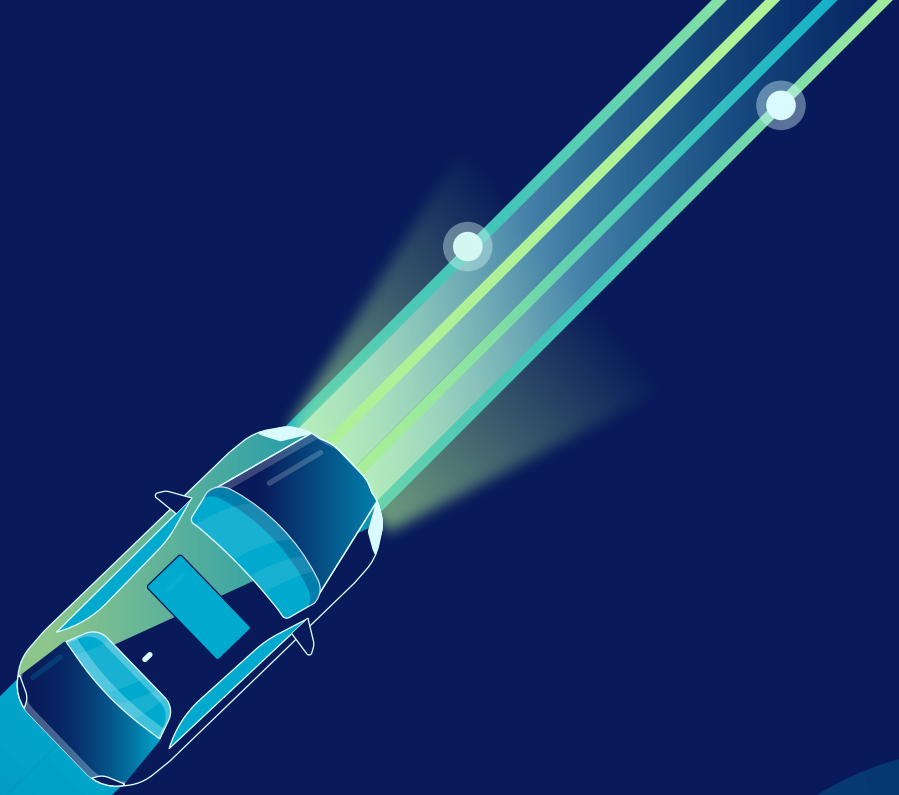
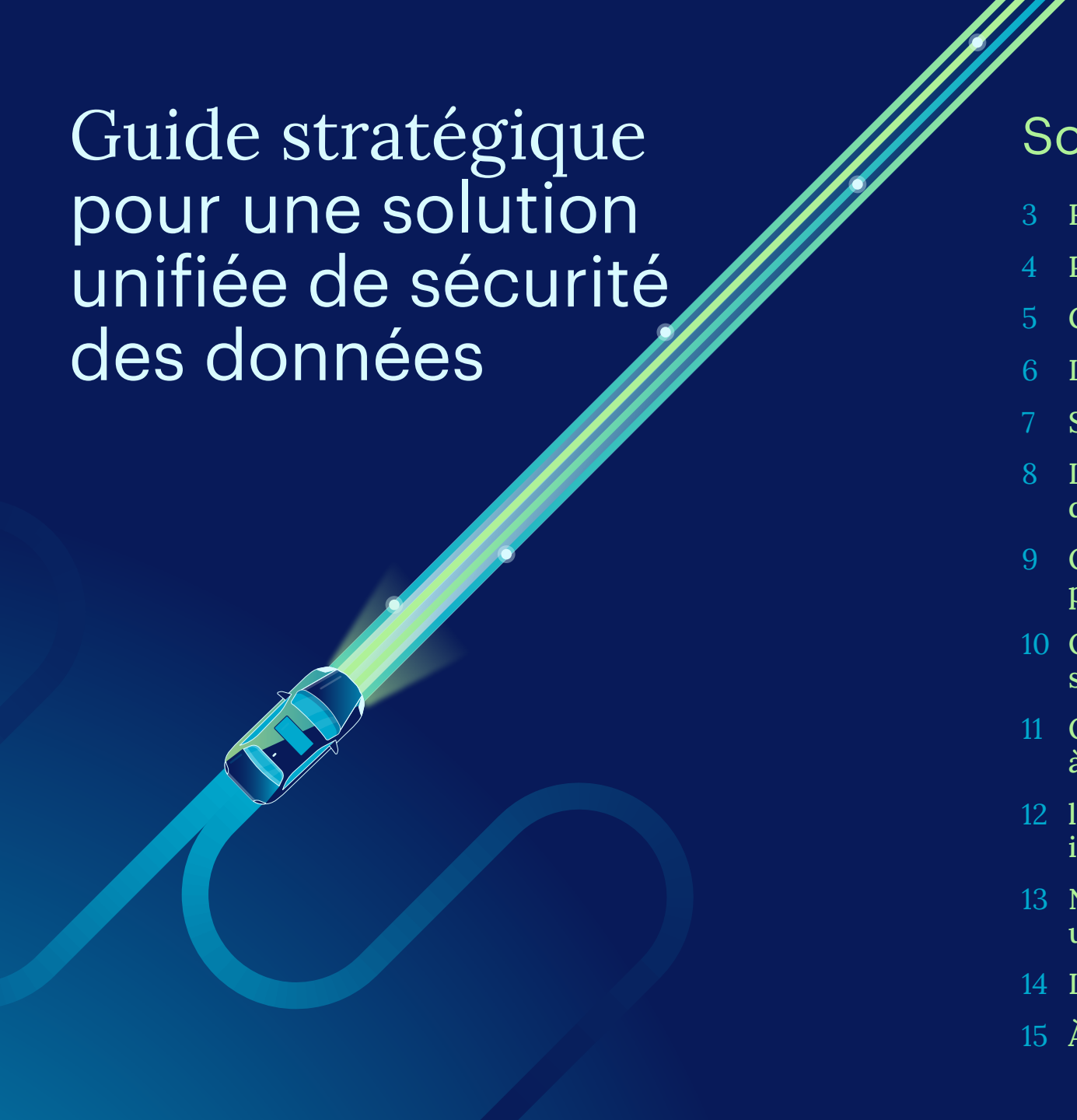
netskope

Guide stratégique pour une solution unifiée de sécurité des données



Une protection des données boostée grâce une solution unifiée associant DSPM et DLP

Guide stratégique pour une solution unifiée de sécurité des données



Sommaire

Résumé

Les équipes chargées de la sécurité, de la gestion des risques et de la conformité au sein des entreprises se sentent parfois prises au piège d'une course sans fin, tentant de garder une longueur d'avance sur une multitude d'acteurs malveillants. Et ce à juste titre. Chaque année, les violations de données se multiplient de manière exponentielle, et aucune organisation n'y échappe. Ce problème touche les entreprises de toutes tailles, dans tous les secteurs et dans toutes les zones géographiques.

Bien que les consommateurs soient conscients du risque, ils attendent des entreprises avec lesquelles ils font affaire qu'elles protègent leurs informations. Il n'y a pas pire fléau qu'une cyberattaque à grande échelle pour compromettre la réputation de la marque d'une entreprise.

Face à ce paysage de menaces, les régulateurs ont revu à la hausse leurs exigences en matière de confidentialité des données d'entreprise. Les violations surviennent souvent après que les entreprises n'ont pas respecté les règles visant à assurer la sécurité des données sensibles. Quand ils découvrent qu'une société ciblée n'a pas respecté les réglementations obligatoires, les régulateurs ont tendance à réagir sévèrement, en la sanctionnant par des amendes.

Il était déjà difficile de garantir la sécurité et la conformité dans une entreprise quand l'ensemble de ses informations critiques résidaient au sein de son propre périmètre. Aujourd'hui, c'est encore plus complexe, car 60 % des données client d'une entreprise type se trouvent dans le cloud.[1] Ces informations extrêmement précieuses échappent au champ de contrôle traditionnel de l'équipe informatique.

Sécuriser les actifs numériques de l'entreprise d'aujourd'hui demande une nouvelle approche. Une solution unifiée de sécurité des données associe des fonctionnalités de reconnaissance des données, de classification, de gouvernance des accès et d'évaluation des risques (présentes dans les outils de gestion de la posture de sécurité des données [DSPM]), à des technologies de prévention des pertes de données (DLP) assurant une protection en temps réel. Ces solutions entièrement intégrées verrouillent les données d'une entreprise, y compris les données stockées dans des applications fantômes non gérées par son service informatique, grâce à six fonctionnalités clés.

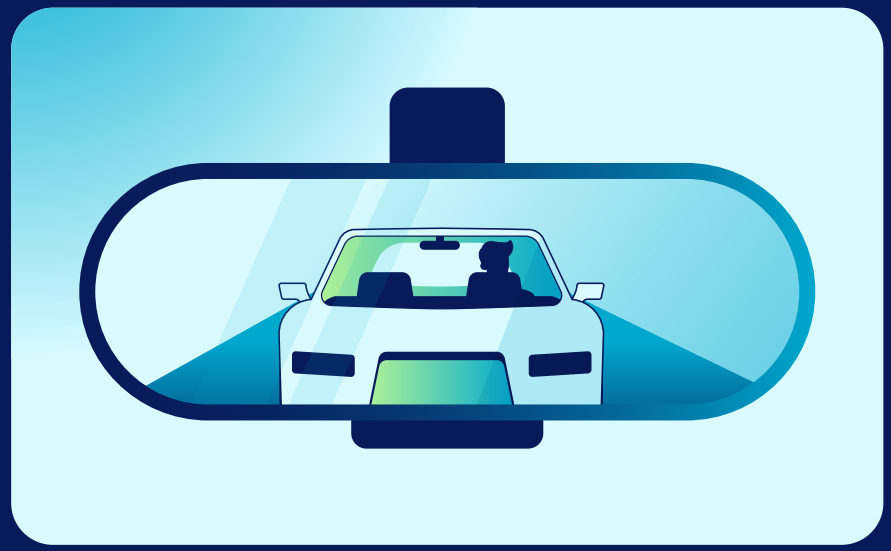
[1] Source : Statista. « Share of corporate data stored in the cloud in organizations worldwide », mars 2022.

Principes de base de la sécurité des données à l'ère de l'IA

Les entreprises doivent identifier leurs points faibles en matière de sécurité pour bloquer de façon efficace les pirates qui tentent de forcer leurs systèmes de protection. Pour s'assurer qu'elles ont une visibilité directe sur toutes les applications et données auxquelles accèdent les utilisateurs, les équipes informatiques doivent se poser plusieurs questions essentielles :

- Où toutes nos données se trouvent-elles ?
- Quelle est la nature de ces données ?
- Qui a accès aux données sensibles ?
- Quel est le niveau de risque de nos interactions de données ?

Le but de cet exercice est simple : si une solution ou une base de données dans le cloud contient des informations personnelles identifiables (PII) de clients, telles que des adresses ou des numéros de sécurité sociale, ou toute autre information sensible pour l'entreprise, cette dernière doit connaître les garde-fous dont elle dispose pour modérer les risques liés aux données.



Conseil d'expert

Si une solution ou une base de données dans le cloud contient des informations personnelles identifiables (PII) de clients, ou d'autres informations sensibles pour l'entreprise, cette dernière doit connaître les garde-fous dont elle dispose pour modérer les risques liés aux données.

Gérer les risques liés aux données

Les données qui passent inaperçues sont difficiles à déceler en raison de la diversité des informations à sécuriser par l'entreprise et de leur circulation désordonnée. Les équipes de sécurité peuvent avoir à gérer les données sur un large éventail de terminaux, de sites web et de systèmes de messagerie. Les informations sensibles peuvent également résider dans des bases de données, des lacs de données et/ou des entrepôts de données, ainsi que dans une vaste de gamme de modèles cloud, qu'il s'agisse de Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) et Platform-as-a-Service (PaaS).

Certaines de ces données sont hébergées sur site mais d'autres le sont dans le cloud. Leur sécurité doit être assurée lors de leur transmission, de leur utilisation et quand elles sont au repos.

La difficulté est d'autant plus grande qu'environ 90 % des données d'entreprise sont non structurées.[2] Les informations critiques figurent dans des documents Word, des fichiers PDF, des fichiers images et d'autres formats. Bien que ces données puissent être difficilement accessibles, elles requièrent autant de protection que les informations des bases de données et d'autres applications structurées.

Enfin, alors que les informations critiques devraient résider dans des applications gérées par le service informatique de l'entreprise, l'informatique fantôme constitue un problème permanent. Les succursales déploient souvent des technologies non gérées répondant à leurs besoins spécifiques, sans l'aval du service informatique. 97 % des applications cloud utilisées par les employés types échappent à la vigilance du service informatique.[3]

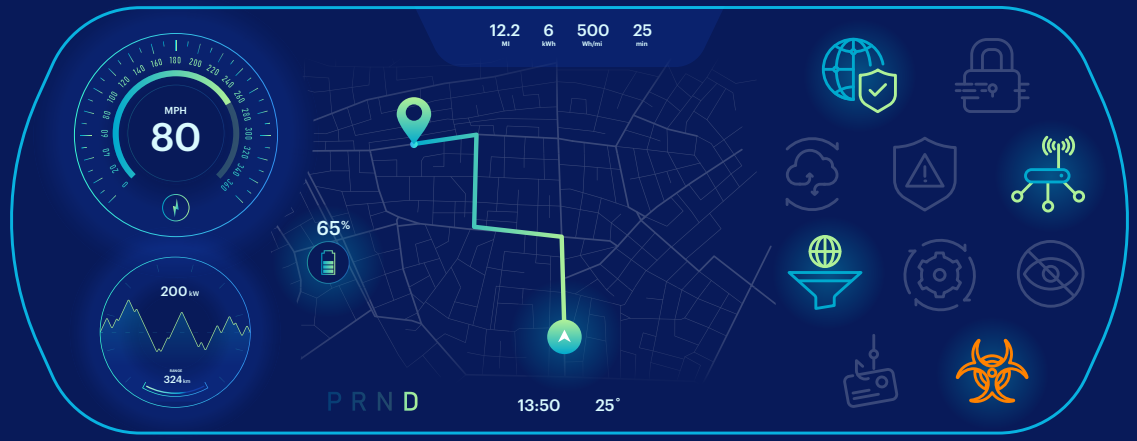
Environ

90 %

des données d'entreprise sont non structurées.

88 %

des utilisateurs interagissent avec des applications cloud personnelles — informatique fantôme[4]



[2] IDC. « Untapped Value: What Every Executive Needs to Know About Unstructured Data », août 2023.

[3] Rapport de Netskope Threat Labs sur le cloud et les menaces : 2025.

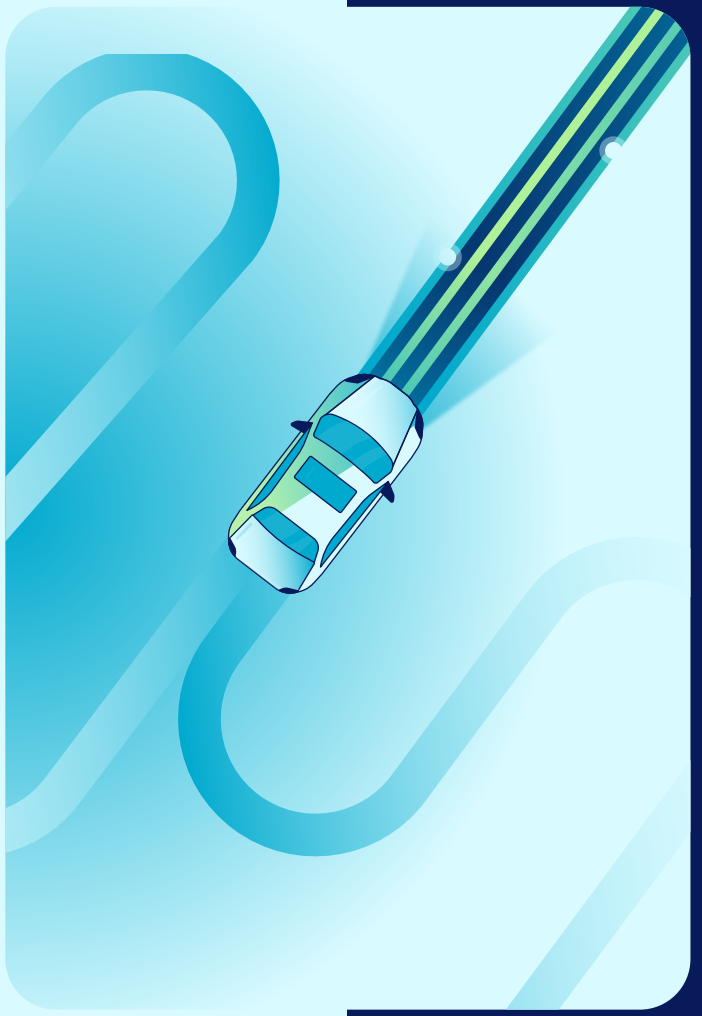
[4] Rapport de Netskope Threat Labs sur le cloud et les menaces : IA générative, 2025.

Les technologies disparates ne sont pas une bonne réponse

Bien que de nombreuses options s'offrent aux entreprises pour protéger les différents types de données, elles ont généralement besoin d'un ensemble de solutions pour couvrir l'ensemble de leurs données. Au fil des ans, les équipes informatiques ont dû augmenter leur couverture, et cette tendance devrait se poursuivre à mesure qu'apparaissent de nouvelles technologies et vulnérabilités.

Les systèmes de DLP destinés aux terminaux sont efficaces pour sécuriser les données sur les terminaux de l'entreprise. Mais pour protéger les informations sensibles des messageries, une entreprise a besoin d'une DLP de messagerie ou d'une autre solution. Certaines organisations disposent d'une solution distincte pour sécuriser l'utilisation de l'IA générative au sein de leur environnement. Cette solution peut fonctionner pour empêcher les fuites accidentelles des données de l'entreprise dans le domaine public, mais ne garantit pas systématiquement la conformité de l'entreprise. Pour contrer les menaces internes et éviter le sabotage, une organisation devra peut-être recourir à un outil d'analyse de comportement. Et pour la reconnaissance et la classification des données sensibles, le DSPM s'avère le meilleur choix.

Or, le déploiement de toutes ces solutions différentes crée un paysage complexe de technologies disparates qui met à rude épreuve les ressources informatiques et nuit à la sécurité des données de l'entreprise.



« Il est temps de repenser la sécurité des données si vos DSPM et DLP sont structurés en silos séparés. Ils peuvent être associés pour former l'ossature d'une approche complète qui non seulement sécurise vos données, mais confère à votre organisation un avantage concurrentiel indéniable qui lui permet de se positionner en leader dans l'économie d'aujourd'hui où tout repose sur les données. »

Ankur Chadda

Responsable marketing pour la sécurité des données — Netskope

Solution unifiée de sécurité des données

Les équipes informatiques ont besoin d'une plateforme de sécurité capable de protéger tous les types de données tout en offrant la visibilité d'un tableau de bord unique. C'est pourquoi nous proposons des plateformes de sécurité des données unifiée qui regroupent les fonctionnalités DSPM et DLP en une seule solution.

Cette stratégie de solution unique pour toutes les données de l'entreprise présente plusieurs avantages importants :

- **Visibilité accrue.** Il suffit à l'équipe informatique de jeter un coup d'œil à un tableau de bord unique pour identifier les problèmes de sécurité susceptibles de survenir sur site ou dans le cloud, pour les données gérées et non gérées qui sont transmises, utilisées ou au repos.
- **Sécurité améliorée.** Des systèmes disparates rendent la réponse aux menaces incohérente. En revanche, une plateforme étroitement intégrée garantit que les informations sur les risques et les menaces recueillies par une solution sont partagées avec les autres solutions, ce qui permet une réponse coordonnée à tous les emplacements de stockage de données de l'entreprise.
- **Gestion facile.** L'administration de l'infrastructure de sécurité sollicite moins les équipes qui n'ont plus à contrer les problèmes au coup par coup, mais peuvent se consacrer à l'atténuation des vulnérabilités, la planification à long terme et d'autres projets stratégiques.

« À la différence de certaines de nos applications héritées, qui me demandaient de gérer une seule application et ses fonctionnalités à quatre emplacements différents, je connais l'état de mon ensemble de règles sur plusieurs fonctions et applications. »

VP Infrastructure

Technologie

L’approche de Netskope One en matière de sécurité des données unifiée

Netskope One aide les organisations à passer à la vitesse supérieure car il s’agit d’une plateforme unifiée garantissant la sécurité complète des données. Elle réunit DSPM et DLP pour que la détection des risques et l’atténuation des menaces gagnent en précision et en exactitude.

Elle se distingue principalement des autres solutions par sa capacité à sécuriser les données au repos, qui circulent ou sont utilisées sur l’ensemble des vecteurs d’attaque les plus courants. En consolidant un si grand nombre de fonctionnalités, elle permet le partage de contexte au niveau des utilisateurs, des applications et des opérations, par tous les outils qui protègent des informations sensibles.

Cette approche renforce la sécurité de cinq façons essentielles :

1. Réduction de la surface d’attaque de l’entreprise : Netskope One contrôle l’accès à l’ensemble des applications web, SaaS et privées dans lesquelles résident les données
2. Accélération de la reconnaissance des données
3. Meilleure connaissance des données de l’entreprise, notamment de la lignée et du mouvement des données
4. Contrôle automatisé en temps réel des risques liés aux données
5. Prise en charge de l’évolutivité : Possibilité de créer des règles et des profils de données en une seule fois, puis de les déployer partout

Netskope One fournit la couverture la plus étendue et la plus approfondie du marché partout où résident les données de l’entreprise. Examinons maintenant trois questions qui vous permettront d’évaluer l’environnement de votre organisation :

Question 1 : Quel niveau de risque votre surface présente-t-elle ?

Question 2 : Quelle est la rapidité de réaction de vos solutions de sécurité en cas de comportement risqué ?

Question 3 : Comment appliquez-vous les règles DLP à votre trafic restant ?

« Grâce à Netskope, nous pouvons quantifier l’exfiltration des données et relier les comportements risqués aux individus, afin de réagir rapidement. »

Directeur principal

Programme mondial contre les risques internes, grande entreprise de services financiers

Question 1 : Quel niveau de risque votre surface présente-t-elle ?

Netskope One prend des décisions adaptées, selon le niveau de confiance, en temps réel et en continu. Chaque fois qu'un utilisateur tente de stocker, de déplacer ou de manipuler des données, la plateforme évalue les risques selon les quatre vecteurs suivants :

- **Risque lié aux utilisateurs :** Vos données sont-elles sécurisées contre les emprunts d'identité ? Êtes-vous en mesure de vérifier que les utilisateurs sont bien les personnes qu'ils prétendent être ?
- **Risque lié aux appareils :** Un individu est-il sur un appareil géré, à un emplacement connu et digne de confiance ?
- **Risque lié à l'application :** Le logiciel fonctionne-t-il avec une application gérée par le service informatique ? Et s'agit-il d'une instance de l'entreprise ou personnelle du logiciel ?
- **Risque lié aux données :** S'agit-il d'informations confidentielles ou sensibles pour l'entreprise ?

Netskope a analysé et noté plus de 80 000 applications et développé 130 catégories d'URL. La plateforme Netskope trie le trafic en fonction de ces informations, ce qui permet de gérer plus rapidement les menaces éventuelles. Elle peut également distinguer une instance SaaS parmi des milliers.

Netskope One regroupe toutes ces données puis exécute une analyse du comportement des utilisateurs et des entités (UEBA), ainsi qu'une analyse de Threat Intelligence en temps réel pour noter l'activité tentée par l'utilisateur sur une échelle de comportements risqués.

Question 2 : Quelle est la rapidité de réaction de vos solutions de sécurité en cas de comportement risqué ?

Après avoir effectué l'analyse des risques, Netskope One Data Security applique ses règles de sécurité pour interrompre le trafic suspect jusqu'à ce que l'utilisateur s'authentifie à nouveau ou justifie son comportement. Il peut aussi bloquer automatiquement le trafic et, dans le pire des cas, isoler l'utilisateur et/ou l'appareil jusqu'à ce qu'une personne réelle puisse évaluer l'activité.

Les entreprises peuvent utiliser Netskope One Data Security pour instaurer des contrôles granulaires qui permettent, entre autres, les actions suivantes :

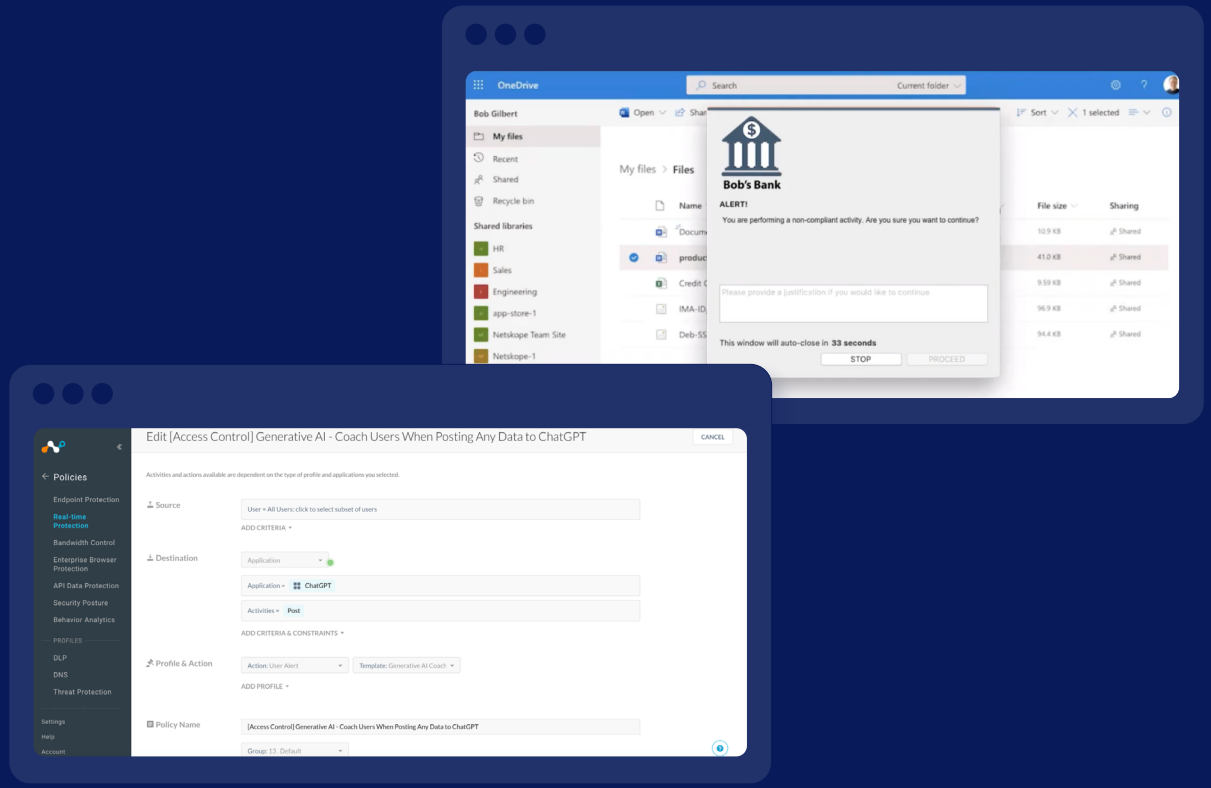
- Bloquer les logiciels malveillants et les contenus qui enfreignent la politique d'utilisation acceptable (AUP)
- Interrompre les activités et/ou les applications cloud jugées risquées
- Empêcher les téléchargements vers une application ou une instance d'application dans le cloud, non gérée par le service informatique
- Restreindre les activités de partage à certains domaines du web
- Limiter le trafic en fonction d'autres informations telles que les caractéristiques de l'utilisateur

Netskope One Data Security offre une fonction exclusive : il peut être configuré pour fournir un accompagnement en temps réel des utilisateurs dont le comportement enfreint les règles qui régissent les données de l'entreprise.

« Nous commençons à nous inquiéter sérieusement des auteurs de menaces persistantes avancées qui s'en prennent à nos données. La solution Netskope SSE nous aide à contrôler la situation de façon bien plus efficace. »

VP Infrastructure,

Entreprise technologique



Question 3 : Comment appliquez-vous les règles DLP à votre trafic restant ?

Pour le trafic non décelé par l'analyse DSPM, Netskope One Data Security applique les techniques DLP afin de garantir que les utilisateurs n'exfiltrent pas de données. Les fonctionnalités de cette plateforme examinent les données dans les messageries, sur les terminaux, les sites web et différents formats de stockage de données, sur site ou dans le cloud.

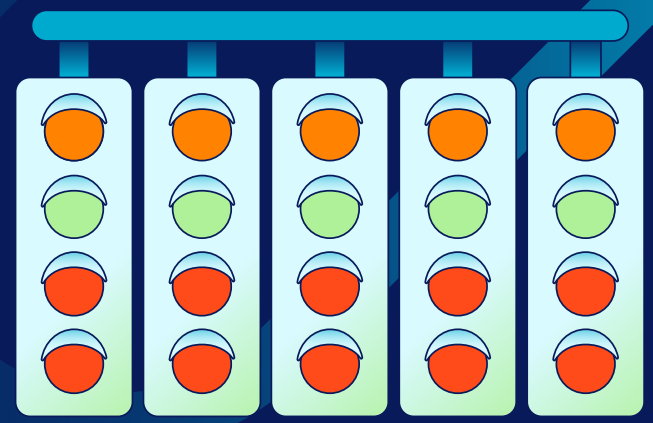
Tout comme les itérations précédentes de la DLP, Netskope One Data Security identifie les données au moyen d'expressions régulières personnalisées, de mots-clés, de dictionnaires, de la correspondance exacte des données (EDM) et de la correspondance de documents indexés (IDM). Elle recueille des indices contextuels transmis par la plateforme — des paramètres tels que le risque lié à l'utilisateur ou des informations provenant du courtier en sécurité d'accès au cloud (CASB) ou des fonctions de gestion de posture de sécurité SaaS (SSPM) — et de sources externes, telles que les fonctions intégrées d'authentification unique (SSO) ou la passerelle de messagerie sécurisée (SEG). Tout comme le DSPM, la DLP de Netskope One optimise l'inspection du contenu au moyen de modèles d'AA afin de rechercher les données PII, PHI ou d'autres types.

84 % des organisations doivent respecter une infrastructure de conformité externe,[5] et ces fonctionnalités sont cruciales. Netskope One comprend 38 modèles de conformité réglementaire et juridique prédéfinis pour aider les unités opérationnelles du monde entier à respecter les exigences locales. Et il y a mieux : alors même qu'elle améliore la conformité, cette plateforme réduit la friction due à la sécurité pour les utilisateurs et ne nuit donc pas à la productivité de l'entreprise.

« Netskope nous fournit les outils et les fonctionnalités qui nous permettent d'adopter les technologies du cloud tout en gardant le contrôle et restant en conformité. »

Responsable de la sécurité

Groupe Apex



[5] Source : Coalfire. « Securealities Report: Compliance 2023 », mai 2023.

L’AA de Netskope One interprète les données structurées et non structurées

Netskope One a recours à l’apprentissage automatique (AA) pour déterminer le contenu des données non structurées et pour catégoriser les données. Ainsi, le processus de classification d’images de la plateforme utilise un algorithme d’AA entraîné pour identifier les documents sensibles tels que les passeports ou les permis de conduire, sans examiner le texte. Dans le même temps, la technologie de reconnaissance optique des caractères (OCR) intégrée à la plateforme peut extraire du texte depuis des images à des fins d’analyse.

Les fonctionnalités d’AA de Netskope One emploient des attributs de données structurées et non structurées pour étiqueter ces données en tant que PII, informations de santé personnelles (PHI), données soumises au règlement général de protection des données (RGPD) ou à la loi HIPAA (Health Insurance Portability and Accountability Act), etc. Cette plateforme intègre plus de 3 000 classificateurs de risques liés aux données et les entreprises peuvent également développer leurs propres classificateurs d’AA.

Il est également possible d’entraîner Netskope One à rechercher des combinaisons d’identificateurs, telles que des numéros de sécurité sociale dans des documents fiscaux, ou d’effectuer une analyse des droits en comparant les données aux caractéristiques des utilisateurs. Une telle exploitation de l’apprentissage automatique réduit les coûts de fonctionnement de la sécurité en minimisant l’intervention humaine dans la prise de décisions courantes. Elle en améliore l’efficacité en éliminant le risque d’erreur humaine.

Conseil d’expert

L’apprentissage automatique réduit les coûts de fonctionnement de la sécurité en minimisant l’intervention humaine dans la prise de décisions courantes. Il améliore également l’efficacité des décisions.

Netskope One : La solution de sécurité des données unifiée qu'il vous faut

Netskope One anticipe les menaces potentielles en associant des fonctionnalités DSPM à un moteur de DLP unifiée qui gère toutes les sources de données, qu'elles se trouvent sur site ou dans le cloud. Cette plateforme comprend un tableau de bord unique qui présente les problèmes de sécurité, les contrôles ainsi que les réponses aux menaces sur l'ensemble du cycle de vie des données. Et les indications qu'elle donne facilitent l'application des règles en temps réel.

La plateforme Netskope One sécurise l'ensemble des données d'une entreprise, qu'elles soient structurées ou non, gérées ou non, et hébergées dans un datacenter ou dans le cloud. Une étude d'incidence économique totale réalisée par Forrester a montré qu'un client type de Netskope obtenait les résultats opérationnels suivants :[6]

> « Je peux affirmer sans hésitation que nous avons diminué le risque [en déployant Netskope SSE] car au lieu de parer à l'urgence, nous pouvons nous concentrer sur les vulnérabilités et le travail concret. »
>
> **VP Expérience numérique**
>
> Entreprise de services financiers

Résultats opérationnels

- **Réduction de 80 % du risque d'une grave violation de données par une attaque externe**
- **Réduction de 60 % du délai moyen de résolution (MTTR)**
- **Réduction de 10 % des coûts d'infrastructure**
- **Réduction de 80 % du volume des tickets du service d'assistance**
- **Réduction de 15 % des interruptions non planifiées**
- **Augmentation de 30 % de l'efficacité des opérations réseau et de sécurité**
- **Amélioration de la protection de la propriété intellectuelle par la DLP**
- **Amélioration de la conformité réglementaire, en étant mieux préparé et plus réactif**
- **Meilleure résolution des problématiques ESG (environnementales, sociétales et de gouvernance)**

6. Forrester. « The Total Economic Impact of Netskope SSE », octobre 2024.

Le tour d'honneur grâce à Netskope One

Remporter la course contre la cybercriminalité requiert une stratégie, de la préparation et une bonne exécution. Lorsque la situation devient critique, il faut tout donner.

La solution unifiée de sécurité des données de Netskope One offre toutes les fonctionnalités dont les experts de la sécurité ont besoin pour protéger leurs précieuses machines :

- **Automatiser la reconnaissance et la classification des données d'entreprise où qu'elles résident ou circulent**
- **Remédier rapidement au risque d'exfiltration des données**
- **Parvenir efficacement à la conformité et à la confidentialité des données**
- **Réduire considérablement les risques internes**
- **Réduire l'exposition des données**
- **Fournir une expérience fluide à l'utilisateur final**
- **Garantir une utilisation sûre de l'IA générative dans l'organisation**
- **Gérer l'ensemble du cycle de vie des données**

« Nous considérons la cybersécurité comme un avantage concurrentiel, car elle nous aide à attirer de nouveaux clients, notamment ceux issus de secteurs pour lesquels une protection des données solide est un atout. »

CISO

Entreprise de services mondiale

« Netskope SSE nous a permis d'identifier de nombreux problèmes dont nous ignorions l'existence. Nous avons détecté des systèmes sur Internet qui échappaient à nos contrôles de sécurité … Cette découverte a été un choc et nous avons résolu ces problèmes. »

VP Expérience numérique

Entreprise de services financiers[7]

Netskope One

Protégez vos données grâce à la sécurité de Netskope One.

En savoir plus →

[7] Forrester. « The Total Economic Impact of Netskope SSE », octobre 2024.

À propos de Netskope

Netskope, un leader de la sécurité et des réseaux modernes, répond aux besoins des équipes de sécurité et de mise en réseau en fournissant un accès optimisé et une sécurité contextuelle en temps réel pour les utilisateurs, les appareils et les données, où qu'ils se trouvent. Des milliers de clients, dont plus de 30 parmi les entreprises du Fortune 100, font confiance à la plateforme Netskope One, à son moteur Zero Trust Engine et à son puissant réseau NewEdge pour réduire les risques et obtenir une visibilité et un contrôle complets sur l'activité du cloud, de l'IA, du SaaS, du web et des applications privées, en assurant la sécurité et en accélérant les performances sans sacrifice ni compromis.

Vous souhaitez en savoir plus ?

Demander une démo

Ressources associées

- La valeur d'une solution unifiée de sécurité des données
- Bilan de la gestion des risques liés aux données
- Exercices pratiques d'initiation à Netskope One SSE
- Exercices pratiques d'initiation à la DLP (Data Loss Prevention) de Netskope One

netskope