



10 façons de moderniser votre stratégie API.

Comment maîtriser la planification, la protection, et les performances des API pour accélérer la transformation digitale et le retour sur investissement ?

API : la voie vers la modernisation et l'innovation continue.

Les API sont basées sur un concept simple : elles relient les données pour créer de nouvelles expériences digitales. Toutes les tendances de la modernisation vers la transformation digitale de l'informatique reposent sur les API. Les projets Cloud utilisent des API. Les logiciels interagissant avec des capteurs IoT utilisent des API. Les applications mobiles contextuelles utilisent des API. Et ce sont les API qui transfèrent les Big Data aux systèmes qui doivent les absorber et les analyser. Elles ne sont pas qu'une simple mode ; elles constituent le socle technologique qui rend possible la mise en place de nouveaux modèles économiques, de nouvelles offres, de nouvelles perspectives et de nombreux autres changements informatiques. Elles sont de plus en plus considérées comme un élément essentiel du succès de la transformation digitale de toute entreprise.

Indépendamment de l'utilisation que vous faites des API, il est crucial que vous adoptiez une approche de planification, de conception, de sécurisation et de gestion stratégique plutôt que tactique. En effet, une vue stratégique vous permettra de répondre aux besoins tactiques actuels, tout en vous offrant la flexibilité indispensable pour vous moderniser et prospérer dans le monde digital.

Ces 10 bonnes pratiques peuvent vous aider à moderniser votre infrastructure informatique avec une stratégie à base d'API qui soutient l'innovation continue tout en optimisant les coûts, la flexibilité et la sécurité :

01

Visez un ROI positif.

02

Adaptez votre stratégie de gouvernance à vos besoins.

03

Utilisez une couche d'API commune pour soutenir le Cloud.

04

Coordonnez la surveillance technique et métier.

05

Garantissez une expérience utilisateur positive et respectez les SLA.

06

Organisez des audits régulièrement.

07

Faites de la sécurité une fonctionnalité et non un obstacle.

08

Maîtrisez la gestion des identités.

09

Distinguez les règles des API.

10

Utilisez la limitation et la gestion des quotas.

Le changement est permanent et révolutionne l'informatique d'entreprise

Les innovateurs digitaux d'aujourd'hui ont prouvé la valeur d'une approche IT plus agile. Une architecture IT moderne à plusieurs vitesses sépare les systèmes d'enregistrement plus lents des systèmes d'engagement plus rapides, qui gèrent les interactions avec les clients, les partenaires, les communautés de développeurs et les employés.

Ce sont ces systèmes d'engagement qui doivent s'adapter à des changements constants et à une innovation continue. Les API, et les méthodes que vous utilisez pour les gérer, permettent à ces deux rythmes de coexister.



01 **Visez un ROI positif.**

Pour une infrastructure informatique moderne, il n'est plus viable d'investir pour simplement couvrir les besoins d'un projet actuel. Il faut mettre en place un certain nombre de ressources suffisamment génériques pour pouvoir être appliquées à différents projets. La réutilisation des capacités améliore l'efficacité, tout en réduisant les coûts et en augmentant le retour potentiel des projets.

Mais vous vous demandez sans doute par où commencer. Il faut s'attaquer en premier lieu aux projets qui offrent le plus de bénéfices en un temps réduit. Ces projets généreront des résultats rapidement et optimiseront les performances de l'organisation, tout en subventionnant une infrastructure qui pourra ensuite être déployée pour d'autres projets.

Parallèlement, il est vital de remporter l'adhésion des cadres en charge du budget. Trop souvent, les décideurs pensent que les demandes de dépenses du service IT ne servent qu'à « acheter des équipements flambant neufs ». Pour changer leur perception, il est important de leur expliquer les changements fondamentaux qui s'opèrent, à la fois au niveau macroéconomique et au niveau de l'entreprise. Cela leur permettra d'évaluer à leur juste valeur les projets que vous proposez.

Avec le soutien des bonnes personnes, vous ne perdrez plus de temps à discuter de ce que les différentes divisions doivent payer. Vous mènerez tout simplement votre projet à bien.

Rendez les ressources aussi génériques que possible, afin qu'elles puissent donner des résultats rapidement et être déployées pour répondre à des problématiques diverses.

02 Adaptez votre stratégie de gouvernance à vos besoins.

La gouvernance est une question d'équilibre. Il est évidemment important de superviser les projets, les rôles et les budgets, mais il est difficile de définir des paramètres distincts pour des projets, lorsque l'organisation est soumise à des fluctuations perpétuelles. Il faut mettre en place un processus de gouvernance suffisant pour assurer le contrôle, sans ralentir l'ensemble du processus de conception de produits et de services.

Une solution telle que Axway AMPLIFY™ API Management permet d'instaurer une gouvernance solide, mais pas trop contraignante, en vous permettant de définir un large catalogue d'API et de le mettre à disposition via un portail d'API en libre-service. Un portail peut ne pas sembler être un besoin essentiel dans le cadre du projet initial, mais en le prévoyant dès le départ, vous pourrez envisager la gouvernance dans sa globalité. Ainsi, des aspects tels que le processus de validation d'une API pourront être appréhendés dans le cadre d'une stratégie d'API plus large.

Au fil du temps, vous pouvez utiliser le portail pour partager en toute sécurité des bonnes pratiques, des exemples de code et des ressources avec un nombre croissant d'équipes internes, de partenaires et de communautés de développeurs d'API. Il s'agit en fait d'un investissement limité pour assurer que votre plateforme est, autant que possible, prête pour l'avenir.

03 Utilisez une couche d'API commune pour soutenir le Cloud.

De nombreuses personnes pensent que les API impliquent la migration de toutes vos informations dans le Cloud ou, au moins, dans de nouvelles architectures. La réalité est différente. Les solutions sur site persistent pour diverses raisons. Les applications Cloud ne s'intègrent pas aux applications sur site d'un coup de baguette magique.

Pour faire le lien, vous devez unifier les applications sur site dans une couche API commune, qui leur permet de communiquer avec le monde extérieur tout en étant exécutées sur des architectures et infrastructures conventionnelles. L'idée d'une couche tampon s'étend également aux éléments d'infrastructure, canaux de communication, appareils mobiles, composants d'application qui nécessitent une interaction entre les ressources sur site et le monde extérieur.

AMPLIFY API Management est un exemple d'investissement avisé qui peut être déployé dans le Cloud, sur site ou dans une configuration hybride, et utilisé pour créer une couche API commune. Dans ce cas également, la réutilisation d'éléments pour des projets ultérieurs réduira les coûts à long terme et vous aidera à maximiser votre ROI, facilitant ainsi l'adoption de vos futurs projets.

Envisagez la gouvernance comme un élément essentiel de la rationalisation de chaque projet de bout en bout.

Créez une couche d'intégration qui relie les solutions derrière le pare-feu et celles de l'autre côté, et qui gère les erreurs et les problèmes d'impédance d'API.

Avantages d'un catalogue d'API et d'un portail en libre-service :

- Un portail d'API contient des composants réutilisables qui peuvent vous aider à passer d'un projet réussi ou d'une équipe à un grand nombre d'utilisateurs à l'échelle de l'entreprise, de façon à réduire le coût et les délais des produits et projets ultérieurs.
- En implémentant un large catalogue d'API, vous pouvez répartir le coût de la gouvernance sur plusieurs projets et réduire ainsi le coût pour chaque projet distinct.

04 **Coordonnez la surveillance technique et métier.**

Aujourd'hui, l'informatique est caractérisée par une itération rapide et de nombreux petits projets. Chaque projet ou application est souvent constitué d'un vaste ensemble de composants répartis, et les développeurs peuvent collecter et choisir ceux qui correspondent le mieux à leur utilisation spécifique. En raison de ce paradigme, il est encore plus important de mettre en place une surveillance robuste, à la fois métier et technique.

Par le passé, la surveillance technique (disponibilité, performance, etc.) était généralement distincte de la surveillance métier (coûts, ROI, etc.). Aujourd'hui, elles sont étroitement liées. Il faut se poser deux questions essentielles :

1. Vous devrez transmettre les données de performances techniques et métier extraites aux autres systèmes d'enregistrement. Par exemple, votre application financière doit pouvoir tenir compte des données métier provenant d'une plateforme technique. C'est essentiel pour relier les différents systèmes et mettre en avant la valeur de l'initiative API.
2. Vous devrez intégrer les données liées à la surveillance technique et métier, provenant de la solution de gestion d'API, aux autres données, qu'elles proviennent de l'organisation ou de l'extérieur. Dans ce contexte, la visibilité et les métriques métier de bout en bout jouent un rôle clé et ce n'est qu'en intégrant de multiples sources de données que vous pourrez obtenir une vue claire.

AMPLIFY API Management comprend des métriques métier et techniques complètes qui apportent une visibilité vous permettant de savoir où et comment votre programme API remplit ses objectifs ou non. Les métriques mobiles mesurent les performances au niveau de l'utilisateur final. Des tendances de référence permettent de mieux anticiper les situations anormales. Des tableaux de bord analytiques peuvent être personnalisés pour une fonction métier spécifique et des métriques peuvent être exportées et combinées avec des données externes pour permettre une compréhension plus approfondie.

Assurez-vous d'avoir une visibilité opérationnelle en temps réel pour surveiller les performances des API, ainsi que des métriques d'adoption et d'utilisation pour évaluer le succès commercial d'un programme d'API.





05 **Garantissez une expérience utilisateur positive et respectez les SLA.**

La bonne pratique numéro 4 explique qu'il est vital de permettre à toutes les personnes de l'organisation d'obtenir une visibilité claire des performances techniques et métier de la plateforme d'API. Outre le fait qu'elle justifie l'existence de la plateforme et ce qui est basé sur celle-ci, cette visibilité est essentielle pour garantir la satisfaction des utilisateurs et le respect des SLA.

La violation des accords sur les niveaux de service peut avoir des conséquences graves. Par exemple, des études ont montré que même une légère augmentation des temps de chargement de page pour une application ou un service peut avoir un impact important sur les taux de conversion. Si votre expérience à base d'API est constituée de nombreux composants communiquant chacun via des API différentes, il existe un risque significatif de dégradation ou d'interruption de service. Si ce risque se concrétise, les utilisateurs seront mécontents et vous encourrez des amendes pour non-respect des SLA.

Afin de garantir une expérience utilisateur positive ainsi que le respect des SLA, vous avez besoin d'une vue claire des niveaux de service attendus pour les différents composants de la plateforme. Des métriques et des analyses prédictives telles que celles fournies par AMPLIFY API Management vous permettent de mesurer ce qui est important, et de donner aux utilisateurs métier et techniques la capacité de surveiller, prédire et agir de façon proactive sur les changements de performance.

06 **Organisez des audits régulièrement.**

Audit. Ce simple mot fait probablement frémir tout votre service informatique. Pourtant, les audits présentent des avantages. En organisant régulièrement des audits sur les exigences de sécurité internes, les exigences réglementaires externes ou même une enquête ponctuelle sur une activité suspectieuse, vous pouvez garantir que les services sont utilisés correctement, par les bonnes personnes, à des fins appropriées.

Que vous considériez les audits comme une opportunité ou une contrainte, ils constituent généralement une exigence critique non négociable pour votre plateforme d'API. Par conséquent, assurez-vous d'adopter une solution telle que AMPLIFY API Management, qui peut capturer et archiver les pistes d'audit pour rationaliser le processus.

Déterminez les SLA appropriés pour différentes parties de votre plateforme d'API et pour chaque application ou service. Ainsi, les SLA deviendront un outil utile, directement lié à la valeur métier.

Les données d'audit d'utilisation sont également une source considérable d'informations qui peuvent être exploitées pour obtenir des informations dont la valeur augmentera au fil du temps.

07 **Faites de la sécurité une fonctionnalité et non un obstacle.**

Auparavant, un architecte sécurité pouvait délimiter une frontière autour de l'infrastructure informatique de l'entreprise. Tout ce qui était à l'extérieur faisait partie de la zone rouge et tout ce qui était à l'intérieur faisait partie de la zone verte. Un pare-feu réseau séparait ces zones et offrait une fausse impression de sécurité, laissant croire que tout ce qui était dans la zone verte était inoffensif.

Aujourd'hui, il n'y a plus de zone rouge et de zone verte. Grâce aux API, l'environnement IT de l'entreprise s'étend au-delà de l'infrastructure sur site et le pare-feu s'étend au Cloud, aux appareils mobiles, à l'IdO et aux différentes communautés d'utilisateurs internes et externes. Ces connexions doivent être sécurisées, ce qui est impossible avec un pare-feu classique, puisqu'il n'y a pas de frontière logique. De fait, la sécurité doit être assurée au niveau de l'infrastructure à l'aide d'une passerelle d'API qui contrôle les accès et protège les données en provenance et à destination des systèmes, des applications et des personnes.

Il faut toutefois être vigilant. Il peut être tentant de permettre aux développeurs de mettre en place leur propre sécurité d'API en mélangeant logique de sécurité et logique métier. Cette approche n'est pas gérable. Une solution telle que AMPLIFY API Management vous permet d'intégrer la sécurité au sein de votre infrastructure d'API et de la gérer de façon centralisée, de façon à permettre aux employés chargés des opérations et de la sécurité d'assumer leur rôle, puisqu'ils contrôlent les éléments importants, tels que les clés d'API et les identifiants utilisateur.

Si vous sécurisez les données, vous pouvez satisfaire à des exigences élevées de sécurité et de confidentialité à l'échelle d'une architecture moderne, reliée à divers services sur site, Cloud, mobiles et IdO.

08 Maîtrisez la gestion des identités.

Les API sont faciles à utiliser et à réutiliser. C'est l'un de leurs principaux avantages. Il est relativement simple pour les développeurs d'utiliser des API dans une application mobile ou d'appeler une API Cloud à partir de Salesforce.com ou d'Amazon Web Services. La facilité d'utilisation est également profitable aux utilisateurs finaux qui disposent d'applications plus sophistiquées et plus conviviales sur leurs appareils mobiles.

Mais cette facilité d'utilisation s'accompagne d'un problème d'identité. Les utilisateurs accèdent désormais à des services sur site et dans le Cloud, via diverses interfaces, notamment mobiles. Il est important qu'ils n'aient pas à se connecter individuellement à chaque service. Ce n'est pas pratique et cela pourrait les encourager à utiliser le même mot de passe partout, ce qui constituerait un risque de sécurité élevé si ce mot de passe était compromis.

AMPLIFY API Management prend en charge les normes d'identité actuelles, comme OAuth 2.0, et permet de résoudre ce problème en s'appuyant sur la fédération des identités. Cette fonctionnalité étend l'authentification unique aux applications Cloud, mobiles et sur site et offre différents niveaux d'autorisation en fonction des préférences de l'utilisateur ou du fournisseur. Les boutons « Se connecter avec Google » ou « Se connecter avec Facebook » que l'on voit fleurir sur Internet sont des exemples d'authentification unique soutenue par des API, à l'aide de normes telles qu'OAuth et OpenID.

Implémentez la fédération des identités et l'authentification unique au niveau de l'infrastructure pour centraliser la gestion, simplifier l'expérience utilisateur et créer un environnement plus sécurisé.





09 Distinguez les règles des API.

L'exposition de services tels que des API facilite leur gestion, mais nécessite également que les règles soient séparées des API. En effet, les règles s'appliquent indépendamment pour chaque API, en fonction de l'identité de l'utilisateur, du contexte et de l'application.

Étant donné que les règles imposent des exigences métier et techniques, elles doivent reposer sur des politiques de niveau supérieur que les analystes et acteurs métier peuvent comprendre. Elles doivent également être suffisamment flexibles pour être pilotées par les données, les rôles, l'utilisation des API et d'autres critères. Si ce n'est pas le cas, la définition et la modification de règles prendront trop de temps et rallongeront les délais de déploiement.

Les règles doivent aussi être réutilisables pour économiser du temps et de l'argent et éviter les erreurs. Une organisation qui compte 100 opérations d'API peut avoir seulement quelques règles réutilisables, applicables partout, telles qu'une règle de limitation d'utilisation. En distinguant la gestion des règles des API, vous pouvez retirer d'autres avantages. Par exemple, les cycles de vie de règle peuvent être gérés séparément des cycles de vie d'API ; ainsi, un changement d'API ne nécessitera pas de changer de règle.

La gestion des règles peut être complexe et nécessite des compétences spécifiques. Il est pertinent de permettre à des spécialistes de définir des règles, à l'aide d'un outil tel que AMPLIFY API Management Policy Studio, qui rationalise la réutilisation et comporte plus de 200 filtres de règle prédéfinis.

Permettez aux développeurs de se focaliser sur la logique métier, sans avoir à définir et à gérer des règles.

10 Utilisez la limitation et la gestion des quotas.

Lorsque vous ouvrez les transactions soutenues par des systèmes internes au monde extérieur, vos volumes de transactions annuels peuvent facilement être multipliés par 4 ou 5. Si vous ne l'anticipez pas, votre infrastructure peut être dépassée. C'est pourquoi la limitation et la gestion des quotas sont essentielles à la réussite d'un programme d'API. Elles vous permettent d'appliquer des règles pour différents niveaux d'accès à une API (par exemple, « 10 000 requêtes par jour » ou « 1 000 appels d'API par seconde »).

La limitation est liée au réseau utilisant une passerelle d'API et non à l'application elle-même. De fait, lorsque le back-end de l'API est affecté par un pic de trafic, il est souvent trop tard pour agir. Au niveau du réseau, il est possible de gérer les pics d'utilisation en mettant le trafic en file d'attente ou en le réacheminant.

AMPLIFY API Management est un exemple de solution qui associe la limitation et la gestion des quotas à base de politiques avec la prise en charge complète du cycle de vie des API, afin de simplifier toutes les phases, du déploiement initial à l'adoption virale, et d'apporter la fiabilité dont votre entreprise a besoin pour passer au monde digital.

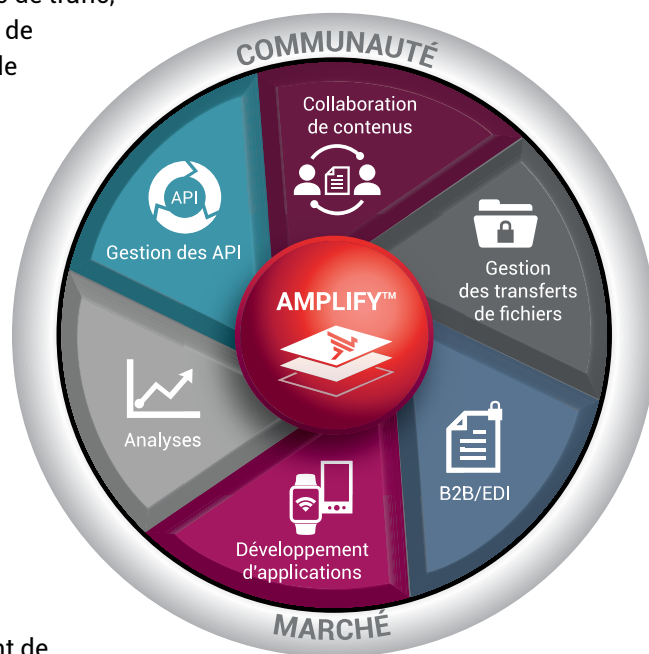
Et ensuite ?

Les API sont un outil précieux pour la modernisation des services informatiques. Elles libèrent les données, renforcent l'agilité, stimulent l'innovation et offrent un retour sur investissement plus rapide. C'est pourquoi il est d'une importance cruciale de repenser les tâches liées aux API et les aspects transverses du développement de produits et solutions.

Cette liste est loin d'être exhaustive, mais il s'agit d'une base solide pour planifier et implémenter un programme d'API qui vous permettra de réussir à l'ère du digital. L'approche de modernisation pragmatique et stratégique définie par ces meilleures pratiques éprouvées a été un élément moteur dans le développement de AMPLIFY API Management, qui offre un ensemble complet de services de bout en bout qui simplifient l'accès aux données d'entreprise, prennent complètement en charge le cycle de vie des API et rationalisent la conception de vos applications pour accélérer la génération de valeur pour votre entreprise.

AMPLIFY API Management fait partie de la plateforme hybride d'intégration, d'engagement et de collaboration Axway AMPLIFY, qui inclut également les solutions de gestion des transferts de fichiers, d'analyse, de développement d'application, d'intégration B2B et de collaboration de contenus et de partage de fichiers sécurisé.

Imposez des quotas et empêchez l'utilisation incorrecte des API avec une limitation basée sur les priorités, les performances actuelles et l'utilisation globale.



**Essayez gratuitement
AMPLIFY API
Management en ligne**

ENREGISTREZ-VOUS MAINTENANT

axway.com/api-management