Enterprise API Security

Summary

APIs are the backbone of modern web, cloud, and mobile applications. Signal Sciences protects APIs no matter where or how our customers deploy them.

Application Programming Interfaces (APIs) enable organizations to share data with authorized software developers who leverage that valuable data in their own applications. As a component of modern business innovation and software development, APIs enable applications to exchange data and, in effect, "talk to" one another. But the risk of exposing valuable data via APIs is real: Gartner estimates that by 2022, API abuses will be the most-frequent attack vector for enterprise web applications data breaches[1]. Clearly, API security must be part of any strategic security plan.

Signal Sciences is the only web application security solution that defends against a wide variety of threats at the API layer, including the following major API security categories

[1] Gartner: How to Build an Effective API Security Strategy

API Security Categories

Category	Attack Scenarios
Unique Identifier Enumeration	Brute forcing sensitive IDs or tokens in APIs that are not searchable or public leads to discovery and exposure of sensitive customer data, unpublished media, payment information, PII, and other confidential data.
Account Takeover (a.k.a. “Credential Stuffing”)	Attackers use known lists of compromised credentials from common password lists and breach data dumps to try to gain access to customer accounts through authentication APIs.
Sensitive API Abuse	Targeting sensitive APIs such as gift card and credit card validation and attempting to validate stolen credit cards, perform ecommerce gift card fraud, obtain patient healthcare records.
Malicious bots	Malicious automation and bots are used to perform content scraping, tie up system resources, perform account brute forcing, and other actions.
Partner misuse	While organizations want to provide partners with access to APIs to automate workflow, partners can easily accidentally overwhelm API endpoints and create resource exhaustion or excessive costs through unintended spikes in API requests.
Malicious or disallowed traffic sources	Bad actors using Tor attempt to access APIs from countries or geographies where services aren’t legitimately provided. Or they attempt to perform transactions from OFAC countries blocked due to regulatory compliance.
Insider Threat	User management APIs abused by insiders to grant elevated access or perform a high number of permissions changes.

Category	Attack Scenarios
Policy Enforcement	APIs attempting to be used from an untrusted device that does not contain the right cookie or device identifier.
OWASP Injection Issues / Virtual Patching	APIs using unpatched or outdated third party frameworks / libraries, and injection issues such as Command Execution, XSS, SQL Injection, and others.
Rate limiting	Malicious attack tooling that performs a high velocity of requests leading to stolen content or resource exhaustion.
Denial of Service	Targeting high system cost APIs such as database queries, search pagination, data exports, etc.

Signal Sciences prevents the above API layer attacks with our patented architecture that provides organizations working in a modern development environment with comprehensive and scalable threat protection and security visibility.

No matter how you deploy your APIs, Signal Sciences can protect them.

Signal Sciences runs natively in any cloud, data center, or container, with a variety of deployment options at the code, web server or API layer. Learn how our patented approach can help secure your web layer assets at signalsciences.com.

> **“ Getting Signal Sciences up and running is quick and easy. It was literally a five minute process: with just a few Signal Sciences rules changes specific to our authentication flows, we were able to effectively block account takeover attempts in production.**
>
> Robert Davis, Director of Cybersecurity, Chick fil-A