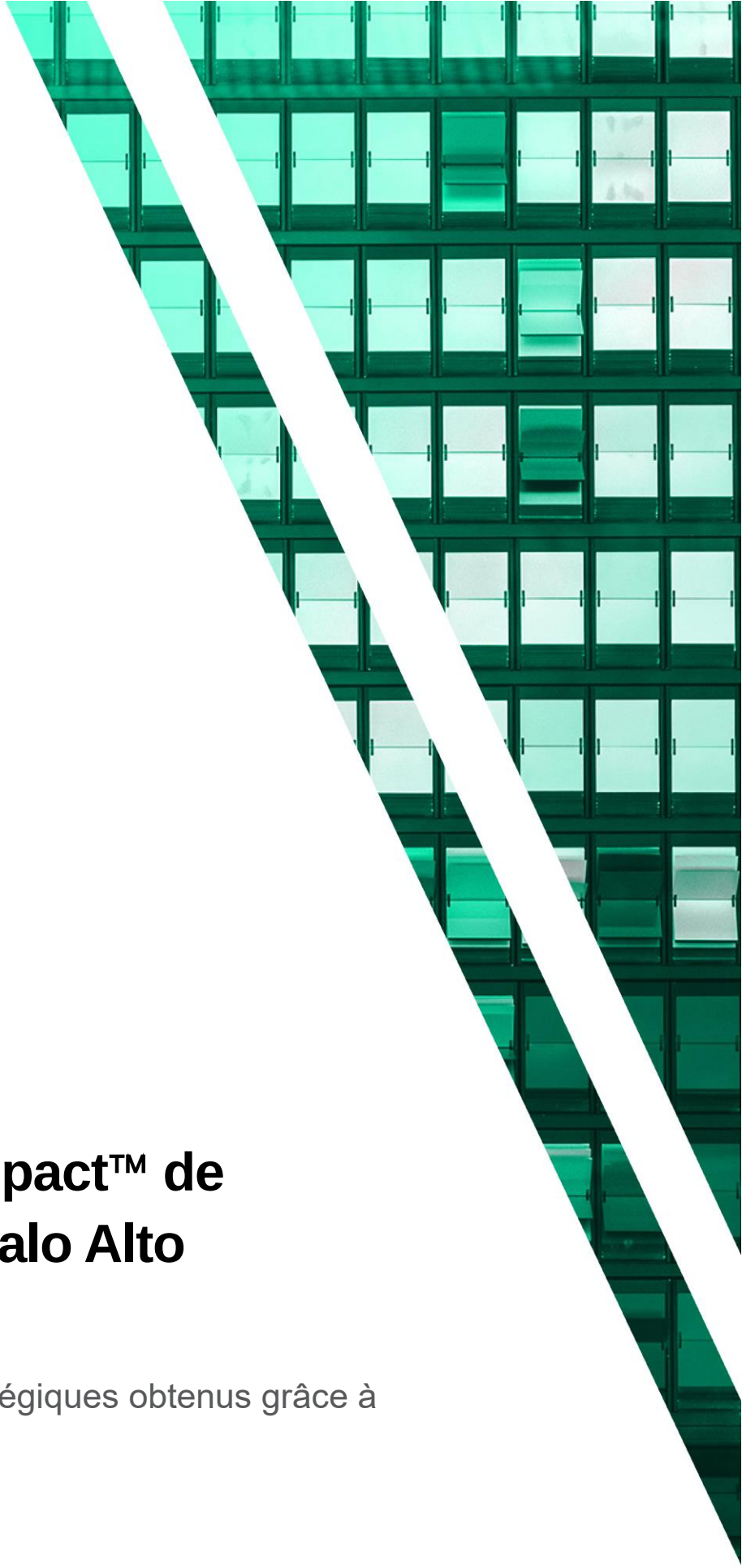
FORRESTER®



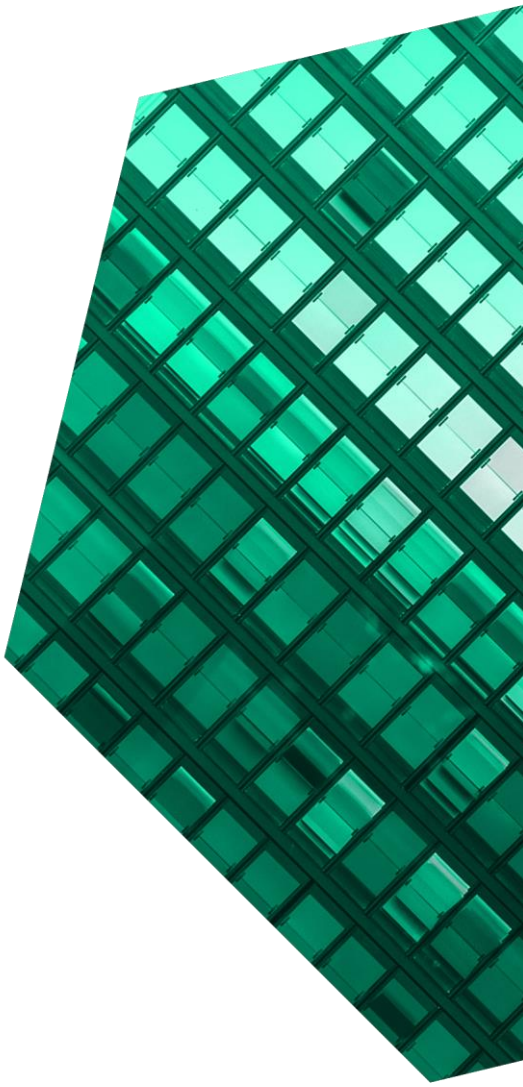
Total Economic Impact™ de Prisma SASE de Palo Alto Networks

Économies et avantages stratégiques obtenus grâce à Palo Alto Networks

DÉCEMBRE 2023

Table des matières

Équipe de consultants : *Adi Sarosa*
Isabel Carey



À PROPOS DE FORRESTER CONSULTING

Forrester Consulting propose des services de conseil indépendants et objectifs, basés sur un travail de recherche, pour aider les dirigeants à obtenir des résultats clés. Alimentés par nos recherches axées sur le client, les consultants chevronnés de Forrester collaborent avec les dirigeants pour mettre en œuvre leurs priorités spécifiques en utilisant un modèle d'engagement unique qui garantit un impact durable. Pour en savoir plus, rendez-vous sur forrester.com/consulting.

Résumé

Les entreprises fortement distribuées, c'est-à-dire implantées sur de nombreux sites ou qui comptent un pourcentage élevé d'effectifs distants, recherchent souvent une architecture Secure Access Service Edge (SASE), principalement car elle permet d'authentifier les utilisateurs et de les autoriser à se connecter à leur plateforme et à passer par celle-ci. Cependant, SASE est une technologie transformatrice qui centralise de multiples fonctionnalités de connectivité réseau et de sécurité, au sein d'une solution unifiée dotée d'une interface et d'un lac de données uniques. Le choix du fournisseur de solutions qui convient peut être une décision à la fois risquée et payante.

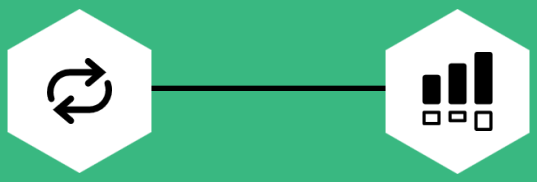
Prisma SASE fait converger la sécurité réseau, le SD-WAN et la gestion autonome de l'expérience numérique (autonomous digital experience management ou ADEM) dans le cloud. Cela permet de sécuriser toutes les applications utilisées par une entreprise, quel que soit le lieu où se trouve l'utilisateur.

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 Prisma SASE[1]. Le but de cette étude est de fournir aux lecteurs un cadre de référence qui leur permet d'évaluer l'impact financier potentiel de l'utilisation de Prisma SASE dans leur entreprise.

Pour mieux comprendre les bénéfices, les coûts et les risques associés à cet investissement, Forrester a interrogé quatre représentants d'entreprises qui utilisaient déjà Prisma SASE. Pour les besoins de cette étude, Forrester a regroupé les expériences des personnes interrogées et combiné les résultats en une seule entreprise de référence, soit une grande entreprise distribuée, qui réalise un chiffre d'affaires annuel de 7 milliards de dollars et compte 50 000 employés, dont 33 % travaillent à distance ou en mode hybride.

Avant d'utiliser Prisma SASE, les entreprises étaient généralement obligées de composer avec une sécurité aléatoire et insuffisante, une expérience utilisateur médiocre en raison de la nécessité de réacheminer le trafic vers des centres de données et une faible évolutivité alors qu'elles adoptaient de plus en plus le travail hybride et le cloud. De plus, la gestion des services d'accès de ces entreprises impliquait l'installation de différentes solutions ponctuelles pour sécuriser leurs environnements. Elles manquaient de technologies de sécurité modernes, ce qui impactait les équipes de sécurité et les équipes informatiques qui s'efforçaient de suivre l'évolution des besoins de l'entreprise. Les initiatives de transformation numérique déplaçaient davantage de données, d'applications et de processus dans le cloud, tandis que d'autres fonctions essentielles de l'entreprise continuaient d'être gérées sur site. Du fait de cette approche fragmentaire, les entreprises des personnes interrogées devaient travailler avec de nombreux fournisseurs différents pour leur infrastructure de sécurité, et les équipes chargées des opérations de sécurité (SecOps) rencontraient des difficultés pour intégrer les technologies, tirer parti des analyses, appliquer des politiques

CHIFFRES CLÉS



Retour sur investissement (ROI)
107 %

Valeur actuelle nette (VAN)
9,49 M$

cohérentes et offrir une expérience uniforme aux utilisateurs finaux.

Après avoir investi dans Prisma SASE, les personnes interrogées ont indiqué qu'elles étaient parvenues à réduire en grande partie le temps consacré à certaines activités de gestion et à leurs dépenses fournisseurs, ce qui a permis de réaliser des gains d'efficacité opérationnelle. Elles ont pu améliorer la productivité des utilisateurs finaux, notamment celle des effectifs distants et en déplacement. Elles ont également noté que Prisma SASE réduisait considérablement la probabilité d'une atteinte à la sécurité des données lorsqu'il était associé à d'autres solutions de Palo Alto Networks installées dans leur environnement.

Gains d'efficacité dans la gestion SASE et dans la modification des politiques

75 %

PRINCIPALES CONCLUSIONS

Bénéfices quantifiés. Pour l'entreprise de référence, les bénéfices quantifiés en valeur actuelle (VA) ajustée en fonction des risques sur une période de trois ans sont les suivants :

- **Gains d'efficacité de 75 % dans la gestion SASE et dans la modification des politiques, ainsi que dans la réponse aux incidents de sécurité, et gain de temps de 80 % pour la mise à l'échelle et la mise en place de nouveaux sites.** Alors qu'auparavant l'entreprise de référence déployait plusieurs équipes pour la gestion de sa solution SASE, les équipes SecOps et NetOps (opérations réseau) réalisent désormais des gains de temps et d'efficacité sur de multiples activités grâce à Prisma SASE. Sur trois ans, ces gains d'efficacité représentent 2,2 millions de dollars pour l'entreprise de référence.
- **Amélioration de la productivité des utilisateurs finaux grâce à une meilleure disponibilité des systèmes et à une réduction des intrusions dans leur réseau, ce qui représente une valeur totale pour l'entreprise de 12,2 millions de dollars sur trois ans.** L'entreprise de référence a également amélioré la productivité des utilisateurs finaux, en particulier lorsqu'ils travaillent à distance ou sont en déplacement, en réduisant les perturbations causées par leurs activités de sécurité et en assurant une plus grande disponibilité de leur environnement. Ce résultat est le fruit d'une intégration et d'une compatibilité accrues des différentes solutions Palo Alto Networks ainsi que d'une meilleure performance globale. Sur trois ans, cette amélioration de la productivité des utilisateurs finaux représente une valeur de près de 12,2 millions de dollars pour l'entreprise de référence.
- **Réduction de 50 % de la probabilité d'une atteinte à la sécurité des données au bout de trois ans.** En remplaçant de multiples solutions de sécurité distinctes par une solution intégrée unique, Prisma SASE comble mieux les failles de sécurité qui existaient auparavant dans l'entreprise de référence. Par conséquent, cela réduit la probabilité d'une atteinte importante à la sécurité des données. Sur trois ans, cette réduction du risque d'atteinte à la sécurité des données représente une valeur de près de 3 millions de dollars pour l'entreprise de référence.
- **Économies générées par la rationalisation de l'infrastructure réseau et de sécurité, soit 846 000 dollars sur trois ans.** L'utilisation de Prisma SASE permet également à l'entreprise de référence de diminuer le nombre de ses

fournisseurs de technologies de sécurité et d'éviter ainsi certaines dépenses. Sur trois ans, les économies réalisées grâce à la diminution du nombre de fournisseurs s'élèvent à 846 000 $ pour l'entreprise de référence.

Bénéfices non quantifiés. Les bénéfices qui apportent de la valeur à l'entreprise de référence, mais ne sont pas quantifiés dans cette étude comprennent les suivants :

- **Amélioration de la visibilité sur l'environnement de sécurité.** Prisma SASE permet à l'entreprise de référence de mieux surveiller le trafic et de comprendre réellement ce qui se passe sur son réseau.
- **Amélioration de l'expérience des employés.** Qu'ils soient membres de l'équipe chargée de la sécurité ou utilisateurs finaux, les employés de l'entreprise de référence apprécient aussi la facilité et le confort d'utilisation de Prisma SASE et ont la certitude d'être très bien protégés contre les attaques et les menaces potentielles. Outre l'amélioration de la productivité quantifiée ci-dessus, ces bénéfices peuvent également avoir un impact sur l'attachement des parties prenantes internes et externes à la marque ainsi qu'à l'entreprise en tant que telle.

Coûts. Les coûts sur trois ans en VA ajustée en fonction des risques pour l'entreprise de référence incluent les suivants :

- **Les coûts d'installation et de déploiement s'élèvent à 436 000 dollars sur trois ans.** Le déploiement et l'installation de la solution Palo Alto Networks dans l'ensemble de l'entreprise de référence nécessitent du temps et de la main-d'œuvre. Lors du déploiement de Prisma SASE et des autres solutions de Palo Alto Networks (c.-à-d. NGFW et CDSS), on suppose que 20 % du temps du personnel chargé de ce déploiement est consacré à Prisma SASE.
- **Les coûts de formation et l'investissement en temps pour la gestion en continu s'élèvent à 63 000 dollars sur trois ans.** Palo Alto Networks nécessite moins de formation que les solutions traditionnelles. Selon les personnes interrogées, les formations proposées étaient plus efficaces et économiques et permettaient aux employés d'acquérir rapidement les connaissances nécessaires et d'élargir leurs compétences. Une fois formée, l'équipe consacre une partie de son temps à la maintenance et à la gestion en continu du système.
- **Les coûts annuels de licence de Prisma SASE de Palo Alto Networks s'élèvent à 8,3 millions de dollars sur trois ans.** Le coût de Prisma SASE comprend le paiement de Prisma Access, celui de l'appliance physique Prisma SD-WAN et celui de l'abonnement, qui dépendent tous du nombre de sites sur lesquels ils sont installés.

Perspective de Forrester : Fusion des équipes chargées de la sécurité et des réseaux

Bien que la relation entre les réseaux et la sécurité soit ancienne et complexe, l'approche consistant à les gérer séparément n'est pas acceptable, car elle a tendance à annuler les bénéfices des initiatives numériques.

Actuellement, une infrastructure réseau à l'échelle de l'entreprise relie les actifs commerciaux, les clients, les partenaires et les biens numériques de l'entreprise pour connecter l'écosystème d'affaires tout entier. Or, cela n'est possible que si la sécurité fait partie de l'ADN du réseau.

Source : « Introducing The Zero Trust Edge Architecture For Security And Network Services », Forrester Research, Inc., 2 août 2021.

Les entretiens avec les personnes interrogées ainsi que l'analyse financière ont révélé que l'entreprise de référence avait enregistré des bénéfices de 18,34 millions de dollars sur trois ans, pour des coûts de 8,85 millions de dollars, soit une valeur actuelle nette (VAN) de 9,49 millions de dollars et un retour sur investissement (ROI) de 107 %.

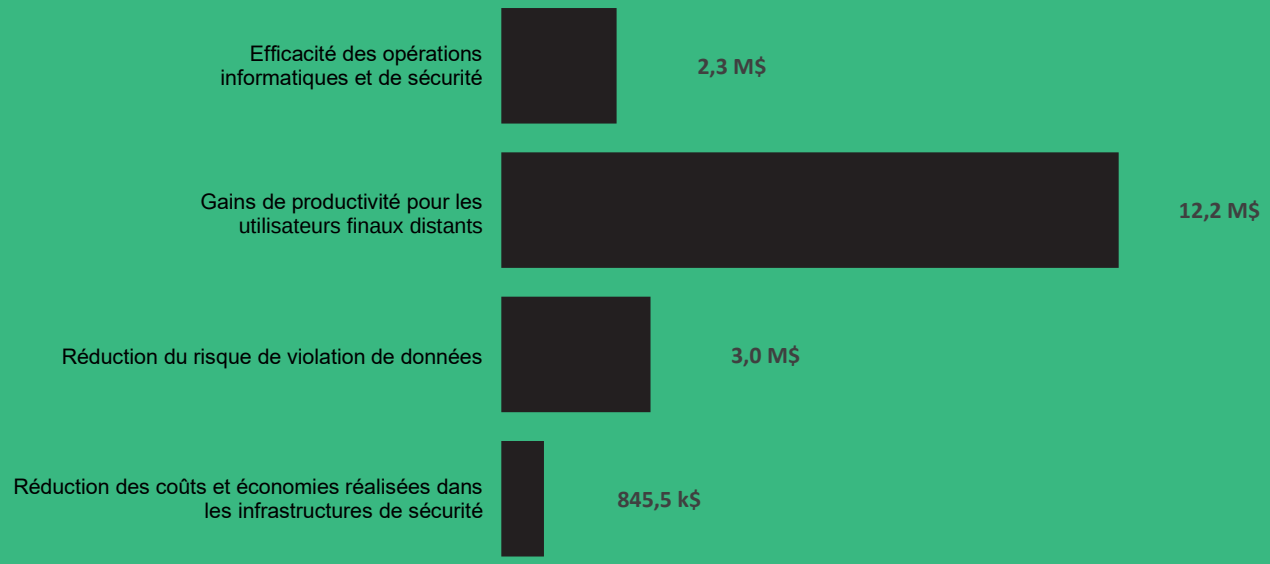
ROI
107 %

BÉNÉFICES EN VA
18,34 M$

VAN
9,49 M$

DÉLAI DE RÉCUPÉRATION
< 6 mois

Bénéfices (sur trois ans)



« Les gains de productivité obtenus par les utilisateurs, même distants, le fait de ne pas avoir à se soucier de l'intégration avec d'autres systèmes et le niveau de sécurité atteint : rien de tout cela n'est possible sans Prisma SASE. »

— Architecte principal, secteur de la santé

CADRE ET MÉTHODOLOGIE DE L'ÉTUDE TEI

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

L'objectif de ce cadre de référence est d'identifier les différents facteurs, tels que les coûts, les bénéfices, la flexibilité et les risques, qui influencent la décision d'investissement. Forrester a utilisé une approche en plusieurs étapes pour évaluer l'impact que Prisma SASE peut 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 responsables des prises de décisions, des opérations et du reporting dans le domaine de la cybersécurité. Les questions posées aux participants visaient à évaluer les stratégies des dirigeants en matière de cybersécurité et les éventuelles atteintes à la sécurité survenues dans leur entreprise. Les personnes interrogées ont accepté de participer à l'enquête via un panel de recherche tiers ; ce dernier a réalisé l'enquête pour le compte de Forrester en novembre 2020.

AVERTISSEMENTS

Remarques à l'intention des lecteurs :

L'étude est commandée par Palo Alto Networks et réalisée par Forrester Consulting. Elle n'est pas destinée à être utilisée en tant qu'analyse concurrentielle.

Forrester ne fait aucun postulat concernant le ROI potentiel que d'autres entreprises obtiendront. 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 Prisma SASE.

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

Nous nous sommes entretenus avec les parties prenantes de Palo Alto Networks et les analystes de Forrester pour recueillir des données relatives à Prisma SASE.

ENTRETIENS

Nous nous sommes entretenus avec quatre représentants issus d'entreprises qui utilisent Prisma SASE pour obtenir des données concernant les coûts, les bénéfices et les risques.

ENTREPRISE DE RÉFÉRENCE

Nous avons défini l'entreprise de référence sur la base des caractéristiques des entreprises des personnes interrogées.

CADRE DU MODÈLE FINANCIER

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

ÉTUDE DE CAS

Nous avons utilisé les quatre éléments fondamentaux du TEI pour modéliser l'impact de l'investissement : bénéfices, coûts, flexibilité et risques. Étant donné la sophistication croissante des analyses de ROI liées aux investissements informatiques, la méthodologie TEI de Forrester dresse un tableau complet de l'impact économique total des décisions d'achat. Veuillez consulter l'Annexe A pour de plus amples informations sur la méthodologie TEI.

Le parcours client avec Prisma SASE de Palo Alto Networks

Facteurs qui ont conduit à investir dans Prisma SASE

Entretiens			
Rôle	**Secteur d'activité**	**Chiffre d'affaires**	**Nombre total d'employés**
Architecte principal	Santé	30 G$	15 000
Directeur de l'architecture et de l'ingénierie de la sécurité	Industrie manufacturière	17 G$	160 000
VP principal du service informatique	Services financiers	3 G$	3 000
Directeur principal	Hôtellerie	20 G$	380 000

PRINCIPAUX DÉFIS

Avant d'utiliser Prisma SASE, les personnes interrogées ont déclaré à Forrester qu'elles travaillaient généralement dans un environnement où la sécurité était aléatoire et insuffisante. Elles devaient souvent réacheminer le trafic réseau vers leurs centres de données pour appliquer la politique de sécurité, ce qui se traduisait par une expérience négative pour les utilisateurs finaux. De plus, l'élargissement à de nouveaux sites ainsi que la fourniture d'une connexion sécurisée aux effectifs hybrides et distants étaient extrêmement difficiles.

Les entreprises interrogées étaient régulièrement confrontées à des défis, notamment les suivants :

- **La nécessité de mettre à jour les systèmes de sécurité pour les adapter à un environnement de travail moderne.** Selon les personnes interrogées, les facteurs combinés de la croissance du travail à distance et en mode hybride, de l'adoption des technologies cloud et de la sophistication grandissante des cyberattaques les ont amenées à prendre conscience des failles de sécurité dans leur environnement actuel. Il était primordial de trouver un système de sécurité plus moderne et plus complet pour leur environnement de travail. L'architecte principal d'une entreprise du secteur de la santé a déclaré : « Nous n'avons pratiquement personne qui travaille à temps plein au bureau, c'est pourquoi nous nous appuyons fortement sur les solutions Prisma SASE de Palo Alto Networks ».

« L'un des plus grands risques auxquels nous sommes confrontés aujourd'hui est la vitesse d'adoption et d'évolution des technologies dans les entreprises. De plus en plus de personnes travaillent à distance. L'ancienne méthode pour assurer la sécurité consistait à connecter tout le monde au même réseau, dans des lieux clos. Cela ne fonctionne plus. »

Directeur de l'architecture et de l'ingénierie de la sécurité, industrie manufacturière

- **Le manque d'uniformité dans l'expérience utilisateur et l'impact sur la productivité.** Les personnes interrogées ont également noté que, dans leur ancien environnement, elles avaient subi de nombreuses perturbations, causées soit par des cybermenaces, soit par une mesure de sécurité prise pour répondre à une éventuelle menace et qui s'avérait être invasive pour l'ensemble du système. En conséquence, un grand nombre d'entreprises et d'utilisateurs finaux voyaient leur travail interrompu pendant un temps non négligeable, ce qui pouvait devenir très vite frustrant. Le vice-président principal du service informatique d'une entreprise dans le secteur des services financiers a déclaré : « Pour les utilisateurs, se servir de leur ordinateur portable à la maison ou au bureau constitue deux expériences totalement différentes, [avec] des technologies différentes au niveau du back-end. Cela peut perturber leur travail et les obliger à envoyer des demandes d'assistance ou à solliciter notre équipe chargée des opérations pour enquêter sur ce qui se passe. Si les politiques ne sont pas adaptées ou si un fournisseur ne prend pas en charge ce que l'utilisateur essaie de faire, c'est de ce point de vue très coûteux en termes de productivité ».

« Nous avions de nombreux problèmes de fiabilité avec notre VPN traditionnel avant de passer à Prisma Access. Interruption constante de la connexion, connectivité lente, latence élevée : cela représente une grosse perte de temps et de productivité pour les utilisateurs finaux. »

Vice-président principal du service informatique, services financiers

- **Des difficultés liées à l'évolutivité de l'ancien environnement de sécurité.** Enfin, selon les personnes interrogées, leur ancien système de sécurité n'était pas en mesure de répondre à la croissance de leur entreprise. Le directeur principal dans le secteur de l'hôtellerie a déclaré : « Notre entreprise s'est beaucoup développée. La gestion individuelle des routeurs est devenue un cauchemar. En particulier lorsque nous souhaitons modifier une politique. Traditionnellement, nous devons intervenir sur chaque routeur de l'environnement ».

OBJECTIFS DE L'INVESTISSEMENT

Les entreprises interrogées recherchaient une solution qui pouvait :

- **Améliorer l'efficacité de leur environnement de sécurité sur le plan opérationnel.** Les personnes interrogées ont indiqué qu'elles souhaitaient une solution qui leur ferait gagner du temps, de l'argent ou, idéalement, les deux à la fois, ce qui permettrait éventuellement de réaffecter des ressources à des tâches plus stratégiques. L'architecte principal dans le secteur de la santé a précisé : « L'une des raisons pour lesquelles nous avons opté pour Prisma SASE est que la configuration se fait entièrement dans le cloud. Nous n'avons plus à dépendre de centres de données ou de matériel dont nous devons nous occuper ».

  Le directeur principal dans le secteur de l'hôtellerie a ajouté : « La gestion centralisée et l'intégration avec d'autres solutions ont été les principaux [critères] dans notre processus de décision [qui nous ont conduits à choisir Palo Alto Networks]. »

- **Apporter de la fiabilité et de l'exhaustivité en termes de performances.** Les personnes interrogées ont également souligné que la performance de la solution avait été un autre facteur clé dans leur décision. Le directeur dans l'industrie manufacturière nous a fait part de son

expérience : « Nous avons choisi Palo Alto Networks parce qu'il s'agit de la meilleure technologie en matière de pare-feu. Nous souhaitions offrir une expérience de qualité aux utilisateurs finaux, tout en maximisant la sécurité ».

ENTREPRISE DE RÉFÉRENCE

Sur la base des entretiens, Forrester a défini un cadre de référence TEI, une entreprise de référence ainsi qu'une analyse du ROI qui illustre les domaines affectés financièrement. L'entreprise de référence est représentative des entreprises des quatre personnes interrogées. Elle est utilisée pour présenter l'analyse financière sous forme agrégée à 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 compte 50 000 employés et enregistre un chiffre d'affaires annuel de 7 milliards de dollars et dont 33 % du personnel travaille à distance ou en mode hybride. Elle possède 400 sites, comprenant le siège social, le centre de données, une infrastructure cloud, des succursales, ainsi que des sites de vente au détail et de production. En moyenne, l'équipe de sécurité de l'entreprise de référence traite 1 200 incidents par semaine, soit 62 400 au cours de la première année, chaque incident étant résolu en 2 heures en moyenne.

Caractéristiques du déploiement. L'entreprise utilise Prisma SASE de Palo Alto Networks pour relier les réseaux distants de ses sites de vente au détail et de ses succursales, ainsi que ses effectifs distants et hybrides. Elle tire parti des cycles de fin de vie et prend le temps de tester le déploiement, ce qui allonge les délais, mais assure aussi une transition en douceur depuis son ancienne solution. L'équipe de sécurité réseau est impliquée dans le déploiement.

Hypothèses principales

- **7 G$ de CA annuel**
- **50 000 employés**
- **33 % d'effectifs distants ou hybrides**
- **400 sites**
- **4 centres de données**

Analyse des bénéfices

Données chiffrées sur les bénéfices quantifiés applicables à l'entreprise de référence

Total des bénéfices

Réf.	Bénéfice	Année 1	Année 2	Année 3	Total	Valeur actuelle
Atr	Efficacité des opérations informatiques et de sécurité	911 250 $	920 363 $	929 475 $	2 761 088 $	2 287 368 $
Btr	Gains de productivité pour les utilisateurs finaux	4 925 580 $	4 925 580 $	4 925 580 $	14 776 740 $	12 249 188 $
Ctr	Réduction du risque de violation de données	1 189 320 $	1 189 320 $	1 189 320 $	3 567 960 $	2 957 663 $
Dtr	Réduction des coûts et économies réalisées dans les infrastructures de sécurité	340 000 $	340 000 $	340 000 $	1 020 000 $	845 530 $
	Total des bénéfices (valeurs ajustées en fonction des risques)	7 366 150 $	7 375 263 $	7 384 375 $	22 125 788 $	18 339 749 $

EFFICACITÉ DES OPÉRATIONS INFORMATIQUES ET DE SÉCURITÉ

Éléments probants et données. Selon les personnes interrogées, le passage à Prisma SASE leur a permis d'alléger la charge de travail des membres des équipes SecOps et NetOps. Cela est dû à l'infogérance de la solution, ainsi qu'à l'automatisation de différentes activités qui peuvent être mises en œuvre dans le processus.

- L'architecte principal dans le secteur de la santé a noté : « Plusieurs équipes étaient auparavant impliquées dans les SecOps. Il y avait une couche logicielle, une couche matérielle et une couche applicative. Ces trois couches ont été supprimées. Nous n'avons que des spécialistes des applications. Nous n'avons besoin que d'une ou de deux personnes contre cinq à dix auparavant ».
- Soulignant la facilité de la mise à l'échelle, cette même personne a déclaré à Forrester : « La mise à l'échelle est beaucoup plus facile. Les mêmes politiques s'appliquent. La mise à l'échelle se fait automatiquement. Sans PANW, nous devrions ajouter nous-mêmes des passerelles supplémentaires. Il nous faudrait augmenter le nombre de systèmes de back-end qui gèrent les bases de données et toutes les tâches de back-end qui en découlent ».
- Le directeur dans l'industrie manufacturière a précisé : « En ce qui concerne les modifications des politiques, nous sommes passés de quatre jours ouvrables à moins d'une heure. Nous effectuons environ 120 modifications par jour (80 % du temps) ».

> **« Prisma SASE est essentiellement un service infogéré. Ce n'est pas quelque chose que nous devons surveiller tous les jours. Nous n'avons pas à nous préoccuper du système, des passerelles ou de la latence du réseau. Tout cela ne nous concerne plus. »**
>
> *Architecte principal, secteur de la santé*

- Ce directeur a également souligné la valeur ajoutée de l'utilisation du module ADEM pour son entreprise : « Mon équipe réseau utilise le module ADEM à chaque fois qu'elle reçoit un ticket du centre d'assistance ou du centre de services concernant la latence du réseau. Elle utilise le modèle ADEM pour comprendre où se situe le problème ».
- Le directeur principal dans le secteur de l'hôtellerie a déclaré : « Avec le SD-WAN, l'installation se fait en une seule opération. Cela ne prend que quelques minutes ou quelques heures et non plus des semaines avec la mobilisation de nombreuses personnes. Auparavant, cinq ou six personnes travaillaient sur des modifications de ce type pendant deux semaines. Nous effectuons maintenant deux à trois cycles de modifications par trimestre ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- L'entreprise compte une équipe SecOps de 20 employés et une équipe NetOps de 12 employés.
- Un employé SecOps consacre en moyenne 80 % de son temps de travail à gérer des outils et à effectuer des modifications de politique. Il consacre 10 % supplémentaires de son temps à gérer les incidents de sécurité.
- Les gains d'efficacité pour l'équipe SecOps grâce à l'utilisation de la solution Prisma SASE se traduisent par un gain de temps de 75 %.
- Un employé NetOps consacre en moyenne 25 % de son temps de travail à la mise à l'échelle et à la mise en place de nouveaux sites.
- Les gains d'efficacité de l'équipe NetOps grâce à l'utilisation de Prisma SASE se traduisent par un gain de temps de 80 % l'Année 1. Ce chiffre passe à 85 % l'Année 2, puis à 90 % l'Année 3.
- Le salaire annuel moyen toutes charges comprises d'un employé SecOps est de 121 500 dollars, tandis que celui d'un employé NetOps est de 135 000 dollars.
- Cela représente un taux de productivité récupérée de 50 %, en partant du principe que le temps économisé ne se traduira entièrement pas par un gain de productivité de l'employé.

Risques. Ce bénéfice pour une entreprise peut varier en fonction des facteurs suivants :

- La taille et les compétences de l'équipe de gestion de la sécurité de l'entreprise.
- Les moyens et les systèmes en place avant le déploiement de Prisma SASE.
- La complexité de l'environnement de sécurité.
- Le nombre d'incidents de sécurité qui nécessitaient une intervention manuelle avant la mise en œuvre de Prisma SASE.
- Les autres solutions et outils mis en œuvre pour soutenir le travail de l'équipe SecOps et des opérations informatiques.
- Le salaire moyen des équipes SecOps et NetOps.

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) totale ajustée en fonction des risques de 2,3 millions de dollars sur trois ans.

Efficacité des opérations informatiques et de sécurité

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
A1	Taille de l'équipe SecOps (ETP)	Entreprise de référence	20	20	20
A2	Pourcentage de temps consacré à la gestion des outils et aux modifications des politiques	Entreprise de référence	80 %	80 %	80 %
A3	Pourcentage de gains d'efficacité grâce à Prisma SASE	Entretiens	75 %	75 %	75 %
A4	Sous-total : Gain de temps total dans la gestion des outils et les modifications des politiques (ETP)	A1*A2*A3	12	12	12
A5	Pourcentage de temps consacré à la gestion des incidents de sécurité	Entreprise de référence	10 %	10 %	10 %
A6	Pourcentage de gains d'efficacité grâce à Prisma SASE	Entretiens	75 %	75 %	75 %
A7	Sous-total : Gain de temps total dans la gestion des incidents de sécurité (ETP)	A1*A5*A6	2	2	2
A8	Salaire annuel moyen toutes charges comprises d'un employé SecOps	Norme TEI	121 500 $	121 500 $	121 500 $
A9	Sous-total : Valeur totale des gains d'efficacité de l'équipe SecOps	(A4+A7)*A8	1 701 000 $	1 701 000 $	1 701 000 $
A10	Taille de l'équipe NetOps (ETP)	Entreprise de référence	12	12	12
A11	Pourcentage de temps consacré à la mise à l'échelle et à la mise en place de nouveaux sites	Entreprise de référence	25 %	25 %	25 %
A12	Pourcentage de gains d'efficacité grâce à Prisma SASE	Entretiens	80 %	85 %	90 %
A13	Salaire annuel moyen toutes charges comprises d'un employé NetOps	Norme TEI	135 000 $	135 000 $	135 000 $
A14	Sous-total : Valeur totale des gains d'efficacité de l'équipe NetOps	A10*A11*A12*A13	324 000 $	344 250 $	364 500 $
A15	Productivité récupérée	Norme TEI	50 %	50 %	50 %
At	Efficacité des opérations informatiques et de sécurité	(A9+A14)*A15	1 012 500 $	1 022 625 $	1 032 750 $
	Ajustement en fonction des risques	↓10 %			
Atr	Efficacité des opérations informatiques et de sécurité (valeurs ajustées en fonction des risques)		911 250 $	920 363 $	929 475 $
	Total sur trois ans : 2 761 088 $		**Valeur actuelle sur trois ans : 2 287 368 $**		

GAINS DE PRODUCTIVITÉ POUR LES UTILISATEURS FINAUX

Éléments probants et données. Selon les personnes interrogées, avant l'utilisation de Prisma SASE, leur ancien environnement de sécurité perturbait parfois le travail des utilisateurs finaux. Cela pouvait être dû à des procédures d'investigation trop perturbantes. Dans d'autres cas, les failles de sécurité qui existaient dans l'ancien environnement étaient la cible de cyberattaques susceptibles de perturber considérablement la productivité des employés, en particulier ceux qui travaillent à distance.

- Le vice-président principal du service informatique dans le secteur des services financiers a déclaré à Forrester : « Je travaille à 100 % à distance ou en mode hybride, et certains travaillent même entièrement depuis leur domicile. Il est donc essentiel aujourd'hui de disposer d'une infrastructure qui permet de travailler trois jours au bureau et deux jours à la maison. Le passage d'un environnement à l'autre doit être fluide pendant ces deux jours : si les collaborateurs travaillent sur leur ordinateur portable à leur domicile, ils utilisent en back-end une infrastructure différente de celle du bureau, où ils ont un pare-feu matériel ».
- L'architecte principal dans le secteur de la santé a ajouté : « Si [nos employés] subissent une attaque, ils ne sont pas en mesure de faire leur travail. Un week-end, nous avons eu une panne parce que [notre ancien fournisseur] avait effectué une mise à jour qui n'avait pas été entièrement testée. Cela nous a empêchés de nous connecter à notre réseau. Personne n'a rien pu faire pendant 8 heures ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Elle compte 50 000 employés.
- Trente-trois pour cent de tous les employés travaillent à distance ou en mode hybride.
- Cinquante pour cent des employés travaillent directement avec des produits basés sur le cloud, et ces employés sont considérés comme les plus concernés par les solutions de Palo Alto Networks.
- On suppose qu'un arrêt du système impacte la productivité de 20 % des employés qui travaillent directement avec des produits basés sur le cloud.
- Les solutions de Palo Alto Networks permettent de récupérer 8 % du temps et de la productivité perdus en raison de l'arrêt du système.
- Le salaire annuel moyen toutes charges comprises d'un utilisateur final est estimé à 87 750 dollars.
- L'entreprise de référence récupère 50 % des gains d'efficacité pour du travail productif.

Risques. Ce bénéfice pour une entreprise peut varier en fonction des facteurs suivants :

- La taille de l'entreprise et le pourcentage d'utilisateurs finaux dont la productivité peut être impactée par les temps d'arrêt des solutions de sécurité.
- La complexité de l'environnement informatique, qui peut avoir un impact sur le nombre et l'ampleur des temps d'arrêt dus aux investigations et à la réinstallation des appareils.
- La région géographique et le secteur dans lesquels l'entreprise exerce ses activités, qui peuvent avoir un impact sur le salaire moyen toutes charges comprises des utilisateurs finaux.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 15 % et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques de 12,2 millions de dollars sur trois ans.

Gains de productivité pour les utilisateurs finaux

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
B1	Nombre total d'employés	Entreprise de référence	50 000	50 000	50 000
B2	Pourcentage d'effectifs distants/hybrides	Entreprise de référence	33 %	33 %	33 %
B3	Pourcentage de travail effectué dans le cloud	Entreprise de référence	50 %	50 %	50 %
B4	Pourcentage d'utilisateurs finaux affectés par les temps d'arrêt du système	Entreprise de référence	20 %	20 %	20 %
B5	Pourcentage du temps récupéré grâce à une meilleure disponibilité/diminution des temps d'arrêt	Entretiens	8 %	8 %	8 %
B6	Salaire annuel moyen toutes charges comprises d'un utilisateur professionnel	Norme TEI	87 750 $	87 750 $	87 750 $
B7	Productivité récupérée	Norme TEI	50 %	50 %	50 %
Bt	Gains de productivité pour les utilisateurs finaux	B1*B2*B3*B4*B5*B6*B7	5 794 800 $	5 794 800 $	5 794 800 $
	Ajustement en fonction des risques	↓15 %			
Btr	Gains de productivité pour l'utilisateur final (valeurs ajustées en fonction des risques)		4 925 580 $	4 925 580 $	4 925 580 $
	Total sur trois ans : 14 776 740 $		**Valeur actuelle sur trois ans : 12 249 188 $**		

RÉDUCTION DU RISQUE DE VIOLATION DES DONNÉES

Éléments probants et données. La réduction de la complexité de l'environnement de sécurité se traduit également par une réduction du risque lié à la sécurité. Dans l'ancien environnement des entreprises, les différentes solutions ponctuelles ne s'intégraient pas bien ou ne communiquaient pas entre elles, ce qui créait des failles de sécurité potentielles qui pouvaient conduire à un risque accru de violation des données. L'utilisation de Prisma SASE a considérablement réduit ce risque. Cela était encore plus évident au sein des entreprises ayant des effectifs distants et/ou hybrides.

- L'architecte principal dans le secteur de la santé a déclaré à Forrester : « Nous sommes capables d'offrir des services de manière sécurisée en ayant ce que nous considérons comme une visibilité totale sur les activités des utilisateurs ».
- Le directeur dans l'industrie manufacturière a noté : « Le fait d'avoir un périmètre de sécurité qui suit l'utilisateur plutôt qu'il ne soit limité à un site particulier réduit le risque ».

« Sans PANW, nous serions exposés à différents types d'attaques. Lorsqu'ils sont sur site, les utilisateurs se trouvent derrière un pare-feu. Aujourd'hui, avec des personnes à distance ou à l'étranger, vous perdez cela. Des outils tels que Prisma SASE vous permettent de continuer à avoir le même niveau de visibilité, de contrôle et de protection ».

Architecte principal, secteur de la santé

- Le vice-président principal du service informatique dans le secteur des services financiers a remarqué : « L'une des valeurs est la posture de sécurité et la capacité d'identifier le trafic sortant, la possibilité de surveiller facilement le trafic Internet et de voir ce qui se passe sur le réseau ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Selon les données de Forrester, l'entreprise de référence peut s'attendre à subir en moyenne 3,2 atteintes à la sécurité par an lorsqu'elle s'en remet à des solutions individuelles[2].
- Forrester modélise le coût d'une atteinte à la sécurité en fonction du nombre d'employés dans les entreprises. Pour l'entreprise de référence, ce coût s'élève à 53 $ par employé, sans compter la perte de productivité[3]. Ce coût inclut les éléments suivants :
  - Amendes infligées par les organismes de réglementation.
  - Remboursement des clients/poursuites judiciaires.
  - Réponse aux incidents et actions correctives.
  - Manque à gagner.
  - Coût de la restauration de l'image de marque.
  - Coût de réacquisition de clients.
- Avec Prisma SASE, les entreprises peuvent s'attendre à réduire de 50 % la probabilité d'une violation de données au bout de trois ans.
- L'attribution à Prisma SASE est égale au pourcentage d'effectifs distants de l'entreprise, soit 33 %.

Risques. Ce bénéfice pour une entreprise peut varier en fonction des facteurs suivants :

- L'impact de Palo Alto Networks sur la posture de sécurité globale de l'entreprise par rapport à l'ancienne solution.
- Le pourcentage d'employés touchés par une atteinte à la sécurité et la durée des temps d'arrêt associée.
- Le salaire moyen des utilisateurs de l'entreprise.

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

Réduction du risque de violation de données

Réf.	Indicateur	Source	Année 1	Année 2	Année 3
C1	Nombre moyen de violations de données par an	Études Forrester	3,2	3,2	3,2
C2	Nombre total d'employés	B1	50 000	50 000	50 000
C3	Coût potentiel moyen d'une violation de données par employé, sans compter les temps d'arrêt des utilisateurs internes	Études Forrester	53 $	53 $	53 $
C4	Réduction de la probabilité d'une violation	Entretiens	50 %	50 %	50 %
C5	Attribution à Prisma SASE	B2	33 %	33 %	33 %
Ct	Réduction du risque de violation de données	C1*C2*C3*C4*C5	1 399 200 $	1 399 200 $	1 399 200 $
	Ajustement en fonction des risques	↓15 %			
Ctr	Réduction du risque de violation de données (valeurs ajustées en fonction des risques)		1 189 320 $	1 189 320 $	1 189 320 $
	Total sur trois ans : 3 567 960 $		**Valeur actuelle sur trois ans : 2 957 663 $**		

RÉDUCTION DES COÛTS ET ÉCONOMIES RÉALISÉES DANS LES INFRASTRUCTURES RÉSEAU ET DE SÉCURITÉ

Éléments probants et données. Selon les personnes interrogées, leur investissement dans Prisma SASE leur a apporté différentes solutions et fonctionnalités qui leur ont permis de réduire ou d'éliminer une partie de leurs dépenses annuelles en matière de technologies réseau et de sécurité.

- L'architecte principal dans le secteur de la santé a décrit les différentes solutions de l'ancien environnement de son entreprise qu'il a pu éliminer grâce à l'investissement dans Prisma SASE, et a expliqué à Forrester : « Nous avions un produit spécifique pour l'accès à distance. Ensuite, nous avions ce que nous appelions notre sécurité H, ou la passerelle sécurisée. C'est la sécurité pour les utilisateurs distants. Enfin, nous avions un système distinct pour la prévention des pertes de données (DLP). Nous avions trois solutions distinctes nécessitant des compétences différentes et des équipes différentes. Aujourd'hui, tout est intégré ».
- Le directeur dans l'industrie manufacturière a ajouté : « J'ai pu me passer de mon fournisseur de proxy Web, entre autres. J'économise ainsi plusieurs millions de dollars chaque année ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Les dépenses annuelles de l'entreprise en matière de technologies de sécurité s'élèvent à 8 millions de dollars.
- La diminution du nombre de fournisseurs rendue possible par l'utilisation de Prisma SASE de Palo Alto Networks représente 5 % des dépenses annuelles en technologies de sécurité.

Risques. Ce bénéfice pour une entreprise peut varier en fonction des facteurs suivants :

- Le coût annuel associé à chaque technologie remplacée.
- La vitesse à laquelle l'entreprise peut remplacer ces technologies en raison des accords/termes de licence et des configurations de leur réseau.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce bénéfice par une baisse de 15 % et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques de 846 000 dollars sur trois ans.

> **« Avec Prisma SASE, vous disposez d'une plateforme polyvalente. Nous avons pu regrouper trois solutions différentes en une seule. En termes de coûts, cela représente une économie importante. »**
>
> *Architecte principal, secteur de la santé*

Réduction des coûts et économies réalisées dans les infrastructures réseau et de sécurité					
Réf.	**Indicateur**	**Source**	**Année 1**	**Année 2**	**Année 3**
D1	Dépenses annuelles en technologies de sécurité	Entreprise de référence	8 000 000 $	8 000 000 $	8 000 000 $
D2	Pourcentage d'économies réalisées grâce à la diminution du nombre de fournisseurs rendue possible par l'adoption de Prisma SASE et SD-WAN	Entretiens	5 %	5 %	5 %
Dt	Réduction des coûts et économies réalisées dans les infrastructures réseau et de sécurité	D1*D2	400 000 $	400 000 $	400 000 $
	Ajustement en fonction des risques	↓15 %			
Dtr	Réduction des coûts et économies réalisées dans les infrastructures réseau et de sécurité (valeurs ajustées en fonction des risques)		340 000 $	340 000 $	340 000 $
	Total sur trois ans : 1 020 000 $			**Valeur actuelle sur trois ans : 845 530 $**	

BÉNÉFICES NON QUANTIFIÉS

Les personnes interrogées ont mentionné d'autres avantages dont leurs entreprises ont bénéficié, mais qu'elles n'ont pas été en mesure de quantifier :

- **Meilleure visibilité sur l'environnement de sécurité.** Selon les personnes interrogées, l'un des avantages les plus précieux de Prisma SASE est leur meilleure visibilité actuelle sur l'état, la performance et l'utilisation des différentes parties du système de sécurité. L'architecte principal dans le secteur de la santé a déclaré : « Nous sommes en mesure de surveiller facilement le trafic et de voir ce qui se passe réellement sur le réseau ».

  Le vice-président principal du service informatique dans le secteur des services financiers a ajouté : « L'aspect intéressant de Palo Alto Networks était l'interface et la visibilité. Le reporting était la meilleure fonctionnalité pour nous en termes d'interface utilisateur. Il a immédiatement été plus performant que notre logiciel de reporting spécifique qui nous posait des problèmes de maintenance ».

- **Une meilleure expérience pour les employés, tant au niveau de l'utilisation des différentes solutions que de l'environnement de sécurité plus robuste et moins intrusif.** Selon les personnes interrogées, la combinaison de tous les avantages susmentionnés a permis d'améliorer l'expérience des employés au sein de l'entreprise. Le directeur de l'industrie manufacturière a noté : « Palo Alto Networks a été implémenté et a parfaitement fonctionné. Nous avons eu de très bons retours de la part des employés en termes de qualité de l'expérience ».

« PANW vous prépare pour la suite, qui consiste à intégrer d'autres éléments tels que les réseaux distants, les succursales et le CASB. »

Directeur de l'architecture et de l'ingénierie de la sécurité, industrie manufacturière

FLEXIBILITÉ

La valeur de la flexibilité est propre à chaque client. Il existe de nombreux scénarios dans lesquels un client déploie Prisma SASE, avant d'entrevoir d'autres utilisations et débouchés :

- **L'impact vertueux à long terme de posséder une solution de sécurité complète dans l'environnement.** À long terme, la mise en place d'un environnement de sécurité efficace et complet peut avoir un impact durable sur les performances d'une entreprise, sur sa marque et sur sa réponse aux menaces nouvelles et émergentes. Le directeur dans l'industrie manufacturière a expliqué : « Le fait d'avoir Palo Alto Networks vous prépare pour la suite, c'est-à-dire à intégrer davantage de choses, comme les réseaux distants, les succursales, les CASB, etc. La prochaine génération d'outils et de fonctionnalités que Palo Alto Networks va introduire nous permettra de simplifier encore plus la conception de la sécurité et les politiques de pare-feu ».

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

Le point de vue de Forrester : Les principales cybermenaces en 2023 comprendront des menaces existantes et émergentes

La défense contre les attaques visant l'apprentissage machine et l'intelligence artificielle était une discipline de niche... jusqu'à récemment. Des cas d'utilisation de l'IA par des adversaires sont également apparus, ce qui leur permet de s'adapter et de faire plus de ravages qu'ils ne le pouvaient avant l'émergence de ces technologies.

L'informatique en nuage pose des problèmes de sécurité en raison de l'empreinte du cloud et de la complexité des environnements dans le cloud. Les cybermenaces seront exacerbées par la multiplication des variantes des infrastructures de calcul et de stockage dans le cloud, ainsi que par l'impossibilité pour les fournisseurs d'IaaS de couvrir ces nouvelles variantes d'infrastructures de calcul et de stockage.

Source : « The Future Of Cybersecurity And Privacy », Forrester Research, Inc., 3 août 2023.

Analyse des coûts

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

Total des coûts							
Réf.	**Coût**	**Situation initiale**	**Année 1**	**Année 2**	**Année 3**	**Total**	**Valeur actuelle**
Etr	Investissement en temps des équipes internes pour l'installation et le déploiement	248 400 $	124 200 $	62 100 $	31 050 $	465 750 $	435 960 $
Ftr	Investissement en temps des équipes internes pour la formation des utilisateurs et la gestion en continu	950 $	24 948 $	24 948 $	24 948 $	75 794 $	62 992 $
Gtr	Coûts de Prisma SASE	162 068 $	3 291 750 $	3 291 750 $	3 291 750 $	10 037 318 $	8 348 163 $
	Total des coûts (valeurs ajustées en fonction des risques)	411 418 $	3 440 898 $	3 378 798 $	3 347 748 $	10 578 862 $	8 847 115 $

INVESTISSEMENT EN TEMPS DES ÉQUIPES INTERNES POUR L'INSTALLATION ET LE DÉPLOIEMENT

Éléments probants et données. Selon les personnes interrogées, le déploiement de Prisma SASE a été un processus complexe, qui a nécessité la collaboration de différentes équipes de leur entreprise (informatique, SecOps et NetOps) avec l'équipe de Palo Alto Networks.

- L'architecte principal dans le secteur de la santé a fait part de son processus de mise en œuvre à Forrester : « Après avoir évalué différents fournisseurs et choisi Palo Alto Networks, nous avons mis en place l'ensemble de la solution en un an. Plusieurs équipes y ont participé : sécurité informatique, conformité et réseau. Nous avons également impliqué l'équipe de support pour le déploiement de l'agent. Au total, entre 10 et 20 personnes ont consacré environ 50 % de leur temps [à la mise en œuvre] ».
- Le directeur dans l'industrie manufacturière a ajouté : « Nous avons fait appel à une personne de mon équipe réseau ainsi qu'à une personne de l'équipe informatique. Les deux premiers jours, ils y ont consacré 50 % de leur temps, car la majeure partie du travail était effectuée par le personnel de Palo Alto Networks. Dès que le tenant sur le cloud était prêt à être utilisé, mon équipe y a consacré 100 % de son temps ».
- Pour le déploiement du SD-WAN de Prisma, le directeur principal dans le secteur de l'hôtellerie a noté : « Nous avions un certain nombre de personnes qui se concentraient à plein temps sur le déploiement. Lorsqu'il est effectué de manière efficace, le déploiement peut être réalisé par 16 à 18 personnes qui travaillent activement sur le projet. La majorité d'entre elles sont des spécialistes réseau auxquels s'ajoutent quelques ingénieurs ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Pour l'ensemble du déploiement de Palo Alto Networks, 10 employés NetOps consacrent un total de neuf mois à la mise à niveau des pare-feu et à l'alignement des politiques au cours de la période initiale, et près de cinq mois à la mise au point l'Année 1. L'entreprise tire parti des cycles de fin de vie et prend le temps de tester le déploiement, ce qui allonge les délais, mais

assure aussi une transition en douceur depuis son ancienne solution.

- Les employés concernés consacrent initialement 80 % de leur temps au déploiement, pourcentage qui se réduit progressivement au cours des années suivantes.
- Le salaire annuel moyen toutes charges comprises d'un employé de l'équipe NetOps est de 135 000 dollars.
- Étant donné que les entreprises déploient généralement Prisma SASE en conjonction avec d'autres solutions de Palo Alto Networks, le modèle suppose que l'entreprise de référence consacre 20 % du temps total d'installation et de déploiement à Prisma SASE.

Risques. Le coût exact pour une entreprise varie en fonction des facteurs suivants :

- Les compétences des employés internes concernés.
- La complexité de l'ancien environnement.
- Le salaire annuel des employés concernés.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 15 % et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques de 436 000 dollars sur trois ans.

Investissement en temps des équipes internes pour l'installation et le déploiement

Réf.	Indicateur	Source	Situation initiale	Année 1	Année 2	Année 3
E1	Équipe réseau qui travaille sur l'installation de PAN	Entreprise de référence	10	10	10	10
E2	Temps passé par membre de l'équipe réseau	Entretiens	80 %	40 %	20 %	10 %
E3	Salaire annuel : employé de l'équipe NetOps	Norme TEI	135 000 $	135 000 $	135 000 $	135 000 $
E4	Pourcentage attribué à Prisma SASE	Entretiens	20 %	20 %	20 %	20 %
Et	Investissement en temps des équipes internes pour l'installation et le déploiement	E1*E2*E3*E4	216 000 $	108 000 $	54 000 $	27 000 $
	Ajustement en fonction des risques	↑15 %				
Etr	Investissement en temps des équipes internes pour l'installation et le déploiement (valeurs ajustées en fonction des risques)		248 400 $	124 200 $	62 100 $	31 050 $
	Total sur trois ans : 465 750 $			**Valeur actuelle sur trois ans : 435 960 $**		

INVESTISSEMENT EN TEMPS DES ÉQUIPES INTERNES POUR LA FORMATION DES UTILISATEURS ET LA GESTION EN CONTINU

Éléments probants et données. Une fois le système mis en place, les personnes interrogées ont fait état de différents degrés de gestion en continu de Prisma SASE. Pour certains, il s'agissait d'une plateforme facile à surveiller, tandis que d'autres ont consacré davantage de temps et d'investissements pour s'assurer de maximiser les avantages qu'offre la solution à leurs entreprises.

- L'architecte principal a noté : « Nous avons une ou deux personnes qui gèrent l'outil pour répondre aux demandes de modification de politique et surveiller les alertes. Il s'agit en grande partie d'un travail sur la couche d'application de la sécurité ».
- Le directeur dans l'industrie manufacturière a ajouté : « Pour la gestion en continu de Prisma SASE, j'estime qu'elle mobilise 10 % du temps de mon équipe. Il est vraiment facile à utiliser ».
- Pour Prisma SD-WAN, le directeur principal dans le secteur de l'hôtellerie a déclaré à Forrester : « Nous organisons des réunions périodiques avec l'équipe de Palo Alto Networks pour comprendre l'évolution de leur plateforme. Nous échangeons sur les enseignements à tirer et les défis à relever, le cas échéant. Nous avons une équipe qui s'occupe de la maintenance de la plateforme et une autre qui s'occupe de son optimisation ».

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Au total, 20 heures de formation sont requises pour les employés qui n'ont jamais utilisé Palo Alto Networks. Les années suivantes, 8 heures de formation sont nécessaires pour partager les nouvelles fonctionnalités, les mises à jour et les améliorations.
- Le salaire horaire moyen toutes charges comprises d'un employé du service informatique est de 54 dollars.
- Une fois la formation achevée, la gestion en continu est supposée impliquer les 10 employés formés chaque année. Ils consacrent 10 % de leur temps à la gestion de Prisma SASE.
- Étant donné que les entreprises gèrent NGFW et CDSS en même temps, le modèle suppose que 20 % du temps total consacré à la gestion en continu est dédié à Prisma SASE.

Risques. Le coût exact pour une entreprise varie en fonction des facteurs suivants :

- La taille du service informatique et sa maîtrise des solutions Palo Alto Networks.
- Le salaire moyen des employés du service informatique.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 10 % et a ainsi obtenu une valeur actuelle (VA) totale ajustée en fonction des risques de 63 000 dollars sur trois ans.

Investissement en temps des équipes internes pour la formation des utilisateurs et la gestion en continu						
Réf.	**Indicateur**	**Source**	**Situation initiale**	**Année 1**	**Année 2**	**Année 3**
F1	Nombre d'ETP qui reçoivent une formation pour la gestion en continu	Entreprise de référence	10	10	10	10
F2	Nombre d'heures par session de formation	Entretiens	8	2	2	2
F3	Salaire horaire moyen toutes charges comprises d'un employé du service informatique (y compris SecOps, NetOps et opérations informatiques)	Norme TEI	54 $	54 $	54 $	54 $
F4	Investissement en temps des équipes internes pour la formation des utilisateurs	F1*F2*F3	4 320 $	1 080 $	1 080 $	1 080 $
F5	Pourcentage de temps consacré à la gestion en continu	Entretiens		10 %	10 %	10 %
F6	Valeur de l'investissement en temps des équipes internes pour la gestion en continu	F1*F3*2 080*F5		112 320 $	112 320 $	112 320 $
F7	Attribution à Prisma SASE	Entretiens	0 $	20 %	20 %	20 %
Ft	Investissement en temps des équipes internes pour la formation des utilisateurs et la gestion en continu	(F4+F6)*F7	864 $	22 680 $	22 680 $	22 680 $
	Ajustement en fonction des risques	↑10 %				
Ftr	Investissement en temps des équipes internes pour la formation des utilisateurs et la gestion en continu (valeurs ajustées en fonction des risques)		950 $	24 948 $	24 948 $	24 948 $
	Total sur trois ans : 75 794 $			**Valeur actuelle sur trois ans : 62 992 $**		

COÛTS DE PRISMA SASE

Éléments probants et données. Les personnes interrogées ont acheté le matériel à l'avance et ont pu amortir les coûts d'abonnement sur la durée de trois ans du contrat, ce qui a permis de prévoir les coûts annuels.

Modélisation et hypothèses. Forrester émet les hypothèses suivantes en ce qui concerne l'entreprise de référence :

- Les coûts annuels comprennent à la fois le matériel qui doit être acheté et les frais d'abonnement à la solution.
- Les contrats d'abonnement sont amortis sur la période de trois ans de l'étude.
- Les prix peuvent varier. Veuillez contacter Palo Alto Networks pour plus d'informations.

Risques. Le coût exact pour une entreprise varie en fonction des facteurs suivants :

- Le nombre d'utilisateurs et de sites dans lesquels la solution sera mise en œuvre.
- Les modules supplémentaires spécifiques qui devraient être mis en œuvre pour améliorer encore les performances.

Résultats. Pour tenir compte de ces risques, Forrester a ajusté ce coût par une hausse de 5 % et a ainsi obtenu une valeur actuelle totale ajustée en fonction des risques de 8,3 millions de dollars sur trois ans.

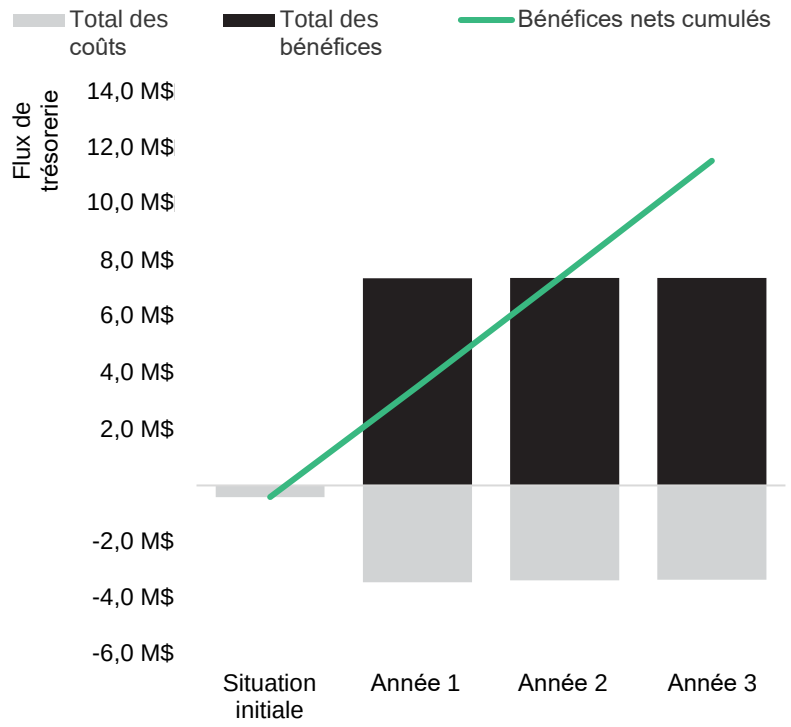
Coûts de Prisma SASE

Réf.	Indicateur	Source	Situation initiale	Année 1	Année 2	Année 3
G1	Coût annuel de Prisma SASE	Entreprise de référence	154 350 $	3 135 000 $	3 135 000 $	3 135 000 $
Gt	Coûts de Prisma SASE	G1	154 350 $	3 135 000 $	3 135 000 $	3 135 000 $
	Ajustement en fonction des risques	↑5 %				
Gtr	Coûts de Prisma SASE (valeurs ajustées en fonction des risques)		162 068 $	3 291 750 $	3 291 750 $	3 291 750 $
	Total sur trois ans : 10 037 318 $			**Valeur actuelle sur trois ans : 8 348 163 $**		

Récapitulatif des aspects financiers

INDICATEURS CONSOLIDÉS SUR TROIS ANS ET AJUSTÉS EN FONCTION DES RISQUES

Graphique des flux de trésorerie (valeurs ajustées en fonction des risques)



Les résultats financiers calculés dans les sections Bénéfices et Coûts peuvent être utilisés pour déterminer le ROI, la VAN et le délai de récupération pour l'entreprise de référence. Forrester se base sur un taux d'actualisation annuel de 10 % pour cette analyse.

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

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

	Situation initiale	Année 1	Année 2	Année 3	Total	Valeur actuelle
Total des coûts	(411 418 $)	(3 440 898 $)	(3 378 798 $)	(3 347 748 $)	(10 578 862 $)	(8 847 115 $)
Total des bénéfices	0 $	7 366 150 $	7 375 263 $	7 384 375 $	22 125 788 $	18 339 749 $
Bénéfices nets	(411 418 $)	3 925 252 $	3 996 465 $	4 036 627 $	11 546 926 $	9 492 634 $
ROI						107 %
Délai de récupération						< 6 mois

Annexe A : Total Economic Impact

La méthodologie Total Economic Impact (TEI) a été développée par Forrester Research pour améliorer les processus de décision des entreprises en matière de technologie et aider les fournisseurs à communiquer à leurs clients la valeur de leurs produits et services. La méthodologie TEI aide les entreprises à démontrer, justifier et concrétiser la valeur tangible des initiatives informatiques auprès de la direction et d'autres parties prenantes clés de l'entreprise.

L'APPROCHE TOTAL ECONOMIC IMPACT

Les bénéfices représentent la valeur apportée par le produit à l'entreprise. La méthodologie TEI pondère les bénéfices et les coûts de la même manière, ce qui permet d'examiner pleinement l'impact de la technologie sur l'ensemble de l'entreprise.

Les coûts tiennent compte de toutes les dépenses nécessaires pour obtenir la valeur ou les bénéfices attendus du produit. La catégorie coût du TEI correspond aux coûts incrémentaux par rapport à l'ancien environnement pour les coûts continus liés à la solution.

La flexibilité représente 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 de bénéfices et de coûts en considérant : 1) la probabilité que les estimations correspondent aux projections initiales et 2) la probabilité qu'un suivi des estimations soit fait sur la durée. Les facteurs de risque de la méthode 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 se voient appliquer le 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 sommes et les calculs de valeur actuelle des tableaux Total des bénéfices, Total des coûts et Flux de trésorerie ne coïncident pas totalement, certains nombres étant arrondis.

VALEUR ACTUELLE (VA)

Valeur actuelle ou courante des estimations (actualisées) des coûts et des bénéfices à un taux d'intérêt donné (taux d'actualisation). La VA des coûts et des bénéfices entre dans la VAN 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). Une VAN positive pour un projet indique normalement que l'investissement est justifié, à moins que d'autres projets 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 %.

DÉLAI DE RÉCUPÉRATION

Seuil de rentabilité d'un investissement. Il s'agit du moment où les bénéfices nets (bénéfices moins coûts) sont égaux à l'investissement ou au coût initial.

Annexe B : Documents complémentaires

Études Forrester connexes

« The Future Of Cybersecurity And Privacy », Forrester Research, Inc., 3 août 2023

« Top Cybersecurity Threats In 2023 », Forrester Research, Inc., 17 avril 2023

« Introducing The Zero Trust Edge Architecture For Security And Network Services », Forrester Research, Inc., 2 août 2023

Annexe C : Notes de fin

[1] La méthodologie Total Economic Impact développée par Forrester Research améliore les processus de décision d'une entreprise en matière de technologies et aide les éditeurs de logiciels à communiquer la valeur de leurs produits et services à leurs clients. La méthodologie TEI aide les entreprises à démontrer, justifier et concrétiser la valeur tangible des initiatives informatiques auprès de la direction et d'autres parties prenantes clés de l'entreprise.

[2] Source : Forrester Consulting Cost Of A Cybersecurity Breach Survey, premier trimestre 2021.

[3] Ibid.


FORRESTER®