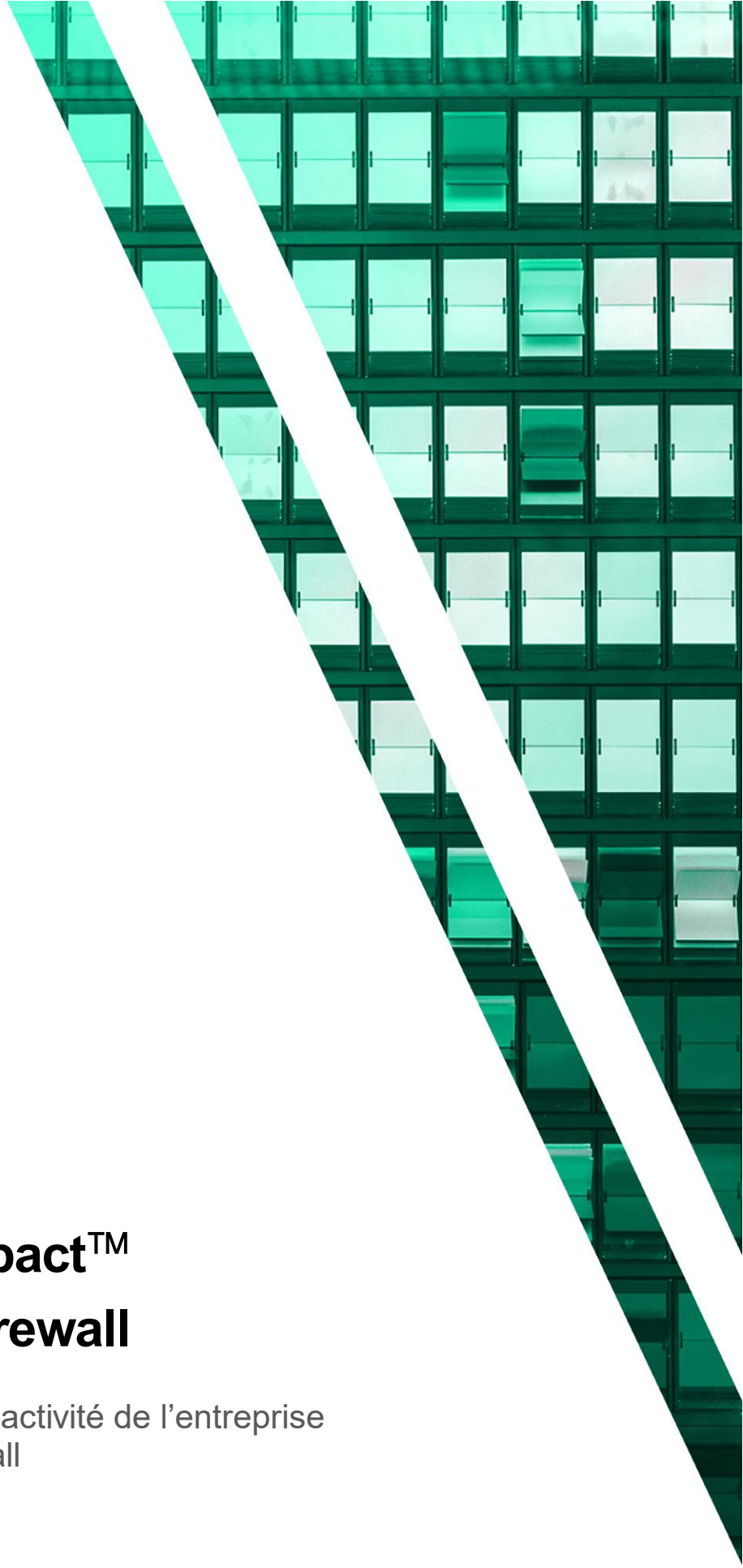
FORRESTER®



Total Economic Impact™ de Cisco Secure Firewall

Économies et bénéfices pour l'activité de l'entreprise réalisés grâce à Secure Firewall

MARS 2022

Sommaire

Résumé..... 1

Le parcours client avec Cisco Secure Firewall.... 6

Principaux défis 6

Entreprise de référence 7

Analyse des bénéfices..... 9

Amélioration de la gestion des pare-feux 9

Amélioration des processus de sécurité 12

Réduction du risque de compromission matérielle et de perte de productivité 15

Bénéfices en matière de performance pour la productivité des employés.....18

Coûts réduits et évités des anciennes solutions ..20

Bénéfices non quantifiés.....22

Flexibilité 23

Analyse des coûts.....24

Coûts de licence.....24

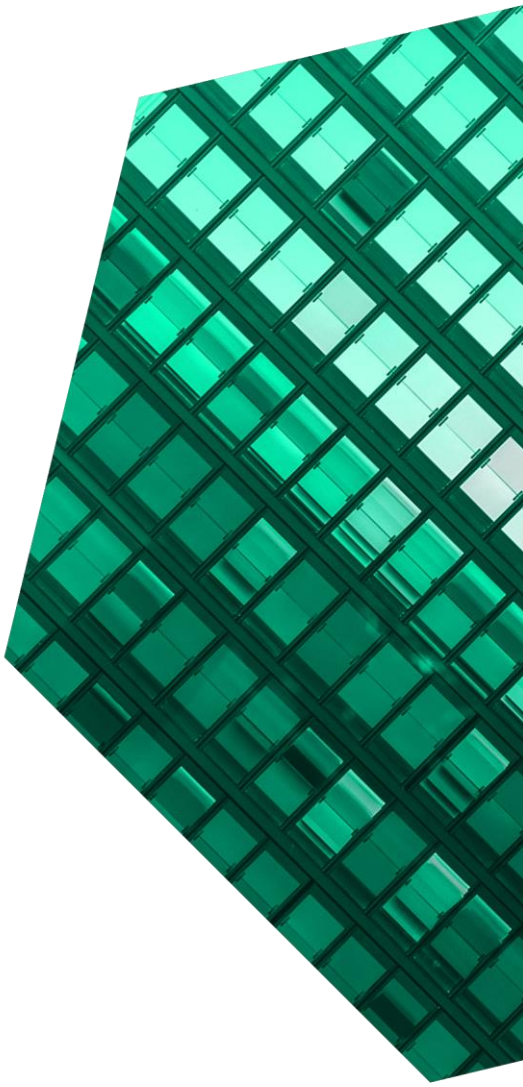
Coûts de mise en œuvre, de création de politiques et de formation.....27

Bilan financier 29

Annexe A : Total Economic Impact.....30

Annexe B : Notes de bas de page 31

Équipe de consultants : Henry Huang
Nick Mayberry



À PROPOS DE FORRESTER CONSULTING

Forrester Consulting propose des services de conseil indépendants et objectifs, basés sur un travail de recherche, pour accompagner les dirigeants sur la voie de la réussite. Pour en savoir plus, rendez-vous sur forrester.com/consulting.

© Forrester Research, Inc. Tous droits réservés. Toute reproduction sans autorisation préalable est strictement interdite. Les informations fournies s'appuient sur les meilleures ressources disponibles. Les opinions exprimées reflètent notre avis à la date de publication du document et sont susceptibles de changer. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar et Total Economic Impact sont des marques commerciales de Forrester Research, Inc. Toutes les autres marques commerciales sont la propriété de leurs détenteurs respectifs.

Résumé

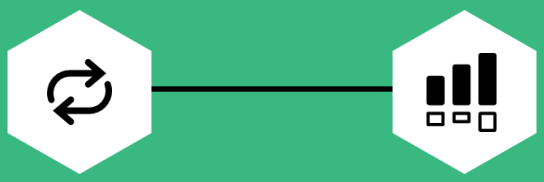
Cisco Secure Firewall et Firewall Management Center améliorent la visibilité et le contrôle de la sécurité du réseau. Les entreprises des personnes interrogées ont économisé jusqu'à 95 % sur le travail des professionnels des réseaux chargés des pare-feux et jusqu'à 83 % sur le travail des professionnels de la sécurité. Elles ont également réduit jusqu'à 80 % le risque de faille de sécurité, tout en améliorant la productivité des utilisateurs finaux grâce à la minimisation des perturbations du réseau et du VPN. Le niveau de sécurité a été améliorée même en réduisant les déploiements de pare-feux de 25 %.

Cisco Secure Firewall est une solution de sécurité réseau de nouvelle génération au niveau de la couche 7, qui protège les entreprises contre les menaces externes et internes, tout en allégeant la charge des équipes chargées du réseau et de la sécurité en matière de gestion des pare-feux et des menaces. Les entreprises peuvent gérer Cisco Secure Firewall avec Firewall Management Center (FMC), un centre d'administration centralisée des pare-feux et de défense contre les menaces, qui offre aux équipes chargées du réseau et de la sécurité une visibilité accrue sur les activités du réseau dans une vue plus unifiée et holistique, même au niveau de la couche applicative et pour les menaces détectées dans le trafic crypté. En outre, il offre un contrôle accru avec le système de prévention des intrusions (IPS) Snort 3, et des améliorations logicielles pour le filtrage des URL et la défense contre les logiciels malveillants.

La licence Cisco Secure Firewall comprend l'utilisation de SecureX, la plateforme intégrée de Cisco qui permet aux entreprises de consolider les données sur les menaces provenant du portefeuille Cisco Secure et d'outils de sécurité tiers en une seule vue globale de données enrichies en contexte, conçue pour faciliter les investigations et les réponses rapides.

Cisco a chargé Forrester Consulting de réaliser une étude de l'impact économique global (Total Economic Impact™, TEI) et d'analyser le retour sur investissement (ROI) que les entreprises pourraient obtenir en déployant Secure Firewall[1]. Cette étude a pour objectif de fournir aux lecteurs un cadre de référence qui leur permet d'évaluer l'impact financier potentiel de l'utilisation de Secure Firewall dans leur entreprise.

STATISTIQUES CLÉS



Retour sur investissement (ROI)
195 %

Valeur actuelle nette (VAN)
12,29 M$

Pour mieux cerner les bénéfices, les coûts et les risques de cet investissement, Forrester a interrogé dix décideurs de huit entreprises qui utilisent Secure Firewall. Pour les besoins de cette étude, Forrester a agrégé les expériences des personnes interrogées, puis a consolidé les résultats dans une entreprise de référence.

Avant d'utiliser Secure Firewall, ces personnes interrogées ont constaté que leurs entreprises ne disposaient pas de la visibilité et de la facilité de gestion nécessaires pour administrer de manière adéquate et sécuriser de manière efficace leurs réseaux. En l'absence de cette visibilité et d'une interface utilisateur graphique (GUI) efficace, les personnes interrogées ont noté que les processus du réseau tels que le déploiement de pare-feux, la création de politiques, les mises à niveau de pare-feux et les mises à jour de politiques prenaient beaucoup de temps. Du temps supplémentaire était également consacré aux processus de sécurité tels que l'investigation et la réponse aux menaces et l'administration de l'accès à distance. Les personnes interrogées ont constaté par ailleurs une mauvaise performance du réseau pendant les périodes de forte demande et des complications liées à la gestion de solutions de fournisseurs multiples.

Après avoir investi dans Secure Firewall, les personnes interrogées ont non seulement réduit le temps nécessaire pour accomplir les tâches liées au réseau et à la sécurité mentionnées ci-dessus, mais elles ont également amélioré la sécurité globale de leurs entreprises. Parallèlement, les entreprises ont amélioré la productivité de leurs employés grâce à des mises à jour plus rapides des politiques, à une meilleure inspection du trafic réseau et à une amélioration des performances globales du réseau, tout en mettant hors service les anciennes solutions et en éliminant en grande partie les coûts associés au temps de gestion.

Total des bénéfices

18,6 millions de dollars

PRINCIPALES CONCLUSIONS

Bénéfices quantifiés. Les bénéfices quantifiés en valeur actuelle (VA) ajustés en fonction des risques incluent les suivants :

- **Réduction des processus liés à l'exploitation du réseau jusqu'à 95 %.** Grâce aux dernières fonctionnalités de Cisco Secure Firewall et à la facilité de gestion via Firewall Management Center, les entreprises des personnes interrogées ont réduit le temps de :
  - Déploiement d'un pare-feu de 36 %.
  - Mise à jour d'un pare-feu de 90 %.
  - Mise à jour des politiques de pare-feu de 95 %, par rapport aux pare-feux traditionnels Adaptive Security Appliances (ASA) 5500-X.
  - Mise à jour des politiques de pare-feu de 80 % par rapport aux premières versions des politiques basées sur Firewall Threat Defense (FTD).
  - Mise à jour des pare-feux virtuels de 80 %.
- **Réduction du temps consacré aux investigations de sécurité et aux réponses jusqu'à 83 %.** Les personnes interrogées ont constaté par ailleurs des économies substantielles sur le travail des professionnels de la sécurité grâce à la combinaison de Cisco Secure Firewall et de Firewall Management Center, les informations étant mieux organisées pour être exploitées et analysées. Les personnes interrogées ont noté une réduction de 49 % du temps consacré aux investigations sur les menaces potentielles et de 83 % du temps consacré à la réponse aux menaces. L'utilisation de SecureX en plus de Secure Firewall et FMC a permis aux entreprises d'économiser jusqu'à 77 % du temps restant consacré aux investigations et aux réponses.

> **« Nous sommes très soucieux de la sécurité et souhaitons tirer parti des produits pour protéger notre entreprise. C'est pourquoi nous avons choisi Cisco. Ils ont grandi avec la sécurité ; pour eux, ce n'est pas une simple option. »**
> *Ingénieur réseau senior, fabrication*

- **Réduction du risque de faille de sécurité jusqu'à 80 %.** La visibilité et le contrôle combinés fournis par Cisco Secure Firewall et Firewall Management Center ont permis aux entreprises des personnes interrogées de réduire le risque de vol de données potentiel et les coûts associés. Ces solutions ont réduit le risque de faille de sécurité de 80 % par rapport aux pare-feux traditionnels ASA 5500-X et de 15 % par rapport aux premiers pare-feux basés sur FTD. SecureX a permis aux entreprises des personnes interrogées de réduire le risque résiduel et les coûts liés à une faille de sécurité jusqu'à 23 % supplémentaires.
- **Amélioration de la productivité des utilisateurs finaux évaluée à environ 2 millions de dollars par an.** Le déploiement de Cisco Secure Firewall et de

Firewall Management Center a amélioré la productivité des entreprises des personnes interrogées de deux manières. Tout d'abord, il a permis aux professionnels du réseau de corriger les erreurs de mise à jour des politiques perturbatrices 80 % plus rapidement. Par ailleurs, il a réduit la gravité de la dégradation des performances du réseau, permettant à chaque utilisateur final concerné de récupérer près de 9 heures de travail par an.

- **Réduction des coûts grâce à la mise hors service des anciens outils.** Les personnes interrogées ont également noté que Cisco Secure Firewall leur avait permis de mettre hors service les anciennes solutions de sécurité coûteuses qu'elles avaient précédemment mises en œuvre. Les personnes interrogées ont indiqué qu'elles avaient économisé des centaines de milliers de dollars par an sur les IPS autonomes, des millions de dollars en évitant le coût lié au remplacement de leurs solutions de sécurité existantes, et 25 % de coûts supplémentaires car Cisco Secure Firewall fournissait le même niveau de protection avec moins de pare-feux.

Bénéfices non quantifiés. Les bénéfices non quantifiés dans le cadre de cette étude sont les suivants :

- **Amélioration de la productivité et de la sécurité des VPN.** Cisco Secure Firewall a également permis d'améliorer la productivité et la sécurité des VPN d'accès à distance grâce à l'équilibrage des charges, à l'authentification locale et à l'authentification multicertificat. Les utilisateurs finaux ont établi de meilleures connexions via le VPN, tandis que les entreprises ont pu mieux contrôler l'accès.
- **Amélioration des opérations pour le travail à domicile.** Les contrôles de Cisco Secure Firewall ont également contribué au maintien des activités lorsque l'utilisation du VPN a explosé et que les employés ont fait la transition vers le travail à domicile. Les professionnels des réseaux ont pu tirer parti de la limitation du débit et des améliorations en matière de redondance pour améliorer l'expérience et la productivité des employés, même lors des pics de demande.
- **Facilité de transition vers le cloud.** Enfin, les personnes interrogées ont indiqué que Cisco Secure Firewall avait facilité la concrétisation de leurs initiatives de transition vers le cloud, en fournissant une plateforme qui protège le trafic au sein des sites, entre les sites, et entre l'entreprise et plusieurs plateformes cloud. Plus précisément, Cisco fournit des politiques normalisées et des moyens validés pour déployer Secure Firewall via les marchés de plateformes cloud.

Coûts. Les coûts en valeur actuelle avec ajustement des risques sont les suivants :

- **Coûts de licence.** Bien que les coûts de licence aient été les coûts les plus élevés encourus par les entreprises des personnes interrogées, la mise en place d'un contrat Cisco Enterprise Agreement a permis d'économiser des centaines de milliers de dollars sur des fonctionnalités et des solutions supplémentaires dont les entreprises ne disposaient pas auparavant, mais qui ont permis de renforcer davantage leur sécurité. Les droits de licence SecureX sont inclus dans Secure Firewall.
- **Coûts de mise en œuvre, de création de politiques et de formation.** Les personnes interrogées ont fait état de coûts internes pour la mise en œuvre et le déploiement des pare-feux et pour la création de leurs politiques. Le temps de déploiement des pare-feux est estimé à 6 heures par site, tandis que la création des politiques prend environ 30 heures. SecureX nécessite 20 heures de travail supplémentaires pour sa mise en œuvre et 100 heures par an pour sa gestion de manière continue. Certaines personnes interrogées ont également noté la nécessité de former leurs professionnels de la sécurité et des réseaux à l'utilisation de Cisco Secure Firewall et de Firewall Management Center. Les coûts internes de la formation s'élèvent à 2 heures par employé formé, sachant que les personnes interrogées ont indiqué qu'elles avaient tiré parti des vidéos de formation accessibles au public, présentées par des experts en sécurité informatique de Cisco.

Les entretiens avec les décideurs et l'analyse financière ont montré que l'entreprise de référence réalisait 18,59 millions de dollars de bénéfices sur trois ans pour des coûts de 6,30 millions de dollars, ce qui représente une valeur actuelle nette (VAN) de 12,29 millions de dollars et un ROI de 195 %.

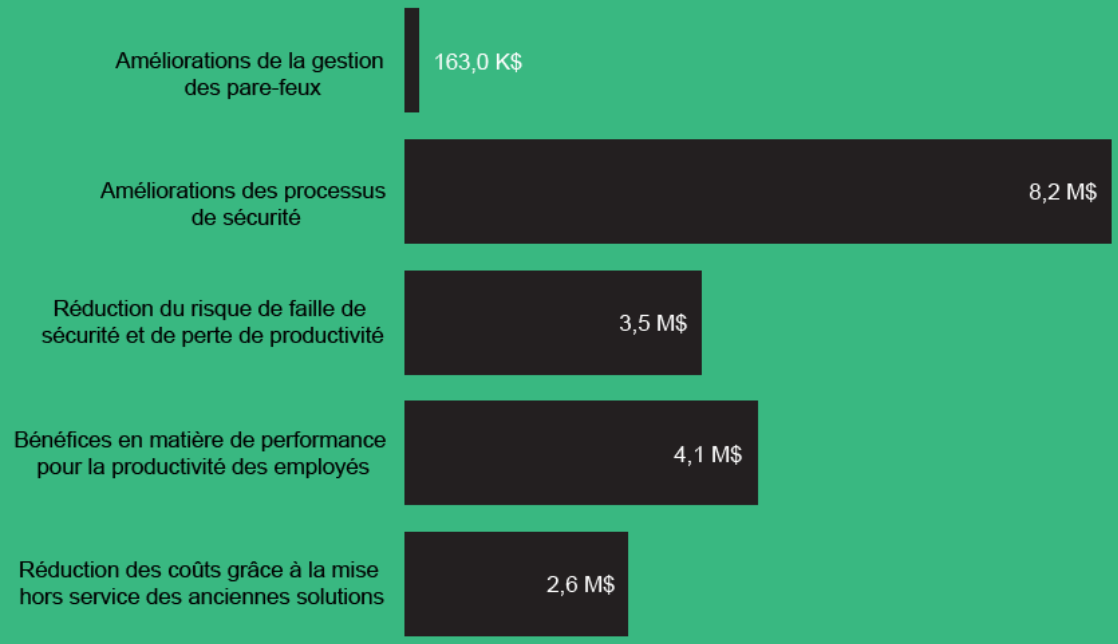
ROI
195 %

BÉNÉFICES EN VA
18,59 M$

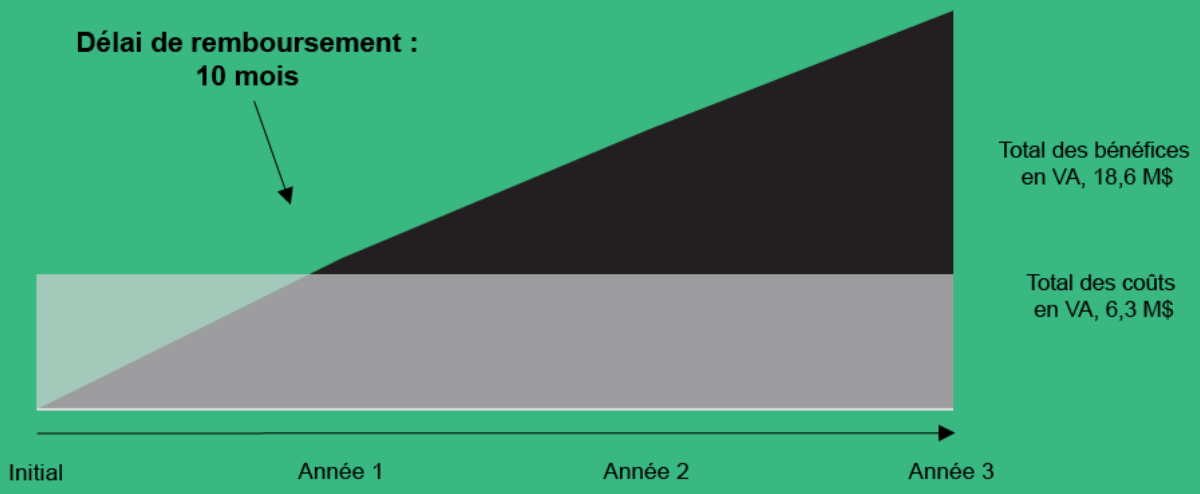
VAN
12,29 M$

DÉLAI DE REMBOURSEMENT
10 mois

Bénéfices (sur trois ans)



Bilan financier



CADRE DE REFERENCE ET METHODOLOGIE TEI

À partir des informations collectées lors de ces entretiens, Forrester a créé un cadre de référence Total Economic Impact™ pour les entreprises qui envisagent d'investir dans Cisco Secure Firewall.

L'objectif de ce cadre est d'identifier les différents facteurs (coûts, bénéfices, flexibilité et risques) qui affectent la décision d'investissement. Forrester a utilisé une approche en plusieurs étapes pour évaluer l'impact que Secure Firewall peut avoir sur une entreprise.

AVERTISSEMENTS

Les lecteurs doivent être avisés de ce qui suit :

L'étude est commandée par Cisco et réalisée par Forrester Consulting. Elle n'est pas destinée à être utilisée comme une analyse concurrentielle.

Forrester ne fait aucun postulat concernant le retour sur investissement que d'autres entreprises pourraient obtenir. Forrester recommande vivement aux lecteurs d'utiliser leurs propres estimations dans les limites du cadre de référence fourni dans l'étude pour déterminer la pertinence d'investir dans Secure Firewall.

Cisco a relu l'étude et fourni des commentaires à Forrester, mais Forrester garde le contrôle éditorial de l'étude et de ses conclusions et n'accepte pas de modifications de l'étude qui contrediraient les conclusions de Forrester ou occulteraient le propos de l'étude.

Cisco a fourni les noms des clients pour les entretiens, mais n'a pas participé a ces entretiens.

VÉRIFICATION NÉCESSAIRE

Entretien avec les parties prenantes de Cisco et les analystes de Forrester pour recueillir des données relatives à Secure Firewall.

ENTRETIENS AVEC DES DÉCIDEURS

Enquête auprès de dix décideurs d'entreprises qui utilisent Secure Firewall pour obtenir des données sur les coûts, les bénéfices et les risques.

ENTREPRISE DE RÉFÉRENCE

Nous avons conçu une entreprise de référence d'après les caractéristiques des entreprises interrogées dans le cadre de l'enquête.

CADRE DE RÉFÉRENCE DU MODÈLE FINANCIER

Nous avons créé un modèle financier représentatif des entretiens à l'aide de la méthodologie TEI, puis nous l'avons ajusté en fonction des risques en nous appuyant sur les questions et préoccupations des décideurs.

ÉTUDE DE CAS

Nous avons utilisé quatre éléments fondamentaux du TEI pour modéliser l'impact de l'investissement : bénéfices, coûts, flexibilité et risques. Compte tenu de la sophistication croissante des analyses du ROI concernant les investissements informatiques, la méthodologie TEI de Forrester offre un panorama complet de l'impact économique total des décisions d'achat. Veuillez vous reporter à l'Annexe A pour en savoir plus sur la méthodologie TEI.

Le parcours client avec Cisco Secure Firewall

Facteurs déterminant l'investissement dans Secure Firewall

Décideurs interrogés

Personne interrogée	Secteur	Région	Nombre total d'employés
Responsable des services d'ingénierie	Services informatiques	Amérique du Nord	750
Ingénieur principal des infrastructures	Services financiers	Amérique du Nord	2 800
Manager assistant des services de télécommunications et de téléphonie	Services financiers	Amérique du Nord	2 800
Ingénieur Senior Cybersécurité	Services de sécurité	Amérique du Nord	3 000
Ingénieur Senior Réseau	Fabrication	Monde	5 500
Responsable Senior Ingénierie des Réseaux	Technologies	Monde	40 000
Ingénieur Senior Sécurité	Technologies	Monde	40 000
Responsable Opérations de Sécurité	Enseignement	Amérique du Nord	46 000
Architecte de l'infrastructure du personnel	Industriel	Monde	205 000
Ingénieur Senior Réseau	Technologies	Monde	275 000

PRINCIPAUX DEFIS

Avant de déployer Cisco Secure Firewall et Firewall Management Center, les entreprises des personnes interrogées utilisaient principalement des appliances basées sur les pare-feux traditionnels ASA 5500-X pour protéger leurs environnements. Certaines personnes interrogées étaient passées des pare-feux traditionnels basés sur les ASA aux premiers pare-feux basés sur FTD il y a plusieurs années et ont indiqué avoir bénéficié d'avantages supplémentaires après la mise à niveau vers la dernière version de FTD sur Cisco Secure Firewall et Firewall Management Center.

Les personnes interrogées ont noté comment leurs organisations étaient aux prises avec des défis communs, notamment :

- **Visibilité limitée.** Les personnes interrogées ont noté que leurs environnements précédents, qui reposaient sur des pare-feux basés sur les ASA 5500-X, offraient une visibilité limitée de leur sécurité globale. L'une des raisons était le manque d'intégration. Dans les environnements précédents, il était difficile pour les entreprises interrogées d'intégrer diverses solutions de sécurité pour établir une gestion unifiée et des politiques cohérentes, tout en obtenant une unique version de référence. Une autre raison de la visibilité limitée était que les anciens environnements s'appuyaient sur les inspections de port comme point de vue central sur le réseau. Les personnes interrogées ont indiqué que cela les empêchait d'examiner les données en profondeur, avec une visibilité limitée des applications et un contexte historique restreint.

> **« Nous manquions auparavant de capacités telles que le contrôle moderne des applications. Nous ne pouvions pas savoir comment nos utilisateurs utilisaient le réseau et ne pouvions pas répondre à cette utilisation de manière adéquate. »**
> *Responsable Opérations de Sécurité, éducation*

- **Coûts élevés en termes de temps pour mettre en œuvre et gérer les pare-feux.** Les personnes interrogées ont également noté que le déploiement et la gestion de leurs anciens pare-feux prenaient beaucoup de temps. Cela s'explique en grande partie par l'impossibilité d'envoyer des mises à jour à plusieurs équipements à la fois. Le responsable opérations de sécurité dans le secteur de l'éducation a estimé que le déploiement d'une simple règle de pare-feu prenait auparavant entre 45 minutes et une heure. En outre, les personnes interrogées ont noté que le manque de visibilité de leurs anciens environnements signifiait qu'elles passaient un temps excessif à corréler les données entre différents systèmes pour confirmer le niveau de sécurité.

« La facilité d'administration et d'intégration a été l'un des avantages de Cisco. Nous bénéficions également d'un enrichissement des données car les différents systèmes s'alimentent plus facilement les uns les autres. Nous avons également mis en place des réponses autonomes à certaines menaces. Nous ne pouvions rien faire de tout cela auparavant. »
Ingénieur Senior Cybersécurité, services de sécurité

- **Mauvaise performance.** Les personnes interrogées ont également noté que leurs anciens systèmes souffraient de mauvaises performances. Par exemple, le responsable opérations de sécurité dans le secteur de l'éducation a déclaré que, lorsque la charge de leur réseau et de leur infrastructure de sécurité montait en flèche, leurs anciennes solutions « tombaient en panne, redémarraient constamment et perdaient des paquets. » Cela allait jusqu'à avoir un impact sur la productivité, car « les professeurs qui utilisaient le réseau pour diffuser une vidéo ou faire une démonstration en classe ne pouvaient pas le faire. »
- **Gestion des fournisseurs.** Enfin, les clients ont fait remarquer que le fait d'avoir plusieurs fournisseurs dans leur ancien environnement créait des problèmes de gestion des fournisseurs. L'ingénieur en charge de l'infrastructures de l'entreprise de services financiers a noté : « Avec plusieurs fournisseurs, tout devait être fait plusieurs fois, en accédant à plusieurs plans de contrôle pour appliquer les mêmes changements ou mises à jour sur les systèmes différents. »

ENTREPRISE DE REFERENCE

À partir des entretiens, Forrester a établi un cadre de référence TEI, une entreprise de référence et une analyse de son ROI qui montre les domaines touchés sur le plan financier. L'entreprise de référence est représentative des neuf décideurs d'entreprise interrogés par Forrester. Elle est utilisée pour présenter l'analyse financière agrégée dans la prochaine section. L'entreprise de référence présente les caractéristiques suivantes :

Description de l'entreprise de référence. L'entreprise de référence est une entreprise technologique B2B dont le chiffre d'affaires annuel s'élève à 5 milliards de dollars et qui compte 16 000 employés. Elle sert des clients dans le monde entier. L'entreprise a besoin d'une haute disponibilité dans ses centres de données pour garantir aux clients un accès constant aux données qui y sont stockées. Ces centres de données nécessitent également une sécurité renforcée pour protéger les données sensibles des clients contre les accès indésirables ou les attaques. En plus des centres de données, l'entreprise s'oriente vers une approche plus distribuée avec l'utilisation du multicloud. En outre, l'entreprise utilise également des pare-feux sécurisés pour protéger ses sites périphériques/succursales.

Caractéristiques du déploiement. L'entreprise de référence a déjà investi dans des pare-feux Cisco de nouvelle génération. Les deux tiers de son parc de pare-feux sont composés d'équipements Cisco Firepower, tandis qu'un tiers est composé de pare-feux ASA 5500-X. Elle procède actuellement à la transition de l'ensemble de ses 102 pare-feux de bureaux à domicile, de centres de données et de bureaux principaux vers la dernière version de Cisco Secure Firewall, en mettant à jour ses 68 équipements Firepower et en remplaçant ses 34 équipements ASA. Certaines personnes interrogées ont choisi de mettre à jour les appareils traditionnels existants avec le logiciel FTD sans changer leur matériel. Elle déploie également des pare-feux virtuels Cisco Secure Firewall dans ses centres de données pour gérer le trafic est-ouest entre les centres de données et les succursales, ainsi que le trafic entre les centres de données et plusieurs plateformes de cloud public. Elle profite de la disponibilité de SecureX dans sa licence Secure Firewall pour améliorer encore le travail d'investigation et de réponse aux menaces de son équipe de sécurité.

Hypothèses principales

- **5 G$ de chiffre d'affaires**
- **16 000 employés**
- **Remplacement de 34 pare-feux ASA**
- **Mise à jour de 68 pare-feux Firepower vers la dernière version de Cisco Secure Firewall**

Analyse des bénéfices

Données sur les bénéfices quantifiés appliquées à l'entreprise de référence

Total des bénéfices

Réf.	Bénéfice	Année 1	Année 2	Année 3	Total	Valeur actuelle
Atr	Amélioration de la gestion des pare-feux	134 951 $	25 556 $	25 556 $	186 064 $	163 005 $
Btr	Amélioration des processus de sécurité	2 669 879 $	3 685 484 $	3 685 484 $	10 040 848 $	8 241 976 $
Ctr	Réduction du risque de faille de sécurité et de perte de productivité	1 291 446 $	1 393 402 $	1 520 848 $	4 205 696 $	3 468 249 $
Dtr	Bénéfices en matière de performance pour la productivité des employés	1 656 403 $	1 656 403 $	1 656 403 $	4 969 210 $	4 119 230 $
Etr	Réduction des coûts grâce à la mise hors service des anciennes solutions	1 985 115 $	503 513 $	503 513 $	2 992 142 $	2 599 074 $
	Total des bénéfices (ajusté en fonction des risques)	7 737 795 $	7 264 360 $	7 391 805 $	22 393 959 $	18 591 534 $

AMELIORATION DE LA GESTION DES PARE-FEUX

Preuves et données. Les décideurs interrogés ont fait état d'un gain de temps et d'une réduction des coûts liés à la gestion des pare-feux après le déploiement de Cisco Secure Firewall, qu'il s'agisse du remplacement de pare-feux existants ou de la mise à jour d'anciennes versions de Firepower Threat Defense. Une bonne partie de ces améliorations est due au fait que Firewall Management Center a aidé les professionnels des réseaux en fournissant une gestion centralisée des pare-feux via une unique interface qui leur permet d'apporter des changements à de nombreux équipements.

« FMC nous offre un seul outil pour gérer et mettre à niveau les pare-feux, au lieu d'aller et venir constamment entre différents pare-feux comme nous le faisions auparavant. »
Responsable des services d'ingénierie, services informatiques

Les entreprises des personnes interrogées ont fait part des économies de temps et de coûts liées au déploiement des pare-feux. Avec les pare-feux traditionnels ASA, les personnes interrogées ont noté que le déploiement des pare-feux prenait beaucoup de temps, car il fallait rédiger des règles de pare-feu spécifiques à chaque cas d'utilisation et les mettre en place manuellement dans les différentes politiques existantes sur les pare-feux.

« Cisco Secure Firewall nous a permis de monter en puissance et de déployer rapidement de nouveaux pare-feux. Nous n'avons pas eu à augmenter le nombre d'employés avec ces nouveaux pare-feux. »
Responsable Senior Ingénierie des Réseaux, technologie

Après le passage à Cisco Secure Firewall et Firewall Management Center, les personnes interrogées ont noté un gain de temps de 30 à 40 % dans le déploiement des pare-feux. La réduction du temps était attribuable à la

capacité d'automatiser le déploiement de Cisco Secure Firewall. Par exemple, le responsable senior ingénierie des réseaux dans le secteur technologique a déclaré : « Nous avons automatisé le déploiement avec Cisco Secure Firewall. Nous avons un process automatisé pour envoyer l'équipement, définir les adresses IP, configurer le châssis et appliquer les politiques. »

« L'automatisation intégrée nous fait gagner le plus de temps. Même pour les mises à niveau. Je n'ai plus à attendre et à surveiller le processus de mise à niveau comme je devais le faire avec les ASA. Je peux m'absenter, et Firepower m'avertit si le système ne revient pas en ligne dans un délai suffisant. »
Responsable Senior Ingénierie des Réseaux, technologie

L'automatisation a également aidé les personnes interrogées lorsqu'il était question de gérer et de maintenir leurs pare-feux Cisco Secure Firewall après le déploiement. Cisco Secure Firewall est livré avec des mises à niveau automatiques intégrées. Les personnes interrogées ont indiqué que la mise à niveau des pare-feux ASA pouvait prendre plusieurs heures, passant d'un pare-feu à l'autre, téléchargeant les fichiers de mise à jour et redémarrant les systèmes. En utilisant Cisco Secure Firewall et Firewall Management Center, les personnes interrogées ont déclaré qu'il suffisait de cliquer sur l'interface pour mettre à niveau les pare-feux, puis de vérifier au bout de 30 minutes si les mises à niveau avaient réussi.

« Nous constatons des économies de 60 à 70 % sur la gestion des politiques après le passage des ASA à Cisco Secure Firewall. »
Responsable des services d'ingénierie, services informatiques

Avec Cisco Secure Firewall et Firewall Management Center, les personnes interrogées ont noté que les politiques pouvaient être organisées en catégories et en zones sans avoir besoin de longues listes de contrôle d'accès (ACL) grâce à un système orienté objet. Les politiques peuvent également être déployées et mises à jour automatiquement. Inutile de mettre à jour manuellement chaque appareil.

« Cisco Secure Firewall déploie automatiquement 90 % des politiques pour vous. Nous ne sommes plus confrontés à des configurations ponctuelles. »
Responsable Senior Ingénierie des Réseaux, technologie

Les personnes interrogées ont noté des gains de temps supplémentaires après avoir effectué une mise à niveau de l'ancien FTD vers le nouveau FTD avec Cisco Secure Firepower. Par exemple, l'ingénieur principal des infrastructures du secteur des services financiers a noté qu'avec les anciens FTD, le déploiement des politiques prenait entre 10 et 15 minutes, mais qu'avec les FTD mis à niveau, les temps de déploiement sont tombés à environ 3 minutes.

« La gestion des politiques avec Cisco Secure Firewall est simple et facile. L'interface graphique de Firewall Management Center est légère, propre et intuitive. »
Responsable Senior Ingénierie des Réseaux, technologie

L'une des personnes interrogées n'utilisait pas Firewall Management Center, mais le logiciel de gestion en ligne SaaS (software-as-a-service) Cisco Defense Orchestrator (CDO). En ce qui concerne CDO, l'équipe d'architecte en charge de l'infrastructure dans le secteur industriel a déclaré : « L'adoption de CDO s'est faite sans difficulté. Comme nos ingénieurs étaient déjà familiarisés avec [Cisco Security Manager (CSM)], ils pouvaient déjà utiliser l'interface ligne de commande et créer des macros. C'était beaucoup plus facile que de passer à un autre fournisseur où il aurait été plus compliqué d'apprendre les nouveaux concepts sur les couches supérieures. »

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- Trente-quatre pare-feux traditionnels ASA 5500-X sont remplacés par des pare-feux Cisco Secure Firewall.
- L'entreprise de référence économise 55 heures de travail qu'il faudrait pour déployer et créer des politiques pour chaque pare-feu traditionnel remplacé.
- L'entreprise de référence évite 90 % des 30 minutes qu'il fallait auparavant consacrer à la mise à niveau de chaque pare-feu chaque trimestre.
- L'entreprise de référence met à jour une politique de pare-feux en moyenne une fois par jour. En passant à Cisco Secure Firewall, cela évite 95 % de l'heure qu'il fallait auparavant pour effectuer chacune de ces mises à jour.
- Le taux horaire moyen toutes charges comprises d'un professionnel des opérations de sécurité réseau (NetSecOps) est de 65 $.
- Soixante-huit pare-feux FTD sont mis à niveau vers la dernière version de Cisco Secure Firewall. Pour chaque mise à jour quotidienne de politique, l'entreprise de référence économise 80 % du temps qu'elle prenait sur les pare-feux FTD de première génération.
- De plus, l'entreprise de référence économise 80 % du temps nécessaire à la mise à jour des politiques de pare-feu virtuel.

Risques. Les améliorations de la gestion des pare-feux peuvent varier en fonction des facteurs suivants :

- Le type et le nombre de pare-feux existants.
- Le nombre de pare-feux remplacés par des pare-feux Cisco Secure Firewall et le rythme de ce déploiement.
- La décision de déployer des pare-feux virtuels dans les centres de données pour gérer le trafic est-ouest et le trafic du cloud public.

Résultats. Pour tenir compte de ces risques, Forrester a réduit ce bénéfice de 10 %, ce qui a donné une valeur actuelle (VA) ajustée en fonction des risques (taux d'actualisation de 10 %) d'environ 163 000 dollars sur trois ans.

Amélioration de la gestion des pare-feux					
Réf.	**Métrique**	**Source**	**Année 1**	**Année 2**	**Année 3**
A1	Nombre de pare-feux de nouvelle génération qui remplacent les pare-feux traditionnels	Entreprise de référence ; 1/3 du total de 102	34	0	0
A2	Heures économisées pour le déploiement de chaque pare-feu	Entretiens	55,00	55,00	55,00
A3	Heures économisées pour mettre à jour chaque pare-feu ASA	90 % * 17 heures par trimestre	61,2	61,2	61,2
A4	Heures économisées pour mettre à jour manuellement les politiques pour les pare-feux ASA	95 % * 1 heure, une fois par jour * 33 % de l'environnement	114	114	114
A5	Taux horaire pour un professionnel NetSecOps	Entreprise de référence	65 $	65 $	65 $
A6	Sous-total : réduction du temps de déploiement et de mise à niveau vers les pare-feux de nouvelle génération à partir des anciens pare-feux de couche 4	((A1*A2)+(A3+A4))*A5	132 938 $	11 388 $	11 388 $
A7	Nombre de pare-feux FTD mis à jour	Entreprise de référence ; 2/3 du total de 102	68	68	68
A8	Heures requises précédemment pour le déploiement des politiques avec les anciens FTD	Entretiens	0,25	0,25	0,25
A9	Réduction du temps de déploiement des politiques grâce à la mise à niveau vers un FTD récent.	Entretiens ; de 15 minutes à 3 minutes	80 %	80 %	80 %
A10	Sous-total : réduction du temps de déploiement des politiques sur Firepower par rapport aux anciens pare-feux de couche 7	365*A8*A9*A5*A7/102	3 163 $	3 163 $	3 163 $
A11	Nombre total de pare-feux virtuels	Entreprise de référence	100	100	100
A12	Heures annuelles économisées pour mettre à jour les politiques des pare-feux virtuels	80 % * 266 heures par an	213	213	213
A13	Sous-total : réduction du temps consacré à la gestion des pare-feux virtuels	A12*A5	13 845 $	13 845 $	13 845 $
At	Amélioration de la gestion des pare-feux	A6+A10+A13	149 946 $	28 396 $	28 396 $
	Ajustement en fonction des risques	↓10 %			
Atr	Amélioration de la gestion des pare-feux (ajustée en fonction des risques)		134 951 $	25 556 $	25 556 $
	Total sur trois ans : 186 064 $		**Valeur actuelle sur trois ans : 163 005 $**		

AMELIORATION DES PROCESSUS DE SECURITE

Preuves et données. Le déploiement de Cisco Secure Firewall et l'utilisation de FMC ont également aidé les personnes interrogées à rationaliser les processus de sécurité. Les décideurs ont noté que les équipements ASA nécessitaient des outils multiples et distincts pour suivre et journaliser les événements sur les pare-feux. Avec FMC, les données de Cisco Secure Firewall ont été regroupées en un seul endroit où les indicateurs de compromission (IOC) et les intrusions bloquées pouvaient être suivis ou remontés de manière cohérente vers une solution de gestion des informations et des événements de sécurité

> **« Les investigations de sécurité donnaient l'impression de construire un puzzle avec une seule pièce. »**
> *Responsable Opérations de Sécurité, éducation*

(SIEM). Grâce à FMC, les personnes interrogées ont pu examiner les connexions, les événements et la télémétrie dans leur ensemble, de manière plus corrélée, sur l'ensemble du réseau.

Grâce à la consolidation via le Firewall Management Center, les personnes interrogées ont déclaré avoir réduit les coûts en temps des enquêtes de sécurité. Par exemple, l'ingénieur senior cybersécurité dans le secteur des services de sécurité a constaté une réduction du temps d'investigation de plusieurs heures à 3 ou 5 minutes grâce à Secure Firewall et de Firewall Management Center. Auparavant, cette personne interrogée a indiqué qu'elle devait passer par plusieurs systèmes, dont un SIEM et une console de messagerie, pour se connecter et coordonner les données. Maintenant, ils peuvent se connecter à FMC et rechercher des IOC spécifiques dans cet environnement.

« Firewall Management Center agit comme une console unique pour gérer tous les pare-feux Cisco Secure Firewall. Il facilite l'administration et permet de gagner du temps pour investiguer et rassembler les événements, et pour prendre des décisions concernant les activités malveillantes. »
Responsable des services d'ingénierie, services informatiques

Les personnes interrogées ont également noté une réduction de leurs temps de réponse. Par exemple, le responsable opérations de sécurité dans le secteur de l'éducation a indiqué qu'il devait envoyer des tickets au support client plusieurs fois par semaine avant d'investir dans Cisco Secure Firewall. Le support client devait ensuite retrouver l'utilisateur et effectuer une recherche de logiciels malveillants, ce qui pouvait prendre des heures. Ensuite, l'équipe de la personne interrogée devait nettoyer le système ou même le réinitialiser. Ce processus peut prendre jusqu'à une journée entière. Avec Cisco Secure Firewall, cette personne interrogée envoie un ticket

« Nos anciens pare-feux nécessitaient des frais généraux importants pour gérer la réponse aux incidents de sécurité ; cela prenait beaucoup de temps et coûtait beaucoup d'argent. Avec Firepower, nous constatons des gains de temps massifs et avons beaucoup moins de réponses aux incidents à traiter, car davantage de menaces sont bloquées. »
Responsable Opérations de Sécurité, éducation

similaire une fois par mois et celui-ci va directement dans FMC pour résoudre le problème, ce qui prend environ une heure.

Les personnes interrogées qui sont passées d'une ancienne version de FTD à une version récente ont également constaté des avantages liés aux processus d'investigation de sécurité et de réponse aux incidents. Comme l'a indiqué l'ingénieur principal en infrastructures du secteur des services financiers, une ancienne version de FTD permettait déjà d'obtenir une vue d'ensemble des

« FMC nous donne une grande visibilité. Maintenant, avec cette visibilité, nous passons plus de temps à surveiller et à nous assurer que tout va bien. Mais nous consacrons toujours moins de temps qu'avant à la réponse aux incidents. »
Responsable Opérations de Sécurité, éducation

alertes de sécurité via Firewall Management Center, mais après la mise à jour, les définitions et les capacités se sont améliorées. Cette personne interrogée a également noté que les intégrations supplémentaires avec les produits Cisco, notamment AMP et Umbrella, offraient encore plus d'avantages grâce à une corrélation supplémentaire.

Les entreprises qui ont profité de l'intégration de SecureX avec leur licence Secure Firewall ont amélioré davantage l'efficacité opérationnelle de leurs équipes de sécurité grâce à la visibilité et à la personnalisation. Par exemple, le responsable opérations de sécurité dans le secteur de l'éducation a également noté que SecureX permettait de personnaliser et d'adapter les tableaux de bord, de sorte que son équipe obtenait non seulement une visibilité supplémentaire de l'environnement, mais montrait également aux différents utilisateurs les informations les plus importantes pour eux.

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- Total annuel des alertes de sécurité de 100 000.
- Vingt-six pour cent d'entre elles nécessitent l'attention d'un analyste sécurité.
- Soixante-dix pour cent des alertes qui nécessitent une attention doivent également faire l'objet d'une investigation.
- Cisco Secure Firewall et Firewall Management Center permettent d'économiser 49 % des 2,8 heures qu'il fallait auparavant pour investiguer les alertes.
- Dix pour cent des alertes qui nécessitent une investigation ont besoin d'une réponse.
- Cisco Secure Firewall et Firewall Management Center permettent d'économiser 83 % des 6 heures que prenait auparavant la réponse.
- SecureX permet des gains de temps supplémentaires dans les processus d'investigation et de réponse de 42 % au cours de l'Année 1 et de 77 % au cours des Années 2 et 3.

Risques. L'amélioration des processus de sécurité peut varier en fonction des facteurs suivants :

- Le nombre d'alertes annuelles, d'alertes qui nécessitent une attention, d'alertes qui nécessitent une investigation et d'alertes qui nécessitent une réponse.
- Le taux horaire toutes charges comprises des professionnels NetSecOps.

Résultats. Pour tenir compte de ces risques, Forrester a réduit cet avantage de 15 %, ce qui a donné une valeur actuelle ajustée en fonction des risques de plus de 8,2 millions de dollars sur trois ans.

Amélioration des processus de sécurité					
Réf.	**Métrique**	**Source**	**Année 1**	**Année 2**	**Année 3**
B1	Total des alertes annuelles	Entreprise de référence	100 000	100 000	100 000
B2	Alertes qui nécessitent l'attention des analystes	Études Forrester ; 26 %	26 000	26 000	26 000
B3	Pourcentage d'alertes qui nécessitent une investigation	Entretiens	70 %	70 %	70 %
B4	Nombre moyen d'heures requises auparavant pour investiguer	Entretiens	2,8	2,8	2,8
B5	Réduction du temps d'investigation grâce à FMC	Entretiens	49 %	49 %	49 %
B6	Alertes qui nécessitent une réponse	Entretiens	260	260	260
B7	Nombre moyen d'heures requises auparavant pour répondre	Entretiens	6	6	6
B8	Réduction du temps de réponse grâce à FMC	Entretiens	83 %	83 %	83 %
B9	Réduction supplémentaire du temps d'investigation et de réponse grâce à SecureX	Entretiens	42 %	77 %	77 %
B10	Taux horaire toutes charges comprises d'un professionnel de la sécurité	A5	65 $	65 $	65 $
Bt	Amélioration des processus de sécurité	((B2*B3*B4*B5)+(B6*B7*B8)+(B2*B3*B4*B5)+(B6*B7*B9))*B10	3 141 034 $	4 335 864 $	4 335 864 $
	Ajustement en fonction des risques	↓15 %			
Btr	Amélioration des processus de sécurité (ajustée en fonction des risques)		2 669 879 $	3 685 484 $	3 685 484 $
	Total sur trois ans : 10 040 848 $			**Valeur actuelle sur trois ans : 8 241 976 $**	

REDUCTION DU RISQUE DE COMPROMISSION MATERIELLE ET DE PERTE DE PRODUCTIVITE

Preuves et données. Les personnes interrogées ont également fait état de bénéfices financiers liés à la réduction du risque de faille de sécurité et des coûts de productivité associés après le déploiement de Cisco Secure Firewall.

L'amélioration du niveau de sécurité des entreprises des personnes interrogées s'explique notamment par la visibilité accrue qu'offrent Cisco Secure Firewall et Firewall Management Center. Par exemple, le responsable opérations de sécurité dans le secteur de l'éducation a fait remarquer : « Par rapport aux ASA traditionnels, Cisco Secure Firewall nous donne une meilleure visibilité. C'est d'autant plus important que les utilisateurs apportent un nombre croissant d'appareils mobiles sur notre réseau et accèdent à des services comme l'impression via le réseau. La modernisation vers Firepower nous offre une meilleure

« Nous avons constaté une amélioration considérable du nombre de menaces et d'IOC bloqués. C'est une différence de plusieurs ordres de grandeur. Avant, notre entreprise était en à risque chaque jour où nous n'utilisions pas Secure Firewall. Nous avons désormais une visibilité accrue, et les risques ont considérablement diminué. Nous sommes rassurés maintenant. »
Responsable des services d'ingénierie, services informatiques

visibilité et la possibilité de filtrer le trafic du réseau interne ainsi que le trafic nord-sud. »

L'amélioration du blocage automatique a également contribué à réduire le risque potentiel d'utilisation réussie d'une faille de sécurité. Le responsable senior ingénierie des réseaux dans le secteur technologique a noté : « Firepower est un leader du secteur des [systèmes de protection contre les intrusions (IPS)]. Nous avons été en mesure d'améliorer notre niveau de sécurité et de remédier aux problèmes dès leur apparition. Pour chaque incident potentiel auquel nous remédions rapidement, nous économisons de l'argent. » Ce même client a fait part d'une amélioration de 80 % du blocage en passant d'un système basé sur les ASA à Cisco Secure Firewall.

« Avec Secure Firewall, nous avons éliminé immédiatement 80 % de nos menaces sans avoir besoin d'effectifs supplémentaires. »
Responsable Senior Ingénierie des Réseaux, technologie

Plus important encore, les personnes interrogées ont également constaté une amélioration du blocage grâce à la mise à jour de leurs pare-feux FTD aux dernières versions. L'ingénieur réseau senior de l'entreprise technologique a indiqué que la mise à niveau vers la dernière version de FTD permettait un blocage automatisé supérieur de 10 à 15 % à celui des anciennes versions.

Cette même personne interrogée a également partagé une anecdote sur l'impact que pourrait avoir le blocage automatisé : « Nous avons eu une fois une compromission potentielle basée sur l'ingénierie sociale par le biais de laquelle un pirate a pu obtenir un jeton d'accès de 24 heures d'un utilisateur déjà authentifié. Lorsque le pirate a essayé d'utiliser [le jeton], les pare-feux sécurisés de Cisco nous ont sauvés. Nous avons pu contrôler le niveau de sécurité et vérifier si l'attaquant utilisait un équipement du parc de l'entreprise. Secure Firewall a automatiquement refusé au pirate l'accès au VPN. Sans cela, le pirate aurait eu accès à notre réseau d'entreprise, et je ne suis pas sûr de l'impact que cela aurait pu avoir sur nous. »

« Cisco Secure Firewall est un guichet unique. Il possède toutes les capacités d'intégration avec d'autres outils afin de fournir des données pertinentes pour aider à la sécurité. Il offre plusieurs possibilités permettant de répondre à des besoins variés en bande passante, et prend en charge la mise à l'échelle verticale et horizontale. Il dispose de toutes les fonctionnalités nécessaires pour faire face aux risques de sécurité actuels, et il s'améliore en permanence. »
Ingénieur réseau senior, Internet

L'ingénieur réseau senior de l'entreprise technologique a également noté un avantage en matière de sécurité que Secure Firewall apporte en permettant de gérer l'accès au niveau de l'application : « Nous avons constaté une utilisation massive de BitTorrent sur notre réseau invité. En tirant parti de FTD pour bloquer BitTorrent, non seulement nous empêchons les menaces potentielles pour les autres invités, mais nous avons également réduit l'utilisation des circuits d'environ 400 Mb/s. »

En complément de la détection et du blocage au niveau applicatif, les personnes interrogées ont noté que l'utilisation par Cisco Secure Firewall de flux de menaces automatisés basés sur Snort diminuait également le risque d'intrusion dans leur entreprise. L'ingénieur en charge des infrastructures d'une entreprise de services financiers a déclaré : « Nous voulions Cisco Secure Firewall pour la visibilité accrue et la réponse automatisée de Snort, qui recherche des éléments tels que les serveurs sans

correctifs exposés à Internet et bloque globalement le trafic malveillant. »

Les entreprises qui ont tiré parti de l'inclusion de SecureX dans leur licence Secure Firewall ont d'autant plus réduit le risque ainsi que le coût d'une intrusion. Par exemple, l'ingénieur en charge des infrastructures d'une entreprise de services financiers a noté que SecureX leur avait permis d'obtenir encore plus de visibilité pour identifier les problèmes de sécurité et déterminer l'origine détaillée des menaces potentielles.

« SecureX peut nous donner une vue unique de l'ensemble de notre environnement de sécurité. Avec FMC, nous avons une vue sur tous nos pare-feux, avec SecureX nous avons une vue globale sur la FMC, ainsi que sur toutes nos solutions de sécurité Cisco intégrées. »
Responsable Opérations de Sécurité, éducation

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- Un nombre antérieur de failles de sécurité de trois par an.
- La moyenne des coûts internes et externes combinés d'une faille de sécurité est de 968 480 $.
- Le pourcentage d'attaques externes, d'incidents internes et d'attaques/incidents qui impliquent des partenaires et des tiers est de 79 %.
- Cisco Secure Firewall et Firewall Management Center réduisent le risque de faille de sécurité de 80 % pour le pourcentage de l'entreprise précédemment couvert par les pare-feux ASA traditionnels.
- Cisco Secure Firewall et Firewall Management Center réduisent le risque de faille de sécurité de 15 % pour le pourcentage de l'entreprise précédemment protégée par les pare-feux basés sur FTD.
- Soixante-six pour cent des employés de l'entreprise de référence sont affectés par chaque faille de sécurité. Ils retrouvent 70 % de leur productivité grâce à la réduction des risques d'intrusion avec Cisco Secure Firewall et Firewall Management Center.
- Un taux horaire toutes charges comprises par employé non spécialiste de 40 $.

Risques. Le risque réduit d'une faille de sécurité peut varier en fonction des facteurs suivants :

- Le nombre de failles de sécurité annuelles actuellement constatées.
- Le total des coûts internes et externes d'une faille de sécurité.
- Le pourcentage d'attaques externes, d'incidents internes et d'attaques/incidents qui impliquent des partenaires et des tiers.
- Le type et le nombre de pare-feux existants.
- Le nombre d'employés touchés par une faille de sécurité, leur taux horaire toutes charges comprises, et leur capacité à récupérer leur productivité lorsque ces failles de sécurité sont réduites.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 15 %, et a ainsi obtenu une valeur actuelle ajustée en fonction des risques de près de 3,5 millions de dollars sur trois ans.

Réduction du risque de faille de sécurité et de perte de productivité					
Réf.	**Métrique**	**Source**	**Année 1**	**Année 2**	**Année 3**
C1	Nombre moyen de failles de sécurité	Études Forrester	3	3	3
C2	Coût moyen par faille de sécurité	Études Forrester	968 480 $	968 480 $	968 480 $
C3	Pourcentage d'attaques externes, d'incidents internes et d'attaques/incidents qui impliquent des partenaires et des tiers	Entretiens	79 %	79 %	79 %
C4	Pourcentage de l'entreprise qui passe des ASA à Firepower	Entreprise de référence	33 %	33 %	33 %
C5	Pourcentage de réduction des risques avec Firepower	Entretiens	80 %	80 %	80 %
C6	Pourcentage de l'entreprise qui passe d'une ancienne version de Firepower à une version mise à niveau de Firepower	Entreprise de référence	67 %	67 %	67 %
C7	Pourcentage de réduction des risques depuis la mise à jour de Firepower	Entretiens	15 %	15 %	15 %
C8	Réduction supplémentaire grâce à SecureX	Entretiens	14 %	18 %	23 %
C9	Sous-total : réduction du risque de faille de sécurité	(C1*C2*C3*(C4*C5+C6*C7))+(C1*C2*C3*C8)	1 162 951 $	1 254 763 $	1 369 528 $
C10	Nombre d'utilisateurs touchés par chaque faille de sécurité	Études Forrester	10 600	10 600	10 600
C11	Taux horaire moyen toutes charges comprises par employé non spécialiste	Entreprise de référence	40 $	40 $	40 $
C12	Gain de productivité	Entreprise de référence	70 %	70 %	70 %
C13	Sous-total : amélioration de la productivité grâce à la réduction du risque de faille de sécurité	(C1*C10*C11*C12*C3*(C4*C5+C6*C7))+(C1*C10*C11*C12*C3*C8	356 397 $	384 534 $	419 705 $
Ct	Réduction du risque de faille de sécurité et de perte de productivité	C9+C13	1 519 348 $	1 639 297 $	1 789 232 $
	Ajustement en fonction des risques	↓15 %			
Ctr	Réduction du risque de faille de sécurité et de perte de productivité (ajustée en fonction des risques)		1 291 446 $	1 393 402 $	1 520 848 $
	Total sur trois ans : 4 205 696 $		**Valeur actuelle sur trois ans : 3 468 249 $**		

BENEFICES EN MATIERE DE PERFORMANCE POUR LA PRODUCTIVITE DES EMPLOYES

Preuves et données. Cisco Secure Firewall a permis aux entreprises des personnes interrogées d'améliorer la productivité de leurs employés de deux manières : 1) en fournissant une visibilité et un contrôle au niveau des applications qui ont amélioré les performances du réseau et 2) en limitant les temps d'arrêt dus aux mises à jour des politiques.

Les personnes interrogées ont noté que les performances de leur réseau se dégradaient moins souvent après la mise en œuvre de Cisco Secure Firewall, grâce à sa capacité à contrôler l'accès au réseau au niveau de la couche applicative. Auparavant, les clients signalaient que leurs réseaux ralentissaient fréquemment et que les performances se dégradaient au point d'avoir un impact sur la productivité des employés en cas de forte demande d'applications spécifiques, notamment celles liées aux médias vidéo. Le responsable opérations de sécurité dans le secteur de l'éducation a partagé : « Même si le réseau ralentissait notablement tous les jours, la dégradation était si importante qu'elle affectait la productivité une fois toutes les deux semaines. Cela se produisait surtout lorsque nous avions un pic d'activité, par exemple lorsque des milliers d'utilisateurs regardaient une vidéo. »

Comme Cisco Secure Firewall permettait aux entreprises interrogées de définir des politiques de sécurité du réseau sur de multiples couches, y compris la couche applicative, les personnes interrogées avaient un contrôle plus granulaire sur les autorisations du réseau. En conséquence, ces entreprises ont pu mieux contrôler quelles applications pouvaient accéder à leurs réseaux et à quel moment, ce qui a permis d'éviter la surcharge du réseau par des applications à large bande passante, d'améliorer les performances du réseau et d'accroître la productivité de leurs employés.

« Cisco Secure Firewall nous donne une bien meilleure visibilité sur la façon dont le réseau est utilisé et la possibilité de contrôler cette utilisation. Nous avons actuellement 4 000 systèmes différents sous surveillance, donc si je le voulais, je pourrais voir combien [une application sociale populaire basée sur la vidéo] a été utilisée la semaine dernière. Nous pourrions établir des règles pour interdire ce type de trafic si nécessaire. »
Responsable Opérations de Sécurité, éducation

D'autres personnes interrogées ont indiqué que leurs entreprises avaient stimulé la productivité des employés en limitant l'impact négatif que les erreurs humaines dans la mise à jour des politiques pouvaient parfois créer. Par exemple, le responsable des services d'ingénierie de l'entreprise de services informatiques a noté que, comme les politiques pouvaient être créées et mises à jour beaucoup plus rapidement avec Firewall Management Center, ils recevaient également plus rapidement des retours sur le succès des mises à jour.

Avant que cette entreprise ne mette en œuvre Secure Firewall, il fallait 15 minutes pour mettre à jour une politique et 15 minutes supplémentaires pour savoir si elle était correctement définie. Si ce n'était pas le cas, il fallait encore 15 minutes supplémentaires pour mettre à jour la politique une deuxième fois. Parfois, une politique mise à jour de manière erronée peut avoir un impact négatif sur la productivité des employés, notamment dans les environnements de production.
Après la mise à niveau vers la dernière version de FTD avec Cisco Secure Firewall, le responsable des services d'ingénierie a remarqué que la réduction du temps de mise à jour et de retour des politiques à 3 minutes en sortie et 3 minutes en entrée a permis de réduire le temps total de mise à jour, de retour et de dépannage de 80 %, passant de 60 minutes à 12 minutes.

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- Il faut une heure entière pour corriger une politique mise à jour de manière erronée (15 minutes pour envoyer la mise à jour erronée, 15 minutes pour recevoir un retour d'information, et 30 minutes pour mettre à jour et recevoir un retour d'information une fois la correction effectuée).
- Cisco Secure Firewall et Firewall Management Center réduisent de 80 % le temps nécessaire à la correction des politiques erronées.
- On suppose que l'entreprise est affectée par des mises à jour erronées des politiques à hauteur de 2 % en moyenne.
- Une fois toutes les deux semaines environ, le réseau subissait des dégradations graves qui affectaient la productivité des employés pendant 20 minutes en moyenne.
- Trente-trois pour cent des employés que les pare-feux ASA traditionnels protégeaient étaient affectés par la dégradation du réseau.

Risques. Les bénéfices en matière de performance pour la productivité des employés peuvent varier en fonction des facteurs suivants :

- Le pourcentage d'employés affectés par des mises à jour de politiques erronées.
- La fréquence et la durée des dégradations du réseau ayant un impact sur la productivité des employés.
- Le nombre d'employés affectés par la dégradation du réseau.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 10 % et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de plus de 4,1 millions de dollars sur trois ans.

Bénéfices en matière de performance pour la productivité des employés

Réf.	Métrique	Source	Année 1	Année 2	Année 3
D1	Heures requises précédemment pour l'ajustement des politiques avec les anciennes versions de FTD	Entretiens	1	1	1
D2	Nouveau nombre d'heures pour ajuster les politiques avec le FTD mis à jour	Entretiens	0,2	0,2	0,2
D3	Nombre moyen d'employés affectés	Entreprise de référence	320	320	320
D4	Taux horaire moyen toutes charges comprises par employé non spécialiste	C10	40 $	40 $	40 $
D5	Taux de récupération de la productivité	Entreprise de référence	25 %	25 %	25 %
D6	Sous-total : gain de productivité obtenue suite aux retours d'information sur l'utilisation des politiques des anciennes versions	365*(D1-D2)*D3*D4*D5	934 400 $	934 400 $	934 400 $
D7	Fréquence de la dégradation des performances due à une utilisation abusive du réseau	Entretiens	26	26	26
D8	Durée moyenne de la dégradation des performances en heures	Entretiens	0,33	0,33	0,33
D9	Nombre d'employés affectés (migrations ASA uniquement)	Entreprise de référence	5 280	5 280	5 280
D10	Taux horaire moyen toutes charges comprises par employé non spécialiste	C11	40 $	40 $	40 $
D11	Taux de récupération de la productivité	Entreprise de référence	50 %	50 %	50 %
D12	Sous-total : amélioration de la productivité des employés utilisateurs finaux	D7*D8*D9*D10*D11	906 048 $	906 048 $	906 048 $
Dt	Bénéfices en matière de performance pour la productivité des employés	D6+D12	1 840 448 $	1 840 448 $	1 840 448 $
	Ajustement en fonction des risques	↓10 %			
Dtr	Bénéfices en termes de productivité des employés (ajustés en fonction des risques)		1 656 403 $	1 656 403 $	1 656 403 $
	Total sur trois ans : 4 969 210 $		**Valeur actuelle sur trois ans : 4 119 230 $**		

COUTS REDUITS ET EVITES DES ANCIENNES SOLUTIONS

Preuves et données. En migrant leur infrastructure de sécurité réseau vers la dernière version de Cisco Secure Firewall, les entreprises des personnes interrogées ont réduit et évité les coûts associés à leur ancienne infrastructure réseau. Il n'est pas surprenant que les personnes interrogées aient déclaré avoir évité les coûts liés au renouvellement des licences de leurs pare-feux traditionnels en ASA, ainsi que celles des anciens pare-feux en FTD, étant donné que Cisco Secure Firewall les a remplacés.

En plus du remplacement des pare-feux physiques et virtuels, les entreprises interrogées qui ont abandonné l'environnement en ASA ont déprovisionné leurs solutions IPS autonomes étant donné que Cisco Secure Firewall intègre cette fonctionnalité.

« Avec les pare-feux ASA traditionnels, nous devions également investir dans des unités IPS à placer entre les liens et le pare-feu. Avec Cisco Secure Firewall, l'IPS est intégré. Nous ne gérons plus deux solutions différentes avec deux écosystèmes différents, et nous ne dépendons plus des ingénieurs IPS. »
Responsable Senior Ingénierie des Réseaux, technologie

Plus important encore, les personnes interrogées ont constaté des économies supplémentaires lors de la mise à niveau des pare-feux de leurs entreprises des anciens FTD vers Cisco Secure Firewall. Grâce aux performances de ces nouveaux pare-feux, les personnes interrogées ont déclaré avoir besoin de 20 à 25 % de boîtiers en moins pour obtenir les mêmes résultats.

« En passant sur les nouvelles versions de FTD sur les Cisco Secure Firewall, nous avons constaté une meilleure efficacité de traitement. Cisco Secure Firewall a une efficacité supérieure de 20 à 25 % par rapport aux anciennes versions, ce qui signifie que nous avons besoin de moins de pare-feux. »
Ingénieur réseau senior, Internet

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- Une réduction des coûts de licences d'IPS de 171 600 $ par an grâce au remplacement des pare-feux ASA traditionnels par des pare-feux Cisco Secure Firewall.
- Économie de 20 % liée au support des licences IPS autonomes qui n'est plus à renouveler.
- Une réduction des coûts de gestion courante liés à l'IPS de 80 % de 30 minutes pour 2 ETP par semaine.
- Économie de 1,3 millions de dollars au cours de l'Année 1 liée au non remplacement des pare-feux existants.
- Coûts évités de remplacement des pare-feux virtuels de 300 000 $ par an.
- Coûts évités de 25 % de pare-feux physiques supplémentaires grâce à l'efficacité de Cisco Secure Firewall.

« Nous avons finalement abandonné nos appliances IPS, plus coûteuses et moins performantes, en déployant Cisco Secure Firewall. »
Ingénieur principal des infrastructures, services financiers

Risques. La réduction des coûts des anciennes solutions variera en fonction des facteurs suivants :

- Le nombre et le type de pare-feux existants.
- La possibilité de mettre hors service des solutions IPS autonomes.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice à la baisse de 10 %, et a ainsi obtenu une valeur actuelle ajustée en fonction des risques de près de 2,6 millions de dollars sur trois ans.

Réduction des coûts grâce à la mise hors service des anciennes solutions

Réf.	Métrique	Source	Année 1	Année 2	Année 3
E1	Réduction du coût des anciens IPS	Entretiens	171 600 $	171 600 $	171 600 $
E2	Réduction du coût des frais de maintenance	E1*20 %	34 320 $	34 320 $	34 320 $
E3	Réduction du coût de la gestion courante des anciens IPS	Entretiens	53 539 $	53 539 $	53 539 $
E4	Coût évité des pare-feux pour le cycle de remplacement	Entreprise de référence	1 616 980 $	300 000 $	300 000 $
E5	Coûts évités grâce à l'efficacité supplémentaire du pare-feu	Entreprise de référence	329 245 $	0 $	0 $
Et	Réduction des coûts grâce à la mise hors service des anciennes solutions	E1+E2+E3+E4+E5	2 205 684 $	559 459 $	559 459 $
	Ajustement en fonction des risques	↓10 %			
Etr	Réduction des coûts grâce à la mise hors service des anciennes solutions (ajustée en fonction des risques)		1 985 115 $	503 513 $	503 513 $
	Total sur trois ans : 2 992 142 $			**Valeur actuelle sur trois ans : 2 599 074 $**	

BENEFICES NON QUANTIFIES

Les clients ont identifié d'autres bénéfices, mais n'ont pu les quantifier :

- **Amélioration de la productivité et de la sécurité des VPN.** Les personnes interrogées ont également noté que Cisco Secure Firewall permettait d'améliorer la productivité et la sécurité des VPN d'accès à distance. Grâce à l'équilibrage de charges, Secure Firewall a réparti les sessions entre des appareils groupés, ce qui permet d'améliorer les performances, la résilience et la productivité des utilisateurs finaux. De même, l'authentification locale avec Secure Firewall a permis aux utilisateurs de rester productifs en cas d'inaccessibilité d'un serveur distant AAA. Pour des raisons de sécurité, Cisco Secure Firewall permet l'authentification multicertificat, de sorte que les entreprises s'assurent qu'un appareil distant ait été délivré par l'entreprise, en plus de valider l'utilisateur final lui-même.
- **Amélioration de la conformité.** Les personnes interrogées ont également déclaré que Cisco Secure Firewall et Firewall Management Center apportaient un bénéfice non quantifiable aux processus de conformité. L'ingénieur en chef des infrastructures de l'entreprise de services financiers a fait part du fait qu'avant le déploiement de Secure Firewall et FMC, il était plus difficile d'établir des rapports de conformité. Les anciennes solutions manquaient d'une fonctionnalité simplifiant le rapport. Cependant, Secure Firewall et FMC ont permis à leur entreprise d'exécuter des rapports qui englobaient davantage de composants et étaient plus détaillés quant aux activités et aux vues. Les personnes interrogées ont également indiqué que Cisco Secure Firewall prenait en charge la norme de chiffrement Transport Layer Security (TLS) 1.3. Par exemple, l'ingénieur réseau senior de l'entreprise Internet a pu noter que son équipe ne déchiffrait actuellement pas ces flux en raison de la charge administrative. Après avoir investi dans Cisco Secure Firewall, le déchiffrement du TLS 1.3 est devenu plus facile et plus efficace.

« Auparavant nous n'avions pas de rapports générés pour un grand nombre de différents éléments de configuration, mais maintenant nous pouvons obtenir une gamme diversifiée et détaillée de rapports, plus simplement. Par exemple, je viens de recevoir un rapport résumant tous les changements de contrôle d'accès que j'ai pu effectuer au cours de l'année dernière. Il montre le résultat de toutes les pages consultées, ainsi que les modifications apportées. »
Ingénieur principal des infrastructures, services financiers

- Amélioration **de l'expérience des employés.** Les personnes interrogées ont également noté que l'expérience des employés vis-à-vis de leur entreprise s'était améliorée. Par exemple, l'ingénieur réseau senior de l'entreprise Internet a déclaré : « Le fait de pouvoir mieux contrôler l'accès aux applications sur nos réseaux a amélioré la satisfaction des employés. Nos équipes informatiques locales avaient du mal à retracer certains utilisateurs pour leur demander d'arrêter d'utiliser certaines applications ou pour leur en bloquer l'accès. Avec Secure Firewall et FMC, nous pouvons désormais le faire à distance. »

FLEXIBILITE

L'intérêt de la flexibilité est propre à chaque client. Il existe de nombreux scénarios dans lesquels un client met Secure Firewall en œuvre, puis trouve par la suite d'autres possibilités d'utilisation et opportunités commerciales, notamment :

- **Intégrations supplémentaires de Cisco Security.** Outre les avantages de SecureX, les personnes interrogées ont noté que l'écosystème des offres de sécurité de Cisco offrait la flexibilité nécessaire pour renforcer davantage le niveau de sécurité de leur entreprise. Par exemple, le responsable des services d'ingénierie de l'entreprise de services informatiques a déclaré : « Cisco Security dispose d'une pile profonde de solutions de sécurité intégrées, ce que les autres fournisseurs n'arrivent pas à proposer. Il ne s'agit pas seulement de Secure Firewall, mais de tous les autres outils qui s'intègrent parfaitement et nous permettent de mieux construire nos défenses. »
- **Amélioration des opérations pour le travail à domicile.** Les contrôles de Cisco Secure Firewall ont également contribué au bon déroulement des opérations lorsque l'utilisation du VPN a explosé et que les employés ont fait la transition vers le télétravail. L'ingénieur réseau senior de l'entreprise Internet a déclaré : « Pendant la pandémie, nos connexions VPN simultanées sont passées d'une moyenne de 100 000 à près de 350 000 dans le monde. Afin de maintenir la viabilité de notre réseau, nous avons utilisé Cisco Secure Firewall pour fixer des limites de débit, ce qui a permis de lisser les opérations. »
- **Facilité de transition vers le cloud.** Enfin, les personnes interrogées ont déclaré que Cisco Secure Firewall avait facilité la réalisation de leurs initiatives cloud. Le responsable des services d'ingénierie de l'entreprise de services informatiques a déclaré : « nous avions besoin d'une plateforme unique pour atteindre les sites locaux, les sites distants et également le cloud, mais celle-ci devait être facile à déployer. D'ailleurs, avec les plateformes cloud il est possible de déployer une plateforme FTD, l'installer et la connecter directement au Firewall Management Center. La mise en place et le déploiement ont été très rapides. Et nous pouvions appliquer une politique normalisée à ces boîtiers. »

La flexibilité peut également être mesurée lors de son évaluation dans le cadre d'un projet spécifique (voir l'Annexe A pour plus de détails).

Analyse des coûts

Données sur les coûts quantifiés appliquées à l'entreprise de référence

Total des coûts							
Réf.	**Coût**	**Initial**	**Année 1**	**Année 2**	**Année 3**	**Total**	**Valeur actuelle**
Ftr	Coûts de licence	6 000 690 $	0 $	0 $	0 $	6 000 690 $	6 000 690 $
Gtr	Coûts de mise en œuvre, de création de politiques et de formation	278 220 $	7 924 $	7 924 $	7 924 $	301 990 $	297 924 $
	Total des coûts (ajusté en fonction des risques)	6 278 910 $	7 924 $	7 924 $	7 924 $	6 302 680 $	6 298 614 $

COUTS DE LICENCE

Preuves et données. Les clients ont déclaré encourir plusieurs coûts différents associés à leur investissement dans Secure Firewall, notamment :

- Les coûts des pare-feux physiques, qui varient en fonction du débit requis.
- Les pare-feux virtuels déployés dans le ou les centres de données pour gérer le trafic est-ouest.
- Les coûts des licences de protection contre les menaces, de défense contre les logiciels malveillants et de filtrage des URL.
- Les licences de Firewall Management Center.

« Nous avons eu du mal à trouver une autre option offrant une architecture, un ensemble d'outils et des fonctionnalités aussi complets que ceux de Cisco Secure Firewall, le tout dans un seul boîtier. Mais en plus, le rapport prix/performance était également convaincant. »
Ingénieur principal des infrastructures, services financiers

Les clients ont noté qu'ils ont pu déployer Cisco SecureX sans coût supplémentaire, car il était inclus dans leurs licences Secure Firewall.

Modélisation et hypothèses. Pour l'entreprise de référence, qui compte 100 bureaux et quatre centres de données physiques nécessitant une redondance, Forrester émet les hypothèses suivantes :

- Toutes les licences sont au prix catalogue pour une durée de trois ans.
- Le coût d'un pare-feu pour le siège social est de 328 443 $. Le siège social a besoin d'un grand pare-feu de classe entreprise, avec un débit pouvant atteindre 75 Gb/s.
- Le coût des pare-feux des centres de données est de 978 067 $. Dans chaque centre de données, l'entreprise de référence déploie un groupe de deux pare-feux physiques en cluster ou en haute disponibilité à l'intérieur du périmètre afin de gérer le trafic nord-sud entrant et sortant du centre de données.
- Le coût de 100 pare-feux virtuels est de 2 628 561 $. Ces pare-feux virtuels gèrent le trafic est-ouest au sein des centres de données ainsi qu'entre les centres de données et les plateformes de cloud public.
- Les pare-feux physiques et virtuels des centres de données disposent tous d'une licence supplémentaire de protection contre les menaces, moyennant un abonnement de trois ans. Cette licence offre une sécurité supplémentaire, notamment Snort 3, qui permet de mieux détecter et atténuer les indicateurs de compromission et le trafic malveillant.

- Le coût total de 60 pare-feux de succursales est de 1 848 160 $. Soixante bureaux ont besoin de pare-feux Secure Firewall dont le débit peut atteindre 1,9 Gb/s.
- Le coût total de 39 pare-feux de petites succursales est de 137 779 $. Les 39 bureaux restants n'avaient besoin que d'un débit allant jusqu'à 650 Mb/s.
- Tous les pare-feux de bureau disposent de licences supplémentaires pour la protection contre les menaces, la défense contre les logiciels malveillants et le filtrage des URL, moyennant un abonnement de trois ans.
- Firewall Management Center fait également l'objet d'une licence dont la taille est adaptée à la gestion de tous ces pare-feux. Le coût de Firewall Management Center est de 79 680 $.

Risques. Les coûts de licence de Cisco Secure Firewall et de Firewall Management Center varient en fonction des facteurs suivants :

- Le nombre de pare-feux virtuels souhaité.
- Le nombre de pare-feux de classe entreprise nécessaires.
- La taille et le nombre de centres de données et le besoin de haute disponibilité.
- La taille et le nombre de succursales.

Résultats. Comme Forrester a déterminé le prix de l'entreprise de référence directement avec Cisco, nous n'avons pas ajusté ce coût en fonction du risque, ce qui donne une VA totale sur trois ans (taux d'actualisation de 10 %) de 6 millions de dollars.

« Avec notre contrat de sécurité d'entreprise Cisco, notre coût total est moins élevé que ce qu'il serait à la carte. Bien que Firepower représente la majeure partie de ce coût, nous économisons des centaines de milliers de dollars en obtenant une protection supplémentaire avec des produits que nous n'avions pas auparavant. »
Responsable Opérations de Sécurité, éducation

Coûts des licences

Réf.	Métrique	Source	Initial	Année 1	Année 2	Année 3
F1	Coût des pare-feux virtuels	Cisco	2 628 561 $			
F2	Coût du pare-feu du siège social	Cisco	328 443 $			
F3	Coût des pare-feux physiques des centres de données	Cisco	978 067 $			
F4	Coût des pare-feux des petites succursales	Cisco	137 779 $			
F5	Coût des pare-feux des grandes succursales	Cisco	1 848 160 $			
F6	Coût de Firewall Management Center	Cisco	79 680 $			
Ft	Coûts de licence	F1+F2+F3+F4+F5+F6	6 000 690 $	0 $	0 $	0 $
	Ajustement en fonction des risques	0 %				
Ftr	Coût des licences (ajusté en fonction des risques)		6 000 690 $	0 $	0 $	0 $
	Total sur trois ans : 6 000 690 $			**Valeur actuelle sur trois ans : 6 000 690 $**		

COUTS DE MISE EN ŒUVRE, DE CREATION DE POLITIQUES ET DE FORMATION

Preuves et données. Les personnes interrogées ont déclaré avoir subi des coûts internes (temps et main-d'œuvre) liés au déploiement et à la mise en œuvre de pare-feux dans leurs centres de données et leurs bureaux. Le premier de ces coûts concernait le déploiement physique des pare-feux sur chaque site. Le second était lié à la mise en œuvre de ces pare-feux, qui impliquait la création et le déploiement de politiques appropriées sur chaque groupe de pare-feux.

« La mise en œuvre et le déploiement ont été vraiment rapides et relativement simples. La migration a duré trois semaines, car nous avions déjà un design en place et savions comment tout mettre en marche. »
Responsable Opérations de Sécurité, éducation

Enfin, les décideurs interrogés ont également constaté des coûts en temps liés à la formation. La formation a duré environ 2 heures pour chaque employé ayant besoin d'une telle formation pour déployer et gérer les pare-feux Cisco Secure Firewall. Certaines personnes interrogées ont indiqué qu'elles avaient tiré parti des vidéos de formation accessibles au public et présentées par des experts en sécurité de Cisco.

Modélisation et hypothèses. Pour l'entreprise de référence, Forrester émet les hypothèses suivantes :

- En moyenne, 6 heures de mise en œuvre sont nécessaires dans chacun des deux centres de données et des 100 bureaux.
- La création des politiques prend en moyenne 30 heures par pare-feu.
- SecureX nécessite 20 heures de travail pour sa mise en œuvre et 100 heures supplémentaires par an pour sa gestion de manière continue.
- Quinze employés ayant besoin d'une formation au départ et trois autres employés ayant besoin d'une formation chaque année en raison de la rotation du personnel.

Risques. Le coût de la mise en œuvre et de la création des politiques variera en fonction de divers facteurs :

- Le nombre de pare-feux Cisco Secure Firewall à déployer.
- Le nombre d'employés devant être formés au départ.
- Le taux de rotation du personnel.
- Le taux horaire toutes charges comprises des professionnels NetSecOps.

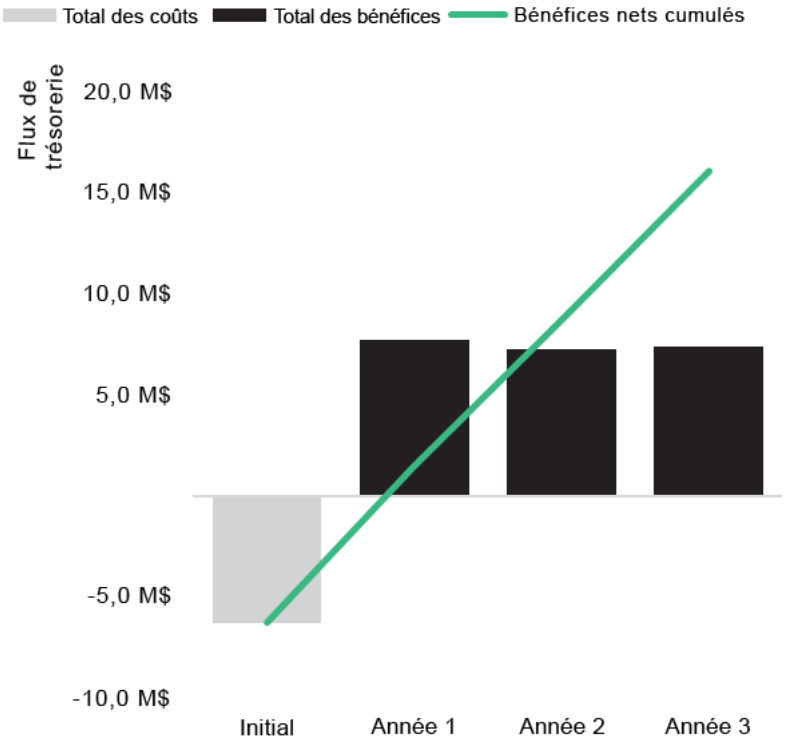
Résultats. Pour tenir compte de ces risques, Forrester a revu ce coût à la hausse de 15 % et obtenu une valeur actuelle (VA) ajustée en fonction des risques de moins de 298 000 dollars sur trois ans.

Coûts de mise en œuvre, de création de politiques et de formation						
Réf.	**Métrique**	**Source**	**Initial**	**Année 1**	**Année 2**	**Année 3**
G1	Sites à déployer	Entreprise de référence	102			
G2	Nombre moyen d'heures pour la mise en œuvre physique sur chaque site	Entreprise de référence	6			
G3	Heures pour la création des politiques	Entretiens	30			
G4	Heures pour la mise en œuvre et la gestion de SecureX	Entretiens	20	100	100	100
G5	Employés ayant besoin d'une formation	Entretiens	15	3	3	3
G6	Heures nécessaires pour la formation	Entretiens	2	2	2	2
G7	Taux moyen toutes charges comprises d'un professionnel NetSecOps	A5	65 $	65 $	65 $	65 $
Gt	Coûts de mise en œuvre, de création de politiques et de formation	((G1*(G2+G3))+,G4+(G5*G6))*G7	241 930 $	6 890 $	6 890 $	6 890 $
	Ajustement en fonction des risques	↑15 %				
Gtr	Coûts de mise en œuvre, de création de politiques et de formation (ajustés en fonction des risques)		278 220 $	7 924 $	7 924 $	7 924 $
	Total sur trois ans : 301 990 $		**Valeur actuelle sur trois ans : 297 924 $**			

Bilan financier

MESURES CONSOLIDEES SUR TROIS ANS ET AJUSTEES EN FONCTION DES RISQUES

Graphique des flux de trésorerie (ajustés en fonction des risques)



Les résultats financiers calculés dans les sections Bénéfices et Coûts peuvent être utilisés pour déterminer le retour sur investissement (ROI), la valeur actuelle nette (VAN) et la période de remboursement de l'entreprise de référence. Forrester estime que le taux d'actualisation annuel pour cette analyse s'élève à 10 %.

Ces valeurs de ROI, de VAN et de délai de remboursement, ajustées en fonction des risques, sont déterminées en appliquant des facteurs d'ajustement en fonction des risques aux résultats bruts de chaque section Bénéfices et Coûts.

Analyse des flux de trésorerie (estimations ajustées en fonction des risques)

	Initial	Année 1	Année 2	Année 3	Total	Valeur actuelle
Total des coûts	(6 278 910 $)	(7 924 $)	(7 924 $)	(7 924 $)	(6 302 680 $)	(6 298 614 $)
Total des bénéfices	0 $	7 737 795 $	7 264 360 $	7 391 805 $	22 393 959 $	18 591 534 $
Bénéfices nets	(6 278 910 $)	7 729 871 $	7 256 436 $	7 383 881 $	16 091 279 $	12 292 920 $
ROI						195 %
Délai de remboursement (mois)						10

Annexe A : Total Economic Impact

Total Economic Impact (TEI) est une méthodologie élaborée par Forrester Research qui améliore les processus décisionnels d'une entreprise en matière de technologies et permet aux fournisseurs de communiquer la proposition de valeur de leurs produits et services aux clients. Elle aide aussi les entreprises à démontrer, justifier et concrétiser la valeur réelle des initiatives IT auprès de leur direction et des autres parties prenantes.

L'APPROCHE TOTAL ECONOMIC IMPACT

Les bénéfices représentent la valeur apportée par le produit à l'entreprise. La méthodologie TEI mesure équitablement les bénéfices et les coûts, ce qui permet de réaliser une étude complète de l'impact de la technologie sur toute l'entreprise.

Les coûts tiennent compte de toutes les dépenses nécessaires pour obtenir la valeur ou les avantages attendus du produit. La catégorie de coûts du TEI correspond aux coûts différentiels par rapport à l'environnement existant pour déterminer les coûts récurrents associés à la solution.

La flexibilité désigne la valeur stratégique qui peut être obtenue pour un futur investissement en complément de l'investissement initial. La possibilité de tirer parti de ce bénéfice présente une VA qui peut être estimée.

Les risques mesurent l'incertitude des estimations des bénéfices et des coûts en considérant : 1) la probabilité que les estimations correspondent aux projections d'origine et 2) la probabilité que les estimations soient suivies dans le temps. Les facteurs de risque du TEI reposent sur une « distribution triangulaire ».

La colonne Investissement initial présente les coûts engagés à « l'instant 0 » ou au début de l'Année 1, et non actualisés. Tous les autres flux de trésorerie sont actualisés au taux d'actualisation en fin d'année. Les calculs de la VA sont effectués pour chaque estimation des coûts et des bénéfices totaux. Les calculs de la VAN qui figurent dans les tableaux de synthèse correspondent à la somme de l'investissement initial et des flux de trésorerie actualisés chaque année. Il est possible que les calculs des sommes et de la valeur actuelle des tableaux Total des bénéfices, Total des coûts et Flux de trésorerie ne s'additionnent pas parfaitement, puisque certains nombres sont arrondis.

VALEUR ACTUELLE (VA)

Valeur actuelle ou courante des estimations de coûts (actualisés) et de bénéfices à un taux d'intérêt donné (taux d'actualisation). La VA des coûts et des bénéfices entre dans la valeur actuelle nette totale des flux de trésorerie.

VALEUR ACTUELLE NETTE (VAN)

Valeur actuelle ou courante des futurs flux de trésorerie nets (actualisés) à un taux d'intérêt donné (taux d'actualisation). La VAN positive d'un projet indique normalement que l'investissement est recommandé, à moins que d'autres projets ne présentent des VAN supérieures.

RETOUR SUR INVESTISSEMENT (ROI)

Rentabilité attendue d'un projet, exprimée en pourcentage. Le ROI se calcule en divisant les bénéfices nets (déduction faite des coûts) par les coûts.

TAUX D'ACTUALISATION

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

DELAI DE REMBOURSEMENT

Seuil de rentabilité d'un investissement. C'est le moment où les bénéfices nets (bénéfices moins coûts) sont égaux à l'investissement ou au coût initial.

Annexe B : Notes de bas de page

[1] Total Economic Impact (TEI) est une méthodologie élaborée par Forrester Research qui améliore les processus décisionnels d'une entreprise en matière de technologies et permet aux fournisseurs de communiquer la proposition de valeur de leurs produits et services aux clients. Elle aide aussi les entreprises à démontrer, justifier et concrétiser la valeur réelle des initiatives IT auprès de leur direction et des autres parties prenantes.

FORRESTER®