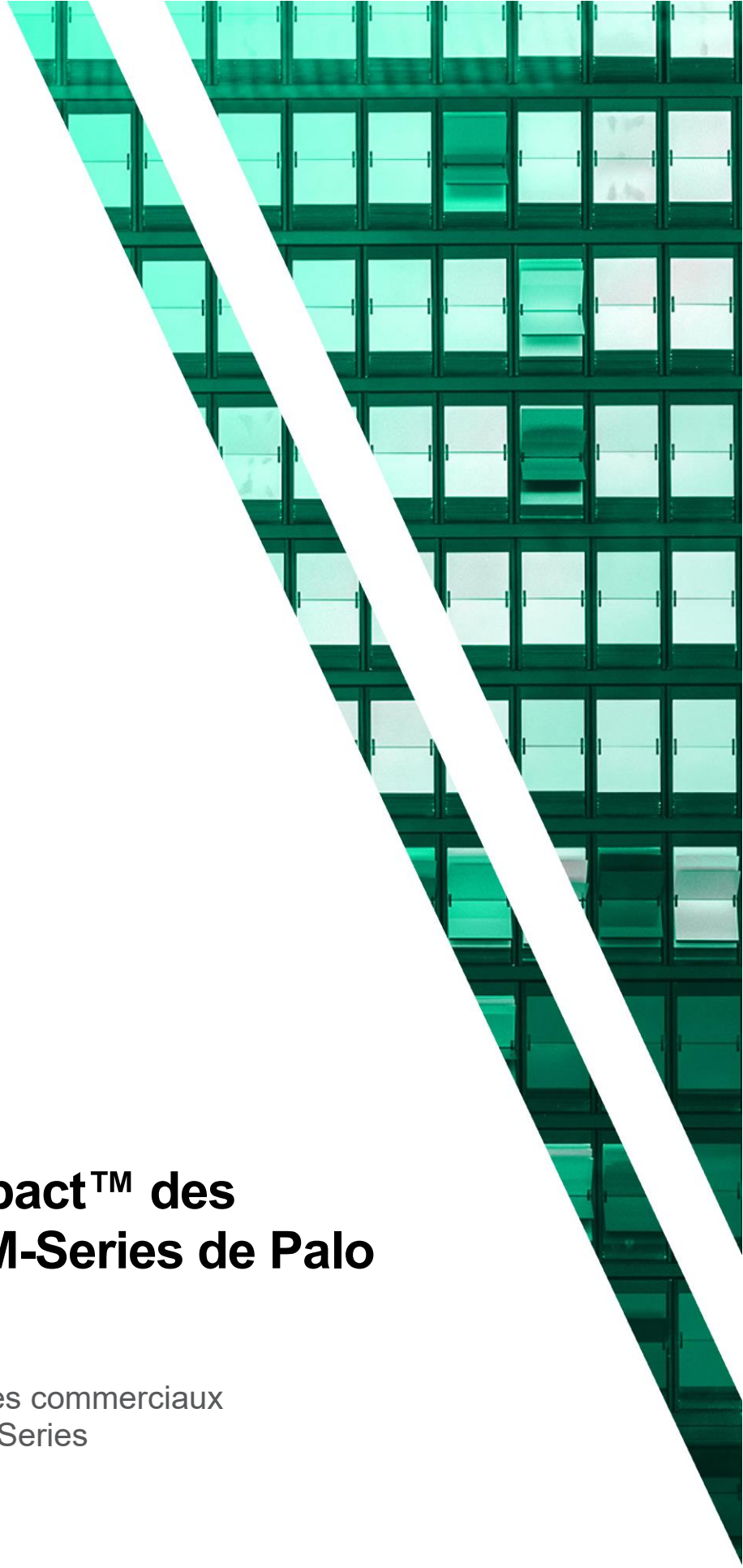
FORRESTER®



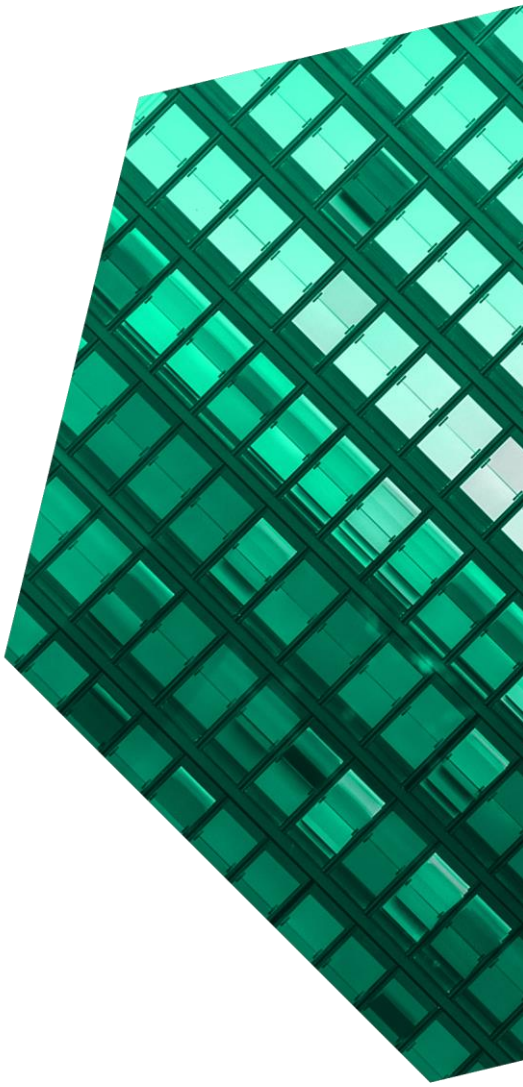
Total Economic Impact™ des pare-feu virtuels VM-Series de Palo Alto Networks

Réduction des coûts et bénéfices commerciaux grâce aux pare-feu virtuels VM-Series

SEPTEMBRE 2021

Table des matières

Équipe de consultants : *Sam Conway*
Isabel Carey



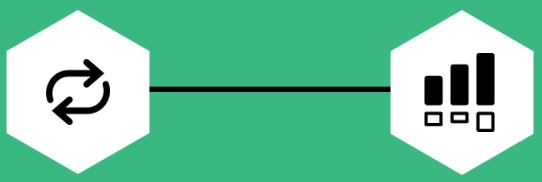
Sommaire

Lorsque les entreprises migrent vers le cloud et explorent les avantages des déploiements hybrides et multicloud, leurs équipes de sécurité doivent faire face à un nouveau type de vulnérabilités et d'exigences en matière de réseau. Tandis que les pare-feu restent l'un des outils les plus fiables pour les professionnels chargés de la sécurité sur site, ceux de nouvelle génération apparaissent aussi comme des outils de contrôle efficaces pour sécuriser le trafic de données vers différents clouds. Les pare-feu VM-Series de Palo Alto Networks offrent des solutions de sécurité flexibles aux entreprises agiles.

Palo Alto Networks a chargé Forrester Consulting de conduire une étude TEI (Total Economic Impact™) afin d'examiner le retour sur investissement (ROI) potentiel que les entreprises peuvent réaliser en déployant les pare-feu virtuels VM-Series[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 des pare-feu virtuels VM-Series de Palo Alto Networks dans leur entreprise.

Les pare-feu VM-Series de Palo Alto Networks offrent toutes les fonctionnalités des pare-feu matériels de nouvelle génération (NGFW) de Palo Alto Networks sous forme de machine virtuelle (VM). Les pare-feu VM-Series proposent un large éventail de fonctionnalités qui permettent de relever les défis actuels en matière de sécurité réseau dans les clouds publics et privés, les centres de données virtualisés et les succursales définies par logiciel. Les entreprises peuvent tirer parti de leurs infrastructures matérielles existantes pour héberger conjointement des pare-feu avec d'autres réseaux, d'autres services de sécurité et même d'autres applications virtualisés.

STATISTIQUES CLÉS



Retour sur investissement (ROI)
115 %

Valeur actuelle nette (VAN)
1,83 MUSD

Délai de récupération :

< 6 mois

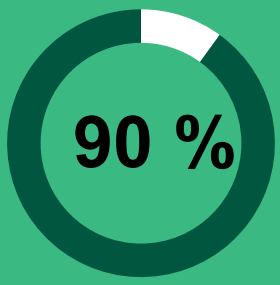
Pour mieux comprendre les bénéfices, les coûts et les risques associés à cet investissement, Forrester a interrogé 8 décideurs et sondé 132 personnes qui avaient une expérience des pare-feu virtuels VM-Series. Pour les besoins de cette étude, Forrester a agrégé les expériences des personnes interrogées, puis a consolidé les résultats dans une entreprise de référence.

Avant d'utiliser les pare-feu virtuels VM-Series, les entreprises interrogées s'appuyaient principalement sur des pare-feu matériels avec des solutions individuelles. Cependant, lorsqu'elles ont entrepris des projets de transformation digitale de plus grande envergure et se sont orientées vers la virtualisation sur l'ensemble de l'entreprise pour consolider les infrastructures de réseau et de sécurité avec les clouds publics, elles ont constaté que les pare-feu existants n'offraient pas la flexibilité dont les équipes avaient besoin. Les entreprises ont étudié la possibilité de s'appuyer sur les fonctionnalités de sécurité natives des prestataires de services de cloud, mais elles ont constaté que ces derniers n'avaient pas la compétence d'un fournisseur de sécurité mature comme Palo Alto Networks. Les entreprises utilisaient par ailleurs en moyenne quatre clouds publics et ne

souhaitaient pas introduire davantage de complexité dans leurs infrastructures de sécurité.

Après avoir investi dans des pare-feu virtuels VM-Series, les entreprises interrogées ont pu résoudre les problèmes de sécurité de leurs environnements hybrides et multiclouds. Leurs équipes de sécurité pouvaient facilement déployer des contrôles de sécurité avancés et définir, appliquer et gérer des politiques de sécurité cohérentes à partir d'une console unique. Grâce à une meilleure visibilité, elles ont obtenu un contrôle précis sur le trafic entrant, sortant et est-ouest, ce qui a permis de réduire considérablement les surfaces d'attaque. Le format des pare-feu VM-Series a également permis aux entreprises d'automatiser leur déploiement et leur provisionnement, et de s'adapter à la demande. Cela a permis de réduire les délais de déploiement et d'éliminer les coûts de surprovisionnement.

Réduction du délai de déploiement des pare-feu



PRINCIPALES CONCLUSIONS

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

- **Réduction de 90 % du temps nécessaire au déploiement des pare-feu et amélioration de 80 % de l'efficacité des équipes chargées du réseau et de la sécurité, soit une économie de 1,3 million USD sur trois ans.** Le déploiement des pare-feu VM-Series prend beaucoup moins de temps que celui des pare-feu traditionnels, pour lesquels il faut expédier, installer et configurer le matériel. Les entreprises interrogées ont également constaté des gains d'efficacité grâce à l'administration centralisée des pare-feu dans Palo Alto Networks Panorama (qui fournit une administration centralisée de la sécurité du réseau), au maintien d'un ensemble unique de politiques dans tous les clouds, à la centralisation des correctifs et aux mises à niveau.
- **Réduction de 30 % du temps nécessaire à l'obtention d'une posture de sécurité appropriée, soit une économie de 436 800 USD sur trois ans.** En tirant parti des NGFW de Palo Alto Networks et des services de sécurité dans le cloud, les entreprises des personnes interrogées ont pu mettre en place leurs solutions de sécurité plus rapidement et atteindre des états stables plus vite. Cela a permis aux équipes de sécurité de commencer à adopter le modèle Zero Trust, ce qu'elles ne pouvaient faire avec les anciennes solutions individuelles.

[Palo Alto Networks] nous a permis de ne plus avoir à gérer différents composants de sécurité et de réseau, et de considérer davantage la sécurité comme une plateforme. Cela nous a aidés à simplifier l'environnement et à passer au cloud. C'est la raison pour laquelle nous avons fait appel à [Palo Alto Networks]. Sinon, il aurait fallu faire appel à différents fournisseurs et à différents outils, puis les assembler.

— Responsable mondial de l'ingénierie informatique, boissons

- **Réduction de 18 % du nombre d'incidents de sécurité qui nécessitent une enquête manuelle et réduction de 25 % du délai moyen de résolution (MTTR), soit une économie de 240 100 USD sur trois ans.** Le déploiement des pare-feu VM-Series administrés de manière centralisée a aidé les professionnels de la sécurité réseau, de l'informatique et des opérations de sécurité (SecOps) à automatiser des processus auparavant manuels et à améliorer la visibilité sur le trafic réseau. Grâce à une meilleure visibilité et à de meilleures données, les équipes ont pu résoudre les problèmes plus rapidement.
- **Réduction des incidents et amélioration de l'efficacité des utilisateurs finaux, pour une économie de 493 400 USD sur trois ans.** Grâce à une meilleure protection contre les menaces et à la réduction du nombre d'incidents, les utilisateurs finaux ont subi moins de temps d'arrêt et ont pu se concentrer sur leurs rôles principaux. Cela a généré de la valeur ajoutée pour les entreprises des personnes interrogées.
- **Réduction du coût total des infrastructures de sécurité par l'élimination des solutions individuelles et la suppression du surprovisionnement, ce qui a permis d'économiser près de 573 800 USD sur trois ans.** Pour les personnes interrogées, les pare-feu VM-Series permettaient à leur entreprise d'utiliser un ensemble d'outils cohérent dans le cadre de déploiements multicloud et de recourir à des services de sécurité dans le cloud. Cela leur a permis de sécuriser en toute confiance l'ensemble du trafic qui traverse n'importe quel réseau ou cloud, et d'éliminer les solutions individuelles. La facilité de déploiement des pare-feu VM-Series a également permis aux entreprises de bénéficier d'un niveau d'évolutivité impossible à atteindre avec les appliances traditionnelles, et a éliminé le besoin de surprovisionner en vue d'une utilisation accrue.

« Si vous gardez deux technologies de pare-feu différentes, vous doublez presque l'effort. »
RSSI, dispositifs médicaux

- **Réduction de 20 % de la probabilité d'une violation des données au bout de trois ans.** Grâce à Palo Alto Networks, les entreprises ont pu mettre en place des modèles de sécurité Zero Trust et appliquer des politiques de sécurité cohérentes. Elles ont utilisé les pare-feu VM-Series pour réduire les surfaces d'attaque grâce à la segmentation et la microsegmentation, à la prévention avancée des menaces et aux pare-feu applicatifs.

Nous sommes parvenus à [notre décision d'investir dans Palo Alto Networks] après en avoir identifié les avantages sur les plans financier, de la sécurité, des économies sur les coûts d'exploitation dues à une meilleure efficacité et aussi des fonctionnalités. Lorsque vous comparez [Palo Alto Networks] à de nombreux autres fournisseurs, ce n'est pas seulement une question de coût.

— Vice-président exécutif de l'ingénierie, services informatiques

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

- **Possibilité d'utiliser les compétences existantes pour éviter la formation et le recrutement.** Les entreprises ont pu déployer et administrer les pare-feu VM-Series de Palo Alto Networks avec les ressources existantes. En tant que leader du secteur des pare-feu, les compétences de Palo Alto Networks en matière de pare-feu sont largement disponibles, ce qui évite d'avoir à recruter et à former des ressources supplémentaires.
- **Évolutivité et flexibilité améliorées.** Grâce à leur forme virtuelle, les pare-feu VM-Series peuvent être rapidement déployés ou retirés selon les besoins. Cela permet aux entreprises de s'adapter rapidement à l'évolution des besoins tout en contrôlant les coûts.
- **Compétitivité améliorée.** Certaines entreprises interrogées ont utilisé Palo Alto Networks comme avantage concurrentiel pour la prestation de services technologiques. Ces entreprises fournissaient des services hébergés dans le cloud et utilisaient la sécurité fournie par la plateforme VM-Series comme facteur de différenciation pour gagner et fidéliser des clients.
- **Garantie que la sécurité n'est pas un obstacle aux efforts de transformation digitale.** Les équipes de sécurité ont pour mandat de veiller à ce que les activités soient aussi sûres que possible, mais elles ne veulent pas être un obstacle aux efforts de transformation digitale de leur entreprise. Avec la plateforme VM-Series, les équipes ont pu déployer rapidement des pare-feu et atteindre le niveau de sécurité requis pour que leur entreprise puisse maximiser les avantages de leur migration vers le cloud public et hybride. Les équipes pouvaient réagir rapidement aux nouveaux vecteurs de menaces créés par la transformation digitale et sécuriser les ressources à la périphérie de leur réseau, notamment les kiosques de vente au détail.

Coûts. Les coûts en VA ajustés en fonction des risques sont les suivants :

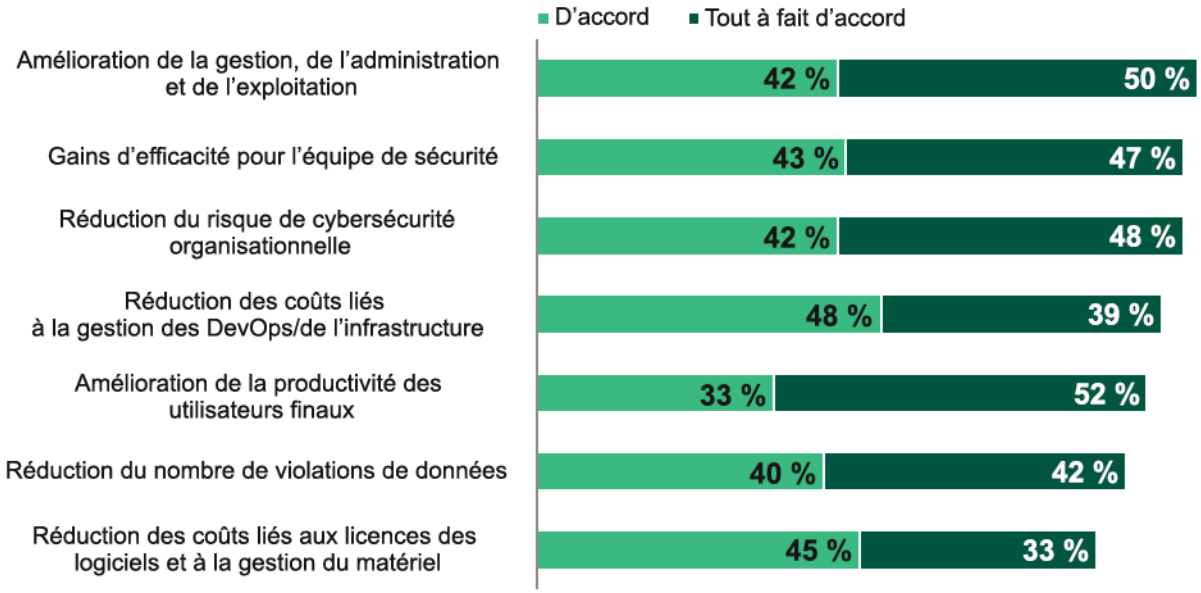
- **Les licences des pare-feu pour un total de 1 million USD sur trois ans.** Les entreprises payaient traditionnellement des frais de licence annuels pour l'utilisation des pare-feu VM-Series et des services de sécurité fournis dans le cloud, mais Palo Alto Networks a récemment introduit un modèle de consommation flexible qui leur permet d'ajuster de façon dynamique la taille de leurs pare-feu en fonction des besoins, et de modifier ou d'ajouter de nouveaux services via un abonnement dans le cloud (CDSS). Ce modèle de tarification flexible (qui a pour objectif de permettre aux clients d'adapter la sécurité à des environnements qui évoluent rapidement) est conçu pour permettre de réaliser des économies encore plus importantes qu'avec les frais de licence annuels modélisés par Forrester pour l'entreprise de référence.
- **Effort de déploiement interne totalisant 4 900 USD sur trois ans.** Pour les personnes interrogées, le déploiement des pare-feu VM-Series a nécessité du temps et de la main-d'œuvre, et des pare-feu supplémentaires ont été installés au cours des années suivantes.
- **Administration continue qui totalise près de 441 000 USD sur trois ans.** Selon les personnes interrogées, leur entreprise a encouru des coûts de main-d'œuvre interne pour l'administration continue des déploiements VM-Series. Cela comprenait la configuration, la mise à jour et l'introduction de nouvelles politiques.
- **Coût des appliances en marque blanche de 151 000 USD sur trois ans.** Les entreprises ont déployé leurs pare-feu VM-Series à l'aide de matériel standard, et ont dû supporter des coûts supplémentaires pour l'achat de nouvelles appliances.

Réduction de la probabilité d'une violation des données

20 % de réduction l'Année 3

Les entretiens avec les clients et l'analyse financière ont montré qu'une entreprise de référence réalise des bénéfices de 3,43 millions USD sur trois ans, contre des coûts de 1,6 million USD, soit une valeur actuelle nette (VAN) de 1,83 million USD et un retour sur investissement de 115 %.

Figure 1. « Sur une échelle de 1 à 5, où 1 signifie "pas du tout d'accord" et 5 signifie "tout à fait d'accord", dans quelle mesure êtes-vous d'accord avec le fait que les pare-feu virtuels VM-Series de Palo Alto Networks (y compris l'utilisation avec tout service de sécurité) présentent les caractéristiques suivantes ? »



Base : 132 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

ROI
115 %

BÉNÉFICES EN VA
3,43 MUSD

VAN
1,83 MUSD

DÉLAI DE RÉCUPÉRATION
< 6 mois

Bénéfices (sur trois ans)

CADRE DE RÉFÉRENCE ET MÉTHODOLOGIE 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 les pare-feu virtuels VM-Series.

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 les pare-feu virtuels VM-Series peuvent avoir sur une entreprise.

Forrester Consulting a mené une enquête en ligne auprès de 351 responsables de la cybersécurité dans des entreprises internationales aux États-Unis, au Royaume-Uni, au Canada, en Allemagne et en Australie. Les participants à l'enquête étaient des managers, des directeurs, des vice-présidents et des cadres dirigeants chargés des décisions, des opérations et des rapports en matière de cybersécurité. Les questions posées aux participants visaient à évaluer les stratégies des dirigeants en matière de cybersécurité et les éventuelles failles de sécurité survenues dans leur entreprise. Les personnes interrogées ont choisi de participer à l'enquête par l'intermédiaire d'un panel de recherche tiers, qui a mené l'enquête pour le compte de Forrester en novembre 2020.

AVERTISSEMENTS

Les lecteurs doivent être avisés de ce qui suit :

L'étude est commandée par Palo Alto Networks et réalisée par Forrester Consulting. Il ne s'agit pas d'une analyse concurrentielle.

Forrester n'établit aucun postulat concernant le retour sur investissement que d'autres entreprises pourraient enregistrer. 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 les pare-feu virtuels VM-Series.

Palo Alto Networks 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.

Palo Alto Networks a fourni les noms des clients pour les entretiens, mais n'y a pas pris part.

DILIGENCE RAISONNABLE

Entretien avec les parties prenantes de Palo Alto Networks et les analystes de Forrester pour recueillir des données relatives aux pare-feu virtuels VM-Series.

ENTRETIENS AVEC DES CLIENTS

Nous avons mené des entretiens individuels avec 8 décideurs et sondé 132 autres décideurs d'entreprises qui utilisent des pare-feu virtuels VM-Series, l'objectif étant de recueillir des données relatives aux coûts, aux bénéfices et aux 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 et avons ajusté ce modèle en fonction des risques sur la base des problèmes et des 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 portant sur 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 les pare-feu virtuels VM-Series de Palo Alto Networks

Facteurs qui ont conduit à l'investissement dans les pare-feu virtuels VM-Series

Décideurs interrogés

Personne interrogée	Secteur	Région	Chiffre d'affaires
Architecte principal	Services informatiques	Europe	80 millions USD
Expert réseau senior	Services informatiques	Europe	80 millions USD
Ingénieur réseau	Infrastructure de communication	États-Unis	6 milliards USD
EVP de l'ingénierie	Services informatiques	États-Unis	S.O.
Responsable mondial de l'ingénierie informatique	Boissons	Monde	37 milliards USD
Ingénieur en sécurité de l'information	Services aux entreprises	Amérique du Nord	3 milliards USD
Ingénieur senior en sécurité	Services aux entreprises	Amérique du Nord	3 milliards USD
RSSI	Dispositifs médicaux	Amérique du Nord	800 millions USD

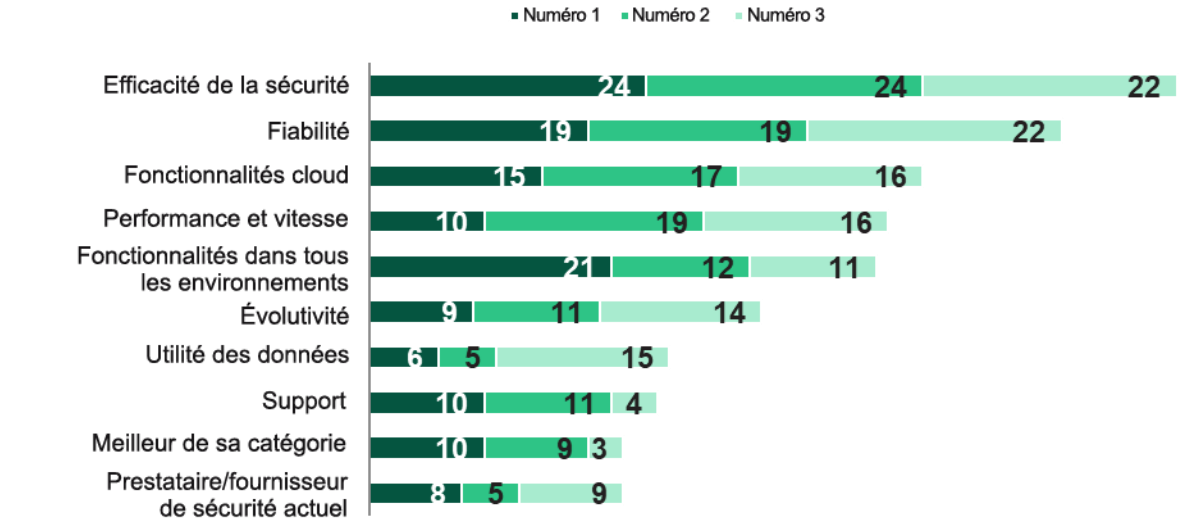
PRINCIPAUX DÉFIS

Les entreprises des personnes interrogées ont été confrontées à des défis communs, notamment :

- **Des solutions individuelles existantes peu performantes.** Selon les personnes interrogées, les anciennes solutions individuelles ne répondaient pas aux attentes en termes de vitesse, de performances et de support client. Les produits précédemment déployés étaient lents à mettre à niveau, et leur déploiement et leur maintenance nécessitaient un effort interne important.
- **Plateformes et fonctionnalités de sécurité décentralisées.** Avant d'utiliser les pare-feu VM-Series, les entreprises des personnes interrogées avaient des difficultés à gérer des outils de sécurité décentralisés, ce qui entraînait des lacunes en termes de visibilité et des tâches redondantes. Par exemple, les entreprises qui utilisaient plusieurs clouds devaient rédiger et diffuser plusieurs versions des mêmes politiques en utilisant des outils natifs.
- **Mandats organisationnels de migration vers le cloud.** Bon nombre d'entreprises fonctionnaient dans des environnements avec un calendrier strict de migration vers le cloud. Ces entreprises avaient besoin de solutions de sécurité qui pouvaient être déployées rapidement et qui leur garantissaient une visibilité suffisante pour protéger de façon adéquate leurs nouveaux déploiements dans le cloud.

« Lorsque nous nous sommes séparés de la société mère, nous n'avons eu qu'un week-end de quatre jours pour nous dissocier localement. Nous avons donc tout construit en parallèle – nouveaux systèmes de pare-feu X, Y et Z – pour réussir la coupure dans un délai aussi court. Notre priorité était de progresser dans nos efforts de transformation. »
RSSI, dispositifs médicaux

Figure 2. « Dans la liste ci-dessous, sélectionnez les trois critères les plus importants pour choisir un fournisseur de sécurité réseau et classez-les de 1 à 3 par ordre d'importance, 1 étant le plus important. »



Base : nombre variable de décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

POURQUOI PALO ALTO NETWORKS

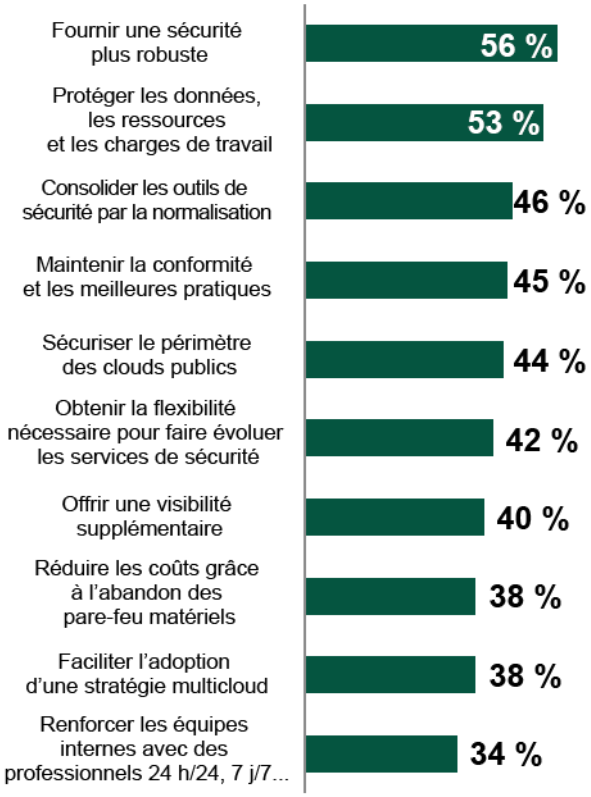
Les entreprises des personnes interrogées ont évalué plusieurs solutions avant de décider d'investir dans les pare-feu virtuels VM-Series. Les fonctionnalités clés qui ont été prises en compte dans les investissements sont les suivantes :

- **Visibilité de la couche 7.** Les pare-feu VM-Series offrent une visibilité sur les applications sur tous les ports, et fournissent des données pertinentes pour la prise de décisions stratégiques.
- **Segmentation des applications.** Les entreprises peuvent utiliser les pare-feu VM-Series pour segmenter et contrôler la communication des applications. Ce dispositif est renforcé par une prévention avancée des menaces qui permet d'identifier et de bloquer les menaces latérales sur le réseau.
- **Sécurité avancée avec CDSS.** Les abonnements de sécurité Palo Alto Networks peuvent être activés sur la plateforme VM-Series sans nécessiter l'installation ou le déploiement de capteurs ou d'appliances supplémentaires. Cela permet aux entreprises de bénéficier d'avantages supplémentaires en matière de protection grâce aux services tels que les systèmes avancés de prévention des intrusions (IPS), la sécurité du système de nom de domaine (DNS), le filtrage des URL, la prévention des menaces zero-day et le sandboxing, sans coûts supplémentaires.
- **Politiques basées sur les utilisateurs.** Les pare-feu VM-Series fournissent nativement des politiques basées sur l'utilisateur, et ils sont intégrés à un large éventail de référentiels d'utilisateurs. Cela permet d'appliquer des politiques de contrôle d'accès dynamiques basées sur les utilisateurs en plus des politiques basées sur les applications.

« Du point de vue de la sécurité, Palo Alto est plus ciblé, et son ADN s'articule autour de l'identité et de la possibilité d'actualiser la sécurité en temps réel. »
Responsable mondial de l'ingénierie informatique, boissons

- **Administration centralisée pour des politiques cohérentes et une administration simplifiée.** Les pare-feu VM-Series peuvent être administrés de manière centralisée via Panorama, ce qui garantit la cohérence des politiques sur différents déploiements dans le cloud et sur site. Panorama évite également aux opérateurs d'avoir à gérer la sécurité de leur réseau à partir de plusieurs consoles disparates.
- **Automatisation du déploiement et des mises à jour des politiques.** Les entreprises peuvent tirer parti des fonctionnalités de la plateforme VM-Series pour intégrer la sécurité dans les workflows de développement des applications, notamment le provisionnement automatique, les mises à jour automatisées des politiques, l'utilisation de modèles de fournisseurs de cloud natifs et l'évolutivité adaptée au cloud.

Figure 3. « Quels sont les facteurs clés qui ont motivé la décision d'investir dans les pare-feu virtuels VM-Series de Palo Alto Networks ? »



Base : 132 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

Hypothèses clés

- **Chiffre d'affaires de 3 milliards USD**
- **Basée aux États-Unis**
- **100 pare-feu VM-Series au début**
- **7 500 employés**
- **12 ETP de SecOps**
- **8 ETP de NetOps**

ENTREPRISE DE RÉFÉRENCE

À partir des entretiens, Forrester a établi un cadre de référence TEI, une entreprise de référence et une analyse de son ROI qui illustre les domaines affectés sur le plan financier. L'entreprise de référence est représentative des 8 décideurs interrogés par Forrester et des 132 entreprises étudiées par Forrester. Elle est utilisée pour présenter l'analyse financière sous forme agrégée dans la section suivante. L'entreprise de référence présente les caractéristiques suivantes :

Description de l'entreprise de référence. L'entreprise de référence est une entreprise distribuée, qui enregistre un chiffre d'affaires annuel de 3 milliards USD et compte 7 500 employés. L'entreprise a son siège aux États-Unis et dispose d'équipes internationales. L'équipe de sécurité de l'entreprise traite 154 incidents par semaine.

Caractéristiques du déploiement. L'entreprise de référence utilise des pare-feu VM-Series pour sécuriser le trafic nord-sud et est-ouest sur plusieurs déploiements dans le cloud. L'entreprise gère 156 pare-feu virtuels qui seront déployés sur des appliances standard d'ici l'Année 3. Elle gère ses pare-feu VM-Series avec Panorama. Les CDSS de Palo Alto Networks améliorent chaque déploiement de NGFW par une prévention en ligne des menaces connues et inconnues (avec la prévention des menaces de Palo Alto Networks et l'analyse des logiciels malveillants de WildFire) et de toutes les menaces transmises par le web (avec le filtrage

des URL de Palo Alto Networks et la sécurité du DNS). Il s'agit notamment de l'allègement des systèmes de commande-contrôle et de la prévention des pertes de données (DLP).

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	Déploiement et maintenance des pare-feu	531 498 USD	517 624 USD	518 780 USD	1 567 902 USD	1 300 736 USD
Btr	Atteinte de la posture de sécurité recherchée	381 758 USD	56 858 USD	56 858 USD	495 473 USD	436 760 USD
Ctr	Efficacité des opérations informatiques et de sécurité	96 562 USD	96 562 USD	96 562 USD	289 686 USD	240 136 USD
Dtr	Réduction des temps d'arrêt pour les utilisateurs finaux	198 398 USD	198 398 USD	198 398 USD	595 195 USD	493 387 USD
Etr	Coûts évités et réduits de l'infrastructure de sécurité	240 996 USD	224 121 USD	225 527 USD	690 645 USD	573 754 USD
Ftr	Réduction du risque de violation des données	105 083 USD	157 624 USD	210 166 USD	472 873 USD	383 699 USD
	Total des bénéfices (ajusté en fonction des risques)	1 554 294 USD	1 251 188 USD	1 306 291 USD	4 111 774 USD	3 428 472 USD

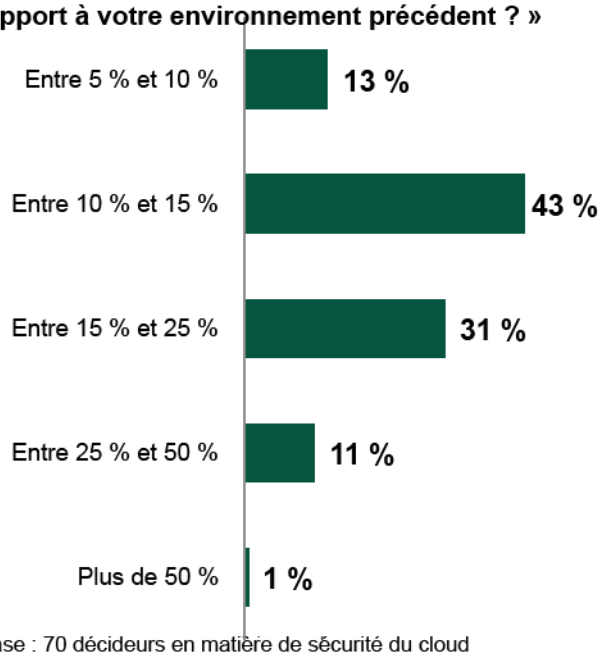
DÉPLOIEMENT ET MAINTENANCE DES PARE-FEU

Preuves et données. Selon les personnes interrogées, grâce à leur forme virtuelle, les pare-feu VM-Series nécessitent beaucoup moins de temps pour le déploiement et la maintenance que les solutions traditionnelles. Auparavant, leurs entreprises utilisaient principalement des appliances physiques traditionnelles dont l'installation et la configuration nécessitaient un travail manuel, ainsi que de longs délais d'expédition. Pour les personnes d'entreprises qui utilisaient des solutions natives de prestataires de services de cloud interrogées, la possibilité de gérer les déploiements de la plateforme VM-Series via Panorama constituait un gain de temps considérable et créait un modèle de politique unique pour les déploiements sur site et dans le cloud.

- Un ingénieur réseau d'une entreprise d'infrastructure de communication a déclaré : « Après nous être débarrassés de toutes les appliances, les coûts d'assistance étaient nettement réduits. De même, le temps requis pour commander ces appareils et les installer sur le terrain, ainsi que le temps nécessaire à la configuration de tous ces équipements ont été supprimés, ce qui nous permet de faire des économies. Par exemple, avec notre ancien pare-feu, si vous ne le dimensionniez pas correctement avec une appliance, vous deviez en acheter une autre plus puissante. Avec [les pare-feu virtuels VM-Series], il suffit d'utiliser une licence différente, et vous avez alors un pare-feu à la bonne taille. »
- Un vice-président exécutif de l'ingénierie d'un prestataire de services informatiques a déclaré : « Lorsque vous déployez des services de sécurité et que vous utilisez un pare-feu, la sécurité est la priorité absolue. Exact ? Ainsi, le nombre d'heures de travail nécessaires pour mettre à jour les pare-feu individuels est tout simplement intenable avec des solutions multiples. Dans le passé, lorsque nous avions à déployer quelque chose, nous passions 2 à 3 heures par pare-feu, et ce, juste pour le mettre en place, le déployer, configurer tous les réseaux et tout le reste. Cela n'incluait aucun ensemble de règles, aucun peaufinage des règles, ni rien de tout cela. Aujourd'hui, nous avons ramené ce [délai] à moins de 10 minutes, et notre équipe de provisionnement peut en faire plusieurs à la fois. Ainsi, non seulement nous sommes passés de 2 à 3 heures [nécessaires] par pare-feu à environ 10 minutes ou moins, mais [notre équipe de provisionnement] peut aussi en faire plusieurs à la fois. Donc, cela a considérablement augmenté notre capacité à les déployer. »

- Un responsable mondial de l'ingénierie d'une entreprise de boissons a déclaré : « Avec les [pare-feu virtuels VM-Series], vous pouvez créer un modèle standard. Une fois que vous l'avez, vous pouvez automatiser beaucoup de choses. Pour nous, je dirais que les coûts et les efforts de déploiement et de configuration ont été réduits d'au moins 90 %. »
- La même personne interrogée a également décrit l'expérience ardue du déploiement d'une solution existante : « Si l'on tient compte du coût d'expédition des composants physiques, des délais d'acheminement de cet équipement sur place, puis de la mise en rack, cela représente beaucoup de temps perdu avant de pouvoir mettre le pare-feu en service. »
- Pour 92 % des personnes interrogées, les pare-feu virtuels VM-Series (et les services de sécurité) ont amélioré les efforts de gestion, d'administration et d'exploitation de leur entreprise en matière de cybersécurité (voir la Figure 1). Selon 58 % de ces personnes interrogées, leur entreprise a bénéficié d'un délai plus court pour déployer les solutions de sécurité de Palo Alto Networks qui ne sont pas des pare-feu physiques, et selon 57 %, leur entreprise a bénéficié d'un déploiement et d'une configuration plus rapides des politiques de sécurité (voir la Figure 4).

Figure 4. « Vous avez constaté un déploiement plus rapide de la sécurité grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Quel est d'après vous le pourcentage d'amélioration par rapport à votre environnement précédent ? »



Base : 70 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

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

- L'entreprise déploie 100 pare-feu VM-Series au cours de l'Année 1.
- Le déploiement de l'entreprise augmente de 25 % par an en fonction de ses besoins.
- Les anciennes solutions nécessitaient 5 heures pour être entièrement déployées et configurées.
- Une équipe de 10 employés était chargée de gérer l'ancienne solution, ce qui consistait à installer la solution, gérer les politiques de sécurité et appliquer les mises à jour et les correctifs dans l'infrastructure. Ces ressources consacraient 75 % de leur temps uniquement aux pare-feu.
- Le salaire annuel moyen toutes charges comprises des membres de l'équipe chargée de gérer l'ancienne solution est de 112 500 USD.
- Le déploiement virtuel des pare-feu VM-Series nécessite 90 % d'efforts en moins, et l'équipe chargée des pare-feu est 80 % plus efficace grâce au contrôle centralisé des politiques, à l'automatisation des mises à jour et des correctifs, et à l'élimination des mises en rack.
- 80 % du temps économisé est redéployé vers un travail productif.

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- La taille et les compétences de l'équipe d'administration de la sécurité de l'entreprise.
- Les moyens et les systèmes mis en place avant de déployer les pare-feu virtuels VM-Series.
- Le salaire moyen des membres de l'équipe chargée du réseau, de la sécurité et des opérations informatiques.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques (taux d'actualisation de 10 %) de 1,3 million USD sur trois ans.

Déploiement et maintenance des pare-feu

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
A1	Nouveaux pare-feu déployés	Entreprise de référence	100	25	31
A2	Temps nécessaire pour déployer les anciens pare-feu (heures)	Entretiens	5	5	5
A3	Réduction du temps nécessaire au déploiement des pare-feu VM-Series	Entretiens	90 %	90 %	90 %
A4	Réduction totale du temps de déploiement annuel (heures)	A1*A2*A3	450	113	141
A5	Nombre d'ETP requis pour l'équipe en charge des pare-feu	Entreprise de référence	10	10	10
A6	Pourcentage du temps consacré au travail sur les pare-feu	Hypothèse	75 %	75 %	75 %
A7	Amélioration de l'administration du réseau et de la sécurité des pare-feu (p. ex. contrôle centralisé, ensemble unique de politiques, mise en rack, routage et correctifs)	Entretiens	80 %	80 %	80 %
A8	Temps d'administration économisé (heures)	A5*2 080 heures*A6*A7	12 480	12 480	12 480
A9	Gain de productivité	Hypothèse	80 %	80 %	80 %
A10	Salaire horaire moyen d'un employé informatique (p. ex. NetOps, SecOps, opérations informatiques)	Hypothèse	54 USD	54 USD	54 USD
At	Déploiement et maintenance des pare-feu	(A4+A8)*A9*A10	559 471 USD	544 868 USD	546 085 USD
	Ajustement en fonction des risques	↓5 %			
Atr	Déploiement et maintenance des pare-feu (bénéfices ajustés en fonction des risques)		538 498 USD	517 624 USD	518 780 USD
	Total sur trois ans : 1 567 902 USD		**Valeur actuelle sur trois ans : 1 300 736 USD**		

ATTEINTE DE LA POSTURE DE SÉCURITÉ RECHERCHÉE

Preuves et données. Selon les personnes interrogées, les technologiques homogènes, la plateforme unifiée et les fonctionnalités d'administration avancée de Palo Alto Networks ont permis à leur entreprise d'atteindre plus rapidement un état stable. Elles ont pu mettre en place leurs infrastructures de sécurité plus rapidement, réduire leurs efforts de mise en œuvre et permettre aux équipes de sécurité de commencer la configuration plus tôt qu'avec des solutions individuelles.

Avec Palo Alto Networks, les entreprises ont pu intégrer tous les composants sur une plateforme commune et leur donner une apparence similaire. Cela a permis d'accélérer les déploiements et de libérer des ressources pour peaufiner la solution, mettre en œuvre des workflows automatisés et trouver des moyens d'améliorer l'efficacité de la sécurité, de l'informatique et des utilisateurs métiers.

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

- L'entreprise utilise la même équipe de déploiement dans les deux scénarios. L'équipe comprend 12 employés de SecOps et 8 employés de NetOps au cours de l'Année 1 du déploiement.
- Le salaire annuel moyen d'un employé de SecOps toutes charges comprises est de 121 500 USD.

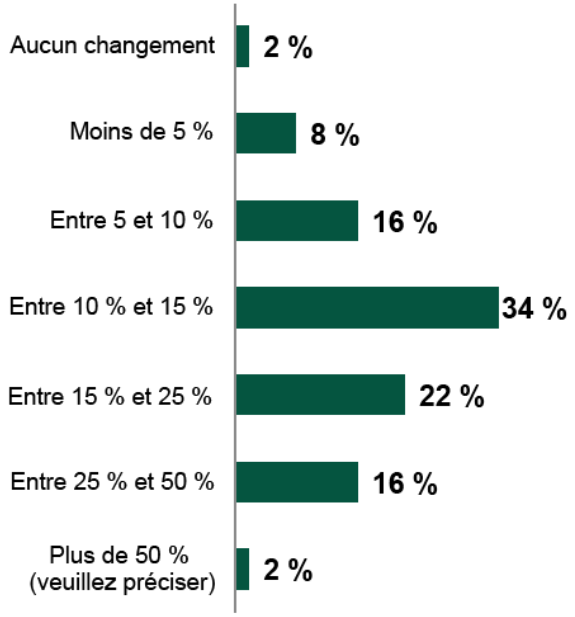
- Le salaire annuel moyen d'un employé de NetOps toutes charges comprises est de 135 000 USD.
- Avec Palo Alto Networks, l'entreprise atteint un état stable 30 % plus rapidement qu'avec des solutions individuelles ; le temps nécessaire pour atteindre un état stable passe ainsi de 6,3 mois à 4,4 mois.

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- La taille de l'équipe de déploiement et les salaires relatifs.
- Les composants spécifiques déployés et le temps nécessaire pour atteindre un état stable.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 436 800 USD sur trois ans.

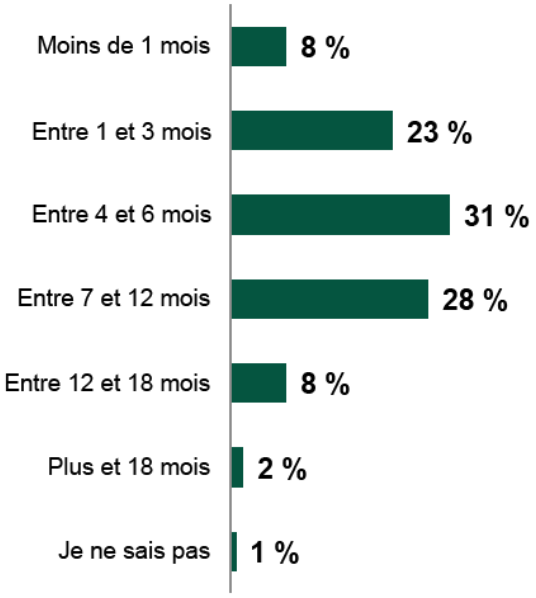
Figure 5. Vous avez constaté un délai plus court pour produire des informations lors des audits grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque) ? Pouvez-vous estimer le pourcentage d'amélioration par rapport à votre environnement précédent ?



Base : 50 décideurs en matière de sécurité du cloud

Source : « PAN Virtual Firewalls TEI », une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

Figure 6. Vous avez constaté une réduction du risque de cybersécurité organisationnelle grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque) ? Pouvez-vous estimer le temps qu'il a fallu à votre entreprise pour atteindre une posture de sécurité « stable » avec les solutions ponctuelles antérieures ?



Base : 119 décideurs en matière de sécurité du cloud

Source : « PAN Virtual Firewalls TEI », une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

Atteinte de la posture de sécurité recherchée					
Réf.	**Indicateur**	**Source**	**Année 1**	**Année 2**	**Année 3**
B1	Salaire annuel des ETP de SecOps toutes charges comprises	Hypothèse	121 500 USD	121 500 USD	121 500 USD
B2	Salaire annuel des ETP de NetOps toutes charges comprises	Hypothèse	135 000 USD	135 000 USD	135 000 USD
B3	Nombre d'ETP de SecOps nécessaires	Entreprise de référence	12	2	2
B4	Nombre d'ETP de NetOps nécessaires	Entreprise de référence	8	1	1
B5	Temps nécessaire pour atteindre une posture de sécurité appropriée avec des solutions individuelles (mois)	Résultats de l'enquête	6,3	6,3	6,3
B6	Temps nécessaire pour atteindre une posture de sécurité appropriée avec Palo Alto Networks (mois)	Résultats de l'enquête	4,4	4,4	4,4
B7	Gain de temps initial et en continu entre les solutions individuelles et les pare-feu virtuels VM-Series (arrondi)	1-(B6/B5)	30 %	30 %	30 %
B8	Coût des solutions individuelles pour atteindre un état stable	(B1*B3/12*B5)+(B2*B4/12*B5)	1 332 450 USD	198 450 USD	198 450 USD
B9	Coût des pare-feu virtuels VM-Series pour atteindre un état stable	(B1*B3/12*B6)+(B2*B4/12*B6)	930 600 USD	138 600 USD	138 600 USD
Bt	Atteinte de la posture de sécurité recherchée	B8-B9	401 850 USD	59 850 USD	59 850 USD
	Ajustement en fonction des risques	↓5 %			
Btr	Atteinte de la posture de sécurité recherchée (bénéfices ajustés en fonction des risques)		381 758 USD	56 858 USD	56 858 USD
	Total sur trois ans : 495 473 USD		**Valeur actuelle sur trois ans : 436 760 USD**		

EFFICACITÉ DES OPÉRATIONS INFORMATIQUES ET DE SÉCURITÉ

Preuves et données. Selon les personnes interrogées, les équipes informatiques et de SecOps ont bénéficié du déploiement de VM-Series dans leur entreprise en termes de réduction du nombre d'enquêtes, de MTTR plus rapide et de réduction du nombre de problèmes de sécurité qui ont un impact sur les appareils. Les équipes des opérations informatiques et de SecOps ont automatisé des processus auparavant manuels et ont amélioré la visibilité sur le trafic réseau, ce qui a permis de réagir plus rapidement aux problèmes. Les entreprises des personnes interrogées ont également tiré parti de l'analyse des journaux dans Prisma cloud pour réduire davantage le MTTR.

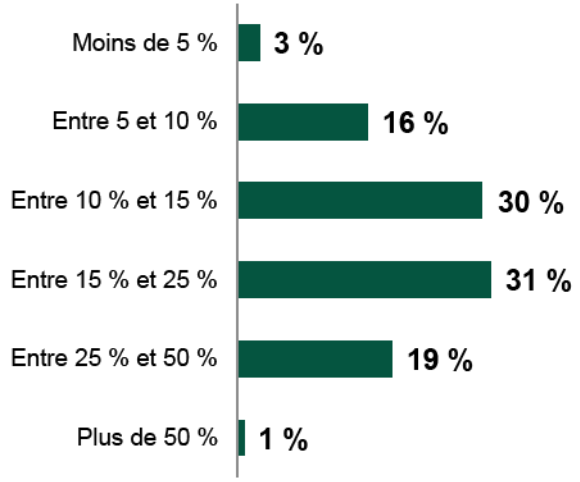
MTTR réduit de

25 %

- Le responsable mondial de l'ingénierie d'une entreprise de boissons a déclaré : « Le taux d'efficacité est vraiment élevé avec Palo Alto Networks, et la possibilité de mettre à jour quotidiennement le contenu et les politiques nous aide beaucoup. Avec VM-Series, nous avons activé dès le départ des politiques utilisateur axées sur les applications. Nous avons réduit le nombre de faux positifs qui nécessitent une

intervention humaine de 40 à 50 %, et nous avons réduit nos tickets d'au moins 40 % grâce
à la fonctionnalité de modélisation des menaces réseau. [L'équipe de support de mon entreprise] reçoit un volume plus faible de tickets, et lorsqu'elle reçoit un ticket, elle ne doute pas de sa validité et sait que c'est un problème qu'elle

Figure 7. « Vous avez constaté un délai moyen de découverte des incidents de sécurité plus rapide grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Pouvez-vous estimer le pourcentage d'amélioration par rapport à votre environnement précédent ? »

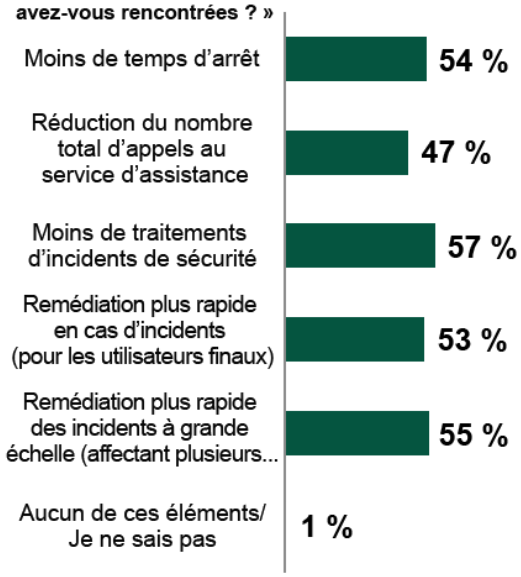


Base : 70 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

doit examiner. »

- L'ingénieur réseau d'une entreprise d'infrastructure de communication a déclaré : « C'est plus facile à gérer. La journalisation depuis le cloud qui passe par le réseau vers les serveurs de journalisation [de Palo Alto Networks] apporte une très grande visibilité sur ce qui se passe dans le cloud. Nous allons dans Panorama, saisissons la configuration souhaitée, puis nous la diffusons. Le gain de temps est donc énorme comparé au temps que devrait mettre une personne pour se rendre sur chaque pare-feu et saisir ces informations. Et il ne faut que quelques minutes pour le faire. Il y a donc un gain de temps certain pour la sécurité, puisque nous pouvons agir sur quelque chose que nous voyons à partir des informations journalisées. »

Figure 8. « Vous avez constaté une amélioration de la productivité des utilisateurs finaux grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Lesquelles des situations suivantes avez-vous rencontrées ? »

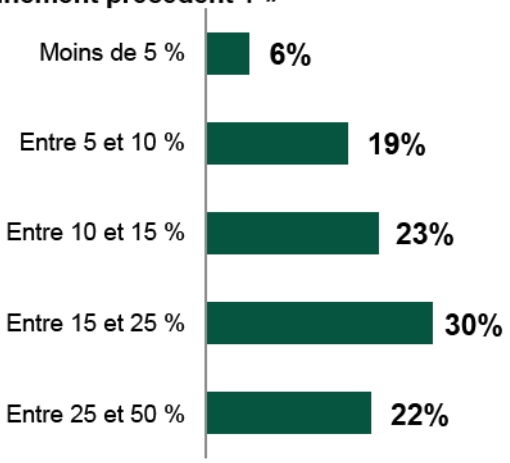


Base : 113 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

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

- Avec sa solution précédente, 154 incidents de sécurité par semaine exigeaient de l'équipe de SecOps un travail d'investigation avancé à plusieurs niveaux. Grâce à des politiques rapidement adaptables et déployées de manière cohérente sur site et dans les clouds, l'entreprise de référence améliore la visibilité sur les menaces et leur prévention, et réduit le nombre d'incidents de 18 %.
- Dans son état antérieur, le MTTR moyen de l'entreprise de référence était de 45 minutes. Avec de meilleures données contextuelles et moins de faux positifs, l'entreprise de référence réduit le MTTR de 25 %.
- Le salaire annuel moyen toutes charges comprises d'un membre de l'équipe de SecOps est de 121 500 USD. Le taux horaire est de 58 USD.
- 80 % du temps économisé est redéployé vers un travail productif.

Figure 9. « Vous avez constaté un taux de détection de faux positifs plus faible grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Pouvez-vous estimer le pourcentage d'amélioration par rapport à votre environnement précédent ? »



Source : « PAN Virtual Firewalls TEI », une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- Le nombre d'incidents de sécurité qui nécessitaient une intervention manuelle avant la mise en œuvre des pare-feu virtuels VM-Series.
- L'impact global sur le MTTR.

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 240 100 USD sur trois ans.

Efficacité des opérations informatiques et de sécurité

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
C1	Nombre d'incidents de sécurité qui nécessitent une investigation/remédiation manuelle avec l'ancienne solution de sécurité	Entreprise de référence	8 008	8 008	8 008
C2	Réduction du nombre d'incidents de sécurité qui nécessitent une investigation/remédiation manuelle avec les pare-feu virtuels VM-Series	Résultats de l'enquête	18 %	18 %	18 %
C3	Nombre d'incidents de sécurité à plusieurs niveaux évités qui nécessitent un traitement manuel (arrondi)	C1*C2	1 441	1 441	1 441
C4	MTTR avec la solution précédente (minutes)	Résultats de l'enquête	45	45	45
C5	Sous-total : enquêtes et mesures correctives évitées grâce aux pare-feu VM-Series	C3*C4/60*C8	62 703 USD	62 703 USD	62 703 USD
C6	Amélioration du MTTR avec les pare-feu VM-Series	Résultats de l'enquête	25,0 %	25,0 %	25,0 %
C7	Temps économisé par incident (minutes)	C4*C6	11	11	11
C8	Salaire horaire moyen toutes charges comprises d'un employé de SecOps (arrondi)	Hypothèse	58 USD	58 USD	58 USD
C9	Sous-total : efficacité des opérations de sécurité liées aux alertes critiques (arrondi)	((C1-C3)*C7/60)*C8	71 411 USD	71 411 USD	71 411 USD
C10	Gains de productivité des ETP de sécurité	Hypothèse	80 %	80 %	80 %
Ct	Efficacité des opérations informatiques et de sécurité	(C5+C9)*C10	107 291 USD	107 291 USD	107 291 USD
	Ajustement en fonction des risques	↓10 %			
Ctr	Efficacité des opérations informatiques et de sécurité (bénéfices ajustés en fonction des risques)		96 562 USD	96 562 USD	96 562 USD
	Total sur trois ans : 289 686 USD		**Valeur actuelle sur trois ans : 240 136 USD**		

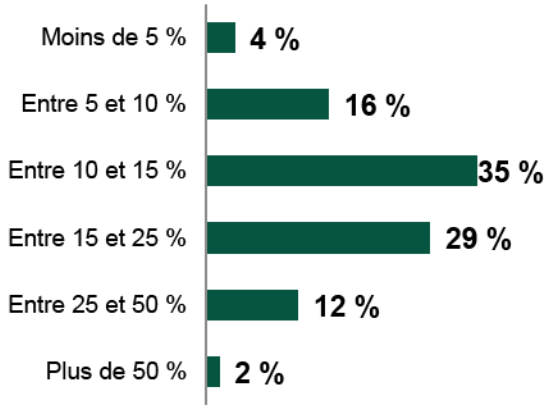
RÉDUCTION DES TEMPS D'ARRÊT POUR LES UTILISATEURS FINAUX

Preuves et données. Selon les personnes interrogées, les pare-feu VM-Series facilitaient le déploiement de politiques cohérentes dans une multitude d'environnements (p. ex. sur site, cloud public, etc.). Une mise en œuvre cohérente a permis de réduire le nombre de menaces qui entraînent un temps d'arrêt, et l'administration centralisée des pare-feu VM-Series a réduit les délais de réponse.

- Selon les personnes interrogées, 18,1 % des utilisateurs finaux en moyenne étaient touchés par des temps d'arrêt avant le déploiement des pare-feu VM-Series. Après le déploiement, ce chiffre est tombé à 5,6 %.
- Un prestataire de services informatiques qui fournit des services de cloud B2B a utilisé des pare-feu VM-Series pour segmenter les environnements des clients. Les défaillances matérielles provoquaient auparavant des pannes qui touchaient des groupes de clients. Mais si un pare-feu VM-Series tombe en panne, le temps d'arrêt ne concerne qu'un seul client. L'architecte principal de l'entreprise a déclaré : « Lorsqu'une mise à jour provoquait une heure d'arrêt, tous nos clients sur cette appliance en ressentaient les effets. Avec les [pare-feu VM-Series], un seul client est concerné. Nous ne subissons aucun temps d'arrêt, mais si c'était le cas, l'impact serait limité. »
- Selon les personnes interrogées, les fonctionnalités des NGFW, telles que la possibilité de décharger le trafic, réduisaient la probabilité que les pare-feu gênent les utilisateurs. Le responsable mondial de l'ingénierie informatique d'une entreprise du secteur des boissons a déclaré : « Grâce à la gestion basée sur des règles, nous avons pu très facilement décharger le trafic qui n'a pas besoin d'être surveillé, comme les sites web sur liste blanche, et tous nos fichiers audio et vidéo. Les gens en utilisent de plus en plus, et je peux décharger le trafic à un point spécifique en un clic, contrairement à d'autres outils qui ne le font pas. Nous pouvons donc proposer une bonne expérience aux utilisateurs et améliorer le débit du réseau. »

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

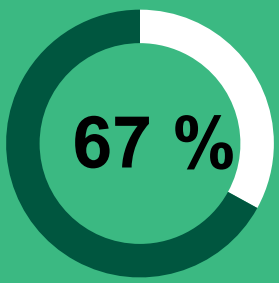
Figure 10. « Vous avez constaté une réduction du délai moyen de triage grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Pouvez-vous estimer le pourcentage d'amélioration par rapport à votre environnement précédent ? »



Base : 49 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

- Avec l'ancien système, 18 % de ses 7 500 employés étaient touchés par des temps d'arrêt chaque année. Avec les pare-feu VM-Series, ce chiffre diminue de 67 % et seuls 6 % des employés subissent des temps d'arrêt.
- Historiquement, les temps d'arrêt duraient en moyenne 4,5 heures. Après le déploiement des pare-feu VM-Series, ce chiffre diminue de 45 % (2 heures) pour les utilisateurs toujours touchés par des temps d'arrêt.

Réduction des temps d'arrêt pour les utilisateurs



- Le salaire annuel moyen toutes charges comprises d'un utilisateur final est de 87 750 USD. Le taux horaire est de 42 USD.

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- Le pourcentage d'incidents de sécurité qui ont un impact sur les utilisateurs finaux.
- Les temps d'arrêt subis en raison des enquêtes.
- Les salaires moyens toutes charges comprises des utilisateurs finaux.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 493 400 USD sur trois ans.

Réduction des temps d'arrêt pour les utilisateurs finaux

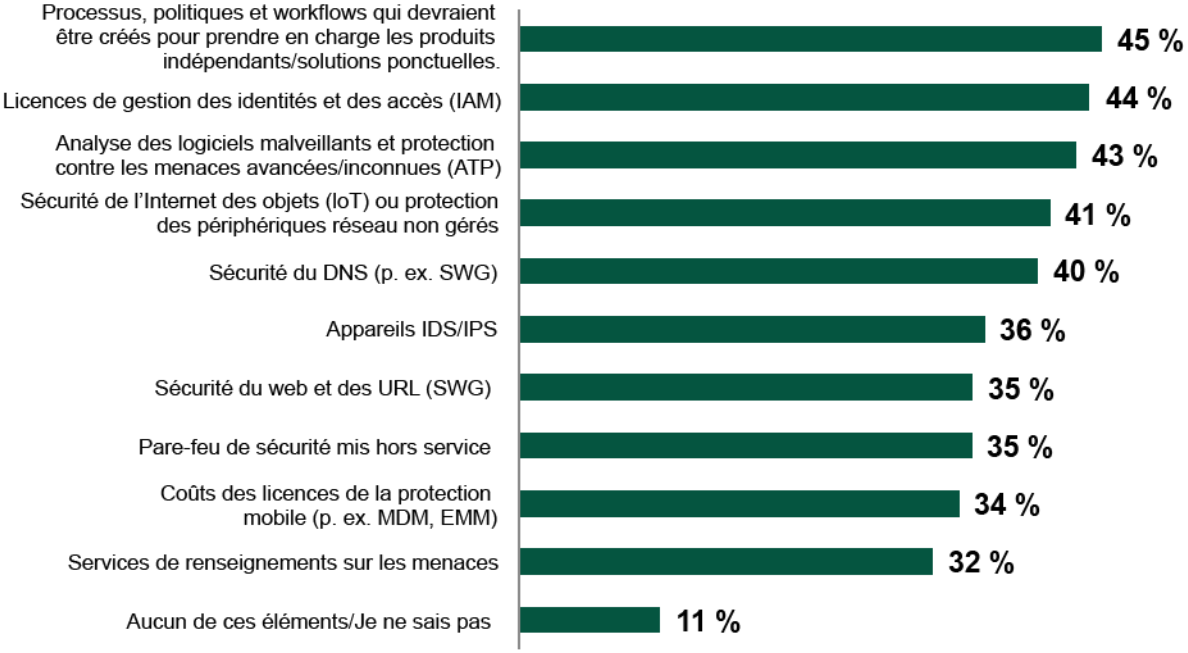
Réf.	Indicateur	Source	Année 1	Année 2	Année 3
D1	Nombre d'utilisateurs	Entreprise de référence	7 500	7 500	7 500
D2	Pourcentage d'utilisateurs affectés par des temps d'arrêt avec l'ancien système	Entretiens	18 %	18 %	18 %
D3	Réduction des temps d'arrêt avec les pare-feu VM-Series	Entretiens	67 %	67 %	67 %
D4	Utilisateurs qui évitent des temps d'arrêt grâce aux pare-feu VM-Series	D1*D2*D3	904,5	904,5	904,5
D5	Durée moyenne des temps d'arrêt avec l'ancien système (heures)	Entreprise de référence	4,5	4,5	4,5
D6	Gain de temps pour les utilisateurs finaux grâce aux événements évités	D4*D5	4 070	4 070	4 070
D7	Utilisateurs finaux qui subissent toujours des temps d'arrêt avec les pare-feu VM-Series	(D1*D2)-D6	445,5	445,5	445,5
D8	Réduction de la durée des temps d'arrêt avec les pare-feu VM-Series	Entretiens	45 %	45 %	45 %
D9	Temps d'arrêt moyen évité par utilisateur affecté avec les pare-feu VM-Series (heures)	D5*D8	2,0	2,0	2,0
D10	Gain de temps pour les utilisateurs finaux pour les événements actuels	D7*D9	902,1	902,1	902,1
D11	Salaire horaire moyen d'un utilisateur final (arrondi)	Hypothèse	42 USD	42 USD	42 USD
Dt	Réduction des temps d'arrêt pour les utilisateurs finaux	(D6+D10)*D11	208 840 USD	208 840 USD	208 840 USD
	Ajustement en fonction des risques	↓5 %			
Dtr	Réduction des temps d'arrêt pour les utilisateurs finaux (bénéfices ajustés en fonction des risques)		198 398 USD	198 398 USD	198 398 USD
	Total sur trois ans : 595 195 USD			**Valeur actuelle sur trois ans : 493 387 USD**	

COÛTS ÉVITÉS ET RÉDUITS DE L'INFRASTRUCTURE DE SÉCURITÉ

Preuves et données. Les pare-feu VM-Series peuvent être associés aux CDSS de Palo Alto Networks pour offrir aux entreprises une protection supplémentaire contre les menaces. En tirant parti de ces solutions, les entreprises des personnes interrogées ont pu éliminer les dépenses liées aux anciennes solutions individuelles dans leurs infrastructures de sécurité.

- Les entreprises ont profité du déploiement de Palo Alto Networks Threat Prevention, DNS Security, GlobalProtect, WildFire et URL Filtering avec leurs pare-feu VM-Series. Un ingénieur principal en sécurité d'un prestataire de services aux entreprises a déclaré :
  « En fait, [nous avons décidé] de passer de l'ancienne infrastructure à un pare-feu de nouvelle génération pour pouvoir intégrer un grand nombre de ces solutions et les gérer au moyen d'une seule plateforme. »
- Les entreprises ont reconnu des avantages supplémentaires du fait de l'évolutivité des pare-feu VM-Series. Elles ont pu déployer rapidement de nouveaux pare-feu en fonction des besoins, au lieu de provisionner des appliances à l'avance, ce qui entraîne souvent des dépenses inutiles. Un RSSI d'une entreprise de dispositifs médicaux a déclaré : « J'ai la possibilité de commencer à petite échelle, et ensuite de monter en puissance si besoin. Ou je peux m'en débarrasser si je n'en ai plus besoin. Avec un système interne sur site, je dois toujours acheter du matériel, je dois toujours disposer de la bonne capacité, etc. Ici, le problème ne se pose pas. Je peux activer des pare-feu, et si je dois [les désactiver] dans quatre mois, je peux le faire et c'est tout. »

Figure 11. « Vous avez constaté une réduction des coûts liés aux licences des logiciels, au matériel et/ou à la gestion de la maintenance et du support grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Parmi les éléments suivants, lesquels ont permis à votre entreprise de réaliser des économies par rapport à votre environnement précédent ? »



Base : 103 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

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

- L'entreprise de référence tire pleinement parti de la suite de produits de CDSS de Palo Alto Networks.
- Avec l'ancien système, l'entreprise surprovisionnait les ressources pour les pare-feu de 25 % (ce que le modèle de consommation flexible récemment annoncé pourrait éviter).

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- Les anciennes solutions de sécurité et la possibilité d'interrompre les contrats.
- Les besoins actuels en matière de sécurité et utilisation des produits de CDSS de Palo Alto Networks.
- Les pratiques typiques de croissance et de surprovisionnement.

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 573 800 USD sur trois ans.

Coûts évités et réduits de l'infrastructure de sécurité

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
E1	Coûts des services de renseignements sur les menaces	Résultats de l'enquête	71 037 USD	71 037 USD	71 037 USD
E2	Coûts des pare-feu de sécurité mis hors service	Résultats de l'enquête	63 665 USD	63 665 USD	63 665 USD
E3	Coûts des appareils d'IDS/d'IPS	Résultats de l'enquête	55 590 USD	55 590 USD	55 590 USD
E4	Coûts de la sécurité du DNS (p. ex. passerelle web sécurisée)	Résultats de l'enquête	21 704 USD	21 704 USD	21 704 USD
E5	Coûts de l'analyse des logiciels malveillants et de la protection contre les menaces avancées/inconnues (p. ex. protection contre les menaces avancées)	Résultats de l'enquête	18 390 USD	18 390 USD	18 390 USD
E6	Coûts de la sécurité de l'Internet des objets (IoT) ou protection des périphériques réseau non gérés	Résultats de l'enquête	12 389 USD	12 389 USD	12 389 USD
E7	Surprovisionnement évité des pare-feu physiques	A1*25 %*1 000	25 000 USD	6 250 USD	7 813 USD
Et	Coûts évités et réduits de l'infrastructure de sécurité	E1+E2+E3+E4+E5+E6+E7	267 774 USD	249 024 USD	250 586 USD
	Ajustement en fonction des risques	↓10 %			
Etr	Coûts évités et réduits de l'infrastructure de sécurité (bénéfices ajustés en fonction des risques)		240 996 USD	224 121 USD	225 527 USD
	Total sur trois ans : 690 645 USD			**Valeur actuelle sur trois ans : 573 754 USD**	

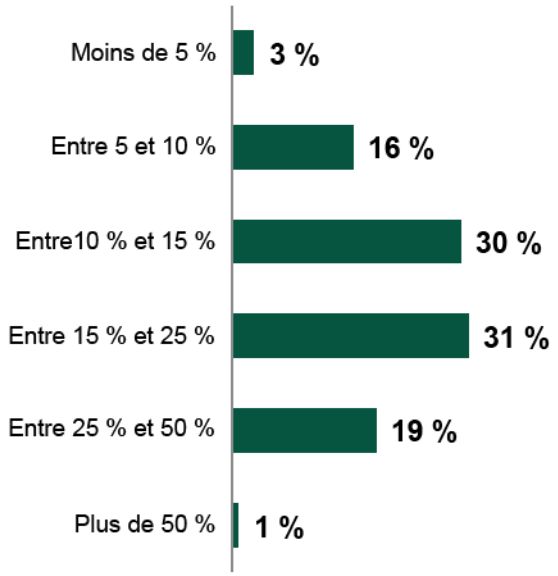
RÉDUCTION DU RISQUE DE VIOLATION DES DONNÉES

Preuves et données. Selon les personnes interrogées, leur entreprise était en mesure d'améliorer sa posture de sécurité globale, de réduire les surfaces d'attaque et de passer à des modèles Zero Trust pour la sécurité réseau**.** Grâce à une solution centralisée et unifiée, les entreprises ont pu mettre en œuvre le modèle Zero Trust qui est pris en charge par la technologie de Palo Alto Networks.

« Nous avons évalué le pare-feu natif [du prestataire de services de cloud] et avons constaté qu'il n'effectuait pas une inspection approfondie des paquets. Nous ne disposions donc pas d'une protection appropriée contre les menaces. Les journaux n'étaient pas aussi pratiques. Nous n'avions pas d'interface d'administration centralisée comme c'est le cas avec Panorama. C'est donc ce genre de choses qui a renforcé la sécurité et la visibilité et nous a permis d'effectuer notre travail avec plus d'efficacité. »
Ingénieur en sécurité de l'information, services aux entreprises

- Selon les personnes interrogées d'entreprises qui s'appuyaient auparavant sur des solutions individuelles, ces dernières ne se complétaient pas nécessairement ou ne communiquaient pas entre elles. Le fait de disposer de plusieurs pare-feu et de solutions de sécurité réseau avancées a également entraîné des incohérences au niveau des politiques et des lacunes dans la couverture de sécurité, notamment entre les infrastructures sur site et dans le cloud.
- Avec les pare-feu VM-Series, les entreprises des personnes interrogées ont obtenu des solutions unifiées qu'elles pouvaient gérer de manière centralisée, ce qui a permis aux équipes de sécurité d'identifier et de combler facilement toute lacune. La fidélité des informations partagées entre les systèmes de sécurité est essentielle pour une prévention automatisée efficace des violations. Les CDSS de Palo Alto Networks viennent encore renforcer la sécurité réseau via une couverture et une assistance 24 heures sur 24 et 7 jours sur 7, avec en particulier des mises à jour automatiques de tous les pare-feu nouvelle génération (NGFW) pour offrir une protection contre les toutes dernières menaces.
- Le responsable mondial de l'ingénierie informatique dans l'industrie des boissons a déclaré : « Nous effectuons des audits internes annuels, et le nombre d'écarts concernant les réseaux et les pare-feu a diminué de 40 % par rapport à l'année précédente, en raison de la gouvernance et des politiques en place, et de la manière dont les règles sont créées. Nous pouvons facilement trouver et corriger les politiques périmées, en fonction des adresses IP, ou celles qui n'ont pas été rédigées en fonction des applications. »

Figure 12. « Vous avez constaté un délai moyen de découverte des incidents de sécurité plus rapide grâce aux pare-feu virtuels VM-Series de Palo Alto Networks (y compris quand ils sont utilisés avec un service de sécurité quelconque). Pouvez-vous estimer le pourcentage d'amélioration par rapport à votre environnement précédent ? »



Base : 70 décideurs en matière de sécurité du cloud
Source : une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, juin 2021

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

- Selon les données de Forrester, l'entreprise de référence subirait en moyenne 3,2 violations par an si elle s'en remettait à des solutions individuelles[2].
- Le coût d'une violation est de 53 USD par employé, sans compter la perte de productivité. Les coûts comprennent les éléments suivants :
    - Amendes auprès des organismes de réglementation
    - Poursuites judiciaires/remboursement des clients
    - Traitement des incidents
    - Perte de revenus
    - Réparation du capital-marque
    - Coût de récupération des clients
- Grâce aux pare-feu VM-Series, l'entreprise réduit la probabilité d'une violation des données de 20 % au bout de trois ans.
- Chaque violation touche 18 % de l'ensemble des employés et entraîne une perte moyenne de 3,6 heures par employé par violation. Ces coûts s'ajoutent aux coûts individuels mentionnés ci-dessus.

Risques. Les risques qui pourraient avoir une incidence sur la réalisation de ce bénéfice sont les suivants :

- L'impact que les pare-feu VM-Series ont sur la posture de sécurité globale de l'entreprise par rapport à sa solution précédente.
- Le pourcentage d'employés touchés par une violation et la durée des temps d'arrêt associée.
- Les salaires moyens des utilisateurs métiers.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 30 % et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 383 700 USD sur trois ans.

Réduction du risque de violation des données					
Réf.	**Indicateur**	**Source**	**Année 1**	**Année 2**	**Année 3**
F1	Nombre moyen de violations des données	Études Forrester	3,2	3,2	3,2
F2	Coût potentiel moyen d'une violation de données, sans compter les temps d'arrêt des utilisateurs internes	Études Forrester	265 000 USD	265 000 USD	265 000 USD
F3	Réduction de la probabilité d'une violation	Entreprise de référence	10 %	15 %	20 %
F4	**Coûts évités de remédiation, de résolution pour les clients, d'amendes, de reconstruction de la marque et de tous les autres coûts externes.**	**F1*F2*F3**	**84 800 USD**	**127 200 USD**	**169 600 USD**
F5	Nombre d'employés internes	Entreprise de référence	7 500	7 500	7 500
F6	Salaire horaire moyen d'un utilisateur métier	D8	42 USD	42 USD	42 USD
F7	Diminution/élimination de la productivité des utilisateurs internes, par violation (heures)	Études Forrester	3,6	3,6	3,6
F8	Pourcentage moyen d'employés concernés, par violation	Entreprise de référence	18 %	18 %	18 %
F9	**Coûts de la perte de productivité interne**	**F1*F3*F5*F6*F7*F8**	**65 318 USD**	**97 978 USD**	**130 637 USD**
Ft	Réduction du risque de violation des données	F4+F9	150 118 USD	225 178 USD	300 237 USD
	Ajustement en fonction des risques	↓30 %			
Ftr	Réduction du risque de violation des données (bénéfices ajustés en fonction des risques)		105 083 USD	157 624 USD	210 166 USD
	Total sur trois ans : 472 873 USD		**Valeur actuelle sur trois ans : 383 699 USD**		

BÉNÉFICES NON QUANTIFIÉS

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

- **Possibilité d'utiliser les compétences existantes pour éviter la formation et le recrutement.** La plupart des entreprises interrogées disposaient de ressources internes facilement disponibles pour déployer les pare-feu VM-Series. Cependant, selon les personnes interrogées dans celles qui n'en disposaient pas, il était relativement facile d'acquérir en externe les compétences nécessaires, en raison de la prévalence de l'utilisation de Palo Alto Networks. Le RSSI d'une entreprise de dispositifs médicaux a déclaré : « Les [produits] Palo Alto Networks sont suffisamment répandus pour que l'on puisse facilement trouver les compétences [nécessaires] et des personnes déjà formées. »
- **Évolutivité et flexibilité améliorées.** Selon les personnes interrogées, les pare-feu VM-Series pouvaient être rapidement déployés ou retirés selon les besoins en raison de leur format virtuel. Cela permet aux entreprises de s'adapter rapidement à l'évolution des besoins tout en contrôlant les coûts. Le RSSI dans le secteur des dispositifs médicaux a déclaré : « L'année dernière, en raison de la pandémie de COVID-19, nous avons dû multiplier notre production par 20. Cela a nécessité la mise à l'échelle de systèmes qui n'étaient pas nécessairement évolutifs. Nous n'aurions pas pu le faire aussi rapidement avec l'ancien matériel. »

- **Compétitivité améliorée.** Selon certaines personnes interrogées, leur entreprise avait fait de l'utilisation des produits Palo Alto Networks un avantage concurrentiel pour la prestation de services technologiques. Un expert senior en réseaux dans le secteur des services informatiques a déclaré : « Je pense que [mon entreprise] s'en est servie pour inciter nos clients à ne pas se contenter de s'intéresser au cloud public, mais également aux clouds privés. S'il existe d'autres réglementations, comme le GDPR [règlement général sur la protection des données] ou autre, nous pourrions alors proposer [au client] une solution sécurisée dans le cloud privé. Donc je pense que cela pourrait nous être bénéfique. »
- **Adoption de nouveaux cas d'utilisation, et réduction des coûts et des nouveaux vecteurs de menace.** Certaines entreprises ont utilisé des pare-feu VM-Series pour sécuriser des ressources situées à la périphérie de leur réseau, telles que les kiosques de vente au détail.
  Le responsable mondial de l'ingénierie informatique d'une entreprise de boissons a déclaré : « Nous utilisions [nos kiosques en magasin] sur un réseau 5G privé, et [les employés] avaient l'habitude d'avoir des cartes 5G. Mais une fois que [le programme] a pris de l'ampleur, nous nous sommes dit : "Ok, nous avons besoin d'une autre façon de faire." Les gens volaient ces cartes 5G. Nous nous sommes donc associés à Palo Alto Networks, qui a pu constituer pour nous un package spécial qui permet à ces machines de communiquer avec nos pare-feu VM-Series ou un VPN. Maintenant, nous pouvons mettre ces machines dans l'environnement des clients, et nous n'avons plus besoin d'aller acheter des cartes 5G. C'est ce que nous a permis le partenariat avec Palo Alto Networks. Ils ont programmé pour nous un terminal client spécial que ces machines peuvent utiliser, ce qui nous
  a permis de réaliser des économies considérables dans ce domaine. »
- **Garantie que la sécurité n'est pas un obstacle aux efforts de transformation digitale.** Les équipes de sécurité ont pour mandat de veiller à ce que les activités soient aussi sécurisées que possible, mais elles ne veulent pas entraver les efforts de transformation digitale. Avec les pare-feu VM-Series, les équipes ont pu déployer rapidement des pare-feu et atteindre le niveau de sécurité requis pour que leur entreprise puisse maximiser les avantages de leur migration vers le cloud public et hybride.

FLEXIBILITÉ

La valeur de la flexibilité est propre à chaque client. Il existe plusieurs scénarios dans lesquels un client peut implémenter les pare-feu VM-Series de Palo Alto Networks, puis se rendre compte plus tard qu'ils offrent d'autres utilisations et opportunités commerciales.

Palo Alto Networks a récemment adopté un modèle de consommation flexible en lieu et place des modèles traditionnels de licence perpétuelle et d'accord de licence pour entreprise (ELA) que les entreprises des personnes interrogées utilisaient auparavant. Grâce à un modèle de consommation flexible, les entreprises ne paient que pour les pare-feu et les services de sécurité dont elles ont besoin à un moment donné, ce qui leur permet d'augmenter ou de réduire leur capacité en fonction de l'utilisation. Cette flexibilité supplémentaire a permis aux entreprises des personnes interrogées de réaliser des économies supplémentaires sur les coûts des pare-feu.

La flexibilité peut également être quantifiée lorsqu'elle est évaluée dans le cadre d'un projet spécifique (voir l'Annexe A pour une description détaillée).

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
Gtr	Licences des pare-feu	0 USD	321 300 USD	401 625 USD	502 031 USD	1 224 956 USD	1 001 196 USD
Htr	Efforts de déploiement internes	3 407 USD	0 USD	852 USD	1 065 USD	5 324 USD	4 911 USD
Itr	Administration continue	0 USD	177 188 USD	177 188 USD	177 188 USD	531 563 USD	440 639 USD
Jtr	Appliances en marque blanche	105 000 USD	0 USD	26 250 USD	32 813 USD	164 063 USD	151 347 USD
	Total des coûts (ajusté en fonction des risques)	108 407 USD	498 488 USD	605 914 USD	713 096 USD	1 925 905 USD	1 598 093 USD

LICENCES DES PARE-FEU

Preuves et données. Selon les personnes interrogées, Palo Alto Networks propose des prix compétitifs avec différentes tailles de pare-feu VM-Series et différents niveaux d'abonnement pour répondre aux besoins des clients.

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

- L'entreprise de référence déploie 100 pare-feu VM-Series au cours de l'Année 1, et la base de déploiement et d'abonnement augmente de 25 % par an.
- Pour modéliser ce coût pour l'entreprise de référence, Forrester a utilisé les modèles ELA que les entreprises des personnes interrogées adoptaient avant de disposer des pare-feu VM-Series, mais Palo Alto Networks est passé à un modèle de tarification basé sur la consommation.

Risques. Les risques qui peuvent avoir un impact sur ces coûts sont les suivants :

- La taille du déploiement des pare-feu.
- Le nombre de services de sécurité fournis via le cloud et le niveau de support nécessaire.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques (taux d'actualisation de 10 %) de 1 million USD sur trois ans.

Licences des pare-feu

Réf.	Indicateur	Source	Initial	Année 1	Année 2	Année 3
G1	Coût par licence par pare-feu VM-Series	Entretiens		3 060 USD	3 060 USD	3 060 USD
G2	Nombre total de pare-feu VM-Series déployés	Entreprise de référence		100	125	156
Gt	Licences des pare-feu	F1*F2		306 000 USD	382 500 USD	478 125 USD
	Ajustement en fonction des risques	↑5 %				
Gtr	Licences des pare-feu (coûts ajustés en fonction des risques)		0 USD	321 300 USD	401 625 USD	502 031 USD
	Total sur trois ans : 1 224 956 USD			**Valeur actuelle sur trois ans : 1 001 196 USD**		

EFFORTS DE DÉPLOIEMENT INTERNES

Preuves et données. Selon les personnes interrogées, bien que le déploiement des produits Palo Alto Network ait pris un certain temps et nécessité des efforts, les déploiements dans leur entreprise se sont déroulés sans heurts et n'ont pas connu de retards ou de blocages importants, en raison de la technologie cohérente de Palo Alto Network et de la capacité à mettre automatiquement à jour les politiques sur le réseau.

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

- L'entreprise est déjà un utilisateur de Palo Alto Networks.
- Les coûts de déploiement ne tiennent pas compte du temps nécessaire à l'implémentation des produits auxiliaires (p. ex. Palo Alto Networks SD-WAN, Prisma Cloud, Panorama, etc.)
- Le déploiement des nouveaux pare-feu VM-Series prend 30 minutes.
- Le salaire annuel moyen toutes charges comprises d'un employé chargé de l'exploitation réseau est de 135 000 USD.

Risques. Les risques qui peuvent avoir un impact sur ces coûts sont les suivants :

- L'utilisation que fait déjà l'entreprise des produits Palo Alto Networks et sa familiarité avec ces derniers.
- Les salaires moyens des membres de l'équipe de déploiement.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 4 900 USD sur trois ans.

Efforts de déploiement internes

Réf.	Indicateur	Source	Initial	Année 1	Année 2	Année 3
H1	Durée du déploiement (heures) (arrondie)	A1*0,5	50		13	16
H2	Salaire horaire moyen d'un membre de l'équipe de déploiement	Hypothèse	65 USD		65 USD	65 USD
Ht	Coûts des efforts de déploiement internes	H1*H2	3 245 USD	0 USD	811 USD	1 014 USD
	Ajustement en fonction des risques	↑5 %	·			
Htr	Efforts de déploiement internes (coûts ajustés en fonction des risques)		3 407 USD	0 USD	852 USD	1 065 USD
	Total sur trois ans : 5 324 USD		**Valeur actuelle sur trois ans : 4 911 USD**			

ADMINISTRATION CONTINUE

Preuves et données. Pour les personnes interrogées, les pare-feu VM-Series nécessitent beaucoup moins d'administration continue que les solutions traditionnelles. Bien que leurs entreprises aient automatisé ou consolidé de nombreuses tâches auparavant manuelles, elles ont demandé un petit effort à leurs équipes internes pour la gestion des pare-feu et des politiques, le dépannage, les mises à jour et d'autres tâches administratives.

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

- L'entreprise de référence compte 10 ETP impliqués dans l'administration continue de son déploiement VM-Series.
- Les ressources internes consacrent 15 % de leur temps à la seule administration des pare-feu.
- Le salaire annuel moyen des ETP concernés est de 112 500 USD.

Risques. Les risques qui peuvent avoir un impact sur ce coût sont les suivants :

- La taille et la portée du déploiement.
- Les compétences internes de l'entreprise et sa capacité à automatiser les tâches.
- Les salaires annuels moyens

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 440 600 USD sur trois ans.

Administration continue

Réf.	Indicateur	Source	Initial	Année 1	Année 2	Année 3
I1	Nombre d'ETP impliqués dans l'administration continue	Entreprise de référence		10	10	10
I2	Pourcentage du temps consacré à l'administration des pare-feu	Entretiens		15 %	15 %	15 %
I3	Taux de rémunération annuel moyen des ETP	Hypothèse		112 500 USD	112 500 USD	112 500 USD
It	Coût de l'administration continue	I1*I2*I3		168 750 USD	168 750 USD	168 750 USD
	Ajustement en fonction des risques	↑5 %				
Itr	Administration continue (coût ajusté en fonction des risques)		0 USD	177 188 USD	177 188 USD	177 188 USD
	Total sur trois ans : 531 563 USD		**Valeur actuelle sur trois ans : 440 639 USD**			

APPLIANCES EN MARQUE BLANCHE

Preuves et données. De nombreuses entreprises interrogées qui exploitent plusieurs centres de données ou succursales ont choisi de déployer leurs pare-feu sur du matériel standard rentable. Selon les personnes interrogées des entreprises qui ont choisi cette voie, l'installation était facile et les employés des succursales sans expérience informatique pouvaient installer le matériel.

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

- L'entreprise de référence déploie ses pare-feu VM-Series à l'aide de nouvelles appliances en marque blanche.
- Comme le déploiement croît de 25 % par an, l'entreprise achète de nouvelles appliances.
- Le coût moyen du matériel standard nécessaire au déploiement d'un pare-feu VM-Series est de 1 000 USD.

Risques. Les risques qui peuvent avoir un impact sur ces coûts sont les suivants :

- La taille du déploiement.
- Les prix du matériel standard.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 5 %, et a ainsi obtenu une valeur actuelle (VA) ajustée en fonction des risques de 151 300 USD sur trois ans.

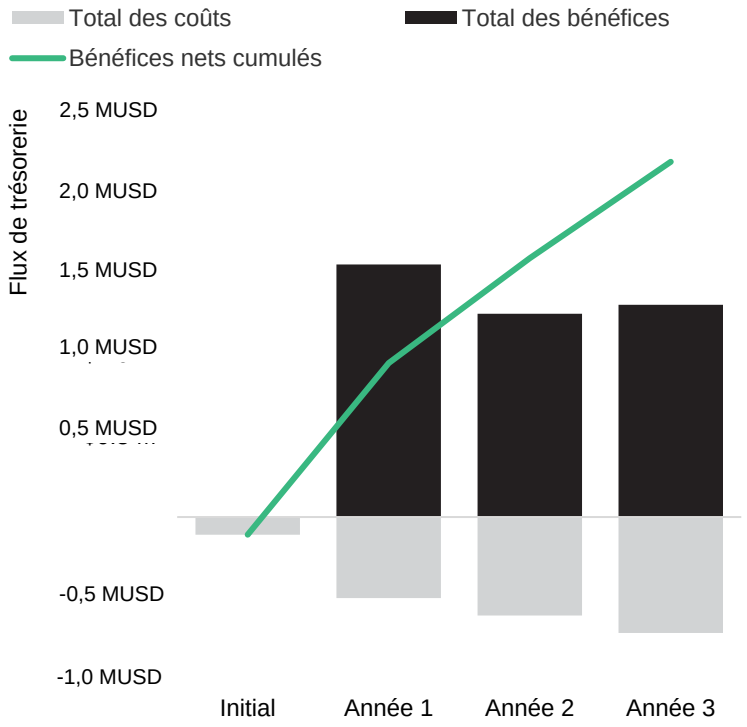
Appliances en marque blanche

Réf.	Indicateur	Source	Initial	Année 1	Année 2	Année 3
J1	Appliances en marque blanche	Entreprise de référence	100	0	25	31
J2	Prix par appliance	Entretiens	1 000 USD	1 000 USD	1 000 USD	1 000 USD
Jt	Coût des appliances en marque blanche	J1*J2	100 000 USD	0 USD	25 000 USD	31 250 USD
	Ajustement en fonction des risques	↑5 %	·			
Jtr	Appliances en marque blanche (coûts ajustés en fonction des risques)		105 000 USD	0 USD	26 250 USD	32 813 USD
	Total sur trois ans : 164 063 USD			**Valeur actuelle sur trois ans : 151 347 USD**		

Bilan financier

INDICATEURS CONSOLIDÉS SUR TROIS ANS ET AJUSTÉS 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 le délai de récupération 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 récupération ajustées en fonction des risques s'obtiennent en appliquant des facteurs d'ajustement aux résultats bruts des sections 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	(108 407 USD)	(498 488 USD)	(605 914 USD)	(713 096 USD)	(1 925 905 USD)	(1 598 093 USD)
Total des bénéfices	0 USD	1 554 294 USD	1 251 188 USD	1 306 291 USD	4 111 774 USD	3 428 472 USD
Bénéfices nets	(108 407 USD)	1 055 807 USD	645 273 USD	593 195 USD	2 185 868 USD	1 830 379 USD
ROI						115 %
Délai de récupération (mois)						<6

Annexe A : Total Economic Impact

Total Economic Impact est une méthodologie élaborée par Forrester Research qui améliore les processus de décision d'une entreprise en matière de technologies. D'une part, elle aide les fournisseurs à communiquer la proposition de valeur de leurs produits et services aux clients. D'autre part, elle aide les entreprises à démontrer, justifier et concrétiser la valeur réelle des initiatives en matière de technologies de l'information auprès de leur direction et des autres parties prenantes.

L'APPROCHE TOTAL ECONOMIC IMPACT

Les bénéfices représentent la valeur apportée à l'entreprise par le produit. La méthodologie 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 bénéfices attendus du produit. La catégorie de coûts du TEI correspond aux coûts incrémentaux 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 indiquant l'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, mais d'autres projets peuvent présenter 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

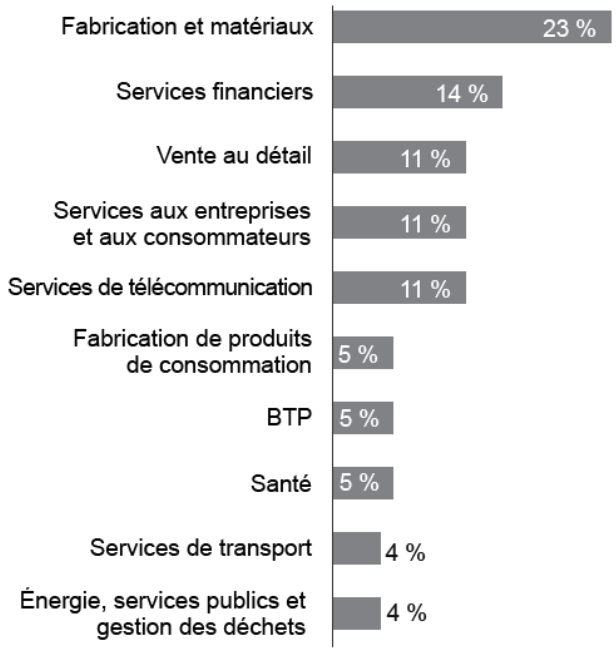
Taux d'intérêt utilisé dans l'analyse des flux de trésorerie pour prendre en compte la valeur temps de l'argent. Les entreprises utilisent généralement des taux d'actualisation compris entre 8 et 16 %.

DÉLAI DE RÉCUPÉRATION

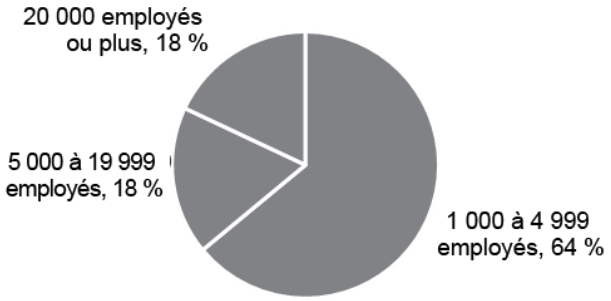
Seuil de rentabilité d'un investissement. C'est le stade auquel les bénéfices nets (déduction faite des coûts) sont équivalents à l'investissement ou au coût initial.

Annexe B : Données de l'enquête

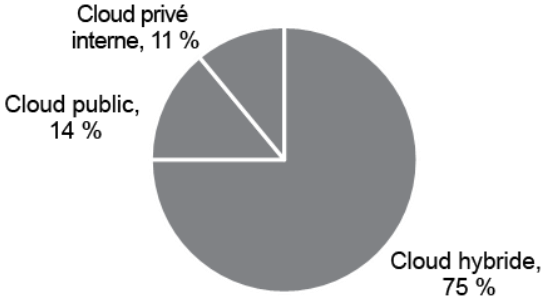
« Parmi les propositions ci-après, laquelle décrit le mieux le secteur d'activité de votre entreprise ? »



« Selon vous, combien d'employés travaillent pour votre entreprise dans le monde ? »



« Où votre entreprise héberge-t-elle actuellement ses données, ses applications et ses charges de travail ? »



« Dans quel pays êtes-vous basé ? »

53 %	États-Unis
19 %	Allemagne
17 %	Royaume-Uni
6 %	France
5 %	Australie

Base : 132 décideurs en matière de sécurité du cloud (la somme des pourcentages n'est pas équivalente à 100, car les valeurs ont été arrondies)
Source : « PAN Virtual Firewalls TEI », une étude menée par Forrester Consulting pour le compte de Palo Alto Networks, octobre 2021

Annexe C : Notes finales

[1] Total Economic Impact 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. D'autre part, elle aide les entreprises à démontrer, justifier et concrétiser la valeur réelle des initiatives en matière de technologies de l'information auprès de leur direction et des autres parties prenantes.

[2] Source : « Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q4 2020 ».


FORRESTER®