EBOOK

Proteggere la tua identità con Proofpoint

Casi d'uso e testimonianze di successi

proofpoint.

Introduzione

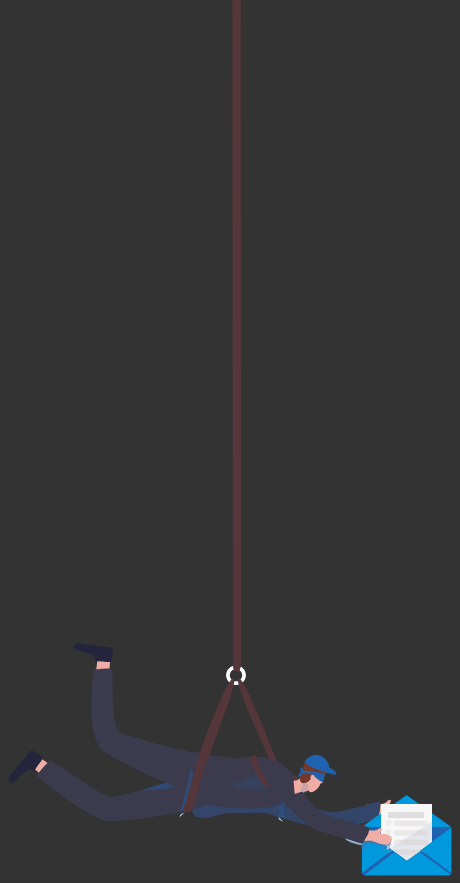
L'escalation dei privilegi e lo spostamento laterale rappresentano una sfida costante per la maggior parte dei team della sicurezza anche nelle più grandi aziende del mondo. Microsoft è l'esempio perfetto. Nel gennaio 2024, l'azienda ha annunciato di essere stata vittima di una violazione da parte di un celebre gruppo di criminali informatici sostenuto dalla Russia.

I criminali informatici hanno sfruttano un vecchio account di test lasciato senza protezione. Una volta violato l'account, hanno elevato i suoi privilegi e si sono spostati lateralmente sui sistemi cloud di Microsoft. Ma ecco il problema: poiché si facevano passare per utenti legittimi, sono sfuggiti a tutti i rilevamenti per oltre un mese[1].

Violazioni come questa evidenziano la debolezza nel mezzo della catena d'attacco. È lì che i criminali informatici utilizzano gli account compromessi per penetrare nei livelli successi delle difese di un'azienda. Per farlo, sfruttano errori di configurazione e identificano le vulnerabilità legate alle identità per ottenere accesso a account con privilegi sempre più elevati.

Escalation dei privilegi e spostamento laterale

1 Bleeping Computer. "Microsoft Reveals How Hackers Breached Its Exchange Online Accounts." (Microsoft rivela come dei criminali informatici hanno violato i suoi account online Exchange), gennaio 2024.



Questa parte della catena d'attacco gioca un ruolo fondamentale negli attacchi informatici. Con un'identità rubata, i criminali informatici assomigliano come una goccia d'acqua a utenti legittimi, il che li rende invisibili. Poiché sono invisibili, possono fare praticamente tutto ciò che desiderano: reimpostare le password, modificare le policy, installare software, estrarre e crittografare dati per richiedere un riscatto, ecc.

Cosa si può fare per bloccarli?

Proofpoint Identity Protection ti fornisce le analisi di cui hai bisogno per identificare le tue identità vulnerabili e correggerle prima che i criminali informatici se ne approprino. Ma non solo. Permette anche di far luce sui criminali informatici attivi una volta che si sono infiltrati nel tuo ambiente.

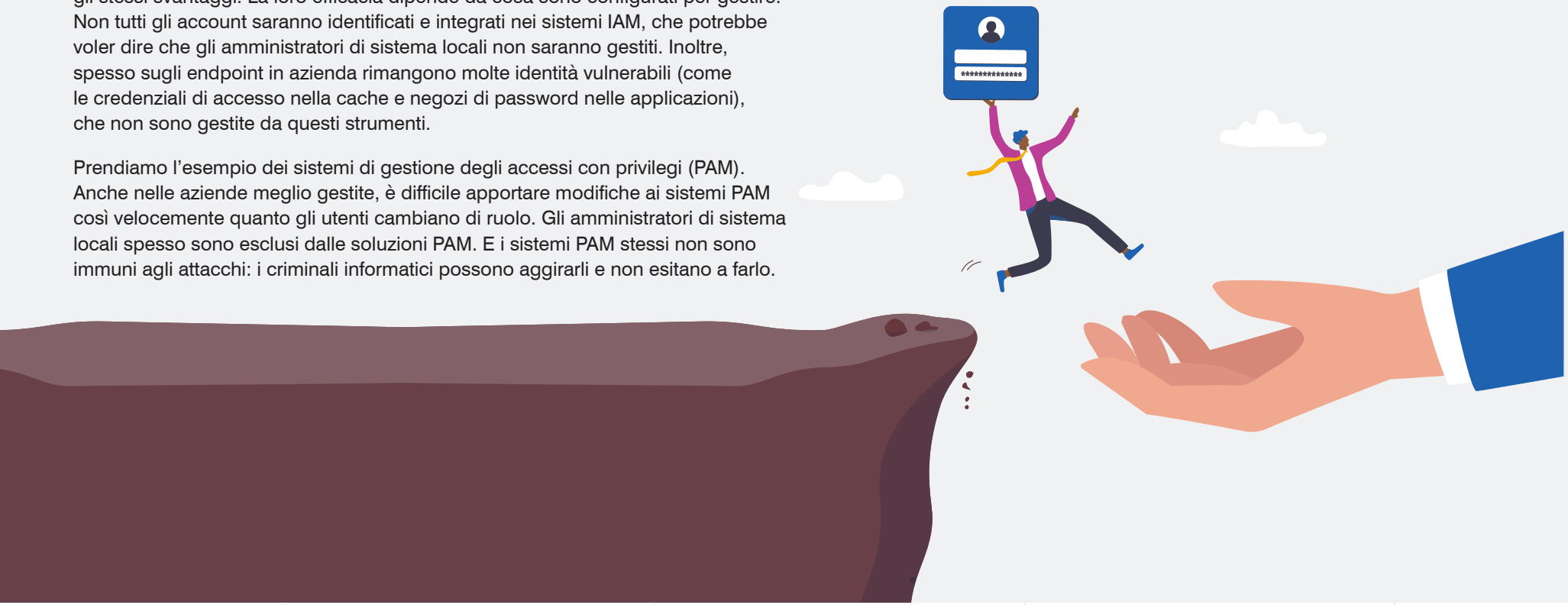
Questo eBook presenta tre casi d'uso volti a illustrare il funzionamento di questa soluzione, Include anche delle testimonianze dei clienti per mostrarti come Proofpoint Identity Protection si comporta in azione.

CASO D'USO 1:

Correggere le lacune di sicurezza lasciate dagli strumenti IAM

Tutti i comuni strumenti di gestione delle identità e degli accessi (IAM) condividono gli stessi svantaggi. La loro efficacia dipende da cosa sono configurati per gestire. Non tutti gli account saranno identificati e integrati nei sistemi IAM, che potrebbe voler dire che gli amministratori di sistema locali non saranno gestiti. Inoltre, spesso sugli endpoint in azienda rimangono molte identità vulnerabili (come le credenziali di accesso nella cache e negozi di password nelle applicazioni), che non sono gestite da questi strumenti.

Prendiamo l'esempio dei sistemi di gestione degli accessi con privilegi (PAM). Anche nelle aziende meglio gestite, è difficile apportare modifiche ai sistemi PAM così velocemente quanto gli utenti cambiano di ruolo. Gli amministratori di sistema locali spesso sono esclusi dalle soluzioni PAM. E i sistemi PAM stessi non sono immuni agli attacchi: i criminali informatici possono aggirarli e non esitano a farlo.



In breve

Una società di finanziamento per veicoli utilizza Proofpoint per ampliare le sue funzionalità di sicurezza per includere la gestione dei rischi legati all'identità.

Profilo del cliente

Settore di attività: servizi finanziari

Collaboratori: 9.000

Sede: mondo

Soluzione

Prodotto: Proofpoint Identity Protection

Componente: Proofpoint Spotlight

Come Proofpoint può aiutarti

Componente di Proofpoint Identity Protection, Proofpoint Spotlight ti aiuta a identificare le tue identità vulnerabili e correggere le lacune di sicurezza delle tue identità prima che i criminali informatici le sfruttino. Per farlo, analizza i tuoi endpoint, i sistemi IAM e i repository delle identità per rilevare tutte le identità non gestite, configurate in modo errato o esposte. I risultati di queste analisi ti vengono presentati in un report facile da assimilare. Il report mostra tutti i percorsi di attacco disponibili e ti fornisce un elenco delle identità che devi correggere per prime.

Proofpoint in azione

Una società di finanziamento per veicoli rafforza le sue funzionalità di sicurezza per proteggere meglio le sue identità.

Questa azienda mondiale di finanziamento per veicoli aveva creato un'infrastruttura IT vasta e complessa nel corso di 30 anni. Sebbene disponesse di un sistema PAM, solo pochi account sulle sue applicazioni legacy erano gestite da tale sistema. Alcuni account amministratore e di servizio ne erano addirittura esclusi. L'azienda non poteva perciò gestire completamente le sue identità e le sue credenziali d'accesso con privilegi, né visualizzare tutti i rischi legati alle sue identità.

Nel corso di una revisione di routine dell'approccio dell'azienda in termini di valutazione automatizzata dei rischi, il team della sicurezza informatica ha rilevato che non disponeva di alcun mezzo per gestire i rischi legati alle sue identità. Ha quindi scelto Proofpoint Spotlight per correggere questa lacuna di sicurezza. Poco dopo, Proofpoint è stato integrato negli endpoint (client e server) e nell'infrastruttura Active Directory (AD) dell'azienda. Ha iniziato quindi a analizzare tutti i suoi endpoint, il suo sistema PAM e altri repository di identità alla ricerca di vulnerabilità.

Il team della sicurezza informatica dell'azienda ha organizzato una riunione con il team responsabile della correzione delle vulnerabilità informatiche per esaminare le sue conclusioni. I due team hanno deciso che era preferibile lavorare insieme per implementare le modifiche necessarie per ridurre i rischi legati alle identità. Hanno anche seguito l'impatto di tali cambiamenti nel tempo.

Dopo poco più di un anno di utilizzo di Proofpoint Spotlight, i team hanno ottenuto dei risultati incredibili. Sebbene diversi nuovi problemi critici continuavano a manifestarsi ogni settimana, disponevano di nuovi processi per risolverli rapidamente.

> "[Proofpoint Spotlight] ci ha offerto nuove prospettive. Precedentemente, sapevamo di dover analizzare in modo approfondito questi rischi legati alle identità, ma non disponevamo di alcun mezzo per farlo."
>
> –Assistant Vice President, IT Vulnerabilities, società di finanziamento per veicoli

Principali punti da ricordare

È sufficiente una sola vulnerabilità legata a un'identità per mettere a repentaglio tutto il tuo ambiente. Hai bisogno di strumenti in grado di far luce sulle vulnerabilità legate alle tue identità per poter identificare i rischi e ridurli nel corso del tempo. In questo modo puoi bloccare migliaia di porte che conducono a delle identità prima che i criminali informatici abbiamo l'occasione di aprirle.

AD e i sistemi d'identità sono complessi e evolvono costantemente, moltiplicando i rischi legati all'identità,

Quando una persona causa la violazione di un'identità, in genere non è malintenzionato, ma ha commesso un errore o ha agito di fretta.

CASO DI UTILIZZO 2:

Superare gli esercizi di simulazione di attacchi

Anche quando le difese falliscono, i veri vincitori degli esercizi di simulazione di attacchi sono le aziende che li utilizzano per rafforzare il loro livello di sicurezza. Ciò nonostante, quando un esercizio espone delle identità non gestite o configurate in modo errato nella tua azienda, non è mai una buona notizia. Ma stai tranquillo: succede quasi a tutti. Infatti, il 95% degli strumenti di simulazione di attacchi identifica le credenziali d'accesso di amministratori dei domini esposti durante i loro esercizi[2].

2. Studio di Illusive.

In breve

Il team SOC di una banca al dettaglio utilizza Proofpoint per impedire a uno strumento di simulazione di attacchi di collegarsi ai suoi account critici e di compromettere i suoi server.

Profilo del cliente

Settore di attività: Finanza

Collaboratori: 1.000

Sede: EMEA

Soluzione

Prodotto: Proofpoint Identity Protection

Componente: Proofpoint Shadow

Come Proofpoint può aiutarti

Proofpoint Identity Protection può aiutarti a rilevare gli attacchi nel mezzo della catena d'attacco e a impedire a uno strumento di simulazione d'attacchi di andare a buon fine senza essere rilevato.

- **Proofpoint Shadow** crea una rete complessa di dati fasulli e vie d'accesso a risorse in apparenza sensibili per poi propagarle in tutta l'azienda. Anche gli strumenti di simulazione di attacchi più avanzati non sanno distinguere ciò che è vero da ciò che è falso. L'unico modo per loro di fare la differenza è di provare a utilizzare ciò che hanno scoperto, avvertendo i team della sicurezza della loro presenza. Con questa rete di esche, è praticamente impossibile per loro spostarsi verso risorse informatiche strategiche senza essere rilevati.
- **Proofpoint Spotlight** può aiutarti a identificare tutte le identità non gestite, configurate in modo errato e esposte nel tuo ambiente. Puoi anche correggerle prima che gli strumenti di simulazione di attacchi - e i criminali informatici - possano sfruttarle.

Proofpoint in azione

Una grande banca al dettaglio blocca due simulazioni di attacchi.

Una grande banca al dettaglio e d'investimento disponeva di molteplici livelli di controlli di sicurezza e di diversi strumenti per bloccare il malware sugli endpoint. Ma a fronte della moltiplicazione delle minacce persistenti avanzate (APT), desiderava aggiungere nuove funzionalità di rilevamento al suo arsenale. Ha quindi installato Proofpoint Shadow. Poco dopo, la banca ha ingaggiato un'azienda rinomata specializzata nei test d'intrusione affinché attaccasse la sua rete. Tuttavia, non ha avvertito l'azienda che avrebbe utilizzato Proofpoint per sventare i suoi attacchi.

Prima dell'inizio del test di intrusione, Proofpoint Shadow ha creato dei falsi dati volti a attirare i criminali informatici su ogni endpoint della rete di 5.000 nodi della banca. Tutti i dati sono stati personalizzati affinché sembrassero appartenere a un ambiente bancario, incluse delle false credenziali d'accesso.

Il primo giorno di test, Proofpoint Shadow ha rilevato dei tentativi di attività dannosa provenienti da un falso utente ("utente A") su uno dei server Citrix della banca. Ha poi raccolto informazioni dettagliate ("chi, cosa, quando e dove") dell'attacco e ha avvisato i team SOC e di risposta agli incidenti.

Nel corso delle loro indagini, i team hanno scoperto che gli specialisti in test di intrusione avevano installato degli strumenti dannosi sulla rete della banca e hanno tentato di utilizzare altri account fasulli, raccolti dopo la violazione iniziale, per far progredire il loro attacco. Gli specialisti in test di intrusione non avevano alcuna idea di essere già stati individuati dai team della sicurezza.

In seguito, il 22° giorno Proofpoint Shadow ha inviato un altro avviso relativo a un'attività dannosa effettuata dall'utente A, ma su un server diverso. Quando il team SOC ha effettuato una seconda analisi forense, ha scoperto dei tentativi aggressivi di connessione a account critici tramite quel server. Il criminale informatico aveva involontariamente fatto scattare l'allarme utilizzando due insiemi diversi di false credenziali di accesso.

Principali punti da ricordare

Se il tuo team SOC può superare degli esercizi di simulazione di attacchi, è più probabile che sia in grado di bloccare dei criminali informatici reali in caso prendano di mira il tuo ambiente.

Un rilevamento precoce dei comportamenti sospetti consente ai team SOC e della sicurezza delle informazioni di neutralizzare i criminali informatici prima che si spostino lateralmente e raggiungano le risorse informatiche strategiche di un'azienda. Questi rilevamenti includono anche dati preziosi che permettono ai team di effettuare un'analisi forense degli attacchi, facilitando la risposta agli incidenti e la riduzione dei rischi.

Il rilevamento di un tentativo di violazione delle password su un account fasullo assicura un avviso estremamente affidabile - un vero positivo che indica un'attività dannosa sulla rete con un tasso di affidabilità del 100%.

CASO DI UTILIZZO 3:

Proteggere le identità ibride in AD e Entra ID

Active Directory (AD) è una pietra miliare della moderna infrastruttura IT aziendale. Secondo alcune stime, il 90% delle aziende utilizza AD come metodo principale di autenticazione e autorizzazione degli utenti. Poiché sempre più aziende migrano verso il cloud, Microsoft Entra ID (in precedenza Azure AD) è diventato onnipresente.

Sebbene diffusi, questi strumenti sono anche noti per essere difficili da gestire e mantenere, soprattutto perché riguardano quasi tutte le postazioni, gli utenti e gli endpoint della rete. Proprio come gli strumenti IAM, gli sforzi compiuti non vengono mai pienamente ripagati perché le autorizzazioni, gli utenti e le aziende evolvono costantemente. Inoltre, non tutte le identità vengono coperte. Prendiamo l'esempio delle credenziali d'accesso nella cache sugli endpoint. AD e Entra ID non le gestiscono, e nemmeno i sistemi IAM. Rappresentano perciò un rischio significativo.

In breve

Una holding bancaria utilizza Proofpoint per valutare il livello di sicurezza di una nuova acquisizione e scopre 3.000 amministratori di dominio sulle sue workstation.

Profilo del cliente

Settore di attività: Finanza

Collaboratori: 25.000

Sede: Stati Uniti

Soluzione

Prodotto: Proofpoint Identity Protection

Componente: Proofpoint Spotlight

Come Proofpoint può aiutarti

Proofpoint Spotlight analizza AD, Entra ID e numerosi altri repository d'identità e rileva gli account con privilegi di cui non dovrebbero disporre. Inoltre, identifica le identità non gestite sugli endpoint, nonché le identità con privilegi che non vengono gestite dalla soluzione PAM o altri sistemi IAM. Puoi così correggerli prima che finiscano nelle mani sbagliate.

Proofpoint Spotlight offre anche una vista ascendente e discendente sui rischi legati alle tue identità non gestite, con errori di configurazione e esposte. I team della sicurezza dispongono così di una visibilità sulle vie d'attacco che potrebbero essere utilizzate dai criminali informatici per implementare ransomware e rubare dati.

Proofpoint in azione

Una holding bancaria valuta i rischi legati alle identità di una nuova acquisizione per intraprendere la fusione-acquisizione in totale sicurezza.

Con circa 200 miliardi di dollari di patrimonio e 1.000 filiali, questa holding bancaria regionale acquisisce una nuova banca ogni tre anni. A ogni fusione-acquisizione, il tuo team IT combina sistemi, software, dati e processi. Ma prima di farlo, la holding deve valutare la sicurezza della banca che acquista. In questo esempio, il team aveva a disposizione meno di quattro mesi per effettuare la sua valutazione.

Il livello di sicurezza di una banca dipende interamente dalla sicurezza delle sue identità. Il team IT della banca sapeva che se fosse stato in grado di identificare le vulnerabilità legate alle identità della nuova acquisizione, avrebbe avuto un'idea precisa del suo livello di sicurezza.

Negli ultimi sei mesi, il team ha utilizzato Proofpoint Identity Protection per analizzare le sue workstation e i repository delle identità. Tali informazioni preziose gli erano perciò famigliari. Per questo motivo ha deciso di utilizzare Proofpoint Spotlight per effettuare la valutazione iniziale della banca acquisita.

> "Sono lieto di aver utilizzato [Proofpoint Spotlight], tutti ne hanno percepito il valore. Procederemo allo stesso modo anche per la nostra prossima fusione-acquisizione."
>
> – Direttore tecnico della sicurezza informatica

Dopo aver analizzato l'ambiente IT della nuova acquisizione, Proofpoint ha generato una scheda di valutazione dei rischi che dettagliava diverse aree di rischio legato alle identità. Una è saltata immediatamente all'occhio: sulle sue workstation erano presenti 3.000 account amministratori di dominio. Se solo uno di questi fosse stato violato da un criminale informatico, il team avrebbe perso il controllo dell'intero ambiente.

Dopo aver appreso le pratiche di sicurezza della nuova banca, i dirigenti hanno deciso che, dati i rischi, era preferibile mantenere separati i due ambienti, almeno in un primo tempo. Senza Proofpoint, sarebbe stato molto più difficile giustificare il rafforzamento della protezione che il team IT ha ritenuto necessaria.

Principali punti da ricordare

Spesso, i rischi legati alle identità derivano dai normali processi aziendali e IT che sono in essere da molti anni. Sono perciò difficili da rilevare e facili da trascurare, in particolare in ambienti di recente acquisizione a seguito di una fusione-acquisizione.

È fondamentale analizzare costantemente AD, Entra ID, gli endpoint e altri repository alla ricerca di vulnerabilità legate alle identità. Un criminale informatico ha bisogno di violare una sola workstation con un solo utente per prendere il controllo di tutto l'ambiente.

Conclusioni

La maggior parte delle aziende cerca regolarmente software e applicazioni vulnerabili, ma si dimentica spesso delle identità vulnerabili. Tuttavia, le identità hanno un valore inestimabile. In effetti, si tratta delle risorse più preziose delle aziende, perché riguardano tutte le altre risorse digitali.

La loro protezione è di importanza capitale. I criminali informatici attuali hanno accesso a un'ampia gamma di strumenti che permettono loro di sfruttare le credenziali d'accesso in modo rapido, semplice e efficace. Peggio ancora, è difficile per le aziende rilevare il loro utilizzo.

Per interrompere la catena d'attacco, devi proteggere le tue identità nello stesso modo in cui proteggi tutte le altre risorse strategiche. Si comincia con l'adozione di misure proattive. Devi correggere le tue identità vulnerabili prima che dei criminali informatici le scoprano e utilizzare delle esche per intercettare i criminali informatici prima che causino danni.

Per scoprire come Proofpoint può aiutarti a proteggere le tue identità, visita la pagina: https://www.proofpoint.com/us/products/identity-protection.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **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 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**.

proofpoint.

0513-002-05-01 4/24