AppSentinels.ai
Application Security Re-invented

# API Security Buyer's Guide

# API Security Buyer's Guide

In the digital age, business leaders see software teams as core to the business and demand them to innovate faster in response to market and competitive demands. Organizations are on the path of fast iteration - experimenting with new products or features, gauging customer feedback, adopting or dropping, and moving to the next thing. The pace of change is not an option but existential for organizations. Organizations that can adapt will gain market shares, and organizations that cannot will cease to exist.

In response to this need, engineering leaders are constantly looking at ways to make software delivery faster and better. Application architectures have evolved with major shifts like Agile delivery, Micro-services architectures, Cloud/SaaS instead of static infrastructure, etc. Engineering and Security leaders are working hard to keep up with the pace but are not expected to slow down even if they are unprepared or have blind spots.

APIs have become critical in helping organizations innovate fast. APIs power all next-generation technologies like Cloud, SaaS, Mobile, IoT, Serverless, and even No-code/Low-code frameworks, as well as integrations with customers, vendors, and partners. While APIs were already ubiquitous, the pandemic has further accelerated growth in innovation and mass adoption of digital services powered by cloud, mobile, and APIs.

By its very nature, APIs expose application logic and sensitive data such as personally identifiable information and hence become attractive targets for hackers. APIs make application development simpler, in a similar way, they also simplify constructing an attack by a malicious user. As a result, APIs are increasingly used by attackers. Infact Gartner says, API-based attacks are the most frequent attack vector since 2022, bypassing all other attack methods. Hence, organizations must take API Security seriously.

Organizations face a variety of API attack techniques, from traditional methods described in OWASP Web Top-10 to relatively newer techniques part of OWASP API Top-10. Unlike the conventional methods that are generic, the attack techniques relevant to APIs are custom & targeted to the application. Detecting and preventing such practices requires a deeper understanding of the application that current generation technologies like SAST, DAST, IAST or WAF, RASP, API-GW's, IDS/IPS, or NGFW lack. Moreover, these products don't have the required architecture to build deeper context & understanding of the applications. Hence these solutions as well as solutions morphing as WAAP are ineffective in protecting against API attacks.

Organizations need to address the critical attack surface that's continuing to expand and bring complex attacks into the organization environment by including API security in their overall application security strategy. While several API security solutions have emerged over the last few years, navigating the multitude of vendors can be difficult. This Buyer's Guide describes the key capabilities necessary for a comprehensive API Security Platform, defining the features and security controls needed to build Secure APIs and protect APIs' in production.

## Key Capabilities for Comprehensive full life-cycle API Security

API Security platform should cover APIs' entire life–cycle from code to cloud. The following are the four essential capabilities:

### Continuous Discovery & Cataloguing of APIs

You can't protect what you can't see. Protecting APIs can be a significant hurdle if an organization lacks visibility. AppSentinels continuously discovers APIs and catalogues them. It tracks API parameters and structure. It maintains updated documentation of the APIs as they change and evolve. It discovers even Third-party APIs from open-sources or other libraries and provides organization visibility and posture of these APIs.

AppSentinels keeps a watch on depreciated, orphaned, zombie, shadow and sensitive APIs in the organization environment.

Every organization today has variety of application architectures and multiple API Ingress points – all of which should be covered. AppSentinels provides the required coverage by providing sensors/connectors of various dev-ops friendly forms & for application-architectures that can be deployed in no-time ensuring organizations have comprehensive view of their API estate.

**AppSentinels API Catalogue allows security engineers to understand the span of the attack surface that needs to be addressed. It also informs them where the sensitive information may be exposed due to vulnerable APIs. Based on these insights engineers can implement controls to reduce the Risk exposed due to insecure APIs.**

## Continuous API Security Testing

Today's business requires software teams to deliver innovation faster than ever. Most organizations struggle to do happy-path testing before a release and as a result security testing is getting short-circuited. Adhoc pen-testing is not a solution as it can't scale.

After getting visibility into the APIs, doing continuous security testing of APIs is essential. This helps in identifying vulnerabilities proactively in the implementation and develop plans to update vulnerable APIs with fixes or upgrades.

Important to note here that the security testing MUST cover OWASP API Top-10 techniques that are Application specific. Most of the current generation SAST, DAST or IAST products are ineffective for API testing as they were tuned for generic OWASP Top-10 techniques. AppSentinels platform provides Intelligent Stateful API Testing that provides coverage for Business-logic, OWASP API Top-10, OWASP Top-10 and beyond. AppSentinels can test complete API workflows in a stateful fashion. This testing process can be integrated into the CI/CD pipeline of the organizations so that any gaps are immediately discovered and addressed on priority.

**AppSentinels has world's first and only Intelligent Stateful API-DAST that test API's by executing complete user-journeys to get deeper coverage. It can test APIs for business logic, OWASP API Top-10, OWASP Top-10 issues and more. Integrated with CI/CD, it effectively works like a 24x7 pen-tester, greatly boosting security testing capability of the organization and helps adapt proactive security posture.**

## Multi-Layer API Protection

Attackers use several techniques to attack APIs. A few examples are techniques part of OWASP API Top-10, OWASP Top-10 and automated attacks. Attackers are continuously evolving, and new techniques keep emerging. What organizations should look for is a multi-layer Defense-in-Depth approach to API Security. Organizations should avoid using traditional signature-based network security tools such as IPS, WAF/WAAP, NGFW as these solutions don't build necessary context to understand the Application. These solutions at-best are effective for generic attacks and not able to effectively protect API attacks that are custom to the Applications.

AppSentinels has Multi-Layer Protection that uses AI/ML and behavior baselines to protection application against all kinds of Known, Unknown and Automated API attacks.

**Business continuity is critical for organizations; hence, AppSentinels sensors come with built-in service-chaining (inline) OR Tap mode deployment options. The sensors also have enterprise-grade features - like fail-open, fail-close, or the ability to trigger fail-open if latency crosses a certain threshold – providing a perfect balance of security with business continuity.**

## Remediation

Compared to generic remediation techniques that mostly involve patching infrastructure, API remediations are unique, as fixes for these vulnerabilities come from product teams. At the same time, SecOps teams need mechanisms/controls to protect production environments. An organization needs a platform that aligns both teams to work collectively towards incrementally addressing the Application Security gaps. This is the sweet-spot AppSentinels offers as it aligns the product & sec-ops team to work together.

Lower False-positive is non-negotiable for such platforms. AppSentinels, with its deeper context and understanding of the application, filters out false signals and provides accurate and actionable insights to the customers.

**Integrations into the organization's existing workflow is also a table-stake and AppSentinels provides a wide variety of integration options with SIEMs/SOARs, integration with identity systems, ticketing tools and messaging systems, to ensure developers & sec-ops focus more on their KPIs rather than to learn a new tool.**

# Conclusion

This buyer's guide is intended to help customers understand the capabilities and features required in an API Security solution.

AppSentinels is redefining Application Security as it used to be. Its complete life-cycle API Security platform provides the industry's most comprehensive and proactive approach to API Security. It helps Developers write Secure APIs and helps the SecOps team protect Applications against run-time attacks. AppSentinels platform builds a deep white box understanding of the Application behaviour, including various user journeys and happy paths workflows. It uses this unique insight to:

1. Discovers all APIs in real-time including shadow, orphan, privilege, zombie, unused, private/public, and third-party APIs. It discovers PII/Sensitive data in the APIs as well as provide real-time risk score of the APIs.
2. Automatically do security testing of the application with a complete understanding of the workflows. It's like a 24x7 pen-tester integrated with the organization's CI/CD cycle to help adopt a proactive security posture. It's the world's first and only Intelligent Stateful API DAST.
3. Blocks known & unknown attacks as well as automated API threats/misuses to protect Applications from breaches, frauds and data loss.
4. Provides pin-pointed remediation to developers to fix API vulnerabilities and insights to security teams to protect applications against run-time attacks.

The platform supports multiple deployment methods and onboards any application in under 60-mins with no impact on API latency or availability. It supports SaaS OR ON-Prem deployment with an option to ensure no API data leaves the organization's boundary. AppSentinels sensors can be deployed in OOB OR service-chaining modes to achieve a critical balance between security efficacy and business continuity. Some of the largest API consumers in the world are engaged with AppSentinels and trust it to secure their APIs.

Contact us to discover more about your APIs:

**contact@appsentinels.ai** | **www.appsentinels.ai**