DESCRIZIONE DEL PRODOTTO AKAMAI

API Security

Akamai API Security offre un modo intelligente per proteggere le API da abusi della logica aziendale e furti di dati

L'evoluzione degli attacchi alle API

Le API favoriscono le vostre attività aziendali ogni giorno, collegandole con partner, fornitori e clienti. Tuttavia, ogni API aumenta anche la superficie soggetta agli attacchi e i criminali lo sanno. Gli attacchi alle API aumentano e si evolvono rapidamente, spesso in modi non facilmente rilevabili dai sistemi di protezione di applicazioni web e API. Inoltre, senza un inventario completo delle API, il vostro team avrà un punto cieco e le API della vostra organizzazione non saranno protette.

Perché Akamai API Security?

La nostra piattaforma protegge le API per tutto il loro ciclo di vita, dallo sviluppo alla produzione. Concepita per le organizzazioni che rendono visibili le API ai loro partner, fornitori e utenti, la soluzione API Security rileva le API, esamina il loro sistema di sicurezza e analizza il loro comportamento per bloccare il proliferare delle minacce all'interno.

Le funzionalità più importanti di API Security

Rilevamento

Spesso, non si conoscono tutte le API di cui si dispone. Senza un inventario accurato, tuttavia, la vostra azienda viene esposta ad una serie di rischi per la sicurezza. Basta andare a tentoni! Lasciatevi aiutare a:

- Individuare e inventariare tutte le API, indipendentemente dalla configurazione o dal tipo, tra cui RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC e gRPC
- Rilevare le API inattive, tradizionali e zombie
- Identificare i domini ombra dimenticati, trascurati o non conosciuti
- Eliminare i punti ciechi e scoprire i potenziali percorsi degli attacchi

Test

Le applicazioni vengono sviluppate ad un ritmo che non è mai stato così veloce, pertanto è più semplice che vulnerabilità o difetti di progettazione passino inosservati. Usufruite della suite di test per la sicurezza delle API per:

- Eseguire automaticamente più di 150 test in grado di simulare il traffico dannoso, inclusi i 10 principali rischi per la sicurezza delle API riportati nell'elenco OWASP
- Scoprire le vulnerabilità prima che le API entrino in fase di produzione per ridurre il rischio di un attacco
- Esaminare le specifiche delle API sulla base delle regole e delle policy di governance stabilite
- Eseguire test sulla sicurezza delle API on-demand o come parte di una pipeline CI/CD

VANTAGGI PER LA VOSTRA AZIENDA

Individuazione
Individuare la superficie di attacco delle API. Ridurre i costi correlati con l'inventario delle API e gli aggiornamenti della documentazione. Migliorare la conformità con requisiti normativi e policy interne.

Test
Ridurre i costi necessari per la mitigazione individuando tempestivamente i problemi. Migliorare la qualità del codice senza compromettere la velocità. Aumentare i ricavi accelerando il time-to-market.

Rilevamento
Acquisire importanti informazioni sul contesto aziendale scoprendo cosa è successo esattamente. Dedurre perché si tratta di un problema e scoprire il suo impatto potenziale. Stabilire come risolvere il problema.

Risposta
Ridurre i rischi bloccando immediatamente gli attacchi. Ridurre i costi rimediando alle vulnerabilità prima dello sfruttamento. Ridurre la perdita di ricavi derivante dal downtime.

Akamai

Rilevamento

Anche un semplice errore di configurazione delle API può lasciare la vostra azienda vulnerabile ai criminali informatici. Una volta penetrati nel sistema, gli hacker possono accedere ed esfiltrare i vostri dati sensibili. Utilizzate la nostra piattaforma per:

- Eseguire una scansione automatica dell'infrastruttura per scoprire eventuali configurazioni errate e rischi nascosti
- Creare workflow personalizzati per informare le principali persone coinvolte sulle vulnerabilità
- Identificare le API e gli utenti interni che possono accedere ai dati sensibili
- Classificare i problemi rilevati in base ai livelli di gravità per dare priorità alla mitigazione

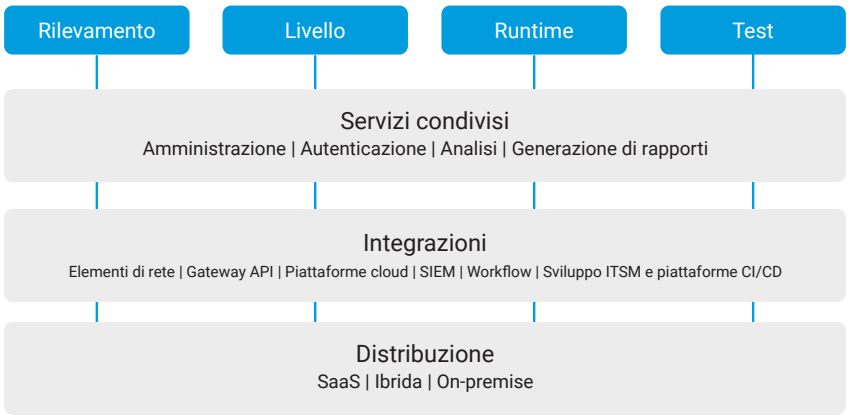
Risposta

Non è più una questione di "se" un'organizzazione subirà un attacco, ma di "quando" lo subirà. Ecco perché è necessario rilevare e bloccare gli attacchi in tempo reale. Utilizzate il nostro sistema di rilevamento delle anomalie basato sull'intelligenza artificiale/apprendimento automatico per:

- Monitorare la manomissione e la fuga di dati, la violazione delle policy, il comportamento sospetto e gli attacchi alle API
- Analizzare il traffico delle API senza apportare ulteriori modifiche alla rete o utilizzare agenti difficili da installare
- Effettuare le opportune integrazioni con i workflow esistenti (creazione di ticket, SIEM [Security Information and Event Management], ecc.) per avvisare i team addetti alla sicurezza/operazioni
- Prevenire attacchi e abusi in tempo reale con una mitigazione parziale o totalmente automatizzata

La differenza di Akamai: bloccare il traffico sull'edge

Akamai App & API Protector riesce a individuare e mitigare le minacce alle API per app e API eseguite tramite Akamai Connected Cloud e può bloccare il traffico contenente potenziali minacce non rilevate da API Security. Se utilizzati insieme, i sistemi di protezione delle API di Akamai offrono un livello completo e costante di visibilità sulle API, consentendo di individuare, controllare, rilevare e rispondere alle specifiche esigenze in termini di sicurezza delle API nell'intero patrimonio delle applicazioni.



Volete vedere la soluzione API Security in azione? Visitate il sito akamai.com/apisecurity e pianificate un appuntamento con il nostro team.