Forcepoint

Datenblatt

Forcepoint Data Security Posture Management

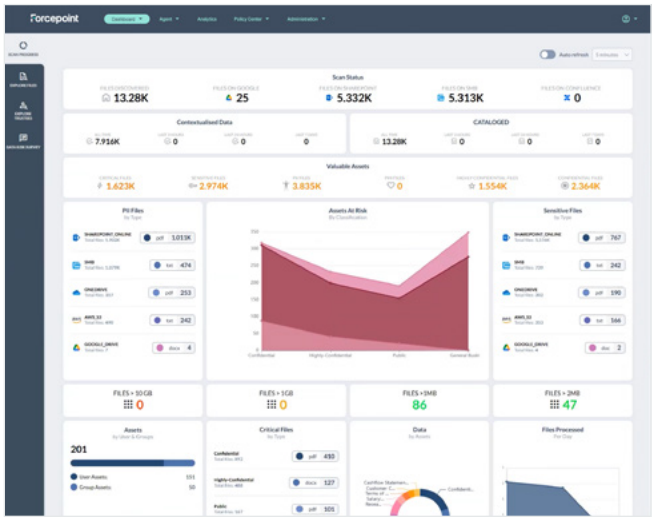
Hauptmerkmale und Vorteile:

- **AI-Mesh-Klassifizierung –** Hochpräzise und effiziente Klassifizierung durch GenAI, Predictive AI und Data-Science-Fähigkeiten.
- **Schnelle Erkennung –** Führen Sie so oft Sie möchten Forcepoint DSPM in der Cloud und an Speicherorten vor Ort aus.
- **Echtzeit-Risikobewertung–** Überprüfen Sie Zugriffsberechtigungen und andere Datenrisiken.
- **Workflow-Orchestrierung –** Implementieren Sie Geschäftsprioritäten für Stakeholder.

Die digitale Transformation hat sich zur KI-Transformation entwickelt, die durch die Integration von KI-Technologien, insbesondere von GenAI-Anwendungen, in Geschäftsprozesse angetrieben wird. In Verbindung mit der Datenausdehnung aus Unternehmen, die Anwendungen und Daten von lokalen Servern in die Cloud migrieren und GenAI-Tools wie ChatGPT, Copilot und Gemini verwenden, stehen sie vor dem anhaltenden Problem, zu verfolgen, wo sich ihre sensiblen Daten befinden, wer darauf zugreifen kann und wie sie verwendet werden. Das exponentielle Wachstum von „dunklen Daten", die sich in Cloud-basierten Repositories verbergen oder auf einzelne Geräte und jetzt Anwendungen der GenAI verteilen, stellt ein erhebliches Risiko dar. Es wird geschätzt, dass bis zu 80 Prozent der Daten eines Unternehmens in diesem obskuren „dunklen" Zustand vorhanden sind und sich der traditionellen Aufsicht entziehen.

Die Konsequenzen aus einer derartig obskuren Datenlandschaft sind kritisch. Ohne klare Transparenz und Verwaltung sind Unternehmen erhöhten Risiken von Sicherheitsverletzungen ausgesetzt mit potenziell verheerenden Folgen für kommerzielle, gemeinnützige Organisationen und staatliche Sektoren. Im Zeitalter der digitalen Transformation von heute war es noch nie so überaus wichtig, die Kontrolle über sensible Informationen zurückzugewinnen.

Forcepoint DSPM erkennt und klassifiziert sensible Daten in großem Umfang – sowohl strukturierte als auch unstrukturierte Daten. Das einzigartige AI Mesh liefert Geschwindigkeit und Nachvollziehbarkeit durch eine hochoptimierte Small Language Model (SLM)-Architektur. Dieses AI Mesh ermöglicht zudem individuelle Anpassungen ohne umfangreiches Retraining der Modelle und stellt eine schnelle, präzise Klassifizierung sicher – für mehr Vertrauen und Compliance.

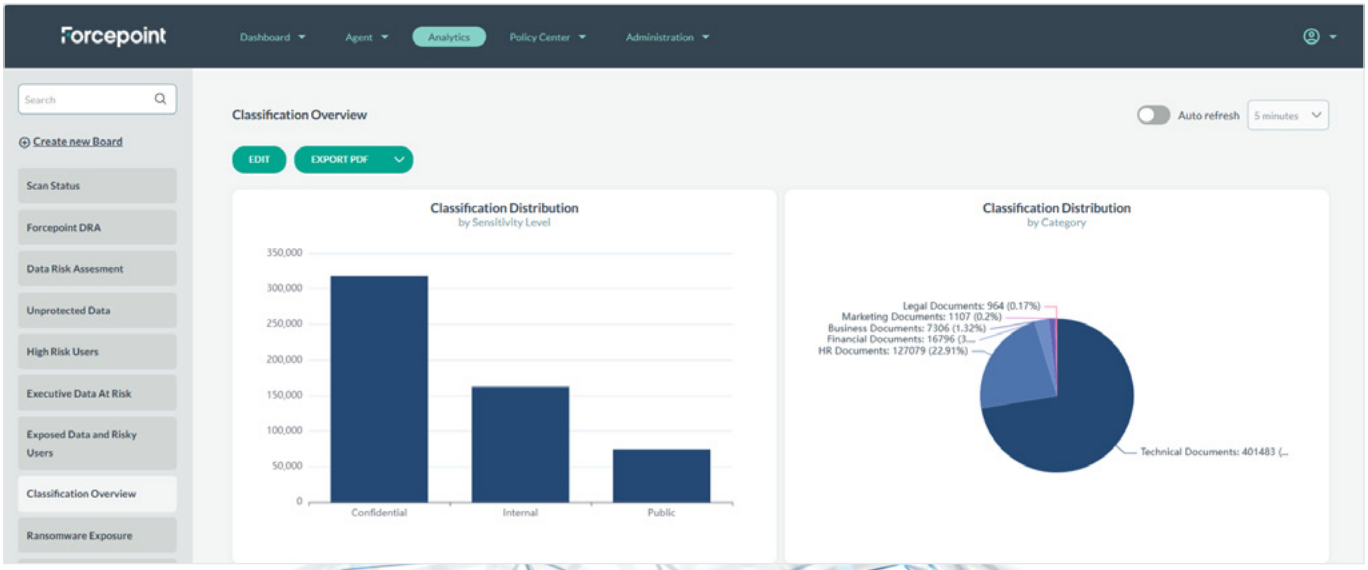


Schnelle, umfassende Erkennung

Mit einer Vielzahl an Konnektoren findet Forcepoint DSPM sensible Daten effizient in unterschiedlichsten Speicherumgebungen – ob in der Cloud oder On-Premises, ob strukturierte oder unstrukturierte Daten. Es scannt über zentrale Plattformen wie Amazon (AWS S3 und IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) und Google (Google Drive und IAM) hinweg sowie über lokale LDAP- und SharePoint-Systeme.

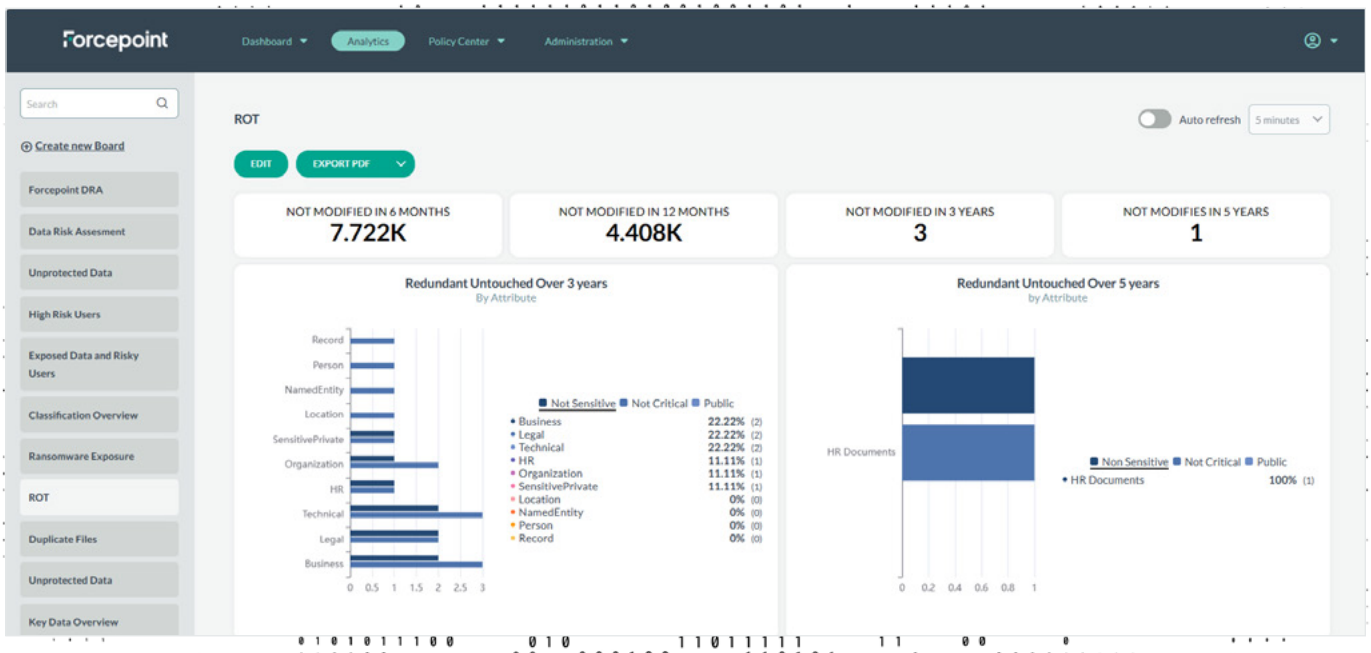
KI Mesh ermöglichte Genauigkeit

Die AI-Mesh-Funktionen von Forcepoint DSPM ermöglichen Unternehmen eine überragende Genauigkeit bei der Datenklassifizierung. Im Gegensatz zu anderen DSPM-Lösungen bietet sie eine Multi-Node- und vernetzte KI-Architektur, die ein GenAI-SLM sowie ein Netzwerk aus fortschrittlichen Daten- und KI-Komponenten nutzt. Diese Struktur erfasst Kontext äußerst effizient und wandelt Text in präzise Dokumentklassifizierungen um. Das AI Mesh ist anpassbar und lässt sich auf Branchenanforderungen sowie regulatorische Vorgaben abstimmen. Es läuft effizient auf Standard-Compute-Ressourcen, ohne GPUs zu benötigen, und liefert dennoch eine leistungsstarke Klassifizierung. Die hohe Genauigkeit wird ohne umfangreiches ML-Training erreicht, was die Wartungskosten reduziert. Die Nachvollziehbarkeit des AI Mesh stärkt Vertrauen und Compliance und stellt eine hochsichere Datenhaltung sowie die Einhaltung von Datenschutzvorschriften sicher.



Leistungsüberwachung und Datenrisikobewertung

Da Forcepoint DSPM Daten scannt und erkennt, liefert es detaillierte Informationen wie die Anzahl der intern freigegebenen Dateien mit kritischen Informationen, die Menge der gefährdeten PII-Dateien und die Anzahl der redundanten, veralteten und trivialen Datendateien (ROT).



Workflow-Orchestrierung

Optimieren Sie die Datensicherheits-Governance mühelos mit Forcepoint DSPM. Seine intuitive Workflow-Orchestrierung gewährleistet eine effiziente Verfolgung der Dateneigentümer und -verantwortlichkeit. Durch die Aufschlüsselung von Silos und die Erleichterung der Zusammenarbeit zwischen Stakeholdern werden die Verantwortlichkeiten entsprechend verteilt, die betriebliche Effizienz verbessert und die Klarheit im gesamten Unternehmen verbessert.

Die Implementierung einer robusten DSPM-Lösung ist entscheidend für Unternehmen, die ihre Datenlage sichern und sensible Informationen in der Cloud und an lokalen Datenspeicherorten schützen möchten. Durch die Verwendung von Forcepoint DSPM können Unternehmen die Produktivität steigern, indem sie die Zuverlässigkeit des Datenzugriffs und der Datenfreigabe verbessern, Innovationen fördern und die Zusammenarbeit fördern. Gleichzeitig können sie Risiken minimieren, indem sie eine unsachgemäße Verwendung sensibler Daten proaktiv erkennen und beheben und so Datenschutzverletzungen verhindern. Letztendlich können Unternehmen die Compliance-Bemühungen optimieren, indem sie in allen Umgebungen eine echte Transparenz und Kontrolle über sensible Daten erhalten.

Robuste Erkennung

FUNKTIONS-	VORTEIL
Schnelle Erkennung und Katalogisierung	Es arbeitet über mehrere Datenquellen hinweg, um größere Datenmengen pro Sekunde bzw. pro Stunde zu scannen, und fasst Details zu unstrukturierten und strukturierten Datenbeständen zusammen – aufbereitet in einem leicht verständlichen Format.
Verbindet mit wichtigen Datenquellen	Verbindet sich mit wichtigen Datenquellen: Bietet durch eine Vielzahl an Datenquellen-Konnektoren eine robuste Transparenz über unstrukturierte und strukturierte Daten.
Überexponierte Datenanalyse	Identifizieren Sie überexponierte Daten, die öffentlich geteilt, extern mit Dritten geteilt und intern exzessiv geteilt werden.
Berechtigungen anzeigen und beheben	Sehen Sie den Zugriff für jede Datei und beheben Sie dies, um das Zero-Trust-Prinzip (POLP) zu etablieren.
Eliminieren Sie Risiken aufgrund von ROT-Daten (redundant, veraltet, trivial)	Identifizieren und beseitigen Sie Dateien, die redundant, veraltet oder trivial (ROT) sind.
Transparenz in Zugriff und Berechtigungen	Die Integrationen in Active Directory und andere IRM-Lösungen verbessern die Zugriffssicherheit innerhalb von Unternehmen.

KI Mesh Data Classification

FUNKTIONS-	VORTEIL
AI Mesh-Klassifizierung von unstrukturierten und strukturierten Daten	Hochgenaue KI-Klassifizierung für unstrukturierte und strukturierte Daten.
Benutzerdefiniertes Modell-Training	Unternehmen können das AI Mesh-Modell an individuelle Datenanforderungen (z. B. IP, Geschäftsgeheimnisse usw.) anpassen, um eine hochgenaue Datenklassifizierung zu ermöglichen und DSPM- und DLP-False-Positives/-Negatives zu reduzieren.
Kann Tags dem Microsoft Purview IP-Tagging zuordnen.	Bietet eine zusätzliche Ebene der Klassifizierungsgranularität und ergänzt die MIP-Tags. Kann MIP-Tagging korrigieren.
Daten-Tagging	Taggt alle gescannten und klassifizierten Dateien mit persistenten Labels, die von DLP mit Standard-Tagging (klassifiziert, hoch klassifiziert, öffentlich) sowie geschäftlichem Katalogisieren/Tagging (HR, Marketing, Finance, Devops – mit Sub-Tags wie Lebensläufen, POs usw.) lesbar sind.
Integration in Forcepoint DLP	Kann in Forcepoint DLP integriert werden, um DSPM AI Mesh-Tagging von Dateien (Klassifizierung) zu nutzen, um starke Richtlinien gegen diese zu erstellen.

Echtzeit-Überwachung und Datenrisikobewertung

FUNKTIONS-	VORTEIL
Datenrisikobewertungen (DRA)	Kostenlose Datenrisikoanalysen sind verfügbar, um die aktuelle Datensicherheitslage eines Unternehmens in mehreren Kategorien zu analysieren.
Detailliertes interaktives Dashboard	Sehen Sie umfassende Details zu Dateien und Datenbanken in einer einzigen Lösung. Mit Drilldown von wichtigen Dateiinformationen, wie Risikostufe, Berechtigungen und Speicherort (IP-Adresse, Pfad).
Reporting-Funktion	Generieren Sie Berichte, die sowohl die allgemeine Compliance-Bereitschaft als auch spezifische Datenschutzbestimmungen zeigen.
Erweitertes Warnsystem	Bietet ausgefeilte Datenkontrollen und Warnmeldungen, die während Scans auf Anomalien oder potenzielle Sicherheitsverletzungen gefunden werden.
Suche nach Data Subject Access Request (DSAR)	Vereinfachen Sie die Erstellung eines DSAR, um Anforderungen der Datenschutzverordnung schnell zu erfüllen.
Analytics-Suite	Erleben Sie eine erweiterte Analyse-Suite für einfachen Zugriff auf Sicherheits- und Klassifizierungsinformationen auf einen Blick. Wählen Sie aus verschiedenen vordefinierten Dashboards oder erstellen Sie Ihre eigenen, und exportieren Sie PDF-Snapshots mühelos mit nur einem Klick. Zu den vordefinierten Dashboards gehören Überexposition und Ransomware-Analyse, kritische Datenduplizierung, Erkennung riskanter Benutzer, Datenaufbewahrung, falsch platzierte Daten, Datenrisikobewertung, Souveränität, Vorfallverfolgung bei Verstößen gegen die Datenkontrolle und vieles mehr.
Ransomware-Expositionsanalyse	Identifizieren Sie kritische Daten, die einem Ransomware-Angriff ausgesetzt sein könnten.
Reporting- und Analyse-Builder ohne Code	Erstellen Sie ganz einfach benutzerdefinierte Anwendungsfälle und Analyseberichte, ohne dass Programmierkenntnisse erforderlich sind.
Riskante Benutzeridentifikation	Identifizieren Sie Benutzer mit erhöhten Risikoprofilen, die Zugriff auf erhebliche Mengen kritischer Informationen haben.
Datenkontrollvorfall	Bietet einen klaren Überblick über alle Verstöße gegen die Datenkontrolle und den Status der Vorfalllösung.