HOLM SECURITY

OUR TOP PRIORITY

Safeguarding your data

MADE IN EUROPE
Stability — Reliability — Unity

Version 5.0

Security from every angle

We work actively and continuously to ensure that our customers' data is secure – our top priority. Below, we outline our most important security and operational practices in our continued work at transparency and data security.

Certifications & compliance

ISO 27001:2022

Holm Security's operations are ISO/IEC 27001:2022 certified, demonstrating a strong and independent commitment to information security best practices.

GDPR compliant

Complying with GDPR is a top priority and we actively protect your personal data as part of our information security efforts.

NIS2 compliant

We comply with NIS and NIS2 requirements for a systematic, risk-based cyber defense, as demonstrated by our ISO/IEC 27001:2022 certification.

Platform security

Proven & secure technologies

We only use mature, established, and well-proven technology in our platform to avoid security risks that new, unproven technology can bring.

Separation of data

Data is separated logically between customers to ensure that it stays with the customer context. We apply an additional layer between our front-end and back-end services that validates the data to ensure it is not cross-accessed by customers. This security layer thus provides an exceedingly high level of security and prevents unauthorized data access.

Encryption

All data stored in our Next-Gen Vulnerability Management Platform (VMP) is encrypted both in transit and at rest using industry standard encryption with TLS 1.2+ as a minimum for communication.

Single sign-on & two-factor authentication

Security Center supports SSO and 2FA to ensure login security. Two-factor authentication can be combined with access based on the user's network, making it impossible to access Security Center from outside your organization's network or VPN.

Password policies

Security Center uses a strict password policy to prevent the use of weak passwords. Customers can customize this to further strengthen user passwords.

Full audit log

User activities in Security Center are logged in detail in a read-only audit log that cannot be manipulated regardless of access rights.

Scanner Appliance

Our remote scanner, Scanner Appliance, is built with a strong focus on secure communication and ensuring that intrusion at one point does not allow intrusion at another. Software updates are signed offline (in an air-gapped environment) to guarantee

that they are from us and minimize the risk of manipulation.

Device Agent
The Device Agent uses industry-standard encryption. Data in transit is, by default, encrypted with the preferred TLS protocol 1.2. Only trusted certificates allow the Device Agent to establish communication. The application executable (.exe) and installation package (.msi) are signed by Digicert® using an offline and secure air-gapped signing routine. This also applies to software updates.

Data centers & data storage

Physical data protection
Our platform is hosted in data centers with strong physical perimeter protection, internet redundancy, and redundancy for power supply.

All sensitive data stored in the EU
To meet demands from European organizations, Holm Security stores data in neutral countries, where authorities and government agencies do not have the legal right to access the data.

ISO 27001 certified data centers
The data center that hosts our platform in Europe is ISO/IEC 27001 and ISO/IEC 9001 certified.

Secure software development

Secure development lifecycle
Security is built into every stage of development, with automated processes and manual reviews.

Continuous security assessment & penetration testing
Holm Security performs continuous and automated penetration testing and vulnerability assessments.

Environment separation
Development, test, and production systems are strictly separated.

Data protection & privacy

Information classification
Customer and vulnerability data are carefully classified and protected based on sensitivity.

Encryption
All sensitive data is encrypted both in transit and at rest.

Data retention
Personal and vulnerability data is retained only as long as necessary and deleted in adherence to strict rules.

Extensive logging
All systems and applications log all events by default to achieve full traceability. We continuously ensure that logs are not tampered with.

Employee & access security

Background checks
Holm Security's employees with access to sensitive data undergo a background check and are evaluated to assess potential future risks.

Continuous awareness training

All employees are continuously trained to meet a high standard of security awareness by running phishing simulations and tailored awareness programs. We also require recurring awareness and information security training.

Restricted access

The basic access principle that applies to all systems on the platform is that each employee only has access on an as-needed basis, meaning that we follow a low-trust model. All internal systems are only accessible via Virtual Private Network (VPN), which utilizes multiple authentication methods.

IT & operational security

Patch management

We perform ongoing vulnerability assessments in our own environment to identify any vulnerabilities and patch critical vulnerabilities immediately.

Endpoint protection

Company laptops and mobile devices are encrypted and monitored to identify malicious activity at all times.

Logging & monitoring

All systems and servers are continuously monitored and logs are centrally stored and continuously reviewed.

Physical & business continuity security

Office security

Our offices maintain badge-controlled access and require visitors to have visitor badges. They also provide secure areas for IT equipment storage and infrastructure.

Backup & recovery

Production data is backed up daily and complete recovery tests are performed continuously.

Business continuity planning

Holm Security has a detailed Business Continuity Plan (BCP) that is tested and developed through continuous disaster simulations.

Disaster recovery plan

We work actively with a disaster recovery plan to ensure business continuity in the event of a disaster with substantial adverse effects on operations.

Incident management

Incident response

Holm Security documents all incidents as part of improving our cyber defense.

Customer-related incidents & communication

If an incident does occur, we notify impacted customers instantly.