INTRODUCTION

The managed service provider (MSP) market, including managed security service providers (MSSP), is projected to continue growing at a healthy pace of 10-12% annually for the next several years, reaching upwards of $200 billion globally by the end of the decade. Yet even with this rapid pace, enterprise IT expectations are changing and will have a significant impact on the evolution of MSP/MSSP services. Key technology innovations promise to greatly transform the next generation of managed services at the customer network, particularly when it comes to customer premises equipment (CPE) at the network edge.

MSP/MSSP INDUSTRY TRENDS

Three of the key IT trends impacting managed service providers are:

Enterprise IT Shift from Capex to Opex—The rapid growth of MSP and MSSP services in recent years has directly reflected the shifting preference of enterprise IT organizations from capex- to opex-based IT spending. But accelerating this trend are technologies such as cloud computing, which have further enabled even what was once capex hardware (e.g., servers, storage, and switching), or application software that can be easily delivered in opex-based IaaS or SaaS clouds.

Cloud Elasticity—Public clouds such as AWS and Azure have been enabling enterprises to rapidly deliver and deploy applications that can scale elastically, and in turn be allocated just the right amount of infrastructure capacity as needed to meet user demand at a given time.

Network Function Virtualization (NFV)—Service providers have jumped enthusiastically beyond virtualization and SDN to further defining standards and architectures for NFV, where proprietary hardware is replaced with virtual network functions (VNFs) encapsulated as virtual machines. More than merely the notion of reducing capex by using more commoditized x86 servers, NFV orchestration has the promise of automating and improving service delivery, including facilitating rapid provisioning and upsell of additional managed services to existing customers.

VIRTUAL CPE: THE FIRST NFV USE CASE?

All of these trends are converging at the edge of the customer network, as analyst firms such as Gartner Research have identified virtual CPE (vCPE) as perhaps the first widespread provider NFV use case. Where MSP/MSSPs may have traditionally deployed edge and gateway services such as routers, load balancers, and firewalls as physical customer premises equipment (CPE), they may now replace those with VNFs consolidated on a single x86 white box or grey box.

Virtual CPE can be deployed in a few different models:

- **Cloud CPE**—One notion of virtualizing CPE involves pulling the VNF functions back from the actual customer premise into the provider data center. In this vCPE approach called cloud CPE, multiple tenant service chains and VNFs may be consolidated on shared NFV infrastructure, such as in a multi-tenant IaaS cloud, to increase utilization and efficiency.

- **Universal CPE**—Where the VNFs continue to reside at the customer edge, as with physical equipment, this may be more specifically referred to as universal CPE (uCPE). In this approach, a dedicated network function virtualization infrastructure (NFVI) white box or grey box is deployed at each customer site.

- **Provider POP**—Another vCPE variant is to pull back the VNFs from the customer site just to the provider edge or point of presence of an MPLS, broadband, or other WAN connection, but still deploy more dedicated NFVI hardware to each customer site as opposed to a consolidated cloud approach.

Regardless of deployment model, SDN and NFV orchestration would generally be controlled from a centralized provider data center or cloud, enabling the MSP/MSSP to roll out additional VNF services to a customer site without needing a physical truck roll or deploying additional hardware.
FORTINET SOLUTIONS FOR NEXT-GENERATION CPE

Fortinet has long invested in technologies such as virtualization and automation that have been enabling transformation of infrastructure, data centers and networks. Starting nearly a decade ago, key network security functions such as next-generation firewalls, intrusion prevention, web applications security, and e-mail security found in Fortinet’s leading hardware solutions also started to be shipped as virtual Fortinet appliances for consolidated data centers and cloud-based services. These technologies are further evolving and expanding to support the next generation of managed services.

FORTIGATE AS VNF: CONSOLIDATED SECURITY, ROUTING, AND SD-WAN SERVICES

The heart of Fortinet’s offerings for MSP/MSSPs is the award-winning FortiGate family, which includes FortiGate VM virtual appliances that can be deployed as VNFs. The FortiGate platform has always innovated on the premise of consolidating multiple security functions efficiently, so it can act not just as a firewall VNF but also provide other VNFs including IPS, application control, anti-malware, and web filtering. These can be consolidated as a single VNF in the service chain or with multiple chained FortiGates in a single-function-per-VNF approach.

Additionally, the FortiGate VM has been validated in independent NFV testing by EANTC and NIA to be able to provide routing VNF services for NFV and virtual CPE, eliminating the need to license and deploy a separate routing VNF. Aside from providing a Layer 3 edge gateway, the FortiGate VM can also provide other network services including DHCP and NAT.

One of the hottest trends in virtual CPE in 2016 has been software-defined WAN (SD-WAN). The FortiGate VM can also provide key SD-WAN functions including aggregating links and balancing WAN connectivity from MPLS to broadband to LTE. In addition, the FortiGate VM offers deep application-level traffic visibility and built-in WAN optimization, bringing security, networking, and SD-WAN functions in a single package and license model.

MULTIPLE FORTINET VNF OFFERINGS

Aside from FortiGate, Fortinet offers a broad lineup of virtual appliances, including web application firewalls, email security, advanced threat sandboxing, and application delivery controllers, all of which can be deployed as VNF services. All told, more than a dozen network and security products such as FortiWeb VM, FortiSandbox VM and FortiMail VM are available as virtualized x86 offerings running on ESXi, KVM, or other hypervisors.

ORCHESTRATED PROVISIONING AND DEPLOYMENT

With hundreds of thousands of FortiGate devices already in use by MSSPs as managed CPE, Fortinet long recognized the need to provide scalable tools to ease the burden of provisioning and deploying devices, whether it be for a large managed customer with CPE equipment at thousands of branch offices or retail stores, or for numerous smaller managed customers and businesses. MSSP tools like FortiDeploy
have been purposefully designed to help ease and scale the provisioning burden for providers for both physical and virtual appliances alike.

But now SDN and NFV orchestration promise to take things to the next level by providing an industry-standard framework for both Fortinet and 3rd-party VNF services to be automatically instantiated and inserted dynamically into multi-tenant service chains. With a highly extensible set of API’s in both the FortiGate VNF's as well as the FortiManager, Fortinet provides the broadest integration across a wide range of SDN and NFV orchestration vendors, and has been the most active security vendor to validate NFV integration and orchestration with vendor partners and independently through 3rd-party test labs, and industry bodies including ETSI, EANTC, and New IP Agency (NIA).

Validated integrations include SDN platforms including VMware NSX and Cisco ACI, and NFV MANO (Management and Orchestration) from Ciena Blue Planet, ADVA, Nuage Networks, Nokia CloudBand, UBlqube, Cisco NSO, OpenStack and Red Hat.

### TABLE 1: COMPARISON OF CPE FORM FACTORS

<table>
<thead>
<tr>
<th>Physical CPE</th>
<th>Virtual CPE</th>
<th>Hybrid CPE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td>✓/✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Supports 3rd-Party VNF</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>NFV Orchestration</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>MSSP Deployment Tools</strong></td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

#### ENABLING AGILE SECURITY AS A SERVICE

While NFV and vCPE can greatly automate and enhance managed service delivery, enterprise expectations are being further pushed by the leading IaaS and SaaS vendors with elastic pricing and self-service. Additional Fortinet offerings developed specifically for MSSPs can be combined with NFV and vCPE to deliver fuller benefits of a true “security-as-a-service” experience.

#### ON-DEMAND LICENSING AND METERING

Many MSSPs are looking at beyond merely offering opex-based subscriptions to true on-demand-based pricing and pay-as-you-go usage models. On-demand offerings can enhance upsell and incremental subscriber revenue by enabling existing customers to easily add additional security or other services from a VNF service catalog without the delay of manual provisioning steps.

Fortinet’s VM On-Demand program provides MSSPs with a flexible, utility-based model for licensing and metering VMs from Fortinet. VM On-Demand is a turnkey platform that streamlines licensing, provisioning, metering, and billing specifically for pay-as-you-grow usage by MSSPs for multiple managed service customers. The program complements NFV orchestration by automating licensing activation and usage monitoring as each VNF is instantiated, and consolidates usage data back to Fortinet’s back-end FortiCare cloud to simplify billing for each time or usage interval.

#### MULTI-TENANT SELF-SERVICE

FortiPortal is a dedicated MSSP offering that enables providers to stand up a multi-tenant web portal to manage multiple physical or virtual FortiGates. FortiPortal software is deployed to sit in front of an existing FortiManager and FortiAnalyzer deployment and can delegate self-service management of FortiGates to each managed service customer, all while providing the MSSP with a consolidated view of the multi-tenant environment.

### SUMMARY

Fortinet, recognized by Frost & Sullivan with Market Leadership Awards for both Global Managed Security Service Providers and for MSSP Firewalls, has developed a flexible range of FortiGate physical, virtual, and hybrid CPE form factors to support the next generation of MSSP services for agile and on-demand service delivery with NFV orchestration, on-demand, and self-service offerings. Fortinet’s Global Platinum and Gold MSSP Partner programs further provide marketing, sales, training, and support services to enable customer success with Fortinet technology solutions.