# Forcepoint DSPM

## Powered by GetVisibility

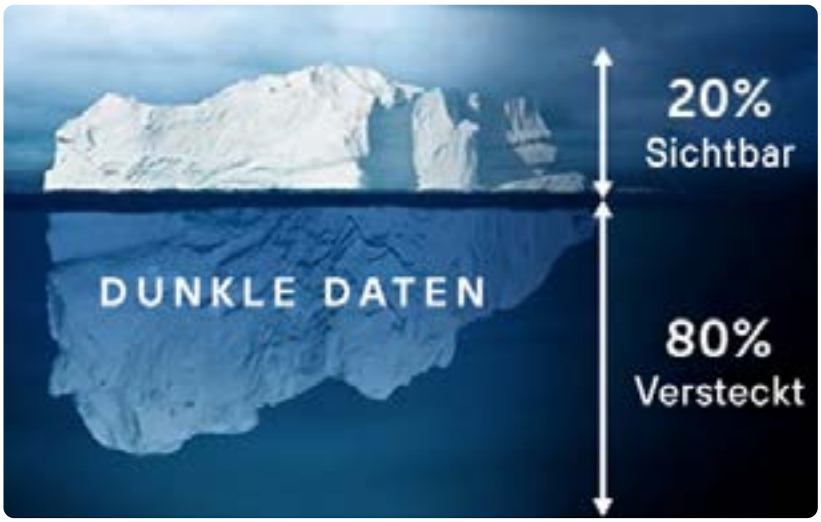
Forcepoint

Broschüre

# Die KI-Transformation ist die nächste Evolutionsstufe der digitalen Transformation

## Sind Ihre Daten in dieser neuen Ära sicher?

Die meisten Unternehmen, die sich der digitalen Transformation unterzogen haben, bereiten sich jetzt auf die nächste Evolution vor: die KI-Transformation. Diese neue Ära der KI wird von den vielen Vorteilen angetrieben, die GenAI-Anwendungen wie ChatGPT, Copilot, Gemini und andere bieten. Unternehmen haben aus ihren Erfahrungen mit der digitalen Transformation gelernt, dass Datensicherheit eine der obersten Prioritäten sein muss. Für viele Unternehmen sind Daten heute jedoch wie ein riesiger Eisberg, dessen Großteil unter der Oberfläche verborgen ist. Oft als „dunkle Daten" oder „Schattendaten" bezeichnet, bleiben sie unsichtbar und unbekannt, enthalten jedoch erhebliche Mengen sensibler Informationen, für die Unternehmen direkte Verantwortung tragen. Jetzt setzen sich Unternehmen mit der




Frage auseinander, wie sie Benutzern die Möglichkeit bieten können, GenAI-Anwendungen sicher zu nutzen, um die Produktivität und Effizienz zu steigern und gleichzeitig den Schutz ihrer sensiblen Daten zu gewährleisten.

DSPM (Data Security Posture Management) bietet einen umfassenden Ansatz zum Schutz Ihrer Informationen vor unbefugtem Zugriff, Offenlegung, Manipulation oder Datenvernichtung. Im Gegensatz zu anderen Arten von Datensicherheitsmethoden, die sich auf Systeme und Geräte konzentrieren, konzentriert sich DSPM auf die Gesamtheit der Daten eines Unternehmens selbst, um die Einhaltung der Compliance zu gewährleisten und das Risiko von Datenschutzverletzungen zu mindern.


Laut IDC sind 80 % der Daten weltweit unstrukturiert und 90 % dieser Daten sind nicht analysiert und werden auch als „dunkle Daten" bezeichnet[1]


94 % der Unternehmen speichern Daten in mehreren Cloud-Umgebungen[2]

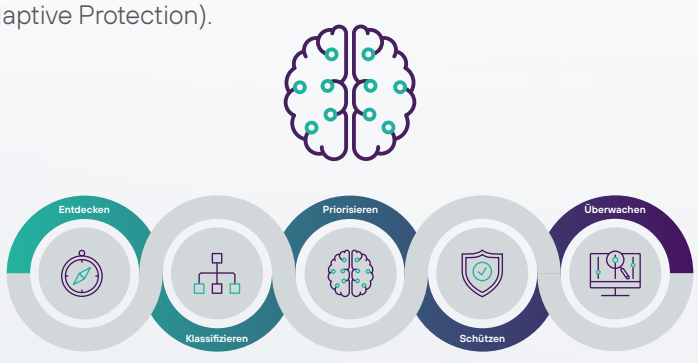

Equifax legt Klage in Höhe von 1,4 Mrd. US-Dollar wegen seiner Datenschutzverletzung[3] bei, verschärft durch Hacker, die auf ein gemeinsames Laufwerk zugreifen, auf dem mehrere Kopien von Benutzernamen und Passwörtern von Mitarbeitern gespeichert sind. Dem Unternehmen fehlten Tools zur Erkennung und Identifizierung redundanter und veralteter Dateien.

1 Das Rätsel der unsichtbaren Daten, Forbes, Februar 2022
2 Dunkle Daten: Das unbekannte Sicherheits- und Datenschutzrisiko der Cloud, Forbes, Juni 2023
3 Equifax stimmt Vergleich über 1,38 Mrd. US-Dollar im Rechtsstreit über Datenschutzverletzung zu Finextra, Januar 2020

## Worauf zielt DSPM ab?

- **Weg zur KI-Transformation:** Entfesseln Sie das Potenzial von KI mit Forcepoint DSPM und schützen Sie Ihre Daten überall mit unserer fortschrittlichen KI Mesh-Technologie. Mit der zentralen Transparenz von Forcepoint DSPM und der Kontrolle von Forcepoint ONE Data Security schützen wir Ihre sensiblen Informationen über wichtige Kanäle hinweg, einschließlich GenAI-Apps wie ChatGPT, Copilot, Gemini und viele andere. So werden mutige Innovationen bei gleichzeitiger Steigerung der Produktivität und Reduzierung von Risiken möglich.
- **Identifizierung sensibler Daten:** DSPM hilft Unternehmen dabei, sensible Daten in mehreren Cloud-Umgebungen und -Diensten sowie an lokalen Standorten zu identifizieren. Dazu gehört das Wissen, wo sich sensible Daten befinden, wie auf sie zugegriffen wird und wer die Berechtigungen hat, mit ihnen zu interagieren.
- **Bewertung von Schwachstellen und Risiken:** DSPM bewertet die Anfälligkeit sensibler Daten für Sicherheitsbedrohungen und das Risiko der Nichteinhaltung von Vorschriften. Durch die Analyse der Datensicherheitslage können Unternehmen potenzielle Risiken proaktiv angehen.
- **Konzentration auf Daten an der Quelle:** Im Gegensatz zu anderen Datensicherheitstools, die in erster Linie Geräte, Systeme und Anwendungen schützen, konzentriert sich DSPM direkt auf den Schutz der gesamten Daten eines Unternehmens. Ziel ist es, Datenschutzverletzungen zu verhindern und die Einhaltung der Compliance zu gewährleisten, indem die Daten im Kern geschützt werden.
- **Abzielen auf dunkle Daten und ROT-Daten:** DSPM zielt direkt auf dunkle Daten ab (Daten, die derzeit nicht in normalen Geschäftsprozessen gesehen oder verwendet werden). In ähnlicher Weise kann DSPM auf ROT-Daten (redundant, veraltet und trivial) abzielen, die ebenfalls dazu neigen, sich in Unternehmen anzuhäufen. Unternehmen speichern aus verschiedenen Gründen nach wie vor große Mengen von Daten, weil sie denken, dass es ihnen bei der Einhaltung der Compliance helfen wird. Dadurch entstehehn sogar noch größere Datenrisiken, und DSPM hilft dabei, dieses Risiko zu managen.
- **Abzielung auf überberechtigte/überexponierte Daten:** Aufgrund der Art und Weise, wie Daten durch das Kopieren und Bearbeiten neuer Versionen von Daten vermehrt werden, können sich auch Datenberechtigungen oft auf Benutzer, Gruppen und sogar das gesamte Unternehmen ausweiten. DSPM hilft dabei, das „Prinzip der geringsten Rechte" oder Zero Trust-Konzept durchzusetzen, das überberechtigte Daten stark reduziert, um Datenschutzverletzungen zu verhindern.
- **Multi-Cloud- und hybride Cloud-Umgebungen:** Während Unternehmen Multi-Cloud- und hybride Cloud-Umgebungen einführen, steigt das Risiko von Datenschutzverletzungen erheblich. DSPM bietet Transparenz und Kontrolle über sensible Daten in diesen verschiedenen Computing-Umgebungen sowie über lokale Standorte.

**Forcepoint DSPM** wurde für das moderne Unternehmen entwickelt, das eine starke Transparenz und Kontrolle seiner Geschäftsdaten benötigt. Es bietet Transparenz in allen verschiedenen Cloud-Umgebungen und Servern, um Datenschutzverletzungen zu verhindern und das Risiko der Nichteinhaltung von Datenschutzbestimmungen zu reduzieren. Forcepoint bietet vollständige Transparenz und Kontrolle über den gesamten Datenlebenszyklus und sorgt überall für Datensicherheit, indem es die **proaktive Erkennung von Datenrisiken (DSPM)** mit **aktiven Kontrollen über die Verwendung** von Daten (DLP und SSE) **kombiniert und sich gleichzeitig kontinuierlich an die Handlungen jedes Benutzers anpasst** (Risk-Adaptive Protection).




KI-gestützte Erkennung, Klassifizierung und Orchestrierung

# Vereinheitlichen Sie die Transparenz und Kontrolle über Ihre Datenlandschaft mit Forcepoint DSPM

Die Verwaltung und Sicherung der Daten Ihres Unternehmens waren noch nie so komplex wie heute. Forcepoint DSPM bietet eine leistungsstarke Lösung, um unabhängig vom Standort umfassende Transparenz und Kontrolle über Ihre Daten zu gewinnen. Forcepoint DSPM bietet Ihnen mit branchenführenden Erkennungsgeschwindigkeiten und erweiterten AI Mesh Data Classification-Funktionen die Möglichkeit, fundierte Entscheidungen über Ihre Datensicherheitslage zu treffen und potenzielle Risiken proaktiv anzugehen.

## Zu den wichtigsten Vorteilen von Forcepoint DSPM gehören:

**Schnelle, umfassende Erkennung:** Forcepoint DSPM ist in der Lage, Dateien über mehrere Clouds und vor Ort hinweg zu scannen. Es ist nicht ungewöhnlich, dass Unternehmen viele Terabytes und sogar einige Petabytes an Daten haben, und sehr große Unternehmen haben sogar Exabytes an Daten, für die sie verantwortlich sind. Mit leistungsstarker Erkennung ermöglicht Forcepoint Unternehmen einen schnellen Überblick über Daten in einer riesigen Datenlandschaft, einschließlich ChatGPT Enterprise. Im Gegensatz zu anderen DSPM-Anbietern erhebt Forcepoint keine Gebühren für Discovery-Scans – Kunden können Discovery-Scans so oft wie gewünscht und ohne zusätzliche Kosten durchführen.

**KI Mesh ermöglichte Genauigkeit:** Forcepoint DSPM erkennt Daten in Cloud- und Netzwerkquellen und klassifiziert diese Daten automatisch unter Verwendung einer erweiterten KI-Klassifizierungs-Engine. AI Mesh von Forcepoint DSPM ermöglicht Unternehmen bei der Data Classification eine überragende Genauigkeit. Seine vernetzte KI-Architektur, die ein GenAI Small Language Model (SLM) und erweiterte Daten- und KI-Komponenten verwendet, erfasst effizient den Kontext von unstrukturiertem Text. Dank seiner Anpassbarkeit und Effizienz gewährleistet es eine schnelle, genaue Klassifizierung ohne umfassende Schulung, was wiederum das Vertrauen und die Compliance verbessert. Letztendlich bot diese hohe Genauigkeit Unternehmen, die Probleme mit anderen gängigen Klassifizierungsmethoden hatten, die Möglichkeit, falsch positive/negative Ergebnisse erheblich zu reduzieren, ihr geistiges Eigentum erfolgreich zu schützen und große Mengen an Zeit und Ressourcen einzusparen.

**Data Visibility in Ihrer Datenlandschaft:** Forcepoint DSPM bietet Ihnen die Möglichkeit, Berechtigungen für alle Dateien und Benutzer zu überprüfen. Datenadministratoren können sehen, welche Personen im gesamten Unternehmen Zugriff auf eine Datei oder Fileshares haben. Mit einem einzigen Klick können Sie die Berechtigungen für alle Dateien, die gescannt werden, sofort anzeigen. Forcepoint DSPM bietet Berichte in Echtzeit zusammen mit einem Dashboard mit umfangreichen Details, die einen Überblick über dunkle Daten aus der Vogelperspektive geben, sowie eine Übersichtsdatenrisikobewertung bieten, die Ihnen dabei hilft, die Bereiche mit dem höchsten Datenrisiko zu erkennen.

**Workflow-Orchestrierung:** Definieren Sie auf einfache Weise die Eigentümerschaft und die Verantwortlichkeit für verschiedene Datensätze, um den Prozess der Abstimmung zwischen den Beteiligten zu rationalisieren. Dadurch werden effizientere Workflows um Handlungen ermöglicht, die an jeder Datenquelle und jeder Ressource durchgeführt werden. Eine wirksame Behebung erfordert ein breites Engagement und die Zusammenarbeit über die Sicherheitsorganisation hinaus mit der CDO/Governance, Risk und Compliance (GRC) Gruppe sowie mit Funktionen wie Marketing, Finanzen, DevOps und vielen anderen. Forcepoint DSPM betrachtet die Sicherung der Datenlage nicht nur als ein Sicherheitsthema, sondern als eine Geschäftspriorität.

# Lassen Sie nicht zu, dass Datenrisiken Ihr Unternehmen lähmen. Forcepoint kann Ihnen helfen

Im heutigen digitalen Zeitalter sind Daten das wertvollste Gut eines Unternehmens, können aber auch eine erhebliche Belastung darstellen, wenn sie nicht ordnungsgemäß verwaltet werden. Forcepoint DSPM bietet einen proaktiven Ansatz für die Sicherung Ihrer sensiblen Daten, die Minderung der Risiken von Datenschutzverletzungen und die Einhaltung von Vorschriften. Durch die Implementierung von Forcepoint DSPM können Sie einen umfassenden Einblick in Ihre Datenlandschaft erhalten, Schwachstellen erkennen und beheben und Ihr Unternehmen proaktiv vor finanziellen Schäden und Rufschädigung schützen, die durch Datenschutzverletzungen und Nichteinhaltung von Vorschriften verursacht werden können und gleichzeitig Ihre Daten in GenAI-Anwendungen schützen. Übernehmen Sie noch heute die Kontrolle über Ihre Datensicherheit. Erkunden Sie, wie DSPM Ihre wertvollen Informationen schützen kann. Gehen Sie auf www.forcepoint.com/de/dspm um eine Demo anzufordern, oder melden Sie sich für eine kostenlose Datenrisikobewertung an, in der ein Sicherheitsingenieur Ihnen einen Beispiellauf Ihrer eigenen Daten bieten kann, um zu sehen, welchen Arten von Datenrisiken Sie derzeit ausgesetzt sind.

Forcepoint

**forcepoint.com/contact**

## Über Forcepoint

Forcepoint vereinfacht die Sicherheit für globale Unternehmen und Behörden. 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 im texanischen Austin schafft sichere, vertrauenswürdige Umgebungen für Kunden und ihre Mitarbeiter in mehr als 150 Ländern. Interagieren Sie mit Forcepoint auf www.forcepoint.com, Twitter und LinkedIn.