WHITE PAPER

# Erkennung von Anomalien mit Akamai API Security

APIs sind eine Schlüsselkomponente für die Fähigkeit Ihres Unternehmens, Kunden zu dienen, Umsätze zu erwirtschaften und effizient zu arbeiten. Das kontinuierliche Wachstum, die Nähe zu sensiblen Daten und das Fehlen von Sicherheitskontrollen machen APIs in der heutigen Zeit jedoch zu einem attraktiven Ziel für Angreifer. Echtzeit-Einblicke in das Nutzerverhalten sind entscheidend, um proaktiv Anzeichen für möglichen API-Missbrauch oder einen Angriff zu erkennen.

Dank der Funktionen von Akamai API Security zur Erkennung von Anomalien wird anormales Nutzerverhalten identifiziert, das auf potenziell böswillige Versuche hinweist, die APIs des Unternehmens auszunutzen. Die Anomalieerkennungsfunktionen von Akamai legen eine Baseline für normalen Traffic fest und können so eingehende Anfragen mit der Baseline vergleichen und feststellen, ob sie möglicherweise von einem Angreifer kommen.

Unser Algorithmus zur Erkennung von Anomalien identifiziert z. B. folgendes anomales Verhalten:

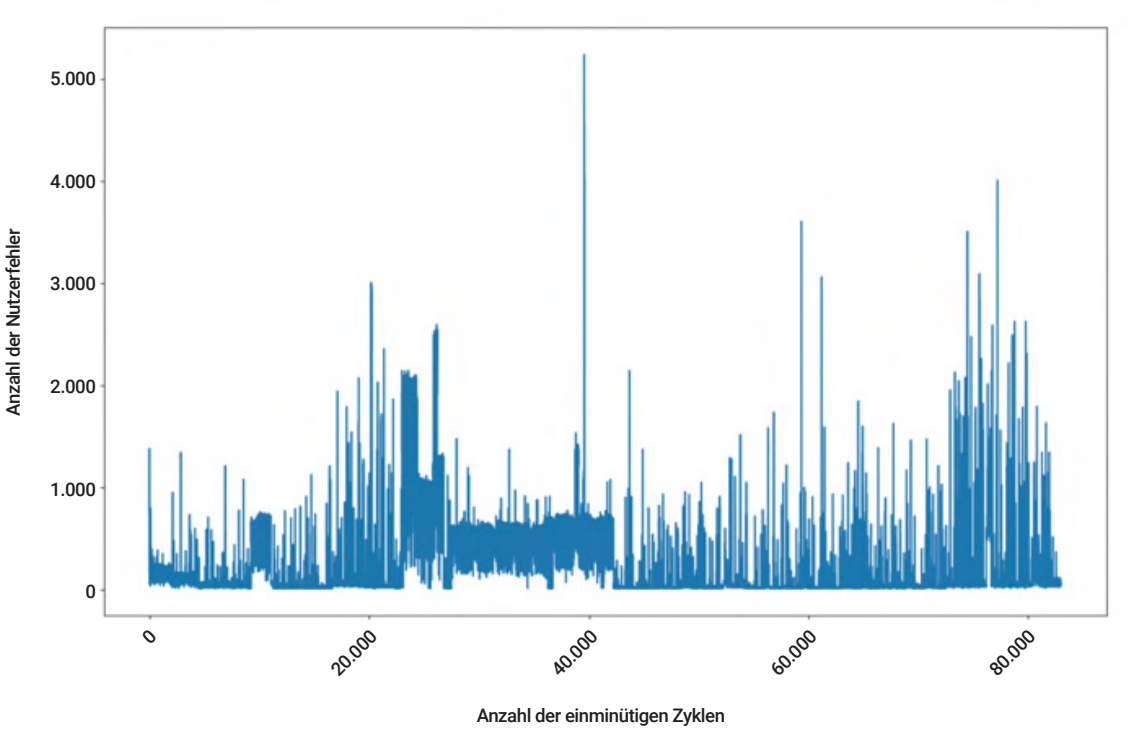
- Es wird ein unerwartetes Feld in der API-Anfrage verwendet.
- Es werden mehr Daten vom Server abgerufen als bei normalen Nutzern.
- Es wird versucht, andere Nutzer-/Admin-Ressourcen zu verwenden.
- Die APIs werden in unerwarteter Reihenfolge aufgerufen.

Der Algorithmus basiert auf einem unbeaufsichtigten Modell mit online lernender KI und maschinellem Lernen (KI/ML), das die vielfältigen Merkmale des statistischen Trafficverhaltens erlernt und nach einer festgelegten Lernphase anormale Vorfälle erkennt. Unser Modell kann sich an Veränderungen im Traffic im Zeitverlauf und an Anomalien, die von Nutzern als False Positives gekennzeichnet werden, anpassen.

Während der Lernphase analysiert unser System die Daten des Kunden und identifiziert die verschiedenen APIs, Authentifizierungsmethoden, Nutzer, Datentypen usw. Wie für jede API entwickelt das Modell eine Liste mit Funktionen des üblichen Nutzertraffics, einschließlich der Anzahl der API-Treffer, der Anzahl der verursachten Fehler, des Prozentsatzes der zugelassenen Anfragen, der Menge der vom Server abgerufenen Daten und mehr. Unser Algorithmus erkennt Nutzeranomalien, indem er die Eigenschaften des Nutzers und der API mit den Ergebnissen des statistischen Modells, das unser Algorithmus erlernt hat, vergleicht.

# Funktionsweise der Anomalieerkennung von Akamai API Security

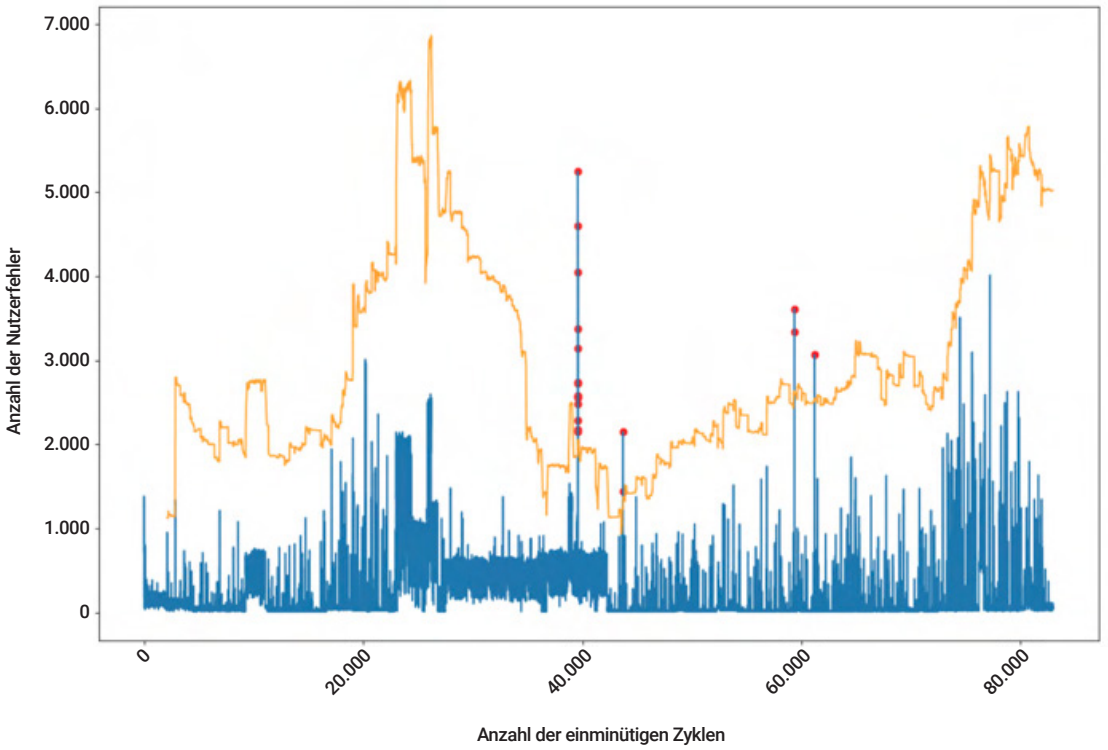
Die Funktionen von Akamai API Security zur Erkennung von Anomalien identifizieren Nutzer, die deutlich mehr Fehler verursachen als andere Nutzer. So können wir Angriffe wie Brute Force, Pfadabtastungen und Scraping identifizieren. Das folgende Diagramm zeigt, wie viele Fehler ein Nutzer in einer Umgebung innerhalb eines einminütigen Zyklus maximal generieren kann.




Beim Identifizieren von Anomalien in diesem Szenario gibt es mehrere Herausforderungen:

1. Das Modell muss bei der Berechnung des Schwellenwerts Datenabweichungen berücksichtigen.
2. Das Modell sollte während der Lernphase keine Anomalien erlernen.
3. Das Lernen erfolgt in Echtzeitströmen, d. h. das Modell sieht nie die gesamten Daten und muss jeden Zeitschritt anpassen.
4. Warnungen müssen in Echtzeit erfolgen, daher kann sich unser Algorithmus nicht auf zukünftige Daten verlassen, um eine Anomalie vorherzusagen.
5. Damit der Nutzer nicht zu viele Warnungen erhält, muss unser Modell einen statistisch garantierten Schwellenwert für die Daten ermitteln.

Die folgende Abbildung zeigt, wie unser Modell diese Anforderungen erfüllt, indem es die Schwellenwerte entsprechend den eingehenden Daten anpasst.




Die orangefarbene Linie stellt die vom Modell berechnete Schwellenwertfunktion dar und die roten Punkte sind die Anomalien, die aufgrund dieser Funktion erkannt wurden.

# Häufig gestellte Fragen

### Wie lange ist die Lernphase des Algorithmus von Akamai zur Anomalieerkennung?

Die meisten unserer Algorithmen benötigen eine Lernphase von zwei bis sieben Tagen. Darüber hinaus hängt die Dauer der Lernphase davon ab, wie viele verschiedene Arten von Nutzerverhalten während der Lernphase beobachtet wurden.

### Wie lange dauert es, bis eine Warnung generiert wird, wenn ein anormales Verhalten erkannt wurde?

Unser Algorithmus erstellt meistens innerhalb von 30 bis 60 Sekunden eine sachdienliche Warnung für den Kunden – gemessen ab dem Zeitpunkt ab dem der anormale Traffic empfangen wurde.

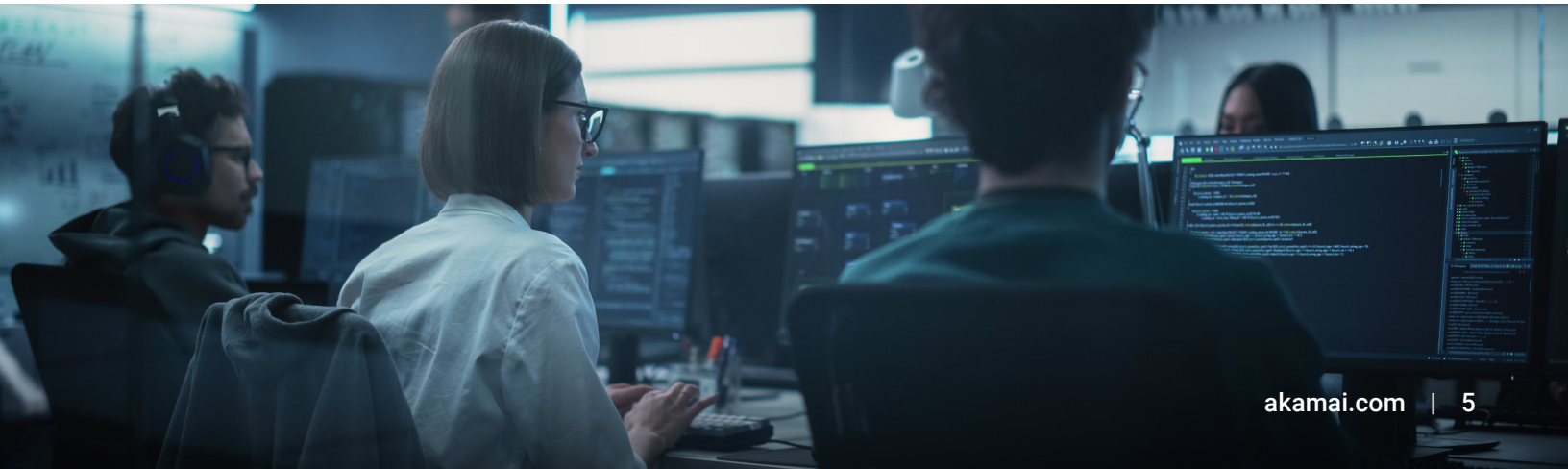
### Verwendet der Algorithmus ein beaufsichtigtes oder unbeaufsichtigtes Modell?

Unser Algorithmus basiert auf einem unbeaufsichtigten Modell, das es ihm ermöglicht, sich an die Umgebung jedes Kunden anzupassen, ohne vorher mehr über ihre Eigenschaften zu wissen. Darüber hinaus nutzt unser Algorithmus Online-Lernen, um sich im Zeitverlauf an Veränderungen in der Umgebung anzupassen.

### Welche Arten von Anomalien werden von Akamai API Security erkannt?

Akamai API Security erkennt zwei Arten von Anomalien:

- Musterbasierte Anomalien: Diese basieren auf der Identifizierung schädlicher Trafficmuster, z. B. Techniken zur Ausnutzung von Internetschwachstellen und bekannte schädliche User-Agents wie Befehlsinjektion, Pfadüberschreitung und verdächtige User-Agents.
- Verhaltensbasierte Anomalien: Diese Anomalien basieren auf dem Erlernen des Nutzerverhaltens und der Identifizierung anormalen Nutzerverhaltens, etwa übermäßige API-Nutzung, Bereichsverletzung und fehlerhafte Autorisierung auf Objektebene (BOLA).



### Welche Parameter berücksichtigt Akamai API Security bei der Anomalieerkennung?

Unsere Algorithmen basieren auf mehreren Funktionen, die auf einer statistischen Analyse des Traffics basieren, darunter:

- Anzahl der unterschiedlichen Nutzer, die eine API verwenden
- Authentifizierungsstatus der API
- Antwortcode des Servers
- Datenmenge, die vom Nutzer abgerufen wird
- IP-Standort des Nutzers
- User-Agent des Nutzers, usw.

### Kann der Nutzers die Empfindlichkeit des Algorithmus steuern?

Ja, der Nutzer kann für jede Anomalie steuern, wie empfindlich die Erkennung reagieren soll, indem er die Empfindlichkeit der entsprechenden Richtlinie verändert. Die Richtlinienempfindlichkeit entspricht einer Zahl zwischen 1 (niedrig) und 5 (hoch), wobei das System beim höchsten Wert am sensibelsten reagiert. Diese Empfindlichkeit kann für jede Anomalierichtlinie in Akamai API Security konfiguriert werden. Unser Algorithmus berücksichtigt diesen Parameter als Teil des Modells.

### Kann der Nutzer ein erkanntes Problem, vor dem Akamai gewarnt hat, als False Positive bewerten? Und wie wirkt sich dies auf den Algorithmus aus?

Ja, zur Verbesserung der Anomalieerkennung können Nutzer bestimmte Probleme als „False Positive“ markieren. Wenn ein Problem als False Positive kategorisiert wird, berücksichtigt unser Algorithmus dies und passt das Modell entsprechend der Nutzereingabe an.

### Wie vermeidet Akamai, dass Kunden zu viele Warnungen erhalten, wenn ein Nutzer immer dasselbe Angriffsszenario auslöst?

Unser Algorithmus identifiziert ähnliche Probleme, die immer wieder von demselben Nutzer und derselben API ausgelöst werden. In diesem Fall ignoriert unser Algorithmus ähnliche Probleme für einen gewissen Zeitraum.

### Wie geht Akamai mit Abweichungen/saisonal bedingten Schwankungen in den Daten um?

Akamai API Security verwendet verschiedene Algorithmen, um Anomalien in den Daten zu erkennen. Je nach zugrunde liegender Datenvorverarbeitung und Komplexität des Algorithmus können wir die Schwellenwertanpassung lockern oder Anpassungen in jedem Zyklus durchsetzen, in dem wir garantierte statistische Schwellenwerte für die Erkennung von Anomalien benötigen. In Verbindung mit der Spam-Kontrolle bieten wir eine problemlose Schnittstelle, selbst wenn ein bestimmter Algorithmus zusätzliche Zyklen benötigt, um die Schwellenwerte anzupassen.

### Wie geht Akamai mit Data Poisoning um?

Als Online-Lernalgorithmus muss Akamai API Security eine Vielzahl von Herausforderungen bewältigen, darunter:

- Neue APIs
- Neue Felder in vorhandenen APIs
- Änderung des Wertetyps/-bereichs in einem Feld
- Probleme mit der Serververfügbarkeit
- Fehler in APIs, die Fehlfunktionen (404, 500 usw.) und andere Herausforderungen verursachen können, wenn der Algorithmus entscheiden muss, ob diese Fehler erlernt werden sollen oder nicht (Akamai trifft Vorsichtsmaßnahmen, um diese Anomalien nicht zu erlernen, indem eine Kombination aus minimaler Nutzeranzahl, Zeitraum und Hartnäckigkeit erforderlich ist, um den Lernprozess auszulösen.)

## Erfahren Sie, wie wir Sie unterstützen können, und vereinbaren Sie eine individuelle Demo zu Akamai API Security.

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. Gemeinsam mit Ihnen können wir auf diese Weise Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn. Veröffentlicht: 12/24.