proofpoint.

FICHE SOLUTION

Protéger les prestataires de soins avec Proofpoint

Protéger les personnes, les agents d'IA et les données des patients pour assurer la sécurité et la résilience des soins

Présentation

Compte tenu de la numérisation, de la distribution et de l'automatisation croissantes des soins, les prestataires de soins de santé doivent composer avec une surface d'attaque qui s'étend de toutes parts. En raison de la pénurie de main-d'œuvre, le personnel est souvent trop occupé pour respecter les protocoles de sécurité. Les services cloud et les dispositifs médicaux connectés ajoutent de nouveaux points d'entrée d'attaque. Et les workflows basés sur l'IA introduisent de nouvelles vulnérabilités.

Les cybercriminels ont pris bonne note de ces changements et en tirent parti. Ils savent que les compromissions des données de santé ont souvent pour origine des personnes ou les agents d'IA qui agissent en leur nom. Ils se concentrent donc sur les attaques axées sur l'identité, l'ingénierie sociale et le détournement des accès légitimes.

Proofpoint aide les hôpitaux, les systèmes de santé, les cliniques et les réseaux de prestataires intégrés à protéger leurs médecins, leur personnel, leurs systèmes et leurs patients. Il sécurise l'ensemble de l'écosystème des personnes, des agents d'IA et des données. Nos solutions intégrées de cybersécurité et de conformité réduisent les risques de compromission, protègent les informations sensibles et soutiennent la fourniture de soins résilients et ininterrompus.

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 l'espace de travail agentique.

Un secteur de la santé riche en cibles de grande valeur

Les prestataires de soins de santé figurent parmi les principales cibles à l'heure actuelle. En plus d'être soumis à une pression intense, ils gèrent de gros volumes de données hautement sensibles, notamment :

- Données médicales personnelles, telles que dossiers médicaux, résultats de diagnostic et données de traitement
- Données personnelles
- Données financières, salariales et de facturation

Toutes ces informations revêtent un très grand intérêt aux yeux des cybercriminels et leur perte coûte très cher. Une compromission peut entraîner des sanctions réglementaires, des litiges, des atteintes à la réputation et des perturbations des soins et de la sécurité des patients.

Les prestataires de soins de santé sont également confrontés à des défis propres à la fourniture de soins :

- Les médecins ont besoin d'un accès rapide et ininterrompu aux systèmes.
- Les communications contiennent souvent des informations sensibles et urgentes.
- Les équipes de soins collaborent avec d'autres hôpitaux, cliniques et laboratoires ainsi qu'avec des tiers.
- Les contrôles juridiques, les audits et les investigations sont fréquents.

Les outils de collaboration par email et dans le cloud sont essentiels à la coordination des soins. Mais ils constituent aussi les principaux points d'entrée des cybercriminels.

Selon le rapport d'enquête 2025 sur lesncompromissions de données de Verizon, 60 % des compromissions impliquent une intervention humaine.

Défis liés à la cybersécurité pour les prestataires de soins

À mesure que les prestataires de soins modernisent leurs opérations, ils font face à des risques croissants.

Sécuriser les données patients et cliniques

Les prestataires de soins doivent protéger les données médicales, personnelles et financières au niveau de la messagerie, des plates-formes cloud et des endpoints. Toute compromission peut entraîner des violations des lois HIPAA et HITECH, des sanctions nationales pour non-respect de la confidentialité, des problèmes de conformité PCI DSS et des litiges coûteux.

Gérer les risques liés aux utilisateurs internes dans les environnements cliniques

Le risque accru associé aux utilisateurs internes est omniprésent. Non seulement le taux de rotation du personnel est important, mais il existe également une liste tournante parmi les membres du personnel, les sous-traitants et les résidents. Les dossiers médicaux électroniques font en outre l'objet d'un large accès. L'exposition accidentelle de données, le partage d'identifiants de connexion et l'utilisation abusive d'accès sont autant de facteurs pouvant entraîner des compromissions qu'il convient de signaler aux autorités.

Bloquer les usurpations d'identité et les prises de contrôle de comptes

Les prestataires de soins de santé s'appuient sur un écosystème complexe de tiers : laboratoires, vendeurs de dispositifs médicaux, fournisseurs, assureurs, organismes gouvernementaux, etc. Pour exploiter ces relations de confiance, les cybercriminels recourent au piratage de la messa-gerie en entreprise (BEC, Business Email Comprode fournisseurs et au phishing d'identifiants de connexion. Les boîtes email partagées et les comptes de service sont des cibles particulièrement attrayantes.

Réagir rapidement aux menaces avancées

Les équipes de sécurité font face à un nombre écrasant d'alertes. De plus, il n'est pas toujours aisé d'adapter les vérifications manuelles, en particulier lorsque les attaques touchent des centaines d'utilisateurs ou proviennent d'identités de confiance qui paraissent légitimes.

Se préparer à un environnement de soins basé dans le cloud

Les médecins accèdent de plus en plus souvent aux systèmes à distance et utilisent souvent leurs terminaux personnels pour ce faire. Soumettre l'intégralité du trafic à des contrôles de sécurité sur site n'est plus judicieux. Pour mettre en place une sécurité efficace, les équipes doivent pouvoir établir qui accède aux données sensibles, comment et pourquoi.

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

Ensemble, les personnes et les agents forment désormais la surface opérationnelle de la prestation de soins de santé. Bien que les médecins et le person-nel soient chargés de mettre en place les processus métier et de soins, ils bénéficient également d'une assistance. De nombreuses tâches sont désormais exécutées par des agents non humains, notamment :

- Boîtes email partagées et comptes de service
- Identités et API cloud
- Workflows d'automatisation et systèmes basés sur l'IA
- Dispositifs médicaux connectés
- Applications cliniques et métier telles que Epic

C'est pourquoi les cyberattaques d'aujourd'hui ne ciblent pas uniquement la technologie. Elles exploitent des personnes et des agents de confiance.

Malheureusement, les outils de sécurité traditionnels basés sur le périmètre sont incapables de distinguer les actions légitimes des comportements malveillants. C'est plus particulièrement vrai lorsque les cybercriminels utilisent des identités compromises plutôt que des malwares pour leurs activités frauduleuses.

Proofpoint sécurise cet environnement en corrélant les identités, les comportements et les accès aux données, tant pour les personnes que pour les agents. Cette approche permet d'éliminer les angles morts que les cybercriminels exploitent activement.

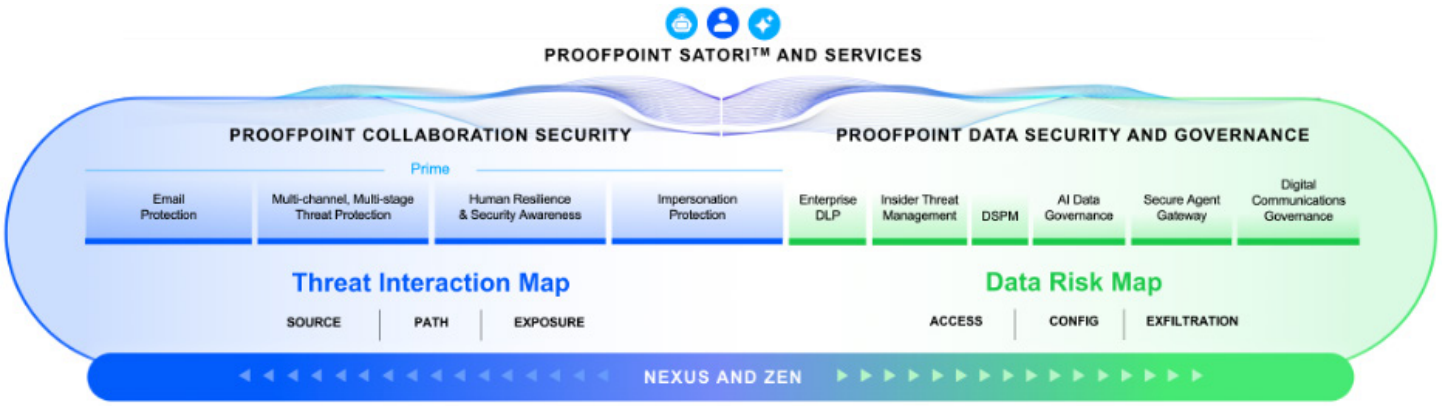


Figure 1. Les solutions Proofpoint sécurisent l'ensemble de l'écosystème constitué des personnes, des agents d'IA et des données.

Produits

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- 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 Digital Communications Governance
- Proofpoint ZenGuide

Comment Proofpoint peut aider les prestataires de soins

Adopté 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.

Cette section examine les nombreuses façons dont nous pouvons aider.

Protection contre les ransomwares et autres menaces avancées

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 — avant la remise, après la remise et au moment du clic.

Sécurisation des communications critiques par email et via des applications

Les prestataires de soins ont tendance à s'appuyer sur des emails générés par le système pour des workflows cliniques et opérationnels essentiels, notamment :

- Notifications aux patients et rappels de rendez-vous
- Coordination des soins et alertes cliniques
- Relevés de facturation et communications financières
- Mise en conformité, rapports et messages administratifs Ces communications sont souvent envoyées en grand nombre par des applications de confiance et doivent être :
  - Délivrées de manière fiable
  - Authentifiées et approuvées par les destinataires
  - Sécurisées et conformes

Proofpoint Secure Email Relay permet aux prestataires de soins d'envoyer en toute sécurité de gros volumes d'emails générés par des applications tout en protégeant leurs patients, leurs partenaires et leur établissement contre l'usurpation d'identité et les fraudes. Proofpoint Secure Email Relay :

- Permet la distribution d'emails conformes à la norme DMARC à partir d'applications critiques telles que Epic, ServiceNow et d'autres plates-formes cliniques et métier
- Protège les emails générés par le système contre l'usurpation d'identité et l'utilisation abusive de domaines similaires
- Garantit la confiance et l'intégrité des communications opérationnelles et avec les patients
- Réduit les risques liés aux emails provenant d'applications compromises ou mal configurées

En assurant la sécurité des expéditeurs non humains, Proofpoint Secure Email Relay étend le modèle de cybersécurité centré sur les agents de Proofpoint. Il veille à ce que les communications essentielles en matière de soins de santé demeurent fiables, conformes et résilientes.

Protection des données des patients Les solutions Proofpoint Data Loss Prevention (DLP)

prévientnt 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. Il prévient les messages adressés au mauvais destinataire et l'exposition des données sans perturber les soins prodigués.

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 — notamment au niveau des banques de données cloud, des plates-formes d'analyse et des pipelines d'IA — sans perturber les workflows cliniques.

Grâce à Proofpoint Satori, les prestataires peuvent :

- Identifier et classer les données patients et cliniques sensibles sur les plates-formes 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

Détection des compromissions et des utilisations abusives à grande échelle

Proofpoint Account Takeover Protection et **Proofpoint Insider Threat Management** détectent les comportements suspects liés aux identités des personnes et des agents. Ils détectent les compromissions d'identifiants de connexion, les utilisations abusives de privilèges, les déplacements latéraux et les exfiltrations 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.

Mise en conformité et préparation aux éventuels litiges

Les solutions P**roofpoint Digital Communications Governance** simplifient le respect des lois HIPAA et HITECH et des exigences en matière de rétention. Elles veillent à ce que les communications cliniques et métier soient capturées, consultables et disponibles pour les audits, les enquêtes et les investigations électroniques (e-discovery).

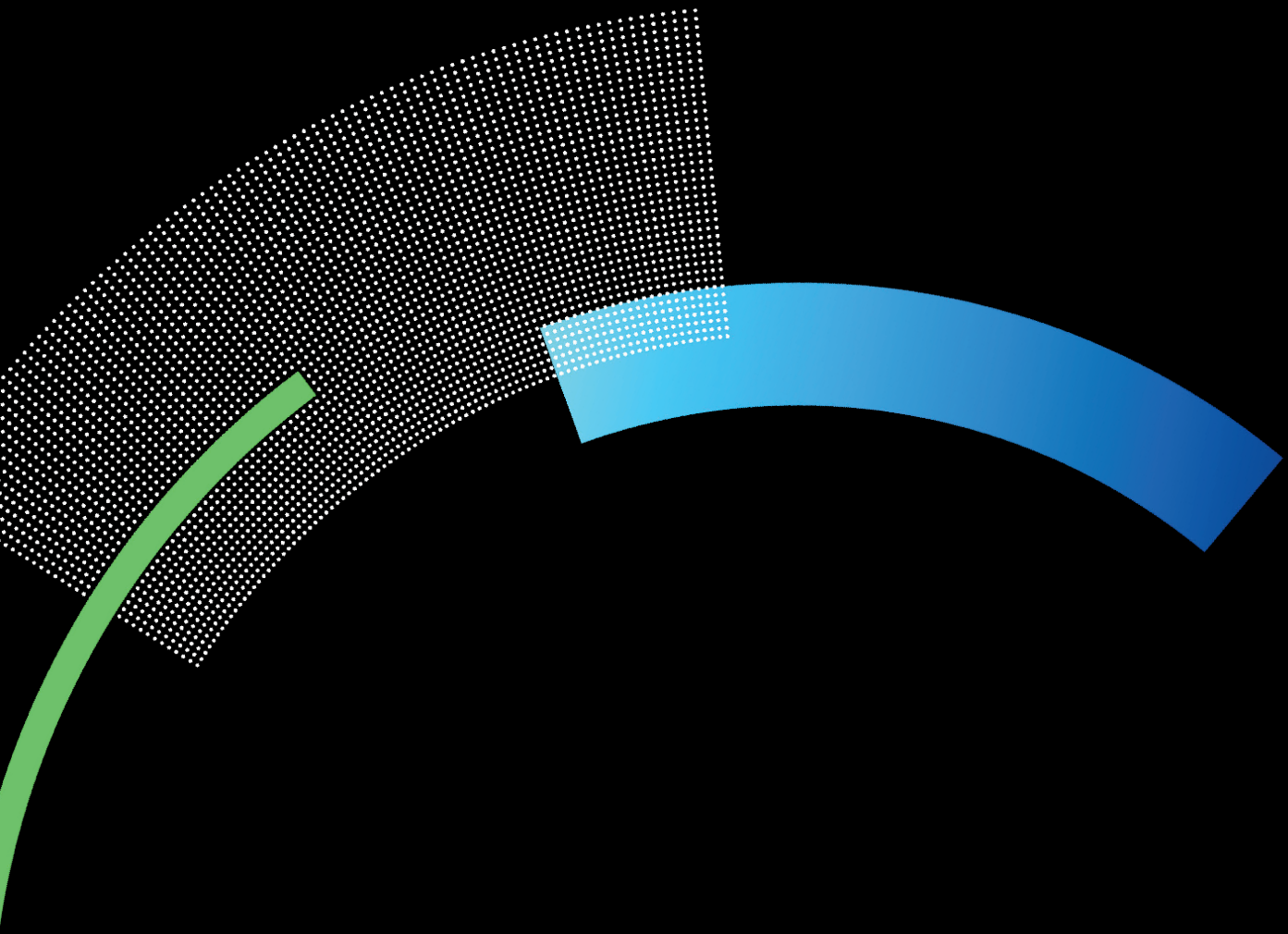
Réduction des risques grâce à un changement des comportements

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

Proofpoint a toujours protégé les personnes. Mais aujourd'hui, notre plate-forme de sécurité centrée sur les personnes et les agents va plus loin encore et étend la protection à l'ensemble des interactions entre les collaborateurs, les données et les agents d'IA. Elle garantit ainsi contrôle, conformité et liberté d'embrasser l'innovation.

Grâce à Proofpoint, les prestataires de soins peuvent réduire le risque de compromission, protéger les données des patients, préserver la conformité et fournir des soins résilients et ininterrompus dans un paysage des menaces complexe.



proofpoint.

À propos de Proofpoint, Inc. Proofpoint, Inc. est un leader mondial de la cybersécurité centrée sur les personnes et les agents, qui sécurise la manière dont les personnes, les données et les agents d'IA se connectent via la messagerie électronique, le cloud et les outils de collaboration. Proofpoint est un partenaire de confiance pour plus de 80 entreprises du classement Fortune 100, plus de 10 000 grandes entreprises et des millions de petites entreprises. Il les aide à bloquer les menaces, à prévenir les fuites de données et à renforcer la résilience des personnes et des workflows d'IA. La plate-forme de collaboration et de sécurité des données de Proofpoint aide les entreprises de toutes tailles à protéger et à responsabiliser leurs collaborateurs tout en adoptant l'IA en toute sécurité et confiance. Pour en savoir plus, consultez le site www.proofpoint.com/fr.
Suivez-nous : LinkedIn

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →