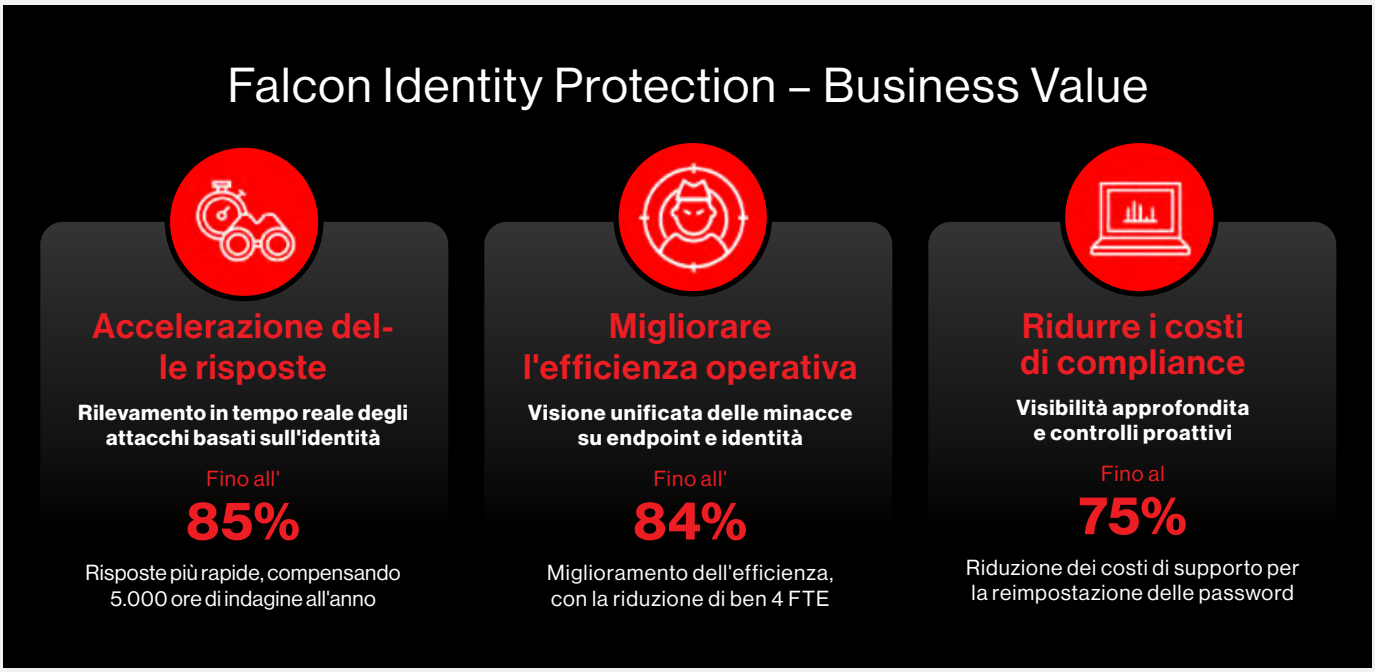
CROWDSTRIKE

I principali motivi per aggiungere subito Falcon Identity Threat Protection al tuo arsenale di difesa informatica

Gli attacchi basati sull'identità sono la prima minaccia alla sicurezza informatica che si presenta oggi alle organizzazioni. Supera addirittura l'80% il numero degli incidenti informatici che prevede l'uso improprio di credenziali valide per accedere alla rete di un'organizzazione.

CrowdStrike Falcon® Identity Threat Protection, un modulo della piattaforma CrowdStrike Falcon®, rileva e blocca in tempo reale le violazioni basate sull'identità in un complesso panorama di identità ibride, con un unico sensore e un'interfaccia unificata per le minacce con correlazione degli attacchi tra endpoint, workload, identità e dati. Ecco cinque vantaggi previsti che puoi aspettarti se aggiungi subito la protezione dell'identità al tuo arsenale di difesa contro le minacce alla sicurezza informatica.*



1. Accelera le risposte alle minacce fino all'85%

Le soluzioni tradizionali limitate agli endpoint non rilevano le minacce all'identità e l'attuale approccio di creazione manuale delle correlazioni delle minacce tra endpoint e identità con più strumenti autonomi (strumenti di AD hygiene, log eventi di Windows, PAM, UEBA, SIEM e altro) rallenta le risposte del SOC. Con la piattaforma unificata CrowdStrike Falcon, i clienti di Falcon Identity Threat Protection sono in grado di visualizzare percorsi di attacco completi e correlare le minacce all'interno di un'unica console. Ciò può comportare **risposte più rapide fino all'85%** e protezione in tempo reale, con una compensazione di migliaia di ore di indagini post-violazione ogni anno.

2. Aumenta l'efficienza operativa fino all'84%

CrowdStrike Falcon è **una soluzione cloud native con un unico sensore** che può essere implementata ovunque nell'ambiente del cliente, semplificando la raccolta della telemetria (da endpoint o identità). Un grande distributore al dettaglio **ha riunito più di 5 strumenti** (tipici di molte aziende) in uno per gestire le minacce all'identità con Falcon Identity Threat Protection. Il consolidamento del SOC con un'unica piattaforma e un unico sensore elimina gli strumenti e gli agenti indipendenti, con conseguente risparmio diretto dei costi operativi e degli strumenti. Inoltre, eliminando la necessità di utilizzare l'acquisizione di log diversi, la detection in tempo reale può ridurre le ore di manutenzione totali e **aumentare l'efficienza operativa fino all'84%**, riducendo l'organico di circa quattro FTE.

3. Riduce i costi di compliance e supporto fino al 75%

La profonda visibilità sulle password compromesse, sugli account con privilegi eccessivi e sull'uso improprio degli account di servizio consente ai clienti di affrontare in modo proattivo i problemi di hygiene di Active Directory e di stabilire controlli proattivi, riducendo così i costi di conformità. In un caso, un CISO ha segnalato **una riduzione del 75% nelle reimpostazioni delle password di supporto e nei costi associati,** una riduzione dell'8% nella suscettibilità al phishing e una riduzione del 32% nei diritti di accesso degli utenti non necessari. Una grande azienda di telecomunicazioni ha dichiarato di aver migliorato la postura di compliance della Cybersecurity Maturity Model Certification (CMMC) utilizzando Falcon Identity Threat Protection per estendere l'autenticazione multifattoriale (MFA) ovunque, anche alle applicazioni legacy.

4. Riduce fino al 57% il rischio che le credenziali rubate conducano a una violazione

Con otto attacchi su 10 che coinvolgono credenziali rubate o compromesse, la riduzione del rischio delle credenziali rubate ha un impatto diretto sul miglioramento della posizione di rischio. La capacità di Falcon Identity Threat Protection di rilevare le minacce specifiche per l'identità consente ai clienti di identificare gli account ad alto rischio e i possibili percorsi di attacco nell'intero ambiente, riducendo la superficie di attacco. Recentemente, il CISO di una catena di hotel ha raccontato come Falcon Identity Threat Protection abbia immediatamente messo in luce 250.000 possibili percorsi di attacco nell'ambiente dell'azienda e come il 93% di questi potesse essere risolto con tre specifiche modifiche alla configurazione. Le valutazioni del valore aziendale di CrowdStrike hanno dimostrato una **riduzione fino al 57% del rischio che le credenziali rubate** conducano a una violazione. Ciò è stato dimostrato anche dai test di penetrazione effettuati con successo da clienti che non avevano superato i medesimi test prima del deployment di Falcon Identity Threat Protection.

5. Migliora l'assicurabilità informatica e riduce i premi

Mentre gli avversari continuano a sfruttare i deboli controlli di sicurezza dell'identità per sferrare attacchi, **le compagnie che offrono polizze assicurative contro gli attacchi informatici sottolineano** la necessità di intensificare i controlli per ridurre il rischio informatico. Poiché il ransomware è uno dei fattori chiave per l'assicurazione della sicurezza informatica, gli assicuratori hanno ribadito alle aziende la necessità di rafforzare AD, di applicare l'autenticazione a più fattori alle applicazioni, comprese quelle legacy, di proteggere gli account privilegiati e di servizio e di implementare il rilevamento e la risposta agli endpoint (EDR) come requisiti per l'assicurabilità informatica. I clienti che hanno implementato Falcon Identity Threat Protection affermano che ha avuto un impatto positivo sul loro programma assicurativo per la sicurezza informatica e ne ha ridotto i premi.

Cosa dicono i clienti di CrowdStrike

"Dopo aver implementato Falcon Identity Threat Protection, abbiamo effettuato un altro test di penetrazione e abbiamo immediatamente visto i vantaggi derivanti dalla maggiore visibilità."

Ryan Melle
SVP, CISO, Berkshire Bank
(**Leggi il caso di studio**)

"Da quando abbiamo implementato Falcon Identity Threat Protection, abbiamo percepito un notevole miglioramento rispetto a quel che osserviamo in relazione a credenziali, identità privilegiate, percorsi di attacco diversi e metodi per contenerli."

Steven Townsley,
Head of Information Security,
Mercedes-AMG Petronas F1 Team
(**Guarda il video**)

"Dopo due ore dal deployment di Falcon Identity Threat Protection, abbiamo identificato 10 account privilegiati con password compromesse e abbiamo iniziato a ripristinarle immediatamente."

CISO di una contea nell'area di Washington, D.C.
(**Leggi il post sul blog**)

"Ci siamo resi conto del valore di Falcon Identity Threat Protection sin dal primo minuto, quando abbiamo visto 250.000 possibili percorsi di attacco il 93% dei quali poteva essere risolto con tre sole modifiche alla configurazione."

CISO di una catena multinazionale di hotel

"È più facile gestire un unico pannello di controllo per la maggior parte del proprio SOC che cercare in 13 console e pagine diverse per analizzare e rilevare qualcosa."

CISO di un'azienda agroalimentare

La protezione dell'identità non è più facoltativa ma fondamentale

Il Global Threat Report 2023 di CrowdStrike mostra che gli attacchi all'identità sono in aumento, con una **crescita del 112% negli annunci di access broker** sul dark web nel 2022. Microsoft Active Directory continua a essere il punto debole preso di mira dagli avversari, con oltre il 90% delle organizzazioni che vi fanno affidamento.[1] Una recente analisi di CrowdStrike relativa ai metadati di milioni di account (umani, di servizio, privilegiati) ha rivelato che uno **sconcertante 50% delle aziende ha account privilegiati con una password compromessa**.

Ad aggravare il problema, le compromissioni dell'identità sono notoriamente difficili da rilevare, poiché richiedono una media di **circa 250 giorni per essere identificate**[2] senza gli strumenti adeguati. In questo lasso di tempo, gli avversari possono muoversi lateralmente senza essere rilevati nel tuo ambiente e lanciare attacchi disastrosi. Con un breakout time medio **ridotto a 84 minuti nel 2022**, secondo il Global Threat Report 2023 di CrowdStrike, le organizzazioni non possono permettersi il lusso di aspettare che si verifichi una grave compromissione dell'identità. L'avversario potrebbe infatti essere già nel tuo ambiente e tu potresti non esserne consapevole.

Ignorare le minacce basate sull'identità potrebbe avere gravi conseguenze, tra cui la compromissione totale del dominio dell'infrastruttura AD, paralizzanti attacchi ransomware e disastrose interruzioni aziendali. Secondo IBM e il Ponemon Institute, il **costo totale medio globale di una violazione dei dati è di 4,35 milioni USD (9,44 milioni USD il costo medio della compromissione negli Stati Uniti)**.[3] Con **8 attacchi su 10** che coinvolgono credenziali rubate o compromesse, l'implementazione della protezione delle identità avrà un impatto immediato, facendoti potenzialmente risparmiare milioni di dollari e proteggendo il tuo marchio e la tua reputazione da danni irreversibili.

Ricorda: gli avversari non aspettano che tu indossi i guantoni per sferrare i loro colpi. Ferma le compromissioni oggi stesso con Falcon Identity Threat Protection.

Contatta il tuo rappresentante CrowdStrike o richiedi la tua Active Directory Risk Review gratuita.

[1]Frost & Sullivan, "Active Directory Holds the Keys to your Kingdom, but is it Secure?"

[2]IBM and Ponemon Institute, "Cost of a Data Breach Report 2022"

[3]IBM and Ponemon Institute, "Cost of a Data Breach Report 2022"

*I risultati previsti e quelli effettivi non sono garantiti e possono variare per ogni cliente. I vantaggi previsti 1, 2 e 4 si basano sulle medie aggregate di oltre 100 casi di valutazione del valore aziendale (BVA, Business Value Assessment) e realizzazione del valore aziendale (BVR, Business Value Realized) condotti sui clienti di CrowdStrike Enterprise e completati dal Business Value team dal 2018 a dicembre 2022.Le BVA sono un'analisi del ROI proiettato basate sul valore di CrowdStrike rispetto alla soluzione esistente del cliente. Le BVR sono un'analisi del ROI realizzato per i clienti impiegati per più di 6 mesi tramite i dati forniti dal cliente e la telemetria registrata. Il vantaggio previsto 3 si basa sui dati condivisi da un cliente direttamente con CrowdStrike.

Informazioni su CrowdStrike

CrowdStrike (Nasdaq: CRWD), leader globale della sicurezza informatica, ha ridefinito la sicurezza moderna con la piattaforma nativa in cloud più avanzata al mondo per la protezione delle aree critiche del rischio aziendale: endpoint e workload cloud, identità e dati.

Con la tecnologia CrowdStrike Security Cloud e l'intelligenza artificiale di prima classe, la piattaforma CrowdStrike Falcon® sfrutta gli indicatori di attacco in tempo reale, le informazioni sulle minacce, lo spionaggio degli avversari in evoluzione e la telemetria arricchita proveniente da tutta l'azienda per fornire rilevamenti estremamente accurati, protezione e ripristino automatici, threat hunting d'élite e osservabilità prioritaria delle vulnerabilità.

Costruita appositamente nel cloud con una singola architettura di lightweight-agent, la piattaforma Falcon assicura una distribuzione rapida e scalabile, protezione e prestazioni superiori, una complessità ridotta e un time-to-value immediato.

CrowdStrike: **We stop breaches.**

Seguici: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Inizia una prova gratuita

Scopri di più su **www.crowdstrike.com/it/**