CATO
NETWORKS

Présentation de la

Data Loss Prevention (DLP) de Cato

Comment mesurez-vous la valeur des données ?

Les données constituent l'atout le plus précieux d'une entreprise moderne. Une étude récente des entreprises du S&P 500 a montré que les actifs incorporels représentent 90 % de leur valeur totale. Qu'il s'agisse de propriété intellectuelle, comme un code source ou des plans, d'informations commerciales sensibles, telles que les mesures financières ou les données des clients, ou d'informations personnelles sensibles, telles que les informations personnelles identifiables (PII) ou les informations médicales personnelles (PHI) des employés ou des clients, leur valeur combinée dépasse largement celle des actifs physiques de l'entreprise. Si les informations sensibles d'une entreprise tombaient entre de mauvaises mains, cela pourrait avoir des conséquences dévastatrices pour elle et nuire à sa réputation, sans parler des poursuites judiciaires éventuelles.

La protection des informations sensibles de l'entreprise est également souvent nécessaire pour assurer la conformité aux réglementations telles que la norme PCI (Payment Card Industry) en matière de sécurité des données ou les lois HIPAA (Health Insurance Portability and Accountability Acts).

Comment protéger vos données d'entreprise ?

L'un des outils les plus efficaces pour aider les entreprises à protéger leurs informations sensibles et à assurer leur conformité réglementaire est la prévention des pertes de données (Data Loss Prevention ou DLP). Une solution DLP peut analyser tout le trafic envoyé vers ou depuis les actifs de l'entreprise afin de détecter les informations sensibles et de prendre les mesures appropriées. Mais qu'est-ce que cela signifie exactement ? Qu'est-ce qu'une information sensible ? Comment identifier une telle situation ? Et quels actifs devons-nous protéger ? Examinons les choses.

Qu'est-ce qu'une information sensible ?

Les informations sensibles relèvent de deux catégories principales :

Données sensibles

Séquences de caractères contenant des données sensibles telles que numéros de sécurité sociale, adresses IP, numéro de carte bancaire, etc.

Fichiers sensibles

Fichiers d'un certain type que l'entreprise considère comme sensibles, tels qu'un code source (par exemple, Java) ou des fichiers de conception (par exemple, AutoCAD).

Comment identifier des données sensibles ?

Des données sensibles sont détectées par la mise en correspondance de leur contenu avec des structures de types de données connues. Par exemple, les numéros de sécurité sociale américains ont une structure adoptant le format 123-45-6789 (3 nombres de 3, 2 et 4 chiffres, respectivement). Lorsqu'une séquence correspondante de chiffres est trouvée dans les données analysées, elle est marquée comme ayant un potentiel élevé d'être un numéro de sécurité sociale, et l'action prévue face à un tel cas est appliquée.

La solution DLP de Cato analyse les données dans les fichiers, par exemple un document Word, ainsi que les informations autonomes envoyées vers ou depuis une application via un formulaire.

Le moteur DLP de Cato comprend plus de 350 types de données couvrant des informations sensibles à l'échelle mondiale (par exemple, les numéros de carte bancaire) ainsi que des informations spécifiques (par exemple, les codes postaux américains) couvrant plus de 30 pays.

Afin de permettre une recherche rapide et efficace, le moteur DLP de Cato classe les types de données sur la base de deux attributs principaux : catégorie et pays.

Types de données basés sur la catégorie

Les catégories de données reposent sur des classifications générales telles que les informations personnelles identifiables (PII) et des classifications réglementaires telles que la loi HIPAA (Health Insurance Portability and Accountability Act). Les catégories couvertes par le moteur DLP de Cato sont indiquées dans la fig.1.

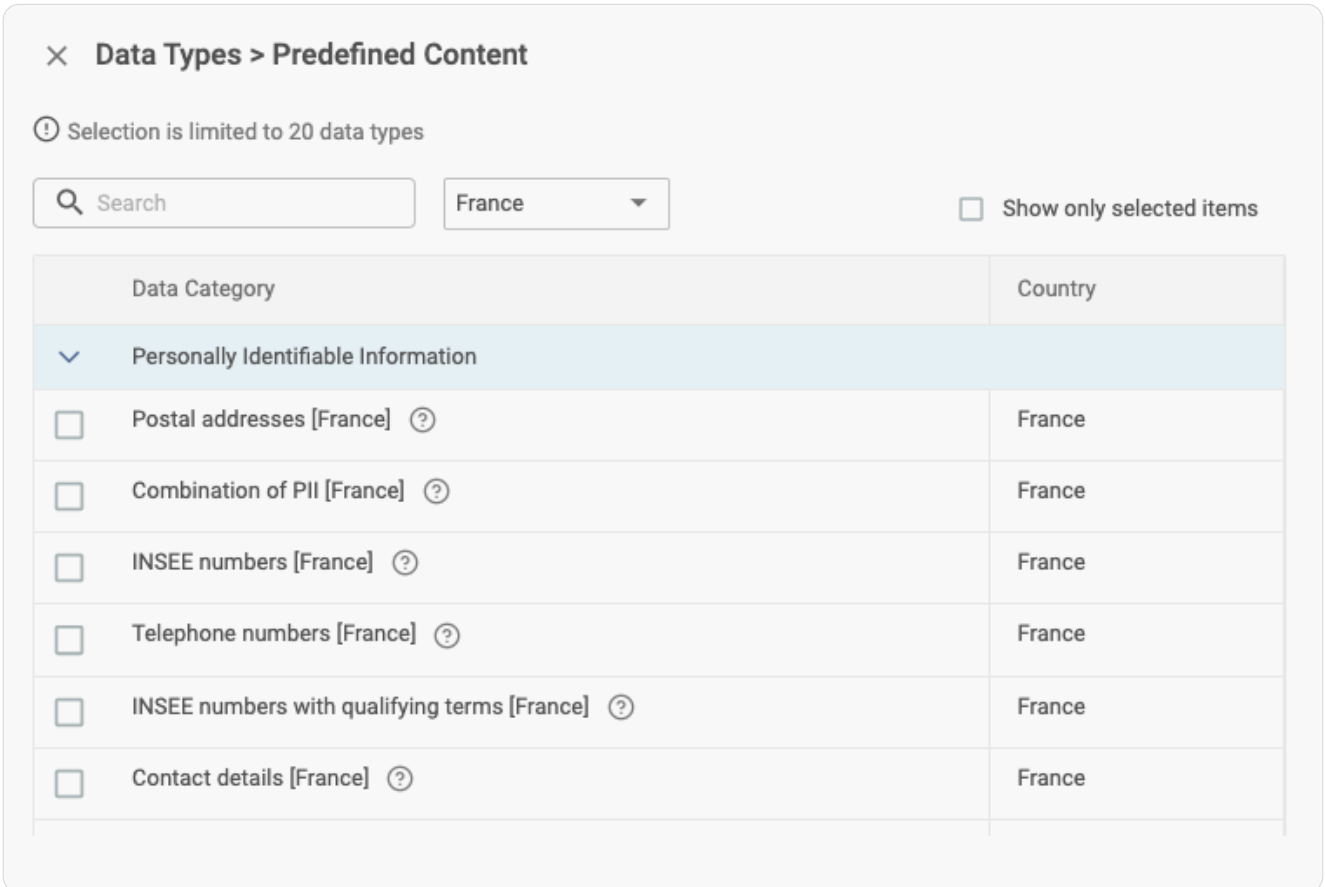


Figure 1 : Catégories de type de données

Types de données basés sur le pays

Les types de données peuvent également être filtrés par pays pour afficher des types de contenu localisés. Par exemple, lors de la sélection du Royaume-Uni, tous les types de données pertinents pour ce pays sont affichés, tels que les adresses postales et les numéros d'identification personnels. Les types de données PII spécifiques au Royaume-Uni sont indiqués dans la fig. 2.

Afin de simplifier la sélection de plusieurs types de données dans une certaine catégorie, le moteur DLP de Cato regroupe les types de données qui sont couramment sélectionnés ensemble dans un type de données combiné, par exemple, « combinaison d'informations personnelles identifiables [R.-U.] ».

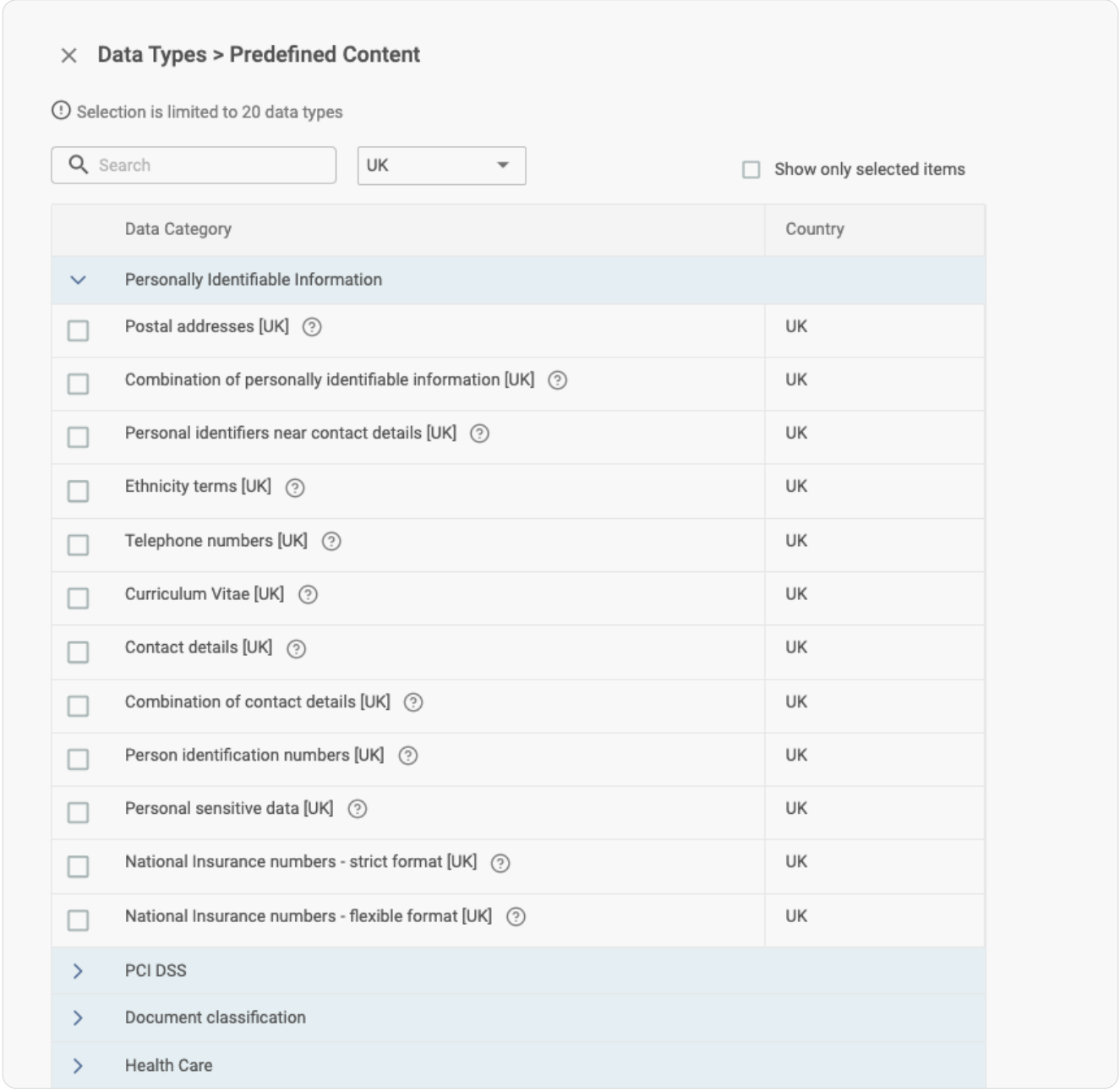


Figure 2 : Informations personnelles identifiables (PII) pour le Royaume-Uni

Le moteur DLP de Cato permet également de rechercher la liste complète des types de données afin de trouver rapidement certains d'entre eux selon leur nom ou en fonction d'un terme connu tel que « personnel » ou « postal ».

Création de types de données et de stratégies DLP modulaires à grande échelle

Lors de la définition des règles de DLP, nous utiliserons généralement une combinaison de types de données, de telles combinaisons étant pertinentes pour plusieurs applications. Afin d'éviter d'avoir à sélectionner le même ensemble de types de données de façon répétitive, potentiellement des centaines de fois, le moteur DLP de Cato adopte une approche modulaire pour définir des règles afin de simplifier le processus, tout en le rendant aussi flexible et personnalisable que nécessaire. Le moteur DLP de Cato permet de regrouper des types de données en profils qui peuvent ensuite être utilisés pour définir rapidement des règles DLP. Par exemple, nous pouvons créer un profil appelé « PII Europe » qui inclut les types de données PII utilisés dans les pays européens (fig. 3).

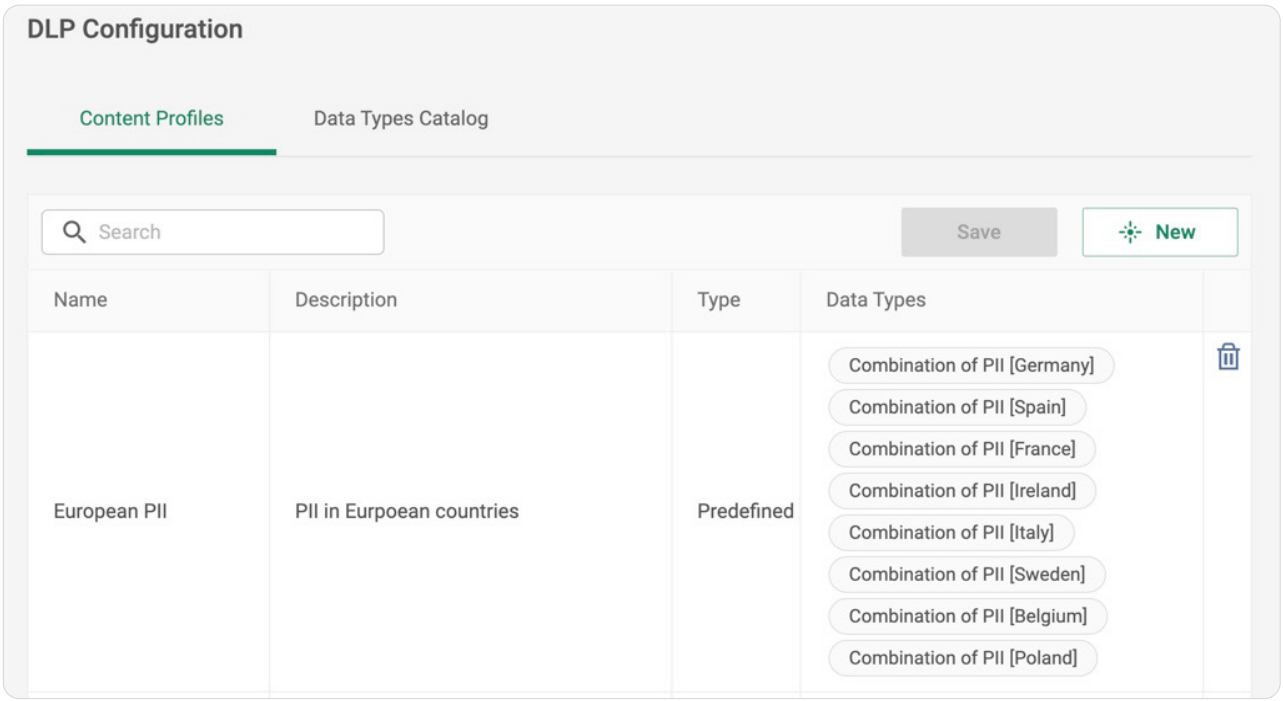


Figure 3 : Profil DLP pour les PII en Europe

Les stratégies DLP de Cato en action

Les règles DLP nous permettent de définir les stratégies que nous voulons mettre en œuvre. Elles combinent les profils de données que nous avons définis pour faire correspondre les informations sensibles avec le comportement en vertu duquel nous voulons appliquer une stratégie spécifique. Vous trouverez à la suite des exemples de cas d'utilisation fréquents du moteur DLP. Chaque exemple montre la stratégie que nous voulons appliquer et la règle DLP qui la met en œuvre.

Cas d'utilisation n°1

Stratégie requise : Bloquer tout téléchargement d'informations de carte bancaire allemande dans Office365

La règle mettant en œuvre cette stratégie est visible dans la Fig. 4. On peut voir la demande de « bloquer » définie dans le paramètre Action, « télécharger » défini dans le Critère : Activités, « carte bancaire allemande » représentée dans le Critère : Profil et « Office365 » défini dans le paramètre Application. « Tout » est défini dans le paramètre source pour indiquer que cela doit être appliqué à toutes les sources tentant un tel téléchargement.

Source	Application	Criteria		Severity	Action
Any	Office365	ACTIVITIES	Download	High	Block
		PROFILES	PCI Germany		

Figure 4 : Stratégie DLP pour bloquer les informations de carte bancaire allemande dans Office365

Cas d'utilisation n°2

Autoriser uniquement les utilisateurs du service R&D à télécharger les fichiers de code source

Dans ce cas, nous voulons autoriser uniquement le service R&D à télécharger des fichiers, donc le paramètre Action de la Fig. 5 sera réglé sur « Autoriser » et le paramètre Source sur « R&D». Comme nous ne limitons pas cette règle à des applications spécifiques, la valeur du paramètre Application sera « Toute application ». Le critère : L'attribut Fichier sera défini sur « Type de contenu est source_code », ce qui signifie que la règle sera appliquée à ce type de fichier, plutôt qu'à tout contenu correspondant spécifique dans le fichier.

Source	Application	Criteria		Severity	Action
R&D	Any Application	ACTIVITIES	Download	Low	Allow
		FILE ATTRIBUTES	Content Type is source_code		

Figure 5 : Stratégie DLP pour autoriser les utilisateurs du service R&D à télécharger les fichiers de code source

Ce qu'il est important de noter dans cet exemple, c'est que pour que tout le trafic des services autres que celui de R&D soit bloqué, nous devrons ajouter une règle bloquant « Tout » autre trafic source. Comme les règles sont appliquées dans leur ordre de définition, tout le trafic R&D sera autorisé à télécharger des fichiers, tandis que tous les autres types d'utilisateurs atteindront la règle de blocage suivante.

Cas d'utilisation n°3

Stratégie requise : Bloquer les téléchargements de PII européennes vers un site chinois

Ce qui est unique dans cet exemple, c'est que nous voulons restreindre l'accès aux données aux utilisateurs situé sur un site dans un emplacement spécifique. Comme on peut le voir sur la Fig. 6, le paramètre Source est défini sur le nom du site tel que défini dans le réseau de l'entreprise : « Pékin ».

Source	Application	Criteria		Severity	Action
Beijing	Any Application	ACTIVITIES	Download	High	Block
		PROFILES	Europe PII		

Figure 6 : Stratégie DLP pour bloquer les PII européennes sur un site chinois

Obtenir des renseignements sur l'activité DLP

Tous les événements en matière de DLP peuvent être consultés dans le visualiseur d'événements (Fig. 7) de CMA (Cato Management Application).

Les événements peuvent être recherchés et filtrés de nombreuses manières pour mieux cerner les tendances DLP ou enquêter sur un événement spécifique. Les événements d'intérêt peuvent être étudiés en détail, pour en extraire des données riches et un aperçu de leurs origines et de leur cause.

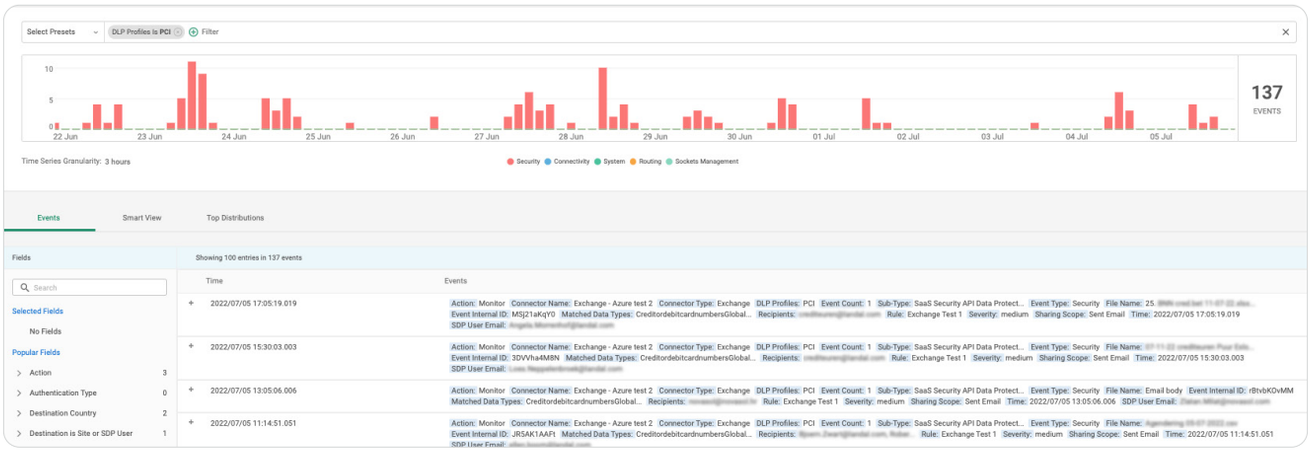


Figure 7 : Vue des événements DLP

Le moteur DLP de Cato vous procure également un tableau de bord qui fournit une vue d'ensemble de l'activité liée en matière de DLP dans le réseau. Cela permet d'avoir un aperçu des indicateurs clés de déplacement des données, tels que les hôtes, les profils, les types de fichiers et les emplacements les plus impliqués dans une violation des règles DLP. En outre, le tableau de bord comprend une ventilation des événements par action et gravité. Le tableau de bord DLP fournit un point de vue unique qui peut aider à identifier les anomalies ou les changements dans l'utilisation des données, indiquant à l'utilisateur un comportement potentiellement suspect.

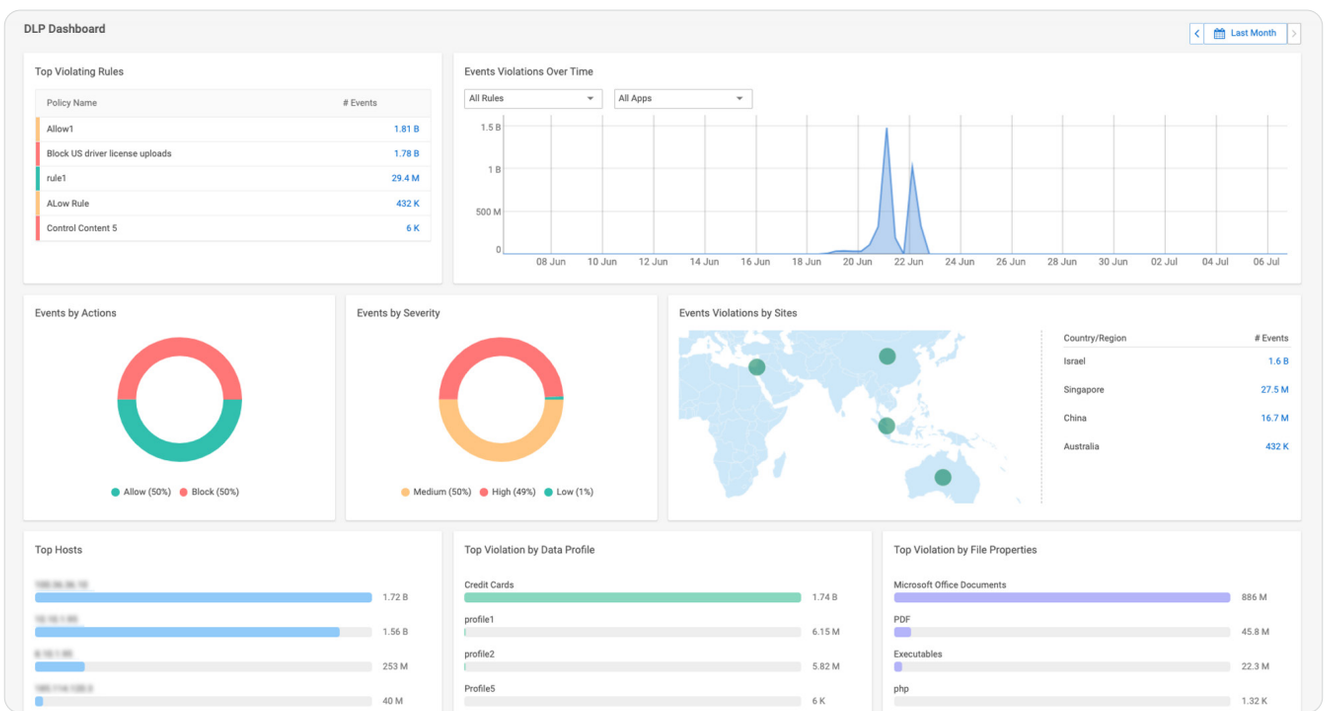


Figure 8 : Tableau de bord DLP de Cato

Quels actifs devons-nous protéger ?

Les informations sensibles résident généralement dans les applications de l'entreprise. Il peut s'agir d'applications exclusives gérées par l'entreprise elle-même ou d'applications SaaS tierces parties telles que Salesforce, Office 365 et Box. Étant donné que la plupart des applications SaaS utilisées dans une entreprise type ne font pas l'objet d'une validation, une solution DLP efficace doit également les couvrir.

Le moteur DLP de CATO est fourni dans le cadre d'un service SASE Cloud. Il assure une couverture pour tout le trafic vers tous les actifs de l'entreprise (fig. 8). Cela inclut également les applications sur site hébergées dans les datacenters physiques de l'entreprise, qui ne sont pas surveillées par la plupart des solutions DLP et qui ne sont donc pas couvertes par elles. En outre, le moteur DLP de Cato suit les principes du zero trust et rend possible la définition de règles DLP pour les applications et les activités pour lesquelles aucune règle explicite n'a été définie. Cela signifie que nous pouvons appliquer des stratégies restrictives pour les applications n'ayant pas fait l'objet d'une approbation (à savoir la shadow IT) et nous assurer que le contenu sensible n'est pas importé vers ces applications ou téléchargé depuis celles-ci avant que nous ayons eu la possibilité de mieux comprendre leur finalité et les risques potentiels.

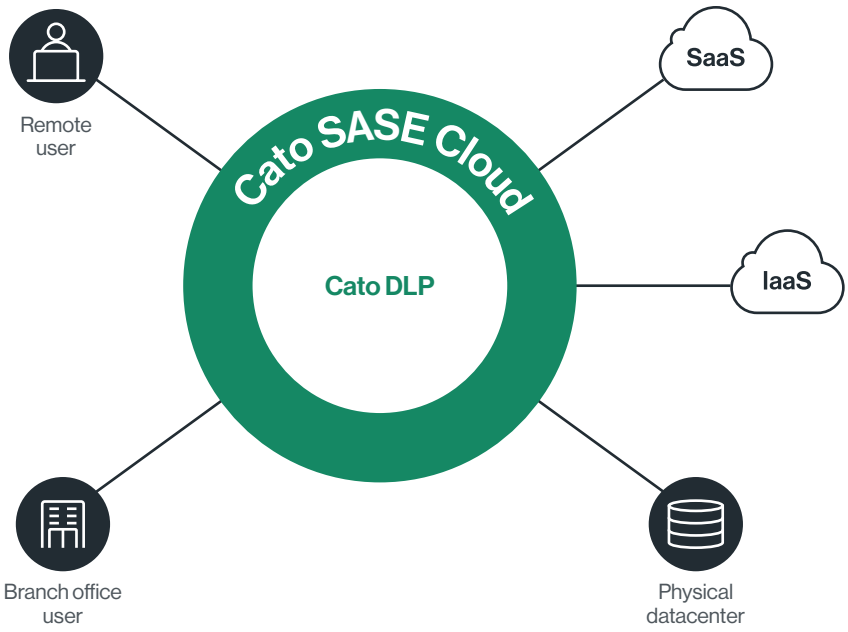


Figure 8 : Couverture Cato SASE pour tout le trafic

DLP de Cato dans le cadre d'un service SSE et SASE entièrement convergé

Security Service Edge (SSE 360) de Cato, qui fait partie du Secure Access Service Edge (SASE) de Cato, fait converger la DLP avec des services supplémentaires d'accès aux applications et d'atténuation des menaces. Cato SSE 360 utilise un Single Pass Cloud Engine (SPACE) pour utiliser ces services simultanément et dans un contexte partagé, permettant à chaque partie prenante d'avoir une visibilité sur les informations collectées et traitées par les autres pour prendre des décisions mieux informées (fig. 11). Cela raccourcit également le délai de traitement global et réduit la latence, un résultat optimisé par le fait que le chiffrement et le déchiffrement TLS doivent être effectués une seule fois pour tous les services.

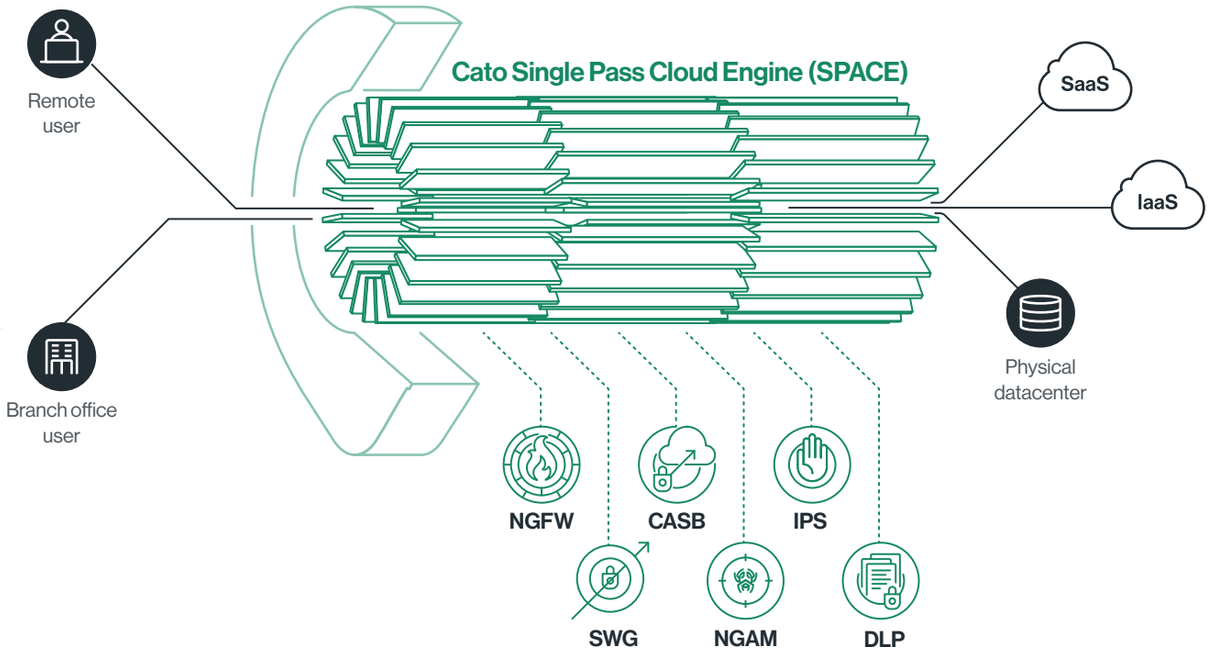


Figure 11 : Cato SPACE

SSE 360 de Cato améliore également la posture de sécurité globale de l'entreprise en mettant en œuvre une approche d'accès et d'inspection en couches du contenu. Dans le contexte de la protection DLP des informations sensibles, les utilisateurs devront franchir plusieurs services de sécurité avant d'être en mesure de seulement tenter d'exporter ou de télécharger des données sensibles.

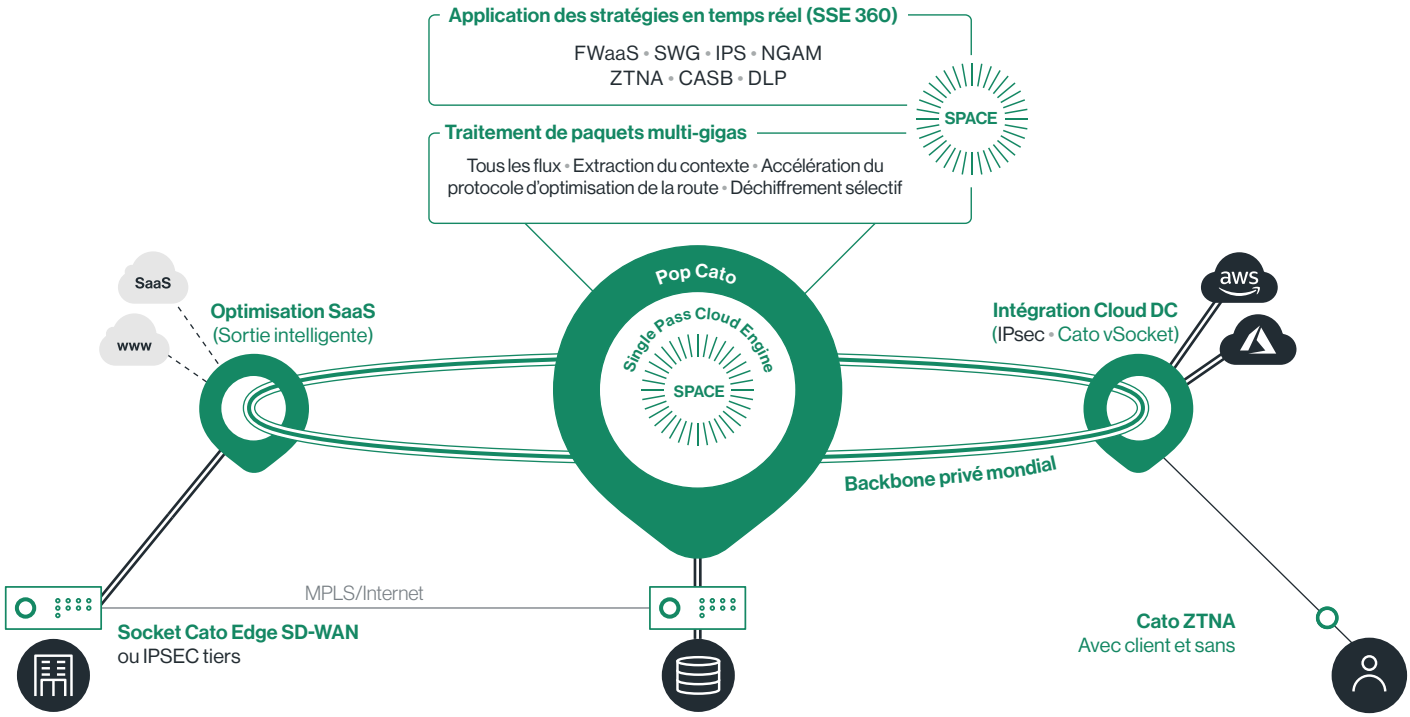
Les utilisateurs doivent d'abord franchir le Next Generation Firewall (NGFW), la Secure Web Gateway (SWG), le Cloud Access Security Broker (CASB) ainsi que le service Zero Trust Network Access (ZTNA) pour ceux situés à distance afin de simplement accéder à une application. Ce n'est qu'à ce moment-là qu'ils pourront tenter de transférer des informations sensibles, auquel cas le moteur DLP prendra des mesures.

Fonctionnant de concert, les services de prévention des menaces de Cato tels que l'IPS (Intrusion Prevention System) analyseront le trafic pour détecter les tentatives d'infiltration malveillantes. Le NGAM (Next Generation Anti-Malware) analysera le trafic pour détecter les tentatives de transfert de contenu malveillant vers les actifs de l'entreprise.

SSE 360 de Cato est une solution de protection holistique qui fournit une sécurité réseau d'entreprise complète et robuste. DLP de Cato est une pièce essentielle du puzzle de la sécurité qui tire parti de l'architecture SPACE unique de Cato pour offrir une sécurité et des performances supérieures. Son utilisation démontre vraiment que l'ensemble est bien plus grand que la somme de ses parties.

À propos de Cato Networks

Cato fournit la plateforme SASE à fournisseur unique la plus avancée au monde, en faisant converger Cato SD-WAN et un service de sécurité cloud-native, Cato SSE 360, dans un service cloud global. Cato SASE Cloud optimise et sécurise l'accès aux applications pour tous les utilisateurs et tous les sites, quel que soit le lieu. Grâce à Cato, les clients peuvent facilement remplacer des MPLS hérités coûteux et rigides par une architecture réseau moderne basée sur SD-WAN, sécuriser et optimiser une main-d'œuvre hybride travaillant de n'importe où, et rendre possible une migration cohérente vers le cloud. Cato applique des politiques d'accès granulaires, protège les utilisateurs contre les menaces et empêche la perte de données sensibles, le tout étant facilement géré à partir d'un seul écran. Avec Cato, votre entreprise est prête pour la suite.



Cato SASE. Prêt pour la suite

Cato SASE Cloud

- Backbone privé mondial
- SD-WAN en périphérie
- Sécurité informatique externalisée
- Intégration de centres de données basés sur le cloud
- Accélération des applications cloud
- Accès distant sécurisé
- Application de gestion unifiée

Cas d'utilisation

- Migration d'un MPLS vers SD-WAN
- Connectivité globale optimisée
- Accès sécurisé à Internet pour les succursales
- Accélération et contrôle du cloud
- Sécurité et optimisation des accès distants
- Gestion flexible

SOC2 Approved

ISO 27001 Certified

GDPR Compliant

Gartner peerinsights. Customer first