Akamai

WHITEPAPER

# 13 Fragen, die Sie Ihrem API-Sicherheitsanbieter stellen sollten

# Einführung

Das Netzwerk von Business-to-Business-APIs wächst exponentiell. Und eine steigende Anzahl an IoT-Geräten (Internet of Things) bietet Entwicklern neue Möglichkeiten, reale Daten über APIs in Anwendungen zu integrieren.

APIs eröffnen zwar viele neue Innovations- und Wachstumschancen, bringen aber auch neue Sicherheitsherausforderungen mit sich, darunter:

- Gestohlene API-Anmeldedaten
- Unerkanntes Ausspähen von APIs
- Falsch konfigurierte Authentifizierung und Autorisierung
- Ungeschützte Shadow- und Zombie-APIs
- Remoteausführung von Code, Injektion, Local File Inclusion und andere Angriffstechniken
- Datenoffenlegungen oder -extraktion
- API-Scraping
- Missbrauch von Geschäftslogik

Sicherheitsanbieter bieten viele Optionen zur Erkennung und Abwehr dieser und anderer API-Bedrohungen an. Nicht alle sind aber gleichermaßen effektiv oder einfach zu bedienen.

Die folgenden 13 Fragen helfen Ihnen im Gespräch mit API-Sicherheitsanbietern und dabei, ihre Produkte auf die API-Sicherheitsanforderungen Ihres Unternehmens hin zu bewerten.

## 1 Kann Ihr API-Sicherheitsprodukt eine unternehmensweite API-Erkennung durchführen?

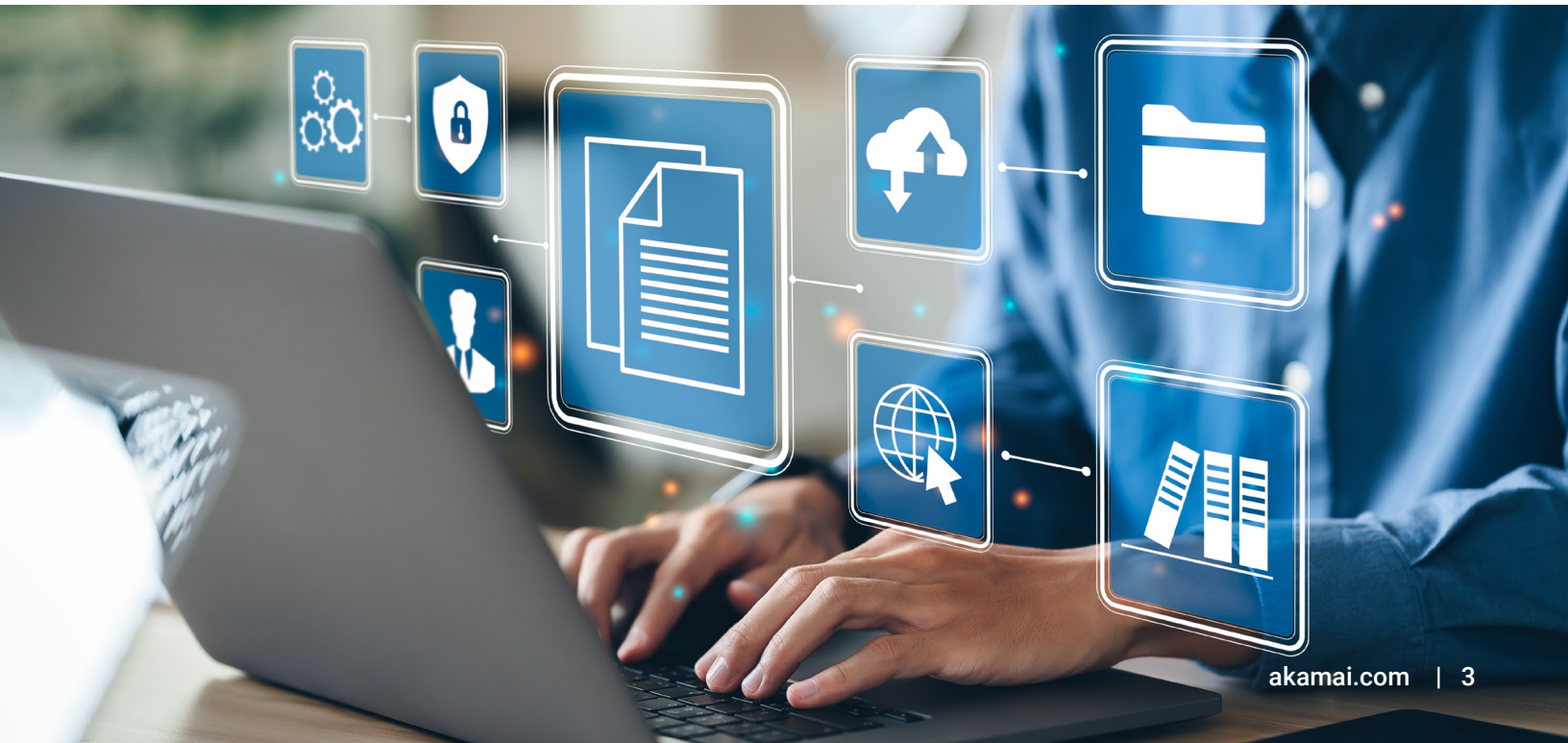
Eines der größten Probleme für Sicherheitsteams besteht darin, dass sie nicht über eine vollständige und genaue Bestandsaufnahme aller APIs verfügen, die in ihrem Unternehmen verfügbar sind. Viele der nicht dokumentierten Shadow-APIs, die Sicherheitsteams nicht vor Augen haben, sind nicht Teil des formalen API-Verwaltungs- und Sicherheitsrahmens. Es ist auch üblich, dass APIs, von denen das Unternehmen dachte, dass sie eingestellt wurden – sogenannte Zombie-APIs – immer noch zugänglich sind. Und selbst unter den genehmigten und dokumentierten APIs können Parameter nicht dokumentierter APIs genutzt werden. Die Erkennung aller North-South-, East-West- und ausgehenden APIs ist unerlässlich. Die einzige Möglichkeit, eine vollständige, unternehmensweite API-Transparenz sicherzustellen, besteht darin, vorhandene API-Aktivitätsdaten aus einer Vielzahl von Technologien und Cloudplattformen zu untersuchen.

## 2 Erkennt Ihr Produkt APIs kontinuierlich und wenn ja, wie viele manuelle Aufgaben benötigt dieser Prozess?

APIs werden aufgrund der sich schnell verändernden DevOps-Prozesse regelmäßig angezeigt und verschwinden wieder. Daher reicht eine zeitnahe Erkennung von APIs nicht aus. Ihr API-Sicherheitsprodukt muss eine kontinuierliche Erkennung durchführen, um neue dokumentierte APIs effektiv zu erfassen, zu analysieren und zu schützen. Es sollte auch zukünftige Vorkommen von Shadow- oder Zombie-APIs erkennen. Darüber hinaus sind Produkte, die Gefahren nicht effektiv interpretieren und abwehren können, sondern dies dem Sicherheitsteam überlassen, langfristig nicht nachhaltig. Produkte, die Automatisierung und maschinelles Lernen sowohl für die Erkennung als auch für die Bewertung von APIs einsetzen, sorgen hingegen dafür, dass Ihr Geschäft reibungslos läuft, und Ihr Team muss sich nicht mehr um manuelle Aufgaben kümmern.

## 3 Wie unterstützt Ihr Produkt meine API-Dokumentationstools und -prozesse?

Ihren Dokumentationsansatz in Ihre API-Sicherheitsplattform zu integrieren hat viele Vorteile. Daher sollten Sie überprüfen, ob Ihr Anbieter über diese Funktion verfügt. Vorhandene Swagger-Dokumentation auf Ihre API-Sicherheitsplattform im Rahmen des CI/CD-Prozesses (Continuous Integration/Continuous Delivery) hochzuladen, sorgt beispielsweise für eine genauere Erkennung von Shadow-APIs und eine bessere Identifizierung von Shadow-Parametern – zumindest dann, wenn der Anbieter erkannte API-Parameter mit bereits dokumentierten Parametern vergleichen kann. Ihre Sicherheitsplattform sollte auch in der Lage sein, nutzerdefinierte Swagger-Dateien mit einem Klick für alle APIs zu erstellen, für die keine Dokumentation vorhanden ist. So können Ihre Entwickler ihre Dokumentationsprozesse beginnen und verbessern.



## 4 Wie viel Zeit und Aufwand wird es in Anspruch nehmen, Ihr Produkt in meiner Umgebung bereitzustellen?

Der schnellste und effektivste Weg ist die Verwendung eines auf Security as a Service (SaaS) basierenden API-Sicherheitsprodukts, das API-Aktivitätsdaten aus Ihren vorhandenen Systemen auf nicht intrusive Weise aufnehmen und analysieren kann. Eine gut konzipierte SaaS-Architektur für API-Sicherheit kann innerhalb von Minuten in Ihre Umgebung integriert werden. Dies kann Ihre Amortisierungszeit deutlich verkürzen und die laufenden Kosten und Risiken im Zusammenhang mit Systemupdates eliminieren. Um noch flexibler zu sein, sollten Sie einen Anbieter finden, der sowohl WAAP (Web Application and API Protection) als auch API-Erkennung und Fehlerbehebung bietet. So können API-Trafficdaten nahtlos zwischen der Lösung, die Ihren eingehenden Traffic schützt, und der Lösung, die den gesamten API-Traffic innerhalb Ihres Unternehmens schützt, fließen.

## 5 Was leistet Ihr Produkt für die Identifizierung und Priorisierung risikobehafteter APIs?

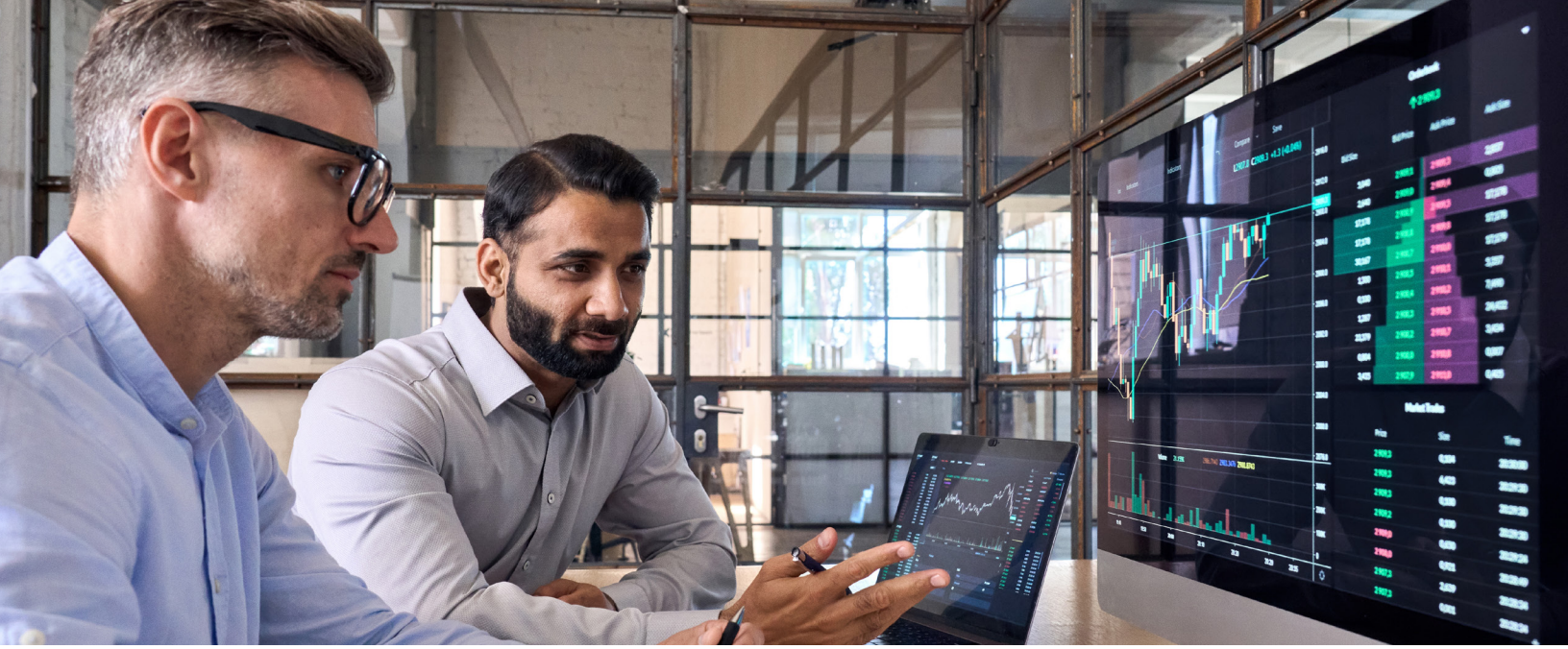
Einen umfassenden API-Bestandsüberblick zum ersten Mal zu sehen, kann zunächst überwältigend sein. Viele Sicherheitsteams werden mit Informationen überflutet und haben daher Schwierigkeiten, die Bereiche zu identifizieren, für die API-Sicherheitsmaßnahmen ergriffen werden sollen. Dies lässt sich am besten vermeiden, wenn Sie ein API-Sicherheitsprodukt auswählen, das einen Großteil dieser Arbeit für Sie erledigt. Dazu gehört:

- Vorhandene APIs hervorheben, die Zugriff auf sensible Daten erlauben
- Sensible Daten automatisch nach Typ kennzeichnen (z. B. personenbezogene Daten, E-Mail-Adressen, Kreditkartendaten usw.)

Ihre API-Sicherheitsplattform sollte es Ihnen auch ermöglichen, nutzerdefinierte Kennzeichnungskategorien zu erstellen, damit Ihre API- und Sicherheitsteams eine gemeinsame Sprache sprechen, die mit Ihren Geschäftszielen und Sicherheitsanliegen in Einklang steht.

## 6 Verwendet Ihr Produkt Verhaltensanalysen, um eine Basis für das erwartete Verhalten zu ermitteln und Auffälligkeiten zu finden?

Viele Arten von Angriffen können mithilfe von Angriffssignaturen, die Angriffe auf WAAP-Ebene blockieren, erkannt werden. Allerdings werden auf diese Weise viele Arten von Angriffen in der Liste der Top 10 in API-Sicherheit des Open Web Application Security Project (OWASP), wie z. B. die Autorisierung auf Objektebene, nicht erkannt. Diese Arten von Angriffen sind passiver und konzentrieren sich auf Geschäftsmissbrauch, sodass sie schwieriger zu erkennen sind. Die einzige Möglichkeit, sich effektiv gegen alle API-Bedrohungsvektoren zu schützen, ist die Verwendung von Verhaltensanalysen und maschinellem Lernen. Echte Verhaltensanalysen erfordern große Datensätze, Algorithmen für maschinelles Lernen, die die Besonderheiten Ihrer Umgebung erlernen, sowie Flexibilität, um sich automatisch auf der Grundlage globaler Informationen zu aktualisieren und anzupassen. Ein SaaS-Modell ist die einzige praktische Möglichkeit, diese Aktivitäten in großem Umfang durchzuführen.



## 7 Können Sie Datensätze erfassen und analysieren, die aussagekräftig genug sind, um eine Basis des normalen Verhaltens effektiv zu ermitteln und Anomalien zu erkennen?

Viele API-Sicherheitsprodukte konzentrieren sich auf die Überwachung einzelner API-Aufrufe oder bestenfalls auf kurzfristige Sitzungsaktivitäten. Dies ist nicht ausreichend, da viele legitime Geschäftsprozesse – und viele Angriffe – über einen viel längeren Zeitraum hinweg stattfinden. Die API-Nutzung muss über einen längeren Zeitraum (mindestens 30 Tage) analysiert werden. Dies bietet eine vollständigere und genauere Basis für das erwartete Verhalten, einschließlich aller Geschäftsprozesse, die nur einmal pro Monat stattfinden (z. B. Abrechnungen). So können auch Angriffe erkannt werden, die langsam über mehrere Tage oder Wochen hinweg ausgeführt werden – und über mehrere API-Sitzungen hinweg.

## 8 Kann Ihr Produkt jede Einheit, Beziehung und Aktivität innerhalb von API-Rohdaten identifizieren, um den Geschäftskontext bereitzustellen?

Die beste Möglichkeit, API-Aktivitätsdaten zu nutzen, besteht darin, sie mit Kontext über die geschäftlichen Auswirkungen der API-Nutzung zu ergänzen. Die folgenden Identifizierungs- und Kennzeichnungsfunktionen sind für Ihre API-Sicherheitsplattform unerlässlich, um die Beziehungen zwischen den verschiedenen Einheiten zu bewerten und zu profilieren:

- Darstellungen von API-Nutzern (Nutzerentitäten), wie IP-Adressen, API-Schlüssel, Zugriffstoken, Nutzer-ID, Partner-ID, Händler-ID, Provider-ID usw.
- Darstellungen von Geschäftsprozessen (Geschäftsprozesseinheiten), wie Reservierungen, Zahlungen, Abrechnungen, Kontoguthaben, usw.

Nur mit einer ausführlichen Analyse auf dieser Ebene kann die riesige Menge an Daten, die von APIs generiert werden, in eine aussagekräftige und verständliche Basis für das erwartete Verhalten umgewandelt werden.

## 9 Kann Ihr Produkt jede Aktivität von jeder Einheit in Ihren APIs auf einer Zeitachse darstellen, um Verhaltensänderungen im Laufe der Zeit anzuzeigen?

Obwohl das Verständnis und die Überwachung von API-Aktivitäten und -Bedrohungen auf Makroebene entscheidend ist, ist es ebenso wichtig, den Schwerpunkt Ihrer Analyse auf bestimmte Entitäten zu beschränken. Wenn beispielsweise ein auffälliges Verhalten für einen bestimmten Geschäftspartner festgestellt wird, müssen alle Aktivitäten dieser Einheit in einer Zeitachse angezeigt werden. Dasselbe gilt für Geschäftsprozesseinheiten. Wenn die Ereignisse in einer Zeitachse für jede Einheit innerhalb Ihrer APIs vollständig dargestellt werden, haben Sie einen leistungsstarken Überblick über die normale Nutzung und den Missbrauch. Die Aktivität zurückverfolgen zu können, um zu sehen, was vor und nach einer Warnung passiert ist, ist von entscheidener Bedeutung, um den Missbrauch von Geschäftslogik zu verstehen.

## 10 Wie kann ich Ihr Produkt in vorhandene Tools, Prozesse und Workflows integrieren?

Das Senden von Warnmeldungen an Ihr SIEM-Produkt (Security Information and Event Management) ist hilfreich, aber nicht ausreichend. Sicherheitsteams verwenden zunehmend ausgefeiltere Tools für Orchestrierung, Automatisierung und Reaktion im Bereich Sicherheit (SOAR), um vordefinierte Workflows zu initiieren, wenn Sicherheitsbedrohungen und -vorfälle erkannt werden. Und da viele API-Sicherheitsprobleme Maßnahmen von Entwicklern außerhalb des Sicherheitsteams erfordern, muss Ihre API-Sicherheitsplattform auch in die Tools zur Problemverfolgung und Workflow-Verwaltung des Entwicklungsteams integriert werden. Wenn Ihr Sicherheitstool API-Traffic analysiert, sollte es auch APIs verwenden, um Antworten in Ihrem CDN, Ihrer Web Application Firewall oder Ihrem API-Gateway zu orchestrieren und Ihnen die Erstellung eigener Playbooks zu ermöglichen.

## 11 Kann ich die API und Aktivitätsdaten Ihres Produkts nach proaktiver Bedrohungssuche und Risikominderung abfragen?

Integrationen von Sicherheits- und Entwicklungstools können nicht nur Blackboxen sein, die einseitige Warnungen an Ihre Tools senden. Ihre Sicherheits- und API-Teams müssen in der Lage sein, die Quelldaten hinter einer Warnung oder einem Problem zu erfassen. Nutzen Sie API-Sicherheitsplattformen, mit denen Nutzer API-Details direkt über eine integrierte Web-Nutzeroberfläche oder über APIs abfragen können, die die Integration der API-Sicherheitsplattform mit anderen bevorzugten Tools und Schnittstellen ermöglichen. So können Sie es Ihrem Sicherheitsteam ermöglichen, eine proaktive Bedrohungssuche effizient und effektiv durchzuführen. Darüber hinaus hilft es Ihren Entwicklern und Stakeholdern außerhalb des Sicherheitsteams zu verstehen, wie APIs angegriffen werden, während sie legitim verwendet werden.

12

## Welche Schritte unternehmen Sie, um sicherzustellen, dass die vertraulichen Daten, die Sie über mein Unternehmen erfassen, geschützt sind?

Die fortschrittlichen Verhaltensanalysen, die erforderlich sind, um APIs vor der heutigen Bedrohungslandschaft zu schützen, sind nur mit der Skalierbarkeit der Cloud möglich. Angesichts der Größe und Vertraulichkeit Ihres API-Datensatzes ist es wichtig, Ihren Sicherheitsanbieter diese Fragen zu stellen, um zu gewährleisten, dass Ihre Daten geschützt werden. Die Praktiken zu überprüfen, die Ihr Anbieter zur Sicherung seiner Cloudinfrastruktur verwendet, ist wichtig, aber nicht ausreichend. Verlangen Sie von Ihrem API-Sicherheitsanbieter die Verwendung von Techniken wie Tokenisierung, d. h. sensible Daten vor der Übertragung an die Cloud durch anonymisierte Token zu ersetzen. Dadurch wird der Datenschutz auch dann gewährleistet, wenn der Anbieter – oder sein vorgelagerter Cloudanbieter – einen Sicherheitsvorfall erlebt.

13

## Bietet die Lösung einen granularen Zugriff auf API-Aktivitätsdaten?

Daten sind ein entscheidendes strategisches Element für alle Bereiche, von Compliance bis hin zu Kontext für den Angriffsschutz. Viele Anbieter bieten im Laufe der Zeit ihre eigene Version des Speichers für API-Daten an. Sie sollten jedoch genauer nachforschen, um zu verstehen, was wirklich angeboten wird. Lösungen, die nur Warnungen anbieten, reichen nicht aus, denn eine kompromittierte API-Aktivität kann langsam und im Laufe der Zeit auftreten – nicht nur dann, wenn eine Warnung erfolgt. Alternativ kann ein umfassender Anbieter Schwachstellen beseitigen, indem er alle API-Aktivitäten aufzeichnet und die Tools zur detaillierten Überprüfung dieser Aktivität bereitstellt, anstatt sie in einem lernfähigen Modell zu verlieren. Dieser granulare Zugriff auf Ihre Daten ermöglicht eine proaktive Überwachung; Sie müssen also nicht mehr nur rückwirkend reagieren, nachdem ein Angriffsangriff ausgelöst wurde.

## 13 Fragen, die Sie Ihrem API-Sicherheitsanbieter stellen sollten

1. Kann Ihr API-Sicherheitsprodukt eine unternehmensweite API-Erkennung durchführen?
2. Erkennt Ihr Produkt APIs kontinuierlich und wenn ja, wie viele manuelle Aufgaben benötigt dieser Prozess?
3. Wie unterstützt Ihr Produkt meine API-Dokumentationstools und -prozesse?
4. Wie viel Zeit und Aufwand wird es in Anspruch nehmen, Ihr Produkt in meiner Umgebung bereitzustellen?
5. Was leistet Ihr Produkt für die Identifizierung und Priorisierung risikobehafteter APIs?
6. Verwendet Ihr Produkt Verhaltensanalysen, um eine Basis für das erwartete Verhalten zu ermitteln und Auffälligkeiten zu finden?
7. Können Sie Datensätze erfassen und analysieren, die aussagekräftig genug sind, um eine Basis des normalen Verhaltens effektiv zu ermitteln und Anomalien zu erkennen?
8. Kann Ihr Produkt jede Einheit, Beziehung und Aktivität innerhalb von API-Rohdaten identifizieren, um den Geschäftskontext bereitzustellen?
9. Kann Ihr Produkt jede Aktivität von jeder Einheit in Ihren APIs auf einer Zeitachse darstellen, um Verhaltensänderungen im Laufe der Zeit anzuzeigen?
10. Wie kann ich Ihr Produkt in vorhandene Tools, Prozesse und Workflows integrieren?
11. Kann ich die API und Aktivitätsdaten Ihres Produkts nach proaktiver Bedrohungssuche und Risikominderung abfragen?
12. Welche Schritte unternehmen Sie, um sicherzustellen, dass die vertraulichen Daten, die Sie über mein Unternehmen erfassen, geschützt sind?
13. Bietet die Lösung einen granularen Zugriff auf API-Aktivitätsdaten?

**Wie Sie vielleicht bereits wissen, bietet Akamai API Security die in dieser Liste empfohlenen Schutzmaßnahmen. Entdecken Sie unsere Lösungen.**