proofpoint.

FICHE SOLUTION

Sécuriser les données de santé avec Proofpoint

Protégez les données des patients contre les menaces internes, les fuites de données et les risques liés au cloud

Principaux avantages

- Identification et limitation des menaces liées aux utilisateurs internes négligents, compromis ou malveillants
- Protection évolutive sur tous les éléments de la surface d'attaque à mesure que les empreintes numériques s'amplifient
- Prévention des fuites de données au niveau de la messagerie, du cloud et des endpoints

10 %

des attaques de ransomwares de ces deux dernières années ont ciblé le secteur de la santé.

Source : SC Media

Le secteur de la santé est depuis longtemps une cible de prédilection des cybercriminels. En effet, les établissements de ce secteur traitent de nombreux types de données, notamment des éléments de propriété intellectuelle, des données d'essais cliniques, des données médicales protégées et des données financières personnelles. Les cybercriminels disposent de nombreuses options pour tirer profit d'une attaque contre n'importe lequel d'entre eux. En adoptant le cloud, le télétravail et la télésanté, les établissements de santé étendent également leur surface d'attaque. Et comme les collaborateurs du secteur travaillent dans des conditions de stress de plus en plus intenses, les établissements sont confrontés à un risque accru émanant d'utilisateurs internes tant malveillants que bien intentionnés.

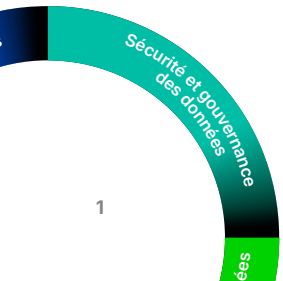
Proofpoint propose une approche centrée sur les personnes pour protéger les données sensibles au sein de réseaux médicaux distribués. Nos solutions de sécurité des données offrent une visibilité et un contrôle inégalés sur les données sensibles. Nous vous aidons à protéger vos collaborateurs et leurs données sensibles contre les divulgations accidentelles, les attaques malveillantes et les risques internes. Notre bouclier de protection s'étend aux services cloud, à la messagerie électronique, aux endpoints et aux partages de fichiers sur site. Votre établissement peut mieux gérer les risques pesant sur les données tout en gagnant du temps et en réduisant les coûts opérationnels.

Une menace grandissante

À l'instar de nombreuses entreprises, les établissements de santé stockent des informations de cartes de paiement et d'autres informations financières. Cependant, ils gèrent également d'énormes quantités de données médicales protégées et de données de recherche clinique. Ils conservent même des données relatives aux subventions publiques. Tout cela fait d'eux une cible lucrative pour les cybercriminels.

Par ailleurs, les empreintes numériques des établissements de santé sont de plus en plus complexes. Le secteur de la santé héberge aujourd'hui de plus en plus de services dans le cloud. Le nombre croissant de dispositifs IoT médicaux permet peut-être de sauver des vies, mais il accroît également la surface d'attaque. Le foisonnement des options de télésanté signifie également que les données sensibles circulent de plus en plus souvent hors du périmètre du réseau. À cela s'ajoute la propension des collaborateurs à travailler à distance lorsque les règles de travail hybride les y autorisent.

Malheureusement, les cybercriminels ont suivi leurs cibles hors du périmètre. Au cours des deux dernières années, le secteur de la santé a essuyé 10 % de toutes les attaques de ransomwares, et les cyberattaques ciblant le secteur médical ont augmenté de 32 %[1]. Ces chiffres sont bien plus élevés que pour les autres secteurs et industries. Les compromissions de données sont également plus coûteuses dans le secteur de la santé que dans tout autre secteur.



1. Shaun Nichols (*SC Media*), « Cyberattacks targeting medial organizations up 32% in 2024 » (Les cyberattaques ciblant les établissements médicaux ont augmenté de 32 % en 2024), février 2025.

32 %

Les cyberattaques ciblant les établissements médicaux ont augmenté de 32 % au cours des deux dernières années.

Source : SC Media

9,77 Mios $

En 2024, une compromission des données de santé coûtait en moyenne 9,77 millions de dollars.

Source : Ponemon Institute et IBM

En 2024, une compromission de données dans le secteur de la santé a coûté en moyenne 9,77 millions de dollars[2]. Ce coût peut inclure les rançons versées, la correction des systèmes, les amendes pour non-conformité, les litiges et la dégradation de l'image de marque. Les indisponibilités système ou la compromission de l'intégrité des données peuvent également avoir des conséquences négatives sur la santé. Elles peuvent même entraîner la perte de vies humaines.

Défis liés à la sécurité des données

Les hôpitaux, cliniques, compagnies d'assurance-maladie et entreprises de biotechnologie doivent faire de la sécurité des données une priorité absolue. Ces établissements doivent protéger leurs propres données de recherche et éléments de propriété intellectuelle. Cependant, ils doivent également préserver les données médicales protégées, personnelles et de cartes de paiement de leurs patients. Pour ce faire, ils sont confrontés à de nombreuses difficultés. Cette section en décrit quelques-unes.

Prévention de l'espionnage de dossiers médicaux électroniques et autres menaces internes

Les établissements de santé comptent parmi les lieux de travail les plus stressants. Cela signifie qu'ils sont exposés à un risque accru de menaces internes.

Par exemple, un collaborateur curieux peut consulter le dossier médical d'un patient connu pour se distraire. C'est ce qu'on appelle l'espionnage de dossiers médicaux électroniques. Ce phénomène présente un risque grave pour un établissement en cas de divulgation des informations concernant un patient fortuné. Des collaborateurs bien intentionnés mais débordés risquent également de cliquer sur un email de phishing ou d'envoyer accidentellement des messages contenant des données sensibles aux mauvais destinataires. Le stress émotionnel peut même être à l'origine de menaces internes malveillantes contre un employeur. Si le compte d'un utilisateur de confiance est compromis par un vol d'identifiants de connexion, cela peut avoir des conséquences désastreuses avant que quiconque ne se rende compte de ce qui s'est passé. La prévention de ces types de menaces nécessite une approche proactive.

Neutralisation des risques de sécurité liés à l'IA générative

Les établissements de santé trouvent de plus en plus d'applications à l'IA générative. Il s'agit notamment d'accroître la productivité des cliniciens, d'améliorer l'engagement des patients et des membres et de rationaliser l'efficacité administrative. Il s'agit également d'optimiser la qualité des soins et des prestations, ainsi que d'aller au-delà des applications cliniques pour améliorer l'ensemble des interactions avec les patients. Cependant, l'utilisation de l'IA comporte des risques. Outre les dangers liés à des résultats inexacts ou biaisés, les prestataires de soins doivent s'assurer que les modèles d'IA n'exposent pas les données médicales protégées par inadvertance ou ne les utilisent pas à mauvais escient. Cela peut par exemple se produire lorsque l'IA traite des données non structurées telles que des notes cliniques. Qui plus est, l'intégration de l'IA générative dans la pratique clinique se heurte souvent à des obstacles réglementaires complexes.

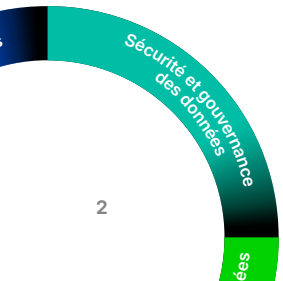
Couverture d'une surface d'attaque toujours plus étendue au fil de la migration vers le cloud

De nombreux établissements de santé ont mis du temps à adopter le cloud. Mais aujourd'hui, la quasi-totalité d'entre eux dispose de nombreux services dans des clouds publics, privés et hybrides. Cela a permis d'améliorer les soins aux patients en mettant les informations à la disposition des prestataires en temps réel. Cela a également permis aux établissements de simplifier leurs opérations et de réduire les capitaux nécessaires pour l'informatique. Toutefois, la migration vers le cloud s'est traduite par une extension de la surface d'attaque.

Même lorsque les dossiers médicaux électroniques sont stockés sur site, certaines données de ces dossiers sont souvent consultées, partagées et stockées ailleurs, notamment sur des terminaux mobiles, des endpoints distants, des dispositifs IoT médicaux et des systèmes de messagerie cloud. Dans la mesure où les données de santé circulent dans des zones géographiques de plus en plus étendues, leur protection constitue un défi de plus en plus complexe.

De plus, l'extension du cloud va de pair avec un risque accru de vol d'identifiants de connexion. De plus en plus de logiciels bureautiques et de fonctions de collaboration sont offerts par le biais de services cloud tels que Microsoft 365 et Google Workspace. C'est pourquoi les cybercriminels exploitent de plus en plus ces services.

2. Ponemon Institute et IBM, « Cost of a Data Breach Report 2024 » (Rapport 2024 sur le coût des compromissions de données).



Solutions

- Proofpoint Adaptive Email DLP
- Proofpoint Enterprise DLP
- Proofpoint Email DLP
- Proofpoint Encryption
- Proofpoint Insider Threat Management
- Proofpoint Data Security Posture Management
- Proofpoint Applied Services for Data Security

Unification de la sécurité des données sur tous les canaux et plates-formes

Les établissements de santé actuels utilisent de nombreux modes de communication et de transfert de données. Il peut s'agir de systèmes de dossiers médicaux électroniques tels qu'Epic, de systèmes de messagerie électronique dans le cloud ou sur site, d'autres systèmes de messagerie et de services de partage de fichiers. Ils disposent également d'un grand nombre d'endpoints, tels que les PC sur les lieux d'intervention, plusieurs centaines de types de dispositifs médicaux, les ordinateurs de bureau, les ordinateurs portables et les terminaux mobiles. De nombreux collaborateurs utilisent plusieurs terminaux au cours d'une même journée. Vos données sensibles sont hébergées sur des serveurs situés à la fois dans le centre de données et dans le cloud, et elles circulent régulièrement entre les deux.

Plus votre surface d'attaque s'accroît et votre infrastructure se complexifie, plus l'intégration de votre protection devient essentielle. Dans le cadre de la sécurité des données, cela implique de disposer d'outils intégrés de prévention des fuites de données (DLP) au niveau des endpoints, de la messagerie électronique et du cloud.

Une approche centrée sur les personnes

Les solutions traditionnelles de sécurité des données s'occupent uniquement des données. Or, les fuites d'informations ne se produisent pas par magie : un être humain en est toujours à l'origine, que ce soit de manière accidentelle ou intentionnelle. Quoi qu'il en soit, en matière de cybersécurité, la visibilité est la clé. Il est donc essentiel d'identifier les personnes associées aux risques les plus élevés. Une approche centrée sur les personnes permet de comprendre la dynamique des utilisateurs qui interagissent avec vos données.

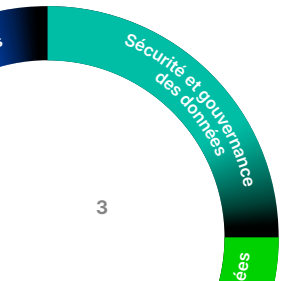
Comment Proofpoint peut vous aider

La solution unifiée de sécurité des données centrée sur les personnes de Proofpoint vous offre une visibilité inégalée. Dotée d'une interface native au cloud, elle vous permet de protéger vos informations sensibles en se concentrant sur les personnes qui interagissent avec elles. Nos solutions tiennent à la fois compte du contenu, du comportement et des menaces. Elles associent la protection des informations sur site à la sécurité du cloud. Cela garantit la protection de votre personnel, de vos collaborateurs médicaux et de vos patients, quel que soit l'endroit où leurs données circulent.

Notre solution unifiée de sécurité des données allie les principaux composants suivants :

Proofpoint Adaptive Email DLP

Proofpoint Adaptive Email DLP s'appuie sur l'IA comportementale pour prévenir tant les fuites de données accidentelles qu'intentionnelles par email. Il analyse plus de 12 mois de données de messagerie pour identifier les comportements normaux des collaborateurs en matière d'envoi d'emails, leurs relations de confiance et la façon dont ils gèrent les données médicales sensibles. Grâce à cette analyse, Proofpoint Adaptive Email DLP peut identifier les comportements anormaux. S'il suspecte un email adressé au mauvais destinataire, une pièce jointe erronée ou une exfiltration de données, il affiche instantanément un message d'avertissement contextuel permettant à l'utilisateur de corriger et de prévenir les fuites de données en temps réel, sans intervention de l'administrateur.



Proofpoint Enterprise DLP

Les solutions DLP de pointe de Proofpoint adoptent une approche adaptative et centrée sur les personnes de la prévention des fuites de données. Elles offrent une visibilité étendue sur les comportements des utilisateurs et les contenus, ce qui permet de détecter et de prévenir efficacement les risques de fuites de données majeures. Proofpoint modernise les stratégies DLP traditionnelles en intégrant la protection de la messagerie électronique, du cloud et des endpoints managés et non managés. Nos solutions DLP reposent sur une architecture native au cloud offrant des contrôles modernes de la confidentialité et un agent extrêmement stable. Elles évoluent automatiquement et sont faciles à déployer et à gérer.

Une console unifiée vous aide à gérer les alertes et à enquêter sur les incidents sur tous les canaux. À l'aide d'analyses puissantes, vous pouvez évaluer rapidement les risques qui pèsent sur les données, parvenir à des verdicts très fiables et prendre des mesures appropriées.

Proofpoint Email DLP

Proofpoint Email DLP réduit le risque de fuites de données sensibles par email et garantit le respect des exigences de conformité grâce à une prévention et à un chiffrement basés sur des règles. Il est facile à déployer en combinaison avec une solution de protection de la messagerie ou dans le cadre d'une solution DLP d'entreprise unifiée. Proofpoint Email DLP automatise la conformité réglementaire grâce à des règles prêtes à l'emploi répondant à des exigences telles que celles de la norme PCI, du RGPD, du code SOX, de la loi HIPAA, des diverses lois de protection des données personnelles, etc. Vous pouvez également utiliser des dictionnaires personnalisés, y compris une classification optimisée par l'IA, pour identifier et protéger les données propres à votre établissement.

Proofpoint Email Encryption

Proofpoint Email Encryption assure le chiffrement automatique des emails et de leurs pièces jointes en toute transparence. Contrairement aux services de messagerie chiffrée traditionnels, tout se passe en arrière-plan — les utilisateurs n'ont rien à faire manuellement. Avec Proofpoint Email Encryption, vous pouvez protéger les emails sensibles tout en permettant à vos collaborateurs, partenaires commerciaux et utilisateurs de continuer à y accéder sans la moindre difficulté sur leurs ordinateurs et terminaux mobiles.

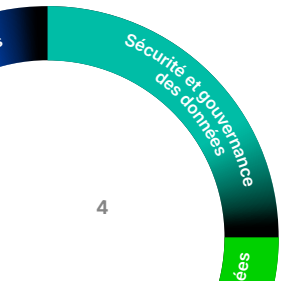
Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) met en corrélation les activités des utilisateurs et les mouvements de données. Il permet à vos équipes de sécurité de détecter, d'analyser et de neutraliser les menaces internes en tenant compte du comportement des utilisateurs. Il fournit également des fonctionnalités de détection et de réponse en temps réel en cas d'exfiltration de données, d'utilisation abusive de privilèges, d'utilisation inappropriée d'applications, d'accès non autorisé, d'activités accidentelles dangereuses ou de comportements anormaux. Vous pouvez ainsi détecter, prévenir et neutraliser des menaces telles que l'espionnage de dossiers médicaux électroniques grâce à des vues et à des analyses chronologiques.

Lorsqu'une menace interne est identifiée, Proofpoint ITM fournit des workflows et des preuves irréfutables des actes malveillants afin d'accélérer la réponse aux incidents. Ces renseignements sont collectés par des capteurs d'endpoint légers. Ils sont ensuite analysés au sein d'une architecture moderne pour assurer l'évolutivité, la sécurité et la confidentialité. Proofpoint ITM peut également être déployé à l'aide de modèles de distribution sur site ou SaaS.

Proofpoint Data Security Posture Management

Proofpoint Data Security Posture Management (DSPM) s'attaque à la cause première de nombreuses compromissions, à savoir les angles morts dans les environnements de données, tout en donnant la priorité à la réduction des risques liés aux personnes dans le domaine de la sécurité des données. En identifiant l'emplacement des données sensibles et de valeur, les utilisateurs qui y ont accès et les risques qui représentent la plus grande menace, Proofpoint DSPM permet aux établissements de santé de combler les lacunes, de réduire la surface d'attaque et d'automatiser la conformité. Proofpoint DSPM favorise également une adoption sécurisée des outils d'IA en identifiant les données sensibles, en appliquant des règles de protection des données et en assurant une analyse de sensibilité en temps réel pour les workflows d'IA.



Proofpoint Applied Services for Data Security

Le secteur de la santé est confronté à une pénurie de main-d'œuvre depuis de nombreuses années. Cette situation représente un véritable défi pour la fourniture de soins de qualité aux patients. Face à la pénurie de personnel qualifié pour gérer la sécurité, de plus en plus d'établissements de santé se tournent vers les services managés pour les aider à répondre à leurs besoins en matière de sécurité. Avec Proofpoint Applied Services for Data Security, vous pouvez faire appel à notre équipe mondiale d'experts en sécurité des données pour renforcer votre équipe. Nous disposons de plusieurs dizaines d'années d'expérience qui nous ont permis d'élaborer de bonnes pratiques et des modèles de maturité pour optimiser votre programme. À cette fin, nous couvrons la gestion des applications, la gouvernance de la portée et des règles, le tri des événements, la gestion des incidents, le signalement et l'analyse. Vous êtes ainsi protégé contre le vol de propriété intellectuelle et les compromissions de données de patients. Nos experts conçoivent, implémentent et exécutent un programme adapté à vos besoins en matière de sécurité et de conformité. Toutes nos solutions, de la prévention des fuites de données (DLP) à la gestion des menaces internes, tirent parti d'un apprentissage automatique avancé et des analyses humaines pour protéger vos informations médicales. Nous analysons les alertes et intervenons rapidement pour contrer les tentatives de compromission. Confiez-nous l'amélioration de votre sécurité et laissez ainsi votre équipe se consacrer à d'autres problèmes.

Conclusion

Les établissements de santé comme le vôtre ont été confrontés à des défis sans précédent au cours des dernières années. Ces turbulences se poursuivent tandis que vous tentez de retrouver une certaine stabilité face aux réductions de coûts, à la baisse des remboursements, à la pénurie de main-d'œuvre et à bien d'autres facteurs. Au niveau de l'infrastructure, les surfaces d'attaque se sont étendues. Le besoin de sécurité des données s'est étendu du centre de données aux différents clouds. Le nombre de connexions des collaborateurs et des patients depuis des emplacements distants demeure élevé, et le nombre de dispositifs IoT médicaux à la périphérie du réseau continue d'augmenter. Pendant près de 20 ans, les établissements de santé se sont concentrés sur la sécurisation du périmètre. Mais les tendances récentes ont présidé à la disparition du périmètre traditionnel. De nos jours, le collaborateur individuel incarne à la fois le périmètre et sa périphérie. Les solutions de sécurité des données de Proofpoint vous permettent d'obtenir des informations en temps réel sur les risques pesant sur les données. Vous pouvez également hiérarchiser et neutraliser les incidents, ainsi que prévenir les fuites de données. La plate-forme offre également un large éventail de fonctionnalités réglementaires et de conformité, notamment la découverte, la classification et le chiffrement de données. Ces fonctionnalités vous aident à répondre aux exigences réglementaires et aux normes sectorielles. En protégeant les collaborateurs qui traitent vos informations sensibles, vous protégerez votre établissement.

proofpoint.

DÉCOUVRIR LA PLATE-FORME PROOFPOINT →