Forcepoint

Datenblatt

Forcepoint Data Security Posture Management

Hauptmerkmale und Vorteile:

- **KI Mesh und ML –** Die KI Mesh-Katalogisierung bietet eine unübertroffene Genauigkeit und Effizienz und wird durch maschinelles Lernen für laufende Verbesserungen kontinuierlich weiterentwickelt.
- **Schnelle Erkennung –** Führen Sie so oft Sie möchten Forcepoint DSPM in der Cloud und an Speicherorten vor Ort aus.
- **Echtzeit-Überwachung und 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, Co-pilot 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.

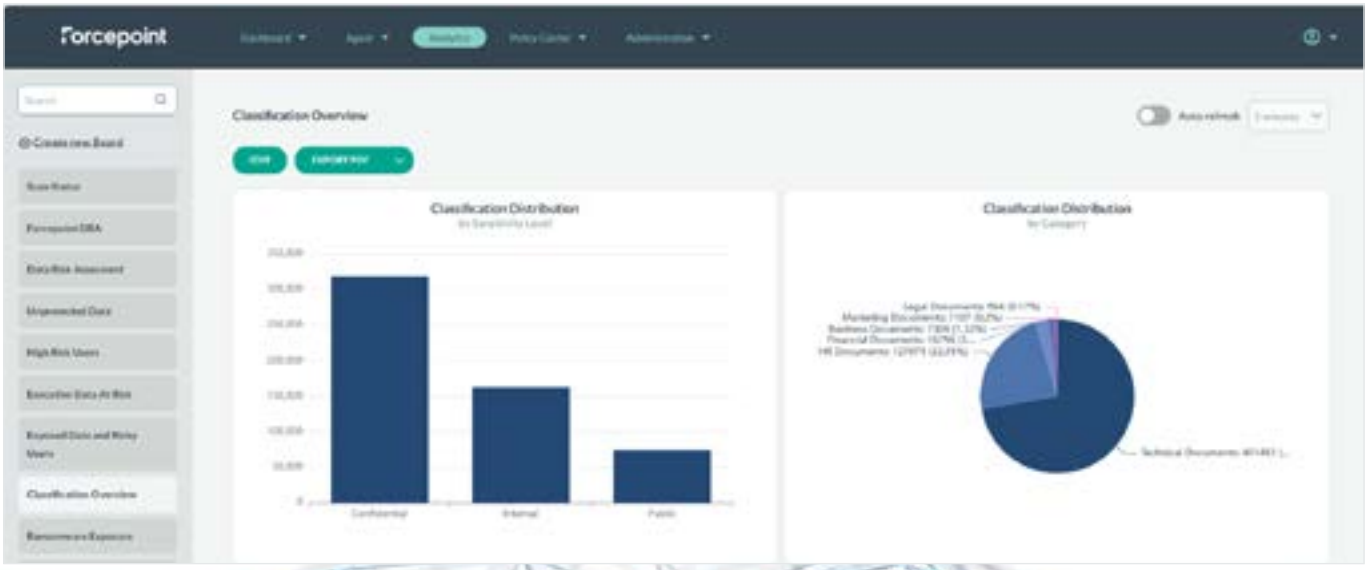
KI Mesh von Forcepoint DSPM ermöglicht Unternehmen eine überragende Genauigkeit der Datenklassifizierung. Seine vernetzte KI-Architektur, die ein GenAI Small Language Model (SLM) und erweiterte Daten- und KI-Komponenten verwendet, erfasst effizient den Kontext von unstrukturiertem Text. Dank seiner Anpassbarkeit und Effizienz gewährleistet es eine schnelle, genaue Klassifizierung ohne umfassende Schulung, was wiederum das Vertrauen und die Compliance verbessert.

Schnelle, umfassende Erkennung

Mit einer Vielzahl von Konnektoren lokalisiert Forcepoint DSPM effizient sensible Daten in verschiedenen Speicherumgebungen, ob in der Cloud oder vor Ort, und scannt etwa eine Million Dateien pro Stunde auf wichtigen Plattformen wie Amazon (AWS S3 und IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) und Google (Google Drive und IAM) sowie lokalen LDAP- und SharePoint-Systemen.

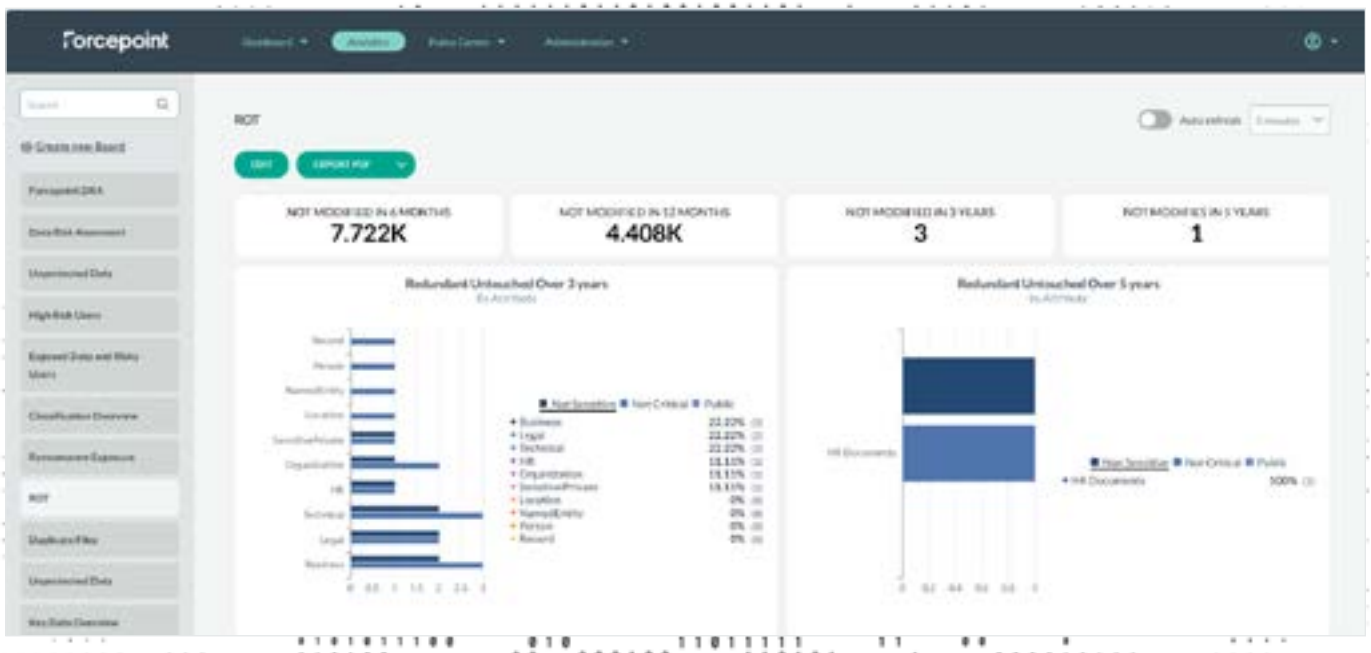
KI Mesh ermöglichte Genauigkeit

Die KI Mesh-Funktion von Forcepoint DSPM zeichnet sich dadurch aus, dass sie heutigen Unternehmen eine überragende Genauigkeit der data classification bietet. Im Gegensatz zu anderen DSPM-Lösungen, Es bietet eine vernetzte KI-Architektur mit mehreren Knotenpunkten, Nutzung eines GenAI SLM und eines Netzwerks von fortschrittlichen Daten und KI-Komponenten. Diese Struktur erfasst effizient den Kontext und wandelt unstrukturierten Text in präzise Dokumentenklassifikationen um. Das KI-Mesh ist anpassbar und auf die Branchenanforderungen und regulatorische Umgebungen zugeschnitten. Es läuft effizient auf Standard-Rechenressourcen ohne GPUs und bietet eine hohe Leistungsbewertung. Eine hohe Genauigkeit wird ohne umfassendes ML-Training erreicht, was die Wartungskosten senkt. Die Erklärbarkeit des AI Mesh verbessert das Vertrauen und die Compliance, gewährleistet eine hochsichere Datenhaltung und die Einhaltung der Datenschutzbestimmungen.



Echtzeit-Überwachung 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 für Unternehmen von entscheidender Bedeutung, die ihre Datenbasis optimieren 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 wird auf mehreren Quellen ausgeführt, um größere Dateimengen pro Sekunde/Stunde zu scannen und Details über unstrukturierte Datenressourcen zu synthetisieren und sie in einem leicht verdaulichen Format zu organisieren.
Umfangreiche Datenquellen-Konnektoren	Robuste Transparenz für stärker unstrukturierte Daten durch das Angebot einer Vielzahl von Datenquellenkonnektoren.
Überexponierte Datenanalyse	Identifizieren Sie überexponierte Daten, die öffentlich geteilt, extern mit Dritten geteilt und intern exzessiv geteilt werden.
Einblick in Berechtigungen für jede einzelne unstrukturierte Datendatei	Sehen Sie sich den individuellen Benutzerzugriff auf einzelne Dateien und die Benutzer mit Zugriff auf die meisten Dateien an.
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
KI Mesh- und ML-Klassifizierung vorhandener unstrukturierter Daten	Hochgenaue Klassifizierungsvorschläge werden für vorhandene unstrukturierte Daten empfohlen, die gescannt werden.
Benutzerdefiniertes Modell-Training	Unternehmen können das KI Mesh-Modell auf die spezifischen Datenanforderungen (z. B. IP, Geschäftsgeheimnisse usw.) zuschneiden und im Laufe der Zeit durch maschinelles Lernen verbessern für größere Genauigkeit.
Kann Tags dem Microsoft Purview IP-Tagging zuordnen.	Bietet eine zusätzliche Ebene der Klassifizierungsgranularität und ergänzt die MPIP-Tags. Kann MPIP-Tagging korrigieren.
Daten-Tagging	Die Optimierung des DLP-Rollouts verbessert die DLP-Effizienz, indem alle gescannten und klassifizierten Dateien mit Labels versehen werden, die von DLP mit typischen Tags (klassifiziert, hoch klassifiziert, öffentlich) gelesen werden können, sowie die Katalogisierung/Tagging von Unternehmen (HR, Marketing, Finanzen, DevOps - mit Unter-Tags wie Lebensläufen, POs usw.) gekennzeichnet werden.
Integration in Forcepoint DLP	Kann integriert werden, um DSPM KI Mesh-Tagging von Dateien (Klassifizierung) zu verwenden, um dagegen starke Richtlinien zu erstellen.

Echtzeit-Überwachung und Datenrisikobewertung

FUNKTIONS-	VORTEIL
Datenrisikobewertungen (DRA)	Kostenlose Datenrisikobewertungen sind verfügbar, um die aktuelle Datenrisikosituation eines Unternehmens in mehreren Kategorien zu analysieren.
Detailliertes interaktives Dashboard	Zeigen Sie umfassende Dateidetails auf einem Bildschirm an. Drilldown für wichtige Dateidaten wie Risikoniveau, Berechtigungen und Standorte (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 Generierung eines DSAR, um Anforderungen von Datenschutzbestimmungen schnell zu erfüllen.
Analytics-Suite	Erleben Sie eine erweiterte Analyse-Suite für einfachen Zugriff auf Sicherheits- und Klassifizierungseinblicke 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 und Vorfallverfolgung bei Verstößen gegen die Datenkontrolle.
Ransomware-Expositionsanalyse	Identifizieren Sie kritische Daten, die einem Ransomware-Angriff ausgesetzt sind.
Reporting- und Analyse-Builder ohne Code	Leichte Erstellung benutzerdefinierter Anwendungsfälle und Analyse-Berichte ohne Codierung.
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.

Workflow-Orchestrierung

FUNKTIONS-	VORTEIL
Dateneigentümer	Definiert mit Leichtigkeit die Verantwortlichkeit und erreicht Stakeholder-Ausrichtung.
Task-Manager	Weist Datenverwaltern und -eigentümern Aufgaben zu und ermöglicht die Verfolgung von DSPM-Statistiken (wie offene, gelöste und geschlossene Tickets, Auflösungszeit).