CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift SECURE Gateways

Wesentliche Bestandteile einer Information Governance-Strategie

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Einleitung

Clearswift verfügt über mehr als 15 Jahre Erfahrung im Bereich IT-Security. Weltweit setzen mehr als 3.000 Unternehmen die content-sensitiven, richtlinien-basierten Lösungen von uns ein. Damit sind unsere Kunden in der Lage, ihre E-Mail- und Web-Sicherheit über alle Gateways hinweg und in alle Richtungen zu gewährleisten und zu steuern.

In der Erfolgsbilanz unserer Innovationen verbuchen wir die Entwicklung einer Vielzahl von Funktionen, die heute in der Sicherheitsindustrie als Standard gelten. Unter anderem sind dies:

- **Deep Content Inspection (DCI)**
- **Richtlinien-basierte Verschlüsselung**
- **Scannen von ein- und ausgehendem Content auf mehreren Kommunikationskanälen**

Clearswift ist Marktführer in der IT-Sicherheitsindustrie bei der Entwicklung produktionsreifer Anwendungen und virtueller Gateways auf der vSphere-Plattform. Mit leistungsstarken, effizienten und bewährten content-sensitiven Richtlinien schützen diese Lösungen unsere Kunden und deren Mitarbeiter.

Geschäftspraktiken werden heutzutage ständig geändert. Sie müssen z.B. an die Einführung von Cloud-Technologie und BYOD (Bring Your Own Device) in Verbindung mit der stetig steigenden Anforderung an Zusammenarbeit angepasst werden. Entsprechend entwickelt auch Clearswift die SECURE Gateways weiter und passt Sie an die veränderten Bedingungen an.

“20 % der Fortune 500 vertrauen auf Clearswift”

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

Clearswift SECURE Gateways

Wesentliche Bestandteile einer Information Governance-Strategie

Internet- und E-Mail-Verkehr sind die beiden häufigsten Wege, auf denen Informationen ein Unternehmen verlassen können. Es ist also sinnvoll, sich hier mit konsistenten und sich ergänzenden Technologien zu schützen. Egal ob Sie eine lokale oder cloud-basierte Sicherheitsstrategie verfolgen, die SECURE Gateways können in verschiedenen Einsatzmodi verwendet werden und Ihre vorhandene Technologie ergänzen oder ersetzen.

Web und Email Gateway können verbunden werden, so dass sie Policy-Elemente wie Wörterbücher, Templates und Regeln gemeinsam nutzen und die Richtlinien über eine gemeinsame Konsole definiert werden können.

Während andere Sicherheitslösungen oft äußerst kompliziert zu bedienen und zu verwalten sind, wurden die SECURE Gateways mit Blick auf Bedienungsfreundlichkeit für Administratoren und Benutzer entwickelt. Die Komplexität der Lösung bleibt im Hintergrund, so dass die Gateways sowohl einfach zu benutzen als auch einfach zu verwalten sind.

Dieses Jahr wird die Lösung um Information Governance-Funktionen erweitert, so dass ein Überprüfen von SMTP-E-Mails, Internetverkehr und Exchange-basierten E-Mails möglich ist. Das alles wird über eine zentrale Konsole verwaltet.

Einfach zu benutzen, effizient zu verwalten

Die Gateways wurden für eine einfache Installation, Implementierung und Verwaltung optimiert. Mit Hilfe vorkonfigurierter Hardware eines vom Kunden bevorzugten Hardwareanbieters oder mit vSphere und Hyper-V können unsere Kunden ein Gateway mit ihren Richtlinien in weniger als 30 Minuten einrichten.

Vorkonfigurierte und Beispiel-Regelsätze einschließlich lexikalischer Vorlagen für PCI und PII in Verbindung mit einer intuitiven Benutzeroberfläche ermöglichen eine einfache Konfiguration kundenspezifischer Richtlinien. Durch den einheitlichen Aufbau von Management- und Benutzeroberfläche bei allen Produkten, ist der Trainingsaufwand für Systemadministratoren sehr gering.

Die Vorteile für Administratoren sind automatisierte Updates, regelmäßige Reports, nächtliche Backups, Datenbankoptimierung sowie Anwendungsüberwachung und Alarmierung.

Allgemeine Funktionalität

Die Clearswift SECURE Gateways setzen auf gemeinsam genutzte Kerntechnologien, um Implementierung und Verwaltung so einfach wie möglich zu gestalten und um die Konsistenz über verschiedene Kommunikationsprotokolle hinweg sicherzustellen. Clearswift hat sich mit seiner Deep Content Inspection Engine einen Namen gemacht, und genau diese Engine ist das Herzstück aller Gateways.

Deep Content Inspection

Deep Content Inspection erkennt sensible Daten beim Filtern von Informationen über die Gateways. Die Deep Content Inspection Engine ist zuständig für das:

- **Erkennen des echten Dateityps**
- **Rekursive Extrahieren von Text**
- **Scannen von Text**

Clearswift hat eine eigene, innovative Engine für das Extrahieren und Scannen entwickelt, so dass zusätzliche wichtige Informationen gewonnen werden können. Die Möglichkeit zu erkennen, ob sich der Text im Header, Footer oder im Fließtext befindet, ist beispielsweise bei der Festlegung von Erkennungsrichtlinien wichtig. Ohne diese zusätzlichen Informationen können False Positives unüberschaubar und die Lösung somit unwirksam werden. Das umfassende Verständnis von Dateitypen und der darin enthaltenen Informationen hat zudem zur Entwicklung einer neuen Technologie geführt, der Adaptive-Redaction-Technologie, mit der Dokumente entsprechend individuell definierter Vorgaben verändert und kritische Informationen, die zu einem Datenleck führen könnten, entfernt werden können.

Nachdem die Inhlate analysiert wurden, können die definierten Richtlinien angewandt werden. Die meisten Richtlinien beschäftigen sich mit Data Loss Prevention.

Data Loss Prevention

Data Loss (oder Leak) Prevention (DLP) ist standardmäßig in die SECURE Gateways integriert und setzt bei Entscheidungen auf die von der Deep Content Inspection Engine gelieferten Informationen. DLP ist richtungsunabhängig, das heißt es kann verhindert werden, dass sebsible Informationen das Unternehmen verlassen bzw. in das Unternehmen hinein gelangen. Auf Grund ständig steigender gesetzlicher Anforderungen gewinnt DLP für Unternehmen jeder Größe immer mehr an Bedeutung. Ehemals eine Domäne globaler Unternehmen ist die Technologie heute auch für kleinste Unternehmen geeignet.

Das Scannen von Textelementen in Nachrichten und Anhängen ermöglicht die Erkennung und Redaktion sensibler Informationen, bevor diese das Unternehmen verlassen, einschließlich:

- Einfache Wörter oder Ausdrücke wie Obszönitäten und vertrauliche Informationen
- Handhabung komplexer Tokens wie Kreditkartennummern, Bankdaten und Sozialversicherungsnummern
- Tokens für Personally Identifiable Information (PII)
- Benutzerdefinierte Tokens
- Benutzerdefinierte Muster und reguläre Ausdrücke
- Boolesche Ausdrücke (AND, OR, XOR und ANDNOT) und Ortsoperatoren (NEAR, BEFORE, AFTER und FOLLOWEDBY)
- Wörterbücher mit kundenspezifischen Ausdrücken
- Vordefinierte Compliance inklusive GLBA, HIPAA, SOX und PCI
- Strukturierte Suche nach Informationen aus Datenbanken, z.B. Kundendaten

Der Schlüssel zu einer effizienten DLP-Lösung ist das einfache Festlegen von Richtlinien und deren flexible Anwendung. Mit einem praxisnahen Ansatz kann auch die kleinste IT-Abteilung schnell und einfach effiziente Richtlinien festlegen.

Während die meisten DLP-Lösungen mit einer “Stop und Block”-Strategie arbeiten, die eine ungehinderte Kommunikation rapide einschränkt, bietet die neue Adaptive-Redaction Technologie wesentlich mehr Flexibilität.

Adaptive Redaction

Die neueste Generation unserer Gateways bietet Optionen zur Integration von Adaptive Redaction in die DLP-Aktionen. Standardmäßig vertraut DLP auf die Erkennung unternehmenskritischer Informationen und deren Blockierung am Gateway. Adaptive Redaction bietet jetzt die Option, nicht den Richtlinien entsprechende Daten zu entfernen und die restlichen Daten weiter zu ihrem Ziel zu senden. Es gibt drei mögliche Optionen für Adaptive Redaction:

1. Data Redaction

Diese Richtlinie basiert auf dem Entfernen von Wörtern, Ausdrücken und Tokens. Um die Integrität des Dokuments zu bewahren, werden diese durch „*“ ersetzt. Bei Kreditkarten-Tokens gibt es die Option, alles bis auf die letzten vier Stellen zu ersetzen.

2. Document Sanitization

Moderne elektronische Dokumente enthalten mehr Informationen, als auf den ersten Blick erkennbar. Es gibt versteckte Metadaten sowie Informationen zum Revisionsverlauf. Alle diese Informationen können automatisch entfernt werden, um eine Verbreitung zu verhindern.

3. Structural Sanitization

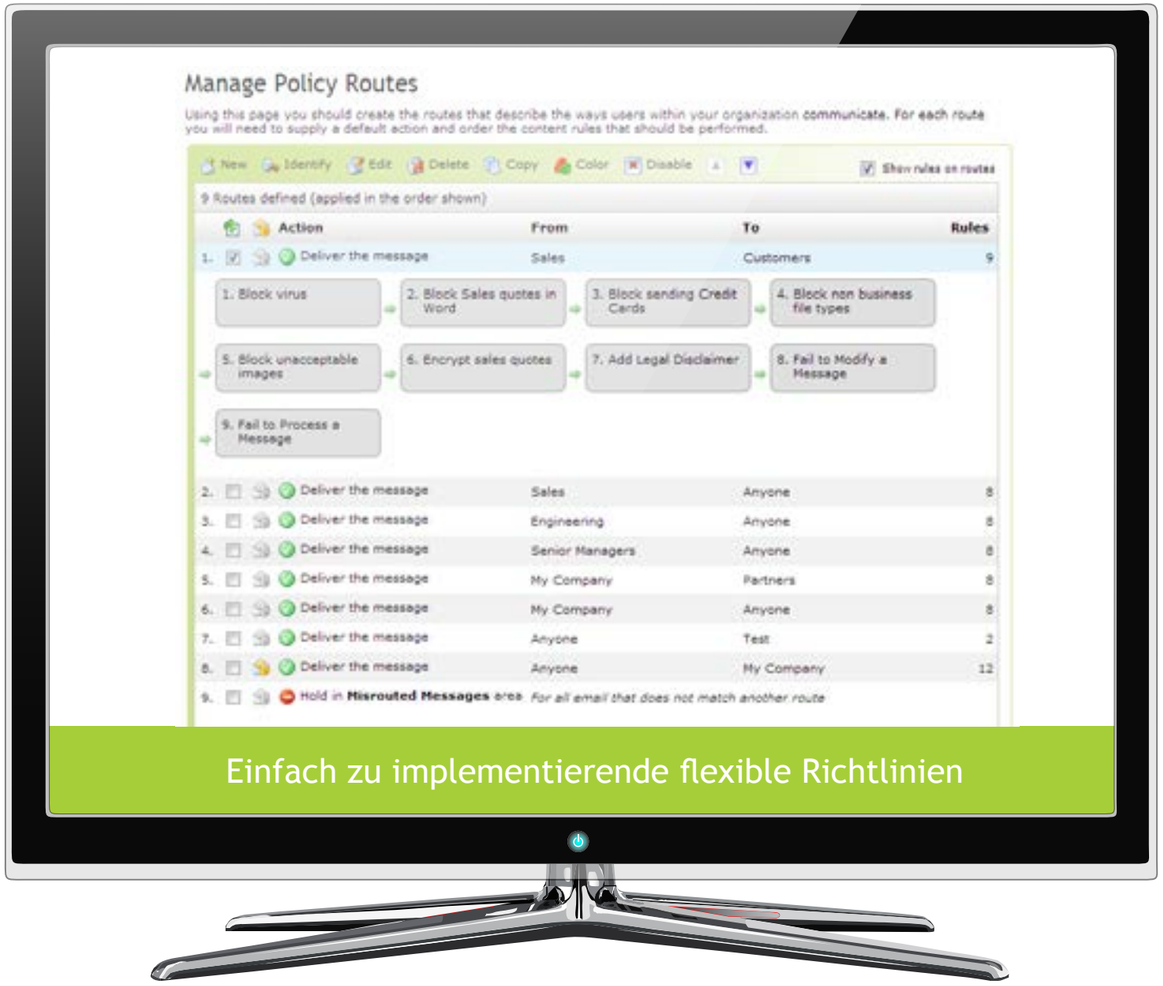
Die Gefahr von Malware in häufig verwendeten Dateiformaten (z. B. Microsoft Office-Dokumenten, Adobe PDFs usw.) steigt ständig. Unsere Gateways können aktive Inhalte aus Dateien entfernen. Die bereinigten Dokumente werden ohne diese Sicherheitsrisiken an ihren Empfänger geliefert.

Adaptive Redaction ist richtungsunabhängig. Das heißt, die Technologie funktioniert bei ein- und ausgehender Kommunikation, so dass damit zum einen beispielsweise verhindert werden kann, dass Kreditkarteninformationen ein Unternehmen verlassen, zum anderen aber auch, dass sie von Mitarbeitern unberechtigterweise empfangen werden.

Von Web-Seiten, die aufgrund unangemessener Inhalte blockiert wurden, können nun die betreffenden Passagen entfernt, und die bereinigte Webseite angezeigt werden. Adaptive Redaction sorgt also beispielsweise dafür, dass Mitarbeiter in Unternehmen soziale Medien nutzen können, ohne anstößige Inhalte zu verbreiten oder zu empfangen.

Ein weiteres Beispiel sind Angebote, die häufig auf Grundlage bestehender Angebote für einen anderen Kunden erstellt werden. Dies hat in der Vergangenheit oft zu peinlichen Momenten geführt, wenn der Kunde im Revisionsverlauf oder in den Metadaten die ursprünglichen Informationen sehen konnte. Die Document Sanitization stellt sicher, dass so etwas nicht mehr passiert.

> Wissensarbeiter verbringen nur 10 % ihrer Zeit mit dem Erstellen „neuen Wissens“, ein Hinweis auf die häufige „Wiederverwendung“.
>
> Reference: International Conference on the Social Impact of Information Technologies, Missouri, 1998.



Schutz vor Sicherheitsrisiken

Während in der Presse viel über die Effizienz von Schutzmaßnahmen wie Antivirus-Lösungen (AV) im Zeitalter von APTs und anderen komplexen Bedrohungen berichtet wird, ist AV nach wie vor eine wirksame Methode zum Schutz vor Viren und anderer Malware in E-Mails und im Internet. Clearswift bietet zwei AV-Lösungen von Sophos oder Kaspersky sowie die Möglichkeit, beide AV Engines gleichzeitig zu verwenden. AV-Definitionen werden von den Gateways automatisch aktualisiert, um den ständigen Schutz der Infrastruktur sicherzustellen. Viele Unternehmen bevorzugen den zusätzlichen Schutz des Einsatzes verschiedener AV-Anbieter am Gateway und an den Endpunkten.

Bedeutung der Mitarbeiter

Das Verstehen der gesendeten Informationen ist nur ein Teil der Lösung. Die Clearswift Gateways werden in Verzeichnissysteme wie Active Directory integriert, um zusätzliche Kontextinformationen auswerten zu können, so dass Richtlinien sowohl personen- als auch gruppenbezogen sein können. Das bedeutet, dass der Geschäftsführer eine andere Richtlinie haben kann als beispielsweise ein Mitarbeiter der Finanzabteilung oder eine Gruppe von Technikern. Diese zusätzliche Dimension für die Richtliniendefinition stellt sicher, dass das System flexibel bleibt und einfach zu implementieren und zu verwalten ist.

Reporting

Alle modernen Sicherheitslösungen müssen Teil eines Information Governance oder Compliance-Programms sein. Die SECURE Gateways bieten umfangreiche Reporting-Funktionen zur Unterstützung dieser Anforderungen, so dass Systemadministratoren schnell sowohl Verwaltungs- als auch Echtzeit-Reports erstellen können. Da solche Berichte häufig gemeinsam genutzt werden müssen, können diese in verschiedenen Formaten erstellt werden, beispielsweise in HTML oder als PDF für die Textdarstellung oder als CSV zum Importieren in eine Tabellenkalkulation.

Für Unternehmen mit einer Security Incident Event Management-Lösung (SIEM) sind die Gateways mit verschiedenen Plattformen kompatibel, unter anderem:

- **RSA Envision**
- **HP ArcSight**
- **Splunk**

Sie können auch SMTP- und SNMP-Alerts einrichten, um Administratoren schneller auf Störungen hinzuweisen. Wird eine Störung erkannt, verringert der einfache Zugang zu detaillierten Protokolldateien die Zeit für die Störungsbehebung.

Alle Änderungen der Systemkonfiguration werden überprüft. Mit der rollenbasierten Zugriffssteuerung können Zuständigkeiten einfach delegiert und jeder Versuch zur Umgehung der Richtlinien erkannt werden.

Clearswift SECURE Email Gateway

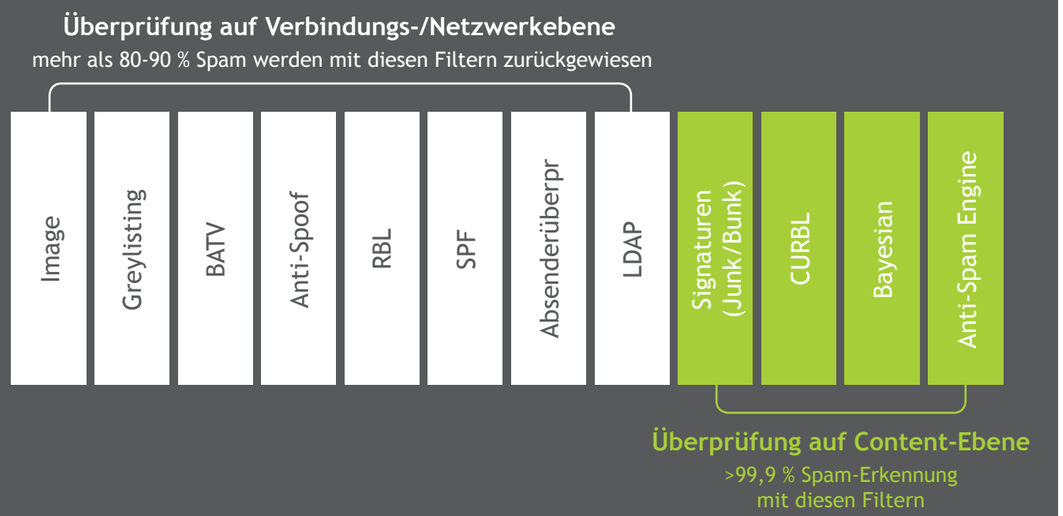
Das SECURE Email Gateway (SEG) basiert auf Clearswift MIMEsweeper. Zusammen mit den oben beschriebenen gemeinsamen Funktionen bietet es sichere, E-Mail-basierte Kommunikation in Übereinstimmung mit den Geschäftsanforderungen eines Unternehmens.

Spam-Schutz

Der Schutz vor Spam auf mehreren Ebenen bietet Prüfungen auf Netzwerk- und auf Verbindungsebene in Kombination mit einer Überwachung der Inhalte. Der Schutz umfasst das TRUSTmanager IP Reputation System, das Rückmeldungen zu vertrauenswürdigen (“guten”) und nicht vertrauenswürdigen („schlechten“) Absendern nutzt, um Spammer und Malware anhand der IP-Verbindung effizient zu blocken. Ein cloud-basiertes System zur Spam-Erkennung identifiziert neue Spam-Wellen, sobald diese auftreten.

Genau wie beim Antivirusschutz werden die Definitionen ständig aktualisiert, um einen umfassenden, aktuellen Schutz auch vor neuesten Bedrohungen sicherzustellen.

Eine Kombination aus verschiedenen Technologien bietet umfassenden Spam-Schutz



Die Belästigung durch Spam ist nach wie vor ein Problem für Unternehmen. Das SEG vereint mehrere Filtertechniken für eine Erkennungsrate von über 99,9 %.

ImageLogic

In der Vergangenheit mussten nur pornografische Bilder gesperrt werden. Dies ist zwar immer noch der Fall, aber die in das Email Gateway integrierte ImageLogic-Funktion kann z.B. auch eingesetzt werden um zu verhindern, dass geistiges Eigentum, das in Bildern enthalten ist, das Unternehmen verlässt.

Verschlüsselung

Da eine sichere Zusammenarbeit immer wichtiger wird, benötigen Unternehmen Methoden zur Verschlüsselung von Inhalten, die auf Absender- und Empfängerseite einfach anzuwenden sind und alle Anforderungen an die Unternehmenssicherheit sowie gesetzliche Vorgaben erfüllen.

Das SEG bietet eine breite Palette an Verschlüsselungsoptionen auf Verbindungs- und Nachrichtenebene, so dass Unternehmen sicher sein können, dass ihre Datenschutzanforderungen erfüllt werden.
Dies sind unter anderem:

- **TLS**
- **S/MIME**
- **PGP**
- **Ad-Hoc passwortgeschützt oder verschlüsselt**
- **Portal (pull and push)**

Diese Methoden können kombiniert eingesetzt werden: Es können beispielsweise Ad-hoc passwortgeschützte Dateien über das Portal versendet werden.

Mit den PKI-Methoden von S/MIME und PGP wird die einfache Verwaltung der Schlüssel wichtig. Das SEG bietet hier eine Funktion für das automatische Abrufen von Zertifikaten und eine Validierung mittels Online Certificate Status Protocol (OCSP). Somit ist nur ein geringer Administrationsaufwand erforderlich.

Verwaltung persönlicher Nachrichten

Die Freigabe von Nachrichten kann von den Benutzern selbst vorgenommen werden. Zu diesem Zweck erhalten sie Zugriff auf den Quarantäne-Ordner und können dann die unter Umständen fälschlicherweise als Spam kategorisierten Nachrichten in eine Whitelist eintragen oder einmalig freigeben. Das SEG erweitert diese Funktion, so dass Benutzer oder delegierte Personen selbst für die Freigabe von ein- und ausgehende Nachrichten entsprechend der Unternehmensrichtlichien verantworltich sind.

Das SEG bietet zudem eine Vielzahl an Methoden, mit denen die Benutzer ihre E-Mails über ein E-Mail-Digest, ein Webportal oder über eine App für Apple iPhone und iPad verwalten können.

So können beispielsweise Rechtsanwälte mit Fällen, bei denen in Gerichtsdokumenten Obszönitäten vorkommen, eine Verletzung der Richtlinien auslösen und gesperrt werden. Dank der Verwaltung persönlicher Nachrichten können diesen nun Berechtigungen zur Freigabe dieser Nachrichten mit Hilfe eines einfachen Hyperlinks eingerichtet werden, ohne dass der Administrator tätig werden muss.

Selbstverständlich werden alle diese Transaktionen für die Compliance überprüft.

Clearswift SECURE Web Gateway

Das SECURE Web Gateway (SWG) umfasst die oben genannten allgemeinen Funktionen, ist jedoch speziell für den Einsatz mit webbasierter Kommunikation über HTTP und HTTPS ausgelegt.

Implementierung

Dank der einfachen Implementierung können Unternehmen das Produkt schnell in ihre Infrastruktur integrieren. Das SWG kann entweder als Proxy (Forward, Explicit), Transparent (WCCP) Proxy oder in Verbindung mit Firewalls mit Unterstützung für richtlinienbasiertes Routing eingerichtet werden.

HTTPS Scanning

Immer mehr Unternehmen sichern ihre Webseiten heute mit HTTPS, um das Abhören von Browsersitzungen zu verhindern. Mit dieser Technologie werden manche Content Scanning-Lösungen unbrauchbar, das SWG verfügt jedoch über eine integrierte SSL-Verschlüsselungs-Engine, so dass diese Sitzungen automatisch entschlüsselt und an die Content Scanning Engine weitergeleitet werden. So ist jederzeit sichergestellt, dass es nicht zu Richtlinenverletzungen kommt.

Flexible Richtlinien

Das Internet gilt heute als Erweiterung ihrer eigenen Infrastruktur, und mehr und mehr Unternehmen vertrauen auf cloud-basierte Dienste wie Salesforce für CRM, Office365 für Nachrichten und Webseiten wie Dropbox für die gemeinsame Nutzung von Dateien.

Mit derart unterschiedlichen Geschäftsanforderungen sind Sicherheitsprofile unumgänglich, um sicherzustellen, dass den Benutzern sowohl im Büro als auch extern Richtlinien zur Verfügung gestellt werden, die ein effizientes und sicheres Arbeiten ermöglichen. Ebenso wie der Zugriff auf Geschäftsseiten erforderlich ist, lassen viele Unternehmen die eingeschränkte Nutzung sozialer Netzwerke durch ihre Mitarbeiter zu.

Unternehmen müssen festlegen können, wer diese Services basierend auf Authentifizierung (ID) oder Abteilung des Unternehmens nutzt, wann diese genutzt werden und wie lange.

So können Regeln erstellt werden wie:

- Personalabteilung kann LinkedIn und Facebook den ganzen Tag lang nutzen
- Alle anderen Benutzer können LinkedIn zwischen 12:00 und 14:00 für max. 1 Stunde verwenden
- Alle Benutzer können Facebook zwischen 12:00 und 14:00 für max. 1 Stunde verwenden und ihren Status aktualisieren, jedoch keine Dateien hochladen

Selbstverständlich unterliegen alle veröffentlichten Inhalte nach wie vor den Sicherheitsrichtlinien des Unternehmens für den jeweiligen Mitarbeiter.

Kategorisierung von Websites

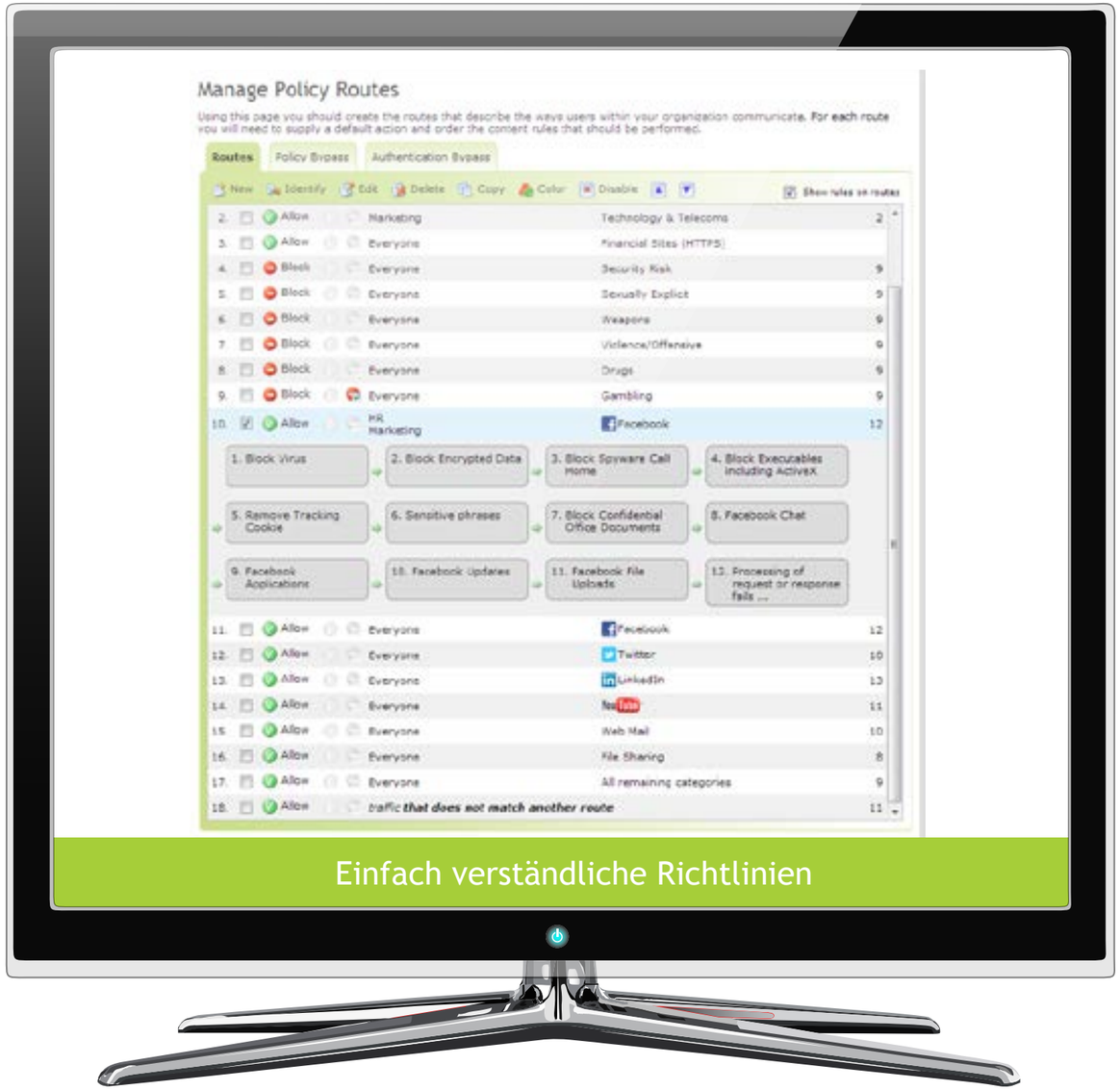
In das SWG ist eine URL-Filter-Engine mit über 50 Millionen URLs integriert, die täglich aktualisiert werden und in mehr als 80 verschiedene Kategorien eingeteilt sind, einschließlich Phishing, Malware und Sicherheitsrisiko. Malware-Definitionen werden stündlich aktualisiert, um den integrierten Viren-Scanner bei allen Downloads zu unterstützen.

Zusammen mit der URL-Datenbank erfolgt eine Kategorisierung in Echtzeit, die den Inhalt der Seite beim Herunterladen erkennt. So kann das SWG feststellen, ob Seiten unter Umständen pornografische Inhalte oder Gewalt enthalten oder auf entferne Proxies zugreifen.

Damit wird sichergestellt, dass Mitarbeiter trotz des ständig steigenden Umfangs persönlicher Inhalte in sozialen Netzwerken vor zwar regelkonformen, aber gehackten oder missbrauchten Seiten geschützt sind.

Remote Client Option

Das SWG unterstützt Remote Clients, das heißt, das Gerät unterliegt nach wie vor den Unternehmensrichtlinien, auch wenn der Benutzer nicht mit dem Unternehmensnetzwerk verbunden ist. BYOD-Plattformen gewährleisten, dass Unternehmensinformationen sicher sind, egal von wo aus der Zugriff darauf erfolgt.



Clearswift SECURE File Gateway (SFG)

Mehr als nur E-Mail

Ihrem Unternehmen sind die Gefahren durch E-Mails sicherlich bekannt, aber wie steht es um Dateien, die zu groß für einen E-Mail-Anhang sind? Das Clearswift SECURE File Gateway kann bis zu 16 GB große Dateien scannen, während diese intern zwischen verschiedenen Abteilungen oder extern über FTP oder andere Übertragungsprotokolle übertragen werden, und so umfassende Datensicherheit gewährleisten.

Inhaltserkennung

Die Content Inspection Engine des File Gateway erkennt mehr als 150 verschiedene Dateiformate mit leistungsfähigen Techniken für das Signatur- und Daten-Parsing, die unzuverlässige externe Indikatoren wie Dateinamenerweiterungen ignorieren. Die Engine führt eine rekursive Zerlegung der Dateien durch, öffnet Archivdateien wie ZIP und TAR systematisch zur Durchsuchung und lokalisiert alle eingebetteten Objekte wie Grafiken oder aktive Inhalte in Office-Dokumenten. Die Untersuchung wird so lange fortgesetzt, bis nichts mehr zu verarbeiten ist.

Dank der Erkennung bestimmter Dateitypen kann mit einer Richtlinie festgelegt werden, welche Dateitypen zulässig sind und welche gesperrt werden. Die Untersuchung umfasst auch Textinhalte und erkennt Wörter und Ausdrücke in den Dateien.

Integrität durch zwei Personen

Da Inhalte unter Umständen äußerst sensibel sind, unterstützt das SFG das Vier-Augen-Prinzip, also die Überprüfung von Änderungen durch zwei Personen. Änderungen werden erst übernommen, wenn ein zweiter Administrator die Änderungen des ersten Administrators bestätigt hat.

Software Developer Kit (SDK)

Die zentrale Technologie aller Clearswift-Produkte, eine Hochleistungs-Content Inspection Engine mit umfassender Datenerkennung und gründlicher Datenverarbeitung, ist für Systemintegratoren auch als Software Developer Kit (SDK) erhältlich. Der SDK bietet Zugriff auf alle Schlüsselfunktionen, unter anderem:

- Datenerkennung mit echter Dateitypisierung, nicht einfach nur Erkennung der Erweiterung
- Erkennung von mehr als 150 Formaten
- Überprüfung und Verifikation der Datenintegrität
- Zerlegung verschachtelter und komprimierter Dateien (inkl. großer Dateien bis 16 GB) und anschließende Analyse der extrahierten Dateien
- Text-Extrahierung aus standardmäßigen Office-Dateien (inkl. MS Office, OpenOffice, PDF und HTML) mit Pattern-Vergleich, programmatischen Operatoren und mehr
- Erkennung aktiver Inhalte inkl. Makros und Skripten in Office- und PDF-Dateien
- Malware-Erkennung inkl. Schnittstellen für AV- Engines von Drittanbietern

Der SDK wird von Unternehmen mit Kunden in allen vertikalen Märkten weltweit verwendet, um die Einhaltung gesetzlicher Bestimmungen sicherzustellen, Lecks sensibler oder geheimer Informationen zu verhindern und unangemessene Kommunikation zu erkennen.

Packaging

Mitgeliefert werden Schnittstellen, Dokumentation und Beispielcode in C, C++ und Java. Unterstützt werden die Plattformen Windows 2003/2008, Red Hat Enterprise Linux 5/6 in 32- und 64-bit. SDK erlaubt Software Entwicklern eigene Client/Server Applikationen zu programmieren, die sensibler mit den Inhalten umgehen.

Optionen für die Gateway-Implementierung

Die Clearswift-Sicherheitslösungen sind mit einer Vielzahl von Implementierungsoptionen passend für Ihre IT-Infrastruktur erhältlich. So sparen Sie Zeit und Kosten.

Für eine schnelle Rentabilität und effiziente Einsparungen ist eine einfache Implementierung unverzichtbar. Mit den Optionen von Clearswift erhalten Sie umfassende Sicherheit für Internet und E-Mail - angepasst an Ihre individuellen Vorstellungen und Anforderungen.

Hardware-Optionen

Die Clearswift SECURE Web und Email Gateways sind als vorkonfigurierte Appliances erhältlich, bereit für die sofortige Implementierung in Ihrem Netzwerk. Eine breite Palette an Hardware-Profilen ermöglicht die Auswahl der passenden Konfiguration für Ihre Filteranforderungen und bietet Optionen für zukünftige Erweiterungen. Hinter den Hardware-Optionen von Clearswift stehen zudem Optionen wie „Nächster Werktag“ oder „Vier Stunden“ für den Vor-Ort-Service.

Software-Optionen

Die Clearswift SECURE Lösungen sind auch für die Implementierung auf Ihrer eigenen Server-Hardware erhältlich, so dass die Konsistenz Ihrer Umgebung mit dem System Ihres bevorzugten Anbieters gewährleistet ist. Die SECURE Gateways laufen auf einer verbesserten Linux-Distribution und bieten höchste Flexibilität für die Hardware Ihrer Wahl.

Virtualisierungsoptionen

Die Clearswift SECURE Lösungen unterstützen zudem die Virtualisierung mit VMware und Hyper-V für das Filtern von E-Mails und ermöglichen so das Erstellen privater Cloud-Sicherheitssysteme für eine noch höhere Flexibilität bei der Netzwerkverwaltung. Ihre Implementierung kann also ensprechend Ihren speziellen Geschäftsanforderungen und Umgebungen aus einer Kombination physischer und virtualisierter Server bestehen.

Peer Gateways

Wird mehr als ein Clearswift Gateway oder mehr als ein Gateway-Typ (z.B. Web und Email) eingesetzt, kommt die Integration an allen Punkten zu tragen. Peer Gateways nutzen gemeinsame Richtlinien und Sicherheitseinstellungen, so dass beim Ausfall eines von zwei Gateways gleichen Typs der verbleibende Gateway die Aufgaben des anderen übernehmen kann. Um unterschiedliche Gateway-Typen innerhalb eines Unternehmen zu konfigurieren, müssen Administratoren nur auf einer Oberfläche arbeiten, und können so konsistente Richtlinien über mehrere Kommunikationsprotokolle sicherstellen.

“Weltklasse Produkte, Support rund um die Uhr und professionelle Services für Unternehmen”

Support und professioneller Service

Die Entwicklung weltweit führender Produkte wird durch Support rund um die Uhr und professionelle Services abgerundet.

Standard-Support

Der Standard-Support bietet schnellen Service rund um die Uhr, so dass Clearswift bei Störungsmeldungen sofort aktiv werden kann. Status und Fortschritt eines Vorfalls sind durch unser End-to-End-Management jederzeit klar ersichtlich.

Erweiterter Support

Der erweiterte Support trägt der geschäftskritischen Bedeutung der Clearswift-Lösungen Rechnung. Er bietet noch breitere Unterstützung einschließlich automatisierter Überwachung des Service und der Reports sowie eine regelmäßige Überprüfung des Service, um durch einen pro-aktiven Ansatz weitere Sicherheit für einen konsistenten Geschäftsbetrieb zu bieten.

Premium-Support

Mit dem Premium-Support bekommen unsere Kunden einen persönlichen Support Account Manager zugewiesen. Außerdem beinhaltet das Angebot Beratung zu Best Practices, Vor-Ort-Support und die regelmäßige Überprüfung der Services vor Ort – eine echte Partnerschaft mit unseren Kunden.

Professional Services

Der professionelle Service für Unternehmen unterstützt Kunden bei allen Sicherheitsaspekten ihrer Infrastruktur. Wir beraten sie bei der Entwicklung der Gateway-Infrastruktur und bieten einen Installations- und Konfigurations-Services. Der Clearswift Professional Service umfasst auch die Entwicklung von Richtlinien, die Systemaktualisierung sowie eine Funktionsprüfung des Systems.

Zusammenfassung

Die Clearswift SECURE Gateways bieten Unternehmen aller Größen die Möglichkeit, eine fortschrittliche Sicherheitslösung für Internet und E-Mail zu implementieren

Mit integrierten Funktionen für Data Loss Prevention (DLP) bieten sie ebenso Schutz vor eingehenden Bedrohungen wie vor Datenlecks. Es gibt neue Technologieoptionen, mit denen die Implementierung von DLP noch kosteneffizienter wird und neue Funktionsweisen unterstützt werden.

Hauptfunktion	SECURE Email Gateway	SECURE Web Gateway
Deep Content Inspection	X	X
Schutz vor Datenverlust (DLP)	X	X
Antivirus	X	X
Verschlüsselung*	X	
Unterstützung von Remote Clients*		X
Textredaktion*	X	X
Document Sanitization*	X	X
Structural Sanitization	X	X
Standard-/Erweiterter*/Premium*-Support	X	X
Professioneller Service*	X	X

*Option mit zusätzlichen Kosten

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 einfache und sichere 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 auf **www.clearswift.com**

CLEARSWIFT
ADAPTIVE CYBER PROTECTION

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
Landsberger Straße 302
D-80687 München
Deutschland

Tel: +49 (0)89 904 05 206
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
Tel (Toll Free): +1 888-937-7938
Technical Support:
+1 856 359 2170
Email: info@us.clearswift.com