

Sécurité et gouvernance des API intégrées pour IBM API Connect et DataPower

La promesse et le défi des API

Les API ont été la force motrice de la transformation digitale, permettant aux entreprises de tous les secteurs de créer de nouveaux services et modèles commerciaux pour accélérer la croissance. Toutefois, à mesure que les API prolifèrent, les risques qu'elles présentent se multiplient également.

- Bien que les dirigeants et les responsables techniques aient rapidement accéléré l'adoption et l'intégration des API au sein de leurs organisations, leur capacité à les gérer efficacement reste un défi.
- Dans la course à la conception et au lancement de nouvelles applications et services optimisés par l'IA, les API sous-jacentes contiennent trop souvent des erreurs de configuration, de codage et des problèmes de logique métier.
- Chaque fois qu'un client, un partenaire ou un fournisseur interagit avec une entreprise par la voie digitale, une API facilite l'échange de données (souvent sensibles) en toute transparence, et les attaquants en ont conscience.

Par conséquent, les API sont devenues l'un des principaux vecteurs d'attaque avec des enjeux élevés. Les attaques contre les API peuvent compromettre le chiffre d'affaires, la résilience et la conformité réglementaire d'une entreprise.

Pour se protéger, les entreprises doivent aborder la gouvernance et la sécurité en tenant compte du cycle de vie complet des API. Cela inclut la conception, le développement, la phase de test, le déploiement, l'exploitation, et la correction. Ensemble, Akamai API Security et IBM permettent aux entreprises de développer, de déployer et de gérer rapidement des API en toute confiance afin de pouvoir prévenir les incidents, y répondre et évoluer avec leur activité.

Défis

-  Maintenir un inventaire des API sur l'ensemble du parc et identifier les API inconnues
-  Identifier les API non conformes, mal configurées ou vulnérables
-  Détecter et mettre fin à la mauvaise utilisation ou à l'utilisation abusive des API, notamment les attaques de logique métier
-  Concevoir des API sécurisées et cohérentes sans sacrifier la vitesse ou l'agilité
-  Assurer l'alignement et la supervision des programmes de sécurité et de gouvernance des API

Comment Akamai et IBM accompagnent leurs clients

Découvrez votre parc d'API

Vous ne pouvez pas protéger ce que vous ne pouvez pas identifier. Avec Akamai API Security, vous pouvez détecter automatiquement les API, les domaines et les problèmes afin de créer un solide inventaire d'API qui offre une visibilité sur l'ensemble de votre parc d'API. Il n'est pas rare que les entreprises découvrent bien plus d'API qu'elles ne l'imaginaient ou ne s'y attendaient. En outre, vous pouvez trouver facilement des informations exploitables, telles que des données divulguées, afin de comprendre les chemins d'attaque que vos opposants peuvent emprunter. Profitez également d'une intégration fluide avec les éléments d'infrastructure les plus courants adjacents à vos passerelles API et plateformes de gestion pour assurer un partage cohérent des données de sécurité dans l'ensemble de l'entreprise.

Renforcez votre dispositif de sécurité et de gouvernance

Adaptez vos opérations et appliquez de meilleures pratiques lors de l'utilisation d'Akamai API Security pour la gouvernance des API :

- Approfondissez votre compréhension de chaque API de votre écosystème en tenant compte de l'ensemble du contexte métier et alignez-vous sur les meilleures pratiques de gestion des API.
- Simplifiez la communication entre les équipes de développement et de sécurité.
- Identifiez les vulnérabilités, allant des erreurs de configuration aux API non conformes.
- Protégez les données sensibles et surveillez les variations de façon proactive afin de réduire les risques auxquels vos API sont exposées.



Mettez fin aux exploitations et attaques d'API grâce à la protection de l'exécution.

Détectez et bloquez les attaques d'API de la bordure jusqu'au cœur de votre infrastructure (notamment les fuites de données, la falsification de données, les violations de politiques de données, les comportements suspects, etc.) grâce à l'analyse du trafic en temps réel, à la surveillance hors bande, aux options de correction en ligne et aux intégrations de flux de travail pour améliorer l'efficacité du centre d'opérations de sécurité (SOC).

Déployez des API sécurisées plus rapidement avec Active Testing

Intégrez en toute fluidité des tests de sécurité des API à chaque phase du développement des API et détectez les vulnérabilités, les erreurs de configuration et les problèmes de conformité avant que les API ne passent au stade de production. Avec Active Testing, l'équipe DevSecOps peut exécuter une série complète de plus de 200 tests de sécurité axés sur les API, à la demande ou dans le cadre des processus d'intégration continue (CI)/de diffusion continue (CD) de l'entreprise. Active Testing trouve et teste chaque API en se reposant sur une compréhension de la logique métier sous-jacente de l'application, ce qui permet aux développeurs d'identifier des vulnérabilités complexes que d'autres outils de test pourraient manquer.

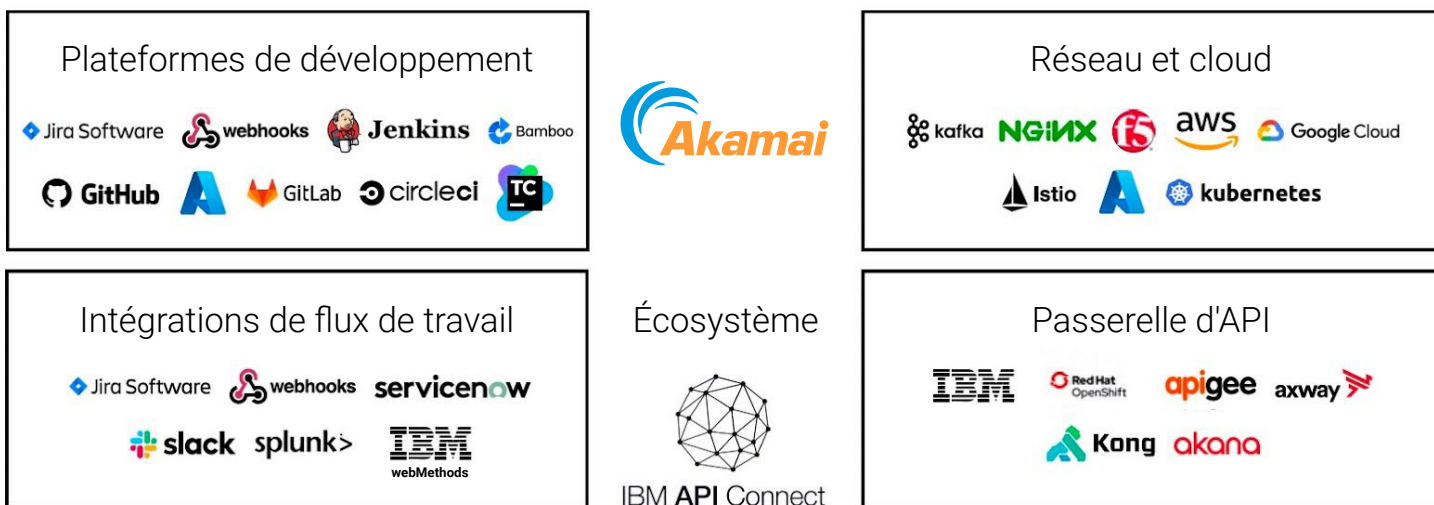
Akamai offre aux utilisateurs IBM une visibilité et une protection accrues grâce à une intégration plus efficace

Akamai API Security s'intègre à API Connect et DataPower sur plusieurs plateformes cloud et options de déploiement. En outre, lorsqu'API Connect gère DataPower, les modifications de configuration unilatérales apportées sont appliquées à tous les systèmes, pour une plus grande efficacité opérationnelle tout en réduisant le risque d'activités de développement non autorisées et non conformes.

Gestion et réponse fluides face aux attaques

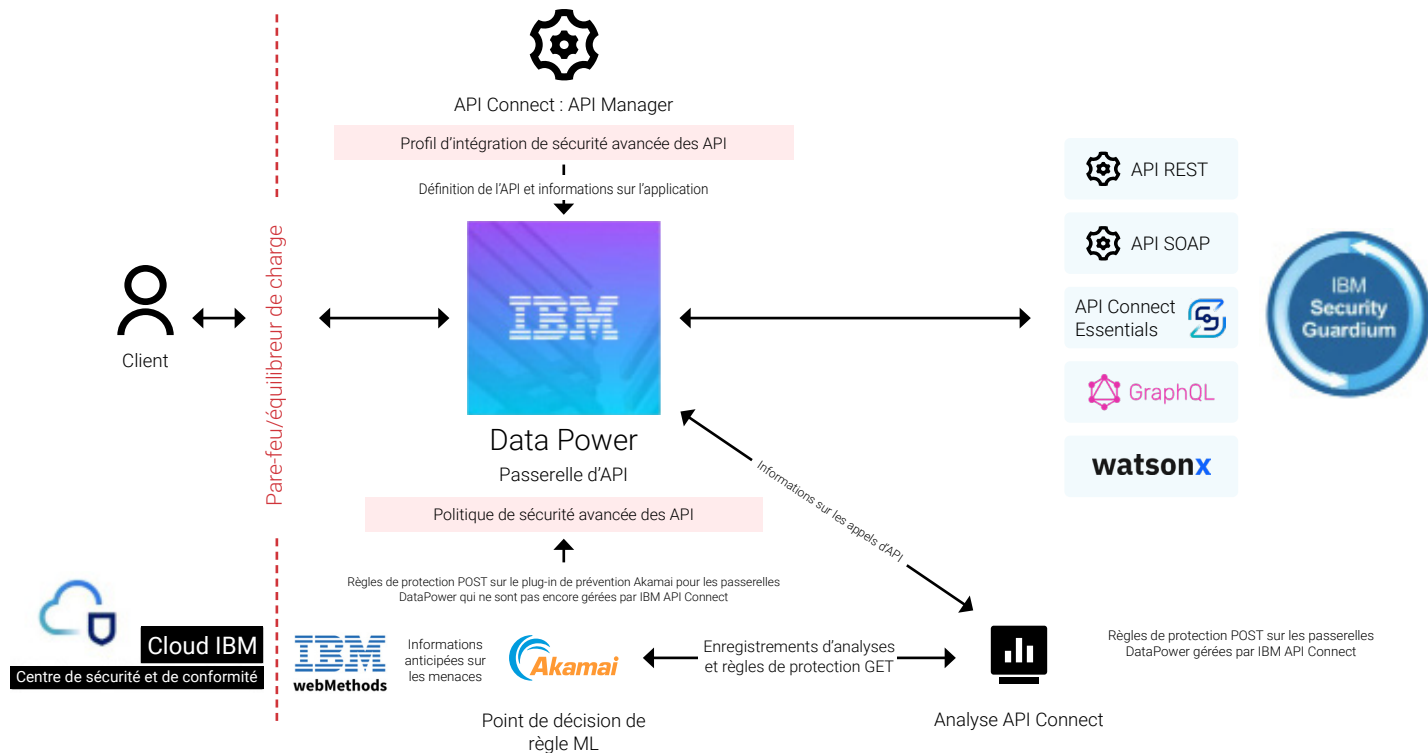
Grâce à l'intégration à la solution Akamai API Security, les clients d'IBM DataPower bénéficient également de la détection et du blocage des menaces en temps quasi réel, sans compromettre les performances ni entraîner de latence, et sans installer de plug-ins supplémentaires sur les passerelles DataPower.

IBM API Connect peut évaluer les demandes d'accès aux ressources en fonction des politiques d'autorisation d'Akamai API Security et mettre en œuvre des règles de blocage sur les clusters IBM DataPower, faisant ainsi passer les délais de correction de quelques jours à quelques minutes ou secondes.



Combinez la puissance d'IBM webMethods et d'Akamai API Security pour une gestion et une protection inégalées des API. Ce partenariat offre une solution complète qui associe les solutions avancées de découverte des API d'Akamai à la gouvernance robuste et à l'intégration des données en temps réel d'IBM webMethods. Bénéficiez d'une visibilité et d'un contrôle complets sur vos API pour garantir la sécurité et la conformité. Cette intégration renforce à la fois vos défenses et votre efficacité, pour que votre entreprise puisse répondre rapidement et en toute sécurité aux demandes dynamiques du marché.

Enfin, les clients d'IBM DataPower peuvent tirer parti de l'intégration eBPF de Red Hat OpenShift d'Akamai pour découvrir les API qui ne sont pas encore gérées par API Connect ou prises en charge par DataPower. Ainsi, ils peuvent détecter et protéger les API qui traitent des données confidentielles et des transactions à haut risque. Ces fonctionnalités s'étendent au-delà des configurations sur site, cloud et hybrides, et sont compatibles avec Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP).



Étapes suivantes

Les API sont l'une des forces motrices qui boostent la capacité des entreprises à répondre aux besoins des clients, à générer des revenus et à se démarquer des concurrents dans une économie digitale qui évolue à toute vitesse. Cependant, leur croissance continue, leur proximité avec les données et la myriade de vulnérabilités auxquelles elles sont exposées en font une cible de choix pour les pirates. Face à l'augmentation constante des incidents de sécurité liés aux API, il est essentiel pour les entreprises de disposer de solutions pour visualiser, sécuriser et tester chaque API dans l'ensemble de leur organisation. Le partenariat entre IBM et Akamai peut fournir aux entreprises la confiance nécessaire pour créer, maintenir et utiliser des API en toute sécurité et à grande échelle.

Découvrez comment nous pouvons vous aider en planifiant une démonstration personnalisée d'Akamai API Security. Vous pouvez également vous adresser à votre contact IBM pour en savoir plus.