

Un'azienda innovatrice nel settore delle tecnologie medicali collabora con Proofpoint per proteggere e accelerare le sue operazioni

La sfida

- Proteggere l'email dal phishing e altre minacce
- Ridurre il più possibile i processi manuali per liberare il team IT
- Migliorare le best practice di sicurezza dell'azienda

La soluzione

- Proofpoint Email Protection
- Proofpoint Email Fraud Defense
- Proofpoint Targeted Attack Protection
- Proofpoint Domain Discover
- Proofpoint Threat Response Auto-Pull
- Proofpoint Closed-Loop Email Analysis and Response
- Proofpoint Security Awareness

I risultati

- La protezione dell'email in tempo reale riduce il rischio di phishing e altre minacce.
- L'automazione della sicurezza dell'email riduce il numero di processi manuali.
- La formazione di sensibilizzazione alla sicurezza informatica rafforza il livello di sicurezza generale.

L'azienda

Con oltre 20 sedi in tutto il mondo e circa 8.000 collaboratori, questa azienda innovatrice nel campo dei dispositivi medici conosce l'importanza di preservare la fiducia nelle comunicazioni digitali. Questo fornitore di servizi globale vanta una solida reputazione nello sviluppo di dispositivi medici innovativi volti a migliorare la qualità della vita. L'azienda è impegnata a proteggere i suoi clienti, i suoi collaboratori e il suo marchio. Si contraddistingue per l'offerta di un livello di servizio e di attenzione ai dettagli che riflette una relazione stretta con i clienti, ma con le risorse di una grande azienda.

La sfida

Protezione dei clienti e dei collaboratori nel settore della sanità

Quest'azienda specializzata nella produzione di dispositivi medici mantiene un netto vantaggio competitivo grazie a un'ampia gamma di competenze, all'integrazione end-to-end, all'avanzata esperienza tecnica, alla costante focalizzazione sui suoi clienti e sull'eccellenza operativa. Come ogni azienda globale, si affida a un'infrastruttura di rete sicura per alimentare tutti i suoi processi aziendali.

Tuttavia, con l'evoluzione del panorama delle minacce, il team della sicurezza dell'azienda si è reso conto di dedicare troppo tempo alla protezione delle comunicazioni aziendali. Il sistema di sicurezza dell'email esistente era difficile da configurare e allineare alle esigenze dell'azienda. Inoltre, non era efficace nel bloccare le minacce più recenti.

“Il nostro sistema di sicurezza dell'email non soddisfaceva le nostre esigenze” spiega il responsabile della sicurezza. “Molte minacce, tra cui attacchi di phishing e raccolta delle credenziali di accesso, aggiravano le nostre difese. Non potevamo fidarci abbastanza della nostra soluzione esistente e dovevamo dedicare molto tempo e numerose risorse per bloccare manualmente gli attacchi. A peggiorare le cose, ci siamo resi conto che la nostra formazione di sensibilizzazione alla sicurezza informatica non era davvero all'altezza”.

L'azienda ha deciso di aggiornare il suo sistema per fornire una protezione più completa contro le minacce avanzate, tra cui phishing, frodi via email e domini fraudolenti che utilizzavano in modo improprio il suo marchio. Desiderava non solo una sicurezza dell'email efficace, ma anche funzionalità di analisi e generazione di report per un processo decisionale migliore e più strategico.

La soluzione

Verso un approccio alla sicurezza incentrato sulle persone

L'azienda ha preso in considerazione diversi prodotti di sicurezza dell'email per trovare quello che meglio rispondeva alle sue esigenze. La scelta è ricaduta su Proofpoint, che offriva la soluzione più completa e con il miglior supporto.

“Abbiamo effettuato valutazioni personalizzate con prodotti della concorrenza e la scelta è stata motivata dal supporto e dal livello di attenzione che ci offriva Proofpoint”, commenta il responsabile della sicurezza. “Proofpoint ci ha fornito una visione della sicurezza incentrata sulle persone”.

“Proofpoint offre un reale risparmio di tempo e risorse. La soluzione permette al nostro team di essere più proattivo nel nostro approccio alla sicurezza, invece che reattivo come in passato. In un certo modo, possiamo utilizzare Proofpoint come se fosse un membro aggiuntivo del team”.

Responsabile della sicurezza, azienda del settore dei dispositivi medici

Il responsabile della sicurezza e il suo team hanno implementato diverse soluzioni che lavorano di concerto per bloccare malware, phishing e frodi, permettendo di automatizzare le operazioni di sicurezza e risposta alle minacce.

“Proofpoint Email Protection, Proofpoint Targeted Attack Protection (TAP), Proofpoint Threat Response Auto-Pull (TRAP) e Proofpoint Closed-Loop Email Analysis and Response (CLEAR), lavorano insieme per chiudere il cerchio e consentire una risposta automatica”, afferma il responsabile della sicurezza. “Questi strumenti eliminano gran parte delle attività manuali che erano necessarie per indagare sulle minacce”.

Il responsabile della sicurezza e il suo team hanno sfruttato la formazione Proofpoint per assicurare una transizione fluida e una migrazione senza problemi alla nuova soluzione.

“L'esperienza vissuta ha sicuramente fatto la differenza”, conferma il responsabile della sicurezza. “Proofpoint ha un approccio basato su roadmap. Si seguono le varie fasi e tutto ha un senso. Potevamo progredire secondo i nostri tempi”.

Il processo di migrazione ha anche aiutato l'azienda a rafforzare le sue policy DMARC (Domain-based Message Authentication, Reporting, and Conformance) per una miglior protezione contro lo spoofing delle email e i tentativi di frode.

“Le nostre policy DMARC generalmente erano per la quarantena, perché non disponevo di una visibilità sufficiente su tutti i miei mittenti”, precisa il responsabile della sicurezza. “Abbiamo avuto modo di comprenderlo meglio durante il processo di migrazione. Abbiamo ottenuto maggior visibilità su tutte le email inviate utilizzando il nostro dominio. Questo ci ha aiutato molto con l'implementazione di Proofpoint Email Fraud Defense nel nostro ambiente”.

Proofpoint Email Fraud Defense offre inoltre visibilità sui domini fotocopia che potrebbero essere utilizzati per siti web di phishing e attacchi email. Per proteggere ulteriormente la reputazione delle aziende, il responsabile della sicurezza ha recentemente aggiunto Proofpoint Virtual Takedown. Questo servizio aggiuntivo aiuta l'azienda a gestire il processo di blocco e smantellamento di domini dannosi.

Il team era inoltre cosciente del ruolo fondamentale che i collaboratori giocano nel difendere l'azienda. Per rafforzare tale aspetto, il responsabile della sicurezza ha acquistato Proofpoint Security Awareness, che utilizza un approccio alla formazione basato sui dati per promuovere una cultura di best practice di sicurezza.

“Gestiamo un programma di formazione trimestrale per tutti i nostri collaboratori, e richiediamo una partecipazione del 100%”, spiega il responsabile della sicurezza.

“Siamo inflessibili su questo punto”.

I risultati

Ridurre al minimo rischi e raccolta di informazioni rilevanti

L'intera gamma di soluzioni Proofpoint di protezione dell'email ha permesso all'azienda di rafforzare e automatizzare le analisi, la protezione e la neutralizzazione delle minacce trasmesse via email, come phishing e malware. La soluzione contribuisce a proteggere l'azienda e i suoi clienti, e riduce inoltre il carico di lavoro del team della sicurezza.

“Ogni volta che si verifica un qualunque incidente di sicurezza, tutto deve essere registrato e categorizzato nel nostro sistema”, afferma il responsabile della sicurezza.

“Siamo passati da 800-1.000 ticket al mese, a meno di 150. Si tratta di un enorme calo, che ha liberato le nostre risorse dalle attività manuali”.

Proofpoint TAP si è anche rivelato utile nel fornire al responsabile della sicurezza e al suo team visibilità in tempo reale e informazioni fruibili sulle minacce e i loro obiettivi, consolidate in una dashboard. La soluzione si è dimostrata particolarmente efficace nel proteggere i collaboratori che ricoprono posizioni sensibili, presi di mira dalla maggior parte delle minacce. L'analisi fornita da Proofpoint aiuta l'azienda a comprendere le caratteristiche ricorrenti e le tendenze delle minacce e gli attacchi contro i suoi VAP™ (Very Attacked People ovvero le persone più attaccate).

“Sulla base delle informazioni che evidenziano i collaboratori più presi di mira e attaccati, abbiamo creato delle policy di accesso condizionale Microsoft per assicurarci che tali utenti siano protetti al meglio”, afferma il responsabile della sicurezza.

Il responsabile della sicurezza apprezza inoltre le funzionalità di reportistica della soluzione, che permette al team di risparmiare tempo prezioso, e li aiuta a mantenere informati i dirigenti in merito al livello di sicurezza complessivo dell'azienda.

“La qualità dell'assistenza che riceviamo da Proofpoint è stato uno dei principali vantaggi per noi”, spiega il responsabile della sicurezza. “I report ci permettono di risparmiare tempo e ci forniscono una visione su tutti i dati. Inoltre, vengono presentati in modo tale da consentirci di modificare i nostri comportamenti e adottare un approccio più proattivo alla sicurezza. Possiamo utilizzarli anche per creare diverse presentazioni per gli incontri con la nostra dirigenza, per aiutarli a comprendere le minacce trasmesse via email e come le gestiamo. Utilizziamo anche la reportistica di Proofpoint Security Awareness per stimolare la sensibilizzazione e la formazione”.

Grazie ai prodotti, servizi e formazione di Proofpoint implementati nel suo ambiente, quest'azienda innovatrice nel settore dei dispositivi medici può ora passare da un approccio reattivo a uno più strategico in termini di sicurezza, che le permette di sfruttare il meglio delle persone e della tecnologia.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito [proofpoint.com/it](https://www.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 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.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.