AppSentinels.ai
Application Security Re-invented

Solution Brief

API Security for Healthcare Industry

API Security for Healthcare Industry

While APIs were already ubiquitous, the pandemic has further accelerated growth in innovation and expansion of digital services. Healthcare is not an exception to this trend. Modern healthcare with the rise of telehealth, Internet-of-Medical-Things, and the hundreds of healthcare devices and apps, relies on many digital services and technologies that create and store patient data – PHI's & EHRs. To provide quality healthcare, this information needs to be shared quickly and easily among providers such as primary and tertiary health-centers, diagnostic firms & labs, insurance providers etc. United States' 21st Century Cures Act mandates sharing electronic health records among various providers. Standards like FHIR (Fast Healthcare Interoperability Resources) and USCDI (US Core Data for Interoperability) make APIs imperative for the healthcare industry's future. Regulations like HITECH & HIPAA require healthcare organizations to maintain a complex balance between being open to sharing PHI and mitigating the risk of a data breach. For attackers, APIs are pathway to a treasure trove of medical and financial data. For healthcare organizations, this data needs to be secured.

Risk to the Business

- The Healthcare industry — with its attractive combination of dealing with money and customer data — is amongst the top target industries for malicious activity.
- Personal health information (PHI) is the most valuable category of personal data, esp, when compromised and sold on the dark web. This data fetches many times more than any other type of data.
- High risk as any disruptions caused by an incident can jeopardize human lives by interrupting life-saving digital services.
- Ransomware is a big threat as healthcare vendors prefer paying ransom rather than investigating or mitigating because their priority is to make systems operational to ensure continuity of care.
- Bad Bots can cause multitude of attacks like gathering PHI OR disrupting digital healthcare services.
- Account takeover is a significant risk given the wealth of data stored in patient portals.

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


Shadow APIs

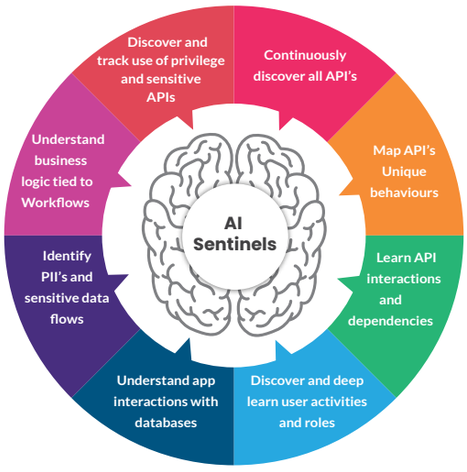

Ransomware

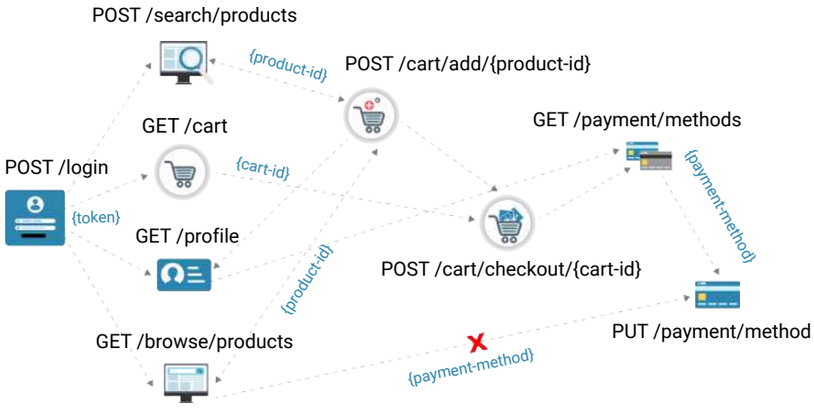

Service Disruptions


Partner Breaches

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 digital healthcare. A successful attack can result in damage to the brand, loss of trust, significant fines due to non-compliance with regulations. As Healthcare organizations continue to adopt digital-first strategy, APIs are increasingly becoming centerpiece to the success of that strategy. Healthcare 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 Healthcare 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**