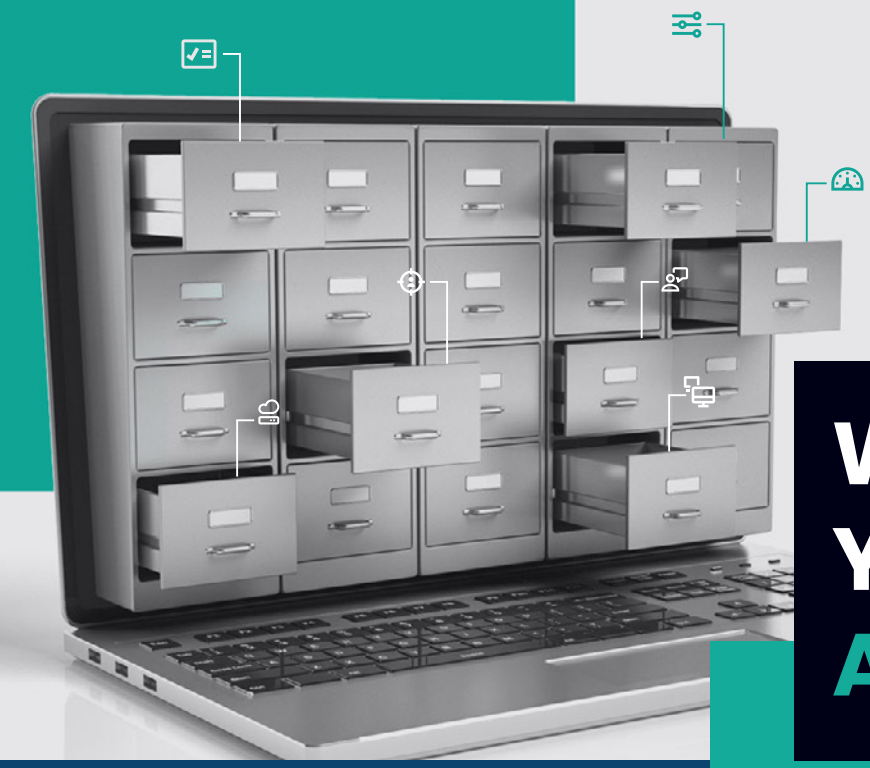
PROXEDO
API SECURITY



WHY DO YOU NEED API SECURITY

Many API applications are vulnerable. And breaches leveraging these vulnerabilities are genuine threats today. API attacks are increasingly complex, targeted and bypass the existing defense lines. This means that organizations operating public API-infrastructures should re-evaluate their risk and compliance posture from an API perspective. Not just end-user companies, but also IT developers should consider deploying/integrating a greater level of API security in their projects. By reducing security gaps in custom-developed applications, they can also increase their credibility and reputation.

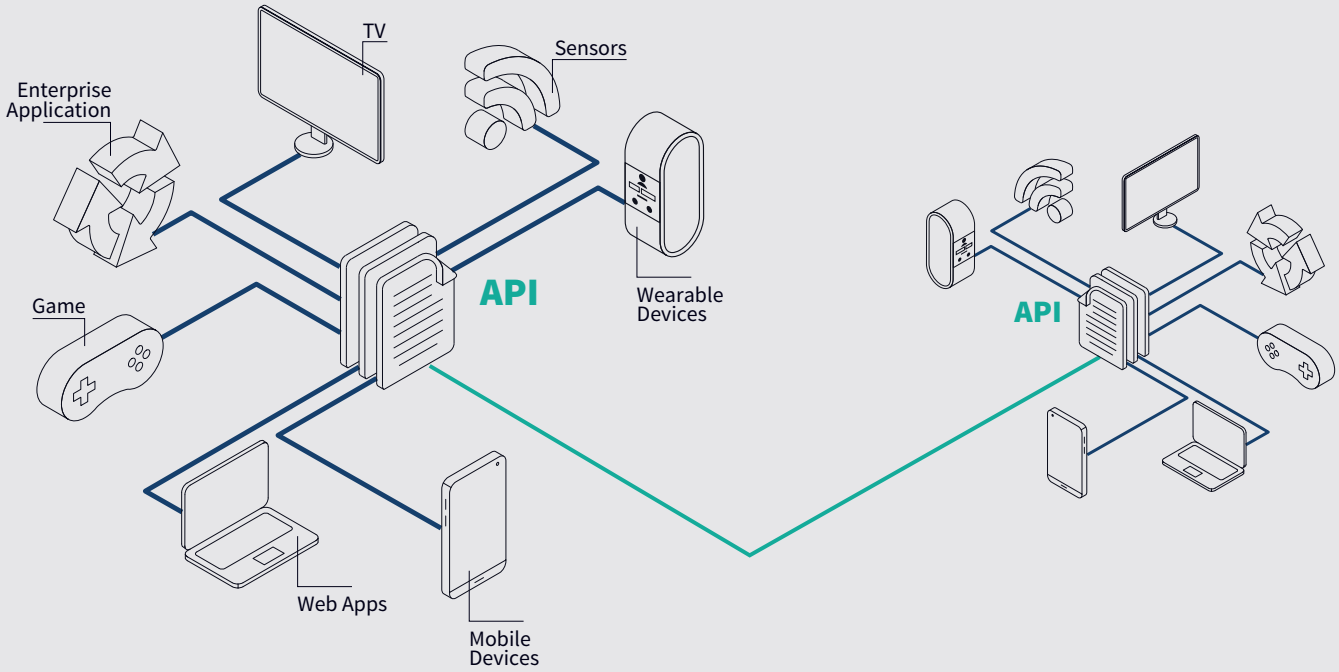
LEARN MORE

In the era of digital transformation, there is a strong focus on interconnectivity and data exchange between customers, businesses and partners. This has resulted in a boom in public-facing APIs (Application Programming Interface), an HTTP-based application integration protocol which exposes application data to connected parties, devices and services. Today, to enable seamless machine-to-machine communication, APIs connect tens of thousands of web and cloud applications, microservices, mobile and IoT devices. And their number is skyrocketing.

APIs don't expose just Facebook messages anymore, but an enormous amount of sensitive information: user IDs, financial data and corporate secrets are also transferred via these interfaces. APIs have become direct shortcuts to the heart of your organization. As a result, the proliferation of API infrastructures has brought with it huge security challenges. This post summarizes the major concerns around API-communication security and introduces a potential solution.

BALASYS

info@balasys.eu



Hackers shift their interest to APIs

The amount of sensitive data exposed via APIs is increasing significantly, making APIs a primary target for attackers. They've started to look for vulnerable, broken APIs to find ways to the back-end systems that store sensitive data. And they are becoming increasingly successful. Many recent huge data breaches have leveraged APIs – just think of the Salesforce.com, the US Post, T-Mobile and Strava incidents.

Traditional security solutions are insufficient

Today's API attacks are increasingly complex, targeted and easily bypass traditional security solutions. These attacks CANNOT be detected by signature-based web application firewalls (WAFs), authentication or other baseline security tools. Advanced API attacks can only be prevented by targeted solutions. Without this knowledge in mind, businesses may expose their core systems data with a false sense of security.

API developers work without focusing on security

Security is not a priority for many application development projects: they focus on the functional specification, user experience and deadlines. Often, security requirements are not specified in detail in these projects. Security teams have either no or limited influence on security during these projects. As a result, the developers' toolset and workflow processes are not security-optimized. They don't think like attackers. They deal with security just on a best-effort basis. This practice leads to unique vulnerabilities in public-facing APIs, which in turn creates risk for the business and opportunities for the bad guys.

Regulations require secure API communication

PSD2 requires banks to open their APIs directly to retailers and third-party payment providers (TPP or fintech). GDPR indirectly requires anonymization or pseudo anonymization of personal data in transit. The PCI DSS requires financial providers to encrypt transmission of cardholder data via public networks… All these regulations have one key requirement in common: they require companies to protect customers' data at rest and also in transit. To meet these criteria, regulated industries like finance or public services must start thinking about how to secure the sensitive data flow via their public-facing APIs.

The Proxedo API Security is a highly flexible API security solution which helps enterprises gain control over their API traffic. With Proxedo API Security, you can enforce, transform, encrypt and analyze the API traffic to prevent API breaches. Thanks to the flexible architecture, your organization can implement custom API security policies without compromise.

Proxedo API Security Homepage

Request a trial

BALASYS