Protezione delle informazioni sanitarie con Proofpoint

Proteggi i dati dei pazienti contro le minacce interne, la perdita di dati e l'espansione del cloud

Prodotti

- 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
- Servizi gestiti Proofpoint per la protezione delle informazioni

Vantaggi principali

- Identificazione e mitigazione dei rischi posti da utenti interni negligenti, compromessi o malintenzionati
- Prevenzione della perdita di dati dall'email, dal cloud e dagli endpoint
- Estensione della protezione scalabile a un crescente numero di servizi cloud ampiamente distribuiti

Il settore della sanità è stato a lungo uno degli obiettivi preferiti dai criminali informatici e la pandemia di COVID-19 ha solo peggiorato la situazione. I criminali informatici hanno intensificato i loro sforzi per ottenere l'accesso a dati preziosi come le informazioni sui test dei vaccini, dati sanitari protetti e dati finanziari. A loro volta, le organizzazioni sanitarie hanno ampliato la loro superficie d'attacco migrando al cloud e permettendo a un maggior numero di dipendenti e pazienti di collegarsi da remoto. Inoltre, affrontano anche un rischio maggiore da parte di minacce interne, sia dolose che involontarie.

Proofpoint offre un approccio incentrato sulle persone per proteggere i dati sensibili nelle reti sanitarie ampiamente distribuite. Le nostre soluzioni per la protezione delle informazioni sono semplici da implementare e gestire. Puoi utilizzarle per creare un'architettura di sicurezza SASE (Secure Access Service Edge) o SSE (Security Service Edge). Ti aiutiamo a proteggere i tuoi dipendenti e i loro dati sensibili da errori accidentali, attacchi e rischi interni in tutto l'ambiente: servizi cloud, email, endpoint e condivisioni di file in locale.

Una minaccia crescente

Una violazione può comportare sanzioni normative e controversie oltre a un danno d'immagine al marchio delle istituzioni sanitarie e persino la morte dei pazienti. Secondo il Dipartimento della Salute e dei Servizi sociali degli Stati Uniti, vi è stato un aumento del 50% delle violazioni di sicurezza in ambito sanitario nella prima metà del 2020. Inoltre, nel 2021 gli attacchi ransomware complessivi sono più che raddoppiati, facendo del settore della sanità uno dei due settori più colpiti.

Il crescente numero di dispositivi IoT (Internet of Things) medici permette di salvare vite umane ma aumenta anche la complessità. A causa della pandemia di COVID-19, molti professionisti si sono rivolti ai servizi di telemedicina, a volte anche da casa piuttosto che da uno studio medico o da un ospedale.

Non sorprende che Moody's Investor Service ritenga che il rischio informatico rimarrà elevato nel settore della sanità per i mesi a venire. Dopo aver gestito quasi due anni di crisi, le organizzazioni sanitarie devono mantenere alta la guardia.

Sfide per la protezione delle informazioni

In questo panorama di minacce preoccupante, ospedali, cliniche, compagnie di assicurazione in ambito sanitario e aziende biotech dovrebbero considerare la protezione delle informazioni una priorità assoluta. Devono salvaguardare le informazioni personali, i dati sanitari e delle carte di credito dei pazienti. Le sfide da affrontare sono numerose.

Prevenzione dello spionaggio delle cartelle cliniche elettroniche e altre minacce interne

Gli operatori sanitari sono gli eroi della pandemia. Durante questo periodo di crisi, hanno svolto il loro lavoro impegnativo e stressante giorno dopo giorno, anche quando non si intravedeva la fine. Una tale situazione di stress può aumentare il rischio di minacce interne. In un momento di relax, dipendenti curiosi potrebbero, per esempio, essere tentati di consultare di nascosto la cartella clinica di un paziente facoltoso. Questo "spionaggio" delle cartelle cliniche elettroniche può rappresentare un grande rischio per un istituto sanitario se le informazioni di un paziente benestante venissero rese pubbliche.

Un dipendente ben intenzionato ma oberato di lavoro, potrebbe fare clic su un'email di phishing, quando in un altro contesto sarebbe in grado di identificarla come pericolosa. Lo stress emotivo può anche essere la fonte di minacce interne dannose contro un datore di lavoro. Un approccio proattivo è quindi essenziale per prevenire tutti questi tipi di minacce.

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 e privati. Ciò ha permesso loro di migliorare l'efficienza operativa ed evitare di impegnare fondi per la creazione di un'infrastruttura IT. Ma la migrazione al cloud ha anche esteso la superficie d'attacco di queste istituzioni.

Anche se le cartelle cliniche elettroniche sono conservate in un'infrastruttura on premise, i dettagli di questi documenti vengono inevitabilmente consultati, condivisi e archiviati altrove, per esempio su dispositivi mobili, endpoint remoti, dispositivi IoT medici e sistemi email basati sul cloud. Più aumentano i canali su cui circolano i dati sanitari, più diventa complicato proteggerli.

Inoltre, 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 spesso software professionali e funzioni di collaborazione. Questi servizi sono vulnerabili alle minacce informatiche. A complicare ulteriormente la situazione, i criminali informatici utilizzano sempre più queste condivisioni di file riconosciute per distribuire i loro exploit.

Protezione del personale sanitario e dei pazienti da remoto a seguito dell'evoluzione dei modelli di distribuzione

Alcuni degli improvvisi cambiamenti che la pandemia ha imposto sul posto di lavoro agli inizi del 2020 si sono rivelati temporanei. Per molti, tuttavia, le conseguenze si faranno sentire per diversi anni a venire. Nel settore della sanità, una tendenza destinata a continuare è l'aumento dell'utilizzo dei servizi di telemedicina. Uno studio ha rilevato che nel febbraio 2021, il ricorso alla telemedicina era ancora 38 volte superiore al livello del 2019. Ciò ha portato un enorme aumento del numero di pazienti con accesso alle risorse delle strutture sanitarie da remoto.

Inoltre, un gran numero di dipendenti è ancora in telelavoro, almeno parzialmente. La maggior parte di loro gestisce cartelle cliniche elettroniche, informazioni finanziarie dei pazienti e dati di ricerca. Il crescente volume di connessioni remote aumenta il rischio di attacchi contro dipendenti che ricoprono ruoli specifici all'interno della struttura.

Adozione di un approccio incentrato sulle persone

Le soluzioni tradizionali di protezione delle informazioni prendono in considerazione solo i dati. Ma le perdite di dati non avvengono per magia: all'origine c'è sempre un'azione umana, che sia accidentale o intenzionale. Nella sicurezza informatica, la visibilità è fondamentale, perciò è necessario comprendere le tipologie di persone che potrebbero rappresentare i rischi maggiori. Un approccio incentrato sulle persone permette di comprendere le dinamiche degli utenti che interagiscono con i dati.

Come Proofpoint può aiutarti

La piattaforma Proofpoint Information and Cloud Security può aiutarti a proteggere le tue informazioni sensibili concentrandosi sulle persone che le gestiscono.

Proofpoint Cloud App Security Broker

Proofpoint Cloud App Security Broker (CASB) protegge gli utenti dalle minacce cloud. Protegge i dati sensibili e gestisce le applicazioni cloud e OAuth all'interno di Microsoft 365, Google Workspace e oltre 900 applicazioni cloud approvate e tollerate dall'IT. Estende ai servizi cloud la visibilità di Proofpoint sui VAP (Very Attacked People™ ovvero le persone più attaccate). Puoi anche migliorare la protezione degli account e dei dati cloud. Proofpoint CASB fornisce una visione granulare dell'accesso al cloud, del comportamento degli utenti e della gestione di dati sensibili come i dati sanitari personali per mantenere la conformità con le normative sulla privacy e sulla sicurezza dei dati.

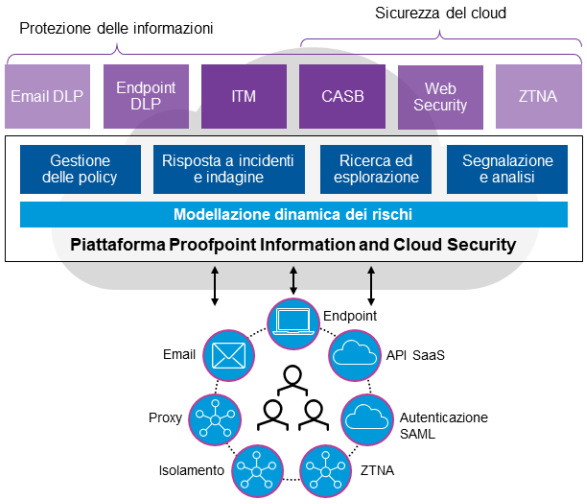

Figura 1. Piattaforma Proofpoint Information and Cloud Security.

Proofpoint CASB può essere distribuito in diversi modi, in base ai casi d'uso. Per una visibilità in tempo reale e una rapida valorizzazione, Proofpoint CASB si integra con i connettori API delle applicazioni cloud e i log alla tua infrastruttura. Per un accesso e controlli dei dati in tempo reale, puoi utilizzare l'autenticazione SAML basata sui rischi, l'isolamento e le funzionalità proxy di trasferimento in linea. Come in una vera architettura SSE, puoi integrare Proofpoint CASB con Proofpoint Web Security e Proofpoint Zero Trust Network Access (ZTNA) per collegare e proteggere i dipendenti remoti nelle applicazioni web e cloud.

Proofpoint Data Loss Prevention

Proofpoint Data Loss Prevention adotta un approccio incentrato sulle persone per la prevenzione della perdita dei dati (DLP). Combina contenuti, comportamenti e minacce e fornisce informazioni contestuali per tutti e tre questi elementi. Queste informazioni sono presentate in una moderna vista temporale, che può fornirti una comprensione più completa e dettagliata di ogni evento. Queste informazioni possono aiutarti a stabilire se un utente segnalato è stato compromesso, ha intenzioni dannose o è semplicemente negligente.

Proofpoint Insider Threat Management

Proofpoint Insider Threat Management (ITM) correla l'attività degli utenti con lo spostamento dei dati. Permette ai team della sicurezza di rilevare, analizzare e neutralizzare le potenziali minacce interne. Offre consapevolezza dei comportamenti incentrata sulle persone. 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 mediche 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. Le informazioni vengono raccolte da sensori endpoint leggeri. Quindi vengono analizzate all'interno di un'architettura moderna per garantire scalabilità, sicurezza e privacy. Proofpoint ITM può anche essere implementato utilizzando modelli di distribuzione on premise o SaaS (Software-as-a-Service).

Proofpoint Web Security

La maggior parte dei tuoi dipendenti si collega dall'esterno del perimetro della rete. Proofpoint Web Security protegge la tua forza lavoro distribuita dalle minacce avanzate quando consultano il web, assicurando la sicurezza della navigazione. Ispezionando tutto il traffico SSL, Proofpoint Web Security rileva e blocca minacce come il ransomware e gli attacchi di phishing zero day. Inoltre, evita che i dipendenti accedano a contenuti pericolosi e non conformi.

Proofpoint Zero Trust Network Access

Con la migrazione delle applicazioni al cloud, il personale sanitario è molto più mobile. Per garantire un accesso sicuro è necessaria un'alternativa più efficace alla VPN. Proofpoint ZTNA sfrutta un perimetro software-defined per ogni utente. Gli utenti dispongono così di un accesso remoto sicuro tramite cloud alle risorse del data center e del cloud.

Ogni utente è autorizzato ad accedere ad applicazioni specifiche e non può vedere il resto della rete. Proofpoint ZTNA convalida gli utenti prima che accedano alla rete migliorando la sicurezza e la visibilità.

Servizi gestiti Proofpoint per la protezione delle informazioni

I nostri servizi gestiti per la protezione delle informazioni offrono ai tuoi team il supporto del nostro gruppo di esperti mondiali di sicurezza dei dati. La nostra esperienza pluriennale ci ha permesso di sviluppare best practice e modelli di maturità per ottimizzare il tuo programma. A tal fine, copriamo la gestione delle applicazioni, l'ambito e la governance delle policy, il triage degli eventi, la gestione degli incidenti, il reporting e l'analisi. Ciò ti protegge 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. Le soluzioni Proofpoint DLP, CASB (Cloud Access Security Broker) e ITM sfruttano il machine learning avanzato e l'analisi umana per proteggere le tue informazioni sanitarie. Gli allarmi vengono analizzati e i team possono intervenire rapidamente nei tentativi di violazione. Lascia che ti aiutiamo a migliorare la tua sicurezza in modo da dare al tuo team più tempo per concentrarsi su altre questioni.

Conclusioni

Le istituzioni sanitarie hanno dovuto affrontare enormi cambiamenti nell'ambiente di lavoro a causa della pandemia di COVID-19. Le superfici d'attacco si sono ampliate. La protezione delle informazioni si è estesa a molteplici cloud. Gli accessi da postazioni remote da parte di dipendenti e pazienti sono in aumento così come il numero di dispositivi IoT medici alla periferia della rete.

Per quasi due decenni, le aziende hanno cercato di proteggere il loro perimetro. La recente esplosione nell'utilizzo dei servizi cloud e la diffusione del telelavoro ha trasformato il telelavoratore nel nuovo perimetro.

Questi rapidi cambiamenti richiedono un'architettura di sicurezza emergente, generalmente conosciuto come architettura SSE ovvero la componente di sicurezza di un'architettura SASE. Una tale architettura fornisce agli utenti l'accesso sicuro di cui hanno bisogno a tutti i servizi cloud attraverso i data center cloud. È all'interno di questa architettura che vengono eseguiti l'accesso alla rete Zero Trust e la gestione delle identità e degli accessi, ed è qui che gli amministratori monitorano gli accessi utilizzando controlli centralizzati.

Puoi anche sfruttare la piattaforma Proofpoint Information and Cloud Security per creare una solida architettura SSE o SASE. In questo modo potrai proteggere l'accesso e garantire la protezione contro le minacce nel momento in cui gli utenti accedono ad applicazioni e dati, indipendentemente da dove si trovano o il tipo di dispositivo che utilizzano. Proteggendo gli utenti che trattano le tue informazioni sensibili, proteggerai la tua organizzazione.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita la pagina **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint 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 più della metà delle Fortune 1000, 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**.

proofpoint.

0207-005-01-01 12/21