AppSentinels.ai
Application Security Re-invented

The Changing API Landscape

A foundational element of innovation in today's app-driven world is the API. From banks, retail and transportation to IoT, autonomous vehicles and smart cities, APIs are a critical part of modern mobile, SaaS and web applications and can be found powering customer, partners and vendor integrations. By nature, APIs expose application logic and sensitive data such as Personally Identifiable Information (PII) and because of this have increasingly become a target for attackers.

As per Gartner, by 2022, API's will be largest attack vector bypassing all other methods

Today's Security Solutions are not effective

Organizations have deployed multiple layers of application security solutions, including Static & Dynamic Application Security Testing (SAST/DAST) products, WAF, RASP, and/or API gateways, but remain unable to detect or prevent API attacks. This is because traditional tools focus on known attacks, have limited view of network session or don't have visibility into production environments. API attacks are application specific and exploit flaws in business logic that require very deep understanding of application's and dataflows patterns that are blind-spots of traditional products.

As per Forrester & Verizon DBIR, 35% to 43% of breaches start with web applications and APIs

It's interesting to note that even the largest technology companies including top cloud-vendors are struggling with API attacks and have themselves faced multiple API breaches. It's not hard to imagine state of most other organizations who don't have similar resources or technical man-power. Few examples of the API attacks:

aws

In Nov'21, Researchers at Palo Alto Networks found that 22 APIs across 16 different AWS services could be exploited to leak Identity and Access Management (IAM) users, roles and tokens.

coinbase

In Feb'22, Coinbase had to suspend trading as a researcher reported API business logic flaw that allowed someone to sell crypto's even without owning them.

BANK

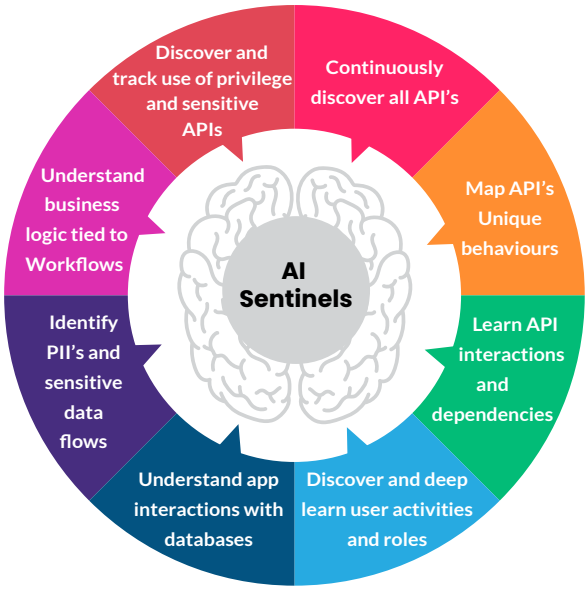
In Nov'21, Alissa Knight reported she was able to access API's of 55 Banks and was able to change PIN numbers of debit cards and moved money between various accounts without user's authorizations.

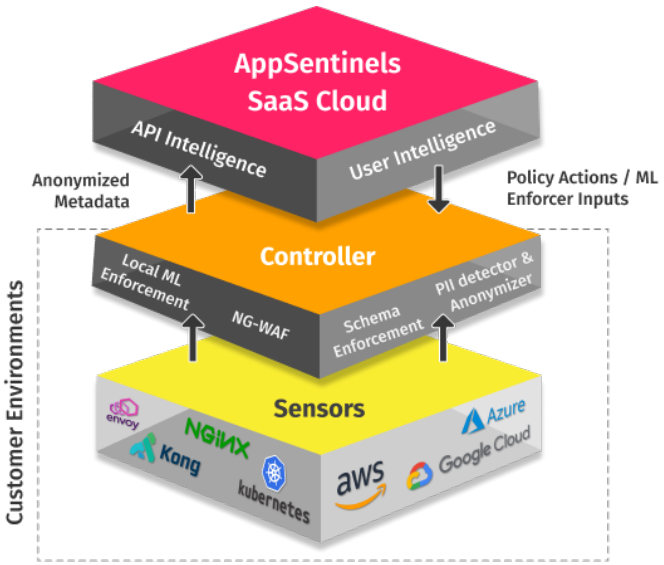
IRCTC

17-year-old boy found BOLA and enumeration attacks – could modify tickets booked by others and change crucial parameters of booked tickets. Got access to 50 million users of the site including their personal information.

Introducing AppSentinels API Security Platform

AppSentinels API Security Platform is purpose built keeping security needs of next generation applications in mind. At its core is it's AI/ML engine, AI Sentinels, that combines multiple intelligence inputs to completely understand and baseline unique application business logic, user contexts and intents as well as dataflow within the application, to provide complete protection your application needs.





With it's unique three tier architecture, AppSentinels guarantees high availability, low latency and high scale. AppSentinels support multiple dev-ops friends deployment modes to onboard an application in under 60 minutes. It can also be deployed on-prem keeping all your data safe within your organization.

AppSentinels Advantages

Discover

AppSentinels 360° Continuous Discovery

Real Time discovery of API's, PII/Sensitive data and various attributes of APIs to eliminate all your blind-spots and provide real-time risk posture.

Test

AppSentinels Intelligent Stateful API Test Platform

Shift-lefts AI/ML learnings from production environment to uncover business logic vulnerabilities in your application like your 24×7 pen-tester.

Defend

AppSentinels AI Powered Multi-Layered Defence Shield

Industry's most comprehensive multi-layered protection to protect your APIs and applications against all unknown and known attacks.

Remediate

AppSentinels Rapid Detection & Response

Helps SoC team with all the data needed to stop attacks with confidence;
Provides deep insights to Developers to remediate security issues

Summary

Business leaders are demanding technology teams deliver faster. As a result, teams have adopted new ways of working and new ways of architecting their solutions. Enter Agile, CI/CD, Cloud-native, Micro-services, DevOps tools, GRPC and GraphQL APIs. It is unacceptable for security to slow progress of innovation. Even with huge blind spots as traditional application security solutions don't provide necessary insights. Security and Dev-ops teams need a solution that can keep pace with rapid innovation. Your Security and Dev-ops teams need AppSentinels.

Contact us to discover more about your APIs: contact@appsentinels.ai **www.appsentinels.ai**