Forcepoint Data Loss Prevention (DLP)

Datenschutz in einer Welt ohne Netzwerkgrenzen

Forcepoint

Broschüre

forcepoint.com

Forcepoint DLP

Am Faktor Mensch orientierte Sicherheit

Datensicherheit ist eine nie endende Herausforderung. Einerseits sind IT-Organisationen verpflichtet, sich an Vorschriften zu halten und geistiges Eigentum vor gezielten Angriffen und versehentlicher Preisgabe zu schützen, andererseits müssen sie sich an tiefgreifende Änderungen in der IT anpassen, wie z. B. die Umstellung auf Cloud-Anwendungen, hybride Cloud-Umgebungen und BYOD-Trends, die alle immer mehr Möglichkeiten bieten, wie Daten aus Ihrem Unternehmen gelangen können.

Diese wachsende Angriffsfläche stellt die größte Herausforderung beim Schutz kritischer Daten dar. Für die Datensicherheit zuständige Teams verfolgen den scheinbar logischen Ansatz bei der Verfolgung von Daten: Auffinden, Katalogisieren, Kontrollieren. Doch dieser konventionelle Ansatz zum Verhindern von Datenverlust ist nicht mehr wirkungsvoll, da dabei die größte Variable im Bereich der Datensicherheit ignoriert wird: Ihr Personal.

Anstatt sich ausschließlich auf Daten zu konzentrieren, sollte das Thema Sicherheit bei den Mitarbeitern beginnen und enden. Entscheidend ist dabei, Einblick in die Interaktion der Benutzer mit Daten und Anwendungen zu gewinnen. Sobald dies erreicht ist, können Sie eine Kontrollebene einführen, die auf dem Risiko des jeweiligen Benutzers und der Vertraulichkeit oder dem Wert der Daten basiert.

Das Programm zum Schutz von Unternehmensdaten muss den menschlichen Aspekt berücksichtigen, d. h. die Schnittmenge von Benutzern, Daten und Netzwerken. Darüber hinaus muss das Unternehmen die Daten im Auge behalten, während sie sich durch das Unternehmen bewegen, und die Personen hervorheben, die Daten erstellen, bearbeiten und verlagern.

Forcepoint DLP begegnet von Menschen ausgehenden Risiken mit Transparenz und Kontrolle, wo auch immer Ihre Mitarbeiter arbeiten und sich Ihre Daten befinden. Sicherheitsteams bewerten Benutzerrisiken, um sich auf die wichtigsten Ereignisse zu konzentrieren und die Einhaltung globaler Datenvorschriften zu forcieren.

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.
- **Schutz geistigen Eigentums** mit ausgefeilten DLP-Funktionen, die die Datennutzung Ihrer Mitarbeiter analysieren, diese bei der Entscheidungsfindung in Datenfragen unterstützen und Vorfälle nach Risiko priorisieren.

Transparenz und Kontrolle unabhängig von Arbeitsplatz und Datenspeicherort

- **Cloud-Anwendungen**
- **Endpunkt**
- **Netzwerk**
- **Erkennung**

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 integriertem DLP, wie sie beispielsweise in Cloud-Anwendungen zu finden ist.

Dennoch sehen sich Sicherheitsteams mit unerwünschter Komplexität und zusätzlichen Kosten konfrontiert, wenn sie getrennte und uneinheitliche Richtlinien in Endpunkten, Cloud-Anwendungen und Netzwerken bereitstellen und verwalten. Mit Forcepoint DLP haben Ihre Bemühungen um Vorschrifteneinhaltung schnellen Erfolg, da die vordefinierte Abdeckung globaler Vorschriften in Ihrer IT-Umgebung mit zentraler Kontrolle kombiniert wird. Forcepoint DLP schützt vertrauliche Kundendaten und regulierte Daten effizient, sodass Sie die ordnungsgemäße Einhaltung aller Vorschriften jederzeit belegen können.

- → **Regulatorische Erfassung**, um die Einhaltung von mehr als 370 Vorschriften, die laut den Vorgaben von 83 Ländern gelten, zeitnah zu erfüllen und beizubehalten.
- → **Auffinden und Klären** regulierter Daten mit Netzwerk-, Cloud- und Endpunktermittlung.
- → **Zentrale Kontrolle** und einheitliche Richtlinien in der gesamten IT-Umgebung.

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 unbeabsichtigter Datenweitergabe.

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

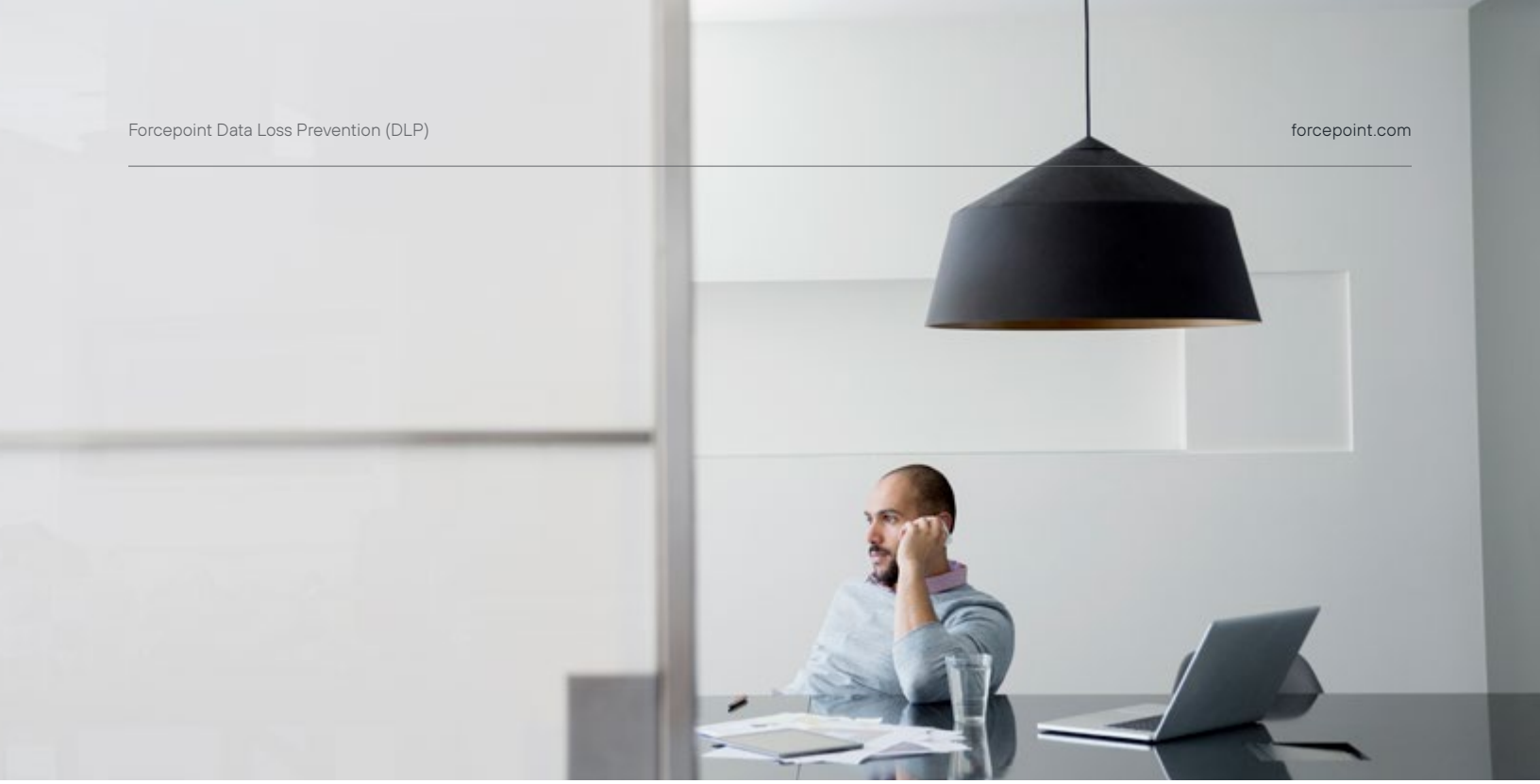
- → **Datenkontrolle und -ermittlung** unabhängig vom Speicherort – ob in der Cloud oder im Netzwerk, in E-Mails oder am Endpunkt.
- → **Mitarbeiter-Coaching** für das Treffen intelligenter Entscheidungen mithilfe von Meldungen, die Benutzeraktionen lenken, Mitarbeiter über Richtlinien informieren und 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.
- → **Automatisierte Datenkennzeichnung und -klassifizierung** durch Integration führender Datenklassifizierungslösungen von Drittanbietern (z. B. Microsoft Azure Information Protection, Titus, Boldon James).

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

Böswillige und versehentliche Datenschutzverletzungen sind komplexe Vorfälle, keine Einzelereignisse. Forcepoint DLP ist eine bewährte Lösung, die von Analysten wie Gartner, Radicati und anderen als branchenführend anerkannt wird. Forcepoint DLP ist in zwei Versionen erhältlich: DLP for Compliance und DLP for IP Protection.

Forcepoint DLP for Compliance und Forcepoint DLP for IP Protection bieten wichtige Funktionen für die Einhaltung von Vorschriften. Dazu 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 in Microsoft Azure Information Protection** analysiert verschlüsselte Dateien und wendet geeignete DLP-Kontrollen auf die Daten an.



Forcepoint DLP for IP Protection schließt neben den zuvor erwähnten Funktionen die fortschrittlichste Erkennung und Kontrolle von potenziellem Datenverlust mit den folgenden Funktionen ein:

- **Maschinelles Lernen** ermöglicht Benutzern, das System so zu trainieren, dass es relevante, bisher nicht bekannte Daten identifiziert. Benutzer geben der Engine positive und negative Beispiele an, um ähnliche Geschäftsdokumente, Quellcode und mehr zu kennzeichnen.
- **Fingerprinting** strukturierter (z. B. Datenbanken) und nicht strukturierter Daten (z. B. Dokumente) ermöglicht Verantwortlichen das Definieren von Datentypen und das Identifizieren von vollständigen und teilweisen Übereinstimmungen zwischen Geschäftsdokumenten, Konstruktionsplänen und Datenbanken, um dann die richtige Kontrolle oder Richtlinie anzuwenden, die den Daten entspricht.
- **Analysen** zu Änderungen beim Benutzerverhalten im Zusammenhang mit der Interaktion mit Daten, z. B. erhöhte Nutzung der privaten E-Mail-Adresse. Mit Dynamic Data Protection (DDP) 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 Vergleich zu statischen, globalen Richtlinien individualisiert sind.

Erkennen, Verwalten und Beheben von Risiken bei der Datensicherheit

Herkömmliche Ansätze für DLP überlasten Benutzer mit Fehlalarmen, während gefährdete Daten unberücksichtigt bleiben. 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. Durch gezielte Analysen kann Forcepoint DLP Fehlalarme reduzieren, was Sicherheitsteams entlastet. Um das Sicherheitsbewusstsein der Mitarbeiter zu erhöhen, unterstützt DLP das Mitarbeiter-Coaching und die Integration von Datenklassifizierungslösungen.

- **Reaktionsteams auf das größte Risiko ansetzen** – mit priorisierten Vorfällen, die Personen mit riskantem Nutzungsverhalten, gefährdete kritische Daten und typische Verhaltensmuster der Benutzer hervorheben.
- **Das Bewusstsein der Mitarbeiter steigern** – für den Umgang mit sensiblen Daten und geistigem Eigentum durch Mitarbeiter-Coaching (Windows oder MacOS) und die Integration von Klassifizierungslösungen wie Boldon James und Microsoft Azure Information Protection.
- **Fortschrittliche DLP-Funktionen zur Datenidentifizierung umsetzen** – z. B. Fingerprinting auf Remote-Endpunkten und in Cloud-Anwendungen des Unternehmens.
- **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.
- **Daten Kontext hinzufügen** – tiefgehende Integration in Forcepoint Insider Threat und Forcepoint Behavioral Analytics ermöglicht eine umfassendere Benutzeranalyse.

Transparenz überall, wo Ihre Mitarbeiter arbeiten; Kontrolle überall, wo sich Ihre Daten befinden

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. Mit Forcepoint DLP for Cloud Applications können Analysen und DLP-Richtlinien auch in kritischen Cloud-Anwendungen angewendet werden. So sind Ihre Daten geschützt, wo auch immer sie sich befinden.

- → **Reaktionsteams ermöglichen, Daten zu identifizieren und zu schützen** – auch über Cloud-Anwendungen, Netzwerkdatenspeicher und verwaltete Endpunkte hinaus.
- → **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, Salesforce, Box, Dropbox, Google Apps, Amazon 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 und Endpunkte) zu definieren und anzuwenden.
- → **Eine von Forcepoint gehostete Lösung implementieren**, die Funktionen für DLP-Richtlinien einschließlich Fingerprinting und maschinellem Lernen auf Cloud-Anwendungen ausweitet und gleichzeitig Vorfälle und forensische Daten innerhalb des Rechenzentrums verwalten kann.

Forcepoint DLP bietet bei jeder Bereitstellung von einer Kontrollzentrale aus erweiterte Analyse- und Regulierungsrichtlinienvorlagen. Unternehmen wählen die für ihre IT-Umgebung passenden Bereitstellungsoptionen.

Anhang A: Übersicht über die Komponenten der DLP-Lösung

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 gespeicherten Daten (Ermittlung), während der Übertragung und im Einsatz. Die Integration in Microsoft Azure Information Protection ermöglicht die Analyse verschlüsselter Daten und die Anwendung geeigneter DLP-Kontrollen. So können Mitarbeiter Datenrisiken selbstständig auf Grundlage des DLP-Coaching beseitigen. Die Lösung überwacht Uploads ins Internet, einschließlich HTTPS, sowie Uploads in Cloud-Dienste wie Office 365 und Box Enterprise. Vollständige Integration in Outlook, Notes und E-Mail-Clients.
Forcepoint DLP – Cloud Applications	Forcepoint DLP – Cloud Applications basiert auf Forcepoint CASB und erweitert die detaillierte Analyse und zentrale Kontrolle von Forcepoint DLP auf kritische Cloud-Anwendungen, u. a. Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom und Slack.
Forcepoint DLP – Discovery	Forcepoint DLP – Discovery identifiziert und schützt sensible Daten über Dateiserver, SharePoint (lokal und in der Cloud) und Exchange (lokal und in der Cloud) hinweg und ermöglicht die Erkennung innerhalb von Datenbanken (z. B. SQL-Server und Oracle). Die fortschrittliche Fingerprinting-Technologie identifiziert regulierte gespeicherte Daten und geistiges Eigentum und schützt diese Daten mithilfe geeigneter Verschlüsselung und Kontrollen. Mittels OCR sind auch Daten innerhalb von Bilddateien sichtbar.
Forcepoint DLP – Network	Forcepoint DLP – Network ist der entscheidende Garant, um den Diebstahl von Daten während der Übertragung per E-Mail und über Webkanäle zu verhindern. Mit dieser Lösung können das Herausschleusen von Daten und versehentliche Datenverluste durch Angriffe von außen oder durch Insider-Bedrohungen erkannt und verhindert werden. OCR erkennt Daten in Bildern. Mithilfe von Analysen kann DLP den Diebstahl von zur Tarnung vereinzelten Datensätzen und anderes risikoreiches Benutzerverhalten erkennen und unterbinden.

Anhang A: Übersicht über die Komponenten der DLP-Lösung

	FORCEPOINT DLP – ENDPOINT	FORCEPOINT DLP – CLOUD APPLICATIONS	FORCEPOINT DLP – DISCOVERY	FORCEPOINT DLP – NETWORK
Wie erfolgt die Bereitstellung?	Forcepoint One Endpoint	Forcepoint Cloud	Von der IT verwalteter Ermittlungsserver	Netzwerkgerät oder öffentliche Cloud
Was ist die Hauptfunktion?	Sammeln von Informationen über das Endgerät des Benutzers	Ermitteln von Daten und Durchsetzen von Richtlinien in der Cloud oder in Cloud-Anwendungen	Ermitteln, Überprüfen und Korrigieren von in Rechenzentren gespeicherten Daten	Transparenz und Kontrolle für Daten während der Übertragung über das Web und per E-Mail
Wo werden gespeicherte Daten ermittelt/geschützt?	Windows-Endpunkte MacOS-Endpunkte	OneDrive, SharePoint Online, Exchange Online, Google Drive, Box, Dropbox, Salesforce, ServiceNow	Lokale File-Server und Netzwerkspeicher, SharePoint-Server, Exchange-Server, Datenbanken wie Microsoft SQL Server, Oracle und IBM DB2	
Wo werden Daten während der Übertragung geschützt?	E-Mail, Internet: HTTP(S), Drucker, Wechselmedien, File-Server/NAS	Uploads, Downloads und Freigabe für Office 365, Google Apps, Salesforce.com, Box, Dropbox und ServiceNow über API und alle anderen großen Anwendungen über den Proxy		E-Mail, ActiveSync-Proxy, Internet: HTTP(S) ICAP
Wo werden Daten während der Nutzung geschützt?	Zoom, Webex, Google Hangouts, Chat, VOIP-Datenfreigabe, Anwendungen (Cloud-Speicher-Clients), Zwischenablage des Betriebssystems	Bei Aktivitäten zur Zusammenarbeit in Cloud-Anwendungen		
Dynamic Data Protection*	Anwendung			Anwendung
Optische Zeichenerkennung (OCR)			Inbegriffen	Inbegriffen
Integrationen zur Datenklassifizierung und -kennzeichnung	Microsoft Azure Information Protection, Boldon James, Titus			
Für welche Daten sind Fingerprints möglich?*	Strukturierte Daten (Datenbank), unstrukturierte Daten (Dokumente), binäre Daten (Nicht-Textdateien)			
Einheitliche Richtlinienverwaltung	Konfiguration und Durchsetzung von Richtlinien über eine einzige Konsole, von Endpunkten bis hin zu Cloud-Anwendungen In Rechenzentren und der öffentlichen Cloud			
Zuverlässige Richtlinienbibliothek	Erkennung aus Durchsetzung von Richtlinien aus einer umfassenden Bibliothek			

Menschen sind der Neue Perimeter..

Forcepoint

forcepoint.com/contact

Über Forcepoint

Forcepoint ist einer der weltweit führenden Anbieter von Cyber-Sicherheit im Bereich Anwender- und Datenschutz und hat es sich zur Aufgabe gemacht, Organisationen zu schützen und gleichzeitig die digitale Transformation und das Wachstum voranzutreiben. Die verhaltensbasierten 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.

[DLP-BROCHURE-DE] 3Nov2020