Cloudflare for Unified Risk Posture

Applicazione automatizzata e dinamica della condizione di rischio su una parte più ampia della superficie d'attacco in espansione.

Problema: Troppa superficie d'attacco

Crescente complessità nella gestione dei rischi

Sta diventando sempre più difficile e inefficiente per le aziende tenere traccia e mitigare rischi sempre più diversificati lungo la loro superficie d'attacco in continua espansione. Oggi i team di sicurezza si trovano a dover affrontare:

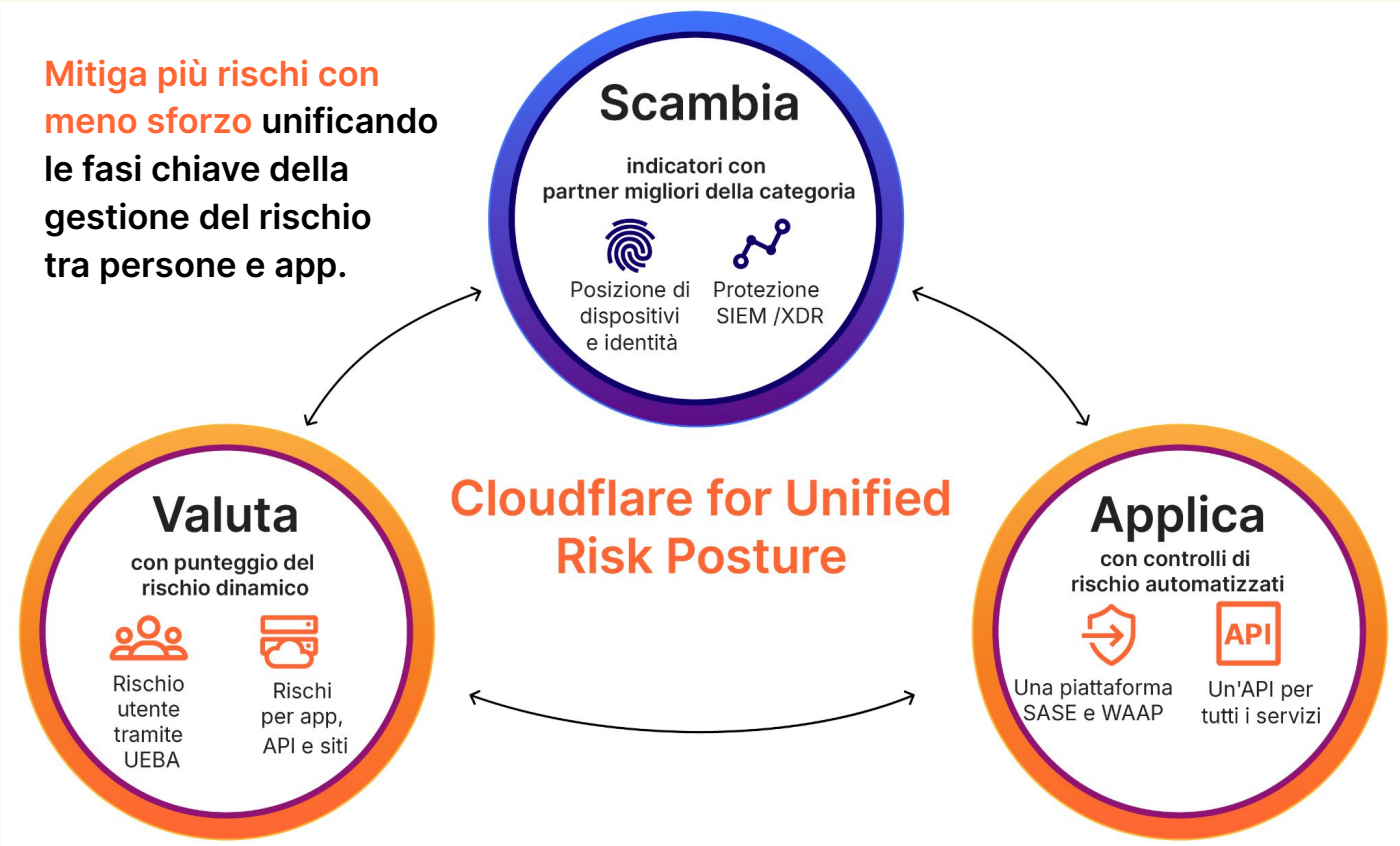
- **Troppi strumenti isolati** con interoperabilità e visibilità limitata per valutare i rischi in maniera olistica
- **Troppi segnali di rischio** che portano a un sovraccarico di informazioni, che rendono difficile stabilire la priorità dei rischi
- **Troppo sforzo manuale** per l'analisi dei rischi che richiede tempo, risorse e competenze

Soluzione: Unificare i controlli sulla condizione di rischio

Una piattaforma per adattarsi ai rischi in evoluzione

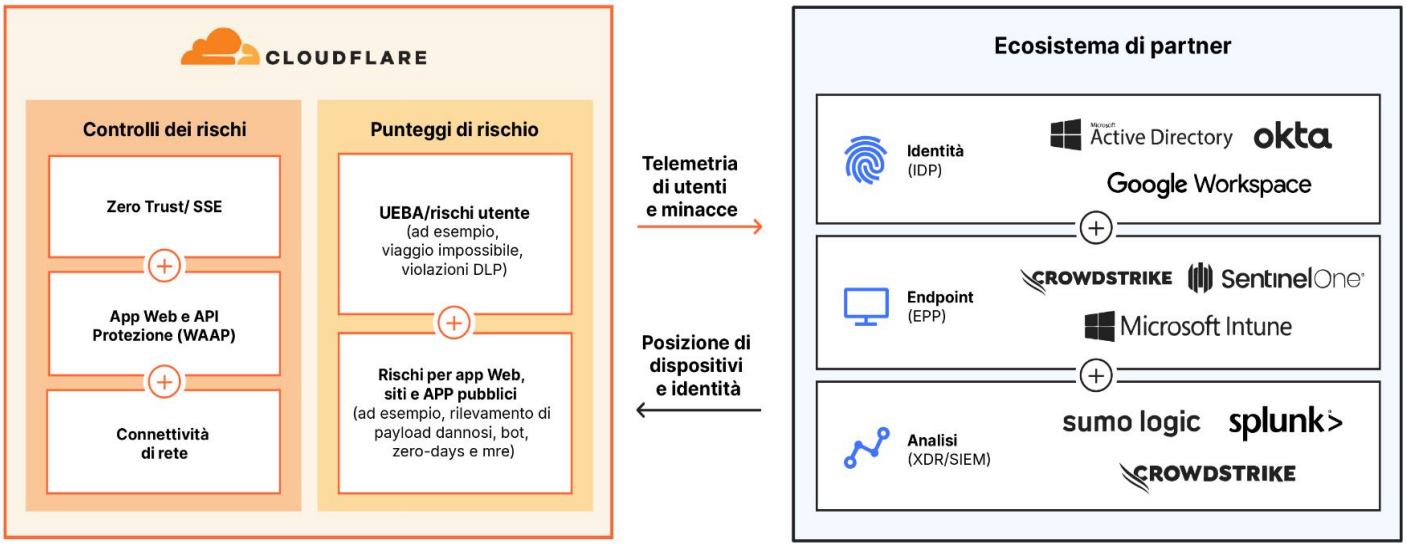
Fai convergere le funzionalità di sicurezza SASE e WAAP sulla rete globale di Cloudflare in modo da gestire i rischi tra persone e app. Semplifica la gestione del rischio realizzando tre attività chiave su un'unica piattaforma:

- **Valuta il rischio tra persone e applicazioni** con modelli dinamici di punteggio del rischio di prima parte
- **Scambia indicatori con gli strumenti migliori della categoria** su piattaforme Endpoint Protection Platform (EPP), IDP, XDR e SIEM
- **Applica controlli automatizzati del rischio su larga scala** in qualsiasi luogo e ambiente IT



Valuta il rischio e scambia i dati con i partner

Cloudflare valuta il rischio aziendale sfruttando modelli dinamici di punteggio di rischio proprietari e scambiando indicatori di rischio con i migliori partner tecnologici della categoria.



Punteggio dinamico del rischio di prima parte

Valuta il rischio tra persone e app con modelli supportati dall'intelligenza artificiale e dal machine learning.

Punteggio del rischio utente (o UEBA)

Rileva il rischio in base al comportamento degli utenti, un approccio noto come analisi delle entità e dei comportamenti degli utenti (UEBA). Cloudflare classifica gli utenti come a rischio alto/medio/basso dopo aver osservato attività sospette o anomale, come viaggi impossibili o violazioni delle policy DLP.

Rischi delle app

Crea politiche per proteggere le app, le API e i siti in base a modelli che identificano payload dannosi, script del browser dannosi, bot e minacce zero-day.

Questi modelli di rischio si applicano a qualsiasi infrastruttura interna o rivolta al pubblico protetta da Cloudflare. Ciò significa che puoi applicare protezioni contro exploit di vulnerabilità delle app, DDoS e bot davanti ad app interne come i server Jira e Confluence self-hosted.

Scambia con i partner

Le integrazioni una tantum con l'API unificata di Cloudflare ti aiutano a fare di più con gli strumenti esistenti.

Acquisisci gli indicatori di rischio

Cloudflare acquisisce i punteggi di rischio da partner di protezione endpoint (EPP) e provider di identità (IDP). Con queste integrazioni, puoi applicare controlli di identità e posizione del dispositivo per qualsiasi richiesta di accesso a qualsiasi destinazione in linea con le migliori pratiche Zero Trust. Integra più provider contemporaneamente per applicare politiche diverse in contesti diversi.

Condividi la telemetria

Invia i log di Cloudflare alle piattaforme di rilevamento e risposta estese (XDR) e di gestione delle informazioni e degli eventi di sicurezza (SIEM) per ulteriori analisi e ulteriori misure di mitigazione del rischio.

Applica controlli automatizzati del rischio su larga scala

Una piattaforma per applicare protezioni basate sui punteggi di rischio propri e di terze parti, alimentata esclusivamente da una rete cloud globale intelligente e programmabile.

Semplifica la gestione del rischio
Consolida i fornitori per ridurre la complessità e il rischio aziendale.

Vedi di più, proteggi di più
Ottieni informazioni automatizzate e dinamiche su rischi e minacce dalla nostra massiccia rete globale.

Scala ovunque
Protezioni resilienti e coerenti in qualsiasi luogo del mondo.

Casi d'uso campione

Caso d'uso: Protezione dei dati sensibili

Problema: l'utente gestisce in modo improprio dati regolamentati (ad esempio informazioni di identificazione personale (PII), sanitarie, finanziarie) o informazioni proprietarie (ad esempio codice sviluppatore).

Soluzione: previeni le fughe di dati con i controlli DLP (Data Loss Prevention). Contrassegna l'utente come rischioso in base a un numero elevato di violazioni DLP e analizza l'attività. Limita o isola l'accesso dell'utente ad altri ambienti con Zero Trust Network Access (ZTNA) o politiche di browser isolation.

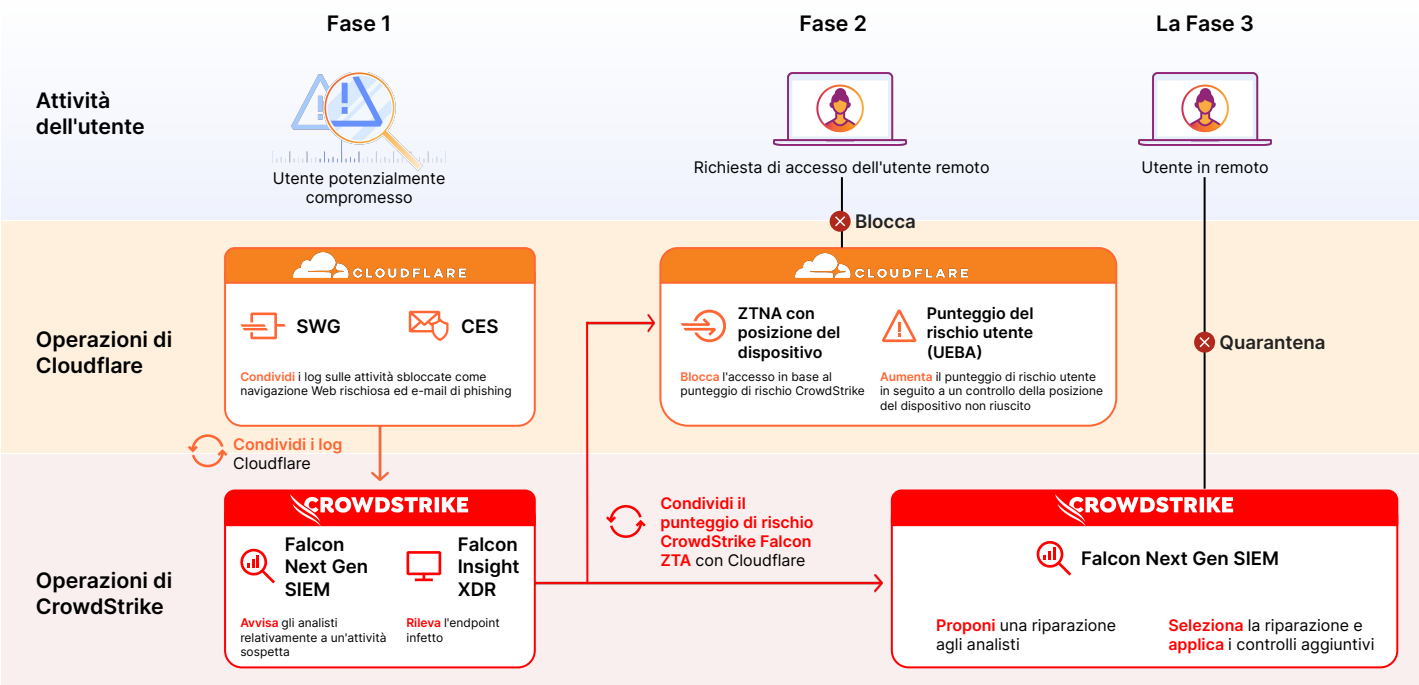
Caso d'uso: Protezione di applicazioni, API e siti Web

Problema: gli autori delle minacce e i bot prendono di mira app, API e siti rivolti al pubblico.

Soluzione: rileva e mitiga payload dannosi, bot e zero-day utilizzando modelli di rischio supportati dal ML come il nostro WAF Attack Score o il punteggio dei bot.
Rivedi potenziali errori di configurazione, rischi di fuga di dati e vulnerabilità che influiscono sull'infrastruttura.

Caso d'uso: Applicazione di Zero Trust con Cloudflare e CrowdStrike

Di seguito è riportato un esempio di flusso di lavoro di come Cloudflare e CrowdStrike lavorano insieme per applicare le politiche Zero Trust e mitigare i rischi emergenti. Insieme, Cloudflare e CrowdStrike si completano a vicenda scambiando dati su attività e rischi e applicando policy basate sul rischio e passaggi di risoluzione.



Fase 1: Analisi automatizzata

Cloudflare e CrowdStrike aiutano le organizzazioni a rilevare che un utente è compromesso.

In questo esempio, Cloudflare ha recentemente bloccato la navigazione Web verso siti Web rischiosi ed e-mail di phishing, fungendo da prima linea di difesa. Tali log vengono quindi inviati a CrowdStrike Falcon Next-Gen SIEM, che avvisa l'analista della tua organizzazione in merito ad attività sospette.

Allo stesso tempo, CrowdStrike Falcon Insight XDR scansiona automaticamente il dispositivo dell'utente e rileva che è infetto. Di conseguenza, il punteggio Falcon ZTA che riflette lo stato di salute del dispositivo viene abbassato.

Fase 2: Applicazione di Zero Trust

Questa organizzazione ha impostato i controlli della postura del dispositivo tramite Zero Trust Network Access (ZTNA) di Cloudflare, consentendo l'accesso solo quando il punteggio di rischio Falcon ZTA è superiore a una soglia specifica da loro definita.

Il nostro ZTNA nega la successiva richiesta dell'utente di accedere a un'applicazione perché il punteggio Falcon ZTA scende al di sotto di tale soglia.

A causa del fallimento del controllo della posizione del dispositivo, Cloudflare aumenta il punteggio di rischio per quell'utente, inserendolo in un gruppo con controlli più restrittivi.

Fase 3: Riparazione

Parallelamente, il SIEM di nuova generazione di CrowdStrike ha continuato ad analizzare l'attività dell'utente specifico e i rischi più ampi in tutto l'ambiente dell'organizzazione. Grazie ai modelli di machine learning, CrowdStrike evidenzia i rischi principali e propone soluzioni per ciascun rischio al tuo analista.

L'analista può quindi rivedere e selezionare le tattiche correttive, ad esempio la messa in quarantena del dispositivo dell'utente, per ridurre ulteriormente i rischi in tutta l'organizzazione.

Impatto sui clienti

Vantaggi	Parametri campione
Riduci gli sforzi in SecOps con meno creazione manuale di policy e maggiore agilità nella risposta agli incidenti	• Aumenta il numero di flussi di lavoro automatizzati • Riduci il numero di clic per creare politiche • Riduci il tempo medio per il rilevamento (MTTD) • Riduci il tempo medio di risposta (MTTR)
Rischio informatico ridotto con l'applicazione automatizzata e dinamica della condizione di rischio su tutta la superficie d'attacco	• Riduci il numero di incidenti critici • Aumenta il numero di minacce bloccate automaticamente

Cosa dicono

"Cloudflare ci aiuta a mitigare i rischi in modo più efficace con meno sforzi e semplifica il modo in cui forniamo Zero Trust nella mia organizzazione".

Anthony Moisant
SVP, Chief Information Officer
e Chief Security Officer, Indeed

Il sito di lavoro numero 1 al mondo con oltre 350 milioni di visitatori unici al mese

"Disporre di un'unica soluzione Cloudflare che ci aiuta a gestire la complessità delle nostre operazioni globali ci ha reso la vita molto più semplice.

Wilson Tang
Direttore dell'ingegneria, Servizi principali della piattaforma, Delivery Hero

Azienda tedesca di ordine e consegna di cibo online che opera in oltre 70 paesi

Leggi il case study

Confronto tra competitor

Sulla base dei dati al 7 maggio 2024

	Cloudflare	Zscaler	Netskope	Palo Alto Networks (Prisma Access)
Valuta il rischio con modelli di punteggio del rischio di prima parte				
Modelli di analisi del comportamento degli utenti e delle entità in tempo reale (UEBA)/punteggio del rischio utente	✅	✅	✅	✅
Accesso ai dati di posta elettronica/rischio di phishing di prima parte	✅	❌	❌	❌
Payload dannoso e rilevamento zero-day tramite WAF	✅	❌	❌	❌
Visualizzazione unica del dashboard per tutti i rischi posti da utenti e app	Lavori in corso all'interno del Centro di sicurezza Cloudflare	✅	La visibilità avanzata della posizione tramite Netskope Cloud deve essere gestita nell'infrastruttura del cliente	Disponibile solo per i rischi relativi all'app e all'utilizzo dell'app
Scambia segnali di rischio con strumenti di terze parti				
Integrazioni con provider Endpoint Protection Platform (EPP) ed Extended Detection & Response (XDR) (ad esempio CrowdStrike, SentinelOne, Microsoft)	✅	✅	✅	✅
Partnership con provider di identità (IDP) e Single SIgn Ons (SSOs) (ad esempio Okta, Ping Identity, Microsoft)	✅	✅	✅	✅
Un'API per tutti i servizi	✅	❌	Funzionalità dell'API Netskope complete disponibili solo con l'intervento dell'assistenza clienti	❌
Configurazione una tantum per integrazioni di terze parti su tutti i servizi	✅	❌	❌	❌
Applica i controlli di rischio				
Crea politiche in base al rischio utente	✅	✅	✅	✅
Un'unica interfaccia di gestione per creare tutte le politiche Security Service Edge (SSE).	✅	❌	✅	✅
Ogni servizio viene eseguito da ogni datacenter.	✅	❌	✅	✅
Copertura dell'intera rete	Più di 320 siti Più di 13.000 punti di peering	70 siti 116 punti di peering	Più di 70 regioni 183 punti di peering	119 on-ramp 47 centri di calcolo
Automazione Terraform	Singolo repository per l'intera piattaforma Cloudflare	19 repository	Nessuna creazione di politiche via Terraform	Richiede più moduli e provider Terraform

Cloudflare fa la differenza

Semplicità della nostra piattaforma unificata

Unifica la gestione della condizione di rischio su un'unica piattaforma che converge i controlli SASE (Secure Access Service Edge) e Web App & API Protection (WAAP).

Interoperabilità illimitata tra i servizi, così puoi iniziare più velocemente e semplificare la gestione continua del rischio.

Orchestra tutti i servizi Cloudflare con la nostra API unica per la personalizzazione e l'automazione con strumenti di infrastruttura come codice come Terraform.

Flessibilità delle nostre integrazioni

Scambia i dati sui rischi con gli strumenti Endpoint Protection Platform (EPP), IDP, XDR e SIEM che già utilizzi per adattarti ai cambiamenti dei rischi in tutta la tua organizzazione.

A differenza di altri fornitori, configura le integrazioni una sola volta e sfrutta tali funzionalità sull'intera piattaforma Cloudflare, in modo da poter estendere i controlli nei tuoi ambienti IT con agilità.

Scala della nostra rete cloud globale senza precedenti

Ogni servizio di sicurezza è disponibile per i clienti in ciascuna delle nostre oltre 320 sedi di rete.

L'ispezione a passaggio singolo e l'applicazione delle policy sono sempre rapide, coerenti e resilienti.

Inoltre, la visibilità unica della nostra rete (che funge da proxy per il 20% del Web e riceve query DNS 3T al giorno) consente ai modelli supportati da IA/ML di difendersi dai rischi emergenti.

Pronto a discutere il tuo approccio alla gestione del rischio?
Richiedi una consulenza

Vuoi saperne di più?
Leggi il nostro blog degli annunci oppure visita il nostro sito Web