

# Proofpoint Threat Response Auto-Pull

## Quarantena automatica delle mail dannose dopo la loro consegna

### VANTAGGI PRINCIPALI

- Quarantena automatica delle email dannose che aggirano le difese perimetrali
- Riduzione in modo esponenziale del tempo che i team di sicurezza e di messaggistica dedicano all'orchestrazione della sicurezza dell'email e alla risposta agli incidenti
- Classificazione delle minacce con il sistema di intelligence sulle minacce di Proofpoint
- Monitoraggio automatico della casella di posta degli abusi per le minacce
- Quarantena dei messaggi inoltrati a singoli o liste di distribuzione
- Monitoraggio delle campagne di phishing segnalate parzialmente ed eliminazione del tempo dedicato ai messaggi segnalati in modo errato

Oltre il 90% delle violazioni inizia con un'email, il principale vettore d'attacco. Con la costante evoluzione delle minacce diffuse via email, le aziende sono esposte a un numero sempre maggiore di messaggi dannosi. Le email dannose possono contenere link di phishing il cui carico dannoso si attiva solo dopo la consegna o utilizzare delle tecniche di elusione che producono falsi negativi che vengono consegnati agli utenti. I team dedicati alla sicurezza dell'email hanno spesso il compito di analizzare ed eliminare i messaggi dannosi per ridurre l'esposizione alle minacce e limitare i danni potenziali. Se mettere in quarantena un singolo messaggio è un processo relativamente semplice che richiede solo 10-15 minuti, quando si tratta di decine di messaggi, il compito può diventare rapidamente noioso e dispendioso in termini di tempo.

### Quarantena automatica delle email dannose

Proofpoint Threat Response Auto-Pull (TRAP) permette agli amministratori del sistema email e della sicurezza di ottimizzare il processo di risposta agli incidenti. Quando viene rilevata un'email pericolosa, TRAP analizza le email e rimuove automaticamente i messaggi dannosi. Inoltre, mette in quarantena la posta indesiderata che ha raggiunto le caselle di posta in arrivo degli utenti. TRAP è una soluzione potente che permette di ridurre in modo esponenziale il tempo che i team dedicati all'email e alla sicurezza dedicano a ripulire l'email dai messaggi dannosi e indesiderati.

### Un potente sistema di intelligence sulle minacce

Il sistema di intelligence sulle minacce di Proofpoint copre numerosi vettori di minacce: email, social media, dispositivi mobile, cloud e rete. Questo ci offre una visibilità unica sulle minacce più recenti e sulle tattiche utilizzate dai criminali informatici. TRAP permette di sfruttare il sistema di informazioni sulle minacce di Proofpoint e quelli di terze parti come i flussi STIX/TAXII, WHOIS, VirusTotal, Soltra e MaxMind. In questo modo è possibile identificare le persone, i dati e i sistemi colpiti dagli attacchi, ordinare e assegnare priorità agli allarmi in modo rapido e liberarsi da compiti ripetitivi.

Una volta rilevata un'email, viene arricchita con le informazioni provenienti dalle fonti sopra menzionate. TRAP abbina i destinatari e le identità degli utenti, identifica le campagne associate e analizza gli indirizzi IP e i domini dell'attacco. Puoi così godere del vantaggio di una classificazione estremamente precisa dei messaggi. Inoltre, i tuoi team della sicurezza possono dedicarsi ad altri compiti e non devono più analizzare manualmente ogni messaggio rilevato.

### Identificazione e riduzione del rischio di phishing con CLEAR

Un dipendente informato può rappresentare la tua ultima linea di difesa contro un attacco informatico. Con Closed-Loop Email Analysis and Response (CLEAR), il processo di segnalazione, analisi e neutralizzazione delle email potenzialmente dannose si riduce da giorni a minuti. Alimentato dal sistema di informazioni sulle minacce di Proofpoint, CLEAR blocca gli attacchi attivi con un solo clic. Il tuo team di sicurezza può risparmiare così tempo ed energia mettendo automaticamente in quarantena i messaggi dannosi.

CLEAR è una soluzione completa che combina le funzionalità di PhishAlarm, il tasto di segnalazione delle email, PhishAlarm Analyzer, la soluzione di categorizzazione e assegnazione delle priorità basata sul sistema di informazioni sulle minacce di Proofpoint, e TRAP, che arricchisce i messaggi e automatizza la messa in quarantena dei messaggi dannosi.

I messaggi segnalati vengono inviati a una casella email di segnalazione degli abusi per essere analizzati da CLEAR e vengono monitorati ed elaborati allo stesso modo da TRAP. Vengono poi analizzati utilizzando il sistema di informazioni sulle minacce di Proofpoint e altre fonti di terze parti per stabilire se uno qualsiasi dei contenuti include dei marcatori dannosi. I messaggi vengono automaticamente rimossi dalla casella di posta in arrivo del destinatario.

### Gestione delle email al di fuori dei canali regolari

TRAP supporta anche i file CSV e Proofpoint SmartSearch. Gli utenti possono caricare i risultati di SmartSearch o i file CSV oppure inserire manualmente gli incidenti con le informazioni fondamentali per avviare un'azione di quarantena per una singola email o migliaia di messaggi. In pochi istanti le email che violano le policy o che rappresentano una minaccia per la sicurezza possono essere rimosse dalle caselle email. Una lista di attività indica chi ha letto le email, così come il successo o il fallimento del tentativo di richiamo del messaggio.

### Quarantena automatica dei messaggi inoltrati

Le email dannose e indesiderate possono essere inoltrate ad altre persone, dipartimenti o liste di distribuzione. Molti amministratori hanno difficoltà a eliminare questi messaggi dopo la consegna. TRAP risolve il problema grazie a una logica di business integrata e a un sistema di intelligence che rileva quando i messaggi vengono inoltrati o inviati alle liste di distribuzione, e poi rintraccia automaticamente i destinatari per ritrovare e cancellare questi messaggi. In questo modo, risparmi tempo ed eviti ogni frustrazione.

## APPROFONDISCI

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