aiculus

Don't let the power of APIs be a double-edged sword

Application Programming Interfaces (APIs) are key to business digitisation, optimisation and innovation. APIs allow businesses, including yours, to tap on functionalities of different applications to obtain and share data without building new applications or data stores. Most APIs today uses common web-based technologies, making APIs extremely easy to deploy. However, easy deployment means that APIs are fast becoming the top attack vectors today due to their proliferation of use. With every new API endpoint you have, you expand your organization's attack surface area.

Attackers are after APIs

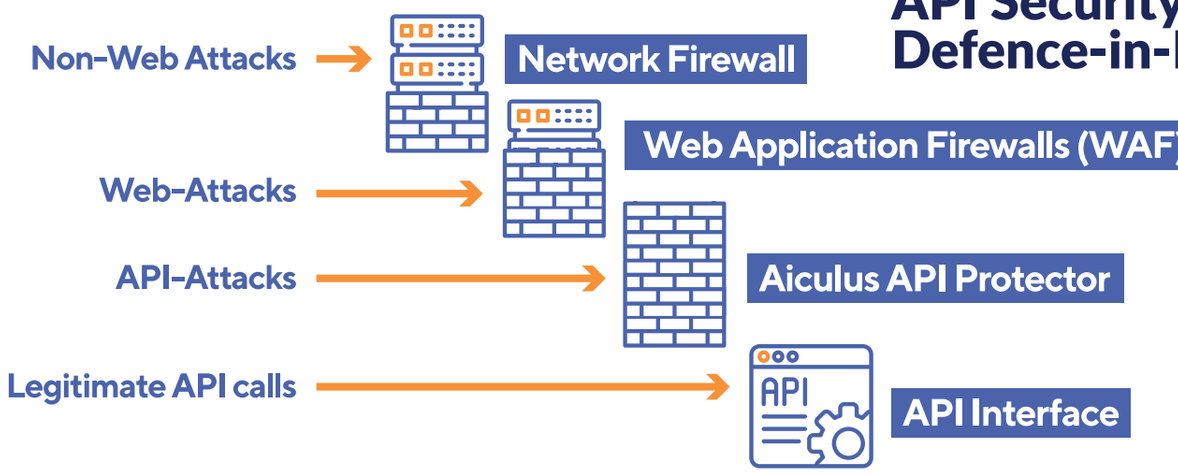
APIs are prime targets for attackers as they carry Personally Identifiable Information (PII) and business critical data. Attackers exploit API vulnerabilities such as weak code, stolen credentials to bypass authentication and authorisation mechanisms.

Your current protection is not enough

Businesses are pivoting from web-based applications to APIs and microservices architecture faster than existing security controls can keep up. Yet security of APIs have been an afterthought for security teams and solution providers.

Rule-based solutions such as WAFs defend against known attacks, and are often generic, lacking appreciation of API and business logic.

API Security Defence-in-Depth



Reap the benefits of Artificial Intelligence

Attackers are increasingly capable of bypassing traditional cybersecurity measures. Defend against sophisticsted attackers by harnessing the power of Artificial Intelligence.

Machine Learning and Deep Learning techniques are powerful data analysis methods that have transitions from theoretical research space to real-world applications, including cybersecurity.

Our AI Engine extrapolate threat activities and patterns with an appreciation of your business logic and unique API behaviour. It intelligently self-learns new attack patterns, which are often variations of previous or known attacks.

1. Keep your API Asset Inventory updated

You won't know what to protect if you don't know what you have. Aiculus conducts reconnaissance of all APIs in your network, uncovering legacy and shadow APIs that may have been hidden unprotected from attackers. Aiculus continues to map your API assets and monitor API traffic as your business innovates with new addition of APIs. Build a robust API risk management strategy with full visibility of your APIs

2. Defence-in-depth strategy against OWASP API | Top 10 attacks

Defend against prevalent API attacks as we continuously screens all your API traffic in real-time to identify malicious behaviour.

3. Mitigate third-party risk

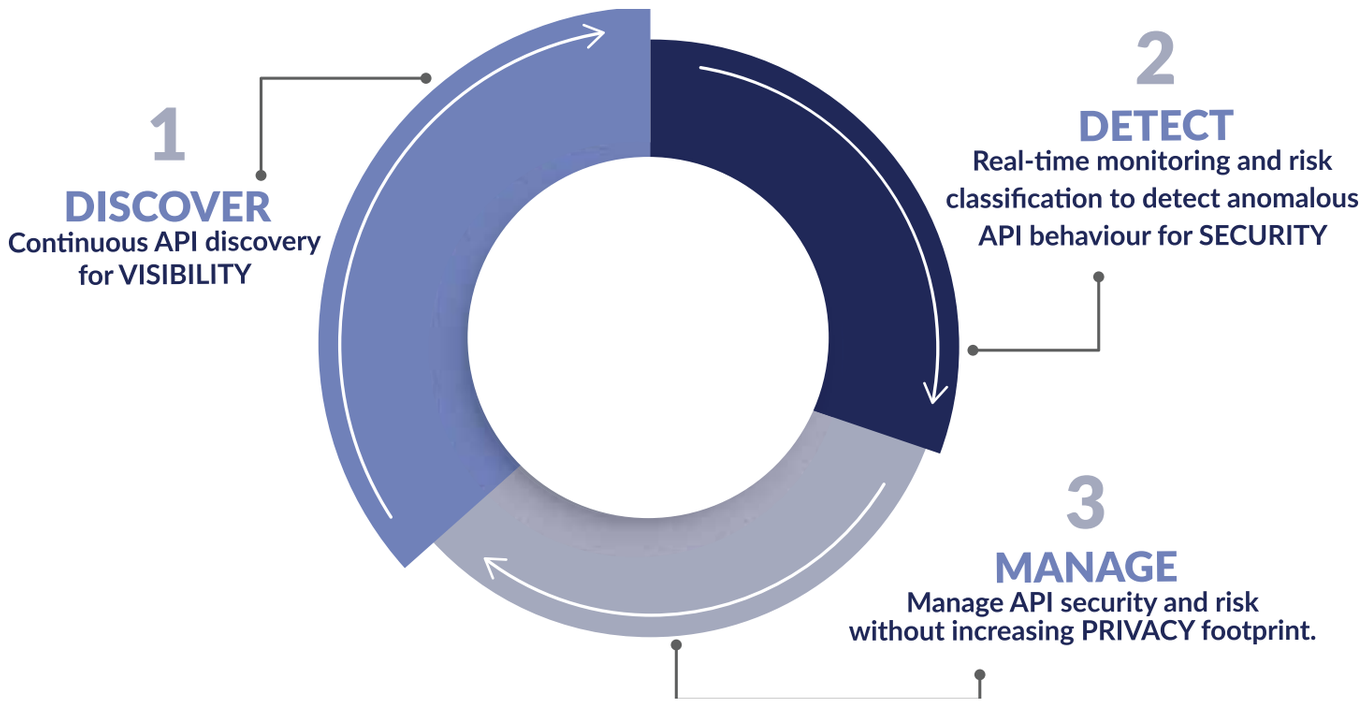
Fundamental to the innovative prowess of APIs is the ability to share data with different applications, such as your B2B partners. Working with third parties partners or suppliers ultimately increase your attack surface to include that of third parties who do not share the same risk level as yours. Don't let the security weakeness of others undermine your own security efforts. Aiculus also maintains your privacy footprint as we do not consume any PII or sensitive information for API traffic analysis

4. Improve Incident Response

Aiculus continuously screens all your API traffic in real-time and automatically identifies malicious behaviour at early stages using our AI engine. It screens at point of entry and point of execution and instantly alerts your response team of suspicious API calls. We reduce monitoring fatigue and improve your team's response time by detecting attackers who use API attacks as part of their kill-chain.

5. Classify and Manage API Risk

Aiculus also performs a risk assessment to reveal the risk level of every API call. Risks can be categorised using an established standard risk matrix or customised to your internal risk classification system. Instantly classify API risk for further risk analysis and management while defending against active threats.



Deploy Aiculus API Protector for Defence-in-Depth Cybersecurity

	North-South	East-West
Monitored terminals	External end user and API endpoint/server	• API endpoint X and API endpoint Y • Applications/services within a datacentre • Containers/devices within a network
Threats and use-cases	• API authentication bypass • API Token abuse • API payload injection	• Compromised endpoint threat • Internal access control abuse • Insider threat
Organisational benefits	• External API traffic security, privacy and visibility	• Internal API threat monitoring • API endpoint segmentation

contact@aiculus.co