Forcepoint

Les 9 étapes pour réussir sa protection des données

Protéger vos données consiste à comprendre les risques potentiels encourus par vos données, et prendre les mesures adéquates si ces risques se concrétisent.

Mais comment trouver l'équilibre entre ce dont votre entreprise a besoin pour travailler, et ce dont elle a besoin pour assurer la sécurité de ses données ?

Ces neuf étapes vous montreront comment mettre en œuvre des contrôles de protection des données qui soient à la fois efficaces et pratiques pour votre fonctionnement quotidien, et identifieront les points où consolider votre solution par une protection des données adaptative aux risques.

1

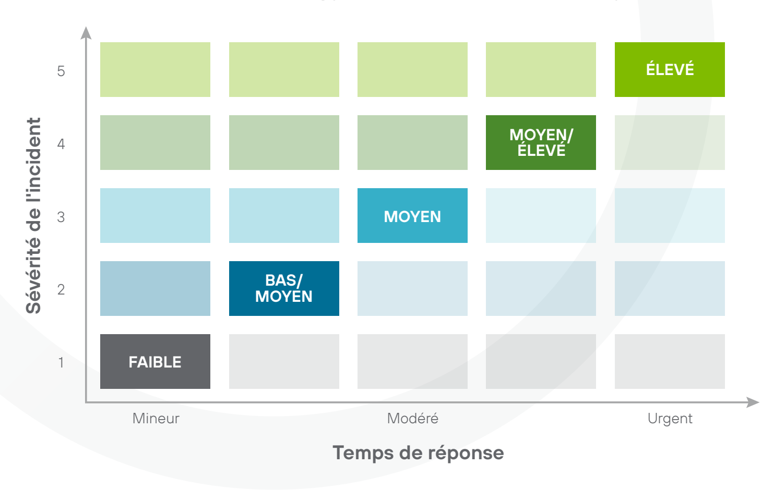
Créer un profil d'information de risque

Un profil de risque vous permet de comprendre ce qu'il vous faut dans votre solution de protection des données. Tout d'abord, énoncez les risques que vous souhaitez atténuer et dressez la liste des types de données concernées, en les regroupant par type de données si nécessaire. Ensuite, définissez les réseaux, les terminaux et les canaux cloud où ces données pourraient potentiellement être perdues, ainsi que les contrôles que vous utilisez actuellement pour les sécuriser.

2

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

Cartographier chaque type de données avec son impact sur l'activité vous permettra de hiérarchiser vos réponses et de concentrer les ressources de sécurité là où elles sont les plus efficaces. Pour certaines entreprises, cela peut être un exercice difficile. Pour commencer, discutez avec les propriétaires de données pour déterminer des types de données à protéger, et les risques encourus en cas d'incident. Ensuite, classez-les sur une échelle de 1 à 5 (1 = impact faible, 5 = impact élevé) et définissez un temps de réponse acceptable pour chacune en fonction de la gravité du risque - vous voulez sécuriser d'abord les types de données à haut risque.



L'avantage d'être adaptatif au risque :
La protection des données adaptative au risque est conçue pour donner la priorité aux activités à haut risque, appliquer de manière autonome les contrôles en fonction du risque et réduire le temps nécessaire pour enquêter sur un incident.

3

Déterminer une réponse à un incident de données selon le canal et sa gravité

Quand il s'agit de protection des données, garder une longueur d'avance signifie savoir comment réagir aux incidents avant qu'ils ne se produisent. Dressez la liste de tous les canaux de votre réseau, des points d'extrémité et du cloud où circulent les données. Ensuite, déterminez une réponse appropriée pour les incidents de faible à fort impact en fonction des besoins du canal.

L'avantage d'être adaptatif au risque :
Une solution adaptative au risque tient compte du niveau de risque de chaque personne qui touche à vos données, ce qui vous permet d'ajuster les réactions aux incidents en fonction du risque individuel. Par exemple, l'adaptation de la réponse à “Audit uniquement” pour les utilisateurs à faible risque, et à “Blocage” pour les utilisateurs à haut risque, garantit que chaque membre de votre équipe peut effectuer son travail sans compromettre les données ni nuire à la productivité des autres utilisateurs.

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

*Granularité supplémentaire disponible avec une protection des données adaptative au risque.

4

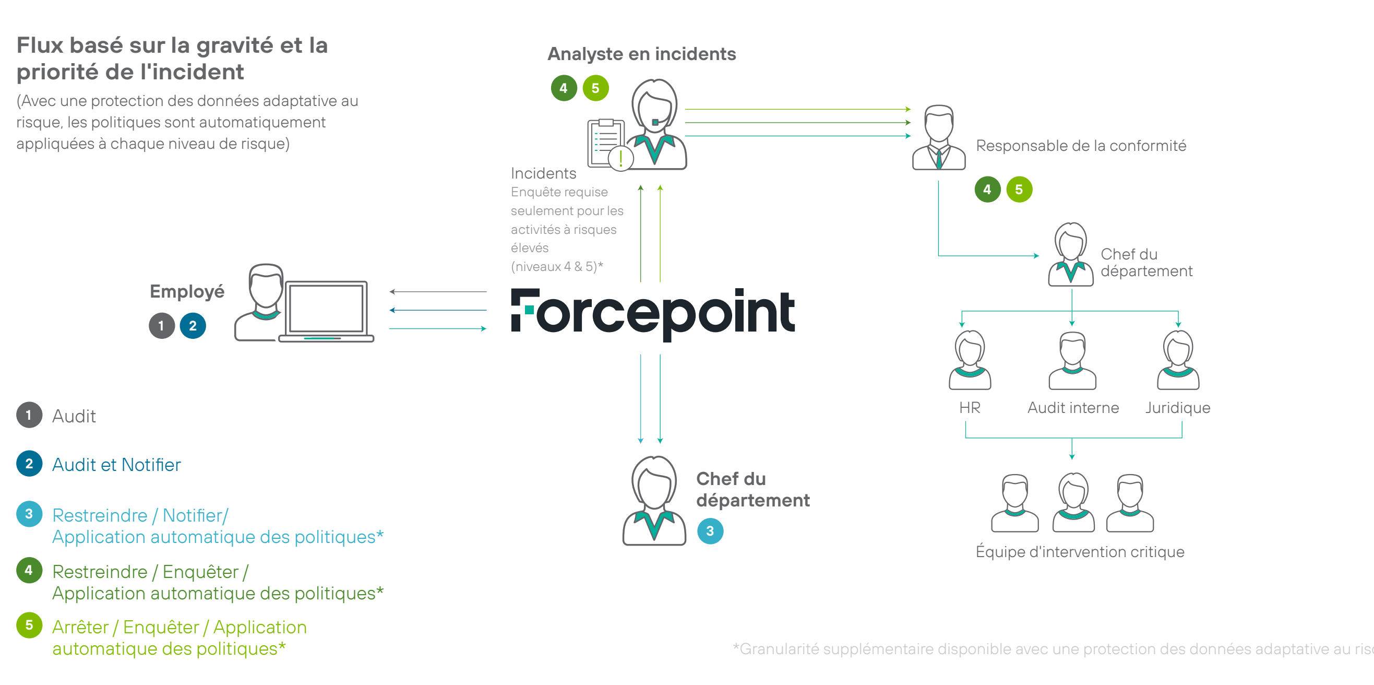
Créez un flux de travail d'incident

Assurez-vous que vos équipes de sécurité peuvent passer à l'action dès qu'un incident est détecté, en définissant clairement le déroulement des opérations de réponse pour les incidents de faible à fort impact. Pour les incidents à faible impact, automatisez autant que possible. Cela permettra de libérer de la bande passante pour appliquer manuellement des mesures correctives adéquates en cas d'incidents à fort impact.

L'avantage d'être adaptatif au risque :
Une solution adaptative aux risques vous permet d'analyser les incidents selon le niveau de risque individuel, sans avoir besoin d'engager un analyste en incidents pour déterminer la meilleure mesure à prendre. Les incidents liés à des personnes à faible risque peuvent ne pas constituer une menace pour votre entreprise, de sorte que leur permettre de continuer (avec des garanties supplémentaires comme le cryptage pour le transfert de fichiers USB ou la suppression automatique des pièces jointes aux courriels) ne ralentit pas la roue de la productivité.

Les administrateurs peuvent adopter la même approche proactive avec les personnes et les incidents à haut risque en bloquant ou en limitant automatiquement des actions spécifiques jusqu'à ce qu'un analyste en incidents puisse enquêter.

Flux basé sur la gravité et la priorité de l'incident
(Avec une protection des données adaptative au risque, les politiques sont automatiquement appliquées à chaque niveau de risque)



- ① Audit
- ② Audit et Notifier
- ③ Restreindre / Notifier/ Application automatique des politiques*
- ④ Restreindre / Enquêter / Application automatique des politiques*
- ⑤ Arrêter / Enquêter / Application automatique des politiques*

*Granularité supplémentaire disponible avec une protection des données adaptative au risque.

5

Attribuer des rôles et des responsabilités

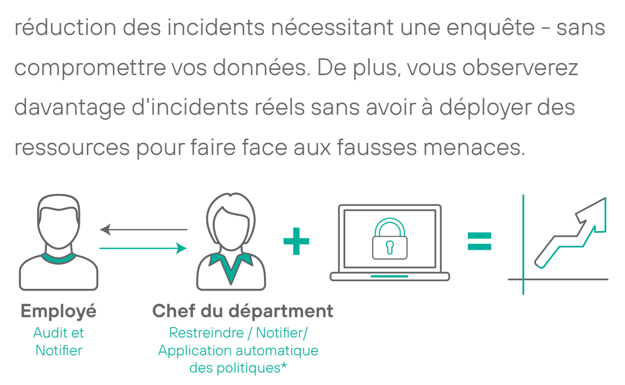
Augmenter la stabilité du programme de protection des données, sa modularité et son efficacité opérationnelle en définissant clairement les rôles dans l'équipe. Attribuer des rôles clés tels que ceux d'administrateur technique, d'analyste en incidents, d'enquêteur et d'auditeur, et accorder à chacun les droits et l'accès appropriés.

6

Démarrer le projet en mode surveillance

Une fois que vous avez mis en place votre solution de protection des données de votre réseau, une période de surveillance vous permettra d'identifier des modèles dans votre activité et de définir une base de référence pour vous aider à reconnaître le comportement normal des utilisateurs. Une fois cette période terminée, analysez les comportements que vous avez observés et présentez vos conclusions à votre équipe de direction, ainsi que vos recommandations sur la manière d'atténuer les risques. Vous pouvez ensuite mettre ces recommandations en pratique, observer leur efficacité et les présenter à nouveau à vos supérieurs.

L'avantage d'être adaptatif au risque :
Avec une solution adaptative aux risques, l'analyse des incidents en mode audit uniquement (par opposition au mode d'application progressive) mettra en évidence la réduction des incidents nécessitant une enquête - sans compromettre vos données. De plus, vous observerez davantage d'incidents réels sans avoir à déployer des ressources pour faire face aux fausses menaces.



7

Adoptez la Protection Proactive

Ce que vous avez appris pendant le mode Surveillance vous donnera la confiance nécessaire pour passer en mode Blocage pour les événements à haut risque, ou conformément à votre plan de réponse aux incidents. Tandis que vous déploierez la protection des données sur les terminaux et les applications cloud sanctionnées, vous surveillerez, analyserez, signalerez, optimiserez et partagerez à nouveau vos conclusions avec l'équipe de direction.

8

Intégrez des contrôles de protection des données à travers toute l'entreprise

Lorsque vous déléguez des responsabilités aux responsables de la sécurité dans les différents services, pensez en termes d'efficacité. Par exemple, les propriétaires de données sont déjà responsables en cas de perte : en les nommant gestionnaires d'incidents, on les aide à comprendre comment les données sont utilisées par d'autres et à évaluer leurs risques, ce qui élimine les allers-retours inutiles.

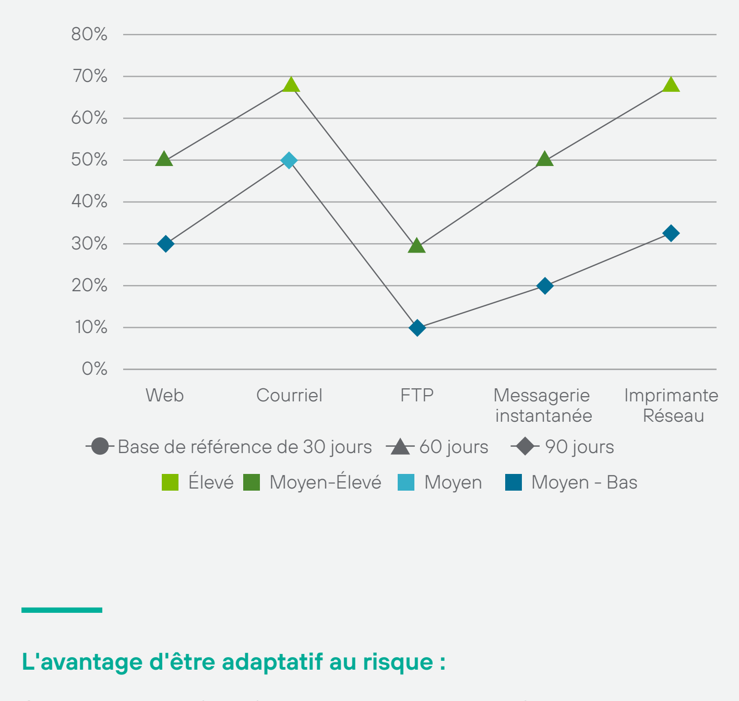
Commencez à passer le flambeau en demandant à l'équipe de sécurité d'organiser une réunion de lancement pour présenter à d'autres personnes les contrôles de protection des données. Suivez ensuite la formation des nouveaux membres de l'équipe, puis définissez une période pendant laquelle vous les aiderez à réagir aux incidents afin qu'ils se sentent à l'aise avec vos processus. Vous pouvez également envisager de proposer un coaching en temps réel pour renforcer ces processus.

9

Suivre les résultats de la réduction des risques

Vous avez commencé à vous préparer pour cela à la sixième étape - voici ce qu'il reste à faire : Regroupez et liez les incidents selon des critères tels que la gravité, le canal, le type de données et la réglementation. Ensuite, définissez une durée égale pour vos périodes de surveillance et de réduction des risques (essayez de commencer par deux semaines chacune) afin de préserver l'intégrité de vos résultats.

Probabilité de la Perte de données



Nombre d'incidents sur 90 jours

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

Objectifs

60 jours
Remise de 25 %

90 jours
Remise de 50 %

L'avantage d'être adaptatif au risque :
Avec 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).

Que vous adoptiez une approche traditionnelle ou que vous renforciez votre sécurité par une protection des données adaptative aux risques, cette formule éprouvée vous guidera vers la réussite.

Forcepoint

Vous voulez voir comment fonctionne une protection adaptative aux risques ?

Venez le voir ici :

À propos de Forcepoint
Forcepoint est l'entreprise leader en cybersécurité pour la protection des utilisateurs et des données, dont l'objectif est de protéger les entreprises tout en stimulant la transformation et la croissance numériques. Les solutions personnalisées de Forcepoint s'adaptent en temps réel à la façon dont les personnes 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 pour des milliers de clients dans le monde entier.[23MAR2020]