FORTINET

SECURITY SOLUTIONS FOR MANAGED SERVICE PROVIDERS AND CLOUD PROVIDERS

SOLUTION GUIDE

INTRODUCTION

Businesses worldwide are experiencing a boom in employee productivity, which is driven in part by the latest innovation in cloud services and pervasiveness of mobile services. Coupled with the relentless goal to drive down operational costs and increase efficiency, businesses of all sizes have embraced these technology advancements in massive numbers, from the largest multinational corporations to the smallest business franchises. All analysts agree that the demand for outsourced IT and cloud services will continue to grow at a rapid pace.

On the flip side, businesses are also facing increasing challenges in the form of complex government compliance regulations and threat of security attacks. It is a proven fact that the increasing complexity and frequency of security attacks against businesses cannot be ignored. Media headlines on the latest security attacks are common, with several of them evolving into stories of stolen information that unveiled shocking security lapses or internal operational blunders that had damaging ripple effects on the businesses' bottom line and brand value.

Verizon 2016 Breach Report summarized it well, as shown in figure 1, that "No locale, industry or organization is bulletproof when it comes to the compromise of data."

The tsunami of volume, as shown in Figure 2, which is multiplied by the diversity of threat vectors, as shown in Figure 3, makes it literally impossible for any business to keep up. A breach and an operational failure are a matter of when, not if.

FIGURE 1: COUNTRIES REPRESENTED IN COMBINED CASELOAD

Per Minute		Per Week		Total Database	
35,000	Threat events	46M	New & updated spam rules	190	Terabytes of threat samples
21,000	Spam emails intercepted	1,000	Intrusion prevention rules generated	18,000	Intrusion prevention rules
470,000	Network intrusions resisted	1.8M	New & updated AV definitions	5,800	Application control rules
95,000	Malware programs neutralized	1.4M	New URL ratings	250M	Rated websites in 78 categories
160,000	Malicious websites blocked	8,000	Hours of threat research globally	312	Zero-day threats discovered
32,000	Botnet C&C attempts thwarted				
43M	Website categorization requests				

FIGURE 2. VOLUME OF SECURITY ATTACKS (FORTINET DATA)

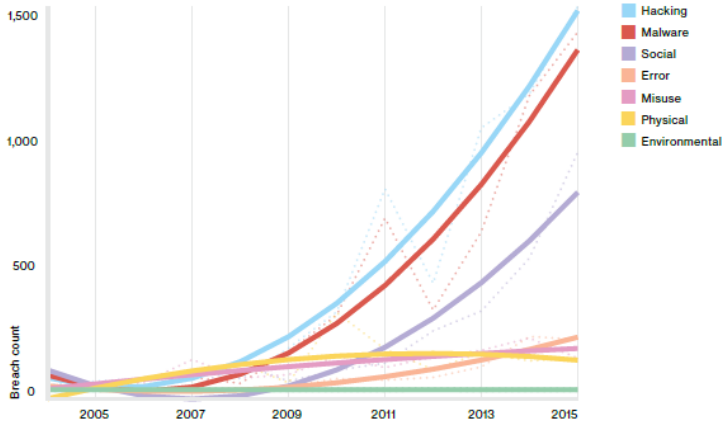

FIGURE 2. NUMBER OF BREACHES PER THREAT ACTION CATEGORY OVERTIME, (N=9,009)

MANAGED SECURITY SERVICE PROVIDERS—THE TRUSTED PARTNERS

Capitalizing on a solid reputation earned by providing support for various IT needs, managed security service providers (MSSPs) have grown into trusted partners with the deep domain expertise to help businesses navigate through complex rules of government compliance mandates and protect their customer's operations security breaches.

The impact of security attacks cannot be underestimated, as businesses are inundated every day by new attacks. Often solutions architected internally end up overwhelming the in-house IT security teams and exposing their limitations.

The growth prospect of managed security services is very bright. In a CRN article published on January 6, 2017, MarketsandMarkets analyst Sarah Kuranda predicted that the market for managed security services will grow to $35.5 billion by 2020, up from around $17.8 billion in 2015. For scale, MarketsandMarkets also predicts that the overall security industry will be $202.4 billion by 2021, up from $112.5 billion in 2016.

Many MSSPs are expanding their offerings to include a complete set of security services. There are two main categories of service deliveries and consumptions, as shown in Figure 4 below.

The first category is the basic on-premise managed security service, which consists of physical CPEs and a cloud-based customer self-service portal to provide device management and threat analytics.

The second category expands on the capabilities of the first one and has proven to be the most profitable outsourced model. Typically, MSSPs like to add virtual CPEs that offer advanced security service to accommodate the customer's varying workload which depends on the nature of the applications that support business operations. This may include advanced sandboxing to detect new threats, secure mail scanning to protect the heavy use of Outlook email systems, secure mission critical SaaS applications with Web Application Firewall (WAF), and protect customer devices with end-point security with integrated antivirus, IT compliance tools, and VPN capabilities.

However, to offer security solutions of this complexity requires significant capital investment and may be inherently difficult to manage. To alleviate that burden, Fortinet offers automation tools and products that can simplify the service delivery model. This discussion will take us to the topic of MSSPs as cloud providers.

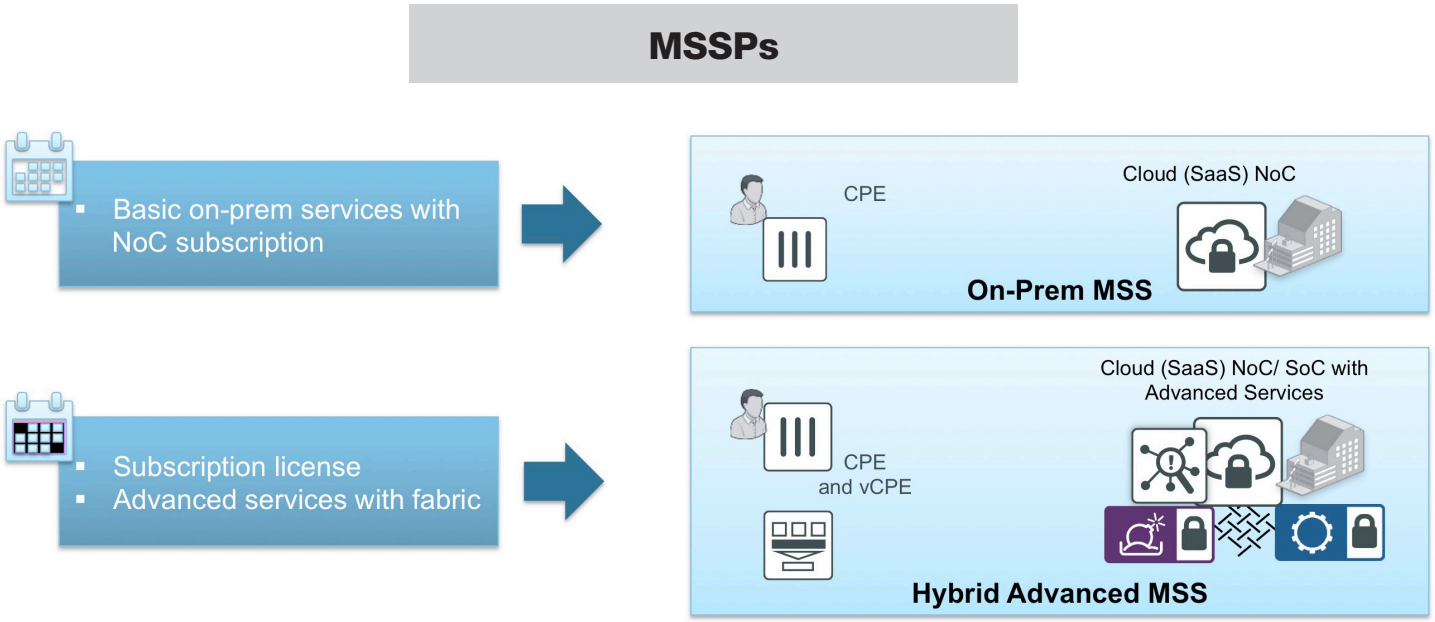

FIGURE 4. MSSP SERVICE DELIVERY AND CONSUMPTION MODELS

MSSPS AS CLOUD PROVIDERS – AUTOMATION WITH ON-DEMAND SERVICES

One way to enable more automation and more efficient operation is to utilize an emerging cloud service delivery model that can provide a highly integrated security services and be remotely deployed over virtual or cloud-based customer premise equipments (CPEs).

FIGURE 5. CLOUD PROVIDER SERVICE DELIVERY AND CONSUMPTION

Such virtual CPEs enable the services to be activated on-demand and billed based on the actual usage rather than pre-paid subscription.

There is a recent game-changing cloud technology designed for the data centers that can enable cloud providers to do just that. This technique is called software-defined data center (SDDC). In addition to delivering the right amount of services based on the actual demand, SDDC also minimizes the risk of overbuilding capacity in the data center through optimized asset utilization and significantly reducing power consumption.

FORTINET ADVANTAGES

COMPREHENSIVE SECURITY COVERAGE FROM THE ENDPOINT TO EDGE AND CORE AND FROM DATA CENTER TO CLOUD

As a pure-play security vendor, Fortinet has the broadest portfolio. As figure 6 shows, Fortinet offers a complete end-to-end security solution that includes advanced management and threat analytics for IoT, PoS, branch offices, business campus to data centers and from the end-points to the cloud.

Fortinet's comprehensive portfolio enables a provider to meet unique customer requirements—regardless of performance, scale, or price points.

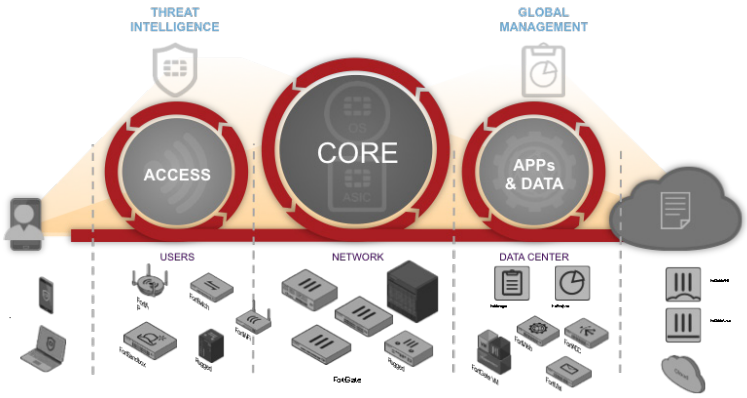

FIGURE 6 - FORTINET PORTFOLIO

SECURITY CPE MARKET SHARE LEADER

The Fortinet FortiGate has been a successful product line since its first launch in 2009. In the branch office market, Fortinet has shipped more FortiGates as security CPEs than any of its competitors (see Figure 7).

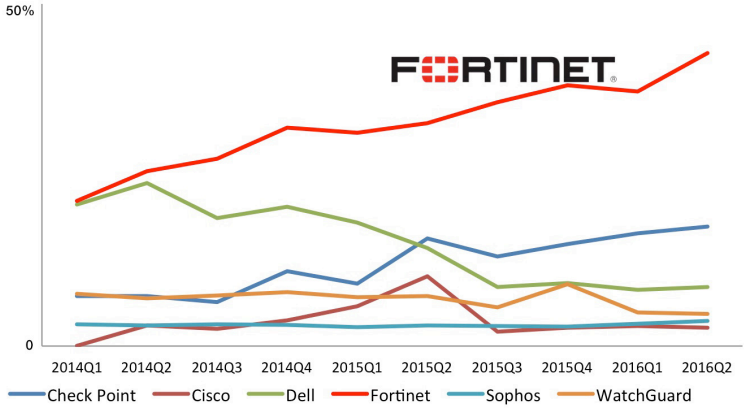

FIGURE 7. IDC WORLDWIDE SECURITY APPLIANCE TRACKER

Fortinet offers the most innovative and broadest form factor of CPEs, which includes:

1. purpose-built physical CPEs that scale up to multigigabit in performance
2. virtual CPE that runs on entry-level to high-end white boxes
3. the highly innovative FortiHypervisor for a provider who wants to build and differentiate its service on the best-of-breed solution platform

As shown in Figure 8, FortiHypervisor is a KVM hypervisor-based gray box with Fortinet's high-performance embedded security processor to accelerate security functions while capable of hosting third-party virtualized network function (VNF).

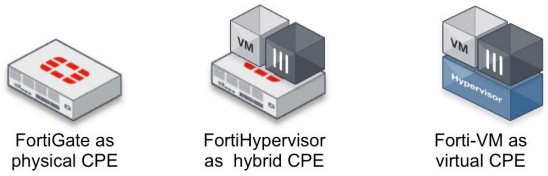

FIGURE 8. FLEXIBLE FORTINET CPE FORM FACTORS

In the aggregate, Fortinet has shipped over 2.8 million devices. This is not only a win for Fortinet but also should build confidence in our platform's ability to meet the expanding security needs of its current and future customers. Each one of these devices acts as a threat intelligence probe and is integrated into a global security fabric responsible for collecting and providing systematic initial identification of critical threat information.

The collected information will then be transmitted to FortiGuard Labs for in-depth analysis and verification.

HIGH-EFFICACY SECURITY OPERATING SYSTEMS AND FORTIGUARD SERVICE

As a pure-play security leader, Fortinet has invested heavily in its operating system, called FortiOS. FortiOS has won numerous awards for its effectiveness in detecting threats. This is the foundation of a strong security protection strategy.

In addition, Fortinet recommends the FortiGuard service for its up-to-date threat intelligence knowledge, collected from the most advanced security fabric available with a global footprint.

FIGURE 9. FORTINET SECURITY OS PLATFORMS

As shown in Figure 3, the security fabric receives a massive influx of information about security attacks on a minute-by-minute basis. FortiGuard Labs can parse the big data streams into insights about any local impending attacks.

The flow of data collection, analysis, and the dissemination of protection knowledge to every subscribed endpoint makes the FortiGuard security platform a powerful, fully automated service.

INCREASE OPERATIONAL EFFICIENCY AND AUTOMATION

In light of the massive scale and complexity presented by the rising threat vectors, automation remains the most effective approach to improve operational efficiency.

For providers with modernization projects that include virtualization, Fortinet offers an extensive high-performance virtualized and cloud-enabled portfolio.

Fortinet provides value-added API connectors to support multivendor environments and open architectures, such as OpenStack and Cisco ACI.

The addition of Fortinet security fabric allows a seamless integration with the existing network infrastructure and delivers a combination that enhances overall operational efficiency through automated service delivery and unmatched granular security control.

BROAD VIRTUALIZED AND CLOUD PORTFOLIO

To complement the north-south firewall functionality served by the purpose-built, high-performance security appliances and carrier-grade chassis, Fortinet also offers a broad set of virtualized security solutions.

The most popular virtual products are the FortiGate-VM and FortiWeb-VM, which enable next-generation firewall and web application firewall functionalities respectively.

For the applications with varying workloads, Fortinet offers three different consumption models to suit both the capex and opex requirements of any businesses, as shown in Figure 11.

1. VM Perpetual is a set of eighteen different functionalities to choose from that follows the traditional licensing model where the license is owned by the purchaser.

   It is suitable to protect heavy workloads because it is a one-time purchase with no recurring cost or expiration.

2. VM Subscription is a program offering FortiGate and FortiWeb functionalities, where the license is owned by the provider and leased to the subscribers.

   It is a program suitable for a sustained workload with lower upfront cost and a recurring billing model based on the reported monthly usage.

3. VM On-Demand is also a program offering similar FortiGate and FortiWeb functionalities with additional metering capability, where the license is owned by the provider and the usage is metered to the customer.

   There are two metering consumption options, by volume or by system resources: vCPU and RAM.

   VM On-Demand is the ultimate choice for any business with variable or bursty workload. The billing is automatically based on the actual usage, which can be as granular on an hourly basis.

Products and Program Type	VM Perpetual Products	VM Subscription Programs	VM On-Demand Program
License Ownership	Traditional license owned by service prov. or subscribers	Subscription license owned by service prov. and leased to subscribers	On-Demand license owned by service prov. and metered to subscribers
Length of Use	Perpetual	Monthly	Hourly to Monthly

FIGURE 11. FORTINET VM CONSUMPTION MODELS

HIGH-PERFORMANCE SECURITY PROCESSOR ENGINES

Building high-performance security platforms is Fortinet's specialty. By investing heavily in the development of security processor units (SPUs) to accelerate the user plane, control plane, and more importantly, deep content processing, high performance is a recognized standard in all of Fortinet's architectures, from the UTM to the high-end, carrier-grade firewall that scales up to 1 Tbps.

Combined with a high throughput and scalable security OS, Fortinet's security platforms offer unmatched industry performance and are well-suited for high-demand networks.

KEY COMPONENTS AND USE CASE FOR MSSP SOLUTION

HYBRID ADVANCED MSS DEPLOYMENT SCENARIO

The deployment scenario shown below is the simplified end-to-end network diagram that shows the key components of Fortinet's MSSP solution.

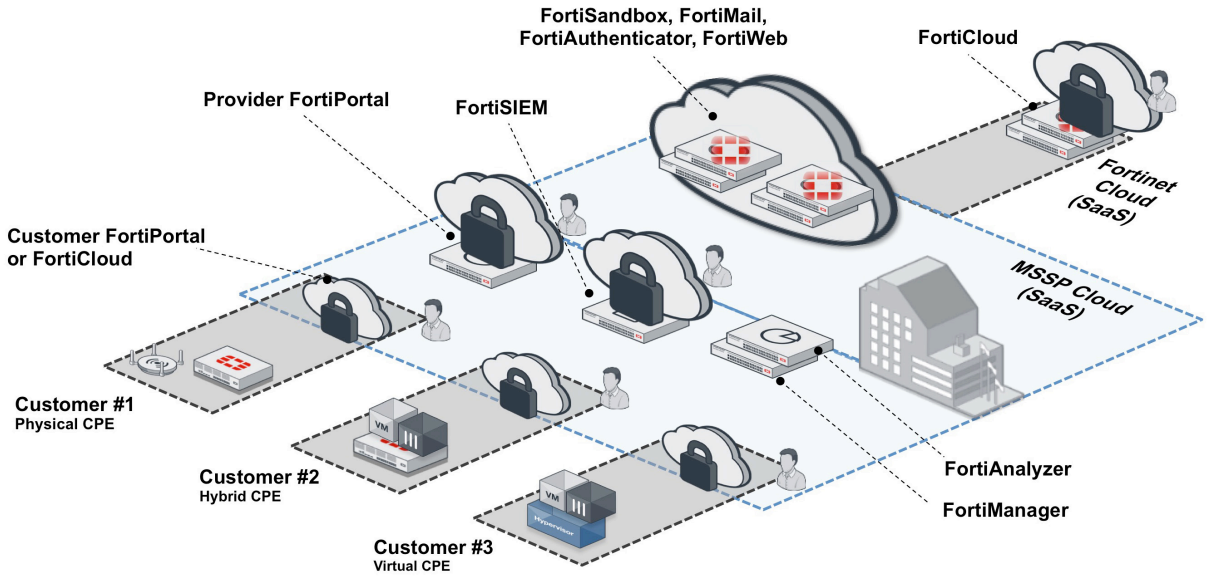

FIGURE 13. HYBRID ADVANCED MSS DEPLOYMENT

A new entrant to the managed security business and a system integrator may choose to start with a basic service consisting of some physical FortiGates with or without FortiAPs and FortiWiFis as managed security CPEs. In the case of a smaller network, the FortiCloud would be the most cost-effective network operations center solution to provide each customer with a self-service portal.

Established MSSPs and incumbent service providers with large networks and more varied customer needs should consider the versatility virtual CPE. For the customer self-service portal, Fortinet recommends a combination of FortiPortal, FortiManager and FortiAnalyzer to provide a carrier-grade, multitenant service foundation that is capable of supporting thousands of customer sites and tens of thousands of devices.

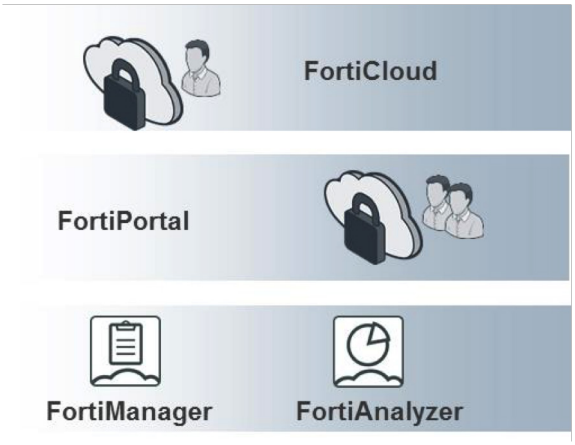

FIGURE 14. PRODUCTS FOR CUSTOMER SELF-SERVICE PORTAL

FortiPortal is a presentation layer that relies on the FortiManager for the device management support and FortiAnalyzer for the threat analytics.

It is purpose-built from the ground up for large-scale deployment, maximum extensibility and a high-degree of customized service level for each customer. It can also be custom labeled to enhance the provider's brand image. With the support of RESTful APIs, FortiPortal can be integrated with the existing multivendor network or OSS/ BSS system.

For an established MSSP looking to grow their business by offering additional security services, Fortinet offers several complementary solutions. A popular solution for businesses is the Advanced Threat Protection solution, which includes FortiMail, FortiSandbox, and FortiClient. FortiClient provides VPN, secure token, antivirus, and corporate compliance enforcement capabilities.

FIGURE 15. FORTIPORTAL THREAT LANDSCAPE ANALYTICS

KEY COMPONENTS AND USE CASE FOR CLOUD PROVIDER SOLUTION

VIRTUAL ON-DEMAND MSS IN AN OPEN MULTIVENDOR SDN/NFV ENVIRONMENT

Several MSSPs have capitalized on their existing data center infrastructures to deliver the flexible on-demand security services. Many businesses find such offerings perfectly suited to protect their variable application workloads, such as financial applications that are run at the end of a quarter.

On-demand security services are built on the new and advanced software-defined data center (SDDC) architectural framework that relies on cost-effective, commodity-based servers (also known as white boxes) and new open standards, such as software-defined networks (SDNs) and network function virtualization (NFV) to ensure multivendor interoperability.

This new approach is a big shift from the commonly deployed architecture that relies on dedicated and high-performance hardware. Fortinet provides security portfolios for both architectures. All cloud providers deploy a combination of both, with the dedicated hardware for north-south, high-performance security protection and virtual security function that runs on commodity servers for flexible on-demand service deliveries.

Fortinet's on-demand security solution consists of three main components:

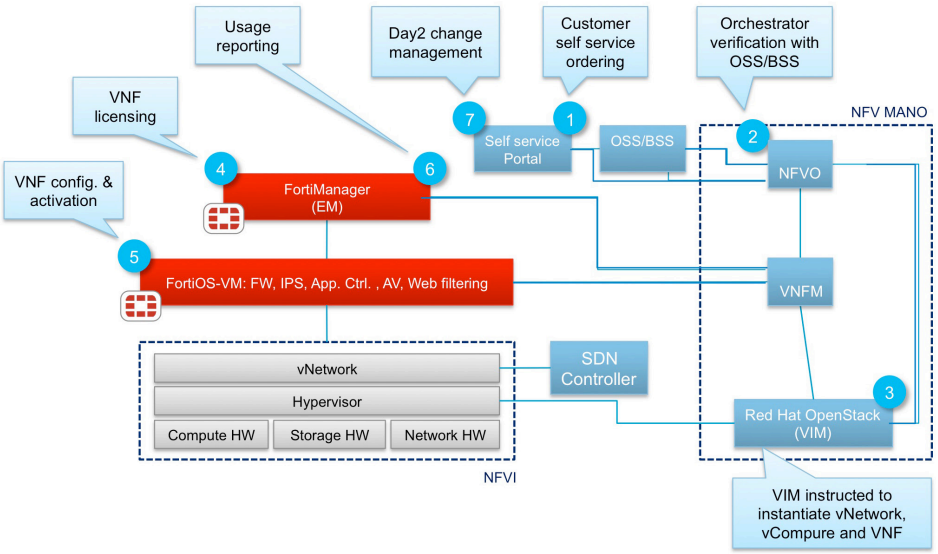

FIGURE 16. VIRTUAL ON-DEMAND MSS ARCHITECTURE

1. VM On-Demand (also known as FortiMeter). It is a program that comes standard with FortiOS-VM for next-generation firewall and FortiWebOS-VM for web application firewall capabilities.
2. For SDN-centric environments, Fortinet offers connectors for OpenStack and Cisco ACI.
3. FortiManager is a necessary component that validates the end-customer credential, instructs the OS to activate corresponding firewall, IPS, application control, antivirus, or URL web filtering. Additionally, FortiManager also meters the on-demand usage and feeds the reports to the OSS/ BSS system.

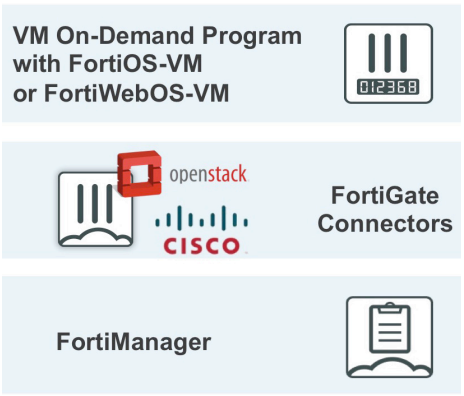

FIGURE 17. PRODUCTS FOR VIRTUAL ON-DEMAND MSS

As with any multivendor and open ecosystem that includes open-source software and vendor-specific components, interoperability is a must.

The figure 16 that shows ETSI-based SDN/NFV environment is no exception and Fortinet understand this importance. Fortinet is committed to complying with the new ETSI-based SDN/NFV standard and has successfully participated in a major vCPE test event conducted by EANTC in May of 2016. The detailed test report can be downloaded directly from http://www.eantc.de/fileadmin/eantc/downloads/News/2016/EANTC-NIA_BCE2016-WhitePaper-Online.pdf.

SUMMARY

The digital transformation to cloud technology and mobile services has enabled businesses around the world to operate in a more productive and cost-effective manner. While exciting times are still ahead, organizations have to think about securing their networks from the ever-increasing frequency of attacks that may impinge on their brand images.

MSSPs are uniquely positioned to alleviate their businesses' customers from this burden. With the deep knowledge in IT and security, MSSPs can offer a rich set of security offerings that effectively meet different levels of market demands.

Fortinet has been the leading provider in the managed security market since its inception in 2009. Currently, the comprehensive portfolio includes advanced solutions that span from the customers' endpoints to the edge and core of the providers. All of these products enable MSSPs to differentiate their service capability and offer programs to allow the customer base to expand seamlessly while increasing the MSSPs' revenue.

For MSSPs with data centers, Fortinet has a broad set of virtualized security products and programs to support the increasingly popular opex business model driven by IaaS/SaaS usage trends.

This is a high-growth area because it delivers higher operational efficiency, helps reduce capital risks and better aligns IT cost with recurring and on-demand services.

Fortinet has been a leader in this area with a portfolio that has received performance recognition and certificates of compliance from various leading organizations, including NIA, VMware, ETSI, and EANTC Labs.

In summary, as the leading vendor for the MSSP and cloud provider security solutions, Fortinet continues to build strong momentum and loyal customers worldwide, as shown by the following facts:

1. Fortinet leads in enterprise security CPE market share for the last few years running.
2. From the customer endpoints to the provider edge and cloud, Fortinet products are architected for high performance and effectiveness in detecting security attacks.
3. The solution portfolio has many successful deployments and is the platform of choice for many telcos and the largest cloud providers.

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

64953-A-0-EN **March 21, 2017**