Le guide ultime de la découverte des API

Table des matières

L'importance de la découverte des API

Que vous commenciez à vous intéresser à la sécurité des API ou que vous cherchiez à affiner votre stratégie, il est essentiel pour votre entreprise d'identifier et de faire l'inventaire de toutes ses API. Pourquoi ? Pour chaque application que votre entreprise crée, chaque charge de travail migrée dans le cloud et chaque outil que ses employés utilisent pour collaborer, il existe des API qui échangent des données en coulisse (entre autres des données confidentielles). Le problème qui se pose à la plupart des entreprises, même celles qui comprennent l'intérêt d'en faire l'inventaire complet, est qu'elles ne peuvent pas voir une grande partie de leurs API.

Et si vous ne pouvez pas les voir, vous ne pouvez pas les sécuriser.

Dans un contexte où les entreprises centrent de plus en plus leurs activités sur le cloud et le numérique, la portée, l'échelle et la complexité de leur parc d'API augmentent. Les API sont souvent réparties dans plusieurs environnements, sur site et dans le cloud hybride. La complexité est encore accrue du fait que votre écosystème d'API s'étend probablement bien au-delà de votre propre réseau et de votre présence dans le cloud. Pensez à la myriade de connexions que vos API ont établies avec des applications, des services et des systèmes appartenant à des tiers et à des réseaux de développeurs.

À mesure que la portée, l'échelle et la complexité de vos API augmentent, il est difficile d'obtenir des informations en temps réel sur les points suivants :

- L'emplacement de vos API dans les différentes unités commerciales qui, dans de nombreux cas, disposent de leurs propres équipes de développeurs
- La manière dont vos API sont configurées et acheminées et la restriction de leur accès par des dispositifs d'authentification et d'autorisation appropriés
- Si vos API renvoient des données sensibles lorsqu'elles sont appelées, et qui peut accéder à ces données

Pour compliquer les choses, une grande partie des API accumulées par les entreprises ne sont pas gérées, ne sont pas visibles et ne sont souvent pas protégées. Il s'agit notamment des API dormantes, fantômes et zombies qui, dans de nombreux cas, échappent aux défenses des outils couramment utilisés tels que les passerelles API et les pare-feux d'applications Web (WAF). Certes, ces outils offrent des avantages et une protection de base, mais l'écosystème actuel des menaces liés aux API exige un degré plus élevé de visibilité, une protection en temps réel et des tests continus que les solutions spécialisées de sécurité des API peuvent fournir.

Si vous parvenez à découvrir toutes vos API, vous disposerez des bases nécessaires pour passer aux étapes suivantes, telles que l'évaluation des risques de chaque API, l'appréhension de la posture de sécurité de votre société en matière d'API et l'utilisation des connaissances acquises pour appliquer une protection en temps réel et prévenir les attaques. Dans ce livre blanc, nous aborderons :

- ce qui rend certains types d'API si insaisissables pour les équipes de sécurité,
- les fonctionnalités de découverte des API qui peuvent vous aider à gagner en visibilité et à prévenir les attaques.

Pourquoi les API sont-elles si difficiles à découvrir ?

Il n'est pas rare d'avoir des API non gérées en production que personne au sein des équipes d'exploitation ou de sécurité ne connaît, ce qui expose l'entreprise à un éventail de risques de cybersécurité et de difficultés opérationnelles. Les API exposées ou mal configurées sont nombreuses, non protégées et faciles à compromettre pour des acteurs malveillants. Et les enjeux sont très importants. Les attaques contre vos API peuvent compromettre les revenus, la résilience et la conformité réglementaire d'une entreprise.

Voici les sources desquelles les API indésirables peuvent provenir :

1. Raccourcis d'API et échecs de processus

Certaines API indésirables viennent du fait que l'on omet d'informer les bonnes personnes. Par exemple, une équipe métier (LOB) peut créer des API pour répondre à des besoins spécifiques sans en informer le service informatique, ou les développeurs peuvent être plus préoccupés par l'exécution que par le respect de la procédure. Les API « héritées » dans le cadre d'une acquisition sont également souvent négligées. Ces types d'API indésirables sont souvent appelées API fantômes.

2. Anciennes versions d'API

Dans de nombreux cas, l'ancienne version d'une API, dont la sécurité est peut-être plus faible ou la vulnérabilité connue, ne sera jamais supprimée. Deux versions différentes peuvent avoir à coexister un certain temps lors de la mise à jour du logiciel. Mais la personne responsable de la désactivation de l'API peut un jour quitter l'entreprise, être mutée ou simplement oublier de désactiver l'ancienne version. Les API peuvent également être officiellement mises hors service, mais restent en service en raison d'oublis opérationnels. L'un de ces scénarios aboutit à ce qui est parfois appelé une API zombie.

3. API héritées

Les API qui ont été « héritées » dans le cadre de fusions ou d'acquisitions sont également souvent négligées et deviennent des API fantômes. Les inventaires (s'ils existent) se perdent souvent dans les tâches difficiles et compliquées d'intégration de systèmes. Les grandes entreprises qui font de nombreuses acquisitions d'entreprises plus petites sont particulièrement à risque, car les stocks d'API des petites entreprises sont souvent tentaculaires et non documentés.

4. API commerciales

Certaines applications logicielles commerciales incluent des API permettant de se connecter à d'autres applications et sources de données externes. Ces API peuvent parfois être activées sans que personne ne s'en aperçoive.

Qu'est-ce que la découverte des API ?

La découverte d'API est un processus et un ensemble de capacités qui aident les entreprises à identifier, cataloguer, gérer et évaluer les risques liés à leurs API. Effectuée correctement, la découverte d'API peut aider les entreprises à :

- réduire la prolifération d'API (l'accumulation croissante d'API sans documentation ni surveillance appropriée) et améliorer la sécurité,
- mieux appréhender leur écosystème d'API actuel et à prendre des décisions éclairées sur le développement futur,
- surveiller et contrôler l'accès à ces API, en veillant à ce que seuls les utilisateurs autorisés puissent y accéder.

Fonctionnalités clés de découverte des API pour accroître la visibilité et réduire les risques

Il n'est pas rare d'avoir des API dont personne ne connaît l'existence. Or, sans inventaire précis, votre entreprise est exposée à toute une série de risques. Pour inventorier efficacement vos API, vous devez être en mesure de :

Localiser
et inventorier vos API, indépendamment de leur configuration ou leur type

Détecter
les API non gérées, telles que les API dormantes et zombies

Identifier
les domaines oubliés, négligés ou autrement inconnus

Éliminer
les lacunes en matière de visibilité et déceler les voies d'attaque potentielles

Lorsque vous évaluez de nouvelles solutions pour la découverte d'API, gardez à l'esprit les fonctionnalités suivantes, car un outil de découverte doit les intégrer toutes.

Découverte de tous les types d'API

Un outil de détection des API doit être capable d'identifier toutes les API, quels que soient leur configuration ou leur type, y compris RESTful, GraphQL, SOAP, XML-RPC, JSON-RPC et gRPC.

Inventaire des API granulaires

Un outil de découverte des API doit également créer un inventaire mis à jour automatiquement pour éviter qu'il ne devienne obsolète, et donner la possibilité de rechercher, d'étiqueter, de filtrer, d'attribuer et d'exporter des API en fonction de n'importe quel attribut.

Détection des API insaisissables

Les API non gérées peuvent être plus anciennes que les initiatives de sécurité des API de votre entreprise. Une équipe de développeurs ne travaillant plus pour votre entreprise peut être à l'origine de la prolifération des API. Ces API n'ont généralement pas de propriétaire et fonctionnent sans visibilité ni contrôle de sécurité. Il est essentiel que l'outil de découverte localise ces API.

Découverte des domaines d'API fantômes

En plus des API fantômes, vous pouvez avoir des domaines fantômes entiers : des noms de domaine API dont vous ne savez rien. Les outils de découverte des API doivent identifier les domaines fantômes oubliés, négligés ou autrement inconnus qui peuvent présenter un risque pour la sécurité.

Analyse automatique des API

L'analyse est essentielle pour éliminer les angles morts et identifier les problèmes critiques, notamment :

- les divulgations de clés d'API et d'informations d'identification ;
- l'exposition de code API et de schémas ;
- les mauvaises configurations d'infrastructure ;
- les vulnérabilités dans la documentation, les référentiels GitHub, les espaces de travail Postman, etc.

L'identification de ces sources et d'autres sources de renseignements exploitables peut également aider les équipes à comprendre les voies d'attaque potentielles pouvant être exploitées par les cybercriminels.

Aucune intégration requise

Un outil de découverte d'API doit être capable de découvrir l'intégralité de votre parc d'API, de trouver les API vulnérables et les domaines fantômes sans nécessiter d'intégrations spéciales ou l'installation d'un logiciel. Ceci est essentiel pour éviter les lacunes de visibilité susceptibles de survenir si vous n'avez pas installé le(s) bon(s) agent(s) ou configuré l'outil correctement.

Développement personnalisé limité

Enfin, un outil de découverte d'API doit être conçu de manière à ne pas nécessiter de développement personnalisé pour les sources de trafic. Ces outils doivent être fournis avec des intégrations prédéfinies pour les principaux composants de l'infrastructure. Le développement personnalisé est généralement chronophage, et si l'origine de la source est modifiée, l'intégration doit probablement être retravaillée, ce qui n'est pas évolutif pour les équipes de sécurité informatique surchargées.

Comment la solution de sécurité Akamai peut vous aider à détecter toutes vos API

Grâce à des fonctionnalités de découverte d'API complètes et continues, les entreprises peuvent bénéficier des avantages suivants :

- Découverte de l'intégralité de la surface d'attaque des API
- Réduction des coûts des inventaires d'API et des mises à jour de la documentation
- Amélioration de la conformité avec les exigences réglementaires et les politiques internes

Les menaces actuelles nécessitent une solution de sécurité des API complète, englobant quatre domaines critiques : découverte des API, gestion de la posture, détection et correction des menaces et tests de sécurité. Akamai API Security fournit ces quatre modules essentiels, protégeant les API tout au long de leur cycle de vie, du développement à la production. Conçue pour les entreprises qui exposent des API à des partenaires, des fournisseurs et des utilisateurs, notre solution API Security détecte vos API, évalue leur niveau de risque, analyse leur comportement et empêche les menaces de pénétrer dans votre réseau.

En savoir plus sur les méthodes d'attaque des API, les vulnérabilités courantes des API et la façon de sécuriser votre organisation.

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

À propos de la solution de sécurité Akamai

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 d'Akamai, rendez-vous sur **akamai.com** et **akamai.com/blog**, ou abonnez-vous à Akamai Technologies sur **X** (anciennement Twitter) et **LinkedIn**. Publication : 10/24.