clearswift
RUAG Cyber Security

Clearswift SECURE Exchange Gateway

Das Clearswift SECURE Exchange Gateway (SXG) schützt in erster Linie vor der internen Verbreitung von kritischen Informationen und der anschließenden externen Versendung, indem es die Umsetzung der Sicherheitspolicies und somit die Einhaltung der Compliance Anforderungen abbildet. SXG erkennt nicht nur Malware, unzulässige Dateitypen und Angriffe durch E-Mail Kommunikation in Exchange 2007, 2010 oder 2013 Umgebungen, sondern entfernt diese auf Basis einer einfach zu definierenden Richtlinie.

Schutz vor Datenverlust

Die Clearswift Advanced Data Loss Prevention-Systeme (DLP-Systeme) sichern die Einhaltung der Richtlinien und Compliance-Vorgaben Ihres Unternehmens. Nachrichten, die nicht den definierten Kriterien entsprechen, können zur späteren Untersuchung in Quarantäne gestellt werden. Anstößige Inhalte werden erkannt und die Verbreitung verhindert. Über eine Stichwortsuche können Begriffe oder Zeichen in E-Mails, PDF- und Office-Anhängen gefunden und dynamisch durch Sternchen ersetzt werden. Dokumenteneigenschaften und Änderungsverläufe in Office- und PDF-Formaten können mit der Funktion Document Sanitization entfernt werden, hieraus resultierende Informationslecks werden somit verhindert.

Einhaltung von Compliance-Vorgaben

Nachrichten und Anhänge können nach Inhalten oder Größe gefiltert werden. Granulare Richtlinien überwachen die Kommunikation zwischen Mitarbeitern oder ganzen Organisationseinheiten. Die Nachrichten können abgewiesen, zur manuellen Freigabe durch autorisierte Mitarbeiter in Quarantäne gestellt oder an Abteilungsleiter weitergeleitet werden, die dann über ihre Freigabe oder Entfernung entscheiden. Diese Prozesse verbessern die Effizienz und entlasten die IT.

Deep Content Filtering und benutzerdefinierte Stichwortsuche

Das Deep Content Filtering einer Nachricht und ihrer Anhänge erkennt unerwünschte Inhalte oder kritische Informationen in über 150 Dateiformaten und in Zeichensätzen von mehr als 200 Sprachen. Unerwünschte Inhalte werden durch eine Stichwortsuche anhand standardisierter und freidefinierbarerer Wörterbücher auf Wort-, Satz- oder Token-Ebene erkannt.

Zusätzlich zur Stichwortsuche können Dateigröße, TrueType-Erkennung und die Analyse nach Dateinamen verwendet werden, um Dateien zu entdecken oder zu entfernen, die nicht geschäftsrelevant sind. Das Versenden von zu großen Dateien, die die Exchange Infrastruktur schädigen oder negativ beeinflussen könnten, wird verhindert.

Umfassende Kontrolle auf Schadsoftware

Mit der Auswahl von Sophos oder Kaspersky erhalten Sie bis zu zwei Antiviren-Engines, die Ihnen die nötige Flexibilität bieten, E-Mails schon beim Erhalt auf gefährliche Inhalte zu überprüfen. Die Exchangeserver werden nicht zusätzlich beansprucht. Strukturelle Gültigkeitsprüfungen von Dateiformaten erkennen, ob Daten entfernt oder hinzugefügt wurden. Structural Sanitization entfernt aktiven Code aus PDF-, Office- und HTML-Dateien zur Minimierung des Risikos von Advanced Persistent Threats im Firmennetzwerk.

Richtlinienbasierte Regeln

Einfach zu definierende Regeln sichern interne und internetbasierte E-Mails ein- und ausgehend. Mittels der AD/LDAP-Integration können Richtlinien auf Benutzerebene, für organisatorische Einheiten oder unternehmensweit aufgestellt werden. Dies ist wichtig, wenn Unternehmen einzelne Abteilungen schützen müssen, bspw. in Banken, Militär und Forschung oder zur Einhaltung der Exportvorgaben innerhalb eines multinationalen Unternehmens.

Monitor-Modus

Ein Monitor-Modus ermöglicht Ihnen die Compliance-Richtlinie zu überprüfen, ohne den Nachrichtenfluss zu beeinträchtigen. SXG verarbeitet Kopien der Nachrichten, um problematische Inhalte in E-Mails aufzuzeigen bzw. herauszufinden und mit Ihren DLP-Richtlinien abzugleichen, ohne False Positives zu produzieren.

Scanprogramme

Anders als die meisten anderen Exchange-Scanning-Produkte bietet Clearswift eine Off-Box-Lösung zur Entlastung Ihrer Exchange-Server. SXG basiert auf einem gehärteten Linux und kann auf physischer Hardware oder virtuell auf vSphere und Hyper-V mit einem Interceptor auf dem Exchange-Server eingesetzt werden, um sicherzustellen, dass die Nachrichten ohne Verzögerung zugestellt werden.

Der SXG Interceptor, eingesetzt auf dem Exchange Transport-Server, leitet eine Kopie der Nachricht an das SXG weiter. Sollte die Nachricht nicht sicher sein, kann diese abgewiesen, verändert oder zur manuellen Überprüfung in Quarantäne gestellt werden.

Implementierungsoptionen

Die Implementierung der SXG-Plattform kann ohne Veränderung der bestehenden Sicherheitsinfrastruktur erfolgen und sowohl über ein ausgelagertes gemanagtes Service-Modell (Abb. 1) als auch über ein mehrschichtiges Sicherheitsmodell vor Ort (Abb. 2) ausgeführt werden.

Verwaltung und Reporting

SECURE Exchange Gateways können zu Gruppen zusammengeführt werden, für die Verwaltung wird nur eine Web UI benötigt. Dies gibt Systemadministratoren mit unterschiedlichen Befugnissen die Möglichkeit, Systemaufgaben wahrzunehmen, wie etwa Unified Policy Definition, Message Management, Reporting und Systemüberwachung.

Exchange-Interceptors werden mit PowerShell konfiguriert und ihre Konfiguration in Active Directory LDS gespeichert, so dass sie von anderen Interceptors in einer Abteilung der Organisation mitgenutzt werden kann.

Abbildung 1: Hygiene Managed Service Model

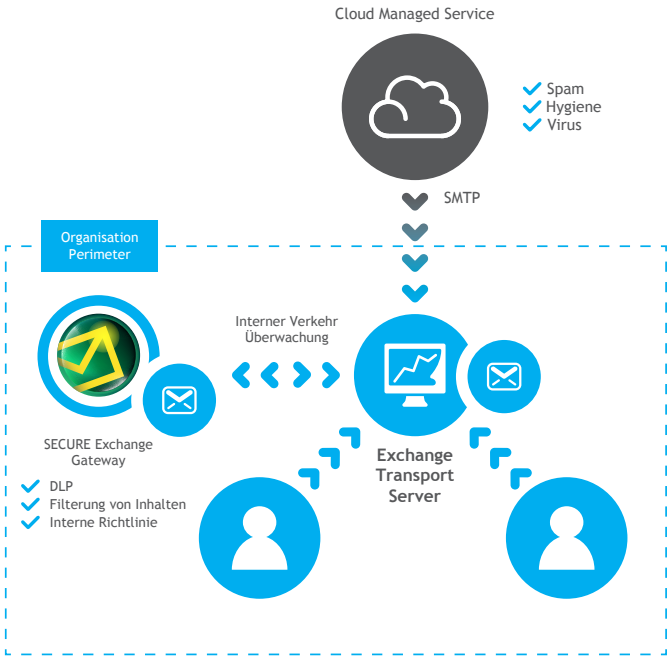
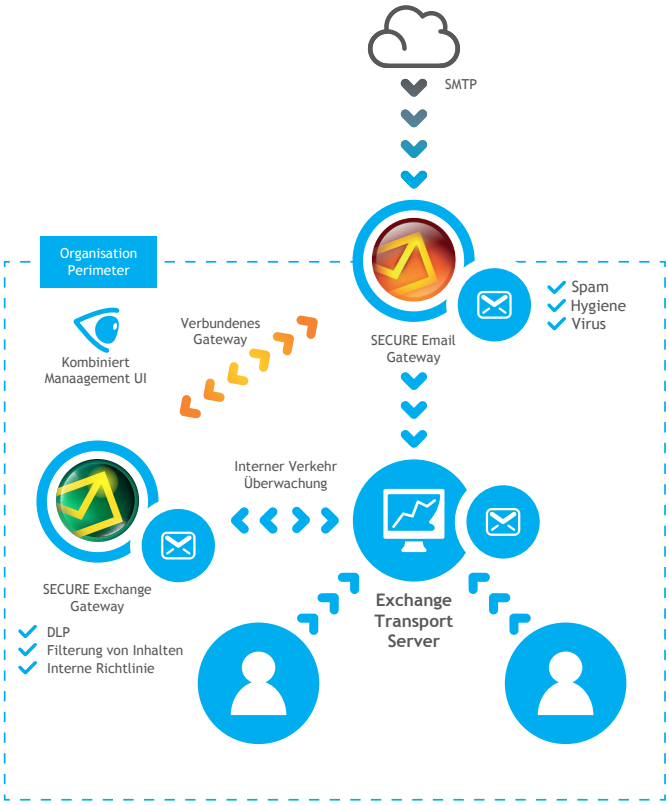


Abbildung 2: Mehrschichtige Sicherheit vor Ort

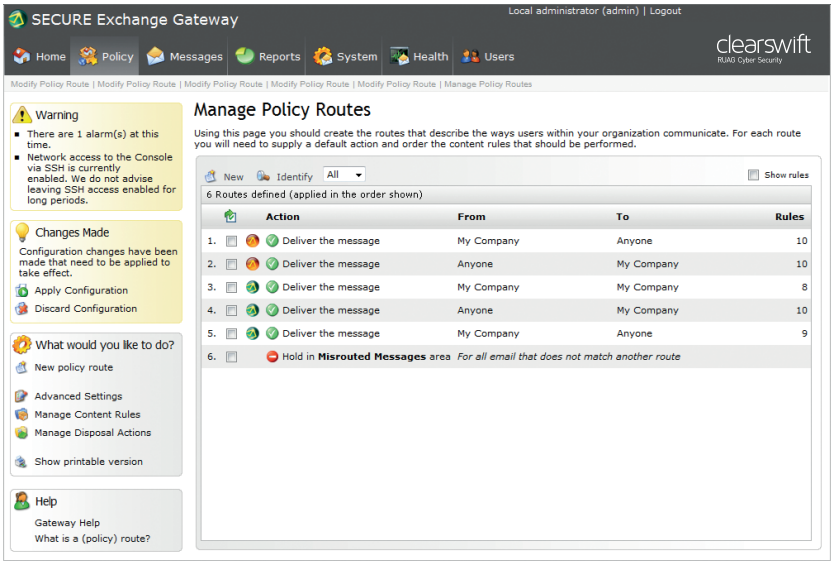


Integration in Clearswift Gateways und IG Server

Das SXG kann auch mit bestehenden SECURE Email und Web Gateways verbunden werden, um Richtlinien und Reportingdaten auszutauschen.

Wenn das SXG in Verbindung mit dem SECURE Email Gateway verwendet wird, kann der Systemadministrator die Messaging-Richtlinien für beide Systeme von einer einzigen Weboberfläche aus verwalten.

Abbildung 3. Verwaltung verbundener Gateways: Systemadministratoren können Messaging-Richtlinien von einem einzigen Dashboard für grenzüberschreitende und interne E-Mails aus verwalten

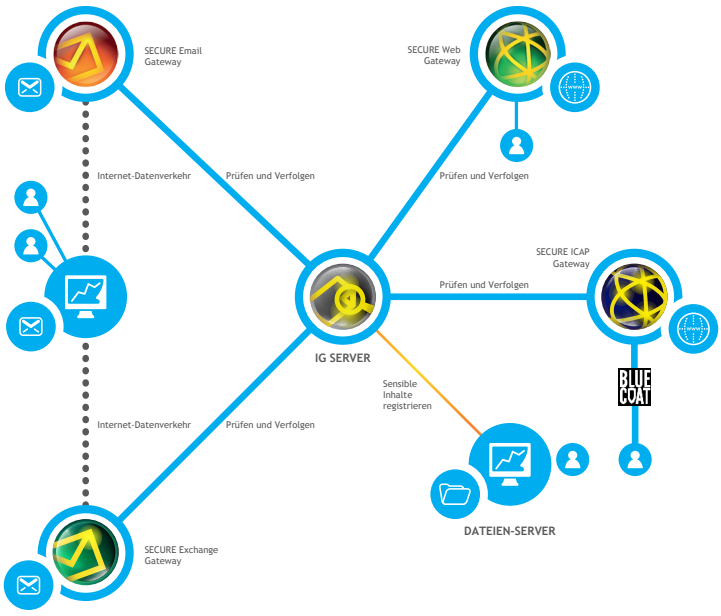


Der Schutz vor Datenverlust erfolgt typischerweise anhand bekannter Stichwörter oder Satzteile. Wie aber verfährt ein Unternehmen mit sensiblen Informationen, die nicht leicht zu kategorisieren sind? Was passiert, wenn jemand sensible Abschnitte aus einem mit “Streng geheim” gekennzeichneten Dokument in ein neues, nicht kategorisiertes Dokument kopiert? Hier können fortschrittliche Fingerabdruck-Algorithmen helfen, sensible Dokumente oder Fragmente zu finden. Der Information Governance (IG) Server gibt Benutzern im Unternehmen die Möglichkeit, sensible Daten auf dem IG Server zu registrieren. Dieser speichert digitale Hashwerte des gesamten Dokumentes sowie seine konstitutiven Elemente wie etwa Absätze, Bilder und andere eingebettete Komponenten.

Der IG Server ist zur Zusammenarbeit mit SECURE Exchange Gateway, SECURE Email Gateway oder SECURE Web Gateway vorgesehen, um einen unternehmensweiten Schutz vor Datenverlust sicherzustellen.

In Verbindung mit dem Information Governance (IG) Server kann das SXG dazu verwendet werden, das Versenden von sensiblen Daten innerhalb des Unternehmens zu überwachen und Missbräuche aufzuspüren. Nachrichten und Anhänge können blockiert werden, wenn sie gegen eine Richtlinie verstoßen.

Der IG Server bietet auch einen Dienst zur Datenverfolgung, mittels dem der Administrator erkennt, wer eine bestimmte Datei oder Teile davon verändert hat.



clearswift
RUAG Cyber Security

Über Clearswift

Clearswift ist ein Spezialist für Informationssicherheit und bietet Unternehmen weltweit anpassungsfähige Cyber-Lösungen zum effektiven Schutz von geschäftskritischen Daten vor internen und externen Bedrohungen.

Clearswift-Lösungen basieren auf einer innovativen Deep Content Inspection Engine, die von einem vollintegrierten Richtlinien-Center gesteuert und kontrolliert wird. Durch die mühelose Verwaltung geschäftskritischer Daten können Unternehmen ferner eine durchgängige Information-Governance-Strategie umsetzen.

Als globales Unternehmen unterhält Clearswift Standorte in Deutschland, Australien, Japan und den USA.

Clearswift hat ein Netzwerk von mehr als 900 Vertriebspartnern weltweit

Weitere Informationen finden Sie unter
www.clearswift.com

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
5th Floor
165 Walker Street, North Sydney
New South Wales, 2060
Australia

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1210
Email: info@clearswift.com.au

Deutschland
Clearswift GmbH
Im Mediapark 8
D-50670 Köln
Deutschland

Tel: +49 (0) 221 8282 9888
Technischer Support: +49 (0)800 1800556
Email: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support: 0066 33 812 501
Email: info.jp@clearswift.com

United States
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

Funktion	Clearswift SECURE Exchange Gateway
Plattform-Informationen	
Unterstützte Plattformen	Exchange 2007, 2010, 2013
Monitor-Modus (Bearbeiten einer Nachrichtenkopie ohne Unterbrechung des Mail-Flows)	Ja
AD/LDAP-Integration	Ja
Einsatzoptionen	N+1-Offbox-Verarbeitungsagenten mit Lastenausgleich (Filterung beeinträchtigt Impact Loading auf Exchange Servern nicht)
DB Maintenance	Automatisch
Hygiene	
Auswahl der AV Engine	Kaspersky und/oder Sophos*
Methoden zur Dateierkennung	File Signature, Dateierweiterung und Checksumme
Erkennung von Dateiformaten	Ja
Image scanning	Ja (inkl.)
Active Content Detection Filters	Ja
Data Loss Prevention	
Adaptive Redaction: Data Redaction	Ja*
Adaptive Redaction: Document Sanitization	Ja*
Adaptive Redaction: Structural Sanitization	Ja*
Textanalyse: Gewichtete Wörter, regelmäßige Ausdrücke, Boolsche Operatoren, Wörterbücher	Ja
Vordefinierte Stichwort-Suchlisten	Multiple, inkl.: PCI, SEC, SOX, Vertraulichkeit, Listen von Schimpfwörtern
Vordefinierte Tokens	Multipel, inkl.: Kreditkarte, Sozialversicherung, IBAN, Steuernummer, deutsche Identität, BIC-Code (Business Identifier Code)
Custom Tokens	Ja
Sprachen der Stichwortsuche	Unterstützt über 200 Zeichencodierungen
System Management	
Eingebautes Reporting	Ja
Automatische Verteilung der Reports	Ja
Persönliche Nachrichtenverwaltung (Quarantäne)/-Portal	Ja
Individuell anpassbare Mitteilungen an Enduser	Ja
iPhone-App für persönliche Nachrichtenverwaltung	Ja
Delegierte Verwaltung	Ja
Automatische Updates	Ja
Support für Virtualisierung	VMware und Microsoft Hyper-V
Benachrichtigungen an	Sender, Empfänger, namentlich genannte Administratoren, Vorgesetzte
Nachrichtenfreigabe über Inform	Ja
Benachrichtigung des Auditors über Nachrichtenfreigabe	Ja
Methoden der Alarmbenachrichtigung	UI, Email, SNMP
Zentralisiertes SYSLOG	Ja
Aufhebung von Richtlinien	Ja
Historie der Richtlinienänderungen	Ja

* Kostenoption