

TEI Spotlight :

Offrez un accès distant sécurisé et gagnez en sérénité grâce à Prisma Access de Palo Alto Networks

Dans le cadre d'une étude Total Economic Impact™ (TEI), Forrester a récemment interrogé plusieurs clients de Palo Alto Networks au sujet de leur investissement dans Prisma Access.¹ Au travers de ces entretiens, Forrester a mis en lumière les nombreux avantages dont bénéficient les clients qui ont adopté Prisma Access, solution cloud de sécurité réseau intégrée à la plateforme SASE (Secure Access Services Edge) de Palo Alto Networks. Prisma Access sert principalement à connecter et sécuriser l'accès des utilisateurs distants, des filiales/sites et d'autres réseaux distants.

A l'heure où de plus en plus d'applications, de serveurs et de services sont fournis dans le cloud et alors que le télétravail devient la norme aux quatre coins du globe, les entreprises réévaluent l'évolutivité des solutions spécialisées d'ancienne génération et leur capacité à fournir un accès sécurisé et fiable aux utilisateurs et sites. Les salariés utilisent généralement un VPN ou des services similaires pour accéder à distance aux données critiques ou effectuer des tâches essentielles dans les temps. L'expérience d'accès sécurisé des utilisateurs peut donc avoir un impact réel sur les résultats d'une entreprise. De plus, face à la complexité et à la sophistication croissantes des cyberattaques, il est essentiel pour les entreprises de centraliser et d'exploiter les données de journaux de tous leurs services afin de combler les écarts de sécurité et de détecter et neutraliser les menaces pour la sécurité du réseau.

Palo Alto Networks propose une plateforme intégrée pour répondre aux besoins réseau et sécurité des entreprises, notamment Prisma Access. Cette solution fournit des services de sécurité réseau homogènes et un accès à tous les types d'applications cloud pour les utilisateurs et sites distants. Avec Prisma Access, les entreprises n'ont plus besoin de recourir à des solutions multipoints et sur site, ce



Retour sur investissement (ROI)
247 %



Valeur actuelle nette (VAN)
28,5 millions \$

qui réduit à la fois les coûts et la complexité tout en améliorant la sécurité globale.

Pour mieux comprendre les avantages, les coûts et les risques associés à Prisma Access, Palo Alto Networks a demandé à Forrester Consulting d'interroger 133 clients, de conduire des entretiens avec 10 d'entre eux et de mener une étude TEI (Total Economic Impact™). Pour ce coup de projecteur sur Prisma Access, Forrester a exploité les données de neuf entreprises interviewées, toutes utilisant Prisma Access pour sécuriser les accès distants aux applications et services critiques de leur structure répartie dans le monde entier.

Ce résumé se concentre sur l'utilisation de Prisma Access par les entreprises interviewées et sur sa valeur pour leur organisation.



Réduction des risques de compromission de données
45 %

VECTEURS D'INVESTISSEMENT

Pour ces entreprises, la décision d'investir dans Prisma Access de Palo Alto Networks s'est fondée sur ces différents facteurs :

- **Connexion sécurisée et fiable, pour tous et partout dans le monde.** Les anciennes solutions de type VPN ou services de proxy web n'offraient pas la visibilité dont les entreprises avaient besoin pour sécuriser leurs réseaux en toute confiance, sans parler de leur manque de fiabilité notoire – les utilisateurs se plaignant de fréquentes déconnexions et de problèmes d'accès. Un vice-président senior du secteur des services financiers témoigne : « Nos utilisateurs se plaignaient souvent de la lenteur de notre ancienne solution d'accès à distance, surtout à l'étranger. En outre, nous n'avons plus à nous soucier de la disponibilité opérationnelle puisqu'elle est garantie par Palo Alto Networks dans le cadre de ses engagements SLA. »

« C'est l'un des avantages de Prisma Access, nous n'y touchons pas du tout. Nous n'avons pas à passer notre temps à installer des correctifs et à assurer le suivi des portails et des passerelles. »

*Directeur des services réseau et monitoring,
secteur de l'enseignement*

- **Evolutivité pour répondre à la demande croissante d'accès à distance avant et après la pandémie.** Même avant que la pandémie de COVID-19 ne contraigne la plupart d'entre elles à basculer en télétravail, les entreprises peinaient déjà à faire évoluer leurs solutions existantes pour répondre à la demande croissante d'accès à distance. Sachant que les entreprises interviewées avaient pris la décision de déployer Prisma Access avant la crise sanitaire, elles ont noté une amélioration de l'évolutivité, un élément crucial pour assurer le bon fonctionnement de l'entreprise dans un contexte de généralisation du télétravail. Un vice-président senior du secteur des services financiers explique : « Prisma Access

a permis à nos utilisateurs d'accéder en toute sécurité aux applications et aux données dont ils avaient besoin, peu importe le lieu de connexion. Cette souplesse s'est avérée cruciale tout au long de la pandémie puisque notre entreprise a est passée au télétravail à 100 %. Il aurait été totalement impossible à notre précédente solution d'accès à distance de s'adapter au basculement en télétravail avec une telle efficacité. »

En outre, les entreprises tenaient à ce que tous les utilisateurs se connectent via Prisma Access pour se protéger des menaces, en particulier lorsqu'ils accèdent aux applications ou aux données depuis des emplacements à risque. Un directeur des services réseau et monitoring dans le secteur de l'enseignement déclare : « Nous avons principalement deux cas d'usage pour lesquels Prisma Access remplace désormais notre ancien VPN. Le premier consiste à fournir aux utilisateurs à distance un accès sécurisé aux applications sur le réseau du campus. Le second vise à fournir une connexion à Internet sécurisée à nos utilisateurs lorsqu'ils se trouvent sur un réseau non sécurisé. Les utilisateurs se connectent souvent depuis des points d'accès publics, des hôtels, des cafés, etc. Nous les encourageons donc tous à exploiter ces services pour protéger leurs propres appareils. »

- **Améliorer les performances tout en réduisant la maintenance et l'assistance.** Avec leurs anciennes solutions, les entreprises étaient principalement confrontées à des problèmes de fiabilité et de performances. Les utilisateurs se plaignaient de fréquentes déconnexions et de la lenteur du service, ce qui provoquait une saturation du helpdesk, réduisait la productivité et affectait l'expérience utilisateur. En plus des problèmes liés aux utilisateurs, les solutions d'ancienne génération devaient faire l'objet d'un suivi, de mises à jour et de correctifs fréquents afin de garantir la sécurité et le bon fonctionnement du réseau. Un directeur des services réseau et monitoring dans le secteur de l'enseignement se souvient : « Nous avons des problèmes [avec notre ancienne solution VPN] qui nous obligeaient à redémarrer



CONSULTEZ L'INTEGRALITE DE L'ETUDE ICI

le serveur VPN et à en assurer le suivi. Pendant trois ans, mon équipe est littéralement restée au chevet du serveur. C'est l'un des avantages de Prisma Access : nous n'y touchons pas du tout. Nous n'avons pas à passer notre temps à le corriger et à en assurer le suivi. »

POURQUOI PRISMA ACCESS DE PALO ALTO NETWORKS ?

Les entreprises ont fait part des principales raisons qui les ont convaincues d'investir dans Prisma Access :

- **Solution évolutive et basée sur le cloud.** Un directeur des services réseau et monitoring dans le secteur de l'enseignement se souvient : « Avec notre ancienne solution, de nombreux utilisateurs, en particulier ceux basés à l'étranger, se plaignaient de la lenteur car nous fournissons un tunnel VPN complet. Avec Prisma Access, nous pouvons conserver le tunnel complet, mais les passerelles peuvent en fait gérer le trafic qui allait auparavant vers Internet. Ce fut l'un des facteurs décisifs dans notre choix. Lorsque nous avons procédé au PoC, nous avons demandé à des utilisateurs et enseignants du monde entier de tester la solution et les retours d'expérience ont été excellents. »
- **Performances, fiabilité et sécurité améliorées.** Un vice-président senior du secteur des services financiers affirme : « L'investissement en sécurité se justifie souvent par la réduction des risques, et Prisma Access réduit sans aucun doute les risques pour nous. Mais c'est également l'un des rares produits de sécurité qui permettent à votre entreprise d'être plus productive et d'améliorer l'efficacité des utilisateurs. »
- **Renforcement de la sécurité de l'entreprise par l'intégration dans l'écosystème Palo Alto Networks.** Un directeur des services réseau et monitoring dans le secteur de l'enseignement déclare : « Nous apprécions l'intégration de Prisma Access avec tous nos mécanismes de journalisation internes, tels que notre système de gestion des événements et des informations de sécurité (SIEM) et notre helpdesk. Notre ancienne solution était très limitée en termes de journaux et d'intégrations, mais

avec Palo Alto Networks et Prisma Access, nous bénéficions d'une meilleure visibilité et pouvons connaître l'origine du trafic sur nos réseaux. »

RESULTATS CLES

Prisma Access a influé sur certains des principaux avantages quantifiés par l'étude TEI portant plus globalement sur l'ensemble du portefeuille de sécurité réseau de Palo Alto Networks. Principaux avantages et impact de Prisma Access sur l'ensemble global de solutions :

9,2 millions \$ d'économies grâce à une réduction de 45 % des risques de compromission de données.

Bien qu'il ne soit pas le seul facteur contribuant, Prisma Access a joué un rôle déterminant dans la réduction de la probabilité et de l'impact d'une compromission de sécurité pour les entreprises.

- **Réduction des risques de compromission de données.** Avec Prisma Access, tous les utilisateurs passent par une passerelle sécurisée pour accéder aux réseaux et applications essentiels, ce qui protège à la fois le réseau et l'appareil de l'utilisateur contre les malwares et les attaques Internet lorsqu'ils sont connectés.
- **Réduction de l'impact d'une compromission de sécurité.** Tous les journaux de sécurité sont facilement intégrés aux solutions SIEM de sécurité existantes et aux autres solutions de sécurité de Palo Alto Networks. Cela améliore la visibilité et les capacités de détection, tout en permettant aux équipes de sécurité d'identifier et de neutraliser les menaces plus rapidement.

Rationalisation et dépenses évitées dans l'infrastructure de sécurité = économies de 9,9 millions \$. Prisma Access a pu aider les entreprises à rationaliser leur infrastructure de sécurité existante en supprimant les technologies redondantes telles que les services VPN et l'infrastructure sur site.

- **Réduction des coûts, de la complexité et amélioration des performances de sécurité.** Avec Prisma Access, les entreprises ont pu supprimer une solution spécialisée devenue redondante, réduire la complexité de leur environnement, réduire le nombre de fournisseurs et résorber les failles de sécurité potentielles.

Les gains d'efficacité dans la gestion de la stack de sécurité réduit la charge de travail de près de 50 %, pour une économie de 1,9 million \$. En adoptant

Prisma Access, les entreprises ne sont plus responsables de la maintenance des anciennes solutions, ce qui réduit les coûts de main d'œuvre et permet de réaffecter des ressources précieuses à des tâches plus importantes.

- **La réduction de la maintenance et l'amélioration des performances satisfont les utilisateurs.** Les entreprises déclarent qu'avec Prisma Access, elles ne passent plus leur temps à appliquer des correctifs et contrôler des portails et passerelles. Les utilisateurs signalent une amélioration des performances en termes de connectivité et de vitesse, et ont moins de problèmes lors de l'installation et de l'exécution de Prisma Access.

Réduction de 30 % du temps d'atteinte d'une sécurité adéquate. Avec Prisma Access, les entreprises peuvent appliquer des politiques et des contrôles de sécurité cohérents à l'ensemble du trafic entrant, ce qui réduit les efforts de déploiement et d'optimisation par rapport à un ensemble de produits spécialisés.

- **Gestion centralisée avec Panorama.** Prisma Access s'intègre aux autres produits de sécurité de Palo Alto Networks, notamment sa solution Panorama de gestion de la sécurité. Avec Panorama, les entreprises peuvent gérer toutes les politiques de sécurité et surveiller les services depuis une console centrale, chaque application ou service apparaissant dans une même interface. Cela réduit ainsi les temps de formation et améliore l'expérience des équipes informatiques et de sécurité. Quant aux clients qui n'utilisent pas Panorama, ils bénéficient de la console de gestion Prisma Access dédiée dans le cloud.

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](#)
- [Synthèse : TEI™ of Palo Alto Networks for Network Security and SD-WAN](#)
- [TEI Spotlight : CloudGenix SD-WAN](#)
- [TEI Spotlight : Cloud-Delivered Security Services](#)

ANALYSE TOTAL ECONOMIC IMPACT

Pour plus d'informations, téléchargez le rapport complet « [The Total Economic Impact™ of Palo Alto Networks For Network Security And SD-WAN](#) », réalisé par Forrester Consulting pour Palo Alto Networks.

RESULTATS DE L'ETUDE

Forrester a interrogé 143 clients, dont 10 lors d'entretiens approfondis. Tous ces clients utilisent Prisma Access de Palo Alto Networks avec d'autres services de sécurité dans le cloud, SD-WAN et pare-feu nouvelle génération (NGFW). Forrester a ensuite combiné les résultats en une analyse financière sur trois ans. Les avantages quantifiés en valeur actualisée ajustée au risque incluent :

- Evitement des coûts d'infrastructure de la stack de sécurité et gestion plus efficace : 11,7 millions \$ au total.
- Gains d'efficacité au niveau de la sécurité, des opérations informatiques et des utilisateurs : 6 millions \$ au total.
- Réduction du risque de compromission de données : économie de 9,2 millions \$.
- Lisez l'étude complète pour découvrir tous les autres avantages et détails.



Retour sur investissement (ROI)
247 %



Valeur actuelle nette (VAN)
28,5 millions \$

Annexe A : Notes de fin

¹ Total Economic Impact est une méthodologie développée par Forrester Research qui améliore les processus de prise de décisions technologiques de l'entreprise et aide les fournisseurs à communiquer la proposition de valeur de leurs produits et services à leurs clients. La méthodologie TEI permet aux entreprises de démontrer, justifier et réaliser la valeur concrète des initiatives informatiques auprès de leur direction et des autres principaux acteurs de l'entreprise.

DECLARATIONS

Le lecteur doit être conscient de ce qui suit :

- L'étude est réalisée par Forrester Consulting pour Palo Alto Networks. Elle n'est pas destinée à servir d'analyse concurrentielle.
- Forrester n'émet aucune hypothèse quant au retour sur investissement potentiel dont pourraient bénéficier d'autres entreprises. Forrester conseille fortement aux lecteurs d'utiliser leurs propres estimations dans le cadre fourni dans le rapport pour déterminer la pertinence d'un investissement dans les solutions de sécurité réseau et de SD-WAN de Palo Alto Networks.
- Palo Alto Networks a examiné le contenu de cette publication et apporté des commentaires à Forrester. Toutefois, nous conservons un contrôle éditorial total sur l'étude et ses résultats et n'acceptons pas de procéder à des modifications qui pourraient entrer en contradiction avec les conclusions de Forrester ou obscurcir la signification de l'étude.
- Palo Alto Networks a fourni les noms des clients pour les entretiens, mais n'a pas participé à ces derniers.

A PROPOS DE TEI

Total Economic Impact™ (TEI) est une méthodologie développée par Forrester Research qui améliore les processus de prise de décisions technologiques de l'entreprise et aide les fournisseurs dans la communication de la proposition de valeur de leurs produits et services aux clients. La méthodologie TEI permet aux entreprises de démontrer, justifier et réaliser la valeur concrète des initiatives informatiques auprès de leur direction et des autres principaux acteurs de l'entreprise. La méthodologie TEI s'appuie sur quatre éléments fondamentaux pour l'évaluation de la valeur des investissements : avantages, coûts, risques et flexibilité.

FORRESTER®