FORRESTER®

Les services de sécurité dans le cloud de Palo Alto Networks renforcent la sécurité et amplifient les avantages des autres investissements en sécurité réseau

A mesure que l'architecture des réseaux devient plus complexe, les équipes de sécurité ont de plus en plus de difficultés à s'adapter et à assurer une sécurité cohérente de tous les appareils et de toutes les données qui transitent sur leurs réseaux et clouds. Les services de sécurité par abonnement prennent une place chaque jour plus importante dans les stratégies de la plupart des entreprises. Ils permettent une montée en puissance rapide de la protection grâce à des mises à jour appliquées parfois toutes les minutes, tout en simplifiant le déploiement et la gestion de la sécurité. Bien que le prix reste une préoccupation majeure pour de nombreuses entreprises, elles doivent également prendre en compte les capacités propres à chaque produit de sécurité (existant et nouveau) afin d'évaluer la manière dont ces services s'intègrent aux systèmes et workflows existants, tout en en améliorant l'efficacité.

Forrester a récemment échangé avec plusieurs clients Palo Alto Networks de leur investissement dans la gamme de services de sécurité dans le cloud. Les entretiens menés dans le cadre d'une étude Total Economic Impact™ (TEI) visaient à comprendre la valeur et l'impact de ces services sur leur stratégie de sécurité globale.

Les entreprises disposent d'une myriade de solutions et de services de sécurité conçus pour répondre à des besoins spécifiques. Les contraintes de ressources, entre autres facteurs, les empêchent d'atteindre le plein potentiel de ces éléments disparates en termes de valeur et de capacités.

Voici quelques-uns des **principaux défis à relever** :

- Gérer des stacks de solutions de sécurité tentaculaires faisant intervenir de multiples fournisseurs, plateformes et fonctionnalités qui se chevauchent.
- Intégrer des services ciblés en mode cloud, de nouveaux appareils ou des configurations réseau avec des systèmes et réseaux existants dans le cloud ou sur site.

Avantages liés aux services de sécurité dans le cloud

Temps nécessaire pour atteindre un niveau de sécurité adéquat à des solutions spécialisées

30 % plus rapide

Réduction du risque de compromission de la sécurité

45 %

Economies d'infrastructure réalisées grâce au déploiement d'une plateforme commune en replacement de solutions spécialisées

9,9 millions de dollars

- Adapter efficacement les mesures, les procédures et les politiques de sécurité afin de réduire au maximum les failles tout en maintenant le contrôle.
- Analyser et suivre les écarts de sécurité entre les différents fournisseurs offrant des produits similaires déployés dans différentes infrastructures.

Forrester a également constaté que la vitesse était importante, notamment lorsqu'il s'agit de se défendre contre des attaques qui s'appuient sur des temps de présence prolongés pour proliférer sur le réseau. Les services Live font une différence considérable pour réduire les risques organisationnels.

Les principaux services abordés dans cette étude incluent les systèmes de détection et de prévention des intrusions (IPS/IDS), l'analyse des malwares et le sandboxing, la sécurité web (passerelle web sécurisée [SWG], sécurité DNS), la sécurité SaaS (Software-as-a-Service), le CASB (Cloud Access Security Broker) et la sécurité de l'Internet des objets (IoT).

Pour relever ces grands défis, les entreprises ont recherché une solution de sécurité unifiée capable :

- De partager automatiquement de la Threat Intelligence pour assurer une défense en profondeur
- D'intégrer toute l'infrastructure existante (matériel, logiciels, services d'abonnement et cloud) sur une plateforme unique
- D'être gérée de manière centralisée sous une interface utilisateur homogène

Palo Alto Networks propose plusieurs services de sécurité dans le cloud spécialement conçus pour se compléter et s'améliorer mutuellement. Ensemble, ils assurent au client la sécurité de tout le trafic transitant par les réseaux ou les clouds. En outre, ces fonctionnalités de sécurité prennent en charge et sous-tendent le modèle de sécurité Zero Trust pour les initiatives de sécurité réseau.

Ce gros plan s'intéresse exclusivement aux services suivants de sécurité dans le cloud de Palo Alto Networks, à leur valeur et à leur impact sur les entreprises interrogées :

- Threat Prevention (pour IPS).
- WildFire (pour l'analyse des malwares et le sandboxing).
- URL Filtering et DNS Security (pour la sécurité web ou SWG).
- IoT Security (pour la protection des appareils IoT, IoMT et OT).
- Prisma SaaS (sécurité SaaS ou CASB).

Ces solutions sont associées aux pare-feu nouvelle génération (NGFW), à la gamme VM-Series et à Prisma Access de Palo Alto Networks pour garantir une sécurité homogène sur tous les sites (siège, datacenters, sites distants et télétravailleurs).

Pour obtenir une description de chaque service de sécurité dans le cloud, reportez-vous au glossaire en fin de document.

RESULTATS CLES

Voici quelques-uns des résultats clés de l'étude TEI :

6 millions de dollars de gains d'efficacité pour les opérations de sécurité et les utilisateurs finaux. Les équipes du centre d'opérations de sécurité (SOC) ont pu réduire de 35 % le nombre d'investigations avancées, améliorer de 20 % la durée moyenne de résolution (MTTR) et réduire de 50 % le nombre d'appareils devant être réimagés. Ces avantages ont eu un impact positif sur les utilisateurs finaux qui ont moins sollicité leurs équipes de sécurité et pour des durées moins longues.

9,2 millions de dollars d'économies grâce à une réduction de 45 % des risques de compromission de données. Chacun des services de sécurité dans le cloud de Palo Alto Networks s'intègre de manière transparente et améliore les capacités des pare-feu nouvelle génération (NGFW) pilotés par machine learning bénéficiant de l'apprentissage automatique. La couverture et les capacités de protection du réseau sont donc meilleures, tout en protégeant l'intégralité de la surface d'attaque. En cas de compromission de données, les entreprises doivent faire face à une myriade de coûts. Les services de sécurité dans le cloud de Palo Alto Networks permettent d'éviter que l'incident ne se produise, ce qui contribue également à réduire les coûts éventuels en aval.

- **Réduire les menaces liées aux appareils et activités des employés.** Les services de sécurité dans le cloud de Palo Alto Networks étant basés sur le modèle de sécurité Zero Trust, les entreprises sont mieux protégées contre les menaces externes et internes. Différents services travaillent ensemble pour surveiller en permanence le trafic web, le trafic applicatif, les données des applications SaaS, les analyses basées sur les utilisateurs et les entités, l'exfiltration des données, ainsi que les vulnérabilités zero-day et les malwares. Une meilleure protection permet de réduire les incidents, ce qui se traduit par une disponibilité opérationnelle accrue des systèmes et des employés.
- **Limiter les attaques coordonnées sur les applications, serveurs et sites.** Grâce aux dernières avancées en matière d'algorithmes de détection, de signatures et de capacités de protection inline par machine learning des produits de Palo Alto Networks, les services de sécurité dans le cloud de l'entreprise

peuvent analyser une menace nouvellement découverte dans une partie de l'organisation d'un client donné, détailler ses composants, partager la Threat Intelligence entre les services de sécurité et diffuser les mesures de prévention en quelques secondes afin que tout autre site ou client puisse se protéger efficacement contre cette menace zero-day ou ses variantes à toutes les étapes du cycle d'attaque. Par exemple, les nouveaux malwares qui tentent de se connecter à un domaine inconnu sont automatiquement analysés. Les solutions Threat Prevention, WildFire, URL Filtering et DNS Security reçoivent alors toutes les mises à jour à partir des renseignements collectés, créant ainsi des mesures de prévention contre cette technique et chaque tactique individuelle pour tous les clients. Cet aspect unique de la protection améliore considérablement la couverture au niveau fondamental des menaces et vulnérabilités zero-day par rapport aux précédentes solutions spécialisées et cloisonnées basées sur le cloud.

9,9 millions de dollars de réduction et évitement des coûts liés à l'infrastructure de sécurité et 1,9 millions de dollars supplémentaire d'économie grâce une gestion plus efficace de la stack de sécurité qui réduit les workloads de près de 50 %. Avec les services de sécurité dans le cloud de Palo Alto Networks, les entreprises peuvent rationaliser et supprimer une grande partie de leur stack de sécurité existante, réduisant ainsi le nombre de fournisseurs dans leur environnement et le volume de licences de sécurité nécessaires pour protéger leurs réseaux.

- **Réduire la complexité pour simplifier la gestion.** Les entreprises interviewées ont pu réaffecter près de la moitié de leurs équipes de gestion de l'infrastructure de sécurité à d'autres tâches grâce à l'efficacité apportée par les services de sécurité dans le cloud de Palo Alto Networks et à leur intégration à Panorama, la console de gestion de la sécurité réseau de Palo Alto Networks qui offre une interface homogène pour tous les produits. Les équipes de gestion ont pu travailler plus en amont pour éliminer le travail d'investigation avancée, réduire les efforts liés aux mises à jour et aux correctifs, et passer moins de temps à gérer les politiques et données grâce au pilotage centralisé de toutes les politiques de sécurité en un seul endroit.

  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. »

- **Une plateforme commune réduit le nombre de fournisseurs et de licences de sécurité, permettant ainsi aux entreprises de consolider et de rationaliser leur stack de sécurité.** En déployant un ensemble complet de produits et de fonctionnalités de sécurité sur une plateforme centralisée, les entreprises peuvent réduire considérablement le coût de leurs stacks de sécurité, éliminer les solutions spécialisées et limiter le nombre de fournisseurs et de technologies disparates dans leurs environnements. Un autre avantage de cette consolidation est que les services de sécurité dans le cloud et les pare-feu nouvelle génération (NGFW) de Palo Alto Networks sont conçus pour fonctionner en synergie : les entreprises interviewées déclarent ainsi qu'elles bénéficiaient d'une meilleure couverture de l'ensemble de leurs réseaux, des datacenters aux télétravailleurs.

> Grâce aux services de sécurité dans le cloud et à Panorama, vous pouvez réaffecter la moitié **de l'équipe de gestion de l'infrastructure de sécurité à d'autres tâches**.

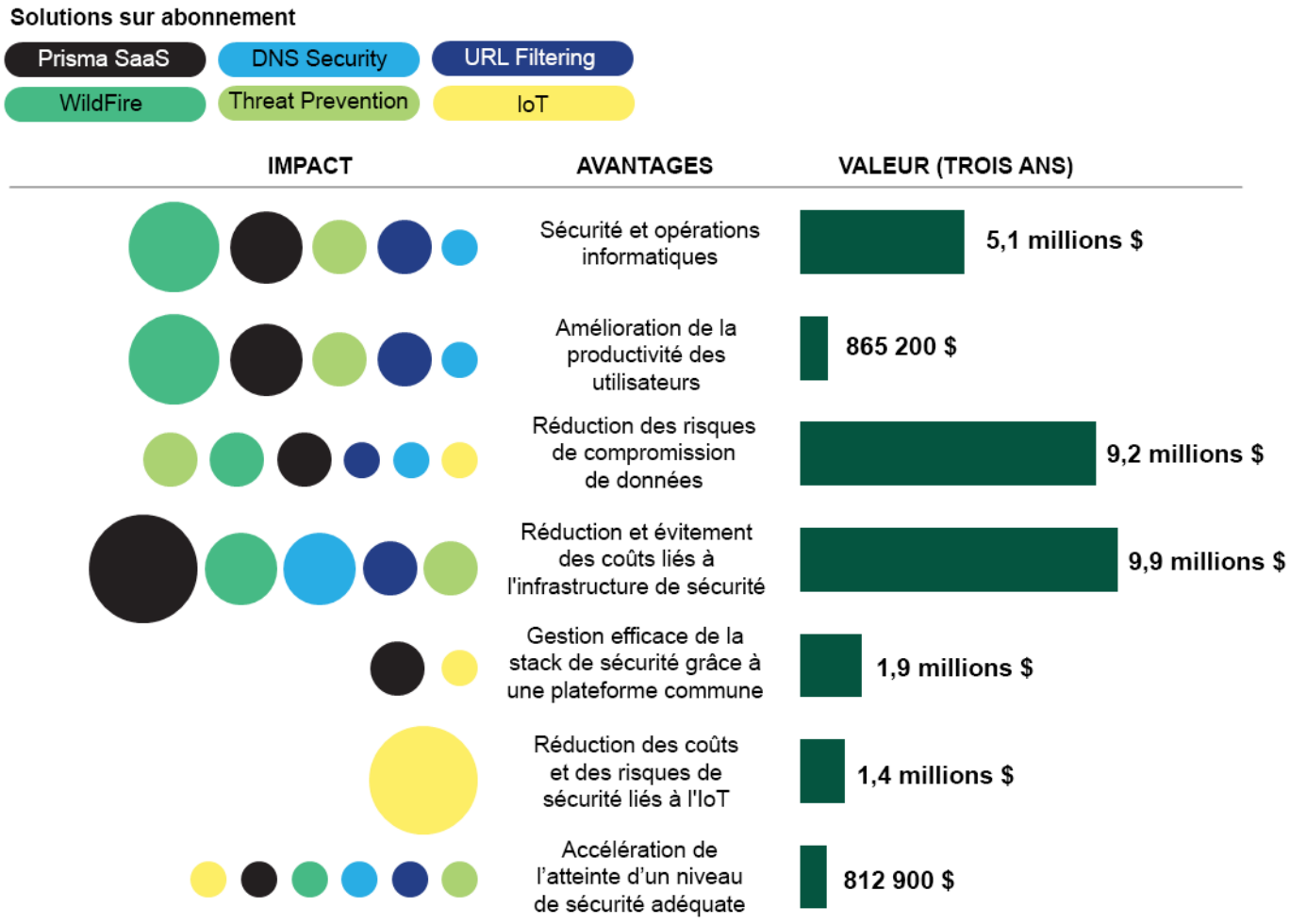
Economie de 1,4 millions de dollars sur l'IoT grâce à la réduction des efforts de gestion et du nombre de nouveaux appareils IoT achetés. Grâce à IoT Security, les entreprises peuvent identifier et sécuriser tous leurs appareils IoT à partir d'une plateforme centrale, comprendre rapidement l'état de 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 dépenses d'achat de nouveaux appareils.

Economie de 812 000 $ grâce à l'accélération de l'atteinte d'un niveau de sécurité adéquat avec Palo Alto Networks, ce qui laisse également plus de temps pour les améliorations. Grâce à Palo Alto Networks, les entreprises ont pu réduire leurs délais de déploiement et d'ajustement. L'intégration native avec les déploiements de NGFW, VM-Series et Prisma Access, ainsi que les fonctionnalités de gestion complémentaires, ont permis aux entreprises de hisser plus facilement leur sécurité à un niveau de stabilité.

Un directeur de la cybersécurité dans le secteur du divertissement témoigne : « Réduire la formation se traduit par une adoption plus rapide et plus cohérente de la solution dans son ensemble. Mon équipe est en mesure de maintenir tout le système à jour plus facilement, ce qui est important car les attaquants innovent constamment. »

- **Réduire le temps consacré à la formation, à la maintenance et aux investigations permet de faire progresser les projets et de créer de la valeur pour l'entreprise.** Un architecte réseau en chef dans le retail / l'industrie explique : « Depuis notre passage à Palo Alto Networks, nous réalisons beaucoup plus de projets. Nous concrétisons enfin cette année plusieurs grands projets pour lesquels nous ne disposions tout simplement pas de ressources suffisantes auparavant. Avec Palo Alto Networks, nous consacrons quotidiennement beaucoup plus de temps à nos projets et beaucoup moins à la surveillance et au suivi. »

Impact relatif des services de sécurité dans le cloud de Palo Alto Networks



Source : tableaux de calcul des avantages de « The Total Economic ImpactTM Of Palo Alto Networks For Network Security And SD-WAN », une étude réalisée par Forrester Consulting pour Palo Alto Networks, novembre 2020

L'IMPACT DE CHAQUE SERVICE DE SECURITE DANS LE CLOUD

Vous trouverez ci-après une description de chaque service de sécurité fourni dans le cloud et de son impact relatif sur les avantages quantifiés susmentionnés.

Prisma SaaS assure la sécurité et la conformité des environnements SaaS et des données cloud. Prisma SaaS rend l'adoption du cloud plus sûre et apporte visibilité, contrôle de conformité et sécurité sur l'ensemble des applications SaaS et des données sensibles. Ce service aide les entreprises à réduire le phénomène de « Shadow IT », à sécuriser les applications SaaS d'entreprise, à limiter les risques de compromission ou d'exposition accidentelle des données dans le cloud, et à améliorer la confidentialité et la conformité des données.

Avec Prisma SaaS, les entreprises bénéficient d'une sécurité cohérente dans le cloud et d'une protection des données sur l'ensemble des applications SaaS, autorisées ou non. Partie intégrante de l'offre de sécurité de Palo Alto Networks, Prisma SaaS s'intègre parfaitement au programme de cybersécurité global des entreprises : son déploiement simplifié permet d'éviter l'approche fragmentée de contrôles isolés, tels que les fonctionnalités de sécurité intégrées CASB et SaaS.

Sécuriser l'accès web réduit le nombre d'alertes et d'investigations. URL Filtering détecte et bloque toute menace basée sur le web, puis transfère les alertes et données dans Panorama pour une seconde analyse et un examen des politiques, si nécessaire. Le service URL Filtering de Palo Alto Networks permet aux utilisateurs d'accéder en toute sécurité au web. Il les protège des attaques de phishing, des malwares, des kits d'exploits et d'autres formes de sites web malveillants. Le service URL Filtering s'intègre nativement à tous les pare-feu nouvelle génération (NGFW) physiques, virtuels et dans le cloud. Les équipes de sécurité n'ont donc besoin de gérer et de déployer qu'un seul ensemble de politiques de sécurité.

Grâce au service URL Filtering, les entreprises réduisent le nombre d'incidents de sécurité nécessitant des investigations avancées, elles limitent les risques de compromission de données et procèdent au retrait de leurs anciennes technologies de sécurité web.

WildFire protège les ressources contre les menaces zero-day. WildFire offre une détection et une analyse en sandbox des malwares dans le cloud, avec des mises à jour en temps réel pour vous protéger contre les menaces inconnues ou contournant vos systèmes de protection, y compris les malwares polymorphes en mutation rapide. Outre la diffusion en temps réel des mises à jour, WildFire est doté d'une capacité de machine learning inline qui bloque instantanément la plupart des nouvelles menaces à base de fichiers. WildFire s'est rapidement imposé comme un élément clé de la stratégie de sécurité des entreprises interviewées, et ce de plusieurs manières : protection immédiate, distribution de la Threat Intelligence pour améliorer d'autres services, réduction du nombre d'événements à analyser par heure grâce à des informations détaillées sur le comportement des menaces identifiées, et transmission d'alertes exploitables au centre d'opérations de sécurité (SOC).

Avec WildFire, les entreprises améliorent l'efficacité des équipes informatiques et de leur SOC, elles réduisent les risques de compromission de données et procèdent au retrait de leurs anciennes technologies de sandboxing.

DNS Security s'appuie sur l'analytique prédictive pour bloquer les domaines malveillants et neutraliser les attaques qui utilisent le DNS pour voler des données ou établir des activités de commande et contrôle (CnC). Le service DNS Security examine le trafic DNS et bloque les tunnels DNS, les algorithmes de génération de domaine et d'autres menaces DNS susceptibles de permettre aux attaquants de se propager latéralement sur le réseau.

DNS Security bloque les menaces au niveau du DNS avant qu'elles ne causent des dommages, ce qui évite aux autres dispositifs et équipes de sécurité de devoir réagir rapidement.

Réduire les dépenses annuelles d'achat de nouveaux appareils IoT

10 %

Threat Prevention bloque plus rapidement des menaces et exploits de vulnérabilités connues. Le service Threat Prevention de Palo Alto Networks intègre des fonctions de prévention des intrusions (IPS) et d'analyse des menaces pour prévenir toutes les menaces et vulnérabilités connues sur l'ensemble du trafic, et ce en une seule passe. Il consolide les capacités de déploiement des pare-feu nouvelle génération (NGFW) en fournissant automatiquement les dernières mises à jour sur les menaces à tous les formats de NGFW. Les exploits, logiciels espions, malwares et autres menaces sont neutralisés à un stade précoce pour contrer toute infection et les investigations d'alertes qui s'ensuivent. En collaboration avec WildFire (qui se charge de la prévention des menaces inconnues), Threat Prevention peut bloquer les malwares en amont en appliquant des mesures de prévention communes à tous les contrôles de sécurité afin de renforcer la sécurité en quasi-temps réel.

Grâce au service Threat Prevention, les entreprises réduisent le nombre d'incidents de sécurité nécessitant des investigations avancées, elles limitent les risques de compromission de données et procèdent au retrait de leurs anciennes solutions IPS.

IoT Security réduit les efforts de gestion et prolonge le cycle de vie des appareils. Le service IoT Security de Palo Alto Networks s'intègre aux NGFW, VM-Series et à la console de gestion des accès Prisma Access de Palo Alto Networks. L'ensemble forme un point unique de visibilité et de gestion des politiques de tous les appareils IoT. Après avoir déployé IoT Security, les entreprises interviewées ont pu facilement retrouver des appareils précédemment inconnus ou perdus pour segmenter et surveiller tout le trafic associé. En outre, IoT Security a pu recommander des politiques de confiance recommandées pour appliquer plus facilement les contrôles de sécurité aux appareils IoT et améliorer la sécurité organisationnelle, réduire la surface d'attaque exposée aux cybercriminels potentiels d'actes malveillants, et contrôler plus précisément les risques.

> **« Je dispose désormais d'une politique de sécurité plus cohérente sur l'ensemble de mon infrastructure, et ce dans le monde entier. »**
>
> *Responsable d'architecture IT chez un fabricant informatique*

POURQUOI DES ENTREPRISES ONT-ELLES CHOISI LES SERVICES DE SECURITE DANS LE CLOUD DE PALO ALTO NETWORKS ?

Les entreprises interviewées ont avancé plusieurs raisons ayant motivé leur choix, notamment :

- **Intégration transparente au sein d'une console de gestion avec Palo Alto Networks Panorama.** Tous ces services s'intègrent en toute transparence aux NGFW et à Panorama, la plateforme de gestion centralisée de Palo Alto Networks. Ensemble, ils réduisent la charge de travail de l'équipe informatique et du SOC en fournissant une plateforme commune avec une plateforme commune dotée d'une même interface pour toutes les technologies et tous les services de sécurité. Un responsable de la sécurité réseau dans le secteur du retail déclare : « Le service URL Filtering fait partie intégrante de notre stratégie de sécurité, et les alertes WildFire sont extrêmement efficaces. »

  Un vice-président senior du secteur des services financiers explique : « Le principal avantage pour nous a été l'amélioration de notre stratégie de sécurité, notamment en matière d'accès à l'internet. Grâce à Palo Alto Networks, nous pouvons identifier le trafic en cours, autoriser uniquement le trafic dont nous avons besoin et bloquer tout le reste, qu'il s'agisse d'une connexion URL ou d'une application. »

  Un vice-président en charge de la cybersécurité dans le secteur du divertissement ajoute : « L'un des principaux avantages est la cohérence de la plateforme. Les personnes en charge de l'administration de Prisma SasS, Prisma Cloud et tous les autres services évoluent dans un environnement homogène. Aujourd'hui, je n'ai plus besoin d'envoyer mes collaborateurs suivre différentes formations pour savoir comment utiliser nos outils. Pour le reste, tout se trouve dans Panorama : Threat Prevention, WildFire, URL Filtering, DNS Security, politiques de pare-feu et règles de déchiffrement... Tout est là, dans Panorama. Tout arrive et part de ce modèle commun d'interface utilisateur. »

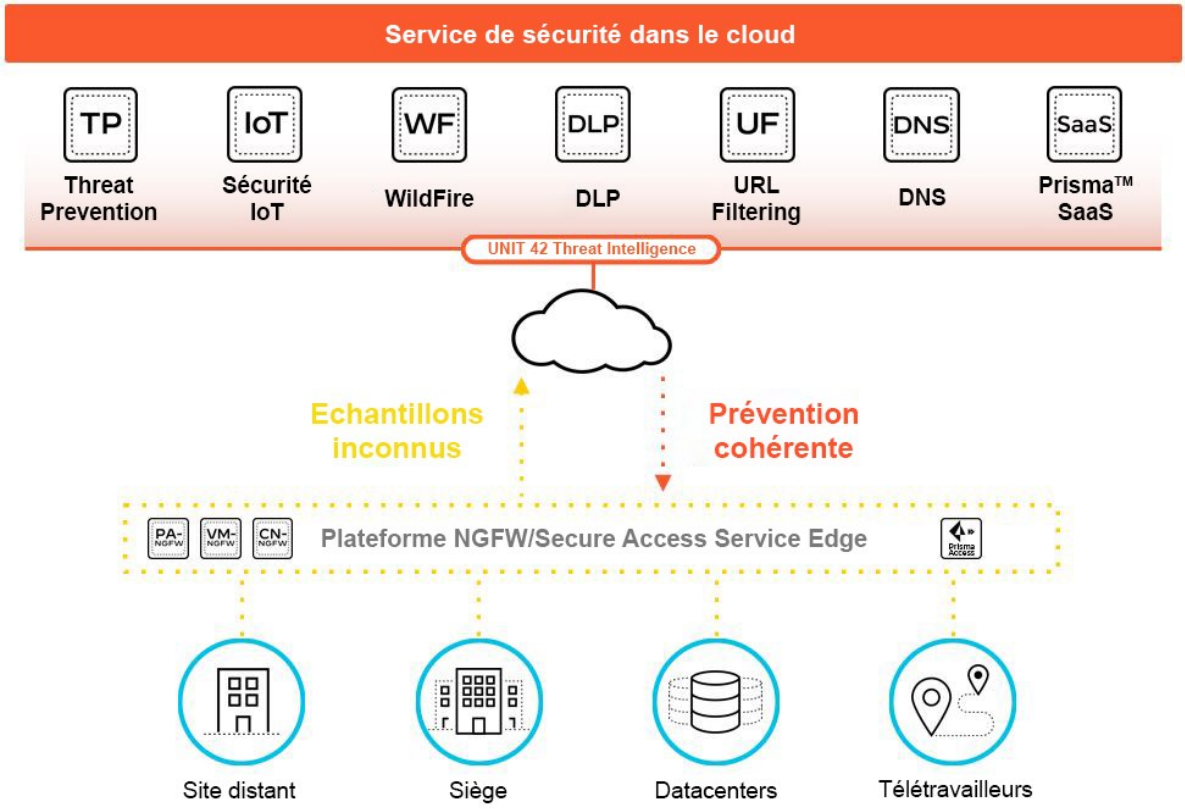
- **La sécurité sans compromettre les performances.** Les entreprises interviewées ont indiqué que le secteur de la sécurité en général s'oriente vers un modèle de services par abonnement et que la technologie de Palo Alto Networks, avec ses capacités de traitement parallèle, est spécifiquement conçue pour surpasser ses concurrents dans ce type d'environnement. De plus, grâce au machine learning inline de Palo Alto Networks, les offres de sécurité sont en constante amélioration et assurent une meilleure protection.

Un responsable de la sécurité des systèmes d'information (RSSI) dans le secteur du retail témoigne : « Nous savions qu'à terme, le secteur de la sécurité allait davantage évoluer vers un modèle d'abonnements liés au matériel existant. C'est l'hypothèse que nous avons adoptée pour nos opérations. Palo Alto Networks est le seul pare-feu conçu avec une architecture de traitement parallèle. Ainsi, lorsque toutes les fonctionnalités sont activées, comme nous envisageons de le faire, il n'y a pas de baisse de performance comme nous avions pu le constater avec les autres technologies. »

Glossaire : produits Palo Alto Networks

Les informations suivantes sont fournies par Palo Alto Networks. Forrester ne valide aucune des déclarations et ne cautionne ni Palo Alto Networks ni ses offres.

- **CLOUDGENIX SD-WAN :** SD-WAN autonome de nouvelle génération permettant de définir les accès des sites distants aux applications cloud en fonction de critères propres à chacune d'elles.
- **DNS SECURITY :** service cloud-native qui utilise des analyses prédictives pour neutraliser les attaques exploitant le DNS à des fins de commande et contrôle (CnC) ou de vol de données.
- **ENTERPRISE DATA LOSS PREVENTION (DLP) :** premier système cloud d'entreprise pour la prévention de fuites de données (DLP) d'entreprise dans le cloud du secteur ; il protège systématiquement les données sensibles sur tous les réseaux, dans tous les clouds et chez tous les utilisateurs. (Le produit Enterprise DLP n'a pas été pris en compte dans l'analyse TEI.)
- **IOT SECURITY :** le seul produit de sécurité IoT complet du marché capable d'offrir une transparence totale sur tous les appareils IoT et OT, tout en les protégeant et en optimisant leur efficacité.
- **PARE-FEU NOUVELLE GENERATION (NGFW) :** gamme leader du marché de pare-feu physiques (PA-Series), virtuels (VM-Series) et conteneurisés (CN-Series) qui s'appuient sur le machine learning pour pour assurer une protection proactive.
- **PANORAMA :** solution de gestion centralisée de la sécurité réseau pour vos pare-feu nouvelle génération Palo Alto Networks – tous formats et tous sites confondus.
- **PRISMA ACCESS :** solution SASE (Secure Access Service Edge) pour les réseaux et la sécurité au sein d'une infrastructure cloud dédiée.
- **PRISMA SAAS :** visibilité, sécurité et conformité totales du plus large éventail d'applications SaaS du marché et des données qu'elles hébergent.
- **THREAT PREVENTION :** système avancé de prévention des intrusions (IPS) leader du marché ; il inspecte l'ensemble du trafic à la recherche de menaces et bloque automatiquement les vulnérabilités identifiées.
- **UNIT 42 :** équipe internationale de Threat Intelligence de Palo Alto Networks et autorité reconnue en matière de cybermenaces. Elle fournit des analyses aux équipes de sécurité et des protections sophistiquées pour l'ensemble du portefeuille de produits, et ce par une étude minutieuse des acteurs et de leurs modes opératoires.
- **URL FILTERING :** solution de sécurité web cloud-native qui protège les entreprises contre les menaces du web telles que le phishing, les malwares et les activités de commande et contrôle (CnC).
- **WILDFIRE :** leader des moteurs d'analyse avancée des malwares qui identifie et neutralise les menaces inconnues à base de fichiers.



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 : Prisma Access

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 » rédigé par Forrester Consulting pour Palo Alto Network.

RESULTATS DE L'ETUDE

Forrester a interviewé neuf décideurs de différentes entreprises ayant déjà utilisé les pare-feu de nouvelle génération (NGFW) et services de sécurité dans le cloud de Palo Alto Networks. Forrester a ensuite combiné les résultats en une analyse financière d'organisation composite sur trois ans. Les avantages quantifiés en valeur actualisée ajustée au risque incluent :

- Les gains en sécurité et efficacité des équipes informatiques incluent une réduction de 35 % des incidents de sécurité nécessitant une investigation avancée et une réduction de 20 % de la durée moyenne de résolution (MTTR), pour une économie totale de 5,1 millions de dollars.
- Réduction du risque de compromission des données de 45 %, soit une économie de 9,2 millions de dollars.
- Evitement des coûts d'infrastructure de la stack de sécurité et gestion plus efficace : 11,7 millions de dollars au total.

Retour sur investissement (ROI)

247 %

Valeur actuelle nette (VAN)

28,5 millions de dollars

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 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 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®