DESCRIZIONE DEL PRODOTTO AKAMAI

App & API Protector

Nel mondo connesso di oggi, la protezione di applicazioni web e API da una vasta gamma di minacce emergenti e in continua evoluzione è fondamentale per il successo di un'azienda. Tuttavia, considerati i processi di migrazione verso il cloud, le moderne pratiche DevOps e la costante evoluzione delle applicazioni, la protezione delle interazioni digitali si scontra con nuove sfide e complessità.

La distribuzione di una soluzione completa per la protezione di applicazioni web e API (WAAP) rafforza la strategia di sicurezza aggiornando i sistemi di protezione in modo adattivo e fornendo preziose informazioni sulle vulnerabilità prese di mira in maniera proattiva.

Akamai App & API Protector riunisce molte tecnologie leader del settore nelle soluzioni WAF (Web Application Firewall), nella mitigazione dei bot, nella protezione delle API e nella difesa dagli attacchi DDoS (Distributed Denial-of-Service) in un unico prodotto. La soluzione App & API Protector è riconosciuta come la principale soluzione WAAP per la sua capacità di identificare e mitigare rapidamente le minacce oltre il WAF tradizionale per proteggere tutto il patrimonio digitale da attacchi multidimensionali. La piattaforma è semplice da implementare e usare, fornisce una visibilità olistica e implementa automaticamente sistemi di protezione aggiornati e personalizzati tramite l'Akamai Adaptive Security Engine.

La potenza della sicurezza adattiva

App & API Protector supera i set di regole con l'Adaptive Security Engine. Con questa tecnologia innovativa, i sistemi di protezione vengono aggiornati costantemente e automaticamente con policy personalizzate tramite una semplice operazione di implementazione. L'Adaptive Security Engine fornisce una soluzione di protezione moderna con la combinazione di apprendimento automatico, intelligence sulla sicurezza in tempo reale, automazione avanzata e informazioni di oltre 400 professionisti della sicurezza e ricercatori sulle minacce. L'Adaptive Security Engine è una tecnologia esclusiva per i seguenti motivi:

- Analizza le caratteristiche di ogni richiesta in tempo reale sull'edge per velocizzare il rilevamento
- Apprende i modelli di attacco tramite i dati ricavati a livello locale e globale per apportare modifiche al sistema di protezione in base alle specifiche esigenze del cliente
- Si adatta alle future minacce per garantire sistemi di protezione aggiornati anche in caso di evoluzione degli attacchi

L'Adaptive Security Engine alleggerisce l'onere associato alle modifiche manuali e dispendiose in termini di tempo con aggiornamenti immediati per un approccio pratico. Al momento del suo lancio, questa tecnologia è riuscita ad aumentare di 2 volte il rilevamento e a ridurre di 5 volte i falsi positivi. I recenti aggiornamenti apportati ai nostri algoritmi supportati dall'apprendimento automatico hanno ridotto i falsi positivi di altre 4 volte. I professionisti della sicurezza possono focalizzarsi maggiormente nell'intento di proteggere e rendere intuitive le operazioni aziendali digitali.

Vantaggi per le aziende

Affidabile rilevamento degli attacchi
Nel mutevole panorama delle minacce, potete migliorare i sistemi di protezione da minacce note ed emergenti, tra cui attacchi DDoS, botnet, attacchi di tipo injection, attacchi alle applicazioni e alle API e molto altro

Un solo prodotto per una maggiore protezione
Sfruttate al massimo gli investimenti effettuati nella sicurezza con una soluzione che include funzionalità WAAP, visibilità e mitigazione dei bot, protezione DDoS, connettori SIEM (Security Information and Event Management), ottimizzazione web, cloud computing, accelerazione delle API e molto altro

Sicurezza pratica
Alleggerite l'onere associato alla manutenzione manuale dispendiosa in termini di tempo con aggiornamenti automatici e consigli proattivi sull'ottimizzazione automatica forniti dall'Akamai Adaptive Security Engine

Facilità di utilizzo
Il design migliorato dell'interfaccia utente semplifica l'onboarding e le operazioni di sicurezza complete con l'ausilio di guide per la configurazione e la risoluzione dei problemi

Visibilità unificata
Potete analizzare l'intero ambito delle metriche di sicurezza in una sola dashboard o nei rapporti di rilevamento proattivi tramite la telemetria condivisa offerta dalle soluzioni per la sicurezza di Akamai

Novità: il motore DDoS comportamentale

Il nuovo motore DDoS comportamentale, basato sull'apprendimento automatico, rafforza e semplifica la difesa dagli attacchi DDoS. I suoi algoritmi di rilevamento basati sulle anomalie e sui comportamenti cercano varie caratteristiche del traffico, come il paese di origine, l'impronta di rete e altri attributi delle richieste HTTPS, per creare sistemi di protezione personalizzati e fornire un approccio pratico nella difesa dagli attacchi DDoS a livello di applicazioni.

L'utilizzo dell'apprendimento automatico da parte del motore DDoS comportamentale migliora l'efficacia e i processi decisionali sulla quantità di traffico per la creazione di standard di riferimento o profili del traffico. Il meccanismo di valutazione per diversi livelli di sensibilità considera la propensione al rischio delle aziende per rilevare gli attacchi e minimizzare i falsi positivi.

App & API Protector supera i set di regole con l'Adaptive Security Engine.

Rilevamento degli attacchi leader del settore: con l'espansione del proprio ambiente digitale, i clienti Akamai registrano un analogo aumento e ampliamento dei sistemi di protezione. Oltre agli aggiornamenti automatici e all'ottimizzazione automatica adattiva che vengono offerte dall'Adaptive Security Engine, App & API Protector fornisce innovativi sistemi apprezzati dagli analisti per il rilevamento di attacchi DDoS, bot, malware e altri vettori di attacco. Verificate i sistemi di protezione di Akamai per contrastare le CVE emergenti e in continua evoluzione con il nostro strumento di ricerca sulle minacce.

Sicurezza delle applicazioni: App & API Protector presenta una suite completa di strumenti di difesa e componenti personalizzabili per consentire di adattare il sistema di sicurezza in uso alle specifiche esigenze aziendali. Funzionalità efficaci, come Client Reputation, elenchi di reti, rilevamento dei nuovi attacchi e molte altre, offrono un vantaggio sui criminali, semplificando, al contempo, le operazioni di sicurezza. Gli avanzati sistemi di difesa a livello di applicazioni della soluzione WAAP di Akamai contrastano gli attacchi DDoS, SQL injection, XSS (Cross-Site Scripting), LFI (Local File Inclusion), SSRF (Server-Side Request Forgery) e altri vettori di attacco.

Protezione DDoS e controlli della frequenza granulari: App & API Protector, riconosciuta come la soluzione di protezione DDoS leader del settore, fornisce una protezione dagli attacchi DDoS su più fronti: inizia a bloccare immediatamente gli attacchi DDoS a livello di rete sull'edge, consentendo di mitigare i rischi e risparmiare sulle risorse, quindi, rileva e mitiga automaticamente i sofisticati attacchi DDoS al livello 7 sull'edge per offrire una protezione pratica e in tempo reale dallo scenario delle minacce DDoS in continua evoluzione. I controlli della frequenza granulari consentono di personalizzare i sistemi di difesa dagli attacchi DDoS per specifici tipi di traffico e profili di attacco.

Visibilità e mitigazione dei bot: potete guadagnare una visibilità in tempo reale sul traffico dei bot accedendo alla directory di Akamai costituita da oltre 1.750 bot noti. Esaminate i dati analitici alterati, prevenite il sovraccarico dei server di origine e create definizioni dei bot personalizzate per consentire l'accesso ai bot di partner e terze parti senza problemi. Estesi controlli dei bot, tra cui il rilevamento dell'impersonificazione del browser, azioni condizionali e sfide crittografiche, sono ora inclusi in App & API Protector.

OWASP Top 10

Akamai mitiga i rischi delle minacce contro le 10 principali vulnerabilità riportate negli elenchi OWASP Top 10 e OWASP API Security Top 10. Scopri come la soluzione App & API Protector e la sicurezza di Akamai possono proteggere i clienti da minacce di vasta portata, comuni o emergenti.

Scaricate il white paper per saperne di più sui sistemi di protezione di Akamai contro le 10 principali vulnerabilità riportate nell'elenco OWASP.

Sistemi di protezione delle API: l'innovativa protezione delle API di Akamai migliora il livello di sicurezza del sistema fornendo visibilità sul traffico legato al patrimonio digitale, rivelando in modo proattivo le vulnerabilità, identificando i cambiamenti ambientali e proteggendo dagli attacchi nascosti. Con le funzioni per le API di App & API Protector, potete:

- Rilevare automaticamente un'ampia gamma di API note, sconosciute e in continua evoluzione all'interno del traffico web, inclusi endpoint, definizioni e profili di traffico
- Registrare facilmente le API rilevate di recente con pochi clic
- Garantire la protezione delle API da attacchi DDoS, attacchi di tipo injection o abuso di credenziali e da episodi di violazione delle specifiche delle API
- Controllare la gestione dei dati sensibili con la funzione di segnalazione delle informazioni di identificazione personale offerta da App & API Protector per garantire la conformità alle normative

Performance e molto altro dalla rete più grande al mondo: la piattaforma di Akamai fornisce ai clienti un vantaggio competitivo grazie alla sua impareggiabile portata globale, offrendo una visibilità in tempo reale su una parte consistente del traffico Internet a livello mondiale. Questa vasta quantità di dati consente ad Akamai di fornire utili informazioni sulle minacce per aiutare le organizzazioni a tenersi al passo con le minacce alla sicurezza in continua evoluzione e a rilevare e mitigare più rapidamente gli attacchi in vari ambienti. La piattaforma offre anche migliori performance e uno SLA con disponibilità del 100%.

Malware Protection: questo componente aggiuntivo può esaminare i file sull'edge prima che vengano caricati per rilevare e bloccare l'accesso di eventuali programmi malware all'interno dei sistemi aziendali con il caricamento di file dannosi. Senza richiedere l'installazione di altre app o una diversa configurazione delle API, potrete evitare di perdere tempo per configurare un livello di protezione singolarmente in ciascun sistema.

Strumento di sicurezza completo e intuitivo: un eccellente strumento di sicurezza funziona solo se viene usato. Akamai si impegna nell'intento di realizzare una piattaforma intuitiva in grado di offrire produttività e solidi sistemi di protezione. Potrete eseguire rapidamente l'onboarding con la nostra funzione Simple Start o applicare i sistemi di protezione alle nuove applicazioni con poche operazioni.

Strumenti di generazione di rapporti, avvisi e dashboard: Web Security Analytics è la dashboard di telemetria dettagliata sugli attacchi offerta da Akamai, che consente di analizzare gli eventi di sicurezza, creare avvisi e-mail in tempo reale tramite soglie e filtri statici e utilizzare strumenti di segnalazione personalizzabili per monitorare e valutare continuamente l'efficacia dei sistemi di protezione in uso sulla piattaforma di Akamai.

Integrazioni DevOps: integrate facilmente il sistema di sicurezza nei workflow DevOps con GitOps, allineandolo allo sviluppo in rapida evoluzione. Le API di Akamai, disponibili tramite CLI o Terraform, consentono una gestione completa di App & API Protector tramite il codice e associano ogni azione disponibile nell'interfaccia utente.

Integrazioni SIEM: nella soluzione App & API Protector, sono anche disponibili API con funzionalità SIEM e sono inclusi automaticamente connettori preintegrati in Splunk, QRadar, ArcSight e molti altri.

Funzionalità incluse: per migliorare la visibilità e le performance, la soluzione App & API Protector ora presenta molti dei prodotti Akamai più apprezzati dai clienti, tra cui:

- Site Shield: impedisce ai criminali di bypassare i sistemi di protezione basati sul cloud e mirare all'infrastruttura di origine
- mPulse Lite: offre una visibilità dettagliata sui comportamenti degli utenti, risolve i problemi legati alle performance in tempo reale e valuta l'impatto sui ricavi derivante dalla trasformazione digitale
- EdgeWorkers: scoprite i vantaggi del computing senza server, tra cui un migliore time-to-market e l'esecuzione della logica il più vicino possibile agli utenti finali
- Image & Video Manager: ottimizzate in modo intelligente immagini e video con la combinazione ottimale di qualità, formato e dimensioni
- API Acceleration: ottimizzate le performance delle API con una semplice gestione degli accessi, la scalabilità per i picchi di domanda e il miglioramento della sicurezza delle API.

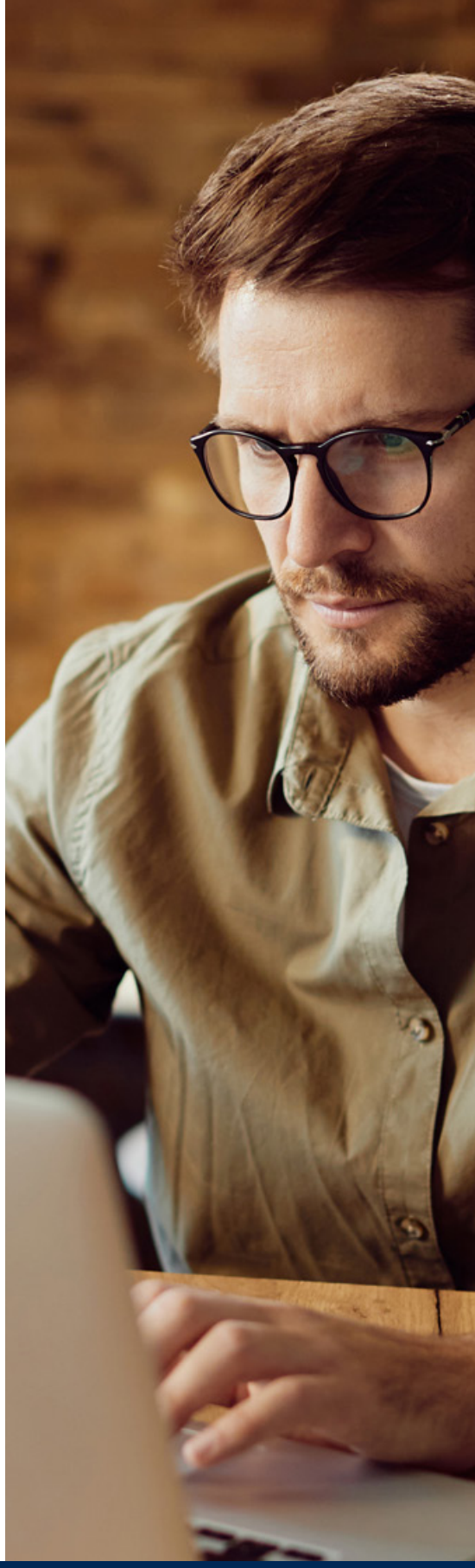
Le soluzioni gratuite potrebbero prevedere restrizioni per l'utilizzo. Contattate Akamai per ulteriori informazioni.

Advanced Security Management

Il modulo opzionale Advanced Security Management offre flessibilità di automazione e configurazione per i clienti con complessi ambienti applicativi ed avanzate esigenze di sicurezza. L'opzione Advanced Security Management include ulteriori configurazioni di sicurezza, policy di velocità e sicurezza, controlli DDoS a livello di applicazione, regole WAF personalizzate, sicurezza positiva delle API e accesso all'intelligence sulle minacce alla reputazione degli IP (Client Reputation) immediatamente disponibili.

Managed Security Service

Il livello di assistenza Standard Support viene offerto a tutti i clienti Akamai 24/7/365. Oltre ai servizi professionali richiesti a scopo di consulenza o per singoli progetti, Akamai offre diversi livelli di servizi gestiti: un servizio WAAP totalmente gestito, un supporto gestito contro gli attacchi e un supporto specializzato fornito dal SOC (Security Operations Center).



Maggiori informazioni su App & API Protector e una prova gratuita della soluzione sono disponibili alla pagina akamai.com/it/aap