Microsoft Security

Trois étapes pour protéger vos données de bout en bout

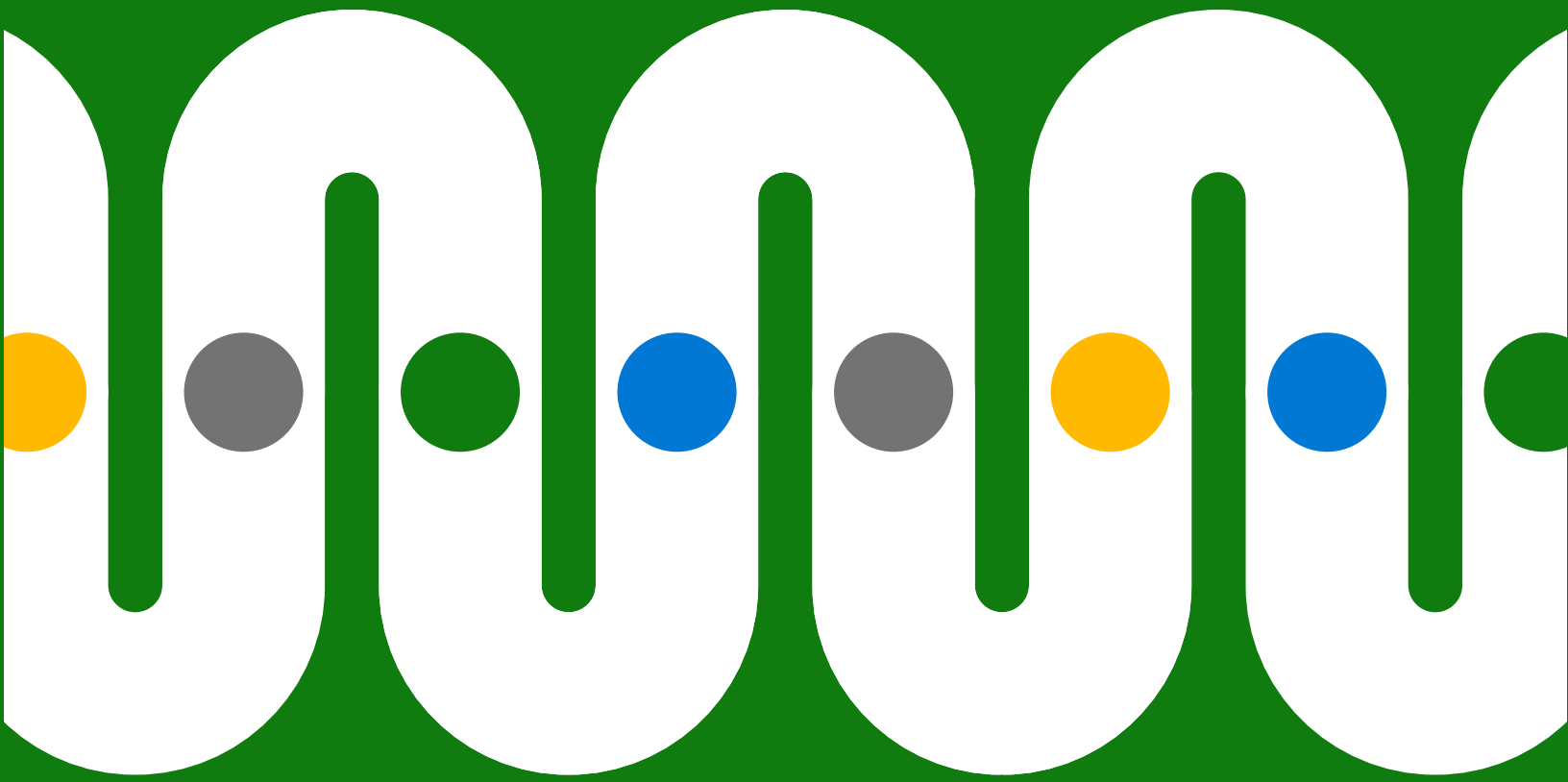


Table des matières

Présentation

Une enquête menée auprès de décideurs en matière de conformité a montré que 95 % d'entre eux étaient préoccupés par les problèmes de protection des données[2].

Les organisations ont constaté une augmentation massive de leur empreinte numérique depuis l'arrivée du travail hybride, qui a poussé les frontières de l'entreprise bien au-delà du bureau classique.

L'hybride a également entraîné une fragmentation et une exfiltration accrues des données, accompagnées par la croissance rapide d'une multitude d'applications, de dispositifs et d'emplacements. De nombreux travailleurs ont également changé de poste à la recherche d'un plus grand épanouissement ou d'une plus grande flexibilité, ce qui n'a fait qu'ajouter à la complexité de la situation, créant de nouveaux angles morts dans des parcs de données toujours plus importants[1].

Tous ces facteurs amènent les DSI et les RSSI à repenser leur approche de la protection des informations. Dans une enquête de suivi menée auprès de plus de 500 décideurs américains en matière de conformité, presque tous (95 %) se sont dits préoccupés par les problèmes de protection des données[2].

[1] « Comment Microsoft peut aider à réduire les risques internes pendant le grand remaniement, Alym Rayani », Sécurité Microsoft. 28 février 2022.

[2] « Enquête de septembre 2021 menée auprès de 512 décideurs américains en matière de conformité commandée par Microsoft à Vital Findings »

Les équipes informatiques et de sécurité recherchent de meilleurs moyens de gérer l'ensemble du cycle de vie des données dans des environnements multinuage, de nuage hybride et sur place. Cette approche de bout en bout comprend trois étapes clés :

Phase 1 : Identifier les données

Déterminez l'emplacement de vos données, leur type et la façon dont elles sont utilisées ou partagées

Étape 2 : Classer les données

Classez et étiquetez vos données afin de connaître les bonnes stratégies et les mesures à appliquer pour minimiser les risques

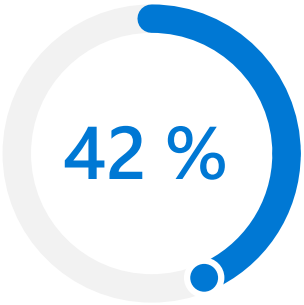
Étape 3 : Prévenir la perte de données

Trouvez un équilibre entre la réduction des risques et la flexibilité pour vos employés grâce à la détection et au contrôle intelligents

Le but de cette approche? Combler les lacunes et minimiser les risques sans sacrifier la productivité.

Étape 1

Identifier les données



42 % des entreprises ont déclaré qu'au moins la moitié de leurs données était « sombre »[3].

Ces données « cachées » peuvent prendre de nombreuses formes : pièces jointes, enregistrements d'appel avec des clients ou encore journaux de machine et séquences vidéo.

Si vous ne savez pas identifier vos données (déterminer où elles se trouvent, leur type et comment elles sont utilisées ou partagées), il est impossible d'appliquer les bonnes stratégies ou mesures de protection.

Les entreprises modernes génèrent en permanence de grandes quantités de données. Il ne s'agit pas seulement de documents, de courriels et de messages, mais aussi d'images de sécurité ou encore de données de géolocalisation. Tous ces éléments se multiplient et se mélangent dans les applications, les appareils et les espaces de stockage, sur place et dans le nuage.

Identifier toutes ces données peut s'avérer difficile. 42 % des entreprises déclarent qu'au moins la moitié de leurs données sont des données dites « sombres »[3], c'est-à-dire qu'il s'agit d'informations collectées mais inconnues ou non utilisées à des fins commerciales. Il arrive que des données deviennent sombres lorsque le travailleur qui les a créées change de projet ou de poste; souvent, il n'y a tout simplement aucun système en place pour identifier les données au moment de leur création ou de leur modification.

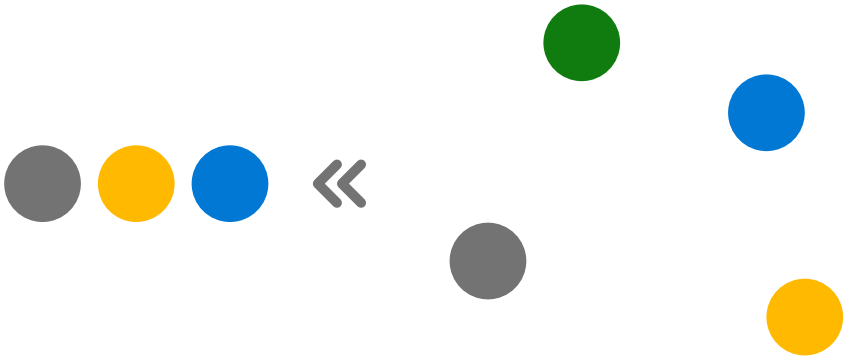
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Juillet 2022.

Vous souhaitez mettre en place un flux de travail de découverte de bout en bout sur une seule plateforme?

En savoir plus sur la découverte de données dans Microsoft Purview sur **Microsoft.com**.

Ces difficultés ne vont faire que s'amplifier. La quantité de nouvelles données créées, capturées, répliquées et consommées devrait être multipliée par deux, voire plus, d'ici 2026, les données d'entreprise augmentant plus de deux fois plus vite que les données des consommateurs[4].

L'intelligence artificielle (IA) et l'apprentissage automatique (AA) peuvent aider en reconnaissant les données sensibles (comme les adresses courriel, les données de santé, les numéros de carte de crédit ou les informations relatives à la propriété intellectuelle) et en les classant automatiquement. L'IA et l'AA peuvent également augmenter la précision de la classification et examiner les données de manière rétroactive. Ces processus d'identification peuvent couvrir l'ensemble de votre parc de données et ainsi préserver, collecter, analyser, examiner et exporter votre contenu où qu'il se trouve, vers tous les types de nuages.



[4] "Worlwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Mai 2022.

Étape 2

Classer les données

Les classifications et les stratégies doivent s'appliquer aux données lors de leur transit.

Par exemple, si un employé copie les numéros de carte de crédit d'un document Microsoft Word dans Excel, la classification et les stratégies doivent s'appliquer automatiquement aux deux documents.

Une classification appropriée des données vous aide à déterminer les bonnes stratégies et les mesures à appliquer pour garantir que les différents types de données ne sont pas accidentellement ou intentionnellement mal utilisés ou accessibles sans autorisation. Le chiffrement et le filigranage permettent de protéger encore davantage les données, qu'elles soient au repos, en transit ou en cours d'utilisation.

Mais la classification et les stratégies doivent aussi s'appliquer aux données lorsqu'elles circulent dans l'entreprise. Les stratégies d'étiquetage et de protection ne peuvent pas se limiter à des documents particuliers, elles doivent couvrir l'ensemble de votre parc numérique : référentiels sur place, référentiels basés sur le nuage, logiciels en tant que service (SaaS), applications natives du système d'exploitation, etc.

Les approches de classification classiques impliquent un travail manuel considérable, ce qui entraîne un risque d'erreur ou d'omission sur les données critiques. Des classificateurs intégrés et adaptatifs peuvent aider à automatiser ce processus, et une solution intégrée permet aux administrateurs de gérer les stratégies de manière centralisée sur tous les systèmes.

Vous souhaitez mieux gérer et protéger les données sensibles dans votre environnement?

En savoir plus sur la classification et la protection de données dans Microsoft Purview sur **Microsoft.com**.

Étape 3

Prévenir la perte de données

Les stratégies DLP permettent d'empêcher les actions non conformes.

Par exemple, si un employé tente de copier une feuille de calcul contenant des numéros de carte de crédit sur une clé USB ou de la mettre en ligne sur un espace de stockage infonuagique, des stratégies DLP permettent de définir l'activité comme étant non conforme et peuvent la bloquer.

Vous souhaitez une détection et un contrôle intelligents des informations sensibles?

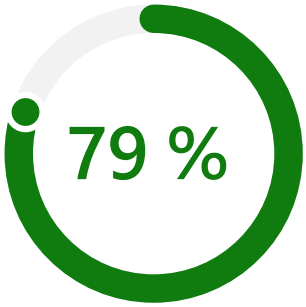
En savoir plus sur la protection contre la perte de données dans Microsoft Purview sur **Microsoft.com**.

Une fois que vous avez défini et classé vos données, des solutions de prévention des pertes de données (DLP) peuvent appliquer des stratégies de protection de bout en bout qui limitent les risques, comme ceux liés aux données sombres et à l'exfiltration de données, et empêchent vos employés actuels et anciens de partager, exposer ou transférer des données sensibles sans autorisation, intentionnellement ou par inadvertance.

Les solutions DLP intelligentes utilisent le contexte pour trouver un équilibre entre la flexibilité et le blocage des actions à haut risque. Par exemple, certaines personnes peuvent être autorisées à poursuivre une action après qu'on leur a précisé les risques potentiels et les stratégies applicables. Cela peut aider à protéger les données sensibles tout en formant les utilisateurs à mieux comprendre les risques.

Une solution DLP est essentielle pour protéger la propriété intellectuelle et d'autres données commerciales critiques, ainsi que pour contribuer à la conformité avec les réglementations comme le règlement général sur la protection des données (RGPD), la loi américaine sur la portabilité et la responsabilité en matière d'assurance maladie (HIPAA) et la loi californienne sur la confidentialité des données (CCPA).

Une approche globale de la DLP applique des stratégies cohérentes dans l'ensemble de l'organisation, ce qui protège les points les plus faibles dans le cycle de vie des données.



Une enquête auprès de décideurs en matière de conformité a montré que 79 % d'entre eux avaient acheté plusieurs produits de conformité et de protection des données.

La majorité d'entre eux en avait acheté trois ou plus[5].

N'ajoutez pas la protection des données comme une option. Intégrez-la à vos systèmes.

De nombreuses entreprises ont tenté d'adopter une approche de la protection des informations consistant à ajouter plusieurs solutions à leur système pour gérer des parties spécifiques du cycle de vie de leurs données. Mais cela oblige les équipes chargées de la sécurité, de la gouvernance des données, de la conformité et des questions juridiques à assembler un ensemble de solutions disparates qui est souvent inefficace et qui pèse sur les ressources.

Une approche « intégrée » peut combler ces lacunes en réunissant l'identification des données, leur classification et la DLP. Avec une solution intégrée, il est plus facile de gérer et d'appliquer les stratégies de manière centralisée. Cela réduit également le temps de formation des utilisateurs, qui sont informés sur les stratégies de manière familière et native au sein des applications.

[5]« Enquête de février 2022 auprès de 200 décideurs américains en matière de conformité (n=100 599-999 employés, n=100 Plus de 1 000 employés) commandée par Microsoft à MDC Research ».

Une solution intégrée : Microsoft Purview

Microsoft Purview vous aide à relever les défis liés à la décentralisation du lieu de travail et aux quantités massives de données modernes, en vous fournissant un ensemble complet de solutions qui vous aident à gouverner, protéger et gérer l'ensemble de votre parc de données.

Aller au-delà de la gouvernance.

En savoir plus sur la protection de vos données avec Microsoft Purview >

Vous êtes intéressé par un domaine spécifique de la protection des données? Obtenez des informations plus détaillées sur la façon dont Microsoft Purview peut vous aider avec les éléments suivants :

Découverte des données >

Classification et protection des données >

Protection contre la perte de données >

Microsoft Security