WHY PROXEDO API SECURITY?

1. **Deep inspection and control of API traffic**
2. **Flexible security enforcement**
3. **Detailed security and audit logging**
4. **Highly flexible and skilled delivery team**
5. **Pioneers in proxy technology**
6. **Made in EU – 'clean' codebase**

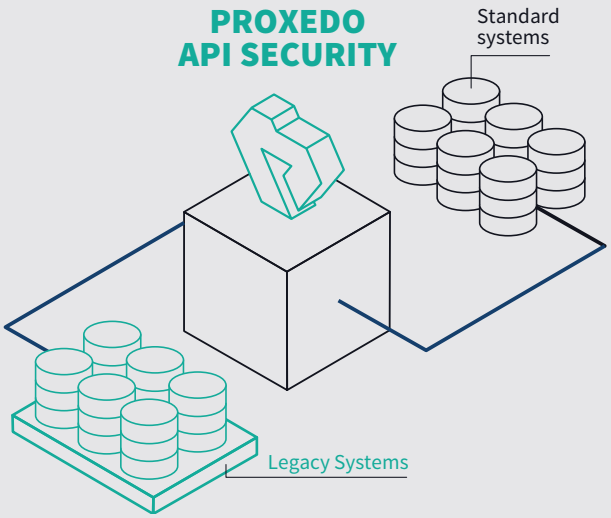
PROXEDO
API SECURITY

"The recent widespread attacks of WannaCry and NotPetya both used known vulnerabilities of legacy operating systems…"

– securityintelligence.com

PROTECTING LEGACY APPLICATIONS

Legacy infrastructure is still a crucial part of enterprises across many industries. Core banking systems hosted by AS/400s, healthcare organizations relying on Windows XP, business applications requiring Linux RHEL4 and ATMs running decade-old Windows versions are just a few examples. Replacing or updating proprietary software is costly and sometimes virtually impossible, so you must mitigate the risk of using legacy applications together with the APIs (Application Programming Interface) that expose them.



Segregation and protection of legacy systems

The Challenge

Old infrastructure - new risk

What seemed secure years ago may be demonstrably insecure today. Many times, legacy systems use outdated encryption protocols or distribute sensitive information about themselves (e.g. version information, error messages, etc.) Unfortunately, in many cases, organizations ignore the advice to patch these systems, leaving several vulnerabilities unmanaged in them. A significant amount of recent widespread attacks (e.g. WannaCry, NotPetya) have exploited the known vulnerabilities of legacy systems.

Internal applications externally exposed

This happens far more than anyone would care to admit. Websites developed for internal use are almost never developed to the same security standard as public websites. However, over time – due to M&As, partnerships and business pressures – internal applications become exposed to the internet. The unsecure public traffic that travels through APIs specifically poses a great risk to your company.

Unsecure legacy components compromise your entire IT

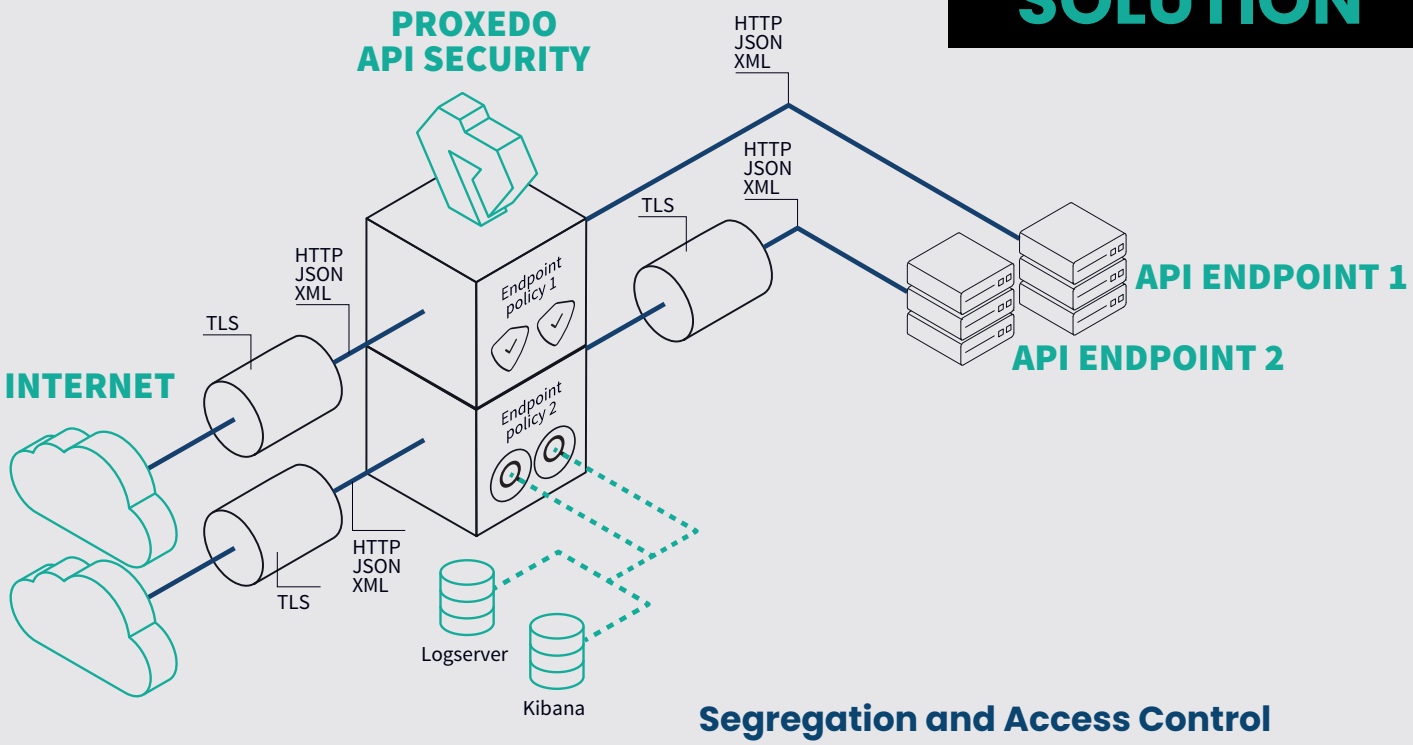
The risk of failing to properly secure legacy systems is extensive and goes beyond the legacy workloads themselves. An unpatched device running Windows XP can easily be exploited to gain access to any data center. Or just think of the recently announced Microsoft Exchange 2013 vulnerability, which enabled attackers to gain Domain Admin privileges in Windows networks.

If attackers gain access to your unpatched legacy machine, they can laterally move deeper into your network. Due to the complex interdependencies among different business applications (legacy and non-legacy), attackers can move undetected across your infrastructure.

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

PAS can hide information about security risks and treat the vulnerabilities of your legacy applications. Both your IT operations and security teams benefit from a proper perimeter protection in front of the APIs exposing your legacy system. PAS can help you reduce the risks that arise when updating or patching a system is simply not an option.

Proxedo API Security Homepage

Request a trial

BALASYS

Segregation and Access Control

Proxedo API Security can separate legacy systems from other systems. PAS ensures that those systems are not directly accessible from the internet and guarantees that any communication with them is authenticated and restricted.

Traffic validation ensures that traffic flowing to and from the legacy application adhere to the specifications. This ensures that only permitted data is ever transmitted through PAS and prevents incorrect or potentially malicious data reaching your legacy system or sensitive data from being leaked.

Encryption and data masking

PAS can handle the TLS protocol in the traffic to ensure a consistent implementation of encryption in front of your legacy systems that don't necessarily support TLS. It can even force legacy encryption protocols to upgrade to the recent TLS version. With PAS you can centrally manage the TLS settings of your APIs to ensure the configuration complies with the latest security requirements.

PAS can ensure compatibility with your legacy systems by modifying certain elements of API traffic. This enables you to hide vulnerabilities. For example, you can remove error messages, banners or other information specific to the application to hide the faulty configuration of your back-end infrastructure.

Monitoring

Security monitoring is especially vital for legacy systems. PAS supports detailed security and audit logging. You can forward relevant logs to the SIEM or SOC to improve your security monitoring and alert capabilities. Traffic logging and monitoring can help you detect threats to your legacy application before they become a data breach.