MuleSoft

LIVRE BLANC

Sécurité des API : top 5 des bonnes pratiques

Comment protéger votre patrimoine numérique

Sommaire

Synthèse

Les équipes IT ont pour responsabilité de sécuriser le patrimoine numérique de leur entreprise, tout en devant faire face à des restrictions budgétaires. Quant aux responsables IT, ils doivent trouver le moyen de sécuriser les API à moindre coût, tout en sachant que la moindre faille de sécurité peut être lourde de conséquences.

La confiance des clients est longue à acquérir et rapide à perdre : une seule violation de données peut faire fuir vos clients les plus fidèles. De ce fait, la mise en place d'une stratégie de sécurité globale des API est incontournable. C'est ce point d'entrée, le plus vulnérable, qui est visé en priorité par les acteurs malveillants.

Ce livre blanc revient sur les défis rencontrés par les équipes IT lors de la mise en place de mesures de sécurisation des API. Après une présentation des cinq étapes clés nécessaires pour relever ces défis, nous reviendrons sur la nécessité d'un déploiement rapide et nous vous donnerons des conseils sur la mise en place d'une stratégie complète de sécurité.

Introduction

À mesure que les entreprises s'efforcent de créer des expériences client de qualité, leur architecture numérique doit évoluer pour répondre à de nouvelles exigences. Si elles se sont rapidement tournées vers les API pour garder une longueur d'avance et assurer la pérennité de leur patrimoine numérique, la multiplication de celles-ci est progressivement devenue problématique.

L'écosystème typique d'une entreprise compte plus de 500 API, le plus souvent caractérisées par des formats et des environnements hétérogènes. Les environnements de conception peuvent respecter des normes de sécurité différentes, ce qui favorise les menaces de la part d'acteurs malveillants.

Des négligences en matière de cybersécurité peuvent coûter très cher aux entreprises. Si toutes celles qui traitent des informations clients doivent prioriser la cybersécurité, certains secteurs de la finance et de la santé ont encore plus à perdre en raison de réglementations externes telles que l'HIPAA. Les gouvernements ont également adopté une position ferme concernant les protections pour les clients, et les violations de ces lois peuvent entraîner de lourdes amendes.

Bien qu'une entreprise puisse survivre financièrement à d'éventuelles amendes, les atteintes à l'image de l'entreprise et la perte de confiance qui en résulte peuvent être difficiles à réparer. La confiance des clients est en effet aussi complexe à acquérir que facile à perdre en un temps record. Une violation de données, et tout est fini.

Cette situation place les responsables des équipes IT dans une position délicate, d'autant plus que les équipes sont actuellement appelées à produire plus avec moins de ressources. D'autre part, ce sont ces mêmes équipes qui sont chargées de sécuriser toutes les API du patrimoine numérique de l'entreprise, ce qui exige un certain laps de temps.

Le besoin de sécurité s'accroît à mesure que les équipes créent des automatisations et des API.

Les API servent désormais de rampe de lancement pour l'automatisation. Celle-ci permet à tous les collaborateurs de prendre part à des projets innovants, sans avoir à coder, contribuant ainsi à la réalisation des objectifs de l'entreprise.

La sécurité des API face à deux challenges

Actuellement, les équipes IT sont obligées de produire plus avec moins de ressources, les besoins des entreprises étant supérieurs à leurs capacités. Un défi difficile à concilier avec la sécurité des API, pourtant indispensable à la préservation du patrimoine numérique.

Outre la nécessité de surmonter la demande accrue en matière d'IT, deux obstacles majeurs se dressent sur la route de la sécurisation des API.

01 La multiplication des API

Alors que le patrimoine numérique d'une entreprise se développe, les systèmes restent souvent cloisonnés les uns par rapport aux autres. Pour assurer leur transformation numérique, de nombreuses entreprises ont rapidement adopté les API afin que tous les collaborateurs accèdent aux données. Parfois, les équipes adoptent des API prédéfinies ou sur mesure proposées par des partenaires ou des fournisseurs, ce qui permet de partager des données et de créer des expériences de qualité. Au même titre que les autres composants du patrimoine numérique, le volume toujours croissant d'API doit être sécurisé.

Mais la multiplication des API a réduit la visibilité globale sur leur parc, ce qui favorise les potentielles attaques malveillantes.

EN CHIFFRES

90 % des applications web risquent davantage d'attaques avec des API exposées.

Source : Gartner MQ Application Security Testing

200 % d'API en plus

Les entreprises ont connu une hausse de 200 % du nombre d'API au cours des 12 derniers mois.

Source : 451 Research API Security Trends Survey

Des problèmes liés à la qualité dans un paysage hétérogène

Au fur et à mesure que le patrimoine numérique d'une entreprise se complexifie, des problèmes cruciaux affectent ce paysage aussi hétérogène que tentaculaire :

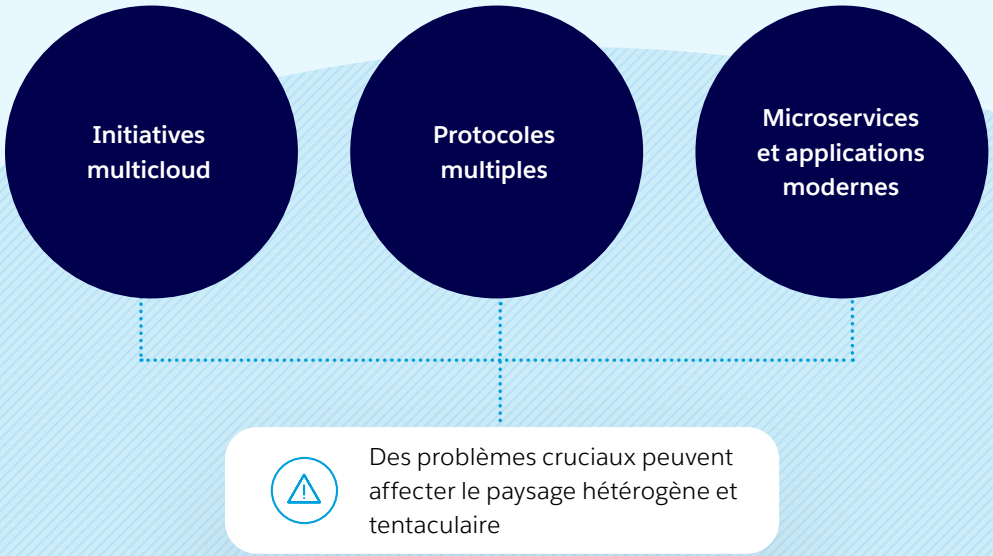
- **des initiatives multi-cloud :** lorsqu'une API est développée puis déployée sur différentes plateformes cloud ayant des exigences de sécurité variables ;
- **des protocoles multiples :** lorsque des API sont conçues et développées à l'aide de protocoles modernes, tels que AsyncAPI et GraphQL ayant différentes implémentations de sécurité ;
- **des microservices et des applications modernes :** des API développées pour soutenir ces initiatives, avec une sécurité incomplète.

02 La standardisation des API

La standardisation garantit que toutes les API du patrimoine numérique respectent les normes de sécurité convenues et définies. Toutefois, ce processus n'est sûr que si toutes les API sont conformes aux règles définies, car il suffit d'une seule API défaillante pour être vulnérable aux violations de données.

Pour parvenir à la normalisation de votre architecture numérique, les équipes IT doivent créer des API de haute qualité et sécurisées, sans toutefois compromettre la vitesse de développement des projets.

Pour compliquer encore la situation, la plupart des entreprises utilisent des API développées sur différentes plateformes. Or la fragmentation peut conduire les responsables IT à penser que les API respectent les « bonnes » normes de sécurité, alors que chaque fournisseur possède ses propres normes. Il appartient donc aux entreprises de les déterminer et de les appliquer.



5 étapes pour sécuriser votre patrimoine numérique

Pour protéger leurs API, les responsables IT doivent prendre en compte cinq étapes essentielles. Celles-ci s'appuient les unes sur les autres et accompagnent la mise en place d'une stratégie de sécurité adaptée.

01 **Protection des API**
02 **Gouvernance des API**
03 **Sécurité des données des API**
04 **API discovery**
05 **Tests de sécurité des API**

01 Protection : contrôlez les accès et autorisations

Les développeurs qui créent des API connaissent bien les processus d'autorisation. Il s'agit des contrôles mis en œuvre pour déterminer qui peut accéder aux données d'une API. Cette étape fondamentale en termes de sécurité des API doit s'accompagner de mesures supplémentaires. Une bonne pratique consiste à mettre en place un contrôle strict de l'accès aux API ainsi que des couches de protection.

Ce contrôle strict peut être mis en œuvre de différentes manières, notamment par l'authentification multifactorielle (MFA) et les passerelles d'API. La mise en œuvre d'une passerelle d'API freine l'expansion qui accompagne la multiplication des API.

Avec une passerelle d'API, des règles supplémentaires peuvent être mises en œuvre, telles qu'une stratégie de limite de charge. Il s'agit d'une règle qui limite le nombre de fois qu'une API est appelée afin d'éviter un déni de service. C'est la garantie que toutes les API contrôlées par la passerelle respectent des règles et des autorisations spécifiques.

La définition d'autorisations renforce la sécurité en contrôlant le niveau d'accès attribué à l'utilisateur d'une API : peut-il lire, écrire ou même supprimer vos API ?

02 Gouvernance : gérez votre patrimoine numérique

Une stratégie de pointe pour sécuriser les API consiste à établir un modèle de gouvernance centralisé afin de définir les normes utilisées lors du développement des API. Garantir leur uniformité permet aux équipes IT de gagner un temps précieux, au lieu de se consacrer à des cycles de révision et de gaspiller ainsi les ressources.

Alors que les responsables IT doivent livrer toujours plus de projets avec des ressources réduites, la gouvernance des API devient une nécessité et non un luxe.

Les architectes IT doivent établir des normes de gouvernance visibles pour aider les développeurs.

Les développeurs doivent adhérer à des pratiques de gouvernance uniformes et faciles à comprendre pour mener à bien des projets sécurisés dans les délais impartis.

Les meilleures pratiques de gouvernance, du développement à l'API discovery, consistent à adopter une approche proactive de la sécurité. En outre, la normalisation obtenue grâce à la gouvernance simplifie la tâche des développeurs en unifiant les règles dans l'ensemble du patrimoine digital.

Plus que jamais, les développeurs doivent mener à bien un nombre croissant de projets, qui requièrent des connaissances techniques spécifiques. L'application de normes de gouvernance permet de réduire leur charge de travail tout en renforçant la sécurité.

03 Sécurité des données : allez encore plus loin

Si la gouvernance des API garantit que toutes celles-ci respectent les mêmes normes, les responsables IT doivent aller plus loin pour sécuriser les données.

Aujourd'hui, presque tous les secteurs et toutes les entreprises se préoccupent de la sécurité des données clients. La protection de ces données personnelles identifiables (PII) est essentielle pour maintenir la réputation d'une entreprise.

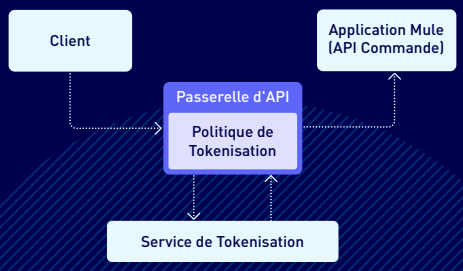
Pour comprendre la sécurité des données, imaginons qu'une API est une île avec un trésor enfoui (les PII) quelque part au milieu de l'océan. La gouvernance des API coordonnerait la patrouille de sécurité de l'île afin d'éloigner les acteurs malveillants à la recherche du trésor des PII.

L'île mettrait en œuvre des mesures de sécurité pour protéger les données des API et restreindre l'accès des visiteurs à certaines zones. C'est ce niveau de contrôle individualisé que sous-tend la tokenisation.

En contrôlant quelles données sont accessibles dans une API, les équipes IT utilisent une couche de protection supplémentaire. Elles s'assurent ainsi que l'API ne communique pas systématiquement toutes les données à chaque utilisateur.

Tokenisation et secteur de la santé

Il serait par exemple absurde qu'un médecin accède aux informations bancaires d'un patient lorsqu'il consulte son profil. La tokenisation est ce qui empêche le médecin ou tout acteur malveillant d'infiltrer les API au cours de ce processus.



04 API discovery : explorez de nouveaux espaces

Les entreprises disposent de patrimoines numériques composés d'API développées dans différents environnements, parfois par des équipes différentes. Pour sécuriser les API, il faut les gérer et les rendre visibles au sein d'une source unique de vérité qui les cataloguerait en totalité. Cette vue unique doit inclure les API développées dans tous les environnements, y compris celles créées sur :

- des plateformes cloud utilisant une architecture cloud-native ;
- des plateformes de conteneurs pour soutenir des applications modernes ;
- des plateformes d'intégration utilisant des applications et sources de données existantes.

En outre, une stratégie complète d'API discovery doit révéler les API tierces utilisées par l'entreprise, les API qui font partie des produits SaaS et les API utilisées dans des contextes web ou mobile.

Un environnement numérique complexe ayant multiplié les API aura certainement des Shadow API, pouvant être utilisées au sein de l'entreprise sans être forcément visibles de tous.

Si une API n'est pas visible et facile à découvrir, elle ne peut pas être sécurisée.

05 Tests de sécurité des API : privilégiez l'intégration

Lorsqu'ils imaginent une stratégie pour protéger les API, les responsables IT pensent tout de suite aux tests de sécurité. Toutefois, il ne s'agit que de la dernière étape de nos lignes directrices, qui succède à la mise en œuvre de la stratégie complète.

Tester la sécurité des API passe par l'identification des vulnérabilités. Deux types de vulnérabilités doivent être pris en compte lors de la conception des tests de sécurité :

- **attaques par injection :** ces attaques se produisent lorsque des acteurs malveillants manipulent des données pour les rendre impossibles à distinguer des données fiables ;
- **attaques ciblées sur les API :** ces attaques ciblent les vulnérabilités spécifiques aux API, notamment les attaques DDoS et les attaques de type « Man in the Middle » :
  - les attaques DDoS visent à submerger les API de centaines ou de milliers de requêtes ;
  - les attaques « Man in the Middle » se produisent lorsque l'acteur malveillant intercepte et relaie des informations entre deux parties lui permettant d'accéder à des PII auxquelles il ne devrait pas avoir accès.

Les équipes IT peuvent uniquement tester la sécurité des API dont elles ont connaissance. Pour être efficaces, des tests de sécurité doivent donc accompagner les bonnes pratiques en matière de sécurité des API.

Donnez à vos équipes IT les moyens de sécuriser leurs API

Au moment de franchir ces cinq étapes, les équipes IT doivent garder à l'esprit quelques points fondamentaux pour mieux s'approprier la sécurité des API.

Donnez une bonne visibilité sur toutes les API

Avoir de la visibilité sur chaque API de votre patrimoine numérique est un défi de taille. Même si votre entreprise applique des normes de gouvernance rigoureuses, l'erreur humaine est inévitable. Au moment de la construction du patrimoine numérique, certaines équipes IT peuvent choisir de monitorer chaque API manuellement.

Bien que séduisante, cette approche est source d'erreurs et n'est pas extensible aux API supplémentaires. Votre stratégie de sécurité doit donc inclure un processus automatisé pour garantir la visibilité de chaque API de votre patrimoine digital.

C'est là que MuleSoft Auto-Cataloging CLI entre en jeu. Auto-Cataloging CLI permet de dévoiler et de cataloguer les API non-Mule en utilisant les pipelines CI/CD au moment de leur création, peu importe l'environnement dans lequel elles sont développées.

Un flux de travail automatisé permet le dévoilement en continu de toutes les API, ce qui se traduit par la détection et le catalogage des API. Une fois cataloguées, celles-ci peuvent être évaluées selon leur conformité aux normes de gouvernance, leurs vulnérabilités en matière de sécurité et leur inclusion dans les services API métiers.

Cinq fonctionnalités clés d'Auto-Cataloging CLI qui renforcent votre stratégie de sécurité des API

1. Identifiez toutes les API d'un répertoire de projet
2. Identifiez toutes les API nouvelles et modifiées et mettez à jour le descriptor file
3. Déclenchez la publication de nouvelles API en fonction de certains critères
4. Définissez une stratégie de version des actifs en fonction de certains critères
5. Publiez des API dans le descriptor file en exécutant des commandes via l'invite de commande ou dans le cadre de pipelines CI/CD ou de scripts personnalisés

Soyez proactif en matière de sécurité

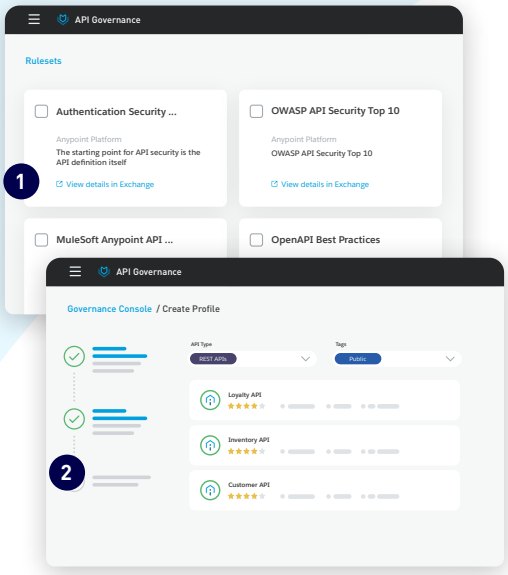
Les architectes IT doivent maintenir une sécurité et une qualité constantes malgré un nombre croissant d'API et d'automatisations développées par des équipes différentes. Dans le même temps, les développeurs ont besoin de flexibilité pour développer des API sans perdre de temps avec des cycles d'examen de conformité qui les empêchent de se consacrer à des sujets plus prioritaires.

La gouvernance des API doit être contrôlée de manière centralisée. Elle doit permettre aux architectes IT d'utiliser le libre-service pour que chaque API et chaque automatisation s'alignent sur les normes. Les entreprises qui, dans le cas contraire, choisissent de créer d'abord et de sécuriser ensuite risquent de développer des API et des automatisations vulnérables aux menaces des acteurs malveillants. En outre, le fait de revenir en arrière pour respecter les normes de conformité prolonge les cycles de révision, ce qui est à la fois coûteux et chronophage.

Anypoint API Governance

Anypoint® API Governance assure la réussite de tous les membres de l'équipe IT, des responsables aux développeurs. Ils peuvent exploiter les ensembles de règles prêts à l'emploi fournis par MuleSoft ou en créer pour éviter de gérer des normes dans des documents cloisonnés.

Les architectes IT peuvent utiliser Anypoint® API Governance pour filtrer et regrouper les API sur la base de métadonnées, telles que des étiquettes ou des catégories. Les profils créés sont dynamiques et appliquent automatiquement les normes à chaque nouvelle API correspondante ajoutée à Anypoint Exchange.



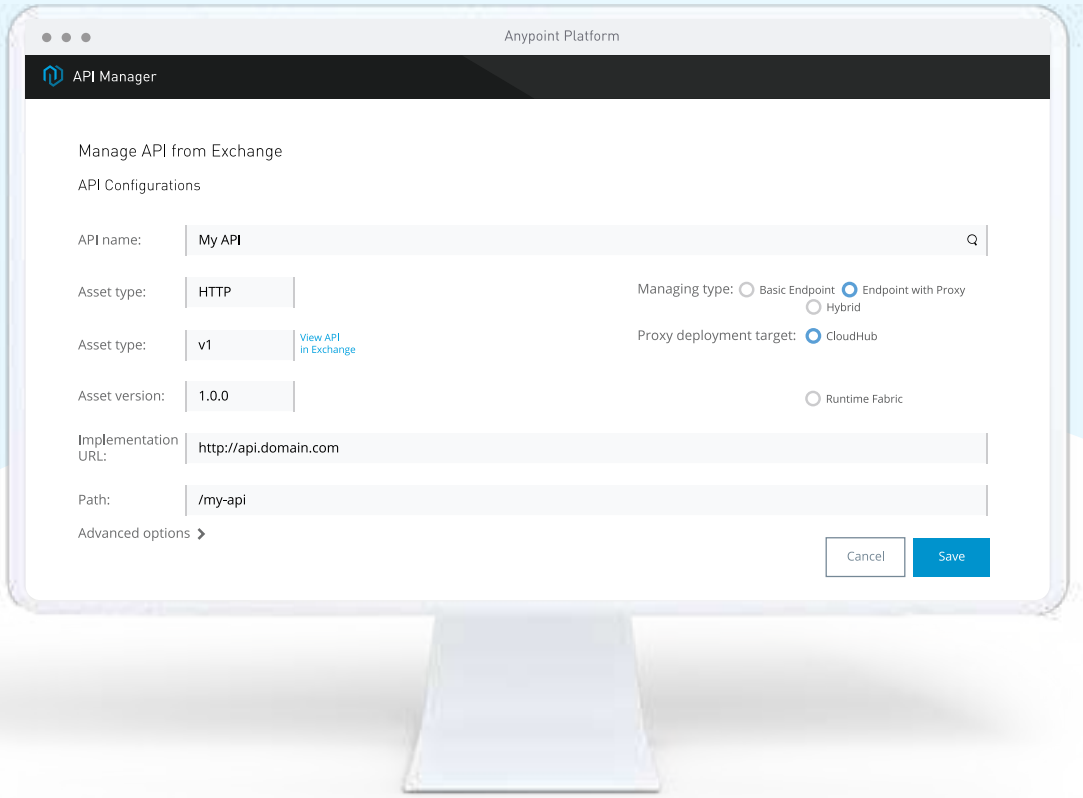
Qu'est-ce qu'un ensemble de règles ?

Un ensemble de règles est un jeu de règles pouvant être appliquées aux métadonnées extraites de toute définition d'API REST. Ces règles sont extensibles et reposent sur des normes ouvertes (W3C, OPA).

1. Les ensembles de règles servent à créer un profil, un jeu de règles ressemblant à une norme de gouvernance. Avec Anypoint® API Governance, un profil peut définir les règles d'un groupe donné d'API.
2. Les équipes IT peuvent créer plusieurs profils afin d'adapter leurs normes de gouvernance aux cas d'usage.

Anypoint API Manager

Les équipes IT ont besoin de rapidement sécuriser les API à l'aide de stratégies, de gérer les accès utilisateurs et de collecter des informations essentielles sur les programmes. Anypoint API Manager vous permet de gérer toutes vos API et tous vos microservices depuis un seul et même endroit, où qu'ils soient stockés.



FONCTIONNALITÉS CLÉS

Déployer et gérer vos API

- déverrouillez et gérez vos services en toute sécurité à l'aide d'une passerelle d'API flexible
- appliquez des politiques de sécurité prédéfinies ou personnalisées lors de l'exécution, sans interruption
- sécurisez et gouvernez les microservices, où qu'ils soient stockés, grâce au maillage de services
- gérez l'accès des utilisateurs individuels et des équipes à vos ressources
- obtenez des informations essentielles concernant la fiabilité, les performances et la conformité de vos API

Mettez en place une surveillance complète avec Runtime Protection

Les responsables IT doivent répondre à deux questions simples mais toutefois épineuses en matière de sécurité :

1. Si quelqu'un abusait des API de votre entreprise, le sauriez-vous ?
2. Comment découvrir les vulnérabilités des API tout au long du cycle de développement, et comment améliorer leur sécurité ?

Votre stratégie de sécurité des API doit garantir la détection des vulnérabilités via des ensembles de règles tels que l'OWASP, la TLS ou en se basant sur des bonnes pratiques. En adoptant un cadre de protection de l'exécution dans l'ensemble de l'entreprise, les équipes IT peuvent contrôler l'accès aux API.

La passerelle d'API de MuleSoft fournit des stratégies intégrées pour authentifier, autoriser et contrôler l'accès aux API. Les équipes IT peuvent ainsi configurer un ensemble solide de stratégies d'authentification, de sécurité et de gestion du trafic Zero Trust. Grâce à la passerelle d'API, les équipes IT peuvent appliquer des mesures de sécurité supplémentaires.

Anypoint® Flex Gateway présente trois fonctions principales :

- la sécurisation de vos API, quel que soit leur environnement d'exécution ;
- l'extension de Anypoint Platform à toutes les API ;
- la création d'expériences réactives.

Anypoint Security propose une approche en couches pour sécuriser votre réseau d'applications. Ces couches s'associent pour contrôler l'accès aux API, appliquer des stratégies, et gérer par proxy tout le trafic entrant ou sortant, afin d'atténuer les menaces et les attaques externes. Anypoint Security fournit également un terminal dédié pour détecter les attaques et valider le trafic sans affecter vos implémentations réseau.

Anypoint Security intègre un WAF (Web Application Firewall) et la tokenisation pour vous protéger contre les menaces :

- **la tokenisation** concerne les données sensibles traitées par l'API, telles que celles liées aux cartes de crédit, à la sécurité sociale ou d'autres informations confidentielles. Le fait de les tokeniser permet de les protéger et de prévenir les violations de données.
- **la stratégie de WAF** ajoute une protection au niveau des applications web.

TÉMOIGNAGE CLIENT

Identifier les Shadow API avec Takeda Pharmaceuticals

Takeda Pharmaceutical Company est l'une des 20 plus grandes entreprises pharmaceutiques au monde. Elle emploie près de 50 000 personnes et fournit des services de santé à des millions de patients.

Takeda s'appuie sur MuleSoft pour gérer ses API. Anypoint® permet à Takeda d'établir des schémas, de mettre en place la gouvernance, et d'accroître l'efficacité de ses API tout en encourageant leur réutilisation.

Cependant, il reste deux défis à relever :

→ gouverner toutes les API dans MuleSoft et AWS ;

→ protéger les données sensibles des patients.

Pour atténuer ces risques, Takeda a complété le déploiement de MuleSoft par la mise en place d'une plateforme de sécurité API à part entière. L'objectif est de surveiller toutes les transactions dans un système reposant sur l'apprentissage automatique de manière asynchrone et d'identifier les menaces.

Grâce à MuleSoft, Takeda a pu identifier 30 % d'API en plus qui n'avaient pas été catégorisées auparavant.

« Chez Takeda, nous nous efforçons d'instaurer une culture de la préparation et de l'anticipation. Mon équipe travaille selon certains principes directeurs, notamment la normalisation, la simplification, l'évolutivité, la réutilisation et l'adoption. MuleSoft nous aide à respecter ces principes. »

SUNDAR KRISHNA, Directeur des plateformes d'ingénierie cloud et responsable des services et produits d'intégration de données, Takeda

En savoir plus

Une stratégie de sécurité des API garante de votre fiabilité

Les enjeux n'ont jamais été aussi élevés pour les responsables IT. Les budgets sont réduits et les attentes toujours croissantes. La sécurité des API peut parfois sembler inutile. Pourtant, il est très risqué de mettre cet aspect de côté. La réputation de votre entreprise est en jeu : une seule violation de données suffit à créer des problèmes conséquents. En définitive, c'est la confiance de vos clients qui est menacée.

L'élaboration d'une stratégie globale de sécurité des API est donc essentielle pour que les équipes IT se protègent et protègent les informations confidentielles des clients. MuleSoft propose plusieurs solutions de sécurité des API. Leur but ? Alléger la tâche des équipes IT en leur permettant de sécuriser les API de l'entreprise dans un délai raisonnable.

CTA

Débutez votre parcours de sécurité dès aujourd'hui

Découvrez comment MuleSoft aide les équipes IT à sécuriser chaque API de votre patrimoine numérique.

En savoir plus sur MuleSoft

Webinaire : Découvrir et gérer les API pour une visibilité universelle

Regardez et découvrez comment appliquer les garde-fous dans Anypoint® Governance.

Voir le webinaire

Puissant, rapide et flexible

Gérez et sécurisez n'importe quelle API créée n'importe où avec Anypoint® Flex Gateway.

Commencez à sécuriser

Webinaire : Services numériques et sécurité des API d'entreprise avec Okta et MuleSoft

MuleSoft et Okta unissent leurs forces pour soutenir les développeurs tout au long du cycle de développement

Regardez la vidéo (en anglais)

En savoir plus sur MuleSoft

Débutez votre parcours de sécurité dès aujourd'hui

Découvrez comment MuleSoft aide les équipes IT à sécuriser chaque API de votre patrimoine numérique.

En savoir plus sur MuleSoft

Webinaire : Découvrir et gérer les API pour une visibilité universelle

Regardez et découvrez comment appliquer les garde-fous dans Anypoint® Governance.

Voir le webinaire

Puissant, rapide et flexible

Gérez et sécurisez n'importe quelle API créée n'importe où avec Anypoint® Flex Gateway.

Commencez à sécuriser

Webinaire : Services numériques et sécurité des API d'entreprise avec Okta et MuleSoft

MuleSoft et Okta unissent leurs forces pour soutenir les développeurs tout au long du cycle de développement.

Regardez la vidéo (en anglais)

Salesforce, le leader mondial des CRM, donne à des entreprises de toute taille et de tout secteur les moyens d'opérer une transformation digitale et de créer une vue à 360 ° de leur clientèle. Pour plus d'informations sur Salesforce (NYSE : CRM), rendez-vous sur salesforce.com.

Tout service ou toute fonctionnalité non lancés, mentionnés dans ce communiqué de presse ou un autre, ou dans des déclarations publiques, ne sont actuellement pas disponibles, et pourraient ne pas être livrés à temps ou du tout. Nous invitons la clientèle qui achète des applications Salesforce à fonder ses décisions d'achat sur les fonctionnalités actuellement disponibles. Le siège de Salesforce se situe à San Francisco, la société dispose de bureaux en Europe et en Asie, et est cotée à la Bourse de New York (NYSE) sous le symbole « CRM ».

Pour en savoir plus, rendez-vous sur salesforce.com ou composez le 1-800-NO-SOFTWARE.