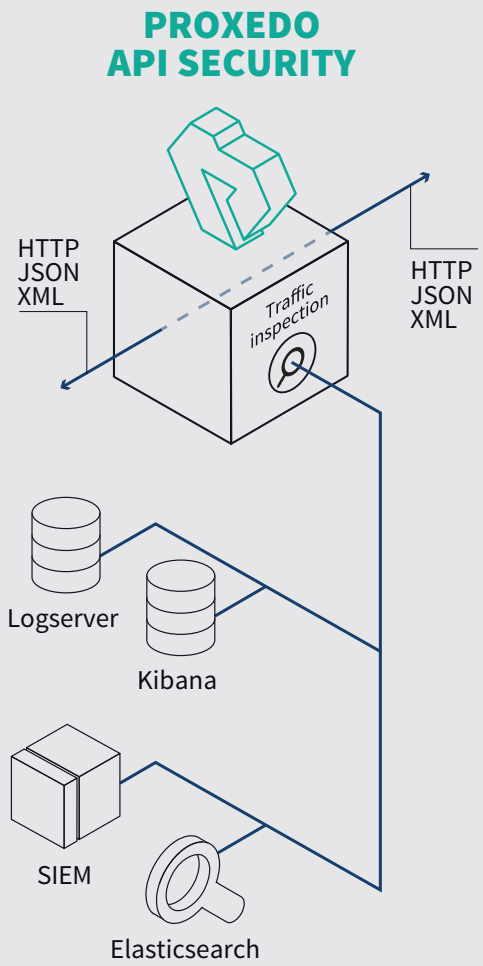
WHY PROXEDO API SECURITY?

1. **Detailed debugging, security and audit logging**
2. **Customizable data extraction from traffic**
3. **Forwarding to big data tools, log analyzers or SOCs/SIEMs**
4. **Highly flexible and skilled delivery team**
5. **Pioneers in proxy technology**
6. **Made in EU – 'clean' codebase**

PROXEDO API SECURITY

"Many major online shops crashed or temporarily stopped on Black Friday in 2019, mainly because of API errors."

MONITORING AND ANALYSIS OF API TRAFFIC



Proxedo API Security analyzes API transactions

The Challenge

Your enterprise has likely built web applications on a foundation of APIs, both internal and external. Since your web services or native applications rely on APIs for critical data transactions, API monitoring and analytics should be an integral part of your API security strategy.

Security and Operations Need to Gain Insight

Due to logging limitations, enterprises operating extended API infrastructure face serious challenges when it comes to monitoring API traffic. Both your IT operations and security teams should proactively monitor API traffic to ensure operational safety and detect threats.

Businesses Suffer from Messy Customer Data

Business managers also suffer from insufficient reports about customers' online behavior. The lack of quality business data might result in non-informed decisions, not to mention the inability to identify suspicious customer behavior, which could lead to a serious data breach, as happened with US Post.

Developers Need Efficient Debugging

The lack of sufficient logging hinders developers to measure API and application performance, transactions or identify errors. Build better relationships with your developers and drive decisions based on valuable insights.

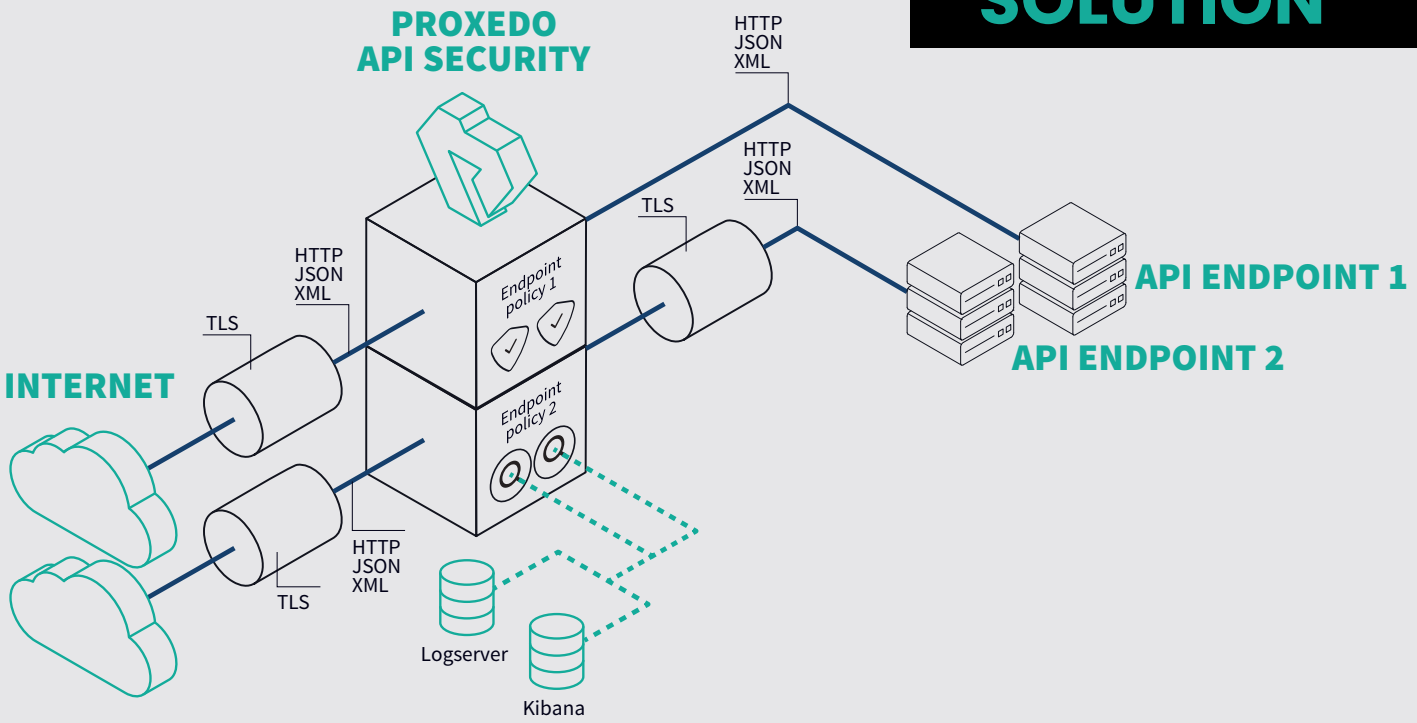
API Failures Are Business Critical

Mainly due to API errors, many online retail sites crashed or had downtimes during Black Friday 2019. In some cases, the crash occurred at third-party providers. For example, the API of the payment gateway failed, causing web shops significant losses. Failure to handle online transactions during peak periods could cost your business millions of dollars.

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

Balasys Proxedo API Security helps you understand what is going through your APIs. Your security team can improve security monitoring to effectively combat threats. IT operations can understand how APIs are being adopted and used, and how APIs can be improved. Your API developers can check how their applications are performing. Business managers can analyze API transactions and make more informed decisions.

Proxedo API Security helps you easily recover in the event of a major application outage and identify bad actors or changes in user behavior. In addition, it also enables you to measure your API program's progress and plan future investments.

Proxedo API Security Homepage

Request a trial

BALASYS

Traffic Insight

Proxedo API Security provides unparalleled means for extracting data from API traffic and transferring them to various third-party tools for analysis. 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.

Security Monitoring and Audit

PAS supports detailed security and audit logging. You can feed your SIEM or SOC with reliable, relevant data to improve your security monitoring and alerting capabilities. Detailed logging of API transactions also helps application audits and supports compliance efforts.

Business Analytics

PAS supports big data tools and data lakes (for example, Kibana, Elasticsearch and Kafka) as potential log destinations. You can send pre-filtered, quality data to these destinations for in-depth business analysis.

Debugging

Detailed debug logs help your developers troubleshoot API problems. This decreases the number of API vulnerabilities and improve application security during the development process and after release. Relevant logs also come in handy for IT operations and can enhance the operational safety of web applications. Capturing HTTP requests from non-browser applications – like mobile apps – is also possible.

Traffic control

Located in front of your backend servers, PAS 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 enforcement policies.