Akamai

LIVRE BLANC

# Sécurité des API dans l'écosystème d'Open Banking

Trouver l'équilibre entre innovation et sécurité pour les banques européennes à l'ère du digital

# Synthèse

En 2023, les banques d'Europe, du Moyen-Orient et d'Afrique (EMEA) ont bénéficié d'une rentabilité significative, qui devrait se poursuivre au cours de l'année à venir. Les interfaces de programmation d'applications (API), qui représentent 31 % de l'ensemble du trafic Web, ont joué un rôle déterminant dans cette croissance, facilitant divers services comme les transactions bancaires, le dépôt de chèques à distance et les emplacements des distributeurs automatiques de billets assistés par GPS, ainsi que des services tiers. Cependant, l'adoption rapide des API a élargi l'écosystème des menaces, incitant les institutions financières à investir massivement dans la cybersécurité.

La directive révisée sur les services de paiement (PSD2) de l'Union européenne et la PSD3 anticipée ont joué un rôle central dans l'organisation des échanges de données entre les banques traditionnelles et les sociétés fintech. Les normes techniques de réglementation imposent une utilisation sécurisée des API, intégrant une authentification forte des utilisateurs et des normes ouvertes de communication communes et sécurisées. Bien que principalement axée sur les paiements, la PSD2 a propulsé le terme « Open Banking » au Royaume-Uni, mettant l'accent sur le partage des données de compte autorisées par les clients et ouvrant la voie à des solutions plus larges d'« Open Finance ». Au cœur de ces solutions d'« Open Finance » se trouvent les API.

La transformation digitale en cours dans le secteur des services financiers de la zone EMEA, pilotée par les API, démontre l'adaptabilité et l'engagement du secteur à répondre aux besoins changeants des clients. Cependant, pendant le déroulement de cette transformation, la vigilance est essentielle pour renforcer la cybersécurité, remédier aux vulnérabilités et faire en sorte que les avantages de l'innovation digitale l'emportent sur la menace toujours présente des cyberattaques. McKinsey rapporte que les grandes banques envisagent d'allouer 14 % aux programmes d'API, ce qui reflète l'augmentation de l'utilisation des API et suscite des investissements substantiels dans la cybersécurité. Les institutions financières accordent désormais la priorité à la sauvegarde des systèmes internes et à la protection des données et des actifs des clients, en mettant l'accent sur la détection des menaces, les stratégies de réponse et la collaboration pour contrer les cyberrisques de manière efficace.

# L'importance croissante des API

La zone EMEA connaît une révolution digitale reposant sur la volonté de fournir des services et des produits plus efficaces et sur mesure à ses clients des services financiers. Les API jouent un rôle central, offrant une commodité, une rapidité et une sécurité inégalées aux clients qui accèdent aux produits bancaires. Les API permettent aux applications tierces de se connecter aux outils, services et actifs précieux d'une banque, simplifiant ainsi les connexions pour les deux parties. Les clients bénéficient désormais d'un large éventail d'activités financières, ce qui a transformé l'expérience utilisateur et propulsé le secteur financier dans l'ère digitale. Les API, évoluant à partir de simples outils de communication, sont devenues l'épine dorsale du trafic Internet, prenant en charge plusieurs applications.

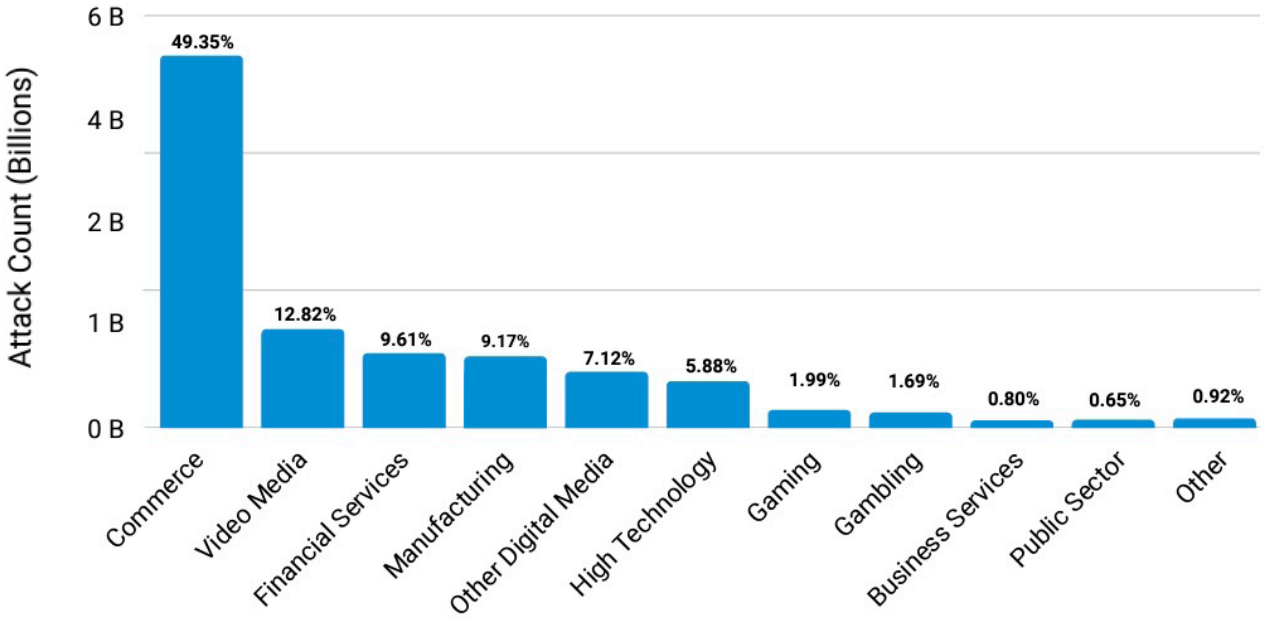
Selon Allied Market Research, le marché européen de l'Open Banking a atteint 6,14 milliards de dollars en 2020 et devrait grimper jusqu'à 48,30 milliards de dollars d'ici 2030, avec un taux de croissance annuel composé de 23,18 % entre 2021 et 2030. Des initiatives telles que l'Open Bank Project, initié par l'entreprise berlinoise TESOBE, accélèrent cette adoption. Collaborant avec plus de 40 banques dans le monde, l'Open Bank Project permet aux banques d'offrir des applications et des services tiers à leurs clients via une API ouverte et une boutique d'applications. En France, la consolidation autour de l'API STET, fournie par la société Systèmes technologiques d'échange et de traitement (STET), contribue à la mise en œuvre des paiements issus de l'Open Banking. Les API sont à l'avant-garde de la refonte rapide de l'écosystème financier dans la zone EMEA et dans le reste du monde.

# Menaces liées aux API dans la zone EMEA

Le secteur des services financiers apparaît comme le troisième secteur le plus ciblé dans la région EMEA ; il a été la cible de près de 10 % des attaques d'applications Web et d'API qui ont eu lieu entre janvier 2022 et juin 2023. Cela se traduit par un chiffre impressionnant de 1 milliard sur les 11 milliards d'attaques Web dans les industries de la zone EMEA, ce qui représente une augmentation significative de 119 % d'une année à l'autre entre le deuxième trimestre 2022 et le deuxième trimestre 2023. En approfondissant notre analyse, nous constatons que le Royaume-Uni est en tête avec 59,2 % des attaques d'applications Web, enregistrant la plus forte croissance d'une année à l'autre qui s'élève à 79 %, suivi des Pays-Bas avec 16,2 %, puis de l'Allemagne avec 10,7 %.

**EMEA : Principaux segments de marché d'applications Web et d'API**

Du 1er janvier 2022 au 30 juin 2023




*Les services financiers sont le troisième segment de marché le plus fréquemment attaqué dans la zone EMEA*

# Risques clés de sécurité des API

Les API peuvent être vulnérables à un large éventail de risques de sécurité, qui peuvent entraîner des violations de données, des accès non autorisés et d'autres formes d'exploitation. Les principaux risques de sécurité des API incluent les API fantômes, les API vulnérables, les abus d'API, le partage excessif d'informations sensibles et les attaques par credential stuffing.

- **API fantômes.** Dans de nombreuses institutions financières, aucune personne ou équipe n'est responsable de la gestion de toutes les API. Ce manque de surveillance crée une lacune importante en matière de sécurité. Pour gouverner et sécuriser les API dans toute l'organisation, il est essentiel de les détecter et d'en faire l'inventaire. Il est important de combler le fossé entre les développeurs et les équipes de sécurité et de détecter les API fantômes dans leur environnement. La découverte continue vous tient au courant des API nouvellement découvertes ou des modifications apportées aux API existantes, ce qui peut éliminer les API fantômes.

- **API vulnérables.** Une fois les API découvertes, les institutions financières doivent évaluer leur posture de risque et identifier les vulnérabilités, en particulier celles qui transportent des données sensibles. Cette étape est essentielle pour hiérarchiser les efforts de sécurité de manière efficace.

- **Abus d'API.** À l'heure où la digitalisation s'accélère, le nombre d'attaques Web dans la zone EMEA continue d'augmenter. Les acteurs malveillants ciblent sans relâche les API, ce qui nécessite des mesures de sécurité robustes pour contrecarrer les abus.

- **Partage excessif d'informations sensibles.** Les applications d'aujourd'hui partagent souvent de manière excessive les données sensibles, ce qui présente un nouveau vecteur d'attaque. Les attaquants peuvent intercepter le trafic et obtenir un accès non autorisé à des informations sensibles.

- **Attaques par credential stuffing.** Les acteurs malveillants ciblent les institutions financières à l'aide d'API pour automatiser les attaques par credential stuffing.

# Défis de sécurité des API

## Inventaire des API

Selon une enquête SANS récente, l'inventaire des API reste un problème critique pour les institutions financières. Ces-dernières peuvent même ne pas connaître toutes les API au sein de leur infrastructure, ce qui crée un angle mort en matière de gouvernance et de sécurité. Ce manque de visibilité peut être l'un des facteurs clés contribuant au fait que les attaques d'API passent souvent inaperçues et ne sont pas signalées. La première étape de la sécurisation des API consiste à les découvrir et à la répertorier de manière exhaustive.

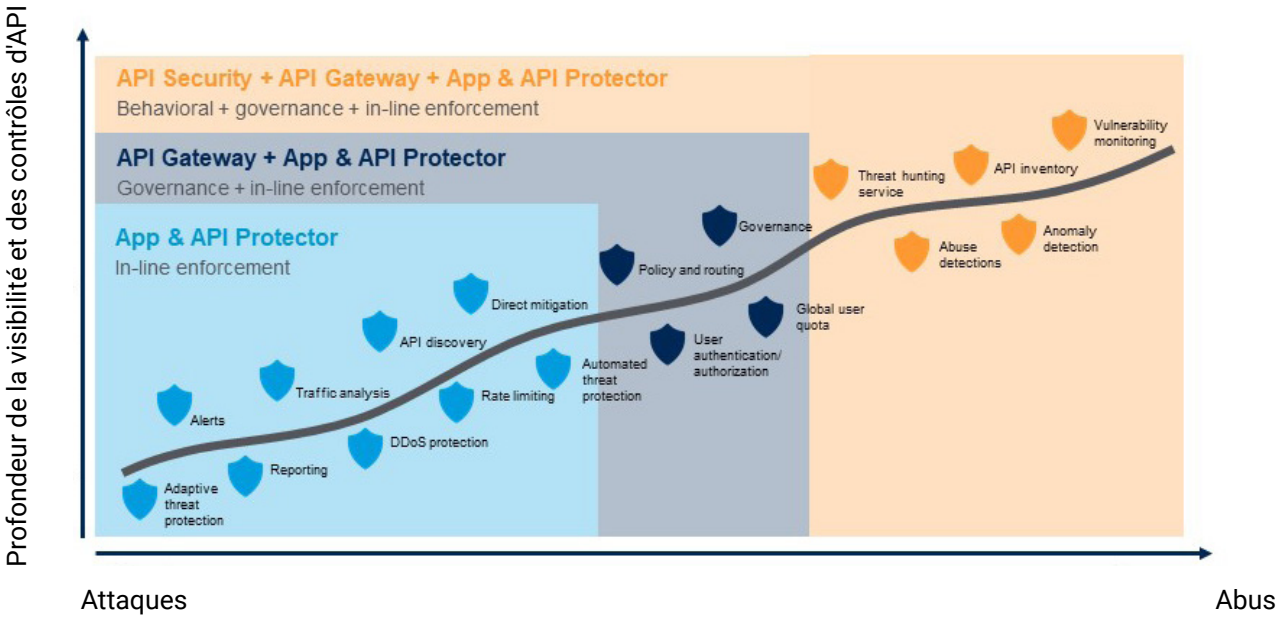
## Les conséquences des attaques d'API perturbatrices

Les perturbations dans la disponibilité des applications Web et des API peuvent avoir d'importantes conséquences sur la satisfaction des clients et la fidélité envers la marque. Avec l'adoption croissante d'une approche axée sur le digital, les API sont devenues encore plus critiques pour la réussite des institutions financières, en particulier dans le contexte de l'Open Banking adopté par les sociétés fintech et les banques traditionnelles.

## Croissance rapide du trafic d'API

Le trafic d'API dans le secteur financier a connu une croissance rapide, le volume du trafic atteignant des nombres à trois chiffres. Cette croissance met au défi les contrôles de sécurité pour suivre l'évolution de l'écosystème des menaces liées aux API.

## Les attaques d'API évoluent



# Réglementation et sécurité

Les institutions financières qui exploitent la puissance des API et d'autres technologies innovantes se trouvent à l'intersection des objectifs de politique publique et de stabilité financière. Le rôle important des API dans l'amélioration des résultats pour les clients en a fait la méthode de connectivité et d'échange de données par défaut dans les environnements de services financiers d'aujourd'hui, et il continuera d'en être ainsi à l'avenir. Les objectifs généraux consistent à élargir la gamme des options financières, à favoriser une concurrence et une accessibilité accrues et à promouvoir l'inclusion financière. Dans toute la zone EMEA, les organismes de réglementation s'efforcent d'élargir le champ d'application des services financiers, ce qui profitera à la fois aux individus et aux organisations.

## Le rôle des réglementations dans la sécurité des API

Des réglementations telles que la PSD2 (et bientôt la PSD3) favorisent la transparence en obligeant les institutions traditionnelles à partager des données avec des entités externes, en accordant la priorité aux données, à la confidentialité et à la sécurité des utilisateurs finaux. Les institutions financières doivent respecter ces réglementations tout en poursuivant activement l'innovation.

Bien que les réglementations favorisent le partage des données, elles précisent également comment les organisations stockent et protègent les données. Les institutions financières ont besoin d'un partenaire technologique qui assure la conformité réglementaire sans entraver l'innovation. Un tel partenaire devrait répondre aux préoccupations concernant la qualité des API et fournir aux autorités des outils pour évaluer les interfaces API dédiées des banques et autres entités financières.

Selon l'Autorité bancaire européenne, « l'expérience acquise lors de la mise en œuvre de la PSD2 met en évidence l'absence d'une norme d'API unique, ce qui a entraîné des solutions d'API variées à l'échelle de l'UE. Cela pose des défis importants pour les fournisseurs de services tiers, qui doivent déployer des efforts considérables pour se connecter aux différentes API des prestataires de services de paiement et adapter les connexions à l'évolution des API. » On s'attend à ce que la DPS3 intègre les leçons tirées de la PSD2.

# 6 étapes pour construire une stratégie de sécurité des API robuste

La stratégie de prévention des attaques basées sur les API en protégeant les terminaux et en vérifiant les informations d'identification ne suffit plus. Aujourd'hui, une stratégie de sécurité des API robuste doit comprendre les six étapes suivantes.

## 1. Collaboration avec les partenaires

Les institutions financières et leurs partenaires de sécurité doivent collaborer étroitement en harmonisant les personnes, les processus et les technologies afin d'établir une solide défense contre les risques de sécurité des API. Cette collaboration comprend des équipes de développement, des équipes d'exploitation réseau et de sécurité, des équipes d'identité, des gestionnaires de risques, des architectes de sécurité et des équipes juridiques et de conformité.

## 2. Découverte et inventaire des API

La première étape de la sécurisation des API consiste à les découvrir et en faire l'inventaire dans toute l'organisation. Ce processus permet aux ingénieurs de sécurité de comprendre la portée de la surface d'attaque et l'exposition potentielle des informations sensibles.

## 3. Test de la vulnérabilité et évaluation des risques

Une fois les API découvertes, les institutions financières doivent effectuer des tests de vulnérabilité et des évaluations des risques pour identifier et corriger les vulnérabilités en temps opportun. Ce processus devrait être intégré dans les cycles de développement et de mise à niveau des API pour assurer une sécurité continue.

## 4. Mise en œuvre de la détection comportementale

Les protections des API sont des composants essentiels de l'infrastructure de sécurité globale des applications. La détection comportementale est une stratégie clé pour empêcher l'exploitation des API vulnérables. Cette approche implique une surveillance et une analyse continues du comportement des API pour identifier les menaces potentielles.

## 5. Priorisation des 10 principaux contrôles OWASP

Les institutions financières doivent donner la priorité aux 10 principaux risques de sécurité des API de l' OWASP (Open Worldwide Application Security Project) afin d'assurer une protection complète. Ces contrôles couvrent les vulnérabilités et les vecteurs d'attaque les plus critiques qui touchent les API.

### OWASP API Top 10 coverage by Akamai

- **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

## 6. Apprentissage par les pairs

Les institutions financières doivent apprendre de leurs pairs et partager les meilleures pratiques. L'adhésion au Centre d'analyse et de partage des informations des services financiers (FS-ISAC) permet aux institutions financières de tirer parti de leur plateforme dédiée, de leurs ressources et de leur réseau d'experts de confiance pour anticiper, atténuer et répondre aux cybermenaces. Une compréhension claire de la façon dont les autres organisations répondent aux défis de sécurité des API peut aider à améliorer les mesures de sécurité pour l'ensemble du secteur.

# Conclusion

En cette période de transformation digitale rapide et d'adoption généralisée des API, conçue pour faciliter une intégration flexible, rapide et rentable sur un large éventail de logiciels, de terminaux et de sources de données, la protection des API est d'une importance capitale pour les institutions financières de la région EMEA. Néanmoins, la sécurité des API présente un acte de jonglage complexe, impliquant diverses caractéristiques, fonctions et exigences de l'entreprise. Négliger la sécurité des API peut entraîner de graves conséquences, y compris des cyberattaques, des violations de données, des infractions réglementaires et une atteinte à la réputation d'une institution.

Nos données indiquent que la fonctionnalité des API se classe parmi les principales cibles pour les acteurs malveillants qui évoluent et adaptent continuellement leurs méthodes d'attaque. Par conséquent, il est impératif que la sécurité des API se déplace vers la bordure de l'Internet, en s'éloignant de l'infrastructure d'une organisation pour se rapprocher des points de contact digitaux où les clients interagissent avec les données et les applications. Cet ajustement stratégique est essentiel pour assurer une protection robuste de vos actifs digitaux.

**Apprenez-en plus sur Akamai pour les services financiers. Ou contactez votre contact Akamai** pour discuter de ce sujet et de son application à votre entreprise.