proofpoint.

PANORAMICA SULLA SOLUZIONE

Proteggere i dati sanitari con Proofpoint

Proteggi i dati dei pazienti contro le minacce interne, la perdita di dati e i rischi legati al cloud

Vantaggi principali

- Identificazione e mitigazione delle minacce legate agli utenti interni negligenti, compromessi o malintenzionati
- Protezione scalabile su tutti gli elementi della superficie d'attacco a fronte dell'ampliamento delle impronte digitali
- Prevenzione della perdita di dati a livello di email, cloud e endpoint

10%

Percentuale degli attacchi ransomware che hanno colpito il settore della sanità negli ultimi due anni.

Fonte: SC Media

Il settore della sanità è da tempo uno degli obiettivi prediletti dei criminali informatici. Le aziende di questo settore trattano diversi tipi di dati, tra cui proprietà intellettuale, dati di studi clinici, informazioni di identificazione sanitaria protette e dettagli finanziari personali. I criminali informatici dispongono di numerose opzioni per trarre profitto da un attacco contro una di queste aziende. Le strutture sanitarie stanno adottando il cloud, il telelavoro e la telemedicina, e al contempo, ampliano anche la loro superficie di attacco. Poiché i collaboratori del settore operano in condizioni di stress sempre più elevato, le strutture si trovano ad affrontare un rischio maggiore da parte di utenti interni sia malintenzionati sia benintenzionati.

Proofpoint offre un approccio incentrato sulle persone per proteggere i dati sensibili nelle reti sanitarie distribuite. Le nostre soluzioni di sicurezza dei dati forniscono visibilità e controllo senza pari sui dati sensibili. Ti aiutiamo a proteggere i tuoi collaboratori e i loro dati sensibili da divulgazioni accidentali, attacchi dannosi e rischi di minacce interne. Il nostro scudo di protezione si estende a servizi cloud, email, endpoint e condivisioni di file in locale. La tua struttura può gestire meglio i rischi per i dati risparmiando tempo e riducendo i costi operativi.

Una minaccia crescente

Così come molte aziende, le strutture sanitarie archiviano le informazioni delle carte di pagamento e altre informazioni finanziarie. Gestiscono anche enormi quantità di informazioni di identificazione sanitaria dei pazienti e dati degli studi clinici. Conservano anche i dati relativi alle sovvenzioni pubbliche. Tutto ciò li rende un obiettivo redditizio per i criminali informatici.

Allo stesso tempo, le impronte digitali degli enti della sanità sono sempre più complesse. Il settore della sanità ora ospita una crescente gamma di servizi nel cloud. Il numero crescente di dispositivi IoT medici può salvare vite umane, ma amplia anche la superficie di attacco. L'ampliamento delle opzioni di telemedicina implica anche che i dati sensibili circolano sempre più spesso al di fuori del perimetro della rete. Inoltre, i collaboratori spesso lavorano da remoto, quando le regole del lavoro ibrido lo consentono.

Purtroppo, i criminali informatici hanno seguito i loro obiettivi al di fuori del perimetro. Negli ultimi due anni, il settore della sanità è stato colpito dal 10% di tutti gli attacchi ransomware e gli attacchi informatici che prendono di mira il settore medico sono aumentati del 32%[1] . Queste cifre sono molto più elevate di quelle di altri settori. Le violazioni dei dati sono anche più costose nel settore della sanità che in tutti gli altri settori.

1. Shaun Nichols (*SC Media*), "Cyberattacks targeting medial organizations up 32% in 2024." (Gli attacchi informatici che prendono di mira le strutture mediche sono aumentate del 32% nel 2024), febbraio 2025.

32%

Gli attacchi informatici che prendono di mira il settore medico sono aumentati del 32% negli ultimi due anni.

Fonte: SC Media

9,77 Mln di dollari

Nel 2024, una violazione dei dati sanitari è costata in media 9,77 milioni di dollari.

Fonte: Ponemon Institute e IBM

Nel 2024, il costo di una violazione dei dati sanitari ammontava in media a 9,77 milioni di dollari[2]. Questo costo può includere pagamento di riscatti, applicazione di misure correttive dei sistemi, sanzioni per la mancata conformità, contenziosi e danneggiamento della reputazione. Anche i tempi di inattività del sistema o la compromissione dell'integrità dei dati possono avere esiti negativi per la salute. Possono anche portare alla perdita di vite umane.

Sfide legate alla sicurezza dei dati

Per ospedali, cliniche, fornitori di polizze sanitarie e aziende di biotecnologie, la sicurezza dei dati dovrebbe essere una priorità assoluta. Queste strutture devono proteggere i loro dati di ricerca e la proprietà intellettuale. Ma devono anche proteggere le informazioni di identificazione sanitaria, i dati a carattere personale e delle carte di credito dei loro pazienti. Per farlo, devono affrontare diverse sfide. Questa sezione ne descrive alcune.

Prevenzione dello spionaggio delle cartelle cliniche elettroniche e altre minacce interne

Le strutture sanitarie sono uno dei luoghi di lavoro più stressanti. Ciò significa che sono più a rischio di minacce interne.

Per esempio, un collaboratore curioso potrebbe consultare le cartelle cliniche di un paziente famoso per distrarsi. Si tratta del cosiddetto spionaggio delle cartelle cliniche elettroniche, che rappresenta un serio rischio per un'ente se le informazioni di un paziente facoltoso vengono rese pubbliche. Impiegati con buone intenzioni, ma oberati, potrebbero aprire email di phishing o inviare accidentalmente email con dati sensibili ai destinatari errati. Lo stress emotivo può anche essere la fonte di minacce interne dannose contro un datore di lavoro. La violazione dell'account di un utente fidato a causa del furto delle credenziali di accesso può comportare gravi conseguenze prima che ci si renda conto dell'accaduto. La prevenzione di questi tipi di minacce richiede un approccio proattivo.

Neutralizzazione dei rischi di sicurezza legati all'IA generativa

Le strutture sanitarie trovano sempre più utilizzi per l'IA generativa, come incrementare la produttività dei medici, migliorare il coinvolgimento dei pazienti e dei membri dello staff e ottimizzare l'efficienza amministrativa. Si tratta anche di ottimizzare la qualità delle cure e dell'assistenza, nonché di andare oltre le applicazioni cliniche per migliorare le interazioni complessive con i pazienti. Ma l'utilizzo dell'IA comporta dei rischi. Al di là dei pericoli legati a risultati imprecisi o distorti, le strutture sanitarie devono garantire che i modelli di IA non espongano inavvertitamente o utilizzino in modo inappropriato le informazioni di identificazione sanitaria. Ciò può accadere, per esempio, quando l'IA gestisce dati non strutturati come le annotazioni cliniche. Inoltre, l'integrazione dell'IA generativa nella pratica medica spesso si scontra con complessi ostacoli normativi.

Copertura di una superficie d'attacco sempre più estesa durante la migrazione al cloud

Molte aziende del settore sanitario hanno adottato il cloud in ritardo. Ma ora, quasi tutte dispongono di molteplici servizi nei cloud pubblici, privati e Ibridi. Ciò ha migliorato l'assistenza sanitaria ai pazienti rendendo le informazioni disponibili ai fornitori in tempo reale. Ha inoltre permesso alle strutture sanitarie di semplificare le operazioni e ridurre i capitali necessari per l'IT. Tuttavia, la migrazione al cloud ha anche esteso la superficie d'attacco.

Anche quando le cartelle cliniche elettroniche sono conservate on premise, i dettagli di questi documenti vengono spesso consultati, condivisi e archiviati altrove, per esempio su dispositivi mobili, endpoint remoti, dispositivi IoT medici e sistemi email basati sul cloud. Poiché i dati sanitari circolano in aree geografiche sempre più ampie, la loro protezione è sempre più complessa.

Man mano che il cloud si espande, aumenta anche il rischio di furto delle credenziali di accesso. I servizi cloud come Microsoft 365 e Google Workspace forniscono sempre più software professionali e funzioni di collaborazione. Di conseguenza, i criminali informatici sfruttano sempre più questi servizi.

2. Ponemon Institute e IBM, "Cost of a Data Breach Report 2024." (Report sul costo delle violazioni dei dati 2024).

Soluzioni

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

Unificazione della sicurezza dei dati su tutti i canali e piattaforme

Gli enti sanitari odierni utilizzano molti modi per comunicare e trasferire i dati, tra cui sistemi di cartelle cliniche elettroniche come Epic, sistemi email in cloud e on premise, altri sistemi di messaggistica e servizi di condivisione di file. Tali enti dispongono anche di una ricca gamma di endpoint, tra cui PC al punto di assistenza, centinaia di tipi di dispositivi medici, computer desktop, notebook e dispositivi mobili. Molti collaboratori utilizzano diversi dispositivi ogni giorno. I tuoi dati sensibili sono conservati su server posizionati nel data center e nel cloud e circolano regolarmente tra i due ambienti.

Man mano che la tua superficie d'attacco cresce e la tua infrastruttura diventa più complessa, l'integrazione della tua protezione diventa essenziale. Nel caso della sicurezza dei dati, ciò significa disporre di strumenti integrati di prevenzione della perdita dei dati (DLP) su endpoint, email e cloud.

Un approccio incentrato sulle persone

Gli approcci tradizionali alla sicurezza dei dati considerano esclusivamente i dati. Ma le perdite di informazioni non avvengono per magia: all'origine c'è sempre un'azione umana, che sia accidentale, o intenzionale. In ogni caso, nella sicurezza informatica, la visibilità è la chiave. È necessario identificare le persone associate ai rischi più elevati. Un approccio incentrato sulle persone permette di comprendere le dinamiche degli utenti che interagiscono con i tuoi dati.

Come Proofpoint può aiutarti

La soluzione unificata di sicurezza dei dati incentrata sulle persone di Proofpoint ti offre una visibilità ineguagliata. Dotata di un'interfaccia cloud, ti permette di proteggere le tue informazioni sensibili, concentrandoti sulle persone che interagiscono con esse. Le nostre soluzioni tengono conto delle minacce, dei comportamenti e dei contenuti. Combinano la protezione delle informazioni on premise con la sicurezza del cloud. Ciò assicura la protezione del tuo personale, degli operatori medici e dei pazienti, indipendentemente dal luogo in cui i loro dati circolano.

La nostra soluzione di sicurezza dei dati unificata combina i seguenti componenti:

Proofpoint Adaptive Email DLP

Proofpoint Adaptive Email DLP utilizza l'IA comportamentale per prevenire la perdita di dati accidentale e intenzionale attraverso l'email. Analizza oltre dodici mesi di dati dell'email per identificare i normali comportamenti di invio delle email dei collaboratori, le loro relazioni di fiducia e come gestiscono i dati sanitari sensibili. Grazie a questa analisi, Proofpoint Adaptive Email DLP è in grado di identificare i comportamenti anomali. Quando sospetta si stia verificando l'invio di email al destinatario errato, di allegati sbagliati o un'esfiltrazione di dati, mostra immediatamente un messaggio di avviso contestuale permettendo all'utente di correggere e prevenire l'incidente di perdita dei dati in tempo reale, senza l'intervento dell'amministratore.

Proofpoint Enterprise DLP

Le avanzate soluzioni DLP di Proofpoint adottano un approccio adattivo incentrato sulle persone per prevenire la perdita di dati. Offrono una visibilità estesa sui comportamenti degli utenti e i contenuti, permettendo di rilevare e prevenire in modo efficace i principali rischi di perdita di dati. Proofpoint aggiorna le strategie DLP tradizionali integrando la protezione di email, cloud e endpoint gestiti e non gestiti. Le nostre soluzioni di prevenzione della perdita di dati si basano su un'architettura cloud-native che offre controlli moderni della privacy e un agent estremamente stabile. Scalano automaticamente e sono semplici da implementare e gestire.

Un'unica console unificata ti aiuta a gestire gli avvisi e indagare sugli incidenti su tutti i canali. Utilizzando analisi potenti, puoi rapidamente valutare i rischi legati ai dati, ottenere verdetti estremamente affidabili e adottare le misure appropriate.

Proofpoint Email DLP

Proofpoint Email DLP riduce il rischio di perdita di dati sensibili attraverso l'email e garantisce la conformità grazie a prevenzione e crittografia basate su policy. È facile da implementare con una soluzione di sicurezza dell'email o come parte di una soluzione DLP aziendale unificata. Proofpoint Email DLP automatizza la conformità normativa con policy pronte all'uso che soddisfano requisiti quali lo standard PCI, il GDPR, il codice SOX, la legge HIPAA, varie leggi di protezione dei dati personali, ecc. Puoi anche utilizzare dizionari personalizzati, tra cui classificazione ottimizzata dall'IA, per identificare e proteggere i dati specifici della tua azienda.

Proofpoint Email Encryption

Proofpoint Email Encryption assicura la crittografia automatica delle email e dei loro allegati con una trasparenza completa. A differenza dei servizi di email crittografata tradizionali, tutto avviene in background: gli utenti non devono compiere alcuna azione manuale. Con Proofpoint Email Encryption puoi proteggere i messaggi email sensibili permettendo ai tuoi collaboratori, partner commerciali e utenti di continuare a accedervi senza problemi sui loro computer e dispositivi mobile.

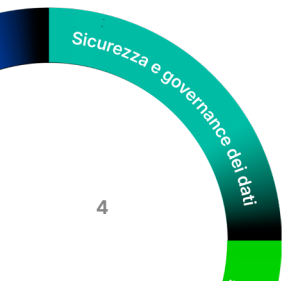
Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) correla l'attività degli utenti con lo spostamento dei dati. Permette ai tuoi team della sicurezza di rilevare, analizzare e neutralizzare le minacce interne tenendo conto del comportamento degli utenti. Inoltre fornisce funzionalità di rilevamento e risposta in tempo reale all'esfiltrazione dei dati, all'abuso di privilegi, all'uso improprio delle applicazioni, all'accesso non autorizzato, alle azioni involontarie pericolose e ai comportamenti anomali. Ciò ti aiuta a rilevare, prevenire e rispondere a minacce come lo spionaggio delle cartelle cliniche elettroniche con visualizzazioni e analisi temporali.

Quando viene identificata una minaccia interna, Proofpoint ITM fornisce flussi di lavoro e prove irrefutabili di violazioni per accelerare la risposta agli incidenti. Queste informazioni vengono raccolte da sensori endpoint leggeri. Quindi vengono analizzate all'interno di un'architettura moderna per garantire scalabilità, sicurezza e privacy. Proofpoint ITM più anche essere implementato utilizzando modelli di distribuzione on premise o SaaS.

Proofpoint Data Security Posture Management

Proofpoint Data Security Posture Management (DSPM) affronta la causa principale di numerose violazioni, ovvero i punti ciechi negli ambienti di dati, dando priorità alla riduzione dei rischi legati alle persone nella sicurezza dei dati. Identificando dove risiedono i dati sensibili e di valore, gli utenti che vi accedono e i rischi che rappresentano la minaccia più grande, Proofpoint DSPM consente alle strutture sanitarie di colmare le lacune, ridurre la superficie d'attacco e automatizzare la conformità. Proofpoint DSPM permette anche un'adozione sicura degli strumenti di IA identificando i dati sensibili, applicando policy di protezione dei dati e fornendo un'analisi della riservatezza in tempo reale per i flussi di lavoro dell'IA.



Proofpoint Applied Services for Data Security

Il settore della sanità affronta una carenza di manodopera da diversi anni. Tale situazione è una vera sfida per la fornitura di cure di qualità ai pazienti. A fronte della carenza di personale qualificato per gestire la sicurezza, sempre più strutture sanitarie si rivolgono ai servizi gestiti per soddisfare le proprie esigenze in termini di sicurezza. I servizi Proofpoint Applied Services for Data Security ti consentono di rivolgerti al nostro team globale di esperti di sicurezza dei dati per rafforzare il tuo team. Abbiamo un'esperienza pluridecennale che ci ha permesso di sviluppare best practice e modelli di maturità per ottimizzare il tuo programma. A tal fine, copriamo la gestione delle applicazioni, la governance dell'ambito e delle policy, il triage degli eventi, la gestione degli incidenti, il reporting e l'analisi. Sei così protetto dal furto di proprietà intellettuale e dalle violazioni dei dati dei pazienti. I nostri esperti progettano, implementano e gestiscono un programma su misura per le tue esigenze di sicurezza e conformità. Tutte le nostre soluzioni, dalla prevenzione della perdita di dati (DLP) alla gestione delle minacce interne, sfruttano un machine learning avanzato e analisi umane per proteggere i tuoi dati sanitari. Esaminiamo gli avvisi e interveniamo rapidamente per contrastare i tentativi di violazione. Lascia che ti aiutiamo a migliorare la tua sicurezza in modo che il tuo team possa concentrarsi su altre questioni.

Conclusione

Le strutture sanitarie come la tua hanno affrontato sfide senza pari negli ultimi anni. Queste turbolenze continuano mentre cerchi di tornare alla stabilità a fronte della riduzione dei costi, della diminuzione dei rimborsi, della carenza di personale e altro ancora. Sul versante dell'infrastruttura, le superfici d'attacco si sono ampliate. La necessità di sicurezza dei dati si è estesa dal data center a diversi cloud. Il numero di accessi da parte di collaboratori e pazienti da postazioni remote rimane elevato, così come il numero di dispositivi IoT medici all'edge della rete continua a aumentare. Per quasi vent'anni, le aziende si sono concentrate sulla protezione del perimetro. Ma le recenti tendenze indicano che il perimetro tradizionale non esiste più. Attualmente, il singolo collaboratore costituisce il perimetro nonché l'edge. Le soluzioni di sicurezza dei dati di Proofpoint ti permettono di ottenere informazioni in tempo reale sui rischi legati ai dati. Puoi anche prioritizzare e neutralizzare gli incidenti e prevenire la perdita di dati. La piattaforma offre anche un'ampia gamma di funzionalità normative e di conformità, tra cui scoperta, classificazione e crittografia dei dati, che ti aiutano a soddisfare i requisiti normativi e gli standard del settore. Proteggendo gli utenti che trattano le tue informazioni sensibili, proteggerai la tua organizzazione.

proofpoint.

Proofpoint, Inc. è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.

Seguici: LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →