Akamai

WHITE PAPER

Dalle soluzioni WAF ai sistemi WAAP: l'approccio di Akamai ad una soluzione olistica per la sicurezza di app e API

Sommario

Introduzione

Considerando la presenza di superfici di attacco sempre più ampie e diversificate, l'aumento dei problemi e dei costi operativi e la continua elusione delle minacce multidimensionali, i team addetti alla sicurezza hanno bisogno di una visibilità in grado di superare le tradizionali soluzioni WAF (Web Application Firewall) e, nello specifico, di strumenti più automatizzati per incrementare l'efficienza, oltre a sistemi di protezione più approfonditi nell'ecosistema delle app e delle API (Application Programming Interface). La terminologia più moderna per questi sistemi di protezione è rappresentata dall'acronimo WAAP (Web Application and API Protection). Le organizzazioni più esigenti che danno priorità alla sicurezza delle loro attività aziendali e alla salvaguardia dei loro clienti richiedono una protezione completa da varie minacce per l'intero patrimonio digitale di cui dispongono. Oltre a proteggere le app da attacchi noti, sconosciuti e zero-day, questi sistemi di protezione includono le seguenti funzionalità:

- Rilevamento adattivo delle minacce
- Aggiornamenti automatizzati delle policy
- Solida difesa dagli attacchi DDoS
- Individuazione e protezione delle API
- Mitigazione e visibilità sui bot
- Semplici integrazioni per i cicli di sviluppo

Questo articolo descrive la tecnologia WAF tradizionale, il passaggio dalle soluzioni WAF ai sistemi WAAP e la continua domanda di innovative soluzioni WAAP da parte del mercato. Akamai è un'azienda leader di fama consolidata nel settore della sicurezza, ambito in cui concentra un approccio di innovazione tecnologica con l'intento di potenziare e proteggere la vita online degli utenti finali.

La definizione tradizionale di soluzione WAF

Una soluzione WAF tradizionale viene posizionata al centro del flusso di traffico che intercorre tra gli utenti finali e un'applicazione web. La soluzione WAF esamina il traffico HTTP crittografato o meno alla ricerca di eventuali attacchi in base ad un elenco di regole specificato.

La maggior parte delle soluzioni WAF si basa su un elenco di regole predefinito per identificare le richieste HTTP dannose che sono inframezzate da traffico HTTP legittimo, allo scopo di proteggere da migliaia di potenziali attacchi noti. Tuttavia, i criminali sfruttano sempre nuovi vettori di attacco o varianti di vettori esistenti in continua evoluzione. Ecco perché una soluzione WAF tradizionale deve aggiornare continuamente le regole impostate per adattarsi alle caratteristiche del traffico legittimo, che sarà diverso a seconda delle applicazioni e dei cambiamenti apportati nel corso del tempo.

Poiché gli utenti finali hanno richiesto un livello maggiore di protezione e performance, le soluzioni WAF hanno ampliato il loro ambito per includere nuove tecnologie e servizi di sicurezza, come le funzionalità di mitigazione dei bot e degli attacchi DDoS (Distributed Denial-of-Service), nonché soluzioni di sicurezza per le API. Questa continua evoluzione giustifica l'adozione di una nuova definizione e di una nuova terminologia.

Le sfide correlate alle soluzioni WAF tradizionali

Le soluzioni WAF, come spesso sostengono le organizzazioni che le hanno implementate, non riescono a soddisfare le loro aspettative iniziali in termini di efficacia, facilità di gestione e impatto sulle applicazioni e sulle API protette. Considerando i problemi legati alle web performance, spesso dovuti al fatto di dover esaminare miliardi di richieste web e API alla ricerca di codice dannoso, le soluzioni WAF, frequentemente, provocano attriti all'interno delle organizzazioni, peggiorano le performance e ostacolano l'implementazione a causa dei protocolli di sicurezza utilizzati.

Tra i problemi di implementazione più significativi che derivano dalle soluzioni WAF tradizionali, figurano i seguenti:

- L'imprecisione nel rilevamento e l'elevato numero di falsi positivi creano troppi avvisi e ulteriori rischi
- Le soluzioni WAF si basano su operazioni manuali di revisione, ottimizzazione e manutenzione
- La mancanza di controlli granulari porta a rigorose policy di rifiuto che interrompono le experience degli utenti finali e i processi aziendali
- Un'intelligence sulle minacce obsoleta aumenta le vulnerabilità
- Il peggioramento delle performance e della copertura causa la presenza di restrizioni e la mancanza di flessibilità
- Scarsa protezione dell'espansione digitale

Le soluzioni WAF tradizionali sono un potente strumento di sicurezza, tuttavia, spesso, possono lasciare le organizzazioni in preda a problemi operativi e rischi non mitigati, che verranno descritti in questo articolo.

Le organizzazioni che cercano di aggiornare la loro tecnologia WAF con una soluzione WAAP devono assicurarsi che questo passaggio riesca ad apportare valore all'azienda insieme ad un solido sistema di sicurezza. Il passaggio dalle soluzioni WAF ai sistemi WAAP combina la potenza offerta dalla protezione con le funzionalità, l'efficienza e la facilità d'uso necessarie per soddisfare le esigenze aziendali, sia per i team addetti alla sicurezza che per altri reparti.

I principi di progettazione dalle soluzioni WAF ai sistemi WAAP

Poiché i prodotti WAF tradizionali si focalizzano sulla creazione di regole per gli utenti finali, i vendor possono creare una soluzione WAF e immetterla sul mercato con relativa facilità, come dimostrato dalla prevalenza dei prodotti commerciali basati sul CRS (Core Rule Set) dell'OWASP (Open Worldwide Application Security Project) con ModSecurity open source.

Per un provider, tuttavia, è difficile progettare una soluzione WAAP completa in grado di:

- Essere implementata online per proteggere applicazioni e API man mano che emergono nuove vulnerabilità
- Tenere il passo con le moderne pratiche di sviluppo delle app
- Fornire livelli ugualmente solidi di difesa dagli attacchi DDoS, mitigazione dei bot, sicurezza delle API e sistemi di protezione delle applicazioni web lato client

Nel momento in cui ci siamo avvicinati alla progettazione della nostra soluzione WAAP, abbiamo voluto che fosse più che "abbastanza buona". La soluzione App & API Protector è stata creata con l'intento di affrontare i rischi per la sicurezza, consentendo alle aziende dei nostri clienti di focalizzarsi sui loro obiettivi più importanti. In base al nostro piano di progettazione, la soluzione WAAP ideale deve essere in grado di fornire:

Una sicurezza efficace
Le applicazioni sono coinvolte in ogni aspetto delle attività aziendali, pertanto la loro protezione dalle minacce è l'obiettivo principale di tutti i team addetti alla sicurezza, che devono riuscire a trovare una soluzione WAAP in grado di fornire le migliori funzionalità di rilevamento possibili. Lo strumento di sicurezza ideale deve considerare prioritaria l'efficacia della funzione di rilevamento, che è l'aspetto più importante di una soluzione WAAP, e deve vantare un'esperienza consolidata nella difesa da attacchi zero-day, exploit e CVE (Common Vulnerabilities and Exposures), nonché un'impeccabile disponibilità continuata nel tempo.

Accuratezza
I team addetti alla sicurezza devono trovare il giusto equilibrio tra la mitigazione dei rischi e la velocità nelle operazioni aziendali. Le soluzioni ideali devono disporre di meccanismi di ottimizzazione automatica in grado di ridurre i falsi positivi senza compromettere le experience degli utenti finali e i processi aziendali.

Moderni sistemi di protezione

Le organizzazioni devono aggiornare i propri sistemi di protezione continuamente (e, spesso, manualmente) in base alle più recenti regole per risolvere le nuove vulnerabilità man mano che vengono individuate. A tale scopo, hanno bisogno di due risorse principali: l'accesso alle informazioni più aggiornate sui vettori di attacco e le competenze dei team addetti alla sicurezza per personalizzare la propria strategia di difesa in modo da mitigare gli attacchi. La soluzione ideale svolge un ruolo di primo piano nella community dell'intelligence sulle minacce e fornisce funzionalità tali da semplificare le operazioni legate alla sicurezza nei sistemi di protezione aziendali.

Capacità di adattamento

Il panorama delle minacce si evolve ad un ritmo rapido. Con gli attacchi basati sull'AI che emergono all'orizzonte, i team addetti alla sicurezza devono essere più efficienti che mai nelle loro attività lavorative. Le soluzioni WAAP ideali devono offrire una combinazione di funzionalità di automazione avanzata, apprendimento automatico e intelligence globale per fornire aggiornamenti automatici e suggerimenti personalizzati sulla modifica delle regole da implementare con un solo clic.

Visibilità

Le soluzioni WAF tradizionali, di solito, inviano un flusso interminabile di avvisi e si affidano agli addetti alla sicurezza per analizzare attentamente ogni avviso urgente tramite le risorse interne. Una soluzione WAAP più efficace fornisce una visibilità basata su più soluzioni e un contesto proattivo sugli attacchi inviando ad un'organizzazione notifiche sul momento, sulla posizione e sul motivo per cui si sono verificati in modo da alleggerire il carico di lavoro che grava sulle loro risorse.

Scalabilità

Una soluzione che non dispone di una scalabilità sufficiente per gestire il traffico in entrata può creare facilmente problemi che aumentano la latenza web e che possono interrompersi in condizioni di carico. Un approccio WAAP efficace consente di scalare in modo semplice e automatico in base alla domanda del traffico e alla variazione degli attacchi nel tempo, fornendo una protezione continua senza interruzioni né riduzione delle performance.

Una facile integrazione
Un'efficace soluzione di sicurezza deve essere integrabile negli strumenti tecnologici attuali, programmabile, semplice da usare e agevole. La soluzione ideale consente ai team addetti alla sicurezza e allo sviluppo di collaborare tra loro.

Supporto
Nei problemi di sicurezza più complessi, le organizzazioni, spesso, sono sovraccaricate dalle competenze e dalle risorse necessarie per fornire una risoluzione tempestiva. La soluzione ideale deve offrire regolarmente opzioni di servizi gestiti oppure on-demand, che possono fornire le competenze e le risorse necessarie per risolvere le situazioni comuni, come attacchi in corso, problemi legati ai servizi, turnazione del personale, lacune di competenze interne, ecc.

Tenendo a mente questi principi di base sulla progettazione, andiamo ad esaminare l'approccio con cui Akamai si è avvicinata alla creazione di App & API Protector, la sua soluzione WAAP principale, cominciando dalla sua tecnologia fondamentale. La nostra soluzione riunisce molti prodotti di sicurezza per risolvere in modo olistico i problemi legati alla protezione delle applicazioni, alla difesa dagli attacchi DDoS volumetrici, alla sicurezza complessiva delle API e al controllo del traffico dei bot.

L'approccio di Akamai alla tecnologia WAAP

Superare i set di regole

Nel passaggio dai principi di progettazione WAF tradizionali alle soluzioni WAAP più moderne ed efficaci, il settore è rimasto focalizzato sull'obiettivo di garantire un'efficace tecnologia di rilevamento e mitigazione.

Akamai ha introdotto la sua soluzione WAF per la prima volta nel 2009 come primo sistema WAF al mondo basato sull'edge. All'epoca, i vendor di soluzioni per la sicurezza offrivano prodotti WAF basati su set di regole statici come base per le loro funzionalità di rilevamento. Akamai si è differenziata dai suoi concorrenti creando un motore proprietario basato su regole e denominato Kona Rule Set, che ha utilizzato un numero ridotto di regole flessibili (anziché regole statiche) insieme ad un modello di valutazione delle anomalie per migliorare l'accuratezza e la visibilità sugli attacchi.

Nel 2017 Akamai ha poi introdotto gruppi di attacchi automatizzati, che hanno eliminato la necessità per le organizzazioni di configurare e aggiornare continuamente le loro regole grazie ai sistemi di protezione gestiti da Akamai. I gruppi di attacchi automatizzati hanno rappresentato una svolta rivoluzionaria, che ha rapidamente consentito a migliaia di policy WAF di clienti Akamai attivi di trarre vantaggio da questo nuovo approccio.

Akamai ha continuato ad evolvere il suo approccio nei confronti della sicurezza delle applicazioni, dando priorità alla protezione combinata di applicazioni e API, incluse le funzionalità di difesa dai bot, con il lancio, nel 2021, di App & API Protector, una soluzione WAAP concepita con l'intento di sostituire Kona Site Defender WAF per le PMI e le grandi aziende internazionali. App & API Protector ha cambiato l'approccio di Akamai alle operazioni legate alla sicurezza modernizzando la tecnologia del motore Kona Rule Set con la soluzione Adaptive Security Engine.

Modernizzare le difese dagli attacchi DDoS a livello di applicazioni superando le limitazioni della velocità

Quando si tratta di attacchi DDoS, la limitazione della velocità è uno strumento efficace e di comprovata validità. Eppure l'aumento di sofisticati attacchi DDoS al livello 7, attacchi multivettore e tentativi di sfruttamento delle API ha reso difficile per i tradizionali sistemi di difesa dagli attacchi DDoS tenere il passo con le nuove minacce. I sistemi di difesa statici, che si basano su soglie stabilite e firme predefinite, sono reattivi e soggetti a falsi positivi, soprattutto considerando il fatto che i criminali mescolano sempre più il traffico dannoso con le richieste legittime. Ecco perché Akamai ha cambiato il suo approccio nei confronti della difesa dagli attacchi DDoS e ha introdotto nuove funzionalità innovative, come URL Protection e Behavioral DDoS Engine.

La funzionalità Behavioral DDoS Engine è un'innovativa aggiunta alla soluzione Akamai App & API Protector, che è stata integrata nell'Adaptive Security Engine come una delle sue tecnologie fondamentali. Insieme, questi motori offrono un'impareggiabile protezione dalle minacce moderne, rendendo Akamai un'azienda leader nelle soluzioni WAAP. Questo approccio basato su due motori distingue Akamai dalla concorrenza per la sua capacità di offrire aggiornamenti automatizzati, funzionalità di ottimizzazione automatica e il rilevamento basato sul contesto per un approccio pratico.

Un'unica soluzione per una protezione completa

Oggi, le innovazioni continuano a ridefinire la sicurezza delle applicazioni con moderne pratiche di sviluppo tramite l'Edge Computing senza server, le architetture basate su microservizi, le applicazioni a pagina singola e i metodi SaaS/IaaS/PaaS/FaaS.

Per proteggere le applicazioni e le API moderne nei complessi ambienti IT, Akamai ha riprogettato la sua tecnologia di sicurezza delle applicazioni con un approccio più adattivo, flessibile e olistico. Nel passaggio dei prodotti WAAP di Akamai da Web Application Protector e Kona Site Defender alla soluzione App & API Protector, è stato incorporato un maggior numero di set di strumenti e funzionalità di sicurezza.

App & API Protector ora offre molti altri miglioramenti in termini di sicurezza, tutti visibili e controllati tramite una sola interfaccia. La soluzione WAAP di Akamai combina i seguenti elementi:

1. Adaptive Security Engine
2. Sicurezza delle applicazioni con controlli granulari
3. Difesa dagli attacchi DDoS, incluso un sistema di protezione dagli attacchi DDoS al livello 7
4. Protezione delle API, incluse le funzioni di individuazione e protezione delle PII
5. Funzionalità di visibilità e mitigazione dei bot
6. Una piattaforma che offre funzioni di scalabilità globale, intelligence sulle minacce e resilienza

Adaptive Security Engine

La soluzione Adaptive Security Engine offre un'innovativa protezione combinando funzionalità di apprendimento automatico (ML), intelligence sulla sicurezza in tempo reale, esperti di cybersecurity e automazione avanzata. Adaptive Security Engine è la tecnologia di base per le funzioni di rilevamento e difesa offerte da Akamai, che fornisce un approccio pratico per proteggere l'intero patrimonio di applicazioni web e API. Inoltre, questo motore si aggiunge alle innovazioni di Akamai fornite nel passaggio dalle soluzioni WAF ai sistemi WAAP, che incorporano soluzioni di sicurezza correlate, come Bot Manager, funzioni di protezione dagli attacchi DDoS, integrazioni del DevOps e molto altro.

Adaptive Security Engine è una tecnologia esclusiva perché apprende i modelli di traffico e di attacco esclusivi per ciascun cliente, analizza le caratteristiche di ogni richiesta in tempo reale e utilizza tali informazioni per intercettare e adattarsi alle minacce future. Inoltre, questa tecnologia usa le stesse informazioni e l'intelligence della piattaforma per ridurre i falsi positivi tramite consigli di ottimizzazione. Questa funzione di ottimizzazione automatica consente ai team addetti alla sicurezza e allo sviluppo di utilizzare facilmente il motore fornendo sistemi di protezione dalle minacce adattivi, oltre ad aggiornamenti proattivi.

Rilevamento adattivo delle minacce

Il motore utilizza un modello multidimensionale di valutazione delle minacce che combina l'intelligence della piattaforma con i dati/metadati di ogni richiesta. Questi dati vengono elaborati con la logica dei processi decisionali per identificare gli attacchi reali in modo accurato.

I rilevamenti adattivi sono particolarmente efficaci nell'identificare attacchi altamente mirati, elusivi e furtivi poiché i criminali sofisticati si impegnano maggiormente e più a lungo nel loro approccio. Mentre i criminali cercano vulnerabilità ed errori di configurazione, Adaptive Security Engine raccoglie e costruisce prove correlate con le loro tattiche per facilitare l'identificazione della cronologia delle attività dei criminali.

Oltre al payload effettivo e alla sua posizione all'interno della richiesta, altri esempi di dimensioni di attacco valutate per ciascun client includono:

- Cronologia della ricognizione e/o degli attacchi (ad es., frequenza, portata, gravità)
- Qualsiasi segno di automazione dannosa e strumenti di attacco
- Correlazione a origini note di traffico generato dagli attacchi

Inoltre, la soluzione Adaptive Security Engine è stata potenziata con due tecnologie proprietarie: Smart Detect, che crea token per l'input in un'impronta digitale per un rilevamento estremamente accurato, e Smart Sniff, che rileva il tipo di contenuto corretto del corpo della richiesta per impedire di manipolare e aggirare il contenuto. I ricercatori delle minacce di Akamai sfruttano i costosi sistemi e le infrastrutture di Akamai per eseguire passivamente nuovi rilevamenti su tutto il traffico in fase di produzione e, quindi, per analizzare tali risultati tramite i modelli di ML.

Aggiornamenti automatici

Oggi, molte organizzazioni non dispongono di competenze sulla sicurezza o risorse adeguate per tenere traccia continuamente delle minacce in fase di evoluzione, per aggiornare le configurazioni e per rieseguire i test sul proprio traffico web allo scopo di ottimizzare le policy adottate. Per rispondere a queste esigenze, Akamai aggiorna continuamente la soluzione Adaptive Security Engine tramite un sistema di test automatici basati sull'AI/ML per tenere conto delle minacce in continua evoluzione, mantenendo, al contempo, un'elevata accuratezza. Questi aggiornamenti, spesso, hanno offerto una protezione dagli attacchi zero-day prima che venissero divulgati.

Esecuzione dei test dei sistemi per garantirne l'accuratezza

L'esecuzione dei test di una soluzione WAAP si basa su una semplice premessa: è necessario eseguire i test di diversi vettori di attacco e fermare gli attacchi web. Tuttavia, bisogna considerare i seguenti fattori:

- Gli ambienti reali sono più complessi degli ambienti di test e, spesso, conducono a falsi positivi e falsi negativi.
- La progettazione di un sistema di test accurato richiede un'ulteriore verifica: bisogna controllare che venga eseguito non solo il rilevamento degli attacchi, ma anche che in questa operazione non vengano creati inavvertitamente falsi positivi o falsi negativi.
- L'esecuzione dei test richiede l'utilizzo di traffico web reale, sia legittimo che relativo agli attacchi.

Gli aggiornamenti di Adaptive Security Engine cono costituiti da più fasi per garantire che il traffico legittimo non venga influenzato in modo negativo:

- Tutti i rilevamenti vengono sottoposti a test in laboratorio utilizzando traffico sintetico per assicurarsi di rilevare correttamente gli attacchi senza introdurre falsi positivi.
- Gli aggiornamenti vengono sottoposti a test utilizzando il traffico live in fase di produzione per garantire che il campione utilizzato sia valido per l'attuale traffico della piattaforma. Questo processo include l'esecuzione dell'aggiornamento in modalità "shadow" sul reale traffico dei clienti. L'esecuzione in modalità "shadow" non influisce sul traffico dei clienti, pur eseguendo i test sull'accuratezza dei sistemi.
- Una volta superata la prima fase dell'aggiornamento, l'apprendimento automatico identifica i modelli o i trigger che potrebbero essere sfuggiti all'analisi degli addetti alla sicurezza, dopodiché il team di ricerca sulle minacce rivede manualmente i risultati.
- Solo dopo aver superato ogni fase di questi controlli, l'aggiornamento può essere implementato su un segmento più grande della rete. Dopo un'implementazione completa, le funzionalità di ottimizzazione automatica eliminano i restanti falsi positivi, specialmente quelli relativi ai modelli di traffico dei clienti.

Ottimizzazione automatica

L'ottimizzazione automatica elimina l'onere di eseguire l'operazione in modalità manuale, che può comportare policy obsolete ed errori umani, garantendo un'experience pratica. Adaptive Security Engine applica l'apprendimento automatico, i modelli statistici e l'euristica a tutti i trigger per ciascuna policy di sicurezza al fine di distinguere in modo accurato tra il traffico degli attacchi reali e quello degli utenti finali identificato erroneamente come attacco. Non si tratta di un generico controllo su tutta la piattaforma che viene applicato solo in fase di onboarding, ma piuttosto di un processo continuo di ottimizzazione che viene eseguito 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, senza richiedere alcuna configurazione o alcun intervento da parte dell'utente finale.

L'ottimizzazione automatica è un processo semplice e agevole. Gli amministratori della sicurezza possono rivedere e accettare facilmente i consigli con un solo clic tramite l'interfaccia utente o possono automatizzare l'operazione con le API AppSec, l'interfaccia della riga di comando (CLI) o Terraform. Per una maggiore trasparenza, un collegamento prefiltrato a Web Security Analytics mostra tutte le richieste considerate falsi positivi e per ogni consiglio di ottimizzazione viene fornita una motivazione.

Flessibilità della configurazione e dell'automazione

Quando un vendor di soluzioni WAAP supera la tradizionale tecnologia basata sui set di regole, la configurazione e l'automazione diventano più flessibili. Adaptive Security Engine offre la possibilità di:

- Disporre di diversi tipi di aggiornamenti WAF (automatici o manuali) per diverse applicazioni e in base ai rischi associati
- Controllare le azioni per gruppo di attacco e fornire le regole necessarie per la personalizzazione se il comportamento delle applicazioni e/o del traffico è insolito
- Configurare condizioni semplici e complesse per le varie caratteristiche delle richieste, come IP, posizione geografica, intestazione, payload, ecc.
- Mitigare in modo proattivo le fonti delle minacce rilevate esaminando app/attacchi WAF sospetti con Penalty Box
- Modificare l'intestazione di debug
- Modificare le impostazioni di registrazione del payload dell'attacco o le dimensioni di ispezione del payload della richiesta
- Eseguire simulazioni dei cambiamenti nella logica del rilevamento per passare gli aggiornamenti in fase di produzione con la massima sicurezza

Verifica reale

La modalità di valutazione fornisce ai clienti di Akamai la flessibilità e la granularità necessarie per la configurazione di specifiche versioni di Adaptive Security Engine e per l'esecuzione di test sugli aggiornamenti o sulle nuove regole/policy. I clienti possono vedere i nuovi aggiornamenti o le modifiche prima di scegliere se attivarle come appropriate o necessarie per l'ambiente delle proprie specifiche applicazioni web. Per un'efficace modernizzazione della sicurezza, Akamai ritiene che i test eseguiti sul traffico in tempo reale consentono di migliorare la sicurezza rispetto ai test condotti sul traffico rilevato in passato. La modalità di valutazione è simile a una regola "shadow", in cui si possono vedere i risultati in tempo reale solo se è stata applicata la policy (senza alcun impatto sugli attuali utenti finali). Le organizzazioni possono scegliere di eseguire questa modalità di valutazione/manuale per minimizzare l'impatto imprevisto sul numero di falsi positivi e falsi negativi.

Integrazione dei sistemi di protezione modernizzati

I team addetti alla sicurezza e DevOps possono anche rendere operativa la sicurezza integrando le chiamate nelle API di Akamai tramite CLI, Akamai Terraform o gli script nella loro pipeline di automazione CI/CD. La flessibilità della configurazione e dell'automazione garantisce che un potente sistema di sicurezza non possa mai ostacolare la velocità dello sviluppo. Queste integrazioni possono:

- Velocizzare l'onboarding delle applicazioni
- Uniformare la gestione delle policy di sicurezza in un'ampia gamma di applicazioni
- Centralizzare l'applicazione della sicurezza in infrastrutture ibride e multicloud
- Migliorare la collaborazione tra i team addetti alla sicurezza e DevOps in un workflow GitOps per una copertura ottimale

Inoltre, il sistema SIEM (Security Information and Event Management) consente di raccogliere informazioni sui problemi di sicurezza che si verificano sulla piattaforma di Akamai. A sua volta, la nostra soluzione di integrazione SIEM offre un modo per distribuire gli eventi SIEM a strumenti analitici on-premise e basati su cloud come Splunk e QRadar, consentendo di incorporare gli eventi di sicurezza di Akamai nell'intera infrastruttura dedicata alla sicurezza e agli eventi in quattro passaggi.

Potete proteggere e controllare i feed di dati con le seguenti funzioni:

- **Filtraggio di eventi**
  La configurazione e le policy di sicurezza vi aiutano a focalizzarvi sulle minacce reali.
- **Conservazione dei dati**
  La funzione di raccolta memorizza i dati per 12 ore così non perderete neanche un evento.
- **Protezione dal sovraccarico del sistema SIEM**
  Nel vostro connettore SIEM, potete definire il numero massimo di eventi di sicurezza recuperati in ciascuna richiesta. per evitare di sovraccaricare l'applicazione SIEM.
- **Intervallo di recupero**
  Potete definire la frequenza con cui i connettori SIEM effettuano una chiamata all'API corrispondente per recuperare i dati sugli eventi di sicurezza.

Sicurezza delle applicazioni e difesa dagli attacchi DDoS

La sicurezza delle applicazioni è un aspetto cruciale della moderna cybersecurity, che garantisce alle applicazioni di rimanere resilienti ad un'ampia gamma di minacce e vulnerabilità. La sua importanza risiede in varie aree principali. L'integrità e la riservatezza dei dati sono fondamentali perché la sicurezza delle applicazioni garantisce la protezione dei dati riservati da tentativi di manomissione e accessi non autorizzati; inoltre, svolge un ruolo essenziale nel garantire la continuità operativa perché protegge le applicazioni da eventuali interruzioni causate da problemi di sicurezza, garantendo così la continua disponibilità di servizi. La sicurezza delle applicazioni è altresì fondamentale perché impedisce di arrecare danni alla reputazione di un'azienda e di minare la fiducia dei clienti. Infine, aiuta le organizzazioni a conformarsi ai requisiti normativi, evitando, pertanto, conseguenze legali e sanzioni finanziarie.

Da un punto di vista funzionale, una soluzione WAAP è progettata per filtrare e monitorare il traffico HTTP tra le applicazioni web e Internet allo scopo di proteggere dai comuni attacchi web come XSS, SQL injection e DDoS.

La soluzione App & API Protector è nota per il suo innovativo sistema di protezione dagli attacchi DDoS, che è stato progettato per contrastare gli attacchi volumetrici concepiti con l'intento di sovraccaricare le risorse prese di mira. La soluzione contrasta gli attacchi DDoS con i seguenti metodi:

- **Mitigazione degli attacchi DDoS basata sull'edge**
  Sfruttando la piattaforma edge di Akamai distribuita a livello globale, App & API Protector può immediatamente bloccare gli attacchi DDoS prima che raggiungano l'origine delle applicazioni. Questo approccio basato sull'edge garantisce una minima latenza e la massima protezione senza influire sulle performance delle applicazioni.
- **Limitazione della velocità**
  App & API Protector include una funzione di limitazione adattiva della velocità per difendere dagli attacchi DDoS distribuiti a livello di applicazioni. Questi controlli possono essere configurati per limitare il numero di richieste in entrata sulla base di vari criteri, tra cui IP, posizione geografica, controlli della reputazione dell'IP, varie intestazioni HTTP e condizioni di corrispondenza.
- **URL Protection con eliminazione del carico intelligente**
  Provate un diverso approccio alla limitazione della velocità: con la funzione URL Protection, potete proteggere la vostra origine da un numero eccessivo di richieste in base al numero accettabile di richieste (n. max di richieste al secondo o RPS) a seconda della capacità dell'origine. Questa funzione è specificamente progettata per proteggere gli URL che richiedono un'elaborazione elevata, gli endpoint delle API, ecc. dagli attacchi DDoS a livello di applicazioni altamente distribuiti.

- **Behavioral DDoS Engine**
  Una novità introdotta nella soluzione App & API Protector, la funzione Behavioral DDoS Engine è un potente strumento per realizzare una strategia di difesa approfondita perché introduce un approccio pratico alla gestione e alla mitigazione degli attacchi DDoS utilizzando l'apprendimento automatica per stabilire standard di riferimento del traffico e per identificare eventuali anomalie rispetto alla norma. Il motore funziona mediante la comprensione dei modelli di traffico in continua evoluzione e consente agli utenti di definire come il sistema deve reagire alle varie anomalie senza impostare soglie esplicite, riducendo il carico operativo legato alla gestione e all'ottimizzazione del sistema.

- **Aggiornamenti automatici e ottimizzazione automatica adattiva**
  Tramite la strategia di Akamai basata su due motori (Adaptive Security Engine e Behavioral DDoS Engine), la soluzione App & API Protector si adatta continuamente alle nuove minacce tramite gli aggiornamenti automatici e all'ottimizzazione automatica basata sull'apprendimento automatico per ridurre il carico operativo.

Behavioral DDoS Engine: come funziona

Il fulcro della funzionalità Behavioral DDoS Engine è rappresentato da un avanzato modello di ML progettato per monitorare continuamente il traffico in tempo reale, stabilendo gli standard di riferimento per i comportamenti normali e rilevando immediatamente eventuali deviazioni che possono indicare un attacco. Analizzando i modelli di traffico in più dimensioni dinamiche, come l'origine del paese, i modelli TLS, l'IP e i fingerprint TLS, questo motore riesce ad identificare tempestivamente le anomalie e ad intervenire prontamente.

Tra i componenti principali della funzionalità Behavioral DDoS Engine, figurano i seguenti:

- **Monitoraggio dei comportamenti in tempo reale**
  Il motore analizza continuamente il traffico per stabilire gli standard di riferimento per le attività normali e rileva immediatamente eventuali deviazioni che possono indicare un attacco DDoS.

- **Apprendimento automatico per una maggiore precisione**
  Gli avanzati modelli di ML consentono al motore di identificare anche le minime anomalie presenti nei modelli di traffico, garantendo una mitigazione accurata senza bloccare i legittimi utenti.

- **Mitigazione proattiva**
  Sfruttando le informazioni sulla rete globale di Akamai (1056 TB di traffico al giorno), il motore riesce a prevedere e a neutralizzare gli attacchi, spesso prima che possano influire sulle attività aziendali.

- **Analisi multidimensionali**
  Il traffico viene valutato rispetto a più dimensioni, tra cui IP, paese e modelli TLS, per fornire una solida protezione personalizzata in base alle esigenze di ciascuna applicazione

Architettura avanzata per una difesa superiore
Behavioral DDoS Engine si basa su una sofisticata architettura che include vari componenti critici:

- **Motore di rilevamento**
  Utilizza dimensioni dinamiche e i dati cronologici sugli attacchi per identificare gli attacchi DDoS in tempo reale.
- **Motore di mitigazione**
  Contrasta automaticamente gli attacchi utilizzando le informazioni ricavate dallo strumento di generazione degli standard di riferimento e dai segnali relativi alle minacce, riducendo i costi operativi per i team addetti alla sicurezza.
- **Riduzione del disturbo e dei falsi positivi**
  I modelli di ML eliminano i dati irrilevanti, garantendo che venga usato solo traffico "pulito" per le operazioni di analisi e mitigazione.
- **Strumento di generazione degli standard di riferimento**
  Ridefinisce continuamente i profili del traffico elaborando dati puliti per un periodo di due settimane, consentendo al motore di tenersi aggiornato con le strategie di attacco più recenti.
- **Strumento di convalida degli standard di riferimento**
  Supportato dall'intelligenza artificiale, questo componente cruciale valuta centinaia di attacchi DDoS al mese per ottimizzare la soluzione.

Questo strumento automatizzato garantisce ai team addetti alla sicurezza di potersi basare sul motore per adattare in modo dinamico i sistemi di difesa senza richiedere un intervento manuale. La soluzione rileva le attività che segnalano la presenza di traffico anomalo, come il traffico generato dai bot o i tentativi di attacchi DDoS, e le elimina per proteggere le applicazioni in modo efficace.

Accuratezza nella sicurezza delle applicazioni

Una soluzione per la sicurezza delle applicazioni (WAF o WAAP) non accurata richiede un maggior numero di risorse interne per gestire l'aumento nel numero di avvisi generati ogni giorno. La mancanza di accuratezza può portare ad un elevato numero di falsi positivi (in cui una richiesta viene segnalata erroneamente come dannosa) e di falsi negativi (in cui una richiesta viene segnalata erroneamente come non dannosa), sprecando importanti competenze per la sicurezza e tempo prezioso per la ricerca e l'analisi di questi tipi di avvisi.

Spesso, le organizzazioni devono affrontare il problema di un eccessivo numero di avvisi, ma rimangono senza una soluzione a causa dei troppi controlli o funzionalità che eseguono correzioni in modo esagerato o limitato, arrivando ad interrompere la loro soluzione WAF o, peggio, ad ignorare gli avvisi e gli aggiornamenti delle versioni. Anche se, in tal modo, molte organizzazioni evitano di bloccare accidentalmente gli utenti legittimi, ne risulta che gli attacchi web e alle API hanno meno probabilità di essere protetti. Inoltre, molte organizzazioni non dispongono di controlli granulari in grado di bilanciare l'accesso al traffico legittimo e di bloccare il traffico dannoso con precisione.

Il vantaggio derivante da un'efficace soluzione WAAP consiste nella sua capacità di ridurre i falsi positivi e i falsi negativi per incrementare la precisione e minimizzare l'impatto sugli utenti legittimi con una serie completa di funzionalità e controlli WAAP.

Che cos'è l'accuratezza?

L'accuratezza misura la capacità, da parte di una soluzione WAF o WAAP, di bloccare simultaneamente gli attacchi senza bloccare inavvertitamente gli utenti legittimi, considerando le seguenti quattro variabili:

- **Veri positivi (TP):** attacchi reali che vengono correttamente identificati come dannosi
- **Falsi positivi (FP):** richieste legittime che vengono erroneamente identificate come dannose
- **Veri negativi (TN):** richieste legittime che transitano nell'applicazione
- **Falsi negativi (FN):** attacchi reali che transitano erroneamente nell'applicazione

I punteggi di Client Reputation

Client Reputation utilizza un sofisticato motore di analisi dei rischi per elaborare una serie di "punteggi di rischio" per ogni indirizzo IP che tenta di accedere al vostro sito. Questa soluzione analizza gli indirizzi IP in entrata utilizzando vari fattori, come la persistenza dei criminali, il numero di applicazioni prese di mira, la gravità dell'attacco, la portata, il settore e gli attacchi precedenti che hanno colpito le applicazioni di un cliente per stabilire un punteggio di probabilità relativo al possibile coinvolgimento in un attacco web di un dato indirizzo IP tra cui:

- **DOSATCK**
  Questo strumento utilizza le botnet per sferrare attacchi DoS (Denial-of-Service). L'obiettivo di un attacco DoS è "inondare" un sito con un numero di richieste fittizie talmente elevato da renderlo lentissimo o, persino, da bloccarlo. In un attacco DDoS (Distributed Denial-of-Service), queste richieste provengono da migliaia di posizioni (di solito, telefoni o computer infettati da malware), rendendo impossibile fermare l'attacco semplicemente bloccando uno specifico indirizzo IP.

- **SCANTL**
  Gli strumenti di scansione possono identificare potenziali rischi per la sicurezza, come attacchi SQL injection, attacchi CSRF (Cross-Site Request Forgery), reindirizzamenti non validi e altre vulnerabilità. Eseguire uno strumento di scansione web del vostro sito è una buona idea, mentre non si può dire lo stesso se la medesima operazione viene eseguita da un criminale.

- **WEBATCK**
  Questo strumento utilizza tecniche come gli attacchi SQL injection, RFI (Remote File Inclusion) o XSS (Cross-Site Scripting) per eseguire varie operazioni dannose, come installare malware o rubare i dati degli utenti. Un hacker potrebbe riuscire a recuperare tutti i dati dei vostri utenti, tra cui password, numeri di carte di credito e codici fiscali, insieme ad altre informazioni memorizzate nel database degli utenti.

- **WEBSCRP**
  Questa tecnologia utilizza strumenti automatizzati per scaricare una copia di una pagina web per poi "esfiltrare" (ossia, copiare) tutti i suoi contenuti in modo da poterli riutilizzare per scopi illegali o immorali.

Con Client Reputation, potete proteggere la vostra organizzazione in modo proattivo da minacce sospette in base all'intelligence sulle minacce cumulative che viene fornita dall'Akamai Connected Cloud.

Protezione dai malware

I criminali utilizzano, comunemente, i malware come tattica di attacco. Per una protezione completa delle applicazioni, Akamai dispone di una soluzione in grado di proteggere dai malware. Le organizzazioni di tutte le dimensioni consentono di caricare file per una maggiore efficienza interna ed esterna, inclusi i seguenti casi di utilizzo comuni:

- Curriculum vitae per domande di lavoro
- Contratti dei dipendenti, accordi di onboarding, E-Verify, richieste di accreditamento diretto e molto altro
- Domande di vario tipo, tra cui prestiti, richieste di account e crediti
- Preventivi di assicurazione o riparazione per auto, abitazioni e molto altro
- Dati sanitari per la stipula di assicurazioni o la configurazione degli account dei pazienti
- Recensione di prodotti o experience da parte dei clienti con immagini

La protezione dai malware nell'ambito della sicurezza di app e API consente di rilevare e isolare i malware sull'edge prima che raggiungano il sistema aziendale che hanno preso di mira. Le organizzazioni possono proteggere il tempo, i budget e la produttività dell'azienda, nonché i loro dati interni e quelli dei loro clienti, aggiungendo anche una serie di vantaggi derivanti dalla protezione dei malware per app e API:

- **Rilevare e bloccare il malware sull'edge**
  Evitate i rischi della scansione sui server, dove il malware potrebbe essersi già diffuso al momento della scansione.
- **Evitare le complessità e liberare tempo per le risorse**
  Eseguite la scansione dei file solo una volta, invece di impostare la protezione in ciascun sistema singolarmente, come con ICAP e scanner basati su agenti.
- **Scalare il sistema di sicurezza per favorire la crescita aziendale**
  Scegliendo un approccio preventivo e su più livelli, le organizzazioni possono scalare il proprio sistema di protezione man mano che l'azienda cresce, con una protezione aggiuntiva sull'edge e la possibilità di eseguire nuovamente la scansione all'origine.
- **Fornire coerenza alle applicazioni**
  Le aziende non devono configurare o modificare il codice delle applicazioni. Il sistema di protezione dai malware viene ospitato completamente sull'Akamai Connected Cloud.

Analisi della sicurezza delle applicazioni

Inclusa in App & API Protector, è la funzione più amata (e utilizzata) di Akamai: Web Security Analytics. Questa soluzione WAAP di Akamai consente di acquisire i problemi di sicurezza riscontrati nelle applicazioni web e nelle API sulla piattaforma di Akamai e di visualizzarli negli strumenti di analisi della sicurezza disponibili.

Web Security Analytics è un componente vitale della cybersecurity moderna perché offre informazioni complete sul traffico web e sulle potenziali minacce. Analizzando una gran quantità di dati, tra cui modelli del traffico, comportamenti degli utenti ed eventi di sicurezza, fornisce una visibilità dettagliata sul livello di sicurezza delle applicazioni web. Questo approccio proattivo consente alle organizzazioni di rilevare e rispondere alle minacce in modo più efficiente, mitigando i rischi prima che possano causare danni significativi. Web Security Analytics non solo aiuta ad identificare le attività dannose, come attacchi bot, attacchi SQL injection e attacchi XSS (Cross-Site Scripting), ma contribuisce anche a comprendere e a risolvere le vulnerabilità presenti nelle applicazioni web. Inoltre, la soluzione supporta le attività di conformità generando rapporti che dimostrano se l'azienda soddisfa le policy di sicurezza e i requisiti normativi.

Individuazione e profilazione delle API

Le API consentono alle organizzazioni di creare web e mobile experience spesso rendendo visibili i dati e la logica di back-end per sviluppare prodotti nuovi e avanzati. Le API, inoltre, espandono la superficie di attacco. Le organizzazioni hanno bisogno di capire quali endpoint delle API si trovano nel loro ambiente, le funzioni delle API e i loro profili di traffico. La funzionalità di individuazione e profilazione delle API di Akamai esegue tutte queste operazioni e molte altre, in modo automatico e continuato.

La funzionalità di individuazione delle API avvisa i team addetti alla sicurezza in caso di nuove app e API spesso non protette, che sono connesse da vari segmenti aziendali. Questa tecnologia di rilevamento automatizzata è una nuova funzione della soluzione WAAP di Akamai, che consente di tenere allineati tra loro i team addetti allo sviluppo e alla sicurezza insieme ai responsabili dei loro segmenti aziendali.

Adaptive Security Engine rileva automaticamente le API ogni 24 ore sulla base di un meccanismo di valutazione che considera il tipo di contenuto della risposta, le caratteristiche del percorso e i modelli di traffico. Tra i dati rilevati, figurano informazioni sulle specifiche delle API osservate, come:

- Nome host
- Percorso base
- Percorso risorsa
- Parametri e relativo tipo di dati
- Metodi
- Formato delle API

I percorsi di base e delle risorse sono stabiliti tramite un algoritmo che considera vari fattori, come la profondità del percorso dell'account, il numero di figli e i fratelli rilevati nel traffico osservato su uno specifico nome host con il traffico delle API. All'interno del percorso delle risorse, un parametro viene contrassegnato, se osservato per un metodo specifico, e viene identificato il tipo di dati ad esso corrispondente.

Il profilo del traffico relativo agli endpoint delle API contiene informazioni approfondite sullo scopo delle API e sul loro livello di rischio, tra cui:

- Numero totale di richieste effettuate dalla prima individuazione delle API, sia nelle ultime 24 ore che nel corso del tempo
- Data in cui le API sono state individuate per la prima e per l'ultima volta
- Numero di richieste effettuate tramite diversi metodi, come GET, PUT, POST, DELETE e OPTIONS
- Numero di richieste che hanno generato 2, 3, 4 e 5 risposte
- Identificazione del client finale in base all'user agent
- Errori nelle risposte come la percentuale del traffico che ha determinato errori nel client e nel server
- Attacchi provenienti da autori noti, inclusa la percentuale del traffico totale proveniente da autori di attacchi noti sulla piattaforma di Akamai, divisi per autori di attacchi web/DoS, scanner web e scraper

La protezione delle API può rappresentare un ostacolo significativo se non si dispone di un'adeguata visibilità. Come fa un'organizzazione a proteggersi da ciò che non vede? Con Akamai, le aziende possono effettuare automaticamente il rilevamento e la profilazione delle API, inclusi i relativi endpoint, definizioni e caratteristiche di risorse e traffico. Una volta identificate le API, Akamai fornisce un'ampia protezione contro gli attacchi DoS, di tipo injection e per l'abuso di credenziali, nonché dai tentativi di violazione delle specifiche delle API. L'approccio di Akamai indipendente dal cloud e dall'origine consente di individuare facilmente le API nell'intero patrimonio delle applicazioni senza richiedere un'ulteriore configurazione all'utente finale. Questa visibilità consente a sviluppatori, proprietari di applicazioni e team addetti alla sicurezza di tenersi aggiornati con tutti i tipi di API (nuove, sconosciute o in evoluzione) e di registrarle facilmente per proteggerle.

Visibilità e mitigazione dei bot

Poiché i bot contribuiscono a più della metà del traffico di un sito web, può risultare difficile sapere quali bot aiutano le organizzazioni a raggiungere i propri obiettivi e, invece, quali hanno scopi dannosi. I bot legittimi migliorano l'efficienza di un'organizzazione perché automatizzano le operazioni di valutazione, le conversazioni o i consigli. I bot dannosi possono ostacolare i percorsi del traffico e influire sulle experience di clienti e operazioni, influendo negativamente sui profitti. All'interno della soluzione App & API Protector, la funzione di visibilità e mitigazione dei bot offre potenti sistemi di rilevamento per individuare quali sono i bot legittimi per farli passare e quali sono, invece, i bot dannosi per bloccarli. In tal modo, le organizzazioni possono:

- **Individuare i bot e capire l'impatto esercitato**
  La visibilità sul traffico dei bot è fondamentale per le moderne aziende digitali, considerando l'uso diffuso dei bot per operazioni come la ricerca, il controllo delle performance dei siti e l'interazione con i partner aziendali.
- **Migliorare il controllo operativo**
  Bloccare i bot dannosi consente di migliorare l'efficienza, ridurre i rischi aziendali e finanziari e controllare i costi dell'IT in modo più accurato.
- **Prendere decisioni migliori e basate sui dati**
  L'analisi e i rapporti dettagliati vi aiutano a fare scelte creative ed efficaci sui percorsi dei clienti, la strategia di sicurezza, la tolleranza ai rischi e le operazioni IT.

Funzionalità di visibilità e mitigazione dei bot incluse nella soluzione App & API Protector

App & API Protector offre funzioni di rilevamento e controllo del traffico dei bot per individuare quelli che possono influire negativamente sulle performance e sulla sicurezza delle proprietà web. La soluzione fornisce una visibilità tempestiva per monitorare in modo proattivo eventuali anomalie e minacce correlate ai bot che possono svilupparsi nel tempo.

L'utilizzo della soluzione di Akamai contro i bot inclusa in App & API Protector consente di:

- Accedere ad oltre 1700 bot definiti, che sono noti ad Akamai
- Ottenere visibilità sul traffico dei bot in tempo reale
- Creare definizioni dei bot personalizzate
- Accettare i bot legittimi e rifiutare i bot dannosi
- Comprendere la visibilità dei bot e i rapporti sulle tendenze

Per siti con problemi avanzati di bot, Akamai offre Bot Manager, che include innovativi sistemi di protezione dai bot per migliorare la sicurezza nell'e-commerce e nelle aziende digitali. Bot Manager fornisce azioni di risposta sfaccettate per bot persistenti e dannosi come quelli utilizzati in attacchi, come:

- Credential stuffing
- Furto di inventari
- Scraping di contenuti e prezzi
- Abuso della logica aziendale

Le principali funzionalità contro i bot

Akamai soddisfa le crescenti esigenze legate alla gestione dei bot tramite la tecnologia WAAP, migliorando i propri strumenti di visibilità e mitigazione dei bot per includere nuove funzionalità integrate, come:

- **Rilevamento dell'impersonificazione del browser**
  Questa apprezzata funzione di Akamai Bot Manager, inclusa nella soluzione App & API Protector, utilizza modelli di valutazione dinamici e l'apprendimento automatico per individuare e contrastare le attività dei bot all'interno del browser.
- **Azioni di risposta condizionali**
  Ora i clienti possono comprendere meglio le attività dei bot che si verificano all'interno del browser e rispondere con azioni condizionali per applicare diverse strategie di risposta contro i bot dannosi.
- **Azioni di sfida**
  I bot vengono mitigati con una serie di diverse azioni di sfida, incluse sfide interstiziali che, se non risolte, consentono di bloccare l'accesso ai contenuti.

Più di un semplice sistema WAF: i vantaggi della soluzione di Akamai

L'approccio di Akamai alla tecnologia WAAP si è tradotto nella soluzione App & API Protector, che, tuttavia, è più di un semplice prodotto da cui possono trarre vantaggio i nostri clienti WAAP. Costruita sulla piattaforma più distribuita al mondo e creata dal lavoro di centinaia di esperti di minacce, l'Akamai Connected Cloud offre un eccellente livello di performance, disponibilità, intelligence, competenze e sicurezza.

Intelligence e rilevamento delle minacce

Disporre di solide funzionalità di intelligence sulle minacce in-house migliora la capacità di rispondere alle minacce in continua evoluzione per un vendor di soluzioni WAAP. Tuttavia, la qualità, la tempestività e la facilità d'uso dell'intelligence stabilisce il tipo di impatto esercitato sull'efficacia della sicurezza delle applicazioni. Akamai analizza continuamente i dati disponibili tramite l'Akamai Connected Cloud per identificare le tendenze correnti nel panorama delle minacce, i nuovi vettori di attacco non appena vengono individuati e i criminali attualmente attivi. Akamai, quindi, incorpora queste informazioni nelle sue soluzioni WAAP in vari modi.

Akamai Adaptive Security Engine, che abbiamo descritto prima in questo articolo, combina due livelli di approfondite informazioni sulle minacce per creare un motore potente e proprietario allo scopo di gestire automaticamente i più recenti sistemi di protezione per i nostri clienti. Oltre all'adozione dell'apprendimento automatico e all'adozione di regole automatizzate, la soluzione Adaptive Security Engine integra le informazioni sulle minacce ricavate dalla piattaforma globale di Akamai e un consistente team di esperti ricercatori sulle minacce.

L'intelligence della piattaforma di Akamai

Disporre di una delle più grandi piattaforme globali fornisce ad Akamai la possibilità di analizzare il traffico degli attacchi su scala globale per ogni cliente di Akamai in modo tempestivo. Il nostro database dell'intelligence include una media di 1056 TB di attacchi al giorno e sfrutta la visibilità di Akamai sul traffico web di migliaia tra le aziende online più grandi, trafficate e attaccate per acquisire dati rilevanti e di alta qualità che vengono analizzati dall'Akamai Threat Research Team:

- **Trigger WAAP**
  I dati vengono acquisiti direttamente dalle implementazioni WAAP globali di Akamai per catturare i reali attacchi che prendono di mira i clienti delle soluzioni per la sicurezza di Akamai.
- **Registri CDN**
  Vengono incorporate le analisi offline eseguite sui registri degli eventi di ogni cliente di Akamai, inclusi quelli che non hanno implementato una soluzione WAAP.

Il database dell'intelligence di Akamai contiene uno dei più grandi dataset al mondo (9 PB). Per le organizzazioni che danno priorità alla sicurezza delle loro aziende e dei loro clienti, l'intelligence sulle minacce di Akamai influisce sui provider di soluzioni WAAP.

Ricerca sulle minacce e risposta agli incidenti

Le organizzazioni che si occupano di ricerca sulle minacce e risposta agli incidenti forniscono informazioni e analisi utili per completare e ampliare la copertura dagli attacchi offerta da una soluzione WAAP. Akamai utilizza più team con diversi obiettivi per supportare i clienti delle proprie soluzioni WAAP, nonché per identificare i nuovi vettori di attacco che potrebbero richiedere ulteriori sistemi di protezione.

Ricerca sulle minacce

L'Akamai Threat Research Team esegue regolari analisi delle tendenze degli attacchi web per tutti i clienti di Akamai, nonché analisi personalizzate per i singoli clienti, in base alle necessità. Inoltre, il team progetta e implementa l'euristica per eseguire query su informazioni utilizzabili in modo da supportare la creazione e gli aggiornamenti alla logica delle regole WAF e a Client Reputation.

Risposta agli incidenti

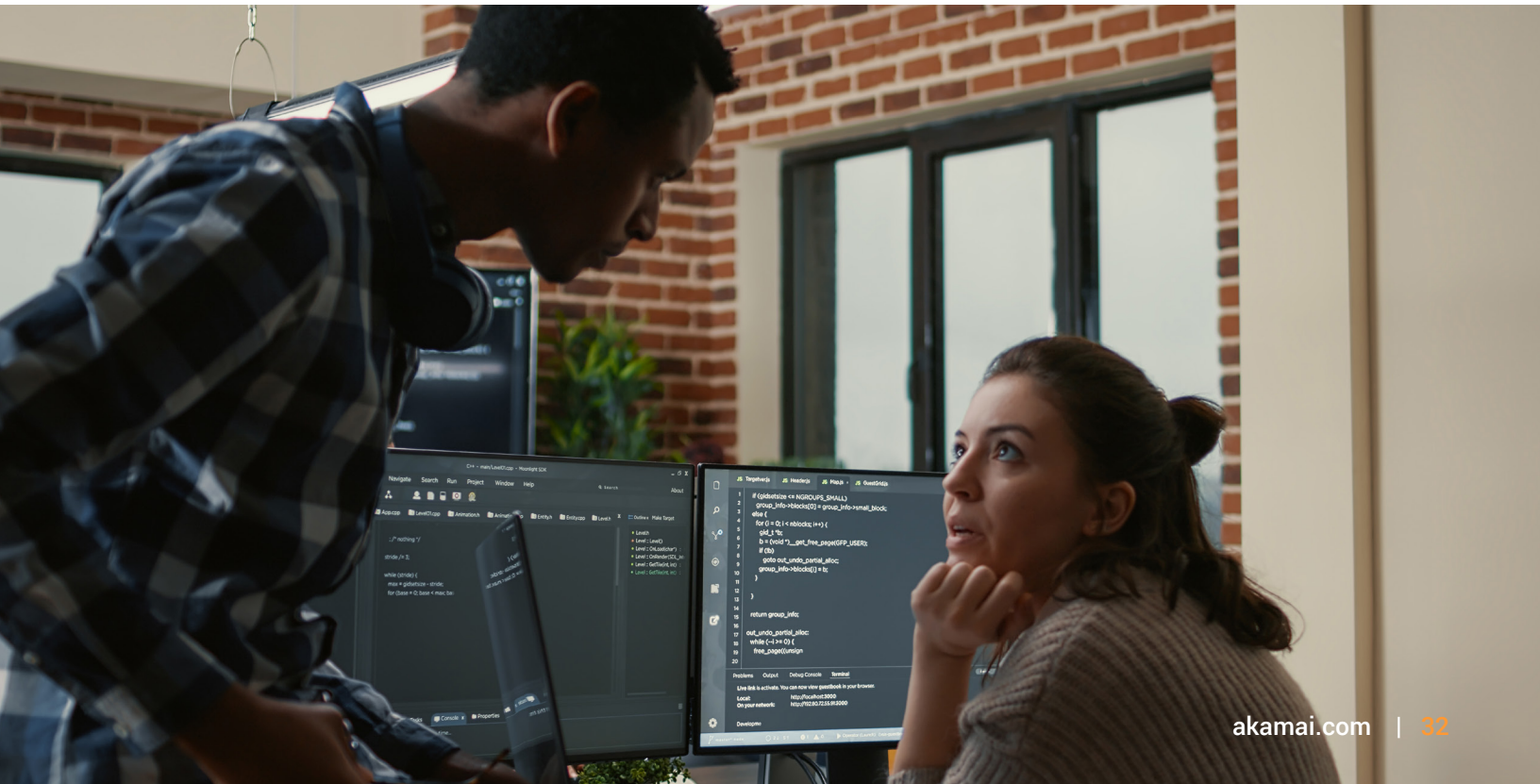
Akamai utilizza due team di risposta agli incidenti: il CSIRT (Computer Security Incident Response Team) e il SIRT (Security Intelligence Response Team). Questi due team collaborano con il SOC (centro operativo per la sicurezza) globale di Akamai per fornire analisi e risposta agli incidenti ai singoli clienti che subiscono un attacco. Inoltre, il CSIRT monitora i clienti di Akamai che vengono attaccati di frequente, rappresentando un'ampia gamma di settori come principale indicatore di nuovi vettori di attacco o nuove tendenze.

Rilevamento rapido delle minacce

Le nostre nuove funzionalità consentono di implementare tempestivamente i sistemi di protezione necessari per contrastare le minacce emergenti e le CVE di alto profilo. Gli aggiornamenti automatici e le operazioni automatizzate vi consentono di gestire i vostri sistemi di difesa con la massima flessibilità.

Protezione delle CVE

L'Akamai Threat Research Team continua a monitorare le CVE (Common Vulnerabilities and Exposures) e garantisce che la soluzione WAAP sia aggiornata per proteggere le applicazioni dei clienti e per fornire la conferma necessaria tramite lo strumento di ricerca delle CVE di Akamai. Questo strumento aiuta a fornire informazioni dettagliate sulle CVE, inclusi i livelli delle minacce e informazioni sugli attuali sistemi di protezione di Akamai. Il catalogo di protezione delle CVE di Akamai vi fornisce la visibilità necessaria per consentirvi di privilegiare le operazioni di sicurezza in linea con i sistemi di protezione di Akamai e di effettuare ricerche nel database delle CVE per stabilire le misure protettive messe in atto da Akamai per risolvere una vulnerabilità, oltre a valutare il livello delle minacce e ad accedere ai dati delle CVE.



Una piattaforma edge distribuita a livello globale

Affidabilità e resilienza

Le soluzioni WAAP di qualità superiore sono progettate su reti ampie e potenti che non bloccano il traffico legittimo dei clienti anche negli attacchi informatici più vasti. Le caratteristiche di comprovata validità in termini di qualità, capacità e facilità di esecuzione offerte dalla piattaforma globale di un provider di soluzioni WAAP devono essere ugualmente importanti quanto le sue funzioni. Se un provider di soluzioni WAAP non riesce a distribuire il traffico legittimo durante un attacco, i clienti devono valutare se hanno investito in una soluzione o semplicemente in uno strumento.

Akamai si impegna nell'intento di offrire eccellenti livelli di performance e protezione ai propri clienti. Questa missione è possibile solo creando i servizi su una base che offre la massima solidità: l'Akamai Connected Cloud. Akamai ha creato la piattaforma cloud più distribuita al mondo, che è costituita da oltre 4200 PoP sull'edge in più di 130 paesi.

Tra i clienti di Akamai, figurano tutte le 10 principali società d'intermediazione immobiliare, tutte le 10 principali banche, tutti i 10 principali fornitori di servizi di streaming video e tutte le 10 principali società che operano nel settore del gaming. I nostri clienti spaziano dalle principali case automobilistiche alle aziende sanitarie, alle società che operano nel settore del retail e agli operatori di telecomunicazioni fino ad un consistente numero di agenzie governative e alle forze armate.

Questi clienti ripongono la loro fiducia nelle capacità dimostrate da Akamai di potenziarle e proteggerle da 40 miliardi di bot al giorno, 780 milioni di attacchi alle app al giorno e 1889 attacchi DDoS che, ogni trimestre, minacciano di detronizzare le loro reti. Akamai distribuisce le sue soluzioni per la sicurezza perché l'intelligence sulle minacce acquisita da un cliente consente di apportare vantaggi e di applicare i sistemi di protezione più appropriati agli altri clienti. La scalabilità della piattaforma globale di Akamai fornisce la quantità e la qualità dei dati necessarie per proteggere le organizzazioni nell'epoca dell'intelligenza artificiale.

Scalabilità globale

Per una soluzione WAF, il problema della scalabilità è incentrato sulla sua capacità di ispezionare sia la quantità richiesta di traffico web, inizialmente e nel corso del tempo, che il numero di regole WAF richieste per valutare questo traffico. Le tradizionali soluzioni WAF basate su hardware, spesso, risentono della scarsa scalabilità perché sono limitate alle risorse della CPU e della memoria disponibili all'interno dell'apparecchiatura e potrebbero dover competere con altre soluzioni presenti nella stessa apparecchiatura.

L'implementazione di una soluzione WAAP integrata nella piattaforma cloud di Akamai elimina il problema della scalabilità sfruttando le risorse del server distribuite di Akamai per ispezionare il traffico web in entrata. Sia gli utenti che i criminali si connettono ai siti web protetti tramite il server Akamai più vicino, che quindi ispeziona il traffico alla ricerca di attacchi e blocca le richieste dannose eventualmente rilevate. In tal modo, la soluzione WAAP di Akamai può scalare facilmente in base all'incremento del traffico delle applicazioni web (sia in caso di picchi improvvisi che di un aumento del traffico a lungo termine) e in base alle nuove posizioni degli utenti in tutto il mondo.

Performance

Le scarse performance possono ostacolare l'implementazione di una soluzione per la sicurezza, specialmente una soluzione WAAP implementata online davanti ad un'applicazione. La riduzione delle performance dei siti web che sono fondamentali per le attività aziendali può causare un peggioramento della produttività, scarse user experience, un rallentamento del time-to-market e la riduzione dei profitti.

La scalabilità globale della piattaforma cloud di Akamai consente alla soluzione WAAP di proteggere le applicazioni web senza ridurre le performance. La soluzione WAAP distribuita a livello globale ispeziona il traffico HTTP non appena arriva sulla piattaforma, distribuendo le risorse della CPU e della memoria richieste per ispezionare il traffico di tutti i server sulla piattaforma. In tal modo, viene eliminato il problema delle performance come fonte di attrito all'interno dell'organizzazione e come ostacolo all'implementazione.

Una piattaforma edge per la massima protezione

Le soluzioni per la sicurezza delle applicazioni web di Akamai indipendenti dal cloud lavorano perfettamente sulla piattaforma per difendere da un'ampia gamma di attacchi alle applicazioni e alle API. L'immagine riportata di seguito illustra la serie completa dei meccanismi e dei controlli di sicurezza multilivello utilizzati da Akamai per tenere lontano le minacce dall'origine, migliorando, al contempo, le performance e l'accesso per gli utenti legittimi.

Akamai App & API Protector include una vasta gamma di meccanismi e controlli di sicurezza automaticamente integrati (illustrati in blu) per offrire una difesa olistica immediatamente disponibile, aggiungendo anche altri prodotti e servizi di Akamai per fornire una protezione completa del livello 7

Supporto gestito contro gli attacchi

Oltre alla gestione WAAP continua, Akamai fornisce anche ai clienti un supporto gestito contro gli attacchi con un monitoraggio dei siti web protetti 24/7 e una risposta gestita agli attacchi rilevati.

Il supporto gestito contro gli attacchi utilizza il personale del SOC globale di Akamai per rispondere ai problemi di sicurezza man mano che si verificano nel modo seguente:

- Rispondendo agli avvisi e alle richieste dei clienti delle soluzioni WAAP ed eseguendo ulteriori indagini sui problemi riscontrati
- Stabilendo appropriate firme degli attacchi e implementando ulteriori misure di mitigazione
- Collaborando con i team addetti alle applicazioni dei clienti per misurare l'efficacia e l'accuratezza delle soluzioni di mitigazione implementate, regolandole, se necessario
- Rivedendo le risposte complessive con i team addetti alle applicazioni dei clienti dopo il problema
- Fornendo pulsanti sull'interfaccia per l'invio di avvisi in caso di attacco, che consentono di attivare una richiesta di supporto di emergenza

SOCC (Security Operations Command Center)

Da più di 10 anni, il SOCC di Akamai aiuta a mitigare molti degli attacchi più vasti al mondo, proteggendo i clienti da un panorama globale delle minacce in continua evoluzione.

Il monitoraggio e la mitigazione di un attacco richiedono quattro funzioni:

- Visibilità globale
- Monitoraggio e creazione di avvisi proattivi
- Agile mitigazione degli attacchi
- Servizio di consulenza continuo fornito da un team di esperti addetti alla sicurezza

Il SOCC di Akamai offre queste funzionalità sull'infrastruttura di sicurezza più grande al mondo. Tutto il traffico di rete passa sulla nostra piattaforma di sicurezza unificata, che raccoglie informazioni in tempo reale. Ad esempio, Akamai ha raccolto le tendenze sulla sicurezza, come un recente aumento consistente di attacchi SQL injection.

Tutto ciò aiuta il team addetto alla sicurezza di Akamai a mitigare le minacce dei clienti con la massima efficacia e il minimo impatto.

Conclusione

Oltre a proteggere dagli attacchi DDoS a livello di reti e applicazioni, le nuove forme di bot automatizzati e attacchi mirati che vengono sferrati tramite le API e i componenti lato client richiedono alle organizzazioni di proteggere applicazioni web, endpoint delle API, browser e infrastrutture con un approccio olistico alla sicurezza basato su una difesa approfondita. Responsabili e addetti alla sicurezza hanno bisogno di soluzioni per le applicazioni web in grado di identificare e mitigare rapidamente le minacce provenienti da vari vettori di attacco e di estendere i tradizionali sistemi di protezione oltre il firewall alle tecnologie di sicurezza correlate per garantire il massimo livello di difesa.

L'approccio di Akamai alla tecnologia WAAP consiste nell'offrire una serie di soluzioni con un livello impareggiabile di ampiezza ed efficacia perché riuniscono tutte le tecnologie necessarie per un moderno sistema di sicurezza. Riteniamo che la soluzione di sicurezza ideale non deve essere concepita solo per i brand più famosi o importanti al mondo. I nostri sistemi di protezione di app e API rendono la sicurezza delle app web disponibile per tutte le organizzazioni che privilegiano la sicurezza tramite una gamma di soluzioni multilivello.

Con una soluzione di sicurezza in grado di evolversi e adattarsi in continuazione grazie ad un'intelligence sugli attacchi vasta e dettagliata, Akamai collabora con le aziende di tutto il mondo per modernizzare e migliorare continuamente i livelli di sicurezza offerti. La nostra azienda si impegna nell'intento di offrire ai team addetti alla sicurezza delle organizzazioni i livelli di intelligence, visibilità, automazione e assistenza necessari per promuovere le iniziative interne e, nello stesso tempo, per tenere i criminali lontani dai loro sistemi aziendali. Ecco perché la nostra azienda viene scelta per proteggere i brand più esigenti che potenziano la vita online.

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo prevenire, rilevare e mitigare le minacce informatiche in ambienti ransomware in modo che voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X e LinkedIn. Data di pubblicazione: 02/25.