WHAT IS IT GOOD FOR?

1. **API breach prevention**
2. **API traffic monitoring and analysis**
3. **Protecting legacy applications**
4. **API compliance and audit**
5. **Complement WAFs & API management**

PROXEDO
API SECURITY

"According to Gartner, while 70% of enterprises consider APIs to be important to digital transformation, they also admit that security remains a key challenge"

PROXEDO API SECURITY

FLEXIBLE PROTECTION OF API BREACHES

Proxedo API Security is an application-level, transparent proxy gateway built on the capabilities of the world's first modular proxy technology, with 20 years of development history.

Hackers shift their interest to APIs

The amount of sensitive data exposed via APIs (Application Programming Interfaces) is increasing significantly, making APIs a primary target for attackers. Many recent huge data breaches have leveraged APIs - just think of the Salesforce.com, US Post, T-Mobile or Verizon-incidents. API attacks are targeted and can easily bypass traditional defense. Traditional Web Application Firewalls CANNOT detect these either, since their capabilities are not tailored to deeply investigate API traffic.

API developers work without focusing on security

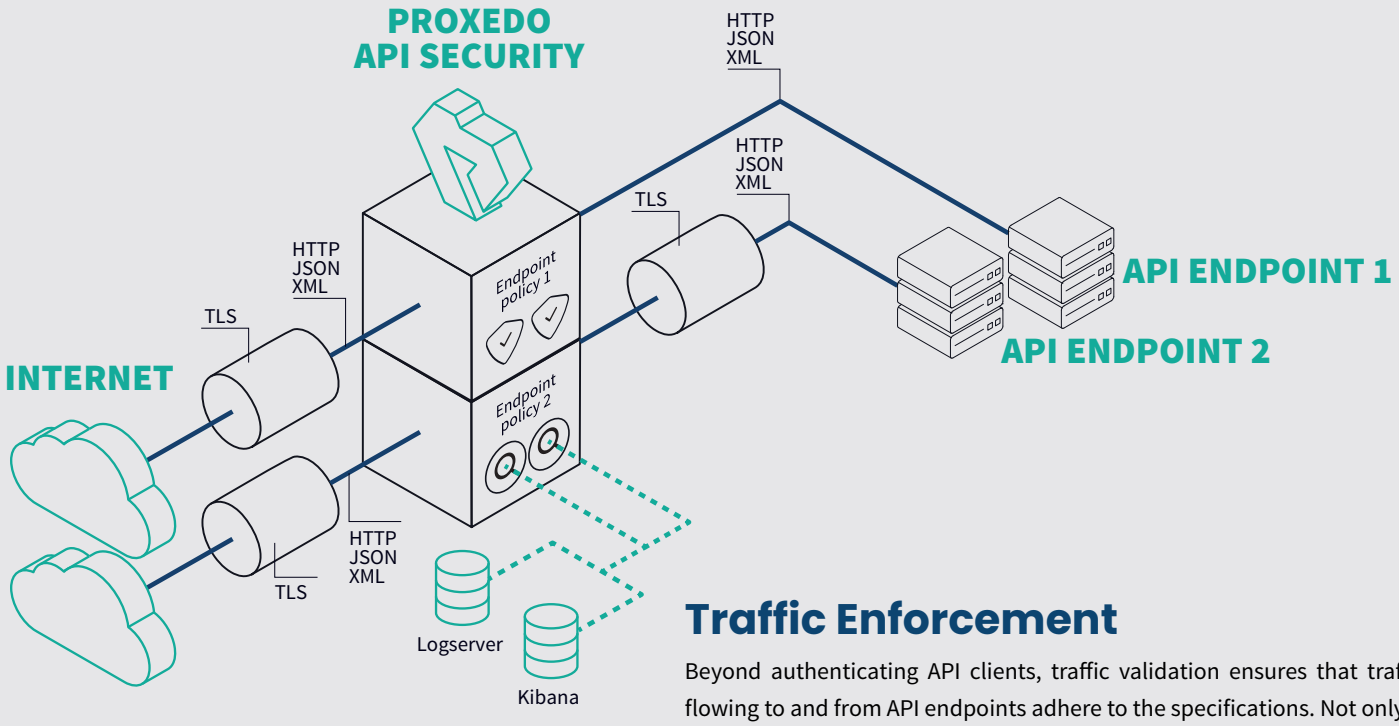
Many application development projects are far more focused on functional specification, the user experience and deadlines than security concerns. Developers don't think like attackers. This practice leaves unique vulnerabilities in public-facing APIs, creating risk for your business and opportunities for the bad guys. Thankfully, help has arrived.

API Security Beyond WAF

Proxedo API Security 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 a signature-based protection. Thanks to our flexible architecture, you can enforce custom security policies without compromise. Proxedo API Security focuses specifically on API security, adding great value even to your traditional WAF and API management tool.

BALASYS

info@balasys.eu



Proxedo API Security sample architecture

WHY PROXEDO API SECURITY

1. **Deep inspection of API traffic**
2. **Flexible security enforcement**
3. **Custom analysis of application traffic**
4. **Highly flexible, black-belt delivery team**
5. **Pioneers in proxy technology**
6. **Made in EU – 'Clean' code base**
7. **'Best-in-class' security**

Proxedo API Security Homepage

Request a trial

BALASYS

Traffic Enforcement

Beyond authenticating API clients, traffic validation ensures that traffic flowing to and from API endpoints adhere to the specifications. Not only is conformance to the HTTP protocol enforced, but each request and response is validated down to the field level against the OpenAPI schema describing the API. This ensures that only permitted data is ever transmitted through the gateway and prevents incorrect or potentially malicious data reaching your servers or sensitive data from being leaked.

Traffic Encryption

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

Traffic Insight

Proxedo API Security supports detailed debugging, security and audit logging. It provides unparalleled means for extracting data of interest from API traffic and transferring them to SOC/SIEM, big data and analytic tools. The deep understanding of calls and flexible configuration helps you extract all relevant data, and only the relevant data, in real time right from the source.

Traffic Control

Located in front of your backend servers, Proxedo API Security can also act as a load balancer for the servers. Thanks to its deep inspection capabilities, the gateway can apply not just 'default-deny' but also versatile security enforcement policies.

Signature-based Protection

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