DESCRIZIONE DELLA SOLUZIONE AKAMAI

Akamai API Security per la gestione delle risorse API

Man mano che le organizzazioni diventano sempre più digitali e incentrate sul cloud, crescono anche la portata, il valore e l'ambito di applicazione delle API che diventano, quindi, un fattore di rischio in aumento.

Le API esposte o non configurate correttamente sono diffuse e facili da violare. Non solo non sono adeguatamente protette, ma spesso risultano anche invisibili e non gestite, come, ad esempio, le "API ombra" altamente vulnerabili. Inoltre, la loro proliferazione rende difficile individuare e inventariare ogni API dell'azienda.

Per aiutare le organizzazioni a ottenere la visibilità di cui hanno bisogno, Akamai API Security fornisce una classificazione e un inventario automatizzati delle API per utenti interni ed esterni.

Per la creazione di un inventario completo, la soluzione Akamai API Security si avvale di molteplici fonti, tra cui gateway API, WAF (Web Application Firewall), servizi cloud pubblici, traffico di rete, documentazione API e altro ancora. Ciò garantisce che le modifiche alle API vengano costantemente monitorate e che la versione più recente venga riportata nella libreria API.

La soluzione Akamai API Security

Akamai API Security si compone di quattro moduli integrati, in grado di garantire la gestione delle risorse API e la sicurezza end-to-end.

Individuazione
Consente di individuare e inventariare le API e i rischi correlati, provenienti sia dall'interno che dall'esterno

Sistema di sicurezza
Consente di scoprire vulnerabilità ed errori di configurazione per accelerare la mitigazione e assicurare la conformità

Runtime
Consente di rilevare e bloccare gli attacchi alle API con analisi del traffico in tempo reale basate sull'apprendimento automatico

Esecuzione di test
Consente di individuare e correggere le vulnerabilità durante il ciclo di vita dello sviluppo

Vantaggi

Catalogo API
Consente di identificare i sistemi, i servizi e le applicazioni che utilizzano le API, con una tassonomia dettagliata

Catalogo query
Consente di esplorare e gestire l'inventario delle APO in base ai diversi quadri normativi o casi di utilizzo specifici

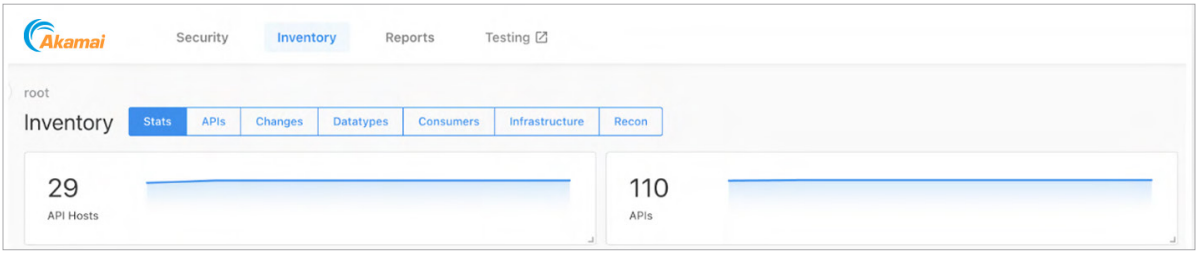
Standard API
Consentono di caricare, visualizzare e analizzare i file OpenAPI Spec e i file di regole di linting

Riutilizzo delle API
Consente di individuare le API esistenti che eseguono l'attività richiesta invece di codificarne di nuove

Per la gestione delle risorse, il punto di partenza è il modulo di individuazione. Analizzando le fonti di traffico nell'ambiente, la soluzione determina quante API sono disponibili e le classifica automaticamente in base a vari modelli.

Catalogo API

Akamai API Security presenta un catalogo completo delle API esistenti. Questo catalogo identifica i sistemi, i servizi e le applicazioni che utilizzano queste API e fornisce una tassonomia dettagliata di ogni singola API.

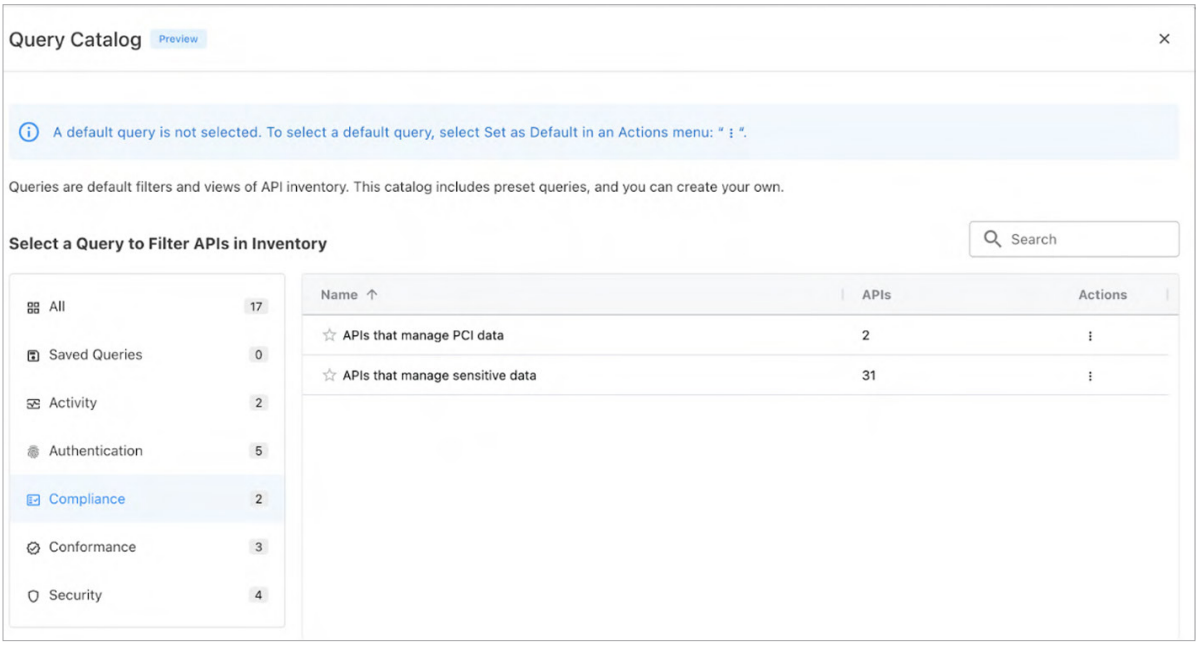


Akamai API Security tiene traccia di tutte le modifiche apportate alle API e consente agli utenti di esportare la documentazione aggiornata sotto forma di file OpenAPI Spec basato su tali modifiche. Inoltre, il sistema può informare gli utenti qualora venissero aggiunte nuove API al loro ambiente.

Infine l'API di gestione integrata in Akamai API Security può essere utilizzata per estrarre informazioni dalla libreria API e creare un CMDB (database di gestione della configurazione) delle API centralizzato.

Catalogo query

Akamai API Security offre un catalogo di query integrato che consente di esplorare e gestire facilmente l'inventario in base ai diversi quadri normativi o casi di utilizzo specifici.



Per ogni API, il sistema fornirà:

- proprietario, tipo e flussi delle chiamate API;
- tipi di dati elaborati;
- metodi di autenticazione supportati;
- origine e posizione dell'API;
- convalida della corrispondenza tra l'API rilevata e la documentazione/le specifiche dell'API;
- infrastruttura su cui si basa l'API;
- grafico di rete completo che mostra le dipendenze dell'API;

Utilizzo degli standard API

La soluzione consente inoltre di caricare, visualizzare e analizzare i file OpenAPI Spec e/o i file di regole di linting. Il linting è il processo di verifica della conformità e correttezza tecnica delle API rispetto a una serie di vincoli aggiuntivi che spesso sono documentati sotto forma di linee guida delle API. Akamai include un set predefinito di regole di linting per Spectral, uno strumento open source che permette agli sviluppatori di creare, documentare e gestire le API. Sono disponibili tre formati di file Spec caricabili:

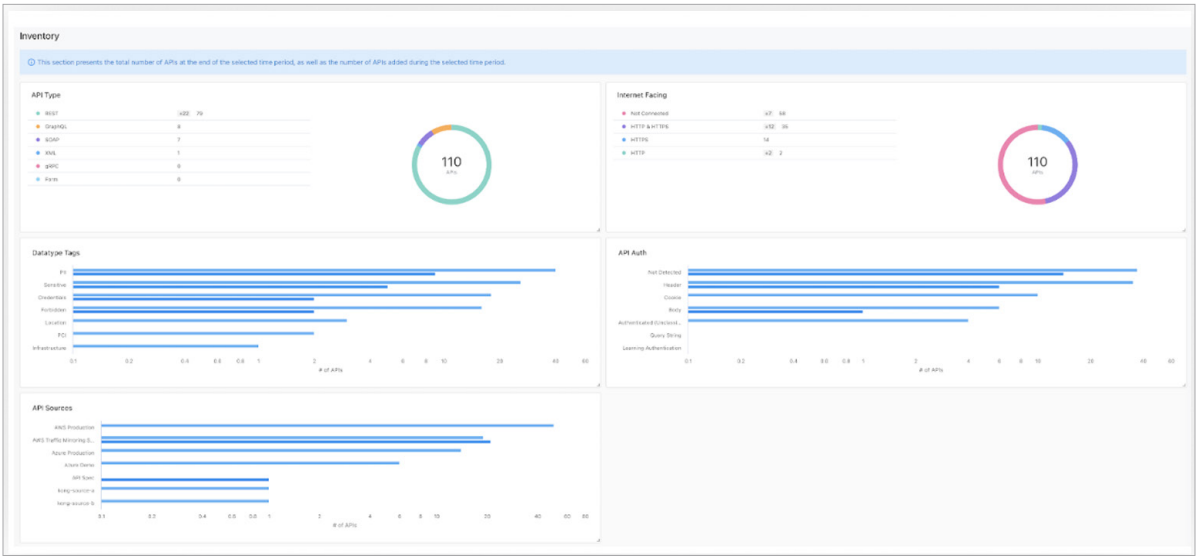
- RESTful API Modeling Language
- Web Services Description Language
- Web Application Description Language

In tal modo, si possono sfruttare gli standard API esistenti o definirne di nuovi applicandoli ai diversi ambienti. Questi standard possono essere specifici del settore, ad esempio API standard di open banking per il settore dei servizi finanziari sulla base della Banking Industry Architecture Network.

La nostra soluzione API Security rileverà anche eventuali deviazioni rispetto allo standard e consentirà di definire policy di mitigazione per gestire questi tipi di rilevamento. Il sistema identificherà e importerà inoltre le API dai file Spec e le confronterà con il traffico di rete effettivo. Utilizzando la recon di Akamai API Security, le API esterne possono essere rilevate e importate sulla base di semplici informazioni sul nome di dominio.

Ottimizzazione dell'utilizzo delle API

Grazie a una libreria API completa, facile da consultare e da navigare, gli sviluppatori saranno in grado di individuare le API esistenti che eseguono l'attività richiesta invece di codificarne di nuove da zero. Grazie al nostro inventario e catalogo API, sarà possibile favorire un migliore utilizzo delle API, limitando eventuali lacune di visibilità negli ambienti per gli sviluppatori e i professionisti della sicurezza.



Ulteriori informazioni

Le API sono essenziali per le organizzazioni poiché consentono di offrire servizi ai clienti, generare profitti e operare in modo efficiente. Tuttavia, la crescita continua, la vicinanza ai dati sensibili e la mancanza di controlli di sicurezza delle API le rendono un bersaglio allettante per i criminali moderni. Le organizzazioni possono ridurre i rischi e proteggersi dagli attacchi alle API con una soluzione completa che offre funzionalità di individuazione, gestione dei sistemi, protezione del runtime e test sulla sicurezza.

Scoprite di più su come Akamai API Security può aiutare la vostra organizzazione.