

Governance e sicurezza delle API integrate per IBM API Connect e DataPower

La promessa e la sfida delle API

In quanto elementi trainanti della trasformazione digitale, le API consentono alle organizzazioni che operano in ogni settore di creare nuovi servizi e modelli aziendali allo scopo di accelerare la loro espansione. Tuttavia, le API proliferano come i rischi correlati.

- Anche se aziende e responsabili della progettazione hanno rapidamente incrementato l'utilizzo e l'integrazione delle API nelle loro organizzazioni, la loro capacità di gestire le API in modo efficace rimane una sfida da affrontare.
- Nella corsa alla creazione e al rilascio di nuove applicazioni e servizi basati sull'intelligenza artificiale sempre più rapidamente, le API sottostanti contengono troppo spesso errori di configurazione e codifica, nonché problemi di logica aziendale.
- Ogni volta che un cliente, un partner o un vendor interagiscono con un'organizzazione in modo digitale, c'è un'API "dietro le quinte" che facilita un perfetto scambio dei dati, spesso sensibili, e i criminali lo sanno bene.

Di conseguenza, le API sono emerse come uno dei principali vettori di attacco ad alto rischio. Gli attacchi sferrati contro le API possono mettere a rischio i profitti, la resilienza e la conformità normativa di un'azienda.

Per affrontare questa sfida, le organizzazioni devono adottare un approccio completo nei confronti della governance e della sicurezza, incluse le operazioni di progettazione, sviluppo, esecuzione dei test, implementazione, funzionamento e mitigazione dei problemi. Insieme, Akamai API Security e IBM consentono alle organizzazioni di sviluppare, implementare e gestire rapidamente le API con la massima tranquillità per poter rispondere e scalare le proprie attività aziendali in modo prevedibile.

Come Akamai e IBM aiutano i clienti

Scoprite il vostro patrimonio delle API

È impossibile proteggersi da ciò che non si vede. Con Akamai API Security, potrete scoprire automaticamente API, domini e problemi per creare un inventario delle API affidabile in grado di offrirvi la visibilità necessaria sul vostro intero patrimonio delle API: le aziende, di solito, individuano un numero notevolmente maggiore di API rispetto a quanto avrebbero pensato di disporre o sospettato di trovare. Potrete anche individuare facilmente informazioni fruibili, come dati esfiltrati, per comprendere i percorsi di attacco disponibili per i criminali e sfruttare un'eccellente integrazione con i più comuni elementi dell'infrastruttura adiacenti ai vostri gateway API e alle piattaforme di gestione per garantire una condivisione coerente dei dati sulla sicurezza all'interno dell'organizzazione.

Rafforzate il vostro sistema di sicurezza e governance

Scalate le vostre operazioni aziendali e applicate le best practice più appropriate con Akamai API Security per la governance delle API:

- Individuate tutte le API nel vostro ecosistema con un contesto aziendale completo e adottate le best practice più appropriate per la gestione delle API
- Semplificate le comunicazioni tra i team addetti alla sicurezza e allo sviluppo
- Individuate le vulnerabilità a partire dagli errori di configurazione fino alle API che non rientrano nelle policy stabilite
- Proteggete i dati sensibili e monitorate in modo proattivo i cambiamenti per ridurre i rischi presenti nelle vostre API

Sfide

-  Stilare un inventario completo delle API e individuare le API sconosciute
-  Identificare le API non conformi, vulnerabili o configurate in modo errato
-  Rilevare e fermare l'abuso o l'uso improprio di API, inclusi gli attacchi alla logica aziendale
-  Creare API sicure e coerenti senza andare a discapito della velocità o dell'agilità
-  Stabilire un processo di allineamento e supervisione dei programmi di sicurezza e governance delle API



Fermate gli abusi e gli attacchi alle API con la protezione del runtime

Rilevate e bloccate gli attacchi alle API dall'edge al core, tra cui fuga e manomissione dei dati, violazioni delle policy relative ai dati, comportamenti sospetti e molto altro, con l'analisi del traffico in tempo reale, il monitoraggio fuori banda e le integrazioni dei workflow per migliorare l'efficacia del SOC (centro operativo per la sicurezza).

Fornite API sicure più rapidamente con Active Testing

Integrate facilmente i test sulla sicurezza delle API in ogni fase del loro ciclo di sviluppo e scoprite eventuali vulnerabilità, errori di configurazione e problemi di conformità prima che le API raggiungano la fase di produzione. Con Active Testing, il personale DevSecOps può eseguire una serie completa di oltre 200 test sulla sicurezza delle API on-demand o come parte dei processi CI/CD dell'azienda. Active Testing individua ed esegue i test di tutte le API sulla base della logica aziendale sottostante dell'applicazione, che consente agli sviluppatori di scoprire vulnerabilità complesse spesso non rilevate da altri strumenti per l'esecuzione dei test.

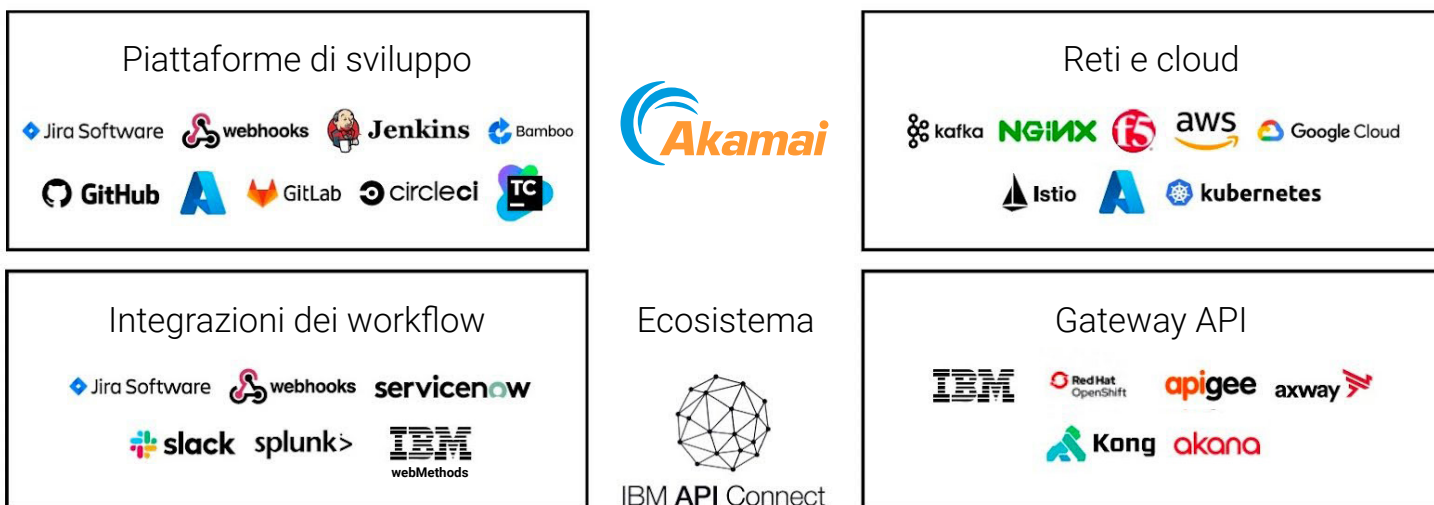
Come Akamai consente agli utenti IBM di ottenere visibilità e protezione con un'integrazione efficiente

Akamai API Security si integra con API Connect e DataPower su più piattaforme cloud e opzioni di implementazione. Inoltre, nel momento in cui DataPower è gestito da API Connect, vengono apportate modifiche alla configurazione dei sistemi, migliorando l'efficienza operativa e riducendo, al contempo, il rischio che si verifichino attività di sviluppo non autorizzate e non conformi

Un livello impeccabile nella gestione e nella risposta agli attacchi

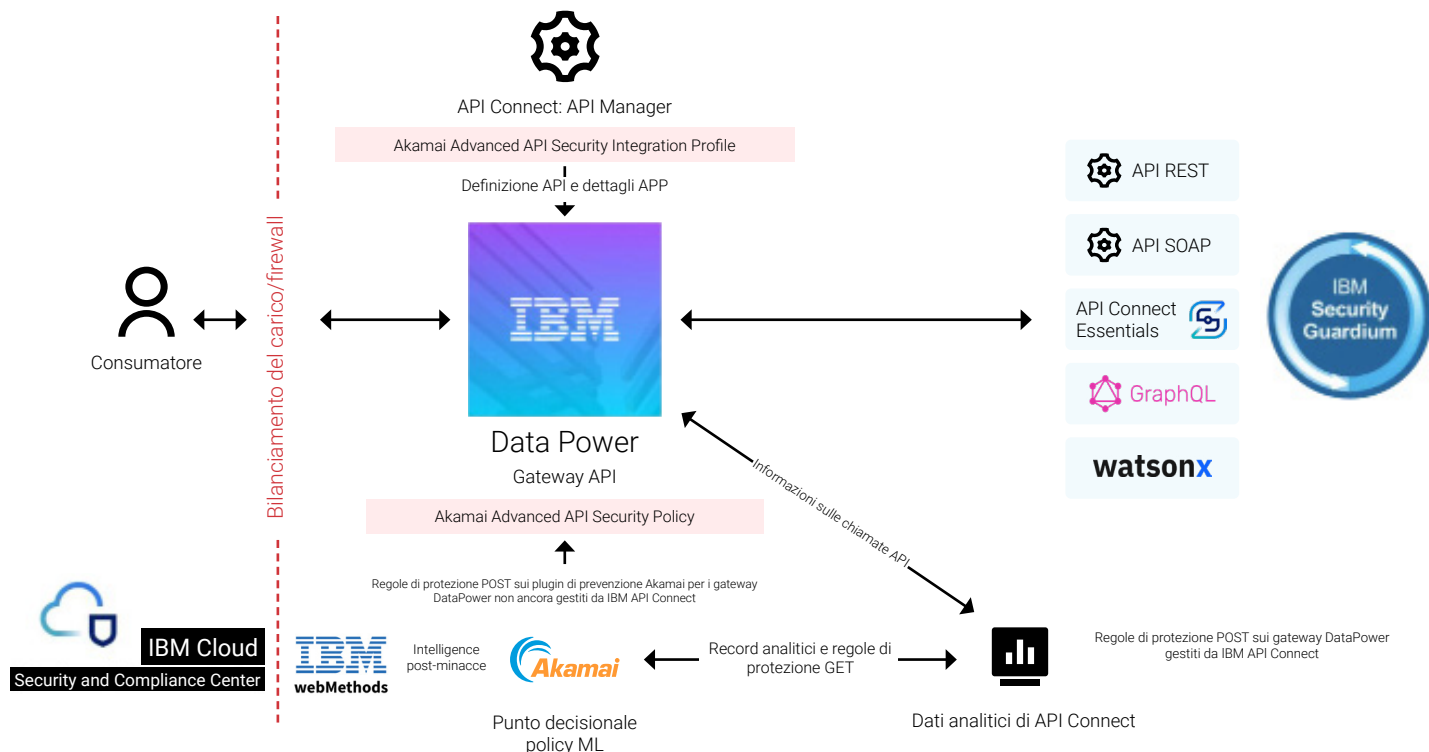
Inoltre, i clienti di IBM DataPower possono utilizzare le funzioni di rilevamento e blocco delle minacce quasi in tempo reale senza influire sulle performance e sulla latenza né installare ulteriori plugin sui gateway DataPower grazie all'integrazione con la soluzione Akamai API Security.

IBM API Connect può valutare le richieste ricevute dalle risorse sulla base delle policy di autorizzazione di Akamai API Security e applicare regole di blocco sui cluster IBM DataPower, riducendo i tempi di mitigazione da giorni a pochi minuti o secondi.



Combinare la potenza di IBM webMethods e Akamai API Security per ottenere un impareggiabile livello di gestione e protezione delle API. Questa partnership offre una soluzione completa che unisce l'avanzata individuazione delle API di Akamai con le affidabili funzioni di governance e integrazione dei dati in tempo reale offerte da IBM webMethods. Raggiungete il massimo livello di visibilità e controllo delle vostre API per garantire sicurezza e conformità. Questa integrazione non solo rafforza i vostri sistemi di difesa, ma potenzia anche il livello di efficienza, consentendo alla vostra azienda di rispondere in modo rapido e sicuro alle esigenze dinamiche del mercato.

Infine, i clienti di IBM DataPower possono usufruire dell'integrazione di Akamai eBPF Red Hat OpenShift per rilevare le API che non sono ancora gestite da API Connect o inoltrate da DataPower in modo da poter individuare e proteggere le API che elaborano transazioni ad alto rischio e dati riservati. Queste funzionalità si estendono oltre le sedi aziendali alle configurazioni ibride e cloud, supportando AWS (Amazon Web Services), Microsoft Azure e GCP (Google Cloud Platform).



Cosa si prospetta per il futuro

Le API sono la forza trainante che consente alle organizzazioni di soddisfare le esigenze dei clienti, generare profitti e competere in un'economia digitale in continua evoluzione. Tuttavia, la crescita continua, la vicinanza ai dati e la miriade di vulnerabilità delle API le rendono un bersaglio allettante per i criminali. Con l'aumento dei problemi di sicurezza delle API, è fondamentale mettere in atto le funzionalità necessarie per individuare, proteggere e sottoporre a test tutte le API presenti nella vostra organizzazione. La partnership tra IBM e Akamai può fornire alle aziende la tranquillità necessaria per creare, mantenere e utilizzare le API in modo sicuro e su larga scala.

Scoprite come possiamo aiutarvi [programmando una demo personalizzata su Akamai API Security](#). Per ulteriori informazioni, potete anche rivolgervi al vostro contatto IBM.