CLOUDFLARE

WHITEPAPER

Fare di più con meno

Strategie utili per la sicurezza delle applicazioni e le prestazioni di sette aziende.

Contenuto

Riepilogo

La maggior parte delle architetture IT è troppo complicata o obsoleta per garantire una sicurezza coerente nelle applicazioni Web. I team di sicurezza sono costretti a mettere insieme manualmente strumenti isolati con visibilità limitata e controlli imprecisi in ambienti cloud, ibridi e in locale, rallentando il business.

Tutta questa complessità ha portato a team oberati di lavoro, a un aumento delle vulnerabilità, ad attacchi più dannosi e a un livello insostenibile di risorse solo per tenere il passo con le minacce di ieri.

La protezione delle applicazioni Web e delle API da bot dannosi, attacchi DDoS, code injection e altre vulnerabilità è un compito fondamentale per le organizzazioni. Tuttavia, implementare una solida strategia di sicurezza delle applicazioni può essere impegnativo, soprattutto quando si ha a che fare con budget limitati e crescita limitata del team.

Questo documento condivide storie di vita reale di aziende che sono riuscite a creare efficienze e tagliare i costi nella loro strategia di sicurezza delle applicazioni. Leggendo queste storie di successo, le aziende ottengono preziose informazioni sull'utilizzo delle pratiche di sicurezza delle applicazioni per ottimizzare le spese.

Quando i team di sicurezza e IT devono fare di più con meno

Quando le organizzazioni hanno a che fare con limitazioni del budget, nessun team è completamente immune. A causa dell'ampia incertezza economica, del calo delle vendite, della ristrutturazione organizzativa o di una serie di altri motivi, i team di sicurezza e IT sono spesso costretti a migliorare le operazioni senza la crescita del budget sperata o, peggio, a farlo riducendo contemporaneamente i costi.

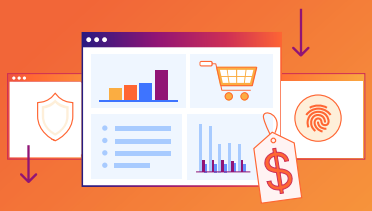
Tuttavia, la sicurezza e le prestazioni delle applicazioni non sono aree che consentono risultati inferiori. Dal punto di vista della sicurezza, la protezione delle applicazioni diventa ogni anno più complicata. Gli attacchi sono più grandi e complessi che mai e, man mano che le organizzazioni crescono, crescono anche le loro superfici di attacco. Ad esempio, c'è stato un aumento del 15% nel numero di CVE comunicati tra il 2022 e il 2023. E mentre nel 2023 sono state rilevate più di 5.000 vulnerabilità critiche, il tempo medio necessario per rilasciare una patch per una vulnerabilità di un'applicazione Web di gravità critica rimane costante su 35 giorni, lasciando l'applicazione non protetta durante quel periodo.

E dal punto di vista delle prestazioni, i consumatori si aspettano che ogni esperienza digitale sia veloce, affidabile e personalizzata. Anche piccoli rallentamenti possono avere un impatto significativo sul coinvolgimento degli utenti e sulle conversioni, lasciando le aziende in asso se non riescono a soddisfare le aspettative dei loro clienti.

Di fronte alla duplice pressione delle limitazioni di budget e delle crescenti aspettative, i team di sicurezza e IT devono trovare il modo di offrire di più con meno. Questo documento esplora le storie di aziende che hanno stabilito in modo efficiente una pratica economicamente vantaggiosa per la sicurezza e le prestazioni delle applicazioni, senza sacrificare i risultati.

Modi per ridurre i costi nella sicurezza delle applicazioni e nelle procedure legate alle prestazioni

Quando si tratta di proteggere le applicazioni Web e le API dalle minacce moderne, la migliore difesa non è solo quella che offre servizi di sicurezza su più livelli, ma quella che consente alle organizzazioni di ridurre le spese non necessarie. Per raggiungere questo obiettivo, le organizzazioni possono utilizzare diverse strategie chiave, tra cui il consolidamento dei fornitori, la gestione semplificata dei certificati, la protezione dedicata dagli attacchi che aumentano i costi del traffico e la riduzione delle tariffe in uscita.



Riduci i costi con il consolidamento dei fornitori di sicurezza

Semplifica i costi di manodopera e infrastruttura con la gestione automatizzata dei certificati

Blocca gli attacchi che fanno aumentare i costi del traffico

Elimina commissioni e costi imprevisti come larghezza di banda, cloud e costi di uscita

Riduci i costi con il consolidamento dei fornitori di sicurezza

Un recente sondaggio di Gartner ha riportato che il 75% delle aziende sta esplorando il consolidamento dei fornitori nelle pratiche di sicurezza. Riducendo il numero di fornitori a cui si appoggiano, le organizzazioni possono ottimizzare i processi della supply chain e ottenere una maggiore efficienza, il che si traduce in una riduzione dei costi.

Chrono24, un mercato online leader per gli orologi di lusso, ha ridotto la propria dipendenza da più fornitori grazie al consolidamento con Cloudflare.

Prima del passaggio, Chrono24 utilizzava una soluzione CDN di EdgeCast e la mitigazione degli attacchi DDoS e un WAF di diversi altri fornitori. Il mix di soluzioni ha funzionato in modo inadeguato, determinando una latenza significativa, prestazioni di sicurezza scadenti e spese inutili per i fornitori.

Dopo il consolidamento con le soluzioni di Cloudflare, tra cui CDN, WAF e mitigazione degli attacchi DDoS, Chrono24 ha registrato una riduzione del 67% dei costi per la sicurezza e le prestazioni del sito Web.

"Il nostro costo base è molto più basso ora che abbiamo consolidato prestazioni e sicurezza sotto un unico fornitore", afferma Sven Ferber, Direttore della tecnologia. "Penso che stiamo spendendo circa un terzo di prima".

Il consolidamento dei fornitori può essere una strategia molto efficace per le aziende per semplificare le spese di acquisto e gestione. Di seguito sono riportate tre domande rapide che puoi utilizzare quando cerchi di consolidare i fornitori:

1. Il tuo fornitore offre protezione dalle minacce e migliora le prestazioni delle app?
2. Puoi gestire le tue applicazioni e API da un'unica console?
3. Più team nella tua organizzazione possono sfruttare lo stesso fornitore per un'efficienza del budget?

Seguendo i suggerimenti di consolidamento sopra riportati, le organizzazioni possono ridurre i costi, semplificare la gestione della catena di fornitura e rafforzare i rapporti con i principali fornitori.

chrono24

Punti chiave

Il **75%** delle aziende sta pensando al consolidamento dei fornitori

Chrono24 ha riscontrato una riduzione del **67%** della sicurezza del sito Web e dei costi IT dopo il consolidamento con Cloudflare

Riducendo il numero di fornitori e consolidando i servizi, le aziende possono **ridurre i costi** e semplificare la gestione della supply chain

Semplifica i costi di manodopera e infrastruttura grazie alla gestione automatizzata dei certificati

L'implementazione delle configurazioni di sicurezza su più domini e aree geografiche può essere un processo costoso e dispendioso in termini di tempo per i team IT. E i costi nascosti possono creare ulteriori grattacapi per le organizzazioni che supportano, in particolare quelle che si trovano a gestire le limitazioni del budget.

Spesso questi costi nascosti sono nascosti nella gestione dei certificati. I certificati SSL/TLS costituiscono l'identità digitale di una rete. In media, la presenza sul Web di un'azienda può richiedere centinaia, se non migliaia, di certificati. Ma la gestione di questi certificati può essere costosa poiché si sommano le spese di manodopera e infrastruttura, per non parlare della perdita di entrate che può derivare da interruzioni impreviste dei certificati.

SHOPPY, una piattaforma di e-commerce, utilizza Cloudflare per automatizzare la gestione dei certificati SSL, inclusa la creazione, la protezione, la convalida del dominio, l'emissione, il rinnovo e la riemissione della chiave privata.

Inizialmente, SHOPPY utilizzava uno strumento di gestione dei certificati gratuito che forniva loro certificati inaffidabili e periodi di validità brevi. Di conseguenza, SHOPPY ha dovuto assumere altri dipendenti per supervisionare la gestione della certificazione e il processo di rinnovo.

Con Cloudflare SSL per SaaS, SHOPPY affida il processo di gestione dei certificati a Cloudflare, richiedendo a un solo dipendente interno di mantenere l'intero processo.

"L'uso dei prodotti Cloudflare ha ridotto i costi del 60% solo per il funzionamento e la manutenzione", ha dichiarato il fondatore e CTO Yuanming Chen.

Anche pratiche inefficaci di gestione dei certificati possono incidere sulle entrate a causa dei certificati scaduti. LendingTree, un mercato di prestiti online, utilizza i certificati TLS di Cloudflare per risparmiare denaro ed evitare interruzioni.

“Abbiamo migliaia di proprietà diverse. Su quella scala, era solo questione di tempo prima di perdere il rinnovo di un certificato", afferma John Turner, responsabile della sicurezza delle applicazioni. “Utilizzando i certificati TLS di Cloudflare, che si rinnovano automaticamente, risparmiamo circa 50.000 dollari all’anno, sia in costi amministrativi che in entrate perse a causa di interruzioni dovute a certificati scaduti”.

Costruire un sistema di gestione dei certificati efficace può anche aiutare a riallocare le risorse in modo appropriato. Fondata in Germania, mogenius, una piattaforma automatizzata che distribuisce applicazioni basate su cloud, automatizza le pratiche di gestione dei certificati con Cloudflare, consentendo all'azienda di dedicare più tempo allo sviluppo del proprio core business.

“Gestire internamente tutto ciò che Cloudflare fa per noi richiederebbe almeno il 20% del nostro tempo." afferma Jan Lepsky, co-fondatore e CPO. **"Con Cloudflare, possiamo concentrarci sull'ottimizzazione delle pipeline di sviluppo e implementazione del cloud per i nostri clienti".**

L'offload della gestione dei certificati è fondamentale per le aziende che cercano di evitare costi nascosti e garantire operazioni aziendali senza intoppi. Pratiche di certificazione inefficienti, manuali o frammentarie portano a costi elevati di manodopera e infrastruttura, mancati guadagni a causa dell'interruzione dei certificati scaduti e allocazione dispendiosa delle risorse.

Implementando la gestione dei certificati con funzionalità come SSL per le certificazioni SaaS o TLS, le aziende possono risparmiare costi significativi e migliorare i profitti.

SHOPYY

lendingtree

mogenius®

Punti chiave

Utilizzando Cloudflare SSL per SaaS, SHOPPY ha ridotto del 60% i costi operativi e di manutenzione

Cloudflare TLS aiuta LendingTree a risparmiare 50.000 dollari all'anno in costi amministrativi e mancati guadagni

Cloudflare consente a mogenius di automatizzare le pratiche di gestione dei certificati, liberando il 20% del tempo da dedicare alla propria attività principale

Blocca gli attacchi che fanno aumentare i costi del traffico

Con l'aumentare dell'utilizzo delle API, aumenta anche la superficie per gli attacchi. Bot dannosi, attacchi DDoS e altre minacce possono compromettere le applicazioni e le API e i dirigenti e i leader tecnici sono consapevoli in modo univoco dell'impatto significativo che tali attacchi possono avere sulle loro attività.

Secondo una stima, l'insicurezza delle API costa alle aziende fino a 75 miliardi di dollari all'anno.

Questi attacchi provocano la sottrazione e uso illecito delle credenziali e gli attacchi DDoS e non solo possono interrompere il servizio per gli utenti legittimi, ma obbligano le organizzazioni a coprire i costi dei picchi di traffico causati dagli attacchi.

LendingTree stava spendendo ingenti somme di denaro con un precedente fornitore di sicurezza che gli addebitava prezzi elevati durante gli attacchi DDoS. Questo modello non solo ha sostenuto enormi costi di eccedenza, ma ha finito per bloccare il traffico legittimo.

"Ogni volta che pubblicavamo un nuovo spot televisivo o una nuova campagna sui social media, le richieste aumentavano oltre il limite arbitrario che il nostro fornitore ci faceva specificare, il che significava che il fornitore interpretava il picco come un attacco DDoS e bloccava il traffico legittimo", aggiunge John Turner, responsabile della sicurezza delle applicazioni. **"Non solo abbiamo perso quei potenziali clienti, ma abbiamo anche perso il denaro che avevamo speso per portarli sul nostro sito e il nostro fornitore ci avrebbe fatturato la protezione da attacchi DDoS".**

Per risolvere queste inefficienze, LendingTree si è rivolta alle funzionalità di gestione dei bot e limitazione della frequenza di Cloudflare. **Nel giro di 48 ore, un attacco a un particolare endpoint API è diminuito del 70% e in meno di cinque mesi, LendingTree ha risparmiato 250.000 dollari bloccando l'abuso degli endpoint API.**

Quando una holding di giochi online, Flutter Entertainment, si rese conto che quasi il 70-90% del suo traffico era dannoso, aveva bisogno di una soluzione per filtrare e bloccare i bot dannosi. Dopo aver implementato la gestione dei bot di Cloudflare, **Flutter ha diminuito il suo traffico dannoso del 90%, risparmiando più di 2 milioni di sterline ogni anno.**

Utilizzando la gestione dei bot e la protezione da attacchi DDoS, le organizzazioni possono prevenire gli attacchi e l'abuso delle API e ridurre le spese relative agli attacchi. Quando si studiano i fornitori di sicurezza, le organizzazioni dovrebbero cercare fornitori che:

- Utilizza il machine learning per impostare limiti di frequenza in base ai dati sul traffico osservati
- Vadano oltre i limiti di velocità basati sulla geografia e sulla posizione IP perché gli attacchi moderni possono aggirare facilmente i limiti IP
- Garantiscano che gli sviluppatori instradino tutto il traffico delle applicazioni Web e delle API pubbliche attraverso un WAF e un gateway API
- Integrino strumenti DDoS, WAF e gateway API per una difesa dalle minacce più stratificata
- Riducano la latenza assicurando che le protezioni siano presenti dove l'azienda serve il proprio traffico
- Offrano una mitigazione DDoS illimitata per eliminare il pagamento di commissioni in eccesso

L'implementazione della giusta strategia di fornitore/sicurezza può comportare risparmi di migliaia, se non milioni, di dollari all'anno.

Flutter™

Punti chiave

È stato scoperto che la mancata sicurezza delle API costa alle aziende **fino a 75 miliardi di dollari l'anno**

L'implementazione dei giusti strumenti di sicurezza delle applicazioni può portare a **risparmi di migliaia, se non milioni, di dollari all'anno**

Con la protezione da attacchi DDoS, LendingTree ha visto un particolare attacco API diminuire del 70% in 48 ore e ha risparmiato 250.000 dollari in meno di cinque mesi fermando gli attacchi

Cloudflare Bot Management ha aiutato Flutter a ridurre il traffico dannoso del 90% e a risparmiare più di 2 milioni di sterline all'anno

Elimina commissioni e costi imprevisti come larghezza di banda, cloud e costi di uscita

Molti servizi di sicurezza dipendono dal cloud e molti fornitori di servizi cloud fanno pagare alle aziende i servizi di archiviazione ed elaborazione. Inoltre, spesso richiedono alle aziende di pagare le tariffe di uscita dei dati, che sono le spese associate al trasferimento dei dati dallo storage.

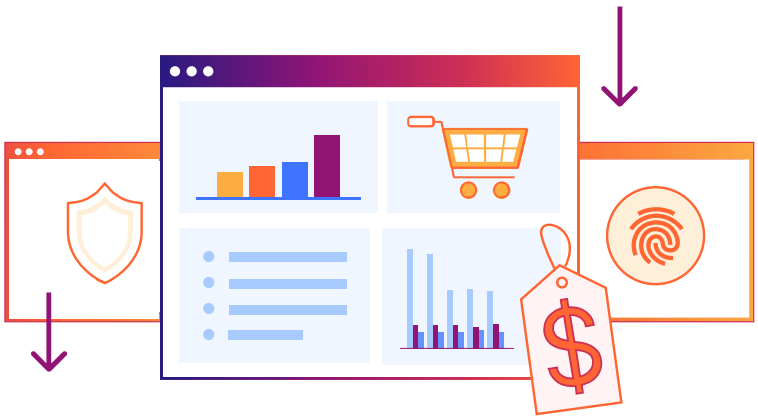
Le tariffe di uscita vengono calcolate in base a molteplici fattori, come il livello del cliente, il tipo di abbonamento e il volume di dati trasferiti. Per questi motivi, queste commissioni tendono ad essere difficili da prevedere, il che può mettere a dura prova le organizzazioni quando iniziano a sommarsi. Infatti IDC stima che gli addebiti in uscita rappresentino almeno il 6% dei costi di archiviazione nel cloud.

Con questo assunto, PagesJaunes, una directory digitale europea e un servizio di ricerca locale, ha deciso di implementare la CDN di Cloudflare per ridurre i costi della larghezza di banda e migliorare la gestione della cache e del DNS.

"Abbiamo subito notato che il traffico assorbito dalla CDN di Cloudflare faceva sì che la nostra infrastruttura fosse meno stressata e più resiliente", insiste Loïc Troquet, Responsabile dell'architettura, delle prestazioni e della sicurezza. **"Il 70% della larghezza di banda non aveva più bisogno di essere servito dall'infrastruttura di Solocal".**

E il risparmio di larghezza di banda si traduce in un risparmio sui costi. Dopo aver adottato CDN, DNS, WAF e i servizi di mitigazione degli attacchi DDoS di Cloudflare, lo strumento di apprendimento e studio online Quizlet **ha risparmiato oltre 10 TB della larghezza di banda totale ogni giorno e ha ridotto di oltre il 50% la bolletta in uscita dalla rete dei servizi Google Cloud.**

L'implementazione di strategie e pratiche di sicurezza delle applicazioni può eliminare costi di uscita imprevisti.



PagesJaunes

Quizlet

Punti chiave

L'implementazione di strategie di sicurezza delle applicazioni come la scelta del giusto fornitore di CDN può eliminare costi di uscita imprevisti

Con il CDN di Cloudflare, PagesJaunes ha ridotto la larghezza di banda del 70%

Quizlet ha utilizzato Cloudflare **per risparmiare oltre 10 TB di larghezza di banda totale ogni giorno** e tagliare di oltre il 50% la bolletta in uscita dalla rete di Google Cloud Services, con un risparmio di migliaia di dollari ogni mese

Semplifica la sicurezza delle applicazioni e taglia i costi con Cloudflare

Con Cloudflare, le organizzazioni possono integrare strategie di sicurezza delle applicazioni per aumentare l'efficienza e semplificare le spese. Il portafoglio integrato di sicurezza delle applicazioni di Cloudflare riunisce la migliore protezione da attacchi DDoS illimitata della categoria, un firewall per applicazioni Web che blocca gli attacchi più avanzati, sicurezza API proattiva, gestione dei bot supportata dall'intelligence sulle minacce e rilevamento avanzato degli attacchi lato client.

Sei interessato?

Contatta Cloudflare oggi stesso

+44 20 3514 6970 | enterprise@cloudflare.com | www.cloudflare.com/it-it/

BDES-5972.2024MAY31