proofpoint.

KURZVORSTELLUNG

Proofpoint Data Security Posture Management

Erkennung und Schutz für Daten in SaaS-Plattformen, Cloud-Infrastrukturen und lokalen Umgebungen

Wichtige Vorteile

- **KI-Klassifizierer** identifizieren vertrauliche und unternehmensspezifische Daten in lokalen, SaaS- und Cloud-Umgebungen, ohne manuelle Regeln zu erfordern
- **Data Risk Map** priorisiert Risiken anhand von Datenvertraulichkeit, Zugriffsrechten, geschäftlichen Auswirkungen und Datenbewegungen
- **Geschäftsorientierte Zugriffskontrolle** optimiert direkte und delegierte Behebungsmaßnahmen sowie die Erstellung von DLP-Richtlinien
- **Integrierte KI-Datensicherheit** identifiziert vertrauliche Daten, auf die KI-Anwendungen und KI-Trainingspipelines Zugriff haben
- **Compliance-Dashboards** verfolgen die Einhaltung anhand von über 25 Frameworks mit entscheidungsrelevanten Berichten
- **Einheitliche Datensicherheit** teilt Informationen mit DSPM, Zugriffskontrolle, DLP und Datensicherheit für KI

Rasante Zunahme von Unternehmensdaten

Der Aufstieg von KI, DBaaS-Plattformen (Database-as-a-Service) und Cloud-Speicher beschleunigt die Datenausbreitung in lokalen, Software-as-a-Service (SaaS)-, Cloud-Umgebungen. Da vertrauliche Daten über verschiedene Systeme und Pipelines verteilt sind, fällt es den Teams schwer, den Überblick darüber zu behalten, wo sich all diese Daten befinden. Dies führt zu blinden Flecken, erhöht das Kompromittierungsrisiko und erschwert die Einhaltung von Vorschriften.

Unkontrollierte Datenzugriffe durch Anwender und KI

Die Ausbreitung von Daten wird dadurch verschärft, dass kaum kontrolliert werden kann, wer – und was – Zugriff auf vertrauliche Informationen hat. Anwender mit zu umfassenden Zugriffsrechten, nicht autorisierte Tools und riskante Freigaben erhöhen das personenbezogene Risiko. Gleichzeitig eröffnen KI-Modelle, Agenten und automatisierte Arbeitsabläufe neue, nicht-menschliche Zugriffswege. Und ohne solide Governance-Maßnahmen können Konfigurationsfehler, übermäßige Berechtigungen und fehlende Überwachung zu Datenlecks, Missbrauch und Verstößen gegen Compliance-Vorschriften führen.

55 %

der Unternehmen sagen, dass 21 % bis 40 % ihrer Daten vertraulich sind.

Quelle: Proofpoint

68 %

der Unternehmen sagen, dass unangemessene KI-Nutzung vertrauliche Daten kompromittiert hat.

Quelle: Proofpoint

Erkennen, Klassifizieren, Kontrollieren und Schützen von Daten

Proofpoint Data Security Posture Management (DSPM) hilft Teams dabei, die Kontrolle über überall verbreitete Daten zurückzugewinnen und riskante Zugriffe durch Menschen und KI zu reduzieren. Die Lösung erkennt und klassifiziert vertrauliche Daten, zeigt, wer und was darauf zugreifen kann, und bewertet die Risiken. Dadurch können Teams Sicherheitslücken schneller beheben und die Datensicherheit verbessern.

Einzigartige Funktionen

Als Teil der Proofpoint-Datensicherheitsplattform teilen Proofpoint DSPM sowie die integrierte Datenzugriffskontrolle das eigene Datenklassifizierungs-Framework mit Proofpoint Enterprise DLP und Proofpoint Data Security for AI. KI-Klassifizierer identifizieren vertrauliche Dokumentenkategorien anhand von Kontext und Bedeutung, nicht nur anhand von Mustern, was bessere Ergebnisse bei Erkennung und Klassifizierung ermöglicht. Die Lösung hilft Teams außerdem bei der Kontrolle der Zugriffe, Erstellung von DLP-Richtlinien (Datenverlustprävention) und beim Schutz von Daten in lokalen, Cloud-, SaaS-, KI-Umgebungen.

Proofpoint DSPM erkennt zu umfassende Berechtigungen, riskante Zugriffe, Konfigurationsfehler, veraltete Daten und Angriffspfade. Die Data Risk Map zeigt, wo sich vertrauliche Daten befinden, inwiefern sie gefährdet sind und welche Anwender, Anwendungen und KI-Tools darauf zugreifen können. Workflows zur Datenzugriffskontrolle unterstützen die Behebung mit delegierten und Bulk-Aktionen. Die Erkenntnisse aus Proofpoint DSPM lassen sich mit wenigen Klicks in DLP-Regeln umwandeln, damit Teams das Datenkompromittierungsrisiko reduzieren und das Least-Privilege-Prinzip durchsetzen können.

Proofpoint DSPM ermöglicht die sichere Nutzung von KI. Dazu findet die Lösung vertrauliche Daten, auf die Copiloten, große Sprachmodelle (LLMs) und KI-Anwendungen zugreifen können.

Durch die Kombination der Datenzugriffskontrolle von Proofpoint DSPM mit Proofpoint Enterprise DLP und Proofpoint Data Security for AI erhalten Teams die Möglichkeit, vertrauliche Daten während des gesamten Lebenszyklus zu erkennen, zu kontrollieren und zu schützen.

Autonome Klassifizierung geschäftskritischer Dokumente

Proofpoint DSPM bietet marktführende Datenklassifizierung und verwendet reguläre Ausdrücke, Verarbeitung natürlicher Sprache und LLMs, um die Leistung zu verbessern und den Ressourcenbedarf zu reduzieren.

Proofpoint Autonomous Custom Classification (ACC) identifiziert unternehmensspezifische Dokumente ohne manuelle Regeln oder KI-Training, sodass Teams proprietäre Daten finden, blinde Flecken schließen und die Risikoerkennung sowie Richtliniendurchsetzung verbessern können.

Proofpoint DSPM kann außerdem Microsoft Information Protection (MIP)-Vertraulichkeitsbezeichnungen auf Basis von KI-Klassifizierern anwenden und vereinfacht die Durchsetzung von Governance-Richtlinien, die Einhaltung von Vorschriften und den Schutz von Microsoft-Daten vor nicht autorisierten Zugriffen oder Missbrauch.

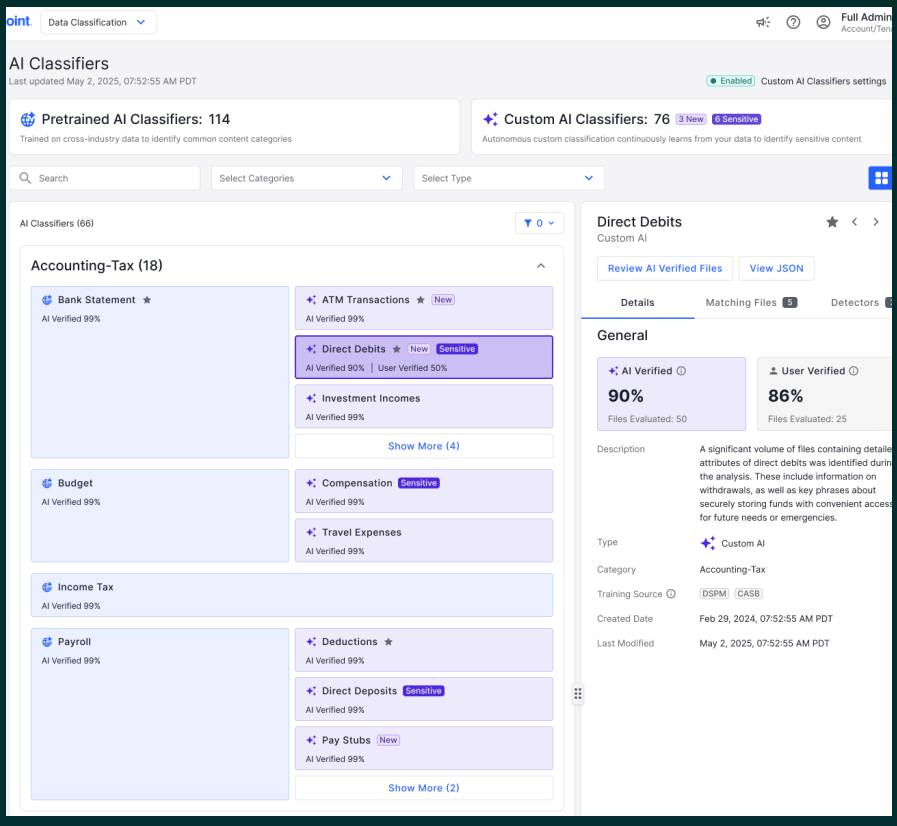

Abb. 1: Die vorab trainierten und autonomen KI-Klassifizierer von Proofpoint DSPM identifizieren gängige und unternehmensspezifische Dokumente, darunter Verträge, Finanzunterlagen, Quellcode und Mitarbeiterdatensätze.

Zuordnung von Datenzugriffsrisiken

Die Data Risk Map zeigt, wo sich vertrauliche Daten in lokalen und SaaS-Systemen befinden, inwiefern der Zugriff auf diese Daten freigegeben wurde und welche Anwender, Anwendungen und KI-Tools darauf zugreifen können. Dabei wird KI-Klassifizierung mit Erkenntnissen in Bezug auf Zugriffe und Nutzung kombiniert.

Sicherheitsteams können übermäßig gefährdete Daten finden, Risiken einstufen, Behebungsmaßnahmen validieren und angesichts der zunehmenden KI-Nutzung gewährleisten, dass der Zugriff angemessen bleibt. Bei der Bewertung von Datenrisiken werden Datenvertraulichkeit, Zugriffsmuster und Kompromittierungsrisiko berücksichtigt, sodass Teams sich auf Daten mit hohem Wert und hohem Risiko konzentrieren können. Dadurch werden die Kosten gesenkt und die Risikofläche des Unternehmens verringert.

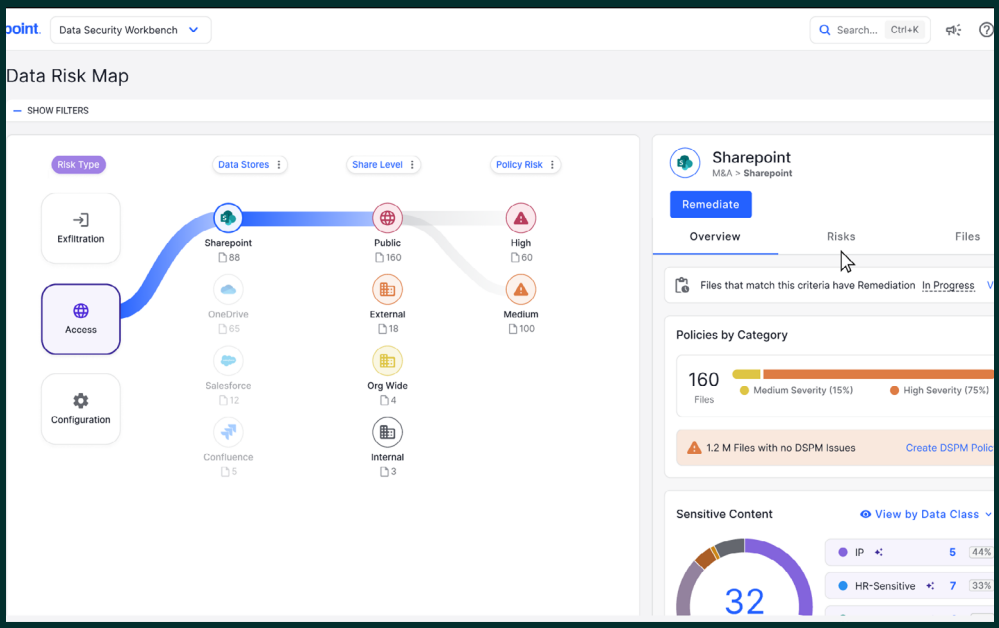

Abb. 2: Die Data Risk Map zeigt, welche Repositories vertrauliche Daten enthalten, inwiefern Daten freigegeben wurden sowie Zugriffe durch Anwender, Anwendungen und KI-Tools.

Priorisieren des Risikos basierend auf dem monetären Wert der Daten

Datensicherheitsteams müssen viele Datenspeicher schützen, doch nicht jeder Speicher hat den gleichen Wert oder das gleiche Risiko. Proofpoint DSPM verwendet eine Datenbewertungstechnologie zum Schätzen der Kosten, die bei einem Datenleck des jeweiligen Datenspeichers entstehen würden. Dies hilft den Teams, sich auf besonders wertvolle Ressourcen zu konzentrieren. Proofpoint DSPM beinhaltet außerdem über 200 vorkonfigurierte Erkenntnisse zu Zugriffen und Kompromittierungsrisiken zur Erkennung toxischer Kombinationen. Diese Risiko-Matrix hebt Datenspeicher mit hohem Risiko und großen finanziellen Folgen hervor.

Minimieren veralteter Daten

In lokalen und SaaS-Systemen findet und entfernt Proofpoint DSPM Dateien, auf die in letzter Zeit nicht zugegriffen wurde. Dabei helfen KI-Klassifizierer, dass geschäftskritische Daten bei Bedarf beibehalten bleiben. In IaaS-Umgebungen (Infrastructure-as-a-Service) findet Proofpoint DSPM nicht benötigte Datenspeicher, z. B. Schattendaten, Datenduplikate und verwaiste Daten wie veraltete Backups und Snapshots.

Dadurch werden die Speicherkosten gesenkt, die Angriffsfläche verkleinert und die Datenverwaltung vereinfacht. Gleichzeitig behalten Teams nur relevante, aktive Daten.

Durchsetzen des Least-Privilege-Prinzips

Die Lösung Proofpoint DSPM unterstützt Zugriffe nach dem Least-Privilege-Prinzip, indem sie Anwender mit übermäßigen Zugriffsrechten, ungenutzte Zugriffsrechte und riskante Konten in allen Datenspeichern findet. Dies unterstützt stärkere Datenzugriffskontrollen und Zero Trust.

Proofpoint DSPM analysiert IAM-Rollen (Identitäts- und Zugriffsverwaltung), Berechtigungen, Datenbankberechtigungen sowie andere Zugriffskontrollen für Personen- und Maschinenidentitäten und zeigt nahezu in Echtzeit an, wer Zugriff auf vertrauliche Daten hat. Teams können unnötige Berechtigungen entfernen und so das Risiko reduzieren.

Proofpoint DSPM kennzeichnet außerdem unzureichend geschützte Konten in SaaS- und Platform-as-a-Service (PaaS)-Umgebungen. Beispiele hierfür sind Anwender mit Zugriff auf vertrauliche Daten, aber ohne Multifaktor-Authentifizierung (MFA), inaktive Konten und Anwendungen mit übermäßigen Administratorrechten.

Erkennen von Angriffspfaden in Cloud-Umgebungen

Proofpoint DSPM erfasst Informationen zu Rechen- und Netzwerkressourcen sowie PaaS- und SaaS-Diensten von verschiedenen Cloud-Anbietern. Die Lösung erkennt Konfigurationsfehler und Sicherheitslücken in diesen Ressourcen. Zudem zeigt ein Diagramm Wege, über die Angreifer an vertrauliche Daten gelangen könnten. Die Überwachung erfolgt nahezu in Echtzeit und macht Veränderungen sichtbar, die das Risiko erhöhen.

Erkenntnisse zu Datenvertraulichkeit, Zugriffsmustern und Risiken stehen auch DLP- und Tools für Datenerkennung und Reaktion (Data Detection and Response, DDR) zur Verfügung.

Zugriffskontrolle – direkt oder durch Delegierung

In lokalen und SaaS-Systemen setzen DSPM-Workflows Erkenntnisse zu Kompromittierungsrisiken in konkrete Maßnahmen um. Da KI-Tools wie Microsoft Copilot die Auswirkungen zu freizügiger Datenfreigaben verstärken, wird die Reduzierung übermäßiger Zugriffe immer wichtiger. Administratoren können öffentliche Links, externe Freigaben und domainweite Zugriffe in Google Workspace und Microsoft 365 widerrufen. Dies ermöglicht Behebungsmaßnahmen für das gesamte Unternehmen.

Sicherheitsteams können nicht für jede Datei bestimmen, ob vorhandene Zugriffsrechte angemessen sind. Mithilfe von Workflows zur Datenzugriffskontrolle können sie Zugriffsüberprüfungen den jeweiligen Dateneigentümern zuweisen. Automatisierte Kampagnen, Erinnerungen und Nachverfolgung vereinfachen die Governance-Maßnahmen.

Durch die Integration mit Proofpoint Enterprise DLP werden nicht nur gespeicherte Daten geschützt. Vertrauliche Daten, die von Proofpoint DSPM klassifiziert und risikobasiert priorisiert wurden, können DLP-Richtlinien zugeordnet werden. Dies ermöglicht durchgehenden Schutz und automatisierte Behebungsmaßnahmen für E-Mail-, Endpunkt-, Cloud- und Collaboration-Kanäle.

In IaaS- und PaaS-Umgebungen helfen entscheidungsrelevante Erkenntnisse und Empfehlungen den Teams, Risiken schnell zu reduzieren. Integrationen mit Ticketing-, Benachrichtigungs- und Automatisierungsplattformen helfen Sicherheitsverantwortlichen, mit DevOps- und Plattform-Teams über bestehende Arbeitsabläufe zusammenzuarbeiten.

Einhaltung von Compliance-Frameworks

Proofpoint DSPM deckt Datenschutz- und Sicherheitslücken in Bezug auf über 25 regulatorischen Compliance-Frameworks auf, darunter EU AI Act, DSGVO, HIPAA, NIST, CMMC und SOC 2.

Verstöße werden nach Framework und Kontrollmaßnahme gekennzeichnet, sodass Analysten die Auswirkungen auf die Vorschriften-Einhaltung erkennen können.

Die Berichtsfunktion zeigt den Compliance-Status der gesamten Infrastruktur auf, aufgeschlüsselt nach Konto, Ressource und Framework. Dies hilft Teams bei der Behebung von Schwachstellen, Vorbereitung auf Audits und Einhaltung von Vorschriften.

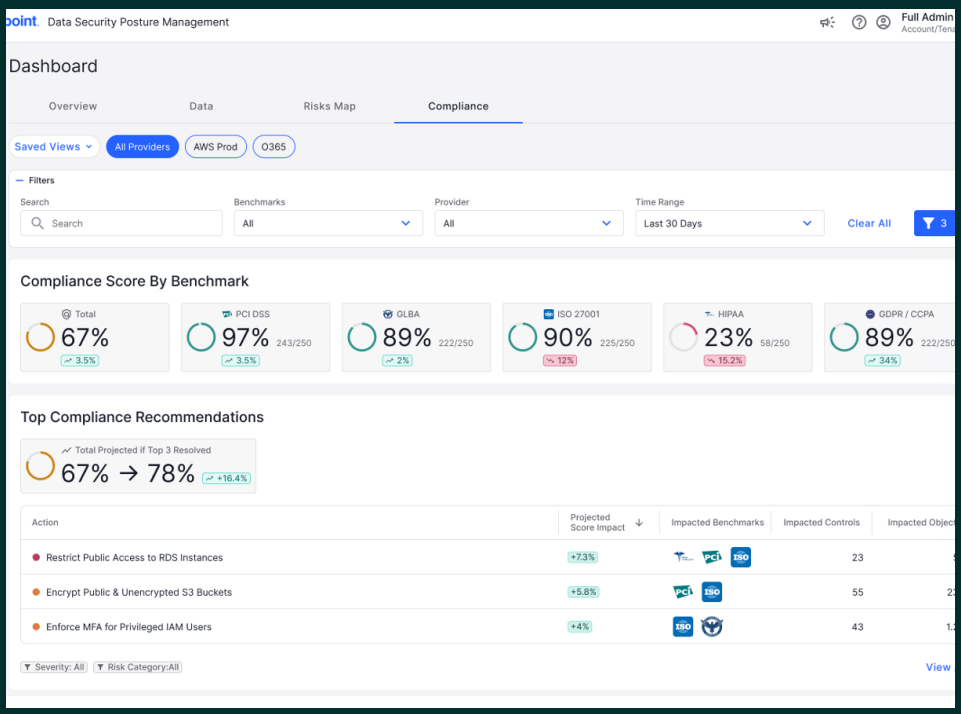

Abb. 3: Dashboard mit Fokus auf den Compliance-Status.

Reduzieren der Datenkompromittierungsrisiken durch KI

Die Lösung Proofpoint DSPM hilft Unternehmen bei der Skalierung von KI, indem sie vertrauliche Daten sichtbar macht, auf die KI-Anwendungen und -Workflows zugreifen können.

Die Erkenntnisse von Proofpoint DSPM zu Kompromittierungsrisiken werden im Dashboard von Proofpoint Data Security for AI angezeigt. In diesem Dashboard haben Sie einen zentralen Überblick über die Datenrisiken durch genehmigte und nicht genehmigte KI-Anwendungen. Proofpoint DSPM überwacht außerdem auf Konfigurationsfehler in KI-Anwendungen und hilft Teams bei deren Behebung. Dies verringert das Risiko von Datenlecks, stärkt die KI-Datenkontrolle und unterstützt die sichere Nutzung von KI.

Proofpoint DSPM sichert kundenspezifische LLMs und KI-Anwendungen auf Plattformen wie AWS Bedrock und Azure ML ab und erkennt vertrauliche Daten, die in Foundation Models, kundenspezifische Modelle und RAG-Workflows (Retrieval-Augmented Generation) übertragen werden.

Proofpoint DSPM bietet außerdem spezialisierte APIs für LLM-Sicherheit. Diese analysieren vertrauliche Daten, die in Echtzeit in und aus LLMs fließen, bieten Datenkontrolle und Transparenz zur Datennutzung und lassen sich in die Arbeitsabläufe der Kunden integrieren.

Unterstützte Plattformen und Technologien

Proofpoint DSPM erkennt und klassifiziert Daten über viele Plattformen und Dienste hinweg und unterstützt eine breite Palette von Datenspeichern, von relationalen Datenbanken über NoSQL-Datenbanken bis hin zu Key-Value-Stores. Dadurch erhalten Teams Transparenz zu strukturierten, unstrukturierten und halbstrukturierten Daten.

Die Unterstützung umfasst alle gängigen Cloud- und SaaS-Plattformen, darunter AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, LLMs und Copiloten.

Durch das gemeinsame Erkennungs- und Klassifizierungs-Framework kann Proofpoint neue Datenspeicherunterstützungen schnell hinzufügen.

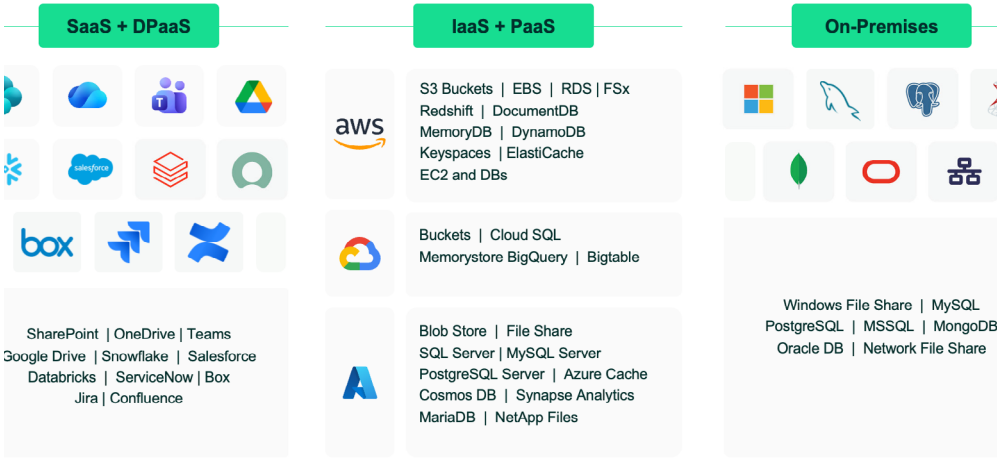

Abb. 4: Proofpoint DSPM erkennt und klassifiziert Daten über zahlreiche Plattformen und Dienste hinweg.

Fazit

Da Unternehmen zunehmend KI einsetzen und immer mehr Daten verwalten, müssen sie wissen, wo sich vertrauliche Daten befinden, wer darauf zugreifen kann und wie sie verwendet werden. Proofpoint DSPM reduziert das Kompromittierungsrisiko, indem vertrauliche Daten klassifiziert, die Risiken bewertet sowie übermäßige Zugriffe erkannt werden und das Least-Privilege-Prinzip in lokalen, Cloud-, SaaS- und KI-Umgebungen durchgesetzt wird.

Als Teil der Proofpoint-Datensicherheitsplattform arbeitet Proofpoint DSPM mit Proofpoint Enterprise DLP zusammen, damit Teams einfacher vertrauliche Daten erkennen, klassifizieren, kontrollieren und schützen können. Unternehmen können die Einhaltung von Vorschriften verbessern, die sichere Nutzung von KI ermöglichen, Risiken reduzieren und ihre wertvollsten Informationen schützen.

proofpoint.