proofpoint®

Proofpoint Information Protection

Architecture des solutions

Protégez les personnes. Défendez les données.

Composants de la solution Proofpoint Information Protection

Proofpoint Information Protection repose sur Proofpoint Nexus, une suite de technologies optimisées par l'IA. Ces technologies sont conçues pour identifier les données sensibles, prévenir les fuites de données et bloquer les menaces internes sur plusieurs canaux. Nexus s'appuie sur des modèles de langage avancés et l'analyse comportementale pour détecter les éventuels partages de données sensibles par des utilisateurs, qu'ils soient accidentels ou délibérés. Il peut également identifier les comportements inhabituels, par exemple lorsque des utilisateurs non autorisés accèdent à des données ou les déplacent.

La solution propose également un contrôle granulaire au moyen de stratégies automatisées capables de bloquer ou de corriger les activités à risque en temps réel. En mettant en corrélation les mouvements des données et l'accès à celles-ci, d'une part, et les comportements des utilisateurs, d'autre part, Nexus contribue à protéger les données sensibles, telles que les données personnelles, les données du secteur des cartes de paiement et d'autres contenus classés, au niveau de la messagerie, des endpoints et des applications cloud.

Par ailleurs, Nexus améliore les capacités de Proofpoint Data Loss Prevention (DLP) en unifiant la gestion et l'analyse grâce à l'IA avancée. Les équipes de sécurité peuvent ainsi surveiller les mouvements des données et l'accès à celles-ci, tout en assurant la conformité aux réglementations en matière de confidentialité, comme le RGPD et la loi HIPAA. Les entreprises peuvent alors adapter les stratégies à leurs besoins, ce qui offre une protection ciblée sans perturber les opérations métier légitimes.

Proofpoint Information Protection comprend plusieurs produits et la plupart des produits suivants peuvent être intégrés à la solution.

Proofpoint Insider Threat Management (ITM) et Proofpoint Endpoint DLP préviennent les fuites de données et les atteintes à la réputation imputables à la malveillance, à la négligence ou au manque de connaissances des utilisateurs internes. Proofpoint met en corrélation les activités des utilisateurs et les mouvements des données, ce qui vous permet d'identifier les risques liés aux utilisateurs, de détecter les compromissions de données induites par des utilisateurs internes et d'accélérer la réponse aux incidents. Il vous aide également à prévenir l'exfiltration de données via des clés USB, des dossiers de synchronisation cloud, des impressions, etc. Son agent d'endpoint léger unique vous offre la flexibilité nécessaire pour surveiller les utilisateurs quotidiens et à risque, ainsi que les collaborateurs à haut risque.

Proofpoint Cloud DLP combine des fonctionnalités de sécurité des données centrée sur les personnes (y compris une DLP en ligne) et de gouvernance des applications cloud. Il protège les données sensibles, gère les applications OAuth et vous aide à préserver votre conformité aux réglementations en matière de confidentialité et de sécurité des données. Cette solution CASB multimodale prend en charge des modèles de déploiement basés sur API et proxy, notamment la DLP pour les terminaux personnels utilisés sur le lieu de travail (BYOD).

Proofpoint Email DLP contribue à prévenir les fuites de données sensibles par email. Il vous aide également à vous conformer aux exigences réglementaires, telles que celles de la norme PCI, du RGPD, des codes PII et SOX, de la loi HIPAA et des diverses lois de protection des données personnelles, grâce à des stratégies prêtes à l'emploi qui s'alignent sur ces normes. Vous pouvez par ailleurs créer des dictionnaires personnalisés, y compris une classification optimisée par l'IA, pour identifier et protéger les données propres à votre entreprise. Proofpoint Email DLP est facile à déployer. Vous pouvez le configurer dans le cadre d'un système de sécurité de la messagerie existant, ou l'intégrer à un programme DLP à l'échelle de l'entreprise.

Proofpoint Adaptive Email DLP s'appuie sur l'IA comportementale pour identifier les comportements normaux de vos collaborateurs en matière d'envoi d'emails, leurs relations de confiance et la façon dont ils communiquent des données sensibles. Il analyse ensuite chaque email pour détecter les comportements anormaux et informe les administrateurs des fuites de données potentielles. Il avertit les utilisateurs en temps réel et prévient les fuites de données sensibles par email. À l'heure actuelle, Proofpoint Adaptive Email DLP ne peut pas être intégré à notre plate-forme Proofpoint Information Protection, de sorte que nous n'en discuterons pas plus avant dans ce document.

Proofpoint Information Protection est entièrement hébergé en mode SaaS. Son application backend Analytics propose des fonctionnalités unifiées de gestion et de génération de rapports, notamment des visualisations, une détection des anomalies, des requêtes de Big Data, des vérifications assistées par machine et une gestion des dossiers. Elle offre également des tableaux de bord vous permettant de surveiller votre niveau de sécurité, les tendances de sécurité et les risques de non-conformité en temps réel. La solution permet de générer des rapports comprenant des indicateurs à l'attention des dirigeants.

Architecture logique de Proofpoint Enterprise DLP

La solution Proofpoint Enterprise DLP fournit aux administrateurs de la sécurité des outils pour protéger les données sensibles et enquêter efficacement sur les incidents au sein des environnements, ce qui réduit considérablement les risques de compromission de données auxquels l'entreprise est exposée.

Sur le plan de la gestion des incidents, le principal objectif de la solution DLP est de mettre à disposition une console unique pour réduire le temps consacré à l'analyse des journaux d'investigation numérique, accélérer les investigations et la correction des incidents et, plus généralement, accroître l'efficacité des équipes.

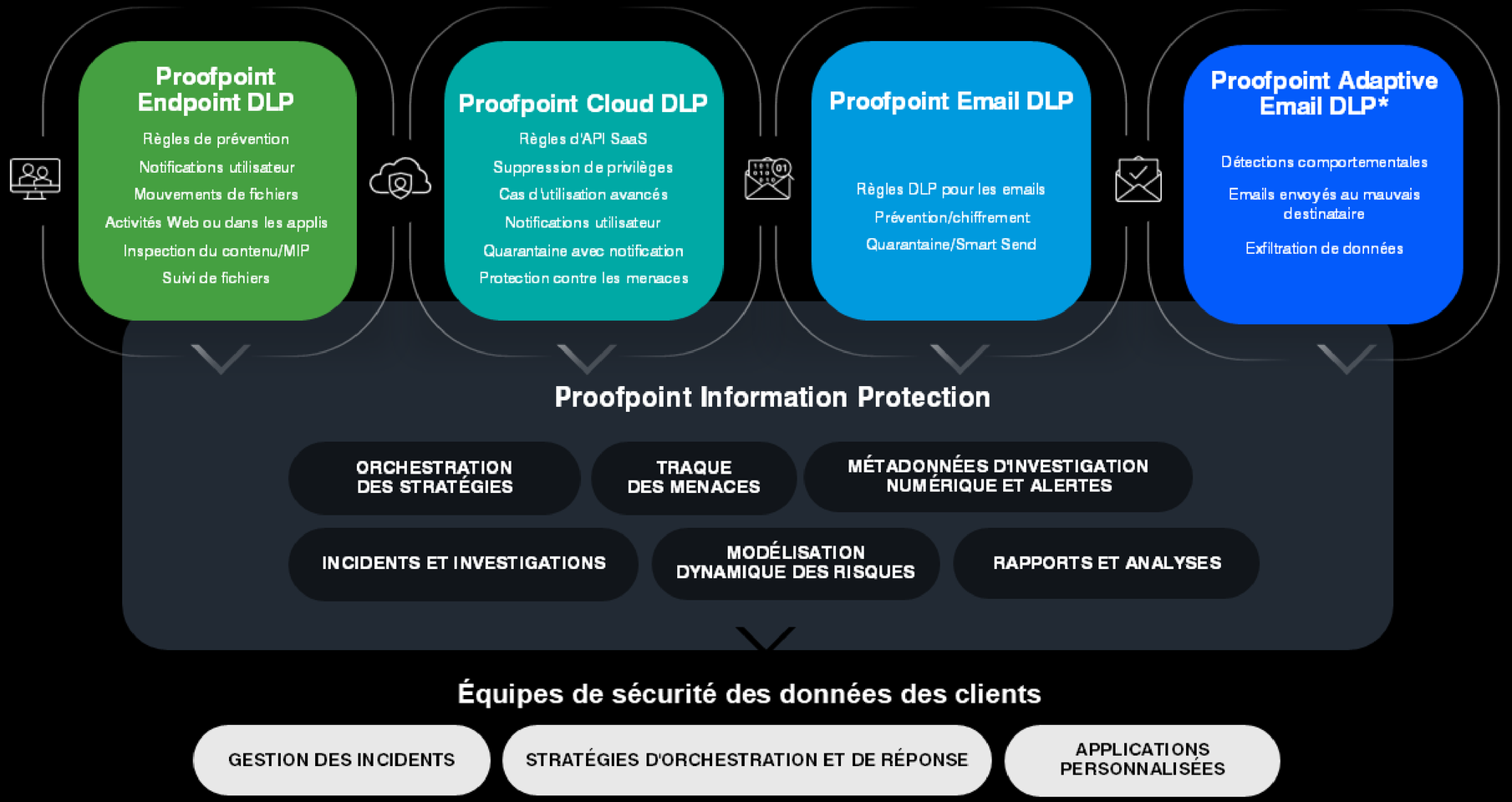
Plusieurs composants de détection distincts fonctionnent ensemble au sein d'une solution intégrée. Une architecture de solution décrit la configuration ainsi que les règles et stratégies pour la mise en œuvre du produit. Elle définit clairement les risques pour l'entreprise et les éléments moteurs du programme DLP.

Des règles propres à l'entreprise peuvent ainsi être créées pour offrir visibilité et contrôle d'activités désignées impliquant des informations d'entreprise. Des règles DLP peuvent être créées pour avertir un analyste des incidents de sécurité ou orchestrer une correction automatique intracanale. Des règles granulaires permettent la mise en œuvre de fonctionnalités de réponse flexibles pour éviter le blocage d'activités métier légitimes.

En outre, les incidents majeurs et les activités à haut risque peuvent être facilement identifiés, réunis, exportés et partagés avec les équipes responsables. Cela réduit la charge de travail et les coûts associés à la gestion des incidents, et permet aux équipes de mieux protéger l'entreprise et ses utilisateurs contre les conséquences négatives des fuites de données.

Architecture de référence de Proofpoint Enterprise DLP

Voici comment se présente le flux d'activité et de communication entre les composants de la solution DLP :

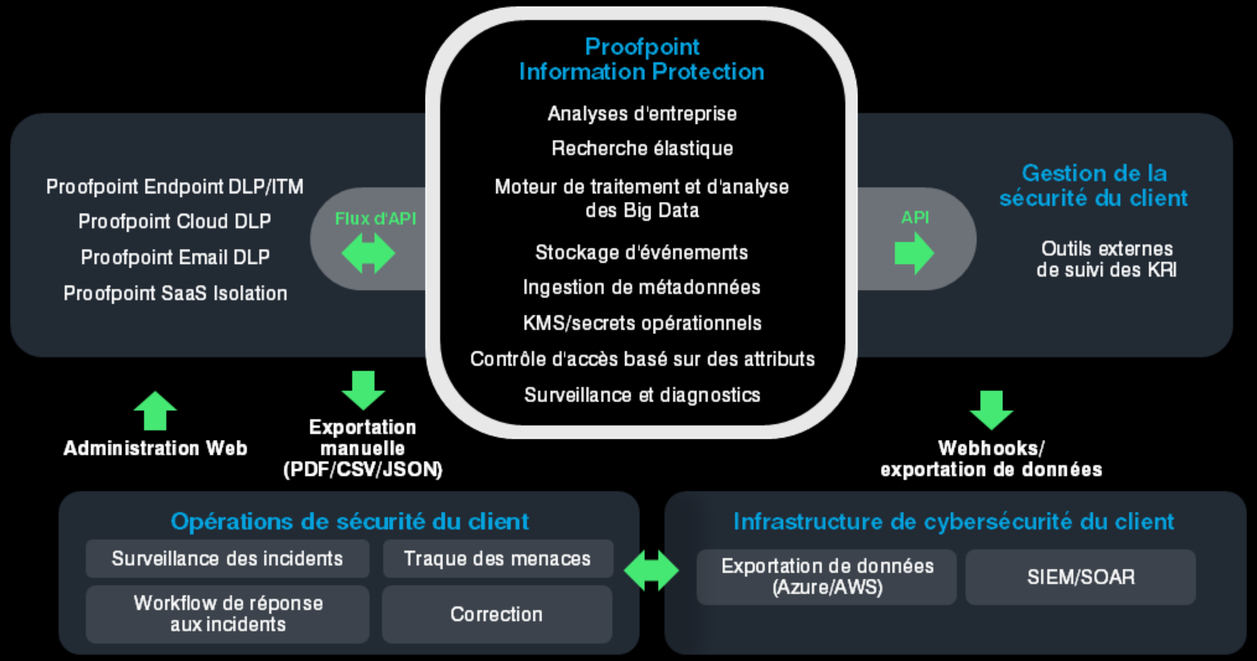


* Intégration à venir

Document n° 1207-005-03-01

Analyse unifiée pour Proofpoint Information Protection

Architecture d'analyse unifiée pour Proofpoint Information Protection au niveau des endpoints, du cloud et de la messagerie



Analyse unifiée pour la gestion des alertes, les investigations et la réponse

Le gestionnaire d'alertes unifié fournit des analyses de données et des rapports pour tous les événements collectés par la solution. Il vous permet également de gérer les workflows d'alerte. De nombreux cas d'utilisation avancés sont pris en charge par cette fonctionnalité d'analyse de données, tels que les explorations dans le cadre de la traque des menaces, la détection des anomalies et le tri des alertes assisté par machine.

L'application Analytics vous permet de créer des règles de détection spécifiques, lesquelles génèrent à leur tour des alertes qu'un analyste des incidents de sécurité peut trier. En cas d'infraction, un email ou un événement de webhook sortant contenant les détails de l'alerte est envoyé à une application réceptrice tierce, comme une solution SIEM/SOAR ou un système de messagerie instantanée.

Les outils SIEM de Splunk et d'autres éditeurs de solutions peuvent être intégrés à Proofpoint Information Protection afin d'offrir une vue unifiée des menaces internes, des déplacements latéraux et des exfiltrations de données. Vous pouvez ainsi identifier rapidement les utilisateurs impliqués et mettre en corrélation les informations avec d'autres sources d'événements.

Notre plate-forme peut aussi informer ServiceNow de toute exfiltration de données ou violation de la conformité via des intégrations. ServiceNow peut alors avertir ses clients et créer d'autres tickets ou workflows en fonction des alertes. Une intégration avec la DLP ServiceNow accélère les investigations et la réponse.

Accès à la plate-forme et contrôles de la confidentialité

Les collaborateurs de Proofpoint n'ont jamais accès à vos données, sauf si votre équipe décide de les partager avec eux. Si vous leur octroyez un accès, les membres du personnel de Proofpoint ou de votre équipe peuvent utiliser Proofpoint User Center pour se connecter au système. Un accès peut également leur être attribué à l'aide d'un profil, c'est-à-dire un utilisateur temporaire.

Les alertes doivent être configurées autour de l'utilisation d'un compte administrateur à privilèges élevés. Pour assurer la sécurité du compte, le mot de passe associé doit être modifié. Il peut également être mis sous séquestre ou réparti entre les parties responsables.

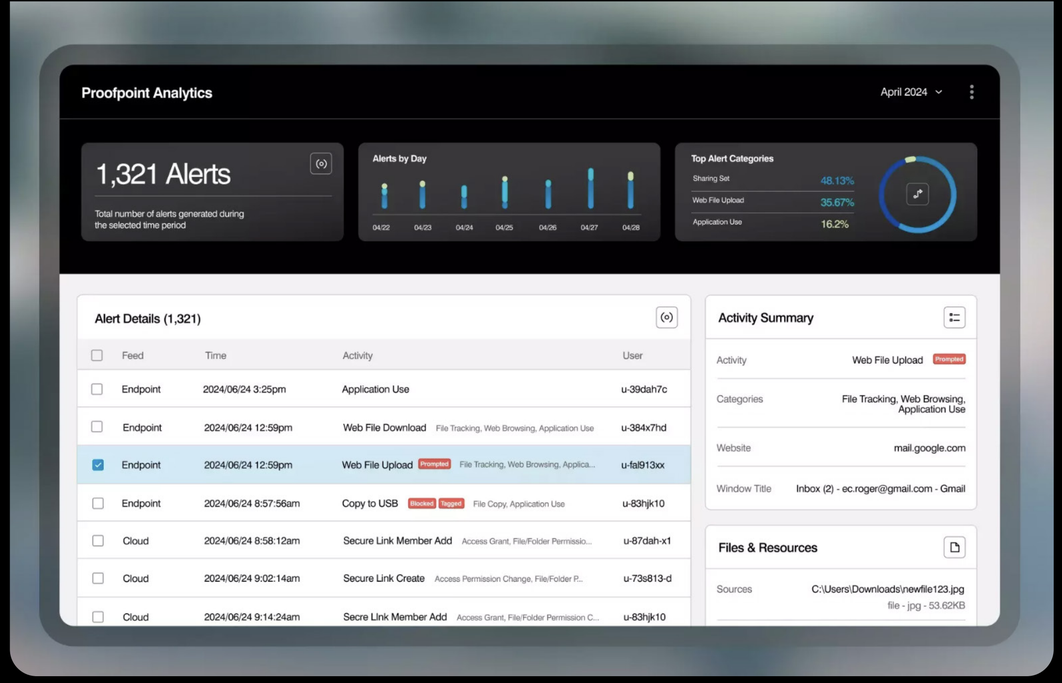
Il est fortement conseillé d'utiliser le protocole SAML ou OAuth 2.0 pour intégrer des méthodes d'authentification cloud, telles que l'authentification unique (SSO) et l'authentification multifacteur (MFA). Vous avez également la possibilité de connecter plusieurs fournisseurs d'identité.

Pour ce faire, vous devez accéder à Administration > User Management (Administration > Gestion des utilisateurs) dans la plate-forme Proofpoint Information Protection pour configurer un fournisseur d'identité à l'aide des paramètres requis. Vous devez également configurer votre fournisseur d'identité de sorte qu'il se connecte à la plate-forme Proofpoint Information Protection.

Le compte administrateur bénéficie d'un accès total et désanonymisé à l'ensemble des paramètres et données de la plate-forme. Les identifiants de connexion doivent par conséquent être protégés et considérés comme hautement confidentiels. Des comptes administrateur locaux supplémentaires peuvent être créés lors des tests produit sous Administration > User Management (Administration > Gestion des utilisateurs). Chaque compte peut se voir attribuer ses propres stratégies d'accès selon les besoins. Toutefois, dans la plupart des cas, l'ajout d'administrateurs nécessitera de limiter leur contrôle et leur accès administrateur.

Proofpoint Information Protection repose sur des principes de confidentialité dès la conception. Seules les personnes qui en ont vraiment besoin peuvent accéder aux données sensibles et aux informations d'identification des utilisateurs. Proofpoint dispose de centres de données régionaux aux États-Unis, en Europe, en Australie, au Canada (fin 2024) et au Japon (données des endpoints uniquement). Vous pouvez donc séparer les données d'un point de vue géographique. Ainsi, un groupement aux États-Unis peut gérer les données des États-Unis, qui sont envoyées au centre de données des États-Unis. Des stratégies d'accès granulaires permettent à votre administrateur d'attribuer un accès afin qu'un analyste en sécurisé basé aux États-Unis ne puisse voir que les données des États-Unis.

Avec Proofpoint Information Protection, les administrateurs système peuvent également configurer les données d'investigation numérique (données personnelles, données médicales personnelles et données du secteur des cartes de paiement) qu'ils souhaitent masquer dans la console et dissimuler l'identité d'un utilisateur pour éliminer les biais de la part des analystes. Vous pouvez anonymiser le nom d'utilisateur, le nom d'hôte, l'adresse IP, les informations de localisation et les noms de fichiers. Lorsque l'identité d'un utilisateur doit être connue plus en aval au cours d'investigations, l'analyste en sécurité peut demander la désanonymisation des données, laquelle peut être accordée par un administrateur.



Accès à la console Web

Les administrateurs et les analystes peuvent se connecter à la plate-forme à l'aide d'un navigateur compatible. Ils peuvent gérer les stratégies et les règles, examiner les alertes, corriger directement les incidents, analyser les ensembles de données collectés et consulter les rapports en fonction des activités utilisateur capturées.

Pour gérer des sous-entités distinctes, de nombreuses entreprises peuvent accéder à plusieurs sous-locataires sur la plate-forme Proofpoint.

Notifications de la plate-forme

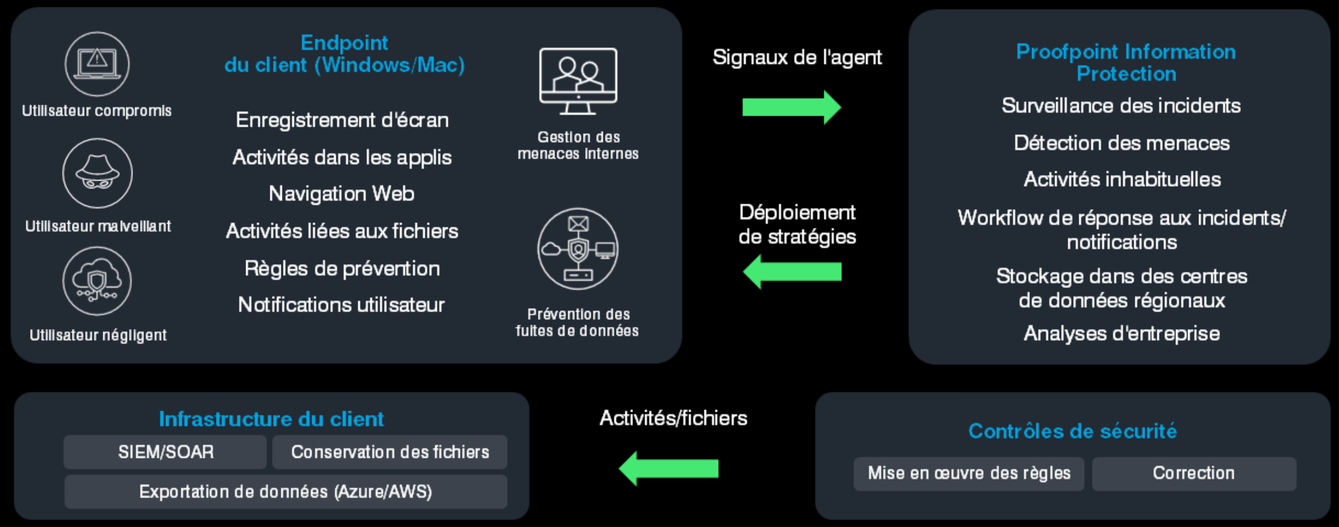
Les alertes peuvent être surveillées et traitées sur la plate-forme Proofpoint. Ces opérations peuvent également être effectuées en externe conformément à vos procédures internes de gestion des incidents. Aux fins de ces notifications, vous devez identifier les adresses email qui recevront les alertes générées par la plate-forme Proofpoint Information Protection. Des systèmes externes (SIEM, SOAR, ITSM) peuvent également être configurés pour recevoir des alertes.

Applications externes

Les applications externes peuvent accéder à la plate-forme Proofpoint via des API REST.

Architecture de référence de Proofpoint Endpoint DLP/ITM

L'agent unique de Proofpoint DLP et Proofpoint ITM collecte les données et les charge sur la plate-forme tout en appliquant des stratégies DLP.



Configuration de l'agent d'endpoint DLP/ITM

L'agent Proofpoint Endpoint DLP est installé sur des endpoints client qui exécutent des versions compatibles de Windows ou de macOS. Pour installer l'agent en production, vous devez employer des méthodes sans surveillance et vos outils standard d'installation de logiciels à distance.

Dès son déploiement, l'agent enregistre des métadonnées qui décrivent les activités des utilisateurs. Il ne requiert pas de règles explicites. Les métadonnées sont chargées et traitées de manière sécurisée par la plate-forme Proofpoint Information Protection. Pour gérer et configurer l'agent, utilisez l'application Administration > Endpoints de la plate-forme.

Les agents d'endpoint Proofpoint peuvent être déployés en mode silencieux. Chacun s'exécute dans la mémoire utilisateur en consommant un minimum de ressources et peut se mettre à jour automatiquement. Après l'installation ou une mise à niveau, aucun redémarrage du système n'est nécessaire. Les agents n'entrent pas en conflit avec les systèmes de sécurité des endpoints existants et ne perturbent pas le fonctionnement ou les performances d'autres applications.

Les agents installés et le serveur ITM communiquent de façon asynchrone via le protocole HTTP. Les agents DLP ont recours au chiffrement TLS pour communiquer avec les services cloud Proofpoint. Vous pouvez trouver les exigences en matière de pare-feu pour la connectivité sur notre portail de documentation en ligne.

Les agents qui doivent se connecter via un proxy dynamique utiliseront les paramètres de proxy définis au niveau du système d'exploitation. Celui-ci doit être configuré pour utiliser un proxy dynamique pour les applications s'exécutant sous le compte système (et non sous le compte utilisateur). Il est également possible d'utiliser un proxy statique. Ce paramètre est configuré au moment de l'installation des agents.

Certains logiciels antivirus et EDR s'exécutent à la demande et analysent les fichiers exécutables et les processus de conservation ou les empêchent de communiquer par défaut. Pour assurer la stabilité des fonctionnalités, vous devez exclure nos processus de l'inspection par d'autres outils de sécurité. Vous ne devriez pas avoir besoin de mettre sur liste d'autorisation des applications spécifiques dans notre propre outil, car il est peu probable que notre approche légère interfère avec les actions d'un agent d'endpoint en mode noyau.

Composants de l'agent d'endpoint Windows pour la mise sur liste d'autorisation
Pour mettre sur liste d'autorisation nos fichiers afin qu'ils soient exclus de l'inspection par les systèmes EDR et antivirus, veuillez consulter **ce guide.**

REMARQUE : pour afficher les notifications ou collecter des captures d'écran sous macOS, vous devez également vous assurer que les paramètres de confidentialité sont octroyés à nos processus en déployant le fichier de configuration mobile. Ce processus est détaillé dans notre documentation en ligne.

L'agent d'endpoint Proofpoint prend en charge deux types de proxys. Dans le cas d'un proxy dynamique, utilisez un fichier de configuration automatique du proxy (PAC) au niveau du système d'exploitation. Dans le cas d'un proxy statique, renseignez le nom d'hôte et le port au moment de l'installation. Pour définir les identifiants de connexion par défaut que l'agent utilisera, remplissez les champs Domaine, Nom d'utilisateur et/ou Mot de passe lors de l'installation.

Mises à jour de l'agent
En tant que plate-forme SaaS, Proofpoint peut intégrer rapidement de nouvelles fonctionnalités à l'agent. Proofpoint propose également une version avec support à long terme (LTS) de l'agent pour les clients qui ne sont pas en mesure de suivre notre calendrier de publication. Toutefois, nous conseillons généralement d'installer la dernière version de l'agent bénéficiant d'un support.

Nous recommandons l'utilisation du service de mise à jour automatique pour maintenir les agents à jour, conformément à une stratégie de mise à jour préconfigurée. Lorsqu'un administrateur décide de mettre à jour l'agent, il lui suffit de modifier ou de créer une stratégie définissant la version cible et les conditions d'application de la mise à niveau. L'outil de mise à jour de l'agent s'exécute sur les endpoints, puis s'assure que les bonnes versions sont téléchargées et installées automatiquement.

Certificat racine
Les endpoints installés doivent disposer d'un certificat racine valide. Proofpoint signe l'agent avec un certificat racine valide pour s'assurer que le client sait qu'il provient de Proofpoint. Ce certificat dépend d'un certificat racine valide et possède une date d'expiration annuelle.

Surveillance de l'intégrité de l'agent
Des informations sur l'intégrité de l'agent, telles que les erreurs et l'horodatage des derniers enregistrements, sont visibles sous Administration > Endpoints > Endpoint Catalog (Administration > Endpoints > Catalogue d'endpoints). L'agent Windows possède des capacités d'autoguérison et inclut un service cloud de surveillance qui redémarre l'agent en cas de désactivation ou d'arrêt de ce dernier. Le processus de journalisation de l'agent Mac est également lancé, ce qui redémarre l'agent en cas de désactivation ou d'arrêt de ce dernier.

Renforcement de l'agent
La configuration de l'agent et les fichiers journaux sur les endpoints peuvent être entièrement chiffrés. Pendant l'installation, des mesures de renforcement supplémentaires, comme l'utilisation d'une clé de sécurité pour empêcher la désinstallation de l'agent ou l'attribution d'un nouveau nom à ses processus, peuvent également être appliquées.

Configuration du groupement d'endpoints
Les groupements d'agents séparent les agents en fonction de l'emplacement de stockage régional et de la durée de conservation des données.

Des règles de prévention au niveau des endpoints sont déployées au moyen de stratégies d'agent différenciées. Elles exécutent des actions telles que l'affichage d'avertissements ou le blocage de l'utilisateur. En parallèle, l'agent journalise les signaux de métadonnées concernant les activités de l'utilisateur liées aux applications. Ces journaux sont envoyés au moteur d'analyse de Proofpoint à des fins de traitement. Les captures d'écran sont facultatives.

Les données traitées sont stockées dans le centre de données AWS régional souhaité (États-Unis, Europe, Asie-Pacifique, Japon et Canada à l'heure actuelle) en fonction du paramètre de groupement d'agents sélectionné.

Paramètres des stratégies d'agent
Les stratégies d'agent définissent le contenu capturé par l'agent Proofpoint et sont attribuées à des groupements d'agents. Vous pouvez donc configurer des paramètres et les appliquer simultanément aux endpoints de plusieurs groupements.

Vous pouvez attribuer plusieurs stratégies d'agent à un groupement d'agents. Dans ce cas, vous pouvez les classer dans l'ordre de votre choix afin de définir plus précisément les paramètres appliqués aux différents agents. Cet ordre détermine les paramètres qui sont activés conformément à la stratégie d'agent.

Prévention au niveau des endpoints et notification des utilisateurs

La modification des comportements des utilisateurs en vue de réduire le risque de compromission de données constitue une composante essentielle de tout programme DLP ou de gestion des risques internes efficace. Lorsque des règles DLP sont déployées sur des endpoints managés, elles peuvent être utilisées pour bloquer les infractions aux stratégies ou en avertir les utilisateurs, ce qui a pour effet d'influencer leur comportement et de réduire ainsi le risque de compromission de données.

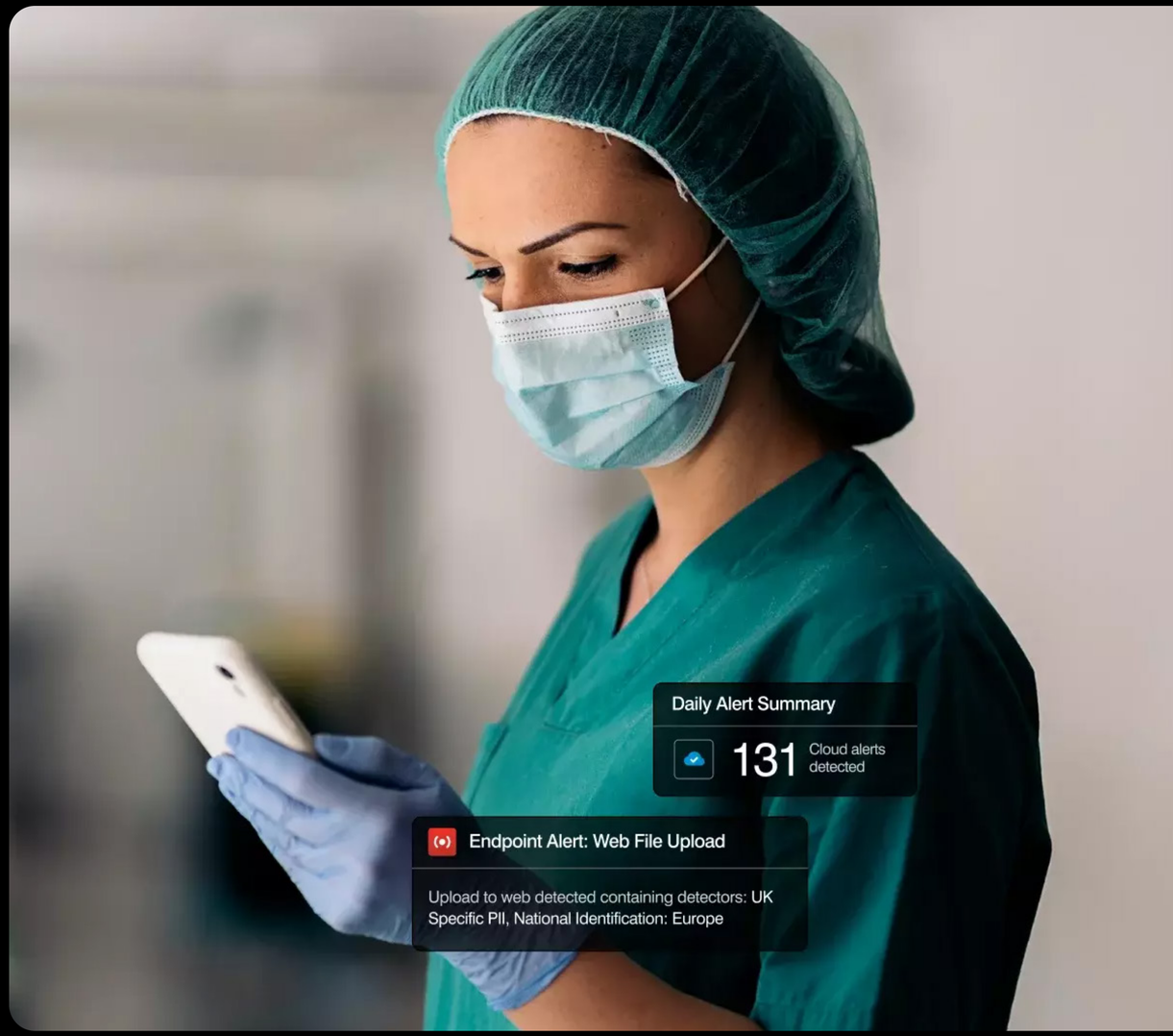
Les règles DLP sont conçues pour modifier les comportements des utilisateurs lorsque des informations d'entreprise sensibles sont exfiltrées. Au début, une approche courante consiste à surveiller ce que font les utilisateurs grâce aux métadonnées d'activité dans les alertes ou les explorations. Lorsque les équipes examinent les alertes, elles peuvent les utiliser pour ajuster les règles de manière à les aligner sur les priorités et les processus de détection des incidents de l'entreprise.

Une fois ce processus mature, des règles peuvent être déployées. À ce stade, lorsque les utilisateurs ne respectent pas les stratégies, ils seront empêchés d'effectuer une action et notifiés par un message de blocage. Pour poursuivre leur activité, ils seront invités à sélectionner une justification prédéfinie ou personnalisée.

Les notifications adressées aux utilisateurs sont généralement personnalisées avec un message qui décrit la stratégie enfreinte. Elles incluent également le logo officiel de l'entreprise et un lien vers une page Web qui détaille ses stratégies de sécurité. La taille de l'image importée pour le logo de l'entreprise doit être inférieure à 56 Ko (type MIME image/*).

Les utilisateurs découvrent les étapes à suivre lorsqu'une activité est bloquée ou comment formuler une plainte concernant l'interruption. Il est également judicieux d'inclure un lien vers la page intranet consacrée à la sécurité d'entreprise, qui explique la nécessité d'un tel programme DLP.

Les règles de détection génèrent des alertes dans notre application Analytics, où un spécialiste de la réponse aux incidents peut les gérer. Elles passent en revue les métadonnées collectées, qui sont générées par certaines activités des utilisateurs sur les endpoints. Les métadonnées sont enregistrées par l'agent conformément aux paramètres de la stratégie d'agent, tels que la fréquence et la résolution des captures d'écran, et sont gérées dans la console d'administration.



Configuration de Proofpoint Cloud DLP

Proofpoint Cloud DLP prend en charge une architecture sans agent. Il utilise des API cloud pour protéger les principales applications cloud. Il offre également une fonctionnalité DLP en ligne pour les terminaux BYOD en utilisant l'isolation du navigateur dès qu'un utilisateur s'authentifie pour accéder à une application cloud.

Proofpoint Cloud DLP se connecte aux principaux services cloud d'une entreprise et à ses applications SaaS/IaaS approuvées via les API correspondantes. Vous bénéficiez ainsi de fonctionnalités bidirectionnelles, notamment d'une correction des incidents de sécurité cloud, en temps quasi réel.

Proofpoint Cloud DLP est extrêmement puissant. Il assure une correction avec la même pile de détecteurs DLP que celle utilisée par Proofpoint Endpoint DLP.

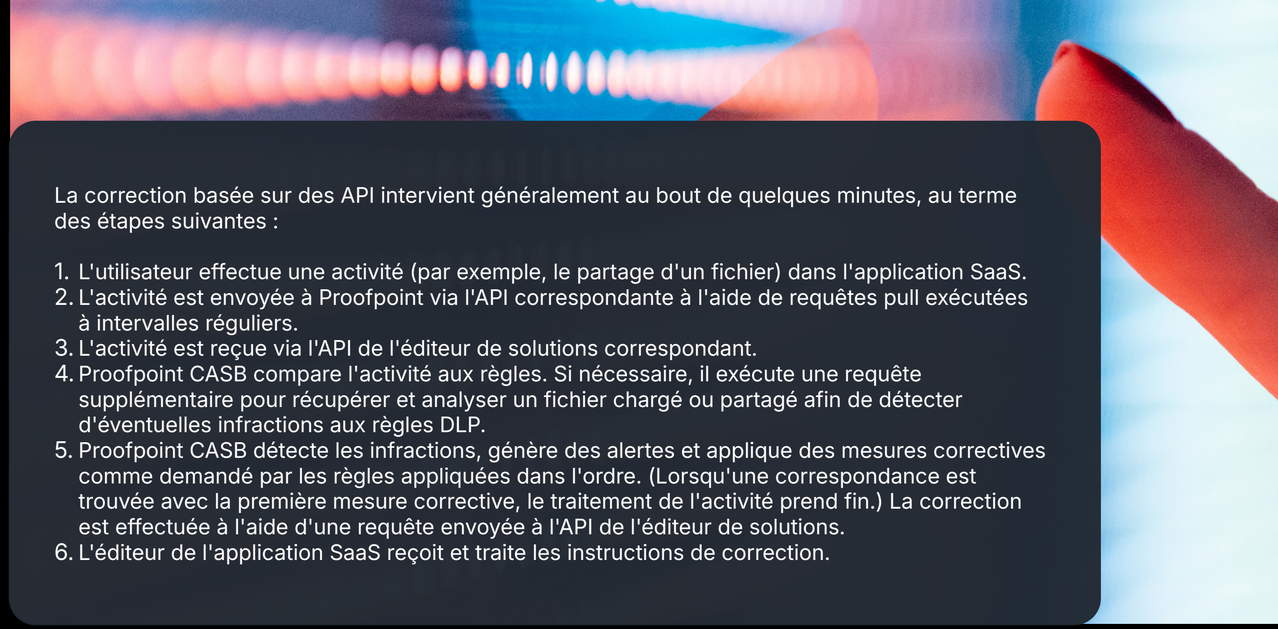
Proofpoint CASB Adaptive Access Controls étend les capacités de Proofpoint Cloud DLP à un large éventail de cas d'utilisation avancés en temps réel, tels que la reconnaissance et le blocage de terminaux non managés, ainsi que l'accès à partir d'emplacements à haut risque par le biais de notre intégration SAML/OIDC avec des fournisseurs d'identité cloud.

Vous pouvez bénéficier d'un contrôle DLP encore plus granulaire sur les chargements et téléchargements de fichiers via un navigateur à l'aide d'une intégration avec Proofpoint SaaS Isolation — et ce sans agent. La solution est donc adaptée à la DLP sur les terminaux BYOD. Notez que les connecteurs API Okta pour Proofpoint simplifient les intégrations SAML. Nous pouvons appliquer automatiquement des contrôles adaptatifs pour les applications fédérées par Okta.

Moyennant une étape supplémentaire, des services IaaS tels qu'Azure et AWS peuvent être configurés pour la surveillance DLP. Proofpoint facture ces API séparément.

Au début, les API d'éditeurs de solutions pour certaines de vos applications cloud d'entreprise seront connectées à Proofpoint Cloud DLP à des fins de surveillance de la sécurité.

Vous pouvez créer des règles spécifiques dans Proofpoint Cloud DLP afin d'identifier et de corriger les infractions aux stratégies DLP d'entreprise dans les services cloud. Vous pouvez également appliquer des règles de gouvernance automatisées aux applications OAuth tierces, qui maintiennent l'accès des systèmes et données à vos principaux services SaaS et d'entreprise, tels que Microsoft 365 et Google Workspace.



La correction basée sur des API intervient généralement au bout de quelques minutes, au terme des étapes suivantes :

1. L'utilisateur effectue une activité (par exemple, le partage d'un fichier) dans l'application SaaS.
2. L'activité est envoyée à Proofpoint via l'API correspondante à l'aide de requêtes pull exécutées à intervalles réguliers.
3. L'activité est reçue via l'API de l'éditeur de solutions correspondant.
4. Proofpoint CASB compare l'activité aux règles. Si nécessaire, il exécute une requête supplémentaire pour récupérer et analyser un fichier chargé ou partagé afin de détecter d'éventuelles infractions aux règles DLP.
5. Proofpoint CASB détecte les infractions, génère des alertes et applique des mesures correctives comme demandé par les règles appliquées dans l'ordre. (Lorsqu'une correspondance est trouvée avec la première mesure corrective, le traitement de l'activité prend fin.) La correction est effectuée à l'aide d'une requête envoyée à l'API de l'éditeur de solutions.
6. L'éditeur de l'application SaaS reçoit et traite les instructions de correction.

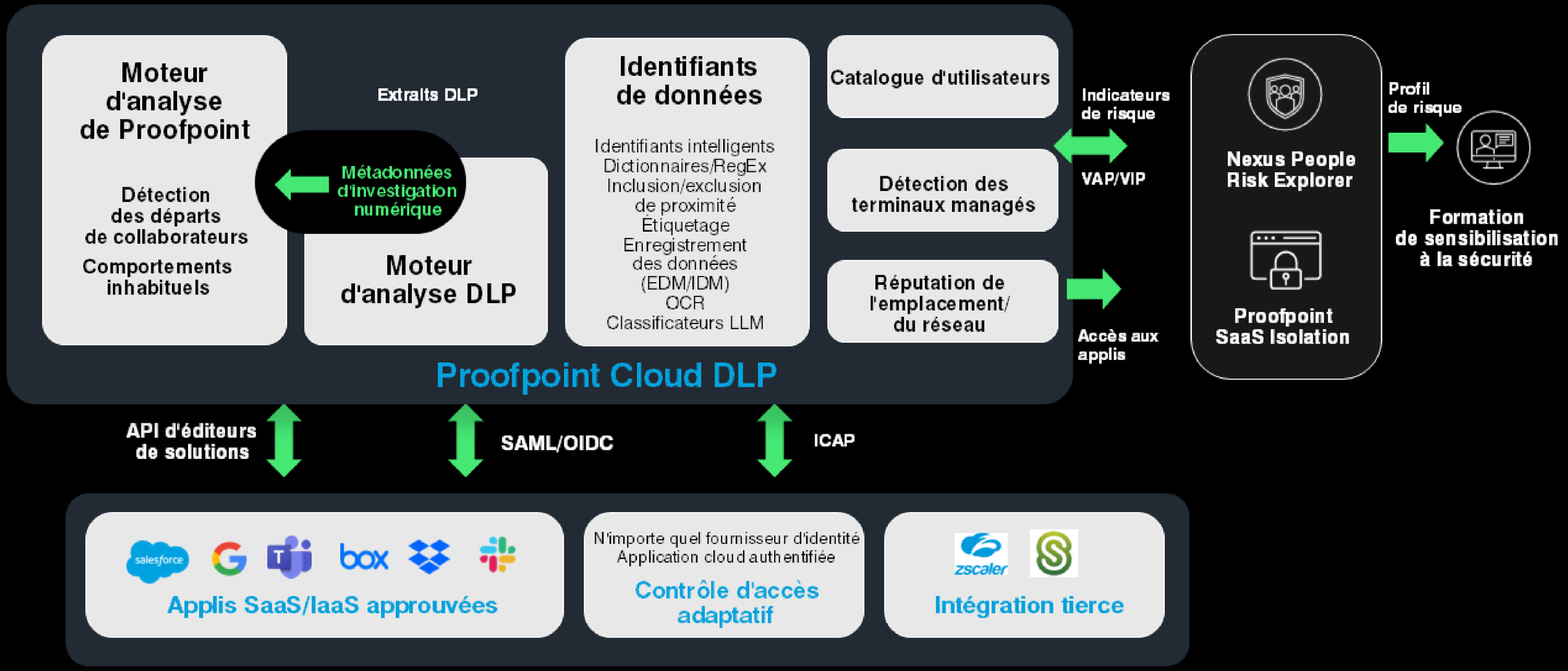
Proofpoint CASB Adaptive Access Controls permet de contrôler en ligne les applications prises en charge, et ce sans agent. Par le biais d'une intégration SAML 2.0 ou OIDC avec votre fournisseur d'identité, nous pouvons appliquer une protection supplémentaire à n'importe quelle application authentifiée à l'aide de Proofpoint Cloud DLP.

Pour configurer Proofpoint CASB Adaptive Access Controls, les demandes de connexion utilisateur doivent être redirigées via Proofpoint avant d'être authentifiées par le fournisseur d'identité. Nous pouvons ensuite appliquer une règle qui autorise l'accès aux applications cloud d'entreprise approuvées, mais seulement sous certaines conditions.

Les stratégies peuvent reposer sur des paramètres tels que le fait qu'un utilisateur accède à l'application SaaS depuis un terminal non managé, en dehors de la plage sortante d'un réseau source d'entreprise, ou à partir d'un emplacement à risque, ou d'autres facteurs à haut risque. Vous pouvez bénéficier d'un contrôle encore plus granulaire sur l'accès aux applications cloud via un navigateur à l'aide d'une intégration supplémentaire avec Proofpoint SaaS Isolation. L'intégration avec notre pile DLP est alors effectuée en temps réel, sans devoir utiliser un agent.

Pour unifier davantage la DLP et offrir une visibilité sur les fuites de données multicanales, Proofpoint prend également en charge l'intégration ICAP avec Zscaler et Citrix ShareFile. Pour ce faire, vous devez configurer le client ICAP de votre application tierce en redirigeant son trafic vers notre service DLP après avoir configuré votre ensemble de détecteurs DLP pour ce canal dans notre plate-forme.

Architecture de référence de Proofpoint Cloud DLP



Document n° 1207-005-03-01

Configuration de Proofpoint Email DLP

Proofpoint Email DLP utilise une passerelle de messagerie en ligne fournie par Proofpoint pour traiter les emails sortants. Cette passerelle est intégrée à votre architecture de messagerie sortante.

Proofpoint vous conseillera sur la façon de configurer votre infrastructure et vos systèmes en fonction de votre architecture de messagerie existante, que vous testiez la passerelle de messagerie sortante de Proofpoint Email DLP ou que vous la mettiez en production.

Si vous utilisez déjà Proofpoint pour votre passerelle de messagerie sortante, Proofpoint Email DLP devra simplement être activé directement sur votre passerelle de messagerie Proofpoint existante en acquérant une licence pour le module de conformité réglementaire. Aucune modification ne sera apportée à votre flux d'emails. Il n'y a aucune conséquence pour les normes SPF et DMARC, ni pour le préchauffage d'adresses IP (« IP warmup »).

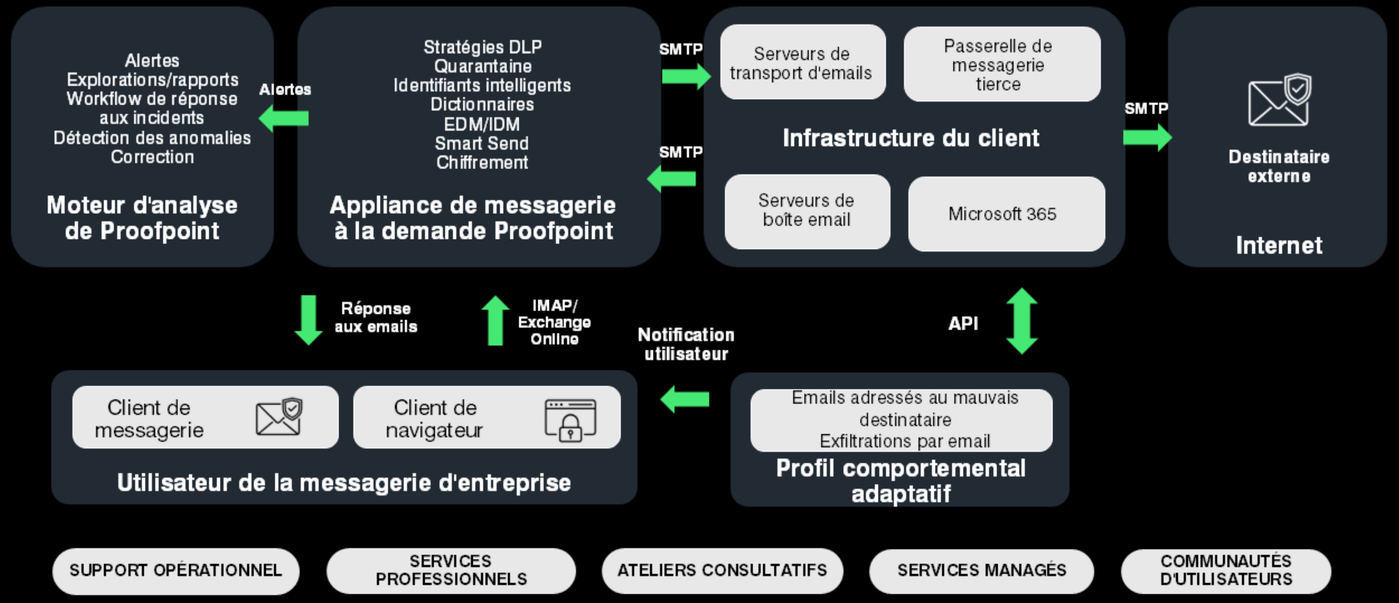
Une fois que Proofpoint Email DLP est activé, vous pouvez évaluer l'ensemble des fonctionnalités DLP, y compris la génération de rapports, la mise en œuvre, les notifications utilisateur et les interactions.

Si vous n'utilisez pas Proofpoint comme dernier tronçon de votre flux de traitement des emails, la passerelle de messagerie cloud Proofpoint sera intégrée à votre infrastructure de messagerie sortante en tant que tronçon SMTP supplémentaire. Idéalement, elle devrait être insérée avant une passerelle de messagerie existante afin d'éviter des modifications supplémentaires de l'infrastructure.

Une fois le service de messagerie sortant intégré, vous pouvez utiliser l'ensemble des fonctionnalités DLP, y compris la génération de rapports, la mise en œuvre, les notifications utilisateur et les interactions.

Architecture de référence de Proofpoint Email DLP

Interconnexion des composants de Proofpoint Email DLP et communication avec un utilisateur de la messagerie d'entreprise



Reprise après sinistre

Proofpoint gère l'intégralité de la reprise après sinistre au sein de sa plate-forme. En cas de perturbation de l'un de nos services, Proofpoint met en œuvre son plan de reprise après sinistre, qui consiste notamment à fournir des rapports réguliers sur la situation. Ces rapports incluent une brève description de l'événement, l'impact sur les clients et une estimation du retour à la normale des opérations. Le programme de continuité des activités documenté de Proofpoint décrit comment les processus métier sont restaurés. Le plan est examiné au minimum une fois par an, et une simulation est effectuée chaque année. Des détails peuvent être demandés dans le cadre d'un examen SOC 2 Type 1 via Proofpoint.

En cas d'indisponibilité des services cloud Proofpoint sur le réseau, l'application des règles DLP existantes n'est pas affectée. Toutes les règles DLP sont appliquées directement à l'agent par le biais de stratégies machine. Leur application n'exige aucune communication avec un serveur.

Si des règles de prévention sont modifiées par l'administrateur pendant cette période, les machines ne reçoivent les changements qu'une fois qu'elles ont établi une connexion avec les services Proofpoint. Cette activité se produit toutes les 10 minutes.

En ce qui concerne la détection, une perte de connectivité entraîne le stockage par l'agent des événements sélectionnés définis dans le groupement d'agents et les paramètres de la stratégie d'agent, qui sont gérés dans la console d'administration. Une fois que le terminal rétablit la communication avec l'application, les métadonnées pour les événements sélectionnés sont chargées.

Niveau de confidentialité des données

Vous pouvez appliquer des contrôles de sécurité de façon cohérente et globale en créant des règles DLP basées sur des identifiants de données sensibles.

Le niveau de confidentialité des données est défini par l'ampleur des conséquences négatives que la divulgation d'un groupe de données aurait sur une entreprise. Ces conséquences incluent l'érosion de la confiance des clients et des actionnaires, les pertes financières directes et les amendes imposées par les autorités de réglementation.

Détecteurs DLP pour Proofpoint Cloud DLP et Proofpoint Endpoint DLP
Les détecteurs DLP Proofpoint identifiés ici s'appliquent uniquement aux règles Proofpoint Cloud DLP et Proofpoint Endpoint DLP. Si vous souhaitez utiliser l'analyse du contenu pour Proofpoint Endpoint DLP, vous devez suivre ces étapes :

- Le composant d'analyse du contenu doit être activé pendant l'installation de l'agent d'endpoint. Sinon, ce dernier doit être mis à jour.
- L'analyse du contenu des endpoints doit être activée au niveau du groupement d'agents pour les activités suivantes : chargement de fichiers Web, synchronisation de fichiers Web, copie sur une clé USB, téléchargement de fichiers Web, ouverture de documents, impression, collage de texte à partir du presse-papiers et copie sur un lecteur réseau.
- Si vous souhaitez utiliser des ensembles de détecteurs DLP pour l'analyse du contenu, ces détecteurs doivent être ajoutés à la configuration du groupement d'agents et déployés sur les agents d'endpoint.

Une fois déployés, les détecteurs peuvent être utilisés dans les règles de détection ou de prévention. La logique des règles de prévention déployée sur l'agent inclut la mise en œuvre des endpoints (justification ou blocage) ainsi que le détecteur de données sensibles.

Pour les applications cloud connectées à Proofpoint Cloud DLP, le moteur de stratégies pourra utiliser les détecteurs DLP peu de temps après leur configuration dans l'application DLP. Les règles Proofpoint Cloud DLP sont configurées pour générer des alertes au sein de la plate-forme. Toutefois, en mode écriture, elles peuvent appliquer des mesures correctives en fonction du type de connexion pour les applications SaaS (API ou en ligne) à l'aide des règles de l'application Proofpoint Cloud DLP. Les règles Proofpoint Cloud DLP peuvent intégrer des infractions aux règles DLP à leur logique. Cette propriété des règles est automatiquement synchronisée avec les détecteurs de l'application DLP. Toutes les activités cloud dans les applications SaaS d'entreprise intégrées alimentent l'application Analytics. Les alertes Proofpoint Cloud DLP configurées apparaissent dans la console. Toutes les mesures correctives peuvent être gérées et visualisées directement à partir des alertes.

Proofpoint DLP reconnaît les données sensibles en mouvement et en cours d'utilisation grâce à ces trois méthodes :

1. **Fichiers comportant une étiquette de confidentialité visuelle (Microsoft Information Protection)**

   Si vous disposez d'un programme de classification des données qui s'appuie sur les étiquettes Microsoft, nous pouvons identifier les étiquettes et les identifiants de locataires Microsoft (MIP). Ceux-ci pourront alors être utilisés dans des règles.

2. **Fichiers contenant des correspondances de contenu définies par les détecteurs DLP Proofpoint**

   Les détecteurs DLP Proofpoint identifient les contenus sensibles à l'aide d'identifiants intelligents prédéfinis, de mots-clés de dictionnaires prêts à l'emploi ou personnalisés, de classificateurs, etc.

3. **Fichiers comportant des marqueurs contextuels tels que des métadonnées (nom du fichier, chemin d'accès, extension du fichier, type réel de fichier, propriétés du document) ou fichiers provenant d'URL surveillées**

   Dans Proofpoint Endpoint DLP, un fichier téléchargé sur l'endpoint à l'aide d'un navigateur pris en charge est automatiquement surveillé. Toutes les activités liées au fichier sur le terminal (copie, déplacement, suppression, changement de nom, etc.) sont surveillées. Une fois que le fichier quitte la machine via un canal de sortie spécifique, il n'est plus surveillé. Toutes les activités liées aux fichiers surveillés sont capturées par l'agent, et un historique peut être consulté dans la vue chronologique des fichiers.

   Les fichiers surveillés proviennent donc toujours d'URL utilisées par un navigateur pour localiser les fichiers. L'agent d'endpoint peut ainsi faire en sorte que les règles de détection et de prévention surveillent et contrôlent les activités effectuée sur des fichiers provenant de services Web sensibles.

Détecteurs DLP pour Proofpoint Email DLP

Les règles DLP pour Proofpoint Email DLP doivent être configurées dans la solution Proofpoint Email Security (PPS/PoD). Toutefois, ce processus ne relève pas de ce document.

Le module de conformité réglementaire de notre solution Proofpoint Email Security est configuré pour effectuer l'analyse requise, journaliser l'alerte requise en fonction d'une règle Proofpoint Email DLP, puis exécuter les actions de traitement intracanales. La correction peut consister à déplacer le message vers un dossier de quarantaine local à des fins de traitement, à chiffrer le message, à répondre à l'utilisateur par email et à supprimer le message, ou à envoyer à l'utilisateur une réponse intelligente l'invitant à examiner son propre message avant de l'approuver.

Toutes les activités qui enfreignent une stratégie Proofpoint Email DLP apparaissent alors dans les alertes. Celles-ci incluent les détails des emails, qui peuvent être téléchargés et examinés directement par un administrateur.

Identifiants, détecteurs et ensembles DLP

Les expressions de nos détecteurs sont écrites dans une syntaxe propriétaire. Elles incluent toute combinaison booléenne pour cinq types de conditions : identifiants intelligents, dictionnaires, inclusion/exclusion de proximité, et ensembles de données EDM et IDM. Leur ordre de traitement est indiqué entre parenthèses (). Les URL surveillées s'affichent sous forme (de listes) d'URL spécifiques visibles par l'agent lorsqu'un fichier est téléchargé avec un navigateur à partir de l'emplacement désigné.

Les dictionnaires personnalisés sont des listes de termes spécifiques au client qui sont utilisées par les détecteurs DLP pour localiser des données potentiellement sensibles dans les fichiers. Lorsqu'un fichier est analysé, un détecteur compare l'ensemble des mots et expressions figurant dans le fichier à tous les termes contenus dans les dictionnaires activés.

Les identifiants intelligents personnalisés sont intégrés de manière plus étroite à la plate-forme et sont gérés par l'équipe d'ingénierie Proofpoint. De tels identifiants doivent parfois être créés pour effectuer des sommes de contrôle sur des valeurs, par exemple un numéro de carte de fidélité propre à un client ou un algorithme qui utilise des expressions régulières et du code.

Une grande partie du déploiement initial est consacrée au perfectionnement et à l'ajustement des marqueurs de données sensibles. Cette approche permet de garantir un faible taux de faux positifs et un taux de précision élevé.

Les détecteurs d'analyse du contenu indiquent les conditions de correspondance pour les données sensibles en fonction des dictionnaires et des identifiants intelligents inclus.

Les ensembles de détecteurs contiennent les détecteurs DLP utilisés par l'agent d'endpoint. Ils doivent être inclus dans les paramètres de configuration du groupement d'agents et déployés.

Autres fonctionnalités avancées d'inspection du contenu :

- Reconnaissance optique des caractères (OCR) permettant d'extraire le texte d'images à des fins d'analyse DLP
- Correspondance exacte des données pour une détection extrêmement précise par le biais de correspondances multicolonnes de données tabulaires structurées
- Correspondance de données indexées (analyse de l'empreinte numérique de documents) pour le chargement de fichiers non structurés et l'exécution d'une analyse de similitude sur les fichiers transmis via un canal de sortie

À l'heure actuelle, les fonctionnalités avancées ne sont pas disponibles sur l'agent d'endpoint en raison de contraintes de ressources. Toutefois, ces contraintes disparaissent lorsque le processus d'analyse a lieu dans le cloud. Ces fonctionnalités ne sont donc disponibles que pour Proofpoint Cloud DLP et Proofpoint Email DLP.

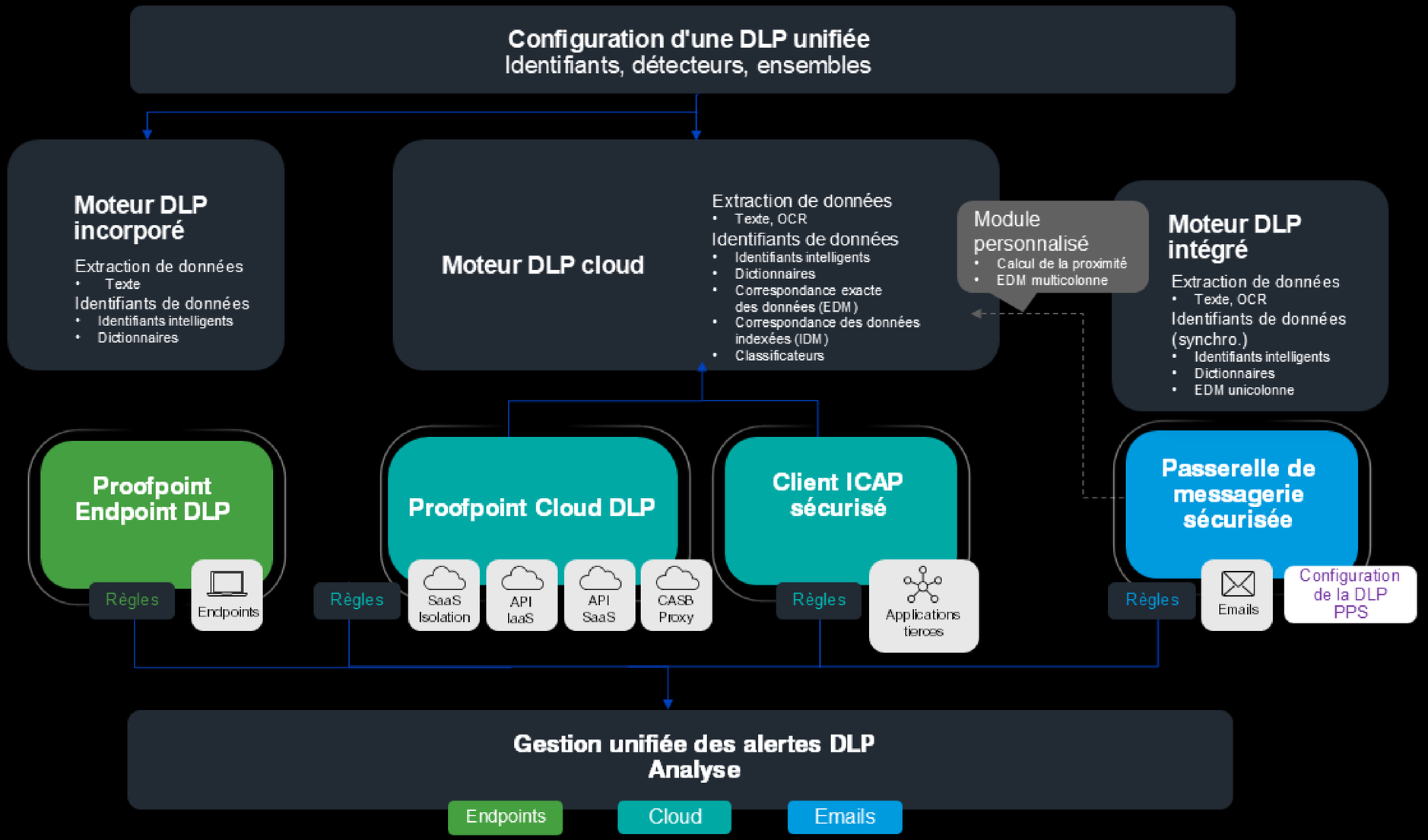
Exportation d'archives/de données hors ligne

Notre fonctionnalité d'exportation de données vous permet de répliquer vos données en toute sécurité en dehors de Proofpoint. C'est vous qui spécifiez les données à exporter, notamment les données d'activité, les alertes et les événements. Aucune limite de conservation ne s'applique aux données exportées. Une fois l'exportation terminée, vous pouvez manipuler les données en vue de les analyser et de les mettre en corrélation.

Les données peuvent être répliquées sur un bucket AWS S3/Azure appartenant au client, qui est indépendant de l'application Proofpoint. Vous pouvez ensuite les intégrer à d'autres outils d'analyse tels que des solutions SIEM et des lacs de données.

Les données exportées datent de 15 minutes avant le déclenchement de l'exportation, laquelle s'exécute tous les quarts d'heure.

Extraction et identifiants de données par canal DLP



proofpoint.

Visitez le site proofpoint.com/fr pour en savoir plus

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr.