SOLUTION BRIEF

Fortinet Adaptive Cloud Security Provides Seamless, Flexible Protection

Executive Summary

As much as public cloud use is growing, both in total volume and in diversification of services, it is not a one-way trend. To meet evolving business needs, organizations are moving applications and workloads back and forth between cloud and on-premises environments. This trend has been affirmed by 74% of respondents in a recent survey.[1] To minimize exploitable vulnerabilities in this dynamic environment, it is essential for security to closely track network traffic, application transactions, and cloud platform activity and configurations. Fortinet Adaptive Cloud Security meets this need, delivering natively integrated network, application, and platform security solutions to support and enhance digital innovation.

Meeting the Needs of Adaptive Cloud Networks

Leveraging the broad, integrated, and automated nature of the Fortinet Security Fabric, the Fortinet Adaptive Cloud Security solutions offer a consistent security posture and enforcement through uniform security management across any cloud or non-cloud infrastructure.

In private clouds: Fortinet network security solutions seamlessly integrate with infrastructure automation systems to enforce security policies that address the dynamic nature of virtual machines and other workloads.

In public clouds: Fortinet network, application, and platform security solutions integrate with cloud networking services. Cloud load balancing and platform application programming interfaces (APIs) provide comprehensive security that addresses the entire attack surface.

In Software-as-a-Service (SaaS) clouds: Fortinet provides visibility and control by connecting to the cloud API in order to mitigate risks associated with SaaS misconfigurations.

Consistent Protection Across All Major Clouds

The evolving threat landscape requires advanced threat protection that goes deep into encrypted traffic and uncovers zero-day threats. Augmenting the basic capabilities of native cloud provider security tools, Fortinet offers a broad set of security functions that includes the following:

Network Security With FortiGate VM next-generation firewalls (NGFWs)

- **Network segmentation** protects both cloud-to-internet (north-south) traffic and lateral cloud-to-cloud or internal (east-west) traffic with predictable application performance. Centrally managed through the Fortinet Security Fabric, Fortinet virtual NGFWs apply security policies consistently across hybrid multi-cloud environments. FortiGate VM solutions deployed in the public cloud can securely communicate and share consistent policies with FortiGate NGFWs of any form factor provisioned in a private data center.

A significant departure from point-product security approaches, Fortinet Adaptive Cloud Security helps organizations maintain consistent protection everywhere, enabling organizations to confidently run any applications anywhere.

Major Public Clouds Supported

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform
- Oracle Cloud
- Alibaba Cloud
- IBM

Private Cloud Technology Vendors Supported

- VMware
- Microsoft
- Xen
- KVM
- Cisco
- OpenStack

- **Advanced threat prevention**, leveraging functionality such as FortiGate VM application control and intrusion prevention system (IPS), helps organizations effectively block application layer threats from propagating and harming cloud-based infrastructures. FortiGate VM advanced threat prevention capabilities are very effective in blocking known attacks.
- Secure software-defined wide-area network **(Secure SD-WAN)** combines intelligent WAN path selection and security functions in a single cloud-based solution. Fortinet Secure SD-WAN helps organizations simplify cloud connectivity while maintaining security and reducing costs, whether they are using it to connect branches to the cloud or for interconnection between clouds and data centers.

Web application security with FortiWeb web application firewalls (WAFs)

Employing a multilayered, machine learning (ML)-enabled approach, FortiWeb defends both web applications and externally facing APIs from known (e.g., OWASP Top 10) and zero-day threats. Using ML, FortiWeb identifies anomalous behavior and distinguishes between malicious and benign anomalies. This results in improved accuracy and considerable time savings compared to the manual application learning required by most WAFs. Additionally, advanced bot mitigation capabilities allow benign bots, such as search engines, to connect, while blocking malicious bot activity. Finally, accommodating a variety of customer requirements, FortiWeb is offered as an easy-to-consume SaaS, as a Docker container, or as a virtual machine (VM).

Consumption Models for Fortinet Adaptive Cloud Security

Fortinet Adaptive Cloud Security includes FortiCWP, FortiWeb, and FortiGate VM, which are available in multiple form factors such as virtual machines, SaaS, and Docker containers to best suit customer needs and use cases. Additionally, various solutions are available as bring-your-own-license (BYOL) options. These may be purchased through the regular cloud supply chain, typically as perpetual licenses or as pay-as-you-go (PAYG) offerings that can be consumed on-demand.

Cloud platform security management with FortiCWP and FortiCASB

Organizations pursuing digital innovation transformations are also relying on cloud workloads and SaaS applications to speed and scale the DevOps and business productivity and operational needs. In order to move fast while moving securely, organizations need deep visibility and security controls into workloads, containers, and SaaS applications. These insights help security administrators and DevOps teams efficiently evaluate their cloud configuration security postures, detect potential threats originating from misconfiguration of cloud resources, identify policy violations, and generate compliance reports.

Wide Range of Form Factors and Options Reduces TCO

Fortinet Adaptive Cloud Security solutions are designed to secure any application on any cloud. They are available for a broad range of resource and performance requirements. These range from very small footprint virtual machines, which maximize the benefits of scale-out architectures, to large footprint virtual machines that take advantage of high-capacity network acceleration technology on the different cloud platforms and allow for support of large-scale network processing for stateful applications that cannot be properly designed using scale-out architectures.

In addition to virtual machines, Fortinet Adaptive Cloud Security solutions form factors also include SaaS, Docker containers, and appliances, giving organizations the freedom to choose the solution form factors that best suit customer needs and use cases.

Consumption models are also a key part of digital innovation strategic decisions for many organizations. Enabling consistent and efficient risk management in multi-cloud infrastructures, various solutions are available as bring-your-own-license (BYOL) options. These may be purchased through the regular cloud supply chain, typically as perpetual licenses or as pay-as-you-go (PAYG) offerings that can be consumed on-demand.

Native Integration Optimizes Security Across Hybrid Multi-cloud Ecosystem

Security gaps arise because of incompatibilities between cloud and on-premises environments as well as between cloud-specific tools and purpose-built security tools. To minimize these gaps, the Fortinet Security Fabric provides architectural consistency by means of cloud-specific integrations. These integrations relieve security staff of the burden of knowing the specific object types and naming conventions of each cloud environment. These are replaced by a single intuitive configuration interface. Fortinet offers three types of integrations:

- **Fabric Connectors** translate cloud-specific security objects and service names into a consistent format for defining security policies throughout the Fortinet Security Fabric.
- **Fabric APIs** standardize the programming of security operations across Fortinet products deployed in the cloud and on-premises.
- **Configurable automated responses** to security events observed by Fortinet products can trigger remediation actions directly onto the different cloud platforms, leveraging serverless functions without the need for deep cloud expertise on the part of the security operator.

Fortinet developed all its connectors and APIs in close collaboration with the cloud service providers and regularly updates them in line with changes in each cloud environment.

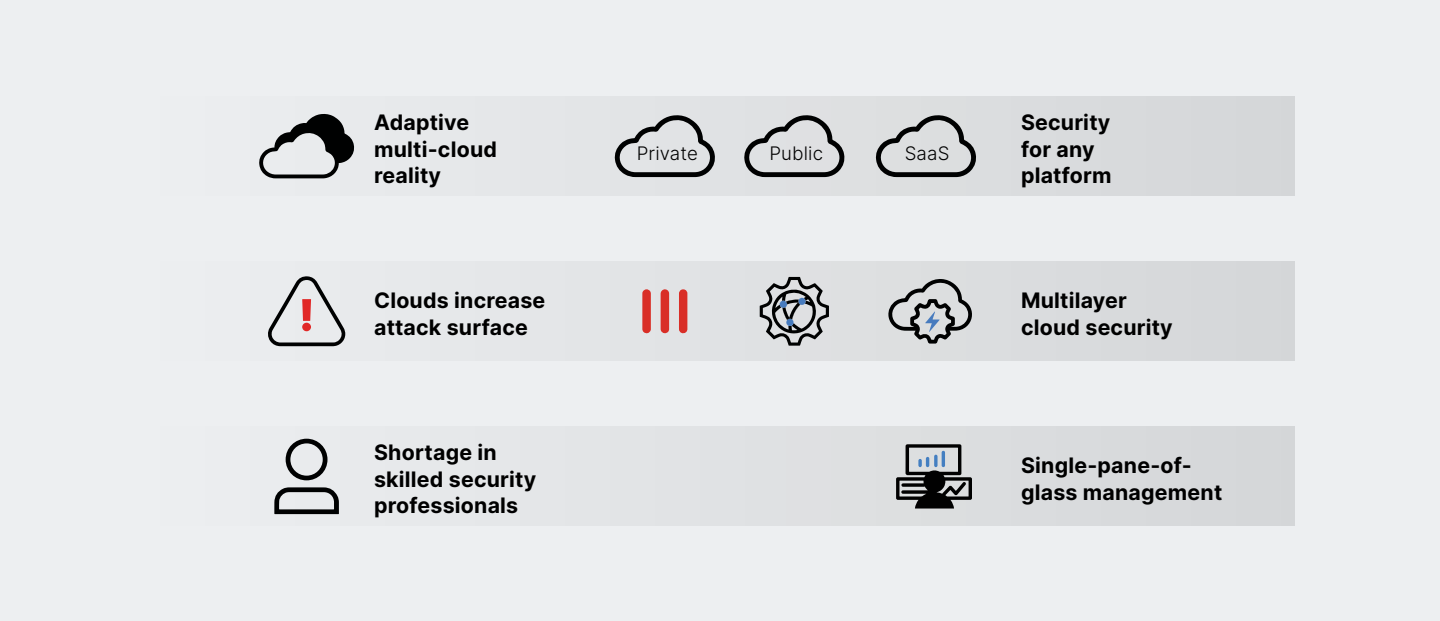

Figure 1: Fortinet Adaptive Cloud Security unlocks business agility.

Management and Automation

Because organizations face accelerating threats and a persistent shortage of skills with which to address them, Fortinet Adaptive Cloud Security offers security management and automation capabilities that uniformly span cloud environments. These capabilities help gain the right level of visibility across the multi-cloud infrastructure, which is essential to define meaningful policies and ultimately gain control over the infrastructure.

Fortinet Adaptive Cloud Security management and automation solutions help security administrators and operators streamline routine operations through a single pane of glass. They also include APIs that help DevOps and DevSecOps teams automate security operations for all routine actions without cloud-specific customizations. In addition to driving operational efficiencies, these tools reduce training and staffing costs, as the same security skills can be leveraged across all clouds. Ultimately, Fortinet Adaptive Cloud Security solutions help organizations maintain a higher security posture at the network level, the application level, and the cloud platform level with minimal overhead.

Investment-worthy Security Solutions

Digital innovation requires security that can keep up with adaptive cloud infrastructures. Fortinet Adaptive Cloud Security solutions offer the following advantages to organizations looking to deliver value quickly and over the long term:

- The ability to scale from the smallest building block units to the largest high-capacity network virtual appliances (NVAs)
- Easy adaptability to a variety of use cases, as well as business- and application-specific security needs
- Security technologies that leverage the latest advances in ML and artificial intelligence (AI) to provide adaptive cloud infrastructures continuously optimized web application protection from rapidly evolving threats
- A truly synergetic security fabric approach that spans network, application, and cloud platform security into a single framework, making business networks more secure and less prone to human error

Fortinet ranks #1 in the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.[2] This record of success, together with Fortinet's commitment to deep ongoing investment in cloud security, gives security leaders the confidence to leverage Fortinet Adaptive Cloud Security solutions to deploy any application on any cloud.

[1] "The Bi-Directional Cloud Highway: User Attitudes about Securing Hybrid- and Multi-Cloud Environments," IHS Markit, Q2 2019.

[2] "20 Years: Two Decades of Cybersecurity Innovation," Fortinet, Q1 2021.

FORTINET

www.fortinet.com

April 22, 2021 9:06 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\April\Refresh\Fortinet Dynamic Cloud\sb-FA-fortinet-adaptive-cloud-security-4222021\sb-FA-fortinet-adaptive-cloud-security-4222021

500499-A-0-EN