PHILIPS

Échographie

Sécurité

# **Protégez-vous** votre équipement médical contre les brèches de données de patients?

Comme toute industrie qui repose sur des réseaux informatiques de plus en plus connectés, l'industrie des soins de santé doit composer avec un nombre croissant de brèches de sécurité.

Lisa Gallagher, directrice principale de la confidentialité et de la sécurité de la Healthcare Information and Management Systems Society (HIMSS), estime qu'entre 40 et 45 millions de dossiers de patients ont été compromis lors de brèches de données HIPAA[1]. Bien que ce nombre soit une estimation, car ce ne sont pas toutes les brèches qui sont signalées, une autre étude tend à démontrer que les brèches de sécurité touchant les dossiers médicaux ont bondi de 138 % entre 2012 et 2014[2].

Que ces brèches soient causées par des pirates informatiques, des programmes malveillants ou qu'il s'agisse de cas d'accès non autorisé, elles représentent une menace pour la sécurité des patients et des données. De plus, le grand nombre d'instruments médicaux en réseau fait du maintien de la cybersécurité une tâche ardue.

### Le défi pour les appareils d'imagerie

Les appareils d'imagerie ne sont pas à l'abri de ces attaques. La plupart ont été conçus en mettant l'accent sur l'utilité clinique, sans tenir compte du risque d'exploitation à des fins illégales de leurs ordinateurs connectés à un réseau. Cela rend les instruments médicaux vulnérables, et les assaillants peuvent utiliser ces appareils fermés comme points de pivot au sein du réseau de la santé.

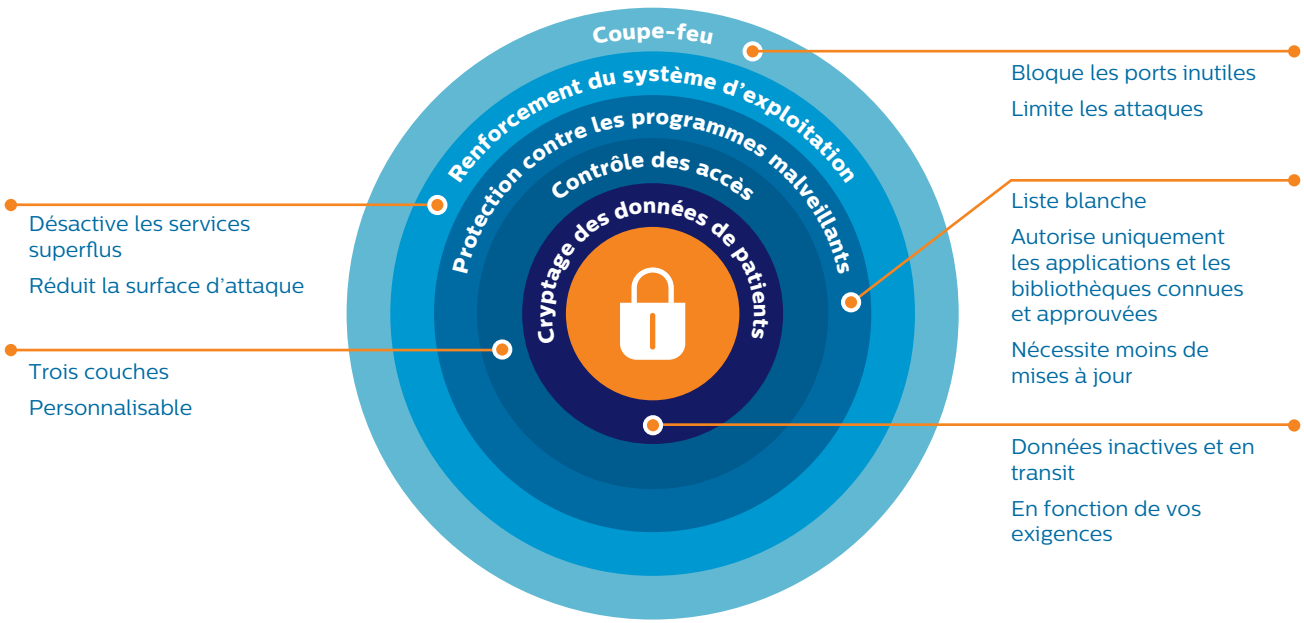
De plus, le coût des brèches de sécurité liées aux données sur la santé peut dépasser plusieurs millions de dollars, et ce coût peut augmenter en cas de poursuites civiles et autres actions en justice, et en cas de dommages causés à la réputation d'un établissement. L'HIMSS conclut que « les hôpitaux et les établissements de santé similaires disposent généralement de 300 % à 400 % plus d'équipements médicaux que d'appareils informatiques[3]. » Par conséquent, la FDA a publié des directives sur la cybersécurité des instruments médicaux en réseau[4].

La division Échographie de Philips reconnaît l'importance de sécuriser vos instruments médicaux et de protéger les données de vos patients. Ensemble, nous pouvons maintenir un environnement sécurisé en restant vigilants et en définissant le paysage des cybermenaces en constante évolution. Nous nous engageons à répondre aux besoins et aux exigences de nos clients.

# Commencer avec la **bonne stratégie**

Une stratégie de défense en profondeur, fondée sur le fait qu'un système de défense à plusieurs couches est plus difficile à pénétrer qu'une seule barrière, constitue la base des meilleures pratiques en matière de sécurité des instruments médicaux. Les couches peuvent comprendre des politiques et procédures de sécurité, des contrôles d'accès, des mesures techniques, des formations et des évaluations des risques.

## Stratégie de défense en profondeur




**Assurer la sécurité des produits EPIQ et Affiniti**

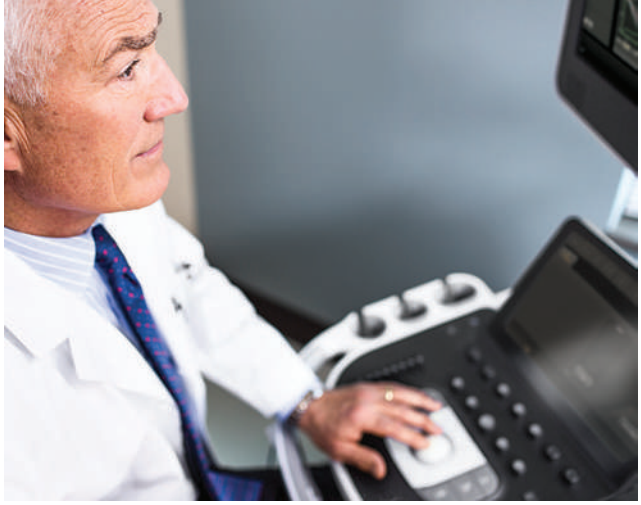
La division Échographie de Philips a appliqué le principe de la stratégie de défense en profondeur à ses systèmes échographiques EPIQ et Affiniti en mettant en œuvre une stratégie de sécurité à cinq couches :

- Coupe-feu
- Renforcement de la sécurité du système d'exploitation
- Protection contre les programmes malveillants
- Contrôle des accès
- Cryptage des données de patients

Chacune de ces couches joue un rôle important en vous aidant à déjouer les pirates, à contrer les programmes malveillants et à empêcher les accès non autorisés.

**Le coupe-feu bloque les ports inutiles**

Des politiques de coupe-feu strictes qui bloquent tous les ports superflus empêchent la communication avec des ordinateurs non autorisés, limitant le profil d'attaque qu'un pirate informatique pourrait essayer d'exploiter.



### Le renforcement de la sécurité du système d'exploitation désactive les services inutiles

Semblable en principe à un coupe-feu, le renforcement du système d'exploitation comprend l'identification de tous les services et fonctions superflus inclus dans le système d'exploitation et la désactivation de ceux qui ne sont pas requis par les systèmes échographiques. Le renforcement du système d'exploitation réduit la surface d'attaque en éliminant les services qui peuvent devenir vulnérables au fil du temps. Philips suit les guides techniques de mise en œuvre de la sécurité (STIG) fournis par la Defense Information Systems Agency (DISA).

### L'utilisation d'une liste blanche contre les programmes malveillants offre une protection exigeant peu de maintenance

La méthode traditionnelle de protection contre les programmes malveillants, le logiciel antivirus, nécessite des mises à jour fréquentes pour rester au fait des nouveaux virus et programmes malveillants lancés chaque jour. Les hôpitaux risquent d'être attaqués avant que les logiciels antivirus ne s'attaquent aux nouveaux programmes malveillants.

Pour atténuer ce risque, Philips a mis en œuvre la solution de contrôle des applications de McAfee. Cette solution, appelée « liste blanche », protège vos systèmes EPIQ et Affiniti contre les programmes malveillants en autorisant uniquement le fonctionnement des applications et bibliothèques connues et approuvées. Étant donné que la liste blanche ne nécessite pas de mise à jour constante comme les logiciels antivirus traditionnels, elle nécessite moins de maintenance et de mises à jour.

### Le contrôle des accès peut être adapté à vos besoins

On estime que 22 % des brèches de sécurité depuis 2009 étaient attribuables à des accès non autorisés[2]. Pour vous aider à contrôler l'accès aux données de vos systèmes échographiques, vous pouvez choisir, avec EPIQ et Affiniti, parmi trois niveaux de contrôle d'accès :

- **Aucune restriction (niveau par défaut) :** un utilisateur clinique peut effectuer des examens et accéder à tous les examens précédents qui sont stockés sur le système sans avoir à se connecter.
- **Verrouillage des données de patients seulement :** chaque utilisateur doit entrer des données de connexion valides avant d'accéder aux examens précédents, mais il peut effectuer un examen d'urgence sans avoir à se connecter.
- **Verrouillage complet du système :** chaque utilisateur doit se connecter avec succès avant de pouvoir effectuer une acquisition ou accéder aux renseignements sur le patient.

### Cryptage de données inactives et en transit

Toutes les données de patient stockées sur le disque dur des systèmes EPIQ et Affiniti peuvent être cryptées selon les exigences propres à votre établissement. De plus, vous pouvez choisir DICOM avec protocole TLS pour l'authentification des nœuds sans cryptage, DICOM utilisant le cryptage par protocole TLS ou une combinaison des deux pour crypter les données de patients en transit. (Cela nécessite une fonctionnalité correspondante sur votre système d'archivage et de transmission d'images.)

### La gestion des utilisateurs simplifie la maintenance des comptes

Avec les systèmes EPIQ et Affiniti, vous avez la possibilité de créer plusieurs comptes d'utilisateurs cliniques et plusieurs comptes d'administrateurs d'hôpital. Avec les deux systèmes, les administrateurs d'hôpital ont la possibilité de préciser des politiques relatives aux mots de passe conformément aux exigences et aux politiques locales en matière de sécurité des données. Les systèmes EPIQ et Affiniti peuvent s'interfacer avec votre environnement LDAP pour authentifier les utilisateurs et les groupes à l'aide de vos comptes réseau standards (p. ex., Active Directory).

### Les listes de contrôle fournissent des données pour l'analyse

La division Échographie de Philips a amélioré les capacités des systèmes EPIQ et Affiniti en matière de listes de contrôle. Les utilisateurs peuvent configurer le système pour qu'il envoie des listes de contrôle à un serveur de journal d'exploitation local à des fins de conservation, d'accessibilité et d'analyse approfondie. Pour faciliter l'analyse médico-légale, les utilisateurs peuvent assurer la cohérence des horodatages en synchronisant l'heure des systèmes échographiques avec l'heure du serveur de votre réseau.

## Options liées à la sécurité

### Fonctions importantes

- Politique en matière de coupe-feu bloquant tous les ports superflus
- Renforcement du système d'exploitation
  - Conformité des paramètres du système d'exploitation aux STIG de la DISA
  - Désactivation des services superflus
  - Désactivation de la fonction d'auto-exécution des supports amovibles
- Sécurité relative à l'exportation vers un support
  - Possibilité de désactiver la fonction d'exportation des données de patients vers un support amovible

### Option SafeGuard (offerte séparément)

- Protection contre les programmes malveillants utilisant la solution de contrôle des applications par liste blanche de McAfee

### Option Security Plus (offerte séparément)

- Niveau d'accès
  - Aucune restriction – les utilisateurs peuvent effectuer des examens et accéder à tous les examens précédents ainsi qu'aux données de MWL
  - Verrouillage des données de patients seulement – les utilisateurs peuvent effectuer des examens sans se connecter, mais ils doivent se connecter avec succès pour accéder aux examens précédents ou aux données MWL
  - Verrouillage complet du système – les utilisateurs et les administrateurs doivent se connecter avec succès avant d'accéder à toute partie du système
- Politique en matière de gestion des utilisateurs
  - Gestion des utilisateurs – local
  - Gestion des utilisateurs locaux
  - Prise en charge de multiples comptes d'utilisateurs distincts
  - Prise en charge de multiples comptes d'administrateurs distincts
  - Gestion des utilisateurs – à distance
  - Prise en charge de l'authentification Active Directory (AD) au moyen du protocole LDAP (le système ne peut être intégré au domaine)
  - Prise en charge de comptes individuels ou de groupes AD pour les utilisateurs et les administrateurs
  - Possibilité d'utiliser les protocoles LDAP ou LDAP sécurisé
  - Possibilité pour le client de configurer le système pour effectuer des liaisons authentifiées
- Politiques en matière de mots de passe
  - Capacité de préciser les politiques en matière de mots de passe pour les comptes locaux
  - Historique des mots de passe (de 1 à 8)
  - Longueur minimale du mot de passe (entre 6 et 14 caractères)
  - Longueur maximale du mot de passe (entre 6 et 63 caractères)
  - Durée de vie minimale du mot de passe (de 0 à 998 jours)
  - Durée de vie maximale du mot de passe (de 1 à 999 jours)
  - Complexité du mot de passe
  - Politiques en matière de blocage du compte
  - Seuil de blocage (entre 1 et 999 minutes)
  - Durée du blocage (entre 1 et 999 minutes)
  - Remise à zéro du compteur lié au blocage (minutes)
- Déconnexion automatique – déconnecte automatiquement un utilisateur après une période d'inactivité définie
  - Désactivé, 5, 10, 20, 30 ou 60 minutes*
- Cryptage du disque dur
  - 128 bits
  - 128 bits avec diffuseur
  - 256 bits
  - 256 bits avec diffuseur
- Message – connexion/avis juridique
  - Configuration d'un avis juridique / message s'affichant lors de la connexion
  - Configuration d'un titre pour l'avis juridique / le message s'affichant lors de la connexion
- Exportation des listes de contrôle
  - Possibilité d'exportation des listes de contrôle en utilisant le journal d'exploitation
  - Protocoles disponibles : UDP ou TLS

* Mettra en pause un examen actif


1. GALLAGHER, L. Présentation, 2012 Boston Privacy and Security Forum.
2. MCCANN, E. « HIPAA data breaches climb 138 percent », Healthcare IT News, 6 février 2014.
3. « Medical Device Security », Healthcare Information and Management Systems Society. http://www.himss.org/resourcelibrary/TopicList.aspx?MetaDataID=1581
4. « Guidance for Industry – Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software », U.S. Food and Drug Administration. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077812.htm





www.philips.com/ultrasound

Imprimé aux Pays-Bas.
4522 991 16001 * NOV. 2015