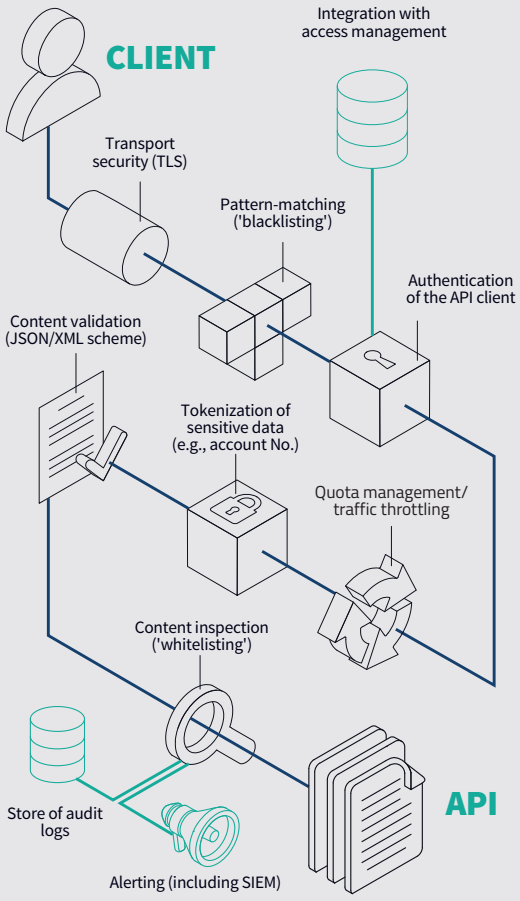
WHY PROXEDO API SECURITY?

1. **Authentication and validation of API calls**
2. **Detailed security and audit logging**
3. **Enforced data encryption**
4. **Highly flexible and skilled delivery team**
5. **Pioneers in proxy technology**
6. **Made in EU – 'clean' codebase**

PROXEDO
API SECURITY

According to the 2019 Cost of a Data Breach Report, compliance failures were one of the biggest contributors to the costs of a data breach.

API SECURITY COMPLIANCE AND AUDIT



Creating an effective API security policy

The Challenge

APIs are increasingly becoming the backbone of both internal and external communication, which means that the proper audit and compliance of API environments should also receive more focus. All compliance regulations have one key requirement in common: regulated companies must protect customers' data at rest and in transit. If data leakage occurs, it can lead to serious consequences, including penalties, loss of customer trust and future sales, additional compliance costs, and even bankruptcy.

PSD2

PSD2 is the second edition of the European Union's Financial Services Directive, which has turned the entire industry upside-down in the EU and even beyond. It requires banks to open their APIs to retailers and fintech providers. It also requires financial providers to secure the financial data flow via their public-facing APIs. Compliance with the requirements of PSD2 depend upon serious investment from both established and new players in the market.

GDPR

Both data controller and processor companies may share, gather and process personal information (email addresses, card numbers, healthcare records, etc.) via APIs. With GDPR, gaining control over these transferred data is mandatory. GDPR also requires the anonymization or pseudo-anonymization of sensitive data both in transit and at rest. It specifically mandates certain measures when data is shared with third party providers.

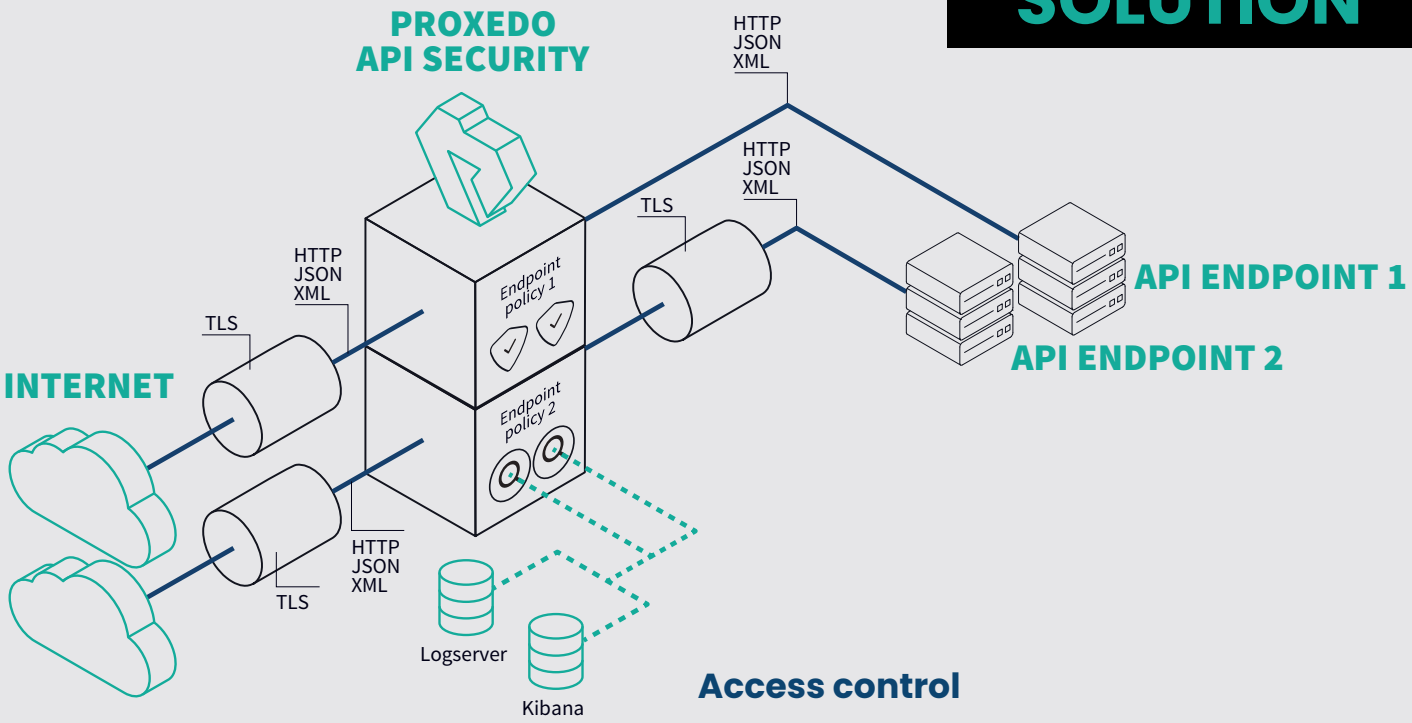
PCI DSS

PCI DSS requires financial providers and retailers to encrypt transmission of cardholder data across open, public networks. If your APIs carry any information related to payment cards, then it is essential that you and your technical partners involved in supporting these APIs meet the requirements and have a PCI certification.

BALASYS

info@balasys.eu

SOLUTION



Proxedo API Security sample architecture

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 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 a signature-based protection. Thanks to our flexible architecture, you can enforce custom security policies without compromise.

BENEFITS

All the regulations have one key requirement in common: they require regulated companies to protect customers' data at rest and in transit. Proxedo API Security helps streamline your compliance efforts in your API environment through its comprehensive access control, encryption and logging capabilities.

Proxedo API Security Homepage

Request a trial

BALASYS

Access control

With PAS, you can authenticate and control API calls. Traffic validation ensures that traffic flowing to and from API endpoints adheres to the specifications. This ensures that only permitted data is ever transmitted through the gateway and also prevents incorrect or potentially malicious data reaching your servers and sensitive data from being leaked.

PAS can also inspect HTTP(S) traffic against a signature database to detect known attack patterns. With these features, you can protect your web services from both known and unknown cyber threats.

Encryption

Proxedo API Security can handle the TLS protocol (the secure layer of HTTP) in the traffic to ensure a consistent implementation of encryption in front of your back-end systems, which don't necessarily support TLS. This setup also allows flexible configuration of encryption policies towards various communicating parties.

Proxedo's data manipulation capability enables the anonymization of sensitive data that supports compliance with various privacy standards such as the GDPR. Data can be transferred anonymously to your external partners.

Logging and Monitoring

Most IT security regulations have strict expectations regarding the logging of sensitive data communication. Proxedo API Security has a powerful log generation and collection capability. The solution can log any data access through all of your APIs. The log files are securely stored, time-stamped and indexed, and can be accessed immediately by the supervisory authorities. You can even forward security logs to your SIEM or SOC to improve your security monitoring posture.