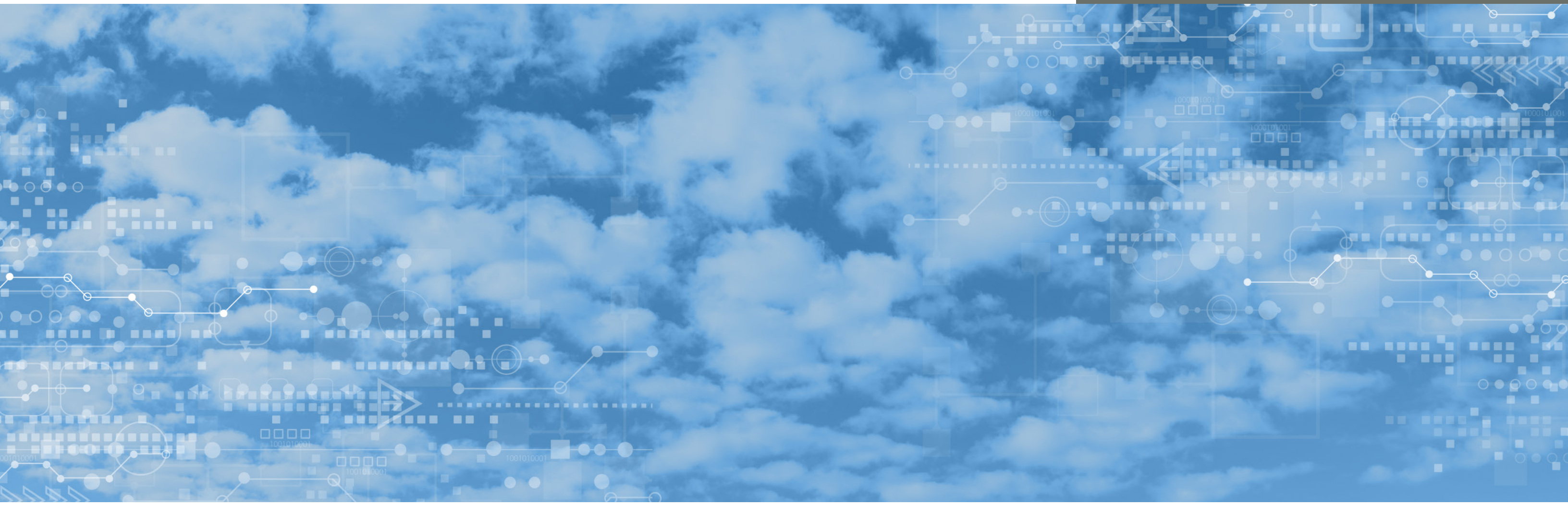
FORTINET

WHITE PAPER



Securing the Cloud

In the emerging digital economy, organizations are driving business value by using technology to connect users, devices, data, goods, and services. Organizations that want to compete successfully in this new economy are adopting new architectures, such as virtualization and cloud, that make them more agile, more responsive to customer needs and market demands, and more relevant to their customers.

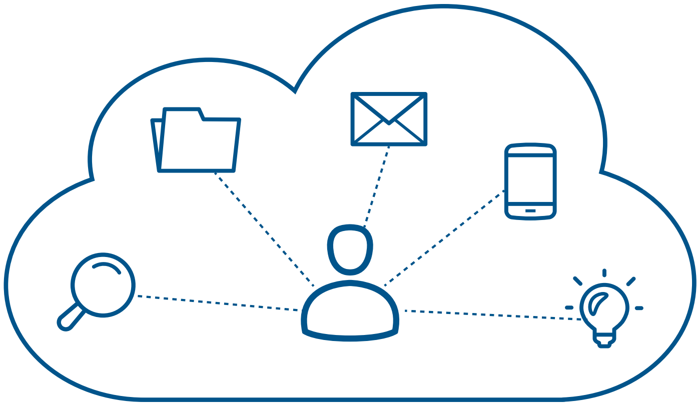
One of the initial drivers of this change was the need for on-demand computing resources to meet the growing demand for data by new users, applications, and devices while controlling overhead. Data centers are expensive to build and operate. And because data doesn't flow at a consistent rate, organizations are faced with the dilemma of either building a very expensive data center where most of the available resources go largely unused (while still needing constant power and cooling) waiting for peak demand, or building a more cost-effective one designed for normal usage that becomes bottlenecked during business-critical data and transaction spikes.

Virtualization, followed by cloud and software-defined networking (SDN), was created to provide the sort of on-demand resources digital businesses demand. What device data is on is less important than that it is available whenever it is needed, regardless of where the user, device, or application requesting it is located.

The adoption of on-demand, location-independent computing environments has affected every aspect of the distributed network. It also represents a number of distinct security challenges that cannot be addressed with the traditional approach of building a network and then bolting on security as an afterthought. When a new virtual server or workload is provisioned, for example, the network needs to intrinsically understand critical security issues, like what devices and applications are allowed to talk to this virtual machine, and where is it allowed and not allowed to send data? The answer to these questions grows exponentially more complicated as more virtual devices are added, and removed, from the environment.

Securing these highly dynamic environments requires tightly integrated security and network technologies that share intelligence, and collaborate to detect, isolate, and respond to threats in real time. Security solutions need to meet extreme performance requirements and be available on-demand, and they need to be provisioned and deprovisioned in real time as the environment they are protecting adapts to demands.

Of course, the problem becomes more complicated when you consider that the cloud is not just a virtualized traditional network. It is a collection of networks working in a synchronistic fashion. Data needs to moves between data centers in order to be delivered to highly mobile users and customers. Some of these data centers are local, some are geographically dispersed, and some are owned and maintained by third-party service providers. Here is a simple overview of some of the more common cloud environments organizations are adopting and the security challenges they represent:



Virtualization and Private Clouds

Even though virtualization has been underway in many organizations for some time, it is still a vulnerable and largely unprotected area of many networks. A strategy for securing virtualized environments needs to take a number of things into account.

The first is that about 75% of all data traffic flows laterally, or east/west inside the data center between traditional and virtual devices. At any given time, these transactions contain business-critical data, including personally identifiable information (PII) of employees and customers, financial transaction data, and intellectual property. Most of this data is unsecured and uninspected, as most organizations have designed their security to simply inspect the 15% of traffic that flows into and out of, or north/south, of the data center. When a threat actor manages to bypass the perimeter security, they can often collect and exfiltrate data at their leisure. In fact, most data center breaches remain undetected for weeks or months.

Further complicating the problem, a bit over 40% of organizations adopting virtualization end up deploying multiple hypervisors, the technology that creates and manages virtual machines and virtual networks. To ensure seamless and consistent security between these virtualized environments, security solutions need to be able to share intelligence, orchestrate responses to threats, and provide consistent policy enforcement. And they need to operate across all the major hypervisor operating systems.

Another challenge is that some virtualization solutions create a gap between physical and virtual resources. Security needs to bridge that gap to ensure consistent threat awareness and security enforcement regardless of the sort of devices that are processing data.

A number of new attacks have been targeted specifically at virtual machines, as well as virtual rootkits designed to mask their presence. In many organizations, traffic between virtual machines is rarely inspected, leaving virtual machines, workloads, and transactions highly vulnerable to attack.

Finally, virtualization allows for the rapid deployment of new workload resources and dynamic scalability to manage unexpected data bursts. Security for virtualized environments needs to be provisioned quickly, and scale rapidly so that critical business transactions and workflows are never interrupted or needlessly rerouted for inspection.

An integrated, fabric-based security approach allows organizations to create, orchestrate, and enforce seamless security policies between their physical, virtual, and private cloud environments, as well as providing uniform security along the data path from remote user to the cloud.

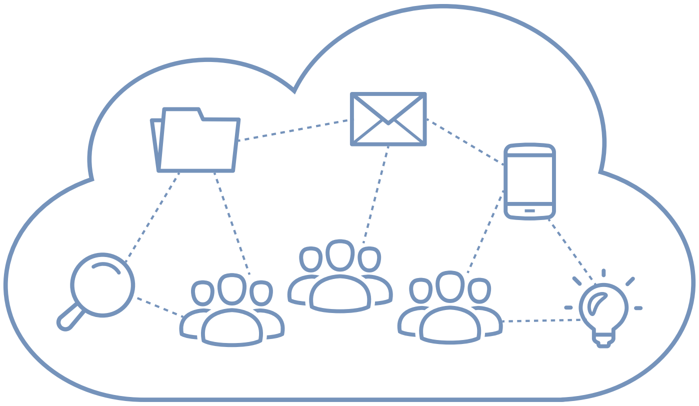
Next-Gen Data Centers

Beyond virtualization, organizations are beginning to plan and implement next-gen, software defined networks and private cloud environments. These new architectures allow for instantaneous provisioning of resources, chaining together of services, and the acceleration of workflows while abstracting away the overhead related to managing the physical layer of ports, servers, and switches.

These new data centers require purpose-built security solutions designed for their unique architectures. However, these new environments also run alongside traditional data centers, making the deployment and orchestration of a single security standard difficult. To complicate things further, some SDN solutions make it difficult to bridge between virtual and physical environments, so establishing and enforcing consistent security policies for data that flows between these domains can be challenging.

The advantage is that being able to stitch security services directly into transaction chains allows security to operate inline to automatically provision East-West security and to dynamically scale security resources as demand ebbs and spikes.

As with virtualization, a security fabric strategy allows organizations to place a variety of purpose-built security devices into different architectural environments, yet still maintain centralized threat intelligence and consistent policy enforcement.



Public Cloud

In addition to corporate data that moves between traditional and private cloud environments, many organizations are adopting public cloud services for everything from on-demand offloading of high-volume traffic, a process known as cloud bursting, to moving some or all of their infrastructure into the cloud with some sort Software, Platform, or Infrastructure as a Service (XaaS) architecture.

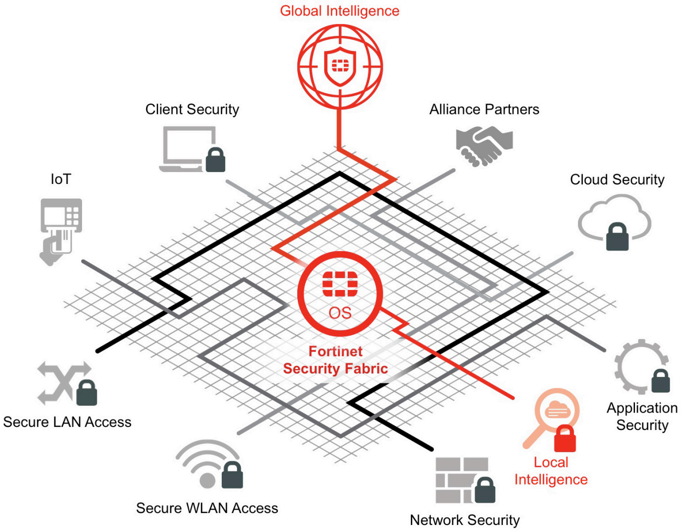
This can range from utilizing public cloud application services such as dropbox and salesforce.com, to cloud-based infrastructures such as Amazon AWS and Microsoft Azure, to complete turn-key cloud infrastructures provided by Telcos, to simplify the storage, transfer and management of data.

From a security perspective, the primary challenge is how to establish and maintain consistent security policy and policy enforcement as data moves back and forth between locally and third-party cloud environments. This is the single most critical gating factor preventing organizations from adopting an XaaS network strategy.

For this to work, two things need to happen. First, organizations need to find and work with a service provider who can assign to the remote cloud environment the same security technology being used in-house. Which also means that organizations need to deploy an in-house security solution that has been widely adopted by the service provider community. And second, they need to adopt a cloud-based security management and orchestration tool that can pass policy and security intelligence seamlessly between security devices deployed across distributed environments.

The Fortinet Security Fabric

Fortinet's Security Fabric provides market-leading security solutions for each of these virtualization and cloud environments, including the most widely adopted service provider security solutions in the market. Using a cloud-based management tool (FortiManager), a common operating system (FortiOS), and a single threat intelligence source for consistent enforcement (FortiGuard), organization can weave together a single, integrated security fabric for complete visibility and control across the entire distributed network environment.



GLOBAL HEADQUARTERS
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
www.fortinet.com/sales

EMEA SALES OFFICE
905 rue Albert Einstein
Valbonee
06560, Aples-Maritimes,
France
Tel: +33.4.8987.0500

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730

LATIN AMERICA SALES OFFICE
Paseo de la Reforma 412 piso 16
Col. Juarez
C.P. 06600
México D.F.
Tel: 011-52-(55) 5524-8428

April 22, 2016