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

Datensicherheit ist heutzutage für Unternehmen jeglicher Art und Größe ein großes Problem. Auf der einen Seite sind IT-Organisationen verpflichtet, die Vorschriften einzuhalten und personenbezogene, identifizierbare Informationen (PII), geschützte Gesundheitsinformationen (PHI) und andere Arten regulierter Informationen vor gezielten böswilligen Angriffen sowie versehentlichem Datenverlust 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. Datensicherheitsteams müssen berücksichtigen, dass Daten heutzutage in rauen Mengen von „innerhalb" des Unternehmens an unterschiedliche Speicherorte und Kanäle verschoben werden. Daher ist die Transparenz aller Daten in der Cloud wie auch lokal gespeicherter Daten wichtig. Datensicherheitsteams müssen zudem volle Transparenz und Kontrolle über alle Kanäle (Endbenutzer, Internet-Traffic, Netzwerk, E-Mail, Cloud- und private Anwendungen) hinweg haben und diese zentral verwalten können.

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 Endbenutzer, 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, wo auch immer Ihre Mitarbeiter arbeiten und 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 DLP-Funktionen, die analysieren, wie Benutzer Daten verwenden, Ihre Mitarbeiter schulen, damit sie gute Datenentscheidungen treffen, und Vorfälle nach Risiko priorisieren.

Wichtige geschützte Kanäle

- **Benutzerdefinierte Anwendungen**
- **Cloud-Anwendungen**
- **Private Anwendungen**
- **Endpunkt**
- **Netzwerk**
- **Endpoint**
- **Discovery**
- **Web**
- **Email**

Einhaltung von Vorschriften beschleunigen

Mitarbeiter befähigen, Daten zu schützen

Erweiterte Erkennung und Kontrolle

Risiken begegnen und abwehren

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 für Endbenutzer, Cloud-Anwendungen und Netzwerke bereitstellen und verwalten. Forcepoint DLP beschleunigt Ihre Compliance-Bemühungen durch die Bereitstellung von über 1600 vordefinierten Klassifizierungen, Richtlinien und Vorlagen. Dies beschleunigt die anfängliche DLP-Bereitstellung und vereinfacht die laufende DLP-Verwaltung. Forcepoint DLP schützt vertrauliche Kundendaten und regulierte Daten effizient, sodass Sie die ordnungsgemäße Einhaltung aller Vorschriften jederzeit belegen können.

- → **Regulieren Sie die Abdeckung**, um ganz einfach die Konformität mit mehr als 1600 vordefinierten Vorlagen, Richtlinien und Klassifizierungen zu erfüllen und aufrechtzuerhalten, die den gesetzlichen Anforderungen von 83 Ländern und über 150 Regionen entsprechen.
- → **Auffinden und Klären** regulierter Daten mit Netzwerk-, Cloud- und Endpunktermittlung.
- → **Zentrale Kontrolle** und einheitliche Richtlinien über alle Kanäle hinweg, einschließlich Cloud- Endpunkte, Netzwerk, Internet und E-Mail.

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** 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.
- → **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, Gartner, 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** unter Verwendung hochgradig trainierter KI/ML-Modelle, um für die in Verwendung befindlichen Daten eine äußerst präzise Klassifizierung zu ermöglichen.

- → **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 unstrukturierter 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. 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 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.
- → **Erhöhen Sie das Bewusstsein der Mitarbeiter** für den Umgang mit sensiblen Daten und geistigem Eigentum durch Mitarbeitercoaching unter Windows und macOS und bieten Sie Mitarbeitern die Integration von Klassifizierungslösungen wie Forcepoint Data Classification und Microsoft Purview 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.
- → **Datenkontext hinzufügen** – für eine umfassendere Benutzeranalyse durch tiefgehende Integration in Forcepoint Risk-Adaptive Protection.

Umfassende Transparenz, sowohl für lokale Daten als auch Daten in der Cloud

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 CASB, SWG und ZTNA erweitert Analysen und DLP-Richtlinien auf kritische Cloud-Anwendungen, Web-Datenverkehr und webbasierte private Anwendungen, damit Ihre Daten geschützt sind, wo auch immer sie sich befinden. REST-APIs wie die Forcepoint DLP-App-Datensicherheits-API bieten Transparenz und DLP-Durchsetzung für interne, spezifisch entwickelte Anwendungen.

- → **Reaktionsteams ermöglichen, Daten zu identifizieren und zu schützen** – auch über Cloud-Anwendungen, Netzwerkdatenspeicher und verwaltete wie nicht 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, 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 einschließlich Fingerprinting und maschinellem Lernen auf Cloud-Anwendungen ausweitet und gleichzeitig Vorfälle und forensische Daten innerhalb des Rechenzentrums verwalten kann.
- → **Vorfälle in Drittanbieter-Tools** über bereitgestellte REST-APIs anzeigen und verwalten. Automatisieren Sie Vorfallsmanagement-Workflows und unterstützen Sie Geschäftsprozesse, die auf DLP-Vorfällen beruhen, durch Automatisierungs- und Service-Tools wie ServiceNow, Nagios und Tableau sowie SIEM/SOAR-Lösungen wie Splunk und XSOAR.

Forcepoint DLP bietet bei jeder Bereitstellung von einer Kontrollzentrale aus erweiterte Analyse- und Regulierungsrichtlinienvorlagen.

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 ONE CASB	Mit Unterstützung von Forcepoint ONE CASB können Sie die erweiterten Analysen und die Einzelkontrolle von Forcepoint DLP auf genehmigte Cloud-Anwendungen ausweiten, darunter Office 365, Salesforce, Box, Dropbox, Google Apps, Amazon AWS, ServiceNow, Zoom, Slack und viele mehr. Verschaffen Sie sich kontinuierliche Kontrolle über geschäftskritische Daten, unabhängig davon, wo sich Benutzer befinden oder welches Gerät sie verwenden.
Forcepoint ONE SWG	Forcepoint ONE SWG ermöglicht Ihnen den sicheren Zugriff auf jede Website oder das Herunterladen von Dokumenten und bietet Ihnen eine Hochgeschwindigkeits-Internet-Performance, auf die sich Ihr Team verlassen kann. Integration mit RBI bietet sichere Container-Renderings riskanter Websites und Zero Trust CDR für die vollständige Bereinigung aller herunterladbaren Dokumente.
Forcepoint ONE ZTNA (demnächst, 2. Hälfte 2023)	Forcepoint ONE ZTNA bietet einfachen, sicheren und skalierbaren Zero Trust Remote-Zugriff auf interne und private Cloud-Anwendungen ohne die Notwendigkeit eines VPNs über verwaltete und nicht verwaltete Geräte hinweg.
Forcepoint DLP —Discover	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. Analysen bieten Drip-DLP, um Diebstahl von einzelnen Datensätzen und anderes risikoreiches Benutzerverhalten 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. Im Gegensatz zu nicht Cloud-basierten Lösungen bietet Forcepoint DLP for Cloud Email ein enormes Skalierbarkeitspotenzial für unvorhergesehene starke Anstiege des E-Mail-Verkehrs. Zudem kann der ausgehende E-Mail-Verkehr problemlos mit Ihrem Unternehmen mitwachsen, ohne dass zusätzliche Hardwareressourcen konfiguriert und verwaltet werden müssen.
Forcepoint DLP-App-Datensicherheits-API	Die Forcepoint DLP-App-Datensicherheits-API macht es Unternehmen einfach, Daten in ihren internen benutzerdefinierten Anwendungen und Diensten zu schützen. Sie ermöglicht die Analyse von Datei- und Datenverkehr und erzwingt DLP-Aktionen wie Zulassen, Blockieren oder Bitten um Bestätigung mit einem personalisierten Pop-up, 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 auch sprachunabhängig und ermöglicht die Entwicklung und Verwendung in jeder Programmiersprache oder Plattform.

Anhang B: DLP-Lösungskomponenten im Überblick

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP-APP-DATENSICH-ERHEITS-API	FORCEPOINT ONE ZTNA (DEMNÄCHST 2H 2023)
Was ist die Haupt-funktion?	Datener-mittlung und Durch-setzung von Daten-schutz-richtlinien für Endbenutzer über Anwend-ungen, Internet, Druck, Wechselmedien-Kanäle hinweg, um nur einige zu nennen.	Ermitteln von Daten und Durchsetzen von Richtlinien in der Cloud oder in Cloud-Anwendungen	Ermittlung, Prüfung und Behebung von Daten im Ruhezustand in Rechenzentren und anderen On-Premise-Umgebungen	Transparenz und Kontrolle für Daten während der Übertragung über das Internet und über Internet-E-Mail im Netzwerk	Transparenz und Kontrolle für Daten während der Übertragung über ausgehende E-Mail	Transparenz und Kontrolle für Daten während der Übertragung über das Internet (nicht innerhalb des Netzwerks)	Transparenz und Kontrolle von Daten in internen benutzer-definierten Anwendungen und Diensten	Transparenz und Durchsetzung von Datenschutzbest-immungen fur Daten bei der Übertragung (Uploads und Downloads) innerhalb einer privaten Unternehmen-sanwendung
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 Netzwerk-speicher, 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, Drucker, Internet: HTTP(S) ICAP	Email	HTTP(S)	Interne benutzer-definierte Anwendungen und benutzer-definierte Dienste	Uploads und Downloads uber ZTNA Connector zu privaten Anwendungen
Wo werden Daten während der Nutzung geschützt?	Zoom, Webex, Google Hangouts IM, OIP-Dateiaustausch, M365-Teams-Austausch, Anwendungen (Cloud-Speicher-Clients), Betriebssystem-zwischenablage	Bei Aktivitäten zur Zusammenarbeit in Cloud-Anwendungen						

Anhang B: DLP-Lösungskomponenten im Vergleich

	FORCEPOINT DLP ENDPOINT	FORCEPOINT ONE CASB	FORCEPOINT DLP—DISCOVER	FORCEPOINT DLP—NETWORK	FORCEPOINT DLP FOR CLOUD EMAIL	FORCEPOINT ONE SWG	FORCEPOINT DLP-APP-DATENSICH-ERHEITS-API	FORCEPOINT ONE ZTNA (DEMNÄCHST 2H 2023)
Risk-Adaptive Protection	Add-on		Add-on	Add-on	Add-on	Add-on; derzeit unterstützt mit GRE/IPSec-Tunneln mit Forcepoint ONE SWG		
Optische Zeichener-kennung (OCR)			Inbegriffen	Inbegriffen	Inbegriffen			OCR-Unterstutzung fur DLPVerbesserung (2. Halfte 2023)
Integrationen Datenklass-ifizierung und -kennzeichnung	Forcepoint Data Classification und Microsoft Purview Information Protection.							
Für welche Daten ist Fingerprinting möglich?*	Strukturierte Daten (Datenbank), unstrukturierte Daten (Dokumente), binäre Daten (Nicht-Textdateien)							Verfügbar 2. Hälfte 2023
Einheitliche Richtlinien-verwaltung	Konfiguration und Durchsetzung von Richtlinien über eine einzige Konsole, von Endpunkten bis zu Cloud-Anwendungen							Verfügbar 2. Hälfte 2023
Zuverlässige Richtlinien-bibliothek	Erkennung und Durchsetzung von Richtlinien aus der umfassendsten Bibliothek in der Branche							

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/de, Twitter und LinkedIn.

[DLP-BROCHURE-DE] 18Aug2023