WHITE PAPER | DICEMBRE 2016

Scegliere la giusta soluzione di API Management per gli utenti aziendali

ca technologies

Le opportunità delle API

Sebbene il concetto di application programming interface (API) possa apparire obsoleto, è in realtà in una fase di profonda trasformazione, perché un numero crescente di aziende, incentivate dalle esigenze di mobility e cloud, sta esponendo le proprie risorse informative a sviluppatori esterni. Esponendo i dati mediante API ai propri sviluppatori, società come eBay, Expedia e Salesforce stanno incrementando con successo le vendite in nuovi mercati. Secondo ProgrammableWeb.com, sono oltre 16.000 le API aperte offerte pubblicamente su Internet: nel 2005 erano solo 32.[1]

Aprire le API agli sviluppatori esterni consente a molte startup tecnologiche di ricreare il proprio modello su piattaforma, promuovendo la formazione di comunità di sviluppatori legate ai propri dati core e alle risorse applicative. Ciò si traduce in un'estensione della portata della startup (si pensi alla rapida crescita di Twitter), in nuovi flussi di ricavo (è il caso di AppExchange di Salesforce.com) o nella fidelizzazione degli utenti (come accade con Facebook).

L'impiego delle API per la condivisione di informazioni e funzionalità con sviluppatori esterni non è limitato alle startup tecnologiche. Un numero sempre maggiore di aziende, spinte da iniziative legate all'integrazione del cloud, della mobility e dei partner, usa le API per collocarsi al centro di un ecosistema di sviluppatori e - così facendo - cercare di raggiungere nuovi utenti, generare revenue e fidelizzare gli utenti. A differenza delle startup, tuttavia, le aziende devono avvicinarsi alla pubblicazione delle API con grande cautela. Per loro, ci sono in gioco reputazione, rispetto delle normative ed esigenze simultanee di clienti, partner, dipendenti e azionisti.

La sfida dell'API Management in azienda

La pubblicazione delle API a una comunità di sviluppatori esterni, sia essa pubblica o di partner, presenta una serie di sfide e rischi per l'azienda. Come proteggere gli asset informativi che vengono esposti da violazioni o attacchi? Come far sì che le API pubbliche diventino servizi affidabili, senza tempi di inattività con impatti negativi sugli utenti delle API stesse? Come amministrare l'accesso e l'uso delle API in modo coerente e basato su policy? Come guadagnare con le API? Come facilitare l'individuazione delle API da parte degli sviluppatori e renderne autonomo l'accesso? Queste domande sono senz'altro importanti per le startup e per le imprese, ma assumono maggiore rilevanza e urgenza per i reparti IT aziendali. Questo non solo perché le aziende non possono permettersi i danni in termini di reputazione che possono derivare da una strategia di API Management impulsiva, ma anche perché hanno posto in essere processi e garanzie IT che devono essere rispettati.

A prescindere dal tipo di API che l'azienda intende esporre, avrà necessità di una soluzione di API Management che intervenga in modo adeguato in alcune aree funzionali di base.

- **Sicurezza delle API** - L'azienda non può consentire l'utilizzo improprio o l'abuso delle proprie informazioni o delle risorse applicative esposte dalle API.
- **Gestione del ciclo di vita delle API** - È indispensabile garantire che gli aggiornamenti delle API non causino problemi quando l'azienda applica un upgrade, adotta nuove versioni delle API oppure le sposta tra diversi ambienti, aree geografiche, data center e cloud.
- **Governance delle API** - L'azienda deve poter controllare e tener traccia dell'aspetto puramente operativo dell'esposizione delle API ai vari partner e sviluppatori, con policy inerenti a misurazione, SLA, disponibilità e performance.
- **Flessibilità del deployment** - Le soluzioni di API management devono integrarsi con l'infrastruttura aziendale esistente.
- **Enablement degli sviluppatori e creazione di community** - È imprescindibile una modalità per eseguire l'onboarding degli sviluppatori, gestirli e assisterli in modo che ottengano il massimo dalle API esposte.
- **Monetizzazione delle API** - In alcune aziende, la pubblicazione delle API non è sufficiente. Esse rappresentano anche una nuova opportunità di ricavo e le diverse soluzioni di API Management offrono diversi livelli di monetizzazione.

Qualunque soluzione di API Management scelta deve necessariamente soddisfare questi requisiti funzionali. Tuttavia, oltre a questi requisiti funzionali, l'azienda si aspetta che la soluzione di API Management fornisca anche alcune caratteristiche operative pertinenti alla sua esclusiva esperienza IT.

- **Sicurezza della soluzione** - Poiché le soluzioni di API Management vengono distribuite nella DMZ, le aziende avranno bisogno di soluzioni API di classe IT solide, capaci di soddisfare una serie di requisiti che vanno dalla protezione dalle violazioni alla compliance PCI, al supporto di FIPS e HSM per la sicurezza della chiave API.
- **Gestibilità della soluzione** - Spesso gli ambienti di sviluppo, test e produzione delle API abbracciano più aree geografiche, data center e cloud. Per questo motivo, la soluzione di API Management scelta dovrà essere adatta agli stili e ai processi di sviluppo specifici dell'azienda.
- **Affidabilità della soluzione** - Le aziende che pubblicano API per finalità commerciali si aspettano un minimo di 5/9 di tempi di attività del servizio e non possono accettare interruzioni. Quali sono le caratteristiche di una soluzione solida e disponibile?

Questo white paper prende in esame i vari requisiti funzionali e operativi elencati per fornire agli IT manager, responsabili web e architetti aziendali alcune informazioni di base per la scelta della giusta soluzione di API Management.

Requisiti funzionali di una soluzione di API Management

Sicurezza delle API

Nella scelta di una soluzione di API Management, gli aspetti legati alla sicurezza rappresentano una delle prime esigenze dei potenziali acquirenti, in particolare quando si tratta di un'azienda che punta a proteggere le informazioni vitali esposte tramite un'API indipendente da standard quali SOAP, REST o JSON. Le problematiche inerenti la sicurezza delle API hanno inizio con il controllo degli accessi. Nel caso delle API esposte all'esterno, occorre essere in grado di:

- Accettare vari tipi di credenziali di autenticazione
- Emettere vari tipi di credenziali per gli sviluppatori
- Supportare diversi schemi di autorizzazione delle risorse, inclusi quelli federati quali OAuth, OpenID Connect e SAML

Nelle aziende, questa sfida è resa più difficile dall'esigenza di integrazione con l'infrastruttura di identità esistente. L'obiettivo principale è quello di ottenere sia flessibilità che integrazione. Per quel che riguarda le policy, è necessario supportare diversi tipi di token di accesso e poter passare da un tipo di chiave API per sviluppatore a un altro, senza toccare il codice. La soluzione deve inoltre supportare una vasta gamma di schemi OAuth, che rappresentano lo standard per la sicurezza mobile e le API, ma anche poter gestire vari stili OAuth quali HMAC e combinazioni con standard aziendali quali SAML. La soluzione deve essere ovviamente compatibile con i sistemi di identità sui quali l'azienda ha già investito, ad esempio CA Technologies, IBM, Oracle e RSA.

La sicurezza delle API non si limita tuttavia al controllo degli accessi. Le API sono finestre di programmazione aperte sui dati. Per questa ragione, la soluzione di gestione scelta deve offrire all'architetto o all'amministratore della sicurezza il controllo granulare sui dati che vengono esposti, su come viene rispettata la riservatezza delle informazioni e sul modo in cui la trasmissione delle stesse è garantita a fronte di potenziali intercettazioni o manomissioni.

Inoltre, la sicurezza delle API si basa sull'integrità dell'API stessa e dei dati e delle funzionalità che espone. Occorre pertanto assicurarsi che le API non siano compromesse da attacchi, eventi DoS o uso improprio. Una soluzione di API Management valida dota l'operatore di una gamma di controlli di protezione dalle minacce in grado di garantire la disponibilità e l'affidabilità dell'API e delle comunicazioni che essa agevola.

Gestione del ciclo di vita delle API

Le API non sono realizzate dal nulla. Come qualsiasi altra funzionalità applicativa, hanno un proprio ciclo di sviluppo che prevede codifica, test e deployment. Si rende pertanto necessario poter registrare le modifiche apportate nel ciclo di vita di sviluppo, a prescindere dal fatto che questa segua un approccio sequenziale o Agile. Ecco perché una soluzione di Api Management deve essere dotata di workflow pienamente funzionali per:

- Pianificare e progettare le API in base a standard del settore
- Integrare e proteggere le API end-to-end
- Testare, distribuire e gestire controllo delle versioni e rollback
- Gestire e monitorare l'utilizzo delle API, compresi report e analisi

Una soluzione di API Management completamente funzionale deve poter consentire l'impiego contemporaneo di più versioni in produzione, per soddisfare i clienti di più lunga data o permettere l'uso di tecnologie di accesso diverse come SOAP (Simple Object Access Protocol), REST (Representational State Transfer) e JSON (JavaScript® Object Notification). Una struttura di gestione del ciclo di vita che consente solo lo sviluppo localizzato non è in grado di soddisfare le esigenze della maggior parte delle aziende moderne. Data la crescente importanza del cloud, sia pubblico sia privato, è necessario che la soluzione di API Management scelta supporti le attività di testing e produzione anche in questo ambiente e consenta di evitare che gli sviluppatori di API siano limitati dalle specificità e dalle topologie di rete.

Governance delle API

Governance è un termine dal significato ampio, spesso utilizzato per accorpare una serie di requisiti di gestione, procedure e visibilità, e definisce i termini e le condizioni in base ai quali un'API viene esposta a uno o più consumatori. Il termine "governance" include i concetti di sicurezza e ciclo di vita ma può articolarsi anche nei vari requisiti in termini di SLA, monitoraggio e reporting. Nel caso delle soluzioni di API Management, la governance indica anche la necessità di abilitare termini e condizioni differenziati per consentire la condivisione dei dati e delle funzionalità delle API a diversi utenti, in funzione delle loro identità, capacità, livelli di registrazione o altri contesti transazionali definibili mediante policy.

Affinché la governance delle API sia efficace, deve essere in primo luogo flessibile. È la tecnologia adottata per controllare la condivisione delle API a dover seguire le preferenze e i processi dell'azienda e non viceversa. Ciò significa che una soluzione di API Management deve essere configurabile in base a qualsiasi SLA, sicurezza, log o altro controllo che adotta le policy. Le policy sono il fulcro della flessibilità e garantiscono la coerenza delle successive implementazioni. Le soluzioni di API Management che vincolano gli amministratori a controlli poco granulari, senza un ambiente di sviluppo integrato delle policy, limitano gli elementi che possono essere amministrati e il modo in cui possono essere controllati.

Flessibilità del deployment

La maggior parte delle aziende dispone di un'infrastruttura progettata in linea con le modalità di business in essere. Nella scelta di una soluzione di API Management è consigliabile prediligere un prodotto in grado di integrarsi nell'ambiente esistente. I team che si occupano di architettura dovrebbero riuscire a gestire la soluzione come se fosse un'estensione della propria infrastruttura e non un ambiente separato. Per ulteriori informazioni su questo livello di integrazione, leggi il solution brief, "Guida per l'architetto all'estensione dell'ambiente ESB/SOA a mobile, cloud e IoT."

Enablement degli sviluppatori e creazione di community

La governance delle API garantisce a chi le pubblica un controllo coerente, ma se un'API non è facile da individuare e utilizzare per gli sviluppatori esterni, il rischio è che non venga utilizzata. Per questa ragione, la maggior parte delle moderne soluzioni supera le tradizionali funzionalità di controllo quali sicurezza, ciclo di vita e governance per fornirne altre che aiutano l'azienda che pubblica le API a esporre le informazioni rilevanti a sviluppatori esterni, spesso tramite portali per sviluppatori. Tali portali offrono un singolo punto di interazione nel quale lo sviluppatore può registrarsi e ottenere un account, richiedere una chiave di accesso all'API, visualizzare le API disponibili e visualizzare codice di esempio.

Un portale per sviluppatori di API incentrato sull'utilizzo aziendale deve:

- Fornire API mobile facilmente utilizzabili (anche per OAuth e OpenID Connect)
- Fornire funzioni di reporting e analisi per gli operatori
- Abilitare la gestione delle relazioni di business

Poiché ogni azienda è diversa, pubblicherà le API con diverse esperienze e priorità; per questa ragione un approccio poco specifico al portale delle API risulterà anche poco attraente, così come accade se il framework di sicurezza, gestione del ciclo di vita e governance delle API risulta generico e omnicomprensivo. Molte aziende possono valutare l'idea di realizzare un portale delle API scomponibile, ad esempio un portale senza etichette specifiche che possa essere personalizzato per adattarsi a una determinata strategia di coinvolgimento degli sviluppatori oppure un portale delle API in cui i componenti possono essere fruiti separatamente tramite un portale degli sviluppatori aziendali preesistente. Anche in questo caso la parola d'ordine è flessibilità.

Monetizzazione delle API

Il concetto di monetizzazione è correlato all'idea di enablement dello sviluppatore. Molte aziende promuovono l'adozione rapida consentendo l'accesso gratuito alle API web e mobile, mentre altre preferiscono opzioni di pagamento a consumo per livelli più elevati di accesso. Anche questo dimostra come non esista una modalità unica e corretta di approcciare il problema della monetizzazione. Alcune opzioni possibili sono:

- Un modello freemium, nel quale è gratuito l'utilizzo inferiore a una determinata soglia della trasmissione dati o delle richieste al client
- Addebito dei livelli specifici di garanzia del servizio o di priorità rispetto ai clienti che non pagano
- Offerta di informazioni o funzionalità premium non disponibili ai clienti che non pagano

Qualunque sia l'approccio adottato, la soluzione di API Management deve poter offrire all'azienda la flessibilità di decidere i propri criteri di generazione dei ricavi. La soluzione deve quindi essere in grado di:

- Acquisire un ventaglio di statistiche di utilizzo con cui creare una base per la misurazione dei consumi
- Fornire capacità avanzate in termini di SLA e classi di servizio, permettendo la definizione delle priorità del traffico
- Comporre API virtuali solo a pagamento che possono essere isolate per i clienti paganti, senza codifica

Requisiti operativi della soluzione di API Management

Sicurezza della soluzione

Poiché la soluzione di API Management risulta essere spesso l'unico componente tecnologico a separare le API aziendali dal mondo esterno, il livello di sicurezza che la soluzione può conferire alle API sarà elevato tanto quanto la sicurezza della soluzione stessa. Se la soluzione è compromessa, lo sarà anche la sicurezza integrata nelle API. Ne consegue pertanto che la sicurezza della soluzione di API Management è un aspetto che merita un'assoluta considerazione da parte delle aziende.

Poiché queste soluzioni assumono un ruolo di intermediazione tra il mondo esterno e le API interne, la prima qualità da valutare è la possibilità di compromissione della soluzione stessa, che dipenderà dal tipo di test di penetrazione al quale la soluzione è stata sottoposta, da quanto sia vincolato l'accesso e dall'aver soddisfatto o meno le principali valutazioni di vulnerabilità. Aspetti di cui tener conto sono le soluzioni testate STIG, la certificazione PCI DSS per le soluzioni che dovranno trasmettere informazioni sulle carte di credito, la compliance FIPS e la certificazione Common Criteria per quelle che devono soddisfare standard di sicurezza governativi più severi.

Per le finalità pratiche più comuni, le aziende considerano soluzioni di API Management basate su proxy per gestire l'intermediazione delle richieste esterne verso un'API interna. I gateway API basati su intermediari offrono il vantaggio di disporre di punti di controllo in linea chiari e di funzioni di isolamento che semplificano la certificazione e l'amministrazione della sicurezza, come nei firewall di rete. Alcune offrono anche il supporto integrato dei moduli HSM per la crittografia delle chiavi API. Poiché le chiavi API rappresentano in molti scenari la principale linea di difesa dell'autenticazione contro le violazioni, adottare la crittografia per proteggere tali chiavi dal furto è senz'altro una strategia prudente.

Gestibilità della soluzione

A differenza di una tipica startup, che potrebbe eseguire il proprio sito web di produzione da una singola istanza Amazon o da un piccolo provider di servizi di hosting, un'azienda presenta in genere vari ambienti di sviluppo e produzione, ad esempio:

- Team di sviluppatori geograficamente distribuiti
- Ambienti di produzione che abbracciano data center globali
- Sistemi di disaster recovery basati su cloud

Alla luce di questi elementi, la gestibilità diventa centrale in qualsiasi decisione. Rispetto ad altre funzionalità, assumono una priorità rilevante aspetti quali la gestione dei cluster di gateway API, il bilanciamento del carico a livello geografico, l'operatività in un ambiente di data center di tipo non presidiato e la gestione dei carichi di picco. Anche in questo caso è vero che non tutte le soluzioni di API Management sono progettate per soddisfare le esigenze specifiche dell'azienda, ed è pertanto necessaria una dovuta cautela nel valutare in che modo le varie soluzioni supportano la gestione dei cluster, il failover, le condizioni di sovraccarico, il disaster recovery e altri aspetti legati alla gestione operativa prima effettuare una scelta specifica.

Affidabilità della soluzione

Una volta che l'azienda ha deciso di intraprendere un programma di pubblicazione delle API, diventa a tutti gli effetti un service provider di API per i propri clienti, che finiranno per affidarsi all'azienda e si aspetteranno tempi di attività continui. In questo scenario, l'affidabilità merita un'attenzione prioritaria nella selezione della soluzione di API Management. L'azienda dovrà individuare una soluzione che integri la ridondanza e riduca al minimo, se non addirittura elimini del tutto, il rischio di tempi di inattività. Le aziende alla ricerca di soluzioni di API Management dovrebbero prendere in considerazione quelle in grado di:

- Essere distribuite on-premise, in cloud o tramite una soluzione ibrida (gateway API on-premise, portale per sviluppatori nel cloud)
- Fornire ridondanza completa indipendentemente dal modello di deployment
- Integrarsi nell'infrastruttura esistente
- Soddisfare gli obblighi di sicurezza

Conclusioni

Poiché non esistono due aziende che abbiano esattamente le stesse esigenze o lo stesso ambiente, non esiste una soluzione di API Management valida a livello universale. Tutte le aziende però condividono il desiderio di eccellenza delle capacità funzionali e operative. Per la maggior parte delle aziende che intendono iniziare a pubblicare le API all'esterno, ciò si traduce nella richiesta di una soluzione di API Management flessibile, basata su policy, che possa soddisfare il rigore di produzione di un service provider di classe dial-tone. A livello funzionale, la soluzione di API Management deve soddisfare una serie di prerequisiti di sicurezza, prevedere cicli di sviluppo comuni, consentire la governance mediante policy, permettere l'onboarding degli sviluppatori, promuoverne il coinvolgimento e consentire la realizzazione del valore economico delle API. Dal punto di vista operativo, la soluzione deve essere sicura, gestibile e affidabile.

Consulta la ricerca per scegliere la soluzione di API Management

Molte delle principali società di analisi si occupano della tecnologia di API Management e pubblicano report con confronti dei diversi vendor, utili alle aziende nella scelta della soluzione giusta per le proprie strategie digitali. Anche siti come IT Central Station possono rappresentare un'eccellente fonte di informazioni per reperire recensioni di clienti e confronti tra vendor.

Per ottenere copie gratuite dei report di confronto dei principali analisti e scoprire le opinioni dei clienti su CA API Management, visita la pagina: **ca.com/it/products/api-management/why-ca-api-management.html**.

Contatta CA Technologies

Siamo a tua disposizione per domande, commenti e feedback.

Per ulteriori informazioni, visita il sito **ca.com/it/api**.

Entra in contatto con CA Technologies all'indirizzo ca.com/it

CA Technologies (NASDAQ: CA) crea software che promuove l'innovazione all'interno delle aziende, consentendo loro di cogliere le opportunità offerte dall'application economy. Il software rappresenta il cuore di qualsiasi business, in ogni settore. Dalla pianificazione allo sviluppo, fino alla gestione e alla sicurezza, CA Technologies lavora con le aziende di tutto il mondo per cambiare il nostro modo di vivere, interagire e comunicare, in ambienti mobile, cloud pubblici e privati, distribuiti e mainframe. Per ulteriori informazioni, visita il sito **ca.com/it**.

1 ProgrammableWeb API Directory, dicembre 2016, www.programmableweb.com/apis/directory

CS200-241661_1216