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. **Fraud management**
6. **Complement WAFs & API management**

PROXEDO
API LIFECYCLE PLATFORM

"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 LIFECYCLE PLATFORM
API SECURITY

DON'T LET YOUR APIS TURN AGAINST YOU

The API Security is an application-level, transparent proxy gateway exclusively for protecting API endpoints. It's built on the capabilities of the world's first modular proxy technology, with 20 years of development history. The API Security is the core module of the Proxedo API Lifecycle Platform.

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

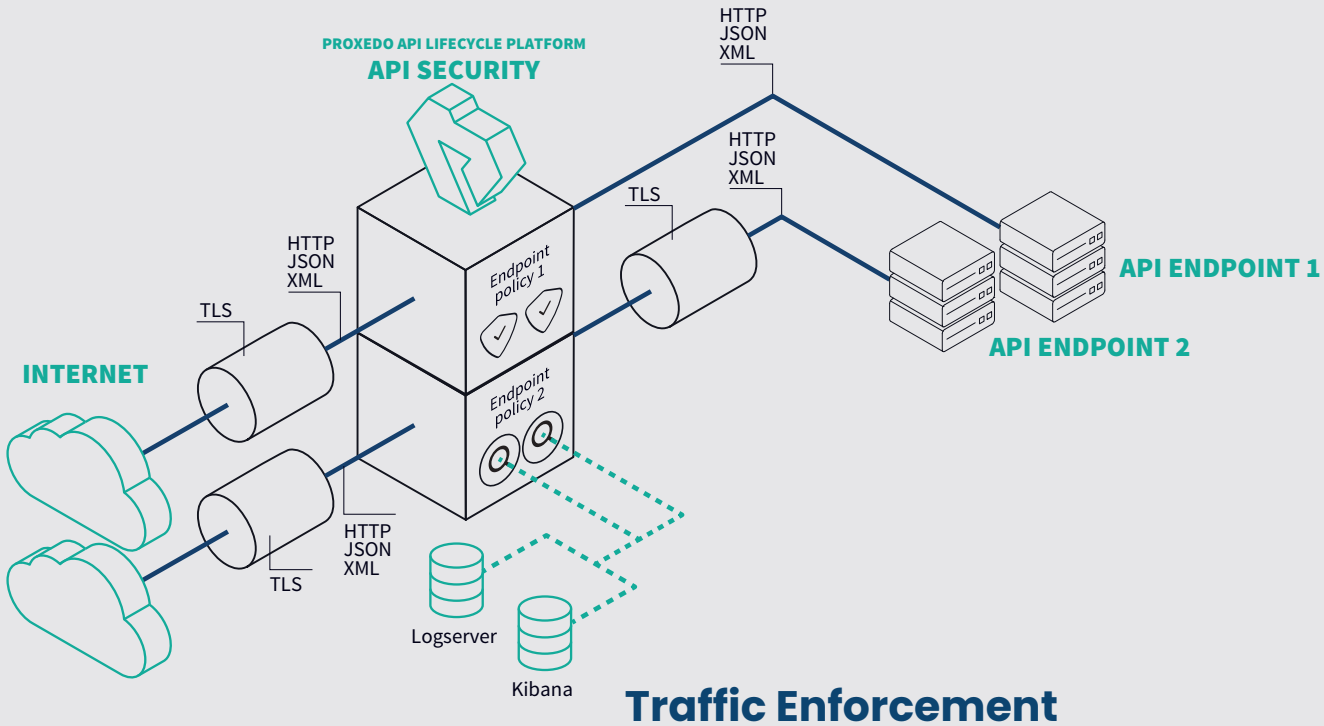
Many application development projects are far more focused on functional specification, the user experience and deadlines than security concerns. Developers don't think like attackers. This practice leaves unique vulnerabilities in public-facing APIs, creating risk for your business and opportunities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

API Security Beyond WAF

The API Security is a specialized security gateway exclusively for protecting API endpoints. It's a highly flexible network security solution that helps your enterprise control and monitor the application traffic to prevent API breaches. Based on our deep packet inspection (DPI) technology, you can validate, encrypt, and analyze API traffic in detail. Thanks to our flexible architecture, you can enforce custom security policies without compromise.

BALASYS

info@balasys.eu



The API Security sample architecture

Traffic Encryption

The 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 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 Insight

The 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, the 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.

WHY API SECURITY

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

Proxedo API Lifecycle Platform homepage

Request a trial

BALASYS

About the Proxedo API Lifecycle Platform

The Proxedo API Lifecycle Platform (PALP) is a modular solution that allows you to protect and manage your APIs. PALP provides an end-to end API security toolset helping your enterprise prevent API-specific threats, automated attacks, APTs and frauds. Its core component is API Security, a specialized security gateway that controls and monitors the API traffic in detail. Beyond the API security core, the portfolio includes API management, web application firewall and fraud detection. These enhanced functional modules work closely with the API security module adding a comprehensive security and management layer to your API environment.