Une étude Forrester
Total Economic Impact™
commandée par Varonis
Mai 2018

Etude Total Economic Impact™ de la Plateforme de Sécurité des Données Varonis

Réduction des coûts et bénéfices commerciaux : les promesses de la Plateforme de Sécurité des Données Varonis

FORRESTER®

Table des matières

Synthèse **1**

Résultats clés 2

Cadre de travail et méthodologie TEI 4

Parcours client avec la Plateforme de Sécurité des Données Varonis **5**

Organisation interrogée 5

Evaluation des risques et résumé des mesures correctives 6

Principaux défis 7

Résultats clés 8

Analyse des avantages et bénéfices **9**

Gain de temps sur les enquêtes d'audit 9

Gain de temps lors de la fourniture d'accès aux fichiers 10

Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations 12

Réduction de l'exposition au risque 14

Flexibilité 16

Analyse des coûts **17**

Coûts d'achat et de maintenance des logiciels 17

Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis 18

Coût de l'effort interne nécessaire pour la planification et le déploiement 19

Résumé financier **21**

Annexe A : Total Economic Impact **22**

Notes de fin **23**

Directeur de projet :
Joe Branca

A PROPOS DE FORRESTER CONSULTING

Forrester Consulting fournit des conseils objectifs, sans parti pris et fondés sur la recherche aux cadres dirigeants afin de faciliter leur réussite au sein de leur entreprise. Qu'il s'agisse de sessions brèves à vocation stratégique ou de projets personnalisés, les services de Forrester Consulting vous mettent en relation directe avec des analystes de recherche qui appliquent leurs connaissances d'expert aux défis spécifiques de votre entreprise. Pour plus d'informations, visitez forrester.com/consulting.

FORRESTER®

ROI
346 %

Bénéfices en valeur actuelle 5,9 millions de dollars

VAN
4,6 millions de dollars

Délai de retour sur investissement < 6 mois

Synthèse

Les violations de sécurité peuvent entraîner une perte monétaire importante, en particulier lorsqu'aucune mesure n'a été prise pour protéger les données stratégiques. Dans de nombreuses organisations, les fichiers et dossiers sont partagés inutilement avec des centaines voire des milliers d'employés, et les utilisateurs ont accès à une quantité de données bien supérieure à celle dont ils ont réellement besoin pour mener à bien leur mission. Les données sensibles sont ainsi bien trop exposées à des personnes malveillantes, aussi bien en interne qu'en externe, car le fait d'accéder aux informations d'identification d'un seul compte peut suffire à déverrouiller l'accès à un trésor d'informations non sécurisées, couvrant aussi bien des business plans que des données du personnel ou des informations client.

Et même si les organisations sont en mesure de localiser leurs données sensibles, assurer leur sécurité peut sembler décourageant. La remédiation de l'accès à un dossier unique peut prendre des heures et nécessiter la mobilisation de plusieurs équipes : service juridique, commercial et sécurité. Ce processus peut se révéler coûteux et, à moins d'être en mesure de déterminer qui a besoin d'accéder aux données, il existe toujours un risque de perturber l'activité.

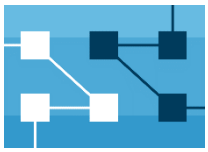
Varonis propose une plateforme de sécurité des données qui permet à ses clients de savoir où résident leurs données sensibles, qui y a accès et, surtout, qui a besoin de cet accès. Les services informatiques peuvent ainsi adopter une stratégie d'accès du moindre privilège, ce qui peut considérablement réduire le risque associé à un incident de sécurité des données tout en maintenant durablement ce statut. Les outils intégrés de machine learning et d'analyse comportementale protègent les données sensibles en permettant aux organisations d'identifier rapidement, entre autres problèmes, les failles et les défauts de configuration.

Varonis a chargé Forrester Consulting d'effectuer une étude Total Economic Impact™ (TEI) et d'examiner le retour sur investissement envisageable pour les entreprises qui déploient la Plateforme de Sécurité des Données Varonis (ou DSP pour Data Security Platform). L'objectif de cette étude est de fournir aux lecteurs un cadre leur permettant d'évaluer l'impact financier potentiel de la Plateforme de Sécurité des Données Varonis sur leur organisation. Afin de mieux comprendre les avantages, les coûts et les risques associés à cet investissement, Forrester a interrogé une entreprise de santé qui utilise des produits Varonis depuis plusieurs années.

Avant de déployer certains composants essentiels de la Plateforme de Sécurité des Données Varonis, le client n'avait pas de visibilité claire sur ce qui se passait sur ses serveurs de fichiers. L'entreprise se savait trop exposée aux ransomwares et à d'autres risques de sécurité, mais ne disposait pas des outils nécessaires pour comprendre la nature exacte de ces menaces et pour prendre d'emblée les mesures adéquates pour les contrer. Avec l'aide de l'équipe Professional Services de Varonis, elle a utilisé la DSP Varonis pour remédier aux problèmes d'accès à plus de 1,5 million de dossiers à haut risque, ce qui a contribué à réduire considérablement le profil de risque de l'organisation.

FORRESTER®

Bénéfices et coûts



Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations :

3 966 948 $

Réduction de l'exposition au risque :

1 893 648 $

Coûts d'achat et de maintenance des logiciels :

898 422 $

Résultats clés

Bénéfices quantifiés. L'organisation interrogée a enregistré les bénéfices suivants, quantifiés en valeur actuelle (VA) pondérée par le risque :

- **Gain de temps sur les enquêtes d'audit, pour une économie totale de 44 651 $.** La plateforme Varonis a permis de réduire de 90 % les efforts liés aux audits et enquêtes du comportement utilisateur, ce qui représente chaque année une économie de 420 heures de travail pour les analystes de sécurité.
- **Gain de temps pour la fourniture d'accès aux fichiers, pour une économie totale de 36 767 $.** Après le déploiement de Varonis, le temps nécessaire à la fourniture des accès aux fichiers (tâche courante pour les analystes de sécurité) a été réduit de 75 %, ce qui a permis à l'entreprise d'économiser chaque année plus de 300 heures de travail.
- **Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations, pour un total de 3 966 948 $ d'économies.** L'organisation cliente a réduit les autorisations pour plus de 1,5 million de dossiers à haut risque. Cependant, cette analyse suppose que, sans logiciel spécialisé, l'organisation aurait tenté de remédier aux problèmes d'accès pour seulement 1 % de ces dossiers afin de protéger les données hautement sensibles. Pour chaque dossier, elle a permis à ses professionnels de la sécurité d'économiser 4,5 heures de travail (3 heures pour un analyste de la sécurité et 1,5 heure pour un employé de niveau cadre) en utilisant Varonis plutôt qu'un traitement manuel.
- **Réduction des risques pour un bénéfice total de 1 893 648 $.** La solution Varonis a aidé l'organisation cliente à réduire son profil de risque de 65 %. Face à un incident de sécurité à grande échelle, un établissement de santé moyen subit des coûts s'élevant à 10 834 560 $. Et au cours d'une année donnée, il existe 14 % de risque que cela se produise. Autrement dit, cette organisation était exposée à un risque total de plus de 1,5 million de dollars. En limitant l'accès partagé aux données et en fournissant de meilleures capacités de détection et de réponse, Varonis a contribué à limiter cette exposition.

Coûts. L'organisation interrogée a enregistré les coûts suivants en valeur actuelle (VA) pondérée par le risque :

- **Coûts d'achat et de maintenance des logiciels, pour un total de 898 422 $.** Le client a payé un prix forfaitaire pour obtenir une licence sur les produits logiciels Varonis ; il paie également des frais de maintenance annuels équivalant à 20 % du prix d'achat initial.
- **Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis, pour un montant total de 488 000 $.** Le client a supporté des coûts en échange des services professionnels fournis par Varonis pour la mise en œuvre et l'opérationnalisation de la Plateforme de Sécurité des Données Varonis ainsi que pour la correction initiale de l'accès aux données stockées sur les systèmes de fichiers du client.
- **Coûts de l'effort interne de planification et de déploiement, pour un total de 5 720 $.** Le client a également engagé des coûts pour les ressources internes qu'il a dû mobiliser pour la planification et la mise en œuvre de la Plateforme de Sécurité des Données Varonis pendant un mois.

L'organisation interrogée a acheté une suite de produits Varonis plus complète que ce qu'achètent au départ la plupart des entreprises. Cet investissement s'est traduit par de plus grands bénéfices sur la période de trois ans d'analyse, mais a également entraîné des coûts plus élevés. La plupart des clients achètent d'abord les composants de base de la plateforme (une offre découverte type pour une organisation qui surveille 1 000 utilisateurs coûte environ 155 000 $) puis ajoutent des produits et des composants au fil du temps.

L'entretien de Forrester avec ce client existant et l'analyse financière qui a suivi ont révélé que cette organisation a pu réaliser des bénéfices de 5 942 014 $ sur trois ans, pour des coûts de 1 332 142 $, ce qui représente une valeur actuelle nette (VAN) de 4 609 872 $ et un ROI de 346 %.

La méthodologie TEI permet aux entreprises de démontrer, justifier et réaliser la valeur tangible des initiatives informatiques aux yeux de la direction et des autres parties prenantes essentielles de l'organisation.

Cadre de travail et méthodologie TEI

Selon les informations fournies par l'organisation interrogée, Forrester a élaboré un cadre de travail Total Economic Impact™ (TEI) pour les organisations qui envisagent de mettre en œuvre la Plateforme de Sécurité des Données Varonis.

L'objectif de ce cadre est d'identifier les coûts, les avantages, le gain de flexibilité et les facteurs de risque qui influent sur la décision d'investissement. Forrester a adopté une approche en plusieurs étapes pour évaluer l'impact de la Plateforme de Sécurité des Données Varonis sur une organisation :

DILIGENCE RAISONNABLE
Entretiens avec des intervenants de Varonis et des analystes de Forrester pour recueillir des données relatives à la Plateforme de Sécurité des Données Varonis.

ENTRETIEN AVEC LE CLIENT
Entretien avec une entreprise qui utilise la Plateforme de Sécurité des Données Varonis afin d'obtenir des données relatives aux coûts, aux avantages et aux risques.

STRUCTURE DU MODELE FINANCIER
Elaboration d'un modèle financier représentatif de l'entretien selon la méthodologie TEI, prise en compte des risques selon les problématiques et les préoccupations de l'organisation interrogée.

ETUDE DE CAS
Emploi de quatre éléments fondamentaux de la TEI dans la modélisation de l'impact de la Plateforme de Sécurité des Données Varonis : les avantages, les coûts, la flexibilité et les risques. Les entreprises recherchent des solutions de plus en plus sophistiquées pour analyser le ROI des investissements informatiques. Pour répondre à leurs attentes, la méthodologie TEI de Forrester offre une visibilité complète sur l'impact économique total des décisions d'achat. Reportez-vous à l'annexe A pour plus d'informations sur la méthodologie TEI.

DECLARATIONS

Les lecteurs doivent être conscients de ce qui suit :

Cette étude est commandée par Varonis et livrée par Forrester Consulting. Elle n'est pas destinée à être utilisée comme une analyse de la concurrence.

Forrester n'émet aucune hypothèse quant au retour sur investissement potentiel dont pourraient bénéficier d'autres organisations. Forrester conseille fortement aux lecteurs d'utiliser leurs propres estimations dans le cadre fourni dans le rapport pour déterminer la pertinence d'un investissement dans la Plateforme de Sécurité des Données Varonis.

Varonis a examiné le contenu de cette publication et proposé des commentaires à Forrester. Toutefois, nous conservons un contrôle éditorial total sur l'étude et ses résultats et n'acceptons pas de procéder à des modifications qui pourraient entrer en contradiction avec les conclusions de Forrester ou obscurcir la signification de l'étude.

Varonis a fourni le nom du client pour l'entretien, mais n'y a pas participé.

Parcours client avec la Plateforme de Sécurité des Données Varonis

AVANT ET APRES L'INVESTISSEMENT DANS LA PLATEFORME DE SECURITE DES DONNEES VARONIS

Organisation interrogée

Pour cette étude, Forrester a interrogé le directeur de la cybersécurité ainsi qu'un analyste de sécurité intervenant auprès d'une compagnie d'assurance-santé qui réalise plusieurs milliards de dollars de chiffre d'affaires. La société fournit une assurance-santé à des personnes et des employeurs dans les 50 états des Etats-Unis. Elle emploie environ 3 000 personnes.

Les indicateurs généraux ci-dessous décrivent les serveurs de fichiers et la structure Active Directory de l'organisation :

- 76 To de données.
- 8,2 millions de dossiers.
- 170 millions de fichiers.
- 8 500 comptes d'utilisateur.
- 11 300 groupes.

En raison de la nature de ses activités, l'organisation cliente gère des données soumises à la règle de confidentialité de la loi sur la transférabilité et la responsabilité de l'assurance-santé (HIPAA).

L'organisation utilise les produits Varonis suivants :

- **DatAdvantage* :** offre aux organisations informatiques une approche efficace de la gestion des autorisations, des audits d'utilisateurs et de la fourniture d'accès aux fichiers.
- **DatAlert :** tire parti du machine learning et de l'analyse comportementale pour déclencher des alertes en cas d'activité suspecte sur les serveurs de fichiers.
- **DataPrivilege :** donne aux utilisateurs métier la possibilité d'examiner et de gérer les contrôles d'accès sans solliciter le service informatique.
- **Data Classification Engine :** recherche les données sensibles et applique des règles de classification pour améliorer la sécurité et la conformité.

L'organisation a choisi Varonis après une étude approfondie des options disponibles sur le marché. « Cela nous est apparu comme une évidence », explique le directeur de la cybersécurité.

**Inclut les composants Windows, SharePoint, Exchange, Active Directory et UNIX.*

> « Si vous connaissez une entreprise ou une autre qui déploie des serveurs de fichiers et des autorisations depuis des dizaines d'années, vous savez que c'est un processus compliqué et fastidieux. Nous avions besoin d'une bonne visibilité sur ce qui se passait sur les serveurs de fichiers et sur les personnes qui y avaient accès. Aujourd'hui, nous pouvons dire sans l'ombre d'un doute que c'est telle ou telle personne qui a touché à telle ou telle chose. Nous n'en avions pas la possibilité avant Varonis, et c'est là que cet ensemble d'outils est d'une valeur inestimable pour nous. »
>
> *Directeur de la cybersécurité*

FORRESTER®

Evaluation des risques et résumé des mesures correctives

Avant le début de la mission, Varonis a procédé à un examen complet des magasins et entrepôts de données du client, conformément aux normes de l'industrie et aux meilleures pratiques de Varonis, afin d'évaluer les risques dans les domaines du contrôle d'accès, de la structure Active Directory, du système de fichiers NTFS, de la structure des autorisations de partage et de la conservation des données.

Cette étude a permis de révéler plusieurs préoccupations impliquant un risque élevé, que Varonis a recommandé de corriger immédiatement :

- 1,5 million de dossiers accessibles par des autorisations globales sur l'ensemble de l'environnement.
- 160 000 fichiers contenant des données sensibles ; 27 % de ces fichiers n'avaient pas été consultés depuis six mois.
- 14 000 fichiers accessibles par des autorisations globales et contenant des fichiers sensibles.
- 3 700 utilisateurs avec des recommandations de suppression.
- 3 000 anciens utilisateurs ayant des autorisations actives (par ex., des employés et sous-traitants qui ont quitté l'entreprise).

L'étude a également permis d'identifier plusieurs préoccupations impliquant un risque faible à moyen :

- 4,1 millions de dossiers, soit près de 17 To de données, contenant des données obsolètes.
- 1 750 utilisateurs avec des mots de passe sans délai d'expiration.
- 960 000 dossiers sur lesquels étaient appliquées des autorisations uniques, directement ou directement et héritées.
- 60 000 dossiers avec des entrées de contrôle d'accès utilisateur (ACE) directes et non de niveau groupe.

Le client a fait appel à l'équipe Professional Services de Varonis pour l'aider à remédier au problème des autorisations sur ses systèmes de fichiers. La mission initiale, qui s'est déroulée sur six mois, a porté sur les mesures correctives suivantes :

- 850 000 dossiers avec des autorisations globales.
- 12 000 dossiers avec des autorisations globales contenant des données sensibles.
- 45 000 fichiers avec des autorisations globales contenant des données sensibles.

Il a fallu 90 jours supplémentaires pour terminer les mesures correctives et atteindre un état d'accès selon le principe du moindre privilège.

> « Du point de vue de la rétention des données, les gens ont toujours un peu peur que quelqu'un puisse avoir besoin de ces fichiers. La question est donc : faut-il s'en débarrasser ou bien les garder sous le coude pour toujours ? Grâce à Varonis, nous sommes en mesure d'informer le reste de l'organisation que les fichiers n'ont pas été consultés depuis six mois ou un an, par exemple. Puisqu'ils ne sont plus nécessaires, nous pouvons les archiver ou les supprimer. »
>
> *Directeur de la cybersécurité*

Principaux défis

Au cours des entrevues, les responsables côté client ont mis en avant les principaux défis suivants qui ont incité l'entreprise à investir dans la Plateforme de Sécurité des Données Varonis :

- **Comprendre l'accès.** L'organisation ne savait pas réellement qui avait accès aux données stockées sur ses serveurs de fichiers et qui en avait besoin à des fins professionnelles. Les autorisations avaient été déployées sur plusieurs décennies. Elles étaient souvent appliquées sans grande cohérence, et beaucoup étaient obsolètes. Résultat : les utilisateurs avaient accès à une quantité de données bien supérieure à celle dont ils avaient réellement besoin pour faire leur travail. Pourtant, sans logiciel spécialisé, il était difficile d'analyser les contrôles d'accès à grande échelle.
- **Comprendre et limiter le risque.** L'organisation avait vu l'impact des violations de données dans l'actualité et cherché des moyens de limiter ces risques. Il lui manquait un moyen de localiser les données sensibles sur ses systèmes de fichiers. Et même en étant en mesure de localiser ces données sensibles, elle était incapable d'annuler les autorisations de manière efficace, sans générer de plaintes de la part des utilisateurs métier.
- **Identifier et traiter les incidents de sécurité.** Avant le déploiement de la plateforme Varonis, l'organisation cliente disposait de certains outils de sécurité, mais qui, selon les personnes interrogées, étaient très insuffisants. Les analystes de sécurité comptaient beaucoup sur les utilisateurs finaux pour leur signaler les problèmes. Dans certains cas, ils ne le faisaient pas, ce qui signifie que des programmes malveillants restaient indétectés pendant plusieurs heures. Et puisqu'il y avait trop d'autorisations sur les fichiers et dossiers, une immense partie des données de l'organisation était exposée. Après coup, les équipes de sécurité avaient du mal à comprendre quelles données avaient été exposées et peinaient à communiquer à la direction les procédures à suivre.

> « Si nous recevons une alerte, que nous commençons à voir certains comportements d'un programme malveillant donné et que nous savons que telle personne a un contrôle total sur un répertoire ou un ensemble de répertoires en particulier, nous pouvons prendre immédiatement des mesures pour contenir la menace. Autrefois, nous n'avions rien. Il fallait que quelqu'un le signale, et dans cet intervalle de temps, la moitié de nos fichiers étaient déjà chiffrés. »
>
> *Directeur de la cybersécurité*

Résultats clés

Au cours des entrevues, les responsables côté client ont mis en avant les principaux résultats suivants découlant de l'investissement dans la Plateforme de Sécurité des Données Varonis :

- **Réduction significative du risque associé à une violation de données.** En limitant l'accès aux seules données dont les employés avaient besoin pour faire leur travail, l'organisation a pu réduire son profil de risque. Avec les produits de Varonis, ainsi qu'avec l'aide de l'équipe Professional Services de Varonis, l'organisation a corrigé les problèmes d'accès à plus de 1,5 million de dossiers ayant un accès ouvert, dont un grand nombre contenait des données sensibles.
- **Amélioration des flux de travail.** Varonis permet aux analystes de sécurité de mener leurs activités quotidiennes avec une plus grande efficacité, ce qui leur libère du temps pour se concentrer sur des activités à plus forte valeur ajoutée. La fourniture des accès aux fichiers et dossiers (procédure nécessaire à chaque fois qu'un nouvel employé rejoint l'organisation) est grandement simplifiée grâce aux solutions proposées par Varonis. De même, dans l'éventualité où un employé serait soupçonné d'accéder à des données d'une manière illicite, il est aujourd'hui bien plus simple de vérifier l'accès de l'utilisateur aux fichiers et dossiers du système.
- **Amélioration de la conservation et de l'archivage.** L'organisation est maintenant en mesure de mieux identifier les données obsolètes et de choisir de les conserver ou les archiver en fonction des besoins métiers. L'évaluation initiale du risque a permis d'identifier plus de 16 To de données obsolètes, soit 22 % de toutes les données de l'environnement contrôlé par Varonis. Ces données représentaient une responsabilité significative, en ce sens que les utilisateurs qui n'avaient pas besoin d'y accéder pouvaient encore le faire. Ces données étaient également soumises à des règles et réglementations sectorielles, et Varonis permet aux analystes de sécurité d'aider les équipes juridiques à s'y conformer.

> « Avec Varonis, il vous suffit de taper un nom d'utilisateur et d'appuyer sur Entrée pour accéder à l'arborescence des fichiers et connaître le niveau d'accès qui lui est accordé. Vous pouvez aller précisément là où il y a des choses à modifier, apporter toutes les modifications nécessaires, puis valider simultanément toutes ces modifications. »
>
> *Analyste Sécurité*

FORRESTER®

Analyse des avantages et bénéfices

DONNEES SUR LES BENEFICES QUANTIFIES

Bénéfice total

REF.	BENEFICE	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3	TOTAL	VALEUR ACTUELLE
Atr	Gain de temps sur les enquêtes d'audit	0 $	17 955 $	17 955 $	17 955 $	53 865 $	44 651 $
Btr	Gain de temps lors de la fourniture d'accès aux fichiers	0 $	14 784 $	14 784 $	14 784 $	44 353 $	36 767 $
Ctr	Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations	2 065 500 $	1 766 700 $	187 200 $	187 200 $	4 206 600 $	3 966 948 $
Dtr	Réduction de l'exposition au risque	0 $	628 540 $	838 053 $	838 053 $	2 304 646 $	1 893 648 $
	Bénéfice total (pondéré par le risque)	2 065 500 $	2 427 979 $	1 057 993 $	1 057 993 $	6 609 464 $	5 942 014 $

Gain de temps sur les enquêtes d'audit

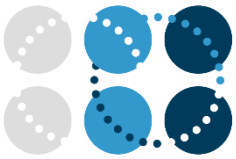
La solution Varonis permet aux analystes de sécurité du client de réaliser plus rapidement des audits et des enquêtes sur la manière dont les utilisateurs accèdent aux fichiers et dossiers.

Avant de déployer DatAdvantage, un à deux jours pouvaient être nécessaires pour effectuer un audit ou une enquête, si tant est que cela fût possible. Les fichiers journaux permettaient aux analystes de sécurité de consulter les accès aux dossiers uniquement sur les 36 heures précédentes, et si le comportement en question s'était produit plus tôt, il était impossible d'en récupérer les enregistrements. Avec Varonis, les analystes peuvent produire des rapports sur les accès utilisateur en quelques minutes, selon les personnes interrogées.

Le modèle financier révèle les constats suivants :

- Avant de déployer la plateforme Varonis, il fallait 12 heures aux analystes de sécurité pour enquêter sur l'historique d'accès aux fichiers d'un utilisateur.
- Chaque année, les analystes de sécurité reçoivent des alertes sur 35 incidents nécessitant une enquête plus approfondie.
- Varonis permet aux analystes de sécurité de mener une enquête sur l'historique d'accès aux fichiers d'un utilisateur avec 90 % d'effort en moins.

Le tableau ci-dessus montre le total de tous les avantages dans les domaines énumérés ci-dessous, ainsi que les valeurs actuelles (VA) minorées de 10 %. Sur une période de trois ans, l'entreprise interrogée s'attend à un bénéfice total de la valeur actuelle pondérée par le risque de plus de 5,9 millions de dollars.



Avant de déployer la solution Varonis, il fallait 12 heures aux analystes de sécurité pour vérifier l'historique d'accès aux fichiers d'un utilisateur.

FORRESTER®

Les risques suivants peuvent affecter cette catégorie d'avantages :

- Le processus que les entreprises ont mis en place pour effectuer cette tâche avant le déploiement d'une solution Varonis.
- La fréquence à laquelle les entreprises devront accomplir cette tâche.

Pour tenir compte de ces risques, Forrester a appliqué une pondération par rapport au risque de 5 %, ce qui donne une valeur actuelle totale pondérée par le risque de 44 651 dollars sur trois ans.

Gain de temps sur les enquêtes d'audit : tableau de calcul

REF.	MESURE	CALC.	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3
A1	Effort nécessaire pour un audit individuel sans Varonis	Heures		12	12	12
A2	Nombre d'incidents nécessitant un audit et une enquête (annuel)			35	35	35
A3	Réduction en pourcentage de l'effort nécessaire pour produire un rapport d'audit			90 %	90 %	90 %
A4	Taux horaire moyen d'un analyste de la sécurité à temps plein			50 $	50 $	50 $
At	Gain de temps sur les enquêtes d'audit	A1*A2*A3*A4	0 $	18 900 $	18 900 $	18 900 $
	Pondération par rapport au risque	↓5 %				
Atr	Gain de temps sur les enquêtes d'audit (pondéré par rapport au risque)		0 $	17 955 $	17 955 $	17 955 $

Gain de temps lors de la fourniture d'accès aux fichiers

La plateforme Varonis permet aux analystes de sécurité de l'organisation cliente de consacrer moins d'heures à la fourniture des accès aux fichiers et dossiers.

Avant le déploiement de la plateforme Varonis, la fourniture des accès aux fichiers et dossiers était un processus manuel qui occasionnait souvent des erreurs, selon un analyste de la sécurité qui consacrait auparavant au moins 8 heures par semaine à cette tâche. Il explique en quoi Varonis a contribué à simplifier ce processus : « Avec Varonis, il vous suffit de taper un nom d'utilisateur et d'appuyer sur Entrée pour accéder à l'arborescence des fichiers et connaître le niveau d'accès qui lui est accordé. Vous pouvez aller précisément là où il y a des choses à modifier, apporter toutes les modifications nécessaires, puis valider simultanément toutes ces modifications. »

(Au moment de l'entrevue, l'organisation cliente n'avait pas encore commencé à utiliser la fonction de demande et d'approbation intégrée à DataPrivilege, qui permet aux utilisateurs métier de demander et d'approuver l'accès aux fichiers et aux dossiers. Elle a utilisé DatAdvantage pour obtenir rapidement une visibilité sur le niveau d'accès d'un utilisateur et pour y apporter efficacement des changements.)

Avant le déploiement de Varonis, les analystes de sécurité consacraient 415 heures chaque année à la fourniture des accès aux fichiers et dossiers.

FORRESTER®

Le modèle financier révèle les constats suivants :

- Avant le déploiement de Varonis, les analystes de sécurité consacraient 415 heures chaque année à la fourniture des accès aux fichiers et dossiers.
- Avec le logiciel Varonis, les analystes de sécurité peuvent réduire de 75 % l'effort nécessaire pour fournir un accès aux fichiers et dossiers.

Les risques suivants peuvent affecter cette catégorie d'avantages :

- Le processus que les entreprises ont mis en place pour effectuer cette tâche avant le déploiement d'une solution Varonis.
- La fréquence à laquelle les entreprises devront accomplir cette tâche.

Pour tenir compte de ces risques, Forrester a appliqué une pondération par rapport au risque de 5 %, ce qui donne une valeur actuelle totale pondérée par le risque de 36 767 dollars sur trois ans.

Gain de temps lors de la fourniture d'accès aux fichiers : tableau de calcul

REF.	MESURE	CALC.	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3
B1	Effort nécessaire pour fournir un accès aux fichiers avant Varonis (annuel)	Heures		415	415	415
B2	Réduction en pourcentage de l'effort nécessaire pour fournir un accès aux fichiers			75 %	75 %	75 %
B3	Taux horaire moyen d'un analyste de la sécurité à temps plein			50 $	50 $	50 $
Bt	Gain de temps lors de la fourniture d'accès aux fichiers	B1*B2*B3	0 $	15 563 $	15 563 $	15 563 $
	Pondération par rapport au risque	↓5 %				
Btr	Gain de temps lors de la fourniture d'accès aux fichiers (pondéré par rapport au risque)		0 $	14 784 $	14 784 $	14 784 $

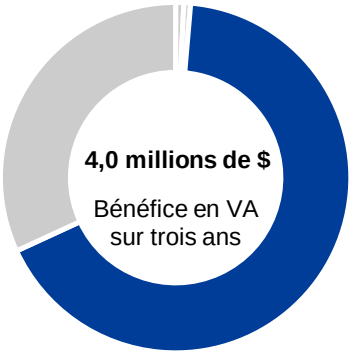
Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations

La plateforme Varonis a permis à l'organisation cliente d'identifier les fichiers et dossiers surpartagés et de corriger leur accès sans impact sur l'activité.

Après de nombreuses années d'octroi d'autorisations, les systèmes de fichiers du client étaient saturés de fichiers et de dossiers surpartagés. Pourtant, le service informatique ne disposait d'aucun moyen de déterminer facilement qui avait eu accès aux fichiers et dossiers et qui avait besoin de cet accès pour faire son travail. Dans la mesure où cela était possible et en l'absence d'une solution logicielle spécialisée, il fallait consacrer énormément de temps et de ressources pour corriger les problèmes liés à l'accès aux éléments surpartagés.

Le modèle financier révèle les constats suivants :

- L'organisation cliente a utilisé la solution Varonis pour comprendre quels utilisateurs avaient eu accès aux fichiers et dossiers et lesquels avaient réellement besoin d'y accéder pour mener à bien leurs fonctions.
- L'évaluation des risques de Varonis a identifié 1,5 million de dossiers associés à un accès global, ce qui représentait un risque élevé.
- Le client, avec l'aide de l'équipe Professional Services de Varonis, a dans un premier temps corrigé l'accès à 850 000 dossiers, suivi de 650 000 dossiers supplémentaires pendant la première année.
- En l'absence d'une solution comme celle de Varonis, l'organisation cliente n'aurait pas tenté d'entreprendre un tel projet, ce qui ne permet pas de calculer ce bénéfice sur la base du nombre total de dossiers dont l'accès a été corrigé.
- L'organisation cliente aurait tenté d'identifier et de corriger l'accès aux dossiers contenant des données hautement sensibles. Le nombre de dossiers qu'elle pourrait identifier et traiter à l'aide d'un processus manuel correspond à 1 % des 1,5 million de dossiers à haut risque identifiés par Varonis. Ce bénéfice est calculé compte tenu uniquement de cette proportion d'1 % des dossiers.
- En l'absence d'une solution spécialisée comme celle de Varonis, il aurait fallu au moins 4,5 heures en moyenne pour corriger l'accès à un seul dossier. Cette estimation inclut 3 heures de travail pour un analyste de la sécurité et 1,5 heure de travail pour un employé de niveau cadre.
- Le coût horaire moyen pour ces ressources suppose un taux horaire de 50,00 $ à temps plein pour l'analyste de sécurité et un taux horaire de 87,50 $ à temps plein pour l'employé de niveau cadre. Ces estimations sont conformes aux taux fournis par l'organisation cliente et sont représentatives du marché régional dans lequel elle recherche des compétences.
- A la suite de la correction initiale, le logiciel de Varonis a permis à l'organisation cliente de maintenir un état d'accès selon le principe du moindre privilège avec deux équivalents temps plein (ETP) de moins que ce qu'il lui aurait fallu employer en d'autres circonstances.



Gain de temps et élimination des coûts associés aux mesures correctives à la gestion des autorisations : **67 %** de bénéfices au total

FORRESTER®

Les risques suivants peuvent affecter cette catégorie d'avantages :

- L'état des systèmes de fichiers d'une entreprise avant le déploiement de Varonis.
- Le coût de recrutement et d'emploi de professionnels de la sécurité sur le marché régional d'une entreprise.

Pour tenir compte de ces risques, Forrester a appliqué une pondération par rapport au risque de 10 %, ce qui donne une valeur actuelle (VA) totale pondérée par le risque de 3 966 948 dollars sur trois ans.

Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations : tableau de calcul

REF.	MESURE	CALC.	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3
C1	Nombre total de dossiers avec accès global supprimé		850 000	650 000		
C2	Pourcentage de dossiers contenant des données sensibles		1,0 %	1,0 %		
C3	Effort nécessaire pour identifier et corriger le problème d'accès global aux dossiers avant le déploiement de Varonis	Heures	4,5	4,5		
C4	Coût horaire moyen des ressources		60 $	60 $		
C5	Coût total des mesures correctives évité grâce à la Plateforme de Sécurité des Données Varonis	C1*C2*C3*C4	2 295 000 $	1 755 000 $		
C6	ETP évités pour la gestion en continu des autorisations	Entretien avec le client		2	2	2
C7	Salaire annuel d'un analyste de la sécurité à temps plein	Entretien avec le client		104 000 $	104 000 $	104 000 $
C8	Economies totales sur les salaires en ETP	C6*C7		208 000 $	208 000 $	208 000 $
Ct	Gain de temps et élimination des coûts associés aux mesures correctives et à la gestion des autorisations	C5+C8	2 295 000 $	1 963 000 $	208 000 $	208 000 $
	Pondération par rapport au risque	↓10 %				
Ctr	Remédiation et gestion des permissions, économies de temps et évitement des coûts (ajustés au risque)		2 065 500 $	1 766 700 $	187 200 $	187 200 $

Réduction de l'exposition au risque

La solution Varonis a aidé l'organisation cliente à réduire son exposition au risque de deux façons : 1) en corrigeant le problème de l'accès global partagé, ce qui peut limiter l'impact d'une violation, et 2) par une détection et une réponse améliorées.

En 2017, les organismes de soins de santé engageaient un coût moyen de 380 $ pour chaque enregistrement perdu ou volé au cours d'une violation de données, selon le Ponemon Institute.[1] En général, plus il y a d'enregistrements perdus ou volés pendant une violation, plus le coût total sera élevé pour l'organisation.

Avec le modèle du moindre privilège, les employés de l'organisation (tout comme ses sous-traitants et consultants) n'ont accès qu'aux données dont ils ont besoin sur le plan professionnel. En limitant l'accès aux données dans l'ensemble de l'organisation, les entreprises sont en mesure de réduire leur exposition à des menaces extérieures en cas de violation d'un compte d'utilisateur. Etre en mesure d'identifier rapidement un incident au moment où il se produit contribue également à réduire encore le risque associé à une violation de données. Pour ces raisons, le client considère la solution Varonis comme une « composante essentielle de la stratégie globale de gestion des risques [de l'organisation] ».

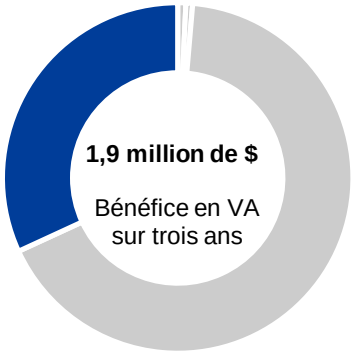
Le modèle financier révèle les constats suivants :

- Au cours d'une année donnée, le client risque, avec une probabilité de 14 %, de subir un incident de sécurité à grande échelle.
- En cas de violation, le nombre moyen de dossiers clients exposés est de 28 512 pour les entreprises américaines.
- Les entreprises de santé supportent un coût moyen de 380 $ pour chaque dossier client exposé en cas de violation.
- En permettant des actions correctives sur l'accès aux fichiers et aux dossiers, Varonis a réduit de 50 % l'exposition de l'organisation cliente à une violation de données.
- En fournissant un mécanisme de détection et de réponse plus rapide, Varonis a réduit de 15 % supplémentaires l'exposition de l'organisation.

Les risques suivants peuvent affecter cette catégorie d'avantages :

- La sophistication des pratiques de sécurité en place avant le déploiement de la solution Varonis.
- Le type de données gérées, qui aura une incidence sur le coût total de son exposition au public.

Pour tenir compte de ces risques, Forrester a appliqué une pondération par rapport au risque de 15 %, ce qui donne une valeur actuelle totale pondérée par le risque de 1 893 648 dollars sur trois ans.



Réduction de l'exposition au risque : **32 %** du total des bénéfices

FORRESTER®

Réduction de l'exposition au risque : tableau de calcul

REF.	MESURE	CALC.	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3
D1	Nombre moyen de documents exposés en cas de violation pour les entreprises américaines	Ponemon		28 512	28 512	28 512
D2	Coût moyen par dossier engagé en cas de vol de données médicales	Ponemon		380 $	380 $	380 $
D3	Coût moyen d'un problème majeur de sécurité des données	D1*D2		10 834 560 $	10 834 560 $	10 834 560 $
D4	Probabilité d'une violation de données au cours d'une année donnée	Ponemon		14 %	14 %	14 %
D5	Réduction de l'exposition à une violation de données par une correction de l'accès partagé global			50 %	50 %	50 %
D6	Réduction de l'exposition à une violation de données grâce à une détection et une réponse améliorées			15 %	15 %	15 %
D7	Réduction totale de l'exposition à une violation de données	D5+D6		65 %	65 %	65 %
D8	Pourcentage de bénéfices réalisés			75 %	100 %	100 %
Dt	Réduction de l'exposition au risque	D3*D4*D7*D8	0 $	739 458,72 $	985 944,96 $	985 944,96 $
	Pondération par rapport au risque	↓15 %				
Dtr	Réduction de l'exposition au risque (pondérée par rapport au risque)		0 $	628 540 $	838 053 $	838 053 $

Flexibilité

La valeur de la flexibilité est propre à chaque client et la mesure de cette valeur varie d'une entreprise à l'autre. Il existe plusieurs scénarios dans lesquels un client peut choisir de mettre en œuvre un ou plusieurs composants de la Plateforme de Sécurité des Données Varonis et se rendre compte ultérieurement des utilisations et opportunités supplémentaires offertes : Les exemples de future valeur attendue mentionnés ci-dessous ont été fournis par le client interrogé par Forrester pour cette étude de cas :

La flexibilité, telle que définie par TEI, représente un investissement dans des capacités supplémentaires ou une capacité susceptible d'être transformée en avantages pour l'entreprise en vue d'un investissement supplémentaire. L'entreprise acquiert ainsi le « droit » ou la capacité de s'engager dans des initiatives à venir, sans y être obligée.

- **Meilleure rétention.** Pour de nombreuses organisations, le fait de conserver trop longtemps des données crée une responsabilité. Pourtant, elles hésitent souvent à déplacer ou à supprimer des données de crainte que cela ait un impact sur l'entreprise. « Grâce à Varonis, nous sommes en mesure d'informer le reste de l'organisation que les fichiers n'ont pas été consultés depuis six mois ou un an, par exemple, et que, puisqu'ils ne sont plus nécessaires, nous pouvons les archiver ou les supprimer », souligne le directeur de la cybersécurité. La suppression d'un fichier réduit le profil de risque de l'organisation, mais son impact ne se limite pas à cela. Comme les données sont répliquées et qu'il existe plusieurs sauvegardes, la suppression d'un fichier source libère les systèmes de stockage primaires et secondaires.
- **Migration de fichiers vers un système de stockage plus économique.** Aujourd'hui, l'organisation cliente développe encore ses stratégies de prévention des pertes de données (DLP) et de classification de données. Mais dès lors qu'elle aura mis en place des règles strictes, elle entend exploiter la solution Data Classification Engine pour identifier des possibilités de migrer ses données vers un système de stockage à moindre coût. Les fichiers volumineux, tels que les MP3 et les vidéos, stockés sur des disques partagés comptent parmi les meilleurs exemples de candidats à la migration, bien qu'il existe de nombreuses opportunités de migration pour tous les types de données, selon les personnes interrogées.
- **Stratégie de classification applicable.** Les documents sensibles de l'organisation cliente sont étiquetés « confidentiels » et « pour usage interne seulement », bien que ces restrictions n'étaient jusqu'à présent que « de simples mots sur un bout de papier », estime le directeur de la cybersécurité. Par la suite, l'organisation projette d'utiliser les solutions Varonis pour créer des stratégies de classification et de partage réalistes et applicables.

La flexibilité est également quantifiée lorsqu'elle est évaluée dans le cadre d'un projet spécifique (voir annexe A).

Analyse des coûts

DONNEES DE COUT QUANTIFIEES

Total des coûts

REF.	COUT	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3	TOTAL	VALEUR ACTUELLE
Etr	Coûts d'achat et de maintenance des logiciels	600 000 $	120 000 $	120 000 $	120 000 $	960 000 $	898 422 $
Ftr	Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis	253 000 $	192 500 $	0 $	0 $	445 500 $	428 000 $
Gtr	Coût de l'effort interne nécessaire pour la planification et le déploiement	5 720 $	0 $	0 $	0 $	5 720 $	5 720 $
	Total des coûts (pondéré par rapport au risque)	858 720 $	312 500 $	120 000 $	120 000 $	1 411 220 $	1 332 142 $

Coûts d'achat et de maintenance des logiciels

Le client a payé un prix forfaitaire pour obtenir une licence sur les produits logiciels Varonis ; il paie également des frais de maintenance annuels équivalant à 20 % du prix d'achat initial.

Au début, le client a dépensé 600 000 $ au total pour obtenir la licence du produit de base DatAdvantage et des modules complémentaires UNIX, SharePoint, Exchange et Directory Services, ainsi que DatAlert, DataPrivilege et le Classification Engine. Au cours de chaque année suivante, le client a payé des frais de maintenance d'un montant de 120 000 $ pour bénéficier d'un accès ininterrompu aux mises à jour logicielles, aux correctifs, au support technique et à la communauté Varonis Connect.

Forrester n'a appliqué aucune pondération par rapport au risque au coût des produits logiciels et aux coûts de maintenance puisque Varonis a communiqué à Forrester ces informations, qui ont été confirmées par le client. Ces coûts sont représentatifs de ceux que d'autres organisations peuvent s'attendre à engager pour une configuration semblable de produits.

Le coût total des logiciels et de la maintenance en valeur actuelle sur trois ans est de 898 422 $.

Le tableau ci-dessus montre le total de tous les coûts dans les domaines énumérés ci-dessous, ainsi que les valeurs actuelles (VA) minorées de 10 %. Sur une période de trois ans, l'entreprise interrogée s'attend à un coût total de la valeur actuelle pondérée par le risque de plus de 1,3 million de dollars.

Le risque de la mise en œuvre correspond au risque qu'un projet d'investissement s'écarte des besoins initiaux ou attendus, résultant en des coûts plus élevés que prévu. Plus l'incertitude est importante, plus les résultats peuvent différer des estimations de coûts.

Coûts d'achat et de maintenance des logiciels : tableau de calcul						
REF.	**MESURE**	**CALC.**	**INITIAL**	**ANNEE 1**	**ANNEE 2**	**ANNEE 3**
E1	Coûts logiciels		600 000 $	0 $	0 $	0 $
E2	Frais de maintenance en pourcentage du prix d'achat initial		0 $	120 000 $	120 000 $	120 000 $
Et	Coûts d'achat et de maintenance des logiciels	E1+E2	600 000 $	120 000 $	120 000 $	120 000 $
	Pondération par rapport au risque	0 %				
Etr	Coûts d'achat et de maintenance des logiciels (pondérés en fonction des risques)		600 000 $	120 000 $	120 000 $	120 000 $

L'organisation interrogée a acheté une suite de produits Varonis plus complète que ce qu'achètent au départ la plupart des entreprises. Cet investissement s'est traduit par de plus grands bénéfices sur la période de trois ans d'analyse, mais a également entraîné des coûts plus élevés. Un client type aura tendance à investir dans les composants suivants de la plateforme au début d'une collaboration avec Varonis :

- DatAdvantage pour un seul dépôt de données (par ex., Windows ou Office 365).
- DatAlert Suite.
- Data Classification Engine.

Cet investissement permettra de fournir un accès à diverses fonctionnalités, comme la gestion des autorisations, l'analyse de fichiers, la détection des menaces, l'analyse du comportement des utilisateurs, la détection des données sensibles et les rapports de conformité, pour un coût d'environ 155 000 $, sur une base d'environ 1 000 utilisateurs surveillés.

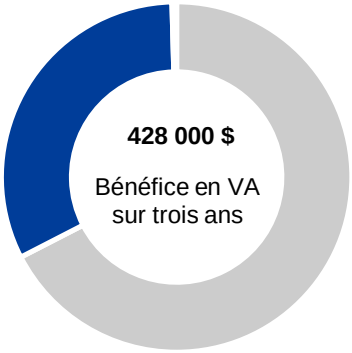
Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis

Le client a engagé des coûts pour la mise en œuvre et l'opérationnalisation de la Plateforme de Sécurité des Données Varonis, ainsi que pour la correction initiale de ses systèmes de fichiers.

Au vu des défis uniques que présentait son environnement, le client a décidé de confier à l'équipe Professional Services de Varonis l'essentiel des travaux de mise en œuvre. Il a choisi de travailler directement avec Varonis, plutôt qu'avec un intégrateur de systèmes tiers, en raison de son expertise.

Dans le cadre de la phase initiale de mise en œuvre et d'opérationnalisation de la solution, l'équipe Professional Services de Varonis a examiné les données non structurées du client et ses services d'annuaire avant de dispenser une formation au personnel du client.

Cette catégorie de coûts comprend également la correction du problème lié à l'accès aux fichiers et dossiers partagés, un effort mené par l'équipe Professional Services de Varonis.



Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis : **32 %** du coût total

FORRESTER®

- La correction a porté dans un premier temps sur 850 000 dossiers à risque élevé.
- Au cours de la première année, elle s'est étendue à 650 000 dossiers à risque élevé supplémentaires.

Forrester a pondéré de 10 % à la hausse les frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis, afin de tenir compte de la variabilité qui peut être observée entre les différentes organisations selon les facteurs suivants :

- La complexité du déploiement.
- La taille et l'état des systèmes de fichiers avant le déploiement de la solution Varonis.

Ce réajustement a donné lieu à un coût total en valeur actuelle sur trois ans de 428 000 $.

Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis : tableau de calcul

REF.	MESURE	CALC.	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3
F1	Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis		230 000 $	175 000 $	0 $	0 $
Ft	Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis		230 000 $	175 000 $	0 $	0 $
	Pondération par rapport au risque	↑10 %				
Ftr	Frais de mise en œuvre, d'opérationnalisation et de correction versés à Varonis (pondérés par rapport au risque)		253 000 $	192 500 $	0 $	0 $

Coût de l'effort interne nécessaire pour la planification et le déploiement

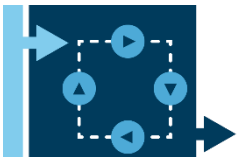
Le client a également engagé des coûts pour les ressources internes qu'il a consacrées au processus de planification et de mise en œuvre.

Cette phase de planification et de mise en œuvre s'est déroulée sur plus d'un mois, bien qu'une grande partie de ce temps ait été consacrée à la socialisation des plans autour du déploiement de la solution Varonis et à l'effort nécessaire pour s'assurer qu'ils étaient bien compris. Personne ne s'est consacré à plein temps à cette initiative : les activités de prédéploiement ont nécessité l'engagement de deux analystes en sécurité à hauteur de 25 % (ou 10 heures par semaine) ainsi que l'engagement d'un gestionnaire de projet expert dans ce domaine à hauteur de 15 % (ou 6 heures par semaine). Sur le marché régional du client, ces employés sont rémunérés au taux annuel de 50 $ par heure à temps plein.

Forrester a pondéré de 10 % à la hausse le coût associé à l'effort de planification et de mise en œuvre en interne, afin de tenir compte de la variabilité qui peut être observée entre les différentes organisations selon les facteurs suivants :

- La complexité du déploiement.
- Le niveau d'expertise nécessaire pour déployer la solution.

Ce réajustement a donné lieu à un coût total en valeur actuelle sur trois ans de 5 720 $.



La phase de planification et de mise en œuvre s'est déroulée sur plus d'un mois, bien qu'une grande partie de ce temps ait été consacrée à la socialisation des plans autour du déploiement.

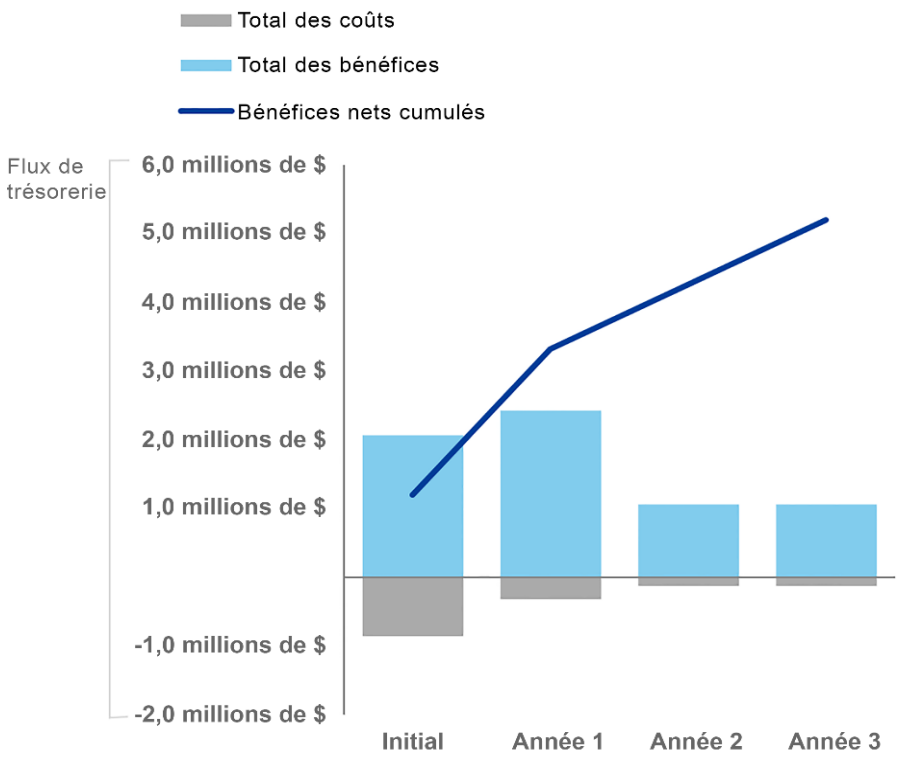
FORRESTER®

Coût de l'effort interne nécessaire pour la planification et le déploiement : tableau de calcul						
REF.	**MESURE**	**CALC.**	**INITIAL**	**ANNEE 1**	**ANNEE 2**	**ANNEE 3**
G1	Taux horaire d'un analyste en sécurité à temps plein		50 $			
G2	Analystes en sécurité dédiés à la planification et à la mise en œuvre		2			
G3	Engagement hebdomadaire par analyste	Heures	10			
G4	Taux horaire d'un responsable de projets informatiques à temps plein		50 $			
G5	Engagement hebdomadaire du responsable de projets		6			
G6	Nombre de semaines entre la planification et le déploiement		4			
Gt	Coût de l'effort interne nécessaire pour la planification et le déploiement	((G1*G2*G3)+ (G4*G5))*G6	5 200 $	0 $	0 $	0 $
	Pondération par rapport au risque	↑10 %				
Gtr	Coût de l'effort interne nécessaire pour la planification et le déploiement (pondéré par rapport au risque)		5 720 $	0 $	0 $	0 $

Résumé financier

MESURES CONSOLIDEES SUR TROIS ANS PONDEREES PAR RAPPORT AU RISQUE

Graphique du flux de trésorerie (pondéré par rapport au risque)



Les résultats financiers calculés dans les sections Avantages et Coûts peuvent être utilisés pour déterminer le retour sur investissement, la valeur actuelle nette et la période de récupération de l'investissement de l'organisation interrogée. Forrester suppose un taux d'actualisation annuel de 10 % pour cette analyse.

Ces valeurs de retour sur investissement, valeur actuelle nette et période de récupération de l'investissement sont déterminées en appliquant les facteurs d'ajustement du risque aux résultats non ajustés dans chaque section sur les avantages et les coûts.

Tableau du flux de trésorerie (pondéré par rapport au risque)

	INITIAL	ANNEE 1	ANNEE 2	ANNEE 3	TOTAL	VALEUR ACTUELLE
Total des coûts	(858 720 $)	(312 500 $)	(120 000 $)	(120 000 $)	(1 411 220 $)	(1 332 142 $)
Bénéfice total	2 065 500 $	2 427 979 $	1 057 993 $	1 057 993 $	6 609 464 $	5 942 014 $
Bénéfices nets	1 206 780 $	2 115 479 $	937 993 $	937 993 $	5 198 244 $	4 609 872 $
ROI						346 %
Période de récupération						< 6 mois

FORRESTER®

Annexe A : Total Economic Impact

Total Economic Impact est une méthodologie développée par Forrester Research qui améliore les processus de prise de décisions technologiques de l'entreprise et aide les fournisseurs dans la communication de la proposition de valeur de leurs produits et services aux clients. La méthodologie TEI permet aux entreprises de démontrer, justifier et réaliser la valeur tangible des initiatives informatiques aux yeux de la direction et des autres parties prenantes essentielles de l'organisation.

Approche Total Economic Impact

Les avantages représentent la valeur fournie à l'entreprise par le produit. La méthodologie TEI accorde autant d'importance à la mesure des avantages et à la mesure des coûts, permettant un examen complet de l'incidence de la technologie sur l'ensemble de l'entreprise.

Les coûts représentent l'ensemble des dépenses nécessaires pour fournir la valeur proposée, ou avantages, du produit. La catégorie Coût du TEI capture les coûts différentiels sur l'environnement existant pour les coûts actuels associés à la solution.

La flexibilité représente la valeur stratégique qui peut être obtenue pour des investissements supplémentaires à venir en s'appuyant sur l'investissement initial déjà réalisé. Le fait d'être capable de capturer cet avantage a une valeur actuelle qui peut être estimée.

Les risques mesurent l'incertitude des estimations de bénéfices et de coûts fournies : 1) la probabilité que les estimations correspondent aux prévisions initiales et 2) la probabilité que les estimations seront suivies dans le temps. Les facteurs de risque TEI sont basés sur une « distribution triangulaire ».

La colonne d'investissement initial contient les coûts engagés à « temps 0 » ou au début de l'année 1 qui ne sont pas actualisés. Tous les autres flux de trésorerie sont actualisés en utilisant le taux d'actualisation à la fin de l'année. Les calculs de la valeur actuelle sont calculés pour chaque estimation d'avantages et de coûts totaux. Les calculs de la valeur actuelle nette dans les tableaux récapitulatifs sont la somme de l'investissement initial et de la valeur actualisée des flux de trésorerie de chaque année. Les sommes et les calculs de la valeur actuelle des tableaux des avantages totaux, des coûts totaux et des tableaux des flux de trésorerie peuvent ne pas s'additionner exactement, car certains arrondis peuvent se produire.

Valeur actuelle (VA)

Valeur actuelle des estimations d'avantages et de coûts (actualisées) à laquelle est appliqué un taux d'intérêt (le taux d'actualisation). La valeur nette des coûts et des avantages se répercute sur la valeur actuelle totale des flux de trésorerie.

Valeur actuelle nette (VAN)

Valeur actuelle des flux de trésorerie nets futurs (actualisés) tenant compte d'un taux d'intérêt (le taux d'actualisation). Une VAN positive pour un projet indique normalement que l'investissement devrait être réalisé, à moins que d'autres projets n'aient des VAN plus élevées.

Retour sur investissement (ROI)

Le rendement attendu d'un projet (en pourcentage). Le ROI se calcule en divisant les bénéfices nets (bénéfices moins coûts) par les coûts.

Taux d'actualisation

Taux d'intérêt utilisé dans l'analyse des flux de trésorerie pour tenir compte de la valeur temporelle de l'argent. Les entreprises utilisent généralement des taux d'actualisation compris entre 8 % et 16 %.

Période de récupération

Le seuil de rentabilité d'un investissement. Il s'agit du moment où les bénéfices nets (bénéfices moins coûts) se retrouvent à l'équilibre avec l'investissement initial ou le coût initial.

FORRESTER®

Notes de fin

[1] Source : « 2017 Cost of Data Breach: Global Overview », Ponemon Institute, 13 juin 2017 (https://www.ponemon.org/library/2017-cost-of-data-breach-study-united-states).