proofpoint.

FICHE SOLUTION

Protéger le secteur de la santé contre les ransomwares avec Proofpoint

Prévenez les attaques qui ciblent les personnes, défendez-vous contre les escroqueries basées sur l'IA et protégez vos données des extorsions

Présentation

Les ransomwares constituent l'une des menaces les plus perturbatrices auxquelles sont aujourd'hui confrontés les établissements de santé. Ces attaques ne se limitent plus au chiffrement des systèmes. Elles combinent désormais vol d'identifiants de connexion, exfiltration de données et extorsion afin de maximiser l'impact opérationnel et financier. Pour les hôpitaux et les prestataires de soins de santé, les conséquences vont bien au-delà des simples temps d'arrêt et affectent directement les soins prodigués aux patients, leur sécurité et la confiance qui leur est accordée.

La plupart des attaques de ransomwares commencent par un email ciblé, un compte compromis ou un message trompeur qui incite un utilisateur à agir. Les emails, les applications cloud et les plates-formes de collaboration demeurent les principaux points d'entrée, les pirates exploitant le comportement humain pour obtenir un accès initial.

L'IA accélère désormais cette menace. Les cybercriminels utilisent l'IA pour rédiger des messages de phishing extrêmement convaincants, usurper l'identité de personnes de confiance et mener des attaques à grande échelle contre les établissements de santé. Dans le même temps, les prestataires de soins de santé adoptent des workflows basés sur l'IA et l'automatisation, créant ainsi de nouvelles identités machines et des interactions automatisées que les pirates peuvent également exploiter.

Proofpoint aide les établissements de santé à contrer les ransomwares en empêchant la compromission des utilisateurs, en détectant les escroqueries basées sur l'IA et en protégeant les données sensibles contre l'exfiltration et l'extorsion.

Impact des ransomwares sur la prise en charge des patients

Les attaques de ransomwares ne sont pas de simples incidents informatiques ; elles impactent directement la sécurité des patients.

Lorsque les systèmes sont indisponibles ou que les données sont compromises, les conséquences sont immédiates et ont des répercussions considérables.

- Accès retardé ou perturbé aux dossiers médicaux électroniques (DME)
- Réorientation des urgences vers d'autres établissements
- Perturbations de la prise en charge des patients en soins intensifs et des workflows cliniques
- Accès impossible aux systèmes de diagnostic, aux résultats de laboratoire ou aux examens d'imagerie
- Divulgation de données patients sensibles, entraînant une perte de confiance

Cette suite de solutions fait partie de la plate-forme Human-Centric Security intégrée de Proofpoint et vise à sécuriser les personnes et les données dans les environnements de travail agentiques.

1,2 Mio $

Montant moyen des rançons versées dans le secteur de la santé[1]

Les défis posés par les ransomwares dans le secteur de la santé

Les ransomwares dans le secteur de la santé sont particulièrement dévastateurs, car ils affectent à la fois le fonctionnement des établissements et la prise en charge des patients. Les cybercriminels ciblent délibérément les environnements où les interruptions de service sont inacceptables.

Ces attaques suivent un schéma prévisible. Les cybercriminels utilisent le phishing ou l'ingénierie sociale pour voler des identifiants de connexion, accéder aux systèmes et se déplacer latéralement au sein de l'établissement.

Une fois à l'intérieur, ils identifient les systèmes et données de grande valeur, exfiltrent des informations sensibles, puis déploient un ransomware afin de maximiser leur pouvoir de pression et, éventuellement, de paralyser les opérations.

Ce qui a changé, c'est la manière dont ces attaques sont menées. Les campagnes de ransomware présentent désormais les caractéristiques suivantes :

- Très ciblées et axées sur des profils spécifiques tels que les médecins, les équipes financières et les cadres dirigeants
- Optimisées par l'IA, ce qui favorise des usurpations d'identité plus convaincantes et une mise au point plus rapide des attaques
- Basées sur les données, priorisant le vol de données patients et d'informations opérationnelles avant le chiffrement
- Étendues à l'ensemble des écosystèmes, grâce à l'exploitation des fournisseurs, des partenaires et des plates-formes partagées

Parallèlement, les établissements de santé doivent assurer la sécurité non seulement des utilisateurs, mais aussi des agents d'IA, des workflows automatisés et des identités non humaines qui interagissent avec les systèmes et données sensibles.

C'est cette convergence entre risques humains, menaces optimisées par l'IA et exposition des données qui rend les ransomwares modernes si efficaces et si difficiles à bloquer avec les contrôles traditionnels.

Une approche centrée sur les personnes et les agents pour assurer la sécurité des soins de santé

Les cyberattaques d'aujourd'hui ne ciblent pas uniquement la technologie. Elles exploitent des personnes et des agents de confiance. Pour contrer les ransomwares, vous devez réorienter votre stratégie de sécurité en vous concentrant sur les premières étapes de la chaîne d'attaque plutôt que sur la phase finale de chiffrement.

Étant donné que les ransomwares sont généralement distribués à la suite d'une interaction humaine (clic sur un lien, ouverture d'un fichier ou réponse à un message), la meilleure défense consiste à empêcher la compromission avant que les cybercriminels n'obtiennent un accès au système.

Cela nécessite une approche de la sécurité qui :

- Comprenne qui est ciblé
- Détecte les escroqueries dans les emails et les services cloud
- Sécurise les interactions basées sur l'IA et les processus automatisés
- Protège les données sensibles contre l'exfiltration

Proofpoint y parvient grâce à une plate-forme unifiée, centrée sur les personnes et les agents, qui établit des corrélations entre les comportements, les identités et les accès aux données afin de bloquer les ransomwares tout au long du cycle de vie de l'attaque.

1. Ponemon Institute, *Study on Cyber Insecurity in Healthcare (Étude sur la cyberinsécurité dans le secteur de la santé),* 2025.

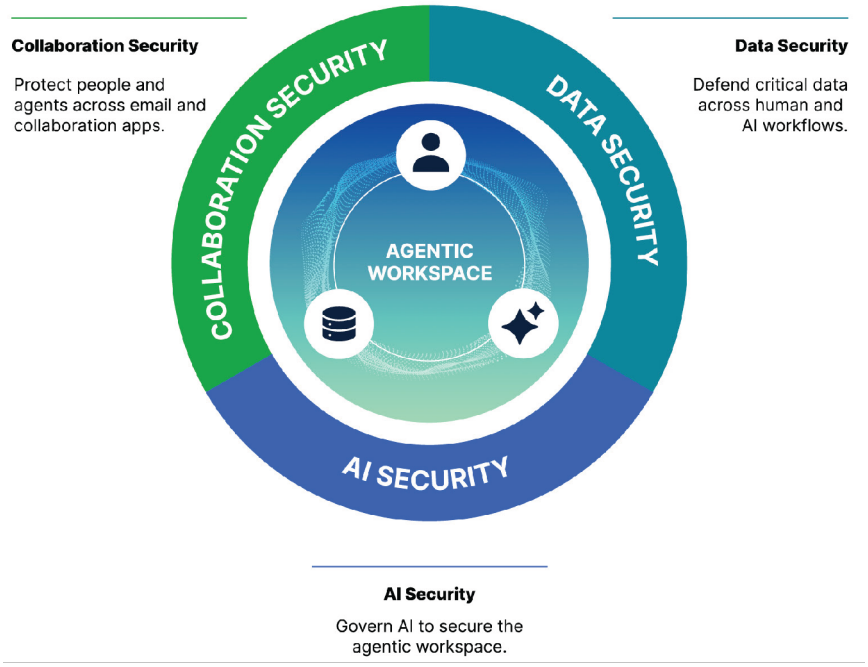

Figure 1. Une approche basée sur une plate-forme qui bloque les ransomwares tout au long du cycle de vie de l'attaque

Solutions

- Proofpoint Collaboration Security Prime
- Proofpoint Nexus
- Proofpoint Data Loss Prevention (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint ZenGuide

Comment Proofpoint peut vous aider

Plébiscité par 67 % des établissements de santé du classement Fortune 500, Proofpoint est le seul éditeur à proposer une plate-forme intégrée qui protège à la fois les personnes, les agents et les données.

Prévenir la compromission initiale

Proofpoint Collaboration Security Prime propose une approche de bout en bout pour bloquer les attaques qui ciblent les personnes et les agents au niveau de la messagerie électronique, des outils de collaboration, des applications cloud, des canaux Web et des réseaux sociaux. Optimisée par Proofpoint Nexus®, cette solution utilise l'IA avancée, l'analyse comportementale et la threat intelligence pour bloquer les attaques tout au long de leur cycle de vie — tant avant la remise qu'après le clic.

Se prémunir contre les escroqueries et les prises de contrôle de comptes basées sur l'IA

Proofpoint Account Takeover Protection et Proofpoint Insider Threat Management détectent les comportements suspects liés aux identités des personnes et des agents, notamment la compromission d'identifiants de connexion, l'utilisation abusive de privilèges, les déplacements latéraux et l'exfiltration de données. Grâce à la mise en corrélation des identités, des comportements et des mouvements de données, Proofpoint permet d'intervenir de manière plus rapide et plus précise, avant que les soins aux patients ne soient perturbés.

Assurer la sécurité des données patients

Les solutions Proofpoint Data Loss Prevention (DLP) préviennent les fuites de données accidentelles et malveillantes par le biais de la messagerie électronique, du cloud et des endpoints en offrant une visibilité étendue sur le comportement des utilisateurs et le contenu.

Proofpoint Adaptive Email DLP utilise l'IA comportementale pour analyser les modèles normaux d'envoi d'emails et fournir des avertissements contextuels en temps réel aux médecins et au personnel – évitant ainsi les messages adressés au mauvais destinataire et l'exposition de données sans perturber les soins.

Proofpoint Data Security Posture Management (DSPM) identifie l'emplacement des données sensibles, les personnes et les agents qui y ont accès, ainsi que les cas où des autorisations excessives ou à risque sont octroyées. Les prestataires peuvent ainsi réduire le risque d'exposition des données et adopter en toute sécurité l'IA et l'automatisation.

Proofpoint Satori™ complète Proofpoint DSPM en prenant en charge la gouvernance des accès aux données en temps réel dans les environnements de soins de santé. Proofpoint Satori surveille et contrôle en permanence l'accès aux données patients sensibles dans les banques de données cloud, les plates-formes d'analyse et les pipelines d'IA, sans perturber les workflows cliniques.

Grâce à Proofpoint Satori, les professionnels de santé peuvent : Identifier et classer les données patients et cliniques sensibles sur l'ensemble des plates-formes de données cloud

- Appliquer le principe du moindre privilège en matière d'accès pour les médecins, le personnel, les applications et les agents d'IA
- Détecter et corriger en temps réel les accès aux données à risque ou anormaux
- Appliquer des contrôles basés sur des règles pour protéger les données médicales tout en favorisant l'analyse, la recherche et l'innovation en matière d'IA

Réduire les risques liés aux utilisateurs grâce à un changement des comportements

Proofpoint ZenGuide propose des formations de sensibilisation à la sécurité informatique basées sur les rôles et les risques, conçues sur mesure pour les médecins et le personnel. Il renforce les comportements sûrs en s'appuyant sur des scénarios de menaces réelles pour les soins de santé sans ralentir la fourniture de soins.

Conclusion

Les attaques de ransomwares dans le secteur de la santé sont inévitables, mais ce n'est pas pour autant que leur succès est garanti. En se concentrant sur les premières étapes de la chaîne d'attaque et en s'attaquant aux causes profondes, les établissements de santé peuvent empêcher les ransomwares de perturber les soins.

Proofpoint permet aux établissements de santé de prévenir les attaques, de protéger les données patients et de préserver leur résilience opérationnelle grâce à une approche moderne et centrée sur les personnes et les agents en matière de protection contre les ransomwares.

proofpoint.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →