AppSentinels.ai
Application Security Re-invented

Solution Brief

API Security for Retail Industry

API Security for Retail Industry

The retail industry is undergoing a massive digital transformation shift as almost 25% of worldwide retail business is expected to be online by 2025. APIs enable retail industry to build end-to-end personalized experiences for their customers while streamlining business operations. APIs has truly revolutionized the shopping experience by connecting the ecosystem of retailers, their partners, and their customers to provide the best customized offers on the fly for the customers. Everything from inventory data, to order submissions, to location data, to payments, to rewards programs that drive customer engagement are delivered via APIs. This digital transformation creates new security risks and retailer's security strategy must consider all these threats that cyber criminals can use to steal data and damage your business.

Risk to the Business

- Retail is amongst the top target industries for malicious activity with an attractive combination of dealing with customer data and payments. They also have a relatively open environment to attract more visitors.
- Around 30 percent of traffic to e-commerce sites are competitors, hackers, and fraudsters including bots that may perform a wide array of malicious activities.
- Service disruptions or latencies that impact customer's secure shopping experience.
- Account takeover is a significant risk given the wealth of data including PII and payment information.

Challenges

API attack techniques are very specific to the Application behavior, unlike the traditional techniques that are generic.

Detecting and preventing newer techniques like OWASP API Top-10 requires deeper understanding of the Application that current generation technologies like SAST, DAST, IAST or WAF, RASP, API-GW's, IDS/IPS or NGFW's lack.

Existing products don't have the right architecture to build deeper context & understanding of the application to protect against business logic API attacks.

Attacks & Threats Faced


Data Exfiltration


Account Take Over


Payment Frauds


Scraping

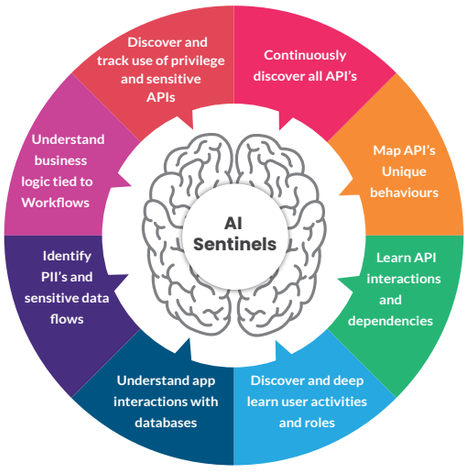

Inventory frauds & scalping

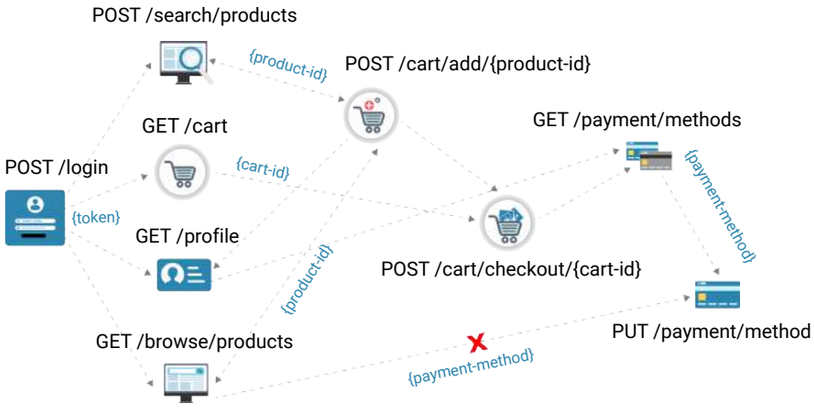

Gift card abuse


Service Disruptions

Secure APIs are possible – AppSentinels Full Life-Cycle API Security Platform

AppSentinels build deep understanding of the application behavior even as it is continuously changing





With the deep understanding, AppSentinels secures APIs across it's entire life-cycle

Shift Left Security

360° Continuous Discovery & Posture Management

- Achieve continuous & comprehensive API visibility in real-time along with always upto date API Catalogue.
- Discover API attributes like shadow, zombie, orphaned, unauth, sensitive, public, internal APIs.
- Discover Sensitive data types & flows.
- Find misconfigurations, vulnerabilities, governance issues to provide real time APIs Risk Posture.
- Find drift compared to documented OpenAPI Schema.

Continuous Stateful API Testing

- Test every API with complete stateful workflows before every deployment.
- Covers Business-logic, OWASP API Top-10 application specific techniques, OWASP Top-10 generic techniques and beyond.
- Identify vulnerabilities proactively as part of CI/CD cycle and address issues before they go to Production.
- Helps prioritize issues that hackers can exploit.

Runtime Security

Remediation for Developers & Sec-Ops

- Provides pin-pointed insights to Developers for fixing API vulnerabilities.
- Unified attack view consolidating all activities of an adversary mapped to attack kill-chain.
- Provides automated OR manual action capability based on threat-actor risk.
- Negligible false positives due to deeper Application context.
- Smartly aggregates Alerts to reduce fatigue and help SoC focus on real issues.

Multi-Layer Protection

- Protection against Unknown Business Logic zero-days attacks.
- Provides controls against APIs not conforming to OpenAPI schemas.
- Protection from known attacks OWASP Web Top-10 and beyond.
- Protection against automated threats like ATOs, stolen credentials, Bots & Frauds.

Summary

Secure APIs are the foundation for safe shopping experience. A successful attack can result in damage to the brand, loss of trust, significant fines due to non-compliance with regulations. As retail organizations continue to adopt digital-first strategy, APIs are increasingly becoming centerpiece to the success of that strategy. Retail organizations need to secure their systems as well as protect valuable customer data. They need to adapt a purpose-built API Security platform that balances features, functions, business demand and aligns various stake holders in the organization. Today, some of the largest retail organizations are engaged and trust AppSentinels for securing their APIs. Talk to us and discover the unknown about your APIs.

Contact us to discover more about your APIs:

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