



## Network Scanning

Gain visibility into your network security

# Network Scanning

Take control of the security of your networks and systems with our network scanning. The service scans for more than 68,000 vulnerabilities. Regardless of whether you manage all of your IT yourself or outsource, our network scanning is the most effective way to understand how secure you are against external threats, to rectify vulnerabilities and increase your cyber security requiring only a small investment in time. The service offers a wide range of compliance functions for GDPR, NIS, PCI DSS, ISO 27001 and more.

## Automatically and continuously

Our network scanning automatically and continuously scans your networks and systems for an ever-increasing number of vulnerabilities. Network scanning detects vulnerabilities related to old software, exposed services and functions, misconfigured systems, weak passwords etc. In addition, the service automatically maps your network to give you a clear overview of all your systems – regardless of geographical location and whether you manage all your IT yourself or outsource all or part of your IT environment.

Using comprehensive information, smart and effective tools as well as our support and specialist help, you or your IT partner can effectively prioritize and rectify detected vulnerabilities before they are exploited by a malicious person.

In parallel with a scheduled scanning of your networks and systems, you can scan on demand at any time, for example in connection with changes and commissioning.

## Covering the entire IT environment

Our scanners scan your public networks and systems, accessible via the Internet. By installing one or more Scanner Appliances in your local environments, behind your firewalls, we can scan all your networks – even if your IT environment is present in several physical locations. All scanned data collected by our Scanner Appliances is presented in our control panel Security Center.

## Scan details

- ✓ Scanning of public networks and systems accessible via the Internet
- ✓ Local scanning of networks and systems behind your firewalls with virtual appliance (Scanner Appliance)
- ✓ Supports scanning of local cloud infrastructure, such as AWS
- ✓ Detects vulnerabilities in, for example, old software and exposed services and functions
- ✓ Detects misconfigured systems
- ✓ Detects weak passwords
- ✓ Maps hosts, ports and services
- ✓ Automatic update of vulnerability database
- ✓ Windows and Linux authenticated scanning
- ✓ High precision with low number of false-positives

## Other details

- ✓ No software or hardware requirements
- ✓ Automated and scheduled scans, as well as scans on demand
- ✓ Detailed device register
- ✓ Automated device mapping (Auto Discovery)
- ✓ Automated and manual structuring and grouping of devices
- ✓ Vulnerability manager – administration of vulnerabilities
- ✓ Continuous Monitoring – monitoring of vulnerabilities and changes
- ✓ Functions for GDPR and NIS compliance
- ✓ Customizable detail and statistical reports
- ✓ Customizable dashboard for quick overview
- ✓ Full IPv6 support
- ✓ Administration via Security Center

## Vulnerability manager

Vulnerability manager is a powerful tool for you to work effectively with vulnerabilities, regardless of whether you have a small number or thousands. You sort, group, ignore and prioritise the vulnerabilities in just the way that works best for you. The tool provides a range of functions for collaboration within your organization and with external partners, such as your IT partner.

## Continuous Monitoring

In Continuous Monitoring, you can quickly and easily set up monitoring of changes that generates notifications and alarms. This tool removes the need to work in Security Center. Instead, you will be notified when new vulnerabilities are detected, when any changes are made and when vulnerabilities have been rectified. You can easily pinpoint, for example, systems handling personal data for GDPR compliance or a specific network to obtain information about ports that are opened or closed.

## Remediation

The service includes a complete tool for remediation. The flow is largely automated. You set up rules for when to create cases and how to assign them. The tool supports integration with external remediation systems.

## Reports

A number of ready-made templates are available in the service, and you can create your own reports – adapted for both technicians and specialists, as well as management, CEO and the board. The reports are distributed in encrypted form to, for example, your IT partner or system vendor. In parallel to creating reports automatically according to your desired schedule, you can create reports on demand at any time.

## Functions for compliance

The service offers a range GDPR, NIS, PCI DSS, ISO 27001 compliance support functions. You can, among other things, pinpoint your personal data systems to monitor these, and automatically generate continuous reports to the data controller.

## Market-leading vulnerability assessments

**Holm Security is a challenger in automated and continuous vulnerability assessments.**

Our Holm Security VMP platform offers the ability for everyone to effectively take control of the security of their networks and systems. But we also offer innovative solutions to assess how secure your users are. Our platform is easy to use and you get extensive support from our support staff and security experts. An investment in our platform is, in short, a smart and efficient investment in increased security – not least when faced with a future where cyber security is becoming increasingly important to meet an increasing number of threats, new and existing laws and recommendations.

## Contact

Holm Security  
Gustavslundsvägen 141  
SE-167 51 Bromma  
Sweden  
Telephone: +46 8-550 05 570  
info@holmsecurity.com  
www.holmsecurity.com