

APX E-Mail-Verschlüsselungsmodul

GEWÄHRLEISTEN SIE EINE SICHERE ZUSTELLUNG VERTRAULICHER E-MAILS

In einer immer enger vernetzten Welt dominieren E-Mails nach wie vor die geschäftliche Kommunikation. Daher bilden sie für Cyberkriminelle ein optimales Ziel. Jedes Unternehmen muss sein geistiges Eigentum, seine geschäftlichen Transaktionen und die Privatsphäre seiner Kunden und Mitarbeiter schützen.

WARUM SOLLTEN SIE SICH FÜR DAS FORCEPOINT™ E-MAIL-VERSCHLÜSSELUNGSMODUL ENTSCHEIDEN?

Bei der Forcepoint-Verschlüsselung handelt es sich um einen richtlinienbasierten Dienst, der eine sichere Zustellung von E-Mail-Nachrichten an Geschäftspartner und sonstige Personen ermöglicht. Die einfache Verwaltung, die ohne komplexes Management oder zusätzliche Hardware auskommt, eliminiert die herkömmlichen Kosten- und Komplexitätsbarrieren für eine E-Mail-Verschlüsselung. Eine vollständige Integration mit TRITON® AP-EMAIL und dem E-Mail-Data-Loss-Prevention (DLP)-Modul bedeutet, dass Sie auch weiterhin in der Lage sind, verschlüsselte E-Mails auf Malware und inhaltliche Verstöße zu untersuchen. Die Forcepoint-Verschlüsselung bietet eine einfache und kostengünstige Lösung, die es Unternehmen ermöglicht, Auflagen schnell zu erfüllen und die Geheimhaltung ihrer vertraulichen Daten zu gewährleisten.

- **Vordefinierte Richtlinien** machen es Ihren aktuellen IT-Mitarbeitern leicht, behördliche Anforderungen wie PCI schnell zu erfüllen und Ihr geistiges Eigentum abzusichern.
- **Das Nutzererlebnis ist nahtlos**, da die Verschlüsselung vertraulicher Informationen dank einfacher aber leistungsstarker Richtlinienkontrollen automatisch verläuft.
- **Die Anwendung der Forcepoint-E-Mail-Verschlüsselung** ist dank einer benutzerfreundlichen Selbstregistrierung und Passwortverwaltung auch für externe Empfänger einfach, so dass der administrative Aufwand für die Verwaltung eines Zugriffs durch den Empfänger entfällt.

- **E-Mails gelangen sicher** und verschlüsselt in den Posteingang des Empfängers.
- **Anhand von optischen Zeichenerkennungs (OCR)-Funktionen** können Richtlinien Daten, die in Screenshots, Faxseiten und eingescannten Dokumenten (z.B. Schecks, Belege, rechtliche Unterlagen oder veraltete Akten) identifiziert wurden, verschlüsseln.
- **Die Integration** aller erforderlichen Dienste und ein starker Automatisierungsgrad reduzieren den Verwaltungsaufwand, so dass die Gesamtbetriebskosten niedrig bleiben.

TEIL EINER VOLLSTÄNDIGEN E-MAIL-ABSICHERUNG

Die Kombination aus TRITON AP-EMAIL, dem E-Mail-DLP-Modul und dem E-Mail-Verschlüsselungsmodul bietet entlang der gesamten „Kill Chain“ Schutz bei eingehenden Bedrohungen und abgehender vertraulicher Kommunikation.

- E-Mails werden auf der Grundlage von Richtlinien verschlüsselt. Dies schützt die vertrauliche Kommunikation mit Ihren Geschäftspartnern und Kunden sowohl mit herkömmlichen E-Mail-Systemen als auch mit Microsoft Office 365.
- **Advanced Persistent Threats (APTs)** und andere fortgeschrittene zielgerichtete Bedrohungen werden anhand von Echtzeitanalysen der ACE unterbunden.
- Mitarbeiter mit riskantem Verhalten werden durch eine Analyse ihrer Aktivität im Vergleich zu ähnlichen Benutzern und früheren Verhaltensweisen identifiziert, um eine Korrektur und Aufklärung zu ermöglichen.
- Durch die Hinzunahme des E-Mail-Sandbox-Moduls für ein verhaltensorientiertes Sandboxing von URLs und Dateien lässt sich die Erkennung von Zero-Day-Bedrohungen verbessern.
- Durch die Hinzunahme des Bildanalysemoduls lassen sich anzügliche Bilder, die einen Verstoß gegen Bestimmungen zur Verhinderung von sexueller Belästigung oder sonstige Vorschriften darstellen, in E-Mails identifizieren.



TRITON AP-EMAIL

Von Ködern, die auf soziale Manipulation setzen, bis hin zu zielgerichteten Phishing-Attacken – die meisten großen Cyberangriffe beginnen mit einer E-Mail. Da diese fortgeschrittenen, mehrstufigen Bedrohungen Web- und E-Mail-Elemente kombinieren, bietet sich eine Reihe – eine „Kill Chain“ – von Gelegenheiten, um sie zu stoppen, noch bevor es zu einer Datenschutzverletzung kommt.

TRITON AP-EMAIL identifiziert zielgerichtete Angriffe, Benutzer mit riskantem Verhalten und Innentäter-Bedrohungen, ermöglicht gleichzeitig jedoch auch Mitarbeitermobilität und die sichere Nutzung neuer Technologien wie Microsoft Office 365 und Box. Egal ob Angriffsaktivitäten von außen, Datendiebstahl von innen oder Botnet-Kommunikationsversuche - Forcepoint TRITON E-Mail-Sicherheit schützt E-Mail-Kommunikation im Rahmen der umfassenden TRITON APX-Abwehr gegen APTs und andere fortgeschrittene Bedrohungen.

► TRITON AP-EMAIL LÖST E-MAIL-SICHERHEITSPROBLEME

- APTs verwenden E-Mails häufig in den frühen Phasen ihrer fortgeschrittenen Angriffe
- Verhinderung von Datendiebstahl und Gefahren durch Innentäter
- Sichere Einführung von Microsoft Office 365 und anderen Diensten, um wachsen und konkurrenzfähig bleiben zu können
- Riskantes Nutzerverhalten kann leicht zu Sicherheitsverletzungen und Datenverlust führen



DER FORCEPOINT-UNTERSCHIED:

ACE (Advanced Classification Engine)

Forcepoint ACE bietet integrierte, kontextbezogene Echtzeit-Verteidigungsmaßnahmen für Web-, E-Mail-, Daten- und mobile Sicherheit. Das System nutzt eine kombinierte Risikobeurteilung sowie vorausschauende Analysen, um eine maximal effektive Sicherheit zu gewährleisten. Zudem ermöglicht es eine Eindämmung potenzieller Schäden durch eine Analyse ein- und abgehenden Datenverkehrs über datensensitive Maßnahmen, die branchenführenden Schutz vor Datendiebstahl bieten. Klassifizierungen für Echtzeitsicherheit sowie Daten- und Inhaltsanalysen, die aus vielen Jahren der Forschung und Entwicklung hervorgegangen sind, versetzen ACE in die Lage, jeden Tag mehr Bedrohungen zu erkennen als herkömmliche Antivirus-Programme (der Nachweis hierzu wird täglich unter <http://securitylabs.forcepoint.com> aktualisiert). ACE ist die primäre Schutzstruktur, auf der alle Forcepoint TRITON®-Lösungen aufbauen. Sie wird durch die Forcepoint ThreatSeeker® Intelligence Cloud unterstützt.

KONTAKT

www.forcepoint.com/contact

ERFAHREN SIE MEHR

Forcepoint™ ist eine Marke von Forcepoint, LLC. SureView®, ThreatSeeker® und TRITON® sind eingetragene Marken von Forcepoint, LLC. Raytheon ist eine eingetragene Marke von Raytheon Company. Alle anderen Marken und eingetragenen Marken sind das Eigentum ihrer jeweiligen Inhaber.

[DATASHEET_MODULE_EMAIL_ENCRYPTION_DE]-100008DE.011416

FORCEPOINT
TRITON® APX