eBook

Les 5 points forts de la DLP moderne

netskope

Dans le monde d'aujourd'hui, où le cloud est le moteur de la transformation numérique et du travail hybride, les entreprises doivent aligner leurs initiatives de sécurité des données sur les dernières méthodes qui évoluent à la vitesse du cloud. En outre, chaque organisation a des besoins spécifiques en matière de protection des données et des cas d'usage uniques, car les programmes de protection des données ne sont jamais exactement les mêmes. C'est pourquoi seule une architecture de prévention des pertes de données (DLP) fournie par le cloud peut garantir une grande flexibilité, une excellente évolutivité et une puissance informatique illimitée. Le cloud signifie également que vous devez rester à jour tout le temps, avec des protections et des mises à jour disponibles en temps réel. Une technologie DLP en mode service dans le cloud est manifestement la bonne approche de protection des données d'entreprise, mais elle ne doit pas être le seul critère à prendre en compte pour passer à une stratégie de protection des données efficace.

Une technologie DLP doit être évolutive, riche en fonctionnalités, efficace et dotée d'une large couverture. Elle doit également offrir une grande efficacité afin de garantir une protection précise de tous les types de données, dans tous les environnements et contre tous les risques de perte de données.

Avant de passer d'un déploiement DLP existant à un déploiement qui répond aux exigences du travail hybride moderne, il convient de tenir compte de certaines directives architecturales et recommandations technologiques :

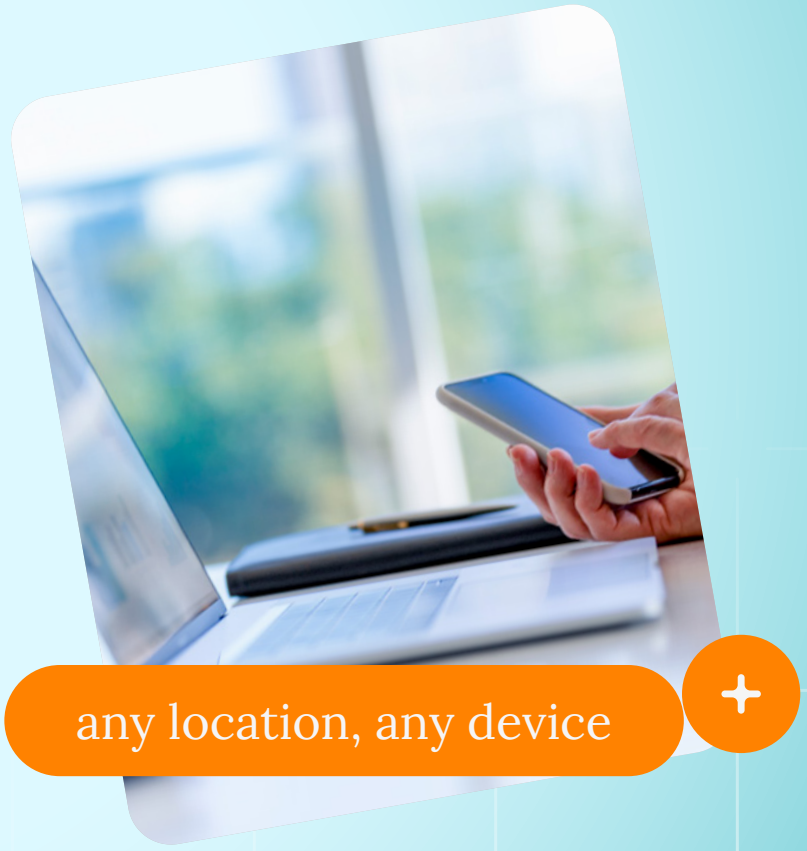
01

Exhaustivité de la couverture

Vous ne pouvez pas protéger ce que vous ne pouvez pas voir, et les données circulent aujourd'hui dans beaucoup plus d'environnements qu'auparavant. Les solutions DLP d'entreprise traditionnelles, généralement déployées sur le réseau physique, offrent une couverture étendue des canaux de données sur site, y compris les transmissions Web, le SMTP par e-mail et les endpoints. On peut raisonnablement s'attendre à ce qu'une solution moderne basée sur le cloud étende la protection aux référentiels basés sur le cloud, tels que les applications SaaS, IaaS et les e-mails dans le cloud, tout en assurant la couverture des environnements sur site, tels que les réseaux, les appareils et les e-mails. Il est toujours recommandé de s'assurer qu'une solution DLP pour le cloud offre une couverture complète de l'entreprise, tant pour le cloud que pour les canaux traditionnels sur site. Dans ce sens, il est également important de savoir que la plupart des solutions DLP dans le cloud sont conçues pour résoudre uniquement les cas d'usage dans le cloud et ne couvrent pas certains canaux sur site tels que les endpoints.

01

Aujourd'hui, de nombreux cas d'usage sont fondamentaux et doivent être correctement traités, comme le transfert de données sensibles à travers des milliers d'applications SaaS à risque non autorisées ou vers des instances personnelles d'applications SaaS autorisées telles qu'un compte Gmail personnel ou une instance OneDrive personnelle, ou encore vers des applications privées dans le cloud public ou dans le datacenter. Pour l'entreprise moderne hautement distribuée, composée de plusieurs succursales et d'une main-d'œuvre hybride à distance, la DLP doit protéger toutes les transmissions de données depuis n'importe où et depuis n'importe quel appareil, y compris les appareils managés et non managés, et même l'IoT. Le transfert de données sensibles sur une clé USB est également un vecteur de perte important qui nécessite d'être contrôlé, même lorsque ces appareils ne sont pas en ligne. Les e-mails sortants, sensibles par nature, sont un autre vecteur important de perte de données, ainsi que les communications confidentielles sur des applications de collaboration comme Slack et Teams.



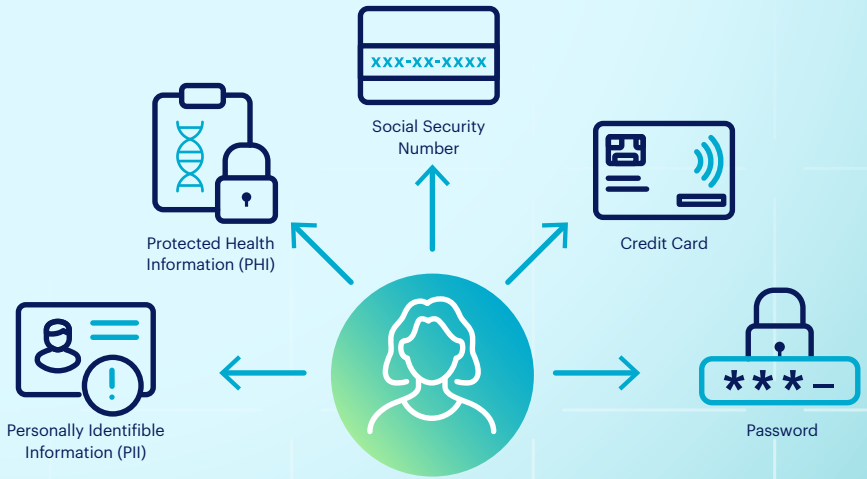
02

Capacités de détection des données de base

Une visibilité précise des données constitue une nécessité stratégique pour évaluer l'ensemble de l'environnement opérationnel et mettre en œuvre la stratégie de protection optimale. Tout commence par la découverte et la classification de toutes les données sensibles, y compris les informations personnelles identifiables (PII) structurées et non structurées, la propriété intellectuelle (PI), les informations confidentielles et les secrets commerciaux.

La classification manuelle des données par le propriétaire des données pouvant être un processus peu fiable, cette tâche doit également être automatisée dans la DLP au moyen d'un ensemble complet, et non partiel, de moteurs de détection. Ces moteurs définissent les politiques de détection ou les profils de données prédéfinis de l'organisation. Plus précisément :

- **Les identifiants de données** ont été et sont toujours incontournables à toute solution DLP. Ils doivent être capables d'identifier des milliers de types différents de données sensibles sur la base de critères de correspondance décrits qui caractérisent généralement des objets tels que le SSN, les informations sur les cartes de paiement ou les numéros de passeport, comme le nombre de chiffres, les modèles de texte, les séquences, les séparations et les mots-clés de proximité. Les fonctionnalités d'expression régulière (regex) sont un élément fondamental, mais encore faut-il savoir les utiliser. De nouveaux types de données et des cas d'usage modernes sont apparus avec les nouvelles exigences de conformité qui demandent de protéger la vie privée des individus de manière plus large. En fait, la présence d'un grand nombre d'identifiants de données prédéfinis est le premier élément à prendre en considération, mais il faut également tenir compte de la granularité des personnalisations des règles, comme les niveaux de gravité, l'étendue des contrôles de proximité, la logique booléenne, etc.



02

- Le nombre de **types de fichiers** pris en charge est un autre élément clé. Il existe des milliers de types de données qui peuvent contenir des informations sensibles : texte, présentation, e-mail, images et captures d'écran, tableur, CAO, posts sociaux, formulaires en ligne, messages Slack et autres canaux de discussion, encapsulation, pièces jointes, graphiques et images comme JPEG et PDF, etc.
- **Les classificateurs de données d'intelligence artificielle/apprentissage automatique (IA/AA)** contribuent à la découverte et à l'identification des données. Les règles définies manuellement constituent le fondement de la détection des données, mais dans le monde moderne, les moteurs automatisés fournissent une aide précieuse en renforçant la précision de la détection et de la catégorisation des données sensibles. Ils s'adaptent également aux conditions changeantes et identifient les similitudes de contenu.
- **La correspondance exacte des données (EDM)** désigne une méthode traditionnelle mais presque infaillible, conçue pour détecter des informations spécifiques issues de sources de données structurées telles que des feuilles de calcul et des bases de données. Avec l'EDM, une solution DLP peut prendre les empreintes digitales et indexer des jeux de données d'enregistrements confidentiels. Ces informations, une fois combinées, peuvent identifier un individu, comme les noms et prénoms des clients, les numéros de sécurité sociale, les adresses, les numéros d'identification, etc., ou des enregistrements financiers qui définissent les ressources financières d'un individu, comme les numéros de carte de crédit ou les numéros de compte bancaire, voire même des informations sur la santé ou des bases de données d'identification et de tarification des produits. Ces informations indexées doivent ensuite être surveillées et identifiées partout où les flux de données sont censés se produire.

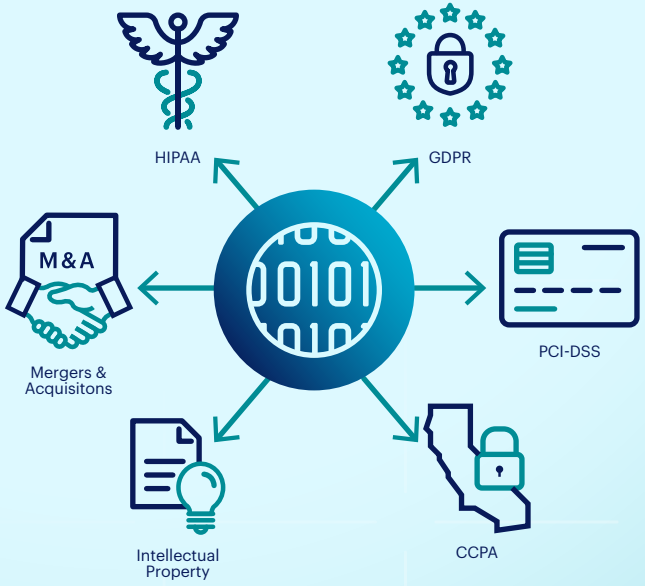
Une remarque concernant l'EDM

Pour que l'EDM soit efficace et précise, elle doit être capable d'exploiter des conditions granulaires pour faire correspondre divers éléments des données indexées et des combinaisons de champs de données d'un enregistrement particulier : ceux présentant une importance particulière. L'EDM à grande échelle est un facteur très important, en particulier pour les grandes entreprises et pour les organisations qui cherchent à se développer. Des millions, voire des milliards de données doivent être pris en charge.

03

Profilage des données de demain

Ne cherchez pas uniquement les identifiants de données dont vous avez besoin aujourd'hui. Recherchez plusieurs milliers d'identifiants de données prédéfinis, y compris des modèles localisés tels que les cartes d'identité nationales, car vos besoins futurs augmenteront très probablement avec la taille de votre entreprise et la maturité de la protection des données. Recherchez la présence de modèles de conformité réglementaire que vous devez prendre en charge pour vérifier que les dernières normes y figurent toutes : RGPD, CCPA, PII, PCI, PHI, pour ne citer que quelques exemples des réglementations et types les plus connus. Comprenez le niveau d'engagement de l'éditeur de manière à respecter les exigences de conformité les plus récentes, et déterminez si l'éditeur est susceptible de les étendre à l'avenir. Il est essentiel de pouvoir modifier les regex ou les identificateurs existants ou de créer des identificateurs de données personnalisés avec des contrôles granulaires. En effet, chaque organisation a des besoins différents, par exemple un type d'information spécifique peut être considéré comme sensible pour cette organisation particulière.



04

Fonctionnalités avancées de détection des données

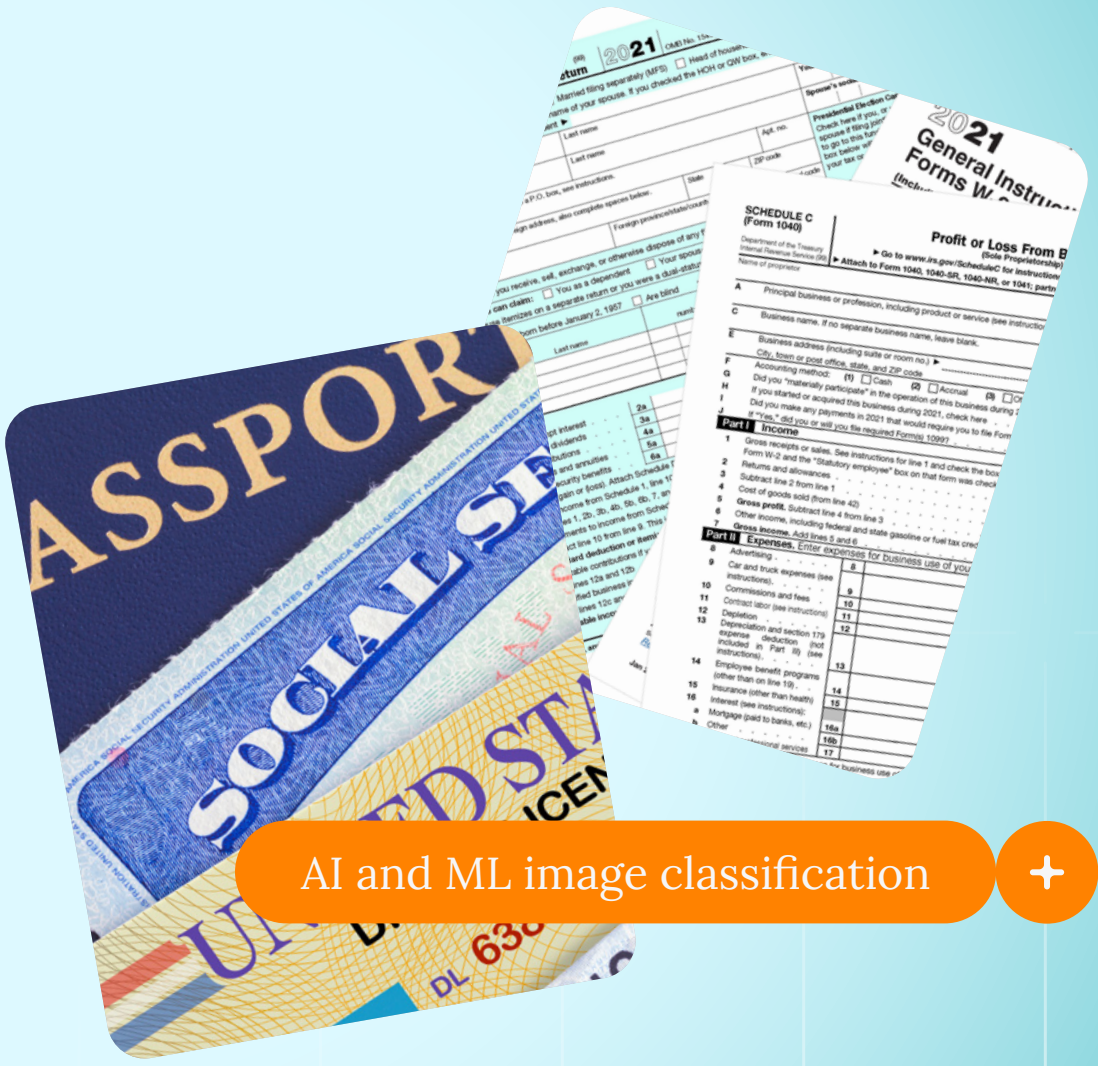
Au fil des ans, les données ont également évolué de manière significative, augmentant en volume, en variété et en vitesse, et sont plus déstructurées que jamais. L'introduction de nouveaux types de données et de méthodes modernes de partage et de transmission des données, la croissance massive des volumes de données et les nouvelles exigences de conformité exigent des moyens avancés de détection des informations sensibles. Les solutions DLP existantes ont introduit des moyens de détection avancées dans le passé, mais commencent à ne plus pouvoir produire des résultats de détection précis en raison d'un manque de puissance de calcul et d'échelle. Par conséquent, elles génèrent de plus en plus de faux positifs qui entravent les flux commerciaux et submergent les équipes de réponse aux incidents.

D'autre part, la majorité des solutions DLP récentes pour le cloud sont peut-être encore immatures et non éprouvées en matière de performance. Il est important de vérifier la présence et le niveau de sophistication des moyens de détection avancés suivants :

- Dans le monde actuel, les utilisateurs trouvent très pratique de prendre des photos de documents, de formulaires, de cartes d'identité, de tableaux blancs, et même des photos d'autres photos. Par exemple, les captures d'écran sont un vecteur très courant pour capturer rapidement des informations et les partager immédiatement avec un collègue. En conséquence, la **reconnaissance optique de caractères (OCR)** et la reconnaissance d'images basée sur l'IA gagnent en importance dans le cadre d'une stratégie de protection des données moderne d'avenir. Avec l'OCR, une solution DLP peut extraire des informations textuelles d'une image et peut ensuite appliquer une classification des données en fonction des politiques de détection mises en place.
- **La classification d'images par IA et AA** est fondamentale pour reconnaître les types de fichiers et de documents courants comme les cartes SSN, les brevets et les documents de fusion et d'acquisition, les formulaires fiscaux, le code source, les captures d'écran de bureau, les passeports et autres pièces d'identité, etc. sans nécessairement extraire le contenu que ces ressources contiennent. Ces méthodes de détection doivent offrir un niveau de sophistication avancé pour être en mesure de reconnaître les images à travers des variations comme des morceaux de contenu flous, émiettés et endommagés, avec des informations qui peuvent être difficiles à lire clairement. Cela s'explique par le fait que les photos et les captures d'écran peuvent être prises rapidement et dans des conditions de lumière médiocres ou inadaptées, ou qu'un document peut être endommagé et vieilli.

04

- **L'empreinte digitale des fichiers et des documents** constitue une autre fonctionnalité avancée que de nombreuses organisations trouvent essentielle. Certains documents stratégiques, la propriété intellectuelle et les fichiers hautement confidentiels doivent être protégés à tout prix contre l'exfiltration partielle et complète et les reproductions. L'empreinte du fichier peut indexer des documents entiers, puis détecter des copies exactes ou même partielles des informations qu'ils contiennent avec certains degrés de similitude, lorsque ce contenu se trouve dans des environnements et des canaux de transmission considérés comme risqués, comme un téléchargement vers une instance privée d'une application e-mail.



05

Protection des données en fonction du risque, un modèle prêt pour le zero trust

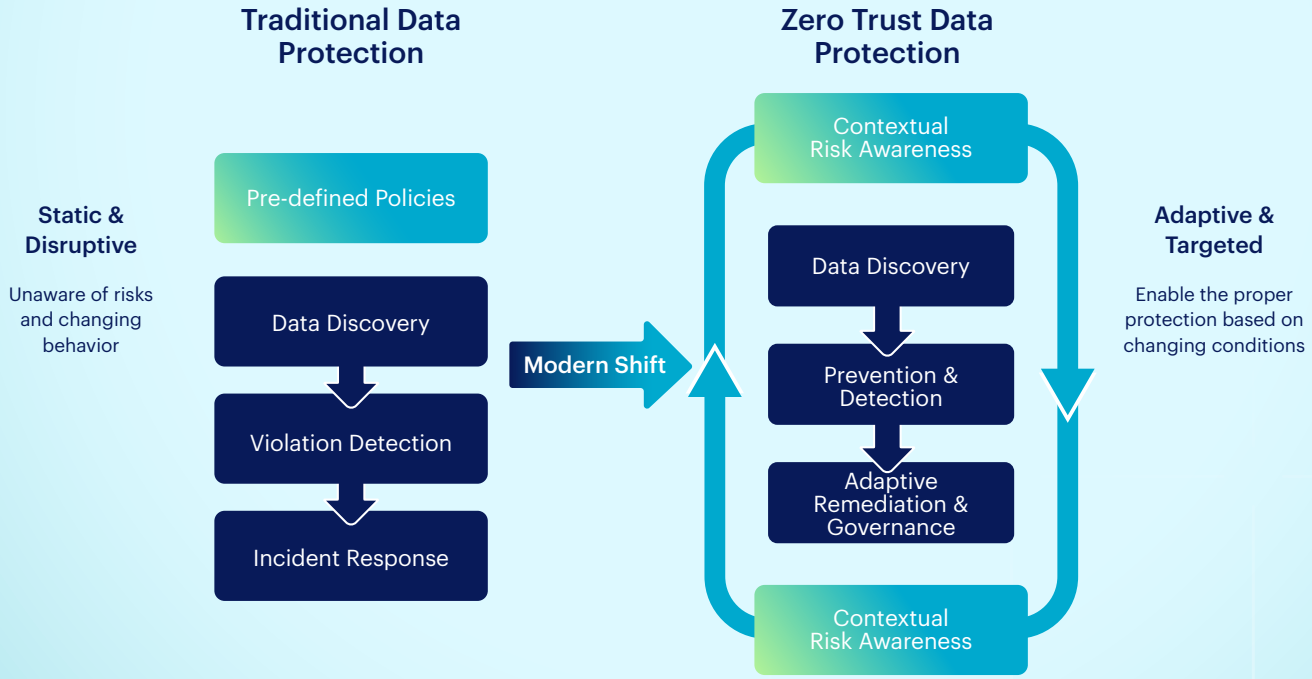
La transformation numérique a changé à jamais notre paradigme opérationnel, et nécessite un modèle à la hauteur. Le zero trust est une stratégie moderne qui place les contrôles de sécurité au niveau des données elles-mêmes en tant que nouveau périmètre, et remplace la confiance implicite par une appréciation continue et évolutive du risque afin de s'adapter en permanence à l'évolution des conditions de risque. Les contrôles de données du passé ont entraîné des frictions opérationnelles et entravé la création de valeur parce qu'ils manquaient de contexte. C'est pourquoi la DLP traditionnelle manque d'efficacité : Le contexte commercial et la conscience des risques n'étaient pas suffisants pour permettre de prévenir les mouvements de données. La plupart des décisions de remédiation des incidents dans la DLP devaient être prises manuellement par l'équipe de réponse aux incidents, qui ne disposait pas non plus d'un contexte de risque et de comportement suffisant. Pour cette raison, la DLP traditionnelle est aujourd'hui perçue comme un frein à l'activité, surtout lorsque le mode blocage est activé, plutôt que comme une solution efficace de protection des données. En réalité, la plupart des entreprises l'utilisent comme un outil de découverte des données et de mise en conformité, travaillant plutôt en mode surveillance afin d'éviter les problèmes.

Avec l'application du zero trust, ces défis appartiennent au passé. La technologie de protection des données doit passer d'un modèle statique composé de politiques fixes prédéfinies, dépourvues de contexte et ignorant les risques et l'évolution des comportements, à une approche zero trust dynamique et évolutive capable d'exploiter le contexte de sécurité et d'activer automatiquement et en permanence l'action de protection appropriée en fonction de l'évolution des conditions.

La réponse automatisée à la protection des données nécessite des processus définis et des politiques granulaires ainsi que des règles d'engagement claires, à savoir quelles actions entreprendre dans quelles conditions et avec quel degré de confiance. La DLP doit s'intégrer au plus grand nombre possible de points de contrôle de sécurité, ingérer continuellement leurs journaux et leurs résultats, et les exploiter de manière dynamique. Une solution DLP prête pour le zero trust doit prendre en compte les risques organisationnels provenant des utilisateurs, des appareils, des données, des mises en réseau et des applications afin d'obtenir une connaissance approfondie des risques et de toujours fournir la bonne action de remédiation. Par exemple, la surveillance du comportement des utilisateurs, des appareils et des applications fournit des informations précieuses sur les activités anormales des utilisateurs, les actions potentiellement malveillantes, les applications à risque, les lieux de connexion dangereux, les positions non sécurisées et les indicateurs de compromission.

05

Pour être vraiment efficace, une solution de protection des données zero trust doit surveiller ce qui se passe et qui fait quoi sur l'ensemble de l'infrastructure de l'entreprise, y compris les clouds, les utilisateurs distants et les appareils non managés.



Pour en savoir plus

Netskope est un leader mondial de la cybersécurité qui révolutionne la sécurité du cloud, des données et des réseaux pour aider les organisations qui appliquent les principes du Zero Trust à protéger leurs données. La plateforme Netskope Intelligent Security Service Edge (SSE) est rapide, facile à utiliser et sécurise vos collaborateurs, vos appareils et vos données, où qu'ils se trouvent.

Découvrez comment Netskope aide ses clients à se préparer à tout, tout au long de leur parcours de protection des données.

netskope