

**PRODUCT SHEET** 

**API Security** 





## Table of contents



# Market-leading capabilities to secure your API applications

## Comprehensive API type support



Protect your businesscritical data by assessing all types of REST APIs, GraphQL, and SOAP APIs.

#### Built-in parser support



Easily import your APIs using our built-in parsers that support various formats, including Postman, Fiddler, Burp Suite, HAR, and many more.

## compliance



Find the most common API application vulnerabilities with the most powerful compliance framework.

OWASP Top 10 API

## Get the hacker's perspective



See what cybercriminals would see if they were to hack into your systems, target you with a phishing attack, or try to spread ransomware.

## Al-driven threat intelligence



Our Al-powered Security Research team keeps you updated with the latest vulnerabilities — around the clock, all year round.

### Support the entire workflow



Our Security Center provides one unified view for discovery, prioritization, remediation, and reporting.

#### **Fully automated**



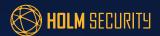
Automated and continuous asset discovery and monitoring, vulnerability assessments, prioritization, reporting, and follow-up.



## Beyond OWASP Top 10 API vulnerabilities

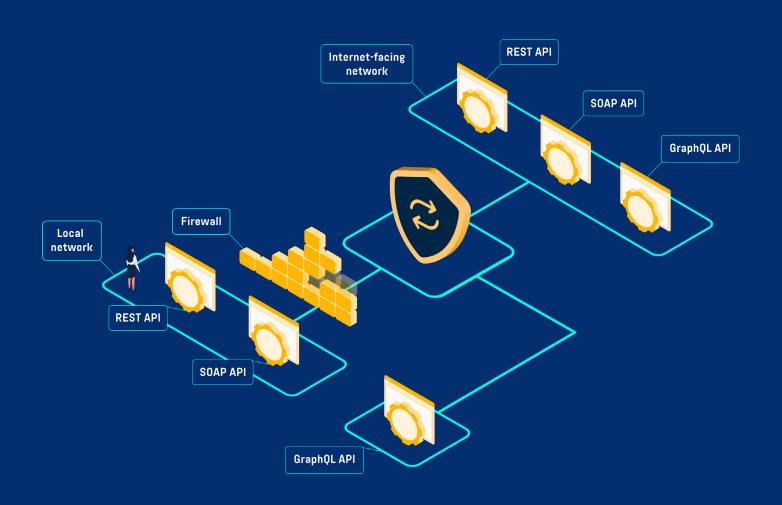
Find the most common API vulnerabilities according to OWASP Top 10 API and beyond.

$\otimes$	Broken Object Level Authorization (BOLA)	Identify vulnerabilities that allow cybercriminals to access or manipulate objects, like database records, leading to data breaches, unauthorized data modifications, or privilege escalation.
$\bigcirc$	Broken authentication	Find common authentication vulnerabilities that allow cybercriminals to impersonate users or gain unauthorized access to API applications.
$\bigcirc$	Excessive data exposure	Discover data exposure vulnerabilities caused by poor design, which can lead to sensitive data leaks, data manipulation, and an increased risk of data misuse.
	Lack of rate	Find APIs without rate-limiting controls that are vulnerable to
$\bigcirc$	limiting or resource management	brute-force attacks, denial of service (DoS), and abuse by bots, to avoid service downtime and unauthorized access.
	_	brute-force attacks, denial of service (DoS), and abuse by bots, to



# A growing number of API applications

More and more systems are integrated using APIs to achieve automated data exchange and the possibility of automating workflows and functions. Accordingly, the risk exposure for APIs and the data linked to them is growing rapidly. We find vulnerabilities in all types of APIs, both self-developed and commercial APIs.





# The most powerful platform for compliance

## Meet today's & future compliance

Along with the growing threat picture, new legal requirements, directives, standards, recommendations, and certifications are continuously introduced. We help you meet current and future requirements with a systematic, risk-based cyber defense, covering NIS, NIS2, DORA, CRA, GDPR, ISO 27001, and PCI DSS.



## Integrated Attack Surface Management (ASM)

#### **API** asset discovery

Continuously uncover hidden, lost, or forgotten local and internet-facing APIs.



## Benchmark with industry colleagues



## A complete toolkit with Security Center

#### Efficiently measure & communicate risk

We provide all the tools you need to measure and communicate risks both internally and externally.

#### Benchmark your risk exposure

Gain insights into your organization's risk exposure compared to others in your industry.

#### Discover

Automatically and continuously discover domain and web assets with Attack Surface Management (ASM) and External Attack Surface Management (EASM).

Automatically and continuously assess web applications.

Assess

#### **Prioritize**

Al-driven threat intelligence to guide your vulnerability prioritization.

#### Remediate

Full workflow support for remediation actions.

## **Streamline** workflows with integrations

#### SIEM, ticketing, CMDB, CI/CD & more

Integrate vulnerability management into your routine workflow. We offer out-of-the-box integrations with a wide range of systems, including Security Information and Event Management (SIEM), Configuration Management Database (CMDB), patch management, ticketing systems, and Continuous Integration/ Continuous Deployment (CI/CD).

#### **Custom integrations**

Using our Application Programming Interface (API), you can create custom integrations tailored to your specific needs.



## **Deployment options**

#### Cloud

#### Get started in hours

Our cloud-based deployment option is a comprehensive solution for automated and continuous vulnerability management with zero system requirements. It supports organizations of all sizes and environments, regardless of previous experience with vulnerability management. Getting started with our powerful and easy-to-manage platform only takes a few hours.

#### On-Prem

#### Full control over sensitive data

Our on-premise deployment option offers a comprehensive solution for automated and continuous vulnerability management, designed to meet the needs of organizations that prefer to keep sensitive data within their own infrastructure.

#### Best choice for data privacy

We provide the best choice for data privacy and data protection in the industry, with data processing and storage in a neutral country.

#### Public & local assessments

Our cloud-based platform enables you to scan both internet-facing systems and local infrastructure, providing you with a simple yet powerful solution with comprehensive asset coverage.

#### Local deployment - local storage

Installed in your virtual environment, supporting all common virtualization platforms. No sensitive data is communicated over the internet.

#### **Unlimited scanners**

Supports unlimited scanners, allowing you to scan your entire infrastructure, all managed through a single pane of glass for streamlined visibility.



## Capabilities overview

A comprehensive product including all the features you need:

Comprehensive API type support, REST APIs, Grapi	nQL, and SOAP APIs.
--	---------------------

- Assessment of internet-facing and local APIs.
- Full workflow support from discovery to remediation.
- OWASP Top 10 API compliance.
- Integrated Attack Surface Management (ASM) and External Attack Surface Management (EASM).
- Support compliance with NIS/NIS2, DORA, GDPR, CRA, ISO 27001 and the NIST framework.



## Why Holm Security?

## Understand your attack surface

One of the key functions in Next-Gen Vulnerability Management is to help understand your attack surface using automated techniques to continuously identify new assets that could potentially expose your organization to risk.

## 2 Unified view to ease prioritization

Reduce business-critical risks with the least amount of effort. This is accomplished by providing a truly unified platform where all your risks are prioritized and listed in one single view.

## Powerful threat intelligence

Our platform lets you focus on high-risk vulnerabilities and users likely to be exploited. Understand the full context of each exposure to maximize your efforts. Our platform also provides superior built-in threat intelligence to help understand and prioritize risk more efficiently.

## Let the platform do the work

Our platform is fully automated.
Once it's been implemented, it runs continuously in the background. No need for software or hardware.

## How can we help?

Want to get in touch? We'd love you hear from you. Here's how you can reach us.

+46 8-550 05 582 sales@holmsecurity.com www.holmsecurity.com





