Acronis

Des solutions de cyberprotection adaptées aux enjeux actuels du secteur de la santé

Comment protéger les données sensibles dans le secteur de la santé face aux cybermenaces actuelles ?

Le secteur de la santé fait l'objet d'une transformation numérique majeure. Il doit abandonner les méthodes dépassées de stockage d'informations sur les patients et adopter de nouvelles applications de diagnostic et de traitement générant une grande quantité de données. Les établissements de santé sont simultanément soumis à d'énormes pressions : il leur faut accroître les bénéfices, respecter les réglementations en matière de confidentialité, optimiser les soins des patients et améliorer l'interopérabilité avec les assurances, les fournisseurs, les prestataires partenaires, les établissements universitaires et les patients.

Le volume croissant de données médicales sensibles est disséminé entre différents emplacements physiques, équipements informatiques et réseaux (y compris des Clouds privés et publics). De nouvelles applications médicales majeures, comme la télémédecine, la télésurveillance des patients et la formation assistée par réalité virtuelle, accroissent le flux de données. D'autres technologies émergentes, comme l'intelligence artificielle, l'apprentissage automatique, l'Internet des objets et la blockchain, rendent la situation encore plus complexe. Sans compter le nombre croissant d'utilisateurs réclamant l'accès à ces données.

Dans le même temps, le secteur est submergé par une vague de nouvelles cybermenaces (violations de conformité, attaques par ransomware et campagnes de cryptopiratage). Il n'a jamais été aussi difficile de maintenir la disponibilité, l'accessibilité et la confidentialité des données de santé.

Le secteur de la santé est une cible de choix pour les cybercriminels et les États hostiles, encouragés par le fait que les attaques par ransomware sont particulièrement efficaces lorsque l'accès aux données sensibles est une question de vie ou de mort.

C'est ce qui explique la soudaine augmentation, ces dernières années, des attaques par ransomware très médiatisées, notamment celle visant le service britannique de santé publique (NHS), l'hôpital Adams Memorial, MedStar Health, Erie County Medical, entre autres. Les compromissions de données dans ce secteur se répètent ; des centaines de millions de dossiers médicaux et de dossiers de remboursement sont volés chaque année.

Le secteur est également dans le viseur des organismes chargés de l'application de réglementations en matière de confidentialité, comme le règlement général sur la protection des données (RGDP) de l'Union européenne ou la loi HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis, sans oublier certaines réglementations régionales. Les acteurs du secteur risquent également d'enfreindre des normes de réglementation des cartes de crédit, comme la norme PCI DSS (Payment Card Industry Data Security Standard).

L'utilisation de plus en plus répandue des dossiers médicaux électroniques renforce la nécessité d'une disponibilité permanente des données. Non seulement les interruptions de service mettent réellement en danger la sécurité des patients, elles sont aussi suffisamment coûteuses pour menacer la viabilité des établissements de santé. Selon le rapport Gartner « Downtime Cost Calculator for Data Center Disaster Recovery Planning, 28 February 2014 », le coût moyen d'une interruption de service, tous types d'établissements confondus, s'élève à 5 600 $ par minute, soit environ 300 000 $ par heure. Information Technology Intelligence Consulting conclut que **pour 98 % des établissements, une seule heure d'interruption de service coûte plus de 100 000 $ et entre 1 et 5 millions pour la plupart des gros établissements.**

Les équipes informatiques des établissements de santé sont confrontées aux mêmes problèmes que dans les autres secteurs : complexité croissante de l'infrastructure, difficultés à recruter et conserver des collaborateurs qualifiés, migration continue des applications vers des Clouds privés et publics, prolifération de terminaux mobiles (smartphones et tablettes), émergence de capteurs IoT, traqueurs de ressources et caméras Web. De plus, elles doivent réaliser une analyse en temps réel des nouvelles données.

Pour relever tous ces défis, il faut mettre en place une nouvelle stratégie de protection des données reposant sur les cinq éléments de la cyberprotection :

FIABILITÉ

Assurer qu'une copie fiable des données est toujours disponible

ACCESSIBILITÉ

Garantir que les données sont disponibles partout et à tout moment

CONFIDENTIALITÉ

Contrôler la visibilité et l'accès aux données

AUTHENTICITÉ

Créer une preuve indéniable qu'une copie est la réplique exacte de l'original

SÉCURITÉ

Protéger les données, les applications et les systèmes contre les cybermenaces

Ce livre blanc met ces principes fondamentaux de la cyberprotection en perspective avec les sept problèmes majeurs du secteur de la santé :

1. **Prévenir** les compromissions de données
2. **Se protéger** contre les attaques par malware, comme les ransomwares et le cryptopiratage
3. **Respecter** la conformité réglementaire
4. **Migrer** les applications critiques et le stockage vers des Clouds publics et privés
5. **Offrir** une disponibilité permanente des données
6. **Intégrer** les terminaux mobiles
7. **Renforcer** la protection des données sans accroître la complexité de l'infrastructure

ÉTAT DES LIEUX

La protection et la sécurité des données demeurent au rang de priorité absolue pour les établissements de santé. Dans son étude sur les violations de sécurité dans le milieu médical, la société de cybersécurité Protenus révèle qu'en 2017, on comptait plus d'une compromission de données par jour.

Cette même année, 5,6 millions de dossiers de patients ont été compromis. Or, il faut en moyenne 308 jours à une entreprise pour identifier un tel incident.

Pour prévenir les compromissions des données de santé, vous devez renforcer la protection de l'ensemble de votre infrastructure informatique, à savoir les systèmes physiques, machines virtuelles, services Cloud et terminaux mobiles. Parmi les contre-mesures de base : protection antimalware des terminaux, défenses contre des menaces réseau externes à l'aide de pare-feux et segmentation du réseau en utilisant des réseaux locaux virtuels (VLAN) ou un réseau software-defined afin de limiter la propagation des attaques aux réseaux internes. Il faut également disposer de sauvegardes et d'une fonction de reprise d'activité après sinistre au cas où une attaque aurait endommagé ou détruit des données sensibles, ou bloqué l'accès à des données. Vous devez donc disposer de sauvegardes et d'un espace de stockage sécurisés, idéalement chiffrés, sur site et dans le Cloud.

ATTAQUES PAR MALWARE

Selon les spécialistes en sécurité, les deux attaques par malware les plus répandues dans le secteur de la santé sont actuellement les ransomwares et le cryptopiratage.

Un ransomware infecte serveurs, ordinateurs de bureau et terminaux mobiles (généralement suite au clic d'un utilisateur sur une pièce jointe ou un lien malveillant dans un e-mail de phishing). Il chiffre ensuite les données qui s'y trouvent, puis demande un paiement en ligne pour fournir la clé de déchiffrement nécessaire au déblocage des fichiers de la victime. Dépourvus de contres-mesures de détection et de neutralisation des attaques par ransomware ou de fonction de restauration à partir d'une sauvegarde récente, de nombreux établissements de santé ont subi des temps d'arrêt qui ont mis en danger la vie des patients et coûté des millions de dollars en perte de productivité et opérations de remédiation.

Le cryptopiratage est une cyberattaque plus discrète, mais de plus en plus fréquente : les équipements médicaux infectés deviennent des zombies en réseaux qui extraient des cryptomonnaies pour le compte de cybercriminels. Le malware ne vole que les ressources de ses victimes (puissance de calcul, mémoire, électricité et climatisation), mais l'augmentation des coûts d'énergie et l'usure accrue des systèmes qui en résultent sont loin d'être négligeables. En outre, un malware de cryptominage injecte souvent d'autres menaces, comme un ransomware, dans le système qu'il infecte.

OBLIGATIONS RÉGLEMENTAIRES

Le contrôle réglementaire du secteur de la santé en a fait une cible privilégiée des cybercriminels spécialisés en malware, comme le ransomware. Le risque de non-conformité en cas de verrouillage de données médicales sensibles par une attaque par ransomware oblige souvent les victimes à payer la rançon pour récupérer l'accès aux données.

Pour la deuxième année consécutive, les attaques par ransomware ont représenté **plus de 70 % de l'ensemble des attaques par malware dans le secteur de la santé,** selon le rapport Verizon « 2019 Data Breach Investigations Report ».

MIGRATION VERS LE CLOUD DES APPLICATIONS ET DU STOCKAGE

Le secteur de la santé, comme les autres secteurs, commence une longue migration de ses données et applications principales vers un mélange d'infrastructure Cloud publique et privée. L'objectif est de réduire les coûts, de remplacer les équipements physiques obsolètes par des services aux coûts prévisibles et d'améliorer l'accessibilité et le partage des données depuis n'importe quel emplacement ou appareil. Pour de nombreux établissements, la migration sécurisée vers le Cloud des ressources de stockage et de protection des données, tout en préservant la confidentialité des données et la conformité réglementaire, n'est pas chose facile.

Pour la deuxième année consécutive, les attaques par ransomware ont représenté plus de 70 % de l'ensemble des attaques par malware dans le secteur de la santé, selon le rapport Verizon « 2019 Data Breach Investigations Report ».

DISPONIBILITÉ DES DONNÉES

En milieu médical, la santé et parfois la vie des patients dépendent de la disponibilité rapide et permanente des données.

Les équipes informatiques des établissements de santé doivent donc évaluer deux indicateurs : l'objectif de point de reprise (RPO) et l'objectif de délai de reprise (RTO). Le RPO indique le volume de données qu'un établissement peut se permettre de perdre à un moment donné, c'est-à-dire la fréquence des sauvegardes de ses données critiques. Le RTO indique la durée d'une interruption de service acceptable par un établissement entre la survenue de la défaillance et la récupération des données. En général, les entreprises arrivent facilement à déterminer les applications nécessitant des RPO et RTO plus stricts, et celles qui peuvent supporter des pertes de données plus importantes et des délais de récupération plus longs.

RISQUES ASSOCIÉS AUX ÉQUIPEMENTS PERSONNELS SUR LE LIEU DE TRAVAIL

L'intégration des appareils personnels des employés sur le lieu de travail présente de nombreux avantages pour le secteur de la santé, notamment en matière d'amélioration de la productivité et de la collaboration. Elle pose également un certain nombre de problèmes de protection des données : dorénavant, les données sensibles peuvent être stockées sur des terminaux plus exposés aux attaques, aux pertes ou aux vols.

UNE CYBERPROTECTION SIMPLIFIÉE

Les équipes informatiques du secteur de la santé ne font pas exception à la règle : elles ont de plus en plus de mal à recruter un personnel qualifié. Il est donc indispensable de réduire la complexité opérationnelle, notamment pour des opérations de routine comme la protection des données. Il est tout à fait contre-productif de déployer de multiples systèmes pour gérer un environnement informatique complexe nécessitant l'intervention de techniciens hautement qualifiés.

Acronis offre aux établissements de santé un ensemble complet de solutions de cyberprotection, stockage et reprise après sinistre à la fois simples d'utilisation, d'une grande flexibilité et parfaitement intégrées.

LES SOLUTIONS DE CYBERPROTECTION ACRONIS POUR LE SECTEUR DE LA SANTÉ

Acronis dispose de plusieurs options de protection contre les compromissions de données. Acronis Cyber Backup effectue un chiffrement des données sensibles en transit et au repos ; même en cas de compromission, les cybercriminels ne pourront pas exploiter les informations subtilisées.

Acronis Cyber Backup permet également de restaurer la totalité des données altérées, détruites ou verrouillées par une cyberattaque.

Acronis Cyber Cloud Storage prévient la compromission des données et des sauvegardes grâce à un formidable réseau de cyberdéfenses, notamment un chiffrement robuste des données et des sauvegardes (en transit et au repos), ainsi que des centres de données Cloud sécurisés certifiés.

SE PROTÉGER CONTRE LES ATTAQUES PAR MALWARE COMME LES RANSOMWARES ET LE CRYPTOPIRATAGE

Acronis Cyber Backup allié à Acronis Active Protection tire parti de l'intelligence artificielle et de l'apprentissage automatique pour détecter, bloquer et annuler les modifications suspectes apportées aux données, aux sauvegardes et aux agents de sauvegarde, et restaure les données à l'aide du cache. Il détecte et neutralise automatiquement les attaques par cryptopiratage.

Vous disposez ainsi d'une protection inégalée contre deux des menaces les plus répandues dans le secteur de la santé, ainsi que d'une protection contre les attaques jour zéro pour compléter les contre-mesures de base comme les solutions antivirus avec signature.

Acronis Cyber Backup renforce également son agent et ses archives de sauvegarde contre les attaques par malware afin qu'en cas de compromission, la capacité de l'établissement à restaurer rapidement ses données et à reprendre son fonctionnement normal ne soit pas affectée.

RESPECTER LA CONFORMITÉ RÉGLEMENTAIRE

Les fonctionnalités de chiffrement d'Acronis Cyber Backup alliées aux fonctions Acronis Active Protection et Acronis Cyber Cloud Storage vous aident également à respecter vos obligations réglementaires en protégeant la confidentialité des données médicales sensibles : en cas de compromission, ces données sont inexploitables par les cybercriminels. Les produits Acronis sont dotés de nombreuses autres fonctions et fonctionnalités natives qui, lorsqu'elles sont configurées et utilisées correctement, assurent votre conformité aux sections applicables des lois HIPAA et HITEC (Health Information Technology for Economic and Clinical Health Act) 2009. Bien qu'il n'existe aucun processus officiel de certification ou d'accréditation pour les lois HIPAA et HITECH, **Acronis possède un programme de sécurité et de conformité conçu pour faciliter la mise en conformité de ses clients.** Pour plus d'informations, consultez le Centre de ressources Acronis.

MIGRATION DES APPLICATIONS CRITIQUES ET DU STOCKAGE VERS DES CLOUDS PUBLICS ET PRIVÉS

Acronis Cyber Backup simplifie le processus de migration des applications médicales vers le Cloud grâce à la prise en charge d'un large éventail de services Cloud, systèmes d'exploitation (physiques et virtuels), ressources applicatives (sur site et dans le Cloud) et terminaux. L'ensemble des outils de gestion de données d'Acronis Cyber Backup simplifie et sécurise le déplacement des ressources entre des environnements physiques, virtuels et Cloud pour permettre une migration rapide et sûre vers de nouvelles plates-formes (Clouds privés, Acronis Cyber Cloud Storage et Clouds publics populaires proposés par Amazon, Google et Microsoft).

DISPONIBILITÉ PERMANENTE DES DONNÉES

Acronis Cyber Backup possède des fonctionnalités qui aideront les établissements de santé à gérer intelligemment les RTO et RPO dans leur environnement applicatif, notamment :

1. Acronis Instant Restore, qui aide à réduire les RTO et les RPO pour les applications les plus critiques.
2. Acronis Universal Restore, qui offre la flexibilité nécessaire pour restaurer un système sur du matériel vierge ou vers une plate-forme différente — par exemple d'une machine physique vers une machine virtuelle, si nécessaire.
3. La fonction intégrée Acronis Active Protection, qui élimine les interruptions de service et la dégradation des performances associées aux attaques par ransomware et cryptopiratage.

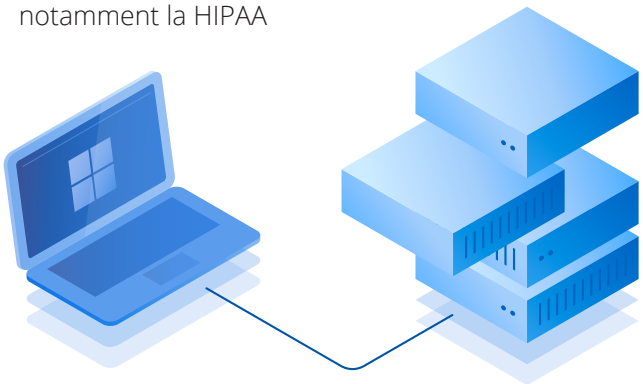
PROTECTION DES DONNÉES SENSIBLES SUR TOUS LES TERMINAUX

Acronis Files Advanced contribue à l'amélioration des soins aux patients et de l'efficacité opérationnelle, tout en veillant au strict respect des normes de sécurité et de conformité, notamment de la loi HIPAA (Health Insurance Portability and Accountability Act). Grâce à cette application, les collaborateurs, partenaires et sous-traitants des établissements de santé peuvent partager des documents sensibles et collaborer. L'établissement conserve un contrôle absolu sur l'emplacement, la gestion et la confidentialité des données.

Le moteur de règles Acronis Files Advanced propose des fonctions de gestion granulaire pour optimiser le contrôle et la conformité du contenu, des utilisateurs et des terminaux. La solution assure également une protection et une confidentialité complètes des données grâce à un chiffrement de bout en bout des données au repos et en transit. Acronis Files Advanced permet en outre aux équipes informatiques de prévenir les fuites d'informations, les compromissions des partages de données et les violations de sécurité grâce à des contrôles centralisés basés sur des règles.

Les professionnels de la santé, cabinets médicaux et patients peuvent utiliser Acronis Files Advanced pour consulter, modifier, créer et partager des données de santé sur différents terminaux (ordinateur de bureau et portable, tablette ou smartphone). Les cabinets médicaux peuvent en outre utiliser la solution pour :

- **Protéger** les données médicales et documents administratifs sensibles (p. ex. informations confidentielles et contrats avec des organismes de recherche, des universités et des entreprises, etc.)
- **Offrir** aux médecins, chercheurs et gestionnaires un accès sécurisé aux données médicales et un partage en toute simplicité depuis n'importe quel terminal
- **Sécuriser** les dossiers médicaux au repos et en transit
- **Collaborer** rapidement et efficacement dans les soins médicaux, en interne (au sein de l'établissement de soins) et en externe (avec des partenaires)
- **Surveiller** la consultation et le partage des fichiers médicaux
- **Respecter** les normes de sécurité et de conformité, notamment la HIPAA



RENFORCEMENT DE LA CYBERPROTECTION SANS ACCROÎTRE LA COMPLEXITÉ DE L'INFRASTRUCTURE

Acronis Cyber Backup simplifie et réduit le coût des opérations de cyberprotection grâce à une plate-forme unique qui protège l'ensemble des ressources d'un établissement de santé.

La solution peut gérer le stockage, la conservation, les sauvegardes et les opérations de restauration dans tout l'établissement, notamment les plates-formes Cloud, virtuelles, physiques et mobiles, ainsi que les ressources courantes de Microsoft, Oracle, Google, etc. Son interface puissante et intuitive et ses outils de surveillance simplifient la prise en main par des informaticiens peu expérimentés et permettent ainsi aux collaborateurs plus chevronnés de se consacrer à des projets plus stratégiques.

Enfin, le module complémentaire Acronis Disaster Recovery est une extension simple et facile à utiliser d'Acronis Cyber Backup. Il permet aux établissements de santé de restaurer instantanément les systèmes informatiques, applications et données critiques en cas de défaillance en basculant automatiquement sur les sauvegardes exécutées sur des machines virtuelles dans le Cloud Acronis sécurisé. Il prend en charge un basculement pour un large éventail de plates-formes informatiques et applications courantes, comme Windows Server, Linux, des plates-formes de virtualisation comme VMware, Hyper-V, KVM, XenServer et Red Hat Virtualization, et des applications Microsoft dont Exchange, SQL Server, SharePoint et Active Directory.

L'ARCHITECTURE CLOUD UNIQUE D'ACRONIS VOUS PERMET DE GARDER LE CONTRÔLE SUR VOS DONNÉES

TOUS LES TYPES DE GESTION

Logiciel de gestion déployé et contrôlé de façon indépendante, avec protection des données contrôlée par le client, un fournisseur de services, un revendeur, un partenaire ou un tiers, à partir d'un Cloud privé/public/de partenaire ou sur le site du client

TOUS LES TYPES DE PROTECTION

- Sauvegarde
- Stockage
- Reprise d'activité après sinistre
- Synchronisation et partage
- Notarisation/signature électronique
- Protection contre les ransomwares

TOUS LES TYPES DE RESSOURCES

- Sur site
- Cloud privé
- Cloud
- Données mobiles
- Applications
- Fichiers
- Systèmes virtuels

TOUS LES TYPES DE STOCKAGE

- Disque, bande
- NAS, SAN
- Cloud de partenaire
- Cloud privé
- Cloud public
- Acronis Cloud

TOUS LES TYPES DE DÉPLOIEMENT

- Site local
- Cloud privé
- Cloud de partenaire
- Acronis Cloud
- Cloud public

TOUS LES TYPES DE RESTAURATION

- Systèmes physiques
- Systèmes virtuels
- Systèmes mobiles
- Applications
- Fichiers
- Cloud

CONCLUSION

La rapide transformation numérique, les volumes croissants de données, l'interopérabilité indispensable et le contrôle renforcé par les actionnaires et les autorités de contrôle font la vie dure au secteur de la santé. Trouver le juste équilibre entre fiabilité, accessibilité, confidentialité, authenticité et sécurité des données n'est pas chose facile, en particulier lorsque des hordes de cybercriminels mettent tout en œuvre pour voler et rançonner des données médicales sensibles. Les établissements de santé doivent utiliser de nouvelles applications complexes, réduire les coûts et améliorer les soins aux patients, tout en relevant des défis informatiques de taille, comme la fidélisation du personnel, la migration vers le Cloud et la prolifération des terminaux mobiles et IoT.

Acronis peut les y aider grâce à sa gamme éprouvée de solutions de cyberprotection, stockage, synchronisation et partage sécurisés des fichiers et reprise d'activité après sinistre, optimisées pour le secteur de la santé.

Découvrez comment les solutions de cyberprotection d'Acronis sont déjà venues en aide à un hôpital américain ici.

Profitez d'une évaluation gratuite de **30 jours des produits Acronis** pour le secteur de la santé :

- Acronis Cyber Backup avec Acronis Active Protection ESSAI GRATUIT DE 30 JOURS
- Module complémentaire Acronis Disaster Recovery pour Acronis Cyber Backup ESSAI GRATUIT DE 30 JOURS
- Acronis Files Advanced ESSAI GRATUIT DE 30 JOURS