API Security Assessment

Prioritize your API security to protect assets, maintain reputation, and achieve long-term success.

APIs (Application Programming Interfaces) are interfaces that allow different software applications to communicate with each other and have become an essential part of modern software development. They enable developers to integrate different applications, services, and systems and create new functionalities. While API providers are responsible for ensuring the security of the API itself, API consumers must also take responsibility for securing their use of the API. This includes implementing proper authentication and authorization controls, encrypting data in transit and at rest, and monitoring API activity for suspicious behavior.

Business Challenge

A secure API provides several benefits to an organization, including protecting sensitive data from unauthorized access, maintaining the trust of customers and partners, ensuring compliance with industry regulations, preventing disruptions to business operations, and enabling scalability and growth. One misconception is that API security is only necessary for external-facing APIs, whereas internal-facing APIs can also pose security risks if they are not properly secured. Organizations must implement proper authentication and access controls for all APIs, regardless of whether they are external or internal. They must also ensure that all API's are updated regularly to address security vulnerabilities and bugs. By prioritizing API security, organizations can protect their assets, maintain their reputation, and achieve long-term success in an increasingly connected and digital world.

A Proven Solution

Organizations and their security teams greatly benefit from this offering by enabling them to protect their data and systems from security threats, comply with industry regulations, and prevent disruptions to business operations. In turn, several ancillary parties also benefit, including the organization's customers and partners knowing their data is secure and maintaining that trust. Developers also have a clear understanding of the coding and deployment practices required to ensure secure API design and implementation.

The EVOTEK team holds vast and varied experience and with the support of industry-leading partners, proactively works with all the nuances needed to prepare for API Security threats.

Preventing Future Data Breaches

Recently, a major player in the finance vertical suffered a critical data breach that exposed the personal information of over 100 million customers. The breach occurred due to a vulnerability in an API that was used to access customer data. As a result, they implemented controls that are seen in the foundation of the EVOTEK API Security offering. This includes increased monitoring, stronger access controls, API testing/ validation, and improved authentication/ authorization.