Forcepoint Data Loss Prevention

Schutz von Daten in einer Welt ohne Perimeter-Sicherheit

Forcepoint

Broschüre

forcepoint.com/de

Forcepoint Data Loss Protection (DLP)

Schützen Sie Ihre KI-Transformation mit Forcepoint

Unternehmen weltweit durchlaufen eine transformative Reise, die durch die Integration von KI, insbesondere GenAI-Anwendungen und -Technologie, in ihre Geschäftsprozesse angetrieben wird. Dies verspricht zwar erhebliche Produktivitätsgewinne, führt aber auch zu neuen Herausforderungen bei der Datensicherheit. Beispielsweise können Benutzer sensible Daten eingeben oder vertrauliche Dateien in GenAI-Anwendungen hochladen, was Datenverletzungen erleichtern könnte. Forcepoint bietet eine Lösung, mit der Sie das Potenzial von KI nutzen können, ohne Ihr wertvollstes Asset zu gefährden: Ihre Daten.

Mit Forcepoint gewährleistet unsere hochmoderne AI Mesh-Technologie eine beispiellose Datenklassifizierungsgenauigkeit und -effizienz. Dies gibt Ihnen den nötigen Seelenfrieden, wenn Sie mit der Komplexität der KI-Transformation umgehen müssen. Egal, ob Sie GenAI-Apps wie ChatGPT, Copilot, Gemini oder andere verwenden, Forcepoint bietet zentrale Transparenz und Kontrolle und schützt Ihre sensiblen Daten in allen Umgebungen.

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

Forcepoint DLP adressiert kritische Datensicherheitsherausforderungen, denen Unternehmen jeder Größe gegenüberstehen. Da sich die regulatorischen Anforderungen verschärfen, wird der Schutz sensibler Informationen – wie personenbezogene Daten (PII) und geschützte Gesundheitsinformationen (PHI) – von größter Bedeutung. Moderne Arbeitsumgebungen, einschließlich Cloud-Anwendungen, Hybrid-Setups und BYOD-Trends, erschweren den Datenschutz zusätzlich.

Die wachsende Angriffsfläche erfordert umfassende Transparenz und Kontrolle. Forcepoint DLP unterstützt Datensicherheitsteams durch die Verwaltung globaler Richtlinien über wichtige alle wichtigen Kanäle: Endpunkte, Netzwerke, Cloud, Internet, private Anwendungen und E-Mail. Unsere vordefinierten Vorlagen und Klassifikatoren optimieren das Incident-Management, sodass Sie sich auf die Produktivität konzentrieren und gleichzeitig Risiken minimieren können. Wo immer Ihre Beschäftigten arbeiten und Ihre Daten gespeichert sind, Forcepoint DLP gewährleistet Transparenz und Kontrolle.

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.

Vereinfachte Compliance

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.

- → **Definieren Sie die Richtlinienabdeckung,** um die Einhaltung von Compliance-Vorgaben sicherzustellen – mit über 1700 vordefinierten Vorlagen, Richtlinien und Klassifikatoren, die auf die regulatorischen Anforderungen aus 90 Ländern und über 160 Regionen abgestimmt sind.
- → **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).
- → **Intelligentere Durchsetzung** durch die Identifizierung von auffälligem Benutzerverhalten im Zusammenhang mit Dateninteraktionen, wie die verstärkte Nutzung von persönlichen E-Mail-Adressen. Mit Risk-Adaptive Protection ist Forcepoint DLP noch effektiver, da man anhand der Verhaltensanalyse das Benutzerrisiko verstehen und diese Erkenntnisse wiederum für die Implementierung automatisierter risikoadaptiver Richtlinien nutzen kann. So können Sicherheitsteams dynamische Richtlinien implementieren, im Gegensatz zu rein statischen, allgemeingültigen Richtlinien.

AI Mesh

Nutzen Sie das ganze Potenzial von KI, ohne das wertvollste Asset Ihres Unternehmens zu gefährden: Ihre Daten. Mit Forcepoint bietet unsere hochmoderne AI Mesh-Technologie eine beispiellose Datenklassifizierungsgenauigkeit und -effizienz, sodass Sie ganz beruhigt sein können. Unsere zentrale Transparenz und Kontrolle schützt Ihre Daten überall, einschließlich in GenAI-Apps wie ChatGPT, Copilot, Gemini und vielen anderen. Steigern Sie die Produktivität, indem Sie Ihrem Team die sichere Verwendung von GenAI und anderen Apps ermöglichen. Senken Sie Kosten mit vereinfachten Abläufen und einheitlichen Richtlinien.

- → **Synchronisieren Sie mit Forcepoint Data Classification** und nutzen Sie hochgradig trainierte AI Mesh- und LLM-Modelle, um eine hochpräzise Klassifizierung von Daten in der Verwendung und im Ruhezustand mit Forcepoint Data Security Postgure Management (DSPM) zu ermöglichen.

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.

Verhindern Sie Datenschutzverletzungen in Echtzeit

Datenschutzverletzungen können im Handumdrehen passieren, und die Folgen können sehr schädlich sein – sowohl finanziell als auch in Bezug auf den Ruf. Forcepoint DLP stattet Ihr Unternehmen mit den Tools aus, um Verstöße direkt dann zu erkennen und zu verhindern, wenn sie auftreten. Sensiblen Daten werden so zuverlässig geschützt. Und durch die Bereitstellung eines fortschrittlichen Echtzeitschutzes mit einheitlichem Management, werden Security Teams in die Lage versetzt, den sich entwickelnden Bedrohungen immer einen Schritt voraus zu sein.

- → **Echtzeitüberwachung und -blockierung:** Erkennen und stoppen Sie Datenschutzverletzungen in Echtzeit, bevor sensible Informationen offengelegt werden.
- → **Einheitliches Richtlinienmanagement:** Vereinfachen Sie die Sicherheit von einer einzigen Konsole aus, die es Ihnen ermöglicht Richtlinien in Ihrer gesamten Umgebung zu managen und umfassende Datensicherheit zu gewährleisten.
- → **Kanalübergreifende Transparenz bei Sicherheitsvorfällen:** Verschaffen Sie sich einen vollständigen Überblick über die Datenbewegung im Web, in der Cloud, in E-Mails und auf Endgeräten, um schnell auf Bedrohungen reagieren zu können.
- → **Forensik:** Decken Sie die gesamte Historie von Datenbewegung auf, um Vorfälle zu untersuchen, Verstöße zu verhindern, Richtlinien zu stärken und die Einhaltung von Compliance-Vorgaben sicherzustellen.
- → **Risk-Adaptive Protection:** Passen Sie Sicherheitskontrollen dynamisch an Benutzerverhalten und Risikostufen an, um sicherzustellen, dass sensible Daten geschützt bleiben, ohne dabei die Produktivität zu beeinträchtigen.

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 (DLP SaaS)	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 Datenverbreitung über Cloud-Plattformen und -Server hinweg, indem es eine beispiellose Transparenz und Kontrolle bietet. Es verwendet die AI Mesh-Technologie, um die Datenerkennungs- und Klassifizierungsgenauigkeit kontinuierlich zu verbessern. Außerdem automatisiert es Aufgaben wie Korrektur und Reporting, um Prozesse zu optimieren 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 ONE Data Security for Email (DLP SaaS)	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 ONE Data Security for Cloud Apps and Web (DLP SaaS)	Forcepoint ONE Data Security for Cloud Apps and Web bietet dieselbe vollständig Cloud-native DLP-Lösung wie Forcepoint ONE Data Security for Endpoint und Forcepoint Data Security for Email. So können Sie einen oder alle der vier Kanäle über eine einzige Benutzeroberfläche verwalten und alle Richtlinien über dieselbe Konsole zur Richtlinienverwaltung synchronisieren. Richtlinien müssen nur einmal erstellt werden und können über alle Kanäle von Forcepoint ONE Data Security bereitgestellt werden – das spart Zeit und Ressourcen bei der Synchronisierung von Richtlinien über mehrere Dienste hinweg.
Forcepoint Data Classification	Forcepoint Data Classification definiert die Datenklassifizierung mit AI Mesh-fähiger Präzision und Automatisierung neu, wodurch manuelle Fehler vermieden und die DLP-Effizienz verbessert wird. Wir nutzen die AI Mesh-Technologie und Large Language Models, um eine überragende Klassifizierungsgenauigkeit zu gewährleisten. Durch kontinuierliches Lernen und Verbesserungen liefert diese Lösung zuverlässige Empfehlungen und verbessert die Richtliniendurchsetzung und Compliance. Sorgen Sie für eine nahtlose Integration in Ihren Workflow, verbessern Sie die Produktivität und reduzieren Sie Fehlalarme.
Forcepoint DLP Endpoint	Forcepoint DLP Endpoint schützt Ihre kritischen Daten auf Windows- und Mac-Endgeräten im Unternehmensnetzwerk und auch außerhalb. Die Lösung umfasst erweiterten Schutz und erweiterte Kontrolle von Data-at-Rest (Discovery), Data-in-Motion und Data-in-Use. Die Integration in Microsoft Azure Information Protection ermöglicht die Analyse verschlüsselter Daten und die Anwendung geeigneter DLP-Kontrollen. Es ermöglicht Mitarbeitern selbstständig Datenrisiken zu beheben, basierend auf Anleitungen aus dem DLP-Coaching-Dialog. Die Lösung überwacht Web-Uploads, einschließlich HTTPS, sowie Uploads an Cloud-Dienste wie Office 365 und Box Enterprise und ist vollständig in Outlook, Notes und E-Mail-Clients integriert.
Forcepoint DLP Discover	Forcepoint DLP Discovery identifiziert und sichert sensible Daten auf Dateiservern, SharePoint (lokal und in der Cloud), Exchange (lokal und in der Cloud) sowie in Datenbanken wie SQL-Server und Oracle. Die fortschrittliche Fingerprinting-Technologie identifiziert sensible Daten und geistiges Eigentum und schützt diese Daten durch Anwendung geeigneter Verschlüsselung und Kontrollen. Mittels OCR sind auch Inhalte innerhalb von Bilddateien sichtbar.
Forcepoint DLP Network	Forcepoint DLP Network bietet einen zentralen Durchsetzungspunkt, um den Diebstahl von Data-in-Motion über E-Mail, Web und FTP zu stoppen. Die Lösung hilft dabei den versehentlichen Datenverlust, das Herausschleusen von Daten, durch Angriffe von außen oder durch Insider-Bedrohungen zu identifizieren und zu verhindern. Zusätzlich erkennt OCR sensible Inhalte in Bildern. Und Analytics mit Drip-DLP hilft dabei Diebstahl von einzelnen Datensätzen und anderes risikoreiches Benutzerverhalten aufzudecken und zu unterbinden.
Forcepoint DLP for Cloud Email	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 DLP App Data Security API	Forcepoint DLP App Data Security API macht es Unternehmen einfach, Daten in ihren eigenen Unternehmensanwendungen und -Diensten zu schützen. Sie ermöglicht die Analyse von Datei- und Datenverkehr und erzwingt DLP-Aktionen wie: Zulassen, Blockieren, Freigabe über Pop-up-Fenster, Verschlüsselung, Freigabeaufhebung und Quarantäne. Dabei handelt es sich um eine REST-API, die ohne umfassende Schulung oder Kenntnisse komplexer Protokolle leicht zu verstehen und einfach zu verwenden ist. Sie ist sprachunabhängig und ermöglicht die Entwicklung und Verwendung in jeder Programmiersprache oder Plattform.

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] 17Jan2025