Étude Total Economic Impact™ réalisée par Forrester pour le compte d'IBM

Directrice du projet : Adrienne Capaldo
Septembre 2015

Étude Total Economic Impact™ d'IBM Security Guardium

La sécurité des données présente un problème complexe pour les entreprises. Non seulement elle leur pose une vraie question, mais les clients sont de plus en plus sensibles à la sécurité de leurs données. Les données clients n'ont cessé de prendre de la valeur au fil du temps, ce qui s'est accompagné en parallèle d'une augmentation des risques et de l'exposition. Si l'on ajoute à cela la croissance rapide de ces données dans les environnements professionnels, la complexité des réglementations et des règles de conformité dans tous les secteurs et la menace d'attaques internes et externes, on comprendra à quel point il est important de mettre en place une stratégie de sécurité et de conformité performante. Par ailleurs, les entreprises ont du mal à voir comment surveiller et contrôler de façon proactive les droits d'accès de leurs utilisateurs et n'identifient souvent pas clairement les données potentiellement menacées. Tout cela peut entraîner des menaces sur la sécurité potentiellement dévastatrices.

IBM a chargé Forrester Consulting de réaliser une étude Total Economic Impact™ (TEI) et de calculer le retour sur investissement (RSI) que les entreprises peuvent espérer obtenir en déployant IBM Security Guardium dans le cadre d'une stratégie globale de sécurité des données et de respect des règles de conformité. L'objet de cette étude est de mettre à la disposition des lecteurs un cadre qui leur permette d'évaluer l'incidence financière potentielle de Guardium sur leur entreprise.

Pour mieux comprendre les avantages, les coûts et les risques liés à la mise en œuvre de Guardium, Forrester a réalisé une enquête et des entretiens auprès de plusieurs clients utilisant la solution depuis plusieurs années. IBM Security Guardium est une gamme de modules intégrés permettant de gérer tout le cycle de vie de la sécurité des données et de la conformité. Ces modules s'appuient sur une infrastructure et une expérience utilisateur unifiées. Guardium a pour objectif de soutenir et de sécuriser un large éventail d'environnement de données, qu'il s'agisse de bases de données, d'entrepôts de données, de systèmes de fichiers ou de systèmes virtuels de big data en ligne.

Nos entretiens et l'analyse financière corollaire ont déterminé qu'une entreprise composite présentait le RSI, les bénéfices et les coûts ajustés en fonction des risques répertoriés ci-dessous.

PRINCIPALES CONCLUSIONS : IBM SECURITY GUARDIUM SÉCURISE EFFICACEMENT LES DONNÉES SENSIBLES DES ENTREPRISES ET LIMITE LES RISQUES

RSI : 218 %	**VAN : 1,8 million d'USD**	**Amortissement : 7,4 mois**

MÉTHODOLOGIE

IBM a chargé Forrester Consulting de réaliser une étude Total Economic Impact™ (TEI) et d'examiner le retour sur investissement potentiel (RSI) que les entreprises peuvent obtenir en déployant Guardium dans le cadre de leur stratégie globale de sécurité des données et de respect des règles de conformité. Pour cela, Forrester a réalisé une enquête auprès de trois grandes entreprises qui utilisent IBM Guardium,

puis conçu une entreprise composite fondée sur les caractéristiques de ces trois entreprises. Un modèle financier représentatif a ensuite été élaboré à l'aide de la méthodologie TEI.

Enfin, Forrester a procédé à un ajustement du modèle financier en fonction des risques, en s'appuyant sur les problèmes et préoccupations soulignés lors de l'enquête. Certaines catégories de coûts et d'avantages entraînaient en effet un large éventail de réponses ou dépendaient d'un certain nombre de facteurs externes susceptibles d'influer sur les résultats. C'est pourquoi certains totaux de coûts et d'avantages ont été ajustés en fonction des risques. Les valeurs obtenues sont détaillées dans les paragraphes concernés.

Pourquoi Guardium ?

Forrester a demandé aux entreprises concernées de décrire les difficultés qu'elles rencontraient en matière de sécurité des données. Les entretiens ont fait apparaître un certain nombre de facteurs communs poussant les entreprises à investir dans la sécurité de leurs données, notamment les suivants :

- Le besoin de respecter les réglementations et les exigences de conformité
- La nécessité d'améliorer la sécurité des données et la conformité pour les projets de big data, tels que Hadoop, NoSQL ou les données en mémoire.
- Le souci d'une stratégie de sécurité, de conformité et de confidentialité des données qui est progressivement devenu plus aigu dans les entreprises.
- Une envie d'être désormais plus proactif que réactif dans les stratégies de sécurité des données et de conformité.
- L'échec d'audits précédents, ce que l'entreprise ne souhaite pas voir se reproduire.

Avant d'investir dans Guardium, ces entreprises géraient la sécurité des données et la conformité de façon disparate à l'aide d'un patchwork d'outils divers, de solutions développées en interne et de processus manuels. Cette façon de faire était souvent jugée inefficace et ne semblait pas pouvoir répondre aux besoins de sécurité et de conformité d'aujourd'hui. Chacune des entreprises interrogées a choisi Guardium de préférence à des produits concurrents. Au cours des entretiens, elles ont expliqué leur choix de la façon suivante :

- **Guardium a aidé les entreprises à répondre à leurs besoins de reporting et d'audit en matière de conformité.** La solution les a en outre aidées à surveiller les utilisateurs disposant de privilèges et à bloquer les accès non autorisés. Guardium fonctionne également dans un grand nombre d'environnements différents, notamment un large éventail de plateformes, de bases et d'entrepôts de données, de systèmes Hadoop ou de big data, de référentiels, de fichiers, d'applications et de protocoles.
- **Guardium améliore la visibilité des données sensibles d'une façon que les environnements précédents ne pouvaient pas offrir.** Les entreprises ont indiqué que Guardium les aidait à voir plus précisément leurs données sensibles, à mieux les détecter, les comprendre et les classer. Nous avons constaté que ces entreprises n'étaient parfois pas conscientes de toutes leurs données sensibles et que Guardium les avait aidées à découvrir de nouvelles sources de risques. À mesure qu'elles abordent davantage de projets de big data, dans lesquels les dangers pesant sur la sécurité des données sont décuplés, il est de plus en plus important pour elles de savoir où se trouvent leurs données sensibles. Guardium les a également aidées à mieux comprendre leurs données, ce qui leur a permis de prendre des décisions plus pertinentes et plus efficaces que jamais pour les sécuriser.
- **Guardium aide les entreprises à sécuriser et à protéger leurs données sensibles sur tout leur environnement.** Non seulement Guardium aide les entreprises à mieux voir leurs données sensibles, mais il contribue également à protéger et à sécuriser ces données en temps réel. Guardium surveille et contrôle en permanence l'accès à tout l'environnement de l'entreprise et sécurise des référentiels tels que les bases ou les entrepôts de données, Hadoop, NoSQL, les systèmes en mémoire et les partages de fichiers.
- **IBM est un leader reconnu de la sécurité des données et de la conformité.** Il est apparu aux entreprises que travailler avec un partenaire de poids dans ce secteur créait un environnement rassurant. En outre, l'évolutivité de la solution lui permet d'accompagner des environnements de tailles différentes et sa dimension non invasive ne peut certes pas nuire aux performances des bases ou des entrepôts de données professionnels. En investissant dans Guardium, ces entreprises ont pu simplifier leur fonctionnement tout en améliorant la qualité de leur stratégie de sécurité des données.

Analyse

À partir de nos entretiens, Forrester a élaboré un cadre TEI, une entreprise composite, ainsi qu'une analyse du RSI présentant les domaines concernés sur le plan financier. L'entreprise composite que Forrester a synthétisée à partir de ces résultats possède les caractéristiques suivantes :

- L'entreprise est une société américaine de services financiers employant 20 000 personnes et affichant plus d'un milliard d'USD de chiffre d'affaires annuel.
- Elle a besoin de capacités de sécurité et d'audit pour que ses bases de données respectent efficacement les obligations d'audit exigées par la loi Sarbanes-Oxley et la norme PCI DSS, et pour protéger la confidentialité des données. Toutes les tentatives d'accès à des données financières doivent être journalisées et les demandes d'accès douteuses doivent être analysées pour vérifier leur conformité aux règles définies. Tout le trafic réseau et local est surveillé par le système Guardium.
- L'entreprise possède un environnement de bases de données vaste et hétérogène. Elle gère actuellement environ 8 000 bases de données auxquelles accèdent un certain nombre d'applications d'entreprise. La taille de ces bases de données varie de 100 Go à 1 To selon le type de données stockées et leur rythme de croissance annuel. Pour ses serveurs, elle utilise des machines IBM System x86.
- L'entreprise a fait l'acquisition de la solution Guardium afin de surveiller tous les accès et les changements touchant les serveurs de bases de données sensibles concernés par les règles de SOX, PCI DSS et de confidentialité des données. Le fait que Guardium couvre une large diversité de bases de données et d'applications a donné à l'entreprise l'assurance de pouvoir déployer partout la même solution.

Avantages

Grâce à son investissement dans Guardium, l'entreprise composite a bénéficié d'un certain nombre d'avantages quantifiés :

- Gains d'efficacité au niveau des processus de respect des exigences de sécurité et de conformité
- Réduction des coûts de restauration en cas de violation de données
- Réduction du risque d'amende pour infraction aux réglementations
- Coûts de main-d'œuvre pour développer des capacités internes de surveillance et d'audit évités
- Coût de main-d'œuvre pour le support régulier de solutions internes de surveillance et d'audit évités

GAINS D'EFFICACITE DES PROCESSUS DE RESPECT DES EXIGENCES DE SECURITE ET DE CONFORMITE

Notre premier avantage concerne la capacité d'améliorer l'efficacité des processus de respect des exigences de sécurité et de conformité. En installant Guardium, l'entreprise représentative a pu améliorer et automatiser la sécurité de ses bases de données, ainsi que ses protocoles d'audits et ses capacités de création de rapports. Son personnel s'est ainsi trouvé en mesure de gérer plus rapidement les exigences de sécurité. Le processus est rationalisé grâce à des contrôles automatisés et centralisés et à des processus simplifiés de consultation des audits, ce qui réduit la durée et le coût de la mise en conformité. Guardium aide des professionnels tels que les administrateurs de bases de données (ABD), les spécialistes de la confidentialité des données ou les responsables d'audits à être plus efficaces et à économiser les ressources financières de l'entreprise.

Pour calculer les gains d'efficacité des processus de respect de la sécurité et les exigences, nous estimons que 45 ABD et cinq autres professionnels parmi les postes mentionnés ci-dessus sont concernés par les exigences de sécurité et de conformité. Nous supposons que ces ABD consacrent en moyenne 40 % de leur temps aux problèmes de sécurité et de conformité, tandis que les autres employés passent en moyenne 20 % du leur à gérer des processus de respect des réglementations et des exigences de sécurité. Nous constatons qu'en mettant en place Guardium, l'entreprise parvient à limiter cette durée de 10 % dès la première année. À mesure que le temps passe, les membres de l'équipe maîtrisent de mieux en mieux la solution et, la troisième année, la réduction du temps passé sur les obligations de sécurité atteint 20 %. Forrester ajuste également les gains de productivité en supposant que 50 % seulement du temps économisé correspond à un travail productif. Le tableau 1 montre comment cela a été calculé.

Il existe un certain nombre de facteurs qui peuvent avoir une incidence sur la capacité de l'équipe à réduire le temps qu'elle consacre aux exigences de sécurité. Pour compenser les écarts entraînés par ces facteurs, Forrester a réduit de 10 % la valeur de ce bénéfice. L'avantage total ajusté en fonction des risques est de 390 242 USD sur trois ans en valeur actuelle.

Forrester conseille vivement au lecteur de prendre en compte l'impact considérable que ces gains d'efficacité peuvent avoir lorsqu'il s'agit d'assurer la sécurité et la conformité de projets de big data, bien que nous ne calculions pas ces gains directement ici.

Tableau 1
Gains d'efficacité des processus de respect des exigences de sécurité et de conformité

Réf.	Critère	Calcul	1re année	2e année	3e année
A1	Nombre d'ABD		45	45	45
A2	Autres employés concernés par la sécurité et la conformité		5	5	5
A3	Pourcentage de temps consacré par les ABD aux questions de sécurité et de conformité		40 %	40 %	40 %
A4	Pourcentage de temps consacré par les autres employés aux questions de sécurité et de conformité		20 %	20 %	20 %
A5	Salaire annuel moyen		125 000 USD	125 000 USD	125 000 USD
A6	Pourcentage de réduction du temps consacré aux exigences de sécurité et de conformité avec IBM Guardium		10 %	15 %	20 %
A7	Pourcentage récupéré		50 %	50 %	50 %
At	Gains d'efficacité au niveau des processus de respect des exigences de sécurité et de conformité	((A1*A3)+(A2*A4)) *A5*A6*A7	118 750 USD	178 125 USD	237 500 USD
	Ajustement en fonction des risques	🡻 10 %			
Atr	**Gains d'efficacité au niveau des processus de respect des exigences de sécurité et de conformité (ajustés en fonction des risques)**		**106 875 USD**	**160 313 USD**	**213 750 USD**

Source : Forrester Research, Inc.

REDUCTION DES COUTS DE RESTAURATION EN CAS DE VIOLATION DE DONNEES

En investissant dans Guardium, notre entreprise représentative a rendu plus efficaces ses capacités liées à la sécurité, à l'audit et au reporting de ses bases de données, ce qui renforce la conformité. En outre, elle est désormais capable de surveiller l'activité des utilisateurs afin de détecter et de contrer les menaces potentielles en temps réel. Avec Guardium, elle identifie et isole plus facilement les menaces internes et externes grâce à des capacités de surveillance, d'audit, de gestion des vulnérabilités, de transformation des données, à des règles de sécurité en temps réel et à la création de rapports intelligents.

Cela lui permet aussi d'éviter les coûts potentiellement élevés qu'entraînerait une violation de ses données. Nous estimons que la probabilité d'une violation de données est d'environ 12 % quelle que soit l'année. Si le coût réel d'une violation de données peut être astronomique, Forrester estime que son coût moyen potentiel pour notre entreprise représentative est d'environ 3 millions de dollars (estimation par défaut), quelle que soit l'année. Cela comprend le coût de la détection, les frais juridiques, les frais d'enquête et les dépenses administratives, ainsi que le coût de l'aide aux clients et la perte de chiffre d'affaires liée à la défection de la clientèle, entre autres dépenses. Grâce aux caractéristiques et aux fonctionnalités de Guardium, l'entreprise peut désormais réduire sensiblement ces risques de violation de données. À mesure que l'équipe de sécurité se perfectionne dans les processus d'analyse des données, ce risque diminue d'année en année. La 3e année, l'entreprise constate qu'il a diminué de 45 %.

Il existe un certain nombre de facteurs externes capables d'influer sur les coûts induits par une violation de données ou sur la réduction du risque de violation. Pour tenir compte ces facteurs, Forrester a réduit de 10 % la valeur de ce bénéfice. Cela se traduit par un bénéfice total ajusté en fonction des risques de 276 897 USD en valeur actuelle. Le tableau 2 illustre ce calcul.

Forrester a choisi de calculer ce bénéfice de façon prudente : grâce aux fonctions de sécurité et de surveillance en temps réel de Guardium, IBM peut aider à protéger proactivement les données et à supprimer les violations. Forrester invite instamment les lecteurs à en tenir compte pour évaluer l'impact global de Guardium sur leur environnement. Il faut en outre envisager l'impact qu'une violation pourrait avoir sur un projet de big data : si une quantité de données bien supérieure est concernée, une telle violation peut devenir d'autant plus dangereuse et coûteuse pour une entreprise.

Tableau 2
Réduction des coûts de restauration en cas de violation de données

Réf.	Critère	Calcul	1re année	2e année	3e année
B1	Coût moyen d'une violation de données		3 000 000 USD	3 000 000 USD	3 000 000 USD
B2	Probabilité d'une violation de données		12 %	12 %	12 %
B3	Réduction de la probabilité d'une violation avec IBM Guardium		25 %	35 %	45 %
Bt	Réduction des coûts de restauration en cas de violation de données	B1*B2*B3	90 000 USD	126 000 USD	162 000 USD
	Ajustement en fonction des risques	🡻 10 %			
Btr	**Réduction des coûts de restauration en cas de violation de données (ajustée en fonction des risques)**		**81 000 USD**	**113 400 USD**	**145 800 USD**

Source : Forrester Research, Inc.

REDUCTION DU RISQUE D'AMENDE POUR INFRACTION AUX REGLEMENTATIONS

Outre le coût qu'entraînent les violations de données, il existe un risque important de se voir infliger une amende par un tribunal ou un autre organisme réglementaire pour non-respect des réglementations. L'investissement dans Guardium a permis à notre entreprise représentative de bénéficier de gains d'efficacité grâce à l'automatisation de tous ses processus d'audit de la conformité.

Elle est ainsi parvenue à réduire le risque de se voir infliger des amendes. Pour calculer ce risque, nous évalué ce que pourrait coûter une amende. Bien qu'il soit difficile d'en prévoir le coût réel, Forrester estime par prudence qu'elle pourrait s'élever à 25 millions d'USD chaque année en l'absence de mesures adéquates pour prouver la conformité. En investissant dans Guardium, l'entreprise représentative est mieux à même de satisfaire à ses exigences de sécurité et réduit ainsi à 2 % le risque d'amende. C'est ce que montrent les calculs du tableau 3. Forrester sait toutefois qu'un certain nombre de facteurs peuvent influer sur ce calcul. Pour tenir compte de cette incertitude, nous avons diminué de 15 % le bénéfice en fonction des risques, ce qui nous donne un montant de 1 056 912 USD sur trois ans en valeur actuelle.

Si l'on envisage les risques d'amende réglementaire dans le cadre des big data, nous pouvons voir que le coût ou la probabilité d'une amende risque d'augmenter. Bien que ce calcul ne soit pas effectué ici, l'utilisation de Guardium aide les entreprises à réduire ce risque.

Tableau 3
Réduction du risque d'amende pour infraction aux réglementations

Réf.	Critère	Calcul	1re année	2e année	3e année
C1	Amende réglementaire potentielle moyenne		25 000 000 USD	25 000 000 USD	25 000 000 USD
C2	Risque d'amende		2 %	2 %	2 %
Ct	Réduction du risque d'amende pour infraction aux réglementations	C1*C2	500 000 USD	500 000 USD	500 000 USD
	Ajustement en fonction des risques	🡻 15 %			
Ctr	**Réduction du risque d'amende pour infraction aux réglementations (ajustée en fonction des risques)**		**425 000 USD**	**425 000 USD**	**425 000 USD**

Source : Forrester Research, Inc.

COUTS DE MAIN-D'ŒUVRE POUR DEVELOPPER DES CAPACITES INTERNES DE SURVEILLANCE ET D'AUDIT EVITES

En investissant dans Guardium, l'entreprise composite a évité les coûts de développement d'une autre solution. « L'autre option » utilisée pour cette comparaison est basée sur les capacités natives de journalisation offertes par les plateformes de bases de données pour enregistrer et stocker les journaux d'audit. Pour analyser et consigner ces informations, l'entreprise devrait développer des logiciels et des scripts nouveaux en interne, puis diffuser les rapports aux responsables des audits et aux autres intervenants chargés de la supervision. Il faut cependant noter que la solution maison ne fournirait pas les contrôles de sécurité en temps réel qu'offre Guardium puisque les utilitaires de journalisation fonctionneraient alors par lots. Elle ne pourrait pas non plus assurer le même niveau de fonctionnalités et d'analyse automatiques.

Pour développer une solution de remplacement telle qu'une solution manuelle interne de surveillance et d'audit des bases de données, l'organisation composite devrait affecter trois ressources sur huit semaines, soit 960 heures-hommes, pour développer, tester et déployer la fonctionnalité requise pour journaliser, stocker, analyser et consigner de façon sécurisée les informations d'accès aux outils de base de données. Au bout de deux ans, il lui faudrait fournir un nouvel effort pour actualiser la solution et y consacrer la moitié de l'investissement initial, soit 480 heures-hommes. Le tableau 4 présente ce calcul.

Un certain nombre de facteurs peuvent peser sur la capacité de l'équipe à développer une telle solution. Pour compenser les écarts entraînés par ces facteurs, Forrester a réduit de 10 % la valeur de ce bénéfice. Les économies réalisées au total sur trois ans s'élèvent à 73 261 USD en valeur actuelle, ajustés en fonction des risques.

Tableau 4
Coûts de main-d'œuvre pour développer des capacités internes de surveillance et d'audit évités

Réf.	Critère	Calcul	Période initiale	1re année	2e année
D1	Heures-hommes nécessaires pour créer des capacités internes de surveillance et d'audit	8 semaines * 3 resources	960		480
D2	Salaire horaire moyen		60 USD		60 USD
Dt	Coûts de main-d'œuvre pour développer des capacités internes de surveillance et d'audit évités	D1*D2	57 600 USD		28 800 USD
	Ajustement en fonction des risques	🡻 10 %			
d'œuvre	**Coûts de main-d'œuvre évités pour développer des capacités internes de surveillance et d'audit (ajustés en fonction des risques)**		**51 840 USD**	**0 USD**	**25 920 USD**

Source : Forrester Research, Inc.

COUT DE MAIN-D'ŒUVRE POUR LE SUPPORT REGULIER DE SOLUTIONS INTERNES DE SURVEILLANCE ET D'AUDIT EVITES

Outre la main-d'œuvre nécessaire pour développer la solution, l'organisation composite aurait besoin de trois ressources pour assurer son entretien régulier. La première ressource serait un ABD chargé d'assurer le support régulier de la base de données pour le stockage et l'analyse des données de journalisation et d'audit. Il devrait également rédiger les rapports sur tous les accès par les ABD aux bases de données. Les deux autres ressources de support régulier seraient deux spécialistes du support aux applications. Ces professionnels seraient responsables des audits et des rapports permanents concernant tous les accès aux bases de données autres que ceux des ABD (applications et super-utilisateurs non-ABD). Ils devraient aussi se charger des diagnostics, des dépannages et de l'amélioration des performances des bases de données, autant d'activités de support actuellement assurées par le système Guardium.

On suppose que ces trois ressources reçoivent un salaire moyen de 125 000 USD, charges comprises. Le tableau 5 illustre le calcul. Les économies réalisées au total sur trois ans s'élèvent à 839 313 USD en valeur actuelle, ajustés en fonction des risques.

Là encore, pour compenser l'effet de facteurs susceptibles de modifier ce calcul, Forrester a appliqué une réduction de 10 % à ce bénéfice.

Tableau 5
Coût de main-d'œuvre pour le support régulier de solutions internes de surveillance et d'audit évités

Réf.	Critère	Calcul	1re année	2e année	3e année
E1	Équivalents temps plein évités		3	3	3
E2	Salaire annuel moyen		125 000 USD	125 000 USD	125 000 USD
Et	Coût de main-d'œuvre pour le support régulier de solutions internes de surveillance et d'audit évités	E1*E2	375 000 USD	375 000 USD	375 000 USD
	Ajustement en fonction des risques	🡻 10 %			
Etr	**Coût de main-d'œuvre pour le support régulier de solutions internes de surveillance et d'audit évités (ajustés en fonction des risques)**		**337 500 USD**	**337 500 USD**	**337 500 USD**

Source : Forrester Research, Inc.

BENEFICES TOTAUX

La somme totale des bénéfices quantifiés, ainsi que les valeurs actuelles (VA) associées, avec un taux d'actualisation de 10 %, figure dans le tableau ci-dessous. Sur trois ans, l'entreprise composite escompte un avantage total ajusté en fonction des risques (VA) de 2,6 millions de dollars.

Tableau 6
Avantages totaux en termes de flux de trésorerie (estimations ajustées aux risques)

Réf.	Catégorie d'avantages	Période initiale	1re année	2e année	3e année	Total	Valeur actuelle
Atr	Gains d'efficacité des processus de respect des exigences de sécurité et de conformité	0 USD	106 875 USD	160 313 USD	213 750 USD	480 938 USD	390 242 USD
Btr	Réduction des coûts de restauration en cas de violation de données	0 USD	81 000 USD	113 400 USD	145 800 USD	340 200 USD	276 897 USD
Ctr	Réduction du risque d'amende pour infraction aux réglementations	0 USD	425 000 USD	425 000 USD	425 000 USD	1 275 000 USD	1 056 912 USD
d'œuvre	Coûts de main-d'œuvre pour développer des capacités internes de surveillance et d'audit évités	51 840 USD	0 USD	25 920 USD	0 USD	77 760 USD	73 261 USD

Etr	Coût de main-d'œuvre pour le support régulier de solutions internes de surveillance et d'audit évités	0 USD	337 500 USD	337 500 USD	337 500 USD	1 012 500 USD	839 313 USD
	Avantages totaux (ajustés en fonction des risques)	**51 840 USD**	**950 375 USD**	**1 062 133 USD**	**1 122 050 USD**	**3 186 398 USD**	**2 636 625 USD**

Source : Forrester Research, Inc.

Coûts

L'entreprise composite a dû gérer certains coûts associés à l'utilisation de la solution Guardium :

- Coûts initiaux et maintenance annuelle de Guardium.
- Planification, mise en œuvre et services professionnels.

Ces postes représentent l'ensemble des coûts internes et externes associés à la solution rencontrés par l'entreprise composite lors de la planification initiale, de la mise en œuvre et de la maintenance courante.

COUTS TOTAUX

La somme totale des coûts, ainsi que les valeurs actuelles (VA) associées, avec un taux d'actualisation de 10 %, figure dans le tableau ci-dessous. Sur trois ans, l'entreprise composite prévoit un coût total de 828 085 USD ajusté en fonction des risques (VA).

Tableau 7
Coûts totaux en termes de flux de trésorerie (estimations ajustées aux risques)

Réf.	Catégorie de coûts	Période initiale	1re année	2e année	3e année	Total	Valeur actuelle
Ftr	Coûts initiaux et maintenance annuelle de Guardium	555 500 USD	99 990 USD	99 990 USD	99 990 USD	855 470 USD	804 160 USD
Gtr	Planification, mise en œuvre et services professionnels	23 925 USD	0 USD	0 USD	0 USD	23 925 USD	23 925 USD
	Coûts totaux (ajustés en fonction des risques)	**579 425 USD**	**99 990 USD**	**99 990 USD**	**99 990 USD**	**879 395 USD**	**828 085 USD**

Source : Forrester Research, Inc.

Synthèse des résultats

Les résultats financiers calculés dans les sections Coûts et Bénéfices peuvent être utilisés pour déterminer le retour sur investissement (RSI), le taux de rentabilité interne (TRI), la valeur actuelle nette (VAN) et le délai d'amortissement de l'investissement réalisé par l'entreprise composite dans IBM Security Guardium.

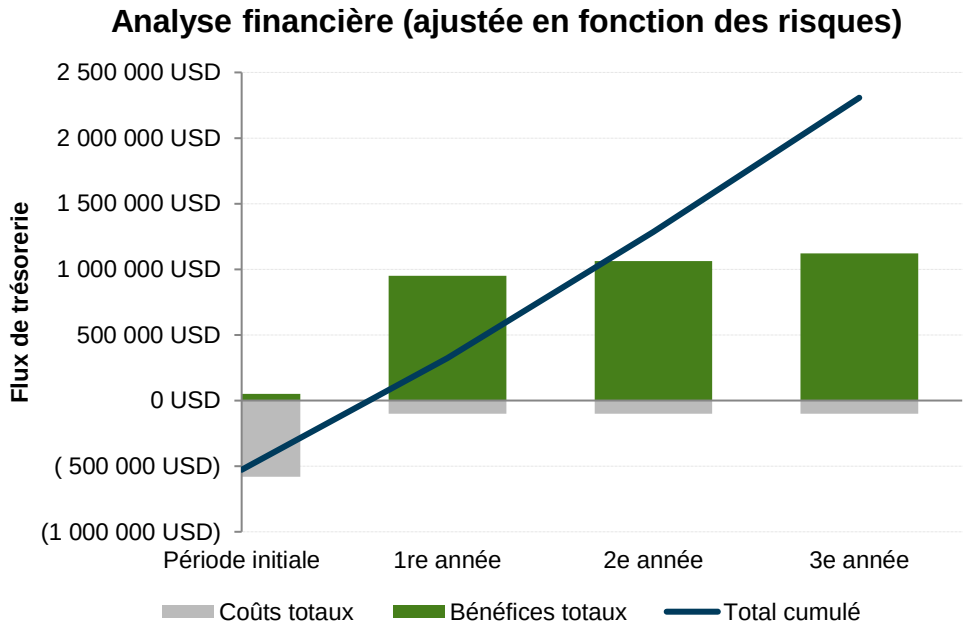
Le tableau 9 ci-dessous montre les valeurs du RSI, de la VAN et du délai d'amortissement ajustées aux risques.

Analyse des flux de trésorerie (estimations ajustées aux risques)

Résumé	Période initiale	1re année	2e année	3e année	Total	Valeur actuelle
Coûts totaux	(579 425 USD)	(99 990 USD)	(99 990 USD)	(99 990 USD)	(879 395 USD)	(828 085 USD)
Bénéfices totaux	51 840 USD	950 375 USD	1 062 133 USD	1 122 050 USD	3 186 398 USD	2 636 625 USD
Total	**(527 585 USD)**	**850 385 USD**	**962 143 USD**	**1 022 060 USD**	**2 307 003 USD**	**1 808 540 USD**
ROI						**218 %**
Délai d'amortissement (mois)						**7,4**

Source : Forrester Research, Inc.

Le graphique ci-dessous montre les flux de trésorerie ajustés au risque.



Source : Forrester Research, Inc.

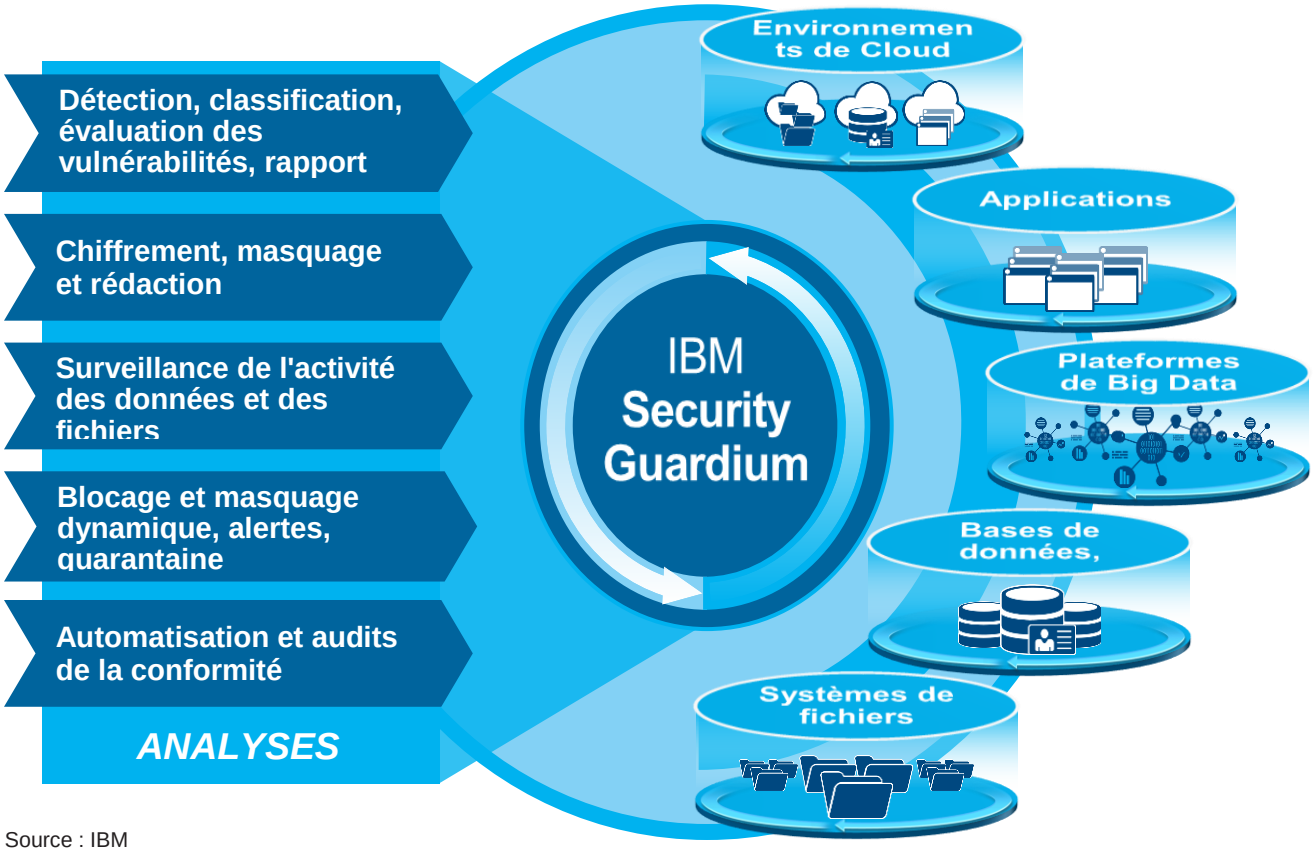
À propos d'IBM Guardium

Les informations suivantes sont fournies par IBM. Forrester n'a validé aucune réclamation et ne soutient en aucune manière IBM ou ses offres.

IBM Security Guardium, anciennement dénommé IBM InfoSphere Guardium, a pour objet de protéger les données critiques partout où elles se trouvent. Cette plateforme complète de protection des données permet aux équipes de sécurité d'analyser automatiquement ce qui se passe dans l'environnement des données afin de mieux réduire les risques, de protéger les données sensibles contre les menaces internes et externes et de s'adapter en toute transparence aux changements qui touchent à la sécurité des données.

Guardium permet d'aborder de façon exhaustive la protection des données cruciales pour la plupart des entreprises (les données sensibles vitales pour leur réussite et leur survie). Grâce à l'interface utilisateur graphique de bout en bout de Guardium, les équipes chargées de la sécurité peuvent identifier et contrer les risques pesant sur les données sensibles, que celles-ci soient en mouvement ou au repos. Cette approche unifiée s'étend en outre à une large gamme de référentiels de données structurées ou non, notamment les bases et les entrepôts de données, les systèmes Hadoop, NoSQL, en mémoire ou les systèmes de fichiers.

Concrètement, Guardium utilise une approche souple et modulaire afin de répondre à un large éventail d'exigences en matière de sécurité et de protection des données, depuis des fonctions de conformité, de surveillance et de chiffrement de base jusqu'à une protection complète des données, le tout de façon économique et évolutive. En outre, contrairement aux solutions ponctuelles, Guardium peut être intégré de façon hétérogène avec d'autres solutions de sécurité, normes de vulnérabilité ou applications standard du secteur, par exemple. Guardium offre également une intégration record avec les solutions de sécurité IBM. IBM est un partenaire stratégique qui permet aux entreprises de réduire la vulnérabilité de leurs systèmes de sécurité et de gérer les risques dans les environnements informatiques les plus complexes.



Source : IBM

DIVULGATIONS

- L'étude a été commandée par IBM et réalisée par Forrester Consulting. Il ne s'agit pas d'une analyse concurrentielle.
- Forrester n'émet aucune hypothèse quant au potentiel retour sur investissement obtenu par d'autres entreprises. Forrester conseille vivement aux lecteurs d'utiliser leurs propres estimations avec le cadre fourni dans le rapport pour déterminer la pertinence d'un investissement dans IBM Security Guardium.
- IBM a examiné l'étude et fait des commentaires à Forrester, qui a conservé un contrôle éditorial sur l'étude et ses conclusions et n'a accepté aucune modification allant à l'encontre de ses propres conclusions ou dénaturant le sens de l'étude.

GLOSSAIRE

Taux d'actualisation : taux d'intérêt utilisé dans le cadre de l'analyse des flux de trésorerie, pour prendre en compte la valeur temporelle de l'argent. Les entreprises déterminent leur propre taux en fonction de leur secteur d'activité et de leur environnement d'investissement. Pour la présente analyse, Forrester se base sur un taux d'actualisation annuel de 10 %. Nous recommandons fortement au lecteur de consulter son entreprise pour déterminer le taux approprié à son environnement.

Valeur actuelle nette (VAN) : valeur actuelle des futurs flux nets de trésorerie (actualisés) selon un taux d'intérêt donné (le taux d'actualisation). Une VAN positive pour un projet indique normalement que l'investissement est souhaitable, à moins que d'autres projets aient une VAN plus élevée.

Valeur actuelle (VA) : valeur actuelle (actualisée) des estimations des coûts et des avantages, calculée selon un taux d'intérêt donné (le taux d'actualisation). La VA des coûts et des avantages s'inscrit dans la VAN des flux de trésorerie.

Délai de récupération : point d'équilibre d'un investissement. Moment à partir duquel la valeur nette des avantages (avantages auxquels sont soustraits les coûts) équivaut à celle de l'investissement ou des coûts initiaux.

Rendement du capital investi (RCI) : mesure, en pourcentage, du rendement prévu d'un projet. On obtient le RSI en divisant la valeur nette des avantages (avantages auxquels on soustrait les coûts) par les coûts.

Taux de rentabilité interne (TRI) : taux d'intérêt qui va transformer une série de flux de trésorerie (positifs et négatifs) en une valeur actuelle nette de zéro.

À PROPOS DE FORRESTER CONSULTING

Forrester Consulting offre des conseils indépendants et impartiaux fondés sur la recherche pour accompagner les dirigeants dans leur succès au sein de leur entreprise. Qu'il s'agisse de courtes sessions consacrées à la stratégie ou de projets personnalisés, les services de Forrester Consulting vous mettent directement en contact avec des analystes qui appliquent leur expertise aux défis spécifiques de votre entreprise. Pour plus d'informations, visitez le site forrester.com/consulting.

À PROPOS DE TEI

La méthodologie TEI™ (Total Economic Impact) a été conçue par Forrester Research. Elle permet aux entreprises d'améliorer leurs processus décisionnels en matière de technologie et aide les fournisseurs à faire part de la proposition de valeur des produits et des services qu'ils offrent à leurs clients. Grâce à cette méthodologie, les entreprises peuvent démontrer, justifier et rendre tangible la valeur de leurs initiatives informatiques auprès des membres de la direction et des autres acteurs clés. La méthodologie TEI est constituée de 4 composantes permettant d'évaluer la valeur d'un investissement : bénéfices, coûts, risques et flexibilité. http://www.forrester.com/marketing/product/consulting/tei.html