FORTINET

WHITE PAPER

Fortinet Cybersecurity Solutions for Managed Security Service Providers

Enabling Partners to Deliver Broad and Integrated Security and Networking Services

Executive Summary

As the threat landscape becomes more advanced and cybersecurity talent becomes more scarce, partnering with a managed security service provider (MSSP) is an increasingly attractive option for many organizations. In order to take advantage of this opportunity, MSSPs must be able to cost-effectively deliver a broad range of security services. Having a plethora of unconnected point products on the back end works against this goal. The Fortinet Security Fabric delivers a broad, integrated, and automated security architecture that enables delivery of effective, comprehensive security services with minimal cost and staff time. It even affords MSSPs an opportunity to expand into networking services, expanding their footprint at existing sites and growing a base of new clients.

"Clients are tired of 'buying' tools and are starting to focus on the success of integrating and successfully deploying their existing investments."[7]

The cybersecurity skills shortage,[1] coupled with the cost and hassle of maintaining 24×7 coverage of an increasingly complex infrastructure, have made MSSPs increasingly attractive to companies of all sizes. One recent analysis projects that companies will spend more than $58 billion on managed security services by 2024,[2] reflecting more than a 14% annual growth rate.

This trend represents an unprecedented opportunity for MSSPs. Providers with a broad set of offerings can increase their footprint at existing client sites, and recruit new clients with the promise of being able to meet their current and future needs.[3] But to take advantage of this growing market need, MSSPs must deliver the right mix of security services cost-effectively—and in ways that align with the business needs and priorities of their target customers.

Fortinet MSSP partners reduce risk and minimize the impact of cyberattacks by providing managed security and monitoring services to protect enterprise data, infrastructure, and users—regardless of who, where, when, and how IT assets are accessed. They extend the security operations of the enterprise by bridging people, skills, process, and technology.

Fortinet offers a broad portfolio of integrated and automated security tools that cover network security, cloud security,[4] application security,[5] access security, and network operations center (NOC) and security operations center (SOC) functions.[6] The ability to bridge security and networking on the same platform is a big advantage for MSSPs, enabling them to offer a broad, single-provider solution and increasing average revenue per user (ARPU).

Key MSSP Cybersecurity Challenges

Visibility

A lack of visibility is one reason that many businesses are turning to MSSPs for help in defending against attacks. They find themselves in this position because over time, they have responded to the growth of the attack surface by deploying unconnected point products, resulting in a disaggregated security architecture. This lack of visibility increases risk, as the organization often does not even know when it has been attacked.[8]

Providing end-to-end visibility is an essential capability for MSSPs seeking to meet the service expectations of their target customers. In the absence of visibility, fast-moving intrusions may cause harm before a response can occur, negating all efforts to maintain an effective security posture.[9] To deliver a value add to customers, MSSPs need to achieve end-to-end visibility across each customer's environment and provide that visibility to them via a customer portal.

Operational efficiency

The point of a managed service is to take advantage of economies of scale to deliver services more cost-effectively than a customer could. But if the MSSP's services are delivered inefficiently, they will not be profitable. Lack of integration across different security elements and architectural fragmentation increase operational inefficiencies. Without integration and automation, many security

workflows must be managed manually.[10] This certainly increases risk, but it can also slow DevOps cycles, degrade customer and employee experience, and increase administrative overhead and operational costs.

End-to-end integration, on the other hand, enables the MSSP to deliver broad services while optimizing staff time and budgetary resources, maximizing margins and potentially increasing ARPU. Silos are eliminated, and the MSSP's customers receive the most complete security protection possible.

"You should explain to them that your security services are about more than just outsourcing, stopgaps, and augmentation. Instead, you should show your customers that your security services give them access to the human talent they can't easily get on their own."[11]

Breadth of offerings

Offering a broad suite of security services to customers enables an MSSP to meet the needs of more current and potential customers. This potentially increases ARPU through the opportunity to upsell in specific accounts. It also enables the organization to compete for business from potential new customers that are looking for a comprehensive set of services under one umbrella.

Adding functionality via unintegrated point products results in technology sprawl with each product operating in its own silo, which necessitates manual correlation with existing services. Ironically, it could mean that customer accounts that leverage more services would be less profitable than those that use fewer services, inhibiting business growth. On the other hand, MSSPs whose offerings are powered by a broad, integrated, and automated security architecture can customize their offerings to each customer's needs. And every newly added service on an account increases both ARPU and profits.

Threat intelligence and analytics

In today's advanced threat landscape, customers need real-time access to robust threat intelligence to counter attacks that move at machine speed. In addition to a customer's own security logs, many subscribe to threat-intelligence feeds pulled from large networks of firewalls around the world, but it is a challenge to aggregate this data across a fragmented security architecture in time to deliver adequate speed of response.

Customers also expect data-driven advice from the professionals they are paying to manage their security infrastructure—a challenge for MSSPs operating in disaggregated environments. In such an environment, providing advice to customers is an expensive proposition, and the insights gained are less valuable due to inevitable human error in the analysis.

Use Cases

Managed Secure SD-WAN Service

The rapid growth of software-defined wide-area networking (SD-WAN) over the past few years[12] affords MSSPs an incredible opportunity. MSSPs now have easy access to tools that can increase their footprint at customer sites by expanding into networking services. The opportunity is equally attractive to customers, as it enables them to scale their network traffic using the public internet without paying for new multiprotocol label switching (MPLS) bandwidth. But security is a big challenge for companies considering SD-WAN, as network traffic moving on the public internet opens a big new element of the attack surface.

Other SD-WAN offerings are often based on point products that are purchased and administered separately from a security solution. This can increase operating costs, reduce margins, degrade security, and reduce the overall quality of the service. FortiGate Secure SD-WAN combines complete security and robust networking performance in a single platform, enabling MSSPs to broaden their reach profitably.

Such an offering also provides the potential for an MSSP to expand its services to secure networking at branch locations—again without adding additional point products. Fortinet SD-Branch includes FortiGate next-generation firewalls (NGFWs) combined with switching, wireless access, and network access control tools to provide complete connectivity and security protection at remote offices.

Offering managed secure SD-WAN services powered by Fortinet brings a number of advantages to MSSPs:

- **The opportunity to grow ARPU** at existing customer sites by expanding into networking services to, from, and within branch locations
- **The ability to grow this new business over time** with a lack of expensive additional contracts and deployments required
- **Operational efficiency and enhanced profitability** by delivering the service via a fully integrated, multi-tenant toolset

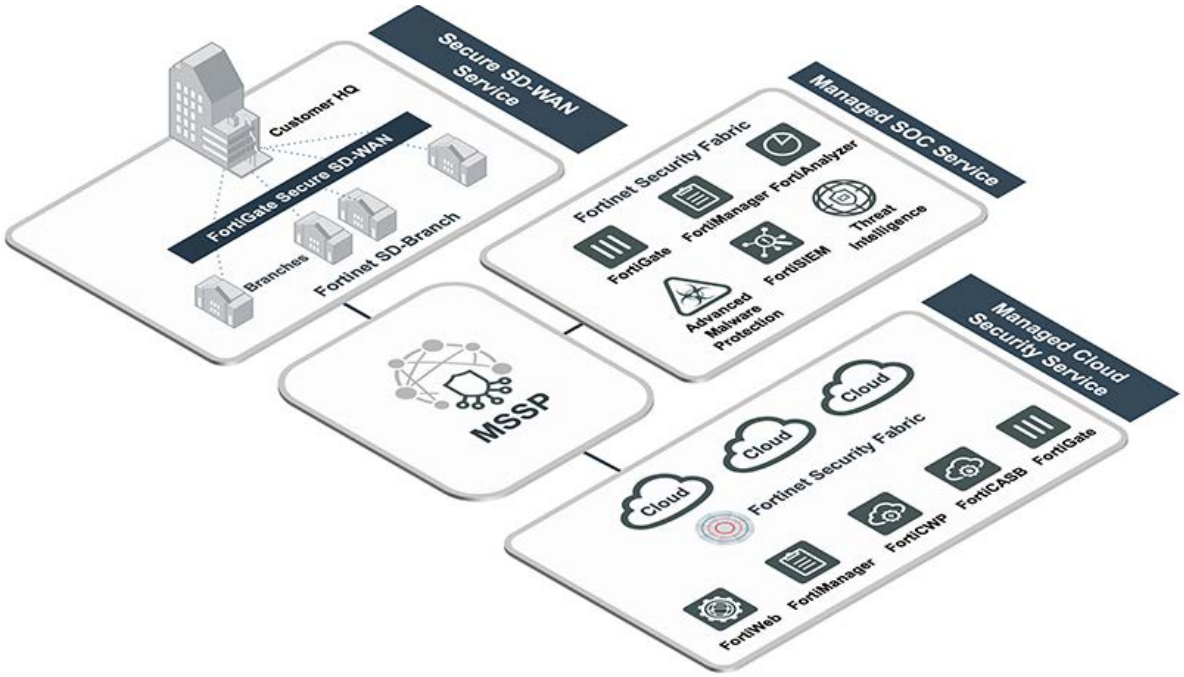

Figure 1: A broad, integrated, and automated security architecture from Fortinet helps MSSPs deliver a wide range of services, including managed SD-WAN services, managed SOC services, and managed cloud security services.

Managed SOC Service

Not every company can afford to have a full-fledged SOC. Designing and building out the space, hiring a team, and providing 24×7 staffing and hardware and software maintenance on an ongoing basis is an expensive proposition. Unfortunately, the cybersecurity skills shortage means that the problem is only getting worse.[13]

That said, the enhanced security, visibility, and actionable insights that can be derived from a SOC are important for the business. MSSPs can fill this gap by delivering a range of services from their own SOC. These services can be offered at specific levels or as tailored services for individual customers' needs.

For example, many customers benefit from managed security information and event management (SIEM) services because of the deep visibility and analytics they provide. And managed detection and response services can leverage artificial intelligence (AI)-driven threat intelligence and indicators of compromise (IOC) feeds to add layers of protection to customer environments. Customers can even have their own log-in credential to view the analytics for themselves.

"In the modern times we live in, formulating new strategies, and remedying existing security measures to combat the changing threat landscape, is of the utmost importance. Keeping this in mind, MSSPs serve as the Holy Grail solution that the cybersecurity realm needs today!"[14]

The Fortinet Security Fabric, powered by FortiGate NGFWs, enables MSSPs to build a full-spectrum SOC with end-to-end integration across the entire architecture. Numerous security tools from Fortinet and third-party Fabric Partners integrate seamlessly into the Fabric. Additionally, the open architecture and robust representational state transfer application programming interface (REST API) enable MSSPs to integrate other solutions to fill niche needs or maximize investment in legacy tools.

Delivering managed SOC services using the Fortinet Security Fabric brings these benefits to MSSPs:

- **The ability to offer comprehensive services** without managing a plethora of point products
- **The benefit of real-time, AI-powered threat intelligence** along with other layers of protection against unknown threats
- **Operational efficiency and enhanced profitability** by delivering the service via a fully integrated, multi-tenant toolset

Managed Cloud Security Service

The explosion in the use of the public cloud by businesses of all sizes does not seem to be slowing. In fact, Software-as-a-Service (SaaS) spending alone is expected to exceed $80 billion this year[15]—an annual growth rate of more than 17%. Unfortunately, the rapid adoption of sprawling cloud infrastructures increases security operations complexity for organizations, and the result is often that cloud-based applications are vulnerable. One key driver of risk is the misconfiguration of cloud-based systems.[16]

With the right infrastructure, MSSPs can offer comprehensive cybersecurity protection for all services running on multiple clouds. Alternatively, they can offer protection on an application-by-application basis using a Web Application Firewall (WAF)-as-a-Service model. Both approaches can increase an MSSP's footprint at customer sites. As they offer more cloud security services within an account, operational efficiencies derived from end-to-end integration can increase their margins.

"Customers are more comfortable sharing data with companies they actually trust; when firms fail to deliver on security, their brand reputation, customer trust, and even revenue are negatively impacted."[17]

Fortinet offers robust, cloud-native tools to bring MSSP customers' entire distributed cloud infrastructure together under a single umbrella, with consistent security protection, policy management, and configuration management. FortiGate VM brings the NGFW to a virtual machine form factor that works well for cloud environments, and the FortiWeb web application firewall (WAF) is available in several form factors as well, including SaaS. The FortiCASB cloud access security broker (CASB) service and the FortiCWP cloud workload protection (CWP) tool deliver visibility, compliance, threat protection, and configuration management across the cloud infrastructure.

A managed cloud security service powered by Fortinet brings these advantages to MSSPs:

- **Security tools native to each cloud** bring a consistent set of security policies and practices to all customer cloud deployments
- **In-line, real-time threat intelligence** in FortiWeb enables instant, automated response to security events
- **Operational efficiency and enhanced profitability** by delivering the service via a fully integrated, multi-tenant toolset

Fortinet Differentiators for MSSPs

Robust, broad-based security products and services to enable a comprehensive menu of services for MSSP customers from a single platform. This can result in higher ARPU and broader revenue opportunities. At the same time, Fortinet Network Security Expert (NSE) training gives MSSPs a consolidated training model for a broad set of security and networking products under management—and a way to differentiate their services.

Multiple product consumption models offer MSSPs and their customers the flexibility they need to secure their data, infrastructure, and applications in the most optimal way. Different Fortinet solutions are available in appliance, virtual machine, cloud, and SaaS form factors. MSSPs can also leverage special pricing programs such as pay-as-you-go and subscriptions, providing the flexibility to address different business models supporting their service offerings.

Recognized leadership in network security, named a Leader in the Gartner Magic Quadrant for Network Firewalls,[18] and scoring best among nine vendors in the NSS Labs Next-generation Firewall Security Value Map.[19] This unparalleled performance enables MSSPs to reduce their capital expenses (CapEx) spend, and a smaller security and network footprint to deploy and manage lowers operational expenses (OpEx) costs.

The ability to leverage **investments in third-party products** via integration through the Fabric Alliance, open APIs, and a robust REST API. This enables MSSPs with rapid scale to remove friction and increase the speed of service rollouts.

Security solutions **designed as multi-tenant from the ground up**, enabling MSSPs to isolate but still manage multiple customer networks from a single console. This increases ARPU while improving operational efficiencies.

Conclusion

As customers look to MSSPs to help them with seemingly intractable cybersecurity challenges, offering limited, cookie-cutter, or disconnected services is not a good way to build business. But MSSPs that base a broad set of services on the Fortinet Security Fabric have the opportunity to become a one-stop shop for security services—and a trusted advisor to a growing client base.

[1] Mekhala Roy, "Effects of cybersecurity skills shortage worsening, new study says," TechTarget, May 10, 2019.

[2] "Managed Security Services Market is Expected to Exceed US$ 58 billion by 2024," MarketWatch, February 27, 2019.

[3] Christophe Voilque, "MSSP 2.0: How to Launch or Expand Managed Security Services with the Fortinet Security Fabric," Fortinet, March 27, 2019.

[4] "Key Principles and Strategies for Securing the Enterprise Cloud: A Cloud Security Blueprint," Fortinet, December 3, 2018.

[5] "Fortinet Web Application Security for the Cloud," Fortinet, March 19, 2019.

[6] "Bridging the NOC-SOC Divide: Understanding the Key Architectural Requirements for Integration," Fortinet, August 23, 2018.

[7] Scott Matteson, "To stay competitive, MSSPs need to grow and evolve," TechRepublic, January 16, 2019.

[8] John Maddison, "The Problem with Too Many Security Options," Fortinet, May 9, 2019.

[9] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018.

[10] "Network Complexity Creates Inefficiencies While Ratcheting Up Risks: Understanding the Causes and Implications," Fortinet, June 1, 2019.

[11] "Managed Security Services' Value Is Scale," Channel Futures, May 14, 2019.

[12] Andy Patrizio, "Enterprises are moving to SD-WAN beyond pilot stages to development," Network World, May 7, 2018.

[13] Jon Oltsik, "Is the cybersecurity skills shortage getting worse?" CSO, May 10, 2019.

[14] Rebecca James, "How Can MSSPs Thrive in the Growing Time of Complex Cyber Threats?" Infosecurity, October 29, 2019.

[15] Louis Columbus, "Roundup Of Cloud Computing Forecasts And Market Estimates, 2018," Forbes, September 23, 2018.

[16] Asher Benbenisty, "Don't Go Once More Unto the Breach: Fix Those Policy Configuration Mistakes," Infosecurity, October 30, 2018.

[17] "Industry leaders struggle to balance digital innovation and security," Help Net Security, April 4, 2018.

[18] "FortiGate Network Firewalls Give MSSPs Another Reason to Select Fortinet," Fortinet, September 24, 2019.

[19] "Independent Validation of Fortinet Solutions: NSS Labs Real-world Group Tests," Fortinet, January 2019.

November 18, 2019 9:37 PM

D:\Fortinet\White Paper\Vertical Marketing Service Provider\wp-fortinet-cybersecurity-solutions-for-managed-security-services-providers-v2

519049-0-0-EN