FORTINET

WHITE PAPER

Securing Dynamic Cloud Environments

Developing Your Solution Checklist in a Changing Paradigm

Cloud computing has transformed how we consume and deploy IT solutions. Compute power is rapidly evolving to a utility model, with shared infrastructure at its core. This shared infrastructure underpinning the cloud revolution has also driven a fundamental shift in how we design and deploy technology within the data center. Servers, storage, networks, even the data center itself has moved beyond physical limits to become virtualized services residing on physical hardware. With this new virtual shared infrastructure model, comes new risks.

According to IDC, 75% of organizations are implementing or considering the implementation of public cloud. Further, they predict that 50% of enterprise workloads will migrate to public cloud by 2018. At the same time, the threat environment is only expanding, and it is no longer the traditional hacker breaching the network perimeter that drives those who manage network security. East-west traffic, traffic between systems inside the network, now dominates the corporate data flow. Hybrid cloud environments link corporate systems and applications to external data sources and customers. Private cloud deployments serve up compute power as a service to application developers deploying new functionality to both internal and external users. The network design paradigm for the data center is now flatter. The net result: once breached, the network is exposed to threats which can remain hidden, lurking or dormant for days or weeks, waiting for the right moment to wreak havoc or steal confidential data. It is just this type of threat that weighs heavily on the minds of those tasked with cloud security.

For those seeking to tackle this challenge, we outline here the key elements to consider in a cloud security solution. Keeping in mind that the first order may not only be to prevent a breach, but also to assume there will be one, and ensure that elements of a cloud solution can remain resilient and protected.

Public Cloud Security

Public cloud security represents the most high-profile security concern. Both business leaders and users have only recently overcome the inherent skepticism of sharing systems and bandwidth with unknown third parties. Concerns over cloud security, until very recently, had been a reason why many were slow to adopt public cloud options. For effective public cloud security, there are two key elements that must be addressed: a shared security model and provider integration.

Shared Security Model – The shared security model not only has to be the approach security teams adopt when securing the cloud, but the solutions companies deploy must be flexible enough to support the deployment of security functionality in a shared model. The shared security model consists of two key components. Security “of” the cloud, which includes all of the data center components on the cloud provider side of the equation, and security “in” the cloud which consists of what you as the cloud subscriber are responsible for providing in terms of your data and applications in the cloud. The components which must be addressed by a solution on the customer side are; your data and applications, operating systems, access and identity management, encryption and network traffic. On the provider side, a solution must integrate with the cloud providers’ security framework protecting the compute power, storage, and networking as well as provide a common dashboard to view both sides and manage all aspects of the solution.

Answering these threat questions will provide a starting point for security professionals to define the requirements of an IoT security solution. Transforming the IoT frontier into a hardened perimeter or at least gaining the visibility to see threats coming and be able to react to and prevent an attack is the baseline for any new solution.

Provider Integration – Beyond defining the areas of responsibilities and making sure there are no gaps in protection, to ensure public cloud security, solutions must be tightly integrated with the public cloud provider. Public cloud security cannot follow the old paradigm of deploying appliance-based solutions or host-based agents. These solutions cannot cover the end to end visibility across all nodes and typically cannot scale with the elasticity required for a cloud solution. For example, users of Amazon Web Services are familiar with the concept of “security groups” to manage basic segmentation, but even AWS recommends using third-party security to add functionality like application control, antivirus, web filtering, DLP and threat research. In the context of public cloud, these solutions must auto-scale with the cloud, based a template approach to provide a level of high availability and performance as cloud resources expand dynamically. For users leveraging Microsoft Azure, a security solution must plug and play with the APIs for Microsoft Azure Resource Manager to fully take advantage of the security functionality.

Private Cloud Security

At the foundation of private cloud is virtualization. In fact, virtualization serves as the building block enabling all forms of cloud computing. Virtualization has ushered in a computing environment more focused on software. It is this shift to a softwarecentric approach that any cloud security solution must take into account.

Software Defined Security - With the growth of Software Defined Networking (SDN), much like cloud itself, networking resources are no longer physically tied to dedicated hardware. Network resources operate as services in the data center, and as such may span physical elements or locations. A cloud security solution must be designed with this in mind, without the requirement to deploy hardware only appliance-based approaches to secure resources. Security functionality must become "services" that can be dynamically configured and provisioned.

Application Centric Security – All applications are not created equal. While many share the same physical infrastructure in a private cloud, they do not meet the same risk profile. This means segmentation is critical, and the security solution must be aligned to the application. Any cloud-based security solution must be able to isolate data and applications as the data center continues to consolidate. As east-west traffic increases in software-defined environments, micro-segmentation, the ability to segment specific types of traffic, also becomes critical.

Does Your Solution Meet the Functionality Requirements of Public, Private, and Hybrid Cloud?

Public Cloud Security

- Shared Security Model
- Provider Integration

Private Cloud Security

- Software Defined Security
- Application Centric Security

Hybrid-Cloud

- Single-Pane Management
- Segmentation
- Secure Connectivity

Hybrid Cloud

Hybrid cloud presents perhaps the most challenging problem when determining the best security solution. With resources spanning both assets you control and either public cloud infrastructure or specific SaaS or data resources, visibility is paramount so the security team can see the entire picture end-to-end. End-to-end management, segmentation and securing external connections become the most critical elements of a hybrid cloud security solution.

Single-Pane Management – With resources spread across both the physical and virtual realm, security professionals can't be bouncing back and forth between dashboards for visibility, or operate without central analytics for threat intelligence. Point solutions with separate management interfaces will not suffice. A cloud security solution must integrate a single view across all systems operating in the cloud with centralized management. This single pane management approach must allow you to track data flows across the entire network in a format which makes that information relevant and actionable. It should also incorporate centralized threat intelligence, informing decisions based on what's happening both on your network and in the outside world.

Segmentation – Segmenting systems and traffic within and across the cloud is most critical when internal resources sit on a network open to the public or third parties. In these inherently mixed environments which include both permanent external connections and temporary data movement, business units and critical applications not directly associated with the hybrid environment must be segmented to minimize the impact if there is a breach.

Secure Connectivity – Any Hybrid solution must allow for robust VPN functionality, including the ability to provide secure temporary access to resources when needed while protecting the rest of the network. Migrating data between locations, loading large data sets from external sources, taking advantage of third party cloud based analytics services, all require discreet connections to external networks which carry with them unique risks. A solution must have the ability to provide the right protection based on the risk profile of these unique network connections.

Security Matching the Cloud Paradigm

In addition to protecting the cloud in its various deployments, public, private, and hybrid, a cloud security solution must also operate to match the nature of cloud itself, as an elastic, dynamic resource that can change rapidly. The solution must address three key aspects of cloud.

Scalable - Since the cloud is dynamic, and scalability is core to the motivation of many users to move solutions to the cloud, the design of a security solution should match the scalability and elasticity of cloud workloads. Solutions that are static, or lack automation, requiring intervention to expand or adapt new requirements, make security a hindrance to achieving the full value of cloud solutions. When evaluating a cloud security solution, automation must be at the heart of the solution. Risk and access policies must also be defined in advance so that when new devices enter the network to accommodate more users or additional bandwidth in the cloud environment, the devices will be automatically configured. Can the solution scale to match the elasticity and dynamic growth of a cloud environment?

Consistent – Threats thrive on finding the right opportunity at the right time. Often, that means exploiting inconsistencies in policies or policy enforcement to gain entry to your network. Cloud raises this need for consistency to a new level. Cloud introduces new variables such as temporary or recurring connections to outside resources and the dynamic expansion and contraction of resources as dictated by demand. Policy, enforcement and the automation that executes both must be consistently applied across both static and dynamic resources. Workloads or systems categorized with a common risk profile must be treated the same as they enter or exit the network, regardless of whether they are in your data center or your providers. Can you maintain consistency in policy enforcement, visibility, and protection across the cloud?

Segmented – Whether its minimizing business risk or meeting regulatory requirements, the cloud introduces new elements into the security protocol. The ability to segment systems, workloads, or even specific network components is critical to managing business risk. Cloud also introduces new risks for compliance. When data can traverse not only your network but leave your network via the public cloud, data compliance must be enforced to ensure you can monitor and control specific traffic, applications or data types. Proper segmentation for cloud solutions also means the ability to inspect persistent traffic between segments of the cloud to protect against data leakage and make sure data is routed based on risk and policy. Can you separate critical systems, workloads, and applications based on unique risk profiles?

Does Your Solution Map to the Cloud Security Paradigm?

Scalable

Can the solution scale to match the elasticity and dynamic growth of a cloud environment?

Consistent

Can you maintain consistency in policy enforcement, visibility, and protection across the cloud?

Segmented

Can you separate critical systems, workloads, and applications based on unique risk profiles?

Conclusions

Cloud computing has changed the paradigm for IT and security professionals. The days of networks having well-defined perimeters, where protection was focused solely on external threats pounding at the firewall door, is over. Cloud security solutions must address the unique requirements of each variant of cloud computing. Public, with its reliance on shared infrastructure and the need to operate in a shared security model. Private, with the inherent risks posed by east-west traffic and virtualized services requiring a software-defined approach to security. And hybrid cloud, posing the challenge of combining critical internal resources with external connections and data sources, increasing the need to segment resources on the network.

At the same time, a solution must match the scalability of the cloud, consistently applying policies and enforcing them across segmented resources both internally and externally. With this combination of functionality and approach, a solution can meet the challenges of cloud security while enabling the organization to reap the benefits of cloud and minimize the business risks of shared public infrastructure.

FORTINET

www.fortinet.com

October 12, 2019 12:39 AM

122915-B-0-EN

D:\Fortinet\White Paper\refresh - Securing Dynamic Cloud Environments\wp-securing-dynamic-cloud-environments