WHY PROXEDO API SECURITY?

1. **Deep traffic inspection**
2. **Flexible security enforcement**
3. **Positive security model**
4. **Highly flexible and skilled delivery team**
5. **Pioneers in proxy technology**
6. **Made in EU – 'clean' codebase**

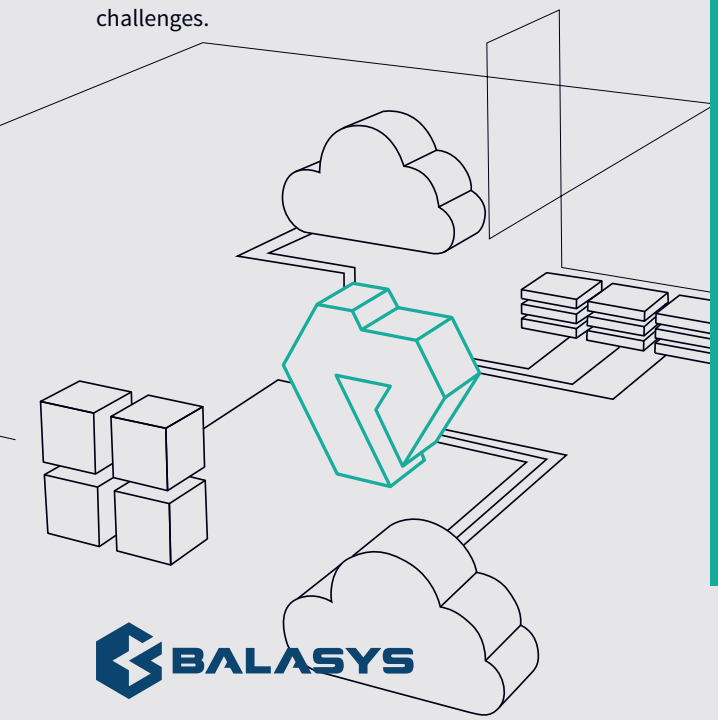
PROXEDO
API SECURITY

"Gartner predicts that by 2022, API abuses will be the most-frequent attack vector resulting in data breaches for enterprise applications."

PREVENT API BREACHES

The Challenge

Today, APIs (Application Programming Interfaces) connect tens of thousands of web and cloud applications, microservices, mobile and IoT devices, enabling seamless machine-to-machine communication. And their number is skyrocketing. An enormous amount of sensitive information in terms of personal identifiers, financial data, medical records and corporate secrets is now 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 huge security challenges.



Hackers attack 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, US Post, T-Mobile and McDonald's incidents. This is an issue that cuts across all company sizes and industries.

API developers work without security focus

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. Developers don't think like attackers. As there are no API standards, they only deal with security 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.

API risks dominate OWASP

The phenomenon of under-protected APIs cracked the OWASP (Open Web Application Security Project) Top 10 list for the first time in 2017. By 2019, API-related risks were dominating this list and OWASP had also published a specific API Security Top 10 list.

Traditional application security is no longer enough

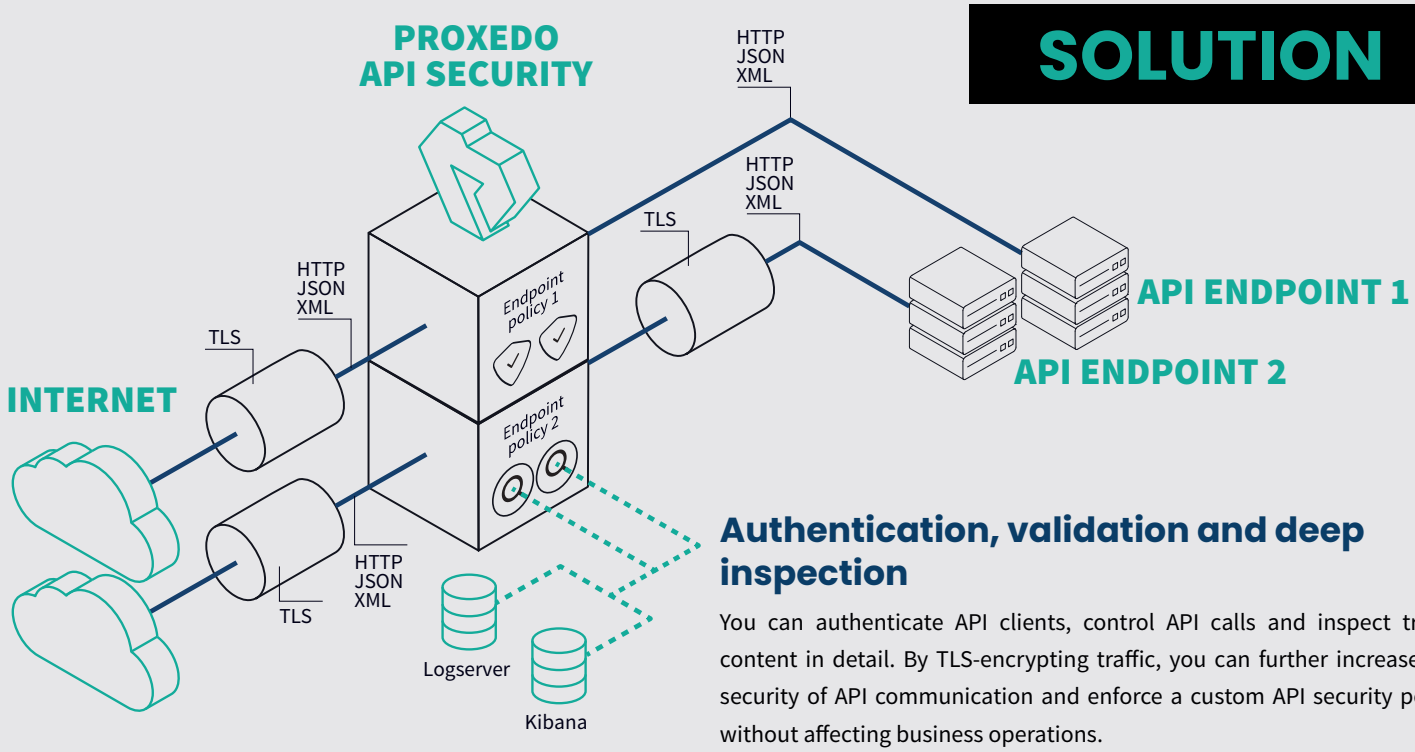
Today's API attacks are increasingly complex, targeted and easily bypass traditional security solutions. These attacks CANNOT be detected by common web application firewalls (WAFs), antivirus or other baseline security tools. Advanced API attacks can only be prevented by dedicated solutions. Without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

BALASYS

info@balasys.eu

Copyright Balasys IT Kft. All rights reserved.

SOLUTION



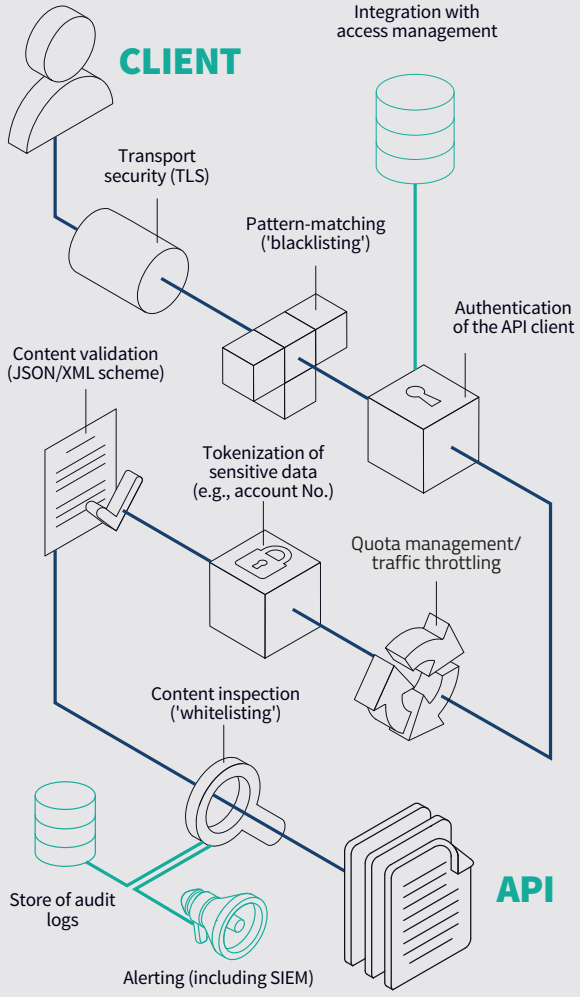
Proxedo API Security sample architecture

Authentication, validation and deep inspection

You can authenticate API clients, control API calls and inspect traffic content in detail. By TLS-encrypting traffic, you can further increase the security of API communication and enforce a custom API security policy without affecting business operations.

Content validation ensures that traffic flowing to and from API endpoints adhere to the specifications. This ensures that only permitted data is ever transmitted through the gateway. The solution also supports customizable security logging and forwarding to SOCs/SIEMs in order to enhance your organization's security monitoring and alerting posture.

Proxedo API Security can also inspect HTTP(S) traffic against a signature database to detect attack patterns. This is a reliable tool for protecting your web application services from known web threats.



Creating an effective API security policy

API Security Beyond WAF

Proxedo API Security (PAS) is a specialized web application firewall exclusively for protecting API endpoints. It's a highly flexible network security solution that helps your enterprise gain control over the application communication to prevent API breaches. Based on our Deep Packet Inspection (DPI) technology, you can validate, encrypt and analyze API traffic in detail and implement signature-based protection. Thanks to our flexible architecture, you can enforce custom security policies without compromise. PAS focuses exclusively on API security, adding an extra security layer even to your traditional WAF solution.

BENEFITS

Protecting your organization from API breaches is the ultimate goal of Proxedo API Security. It extends security practices to focus on attacks specific to APIs. The solution ensures that only permitted data is ever transmitted through your perimeter and prevents incorrect or potentially malicious data reaching your systems or sensitive data from being leaked.

Proxedo API Security Homepage

Request a trial

BALASYS