



Come sfatare i 5 miti sulle tecnologie WAF (Web Application Firewall)

Per le organizzazioni che svolgono attività mission-critical online, il WAF (Web Application Firewall) dovrebbe essere la prima linea di difesa per bloccare il traffico dannoso, consentendo al tempo stesso il passaggio del traffico legittimo. La tecnologia WAF è disponibile da molti anni e la definizione originale di WAF è troppo semplicistica per i suoi usi evoluti e moderni. Ciò fa sì che molti leader aziendali e professionisti della sicurezza si aggrappino a concezioni e miti obsoleti.

Questi miti possono portare le organizzazioni a sottovalutare e sottoutilizzare la potenza del WAF che probabilmente è già incluso nel proprio stack, aprendo la porta ai criminali e aumentando il rischio operativo. La necessità di una sicurezza digitale completa della tecnologia WAF continua a crescere. Per migliorare le strategie di sicurezza e sfruttare le più recenti protezioni della tecnologia WAF, dobbiamo prima sfatare i miti più comuni.

Nel 3° trimestre
2023, abbiamo
registrato 9,93
miliardi di attacchi
alle applicazioni web

Nel 3° trimestre
2023, si sono
raggiunti picchi di
circa 327 milioni di
attacchi al giorno

Fonte: Ricerca sulle minacce Akamai

Mito numero 1

I WAF necessitano di costanti aggiornamenti manuali per restare efficaci

Pur essendo vero che gli aggiornamenti più recenti forniscono le protezioni più recenti, ci sono alcuni miti riguardo a questa affermazione che richiedono chiarimenti. Molte organizzazioni oggi dispongono di risorse o competenze di sicurezza insufficienti per aggiornare e ottimizzare continuamente le regole WAF. L'impatto aziendale degli aggiornamenti automatici e adattivi non è solo il risparmio di tempo

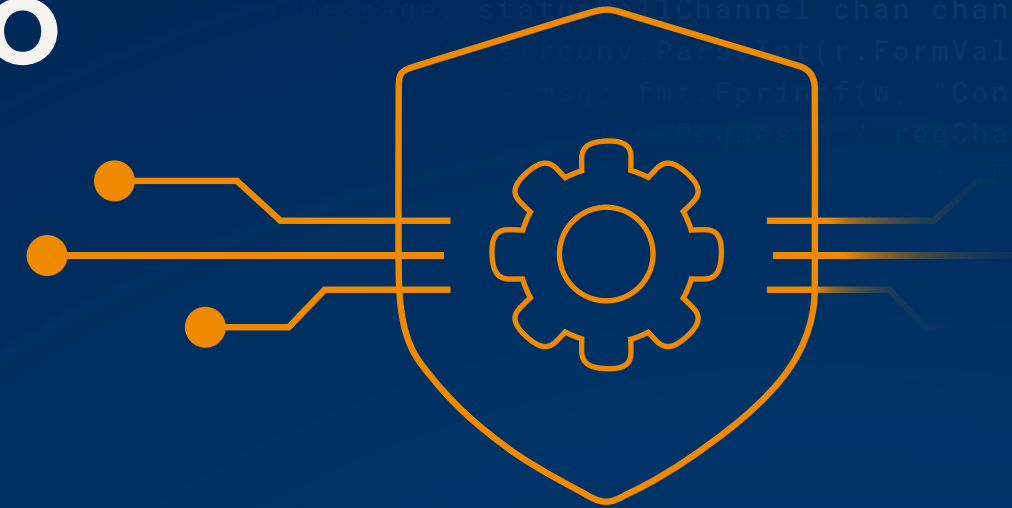
e la facilità d'uso, ma anche la riduzione dei rischi. Quando abbiamo esaminato le aziende che hanno scelto l'aggiornamento manuale, oltre il 77% era in ritardo di cinque o più versioni negli aggiornamenti del set di regole. Akamai invia continuamente e automaticamente gli aggiornamenti WAF, facendo risparmiare tempo all'organizzazione, investimenti in risorse e rischi inutili.

Mito numero 2

I WAF controllano solo il traffico

Un WAF legacy ostacolava il traffico tra gli utenti e un'applicazione web che ispezionava il traffico HTTP rispetto a un elenco definito di regole. In Akamai, la nostra soluzione si è innovata velocemente e rapidamente oltre il tradizionale WAF per fornire più funzionalità e protezioni, tra cui mitigazione DDoS, sicurezza delle API, mitigazione dei bot, rilevamento di malware, rilevamento di dati sensibili e accelerazione delle performance. E con il rilascio di

App & API Protector, la vostra soluzione di sicurezza WAF è ora in bundle con tecnologie ancora più apprezzate dai clienti, tra cui Site Shield, mPulse Lite, EdgeWorkers, Image & Video Manager, API Acceleration e altro ancora. L'esecuzione di una soluzione WAF da parte di Akamai è una tecnologia "molti in uno" che offre ai professionisti della sicurezza visibilità e controlli completi per le protezioni di sicurezza in tutta la struttura.



Mito numero 3

I WAF aumentano i falsi allarmi per gli addetti alla sicurezza

Chiedete a qualsiasi addetto alla sicurezza in prima linea e apprenderete personalmente come i team di sicurezza siano messi a dura prova e sopraffatti dall'enorme volume di avvisi e trigger che devono esaminare, in particolare quelli generati dai sistemi di difesa WAF. Risolvere questo problema è esattamente il motivo per cui Akamai ha sviluppato il nostro [Adaptive Security Engine](#), la tecnologia di base che supporta la soluzione WAF di Akamai. Con [Adaptive Security Engine](#), la vostra organizzazione dispone di una soluzione di protezione moderna resa possibile dalla combinazione di apprendimento automatico, intelligence sulla sicurezza in tempo

reale, automazione avanzata e informazioni di oltre 400 ricercatori sulle minacce di Akamai. Creato per proteggere intere applicazioni web e proprietà API, Adaptive Security Engine è unico perché apprende i modelli di traffico e di attacco specifici per ciascun cliente, analizza le caratteristiche di ogni richiesta in tempo reale e utilizza tali informazioni per intercettare e adattarsi alle minacce future. Affidandosi all'Adaptive Security Engine, gli addetti alla sicurezza possono dire addio ai falsi allarmi, risparmiando tempo prezioso e riducendo il livello di impegno per proteggere le applicazioni e le API.

È stato dimostrato che le raccomandazioni per l'ottimizzazione di Adaptive Security Engine riducono i falsi positivi di

5 volte

Mito numero 4

Regole WAF più personalizzabili offrono una maggiore sicurezza

Più regole possono comportare un maggior numero di operazioni di configurazione, test e analisi. Sebbene più regole non sempre offrano maggiore sicurezza, nemmeno un minor numero di regole apporta sempre maggiore sicurezza. Se siete professionisti della sicurezza che pensano che più equivalga a più, non preoccupatevi. La nostra soluzione WAF viene fornita con regole personalizzate illimitate e i nostri aggiornamenti proattivi e adattivi delle regole vengono forniti indipendentemente dal numero di regole. Con gli aggiornamenti automatici e

l'ottimizzazione automatica, il vostro team può verificare in modo efficiente ed efficace la configurazione WAF su larga scala nell'intero patrimonio digitale. Desiderate aggiungere una nuova regola? La modalità di valutazione consente di valutare l'impatto delle regole nuove e modificate sul traffico in tempo reale, visualizzando immediatamente gli effetti nelle dashboard del portale clienti. Questo stile di test in modalità "shadow" assicura che la nuova regola protegga esattamente come previsto al momento della distribuzione.



Mito numero 5

I WAF sono solo di ostacolo per gli sviluppatori

Gli sviluppatori promuovono il valore riconosciuto dai clienti per le organizzazioni moderne. Se la sicurezza è di ostacolo, l'innovazione rallenta, i cicli di rilascio vengono ritardati e la velocità per ottenere il valore diminuisce. Tuttavia, allo stesso tempo, le versioni non testate potrebbero creare effetti devastanti sulla sicurezza che bloccano le operazioni aziendali. In Akamai sosteniamo i professionisti della sicurezza e gli sviluppatori. Riteniamo che le soluzioni di difesa WAF, quelle che proteggono le app, le API e altro ancora,

possano consentire a una cultura del DevSecOps di promuovere velocità, flessibilità e collaborazione. Ecco perché tutte le nostre funzionalità WAF possono essere gestite tramite un'API AppSec aperta o Terraform che consente al vostro team di automatizzare l'onboarding di applicazioni e API, nonché la gestione delle configurazioni di sicurezza. E quando avete bisogno di un po' di aiuto, Akamai TechDocs offre funzionalità moderne, interattive e intuitive progettate appositamente per gli sviluppatori.

Il contributo di Akamai

Con superfici di attacco in rapida espansione e minacce in continua evoluzione, combinate con criminali altamente motivati, gli addetti alla sicurezza necessitano di visibilità oltre le tradizionali protezioni WAF. Akamai App & API Protector riunisce molte tecnologie leader del settore nelle soluzioni WAF (Web Application Firewall), nella mitigazione dei bot, nella sicurezza delle API e nella protezione DDoS in un unico prodotto. Con App & API Protector, i sistemi di protezione vengono aggiornati costantemente e automaticamente con policy personalizzate tramite una semplice operazione di implementazione. Adaptive Security Engine, la tecnologia alla base della soluzione App & API Protector, fornisce una protezione moderna combinando l'apprendimento automatico, l'intelligence sulla sicurezza in tempo reale, un'avanzata automazione e le informazioni provenienti da oltre 400 ricercatori che si occupano di minacce.

Avviate la [prova gratuita](#) o [scoprite come Akamai protegge](#) le vostre risorse web più critiche per ridurre i rischi e le criticità operative per la vostra organizzazione.