Comment les MSP peuvent-ils se constituer une clientèle dans le secteur dynamique des soins de santé

Les enjeux de la cybersécurité dans le secteur de la santé sont extrêmement élevés. Les défaillances système et l'interruption d'activité peuvent avoir des effets catastrophiques sur les patients. Malheureusement, de nombreux organismes de santé peinent à gérer efficacement la cybersécurité. Il s'agit d'une opportunité majeure pour les fournisseurs de services managés (MSP) d'intervenir pour aider et générer du chiffre d'affaires.

Les données du rapport Black Book Market Research 2025 illustrent l'ampleur du défi :

68 %

des prestataires de soins de santé déclarent ne pas pouvoir répondre de manière adéquate aux cyberrisques en raison de fonds insuffisants.

60 %

Près de 60 % des organisations de santé déclarent rencontrer des difficultés pour recruter et fidéliser des professionnels IT qualifiés.

28 %

des violations sont imputables à une erreur humaine, les menaces internes à l'organisation étant principalement dues au phishing.

En conséquence, l'adoption des services de sécurité managés dans les soins de santé a augmenté de 35 % entre 2024 et 2025. Pour les MSP, l'opportunité est importante et ne cesse de croître.[1]

La nécessité d'aller au-delà des services managés standard

Les environnements cliniques ont besoin de systèmes en fonctionnement permanent tels que les dossiers de santé électroniques, les plateformes d'imagerie et les outils de surveillance des patients. Toute défaillance de l'un de ces systèmes a un impact direct sur les patients. Les MSP peuvent aller au-delà du support informatique traditionnel et devenir des partenaires essentiels pour maintenir les systèmes critiques en fonctionnement, tout en garantissant la continuité clinique, la sécurité et la conformité.

Toutefois, réussir dans le secteur de la santé exige plus que des services managés standard. Les MSP doivent être en mesure de gérer des exigences réglementaires complexes, de sécuriser les systèmes médicaux traditionnels et d'assurer une interruption d'activité quasi nulle dans les environnements où chaque minute est précieuse.

[1] Black Book Market Research, The Black Book of Healthcare Cybersecurity: 2025 Edition

Défis métier et technologiques

Réussir dans le secteur de la santé n'est pas chose facile. Servir des clients du secteur de la santé présente une série de défis avec lesquels de nombreux fournisseurs de services ne sont pas nécessairement familiers. Les MSP sont confrontés à une combinaison unique de pression opérationnelle, de risques de sécurité et de complexité technique.

L'impact des interruptions d'activité sur la sécurité des patients

Les organisations de santé ne peuvent tolérer les pannes. Les défaillances système peuvent retarder les traitements, dérouter les patients et perturber les soins critiques. Et les interruptions d'activité coûtent cher. Le coût moyen d'une violation de données pour les organisations de santé s'élève à 7,42 millions de dollars, selon IBM.[2] Les MSP doivent garantir des objectifs de délai de restauration quasi nuls et une haute disponibilité systématique.

Élargissement de la surface d'attaque lié aux systèmes traditionnels

Les environnements de santé continuent de dépendre d'infrastructures héritées et d'appareils médicaux connectés. Il est souvent impossible d'appliquer des correctifs sur ces systèmes sans perturber les soins, si bien que les MSP se retrouvent responsables de la sécurisation de technologies obsolètes et vulnérables.

La valeur fort attractive des données de santé pour les cybercriminels

Les informations de santé protégées font partie des données les plus précieuses sur le Dark Web et dans la criminalité souterraine. Par conséquent, les organismes de santé sont des cibles de premier plan pour les attaques de ransomware et le vol de données. Les MSP doivent absolument offrir une protection avancée et une restauration rapide.

Intensification de la menace de ransomwares

Les attaques de ransomware visant le secteur de la santé continuent de se multiplier. Le FBI indique que les signalements d'incidents de ransomware visant des organisations de santé ont augmenté de 93 % entre 2024[3] et 2025.[4] Les attaquants exploitent l'urgence des opérations cliniques. Les MSP doivent mettre en œuvre des défenses multicouches incluant la prévention, la détection et une restauration fiable.

Environnements hybrides complexes

Les environnements IT de santé incluent des systèmes sur site, des plateformes cloud et des applications cliniques spécialisées. Le maintien d'une interopérabilité sécurisée entre des systèmes tels que les dossiers de santé électroniques (EHR, electronic health records) et les plateformes d'imagerie ajoute une complexité technique importante.

Prolifération des outils et inefficacité opérationnelle

De nombreux MSP s'appuient sur plusieurs outils non interconnectés pour la sauvegarde, la sécurité et la gestion. Cette approche augmente la charge opérationnelle, induit des lacunes de visibilité et réduit l'efficacité d'intervention en cas d'incident.

[2] IBM. (2025). Cost of a data breach report 2025: The AI oversight gap. IBM & Ponemon Institute.

[3] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2024). 2024 Internet Crime Report.

[4] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3). (2025). 2025 Internet Crime Report.

Défis sectoriels et opérationnels

Au-delà des obstacles techniques, travailler avec des clients du secteur de la santé implique des contraintes réglementaires et opérationnelles strictes.

Conformité réglementaire et pression liée à l'audit

Les MSP doivent satisfaire à des exigences de conformité strictes, en assumant souvent une responsabilité juridique. La préparation à l'audit et la documentation sont indispensables, mais peuvent mobiliser beaucoup de ressources.

Intégrité des données et enjeux de confiance

Les organisations de santé doivent garantir l'exactitude et l'intégrité des données cliniques. La corruption de données silencieuse et les dossiers incohérents peuvent entraîner de graves risques de diagnostic que les MSP doivent contenir.

Exigences en matière de création d'images et de performances des données

Les systèmes d'imagerie médicale génèrent d'immenses volumes de données qui doivent toujours rester accessibles instantanément. Les MSP doivent concevoir des architectures hybrides qui équilibrent performances et stockage sécurisé.

Contraintes de coûts

Les organisations de santé fonctionnent souvent avec des budgets informatiques limités malgré des besoins de sécurité croissants. Les MSP doivent offrir des niveaux de protection élevés tout en maintenant une bonne rentabilité.

Une plateforme conçue pour les MSP du secteur de la santé

Pour réussir dans le secteur de la santé, les MSP ont besoin d'une plateforme qui offre sécurité, protection des données et efficacité opérationnelle via une seule solution. Acronis Cyber Platform permet aux MSP de protéger l'ensemble de l'environnement clinique tout en simplifiant les opérations et en améliorant la rentabilité.

Avec Acronis Cyber Platform, les MSP peuvent :

Garantir la continuité clinique

- Veiller à ce que les systèmes critiques restent disponibles grâce à une restauration instantanée et à des délais de restauration quasi nuls.
- Maintenir l'accès aux dossiers de santé électroniques, aux systèmes d'imagerie et aux appareils au chevet du patient, même en cas d'incident de cybersécurité.

Sécuriser l'ensemble de l'environnement de santé

- Protéger les plateformes cloud modernes et les systèmes médicaux anciens avec un seul agent intégré.
- Réduire les risques sur les terminaux, les workloads et les dispositifs de l'Internet des objets médicaux (IoMT).

Simplifier la conformité et la préparation à l'audit

- Automatiser les processus de conformité avec des cartes de protection des données et un reporting prêt pour l'audit.
- Passer de services informatiques de base à des offres de conformité à forte valeur ajoutée.

Pouvoir restaurer en toute confiance

- Permettre une restauration exempte de malware grâce à des capacités de restauration sécurisée.
- Analyser et nettoyer les données de sauvegarde avant la restauration.

Réduire la complexité et améliorer les marges

- Éliminer la prolifération d'outils en consolidant la sauvegarde, la sécurité et la gestion au sein d'une seule plateforme.
- Améliorer l'efficacité des techniciens et accroître la rentabilité des services.

Acronis Cyber Platform : des fonctionnalités conçues pour le secteur de la santé

Acronis propose un ensemble complet de fonctionnalités conçues spécifiquement pour les environnements de santé :

Plateforme de cyberprotection unifiée : Acronis associe cybersécurité, sauvegarde, reprise d'activités après sinistre et gestion des terminaux en une seule plateforme, réduisant ainsi la complexité opérationnelle et améliorant la visibilité.

Sauvegarde et restauration avancées : les MSP peuvent protéger les systèmes critiques grâce à la sauvegarde d'image, au stockage immuable et à une restauration rapide adaptés aux environnements cliniques et d'imagerie.

Protection des terminaux et EDR : grâce à l'EDR (détection des menaces et réponse sur les terminaux), les fournisseurs de services peuvent sécuriser les postes de travail cliniques, les serveurs et les terminaux distants.

Conformité automatisée et protection des données : Acronis Cyber Platform permet aux MSP d'identifier et de protéger les données de santé sensibles grâce à des outils de découverte automatisés et à un reporting centralisé prêt pour l'audit.

Protection Microsoft 365 : de nombreuses organisations de santé utilisant cette fameuse suite de productivité, les MSP peuvent assurer la continuité de Microsoft 365 et des autres outils de communication et de collaboration, notamment l'e-mail, le stockage de fichiers et les plateformes de coordination des patients.

Prise en charge des systèmes existants : les MSP peuvent étendre la protection aux systèmes d'exploitation anciens et aux équipements médicaux spécialisés sans mises à niveau perturbatrices.

Sauvegarde de données d'investigation et intégrité des données : les fournisseurs de services peuvent capturer des données d'investigation numérique pour l'analyse d'incidents et garantir l'intégrité des dossiers grâce à des technologies de vérification basées sur la blockchain.

Avantages de la plateforme Acronis

Contrairement à des solutions ponctuelles assemblées de manière approximative, Acronis propose une plateforme nativement intégrée avec un point de gestion unique. Ainsi, les MSP peuvent :

- Offrir une cyberprotection complète couvrant tous les environnements de santé.
- Réduire les frais opérationnels et la prolifération des outils.
- Améliorer les délais de réponse et la qualité de service
- Développer des services de conformité et de sécurité à forte valeur ajoutée.
- Augmenter les marges tout en faisant évoluer les offres de santé.

Avec des fonctionnalités essentielles consolidées dans une seule plateforme, les MSP peuvent réduire les coûts et simplifier les opérations tout en assurant la résilience exigée par les organisations de santé.

Commencez à vous constituer une clientèle dans le secteur de la santé

Les organisations de santé ont besoin de partenaires de confiance capables de garantir la continuité, la sécurité et la conformité. Acronis Cyber Platform permet aux MSP de saisir cette opportunité en toute confiance.

↘ Réservez une démo pour découvrir comment Acronis accompagne les MSP travaillant avec des clients du secteur de la santé

↘ Commencez un essai pour fournir dès aujourd'hui des services de santé MSP résilients

Acronis

Pour en savoir plus : acronis.com