



WHITE PAPER

## Gateway API: più sono, meglio è?

Perché le aziende adottano molteplici gateway e come gestirli per dare più valore alla tua attività

Scritto da Erik Wilde

È possibile che la tua organizzazione abbia molteplici gateway API. **The State of API Report di SmartBear** mostra come questa sia una tendenza a livello di mercato: del 66% degli intervistati che utilizza uno strumento di API Management, molti ne utilizzano più di uno.

Le aziende finiscono per adottare molteplici gateway API per diversi ottimi motivi: per soddisfare le varie esigenze di sicurezza, passare al cloud, oppure rendere le proprie infrastrutture e attività più resilienti e agili.

Tuttavia, ciò complica anche le cose. Se i gateway API sono molteplici, è più difficile vedere tutte le API che possiedi effettivamente e capire chi le sta utilizzando. È più costoso gestire diversi gateway API che non comunicano tra loro, soprattutto nelle distribuzioni ibride On-Premise e su cloud. Inoltre, le sfide crescono quando si passa al cloud, si aumenta il traffico API tramite l'adozione di microservizi o si aggiungono semplicemente più API per soddisfare le esigenze aziendali.

Axway si impegna a semplificare la gestione delle API e l'integrazione in generale. All'inizio del 2020, abbiamo condotto ricerche sui clienti e sul mercato con l'obiettivo di rispondere a due domande:

- Perché le aziende adottano più gateway API?
- Quali sfide sorgono in caso di molteplici gateway API?

Questo documento riassume ciò che abbiamo appreso e offre una guida per ottenere la massima resa per creare valore aziendale in caso di molteplici gateway.

## 6 motivi per cui le aziende adottano più gateway API

### 01 Gestire il traffico API interno ed esterno

Molte aziende hanno adottato un'architettura a due gateway: un gateway esterno che controlla il traffico tra l'azienda e il mondo esterno e un gateway interno per le varie applicazioni e i flussi di sistemi all'interno dell'azienda. Perché?

#### *Diversi requisiti di sicurezza*

La logica chiave alla base di un'architettura a due gateway sono i diversi requisiti di sicurezza tra il mondo interno ed esterno:

- Un gateway API verso l'esterno facilita la partecipazione agli ecosistemi digitali, ma rende l'azienda vulnerabile anche a potenziali minacce informatiche e richiede quindi rigorose politiche di sicurezza.
- Anche le applicazioni interne devono essere protette, ma l'approccio è diverso. Infatti, il **2020 Data Breach Investigations Report di Verizon** evidenzia che il 30% delle violazioni di sicurezza proviene dall'interno. Questo avviene perché esiste un livello di fiducia più elevato tra le applicazioni interne; gli sviluppatori interni, inoltre, hanno bisogno di un certo livello di flessibilità per testare e innovare e gli utenti interni possono tollerare processi di accesso più lunghi rispetto a partner e clienti.

Un ulteriore vantaggio dell'architettura a due gateway entra in gioco in caso di violazione o attacco informatico su un gateway: l'altro, infatti, può continuare a funzionare in modo che tutte le applicazioni non si arrestino completamente.

### *Ottimizzazione dei costi*

Per risparmiare denaro, un cliente Axway intervistato ha optato per un'implementazione multi-gateway ibrida: Axway funge da gateway esterno e diversi gateway AWS sono in esecuzione nel cloud privato dell'azienda. L'utilizzo dei gateway interni per le chiamate interne ottimizza i costi.

### *Infrastruttura esistente*

Come ha spiegato uno dei nostri clienti, "volevamo avere più funzionalità all'esterno. Abbiamo molti sistemi complessi già esistenti internamente e bisogna conoscere come funzionano tali sistemi. I nostri partner e clienti non li capiranno mai, quindi stiamo cercando di tradurli per loro. Adottiamo una strategia API-first verso l'esterno, ma non verso l'interno."

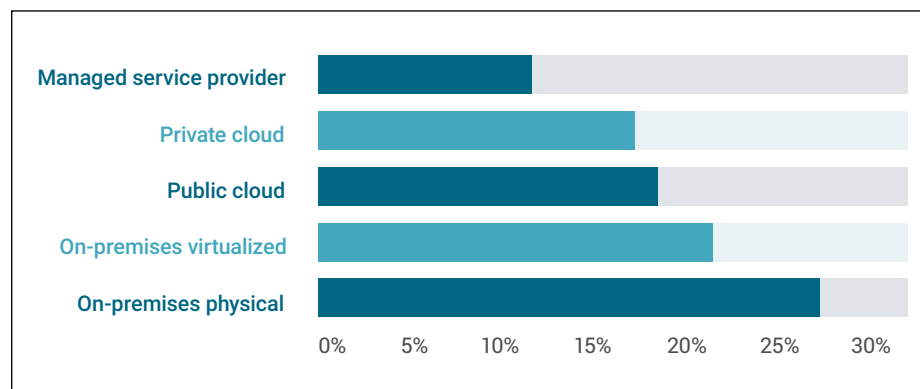
## 02 On-Premise vs. cloud vs. distribuzione ibrida

La maggior parte delle aziende che passano da un'infrastruttura On-Premise al cloud scelgono nuovi gateway API per alcuni motivi: 1) perché un gateway API che ha funzionato bene On-Premise non soddisfa le esigenze cloud emergenti o 2) perché alcune funzionalità di gestione delle API vengono fornite con nuove applicazioni o sistemi basati sul cloud.

In genere, le aziende che operano completamente sul cloud utilizzano due gateway per due o tre anni, durante la transizione di API e funzionalità dal vecchio gateway API On-Premise al nuovo gateway API sul cloud.

Tuttavia, per la maggior parte delle aziende disporre di più gateway API è una soluzione permanente, perché optano per un'architettura ibrida che mantiene alcune applicazioni On-Premise e ne sposta altre sul cloud.

In un **sondaggio che ha interpellato 550 responsabili IT sull'integrazione ibrida**, abbiamo riscontrato che il 51% delle applicazioni viene eseguito su architetture cloud. Sebbene si tratti di un traguardo importante, significa che il 49% delle applicazioni utilizza server fisici o virtuali On-Premise.



Fonte: Axway Hybrid Integration Survey

## 03 Governance centralizzata vs. locale

La legge di Conway afferma che il modo in cui un'organizzazione è strutturata rifletterà il modo in cui il software può essere costruito. Le aziende, in particolare le grandi multinazionali, hanno spesso più gateway perché le diverse unità di business o aree geografiche hanno esigenze e requisiti diversi.



### BNP Paribas Personal Finance

#### Una filosofia e una strategia aziendale

La società leader di credito al consumo **BNP Paribas Personal Finance** commercializza i suoi prodotti attraverso una vasta rete di partner, come commercianti e concessionari automobilistici. Fin dall'inizio del percorso di trasformazione digitale, la società ha deciso che ciascuna delle sue 30 aziende internazionali sarebbe stata responsabile della costruzione, dei test e della gestione delle proprie API, nonché dell'operatività dei propri gateway.

Oltre a permettere a ogni azienda di dare priorità allo sviluppo delle API con il maggiore impatto per gli stakeholder locali, la società era fiduciosa che questo approccio avrebbe offerto una maggiore agilità rispetto a una direttiva top-down, aiutando a far crescere rapidamente il portafoglio API.

[Leggi la storia](#) →



### Novartis

#### Driver normativi

Per **Novartis**, cliente di Axway, i molteplici gateway API garantiscono la conformità ai dati regionali e alle normative sulla privacy.

[Leggi le domande e risposte dei clienti](#) →

#### Cultura

Nel nostro sondaggio, un cliente ha affermato che il suo panorama informatico "è così vasto che probabilmente è possibile trovarci qualunque cosa". Questo cliente ha tentato di centralizzare alcune funzioni di gestione delle API, ma si è scontrato con le unità di business, che hanno preferito fare le cose a modo loro. Oggi l'IT non ha visibilità sulle diverse capacità o risorse digitali implementate in tutta l'azienda.

#### Fusioni e acquisizioni

In alcune aziende, l'utilizzo di più gateway API (temporanei o permanenti) è il risultato dell'unione di entità con sistemi IT completamente diversi.

“

*Ciascuna banca all'interno del gruppo è diversa dalle altre per storia, infrastruttura, sistemi informatici interni, sistemi bancari di base, identity provider e data center.*

Pavel Vybiral, Senior Architect, Erste Group



**Scopri come Erste Group bilancia l'autonomia del paese con l'armonia aziendale** →

“

*Abbiamo cominciato con un'architettura di implementazione API di base, con il gateway di cui disponiamo in Europa e negli Stati Uniti. Vediamo in misura crescente la necessità di ampliare questa architettura con ulteriori gateway in Cina e Giappone, per rispettare i requisiti di residenza dei dati a cui siamo soggetti in quei paesi.*

Pascal Bouquet, Global Head of Architecture for Drug Development presso Novartis

## 04 Risolvere le inefficienze funzionali

Il ruolo di un gateway API è vasto e va dalla **sicurezza**, come l'autenticazione e l'autorizzazione, alla gestione del traffico, inclusi l'instradamento e il bilanciamento, fino al monitoraggio e alla visibilità. Quando un'azienda, o anche una singola unità di business, supera le capacità di un gateway esistente, spesso se ne aggiunge un altro per colmare il divario di funzionalità.

Un cliente Axway con cui abbiamo parlato durante la nostra ricerca inizialmente aveva un unico gateway API che non soddisfaceva tutti i casi d'uso in materia di sicurezza e monitoraggio. L'azienda ha deciso di continuare a utilizzarlo solo per l'ambiente interno e di adottare Axway API Gateway per l'ambiente esterno, creando un'architettura a due gateway.

## 05 Sviluppo vs. testing vs. staging vs. produzione

La maggior parte dei clienti Axway dispone di più gateway API per le diverse fasi del ciclo di vita delle API, evitando confusione su quale endpoint utilizzare in un determinato momento e ambiente. Quando vengono lanciati nuovi progetti, la gestione delle API fa parte di un più ampio ecosistema di componenti.

## 06 Microservizi vs. monoliti

Finora le applicazioni sono state costruite come monoliti: un insieme di codici implementati come una singola unità autosufficiente. Con un'**architettura di microservizi**, gli sviluppatori di software possono gestire un'applicazione come una serie di servizi modulari scalabili e implementabili in maniera indipendente. In genere questo si traduce in traffico API in esecuzione in più service mesh e cloud basati su Kubernetes (da On-Premise ad AWS, Google e Azure).

## 4 sfide da affrontare in caso di molteplici gateway API

### 01 Governance e sicurezza

Le politiche e la maniera in cui vengono impostate sono diverse tra i vari fornitori di gateway API (e persino tra i vari modelli di distribuzione di un singolo fornitore), il che rende difficile un'applicazione uniforme.

Questo rappresenta una doppia sfida:

- La sfida **logica** di dover conoscere tutte le risorse interessate, la loro configurazione di API Management e il tipo di politiche che dovrebbero essere applicate
- La sfida **tecnica** di implementare una politica in diverse soluzioni di API Management, dopo che essa è stata identificata

### 02 Visibilità dell'utilizzo

Dato che ciascun gateway è solitamente legato a un singolo portale, la presenza di più gateway determina un'esperienza a silos, a partire dal lato governance fino al lato utilizzo. Gli utenti non hanno a disposizione un unico luogo per scoprire e accedere facilmente a tutte le API, e i produttori non hanno una visione centralizzata dell'utilizzo delle API.

“

*La crescita significativa e la crescente dipendenza dalle API ci hanno portato a ripensare al modo in cui avremmo impostato API e gateway API. Oggi abbiamo configurato la nostra architettura e i gateway API in container per isolare i carichi di lavoro, che possono essere organizzati in base a funzioni tecniche e processi aziendali. Nel caso in cui si verifichi un problema in un'area, non si estende ad altre aree.*

Darrin Weber, IT Enterprise  
Architecture Lead presso Air Products

Secondo Jérémy Ségura, Enterprise Architect presso BNP Paribas Personal Finance, "dato che ci sono numerosi gateway API, ognuno con i propri cataloghi API, non avevamo nessuna maniera diretta di ottenere una visione unica e accurata di tutte le API utilizzate nell'insieme delle attività. E soprattutto non potevano vedere come i partner stessero usando le nostre API, il che ha reso molto difficile corroborare le nostre idee sulla monetizzazione con dati concreti."

### 03 Compromessi economici

Un'architettura decentralizzata con più gateway API può avere diverse ripercussioni sui costi:

- **È costosa.** Un cliente in Thailandia ha un gateway verso l'esterno gestito da Axway e un gateway verso l'interno gestito da un altro fornitore. Date le ridotte dimensioni del team, si affida ai partner per l'assistenza. Un altro cliente sta effettuando la transizione tra due gateway come parte del passaggio al cloud. Quindi, qualsiasi cosa accada su un gateway deve accadere anche sull'altro, raddoppiando lo sforzo richiesto.
- **Può portare a progetti duplicati.** Avere diversi gateway API rende più difficile sapere quali API l'azienda possiede: i team potrebbero quindi creare un'API già esistente. (Nel [sondaggio di SmartBear](#), il 23% degli intervistati ha indicato la reperibilità come un problema.) Secondo Cloud Elements (2019): The State of Integration Report 2019, un team di sviluppo ha bisogno in media di 41 giorni per costruire una nuova API con funzionalità avanzate.
- **Può ostacolare il riutilizzo.** Come ha spiegato Darrin Weber di Air Products, "il fattore di riutilizzo non misura COSA è il risparmio, ma il NUMERO di volte che si è verificato un risparmio perché non abbiamo dovuto costruire qualcosa di nuovo. La maggior parte delle API richiede molto tempo e risorse per lo sviluppo, in particolare quando si esegue l'integrazione con altri sistemi più grandi, come gli ERP. Ogni volta che si riutilizza quell'API, si risparmiano tempo e risorse".

Nel [sondaggio di SmartBear](#), quasi la metà delle aziende ha identificato la mancanza di riutilizzo multiuso come una sfida, il che è ironico data la definizione stessa di un'API, che dovrebbe essere progettata per il riutilizzo.

### 04 Debugging e monitoraggio

Nel mondo multi-gateway, ogni gateway ha il proprio registro. Il [sondaggio di SmartBear](#) ha riscontrato che i maggiori ostacoli nella risoluzione dei problemi relativi alle API risiedono nel determinare la causa principale del problema (60%) e nell'isolare le API come causa (46%).

Un'azienda intervistata durante la nostra ricerca ha sottolineato che la ricerca dei messaggi difettosi è un processo lungo e complicato, dato che non viene immediatamente a conoscenza di un problema e nel frattempo potrebbero essere passati migliaia di messaggi.

L'automatizzazione del monitoraggio per quanto riguarda il comportamento e l'utilizzo di API è una pratica standard che garantisce sicurezza e affidabilità. La situazione si fa più complessa quando si tratta di tracciare l'utilizzo di API su molteplici gateway che non sono gestiti dalla stessa soluzione di API Management.

“

*Il fattore di riutilizzo non misura COSA è il risparmio, ma il NUMERO di volte che si è verificato un risparmio perché non abbiamo dovuto costruire qualcosa di nuovo.*

*La maggior parte delle API richiede molto tempo e risorse per lo sviluppo, in particolare quando si esegue l'integrazione con altri sistemi più grandi, come gli ERP. Ogni volta che si riutilizza quell'API, si risparmiano tempo e risorse.*

Darrin Weber, IT Enterprise  
Architecture Lead presso Air Products

Come nelle architetture informatiche moderne in generale, l'obiettivo dovrebbe essere quello di smettere di costruire sistemi e iniziare a coltivare ecosistemi. In altre parole, centralizzare laddove è necessario e decentralizzare il più possibile. Lo scopo finale è idealmente quello di fornire più valore all'azienda grazie alle API.

## Sfruttare al meglio molteplici gateway

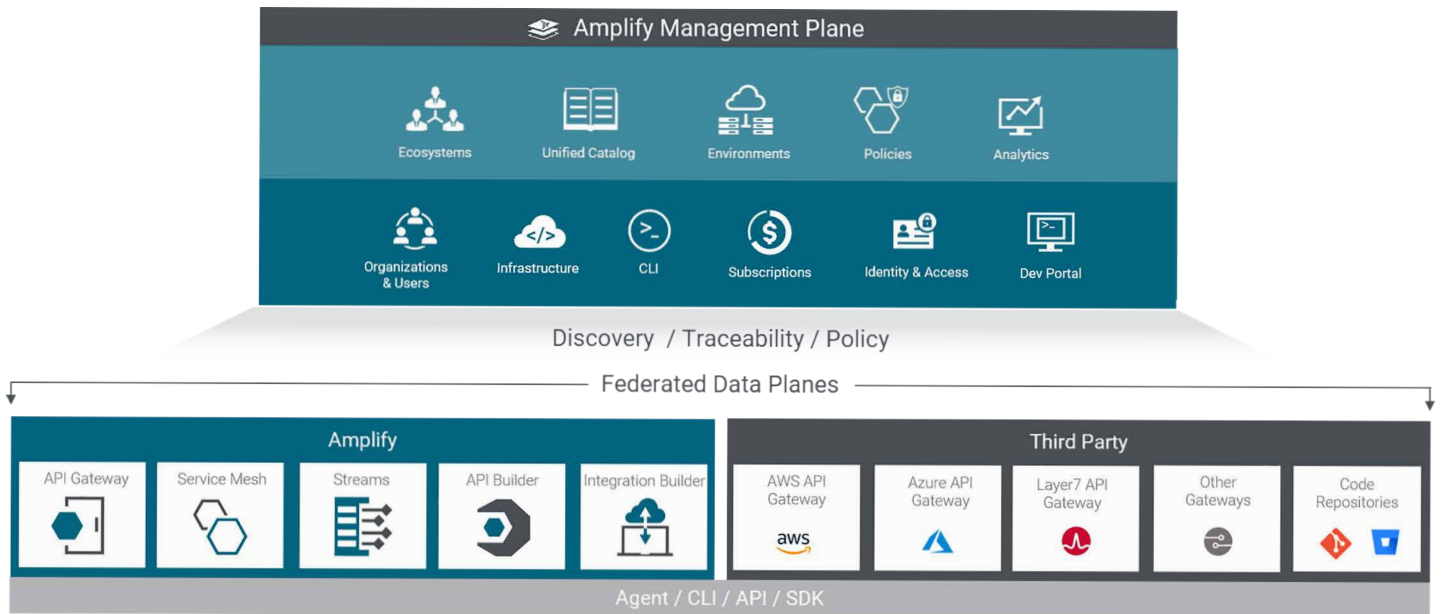
Abbiamo esaminato i vantaggi e gli svantaggi dell'aver diversi gateway API. Ora, il problema è come gestirli in modo sicuro ed efficiente. Come nelle architetture informatiche moderne in generale, l'obiettivo dovrebbe essere quello di smettere di costruire sistemi e iniziare a coltivare ecosistemi. In altre parole, centralizzare laddove è necessario e decentralizzare il più possibile. Lo scopo finale è idealmente quello di fornire più valore all'azienda grazie alle API.

## Rendi la tua piattaforma API aperta

La maggior parte delle tradizionali offerte di API Management permette di controllare solo le "proprie" API. Ma cosa fare con tutte le altre API e integrazioni che connettono sistemi, app, persone, cloud e cose all'interno e all'esterno della tua azienda, sia On-Premise, nel cloud o in modalità ibrida?

Scommettere su un solo cavallo (o un solo gateway API) è sempre una strategia rischiosa. Una piattaforma API Management chiusa ha poca visibilità, ha ripercussioni sui costi e rende difficile l'applicazione coerente degli standard aziendali e delle politiche di sicurezza. Per non parlare del fatto che ostacola la creatività e la velocità nei team, impedendo loro di utilizzare le proprie tecnologie preferite.

La mossa meno rischiosa è progettare tenendo sempre in mente l'apertura e il cambiamento e non presumere mai che tutte le API possano (o debbano) essere gestite con lo stesso gateway. Accogli invece un mondo multi-gateway che promuove il self-service e l'autonomia nei team. Progetta e gestisci una piattaforma API aperta in modo da poter ottenere informazioni dettagliate su ciò che conta (le API stesse, i metadati, l'utilizzo delle API), senza che sia necessario gestire tutto a livello centrale e nello stesso modo. Con una visione unificata, puoi bilanciare la realtà dei prodotti API eterogenei e decentralizzati con la governance di cui hai veramente bisogno.



## La piattaforma Amplify API Management

Per fornire valore con la velocità richiesta dall'azienda, è necessario poter accedere facilmente a tutte le API e ad altre funzionalità digitali (su cloud e On-Premise, con molteplici gateway API e vari modelli di integrazione), indipendentemente da come vengono gestiti. Questo è ciò che ottieni con la piattaforma Amplify API Management: una piattaforma veramente aperta che ti consente di controllare e avere accesso a tutto in un unico posto.

## Gestisci i gateway API di diversi fornitori con Amplify Central

Il cuore della piattaforma è Amplify Central, un piano di controllo e livello di gestione SaaS multi-tenant per la connessione e la gestione di molteplici gateway API e di altre risorse di vari fornitori. Puoi quindi esporli come prodotti in maniera selettiva su Amplify Catalog, affinché possano essere utilizzati dai tuoi team, partner e sviluppatori esterni.

Con Amplify Central, puoi collegare AWS API Gateway, MuleSoft Anypoint, Axway API Gateway e altri tipi di gateway, così puoi finalmente avere visibilità e controllo completi su TUTTE le tue risorse di integrazione e capacità digitali in un unico luogo.

**Maggiori dettagli** →

## Pubblica e condividi con Amplify Catalog

Amplify Catalog supporta sia i provider di API che i consumatori di API semplificando la pubblicazione, l'individuazione, la sottoscrizione e il riutilizzo dei servizi di integrazione, tra cui le API, i microservizi, le integrazioni di applicazioni e i flussi tradizionali.

**Maggiori dettagli** →



## Amplify Catalog presso BNP Personal Finance

Utilizzando gli agent leggeri di Amplify Catalog su ciascuno dei gateway API, BNP Paribas Personal Finance ha sbloccato informazioni granulari e in tempo reale su tutte le API utilizzate nell'organizzazione.

Secondo Jérémy Ségura, architetto aziendale, "quando Axway ci ha parlato di Amplify Catalog, abbiamo immediatamente compreso che ci avrebbe permesso di raccogliere le informazioni di cui avevamo bisogno per mettere in moto la nostra iniziativa di monetizzazione. Dato che Amplify Catalog fa parte dell'offerta SaaS, non è necessario modificare l'architettura dei nostri gateway API: tutto ciò che dobbiamo fare è implementare i client."

"Oggi abbiamo circa 200 API in produzione a livello globale. Quando l'implementazione di Amplify Catalog sarà completa, saremo in grado di identificare facilmente le funzionalità sovrapposte e duplicate nelle nostre API e di adottare come standard le API più efficienti per ogni caso d'uso. Una panoramica singola di tutte le nostre API è anche estremamente preziosa dal punto di vista della governance dei dati e della sicurezza delle informazioni e ci aiuta a incoraggiare l'adozione di standard aziendali e best practice."



Guarda il video del cliente →

Scopri di più sulla piattaforma API aperta di Axway →