FORTRA

DATASHEET *(Cybersecurity)*

Clearswift Secure Exchange Gateway

The Clearswift Secure Exchange Gateway (SXG) helps to safeguard against inappropriate or critical information being distributed internally and subsequently leaving an organization; underpinning both policy and compliance requirements. Working on Exchange 2007, 2010 or 2013 platforms, the SXG detects malware and inappropriate file types and identifies violations in conversations based on an easily defined policy based rules.

Data Loss Prevention

The Clearswift Advanced Data Loss Prevention (DLP) systems ensure that your email matches the confidentiality and compliance policies of your organization. Messages that contain certain violations can be quarantined for manual inspection, or the offending content can be removed through the use of Adaptive Data Redaction. Using keyword search of PDF and Office attachments it is now possible to dynamically replace keywords and phrases with an alternative character such as asterisks, meaning that any sensitive phrase is removed and no longer a threat. To remove any traces of unauthorized sensitive data being distributed internally and subsequently being leaked out of the organization in Office and PDF format, the Document Sanitization feature allows document properties and change tracking to be removed preventing inadvertent leakage.

Enforce Compliance

Messages and attachments can be filtered on message size, message content or attachment content. Policies can be built to control messages flowing between organizational units. Messages can be rejected or quarantined for manual release by approved administrators or distributed to line managers letting them release or delete the message; this leads to improved operational efficiency and less of an IT burden.

Deep Content Filtering & Customized Keyword Search

Deep content filtering of the message and its attachments can ensure that inappropriate content or critical information can be detected. With support for over 150 file formats and character set recognition for over 200 languages, objectionable or sensitive content can be detected using keyword search utilizing standard and easily customized dictionaries. Keyword search allows for words, phrases, tokens (e.g. credit card) and regular expressions to be used to detect content violation.

Along with keyword search; file size, true file type controls and filename blocking can be employed to detect or remove files that may not be business-related or simply over-sized that can have an effect on the Exchange infrastructure.

Comprehensive Malware Control

With a choice of Avira or Sophos, messages can be scanned by up to two engines, without incurring any additional processing cycles on the Exchange server. Structural validation checks can be applied on file formats to detect whether data has been pre-pended or appended to a file to evade detection and Structural Sanitization can be used to remove active code from PDF, Office and HTML to reduce the chance of Advanced Persistent Threats infiltrating in the corporate messaging service.

Policy Based Rules

Rules can be easily defined to cover internal and Internet based email with the use of AD/LDAP integration. Building policies by individuals and organizational units as well as based on

content. This is important when organizations have to ring fence departments; for example in banks, military and research, or simply when a multi-national company has particular export controls that they have to adhere to.

Monitor Mode

A monitor mode enables you to test your DLP policy without impacting your message flow. Copies of messages are processed by the SXG platform and the results of processing used to identify if and where you have issues with email content or whether your DLP policy needs adjusting to prevent false positives.

Scanning Platforms

Unlike most other Exchange scanning products, the Clearswift solution offers an off-box solution designed to reduce the load on your Exchange servers. This platform runs on hardened Linux and can be deployed on physical hardware or virtually on vSphere and Hyper-V with only a lightweight interceptor on the Exchange server to ensure that message delivery times are not compromised.

SXG Interceptor deployed on Exchange Transport server passes a copy of the message to the SXG processing node. If the message is not safe to be delivered it can be rejected, altered or quarantined for manual approval.

Implementation Options

Implementing the SXG platform is agnostic to current security infrastructure and can be run both with an out-sourced managed service model (Fig 1) or when using an on premise layered security model (Fig 2).

Management and Reporting

Secure Exchange gateways can be grouped into resilient processing engines and their management is provided by a Web UI. This allows system administrators of different privileges to perform system tasks such as unified Policy definition, Message Management, Reporting and System monitoring.

Exchange Interceptors are configured using PowerShell and their configuration is saved in Active Directory LDS so that it can be shared by other interceptors in an organizations deployment.

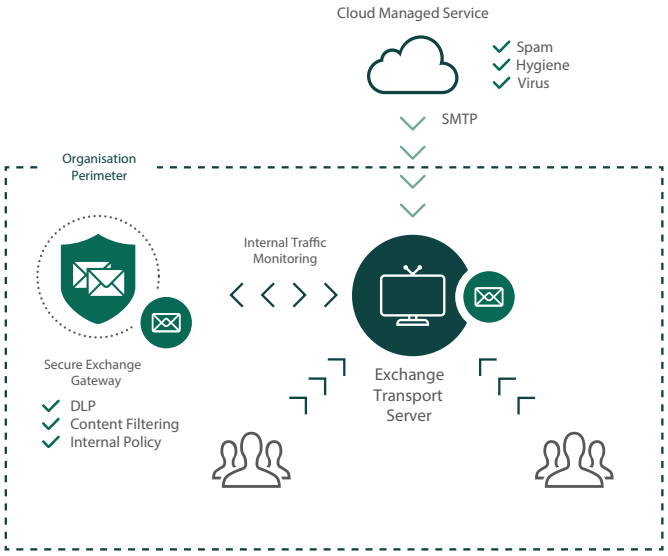


Figure 1: Hygiene Managed Service Model

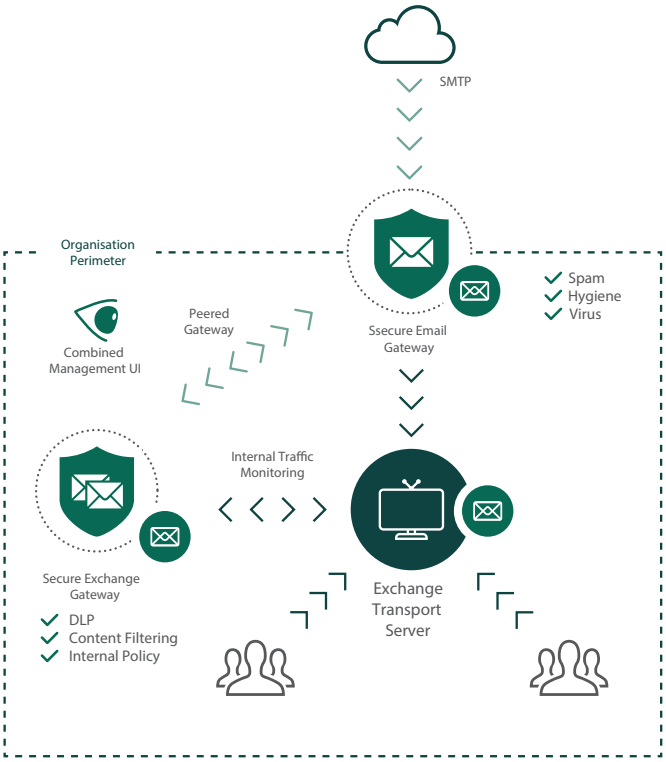


Figure 2: On Premise Layered Security

Integration with Clearswift Gateways and IG Server

The SXG can also be peered with existing Secure Email and Web Gateways to share policies and reporting data.

When the SXG is used in conjunction with the Secure Email Gateway, the System administrator can manage the messaging policies from a single dashboard.

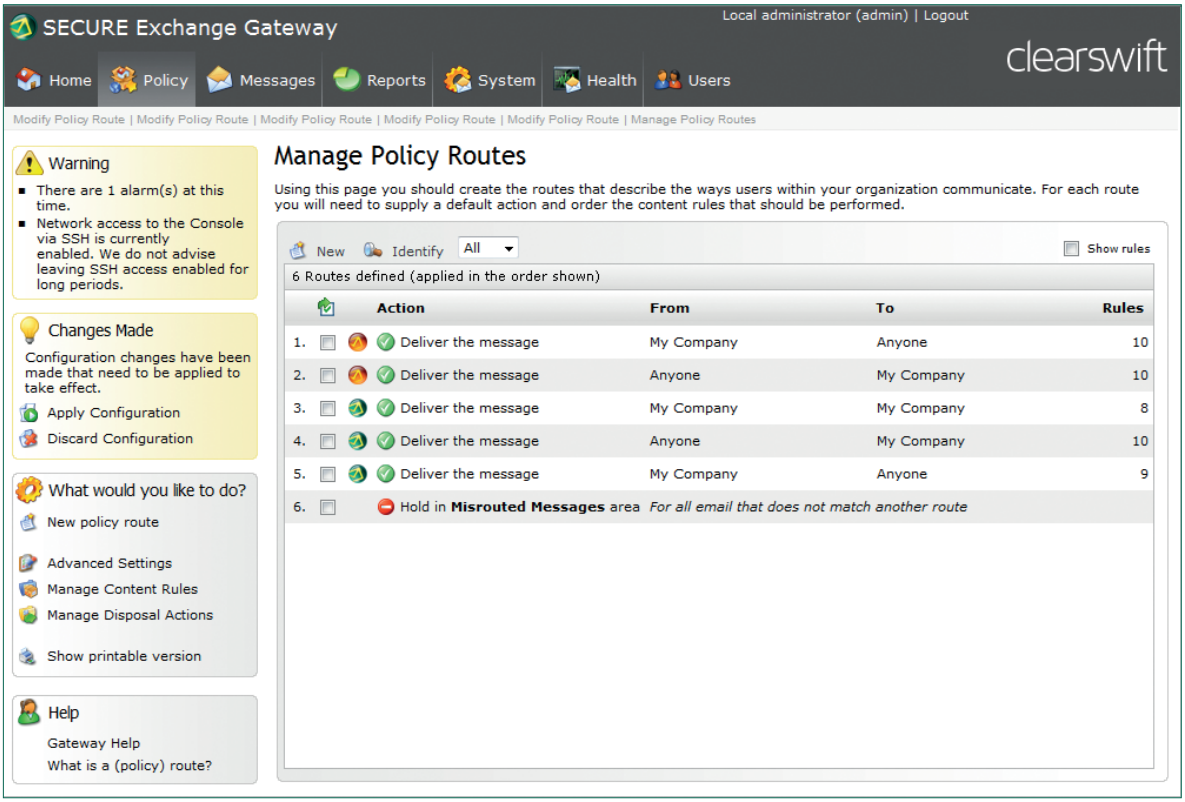


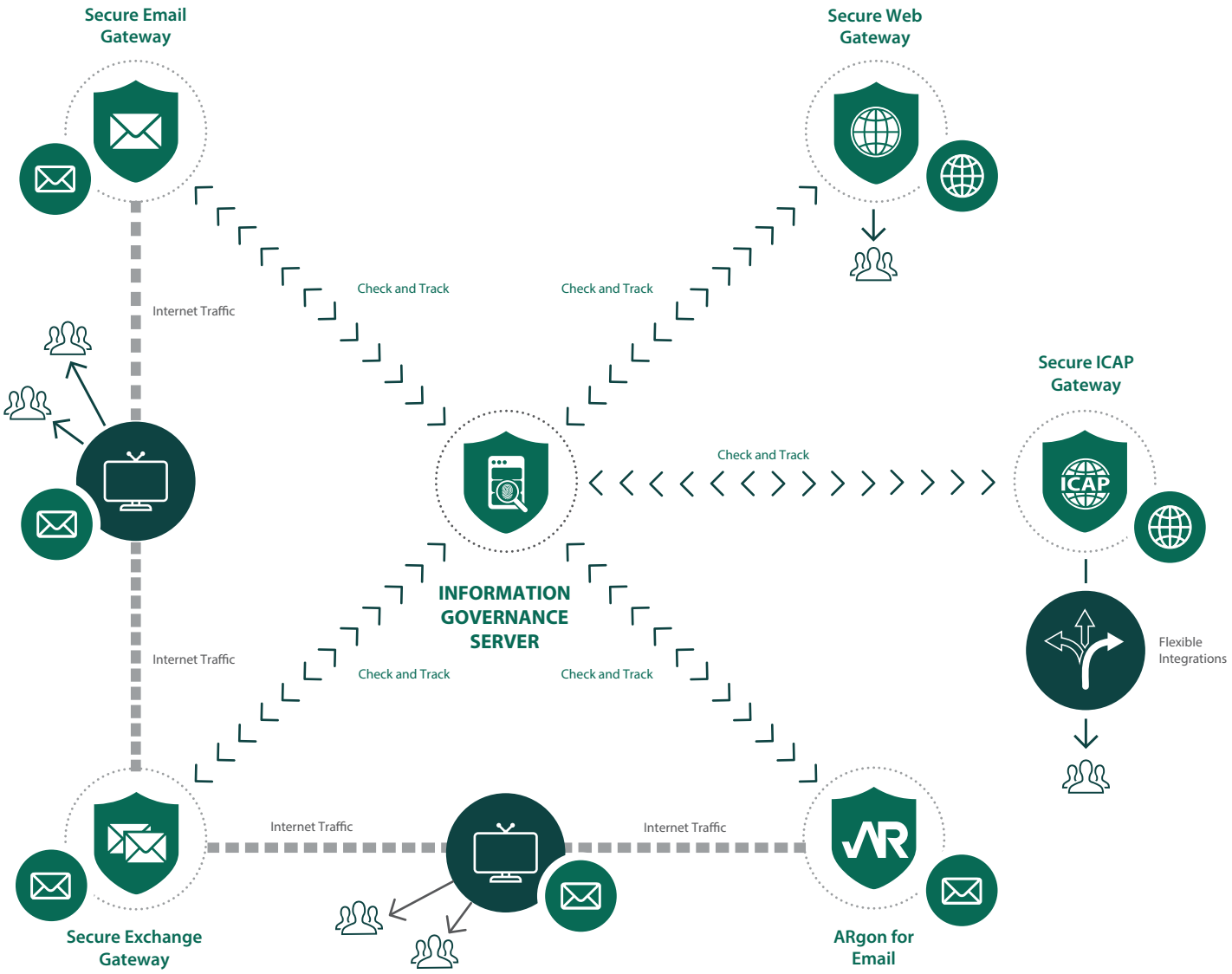
Figure 3. Managing Peered Gateways: System Administrators can manage messaging polices from a single dashboard for Boundary and Internal Email

Data Loss Prevention is typically controlled using known keywords or phrases. However how does an organization deal with sensitive information that is not easy to categorize? Whilst a document may have "Top Secret" in the headers, what happens if someone uses cut-and-paste to copy key sensitive sections into a new uncategorised document? This is where advanced fingerprint algorithms can help to find sensitive documents or even just fragments of them. The Information Governance (IG) Server allows users in the organization to register sensitive data with the IG Server, which stores a digital representation of the whole document as well as the constituent elements, such as paragraphs, images and other embedded content.

The IG server is designed to work with the Secure Exchange Gateway, Secure Email Gateway or Secure Web Gateway concurrently to provide enterprise wide data loss prevention.

When connected to the Information Governance (IG) server, the SXG can be used to detect sensitive content passing internally between users and according to policy the messages and attachment can be blocked if they contravene policy.

The IG server also provides a data tracking service which permits the Administrator to find who may have seen a particular file or document fragment permitting appropriate remediation as required.



Feature	Clearswift SECURE Exchange Gateway
Platform Information	
Platforms supported	Exchange 2007, 2010, 2013
Monitor Mode (process a copy of message without interrupting mail flow)	Yes
AD/LDAP integration	Yes
Deployment options	N+1 offbox load balanced processing agents (filtering does not impact loading on Exchange servers)
DB Maintenance	Automatic
Hygiene	
Choice of AV engine	Avira or Sophos
File detection methods	File Signature, Extension and Checksum
Custom File Format recognition	Yes
Image scanning	Yes (included)
Active Content Detection Filters	Yes
Data Loss Prevention	
Adaptive Redaction: Data Redaction	Yes*
Adaptive Redaction: Document Sanitization	Yes*
Adaptive Redaction: Structural Sanitization	Yes*
Text Analysis: Weighted words, Regular expressions, Boolean operators, Dictionaries	Yes
Predefined Keyword search lists	Multiple, including: PCI, SEC, SOX, Confidentiality, Profanity Lists
Predefined Tokens	Multiple, including: Credit Card, Social Security, IBAN, National Insurance, Tax file number, German Identity, Business Identifier Code
Custom Tokens	Yes
Keyword Search Languages	Supports over 200 character encodings
System Management	
Built-in reporting	Yes
Automated delivery of reports	Yes
End user message release / portal	Yes
Brandable end user release	Yes
iPhone App for end user release system	Yes
Delegated administration	Yes
Automatic patch download	Yes
Virtualization Support	VMware and Microsoft Hyper-V
Notifications to	Sender, Recipient, Named Administrator, Line Manager
Message release via Inform	Yes
Copy Auditor on Message release	Yes
Alarms notification methods	UI, Email, SNMP
Centralized SYSLOG	Yes
Policy Rollback	Yes
Policy Change History	Yes

*Adaptive Redaction has 3 distinct features. A minimum of one is required at implementation. The remaining 2 optional features are available as additional cost options

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.