DESCRIZIONE DELLA SOLUZIONE AKAMAI

API Security for Healthcare

Scoprite come Akamai API Security aiuta le aziende sanitarie ad identificare le minacce alle API e a difendersi in modo efficace.

Le API consentono alle aziende sanitarie di migliorare e semplificare l'assistenza ai pazienti favorendo un agevole scambio di dati tra sistemi, dispositivi e persone. Tuttavia, questi dati sono, spesso, sensibili (ad es., cartelle cliniche dei pazienti o polizze assicurative) e, pertanto, rendono le API un bersaglio privilegiato dai criminali.

Le vostre API sono a rischio? Esaminiamo i seguenti risultati tratti dallo studio sull'impatto della sicurezza delle API 2024:

- Quasi l'85% delle aziende sanitarie ha riscontrato problemi di sicurezza delle API nel 2024, salendo dal 79% registrato nel 2023.
- Solo il 24% delle aziende con un inventario completo delle API sa quali API scambiano dati sensibili, una percentuale scesa dal 40% registrato nel 2023.

Nel contempo, i responsabili dell'IT e della sicurezza in vari settori hanno riferito di spendere, in media, più di 943.000 dollari per affrontare e per recuperare dai problemi di sicurezza delle API.

Le API consentono di scambiare agevolmente i dati, offrendo alle aziende sanitarie i vantaggi apportati da un livello superiore di interoperabilità ed efficienza, tuttavia, espandono anche la loro superficie di attacco: man mano che proliferano all'interno delle applicazioni, negli ambienti cloud e nei modelli di AI, le API causano anche un aumento dei rischi correlati. Le aziende sanitarie stanno implementando inavvertitamente le API che sono configurate in modo errato, sottoposte a test di scarsa qualità e progettate senza controlli degli accessi, il che consente ai criminali di rubare dati e interrompere le operazioni in modo più semplice.

Akamai API Security aiuta i provider di servizi a scoprire di quante API dispongono e i tipi di dati trasmessi dalle API, oltre a fornire i mezzi necessari per proteggere i loro dati in uno specifico intervallo di tempo. Sfortunatamente, molti professionisti del settore sanitario considerano le API come parte di un sistema di sicurezza delle applicazioni tradizionale. Al contrario, il personale dei team AppSec e DevOps deve pensare in modo separato sulle specifiche considerazioni della sicurezza che le API pongono per entrambi. Le API costituiscono la tecnologia su cui si basa l'assistenza sanitaria moderna, quindi presentano nuovi rischi che gli strumenti tradizionali non riescono a gestire.

Per stabilire un solido programma per la governance e la sicurezza delle API, le organizzazioni devono collaborare con il vendor di soluzioni per la sicurezza delle API più appropriato. Nel settore sanitario, i flussi di dati non monitorati rappresentano un rischio notevole, eppure molte organizzazioni non dispongono ancora di un inventario completo delle API di cui dispongono. Akamai API Security aiuta le organizzazioni ad ottenere una piena visibilità sullo scenario delle loro API identificando tutte le API attive e analizzando i tipi di dati che trasmettono. A questo punto, la nostra soluzione offre una protezione continua tramite la gestione delle risorse, l'analisi dei dati sensibili, il rilevamento delle anomalie, i test sulla sicurezza delle API, l'integrazione dei processi CI/CD e la mitigazione manuale e automatizzata, integrandosi facilmente nei workflow di terze parti.

Sfide

Le API espandono la superficie di attacco

Quasi l'85% delle aziende sanitarie ha riscontrato problemi di sicurezza delle API nel 2024

Come Akamai API Security affronta le minacce alle API

La soluzione di Akamai è appositamente progettata per aiutare le aziende sanitarie a proteggere il loro patrimonio delle API.

Individuazione completa delle API

Identificate e create un inventario delle API nel vostro ambiente, incluse le API RESTful, GraphQL, SOAP, XML-RPC e gRPC. Rilevate le API obsolete o non gestite che non sono protette da un gateway API e ottenete una visibilità sui loro attributi e metadati.

Comprensione del comportamento delle API e rilevamento delle minacce

Sfruttate l'analisi basata sull'AI per identificare automaticamente i rischi per la sicurezza come fughe di dati, accessi non autorizzati, errori di configurazione e attività sospette. Tenetevi al passo con le potenziali minacce grazie al monitoraggio e al rilevamento delle anomalie in modo continuo.

Protezione delle API e mitigazione delle falle nella sicurezza

Bloccate gli attacchi in tempo reale, correggete gli errori di configurazione del sistema di sicurezza e aggiornate automaticamente le regole del firewall per fermare il traffico dannoso. Integrate perfettamente la soluzione con gli ecosistemi di sicurezza esistenti, come la soluzione WAF, i sistemi di generazione dei ticket e le piattaforme SIEM, per migliorare le funzionalità di risposta.

Test proattivi delle API prima dell'implementazione

Assicuratevi che le API vengano sottoposte a test accurati durante il ciclo di vita dello sviluppo per scoprire i difetti della logica aziendale, gli errori di configurazione e altre vulnerabilità prima che raggiungano la fase di produzione. Integrando tempestivamente i test sulla sicurezza, le organizzazioni possono affrontare i rischi in modo proattivo e rafforzare i loro sistemi di difesa delle API.

Akamai API Security

Dall'individuazione delle API e dall'analisi dei rischi ai test e alla conformità delle API

Per ulteriori informazioni, visitate la nostra pagina su API Security o contattate il team di vendita di Akamai.