FORTINET
Network Security Expert 7

Private Cloud Security Study Guide

for FortiOS 6.0

FORTINET NSE
NSE Certification Program

Fortinet Training

http://www.fortinet.com/training

Fortinet Document Library

http://docs.fortinet.com

Fortinet Knowledge Base

http://kb.fortinet.com

Fortinet Forums

https://forum.fortinet.com

Fortinet Support

https://support.fortinet.com

FortiGuard Labs

http://www.fortiguard.com

Fortinet Network Security Expert Program (NSE)

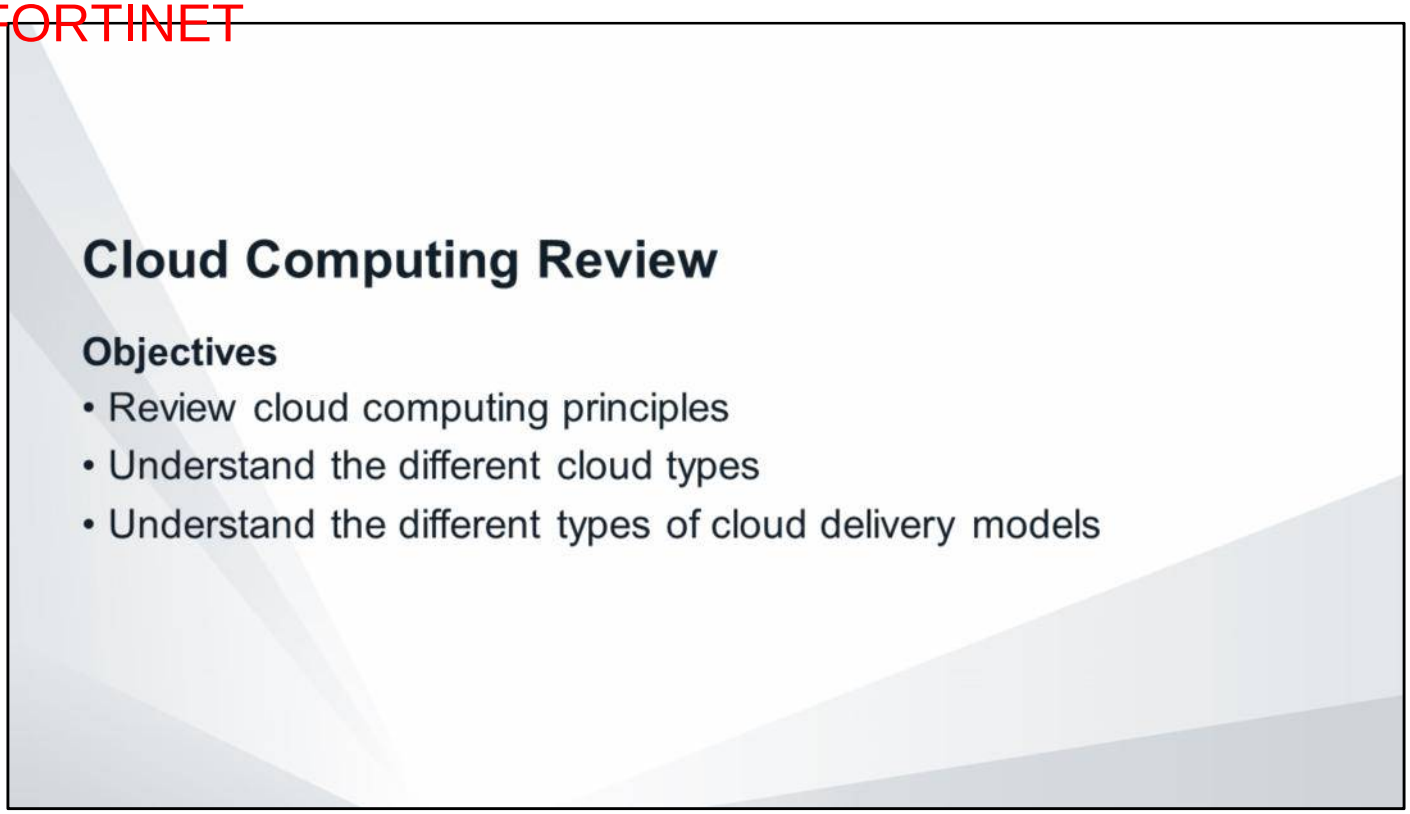
https://www.fortinet.com/support-and-training/training/network-security-expert-program.html

Feedback

Email: courseware@fortinet.com

TABLE OF CONTENTS

In this lesson, you will learn about east-west traffic, cloud security challenges, and the Fortinet cloud security approach.



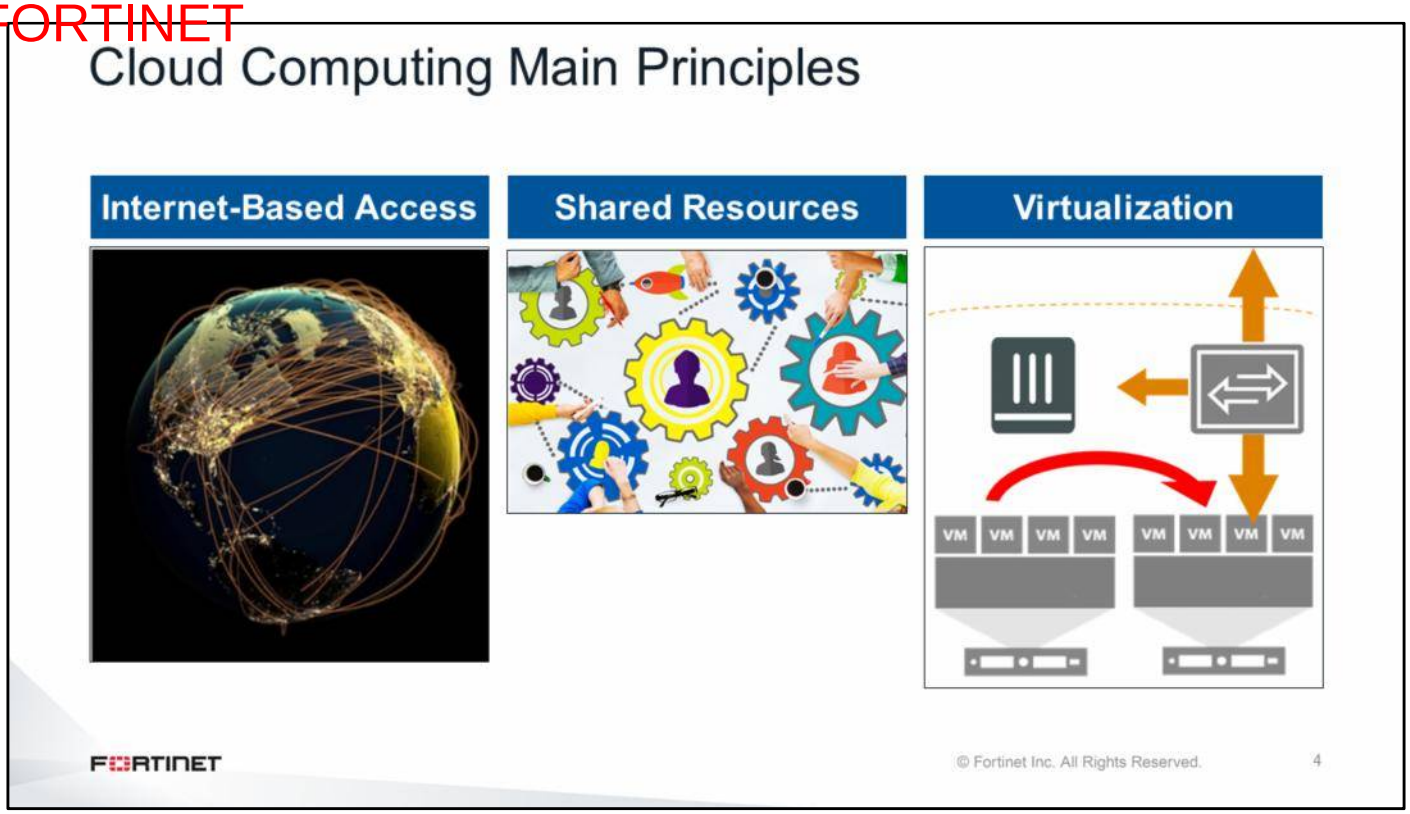
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the concept of east-west traffic, and the different types of cloud delivery models, you will be able to understand how cloud computing applies to your network.

Cloud computing is the on-demand availability of computer system resources—especially data storage and computing power—without direct active management by the user. The term cloud computing is generally used to describe data centers available to many users, over the Internet. What do the terms private cloud and public cloud mean?

Public cloud: Public clouds are available to any organization. Several well-known vendors, including Microsoft, Rackspace, Symantec, and Amazon provide public cloud environments.

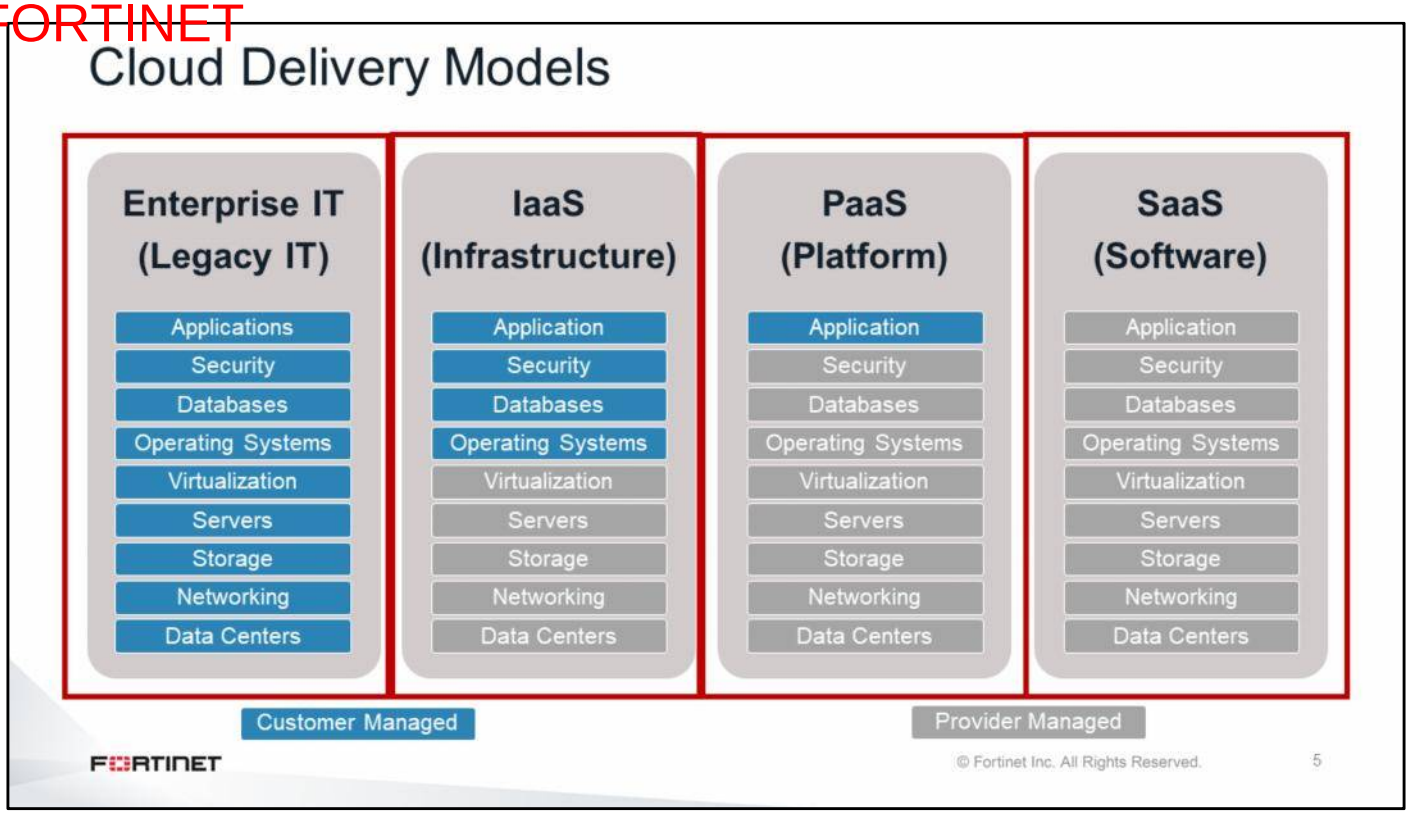
Private cloud: Private clouds are designed to be visible to only the organization that creates them. Private clouds provide many of the same benefits as public clouds, but still allow you to maintain ownership of the data and equipment. A private cloud is essentially a private data center that an organization creates with stacks of servers all running virtual environments, providing a consolidated, efficient platform on which to run applications and store data.



There are three main principles in cloud computing.
Internet-based access: Resources are available and accessible through the Internet. This means that applications and files are hosted on a cloud consisting of thousands of computers and servers, all linked together and accessible through the Internet.

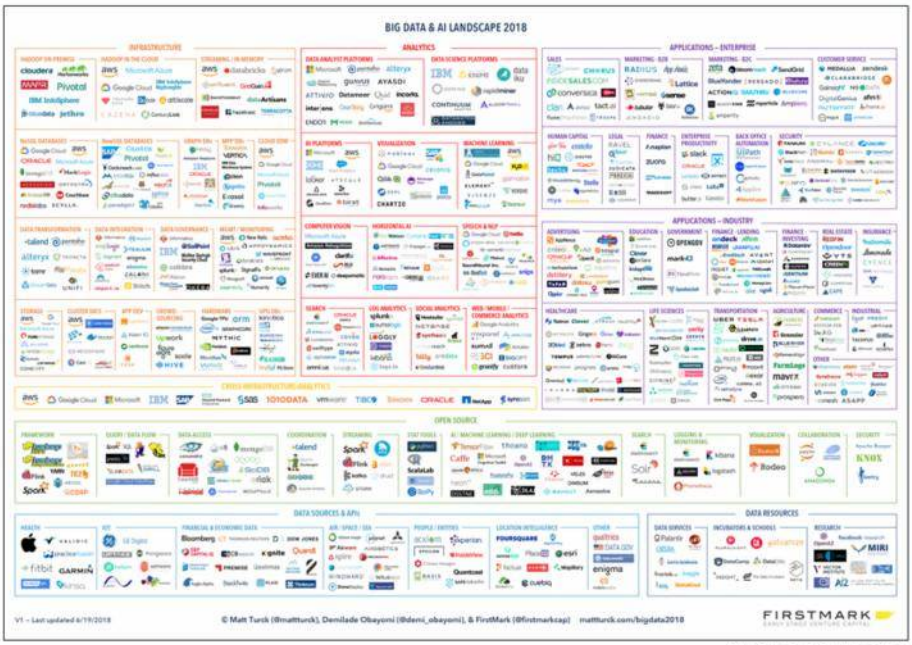
Shared resources: Cloud computing is a shared network information delivery model; users do not need to care about the cloud infrastructure. The name cloud is a virtualization concept, representing an infinite resource pool. Both hardware and software resources are packaged as services that users can access and use on demand, through the Internet. From the user's point of view, these resources are unlimited, and can be expanded and configured dynamically. Physically, these resources are distributed, but, to the end user, they appear as a single, integral form. Users access these resources on demand and pay according to usage.

Virtualization: Virtualization is the concept computer components running in a virtual environment, not real hardware. Virtualization technology is an important part of cloud computing and cloud storage of the data center. Virtualization makes data center computing power more scalable, and makes accessing of data. It also improves the management of cloud computing services, as well as making the management easier. Virtualization dynamically maps the physical resources of the infrastructure to the drive of the application. Virtualized infrastructure creates a virtualized pool of resources, and unifies management servers, storage, and networks.



As shown on this slide, there are many cloud delivery models. In a traditional, enterprise IT scenario, all the servers, switches, and databases run locally on site and managed by the customer. The virtual machines (VMs) that you deploy during the labs are considered to be infrastructure as a service (IaaS) delivery model. In an IaaS model, some parts of networking and services are managed by the vendor, and other parts are managed by the customer. There is also a model called platform as a service (PaaS), where the customer is responsible for programming applications, and all other services are managed by the vendor. Finally, in the software as a service (SaaS) the customer is using the services as a consumer, for running applications. Some examples of these services are Dropbox, Office365, and Salesforce.

Big Data Landscape

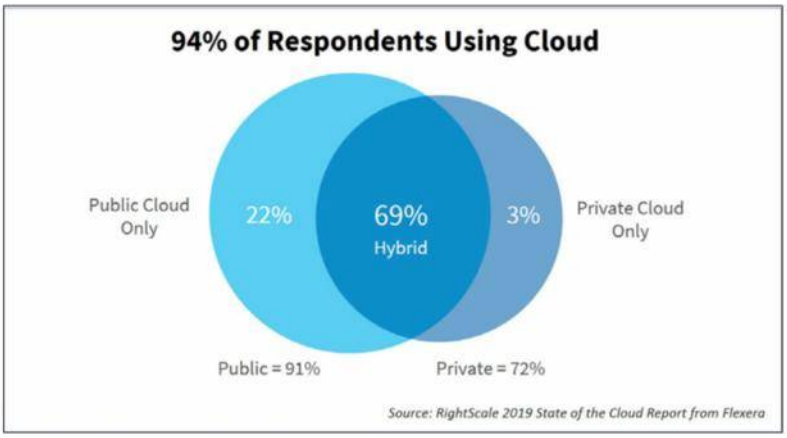


Big data analytics refers to the practice of analyzing large and disparate sets of structured and unstructured data in an effort to gain useful insights that can be used to make sustainable decisions for a business. Data analytics can provide valuable information about consumers shopping patterns, preferences, and demographics. These insights can help organizations create optimal marketing policies, so that they can target their customer base with a viable and results-oriented strategy. As a result, the demand for expert big data analytics services, as well as tools that can provide analysis reports on demand and with minimal coding, is on the rise.

Big data projects typically start with data storage and the application of basic analytics modules. However, as you discover ways to extract data at a much larger scale, you will need to find better methods to process and analyze this data, which will likely require infrastructure upgrades. You may add more capacity to your in-house data warehouse, or add more servers to cater to the rapidly-increasing analytics requirements. However, even if you increase the capacity of your on-premises systems, your infrastructure may eventually be unable to keep up. This is where the cloud comes in, or, more accurately, when your big data moves to the cloud.

Cloud Computing Market Numbers

- Any cloud: 94%
- Public: 91%
- Private: 72%
- Hybrid: 69%
- Public only: 22%
- Private only: 3%



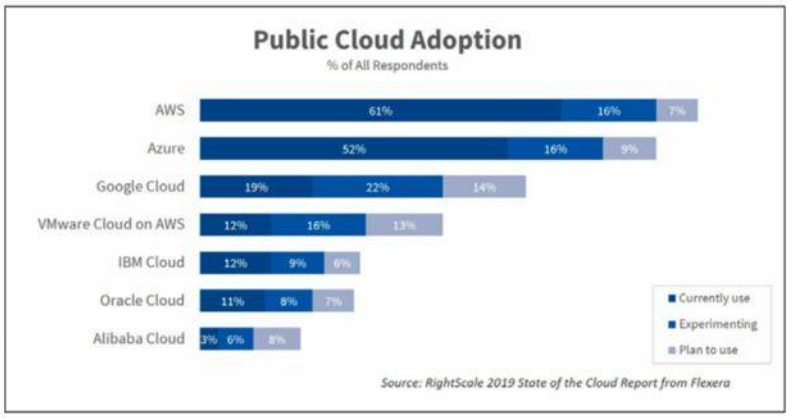
FORTINET

 7

A survey done by Flexera in 2019 shows the number of respondents now adopting public cloud is 91 percent, while the number of respondents now adopting private cloud is 72 percent. As a result, the overall portion of respondents using at least one public or private cloud is now 94 percent.

Cloud Computing Market Numbers (Contd)

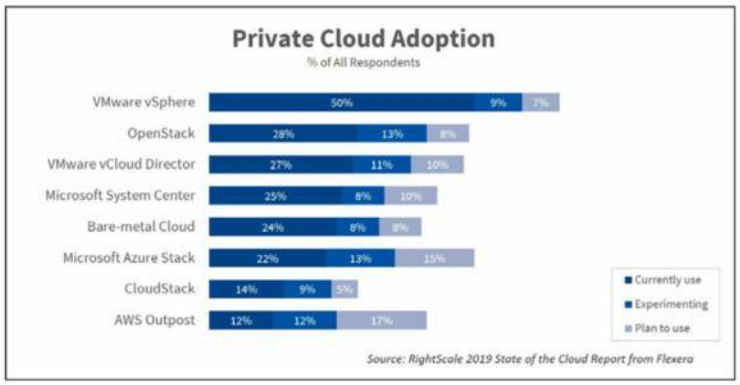
- Amazon AWS is by far the public cloud of choice
- Microsoft Azure comes second, but it is still gaining market share
- Google is still struggling…
- VMware on AWS has significantly increased its market share



 8

In 2019, AWS continues to lead in public cloud adoption, but adoption of other public clouds is growing more quickly. Overall, the adoption of Azure public cloud grew from 45 to 52 percent, narrowing the gap with AWS. As a result, Azure adoption has now reached 85 percent of AWS adoption, up from 70 percent last year. Google maintained its third-place position, increasing slightly from 18 to 19 percent adoption. VMware Cloud on AWS moved up to fourth position this year, increasing to 12 percent from 8 percent in 2018, a growth rate of 50 percent.

Cloud Computing Market Numbers (Contd)



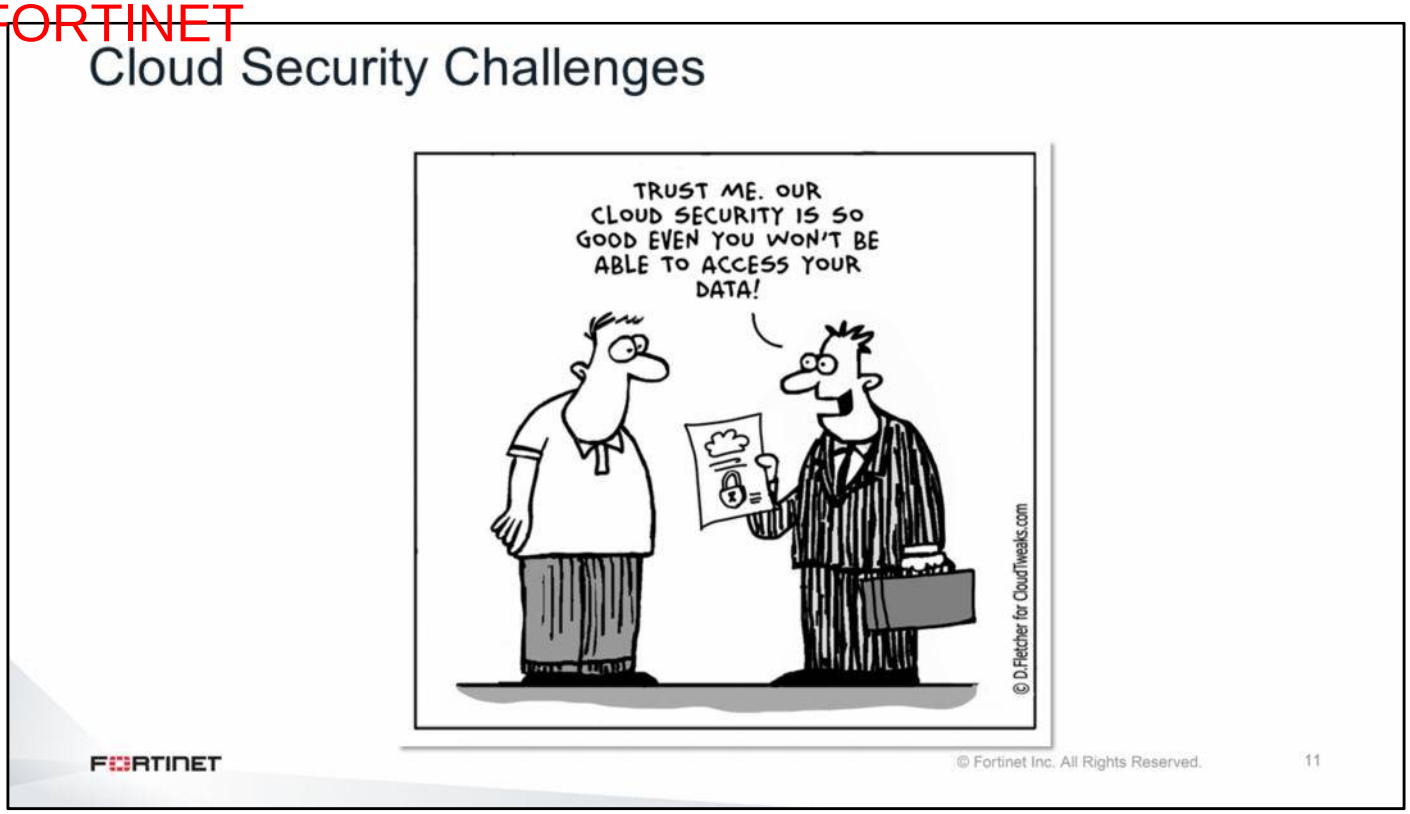
- VMware vSphere is the leader when it comes to private cloud
- OpenStack comes second
- VMware vCD has picked up but still quite expensive
- Microsoft System Center is still growing super fast
- CloudStack is the new kid on the block

 9

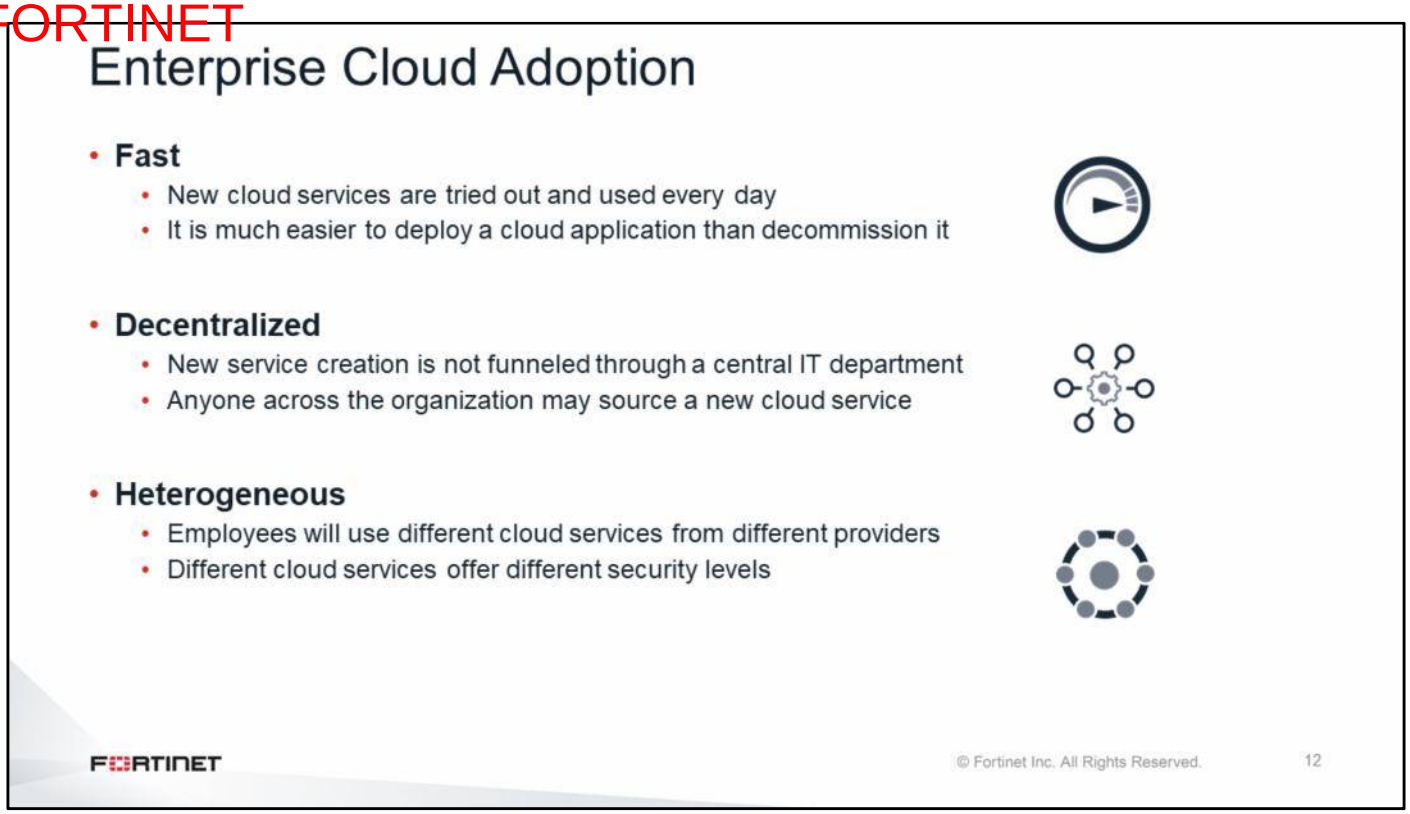
The Flexera 2019 survey shows that the adoption of private cloud increased slowly across most providers except for VMware vSphere. Overall, VMware vSphere continues to lead with 50 percent adoption, flat from last year. This includes respondents who view their vSphere environment as a private cloud—whether or not it meets the accepted definition of cloud computing. OpenStack (28 percent), VMware vCloud Director (27 percent), Microsoft System Center (25 percent), and Bare-metal Cloud (24 percent) all showed small increases over 2018. Azure Stack was in the sixth slot, but showed the highest growth (22 percent in 2019 compared to 17 percent in 2018). AWS Outpost was announced in late 2018 and showed strong adoption out of the gate (12 percent) and strong interest for future use (29 percent).

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the concept of cloud security and its challenges, you will be able to choose the best solution for your organization.

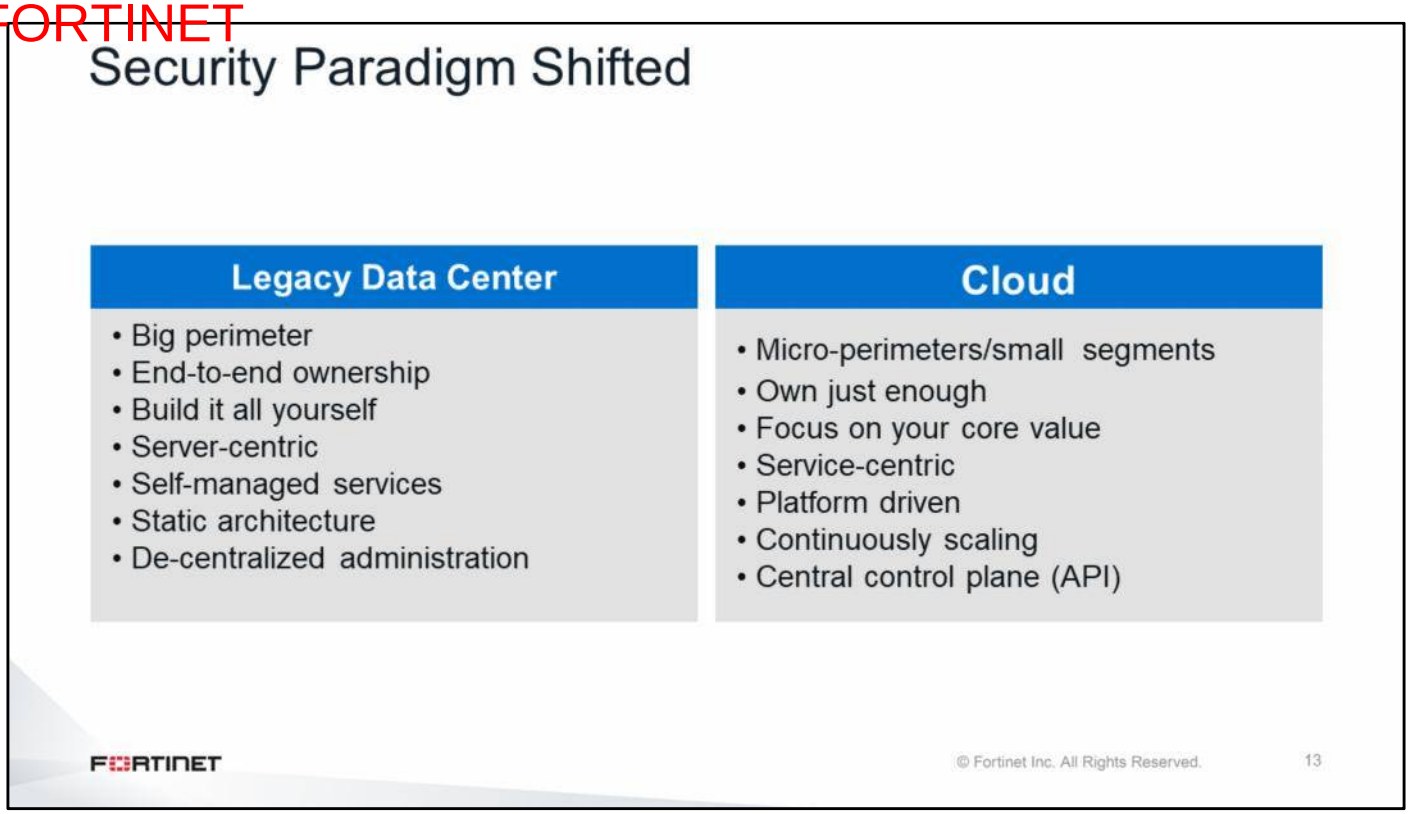


Organizations are embracing multiple public cloud platforms, resulting in increased complexity of management, which impacts security and risk. Additionally, the built-in security tools that come with various cloud platforms are unique to each one, compounding the challenge of consistently managing risk across all clouds in a multicloud world. This challenge renders security operations time consuming and ineffective. As the attack surface expands, organizations need to protect themselves not only from the risks associated with the configuration and management of the application elements themselves, but also from risks originating through cloud application programming interfaces (APIs) and UIs.

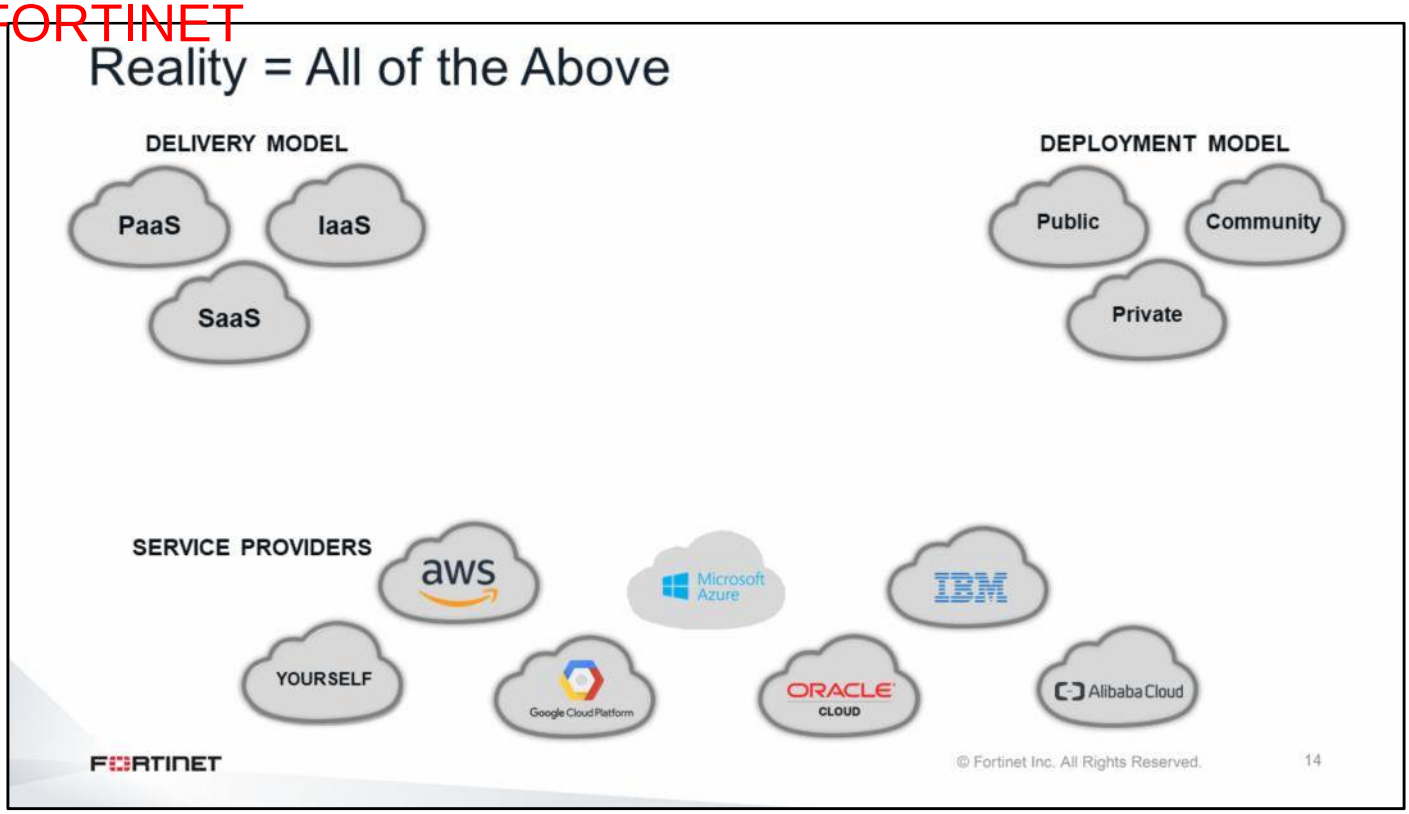


While the business advantages are significant, this rapid migration is also introducing complexities and risks that few organizations have adequately prepared for—right at a time when the cybersecurity skills gap is dangerously wide, and cybercriminals are more capable of exploiting vulnerabilities than ever before. Here are a few of the challenges that unchecked cloud adoption has introduced:

- New cloud services are being adopted and used every day. However, it turns out that it is much easier to deploy a cloud application than to decommission it, so organizations are finding that cloud-based applications and services are piling up, making them increasingly difficult to manage and secure.
- The adoption of cloud-based applications and services is remarkably easy. Anyone across the organization can source a new cloud service. The challenge is that service creation is often not funneled through the central IT department, resulting in the creation of shadow IT. As a result, the organization has little idea of what services are being used, where corporate information is being stored, who has access to it, or what security strategies are in place to protect it.
- Complicating this further, adoption of these services is heterogeneous. Employees use different cloud services from different providers, and these different providers all offer different security tools, different native security controls, and different levels of security. This can make it extremely difficult to impose any sort of consistency to security policy distribution, orchestration, or enforcement.

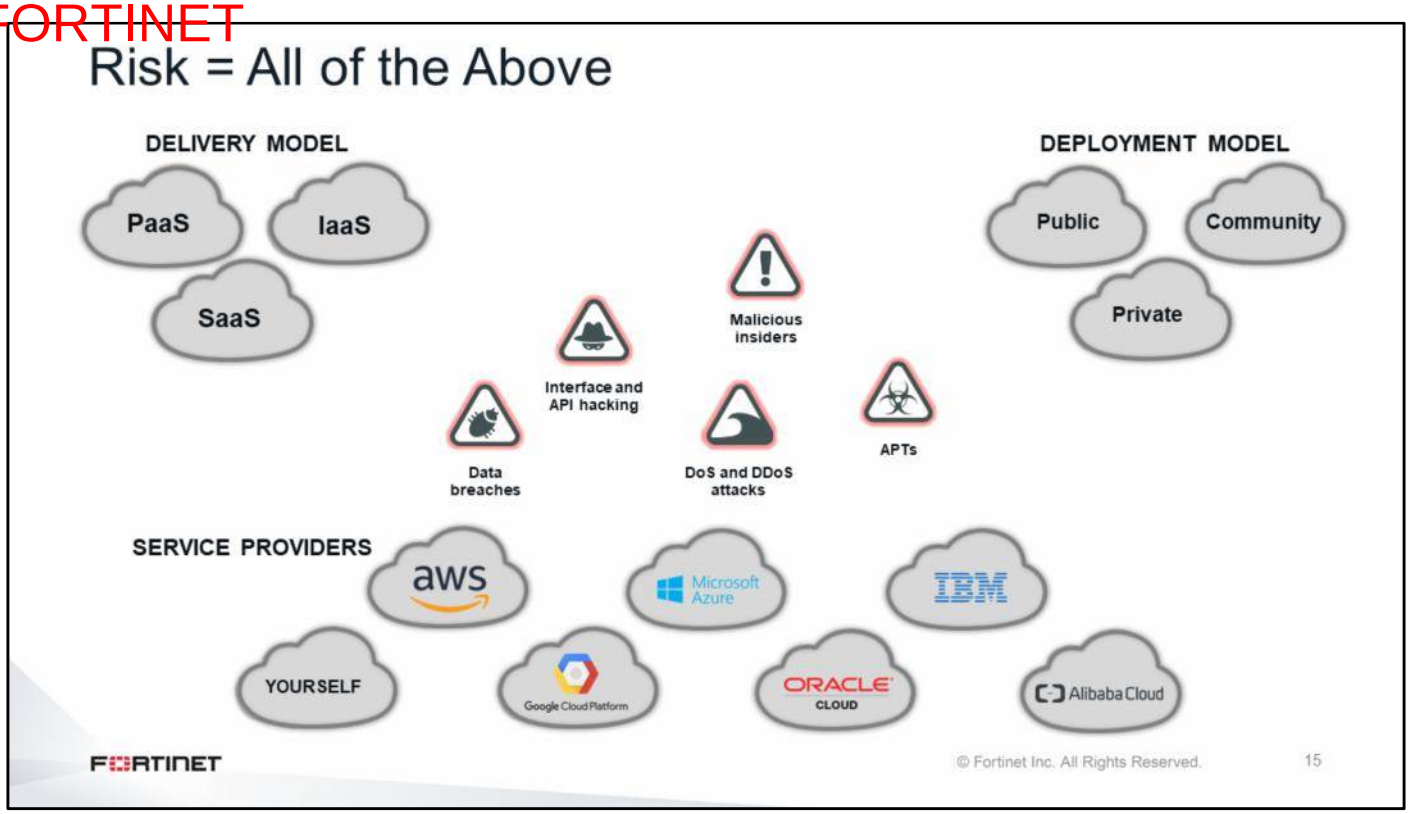


Unlike an organization independently building a data center infrastructure, cloud-based IaaS is built and aggregated through pools of resources and is designed to be elastic to scale with organizational demand. The leasing and subscription model changes how security is designed and implemented, as cloud consumption transitions from traditional CAPEX to OPEX in the public cloud. The security paradigm shifted from protecting a big-perimeter walled garden, to micro-segmented security control of business workloads. IT infrastructure becomes shifted from end-to-end complete data center ownership, to owning just enough for the workload to operate in the cloud. IT architecture becomes shifted from static approaches to elastic capacity with on demand metering consumption. This paradigm shift applies to both cloud ingress/egress (northbound-southbound) and lateral (eastbound-westbound) network traffic flow.



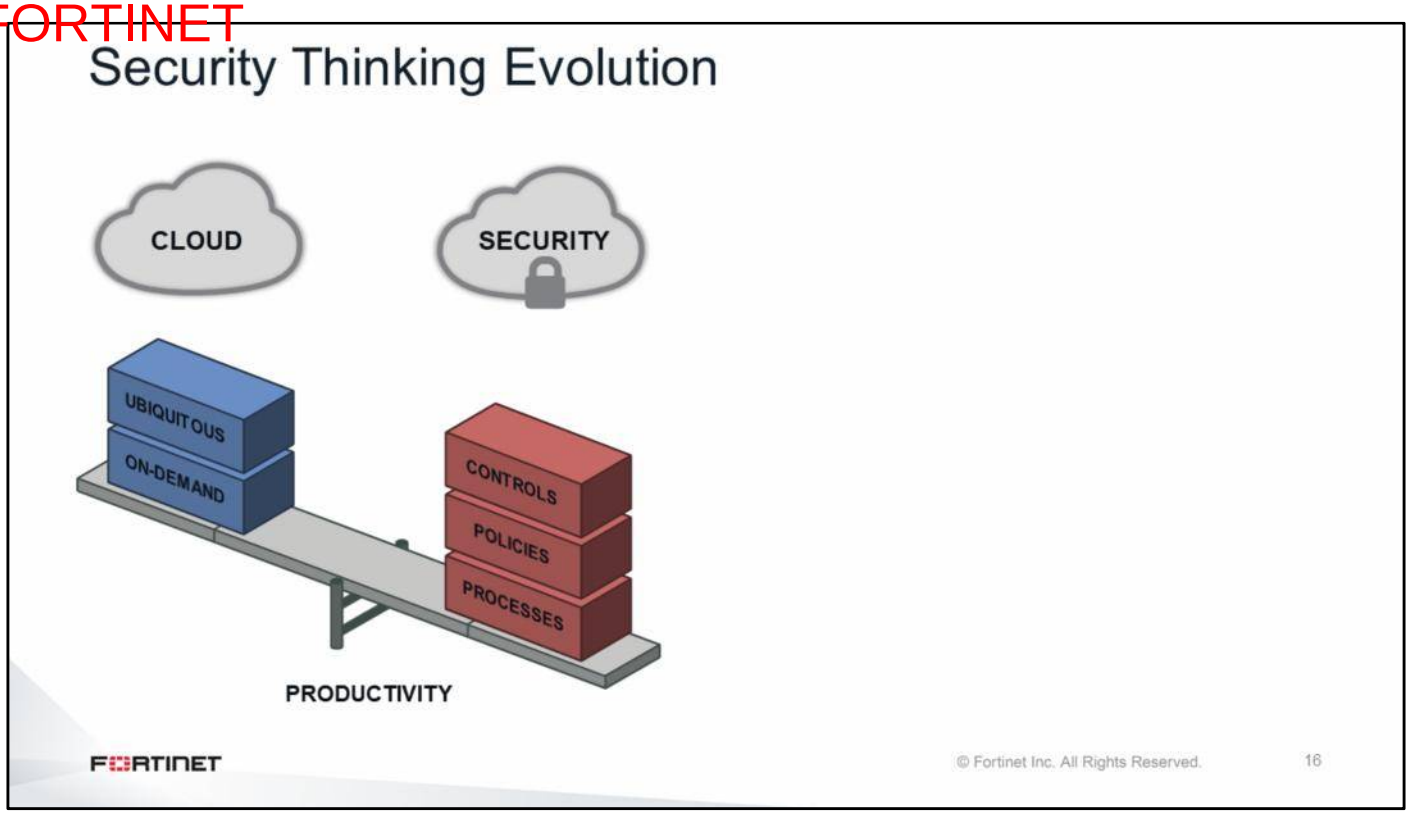
As shown on this slide, cloud solutions can be broken down into three categories: deployment models, delivery models, and service providers.

Delivery models: Organizations have a variety of options for how much of their services they want to implement, from simply adopting specific applications or services to a full-blown infrastructure.
Deployment models: While most people only think of private or public cloud environments, or even hybrid models, a new model is beginning to emerge—the community cloud. A community cloud provides a cloud computing solution to a limited number of individuals or organizations that is governed, managed, and secured commonly by all the participating organizations, or by a third-party managed service provider. AWS GovCloud is a good example of this.
Service providers: A variety of service providers are also available such as AWS, Azure, Google Cloud Platform, and so on. Each include their own native controls and marketplaces for buying technologies and services—either their own or from a third-party vendor—and different environments provide distinct advantages to customers, such as compatibility with existing infrastructures or business objectives.

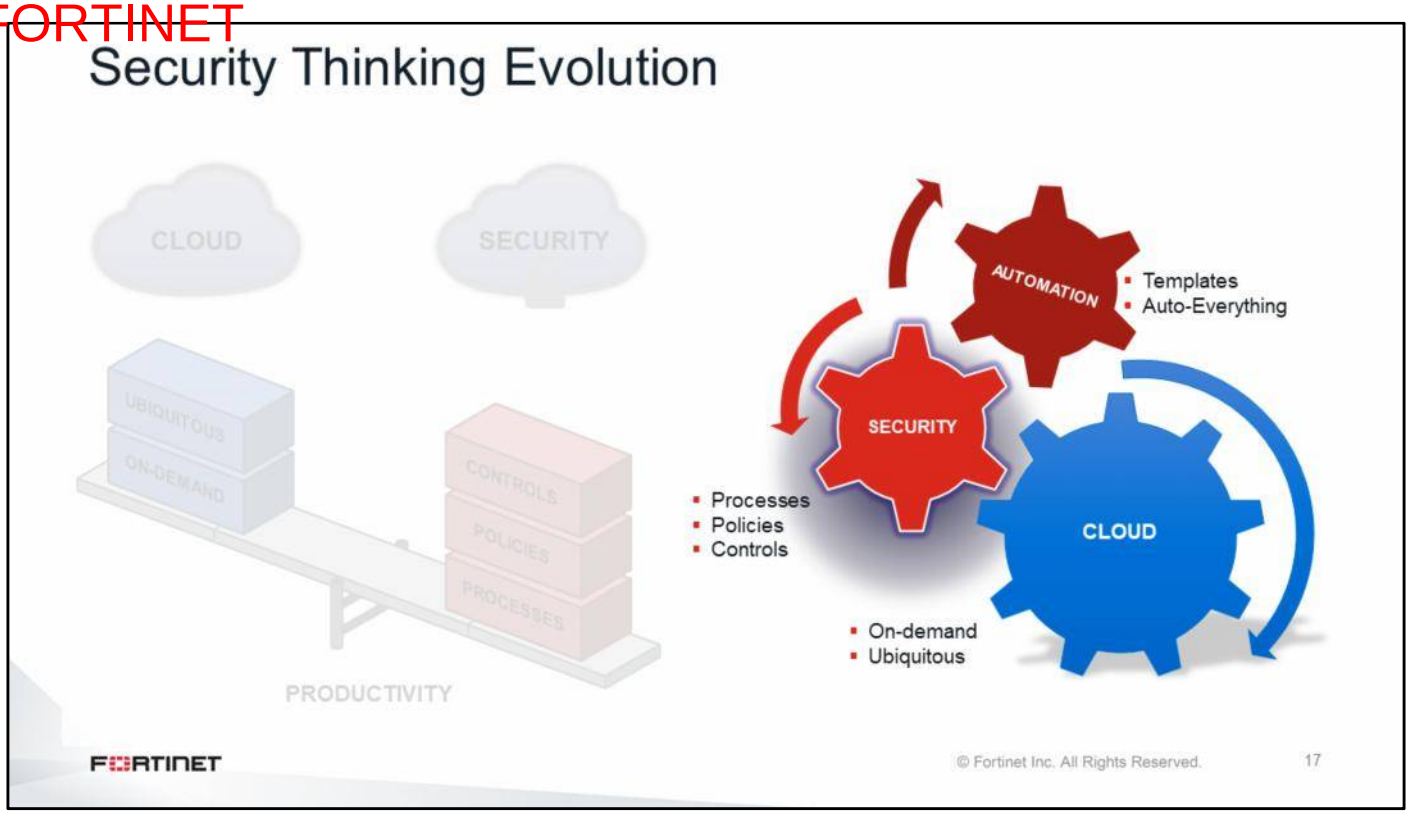


Eventually, all organizations will end up having deployed some combination of the cloud solutions described on this slide. However, adopting multicloud environments not only expands the attack surface and complicates the ability to deploy, manage, and orchestrate security with consistent visibility and control, but it also increases other cyber risks, including:

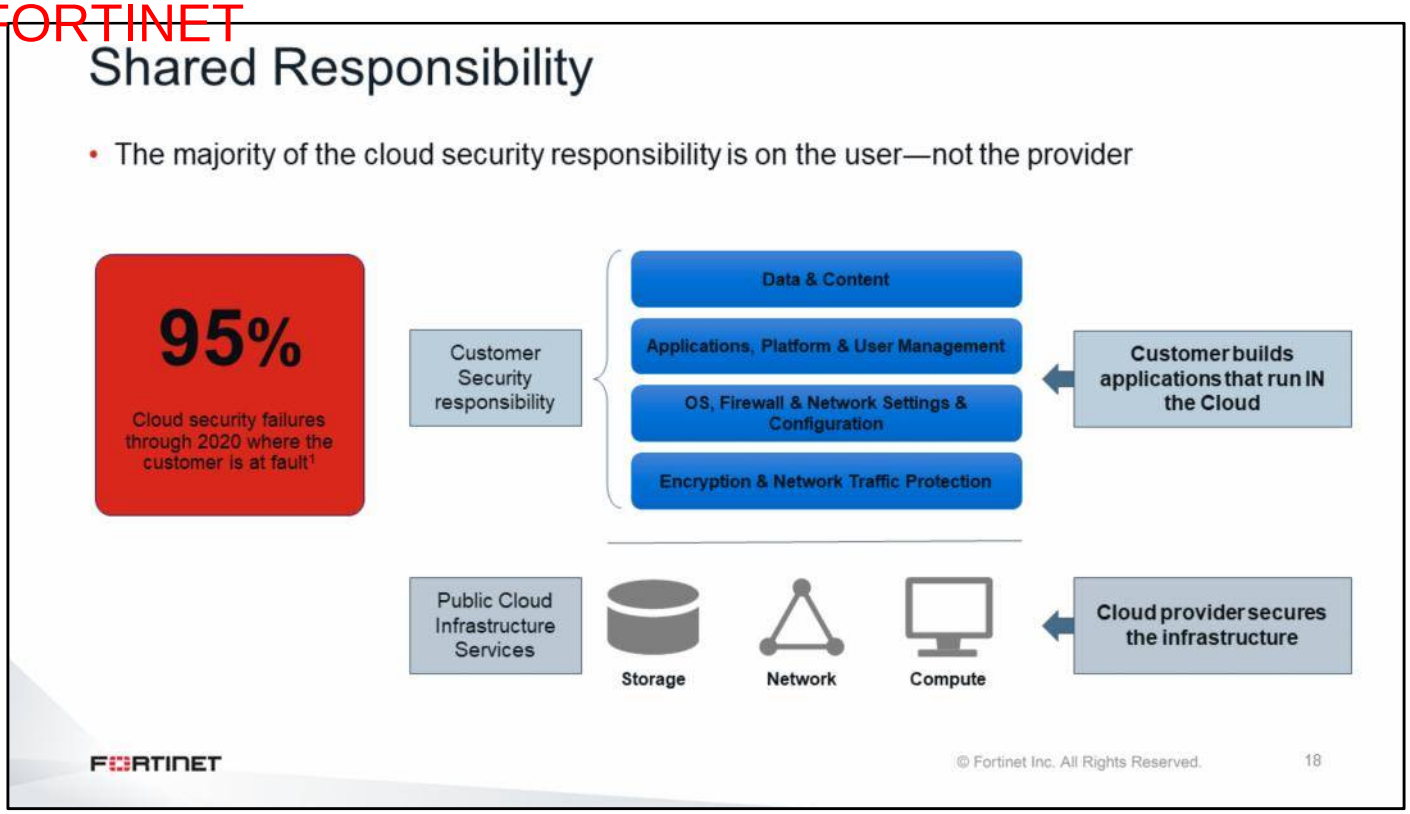
- Data breaches
- Insecure interfaces and APIs
- Increased opportunities for malicious insiders
- An increased footprint for advanced persistent threats
- DoS and DDoS attacks



Addressing cyber security challenges needs to be handled delicately. Performance cannot be sacrificed for security. Instead, organizations need to strike a balance between ubiquitous, on-demand cloud services and establishing consistent controls, policies, and processes. This requires looking for security solutions that help you move from a model where security inhibits business agility, to a model where security can be combined with cloud and automation to help business move faster and more securely.



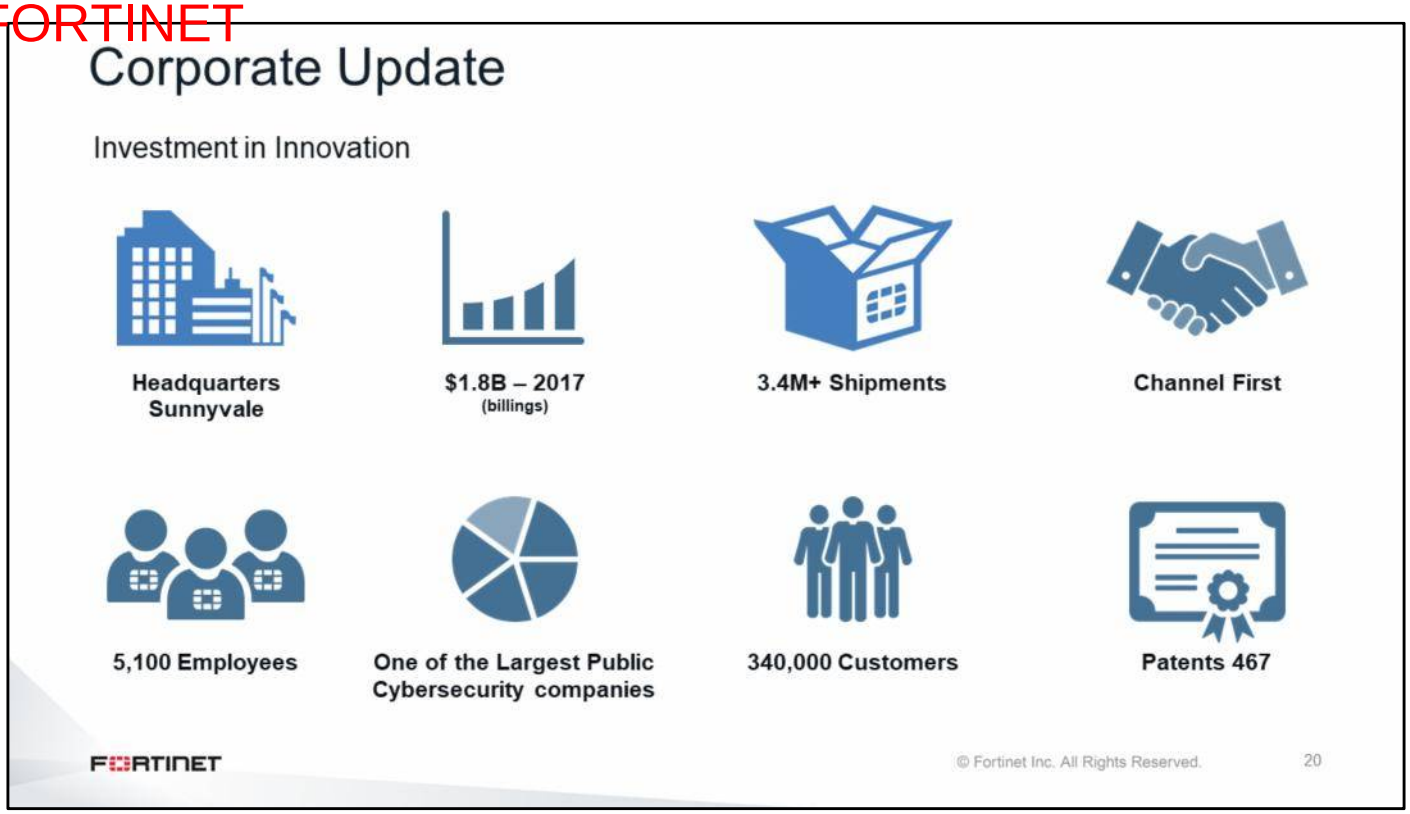
Organizations not only need to deploy security solutions that can function consistently across cloud ecosystems; they also need to be able to push automation into templates so security can be consistently applied simultaneously across every cloud provider's environment, especially when compensating for critical differences in native controls. This includes automating the entire data chain so security can dynamically adapt as workloads and information move within and between different cloud environments. The cloud enables these capabilities.



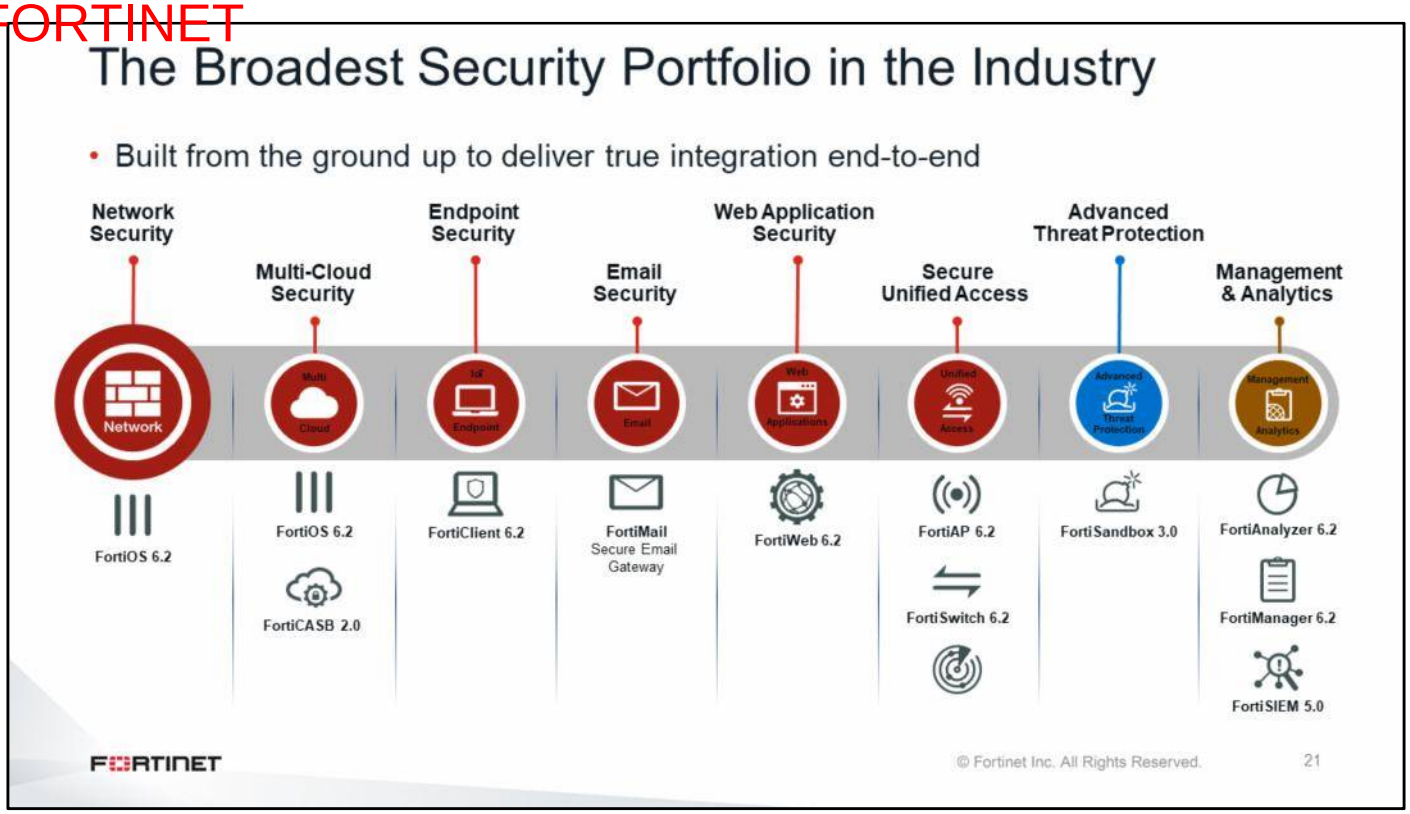
What many organizations may not realize when moving to a cloud environment, is to what extent they are responsible for securing their own cloud environment. Cloud providers secure the infrastructure, such as storage and compute resources shared by everyone, but securing data, content, and applications are all the responsibility of the cloud customer. And those security controls need to be built separately inside each cloud environment that has been adopted. If those security solutions aren't fully integrated and interoperable across multiple environments, then the number and variety of security tools that need to be implemented can compound, quickly overwhelming the resources available to manage them.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the Fortinet cloud security approach, you will be able to understand how Fortinet cloud security is important to your organization.



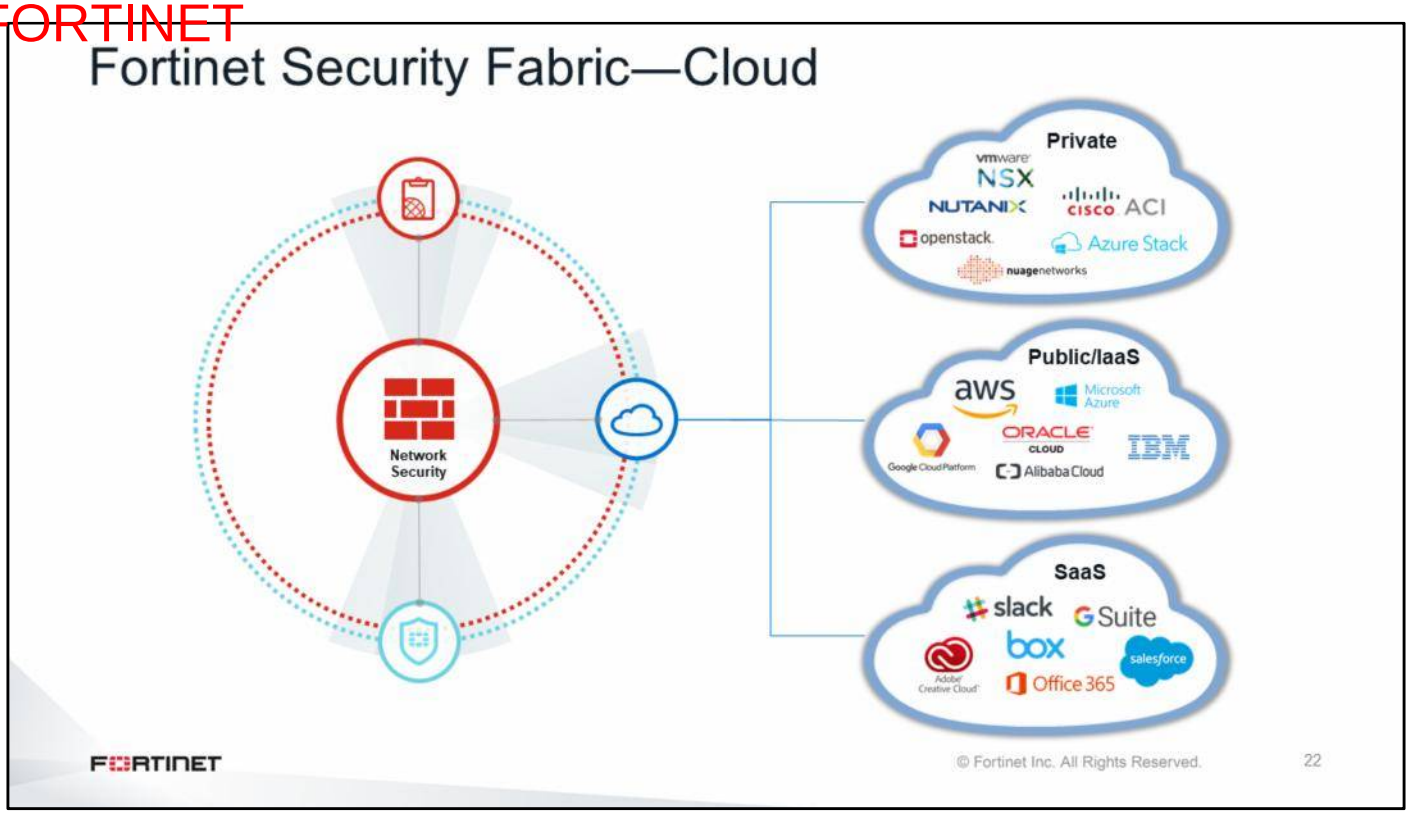
Why should you choose Fortinet as your cloud security vendor? As the global leader in multi-cloud security, Fortinet gives you the confidence to deploy any application in any cloud. The Fortinet cloud security solutions provide broad protection across the entire digital attack surface, in both on-premises and public clouds. Fortinet is headquartered in Sunnyvale, California, with offices around the globe. Fortinet is one of the largest public cybersecurity companies in the world.



As organizations embrace digital business strategies, their networks are evolving to include IoT, multi-cloud, and virtualized environments with complex workflows. Many enterprises are using multi-vendor products, tools, and applications—which leads to isolated security management methodologies.

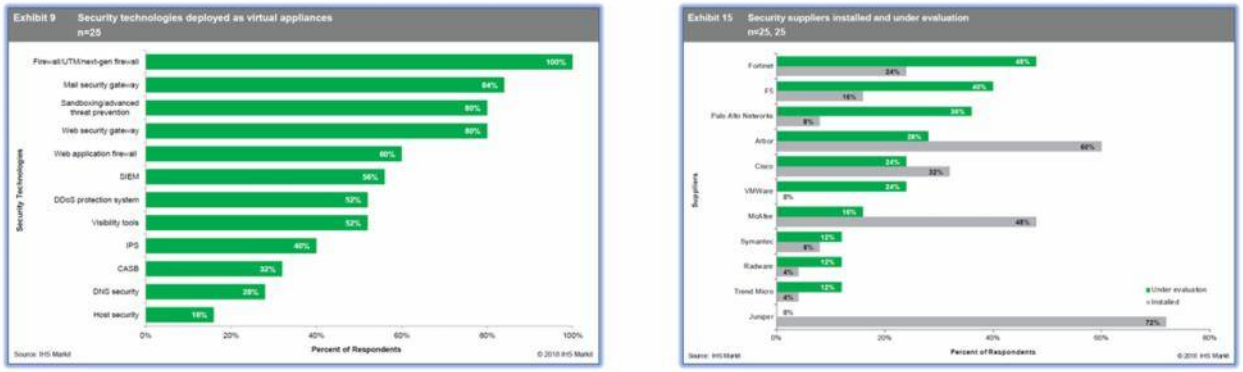
Lack of technology integrations across these complex customer environments make it increasingly difficult to gain visibility into what is happening across the expanded attack surface and identify cyber threats. Isolated security systems cannot share the intelligence needed to rapidly and automatically respond to sophisticated, fast-moving threats.

An integrated, open ecosystem of security solutions—woven together to scale and adapt as business demands change—enables companies to address the full spectrum of challenges across the expanding attack surface.



The Security Fabric is designed to extend deep into different cloud environments to ensure that policies are consistent and enforced across all distributed resources. Within the unified security architecture, virtual firewalls can be deployed across private, public, and hybrid clouds to establish north-south and east-west microsegmentation. The Security Fabric weaves cloud applications into the broader environment, governed by seamless, universal security and compliance policies, and managed using transparent visibility across the entire attack surface. Combining Fortinet Cloud Security with an existing enterprise firewall deployment, extends the same powerful security, as well as the same intelligence and dynamic risk mitigation, to applications located either in the cloud or on-premises.

Fortinet's Leadership Position



Cloud and DC Security Strategies and Vendor Leadership

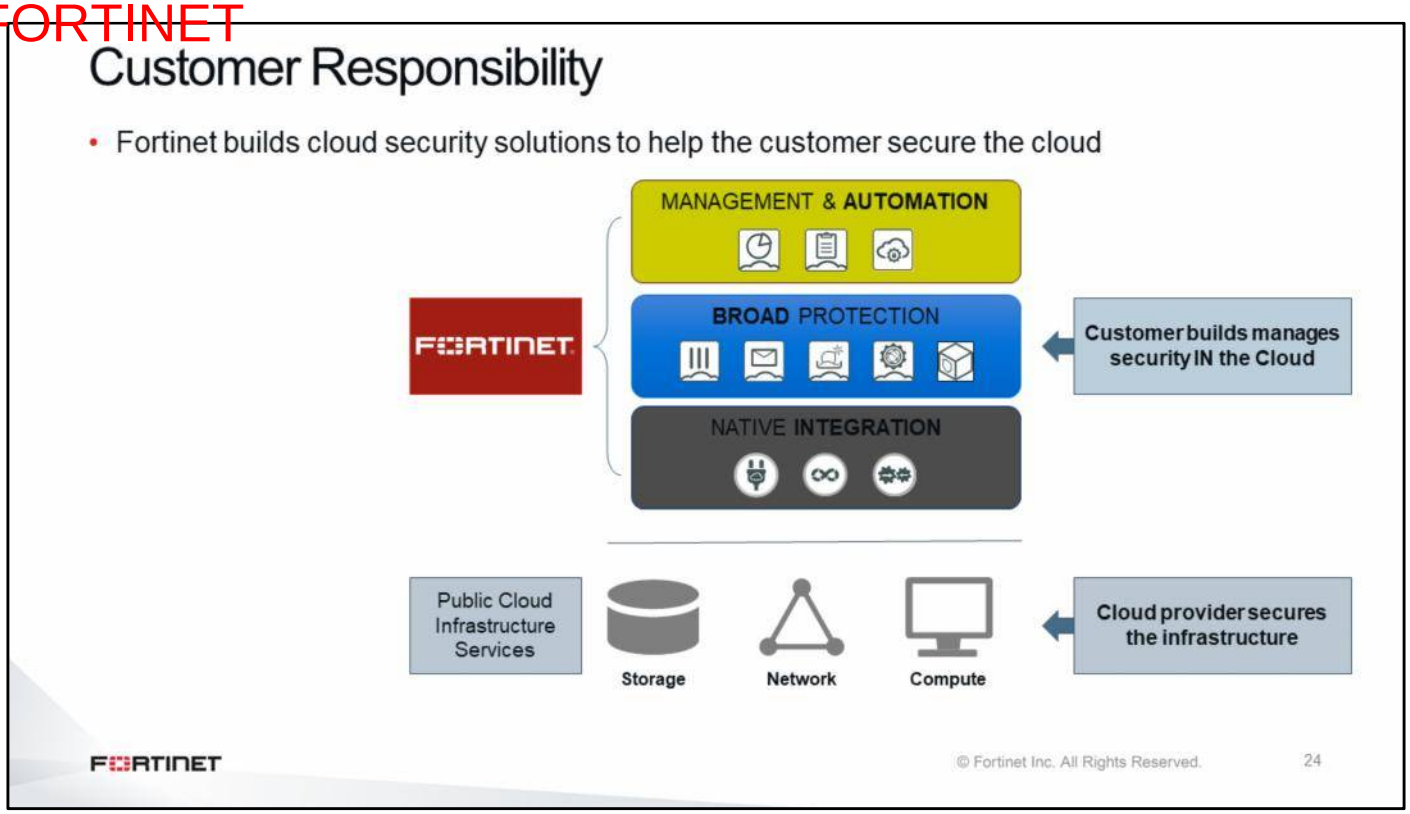
Service Provider Survey
23 July 2018

IHS Markit

FORTINET

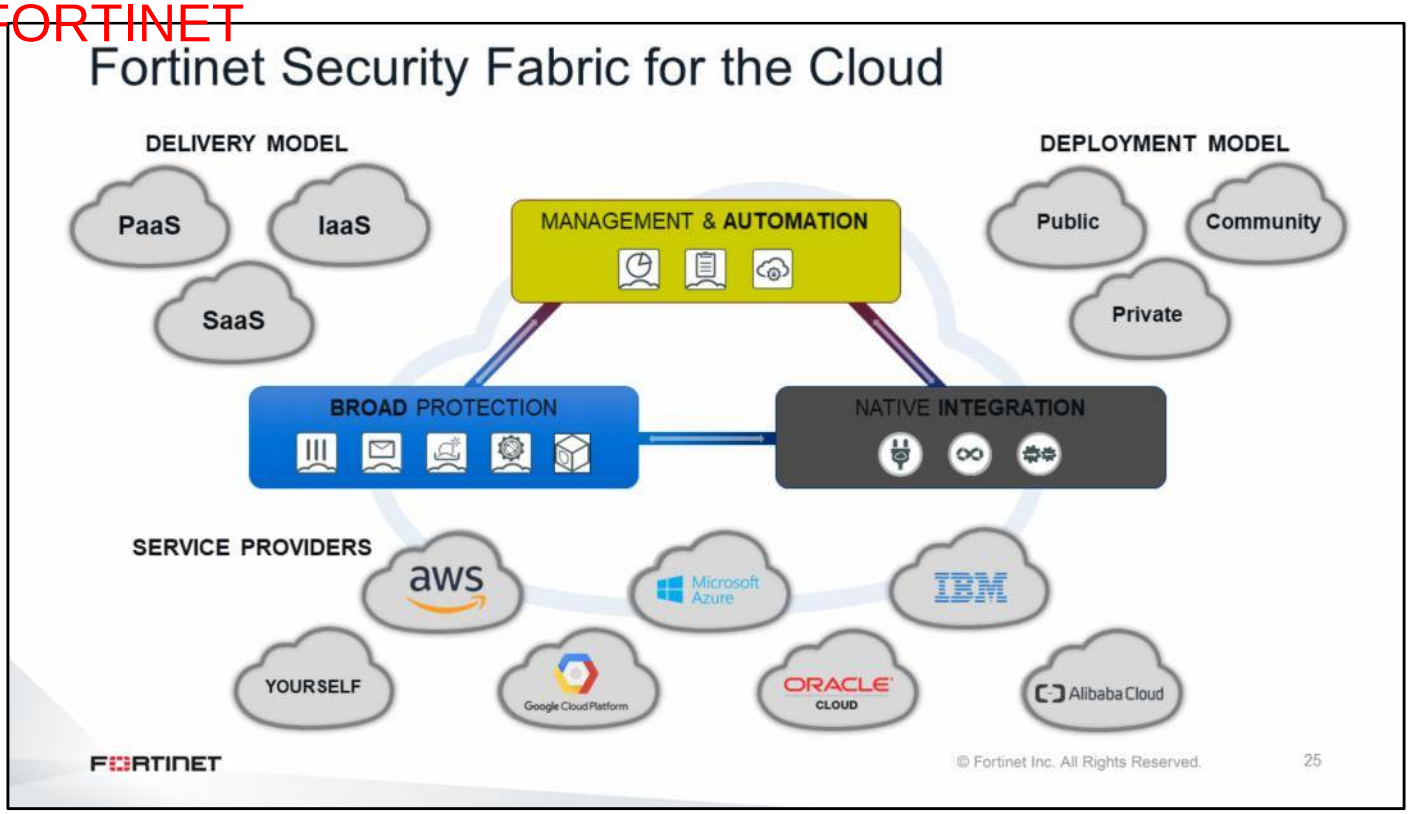
23

According to a recent IHS Markit survey, most of the respondents are using security technologies as virtual appliances, and Fortinet is on the top of the list.

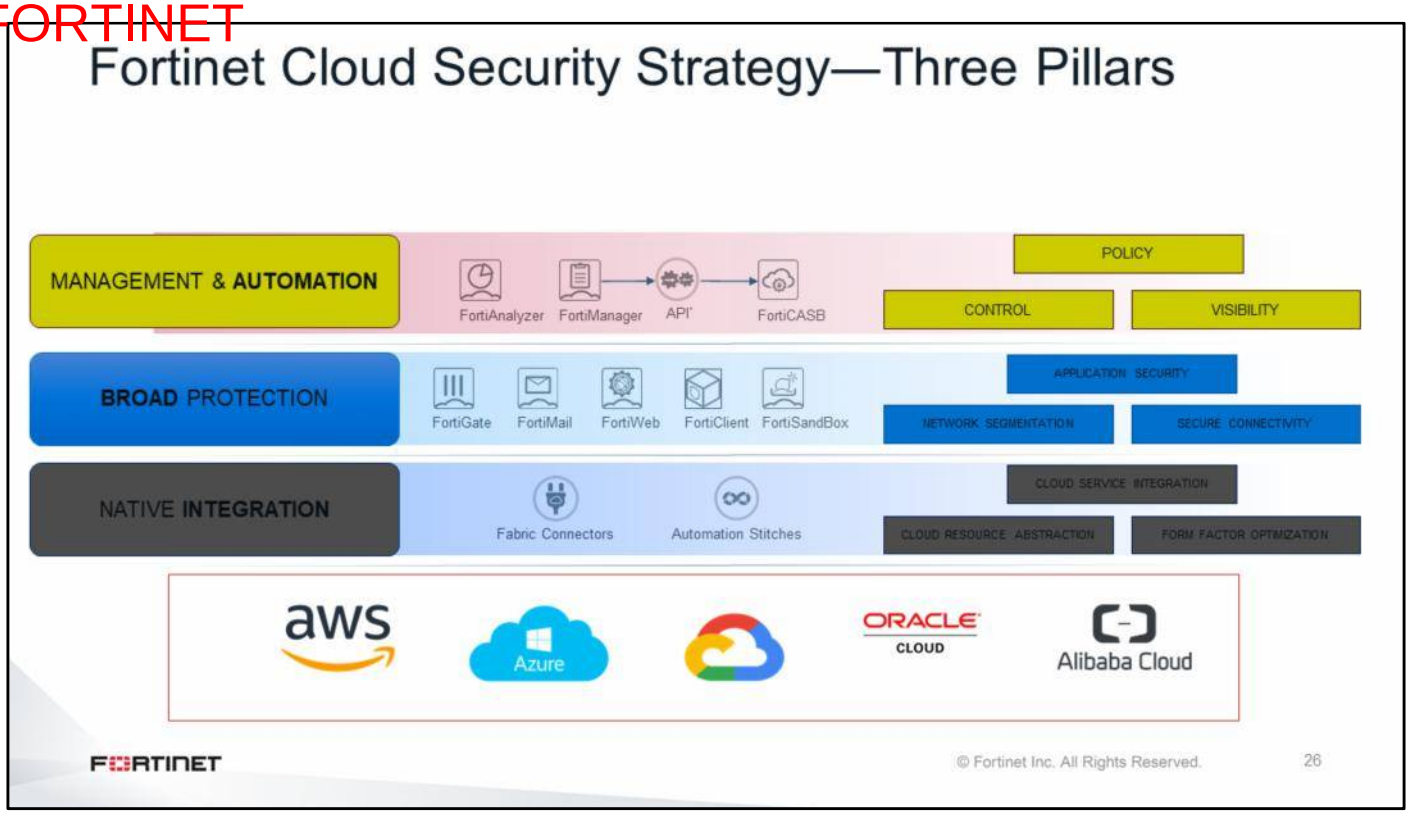


As you learned earlier, cloud providers secure the infrastructure, such as storage and compute resources shared by everyone, but securing data, content, and applications are all the responsibility of the cloud customer. So customer must build and manage security in the cloud. As the leader in multicloud security, Fortinet gives you the confidence to deploy any application in any cloud. Fortinet solutions provide broad protection across the entire digital attack surface, both on-premises and in public clouds. Native integration with each of the major cloud providers enables automated, centralized management across all clouds uniformly and seamlessly. This gives you unified visibility and control, as well as policy management that supports risk management and compliance requirements.

Fortinet cloud security addresses customer components, such as your data and applications, operating systems, access and identity management, encryption, APIs, and network traffic. This complements the public cloud provider's security features to provide complete and compliant protection.



A comprehensive solution built on native integration, broad protection, and security management and automation capabilities must work across different delivery models, deployment models, and service providers. Compliance cannot be achieved with a piecemeal approach across cloud silos and all security elements in general. Instead, organizations must embrace a security architecture that integrates transparency and controls within and across each cloud deployment. This integration must also extend to on-premises environments, resulting in single-pane-of-glass visibility and management. But with IT and security teams stretched when it comes to staff and resources, and an advanced threat landscape that is increasing in volume, velocity, and sophistication, automation of compliance and security workflows, and threat-intelligence protection, detection, and response is also critical. The Fortinet Security Fabric addresses these requirements by enabling broad coverage of the entire attack surface and integrates data aggregation and information sharing between each of the security elements. With data at its core, this is a requisite for a successful compliance strategy. The Security Fabric also automates security and compliance tasks that consume valuable staff time to manage manually—from data aggregation, to notifications, to tracking and reporting—and place organizations at greater risk due to slow threat intelligence sharing and management.

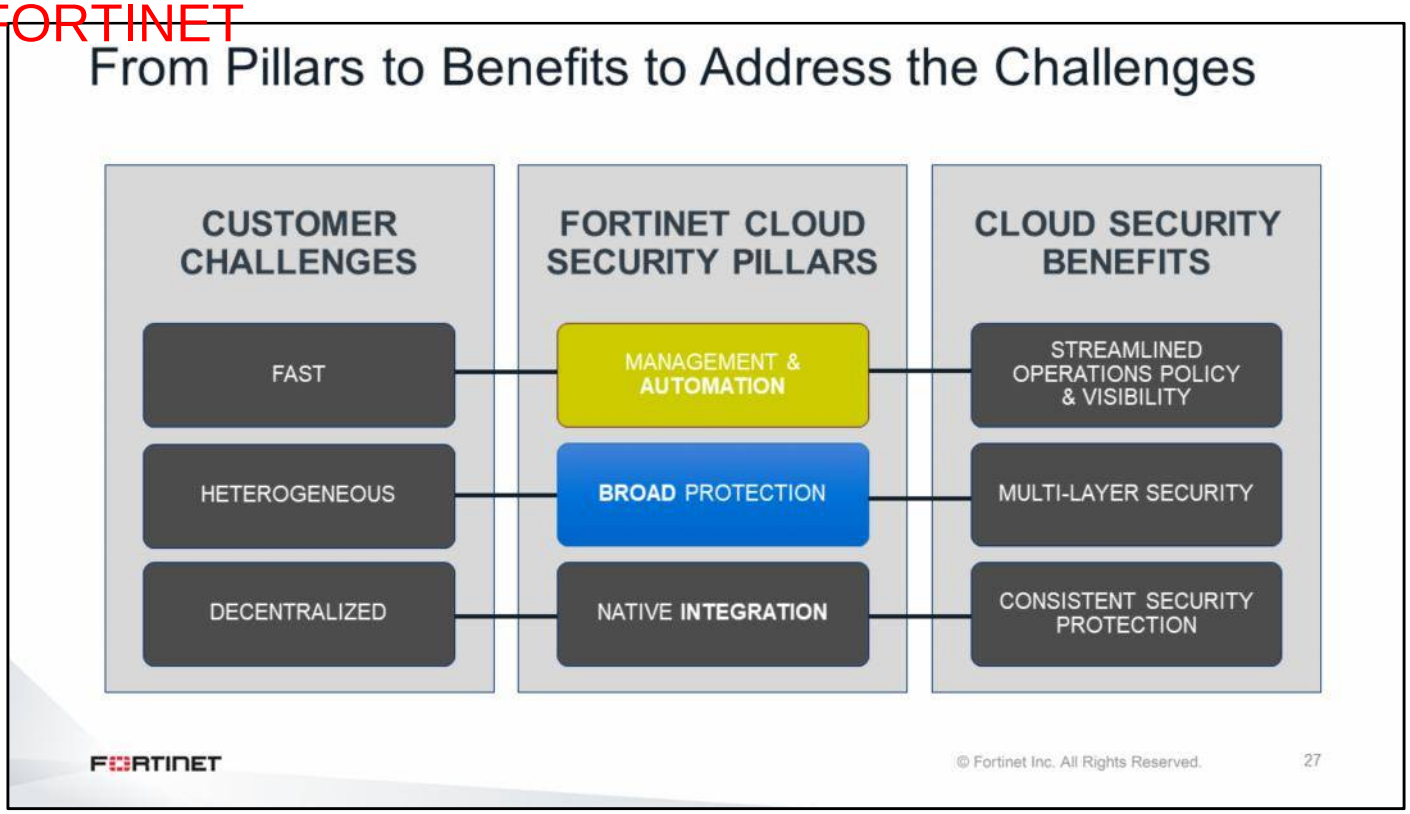


There are three pillars of multicloud security: native integration, broad protection, and management and automation.

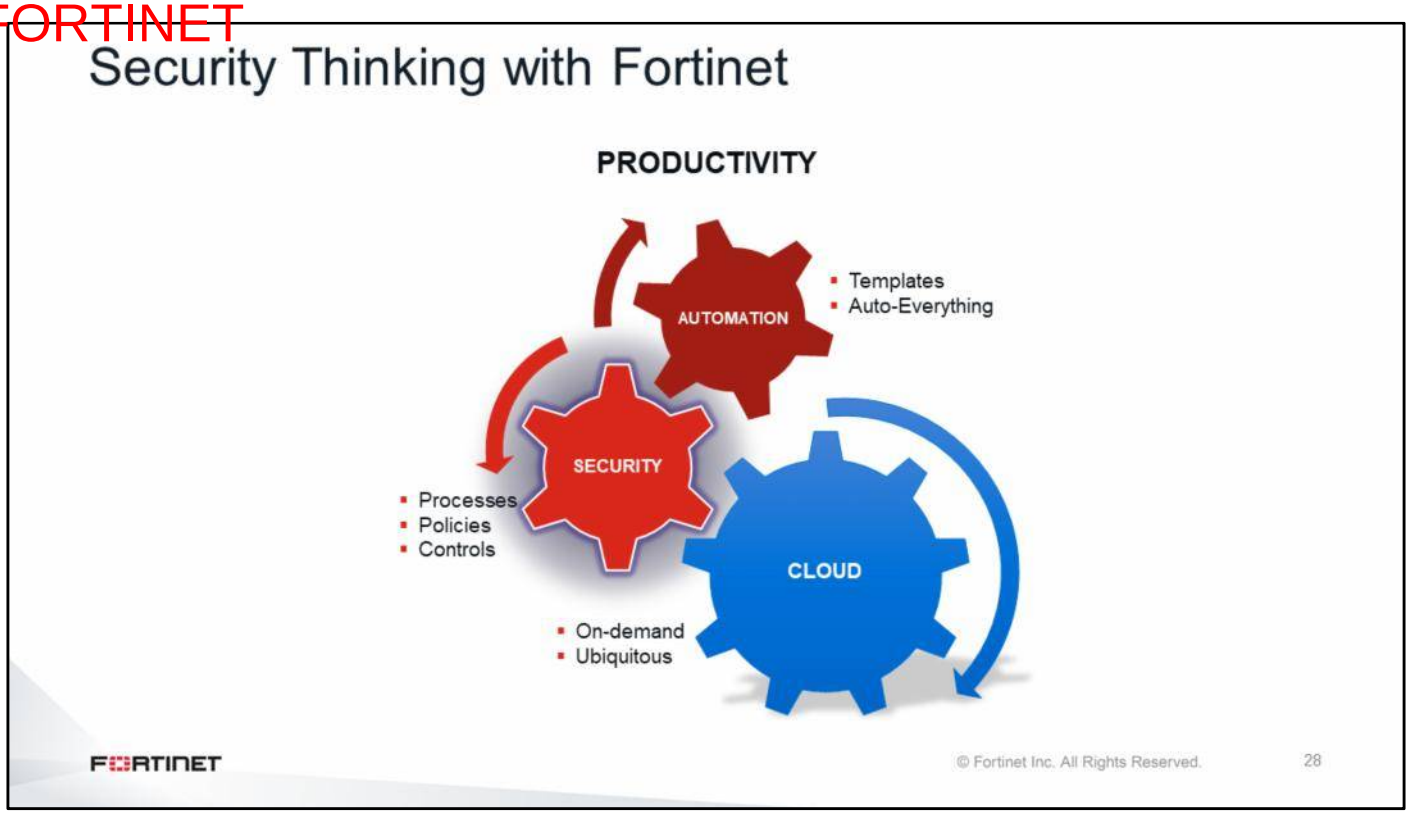
Unifying the management of an organization's network security infrastructure makes the visibility and control throughout the entire infrastructure practical and usable—from the data center to multiple clouds. Further, centralized management enables the automation of security life-cycle management processes as well as the application of consistent security policies across multiple clouds. The goal is to be able to manage the cloud and on-premises infrastructures similarly, by leveraging the same level of visibility and control. This enables organizations to fulfill desired enterprise risk management and regulatory compliance objectives. Effective security management and automation consists of four primary elements: visibility, control, policy, and compliance.

The rapid adoption of cloud infrastructure for business-critical applications requires a new form of coordinated and broad multilayer security solutions. This is especially true given the continued evolution in the advanced threat landscape and the complexity of distributed, multi cloud infrastructures. Organizations using multiple clouds should ensure that every part of the attack surface is protected against every kind of threat.

Native integration pertains to a security solution's ability to understand cloud-based information classification as part of overall security policy management and enforcement capabilities. It also leverages native cloud services as part of the security solution.

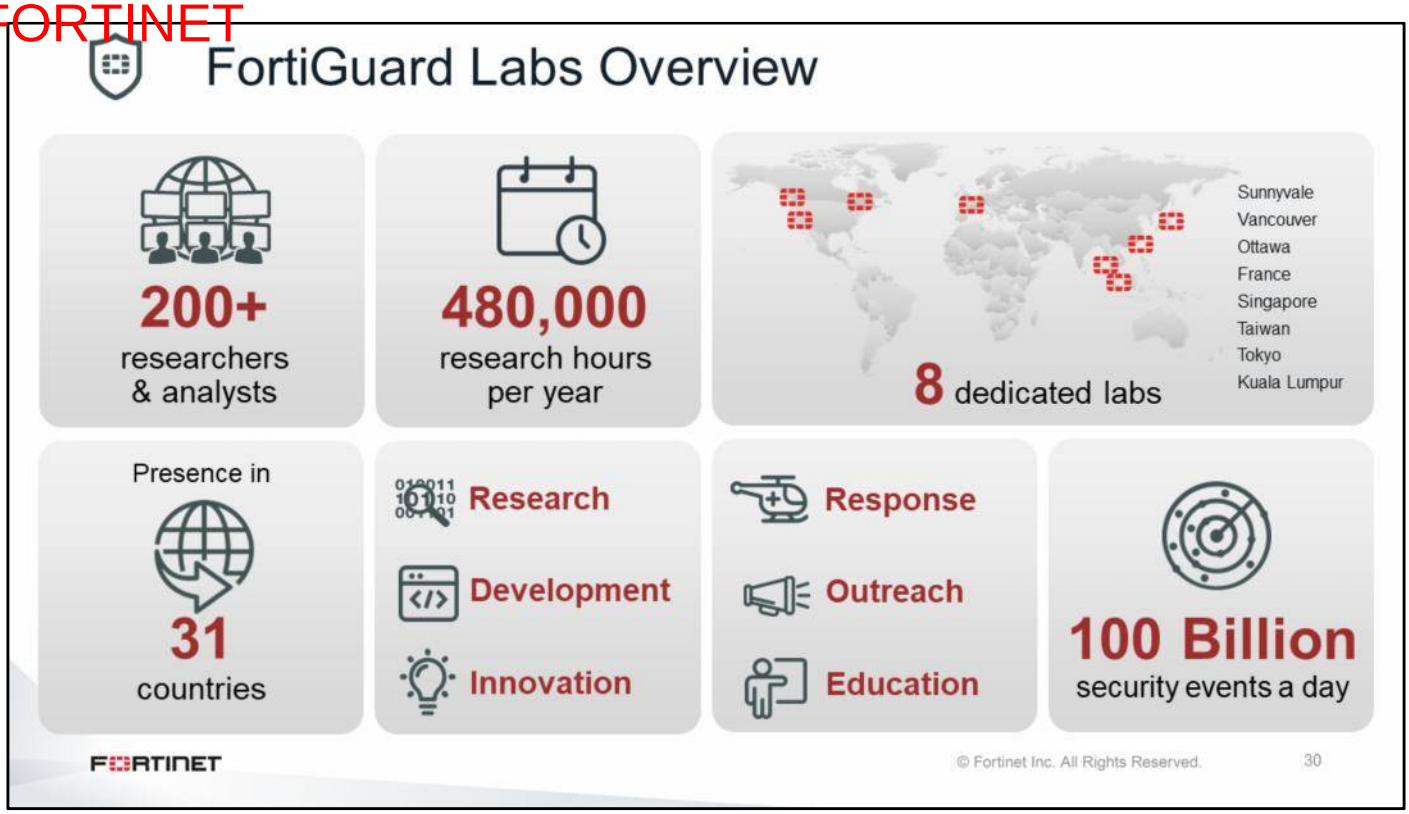


As shown on this slide, Fortinet cloud security pillars help customers to overcome challenges and get the best cloud security in the industry.

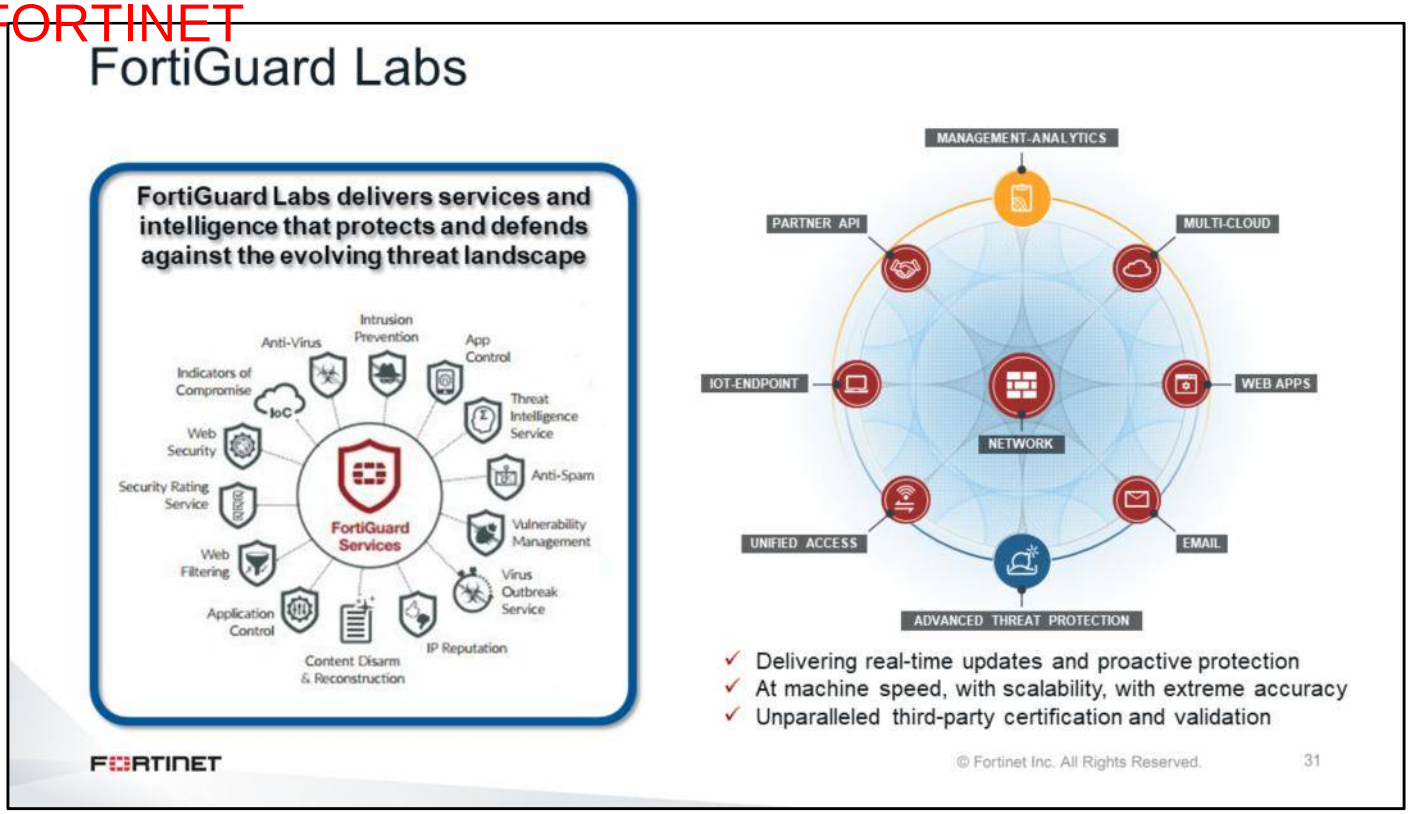


Organizations and branches need both high-performance networks and strong security. Fortinet's Network Security Solution is an integral component of the Fortinet Security Fabric. It enables complete visibility and provides automated threat protection across the entire attack surface. Powered by a single operating system, it delivers industry-leading security, unmatched performance, and reduces complexity. Automation templates help to deploy the security services on demand and quickly, into the cloud environment.

What sets FortiGuard apart is our advanced and proven analytics and artificial intelligence (AI) platform that is developed, innovated, and operated by FortiGuard Labs. Our platform ingests and analyzes 100 billion events every day, on average, to deliver over 1 billion security updates daily, to protect our customers against new, unknown threats across all Security Fabric deployments. Where other vendors measure results in days, weeks, or months, Fortinet can show impressive outcomes by the minute.

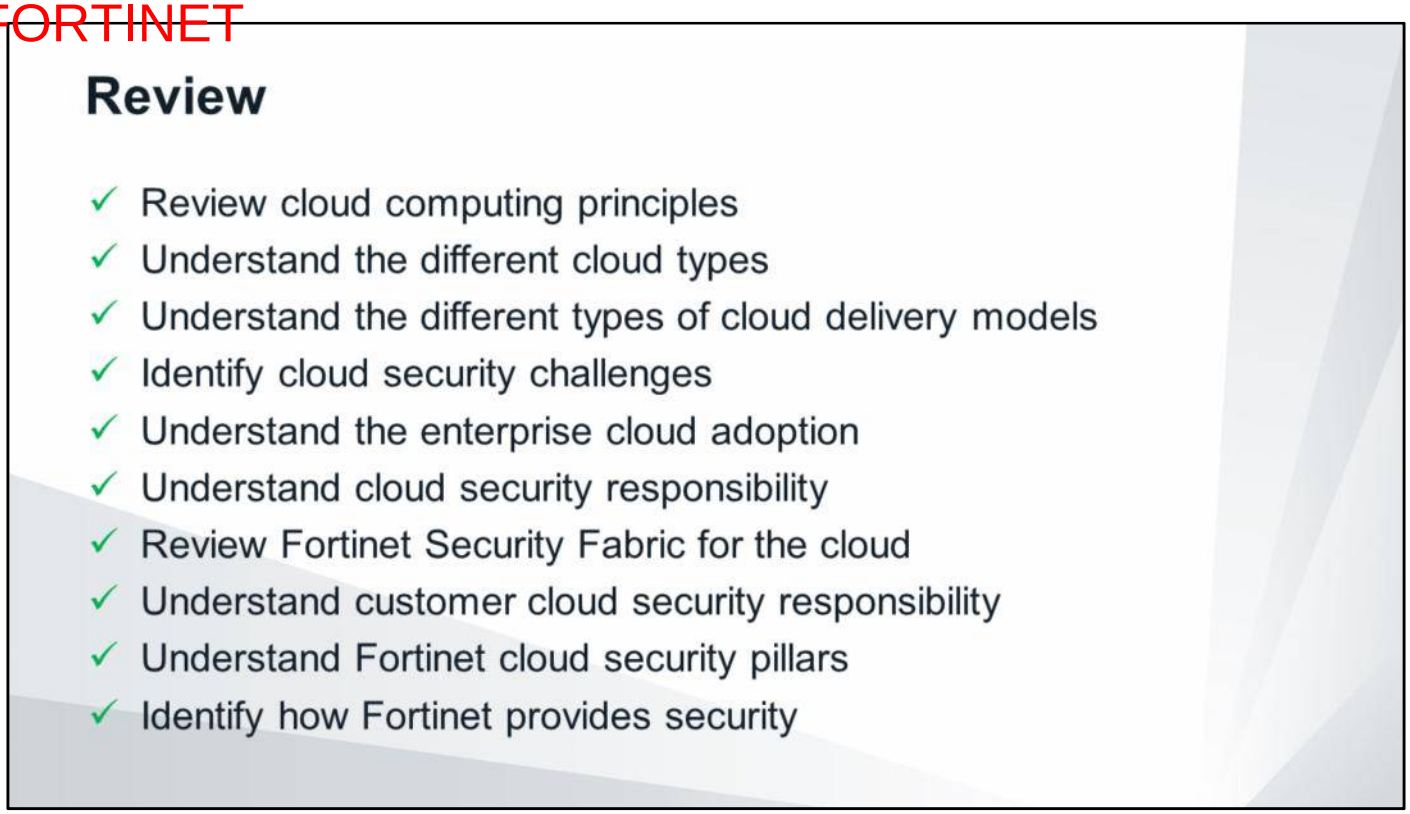


FortiGuard Labs boasts one of the largest security research and analyst teams in the industry, with over 215 expert researchers and analysts around the world. Our dedicated experts are always on the lookout for breaking threats and new techniques—studying every critical area of the threat landscape including malware, botnets, mobile, and zero-day vulnerabilities.



FortiGuard Labs, the threat intelligence and research organization at Fortinet, develops, innovates, and maintains one of the most recognized and seasoned AI and machine learning systems in the industry. We use this to deliver proven, unparalleled protection, visibility, and business continuity across the Fortinet Security Fabric, protecting our customers against the wide range of ever-changing and sophisticated threats.

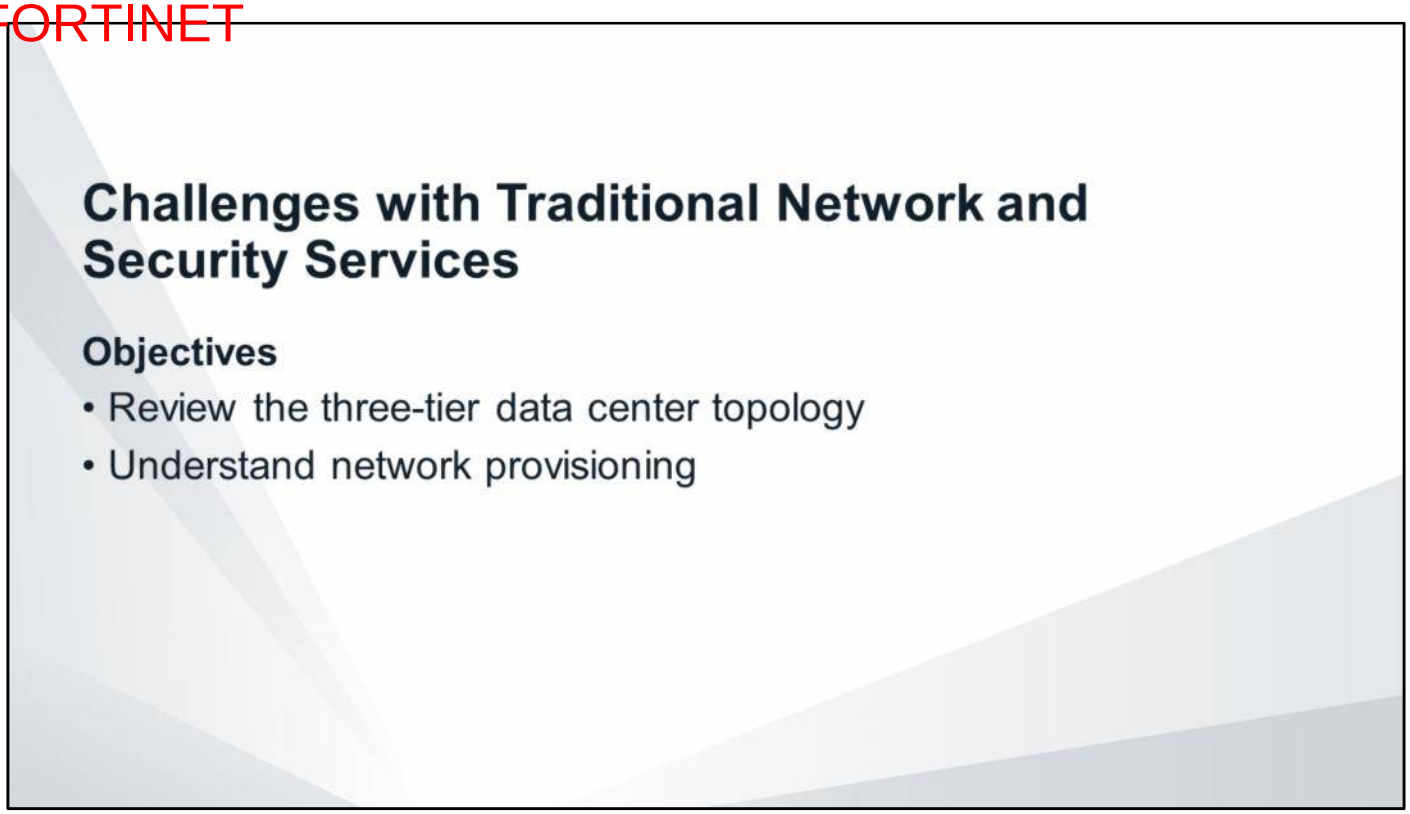
The Fortinet Security Fabric delivers transparent visibility, policies, and controls across the entirety of the cloud attack surface, down to the virtual traffic layer. It seamlessly scales cloud security by including a comprehensive portfolio of security solutions including email, application, endpoint, access security, and more. You can secure your entire network, including your multi-cloud environment, with the Fortinet Security Fabric.



This slide shows the objectives that you covered in this lesson.

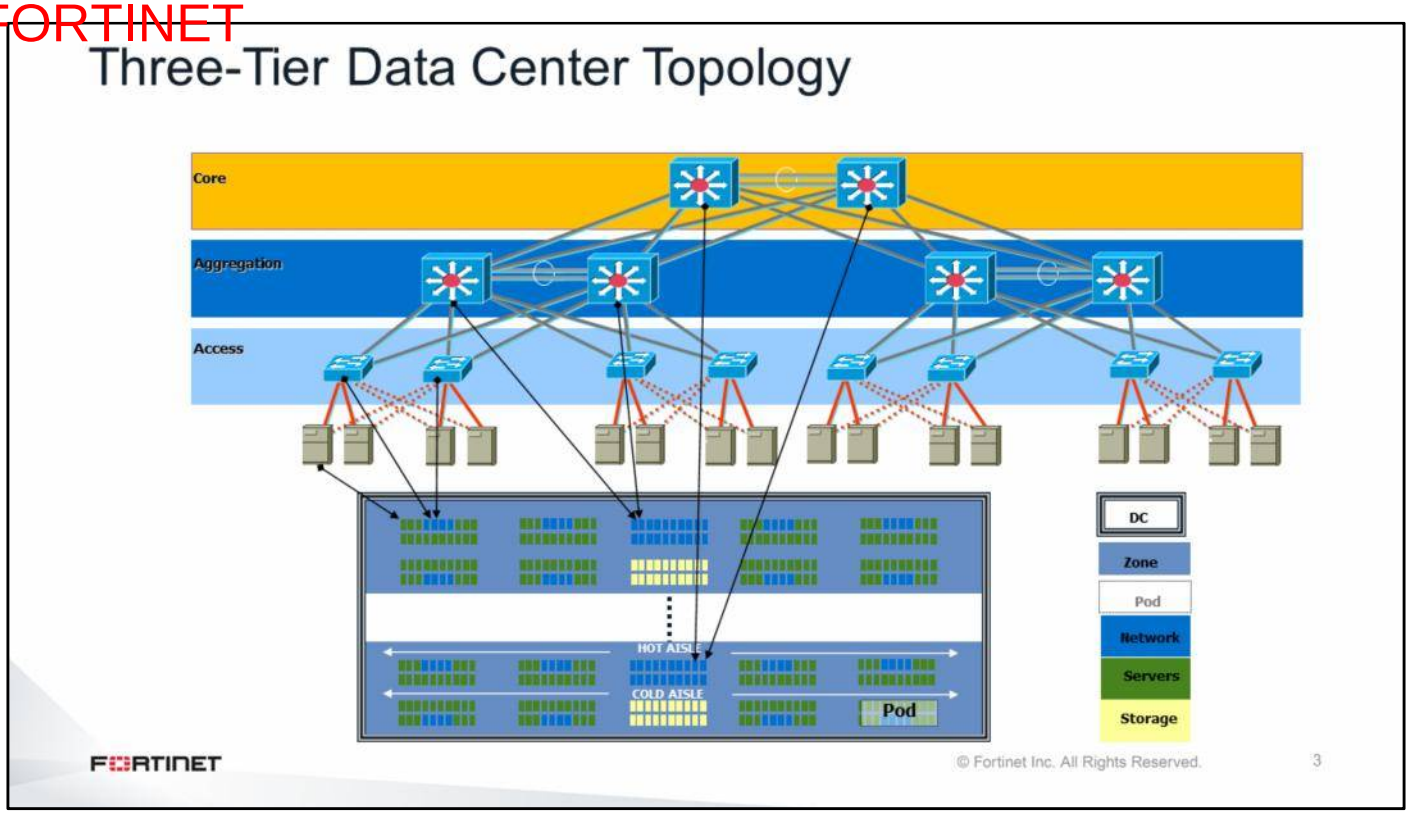
By mastering the objectives covered in this lesson, you learned about east-west traffic, some cloud security challenges, and the Fortinet cloud security approach.

In this lesson, you will learn about private cloud security concepts, virtualization, and how to protect the VMware software-defined data center (SDDC) using FortiGate-VMX.



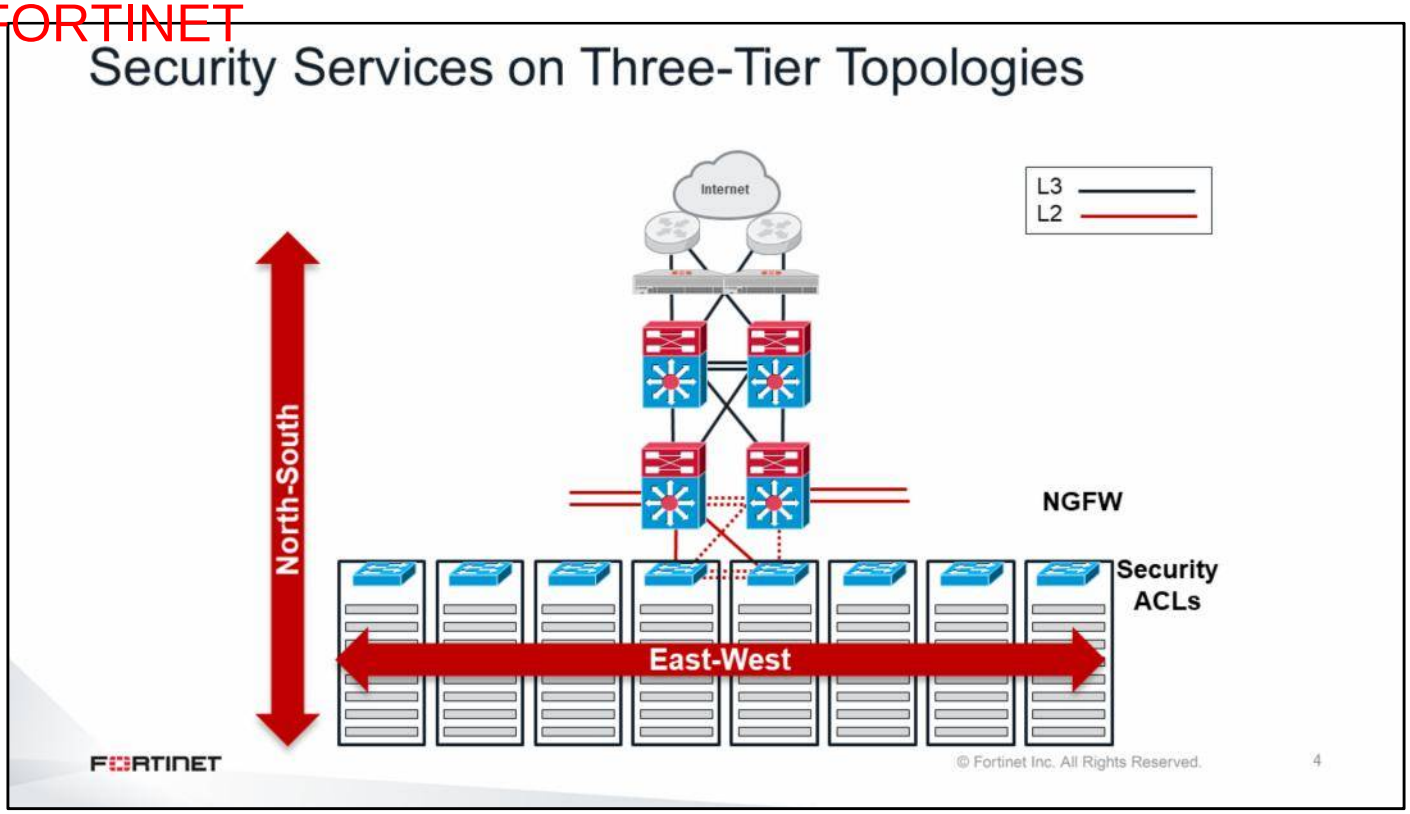
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in the three-tier data center topology, and understanding network provisioning, you will be able to understand how it applies to your network.

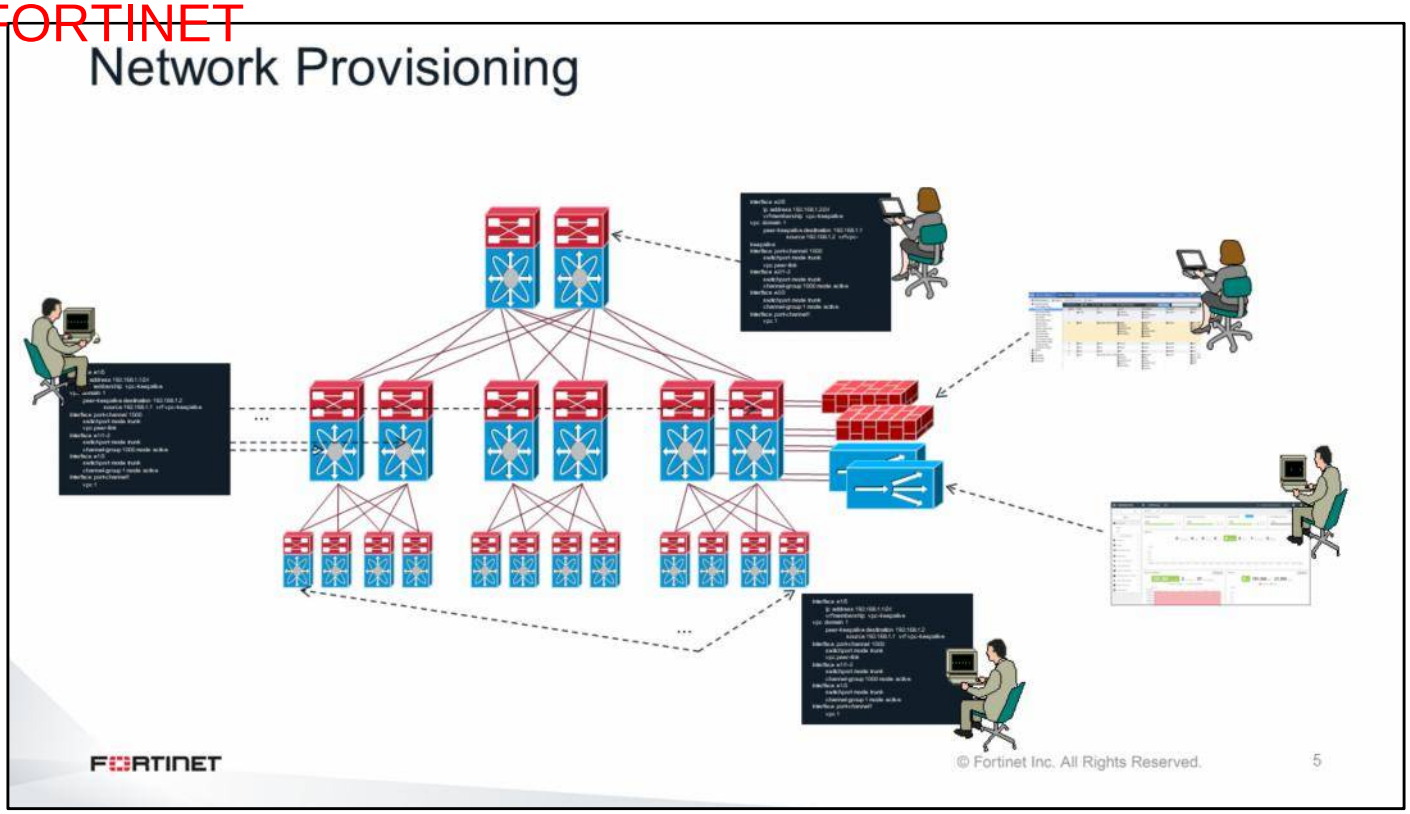


A data center that is traditionally designed based on hardware, consists of a collection of servers and network hardware devices that are arranged in a three-tier topology. The three-tier topology is divided into core, aggregation, and access layers. All resources sit below the access layer. For example, servers, APs, IoT devices, and so on.

Core: This layer includes the main switches and routers that are responsible for connecting and routing the entire network. This is usually referred to as the backbone.
Aggregation: This layer is responsible for providing 10 GB connectivity for the access layer with a large port density.
Access: This layer is where the servers and other network devices connect, in order to have access to the network.



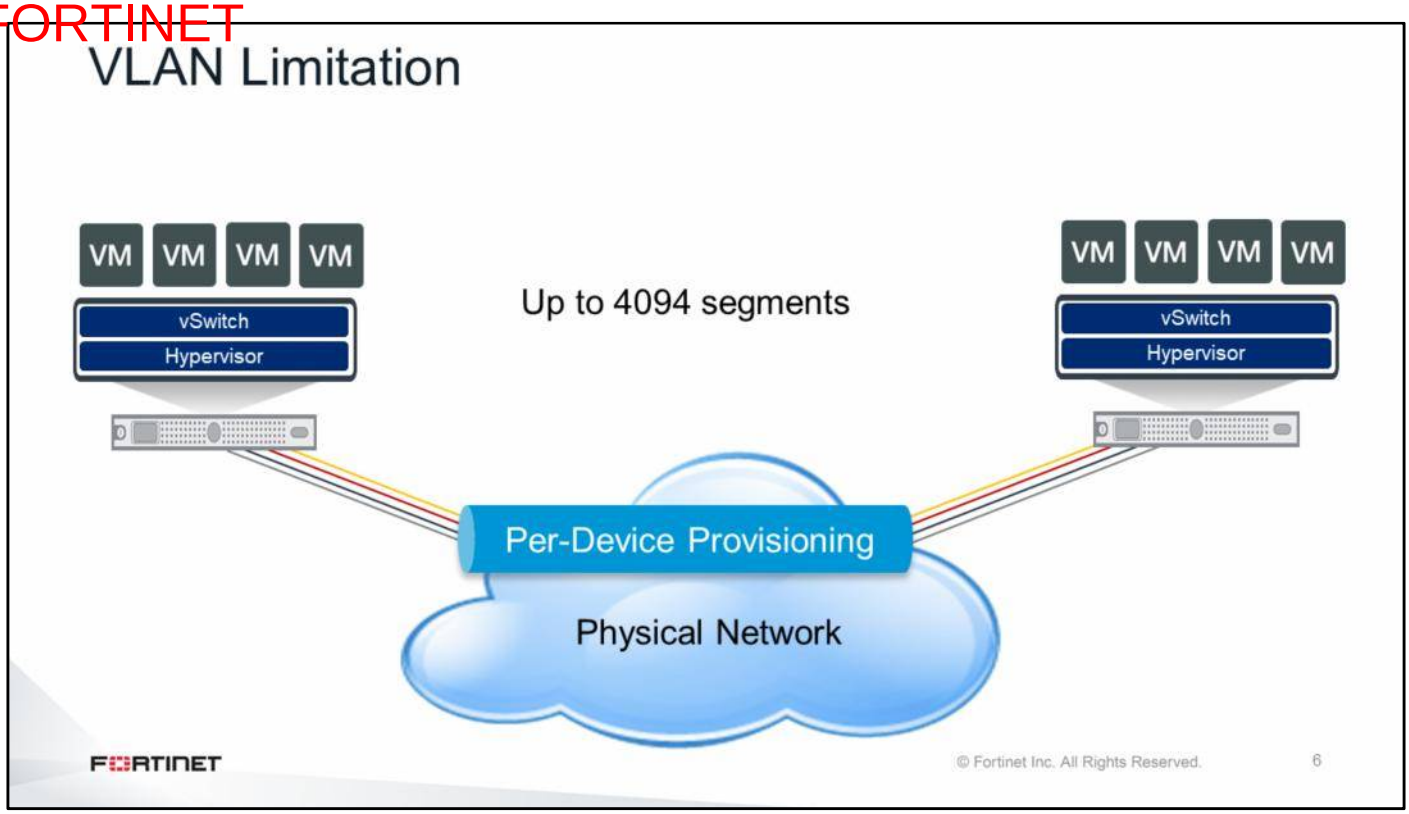
In a hardware-designed data center, there are two types of traffic: north-south and east-west. North-south refers to the traffic that leaves the perimeter, usually though the use of edge gateways. East-west refers to the traffic between racks that usually stays within the access and aggregation layers. The biggest challenge within hardware-based data centers, is bringing security as close as possible to the access layer. The first possible solution is to deploy network firewalls and IPS/IDS on the aggregation layer. This approach provides north-south security, but will fail to fully provide east-west security because traffic within the same rack/VLAN will not reach the security layer. The alternative to in-depth, east-west security would be implementing ACLs on all access switches, to perform per-port filtering. However, this is a manual process and ACLs are quite problematic, due to their stateless nature. So, providing security services to the physical network is quite complex.



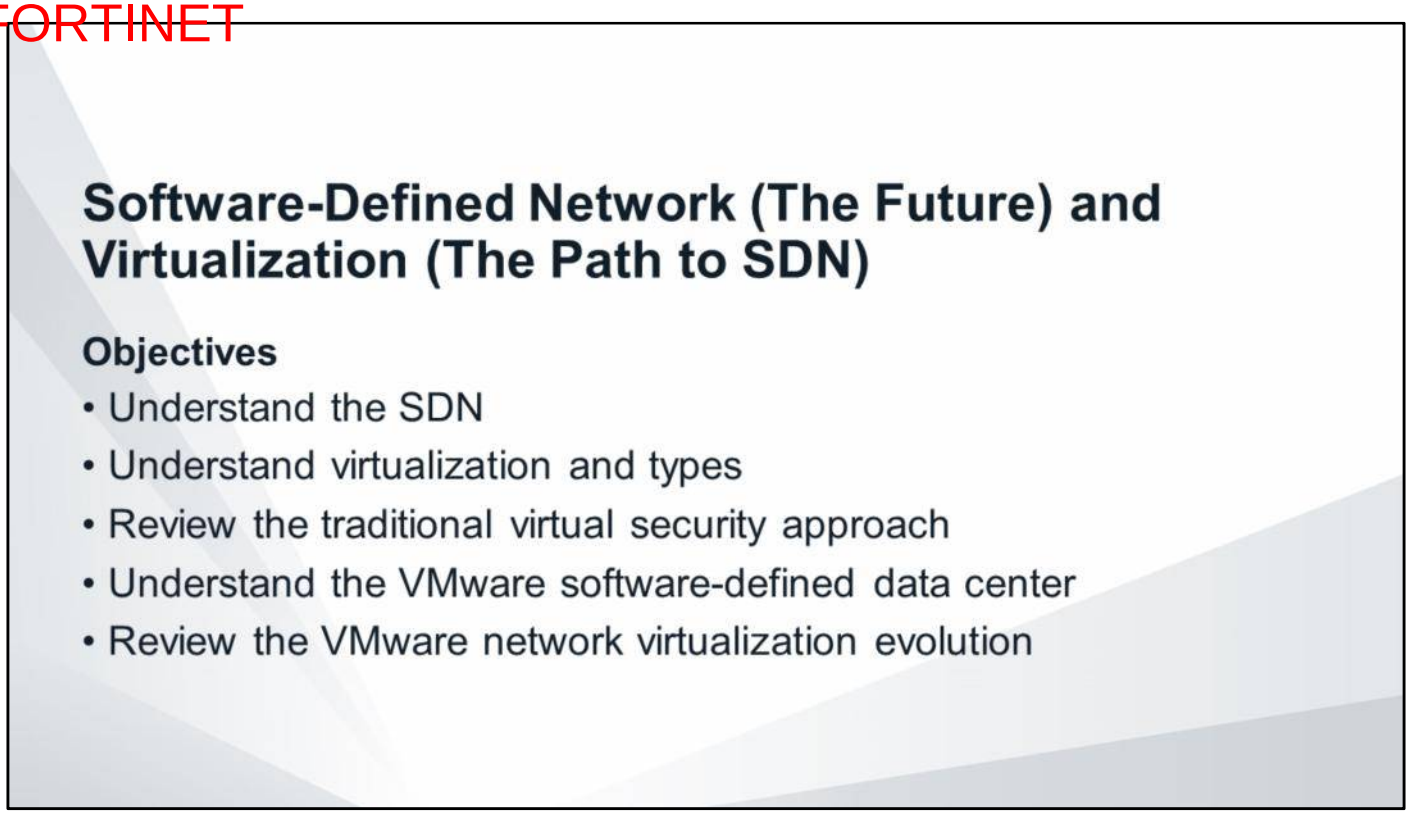
Another challenge is network provisioning. For example, as a service provider team who provides IT solutions for customers, your team is tasked to create a network environment for a new customer. First, your team needs to create all necessary VLANs, routes, and any other network definitions. The usual process is to create all the tasks manually on a per-switch basis, using CLI scripts installed over SSH or a terminal. What if you have hundreds of switches in your network? Configuring hundred of switches manually would be an enormous task. It requires more resources, time, money, and introduces complexity.

Now that the network layer is configured, your team needs to configure the other layers, such as security, load balancing, servers, backups, and so on. Finally, after 15 days, your team finishes the work and the new customer comes on board. How would you keep up this process as your organization expands?

Now, think about the same tasks done through a public cloud vendor. For example, in Amazon AWS, the same environment provisioning can be done in matter of minutes. If a new customer comes on board, a simple template can be used, without creating all the tasks from scratch. So, it is obvious that the customer will not wait 15 days for all the configuration and troubleshooting to be done by the traditional service provider's IT department. Instead, the customer will choose Amazon AWS, over the traditional three-tier data center approach.

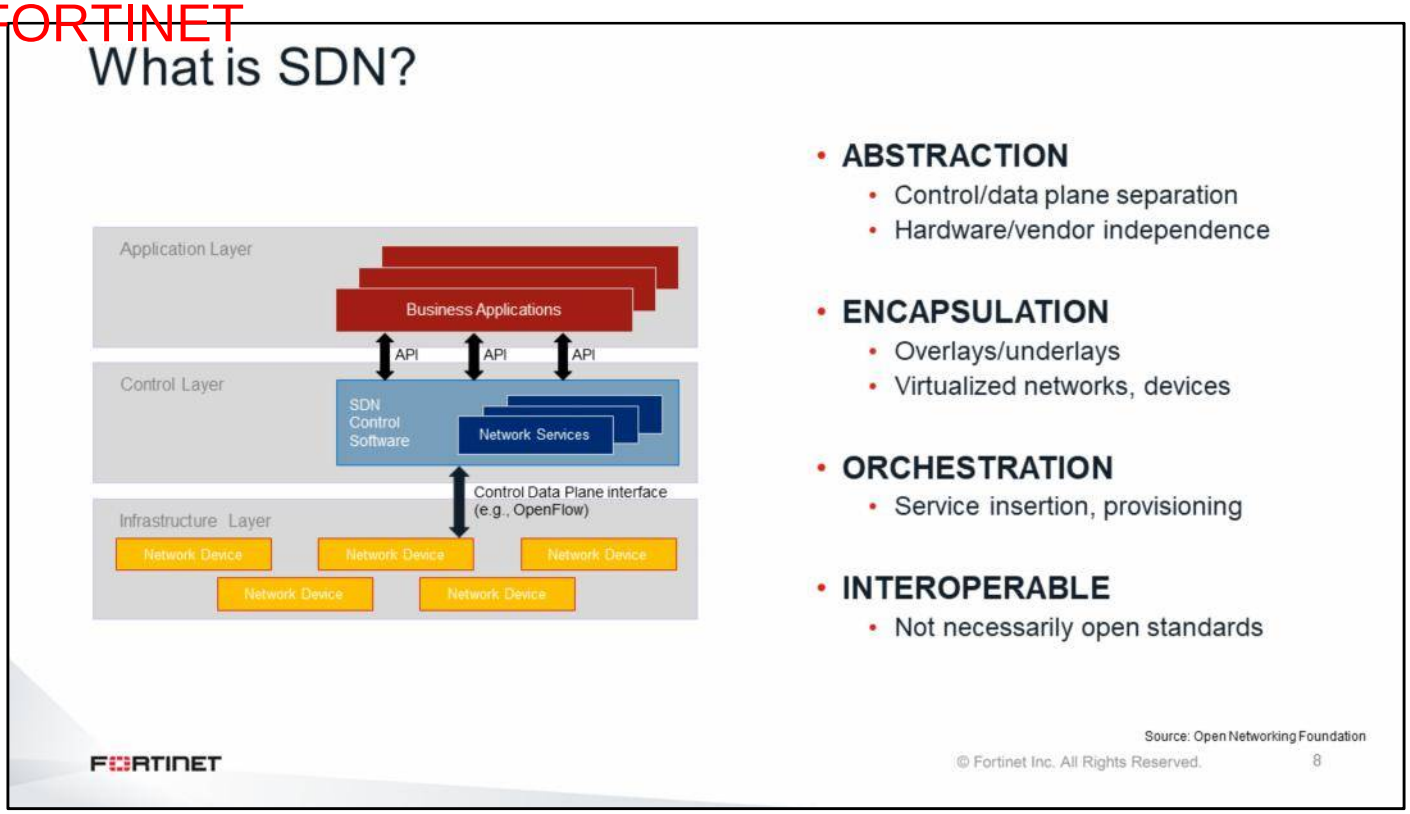


Another challenge in the traditional three-tier topology, is the VLAN limitation. Your team must also consider the VLAN limitation, which can scale up to only 4094 segments. As a service provider, you do not need any limitations. How many customers can your data center host, using only 4094 VLANs? At the same time, your team must provision on a per-device basis. Imagine that Amazon AWS relies on VLANs to segregate customers. There are millions of customers, and using VLANs in cloud computing is not scalable.



After completing this section, you should be able to achieve the objectives shown on this slide.

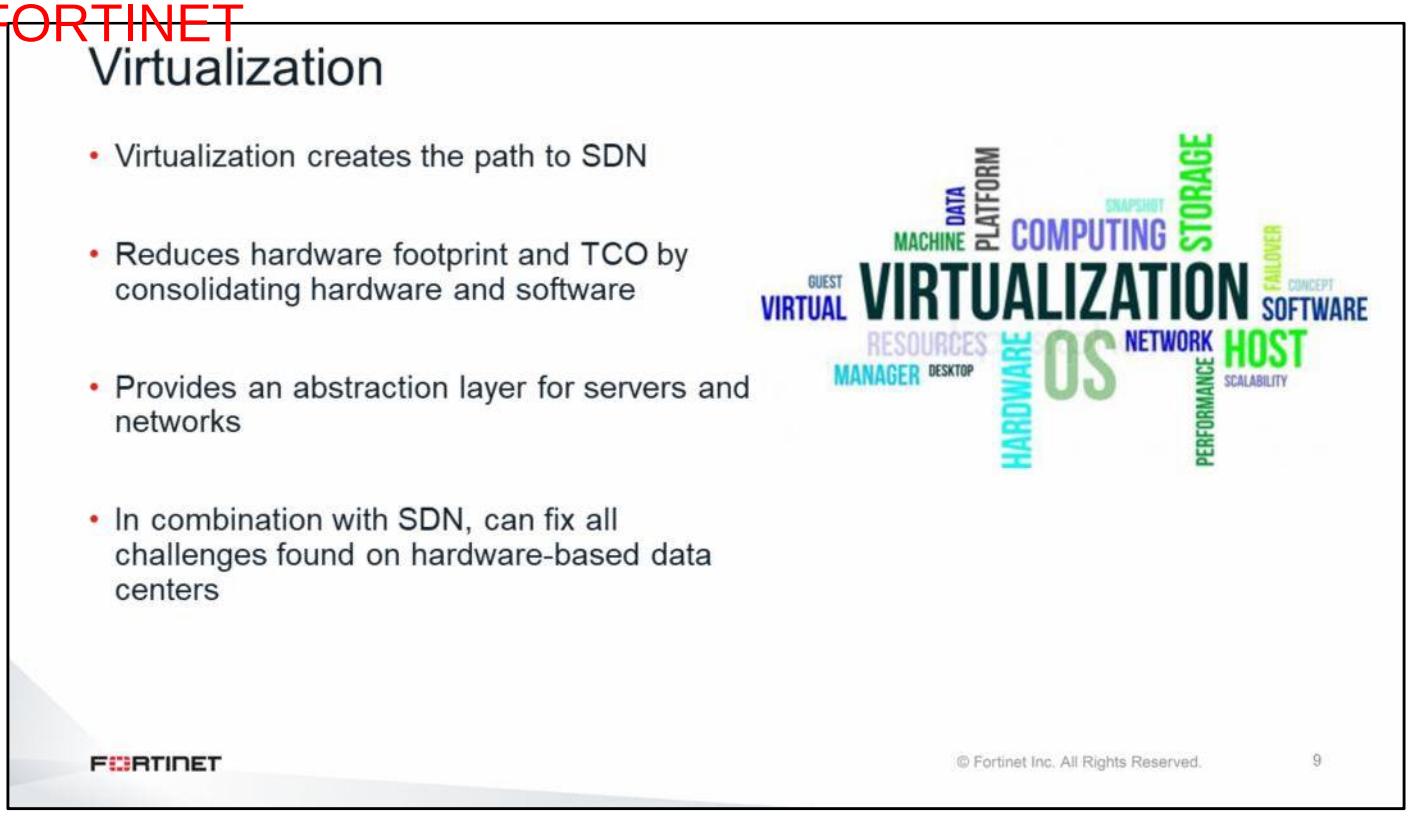
By demonstrating competence in understanding the concept of SDN and virtualization, you will be able to use these technologies in your network successfully.



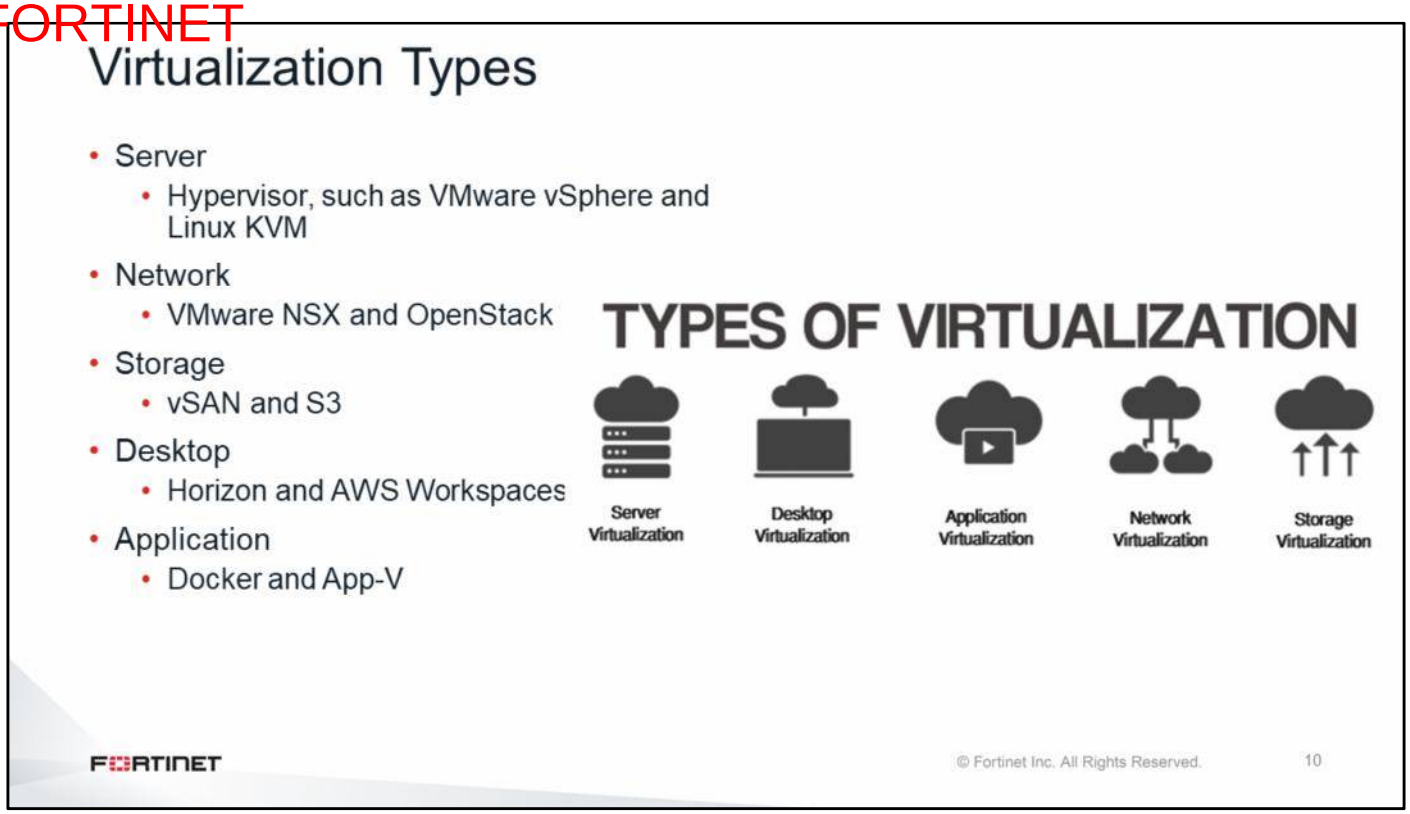
A software-defined network (SDN) is a network made up of software, and it is one of the alternatives for addressing the issues on a hardware-based network. The concept of SDN is simple: to decouple control and forwarding (data) plane functions, which were always embedded on a single device, for example, a hardware switch. SDN enables network control to become directly programmable, and the underlying infrastructure to be abstracted for applications and network services.

This simple idea provides endless possibilities, such as:

- **Vendor neutrality**: Now, network administrators are free to use a mix of devices, since management resides outside the network device and can interoperate with any vendor. Usually, this is achievable by using an open standard, such as OpenFlow, but it is not necessarily true.
- **Central management**: Because the network intelligence now resides on a software-based SDN controller, administrators have a global view of the entire network and can easily expose all functions as if they were a single, logical switch.
- **Agility**: By abstracting control from forwarding (data), administrators can now quickly and dynamically adjust network traffic flows to accommodate changes.
- **Programmatical configuration**: SDN lets network managers configure, manage, secure, and optimize network resources very quickly using dynamic, automated SDN programs, which they can write themselves, because the programs do not depend on proprietary software.



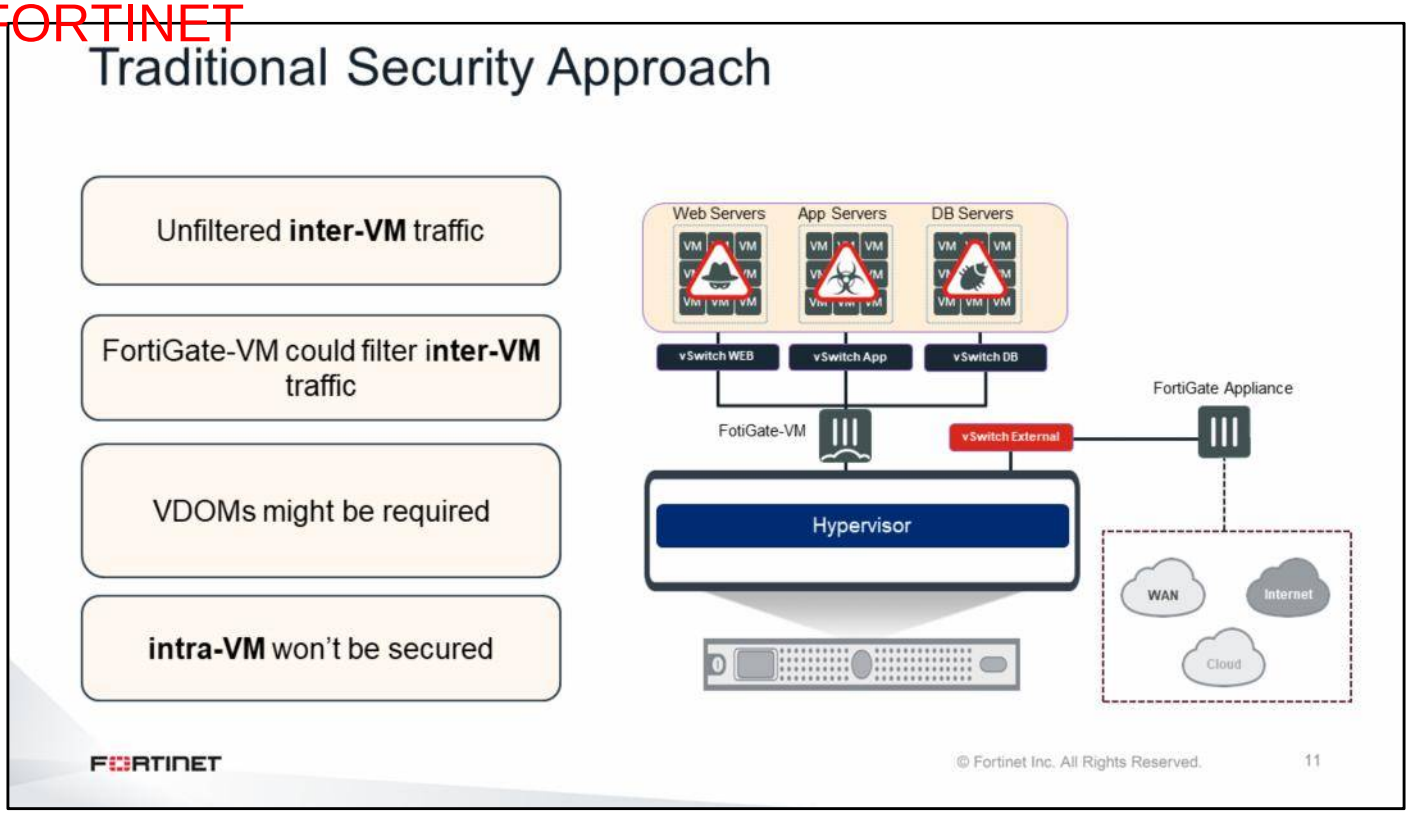
Virtualization is the path to SDN, because it consolidates the use of resources, reducing the hardware footprint, increasing TCO, and providing the abstraction layer that will allow servers and networks to be virtualized. Through the combination of SDN and virtualization, it is possible to solve all challenges found when implementing a hardware-based data center. So this is the actual solution for providing security for east-west traffic inspection.



There are two main types of virtualization, when it comes to a data center:

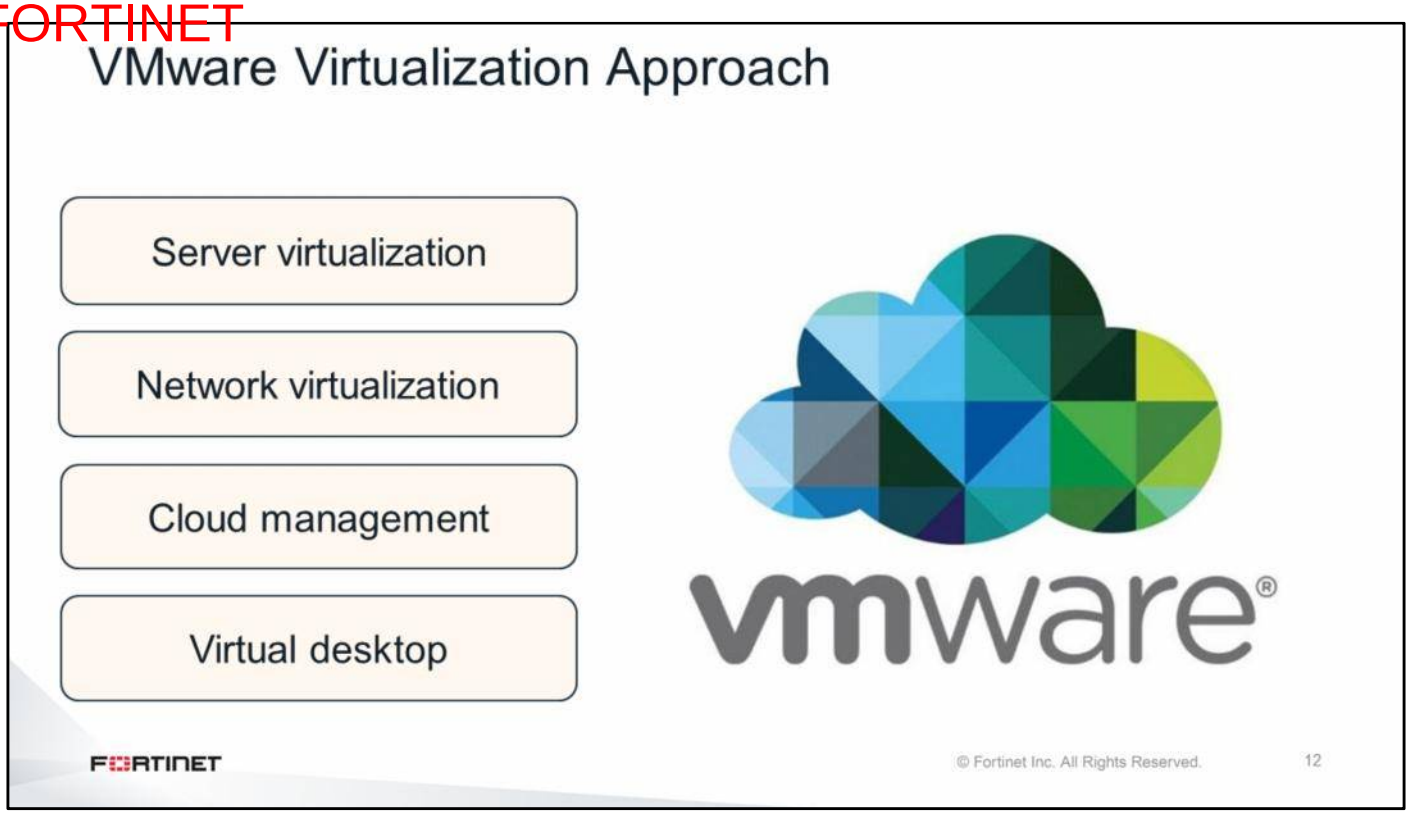
- **Server virtualization**: This is the most common and well-known type of virtualization. It virtualizes many operating systems into a single hardware appliance, using a hypervisor, such as VMware vSphere and Linux KVM.
- **Network virtualization**: This is a new method of virtualization and people are still trying to get used to it. Networks that once were made up of devices, such as routers, switches, and cables, can now be virtually created inside the hypervisor, without the need for those physical devices. For example, VMware NSX, and OpenStack.

Other types of virtualizations are storage, desktop, and application.



This is the traditional hypervisor architecture. So what are the challenges for this architecture?

- Traffic within the VM host is usually not filtered, unless it gets routed somewhere else.
- In order to secure inter-VM traffic, a FortiGate-VM can be deployed in Layer 2/Layer 3 mode.
- It requires the use of VDOMs and VDOM-links, which makes the solution too complex to manage.
- Intra-VM traffic cannot be secured because traffic does not leave the vSwitch.

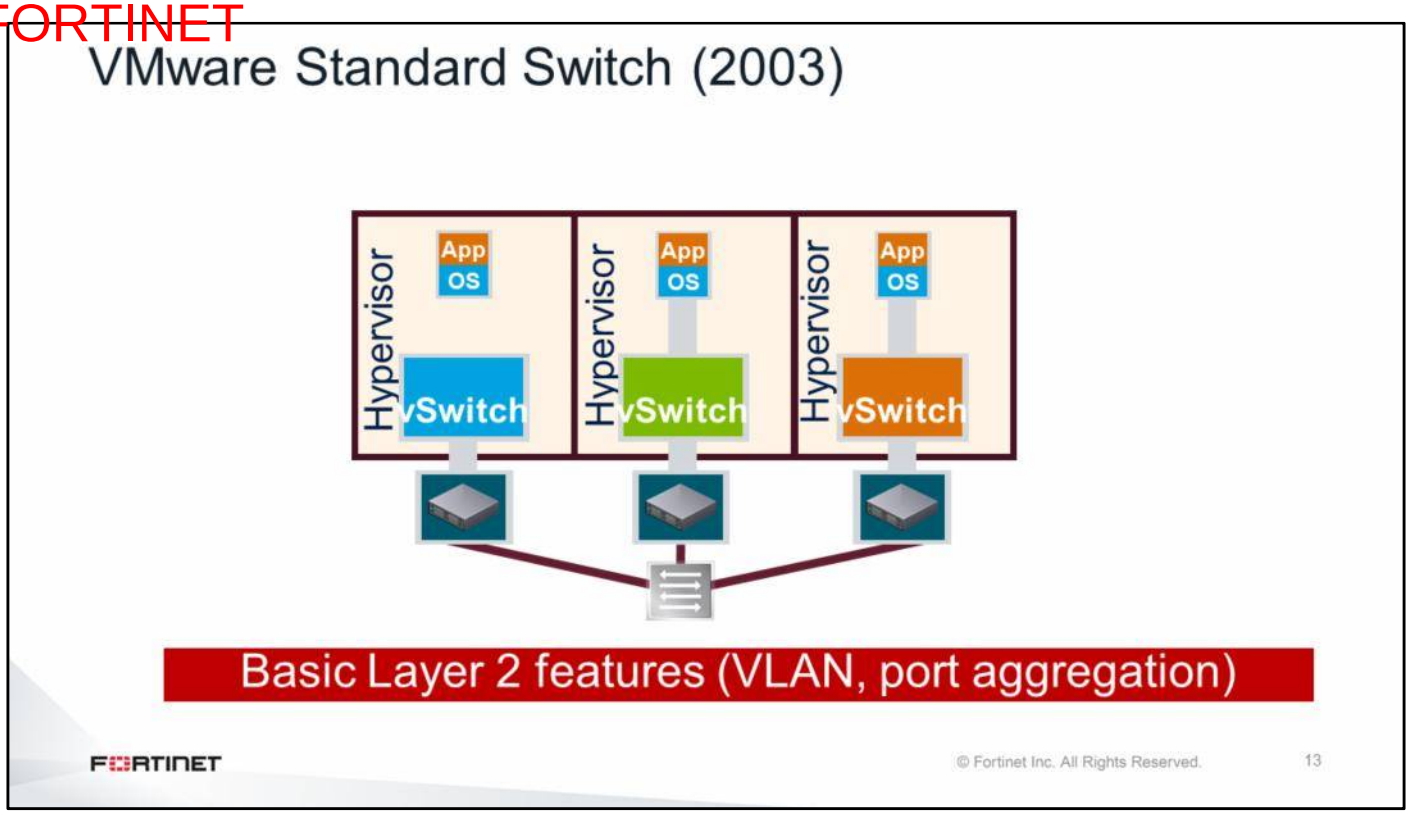


VMware is a well-known vendor that pioneered the virtualization market. VMware is specializes in the following:

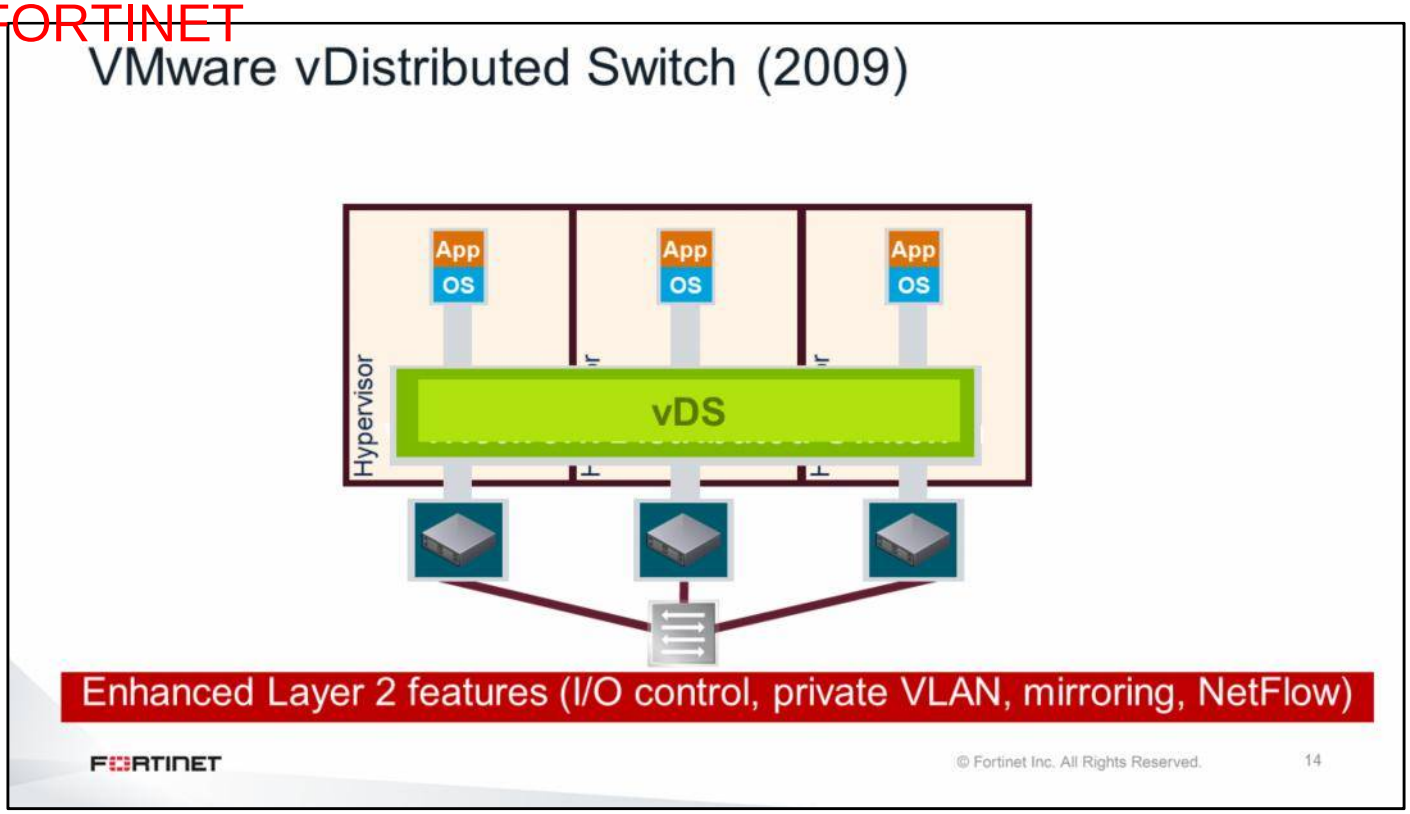
- **Server virtualization**: The main product is the vSphere Suite (ESXi and vCenter)
- **Network virtualization**: The decommissioned vShield and the newest NSX
- **Cloud management**: vCloud Director and vRealize Suite
- **Virtual desktop**: Horizon

Of all types of virtualization, the one this lesson focuses on is network virtualization. Network virtualization allows the creation of virtual networks inside the hypervisor, without the need of physical devices, such as routers or switches.

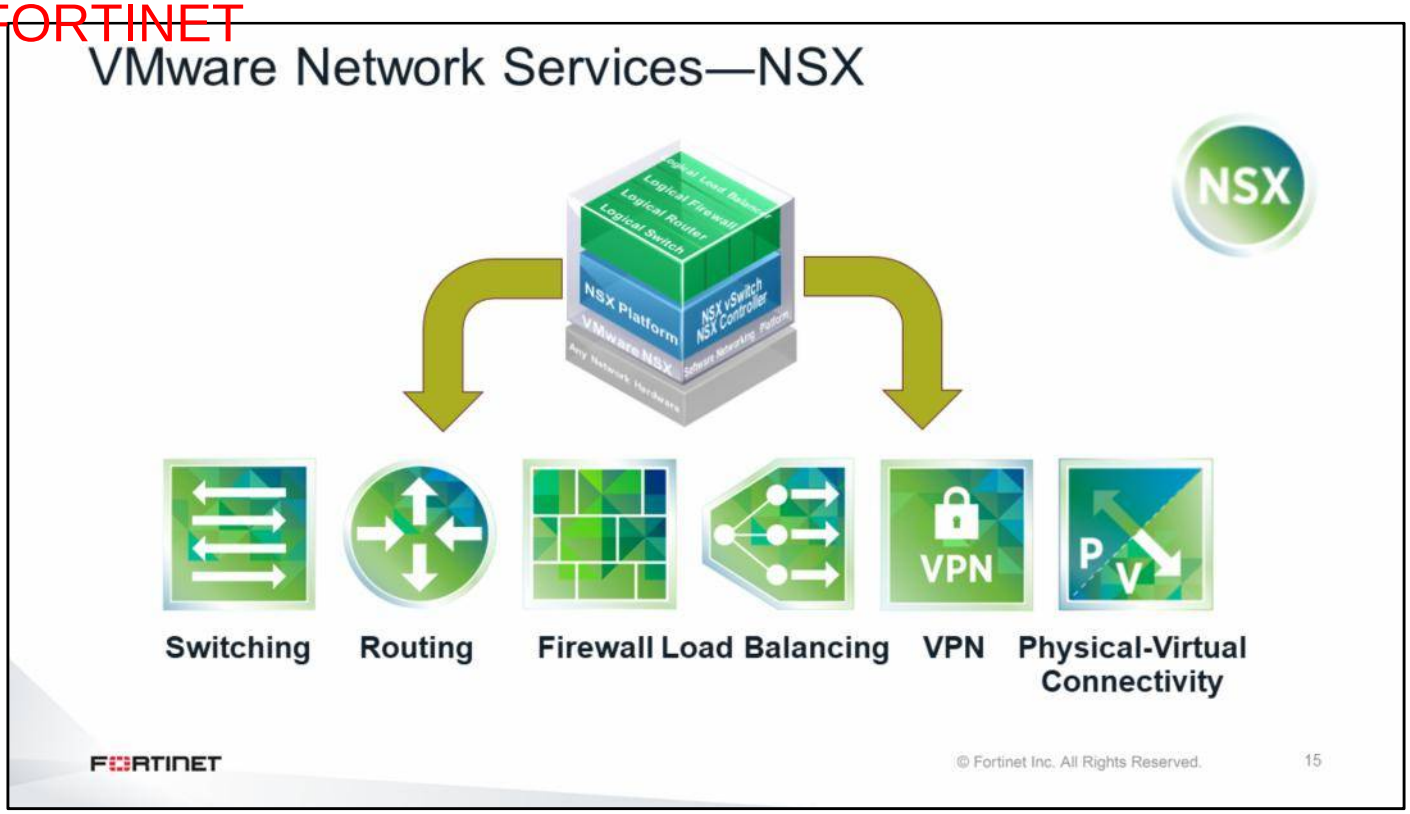
Now, you will learn how VMware evolved on the network virtualization front.



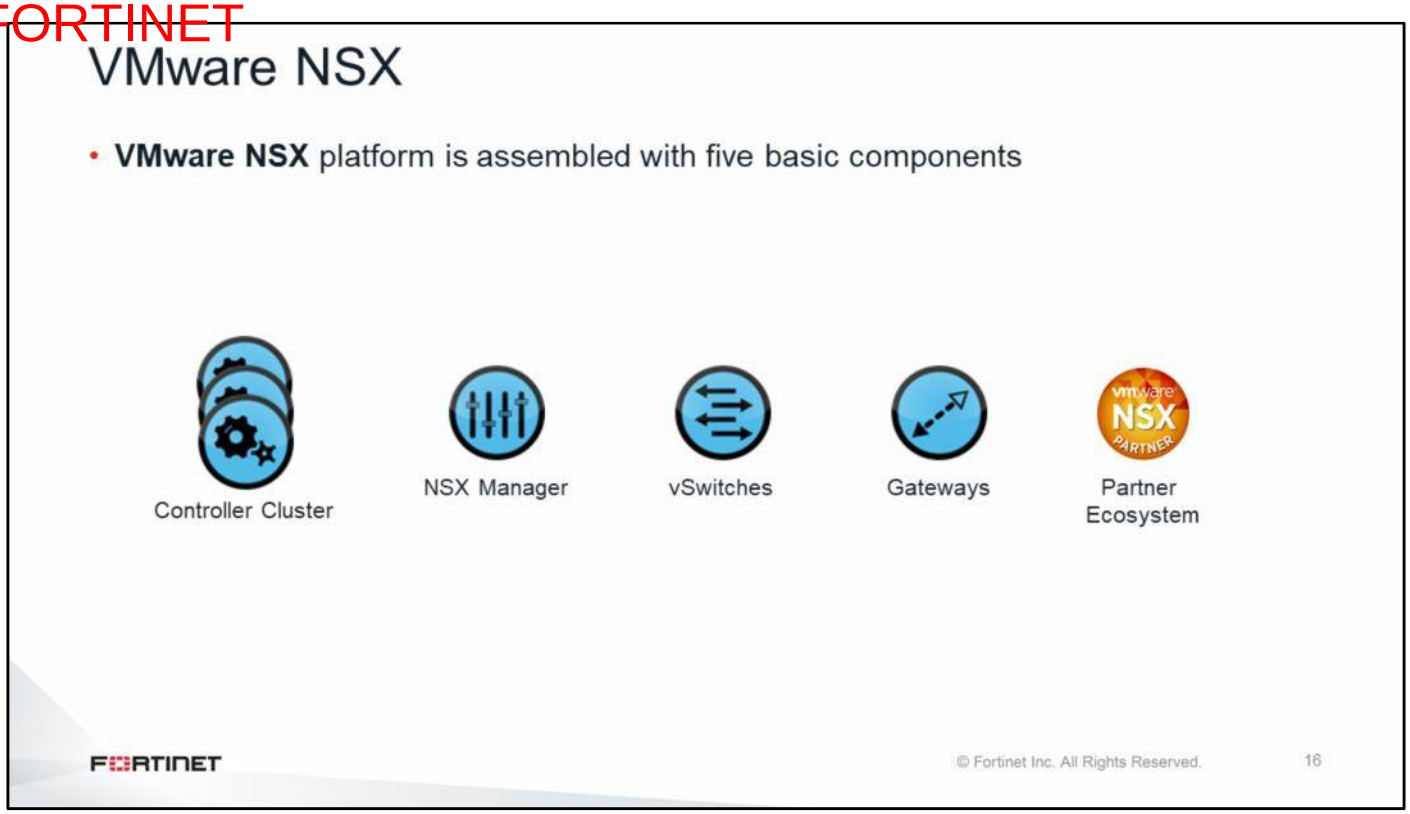
Back in 2003, VMware took the first step into network virtualization when they created the VMware Standard Switch, or vSwitch. This allowed network administrators to create virtual switches inside the hypervisor with basic layer 2 features, such as VLAN and port aggregation. This was a huge step into the future, as it allowed the use of network segmentation inside the virtualized server. However, those virtual switches were contained inside the hypervisors they were attached to, and could not communicate outside, without the help of the physical network.



Six years later, VMware launched the distributed virtual switch. This was a great addition because now the switch could span across all hypervisors that were members of the same cluster, and any VMs belonging to them could talk freely, without the need to configure the physical network. The vDistributed switches also provided enhanced layer 2 capabilities, such as I/O control, private VLAN, mirroring, and so on.



The standard and distributed vSwitch provided only switching capabilities. Then, in 2012, VMware bought a company called Nicira and integrated their Network Virtual Platform (NVP) with VMware vShield to create what is today called NSX Data Center. NSX Data Center extended the concept of network virtualization, to provide not only switching, but also routing, firewalling, load balancing, and VPN services. Now you can create virtual networks inside the hypervisor, which is a full blown network environment.

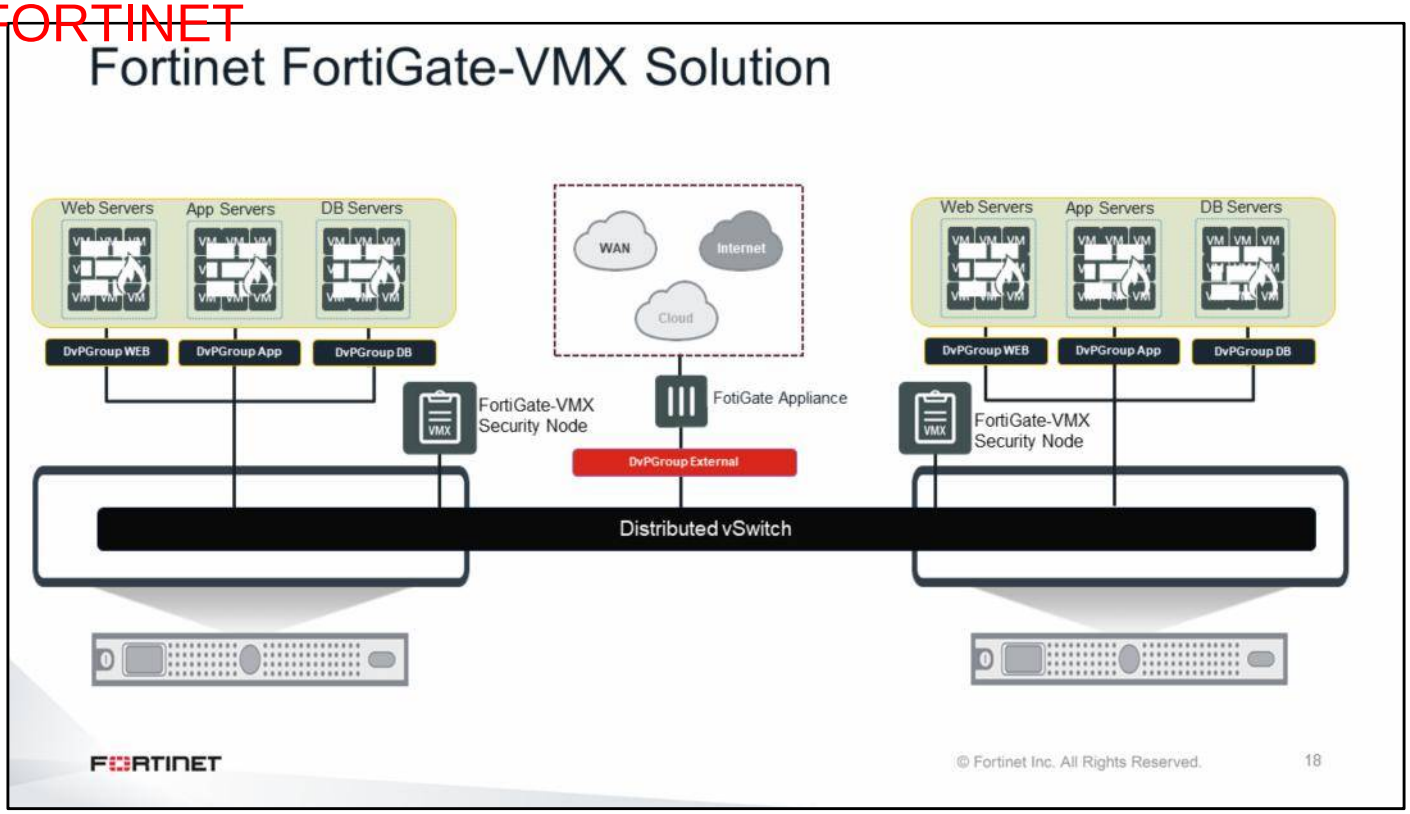


The VMware NSX platform is made up of five basic components:

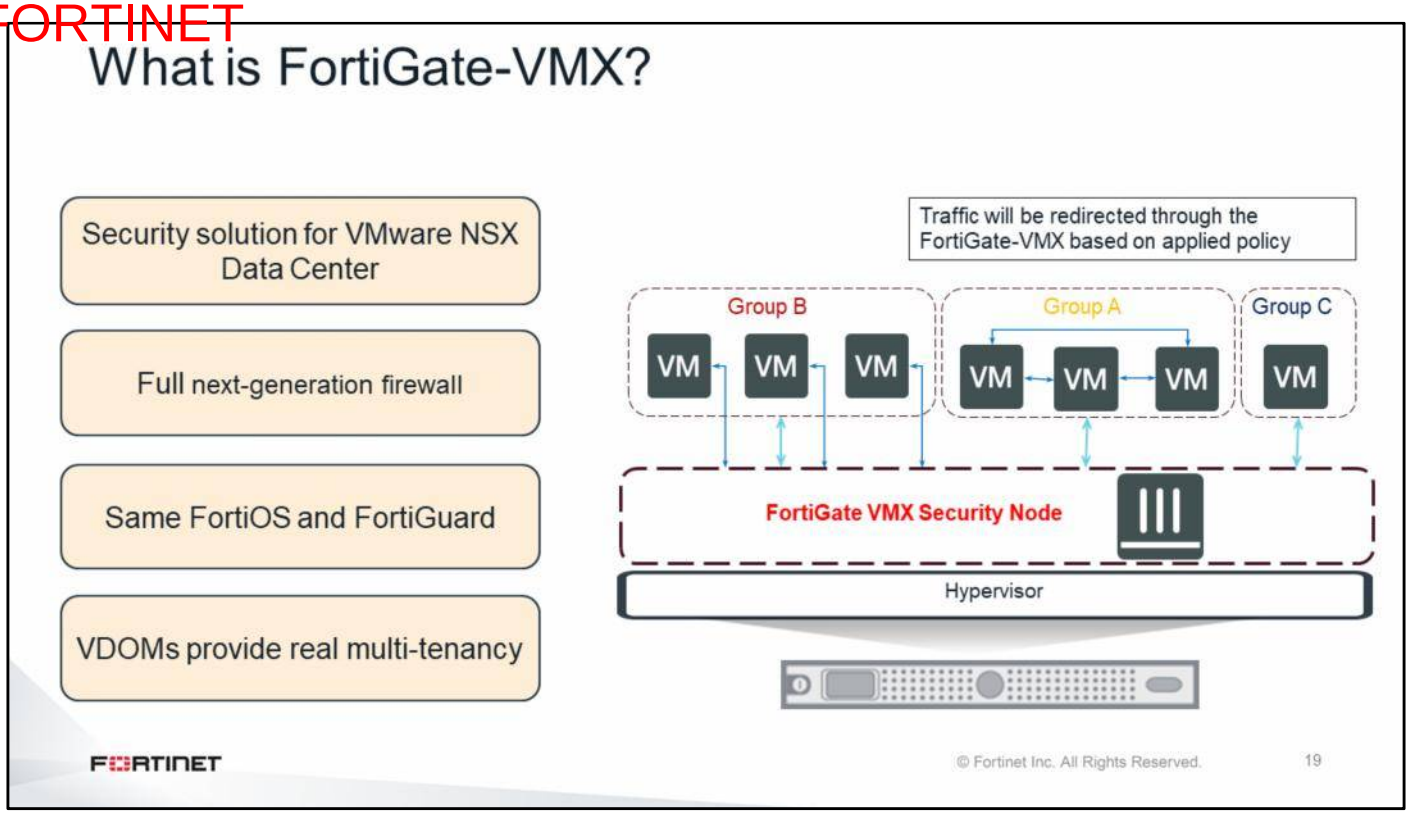
- **NSX controllers**:
  - Physically distributed, logically centralized, highly available system responsible for deployment of virtual networks across the entire architecture
  - Programs the hypervisor vSwitches and gateways
  - Accepts API requests from north-bound management platforms (for example, vCloud, OpenStack)
  - Completely out-of-band, and never handles a data packet
- **NSX Manager**:
  - Provides a web-based GUI management dashboard for interaction with the VMware NSX controller cluster API—system setup, administration, and troubleshooting
- **vSwitches**:
  - Each hypervisor has an in-kernel vSwitch with a programmable layer 2 to layer 4 data plane
  - The controller cluster programs each hypervisor vSwitch with a real-time configuration and forwarding state
- **Gateways**:
  - Scale-out services that connect virtual networks within VMware NSX to non-virtual hosts, remote sites, and external networks
  - Provide basic IP routing, MPLS, NAT, firewall, VPN, and load balancing functionality
- **Partner ecosystem**:
  - Platform that enables partners to register layer 2 to layer 4 services with the VMware NSX controller, and seamlessly insert their capabilities into virtual networks. For example, it allows other companies, such as Fortinet, to develop their own services that can be aggregated in to the NSX environment.

After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the FortiGate-VMX solution, you will be able to successfully deploy the FortiGate-VMX solution in your network.

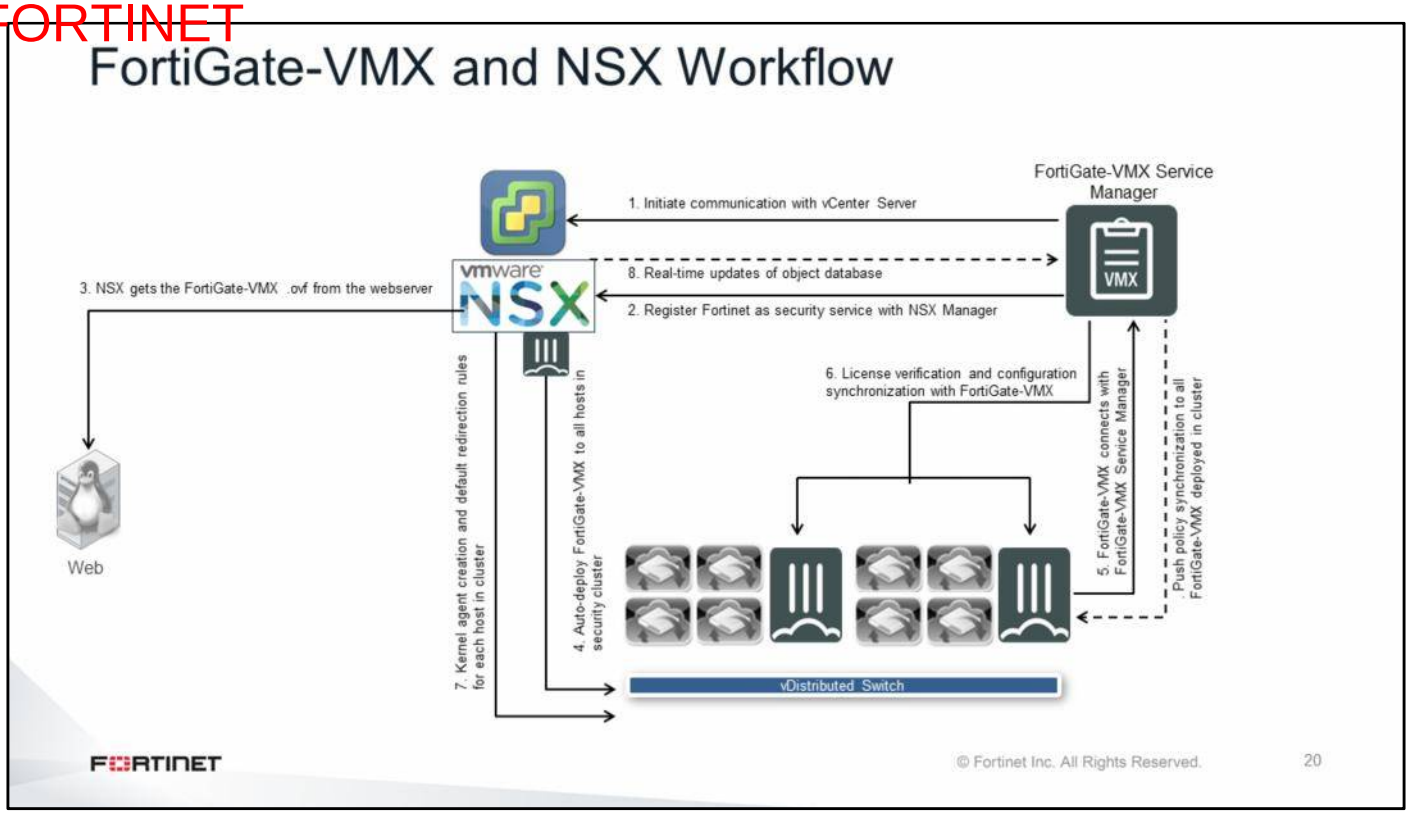


A FortiGate-VMX provides intra-VM and inter-VM security with ease-of-use, allowing for real micro-segmentation. The Fortinet FortiGate-VMX solution uses the NSX NETX API to provide advanced layer 4 to layer 7 services using service insertion, also called service chaining. This enables the additional inspection of VM traffic, prior to that traffic reaching the vSwitch. This enhances micro-segmentation where there is a need for greater application recognition, anti-malware, and other next generation firewall (NGFW) features.



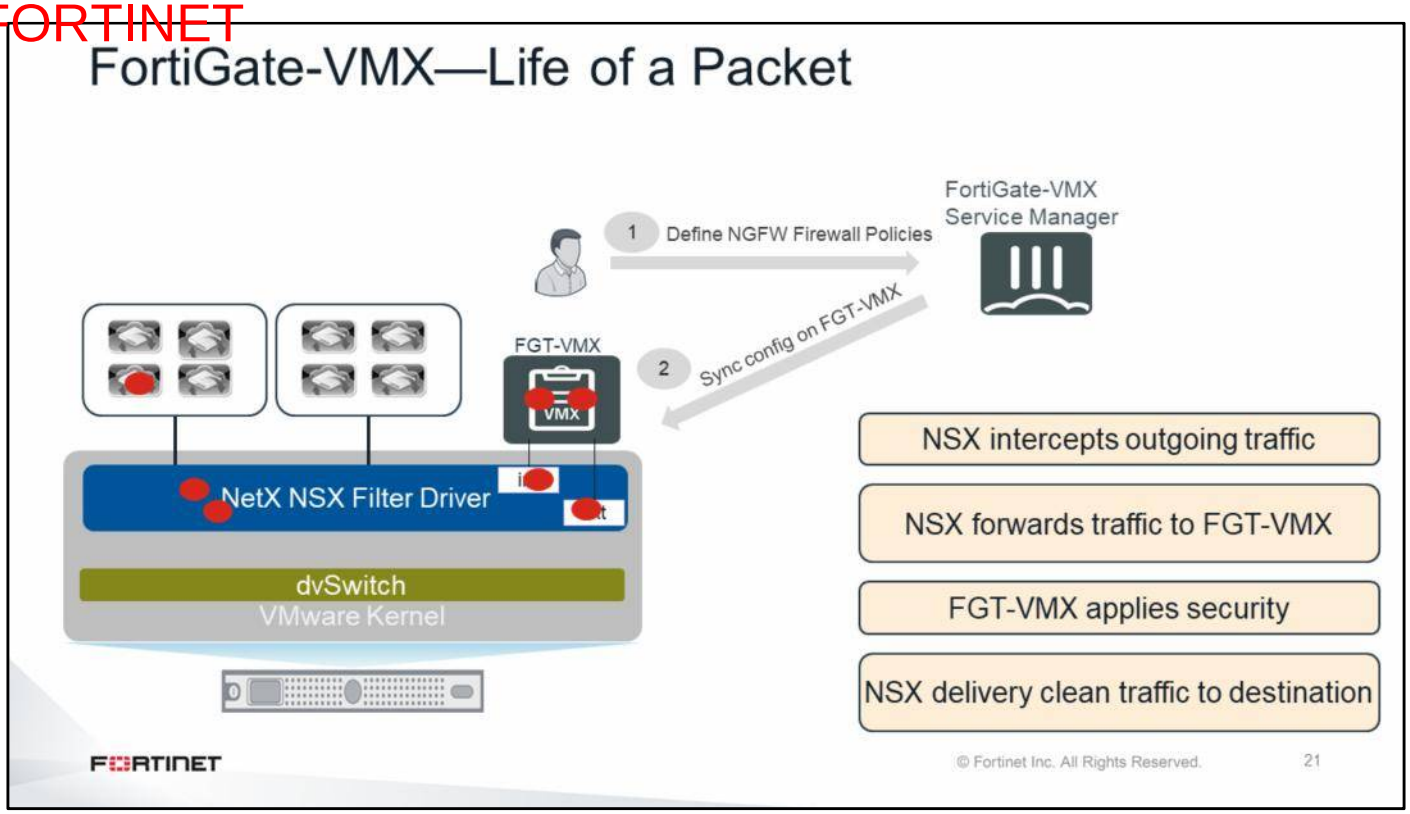
FortiGate-VMX is a security solution for VMware environments that provides purpose-built integration for the VMware software-defined data center (SDDC) — encompassing interoperability with VMware NSX and vSphere. Through direct API integration, FortiGate-VMX has visibility into and can secure virtualized network traffic at, the hypervisor level. The following are the four main benefits of FortiGate-VMX:

- Purpose-built security solution with VMware NSX for SDDC that runs between the VMs
- Full next-generation security functionality solution in one platform
- Backed by FortiOS policy configuration and FortiGuard, for real-time intelligence updates
- Proven multi tenant capable using VDOMs



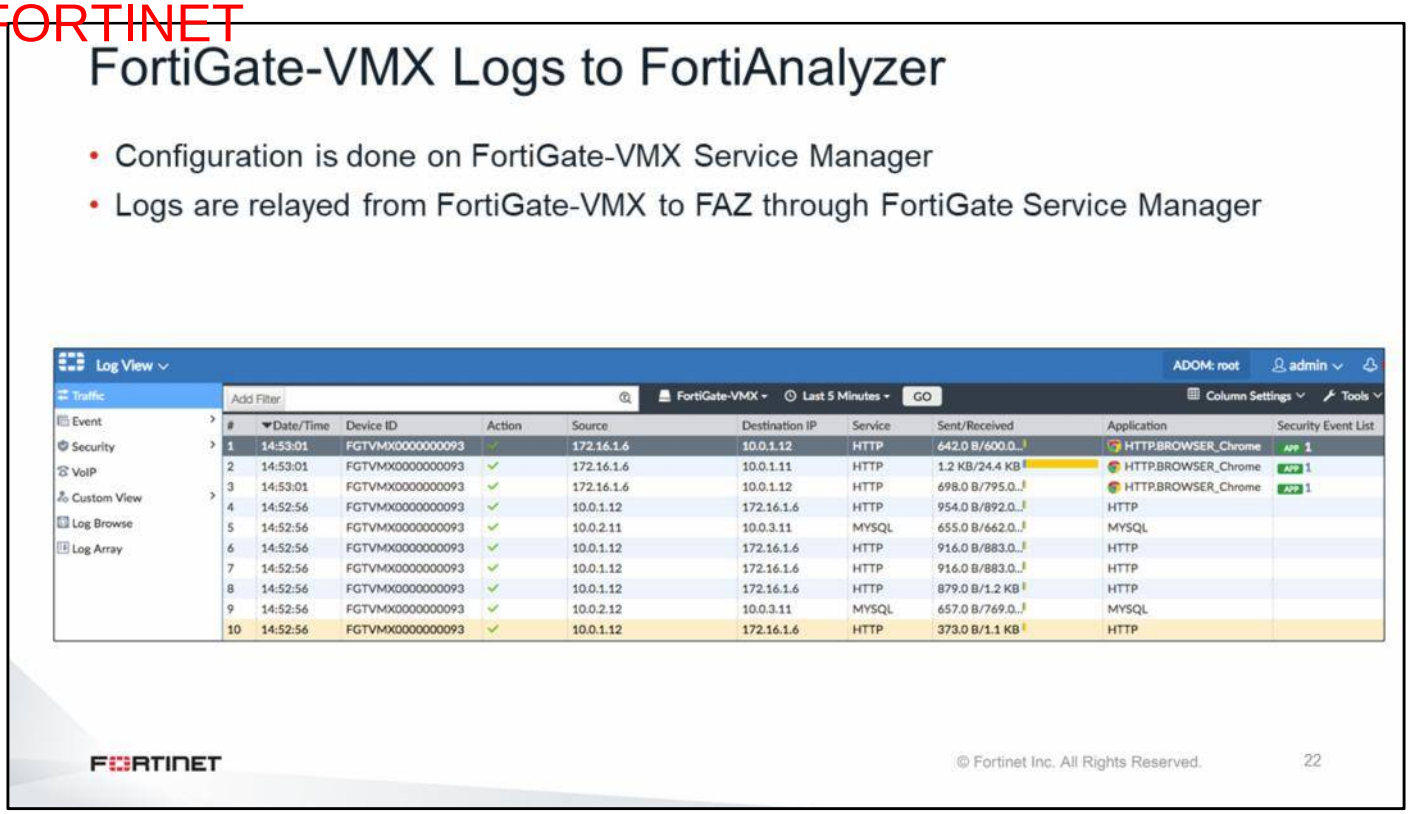
The following is the workflow that occurs when VMWare NSX connects to FortiGate-VMX Service Manager, and then to other components, such as a web server or FortiGate clusters:

1. FortiGate Service Manager initiates communication with vCenter Server.
2. FortiGate Service Manager registers FortiGate-VMX as a security service with NSX.
3. NSX (vCenter server) gets the FortiGate-VMX ovf file published on a web server. VCenter is responsible for deploying VMs, so VCenter goes to the web server and grabs the ovf file. Keep in mind that the ovf file must be published on the web server.
4. NSX deploys a FortiGate-VMX instance on each host within the cluster. If there is only one device, it will deploy only one device.
5. Once deployed, the FortiGate-VMX instances connect to FortiGate Service Manager.
6. FortiGate Service Manager performs license verification and synchronizes configuration, such as FortiGuard databases, with FortiGate-VMX instances.
7. NSX installs a kernel agent and default redirection rules for each host in the cluster.
8. NSX provides real-time updates of the object database to FortiGate Service Manager, which syncs those updates to all FortiGate-VMX instances.
9. FortiGate Service Manager pushes policy synchronization to all FortiGate-VMX instances.



Now, you will learn about the life cycle of a packet in FortiGate-VMX. The following list details the flow of activities in the life cycle of a packet in FortiGate-VMX.

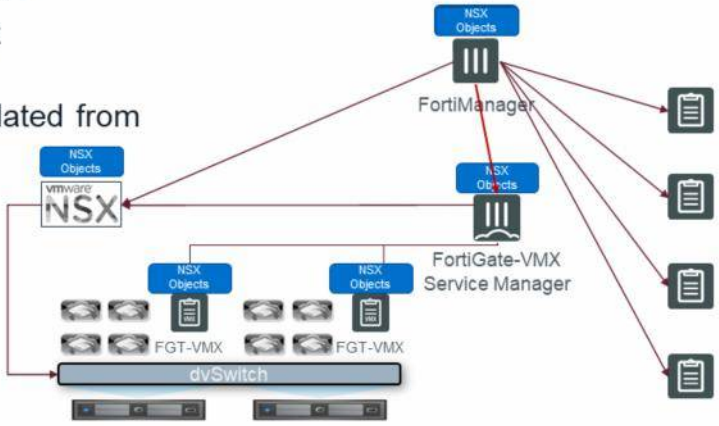
1. The administrator defines all NGFW policies on FortiGate Service Manager.
2. FortiGate Service Manager syncs all policies and configuration with the FortiGate-VMX instance.
3. Outgoing traffic is intercepted by NSX NetX Filter Driver.
4. NSX NetX Filter Driver forwards outgoing traffic to FortiGate-VMX.
5. FortiGate-VMX receives traffic on the *internal* interface, applies security inspection, then sends traffic back to NSX NetX Filter Driver through the *external* interface. Note that FortiGate does not send traffic to the destination, it sends traffic to the kernel. The VMX security node is responsible for east-west traffic inspection, but not north-south traffic inspection. Keep in mind that this is NSX-V, and both internal and external interfaces are configured in a virtual wire pair. It is a transparent bridge in route mode VDOM and no IP addresses are assigned to it.
6. NSX NetX Filter Driver can either perform service chaining or send the packet directly to its destination.



Note that any configuration must be done on FortiGate Service Manager, including logging configuration. Once configured, the FortiGate-VMX instance sends its logs to FortiAnalyzer using FortiGate Service Manager as the gateway. However, the inspection logs come from the FortiGate-VMX security node.

FortiManager and FortiGate-VMX Service Manager

- NSX Security groups objects imported in FortiManager using **dynamic objects**
- FortiManager sends dynamic object references to FortiGate
- Dynamic objects **automatically** updated from NSX Manager
- NSX Security Groups available in hybrid environment for **east-west** and **north-south** security



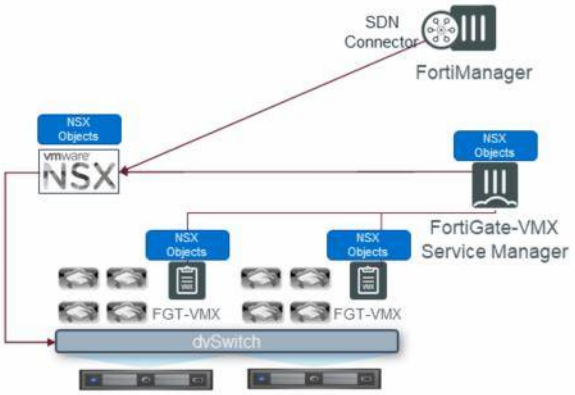
FORTINET

23

FortiManager is supported and can be deployed. FortiManager can connect to NSX Manager and import dynamic objects for policy creation. FortiManager can then send the dynamic object information to FortiGate Service Manager, which will feed it to all FortiGate-VMX instances, as well as any other regular FortiGate devices on the network, allowing NSX Security Groups (dynamic objects) to be used for both east-west and north-south security.

FortiManager and FortiGate-VMX Service Manager (Contd)

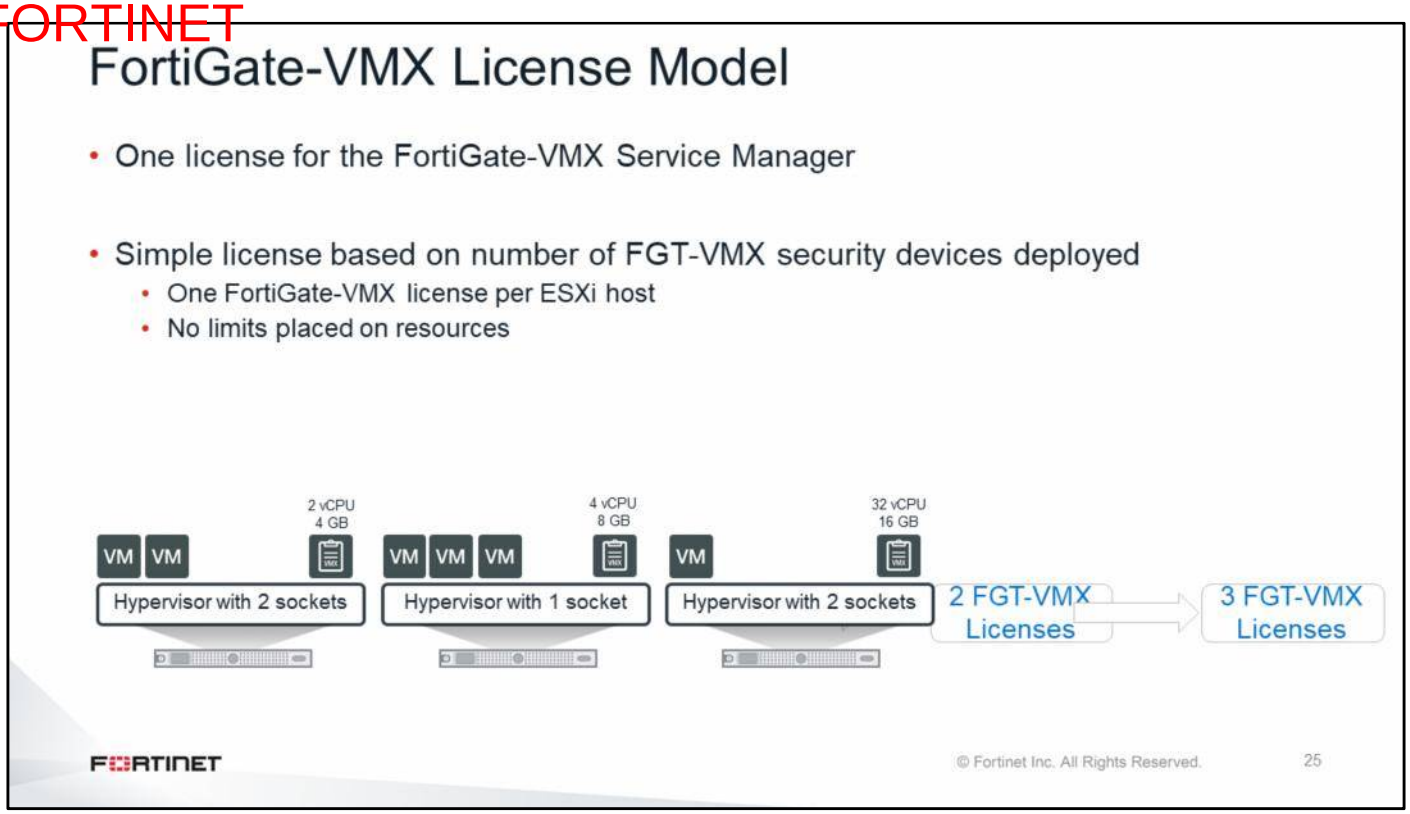
- Central management of FortiGate-VMX
- Fortinet SDN Connector is integrated into FortiManager
- FortiManager can **register** to NSX Security Groups
- SDN Connectors monitor the objects and update FortiManager and FortiGate **dynamic objects** (automatic updates)



FORTINET

24

FortiManager can centrally manage FortiGate-VMX nodes. With FortiManager and Fortinet SDN Connector, you can import security groups from VMware NSX, to automatically create objects that you can use in an IPv4 virtual wire pair policy.

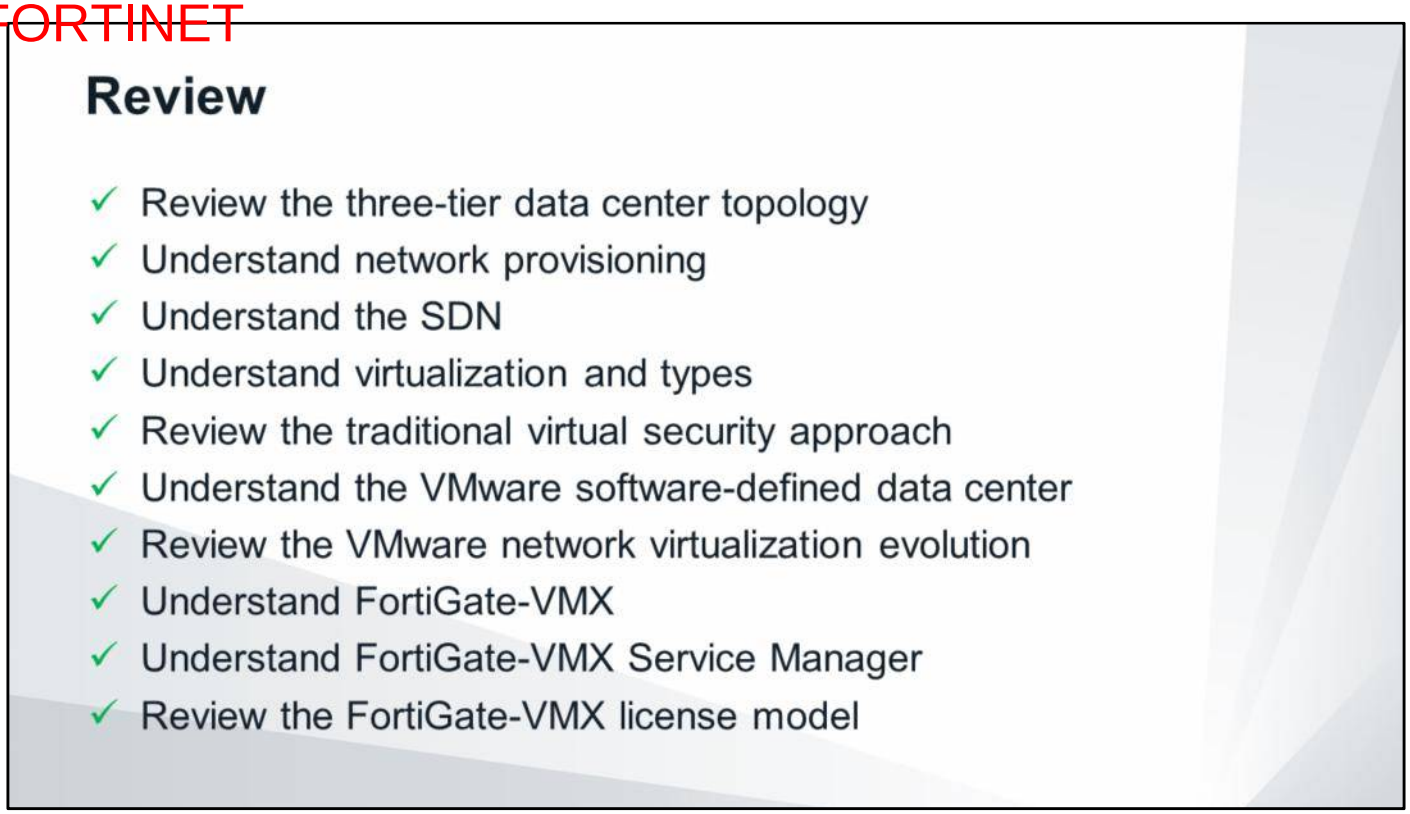


Now, you will learn about the FortiGate-VMX license model. There is one license for FortiGate Service Manager and one license for each FortiGate-VMX instance, which is per ESXi host.

The following are some examples of license models:

- If you have a cluster of 1 ESXi host, you will need 1 FortiGate Service Manager license + 1 FortiGate-VMX license.
- If you have a cluster of 3 ESXi hosts, you will need 1 FortiGate Service Manager license + 3 FortiGate-VMX licenses.

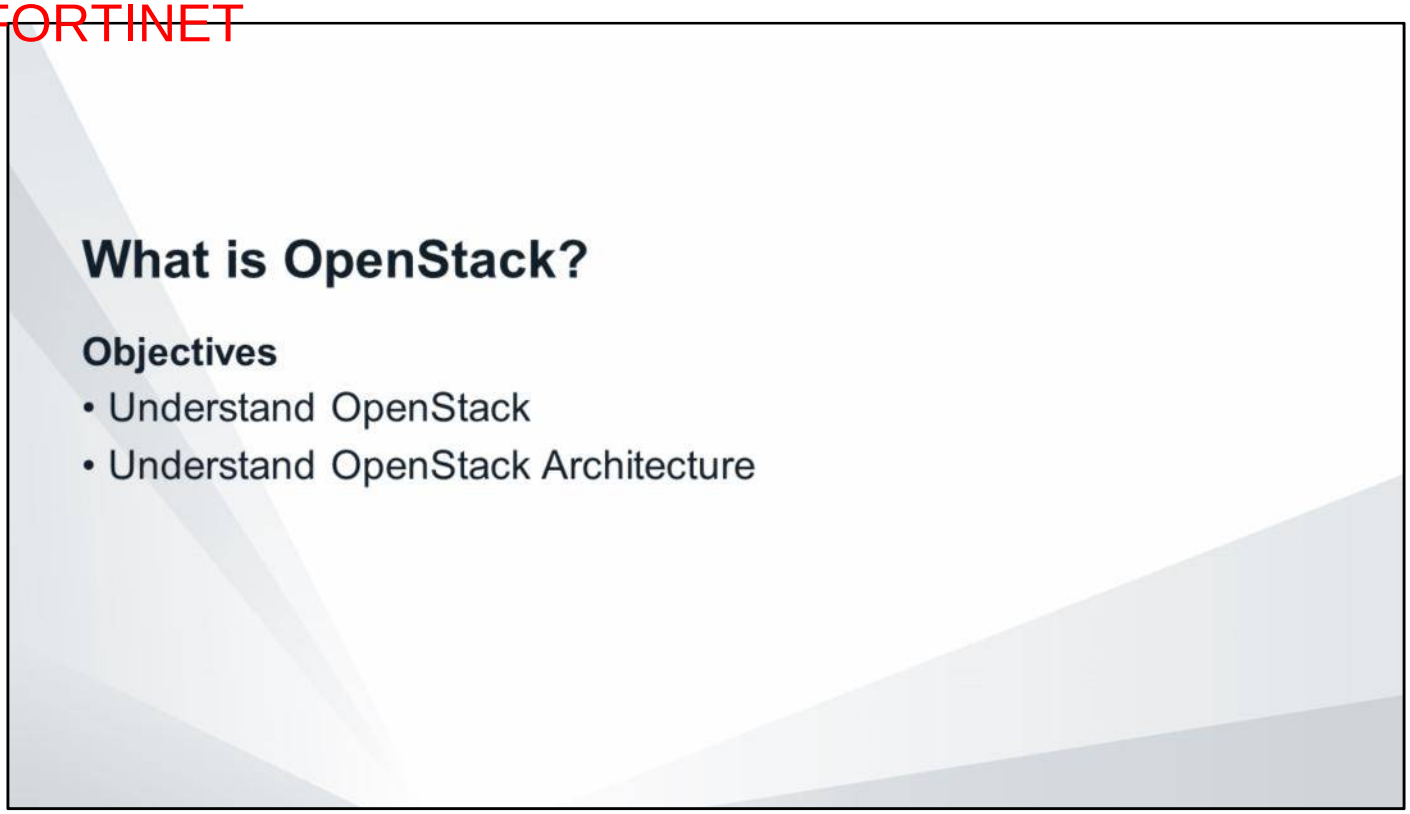
Note that there are no limits on resources, or the number of protected VM workloads.



This slide shows the objectives that you covered in this lesson.

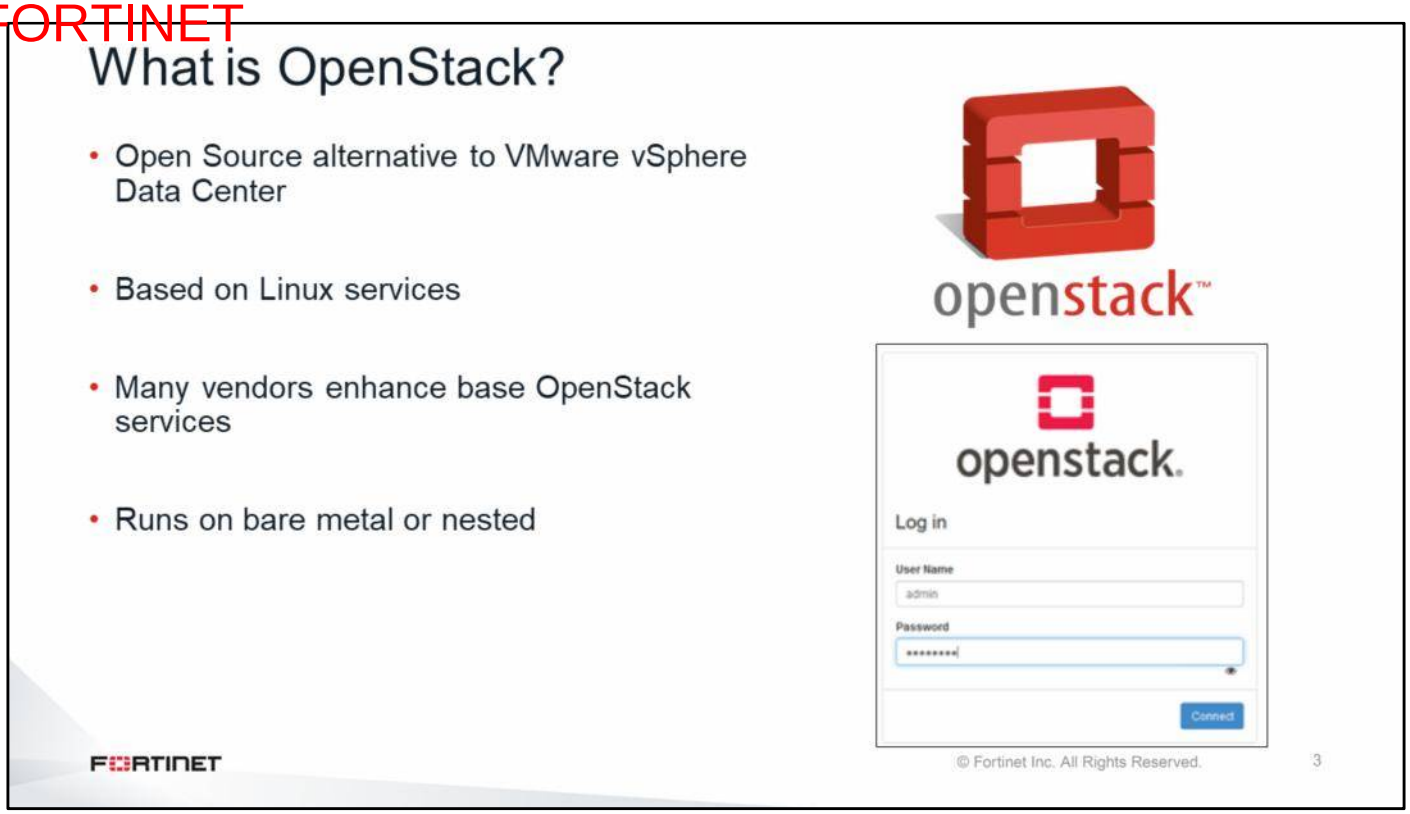
By mastering the objectives covered in this lesson, you learned about private cloud security concepts, virtualization, and how to protect the VMware software-defined data center (SDDC) using FortiGate-VMX.

In this lesson, you will learn about east-west traffic, and FortiGate integration with OpenStack.



After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding OpenStack and its architecture, you will be able to understand cloud computing and how it applies to your network.



OpenStack is a collection of open source technologies that deliver a massively scalable cloud operating system. OpenStack provides you with an infrastructure service that you can set up in your own cloud. OpenStack is a free and open source software platform that provides services that are an alternative to VMware vSphere Data Center.

OpenStack runs on bare metal or nested deployments, and is based on Linux services. Most vendors use the basic OpenStack source code, add features, and release it as a product. For example, Red Hat has its own version of OpenStack, which is not free. Red Hat is an enhanced version of OpenStack with more features, many services, and a different user interface, but the main source code is OpenStack, which is available free of charge.

Note that you need some Linux experience to work with OpenStack.

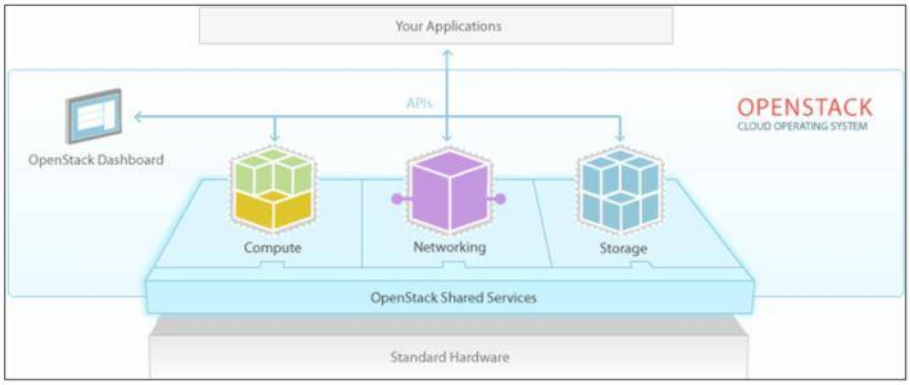
Major companies, such as Google, Facebook, and Amazon have used OpenStack in the past as a basic platform for their services. However, this platform has evolved and they no longer use OpenStack entirely, but instead use only some OpenStack components.

What is commodity hardware? These big companies have no need to use expensive vendor servers, such as Dell and IBM servers. They simply use basic hardware and build technologies on top of it to minimize the cost. It is important to know that hardware components are less important than software. Software, mainly SDN (software-defined networking), is the key component making the intelligence decisions while hardware is only the data plane.

DevOps is the combination of developer and operational teams, which helps to automate everything in the cloud. There is a heavy use of DevOps in the cloud by these big companies, and DevOps is the key to bringing the cloud world and security world together with heavy use of automation. Why do we say that everything is virtual? There is still a lot of hardware involved in the cloud, but most components in the cloud are shared resources, which means virtualization.

OpenStack Architecture

- Automation and orchestration of resources
- Decoupling of physical resources from services



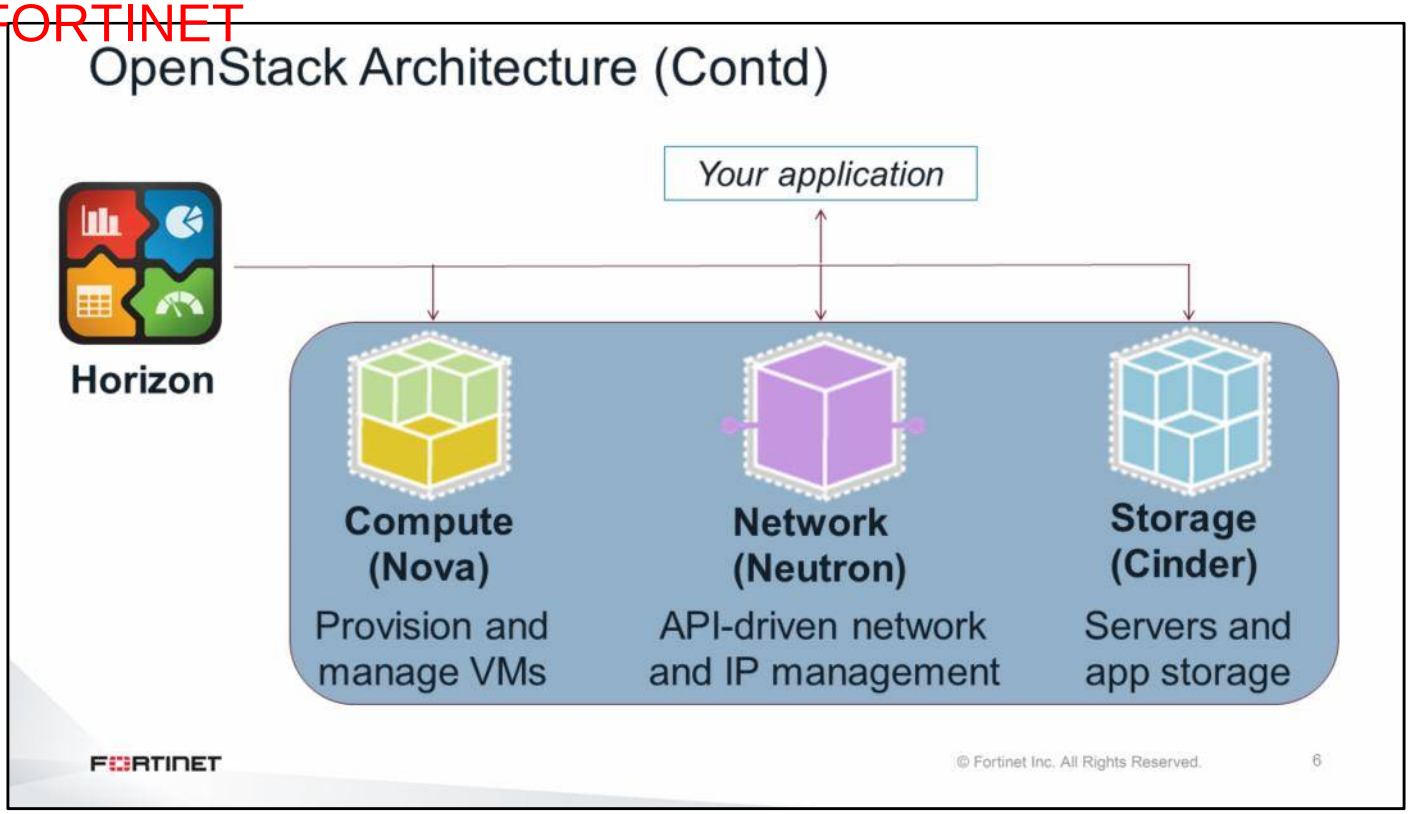
FORTINET

5

OpenStack architecture is very similar to any private cloud environment. As shown on this slide, the base for OpenStack is the standard hardware, then there is OpenStack shared services, with the Linux operating system in between. There are many OpenStack shared services, but the main services are:

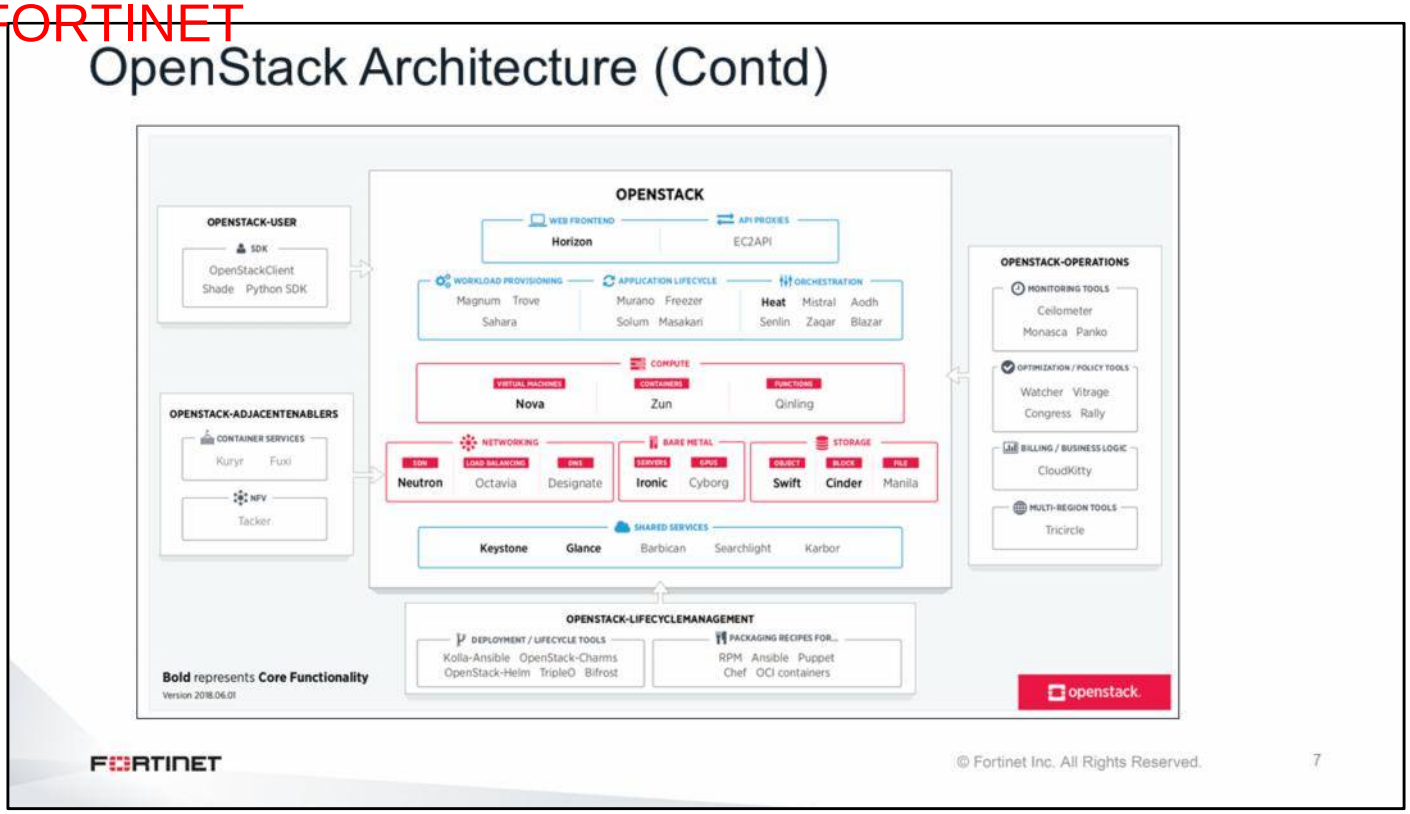
- **OpenStack Compute**: Provision and manage large networks of virtual machines
- **OpenStack Networking**: Pluggable, scalable, API-driven network and IP management
- **OpenStack Storage**: Object and block storage for use with servers and applications

Horizon is the canonical implementation of OpenStack's Dashboard, which provides a web-based user interface to OpenStack services including Nova, Neutron, and Cinder. In the OpenStack labs, you will create tenants and projects. Tenants are the virtual entity of the customers.

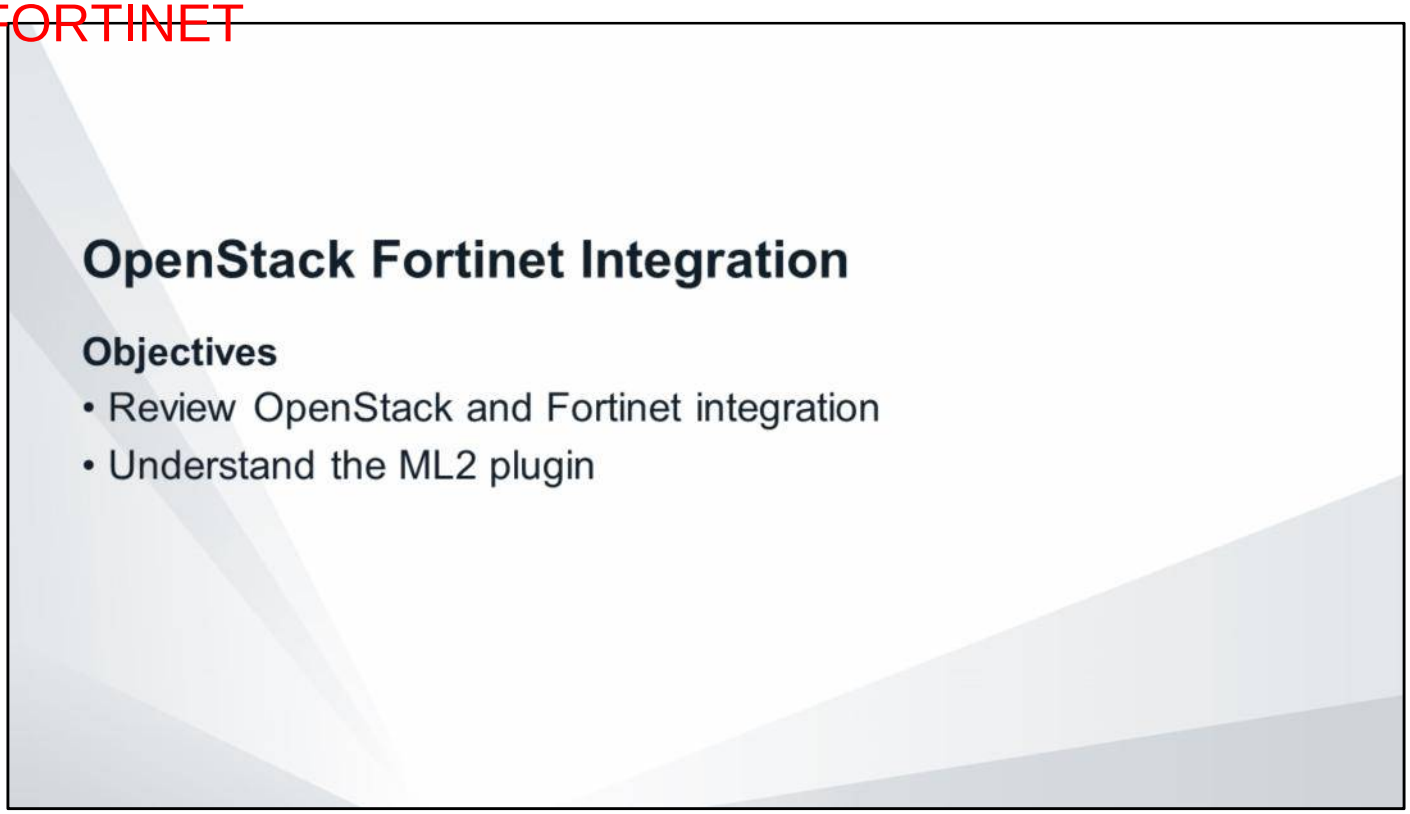


OpenStack is an open-source, scalable platform for building public and private clouds. It works mostly as IaaS (Infrastructure-as-a-Service), consisting of services, such as Compute (Nova), Networking (Neutron), Storage (Cinder), and others. Despite different service names in OpenStack, the functionality is similar to VMware. What are the VMware names for compute, network, and storage? Compute (Nova) is called ESXi, network (Neutron) is called NSX, and storage (Cinder) is called VSan (or it can be the local disk).

There are many applications that help to build your project. However, you will use only the applications that are necessary for your project. Note that you must have at least three main applications, such as compute, network, and storage, to start any OpenStack environment.

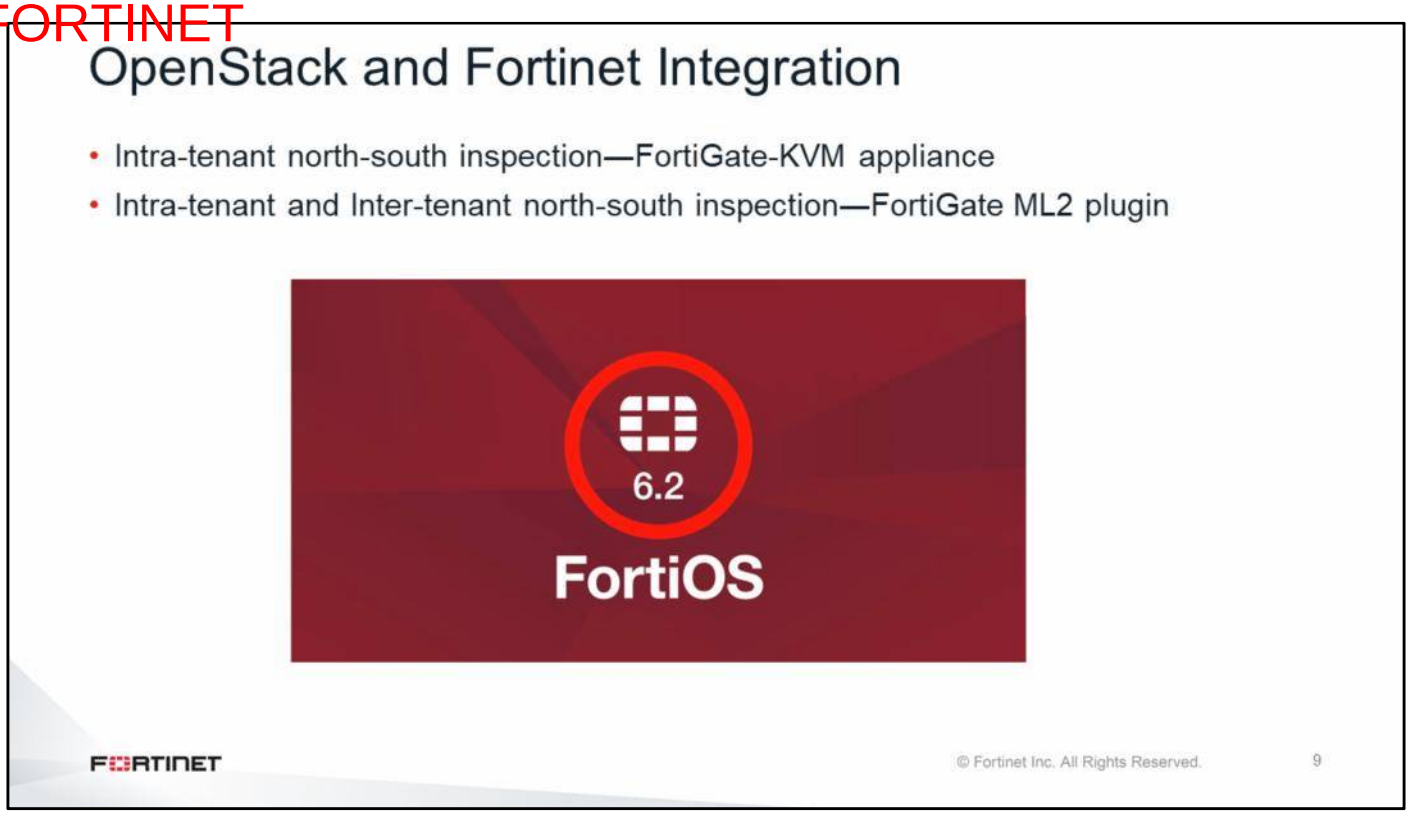


This slide shows the services that are available in the OpenStack architecture. The core functionalities are bolded. For example, Horizon, Nova, Neutron, Cinder, and so on.



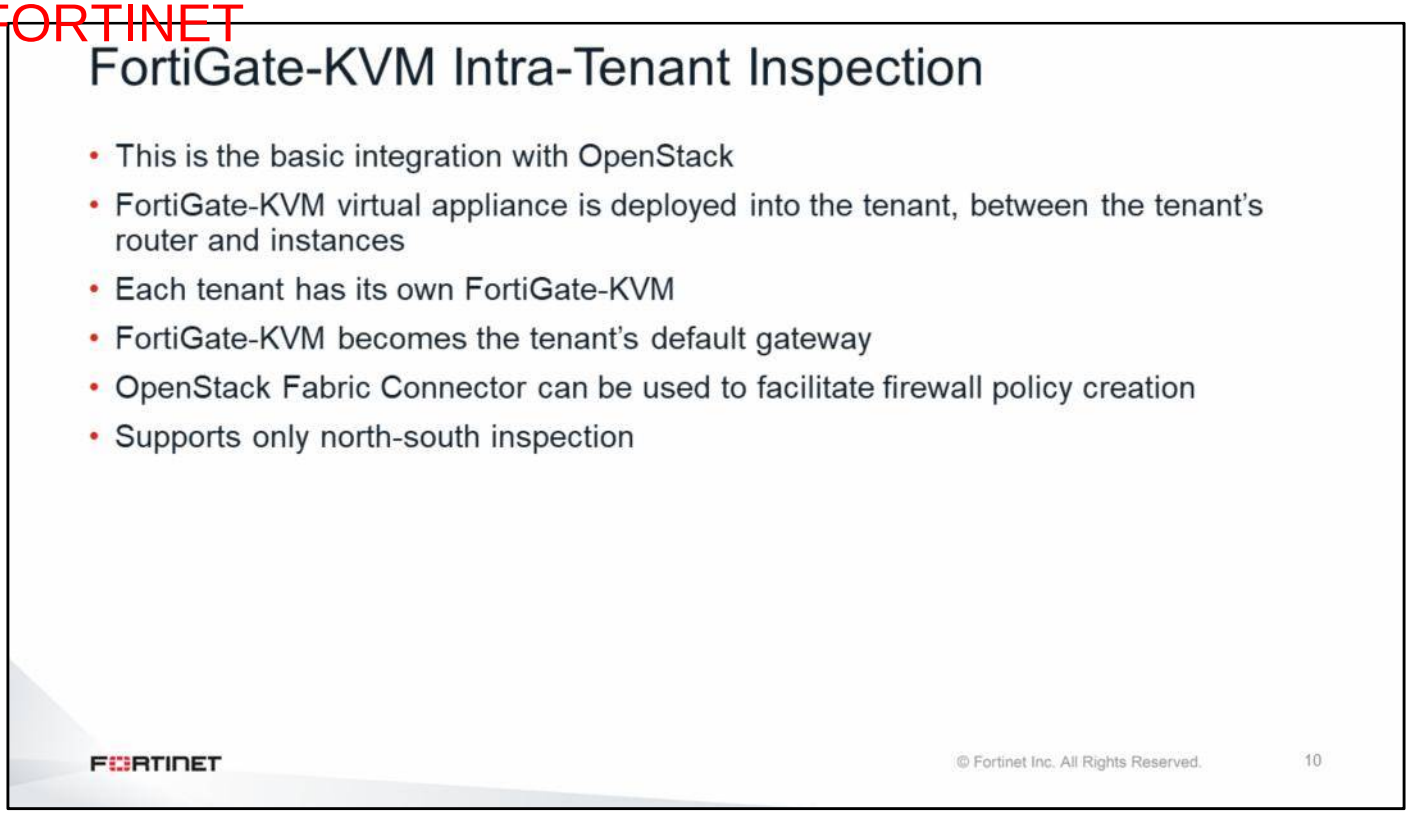
After completing this section, you should be able to achieve the objectives shown on this slide.

By demonstrating competence in understanding the concept of east-west traffic and different types of cloud delivery models, you will be able to understand how they apply to your network.



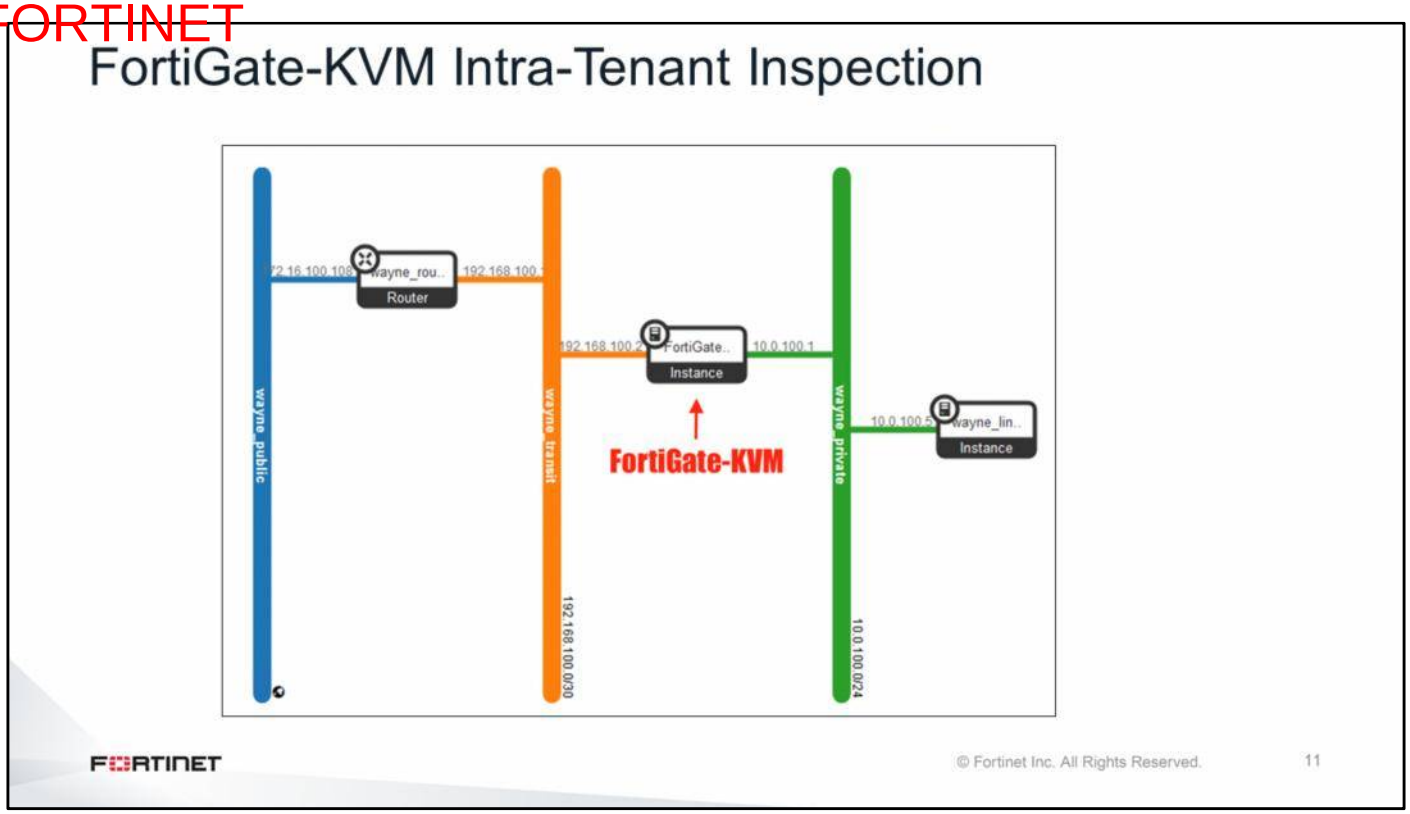
How can Fortinet help customers protect their OpenStack environment? There are two types of integrations:

- Intra-tenant north-south inspection, provided by the FortiGate-KVM appliance
- Intra-tenant and inter-tenant north-south inspection, provided by the FortiGate ML2 plugin



Intra-tenant inspection with the FortiGate-KVM provides security for all applications inside the tenant. As you learned before, OpenStack is divided into projects. The main feature of the private cloud solution is to provide shared services for customers and host many applications per customer. When required, a service provider can create a project (tenant) for a specific customer. By deploying FortiGate-KVM inside the tenant, the service provider can secure all applications inside the tenant for the customer. Note that the FortiGate-KVM deployed inside the tenant is the default gateway for any of the servers or applications behind the tenant, and therefore traffic must flow through and be inspected by the FortiGate-KVM. FortiGate-KVM can only inspect north-south traffic, which means only traffic that is routed by the FortiGate. However, there is no microsegmentation in this scenario, and traffic between VMs belong to different broadcast domains and cannot be inspected.

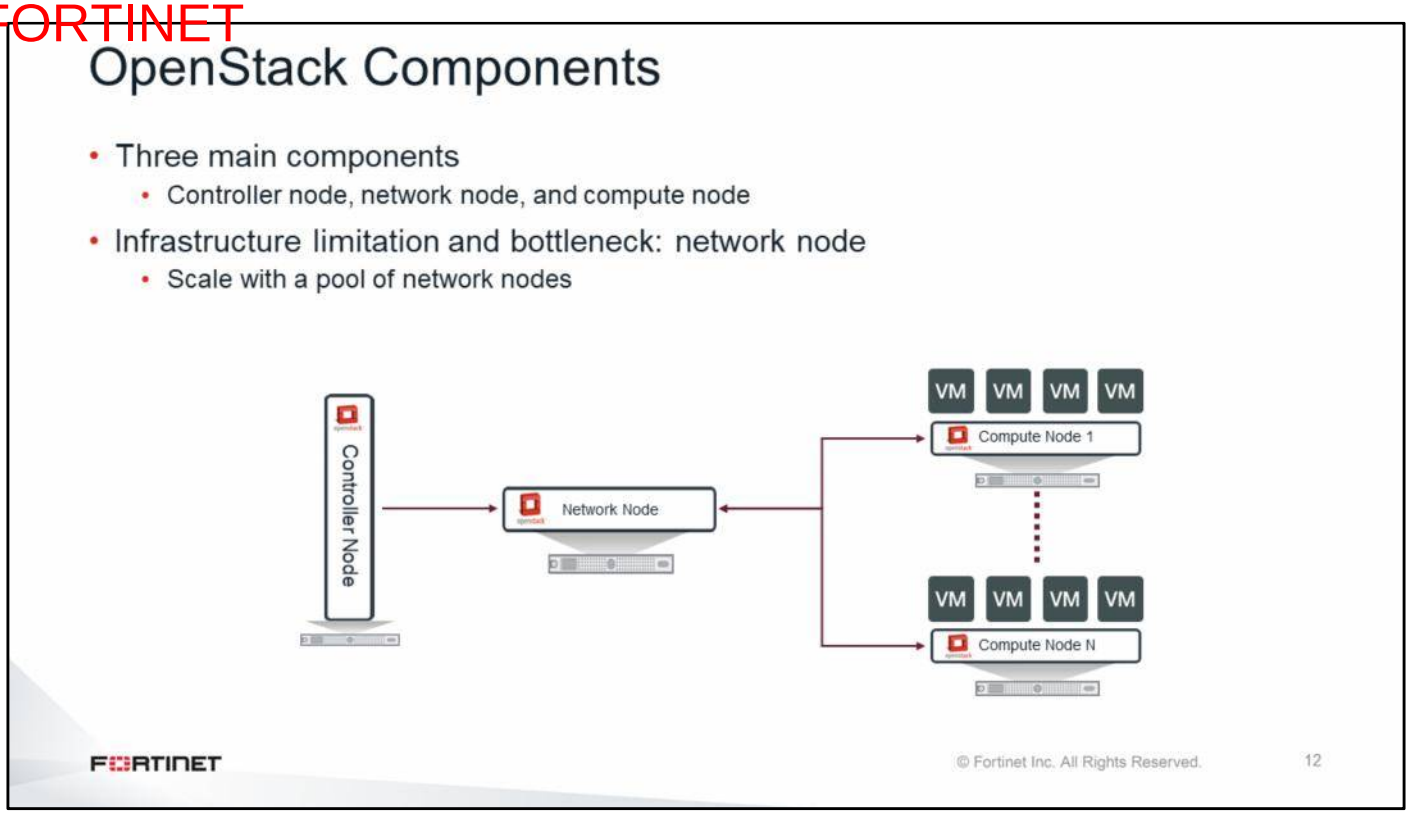
OpenStack Fabric Connector helps to create firewall policies without much effort. You can configure your FortiGate to connect to the dashboard, and then using OpenStack Fabric Connector, you can pull all the IP addresses and services for the tenant that can be used for firewall policy creation.



This slide shows an example topology with FortiGate-KVM deployed inside the tenant.

In OpenStack, Neutron, which is the network portion, has its own virtual default router as a default gateway. All traffic going out and coming in to the private network must go through this router. The main challenge in this scenario is to inspect traffic and provide security for all devices in the private network.

Fortinet has a solution for this scenario. By deploying FortiGate-KVM inside the tenant, in between the router and the tenant private network, a customer can secure all traffic destined to the private network from the public network, and traffic leaving the private network and going to the public network. In this scenario, FortiGate-KVM is the default gateway for all applications and servers behind the FortiGate-KVM. However, customers cannot bypass the router, which defaults to Neutron.



There are three main components in OpenStack:

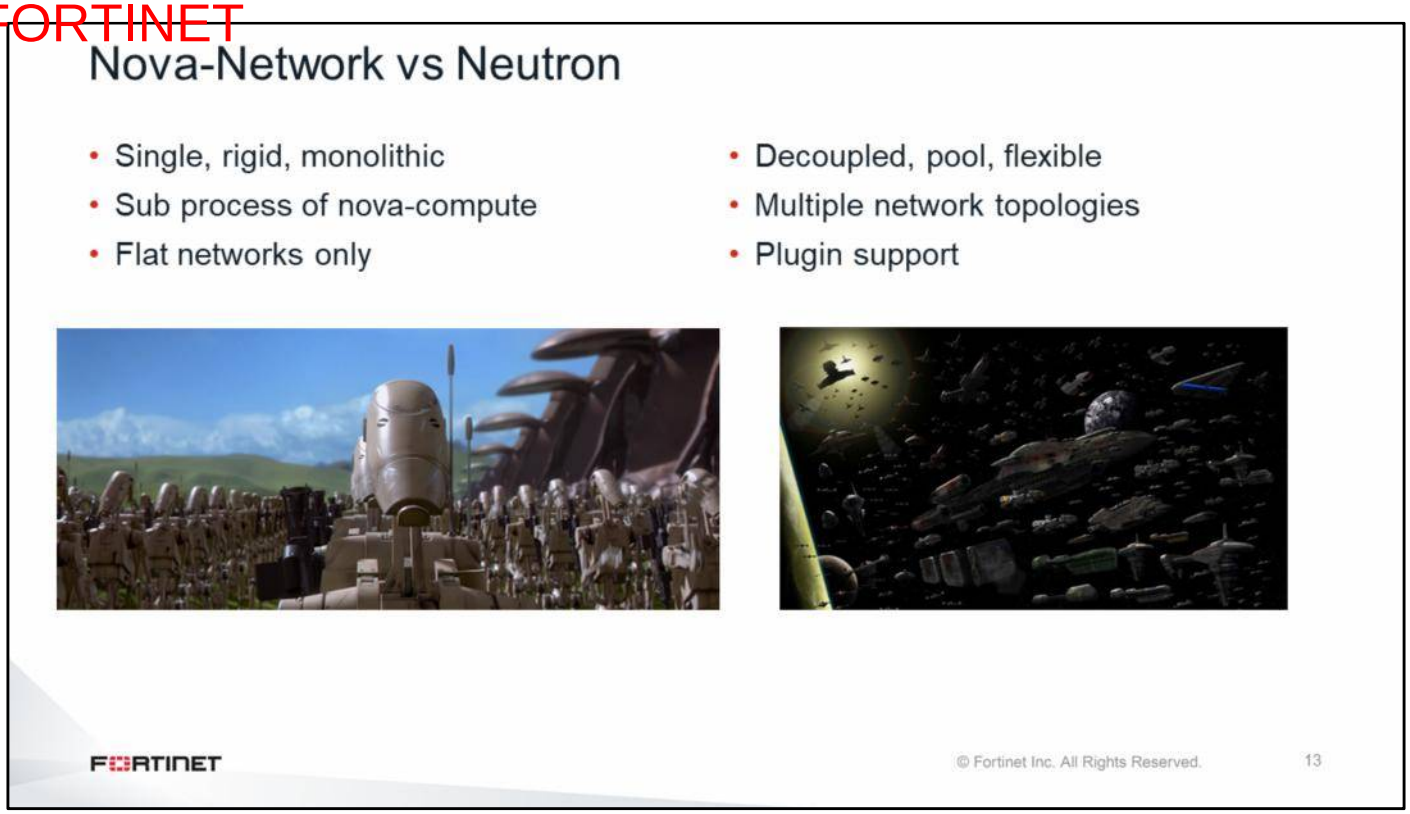
- **Controller Node**: Responsible for managing the whole infrastructure in OpenStack
- **Compute (Nova)**: Provides a way to provision compute instances. Nova runs as a set of daemons on top of existing Linux servers to provide that service.
- **Network node (Neutron)**: Provides networking as a service between interface devices (for example, vNICs) that are managed by other OpenStack services (for example, Nova). Network node is responsible for providing routing, virtual IPs, IP pools, DHCP, and so on. Neutron is a service, but it can run on a separate server.

As shown on this slide, there are four VMs running in each compute node on a single server, and both compute nodes are connected to a network node.

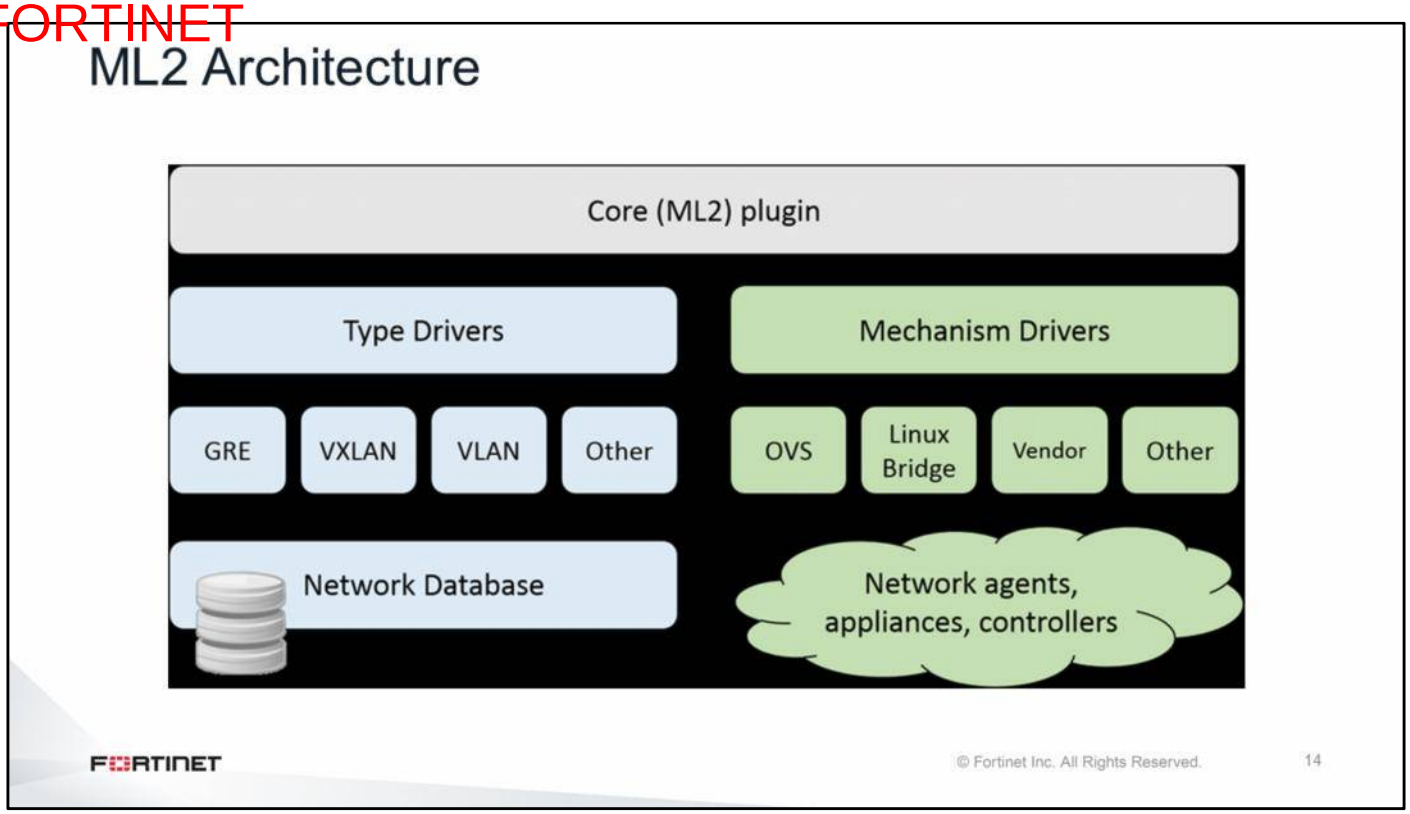
As a customer adds more VMs because of growing requirements, the network node will not be able to handle the extra load, and therefore performance will degrade. There are many solutions that minimize the impact. The customer can use a load balancer to load balance traffic, but the network node will eventually become a bottleneck. A better solution is to replace the regular Neutron with FortiGate.

FortiGate can simply provide the same performance as a number of regular servers, along with added security. Using a high-end physical FortiGate as a network node customer can boost performance and mitigate most of the bottlenecks.

Note that regular Neutron cannot provide Layer 7 security inspection.

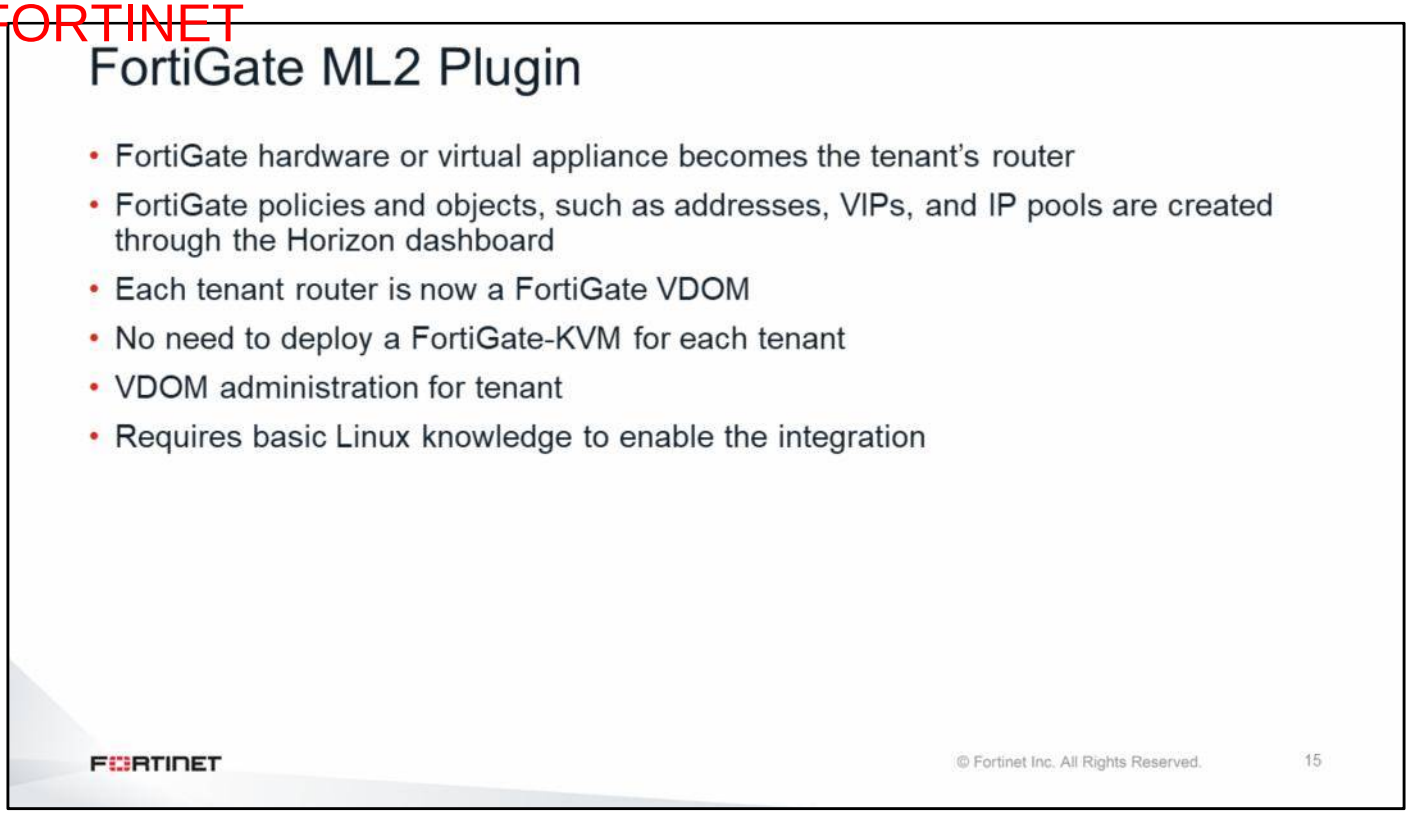


As you learned earlier, Nova is the compute component. Nova-Network basically runs open virtual switches on the compute node to provide Layer 2 services, which is very limited. It supports only flat networks and is a sub process of nova-compute, so performance is very low. In order to enhance the network services in OpenStack, Neutron is the best alternative because it is more powerful and flexible than Nova-Network. Neutron can provide layer 3, DHCP, routing, VIPs, source NAT, security, and filtering up to layer 4. Neutron supports plugins, so vendors like Fortinet can develop plugins to integrate their services using APIs, to use in OpenStack. This is where the ML2 plugin comes into play. The ML2 plugin allows vendors to integrate their products with OpenStack.



This diagram shows the architecture of the ML2. The Modular Layer 2 (ML2) plugin is a framework that allows OpenStack Neutron to simultaneously use the variety of layer 2 networking technologies found in complex real-world data centers. There is a core plugin and type drivers. Types drivers, such as GRE, VXLAN, VLAN control, and instruct, enable OpenStack to send traffic back and forth between compute nodes. For example, there are two compute nodes and an administrator must configure both nodes to talk to each other. The administrator can use VXLAN encapsulation, which helps encapsulate multiple VLANs inside the VXLAN tags. Having encapsulated in VXLAN, the customer can support multiple tenants which eliminates the limitation of VLAN tags.

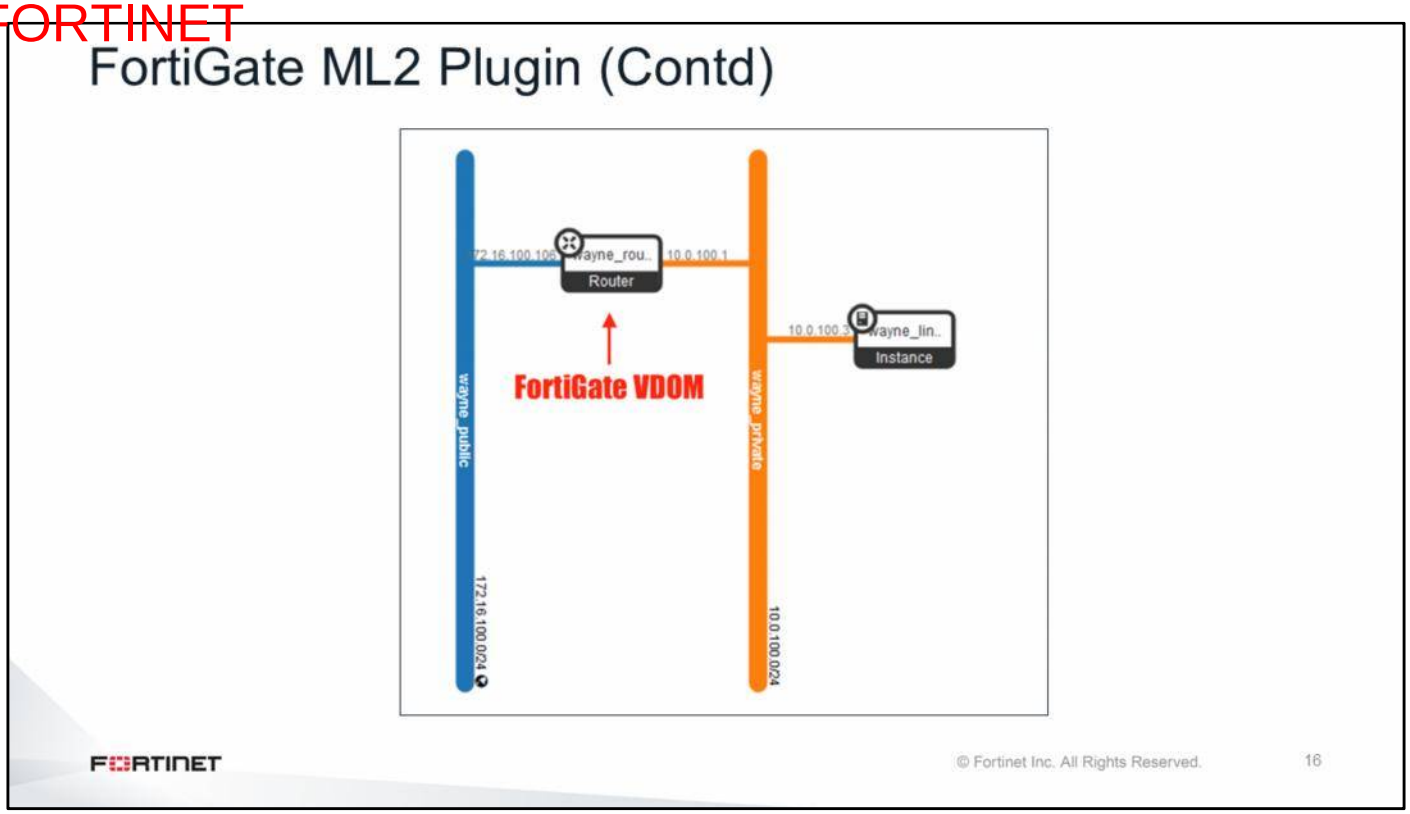
Mechanism drivers are responsible for taking information supplied by type drivers and ensuring it is properly applied given the specific networking mechanisms that are enabled, such as Open vSwitch (OVS), Linux Bridge, vendor specific, or other mechanism drivers. Also, there are network database, network agents, appliances, controllers, and so on.



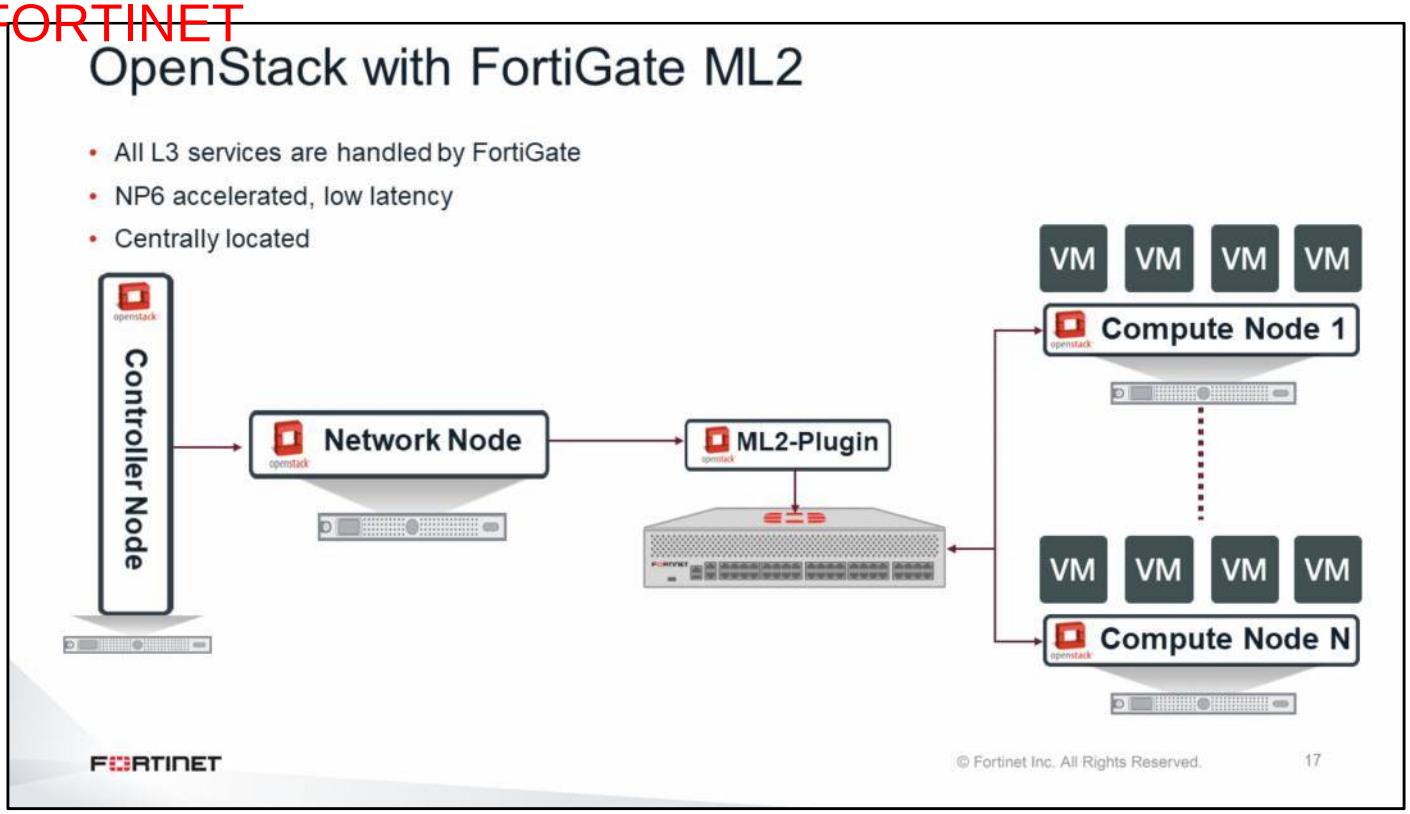
As you learned about the first type of integration with OpenStack earlier, this is the second type of integration with OpenStack, which is provided by the FortiGate ML2 plugin. In the first integration, FortiGate-KVM is deployed between the router and the tenant‘s private network.

In the second type of integration, FortiGate hardware or virtual appliance becomes the tenant’s router. FortiGate policies and objects, such as addresses, VIPs, and IP pools are created through the Horizon dashboard. Therefore, customers can use powerful FortiGate to provide performance and security without deploying a FortiGate-KVM for each tenant. Multiple VDOMs can be used as a tenant.

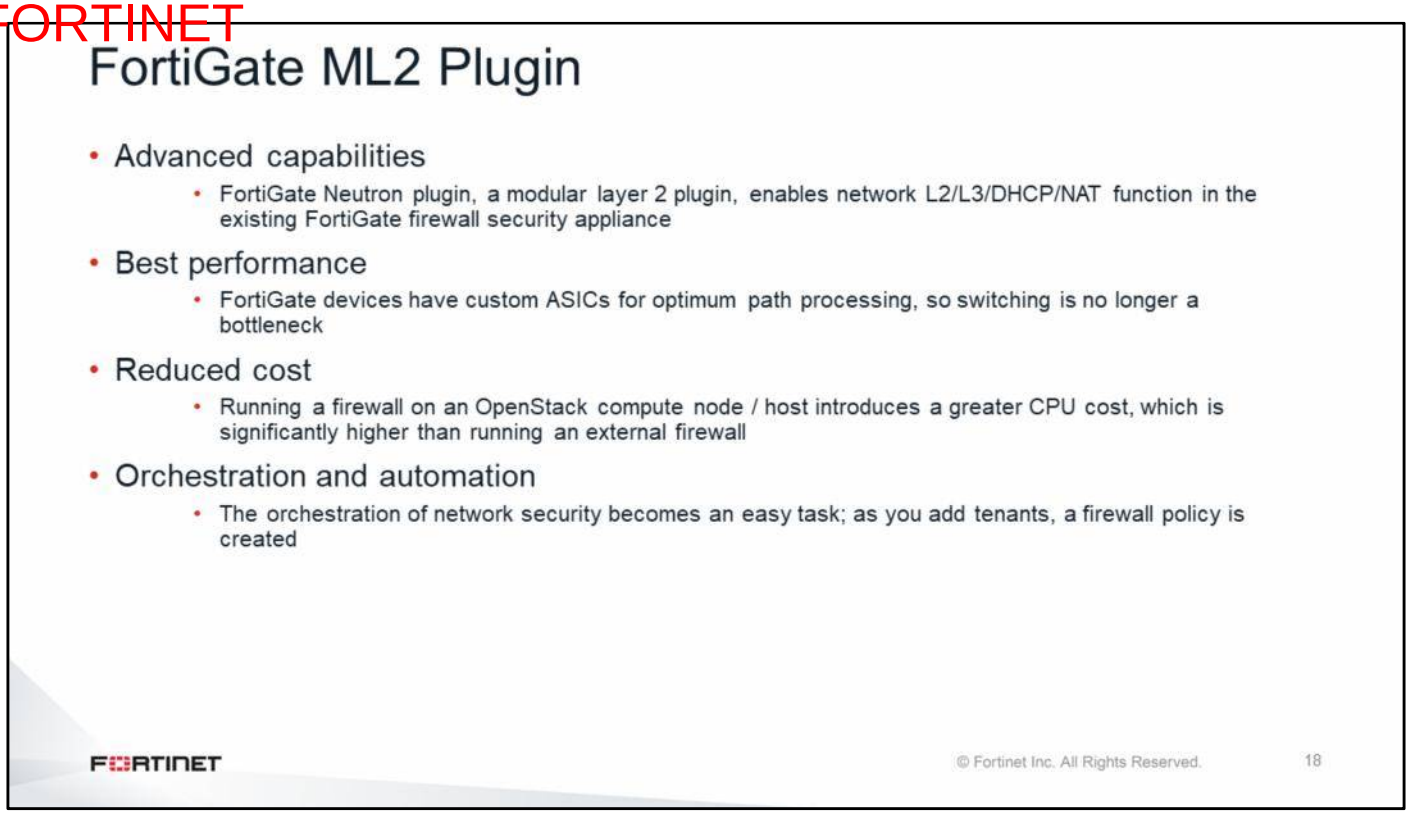
A typical use case is a service provider who provides services to many customers. In this scenario, the service provider can add many tenants without worrying about performance and security, by replacing the Neutron with a FortiGate VDOM. The service provider can use a single FortiGate and divide it into many VDOMs, and then assign one VDOM per customer. Then, the cloud router becomes the FortiGate VDOM. Basic Linux knowledge is required to enable the integration.



As shown on this slide, the topology shows a FortiGate VDOM between the public network and the private network. Note that there is no default router in this topology, as you learned in the first type of integration. Instead, the FortiGate VDOM is the default gateway for all devices in the private network.

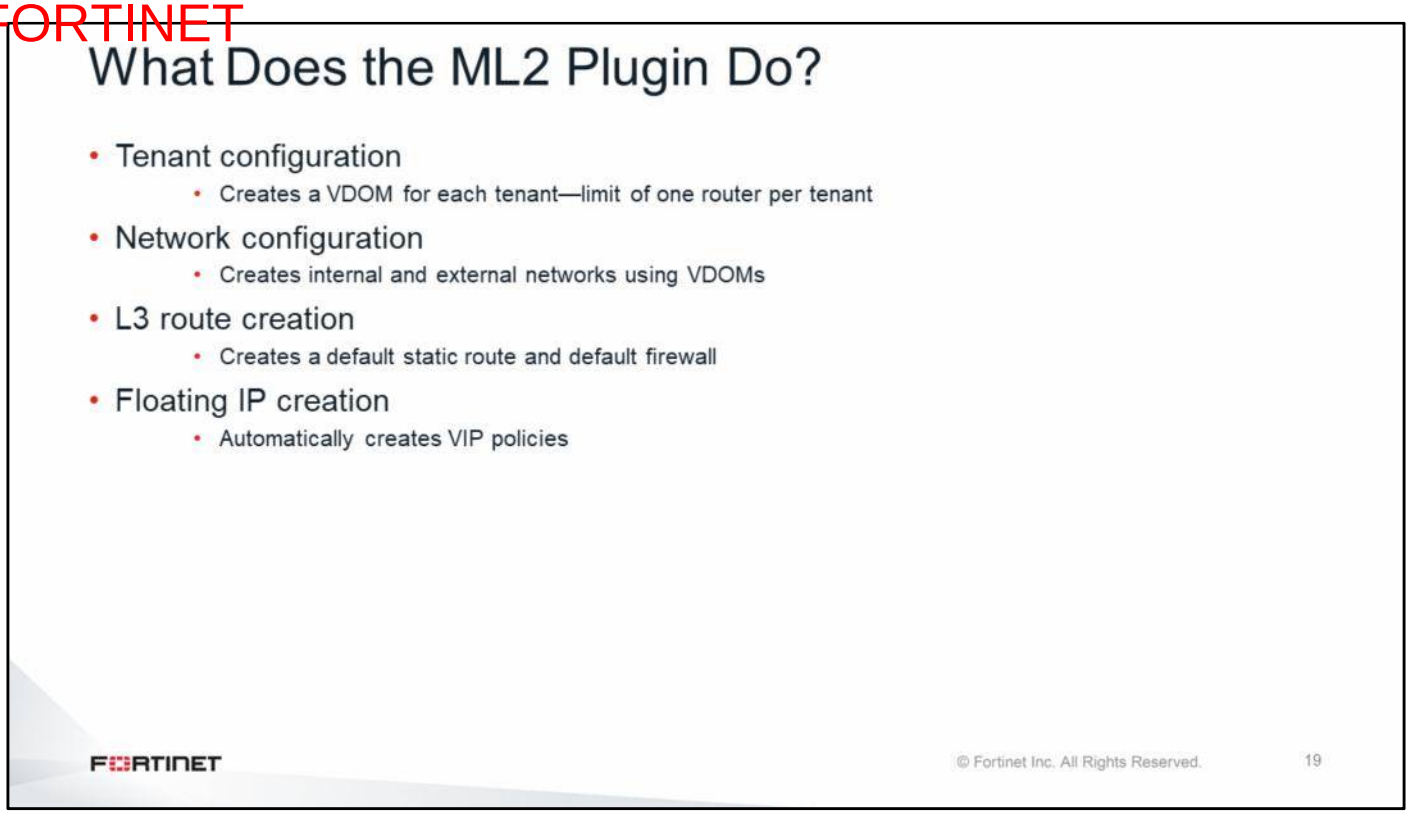


This is the topology where FortiGate acts as a network node. As shown on this slide, the compute node is connected to FortiGate. The FortiGate VDOM becomes the default gateway for VMs. It is important to know that Neutron is also present to provide other services. The controller node talks to Neutron, and Neutron provisions FortiGate. All traffic goes to FortiGate first, and then outside, without going through Neutron. Neutron is present only to provide services other than routing. FortiGate provides layer 3 services, and NP6 acceleration reduces the latency.



What does the FortiGate ML2 plugin provide?

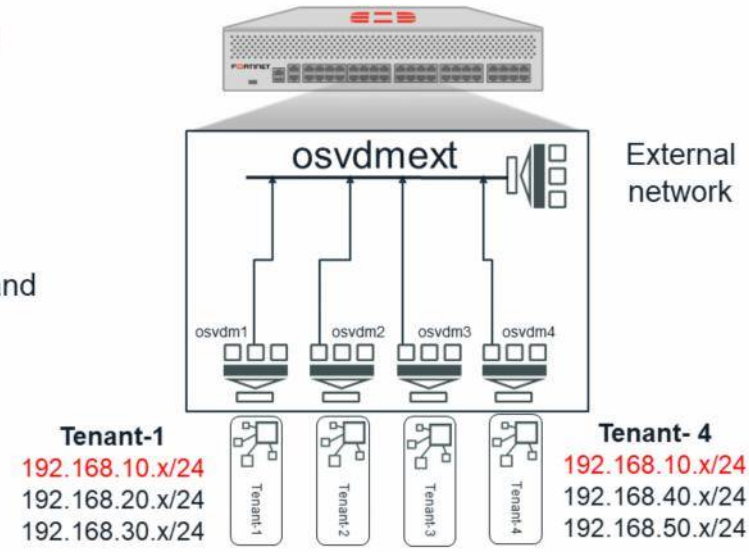
- **Advanced capabilities**: The FortiGate Neutron plugin, a modular layer 2 plugin, enables network layer 2/layer 3/DHCP/NAT function in the existing FortiGate firewall security appliance.
- **Best performance**: FortiGate devices have custom ASICs for optimum path processing, so switching is no longer a bottleneck.
- **Reduced cost**: Running a firewall on FortiGate is much cheaper than running firewall services in Linux, in terms of performance. In Linux, a stack of many servers is needed to get the same performance as a single FortiGate.
- **Orchestration and automation**: The orchestration of network security becomes an easy task; as you add tenants, a firewall policy is created. All tasks can be done using Horizon and there is no need to create them on FortiGate. As soon as you create firewall policies and security profiles on the tenant, Horizon automatically creates those policies and profiles on FortiGate.



What does the ML2 plugin do? The ML2 plugin creates tenant configurations. As soon as you create a tenant on OpenStack, it creates a corresponding VDOM on FortiGate. It also deploys network configuration, such as routing, DHCP, VIPs, IP pools, and so on. Creating network configuration on Horizon creates internal and external networks. Layer 3 route creation creates a default static route and default firewall. Floating IP creation creates VIP and policies on FortiGate.

FortiGate ML2 Architecture

- An external VDOM is automatically created
- Maps one tenant to one VDOM
  - VDOMs are named osvdm{x}
- Inter-VDOM links between tenant and external VDOM
- Supports overlapping IP networks



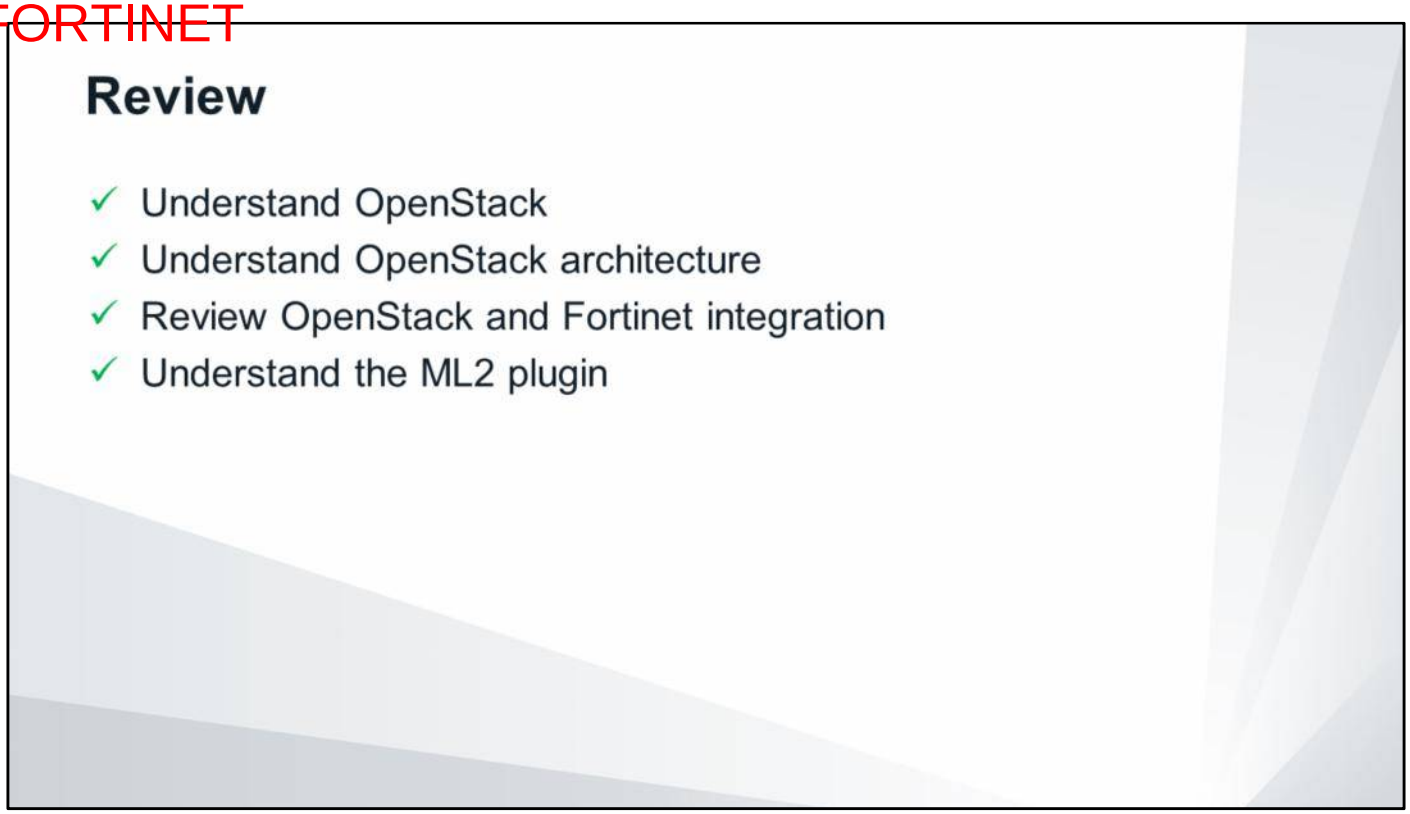
 20

This slide shows the topology of the FortiGate ML2 architecture.

When you deploy OpenStack with the FortiGate ML2 plugin, a default VDOM is created to use as an external VDOM. The external VDOM is responsible for connecting to the Internet, MPLS links, and so on. There is one VDOM per tenant, and the tenant VDOM can connect to the external VDOM through VDOM links. Also, the inter-VDOM links can facilitate the connection between tenants, and the VDOMs are named `osvdm1`, `osvdm2`, `osvdmext`, and so on.

Overlapping IP networks are supported between tenants. For example, Tenant-1 and Tenant-4 can have the same overlapping network (`192.168.10.x/24`).

Note that creation of the VDOMs and other settings are done automatically on the FortiGate.



This slide shows the objectives that you covered in this lesson.

By mastering the objectives covered in this lesson, you learned how to integrate FortiGate devices with OpenStack.