Seclore für Forcepoint DLP

Herausforderung

- DLP kann entweder verhindern, dass sensible Daten das Unternehmen verlassen, oder es kann sie nach Verlassen des Unternehmens überwachen. Das Problem: Wenn Daten am Verlassen des Unternehmens gehindert werden, bricht die Produktivität ein, während die reine Überwachung der Daten diese sich selbst überlässt und erlaubt, dass sie ungeschützt übertragen werden.

Lösung

- Automatisches Hinzufügen von durchgängigen, granularen Nutzungskontrollen zu erkannten Daten
- Dynamisches Zuweisen und Entziehen von Dateiberechtigungen
- Zuordnen von Sicherheitsberechtigungen zu DLP-Geschäftsregeln
- Sichern von Daten an Endpunkten, im Netzwerk oder in E-Mails
- Sammeln forensischer Daten zur Datennutzung

Ergebnis

- DLP-Implementierungen werden beschleunigt, was die Kosten senkt und die Amortisierungsdauer verkürzt.
- Fehlalarme werden minimiert, was wiederum den Verwaltungsaufwand verringert.
- Eine unterbrechungsfreie interne und externe Zusammenarbeit wird ermöglicht.
- Kontrolle und Nachverfolgung sensibler Daten, die das Unternehmen verlassen, werden verbessert.
- Die Einhaltung von Audits und gesetzlichen Vorgaben wird gewährleistet.

Data Loss Prevention (DLP) erkennt sensible Daten und verhindert, dass sie aus Ihrem Netzwerk sickern. Doch was passiert nach der Datenerkennung? Was machen Sie mit all den Vorfällen? Wie gewährleisten Sie die Zusammenarbeit mit externen, unternehmensfremden Geschäftspartnern, wenn E-Mails am Endpunkt blockiert oder ungeschützt versendet werden? Wie schützen Sie Dateien, die über die Cloud ausgetauscht oder von externen Auftragnehmern auf Mobilgeräten angezeigt werden? Wie bekommen Sie Ihre sensiblen Daten zurück, wenn sie in die falschen Hände geraten?

Seclore Rights Management und Forcepoint DLP

DLP kann Inhalte in Dokumenten untersuchen und sensible Daten erkennen. Diese Erkennung sensibler Daten ermöglicht Ihnen, automatisch die entsprechenden Nutzungskontrollen (Rechte) für Dokumente und Interaktionen mit den Daten hinzuzufügen. Durch die Integration von Seclore Rights Management erhalten Sie die vollständige Kontrolle über Ihre Informationen – bis hin zum kompletten Entzug der Zugriffsrechte. Und das auch über Ihre Unternehmensgrenzen hinaus. Sobald Forcepoint DLP sensible Daten erkennt, kann Seclore diese sofort mit den entsprechenden Nutzungsrichtlinien schützen. Die durchgängigen, granularen Datennutzungskontrollen von Seclore begleiten die Datei überall hin, ob innerhalb oder außerhalb des Unternehmens. Sie schützen die Daten während der Nutzung (der Bearbeitung von Dateien), während der Übertragung (beim Senden per E-Mail) und im Ruhezustand (unabhängig von Dateiformat, Gerät oder Betriebssystem).

Die doppelte Power

Wenn Sie bereits Forcepoint DLP nutzen, verhilft Ihnen Seclore Rights Management von einer „reaktiven" zu einer „proaktiven" Sicherheitsstrategie. Normalerweise ist DLP im „Überwachungsmodus" konfiguriert, in dem Dashboards, Berichte und Warnungen bereitgestellt werden, um die Informationen, die das Unternehmen verlassen, nachzuverfolgen. Der Überwachungsmodus ist eine Standardfunktion von DLP. Allerdings sind damit gewisse Sicherheitsbedenken verbunden, da sensible Daten das Unternehmen verlassen. Sollten Ihre sensiblen Daten in die Hände einer böswilligen Person fallen oder Sie diese von einem Dritten zurückfordern müssen, müssen Sie diese Daten nachverfolgen. Mit Seclore sitzen Sie am Steuer.

Seclore Rights Management beschleunigt zudem die Implementierung von Forcepoint DLP erheblich. Wenn Sie sich nicht sicher sind, welche Geschäftsregel Sie auf erkannte Informationen anwenden sollen (Blockieren, Quarantäne, Zulassen usw.), können Sie als Standardreaktion die Informationen automatisch mit Seclore schützen. Außerdem entfällt die laufende Konfiguration.

DLP erkennt

- → Durchsucht Inhalte
  - Schlüsselwörter
  - Muster
  - Digital Fingerprints
  - Optische Zeichenerkennung (OCR)
- → Verhindert, dass vertrauliche Informationen die Unternehmensgrenzen verlassen
- → Protokolliert Vorfälle innerhalb des Unternehmens

Rights Management schützt

- → Schützt Inhalte
  - Granulare Nutzungskontrollen
  - Festlegen, wer, wann, wo, wie und worauf zugreifen darf
  - Zugriff einschränken und widerrufen
  - Derzeit verwendete, derzeit übertragene und ruhende Daten
- → Ermöglicht autorisierten externen Benutzern den Zugriff auf sensible Informationen
- → Verfolgt und prüft Daten innerhalb und außerhalb des Unternehmens

Durch die Kombination von Seclore RM und Forcepoint DLP können Sie kontrollieren, wer auf ein Dokument zugreifen kann und was diese Personen wann und auf welchem Computer oder Gerät damit machen dürfen. Indem durchgängige, datenorientierte Nutzungskontrollen eingebunden werden, kann der Anwendungsbereich von Forcepoint DLP auf Dokumente ausgeweitet werden, die in öffentlichen und Partnernetzwerken übertragen, in der Cloud oder in File-Sharing-Diensten gespeichert oder auf Mobilgeräten aufgerufen werden.

Sofortiger Schutz: Am Endpunkt, im Netzwerk oder in der Cloud

Sensible Daten, die bei Suchläufen von Forcepoint DLP erkannt wurden, ob an Endpunkten, im Netzwerk oder in der Cloud, können durch Seclore Rights Management sofort geschützt werden. Zum Beispiel können Seclore-Schutzrichtlinien auf die Erkennung sensibler Schlüsselwörter oder regulärer Ausdrücke (z. B. Kreditkartennummern) angewendet werden.

Die Nutzungskontrollen stellen sicher, dass kein Benutzer außerhalb der zuständigen Abteilung (geschweige denn außerhalb des Unternehmens) das betreffende Dokument verwenden kann – selbst wenn es an ihn übermittelt wurde. Durch Forcepoint DLP wird dieser Schutz noch erweitert, indem präzises ID-Fingerprinting genutzt wird, um sensible Daten an jedem beliebigen Ort zu erkennen, z. B. auf Dateiservern, oder wenn diese sensiblen Daten von Benutzern weitergegeben werden. Dadurch können Administratoren ihre Aufmerksamkeit auf die Benutzer und das Verhalten mit dem größten Risiko konzentrieren.

Außerdem erfolgt dieser Schutz praktisch sofort und vollkommen automatisch. Die automatische Anwendung von Nutzungskontrollen auf der Grundlage der DLP-Erkennungsrichtlinien führt dazu, dass keine zusätzlichen Schritte für die Mitarbeiter erforderlich sind, weniger Schulungskosten anfallen und der Aufwand für das Änderungsmanagement sinkt.

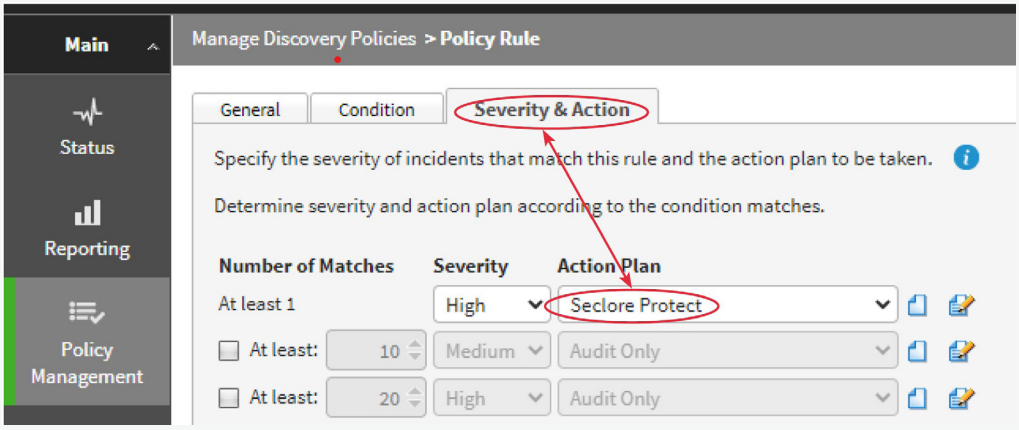

Abbildung 1: Erkennungsergebnisse werden automatisch der Schutzrichtlinie zugeordnet.

Seclore Rights Management und Forcepoint DLP Endpoint

Forcepoint DLP durchsucht Dokumente auf Endpunkten im Netzwerk und erkennt vertrauliche Daten. Forcepoint DLP kann Schlüsselwörter (z. B. Umsatzprognosen), Muster und reguläre Ausdrücke (z. B. Kreditkartennummern) abgleichen und auch in bestimmten Ordnern oder nach Dokumenten in bestimmten Formaten suchen. Nach der Erkennung schützt Seclore diese sensiblen Informationen und wendet die entsprechende Seclore-Richtlinie an, um deren Verlust oder Missbrauch zu verhindern. Dies geschieht auf der Grundlage der vom Administrator des Unternehmens definierten Richtlinien. Mit Forcepoint DLP können Sie netzwerkinterne Richtlinien auf netzwerkexterne Geräte ausdehnen und Richtlinien auf Ebene der einzelnen Endpunkte anwenden, sodass die Daten auch dann geschützt sind, wenn die Benutzer dezentral arbeiten.

Vorteile

- → Automatischer Schutz für sensible Informationen innerhalb und außerhalb des Netzwerks
- → Geringere Abhängigkeit von den Benutzern beim Schutz sensibler Daten
- → Schutz, der mit der Datei verbunden bleibt – während Speicherung, Übertragung und Nutzung

1 Ein Benutzer speichert oder kopiert ein Dokument mit sensiblen Daten auf seinen lokalen Computer.

2 Forcepoint DLP erkennt sensible Daten in einem Dokument auf dem Endpunkt – entweder während einer geplanten oder einer Echtzeitsuche. Im Falle einer Richtlinienverletzung wird die entsprechende Seclore-Nutzungsrichtlinie angewendet.

3 Der Seclore-Schutz bleibt in Kraft, wann immer das Dokument irgendwo auf der Welt geöffnet wird. Alle am Dokument durchgeführten Aktivitäten werden zentral und in Echtzeit protokolliert.

Abbildung 2: Erkennung am Endpunkt

Seclore Rights Management und Forcepoint DLP Network

Forcepoint DLP durchsucht sensible Dokumente auf Dateiservern. Daten, die innerhalb und außerhalb des Unternehmens übertragen werden, müssen zuverlässig geschützt werden. Mit DLP Network schützen Sie Daten während der Nutzung, indem Sie den Datenfluss über verschiedene Kommunikationskanäle wie E-Mail und Web überwachen. Seclore erweitert diesen Schutz, indem es verhindert, dass sensible Informationen nach außen dringen oder missbraucht werden.

1 Ein Benutzer erstellt oder kopiert ein Dokument mit sensiblen Daten …

2 … und speichert es in einem freigegebenen Netzwerkordner.

3 Forcepoint DLP erkennt sensible Daten in dem Dokument – entweder während einer geplanten oder einer Echtzeitsuche. Im Falle einer Richtlinienverletzung wird die entsprechende Seclore-Nutzungsrichtlinie angewendet.

4 Der Seclore-Schutz bleibt in Kraft, wann immer das Dokument irgendwo auf der Welt geöffnet wird. Alle am Dokument durchgeführten Aktivitäten werden zentral und in Echtzeit protokolliert.

Abbildung 3: Erkennung im Netzwerk

Seclore Data Classification und Forcepoint DLP

Seclore Data Classification – entwickelt von Boldon James – arbeitet mit Forcepoint DLP zusammen, um Fehlalarme bei der Datenerkennung zu vermeiden.

- → **Ein Benutzer klassifiziert** zum Beispiel ein Office-Dokument, indem er einfach auf ein Klassifizierungssymbol in der Office-Leiste klickt.
- → **Forcepoint DLP markiert** das Dokument basierend auf der gewählten Klassifizierung.
- → **Seclore Rights Management schützt** das Dokument durch die entsprechende Nutzungsrichtlinie. Der Seclore-Schutz bleibt in Kraft, wann immer das Dokument irgendwo auf der Welt geöffnet wird.
- → **Forcepoint Fingerprinting** ermöglicht festzustellen, wenn Teile des Dokuments kopiert, eingefügt oder bearbeitet werden, wodurch ein Herausschleusen von Daten erkannt und verhindert werden kann.
- → Alle am Dokument durchgeführten Aktivitäten werden zentral und in Echtzeit protokolliert. Da die Klassifizierung des Dokuments vom Benutzer bestimmt wird, sind **Fehlalarme praktisch ausgeschlossen.**

Seclore Automatic Email Protection mit Forcepoint Email Security

DLP Email Security wird aufgrund der Gefahr von Fehlalarmen meist im Erkennungsmodus ausgeführt. Eine Erkennung von anomalem Benutzerverhalten erfolgt erst im Nachhinein. Wenn Daten aus geschäftlichen Gründen das Netzwerk verlassen müssen, bleibt keine andere Wahl, als E-Mails vollkommen ungeschützt zu versenden.

Seclore bietet eine einfache und effiziente Lösung für diese Problematik. Nachdem die E-Mail vom DLP Email Gateway verarbeitet wurde, werden die E-Mail und ihre Anhänge durch die automatische Schutzfunktion von Seclore Rights Management mit der entsprechenden Nutzungsrichtlinie verschlüsselt. Dies stellt sicher, dass die Empfänger die E-Mail nicht missbrauchen oder unbefugt weiterleiten können, nachdem sie sie erhalten und gelesen haben. So wird aus einer „Erlauben"-Richtlinie in DLP eine „für die nächsten 10 Tage"-Richtlinie in Seclore.

Dank des automatischen E-Mail-Schutzes von Seclore Rights Management verhindert Email Security nicht die wichtige Zusammenarbeit per E-Mail. Der Datenaustausch ist weiterhin möglich, wobei Sicherheit und Compliance gewahrt bleiben. Und all dies ist sowohl für den Absender als auch für den Empfänger der E-Mail vollkommen transparent.

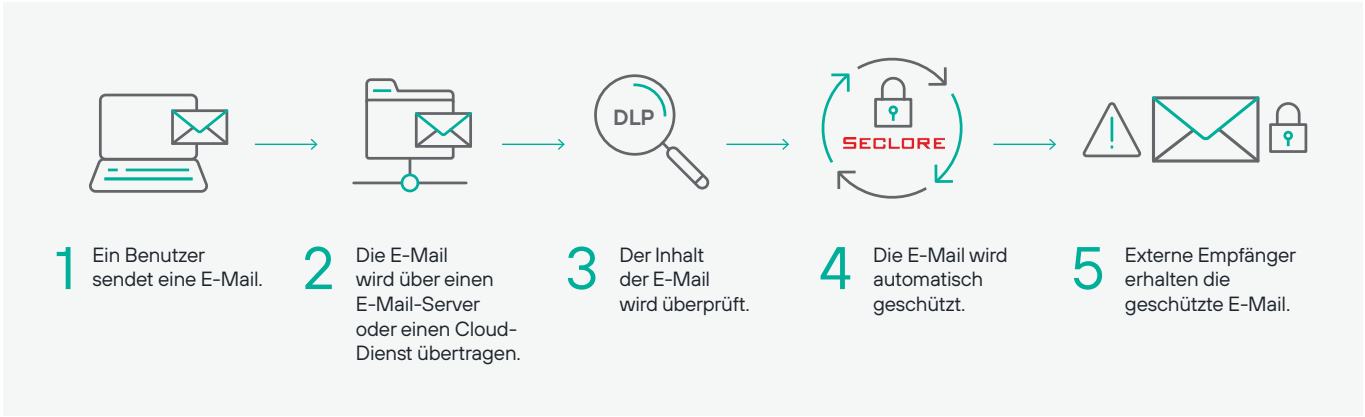

Abbildung 4: Seclore und Forcepoint DLP

Sichere E-Mail-Entschlüsselung zur Erkennung von Inhalten in Forcepoint DLP

Eine Herausforderung für DLP-Systeme besteht darin, sensible Inhalte in verschlüsselten E-Mails und Anhängen zu erkennen, um entscheiden zu können, ob eine E-Mail freigegeben oder blockiert werden sollte. Seclore Decrypter for Email löst dieses Problem, indem es den sicheren Zugriff auf mit Seclore verschlüsselte E-Mails und Anhänge ermöglicht. Nachdem die geschützte E-Mail entschlüsselt wurde, kann Forcepoint DLP nach sensiblen Inhalten und Mustern suchen und entsprechende Entscheidungen treffen (erlauben/blockieren/schützen).

Seclore Decrypter for Email arbeitet mit dem Email Auto-Protector von Seclore zusammen, um den Schutz von E-Mails zu automatisieren, bevor diese an Empfänger außerhalb des Unternehmens gesendet werden.

Unternehmen, die Seclore Rights Management und Forcepoint DLP einsetzen, können nun mit Fug und Recht behaupten, die Vorschriften einzuhalten, da Forcepoint DLP alle Dateien – sowohl ungeschützte als auch geschützte – erkennen, verfolgen und prüfen kann.

Die wichtigsten geschäftlichen Vorteile

Automatischer Datenschutz
Die Integration von DLP und Digital Rights Management (DRM) automatisiert den gesamten Prozess von Klassifizierung, Schutz, Nutzungskontrolle und Prüfung. Der Übergang zwischen Erkennung und Schutz ist fließend. Dabei erfolgt der DRM-Schutz für den Endbenutzer vollkommen transparent.

Schnellere DLP-Implementierung
DRM kann als „Standard-Geschäftsregel" von DLP eingerichtet werden, um sofort nach der Installation von DLP zu profitieren.

Sicherheit und Compliance über die Firewall hinaus
Die Integration von DLP und DRM schützt und prüft Daten an jedem Ort: in Händler- und Partnernetzwerken, in öffentlichen Netzwerken, in der Cloud oder auf Mobilgeräten.

Kürzere Vorfalllisten
DLP kann so konfiguriert werden, dass durch DRM geschützte Dateien als sicher eingestuft werden – und für solche Dateien keine Alarme ausgegeben werden. Dadurch werden deutlich weniger Vorfälle protokolliert.

Minimaler Schulungsaufwand
Der Schulungsaufwand für Endbenutzer liegt praktisch bei null, da der Schutz automatisch erfolgt und ein geschütztes Dokument wie jedes andere Dokument in der Originalanwendung geöffnet werden kann.

Höhere geschäftliche Agilität
Die Fähigkeit, Daten auch außerhalb der Unternehmensgrenzen zu schützen, beseitigt eine knifflige Compliance-Herausforderung. Die Sicherheitsrisiken werden erheblich reduziert und die sichere Einführung von File-Sharing-Diensten, BYOD und Cloud-Computing wird möglich.

Durchgängige Prüfung und Einhaltung gesetzlicher Vorgaben
Die Integration von DLP und DRM ermöglicht die Einhaltung gesetzlicher Vorgaben über den gesamten Lebenszyklus unstrukturierter Daten – sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks.

Durchsetzung von IT-Richtlinien bei Dritten
Die Integration von DLP und DRM hilft bei der Durchsetzung der Data-Governance- und IT-Richtlinien Ihres Unternehmens gegenüber Auftragnehmern, Lieferanten, Partnern und anderen Dritten.

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datensicherheit und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die auf menschlichem Verhalten basierenden Lösungen von Forcepoint passen sich in Echtzeit an das Nutzerverhalten an und ermöglichen Mitarbeitern einen sicheren Datenzugriff bei voller Produktivität. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Tausende von Kunden weltweit.

forcepoint.com/contact

Über Seclore

Seclore hat die erste datenorientierte Sicherheitsplattform für den Browser auf den Markt gebracht. Damit können Unternehmen branchenführende Lösungen nutzen, um die Datennutzung zu erkennen, zu identifizieren, zu schützen und zu prüfen, egal wo sich diese Daten befinden, sowohl innerhalb als auch außerhalb der Unternehmensgrenzen. Durch die Automatisierung des datenorientierten Sicherheitsprozesses können Unternehmen ihre Informationen mit minimalen Reibungsverlusten und Kosten umfassend schützen. Über 2000 Unternehmen in 29 Ländern nutzen bereits Seclore, um ihre Ziele in den Bereichen Datensicherheit, Governance und Compliance zu erreichen.

seclore.com/contact