La sécurité dans le secteur de la santé : une analyse au microscope

Forescout analyse les données de déploiement afin de mieux cerner les risques de cybersécurité auxquels les établissements de soins de santé sont confrontés.

FORESCOUT®

Synthèse

L'Internet des objets médicaux (IoMT, Internet of Medical Things) est riche en potentiel pour les établissements de soins de santé en ce qui concerne la prise en charge des patients. Cependant, cette transformation numérique et la hausse de connectivité qui en découle ouvrent également la porte à de nouveaux risques pour la confidentialité et la sécurité. Le paysage des appareils croît de façon exponentielle, ce qui complexifie encore les réseaux et rend la stratégie de sécurité encore plus difficile à gérer et à améliorer.

Ce rapport s'adresse aux responsables de la sécurité et de la gestion des risques des établissements de soins de santé. Il entend leur proposer des informations utiles sur les types d'appareils qui se connectent à leurs réseaux et les risques associés. Il préconise également l'adoption d'une approche globale de la sécurité qui va au-delà de la simple sécurisation des appareils médicaux.

Les données sources utilisées dans ce rapport proviennent de Forescout Device Cloud, un référentiel d'informations sur les systèmes et les réseaux couvrant plus de huit millions d'appareils, ce qui en fait l'un des plus grands référentiels collaboratifs actuels. Dans le cadre de la présente étude, nous avons limité notre analyse Device Cloud à 75 déploiements dans le secteur de la santé, regroupant plus de 10 000 VLAN et 1,5 million d'appareils. Ce rapport se penche principalement sur le statut des appareils médicaux. Pour cette raison, de nombreux résultats sont basés sur l'analyse de plus de 1 500 VLAN médicaux incluant 430 000 appareils.

Principales observations :

- **Les environnements de soins de santé sont aujourd'hui de plus en plus hétérogènes :** la croissance rapide et la diversité des appareils médicaux connectés et des systèmes d'exploitation compliquent la sécurisation des réseaux.
- **Les anciens systèmes d'exploitation Windows représentent une vulnérabilité majeure :** de nombreux réseaux utilisent encore des systèmes d'exploitation Microsoft Windows qui ne sont plus pris en charge. La situation risque par ailleurs d'empirer avec la sortie prochaine d'une nouvelle version.
- **Les stratégies de segmentation sont trop peu implémentées :** bien qu'il s'agisse d'une bonne pratique permettant de limiter les attaques par mouvement latéral en se concentrant sur la sensibilité, l'emplacement et la criticité des données, la segmentation des réseaux est appliquée de façon incohérente sur les réseaux très variés actuels.
- **La multiplication des fournisseurs d'appareils doit être contrôlée :** le recours à de multiples fournisseurs cause de gros problèmes d'interopérabilité, de sécurité et de gestion des ressources.
- **Les services communs toujours actifs rendent le réseau vulnérable :** les protocoles communs laissés ouverts représentent un accès non contrôlé par lequel les cybercriminels peuvent attaquer.

L'état de la cybersécurité pour les établissements de soins de santé

En raison de sa capacité à améliorer les soins aux patients, à fournir des données cliniques plus fiables, à augmenter l'efficacité et à réduire les coûts, l'IoMT reste une priorité stratégique. Les raisons pour lesquelles les établissements de soins de santé y adhèrent aussi rapidement sont faciles à comprendre : il s'agit d'une infrastructure connectée d'appareils médicaux, d'applications logicielles et de systèmes et services de soins. Cependant, l'adoption accélérée d'appareils connectés présente aussi un effet secondaire grave : elle fait perdre de vue la nécessité plus large de répondre aux besoins de sécurité généraux des environnements convergents modernes, au-delà des appareils médicaux connectés. Une attitude qui risque de créer des failles de cybersécurité significatives.

L'Internet des objets médicaux (IoMT) est une infrastructure connectée d'appareils médicaux, d'applications logicielles et de systèmes et services de soins. Dans le cadre de cette étude, l'IoMT entre dans les catégories de l'Internet des objets (IoT) et des technologies d'exploitation (OT).

L'explosion des appareils IT et OT connectés dans le secteur de la santé

Le nombre d'appareils connectés croît à une vitesse accélérée, élargissant de ce fait la surface d'attaque et rendant plus difficile l'adaptation de la stratégie de sécurité aux nouveaux risques. Ces appareils incluent les équipements médicaux, par exemple les systèmes d'identification et de suivi des patients, les pompes à perfusion et les systèmes d'imagerie. Ils recouvrent aussi les équipements d'infrastructure, comme les systèmes immotiques, les systèmes de sécurité physiques, les blocs d'alimentation sans interruption, les générateurs de secours, et les autres systèmes et appareils OT que l'on voit de plus en plus fréquemment dans les réseaux informatiques. De ce fait, la responsabilité de l'OT incombe aux équipes informatiques. Selon Gartner, « d'ici 2021, 70 % de la sécurité OT sera gérée directement par le DSI, le RSSI ou le directeur de la sécurité, contre 35 % aujourd'hui[1] ».

Comprendre et hiérarchiser les risques

La convergence de ces deux réseaux, autrefois disparates, peut créer une nouvelle classe de risques de sécurité. Les cybercriminels peuvent en effet désormais lancer des attaques en mouvement latéral sur les réseaux IT et OT interconnectés. La hausse des fusions-acquisitions, très fréquente dans le secteur de la santé, amplifie davantage encore cette menace.

Tout comme un médecin va poser un diagnostic clinique et préconiser un traitement, les RSSI doivent détecter les risques très tôt et élaborer le meilleur plan d'action possible. Les équipes de sécurité et de gestion des risques qui tentent d'atténuer chaque menace de façon individuelle obtiendront des résultats limités. En revanche, en comprenant pleinement les menaces qui pèsent sur un réseau et en identifiant les appareils les plus à risque, il est possible d'optimiser la productivité, d'augmenter le retour sur investissement et de réduire les risques sur l'ensemble du réseau.

Remettre à plus tard le confinement des risques : les vrais coûts

Une fois encore, les domaines de la cybersécurité et des soins de santé ont un point commun : non seulement la détection et le traitement précoces donnent de meilleurs résultats, mais ils réduisent considérablement les coûts globaux. Voyez ces statistiques : d'après l'*HIPAA Journal* (une revue en ligne qui traite de sujets liés à la loi américaine Health Insurance Portability and Accountability Act), une compromission moyenne dans le secteur de la santé en 2018 a impliqué 17 974 enregistrements[2]. Le Ponemon Institute estime le coût moyen de résolution par personne/enregistrement d'informations personnelles de santé en 2018 à 408 $[3]. Cela porte les coûts de *confinement, divulgation des résultats d'enquête et notification* à 7,3 millions $ par compromission. Mais le carnage financier ne s'arrête pas là. Les compromissions peuvent nuire considérablement à l'image de marque et à la réputation d'un établissement, ce qui peut en détourner les patients pendant des années, surtout aux États-Unis. Ces organisations se retrouvent en outre obligées de mettre en place un cycle d'audits continus pour un temps indéterminé. L'expression « payez maintenant ou payez après » n'a jamais été aussi appropriée.

[1] « Strategic Roadmap for Integrated IT and OT Security » (Feuille de route stratégique pour la sécurité IT et OT intégrée), Gartner, Inc., mai 2018, www.gartner.com/doc/3873972/-strategic-roadmap-integrated-it

[2] « Analysis of 2018 Healthcare Data Breaches » (Analyse des violations de données dans le secteur de la santé en 2018), HIPAA Journal, janvier 2019, www.hipaajournal.com/analysis-of-healthcare-data-breaches/

[3] « 2018 Cost of a Data Breach Study: Global Overview » (Coût d'une violation de données, étude 2018 : Perspective mondiale), Ponemon Institute, juillet 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf

Le secteur de la santé est une cible de choix pour les cyberattaques

Dans le secteur de la santé, la surface d'attaque s'élargit chaque jour. D'une part, de plus en plus d'appareils médicaux se connectent aux réseaux. D'autre part, les établissements de soins sont une cible privilégiée des cyberpirates, très intéressés par les informations personnelles de santé — les données les plus sensibles qui soient. Les cybercriminels convoitent particulièrement ce type de données en raison de leur grande valeur et de leur variété (date et lieu de naissance, numéro de carte de crédit, numéro de sécurité sociale, adresse postale et adresse e-mail).

Cyberattaques les plus courantes visant les établissements de soins de santé

- **Logiciels de demande de rançon tels que les chevaux de Troie WannaCry et NotPeya :** ce type de logiciel malveillant chiffre les fichiers, ce qui empêche le personnel d'accéder aux systèmes et aux dossiers de santé électroniques, et donc de prodiguer les soins. Tout est rétabli dès le paiement d'une rançon. *Les attaques WannaCry de mai 2018 ont perturbé les soins aux patients dans l'ensemble du système national de soins de santé (National Health Service) au Royaume-Uni, et forcé l'annulation de plus de 19 000 rendez-vous médicaux. Le ministère de la Santé britannique a estimé le coût financier de ces attaques à 92 millions £[4]. En 2016, des attaques similaires ont entraîné la déconnexion des ordinateurs du Hollywood Presbyterian Medical Center pendant une semaine. Le personnel s'est retrouvé dans l'incapacité de fournir des services médicaux jusqu'au paiement d'une rançon de 17 000 $[5].*

- **Déni d'accès et déni de service distribué (DDoS) :** un cybercriminel inonde de paquets le réseau et les serveurs connectés à Internet, perturbant le flux normal du trafic et ralentissant les performances du système et des applications, quasiment jusqu'au blocage complet. Ces attaques sont parfois utilisées également pour détourner l'attention de l'équipe de sécurité alors qu'un vol de données est en cours au même moment. *En 2014, le groupe hacktiviste Anonymous a lancé une attaque DDoS contre le Boston Children's Hospital. Selon le Center for Internet Security, l'hôpital a dépensé plus de 300 000 $ en coûts d'intervention et de correction des dommages[6].*

- **Usurpation d'appareil :** un appareil se connecte au réseau et se comporte comme un appareil autorisé, mais il s'agit en fait d'un appareil non approuvé qui collecte des données. Les cybercriminels utilisent cette technique pour voler des informations personnelles de santé ou pénétrer dans les systèmes principaux. *Les premières inquiétudes sur le Medjacking (ou « piratage médical »), une forme courante d'usurpation d'appareil médical, sont apparues lorsque le vice-président des États-Unis Dick Cheney a demandé que son pacemaker soit mieux protégé des pirates. Selon la revue Wired, les cybercriminels utilisant le Medjacking utilisent aujourd'hui de façon intentionnelle des logiciels malveillants anciens pour cibler des appareils médicaux utilisant des systèmes d'exploitation obsolètes, comme Windows XP et Windows Server 2003[7].*

- **Attaque Man-in-the-Middle :** un cybercriminel s'insère dans les communications entre deux parties (généralement par le biais d'une escroquerie par phishing) pour espionner quelqu'un ou usurper l'identité d'une autre personne. *En avril 2017, le Bureau des droits civiques du ministère de la Santé et des Services sociaux des États-Unis a conseillé aux entités concernées et à leurs associés d'utiliser le protocole HTTPS pour assurer la sécurisation permanente des informations médicales protégées[8].*

- **Logiciel malveillant sans fichier :** les cybercriminels ont appris à contourner les outils traditionnels de protection grâce à un nouveau type de logiciel malveillant qui réside uniquement dans la mémoire dynamique du système. D'après les prévisions du Ponemon Institute, en 2019, les logiciels malveillants sans fichier représenteront 38 % des attaques[9]. En plus d'être lancées via des navigateurs obsolètes ou non corrigés, ces attaques en mémoire exploitent souvent les points faibles de Microsoft Windows®, par exemple PowerShell et Remote Desktop Protocol (RDP).

[4] « Securing cyber resilience in health and care » (Assurer la cyberrésilience dans le secteur de la santé), octobre 2018, www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update

[5] Article du Los Angeles Times, 18 février 2016, www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

[6] « DDOS Attacks: In the Healthcare Sector » (Attaques DDoS dans le secteur de la santé), Center for Internet Security, www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

[7] « Medical Devices are the next security nightmare » (Les appareils médicaux sont le prochain casse-tête de la sécurité), WIRED, mars 2017, www.wired.com/2017/03/medical-devices-next-security-nightmare/

[8] « Healthcare Organizations Warned of Risk of Man-In-The-Middle Attacks » (Les établissements de soins avertis de la possibilité d'attaques Man-In-The-Middle), HIPAA Journal, avril 2017, www.hipaajournal.com/healthcare-organizations-warned-risk- man-middle-attacks-8757/

[9] « State of Endpoint Security Risk » (État du risque de sécurité des points d'extrémité), Ponemon Institute, octobre 2018, https://cdn2.hubspot.net/hubfs/468115/whitepapers/state-of-endpoint-security-2018.pdf

Comprendre ce que sont les dispositifs connectés et les risques associés

Méthodologie

Ce rapport est une analyse intersectionnelle de Forescout Device Cloud, un référentiel d'informations sur les systèmes et les réseaux couvrant plus de huit millions d'empreintes matérielles uniques, ce qui en fait l'un des plus grands référentiels collaboratifs actuels. Device Cloud contient les données de milliers d'appareils de types différents appartenant à plus de 1 000 clients Forescout qui partagent des informations de façon anonyme. Forescout analyse les empreintes matérielles à partir de Device Cloud pour identifier la fonction, le fournisseur et le modèle des appareils, ainsi que leur système d'exploitation et leur version. Cette solution fournit ainsi une classification automatique granulaire complète d'un large éventail d'appareils.

Dans le cadre de la présente étude, nous avons limité notre analyse Device Cloud à 75 déploiements dans le secteur de la santé, regroupant plus de 10 000 VLAN et 1,5 million d'appareils. Ce rapport se penche principalement sur le statut des appareils médicaux. Pour cette raison, de nombreux résultats sont basés sur l'analyse de plus de 1 500 VLAN médicaux incluant 430 000 appareils.

Classes d'appareils sur les VLAN médicaux

De nombreux réseaux fonctionnent encore dans des silos organisationnels, ce qui entraîne des failles sur le plan de la sécurité. Tandis que les ingénieurs cliniques s'occupent souvent de la sécurisation des appareils médicaux connectés, les équipes responsables des installations et des opérations se concentrent sur la sécurisation des systèmes immotiques. Dans un tel contexte où les priorités des uns et des autres sont cloisonnées, qui est responsable de l'examen global de la sécurité ?

Au niveau le plus fondamental, les établissements de soins de santé doivent connaître les appareils IT, IoT et OT qui se connectent à leurs réseaux. Cette connaissance permet d'éliminer les silos, de constituer des groupes pertinents afin de discuter des stratégies et de jeter les bases d'une approche globale de la sécurité.

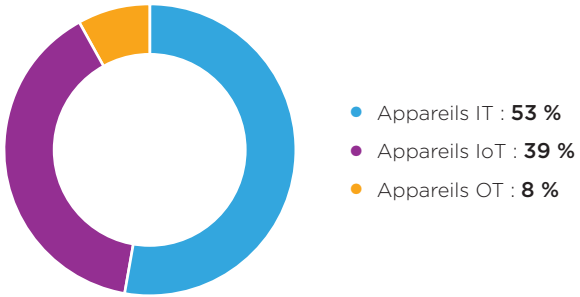
À mesure qu'un plus grand nombre d'appareils médicaux se connecteront aux réseaux, la taille des classes d'appareils changera probablement, d'où l'importance d'examiner et d'adapter régulièrement les stratégies de sécurité.

Figure 1. Classes d'appareils sur les VLAN médicaux

Appareils IT : PC, ordinateurs portables, stations de travail dédiées à des tâches spécifiques, serveurs, clients lourds et légers, hyperviseurs de virtualisation et matériel réseau d'entreprise.

Appareils OT : appareils médicaux, systèmes de soins intensifs, systèmes immotiques/CVCA, générateurs électriques, systèmes d'identification et autres équipements liés aux installations, caméras de sécurité IP et systèmes de sécurité physiques.

Appareils IoT : téléphones VoIP, imprimantes réseau, appareils mobiles, tablettes, contrôleurs et convertisseurs, équipements de vidéoconférence, systèmes de présentation, télévisions intelligentes, consoles de jeu, accessoires variés.

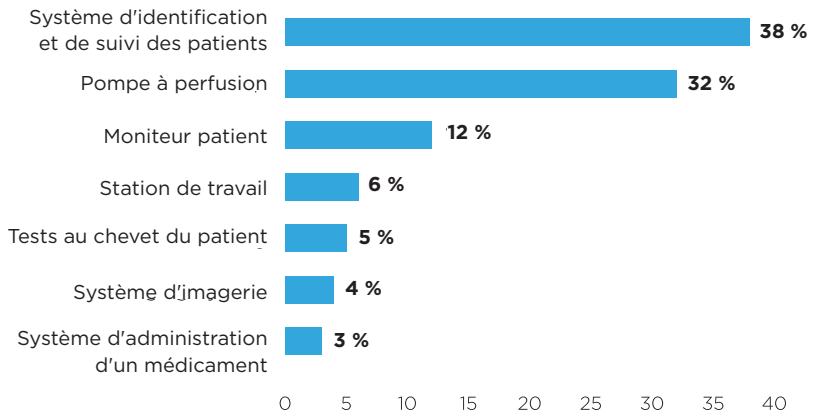


Les appareils médicaux connectés les plus courants

On constate généralement un pourcentage élevé d'appareils « connectés » à un patient hospitalisé. Les appareils rattachés à un patient, tels que les systèmes d'identification et de suivi, les pompes à perfusion et les moniteurs, représentent la majorité des équipements médicaux présents sur les réseaux cliniques. Cela semble logique puisque ce sont eux qui suivent et surveillent les patients de façon individuelle.

Les appareils utilisés pour les diagnostics de laboratoire ou l'imagerie médicale sont moins nombreux, car ils sont partagés. Ces systèmes plus coûteux ont une durée de vie assez longue, ce qui les rend susceptibles à l'obsolescence, et donc difficiles à mettre à jour et à corriger à long terme.

Figure 2. Appareils médicaux connectés les plus courants



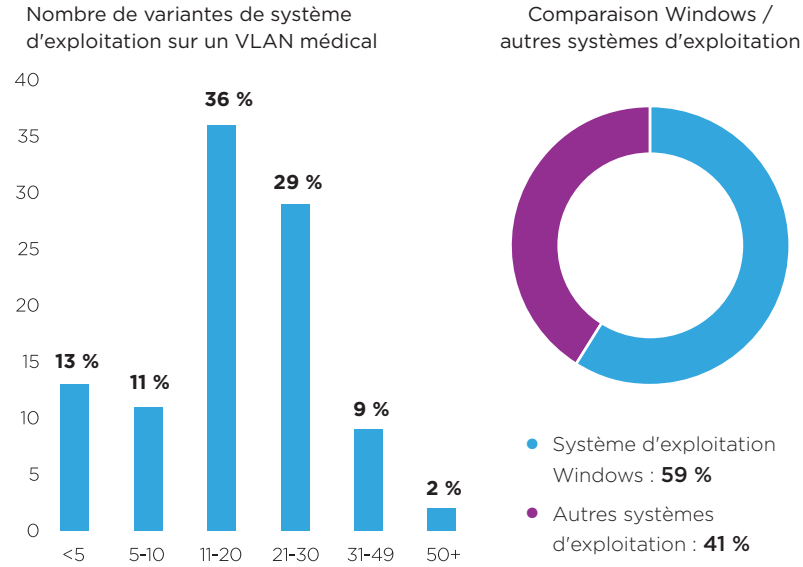
Diversité des systèmes d'exploitation sur les appareils

La diversité des systèmes d'exploitation exécutés sur les appareils peut rendre la gestion de la sécurité encore plus difficile. L'étude a révélé que dans 40 % des déploiements, le VLAN médical comprenait plus de 20 systèmes d'exploitation différents.

Si on examine les différents types de systèmes d'exploitation présents sur les VLAN médicaux, plus de la moitié d'entre eux (59 %) sont des systèmes Windows et 41 % un mélange d'autres variantes, y compris des infrastructures mobiles, à micrologiciel intégré, réseau, etc. La correction et la mise à jour des systèmes d'exploitation dans les environnements de soins de santé (en particulier dans les unités de soins de courte durée) peuvent s'avérer difficiles et exiger que les appareils demeurent en ligne et disponibles. Certains appareils médicaux ne peuvent pas être corrigés, d'autres peuvent nécessiter l'approbation du fournisseur pour l'application d'un correctif, d'autres encore peuvent exiger l'implémentation manuelle des correctifs.

> Dans 40 % des déploiements, le VLAN médical comprend plus de 20 systèmes d'exploitation différents.

Figure 3. Diversité des systèmes d'exploitation exécutés sur un VLAN médical



Le problème des systèmes Windows anciens

Dans notre échantillon de données, plus de 70 % des appareils s'exécutant sous Windows (notamment Windows 7, Windows 2008 et Windows Mobile) sont concernés par l'arrêt de la prise en charge par Microsoft du système d'exploitation d'ici le 14 janvier 2020. L'exécution de systèmes d'exploitation non pris en charge pose un risque qui affecte la conformité à de nombreuses réglementations.

Or, en raison du coût élevé des mises à jour, il est très probable que des appareils médicaux utilisant des systèmes d'exploitation anciens continueront à être présents sur les réseaux. En outre, les systèmes de soins intensifs peuvent difficilement supporter des indisponibilités associées à la mise à jour d'un système d'exploitation. Par ailleurs, certaines applications anciennes ne fonctionneront tout simplement pas sur les versions plus récentes de Windows en raison d'un manque de prise en charge ou de compatibilité, ou de problèmes de licence. Conclusion : les établissements de soins de santé ne sont pas prêts à renoncer à l'exécution de systèmes d'exploitation anciens sur leurs appareils médicaux. Face à cette réalité, il convient de prendre des mesures, notamment la segmentation appropriée des appareils afin de protéger l'accès aux informations et aux services critiques.

À partir du 14 janvier 2020, 71 % des appareils exécuteront une version de Windows non prise en charge.

Figure 4. Systèmes d'exploitation Windows — « Le Bon, la Brute et le Truand »

Le Bon	La Brute	Le Truand
29 %	0,4 %	71 %
des appareils exécutent une version de Windows qui sera prise en charge pendant plus d'un an.	des appareils exécutent une version ancienne/ non prise en charge de Windows.	des appareils exécuteront une version de Windows non prise en charge à partir du 14 janvier 2020.

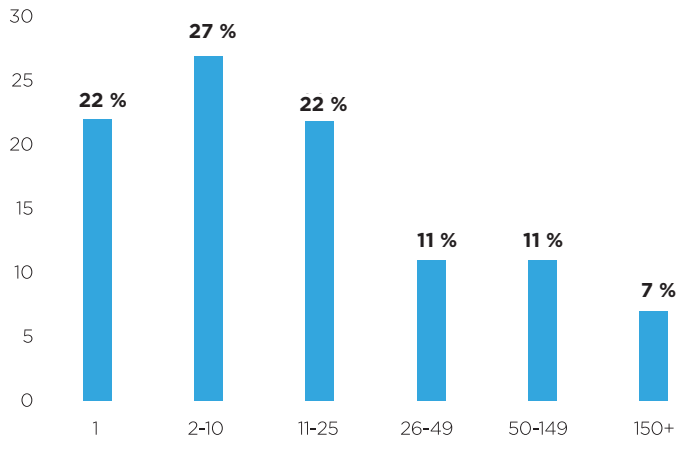
Utilisation de VLAN pour assurer la segmentation

La segmentation réduit considérablement la surface d'attaque des systèmes. Les utilisateurs « voient » uniquement les serveurs et autres appareils dont ils ont besoin pour effectuer leurs tâches quotidiennes. La création de segments s'effectue en regroupant les utilisateurs standard par type et en limitant leur accès réseau aux ressources nécessaires à l'exécution de leur travail.

La segmentation peut être réalisée selon différentes méthodes. Au niveau le plus fondamental, les VLAN peuvent être utilisés pour segmenter le réseau en fonction des besoins et des priorités de l'établissement, en isolant les données critiques, en séparant les appareils similaires par fonction ou en limitant l'accès aux données, aux systèmes et aux autres ressources via un système d'identification des utilisateurs. Les données que nous avons collectées lors de notre étude révèlent un faible nombre de VLAN incluant des appareils médicaux, ce qui semble indiquer que certains établissements de soins de santé n'ont pas encore investi suffisamment dans la segmentation.

49 % des déploiements disposent d'appareils médicaux sur 10 VLAN ou moins, signe d'une segmentation réduite.

Figure 5. Nombre de VLAN incluant des appareils médicaux



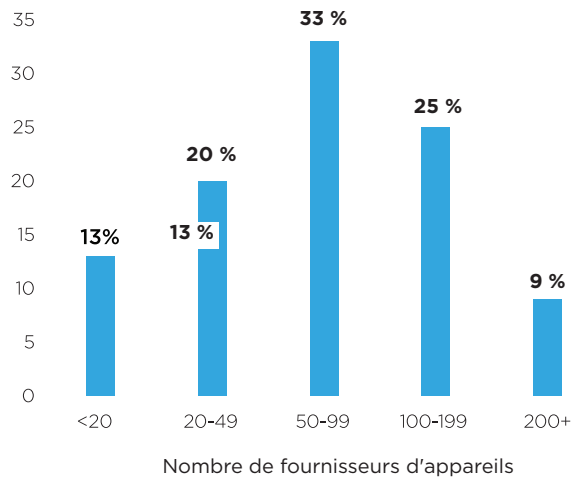
Un paysage de fournisseurs de plus en plus complexe

Les établissements de soins de santé d'aujourd'hui sont des environnements saturés de technologies. Or, les fournisseurs d'appareils n'ont jamais érigé la sécurité en priorité absolue dans la conception de leurs produits, ce qui rend leur gestion et leur sécurisation plus difficiles. De plus, ils proposent aux cliniciens des appareils qui finissent par être connectés au réseau, contournant de la sorte les protocoles de sécurité et de gestion des risques. Certes, les équipes IT et de sécurité sont capables de détecter ces appareils connectés non autorisés, mais généralement pas de les classer ou de les repérer facilement.

Les réseaux campus multisite dans le secteur des soins de santé sont loin d'être techniquement homogènes. Plus de 30 % des VLAN médicaux incluent des appareils de plus d'une centaine de fournisseurs différents. Et ce pourcentage n'inclut pas les fournisseurs des autres réseaux fonctionnels, comme le back office, le front office, etc. Dans de nombreux cas, les fournisseurs eux-mêmes sont responsables de la mise à jour des systèmes cliniques spécialisés et de l'application des correctifs.

> 34 % des VLAN médicaux d'un établissement incluent des appareils de plus de 100 fournisseurs différents.

Figure 6. Nombre de fournisseurs d'appareils sur un VLAN médical



Les services communs toujours actifs rendent le réseau vulnérable

Des services à haut risque sont activés sur un nombre surprenant d'appareils présents sur les VLAN médicaux, ce qui offre aux cybercriminels un accès non contrôlé leur permettant de sortir du périmètre et de se déplacer latéralement. En effet, les exigences en matière d'accès des fournisseurs médicaux et externes impliquent souvent que les appareils soient dotés de services tels que le protocole RDP (Remote Desktop Protocol) de Microsoft. Dans d'autres cas, nous avons constaté que des ports réseau étaient laissés ouverts par défaut à l'insu de l'équipe informatique et de sécurité.

- **Protocole SMB (Server Message Block) :** SMB est le protocole de transport utilisé par les ordinateurs Windows à des fins diverses telles que le partage de fichiers et d'imprimantes, et l'accès aux services Windows distants. WannaCry et NotPetya sont deux exemples de logiciels de demande de rançon qui exploitent les vulnérabilités de SMB.
- **Protocole RDP (Remote Desktop Protocol) :** RDP est un autre protocole commun exploité par les menaces automatisées modernes, par exemple les logiciels malveillants sans fichier.
- **Protocoles FTP (File Transfer Protocol), SSH (Secure Shell), Telnet et DICOM (Digital Imaging and Communications in Medicine) :** moins courants mais souvent exploités, ces protocoles n'assurent pas la sécurisation ni le chiffrement des sessions réseau. Les modèles de sécurité sont très peu compatibles avec les méthodes anciennes où de nombreux appareils reposent sur des services de base non chiffrés.

> Le protocole SMB (Server Message Block) est activé sur 85 % des appareils s'exécutant sous Windows.

Service Windows	Pourcentage en exécution
SMB	85 %
RDP	32 %
FTP*	1 %
SSH	< 1 %
Telnet*	< 1 %
DICOM	< 1 %

* Non chiffré

Recommandations

C'est inévitable : le nombre d'appareils connectés aux réseaux médicaux continuera d'augmenter et les environnements deviendront de plus en plus complexes. Il est temps de développer et d'implémenter une stratégie proactive de sécurité et de gestion des risques à l'échelle de l'organisation.

Permettre la découverte sans agent de tous les appareils

Les agents logiciels facilitent la communication entre les appareils et les systèmes de gestion IT et de la sécurité, ainsi que la surveillance des activités, mais la plupart des appareils médicaux ne les prennent pas en charge. La découverte sans agent de tous les appareils connectés IP sur le réseau étendu est donc essentielle.

Identifier et classer automatiquement les appareils

Il ne suffit pas de simplement détecter l'adresse IP d'un appareil. Une classification automatique rapide et granulaire est vitale pour extraire des informations contextuelles de chaque appareil du réseau et déterminer sa finalité, son propriétaire et son niveau de sécurité. Ces informations serviront à alimenter un inventaire en temps réel des actifs afin de piloter les politiques de contrôle d'accès et d'aider les équipes de sécurité à répondre rapidement à des attaques ciblées sur des systèmes d'exploitation ou des appareils spécifiques.

Surveiller les appareils en continu

Les appareils médicaux doivent faire l'objet d'une surveillance continue afin de détecter tout changement dans le niveau de sécurité. Une approche basée sur des analyses ponctuelles peut mener à une mentalité attentiste, où le suivi de la conformité est négligé et les risques s'accentuent. La surveillance ininterrompue du réseau à l'aide de techniques passives et/ou actives dans les environnements cliniques et OT fournit aux équipes de sécurité une connaissance situationnelle en temps réel. Elle leur permet de suivre en continu les informations et le comportement des ressources tout en renforçant leur efficacité et en leur faisant gagner un temps précieux.

Appliquer la segmentation

La segmentation du réseau est une bonne pratique reconnue, mais elle n'est pas facile à gérer ou à appliquer dans l'ensemble d'un réseau. Les appareils à haut risque, comme les systèmes anciens connus pour être vulnérables, doivent être segmentés pour permettre de contenir une compromission potentielle et de limiter les risques.

Conclusion

Les responsables de la sécurité et de la gestion des risques des établissements de soins de santé doivent impérativement envisager la sécurisation de tous les appareils dans l'entreprise étendue. Se contenter de sécuriser les appareils médicaux individuels plutôt que toutes les classes d'appareils peut donner lieu à des failles de sécurité graves. Une approche globale de la sécurité exige une visibilité et un contrôle continus sur l'ensemble de l'écosystème des appareils connectés. Elle nécessite notamment de comprendre le rôle qu'une plateforme de visibilité et de contrôle des appareils peut jouer dans l'orchestration des actions des divers outils hétérogènes de sécurité et de gestion informatique.

Comme nous l'avons expliqué précédemment, les coûts de l'inaction peuvent être exorbitants. À chaque seconde où un appareil n'est pas conforme, la fenêtre de vulnérabilité s'étend et les facteurs de risque augmentent, exposant ainsi une organisation à des conséquences graves en termes de sécurité des patients, de santé financière et d'activité. Les établissements de soins ont le choix : investir tout de suite dans une stratégie de planification proactive et d'atténuation des risques, ou payer plus tard et courir le risque de subir les foudres des organismes de réglementation, des patients et des législateurs soucieux de sécurité.

À propos de Forescout Technologies

Forescout Technologies est leader sur le marché de la visibilité et du contrôle sur les appareils. Notre plateforme de sécurité unifiée permet aux entreprises et aux organismes du secteur public d'acquérir une connaissance situationnelle complète de leurs environnements à l'échelle de l'entreprise étendue, mais aussi d'orchestrer des actions en vue de réduire les cyberrisques et les risques opérationnels. Les produits Forescout peuvent être déployés rapidement grâce à la découverte et à la classification en temps réel sans agent des appareils connectés IP, ainsi qu'à l'évaluation continue du niveau de sécurité. Depuis le 31 décembre 2018, 3 300 clients dans plus de 80 pays utilisent la solution de Forescout, qui fonctionne indépendamment de l'infrastructure, pour réduire les risques d'interruptions d'activité dues à des incidents ou à des compromissions, pour assurer leur conformité et en donner la preuve, et pour augmenter la productivité des opérations de sécurité. Pour en savoir plus, consultez le site Forescout.fr.

Les chercheurs de Forescout ont limité la portée des résultats de l'étude et les échantillons de données à des fins de cohérence et pour permettre la rédaction d'un rapport ponctuel. Ces limitations sont établies en raison du type et de la durée de l'étude, de sa portée, de l'anonymisation des données, des méthodes passives de capture des données et des erreurs possibles dans la classification basée sur l'intelligence artificielle des fonctions des appareils, des systèmes d'exploitation et des fournisseurs. L'utilisation de données cloud en direct issues d'un environnement de production signifie que la fourniture de données est parfois imparfaite. Travaillant dans les limites de ce cadre, les chercheurs de Forescout ont tout mis en œuvre pour assurer l'uniformité, la fiabilité et l'intégrité de ce rapport.

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Numéro gratuit (États-Unis) +1 866 377 8771

Tél. (International) +1 408 213 3191
Support +1 708 237 6591