FORTRA

DATENBLATT *(E-Mail-Sicherheit)*

Secure Email Gateway

Leistungsstarke Sicherheit für Ihre E-Mails mit Echtzeit-Schutz

Weltweit vertrauen Unternehmen und Organisationen in den Bereichen Finanzen, Energie, Gesundheit, Regierungen Behörden und anderen dem vielfach ausgezeichneten Secure Email Gateway von Clearswift und erhalten damit E-Mail-Sicherheit auf höchstem Niveau.

Das Secure Email Gateway verringert die hohen Risiken in der E-Mail-Kommunikation und macht diese absolut sicher. Mit umfassenden Funktionen zur Inhaltsanalyse (Deep Content Inspection) und leistungsstarken „Adaptive Redaction Features" werden Cyber-Bedrohungen beseitigt und unerwünschte Datenverstöße in Echtzeit verhindert.

Das Secure Email Gateway arbeitet alleine oder zusammen mit Cloud-basierten E-Mail-Anwendungen wie Office 365 und G Suite und ist eine wichtige Sicherheitsschicht zur Maximierung der Cyber-Sicherheit.

Beispiellose Tiefgreifende Deep Content Inspection

Das Secure Email Gateway wurde von Beginn an auf Sicherheit und Leistung ausgelegt und bietet eine herausragende Inhalts- und Datenstruktur-Analyse. Die Deep Content Inspection Engine erkennt und analysiert den Inhalt ein- und ausgehender E-Mails bis zu einer Tiefe von 50 Ebenen. Es bietet die Erkennung von Dateiformaten (true file type), die Überprüfung von Dateistrukturen und die Extraktion sensibler Daten aus komprimierten Dateien, Dokumenttexten, Überschriften, Fußnoten und eingebetteten Objekten.

Adaptive Redaction Setzt Neue Maßstäbe

Statt eines Stop-and-Block-Ansatzes ändert Adaptive Redaction die Nachrichten und Inhalte dynamisch in Echtzeit und stellt so einen unterbrechungsfreien und risikolosen Kommunikationsfluss sicher.

Das Secure Email Gateway bietet drei Primär-Optionen für Adaptive Redaction:

Data Redaction – Sensible Daten werden automatisch aus Dokumenten und Bildern entfernt. OCR (Optical Character Recognition) erkennt in Bildern verborgenen Text.

PRODUCT SUMMARY

KEY FEATURES

- Mehrstufiger Antivirus-Schutz (Avira, Kaspersky und Sophos)
- Zero-Hour Anti Malware Detection
- Cloud-Sandbox von Sophos
- 99.9% Spam-Erkennung durch zwei AV Engines
- Schwärzen von sensiblen Daten (Data Redaction) in Dokumenten und Bildern
- Entfernen von Metadaten, Änderungsverläufen und Eigenschaften (Document und Image Sanitization)
- Entfernen von Active Content (Structural und Message Sanitization)
- Lexical Expression-Qualifikanten zur Minimierung von „False Positives"
- Integrierte Compliance-Wörterbücher
- Auswahl an Encryption-Optionen

SYSTEM MANAGEMENT

- Flexible und granulare Policy-Steuerung
- Aktive Directory oder LDAP-Integration
- Bedienerfreundliche Web-basierte Bedieneroberfläche mit rollenbasierter Zugangskontrolle
- Umfassende Workflow-Optionen
- Zentralisiertes und SIEM-kompatibles Reporting

BEREITSTELLUNGSOPTIONEN

- Managed oder gehostet in ISO-zertifizierten Rechenzentren
- Public Cloud-Bereitstellung in Microsoft Azure oder Amazon Web-Service
- Private Cloud in virtueller Umgebung mit VMware/Hyper V
- Eigene oder Clearswift Hardware-Racks

Document und Image Sanitization – Metadaten, Änderungsverläufe und Eigenschaften werden aus Dateien entfernt. Dies inkludiert auch mithilfe von Steganografie-Tools in Bildern eingebettete Inhalte.

Structural und Message Sanitization – Aktive Codes (Makros, Skripten und Active/X) werden aus Microsoft Office, Open Office und PDF-Dateien entfernt und URLs werden umgeschrieben, bevor sie Schaden anrichten können.

Inbound Threat Protection

Mit der Anti-Virus Software von Avira, Kaspersky oder Sophos erfolgt die Aktualisierung alle 15 Minuten, so dass E-Mails gut geschützt sind. Für zusätzlichen Schutz vor eingebetteten Advanced Persistent Threats (APTs), Ransomware, Spyware und Phishing-E-Mails werden diese Technologien durch Zero-Hour Anti-Malware Funktionen und Active Code Detection ergänzt, die von Message and Structural Sanitization bereitgestellt werden.

Sandbox

Erhöhen Sie die Sicherheit vor Ransomware und gezielten Angriffen mit der Next-Gen Cloud-Sandbox d von Sophos. Wenn Nachrichten am Gateway ankommen, werden sie zur AV-Überprüfung weitergeleitet, und alle Inhalte mit ausführbaren Dateien werden von der Sandbox weiter untersucht. Das Verhalten von Dateien, die in der Sandbox detonieren, wird sorgfältig überwacht, um Anzeichen von schädlicher Software zu erkennen. Die Ergebnisse werden dann an das Gateway weitergeleitet, wo Abhilfemaßnahmen zum Blockieren, Ausliefern oder Unterziehen weiterer Prüfungen, wie z. B. einer Schlüsselwortsuche, bereitgestellt werden.

Mehrstufige Spam-Abwehr

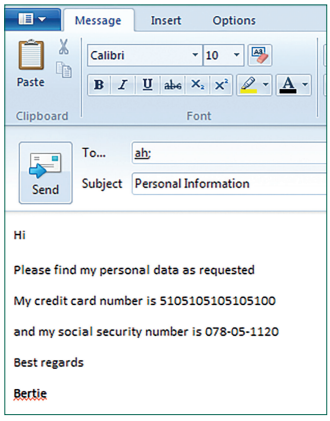
Duale Anti-Spam-Engines verringern die beim Anwender ankommende Menge an Spam und False Positives. DMARC, SPF und DKIM Unterstützung verringern die Spam-Menge noch weiter. Der Spam-Schutz auf mehreren Ebenen erzielt Erkennungsraten von 99.9 %. Der integrierte Outlook Spam Reporter überwacht, registriert und entfernt Spam.

Outbound Data Loss

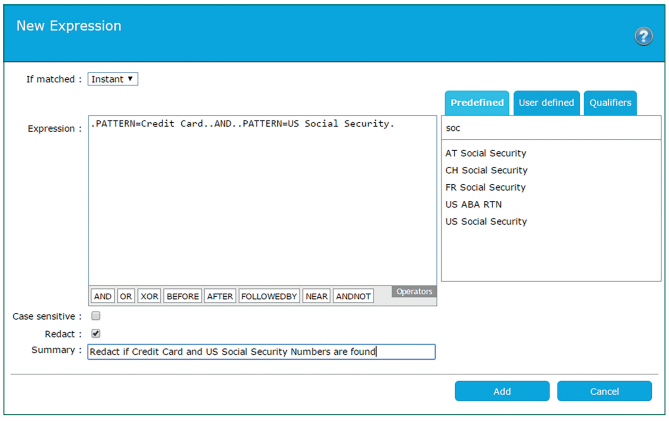
Das Secure E-Mail Gateway minimiert das Risiko der versehentlichen Weitergabe vertraulicher Informationen durch Mitarbeiter und schützt wichtige Unternehmensdaten vor der vorsätzlichen oder fahrlässigen Entwendung durch Insider.

Leistungsstarke lexikalische Analysen und Regeln für reguläre Ausdrücke durchsuchen Nachrichten und Inhalte nach Schlüsselwörtern und Phrasen. Wenn Sie Verstöße gegen die Regelwerke feststellen, können Sie sensible Daten automatisch entfernen oder von Systemverwaltern oder Vorgesetzten managen lassen.

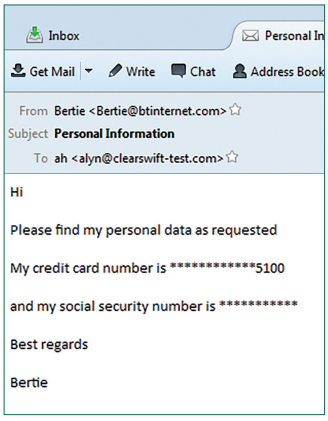
Original-Nachricht



Regeln zur Änderung bestimmter Elemente



Erhaltene Nachricht



Einhalten Gesetzlicher Vorschriften

Data Loss Prevention (DLP) ist ein sensitiver Punkt für Organisationen, die Vorschriften und Regelungen wie GDPR, HIPAA, SEC und SOX einhalten müssen. Um Bereitstellungszeit zu sparen, enthält das Secure Email Gateway integrierte Compliance-Wörterbücher und über 200 vordefinierte PCI- und PII-Token, um die Richtliniendefinition und -Bereitstellung zu vereinfachen

Das Secure Email Gateway erkennt, schützt und prüft strukturierte Daten, denn es bestimmt sprachliche Ausdrücke und ordnet sie ein. So validiert es sensible Informationen. Dieses Verfahren minimiert False Positives, denn es erkennt beispielsweise Zahlen, die wie Kunden-Kennnummern aussehen, aber keine sind.

Flexible Und Detaillierte Richtlinienkontrolle

Anpassbare Policies sind der Schlüssel für die Umsetzung in der Praxis. Wenn E-Mail-Sicherheitslösungen zu restriktiv sind, wirkt sich dies auf die Fähigkeit zur effektiven Arbeit des Unternehmens aus. Wenn sie zu lasch sind, kann die Sicherheit beeinträchtigt werden. Flexible und detaillierte Policies ermöglichen es Unternehmen, die Sicherheit mit der Notwendigkeit einer kontinuierlichen Zusammenarbeit in Einklang zu bringen.

Manager können mit Workflows E-Mails überprüfen und freigeben, um einen besseren Kontext für die Nachrichtenverwaltung zu erhalten. Policies können auf eine Einzelperson, eine Gruppe (Abteilung oder bestimmte Sicherheitsüberprüfungsstufe) oder die gesamte Organisation angewendet werden.

Verschlüsselung

Einige Bestimmungen schreiben die Verschlüsselung sensibler Daten in E-Mails vor. Das Secure Email Gateway bietet standardmäßig TLS (Transport Layer Security), S/MIME und PGP Encryption sowie passwortgeschützte Dateien.

Clearswift-Technologiepartner bieten darüber hinaus Portal-gestützte Verschlüsselung, sicheres Archivieren von E-Mails und die Verwaltung der digitalen Unternehmensrechte (enterprise Digital Rights Management, eDRM).

Lassen Sie Uns Starten

ehen Sie sich das Secure Email Gateway in Aktion an: Besuchen Sie uns unter www.clearswift.de und wir vereinbaren eine Produktdemo.

FORTRA

Fortra.com

Über Fortra

Fortra ist ein Cybersicherheits-Unternehmen wie kein zweites. Wir erschaffen eine einfachere und solidere Zukunft für unsere Kunden. Unsere bewährten Experten und unsere breite Palette integrierter und skalierbarer Lösungen bringen Ausgewogenheit und Kontrolle in Unternehmen auf der ganzen Welt. Bei Ihrer Reise zu mehr Cybersicherheit sind wir Ihr Wegbereiter und Ihr unermüdlicher Verbündeter auf jeder Etappe. Erfahren Sie mehr auf fortra.com/de.