Guide du marché pour la prévention des pertes de données

9 avril 2025 - ID G00801998 - 46 min de lecture

Par Andrew Bales , Franz **Hinner** et **3 autres**

La DLP est un marché mature, mais les organisations modernes explorent des solutions complètes qui vont au-delà des méthodes DLP traditionnelles. Les responsables de la sécurité et de la gestion des risques doivent privilégier des techniques de sécurité des données adaptatives et centrées sur l'utilisateur, basées sur les risques, afin de renforcer la sécurité des données de leur organisation.

Aperçu

Principales conclusions

- Les projets de prévention des pertes de données (DLP) qui ne sont pas liés à des initiatives ou des cas d'utilisation plus vastes axés sur l'entreprise sont souvent le signe d'un programme de gouvernance de la sécurité des données inexistant ou immature . Privilégier des solutions technologiques sans fondement programmatique se traduit par des cas d'utilisation et des exigences incomplets pour les outils DLP, ce qui complique le processus de sélection et réduit les chances de réussite du projet.
- Les solutions DLP intégrées (IDLP) , traditionnellement moins robustes et complètes que les plateformes DLP d'entreprise (EDLP), réduisent l'écart en termes de couverture des canaux DLP, de détection, de précision des politiques et de parité des fonctionnalités.
- Le marché de la DLP est saturé de plateformes DLP traditionnellement axées sur le contenu . Ces solutions ne répondent pas toujours pleinement aux exigences complexes

et volatiles des organisations modernes en matière de sécurité des données, telles que les réglementations sectorielles et de conformité, la minimisation des risques internes et l'évolution des vecteurs d'exfiltration de données.

- La sécurisation des données dans des environnements complexes a compliqué le processus de sélection des fournisseurs de solutions DLP. Il peut être difficile pour les responsables SRM de différencier les fournisseurs proposant des fonctionnalités sur site adaptées au cloud de ceux proposant des solutions cloud natives plus modernes.

Recommandations

- Définissez une stratégie DLP qui s'aligne sur les initiatives commerciales de l'organisation et les meilleures pratiques de gouvernance de la sécurité des données en identifiant les résultats commerciaux critiques et en sélectionnant des produits DLP qui permettent et prennent en charge les résultats définis .
- Évaluer le marché DLP par rapport aux besoins de l'organisation en évaluant les solutions EDLP et IDLP pendant le processus de sélection technologique.
- Répondez à des exigences de sécurité des données de plus en plus complexes et diverses en sélectionnant une solution DLP qui offre des techniques DLP complètes et adaptatives, incluant une détection basée sur le contexte et le contenu , en mettant l'accent sur la détermination de l'intention de l'utilisateur avec les données et la gestion des risques internes.
- Gagnez en visibilité et en contrôle sur les données dans le cloud en investissant dans des outils DLP qui prennent en charge une stratégie cloud native , en particulier si une partie importante des données sensibles réside dans le cloud public ou dans diverses applications SaaS.

Hypothèses de planification stratégique

D'ici 2027, 70 % des RSSI des grandes entreprises adopteront une approche consolidée pour traiter à la fois les risques internes et les cas d'utilisation d'exfiltration de données .

D'ici 2027, les organisations intégrant des capacités de détection des intentions et de correction en temps réel dans les programmes DLP réaliseront une réduction d'un tiers des

risques internes.

Définition du marché

Ce document a été révisé le 25 avril 2025. Le document que vous consultez est la version corrigée. Pour plus d'informations, consultez la page « Corrections » sur gartner.com.

Gartner définit la prévention des pertes de données (DLP) comme un contrôle technique visant à prévenir la perte de données afin de se conformer à la réglementation sur les données personnelles, d'empêcher toute divulgation involontaire, de minimiser les risques internes et de garantir que les données sensibles ne soient pas trop accessibles. Les contrôles DLP sont généralement appliqués pour réduire les risques liés aux données non structurées : les données au repos et les données en mouvement. Selon l'état des données, la DLP applique des contrôles de détection, de prévention ou de correction, notamment l'alerte, la mise en quarantaine, le blocage, la suppression ou la restriction d'accès.

La DLP peut être une mesure efficace pour atténuer les risques liés au traitement des données sensibles, dont beaucoup sont inhérents aux données. Voici quelques exemples de risques inhérents aux données :

- Informations personnelles identifiables (PII) qui, si elles étaient compromises, ne répondraient pas aux exigences réglementaires
- Propriété intellectuelle (PI) qui, si elle était volée, porterait atteinte à l'avantage concurrentiel d'une organisation
- Paiements non sécurisés et données financières qui, en cas de violation, nécessiteraient des dépenses excessives pour être rectifiées

La DLP permet d'identifier les risques liés aux données et de mettre en place des contrôles pour prévenir leur perte. En prévenant la perte ou la divulgation non autorisée de données sensibles, la DLP joue un rôle crucial pour minimiser les atteintes à la réputation de l'organisation, éviter les amendes pour non-conformité et atténuer les risques de vol de propriété intellectuelle et de perte d'avantage concurrentiel.

Les contrôles DLP pour les données en mouvement constituent la dernière ligne de défense contre la perte de données . Ils inspectent les transferts de données vers des destinations externes et filtrent celles qui contiennent des données sensibles afin de minimiser les

risques. Ces contrôles mettent en œuvre diverses mesures, telles que la journalisation et l'audit, les alertes, le blocage ou d'autres méthodes, pour minimiser, voire éliminer, le risque de perte de ces données.

Des outils de prévention des pertes de données (DLP) existent également pour les données sensibles non structurées au repos . Ces solutions analysent les référentiels de stockage à la recherche d'éléments de données sensibles au sein de ces données et appliquent des contrôles pour classer, déplacer, supprimer et restreindre les accès non autorisés, ou pour remédier aux risques liés à ces données sensibles. Des contrôles efficaces des données au repos peuvent minimiser les répercussions d'une violation de données ou prévenir la surexposition des données sensibles.

Caractéristiques obligatoires

Les caractéristiques obligatoires pour ce marché incluent :

- Détection de données sensibles au repos ou en mouvement sur plusieurs canaux (par exemple, courrier électronique, point de terminaison, réseau, navigateur, cloud, IA générative [GenAI])
- Application automatisée de contrôles préventifs (par exemple, blocage, cryptage, alerte, justification de l'utilisateur)
- Flux de travail automatisé de réponse aux incidents
- Logique d'inspection de contenu centrée sur les données via un canal unique (par exemple, détection d'un utilisateur envoyant par courrier électronique des données de carte de crédit d'entreprise à son courrier électronique personnel)
- Modèles de politiques pour les types de données réglementées (par exemple, PII, informations de santé protégées [PHI], données de paiement ou financières)
- Rapports d'incidents granulaires
- Intégration avec les plateformes de gestion des incidents et des événements de sécurité (SIEM) pour la réponse aux incidents

Caractéristiques communes

Les caractéristiques communes de ce marché incluent :

- Intégration avec les solutions d'analyse des entités et du comportement des utilisateurs (UEBA) pour la corrélation entre la perte de données et le risque interne
- Logique d'inspection de contenu centrée sur l'utilisateur via une corrélation multicanal (par exemple, détection d'un utilisateur envoyant par courrier électronique des données de carte de crédit d'entreprise à son courrier électronique personnel *et* détection du même utilisateur téléchargeant des données de vente confidentielles à partir de la plate-forme CRM d'entreprise)
- Notation dynamique des risques utilisateurs basée sur le rôle et le comportement
- Modèles de politiques pour les types de données non réglementés (par exemple, informations non classifiées contrôlées [CUI], IP, code source)
- Application des balises de classification des données
- Contrôles d'accès basés sur les rôles pour la réponse aux incidents et l'examen
- Détection de contenu pour les données stockées sur les appareils mobiles

Description du marché

Les solutions DLP combinent des fonctionnalités pour détecter et prévenir les pertes de données. Celles-ci incluent l'étiquetage de classification des données , des techniques d'inspection de contenu centrées sur les données et l'analyse contextuelle pour identifier les contenus sensibles et analyser les actions liées à leur utilisation . Elles surveillent l'activité des utilisateurs sur les données et évaluent si les actions tentées sont appropriées, conformément à une politique DLP prédéfinie. Cette politique détaille les utilisations acceptables, dans des contextes spécifiques, de types de contenu et/ou d'étiquettes de classification prédéterminés .

Gartner catégorise les solutions DLP comme suit (voir Figure 1) :

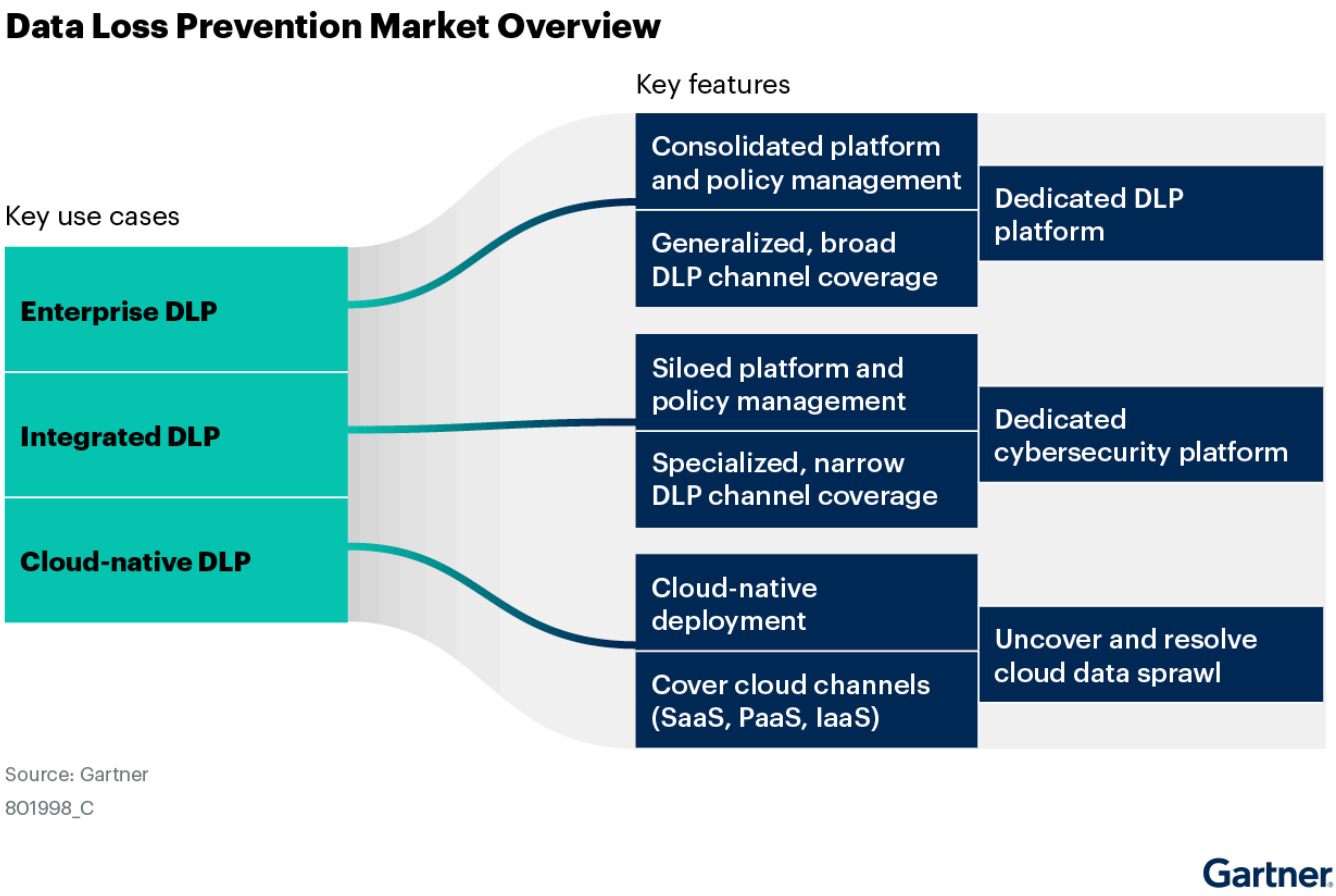
- Les solutions **EDLP** offrent des fonctionnalités centralisées de gestion des politiques et de reporting sur tous les canaux courants d'exfiltration de données (e-mail, terminaux, réseau, navigateur et cloud). Cette plateforme centralisée permet aux responsables de la sécurité et de la gestion des risques (SRM) de définir et de déployer de manière cohérente des politiques DLP, de mettre en œuvre des contrôles et de surveiller les alertes sur un ou plusieurs canaux . Les solutions EDLP intègrent généralement une

logique avancée de détection de contenu pour identifier les contenus complexes et combinent des contrôles granulaires et non binaires afin de prévenir la perte de données et de remédier aux incidents. Les solutions EDLP incluent souvent une détection basée sur le contexte et l'intention, ce qui améliore la précision des politiques et fournit le contexte des risques internes nécessaire aux équipes de réponse aux incidents DLP. Elles sont vastes et offrent des offres flexibles applicables à divers cas d'utilisation, notamment la conformité réglementaire, la conformité aux politiques internes et la sécurité des données de propriété intellectuelle (PI).

- **Les solutions IDLP** incluent des fonctionnalités DLP intégrées nativement à une autre solution, comme une passerelle de messagerie sécurisée ou une plateforme de protection des terminaux (EPP). Les solutions IDLP ne détectent ni ne préviennent généralement la perte de données sur tous les canaux d'exfiltration, couvrant généralement un ou deux canaux. Certaines fonctionnalités, telles que la logique de détection des politiques prêtes à l'emploi, la prise en charge des types de fichiers et de données, les actions préventives ou le reporting, peuvent être limitées par rapport aux solutions EDLP. De plus, l'orchestration des politiques entre d'autres solutions IDLP ou EDLP peut être manuelle , et la corrélation d'événements spécifiques entre plusieurs solutions peut représenter une charge pour les responsables SRM (voir note 1). Ces dernières années, cependant, la parité des fonctionnalités entre les solutions IDLP et EDLP s'est considérablement accrue, et de nombreuses solutions IDLP représentatives offrent désormais des fonctionnalités similaires à leurs homologues EDLP pour le sous-ensemble de canaux qu'elles couvrent.

- Les solutions **DLP cloud-natives** offrent des fonctionnalités DLP aux applications métier SaaS et aux fournisseurs de services cloud (FSC) hyperscale. Elles sont déployées en mode SaaS ou via une intégration API avec les entrepôts de données. Les FSC et les applications métier SaaS incluent généralement une classification et des contrôles DLP des données au sein de leurs propres environnements, sans recourir à des outils tiers. Les fournisseurs de solutions DLP cloud-natives tiers (non FSC) prennent souvent en charge des stratégies multicloud complexes , et certains proposent une classification des données en complément de leurs contrôles DLP.

Figure 1 : Aperçu du marché DLP



Orientation du marché

Aujourd'hui , le marché de la DLP évolue pour pallier les limites bien connues des approches traditionnelles, qui reposaient largement sur une inspection de contenu centrée sur les données, gourmande en ressources, et entraînaient souvent des problèmes de performance avec un nombre élevé de faux positifs. Les approches traditionnelles de la DLP étaient également réactives, prévenant la perte de données uniquement à la frontière de l'entreprise, plutôt que d'analyser les risques utilisateurs et d'adapter les contrôles pour sécuriser les données tout au long de leur cycle de vie. Le marché de la DLP évolue vers une logique de détection plus sophistiquée et des analyses supplémentaires (données ou identité) sont nécessaires pour accroître la fidélité des alertes DLP.

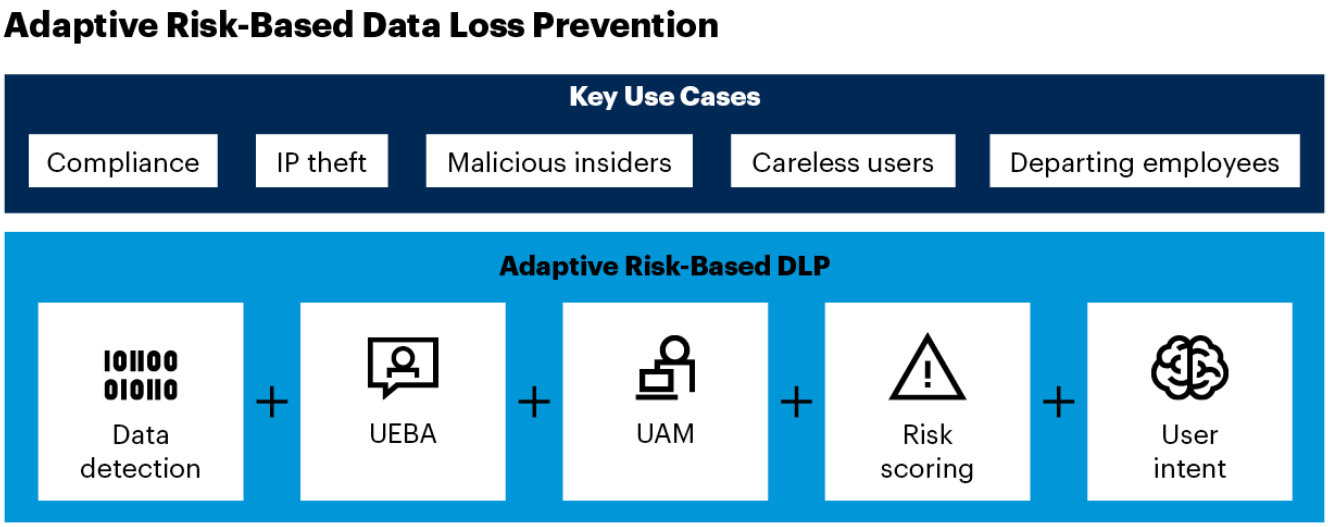
Dans le cadre de cette évolution du marché, Gartner a observé que les entreprises envisagent des approches intégrées de la DLP. En effet, les fonctionnalités DLP deviennent de plus en plus des contrôles standard dans d'autres plateformes de sécurité, telles que la sécurité de la messagerie électronique, la protection des terminaux , la sécurité des services en périphérie (SSE) , les technologies de gestion des risques internes et la gouvernance de l'accès aux données (pour les données au repos) . Bien que la consolidation des fournisseurs de cybersécurité reste un objectif pour les leaders de la SRM, Gartner a observé que les

clients s'orientent dans la direction opposée avec leurs approches DLP, en optant pour des approches IDLP. Pour ces entreprises, les stratégies IDLP complexifient la gestion des politiques et des consoles, mais peuvent réduire les coûts d'approvisionnement, car elles choisissent souvent des outils déjà présents dans leur portefeuille de fournisseurs.

De nombreux fournisseurs de solutions DLP intègrent la classification des données pour améliorer leur logique de détection des politiques. La classification des données, proposée via une fonctionnalité native ou une intégration tierce , fournit une méthode standard pour déterminer la sensibilité des données. Les fournisseurs de solutions DLP qui prennent en charge la classification des données complètent généralement leur logique de politique DLP prête à l'emploi par la détection de l'étiquette de classification des données précédemment appliquée, manuellement ou automatiquement, aux données (voir la note 2) . Concrètement, cela peut ressembler à la création d'une politique DLP avec plusieurs conditions de détection (par exemple, détecter une chaîne d' informations personnelles identifiables (PII) et le mot-clé « confidentiel » dans le même fichier) . L'utilisation de plusieurs conditions de détection permet aux responsables SRM de « superposer » la logique de détection au sein de la politique DLP afin d'en accroître la précision. Un étiquetage approprié des données simplifie le processus global de sécurité des données , car les organisations peuvent facilement distinguer les données sensibles des données non sensibles (voir la note 3).

Les solutions de DLP adaptative basée sur les risques s'appuient souvent sur l'analyse du comportement des utilisateurs et des entités (UEBA) et la surveillance de l'activité des utilisateurs (UAM) pour compléter ou remplacer la détection des données. Ces solutions peuvent analyser les activités des utilisateurs, leurs schémas de communication et d'autres informations contextuelles dérivées de leur activité afin de détecter les écarts anormaux par rapport au comportement normal et d'établir leurs intentions . Cela permet de détecter précocement les comportements à risque des utilisateurs , ce qui permet aux responsables SRM de dissuader les initiés malveillants, de sensibiliser les utilisateurs négligents et de surveiller les départs . Comme ces outils ne reposent pas principalement sur la détection des données, les approches de DLP adaptative basée sur les risques liés aux données peuvent être exploitées pour répondre à un plus large éventail de cas d'utilisation, tels que le vol de propriété intellectuelle, l'utilisation de données sensibles par des initiés malveillants et des utilisateurs négligents, ou le départ d'employés souhaitant conserver leur propriété intellectuelle lorsqu'ils partent chez un concurrent (voir Figure 2).

Figure 2 : DLP adaptatif basé sur les risques



Source: Gartner
Note: IP = intellectual property; UEBA = user and entity behavior analytics; UAM = user activity monitoring
801998_C

Gartner

Grâce à cette approche adaptative basée sur les risques, les fournisseurs de DLP attribuent à chaque utilisateur un score de risque qui, en fonction de son comportement et de ses intentions perçues, augmente ou diminue au fil du temps. Les responsables SRM disposent ainsi d'une vue d'ensemble des utilisateurs les plus à risque et de leurs tendances de risque au fil du temps. Les scores de risque commencent généralement par une valeur de base déterminée par le rôle de l'utilisateur, son activité de base ou des utilisateurs similaires au sein de l'organisation, et peuvent être influencés par divers comportements et indicateurs de risque .

Cette convergence entre surveillance et détection centrées sur les données et analyse comportementale permet une meilleure détection des tentatives d'exfiltration de données. Les alertes DLP sont enrichies d'informations contextuelles issues des comportements anormaux des utilisateurs, de leurs intentions à risque perçues, d'une meilleure notation des risques et d'une surveillance en temps réel. Cela permet aux équipes de sécurité de prioriser plus efficacement leurs efforts de réduction des risques, en se concentrant d'abord sur les risques les plus critiques. De plus, les fournisseurs intègrent l'IA à leurs produits, ce qui joue un rôle essentiel dans l'amélioration de l'élaboration des politiques, de la précision de la détection, ainsi que du tri et de la réponse aux incidents.

Analyse de marché

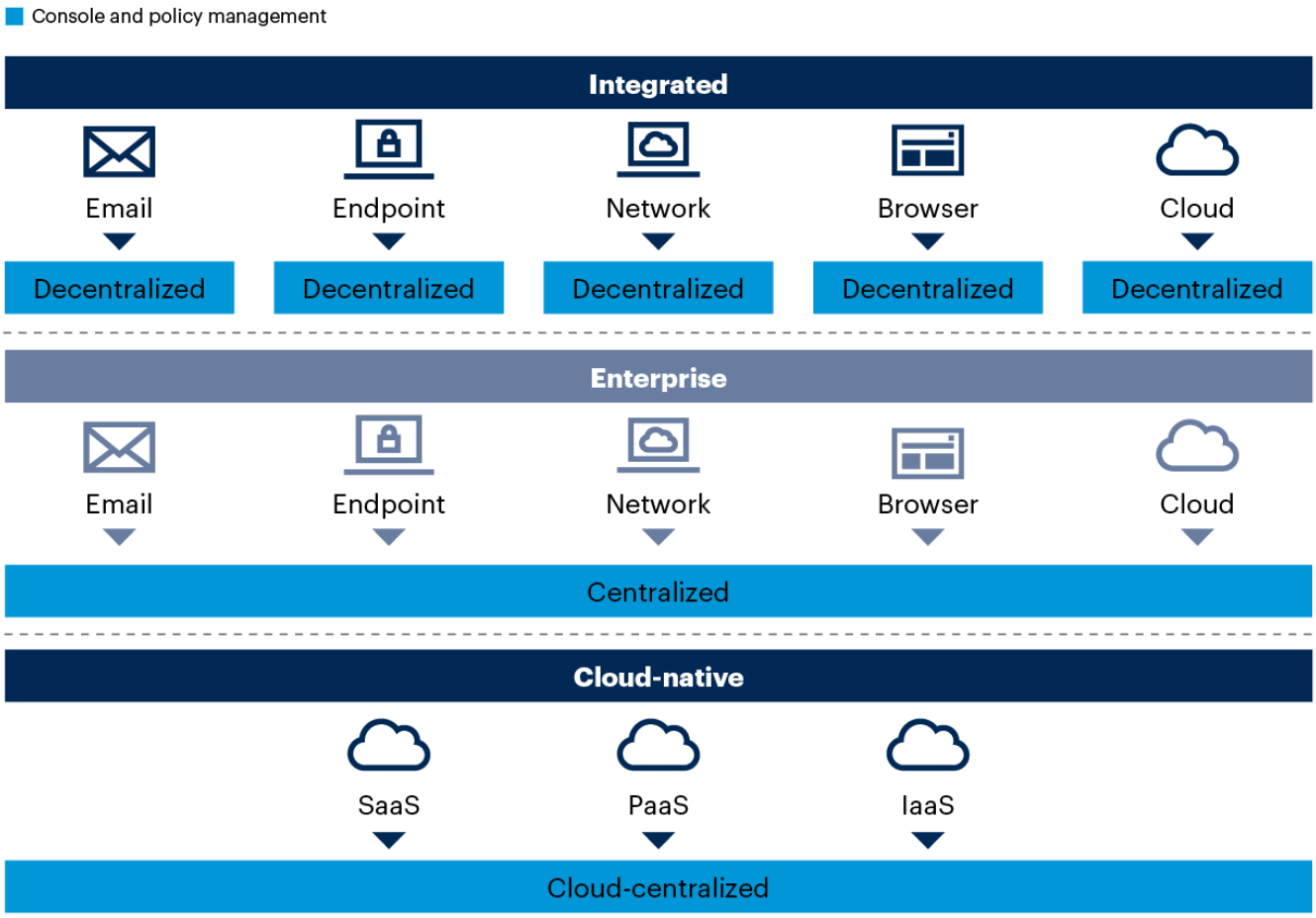
La gestion du risque d'exfiltration de données demeure un défi majeur pour les clients de Gartner, le nombre de demandes de renseignements à ce sujet restant constamment élevé. Les organisations ont recours à la DLP pour diverses raisons, notamment le respect des réglementations en matière de confidentialité, les préoccupations concernant la fuite de données personnelles, ou la sécurisation de la propriété intellectuelle (code source, secrets commerciaux ou brevets). Plus récemment, certaines organisations ont exprimé leur intérêt pour la DLP afin de contrôler l'accès des machines aux informations sensibles. Ce problème a été exacerbé par l'adoption généralisée de l'IA générative (GenAI) et la prolifération continue des données organisationnelles .

Ces problématiques ont donné lieu à un ensemble complexe de problématiques architecturales et opérationnelles auxquelles les responsables SRM doivent faire face. Le cadre AI TRiSM de Gartner complète la DLP, car il vise notamment à minimiser le risque de perte de données sensibles pour GenAI grâce à une gouvernance efficace de l'information. AI TRiSM n'entre pas dans le cadre de cette étude ; pour plus d'informations, consultez **la section Utiliser TRiSM pour gérer la gouvernance, la confiance, les risques et la sécurité de l'IA** .

Ces dernières années, la DLP a commencé à évoluer, passant d'une technologie commerciale à une technologie intégrée, reflétant l'importance cruciale de la sécurité des données pour les responsables SRM . Les contrôles techniques visant à prévenir la perte de données sont devenus moins binaires et ont évolué vers des approches qui favorisent les résultats commerciaux plutôt que de les bloquer complètement. Ces approches incluent la tokenisation, le masquage et les contrôles d'accès granulaires, en complément des contrôles binaires traditionnels de type « blocage ou autorisation ». Si les solutions IDLP étaient initialement moins robustes que les systèmes DLP d'entreprise, leurs fonctionnalités se sont considérablement améliorées et sont désormais très prometteuses. De nombreux fournisseurs qui ont commencé par proposer des fonctionnalités IDLP ont continué à évoluer et peuvent désormais proposer des fonctionnalités d'une complexité similaire à celle de leurs homologues EDLP. La figure 3 offre une comparaison visuelle plus détaillée des différents types de solutions DLP (intégrées, d'entreprise et cloud-natives).

Figure 3 : DLP intégré, d'entreprise ou cloud-natif

Integrated Versus Enterprise Versus Cloud-Native Data Loss Prevention



Source: Gartner
Note: PaaS = platform as a service; IaaS = infrastructure as a service
801998_C

Gartner

Bien que l'IDLP devienne rapidement plus viable pour les organisations, les responsables SRM qui mettent en œuvre un projet DLP doivent d'abord déterminer les canaux d'exfiltration de données les plus risqués pour l'organisation. L'architecture DLP optimale pour une organisation dépendra fortement des cas d'utilisation prédéfinis (voir **Choisir la bonne architecture de prévention des pertes de données**).

> Il n'existe pas de technologie DLP idéale pour toutes les organisations. La meilleure technologie est celle qui répond le mieux aux

besoins spécifiques de l'organisation en matière de DLP.

IDLP

Les fournisseurs proposant l'IDLP proposent des fonctionnalités DLP intégrées à une plateforme de sécurité plus large. Bien que les fournisseurs IDLP ne couvrent généralement qu'un sous-ensemble des canaux d'exfiltration de données couverts par l'EDLP, certains intègrent des fonctionnalités IDLP à plusieurs produits de sécurité. Par exemple, un même fournisseur de cybersécurité peut proposer des fonctionnalités DLP intégrées à ses propres produits de sécurité de messagerie et de protection des terminaux.

En partie en raison de cette approche décentralisée, les organisations manifestent un intérêt croissant pour les approches IDLP comme alternative à l'EDLP. Les fournisseurs IDLP sont présents dans plusieurs produits de sécurité clés : plateformes de sécurité de messagerie, EPP, SSE, gestion des risques internes, gouvernance de l'accès aux données et gestion de la sécurité des données.

Sécurité des e-mails

Le courrier électronique est l'un des moyens les plus courants de transmission d'informations sensibles , que ce soit accidentellement ou intentionnellement. Par conséquent, la sécurisation des e-mails et la mise en place de contrôles pour détecter et prévenir les pertes de données via les e-mails sortants sont une priorité pour la plupart des clients. Parmi les cas d'utilisation courants de la prévention des pertes de données par e-mail, on peut citer :

- Surveillance et contrôle des données sensibles dans le trafic de courrier électronique à l'aide d'une passerelle de messagerie sécurisée (SEG) ou d'un contrôle de sécurité de messagerie cloud intégré (ICES)
- Découverte et contrôle des données sensibles au repos sur le serveur de messagerie

La plupart des fournisseurs de sécurité de messagerie incluent désormais, ou peuvent fournir, des fonctionnalités DLP dans leurs produits. Certaines solutions de sécurité de messagerie peuvent également détecter les pertes de données accidentelles, comme les e-

mails mal acheminés. Ces solutions utilisent des algorithmes basés sur l'IA pour suivre les habitudes d'utilisation des e-mails des utilisateurs et les inviter à confirmer que l'adresse e-mail est correcte. Cela se produit le plus souvent lorsque l'e-mail ou la pièce jointe contient des informations sensibles et est adressé à une adresse externe avec laquelle l'utilisateur n'a jamais eu de correspondance antérieure. La détection et la prévention des e-mails mal acheminés sont essentielles pour les entreprises des secteurs d'activité où la sécurité IP est essentielle (par exemple, l'industrie manufacturière, l'industrie pharmaceutique) ou lorsque les utilisateurs peuvent traiter des informations sensibles pour plusieurs clients (par exemple, les assurances, les cabinets d'avocats, la santé).

En combinant EDLP et une plateforme de sécurité de messagerie, les responsables SRM peuvent utiliser le SEG pour gérer d'autres menaces telles que le phishing, les logiciels malveillants et la compromission de comptes, tout en exploitant l'outil EDLP pour prévenir la perte de données. De plus, l'équipe qui gère la solution EDLP peut gérer la DLP des e-mails dans le cadre de ses opérations quotidiennes. La plupart des fournisseurs EDLP proposent une solution DLP qui consiste à rediriger le trafic e-mail via leur système DLP (voir **le Magic Quadrant des plateformes de sécurité de messagerie**) .

Protection des terminaux

Les solutions DLP pour terminaux sont généralement déployées via un agent permettant aux entreprises de surveiller les mouvements de données sensibles hors du terminal. Ces agents sont fournis sous forme d'IDLP via des EPP ou d'EDLP. L'exfiltration de données sur un terminal se fait généralement par plusieurs méthodes, que la DLP peut détecter et empêcher. Les cas d'utilisation courants de la DLP pour terminaux incluent :

- Identifier et prévenir l'exfiltration de données via l'impression, le Bluetooth et les supports amovibles, tels que les clés USB
- Découverte et contrôle des données sensibles sur les systèmes de stockage locaux
- Identifier et contrôler les données sensibles partagées via Internet
- Empêcher le transfert d'informations sensibles vers des applications ou via une activité de copier-coller

Les données peuvent également résider ou être transférées vers un stockage local (applications SaaS ou lecteurs réseau partagés). Certaines solutions DLP pour terminaux disposent donc de fonctionnalités de découverte pour analyser les données sensibles au

repos et les déplacer vers un emplacement autorisé. Comme les solutions DLP pour terminaux sont souvent intégrées au noyau , certains fournisseurs de DLP peuvent également surveiller le trafic des navigateurs web et des e-mails. L'inspection du trafic des navigateurs web permet aux solutions EPP avec contrôles DLP pour navigateurs de prévenir la perte de données par des applications GenAI non autorisées. Malgré leur grande polyvalence, l'exploitation complète de toutes les capacités de détection sur les canaux d'exfiltration peut impacter négativement les performances du système.

Les solutions DLP pour terminaux nécessitant un agent déployé, elles se limitent à la gestion des pertes de données sur les terminaux gérés. Par conséquent, si une organisation applique une politique BYOD (apportez vos propres appareils), une solution DLP traditionnelle pour terminaux ne sera d'aucune utilité, sauf si les utilisateurs autorisent les équipes informatiques à installer des agents sur ces terminaux. Pour les organisations appliquant une politique BYOD, la détection des mouvements de données, qu'ils soient gérés ou non, à partir d'applications cloud autorisées, est optimisée par l'utilisation d'un courtier de sécurité d'accès au cloud (CASB) comme couche de proxy inverse entre les applications d'entreprise et l'appareil non géré. Les CASB en proxy inverse peuvent détecter et empêcher la fuite de données sensibles depuis le cloud autorisé grâce à des contrôles de blocage ou un contrôle d'accès basé sur les attributs.

De plus, de nombreux fournisseurs EPP incluent e DLP dans leur offre I DLP et prennent en charge des systèmes d'exploitation tels que Microsoft Windows et macOS, avec une prise en charge limitée de Linux en raison de problèmes de compatibilité avec les nombreuses versions de noyau et de distribution Linux utilisées. Pour plus d'informations, consultez **le Magic Quadrant des plateformes de protection des terminaux** .

Service de sécurité Edge

Les solutions SSE sécurisent l'accès au web, aux services cloud et aux applications privées. Elles incluent généralement le contrôle d'accès, la protection contre les menaces, la prévention des pertes de données (DLP), la surveillance de la sécurité et le contrôle des utilisations acceptables, le tout assuré par des intégrations réseau et API. Les fonctionnalités SSE sont principalement fournies sous forme de service cloud et peuvent inclure des composants sur site ou basés sur des agents. Les cas d'utilisation courants de l'IDLP dans SSE incluent :

- Surveillance et contrôle des données sensibles consultées ou déplacées depuis des applications cloud vers des appareils gérés ou non gérés

- Surveillance et contrôle des données sensibles au repos dans les applications cloud autorisées
- Détecter et prévenir la perte de données dans les flux de données à travers le réseau

En raison de la convergence des services CASB et de passerelle Web sécurisée (SWG) vers SSE, la capacité de nombreux fournisseurs SSE à sécuriser les données sensibles a initialement concentré leurs produits DLP sur les charges de travail SaaS et les flux de données réseau. Cependant, le reconditionnement de services basés sur des agents sur site existants (ou le développement de nouveaux services) a permis à certains fournisseurs SSE d'étendre les contrôles de sécurité des données aux données sensibles dans l'ensemble de l'écosystème organisationnel .

Les offres SSE explorent également de manière proactive les améliorations possibles en matière de DLP, certaines sous la forme de méthodes alternatives de dissuasion DLP (par exemple, des politiques et des contrôles d'accès précis, l'association d'indicateurs de risque avec les activités de perte de données), et d'autres du côté de la détection (par exemple, l' acquisition ou la création de fournisseurs de gestion de la posture de sécurité des données [DSPM] pour la classification des données ou la création d'une classification interne des données et d'une détection contextuelle des données basée sur l'IA), ainsi que l'extension de leur prise en charge de plusieurs canaux d'exfiltration. Certains fournisseurs SSE proposent même la DLP sur tous les canaux d'exfiltration (c'est-à-dire E DLP). Pour plus d'informations, consultez **le Magic Quadrant pour Security Service Edge** .

Gestion des risques internes

Gartner définit la gestion des risques internes comme une méthodologie incluant des outils et des capacités permettant de mesurer, détecter et contenir les comportements indésirables des comptes de confiance au sein de l'organisation. Elle implique des solutions qui surveillent le comportement des employés (comme l'UEBA), des partenaires de service et des principaux fournisseurs opérant au sein de l'organisation. Ces outils évaluent ensuite si le comportement est conforme aux attentes du poste et à la tolérance au risque de l'organisation.

Les solutions DLP traditionnelles se concentrent davantage sur le contenu et sont centrées sur les données. Elles ne permettent donc pas de distinguer facilement les divulgations de données malveillantes des divulgations accidentelles. Cependant, en enrichissant les événements DLP avec le contexte du comportement de l'utilisateur, il sera beaucoup plus facile de distinguer les actes malveillants des actes négligents et d'appliquer des contrôles.

À mesure que les fournisseurs de solutions DLP élargissent leurs cas d'utilisation et améliorent la précision de détection et la convivialité de leurs solutions, nous constatons qu'ils s'efforcent d'intégrer des indicateurs de risque et de comportement utilisateur à leur logique de détection DLP. Cette approche s'appuie sur des capacités d'inspection de contenu, l'analyse comportementale et l'apprentissage automatique, et contribue également à réduire le nombre de faux positifs (voir le **Guide du marché pour la gestion des risques internes**) .

Gouvernance de l'accès aux données et gestion de la posture de sécurité des données

La gouvernance de l'accès aux données constitue la principale protection des données non structurées au repos, quel que soit leur emplacement (sur site, cloud ou SaaS). Les produits de gouvernance de l'accès aux données permettent aux organisations d'analyser et de corriger les droits d'accès excessifs aux données non structurées. Parmi les cas d'utilisation courants de l'IDLP dans la gouvernance de l'accès aux données, on peut citer :

- Identification et contrôle des données sensibles au repos dans les magasins de données non structurées
- Surveiller les données sensibles pour garantir que les droits d'accès appropriés sont en place et appliquer des contrôles d'accès aux données trop permissives

Grâce à la gouvernance de l'accès aux données, les organisations peuvent garantir le strict respect de leurs politiques d'accès et d'utilisation des données, empêchant ainsi tout accès non autorisé ou partage excessif d'informations sensibles. Les outils de gouvernance de l'accès aux données recoupent les fonctionnalités d'analyse des utilisateurs, de découverte de données et de prévention des pertes de données (DLP). Si la gouvernance de l'accès aux données est un contrôle généralement appliqué de manière rythmée, les fournisseurs commencent à privilégier les fonctionnalités en temps réel, parfaitement compatibles avec la DLP de nouvelle génération.

Bien que la gouvernance de l'accès aux données puisse se concentrer principalement sur les données au repos, les solutions de gouvernance de l'accès aux données peuvent devenir essentielles pour les organisations afin de compléter leur portefeuille de sécurité des données. De plus, de nombreux clients de Gartner ont indiqué que très peu de données organisationnelles au repos étaient gérées par des contrôles d'accès appropriés. Pour plus

d'informations, consultez **la Feuille de route stratégique 2024 pour une sécurité de classe mondiale des données non structurées** .

DSPM fournit généralement les éléments fondamentaux de la découverte et de la classification des données, nécessaires à une gouvernance efficace des données au repos. DSPM découvre les données connues et inconnues (ou fantômes) et crée une analyse des flux et des cartes de données pour permettre une identification plus cohérente de l'emplacement des données et une classification des données sensibles et réglementées. Cela fonctionne pour les données structurées et non structurées sur les plateformes de services cloud. De plus, les solutions DSPM identifient les risques de sécurité et de confidentialité liés aux données circulant dans les pipelines et entre les IaaS, PaaS et SaaS, et peuvent aider à évaluer la sécurité des données d'une organisation auprès des différents fournisseurs de services cloud. Les solutions de gestion de la sécurité des données offrent une visibilité au niveau du locataire, évitant ainsi aux organisations de connecter manuellement chaque nouvelle ressource déployée au sein de ce locataire pour l'auditer.

Certains fournisseurs reconnaissent le manque de contrôles préventifs offerts par DSPM et ont commencé à intégrer des fonctionnalités et des contrôles DLP pour compléter les capacités de cartographie et de découverte des données. Leurs méthodes de contrôle sont généralement non binaires, comme les contrôles d'accès et le masquage des données. Certains fournisseurs ont acquis des startups DLP afin de fournir les contrôles nécessaires à la prévention des pertes de données (voir **Innovation Insight : Data Security Posture Management**) .

Fournisseurs représentatifs

La liste des fournisseurs mentionnés dans ce guide du marché n'est pas exhaustive. Cette section vise à mieux comprendre le marché et ses offres.

Sélection du fournisseur

Le tableau 1 répertorie les fournisseurs DLP représentatifs qui proposent des solutions prenant en charge un ou plusieurs types de DLP (y compris les points de terminaison, la messagerie électronique, le réseau et le cloud), prenant en charge plusieurs applications et pouvant être appliquées à plusieurs canaux de sortie.

Tableau 1 : Fournisseurs représentatifs en matière de prévention des pertes de données

Fournisseur	Nom du produit	Catégorie DLP	Quartier général	Classification des données natives	UEBA d'init
Grand ID	BigID Suivant	Cloud natif	New York, État de New York	Oui	Oui
Broadcom	Symantec DLP	Entreprise	Palo Alto, Californie	Oui	Oui
CrowdStrike	Protection des données Falcon	Intégré	Austin, Texas	Non	Oui
Cyberhaven	Détection et réponse aux données	Cloud natif	Palo Alto, Californie	Oui	Oui

Source : Gartner (avril 2025)

Profils des fournisseurs

Grand ID

Fondée en 2016, BigID se concentre sur la découverte, la classification, la gouvernance et les contrôles de confidentialité des données plutôt que sur les contrôles préventifs traditionnels des données en mouvement. BigID a développé une plateforme qui s'intègre aux sources de données cloud et sur site, notamment les bases de données, les partages de fichiers et les applications d'entreprise et SaaS.

- **Email DLP :** surveille et contrôle les données sensibles au repos dans les serveurs d'échange de courrier électronique
- **Cloud DLP :** identifie et contrôle les données dans les magasins de données SaaS et cloud
- **Découverte et classification des données :** identifie et catégorise les données sensibles pour appliquer les politiques de sécurité des données

BigID's approach to DLP prioritizes security controls for data at rest, including data governance. The platform integrates with a wide range of data sources, including databases, cloud environments and enterprise applications, to provide insights into organizational data sprawl. BigID does not offer endpoint DLP or address traditional data in motion use cases for DLP (it supports Apache Kafka and Amazon Kinesis). They can, however, identify and classify data across the data sources they integrate with, offering options for minimizing the risk posed by this data. These options include alerting security administrators to automatically applying data access revocation or data minimization.

Broadcom

Broadcom's DLP features were introduced in 2019, following the acquisition of Symantec. Broadcom offers DLP coverage for each exfiltration channel, and offers UEBA through the utility of Symantec Information Centric Analytics (ICA) to manage insider risks.

- **Email DLP:** Monitors data exfiltration attempts via email, and provides controls to keep sensitive information secure
- **Endpoint DLP:** Provides DLP for user devices (supporting Windows, macOS and Linux endpoints), preventing unauthorized data access and transfer
- **Network and browser DLP:** Monitors and controls data in motion across the network and via web browsers to prevent data exfiltration attempts
- **Cloud DLP:** Extends DLP to cloud environments, ensuring secure usage of data and compliance
- **Data discovery and classification:** Discovers and classifies sensitive data across user endpoints and on-premises and cloud data stores

Broadcom DLP provides coverage across multiple data channels, using a single console for policy and incident management. It utilizes a variety of data detection methods to identify and secure sensitive information. Additionally, integrating DLP with Symantec ICA allows SRM leaders to better mitigate insider threats by analyzing user behavior and implementing appropriate access controls. Native data tagging from Broadcom has been deprecated, but Broadcom DLP supports other common data tagging technologies, such as sensitivity labels from Microsoft Purview.

CrowdStrike

CrowdStrike, established in 2011, traditionally focused primarily on endpoint security, but has recently expanded its offerings to include DLP functionalities, leveraging the Falcon agent and management platform.

- **Endpoint DLP:** Supports limited use cases for data security on Windows endpoints, including data transfers to removable media and clipboard functions
- **Browser DLP:** Provides DLP for browser-based activities and some SaaS applications

CrowdStrike has developed DLP functionalities based on a wide array of default content patterns (called “data classifications”), web sources and more. It supports both the endpoint, with limited use cases, and browser DLP channels, with further support for some SaaS applications accessible via the browser. CrowdStrike’s DLP solution combines behavioral analytics context (such as users’ unusual data access patterns or unauthorized data transfers) with content inspection (such as sensitive data content or an inherited classification label) to prevent data loss.

Although CrowdStrike uses the terminology “data classification,” it does not have the ability to append or modify classification labels within a document like some other DLP providers do. The Falcon Data Protection management console provides security teams with visibility of the organization’s security posture (beyond data security), enabling it to correlate data loss and anomalous behavior events with other security incidents when responding to incidents.

Cyberhaven

Cyberhaven, established in 2016, positions itself in the data security market with its Data Detection and Response product, which offers visibility into data throughout its life cycle. Cyberhaven combines data detection with user behavior analytics to provide security teams with visibility into and control over their organization's data.

- **Email DLP:** Monitors and controls sensitive data sent via email from corporate devices
- **Endpoint DLP:** Monitors and secures data on user devices, with agent support for Windows, macOS and Linux devices
- **Browser DLP:** Secures data shared to supported applications accessed via the browser
- **Cloud DLP:** Connects via APIs to sanctioned SaaS applications to gain visibility and control over data access and movement in these applications
- **Data discovery and classification:** Discovers and classifies sensitive data to inform DLP policies

Cyberhaven Data Detection and Response combines telemetry from the endpoint agent with context from API connectors to sanctioned SaaS applications to build a data lineage. This data lineage provides visibility into user behavior with data and supports proactive insider threat detection and DLP, allowing organizations to identify and mitigate potential data risks before they escalate. Cyberhaven can detect both regulated and unregulated data types, such as IP and source code, the latter of which is often a detection challenge for DLP solutions that rely on traditional, noncontextual detection methods.

Digital Guardian

Digital Guardian was founded in 2003 and acquired by Fortra in 2021. Digital Guardian initially focused on endpoint DLP, but has since expanded its offerings to include DLP coverage for network and browsers, email, and cloud.

- **Email DLP:** Monitors data exfiltration attempts via email and provides controls to keep sensitive information secure
- **Endpoint DLP:** Provides DLP for user devices (supports Windows, macOS and Linux endpoints), preventing unauthorized data access and transfer
- **Network and browser DLP:** Monitors and controls data in motion across the network and via web browsers to prevent data exfiltration attempts

- **Data discovery and classification:** Identifies and classifies sensitive data to supplement DLP strategies

Digital Guardian's DLP solution is deployed via an endpoint agent, or network appliance, and focuses on securing sensitive data across diverse environments, including on-premises, cloud and hybrid systems. The platform integrates with various data sources and systems, offering visibility into data movement and user activities. Digital Guardian employs a combination of data classification and contextual awareness to detect and prevent data loss. Its methodology includes monitoring data in motion and at rest, allowing for policy enforcement customized to specific needs.

DTEX

DTEX, founded in 2000, combines user behavior intelligence and activity monitoring with DLP controls to reduce data loss and minimize insider risk.

- **Endpoint DLP:** Monitors user behavior and file activity and controls sensitive data movement on user endpoints (supporting Windows, macOS and Linux endpoints)
- **Cloud DLP:** Monitors and controls sensitive data movement to storage applications
- **Data discovery and classification:** Identifies and classifies data based on inferred sensitivity

DTEX provides a single agent that monitors and prevents data loss, minimizes insider risk, and identifies account compromise. DTEX's platform is deployed as an endpoint agent on Windows, macOS and Linux devices, and gathers telemetry data to inform usage of controls. DTEX does not inspect the data, instead inferring sensitivity about it from various metadata attributes, including inherited classification labels and insider risk telemetry. Because their detection is purely focused on user behavior, organizations with a content-centric focus may find DTEX lacking — although, because of their context-centric focus, overall DLP policy accuracy may increase. Further, using predictive analytics and identification of anomalous user behaviors, DTEX attempts to determine user intent and correlates this with data sensitivity to try to prevent data loss.

Forcepoint

Forcepoint was formed in 2016 from the merger of Websense, Stonesoft, Sidewinder and Raytheon's "Cyber Products" business. Forcepoint has expanded its SSE capabilities through the acquisition of Bitglass in 2021 and, in 2025, it announced intent to acquire Getvisibility to expand its data discovery and classification capabilities. Forcepoint DLP unifies policy management and enforcement across cloud, web, email, endpoint and network.

- **Email DLP:** Prevents data loss through email, integrating with popular email providers and offering prebuilt security policies
- **Endpoint DLP:** Secures data on Windows and macOS endpoints, on and off the corporate network
- **Network and browser DLP:** Prevents data loss in motion through web channels and FTP, identifying and preventing intentional data exfiltration and accidental data loss
- **Cloud DLP:** Extends DLP to cloud environments, including cloud applications, web traffic and private cloud applications.
- **Data discovery and classification:** Identifies sensitive data across file servers, SharePoint, Exchange and databases

Forcepoint's DLP incorporates a risk-adaptive protection approach focusing on understanding user behavior and prioritizing high-risk users via real-time risk calculations. Its policy enforcement is based on user intent and context to reduce false positives. Forcepoint integrates with various security tools and threat intelligence platforms to assist security teams with incident response.

Fortinet

Fortinet, established in 2000, integrated DLP capabilities into its FortiGate firewalls and other security products. In 2024, Fortinet acquired Next DLP to supplement its offerings in stand-alone and IDLP. FortiDLP provides DLP coverage and visibility for network, endpoint and cloud, combining content inspection with UEBA.

- **Email DLP:** Monitors data exfiltration attempts via email, providing controls to keep sensitive information secure
- **Endpoint DLP:** Provides DLP capabilities preventing unauthorized data access and transfer for Windows, macOS and Linux endpoints

- **Network and browser DLP:** Monitors and controls data in motion across the network and browsers to prevent data exfiltration attempts
- **Cloud DLP:** Extends DLP to cloud environments, ensuring secure usage of data
- **Data discovery and classification:** Identifies and classifies sensitive data to supplement DLP strategies through FortiData

FortiDLP is a SaaS-deployed, agent-based platform that provides data coverage and tracking across multiple channels and insider risk management capability into its unified endpoint. When deployed, FortiDLP builds a baseline user risk profile and understands how user behavior changes over time. FortiDLP includes Secure Data Flow that identifies sensitive data at the point of origin and builds a data lineage of manipulations on the data.

GTB Technologies

GTB Technologies, founded in 2004, has been a provider of DLP for over 20 years. GTB Technologies has focused on securing sensitive data across multiple exfiltration channels.

- **Email DLP:** Inspects email traffic and prevents sensitive data loss
- **Endpoint DLP:** Monitors user activity and prevents data loss on user endpoints, with support for Windows, macOS and Linux endpoints
- **Network and browser DLP:** Monitors and controls data in motion across the network and via web browsers to prevent data exfiltration attempts
- **Cloud DLP:** Monitors and controls data in common cloud applications
- **Data discovery and classification:** Utilizes data classification to enhance data detection accuracy

GTB Technologies provides DLP for multiple data exfiltration channels, including endpoints, network, browsers and cloud applications. The platform integrates with common data sources, providing visibility and control over data movement to minimize the risk of data exfiltration. The solution employs a combination of data classification and content inspection techniques (such as OCR and fingerprinting) to monitor user activity and prevent potential data loss.

Harmonic

Harmonic is a relatively new entrant in the DLP market, founded in 2023. Its focus is on GenAI applications, first determining the risk posed by such applications and then preventing data loss to risky applications.

- **Browser DLP:** Deployed via webhooks or browser extensions to detect sensitive data usage and prevent sensitive data loss in browsers used to access GenAI applications
- **Cloud DLP:** Utilizes APIs to connect to and secure sensitive data used by GenAI SaaS applications

Harmonic's solution approaches DLP by adaptive security and threat intelligence, particularly for GenAI applications. Although offering deployment through browser extensions and endpoint agents (for Windows endpoints), Harmonic focuses on DLP for GenAI applications and does not address typical use cases for endpoint DLP, such as controls for data loss to removable media and printing. Instead of relying on regular expressions and pattern matching for sensitive data detection, Harmonic's DLP policies leverage proprietary data security small language models that detect and respond to potential data loss incidents. These small language models also allow for natural language DLP policy development specific to organizational needs, which can increase the accuracy of detection and response to data loss incidents.

Microsoft

Microsoft entered the DLP market in 2012. Microsoft Purview is its suite of data security, governance and compliance solutions. Purview integrates with Microsoft 365 and other data services (both Microsoft and non-Microsoft). Microsoft continues to expand its Purview product suite, frequently adding new features and building new integrations.

- **Email DLP:** Monitors and controls sensitive data loss through email traffic
- **Endpoint DLP:** Monitors and controls data exfiltration from macOS and Windows endpoints
- **Network and browser DLP:** Prevents data loss for web browsers and for network traffic from managed devices to cloud services and applications

- **Cloud DLP:** Monitors and controls sensitive data across cloud environments and SaaS applications
- **Data discovery and classification:** Discovers and classifies data using Microsoft Purview Information Protection

Purview allows security teams to classify data and build and manage DLP policies across Microsoft 365 apps and services, including Exchange, SharePoint, OneDrive and Teams, as well as non-Microsoft data sources. While Microsoft Purview's DLP features integrate with non-Microsoft cloud services and on-premises file shares, organizations using a diverse mix of platforms should carefully evaluate the extent of integrations available for their specific non-Microsoft environment and systems.

Mimecast

Mimecast, established in 2003, historically has provided solely email DLP capabilities but, through its acquisitions of Aware and Code42 in 2024, has expanded its DLP coverage of data exfiltration vectors beyond email to endpoint, browser and cloud applications.

- **Email DLP:** Monitors and controls email communications for sensitive data, minimizing unauthorized sharing
- **Endpoint DLP:** Monitors and controls endpoint activities to control unauthorized sharing of sensitive information, with support for Windows, macOS and Linux endpoints
- **Browser DLP:** Monitors and controls sensitive data in web browser uploads
- **Cloud DLP:** Extends data security to cloud-based email and collaboration platforms
- **Data discovery and classification:** Identifies and categorizes sensitive data to enforce data security policies

Mimecast's email DLP solution prevents unauthorized sharing of sensitive information by applying policies that detect and block potential data breaches. Through IP acquired from Code42 and Aware, Mimecast extends DLP beyond email by providing endpoint and cloud DLP capabilities. It correlates endpoint DLP functionalities with UEBA to minimize insider risks and prevent data loss based on user risks.

Netskope

Netskope was founded in 2012 and has a cloud-based DLP product that can provide security for sensitive data in cloud, on-premises and hybrid environments. Netskope's DLP is part of its SSE offering and it supports an agent-based approach for endpoint DLP.

- **Email DLP:** Detects and prevents sensitive data egress through email
- **Endpoint DLP:** Monitors and controls data loss using the Netskope client deployed on macOS and Windows devices
- **Network and browser DLP:** Detects and prevents loss of sensitive data through the Netskope SWG
- **Cloud DLP:** Provides DLP for sanctioned and unsanctioned SaaS applications and cloud data stores
- **Data discovery and classification:** Discovers sensitive data at rest in the cloud and appends data classifications based on detection of sensitive data

Netskope can correlate content detection with user behavior analytics to address insider risk use cases and add context to DLP alerts, which can increase the accuracy of existing DLP policies. Further, Netskope integrates with other systems, such as Microsoft Purview, to append data classification labels and increase the accuracy of DLP policies.

Nightfall

Nightfall emerged in the DLP market in 2018, offering a cloud-native DLP solution deployed via APIs to secure sensitive data across cloud applications. More recently, its coverage has expanded beyond SaaS applications to also offer some email and endpoint DLP capabilities.

- **Email DLP:** Monitors and controls email traffic for Gmail and Exchange
- **Endpoint DLP:** Monitors and prevents loss of sensitive data on user endpoints (endpoint agent support for macOS and Windows)
- **Browser DLP:** Monitors and controls sensitive data movement to SaaS applications
- **Cloud DLP:** Monitors and controls sensitive data in cloud applications
- **Data discovery and classification:** Discovers and classifies sensitive data at rest in SaaS applications

Nightfall offers a cloud-native DLP solution with limited default coverage, but has made its APIs configurable for SRM leaders to increase visibility by building integrations for unsupported applications and use cases. Nightfall's default email DLP coverage supports Gmail and Exchange Online, with the option to encrypt emails containing sensitive data. Its browser extension is built for Chromium-based browsers, Mozilla Firefox and Apple Safari, and can extend DLP coverage to GenAI applications. Nightfall's endpoint agent supports macOS and Windows and can be used to detect and prevent data loss via browser uploads and cloud storage sync applications.

Palo Alto Networks

Palo Alto Networks, founded in 2005, offers its integrated, cloud-delivered DLP product (called Enterprise Data Loss Prevention) to discover, monitor and secure sensitive data across email, endpoints, networks, and cloud environments.

- **Email DLP:** Identifies and secures data sent via email, regardless of the device or email client
- **Endpoint DLP:** Identifies and prevents data loss via the Prisma Access agent deployed on macOS and Window endpoints
- **Network and Browser DLP:** Inspects web traffic and monitors data in motion across on-premises, hybrid, and multicloud environments
- **Cloud DLP:** Monitors and secures data in motion for remote users, natively integrated into its secure access service edge (SASE); also extends to SaaS applications and public clouds
- **Data discovery and classification:** Utilizes multiple detection techniques to identify and classify data

Palo Alto Networks' Enterprise Data Loss Prevention is natively integrated with its broader security ecosystem, including its next-generation firewalls (NGFWs), Prisma Access for secure remote access and security for SaaS through Prisma SaaS. The solution offers a unified policy framework for consistent data security across hybrid environments, providing enterprises with visibility and control at scale. Palo Alto Networks leverages large language models to enhance contextual analysis, enabling more precise detection of potential data loss.

Proofpoint

Proofpoint, founded in 2002, is a vendor in the email security space. It launched its DLP solution in 2020 and has integrated DLP into many of its other products. Proofpoint acquired Tessian in late 2023, enhancing its email DLP capabilities.

- **Email DLP:** Identifies and secures sensitive data, automates compliance, and prevents data loss via email transfer
- **Endpoint DLP:** Detects and prevents data loss via agents deployed on macOS and Windows endpoints
- **Network and Browser DLP:** Secures data in motion shared through the network or via the browser
- **Cloud DLP:** Extends data security to cloud use cases such as securing cloud data and ensuring acceptable use of GenAI tools in cloud environments
- **Data discovery and classification:** Detects, identifies and classifies sensitive data in cloud data stores and applications

Proofpoint's human-centric approach to data security integrates user behavior analysis with content detection to prevent data loss. The platform offers centralized policy management for email, endpoint, browser and cloud DLP, combined with the Proofpoint Insider Threat Management (ITM) console for incident management and response. The centralized incident management console allows analysts to review incidents, respond and enforce policies across all channels. To classify data, Proofpoint extends Microsoft sensitivity labels for data in the cloud and on the endpoint.

SkyGuard

SkyGuard, established in 2015, offers an EDLP solution designed to safeguard data across diverse environments, including endpoints, network, on-premises and cloud services.

- **Email DLP:** Detects and prevents sensitive data exfiltration through email services
- **Endpoint DLP:** Prevents data loss on endpoints, with support for Windows, macOS and Linux

- **Network DLP:** Inspects network traffic, including email and instant messaging, for visibility of data transfer and mandatory data security policy enforcement
- **Cloud DLP:** Extends on-premises DLP solutions to the cloud, addressing the challenges of securing sensitive data in cloud applications, remote offices and mobile endpoints
- **Data discovery and classification:** Scans laptops, servers, file shares, cloud storage, SaaS applications and databases to identify and classify sensitive information residing across these locations

SkyGuard DLP combines data classification, real-time monitoring and contextual analysis to detect and prevent unauthorized data access and exfiltration. It supports both API-based and agent-based deployments and hybrid cloud deployment, enabling centralized management across fragmented DLP implementations in decentralized or multilocation enterprises by unifying security policies, visualizing data risk events and threat reports, and supporting large volumes of events/logs. SkyGuard offers policy templates for geographic- and industry-specific regulations, but its limited global presence and integration with certain international platforms could pose challenges for multinational organizations.

Trellix

Trellix was formed in the 2021 merger of McAfee Enterprise and FireEye, and offers DLP for multiple use cases. Trellix partners closely with Skyhigh Security and although the two are under common ownership (Symphony Technology Group) and leadership, they are technically separate entities.

- **Email DLP:** Monitors and controls sensitive data shared in email communications
- **Endpoint DLP:** Monitors and secures sensitive data via an agent installed on Windows and macOS endpoints
- **Network and Browser DLP:** Secures data in motion shared through the network or via the browser
- **Cloud DLP:** Monitors and controls sensitive data movement to cloud applications (primarily through a partnership with Skyhigh Security)
- **Data discovery and classification:** Discovers and classifies data on user endpoints, servers and in some cloud applications

Trellix Data Loss Prevention offers an EDLP solution for securing sensitive data across multiple exfiltration channels, including endpoints, networks, email and cloud environments. While Trellix provides DLP functionality across on-premises workloads and user endpoints, visibility and control over sensitive data in the cloud are enhanced through an integration with Skyhigh Security. This partnership allows security teams to apply policies and view cloud DLP events through the Trellix ePolicy Orchestrator (ePO) management console.

Varonis

Varonis, founded in 2005, offers DLP functionalities across a variety of data sources, including SaaS, on-premises and cloud environments. Varonis's DLP capabilities are isolated to data at rest, and its control sets include data access governance and data deidentification.

- **Email DLP:** Monitors and controls sensitive data at rest in email exchange servers
- **Cloud DLP:** Identifies and controls data at rest in SaaS and cloud data stores
- **Data discovery and classification:** Identifies and categorizes sensitive data to enforce data security policies

Varonis provides DLP functionalities primarily for data at rest (not data in motion) by focusing on securing data at rest across various repositories, including SaaS, on-premises and cloud environments. Varonis begins with data classification, identifying sensitive data and evaluating data sprawl to help SRM leaders understand their data at rest. Varonis relies on several methods for securing data at rest, including access controls (offered as policy, attribute and role-based) and data masking. Varonis's coverage of data at rest allows it to address the needs of organizations seeking to manage sensitive data across diverse storage environments.

Zscaler

Zscaler was founded in 2007 and provides IDLP throughout its platform. Its DLP spans across most common data exfiltration channels, email, endpoint, network, browser and cloud, specifically cloud services and SaaS applications.

- **Email DLP:** Detects and prevents sensitive data exfiltration through cloud email services

- **Endpoint DLP:** Monitors and controls data loss using the Zscaler Client Connector deployed on macOS and Windows devices
- **Network and browser DLP:** Detects and prevents loss of sensitive data across the network and via web browsers
- **Cloud DLP:** Provides DLP for sanctioned and unsanctioned applications and cloud data stores
- **Data discovery and classification:** Discovers sensitive data in the cloud and appends data labels based on detection of sensitive data (in specific applications)

Zscaler Data Protection is built to provide DLP across an array of data sources, systems and data exfiltration channels, leveraging its cloud-native architecture to integrate with cloud services, on-premises systems and SaaS applications. Zscaler's DLP relies on content inspection, contextual analysis and machine learning to identify sensitive data and prevent data exfiltration across the channels it covers.

Market Recommendations

When preparing for a DLP project, SRM leaders should:

- Consider DLP technology as a deliverable within a DLP program. SRM leaders with effective data security programs start with data risk assessments and data security governance to define the business use cases in scope for the DLP project, and align them with the requirements for DLP technology procurement.
- Engage business stakeholders to identify business needs and data risks to determine the riskiest data exfiltration vectors. Evaluate existing IDLP options to obtain better visibility of data usage and movement across the organizational ecosystem.
- Classify and label data. Labeling data brings consistency to what is considered sensitive information in an environment, which makes it easier to define DLP policies. Accurate data classification adds a layer to DLP detection, which minimizes false positives that introduce friction between security and business teams. Data labeling also helps minimize the false negatives that prevent DLP controls from being effective.
- Use EDLP if you have limited resources or if it is determined that users are transacting sensitive information through multiple channels. Leveraging multiple IDLP providers may

lead to issues such as administrative overhead (from managing multiple IDLP consoles) and policy inconsistency (IDLP vendor policy integration may be limited) across exfiltration channels. Although potentially more expensive, choosing an EDLP vendor may support the business and resourcing needs of the organization, while potentially reducing the total cost of ownership (TCO) of the DLP program.

- Invest in a DLP solution that can understand the full context surrounding the data, identify baseline user risk, and compare subsequent actions to the baseline activity by gathering contextual clues about the who, what, when and where of the data. This should be a priority for organizations with heightened concern about insider risk.

- Use cloud-native DLP solutions for public cloud data security in organizations with a hybrid or cloud-first strategy. Many of these vendors can also provide data security for multiple platforms and often integrate with both unstructured and structured data repositories.

- Use additional data security controls to fill any gaps that are not addressed by reactive and preventative controls. This includes securing the data at the source (in a database or file repository), rather than applying controls to secure the data at only the corporate boundary.

Acronym Key and Glossary Terms

BYOD	bring your own device
CASB	cloud access security broker
DLP	data loss prevention
DSPM	data security posture management
EDLP	enterprise DLP
EPP	endpoint protection platform

ICES	integrated cloud email security
IDLP	integrated DLP
PII	personally identifiable information
SEG	secure email gateway
SIEM	security information and event management
SSE	security service edge
SWG	secure web gateway
UAM	user activity monitoring
UEBA	user and entity behavior analytics

⊕ Evidence

Note 1: Consolidated Incident Response

Incident response with multiple DLP platforms is a difficult process, often requiring manual correlation across platforms. Some security teams choose to centralize incident response using a security information and event management (SIEM) or security orchestration, automation and response (SOAR) tools to aggregate logs from disparate platforms into a single platform.

Note 2: Methods for Classifying Data

Data classification, in the context of this research, is accomplished through placing a marker within the file that indicates the organization's view of the classification. Some data classification products can add metadata to a database table, record or column, but this is outside the scope of this research.

La classification des documents peut être déterminée par diverses méthodes, notamment l'application manuelle, l'analyse du contenu ou l'analyse des métadonnées.[1] L'étiquette accompagne les données et peut être facilement lue par d'autres contrôles et systèmes, assurant ainsi la continuité de la gestion et de la sécurisation des données. Les marqueurs peuvent prendre la forme d'un en-tête ou d'un pied de page dans le format du document, d'un filigrane ou d'un texte intégré au document.

Remarque 3 : Politiques de classification des données

La classification des données peut accroître l'efficacité du programme DLP, même si elle peut perturber les processus opérationnels existants. En raison des perturbations potentielles liées à la classification des données, l'élaboration d'une analyse de rentabilisation pour la classification des données nécessite généralement des politiques de gouvernance solides, approuvées par les parties prenantes concernées (voir **Boîte à outils : Classification et traitement des données sensibles** et **Élaboration de politiques efficaces de classification des données et de documents de traitement des données**).