the life of the contract, which is usually three to five years in duration.

It's a different mindset, but those firms that take the plunge can reap significant rewards. Key among the benefits for resellers that add security services to their portfolio is the potential to achieve much higher margins. For example, based on internal Fortinet research, the average margin for reselling security hardware is 14%, whereas for managed security services it's typically between 50% and 60%.

Another important benefit of operating as a security provider is the stickiness of the customer base. Just as the MSSP model gives customers predictability in their security spending, it also builds reliable revenue streams for the service provider. Contracts guarantee customers' revenue stream for several years. Opportunities for profitable resale business have shrunk as margins have eroded and outright security acquisition has become commoditized with customers seeking higher value from their technology partners. This trend is driving up the MSSP model's appeal to resellers as they look to move with the market.

KEYS TO SUCCESS

There are five different actions security resellers can take to help ensure a successful migration to an MSSP model:

1. Define service offerings with the requirements of common or targeted customer profiles. New security providers must delineate a handful of discrete security service packages that customers can choose from that will reduce custom configuration requests, and they should simplify the bundling of security controls to reach desired customer outcomes (e.g., vertical compliance, IoT segmentation, etc.).

2. Keep the pricing model as simple as possible. Customers moving away from managing their own security are looking for simplicity in configuring the MSSP offering. An overly complicated list of available options will not be appealing. Having a complete and simplified set of packages has the added benefit of ensuring the sales force understands security opportunities before getting deep into technical details.

3. Build the business around a standardized technology stack. Managing disjointed security architectures and multiple vendors will require considerably more effort than managing a standardized technology stack. The more vendor-trained resources a security provider needs to manage customer solutions, the lower its margin and likelihood of customer satisfaction. Standardizing on a limited set of vendors improves customer satisfaction, sales uptake, and profit margins, whereas trying to be all things to all customers usually fails. The successful security provider should be selling its smart humans, process, and strategy—not security vendors.

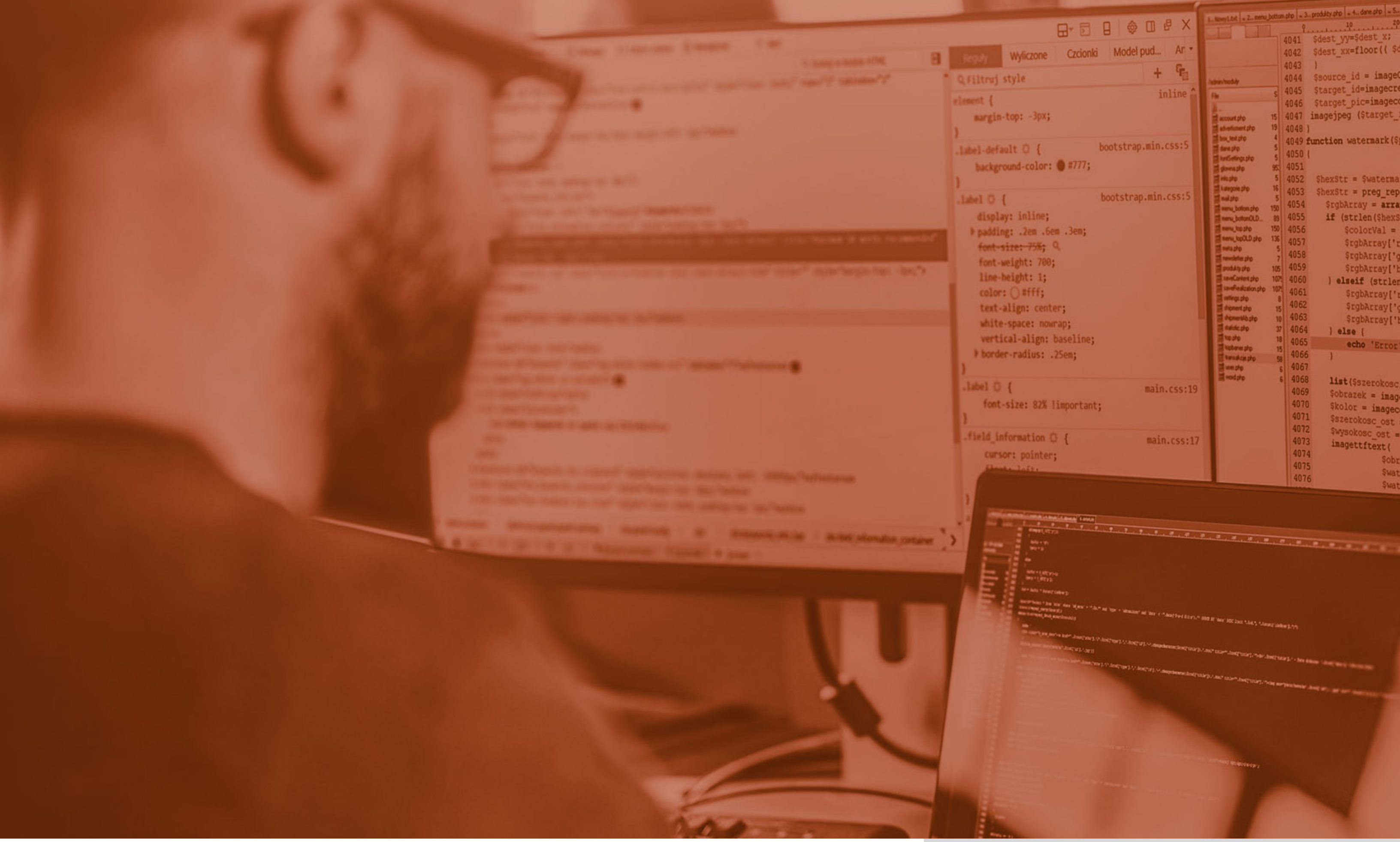
4. Carefully define the level of support included at each price point, down to the number of calls per month. The security provider must meet the typical customer's needs, but unlimited support calls for a fixed monthly rate will quickly drain margins.

5. Invest in good legal hygiene. Ensure liability is limited through a strong customer contract and a service level agreement (SLA) that can be referenced during operations and customer support. Liability for network interruptions should be limited to billing credit for downtime. Also, consider cyber insurance for protection in the event the service provider is actually breached.

CUSTOMER QUOTE

"We like to make the fees predictable and easy to calculate so a customer knows the exact cost of adding new resources and capabilities."

– Brian Thomas
CTO
Security7[3]



UNDERSTANDING CURRENT CUSTOMERS TO PREPARE FOR THE TRANSITION

The first place for a security hardware reseller to start in adding security services to its portfolio is to conduct a thorough analysis of its current customer base. A good idea is to dig into the current customer database to ensure assumptions about the size and security needs of the firm's clientele are accurate and consider what the ideal customer looks like. The business development team should evaluate the following questions:

- Customer size: How large is the typical customer office? How many people are using its network at each site? Will the service provider want to target the same sizes of businesses with its security services, or should it look at either larger or smaller prospects?
- Types of business: Do current customers commonly fall within a specific segment and vertical? Does it make sense to focus the security provider business on the same industries?
- Security needs: What security capabilities do most customers currently use? What controls or options do they want in their NGFW solution? What outcomes will the customer be looking for?
- Expected reports: What are their reporting needs? Are they usage- or compliance-oriented?
- Time to deploy: Realistically, how long will setup take per NGFW device? Is automation considered in this time estimate?
- Maintenance and support needs: How much time will staff need to spend with each customer every month over a three- to five-year period? Break this down into an hourly estimate of time per firewall.

The first place for a **security hardware reseller** to start in **adding security services** to its portfolio is to conduct a **thorough analysis of its** current or targeted **customer base.**

BUSINESS STRENGTHS AND DIFFERENTIATORS

Security resellers seeking to launch a new MSSP practice also need clear insight into their own operational maturity. They should take a hard look at the competencies of their organizations in key functional areas such as security operations, services and support handling, service strategy, and sales. Understanding strengths and weaknesses in each of these areas enables an organization to determine how long it will require to ramp up the MSSP business, where to focus its investment efforts, what can be done internally, and what to partner out.

The prospective security provider also needs a strong grasp on its own competencies, which will determine the level of sophistication it can offer in its new service model. What level of security depth does its security operations staff possess, and for what support time frames? Where is development needed? Likewise, decision-makers should consider what currently makes their organization special. They need to understand their firm's competitive differentiators and then play heavily to those characteristics as they build their MSSP business. Does it have a strong local presence? National reach? Compliance strength? Military-trained staff? Blue-chip leadership heritage?

Successful MSSPs do not sell security vendors; they sell their smart humans, security expertise, processes, and value-added services. Service providers that offer whatever security products the customer asks for will be challenged to attain profitability and maintain a high level of customer satisfaction. This is why standardizing on a technology stack is critical in developing a successful MSSP service model.

MAKING THE MOVE

Adding a managed security service to their portfolio is a major step for security resellers. However, this alternative approach to delivering security technology offers some attractive benefits compared with traditional reselling. It's important to carefully weigh the pros and cons. But for companies considering this move, now is a good time to take the leap, while the market is relatively nascent and growing fast.

Those that decide to take the leap will need to work out the details of their managed security service. They will need to:

- Define a small number of standard security bundles
- Determine which extra security services to make available at added cost
- Select a technology stack that enables efficient and effective security management

Where there is mystery, there is margin. With this in mind, a new MSSP will find its efforts to simplify security for customers will pay off in spades. Starting with an attractive NGFW-as-a-service beachhead, a firm then can expand its share of customer wallet with other value-added security services such as secure access infrastructure, SD-WAN, IoT/operational technology (OT) segmentation, and multi-cloud security.

Look for Fortinet's next white paper on this topic, which gets into details on the decisions successful MSSPs take in building out their service portfolio.

[1] Dan Kobialka, "Managed Security Services Market Forecast: $45B by 2022, Research Report Shows," MSSP Alert, June 9, 2017.

[2] Dan Kobialka, "Managed Security Services Market Forecast: $45B by 2022, Research Report Shows," MSSP Alert, June 9, 2017.

[3] John Maddison "Fireside Chat with Security7: How this MSSP is Enhancing Security through the Cloud while Reducing Customer Costs," CSO Online, December 19, 2017.

GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
06560 Valbonne
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA HEADQUARTERS
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1.954.368.9990