FORTINET

SOLUTION BRIEF

Secure Web Applications and APIs with Fortinet FortiWeb

Executive Summary

Protecting modern applications can't get much more complicated when throwing into the mix multi-cloud environments, emerging architectures, agile development, evolving threats, and skills shortages. This complexity creates evasive attack surface blind spots and raises the probability of human errors, making keeping consistent and up-to-date security policies unrealistic. Is it, though?

Fortinet FortiWeb, in its various forms (hardware, virtual machine, or SaaS), simplifies application security and overcomes the above challenges. Using machine learning (ML) algorithms, it protects applications and APIs from inherent risks, exploitable vulnerabilities, and malicious bots.

SaaS, virtual or hardware, FortiWeb consolidated web application, bot, and API protection provide unified, consistent, and extensive security for data centers, and hybrid and multi-cloud environments.

FortiWeb Reduces Risk Exposure and Accelerates Productivity

Reduce threat exposure

FortiWeb delivers comprehensive security against credential abuse by bots, API manipulations, protocol attacks, and traditional OWASP Top 10 risks, such as SQL injections, cross-site scripting, and other web attacks.

Prevent alert fatigue with threat analytics

FortiWeb ML algorithms make correlations between what may appear as random events to identify attack patterns and sequences. It helps security teams to focus on the big events and eliminate a lot of forensics and investigation time.

Flexible deployment options for consistent security in hybrid environments

FortiWeb comes in multiple forms, HW, VM, or a SaaS service, to ensure the same security policy is applied wherever the applications are hosted, be it a datcenter, private, or public cloud. User access and behavior, protocols, regular expressions, authentication, and DDoS mitigation are just part of FortiWeb unified application protection. Furthermore, FortiWeb is integrated with the Fortinet Security Fabric to provide comprehensive visibility across environments.

FortiWeb Protects Applications Wherever They Live

FortiWeb enables managing a consistent application security policy. It protects applications and APIs from vulnerability exploits, bots, malware uploads, DDoS attacks, advanced persistent threats (APTs), and zero-day attacks. In addition, a subscription to FortiWeb Cloud Service includes continuous updates for signatures, antivirus, IP reputation, and sandboxing from FortiGuard Labs at no additional cost.

FortiWeb main features

- Advanced protection against OWASP Top 10 threats, zero-day threats, and bot attacks
- Machine learning to detect sophisticated attack campaigns and bot behaviors
- Minutes to protection: easy deployment with a setup wizard and predefined policies
- Streamlined management with an intuitive dashboard for end-to-end security visibility
- Purchasing flexibility: subscription, BYOL, PAYG, or with FortiFlex program

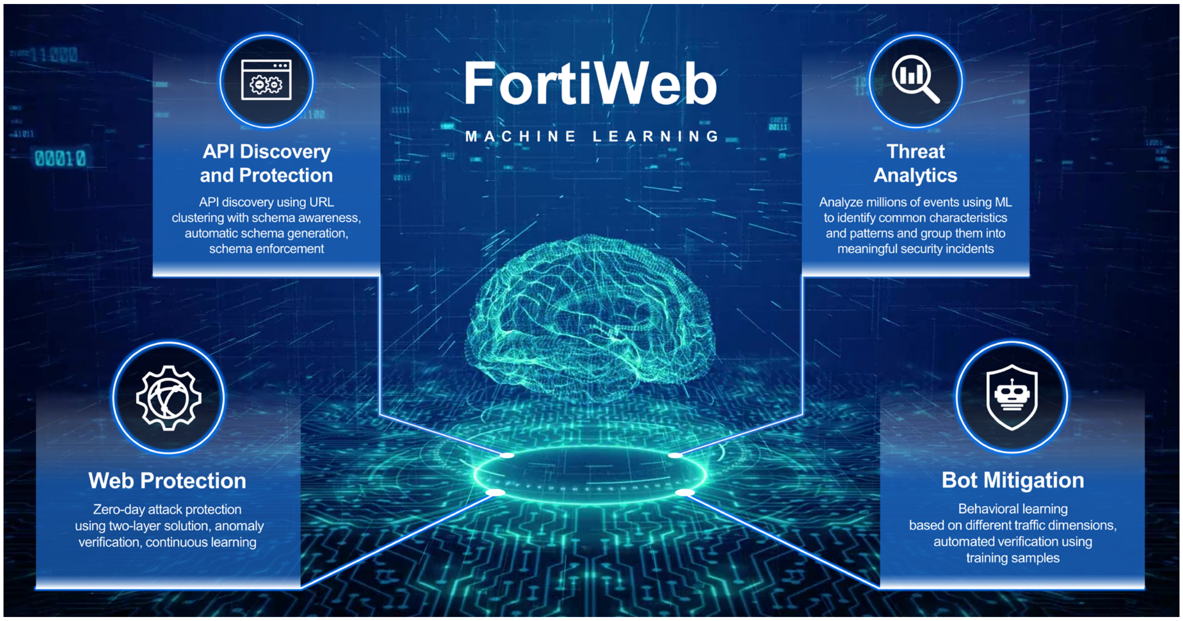

FortiWeb
MACHINE LEARNING
API Discovery and Protection
API discovery using URL clustering with schema awareness, automatic schema generation, schema enforcement
Threat Analytics
Analyze millions of events using ML to identify common characteristics and patterns and group them into meaningful security incidents
Web Protection
Zero-day attack protection using two-layer solution, anomaly verification, continuous learning
Bot Mitigation
Behavioral learning based on different traffic dimensions, automated verification using training samples

Figure 1: FortiWeb multi-purpose machine learning algorithms

Cloud deployment options:

For organizations looking to secure cloud-hosted applications, Fortinet offers a complete line of security solutions for AWS, of which the FortiWeb Cloud Service is the flagship product. Other offerings include Fortinet Managed WAF Rules and 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.
- **Fortinet Managed WAF Rules** packages enable businesses that are starting out their cloud journey to quickly and easily establish more robust application protection than the standard Amazon Web Services (AWS) WAF without managing any infrastructure. Rules are automatically updated as new vulnerabilities and bad actors emerge, keeping security policies up to date. DevOps staff can spend their time building applications rather than maintaining the web application firewall.
- **FortiWeb Cloud WAF Service** delivers full-featured, cost-effective security for web applications with a minimum of configuration and management. Delivered through any cloud service provider (CSP), such as AWS, Azure, GCP, OCI, or Alibaba Cloud, the FortiWeb Cloud Service features high scalability and on-demand pricing. Benefits include reduced latency, simplified compliance, and lower bandwidth costs for secured delivery of cloud-hosted applications.

The FortiWeb Cloud Service Delivers Easy-to-Deploy, Cost-Effective Security

The FortiWeb Cloud Service features lower capital expenditures (CapEx) and operational expenditures (OpEx) than on-premises solutions. The CSP provides the hardware and software components of the infrastructure, virtually eliminating the need for capital investments and 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 FortiWeb Cloud Service enables rapid application deployments with a setup wizard and a default configuration that can be easily modified to meet individual requirements. It delivers cloud-native application security that can be deployed in minutes.

Additional benefits:

Extensive threat coverage

Get comprehensive security that addresses a broad spectrum of threats, attacks, and exploits.

Superior detection

Detect known and unknown attacks, accurately classify incoming requests as legitimate or suspicious, and correlate between random events to show attack campaigns

Consistent security

Deploy a single application security policy and roll it out over different platforms, data centers, and cloud infrastructures

Compliance

Meet regulatory and industry standards to secure customer data privacy and integrity

Increased productivity

Focus resources on high-priority tasks instead of manual event analysis and exception handling

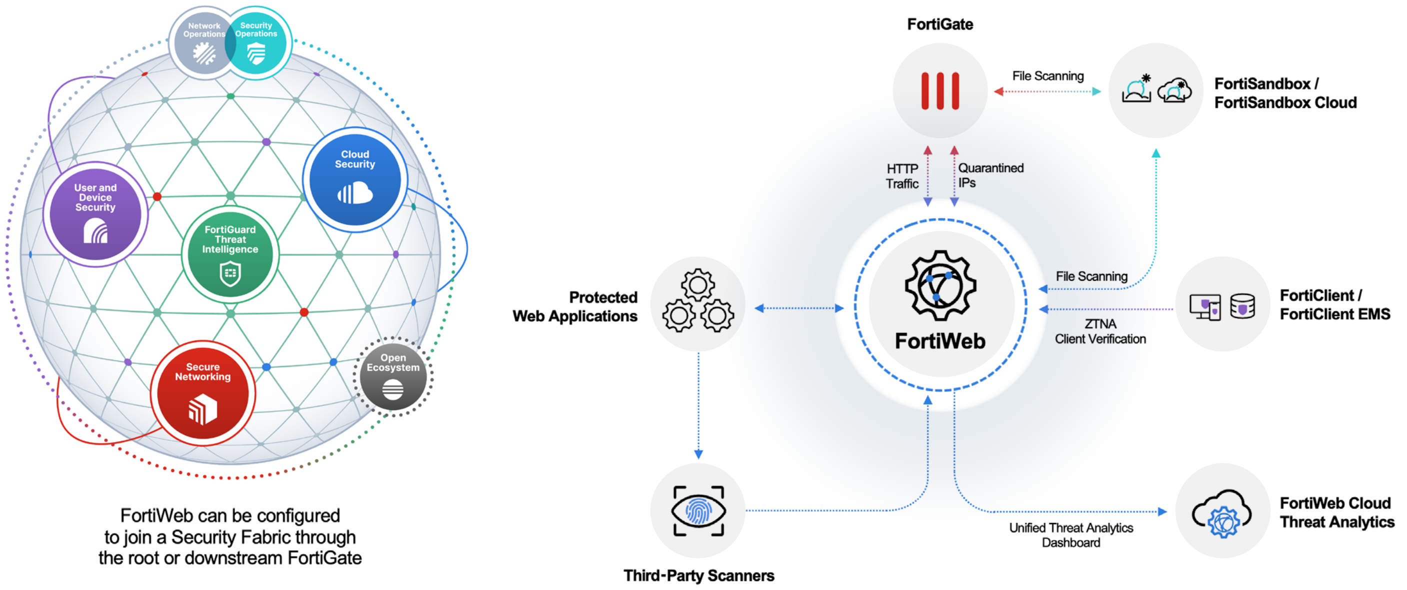
Lower TCO

Considering acquisition, services, maintenance, or the public cloud BOYL and PAYG models to begin at low investment and grow as resources become available

Fortinet Security Fabric integration

The FortiWeb Cloud Service is natively integrated with the Fortinet Security Fabric. This platform approach delivers holistic network and application protection, empowering organizations with centralized management, visibility, and consistent security wherever applications live.

FortiWeb Security Fabric Integrations



FortiWeb can be configured
to join a Security Fabric through
the root or downstream FortiGate

Figure 2: FortiWeb integration with the Fortinet Security Fabric

Conclusion

The FortiWeb Cloud Service delivers full-featured, cost-effective security for web applications and APIs with minimum configuration and management overhead. The FortiWeb Cloud Service features high scalability and on-demand flexible pricing and onboarding options. It protects applications deployed anywhere, and customers benefit from consistency, centralized management, reduced latency, simplified compliance, and lower bandwidth costs. It is also integrated with the Fortinet Security Fabric, making it the only network and application security suite defending the entire attack surface.

www.fortinet.com

September 26, 2023 12:58 PM

2337202-0-0-EN