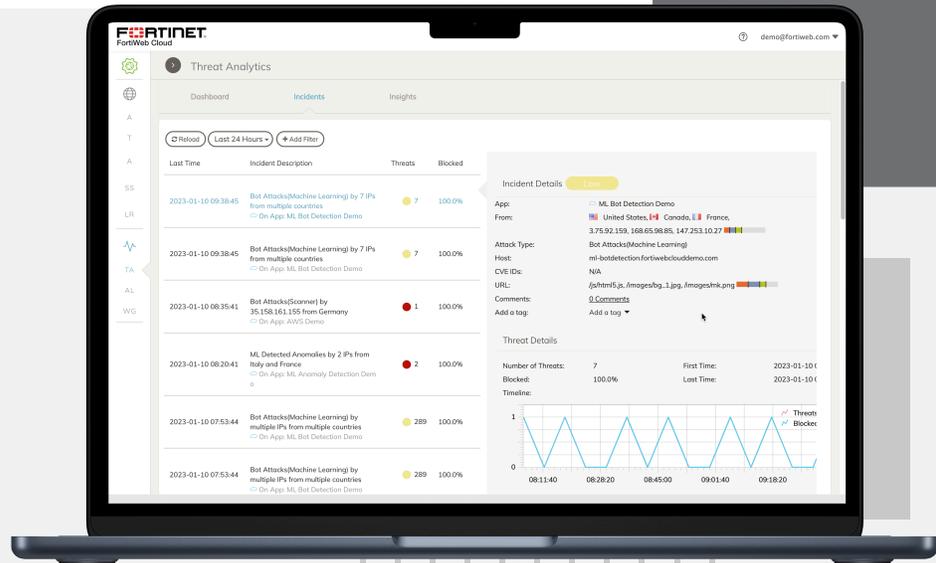


# FortiWeb™ Cloud WAF as a Service



## Highlights

- 100% cloud-based WAF-as-a-Service, delivered within the same public cloud region as your application. This provides improved performance, a simplified regulatory environment, and reduced bandwidth costs
- Bot defense to block the full range of malicious bot activity (including content scraping, denial of service, data harvesting, and transaction fraud)
- Rapid deployment via AWS, Azure, and Google Cloud Marketplaces
- Advanced analytics and reporting

## Protection for web applications and APIs, enhanced with machine learning

Protect hosted web applications and APIs without deploying and managing infrastructure. FortiWeb Cloud can be deployed and configured in minutes, with a streamlined deployment wizard.

Turn on anomaly detection and FortiWeb Cloud will identify and block malicious anomalies with no need to spend time on tedious manual rule creation.

FortiWeb Cloud leverages unique deep learning technology to deliver better protection without additional administrative overhead. It continuously models the behavior of applications, enabling deployment of the latest code into production quickly without the manual tuning required by other Web Application Firewalls (WAFs).



## Capabilities

### Easy to Deploy and Manage Full-Featured WAF

FortiWeb Cloud WAF-as-a-Service delivers the protection of a full-featured WAF as you rapidly roll out applications in public cloud environments. There's no need to manage and maintain your own infrastructure. Your attack surface changes every time you deploy a new internet-facing application, and with public clouds, you can deploy those internet-facing applications more rapidly than ever.

FortiWeb can defend the attack surface of any web-based application you deploy. This includes both applications that may only run for a short time and long-lived applications that can evolve rapidly as you adopt a DevOps approach to deliver applications and services at high velocity. Protecting applications with a SaaS-delivered WAF solution also provides the option to pay as you go. This enables the same protection for all of your public cloud hosted applications without standing up excess capacity that might be underutilized.

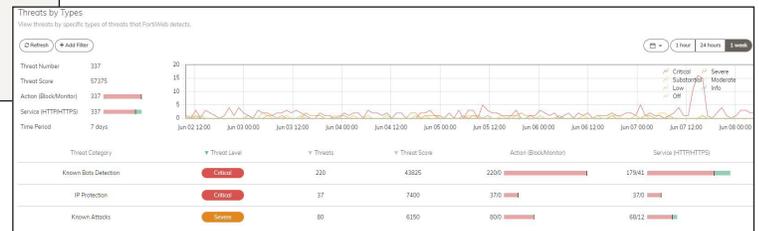
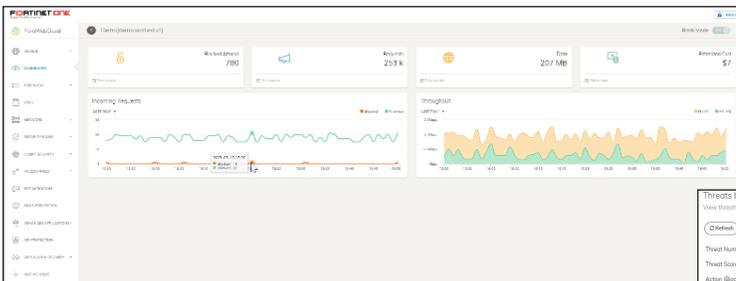
### Web Application Security

Protect against the OWASP Top 10 and other known and unknown threats using FortiWeb Cloud's comprehensive web application security, including IP reputation, DDoS protection, protocol validation, and application attack signatures.

### Internet-Facing API Protection

Seamlessly and automatically discover API endpoints and enforce security without having to manually publish APIs or integrate into CI/CD processes. FortiWeb Cloud uses sophisticated machine learning algorithms to automatically analyze and catalog APIs and their schema.

FortiWeb Cloud quickly deploys positive and negative security model policies without requiring any manual intervention and provides security teams with the visibility and security they require without slowing down software release cycles.



### AI-based Bot Defense

Block the full range of malicious bot activity (content scraping, denial of service, data harvesting, transaction fraud) quickly and easily. This feature protects websites, mobile applications, and APIs from automated threats. FortiWeb Cloud bot mitigation features include thresholds, biometric bot detection, bot deception, and machine learning-based bot mitigation.



## Capabilities

### Simplified Deployment

Once activated via your favorite cloud marketplace or via an annual contract purchase, follow the built-in setup wizard to deploy in minutes. With predefined policies and machine learning to automatically keep up with your changing application, FortiWeb Cloud delivers the security you need within minutes without the complexity required when setting up other WAF solutions. More advanced users can easily enable additional security modules if needed, free of charge. Deploy in minutes and you're protected from threats such as cross-site scripting, cross-site request forgery, denial-of-service, brute-force attacks, and SQL injection.

---

### Low Latency and Intra-region Bandwidth Rates

Fortinet delivers the service using a colony of WAF gateways in the same public cloud region as your application, enabling low latency and intra-region bandwidth rates for traffic between your application and the WAF. This method also simplifies the regulatory environment.

---

### Regulatory Compliance

Address regulatory compliance requirements for public-facing applications, including the PCI DSS 6.6. WAF requirement.

---

### FortiGuard Labs Services

FortiGuard Labs is the backbone for FortiWeb Cloud signatures and IP reputation. As an active FortiWeb Cloud Subscriber you automatically have the latest protections and updates.

---

### Content Delivery Network (CDN)

FortiWeb Cloud includes an optional CDN available at no additional charge. When activated, the CDN directs requests to the nearest and fastest point of presence, leveraging a global distribution of WAF clusters. Combined with sophisticated caching and optimization techniques, FortiWeb Cloud enables your users to access your application from anywhere in the world while delivering the performance your users demand.

---

### DDoS Protection

DoS attacks can be devastating and costly. Protect against volumetric based attacks and more sophisticated low-and-slow attacks that can cripple web servers.

Minimize downtime and ensure business continuity with FortiWeb Cloud DDoS protection for L3/4 and Layer7 attacks.



# Capabilities

## Threat Analytics

Security teams around the world are suffering from an overwhelming amount of security alerts as the attack surface expands, attack campaigns become more sophisticated, and new security challenges arise due to the migration of applications to the cloud. Security teams are struggling to identify and prioritize the real threats from all the informational and contextless alerts and require a tool that will be able to distill all alerts and focus SOC analysts on the right events.

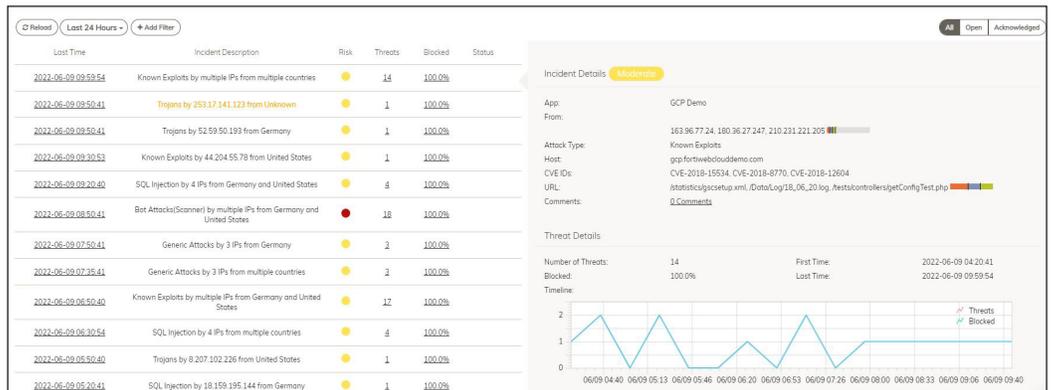
Fortinet's Threat Analytics uses machine learning algorithms to identify attack patterns across your entire application assets and aggregate them into security incidents and assign severity. It helps separate real threats from informational alerts and false positives and help you focus on the threats that matter. SOC analysts no longer have to manually sift through all the noise. Threat Analytics addresses alert fatigue and makes sure analysts can quickly focus on the most important threats.



Dashboard 1



Dashboard 2



Incidents 1



Incidents 2



## Application Delivery

### Optional CDN

- URL rewriting
- Content routing
- HTTPS/SSL offloading
- HTTP compression
- Caching

### Authentication

- Active and passive authentication
- Site publishing and SSO
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

### Management and Reporting

- Web user interface
- FortiView graphical analysis and reporting tools
- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP analytics

### Other

- Seamless PKI integration
- Auto setup and default configuration settings
- Setup wizards for common applications
- Preconfigured for common Microsoft applications such as Exchange, SharePoint, OWA, WordPress, and Drupal
- WebSockets support

### Deployment Option

- Reverse Proxy

### Web Security

- AI-based machine learning
- Automatic profiling (allow list)
- Web server and application signatures (deny list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- OpenAPI 3.0 verification
- WebSocket protection and signature enforcement
- Man-in-the-Browser (MiTB) protection

### Application Attack Protection

- OWASP Top 10
- Cross-site scripting
- SQL injection
- Cross-site request forgery
- Session hijacking
- File upload scanning with AV and sandbox

### Security Services

- Web services signatures
- XML and JSON protocol conformance
- Malware detection
- Protocol validation
- Brute-force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi detection
- HTTP header security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- DDoS prevention
- Data loss prevention



## Ordering Information

Available through the Amazon Web Services, Azure, and Google Cloud marketplaces or via annual contracts.

The following lists marketplace pricing.

Units	Price
Total number of web applications protected by FortiWeb Cloud	\$0.03 / unit
Total data transferred via FortiWeb Cloud (GB)	\$0.40 / unit

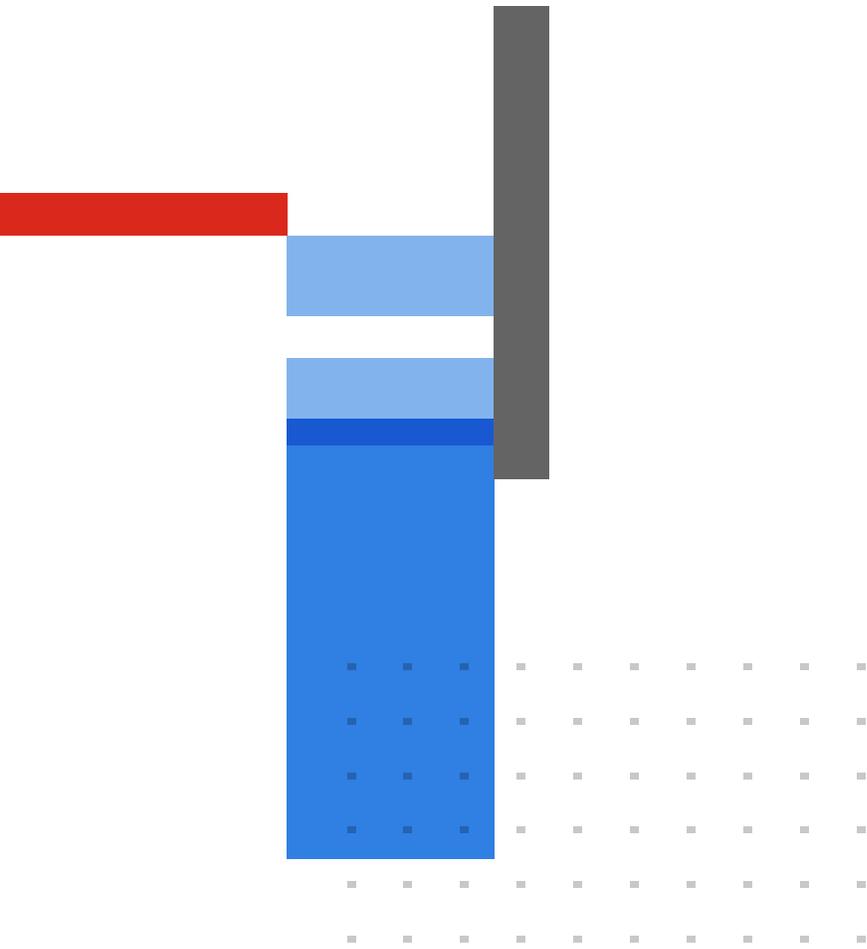
The following lists annual contract SKUs:

Product	SKU	Description
FortiWeb-Cloud-WAF-as-a-Service	FC1-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service - 20 Mbps average throughput - Annual Subscription. Select number of sites separately.
	FC2-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service - 50 Mbps average throughput - Annual Subscription. Select number of sites separately.
	FC3-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service - 100 Mbps average throughput - Annual Subscription. Select number of sites separately.
	FC4-10-WBCLD-654-02-DD	FortiWeb Cloud WAF-as-a-Service - 500 Mbps average throughput - Annual Subscription. Select number of sites separately.
	FC1-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service - Additional 1 website - Annual Subscription.
	FC2-10-WBCLD-655-02-DD	FortiWeb Cloud WAF-as-a-Service - Additional 5 websites - Annual Subscription.

### Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the [Fortinet EULA](#) and report any suspected violations of the EULA via the procedures outlined in the [Fortinet Whistleblower Policy](#).





**FORTINET**

[www.fortinet.com](http://www.fortinet.com)

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

March 26, 2024

FWEB-CL-DAT-R7-20240326