Protection des informations médicales avec Proofpoint

Protégez les données des patients contre les menaces internes, les fuites de données et l'extension du cloud

Produits

- Proofpoint Cloud App Security Broker
- Proofpoint Email Data Loss Prevention
- Proofpoint Endpoint Data Loss Prevention
- Proofpoint Insider Threat Management
- Proofpoint Web Security
- Proofpoint Zero Trust Network Access
- Services gérés Proofpoint de protection des informations

Principaux avantages

- Identification et limitation des risques dus à des utilisateurs internes négligents, compromis ou malveillants
- Prévention des fuites de données depuis la messagerie, le cloud et les endpoints
- Extension de la protection évolutive à un nombre croissant de services cloud largement distribués

Le secteur de la santé est depuis longtemps une cible privilégiée des cybercriminels, et la pandémie de COVID-19 n'a fait qu'aggraver la situation. Les cybercriminels ont redoublé d'efforts pour accéder à des données précieuses, telles que des informations sur les essais des vaccins, des données médicales protégées et des données financières. De leur côté, les établissements de santé ont augmenté leur surface d'attaque en migrant vers le cloud et en accordant un accès à distance à davantage de collaborateurs et patients. Ces établissements sont également confrontés à un risque accru de menaces internes, qu'elles soient malveillantes ou involontaires.

Proofpoint propose une approche centrée sur les personnes pour préserver les données sensibles au sein de réseaux médicaux largement distribués. Nos solutions de protection des informations sont faciles à déployer et à gérer. Vous pouvez les utiliser pour ériger une architecture de sécurité SASE (Secure Access Service Edge) ou SSE (Security Service Edge). Nous vous aidons à protéger vos collaborateurs et leurs données sensibles contre les erreurs accidentelles, les attaques et les risques internes dans tout l'environnement : services cloud, messagerie électronique, endpoints et partages de fichiers sur site.

Une menace grandissante

Une compromission peut entraîner des amendes réglementaires et des litiges, de même que porter atteinte à l'image de marque des établissements de santé, voire provoquer le décès de patients. Selon le département américain de la Santé et des Services sociaux, une augmentation de 50 % du nombre de compromissions de sécurité a été observée dans le secteur de la santé au premier semestre 2020. Par ailleurs, en 2021, le nombre global d'attaques de ransomwares a plus que doublé, faisant du secteur de la santé l'un des deux secteurs les plus ciblés.

Le nombre croissant de dispositifs IoT (Internet of Things) médicaux permet peut-être de sauver des vies, mais il accroît également la complexité de la gestion. En raison de la pandémie de COVID-19, de nombreux professionnels se sont tournés vers les services de télésanté, parfois même depuis leur domicile plutôt que depuis un cabinet médical ou un hôpital.

Rien d'étonnant dès lors que Moody's Investors Service estime que le cyberrisque restera élevé dans le secteur de la santé dans les semaines, voire les mois à venir. Après avoir géré pendant près de deux ans une crise existentielle, les établissements de santé doivent rester sur leurs gardes.

Défis liés à la protection des informations

Face à ce paysage des menaces peu réjouissant, les hôpitaux, les cliniques, les compagnies d'assurance-maladie et les entreprises de biotechnologie doivent faire de la protection des informations une priorité absolue. Ils doivent impérativement préserver les données médicales, personnelles et de cartes de paiement de leurs patients. Les défis à relever sont nombreux.

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

Les professionnels de santé sont les héros de la pandémie. Ils ont assumé leur fonction dans le stress et l'urgence, jour après jour, alors même qu'aucune issue n'était en vue. Un tel stress peut accroître le risque de menace interne. Pour se détendre, des collaborateurs curieux ont pu, par exemple, être tentés de jeter un œil sur le dossier médical d'un patient connu. Cet « espionnage » des dossiers médicaux électroniques peut présenter un risque élevé pour un établissement en cas de divulgation des informations concernant un riche patient.

Des collaborateurs bien intentionnés mais débordés risquent également de cliquer sur un email de phishing qu'ils auraient détecté dans un autre contexte. Le stress émotionnel peut même être à l'origine de menaces internes malveillantes contre un employeur. Une approche proactive est donc essentielle pour prévenir tous ces types de menaces.

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. Aujourd'hui, presque tous disposent de multiples services dans des clouds publics et privés, ce qui leur a permis d'améliorer leur efficacité opérationnelle et d'éviter d'engager des fonds pour se doter d'une infrastructure informatique. Mais la migration vers le cloud s'est traduite par une extension de la surface d'attaque de ces établissements.

Même si les dossiers médicaux électroniques sont stockés dans une infrastructure sur site, certaines données de ces dossiers sont inévitablement consultées, partagées et stockées ailleurs, notamment sur des terminaux mobiles, des endpoints distants, des dispositifs IoT médicaux et des systèmes de messagerie cloud. Plus les canaux de circulation des données médicales se multiplient, plus il devient compliqué de protéger ces dernières.

De plus, l'extension du cloud va de pair avec un risque accru de vol d'identifiants de connexion. Des services cloud tels que Microsoft 365 et Google Workspace fournissent de plus en plus de logiciels bureautiques et de fonctions de collaboration. Or, ils sont vulnérables aux cybermenaces. Pour compliquer encore la donne, les cybercriminels recourent de plus en plus à ces partages de fichier reconnus pour distribuer leurs exploits.

Protection du personnel médical et des patients distants au fil de l'évolution des modèles de distribution

Certains des changements soudains de l'environnement de travail causés par la pandémie au début de l'année 2020 ont été temporaires. Pour bon nombre d'entre eux, en revanche, les conséquences se feront ressentir pendant encore plusieurs années. Dans le secteur de la santé, le recours accru aux services de télésanté est une tendance vouée à perdurer. Une étude a montré qu'en février 2021, l'utilisation de la télésanté était toujours 38 fois supérieure au chiffre de référence de 2019. Cette situation a entraîné une augmentation considérable du nombre de patients accédant à distance aux ressources des établissements de santé.

Par ailleurs, bon nombre de collaborateurs sont toujours en télétravail, à tout le moins à temps partiel. La plupart d'entre eux gèrent des dossiers médicaux électroniques, des informations financières des patients et des données de recherche. Le volume croissant de connexions à distance augmente le risque d'attaques visant des collaborateurs endossant des fonctions spécifiques au sein de l'établissement.

Adoption d'une approche centrée sur les personnes

Les solutions traditionnelles de protection des informations 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. 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 les données.

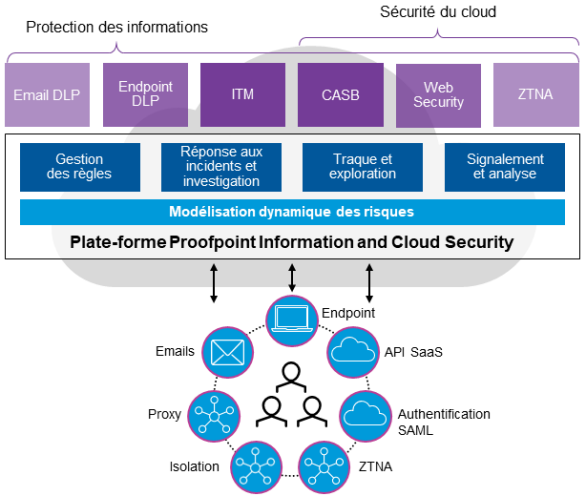

Figure 1. Plate-forme Proofpoint Information and Cloud Security

Comment Proofpoint peut vous aider

La plate-forme Proofpoint Information and Cloud Security peut vous aider à protéger vos informations sensibles en se concentrant sur les personnes qui les gèrent.

Proofpoint Cloud App Security Broker

Proofpoint Cloud App Security Broker (CASB) protège les utilisateurs contre les menaces dans le cloud. Il protège les données sensibles et gère les applications cloud et OAuth dans Microsoft 365, Google Workspace et plus de 900 applications cloud approuvées et tolérées par le département informatique. Il étend aux services cloud la visibilité de Proofpoint sur les VAP (Very Attacked People™, ou personnes très attaquées). Vous pouvez ainsi protéger plus efficacement les comptes et données cloud. Proofpoint CASB offre une vue granulaire de l'accès au cloud, du comportement des utilisateurs et du traitement des données sensibles (données médicales personnelles, par exemple), de façon à préserver votre conformité aux réglementations en matière de confidentialité et de sécurité des données.

Proofpoint CASB peut être déployé selon différents modes, en fonction des cas d'utilisation. Pour garantir une visibilité en temps réel et une réduction du délai de rentabilisation, Proofpoint CASB s'intègre avec les connecteurs API de vos applications cloud et les journaux de votre infrastructure. Pour un accès et des contrôles de données en temps réel, vous pouvez utiliser l'authentification SAML basée sur les risques, l'isolation et des fonctionnalités de proxy de transfert en ligne. Comme dans une véritable architecture SSE, vous pouvez intégrer Proofpoint CASB avec Proofpoint Web Security et Proofpoint Zero Trust Network Access (ZTNA) pour connecter et protéger les collaborateurs distants dans les applications Web et cloud.

Proofpoint Data Loss Prevention

Proofpoint Data Loss Prevention adopte une approche centrée sur les personnes de la prévention des fuites de données (DLP). Il combine contenu, comportements et menaces et fournit des informations contextuelles sur ces trois aspects. Ces renseignements sont présentés sous la forme d'une vue chronologique moderne, qui vous procure un éclairage plus complet et nuancé sur chaque événement. Ces informations vous aident à déterminer si l'utilisateur signalé a été victime d'une compromission, a des intentions malveillantes ou est simplement négligent.

Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) met en corrélation les activités des utilisateurs et les mouvements de données. Il permet aux équipes de sécurité de détecter, d'analyser et de neutraliser les menaces internes. Il offre une sensibilisation aux comportements centrée sur les personnes. 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. Les 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 (Software-as-a-Service).

Proofpoint Web Security

La plupart de vos collaborateurs se connectent depuis l'extérieur du périmètre réseau. Proofpoint Web Security protège vos effectifs dispersés contre les menaces avancées lorsqu'ils parcourent le Web en assurant la sécurité de la navigation. Grâce à l'inspection de l'ensemble du trafic SSL, Proofpoint Web Security détecte et bloque des menaces telles que les ransomwares et les attaques de phishing « zero-day ». La solution empêche également les collaborateurs d'accéder à des contenus dangereux et non conformes.

Proofpoint Zero Trust Network Access

Avec la migration des applications vers le cloud, les professionnels de santé sont de plus en plus mobiles. Une alternative plus efficace aux VPN est par conséquent nécessaire pour sécuriser l'accès. Proofpoint ZTNA tire parti d'un périmètre défini par logiciel pour chaque utilisateur. Les utilisateurs disposent ainsi d'un accès distant sécurisé fourni dans le cloud aux ressources du centre de données et du cloud.

Chaque utilisateur est autorisé à accéder à des applications spécifiques. Le reste du réseau est masqué. Proofpoint ZTNA valide les utilisateurs avant qu'ils accèdent au réseau, ce qui permet de renforcer la sécurité et la visibilité.

Services gérés Proofpoint de protection des informations

Grâce aux services gérés de protection des informations, nos experts mondiaux en sécurité des données viennent renforcer votre équipe. Nos longues années d'expérience 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. Les solutions Proofpoint DLP, CASB (Cloud Access Security Broker) et ITM tirent parti d'un apprentissage automatique avancé et des analyses humaines pour protéger vos informations médicales.

Les alertes sont analysées et les équipes peuvent intervenir rapidement pour contrer les tentatives de compromission. Confiez-nous l'amélioration de votre sécurité et laissez ainsi à votre équipe plus de temps pour se consacrer à d'autres problèmes.

Conclusion

Les établissements de santé ont dû s'adapter aux bouleversements de l'environnement de travail provoqués par la pandémie de COVID-19. Les surfaces d'attaque se sont étendues. La protection des informations couvre désormais de multiples clouds. Les connexions des collaborateurs et des patients depuis des emplacements distants sont en hausse, tout comme le nombre de dispositifs IoT médicaux à la périphérie du réseau.

Depuis près de 20 ans, les entreprises s'efforcent de sécuriser leur périmètre. La récente explosion de l'utilisation des services cloud et l'expansion du télétravail ont fait du télétravailleur le nouveau périmètre.

Ces changements rapides nécessitent une architecture de sécurité émergente, généralement connue sous le nom d'architecture SSE (la composante de sécurité d'une architecture SASE). Une telle architecture offre aux utilisateurs l'accès sécurisé nécessaire à l'ensemble des services cloud via des centres de données cloud. C'est au sein de cette architecture que s'effectuent l'accès réseau Zero Trust et la gestion des identités et accès, et que les administrateurs surveillent les accès au moyen de contrôles centralisés.

Vous pouvez vous appuyer sur la plate-forme Proofpoint Information and Cloud Security pour ériger une architecture SSE ou SASE robuste. Vous pourrez ainsi sécuriser l'accès et assurer une protection contre les menaces lorsque les utilisateurs accèdent à des applications et à des données, où qu'ils se trouvent et quel que soit le type de terminal utilisé. En protégeant les collaborateurs qui traitent vos informations sensibles, vous protègerez votre établissement.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

proofpoint.

0207-005-01-01 12/21