proofpoint.

GUIDA ALL'ACQUISTO

Come scegliere la miglior soluzione di sicurezza dell'email per la tua azienda

Principali funzionalità

Ecco le principali funzionalità da prendere in considerazione quando si cerca una soluzione di sicurezza dell'email moderna:

1. Protezione contro la più ampia gamma di minacce
2. Rilevamento e neutralizzazione automatizzati delle minacce
3. Opzioni di implementazione flessibili
4. Esperienza utente eccellente
5. Protezione contro le minacce oltre le email

Panoramica

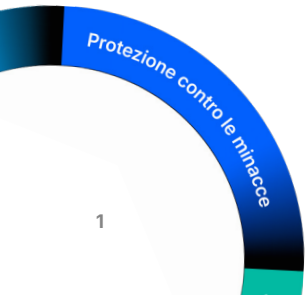
L'email rimane uno dei principali vettori degli attacchi informatici. Tuttavia, negli anni recenti, la superficie d'attacco si è ampliata oltre l'email e gli utenti utilizzano oggi diversi canali digitali per comunicare e collaborare. Non sorprende perciò che i criminali informatici si adattino e traggano profitto da questa tendenza. Di fatto, distribuiscono con grande successo un'ampia gamma di minacce incentrate sulle persone su tutti i canali digitali.

In risposta, le aziende assemblano un patchwork di diversi prodotti isolati avanzati per contrastare le minacce.

Purtroppo, questo approccio crea lacune nelle loro difese e non tiene conto di molti rischi. Inoltre, la gestione e l'integrazione di strumenti di sicurezza diversi sono complesse e costose. Per evitare queste insidie, le aziende hanno bisogno di una soluzione completa di sicurezza dell'email, in grado di difenderle dalle minacce attuali e emergenti incentrate sulle persone, sotto forma di un'unica piattaforma.

In questa guida, delineiamo le funzionalità chiave indispensabili di una soluzione di sicurezza dell'email completa, nonché i motivi della loro importanza.

Figura 1. Ripartizione dei tipi di minacce distribuite via email



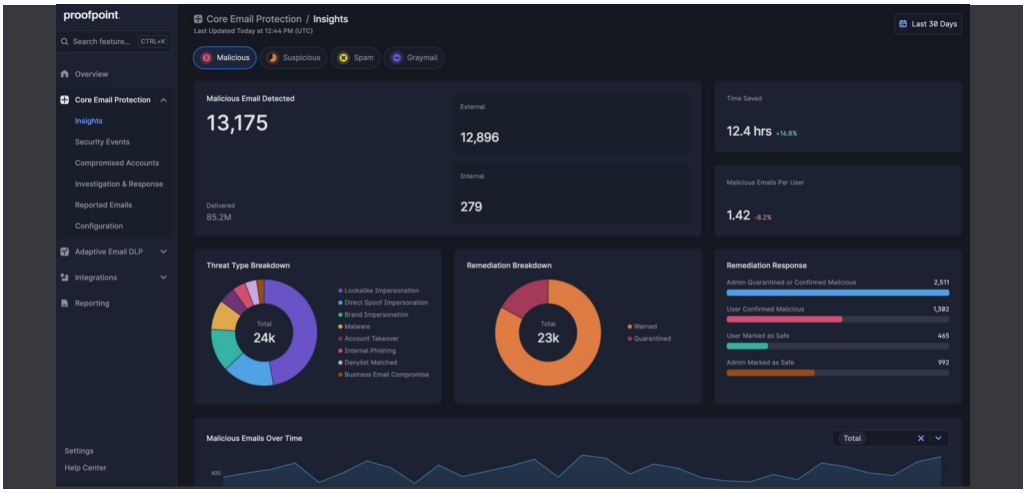


Figura 2. Vista completa delle minacce via email bloccate da Proofpoint Core Email Protection

55 Mld di dollari

Perdite causate dagli attacchi BEC tra il 2013 e il 2023 nel mondo[2]

60 secondi

Tempo medio necessario a un utente per cadere nella trappola di un'email di phishing[3]

1. Protezione contro la più ampia gamma di minacce

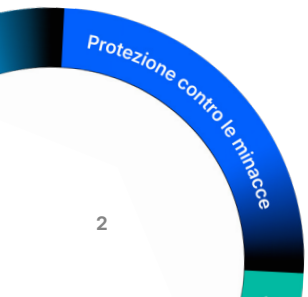
Il costo medio di una violazione di dati causata da un attacco di phishing o di violazione dell'email aziendale (BEC, Business Email Compromise). Ammonta a 4,88 milioni di dollari[1]. Si tratta del secondo costo di violazione più elevato, dopo quello degli attacchi causati da utenti interni malintenzionati. Ma ogni minaccia che sfugge alle protezioni può costare cara in termini di perdite finanziarie e danni all'immagine del marchio.

I team della sicurezza fanno del loro meglio per ridurre il più possibile l'esposizione dell'azienda ai rischi. L'unico modo per raggiungere questo obiettivo è bloccare la più ampia gamma possibile di minacce.

Ecco le caratteristiche essenziali di una soluzione di sicurezza dell'email a tal proposito:

- **Utilizzo di una threat intelligence in tempo reale.** Una threat intelligence costantemente aggiornata facilita l'identificazione delle minacce emergenti. Tuttavia, la threat intelligence non si limita ai dati, deve anche coinvolgere dei team di ricercatori sulle minacce informatiche altamente qualificati. Quando una soluzione dispone di queste due caratteristiche, è in grado di analizzare le tendenze su scala globale più rapidamente e efficacemente. Può per esempio rilevare e seguire dei criminali informatici e attori legati agli stati sofisticati, nonché identificare le evoluzioni del paesaggio delle minacce.
- **Sfruttamento dell'IA per il rilevamento delle minacce.** Per bloccare gli attacchi via email che si basano sulla manipolazione associata a payload dannosi, è essenziale uno stack di rilevamento multilivello ottimizzato dall'IA. I modelli linguistici di grandi dimensioni, i grafici relazionali e comportamentali, il machine learning e la capacità di analisi delle immagini sono tutte funzionalità fondamentali, perché garantiscono il blocco delle minacce su larga scala.
- **Monitoraggio continuo delle minacce.** La capacità di analizzare gli URL e gli allegati in ambiente sandbox è importante. Lo stesso vale per *il momento in cui* effettui questo sandboxing. Per identificare gli attacchi che hanno eluso le difese o le minacce a attivazione ritardata, è necessario adottare una soluzione che rileva e blocca le minacce durante tutto il loro ciclo di vita: prima della consegna, dopo la consegna e al momento del clic.
- **Visibilità sugli utenti presi di mira.** Devi identificare le vittime degli attacchi, i metodi utilizzati e se l'attacco è andato a segno. È inoltre importante sapere in che modo gli utenti vengono colpiti, i dati a cui hanno accesso e se tendono facilmente a farsi trarre in inganno. Con queste informazioni, puoi implementare le misure di protezione adeguate al momento opportuno.

Quanto prima vengono identificate le minacce, più la tua azienda è al sicuro. Inoltre, i tuoi team informatici e della sicurezza non dovranno più dedicare il loro tempo prezioso alla risposta agli incidenti e alla correzione.



1. IBM, *Cost of a Data Breach Report* (Report sul costo delle violazioni dei dati), 2024.
2. FBI, "Business Email Compromise: The $55 Billion Scam" (Violazione dell'email aziendale: una truffa da 55 miliardi di dollari), settembre 2024.
3. Verizon, *Data Breach Investigations Report* (Report sulle violazioni dei dati), 2024.

2. Rilevamento e neutralizzazione automatizzati delle minacce

I messaggi dannosi che raggiungono le caselle email o vengono segnalate dagli utenti possono monopolizzare i team della sicurezza e ridurre la loro produttività. L'analisi e la rimozione manuali di queste minacce richiedono molto tempo. È essenziale rilevare e neutralizzare queste minacce rapidamente. Un intervento rapido può fare la differenza tra un incidente minore e una violazione su larga scala.

Ecco le caratteristiche essenziali di una soluzione di sicurezza dell'email a tal proposito:

- **Casella di posta per gli abusi ottimizzata dall'IA.** I messaggi segnalati dagli utenti devono essere gestiti il più rapidamente possibile. Quando sono automaticamente indirizzati verso una casella email monitorata da una macchina, possono essere analizzati dall'IA e neutralizzati senza l'intervento del tuo team IT o della sicurezza. Un sistema di risposta automatica deve anche informare gli utenti che le loro segnalazioni sono state ricevute. Questo chiude il circuito di riscontri e rafforza i comportamenti positivi.
- **Orchestrazione e remediation automatiche.** Le email dannose non devono in alcun caso rimanere nelle caselle email degli utenti. Al contrario, devono essere immediatamente rimosse dalle caselle email di tutta l'azienda. Assicurati anche che la soluzione si integri facilmente con i tuoi strumenti SIEM/SOAR esistenti. Avrai così a disposizione una vista più unificata del tuo ecosistema di sicurezza.
- **Flussi di lavoro semplificati.** Gli strumenti di sicurezza devono facilitare il lavoro degli analisti. Per esempio, i flussi di lavoro intuitivi e i chiari riepiloghi delle minacce generati dall'IA sono fondamentali per la loro produttività. Funzionalità come la ricerca integrata e gli avvisi prioritari possono aiutarli a rintracciare rapidamente le minacce. Lo stesso vale per gli strumenti che accelerano le misure correttive che devono essere adottate dopo le azioni automatizzate.

Quando l'efficienza del tuo team della sicurezza migliora, le tue difese si rafforzano. Inoltre, sfrutti al meglio le risorse e gli investimenti di sicurezza esistenti.

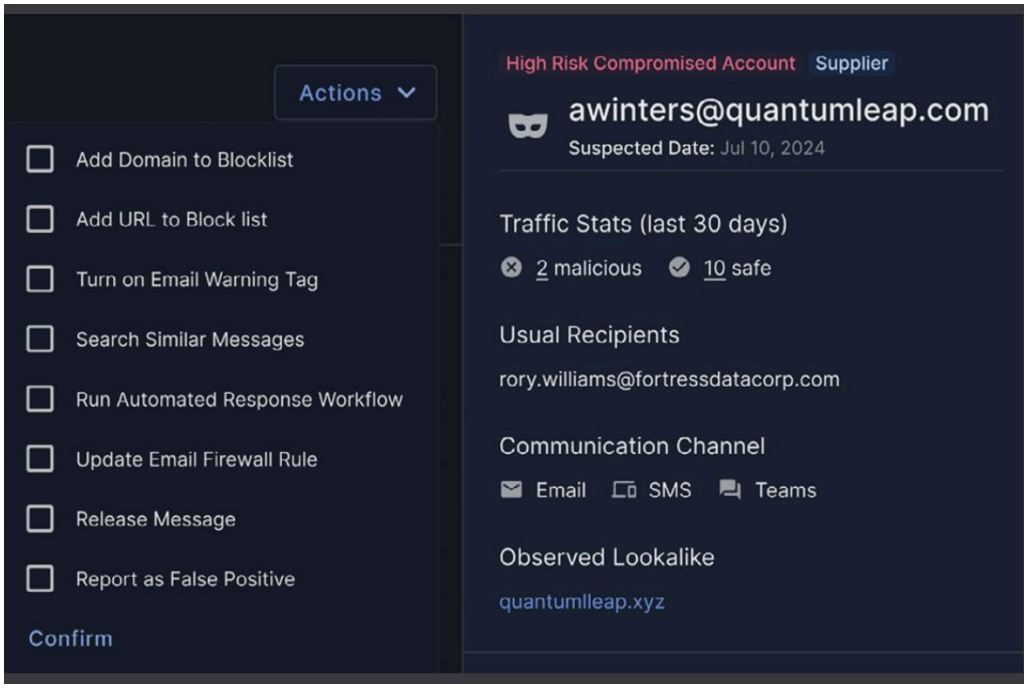


Figura 3. Esempi di flussi di lavoro automatici di rilevamento e risposta di Proofpoint Core Email Protection

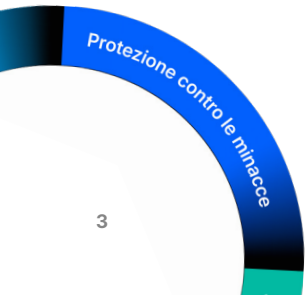


Figura 4. Vantaggi dell'implementazione tramite API e gateway email sicuro di Proofpoint Core Email Protection

3. Opzioni di implementazione flessibili

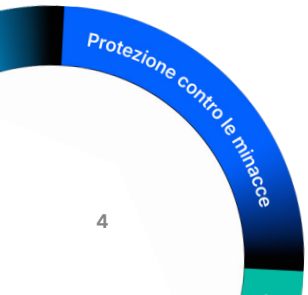
La tua architettura, le tue priorità di sicurezza e le tue esigenze di conformità sono in costante evoluzione. Una soluzione di sicurezza dell'email deve essere in grado di evolvere e scalare in parallelo. Anche se un'implementazione tramite API rappresenta il miglior approccio oggi, è possibile che non lo sarà in futuro. Non legandoti a un solo approccio di distribuzione, hai la garanzia di poter ottimizzare la tua copertura in base ai tuoi rischi.

Infine, quando disponi di una scelta, i tuoi team IT e della sicurezza possono far scalare e rafforzare le tue difese affinché rimangano efficaci nel lungo periodo. E la tua azienda può mantenere una solida protezione di pari passo con la sua crescita.

Ecco le funzionalità da prendere in considerazione:

- **Implementazione tramite gateway email sicuro.** I gateway email sicuri assicurano una protezione completa per numerosi tipi di ambienti. È l'opzione da privilegiare se desideri avere una sicurezza dell'email altamente personalizzabile. Questi gateway ti permettono di massimizzare il tuo livello di protezione end-to-end grazie a una protezione prima della consegna, dopo la consegna e al momento del clic. Forniscono opzioni di configurazione flessibili, nonché visibilità sui rischi legati alle persone.
- **Implementazione basata su API.** Quest'opzione offre un onboarding semplice e controlli predefiniti all'interno di piattaforme cloud come Microsoft 365. L'implementazione può essere completata in pochi minuti. Questa è la scelta più adatta se desideri una sicurezza dell'email potente ma che richiede poche attività di configurazione, nonché un'esperienza di amministrazione altamente automatizzata, con informazioni sulle minacce facili da comprendere e azioni di remediation automatiche.

Scegliendo un fornitore di soluzioni che offre opzioni di implementazione flessibili, disponi del tipo di rilevamento più adatto a te, assicurando al contempo la longevità della tua sicurezza.



74%

Percentuale di CISO che ritengono il fattore umano come la più grande vulnerabilità della loro azienda[4]

40%

La sensibilizzazione alla sicurezza può ridurre il numero di clic su minacce reali di oltre il 40% in meno di sei mesi[5]

4. Esperienza utente eccellente

Si dice che il tuo rischio maggiore e la tua miglior arma di rilevamento occupino lo stesso spazio: quello tra la sedia e la tastiera. Affinché i messaggi dannosi vengano bloccati, gli utenti devono disporre dei giusti strumenti.

Quando sono sovraccarichi, è più probabile che ignorino le minacce reali o commettano errori. Spam, graymail e falsi allarmi incessanti aumentano questo rischio. I collaboratori hanno bisogno di avvisi chiari e fruibili, strumenti di generazione dei report intuitivi e simulazioni di phishing ben concepite per rafforzare i comportamenti di sicurezza positivi.

Ecco le caratteristiche essenziali di una soluzione di sicurezza dell'email:

- **Rilevamento di spam e graymail.** Lo spam e i messaggi inviati in blocco ingombrano le caselle email e distraggono gli utenti. Anche la graymail, come le email commerciali non richieste, possono minare la produttività. La sicurezza dell'email mantiene le caselle email pulite e in ordine, migliorando l'esperienza dell'utente e aiutando i collaboratori a rimanere concentrati.
- **Avvisi agli utenti in caso di messaggi sospetti.** Le email sospette possono essere di natura dannosa o legittima, e solo un utente può distinguerle. Le notifiche contestuali preliminari informano gli utenti dei segnali di minacce identificati nei messaggi. Allo stesso tempo, neutralizzano automaticamente gli allegati o gli URL dannosi associati al messaggio sospetto, imponendo all'utente di interagire con la notifica prima di poterlo fare con l'email stessa.
- **Protezione al momento del clic.** Anche i collaboratori con le migliori intenzioni possono commettere un errore e fare clic su una minaccia quando sono sommersi dal lavoro. Le protezioni al momento del clic come i banner di avviso permettono agli utenti di fermarsi e riflettere prima di agire. Inoltre, le finestre di navigazione virtuale aggiungono un livello di protezione aggiuntivo prevenendo il furto delle credenziali di accesso e il download di malware.
- **Sensibilizzazione alla sicurezza personalizzata.** Spesso, le simulazioni di phishing e la formazione di sensibilizzazione sono i metodi principali di interazione tra i collaboratori e le soluzioni di protezione dell'email. Gli strumenti di formazione più efficaci offrono apprendimento in tempo reale agli utenti quando gli utenti fanno clic su un messaggio di phishing. Offrono anche devi brevi moduli interattivi, adattati al livello di conoscenze di ogni utente. Questo approccio personalizzato favorisce la sensibilizzazione e comportamenti migliori sul lungo periodo.

Un'esperienza utente coerente aiuta i tuoi utenti a rimanere vigili e concentrati sulla propria attività.

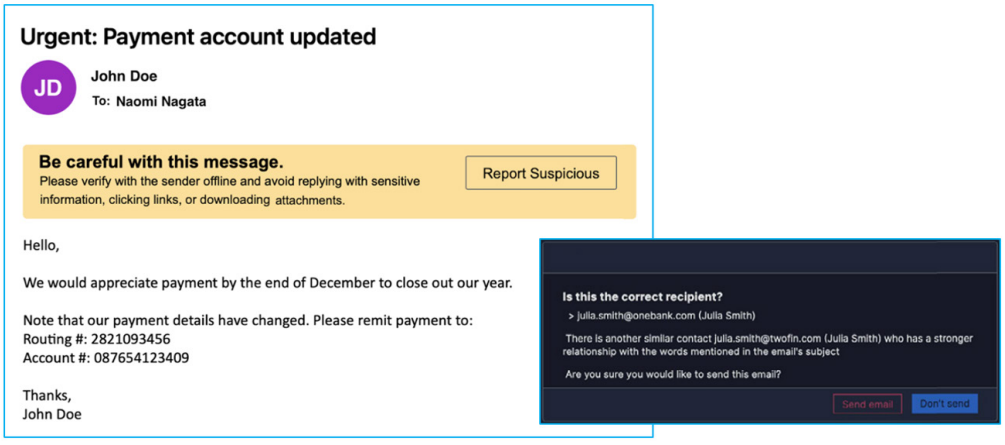
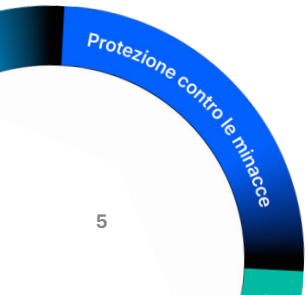


Figura 5. Esempio di messaggio di avviso che segnala un errore potenziale del destinatario e banner di avviso relativo visualizzato nell'email

4. Proofpoint, *Voice of the CISO,* 2024.
5. Ricerca Proofpoint ZenGuide.



2.524%

Aumento del numero di URL dannosi diffuso nell'ambito degli attacchi di phishing tramite SMS nel corso degli ultimi tre anni[6]

5. Protezione contro le minacce oltre le email

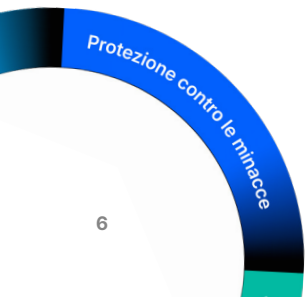
A fronte dell'espansione degli spazi di lavoro digitali, è importante disporre di una piattaforma adattabile. Tale soluzione deve essere in grado di proteggere non solo l'email, ma anche i nuovi canali di comunicazione digitali. I criminali informatici non limitano più i loro attacchi all'email. Hanno seguito gli utenti su piattaforme come Microsoft Teams, Slack, Zoom, LinkedIn e WhatsApp, che sono perciò nuovi vettori d'attacco.

Per essere longeva, una soluzione deve include protezioni avanzate aggiuntive, come l'autenticazione delle email DMARC, il rilevamento affidabile degli account cloud compromessi e visibilità sulle minacce email provenienti dai fornitori.

Ecco gli altri elementi da prendere in considerazione:

- **Autenticazione ottimizzata delle email.** L'autenticazione delle email in entrata e in uscita è uno dei mezzi più efficaci per contrastare le email fraudolente. Per proteggere il tuo marchio, scegli un fornitore di soluzioni che propone servizi gestiti o in hosting per ottimizzare l'implementazione dell'autenticazione. I consigli di esperti possono essere impagabili quando si tratta del protocollo DMARC.
- **Rilevamento di account compromessi.** Associare la visibilità sulle minacce via email (come i clic reali sui messaggi di phishing) e gli avvisi CASB (Cloud Access Security Broker) garantisce un rilevamento più preciso degli account compromessi. Tale approccio limita il numero di falsi positivi e permette di applicare risposte automatiche, come forzare la reimpostazione delle password o eliminare la condivisione di file sensibili.
- **Protezione contro il phishing oltre le email.** Gli URL dannosi sono oggi il vettore d'attacco più comune, in parte perché possono essere inviati tramite tutti i canali, incluse le applicazioni di messaggistica immediata, gli strumenti di collaborazione e i social media. Scegli una soluzione in grado di analizzare gli URL in tempo reale, in modo che i link dannosi vengano bloccati ovunque e ogni volta che un utente cerca di accedervi.
- **Riduzione dei rischi legati ai fornitori.** Può essere complesso identificare le minacce all'interno della tua supply chain senza una visibilità sufficiente. Le soluzioni di protezione dell'email con funzionalità integrate di identificazione dei rischi legati ai fornitori possono attribuire dei punteggi di rischio e rilevare gli account dei fornitori compromessi, contribuendo a limitare le frodi. Associato all'autenticazione, questo approccio proattivo può rafforzare la protezione contro uno dei vettori d'attacco più difficili da identificare.

Grazie a queste funzionalità, i tuoi team possono gestire in modo efficace le minacce nuove e emergenti, qualunque sia la loro origine.



6. Ricerca Proofpoint.

Conclusione

Oltre il 94% delle minacce che prendono di mira i tuoi collaboratori vengono trasmesse via email[7], motivo per cui una solida protezione di questo vettore è fondamentale.

Per ottimizzare la tua protezione contro le minacce, scegli una soluzione di sicurezza dell'email completa, che includa funzionalità di base e avanzate. Tale soluzione deve essere in grado di rilevare e neutralizzare le minacce in modo automatico, nonché offrire un'esperienza utente eccellente. Idealmente, deve anche offrire opzioni di implementazione flessibili per adattarsi all'evoluzione delle tue esigenze. Infine, deve proteggere altri canali digitali oltre l'email, come gli strumenti di collaborazione, le piattaforme di messaggeria immediata e le applicazioni cloud.

Ti affidi a soluzioni a un insieme di soluzioni singole e frammentate? Se la risposta è sì, hai la possibilità di migliorare la protezione del tuo sistema email. È giunto il momento di valutare l'efficacia della tua sicurezza attuale contro tutte le minacce incentrate sulle persone per l'email e altri vettori.

Proofpoint offre sicurezza incentrata sulle persone

Proofpoint Core Email Protection permette alla tua azienda di ridurre i rischi in tutti i punti di interazione degli utenti, oggi e in futuro.

Proofpoint Core Email Protection blocca il 99,99% delle minacce trasmesse via email prima che si trasformino in violazioni. Alimentato da Proofpoint Nexus, il nostro stack di rilevamento avanzato ottimizzato dall'IA, Proofpoint Core Email Protection identifica e neutralizza le minacce email avanzate, incluso il phishing, la violazione delle email aziendali (BEC), il malware, il ransomware, il takeover degli account, il furto d'identità, il social engineering, ecc. Grazie alla console moderna e intuitiva che offre visibilità completa sulle minacce e flussi di lavoro di remediation automatizzati, gli analisti della sicurezza lavorano in modo più efficiente. L'architettura a lungo termine della soluzione la prepara a affrontare il panorama delle minacce di domani, grazie a opzioni di implementazione flessibili di tipo API o gateway email sicuro.

Eco perché oltre due milioni di clienti, di cui l'85% delle aziende della classifica Fortune 100, si affidano a soluzioni di sicurezza incentrate sulle persone di Proofpoint per proteggere i loro utenti e la loro attività.

Per saperne di più, contatta il nostro team delle vendite all'indirizzo sales@proofpoint.com.

7. Ricerca Proofpoint.

proofpoint.

Proofpoint, Inc. 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.

Seguici: LinkedIn

SCOPRI LA PIATTAFORMA PROOFPOINT →

0203-010-05-02