proofpoint®

Proofpoint Information Protection

Lösungsarchitektur

Menschen schützen. Daten sichern.

Komponenten der Proofpoint Information Protection-Plattform

Die Proofpoint Information Protection-Plattform basiert auf Proofpoint Nexus, einer Suite von KI-gestützten Technologien, die kanalübergreifend vertrauliche Daten identifizieren, Datenverlust verhindern und Insider-Bedrohungen eindämmen. Proofpoint Nexus nutzt fortschrittliche Sprachmodelle und Verhaltensanalysen, um Anwender zu erkennen, die absichtlich oder unabsichtlich vertrauliche Daten weitergeben. Zudem identifiziert die Suite ungewöhnliche Verhaltensweisen, z. B. wenn unbefugte Anwender auf Daten zugreifen oder Daten verschieben.

Die Lösung ermöglicht durch automatisierte Richtlinien, die riskante Aktivitäten in Echtzeit blockieren oder korrigieren, zudem eine granulare Kontrolle. Durch die Korrelation der Datenzugriffe und -bewegungen mit Anwenderverhalten schützt Proofpoint Nexus vertrauliche Daten (z. B. personenbezogene Daten, Zahlungskartendaten und andere geheime Inhalte) von E-Mail-, Endpunkt- und Cloud-Anwendungen.

Zusätzlich erweitert die Proofpoint Nexus-Suite die Funktionen von Proofpoint Data Loss Prevention (DLP), indem sie die Verwaltung und Analyse mithilfe fortschrittlicher KI vereinheitlicht. Auf diese Weise können Sicherheitsteams die Datenzugriffe und -bewegungen überwachen und die Einhaltung von Datenschutzbestimmungen wie DSGVO und HIPAA gewährleisten. Darüber hinaus können Unternehmen ihre Richtlinien genau auf ihre spezifischen Bedürfnisse zuschneiden und damit gezielten Schutz implementieren, ohne die normalen Geschäftsaktivitäten zu stören.

Die Proofpoint Information Protection-Plattform umfasst mehrere Produkte. Die meisten der folgenden Produkte lassen sich in diese Plattform integrieren.

Proofpoint Insider Threat Management (ITM) und Proofpoint Endpoint DLP schützen vor Datenverlust und Markenschädigung durch Insider, die böswillig, fahrlässig oder unbewusst falsch handeln. Proofpoint korreliert Anwenderaktivitäten mit Datenbewegungen und unterstützt Sie bei der Identifizierung von Anwenderrisiken, bei der Erkennung von Datenschutzverletzungen durch Insider sowie bei der Beschleunigung von Reaktionen auf Zwischenfälle. Darüber hinaus verhindert Proofpoint die Datenexfiltration über USB-Geräte, Cloud-Synchronisationsordner, Ausdrucke und andere Kanäle. Der zentrale ressourcenschonende Endpunkt-Agent bietet Ihnen die Flexibilität, Anwender mit alltäglichen Risiken sowie Hochrisiko-Anwender zu überwachen.

Proofpoint Cloud DLP bietet Funktionen für einen personenzentrierten Datenschutz (einschließlich Inline-DLP) und die Kontrolle von Cloud-Anwendungen. Die Lösung schützt vertrauliche Daten, kontrolliert OAuth-Anwendungen und hilft Ihnen bei der Einhaltung der Datenschutzgesetze. Dieser Multimodus-CASB unterstützt sowohl API- als auch Proxy-basierte Bereitstellungsmodelle, einschließlich DLP für BYOD (Bring Your Own Device).

Proofpoint Email DLP verhindert den Verlust vertraulicher Daten über E-Mails. Darüber hinaus hilft die Lösung Ihnen mit sofort einsatzbereiten Richtlinien, gesetzliche Anforderungen von DSGVO, SOX und HIPAA zum Schutz von personenbezogenen, Gesundheits- und Zahlungskartendaten einzuhalten. Zusätzlich können Sie (z. B. mit KI-gestützter Klassifizierung) eigene Wörterbücher erstellen, mit denen Sie für Ihr Unternehmen spezifische Daten identifizieren und schützen können. Proofpoint Email DLP lässt sich ganz einfach implementieren und kann im Rahmen eines bestehenden E-Mail-Sicherheitssystems eingerichtet oder in ein unternehmensweites DLP-Programm integriert werden.

Proofpoint Adaptive Email DLP nutzt verhaltensbasierte KI, um das normale E-Mail-Sendeverhalten Ihrer Mitarbeiter, ihre vertrauenswürdigen Beziehungen und ihr Verhalten bei der Kommunikation vertraulicher Daten zu verstehen und bei der Analyse aller E-Mails basierend auf den gewonnenen Erkenntnissen ungewöhnliches Verhalten feststellen zu können. Wenn potenzielle Datenverlustereignisse erkannt werden, werden Administratoren benachrichtigt, die Anwender in Echtzeit gewarnt und der Verlust vertraulicher Daten durch E-Mails verhindert. Proofpoint Adaptive Email DLP ist derzeit nicht in unsere Proofpoint Information Protection-Plattform integriert und wird in diesem Dokument nicht weiter thematisiert.

Die Proofpoint Information Protection-Plattform ist vollständig SaaS-basiert. Das Backend-Analysemodul stellt einheitliche Verwaltungs- und Berichtsfunktionen bereit, darunter Visualisierungen, Erkennung von Anomalien, Big Data-Abfragen, computergestützte Überprüfungen und Fall-Management. Außerdem bietet es Dashboards für die Echtzeitüberwachung Ihrer Sicherheitslage, Sicherheitstrends und Compliance-Risiken. Zudem stellt die Plattform die Kennzahlen bereit, die Führungskräfte benötigen.

Logische Enterprise DLP-Architektur

Die Proofpoint Enterprise DLP-Lösung gibt Sicherheitsadministratoren Werkzeuge an die Hand, mit denen sie vertrauliche Daten schützen, Zwischenfälle in verschiedenen Umgebungen effizient untersuchen und auf diese Weise das Risiko von Datenschutzverletzungen im Unternehmen deutlich senken können.

In Bezug auf die Verwaltung von Zwischenfällen stellt die DLP-Lösung vor allem einen umfassenden Überblick bereit, der den Zeitaufwand für forensische Protokollanalysen reduziert, die Untersuchung und Behebung von Zwischenfällen beschleunigt und Teams insgesamt hilft, mit weniger Aufwand mehr zu erreichen.

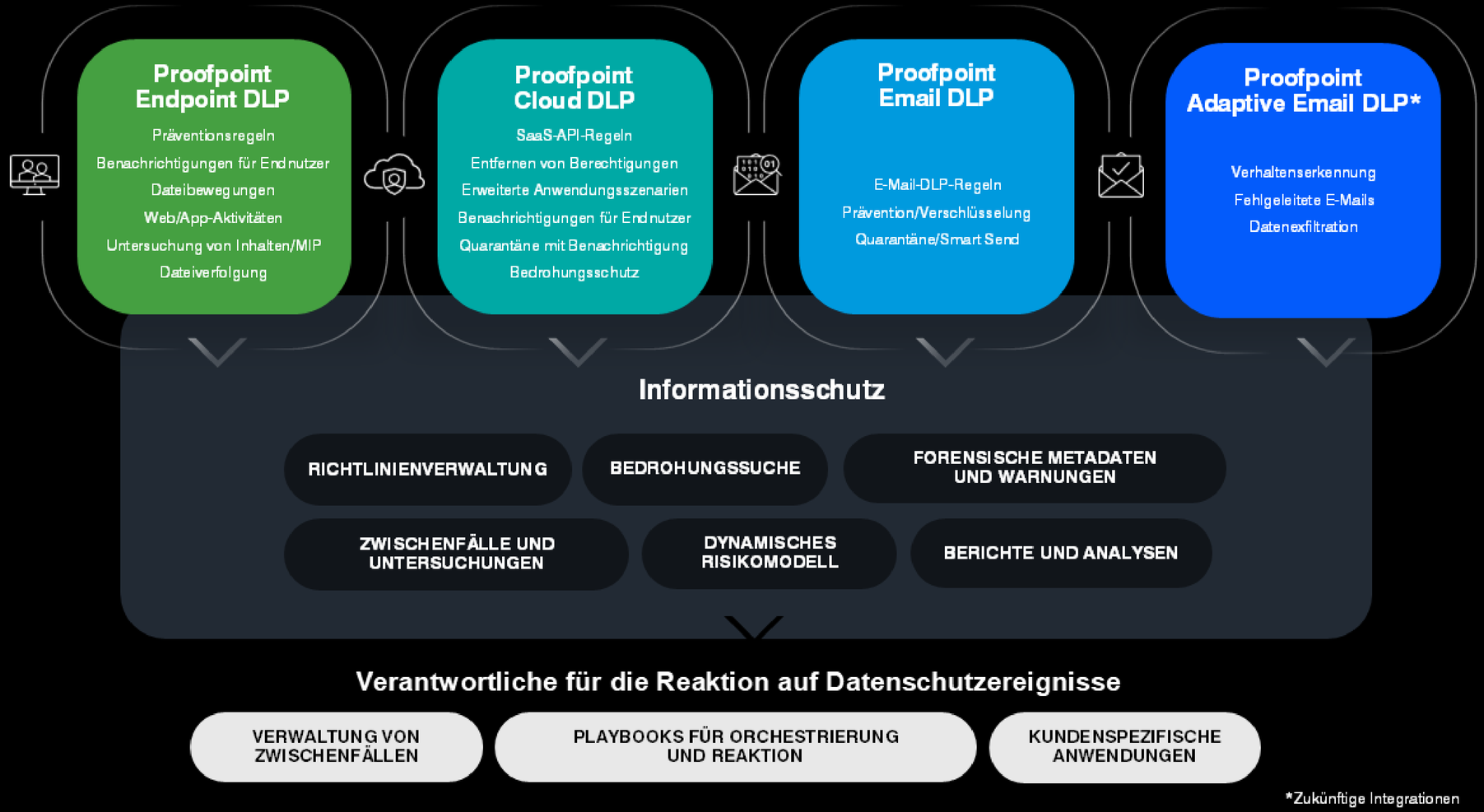
Bei einer integrierten Lösung arbeiten verschiedene Erkennungskomponenten zusammen. Eine Lösungsarchitektur beschreibt die Konfiguration sowie die Regeln und Richtlinien für die Produktimplementierung und legt die organisatorischen Risiken und geschäftlichen Faktoren für das DLP-Programm eindeutig dar.

Mithilfe unternehmensspezifischer Regeln können Sie die Transparenz und Kontrolle für bestimmte Aktivitäten im Zusammenhang mit Unternehmens-informationen sicherstellen, Analysten auf Sicherheitszwischenfälle hinweisen und automatische Behebungsmaßnahmen orchestrieren. Granulare Regeln ermöglichen flexible Reaktionsmöglichkeiten, ohne normale Geschäftsaktivitäten zu blockieren.

Außerdem können wichtige Zwischenfälle und besonders riskante Aktivitäten leicht identifiziert, erfasst und exportiert und diese Informationen an die zuständigen Teams weitergeleitet werden. Dies reduziert den Aufwand und die Kosten für die Zwischenfallverwaltung und sorgt dafür, dass die Teams das Unternehmen und seine Anwender besser vor den negativen Folgen von Datenverlusten schützen können.

Proofpoint Enterprise DLP-Referenzarchitektur

Aktivitäts- und Kommunikationsfluss zwischen den Komponenten der DLP-Lösung

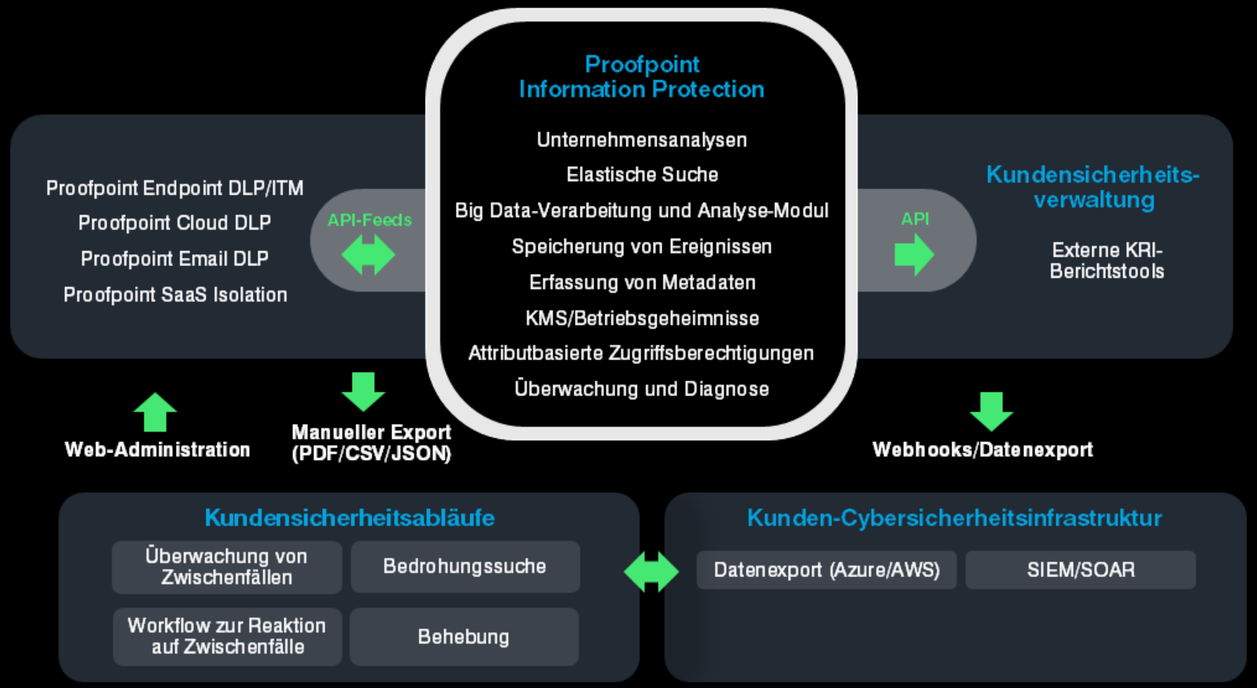


*Zukünftige Integrationen

Dokument-Nr.: 1207-005-04-01

Einheitliche Analysen in der Proofpoint Information Protection-Plattform

Einheitliche Analysearchitektur der Proofpoint Information Protection-Plattform für den Schutz von Informationen auf Endpunkten, in der Cloud und in E-Mails



Einheitliche Analysen für die Verwaltung von Warnmeldungen, Untersuchungen und Reaktionen

Die einheitliche Verwaltungsübersicht stellt Ihnen alle Datenanalyse- und Berichtsfunktionen für alle von der Lösung erfassten Ereignisse zur Verfügung und ermöglicht die Verwaltung der Workflows für Warnmeldungen. Die hier bereitgestellten Datenanalysefunktionen ermöglichen viele komplexe Anwendungsszenarien, darunter Untersuchungen im Rahmen der Bedrohungssuche, die Erkennung von Anomalien und die computergestützte Triage von Warnmeldungen.

Das Analysemodul ermöglicht die Entwicklung spezifischer Erkennungsregeln, mit denen Sie Warnmeldungen für die Triage durch Sicherheitsanalysten generieren können. Bei einem Verstoß wird eine E-Mail oder ein ausgehendes Webhook-Ereignis mit den entsprechenden Alarmdetails an eine Empfängeranwendung eines Drittanbieters (z. B. ein SIEM/SOAR- oder Instant-Messaging-System) gesendet.

Splunk und andere SIEM-Anbieter können in die Proofpoint Information Protection-Plattform integriert werden, um einen einheitlichen Überblick über Insider-Bedrohungen, laterale Bewegungen und Datenexfiltrationen bereitzustellen. Dadurch können Sie schnell feststellen, welche Anwender beteiligt waren, und die Details mit anderen Ereignisquellen korrelieren.

Über Integrationen kann unsere Plattform auch ServiceNow über jegliche Datenexfiltrationen oder Compliance-Verstöße informieren. ServiceNow wiederum kann dann seine Kunden warnen und basierend auf den Warnmeldungen neue Tickets oder Workflows erstellen. Eine Integration mit ServiceNow DLP beschleunigt Untersuchungen und Reaktionen.

Zugang zur Plattform und Datenschutzkontrollen

Proofpoint-Mitarbeiter können zu keinem Zeitpunkt auf Ihre Daten zugreifen – es sei denn, Ihr Team gibt sie für sie frei. Wenn Sie Zugriff gewähren, können sich Proofpoint-Mitarbeiter oder Ihre Teammitglieder über das Proofpoint User Center beim System anmelden. Alternativ kann ihnen der Zugang über eine Identität zugewiesen werden, bei der es sich im Grunde um einen vorübergehend generierten Anwender handelt.

Wenn ein Administratorkonto mit umfangreichen Berechtigungen verwendet wird, sollten dafür entsprechende Warnmeldungen eingerichtet werden. Damit das Konto sicher bleibt, muss sein Kennwort geändert werden. Das Kennwort könnte auch hinterlegt oder auf mehrere verantwortliche Parteien aufgeteilt werden.

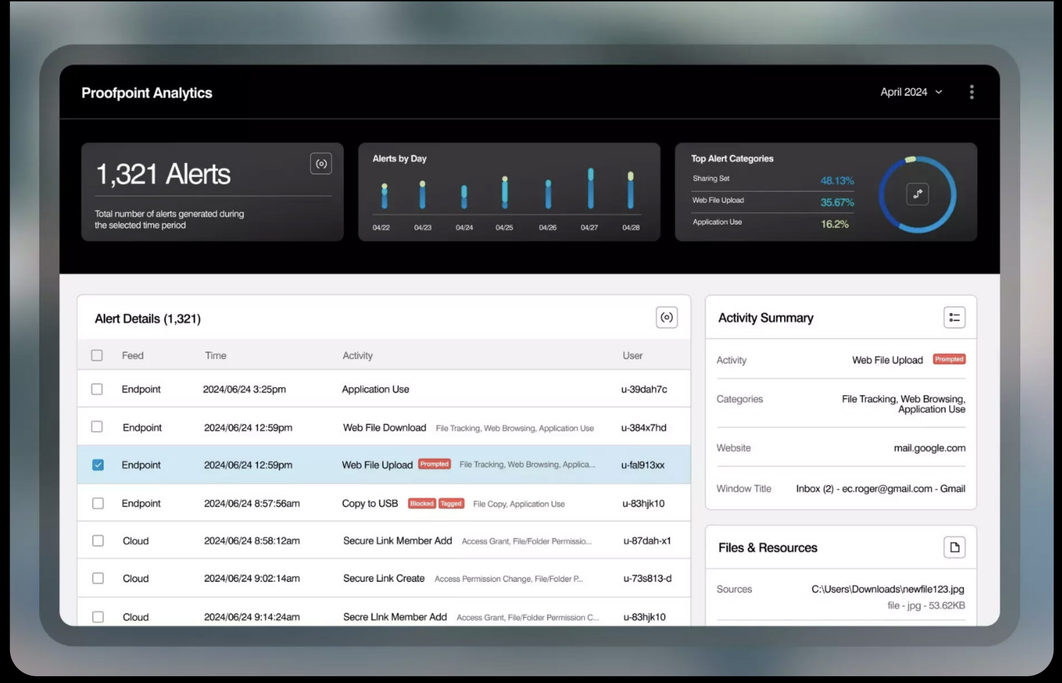
Es wird dringend empfohlen, SAML oder OAuth 2.0 zu verwenden, um Cloud-basierte Authentifizierungsmethoden wie Single Sign-On (SSO) und Multifaktor-Authentifizierung (MFA) zu integrieren. Optional können Sie auch mehrere Identitätsanbieter kombinieren.

Dazu müssen Sie in der Proofpoint Information Protection-Plattform unter „Administration“ > „Account Settings“ (Verwaltung > Kontoeinstellungen) für jeden Identitätsanbieter die erforderlichen Einstellungen konfigurieren. Außerdem müssen Sie Ihren Identitätsanbieter so konfigurieren, dass er sich mit der Proofpoint Information Protection-Plattform verbindet.

Das Administratorkonto hat vollen, deanonymisierten Zugriff auf alle Einstellungen und Daten der Plattform. Deshalb müssen die Anmeldedaten geschützt und streng vertraulich behandelt werden. Während der Produkttests können unter „Administration“ > „User Management“ (Verwaltung > Anwenderverwaltung) weitere lokale Administratorkonten erstellt werden. Jedem Konto können je nach Bedarf eigene Zugriffsrichtlinien zugewiesen werden. Wenn weitere Administratoranwender hinzugefügt werden, müssen die Kontrolle und der administrative Zugriff jedoch meist eingeschränkt werden.

Proofpoint Information Protection basiert auf den Grundsätzen des standardmäßig integrierten Datenschutzes, d. h. nur Personen, die die vertraulichen Daten und persönlichen Informationen der Anwender kennen müssen, haben auch Zugriff darauf. Proofpoint nutzt regionale Rechenzentren in den USA, Europa, Australien, Kanada (Ende 2024) und Japan (nur Endpunktdaten). Auf diese Weise können Sie die Daten auf einfache Weise geografisch trennen, z. B. indem Sie eine US-Gruppe erstellen, die Daten zu Endpunkten in den USA verwaltet und in einem Rechenzentrum in USA speichert. Mithilfe granularer Zugriffsrichtlinien kann Ihr Administrator den Zugriff so zuweisen, dass ein in den USA ansässiger Sicherheitsanalyst nur US-bezogene Daten einsehen kann.

Mit Proofpoint Information Protection können Systemadministratoren auch die forensischen Daten (personenbezogene, Gesundheits- und Zahlungskartendaten) konfigurieren, die in der Konsole maskiert werden sollen, um die Identität von Anwendern zu verbergen und jede Beeinflussung der Analysten zu vermeiden. Sie können den Namen des Anwenders, den Hostnamen, die IP-Adresse, die Standortdaten und die Dateinamen anonymisieren. Falls die Identität des Anwenders im Laufe einer Untersuchung benötigt wird, kann der Sicherheitsanalyst die Deanonymisierung beantragen und ein Administrator kann diese gewähren.



Web-Konsolenzugriff

Administratoren und Analysten können sich über einen unterstützten Browser mit der Plattform verbinden. Sie können Richtlinien und Regeln verwalten, Warnmeldungen überprüfen, auf Zwischenfälle direkt reagieren, erfasste Datensätze analysieren und Berichte zu erfassten Anwenderaktivitäten prüfen.

Zur Verwaltung separater Untereinheiten können viele Unternehmen auf mehrere Untermandaten auf der Proofpoint-Plattform zugreifen.

Plattformbenachrichtigungen

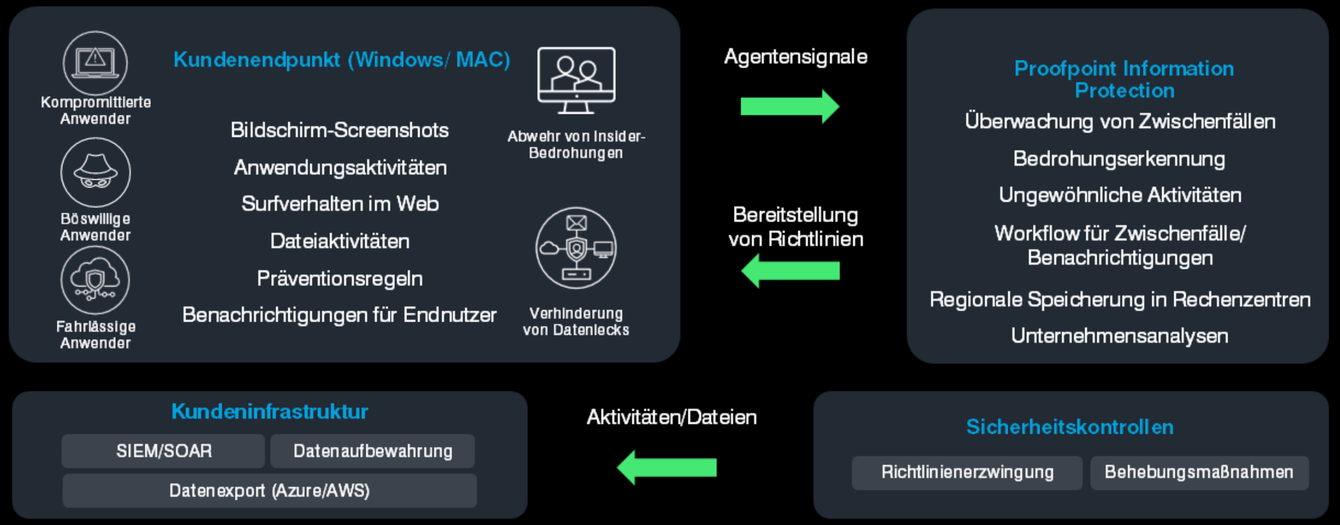
Auf der Proofpoint-Plattform können Warnmeldungen überwacht und verarbeitet werden. Alternativ kann dies auch extern nach Ihren internen Verfahren zur Verwaltung von Zwischenfällen erfolgen. Sie müssen alle E-Mail-Adressen angeben, die die von der Proofpoint Information Protection-Plattform generierten Warnmeldungen erhalten sollen. Auch externe Systeme (SIEM, SOAR, ITSM) können für den Empfang von Warnmeldungen konfiguriert werden.

Externe Anwendungen

Externe Anwendungen können über REST-APIs auf die Proofpoint-Plattform zugreifen.

Proofpoint Endpoint DLP/ITM-Referenzarchitektur

Erfassung von DLP- und ITM-Daten, Upload dieser Daten auf die Plattform und Durchsetzung der DLP-Richtlinien mit nur einem Agenten



Konfiguration des DLP/ITM-Endpunkt-Agenten

Der Endpoint DLP-Agent wird auf Kundenendpunkten mit den unterstützten Windows- oder macOS-Versionen installiert. Für die Installation des Agenten in der Produktionsumgebung sollten Sie unbeaufsichtigte Methoden und die Standardtools Ihres Unternehmens für Remote-Softwareinstallationen verwenden.

Nach seiner Bereitstellung zeichnet der Agent Metadaten zu den Anwenderaktivitäten auf. Dabei sind keine expliziten Regeln erforderlich. Die Metadaten werden sicher hochgeladen und von der Proofpoint Information Protection-Plattform verarbeitet. Die Verwaltung und Konfiguration des Agenten erfolgt in der Plattform über „Administration“ > „Endpoints” (Verwaltung > Endpunkte).

Proofpoint-Endpunkt-Agenten können im Hintergrund installiert werden. Sie werden im Arbeitsspeicher des Endpunkts ausgeführt, belegen nur minimale Ressourcen und können sich automatisch aktualisieren. Das System muss nach der Installation oder dem Upgrade nicht neu gestartet werden. Agenten verursachen keine Konflikte mit der bestehenden Endpunktsicherheit und beeinträchtigen auch nicht die Funktionalität anderer Anwendungen.

Installierte Agenten und der ITM-Server kommunizieren asynchron über das HTTP-Protokoll. Die Kommunikation der DLP-Agenten mit den Proofpoint-Cloud-Diensten wird per TLS verschlüsselt. Die Firewall-Anforderungen für die Konnektivität finden Sie in unserem Online-Dokumentationsportal.

Agenten, die sich über einen dynamischen Proxy verbinden müssen, verwenden die auf Betriebssystemebene definierten Proxy-Einstellungen. Im Betriebssystem muss die Verwendung eines dynamischen Proxys für Anwendungen konfiguriert werden, die unter dem Systemkonto (nicht dem Anwenderkonto) ausgeführt werden. Die Verwendung eines statischen Proxys wird ebenfalls unterstützt (dies wird bei der Installation der Agenten konfiguriert).

Einige Virenschutz- und EDR-Programme werden standardmäßig on-demand ausgeführt, scannen ausführbare Dateien und halten Prozesse an oder blockieren ihre Kommunikation. Um einen stabilen Betrieb zu gewährleisten, müssen Sie unsere Prozesse von der Prüfung durch andere Sicherheitstools ausnehmen. Proofpoint geht nicht davon aus, dass bestimmte Anwendungen unseres eigenen Tools auf eine Whitelist gesetzt werden müssen, denn es ist unwahrscheinlich, dass unser ressourcenschonender Ansatz die Aktionen eines Kernel-Endpunkt-Agenten stört.

Komponenten von Windows-Endpunkt-Agenten für Safelists
Informationen dazu, wie Sie unsere Dateien vor Beeinträchtigungen durch EDR- oder Virenschutzsysteme schützen, erhalten Sie in **diesen Leitfaden**.

HINWEIS: Wenn Sie in macOS Benachrichtigungen anzeigen oder Screenshots erstellen möchten, müssen Sie die mobile Konfigurationsdatei bereitstellen, damit unsere Prozesse über die entsprechenden Berechtigungen verfügen. Informationen dazu, wie Sie dazu vorgehen, erhalten Sie in unserer Online-Dokumentation.

Der Proofpoint-Endpunkt-Agent unterstützt zwei Arten von Proxys. Für einen dynamischen Proxy verwenden Sie eine PAC-Autokonfigurationsdatei auf Betriebssystemebene. Für einen statischen Proxy geben Sie bei der Installation den Hostnamen und den Port an. Um Standard-Anmeldedaten für den Agenten festzulegen, füllen Sie während der Installation die Felder „Domain", „Username" (Benutzername) bzw. „Password" (Kennwort) aus.

Updates für Agenten
Da Proofpoint Information Protection als SaaS-Plattform bereitgestellt wird, kann Proofpoint neue Funktionen schnell in den Agenten integrieren. Für Kunden, für die sich unser Aktualisierungsplan nicht eignet, bietet Proofpoint eine Agentenversion mit Langzeit-Support (LTS) an. Generell empfehlen wir jedoch, immer unsere neueste unterstützte Agentenversion zu verwenden.

Wir empfehlen den automatischen Update-Dienst, mit dem die Agenten entsprechend einer vorkonfigurierten Update-Richtlinie jederzeit auf dem neuesten Stand bleiben. Wenn der Agent aktualisiert werden soll, aktualisiert oder erstellt der Administrator einfach eine Richtlinie, in der die Zielversion und die Bedingungen für die Durchführung des Upgrades festgelegt sind. Diese Richtlinie wird auf dem Agenten auf den Endpunkten verarbeitet und gewährleistet, dass automatisch die richtigen Versionen heruntergeladen und installiert werden.

Root-Zertifikat
Die verwalteten Endpunkte müssen über ein gültiges Root-Zertifikat verfügen. Proofpoint signiert den Agenten mit einem gültigen Root-Zertifikat, damit der Kunde weiß, dass er von Proofpoint stammt. Dieses Zertifikat hängt von einem gültigen Root-Zertifikat ab und hat ein jährliches Ablaufdatum.

Überwachung des Agentenzustands
Informationen zum Agentenzustand (z. B. Fehler und letzte Anmeldezeiten) sind in der Endpunktübersicht der Plattform verfügbar. Der Windows-Agent kann sich weitgehend selbst reparieren und enthält einen Watchdog-Dienst (IT-Cloud-Dienst), der einen Neustart auslöst, sobald er beendet wird oder ausfällt. Der Logger-Prozess des Mac-Agenten wird ebenfalls überwacht; falls der Agent beendet oder ausfällt, wird er von launchd neu gestartet.

Stärkung der Agentenresilienz
Die Agentenkonfiguration und die Protokolldateien auf den Endpunkten können vollständig verschlüsselt werden. Während der Installation können zusätzliche Schutzmaßnahmen aktiviert werden. So können Sie z. B. einen Sicherheitsschlüssel anwenden, der die Deinstallation des Agenten oder die Umbenennung seiner Prozesse verhindert.

Konfiguration von Endpunktgruppen
Agentengruppen (Agent Realms) unterteilen die Agenten nach ihrem regionalen Speicherort und Datenaufbewahrungszeitraum.

Präventionsregeln für Endpunkte werden über abgestufte Agentenrichtlinien bereitgestellt und setzen Maßnahmen wie Warnungen oder die Blockierung des Anwenders durch. Gleichzeitig protokolliert der Agent Metadatensignale über Anwendungsaktivitäten. Diese Protokolle werden zur Verarbeitung an das Analysemodul gesendet. Optional können Screenshots erstellt werden.

Die verarbeiteten Daten werden je nach gewählter Agentengruppen-Einstellung im regionalen AWS-Rechenzentrum Ihrer Wahl gespeichert (derzeit USA, Europa, Asien-Pazifik, Japan, Kanada).

Einstellungen für Agentenrichtlinien
Agentenrichtlinien definieren, was der Proofpoint-Agent erfasst. Sie werden Agentengruppen zugewiesen, d. h. Sie können Einstellungen konfigurieren und parallel auf Endpunkte in mehreren Gruppen anwenden.

Sie können einer Agentengruppe mehr als eine Agentenrichtlinie zuweisen. Wenn Sie mehrere Richtlinien zuweisen möchten, können Sie eine Reihenfolge festlegen und auf diese Weise auch genauer definieren, welche Einstellungen auf welche Agenten angewendet werden. Die Reihenfolge bestimmt, welche Einstellungen für welche Agentenrichtlinie aktiviert werden.

Prävention für Endpunkte und Benachrichtigungen für Endnutzer

Eine zentrale Aufgabe eines DLP- oder ITM-Programms besteht darin, das Verhalten der Endnutzer so zu beeinflussen, dass das Risiko von Datenschutzverletzungen sinkt. Wenn DLP-Richtlinien auf verwalteten Endpunkten bereitgestellt werden, können Endnutzer damit im Falle von Richtlinienverstößen blockiert oder gewarnt werden. So wird ihr Verhalten beeinflusst und das Risiko von Datenschutzverletzungen reduziert.

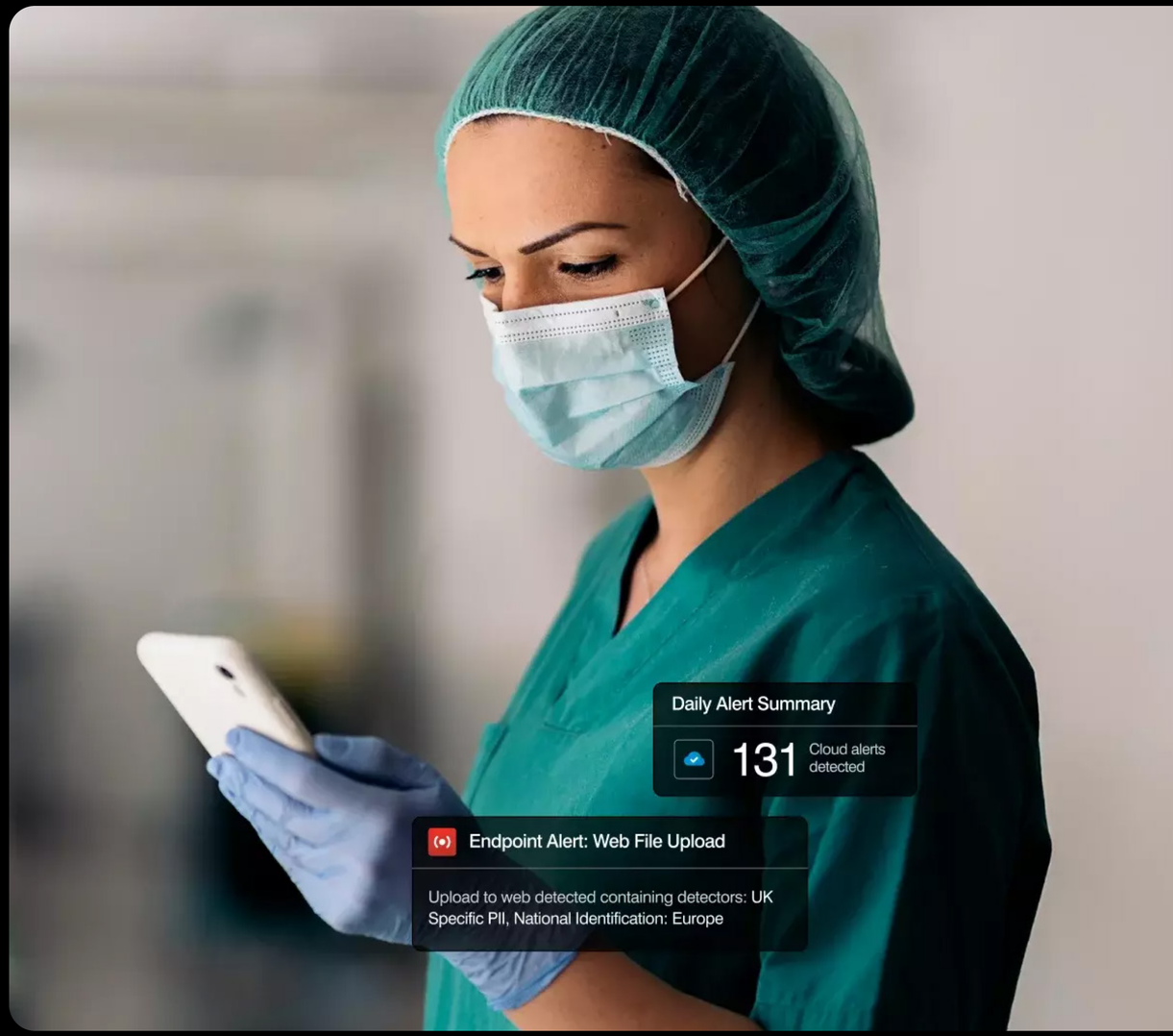
DLP-Regeln sollen das Verhalten von Endnutzern ändern, wenn eine Exfiltration vertraulicher Unternehmensdaten erkannt wird. Ein gängiger Ansatz besteht darin, zunächst die Aktivitätenmetadaten aus Warnmeldungen zu überwachen oder Aktivitätsuntersuchungen durchzuführen. Während die Teams die Warnmeldungen überprüfen, können sie die Regeln an die Prioritäten des Unternehmens und dessen Prozesse zur Zwischenfallerkennung anpassen.

Sobald dieser Prozess ausgereift ist, können die Regeln bereitgestellt werden. Wenn Endnutzer zu diesem Zeitpunkt gegen die Richtlinien verstoßen, wird die Aktivität blockiert und ein Hinweis zur Blockierung angezeigt. Bevor sie fortfahren dürfen, müssen sie ihre Aktivität rechtfertigen. Dabei können sie aus verschiedenen Standard- oder angepassten Textbausteinen wählen.

Die Benachrichtigungen für Endnutzer enthalten meist eine individuelle Erklärung zu der Richtlinie, gegen die der Anwender gerade verstoßen hat, sowie das offizielle Logo des Unternehmens und einen Link zu einer Webseite, auf der die Sicherheitsrichtlinien des Unternehmens erläutert werden. Das Firmenlogo darf dabei max. 56 KB groß sein (MIME-Type).

Die Benachrichtigung informiert die Anwender außerdem darüber, wie sie nach einer blockierten Aktivität vorgehen sollen und an wen sie sich wenden müssen, wenn die Blockierung fälschlicherweise erfolgte. Sinnvoll ist zudem ein Link zu einer Intranetseite, die die Notwendigkeit des DLP-Programms erklärt.

Die Erkennungsregeln generieren Warnmeldungen in unserem Analysemodul. Ein zuständiger Mitarbeiter kann diese Meldungen sowie alle erfassten Metadaten prüfen, die durch bestimmte Anwenderaktivitäten auf den Endpunkten generiert werden. Die Metadaten werden vom Agenten gemäß den Einstellungen der Agentenrichtlinie (z. B. für die Häufigkeit und die Auflösung der Screenshots) aufgezeichnet und in der Administrationskonsole verwaltet.



Konfiguration von Proofpoint Cloud DLP

Proofpoint Cloud DLP unterstützt eine agentenlose Architektur und nutzt Cloud-APIs, um wichtige Cloud-Anwendungen zu schützen. Darüber hinaus bietet die Lösung für BYOD-Geräte Inline-DLP mit Browser-Isolierung, die nach der Authentifizierung für den Zugriff auf eine Cloud-Anwendung aktiv wird.

Proofpoint Cloud DLP stellt eine Verbindung zu den primären Cloud-Diensten eines Unternehmens und zu genehmigten SaaS/IaaS-Anwendungen über deren jeweilige APIs her. Dadurch können bidirektionale Funktionen (darunter die Behebung von Cloud-bezogenen Sicherheitszwischenfällen) nahezu in Echtzeit genutzt werden.

Proofpoint Cloud DLP ist äußerst leistungsstark und bietet Behebungsmaßnahmen mit denselben DLP-Erkennungstechnologie, die auch bei Proofpoint Endpoint DLP verfügbar sind.

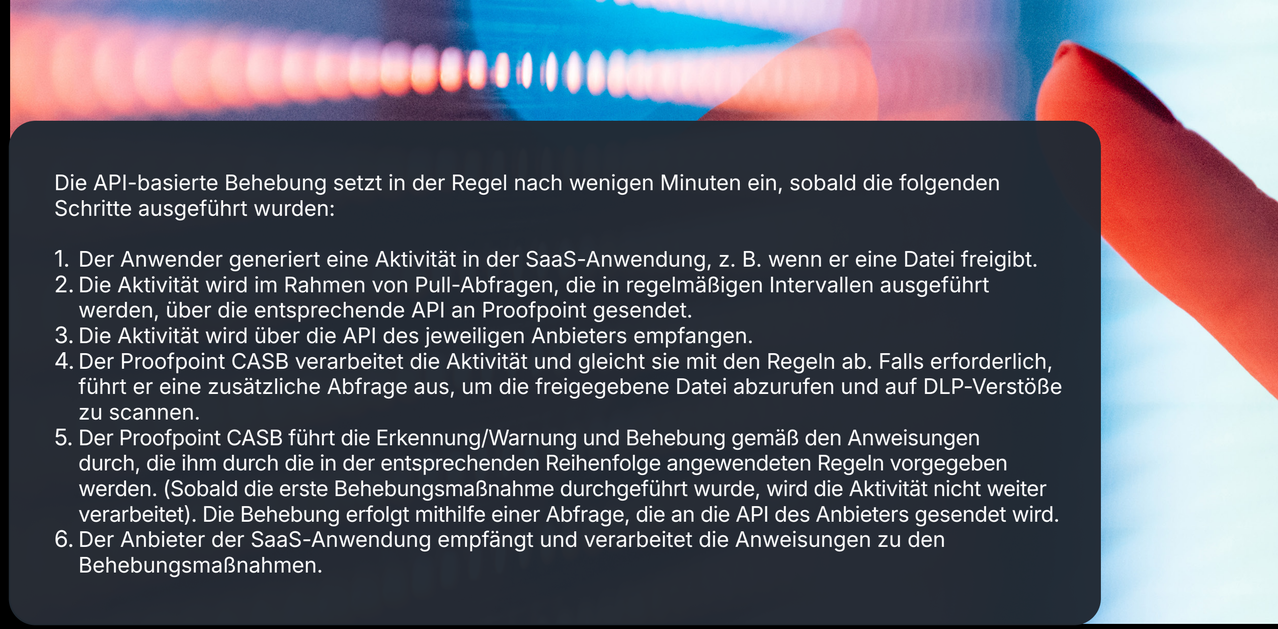
Proofpoint CASB Adaptive Access Controls erweitert den Funktionsumfang von Proofpoint Cloud DLP, sodass verschiedene komplexe Echtzeit-Anwendungsszenarien umgesetzt werden können. Dazu gehören die Erkennung und Blockierung nicht verwalteter Geräte sowie die Erkennung von Zugriffsversuchen von risikoreichen Standorten aus. Dazu stehen SAML/OIDC-Integrationen mit Cloud-Identitätsanbietern zur Verfügung.

Die Integration von Proofpoint SaaS Isolation ermöglicht eine noch detailliertere DLP-Kontrolle über browserbasierte Datei-Uploads und -Downloads, ohne dass dafür ein Agent benötigt wird. Daher lässt sich auch DLP auf BYOD-Geräten umsetzen. Okta-API-Konnektoren von Proofpoint vereinfachen SAML-Integrationen, sodass wir für föderierte Okta-Anwendungen automatisch adaptive Kontrollen implementieren können.

In einem zusätzlichen Schritt können IaaS-Dienste wie Azure und AWS für die DLP-Überwachung konfiguriert werden. Proofpoint berechnet diese APIs separat.

Zunächst werden die Anbieter-APIs für die von Ihnen ausgewählten Cloud-Unternehmensanwendungen für die Sicherheitsüberwachung mit Proofpoint Cloud DLP verbunden.

Dort können Sie spezifische Regeln entwickeln, um DLP-Regelverstöße in Cloud-Diensten zu erkennen und zu beheben. Darüber hinaus können Sie automatisierte Governance-Regeln auf OAuth-Anwendungen von Drittanbietern anwenden, die den System- und Datenzugriff auf Ihre primären SaaS- und Unternehmensdienste wie Microsoft 365 und Google Workspace verwalten.



Die API-basierte Behebung setzt in der Regel nach wenigen Minuten ein, sobald die folgenden Schritte ausgeführt wurden:

1. Der Anwender generiert eine Aktivität in der SaaS-Anwendung, z. B. wenn er eine Datei freigibt.
2. Die Aktivität wird im Rahmen von Pull-Abfragen, die in regelmäßigen Intervallen ausgeführt werden, über die entsprechende API an Proofpoint gesendet.
3. Die Aktivität wird über die API des jeweiligen Anbieters empfangen.
4. Der Proofpoint CASB verarbeitet die Aktivität und gleicht sie mit den Regeln ab. Falls erforderlich, führt er eine zusätzliche Abfrage aus, um die freigegebene Datei abzurufen und auf DLP-Verstöße zu scannen.
5. Der Proofpoint CASB führt die Erkennung/Warnung und Behebung gemäß den Anweisungen durch, die ihm durch die in der entsprechenden Reihenfolge angewendeten Regeln vorgegeben werden. (Sobald die erste Behebungsmaßnahme durchgeführt wurde, wird die Aktivität nicht weiter verarbeitet). Die Behebung erfolgt mithilfe einer Abfrage, die an die API des Anbieters gesendet wird.
6. Der Anbieter der SaaS-Anwendung empfängt und verarbeitet die Anweisungen zu den Behebungsmaßnahmen.

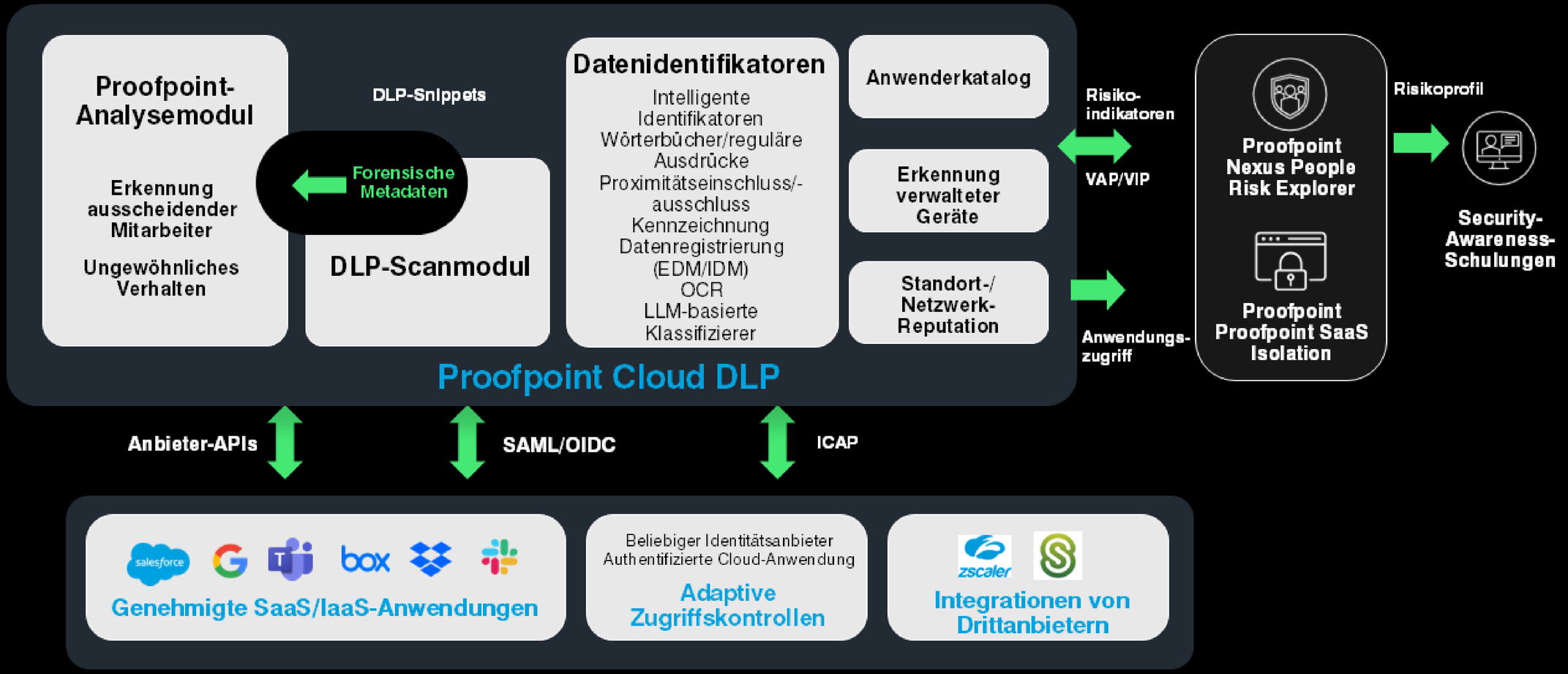
Proofpoint CASB Adaptive Access Controls ermöglicht die Inline-Kontrolle von unterstützten Anwendungen ohne einen Agenten. Durch die SAML 2.0- oder OIDC-Integration mit Ihrem Identitätsanbieter können wir mit Proofpoint Cloud DLP für jede authentifizierte Anwendung zusätzlichen Schutz implementieren.

Für die Einrichtung von Proofpoint CASB Adaptive Access Controls müssen die Anmelde-Aufforderungen der Anwendung über Proofpoint umgeleitet werden, bevor sie vom Identitätsanbieter authentifiziert werden. Wir können dann eine Regel anwenden, die bei Einhaltung bestimmter Bedingungen den Zugriff auf genehmigte Cloud-Anwendungen des Unternehmens erlaubt.

Richtlinien können auf Parametern basieren, z. B. ob ein Anwender von einem nicht verwalteten Gerät, außerhalb des Egress-Bereichs eines Büroquellnetzwerks, von einem riskanten Standort zugreift oder ob andere SaaS-typische Risikofaktoren vorhanden sind. Die zusätzliche Integration mit Proofpoint SaaS Isolation ermöglicht eine noch genauere Kontrolle des browserbasierten Zugriffs auf Cloud-Anwendungen. Dabei profitieren Sie von einer Echtzeit-Integration mit unserer DLP-Technologie, ohne dafür einen Agenten zu benötigen.

Um DLP weiter zu vereinheitlichen und kanalübergreifende Transparenz zu Datenverlustereignissen zu ermöglichen, unterstützt Proofpoint auch die ICAP-Integration mit Zscaler und Citrix ShareFile. Dazu müssen Sie zuerst das DLP-Detektor-Set für diesen Kanal in unserer Plattform konfigurieren und dann den ICAP-Client Ihrer Drittanbieter-Anwendung so konfigurieren, dass seine Daten über unseren DLP-Dienst geführt werden.

Proofpoint Cloud DLP-Referenzarchitektur



Dokument-Nr.: 1207-005-04-01

Konfiguration von Proofpoint Email DLP

Proofpoint Email DLP verwendet ein Inline-E-Mail-Gateway, das von Proofpoint bereitgestellt wird und ausgehende E-Mails verarbeitet. Dieses Gateway integriert sich in Ihre Architektur für ausgehende E-Mails.

Proofpoint berät Sie zur Konfiguration Ihrer Infrastruktur und Systeme auf der Grundlage Ihrer bestehenden E-Mail-Architektur, unabhängig davon, ob Sie Proofpoint Email DLP für ausgehende E-Mails testen oder in Ihrer Produktionsumgebung einsetzen möchten.

Wenn Sie Proofpoint bereits als Gateway für Ihre ausgehende E-Mails verwenden, wird Proofpoint Email DLP einfach direkt auf Ihrem bestehenden Proofpoint-E-Mail-Gateway aktiviert, indem Sie das Modul für gesetzliche Compliance lizenzieren. Es werden keine Änderungen an Ihrem E-Mail-Fluss vorgenommen und es gibt keine Auswirkungen auf SPF, DMARC oder das IP Warm-Up (Aufwärmen einer IP-Adresse).

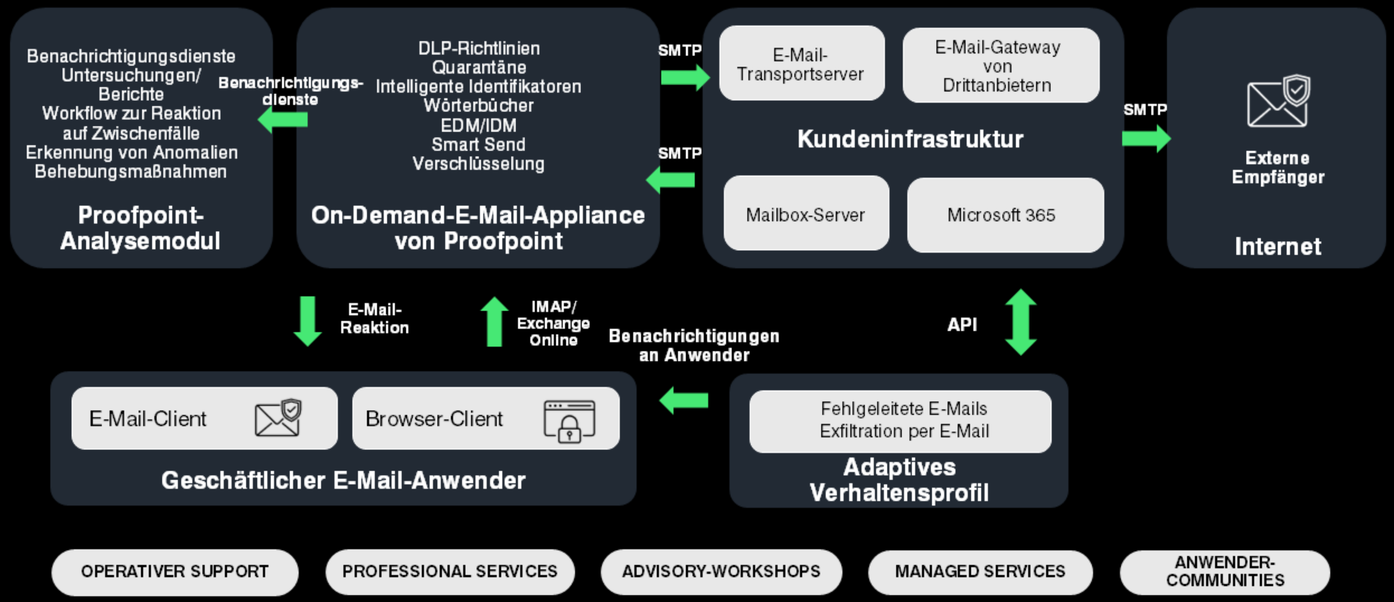
Sobald Proofpoint Email DLP aktiviert ist, können Sie den gesamten Funktionsumfang testen, einschließlich der Funktionen für Berichte, Durchsetzung, Benachrichtigungen für Endnutzer und Interaktionen.

Wenn Proofpoint nicht der letzte Routing-Punkt in Ihrem E-Mail-Verarbeitungsfluss ist, wird das Cloud-basierte Proofpoint-E-Mail-Gateway als zusätzlicher SMTP-Routing-Punkt in Ihre Infrastruktur für ausgehende E-Mails integriert. Idealerweise sollte das Proofpoint-Gateway vor einem bestehenden E-Mail-Gateway eingefügt werden, um zusätzliche Änderungen an der Infrastruktur zu vermeiden.

Sobald der Dienst für ausgehende E-Mails integriert wurde, können Sie den gesamten Umfang der DLP-Funktionen uneingeschränkt nutzen, einschließlich der Funktionen für Berichte, Durchsetzung, Benachrichtigungen für Endnutzer und Interaktionen.

Proofpoint Email DLP-Referenzarchitektur

Wechselbeziehungen und Kommunikation zwischen Proofpoint Email DLP-Komponenten bei E-Mail-Unternehmensanwendern



Dokument-Nr.: 1207-005-04-01

Wiederherstellung nach einem Zwischenfall

Proofpoint verwaltet und betreibt die Wiederherstellung nach einem Zwischenfall vollständig innerhalb unserer Plattform. Sollte es bei einem unserer Dienste zu einer Betriebsunterbrechung kommen, wird Proofpoint unseren Plan für die Wiederherstellung nach einem Zwischenfall umsetzen. Dazu gehört auch die regelmäßige Erstellung von Lageberichten. Diese enthalten eine zusammenfassende Beschreibung des Ereignisses, die Auswirkungen auf den Kunden sowie eine Schätzung dazu, wann der normale Betrieb wieder aufgenommen werden kann. Das dokumentierte Proofpoint-Geschäftskontinuitätsprogramm beschreibt, wie Geschäftsprozesse wiederhergestellt werden. Der Plan wird mindestens einmal jährlich überprüft. Ebenfalls jährlich findet ein Tabletop-Test statt. Einzelheiten können im Rahmen einer SOC 2 Typ 1-Anfrage über Proofpoint angefordert werden.

Auch wenn die Netzwerkverbindung zu den Proofpoint-Cloud-Diensten einmal verloren gehen sollte, werden die bestehenden DLP-Regeln weiterhin durchgesetzt und über Rechnerregeln direkt auf den Agenten angewendet. Für die Durchsetzung ist keine Kommunikation mit einem Server erforderlich.

Sollte der Administrator in diesem Zeitraum Präventionsregeln ändern, erhalten die Rechner diese Änderungen erst, wenn sie wieder mit den Proofpoint-Diensten verbunden sind. Diese regelmäßige Heartbeat-Aktivität wird alle 10 Minuten ausgeführt.

Bei einem Konnektivitätsverlust speichert der Agent die ausgewählten Ereignisse, die über die Administrationskonsole in den Einstellungen „Agent Realm“ (Agentengruppe) und „Agent Policy“ (Agentenrichtlinie) definiert wurden. Sobald das Gerät wieder mit der Anwendung kommuniziert, werden die Metadaten für die ausgewählten Ereignisse hochgeladen.

Vertraulichkeit der Daten

Sie können Sicherheitskontrollen konsistent und ganzheitlich anwenden, indem Sie DLP-Regeln entwickeln, die auf Identifikatoren für vertrauliche Daten basieren.

Die Vertraulichkeit von Daten richtet sich danach, wie negativ sich die Offenlegung von Daten dieser Art auf das Unternehmen auswirken würde. Zu den Auswirkungen gehören der Verlust des Kundenvertrauens, der Verlust des Vertrauens der Aktionäre, direkte finanzielle Schäden oder Geldstrafen durch eine Aufsichtsbehörde.

DLP-Detektoren für Cloud-DLP und Endpunkt-DLP
Die hier genannten Proofpoint-DLP-Detektoren gelten nur für Cloud-DLP- und Endpunkt-DLP-Regeln. Wenn Sie die Inhaltsprüfung für Endpunkt-DLP verwenden möchten, müssen Sie wie folgt vorgehen:

- Bei der Installation des Endpunkt-Agenten muss die Komponente für die Inhaltsprüfung aktiviert oder der Agent mit dieser Komponente aktualisiert werden.
- Das Scannen von Endpunktinhalten muss für die Agentengruppe im Falle der folgenden ausgewählten Endpunktaktivitäten aktiviert werden: Web-Datei-Upload, Web-Datei-Synchronisation, Kopieren auf USB, Web-Datei-Download, Dokumentöffnung, Drucken, Einfügen aus Zwischenspeicher und Kopieren in Netzlaufwerk.
- Wenn Sie Inhalte mit DLP-Detektor-Sets scannen möchten, müssen diese zur Konfiguration der Agentengruppe hinzugefügt und für die Endpunkt-Agenten bereitgestellt werden.

Sobald die Detektoren bereitgestellt wurden, können sie in Erkennungs- oder Präventionsregeln genutzt werden. Die für den Agenten bereitgestellte Präventionsregel-Logik beinhaltet die Durchsetzung von Regeln auf den Endpunkten (Rechtfertigung oder Blockierung) sowie den Detektor für vertrauliche Daten.

Bei Cloud-Anwendungen, die mit Proofpoint Cloud DLP verbunden sind, kann das Richtlinienmodul DLP-Detektoren bereits kurz nach ihrer Konfiguration in der DLP-Anwendung verwenden. Cloud-DLP-Regeln werden so konfiguriert, dass sie Warnmeldungen innerhalb der Plattform ausgeben. Im Schreibmodus können sie jedoch Behebungsmaßnahmen basierend auf der Verbindungsart für die SaaS-Anwendungen (API oder Inline) mithilfe der Cloud-DLP-Regeln durchführen. Cloud DLP-Regeln können DLP-Verstöße in ihre Logik einbauen. Diese Regeleigenschaft wird automatisch mit den DLP-Anwendungsdetektoren synchronisiert. Das Analysemodul wird über alle Cloud-Aktivitäten in den eingebundenen SaaS-Unternehmensanwendungen informiert. In der Konsole werden konfigurierte Cloud-DLP-Warnungen angezeigt. Alle Behebungsmaßnahmen können direkt über die Warnmeldungen verwaltet und angezeigt werden.

Proofpoint DLP bietet drei Möglichkeiten zur Erkennung vertraulicher Daten, die gerade übertragen oder verwendet werden:

1. **Dateien mit einer visuellen Vertraulichkeitsbezeichnung (Microsoft Information Protection)**

   Wenn Sie ein Datenklassifizierungsprogramm haben, das Microsoft-Bezeichnungen verwendet, können wir Microsoft-Labels (MIP) von Mandanten identifizieren und anschließen in Regeln nutzen.

2. **Dateien mit übereinstimmenden Inhalten gemäß Definition von Proofpoint-DLP-Detektoren**

   Die Proofpoint-DLP-Detektoren identifizieren vertrauliche Inhalte mithilfe von vorab konfigurierten intelligenten Identifikatoren, sofort einsatzbereiten oder anwenderdefinierten Schlüsselwörtern, Klassifizierern usw.

3. **Dateien mit kontextbezogenen Markierungen wie Metadaten (Dateiname, Pfad, Dateierweiterung, echter Dateityp, Dokumenteigenschaften) oder Dateien aus überwachten URLs**

   In Proofpoint Endpoint DLP werden Dateien, die mit einem unterstützten Browser auf einen Endpunkt heruntergeladen werden, automatisch überwacht, einschließlich alle Aktivitäten mit der Datei auf dem Gerät (z. B. Kopieren, Verschieben, Löschen, Umbenennen). Sobald die Datei den Rechner über einen bestimmten Ausgangskanal wieder verlässt, endet die Überwachung. Alle Aktivitäten im Zusammenhang mit überwachten Dateien werden vom Agenten aufgezeichnet. Der Verlauf kann in einer Zeitleiste angezeigt werden.

   Überwachte Dateien stammen daher immer von URLs, mit denen ein Browser nach den Dateien sucht (auch bekannt als Ressourcen-URL für die Ursprungsüberwachung). Sie kann vom Endpunkt-Agenten für Erkennungs- und Präventionsregeln verwendet werden, um das Verhalten von Dateien, die von vertraulichen Webdiensten stammen, zu überwachen und zu kontrollieren.

DLP-Detektoren für E-Mail-DLP

DLP-Regeln für E-Mail-DLP müssen in der E-Mail-Sicherheitslösung von Proofpoint (PPS/PoD) konfiguriert werden. Das betreffende Verfahren gehört jedoch nicht zum Thema des vorliegenden Dokuments.

Das in unserer E-Mail-Sicherheitslösung enthaltene Modul für gesetzliche Compliance ist so konfiguriert, dass es die erforderlichen Scans durchführt, die erforderlichen Warnmeldungen auf Basis einer E-Mail-DLP-Regel protokolliert und die kanalinternen Verarbeitungsprozesse implementiert. Es stehen mehrere Behebungsstrategien zur Verfügung: Verschieben der Meldung in einen lokalen Quarantäneordner, Verschlüsseln der Meldung, Senden einer E-Mail-Antwort an den Endnutzer und Löschen der Nachricht oder Anzeigen einer intelligenten Antwort mit der Bitte, die Nachricht zu überprüfen, bevor sie genehmigt werden kann.

Alle Aktivitäten, die gegen eine E-Mail-DLP-Richtlinie verstoßen, werden anschließend in den Warnmeldungen angezeigt. Dazu gehören auch E-Mail-Details, die direkt von einem Administrator heruntergeladen und überprüft werden können.

Identifikatoren, Detektoren und Detektor-Sets

Unsere Detektorenausdrücke sind in einer proprietären Syntax geschrieben, die boolesche Kombinationen für fünf Bedingungstypen verwendet: Smart-IDs, Wörterbücher, Proximitätseinschluss/-ausschluss sowie EDM- und IDM-Datensätze. Die Reihenfolge ihrer Verarbeitung wird mit Klammern () angegeben. Bei den überwachten URLs handelt es sich um bestimmte URLs (bzw. Listen von URLs), die für den Agenten sichtbar sind, wenn eine Datei mit einem Browser heruntergeladen wird.

Bei benutzerdefinierten Wörterbüchern handelt es sich um Listen mit kundenspezifischen Begriffen, mit denen DLP-Detektoren in Dateien nach potenziell vertraulichen Daten suchen. Wenn eine Datei gescannt wird, vergleicht ein Detektor alle Wörter und Ausdrücke in der Datei mit allen Begriffen in den aktivierten Wörterbüchern.

Benutzerdefinierte Smart-IDs sind tiefer in die Plattform integriert und werden von Proofpoint-Entwicklern verwaltet. In einigen Fällen müssen sie erstellt werden, um Werte mithilfe von Prüfsummen zu verifizieren, z. B. die Nummer einer Kundenkarte oder einen Algorithmus, der reguläre Ausdrücke und Code verwendet.

Ein großer Teil des Aufwands bei der erstmaligen Bereitstellung entfällt auf die Verfeinerung und Optimierung der Markierungen für vertrauliche Daten. Dieser Schritt reduziert jedoch die Zahl der falsch-positiven Warnmeldungen und verbessert die Genauigkeit.

Detektoren für das Scannen von Inhalten geben die Übereinstimmungsbedingungen für vertrauliche Daten auf Basis der eingebundenen Wörterbücher und Smart-IDs an.

Detektor-Sets enthalten die vom Endpunkt-Agenten verwendeten DLP-Detektoren und müssen in die Konfigurationseinstellungen der Agentengruppe aufgenommen sowie bereitgestellt werden.

Zu den erweiterten Funktionen zur Inhaltsprüfung gehören außerdem:

- Optische Zeichenerkennung zur Verarbeitung von Bildern in extrahierten Texten (zur DLP-Analyse)
- Exakter Datenabgleich für die hochpräzise Erkennung durch mehrspaltige Übereinstimmungen in strukturierten Tabellendaten
- Abgleich indexierter Dokumente (per Dokumenten-Fingerabdruck) beim Hochladen unstrukturierter Dateien und Durchführen von Ähnlichkeitsanalysen für Dateien, die über einen Egress-Kanal übertragen werden

Aufgrund von Ressourcenbeschränkungen sind derzeit keine erweiterten Funktionen auf dem Endpunkt-Agenten verfügbar. Diese Einschränkung entfällt jedoch, wenn der Scanvorgang in der Cloud stattfindet. Diese Funktionen sind daher nur für Proofpoint Cloud DLP und Proofpoint Email DLP verfügbar.

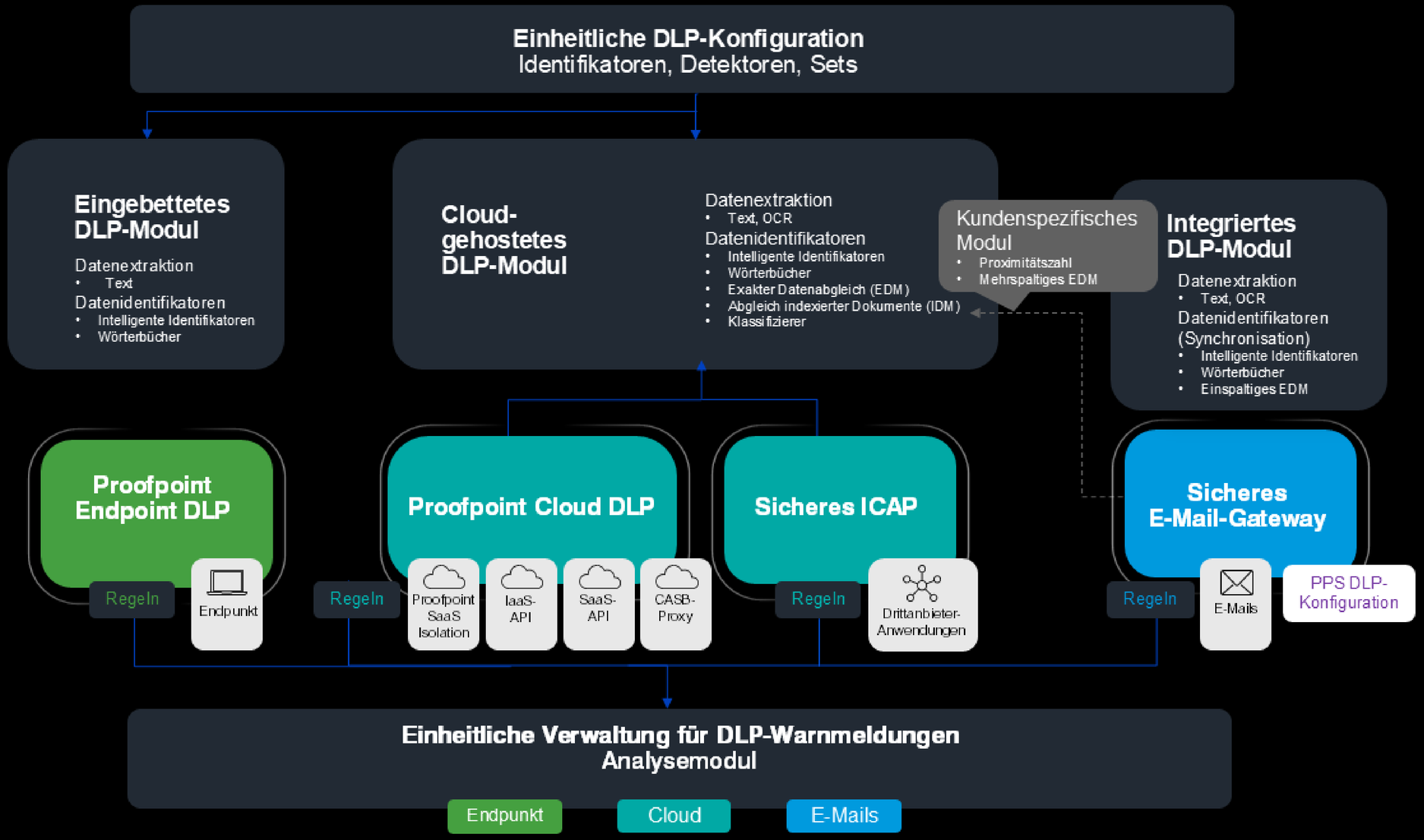
Offline-Archiv/Datenexport

Mit unserer Datenexportfunktion können Sie Ihre Daten außerhalb von Proofpoint sicher replizieren. Dabei legen Sie fest, welche Daten Sie exportieren möchten (z. B. Aktivitätsdaten, Warnmeldungen und Ereignisse). Für die exportierten Daten gelten keine Aufbewahrungsfristen. Nach dem Export können Sie die Daten bearbeiten, um sie zu analysieren und zu korrelieren.

Daten können in einen kundeneigenen AWS S3/Azure-Bucket jenseits der Proofpoint-Umgebung repliziert und von dort in andere Analysetools wie SIEMs und Data Lakes übertragen werden.

Die Daten werden immer mit dem Stand von 15 Minuten vor der tatsächlichen Auslösung des Exports exportiert. Der Export findet alle 15 Minuten statt.

Datenextraktion und Identifikatoren nach DLP-Kanal



Dokument-Nr.: 1207-005-04-01

proofpoint.

Mehr unter Proofpoint.com/de

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 85 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter www.proofpoint.de.