Proofpoint Email Protection

Rilevamento e blocco delle minacce email dannose e senza malware

VANTAGGI PRINCIPALI

- Blocco degli attacchi BEC e di phishing nonché del malware avanzato in ingresso
- Sensibilizzazione alla sicurezza degli utenti tramite la visualizzazione di avvisi relativi alle email
- Aumento della produttività grazie a un rapido tracciamento delle email e all'applicazione di best practice
- Flessibilità totale per garantire la scalabilità necessaria alle grandi aziende
- Maggiore efficienza operativa tramite l'automazione delle operazioni di sicurezza e della risposta alle minacce
- Protezione estesa grazie all'autenticazione integrata e alla crittografia delle email, alla prevenzione della perdita di dati tramite email, alla soluzione Targeted Attack Protection e altro ancora
- Accordi di livello di servizio (SLA) di prim'ordine per l'implementazione nel cloud:
  - Percentuale di disponibilità di servizio: 99,999%
  - Efficacia della protezione contro i virus: 100%
  - Tempi di latenza delle email: inferiore a 1 minuto
  - Percentuale di blocco o di reindirizzamento dello spam: 99%

Proofpoint Email Protection aiuta a proteggere e controllare le email in entrata e in uscita. Sfrutta il machine learning e le tecniche di rilevamento multilivello per identificare e bloccare le email dannose. Inoltre, classifica in modo dinamico le minacce attuali e altri problemi comuni e fornisce un controllo granulare su numerosi tipi di email, tra cui email fraudolente, phishing, malware, spam, email inviate in blocco e altro ancora. Offre anche flessibilità completa con policy di sicurezza personalizzate e regole per il routing dei messaggi. Si tratta della soluzione di email security più adottata dalle aziende Fortune 1000 ed è in grado di adattarsi anche alle aziende di più grandi dimensioni. Non ultimo può essere installata in ambienti cloud, ibridi e on-premise.

L'email è il principale vettore delle minacce. Infatti, il 96% delle minacce sospette che sfruttano il social engineering è veicolato tramite l'email[1]. Oltre alle minacce comuni distribuite via email come gli attacchi di phishing e il malware, la violazione delle email aziendali (BEC, Business Email Compromise) rappresenta un nuovo pericolo per le aziende. Proofpoint Email Protection rileva sia le minacce note che quelle sconosciute, che altre soluzioni non sono in grado di rilevare. Elaborando miliardi di messaggi ogni giorno, Proofpoint è in grado di identificare un maggior numero di minacce, rilevarle più rapidamente e offrire una miglior protezione contro le minacce senza malware più difficili da individuare, come le email fraudolente. Con Proofpoint Email Protection puoi bloccare la maggior parte delle minacce prima che raggiungano la casella email degli utenti.

Intercettazione delle minacce emergenti che altre soluzioni non rilevano

Rilevamento delle email fraudolente, dei truffatori e del phishing

Proofpoint Email Protection rileva le minacce emergenti prima che raggiungano le caselle email dei tuoi utenti. Alimentato da NexusAI, Proofpoint Advanced BEC Defence è progettato per bloccare in modo efficace un'ampia gamma di frodi via email, tra cui il reindirizzamento dei pagamenti e le frodi delle fatture dei fornitori da account compromessi. Poiché queste sono spesso prive di payload dannosi, richiedono una tecnica di rilevamento più sofisticata.

1 Data Breach Investigations Report (Report Investigativo sulle Violazioni dei Dati), Verizon, 2020.

Proofpoint Advanced BEC Defense è il nostro motore di rilevamento basato sul machine learning e l'intelligenza artificiale. È progettato specificamente per individuare e bloccare gli attacchi BEC. Rileva in modo dinamico gli attacchi BEC analizzando diversi attributi dei messaggi, come per esempio:

- Dati dell'intestazione del messaggio
- Indirizzo IP del mittente (indirizzo IP d'origine, reputazione)
- Corpo del messaggio (parole o espressioni che trasmettono un senso di urgenza)

Stabilisce se il messaggio rappresenta una minaccia BEC. Inoltre, rileva diverse tattiche BEC utilizzate dai criminali informatici come ad esempio:

- Dirottamento degli indirizzi di risposta
- Utilizzo di indirizzi IP dannosi
- Utilizzo di domini di fornitori la cui identità è stata usurpata

Proofpoint Advanced BEC Defense offre inoltre visibilità granulare sui dettagli di un attacco BEC, (tema, truffe delle carte regalo, dirottamento dei libri paga, fatturazione, esca, compito, ecc.). Spiega perché il messaggio è sospetto, con esempio per illustrarlo. Questo permette al tuo team della sicurezza di comprendere meglio l'attacco e comunicarlo. I dati raccolti da NexusAI vengono poi inseriti nel grafico delle minacce Nexus di Proofpoint. Quest'ultimo analizza e correla le informazioni sulle minacce a livello di email, cloud, rete e social media di tutti i nostri clienti offrendoti la protezione necessaria per stare un passo avanti le minacce.

Blocco delle email dannose e indesiderate

Abbiamo integrato tecniche di rilevamento multi-livello all'interno di Proofpoint Email Protection per proteggerti dalle minacce in costante evoluzione. Il rilevamento basato su firme blocca le minacce note come virus, trojan horse e ransomware, mentre l'analisi dinamica della reputazione valuta costantemente gli indirizzi IP locali e globali per stabilire se accettare o negare le connessioni utilizzate dall'email. Il nostro esclusivo sistema di classificazione, classifica dinamicamente anche più tipi di email, tra cui le email fraudolente, il phishing, il malware, lo spam, la bulk mail, i contenuti per adulti e valuta il circle of trust. Inoltre, mette in quarantena le email in entrata per tipo. Insieme, queste funzioni ti proteggono fin dai primi segnali di un'attività dannosa.

Tracciamento di qualsiasi email in pochi secondi

Proofpoint Email Protection dispone di una funzione di ricerca estremamente potente. Grazie a dozzine di criteri, questa funzione di ricerca intelligente ti permette di individuare rapidamente i log, generalmente difficili da trovare. Puoi anche tracciare le email, compresa la loro origine e la loro destinazione, in pochissimo tempo. Proofpoint Email Protection fornisce dettagli granulari sui risultati di ricerca, compresi i metadati che includono più di un centinaio di attributi. La ricerca viene completata in pochi secondi. Puoi scaricare ed esportare i risultati della ricerca (fino a un milione di record). Inoltre, sono integrati nel prodotto diversi report real-time, offrendoti una visibilità dettagliata sul flusso e sulle tendenze dell'email. Grazie a questi dati puoi affrontare i problemi man mano che si presentano.

Flessibilità totale per garantire la scalabilità delle grandi aziende

Proofpoint Email Protection soddisfa le esigenze delle più grandi aziende nel mondo. Permette di definire regole firewall per l'email altamente personalizzabili a livello globale, di gruppo o di utente. Consente di creare policy di sicurezza e regole di instradamento dell'email che soddisfino le tue esigenze e applicarle facilmente. Proofpoint Email Protection offre gli stessi vantaggi e una maggiore flessibilità con diverse opzioni di deployment (Hardware on-prem, virtuale e SaaS).

Sensibilizzazione degli utenti alla sicurezza

La visualizzazione degli avvisi sulle email permette ai tuoi utenti di prendere delle decisioni più consapevoli sui messaggi sospetti, ignorando se sono legittimi o dannosi. Mostra una breve descrizione dei rischi associati a un'email specifica e indica il livello di rischio mediante la codifica a colori, di facile interpretazione da parte degli utenti che possono segnalare le email sospette direttamente a partire dall'avviso, anche quando accedono all'email tramite dispositivi mobili. Questa funzione aiuta a controllare meglio il rischio di potenziali violazioni rendendo gli utenti più cauti nei confronti di email sospette.

Grazie a Proofpoint Email Protection, gli amministratori dell'email possono anche consentire agli utenti di gestire i messaggi crittografati e non prioritari come i messaggi inviati in blocco, rivedere i messaggi in quarantena e adottare le misure appropriate direttamente nel pannello delle attività di Outlook. I commenti degli utenti vengono poi inoltrati a Proofpoint, contribuendo a migliorare l'accuratezza complessiva della classificazione dei messaggi inviati in blocco.

Gestione centralizzata per Proofpoint Email Encryption e Proofpoint Email DLP

Puoi estendere facilmente la tua protezione aggiungendo le soluzioni Proofpoint Targeted Attack Protection, Proofpoint Email Fraud Defense, Proofpoint Email Encryption o Proofpoint Email Data Loss Prevention (DLP). Anche se Proofpoint Email Protection fornisce funzioni di base per la crittografia dell'email e per DLP, puoi ottenere soluzioni più avanzate tramite la stessa console di gestione. Questa integrazione spinta ti aiuta a gestire i dati sensibili inviati attraverso l'email. Previene inoltre la fuga o la perdita dei dati via email. Infine, soddisfa diversi requisiti di conformità.

PER SAPERNE DI PIÙ

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

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) 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.