API Security Case Study

A large medical insurance company needed help to determine which API security product to invest in based on their specific needs. Their security team was spread thin with other projects and they lacked expertise in the newer to market API space. They engaged with K logix's Security Technology Consultants to help identify their requirements and determine which technologies to evaluate.

With the help of K logix, the customer identified these requirements when evaluating API technologies:

- **Continuous Threat Detection and Protection:** Utilize behavior analysis to detect complex attack patterns and identify, prioritize, and assist with the remediation of vulnerabilities in APIs
- **Shift Left Development Assistance:** Assist developers with ensuring safe coding practices are used and test APIs in pre-production to ensure secure functionality.
- **Visibility and Consistent Documentation:** Visibility into all APIs including shadow, zombie, and third-party APIs and track information being carried by APIs

Challenge
- Small team spread thin
- Lacked API security expertise
- Short timeline

Result
After evaluating four API security technologies against the customer's core requirements, the customer determined one best fit technology that would comprehensively meet their needs.

K LOGIX'S VENDOR-AGNOSTIC API SECURITY EVALUATION

K logix's Technology Advisory service leverages our proven methodology using a vendor-agnostic, technology and business use case driven approach. The result is an analysis-backed, justified API security product decision that aligns with the organization's requirements.
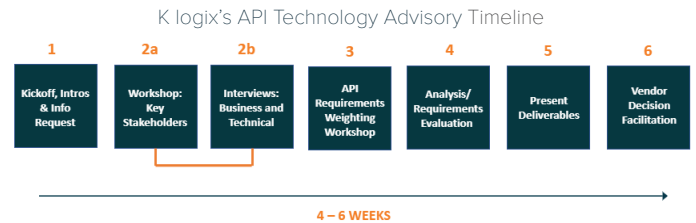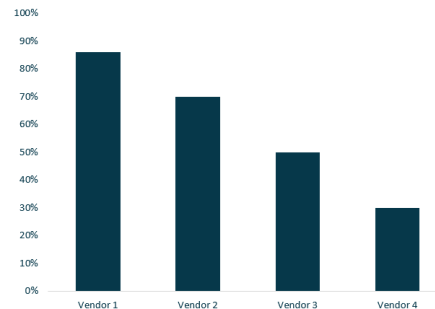
TECHNOLOGY ADVISORY DELIVERABLES:
- **Heatmap:** Identification of where products had critically different scores and which products meet (and miss) identified key requirements
- **Technology Scoring:** Using visual charts, compare product scoring using weighted domains and requirements
- **Vendor Demos:** Script and scorecard based on specific customer requirements combined with facilitated vendor demos that speak directly to the key customer requirements

All visuals and content are wrapped up into an engagement overview and executive-friendly PowerPoint presentation.

K logix's API Technology Advisory Timeline

1	2a	2b	3	4	5	6
Kickoff, Intros & Info Request	Workshop: Key Stakeholders	Interviews: Business and Technical	API Requirements Weighting Workshop	Analysis/ Requirements Evaluation	Present Deliverables	Vendor Decision Facilitation

4 – 6 WEEKS

Sample Deliverable: Technology Scoring Against Weighted Requirements

Evaluation Domains	Weight
Architecture	8.33%
Dashboards and Reporting	8.33%
API Discovery	8.33%
API Inventory	8.33%
Access Control	8.33%
Content Validation	8.33%
API Threat Detection	8.33%
API Threat Prevention	8.33%
API Behavior Analytics	8.33%
Vulnerability Management	8.33%
API Security Testing	8.33%
Technology Integrations	8.33%

API Security

API MARKETSPACE OVERVIEW

APIs have become pivotal drivers of digital transformation and innovation yet securing them poses many challenges for security professionals. APIs are increasingly part of strategic advancements around digital transformation and lead to rapid modernization within organizations. They are used as communication methods between critical applications, so they may expose highly sensitive data such as Personal Identifiable Information (PII), making them a prime target for attackers. The growing attack surface from APIs is complex and often overlooked. APIs are used for internal use, Business to Business (B2B), and Business to Customer (B2C), making tracking and securing them a difficult task. Many organizations are also looking to shift their security left, baking security directly into the software development lifecycle rather than playing security catch-up once APIs have already been developed.

With vendors providing varying capabilities and architectures in the API security space, K logix identified the need to bring our proven methodology to this new market. Finding the best fit technology in the API security space is complex, with many considerations to be made. For example, some organizations value security and protection of PII as most important, while others see the risk of API downtime as a greater threat. Engaging with K logix's Internal Research Department helps an organization better understand their own needs, ultimately informing the domain and requirement weighting that illuminates capabilities and drives ideal outcomes.