Prodotti Proofpoint

Proofpoint offre protezione e visibilità per le risorse più importanti e più pericolose della tua azienda: le persone. Forniamo gli strumenti più efficaci oggi disponibili per proteggere le persone dalle minacce, per salvaguardare le informazioni che creano e a cui accedono e per proteggere gli utenti stessi.

Le nostre soluzioni per la sicurezza informatica e la conformità proteggono email, social media, web, rete e cloud, compreso Microsoft Office 365, Offriamo inoltre integrazioni tecnologiche strategiche con i principali fornitori di soluzioni di sicurezza del settore. Puoi così proteggere meglio le tue persone, i tuoi dati e il tuo marchio.

PROTEZIONE DELL'EMAIL

Proteggiti dalle minacce email, assicura la continuità delle comunicazioni tramite email e implementa delle policy per i messaggi in ingresso e in uscita.

Email Protection

Proofpoint Email Protection protegge gli utenti da email indesiderate e pericolose, che contengono o meno malware, come per esempio le email di truffatori o la violazione delle email aziendali. La nostra soluzione garantisce una visibilità estremamente accurata e la business continuity ad aziende di tutte le dimensioni. Controllando tutti gli aspetti delle email in ingresso e in uscita e impostandone le relative policy, aiutiamo i tuoi team dedicati all'IT e alla sicurezza a proteggere gli utenti finali dalle minacce email e ad assicurare la continuità delle comunicazioni email in caso di interruzione del servizio.

Email Fraud Defense (EFD)

Proofpoint Email Fraud Defense (EFD) protegge i tuoi collaboratori, i tuoi clienti e i tuoi partner commerciali da ogni forma di frode via email bloccando gli attacchi fraudolenti prima che possano raggiungere la casella di posta in arrivo. Puoi autorizzare le email legittime, bloccare i messaggi fraudolenti e visualizzare tutte le minacce, a prescindere dalla tattica usata o dalla persona presa di mira, da un unico portale. Grazie all'autenticazione dell'email combinata con machine learning e policy e all'applicazione dell'autenticazione DMARC, Proofpoint Email Fraud Defense ti aiuta a contrastare tutte le varie tattiche fraudolente utilizzare dai criminali per sferrare attacchi avanzati.

Threat Response Auto-Pull (TRAP)

Proofpoint Threat Response Auto-Pull (TRAP) utilizza funzionalità di orchestrazione e automazione per ritirare le email dannose già recapitate nella casella di posta in arrivo degli utenti. Questa versione di base della soluzione Threat Response identifica e rimuove le email dannose in base agli avvisi generati dalla soluzione Proofpoint Targeted Attack Protection (TAP). Quindi, utilizza una logica di business per tracciare le copie consegnate ad altri destinatari al fine di eliminarle. TRAP genera anche dei report che mostrano i tentativi di quarantena, il fallimento o il successo di tali tentativi, oltre a un elenco degli utenti più colpiti, riducendo così il carico di lavoro del team di sicurezza.

Internal Mail Defense

Proofpoint Internal Mail Defense utilizza un solido approccio di sicurezza multi-livello per proteggere il sistema email interno delle aziende e facilitare l'identificazione degli account compromessi. La soluzione analizza tutte le email interne alla ricerca di spam, allegati dannosi e URL pericolosi. I messaggi email contrassegnati, vengono rimossi e messi in quarantena automaticamente. Inoltre, il team della sicurezza ha anche visibilità sugli account che hanno inviato tali URL pericolosi, e può rintracciarli rapidamente e agire su quelli potenzialmente compromessi.

Essentials per le piccole aziende

Proofpoint Essentials adatta le funzionalità di Email Protection alle necessità delle piccole imprese. La soluzione offre molteplici funzionalità: filtraggio dello spam, rilevamento del phishing, antivirus multi-livello, sandboxing dinamico degli URL, un potente motore per le regole di filtraggio, continuità dell'email, crittografia basata su policy, archiviazione delle email e protezione degli account social media. Un'interfaccia semplice e intuitiva ne facilita la gestione, una risorsa preziosa per le PMI che dispongono di team dedicati alla sicurezza ridotti.

PROTEZIONE CONTRO LE MINACCE AVANZATE

Rileva, ricerca e rispondi alle minacce in modo più rapido, preciso e affidabile.

Targeted Attack Protection (TAP)

Proofpoint Targeted Attack Protection (TAP) aiuta a rilevare, mitigare e bloccare le minacce avanzate che contengono allegati e URL dannosi che colpiscono le persone attraverso l'email e altre app cloud, come Microsoft Office 365 e Google G Suite. TAP offre visibilità completa sui VAP (Very Attacked People ovvero le persone più attaccate) all'interno della tua azienda. Offre inoltre gli strumenti necessari per riscrivere tutti gli URL incorporati per proteggere gli utenti su tutti i dispositivi e tracciare i clic sui collegamenti pericolosi.

Email Isolation

Proofpoint Email Isolation permette ai team IT e della sicurezza di garantire agli utenti l'accesso alla webmail aziendale dai dispositivi dell'azienda in totale sicurezza. La soluzione può essere integrata con Targeted Attack Protection (TAP) per rafforzare ulteriormente la sicurezza dei tuoi VAP, proteggendo comunque tutti gli utenti da siti web sconosciuti o pericolosi. Tale protezione è assicurata evitando che malware o contenuto dannoso raggiungano l'utente o il dispositivo. Il nostro servizio cloud isola il contenuto web dai dati e dalle reti aziendali. Inoltre, semplifica la governance dei rischi e il controllo dei costi operativi, migliorando il livello di sicurezza.

Browser Isolation

Proofpoint Browser Isolation estende le funzionalità di Proofpoint Email Isolation per proteggere tutte le attività di navigazione sul web per tutti gli utenti, inclusi i VAP. Offre un servizio di navigazione web sicuro e anonimo, che il tuo team IT può distribuire, gestire e supportare con facilità. La privacy dei tuoi utenti viene così preservata quando accedono a siti come la webmail e senza ulteriori rischi per la tua azienda.

Threat Response

Proofpoint Threat Response è progettato per migliorare l'efficacia degli addetti alle operazioni di sicurezza. Offre una vista fruibile delle minacce di rete, permette di integrare gli avvisi e di automatizzare la raccolta e il confronto dei dati di analisi. La soluzione permette anche di eliminare il lavoro manuale e le ipotesi dalle attività di risposta agli eventi. Il tuo team della sicurezza può così porre rimedio alle minacce in modo più rapido ed efficiente. E a differenza degli strumenti tradizionali per l'elaborazione della risposta agli eventi, la soluzione conferma automaticamente le infezioni da parte del malware, verifica le prove di precedenti infezioni e e aggiunge automaticamente agli avvisi di sicurezza le informazioni e il contesto pertinenti raccolti da fonti interne ed esterne.

Emerging Threats Intelligence

Proofpoint Emerging Threats Intelligence (ET) è la soluzione più accurata per i ricercatori delle minacce. Offre informazioni sulle minacce verificate al 100% da una delle più grandi piattaforme di interscambio di malware al mondo. E permette di comprendere meglio il contesto cronologico dettagliato dell'origine e dell'autore di una minaccia, integrandosi in totale trasparenza con gli strumenti di sicurezza che già utilizzi. A differenza delle altre fonti di informazioni similari che segnalano solo domini o indirizzi IP all'origine delle minacce, il nostro sistema include uno storico di 10 anni, un "verdetto di colpevolezza" e oltre 40 categorie di minaccia con relativi IP, domini e campioni.

Emerging Threats Pro Ruleset

Proofpoint Emerging Threats (ET) Pro Ruleset è una serie di regole che permette di rilevare e bloccare le minacce, in modo preciso e immediato, usando le appliance di sicurezza della rete esistenti, come i firewall di nuova generazione e i sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS). Aggiornato quotidianamente nei formati Suricata e SNORT, ET Pro Ruleset copre oltre 40 diverse categorie di comportamenti in rete, comando e controllo del malware, attacchi DoS, botnet, exploit, vulnerabilità, protocolli di rete SCADA, attività dei kit di exploit e molto altro ancora. Grazie ad aggiornamenti quotidiani e all'utilizzo di un ambiente sandbox automatizzato, il tuo team della sicurezza ha la certezza che tutte le minacce siano valutate con successo.

Premium Threat Information Service (PTIS)

Premium Threat Information Service (PTIS) permette di stabilire le priorità in materia di decisioni per la sicurezza fornendo informazioni di contesto più approfondite sulla situazione del panorama delle minacce in costante evoluzione. Include tre componenti: accesso diretto ai nostri ricercatori delle minacce, leader del settore, report mensili personalizzati sulle minacce e avvisi avanzati relativi alle minacce emergenti grazie all'accesso ai registri degli analisti. Questo servizio permette di fidelizzare esperti analisti, difficili da trovare, e li aiuta riducendo i processi manuali e consentendo loro di concentrarsi sulle problematiche più cruciali per l'azienda.

SECURITY AWARENESS TRAINING

Trasforma gli utenti finali nella tua ultima e solida linea di difesa contro il phishing e gli altri attacchi informatici insegnando loro a identificare e segnalare le minacce.

Anti-Phishing Suite

Proofpoint Anti-Phishing Suite aiuta ad identificare e ridurre fino al 90% la vulnerabilità dei dipendenti agli attacchi di phishing e alle infezioni da malware. Se un utente si lascia ingannare da un attacco di phishing simulato ThreatSim, gli viene proposto un "messaggio educativo" con consigli su come rimanere al sicuro in futuro. Gli utenti che si fanno ingannare da un attacco simulato possono essere automaticamente iscritti a uno dei nostri 8 moduli di formazione antiphishing. Possono anche essere assegnati in

modo selettivo. Inoltre, grazie a questo pacchetto, gli amministratori hanno accesso al nostro tasto di segnalazione email PhishAlarm® e agli strumenti di analisi delle email PhishAlarm Analyzer. Questi strumenti costituiscono il primo elemento della nostra soluzione Closed Loop Email Analysis and Response (CLEAR), una soluzione che razionalizza la procedura di segnalazione e automatizza la risposta agli attacchi di phishing attivi.

Security Awareness Training Enterprise

Il pacchetto Proofpoint Security Awareness Training Enterprise include tutti i componenti della suite Proofpoint Anti-Phishing Suite e aggiunge le simulazioni d'attacco tramite USB ThreatSim, le valutazioni delle conoscenze CyberStrength®, la nostra intera libreria di moduli di formazione e tutti i nostri materiali di sensibilizzazione alla sicurezza, video inclusi. Quest'offerta è ideale per i clienti che desiderano attivare un programma di formazione e sensibilizzazione alla sicurezza completo ed efficace. Grazie alla disponibilità di più strumenti per identificare il rischio, cambiare il comportamento e ridurre l'esposizione ai rischi, puoi implementare una strategia più efficace volta alla riduzione del rischio incentrata sulle persone.

PROTEZIONE DELLE APP CLOUD

Proteggi i tuoi dipendenti e i tuoi dati da minacce, perdite di dati e rischi di conformità nelle applicazioni cloud.

Cloud Account Defense (CAD)

Proofpoint Cloud Account Defense (CAD) offre protezione automatica contro la violazione degli account e i file dannosi in Microsoft Office 365 e Google G Suite. La violazione degli account inizia tipicamente con un attacco di phishing, un malware per il furto delle credenziali oppure attacchi di forza bruta come il riciclaggio degli identificativi di connessione, noto come credential stuffing. Gli account compromessi sono generalmente utilizzati per lanciare ulteriori attacchi interni o esterni, come la violazione dell'email aziendale o il phishing. Proofpoint CAD permette di rilevare, analizzare e proteggersi rapidamente dai criminali informatici che accedono a dati sensibili e account affidabili. La soluzione fornisce funzioni di rilevamento delle minacce incentrato sulle persone, correlazione dell'attività delle minacce, analisi granulari con informazioni complete sulle minacce e policy flessibili per risposte automatizzate.

Cloud App Security Broker

Proofpoint Cloud App Security Broker (PCASB) protegge le aziende dalla violazione degli account nel cloud, dalla condivisione accidentale di dati sensibili e dai rischi per la conformità nel cloud. PCASB offre una visione granulare incentrata sulle persone per quanto riguarda l'accesso alle app e la gestione dei dati. La nostra soluzione combina funzioni di rilevamento degli account compromessi, controllo degli accessi, prevenzione della perdita di dati (DLP), controllo delle app di terze parti e analisi per proteggere le piattaforme Microsoft Office 365, Google G Suite, Box e altro ancora. I nostri potenti strumenti di analisi aiutano a garantire i giusti livelli di accesso agli utenti e alle app di terze parti in base ai fattori di rischio che sono per te importanti.

PROTEZIONE DELLE INFORMAZIONI

Una soluzione che Individua, monitora e proteggi i dati delle email, delle applicazioni Cloud, delle condivisioni di file in sede e di siti SharePoint.

Email Data Loss Prevention (DLP)

Proofpoint Email DLP previene gli incidenti causati dalla negligenza di alcuni dipendenti relativamente alle comunicazioni in uscita grazie a una soluzione di prevenzione della perdita di informazioni private e sensibili. Invece di costringere gli utenti finali a prendere delle decisioni in merito alla natura dei contenuti che inviano e alla protezione di cui hanno bisogno (che potrebbe complicare la loro attività e far perdere loro del tempo prezioso), puoi permettere loro di operare normalmente lasciando che la soluzione applichi le policy per le comunicazioni email in modo centralizzato e automatizzato. Grazie ad oltre 80 policy ottimizzate che individuano, classificano e bloccano automaticamente i messaggi sensibili, la soluzione riduce le probabilità di una violazione dei dati.

Email Encryption

Proofpoint Email Encryption fornisce agli utenti una soluzione in grado di proteggere le comunicazioni email in modo semplice, trasparente e automatizzato attraverso la crittografia dei messaggi e degli allegati basata su policy. I tradizionali servizi di crittografia dell'email possono essere talvolta complessi per gli utenti. Con Proofpoint Email Encryption non dovranno più crittografare manualmente i messaggi email che inviano e ricevono poiché la soluzione si occupa di tutto, dietro le quinte. Grazie a noi, puoi proteggere in modo efficace i messaggi email sensibili, consentendo ai tuoi collaboratori, partner commerciali e utenti finali di continuare ad accedervi senza alcun problema sui loro computer e dispositivi mobili.

Data Discover

Proofpoint Data Discover rileva, monitora e protegge i dati sensibili in file condivisi, archivi dati e siti SharePoint automatizzando l'analisi dei contenuti per tracciare le informazioni sulla rete on premise della tua azienda. Quindi, identifica automaticamente i dati sensibili - informazioni d'identificazione personale e informazioni sanitarie protette - a rischio di divulgazione non autorizzata. Inoltre, consente di applicare misure correttive in tempo reale tramite quarantena, blocco o cancellazione.

Meta

Proofpoint Meta è la soluzione di nuova generazione per l'accesso sicuro alle applicazioni aziendali. Meta è una soluzione incentrata sulle persone che assicura che dipendenti, collaboratori esterni e partner dispongano di un accesso Zero Trust e basato sull'identità alle risorse aziendali, sia che si trovino in un datacenter che nel cloud.

ObserveIT Insider Threat Management

Proofpoint ha acquisito ObserveIT nel novembre 2019. Insider Threat Management è una soluzione non intrusiva per la protezione degli endpoint che aiuta le aziende a identificare e ridurre i rischi associati alle minacce interne. Grazie alle funzioni di rilevamento e prevenzione, protegge i dati da comportamenti negligenti o dolosi da parte di dipendenti, utenti con privilegi e terze parti.

Con Insider Threat Management, le aziende sono in grado di ridurre in modo significativo il rischio di incidenti di sicurezza monitorando il comportamento degli utenti, offrendo formazione in tempo reale e scoraggiando comportamenti impropri. ObservelT riduce il tempo di indagine da giorni a pochi minuti e permette di ricostruire gli incidenti di sicurezza per migliorare i tempi di risposta e semplificare la conformità.

PROTEZIONE DAI RISCHI DIGITALI

Proteggi il tuo marchio e i tuoi clienti dalle minacce associate a social media, domini web e dark web

Digital Risk Protection

Proofpoint Digital Risk Protection protegge il cliente e il suo marchio dai rischi per la sicurezza digitale provenienti da domini web, social media e deep web. Protegge i domini aziendali dalle frodi a danno del marchio, controlla e protegge gli account social media per bloccare tentativi di phishing, spam e appropriazione degli account. Monitora anche l'attività sul deep e dark web per identificare le minacce contro i dirigenti aziendali, la perdita di credenziali d'accesso, le posizioni degli attacchi fisici e gli eventi nelle vicinanze ad impatto elevato. Grazie all'utilizzo del machine learning, puoi giocare d'anticipo rispetto alle minacce, che siano esse solo progettate, imminenti oppure già in corso.

ARCHIVIAZIONE E CONFORMITÀ

Garantisci la conformità della tua azienda grazie alle funzioni di conservazione, ricerca e supervisione dei dati su tutte le piattaforme di comunicazione.

Enterprise Archive

Proofpoint Enterprise Archive utilizza informazioni provenienti dal cloud e machine learning per rilevare e salvaguardare in modo semplice le informazioni strategiche per l'azienda. Questa soluzione risponde a tre sfide fondamentali: reperimento a fini legali, conformità normativa e riduzione di costi e complessità, senza le preoccupazioni di un team IT che gestisce l'archiviazione internamente. La nostra architettura cloud scalabile, prestazioni di ricerca garantite, soddisfazione della clientela senza confronti e la crittografia più sofisticata del settore ti offrono un completo controllo a livello legale e di conformità.

Enterprise Collaboration Archive

Proofpoint Enterprise Collaboration Archive applica controlli basati sulle policy per acquisire i contenuti social provenienti da piattaforme come Salesforce Chatter, Jive, Skype Enterprise, LinkedIn, Twitter e altre ancora in modo che vengano gestiti ed esaminati come qualsiasi altra risorsa di dati critica all'interno della tua piattaforma di archiviazione o di supervisione. In questo modo la conformità con gli obblighi normativi è assicurata. Inoltre, offre funzioni avanzate che automatizzano e razionalizzano le attività cruciali per la conformità.

Intelligent Supervision

Proofpoint Intelligent Supervision aiuta le società di servizi finanziari a ottimizzare la conformità con alcune delle più complesse e severe normative al mondo che si trovano a dover gestire, come quelle di FINRA, SEC e IIROC. La soluzione si integra perfettamente con Enterprise Archive e sfrutta il machine learning per facilitare l'acquisizione e ottimizzare la disamina ed i report a fini normativi. Puoi così godere di visibilità completa su email, messaggistica immediata, strumenti di collaborazione, SMS, messaggi vocali e social media.

E-Discovery Analytics

Proofpoint E-Discovery Analytics offre agli uffici legali un flusso di lavoro intuitivo per le indagini elettroniche (e-discovery). La soluzione utilizza il machine learning unitamente a risultati di ricerca in tempo reale e all'analisi integrata dei casi per offrirti informazioni più dettagliate e complete. Ti consente di prepararti proattivamente ad eventuali controversie legali, assicurandoti maggior controllo e meno rischi.

Social Media Compliance

Proofpoint aiuta ad allineare la conformità dei social network con le pratiche di marketing per aiutare gli utenti a rispettare le attuali normative sui social media. Proofpoint Digital Risk Protection si integra con le principali soluzioni di archiviazione per raccogliere e classificare i contenuti delle piattaforme social in modo intelligente per ulteriori ricerche e indagini elettroniche future. In questo modo risparmi tempo prezioso e denaro in caso di accertamenti.

APPROFONDISCI

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

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity, 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**.