Prévenir la perte des données : le guide du dirigeant

Implémenter un programme de sécurisation des données en 5 phases

Forcepoint

Livre blanc

Sommaire

Le problème

Il y a eu beaucoup de confusion sur le marché concernant les contrôles de prévention de la perte de données (anglais Data Loss Prevention, DLP). De nombreux facteurs y contribuent, notamment un manque général de compréhension de la part de la communauté des prestataires sur le fonctionnement de la sécurité des données, ou sur ce qui transmet des risques à une entreprise. Des processus peu pratiques ont été mis en place, menant à la création de goulots d'étranglement qui ralentissent les activités. Cependant, le risque de perte et de vol de données est toujours présent. Les mauvaises expériences subies par une entreprise peuvent être directement liées au manque de clarté des objectifs du programme, à une planification insuffisante et à une mauvaise mise en œuvre.

En conséquence, les entreprises qui souhaitent protéger leurs données confidentielles, sécuriser l'accès et leur personnel de plus en plus hybride tout en restant conformes aux lois et réglementations sont souvent sceptiques, et ne savent plus vers qui se tourner. Certaines ont été mises en difficulté par des implémentations infructueuses.

Il est important de comprendre que ce n'est pas la technologie derrière les contrôles DLP qui est le facteur critique déterminant votre réussite – c'est la méthodologie et la stratégie d'exécution de votre fournisseur qui dicteront à la fois votre expérience et vos résultats.

Ce livre blanc fournit des conseils et des éclaircissements sur les points suivants :

- Il explique le défi : sécuriser la main-d'œuvre hybride et le contexte pour mettre la sécurité des données au cœur d'un programme d'accès sécurisé ;
- Il explique les distinctions importantes à faire, et donne des conseils sur la manière d'évaluer un prestataire potentiel ;
- Il fournit des informations précieuses sur les tendances en matière de fuites de données ;
- Il propose un processus en cinq phases facile à exécuter pour mettre en œuvre une stratégie de sécurisation des données pratique, mesurable et adaptée aux risques ; et enfin,
- Il propose de nombreuses « meilleures pratiques » pour éviter les pièges courants et éliminer la plupart des défis opérationnels qui se posent lors de la mise en œuvre du DLP.

« Ce n'est pas la technologie derrière les contrôles DLP qui détermine votre réussite – c'est la méthodologie et la stratégie d'exécution de votre fournisseur qui dicteront à la fois votre expérience et vos résultats. »

Un point de départ

Tous vos contrôles DLP doivent répondre aux deux premiers objectifs de la liste suivante.

1. Ils vous donnent la capacité d'identifier les données.

- → **Données dynamiques** (qui circulent dans le réseau)
- → **Données en cours d'utilisation** (utilisées sur le terminal)
- → **Données statiques** (inactives, dans un système de stockage)
- → **Données dans le cloud** (utilisées, en mouvement, statiques)

2. Elles sont capables d'identifier les données comme étant décrites ou inscrites

- → **Décrites :** Des classificateurs et des modèles de politique prêts à l'emploi vous aident à identifier les types de données. Ceci est utile lorsque l'on recherche des contenus comme des informations personnelles identifiables (PII).
- → **Inscrites :** Les données sont inscrites dans le système pour y laisser leur empreinte, ce qui permet une comparaison totale ou partielle des informations spécifiques, par exemple les propriétés intellectuelles (PI).

Cependant, une solution DLP plus avancée sera équipée du troisième élément.

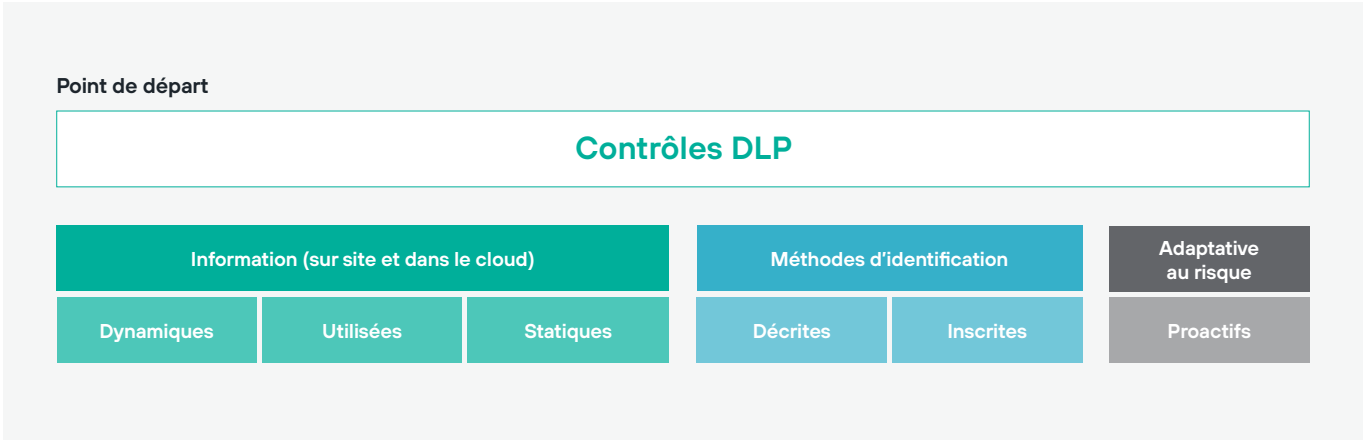
3. Elles adoptent une approche adaptative au risque avec la DLP

- → Les solutions modernes de prévention de perte des données par méthodologie adaptative se distinguent des autres suites d'outils DLP. Selon l'approche CARTA (l'évaluation continue de gestion de risque) de Gartner, la protection adaptée au risque renforce la flexibilité et les actions préventives dans une solution DLP. Elle ajuste et applique de manière autonome la stratégie DLP en fonction du risque qu'une personne pose pour une entreprise à un moment donné. L'application des règles en temps réel est alors en mesure de prévoir et d'arrêter les violations avant qu'elles ne se produisent. La productivité augmente, car les utilisateurs sont moins exposés à des mesures de sécurité intrusives, tandis que les enquêtes informatiques sont facilitées par la réduction des faux positifs et le classement des risques d'incidents.

Pour expliquer comment fonctionnent les deux premières capacités communes, on indique à un contrôle DLP :

- → Ce qu'il faut rechercher (par exemple, des numéros de carte de crédit).
- → a méthode d'identification de l'information (inscrite/enregistrée).
- → Où rechercher (par exemple sur le réseau, les terminaux, le stockage, dans le cloud).

Ce qui se passe après qu'une commande DLP a identifié les informations est dépendant a) de la tolérance au risque du propriétaire des données, b) des options d'intervention disponibles lorsque la perte de données est détectée et c) de la capacité d'adaptation au risque de la solution.



De la vision à l'implémentation

Bien que tous les contrôles DLP disposent de capacités identiques, il est important de comprendre que tous les prestataires ne partagent pas la même vision quant à son fonctionnement, et quant à la manière de résoudre les problèmes de pertes de données. Votre première tâche sera de connaître la méthodologie et la stratégie d'exécution de chaque prestataire que vous envisagez d'engager.

En demandant à un prestataire quelle est sa méthodologie, vous lui demandez en fait quelle est sa vision sur la façon dont cet outil vous aidera à résoudre le problème posé par la perte de données.

C'est une question importante, mais rarement posée. La réponse vous permet de comprendre la vision du prestataire, ce qui vous permet d'identifier ses capacités uniques et l'orientation probable de sa feuille de route. Si vous êtes un décideur, savoir pourquoi les prestataires agissent ainsi contribuera à votre succès et votre satisfaction à long terme.

La méthodologie d'un prestataire a également une grande influence sur sa stratégie d'exécution ou de mise en œuvre. Par exemple, si la méthodologie d'un prestataire commence par l'évaluation des données statiques, tandis que celle d'un autre commence par l'évaluation des données dynamiques par des contrôles adaptatifs, on peut voir que leurs stratégies d'exécution diffèrent considérablement. La manière dont un prestataire exécute les contrôles DLP est importante, car elle a un impact sur votre coût total d'acquisition (CTA) et sur la rentabilité prévue, deux éléments essentiels pour prendre une bonne décision d'achat et définir correctement les attentes avec vos parties prenantes.

Remarque importante : vous devez éviter d'appliquer la méthodologie d'un prestataire avec la technologie d'un autre. La méthodologie définit et oriente la feuille de route technologique d'un prestataire. Si vous mélangez ces deux aspects, vous risquez d'investir dans une technologie qui ne répondra pas à vos besoins à long terme.

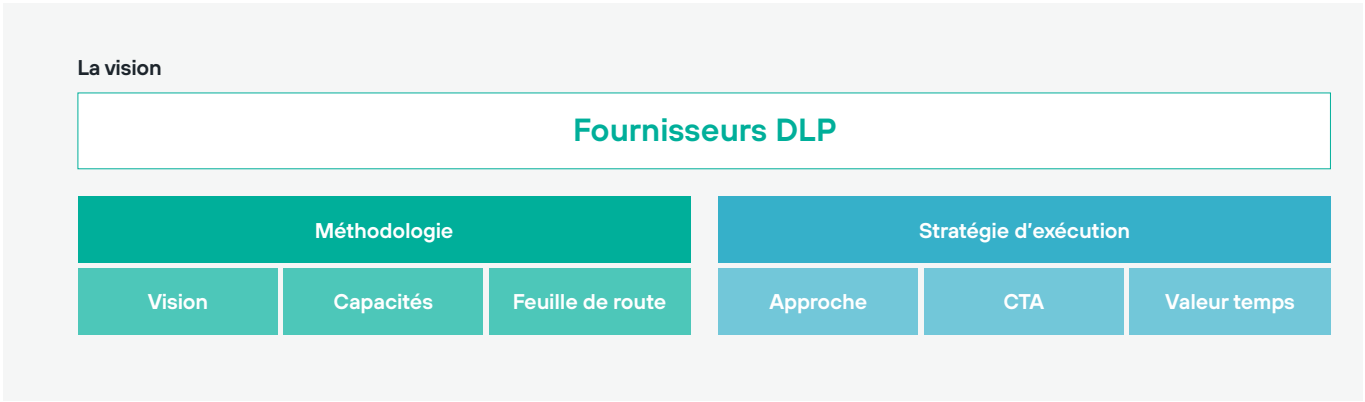
Une DLP quantifiable et pratique

Si vous avez assisté à une conférence ou lu un article sur les meilleures pratiques de DLP, vous savez probablement déjà compris qu'il ne faut pas « Essayer de tout faire à la fois ». Cela signifie que vous ne pouvez pas exécuter un programme DLP complet en une seule fois. Ce n'est pas une bonne pratique, car cela ne vous aide pas à savoir que faire, et quand. À bien des égards, « N'essayez pas de tout faire à la fois » est davantage un avertissement qu'un principe inscrit dans les bonnes pratiques.

Malheureusement, beaucoup de bonnes pratiques, telles qu'elles sont publiées, ne sont pas toujours pragmatiques. Le manque de ressources, financières ou autres, et d'autres problèmes d'organisation empêchent souvent de suivre les bonnes pratiques – ce qui les rend inutilisables en pratique. De même, de nombreuses directives vont trop loin dans la prudence. Les données doivent être sécurisées, mais accessibles – des politiques trop intrusives et corrigées peuvent devenir un obstacle à la productivité et un risque pour les entreprises. Les bonnes pratiques pragmatiques, qui prennent en compte les coûts, les avantages et les efforts nécessaires pour les appliquer, ont beaucoup plus de valeur et peuvent être mesurées pour déterminer leur adoption par vous et votre entreprise.

Pour que votre contrôle DLP soit mesurable et pragmatique dans la gestion et l'atténuation des risques de perte de données, vous devez connaître et comprendre deux informations clés :

1. Pour être mesurable, vous devez connaître et appliquer la formule de risque de perte de données. Bien qu'elle soit similaire aux autres modèles de risque, la formule de risque de perte de données présente une différence importante, que nous expliquons ci-dessous.
2. Pour être pragmatique, vous devez comprendre les endroits où vous êtes le plus susceptible de subir une violation de données à fort impact, et utiliser la règle des 80/20 pour concentrer votre attention et vos ressources.



La formule du risque de perte de données

La formule de base de calcul de risque que la plupart d'entre nous connaissent est la suivante :

Risque = Impact x Probabilité

Le défi posé à la plupart des modèles de risque consiste à déterminer la probabilité qu'une menace se concrétise. Cette probabilité est cruciale pour déterminer s'il convient de dépenser de l'argent pour une solution de prévention des menaces, ou de renoncer à un tel investissement et d'accepter de vivre avec ce risque.

La différence avec la formule de risque de perte de données est que vous ne traitez pas avec un paramètre inconnu. La probabilité admet le fait que la perte de données est inévitable et généralement non intentionnelle. Plus important encore, la formule de calcul de risque permet de quantifier et d'atténuer les risques à un niveau acceptable pour votre entreprise.

Par conséquent, la mesure utilisée pour suivre la réduction du risque de perte de données et le retour sur investissement des contrôles DLP est la méthode basée sur le risque d'occurrence (RO).

Risque = Impact x Risque d'occurrence (RO)

Le RO indique la fréquence à laquelle, sur une période donnée, les données sont utilisées ou transmises via des moyens présentant des risques de perte, de vol ou de compromission. Le RO est mesuré avant et après l'exécution des contrôles DLP pour démontrer le taux de réduction du risque.

Par exemple, si vous démarrez avec un RO de 100 incidents sur une période de deux semaines, et que vous pouvez réduire ce nombre à 50 incidents sur une période de deux semaines après la mise en œuvre des contrôles DLP, vous avez alors réduit la probabilité d'un incident de sécurité des données de 50 %.

Les solutions adaptatives au risque sont particulièrement efficaces pour minimiser le RO. En effet, elles sont beaucoup plus précises pour identifier le véritable risque lié aux données dans le contexte des interactions plus larges d'un utilisateur. Elles réduisent considérablement les faux positifs et offrent donc un avantage par rapport à une solution DLP traditionnelle en ne se contentant pas de minimiser le risque, mais en le présentant de manière plus précise.

La règle 80/20 de la DLP

En plus d'identifier le risque d'occurrence, il est important de découvrir quel est l'endroit où votre entreprise risque de subir un incident de compromission des données. Pour cela, vous devez étudier les dernières tendances en matière d'infraction, puis utiliser la règle des 80/20 pour déterminer où déployer vos efforts DLP. Une étude récente présente ces informations.

Selon une étude réalisée en 2021 par le Ponemon Institute, les informations d'identification compromises sont le vecteur d'attaque initial le plus courant, représentant 20 % des intrusions, suivi par le phishing (17 %).[1]

Pour véritablement disposer d'un programme efficace de protection contre la perte de données, vous devez avoir confiance en votre capacité de détection et de réaction face aux mouvements de données survenant sur le Web, la messagerie électronique, le cloud et les supports amovibles.

C'est ici qu'une solution DLP adaptable aux risques peut offrir un avantage. Les solutions DLP traditionnelles ont souvent du mal à identifier des éléments tels que des processus d'activité défaillants ou des activités irrégulières, qui peuvent entraîner une perte de données significative. Une solution DLP adaptative comprend le comportement des utilisateurs et les compare avec une base de référence pour renforcer rapidement et de manière autonome les mesures DLP, lorsque l'activité n'est pas conforme à la fonction de l'utilisateur final ou avec son comportement normal. Cette approche proactive peut réduire les risques d'exposition ou de perte de données accidentelle.

[1] Coût moyen d'un incident de compromission des données 2021 Rapport du Ponemon Institute pour le compte d'IBM.

La méthodologie DLP Forcepoint et sa stratégie d'exécution

Les dernières tendances en matière de perte de données, et l'application de la formule de risque de la perte de données sont les premières étapes pour la création d'une stratégie de prévention de perte de données. La méthodologie DLP la plus efficace se concentre sur la compréhension des intentions de l'utilisateur, pour empêcher la perte de données avant qu'elle ne survienne. L'exécution devrait se concentrer à apporter la meilleure rentabilité pour une réduction des risques mesurable.

Valeur temps

La valeur temps est le délai séparant l'implémentation des contrôles de DLP de la constatation d'une réduction mesurable des risques. Étant donné que l'utilisateur constitue le principal point de risque pour les données, qu'il s'agisse d'une personne interne accidentelle ou malveillante ou de la cible de vecteurs d'attaque externes, vous obtenez le meilleur délai de rentabilité avec une solution DLP axée sur les données statiques et en transit, grâce à une technologie d'adaptation au risque en arrière-plan.

Vous devez à ce stade être assez sceptique, si d'autres prestataires ou maîtres à penser vous ont dit que votre solution DLP devrait privilégier avant tout les données statiques. Ils disent souvent que, « si vous ne savez pas ce que vous avez, et où ces données se trouvent, vous ne pouvez prétendre à les protéger ». Mais ce n'est pas vrai : en fait, les contrôles DLP sont conçus pour assurer cette protection. Soit les autres prestataires et les experts ne comprennent pas comment correctement évaluer et traiter les risques, soit ils répètent simplement ce que d'autres ont dit, parce que cela les rassure.

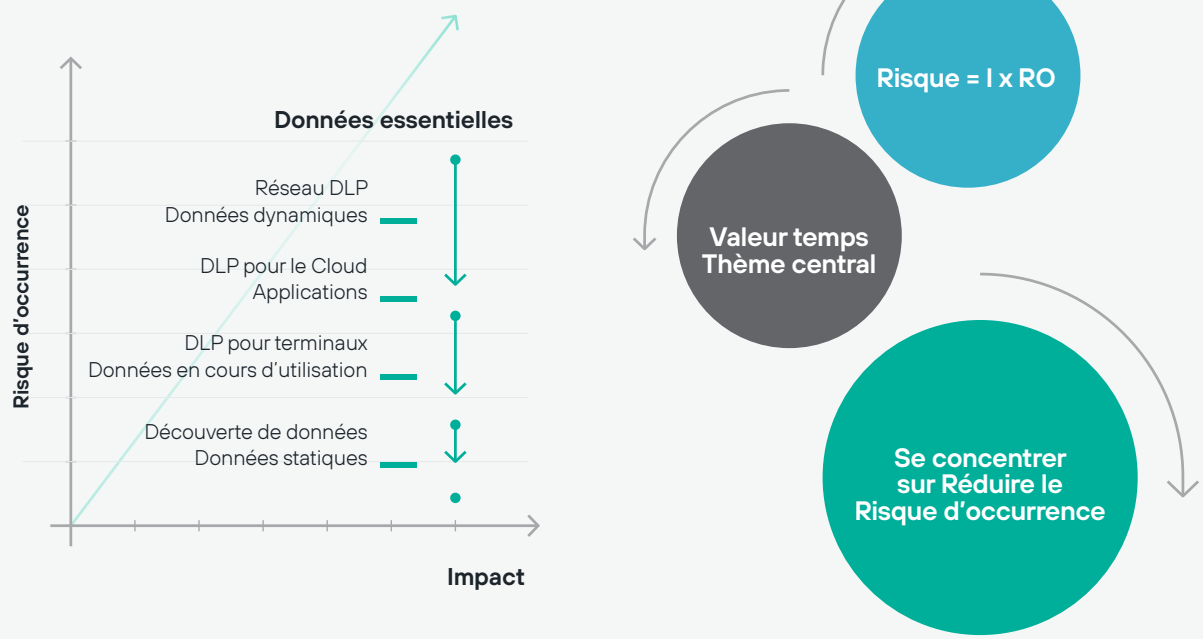


Figure 1. La méthodologie DLP Forcepoint et sa stratégie d'exécution

Pourquoi douter d'un conseil concernant les données statiques ? Envisagez les questions suivantes :

1. Connaissez-vous une organisation qui a réussi à identifier et à sécuriser toutes ses données sensibles, spécialement après une adoption cloud accélérée ?
2. Avez-vous une idée du temps qu'il faudra pour analyser, identifier et sécuriser chaque fichier contenant des informations sensibles ?
3. Savez-vous quelle sera la réduction de risque qui en résultera ?

Le problème, en se concentrant initialement sur les données statiques, est que l'on se concentre sur le risque implicite, et non sur le risque réel, et que cela ne peut donc pas être mesuré dans le contexte de la réduction du risque. Le risque implicite signifie que d'autres conditions doivent être remplies avant qu'une conséquence négative se produise. Dans un contexte de perte de données, ces conditions sont :

- → Quelqu'un ou quelque chose ayant une intention malveillante doit être présent sur votre réseau ou doit pouvoir accéder à vos environnements cloud.
- → Ils doivent rechercher activement vos données sensibles.
- → Ils doivent les trouver.
- → Ils doivent les déplacer.

Ceci est vrai pour chaque entreprise, et nous conduit à la question la plus importante : « Avez-vous confiance en la capacité de détection et de réaction de votre entreprise, lorsque vos données se déplacent ? »

Il y a trois canaux susceptibles de causer la perte de données, et c'est là que vous détectez et réagissez face à un risque réel :

- → Le canal Réseau (p. ex. courriel, web, points d'accès distants, FTP)
- → Le canal Terminal (p. ex. stockage USB, imprimantes)
- → Le canal Cloud (p. ex. Office 365, Box)

Que faire pour les données statiques et la conformité ?

De nombreuses réglementations vous obligent à analyser vos systèmes de stockage pour rechercher des données statiques non protégées. Vous pouvez donc vous demander pourquoi une méthodologie et une stratégie d'exécution DLP ne commenceraient pas là. Mais la vérité, c'est que les auditeurs s'inquiètent davantage du fait de savoir si vous êtes en marche vers la conformité, plutôt que savoir si vous vous êtes conformé.

Ainsi, la recherche de données statiques est importante pour être en marche vers la conformité, mais pas pour l'objectif principal ni pour la valeur de votre contrôle DLP. Prévoyez donc d'utiliser une méthode DLP pour la découverte de données et la mise en conformité, mais d'une manière pratique et atteignable par votre organisation.

Créez des politiques de suppression justifiable (destruction des fichiers dont vous n'avez plus besoin) pour réduire les risques et la conservation à long terme lorsque la loi l'exige. Le meilleur endroit pour commencer est d'utiliser le contrôle DLP pour mettre automatiquement en quarantaine les fichiers qui n'ont pas été consultés depuis au moins six mois. Mandatez vos équipes juridiques afin qu'elles puissent prendre des décisions en fonction des politiques de conservation des données.

Les cinq phases de la réussite DLP

Les cinq phases qui suivent vous donnent un processus de mise en œuvre de contrôles DLP, facile à suivre pour votre entreprise et capable de produire des résultats mesurables. Que vous soyez au début de votre maturité DLP ou que vous ayez bien avancé, utilisez ces étapes comme plan pour implémenter avec succès des applications DLP traditionnelles, ou pour améliorer une approche DLP bien adaptée aux risques encourus.

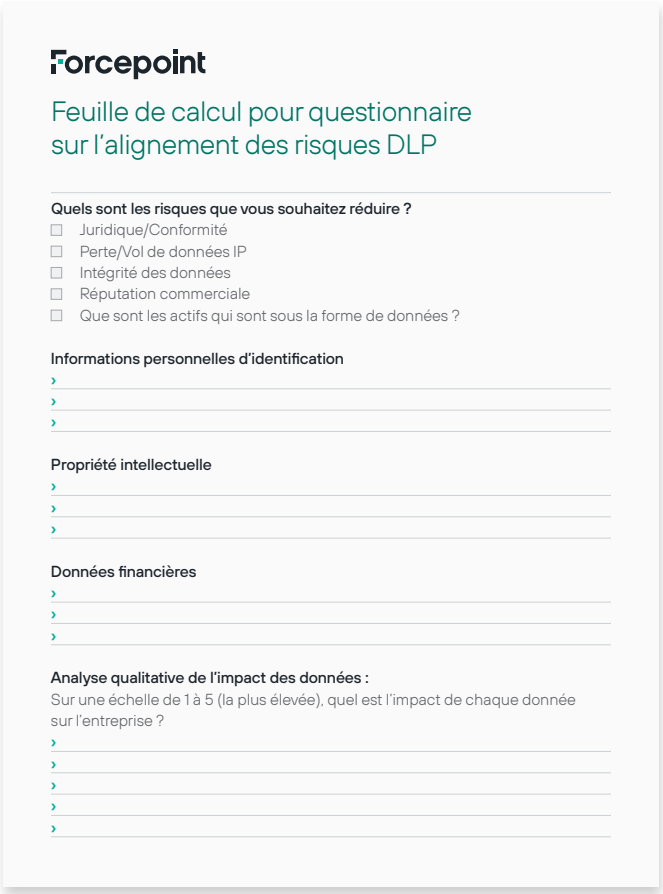
Phase 1 :

Créer un profil d'information de risque

Objectif : Comprendre la portée de vos besoins en matière de protection des données.
Vue d'ensemble : Créez un profil d'information de risque initial qui inclut :

- → Une déclaration expliquant les conséquences potentielles en cas d'inaction.
- → Une description des types de données concernées (par exemple, PII, PI, données financières).
- → Les définitions des canaux de Réseau, de Terminaux et de Cloud, dans lesquels les informations peuvent être perdues ou volées.
- → Une liste des contrôles de sécurité existants en cours d'utilisation pour la protection des données (p. ex. cryptage)

1. **Déterminez les risques que vous souhaitez réduire**
2. **Commencez à dresser une liste détaillant votre capital-données et ventilez-la par type.**
3. **Interrogez les propriétaires des données pour déterminer l'impact.**
4. **Faites une liste des canaux de transmission des informations.**



Forcepoint

Feuille de calcul pour questionnaire sur l'alignement des risques DLP

Quels sont les risques que vous souhaitez réduire ?
- ☐ Juridique/Conformité
- ☐ Perte/Vol de données IP
- ☐ Intégrité des données
- ☐ Réputation commerciale
- ☐ Que sont les actifs qui sont sous la forme de données ?

Informations personnelles d'identification
›
›
›

Propriété intellectuelle
›
›
›

Données financières
›
›
›

Analyse qualitative de l'impact des données :
Sur une échelle de 1 à 5 (la plus élevée), quel est l'impact de chaque donnée sur l'entreprise ?
›
›
›
›
›

Phase 2 :

Créez un diagramme de Sévérité d'Incident et d'Intervention

Objectif : Déterminez les temps de réaction en cas d'incident de perte de données selon le degré de gravité.

Vue d'ensemble : Demandez à votre équipe de déploiement DLP de rencontrer les propriétaires des données pour déterminer le niveau d'impact en cas de perte, de vol ou de compromission. Utilisez une méthode d'analyse quantitative pour décrire l'impact, par exemple une échelle de 1 à 5. Cela aide à hiérarchiser les interventions en cas d'incident, et à déterminer le temps de réaction approprié.

Option DLP adaptative au risque : N'oubliez pas qu'une solution DLP qui adopte une approche adaptative au risque est conçue pour hiérarchiser les activités à haut risque, appliquer de manière autonome des contrôles basés sur le risque et réduire la durée de l'enquête sur un incident. Il en résulte un risque d'impact moindre et un contrôle proactif sur les données critiques.

Les étapes initiales s'appliquent toujours, mais seront complétées par des DLP s'adaptant au risque.

1. **Commencez par discuter des types de données à protéger.**
2. **Déterminez les réglementations relatives aux types de données identifiés.**
3. **Déterminez comment vous identifierez les données.**
4. **Déterminez la gravité de l'impact et l'intervention nécessaire**

« Les violations de données à caractère personnel doivent être signalées à l'autorité de surveillance compétente dans les 72 heures suivant la prise de connaissance de la violation », selon le RGPD.

Réglementations			**Étape 1 :** Discuter des types de données généraux **Étape 2 :** Règlements relatifs (Assistant disponible) **Étape 3 :** « D » - Enregistré ou décrit **Étape 4 :** Quantité ou % pour Élevée Moyenne Faible		Légende Taux d'impact		
Notification de Faille	HIPPA	PCI/PCI-DSS			5, 4	3, 2	1
			Informations personnelles d'identification	ID	Élevée	Moyen	Faible
			VIP PII	R	1	-	-
			IIP	D	>100	>25	>2
			DAR	D	>100	>50	>2
			Informations financières	ID	Élevée	Moyen	Faible
			Cartes de crédit	D	>25	>5	>2
			Informations sur les salariés	D	>25	>5	>2
			Propriété intellectuelle	ID	Élevée	Moyen	Faible
			Projet X	R	>25 %	>10 %	< 10 %
			Document de conception	R	>25 %	>10 %	< 10 %
			Noms d'utilisateurs et mots de passe	R	>25 %	>10 %	< 10 %

Étape 1 : Déterminez l'intervention face à l'incident selon la sévérité et le canal

Objectif : Définissez ce qui se passe suite à un incident de perte de données, selon sa sévérité et son canal.

Vue d'ensemble : Votre entreprise dispose d'un nombre limité de canaux via lesquels circulent les informations. Ces canaux deviennent les points de surveillance utilisés par les contrôles DLP pour détecter les pertes de données et pouvoir intervenir. Répertoriez tous les canaux de communication disponibles sur votre réseau, sur les terminaux et dans le cloud (par exemple les applications cloud autorisées) sur une feuille de calcul. Appliquez ensuite une intervention (en fonction de la gravité de l'incident) à l'aide de l'une des options d'intervention disponibles dans les contrôles DLP de ce canal.

Vous pouvez également clarifier toute exigence supplémentaire de votre entreprise pour effectuer l'intervention souhaitée, comme le cryptage ou l'inspection SSL. Par exemple, les supports amovibles sont l'un des trois principaux vecteurs de perte de données. Cependant, c'est aussi un excellent outil pour augmenter la productivité.

L'une des options permettant d'atténuer le risque de perte de données dans Box ou Google Drive consiste à supprimer automatiquement le partage des fichiers contenant des informations sensibles, et qui sont transférés vers le stockage cloud et partagés en externe.

Option DLP adaptative au risque : Une solution DLP adaptative peut fournir aux entreprises des contrôles d'application granulaires sur tous les canaux, offrant ainsi la possibilité d'ajuster les interventions en fonction du niveau de risque de l'utilisateur (par exemple, audit uniquement pour les utilisateurs à faible risque et blocage pour les utilisateurs à haut risque). Cela permet aux utilisateurs d'exécuter efficacement leurs tâches sans risquer de compromettre les données.

1. **Choisir les données ou le type de données**
2. **Confirmer les canaux à surveiller**
3. **Déterminer l'intervention selon la gravité.**
4. **Noter les exigences supplémentaires pour l'intervention souhaitée.**

Canaux	Niveau 1 **Faible**	Niveau 2* **Faible-Moyen**	Niveau 3 **Moyen**	Niveau 4 **Moyen-Élevé**	Niveau 5 **Élevée**	Notes
Web	Audit	Audit/Notifier	Bloquer/Notifier	Bloquer/Alerter	Bloquer	Proxy pour bloquer
Web sécurisé	Audit	Audit/Notifier	Bloquer/Notifier	Bloquer/Alerter	Bloquer	Inspection du SSL
Courriel	Crypter	Supprimer les pièces jointes des courriels	Mise en quarantaine	Mise en quarantaine	Bloquer	Chiffrement
FTP	Audit	Audit/Notifier	Bloquer/Notifier	Bloquer/Alerter	Bloquer	Proxy pour bloquer
Imprimante réseau	Audit	Audit/Notifier	Bloquer/Notifier	Bloquer/Alerter	Bloquer	Installer des agents DLP pour imprimante
Applications Cloud	Audit	Audit/Notifier	Mise en quarantaine avec remarque	Mise en quarantaine	Bloquer	
Personnalisé	Audit	Audit/Notifier	Bloquer/Notifier	Bloquer/Alerter	Bloquer	À déterminer

*Granularité supplémentaire disponible avec une DLP adaptative au risque.

Figure 2. Feuille de route des politiques des canaux DLP

Étape 2 : Créez un flux de travail d'incident

Objectif : S'assurer que les procédures d'identification et d'intervention en cas incident sont suivies.

Vue d'ensemble : Consultez la figure 3. Reportez-vous au diagramme de flux de travail de réponse aux incidents ci-dessous pour afficher le processus de gestion des incidents en fonction de leur gravité et voir ce qui se passe une fois l'incident détecté. Pour les incidents peu graves, appliquez une automatisation lorsque la chose est possible. Cela inclut généralement l'envoi de notification aux utilisateurs et aux managers en cas de comportement à risque. Cela peut également inclure des mesures de formation des employés pour permettre l'autocorrection des risques.

Les incidents à impact plus élevé nécessitent l'intervention d'un analyste en incidents, qui enquêtera et déterminera le type de menace (p. ex. accidentelle, intentionnelle ou malveillante). L'analyste en incidents transmet l'incident et son analyse au responsable de programme (généralement le responsable de la sécurité ou de la conformité), qui détermine ensuite les actions à entreprendre et les équipes à inclure.

Option DLP adaptative au risque : Si vous choisissez de tirer parti des avantages d'une solution adaptative, l'enquête d'un analyste en incidents n'est pas nécessaire avant la prise de mesures. Les incidents attribués aux utilisateurs et présentant un risque peu élevé peuvent ne pas représenter une menace pour l'organisation, et ils ne doivent donc pas entraîner des actions qui risqueraient d'impacter la productivité. Ces actions autorisées incluraient cependant des mesures de protection, comme le cryptage requis lors de la sauvegarde de données sur un périphérique USB ou la suppression de pièces jointes envoyées par courrier électronique.

Pour les utilisateurs présentant un risque élevé et les incidents qui leur sont associés, les administrateurs peuvent adopter une approche proactive en bloquant ou en limitant automatiquement certaines actions jusqu'à ce que l'analyste en incidents puisse enquêter.

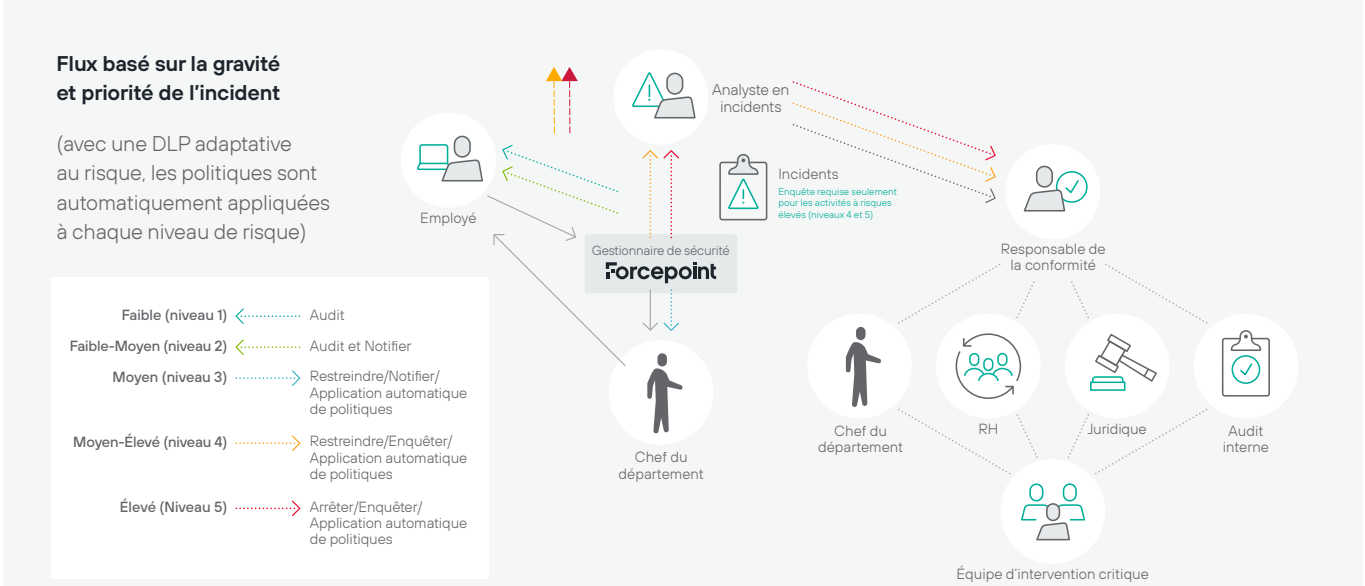


Figure 3. Flux de travail en cas d'incident

Phase 3 :

Piloter le programme de surveillance

Objectif : Implémenter un contrôle DLP sur le réseau pour quantifier et commencer à réduire les risques

Vue d'ensemble : La Phase 3 comporte quatre étapes supplémentaires. Au cours de l'étape 1, vous attribuez des rôles et des responsabilités aux principales parties prenantes. À l'étape 2, vous établissez le cadre technique. À l'étape 3, vous élargissez la couverture des contrôles DLP. Puis, à l'étape 4, vous intégrez ces contrôles à l'ensemble de votre entreprise.

Avant d'être appliquée activement, la DLP doit fonctionner de manière passive, pour vous permettre de comprendre les effets de vos politiques. Alors que vous approfondissez votre connaissance des mouvements et de l'utilisation des données dans votre entreprise, vous pouvez ajuster les contrôles pour appliquer des règles destinées aux utilisateurs présentant un risque plus élevé.

Après la surveillance initiale, au cours de laquelle vous déployez un contrôle DLP réseau, effectuez une analyse et présentez les résultats clés à l'équipe de direction. Vous devriez inclure des recommandations pour les activités d'atténuation des risques susceptibles de réduire le risque d'occurrence des données présentant un risque. Synthétisez ensuite les résultats et présentez-les à l'équipe de direction.

Option DLP adaptative au risque : Si vous choisissez d'implémenter un système DLP adaptatif aux risques, vous pouvez exécuter une analyse des incidents en mode audit uniquement ou en mode d'application progressive des règles.

Ces données contrastées souligneront la réduction du nombre d'incidents nécessitant une enquête sans compromettre vos données. Les résultats observés seront plus révélateurs que de vrais positifs. Ils peuvent également démontrer les avantages de l'automatisation, la réduction des ressources nécessaires pour surveiller et gérer les incidents et la productivité accrue des équipes concernées.

Étape 1 : Attribuer des rôles et des responsabilités

Objectif : Augmenter la stabilité du programme DLP, sa modularité et son efficacité opérationnelle.

Vue d'ensemble : Quatre rôles différents sont généralement attribués pour préserver l'intégrité des contrôles DLP et accroître leur efficacité opérationnelle.

- → Administrateur technique
- → Analyste en incidents/manager
- → Enquêteur en examen de preuves
- → Auditeur

Chaque rôle est défini en fonction de ses responsabilités et attribué à l'acteur concerné. À ce stade, il est courant de voir des membres de l'équipe de l'implémentation DLP agir en tant que managers d'incidents. Toutefois, à mesure que les contrôles DLP atteignent leur maturité et présentent un niveau de confiance élevé, ces rôles sont transférés au propriétaire adéquat des données.

Figure 4. Attribuer des rôles et des responsabilités

Étape 2 : Mettre en place le cadre de travail technique

Objectif : Créer une base de référence pour les contrôles de sécurité des donnes, afin d'aider votre entreprise à déterminer ce qu'est le comportement normal des utilisateurs, et pour empêcher les violations de données à fort impact.

Vue d'ensemble : À ce stade, le rôle du contrôle DLP est principalement un rôle de surveillance, en ne bloquant que les incidents graves (par exemple, le téléchargement de données vers des destinations malveillantes connues, le téléchargement en masse de données non protégées en une seule opération). Cette approche utilisant uniquement un audit peut également être réalisée à l'aide d'une solution DLP adaptative au risque en définissant chaque niveau de risque sur « audit uniquement ».

1. **Installez et configurez**
2. **Surveillez le réseau**
3. **Analysez les résultats**
4. **Informations aux Dirigeants 1**
5. **Activités de réduction des risques** (p. ex. activer des politiques de blocage)
6. **Analysez les résultats**
7. **Informations aux Dirigeants 2**

Les phases 4 et 5 abordent en profondeur le retour sur investissement et le suivi de la réduction des risques.

Mettre en place le cadre de travail technique	Lundi	Mardi	Mercredi	Jeudi	Vendredi
Semaine 1 : Installer / Régler / Former					
Semaine 2 : Surveiller					
Semaine 3 : Surveiller					
Semaine 4 : Informations aux Dirigeants 1					
Semaine 5 : Réduction des risques					
Semaine 6 : Informations aux Dirigeants 2					

Figure 5. Chronologie de l'implémentation - Partie 1

Étape 3 : Étendre la couverture des contrôles DLP

Objectif : Implémenter un DLP sur les terminaux et les applications cloud autorisées pour quantifier et commencer à réduire les risques.

Vue d'ensemble : Vous êtes maintenant prêt à traiter les données en cours d'utilisation et les données statiques. Au cours de cette étape, vous allez déployer votre solution DLP sur les terminaux et les applications cloud autorisées, surveiller et analyses et vos données, informer l'équipe de direction et exécuter des activités d'atténuation des risques, comme vous l'avez fait au début de la Phase 3. La principale différence est que vous choisissez maintenant de réagir aux incidents selon les différents canaux et les options disponibles pour les données en cours d'utilisation, ce qui se produit au niveau du terminal et des applications cloud. (Vous avez déterminé la gravité de l'incident et de l'intervention selon le canal pendant la Phase 2.)

Pour les données statiques, le processus identifie et hiérarchise les cibles à analyser et déplace toutes les données non utilisées depuis longtemps en un espace de quarantaine. Vos équipes juridiques et de la mise en conformité peuvent alors les traiter, conformément aux stratégies de conservation des données en vigueur dans votre entreprise. En ce qui concerne la conformité, il s'agit avant tout d'une question de coopération – coopérez, mais à un rythme raisonnable pour votre entreprise. Ce n'est pas un concours : il n'y a pas de médaille remise à celui qui termine en premier.

Si vous devez effectuer une tâche de découverte au plus vite, sachez que vous pouvez augmenter temporairement (ou définitivement) la vitesse à laquelle la recherche est effectuée à l'aide d'agents de découverte locaux, ou en déployant simultanément plusieurs appareils de découverte sur le réseau.

1. **Déploiement sur les terminaux et les applications cloud autorisées et surveillance**
2. **Lancez les analyses de découverte**
3. **Analysez les résultats**
4. **Informations aux Dirigeants 3**
5. **Activités de réduction des risques**
6. **Analysez les résultats**
7. **Informations aux Dirigeants 4**

Étendre la couverture des contrôles DLP	Lundi	Mardi	Mercredi	Jeudi	Vendredi
Semaine 7 : Déployez sur les terminaux et les applications cloud (autorisées)					
Semaine 8 : Surveillance des terminaux et des applications cloud (autorisées) / Données statiques					
Semaine 9 : Surveillance des terminaux et des applications cloud (autorisées) / Données statiques					
Semaine 10 : Informations aux Dirigeants 3					
Semaine 11 : Réduction des risques					
Semaine 12 : Informations aux Dirigeants 4					

Figure 6. Chronologie de l'implémentation - Partie 2

Étape 4 : Intégrer les contrôles DLP dans le reste de l'entreprise

Objectif : La gestion des incidents est déléguée aux principaux intervenants des principales unités d'activité.

Vue d'ensemble : Si vous n'avez pas encore impliqué directement les propriétaires des données et d'autres parties prenantes clés dans l'implémentation de votre DLP, c'est maintenant le moment de le faire.

En particulier, le rôle de manager d'incidents convient mieux aux propriétaires des données, car leur responsabilité est engagée en cas de perte de données. Le fait de leur confier la gestion des incidents élimine un intermédiaire et améliore l'efficacité opérationnelle. En outre, cela leur permet d'estimer avec précision leur tolérance au risque et de bien comprendre comment leurs capitaux de données sont utilisés par d'autres.

Au cours de cette étape, demandez à l'équipe chargée du déploiement DLP d'organiser une réunion de lancement pour présenter les contrôles DLP aux autres parties prenantes. Poursuivez cela avec une formation pour familiariser les nouveaux membres de l'équipe avec l'application de la gestion des incidents. Avant de transférer les responsabilités de gestion des incidents, définissez une période pendant laquelle vous apportez de l'assistance à l'équipe lors de l'intervention sur un incident, pour que les nouveaux membres soient opérationnels.

1. **Créez et impliquez le comité**
2. **Mise à jour du programme et des rôles**
3. **Formation**
4. **Intervention assistée sur un incident**
5. **Informations aux Dirigeants 5**
6. **Intervention sur un incident par le comité**
7. **Informations aux Dirigeants 6**

Intégrer les contrôles DLP dans le reste de l'entreprise	Lundi	Mardi	Mercredi	Jeudi	Vendredi
Semaine 13 : Sélection et Notification					
Semaine 14 : Mise à jour du programme et des rôles					
Semaine 15 : Formation avec assistance sur intervention					
Semaine 16 : Informations aux Dirigeants 5					
Semaine 17 : Intervention sur un incident par le comité					
Semaine 18 : Informations aux Dirigeants 6					

Figure 7. Chronologie de l'implémentation - Partie 3

Phase 4 :

Adoptez la Protection Proactive

Objectif : Passer à une protection et une réponse automatisées pour les événements à haut risque.

Vue d'ensemble : Les entreprises passent généralement à la protection proactive et automatisée et à la personnalisation en deux étapes. La première étape consiste à passer de l'audit à l'analyse. La seconde étape consiste à automatiser les interventions. Gardez à l'esprit que, dans la plupart des cas, il n'est pas possible de sauter des étapes dans ce parcours.

Étape 1 : Analyses et alertes

Objectif : Commencez à analyser les données et leurs mouvements au sein d'une entreprise pour comprendre ce qui s'est passé lors d'une incident de compromission des données.

Vue d'ensemble : Vous devez quitter l'audit pour analyser comment une infraction s'est produite. Pour cela, vous devez savoir où se trouvent les données, ce qu'elles font et où elles vont. Le problème, avec les outils de recherche Big Data et les produits DLP traditionnels qui n'offrent que des fonctionnalités de découverte et de commande des données, c'est qu'ils n'alertent les administrateurs en cybersécurité des violations de données qu'après coup, et qu'ils n'incluent pas de bons outils d'analyse post-incident. Ils sont réglés en mode « audit uniquement » avec de bonnes intentions – éviter de perturber les opérations commerciales légitimes – mais, de ce fait, ils n'offrent pas autant d'aide pour prévenir les incidents ultérieurs. À ce stade, les entreprises peuvent être « en conformité » mais non sécurisées.

Cette analyse post-piratage peut être très solide et utiliser les meilleurs outils d'analyse post-incident disponibles, mais elle reste par nature réactive. Néanmoins, les entreprises qui en sont à ce stade de leur parcours sont en mesure de tirer les leçons qui s'imposent et d'adapter manuellement leurs politiques de sécurité des données pour aider à prévenir le prochain incident.

Étape 2 : Automatisation proactive et personnalisation de la sécurisation des données

Objectif : Devenir totalement proactif dans la prévention d'une violation de données par infiltration ou exfiltration, en analysant automatiquement le comportement de l'utilisateur et du système, en bloquant l'accès et l'activité considérés comme une menace, et en ajustant automatiquement les politiques aux individus à mesure qu'elles apprennent le contexte autour du comportement constaté. Une approche entièrement automatisée fournit un score de risque comportemental pour un utilisateur dans une entreprise. Ce score permet d'adapter proactivement la sécurité selon l'individu, sans gêner l'utilisateur. Les scores de risque tiennent compte des aléas de l'interaction des utilisateurs avec les données, les systèmes et les applications, et fournissent le contexte nécessaire au comportement, ce qui aide à réduire les faux positifs. Les actions qui représentent un faible risque sont autorisées, tandis que les activités à plus haut risque génèrent des réponses automatisées qui vont des alertes aux administrateurs, au cryptage, au blocage complet et à d'autres mesures de sécurité prédéfinies.

Voilà ce qu'est la sécurité moderne des données : il s'agit d'un processus adaptatif et automatisé qui crée le moins de frictions possible dans l'entreprise en stoppant les activités dangereuses, mais qui ne gêne pas les utilisateurs et les systèmes par un blocage trop zélé. Les solutions DLP basées sur les risques sont conçues pour renforcer les activités de l'entreprise plutôt que de les freiner, en protégeant les personnes et les données sans impacter la façon dont les personnes utilisent les données pour travailler.

> **« Les solutions DLP basées sur les risques sont conçues pour renforcer les activités de l'entreprise plutôt que de les freiner, en protégeant les personnes et les données sans impacter la façon dont les personnes utilisent les données pour travailler. »**

En passant d'une prévention passive des pertes de données à une sécurité adaptée au risque, les entreprises peuvent réduire le risque de dégât sur l'image de marque ou mitiger les pénalités financières résultant d'incidents, tout en tirant parti de l'intelligence comportementale pour mieux atteindre leurs objectifs.

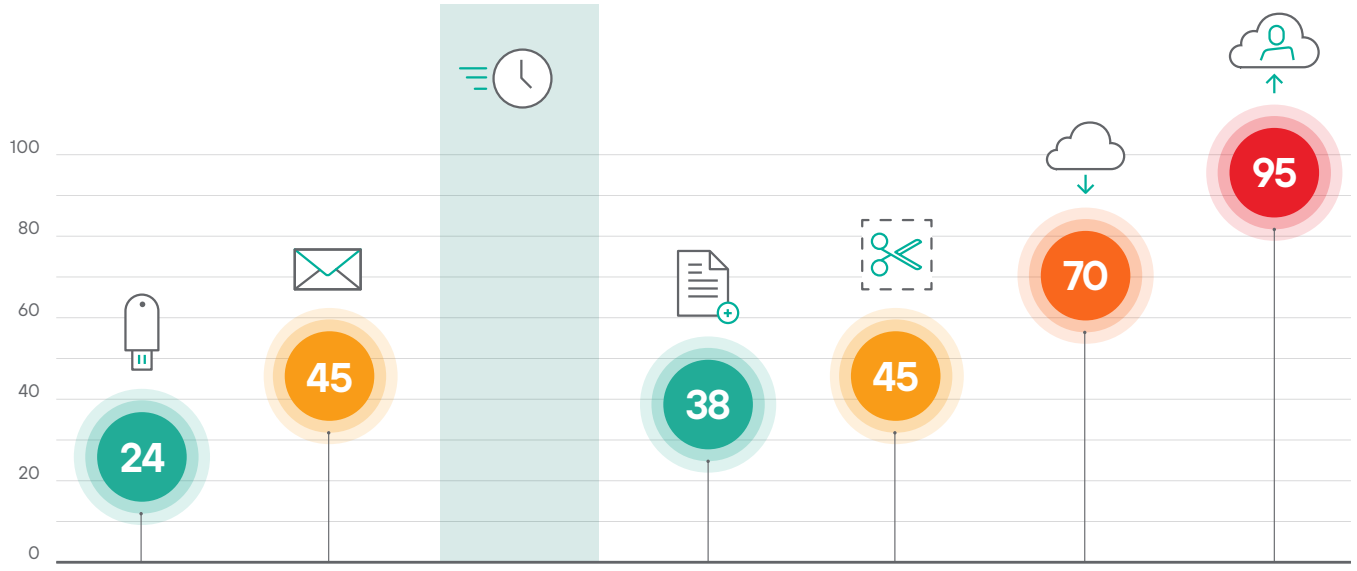


Figure 8. Montrer comment l'activité d'un utilisateur peut augmenter son score de risque

Phase 5 :

Suivre les résultats de la réduction des risques

Objectif : Montrer le ROI en prouvant une réduction quantifiable des risques.

Vue d'ensemble : Il y a deux points clés à ajouter au processus de suivi de réduction des risques, qui ont été mentionnés dans la 3e phase. Ce sont :

1. Les incidents relatifs devraient être groupés ensemble.
Les groupes les plus fréquemment utilisés incluent la gravité, le canal, le type de données et la réglementation. Pour les entreprises les plus importantes, des sous-groupes supplémentaires devraient aider à clarifier davantage le risque en fonction de la localisation géographique ou des filiales.

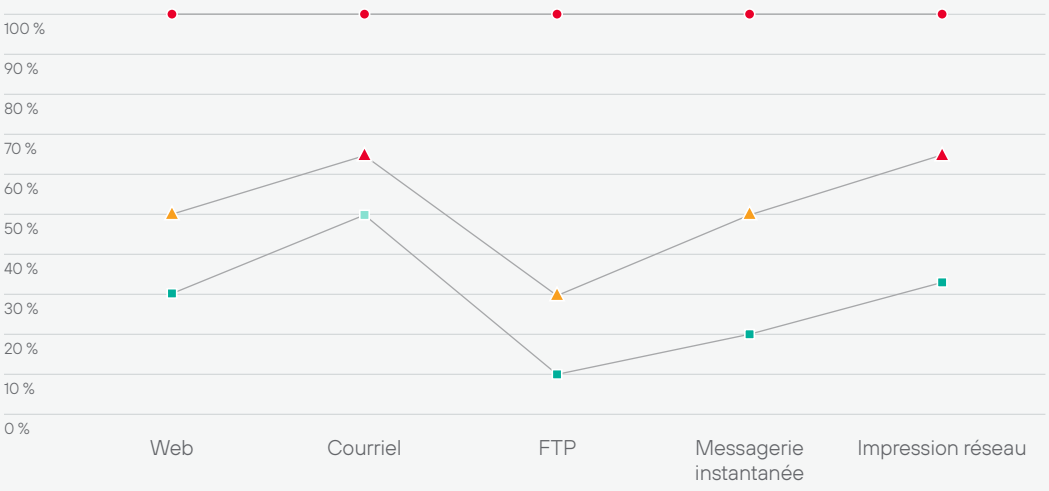
2. Maintenez l'homogénéité entre les phases de réduction des risques.
Pour préserver l'intégrité de vos résultats, les périodes de surveillance et de réduction des risques doivent être d'une durée égale. Au début, nous recommandons deux semaines pour améliorer le délai de rentabilisation et simplifier l'analyse. Cependant, vous êtes le mieux placé pour déterminer ce qui est le plus raisonnable pour votre entreprise.

Vous trouverez ci-dessous un exemple de la mise en groupe et le suivi de la réduction des risques. Notez qu'il y a une période de temps homogène, une concentration sur les incidents à haut risque et que ces incidents sont regroupés selon leur canal relatif.

Option DLP adaptative au risque : Si vous avez décidé d'adopter une approche adaptative au risque, vous devrez fournir une comparaison des incidents capturés en mode audit uniquement (tous les incidents) par rapport aux incidents nécessitant une enquête avec une exécution graduée. La synthèse doit indiquer le nombre d'incidents pour chaque niveau de risque classé de 1 à 5, par opposition à ceux nécessitant une enquête (niveaux de risque 4 et 5).

Enfin, lorsque vous informez votre équipe de direction sur le processus DLP et ses résultats, rappelez-vous que moins, c'est plus. Concentrez-vous sur l'ensemble de la situation lorsque vous expliquez les vecteurs à haut risque de votre entreprise, et décrivez les activités recommandées d'atténuation des risques ainsi que les coûts, les avantages et les efforts requis.

Probabilité de la Perte de données



Légende marqueur

- Élevée
- Modérée
- Faible
- Acceptable
- Base de référence de 30 jours
- 60 jours
- 90 jours

Nombre d'incidents pendant 90 jours

Incidents	Web	Courriel	FTP	Messagerie instantanée	Impression réseau
Base de référence de 30 jours	200	150	50	10	45
Base de référence de 60 jours	100	100	15	15	30
› Réduction des risques sur 60 jours	50 %	33 %	70 %	50 %	33 %
Base de référence de 90 jours	60	76	5	2	15
› Réduction des risques sur 90 jours	70 %	49 %	90 %	80 %	67 %

Objectifs

- **60 jours** 25 % de réduction et +
- **90 jours** 50 % de réduction et +

Figure 9. Suivre le risque de perte de données

Conclusion

Une implémentation DLP réussie ne sera pas le fruit d'une dernière technique à la mode, et elle ne peut pas être simplement mise sur une étagère et stockée dans le centre de données. En fait, elle dépend de votre aptitude à :

1. Comprendre la méthodologie d'un fournisseur DLP et sa stratégie d'exécution. Votre entreprise tirera un avantage en distinguant l'approche DLP des différents prestataires. Cela vous permet de déterminer les méthodologies les plus prometteuses pour votre environnement, et les technologies DLP à évaluer. Envisager un prestataire qui fournit une solution adaptative peut apporter des avantages durables à une entreprise, notamment une efficacité et une productivité accrues.Et n'oubliez pas : appliquer la méthodologie d'un fournisseur à la technologie d'un autre a des conséquences négatives à long terme.

2. Appliquez la formule de risque de perte de données. Une fois que votre équipe de sécurité a compris et appliqué la formule de risque de perte de données, elle peut collaborer avec les propriétaires des données pour identifier et hiérarchiser leur capital de données. En outre, chaque activité d'atténuation des risques doit être conçue dans le seul but de réduire le risque d'occurrence de perte des données. Le risque d'occurrence est la meilleure façon de quantifier et de suivre la réduction des risques, et affiche également le ROI des contrôles DLP. Rappelez-vous : comparez les solutions DLP traditionnelles avec une technologie DLP à technologie adaptative au risque, afin de ne pas comparer les faux positifs aux vrais positifs.

3. Appliquez la règle 80/20 pour l'allocation de ressources. En identifiant les vecteurs de perte de données posant le plus grand risque de violation à impact élevé, votre entreprise peut utiliser la règle 80/20 pour l'allocation de ressources et établir des stratégies de protection efficaces.

4. Suivez les neuf étapes de la réussite DLP. Que vous adoptiez une approche DLP traditionnelle ou une approche s'adaptant aux risques, notre processus en 9 étapes est une formule éprouvée pour mettre en œuvre les contrôles DLP de manière pratique pour votre entreprise, produisant des résultats exploitables, mesurables et adaptatifs aux menaces.

Forcepoint

forcepoint.com/contact

À propos de Forcepoint

Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données. Son objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Nos solutions à facteur humain s'adaptent en temps réel à la façon selon laquelle les individus interagissent avec les données, et offrent un accès sécurisé tout en permettant aux employés de créer de la valeur. Basé à Austin, au Texas, Forcepoint crée des environnements sûrs et fiables protégeant des milliers de clients dans le monde entier.