Naviguer dans les méandres de la sécurité SaaS

Le seul CASB intégré capable d'absorber l'explosion du SaaS

Sommaire

3 Introduction

4 Adoption du SaaS : un chemin semé d'embûches

5 Protection des données : le prix élevé d'une non-conformité

6 Relever les défis de visibilité et de sécurité

7 Les remèdes traditionnels ne fonctionnent plus

9 Adopter les applications SaaS en toute sécurité

10 Stratégie de sécurité SaaS pour vos données

11 SaaS Security : au cœur du modèle SASE

12 Sécurité SaaS : la différence Palo Alto Networks

13 Conclusion

Introduction

Avec l'émergence de technologies innovantes ces dernières années, les entreprises ont entamé la migration de leurs applications et données vers le cloud, en particulier vers des plateformes SaaS comme Microsoft Office 365®, Box et Salesforce, mais aussi des services IaaS et PaaS comme Google Cloud Platform (GCP®), Amazon Web Services (AWS®) ou Microsoft Azure®. Par rapport aux solutions sur site, le cloud offre de sérieux avantages, à commencer par des économies substantielles et une meilleure collaboration des utilisateurs à travers le monde.

Seule ombre au tableau, ces technologies peuvent présenter des risques de sécurité importants, parmi lesquels :

- **Shadow IT –** Les salariés utilisent un grand nombre d'applications SaaS sans passer par le réseau de l'entreprise, et souvent même à l'insu du département informatique. Il en découle une perte de visibilité et de contrôle sur le parc applicatif et les risques associés.
- **Expansion du périmètre réseau –** Avec l'adoption du cloud, les données, les applications et les utilisateurs sortent du réseau traditionnel sur site. L'entreprise doit donc protéger un périmètre réseau bien plus étendu.
- **Partage accru des données sur le web –** Les entreprises doivent désormais gérer une montagne de données, des plus anodines aux plus stratégiques et confidentielles, à travers une multitude d'environnements (applications SaaS, cloud public, data center, terminaux utilisateurs, etc.).
- **Co-responsabilité en matière de conformité et de sécurité –** Dans l'univers du cloud, clients et fournisseurs se partagent les responsabilités en matière de sécurité et de conformité. Les entreprises utilisatrices ne peuvent donc se délester entièrement de leurs devoirs sur ces questions.

La convergence de toutes ces causes engendre une perte de visibilité et de contrôle sur les réseaux, en particulier sur l'activité en ligne des salariés, les ressources qu'ils utilisent, l'emplacement et la protection des données sensibles, et enfin la sécurité de l'entreprise dans son ensemble.

Cet eBook dresse un état des lieux des principaux obstacles sur la voie du cloud. Vous y trouverez des éclairages utiles qui vous aideront à mieux protéger vos applications, vos données et vos utilisateurs.

Adoption du SaaS : un chemin semé d'embûches

On ne compte plus les entreprises qui, depuis quelques années, se tournent vers les applications SaaS pour leur plus grande disponibilité, leur simplicité d'utilisation et leurs faibles coûts.

Selon Gartner, le marché des services de cloud public devrait afficher une croissance de 18,4 % en 2021, soit un total de 304,9 milliards de dollars par rapport aux 257,5 milliards de 2020. Le cabinet prévoit également que les ventes mondiales d'applications SaaS dépasseront, à elles seules, les 117 milliards de dollars en 2021[1].

Pour autant, simplicité et sécurité ne vont pas toujours de pair et bien des entreprises peinent à adopter et à utiliser des applications SaaS en toute confiance. En voici les deux principales raisons :

- Elles gèrent une constellation d'applications SaaS à usage personnel ou professionnel, avec ou sans l'assentiment du département informatique (applications approuvées, tolérées ou non approuvées dans le cas du Shadow IT).
- Elles stockent et exploitent toujours plus de données dans le cloud, y compris des informations sensibles concernant leurs activités et leurs clients. Or, il est extrêmement difficile de protéger de tels volumes dès lors que les données quittent le réseau et circulent librement entre une multitude d'utilisateurs et d'applications cloud.

Selon une étude ESG, le Shadow IT et la protection des données sont aujourd'hui les deux grands casse-tête des entreprises en matière de sécurité dans le cloud. Leurs préoccupations portent en particulier sur la souscription d'applications et services cloud sans aval ni contrôle du département informatique (35 %), et sur la difficulté à identifier et classer les données personnelles à des fins de confidentialité et de conformité réglementaire (30 %)[2].

Le cloud n'a pas de barrières

- Accès direct au cloud
- Shadow IT
- Partage externe de données

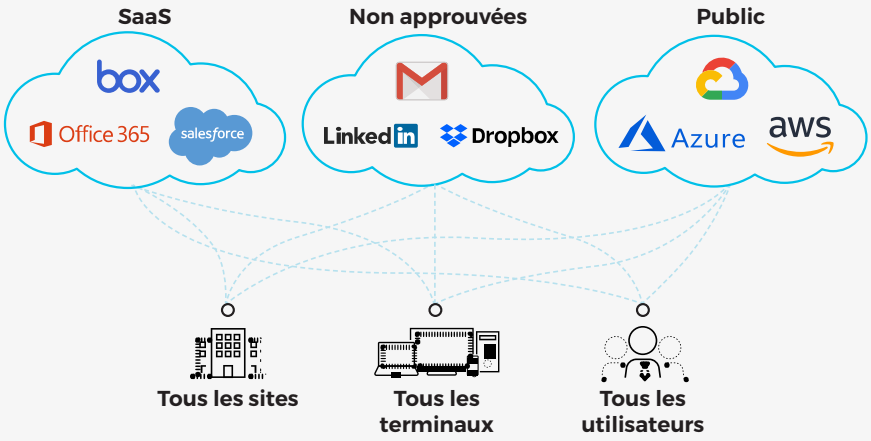


Figure 1 : L'ubiquité du cloud

1. « Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021 », Gartner, 17 novembre 2020, https://www.gartner.com/en/newsroom/press-releases/2020-11-17-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-grow-18-percent-in-2021.
2. « ESG Master Survey Results: Trends in Data Security », ESG, 28 janvier 2019, https://www.esg-global.com/research/esg-master-survey-results-trends-in-cloud-data-security.

Protection des données : le prix élevé d'une non-conformité

C'est lorsque les données circulent librement entre réseaux internes et externes que leur protection devient un réel problème. Une fois sur des applications SaaS, difficile de contrôler qui peut ou ne peut pas accéder à ces informations. Plus les fournisseurs SaaS sont nombreux, plus le risque de faille est élevé, tant en termes de sécurité que de conformité. En effet, la prolifération des points de sortie et des ressources mutualisées rend très difficile l'identification, la localisation, le suivi et la protection des données sensibles et réglementées.

Le problème est exacerbé par les nombreuses lois et réglementations qui encadrent la confidentialité des données dans divers secteurs et régions du monde. En Europe, ces préoccupations tombent sous la coupe du Règlement général sur la protection des données (RGPD), même si d'autres textes s'appliquent à travers le monde (HIPAA, PCIDSS, CCPA, etc.).

Il convient enfin de noter que la majorité des entreprises seront tôt ou tard frappées par une compromission ou un incident de sécurité. Et la facture est souvent très salée ! Outre de lourdes amendes, elles s'exposent à des recours judiciaires collectifs et à une érosion de leur image. De quoi pousser leurs clients tout droit vers la concurrence.

3,92 M$

Coût moyen d'une compromission en 2019.[3]

36 %

Baisse de chiffre d'affaires résultant d'une perte de réputation post-incident de sécurité.[3]

11,45 M$

Coût annuel moyen des attaques internes par entreprise en 2020.[4]

644 000 $

Coût moyen d'un incident de sécurité.[4]

20 € ou 4 %

Le RGPD prévoit des amendes pouvant atteindre 20 millions d'euros ou 4 % du CA annuel mondial de l'entreprise contrevenante (selon le montant le plus élevé).[5]

3. « 2019 Cost of a Data Breach Report », Ponemon Institute, juillet 2019, https://www.ibm.com/security/data-breach.
4. « 2020 Cost of Insider Threats Global Report », Ponemon Institute, janvier 2020 https://www.observeit.com/cost-of-insider-threats.
5. « Understanding GDPR Fines », GDPR Associates, consulté le 22 avril 2020, https://www.gdpr.associates/what-is-gdpr/understanding-gdpr-fines.

Relever les défis de visibilité et de sécurité

Pour migrer vers le cloud tout en protégeant votre entreprise, vos données et vos utilisateurs, vous devez vous poser les bonnes questions.

- **Quelles applications cloud vos collaborateurs utilisent-ils, avec quelle fréquence et quels risques ?** C'est là le point de départ d'une politique efficace de maîtrise du Shadow IT.
- **Quels utilisateurs et quels terminaux ont accès aux applications SaaS approuvées par votre entreprise (Microsoft Office 365®**, G Suite®, Salesforce, Box…) ? Seuls les salariés et terminaux de confiance doivent disposer d'un accès.
- **Quelles sont les données sensibles stockées dans le cloud ou téléchargées vers/depuis celui-ci ?** Connaissez-vous leur emplacement exact ?
- **Comment ces données sont-elles utilisées et partagées dans vos applications SaaS ?** Ces pratiques de partage obéissent-elles à vos politiques internes (tiers autorisés ou non autorisés, etc.) ?
- **Quels sont les risques pour la conformité de vos données et applications cloud ?** Comment les réduire ?
- **Quelles menaces planent sur vos applications approuvées ?** Quels sont les comportements utilisateurs à risque et comment changer ces habitudes ?

Quelles applications les salariés utilisent-ils, et comment ?

Comment protéger mes données sensibles dans le cloud ?

Puis-je contrôler et sécuriser l'accès aux applications SaaS ?

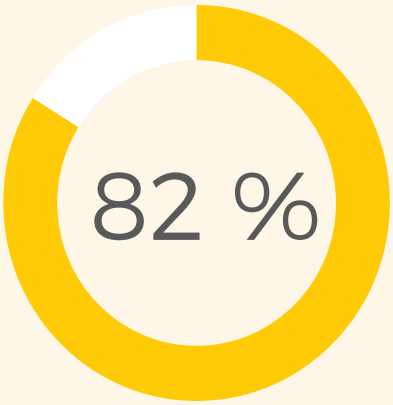
Les remèdes traditionnels ne fonctionnent plus

Pour protéger leurs environnements cloud, bon nombre d'entreprises se tournent dans un premier temps vers différentes solutions traditionnelles, parmi lesquelles :

- **Fonctionnalités intégrées de protection des données** – Hormis le fait qu'elles varient d'un fournisseur à l'autre, les fonctions de sécurité intégrées aux applications SaaS et plateformes IaaS/PaaS n'offrent qu'une protection limitée.
- **Cloud Access Security Brokers (CASB)** – Ces outils ont été spécialement conçus pour conjuguer sécurité et conformité des données sur toutes vos applications SaaS.

  Les CASB présentent cependant d'importantes limites :

  - Ils sont incapables de faire face à l'explosion du SaaS, car ils ne disposent ni d'un moteur de classification automatique ni de fonctionnalités permettant d'identifier les nouvelles applications de manière fiable.
  - Ils n'offrent qu'une sécurité cloud de base. Et leur approche de la protection des données n'a ni l'ampleur ni la profondeur d'une DLP d'entreprise.
  - Ils sont difficiles à déployer et leur architecture composite affiche un coût total de possession (TCO) élevé. Et parce qu'ils s'intègrent très mal avec d'autres outils de sécurité, ils exigent une redirection complexe du trafic depuis le pare-feu et reposent sur des fichiers PAC.

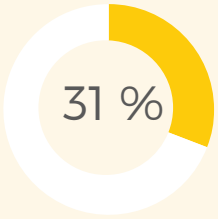


des professionnels de sécurité estiment que les solutions traditionnelles sont partiellement voire totalement inefficaces dans le cloud.[6]

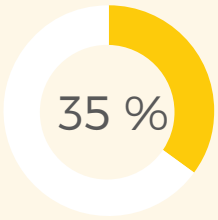
6. « 2020 Cloud Security Report », Cybersecurity Insiders, août 2020.

- **Proxys web** – Ces composants sont connus pour leur faible degré d'interopérabilité, notamment entre eux et avec les pare-feu. Sans oublier qu'ils n'analysent qu'une partie du trafic.
- **Outils de sécurité indépendants** – Parmi ceux-ci figurent les CASB (Cloud Access Security Broker), les passerelles web sécurisées (SWG) et les solutions de prévention des pertes de données (DLP) dans le cloud. Les entreprises se retrouvent alors avec une mosaïque d'outils isolés et déconnectés de leurs équipements de sécurité sur site.

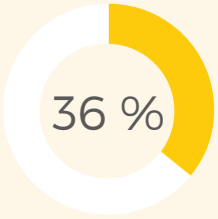
Malheureusement, toutes ces solutions partagent le même défaut : elles sont difficiles à adopter, à déployer et à intégrer au dispositif de sécurité en place dans l'entreprise. Elles présentent par ailleurs souvent des lacunes en termes de sécurité et de visibilité. Au final, leur utilisation crée des environnements fragmentés et complexes à gérer, sans parler des incohérences qui s'immiscent dans les politiques de sécurité et de conformité régissant les diverses applications.



déclarent que leur système de sécurité est incapable de suivre le rythme d'évolution des applications.[7]



pensent que les risques de sécurité, de perte et de fuite de données freinent l'adoption du cloud.[8]



peinent à définir des politiques de sécurité cohérentes sur site et dans le cloud.[9]

7-9. « 2020 Cloud Security Report », Cybersecurity Insiders, août 2020.

Adopter les applications SaaS en toute sécurité

Pour adopter le cloud sans s'exposer, les entreprises doivent miser sur…

… une approche unique et cohérente pour protéger leurs…

Utilisateurs | **Applications** | **Données** | **Activités**

Cette approche doit reposer sur plusieurs piliers :

Visibilité – Une visibilité complète sur le trafic permet d'identifier les applications déployées et l'usage qui en est fait. Les entreprises peuvent ainsi identifier et évaluer les nouveaux risques associés au Shadow IT, mais aussi exercer un contrôle granulaire sur l'utilisation du cloud.

Contrôle des accès – Les entreprises doivent pouvoir contrôler l'accès à leurs applications, ce qui passe par la vérification des identités et l'application des politiques internes associées.

Sécurité intégrale – Une solution de sécurité exhaustive protège les données, applications et utilisateurs où qu'ils se trouvent, sur le réseau interne comme dans le cloud. Elle supprime aussi la complexité inhérente à la multiplicité de produits isolés.

Protection des données – Les entreprises peuvent rechercher, détecter et sécuriser toutes leurs données sensibles et réglementées, stockées ou en transit, quel que soit leur emplacement (cloud, réseau, appareil utilisateur).

Prévention des menaces avancées (ATP) – Une fonctionnalité essentielle pour bloquer les menaces dans le cloud, en temps réel et de façon fiable, sans avoir à adopter des outils tiers.

Gestion du risque et de la conformité – Un outil indispensable pour identifier et neutraliser les risques, zones d'exposition et liens publics dans toutes les applications SaaS, mais aussi protéger toutes les données sensibles et veiller à l'application cohérente des règles de conformité dans le cloud.

Stratégie de sécurité SaaS pour vos données

Adopter le cloud en toute sécurité, c'est d'abord protéger le stockage et l'utilisation des données hors du réseau traditionnel. Ici, les entreprises auront besoin d'une approche méthodique pour récolter tous les fruits d'une stratégie de sécurité SaaS. Trois instruments leur seront indispensables :

L'identification et la classification automatiques permettent de répertorier l'ensemble des données sensibles et réglementées stockées dans ou transitant par le cloud, y compris la propriété intellectuelle et les données personnelles.

La protection des données sécurise les informations au repos et en mouvement (alertes, chiffrement, annulation de partage, application des droits numériques, blocage des transferts dangereux...). Grâce à un système automatique de protection et de prévention des fuites de données, les entreprises réduisent les erreurs humaines et neutralisent tout comportement risqué ou malveillant.

La gestion de la conformité assure d'un côté la confidentialité et le traitement adapté des données sensibles réglementées, et d'un autre le suivi et le contrôle des informations partageables (y compris des destinataires et modes de partage autorisés). Elle simplifie en outre le reporting de conformité et la résolution d'incidents.

Pour en savoir plus sur la protection des données dans le cloud, rendez-vous sur

paloaltonetworks.com/cyberpedia/what-is-cloud-data-protection

SaaS Security : au cœur du modèle SASE

Pour garantir la protection de ses données dans le cloud, votre entreprise a besoin d'une architecture pensée à la fois pour le réseau et pour la sécurité des applications et données, quel que soit leur emplacement : des filiales jusqu'aux succursales et points de vente, en passant par les équipes mobiles.

C'est ici que le Secure Access Service Edge (SASE) entre en jeu. Sa mission : centraliser les services réseau et de sécurité au sein d'une plateforme unique hébergée dans le cloud. Palo Alto Networks vous propose une solution SASE complète pour vous protéger et vous accompagner dans la transformation de votre réseau et l'adoption d'applications SaaS.

Au cœur du modèle SASE de Palo Alto Networks, SaaS Security aide les entreprises à protéger leurs données, applications et utilisateurs de façon homogène, sur leurs propres réseaux comme dans le cloud. Elle leur évite ainsi de recourir à un patchwork complexe de produits isolés (CASB traditionnels, proxys web, etc.), et simplifie le processus d'adoption tout en optimisant l'utilisation des ressources techniques, humaines et financières.

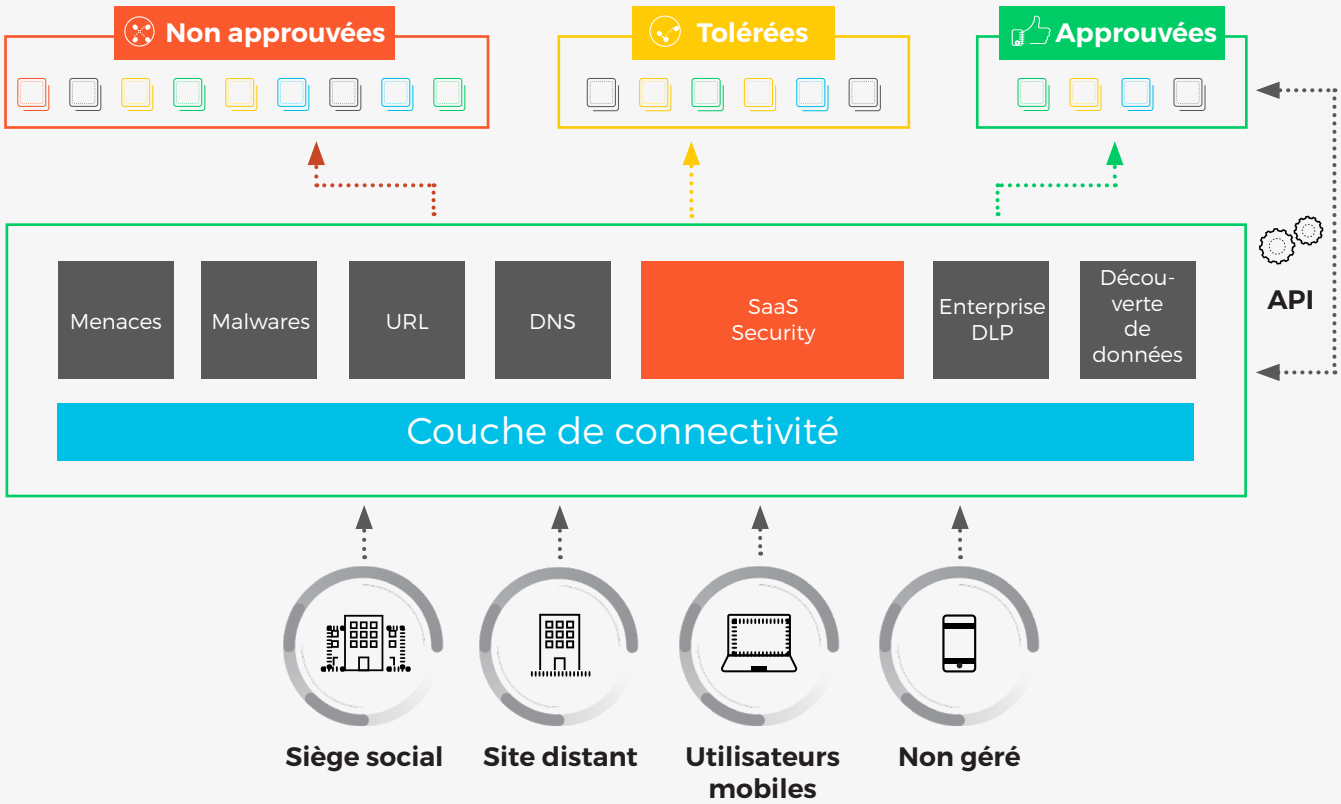


Figure 6 : Les services Palo Alto Networks forment un tout homogène

SaaS Security : la différence Palo Alto Networks

Palo Alto Networks SaaS Security est le seul CASB intégré capable de faire face à l'explosion du SaaS. Intégré en natif aux NGFW Palo Alto Networks, il offre une visibilité proactive, une protection de pointe et la rentabilité la plus rapide pour toutes les applications SaaS.

Ses principales fonctionnalités de sécurité :

- Visibilité complète, catégorisation continue et contrôle granulaire basé sur les risques à l'échelle de milliers d'applications SaaS. Grâce aux données fournies par la communauté mondiale de Palo Alto Networks, SaaS Security sécurise TOUT le trafic, web ou non-web, assurant ainsi la détection automatique des nouvelles applications à mesure qu'elles se répandent.
- Prévention des pertes de données (DLP) pour détecter, surveiller et protéger toutes les données sensibles de l'entreprise, au repos comme en transit, y compris les chargements (sur des applications approuvées ou non approuvées), et les stockages et partages (plateformes IaaS, applications approuvées, utilisateurs de l'entreprise).
- Contrôle des accès pour restreindre l'usage des applications SaaS aux seuls collaborateurs autorisés tout en assurant une expérience utilisateur parfaitement fluide et sécurisée.
- Solution de sécurité complète, homogène et automatisée pour protéger toutes vos données et applications dans le cloud.
- Protection contre les cyberattaques et comportements utilisateurs à risque.
- Fonctionnalité robuste de gestion et résolution des incidents.

Visibilité SaaS à grande échelle

Découverte et contrôle continus des nouvelles applications grâce aux remontées d'informations d'une vaste communauté mondiale.

Protection des données d'entreprise (DLP)

DLP et conformité cohérentes sur tout l'environnement (applications SaaS, réseaux et utilisateurs).

Sécurité optimale

Prévention par ML en temps réel contre les menaces, sans outils de sécurité tiers.

Économies et rentabilité

Solution de sécurité SaaS facile à déployer et offrant un TCO plus bas que les CASB traditionnels.

Conclusion

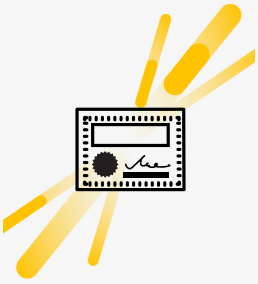
Que vous soyez à l'aube de votre migration ou que vous repensiez votre stratégie de sécurité cloud, n'oubliez pas de réfléchir aux avantages d'une solution SASE complète pour la sécurité de vos applications SaaS. Palo Alto Networks vous prête main-forte en protégeant vos données, vos utilisateurs et vos réseaux contre les risques issus du cloud. La solution SaaS Security de Palo Alto Networks se décline sous la forme d'une console cloud centralisée qui assure une protection homogène de l'ensemble de vos données et applications dans le cloud. Les avantages :

Visibilité complète sur le cloud

- Visibilité sur l'usage du cloud dans l'entreprise : qui, où, quoi, comment ?
- Détection des pratiques de Shadow IT pour en réduire les risques
- Surveillance constante des comportements utilisateurs pour détecter toute activité suspecte

Sécurité cloud complète et homogène

- Protection à tous les niveaux – adoption du cloud, ouverture de nouveaux bureaux, mobilité des utilisateurs…
- Extension des politiques internes au SaaS, notamment pour le contrôle, la conformité et la protection des données
- Suppression des produits de sécurité inutiles



Conformité et confidentialité dans le cloud

- Gestion des accès et contrôle des droits pour éviter les abus de privilèges
- Identification, classification et protection automatiques des données réglementées sur vos diverses applications
- Accompagnement vers vos objectifs de conformité et de confidentialité des données

Pour plus d'informations sur Palo Alto Networks SaaS Security, rendez-vous sur

paloaltonetworks.com/network-security/saas-security

À propos de Palo Alto Networks

Leader mondial de la cybersécurité, Palo Alto Networks développe des technologies qui transforment le quotidien des utilisateurs et des entreprises dans un avenir placé sous le signe du cloud. Notre mission : protéger les modes de vie numériques contre les cyberattaques. Intelligence artificielle, analytique, automatisation, orchestration… nous innovons sur tous les fronts pour aider les entreprises à relever les défis de sécurité les plus sensibles. Grâce à notre plateforme intégrée et à un écosystème de partenaires en pleine croissance, nous assurons la sécurité de dizaines de milliers d'entreprises sur le cloud, les réseaux et les terminaux mobiles. Nous comptons ainsi œuvrer pour un monde où chaque nouveau jour est plus sûr que le précédent. Pour de plus amples informations, **rendez-vous sur www.paloaltonetworks.fr.**

www.paloaltonetworks.fr

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone : +31 20 888 1883