Sécurité IoMT :
le guide du RSSI de la santé

Une approche en 6 étapes de la gestion des workflows pour protéger tous vos terminaux

Sommaire

1. L'essor fulgurant de l'Internet des objets médicaux (IoMT)...3
2. La sécurité comme principal frein à l'adoption 4
3. Établissements de santé :
   état des lieux du parc IT, IoT et IoMT.....5
4. Protection des objets médicaux :
   les lacunes des solutions classiques.....6
5. Appareils médicaux : la nécessité d'une gestion de A à Z 7
6. Gestion et sécurisation des workflows
   de terminaux et appareils médicaux :
   une implémentation en 6 étapes..... 8
7. IoT Security par Palo Alto Networks
   pour les acteurs de la santé 15
8. Synthèse des avantages 17

L'essor fulgurant de l'Internet des objets médicaux (IoMT)

L'IoT donne un nouveau souffle aux établissements de santé. Et la pandémie n'a fait qu'accentuer la tendance.

Pour les acteurs de la santé, les objets connectés changent véritablement la donne. Depuis la crise sanitaire mondiale, la demande en appareils IoT n'a jamais été aussi forte dans des domaines comme le suivi médical à distance et le traçage numérique. Mais même avant, l'adoption de l'IoT connaissait un essor considérable.

Cela fait en effet près de 10 ans que les objets connectés réinventent le concept même des prestations de santé. Suivi et diagnostics à distance, gestion des soins d'hygiène, observation et prise en charge des patients, maintenance prédictive des appareils médicaux… les cas d'usage des objets connectés se sont multipliés dans le secteur de la santé.

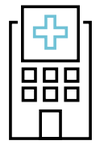
Pour preuve, selon une enquête Gartner publiée en janvier 2020, 86 % des établissements de santé sondés confirmaient l'implémentation d'une solution IoT dans la plupart de leurs services[1]. Par ailleurs, une étude Omdia a estimé à plus de 250 millions le nombre d'appareils médicaux lancés sur le marché mondial en 2020, un chiffre qui pourrait aisément atteindre 750 millions d'ici 2025[2].

48 %

des établissements de santé exploitent l'IoT à grande échelle (multiples projets et cas d'usage)[3]

31 %

des établissements de santé exploitent l'IoT pour un seul cas d'usage (projets et cas d'usage uniques)[4]

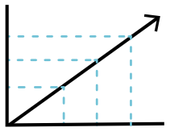


21 Mds

Dépenses IoT par les prestataires de santé en 2019[5]

54 Mds

Dépenses IoT par les prestataires de santé en 2029[6]



10 %

Croissance annuelle[7]

La santé s'approprie l'IoT à un rythme effréné. Mais le secteur est-il prêt à relever les défis majeurs de sécurité que soulèvent tous ces objets connectés ?

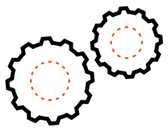
Sources :

1, 3-4 Gartner Survey Analysis: Healthcare Provider IoT Adoption Is Becoming Mainstream, 2020
2 Omdia IoT Devices Intelligence, 2020
5-7 Gartner Forecast Analysis, Healthcare Providers IoT Endpoint Electronics and Communications Revenue, Worldwide, 2020

La sécurité comme principal frein à l'adoption

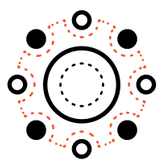
Pour les cyberattaquants, les appareils médicaux connectés offrent une porte particulièrement facile à enfoncer. D'où la nécessité d'une nouvelle approche de la sécurité.

Si l'Internet des objets révolutionne indéniablement les prestations de santé, il apporte également son lot de problématiques. Parmi elles, la sécurité demeure le plus grand frein à l'adoption des objets connectés. De fait, la santé est devenue une cible stratégique pour des cybercriminels attirés par les données sensibles que les acteurs de ce secteur brassent chaque jour. Dans leur ligne de mire : les millions d'appareils IoMT qui collectent et stockent ces données. Connus pour être difficiles à sécuriser, ces équipements posent des risques de sécurité majeurs, à l'instar des objets connectés génériques.



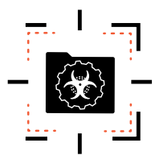
SYSTÈMES D'EXPLOITATION D'ANCIENNE GÉNÉRATION

Les appareils IoMT fonctionnent généralement sous des systèmes d'exploitation obsolètes et n'ont pas tous été initialement conçus pour être connectés à Internet. D'où le manque de prévention ou de contrôles intégrés.



RÉSEAUX NON SEGMENTÉS

Dans la plupart des centres hospitaliers, les réseaux ne sont pas segmentés. Les attaquants ont donc le champ libre pour contaminer des équipements IT puis se déplacer latéralement dans l'environnement pour compromettre des objets connectés, et vice-versa.



VULNÉRABILITÉS PRÉ-EXISTANTES

Les équipements médicaux sont souvent livrés avec des vulnérabilités déjà présentes qui sont difficiles à corriger. Et comme leur durée de vie tend à être longue, beaucoup ne font l'objet d'aucun rappel ou remplacement régulier.

En 2020, les établissements de santé ont rapporté 616 compromissions de données portant sur 500 dossiers ou plus, soit une compromission totale de 28 756 445 dossiers médicaux[8].

Le saviez-vous ?

41 % des attaques exploitent des vulnérabilités sur des objets connectés

57 % des attaques de sévérité moyenne à grave impliquent des appareils IoMT

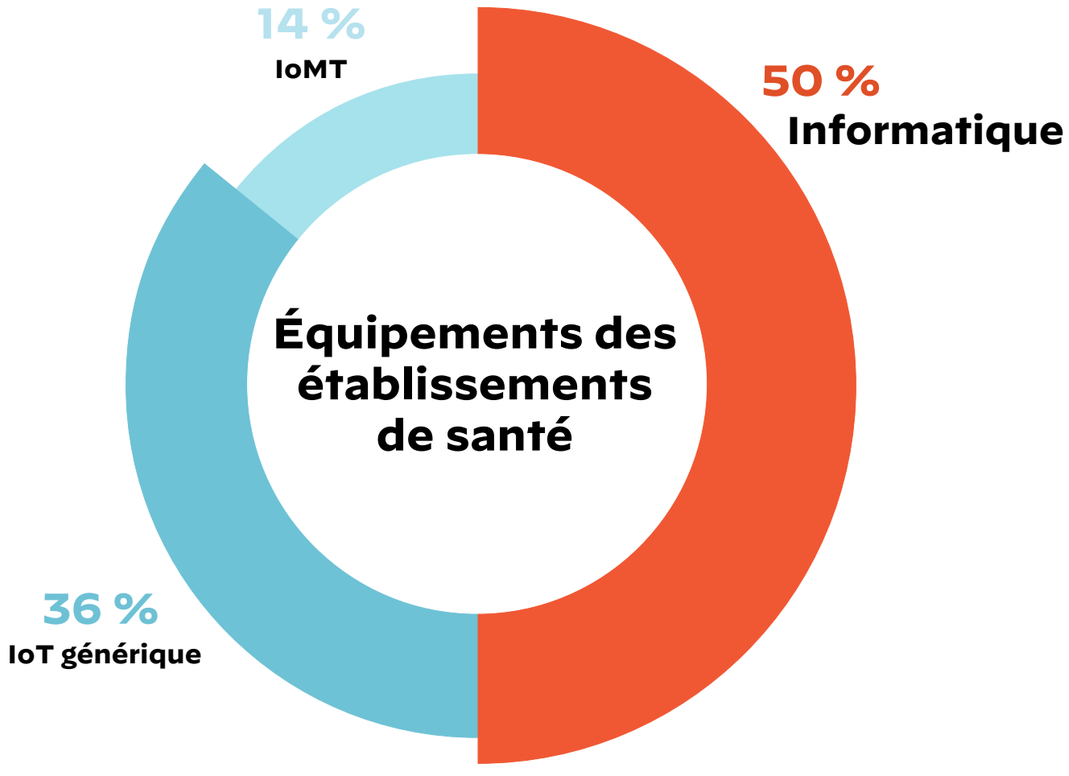
72 % des VLAN d'établissements de santé contiennent un mix d'équipements IoT/IoMT et informatiques

83 % des appareils d'imagerie médicale fonctionnent sous des systèmes d'exploitation en fin de support, soit un bond de 56 % par rapport à 2018

Sources :
Rapport Unit 42 sur les menaces IoT (édition 2020)
8 HIP Journal 2021

Établissements de santé : état des lieux du parc IT, IoT et IoMT

Pour les cyberattaquants, les appareils médicaux connectés offrent une porte particulièrement facile à enfoncer. D'où la nécessité d'une nouvelle approche de la sécurité.



50 % de tous les appareils dans les établissements de santé sont non gérés

Source :
Rapport Zingbox sur les menaces dans le secteur médical (2019)
Rapport Unit 42 sur les menaces IoT (édition 2020)

Appareils IoMT les plus déployés

46 %
Pompes à perfusion

19 %
Systèmes d'imagerie médicale

17 %
Systèmes de suivi des patients

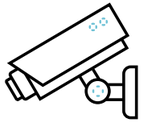
Appareils médicaux connectés les plus à risque

51 %
Systèmes d'imagerie médicale

26 %
Systèmes de suivi des patients

9 %
Passerelles pour appareils médicaux

Appareils IoT génériques les plus à risque et présents dans toutes les entreprises et établissements de santé



33 %
Caméras de sécurité

24 %
Imprimantes

10 %
Consoles de jeux vidéo

Protection des objets médicaux : les lacunes des solutions classiques

Les mécanismes de sécurité traditionnels ne suffisent plus pour protéger la multiplicité des appareils. Ils vont même jusqu'à alourdir la charge de travail des équipes de sécurité, d'infrastructure et médicales.

Détournement d'appareils médicaux, vol de données d'assurance-maladie et d'informations patient confidentielles, extorsion de dossiers médicaux, dissimulation de trafic réseau, perturbation des prestations de soins, verrouillage par ransomware de tous les systèmes informatiques… toute vulnérabilité sur l'IoMT peut provoquer un déferlement d'attaques. Aujourd'hui, si le marché foisonne de nouvelles solutions de sécurité IoT, rares sont celles qui offrent une stratégie de sécurité suffisamment complète pour protéger la totalité des appareils médicaux sur votre réseau.

Faiblesses des solutions actuelles de protection IoT et IoMT

SOLUTIONS BASÉES SUR DES SIGNATURES

Manquent de précision et de puissance pour répondre à la prolifération massive des nouveaux appareils ou à la variété des équipements qui débarquent chaque jour sur le marché.

APPROCHES REPOSANT UNIQUEMENT SUR DES ALERTES

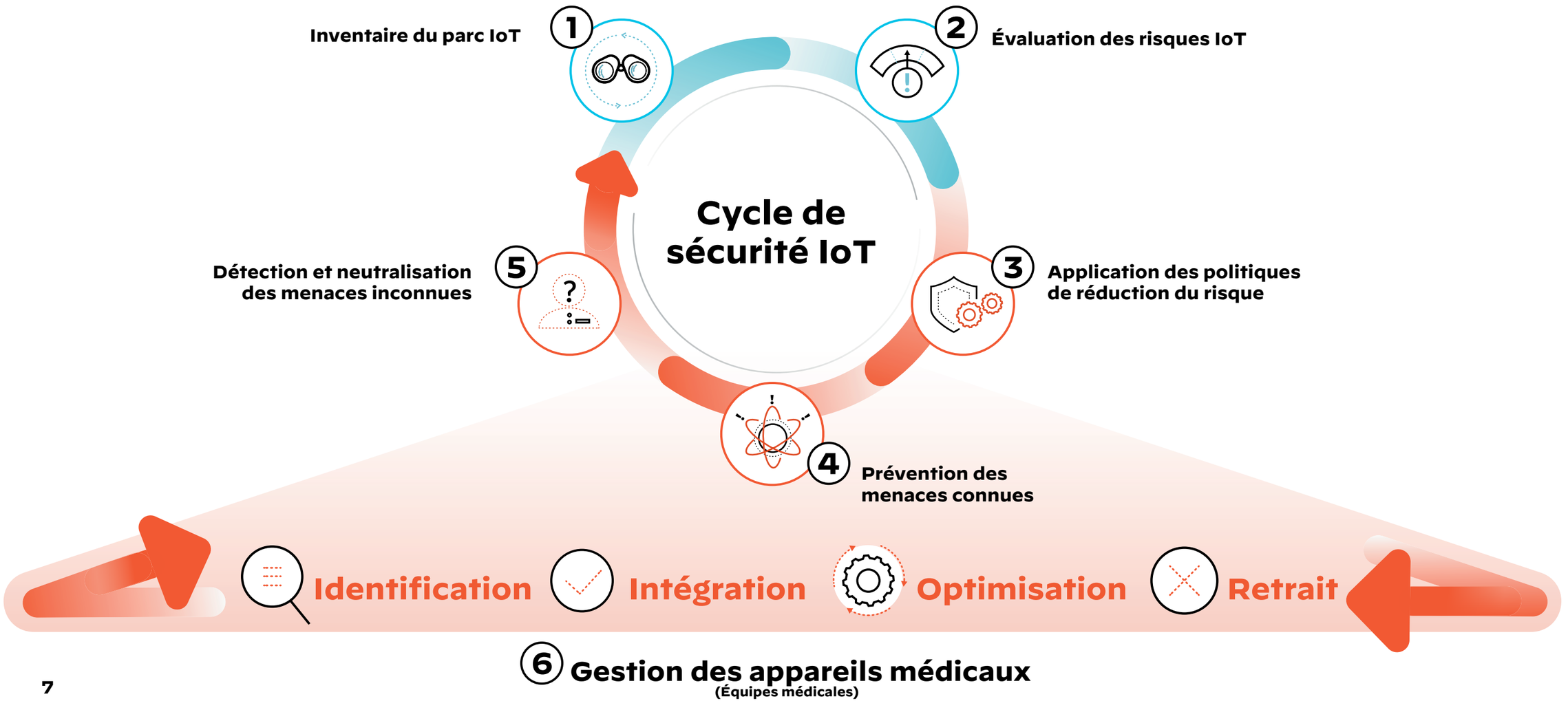
Incapables de recommander des politiques ou de les appliquer, et encore moins de prévenir les menaces connues ou inconnues sur les appareils IoT ou IoMT.

SOLUTIONS SPÉCIALISÉES

Compliquent fortement les déploiements, car elles nécessitent de modifier l'infrastructure réseau ou de déployer de nouveaux capteurs réseau pour traiter le trafic et identifier les appareils.

Appareils médicaux : la nécessité d'une gestion et d'une sécurisation de A à Z

Pour réduire les risques aussi bien pour le réseau que pour les patients, l'IoMT doit s'inscrire dans une approche de gestion intégrale des appareils médicaux. Idéalement, cette approche délestera les équipes médicales et de sécurité réseau du poids des opérations quotidiennes qui consistent à sécuriser et à gérer manuellement ces appareils.



À l'heure où les surfaces d'attaque s'étendent et où la sophistication des modes opératoires atteint de nouveaux sommets, il devient urgent d'évoluer vers une sécurité IoMT à la hauteur des dangers.

Gestion et sécurisation des workflows de terminaux et d'appareils médicaux : l'approche en 6 étapes

1

Obtenez une visibilité à 360° des appareils IoMT dans votre établissement de santé

Une visibilité complète sur votre surface d'attaque permet d'établir un état des lieux de votre écosystème de sécurité. C'est la première étape du cycle de sécurité IoMT. Grâce à cet inventaire complet des appareils en place, tous les acteurs d'un établissement de santé (fonctions IT, sécurité, médicales, etc.) bénéficient d'une vue complète de leurs ressources IoMT. Un inventaire à jour permet de recenser tous les appareils connus et inconnus, mais aussi ceux qui ont été oubliés. Pendant cette phase de découverte, la solution de sécurité IoMT doit également être capable d'identifier les principales caractéristiques des appareils détectés pour en dresser un profil détaillé.

Fonctionnalités indispensables d'une solution de sécurité IoMT :

- ✓ Identifie au moins 90 % des appareils sur les segments visibles dans un délai de 48 heures
- ✓ Détecte les tout nouveaux appareils grâce à une catégorisation par ML basée sur différents critères (constructeur, marque, modèle, type, système d'exploitation, firmware, emplacement, sous-réseau, score de risque, type d'information de santé protégée, informations MDS2, etc.)
- ✓ Repère les appareils nouvellement connectés en quelques minutes, et non plus en plusieurs heures voire plusieurs semaines
- ✓ Distingue les appareils IoT et IoMT non gérés des ressources IT gérées
- ✓ Comptabilise tous les équipements informatiques pour permettre aux équipes IT et de sécurité d'identifier les équipements non gérés
- ✓ Met à jour automatiquement vos solutions de gestion des ressources (CMMS, ITSM, CMDB, etc.) avec une mine d'informations sur les appareils IoMT
- ✓ Exploite des capteurs polyvalents intégrables à l'infrastructure existante

2

Réduisez les risques par une approche continuelle et proactive de la surveillance et de l'évaluation des vulnérabilités IoMT

Lors de la phase d'**évaluation des risques** du cycle de sécurité IoT, il est capital d'établir un suivi actif et continu des objets médicaux connectés. Une surveillance des risques, un reporting et des alertes en temps réel sont essentiels à une réduction efficace des risques de l'IoMT et de la surface d'attaque. D'où l'insuffisance des solutions basées sur des signatures, dont le manque de précision et de rapidité limite la protection des ressources. Grâce à une évaluation précise des risques dans votre cycle de sécurité IoT, vos équipes de sécurité peuvent surveiller les appareils et inspecter leurs schémas de trafic en continu. L'objectif : segmenter les contrôles d'accès réseau (NAC) de manière proactive et réduire ainsi la surface d'attaque. Et pour tuer dans l'œuf toute tentative de mouvement latéral, les équipes IT peuvent également microsegmenter le réseau par types et classes d'appareils (IoMT, IoT ou IT).

Fonctionnalités indispensables d'une solution de sécurité IoMT :

- S'intègre à plusieurs flux CTI (CVE, MDS2, RSSI, etc.) pour catégoriser avec précision les vulnérabilités des ressources IoMT inventoriées
- Inclut les spécifications MDS2 (Manufacturer Disclosure Statement for Medical Device Security) telles que les fonctions antivirus, les données médicales sensibles, les rappels de produits par les autorités sanitaires et les avis de publication de correctifs
- Détecte et signale en temps réel les anomalies sur les appareils IoMT pouvant impacter les scores de risques
- Calcule les scores de risque sur les appareils et les catégories d'appareils IoT
- Suit l'évolution des scores de risque et en conserve un historique complet à des fins de conformité
- S'intègre aux systèmes de gestion des vulnérabilités et aux appareils de différentes marques pour fournir des informations aux équipes de sécurité par le biais d'une gestion centralisée des risques IoMT

3

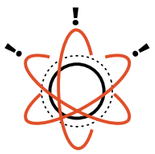
Optez pour une recommandation et une application automatisées de politiques de sécurité basées sur les risques

Une solution de sécurité IoMT dite « simple » ne doit requérir aucune infrastructure ni aucun investissement supplémentaire. Pour une sécurité complète et intégrée, elle doit, au contraire, pouvoir fonctionner en parfaite synergie avec vos pare-feu existants afin de **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 IoMT 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.

Fonctionnalités indispensables d'une solution de sécurité IoMT :

- Définit des politiques de sécurité sur la base des comportements normaux des appareils IoMT afin de bloquer tout écart
- Automatise l'application de politiques dès l'identification des appareils et applications
- 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
- S'intègre au NAC et diffuse automatiquement les informations des appareils IoT pour appliquer les contrôles sur les équipements et opérer une segmentation contextuelle

4



Prévenez rapidement les menaces connues

L'hétérogénéité des parcs d'appareils IoMT 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 IoMT. Mais aussi et surtout, vous bloquerez automatiquement les menaces connues pour réduire le volume d'alertes à traiter par vos équipes de sécurité.

Fonctionnalités indispensables d'une solution de sécurité IoMT :

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

5

Détectez les menaces inconnues et réagissez sans délai

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 SSI 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 IoMT. 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.

Fonctionnalités indispensables d'une solution de sécurité IoMT :

- 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 au SIEM et au SOAR à l'aide d'une approche simplifiée basée sur des playbooks pour orchestrer les réponses aux incidents et la prévention des menaces
- Aide les chercheurs en sécurité à détecter plus facilement toutes les nouvelles menaces IoT

6

Dotez les équipes cliniques et biomédicales d'une intelligence opérationnelle

Bien que la plupart des appareils médicaux demeurent sous-exploités en raison d'un surplus d'équipements, ceux-ci entraînent souvent des dépenses opérationnelles qui pourraient être économisées. En outre, ces appareils étant réglementés par les autorités sanitaires, toutes les mises à jour logicielles doivent être validées par le constructeur d'origine (OEM) pour garantir la sécurité de l'appareil en cas de changement. Les équipes médicales chargées de l'utilisation et de la gestion de ces appareils ont donc besoin d'informations métiers et opérationnelles pour réduire les lourdeurs liées à la planification des investissements et à la maintenance préventive. Mais elles doivent aussi être au fait des éventuels correctifs et mises à jour à appliquer sur les appareils. C'est là qu'une solution de sécurité IoT digne de ce nom doit entrer en jeu. Grâce aux informations opérationnelles qu'elle génère, les équipes peuvent **identifier** les appareils, les **rendre opérationnels**, **optimiser** leurs performances en fonction des données d'utilisation, et les **décommissionner** dans le respect des réglementations en vigueur.

Fonctionnalités indispensables d'une solution de sécurité IoMT :

- Suit et documente les statistiques d'utilisation de chacun des appareils pour orienter les décisions d'achat ou de remplacement des équipements
- Informe sur les pics d'utilisation pour prévoir la maintenance préventive et les mises à jour logicielles sans nuire à la planification des prestations médicales ou à l'expérience des patients
- Fournit des analyses de l'utilisation des appareils d'imagerie (membres habilités à l'utilisation, modes d'utilisation, etc.) pour garantir la proximité physique des appareils et de leurs utilisateurs
- Gère sans délai les avis des constructeurs, les rappels de produits et tout autre problème depuis une seule et même console, sans devoir passer par une investigation manuelle
- Actualise les systèmes d'inventaire pour maintenir une journalisation continue des appareils et informer tous les autres départements des appareils nouvellement intégrés et décommissionnés
- Protège les données patient par le suivi de l'utilisation et du stockage des données sur chaque appareil, ce qui facilite la mise en conformité HIPAA lors de l'intégration et du décommissionnement des appareils

IoT Security par Palo Alto Networks pour les acteurs de la santé

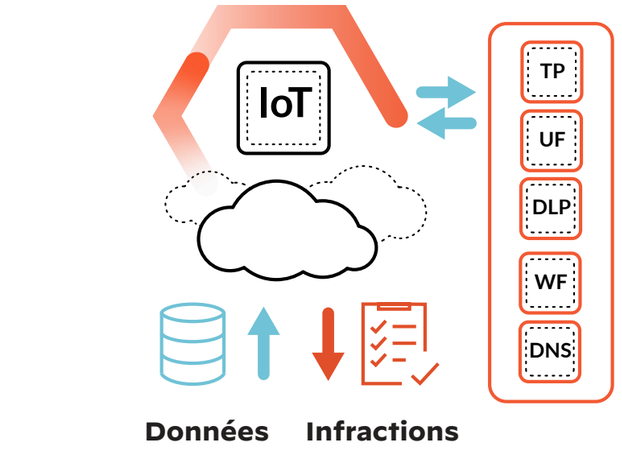
La solution de sécurité IoMT la plus complète du marché

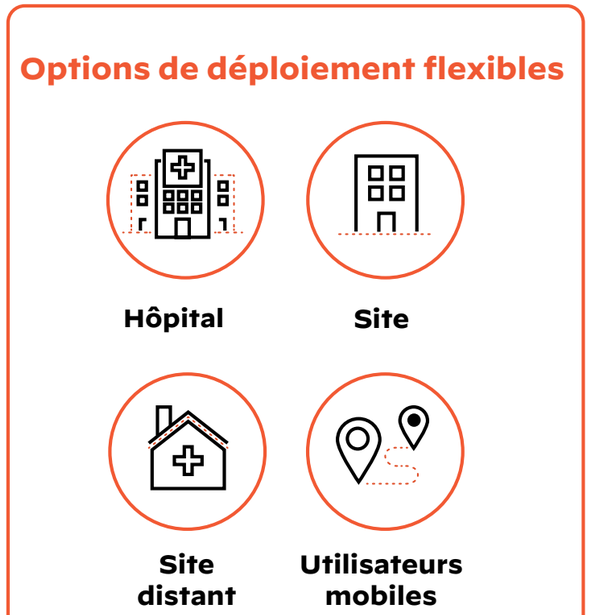
Palo Alto Networks IoT Security est la seule solution de sécurité des appareils médicaux à conjuguer visibilité, prévention et déclenchement des mesures de sécurité pilotés par ML, ainsi que des éclairages opérationnels depuis une seule et même plateforme.

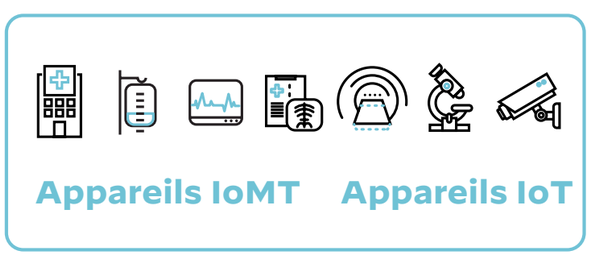
Découvrez tout ce qu'IoT Security peut faire pour vous.

- La seule solution à combiner **machine learning et Threat Intelligence collective** pour détecter rapidement et avec précision tous les appareils, même inconnus.
- La seule solution à offrir une **prévention intégrée.** À l'inverse de solutions basées uniquement sur des alertes, IoT Security prévient les menaces et empêche toute vulnérabilité de s'installer sur votre réseau pour protéger les appareils non gérés contre les risques connus/inconnus.
- IoT Security réduit également le coût des soins grâce à des **informations opérationnelles** destinées aux équipes médicales et à **l'application automatique des politiques, soit directement soit via des intégrations.** Résultat : moins de pression sur votre réseau comme sur vos équipes SecOps, avec en prime une meilleure disponibilité des appareils.
- Livré sur une seule et même plateforme, IoT Security **se déploie en toute simplicité** sans nécessiter aucune infrastructure supplémentaire.

Palo Alto Networks IoT Security est la seule solution du marché capable de maximiser le retour sur investissement (ROI) tout en optimisant l'expérience des patients. Au menu : une visibilité approfondie, des informations opérationnelles ciblées et une sécurité renforcée des appareils médicaux, le tout depuis une plateforme unique. **1 hôpital sur 5 aux États-Unis nous fait confiance !**







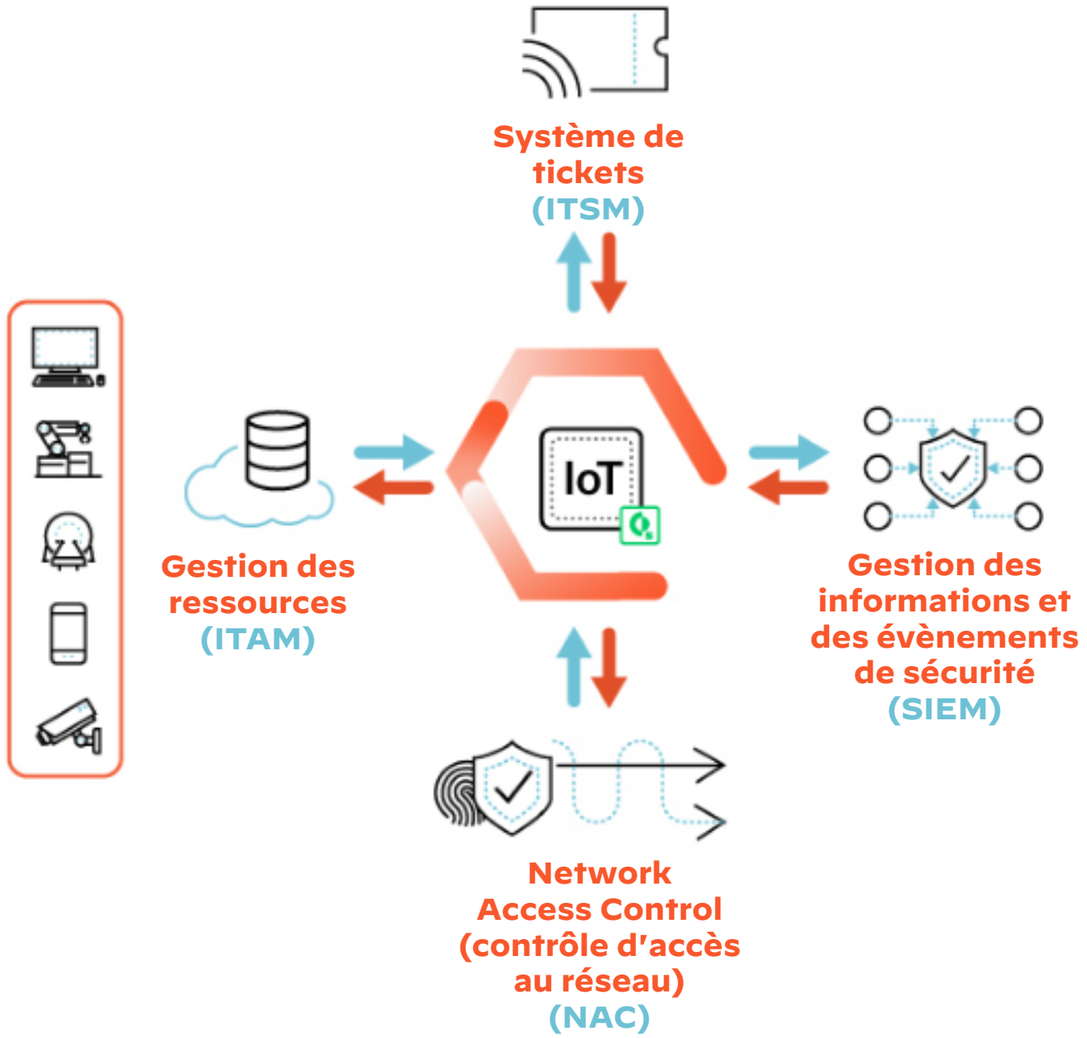
Intégration à des solutions tierces

Technologie XSOAR intégrée

Grâce à son intégration transparente à vos workflows existants, IoT Security évite les intégrations par API gourmandes en ressources, allégeant ainsi la pression sur l'infrastructure et la charge de travail des équipes de sécurité.

Bénéficiez d'intégrations natives à vos workflows informatiques et de sécurité existants pour renforcer vos pratiques et systèmes en place (ITSM, SIEM, NAC, etc.).

Pour votre équipe de sécurité, les avantages d'une orchestration modulaire, personnalisée et basée sur des playbooks sont multiples : gain d'efficacité opérationnelle, enrichissement des inventaires de ressources, intégration correcte des appareils IoMT, application des contrôles des appareils et automatisation des réponses aux incidents, le tout sans avoir à développer de nouvelles intégrations.

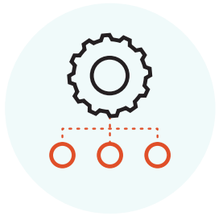


Exploitez tout le potentiel de votre équipe de sécurité IT

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

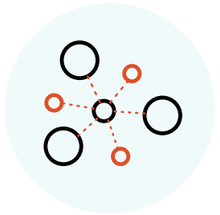
Visibilité et protection sans précédent

- 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

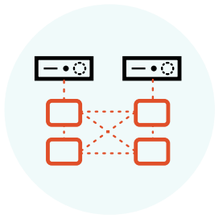
- Pare-feu matériels
- Pare-feu logiciels
- Pare-feu cloud



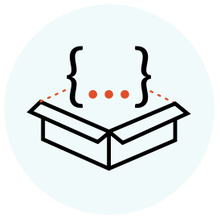
Couverture d'une gamme complète d'équipements IoT, IoMT et IT

- Appareils IoMT non gérés
- Appareils IoT non gérés
- Appareils IT gérés

Exploitation des fonctions de prévention d'autres services de sécurité



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



Automatisez les workflows à l'aide d'intégrations basées sur des playbooks

Pensez sécurité IoMT.

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 plus d'informations, rendez-vous sur : 🌐 www.paloaltonetworks.fr

Vous voulez en savoir plus ? **Visionnez la démo produit**

Témoignage client

« *IoT Security par Palo Alto Networks se déploie rapidement dans le cloud et est simple d'utilisation. Grâce à cet outil, nous obtenons une visibilité complète sur plus de 4 000 appareils IoT et médicaux, soit 30 % d'équipements en plus par rapport à notre ancienne solution.* »

Miroslav Belote
Responsable de la sécurité des systèmes d'information
Valley Health System

Valley Health System

www.paloaltonetworks.fr

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

Téléphone : +31 20 888 1883