HOLM SECURITY

PRODUCT SHEET

Web Application Security

MADE IN EUROPE

Stability — Reliability — Unity

Version 5.0

Table of contents

Market-leading capabilities to secure your applications

Comprehensive assessment capabilities

Finding vulnerabilities like Cross Site Request Forgery (CSRF), Remote File Inclusion (RFI), as well as outdated JavaScript components, weak passwords, and web server and web framework misconfigurations.

OWASP Top 10 compliance

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

Advanced authentication features

Supports a wide range of authentication methods for scanning web appications "behind" a login.

Modern web app support

Supports scanning of modern JavaScript-powered web applications using AI-driven threat intelligence.

Get the hacker's perspective

Determine how secure your organization is if cybercriminals attempt to hack your systems, target you with phishing attacks, or try to spread ransomware.

AI-driven threat intelligence

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

Supports the entire workflow

Our Security Center offers a single pane of glass for discovery, prioritization, remediation, and reporting.

Fully automated

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

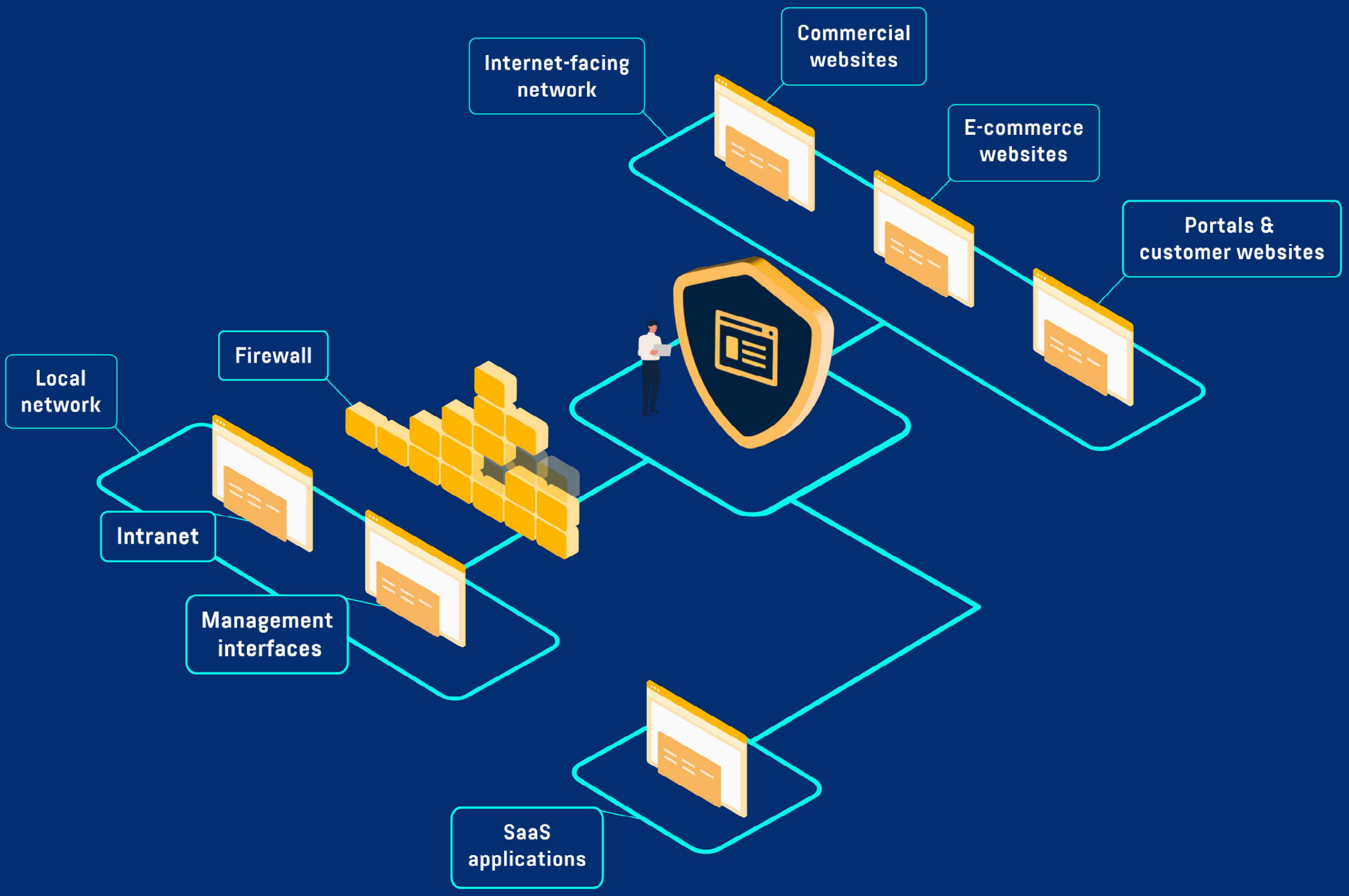
Beyond OWASP Top 10 vulnerabilities

Full support for compliance assessments according to OWASP Top 10 versions 2017 and 2021.

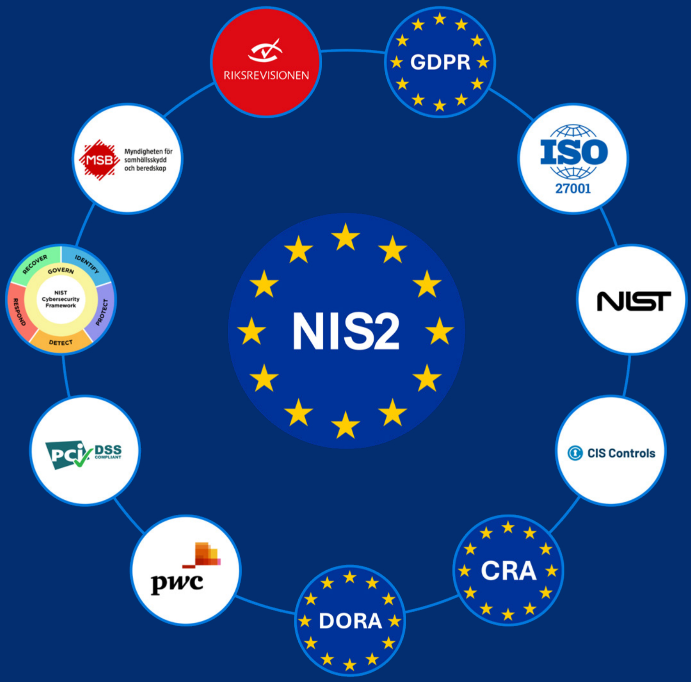
SQL injection, XSS, CSRF, IDOR & much more	Find all common web application vulnerabilities such as SQL injection, Cross-Site Scripting, Cross-Site Request Forgery, Insecure, and Direct Object References.
Security misconfigurations	Identifies poorly configured web servers and web applications.
Outdated frameworks & components	Identify vulnerabilities in outdated programming languages and components, such as old PHP and JavaScript versions.
Sensitive data exposure	Misconfigurations exposing sensitive system information and sensitive data.
Weak passwords	Finds weak passwords used for authentication in all types of web applications – internal and internet-facing.
Web & domain blank spots	Continuous and automated asset discovery of web and domain assets with Attack Surface Management (ASM) and External Attack Surface Management (EASM).

A growing number of web apps

What used to be desktop apps are today web apps. Accordingly, the risk exposure for web applications is growing rapidly. We find vulnerabilities in all types of web applications, both self-developed and commercial applications, such as commercial websites, specific web application systems, Intranets, portals and control panels, and admin interfaces.



The most powerful platform for compliance



Meet today's & future compliance

Along with the growing threat landscape, 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)

Web asset discovery

Automatically discovers, monitors, and continuously tracks web applications in your infrastructure with Attack Surface Management (ASM).

Domain asset discovery

Automatically discovers, monitors, and continuously tracks internet-facing domain assets with External Attack Surface Management (EASM).

Benchmark against industry colleagues

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.

A complete toolkit with Security Center

Discover

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

Prioritize

AI-driven threat intelligence to guide your vulnerability prioritization.

Assess

Automatically and continuously assess web applications.

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.

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.

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.

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:

- ✓ Assessment of both internet-facing and local web applications.
- ✓ Unauthenticated and authenticated scanning.
- ✓ Full workflow support from discovery to remediation.
- ✓ Compliance with OWASP Top 10.
- ✓ Detection of CMS vulnerabilities.
- ✓ JavaScript support.
- ✓ Integrated Attack Surface Management (ASM) and External Attack Surface Management (EASM).
- ✓ Compliance support for NIS/NIS2, DORA, GDPR, CRA, ISO 27001, and the NIST framework.

Assessment technologies

Technologies:	Description:
DAST and SCA technology	Our web application scanner is based on Dynamic Application Security Testing (DAST) and Software Composition Analysis (SCA).
Internet-facing and local web apps	Scans internet-facing and local web applications.
Automatic detection	Automatically identifies web servers, programming languages, and databases.
JavaScript support	Supports scanning web pages built with JavaScript technology with any popular frameworks such as AngularJS, VueJS, ReactJS, etc.
API vulnerabilities	Automatically detects SOAP APIs and supports scanning REST APIs such as those using OpenAPI v2 and v3.
CMS vulnerabilities	Finds vulnerabilities in CMSs such as WordPress and WordPress plugins.
Standard authentication support	Basic authentication using Basic auth, Static Forms, dynamic JavaScript forms, or special headers to scan for vulnerabilities as an authorized user.
Advanced authentication support	Record a login authentication sequence in the web browser to scan for vulnerabilities behind login for advanced login use cases such as single sign-on or multi-step authentications.

Vulnerability finding capabilities

Capabilities:	Description:
Misconfigured web servers	Find vulnerabilities like exposed directory listing or public access.
Weak passwords	Brute force logins using common usernames and passwords.
Outdated JavaScript components	Detects outdated and vulnerable JavaScript components.
Exposed personal details and financial information	Find exposed personal information like personal IDs and credit card details.
OWASP Top 10	Full support for both OWASP Top 10 versions 2017 and 2021.
Exposed sensitive information	Detects exposed system or application information such as source code or configuration values.
Faulty SSL certificates	Detects SSL certificates that are about to expire, have expired, are deprecated, or are vulnerable.
Fuzz testing	Detects if a web application behaves irrationally or unexpectedly.

More capabilities →

Vulnerability finding capabilities

Capabilities:	Description:
SQL injection	Detects SQL injections and blind SQL injection vulnerabilities.
Cross-Site Request Forgery (CSRF)	CSRF is an attack that forces an end user to execute unwanted actions in a web application in which they're currently authenticated.
Remote File Inclusion (RFI)	The RFI vulnerability allows an attacker to download and execute a file.
PHP misconfiguration	Detects common PHP misconfiguration vulnerabilities.
Virtual host identifications	Identify exposed virtual hosts that are configured on the web server.
Server-side Include (SSI)	SSI injections occur when user-controlled input is embedded into a server-side template, allowing users to inject template directives.
Exposed email addresses	Detect exposed email addresses that could be used in social engineering, such as phishing, spear phishing, and ransomware attacks.

Why Holm Security?

1 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.

3 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.

4 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

NIS2 Directive Compliant

CERTIFIED ISO 27001 SVENSK CERTIFIERING

MADE IN EUROPE Stability Reliability Unity