

Forcepoint Cloud Services Service Level Agreement

1. Terms and Conditions

1.1 Forcepoint provides these SLAs subject to the terms and conditions of the then current Forcepoint Subscription Agreement at: [Subscription Agreement](#), the Forcepoint Network Security Products License Agreement at: [Network Security License Agreement](#), and any other Forcepoint end user agreement incorporating these SLAs, as applicable and as may be updated by Forcepoint from time to time (the “Agreement”). The defined terms therein have the same meaning when used in this Service Level Agreement. “Subscriber” and “Licensee” under the Agreement are referred to as “Customer” in these SLAs. The current version of these SLAs can be found at: [Cloud Services Service Level Agreement](#) and may be modified or updated by Forcepoint from time to time in its sole discretion with or without notice to the Customer.

1.2 A Customer must submit a claim in writing within 5 days of the occurrence of the failure to meet an SLA (or earlier if specifically set forth below) (the “Credit Request”), and promptly provide Forcepoint with reasonable evidence to support the basis for the Credit Request. If Forcepoint confirms that an SLA was not met, then Customer will be eligible for a “Service Credit” entitling the Customer to the free use of the affected Cloud Services for the time period set forth in the applicable SLA.

1.3 Service Credits for any failure to meet an SLA will only be provided under a single SLA for a single claim, as identified by the Customer in the Credit Request. One claim cannot result in Service Credits under multiple SLAs.

1.4 The SLAs will not apply to situations where:

General

- The Cloud Services is unavailable for 1 hour or less or the Customer fails to timely submit a Credit Request in compliance with Section 1.2
- The Customer has used the Cloud Services for 30 days or less
- The Customer is a trial or evaluation customer
- The Customer is misusing the Cloud Services (including without limitation acting as an open relay or open proxy, or using the service to send spam or viruses) or is otherwise in violation of the Agreement
- The failure to comply with the SLA is based on reasons beyond Forcepoint’s reasonable control as set out in the Agreement

Configuration

- The Cloud Services is incorrectly configured by the Customer, including use of Customer-provided networking equipment that does not meet the guidance in the Documentation
- The Customer configures equipment, network, or software in a manner such that Customer’s connection does not utilize the high-availability capabilities of the Cloud Services
- The Customer provides incorrect or inaccurate information (including change information) to Forcepoint
- For Cloud Email, where an account is not configured to use two or more co-location sites (clusters)

Operation

- Forcepoint is performing scheduled or routine maintenance of the Cloud Services, where the Customer has been notified of the maintenance no less than 5 days in advance, or as otherwise set forth below
- Forcepoint is performing emergency maintenance to apply security patches to the Cloud Services

Connectivity

- The Customer’s applications or equipment or Internet connection has failed, or equipment is switching between service connection points
- There is an issue with the Customer’s or a third party’s hardware or software, or an issue caused by third parties who gain access to the Cloud Services using Customer’s accounts or equipment
- There is an issue with the Customer’s routing infrastructure (e.g. router, identity-provider or secure web proxy of a third-party)
- There is a network unavailability outside of Forcepoint-controlled systems (servers, hardware, and associated software) that are responsible for delivering the Cloud Services

1.5 The remedies set forth in this Service Level Agreement are the Customer’s sole and exclusive remedy for any failure by Forcepoint to comply with the SLAs. Further information regarding remedies is set forth in the Agreement.

2. SLAs for Forcepoint's security access policy enforcement Cloud Services solution ("**Forcepoint ONE**")

2.1 **Network Infrastructure Availability**

- Forcepoint controlled systems (servers, hardware, and associated software) that are responsible for delivering Forcepoint ONE ("Network Infrastructure") will be available 99.9% of the time.
- Network Infrastructure "Service Unavailability" means a period when the Network Infrastructure fails to process proxied traffic in substantial conformance with Forcepoint's published Documentation as may be updated by Forcepoint from time to time, measured during any given calendar month.
- In the event of Service Unavailability for 0.1% or more of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

2.2 **Peripheral Infrastructure Availability**

- The configuration management and non-inline networking capabilities provided by Forcepoint to Customer for use in connection with Forcepoint ONE ("Peripheral Infrastructure") will be available 99.9% of the time.
- Peripheral Infrastructure "Service Unavailability" means a period when the Peripheral Infrastructure is unavailable to Forcepoint ONE administrators in substantial conformance with Forcepoint's published Documentation as may be updated by Forcepoint from time to time, measured during any given calendar month.
- In the event of Service Unavailability for 0.1% or more of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

2.3 **Service Latency**

- Forcepoint ONE will process proxied requests consisting of units of data made into single Internet protocol packages traveling along a network path ("Requests") in no more than 100 milliseconds 95% of the time over any calendar month measured from the time Forcepoint ONE receives the content to the time Forcepoint ONE attempts to transmit the content.
- This service latency SLA only applies to "Qualified Content", which means Requests that are: less than 1 MB HTTP GET request and response; not subject to DLP analysis or threat scanning; and not related to streaming applications.
- If in any one calendar month 5% or more of the Qualified Content is not processed in 100 milliseconds or less as determined by the monthly average Forcepoint ONE proxied request processing time among samples taken by Forcepoint in a given calendar month ("Missed Latency SLA"), Customer may be eligible for a Service Credit equal to 1 week as a result of the Missed Latency SLA subject to a maximum aggregate Service Credit of 4 weeks during any 12-month term.

3. SLAs for Forcepoint's Internet and internal application access policy enforcement Cloud Services solution ("**Private Access**")

3.1 **Service Availability (Uptime)**

- Private Access will be available 99.999% of the time
- Private Access "Service Unavailability" means the inability of Private Access to receive, process and forward web (HTTP/HTTPS) and non-web traffic in substantial conformance with Forcepoint's Documentation, on behalf of the Customer and measured during any given calendar month.
- In the event of Service Unavailability for more than 0.001% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2 hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

3.2 **Service Latency**

- Private Access will process HTTP and HTTPS requests consisting of units of data made into single Internet protocol packages traveling along a network path ("Requests") in no more than 100 milliseconds 95% of the time over any calendar month measured from the time Private Access receives the content to the time Private Access attempts to transmit the content. Communication times outside of Private Access are not included in this SLA

- This service latency SLA only applies to “Qualified Content”, which means Requests that are: less than 1 MB HTTP GET request and response; not SSL-intercepted; not related to streaming applications; not subject to bandwidth management rules (e.g. QoS enforcement); and resulting from a reasonable level of consumption (not more than 2,000 Requests per User per day on average).
- If in any one calendar month 5% or more of the Qualified Content is not processed in 100 milliseconds or less as determined by the monthly average Private Access processing time among samples taken by Forcepoint in a given calendar month (“Missed Latency SLA”), Customer may be eligible for a Service Credit equal to 1 week as a result of the Missed Latency SLA subject to a maximum aggregate Service Credit of 4 weeks during any 12-month term.

4. SLAs for Forcepoint’s user risk analysis Cloud Services solution (“**Dynamic User Protection**”)

4.1 **Service Availability**

- Dynamic User Protection will be available 99.9% of the time
- Dynamic User Protection “Service Unavailability” means the inability of Customer to access the Dynamic User Protection management portal in substantial conformance with Forcepoint’s published Documentation (as may be updated by Forcepoint from time to time) and measured over a calendar month.
- In the event of Service Unavailability for more than 0.1% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

5. SLAs for Forcepoint’s inbound and outbound email scanning Cloud Services solution (“**Cloud Email**”)

5.1 **Message Tracking**

- For 95% of all emails processed, the following will be available for review in the Message Center within 5 minutes of receipt of an email: Detailed SMTP logs; and all emails that are quarantined (including those that failed a content filtering rule, were classified as spam or were infected with a virus).
- If more than 5% of email logs or quarantined emails processed in any calendar month are not available for review within 5 minutes when the Customer is using the portal, Customer may be eligible for a Service Credit equal to 1 day for each email log or quarantined email that did not meet this SLA, subject to a maximum credit of 5 days in any 1 month.

5.2 **Service Availability**

- Cloud Email will be available 99.999% of the time
- Cloud Email “Service Unavailability” means the inability of the email filtering service to receive and process email in substantial conformance with Forcepoint’s published Documentation for the email filtering service, as may be updated by Forcepoint from time to time, on behalf of the Customer and measured during any given calendar month.
- In the event of Service Unavailability for more than 0.001% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 month.

5.3 **Service Management**

- For 99% of all non-spam emails less than 2 Mega Bytes in size, the time required to process an email will be less than 60 seconds.
- If in any 1 calendar month, 1% or more of all processed non-spam emails less than 2 Mega Bytes in size takes 60 seconds or longer for Forcepoint to process (following receipt, ready for processing, to attempted delivery), Customer may be eligible for a Service Credit equal to 1 day for each email that takes 60 seconds or longer to receive, process and attempt to deliver, subject to a maximum credit of 5 days in any 1 month. This SLA applies only to legitimate business email (non-bulk email) and does not apply to emails 2 Mega Bytes or larger in size, denial of service (DOS) attacks, or email loops.

5.4 **Spam Detection Rates**

- Spam will be detected at a rate of 99% or above during each calendar month for Customer's use of the anti-spam service.
- The spam SLA does not apply to emails using a majority of Asian language (or other non-English or non-European language) or emails sent to invalid mailboxes.
- In the event the spam detection rate drops below 99% for a period of more than 5 days in any 1 calendar month, Customer may be eligible for a Service Credit equal to 1 month.

5.5 Virus Detection

- For Customers subscribing to the anti-virus service, Forcepoint will protect the Customer from infection by 100% of all Known Viruses contained inside email that has passed through Cloud Email. This excludes links (URLs) inside email messages that take the Customer to a website where Viruses can be downloaded.
- A "Known Virus" means a Virus which has already been identified and a Virus definition has been made available by 1 of the anti-virus services whose technology is used within Forcepoint's Cloud Email, at least 30 minutes before the time the email was processed by Cloud Email. This SLA does not apply to forms of email abuse that are not classified as viruses or malware, such as phishing, adware, spyware, and spam.
- In the event that Forcepoint identifies a Known Virus but does not stop the infected email, Forcepoint will use commercially reasonable efforts to promptly notify the Customer, providing information to enable the Customer to identify and delete the Virus-infected email. If such action prevents the infection of the Customer's systems, then the remedy defined in this Section 5.5 shall not apply. Customer's failure to promptly act on such information will also result in the remedy defined in this Section 5.5 being inapplicable.
- In the event that 1 or more Known Viruses in any calendar month passes through the email filtering service undetected and infects the Customer's systems, Customer may be eligible for a Service Credit equal to 1 month, subject to the Customer providing evidence acceptable to Forcepoint that Cloud Email failed to detect the Known Virus within 5 working days of the Virus infection.
- The SLA under this Section 5.5 will not apply if (a) the Virus was contained inside an email that could not be analyzed by the email filtering service, such as an encrypted email or a password-protected file, (b) the Virus infection occurred because an email which had been identified as containing a Virus was released by Forcepoint on the request of the Customer, or by the Customer through the email filtering portal, or (c) there is deliberate self-infection by the Customer or its authorized user.

6. SLAs for Forcepoint's web access filtering Cloud Services solution ("Cloud Web")

6.1 Service Availability

- Cloud Web will be available 99.999% of the time
- Cloud Web "Service Unavailability" means Cloud Web being unable to receive, process and forward Web Content in substantial conformance with Forcepoint's published Documentation as may be updated by Forcepoint from time to time, on behalf of the Customer and measured during any given calendar month.
- In the event of Service Unavailability for 0.001% or more of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

6.2 Service Latency

- Cloud Web will process HTTP and HTTPS requests consisting of units of data made into single Internet protocol packages traveling along a network path ("Requests") in no more than 100 milliseconds 95% of the time over any calendar month measured from the time Cloud Web receives the content to the time Cloud Web attempts to transmit the content. Communication times outside Forcepoint's data center are not included in this SLA.
- This service latency SLA only applies to "Qualified Content", which means Requests that are: less than 1 MB HTTP GET request and response; not SSL-intercepted; not related to streaming applications; not subject to bandwidth management rules (e.g. QoS enforcement); and resulting from a reasonable level of consumption (not more than 2,000 Requests per User per day on average).

- If in any 1 calendar month 5% or more of the Qualified Content is not processed in 100 milliseconds or less as determined by the monthly average Cloud Web processing time among samples taken by Forcepoint in a given calendar month (“Missed Latency SLA”), Customer may be eligible for a Service Credit equal to 1 week as a result of the Missed Latency SLA, subject to a maximum aggregate Service Credit of 4 weeks during any 12-month term.

6.3 Virus Detection

- Forcepoint will protect the Customer from infection by 100% of all Known Viruses contained inside Web Content that has passed through the cloud web protection service module of Cloud Web.
- A “Known Virus” means a Virus which has already been identified and a Virus definition has been made available by 1 of the anti-virus services whose technology is used within Forcepoint’s Cloud Web, at least 30 minutes before the time the Web Content was processed by the web filtering service. This SLA does not apply to forms of Web Content abuse that are not classified as viruses or malware, such as phishing, adware, spyware, and spam
- In the event that Forcepoint identifies a Known Virus but does not stop the infected Web Content, Forcepoint will use commercially reasonable efforts to promptly notify the Customer, providing information to enable the Customer to identify and delete the Virus-infected Web Content. If such action prevents the infection of the Customer’s systems, then the remedy defined in this Section 6.3 shall not apply. Customer’s failure to promptly act on such information will also result in the remedy defined in this Section 6.3 being inapplicable.
- In the event that 1 or more Known Viruses in any calendar month passes through Cloud Web undetected and infects the Customer’s systems, Customer may be eligible for a Service Credit equal to 1 month, subject to the Customer providing evidence that Cloud Web failed to detect the Known Virus within 5 working days of the Virus infection.
- The SLA under this Section 6.3 will not apply if (a) the Virus was contained inside Web Content that could not be analyzed by the web security service, such as HTTPS or a password-protected file, (b) the user bypassed the web security service when downloading the Web Content, (c) the Customer configured the Cloud Services to not filter the web content, or (d) there is deliberate self-infection by the Customer or its authorized user.

7. SLAs for Forcepoint’s Cloud Email archiving Cloud Services solution (“**Email Archiving**”)

7.1 Service Availability

- Email Archiving will be available 99.99% of the time
- Email Archiving “Service Unavailability” means the inability of the email archiving server to receive and transmit Customer’s requests to store and retrieve archived email in substantial conformance with Forcepoint’s published Documentation, as may be updated by Forcepoint from time to time and measured over a full calendar month.
- In the event of Service Unavailability for more than 0.01% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each calendar month where Service Unavailability exceeds 0.01%.

8. SLAs for the application programming interface (“**API**”) for Forcepoint’s cloud content disarm reconstruction Cloud Services solution (“**CDR**”)

8.1 Service Availability

- API will be available 97% of the time
- API “Service Unavailability” means the inability of the most up to date API for CDR to report the CDR as responsive or contactable in substantial conformance with Forcepoint’s published Documentation, as may be updated by Forcepoint from time to time and measured over a full calendar month.
- In the event of Service Unavailability for more than 3% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

9. SLAs for Forcepoint’s internet and internal application access policy enforcement (“**RBI**”)

9.1 Service Availability

- RBI will be available 99.9% of the time
- RBI “Service Unavailability” means the inability of RBI to receive, process and forward web content in substantial conformance with Forcepoint’s published Documentation, as may be updated by Forcepoint from time to time and measured over a full calendar month.
- In the event of Service Unavailability for more than 0.1% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

10. SLAs for Forcepoint’s advanced malware detection and protection Cloud Services solution (“AMDP”)

10.1 Service Availability

- AMDP will be available 99.5% of the time
- AMDP “Service Unavailability” means the inability of AMDP to process file submissions that have been received by AMDP from Customer in substantial conformance with Forcepoint’s published Documentation, as may be updated by Forcepoint from time to time and measured over a calendar month.
- In the event of Service Unavailability for more than 0.5% of any calendar month, Customer may be eligible for a Service Credit equal to 1 day for each 2-hour period of Service Unavailability, subject to a maximum credit of 5 days in any 1 calendar month.

11. SLAs for Forcepoint’s security access policy enforcement Cloud Services solution (“CASB”)

11.1 Definitions

- “NI” or ‘Network Infrastructure’ means the group of Forcepoint controlled systems (servers, hardware, and associated software) that are responsible for delivering CASB.
- “NI Outage” means a period when the Forcepoint NI fails to direct web traffic to the Customer site.
- “PI” or ‘Peripheral Infrastructure’ means the application access, configuration management, and all non-inline networking capabilities provided by Forcepoint to Customer for use in connection with CASB.
- “PI Outage” means a period when the Forcepoint PI is unavailable, outside a Scheduled Maintenance window.
- “Outage” means a NI Outage or PI Outage, as applicable.
- “Scheduled Maintenance” means maintenance performed (a) in which Customer is provided electronic notice at least 48 hours in advance if Customer has enrolled in automatic notifications, and (b) a recurring weekly maintenance window pertaining to the “PI” every Sunday between 3:00 AM Pacific to 3:00 PM Pacific. During this maintenance window the “PI” might be intermittently unavailable.

11.2 CASB Availability (Uptime)

- CASB will have a NI monthly uptime percentage of 99.999%.
- CASB will have a PI monthly uptime percentage of 99.5%.
- Monthly uptime percentage is calculated by subtracting from 100% the percentage of 60 second periods during the calendar month in which CASB is in a state of Outage. In the event Forcepoint does not meet the Monthly Uptime Percentage commitment, then Customer may be eligible to receive Service Credits calculated and applied as follows:
 - Forcepoint will use all information reasonably available to it to calculate the Outage length, including analysis of service data immediately prior to the Outage period. If Forcepoint determines that there has been a NI Outage for more than 0.001% or a PI Outage for more than 0.5% of any calendar month, then Forcepoint will make the following Service Credits available to Customer, subject to the conditions of this Service Level Agreement:

<u>Outage Length</u>	<u>Service Credit(s)</u>
1 min. – 120 min.	1 day’s credit
Outages of more than 120 min	1 day’s credit for every 2 full hours of outage

- A Service Credit due to a Customer will: (a) not exceed 30 days in any one month period; and (b) be applied by Forcepoint to Customer's account. Service Credits for the SLA under this Section 2 will only be credited toward Customer's use of CASB.