Forcepoint Data Loss Prevention for Cloud Email

Schutz und Kontrolle Ihrer E-Mail mit der zuverlässigsten DLP-Lösung der Branche

Herausforderung

- Vertrauliche Daten verlassen Unternehmen immer häufiger über unterschiedliche Kanäle.
- E-Mail wird als beliebtester Angriffsvektor genannt.
- Der Schutz von Daten ohne Einschränkung der Produktivität war noch nie so wichtig und komplex.

Lösung

- Forcepoint weitet die zuverlässigste Data Loss Prevention (DLP)-Lösung der Branche auf den E-Mail-Kanal aus.
- Genaue Überwachung und Vermeidung von Datenverlust über E-Mail
- Mit einer vollständig verwalteten Cloud-Lösung kann der Schutz ausgehender E-Mails an Ihre Unternehmensanforderungen angepasst werden.

Ergebnis

- Mehr Effizienz durch drastische Reduzierung der Zahl der Fehlalarme über E-Mail
- Verbesserte Compliance durch 3-mal mehr vordefinierte Richtlinien als bei anderen DLP-Anbietern
- Migration Ihrer DLP in Forcepoint in nur 6 Wochen dank Know-how, sofort einsatzbereiter Richtlinien und erstklassigem Wissenstransfer von Forcepoint

Datensicherheit ist für Unternehmen von wachsender Bedeutung. Unabhängig davon, ob Mitarbeiter in der traditionellen Büroumgebung oder im Rahmen eines neuen Arbeitsmodells an einem Fern- oder Hybrid-Arbeitsplatz arbeiten – der Schutz von Daten über mehrere Kanäle hinweg ist wesentlich komplexer geworden. E-Mail ist für Unternehmen ein wichtiger Kanal, wenn es darum geht, Transparenz und Kontrolle zu gewinnen, um die unerwünschte Datenexfiltration von wertvollen Dateien, intellektuellem Eigentum und Daten zu unterbinden. Bekannte Beispiele für Datenverlust über E-Mail sind:

→ **Das Senden von Unternehmensdateien und -daten** vom geschäftlichen an das private E-Mail-Konto

→ **Vertrauliche Daten,** die das Unternehmen durch Fahrlässigkeit oder kompromittierte Konten von Benutzern verlassen

→ **Ein Insider, der vertrauliche Daten und Dateien** in böswilliger Absicht an die Konkurrenz, Nachrichtenquellen und Websites weitergibt. Dies geschieht häufig in betrügerischer Absicht oder hat das Ziel, das Unternehmen zu sabotieren oder geschützte Daten zu entwenden.

→ **Durch Phishing- und Malware-Angriffe oder Adware und Spam** werden gutgläubige Mitarbeiter zu Komplizen dieser Angreifer und helfen unwissentlich dabei, wichtige Daten und intellektuelles Eigentum herauszuschleusen.

"E-Mail ist der beliebteste Angriffsweg von Angreifern, um Malware in ein Unternehmen einzuschleusen. E-Mail ist auch ein direkter Kontaktweg zwischen Benutzern und Cyber-Kriminellen und kostet Unternehmen jährlich Milliarden von Dollar aufgrund von Betrug und gehackten geschäftlichen E-Mails."

IDC, WORLDWIDE MESSAGING SECURITY MARKET SHARES, 2021: HYBRID WORK DRIVES NEED FOR THREAT INVESTIGATION INTEGRATION, DOC # US49144522, JUNE 2022

Für Unternehmen ist eine umfassende Transparenz und Kontrolle ihrer ausgehenden E-Mails unerlässlich, um intellektuelles Eigentum vor gezielten Angriffen und versehentlicher Preisgabe zu schützen. DLP-Technologie ist hier das Mittel der Wahl. Laut IDC „haben Technologien zum Schutz vor Datenverlust in den vergangenen 24 Monaten eine Renaissance erlebt. Manuelle und obskure Klassifizierungsmethoden werden durch maschinelles Lernen und Automatisierung ersetzt. Kontext fungiert dabei als Wegbereiter. Die Effektivität und Effizienz der Lösungen hat sich verbessert." [1] E-Mail-Sicherheit ist in Kombination mit den neuen DLP-Verbesserungen zur Erkennung, zum Schutz und zur Kontrolle vertraulicher Informationen unerlässlich, um den wichtigen Angriffsvektor E-Mail unter Kontrolle zu bekommen. Ohne den Einsatz starker DLP-Funktionen können E-Mail-Sicherheitsverletzungen den Geschäftsaktivitäten und dem Ruf Ihres Unternehmens erheblichen Schaden zufügen.

Vorteil von Forcepoint DLP for Cloud Email

Als führender Anbieter von Datensicherheitslösungen liefert Forcepoint DLP for Cloud Email eine einzigartige Transparenz und Kontrolle für ausgehende E-Mails. In Kombination mit DLP für Endpunkte, Cloud, Internet und Netzwerk bietet DLP for Cloud Email eine leistungsstarke, breit gefächerte Lösung für den Schutz von Unternehmensdaten. Forcepoint DLP verhindert Datenverlust überall dort, wo Ihre Mitarbeiter arbeiten und Ihre Daten gespeichert sind.

Extreme Datenidentifizierung

Forcepoint DLP umfasst über 1.600 Klassifizierungen und vordefinierte Vorlagen zur schnellen Bereitstellung und Erkennung sensibler Daten. Darüber hinaus werden mithilfe moderner Technologien, der Analyse natürlicher Sprache, maschinellem Lernen und einer der stärksten Fingerprinting-Technologien der Branche Daten im Speicher, bei der Übertragung und bei der Verwendung präzise identifiziert. Bei der Datensicherheit spielt Transparenz eine wichtige Rolle. Forcepoint DLP Discover bietet umfassende Transparenz und die anschließende Identifizierung von Daten, sodass alle Typen von Daten angemessen überprüft werden können. Dies ist aus mehreren Gründen wichtig:

- → **Compliance:** Forcepoint DLP deckt wichtige Vorschriften wie DSGVO, HIPAA und viele mehr in über 83 Ländern ab, um sicherzustellen, dass Unternehmen jederzeit die Compliance-Standards erfüllen.
- → **Einfachheit:** Die Erstellung und Implementierung von Klassifizierungen, die die Bedürfnisse und betrieblichen Anforderungen eines Unternehmens erfüllen, nimmt bei einer DLP-Bereitstellung sehr viel Zeit und Ressourcen in Anspruch. Dank der vordefinierten Vorlagen und Klassifizierungen von Forcepoint können Unternehmen Klassifizierungen, die auf eine Reihe von Branchen und Datentypen zugeschnitten sind, schnell bereitstellen und DLP so erheblich vereinfachen.
- → **Effizienz:** Dank Forcepoints umfassender Technologie zur Datenidentifizierung senkt Forcepoint DLP die Zahl der Fehlalarme drastisch. Gleichzeitig werden sicherheitskritische Ereignisse zur näheren Untersuchung priorisiert und eingestuft.

Einheitliche Richtlinienkontrolle

Eine überzeugende DLP-Strategie muss alle wichtigen Kanäle berücksichtigen, wie Endpunkt, Cloud, Internet und E-Mail. Unternehmen setzen für jeden dieser Kanäle häufig Einzellösungen mit unterschiedlichen DLP-Produkten ein, die nur einen Kanal ins Visier nehmen, wie Cloud oder E-Mail. Mit Forcepoint können Sie sämtliche Kanäle mit einer einzigen Lösung schützen und über eine zentrale Richtlinie verwalten. Wenn Sie Richtlinien nur einmal erstellen und mehrmals anwenden, erzielen Sie eine beispiellose Kontrolle über die Daten in Ihrem Unternehmen und können alle wichtigen Kanäle, in denen Datenverluste auftreten, zentral verwalten. Wenn Sie mit DLP for Cloud Email Richtlinien anwenden, können Sie die Transparenz auch auf weitere Geräte erweitern, wie Tablets und Telefone, die bei herkömmlichen Endpunktlösungen in der Regel nicht berücksichtigt werden.

Einzigartige Skalierbarkeit

Der Vorteil von Forcepoint DLP for Cloud Email ist, das dies ein vollständig verwalteter Cloud-Service ist und somit die für Cloud-Bereitstellungen typischen flexiblen Ressourcen bietet. Wenn der ausgehende E-Mail-Verkehr beispielsweise plötzlich stark ansteigt, können die Ressourcen dank DLP for Cloud Email rasch hochgefahren und anschließend wieder verringert werden, um Bedarfsspitzen gerecht zu werden. Zudem kann so ein durchgängiger DLP-Service angeboten werden, um die wachsenden Anforderungen Ihres Unternehmens zu erfüllen, ohne dafür zusätzliche Hardware bereitstellen und konfigurieren zu müssen.

Risikoadaptierter Schutz

Forcepoint ist der erste Anbieter in der Branche, der eine risikoadaptierte DLP-Lösung bereitstellt. Da die Lösung die Benutzeraktivität ständig überwacht, haben Ihre Mitarbeiter bei der Arbeit mehr Freiheit. Es wird nur dann eingegriffen, wenn risikobehaftete Aktivitäten oder Verhaltensmuster festgestellt werden. Die Automatisierung ermöglicht die Durchsetzung nahezu in Echtzeit, d. h. Verstöße können antizipiert und verhindert werden, bevor sie auftreten.

1 IDC, Worldwide Digital Loss Technologies Market Shares, 2020: DLP Is Dead, Long Live DLP, Doc # US48261521, Oktober 2021

Forcepoint DLP-Lösungen für Cloud-E-Mail

DLP for Cloud Email – Schutz von ausgehenden Daten

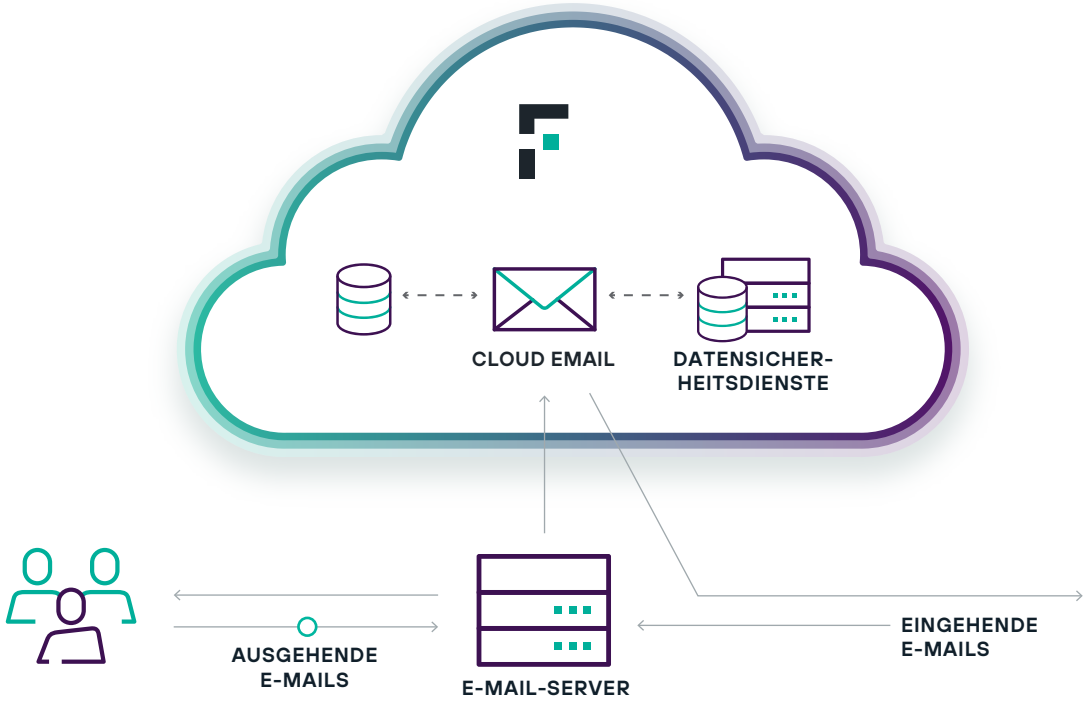
Forcepoint kann in Ihre bestehende E-Mail-Sicherheitslösung integriert werden, um ausgehende E-Mails zu prüfen, und vereinfacht somit die Bereitstellung von DLP for Cloud Email. Durch den Einsatz von DLP for Cloud Email Universal Connectors kann Forcepoint in beliebte Drittanbieterprodukte wie Google und Microsoft integriert werden, sodass alle oder ausgewählte ausgehende E-Mails an die Forcepoint-Cloud weitergeleitet werden. Dort prüft Forcepoint DLP die E-Mails anhand der DLP-Richtlinien und -Aktionen, die in Ihrem vordefinierten DLP-Plan festgelegt sind. E-Mails können genehmigt, in Quarantäne verschoben oder vor dem Senden (mit einem separaten Verschlüsselungsmodul) verschlüsselt werden. Bei E-Mails, die in Quarantäne verschoben wurden, werden Benachrichtigungen gesendet. Die Quarantäne kann je nach Konfiguration bis zu 30 Tage dauern, sofern sie nicht von einem autorisierten Administrator aufgehoben wird. Um den guten Ruf eines Unternehmens zu schützen, werden alle ausgehenden E-Mails zusätzlich auf Spam, Viren und Malware überprüft.

Standard features:

- → **Simple policy interface** providing protection across virus, malware, and spam
- → **Dashboards, logs, and presentation reports**
- → **Personal email subscription**

Add-ons:

- → **Forcepoint Cloud Email Extended Reporting History** (options for 6, 12, and 18 months)
- → **Forcepoint Email Security Encryption Module**
- → **Forcepoint Email Security Image Analysis Module**



forcepoint.com/contact

© 2023 Forcepoint. Forcepoint und das FORCEPOINT-Logo sind Marken von Forcepoint.
Alle anderen hier genannten Marken sind Eigentum ihrer jeweiligen Inhaber.
[FP-DLP For Cloud Email-Solution-Brief-DE] 24Jul2023