SERVICE DESCRIPTION

FORTIANALYZER™ CLOUD

1. Introduction

FortiAnalyzer Cloud is a cloud-based SaaS-hosted analytics-powered security and log management service for FortiGate™ and supported Fortinet security products as described in the then-current product data sheets and release notes (the "Supported Products" and the "Service"). The Service provides centralized reporting, traffic analysis, event and incident management, and log retention without the need for additional hardware, software, or management overhead.

Using a web-based portal, a number of product management benefits may be achieved through the Service, including:

- End-to-end visibility with event correlation and threat detection.
- Hosted log retention with cloud based storage.
- Security intelligence and analytics with SOC views.
- Automation through scripts and connectors.
- Indicators of compromise detection service.
- Event alerts and incident management.

For clarity, the Service provides a consistent set of features for the Supported Products and product-specific functionality is provided based on the product type.

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 and Deliverables

The Service will be made available on a twenty-four hours a day by seven days a week basis and available in various regional secure datacenters that enable the Customer to keep its data within defined boundaries. The Service does not share any Customer logs or configurations between regional datacenter instances. The following features are included as part of the Service for the Supported Products:

- Traffic and application visibility through a dashboard view that displays various system and log widgets with real-time monitors.
- Automated incident response capability for improved management and analytics with a focus on event management and identifying compromised endpoints.
- Log retention based on subscription levels.

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:

- To register all Supported Products to be covered under the Service in the Support Portal.
- To appropriately configure the Supported Products, to be covered under the Service, to use the Service.
- To provide network connectivity with appropriate configuration to enable the Supported Products, to be covered under the Service, to communicate with the Service. Internet connectivity must be continuously available as logs are sent periodically.
- To ensure the products and versions to be covered by the Services correspond to the Supported Products and are supported by the Service.
- To manage configurations of the Supported Products, to be covered by the Service, to ensure any data transmitted is done in accordance with Customer's data privacy requirements.
- The flow of logs and bandwidth between the FortiAnalyzer Cloud instance and the Supported Products, to be

covered by the Service, are regulated based on product log rate limits. Restrictions may apply if the bandwidth exceeds the daily allotted bandwidth amount set per product unit.

- FortiAnalyzer log data analytics retention cannot exceed more than three (3) months or one-hundred (100) calendar days.
- FortiAnalyzer log data retention cannot exceed more than twelve (12) months or three-hundred and sixty-five (365) calendar days.
- To be responsible for performing external back-ups and storage of their logs and data as needed beyond the retention periods, if required for compliance or other purposes.
- The firmware of the FortiAnalyzer Cloud instance must be upgraded regularly to the latest build for stability and support-availability purposes. Customers will be notified when a new build is available and that an upgrade is required providing a period before an automatic upgrade occurs (the "Upgrade Period"). The Customer may initiate the upgrade at any time during the Upgrade Period. Additionally, if it is discovered that there is a vulnerability in a firmware build which is determined to be material by Fortinet, Fortinet may upgrade the FortiAnalyzer Cloud instance without notice to or acceptance from the Customer.
- To complete the Service renewal before the expiration of the Service term. Otherwise, log files will be purged after seven (7) days and will not be recoverable with no grace period. At least thirty (30) days prior to the Service expiration, the Customer will receive a renewal notification from the cloud portal on a weekly basis. The Service expiration date and daily notifications for Service renewal will be displayed within the FortiAnalyzer Cloud instance. Upon Service expiration, the FortiAnalyzer Cloud instance will be shut down and an email notification will be sent to the Customer. The Customer then has thirty (30) days to purchase a renewal of the Service from a Channel Partner and contact support to renew their license and regain access to the FortiAnalyzer Cloud instance. After thirty (30) days as of the Service expiration or termination, the FortiAnalyzer Cloud instance will be deleted and an email notification sent to the Customer. For clarity, the Customer is explicitly advised that the data will be no longer recoverable, upon the deletion of the FortiAnalyzer Cloud instance.
- The effectiveness of the Service is dependent on the configuration utilized by the Customer on their local platform and the available bandwidth for communicating the data.

4. Scope and Conditions

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

- The Customer acknowledges and agrees that Fortinet may access the Customer's FortiAnalyzer Cloud instance for the purpose of troubleshooting and applying fixes in relation to support tickets submitted or otherwise reported by the Customer or identified through established monitoring and/or system notifications and will be entitled to perform maintenance and fixes on the FortiAnalyzer Cloud instance without Customer's consent or prior notice.
- The Service will be delivered in accordance with Fortinet's privacy policy made available and updated from time to time at https://www.fortinet.com/corporate/about-us/privacy.
- The Service is subject to the terms of Fortinet's then-current 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 (the "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. The registration and delivery of the Service covered by this service description must commence in accordance with service activation policies made available at https://www.fortinet.com/corporate/about-us/legal, failure of which, will result in, as the case may be, the Service being partially or completely forfeited without any right to obtain a refund. In no circumstances will the duration of the Service be extended. All sales are final.

Purchasing Information:

Unit	Options	SKU
FortiAnalyzer Cloud Service	*FortiAnalyzer Cloud: cloud-Based central logging & analytics. Include All FortiGate log types, IOC Service, Security Automation Service and FortiGuard Outbreak Detection Service.*	FC-10-[FortiGate Model Code]-585-02-DD
FortiAnalyzer Cloud Service with SOCaaS	*FortiAnalyzer Cloud with SOCaaS: Cloud-based Log Monitoring (PaaS), including IOC Service and FortiCloud SOCaaS.*	FC-10-[FortiGate Model Code]-464-02-DD

Please refer to Fortinet's then-current price list to identify the specific SKU for the appropriate product.