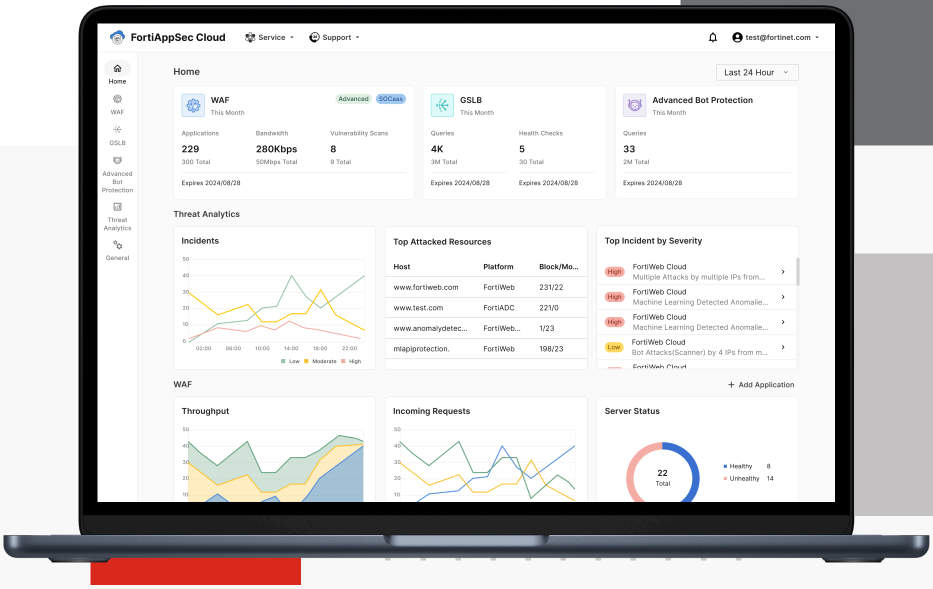
FortiAppSec Cloud

Web and API Security, Availability, and Performance



Home

WAF — This Month
Applications: 229 (300 Total)
Bandwidth: 280Kbps (50Mbps Total)
Vulnerability Scans: 8 (9 Total)
Expires 2024/08/28

GSLB — This Month
Queries: 4K (3M Total)
Expires 2024/08/28
Health Checks: 5 (30 Total)
Expires 2024/08/28

Advanced Bot Protection — This Month
Queries: 33 (2M Total)
Expires 2024/08/28

Threat Analytics

Top Attacked Resources

Host	Platform	Block/Mo...
www.fortiweb.com	FortiWeb	231/22
www.test.com	FortiADC	221/0
www.anomalydetec...	FortiWeb...	1/23
mlapiprotection.	FortiWeb	198/23

Top Incident by Severity

- High — FortiWeb Cloud: Multiple Attacks by multiple IPs from...
- High — FortiWeb Cloud: Machine Learning Detected Anomalie...
- High — FortiWeb Cloud: Machine Learning Detected Anomalie...
- Low — FortiWeb Cloud: Bot Attacks(Scanner) by 4 IPs from m...
- FortiWeb Cloud

WAF

Highlights

- **Comprehensive Application Security:** Advanced protection against OWASP Top 10 and bot-based attacks using advanced AI/ML techniques
- **Application Delivery:** Accelerates content and enhances user experience with full CDN and advanced GSLB capabilities
- **Threat Analytics:** Addresses alert fatigue and speeds up alert security investigation
- **Unified Management:** Manage security, traffic, and insights from a single, intuitive dashboard
- **Visibility 360:** Gain complete application security and monitoring insights for proactive threat response

Comprehensive application security and performance optimization across environments

The Fortinet **FortiAppSec Cloud** platform combines advanced web application firewall (WAF), API security, Advanced Bot Protection, Global Server Load Balancing (GSLB), and Threat Analytics into a single, unified platform. This all-in-one solution delivers robust application security, enhanced performance, and operational simplicity for web applications, ensuring seamless protection, visibility, and optimization under a unified management interface.

Key Benefits

Lower TCO

Operational Efficiency

Optimization

Traffic Shaping

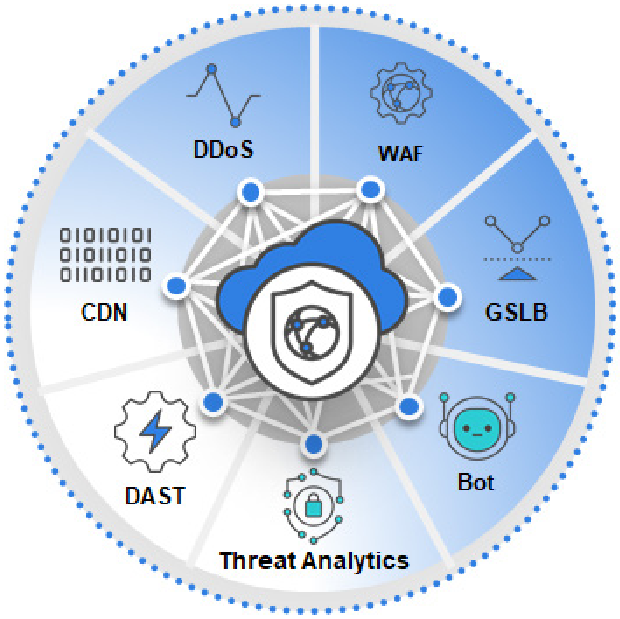
Threat Detection and Response

Challenges

The shift to multi-cloud and hybrid cloud environments has created new challenges for organizations. As businesses expand their online presence, using more of web applications and APIs, the attack surface grows, increasing the complexity of managing consistent application security. Sophisticated cyber threats, such as OWASP Top-10 vulnerabilities, zero-day attacks (some of which are generated by LLM), and bot-driven fraud, target critical web assets, exposing organizations to data breaches and service disruptions.

Traditional security measures often struggle to keep up with these evolving threats, leaving gaps that cybercriminals eagerly exploit. Compounding the issue, traffic management across global data centers and hybrid cloud environments adds another layer of complexity, with organizations needing to ensure both optimal performance and security for users across diverse regions. This fragmented approach results in inconsistent security policies, reduced visibility, and greater operational complexity.

The Fortinet **FortiAppSec Cloud Platform** addresses these challenges by providing an integrated solution that ensures that organizations can not only protect their applications from modern threats but also gain real-time insights into security events and performance metrics, enabling proactive risk management across hybrid and multi-cloud environments.



The Need for Solution Consolidation

Web applications and APIs are integral to modern business, but they also introduce new security risks that cybercriminals can exploit. As organizations scale their applications across hybrid and multi-cloud environments, more applications and APIs are being deployed, complicating the ability to consistently secure data in transit or at rest. Consequently, security gaps emerge, and organizations are exhausted by the growing number of security solutions they need to not only master but also synchronize. The increasing difficulty in protecting sensitive data and delivering optimal user experiences pushes them toward unified platforms.

Delivered as SaaS, the Fortinet FortiAppSec Cloud Platform consolidates essential application delivery and security services, simplifying management, delivering robust protection, and allowing centralized visibility, consistent security policies, and optimized traffic management across distributed environments. This integrated approach reduces the complexity of managing multiple solutions while strengthening security and improving the performance of applications and APIs globally.

Use Cases

Comprehensive Web and API Security, Including Advanced Bot Protection

FortiAppSec Cloud offers robust Web Application Firewall (WAF) and API security, complemented by Advanced Bot Protection, which detects and blocks sophisticated bot behaviors to different legitimate users from automated attacks. This use case is ideal for organizations looking to secure web applications and APIs while preventing bot-driven fraud and abuse.

Optimized Global Traffic Management with Enhanced Security

The FortiAppSec Cloud Platform uses Global Server Load Balancing (GSLB) to dynamically route traffic across multiple data centers, ensuring high availability and optimized performance, while WAF and API security protect the application layer from vulnerabilities. This solution is especially effective for organizations needing to deliver secure and optimized content globally with integrated protection.

Multi-Cloud and Hybrid Application Deployment

FortiAppSec Cloud ensures consistent security policies across all environments, with global load balancing to distribute traffic efficiently between clouds and data centers. This deployment is particularly useful for ensuring high availability and failover, guaranteeing application uptime even during outages or regional disruptions.

API Protection for Microservices Architectures

FortiAppSec Cloud ensures that API traffic is protected against common threats, such as injection attacks or API-specific vulnerabilities, with advanced security measures like deep packet inspection. API discovery helps identify and catalog APIs across environments to ensure comprehensive protection. Combined with bot protection, this solution safeguards APIs from being exploited by automated attacks, ensuring business continuity and integrity in modern application designs.

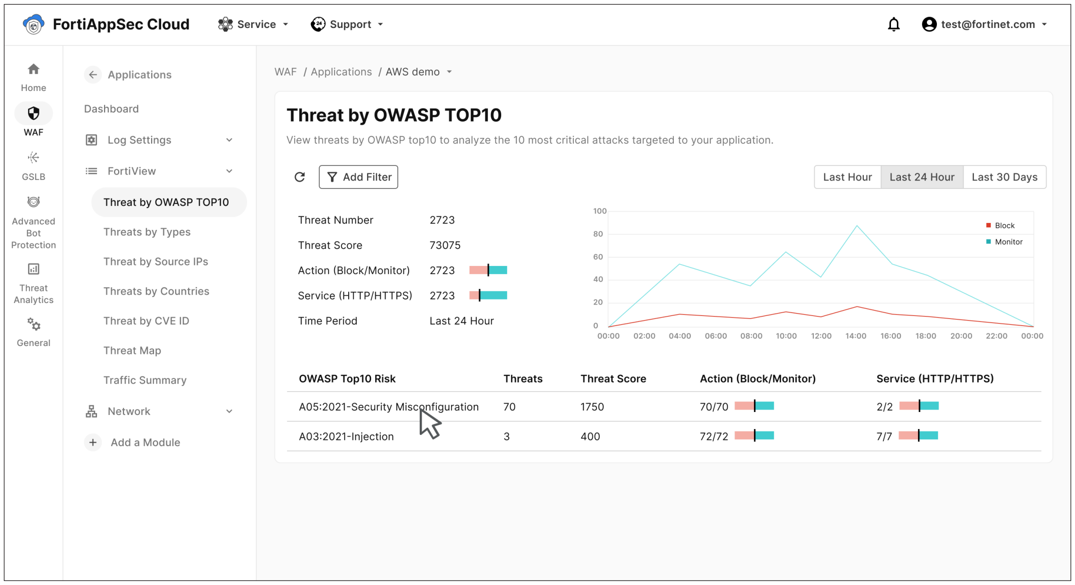
Proactive Threat Monitoring and Analytics

With Threat Analytics, organizations gain real-time visibility into potential threats, anomalies, and incidents across their cloud infrastructure. By integrating threat intelligence and security event monitoring into the FortiAppSec Cloud platform, customers can proactively respond to emerging threats and mitigate risks before they impact critical applications.

Features and Capabilities

Web Application Firewall (WAF) and API Security

- **Zero day attack protection:** dual machine learning to detect and eliminate emerging threats and AI-generated exploits
- **Eliminate False Positives**: Traffic is analyzed and scrubbed of threats before reaching your applications, ensuring only safe traffic is delivered
- **OWASP top 10 Security Risks:** Shield your web applications and APIs from attacks targeting the OWASP Top-10 risks to web applications and secure any vulnerabilities
- **Automated Updates:** Integrated with FortiGuard Labs for real-time threat intelligence, ensuring the latest protection against evolving threats
- **Simplified Configuration:** Configure and manage WAF policies through a user-friendly interface with minimal resource investment



Threat by OWASP TOP10

View threats by OWASP top10 to analyze the 10 most critical attacks targeted to your application.

Threat Number	2723
Threat Score	73075
Action (Block/Monitor)	2723
Service (HTTP/HTTPS)	2723
Time Period	Last 24 Hour

OWASP Top10 Risk	Threats	Threat Score	Action (Block/Monitor)	Service (HTTP/HTTPS)
A05:2021-Security Misconfiguration	70	1750	70/70	2/2
A03:2021-Injection	3	400	72/72	7/7

Advanced Bot Protection

- **Behavioral-Based Detection:** Biometric and behavioral analysis to detect sophisticated, human-like bot behaviors, ensuring real users can access your applications without disruption
- **Device Fingerprinting:** IP-agnostic profiling of user devices with advanced fingerprinting techniques to block bot attacks using browser or IP rotation
- **Crawler Detection:** Identify and block unwanted web crawlers, scrapers, and other automated threats compromising sensitive data
- **Historical and Real-Time Analytics:** Access real-time and historical traffic monitoring and bot-related insights for enhanced decision-making

Please refer to the relevant datasheet for more information:

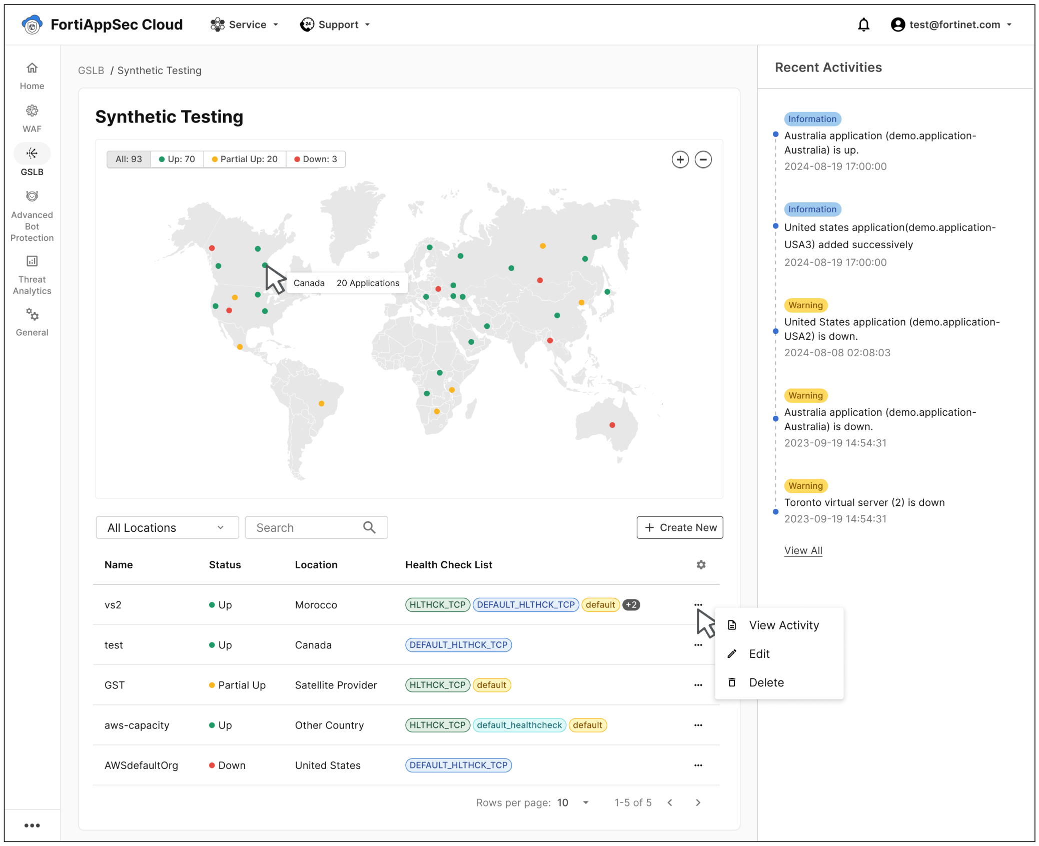
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortiguard-ad-bot-protect.pdf

Global Server Load Balancing (GSLB)

- **DNS-Based Load Balancing:** Distributes application traffic across multiple data centers and server pools, enhancing availability and resilience
- **Geographic Traffic Distribution:** Use Geo-IP and server health metrics to dynamically route traffic to the nearest or best-performing data center
- **One-Click Integration:** Easy integration with FortiWeb Cloud, ensuring that both security and load balancing are managed within the same platform
- **High Availability:** Ensure continuous application availability even during regional outages or spikes in demand

Please refer to the relevant datasheet for more information:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigslb.pdf



Synthetic Testing

Name	Status	Location	Health Check List
vs2	● Up	Morocco	HLTHCK_TCP DEFAULT_HLTHCK_TCP default +2
test	● Up	Canada	DEFAULT_HLTHCK_TCP
GST	● Partial Up	Satellite Provider	HLTHCK_TCP default
aws-capacity	● Up	Other Country	HLTHCK_TCP default_healthcheck default
AWSdefaultOrg	● Down	United States	DEFAULT_HLTHCK_TCP

Rows per page: 10 1-5 of 5

Recent Activities

Information
Australia application (demo.application-Australia) is up.
2024-08-19 17:00:00

Information
United states application(demo.application-USA3) added successively
2024-08-19 17:00:00

Warning
United States application (demo.application-USA2) is down.
2024-08-08 02:08:03

Warning
Australia application (demo.application-Australia) is down.
2023-09-19 14:54:31

Warning
Toronto virtual server (2) is down
2023-09-19 14:54:31

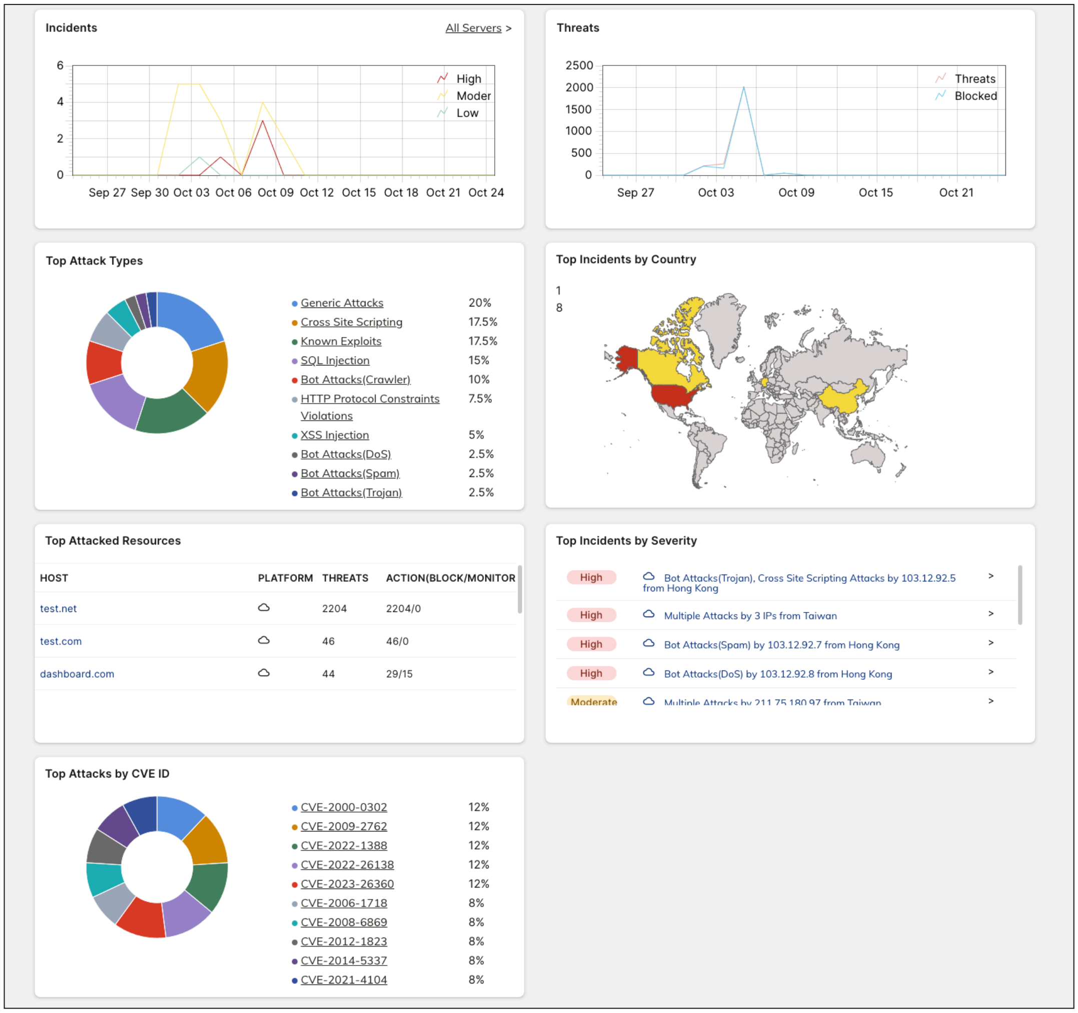
View All

Threat Analytics

- **Identify Hidden Attack Patterns:** AI-based event-correlation and analysis of attack patterns to reveal adversarial campaigns that are likely to go under the radar
- **Real-Time Visibility Across the Application Infrastructure:** Monitor security events in real-time across all applications and infrastructure, providing actionable insights into potential attacks and vulnerabilities
- **Proactive Incident Response:** threat intelligence and automated response workflows to quickly mitigate risks before they impact operations
- **Centralized Dashboard:** Consolidate security data and performance metrics in a single view, simplifying monitoring and decision-making across hybrid and multi-cloud environments
- **Reduce Alert Fatigue:** Let Threat Analytics AI compile multiple alerts into a handful of meaningful incidents, helping organizations prioritize and respond to threats more efficiently

Please refer to the relevant datasheet for more information:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortinet-threat-analytics.pdf



Top Attack Types

● Generic Attacks	20%
● Cross Site Scripting	17.5%
● Known Exploits	17.5%
● SQL Injection	15%
● Bot Attacks(Crawler)	10%
● HTTP Protocol Constraints Violations	7.5%
● XSS Injection	5%
● Bot Attacks(DoS)	2.5%
● Bot Attacks(Spam)	2.5%
● Bot Attacks(Trojan)	2.5%

Top Attacked Resources

HOST	PLATFORM	THREATS	ACTION(BLOCK/MONITOR
test.net	☁	2204	2204/0
test.com	☁	46	46/0
dashboard.com	☁	44	29/15

Top Incidents by Severity

High	☁ Bot Attacks(Trojan), Cross Site Scripting Attacks by 103.12.92.5 from Hong Kong	>
High	☁ Multiple Attacks by 3 IPs from Taiwan	>
High	☁ Bot Attacks(Spam) by 103.12.92.7 from Hong Kong	>
High	☁ Bot Attacks(DoS) by 103.12.92.8 from Hong Kong	>
Moderate	☁ Multiple Attacks by 211.75.180.97 from Taiwan	>

Top Attacks by CVE ID

● CVE-2000-0302	12%
● CVE-2009-2762	12%
● CVE-2022-1388	12%
● CVE-2022-26138	12%
● CVE-2023-26360	12%
● CVE-2006-1718	8%
● CVE-2008-6869	8%
● CVE-2012-1823	8%
● CVE-2014-5337	8%
● CVE-2021-4104	8%

License Options

Standard Package: Includes core WAF and API security features to protect against common threats.

Premium Package: Offers advanced WAF features, expanded bot protection capabilities, and GSLB for enhanced load balancing and security.

Feature Category	Standard	Premium
Web Application Protection		
Signature based Protection	✓	✓
IP Threat Intelligence	✓	✓
GEO-IP Intelligence	✓	✓
Custom Security Rules	✓	✓
HTTP Compliance	✓	✓
URL, Parameter and CORS Protection	✓	✓
Cookie Protection	✓	✓
Information Leakage	✓	✓
AV for File Uploads	✓	✓
Sandboxing for File Uploads		✓
Zero Day Attack Protection - Machine Learning based Anomaly Detection		✓
API Security		
Schema Enforcement (OpenAPI, XML, JSON)	✓	✓
API Gateway		✓
Mobile API Protection		✓
Machine Learning based - Discovery, PII Catalog, Protection		✓
Client Security		
HTTP Header Protection	✓	✓
CSRF and MiTB Protection	✓	✓
Bot Defense		
Signature, Threshold, Biometric and Deception	✓	✓
Machine Learning based Bot Defense		✓
Advanced Bot Protection	Available Separately	Available Separately
Account Takeover		
User Tracking		✓
Session Fixation Protection		✓
Credential Stuffing Defense		✓
DDoS Protection		
Layer 3-4 DDoS Mitigation	✓	✓
Layer 7 DDoS Mitigation	✓	✓

Feature Category	Standard	Premium
Application Delivery		
SSL Certificates - Automatic and Custom	✓	✓
Client Authentication\Mutual TLS		✓
Content Delivery Network (CDN)	✓	✓
Limited GEO CDN	✓	✓
Load Balancing and Server Health Monitoring	✓	✓
Origin Server Content Routing		✓
Waiting Room		✓
Global Server LB		
DNS Load Balancing	Available Separately	Available Separately
DNS Services + DNSSEC	Available Separately	Available Separately
Health Check (Synthetic Testing)	Available Separately	Available Separately
DAST Scanning		
Vulnerability Assessment	Available Separately	Available Separately
API Scanning	Available Separately	Available Separately
Reporting and Analytics		
Attack Logs	✓	✓
Alert Notifications	✓	✓
SIEM Integration	✓	✓
Log Sensitive Data Masking	✓	✓
FortiView - Realtime and historical log Analysis	✓	✓
Dashboards and Reports	✓	✓
Traffic Logs		✓
Threat Analytics AI		✓
Management		
Role Based Access Control	✓	✓
Single-Sign-On Support	✓	✓
API Support	✓	✓
Services		
24×7 Support	✓	✓
SOCaaS	Available Separately	Available Separately

Ordering Information

The service requires a FortiCloud Premium subscription as described in the FortiCloud service description, along with the following product-specific license.

SOLUTION	SKU	DESCRIPTION
FortiAppSec Cloud WAF		
Bandwidth	FC1-10-UCAPF-1114-02-DD	FortiAppSec Cloud. Cloud WAF, 25 Mbps Standard Plan (Use seat 1). Includes FortiCare premium support.
	FC2-10-UCAPF-1114-02-DD	FortiAppSec Cloud. Cloud WAF, 50-99 Mbps Standard Plan (25Mbps/seat). Includes FortiCare premium support.
	FC3-10-UCAPF-1114-02-DD	FortiAppSec Cloud. Cloud WAF, 100+ Mbps Standard Plan (25Mbps/seat). Includes FortiCare premium support.
	FC1-10-UCAPF-1115-02-DD	FortiAppSec Cloud. Cloud WAF, 25 Mbps Premium Plan (Use seat 1). Includes FortiCare premium support.
	FC2-10-UCAPF-1115-02-DD	FortiAppSec Cloud. Cloud WAF, 50-99 Mbps Premium Plan (25Mbps/seat). Includes FortiCare premium support.
	FC3-10-UCAPF-1115-02-DD	FortiAppSec Cloud. Cloud WAF, 100+ Mbps Premium Plan (25Mbps/seat). Includes FortiCare premium support.
Applications	FC1-10-UCAPF-1116-02-DD	FortiAppSec Cloud. Cloud WAF, 1-4 Applications, Standard Plan. Must be combined with a Bandwidth Standard plan. Includes FortiCare premium support.
	FC2-10-UCAPF-1116-02-DD	FortiAppSec Cloud. Cloud WAF, 5-24 Applications, Standard Plan. Must be combined with a Bandwidth Standard plan. Includes FortiCare premium support.
	FC3-10-UCAPF-1116-02-DD	FortiAppSec Cloud. Cloud WAF, 25+ Applications, Standard Plan. Must be combined with a Bandwidth Standard plan. Includes FortiCare premium support.
	FC1-10-UCAPF-1117-02-DD	FortiAppSec Cloud. Cloud WAF, 1-4 Applications, Premium Plan. Must be combined with a Bandwidth Premium plan. Includes FortiCare premium support.
	FC2-10-UCAPF-1117-02-DD	FortiAppSec Cloud. Cloud WAF, 5-24 Applications, Premium Plan. Must be combined with a Bandwidth Premium plan. Includes FortiCare premium support.
	FC3-10-UCAPF-1117-02-DD	FortiAppSec Cloud. Cloud WAF, 25+ Applications, Premium Plan. Must be combined with a Bandwidth Premium plan. Includes FortiCare premium support.
FortiAppSec Cloud Add-ons		
DAST	FC1-10-UCAPF-216-02-DD	FortiAppSec Cloud. Vulnerability Scanning Service, 10 IP/FQDN. Must purchase Cloud WAF as well.
SOCaaS	FC1-10-UCAPF-464-02-DD	24×7 cloud-based managed log monitoring, incident triage and SOC escalation service for Cloud WAF. 1-4 applications (seats), price per application. Must purchase for all applications in account.
	FC2-10-UCAPF-464-02-DD	24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service for Cloud WAF. 5+ applications (seats), price per application. Must purchase for all applications in account.
FortiAppSec Cloud Standalone Services		
GSLB	FC1-10-UCAPF-330-02-DD	FortiAppSec Cloud. Global Server Load Balancing, 100 QPS (queries per second). Includes FortiCare premium support.
	FC1-10-UCAPF-332-02-DD	FortiAppSec Cloud. Global Server Load Balancing, 10 Health Checks. Includes FortiCare premium support.
Advanced Bot Protection	FC1-10-UCAPF-726-02-DD	FortiAppSec Cloud. Advanced Bot Protection, 1M Trans/Month. Includes FortiCare premium support.

Licensing and Availability

The Service is available as a subscription via the FortiCloud portal. Customers can choose between the **Standard** and **Premium** packages, with options to add Advanced Bot Protection, GSLB, or Threat Analytics as standalone services, if necessary.

For more information, please visit fortinet.com or contact your Fortinet sales representative.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

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.

www.fortinet.com

December 11, 2024