I 5 pilastri della gestione delle API con CA Layer 7

ca technologies





Introduzione:

Gestire la nuova azienda aperta

Realizzare le opportunità dell'economia basata sulle API

All'interno dei diversi settori industriali, i confini dell'impresa tradizionale tendono a confondersi, con l'apertura delle proprie funzionalità di dati e app on-premise, da parte delle aziende, alle organizzazioni partner, al web, alle app mobile, ai device intelligenti e al cloud. Le API (Application Programming Interface) costituiscono le fondamenta di questo nuova azienda "aperta", consentendo alle aziende di riutilizzare le risorse informative esistenti al di là dei confini dell'organizzazione.

Affrontare le sfide di una pubblicazione delle API sicura e gestibile

Le API mettono le aziende in condizione di riutilizzare rapidamente i sistemi IT, aggiungere valore alle offerte esistenti e attivare nuovi flussi di ricavi. Non dovrebbe costituire una sorpresa, tuttavia, che l'esposizione dei sistemi on-premise tramite API crei anche una serie di nuove sfide a livello di sicurezza e di gestione. Per "gestione delle API" si intende un insieme di processi e di tecnologie emersi negli ultimi anni per facilitare alle aziende il superamento di queste sfide.

Le soluzioni di gestione delle API mirano a facilitare anche alle organizzazioni più attente alla sicurezza l'apertura delle proprie risorse informative per l'utilizzo da parte di organizzazioni partner, sviluppatori terzi, app mobile e servizi cloud, senza compromettere la sicurezza dei dati e le prestazioni dei sistemi backend. Soluzioni complete per la gestione delle API forniscono anche funzionalità per gestire gli sviluppatori di app che sfruttano le API aziendali.

Panoramica:

I 5 pilastri della gestione delle API

Esporre i dati e le funzionalità aziendali in formati compatibili con le API

Convertire complessi servizi applicativi on-premise in API RESTful immediatamente utilizzabili dagli sviluppatori

Proteggere le risorse informative esposte tramite API per evitare abusi

Garantire che i sistemi aziendali siano protetti dagli attacchi a livello di messaggio e di tipo hijack

Autorizzare un accesso sicuro e senza soluzione di continuità per le identità valide

Implementare funzionalità solide di controllo degli accessi, federazione delle identità e login social

Ottimizzare le prestazioni dei sistemi e gestire il ciclo di vita delle API

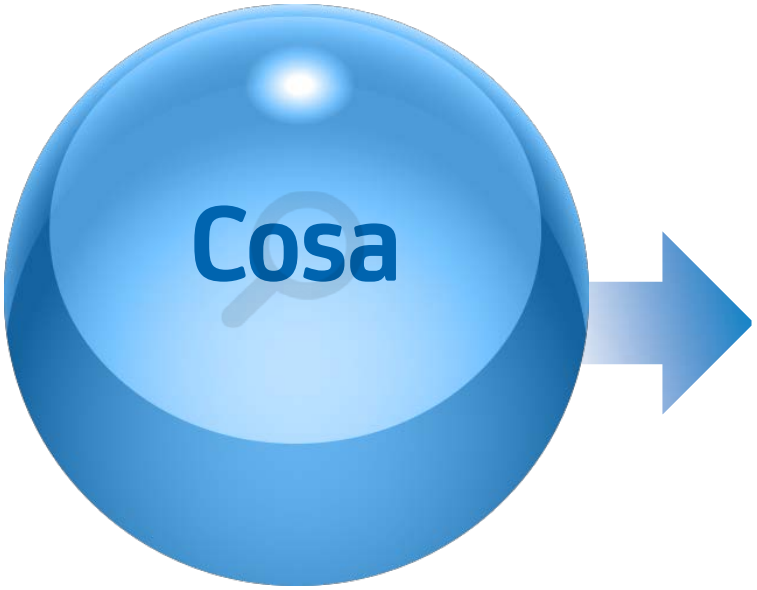
Conservare la disponibilità dei sistemi backend per le API, le app e gli utenti finali

Coinvolgere, eseguire l'onboarding, formare e gestire gli sviluppatori

Fornire agli sviluppatori le risorse di cui hanno bisogno per creare app che offrano un valore reale

Esporre i dati e le funzionalità aziendali in formati compatibili con le API

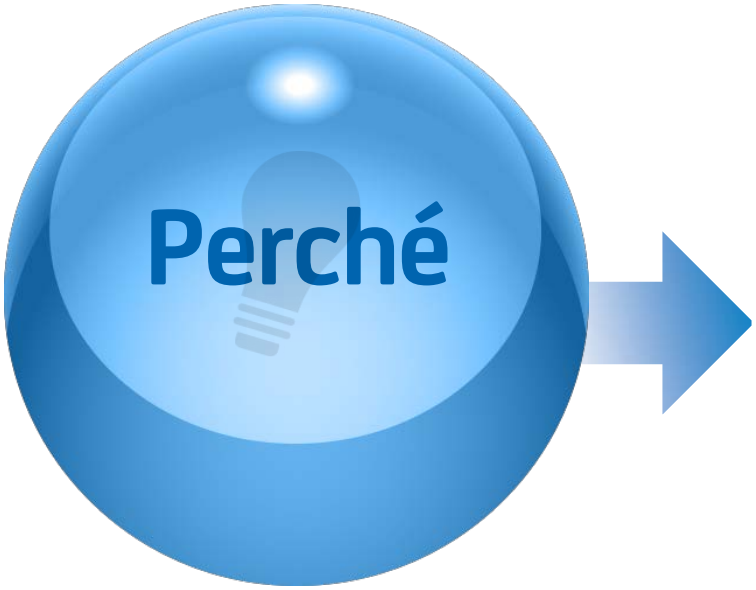
Convertire complessi servizi applicativi on-premise in API RESTful immediatamente utilizzabili dagli sviluppatori



I dati e le app aziendali comprendono tipicamente una complessa rete di standard, protocolli, linguaggi di programmazione e formati di file.

La prima fase della gestione delle API consiste nel presentare queste diverse risorse informative in un formato che gli sviluppatori possano comprendere e sfruttare.

Comunemente, questo corrisponde a pubblicare interfacce di programmazione delle app che utilizzano il protocollo REST (API RESTful).



I sistemi on-premise si affidano comunemente a servizi applicativi erogati in formati proprietari troppo dettagliati per funzionare in modo efficiente tramite web o app mobile.

I servizi applicativi connessi allo stile SOA (Service Oriented Architecture) comune generalmente impiegano il protocollo SOAP, mentre gli sviluppatori mobile/web si basano su REST.

Se le API non vengono erogate in un formato che gli sviluppatori interni e terzi possono sfruttare facilmente, la creazione di nuove app effettivamente portatrici di valore non risulterà agevolata.

Le più efficaci soluzioni di gestione delle API includono funzionalità per la presentazione di servizi legacy aziendali come API RESTful.

In genere, questo comporterà l'utilizzo di una SOA o di un API Gateway per convertire automaticamente i dati dai servizi basati su SOAP in API RESTful.

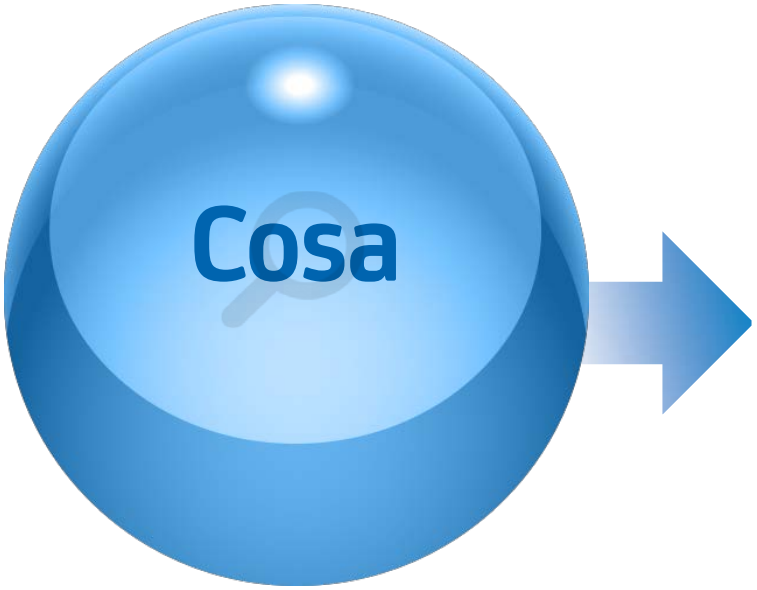
Per essere veramente efficace, il gateway deve consentire di comporre in modo efficiente API RESTful da combinazioni di molteplici servizi applicativi esistenti.

Ulteriori informazioni

API Tech Talk: Semplificare l'adattamento REST
api.co/RESTadaptation

Proteggere le risorse informative esposte tramite API per evitare abusi

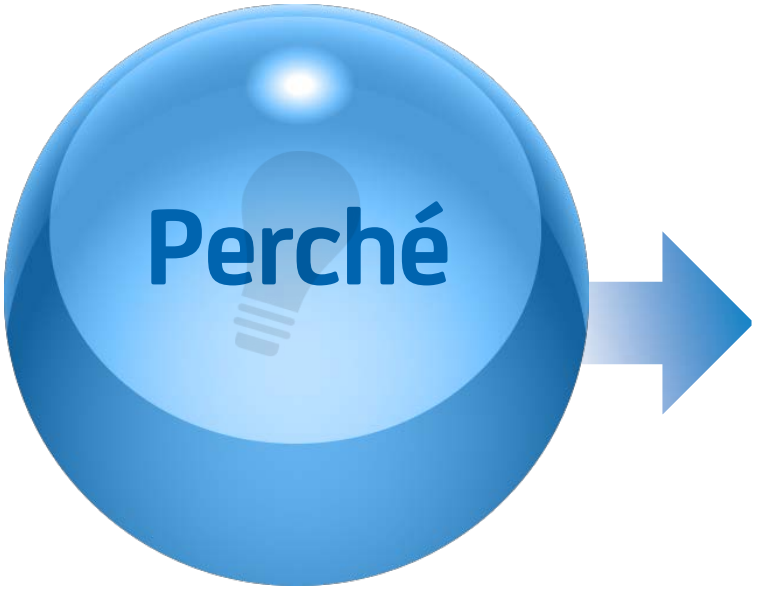
Garantire che i sistemi aziendali siano protetti dagli attacchi a livello di messaggio e di tipo hijack



L'apertura delle risorse informative aziendali per l'utilizzo in nuove app le espone a molte delle stesse minacce per la sicurezza che affliggono il web, ad esempio virus e attacchi DoS.

In aggiunta, le API creano una serie di sfide per la sicurezza nuove e specifiche, che vanno oltre ciò che le imprese sono abituate ad affrontare sul web.

Forse la funzione più essenziale della gestione delle API è la creazione di un livello di sicurezza finalizzato a garantire che eventuali hacker non siano in grado di accedere, utilizzare in modo improprio o attaccare i sistemi esposti.



Le API sono finestre aperte sulle app e sui dati, che potenzialmente forniscono agli hacker una vista sul funzionamento interno dei sistemi aziendali e un percorso per accedere a essi.

Questo aumenta la possibilità che gli hacker siano in grado di sottrarre dati riservati, dirottare le interfacce rivolte al pubblico per scopi dannosi o bloccare la funzionalità di sistemi critici.

Le soluzioni di sicurezza online convenzionali, progettate per il web, non esauriscono tutte le minacce potenziali create dalla pubblicazione delle API, motivo per il quale è necessario implementare una sicurezza API specifica.

Probabilmente la funzione chiave del tipo di API Gateway sopra citato consiste nel controllare e filtrare tutto il traffico API per identificare e quindi neutralizzare le minacce comuni o emergenti.

Per essere efficace, il gateway deve essere progettato e certificato per affrontare le minacce a livello di messaggio e specifiche delle API come SQL Injection, attacchi DoS e virus.

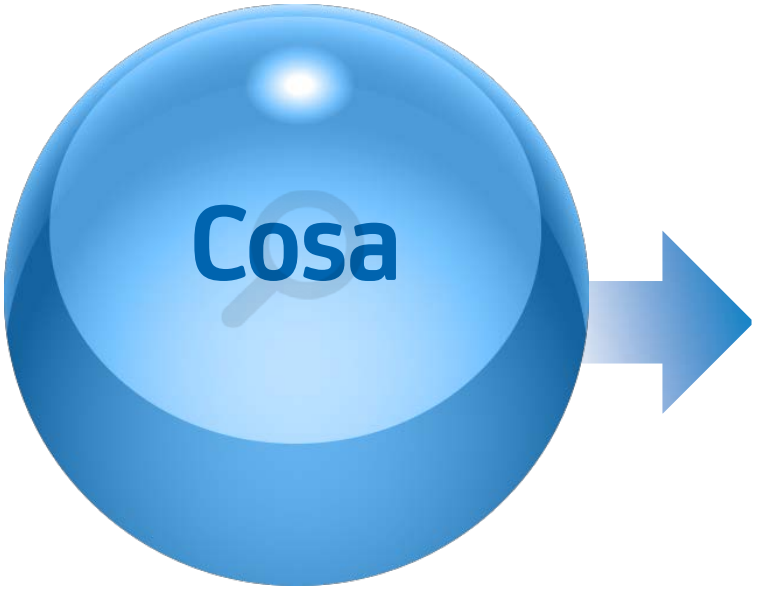
La funzionalità di sicurezza del gateway e i profili delle minacce dovrebbero inoltre essere facilmente aggiornabili, per affrontare i nuovi tipi di minacce emergenti.

Ulteriori informazioni

White paper: Proteggere le API da attacchi e hijacking api.co/APIsecurity

Autorizzare un accesso sicuro e senza soluzione di continuità per le identità valide

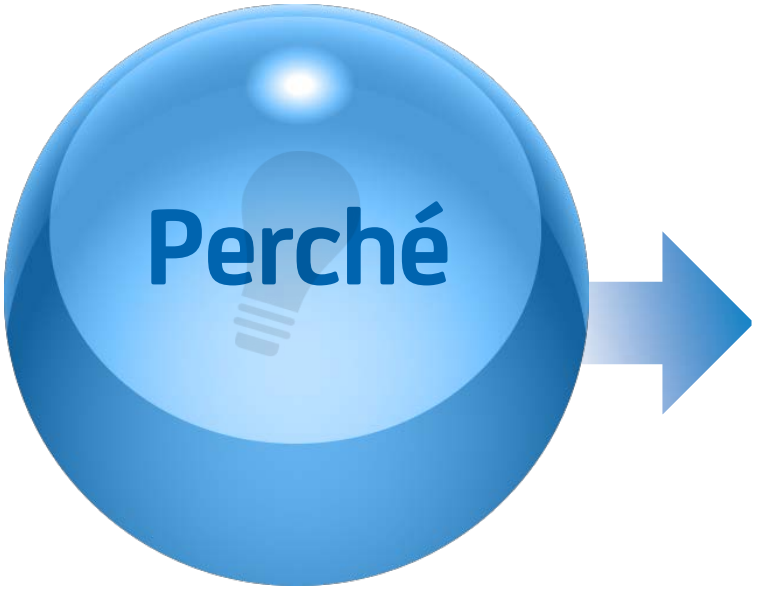
Implementare funzionalità solide di controllo degli accessi, federazione delle identità e login social



Ogni azienda che voglia proteggere appieno le proprie API contro gli attacchi deve fornire agli sviluppatori un framework per controllare le modalità con cui gli utenti accedono alle risorse aziendali tramite le API stesse.

Questo framework dovrebbe comporre un equilibrio tra sicurezza backend ed experience dell'utente finale, sfruttando i principali standard IAM (Identity and Access Management), come OAuth.

Per un equilibrio ideale, il framework dovrebbe essere in grado di utilizzare l'infrastruttura IAM esistente e di consentire l'accesso agli utenti finali tramite login sociali o SSO (Single Sign-On) aziendale.



Il controllo degli accessi è la pietra angolare della sicurezza API: la chiave consiste nell'impedire agli utenti non autorizzati di ottenere livelli inadeguati di accesso alle risorse aziendali.

OAuth è particolarmente utile in quanto consente ai publisher di implementare in modo flessibile livelli adeguati di sicurezza e di eseguire la federazione delle identità da sistemi IAM esistenti e account social.

Sfruttando l'infrastruttura IAM esistente si ottengono anche riduzioni dei costi, velocizzazione dei tempi di configurazione e massimizzazione della gestibilità a lungo termine, impedendo la creazione di silos di identità.

Un API Gateway dovrebbe includere funzionalità out-of-the-box per la costruzione di un'infrastruttura di controllo degli accessi che ruoti intorno alle API, sulla base di standard di utilizzo comune e risorse esistenti.

Il gateway deve essere in grado di integrarsi perfettamente con sistemi IAM leader come CA SiteMinder®, Oracle Access Manager, Microsoft Active Directory e IBM Tivoli.

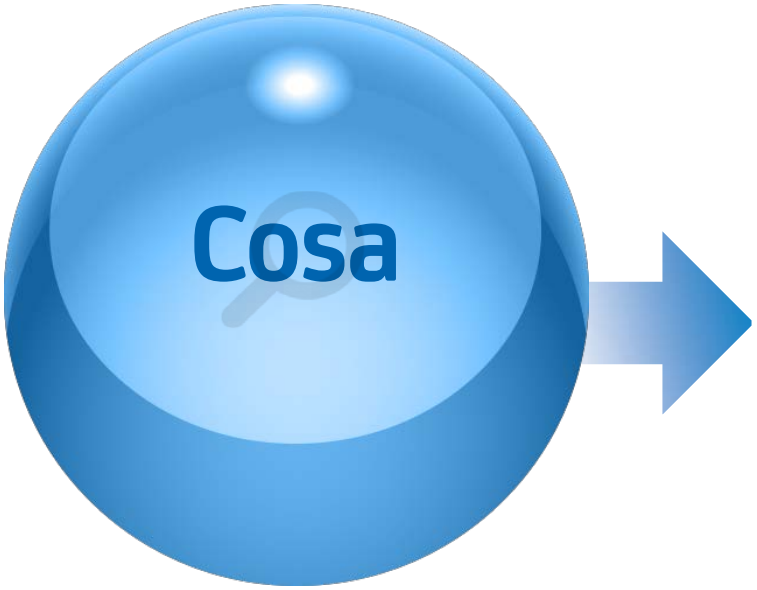
Inoltre, dovrebbe comprendere modelli configurabili per l'implementazione del controllo degli accessi, SSO e login social in casi tipici di utilizzo, sulla base di OAuth e altri standard diffusi.

Ulteriori informazioni

eBook: 5 elementi OAuth essenziali per il controllo degli accessi API api.co/oauthebook

Ottimizzare le prestazioni dei sistemi e gestire il ciclo di vita delle API

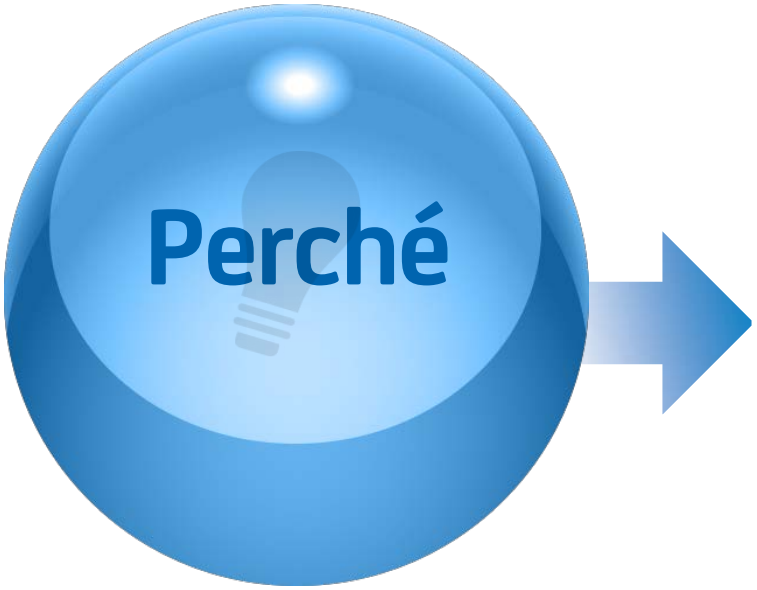
Conservare la disponibilità dei sistemi backend per le API, le app e gli utenti finali



Il traffico API deve essere gestito in modo efficiente per garantire che le app basate sulle API funzionino in modo coerente e che le prestazioni dei sistemi di backend non vengano compromesse.

I dati provenienti dai sistemi backend devono essere erogati in formati leggeri, ottimizzati per i modelli di utilizzo e filtrati in modo adeguato.

Per la fruibilità delle app a lungo termine, è inoltre necessario gestire con attenzione il ciclo di vita di API nel loro passaggio alle fasi di sviluppo, test e produzione.



L'introduzione delle app web e mobile che sfruttano i sistemi backend può portare a una crescita improvvisa del traffico IT, e di conseguenza a blocchi e indisponibilità.

Ottimizzare il flusso del traffico API è fondamentale, per garantire una user experience soddisfacente e coerente per sviluppatori, utenti delle app che dalle API dipendono, così come per gli utenti interni.

La gestione del ciclo di vita delle API rimane al contempo fondamentale per garantire che le app esistenti rimangano funzionali quando API, client e sistemi operativi vengono aggiornati.

Un API Gateway dovrebbe includere funzionalità out-of-the-box per la costruzione di un'infrastruttura di controllo degli accessi che ruoti intorno alle API, sulla base di standard di utilizzo comune e risorse esistenti.

Il gateway deve essere in grado di integrarsi perfettamente con sistemi IAM leader come CA SiteMinder, Oracle Access Manager, Microsoft Active Directory e IBM Tivoli.

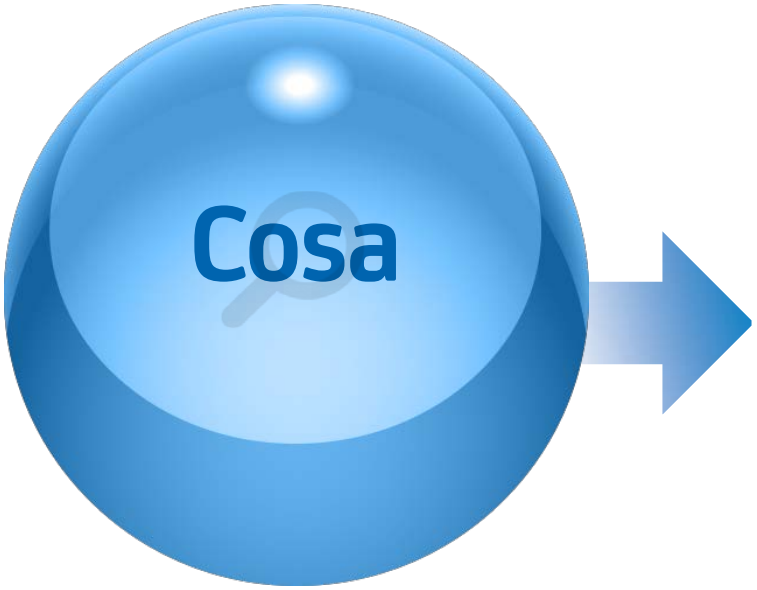
Inoltre, dovrebbe comprendere modelli configurabili per l'implementazione del controllo degli accessi, SSO e login social in casi tipici di utilizzo, sulla base di OAuth e altri standard diffusi.

Ulteriori informazioni

API Tech Talk: Caching e ottimizzazione delle API
api.co/APIoptimization

Coinvolgere, eseguire l'onboarding, formare e gestire gli sviluppatori

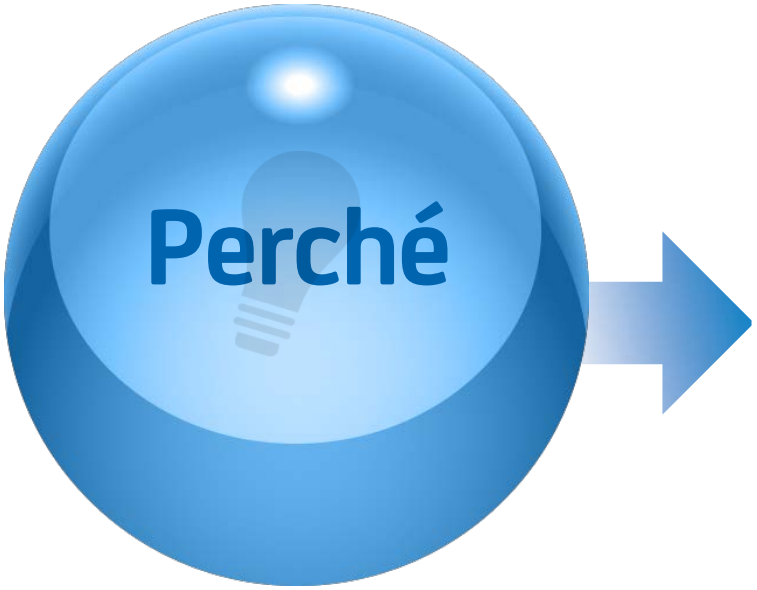
Fornire agli sviluppatori le risorse di cui hanno bisogno per creare app che offrano un valore reale



Gran parte dell'effettivo valore delle API di un'organizzazione deriva dagli sviluppatori, che creano app web e mobile o nuovi sistemi aziendali basati su di esse.

È essenziale mettere a disposizione degli sviluppatori gli strumenti e i materiali di cui hanno bisogno per individuare, formarsi, provare e creare app basate sulle API dell'organizzazione.

Questi sviluppatori possono essere dipendenti interni, partner, consulenti o sviluppatori indipendenti di nicchia. Per ogni gruppo sarà necessario un particolare insieme di risorse, mirate alle sue esigenze.



Gli sviluppatori sono la linfa vitale di qualsiasi strategia di pubblicazione delle API. I publisher di API hanno bisogno che gli sviluppatori creino app effettivamente utili e vantaggiose per dipendenti, partner e clienti.

Per fare in modo che gli sviluppatori creino app veramente significative, il publisher deve essere in grado di attrarre sviluppatori di talento e di fornire loro gli strumenti necessari per sfruttare le API.

Più coinvolgenti e interattivi sono gli strumenti forniti dal publisher delle API per facilitare il lavoro degli sviluppatori e formarli, più utili saranno le app offerte da questi sviluppatori.

Per sviluppatori interni come esterni, la modalità di coinvolgimento e formazione più efficace passa da un portale online interattivo e brandizzato.

Questo portale dovrebbe rendere più semplice agli sviluppatori la registrazione per l'utilizzo delle API e l'accesso a documentazione interattiva, app campione, esempi di codice, strumenti di test e forum di discussione.

Soluzioni efficaci per la gestione delle API includono funzionalità che semplificano la creazione di un portale per gli sviluppatori completo, pre-integrato nell'API Gateway.

Ulteriori informazioni

Webinar: Gli sviluppatori al centro di tutto - L'importanza della gestione delle API
api.co/DevManagement

Conclusione: Distribuire una soluzione completa per la gestione delle API

Con la sempre maggiore centralità delle tecnologie web, mobile e cloud per le aziende di tutto il mondo, l'API emerge come enabler chiave per le imprese smart. Per comprendere il valore delle API ed evitare le insidie connesse all'esposizione dei sistemi aziendali, è di vitale importanza distribuire tecnologia che renda possibile e semplifichi i processi chiave per la gestione delle API, connessi alla composizione dei servizi, alla sicurezza, all'ottimizzazione delle prestazioni, alla gestione del ciclo di vita e al coinvolgimento degli sviluppatori.

L'API Management Suite di CA Layer 7 fornisce tutti i componenti necessari per una gestione delle API efficace a livello aziendale, inclusa una serie di API Gateway progettati per semplificare tutti i processi fondamentali di sicurezza e di gestione API. La suite include inoltre un portale API per il coinvolgimento e la gestione degli sviluppatori, e un toolkit OAuth per garantire una gestione degli accessi sicura e basata su standard per le API aziendali.

Inoltre, la suite offre:

- Una serie di implementazioni alternative: ibride, nel cloud o on-premise
- Sicurezza dei dati e delle app di qualità militare
- Dati analitici sull'utilizzo delle API
- Gestione delle operazioni estendibile a data center distribuiti e cloud
- Adattamento delle app e gestione delle interfacce con connettività SOA avanzata

Informazioni su CA Layer 7

L'economia delle API sta esplodendo, i device mobile proliferano nei luoghi di lavoro e le grandi organizzazioni stanno spostando l'infrastruttura IT nel cloud. Questo crea l'esigenza di una tecnologia in grado di entrare in contatto in modo sicuro con gli sviluppatori esterni, le app mobile e i servizi cloud. All'interno di questo mercato così attivo, CA Layer 7 è all'avanguardia.

Leader di settore, i prodotti gateway di CA Layer 7 semplificano alle imprese la condivisione dei dati con clienti, app mobile e servizi cloud. Erogati sotto forma di appliance di rete hardware, appliance virtuali o software, i nostri prodotti aiutano le grandi organizzazioni ad aprirsi al web, alle reti mobile e al cloud, senza compromettere la sicurezza o le prestazioni.

Nel febbraio 2013, CA Layer 7 è stato riconosciuto come leader nell'ambito della gestione API da una società di analisi primaria come Forrester Research, nel suo report The Forrester Wave: API Management Platforms. Nel giugno 2013, Layer 7 è stata acquisita da CA Technologies, che fornisce soluzioni per le imprese che necessitano di proteggere e gestire ambienti IT complessi a supporto di processi aziendali agili.

Ulteriori informazioni

Data sheet: Suite di gestione API CA Layer 7
api.co/MgmtSuite

CA Technologies (NASDAQ: CA) fornisce soluzioni di gestione IT che aiutano i clienti nella gestione e nella protezione di ambienti IT complessi a supporto di servizi aziendali agili. Le organizzazioni utilizzano il software e le soluzioni SaaS di CA Technologies per accelerare l'innovazione, trasformare l'infrastruttura e proteggere dati e identità, dal data center al cloud.

ca technologies