SOLUTION BRIEF

Fortinet Secure Application Journey 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 and people resource shortage, and lack of a cohesive, converged security solution. The result is significant headwinds and barriers to digital acceleration.

Fortinet Secure Application Journey 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 62% of cybersecurity professionals… followed by **exfiltration of sensitive data** (51%), **unauthorized access** (50%), **and insecure interfaces/APIs** (52%)."[1]

Application Journey Challenges

The desire for digital acceleration has led organizations to drive toward delivering faster and better applications 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. Now, 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 exascerbate existing operational issues that organizations are already dealing with. According to the 2022 Cloud Security Report, a global survey of over 800 cybersecurity professionals conducted by Cybersecurity Insiders, the top challenges organizations face are:

- **Lack of visibility (49%)**
- **Not enough control (42%)**
- **Lack of staff resources or expertise (40%)**[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 Secure Application Journey solutions empower organizations with the flexibility to secure applications wherever they may be deployed, but also the flexibility to evolve as their application journey progresses in the future.

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. Regardless of the form factor, all FortiGates are powered by FortiOS, the world's most widely distributed security operating system. This provides for consistent policies no matter where the application needs to be deployed, which ultimately reduces operational complexities that often happen 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 deliver the best application experiences possible.

"**78% of cybersecurity professionals want a single cloud security platform** for consistent security policy across all cloud environments."[3]

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. Additionally, 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 as a 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, allowing security teams to increase their 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.

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.

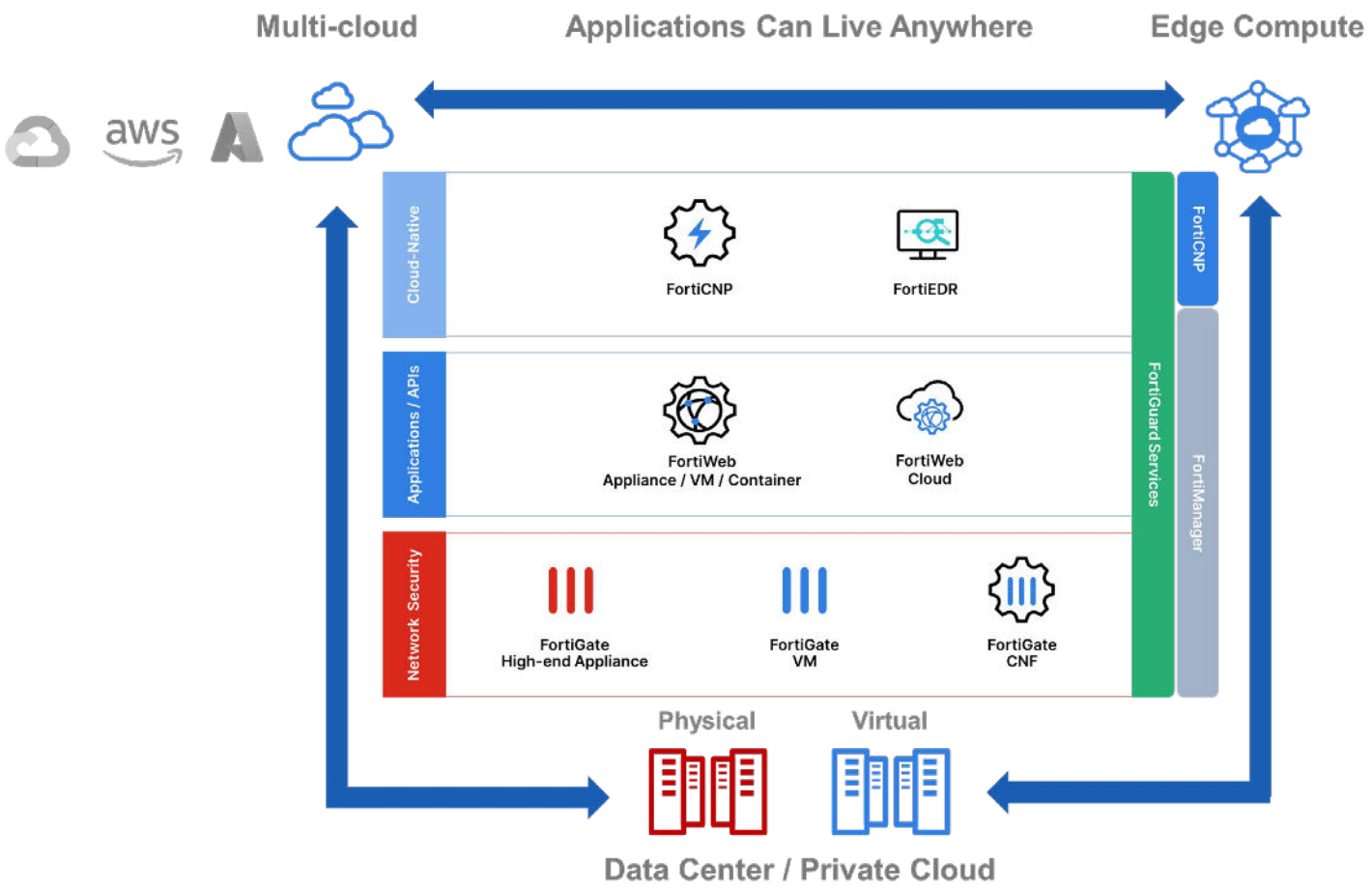

Figure 1: Consistent, secured, and optimized experience to build, deploy, and run cloud applications across all cloud and hybrid deployments

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 levels of 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.

Simplified and Secure Application Journeys

With broad coverage of application journey use cases and form factor options that allow organizations to deploy Fortinet Secure Application Journey 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 Secure Application Journey 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 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 provide organizations with greater visibility and robust security effectiveness for reduced operational complexity. Fortinet security solutions can provide consistent policies across all hybrid and multi-clouds, with centralized management and FortiGuard-delivered protection and intelligence.

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 an enterprise agreement program called Flex-VM that is well-suited for dynamic environments where flexible scaling is needed.

[1] 2022 Cloud Security Report, Cybersecurity Insiders.

[2] Ibid.

[3] Ibid.

www.fortinet.com

January 21, 2023 4:04 PM

1921638-0-0-EN