

Echoworx E-Mail-Verschlüsselungsplattform

Echoworx E-Mail-Verschlüsselungsplattform

Es handelt sich um einen leistungsstarken, grenzbasierten Dienst zum Schutz von E-Mail-Daten, der darauf ausgelegt ist, Ihre sensiblen Informationen dauerhaft zu schützen. Dabei werden E-Mail- und Dokumentenzustellung in einem einheitlichen System gebündelt.

Echoworx E-Mail-Verschlüsselung: Eine Zustellmethode

Bietet Unternehmen die Möglichkeit, aus unserer Plattform zum Schutz von E-Mail-Daten eine einzelne sichere Zustellmethode auszuwählen.

Echoworx E-Mail-Verschlüsselung: Volumendokumente

Diese Option wurde für hohe Anforderungen und den Massenversand entwickelt und ermöglicht es Unternehmen, praktisch unbegrenzte Mengen verschlüsselter Dokumente und sicherer Mitteilungen zu versenden.

Wesentliche Differenzierungsmerkmale und Vorteile

- **Zahlreiche Zustellmethoden (Push/Pull)**
Wir unterstützen Webportal, TLS (mit Fallback), vollständige Nachrichtenverschlüsselung, ausschließlich verschlüsselte Anhänge (PDF, ZIP, Office XML), S/MIME und PGP. Das macht die Nutzung sowohl für Absender als auch für Empfänger einfach. Für mobile Geräte optimiert. Nutzer können ihre bevorzugte sichere Zustellmethode wählen, einschließlich Optionen ohne Registrierung.
- **S/MIME-Zertifikatsmanagement**
Vereinfachen Sie Ihren S/MIME-Prozess mandantenbezogen. Rufen Sie Empfängerzertifikate automatisch ab, generieren Sie neue Schlüssel und integrieren Sie vertrauenswürdige Zertifizierungsstellen wie DigiCert und SwissSign. Sie können selbstsignierte Anmeldeinformationen erzeugen oder Empfänger ihre eigenen X.509-Zertifikate hochladen lassen. Unser System unterstützt sowohl opaque-signed als auch clear-signed S/MIME-Nachrichten zur eingehenden Signaturprüfung.
- **PGP-Schlüsselmanagement**
Nutzen Sie eine vollständig verwaltete, cloudbasierte PGP-Lösung für automatisierte Schlüsselerzeugung, sichere Speicherung und nahtlose Schlüsselmigration. Wir unterstützen LDAP-basierten Schlüsselabruf sowie von Empfängern hochgeladene öffentliche Schlüssel.
- **Hardware-gestützte Kontrolle**
Wir bieten Manage Your Own Key (MYOK)-Funktionen zusammen mit vollständigen Hardware Security Modules (HSM), betrieben mit AWS KMS und validiert nach FIPS 140-3 Level 3.
- **Authentifizierungskontrollen und Zugriff**
Die Authentifizierung kann per Richtlinie, durch den Absender oder durch den Empfänger festgelegt werden. Zu den Optionen gehören: Selbstregistrierung, vom Absender festgelegte Passphrase, Social Connectors (OAuth), OpenID und Single Sign-On (SSO), systemgenerierte Verifizierungscodes sowie Zwei-Faktor-Authentifizierung (2FA). Darüber hinaus unterstützen wir biometrische Verfahren wie Passkeys und Fingerabdruckscanner und verbinden damit Benutzerfreundlichkeit auf Consumer-Niveau mit Sicherheit auf Enterprise-Niveau.
- **Umfassender Markenschutz**
Schützen Sie Ihre Markenintegrität mit Funktionen wie Vanity-Domains, Brand Indicators for Message Identification (BIMI) und anpassbaren Vorlagen. Wenden Sie Markenelemente auf Benachrichtigungen an, um Ihre Identität zu stärken und Ihre Reputation zu schützen. Wir unterstützen Multi-Branding über Profil- und Vorlagenrichtlinien und gewährleisten DMARC-konformes Routing für alle ausgehenden Nachrichten.
- **Inklusives Design**
Unser Markenschutz und unsere Interface-Compliance erfüllen die strengen Anforderungen der WCAG 2.2 auf Level AA.
- **Maßgeschneiderte Lokalisierung**
Wählen Sie aus 28 Sprachoptionen, einschließlich Double-Byte-Zeichen für Sprachen wie Chinesisch und Japanisch. Anpassbare Inline-Warnhinweise können nahtlos sowohl in Header als auch Footer eingebettet werden.
- **API-gesteuertes Reporting und Transparenz**
Echoworx vereinfacht IT-Teams den Zugriff auf Logdateien. Sie können Audit-Daten sicher mithilfe von API-Schlüsseln abrufen. Jede Admin-Aktion und jedes Nachrichtenverarbeitungsprotokoll speist sich direkt in Ihr SIEM ein und ermöglicht präzises, verlässliches Reporting sowie eine unkomplizierte Ereignisprotokollierung, etwa für geöffnete, weitergeleitete und zurückgerufene E-Mails.

ERZIELEN SIE GESCHÄFTLICHE VORTEILE DURCH INTELLIGENTERE AUSGABEN

Mit einer jährlichen Verlängerungsrate von über 98 % sind wir stolz darauf, die ideale Verbindung aus E-Mail-Datenschutz und Benutzerfreundlichkeit zu bieten.

KOSTEN- UND RESSOURCENEFFIZIENT

Wir konzentrieren uns zu 100 % auf den Schutz der Daten, die Sie per E-Mail versenden. Unsere kundenorientierte Roadmap liefert praxisnahe Weiterentwicklungen – sie optimiert Workflows, stärkt die Sicherheit und reduziert Reibungsverluste. So helfen wir Ihnen, heutige geschäftliche Anforderungen zu erfüllen und den Herausforderungen von morgen einen Schritt voraus zu sein.

BEHALTEN SIE DIE KONTROLLE ÜBER IHRE INFORMATIONEN

Echoworx betreibt Rechenzentren in den USA, im Vereinigten Königreich, in Deutschland, Irland und Kanada. Die Einhaltung moderner Vorgaben wie KRITIS-DachG, NIS 2 und DORA erfordert Verschlüsselungslösungen der nächsten Generation. Wir sorgen dafür, dass Ihre Daten eng kontrolliert und nah am Einsatzort bleiben – und gleichzeitig diese strengen, sich weiterentwickelnden regulatorischen Anforderungen erfüllen.

BAUEN SIE IHR DIGITALES GESCHÄFT AUS

Unsere Plattform für E-Mail-Datenverschlüsselung konsolidiert E-Mail- und Dokumentenzustellung in einer einzigen Plattform, die für hohe Anforderungen ausgelegt ist – nicht dafür, sie auszubremsten. So unterstützen wir Sie dabei, echte Kosteneffizienz zu erreichen.

STEIGERN SIE DIE OPERATIVE EFFIZIENZ

Echoworx integriert sich nahtlos in Ihren bestehenden Security-Stack, einschließlich Gmail, Outlook, Proofpoint und Mimecast, und harmonisiert zugleich mit komplexen DLP-Regeln. Ob On-Premises, in der Cloud oder in hybriden Umgebungen – unsere Plattform stellt sicher, dass Verschlüsselung unsichtbar in Ihren Workflows funktioniert.

VALIDIERTE SICHERHEITSGEWÄHRLEISTUNG

Wir unterziehen unsere Sicherheitspraktiken strengen Audits, die sämtliche Bereiche unseres Unternehmens abdecken. Zu unseren Zertifizierungen gehören das SOC2-Audit, die PCI DSS Level 1-Zertifizierung, FSQS (Financial Services Qualification System), die AWS-Qualifizierung sowie die OpenID Connect RP-Zertifizierung.

