FORRESTER®

Synthèse :

The Total Economic Impact™ Of Palo Alto Networks For Network Security And SD-WAN

Palo Alto Networks a demandé à Forrester Consulting de mener une étude TEI (Total Economic Impact™) objective et de calculer le retour sur investissement potentiel de l'offre combinée SD-WAN et sécurité des réseaux de Palo Alto Networks pour les entreprises. L'objectif de cette étude est d'évaluer les retombées financières potentielles des produits de Palo Alto Networks sur leur organisation. Ces produits incluent les pare-feu nouvelle génération (NGFW), Prisma SD-WAN, les services cloud de prévention des intrusions (IPS), la passerelle web sécurisée (SWG) et le filtrage d'URL, l'analyse des malwares ou « sandboxing », la sécurité DNS et la sécurité de l'Internet des objets (IoT).

Les solutions SD-WAN et de sécurité réseau de Palo Alto Networks couvrent les principaux contrôles de sécurité. Elles aident les entreprises à centraliser la gestion, à maintenir une connectivité optimale et à étendre les politiques et contrôles de sécurité à tous les utilisateurs, applications et appareils.

Pour mieux comprendre les avantages, les coûts et les risques associés à cet investissement, Forrester a interrogé 142 clients des solutions Palo Alto Networks, dont 9 lors d'entretiens approfondis. Dans le cadre de cette étude, Forrester a rassemblé les retours d'expérience des clients ayant pris part à l'enquête (sondés) et aux entretiens approfondis (interviewés), puis les a combinés en une seule organisation composite.

Avant de déployer les solutions de sécurité réseau de Palo Alto Networks, les clients utilisaient des pare-feu traditionnels associés à de multiples solutions spécialisées pour sécuriser leurs environnements. conséquence directe de leurs efforts de transformation numérique. Les entreprises ne disposaient pas de technologies de sécurité suffisamment modernes. De même, les équipes informatiques et de sécurité manquaient d'efficacité pour s'adapter à l'évolution des besoins de l'entreprise. Les initiatives de transformation numérique ont donné l'impulsion à une grande migration de données, applications et processus vers le cloud, tandis que d'autres fonctions de cœur de métier restaient sur site.

Retour sur investissement (ROI)
247 %

Valeur actuelle nette (VAN)
28,5 millions $

Délai d'amortissement
6 mois

Au terme de leur investissement dans la solution de sécurité réseau de Palo Alto Networks, les clients disposaient d'une plateforme commune alimentant un outil centralisé : Panorama, la solution de gestion de la sécurité de Palo Alto Networks. Cela a permis de réduire considérablement les efforts d'investigation et de libérer des ressources précieuses pour se concentrer sur les améliorations et sécuriser une plus grande partie du réseau. Pour leur part, les entreprises interviewées ont déployé tout ou partie des solutions SD-WAN et de sécurité réseau de Palo Alto Networks.

Les principaux résultats de l'investissement sont les suivants : gains d'efficacité pour les équipes ITOPs, SecOps et NetOps, ainsi que pour les utilisateurs métiers et salariés en magasin ; réduction significative des risques de compromission de données ; réduction des coûts associés à la gestion des licences et à la gestion de l'infrastructure de solutions spécialisées ; couverture de sécurité accrue ; et améliorations des fonctionnalités IoT Security, Zero Trust et SD-WAN.

Résultats clés

Les avantages quantifiés en valeur actualisée ajustée au risque incluent :

Réduction des risques de compromission de données

- **Réduction de 45 % des probabilités de compromission de données après trois ans.** Grâce à Palo Alto Networks, les entreprises ont pu réduire les risques de compromission de données, gagner en visibilité, mettre en place un modèle de sécurité Zero Trust et appliquer des politiques de sécurité cohérentes à l'échelle de toute l'entreprise. Des services de sécurité en mode cloud sont intervenus en appui de l'équipe SecOps, avec un support 24h/7j et une prévention des vulnérabilités et de toutes les menaces connues et inconnues.

Sécurité et rendement opérationnel des équipes informatiques

- **Les équipes SOC ont pu réduire de 35 % le nombre d'investigations avancées, améliorer le MTTR de 20 % et réduire de moitié le nombre d'appareils à réimager.** Tout cela a permis d'économiser 5,1 millions $ sur trois ans. Le déploiement des solutions de sécurité de Palo Alto Networks a considérablement amélioré la visibilité sur les réseaux des entreprises et introduit des fonctionnalités d'automatisation qui ont fait baisser le nombre d'alertes critiques, y compris de faux positifs, au fil du temps. En outre, les entreprises ont pu réduire la durée moyenne de réparation (MTTR), car les analystes ont désormais à portée de main les données dont ils ont besoin. Par conséquent, le nombre de terminaux touchés par des malwares ou d'autres problèmes a diminué, ce qui a réduit la charge de travail de l'équipe informatique.

Réduction des efforts de gestion de la stack de sécurité

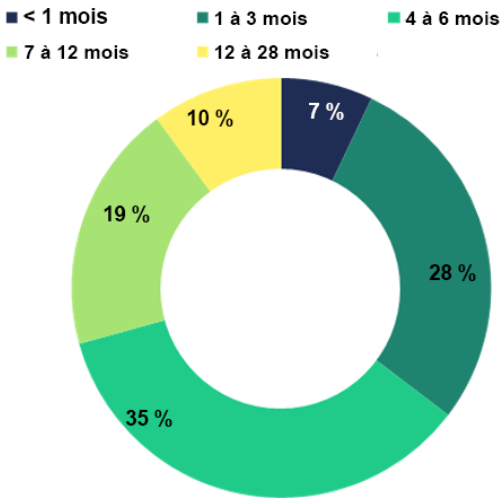
50 %

Amélioration de la productivité des utilisateurs

- **Amélioration de la productivité des utilisateurs grâce à la baisse du nombre d'incidents et donc des investigations, pour une économie totale de 865 226 $ sur trois ans.** Grâce aux solutions de sécurité de Palo Alto Networks, les utilisateurs passent moins de temps à interagir avec les équipes IT et sécurité, ce qui leur permet de se recentrer sur leurs missions et de générer de la valeur pour leur entreprise.

« Combien de temps, selon vous, a-t-il fallu à votre entreprise pour parvenir à un niveau de sécurité stable avec un NGFW par rapport à des solutions spécialisées ? »

(Affichage des 5 meilleurs résultats uniquement)



Base : 83 utilisateurs de produits Palo Alto Networks ayant considéré « la réduction du risque de cyberattaques sur l'entreprise » comme un avantage
Source : Etude réalisée par Forrester Consulting sur demande de Palo Alto, octobre 2020

Choisissez Palo Alto Networks et adoptez une stratégie de sécurité stable en 6 mois

70 % des clients

CONSULTEZ L'INTEGRALITE DE L'ETUDE ICI

Réduction et évitement des coûts d'infrastructure de sécurité

- **Rationalisation et dépenses évitées dans l'infrastructure de sécurité = économies de 9,9 millions $ sur trois ans.** Au terme du déploiement des solutions de Palo Alto Networks, les entreprises ont pu décommissionner leurs systèmes et produits de sécurité existants. Avant d'investir, certaines entreprises comptaient jusqu'à 17 fournisseurs dans leur stack de sécurité. La simplification de l'environnement et la réduction du nombre de fournisseurs étaient donc une priorité pour elles. Avec la solution Palo Alto Networks, ils bénéficient d'une couverture supérieure à moindre frais. Parmi les technologies supplantées par les services de sécurité dans le cloud de Palo Alto Networks, on peut citer la prévention des intrusions (IPS/IDS), la passerelle web sécurisée (SWG), le proxy web, l'analyse des malwares sur VPN (ou Sandboxing), les DNS et la sécurité des applications SaaS (Software-as-a-Service).

Efficacité de la gestion de la stack de sécurité à partir d'une plateforme commune

- **Réaffectation de 50 % environ des professionnels de la sécurité à temps plein à des initiatives porteuses d'une plus forte valeur grâce à une gestion plus efficace depuis une plateforme commune, pour une économie de 1,9 million $ sur trois ans.** Grâce à la réduction du nombre de fournisseurs et à la consolidation sur une plateforme commune, il faut aujourd'hui moins de personnes pour réaliser une même tâche. Les entreprises peuvent ainsi réduire de moitié leurs équipes de gestion. En outre, la plateforme commune a permis aux entreprises de déployer rapidement des mises à jour, des correctifs et des politiques de sécurité sur l'ensemble de la plateforme à partir d'une console centrale, plutôt que de mettre à jour chaque équipement de sécurité manuellement et via les outils de plusieurs fournisseurs.

Temps d'atteinte d'une sécurité adéquate

30 % plus rapide

Réduction des coûts et des risques de sécurité de l'IoT

- **Economie de 1,4 million $ sur l'IoT grâce à la réduction des efforts de gestion et du nombre de nouveaux appareils IoT achetés.** Grâce à IoT Security, les entreprises ont pu identifier et sécuriser tous leurs appareils IoT à partir d'une plateforme centrale, déterminer rapidement l'état et le lieu de chaque appareil et connaître leur emplacement, et optimiser la valeur et l'utilisation de chaque appareil grâce à des fonctionnalités de reporting améliorées. Cela a permis de réduire de 10 % les nouveaux achats.

Diminution de la probabilité d'une compromission de données après 3 ans

45 %

Accélération de l'atteinte d'une protection adéquate

- **Réduction de 30 % du temps nécessaire à l'adoption d'une stratégie de sécurité adéquate, soit une économie de 812 860 $ sur trois ans.** Grâce aux pare-feu nouvelle génération (NGFW) et aux services de sécurité en mode cloud de Palo Alto Networks, les entreprises ont pu accélérer la mise en place de leurs solutions de sécurité et devenir plus rapidement opérationnelles. En comparaison avec les solutions spécialisées d'avant, les équipes de sécurité ont pu prendre une longueur d'avance pour optimiser la solution et appliquer le Zero Trust.

Réduction des coûts de matériel et de connectivité WAN

- **Réduction de plus de 90 % des coûts de matériel et de connectivité WAN sur les sites distants, soit 6,04 millions $ d'économies sur trois ans.** En abandonnant le Multipropotocol Label Switching (MPLS) au profit de Prisma SD-WAN de Palo Alto Networks, les entreprises ont considérablement réduit les coûts d'exploitation mensuels de leurs sites tout en améliorant la visibilité et le contrôle du trafic réseau.

Gestion efficace du SD-WAN

- **Réduction de moitié des efforts de gestion qui pesaient sur les équipes informatiques et amélioration de 12 % de l'efficacité des salariés des sites distants et magasins grâce à Prisma SD-WAN, soit une économie de 4,9 millions $ sur trois ans.** Avec son interface utilisateur intuitive et sa conception matérielle spécialement adaptée, Prisma SD-WAN a permis aux équipes informatiques de centraliser la gestion du SD-WAN. En outre, grâce à l'amélioration des contrôles de la bande passante, des performances réseau et des contrôles de sécurité, les entreprises ont pu déployer de meilleures technologies pour leurs salariés en télétravail, améliorant ainsi la productivité et l'expérience client.

ORGANISATION COMPOSITE

A partir des entretiens et de l'enquête, Forrester a établi un cadre TEI, sous la forme d'une organisation composite, puis effectué une analyse du retour sur investissement illustrant les domaines concernés sur le plan financier. Cette organisation composite est représentative des neuf sociétés que Forrester a interviewées et des 133 autres qui ont participé à l'enquête. Elle sert de base à l'analyse financière globale dans la section suivante. L'organisation composite possède les caractéristiques suivantes :

- **Description de l'organisation composite.** L'organisation composite est une entreprise distribuée comptant 50 000 salariés et réalisant 7 milliards $ de chiffre d'affaires par an. Elle possède 400 sites, dont son siège social, un datacenter, un cloud, des sites distants, des magasins et des usines. L'équipe de sécurité de l'organisation composite répond à 1 200 incidents par semaine, soit 62 400 au cours de la première année, chaque incident nécessitant en moyenne 2 heures pour être résolu.

VECTEURS D'INVESTISSEMENT

Les entreprises interviewées et sondées avaient en commun un certain nombre de difficultés, notamment :

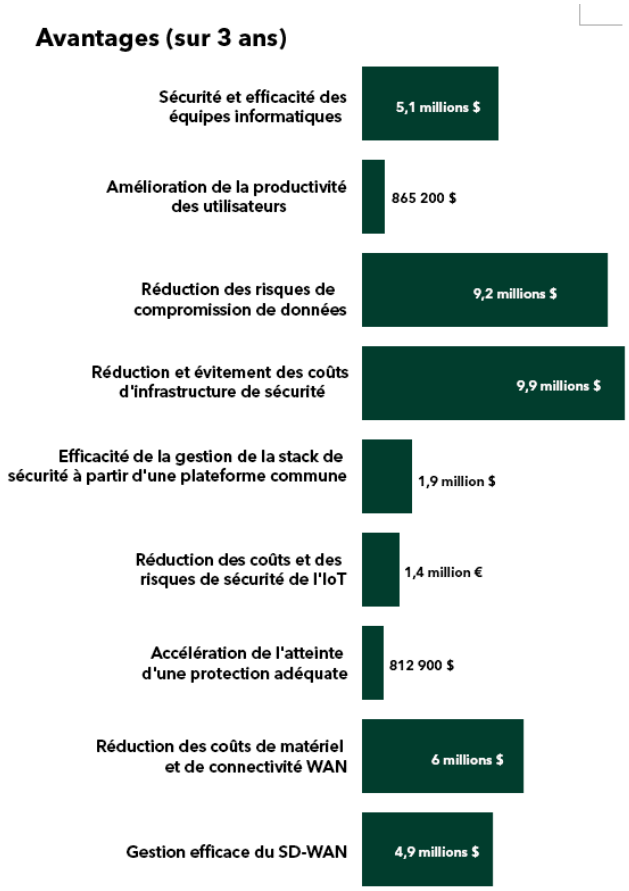
- **Solutions spécialisées de cybersécurité anciennes et peu performantes.** Les entreprises interrogées ont déclaré que leurs anciennes solutions étaient ponctuelles et ne répondaient pas aux attentes de vitesse, de performances, ni de support client du fournisseur, en plus de ne pas s'aligner sur les stratégies Zero Trust. Les produits précédemment déployés étaient lents à mettre à niveau et demandaient des investissements importants en capital pour maintenir le matériel nécessaire à jour, ainsi que des investissements opérationnels considérables pour assurer le bon fonctionnement des solutions.
- **Fonctionnalités et plateformes de sécurité décentralisées et segmentées.** Plusieurs entreprises interviewées ont déclaré qu'avant que leur organisation ne déploie diverses variantes de NGFW et de services de sécurité en mode cloud de Palo Alto Networks pour protéger leurs infrastructures sur site et dans le cloud, elles utilisaient des solutions de sécurité disparates qui nécessitaient des compétences variées pour effectuer des tâches simples. Les équipes de sécurité n'avaient pas de visibilité transverse sur ces technologies disparates. Elles ne pouvaient pas communiquer la Threat Intelligence suffisamment rapidement, ne disposaient pas d'une suite cohérente pour surveiller leurs réseaux et ne pouvaient pas quantifier les risques du fait des écarts et lacunes entre infrastructures.
- **Protection contre des attaques de plus en plus sophistiquées et volonté de visibilité et de contrôle sur les applications en couche 7.** A l'heure où les menaces de cybersécurité deviennent plus sophistiquées, les entreprises interviewées ont déclaré que leur organisation cherchait à moderniser ses infrastructures de sécurité vieillissantes et à se séparer de ses solutions spécialisées sur site. Elles recherchaient une visibilité plus granulaire sur leurs réseaux en couche 7 et exigeaient plus d'analyses au niveau des applications. Leurs anciennes solutions ne pouvaient pas apporter ce niveau de visibilité, ni le déchiffrement ou les performances nécessaires.

POURQUOI PALO ALTO NETWORKS ?

Les entreprises interrogées recherchaient une solution pouvant :

- **Unifier la sécurité, les politiques et la gestion de l'ensemble du réseau et du cloud sur une même plateforme centralisée.** Un responsable d'architecture IT chez un fabricant informatique déclare : « Je dispose désormais d'une politique de sécurité plus cohérente sur l'ensemble de mon infrastructure, et ce dans le monde entier. Je n'ai plus à gérer de multiples fournisseurs avec chacun ses propres politiques et mises à jour. J'assure une sécurité cohérente dans tous les environnements. Cela vient certes de la console de gestion centralisée, mais je sais aussi que je n'ai qu'à définir une seule politique de sécurité et à l'appliquer où je veux. »

- **Gestion centralisée et visibilité améliorée durant la transition vers le cloud.** Pour un RSSI dans le secteur du retail, les avantages d'une solution intégrée et connectée sont indéniables : « L'avantage de cette technologie est qu'elle s'intègre parfaitement à Panorama. Dans Panorama, nous pouvons tout contrôler depuis une seule console. Au lieu de gérer individuellement 600 pare-feu, je peux surveiller le flux des menaces depuis une seule et même console. Les résultat parlent d'eux-mêmes. »
- **Intégration transparente avec les plateformes existantes pour permettre l'automatisation.** Les services de sécurité en mode cloud s'appuient sur la force du collectif pour automatiser l'analyse d'une menace rencontrée par un client et prémunir tous les autres clients du service contre les menaces similaires en quelques secondes ou moins. Un responsable d'architecture IT chez un fabricant informatique témoigne : « Nous recherchions des solutions d'automatisation prêtes à l'emploi. Nous ne voulions pas avoir à acheter tous les produits et ensuite dépenser encore un million de dollars en automatisation. Nous recherchions une bonne intégration avec nos plateformes existantes, avec une marge suffisante pour évoluer vers des domaines dans lesquels nous n'avions pas encore forcément investi. »



RESSOURCES SUPPLEMENTAIRES

Forrester a développé des ressources supplémentaires pour étudier plus en détail l'impact et les avantages des solutions incluses dans cette étude. Vous trouverez plus d'informations ainsi qu'un accès à ces ressources supplémentaires ici :

- The Total Economic Impact™ of Palo Alto Networks for Network Security and SD-WAN
- TEI Spotlight : Prisma SD-WAN
- TEI Spotlight : Cloud-Delivered Security Services
- TEI Spotlight : Prisma Access


FORRESTER®