SOLUTION BRIEF

Fortinet Cloud Security Solutions

Executive Summary

Organizations have embraced the reality that to achieve their digital acceleration goals of today and tomorrow, their applications must live anywhere needed to deliver upon their business outcomes. This means that applications can live anywhere across data centers, multi-clouds, and edge compute.

Unfortunately, such distributed and porous environments can result in significant complexity and risks on top of those already being faced by organizations, including the cybersecurity skills, people resource shortage, and lack of a cohesive, converged security solution. The result is significant headwinds and barriers to digital acceleration.

As part of Fortinet Universal SASE, Fortinet Cloud Security Solutions empower organizations with consistent, secured, and optimized tools to build, deploy, and run cloud applications across all deployments wherever their applications will live.

"Misconfiguration of cloud security remains the biggest cloud security risk according to 59% of cybersecurity professionals... followed by exfiltration of sensitive data (51%), insecure interfaces/APIs (51%), and unauthorized access (49%)."[1]

Application Journey Challenges

The desire for digital acceleration has led organizations to drive toward delivering faster and better application experiences and to bring applications and data closer to users and devices. Previously, most people thought this application journey was unidirectional, migrating from on-premises to the cloud. However, many organizations now realize that application journeys are much more fluid in practice in that applications can live anywhere from the data center to hybrid and multi-clouds to edge compute. The reason for this is simple: Applications need to live wherever they deliver the most optimal desired business outcomes. Such outcomes include customer experience, performance, cost optimization, and more.

Unfortunately, this fluid environment creates challenges for CIOs and CISOs alike. They must address even greater challenges in securing their networks because of the now more porous environment. These challenges include increased operational complexity, visibility gaps, an explosion of cloud platforms and tools, and "accidental multi-clouds."

These added challenges further exacerbate existing operational issues. According to the 2023 Cloud Security Report, a global survey of over 750 cybersecurity professionals conducted by Cybersecurity Insiders, the top challenges organizations face are:

- Lack of visibility (32%)
- Lack of consistent security policies (32%)
- Lack of staff resources or expertise (43%)[2]

Organizations are also all at different stages of their application journey; many are still unsure where their application journey will take them. In response, Fortinet Cloud Security Solutions empower organizations with the flexibility to secure applications wherever they may be deployed and the flexibility to evolve as their application journey progresses.

Secure Data Center, Cloud, and Edge Compute Networks with FortiGate

FortiGate is a next-generation network firewall (NGFW) solution that is deployable in the cloud and on-premises at physical and virtual data centers or private clouds. It is available as a high-end hardware appliance that is built for the demands of a data center or as a virtual appliance that offers the flexibility to extend the same technology into virtual data centers and cloud networks.

All FortiGates are powered by FortiOS, the world's most widely distributed security operating system, regardless of the form factor. This provides consistent policies no matter where the application needs to be deployed, which often reduces operational complexities in multi-cloud and hybrid-cloud deployments.

Additionally, FortiGate firewalls are the only solution that delivers secure multi-cloud SD-WAN connectivity and can orchestrate between all cloud and hybrid-cloud instances to help provide the best application experiences possible.

Secure Web Applications and APIs with FortiWeb

FortiWeb web application firewall (WAF) protects business-critical web applications from attacks that target known and unknown vulnerabilities. Advanced machine learning (ML)-powered features improve security and reduce administrative overhead. Capabilities include anomaly detection, API discovery and protection, bot mitigation, and advanced threat analytics to identify the most critical threats across all protected applications. FortiWeb also offers threat analytics to consolidate raw event data into a clear picture of the most significant threats.

FortiWeb is available as a hardware appliance, virtual appliance, cloud-hosted Software-as-a-Service (SaaS), and containerized solution.

Secure Clouds Natively with FortiCNP and FortiGate CNF

FortiCNP is a cloud-native protection platform natively integrated with cloud service providers' (CSP) security services and the Fortinet Security Fabric to deliver a comprehensive, full-stack cloud security solution for securing cloud workloads. FortiCNP patented Risk Resource Insights (RRI) technology simplifies security by contextualizing security findings and prioritizing the most critical resources with actionable insights to help security teams effectively manage cloud risk. Native integrations with CSP security services, such as Amazon GuardDuty Malware Protection and Amazon Inspector, and Fortinet Security Fabric solutions, deliver real-time threat protection with zero-permission security coverage. Ultimately, this helps reduce complexity and overhead in cloud operations, increasing security teams' efficiency and effectiveness.

FortiCNP also helps organizations secure their data and containers in the cloud. It detects and protects against malware, sensitive data, data loss, and misconfigurations in cloud storage repositories. FortiCNP also protects against vulnerabilities in container images and registries throughout the application life cycle; integrations with Kubernetes environments continuously monitor risk posture and activity for new and evolving threats.

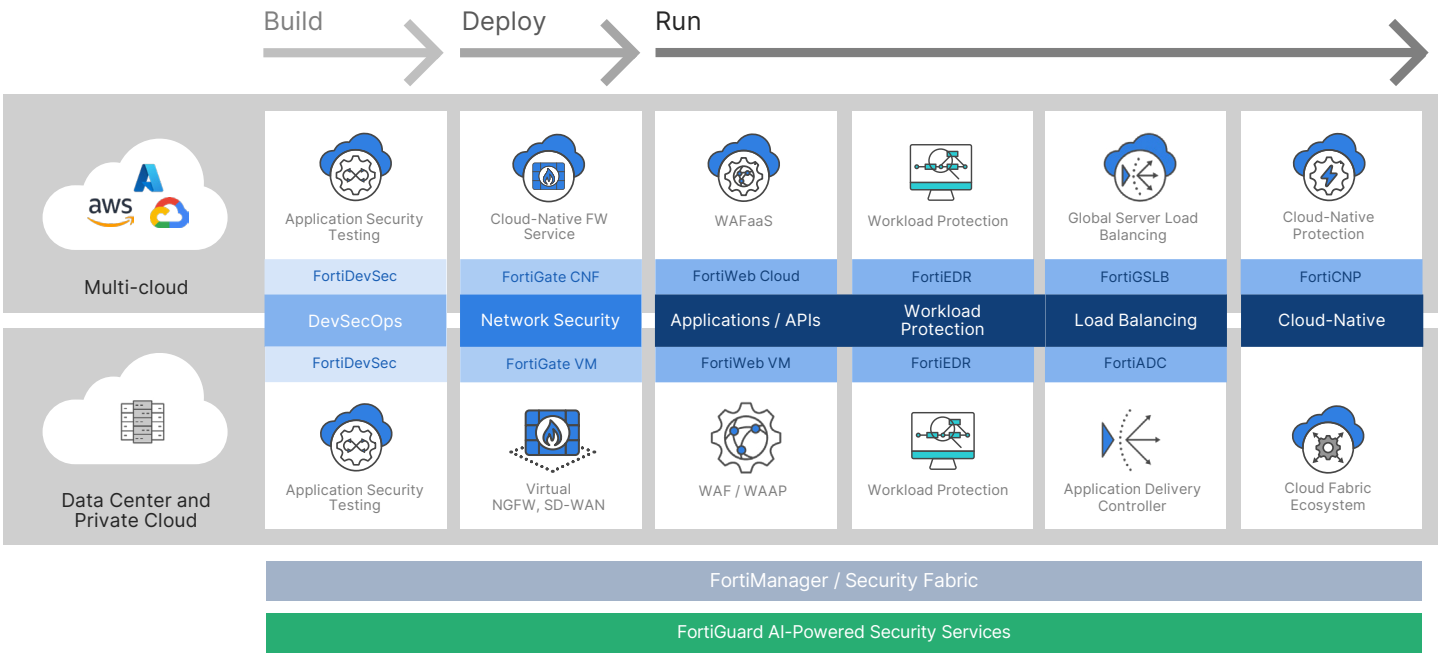
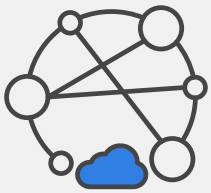


Figure 1: Consistent, secured, and optimized experience to build, deploy, and run cloud applications across all cloud and hybrid deployments

For organizations looking to further simplify their cloud operations, FortiGate CNF is a cloud-native firewall service that allows organizations to offload the management of their own cloud network security infrastructure and, in turn, lower costs. Security teams are then able to focus on the things that matter most: configuring policies and securing their cloud networks and applications. FortiGate CNF is also powered by FortiOS and offers the same industry-leading network firewall capabilities as FortiGate hardware appliances and VMs.



"90% of cybersecurity professionals want a single cloud security platform for consistent security policy across all cloud environments."[3]

Secure Workloads with FortiEDR

In addition to securing workloads with FortiCNP, Fortinet also helps organizations better secure their critical workloads with FortiEDR endpoint detection and response that can be deployed with the workload itself, offering deeper visibility and protection. FortiEDR delivers innovative endpoint security with real-time visibility, analysis, protection, and remediation. As proven in MITRE ATT&CK Evaluations, FortiEDR proactively shrinks the attack surface, prevents malware infection, detects and defuses potential threats in real time, and automates response and remediation procedures with customizable playbooks.

Secure and Optimized Application Delivery with FortiADC and FortiGSLB

FortiADC enhances your applications' scalability, performance, and security, whether hosted on-premises or in the cloud. Our advanced application delivery controller optimizes application performance and availability while securing the application with both its native security tools and by integrating application delivery into the Fortinet Security Fabric.

FortiADC provides unmatched application acceleration, load balancing, and web security, regardless of whether it is used for applications within a single data center or serves multiple applications for millions of users around the globe. FortiADC includes application acceleration, WAF, IPS, SSLi, link load balancing, and user authentication in one solution. The solution delivers availability, performance, and security in a single, all-inclusive license.

FortiGSLB Cloud is a DNS-based service that helps ensure business continuity by keeping applications online and available when a local area experiences unexpected traffic spikes or network downtime. FortiGSLB enables organizations to deploy redundant resources around the globe to maintain the availability of mission-critical applications.

Simplified and Secure Application Journeys

With broad coverage of application journey use cases and form factor options that allow organizations to deploy Fortinet Cloud Security Solutions anywhere their applications need to live, Fortinet helps organizations achieve their digital acceleration goals while lowering complexity and risks.

Integrated with the Fortinet Security Fabric, a broad, integrated, and automated cybersecurity mesh platform, Fortinet Cloud Security Solutions offer organizations centralized visibility and management, automation across all solution points, and intelligence sharing for the fastest response to threats. Ultimately, this reduces complexities, solves for cloud cybersecurity skills and resource gaps, and increases overall security effectiveness.

Fortinet Cloud Security also supports a wide range of deployment and consumption models. Our solutions are deployable directly from cloud marketplaces, as physical and virtual appliances, and as SaaS-based and cloud-native options. Additionally, our solutions are consumable as bring your own license (BYOL), pay as you go (PAYG), and as part of FortiFlex that is well-suited for dynamic environments where flexible scaling is needed.

FortiFlex delivers usage-based security licensing that moves at the speed of digital acceleration. It offers a simple, transparent, points-based approach to provide organizations with flexibility and agility to right-size their cybersecurity services and spend. Organizations can freely deploy cybersecurity from Fortinet and scale them up, down, in, or out dynamically, without excessive procurement cycles. When acquired through private offers from AWS, Azure, Google Cloud, and Oracle Cloud marketplaces, FortiFlex can help organizations draw down their committed minimum use obligations with these providers and extend the life of those dollars by up to 60 months.

Fortinet Secures Any Application Journey on Any Cloud

Delivering consistent, secured, and optimized experiences for organizations to build, deploy, and run cloud applications across all data center, cloud, hybrid, and edge compute deployments, Fortinet empowers organizations to achieve their digital acceleration goals for today and tomorrow. We do this by offering cloud security solutions that are natively integrated across major cloud platforms and technologies alongside the ability to extend the Fortinet Security Fabric across anywhere applications live. Together, these can give organizations greater visibility and robust security effectiveness for reduced operational complexity. And, with consistent security policies across all hybrid and multi-clouds, with centralized management and FortiGuard-delivered protection and intelligence, Fortinet Cloud Security helps organizations eliminate security and operational challenges that stand in the way of digital acceleration success.

[1] Cybersecurity Insiders, 2023 Cloud Security Report.

[2] Ibid.

[3] Ibid.

FORTINET

www.fortinet.com

December 13, 2023 3:37 PM

1852116-A-0-EN