SNG
Grant Thornton

API Security

API security requires much more than the traditional rules-based approach to security

Today's business applications have become API-centric as businesses have accelerated on their digital journeys. This transformation has had to take place in order to keep pace with the demands of their markets, whether that's business to business or business to customer. The cliché of "there's an app for that" should be viewed rather as "there's an API for that."

Legacy applications were comprised of a single code base and required massively disruptive processes for releases of new features and enhancements, and what we see today is these monoliths are quickly being transformed to modern micro-services based architectures broken out into smaller focused services that together provide an application's full functionality. These micro-services each have their own code base and are architected to each reside behind their own set of APIs. The result of this shift is that today's applications are comprised of many APIs.

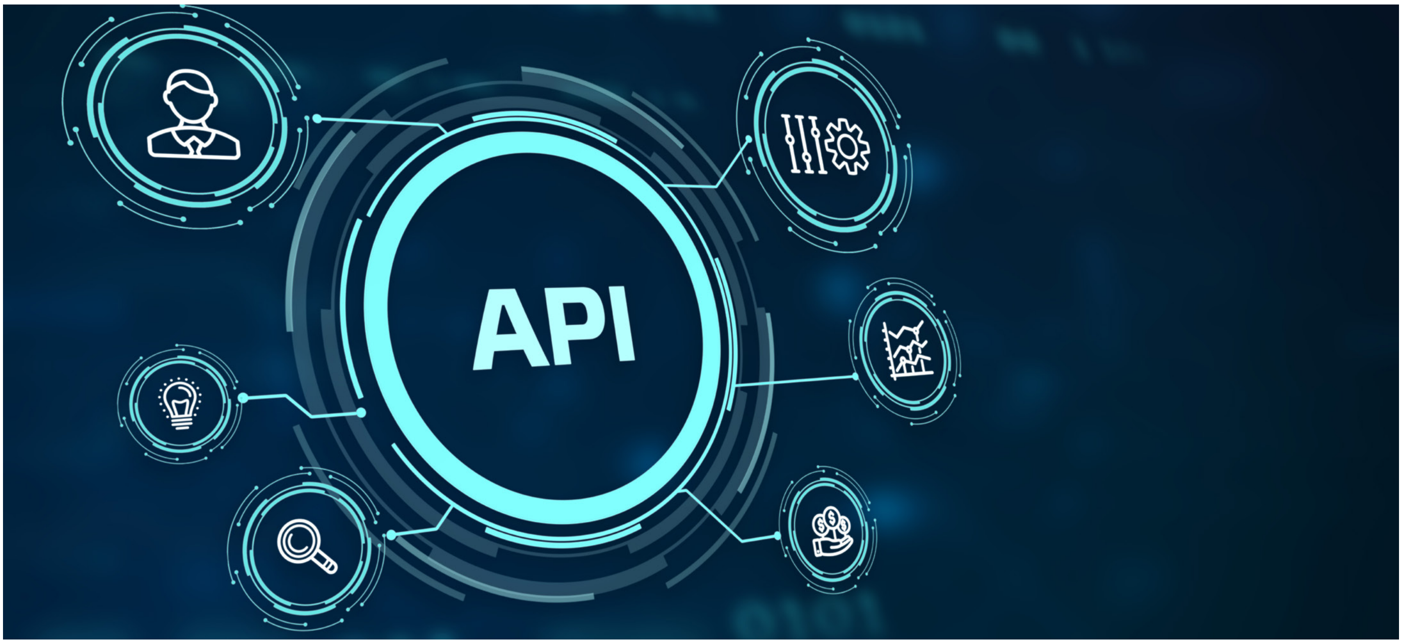
Today's threat actors are entirely aware of the prevalence of APIs for business operations and the opportunity to exploit the blind spots which may exist in them to gain access to organisations' sensitive data. APIs are quickly becoming the most frequent attack vector for organisations.

A common approach to protect APIs is to utilise some but often all of the following technologies to combat these threats: Web Application Firewalls (WAFs), API Gateways, Load-balancers and Edge technologies such as CDNs. All of these technologies take a layered and rule-based approach to securing APIs meaning that firstly you need to know of every API and every API endpoint you wish to protect (the what), and secondly you need to define what types of attacks to protect against (the how). This requires discipline and mature governance to maintain and there is plenty of associated administration when it comes to keeping these rules in check.

If you're going to have peace of mind when it comes to securing your APIs you firstly need real-time discovery and visibility of them and their associated endpoints, and secondly the same for their usage and behaviours including what type of information they are exposing. Rules-based technologies cannot dynamically achieve this as they rely on humans to define what to and how to protect.

Today's threat actors know this and have rather progressed from known methods, typically your "one and done" known types of attacks which a rules-based approach may protect against, to "low and slow" systematic attacks which attempt to manipulate the business logic of APIs to compromise sensitive information. The rules-based approach isn't able to protect against this new type of attack vector because in order to achieve this, additional context is required.

So to truly understand and protect APIs requires a unique approach to the problem and this is a shift that's taking place within the cybersecurity industry, even beyond APIs. Rather than only considering what traffic's being allowed by a rules-based approach, let's look at all of the data from all of the components involved in serving the responses sent and requests received for APIs. This would comprise of large amounts of unstructured data, that is, Big Data. We store this in a Big Data engine and then Machine Learning (ML) and Artificial Intelligence (AI) is programmed and utilised to be able to correlate today's most frequent attack types as well as learn the expected behaviour of your APIs. This is the context that's required.



To illustrate this requirement we only have to consider one example, and that is today's number one API attack type as published in the OWASP API Top 10 is the BOLA Broken Object Level Authorisation (BOLA) attack type. It's represented in approximately 40% of all API attacks. Rules-based approaches are simply unable to identify and protect against this attack type because an understanding of the API's business logic is required in order to do so.

The behavioural and contextual analysis that is achieved with this new approach identifies when an API is behaving outside of the norm which could be as simple as where it's being accessed from and/or by who it's being accessed. More importantly, you begin to understand when an API is behaving outside of its intended design parameters.

In conclusion, to discover, protect and improve the posture of your organisation's APIs from today's threats you need more than the traditional rule-based solutions. You can only derive the required context to protect them adequately by utilising solutions enabled by always-improving real-time analysis of Big Data with AI and ML.

SNG
Grant Thornton

sng-grantthornton.co.za

"Grant Thornton" refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires. SNG Grant Thornton is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.