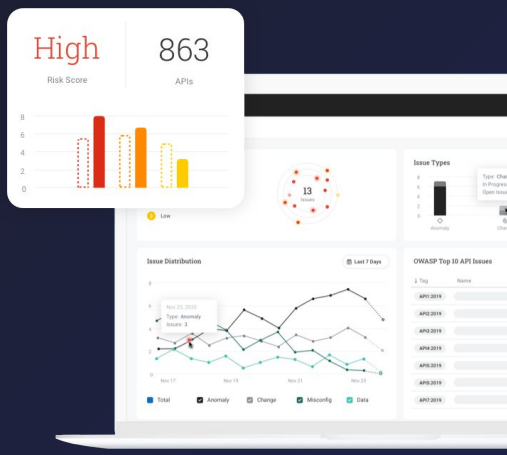
noname

Product Brief

API-Sicherheitsplattform der Enterprise-Klasse



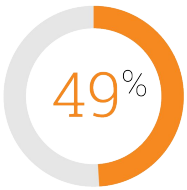
Noname Security ist ein führender Anbieter von Lösungen für das **API-Sicherheitsmanagement**, die **Erkennung und Abwehr API-basierter Bedrohungen** und die **Sicherung des API-Entwicklungszyklus**.

Die digitale Transformation erfordert eine API-Transformation

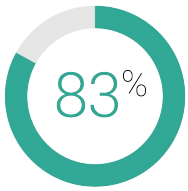
APIs gehören zu den Grundbausteinen der digitalen Welt. Sie (APIs) sind eine effiziente und entwickler freundliche Wertschöpfungsmethode, da sie zur flexiblen, schnellen und portablen Verknüpfung von Software und Datenressourcen genutzt werden können. Viele Initiativen zur digitalen Transformation beschleunigen die Nutzung von APIs, darunter:

- Services in öffentlichen Clouds
- auf Microservices beruhende Anwendungs-designs
- Open Banking
- Gesundheits-Apps
- neue Ökosysteme für Unternehmen und Entwickler
- Back-Office-Digitalisierung
- Wachstumstrends – GraphQL, gRPC, Webhooks

2022 wird die API-Nutzung weiter stark steigen



2020 stieg die Zahl der API-Aufrufe um 49%



2019 wurden 83% des Webtraffics von APIs verschickt

In Unternehmen, die ihre Geschäftsprozesse auf APIs aufgebaut haben, ist die Anzahl der API-bedingten Sicherheitsvorfälle jedoch erheblich gestiegen. Gartner zufolge werden APIs schon 2022 der wichtigste Angriffsvektor für Webanwendungen sein. Und laut IBM spielen falsch konfigurierte APIs bei zwei Drittel aller Cyberangriffe in der Cloud eine maßgebliche Rolle.

Noname Security schützt APIs in Echtzeit und erkennt Schwachstellen und Fehlkonfigurationen, bevor sie ausgenutzt werden. Die Noname API Security Platform ist eine Out-of-Band-Lösung, die sich mit Ihren API-Gateways, Load Balancern und WAFs verknüpfen lässt, um sowohl die Transparenz als auch die Sicherheit zu verbessern.

API-Sicherheit

Erstellen Sie ein Register sämtlicher APIs, einschließlich älterer und Schatten-APIs, mit **Datenklassifizierung.**

Identifizieren Sie **Fehlkonfigurationen** und **Schwachstellen** in Quellcode, Netzwerkkonfigurationen und Richtlinien.

Erkennung und Abwehr

Nutzen Sie verhaltensbasierte Modelle zur **Laufzeiterkennung von API-Bedrohungen.**

Automatisieren Sie das **Blockieren und Beseitigen** von Bedrohungen ganz oder teilweise.

Vertrauenswürdiger API-Code

Testen Sie APIs kontinuierlich, um Risiken aufzudecken, bevor sie ausgenutzt werden.

Erstellen Sie automatisch und dynamisch Tests und binden Sie diese in die CI/CD-Pipelines ein.

So geht Noname die API-Sicherheit an

Inventarisierung aller APIs, Daten und Metadaten

Finden und inventarisieren Sie APIs aller Art, wie HTTP, RESTful, GraphQL, SOAP, XML-RPC und gRPC. Identifizieren und katalogisieren Sie auch ältere und nicht konforme APIs, die von keinem API-Gateway verwaltet werden, sowie deren Merkmale und Metadaten.

Analyse des API-Verhaltens und Erkennung API-basierter Bedrohungen

Nutzen Sie automatisierte, KI-basierte Erkennungsmethoden, um ein extrem breites Spektrum an API-Schwachstellen aufzudecken, darunter Datenlecks, Datenmanipulation, Fehlkonfigurationen, Verstöße gegen Datenrichtlinien, verdächtiges Verhalten und Angriffe.

Verhinderung von Angriffen und Behebung von API-Schwachstellen

Verhindern Sie Angriffe in Echtzeit, beheben Sie Fehlkonfigurationen, lassen Sie Firewallregeln automatisch aktualisieren, richten Sie Webhooks in Ihren WAFs ein, die neue Richtlinien zum Unterbinden verdächtiger Verhaltensweisen erstellen, und binden Sie diese in Ihre vorhandenen Arbeitsabläufe (wie die Ticket-Erstellung und SIEMs) ein.

Aktive API-Tests vor der Produktivsetzung

Die meisten Anwendungen werden vor der Überführung in die Produktion getestet. Die meisten APIs hingegen nicht. Testen Sie APIs im Rahmen des Softwareentwicklungszyklus (Shift Left Approach) aktiv, um etwaige Probleme vor der Produktivsetzung zu identifizieren.

noname

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD API Security category North America

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2022 GOLD Fastest Growing Cybersecurity Company North America

Über Noname Security

Noname Security bietet eine äußerst leistungsstarke, umfassende und anwenderfreundliche API-Sicherheitsplattform, mit der Unternehmen alle älteren und modernen APIs finden, analysieren, testen und etwaige Regelwidrigkeiten beheben können. Fortune 500-Unternehmen nutzen die Noname API Security Platform zum Schutz ihrer Umgebungen vor API-Angriffen sowie zur Behebung von Schwachstellen und Fehlkonfigurationen. Noname ist ein privat geführtes Unternehmen mit Hauptsitz in Palo Alto, Kalifornien, und einer Niederlassung in Tel Aviv und Amsterdam.

Nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371