

Axway Secure Messenger

Schützen Sie Ihr Unternehmen mit richtlinienbasierter E-Mail-Verschlüsselung



Kein Unternehmen möchte wegen eines Datenlecks in die Schlagzeilen geraten — erst recht nicht wegen einer unbeabsichtigten Offenlegung sensibler Daten durch einen Mitarbeiter, der eine ungesicherte E-Mail-Nachricht oder -Anlage an die falsche Adresse sendet. Sicherheitsverstöße dieser Art können verheerende Folgen haben — von Datenverlust und Betriebsausfall über Beschädigung von Marke und Ruf bis hin zu Gerichtsverfahren und Strafzahlungen.

Axway Secure Messenger kann Ihr Unternehmen durch verbesserte E-Mail-Sicherheit, Governance und Compliance vor diesen Gefahren schützen. Mit einem State-of-the-Art SMTP Relay, kombiniert mit leistungsfähiger policy-basierter Inhaltsfilterung, überprüft Secure Messenger alle ankommenden und abgehenden E-Mail-Nachrichten am Internet-Gateway. E-Mail-Inhalte und angehängte Dateien, die die Sicherheitsrichtlinien Ihres Unternehmens verletzen, werden erkannt und verdächtige Nachrichten automatisch auf einen sicheren Kanal umgeleitet, sodass entsprechende Maßnahmen, verschlüsselte Auslieferung, Löschung, Quarantäne usw., getroffen werden können. Dieser perimeterbasierte Ansatz stellt sicher, dass alle internen und externen Benutzer zu jeder Zeit die Unternehmensrichtlinien einhalten, ohne auf ihren Desktops selbst Verschlüsselungssoftware einrichten und verwalten oder von ihren üblichen Nutzungsmustern abweichen zu müssen.

Wesentliche Leistungsmerkmale und Vorteile

Umfassende

Verschlüsselungsfunktionen

Sicherer ankommender und abgehender E-Mail-Verkehr für Gateway-to-Gateway-, Gateway-to-Desktop- oder Web-Auslieferung.

- Verschlüsseln und authentisieren Sie Nachrichten basierend auf zentralisierten Richtlinien und automatischem Nachrichten-Routing.
- Verwenden Sie E-Mail zur Auslieferung vertraulicher Informationen und geistigem Eigentum sowie zur Dokumentation sensibler geschäftlicher Transaktionen.
- Stellen Sie sichere E-Mail-Funktionen für jeden Mitarbeiter, Kunden oder Partner bereit, ohne dass dieser neue Software installieren und erlernen muss. Automatische Gateway-to-Gateway-Verschlüsselung erfordert keinerlei Eingriffe von Seiten des Endbenutzers.



Wesentliche Leistungsmerkmale und Vorteile**Leistungsfähiges E-Mail-Policy-Management**

Definieren und verwalten Sie Richtlinien für Analyse, Management, Schutz, Rückverfolgung und Reporting des ankommenden und abgehenden E-Mail-Verkehrs.

- Einfache Inhaltsfilterung per Kontrollkästchen, intuitives Richtlinienmanagement und automatische Gateway-to-Gateway-Verschlüsselung verhindern die unbeabsichtigte Offenlegung von Daten.
- Nutzen Sie vorhandene Anwendungen und Netzwerke mit Passwortanmeldung und Verwaltungsdiensten und binden Sie problemlos Identitätsmanagementsysteme anderer Hersteller ein.
- Definieren Sie Messaging-Richtlinien und setzen Sie diese auf Domänen-, Gruppen- und Benutzerebene ein.

Vereinfachte Governance und Einhaltung gesetzlicher Vorschriften

Spezielle Compliance-Lexika sowie erweiterte Scanning- und Tracking-Funktionen erleichtern die Einhaltung neuer Branchenstandards und Gesetzesvorschriften.

- Erstellen Sie Inhaltsfilter zur Erkennung persönlicher Daten, die durch Gesetze wie den U.S. PCI Data Security Standard, die EU-Datenschutzrichtlinie oder das japanische Personendatenschutzgesetz geschützt sind.
- Ein Lexikon für Finanzdienste untersucht Nachrichten und Anhänge nach betrieblichen und persönlichen Finanzdaten, um die Einhaltung von SOX-, GLBA- und anderen Vorschriften zu vereinfachen.
- Ein HIPAA-Lexikon sucht nach geschützten Krankenakten, um die Einhaltung der HITECH/HIPAA- und anderer Vorschriften für das Gesundheitswesen zu erzwingen.
- Durch die Verfolgung der Nachrichten bis zur Auslieferung auf dem Desktop des Empfängers wird die Übertragung zu E-Mail-Compliance- und Prüfzwecken lückenlos dokumentiert.

Die branchenweit zugänglichste E-Mail-Datenverschlüsselungslösung

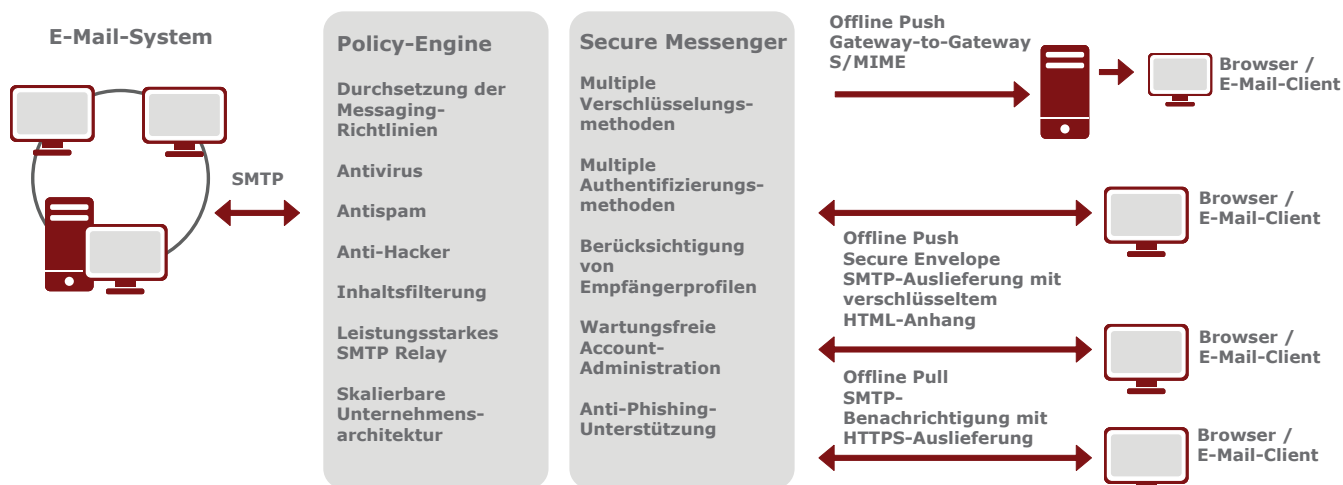
In der Regel kann ein Unternehmen Benutzern außerhalb des eigenen Netzwerks nicht vorschreiben, welche Desktop-Software sie für den Empfang oder Versand sicherer E-Mail-Nachrichten verwenden sollen. Aus diesem Grund stellt Secure Messenger eine Reihe von Methoden für die Auslieferung von Nachrichten über standardmäßige E-Mail-Clients und Webbrowser bereit, sodass keine spezielle Desktop-Software installiert oder verwaltet werden muss.

Online Pull-Auslieferung über einen Webbrowser (Secure Webmail)

Secure Webmail leitet den Empfänger über einen in eine E-Mail eingebetteten Link auf einen sicheren Server weiter, wo er die eigentliche Nachricht im Webbrowser lesen kann. Dies Verfahren ergänzt die vorhandenen SSL-Verschlüsselungsfunktionen des Browsers für die sichere Auslieferung der Nachricht, während durch Unterstützung browserbasierter Authentifizierungsmethoden gewährleistet wird, dass nur der richtige Empfänger die Nachricht anzeigen kann.

Die Empfänger können unabhängig von ihrem Standort per Internet auf ihre Nachrichten zugreifen und sie über denselben sicheren Auslieferungskanal beantworten. Alle Benutzer haben eine sichere webbasierte Mailbox (Secure Inbox), die ihnen ermöglicht, Nachrichten von überall über das Internet zu versenden, zu empfangen, zu sortieren, zu suchen, zu löschen, zu speichern und zu organisieren.





Offline Push-Auslieferung über einen Webbrowser (Secure Envelope)

Secure Envelope liefert eine verschlüsselte Nachricht als standardmäßige SMTP-E-Mail direkt an den E-Mail-Eingang des Empfängers aus, fügt den verschlüsselten Nachrichteninhalte jedoch in Form eines HTML-Anhangs bei. Der Empfänger öffnet den Anhang mit einem Online- oder Offline-Browser und gibt ein Passwort ein, um die Nachricht zu entschlüsseln und zu lesen.

Bereitstellungsoptionen

Hardened Linux-Appliance
 - Axway/Dell-Appliance
 - Virtuelle VMware-Appliance

Gateway-to-Gateway-Auslieferung mit S/Mime

Wenn auf Empfängerseite für die Verschlüsselung ein digitales Zertifikat zur Verfügung steht und die E-Mail-Infrastruktur den S/MIME-Standard unterstützt, ermöglicht Secure Messenger die Nachrichtenauslieferung mit Gateway-to-Gateway S/MIME-Verschlüsselung.

Allumfassende E-Mail-Sicherheit

- Stellen Sie Axway Secure Messenger in Verbindung mit Axway MailGate, einem unternehmenstauglichen Hygiene-Manager für ankommende/abgehende E-Mail-Nachrichten, auf einer gehärteten, IPv6-unterstützten Linux-Appliance bereit, um alle Ihre E-Mail-Sicherheitsprobleme mit einer umfassenden Lösung auf einer Appliance zu lösen.
- Nutzen Sie Secure Messenger und MailGate separat oder gemeinsam. Aktivieren Sie beide Lösungen gleichzeitig oder unabhängig voneinander je nach Bedarf und Wachstum Ihrer Organisation.
- Ein gemeinsamer Installationsassistent, eine gemeinsame Administrationsumgebung und eine gemeinsame Benutzeroberfläche erleichtern die Installation und Bedienung.

Hochverfügbarkeit / Disaster Recovery

- Nutzen Sie Funktionen für den Wiederanlauf nach Störfällen, um Daten- oder Serverkatastrophen ohne Beschädigung der E-Mail-Umgebung zu überstehen. Gesicherte Daten können wiederhergestellt werden.
- Nutzen Sie NAS-Speicher (Network-Attached Storage) für echte anwendungsbasierte Hochverfügbarkeit und die Aufrechterhaltung sämtlicher Betriebsfunktionen bei einem Systemausfall.

Weitere Informationen

Möchten Sie mehr darüber erfahren, wie Axway Secure Messenger Ihr Unternehmen durch Verbessern der E-Mail-Sicherheit, Governance und Compliance vor den Gefahren durch Datenlecks schützen kann? Dann schreiben Sie an contactgermany@axway.com oder besuchen Sie uns unter www.axway.de/kontaktformular.