SOLUTION BRIEF

Cloud-native Solution for Web Application Security: FortiWeb Cloud WAF-as-a-Service for AWS, Azure, Google Cloud, and Oracle Cloud

Executive Summary

FortiWeb Cloud Web Application Firewall-as-a-Service (WAFaaS) delivers full-featured, cost-effective security for web applications with a minimum of configuration and management. Delivered through major cloud platforms, including AWS, Azure, Google Cloud, and Oracle Cloud, FortiWeb Cloud features a high level of scalability as well as on-demand pricing. While FortiWeb Cloud can protect applications deployed in the data center or in the cloud, customers who host their applications on these public clouds can achieve benefits such as reduced latency, simplified compliance, and lower bandwidth costs.

Securing Web Applications

Cloud service providers and application owners share the responsibility for securing web applications deployed to the cloud. This arrangement has advantages in that providers typically deploy robust security for the platform itself, removing that burden from the application owner. However, securing the application itself rests squarely with the owner, a stipulation that AWS[1] and other providers make clear in their service agreements.

Best practices for web application security include the deployment of a WAF as the cornerstone of a comprehensive security solution. WAFs use a combination of rules, threat intelligence, and heuristic analysis of traffic to ensure that malicious traffic is detected and blocked before reaching web applications.

The task of protecting on-premises application software typically falls to a security architect or other security professional within the CIO or CISO organization. In contrast, the DevOps team often fills this role for cloud-based applications, consistent with DevOps principles of end-to-end responsibility and cross-functional, autonomous teams. As a result, DevOps teams need the right tools to embed effective security controls into their process—simply repurposing traditional workflows and processes will not do the job. Also, the additional workload of managing WAFs consumes valuable time on the part of DevOps teams and can elongate time-to-release cycles and inhibit continuous improvement efforts.

FortiWeb Cloud Features

- Advanced protection against OWASP Top 10 threats, zero-day threats, and more
- Purchasing flexibility—buy directly through a cloud marketplace or your preferred reseller
- Easy deployment with a setup wizard and predefined policies
- Streamlined management with an intuitive dashboard for end-to-end security visibility and management
- Delivered on public cloud, including AWS, Azure, Google Cloud, and Oracle Cloud, which offers low latency and unmatched elasticity and scalability

The Expanding Attack Surface

The threat landscape today can be daunting for organizations considering a move to the cloud. More than three-quarters of successful attacks are motivated by financial gain,[2] which can take the form of ransomware, exfiltration of valuable personal information, or compromised intellectual property. Furthermore, breaches happen fast—87% take place in just minutes[3]—and most go undiscovered for months or more (Figure 1).[4]

Figure 1: Threat statistics from recent published studies.

Internet-facing web applications pose unique security challenges compared to traditional solutions deployed within the organization's network perimeter. Every time a company deploys a new internet-facing web application, the attack surface grows. As DevOps teams accelerate the rate of development and new releases, the attack surface evolves more rapidly than ever. This expanded attack surface challenges traditional approaches to application security.

Enhanced Protection With FortiWeb

To address the diverse needs of organizations for web application security, Fortinet offers the FortiWeb family of solutions. FortiWeb WAF provides advanced features that defend web applications from known and zero-day threats. Using an advanced multilayered and correlated approach, FortiWeb delivers complete security for external and internal web-based applications from the OWASP Top 10 and many other threats. At the heart of FortiWeb are its dual-layer artificial intelligence (AI)-based detection engines that intelligently detect threats with nearly no false-positive detections.

FortiWeb Cloud WAF-as-a-Service

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, FortiWeb Cloud delivers a true Software-as-a-Service (SaaS) solution that leverages public cloud to offer highly scalable and low-latency application security.

FortiWeb VM

FortiWeb VM is an enterprise-class offering that provides the FortiWeb functionality in a virtual form factor. Designed for hybrid environments, the virtual version of FortiWeb includes protection for container-based applications. FortiWeb VM can be deployed in VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, and Docker platforms.

Advanced Protection

Using the multilayered and correlated approach of a full enterprise-class WAF, FortiWeb Cloud protects web applications from the OWASP Top 10 threats[5] and more. Specifically, FortiWeb Cloud safeguards applications from vulnerability exploits, bots, malware uploads, distributed denial-of-service (DDoS) attacks, advanced persistent threats (APTs), and zero-day attacks.

A significant pain point associated with many WAF solutions is the large number of false positives, which can add management overhead for busy DevOps staff and increase the chances that a real vulnerability is left undetected. However, FortiWeb Cloud uses machine learning (ML)-enabled technology to minimize false positives while accurately identifying real threats.

Attacks/Threats	Application
Botnets, Malicious Hosts, Anonymous Proxies, DDoS Sources	IP Reputation
Application-level DDoS Attacks	DDoS Protection
Improper HTTP RFC	Protocol Validation
Known Application Attack Types	Attack Signatures
Viruses, Malware, Loss of Data	Antivirus/DLP
FortiGate and FortiSandbox APT Detection	Integration
Scanners, Crawlers, Scrapers, Credential Stuffing	Advanced Protection
Unknown Application Attacks With Machine Learning	Behavioral Validation

Correlation

User/Device Threat Scoring

Figure 2: Common attack vectors and remediation techniques.

Easy to Deploy and Manage

FortiWeb Cloud enables rapid application deployments in the public cloud while addressing compliance standards and protecting business-critical web applications. To facilitate use by nonsecurity professionals, FortiWeb Cloud comes with a setup wizard and a default configuration that can be easily modified to meet individual requirements. FortiWeb Cloud delivers cloud-native application security that can be deployed in minutes. After going through the setup wizard, simply update your DNS setting and your web application is protected.

Busy DevOps staff have no time for extensive WAF training. To address this issue, FortiWeb Cloud features an intuitive real-time dashboard that allows DevOps staff and other nonsecurity professionals to see and understand quickly the security status of their web applications (Figure 3).

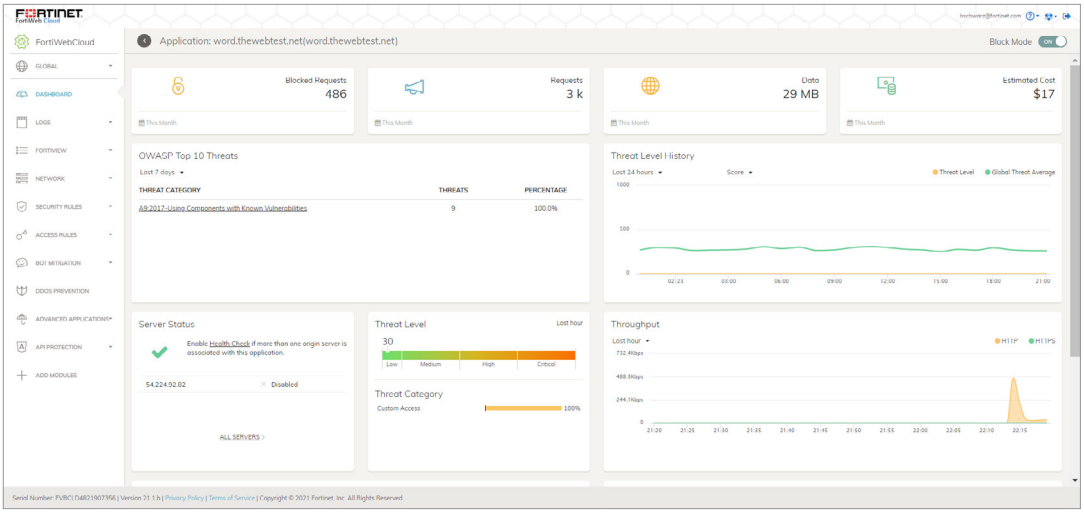

Figure 3: FortiWeb Cloud dashboard.

Cost-effective Security

As a cloud-native SaaS solution, FortiWeb Cloud features lower capital expenditures (CapEx) and operational expenditures (OpEx) compared to on-premises solutions. AWS, Azure, Google Cloud, and Oracle Cloud provide the hardware and software components of the infrastructure, virtually eliminating the need for capital investments as well as the operating costs associated with platform maintenance. By removing the burden of maintaining and upgrading the platform, customers can focus on improving the application and delivering business value to their organizations.

The SaaS business model—pay only for what you use—gives customers flexibility in managing their security budgets as well as the ability to institute chargebacks and other cost-control measures. Customers who host their applications on these clouds can reduce costs significantly because they must only pay data transfer fees for traffic from the application to the WAF—as the data transfer costs for outbound traffic are included in the FortiWeb subscription (Figure 4).

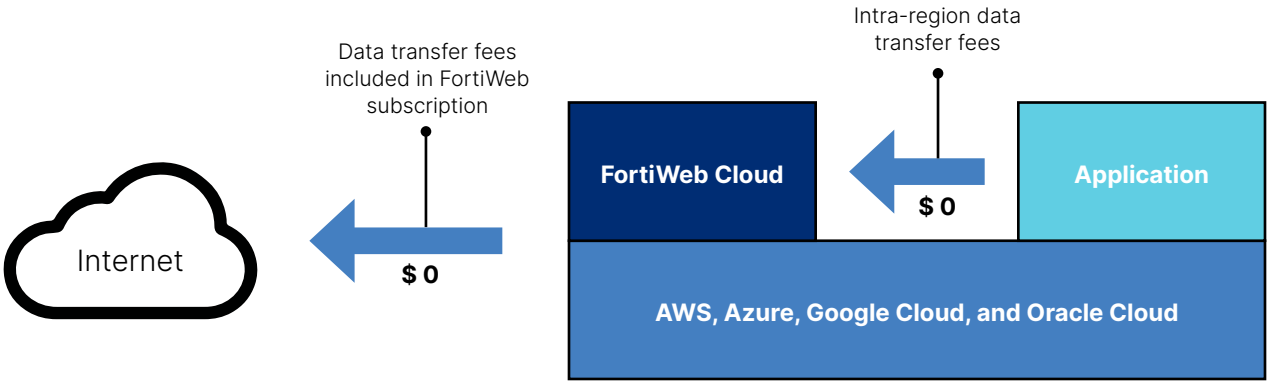

Figure 4: Data transfer fees for applications hosted on public clouds.

Conclusion

Utilizing a comprehensive, correlated, multilayer approach to web application security, FortiWeb Cloud protects web-based applications from all of the Top 10 OWASP security risks and many more. Unique among WAFs on the market, FortiWeb Cloud leverages ML capabilities to detect both known and unknown exploits targeting web applications with almost no false positives. Delivered via public cloud providers including AWS, Azure, Google Cloud, and Oracle Cloud, FortiWeb Cloud features low latency and high elasticity and can easily and quickly scale to accommodate changes in traffic. Further, FortiWeb Cloud keeps web applications safe from vulnerability exploits, bots, malware uploads, DDoS attacks, APTs, and zero-day attacks.

[1] "Shared Responsibility Model," AWS, accessed June 20, 2019.

[2] "2018 Data Breach Investigations Report," Verizon, accessed June 18, 2019.

[3] Ibid.

[4] Ibid.

[5] "OWASP Top 10-2017: The Ten Most Critical Web Application Security Risks," OWASP, accessed May 25, 2018.

April 6, 2021 11:46 PM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\April\Cloud-native Solution for Web App\sb-FA-cloud-native-solution-for-waf-462021\sb-FA-cloud-native-solution-for-waf-462021

442663-A-0-EN