SOLUTION BRIEF

Using FortiCloud to Secure Your Cloud Infrastructure and Applications

Executive Summary

Proper security of cloud infrastructure and applications requires a solution that is purpose-built for the cloud and can be delivered, as a service, from the cloud. The FortiCloud offering suite protects your applications, your workloads, your data, and your email without up-front investment and without hardware. FortiCloud is ideal for organizations that need the agility and flexibility of cloud computing without sacrificing security.

The Challenges of Securing Cloud-native Applications

Many organizations are moving computing resources to the cloud to reduce capital expenses, become more agile, and take advantage of powerful services such as artificial intelligence (AI) engines and advanced analytics tools. Businesses of all sizes have found that the cloud allows them to leverage sophisticated applications without having to build and maintain their own data centers.

Cloud computing can be made as secure as on-premises infrastructure, but cloud also introduces a number of new security challenges. These include an expanded attack surface, the need to secure multiple apps that may reside on multiple clouds or that may span cloud and data center, and an overall shortage of skilled cloud security professionals.

Because cloud computing utilizes a host of new management, orchestration, and analytic systems and because the app and the user are not working within a secured network, cloud computing further expands the attack surface.

The attack surface is the sum of all the different vectors through which an attacker can penetrate, alter, or disrupt a computing system. Because cloud computing utilizes a host of new management, orchestration, and analytic systems and because the app and the user are not working within a secured network, cloud computing further expands the attack surface. What's more, application programming interface (API)-driven, cloud-native applications can be managed programmatically, creating yet another attack vector. Meanwhile, the prevalence of DevOps methodologies in cloud app development means that development teams with elevated privileges are posting new or updated applications—often without review by a team of security professionals.

To address new vulnerabilities introduced by cloud adoption, many organizations have deployed an array of disaggregated point security products. Upwards of 75 different security solutions are in use at the average enterprise—and many of these only address a single risk exposure or compliance requirement. Beyond the ongoing capital expenses of continuously buying new, one-off products, these different solutions typically do not communicate with each other—which increases management burdens while creating new security gaps for threats to slip through defenses. A cohesive approach is needed for organizations to manage cloud infrastructure and applications—one that relieves the burden on security teams, offers good ROI, and keeps organizations continuously compliant, secure, and resilient.

Securing Cloud-native Applications with Fortinet

Traditional security solutions are designed to establish a secure perimeter around your network. But in the age of the cloud this is impossible—the "perimeter" is everywhere. Instead, securing cloud-native applications requires solutions that are both built for the cloud and can be delivered from the cloud. Elements of cloud security include (but are not limited to):

- Application protection
- Workload and storage protection
- Email protection
- Securing SaaS apps such as Microsoft 365 and Salesforce
- Configuration and compliance management
- Sandboxing
- Advanced threat protection with real-time threat feeds backed by machine learning and artificial intelligence
- Central management and analytics

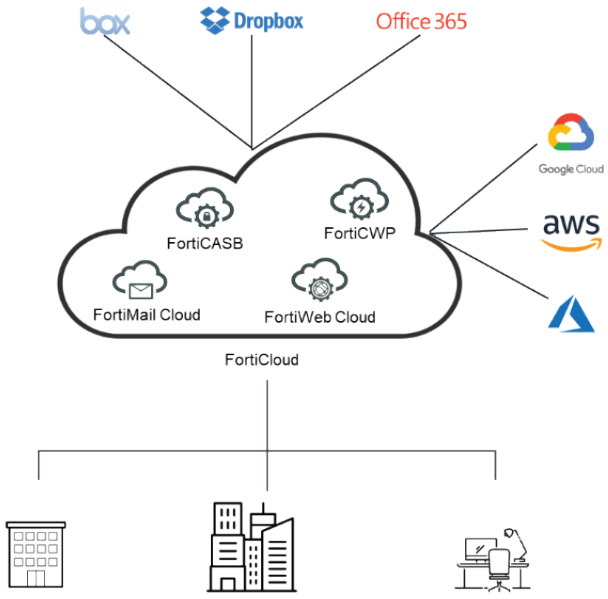

Figure 1: Securing cloud-native applications with Fortinet.

Unlike competitive approaches, FortiCloud addresses all elements of securing cloud-native applications and it does so in a manner that is both effective and scalable. FortiCloud provides tools that deliver security-as-a-service, such as FortiWeb Cloud and FortiCASB, tools that manage other security tools, such as FortiGate Cloud and FortiManager, and tools that are used for tracking assets, licenses, and return merchandise authorizations (RMAs), such as FortiCare.

As a full solution, FortiCloud is an important part of the Fortinet Security Fabric, which ties Fortinet security solutions together to collect, coordinate, and respond to malicious behavior wherever it occurs.

Cloud security may only be one part of the broader issue of cybersecurity, but its importance can't be overstated. Key components of the FortiCloud offering suite for cloud security include the following.

The full Fortinet Security Fabric covers:

- Endpoint client security
- Secure wired, wireless, and VPN access
- Network security
- Data-center security (physical and virtual)
- Application (OTS and custom) security
- Cloud security
- Content (email and web) security
- Infrastructure (switching and routing) security

FortiWeb Cloud

Designed for web applications that demand the highest level of protection, FortiWeb Cloud provides robust security that is simple to deploy, easy to manage, and cost-effective. With FortiWeb Cloud, DevOps teams and security architects alike have access to the same proven detection techniques used in other FortiWeb form factors without the need for costly capital investments. Unlike solutions that simply spin up virtual machines for each customer and increase the management workload on already-stretched teams, FortiWeb Cloud delivers a true Software-as-a-Service (SaaS) solution that leverages the leading public clouds to offer highly scalable and low-latency application security.

At the heart of FortiWeb is an AI-based detection engine that uses ML to identify requests that stray from normal patterns, taking action to protect applications from known and unknown zero-day threats. FortiWeb also integrates with FortiSandbox, which further utilizes AI to detect new or previously unknown threats as well as the MITRE ATT&CK Framework, OWASP Top 10 vulnerability inspection, and real-time threat feeds from FortiGuard Labs.

FortiWeb will protect web-based applications and the APIs they rely on. FortiWeb Cloud is a true SaaS application, delivered from the cloud, allowing you to pay only for what you use, and requiring no additional hardware.

FortiCWP

FortiCWP offers security administrators and DevOps teams the ability to evaluate their cloud configuration security posture, detect potential threats originating from misconfiguration of cloud resources, analyze traffic across cloud resources (in and out of the cloud), and evaluate cloud configuration against best practices. It enables the ability to manage risk throughout multi-cloud infrastructures, provides regulatory compliance reporting, and integrates remediation into the cloud infrastructure life-cycle automation framework.

FortiCASB

FortiCASB is a Fortinet-developed cloud-native cloud access security broker (CASB) subscription with an extensive set of cloud security posture management (CSPM) capabilities that are designed to provide visibility, compliance, data security, and threat protection for cloud-based services employed by an organization. FortiCASB provides policy-based insights into users, behaviors, and data stored in major SaaS applications as well as comprehensive reporting tools. FortiCASB offers a full API integration with leading SaaS and cloud services including Microsoft Office 365, Microsoft OneDrive, Google Drive, Salesforce.com, Dropbox, and Box as well as compliance reporting and Shadow IT detection.

FortiCASB offers a full API integration with leading SaaS and Cloud services including Microsoft Office 365, OneDrive, Google Drive, Salesforce.com, Dropbox, and Box as well as compliance reporting and shadow IT detection.

FortiMail Cloud

FortiMail Cloud delivers comprehensive email security to protect your employees and data from cyberattacks. It provides the industry's most independently validated security effectiveness.[1] Delivered as a SaaS solution, it is easy to enable and requires minimal ongoing management—most of which can be easily extended to end-users. FortiMail delivers a greater-than-99.5% spam detection rate and multiple layers of malware detection, all with extremely few false positives. Fully managed by Fortinet, FortiMail Cloud allows you to focus on your business while Fortinet secures your email.

FortiSandbox

Top-rated AI-powered FortiSandbox is part of the Fortinet breach protection solution that integrates with the Fortinet Security Fabric platform to address rapidly evolving and more targeted threats including ransomware, crypto-malware, and others across a broad digital attack surface. Specifically, it delivers real-time actionable intelligence through the automation of zero-day, advanced malware detection and response. FortiSandbox improves zero-day threat detection efficacy and performance by leveraging two ML models—patent-pending enhanced random forest with boost tree and least squares optimization applied to static and dynamic analysis of suspicious objects. It also accelerates threat investigation and management processes by adhering to standards based on the MITRE ATT&CK framework for malware reporting.

Next steps

FortiCloud is ideal for organizations that need the agility and flexibility of cloud computing without sacrificing security. By providing security-as-a-service, management of other security tools, and tracking for licenses and other assets, FortiCloud offers a full solution for securing cloud-native applications, especially when delivered as part of the full Fortinet Security Fabric.

[1] "Email Security Services Protection," SE Labs, January-March 2020.

FORTINET

www.fortinet.com

June 14, 2020 10:35 PM

697050-0-0-EN

D:\Fortinet\Work\2020\June\061420\sb-forticloud