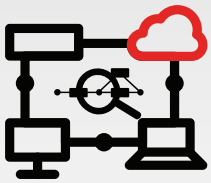
WHITE PAPER

Securing Hybrid and Multi-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, and even the data center itself have moved beyond physical limits to become virtualized services residing on physical hardware. With this new virtual shared infrastructure model come new risks.



According to the Flexera 2021 State of the Cloud Report, 92% of enterprises already have a multi-cloud strategy in place, with 80% using a hybrid cloud strategy.

According to the Flexera 2021 State of the Cloud Report, 92% of enterprises already have a multi-cloud strategy in place, with 80% using a hybrid cloud strategy. The report also notes that 61% of organizations plan to optimize cloud costs in 2021, making it the top initiative for the fifth year in a row. With the need to support applications located across multiple points of deployment across data centers, hybrid clouds, and multi-clouds, the threat environment continues to expand. 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 that 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 that 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 providing a common dashboard to view both sides and manage all aspects of the solution.

Cloud-native 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, data loss prevention (DLP), and threat research. In the context of public cloud, these solutions must auto-scale with the cloud, based on a template approach to provide a level of high availability and performance as cloud resources expand dynamically. For users leveraging Microsoft Azure, for example, a security solution must plug and play with the application programming interfaces (APIs) for Microsoft Azure Resource Manager to fully take advantage of the security functionality.

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

Private Cloud Security

At the foundation of private cloud is virtualization. In fact, virtualization serves as the building block that enables all forms of cloud computing. Virtualization has ushered in a computing environment more focused on software. It is this shift to a software-centric 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, microsegmentation, the ability to segment specific types of traffic, also becomes critical.

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 Software-as-a-Service (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 track data flows across the entire network in a format that makes that information relevant and actionable. It should also incorporate centralized threat intelligence, informing decisions based on what's happening both on the 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 virtual private network (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 datasets from external sources, and taking advantage of third-party cloud-based analytics services all require discreet connections to external networks that 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, adaptive resource that can change rapidly. The solution must address four key aspects of cloud: It must be scalable, consistent, segmented, and adaptive.

Scalable: Because 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?

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?

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 a 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 provider's. Are consistency in policy enforcement, visibility, and protection across the cloud maintained?

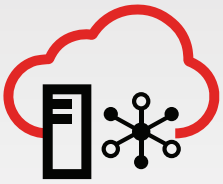
Segmented: Whether it's minimizing business risk or meeting regulatory requirements, the cloud introduces new elements into the security protocol. The ability to segment systems, workloads, or even specific network components is critical to managing business risk. Cloud also introduces new risks for compliance. When data can traverse the network and also leave it via the public cloud, data compliance must be enforced to ensure monitoring and controlling specific traffic, applications, and 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. Are critical systems, workloads, and applications based on unique risk profiles segmented?

Adaptive: Digital innovations equals cloud transformation. With any transformation journey, things change. As a result, cloud security must also be equally adaptive to those changes. This allows organizations to freely choose the right platform or cloud infrastructure for their needs, be it cloud, data center, hybrid, multi-cloud, or SaaS, without worrying about limitations to securing those applications. Can the cloud security solution follow applications and their data to any cloud? And, is there the flexibility to shift cloud strategies and readily secure those changes easily without taking on additional complexity or sacrificing security?

Conclusion

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, are 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.



Cloud security solutions must address the unique requirements of each variant of cloud computing.

For more information, contact sales@spectrotel.com | 877.542.9200

FORTINET

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 13, 2021 1:11 PM

D:\Fortinet\Work\2021\0513\wp-securing-hybrid-and-multicloud

122915-C-0-EN