

# Cybersécurité dans le secteur de la santé : 10 façons de déjouer les cyberattaques et les violations de données dans le secteur des soins de santé.





## Les défis de la santé : Cela aussi passera

Du coronavirus au changement climatique, il est presque impossible de trouver des solutions aux menaces systémiques auxquelles l'homme est confronté à l'échelle mondiale sans l'aide de la médecine moderne. Alors que nous réalisons des découvertes majeures en quelques mois plutôt qu'en quelques années, nous nous rendons compte que les défis opérationnels dans le secteur des soins de santé ne cessent également d'évoluer. De l'adoption de la cybersécurité et de la transformation digitale à la réimagination de la santé publique et de la prestation des soins de santé, nous devons savoir si le secteur des soins de santé a ce qu'il faut pour une croissance soutenue qui pourrait améliorer largement nos vies ?

Dans cet e-book, nous nous concentrerons principalement sur les défis en matière de technologie de l'information et de technologie opérationnelle dans le domaine des soins de santé, à savoir les cousins IT et OT. L'informatique fait référence à la technologie des ordinateurs, y compris le matériel et les logiciels, et se concentre principalement sur les données. La technologie opérationnelle, en revanche, concerne les processus et les dispositifs qui, dans un environnement de soins de santé, comprennent souvent des équipements anciens et disparates. Nous analyserons l'état actuel des technologies de l'information dans le domaine des soins de santé et examinerons les moyens de minimiser les risques de cybermenaces dans le but de fournir des services de soins de santé transparents et sécurisés.



# Principaux obstacles informatiques rencontrés par le secteur des soins

Quels sont les défis que doit relever un administrateur informatique dans le secteur des soins de santé ?

01

Incidents de sécurité

02

Une violation de données mettant en danger la vie privée des patients et les informations confidentielles des professionnels

03

Manque de visibilité du réseau

04

L'adaptation à la transformation digitale

05

L'adoption des nouvelles technologies

06

Traitement de la conformité

## 01

## Réduire au minimum les incidents de sécurité

Les incidents de sécurité dans le secteur des soins de santé varient des attaques par ransomware qui endommagent les systèmes informatiques des hôpitaux à la compromission de la vie privée des patients, par exemple par une violation des informations personnelles identifiables.

Au-delà de ces perturbations opérationnelles dommageables, l'évolution des stratégies de cyberattaque ces derniers temps a eu de graves répercussions.

Le premier **décès documenté dû à une cyberattaque** est survenu en septembre 2020, lorsqu'un hôpital allemand victime d'une attaque par ransomware n'a pas pu accueillir un patient de 78 ans souffrant d'un anévrisme.

La raison : une défaillance des systèmes numériques chargés de coordonner les équipes médicales et les lits d'hôpital. Le temps qu'elle puisse être admise dans un autre hôpital, il était trop tard.

## 02

## Lutter contre les violations de données

Dans le secteur de la santé et de la pharmacie, deux groupes spécifiques sont principalement visés par les hackers. Le premier est celui des clients, c'est-à-dire des patients, et le second celui des fournisseurs ou des organismes de santé. Ces deux groupes possèdent leur propre ensemble de données et de ressources sensibles auxquelles il est possible d'accéder et d'altérer. Une part importante des données est également stockée et gérée par de multiples fournisseurs qui traitent les données pour le compte de l'hôpital. Avec autant de variables, et des données stockées et traitées par de multiples entités, il devient difficile de les localiser et de les sécuriser.

## 03

## Manque de visibilité sur le réseau informatique et opérationnel de l'hôpital.

Outre les biens informatiques, tels que les ordinateurs, les ordinateurs portables et les appareils mobiles, le réseau hospitalier se compose également de systèmes et d'appareils IoT, tels que les systèmes CVC, les systèmes de surveillance des patients, les équipements utilisés dans les unités de soins intensifs, etc. L'utilisation des appareils intelligents et des appareils IoT a également connu un pic, car de plus en plus d'appareils sont intégrés et connectés les uns aux autres.

Avec autant de types d'appareils différents sur le réseau, un administrateur informatique peut ne pas avoir une compréhension complète et les outils nécessaires pour répondre à tous les appareils, ce qui entraîne des angles morts informatiques. Ces angles morts du réseau sont essentiellement les zones sombres qui sont négligées, mais qui jouent un rôle majeur dans les systèmes informatiques et technologiques des hôpitaux. Les choses peuvent empirer lors d'une fusion ou d'une acquisition, car les organisations ont du mal à comprendre pleinement le comportement du réseau, des données et des applications. Dans ce processus, les angles morts se multiplient.

## 04

## S'adapter à la transformation digitale et à l'innovation perturbatrice

Si le secteur des soins de santé est fortement axé sur l'innovation, il a aussi la mauvaise réputation d'être le secteur le plus vulnérable aux cyberattaques. Le coût moyen d'une violation de données dans le secteur de la santé est de **9,23 millions** de dollars, soit près du double de celui du secteur financier, qui occupe la deuxième place en termes de coûts liés aux violations de données.

Alors que les hôpitaux et les équipes médicales tentent d'adopter de nouvelles technologies permettant de sauver des vies et des pratiques transformatrices, ils risquent également de laisser leurs infrastructures critiques sans surveillance, au gré des intrus et des acteurs de la menace. [Le Third-Party Breach Report](#) a révélé que le secteur de la santé était la victime la plus ciblée par les cyberattaques en 2021, avec 33 %, le secteur gouvernemental étant loin derrière avec moins de la moitié de ce chiffre. Mais l'investissement pour s'adapter aux nouvelles technologies peut être un énorme facteur limitant pour les organisations qui cherchent à adopter la transformation digitale.

## 05

### Conformité et organismes de réglementation

La plupart des organismes de santé considèrent les réglementations, telles que [l'HIPAA](#), comme des obstacles. En réalité, ces réglementations sont plutôt des anges gardiens qui aident les organisations à traiter les ePHI en toute sécurité, à l'abri des regards indiscrets des cybercriminels. S'il peut être difficile d'appliquer les politiques strictes des organismes de réglementation, le résultat en vaut la peine.



## Analyser les exploits récents dans le domaine de la santé et en tirer des leçons

Un écosystème de soins de santé typique est composé de multiples systèmes informatiques et OT allant des ordinateurs et serveurs aux appareils de niche tels que les moniteurs de chevet et les ventilateurs. Alors que les hôpitaux modernisent leurs infrastructures et leurs services publics avec des appareils innovants et des solutions IoT intelligentes, ils risquent également d'exposer ces actifs à divers attaquants et acteurs de la menace. Selon le rapport **2021 Cost of a Data Breach Report** compilé par le Poneman Institute, les organisations de soins de santé ont connu le coût moyen le plus élevé d'une violation de données pour la 11e année consécutive, et une augmentation de près de 30 % par rapport à l'année précédente.





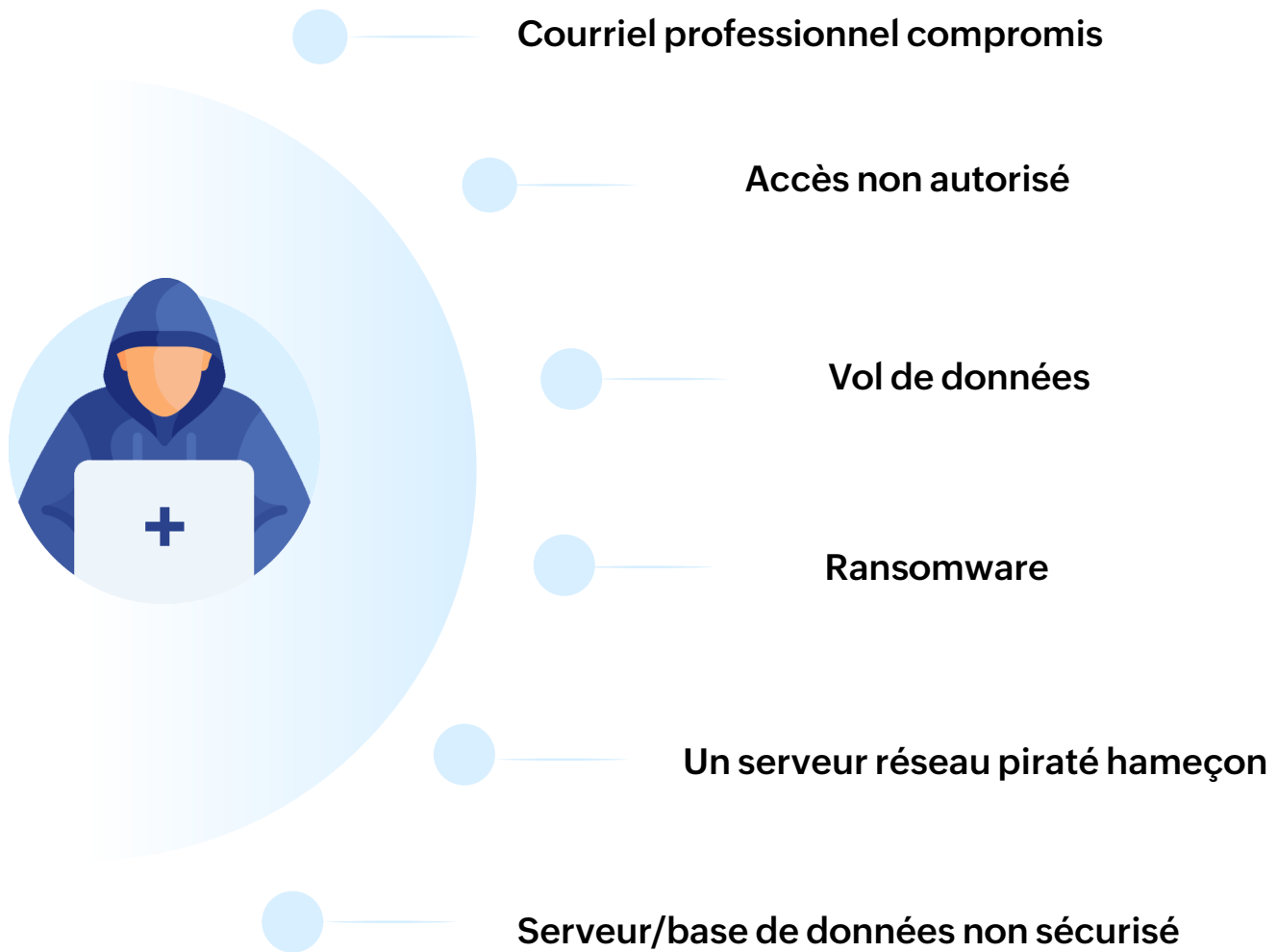
**Coût moyen d'une violation des données de santé : 9,23 millions** de dollars en 2021.

Une augmentation de 29.5% par rapport à 2020 (qui était de 7,13 millions de dollars)



**Le secteur de la santé est le plus exposé aux cyberattaques,** suivi des services Financiers

Selon des chiffres tirés du rapport [Breach of Unsecured Protected Health Information](#) du United States Health and Human Services Office, rien qu'en janvier 2022, plus de 2,3 millions de patients ont été touchés par des violations de données. Après avoir fait le tour et compris la nature des cyberattaques survenant dans le secteur des soins de santé, certaines des sources communes des brèches peuvent être attribuées à :



Au lieu de chercher le quoi et le comment de chaque cyberattaque ci-dessus, ce qui peut être fait par une simple recherche Google (ou en consultant [cet article](#)), essayons de réduire le risque posé par ces vecteurs et de protéger votre informatique contre les cyberattaques.



# 10 façons pour minimiser les **Cyberattaques** dans le secteur de la santé

## 01 Instaurer le Zero Trust

Le Zero Trust est un modèle de défense du réseau déployé pour restreindre l'accès au réseau et aux applications. Il s'agit d'un modèle de réseau fondé sur le principe selon lequel il ne faut faire confiance à personne. L'accès au réseau par Zero Trust (ZTNA) considère chaque dispositif du réseau comme hostile jusqu'à ce qu'il soit prouvé qu'il est digne de confiance, ce qui est contraire à l'approche traditionnelle du réseau qui considère qu'un dispositif est digne de confiance dès qu'il passe la couche de sécurité.

L'approche **ZTNA**, qui consiste à ne faire confiance à aucun utilisateur ou entité par défaut, peut être appliquée aux services VPN et proxy, ainsi qu'à d'autres services qui reposent sur la confiance entre le client et le serveur.

## 02 Renforcer le MFA

L'authentification multifactorielle (AMF) est un moyen d'ajouter une barrière de sécurité supplémentaire pour vérifier l'identité d'une personne pendant le processus de connexion. Lorsque l'authentification multifactorielle est activée, les utilisateurs doivent s'authentifier de deux façons ou plus pour accéder aux informations de leur organisation. Ainsi, même si le mot de passe d'un employé est compromis, son authentification alternative empêchera les acteurs de la menace de se connecter.

Ces facteurs d'authentification supplémentaires sont généralement un mot de passe unique basé sur le temps de réponse, un scan biométrique ou un code provenant d'une application d'authentification. L'AMF offre de nombreux avantages et constitue peut-être le mécanisme de cyberdéfense le plus simple pour les utilisateurs.

L'AMF est le **mécanisme de cyberdéfense** le plus facile à mettre en œuvre pour les organisations.

## 03

## Réduire la surface d'attaque

La surface d'attaque est l'ensemble des actifs physiques et digitaux de votre réseau par lesquels un utilisateur non autorisé peut accéder à votre réseau et extraire des données privées. Parmi les exemples courants de votre surface d'attaque figurent les ordinateurs, les commutateurs, les applications, le code, les ports, les serveurs et les sites web. Vous pouvez gérer et sécuriser votre surface d'attaque en traçant la carte de vos actifs dans le cloud et sur site, en découvrant les vulnérabilités ou faiblesses potentielles, en contrôlant les rôles des utilisateurs et les niveaux de privilèges.

Alors que le secteur des soins de santé devient plus intelligent et que des solutions innovantes nous permettent de franchir la prochaine génération de technologies, l'expansion de l'empreinte numérique des organisations ne doit pas être une source d'inquiétude. Il est préférable de surveiller et de sécuriser votre surface d'attaque existante plutôt que d'essayer de la réduire. En bref, l'adoption de nouvelles technologies ne devrait pas être entravée par la menace de cyberattaques potentielles.

## 04

## Patch et mise à jour automatique du système d'exploitation et des applications

L'application des derniers correctifs et la mise à jour des logiciels et des applications en temps voulu restent des éléments essentiels de tout plan de prévention des cyberattaques. Les responsables informatiques ne peuvent se permettre de minimiser l'importance des correctifs et des mises à jour de leurs logiciels.

Le timing étant crucial pour l'application des correctifs et des mises à jour logicielles, il est important d'automatiser ces processus pour limiter l'exposition de votre informatique de santé aux vulnérabilités. Les systèmes non corrigés restent une cible majeure des cyberattaques, c'est pourquoi **l'automatisation** des mises à jour logicielles et l'installation des correctifs dès leur publication est la bonne chose à faire.

## 05

### Assurer un contrôle rigoureux des dispositifs et des applications

Les attaquants qui utilisent un dispositif de mémoire pour pirater les systèmes hospitaliers dépassent le cadre de la scène de science-fiction. Les acteurs de la menace peuvent brancher des dispositifs sur vos ports USB et exécuter un script qui peut rendre les installations de santé inutilisables.

Une façon de limiter ce problème est de bloquer l'utilisation de périphériques de stockage externes. Pour ce faire, vous pouvez utiliser une **solution de contrôle** des périphériques qui vous permet de garder un œil sur les périphériques et les ports. Vous pouvez également surveiller les appareils connectés et analyser le comportement des utilisateurs dans votre établissement pour prévenir les menaces internes.

Outre la surveillance des actions potentiellement nuisibles entourant le matériel, vous pouvez également appliquer les mesures de sécurité des terminaux de votre entreprise en accordant des privilèges d'accès uniquement à un groupe particulier ou en restreignant **l'utilisation d'applications ou de logiciels non autorisés** sur les machines de l'entreprise.

## 06 Appliquer le contrôle d'accès

Du chirurgien en chef à l'infirmière débutante, tout le personnel hospitalier a besoin d'un accès rapide et facile aux données pour favoriser une expérience saine pour le patient. Un contrôle d'accès adéquat permet de s'assurer que chaque utilisateur dispose d'un accès approprié, ce qui évite de devoir accorder un accès administrateur à tout le monde, tout le temps.

Si le personnel de santé doit accéder à des ressources nécessitant un privilège d'administrateur, vous pouvez élever temporairement ses privilèges afin qu'il puisse accomplir son travail efficacement. Le contrôle d'accès permet de sécuriser vos données, d'assurer la responsabilité en suivant l'accès des utilisateurs et de garantir la conformité aux réglementations informatiques.

## 07 Remédier aux vulnérabilités

Les correctifs traditionnels ne traitent que les vulnérabilités connues qui sont documentées par les fournisseurs. D'autres vulnérabilités inconnues ne sont pas documentées et passent généralement inaperçues avant de faire des dommages.

Les solutions de **gestion des vulnérabilités** offrent une visibilité continue, détectent les faiblesses, évaluent les risques et remédient aux menaces. Ainsi, vous pouvez auditer et maintenir vos systèmes en conformité avec les normes de référence et rester à jour avec des informations détaillées sur les mesures correctives.

## 08

## Incorporer plusieurs couches de sécurité

Le périmètre de sécurité de votre entreprise doit comporter plusieurs couches de sécurité afin d'offrir plus de profondeur. En fonction des besoins, vous pouvez mettre en place plusieurs couches de sécurité avec différents niveaux de protection, comme par exemple :

- Pare-feu
- Systèmes de détection et de prévention des intrusions tels que les antivirus et les logiciels malveillants
- Systèmes de surveillance du réseau
- Authentification sécurisée

## 09

## Mettre en œuvre le cryptage et la sauvegarde des données

Le cryptage rend les informations sensibles de votre organisation, telles que les informations hospitalières et les dossiers des patients, illisibles pour toute personne qui ne devrait pas y avoir accès, comme les utilisateurs non autorisés ou les hackers. Cela est particulièrement utile lors d'une attaque par ransomware. Même si vos données sont compromises, les acteurs de la menace ne seront pas en mesure de divulguer leur contenu, mettant ainsi votre organisation à l'abri du danger.

Le cryptage est incomplet sans des sauvegardes de données appropriées. Il est essentiel de sauvegarder les informations importantes et sensibles de l'entreprise. En procédant ainsi, vous pouvez assurer une transition en douceur en cas de violation des données. Disposer d'un plan de sauvegarde et de récupération des données est également un processus essentiel.

Il s'agit de dresser la liste des éléments qui doivent être sauvegardés hors ligne sur des dispositifs de stockage, ou sur un stockage sécurisé sur le cloud, tels que les fichiers et dossiers de données, les images des systèmes d'exploitation, les bases de données des clients, les images des machines, les systèmes d'exploitation et les fichiers de registre. Les besoins de chaque service, de la biochimie à la radiologie, doivent être pris en compte. De nombreux fournisseurs proposent des solutions de sauvegarde et de récupération des données conformes à la loi HIPAA qui rationalisent ce processus et garantissent une perturbation minimale.

## 10

### Assurer la gestion et la protection des terminaux

Les terminaux peuvent être des ordinateurs de bureau, des téléphones portables, des tablettes, des routeurs et d'autres appareils, et ils peuvent accéder à un réseau depuis des sites sur place ou à distance. La protection des terminaux est un terme large qui comprend de multiples facettes telles que la gestion des vulnérabilités, la sécurité des navigateurs et le contrôle des applications.

**ManageEngine Desktop Central** est une solution de protection des terminaux qui protège vos terminaux de plusieurs façons, de la sécurisation des navigateurs des utilisateurs finaux au contrôle de vos périphériques et applications externes. Vous pouvez utiliser la suite complète de fonctions de sécurité avec un **seul add-on de sécurité**. En outre, Desktop Central peut gérer et surveiller de manière centralisée tous vos périphériques sur plusieurs plates-formes dans un réseau distribué. Un réseau bien sécurisé est un réseau bien géré.

# Feuille de route pour l'informatique de santé et les technologies opérationnelles

## 01

### Gagner en visibilité

- Déterminer la surface d'attaque en localisant les actifs.
- Identifier les angles morts du réseau
- Effectuer des contrôles de conformité
- Lancer une analyse des lacunes et des contrôles de santé
- Analyser les exigences

## 02

### Renforcer votre périmètre de sécurité

- Utiliser des pare-feu
- Activer le Zero Trust
- Installer des systèmes de détection des intrusions
- Déployer des systèmes de prévention des menaces
- Exploiter l'authentification sécurisée à l'aide de MFA
- Enact password management
- Utiliser les VPN

## 03

### Surveiller en permanence

- Déployer des outils de sécurité des terminaux
- Mettre en œuvre des stratégies de prévention des pertes de données
- Adopter un contrôle des dispositifs et des applications
- Appliquer l'accès privilégié
- Utiliser un scanner de vulnérabilité

## 04

### Assurer une disponibilité maximale des services de santé

- Assurer la disponibilité des services de santé essentiels
- Effectuer des sauvegardes de données
- Crypter les informations
- Trouver un équilibre entre cyber-résilience et productivité
- Utiliser la protection des terminaux

## 05

### Valider et évoluer

- Tester simultanément la sécurité du réseau
- Qualifier et vérifier les mises à niveau des dispositifs et les déploiements technologiques.
- Crypter les informations
- Mettre en place un environnement de test pour vérifier les dernières mises à jour et correctifs logiciels

# À propos de ManageEngine

## Gestion et sécurité unifiées des terminaux

ManageEngine UEMS développe des outils de gestion et de sécurité des terminaux pour les équipes qui cherchent à adopter le changement et à innover sans crainte. Notre solution de gestion unifiée des terminaux (**UEM**) automatise les tâches, fournit des informations et constitue un moyen fiable d'assurer la gestion et la sécurité de votre personnel. À partir d'un tableau de bord unique, vous êtes en mesure de sécuriser votre organisation en minimisant les risques sans affecter votre agilité. Travaillez plus intelligemment, restez informé et accélérez vos opérations sans aucun obstacle.

Obtenez ManageEngine UEM pour votre IT >>>

Retrouvez-nous sur



[commercial@pgsoftware.fr](mailto:commercial@pgsoftware.fr)

Suivez-nous sur 