FORTRA™

DATASHEET *(Clearswift)*

Secure Email Gateway

Powerful Email Security with Real-Time Protection

Around the world, defense agencies, governments, and financial institutions rely on Fortra's award-winning, on-premise Clearswift Secure Email Gateway to provide the highest level of protection for email, transforming it from a high-risk communication channel to one that is safe and secure. With deep content inspection capability and powerful adaptive redaction features, it removes evasive cyber threats and prevents unwanted data breaches in real time.

Working alone or alongside cloud-based email applications, such as Microsoft 365 and Google Workspace, the Secure Email Gateway appliance is an essential security layer to maximize cybersecurity defenses.

Unparalleled Deep Content Inspection

Developed with security and performance in mind, the on-premise Secure Email Gateway provides an unparalleled level of content inspection and structural verification.

A Deep Content Inspection Engine detects and analyzes the content of incoming and outgoing emails down to 50 levels. It offers true file-type detection, file structure verification and extracts sensitive data from compressed files, document body, header and footers, or embedded objects.

Game-Changing Adaptive Redaction

Rather than a stop-and-block approach, unique Adaptive Redaction features dynamically modify messages and content in real time, keeping communications flowing and risk-free.

Data Redaction – sensitive data is automatically removed from documents and images. Text in images is identified using Optical Character Recognition (OCR).

Document and Image Sanitization – metadata, change history, and properties are removed from files, including content embedded in images using steganography tools.

Message and Structural Sanitization – URLs are rewritten before they cause harm and active code (macros, scripts and Active/X) is removed from Microsoft Office, Open Office, and PDF files.

PRODUCT SUMMARY

KEY FEATURES

- Multi-layer anti-virus protection (Avira and Sophos)
- Zero-hour anti-malware detection
- Cloud Sandbox from Sophos
- 99.9% spam detection with dual engines
- Sensitive Data Redaction from documents and images
- Document and Image Sanitization
- Structural and Message Sanitization
- Lexical Expression Qualifiers to minimize false positives
- Built-in compliance dictionaries
- Choice of email encryption options

SYSTEM MANAGEMENT

- Flexible and granular policy control
- Active directory or LDAP integration
- Easy-to-use web-based management interface with role-based access control
- Comprehensive workflow options
- Centralized reporting with SIEM compatibility

DEPLOYMENT OPTIONS

- Managed or hosted in ISO-certified data centers
- Public cloud deployment on Microsoft Azure or Amazon Web Services
- Private cloud virtual environment running VMware/Hyper V
- Own or packaged hardware

Inbound Threat Protection

With a choice of Avira or Sophos anti-virus software engines that update every fifteen minutes, email is well-protected. For additional protection against embedded Advanced Persistent Threats (APTs), ransomware, spyware, and phishing emails, these technologies are supplemented with zero-hour anti-malware features and active code detection that the Message and Structural Sanitization provides.

Sandbox

Add additional layers of security against ransomware and targeted attacks with the next-gen Cloud Sandbox from Sophos. As messages arrive at the SEG, they are submitted for AV scanning and any content with executables will be further inspected by the sandbox. The behaviour of files detonated within the sandbox are carefully monitored for tell-tale signs of malicious software. The results are then shared with the SEG where remedial actions to block, deliver, or subject to further checks, such as keyword search, are deployed.

Multi-Layered Spam Defences

Dual anti-spam engines reduce the amount of spam reaching the end user and the number of false positives. DMARC, SPF, and DKIM support reduces spam even further. The multi-layered spam defense mechanism achieves 99.9% detection rates. An Outlook Spam Reporter is included so that spam can be monitored, registered, and eliminated.

Outbound Data Loss

The on-premise Secure Email Gateway minimizes the risk of employees accidentally sharing confidential information and protects valuable company data that malicious insiders may try to exfiltrate.

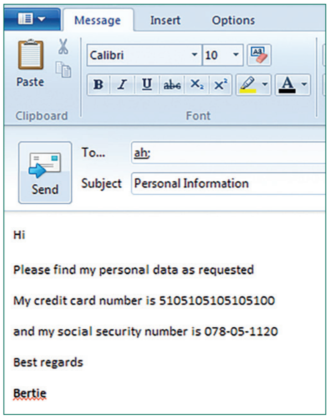
Powerful lexical analysis and regular expression rules search messages and content for keywords and phrases. When policy violations are found, sensitive data can be automatically removed, or managed by System Administrators or Line Managers.

Regulatory Compliance

Data Loss Prevention (DLP) is a key concern for organizations who need to comply with regulatory requirements, such as GDPR, HIPAA, SEC, and SOX. To save deployment time, the on-premise Secure Email Gateway includes built-in compliance dictionaries and over 200 pre-defined PCI and PII tokens to simplify policy definition and deployment.

The Secure Email Gateway appliance can detect, protect, and audit structured data using Lexical Expression Qualifiers to validate sensitive information. This minimizes the number of false positives as it understands when a number might look like a customer ID number, but isn't.

Original Message



To... ah;

Subject Personal Information

Hi

Please find my personal data as requested

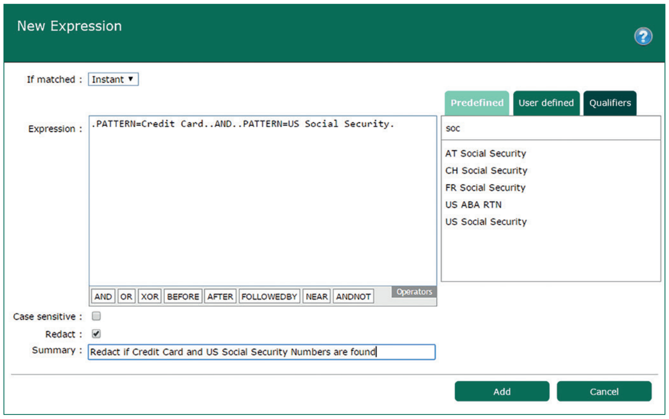
My credit card number is 5105105105105100

and my social security number is 078-05-1120

Best regards

Bertie

Policy to change certain elements



If matched : Instant ▾

Expression : .PATTERN=Credit Card..AND..PATTERN=US Social Security.

soc

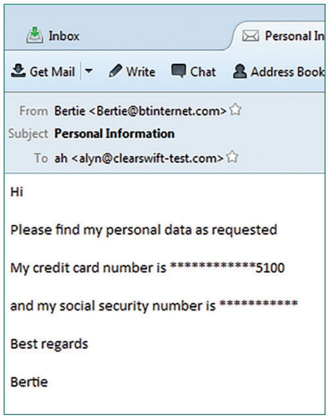
AT Social Security
CH Social Security
FR Social Security
US ABA RTN
US Social Security

Case sensitive : □

Redact : ☑

Summary : Redact if Credit Card and US Social Security Numbers are found

Received Message



From Bertie <Bertie@btinternet.com>

Subject **Personal Information**

To ah <alyn@clearswift-test.com>

Hi

Please find my personal data as requested

My credit card number is ************5100

and my social security number is ***********

Best regards

Bertie

Flexible and Granular Policy Control

Adaptable policies are the key to real-world deployment. If email security solutions are too restrictive, it impacts the organization's ability to work effectively. If they are too lax, security could be compromised. Flexible and granular policy controls enable organizations to balance security with the need to continuously collaborate.

Workflows permit managers to review and release emails so that better context can be applied to message management. Policies can be applied to an individual, a group (department or specific security clearance level), or the whole organization.

Encryption

Some regulations require emails containing sensitive data to be encrypted. The Secure Email Gateway appliance provides Transport Layer Security (TLS) encryption as standard with options to provide S/MIME and PGP message encryption and password-protected files. Additionally, Clearswift works with technology partners to provide portal-based encryption, secure email archiving, and enterprise Digital Rights Management (eDRM).

Let's Get Started

See Fortra's Clearswift Secure Email Gateway in action. Visit us at www.clearswift.com to arrange a demo.

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.