clearswift
RUAG Cyber Security

Clearswift Managed Security Service for Email

Service Description

Revision 1.0

Copyright

Contents

1 Introduction

Clearswift is dedicated to optimizing email security for its customers through the delivery of a professional, efficient and high-quality Managed Security Service (MSS) for Email.

Clearswift delivers the managed service to its customers under the terms of a Managed Services Agreement (MSA).

1.1 Purpose

The purpose of this document is to describe the MSS for Email offering available from Clearswift and how the service is delivered to customers. This document is designed to be viewed both as a stand-alone reference and as an addendum to the Clearswift MSA.

1.2 Scope

This document applies to the Clearswift MSS for Email covered under the terms of the Clearswift MSA. All references to the service in this document refer to the MSS for Email. Please refer to the Clearswift MSA for details on service terms and conditions.

Note: This document will be revised periodically to reflect changes in the processes, procedures and technologies being used to deliver MSS for Emails. The latest version of this document is posted on the Clearswift Support Portal (www.clearswift.com/support/portals).

1.3 Reference Documents

Clearswift Customer Support Handbook
Clearswift Managed Services Agreement

2 Managed Email Security Service

Clearswift recognizes the increasing challenges that organizations face in managing a broad range of IT Security solutions, specifically the associated costs in terms of resource for ongoing maintenance, administration and general management. Through subscription to the MSS for Email, Clearswift will help customers to optimize their investment in their Clearswift solution. Utilizing our product and service expertise, we aim to provide the highest level of protection with a significant reduction in the day-to-day management and administrative overhead, while keeping customers in control of policy and messages management.

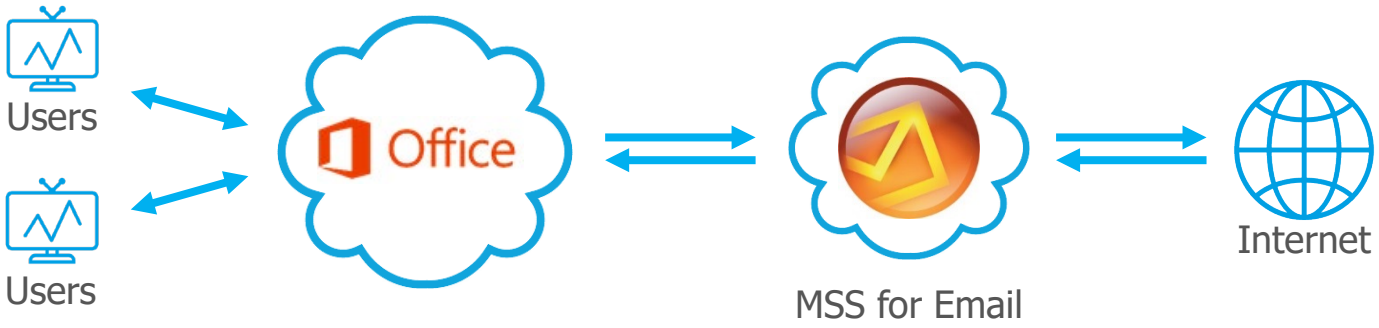
2.1 The Service Offering

The MSS for Email is hosted on a secure cloud infrastructure, pre-built with the Clearswift best practice policy offering:

- 100% email delivery
- Anti-Virus protection
- Anti-spam protection
- Ongoing application of solution updates
- Best practice (ITIL) change management
- Regular service reporting

2.2 The Functional Deployment

The following diagram illustrates the typical functional deployment of the MSS for Email and how it integrates within a customer's mail flow.



2.3 Service Access

Clearswift provides access to the MSS for Email via the Web User Interface (UI) of the application, including visibility and management of the application Security Policy, Messages, Logs, Reporting, and User management.

2.4 Reporting and Alerting

With the Clearswift MSS for Email, customer systems are monitored continuously via system and application alerts and event logging. Monthly service reports are generated and made available to customers, starting at the end of the first contracted month.

At the end of the first 12 months of service, Clearswift will review the Security Policy and offer recommendations to improve the email security and ensure compliance to the service requirements.

2.5 Upgrades and Patches

Clearswift's commitment to consistent product quality and performance is backed by measures to proactively adjust and update core products in line with technological advances and market developments, while reactively releasing periodic service packs to continuously improve the underlying operation of products and to resolve and prevent problems.

As part of the Clearswift MSS for Email, customers are provided with:

- **Software upgrades (X.Y)** - The Clearswift MSS for Email will present the main additional features and benefits provided by the latest product release and define a timeframe to apply it. Customers have the final approval on time and dates for the upgrade to be applied.
- **Patch releases (x.y.Z)** - The Clearswift MSS for Email will present the main benefits provided by the latest patch and define a timeframe to apply it. Customers have the final approval on time and dates for the upgrade to be applied.
- **Operating System patches (RHEL)** – The Clearswift MSS for Email will apply Operating System patches at the same time as software upgrades and patch releases. Emergency Operating System patch application may be required from time to time to address any known vulnerabilities directly impacting the service. The Clearswift MSS for Email will define a timeframe to apply them and will endeavor to inform customers of the patch application time and dates.
- **Hot fixes** – The Clearswift MSS for Email will only apply a hot fix in case of emergency to restore the service, or upon customer request through the Change Management process.

2.6 Service Level Agreements

Clearswift agrees to maintain the following Service Level Agreements outlined below in connection with the Services. In the event Clearswift is unable to meet the defined Service Levels the Customer may be entitled to a Service Credit as detailed in Appendix A – Service Credits.

2.6.1 Email Delivery SLA

Email Delivery Service Level is defined as Clearswift's ability to accept and process email sent through the Service subject to: (i) the email must have been received by Clearswift systems (ii) it being possible to process the email without content that would result in it being intercepted and/or held by the Service.
For Customers who have chosen to purchase a single instance, this SLA will not apply.

2.6.2 Spam Detection Rate SLA

The Spam Capture Rate Service Level defines the minimum Spam Detection Rate. This service level applies to all Email traffic and connection attempts to Clearswift systems. The service level will only apply if the Customer implements and maintains Clearswift's Best Practice Settings as provided by Customer Support. The service level corresponds to the number of **Spam False Negatives, undetected genuine spam,** measured in a calendar month. All Spam False Negatives must be submitted via Clearswift's Outlook Spam reporting add-in or by forwarding the email as an attachment to spam@clearswift.com. Submission through any other method will result in the submission/Spam not being recorded against this Service Level.

2.6.3 Anti-Virus Detection Rate SLA

If the Customer systems are infected by known or unknown malware that propagates via email(s) and is passed through the service, the Customer may be entitled to a service credit of the fees for any affected calendar month. The Customer must notify Clearswift within seven (7) days of learning of such malware and such notification must be logged, investigated, and validated by Clearswift. To avoid doubt, Customer systems are deemed to be infected if a malware attached to an email was received through the Service and there is evidence that the malware has been activated within Customer's system(s) either automatically or with manual intervention.

It is not technically possible to scan encrypted content. In the event the system infection occurs from an email that contains password protected and/or encrypted attachments, such email and/or attachments are excluded from the service level.

3 How to Engage Clearswift Services

Clearswift services are designed to offer a seamless case handling (including incident management and change management) experience, so that customers always know the status of their open cases. The services process is based on a well-defined, transparent case flow methodology. From initiation through to resolution, this methodology ensures that Clearswift takes ownership of cases and efficiently advances them across the different levels of the support organization.

3.1 Technical Contacts

Only registered Technical Contacts are permitted to open or update cases. Technical Contacts should be suitably trained on Clearswift software products prior to opening any incidents.

3.2 Services Communication Channels

Clearswift offer various communication channels for services. The Clearswift Support Portal is the most efficient and preferred channel for raising incidents or change requests and providing updates, but service requests can also be initiated by telephone and email. The following channels are available:

Channel	Service	Description
Support Portal	www.clearswift.com/support/portals	The most efficient method for opening cases and finding updates.
Telephone	APAC: +61 2 9424 1210 EUROPE: +44 (0)118 9038200 GERMANY: 0800 1800 556 JAPAN: 0066 33 812 501 US: +1 856 359 2170	The recommended communication method for critical/high severity issues or requests that require rapid response and action.
Email	support@clearswift.com change.request@clearswift.com	For users who experience difficulties using the Support Portal, email is a suitable alternative.

This information may be updated periodically and can be verified at the following URL: www.clearswift.com/support

4 Case Management

As part of the MSS for Email, customers have access to Clearswift Support as standard, with the addition of infrastructure change requests that will also be managed via the Support service.

4.1 Change requests

Clearswift carries the sole administrator role of the MSS for Email infrastructure even where the service is provided partly or wholly through a hosting provider. Any changes to the infrastructure will be handled directly and throughout by the Clearswift Managed Security Service team. To maintain effective communications with our customers, the handling of change requests flows through an agreed chain of actions.

When infrastructure changes are required, customers raise the request with Clearswift Support providing the following information:

- Change request nature and details
- Supporting information (External servers or services, business requirement, etc.)
- Contact details where required
- Impact and urgency

Each change request has a unique ID number. Clearswift will allocate a Severity (see table 4.1.1) which will be acknowledged via email.

Note: Before a customer can raise a request, they must be registered with Clearswift as a Technical Contact. To register, please contact Clearswift Support or log on to the Clearswift Support Portal.

4.1.1 Change Request Severity

Severity	Description
Emergency	Needing to be urgently performed due to a major fault, the presence of a security risk or where failure to undertake the change is likely to result in a loss of service or exposure to significant risk
Minor	A change not causing an outage or impact to performance, and does not require scheduling or approval
Standard	Changes that are defined as low risk or non-service affecting but still requiring CAB approval
Complex	Reserved for any change which carries an identified risk or impact, or changes which require detailed input from parties other than the customer and Clearswift

4.1.2 Change Request Service Targets

This section describes the service milestones and the targeted service times to deliver against those milestones.

4.1.2.1 Change Request Service Milestones

Milestone	Description
Response	Initialization of the support process, through engagement with the customer to progress information gathering, analysis or issue replication.
Execute	Provision of a change in response to a received request.

4.1.2.2 Change Request Service Targets per Milestone

Severity	Service Level Target
Emergency	Respond within 2 Business Hours Evaluate and execute within 4 Business Hours
Minor	Respond within 1 Business Day Evaluate and execute within 2 Business Days
Standard	Respond within 4 Business Hours Evaluate and execute within 5 Business Days
Complex	Respond within 1 Business Day Evaluate and execute within 8 Business Days

4.1.3 Change Request Workflow

The following points define the key responsibilities of each Service Level in the provision of Change Management to the MSS for Email infrastructure.

4.1.3.1 Clearswift Application Support (Level 1)

Clearswift provides first line (L1) contact point for requests that can't be handled by the customer or for which customer's require additional information/clarification to ensure continued system availability.

Key responsibilities include:

- Response to requests raised by Technical Contacts
- Qualification of the request severity and urgency
- Information gathering to ensure complete availability of details required for impact analysis
- Request routing/escalation to second/third level support or third parties

4.1.3.2 Clearswift Managed Services (Level 2)

Clearswift provides second line (L2) Managed Services personnel, with Senior Engineers providing impact analysis and delivery of infrastructure changes.

Key responsibilities include:

- Qualification of nature of change request
- Validation that the request is supported operation does not impact the Service Levels
- Escalation to Hosting Provider where required
- Documentation of Impact Analysis including risk assessment and rollback solution
- Request Approval from Customers prior to execution
- Delivery of change request in agreement with the customer
- Validation of change requests delivered by the Hosting Provider

4.1.3.3 Hosting Provider (Level 3)

The Hosting Provider of the MSS for Email platform provides third line (L3) support for infrastructure changes where changes to the platform or environment are required. This is between Clearswift and the hosting provider only and does not affect the customer in any way – all communications shall remain between Clearswift and the customer.

Key responsibilities include:

- Qualification of nature change request
- Review and approval of change request
- Delivery of change request in agreement with Clearswift MSS for Emails

4.2 Incidents

Clearswift provides standard support as defined in the Customer Support Handbook to MSS for Email customers with full visibility of functional escalation between support tiers provided to Technical Contacts through the status of the incident. Clearswift maintains 24/7 365 days a year support for Category 1 incidents

4.2.1 Incident Workflow

The incident workflow and the key responsibilities are defined in the Customer Support Handbook. Where the issue is identified to be directly related to the MSS for Email, Clearswift may be required to engage with the Hosting Provider. The following points define the key responsibilities for each party.

4.2.1.1 Clearswift Managed Services (Level 2)

Clearswift provides second line (L2) support, with Senior Technical Support professionals providing analysis and resolution of reported issues.
Key responsibilities include:

- Qualification of the reported issue with the MSS for Email
- In depth incident analysis
- System infrastructure problem diagnostic
- Provision of technical resolution or problem workaround
- Hosting provider (Level 3) escalation
- Risk assessment with full documentation of steps to restore full service
- Delivery of workarounds/fixes provided by Level 3 to restore full service
- Trigger Disaster Recovery Plan with Level 3

4.2.1.2 Hosting Provider (Level 3)

The Hosting Provider of the MSS for Email platform provides third line (L3) support services for back-to-back consultation with Clearswift Managed Services, including the delivery of Disaster Recovery. This is between Clearswift and the hosting provider only and does not affect the customer in any way – all communications shall remain between Clearswift and the customer

Key responsibilities include:

- In depth analysis of Platform and external environment
- Provision of platform and external environment technical resolution or problem workaround
- Restoration of service outage
- Respond to Disaster Recovery Plan request
- Delivery of Disaster Recovery Plan to Clearswift Managed Service

4.3 Escalation

Escalation is the process by which incident details are made known to other personnel for the purpose of notification or to obtain additional resources to assist in problem resolution. Escalation usually occurs when difficulties or delays are being experienced, or are considered likely, in resolving an issue.

4.3.1 Functional Escalation

The objective of functional escalation is to obtain the additional resources and expertise required to resolve a particularly difficult or complex incident.

4.3.2 Hierarchical Escalation

The objective of hierarchical escalation is to ensure that potential problems are made known to the relevant managers and resource owners within Clearswift. This ensures the right level of focus across the organization and the engagement of appropriate resources and expertise to expedite the resolution of customer issues. Customers can request this type of escalation if they experience or foresee delays or other problems with the resolution of issues, as set out below.

Level	Contact	Escalation Procedure
1	Technical Support Incident Owner	Support will escalate the incident on request and change the priority of the incident providing visibility to the Technical Support Manager or local Country Manager. The incident owner will contact the customer within 1 business day and agree a plan of action for progression with an agreed target timescale for communication of updates and resolution.
2	Service Delivery Manager (or nominated local representative)	The Service Delivery Manager or local Country Manager will be assigned as key contacts within the Escalation Team for the incident and will contact the customer within 1 business day to communicate a rescue plan for the Incident. If the problem is not resolved within target timeframe for the rescue plan, the incident shall automatically be notified to the next level of escalation.
3	Technical Support Director (or local Country Manager)	The Technical Support Director or local Country Manager will work with the Technical Support Manager and assigned Escalation Team members to determine a rescue plan for the incident, with agreed communication updates to the customer and a target resolution date. If the incident is still not resolved, the customer may request an escalation to the Chief Executive Officer. The Chief Executive Officer will contact the Customer at the earliest possible opportunity and agree a plan for resolution. The Chief Executive Officer is the final point of escalation.

5 Service Requirements

5.1 Clearswift Obligations

1. Clearswift delivers the Service as described within this document to customers with access to the application Web User Interface.

2. Clearswift shall alert and maintain communication with the customers throughout the course of any planned or unplanned Service outage.

3. Clearswift will provide a Service Desk function via www.clearswift.com/support/portals, giving specified Technical Contacts access to Clearswift Managed Services during the hours specified for the service offering purchased. Customers shall report cases primarily via the Clearswift Support Portal but may also do so via telephone or email. This access should be used for, but not limited to:

4. Infrastructure Change requests
5. Technical Query and Problem Reports against the Service

6. Clearswift Managed Services will work on the customer's change requests during stated service hours, excluding the days declared as public holiday close days.

7. Clearswift shall provide each Technical Contact with individual accounts to access the Clearswift Support Portal, with sufficient privileges to enable access to all cases raised by the Customer.

8. Clearswift shall be responsible for ensuring that it has back-to-back support agreements in place with its key suppliers to ensure that it can meet the requirements specified by this agreement.

9. Clearswift shall supply to customers, on request, details of any back-to-back support agreements with third party suppliers.

10. Clearswift shall retain ownership of any cases, relating to services provided by Clearswift and assigned to them, until that problem is effectively resolved by mutual agreement.

11. Clearswift shall track and escalate problems based on the agreed 'Service Level Targets' defined in this document.

5.2 Customer Obligations

1. Customers retain full ownership and management at the application level and are responsible for policy and message management.

2. Customers must inform Clearswift of any changes or service downtime in their environment that would directly impact the Service Level (i.e. downstream/upstream mails server outages).

3. Customers shall formally raise infrastructure change requests to Clearswift Managed Services and obtain a change request reference number. A change request is only tracked by Clearswift once a change request number is issued.

4. Customers shall provide Clearswift with up-to-date contact details of their named representatives appointed as Technical Contacts.

5. Customers must ensure that users of Clearswift Products and Services are suitably qualified and trained on the use of the applications.

6. If a Service Level impacting Incident reported to Clearswift Support is determined to be due to the use of third-party products outside of the scope of the Clearswift Support and Maintenance agreement, it is the responsibility of the customer to work with their third-party supplier to resolve the issue.

7. The customer is responsible for ensuring that services fees are paid within agreed payment terms.

5.3 Remote Access

Clearswift do not have access to the application Web User Interface (UI). Clearswift may request customers to provide access to the application Web UI to troubleshoot problems. Customers are requested to provide Clearswift Support with external access to environments in order to aid the resolution of reported problems.

5.4 Out of Scope

The following services are not included within the scope of the offerings:

- Policy Management. Clearswift will not modify the security policy configured on the application. Policy Definition Services can be defined and priced separately under the terms of Professional Services
- Message Management. Clearswift will not have access to the Message Management Centre offered by the application. It is the customer responsibility to manage the messages processed and held by the application
- On-site delivery. Unless agreed with the Clearswift Regional Service Delivery Manager, as part of an active plan of action to resolve an escalation scenario
- Professional Services. Unless specified in the service offering purchased, such as, but not limited to, system audits, system benchmarking or custom report generation. These services would need to be defined and priced separately under the terms of Professional Services
- Support for interfaces to data sources not expressly included in the License Agreement
- Data management, data retrieval, data file copying or distribution, administration and other routine operational responsibilities

Appendix A - Service Credits

Clearswift agrees to maintain the following Service Level Agreements outlined below in connection with the Services. In the event Clearswift is unable to meet the defined Service Levels the Customer may be entitled to a Service Credit as set out below.

1. Email Delivery

Email Delivery Service Level is defined as Clearswift's ability to accept and process email sent through the Service subject to: (i) the email must have been received by Clearswift systems (ii) it being possible to process the email without content that would result in it being intercepted and/or held by the Service.
For Customers who have chosen to purchase a single instance, this SLA will not apply.

Percentage available in a calendar month	Percentage credit for the affected month
Below 100% and above or equal to 99%	10%
Below 99% and above or equal to 98%	20%
Below 98% and above or equal to 97%	30%
Below 97% and above or equal to 96%	40%
Below 96%	50%

2. Spam Detection Rate

The Spam Capture Rate Service Level defines the minimum Spam Detection Rate. This service level applies to all Email traffic and connection attempts to Clearswift systems. The service level will only apply if the Customer implements and maintains Clearswift's Best Practice Settings as provided by Customer Support. The service level corresponds to the number of **Spam False Negatives, undetected genuine spam**, measured in a calendar month. All Spam False Negatives must be submitted via Clearswift's Outlook Spam reporting add-in or by forwarding the email as an attachment to spam@clearswift.com. Submission through any other method will result in the submission/Spam not being recorded against this Service Level.

Spam capture rate in a calendar month	Percentage credit for the affected month
Below 99%	50%

3. Anti-Virus Detection Rate

If the Customer systems are infected by known or unknown malware that propagates via email(s) and is passed through the service, the Customer may be entitled to a service credit in the amount equal to 50% of the fees for any affected calendar month. The Customer must notify Clearswift within seven (7) days of learning of such malware and such notification must be logged, investigated, and validated by Clearswift. To avoid doubt, Customer systems are deemed to be infected if a malware attached to an email was received through the Service and there is evidence that the malware has been activated within Customer's system(s) either automatically or with manual intervention.

The Customer must be utilising a minimum of two antivirus engines within the Clearswift product. Failure to operate both engines invalidates this Service Level. It is not technically possible to scan encrypted content. In the event the system infection occurs from an email that contains password protected and/or encrypted attachments, such email and/or attachments are excluded from the service level.