FORTINET

WHITE PAPER

The ABCs of On-Demand Infrastructure

Introduction

We have been and continue to be on a voyage to becoming an "ondemand" society. Our social and cultural environments are increasingly shaped and defined by their on-demand nature, availability, and consumption. On this voyage, technology plays a primordial role—and its adaptation by enterprises—the engine that drives us forward.

Information technology (IT) is at the core of the modern enterprise, and as such, on-demand IT is gradually becoming a reality with the growing business demand for cost-effective, on-demand services and resources for internal and external customers.

True on-demand IT—or IT as a service (ITaaS)—can become a reality only after all core aspects of IT have been transformed to enable and integrate into on-demand environments:

- **On-demand compute via compute virtualization and cloud**
- On-demand storage via storage virtualization and software-defined storage
- On-demand network via network virtualization, virtual network functions (VNFs)and software-defined networking (SDN)
- On-demand security via VNFs and SDN

The Alphabet of On-Demand IT

A. Definition of On-Demand

Providing on-demand [X] implies providing [X] as soon as it is requested, where [X] may be a service, a resource, or a combination of the two.

B. On-Demand Implies On-Demand Service Chain

The strong integration and interdependency between the different IT infrastructure components—compute, storage, network, security—dictate that on-demand delivery consists of a step-by-step enforcement of services, all working together to ensure that the requested service is delivered in an appropriate fashion based on defined KPIs such as performance, availability, cost, and security. These service chains must be well-defined to ensure their on-demand delivery as part of the service/resource.

Once an on-demand request is introduced, a complete service chain must be instantiated, configured, and managed for the on-demand service delivery. Although virtualization and VNFs are the building blocks for creating on-demand service chains, physical appliances may participate in on-demand service chains via the redirection of flows between the virtual and physical domains.

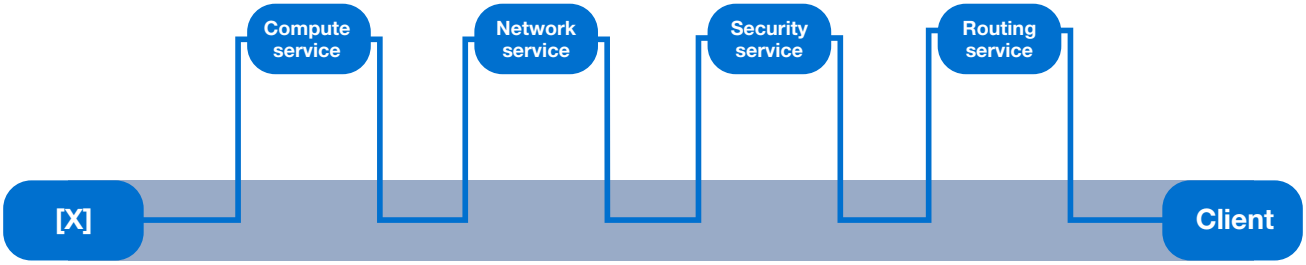

Figure 1: Service chain example.

C. Instantaneity

On-demand services and resources must be available within a defined and accepted time interval (Δt) to meet the core definition of on demand and ensure appropriate service level/KPIs. This implies that the entire service chain instantiation and configuration delay—associated with the service—must be taken into consideration. Different on-demand services may have different acceptable Δt. For example, Δt for an on-demand [virtual machine] may be measured in minutes, while a security service chain associated with it may be measured in seconds or less.

D. Reversibility

On-demand resources and services must be able to be "decommissioned" once no longer required. This is a critical factor in making the infrastructure scalable and cost-effective. Any associated service chain should be "decommissioned" as part of the overall decommission process.

E. Resiliency

On-demand IT ecosystems serve sensitive and business-critical applications and services and therefore must deliver the appropriate resiliency and uptime required to meet appropriate service levels. The fact that on demand services heavily rely on virtualized resources that may exist for a precise and finite amount of time does not necessarily reduce its criticality and availability. And as the delivery of the service will, in most cases, include an associated service chain, this service chain must also be resilient.

F. Automation and Orchestration

In order to meet Δt requirements—as previously discussed—the IT infrastructure must be automated and orchestrated so that any delay-inducing factor, such as manual resource provisioning and configuration, is avoided.

Automation may cover aspects such as:

- The instantiation of resources and services
- The configuration of service chain elements

In this hybrid, multi-vendor, and complex ecosystem, the orchestration element is required to homogenize higher-level management and operation of the ecosystem to enable the working together of the different elements and components delivering the overall on-demand service.

The ecosystem should provide service assurance in a very dynamic environment. The best way of doing so is via the integration of analytic capabilities/solutions that can, in real time, analyze the behavior of the services and resources and provide such visibility so that the automation and orchestration component can take the appropriate actions to proactively ensure the service availability and service levels.

Orchestration may cover aspects such as:

- End-to-end policies and KPI enforcement
- Service chains instantiation
- Auto scaling of resources

G. Openness

Building an on-demand infrastructure and ecosystem creates a multi-vendor environment that works together to provide the required functionality in an automated, controlled, and managed fashion. The fact that this is an on-demand environment, where change and agility is the norm and where automation plays a key role, enhances the importance of openness via APIs.

From physical and virtual resources to overall management—the different components must provide open APIs to allow the cooperative integration and orchestration that will deliver on-demand services and resources.

H. It Is an Ecosystem

The relationship and dependencies between different IT technologies (compute, storage, networking, and security) required to deliver an end-to-end service exist in both a static IT environment and an agile and dynamic on-demand IT environment.

The notions of time and agility are of great importance in an on-demand environment. The technologies and mechanisms that bind all together to dynamically create on-demand service chains will form a well-defined and integrated ecosystem, as described in Figure 2:

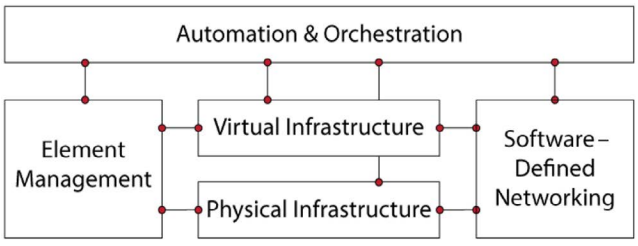

Figure 2: On-demand ecosystem.

On-Demand Core Technologies in a Nutshell

Building an on-demand environment and ecosystem is, in most cases, an evaluative process driven by progress in technology and competitive pressure. At the core of the on-demand revolution lie the following key technologies:

I. Software-Defined [X]

A software-defined technology enables the complete control of software over infrastructure, be it physical, virtual, or a mix of both. This implies minimal or no human intervention and independency of any hardware-specific dependencies. As software is fast, software-defined technologies are fast and therefore a fundamental building block in on-demand environments.

As on-demand requires service chains across all IT technologies (compute, storage, networking, and security), software-defined is implemented across all of IT:

- **Software-defined compute (SDC)**—Based on compute virtualization, SDC software enables the instantiation, provisioning, and lifecycle management of virtual compute resources, or virtual machines (VMs), on top of x86 hardware.
- **Software-defined storage (SDS)**—Based on storage virtualization, SDS software enables the instantiation, provisioning. and management of virtual data storage independent of the underlying physical storage hardware.
- **Software-defined networking (SDN)**—Based on control and data planes separation, the SDN framework enables the dynamic provisioning and management of networking and security service chains on physical and virtual infrastructures.

J. Network Function Virtualization (NFV)

NFV is a virtual network architecture whereby networking and security functions are virtualized as VNFs on top of a virtualized compute infrastructure. VNFs may include functions such as routing, load balancing, next-generation firewalling, etc.

NFV enables the instantiation, provisioning, and lifecycle management of the different VNFs. These VNFs are then used to deliver services and chains, as required, via the integration with SDN.

Based on SD[X] and NFV technologies, we can now present the on-demand ecosystem with more details:

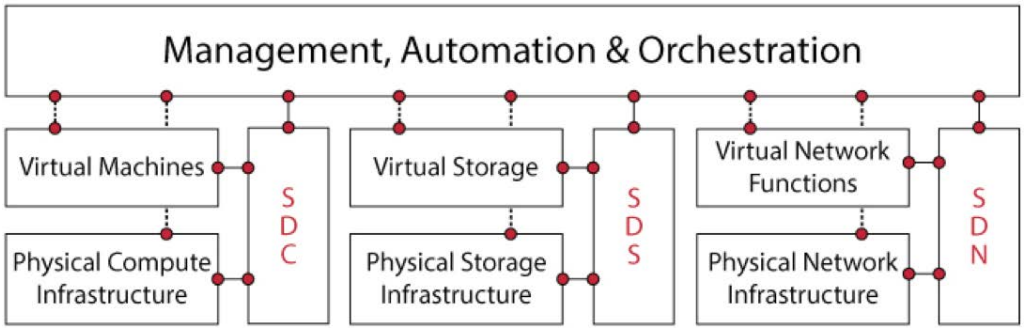

Figure 3: On-demand ecosystem technologies.

K. The Cloud

The most popular and well-known name for an on-demand environment is the cloud. Although not a technology, the cloud is a key term in on-demand IT and understanding what it means is important when considering security in an on-demand IT environment.

In general—and from an enterprise point of view—we can distinguish between "two-and-a-half" types of cloud:

- **Private cloud**—The on-demand IT environment (physical and virtual) is owned and under full management and responsibility of enterprise IT. This is a single-tenant environment—the enterprise itself. Security is under the full responsibility of the enterprise.
- **Public cloud**—The on-demand IT environment (physical and virtual) is owned by a third party (a cloud provider). This is a multitenant environment whereby the enterprise is one tenant (out of many) sharing a pool of shared resources for which he has partial control and management. Based on the type of cloud services consumed by the enterprise (IaaS, PaaS, or SaaS), different security considerations and responsibilities are required from the enterprise.
- **Hybrid cloud**—This is the "half" type of cloud, as it describes an enterprise IT environment where both private and public clouds are used.

On-Demand Security for On-Demand IT

In an on-demand IT environment, security is provided as part of an on-demand [X]'s service chain. These are the main considerations in deploying security in such an environment:

The appropriate security services and controls are mostly, but not solely, delivered as VNFs:

Instantaneity—Implemented purely in software, the instantiation of security VNFs represents a very small Δt, which facilitates the creation of on-demand services and service chains.

East-west traffic visibility and control—Most data center and cloud traffic flows between workloads (the VMs and their applications) and therefore is not "naturally" visible to physical security appliances in the core of the edge of the data center. This is east-west traffic. Security VNFs integrate as part of the virtual ecosystem (as a VM or at the hypervisor level) and provide both visibility and security for these traffic flows.

1. **Reversibility**—Similar to instantiation, VNFs' "decommissioning" and removal from service chains is instant and meets on-demand Δt requirements.
2. **Public cloud ready**—For all practical considerations, public cloud environments are 100% software defined and therefore only VNFs can be used to provide security in such environments.
3. **Cloud migration**—Workloads, data, and applications migration between private and public/hybrid clouds is facilitated, as the same security VNFs can be easily deployed in the private and public/hybrid clouds.
4. **OPEX vs. CAPEX**—With an ever-existing pressure on IT-related costs, VNFs facilitate the move towards a more OPEX-based expenditure model.

However, a service chain may include security services delivered by a physical security appliance, not a security VNF. This can be achieved via flow redirection—controlled and managed by SDN and SDN switches—or by the security appliance's integration with an existing SDN solution. Using a physical security appliance to participate in on-demand service chains may be required in the following cases:

1. **High-performance/low-delay requirements**—Physical appliances use dedicated hardware and ASICs that allow for significantly higher performance levels and lower delay compared to security NFVs.
2. **North-south traffic visibility and control**—As on-demand IT environments will expand beyond the data center and the cloud into other parts of the enterprise, security in service chains may include data flows leaving and entering the cloud. These flows are known as north-south traffic, and security visibility and enforcement are provided via physical security appliances.

The NFV and SDN frameworks are deployed in complementary roles—NFV provides the agility required for the instantiation of the security components (and any other networking component) that make up the service chain (AV, IPS, app. control, etc.), while SDN configures these components and forms the service chain itself, via the direction of the appropriate traffic flows to the appropriate components in the service chain.

On-demand environments MUST include these two components (NFV and SDN) and the presence of an automation and orchestration layer. Therefore, any security infrastructure—physical and virtual—must integrate with these three components.

These components are available in many colors and flavors. Some provide solutions covering hybrid physical and virtual environments while some only cover physical or virtual resources. Some are open source while some are commercial solutions. Some are standards' based, while others are proprietary. It is therefore important that whatever security VNF and physical appliances are used in the on-demand ecosystem, they should provide the widest support for the required integration points to the implemented SDN, automation, and orchestration solutions, via either exhaustive API capabilities or pre-integration with commercial solutions.

Fortinet Solutions for On-Demand IT

Fortinet provides a rich set of security solutions that integrate into on-demand environments in a coherent approach, covering the different aspects of this environment via open and commercially integrated solutions as outlined in the following diagram:

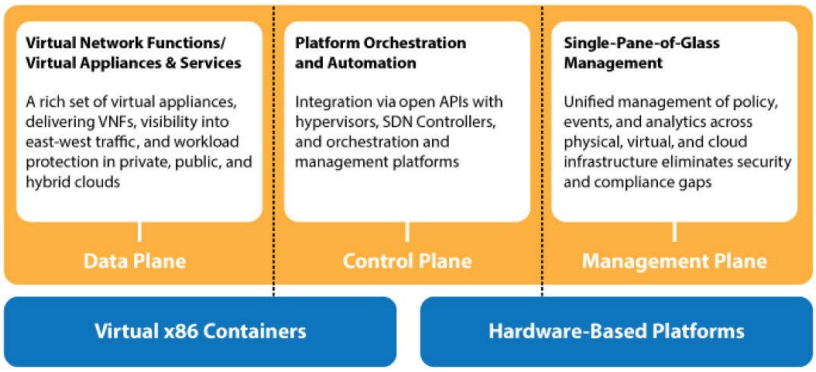

Figure 4: Fortinet SDN Security (SDNS) framework.

Fortinet's SDNS framework provides the following main building blocks:

Fortinet's Security VNFs

The table below provides an insight into the security VNFs provided by Fortinet. This is the richest set of security VNFs in the market, and they are available for the widest range of compute virtualization solutions from leading commercial platforms, open source, and public clouds:

	VMware vSphere v4.0/4.1	VMware vSphere v5.0/5.1/5.5	VMware vSphere v6.0	Citrix Xen Server v5.6 SP2	Citrix Xen Server v6.0/6.2	Xen	KVM	Amazon AWS	Microsoft Hyper-V 2008 R2	Microsoft Hyper-V 2012	Microsoft Azure
FortiGate-VM *	•	•	•	•	•	•	•	• **	•	•	•
FortiManager-VM	•	•	•		•	•	•	•	•	•	
FortiAnalyzer-VM	•	•	•		•	•	•	• **	•	•	
FortiWeb-VM	•	•	•		•	•	•	•		•	•
FortiMail-VM	•	•	•		•		•		•	•	
FortiAuthenticator-VM	•	•	•						•	•	
FortiADC-VM		•	•		6.2	•	•			•	
FortiCache-VM	•	•	•								
FortiVoice-VM		•	•		•		•			•	
FortiRecorder-VM		•	•		•		•			•	
FortiSandbox-VM		5.5	•								
FortiWAN-VM		5.5	•								

Platform Orchestration and Automation

As previously discussed, the overall on-demand environment, consisting of the different technologies and resources, is delivered as a unified and coherent platform via the automation and orchestration components, which serve as the binding glue of the ecosystem.

Fortinet's VNFs and physical security appliances integrate into automation and orchestration components of the on-demand platform via the following two main methods:

Platform Orchestration and Automation

As previously discussed, the overall on-demand environment, consisting of the different technologies and resources, is delivered as a unified and coherent platform via the automation and orchestration components, which serve as the binding glue of the ecosystem.

1. Pre-integrated and supported solutions such as:
   - FortiGate VMX for VMware NSX
   - FortiGate ACI Connector for Cisco ACI
   - FortiGate OpenStack Connector for OpenStack
   - FortiGate VAN Connector for HPE VAN
2. Open APIs, including REST and JSON, and support for standards such as OpenStack and ML2, for integration with third-party automation and orchestration solutions.

Single-Pane-of-Glass Management

The Fortinet suite of centralized security management provides unified management of security policy, events, and analytics across physical, virtual, and cloud infrastructure and eliminates security and compliance gaps:

1. **FortiManager** ensures that security VNFs and security service chain components are configured according to the predefined policies and that the enterprise's end-to-end security posture and compliance are maintained. Open APIs are provided for integration with orchestration and automation solutions.
2. **FortiAnalyzer** provides extended data collection and analysis, giving valuable insight into threats and users and applications behavior on the network and in the on-demand environment. Open APIs allow the integration of third-party analytics and big data solutions.
3. **FortiSIEM** With provides a comprehensive and holistic end-to- end solution, with unified NOC and SOC analytics and real-time event correlation to tightly manage network security, performance, and compliance standards, all delivered through a single-pane-of-glass view of the organization. A rich set of APIs allows for integration with orchestration, management, big data, threat intelligence, and other thirdparty solutions.

Fortinet provides a rich set of security solutions—as VNFs and physical appliances, in private and public clouds, pre-integrated and open via a rich set of open APIs—that help make on-demand IT a reality for many enterprises.

October 12, 2019 1:59 AM

488922-A-0-EN

D:\Fortinet\White Paper\ABCs of On-Demand Infrastructure\wp-the-abcs-of-on-demand-instratructure-v1