

# Proofpoint Security Awareness Enterprise

## Rafforzare la resilienza degli utenti adottando un approccio basato sulle minacce

### Vantaggi principali

- Riduci del 40 % il numero di clic su email dannose in meno di sei mesi.
- Mostra al tuo CISO i parametri di riduzione dei rischi.
- Stimola dei cambiamenti di comportamento grazie a un'esperienza di apprendimento personalizzata.
- Analizza automaticamente le minacce segnalate dagli utenti senza aumentare il carico di lavoro dell'IT.

Proofpoint Security Awareness Enterprise ti aiuta ad affrontare una delle sfide più pressanti cui si trovano di fronte tutte le aziende: ridurre il rischio di sicurezza posto dai collaboratori. Secondo il report Proofpoint State of the Phish 2023, il nostro studio annuale sul phishing, il 98% di tutte le aziende dispone di una qualche forma di formazione di sensibilizzazione alla sicurezza informatica. Ciò indica un diffuso riconoscimento della sua importanza, ma la formazione da sola non sempre permette di ottenere i risultati desiderati.

Affinché un programma di sicurezza abbia la massima efficacia, gli utenti devono essere attivamente coinvolti nel processo di apprendimento e devono essere in grado di fare scelte corrette in situazioni di vita reale. Inoltre, i loro comportamenti devono avere un impatto misurabile sulla sicurezza.

È qui che entra in gioco Proofpoint Security Awareness Enterprise. Il framework ACE, il nostro approccio globale per la sensibilizzazione alla sicurezza informatica, permette di risolvere questa problematica. Questo quadro formativo si basa su tre fasi fondamentali: valutare la vulnerabilità dell'utente, modificarne il comportamento e misurare l'efficacia del programma. La nostra soluzione migliora l'efficienza operativa e consente agli amministratori della sicurezza di scalare il programma a livello globale.



Figura 1. Framework ACE.

## Sfrutta una threat intelligence all'avanguardia

Proofpoint Security Awareness Enterprise è ottimizzato dalla nostra threat intelligence avanzata, acquisita dalla nostra vasta clientela. La utilizziamo per aiutarti a creare un programma di formazione efficace, che ti aiuta a condurre campagne di simulazione di attacchi di phishing sofisticati che imitano gli attacchi reali. Puoi identificare i tuoi VAP (Very Attacked People™ ovvero le persone più attaccate) e istruirli sulle minacce da cui vengono presi di mira, osservare il comportamento degli utenti di fronte alle minacce reali ed evidenziare le tendenze degli attacchi nelle newsletter inviate ai collaboratori.

## Valuta le vulnerabilità degli utenti

Proofpoint Security Awareness Enterprise ti aiuta a valutare le conoscenze, le competenze e le convinzioni dei tuoi utenti in materia di sicurezza informatica. Inoltre, indica il loro livello di attrattiva come bersagli. Tutte queste informazioni ti permettono di identificare gli utenti altamente vulnerabili e di determinare la loro capacità di adottare comportamenti corretti. Puoi così comprendere quali sono i collaboratori che necessitano di maggior formazione e creare un programma su misura in base alle loro lacune e al loro comportamento previsto.

Grazie a Proofpoint Security Awareness Enterprise puoi:

- Identificare le lacune con test rapidi e mirati basati sulla nostra threat intelligence avanzata
- Eseguire test di phishing che incorporano le minacce osservate in circolazione
- Analizzare la vulnerabilità dei collaboratori in base alla loro partecipazione, rendimento e probabilità di essere attaccati
- Identificare le convinzioni in materia di sicurezza per determinare come incoraggiare i collaboratori ad adottare comportamenti corretti

- Identificare i VAP e i collaboratori che si lasciano più ingannare quando la soluzione è integrata con la piattaforma Proofpoint

## Determina il livello di conoscenza dei tuoi utenti

Le nostre valutazioni adattive ti aiutano a determinare il livello delle conoscenze dei tuoi utenti e i problemi che si trovano ad affrontare. Le valutazioni sono moduli di formazione specifici, concisi e precisi. Puoi scegliere fra una larga selezione di test che rispondono a specifici obiettivi di apprendimento e tra moduli di microapprendimento con vari livelli di difficoltà.

## Anticipa il comportamento dei tuoi utenti

Le nostre simulazioni del phishing aiutano a garantire che i tuoi utenti siano preparati ad affrontare le minacce reali. Proofpoint utilizza la threat intelligence proveniente dagli oltre 2,6 miliardi di email che analizziamo ogni giorno. Questa visibilità ci consente di offrirti migliaia di modelli di phishing che simulano più tipi di minacce. Puoi anche personalizzare i tuoi modelli in base ai tipi di minacce nel tuo ambiente e iscrivere automaticamente alla formazione gli utenti che si lasciano ingannare da una simulazione di attacchi di phishing.

## Scopri le convinzioni dei tuoi utenti

Per creare una solida cultura della sicurezza informatica devi conoscere le convinzioni dei tuoi utenti in materia di sicurezza informatica. Le nostre valutazioni della cultura ti aiutano a determinare lo stato attuale della tua cultura della sicurezza informatica. Utilizzano brevi questionari che consentono di analizzare e misurare i tre principali fattori che contribuiscono a tale cultura: responsabilità, importanza e autonomia. Puoi quindi personalizzare il programma per modificare le convinzioni delle persone e incoraggiarle a mettere in pratica quanto appreso.

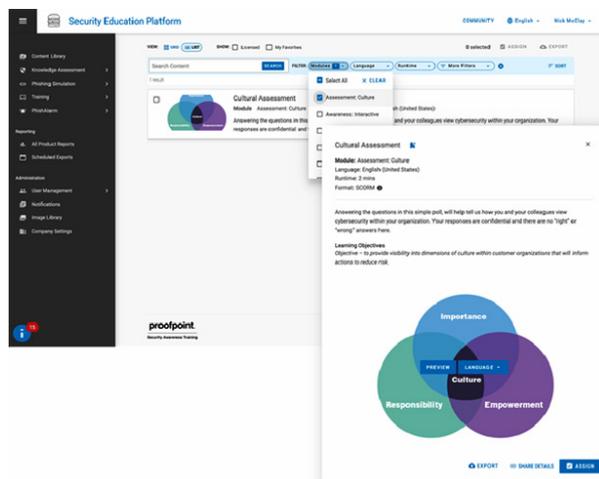


Figura 2. Valutazioni della cultura e filtraggio e libreria dei contenuti migliorati.

## Identifica gli utenti più a rischio

Se integrata con la piattaforma Proofpoint Threat Protection, la nostra soluzione ti aiuta a identificare i VAP e i collaboratori che si lasciano più ingannare. Grazie a queste informazioni puoi offrire una formazione mirata agli utenti più attaccati in base alle minacce da cui vengono colpiti. L'integrazione con Nexus People Risk Explorer ti offre una visione ancora più approfondita degli utenti più a rischio. Valuta la loro vulnerabilità, l'indice d'attacco (Attack Index) e i privilegi aziendali. In tal modo puoi concentrare il tuo programma e le tue risorse sui rischi reali per la tua azienda.

Per saperne di più sulla formazione mirata di Proofpoint Security Awareness, consulta il documento **Come Proofpoint Security Awareness stimola il coinvolgimento degli utenti gli utenti.**

## Modifica il comportamento degli utenti

Una volta stabilita una linea di base relativa a conoscenze, comportamenti e convinzioni dei tuoi utenti, puoi iniziare a modificare i loro comportamenti non sicuri. Proofpoint Security Awareness Enterprise ti aiuta a stimolare un cambiamento di comportamento grazie alla formazione e ad attività di rinforzo su misura. Puoi così offrire a ogni persona le conoscenze di cui ha bisogno e proporre contenuti rilevanti per la sua situazione. Questo ti aiuta a massimizzare il tempo limitato a disposizione per la formazione degli utenti e ad aumentare l'impatto di tale formazione.

Grazie a Proofpoint Security Awareness Enterprise puoi:

- Motivare gli utenti offrendo un'esperienza di apprendimento personalizzata
- Creare una formazione concisa e specifica per ogni obiettivo di apprendimento
- Proporre contenuti coinvolgenti che riflettono l'attuale panorama delle minacce
- Rafforzare l'efficacia dell'apprendimento con una formazione pertinente proposta al momento opportuno

## Utilizza un framework adattivo e moduli di microapprendimento

Proofpoint Security Awareness Enterprise utilizza un framework di apprendimento adattivo, che è agli antipodi di un approccio universale. Il framework fornisce una formazione alla sicurezza su una scala progressiva a quattro livelli, dai principi di base ai concetti avanzati. Ciò significa che i tuoi utenti possono seguire la formazione di cui hanno bisogno con il livello di difficoltà appropriato.

Il framework adattivo è inoltre accompagnato da moduli di microapprendimento della durata di tre minuti che rispondono a obiettivi di apprendimento specifici. I tuoi utenti ricevono una formazione continua e facile da assimilare. Inoltre, la formazione è personalizzata in base a fattori individuali, come il ruolo, lo stile di apprendimento, le competenze, il livello di vulnerabilità e la lingua del collaboratore.

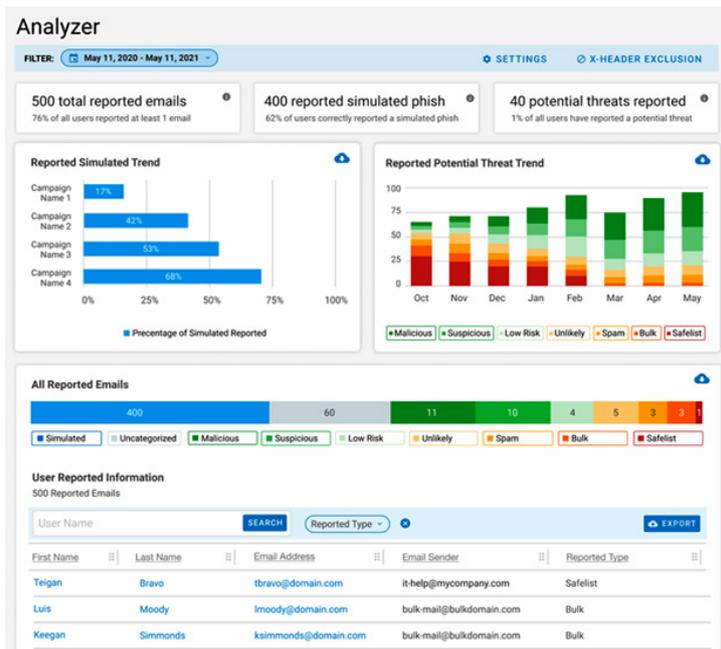


Figura 3. Analisi in tempo reale dei comportamenti in risposta a simulazioni di attacchi di phishing e alle minacce reali.

### Offri contenuti basati sulle minacce e formazione al momento opportuno

Le tendenze e le tattiche dell'attuale panorama delle minacce orientano i contenuti di Proofpoint Security Awareness Enterprise. Ciò ti consente di preparare meglio i tuoi utenti ad affrontare le minacce reali in circolazione. I nostri avvisi settimanali sulle minacce descrivono gli ultimi attacchi osservati fra la nostra clientela, mentre i nostri avvisi Attack Spotlight migliorano il tuo programma con una formazione tempestiva.

Quando Proofpoint Security Awareness Enterprise è integrato con la piattaforma Proofpoint, puoi fornire ai tuoi utenti suggerimenti contestuali e rafforzare i comportamenti positivi. I messaggi formativi spiegano agli utenti perché non devono fare clic su un collegamento durante la simulazione di un attacco di phishing. Gli avvisi interni all'applicazione in caso di email sospette segnalano agli utenti i messaggi potenzialmente dannosi. Infine, il pulsante "Report Suspicious" (Segnala come sospetto) attiva il nostro flusso di lavoro automatizzato Proofpoint Closed-Loop Email Analysis and Response (CLEAR), che fornisce agli utenti un riscontro personalizzato sull'email segnalata.

### Valuta l'impatto del programma

Valutare l'impatto del programma di sensibilizzazione sulla tua sicurezza è fondamentale. Proofpoint Security Awareness Enterprise fornisce dei parametri comportamentali che evidenziano le prestazioni dei tuoi

collaboratori e del programma, così puoi dimostrare chiaramente l'impatto del programma sulla sicurezza. Ad esempio, i nostri clienti hanno registrato una diminuzione del 40% del numero di clic sulle minacce reali in soli sei mesi. Inoltre, hanno osservato che il numero di email segnalate dagli utenti è triplicato. Puoi presentare i parametri di riduzione del rischio al tuo CISO per dimostrare l'efficacia del programma e ottenere la sua approvazione per investire ulteriormente nel programma e nel suo sviluppo.

Grazie a Proofpoint Security Awareness Enterprise puoi:

- Monitorare il comportamento degli utenti in relazione alla segnalazione delle minacce reali
- Confrontare i parametri chiave con quelli di altre aziende nel settore
- Dimostrare un cambiamento positivo dei comportamenti degli utenti per ottenere il supporto della dirigenza.

### Monitora i comportamenti in risposta a simulazioni e a email realmente dannose

La nostra dashboard del CISO mostra l'impatto della formazione sul comportamento dei tuoi collaboratori. Monitora le segnalazioni delle email realmente dannose da parte degli utenti e ne mostra l'evoluzione nel tempo. In questo modo puoi capire come è migliorato il loro comportamento. Parametri come il tasso di segnalazione delle email sospette e l'accuratezza di tali segnalazioni ti aiutano a misurare le prestazioni degli utenti al di là dei tassi di completamento della formazione.

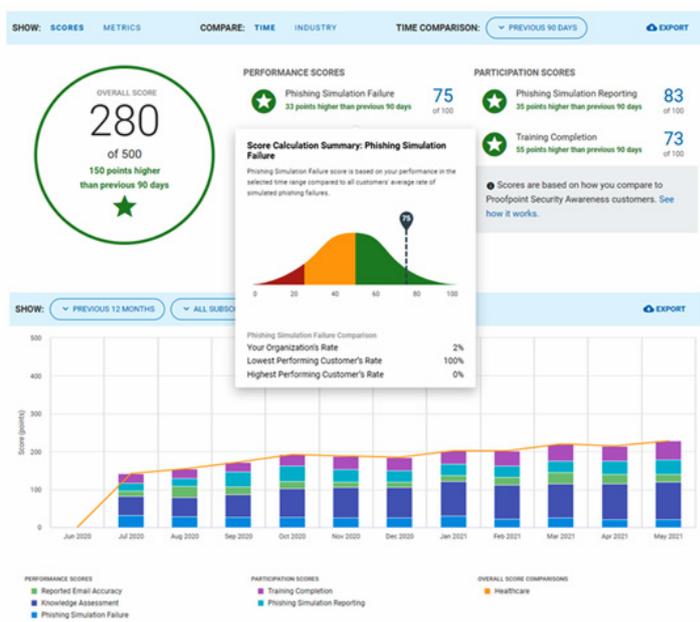


Figura 4. Monitoraggio delle prestazioni del programma nel riepilogo dei punteggi integrato nella dashboard del CISO.

### Confronta i tuoi risultati con quelli di altre aziende del tuo settore

La dashboard del CISO confronta anche le prestazioni del tuo programma rispetto a quelle di altre aziende del tuo settore. Ti consente di vedere i cambiamenti nel comportamento dei tuoi utenti come, ad esempio, la percentuale di coloro che segnalano le email sospette. Poi puoi confrontarne il loro tasso di accuratezza con quelli riportati da altre aziende, permettendo di valutare l'impatto del tuo programma rispetto a tuoi omologhi e evidenziarne l'efficacia.

### Identifica i comportamenti ripetuti

Proofpoint Security Awareness Enterprise fornisce dati giornalieri dei test interni e delle minacce esterne. Ad esempio, puoi monitorare e identificare i comportamenti che si ripetono. La nostra soluzione ti consente di filtrare e raggruppare gli utenti che hanno fallito una simulazione di attacco di phishing più volte entro un intervallo di tempo definito. In questo modo, gli amministratori possono prendere provvedimenti adeguati, per esempio proponendo formazione supplementare.

### Amplia e sviluppa il tuo programma

Proofpoint Security Awareness Enterprise ti permette di sfruttare la potenza dell'automazione e della scalabilità. I processi automatizzati riducono il lavoro manuale e aumentano la flessibilità e l'efficienza delle tue operazioni.

La nostra soluzione ti consente inoltre di scalare il tuo programma a livello mondiale.

Grazie a Proofpoint Security Awareness Enterprise puoi:

- Migliorare l'esperienza dell'amministratore grazie a processi flessibili e automatizzati
- Rivolgerti al tuo pubblico internazionale nella lingua preferita dagli utenti
- Promuovere il tuo programma di sensibilizzazione alla sicurezza informatica in un'ampia gamma di lingue
- Adottare le best practice e ottenere assistenza costante grazie ai servizi gestiti di Proofpoint
- Semplificare la segnalazione delle email sospette da parte degli utenti e fornire loro un riscontro positivo
- Analizzare e neutralizzare automaticamente le email segnalate dagli utenti grazie all'integrazione con la piattaforma Proofpoint.

### Supporta più lingue

Puoi coinvolgere il tuo pubblico internazionale nella lingua preferita dagli utenti. Proofpoint Security Awareness Enterprise supporta oltre 40 lingue per i nostri moduli di formazione e servizi di personalizzazione, compresi sottotitoli e voci fuori campo. Inoltre, aggiungiamo continuamente nuove lingue.

## Godi di un'implementazione flessibile grazie all'amministrazione multitenant

Con l'amministrazione multitenant la configurazione è più semplice e può essere implementata in modo flessibile e adattata al tuo caso d'uso specifico. Il team della sicurezza della tua azienda supervisiona il programma nel suo insieme e può prendere decisioni a livello di gruppo. I singoli gruppi (ad esempio una filiale o una divisione regionale), possono adattare la formazione ai loro utenti e a requisiti specifici. Questo flusso di lavoro è ideale per le grandi aziende complesse con una presenza globale o distribuita.

## Migliora la produttività grazie ai servizi gestiti

Proofpoint ti aiuta a rafforzare il tuo team della sicurezza e ad adottare le best practice. Grazie ai **servizi gestiti** ci facciamo carico delle attività quotidiane associate all'esecuzione e alla valutazione del tuo programma di sensibilizzazione alla sicurezza informatica. Il tuo team della sicurezza può così concentrarsi sulle sue attività principali. Con i **servizi di personalizzazione di Proofpoint Security Awareness** puoi presentare un programma specifico della tua azienda e rafforzare la cultura della sicurezza personalizzando i moduli di microapprendimento (logo aziendale, colori, immagini, testo, voce fuori campo, traduzione, ecc.).

## Automatizza le segnalazioni degli utenti e la risposta alle minacce

Quando un utente segnala un'email sospetta nel proprio client email, la tecnologia di rilevamento delle minacce di Proofpoint analizza automaticamente l'email. Ciò riduce la tua esposizione alle minacce di phishing che potrebbero eludere le tue difese, riduce le attività manuali e migliora l'efficienza operativa. Se la nostra tecnologia di rilevamento delle minacce identifica un'email sospetta come minaccia e la soluzione è integrata con la piattaforma Proofpoint, viene attivato il nostro flusso di lavoro automatizzato CLEAR. Neutralizza l'email e invia un riscontro all'utente che l'ha segnalata. Questo processo rafforza i comportamenti positivi e riduce del 90% il carico di lavoro di correzione per gli amministratori.

## PER SAPERNE DI PIÙ

Per maggiori informazioni visita [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 il 75% 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](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.