Sécurité IoT :
guide d'achat des entreprises

Cinq fonctionnalités indispensables d'une solution de sécurité IoT à la hauteur de vos enjeux

Sommaire

L'IoT se généralise dans l'entreprise

Les entreprises qui parviennent à intégrer l'IoT (Internet des objets) à leurs modèles économiques en récoltent les nombreux fruits, tant au niveau de leurs processus internes que de leurs clients et collaborateurs.

Si l'IoT séduit avant tout par ses avantages en termes d'efficacité, de productivité et d'économies, un nombre croissant d'entreprises y voient également une formidable source d'informations sur l'impact réel des produits sur la vie de leurs clients et de leurs salariés.

Ce constat est somme toute logique dans la mesure où l'IoT ne vaut que par les données qu'il génère, véritable atout dans le jeu des décideurs.

Aujourd'hui, plus de 30 % de tous les terminaux connectés aux réseaux d'entreprise sont des appareils IoT, sans compter les périphériques mobiles. Il va sans dire que cette progression est appelée à se poursuivre. Selon un rapport Gartner, le nombre de terminaux IoT devrait atteindre 5,81 milliards cette année.[1]

Sources :

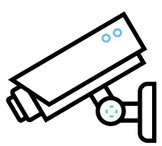
1 – Gartner: Scenarios for the IoT Marketplace, 2019
2, 3, 4 – 451 Research's Voice of the Enterprise: Internet of Things, Budgets and Outlook, 2019

46 %
Entreprises exploitant déjà l'IoT (y compris pour des projets pilotes payants)[2]

23 %
Entreprises en cours de preuve de concept (PoC) IoT[3]

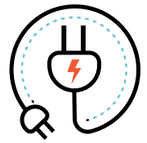
18 %
Entreprises prévoyant de déployer l'IoT au cours des deux prochaines années[4]

SECTEURS D'ACTIVITÉ À PLUS FORTE UTILISATION EN 2020



SÉCURITÉ PHYSIQUE

1,09 Md
appareils IoT en 2020



FOURNISSEURS D'ÉNERGIE

1,37 Md
appareils IoT en 2020

SECTEURS D'ACTIVITÉ À PLUS FORTE CROISSANCE EN 2020

42 % Domotique

31 % Automobile

29 % Santé

Les opportunités de transition vers des modèles économiques orientés OT et IoT sont énormes. Mais pour en concrétiser tous les avantages, les entreprises ont besoin d'une sécurité de pointe.

Qui dit croissance, dit nouveaux défis de sécurité

La prolifération des appareils IoT en entreprise apporte avec elle son lot de problématiques, en particulier pour les équipes de sécurité.

Aujourd'hui, les équipes de sécurité ne sont plus seulement en charge de protéger les terminaux informatiques connectés au réseau de leur entreprise. L'avènement de l'IoT les oblige désormais à faire face aux défis émanant de la multiplication d'objets connectés à leur réseau central, mais échappant à tout contrôle.

Problématiques de sécurité propres à l'IoT en entreprise

INVENTAIRE

Manque de visibilité sur les appareils IoT reliés au réseau et absence d'outils pour suivre les appareils nouvellement connectés

VOLUME DE DONNÉES

Gestion de vastes quantités de données issues d'appareils IoT gérés et non gérés

DIVERSITÉ

Appareils IoT aux formats et fonctions infiniment variés

MENACES

Absence de sécurité intégrée à des systèmes d'exploitation sur lesquels il est difficile, voire impossible d'appliquer des correctifs

RESPONSABILITÉ

Nouveaux risques liés à une gestion disparate des appareils IoT par différentes équipes

OPÉRATIONS

Difficulté pour la fonction IT d'intégrer leurs appareils IoT critiques à leur système de sécurité centralisé

Les solutions actuelles n'ont pas la réponse

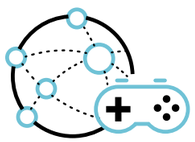
Les mécanismes de sécurité traditionnels se révèlent souvent inefficaces et inadaptés face aux enjeux de la sécurité IoT.

Un nombre croissant d'appareils IoT quasiment invisibles deviennent des composants incontournables des réseaux d'entreprise. Moniteurs de débit, caméras de surveillance, capteurs de luminosité en intérieur et extérieur, téléphones IP, terminaux de point de vente, technologies pour salles de conférence… les dispositifs OT et IoT sont partout sur le réseau, augmentant considérablement la surface d'attaque d'une organisation. Or, les défenses périmétriques en place ne sont pas suffisamment équipées pour relever un tel défi.

Les solutions actuelles ne sont pas à la hauteur

Évaluation des vulnérabilités

Compte tenu de la diversité des matériels, logiciels et protocoles de communication impliqués, une évaluation des vulnérabilités est par essence beaucoup plus complexe pour les appareils IoT. Bien qu'utile dans une certaine mesure pour identifier les failles potentielles, elle n'apporte pas réellement de solution au problème de sécurité.



Contrôle des accès au réseau (NAC)

Les solutions et méthodologies NAC ne passent tout simplement pas à l'échelle de l'IoT. Dans le contexte de menaces actuel, elles ne fournissent pas le niveau de sophistication nécessaire à une identification et une sécurisation adéquates des appareils IoT. En fait, elles peuvent tout juste être exploitées une fois les problèmes identifiés.

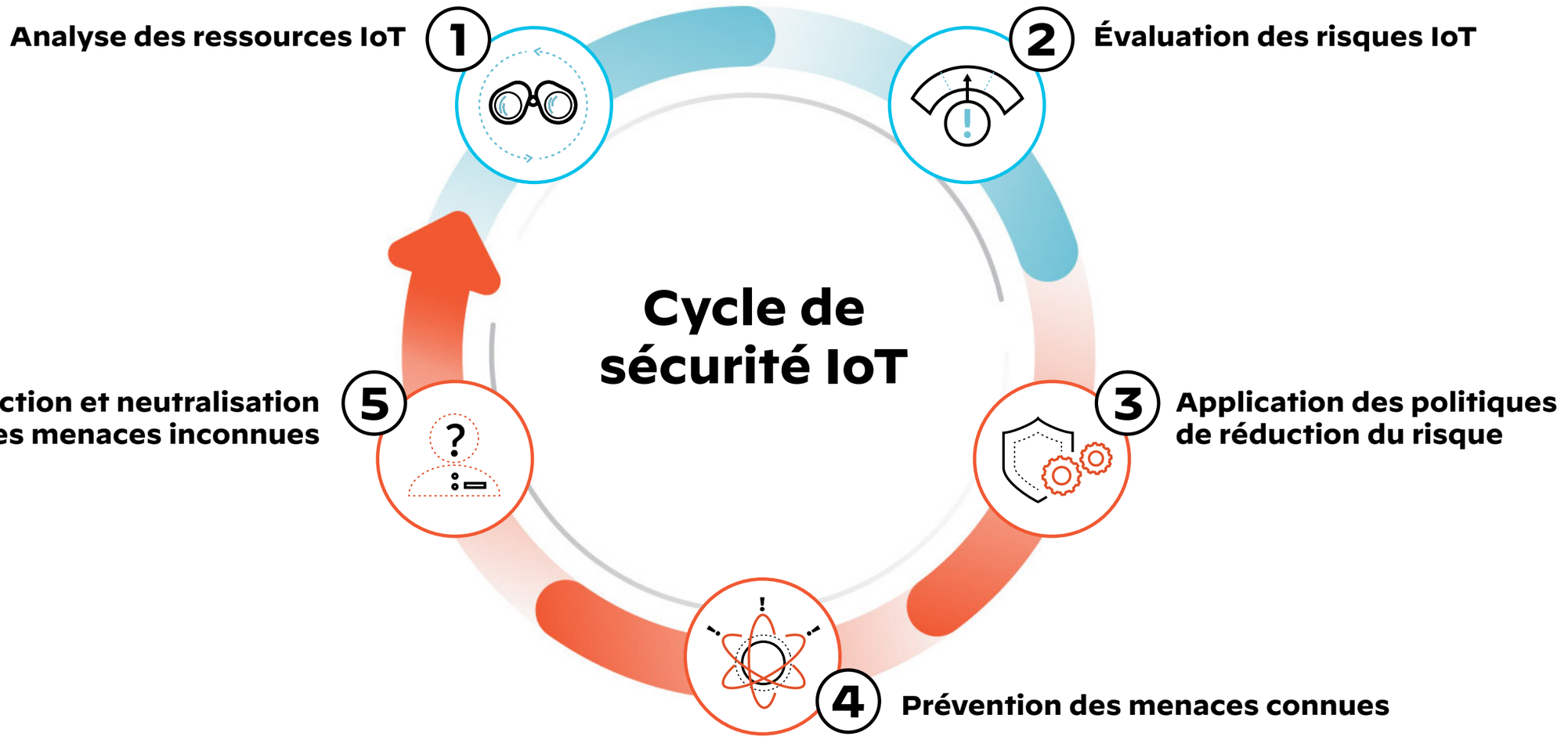
Solutions spécialisées de sécurité IoT

Implémentation de capteurs à usage unique, intégration aux systèmes existants, prise en main difficile… ces solutions exigent trop d'efforts de la part des équipes de sécurité.

Pour renforcer leur stratégie, les RSSI doivent envisager une approche basée sur le cycle de la sécurité IoT.

Sécurité IoT : les avantages d'une approche cyclique

La protection des équipements OT et IoT nécessite d'adopter une approche basée sur le cycle de sécurité. Dans l'idéal, votre solution devra intégrer toutes les étapes du cycle de la sécurité IoT – de la détection des appareils et des risques associés jusqu'aux mesures de réponse aux menaces connues et inconnues.



L'adoption d'une approche cyclique de la sécurité IoT passe par une solution reposant sur *5 piliers*.

Fonctionnalités indispensables d'une solution de sécurité IoT

1

Visibilité complète sur tous les appareils IoT connectés au réseau de l'entreprise

Avant de décider d'une stratégie de sécurité, vous devez disposer d'une visibilité complète sur votre surface d'attaque IoT. C'est la première étape du cycle de sécurité IoT. Pour **dresser un inventaire complet de votre parc IoT**, il vous faut un outil de détection fiable, capable de détecter le nombre exact d'appareils connectés à votre réseau : ceux dont vous avez connaissance, ceux dont vous ignorez l'existence et ceux dont vous avez oublié la présence. Ce n'est qu'à cette condition que vous pourrez dresser un inventaire actualisé de toutes les ressources IoT. La solution doit également être capable d'identifier les principales caractéristiques des appareils détectés pour en dresser un profil détaillé.

Misez sur une solution qui :

- ✓ Exploite des capteurs polyvalents intégrables à l'infrastructure existante
- ✓ Détecte les caractéristiques essentielles des appareils IoT (marque, modèle, système d'exploitation, firmware, ports, applications, VLAN, sous-réseau, présence, état du logiciel antivirus, etc.)
- ✓ Détecte des appareils jamais rencontrés auparavant, sans intervention humaine ni mise à jour constante des signatures
- ✓ Repère les appareils nouvellement connectés en quelques minutes
- ✓ Identifie au moins 80 % des appareils sur les segments visibles dans un délai de 48 heures
- ✓ Distingue les appareils IoT non gérés des ressources IT gérées
- ✓ Comptabilise les équipements IT pour permettre aux équipes de sécurité des postes de travail d'identifier les équipements IT non gérés

Fonctionnalités indispensables d'une solution de sécurité IoT

2

Surveillance proactive des appareils IoT pour une détection continue des comportements à risque

Pour une **évaluation fiable des risques IoT,** votre solution doit pouvoir surveiller les objets connectés de manière active et continue. Une surveillance, un reporting et des alertes en temps réel sont essentiels à la gestion des risques de l'IoT. Or, les solutions traditionnelles de sécurité des terminaux sont incapables de protéger les ressources IoT dans la mesure où elles exigent l'installation d'agents logiciels, chose pour laquelle les objets connectés n'ont pas été conçus. Heureusement, il existe une meilleure approche qui consiste à déployer une solution de surveillance temps réel qui analyse en permanence le comportement de tous les appareils IoT connectés au réseau. Elle vous permet ainsi d'effectuer une segmentation contextuelle du réseau, garante d'un contrôle granulaire des mouvements latéraux du trafic entre les équipements IT et IoT, ainsi que leurs workloads.

Misez sur une solution qui :

- ✓ S'intègre à plusieurs flux de menaces pour catégoriser avec précision les vulnérabilités des ressources IoT inventoriées
- ✓ Détecte et signale les comportements anormaux des appareils IoT susceptibles de représenter un risque
- ✓ Suit l'évolution des risques associés aux appareils IoT et en conserve un historique complet à des fins de conformité
- ✓ Calcule les scores de risque sur les appareils IoT et les catégories d'appareils à signaler
- ✓ S'intègre aux systèmes de gestion des vulnérabilités pour centraliser la gestion des risques IoT
- ✓ S'intègre aux appareils IoT tiers pour fournir des informations aux équipes de sécurité

Fonctionnalités indispensables d'une solution de sécurité IoT

3

Recommandation et application automatisées de politiques de sécurité basées sur les risques

Votre solution doit être facile à déployer et ne nécessiter aucune infrastructure ou investissement supplémentaire de votre part. Pour une sécurité complète et intégrée, privilégiez une solution capable de fonctionner en parfaite synergie avec vos pare-feu existants pour **recommander automatiquement et appliquer nativement des politiques de sécurité** selon le niveau de risque et les comportements suspects détectés sur vos appareils IoT.

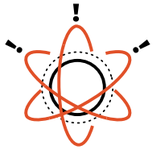
Sachant qu'en matière de sécurité, la confiance n'est ni plus ni moins qu'un aveu d'impuissance, votre solution IoT devra s'aligner directement sur votre modèle Zero Trust pour appliquer un contrôle d'accès basé sur le principe du moindre privilège. Cette approche réduira considérablement les possibilités d'accès non autorisé à vos ressources IoT critiques, tant pour les acteurs internes qu'externes.

Misez sur une solution qui :

- ✓ Convertit automatiquement les comportements des appareils IoT en politiques afin de n'autoriser que les comportements de confiance
- ✓ Permet d'appliquer des politiques multi-niveaux pour un groupe d'appareils
- ✓ Prend en charge les listes d'autorisation et les listes de blocage
- ✓ Assure le traçage des appareils et applications pour appliquer les politiques indépendamment de leur emplacement sur le réseau
- ✓ Actualise automatiquement les politiques définies pour limiter les mises à jour manuelles à chaque changement

Fonctionnalités indispensables d'une solution de sécurité IoT

4



Prévention rapide contre les menaces connues

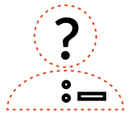
L'hétérogénéité des parcs d'appareils IoT crée un environnement réseau hautement distribué comportant de nombreux points de compromission. Pour une neutralisation rapide des menaces, la quatrième étape du cycle de sécurité IoT nécessite des **données de détection directement exploitables pour prévenir les menaces connues** ciblant ces appareils. Pour bloquer les menaces IoT avancées, optez pour une solution de prévention qui s'appuie sur des signatures basées sur les payloads. Vous bénéficierez ainsi d'une sécurité constamment à jour pour réagir en temps réel aux vulnérabilités du réseau et des appareils IoT. Mais aussi et surtout, vous bloquerez automatiquement les menaces connues pour réduire le volume d'alertes à traiter par vos équipes de sécurité.

Misez sur une solution qui :

- ✓ Active les protections en fonction du niveau de menace observé pour le groupe d'appareils IoT concernés
- ✓ Détecte et neutralise les menaces IoT connues (malwares, spywares, exploits, etc.)
- ✓ Bloque les attaques IoT provenant d'URL et de sites web malveillants
- ✓ Prévient les attaques IoT qui exploitent le DNS pour voler des données et établir des communications CnC
- ✓ Stoppe les menaces IoT inconnues déclenchées par des payloads

Fonctionnalités indispensables d'une solution de sécurité IoT

5



Détection et neutralisation rapides des menaces inconnues

Pour **détecter et prévenir des menaces totalement inconnues**, les approches traditionnelles isolent les données de Threat Intelligence reçues et générées par chaque organisation, ce qui crée des silos et réduit les capacités de prévention. La dernière étape du cycle de sécurité IoT exige une nouvelle approche basée sur un moteur de Threat Intelligence collective intégrant une analyse anti-malware en temps réel et une protection contre les attaques zero-day. L'exploitation d'un pool de données issu d'une communauté mondiale d'utilisateurs met la force du collectif au service de la sécurité. Votre équipe de sécurité gagne ainsi un temps précieux grâce à une série d'informations (identité des appareils, scores de risque, données de vulnérabilité, analyses comportementales, etc.) qui lui permettent d'investiguer rapidement des menaces jusqu'alors inconnues et ciblées sur votre environnement IoT. Cette dernière étape permet également de détecter les menaces passées entre les mailles du filet lors des phases précédentes et enclenche un processus cyclique d'amélioration continue.

Misez sur une solution qui :

- ✓ Détecte les comportements anormaux des appareils à différents niveaux : catégorie, fournisseur/modèle, instance
- ✓ S'appuie sur une Threat Intelligence collective, le machine learning et la modélisation des menaces pour détecter les attaques inconnues et fournir des notifications ou des mesures proactives
- ✓ S'intègre aux solutions d'orchestration, automatisation et réponse aux incidents de sécurité (SOAR) pour un processus de réponse basé sur des playbooks
- ✓ Rationalise les travaux des chercheurs pour détecter toutes les nouvelles menaces de sécurité IoT

Solution IoT Security de Palo Alto Networks

Présente sur les cinq fronts

Notre solution IoT Security associe le machine learning (ML) à la fonctionnalité brevetée App-ID de nos pare-feu nouvelle génération pour une visibilité totale sur vos équipements OT et IoT, créant ainsi une base de référence précise de leurs comportements normaux. IoT Security permet aux équipes de sécurité de prévenir les menaces de manière proactive, surveiller les risques pour chaque appareil, détecter les anomalies, et recommander puis appliquer des politiques de sécurité.

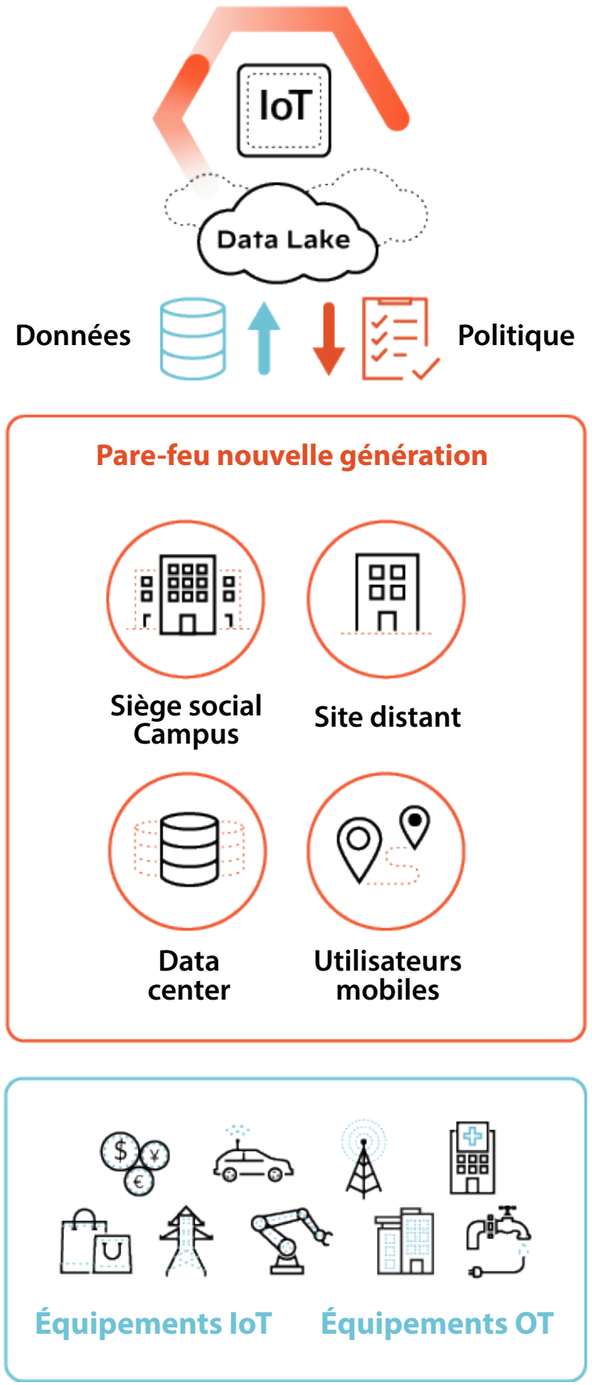
Basée sur un modèle d'abonnement cloud, IoT Security est simple à déployer et ne nécessite aucun capteur à usage unique ou investissement en infrastructure. Il vous suffit d'activer le service sur votre pare-feu nouvelle génération Palo Alto Networks piloté par ML pour étendre vos systèmes de protection avancée à vos ressources OT et IoT jusqu'alors non gérées.

Si vous n'êtes pas client de Palo Alto Networks, notre pare-feu nouvelle génération piloté par ML sert également de capteur et de point de contrôle pour IoT Security à un prix compétitif pour vos produits silotés de sécurité IoT installés là où vous ne disposez pas de pare-feu.

En combinaison avec les fonctionnalités App-ID et User-ID déjà intégrées à notre pare-feu nouvelle génération piloté par ML, notre solution applique automatiquement des politiques de réduction des risques – y compris une **« nouvelle »** structure de politiques basée sur Device ID – visant à n'autoriser que les comportements fiables des appareils IoT sur le réseau.

Cette association unique de fonctionnalités permet une segmentation contextuelle du réseau pour minimiser l'exposition aux risques résultant de déplacements latéraux. Enfin, IoT Security intègre nos principaux services de prévention des menaces pour protéger vos appareils IoT des menaces connues et inconnues.

Misez sur Palo Alto Networks pour sécuriser vos équipements OT et IoT non gérés !

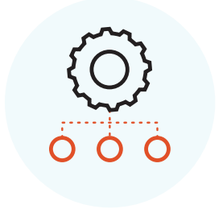


Donnez l'avantage à votre équipe de sécurité…

… sans avoir à former de nouvelles recrues, déployer une nouvelle infrastructure ou modifier les processus opérationnels existants

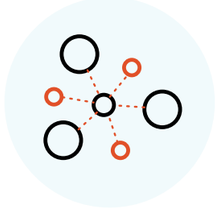
Visibilité et protection sans précédent

- Détection des appareils IoT basée sur le ML
- Évaluation automatique des risques
- Application native des politiques de sécurité
- Segmentation contextualisée du réseau



Déploiement simple et formats flexibles

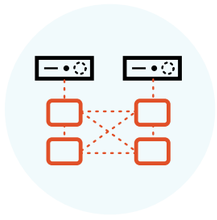
- Pare-feu matériels PA-Series
- Pare-feu virtuels VM-Series
- SASE Prisma Access en mode cloud



Couverture d'une gamme complète d'équipements OT et IoT

- Appareils IoT d'entreprise et grand public
- Équipements OT critiques
- Systèmes d'ancienne génération non gérés

- **Déployez des services de prévention des menaces avancées pour renforcer votre sécurité**



- **Misez sur une infrastructure cloud élastique pour évoluer au rythme de croissance de votre entreprise**

- **Exploitez un ensemble complet d'intégrations avec des produits et solutions tiers pour l'inventaire, la journalisation et le contrôle des ressources**

Pensez sécurité de l'IoT.
Pensez Palo Alto Networks.

Chez Palo Alto Networks, nous avons pour mission de protéger les modes de vie numériques contre les cyberattaques. Nous sommes présents en première ligne pour assurer la sécurité de dizaines de milliers d'entreprises sur le cloud, les réseaux et les terminaux. Intelligence artificielle, analytique, automatisation, orchestration… nous innovons sur tous les fronts pour vous aider à relever les défis de sécurité les plus sensibles.

Fondée en 2005, Palo Alto Networks est basée à Santa Clara, en Californie, et accompagne des clients dans le monde entier.

Pour de plus amples informations, rendez-vous sur :
www.paloaltonetworks.fr

Témoignage client

"Quelques heures après le déploiement, nous avons détecté et identifié des milliers d'appareils, dont certains nous ont fourni des informations critiques qui ont permis de mettre en œuvre des mesures préventives."

BayCare Medical Group

Envie d'en savoir plus ? **Visionnez la démo produit**

www.paloaltonetworks.fr

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

+31 20 888 1883