SERVICE DESCRIPTION
FORTIAPPSEC CLOUD

1. Introduction

FortiAppSec Cloud is a comprehensive cloud-based service designed to provide critical security needs of modern web applications (the "Service"). The Service provides a single interface to manage security policies and enhance application performance through Cloud Web Application Firewall (WAF), API Security, with integrated support for Advanced Bot Protection, Global Load Balancing, and FortiGuard automatic updates and threat intelligence.

Using the Service, end-customers ("Customer") can:

- Direct web application traffic through the Service for security analysis and optimized load distribution.
- Receive analyzed and clean traffic back to original web applications.
- Block known malicious activities, attacks, and sophisticated bot threats.
- Utilize advanced load-balancing policies (including Geo-IP, server load) for dynamic selection of preferred pools of servers.

FortiAppSec Cloud is available in three service tiers with the following features included in each tier:

- Standard tier: Cloud WAF and API, DDoS Protection, and Content Delivery Network.
- Advanced tier: Cloud WAF and API, DDoS Protection, Content Delivery Network, API security, DAST, and Threat Analytics
- Enterprise tier: Cloud WAF and API, DDoS Protection, Content Delivery Network, API security, DAST, Threat Analytics, Global Server LB, Advanced Bot Protection, and SOCaaS

The Service is hosted on the FortiCloud™ service portal whose features, deliverables and terms of use are described in the then-current FortiCloud service description made available at https://support.fortinet.com/Information/DocumentList.aspx (the "FortiCloud Service Description"). The terms of the FortiCloud Service Description are incorporated herein by reference and in the event of a conflict, this service description shall prevail over the FortiCloud Service Description.

2. Service Features

The Service is managed by Fortinet on a 24/7 basis, targeting an availability of 99.99% uptime, each calendar month. The Service is available in various regional SSAE 16-compliant datacenters enabling the Customer to keep data within defined boundaries.

FortiAppSec Cloud provides the Customer with the following features:

- Unified Management Interface
  - A single dashboard for comprehensive management and visibility including traffic and application visibility displaying various systems and attacks logs for analysis, available at https://appsec.fortinet.com
  - Centralized configuration and monitoring of security policies and traffic.
- DDoS Protection
  - Active protection for layer 3, 4, and 7 DDoS attacks.
- Application Security (WAF and API)
  - Web and API security against Open Worldwide Application Security Project's (OWASP) most recent Top 10 critical security risks, injection attacks, and zero-days.
  - ML-Based threat detection, monitoring application behavior to reduce false positives.
  - API discovery and protection to secure registered apps with automatic validation.
- Content Delivery Network (CDN)
  - Access to a globally distributed access network, utilizing content caching and compression.
- Threat Analytics

- Centralized threat visibility across Fortinet security fabric and application layers.
- Use of AI to detect anomalies, attack patterns, and bot behavior in real time.

- Vulnerability Scanning (DAST)
  - Evaluate application security in real time by detecting critical vulnerabilities (as defined by OWASP most recent Top 10 critical security risks).
- Advanced Bot Protection *Only with Enterprise*
  - Detect bots using behavior analysis and device fingerprinting to differentiate between human users and automated bots with comprehensive device profiles including hardware and software attributes.
  - Monitor client events including mouse and keyboard interactions to detect suspicious activity.
  - Algorithms for detecting crawler-type bots using user agent strings and HTTP headers.
  - Custom rules for identifying and mitigating bot behaviors.
  - Granular control of mitigation actions including block, redirect, or challenging bots by type.
  - Historical analytics including real-time traffic monitoring and user success and failure attempts over time.
- Global Server Load Balancing (GSLB) *Included with Enterprise; Add-On Purchase for Standard and Advanced Tiers*
  - A full list of features, customer responsibilities, and scope and conditions are available in the then-current FortiGSLB Cloud service description, made available at https://support.fortinet.com/.
- Security Operation Center-as-a-Service (SOCaaS) *Included with Enterprise; Add-On Purchase for Standard and Advanced Tiers*
  - A full list of features, customer responsibilities, and scope and conditions are available in the then-current service description for the FortiCloud Security Operation Center-As-A Service , made available at https://support.fortinet.com.
- Support and Compliance
  - 24x7 technical support available over email and phone for each subscribed instance.
  - Compliance with regional data residency requirements, ensuring that customer data remains within defined regions.
  - Attack log information is retained for 60 calendar days for analysis and auditing.

3. Customer Required Contributions and Responsibilities

In addition to the Customer-required contributions and responsibilities included in the FortiCloud Service Description, the customer agrees for the duration of the service:

- Maintain an admin-level FortiCare account (https://support.fortinet.com)
- Be responsible for creating and maintaining bot-management policies through https://appsec.fortinet.com.
- Configure the appropriate DNS settings to route web application traffic through FortiAppSec Cloud, and ensure the integration is correctly established.
- Provide up-to-date information about web applications routing through the Service, including IP addresses, domains, and server configurations.
- Ensure the accuracy and integrity of traffic-related data provided for analysis, load balancing, and bot detection. This includes managing information on server locations, application configurations, and an updates related to changes in the Customer's infrastructure.
- Provide accurate information in a timely fashion when requested by Fortinet to resolve Support tickets.
- Enable security policies for monitored apps, configuring the app policy to "Block" to actively block attacks.

4. Scope and Conditions

In addition to the scope and conditions included in the FortiCloud Service Description, the following terms apply:

- Agree to use the Service for legitimate and lawful business purposes only. In particular, the Customer is responsible for ensuring that its usage of the Service shall be in accordance with all applicable laws (including, but not limited to, privacy and security laws) and that it has all necessary licenses, permissions, clearances, rights and has in place proper controls and processes, implemented and maintained in this respect. Therefore, Fortinet explicitly advises the Customer to always assess and ensure that the usage of the Service complies with local legislation prior to its deployment. Should Fortinet discover illegal activity, the Service may be terminated without notice, and the relevant authorities may be notified regardless of intent.

- The Customer acknowledges and agrees that Fortinet may access the Customer's FortiAppSec instance for the purpose of troubleshooting support issues reported by the Customer.
- If a Customer exceeds their purchased bandwidth allotment in a given month, Fortinet will notify the Customer over email and may apply a one-time fee or begin contract renegotiations. Fortinet reserves the right to suspend access to the Service if a Customer exceeds their data allotment for two (2) consecutive months without payment of fees.
- Following non-renewal or termination of the All customer data, logs, and configuration within the Service are automatically deleted after seven (7) days. Customer logs are deleted from Fortinet records following sixty (60) days of Service termination.
- Any loss of internet network connectivity by the Customer is the responsibility of the Customer with the Service continuing to be considered being utilized.
- During maintenance activity that requires Fortinet to make the Service unavailable, Fortinet will use reasonable efforts and work with the Customer to configure the traffic to bypass and forward it directly to the origin web servers to minimize the impact on the Customer and Customer availability.
- It is accepted that this Service can only help to prevent, find, or eliminate web attacks and security breaches, but it is technically impossible to guarantee that these will never occur as no security device or service can guarantee 100% security or the blocking of all known malicious activity and attacks.
- Guarantee appropriate agreement within the customer organization for change requests when non-standard configurations are applied at the Customer´s request.
- Activation of the Service takes place in accordance with Fortinet's Service Contract Activation and Grace Period Policy, made available at: https://www.fortinet.com/corporate/about-us/legal/service-contract-activation-grace-period-policy.
- The Service is delivered in accordance with any data processing agreement between the parties and Fortinet's Privacy Policy, made available at: https://www.fortinet.com/corporate/about-us/privacy.html.
- The Service is subject to the terms of then-current Fortinet's Service Terms & Conditions located at https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf.

5. Eligibility & Purchasing

The Service is available for purchase by an end-customer through authorized Fortinet resellers and distributors globally ("Channel Partners"). Channel Partners are independent third parties that conduct business in their own name and account and, consequently, cannot bind Fortinet in any way. The Service is delivered to the Customer as referenced in the purchase order placed with Fortinet by a Customer or a Channel Partner. This Service is separate from any purchase of other Fortinet's products or other services.

The date of the Service registration determines the start date of the Service which will run for the period determined by the Service SKU purchased by Customer notwithstanding if the Service entitlements are not fully consumed. In no circumstances will the duration of the Service be extended. All sales are final.

Depending on the selected tier, the Customer must select a monthly bandwidth SKU and an application seat count SKU.

Service Tier	Description	SKU
FortiAppSec Standard	Monthly Bandwidth: 25 Mbps (no application seats)	FC1-10-UCAPF-1114-02-DD
	Monthly Bandwidth 50-99 Mbps (25Mbps/seat)	FC2-10-UCAPF-1114-02-DD
	Monthly Bandwidth 100+ Mbps (25Mbps/seat)	FC3-10-UCAPF-1114-02-DD
	Application Seat Count: 1-4 Apps	FC1-10-UCAPF-1116-02-DD
	Application Seat Count: 5-24 Apps	FC2-10-UCAPF-1116-02-DD
	Application Seat Count: 25-74 Apps	FC3-10-UCAPF-1116-02-DD
	Application Seat Count: 75+ Apps	FC4-10-UCAPF-1116-02-DD

FortiAppSec Advanced	Monthly Bandwidth: 25 Mbps (no application seats)	FC1-10-UCAPF-1115-02-DD
	Monthly Bandwidth 50-99 Mbps (25Mbps/seat)	FC2-10-UCAPF-1115-02-DD
	Monthly Bandwidth 100+ Mbps (25Mbps/seat)	FC3-10-UCAPF-1115-02-DD
	Application Seat Count: 1-4 Apps	FC1-10-UCAPF-1257-02-DD
	Application Seat Count: 5-24 Apps	FC2-10-UCAPF-1257-02-DD
	Application Seat Count: 25-74 Apps	FC3-10-UCAPF-1257-02-DD
FortiAppSec Enterprise	Monthly Bandwidth: 25 Mbps (no application seats)	FC1-10-UCAPF-1254-02-DD
	Monthly Bandwidth 50-99 Mbps (25Mbps/seat)	FC2-10-UCAPF-1254-02-DD
	Monthly Bandwidth 100+ Mbps (25Mbps/seat)	FC3-10-UCAPF-1254-02-DD
	Application Seat Count: 1-4 Apps	FC1-10-UCAPF-1256-02-DD
	Application Seat Count: 5-24 Apps	FC2-10-UCAPF-1256-02-DD
	Application Seat Count: 25-74 Apps	FC3-10-UCAPF-1256-02-DD

FortiAppSec Add-Ons

The following SKUs are available for purchase for Standard and Advanced Service tiers.

Service Add-Ons	Description	SKU
FortiAppSec Cloud - Global Server Load Balancing	Global Server Load Balancing: 100 queries/second	FC1-10-UCAPF-330-02-DD
	Global Service Load Balancing: 10 health checks	FC1-10-UCAPF-332-02-DD
FortiAppSec Cloud - SOCaaS Service	24x7 Cloud-based managed service per application*, 1-5 Apps	FC1-10-UCAPF-464-02-DD
	24x7 Cloud-based managed service per application*, 5+ Apps	FC2-10-UCAPF-464-02-DD

**Purchase must be made for all applications in account*