ivanti Neurons

IT de Santé, Biomédical et Sécurité

Guide pour améliorer la visibilité et limiter les risques de sécurité pour les dispositifs médicaux

Contenu

Introduction

Les dispositifs médicaux connectés représentent un vrai défi pour l'IT de santé, le biomédical et les entreprises de sécurité. Ces périphériques sont par nature vulnérables aux cybermenaces, et une cyberattaque réussie peut avoir des conséquences dramatiques. Pourtant, il est impossible de leur appliquer les mesures de cybersécurité traditionnelle, car elles risquent d'interférer avec des opérations cliniques essentielles.

Ce guide détaille une procédure en trois étapes qui aide à améliorer la visibilité des dispositifs médicaux et à renforcer le contrôle des risques de sécurité. La mise en place de niveaux de cybersécurité pour les dispositifs médicaux est un processus continu en plusieurs étapes, qui peut être efficace s'il part de fondations solides, et adopte une approche méthodique et systématique.

Apprenez comment découvrir, évaluer et limiter les risques de cybersécurité associés aux dispositifs médicaux connectés. Les trois phases présentées dans ce guide ne constituent pas un processus ponctuel ; vous devez les considérer comme un cycle. Les équipes IT et Sécurité des établissements de santé doivent répéter ces phases en continu : examen de l'environnement, évaluation des risques et traitement des problèmes de sécurité détectés, jour après jour.

À quel point les dispositifs médicaux sont-ils vulnérables aux cyberattaques ?

Un nombre croissant de dispositifs médicaux sont connectés à des réseaux ou à d'autres périphériques, ce qui représente une vulnérabilité extrême pour les hôpitaux et autres acteurs de la santé. La plupart de ces périphériques ne sont pas sécurisés ni activement gérés, ce qui ouvre la porte à toute une variété de menaces de cybersécurité.

Pourquoi les dispositifs médicaux sont-ils vulnérables ?

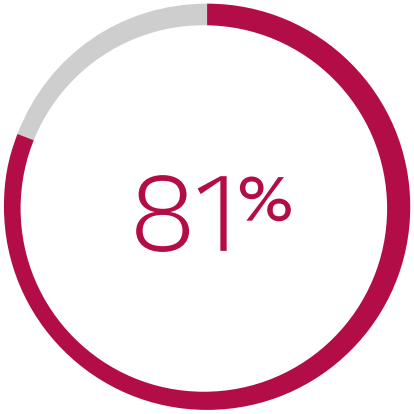
- Leur code logiciel n'a pas subi de contrôle de sécurité.
- L'authentification est faible, voire inexistante.
- Les canaux de transfert de données sont souvent non sécurisés et non cryptés.
- L'on dispose d'une visibilité limitée des périphériques activement utilisés.
- Il est impossible de surveiller l'activité des périphériques et les incidents de sécurité.
- Les périphériques qui ne sont plus utilisés ne sont pas mis au rebut en toute sécurité.
- Les mises à jour logicielles ne sont pas disponibles ou sont rarement déployées.

Comprendre l'environnement
Découvrir les périphériques IT et médicaux présents, les classifier correctement, comprendre leur contexte clinique et identifier leurs besoins en matière de réseau.

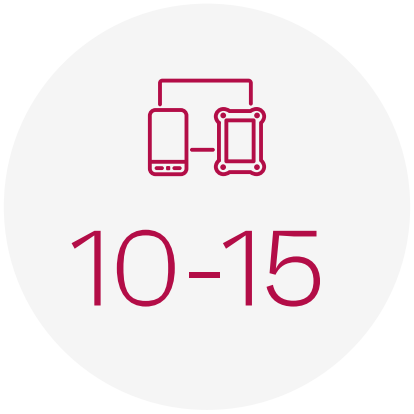
Évaluer les risques
Identifier les vulnérabilités des périphériques et les risques liés au réseau, en attribuant à chaque périphérique un indice de dangerosité et en fournissant des recommandations de correction.

Protéger les périphériques
Gérer la sécurité au niveau du périphérique, en isolant les périphériques au sein du LAN et en bloquant les communications non voulues sur le LAN/WAN, et en préparant une stratégie de détection des incidents de sécurité dès qu'ils se produisent.

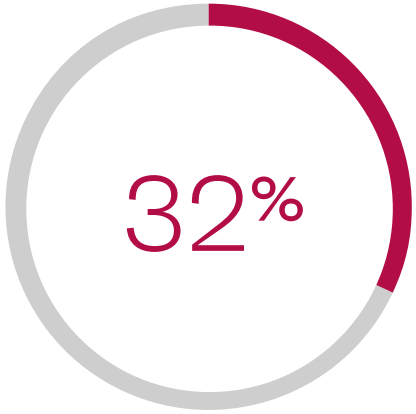
À quel point est-ce inquiétant ?



81 % des établissements de santé signalent qu'ils ont subi les dommages d'une cyberattaque ces deux dernières années.



Les hôpitaux gèrent 10 à 15 dispositifs médicaux connectés par lit, soit plus de 3,7 millions de périphériques activement utilisés.



32 % des établissements de santé disent que les dispositifs médicaux sont leur principale inquiétude en matière de sécurité.

Source : KPMG, Wired

Quels sont les vecteurs d'attaque qui affectent les dispositifs médicaux ?

Malware
En général, les dispositifs médicaux n'ont aucune protection de poste client et sont particulièrement vulnérables aux malwares.

Menaces internes
En raison de la faiblesse de l'authentification, des personnes malveillantes venues de l'intérieur peuvent facilement obtenir un accès non autorisé et saboter les périphériques.

Attaques par application Web
Certains dispositifs médicaux sont gérés via une interface Web, ce qui génère toute une série de risques de cybersécurité : injection de code, scripts intersites (XSS), Path Traversal, etc.

Mauvaise utilisation des périphériques
Les dispositifs médicaux connectés sont souvent basés sur des PC Windows. Le personnel hospitalier peut utiliser ces machines pour surfer sur Internet ou installer des logiciels, ce qui multiplie les risques.

Comment évaluer les risques de cybersécurité et l'impact d'une attaque ?

Les consignes du FDA concernant les dispositifs médicaux contiennent des informations utiles pour la classification du niveau de risque des périphériques.

Niveau 1 : Risques de cybersécurité élevés	Niveau 2 : Risques de cybersécurité standard
Le périphérique :	**Le périphérique :**
Peut se connecter à un autre produit, médical ou non, à un réseau ou à Internet. OU Un incident de cybersécurité affectant le périphérique pourrait directement causer préjudice à un ou plusieurs patients.	Peut se connecter à un autre périphérique ou réseau, mais ne peut pas directement causer préjudice à un patient. OU Peut directement causer préjudice à un patient mais ne peut pas se connecter à un réseau.

Pour une évaluation plus précise des risques, utilisez une structure telle que le calcul des risques CVSS. Tenez compte des facteurs suivants pour évaluer les risques de cybersécurité :

- Vulnérabilités logicielles
- Sécurité des patients
- Authentification
- Confidentialité
- Réseaux
- Perturbation des services

Phase I:

Comprendre l'environnement des périphériques connectés

Pour résoudre un problème, la première étape consiste à reconnaître qu'il existe et à comprendre son étendue. Les problèmes des dispositifs médicaux connectés sont mal compris par les équipes IT, biomédicales et de sécurité des hôpitaux et des établissements de santé, en raison d'une visibilité extrêmement limitée.

Les équipes de sécurité voient les dispositifs médicaux comme des boîtes noires ou ne les voient pas du tout.

La sécurité des dispositifs médicaux devient la responsabilité commune des équipes d'ingénierie clinique et des départements IT. Même s'il existe des informations sur ces périphériques dans les établissements de santé, les équipes de sécurité n'y accèdent pas facilement.

Les questions suivantes, très importantes, restent sans réponse :

1. Combien y a-t-il de périphériques connectés ?
2. De quels types de périphérique s'agit-il ?
3. Avec quels autres périphériques ou réseaux communiquent-ils ?
4. Leur comportement réseau est-il normal et attendu, ou anormal ?

Pourquoi est-il difficile de créer un inventaire des dispositifs médicaux connectés ?

Vous ne pouvez pas simplement lancer une analyse réseau pour identifier les dispositifs médicaux comme vous le feriez sur un réseau IT ordinaire :

- Périphériques sensibles — Une analyse réseau active pourrait perturber le fonctionnement des dispositifs médicaux. Il faut donc utiliser la découverte passive.
- Invisibles pour les outils de découverte réseau — Les outils traditionnels sont incapables de découvrir la vaste majorité des dispositifs médicaux connectés ou les reconnaissent par erreur comme étant des postes de travail Windows. La plupart des dispositifs médicaux connectés ne diffusent pas leurs informations, et leur détection sur le réseau nécessite une analyse attentive du trafic dans la couche Applications.
- Nombre important et grande variété de périphériques — Il peut exister des dizaines de milliers de périphériques de différents types, fournisseurs et versions.
- Flux constant — Des périphériques sont sans cesse ajoutés, remplacés ou supprimés du réseau, souvent sans intervention du département IT. La découverte et l'inventaire doivent donc faire l'objet d'un processus continu.

Étape 1. Découverte

Le but est de construire une base de données des dispositifs médicaux, avec des données sur chaque périphérique. Ciblez des données de haute qualité qui vous aideront à déterminer les risques et les vulnérabilités. Notamment :

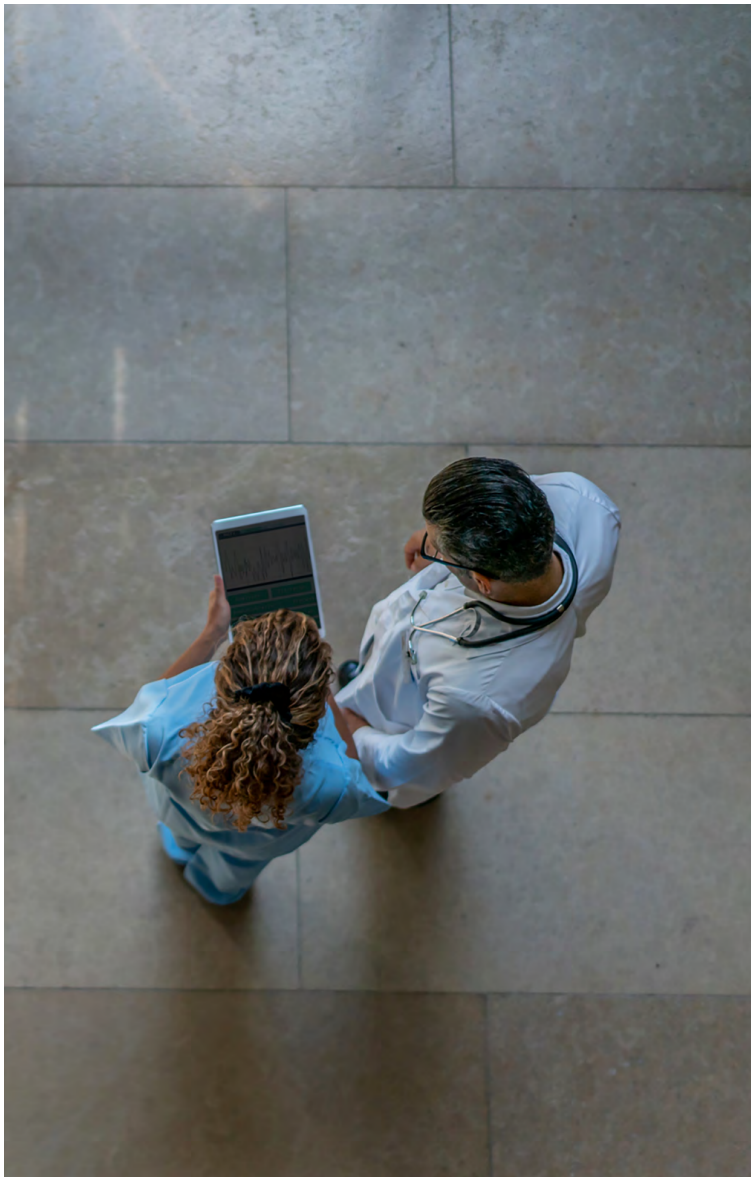
- Type de périphérique
- Service et salle
- Fournisseur
- Modèle
- Adresse IP
- Système d'exploitation
- Version logicielle des applications
- Dernier correctif de sécurité

Étape 2. Mappage réseau et contexte clinique

La compréhension du comportement réseau d'un périphérique permet de savoir à quel point il est exposé aux menaces internes et externes. Essayez d'obtenir les informations suivantes pour chacun de vos périphériques connectés :

- Avec quels autres périphériques communique-t-il ?
- Ce périphérique dispose-t-il d'un accès inutile à d'autres périphériques, à des réseaux ou à Internet ?
- Les communications réseau de ce périphérique sont-elles isolées sur un VLAN ?
- Quels types de protocole utilise-t-il ?
- Où ce périphérique envoie-t-il ou d'où reçoit-il des informations PHI (Public Health Information - Données de santé publiques), et de quel type de PHI s'agit-il ?
- Communique-t-il en externe sur Internet ?
- Ce périphérique a-t-il besoin de communiquer avec le site de son fournisseur à intervalle régulier ?
- Les communications Internet sont-elles normales pour ce type de périphérique ?
- Les communications Internet de ce périphérique sont-elles isolées dans un tunnel VPN ?

Examinez l'utilisation clinique de chaque périphérique et, par extension, son exposition aux risques. Il peut s'avérer extrêmement difficile d'obtenir ces données sans l'aide d'outils automatisés.



Phase II:

Évaluer les risques

Lorsque vous comprenez mieux vos dispositifs médicaux connectés, et que vous avez établi un inventaire des périphériques, de leur contexte et de leur comportement réseau, vous pouvez vous appuyer sur cet inventaire pour évaluer les risques de chaque périphérique et leur impact sur l'organisation.

Étape 1. Identification des vulnérabilités des périphériques et des possibilités de correction

Collectez des données sur les vulnérabilités pour chacun de vos modèles de périphérique, systèmes d'exploitation et versions d'application.

Tout aussi important : découvrez le propriétaire du périphérique et votre niveau d'accès pour corriger les problèmes de sécurité.

Impact des vulnérabilités logicielles
Utilisez le calcul des risques CVSS pour identifier l'impact des vulnérabilités logicielles connues de vos périphériques connectés.

Configurations incorrectes
Recherchez les vulnérabilités d'ordre général, comme les mots de passe par défaut ou codés en dur, ou les systèmes d'exploitation/logiciels sans correctifs.

Authentification du périphérique
Vérifiez si le périphérique utilise un outil d'authentification et, si tel est le cas, contrôlez sa puissance et vérifiez si des mots de passe sécurisés ont été définis.

Point de contact
Qui gère le périphérique ? Ingénieur clinique, département IT, fabricant ou sous-traitant tiers ?

Facilité d'accès
L'équipe Sécurité a-t-elle accès à ce périphérique pour implémenter des contrôles de sécurité ou réagir aux incidents ?

Sauvegarde
Le périphérique possède-t-il une sauvegarde ou un outil de redondance, et quel est l'impact de la perturbation des services ?

Étape 2. Identification des risques liés au réseau

Les vulnérabilités des dispositifs médicaux ne représentent qu'un des aspects des risques. Analysez les connexions réseau et identifiez les vecteurs pouvant permettre à des pirates de se connecter à vos périphériques.

Connexion Internet
Vérifiez si le périphérique se connecte à d'autres systèmes sur Internet, par exemple au site d'une entreprise tierce, ou à celui du fabricant pour la maintenance ou les mises à jour.

Connexion à des périphériques moins sécurisés
Vérifiez si le périphérique peut se connecter à un périphérique ou poste client moins sécurisé, comme le poste de travail d'un docteur, et s'il expose des services de gestion ou de données, comme le FTP ou le SSH.

Cryptage
Vérifiez si le périphérique émet ou reçoit des flux de données non cryptés.

Protocoles non sécurisés
Vérifiez si le périphérique utilise des protocoles offrant une authentification faible (voire aucune) ou comportant des vulnérabilités.

Étape 3. Identification de la gravité des risques

Posez-vous ces questions : Quel serait l'impact d'une cyberattaque réussie sur chacun de vos périphériques ? Contrairement aux attaques sur les systèmes IT de santé, l'impact d'une attaque sur des périphériques connectés ne se limite pas à la sécurité et à la confidentialité des données. Une cyberattaque réussie peut perturber les soins cliniques et causer des préjudices directement aux patients.

Nous vous recommandons d'identifier la gravité des risques d'après les trois mesures d'impact du calcul des risques CVSS :

- Confidentialité — Correspond à l'exposition risquée des données PHI (Protected Health Information - Données de santé protégées) stockées ou transmises par le périphérique.
- Intégrité — Correspond aux risques pour la sécurité du patient, pour les périphériques directement utilisés pour les soins au patient.
- Disponibilité — Correspond aux risques de perturbation des services.

Sécurité des patients	Confidentialité	Perturbation des services
FAIBLE : Dispositif médical FDA Classe I : risque faible à modéré pour le patient ou l'utilisateur	FAIBLE : Le périphérique ne stocke aucune donnée PHI.	**FAIBLE :** Une panne du périphérique ne perturbe pas les soins au patient.
MOYEN : Dispositif médical FDA Classe II : risque modéré à élevé	**MOYEN :** Le périphérique stocke une faible quantité de données PHI sur une durée limitée, pour un test ou un traitement.	**MOYEN :** Une panne du périphérique peut perturber les soins au patient mais aucun traitement médical critique.
ÉLEVÉ : Périphérique FDA Classe III : risque élevé, périphériques d'assistance vitale ou de maintien des fonctions vitales, dispositifs implantés, ou équipement induisant de forts risques de maladie ou de blessure	**ÉLEVÉ :** Le périphérique stocke une grande quantité de données PHI pour plusieurs tests ou traitements.	**ÉLEVÉ : Une panne du périphérique peut perturber un traitement médical critique, comme la chirurgie, l'assistance respiratoire ou la délivrance d'un médicament d'assistance vitale.**

Phase III:

Protéger les dispositifs médicaux connectés

L'avantage de notre processus structuré de découverte et d'évaluation des risques est qu'il permet de classer les périphériques en fonction des dangers qu'ils présentent. Chaque périphérique doit porter un score de niveau de risque (concernant la sécurité des patients, la confidentialité et la perturbation des services).

Votre entreprise peut définir le niveau de risque acceptable. L'équipe de sécurité peut se concentrer sur la protection des périphériques dont le score de niveau de risque dépasse le niveau acceptable, et appliquer les mesures de sécurité appropriées aux périphériques pour chaque score de niveau de risque.

Nous vous conseillons de protéger les dispositifs médicaux connectés en quatre étapes :

1. Protection de la couche Périphériques — Application des correctifs, désactivation des services vulnérables, adoption d'une configuration conforme aux meilleures pratiques.
2. Protection de la couche Réseau — Isolement au niveau du LAN (blocage des communications inutiles avec le réseau local) et isolement au niveau du WAN (autoriser le périphérique à communiquer uniquement avec les entités externes connues).
3. Détection des incidents — Mise en place d'une stratégie pour détecter les incidents de sécurité dès qu'ils se produisent.
4. Mesures et analyse — Analyse en continu du résultat des programmes de sécurité, ajustement et amélioration.

Étape 1. Durcissement des périphériques

Comme pour n'importe quel périphérique informatique, vous devez vous assurer que les dispositifs médicaux connectés disposent des mises à jour et des correctifs de sécurité les plus récents. La configuration doit être durcie pour permettre une authentification sécurisée. Fermez les ports non utilisés, limitez les fonctions inutiles et, plus généralement, réduisez votre surface d'attaque.

La plupart des dispositifs médicaux fonctionnent sous un système d'exploitation Windows. Cependant, l'application d'un correctif n'est pas aussi simple qu'avec un poste de travail ou un serveur Windows.

Difficultés du durcissement des dispositifs médicaux

- Les correctifs de sécurité Windows doivent être vérifiés et approuvés par le fabricant du périphérique.
- Les ingénieurs cliniques doivent vérifier que les correctifs et mises à jour n'impactent pas le fonctionnement du dispositif médical.

Consignes

- Vous ne pourrez pas déployer tous les correctifs de sécurité ou durcir tous les périphériques.
- Concentrez-vous sur les périphériques dont le score de niveau de risque est élevé.
- Donnez la priorité aux correctifs de sécurité ou aux changements de configuration qui traitent les vulnérabilités connues identifiées lors de votre évaluation des risques.

Étape 2. Isolement réseau

Une stratégie clé pour sécuriser les dispositifs médicaux connectés consiste à les isoler autant que possible des communications cliniques non essentielles, afin de limiter la surface d'attaque. Cette approche a deux composantes :

- Définition de la segmentation réseau pour garantir que les dispositifs médicaux connectés communiquent uniquement avec les périphériques ou systèmes qui font partie de leur processus clinique.
- Blocage des communications externes pour garantir que les dispositifs médicaux connectés ne se connectent jamais à Internet, sauf si c'est nécessaire pour communiquer avec le fournisseur du périphérique ou une autre entité connue.

Points à prendre en compte pour l'isolement des dispositifs médicaux

- Isolez les flux de données cliniques des flux de données non cliniques.
- Les communications cliniques sont essentielles mais toutes les autres communications doivent être bloquées.

Consignes

- Définissez des stratégies d'accès strictes et une segmentation réseau correcte pour limiter les communications non essentielles vers et depuis les périphériques.
- Définissez une stratégie de segmentation pour traiter les risques et les vulnérabilités découverts lors de votre analyse d'impact.
- Empêchez le périphérique de se connecter à Internet, sauf si c'est absolument nécessaire pour son bon fonctionnement et seulement s'il s'agit d'entités connues.
- Coopérez étroitement avec les ingénieurs cliniques et le HTM (Healthcare Technology Management - Service de gestion des technologies médicales) pour vous assurer que vous n'interrompez aucun flux de données critique.

Étape 3. Détection et résolution des incidents

La plupart des dispositifs médicaux connectés ne peuvent pas être protégés de toutes les menaces potentielles, parce qu'il y aura toujours des périphériques ancienne version critiques impossibles à remplacer, et que vous ne pouvez pas entièrement isoler ni doter de correctifs, ce qui signifie que vous pouvez réduire la surface d'attaque mais pas l'éliminer. De plus, l'isolement peut être un processus assez long et, en attendant, certains périphériques restent vulnérables. C'est pourquoi il est essentiel de surveiller les périphériques, afin de détecter immédiatement toute activité inhabituelle et d'émettre une alerte immédiate.

Points à prendre en compte pour la surveillance des incidents de sécurité

- Faites appel à la surveillance passive, par exemple via un TAP réseau ou un port en miroir, pour éviter toute interruption des opérations du périphérique.
- Exploitez les informations collectées sur le contexte clinique de chaque périphérique, pour reconnaître ce qui constitue une communication clinique normale.
- Comparez le comportement actuel aux spécifications du fabricant, au comportement passé, et au comportement d'un groupe de périphériques semblables dans votre environnement et dans d'autres entreprises.

Consignes

- Surveillez en continu tous les périphériques, en insistant surtout sur ceux qui présentent un score de niveau de risque élevé.
- Définissez une stratégie pour comparer les communications en continu aux communications cliniques normales.
- Avertissez l'équipe Sécurité de toute déviation importante par rapport au comportement normal.

- Intégrez des outils tiers capables de réaliser une correction rapide via une intervention à distance, comme la segmentation réseau à la demande.

Étape 4. Mesures et analyses

La cybersécurité des dispositifs médicaux est un processus à long terme, qu'il faut maintenir et améliorer au fil du temps pour l'adapter aux changements constants du paysage des menaces.

Le suivi de votre progression vous aide à savoir si vous partez dans la bonne direction et à apporter des corrections si vos efforts n'améliorent pas la situation en matière de sécurité. Voici quelques consignes pour suivre la progression de votre projet de sécurisation des dispositifs médicaux.

- Créez une fiche d'évaluation des dispositifs médicaux, avec la chronologie des scores de risque, pour garantir que les risques diminuent avec le temps.
- Identifiez les activités et les stratégies qui ont amélioré les KPI et réduit les indices de risque globaux.
- Définissez des KPI (indicateurs clés de performances) sur la base des risques des périphériques importants, et surveillez leur amélioration. Liez ces KPI aux objectifs de l'entreprise, comme la sécurité des patients et la disponibilité des services, pour garantir l'approbation de la Direction.
- Collectez des données sur les indices de risque et le comportement historique des périphériques, et utilisez-les pour prendre de meilleures décisions d'approvisionnement.

Améliorez la visibilité des biens et limitez les risques de sécurité des dispositifs médicaux avec Ivanti Neurons for Healthcare

Ivanti® Neurons for Healthcare améliore la visibilité des biens et limite les risques de sécurité pour les dispositifs médicaux. La solution découvre et profile intelligemment les dispositifs médicaux et les périphériques IoMT (Internet of Medical Things), en évaluant les risques de sécurité, en faisant un rapport des menaces et en rapprochant les informations de périphérique provenant de plusieurs sources de données. Vous pourrez en savoir plus sur les différents périphériques propres à la santé sur l'ensemble de vos sites, avec leur classification et les détails de leur utilisation, et obtenir des informations pour limiter les risques et gérer les anomalies. Collectez et rapprochez les données fournisseur afin de créer une « source de vérité » unique pour tous vos dispositifs médicaux.

Pour en savoir plus, visitez le site ivanti.fr/neurons

ivanti Neurons

ivanti.fr/neurons
contact@ivanti.fr