Akamai

LIVRE BLANC

11 fonctionnalités essentielles pour détecter les menaces visant les API et y répondre

Faire évoluer votre stratégie de sécurité des API

Introduction

Les API jouent un rôle essentiel dans chaque application que votre entreprise crée pour ses clients, utilise en interne et met à la disposition de ses fournisseurs. Leur mission consiste à échanger des informations (souvent composées de données sensibles) entre les technologies. Où se trouvent-elles ? Dans vos applications, mais également dans vos migrations vers le cloud, dans les outils d'IA générative et tout au long de la chaîne logistique digitale.

Les API ont toutefois également pris une place importante dans la surface d'attaque de votre entreprise.

Alors que la course à l'innovation fait rage au sein des entreprises, les API sont souvent développées hâtivement, insuffisamment testées et mises en production avec de mauvaises configurations et des contrôles de sécurité manquants. De plus, ces API se sont accumulées dans une dynamique de prolifération jusqu'au point où les équipes de sécurité manquent aujourd'hui de visibilité sur une grande partie de leur parc d'API. Sans une bonne visibilité, les entreprises :

1. Ne peuvent pas détecter les API non gérées, oubliées et exposées de façon non contrôlée aux données sensibles, à Internet et aux pirates.
2. Par conséquent, ne peuvent pas évaluer les risques des API. Par exemple, seules 27 % des entreprises disposant d'un inventaire complet de leurs API savent lesquelles d'entre elles renvoient des données sensibles, contre 40 % en 2023.
3. Se retrouvent avec une surface d'attaque gorgée de vulnérabilités axées sur les API que les pirates exploitent fréquemment, et facilement.

Jusqu'à récemment, les entreprises se sont satisfaites d'une liste d'outils couramment utilisés pour gérer les API et obtenir une base de protection. Cependant, avec 84 % des entreprises ayant subi un incident de sécurité affectant les API au cours des 12 derniers mois (contre 78 % en 2023), les choses doivent changer.

À mesure que les attaques d'API augmentent en nombre et en complexité, il est temps d'envisager d'ajouter de nouvelles couches de protection aux outils tels que les passerelles d'API, les pare-feux d'applications Web (WAF) et les plateformes de protection des applications Web et des API (WAAP).

Ces nouvelles couches doivent offrir une meilleure visibilité sur toutes les API de votre environnement et sur leurs risques, y compris la grande partie des API non gérées, telles que :

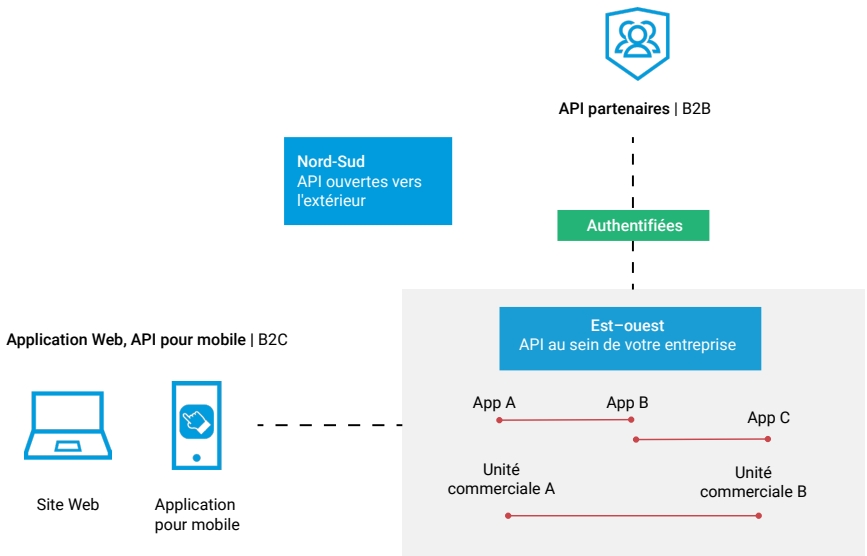
- Les API zombies qui auraient dû être rendues obsolètes, mais qui restent actives.
- Les API fantômes qui ne sont pas documentées et doivent être éliminées ou intégrées dans des processus de gouvernance formels.

Les entreprises ont également besoin de fonctionnalités plus approfondies pour détecter et traiter les abus et les attaques d'API, y compris toutes les menaces détaillées dans la liste des 10 principaux risques pour la sécurité des API de l'OWASP. De plus, dans le but de détecter et de corriger les vulnérabilités tout au long du cycle de vie des API, les entreprises doivent mettre en place des tests de sécurité rigoureux et en temps réel pour les API, depuis les premières étapes de développement jusqu'à la production.

Cela implique-t-il d'utiliser un nouvel outil pour chaque problème ? Non. C'est plutôt comme s'assurer qu'un orchestre ait les bons musiciens, que ceux-ci jouent les bonnes notes au bon moment, et qu'ils se coordonnent avec précision entre eux.

Lorsque vous réfléchissez à la manière d'ajouter de nouvelles couches à votre pile de protection des API, pensez à l'approche de défense en profondeur que les équipes de sécurité appliquent à d'autres menaces, par exemple en déployant un ensemble de contrôles pour détecter, prévenir et atténuer les effets d'une attaque par ransomware. C'est précisément en ces termes que les entreprises doivent envisager les API.

Dans ce livre blanc, nous allons explorer 11 fonctionnalités essentielles que vous pouvez intégrer à votre stratégie de sécurité des API, en vous concentrant sur la détection des menaces ciblant les API et les réponses à apporter pour y remédier.



Le contexte est essentiel

Quelle est la place de la détection des menaces et des réponses à celles-ci dans votre stratégie de sécurité des API ?

Comme vous l'avez probablement déjà vu, les API ont changé la façon dont les entreprises fonctionnent en couvrant davantage de cas d'utilisation, en accélérant les changements, en transportant plus de données sensibles et en étant ouvertes à plus d'utilisateurs. Il n'est pas surprenant que les entreprises aient créé beaucoup plus de canaux d'API que d'interfaces d'applications Web. Les risques augmentent à mesure que ces API prolifèrent et comportent des volumes croissants de données métiers et davantage de logique métier.

Compte tenu de la prévalence des API dans la myriade de technologies déjà protégées par les équipes de sécurité (c'est-à-dire les applications), la plupart des catégories de produits de sécurité prennent en charge ces API d'une manière ou d'une autre. Cependant, les API et les applications ne désignent pas la même chose ; elles apparaissent même comme des actifs différents dans certains cadres de conformité. Il ne suffit pas d'ajouter des fonctionnalités fragmentées de protection contre les menaces ciblant les API à un produit de sécurité d'application existant, par exemple. Les API méritent plus d'attention que ce qu'elles reçoivent dans la plupart des entreprises. Aujourd'hui, les équipes de sécurité doivent considérer les API comme une classe d'actifs distincte avec un ensemble distinct d'attributs de risque. Elles doivent également rechercher des fonctionnalités essentielles pour voir et sécuriser chaque API à l'échelle requise.

Par le passé, si une entreprise disposait d'un inventaire des API et de certains outils de base pour la gestion et la protection des API, elle était dans de bonnes dispositions pour prévenir des attaques courantes visant les API. Malheureusement, les pirates d'aujourd'hui innovent souvent au même titre que les entreprises, en portant une attention similaire à l'amélioration continue.

- Les acteurs malveillants font évoluer de manière logique leurs tactiques pour contourner les outils utilisés par la plupart des entreprises pour défendre leurs API.
- De la même manière que la plupart des entreprises utilisent l'IA, les pirates augmentent leurs capacités humaines limitées avec une assistance disponible 24 heures sur 24, et ce, grâce à l'IA générative.
- Les pirates recherchent de plus en plus de maillons faibles dans l'ensemble de la chaîne logistique digitale connectée aux API d'une entreprise. Cela peut comprendre des partenaires B2B qui ne font pas de la protection des API une priorité.

Par exemple, certaines formes d'abus d'API proviennent de clients et de partenaires qui ont obtenu des informations d'identification d'API, mais qui les utilisent de manière non autorisée. Il existe également des moyens de pirater des informations d'identification d'API ou des jetons de sécurité apparemment légitimes. Les vulnérabilités cachées dans les implémentations de clients API constituent un autre vecteur d'attaque que les acteurs malveillants peuvent exploiter pour abuser des API de manière non détectable par les outils de sécurité traditionnels.

La bonne nouvelle est que les fonctionnalités essentielles nécessaires pour protéger les API contre les méthodes d'attaque qui évoluent rapidement sont déjà disponibles à grande échelle pour les entreprises. Lisez la suite pour en savoir plus sur les 11 fonctionnalités essentielles que votre équipe peut utiliser au fur et à mesure que vous prenez des mesures pour protéger vos API et les données qu'elles échangent contre les attaques.

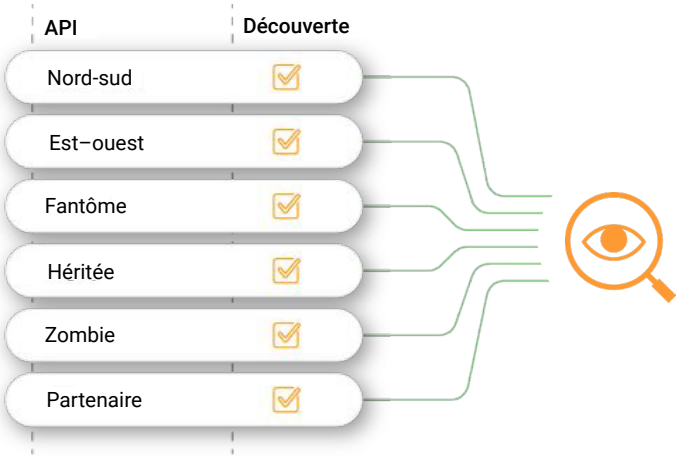
Fonctionnalité essentielle n° 1
Découverte continue des API et gestion de la posture

Toute stratégie de sécurité des API repose sur un inventaire complet et continuellement mis à jour des API utilisées dans l'entreprise. Cela est vrai tout simplement parce qu'une organisation ne peut pas protéger quelque chose dont elle ignore la présence dans son environnement. De nombreux produits de sécurité des API prétendent assurer un certain niveau de découverte des API, mais sont limités à un fonctionnement à la demande ou journalier. Il est important de s'assurer que les capacités de détection des API de votre plateforme incluent :

- La détection automatisée et continue des API 24 heures sur 24, y compris la détection des API qui ne sont utilisées qu'une seule fois (la détection à la demande ou journalière est insuffisante).
- La détection des API à travers différentes technologies et infrastructures.
- La détection des API nouvellement déployées et la comparaison avec des API bien documentées pour identifier les API fantômes.
- L'évaluation des risques de chaque service et point de terminaison d'API : cela permet aux équipes de sécurité et de développement de surmonter le bruit et de hiérarchiser les API pouvant avoir le plus gros impact si elles sont compromises.
- La détection des vulnérabilités des API connues, telles que celles décrites dans les 10 principaux risques liés à la sécurité des API identifiés par l'OWASP.

Visibilité améliorée

Ne perdez plus jamais de vue votre inventaire API



Fonctionnalité essentielle n° 2
Visualisation du comportement des API

La capacité à visualiser le comportement réel des API (appels d'API) est fondamentale pour une plateforme de sécurité des API. Cette fonctionnalité est nécessaire pour permettre aux principales parties prenantes des services de sécurité, de développement et des opérations de visualiser et comprendre de quelle manière les API sont utilisées ou exploitées, afin qu'elles puissent communiquer entre elles et enquêter. Les fonctionnalités de visualisation spécifiques à rechercher sont les suivantes :

- **Enquête :** toute alerte doit inclure la possibilité d'inspecter l'activité de l'API d'origine, appel par appel, pour identifier le déclencheur spécifique de l'alerte.
- **Fidélité et enrichissement des données :** pour chaque appel d'API, il devrait être possible d'identifier l'utilisateur, l'opération qu'il a effectuée, les enregistrements auxquels il a accédé ou qu'il a manipulés, les en-têtes et paramètres utilisés, etc.
- **Confidentialité des données :** bien que la fidélité des données soit importante, les données sensibles ne peuvent pas être stockées au repos. Une solution doit analyser le trafic et envoyer uniquement les métadonnées pertinentes pour mettre à jour les tableaux de bord.

Fonctionnalité essentielle n° 3

Détection des tentatives d'abus d'API via le contexte sur les entités utilisateur

Les équipes de sécurité ont besoin de pouvoir suivre les activités malveillantes des entités telles que les adresses IP et les entités de processus métier telles que les ID de paiement. Cette capacité peut s'avérer extrêmement utile si elle est associée à des compétences de corrélation des attaques provenant de différentes adresses IP dans les cas où d'autres identificateurs pertinents peuvent apporter du contexte aux abus d'API.

Imaginons qu'un utilisateur inconnu appelle l'API d'une entreprise de commerce de détail en utilisant /api/getpaymentID/50 comme ID. Dans ce scénario, l'équipe de sécurité du concessionnaire sait que tous les autres utilisateurs de la plateforme de l'entreprise sont liés à un type d'ID de paiement. Si un analyste de sécurité constate que soudainement, l'utilisateur inconnu effectue des appels répétés, en ajustant à chaque fois légèrement le numéro d'ID (/api/getPaymentID/51 … 52 … 53 … 54), il s'agit d'un indicateur clé de tentative d'abus d'API.

Disposer d'une visibilité en temps réel du comportement atypique des utilisateurs peut faire la différence entre une tentative de violation et une attaque d'API réussie.

943 162 $

Coût moyen de correction des incidents de sécurité des API, selon des RSSI, des DSI et des CTO basés aux États-Unis qui ont signalé avoir subi de tels événements au cours des 12 derniers mois.

Pour en savoir plus sur les points de vue et les expériences de vos pairs, consultez l'étude 2024 des impacts sur la sécurité des API.

Fonctionnalité essentielle n° 4
Analyse comportementale et détection

Bien que l'analyse des appels d'API individuels provenant d'entités utilisateur, voire de sessions individuelles, puisse aider les équipes de sécurité, il est important de disposer d'une détection complète des menaces d'API axée sur une vue d'ensemble. Recherchez des fonctionnalités permettant d'acquérir une compréhension approfondie des modèles comportementaux et des anomalies sur l'ensemble du parc d'API. Pour déterminer si le comportement d'une API est anormal, ce qui indique qu'il peut être compromis, l'utilisation de l'API doit être analysée sur des périodes plus longues et avec un contexte de référence élaboré à partir d'un suivi du comportement long et rigoureux. Les équipes de sécurité disposent ainsi d'une base de référence fiable qui leur permet de surveiller le comportement en permanence pour détecter des anomalies.

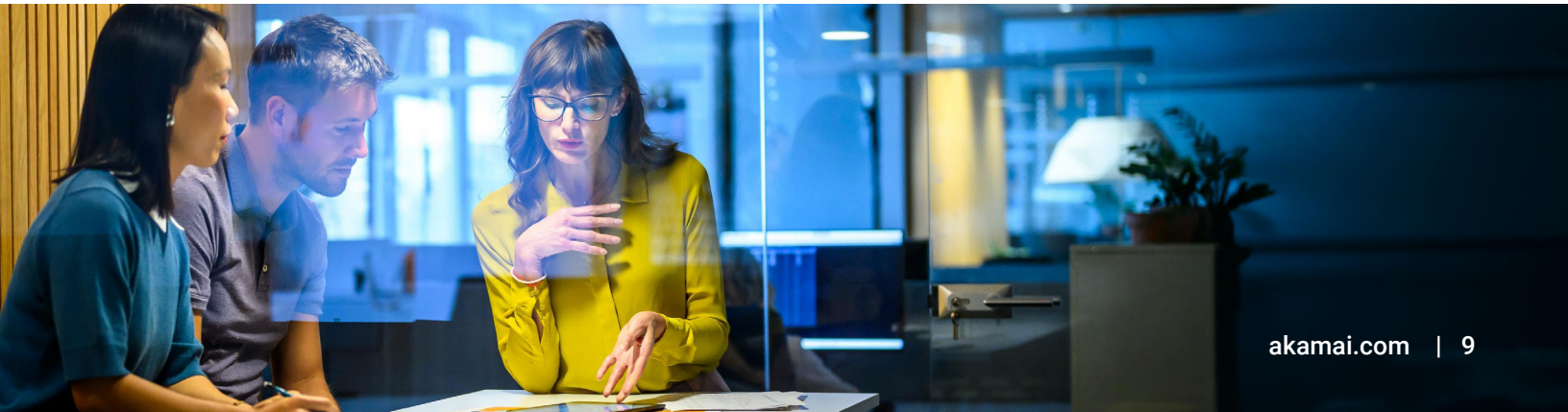
Fonctionnalité essentielle n° 5
Détection des dérives des spécifications d'API

Les API sont en constante évolution dans un contexte où la demande du marché et les besoins des entreprises changent également. En conséquence, les entreprises mettent continuellement à jour de nouvelles implémentations de points de terminaison pour répondre aux besoins en constante évolution des entreprises, corriger des bogues et apporter des améliorations techniques. La mise à jour de la documentation des API en parallèle de ces modifications, en fonction des spécifications des API, est essentielle. Une attention particulière doit être accordée pour s'assurer que le trafic d'une API est toujours conforme à ses spécifications.

Pour rendre les API résilientes face aux abus et aux attaques, les entreprises doivent pouvoir détecter les dérives des spécifications des API. Cela leur permet d'identifier les écarts ou les lacunes dans la documentation des API en comparant de manière continue et en temps réel le trafic des API et les spécifications définies.

Si la fonction de dérive des spécifications de l'API révèle des incohérences ou des points de terminaison non documentés consultés ou manipulés en production, elle peut alerter les développeurs et les équipes de sécurité, leur permettant ainsi :

- de garder une longueur d'avance sur les problèmes avant qu'ils ne deviennent critiques ;
- d'assurer que les API fonctionnent comme prévu ;
- de renforcer la sécurité des applications prises en charge par ces API ;
- de maintenir l'intégrité de l'écosystème d'API de l'entreprise.



Fonctionnalité essentielle n° 6
B2B et couverture API est-ouest

Le domaine de croissance le plus important dans l'utilisation des API se trouve dans les cas d'utilisation B2B, à la fois internes et externes. La sécurité des API doit couvrir les API B2B et machine à machine, y compris les instances nord-sud (orientées vers l'extérieur) et est-ouest (orientées vers l'intérieur).

Bien que les applications Web B2C bénéficient d'une protection de la part des plateformes WAAP et WAF, certains des types d'activité d'API les plus sensibles, tels que les API internes est-ouest ou les fonctionnalités d'applications propriétaires exposées aux partenaires via des API B2B, peuvent encore être compromis même lorsqu'ils traversent les WAAP.

Souvent, une fois qu'un utilisateur est authentifié sur une API d'un partenaire B2B, il est considéré comme sûr et aucune surveillance supplémentaire n'est effectuée. Cela crée une lacune critique dans la posture de sécurité des API de nombreuses organisations. Pour fournir une image complète de l'activité des API et de l'écosystème des menaces plus vaste, les organisations doivent utiliser une approche qui offre une visibilité, une observabilité et une surveillance efficaces pour tous les cas d'utilisation.

Fonctionnalité essentielle n° 7
Alertes pertinentes en contexte

Une fois qu'une organisation dispose d'une visibilité sur l'activité de ses API et d'analyses comportementales à grande échelle, les alertes sur l'activité des API prennent tout leur sens. Mais comment pouvez-vous vous assurer que vous concentrez l'attention et les ressources sur les véritables menaces visant les API ? Un moteur d'évaluation de la confiance des pirates peut utiliser des algorithmes d'apprentissage automatique avancés conçus pour évaluer des signaux externes et internes. Ces derniers comprennent le comportement des API, les modèles de trafic réseau, les données de géolocalisation, les flux de renseignements sur les menaces et d'autres facteurs contextuels, afin de déterminer le niveau de confiance selon lequel un incident de durée d'exécution détecté est le résultat d'une activité malveillante. Cette fonctionnalité peut aider une équipe de sécurité à se concentrer rapidement sur les menaces critiques et doit s'accompagner de fonctions qui créent des flux de correction et de notification automatiques pour les attaques à probabilité élevée.

Fonctionnalité essentielle n° 8
Réponses personnalisées et automatisées

Les approches d'API traditionnelles en ligne peuvent comprendre des mesures automatisées pour bloquer les potentielles attaques d'API, à cela près que les entreprises doivent être en mesure d'identifier l'attaque en question. L'analyse comportementale et la détection d'anomalies sur les API sont effectuées au fil du temps, avec un contexte métier beaucoup plus important ; la profondeur de la détection permet donc aux anomalies de faire surface. Cela permet un vaste éventail de réponses automatisées et personnalisées pouvant être fournies avec une grande précision. Quelques exemples :

- Blocage ou limitation du trafic au niveau des passerelles d'API et des filtres de réseau de diffusion de contenu (CDN) en bordure de l'Internet pris en charge
- Notifications par e-mail pour les décisionnaires en matière de sécurité et les parties prenantes de l'entreprise
- Création de tickets pour les développeurs
- Déclenchement de webhooks

Que peuvent faire les entreprises pour aider les équipes de sécurité étendues à optimiser leur coordination et leur énergie à mesure que les menaces liées aux API augmentent ? Rechercher des fonctionnalités d'automatisation qui améliorent l'efficacité et la productivité en simplifiant la création et la gestion des flux de travail multi-actions. Des fonctionnalités d'automatisation appropriées doivent offrir une interface de conception visuelle sans code capable de créer des processus de réponse à des événements complexes et de synchroniser les données liées aux incidents entre vos principales solutions de sécurité d'API et une multitude de services tiers, notamment ServiceNow, JIRA et Azure DevOps.

Fonctionnalité essentielle n° 9
Analyse du trafic des API

Les entreprises ont besoin de fonctionnalités opérationnelles en permanence pour enregistrer, visualiser et analyser le trafic des API dans leurs environnements sans déployer de lac de données. En enregistrant les flux de données d'API qui correspondent à des critères spécifiques dans les environnements applicatifs, y compris l'activité typique et anormale des API, les entreprises peuvent détecter les menaces plus efficacement tout en gérant l'exposition aux risques des utilisateurs suspects et les comportements inhabituels des API. Il est important de disposer de fonctions d'audit du trafic des API personnalisées en fonction de cas d'utilisation particuliers. Cela permet aux entreprises de capter et de conserver le trafic en fonction de filtres et de règles prédéterminés.

Fonctionnalité essentielle n° 10
Tests d'API rigoureux en temps réel

Dans la course à l'innovation, les entreprises mettent en production des API présentant des vulnérabilités et des défauts de conception qui passent souvent inaperçus. Elles peuvent éviter ces problèmes en adoptant une approche shift-left, visant à tester les API pendant la phase de développement. Voici les principales fonctionnalités de cette approche :

- Exécution de tests automatisés qui simulent le trafic malveillant, y compris les types décrits dans la liste des 10 principaux risques pour la sécurité des API de l'OWASP
- Inspection des spécifications des API par rapport aux politiques et règles de gouvernance établies
- Test des API à la demande ou dans le cadre d'un pipeline CI/CD

Fonctionnalité essentielle n° 11
Protection indépendante de la plateforme

Les services d'API sont généralement mis en œuvre par différents groupes au sein d'une entreprise, qui utilisent souvent un ensemble diversifié de plateformes et de technologies. Par exemple, certaines API sont mises en place sur site, tandis que d'autres sont exécutées dans le cloud public. Souvent, les entreprises utilisent des technologies intermédiaires, telles que des proxys inverses, des passerelles d'API, des WAF et des CDN, qui offrent de la valeur métier, mais créent de la complexité pour la visibilité des API.

Il est impératif de pouvoir accéder aux données d'activité d'API de chacune de ces technologies. Une approche de protection contre les menaces des API indépendante de la plateforme garantit que votre entreprise dispose toujours d'une image exhaustive des activités des API, quels que soient les détails de la mise en œuvre ou l'infrastructure utilisée. Cela fournira une couverture de protection pour :

- Tous les services, sociétés acquises et environnements
- Les API approuvées et les API fantômes, qu'elles utilisent la passerelle API ou non

Une approche indépendante de la plateforme permettra également d'étendre la visibilité au-delà des API nord-sud et inclura les API publiques, partenaires et internes est-ouest.

Veiller à ce que la visibilité de votre plateforme de protection contre les menaces liées aux API soit aussi vaste que possible protégera votre entreprise contre les menaces internes et les abus d'API par les organisations partenaires, et contre les risques liés aux acteurs malveillants externes.

Conclusion

Les API sont une composante essentielle de la capacité des organisations à servir leurs clients, générer des revenus et fonctionner efficacement dans l'économie digitale actuelle, centrée sur le cloud. Cependant, leur croissance continue, leur proximité avec les données sensibles et l'absence de contrôles de sécurité font des API une importante source de risques.

Akamai API Security fournit les 11 fonctionnalités essentielles abordées dans ce livre blanc et aide ainsi les entreprises à enrichir leurs approches existantes avec des fonctions essentielles, telles que :

- Découverte des API
- Évaluation des risques (y compris l'exposition aux données sensibles)
- Détection des abus et des attaques d'API
- Test des API pour détecter les risques pour la sécurité et les vulnérabilités

Apprenez-en plus sur la façon de se protéger contre les 10 principaux risques liés à la sécurité des API identifiés par l'OWASP.

Découvrez comment nous pouvons vous aider en planifiant une démonstration personnalisée d'Akamai API Security.

La solution de sécurité d'Akamai protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de cloud computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 01/25.