# La cyberpandémie

## Attaques informatiques dans le secteur de la santé




panda

# La cyberpandémie

Aucun secteur ne peut être considéré plus noble et désintéressé que celui de la santé. Ce secteur est d'un caractère tellement humanitaire que même en situation de conflit, il respecte et protège l'être humain de toutes les façons dont il le peut. Il est très difficile d'imaginer que quelqu'un envisagerait de porter atteinte à l'apport social du secteur de la santé, voire de le cibler délibérément par des cyber-attaques très importantes.

Mais l'argent est le moteur du monde, et malheureusement, il ignore les classes, les conditions ou les secteurs. L'argent est la motivation principale de nombreux cybercriminels qui ont découvert

dans le secteur de la santé un filon majeur parmi les secteurs vulnérables.

Le secteur de la santé est tellement concentré sur d'autres préoccupations qu'il en a peut-être négligé sa sécurité informatique pendant de nombreuses années. Le fait qu'un domaine technologiquement avancé néglige la sécurité informatique pose un très gros problème.

# Un contexte de menaces

Les logiciels de rançon (ransomwares) sont devenus aujourd'hui l'une des menaces les plus répandues, un exemple de plus démontrant que l'appat du gain reste la motivation majeure des cybercriminels. Les logiciels de rançon sont une arme idéale pour attaquer des victimes qui disposent d'informations précieuses et sont prêtes à payer des rançons pour les récupérer.

Nous avons été les témoins d'attaques ciblant des secteurs spécifiques. Dans le secteur financier, par exemple, l'intérêt d'un pirate est plus qu'évident : vider les comptes bancaires. Même si la victime est la banque elle-même, l'objectif reste le même, comme nous l'avons vu il y a peu de temps dans le cas de la Banque centrale du Bangladesh.

D'autres secteurs peuvent ne pas subir des vols directs d'argent, mais l'objectif reste très clair. Comme le démontre  notre récent livre blanc « The Hotel Hijackers » (Les pirates d'hôtels), les cyber-attaques contre des magasins, des services et des hôtels ciblaient les données de cartes de crédit des clients en infectant les terminaux de points de vente.

Mais dans le secteur de la santé, les motivations ne sont pas aussi claires. Dans de nombreux pays, il est peu courant qu'un patient paye ces services par carte de crédit, car ceux-ci sont financés par l'État ou payés par des assurances privés. Et malgré cela, les hôpitaux, les cliniques et les laboratoires sont de plus en plus souvent victimes de cyber-attaques.

# Pourquoi les réseaux de santé sont-ils devenus la cible des cybercriminels ?

Selon le Bureau des droits civils des États-Unis, **il y a eu en 2015 253 failles de sécurité dans le secteur de la santé, qui ont affecté plus de 500 personnes et ont entraîné le vol de 112 millions de dossiers.** Selon IBM, ce secteur a connu en 2015 plus d'attaques que n'importe quel autre secteur.

Il est au cœur d'une révolution technologique. Le secteur de la santé évolue vers le stockage électronique de toutes les informations, ce qui est sans aucun doute très avantageux aussi bien pour les patients que pour le personnel soignant.

Ces informations sont disponibles en réseau pour être exploitables, par exemple, en cas de changement de praticien, et on peut y accéder facilement en consultant l'historique d'un patient. Cette facilité est aussi à la source du grave problème de sécurité posé au secteur de la santé.

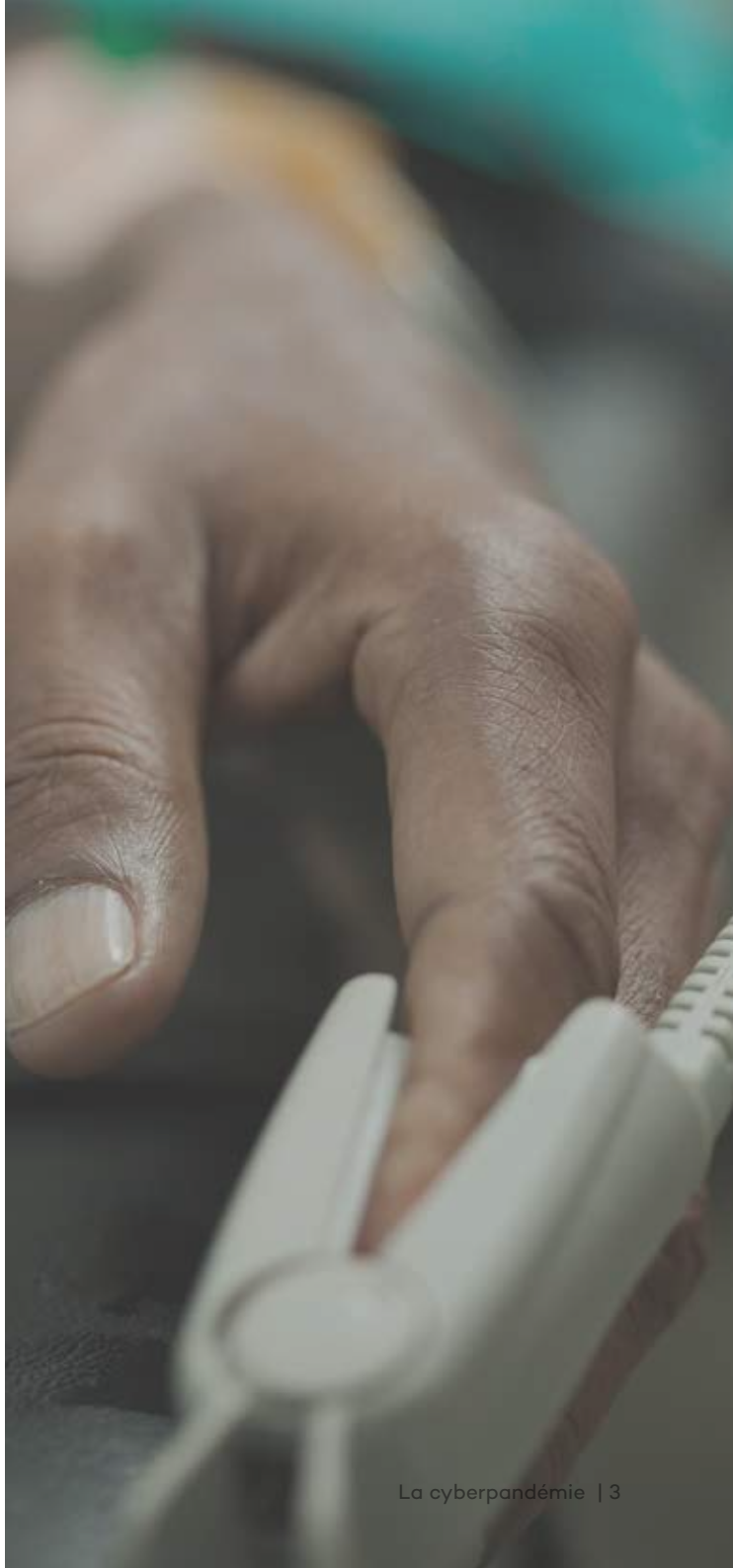
Les informations médicales sont très précieuses et hautement sensibles, et les contrôler peut rapporter gros.

Il est possible dans certains pays de vendre ces informations volées, et certaines entreprises telles que des centres de recherche ou des compagnies d'assurance sont mêmes intéressées par l'achat de ce type de données. Puis il y a évidemment le marché noir, dans lequel un historique de données clinique peut avoir beaucoup plus de valeur que des données de carte de crédit.

Les dossiers médicaux contiennent une grande quantité d'informations personnelles qui peuvent être utilisées ensuite pour mener des attaques ciblées. Songez aux personnes de pouvoir, qui sont particulièrement attentives au respect de leur vie privée et évitent de divulguer des informations personnelles en ligne sur les réseaux sociaux, etc. Même les plus prudentes ne peuvent empêcher des centres médicaux de conserver des dossiers les concernant. Si ces informations confidentielles tombent entre de mauvaises mains, comme celles d'un cybercriminel, leurs données personnelles peuvent se retrouver sur la place publique.

L'accès aux informations confidentielles d'études pharmaceutiques est également critique, car des entreprises seraient prêtes à payer très cher pour soustraire un brevet à l'un de leurs concurrents. Un autre exemple moins extrême pourrait consister à récupérer les informations privées d'un médecin afin de les utiliser pour prescrire illégalement des médicaments.

Historiques médicaux, résultats de tests, adresses e-mail, mots de passe, numéros de sécurité sociale, informations confidentielles d'employés, données de patients et d'entreprises : toutes ces informations sont d'une grande valeur et s'integrent dans les toutes dernières technologies. **Mais elles sont protégées par un système de sécurité qui est à présent obsolète.**



# Quelques attaques lucratives

## Croix-Rouge américaine

En 2006, un employé de la Croix-Rouge américaine à St. Louis a dérobé les identités et les informations de trois donneurs de sang. Cela aurait pu être beaucoup plus grave car cet employé avait accès aux données de plus de 1 million de donneurs

**Accès aux données de plus de 1 million de donneurs**

## Hôpital universitaire des enfants de Temple Street

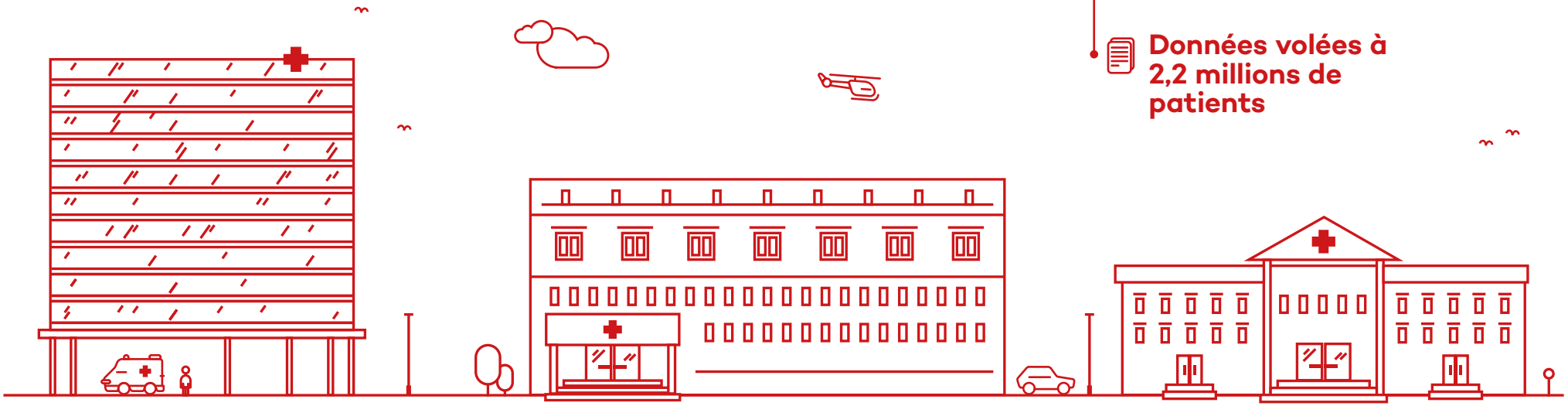
Un an plus tard, deux serveurs contenant les données de presque un million de patients ont été dérobés à l'Hôpital universitaire des enfants de Temple Street en Irlande. Ces serveurs contenaient les données des patients, notamment leur nom, leur date de naissance et la raison de leur admission.

**Vol des données de 1 million de patients**

## The University of Utah Hospitals & Clinics

En 2008, les Hôpitaux et cliniques de l'Université de l'Utah ont annoncé que les données de 2,2 millions de patients avaient été dérobées. Ces données se trouvaient sur des cartouches de sauvegarde, dans le véhicule d'un employé de l'entreprise de stockage travaillant pour l'hôpital. Dans ce cas précis, l'employé ne s'était pas conformé aux protocoles établis pour le transport des informations, et les données privées de millions de personnes ont été mises en péril

**Données volées à 2,2 millions de patients**



Jusqu'à présent, nous n'avons présenté que des cas spécifiques, non des attaques à grande échelle. Toutefois, les années passant, le paysage a considérablement évolué. **Selon une étude publiée par le Ponemon Institute, les attaques dans le secteur de la santé ont augmenté de 125 % ces 5 dernières années. Les cyber-attaques sont devenues la cause principale de la perte d'informations.**

Cette situation est préoccupante, particulièrement du fait que 91 % des organisations analysées par cette étude ont subi au moins une attaque aboutissant à une perte de données ces deux dernières années. 40 % ont reconnu avoir subi au moins cinq événements de perte de données sur la même période.

## Anthem Insurance Company

Une des attaques les plus tristement célèbres dans ce secteur s'est produite en février 2015. La deuxième plus grande compagnie d'assurance des États-Unis, Anthem, a subi une attaque ayant pour conséquence la perte de 80 millions de dossiers clients contenant des données extrêmement sensibles telles que des numéros de sécurité sociale.

En plus du vol d'informations et de la possibilité que ces informations soient vendues, il existe également les attaques de rançon, qui ont un impact économique direct sur leurs victimes. Les établissements tels que les hôpitaux, les entreprises pharmaceutiques et les compagnies d'assurance détiennent une si grande quantité d'informations précieuses que des attaques par rançogiciels ont affecté ce secteur avec une extrême virulence. Les cybercriminels portent sur ces établissements une attention presque disproportionnée. Ils recherchent sans cesse de nouvelles opportunités de pirater ces informations afin de pouvoir par la suite en tirer profit.

## Centre médical presbytérien d'Hollywood

En février 2016, le Centre médical presbytérien d'Hollywood à Los Angeles a déclaré un « état d'urgence interne » du fait que ses employés ne parvenaient plus à accéder aux dossiers médicaux, e-mails et autres systèmes.

Certains patients n'ont pas pu recevoir leur traitement et ont dû être transférés vers d'autres hôpitaux. La rançon demandée par les cybercriminels était de 3,7 millions de dollars. Le directeur général de l'hôpital est finalement parvenu à un accord et a payé environ 17 000 dollars pour pouvoir récupérer les fichiers pris en otage.

## MedStar Health à Baltimore

Le mois suivant, l'organisme MedStar Health basé à Baltimore a reconnu avoir dû déconnecter certains des systèmes de son hôpital à cause d'une attaque similaire.

**Ils ont dû déconnecter les systèmes de leur hôpital**

## Hôpital méthodiste d'Henderson

L'hôpital méthodiste d'Henderson, dans le Kentucky, a également été victime d'une attaque.

Dans ce cas, une rançon non confirmée de 17 000 dollars a été payée, bien que le bruit ait couru que le paiement avait été beaucoup plus élevé.

**$17,000 ont été payés**

## Prime Healthcare Management

L'opérateur américain de premier plan Prime Healthcare Management, Inc. a également été victime de cyber-attaques. Deux de ses hôpitaux (le Chinese Valley Medical Center et le Desert Valley Hospital) ont été attaqués par des cybercriminels. Cela a provoqué des coupures du réseau, et de nombreuses autres installations ont été affectées. Dans ce cas-ci, l'entreprise n'a pas payé la rançon.

**Deux de leurs hôpitaux ont été attaqués**

## Hôpital Lukas et clinique Arnsberg

Les hôpitaux américains ne sont pas les seules cibles. Les hôpitaux allemands ont aussi été victimes d'attaques similaires.

Selon le diffuseur international Deutsche Welle, plusieurs hôpitaux ont subi des attaques de rançon, comme l'hôpital Lukas à Neuss et la clinique Arnsberg en Rhénanie-du-Nord-Westphalie. Aucun de ces établissements n'a payé la rançon

**Plusieurs hôpitaux allemands ont été attaqués**

## Hôpital Kansas Heart

Il est à noter que payer une rançon dans un de ces exemples ne garantit pas que vos informations vous soient rendues. Cela apparaît clairement dans l'attaque de rançon subie par l'hôpital Kansas Heart en mai 2016. La direction de l'hôpital avait décidé de payer la rançon, mais les pirates, ayant réalisé la valeur des données, ont demandé un deuxième paiement pour rendre le reste des informations. L'hôpital a décidé de ne pas effectuer le deuxième paiement

**Les pirates ont demandé une deuxième rançon**

## « La prévention est le meilleur des remèdes »

Face à tous ces cas de piratage, le secteur de la santé devrait suivre ses propres conseils.

# Une réalité digne de la science-fiction

Comme les exemples ci-dessus le montrent, ces types d'attaques sont tout à fait en mesure d'arrêter le fonctionnement d'un hôpital en refusant l'accès à ces fichiers, en dérobant des milliers de dossiers et en prenant en otage les informations sensibles.

Mais il est une conséquence qui nous affecte tous d'encore plus près. Pratiquement tous les équipements médicaux (stimulateurs cardiaques, scanners, rayons X, pompes, respirateurs, etc.) sont connectés à un réseau. Il est tout à fait réaliste que ces appareils médicaux puissent être piratés d'une façon ou d'une autre.

En 2013, l'ancien vice-président américain Dick Cheney a révélé que ses médecins avaient désactivé la fonction de communication sans fil de son stimulateur cardiaque car ils avaient constaté qu'il était possible d'attaquer l'appareil à distance.

Un an auparavant, Barnaby Jack, un pirate néo-zélandais, avait montré lors d'une conférence sur la sécurité comment **un stimulateur cardiaque pouvait être piraté à distance, en produisant un choc électrique dangereux.** Barnaby avait mis au point une attaque susceptible d'affecter tous les stimulateurs cardiaques dans un rayon de 15 mètres.

Il avait aussi montré comment une pompe à insuline portable utilisée pour les patients diabétiques pouvait être altérée à distance, et conduire à l'injection d'une dose mortelle d'insuline par tous les appareils dans un rayon de 90 mètres.

Jack est décédé une semaine avant de pouvoir montrer comment pirater des cœurs artificiels. Dans la Black Hat Conference de 2013, il aurait

révélé comment modifier le rythme de ces implants.


**Rayons X, scanners, respirateurs, ...**

Des appareils médicaux actuellement non protégés

**Un stimulateur cardiaque a été piraté**

par une attaque pouvant envoyer un choc mortel.

**Des pompes à insuline ont été altérées**

pour injecter une dose mortelle.

Richard Rios a également entrepris de révéler les vulnérabilités des appareils médicaux. Un polype dans le système respiratoire avait obligé cet enquêteur à séjourner à l'hôpital Stanford pendant deux semaines. Pendant cette période, Rios s'est aperçu que son lit était connecté à un ordinateur. Des ceintures maintenaient ses jambes levées et une pompe lui injectait son médicament quotidiennement. Il a fait des recherches et découvert jusqu'à 16 réseaux et huit hotspots Wi-Fi sans quitter sa chambre.

Après être resté allongé dans son lit pendant plusieurs jours, il s'est levé et a marché jusqu'au couloir pour se dégourdir les jambes. Durant cette courte promenade, il a découvert un distributeur de médicaments informatisé. La distribution de tous les médicaments était en fait contrôlée par un ordinateur, auquel médecins et infirmières accédaient au moyen d'une carte d'identification codée. Avant de trouver cet appareil, Rios avait déjà compris que ce système possédait une vulnérabilité : un mot de passe incorporé (« en dur ») dans le code source du programme permettait à d'autres personnes de manipuler le distributeur de médicaments.

Avec son partenaire Terry McCorkle, Rios a identifié plus de 300 appareils vulnérables dans une quarantaine d'entreprises différentes de l'environnement médico-social. Les noms de ces entreprises n'ont jamais été rendus publics mais Rios est sûr que ces vulnérabilités existent toujours aujourd'hui.

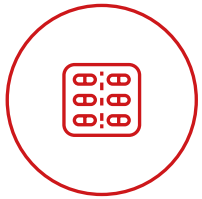
Dans le but d'exposer le danger lié à ces failles de sécurité, **Richard Rios a montré comment il était possible de manipuler à distance les pompes à médicaments utilisées dans les hôpitaux du monde entier.**

Il a piraté plusieurs de ces appareils pour modifier la dose médicamenteuse jusqu'à un niveau mortel. Rios a indiqué que cette opération pouvait être effectuée sur plus de 400 000 pompes toujours vulnérables dans le monde entier.

Presque au même moment, plusieurs analystes de TrapX Security à San Mateo, en Californie, ont commencé à surveiller les appareils vulnérables dans plus de 60 hôpitaux. **Ils ont infecté des centaines d'appareils par un programme remplaçant une partie de leur système d'exploitation.** Les machines restaient totalement opérationnelles, de sorte que personne n'avait remarqué qu'il y avait un problème, mais ces six mois ont permis à TrapX de surveiller toutes les activités de l'hôpital sur le réseau.

Parmi les appareils auxquels ils avaient accès figuraient des machines à rayon X, des machines de test sanguin et de gaz, des pompes et, bien sûr, des ordinateurs utilisés par l'équipe médicale. La plupart de ces ordinateurs étaient équipés de systèmes d'exploitation non supportés et donc plus vulnérables, comme Windows XP ou Windows 2000.

Le fait que la protection antivirus de la plupart de ces hôpitaux n'avait pas détecté l'infection TrapX indique que les appareils n'étaient également pas très bien protégés. Ils sont restés infectés jusqu'à ce que TrapX Security donne l'alerte.



**Des distributeurs de médicaments non contrôlés**

permettant de manipuler la distribution des médicaments.

**400.000 pompes de médicaments pouvant être altérées**

pour modifier le dosage des médicaments.

**Des centaines d'appareils infectés**

qui sont restés infectés pendant des mois.

# Comment ces attaques auraient-elles pu être évitées ?

Nous avons vu comment les criminels mènent des attaques pour dérober des informations sensibles, des dossiers médicaux, des études pharmaceutiques ou des données d'assurés. Nous avons vu comment ils accèdent à des adresses e-mail, des mots de passe et des numéros de sécurité sociale sans problème. Ou comment les logiciels de rançon prennent en otage des informations vitales en paralysant l'activité d'un hôpital tout entier, pour de l'argent.

Éviter ces attaques sophistiquées n'est pas une tâche simple. Nous entendons par là qu'un ensemble d'actions doivent être mises en œuvre : des ressources et des stratégies spécifiquement conçues pour assurer la sécurité des appareils, des données et des individus.

La première recommandation est fondamentale et cruciale : **s'appuyer sur une solution de cyber-sécurité offrant des fonctions de protection avancées et la capacité à détecter les menaces possibles et à y remédier.**

La majorité de ces attaques exploitent une caractéristique simple à expliquer mais complexe à résoudre : le manque de contrôle des systèmes informatiques.

Nous recommandons de mettre en œuvre un modèle capable de contrôler tous les processus actifs sur les appareils connectés au réseau de l'entreprise.

Avoir une visibilité totale de ce qui se passe vous permettra de contrôler tout comportement anormal sur vos systèmes et d'agir avant qu'un dommage ne survienne.

En outre, les entreprises qui gèrent des informations sensibles devraient **revoir leurs stratégies de gestion et leurs systèmes de contrôle du personnel pour ajuster les exigences de confidentialité et les adapter à la technologie disponible.**

Notre dernier conseil, nous le réitérons toujours, et il est beaucoup plus simple à suivre qu'il n'y paraît et pourtant rarement suivi : **vous devez toujours maintenir les systèmes d'exploitation et les programmes de votre entreprise à jour.** Cela ferme la porte à toutes les vulnérabilités connues, grâce aux correctifs publiés par les éditeurs.

**Il est recommandé d'avoir une stratégie et un contrôle à jour des appareils disponibles.** Ce type de système de gestion dispose d'outils de surveillance et d'inventaire susceptibles de vous aider à rendre la maintenance des équipements et des systèmes plus performante, plus uniforme, plus centralisée et plus sûre.

# La solution

Pour assurer la protection contre les menaces avancées et les attaques ciblées, les hopitaux ont besoin d'un système garantissant la confidentialité de leurs données, la protection de leurs informations, de leur réputation ainsi que de leurs systèmes existants.

Adaptive Defense 360 **est le premier et le seul service de cyber-sécurité à associer l'antivirus traditionnel le plus performant avec la capacité à classifier tous les processus exécutés.**

Adaptive Defense 360 peut détecter des logiciels malveillants et des comportements anormaux que d'autres services de protection ne sont pas en mesure de détecter, car il classifie tous les processus en cours et les processus exécutés.

Il assure ainsi la protection contre les logiciels malveillants connus et les menaces Zero Day, les menaces persistantes avancées et les attaques directes.

Avec Adaptive Defense 360, vous saurez toujours ce qui arrive à chacun de vos fichiers et chacun de vos processus.

Des graphiques détaillés montrent tout ce qui se passe dans le réseau : chronologie des processus d'attaque des menaces, circulation des informations, comment les processus actifs se comportent, comment le logiciel malveillant est entré dans le système, où il va, qui a voulu faire quoi et comment telle information a été obtenue, etc.

Adaptive Defense 360 permet de découvrir et de corriger facilement ces vulnérabilités tout en se protégeant également contre les rançogiciels , les cryptovirus et les autres éléments indésirables (tels que barres de navigation, logiciels publicitaires, modules additionnels...).

**Adaptive Defense 360 : une visibilité sans limite, un contrôle absolu.**

Plus d'informations à :

**pandasecurity.com/enterprise/solutions/adaptive-defense-360/**

# Pour plus d'informations :

**BENELUX**
+32 15 45 12 80
belgium@pandasecurity.com

**BRAZIL**
+55 11 3054-1722
brazil@pandasecurity.com

**FRANCE**
+33 (0) 1 46 84 20 00
commercial@fr.pandasecurity.com

**GERMANY (& AUSTRIA)**
+49 (0) 2065 961-0
sales@de.pandasecurity.com

**HUNGARY**
+36 1 224 03 16
hungary@pandasecurity.com

**ITALY**
+39 02 24 20 22 08
italy@pandasecurity.com

**MEXICO**
+52 55 8000 2381
mexico@pandasecurity.com

**NORWAY**
+47 93 409 300
norway@pandasecurity.com

**PORTUGAL**
+351 210 414 400
geral@pt.pandasecurity.com

**SOUTH AFRICA**
+27 21 683 3899
sales@za.pandasecurity.com

**SPAIN**
+34 900 90 70 80
comercialpanda@pandasecurity.com

**SWEDEN (FINLAND & DENMARK)**
+46 0850 553 200
sweden@pandasecurity.com

**SWITZERLAND**
+41 22 994 89 40
info@ch.pandasecurity.com

**UNITED KINGDOM**
+44 (0) 844 335 3791
sales@uk.pandasecurity.com

**USA (& CANADA)**
+1 877 263 3881
sales@us.pandasecurity.com

# Adaptive Defense 360

## Visibilité sans limite, contrôle absolu