proofpoint.

EBOOK

Le coût d'une sécurité « acceptable »

Calcul de la valeur réelle des solutions de cybersécurité

Cybercriminalité et risques métier

L'adage « Le crime ne paie pas » est mis à mal par les cyberattaques modernes. Le coût moyen d'une compromission de données pour les entreprises américaines concernées est passé de 5,4 millions de dollars en 2013 à 9,44 millions de dollars en 2022[1], une hausse nettement supérieure à l'inflation sur la même période. Collectivement, les compromissions de données coûtent aux entreprises américaines environ 1,4 milliard de dollars par an, soit 5 400 dollars par adulte américain[2].

À l'échelle mondiale, la cybercriminalité pourrait coûter au monde 10,5 billions de dollars par an d'ici 2025[3]. D'autres chercheurs estiment que la cybercriminalité coûte 1,79 million de dollars chaque *minute* aux entreprises[4].

Ces coûts sont astronomiques et ne se limitent pas aux pertes financières directes. En effet, les cyberattaques peuvent porter atteinte à la réputation de votre entreprise ou vous faire encourir des amendes réglementaires. Elles peuvent perturber vos activités et même fragiliser votre modèle économique, vous empêchant ainsi de suivre votre stratégie fondamentale.

Rien ne permet d'éviter totalement les risques associés à la cybercriminalité. Ils font désormais partie intégrante de l'environnement professionnel.

Il est toutefois possible de gérer ces risques. De même que les dirigeants d'entreprise et les responsables de la gestion des risques se préparent à affronter d'autres risques indissociables de toute activité professionnelle, vous pouvez limiter votre exposition aux risques de cybersécurité. Comme pour d'autres types de risques métier, il vous faudra modéliser les pertes financières pouvant découler d'une cyberattaque contre votre entreprise. Vous pourrez ensuite élaborer un plan afin de mettre en balance les risques et les coûts de réduction de ceux-ci.

À l'échelle mondiale, le coût moyen d'une compromission de données s'élève désormais à **4,24 millions de dollars**[5].

Les experts estiment que la cybercriminalité pourrait coûter au monde **10,5 billions de dollars**[6].

1 %

Les pertes dues à la cybercriminalité s'élèvent désormais à 1 % du PIB mondial[7].

La cybercriminalité coûte **1,79 million de dollars** par minute aux entreprises.

1 IBM, « **Cost of Data Breach Report 2022** » (Rapport 2022 sur le coût des compromissions de données), juillet 2022.
2 Rick Newman *(Yahoo Finance)*, « **We're all paying a cybersecurity tax** » (Nous payons tous une taxe de cybersécurité), mai 2021.
3 Steve Morgan *(Cybersecurity Ventures)*, « **Cybercrime to Cost the World $10.5 Trillion Annually by 2025** » (La cybercriminalité pourrait coûter au monde 10,5 billions de dollars par an d'ici 2025), novembre 2020.
4 James Coker *(Infosecurity Magazine)*, « **Cybercrime Costs Organizations Nearly $1.79 Million Per Minute** » (La cybercriminalité coûte environ 1,79 million de dollars par minute aux entreprises), juillet 2021.
5 IBM, « **Cost of Data Breach Report 2022** » (Rapport 2022 sur le coût des compromissions de données), juillet 2022.
6 Steve Morgan *(Cybersecurity Ventures)*, « **Cybercrime to Cost the World $10.5 Trillion Annually by 2025** » (La cybercriminalité pourrait coûter au monde 10,5 billions de dollars par an d'ici 2025), novembre 2020.
7 Zhanna Malekos Smith et Eugenia Lostri *(Center for Strategic and International Studies)*, « **The Hidden Cost of Cybercrime: Report** » (Rapport sur le coût caché de la cybercriminalité), décembre 2020.

La première étape de l'évaluation des solutions consiste à comparer la résistance aux risques d'une solution à son coût, afin de vous assurer que vous bénéficiez du meilleur rapport qualité-prix.

Investir dans des technologies de sécurité fait partie des stratégies de réduction de ces risques. Mais comment être sûr que les investissements que vous consentez sont les plus judicieux ?

En tant que RSSI, la réduction des risques est votre objectif n° 1. La première étape de l'évaluation des solutions consiste à comparer la résistance aux risques d'une solution à son coût, afin de vous assurer que vous bénéficiez du meilleur rapport qualité-prix. Vous devez également tenir compte des coûts autres que les licences, par exemple les coûts de matériel, de déploiement, de fonctionnement et de maintenance continue. Réfléchissez également aux autres avantages que les solutions peuvent vous offrir, notamment en ce qui concerne l'efficacité des collaborateurs.

À titre d'exemple, prenons la pression qui pèse sur les épaules de votre équipe de sécurité interne. Aujourd'hui, les RSSI font face à des pénuries de personnel dans leurs programmes d'opérations de sécurité. À l'échelle mondiale, 2,72 millions de postes restent à pourvoir dans le domaine de la cybersécurité[8]. Pour défendre efficacement les ressources stratégiques des entreprises, il faudrait que les effectifs de cybersécurité augmentent de près de 65 %[9]. Pour les RSSI, ces difficultés sont une réalité quotidienne.

Il est évident que le temps des professionnels de la sécurité est précieux et que la charge administrative doit être prise en compte dans les coûts d'une solution de cybersécurité. Mais qu'en est-il de la productivité des utilisateurs finaux ? Des coûts de main-d'œuvre associés à la réponse aux incidents ? De ceux liés au signalement d'un incident ?

Dans ce guide, nous nous intéresserons de plus près aux coûts associés au déploiement et à l'exécution d'une solution de cybersécurité. Nous examinerons tous les facteurs qui peuvent influer sur la valeur totale d'une solution, y compris ceux auxquels vous n'avez peut-être pas pensé. Nous déterminerons à quel moment il devient plus rentable d'investir dans une solution de protection avancée de la messagerie ou une solution complète de protection contre les menaces email et cloud, plutôt que de vous contenter de modules complémentaires ou de solutions d'ancienne génération à bas prix.

8 (ISC)2, « **Cybersecurity Workforce Study** » (Étude sur les effectifs de cybersécurité), mars 2022.
9 Ibid.

Le coût réel de la gestion des risques de cybersécurité

Vos investissements dans la cybersécurité constituent un moyen de réduire les risques opérationnels et métier. Mais il n'existe pas nécessairement de lien univoque entre les dépenses consenties et l'étendue de la couverture. Vous avez besoin d'une approche multicouche de la sécurité pour bénéficier d'une défense solide.

Certaines solutions de sécurité réduisent plus que d'autres les risques auxquels vous êtes exposé. De légères différences en termes d'efficacité peuvent avoir un impact considérable sur le risque de compromission (et son coût potentiel). De même, il existe des solutions à tous les prix.

Il est essentiel de tenir compte de tous ces facteurs dans votre décision d'achat. Vous devez également prendre en compte votre retour sur investissement potentiel.

Pour ce faire, vous devez réfléchir à toutes les pertes engendrées par une compromission majeure. Celles-ci vont bien au-delà des coûts associés à la compromission en elle-même. Le préjudice porté à votre entreprise et à sa réputation peut avoir des conséquences négatives pendant des années.

Vous devez mettre en balance ces pertes potentielles avec le coût de la solution de cybersécurité en elle-même. À première vue, le calcul peut paraître simple : il suffit de connaître les frais de licence, non ?

Mais lorsqu'il s'agit d'évaluer la valeur économique totale d'une solution de cybersécurité, les coûts de licence ne sont que la partie émergée de l'iceberg. Si vous ne tenez compte que des licences, vous ne bénéficiez pas d'une vue d'ensemble de ce qu'une solution va coûter à votre entreprise. Il existe de nombreux autres coûts cachés, qui peuvent considérablement augmenter le coût global d'une solution.

Et la réduction des risques n'est pas toujours aussi simple. Si vous tirez parti de toutes les fonctionnalités d'une solution, vous pouvez réduire de moitié les risques auxquels vous êtes exposé, mais vous ne pourrez probablement pas exploiter l'ensemble des fonctionnalités d'un produit dès sa mise en service. Par ailleurs, la plupart des solutions offrent des avantages en plus de la réduction des risques. Elles permettent par exemple d'améliorer l'efficacité de l'équipe de sécurité, ce qui augmente leur valeur.

Les répercussions d'une compromission

Les pertes causées par les compromissions peuvent inclure ce qui suit :

- Perte de revenus et de clients
- Perte de données (et de la valeur qui aurait pu être tirée de leur analyse)
- Pertes financières directes*
- Atteinte à la réputation
- Perte de productivité des collaborateurs
- Interruptions d'activité
- Baisse de la valeur des actions
- Perte de propriété intellectuelle
- Perte d'un avantage concurrentiel
- Amendes ou sanctions pour non-conformité

* Ces pertes peuvent inclure le paiement de rançons et les coûts de main-d'œuvre et de service pour la réponse aux incidents et la reprise des activités.

Additionnez les coûts

L'adoption d'une nouvelle solution de cybersécurité peut s'avérer coûteuse et chronophage pour la plupart des entreprises. Le processus peut également perturber les activités des utilisateurs, des équipes informatiques et de celles chargées des opérations de sécurité. Certains outils sont difficiles à gérer, ce qui accroît la charge de travail des équipes de sécurité déjà très sollicitées. Pour estimer l'impact financier total de cet achat sur votre entreprise, vous devez tenir compte de plusieurs facteurs :

Licences

Combien payez-vous par an et par utilisateur pour la solution ? Les coûts de licence totaux correspondent au coût par utilisateur par an multiplié par le nombre d'utilisateurs.

Gestion continue

Les coûts de gestion continue correspondent au temps consacré par des collaborateurs spécialisés aux activités de gestion continue. Il est important de prendre ce facteur en considération. Imaginez que la gestion d'une solution nécessite deux collaborateurs à temps plein, alors qu'une autre n'en requiert qu'un. Vous devez prendre en compte le fait que la gestion continue de la première solution coûtera deux fois plus cher sur le long terme. Vue sous cet angle, une solution soi-disant gratuite peut vite devenir bien plus onéreuse qu'un produit payant mais facile à gérer, en particulier si le fournisseur de ce produit propose un support de premier ordre.

Matériel

Certaines solutions peuvent s'accompagner de matériel, ce qui entraîne des coûts supplémentaires pour votre entreprise, en particulier si vous gérez ce matériel sur site. Combien le maintien à jour de ce matériel, la préservation de la connectivité et la maintenance des installations adéquates vont-ils vous coûter, par rapport à la préparation aux attaques et à la reprise d'activité après sinistre ? Combien de vos collaborateurs assureront la maintenance de l'équipement ?

Déploiement

Services professionnels
De nombreux fournisseurs recommandent, voire exigent, que leur équipe de services professionnels vous aide à configurer et à déployer la solution. Bien évidemment, ces services ne sont pas gratuits.

Temps consacré par les ressources
Que l'équipe de services professionnels du fournisseur intervienne ou non, le déploiement d'un nouveau produit nécessite une implication plus ou moins importante de vos collaborateurs internes. Combien d'heures de travail vont-ils consacrer à ce projet ? Quels collaborateurs devront s'en charger ? L'estimation du nombre d'heures de travail de vos collaborateurs salariés ne constitue que la première étape. Quelles autres responsabilités devront-ils mettre de côté pour se concentrer sur ce projet ? Vous devrez également réfléchir à ce que vous pourriez perdre si les professionnels n'effectuent pas d'autres tâches à forte valeur ajoutée.

Lorsque l'on se penche sur le coût total de possession d'une solution de cybersécurité, il devient rapidement évident que les coûts d'implémentation et de maintenance continue peuvent dépasser les dépenses associées aux licences.

Tenez compte des avantages

Pour estimer la valeur totale d'une solution, mettez en balance tous les coûts susmentionnés avec les avantages offerts par le produit. La résistance aux risques est clairement le principal avantage de toute solution de sécurité. Mais, comme pour les coûts, vous devez prendre en compte d'autres facteurs.

Voici les avantages que vous devez garder à l'esprit :

- **Résistance aux risques**

  Pour calculer la résistance aux risques d'une solution, vous devez d'abord mesurer l'ampleur des pertes potentielles pour votre entreprise. Quel est le coût moyen d'une compromission de données dans votre secteur et votre région, et pour une entreprise de la taille de la vôtre ? Vous devrez mettre en balance ce coût avec votre vulnérabilité et la résistance aux risques de la solution. Enfin, gardez à l'esprit qu'il vous faudra un peu de temps pour tirer pleinement parti des avantages d'une solution.

- **Efficacité des collaborateurs**

  Productivité des utilisateurs
  La productivité peut prendre de nombreuses formes. Les deux plus importantes pour les responsables de la sécurité sont la productivité des utilisateurs et la productivité des équipes informatique et de sécurité. Une solution de cybersécurité peut affecter la productivité des collaborateurs de manières variées et complexes. Ces effets s'étendent aux utilisateurs finaux ainsi qu'aux équipes informatiques et de cybersécurité. Combien de minutes ou d'heures les analystes perdraient-ils s'ils n'avaient pas accès à leur ordinateur portable pendant l'élimination d'un malware, par exemple ? Quel serait le coût pour votre entreprise si les membres de l'équipe commerciale ne pouvaient pas interagir avec les clients en raison de la compromission d'un compte cloud ? Chaque fois qu'un spam ou un email malveillant est bloqué, vous évitez une interruption d'activité qui nuirait à votre entreprise. En outre, chaque fois qu'un email malveillant passe entre les mailles du filet, l'incident pourrait faire perdre du temps aux professionnels du service d'assistance et aux administrateurs informatiques.

Le coût annuel moyen des attaques de phishing s'élève désormais à plus de

14,7 millions de dollars[10].

Chaque professionnel de la connaissance perd en moyenne

sept heures

de temps productif chaque année à cause du phishing[11].

En 2021, les attaques de ransomwares ont coûté en moyenne

4,54 millions de dollars

à leurs victimes[12].

Les victimes de piratage de la messagerie en entreprise (BEC) ont versé plus de

43 milliards de dollars

aux cybercriminels entre 2016 et 2021[13].

10 Ponemon Institute, « **2021 Cost of Phishing Study** » (Étude 2021 sur le coût du phishing), juin 2021.
11 Ibid.
12 IBM, « **Cost of a Data Breach Report 2022** » (Rapport 2022 sur le coût des compromissions de données), juillet 2022.
13 Federal Bureau of Investigation, « **Business Email Compromise: The $43 Billion Scam** » (Piratage de la messagerie en entreprise : des arnaques chiffrées à 43 milliards de dollars), mai 2022.

Surveillance, tri et analyse
Les analystes en cybersécurité font partie des professionnels les plus qualifiés et les mieux payés des effectifs informatiques modernes. Et ils se font rares. Les tâches auxquelles les équipes chargées des opérations de sécurité consacrent leur temps et leur attention revêtent une importance stratégique pour votre entreprise. La solution que vous envisagez d'adopter rend-elle leur travail plus simple ou plus compliqué ? S'intègre-t-elle facilement aux solutions de surveillance ou de détection et de réponse aux incidents actuellement déployées dans votre environnement ? Vous pourriez peut-être externaliser ces responsabilités à un fournisseur de services. Dans ce cas, la solution permettra-t-elle à votre partenaire de garantir une visibilité et une couverture optimales ?

Réponse et correction
Chaque minute compte dès lors qu'il s'agit d'empêcher les cybercriminels de se déplacer dans votre environnement. La solution propose-t-elle une plate-forme consolidée ? Pouvez-vous utiliser la gestion des règles pour accélérer les changements de configuration ? Plus vite vous pouvez bloquer et neutraliser les menaces entrantes, moins elles sont susceptibles de devenir des compromissions dévastatrices.

Automatisation
La solution en question inclut-elle des workflows d'automatisation prédéfinis permettant de réaliser vos tâches informatiques ou de protection de la messagerie habituelles ? Si votre équipe a besoin de déployer des efforts conséquents de conception et de configuration afin que la solution puisse exécuter des workflows automatisés, vous devez également en tenir compte. Si deux solutions peuvent accomplir la même tâche, mais que l'une d'entre elles est plus longue à configurer ou requiert un travail de codage ou de gestion continue plus important, elle vous coûtera plus cher que l'autre.

Threat intelligence
La traque des menaces est une fonction de sécurité hautement spécialisée qui vous aide à détecter les vulnérabilités ou à empêcher des incidents mineurs de devenir des compromissions. Elle requiert des compétences et une expertise dont votre personnel ne dispose peut-être pas. La solution que vous envisagez d'adopter fournit-elle une threat intelligence qui contribuera à réduire la charge de travail de votre équipe ? Offre-t-elle une visibilité permettant à votre équipe de consacrer moins de temps et d'efforts à la traque des menaces, ou d'aller plus loin avec les mêmes effectifs ?

Mettre en balance les coûts et les avantages réels

Maintenant que nous avons passé en revue les coûts et les avantages qu'une solution de sécurité peut offrir à votre entreprise, voyons comment calculer la valeur totale des solutions dans le monde réel.

Quelles sont les différences de valeur *réelle* entre les fonctionnalités soi-disant gratuites ou à bas prix et celles que vous offre une solution de pointe ?

Pour évaluer vos options, vous pouvez calculer la valeur totale de chaque solution en soustrayant les coûts des économies réalisables. Voici deux exemples :

Exemple 1

Protection de la messagerie

Les attaques email d'aujourd'hui ciblent les personnes, pas les systèmes. Elles ont recours à des tactiques d'ingénierie sociale pour inciter les utilisateurs à visiter des sites malveillants et à divulguer leurs identifiants de connexion. Une solution efficace de protection de la messagerie doit être capable de prévenir, de détecter et de neutraliser les menaces qui visent vos collaborateurs. Elle doit également offrir aux équipes de sécurité la visibilité et les informations dont elles ont besoin pour être efficaces, sans être difficile à configurer ou à gérer.

Évaluation des coûts

Imaginons que vous êtes une société de services financiers basée aux États-Unis et comptant 15 000 collaborateurs. Vous évaluez deux solutions de protection de la messagerie, dont l'une est une solution soi-disant gratuite intégrée à un produit pour lequel vous possédez déjà une licence. Dans cet exemple, un collaborateur à temps plein coûte 150 000 dollars par an.

Vos coûts (sur trois ans) pourraient ressembler à ceci :

CATÉGORIE DE COÛTS	SOLUTION DE PROTECTION DE LA MESSAGERIE A	SOLUTION DE PROTECTION DE LA MESSAGERIE B
Coûts de licence	-787 500 $	-0 $ (la solution étant intégrée à un produit pour lequel vous possédez déjà une licence)
Services professionnels	-27 000 $	-0 $ (déjà déployée)
Temps consacré au déploiement par les collaborateurs	-6 250 $ (1 équivalent temps plein pendant 0,5 mois)	-0 $ (déjà déployée)
Temps consacré à la gestion continue par les collaborateurs	-450 000 $ (1 équivalent temps plein par an)	-450 000 $
Total	**-1 270 750 $**	**-450 000 $**

À première vue, vous pourriez penser que la solution B est plus intéressante, car la solution A coûte plus de 700 000 dollars de plus que la solution B. Les services professionnels et le déploiement de ces solutions étant des dépenses préalables, nous avons exclu ces valeurs.

Avantages des solutions de protection de la messagerie

Pour comprendre la valeur totale des solutions, vous devez également prendre en considération leurs avantages, y compris leur résistance aux risques et leur effet sur l'efficacité des collaborateurs.

Vos coûts (sur trois ans) pourraient ressembler à ceci :

CATÉGORIE D'AVANTAGES	SOLUTION DE PROTECTION DE LA MESSAGERIE A	SOLUTION DE PROTECTION DE LA MESSAGERIE B
Résistance aux risques	5 707 901 $	4 442 698 $
Productivité des utilisateurs	1 200 208 $	974 788 $
Surveillance, tri et analyse	1 532 510 $	1 224 135 $
Réponse et correction	2 651 671 $	2 153 641 $
Automatisation	0 $	756 685 $
Threat intelligence	0 $	0 $
Total	**11 092 290 $**	**9 551 947 $**

La solution A présente une résistance aux risques nettement supérieure et améliore davantage l'efficacité des collaborateurs, ce qui complique le tableau. La solution B offre une fonctionnalité supplémentaire. Dans ce cas, il faudrait donc déterminer s'il est possible d'ajouter cette option à la solution A, ce qui augmenterait notre retour sur investissement potentiel.

Enfin, vous devez mettre en balance les coûts totaux avec les avantages pour obtenir la valeur totale de chacune d'entre elles :

CATÉGORIE	SOLUTION DE PROTECTION DE LA MESSAGERIE A	SOLUTION DE PROTECTION DE LA MESSAGERIE B
Avantages	11 092 290 $	9 551 947 $
Coûts	-1 270 750 $	-450 000 $
Valeur totale	**9 821 540 $**	**9 101 947 $**

Vous bénéficiez maintenant d'une vue d'ensemble. Bien que la solution A soit plus chère, sa valeur totale dépasse celle de la solution B, soi-disant gratuite, de plus de 700 000 dollars. Tenez également compte de vos exigences métier lors de la comparaison.

Exemple 2

Sécurité du cloud

Les solutions modernes de protection des applications cloud aident les entreprises à gérer les risques liés aux utilisateurs dans le cloud. Les entreprises n'ont jamais autant utilisé de plates-formes et de services cloud qu'aujourd'hui. Ceux-ci leur permettent de prendre en charge les modèles de travail à distance et hybrides, ainsi que de profiter de la flexibilité et de l'agilité qu'offre le cloud. Cependant, même si leurs avantages ne sont plus à démontrer, les applications et services cloud engendrent de nouveaux risques. Une solution CASB (Cloud Application Security Broker) sécurise les applications approuvées par l'équipe informatique dans le cloud. Elle offre en outre visibilité et contrôle sur l'accès et l'utilisation des applications cloud par les utilisateurs, ainsi que sur le partage de données sensibles.

En 2021, le nombre de compromissions impliquant des ressources cloud a pour la première fois dépassé le nombre de compromissions visant des ressources sur site[14]. À mesure que les entreprises migrent vers le cloud, les cybercriminels leur emboîtent le pas. Étant donné que les entreprises utilisent de plus en plus d'applications SaaS (Software-as-a-Service) comme Microsoft 365 et Google Workspace, cette tendance devrait se poursuivre.

Si vous migrez une part considérable de votre infrastructure vers le cloud, ne vous demandez pas si vous avez besoin d'une solution de sécurité cloud, mais plutôt laquelle adopter.

Évaluation des coûts

Imaginons que vous êtes un établissement de santé basé aux États-Unis et comptant 15 000 collaborateurs. Vous envisagez d'adopter une nouvelle solution cloud (solution A), que vous comparez à votre solution existante (solution B). Dans cet exemple, un collaborateur à temps plein coûte 150 000 dollars par an.

Vos coûts (sur trois ans) pourraient ressembler à ceci :

CATÉGORIE DE COÛTS	SOLUTION DE SÉCURITÉ CLOUD A	SOLUTION DE SÉCURITÉ CLOUD B
Coûts de licence	-776 250 $	-765 000 $
Services professionnels	-26 000 $	-0 $ (déjà déployée)
Temps consacré au déploiement par les collaborateurs	-6 250 $ (1 équivalent temps plein pendant 0,5 mois)	-0 $ (déjà déployée)
Temps consacré à la gestion continue par les collaborateurs	-450 000 $ (1 équivalent temps plein par an)	-450 000 $
Total	**-1 258 500 $**	**-1 215 000 $**

Dans cet exemple, le coût de la solution A dépasse légèrement celui de la solution B. Les services professionnels et le déploiement de ces solutions étant des dépenses préalables, nous avons exclu ces valeurs. Pour connaître la véritable différence entre les solutions, vous devez comparer les économies qu'elles vous permettent de réaliser.

REMARQUE IMPORTANTE : Si votre solution existante est une solution de gestion des identités et des accès hébergée sur site et que vous envisagez de migrer vers une solution CASB, il vous faudra peut-être ajouter des coûts de matériel. La migration vers le cloud permet généralement de diminuer les dépenses en matériel, mais vos économies globales dépendront du fournisseur cloud que vous choisissez.

14 Verizon, « **2021 Data Breach Investigations Report** » (Rapport d'enquête 2021 sur les compromissions de données), mai 2021.

Évaluation des avantages

Comme pour votre évaluation de la protection de la messagerie, vous devez également prendre en considération les avantages de chaque solution pour comparer la valeur totale de chaque option. Vos coûts (sur trois ans) pourraient ressembler à ceci :

CATÉGORIE D'AVANTAGES	SOLUTION DE SÉCURITÉ CLOUD A	SOLUTION DE SÉCURITÉ CLOUD B
Résistance aux risques	6 137 377 $	3 625 216 $
Productivité des utilisateurs	42 684 $	34 667 $
Surveillance, tri et analyse	104 339 $	84 742 $
Réponse et correction	94 853 $	77 038 $
Threat intelligence	**1 264 707 $**	**1 027 174 $**
Total	**7 643 961 $**	**4 848 837 $**

Dans cet exemple, la solution A présente une résistance aux risques nettement supérieure et améliore davantage l'efficacité des collaborateurs.

	SOLUTION DE SÉCURITÉ CLOUD A	SOLUTION DE SÉCURITÉ CLOUD B
Avantages	**7 643 961 $**	**4 848 837 $**
Coûts	-1 258 500 $	-1 215 000 $
Valeur totale	6 385 461 $	3 633 837 $

Grâce à sa plus grande résistance aux risques et à son effet plus important sur l'efficacité des collaborateurs, la solution A offre une valeur près de deux fois supérieure à celle de la solution B.

Vue d'ensemble

Avant de prendre la décision d'investir dans une solution de sécurité, vous devez mettre en balance les coûts et les avantages associés à chacune des options disponibles. Il est essentiel d'opter pour une solution qui respectera votre budget à court terme, mais aussi qui réduira les risques financiers auxquels les cyberattaques exposent votre entreprise sur le long terme.

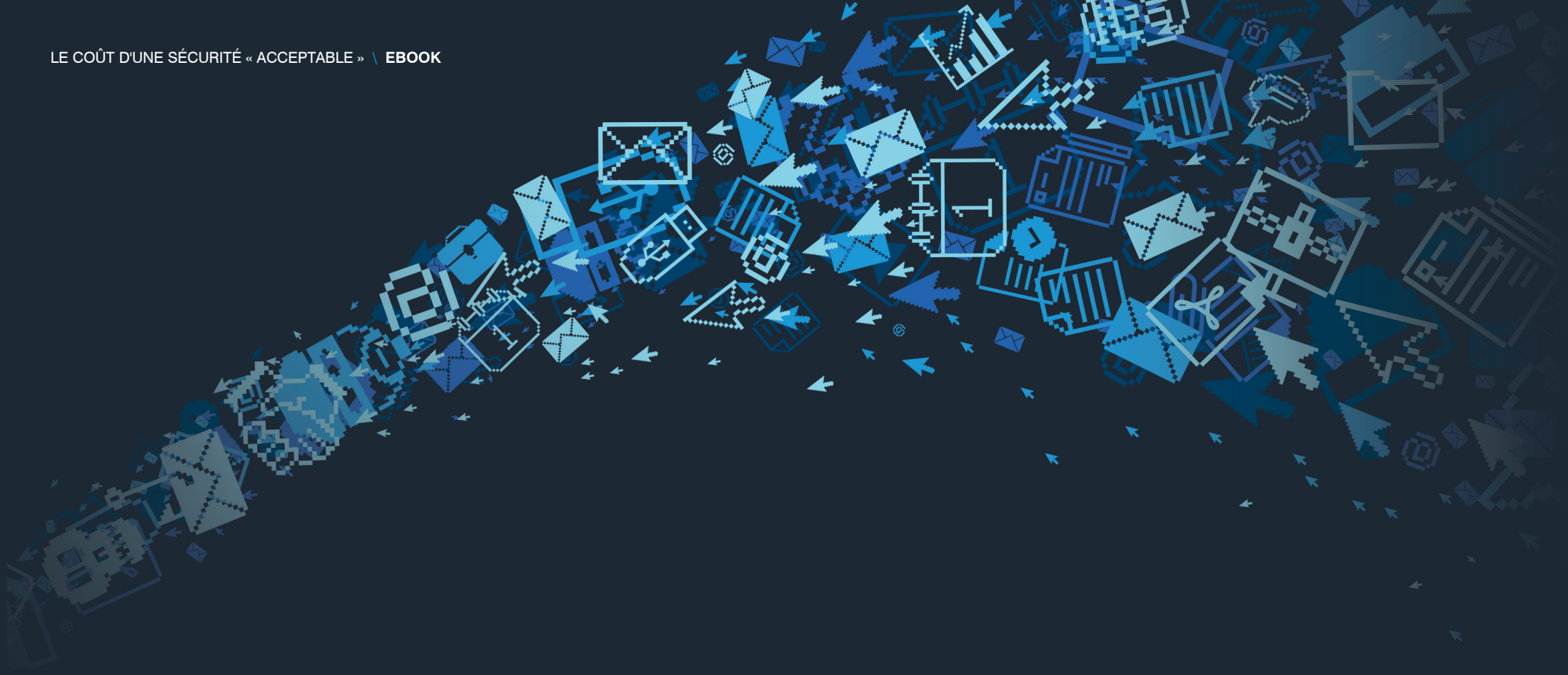
Les options dont les coûts de licence sont faibles peuvent sembler être une bonne affaire au premier abord, mais vous devez tenir compte d'un éventail bien plus large de facteurs pour prendre la décision la plus judicieuse possible. Mettez-vous à la recherche d'un fournisseur dont la solution offre une couverture globale et complète des vecteurs d'attaque les plus exploités actuellement.

N'oubliez pas que les intégrations avec d'autres solutions de sécurité fourniront à votre équipe une visibilité plus que nécessaire. Gardez à l'esprit que cette visibilité peut vous procurer les informations dont vous avez besoin pour implémenter des contrôles à même de réduire les risques, tout comme les workflows faciles à utiliser et à gérer, ainsi que le blocage automatisé et ultraperformant des menaces. Dans un contexte de pénurie de professionnels de la sécurité, tout ce qui facilite le travail des membres de votre équipe contribuera à réduire les coûts de main-d'œuvre et à créer plus de valeur.

Cette visibilité vous permettra également d'identifier les risques liés aux utilisateurs qui auraient pu échapper à toute détection. Aujourd'hui, les cybercriminels savent que vos collaborateurs sont le moyen le plus facile d'infiltrer votre entreprise. Par conséquent, les solutions les plus efficaces sont celles qui se concentrent sur l'identification et la réduction de ces risques. La meilleure stratégie pour optimiser vos dépenses de sécurité consiste à centrer votre attention sur les risques liés aux utilisateurs.

Étapes suivantes

Proofpoint propose des solutions complètes et intelligentes de protection de la messagerie et du cloud conçues pour protéger vos collaborateurs des menaces actuelles les plus dangereuses. Pour en savoir plus et demander une évaluation rapide des risques auxquels votre entreprise est exposée, visitez notre site à l'adresse : **proofpoint.com/fr**.



EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0501-012-03-01 09/22