CHECKLIST

Essential Guidelines to Protecting Your Application Deployments Across Clouds and Data Centers

A recent Fortinet survey found that nearly seven out of 10 companies use two or more cloud providers, while many also maintain data centers and branch offices.[1] The new reality isn't cloud computing or even multi-cloud computing—the new reality is the use of complex, hybrid infrastructures that are expected to be able to adapt to rapidly changing business needs. This complexity demands a more holistic security solutions, one that is able to deliver state-of-the-art security wherever the compute occurs.

This requires a new approach to network security, one in which network security tools such as firewalls along with supporting management and analytics platforms work together in a mesh or a fabric. This new approach is called a hybrid mesh firewall (HMF), a unified security platform that provides coordinated protection to multiple areas of enterprise IT, including corporate sites, such as branches, campuses, and the data center.

How Are You Protecting Your Application Deployment?

At the core of any organization's digital acceleration initiatives is the application journey. Organizations are planning and executing projects to build, deploy, and run applications on one or more clouds and in on-premises virtual data centers. From a security perspective, the key initiatives for application deployment involve creating a secure transport to access cloud applications and data from anywhere, providing advanced security in the cloud to protect and get visibility everywhere, and lastly establishing a homogenous network with a consistent security posture across diverse cloud and on-premises deployments.

Secure connectivity into the cloud

The primary goal is to provide an encrypted high-speed connection for application traffic and sensitive data between on-premises locations like branches and data centers, and also to connect remote workers to the public cloud virtual network where the application workloads are running. These connections are typically based on VPN technology where a number of spoke locations connect to a hub location or VPN gateway located in a cloud virtual network. Increasingly, organizations are looking to replace VPN with a faster and more agile option. Choose a gateway solution that offers Secure SD-WAN to provide a faster, more intelligent and application-aware transport that delivers better application experiences for users.

Secure perimeter in the cloud

Providing a security boundary around data and application infrastructure in the cloud offers a line of defense both to improper access to sensitive information and the exfiltration of information outside the organization. Perimeters can be implemented in the cloud in a similar way to their usage on-premises. The perimeter can be enhanced by integration with cloud-native constructs and cloud-provider security services. Choose a network security solution that factors in elastic scaling, depth of inspection, flexibility, and customization of policies, canned policies, performance, and reliability.

Secure networking across clouds and data centers

Complexity is the enemy of security. The proliferation of compute platforms, both on-premises and off, can lead to complex array of incompatible security systems that overwhelm staff and lead to security failures. It is important for organizations to reduce operational overhead and management complexity by utilizing products and services that remove the need for multiple disjointed cloud-provider consoles. A key part of this is the deployment of next-generation firewalls (NGFWs) that can be woven into an HMF infrastructure and managed through a single management interface. Another key aspect to be wary of is network and security policies fragmentation across cloud deployments and on-premises locations. Choose a solution that provides SD-WAN connectivity across multiple clouds and virtual data centers, and also offers continuous visibility into threats across clouds and on-premises locations.

Top Three Considerations to Secure Your Cloud Network

☑ Can the solutions be deployed on any cloud or data center?

Ensure the solutions you are choosing to secure the network can extend to all the environments where your applications run.

There is a broad array of public cloud providers and virtualization platform vendors that organizations use for hybrid-cloud and multicloud application deployment. It is important that organizations do not limit themselves to security and connectivity tools and solutions available on specific clouds or virtualization platforms. On the contrary, they should use network security solutions that enable them to have the freedom of choosing the environments where they want to run their applications. Organizations should at all costs avoid the option of not implementing any security at all in the cloud hoping that the cloud is safe. That will be an expensive mistake that may damage the future of the organization.

The right network security solutions should lower cloud security operations friction; therefore, they should be integrated with the latest technologies and capabilities available from major cloud platforms like AWS, Azure, and Google Cloud for seamless security and deployments on these platforms. Solutions that provide a broad range of deployment flexibility and deep integration levels with major cloud platforms will help organizations future-proof their application journey investments, allowing them to readily adapt and expand their cloud security strategy as their needs evolve.

☑ Can the solutions support both security and networking?

The era of network and security silos is fading away fast as a new era of secure networking is being ushered in. The network presents one of the largest attack surfaces for any organization's IT infrastructure. Therefore, operating the network separately from security leads to security gaps and increased burden. This problem gets even bigger when the cloud becomes an integral part of the IT infrastructure.

Ideally, solutions should converge security and networking functions into one form factor and streamline network and security operations. This approach yields multiple benefits, including better security, integrated routing, unified management, and reduced training burden. Organizations will further benefit if these solutions implement packet-acceleration technologies to deliver high throughput and more bandwidth. Scaling up network performance is essential when the deployed applications themselves cannot be easily scaled out.

☑ Can the solutions support centralized management and visibility?

When it comes to IT infrastructure costs, the OpEx spend for management and operations between refresh timelines exceeds the CapEx spend. This problem is exacerbated when organizations are burdened with operating multiple disparate management tools, especially in cloud environments. In addition to the financial inefficiencies, these disconnected tools cause gaps in visibility that can hide critical vulnerabilities and may lead to damaging attacks and data breaches.

The right solution provides centralized security and networking management across all cloud and on-premises application deployments. It should also offer comprehensive and deep visibility into ingress and egress traffic in the IT infrastructure and block known and unknown threats.

Fortinet Cloud Network Security Secures Application Deployment across Clouds and Data Centers

Fortinet helps secure digital acceleration across clouds and data centers. We do this by offering cloud network security solutions that are natively integrated across major cloud platforms and technologies alongside the ability to extend your HMF from on-premises to the cloud. Fortinet's HMF infrastructure provides reduced operational complexity, greater visibility, and robust security effectiveness, delivering capabilities such as consistent policies across all hybrid and multi-clouds, centralized management, deep visibility across applications and workloads, and FortiGuard delivered protection and intelligence to protect deployment of any application on any cloud.

Fortinet Cloud Network Security also supports a wide range of deployment and consumption models. Our solutions are deployable directly from cloud marketplaces as virtual appliances. Additionally, our solutions are consumable as BYOL, PAYG, and as part of a flexible enterprise agreement program called FortiFlex.

[1] Fortinet 2023 Cloud Security Report, 2023.

June 29, 2023 5:05 AM

2243760-0-0-EN