SERVICE DESCRIPTION

FORTIMAIL™ CLOUD

1. Introduction

FortiMail™ Cloud is an email security service managed by Fortinet which provides multiple layers of malware, spam and content detection as specified herein (the "Service"). The Service is available to the end-customer (the "Customer") in accordance with two deployment options;

- **Gateway** – The customer's email is routed to Fortinet's Cloud where it is sanitized and forwarded onwards to the customer's email server(s) in accordance with the configuration provided by the customer. Gateway deployments are available in multiple different deployment options detailed below.
- **Server** – Fortinet hosts customer's email infrastructure, providing end-user access to mailboxes. Email security is also provided through Fortinet's Cloud. Only available for customers up to 100 mailboxes.

For both deployments, there is a Premium Service option which adds additional features (a) Data Leak Prevention ("DLP"); (b) Identity Based Encryption ("IBE"); (c) File and URL Sandboxing and (d) additional mailbox storage (only available for the Server deployment option). For both deployments, there is an additional cost content analysis service add-on option which provides an image scanning feature to detect adult content.

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 Options and Deliverables

2.1 FortiMail Cloud – Gateway*

This Service deployment option provides cloud-based email security for Customers with either on-premises or third-party hosted email deployments based on the following security features:

Feature	FortiMail Cloud Gateway	FortiMail Cloud Gateway Premium	FortiMail Cloud - Gateway Premium w. Cloud API support**
Managed service	●	●	●
Anti-malware	●	●	●
Antispam	●	●	●
Inbound and outbound filtering	●	●	●*
Integration with customer LDAP	●	●	●
Secure message delivery (TLS)	●	●	●*
Message tracking	●	●	●*
Reporting	●	●	●
Cloud sandboxing		●	●
Data Leak Prevention		●	●
Identity-Based Encryption (IBE)		●	●
Protected Domains* **	10	10	10
Content (image) analysis		Add-on	Add-on
User mailbox continuity		Add-on	Add-on

** Requires outbound mail to be relayed via the FortiMail Cloud service via MX redirection.*
***Requires a licensed Microsoft 365 (Exchange Online) or Google Workspace (Google Mail) corporate account.*
****Protected domain refers to the primary domain of a mailbox server. Additional alias email domains can be added to each protected domain using the associated domains feature*

This Service deployment option includes a feature for email protection in the event the Customer´s email server is unreachable by 'spooling' and holding emails until connection can be re-established subject to: (a) a time limitation of up to four (4) days from the email date of receipt; and (b) an aggregate storage limitation of 200GB of email data. Emails exceeding such limitations will be rejected and may not be recoverable. Emails stored awaiting delivery will not be accessible. The Customer acknowledges and agrees that Fortinet shall not be liable for any damages caused by the Customer's email server unreachability and deletion of emails.

Along with our spooling service, there is an optional email mailbox continuity add-on which provides end users access to an emergency mailbox, containing a rolling thirty days of messages, for additional cost.

2.2 FortiMail Cloud – Gateway Premium for MSSP

FortiMail Cloud - Gateway Premium for MSSP is a Service deployment option for Fortinet´s authorized Managed Security Service Providers ("MSSP") and Enterprises requiring advanced features such as multi-tenancy support, and act as the contracted customer. This Service option is deployed as an inbound and outbound gateway filtering email for spam and malware before forwarding to its destination, a customer domain of the MSSP/contracted customer. Fortinet is responsible for scaling the required resources according to service demand.

This Service deployment option offers the same security features as FortiMail Cloud Gateway Premium in addition to additional permissions allowing the contracting customer to sub-divide the Service into up into end-customer protected domains. For clarity, these end-customer domains and the associated end-users shall be entirely managed directly by the contracting customer. Fortinet will not provide any direct support to the contracting customer's end user.

Features with this option include but are not limited to;

- Additional support for up to 2000 protected domains, subject to Fortinet prior agreement.
- Mailbox accounting service
- Intra domain protection for internal sub-customer filtering
- Advanced MTA features

2.3 FortiMail Cloud – Server

This Service deployment option provides cloud-based email hosting and security based on the following features:

Feature	FortiMail Cloud Server	FortiMail Cloud Server Premium
Email hosting with POP3, IMAP & Webmail access	●	●
Anti-malware	●	●
Antispam	●	●
Managed service	●	●
Inbound and outbound filtering	●	●
Integration with customer LDAP	●	●
Secure message delivery (TLS)	●	●
Message tracking	●	●
Reporting	●	●
Data Leak Prevention		●
Identity-Based Encryption (IBE)		●
Cloud sandboxing		●
Mailbox size (per user)	5GB	20GB
Content (image) analysis		Add-on

3. Service Features

The Service makes available the security features specified herein that can be configured and benefit from the threat research and intelligence performed by FortiGuard™ Labs. The availability of the security features may be reasonably amended from time to time, at Fortinet's discretion, to address changes within the threat landscape and in accordance with Fortinet's then-current life cycle policies. Any amendments will be communicated through product or FortiGuard subscription documentation as designated by Fortinet or as otherwise determined by Fortinet.

The Service is intended to be delivered from several datacenter pairs that remain in-region, based on customer selection. If a region isn't explicitly chosen, customers will be provisioned in the Canadian datacenters;

ForMail Cloud datacenter regions;

- Canada (default)
- USA
- Europe
- APAC

The Service is intended to be provisioned under the following Service Level Targets:

Service	Service Level Target
Service Availability	99.999% for high availability ("HA") deployments
Email delivery after analysis	100% (within the Service availability targets)
Average email scanning time (Gateway scanning)	below 60 seconds (excluding samples triggering FortiSandbox™ inspection, where supported and enabled)

The Service features consist of:

3.1 Anti-malware

The anti-malware feature is provided through multiple layers of antivirus detection methods which may consist of:

- FortiClient™ antivirus
- FortiGuard Outbreak Protection
- FortiSandbox (available only for the Premium deployment options)

This Service feature intends to operate in accordance with the following Service Level Targets:

Feature	Service Level Target
Protection against known email viruses to FortiMail at the time of scanning	100%
False Positive Rate on email viruses known to FortiMail	Below 0.0001%

This Service feature will be configured in accordance with a best practice standard configuration by the Fortinet´s assigned technical contact in view of the configuration provided by the Customer.

When inbound email attachments of a protected domain covered by the Services are found to contain or potentially contain malware, the email and attachment will be quarantined in the FortiMail Cloud system virus folder by default. Quarantined emails will be held for thirty (30) days before deletion. Deleted emails will not be recoverable. The Customer acknowledges and agrees that Fortinet shall not be liable for any damages caused by the deletion of such emails.

If the Customer chooses to release an email infected or potentially infected by malware, the Customer agrees and acknowledges that Fortinet will not be liable for any damages caused as a result of the action taken by the Customer to release the email. Email will only be released to its original recipient or to the system administrator named by the Customer. Fortinet may, at its discretion, refuse to release malware for security reasons.

3.2 Anti-Spam

Inbound email to the protected domain covered by the Service will be scanned using a number of different detection methods to determine whether it is spam email, namely:

- FortiGuard anti-spam
- Behavioral analysis
- Uniform Resource Identifier ("URI") filtering
- Sender policy framework and domain-based message authentication, reporting and conformance check
- Sender reputation

This Service feature will be by the Fortinet technical contact based on the application of Fortinet best practices to the configuration provided by the Customer.

The Service feature intends to operate in accordance with the following Service Targets:

Feature	Service Level Target
Identification rate of spam known FortiMail	above 99.5%, excluding emails with Asian characters which is set at 95%
False Positive Rate of spam known FortiMail	Below 0.0003%

Where an email is detected as spam, there are multiple anti-spam actions that are available to the Customer:

- Tag suspected email within the subject line
- Tag suspected email within the header
- Quarantine email to the end-user's personal quarantine
- Reject suspected email
- Delete suspected email

As Customer´s organizations may have widely varying requirements for the proper action to take with spam content, Fortinet will require the Customer to define the appropriate action(s) when provisioning the Service. The Customer agrees and acknowledges that Fortinet will not be liable for any damages caused as a result of the action taken by the Customer with respect to the spam email.

In addition to the inbound emails themselves, URIs embedded within the email body will be scanned and checked against the FortiGuard URI database. By default, emails that the Service determines are in the following categories will be treated as spam and blocked as a security risk:

- Phishing
- Malware
- SPAM URLs

Additional URI categories may be made available for configuration upon request. See https://fortiguard.com/webfilter/categories for a full list of web filter categories.

3.3 Data Leak Prevention (only available for the Premium Service options)

This Service feature enables the Customer to select security policies that identify particular file types, message contents or other criteria and block them from being sent to external parties. When enabled, these policies are configured to enable the FortiMail Cloud platform to identify traffic types the Customer wishes to protect and block from being sent.

3.4 Identity Based Encryption (only available for the Premium Service options)

This Service feature allows the Customer to deliver confidential and regulated emails with a high level of security. When enabled, this Service feature captures email that meets pre-defined policies, and sends a HTML notification to the recipient, through a separate email, detailing instructions to retrieve the captured email.

Policies may be defined based on sender, recipient, or content, and allow Customer to ensure that potentially secure content is viewed in a secure fashion. The currently available policies are:

- Policy-based encryption which automatically encrypts messages based on content or recipient
- Push or pull modes

3.5 FortiMail Cloud Sandboxing (only available for the Premium Service options)

When integrated with FortiSandbox Cloud, the Service queues emails containing suspicious attachments and URLs to be inspected for security threats. Suspicious codes are subjected to multi-layer pre-filters prior to execution in the virtual OS for detailed behavioral analysis. These pre-filters provide screening by the antivirus engine, querying cloud-based threat databases and OS-independent simulation with a code emulator, followed by execution in the full virtual runtime

environment. Once malicious code is detected, the threat is quarantined to prevent propagation into the Customer's network.

3.6 Cloud API support (only available with FortiMail Cloud - Gateway Premium with Cloud API support budle)

When integrated with either Microsoft 365 email or Google Workspace email, FortiMail Cloud will receive a notification on arrival of an email, which is then retrieved (header and content including attachments) and scanned using FortiMail anti-malware and antispam policy (outlined in 3.1 and 3.2). FortiMail will then quarantine (claw-back) messages from the Microsoft 365 or Google Workspace user mailbox if found malicious.

This feature is not subject to time-based scanning SLAs due to the dependency on 3rd party systems.

3.7 User Mailbox Continuity

When the Mailbox Continuity add-on is issued following registration, FortiMail Cloud will store user email by 'spooling' and holding emails when the Customer's email serve is unreachable. Use of Mailbox Continuity is subject to: (a) a time limitation of up to thirty (30) days from the date of email receipt; and (b) an aggregate storage limitation of 200GB of email data. Emails received beyond such limitations will be rejected and may not be recoverable. Users will need a working internet connection to access the FortiMail user portal to receive and send emails during a customer mail server outage event. This feature is only supported when FortiMail Cloud is listed as the only MX (Mail eXchange) record in DNS (Domain Name System).

3.8 High Availability

As part of the standard configuration: (a) High Availablity pairs of virtual instances will be deployed for any new deployments from June 2022 onwards. For pre-June 2022 Cloud infrastructure, deployments of one hundred (100) mailboxes and above; and (b) standalone virtual instances will be deployed for deployments below said threshold.

3.9 Service Targets

All service levels described in this document are targets which Fortinet will use reasonable efforts to achieve. Service targets are measured as of the submission of the support ticket to Fortinet and will exclude delays related to Service unavailability or disruption caused by any of following events, without limitation:

i. Scheduled maintenance or emergency maintenance;
ii. Unauthorized user changes;
iii. Customer or MSSP's -initiated changes whether implemented by Customer or Fortinet or a third party on behalf of Customer;
iv. Customer or MSSP exceeding the subscribed Service capacity;
v. Customer's or MSSP's failure to adhere to Fortinet implementation, support processes and procedures;
vi. Acts or omissions of the Customer, MSSP. its employees, agents, third party contractors or vendors or any third party accessing the Service;
vii. Any violations of the Customer or MSSP's responsibilities or Scope & Conditions defined above;
viii. Any event not wholly within the control of Fortinet;
ix. Negligence or willful misconduct of the Customer, MSSP, or others authorized by the Customer to use the Services provided by Fortinet;
x. Any failure of any component for which Fortinet is not responsible, including but not limited to all Customer or MSSP infrastructure including electrical power sources, networking equipment, computer hardware, computer software or email content;
xi. Any failures that cannot be corrected because the Customer or MSSP, its systems or networks are not reasonably accessible to Fortinet. It is the Customer's and/or MSSP's (if applicable) responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing the technical contact details.

4 Customer Required Contributions and Responsibilities

The customer agrees for the duration of the service:

- Maintain an administration account provided by Fortinet along with creation of any further required user accounts.
- Make available and maintain network security skilled personnel to interact with Fortinet for the duration of the Service.
- Perform any changes to configuration of profiles and settings as required to customize the Service environment beyond the standard baseline configuration provided by the Service. Any update to configuration must be performed by Customer's skilled personnel meeting Fortinet's best practices. For clarity, any customization of the Service shall be agreed in advance by Fortinet.
- Assist with all reasonable requests to provide the information made by Fortinet including, without limitation, any information required to resolve incidents or meet Customer's requested configurations. This includes collaborating with Fortinet for resolution of technical issues, accepting that these actions may include service-impacting actions such as, without limitation, a reset or the reloading of a known working Customer's configuration.
- Implement any corrective configuration changes required to resolve or mitigate an incident.
- Correct technical issues and minimize the recurrence of technical issues for which the Customer is responsible that may prevent Fortinet from meeting the Service level targets.
- Specifically, for FortiMail Cloud Gateway for MSSPs, it is the MSSPs sole responsibility to:
    - Make all necessary configuration to the FortiMail Cloud configuration according to the end-customer domain
    - Ensure the customer makes the necessary changes to their MX records to point at the FortiMail Cloud service
    - Ensure that SMTP mailbox verification is enabled on the customer system
    - Provide all support to the end-customer
- By purchasing the Service, the Customer understands and agrees that Fortinet is not obligated to provide the Service if the Customer fails to meet the requirements herein (as amended from time-to-time at Fortinet's discretion).

5 Scope and Conditions

The Service is subject to the following terms and conditions:

- Customer Infrastructure. The Service is available only if the Customer's email systems are permanently connected to the internet with a fixed IP address communicated by the Customer to Fortinet. Email systems connected to the Internet via dial-up, ISDN lines or using dynamic IP addresses are not supported. Any loss of connectivity by the Customer is the sole responsibility of the Customer and the Service shall be considered to be utilized regardless of such loss or absence of Customer's actual usage of the Service.
- Configuration. The configuration of the Services will be entirely based on the information provided by the Customer.
- Usage Policy. The Customer understands that the Services are designed to supplement and support, but not to replace, the implementation of an effective end-user computer usage policy by the Customer across its organization.
- Lawful Use Only. The Customer acknowledges and agrees that information sent to and from Customer will pass through the Service and Fortinet's cloud platform. Accordingly, Customer agrees 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, privacy and security laws) and proper controls and processes shall be implemented 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 any deployment. Should Fortinet discover illegal activity, the Service may be terminated without notice and the relevant authorities may be notified regardless of intent. In the event that the continued provision of the Service to the Customer would compromise the security of the Service or Fortinet's systems, networks or reputation, the Customer agrees that Fortinet may temporarily or permanently suspend the Service to the Customer. The Customer accepts and acknowledges that: (a) Fortinet shall not be liable for any

damages, fines, claims, costs or expenses incurred or suffered by the Customer or any third parties as a result of or in connection with the breach of these warranties; and (b) it shall fully indemnify and hold Fortinet harmless from and against any and all claims, liabilities, losses, damages, penalties or fines, including all reasonable legal fees, arisen directly or indirectly as a consequence of the breach of these warranties.

- Internal Use and Bulk Mailing Services. This Service is provided for the Customer internal business use and shall not be resold -or use for the provision of services- to third parties with the exception of the FortiMail Cloud – Gateway Premium for MSSPs. If the Customer is likely to be sending solicited bulk or marketing email, it is essential that this is communicated to Fortinet in advance otherwise it may lead to restriction or suspension of Service. Sending of unsolicited bulk email via the Service will be considered an abuse of the Service and will result in immediate suspension of Service.
- Service Cessation & Data Removal. Fortinet will cease in processing emails upon the expiration or termination of the Service subscription or the agreed Service´s evaluation period. Fortinet will retain the configuration and any associated data only for a period of fourteen (14) days to allow data collection or service re-initiation following termination or expiration of the Service subscription or the end of agreed Service's evaluation period. Once such period is elapsed, the Customer instance will be deleted along with any associated data. Deleted data will not be recoverable.
- Planned Maintenance. Fortinet will target to provide forty-eight (48) hours prior notification of any planned maintenance activity which may cause disruption of Service due to non-availability of sections of the FortiMail Cloud infrastructure. Where possible, maintenance activity will be carried out without affecting the Service for which traffic may be temporarily diverted through sections of the infrastructure that are not affected. Fortinet will use reasonable efforts to avoid not accumulating planned maintenance exceeding eight (8) hours per calendar month and such planned maintenance taking place between 8am and 6pm in the time zone in which Fortinet's infrastructure is located.
- Emergency Maintenance. In order to maintain the stability and security of the Service, emergency maintenance may be necessary without notice and may likely affect the Service. Fortinet will use reasonable efforts to inform the affected Customers as soon as practicable within at least one (24) hours of the start of the emergency maintenance.
- No warranties. The Customer acknowledges and agrees that: (a) Service is subject to intrinsic reliability and technical limitations; (b) Service may help to prevent, find or eliminate malware embedded in email and email spam, to prevent data leaks, or to deliver email securely but it is technically impossible to guarantee email or network security as no security device or service can guarantee full security or the blocking of all known malicious activity, attacks, and spam; and (c) Fortinet accepts no liability for any damage or loss resulting directly or indirectly from any failure of the service to detect spam or malware, or data leaks or for false positives in identifying and an email as spam, data leak, or an attachment as malware including security breach, data loss, data corruption, and service interruptions and/or degradations of the Company's network, systems.
- MSSP. The MSSP understands and acknowledges that Fortinet will not provide direct support to any end customers of an MSSP system or any domain configuration for the sub-domain customers. Only the MSSP can raise support tickets and the MSSP must provide all end customer support. For clarity, the Service is only provided with respect to the MSSP and Fortinet does not accept any responsibility with respect to the service between the MSSP and its end-customers. MSSP shall fully indemnify and hold Fortinet harmless from and against any and all claims, liabilities, losses, damages, penalties or fines, including all reasonable legal fees, arisen directly or indirectly as a consequence of its end-customer's use of the underlying Service.
- Privacy. Customer and MSSP represent and warrant that it has all rights, permissions, and consents necessary to: (a) submit personal data to deliver the Service and necessary support; and (b) grant Fortinet the right to process personal data for the provision of the Services and support: (i) as required by applicable law; (ii) as reasonably requested by the Customer via available access controls; (iii) as necessary to provide the Services, and related support, and prevent or address technical problems or violations of the Service; and (iv) as set forth in the following sentence. Fortinet will process the personal data that Fortinet receives through the Service pursuant to: (i) a data processing agreement executed between the parties where required under applicable law, and (ii) the provisions of the Fortinet Privacy Policy located at http://www.fortinet.com/aboutus/privacy.html ("Privacy Policy"). When the Service provides Customer with new personal data that Customer did not already possess (such as the Service's determination that a particular email poses a security threat), Customer may use this new personal data solely for Customer's lawful internal cybersecurity purposes.

- 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.
- Terms. The service is subject to the terms of then-current Fortinet's Service Terms & Conditions located at https://www.fortinet.com/corporate/about-us/legal.html.

6 Eligibility & Purchasing

The Service is available for purchase by an end-customer including Fortinet's authorized MSSPs (the "Customer") through authorized Fortinet resellers and distributors. Fortinet resellers and distributors 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 of Fortinet products as referenced in the purchase order placed with Fortinet by a Customer or Fortinet authorized partner or distributor. This Service is separate from any purchase of other Fortinet's products or other services. In no circumstances will the duration of the Service be extended. All sales are final.

Purchasing Information:
The Service is available in a number of formats and options as listed in the then-current Fortinet price list:

Unit
FortiMail Cloud – Gateway
FortiMail Cloud – Gateway Premium
FortiMail Cloud – Gateway Premium w. Cloud API support
FortiMail Cloud – Server
FortiMail Cloud – Server Premium
FortiMail Cloud – Gateway Premium for MSSP (including Monthly billing options)

The standard lead time for initiating the provision of the Service depends on a number of factors, including Customer's availability, and generally takes five (5) business days from the date of receipt of the onboarding information from the Customer. This tentative period may be extended if additional configuration and customization is required.