proofpoint.

Panoramica sulla soluzione

Garantire la sicurezza delle strutture sanitarie con Proofpoint

Proteggere le persone, gli agenti IA e i dati dei pazienti per garantire un'assistenza sanitaria sicura e resiliente

Panoramica

Data la crescente digitalizzazione, distribuzione e automatizzazione dell'assistenza sanitaria, gli operatori sanitari devono fare i conti con una superficie d'attacco che si estende in tutte le direzioni. Data la carenza di personale, il personale è spesso troppo occupato per rispettare i protocolli di sicurezza. I servizi cloud e i dispositivi medici connessi aggiungono nuovi punti di accesso per gli attacchi. E i flussi di lavoro basati sull'IA introducono nuove vulnerabilità.

I criminali informatici hanno preso atto della situazione e la sfruttano a loro vantaggio. Sanno che le violazioni dei dati del settore sanitario spesso hanno origine dalle persone o dagli agenti IA che agiscono per loro conto. Quindi, si concentrano sugli attacchi basati sull'identità, ingegneria sociale e l'abuso di accessi legittimi.

Proofpoint aiuta ospedali, sistemi sanitari, cliniche e reti integrate di assistenza sanitaria a proteggere i loro medici, il personale, i sistemi e i pazienti. Protegge l'intero ecosistema di persone, agenti IA e dati. Le nostre soluzioni integrate di sicurezza informatica e conformità riducono il rischio di violazioni, proteggono le informazioni sensibili e garantiscono l'erogazione di cure resilienti e senza sosta.

Un settore sanitario ricco di obiettivi di grande valore

Gli operatori sanitari sono tra i principali obiettivi al giorno d'oggi. Non solo operano sotto forte pressione, ma gestiscono anche grandi volumi di dati altamente sensibili, tra cui:

- Informazioni sanitarie protette quali cartelle cliniche, risultati diagnostici e dati relativi alle cure
- Dati di identificazione personale
- Dati finanziari, di fatturazione e relativi alle retribuzioni

Queste informazioni sono di grande valore per i criminali informatici e la loro perdita comporta costi elevati. Una violazione può comportare sanzioni normative, azioni legali, danni alla reputazione e interruzione dell'assistenza e della sicurezza dei pazienti.

Gli operatori sanitari devono inoltre affrontare sfide specifiche legate alla prestazione di assistenza sanitaria:

- I medici hanno bisogno di un accesso rapido e ininterrotto ai sistemi.
- Le comunicazioni contengono frequentemente informazioni sensibili e urgenti.
- I team di assistenza sanitaria collaborano con altri ospedali, cliniche, laboratori e terze parti.
- Controlli legali, verifiche e indagini sono comuni.

Questa suite di soluzioni fa parte della piattaforma Human-Centric Security integrata di Proofpoint volta a proteggere persone e dati nell'ambiente di lavoro agentico.

Gli strumenti di collaborazione via email e cloud sono essenziali per un'assistenza coordinata. Tuttavia, sono anche i principali punti di accesso per i criminali informatici.

In base *alreport 2025 sulle violazioni dei dati* di Verizon il 60% delle violazioni implica un intervento umano.

Sfide legate alla sicurezza informatica per gli operatori sanitari

Man mano che gli operatori sanitari modernizzano le loro operazioni, devono affrontare rischi crescenti.

Proteggere i dati dei pazienti e i dati clinici

Gli operatori sanitari devono proteggere le informazioni di identificazione sanitaria, i dati a carattere personale e i dati finanziari a livello di email, piattaforme cloud e endpoint. Qualsiasi violazione può comportare violazioni delle leggi HIPAA e HITECH, sanzioni nazionali in materia di privacy, problemi di conformità PCI DSS e costosi contenziosi legali.

Gestire i rischi legati agli utenti interni negli ambienti clinici

Il rischio elevato associato agli utenti interni è ovunque. Non solo il turnover del personale è elevato, ma c'è anche un continuo avvicendamento tra i membri del personale, collaboratori esterni e residenti. Inoltre, le cartelle cliniche elettroniche sono inoltre oggetto di un ampio accesso. L'esposizione accidentale dei dati, la condivisione delle credenziali d'accesso e l'uso improprio degli accessi sono tutti fattori che possono portare a violazioni che devono essere segnalate alle autorità.

Bloccare i furti d'identità e i takeover degli account

Gli operatori sanitari si affidano a un complesso ecosistema di terze parti: laboratori, venditori di dispositivi medici, fornitori, assicuratori, agenzie governative, ecc. I criminali informatici sfruttano queste relazioni di fiducia utilizzando tecniche quali la violazione dell'email aziendale (Business Email Compromise, BEC), il furto d'identità dei fornitori e il phishing delle credenziali d'accesso. Le caselle email condivise e gli account di servizio sono obiettivi particolarmente allettanti.

Rispondere rapidamente alle minacce avanzate

I team della sicurezza affrontano un numero di avvisi enorme. Inoltre, non è sempre facile adattare le verifiche manuali, in particolare quando gli attacchi raggiungono centinaia di utenti o provengono da identità affidabili che sembrano legittime.

Prepararsi per un ambiente di assistenza sanitaria basato sul cloud

I medici accedono sempre più spesso a sistemi da remoto e utilizzano spesso i loro dispositivi personali per farlo. Instradare tutto il traffico attraverso controlli di sicurezza in sede non è più pratico. Per garantire una sicurezza efficace, i Team devono poter stabilire chi accede ai dati sensibili, come e perché.

Un approccio alla sicurezza sanitaria incentrato sulle persone e sugli agenti

Insieme, persone e agenti costituiscono oggi la superficie operativa dell'erogazione dell'assistenza sanitaria. Sebbene i medici e il personale siano responsabili dell'implementazione dei processi aziendali e di cura, beneficiano anche di assistenza. Molti compiti vengono ora eseguiti da agenti non umani, tra cui:

- Caselle email condivise e account di servizio
- Identità e API cloud
- Flussi di lavoro di automazione e sistemi basati sull'IA
- Dispositivi medici connessi
- Applicazioni cliniche e aziendali come Epic

Ecco perché gli attacchi informatici odierni non prendono di mira solo la tecnologia. Sfruttano persone e agenti fidati.

Sfortunatamente, gli strumenti di sicurezza tradizionali basati sul perimetro non sono in grado di distinguere tra azioni legittime e comportamenti dannosi. Ciò è particolarmente vero quando i criminali informatici utilizzano identità compromesse anziché malware per le loro attività fraudolente.

Proofpoint protegge questo ambiente correlando identità, comportamenti e accessi ai dati sia delle persone sia degli agenti. Questo approccio permette di eliminare i punti ciechi che i criminali informatici sfruttano attivamente.

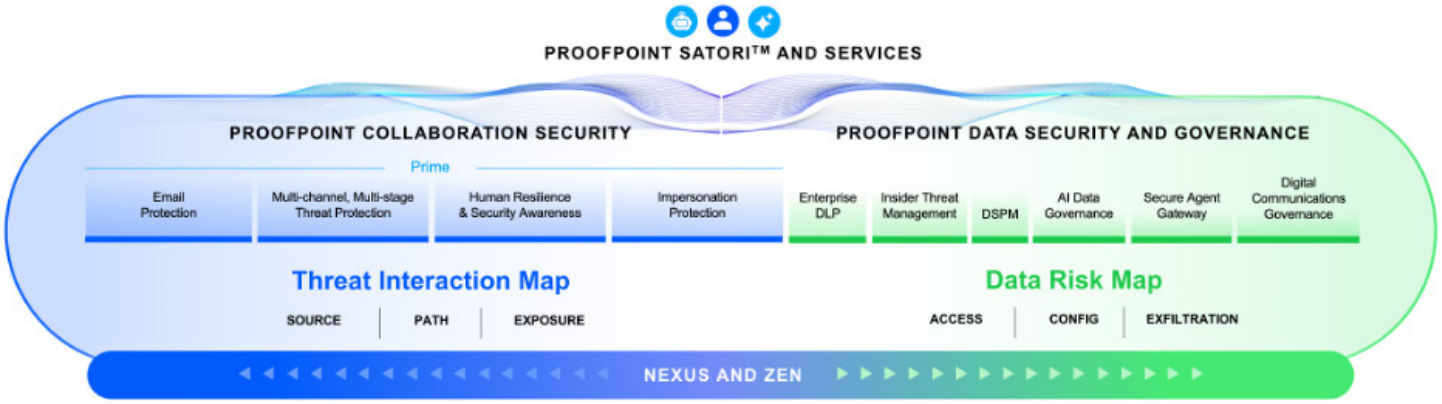


Figura 1. Le soluzioni Proofpoint proteggono l'intero ecosistema composto da persone, agenti IA e dati.

Prodotti

- Proofpoint Collaboration Security Prime
- Proofpoint Secure Email Relay
- Proofpoint Data Loss Protection (DLP)
- Proofpoint Adaptive Email DLP
- Proofpoint Data Security Posture Management (DSPM)
- Proofpoint Satori
- Proofpoint Account Takeover Protection
- Proofpoint Insider Threat Management
- Proofpoint Communications Governance
- Proofpoint ZenGuide

Come Proofpoint può aiutare gli operatori sanitari

Adottata dal 67% delle aziende della classifica Fortune 500 operanti nel settore sanitario, Proofpoint è l'unico fornitore a offrire una piattaforma integrata che protegge al contempo persone, agenti e dati. Questa sezione illustra i numerosi modi in cui possiamo aiutarti.

Protezione contro il ransomware e altre minacce avanzate

Proofpoint Collaboration Security Prime offre un approccio end-to-end per bloccare gli attacchi che prendono di mira le persone e gli agenti a livello di email, strumenti di collaborazione, applicazioni cloud, canali web e piattaforme social. Ottimizzato da **ProofpointNexus®**, utilizza IA avanzata, analisi comportamentale e threat intelligence per bloccare gli attacchi durante l'intero ciclo di vita della minaccia, prima della consegna, dopo la consegna e al momento del clic.

Protezione delle comunicazioni critiche tramite email e applicazioni

Gli operatori sanitari si affidano alle email generate dal sistema per i flussi di lavoro clinici e operativi essenziali, tra cui:

- Notifiche ai pazienti e promemoria degli appuntamenti
- Coordinamento delle cure e avvisi clinici
- Estratti conto e comunicazioni finanziarie
- Conformità, report e messaggi amministrativi: Queste comunicazioni vengono spesso inviate in grandi quantità da applicazioni affidabili e devono essere:
  - Consegnate in modo affidabile
  - Autenticate e approvate dai destinatari
  - Sicure e conformi

Proofpoint Secure Email Relay consente agli operatori sanitari di inviare in modo sicuro grandi volumi di email generate dalle applicazioni, proteggendo al contempo pazienti, partner e l'azienda da furto d'identità e frodi. Proofpoint Secure Email Relay:

- Consente la consegna di email conformi allo standard DMARC da applicazioni critiche quali Epic, ServiceNow e altre piattaforme cliniche e aziendali.
- Protegge le email generate dal sistema dal furto d'identità e dall'utilizzo improprio di domini fotocopia
- Garantisce la fiducia e l'integrità delle comunicazioni operative e rivolte ai pazienti.
- Riduce i rischi legati provenienti da applicazioni compromesse o configurate in modo errato.

Proteggendo i mittenti non umani, Proofpoint Secure Email Relay amplia il modello di sicurezza informatica incentrato sugli agenti di Proofpoint. Garantisce che le comunicazioni sanitarie critiche rimangano affidabili, conformi e resilienti.

Protezione dei dati dei pazientiLe soluzioni P**roofpoint Data Loss Prevention (DLP)** prevengono la perdita accidentale e dannosa di dati tramite email, cloud ed endpoint fornendo una visibilità estesa sul comportamento degli utenti e sui contenuti.

Proofpoint Adaptive Email DLP utilizza l'IA comportamentale per analizzare i normali modelli di invio delle email e fornire avvisi contestuali in tempo reale ai medici e al personale. Impedisce l'invio di messaggi al destinatario errato e l'esposizione dei dati senza interrompere l'erogazione delle cure.

Proofpoint Data Security Posture Management (DSPM) identifica dove risiedono i dati sensibili, quali persone e agenti possono accedervi così come i casi in cui vengono concesse autorizzazioni eccessive

o rischiose. I fornitori possono così ridurre l'esposizione e adottare in modo sicuro l'IA e l'automazione.

Proofpoint Satori™ amplia Proofpoint DSPM con la governance dell'accesso ai dati in tempo reale per gli ambienti sanitari. Proofpoint Satori monitora e controlla costantemente l'accesso ai dati sensibili dei pazienti, in particolare per quanto riguarda archivi dati cloud, piattaforme di analisi e pipeline di IA, senza interferire con i flussi di lavoro clinici.

Grazie a Proofpoint Satori, i fornitori possono:

- Identificare e classificare i dati sensibili dei pazienti e i dati clinici su tutte le piattaforme cloud
- Applicare l'accesso del minimo privilegio per medici, personale, applicazioni e agenti IA
- Rilevare e correggere in tempo reale gli accessi ai dati a rischio o anomali
- Applicare controlli basati su policy per proteggere le informazioni di identificazione sanitaria consentendo l'analisi, la ricerca e l'innovazione nell'ambito dell'IA.

Rilevamento delle violazioni e degli usi impropri su larga scala

Proofpoint Account Takeover Protection e **Proofpoint Insider Threat Management** rilevano comportamenti sospetti sia nelle identità delle persone sia in quelle degli agenti. Identificano le violazioni delle credenziali, d'accesso l'abuso dei privilegi, gli spostamenti laterali e le sottrazioni di dati. Correlando identità, comportamenti e spostamenti dei dati, Proofpoint permette di intervenire in modo più rapido e preciso prima che l'assistenza sanitaria venga interrotta.

Conformità e preparazione ad eventuali contenziosi

Le soluzioni Proofpoint Digital Communications Governance semplificano il rispetto delle leggi HIPAA e HITECH e i requisiti di conservazione dei dati. Garantiscono che le comunicazioni cliniche e aziendali siano acquisite, consultabili e disponibili per revisioni, indagini ed eDiscovery.

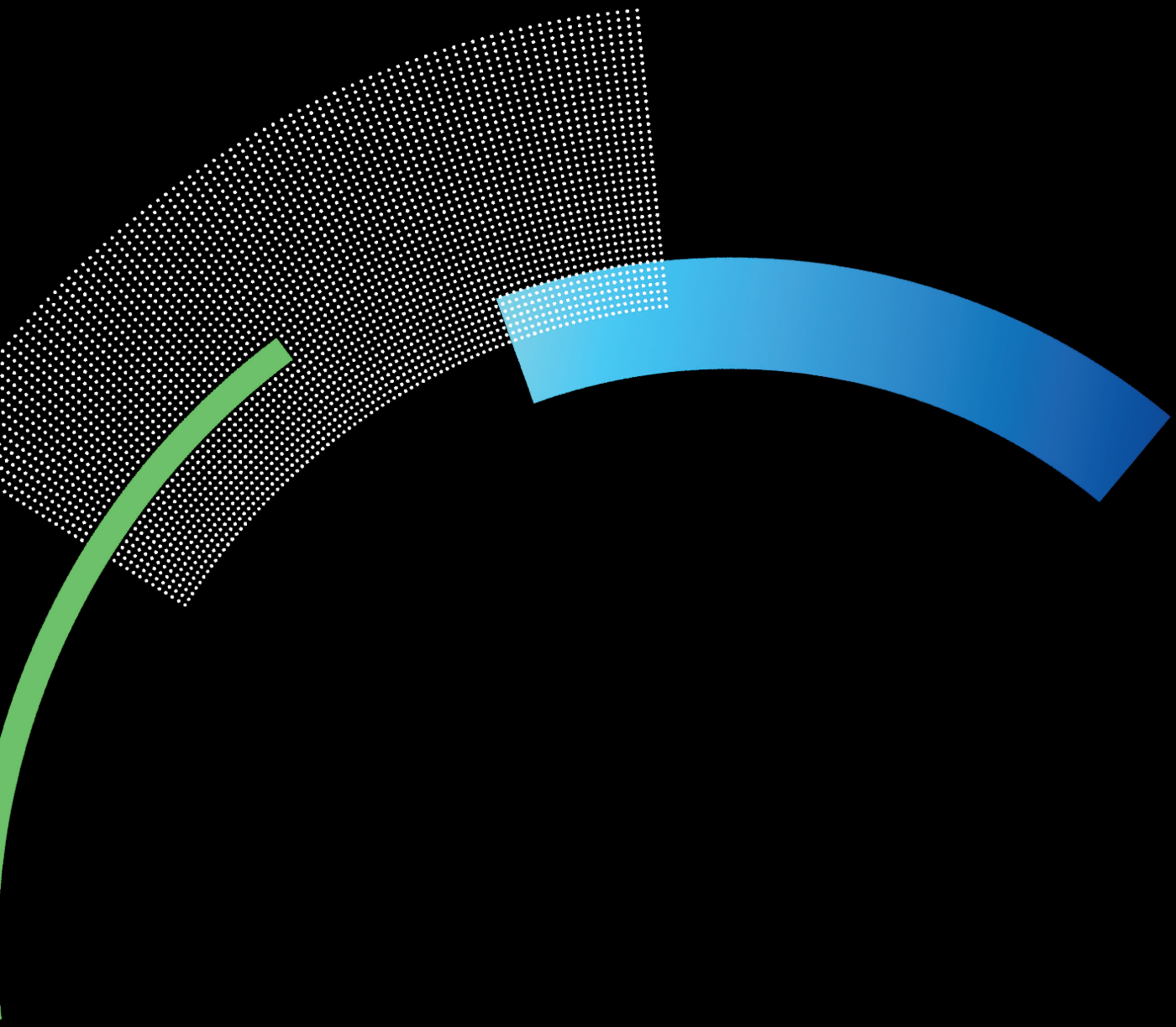
Riduzione dei rischi attraverso un cambiamento dei comportamenti

Proofpoint ZenGuide™ offre formazione di sensibilizzazione alla sicurezza basata sui ruoli e sui rischi, pensata su misura per medici e personale sanitario. Rafforza i comportamenti sicuri utilizzando scenari di minaccia reali per la sanità senza rallentare l'erogazione delle cure.

Conclusione

Proofpoint ha sempre protetto le persone. Ora la nostra piattaforma di sicurezza incentrata sulle persone e sugli agenti estende la protezione a ogni interazione tra collaboratori, dati e agenti IA. Garantisce controllo, conformità e la libertà di abbracciare l'innovazione.

Grazie a Proofpoint, gli operatori sanitari possono ridurre il rischio di violazioni, proteggere i dati dei pazienti, garantire la conformità e fornire assistenza sanitaria resiliente e ininterrotta in un panorama di minacce complesso.



proofpoint.

Informazionisu Proofpoint, Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 delle aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiutaaziendeditutteledimensioniaproteggeree responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per ulteriori informazioni, visitare il sito: www.proofpoint.com/it.

Seguici : LinkedIn

SCOPRIO LA PIATTA FORMA PROOFPOINT →