Forcepoint Data Loss Prevention

Schutz von Daten in einer Welt ohne Perimeter-Sicherheit

Forcepoint

Broschüre

forcepoint.com/de

Forcepoint Data Loss Protection (DLP)

Datensicherheit überall dort, wo Ihre Mitarbeiter arbeiten und sich die Daten befinden

Unternehmen jeder Größe stehen heute im Bereich der Sicherheit von kritischen Daten vor großen Herausforderungen. Sie müssen die gesetzlichen Vorschriften zum Schutz sensibler Daten wie personenbezogener Daten (PII), geschützter Gesundheitsinformationen (PHI) und anderer regulierter Daten einhalten. Gleichzeitig müssen sie sich an moderne Arbeitsumgebungen wie Cloud-Anwendungen, hybride Arbeitsumgebungen und BYOD-Trends anpassen, die die Möglichkeiten erhöhen, wie Daten das Unternehmen verlassen können.

Diese wachsende Angriffsfläche stellt heute die größte Herausforderung für den Schutz kritischer Daten dar. Datensicherheitsteams müssen die zunehmende Datenbewegung innerhalb und außerhalb des Unternehmensbereichs bewältigen. Sie benötigen umfassende Transparenz über Cloud-, Web- und lokale Daten. Darüber hinaus sind Kontrolle und Aufsicht über alle Kanäle unerlässlich: Endpunkte, Webverkehr, Netzwerk, E-Mail, Cloud-Anwendungen und private Anwendungen werden zentral verwaltet.

Forcepoint DLP ist die branchenweit zuverlässigste Lösung und bietet Ihnen die notwendigen Tools, um globale Richtlinien über alle wichtigen Kanäle hinweg einfach verwalten zu können, ob Endgeräte, Netzwerk, Cloud, Internet, private Anwendungen oder E-Mail. Wir erleichtern Ihnen die Arbeit mit den am stärksten vordefinierten Vorlagen, Richtlinien und Klassifizierungen aller DLP-Anbieter auf dem Markt. Dadurch lässt sich Ihr Störungsmanagement drastisch rationalisieren, damit Sie sich auf das Wesentliche konzentrieren können. Darüber hinaus werden Risiken eliminiert, damit Ihre Mitarbeiter produktiver arbeiten können. Forcepoint DLP begegnet Risiken mit Transparenz und Kontrolle, egal wo Ihre Mitarbeiter arbeiten und wo sich Ihre Daten befinden.

Beim Schutz von Daten steht Folgendes im Vordergrund:

- **Absicherung regulierter Daten** mithilfe einer Kontrollzentrale für alle Anwendungen, mit denen Ihre Mitarbeiter Daten erstellen, speichern und übertragen.
- **Schützen Sie sensible Daten** mit erweiterten DLPFunktionen, die analysieren, wie Benutzer Daten verwenden, Ihre Mitarbeiter schulen, damit sie gute Datenentscheidungen treffen, und Vorfälle nach Risiko priorisieren.
- **Sorgen Sie für die sichere Nutzung von generativer KI,** indem Sie robuste DLP-Kontrollen und -Richtlinien implementieren, um die Nutzung an allen Standorten und in allen Anwendungen zu schützen, vom Endbenutzer über das Web bis hin zur Cloud.

Einhaltung von Vorschriften beschleunigen

Moderne IT-Umgebungen stellen eine große Herausforderung für Unternehmen dar, die Dutzende von globalen Datensicherheitsvorschriften einhalten müssen, insbesondere bei der Umstellung auf Cloud-Anwendungen und mobile Belegschaften. Viele Sicherheitslösungen bieten eine Form von integrierten DLP-Funktionen, wie sie beispielsweise in CASB- und SWG-Anwendungen zu finden ist.

Dennoch sehen sich Sicherheitsteams mit unerwünschter Komplexität und zusätzlichen Kosten konfrontiert, wenn sie getrennte und uneinheitliche DLP-Richtlinien für Endpunkte, Cloud-Anwendungen und Datenverkehr im Web bereitstellen und verwalten. Forcepoint DLP beschleunigt Ihre Compliance-Bemühungen, indem es mehr sofort einsatzbereite vordefinierte Klassifizierer, Richtlinien und Vorlagen als jeder andere große Anbieter bereitstellt. Dies beschleunigt die anfängliche DLP-Bereitstellung und vereinfacht die laufende DLP-Verwaltung.

- → **Regulieren Sie die Abdeckung**, um ganz einfach die Konformität mit mehr als 1700 vordefinierten Vorlagen, Richtlinien und Klassifizierungen zu erfüllen und aufrechtzuerhalten, die den gesetzlichen Anforderungen von 90 Ländern und über 150 Regionen entsprechen.
- → **Zentralisierte Kontrolle** und einheitliche Richtlinien über alle Kanäle hinweg, einschließlich Cloud-Anwendungen, Web, E-Mail und Endpunkte.

Mitarbeiter befähigen, Daten zu schützen

Eine DLP-Lösung mit rein präventiven Kontrollmechanismen frustriert Benutzer und bringt sie dazu, diese zu umgehen, um ihre Aufgabe erledigen zu können. Das Umgehen von Sicherheitsmaßnahmen führt allerdings zu unnötigen Risiken und evtl. zu unbeabsichtigter Datenweitergabe.

Für Forcepoint DLP sind Ihre Mitarbeiter die erste Verteidigungslinie gegen die heutigen Cyber-Bedrohungen.

- → **Datenkontrolle und -ermittlung**, wo immer sie sich befinden, sei es in Cloud-Anwendungen, im Datenverkehr im Internet, in E-Mails oder an Endpunkten.
- → **Mitarbeiter-Coaching** für das Treffen intelligenter Entscheidungen mithilfe von benutzerdefinierten Meldungen, die Benutzeraktionen lenken, Mitarbeiter über Richtlinien informieren und die Benutzerabsicht bei der Interaktion mit kritischen Daten überprüfen.
- → **Sichere Zusammenarbeit** mit vertrauenswürdigen Partnern durch richtlinienbasierte automatische Verschlüsselung, die Daten bei der Übertragung außerhalb Ihres Unternehmens schützt.
- → **Automatisieren Sie die Datenkennzeichnung und-klassifizierung** bdurch Integration mit Forcepoint Data Classification sowie Microsoft Purview Information Protection.

Erweiterte Erkennungs- und Kontrollfunktionen, die sich an den Daten orientieren

Böswillige und versehentliche Datenschutzverletzungen sind komplexe Vorfälle, keine Einzelereignisse. Forcepoint DLP wird von Forrester, Radicati Group und Frost & Sullivan als Branchenführer für DLP-Lösungen anerkannt. Eines der wichtigsten Merkmale von Forcepoint DLP ist die Fähigkeit, Daten im Speicher, bei der Übertragung und bei der Verwendung zu identifizieren. Zu den Funktionen zur Datenidentifizierung gehören:

- → **Optische Zeichenerkennung (OCR)** identifiziert Daten, die in Bilder eingebettet sind, egal ob im Speicher oder während der Übertragung.
- → **Zuverlässige Ermittlung** personenbezogener Daten für Datenvalidierungsprüfungen, Echtnamenerkennung, Nachbarschaftsanalyse und Kontextbezeichner.
- → **Benutzerdefinierte Erkennung von Verschlüsselung** enthüllt Daten, die für die Ermittlung und die maßgeblichen Kontrollen unsichtbar sind.
- → **Kumulative Analyse** für „Drip- DLP-Erkennung" (also für Daten, die nach und nach durchsickern).
- → **Integration mit Forcepoint Data Classification**, die hochgradig trainierte KI/LLM-Modelle nutzt, um eine hochpräzise Klassifizierung für derzeit verwendete Daten und Daten im Ruhezustand mit Forcepoint Data Security Posture Management (DSPM).

- → **Analysen** zu Änderungen beim Benutzerverhalten im Zusammenhang mit der Interaktion mit Daten, z. B. erhöhte Nutzung der privaten E-Mail-Adresse. Durch risikogerechten Schutz ist Forcepoint DLP noch effektiver, da man anhand der Verhaltensanalyse das Benutzerrisiko verstehen und diese Erkenntnisse wiederum für die Implementierung risikoadaptiver Richtlinien nutzen kann. So können Sicherheitsteams dynamische Richtlinien implementieren, die im Gegensatz zu statischen, globalen Richtlinien individualisiert sind.

Erkennen, Verwalten und Beheben von Risiken bei der Datensicherheit

Den meisten DLP-Lösungen fehlt die Robustheit einer starken, vordefinierten Klassifizierungsbibliothek und die Transparenz über sämtliche Daten hinweg, wodurch Benutzer mit False-Positive-Meldungen überhäuft werden und gefährdete Daten übersehen. Dies schränkt nicht nur die Effizienz der Sicherheitsteams ein, sondern führt auch zu Frustration bei Mitarbeitern bzw. Endbenutzern, da Sicherheitslösungen so zum Hindernis für die betriebliche Produktivität werden. Dank Analysen und der umfangreichsten Bibliothek an vordefinierten Vorlagen und Richtlinien in der Branche reduziert Forcepoint DLP False Positives drastisch und sorgt somit für effizientere Sicherheitsmaßnahmen. Um das Sicherheitsbewusstsein der Mitarbeiter zu erhöhen, unterstützt DLP das Mitarbeiter-Coaching und die

- → **Reaktionsteams auf das größte Risiko ansetzen** – mit priorisierten Vorfällen, die Personen mit riskantem Nutzungsverhalten, gefährdete kritische Daten und typische Verhaltensmuster der Benutzer hervorheben.
- → **Das Mitarbeiter-Coaching** erfolgt in Form von Pop-ups. Diese können mit dem Namen des Unternehmens, einer kurzen Schulungsanweisung für den Grund des Pop-ups und einer URL, auf die der Benutzer klicken kann, um weitere Informationen über die relevanten Sicherheitsrichtlinien des Unternehmens zu erhalten, personalisiert werden.
- → **Dateninhaber und Manager in Entscheidungen einbinden**, indem DLP-Vorfälle zum Überprüfen und zum Ergreifen weiterer Maßnahmen über einen E-Mail-basierten Workflow an sie weitergeleitet werden.
- → **Benutzerdaten schützen** – mit Anonymisierungsoptionen und Zugriffskontrollen.
- → **Datenkontext hinzufügen** – für eine umfassendere Benutzeranalyse durch tiefgehende Integration in Forcepoint Risk-Adaptive Protection.

Data Visibility überall, auch in der Cloud und vor Ort

Unternehmen müssen heute mit komplexen Umgebungen umgehen, in denen Daten praktisch überall sind und auch an Orten geschützt werden müssen, die das Unternehmen nicht verwaltet oder besitzt. Forcepoint ONE Data Security for CASB and SWG erweitert Analysen und DLP-Richtlinien auf kritische Cloud-Anwendungen und den Datenverkehr im Web. So sind Ihre Daten geschützt, wo immer sie sich befinden.

- → **Reaktionsteams ermöglichen, Daten zu identifizieren und zu schützen – auch über** Cloud-Anwendungen, im Web sowie in E-Mails und auf Endgeräten, mit Forcepoint ONE for Email und Forcepoint ONE for Endpoints.
- → **Weitergabe sensibler Daten** an externe oder nicht autorisierte interne Benutzer identifizieren und automatisch unterbinden.
- → **Daten** für Uploads in und Downloads aus kritischen Cloud-Anwendungen (Office 365, Teams, SharePoint, OneDrive, Salesforce, Box, Dropbox, Google Apps, AWS, ServiceNow, Zoom, Slack etc.) in Echtzeit schützen.
- → **Durchsetzung von Richtlinien über eine einzige Konsole vereinheitlichen**, um Richtlinien zu Daten während der Übertragung und zur Datenerkennung über alle Kanäle hinweg (Cloud, Netzwerk, Endpunkte, Internet und E-Mail) zu definieren und anzuwenden.
- → **Eine von Forcepoint gehostete Lösung implementieren**, die Funktionen für DLP-Richtlinien auf Cloud-Anwendungen ausweitet und gleichzeitig Vorfälle und forensische Daten innerhalb des Rechenzentrums verwalten kann.

Weitere Informationen über DLP

Demo anfordern

Forcepoint Data Security – Lösungen

Forcepoint ONE Data Security	Forcepoint ONE Data Security, eine Cloud-native Lösung, schützt sensible Daten, verhindert Sicherheitsverletzungen und sorgt für globale Compliance. Durch die schnelle Bereitstellung und Richtlinienverwaltung wird die Datensicherung optimiert. Es bietet eine einheitliche Verwaltung für Cloud-Apps, Web, E-Mail und Endpunkte. Mit Forcepoint Risk-Adaptive Protection bietet es Echtzeit-Einblicke in Benutzerrisiken. Erleben Sie reduzierte Kosten, Risiken und eine erhöhte Produktivität mit Forcepoint ONE Data Security.
Forcepoint DSPM	Forcepoint DSPM meistert die Herausforderung der ausufernden Datenmengen über Cloud-Plattformen und -Server hinweg, indem es eine beispiellose Transparenz und Kontrolle bietet. Es verwendet KI-gestütztes maschinelles Lernen, um die Datenerkennung und -klassifizierung kontinuierlich zu verbessern. Darüber hinaus automatisiert es Aufgaben wie die Behebung von Mängeln und die Erstellung von Berichten, um Prozesse zu rationalisieren und Kosten zu senken.
Risk-Adaptive Protection	Im Gegensatz zu herkömmlichen richtlinienorientierten DLP-Lösungen stellt unsere Risk-Adaptive Protection (RAP) den Menschen in den Vordergrund, der sein Verhalten versteht, um das Risiko proaktiv zu mindern. RAP priorisiert Benutzer mit hohem Risiko und bietet Risikoberechnungen in Echtzeit, über 130 Verhaltensindikatoren und eine reibungslose Bereitstellung. Gewinnen Sie Einblicke mit übersichtlichen Dashboards, steigern Sie die Produktivität mit granularer Richtliniendurchsetzung, und entschärfen Sie Insider-Bedrohungen proaktiv durch dynamische Automatisierung.
Forcepoint Data Classification	Forcepoint Data Classification definiert die Datenklassifizierung mit KI-gesteuerter Präzision und Automatisierung neu, eliminiert manuelle Fehler und verbessert die DLP-Effizienz. Wir nutzen generative KI und große Sprachmodelle, um eine hervorragende Klassifizierungsgenauigkeit zu erzielen. Durch ständiges Lernen und Verbessern liefert es zuverlässige Empfehlungen und sorgt für eine verstärkte Durchsetzung von Richtlinien und Compliance. Gewährleisten Sie eine nahtlose Integration in Ihren Workflow, verbessern Sie die Produktivität und reduzieren Sie Fehlalarme.
Forcepoint ONE Data Security for Email	Forcepoint ONE Data Security for Email schützt vor sensiblen Datenlecks über den kritischen E-Mail-Kanal. Diese vollständig Cloud-native Lösung wehrt E-Mail-Sicherheitsverletzungen und Datenverlust über E-Mail sowohl auf Endgeräten als auch auf mobilen Geräten ab. Die Lösung ist nahtlos in gängige E-Mail-Provider integriert und bietet eine unkomplizierte Verwaltung mit vorgefertigten Sicherheitsrichtlinien, Klassifizierern und Vorlagen.
Forcepoint DLP for Cloud Email (lokal Enterprise DLP)	Forcepoint DLP for Cloud Email verhindert unerwünschtes Herausschleusen von Daten und intellektuellem Eigentum über ausgehende E-Mails. Diese Lösung kann mit anderen Forcepoint DLP-Lösungen für Kanäle, wie Endbenutzer, Netzwerk, Cloud und Internet, kombiniert werden, um die DLP-Verwaltung sowie das Schreiben und Bereitstellen von Richtlinien über mehrere Kanäle hinweg zu erleichtern. Forcepoint DLP for Cloud Email bietet ein enormes Skalierungspotenzial für unvorhergesehenen Mengen an E-Mail-Verkehr. Zudem kann der ausgehende E-Mail-Verkehr problemlos mit Ihrem Unternehmen mitwachsen, ohne dass zusätzliche Hardwareressourcen konfiguriert und verwaltet werden müssen.
Forcepoint ONE CASB und SWG	Forcepoint ONE Data Security für CASB und SWG bietet dieselbe vollständig Cloud-native DLP-Lösung wie Forcepoint ONE Data Security for Endpoint und Forcepoint Data Security for Email, die es Ihnen ermöglicht, einen oder alle 4 Kanäle von einer einzigen Benutzeroberfläche aus zu verwalten. Außerdem können Sie alle Richtlinien über dieselbe Konsole zur Richtlinienverwaltung synchronisieren. Schreiben Sie Richtlinien nur einmal und stellen Sie sie über alle Kanäle von Forcepoint ONE Data Security bereit – das spart Zeit und Ressourcen bei der Synchronisierung von Richtlinien über mehrere Dienste hinweg.

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint vereinfacht die Sicherheit für internationale Unternehmen und die öffentliche Hand. Die für die Cloud konzipierte All-in-One-Plattform von Forcepoint erleichtert das Einführen von Zero Trust und das Verhindern des Diebstahls und Verlusts sensibler Daten und intellektuellen Eigentums, ganz gleich, wo Ihre Mitarbeiter arbeiten. Forcepoint mit Sitz in Austin, Texas, schafft sichere, vertrauenswürdige Umgebungen für Kunden und ihre Mitarbeiter in mehr als 150 Ländern. Kontaktieren Sie Forcepoint auf www.forcepoint.com, Twitter und LinkedIn.

[DLP-BROCHURE-DE] 23Aug2024