



HOLM SECURITY

Prioritizes your Cybersecurity Risks proactive and easy

WATERSCHAP ZUIDERZEELAND

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

CUSTOMER EXAMPLES

1,000+ customers

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

Our platform protects your most important assets

Risks

- Phishing attacks
- Ransomware
- Intrusion
- Operational disruptions and sabotage

Incidents

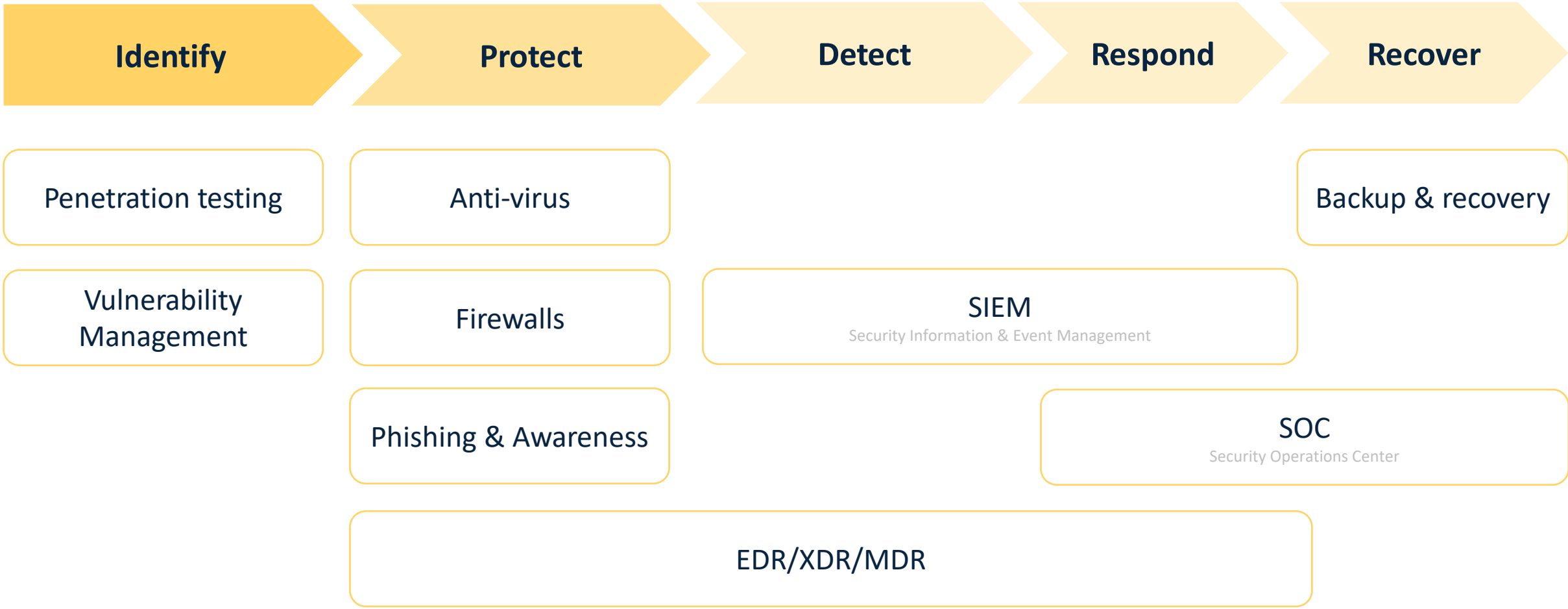
- Production disruptions/ reduced productivity
- Data leakage and lost data
- Violation of regulatory requirements and legislation

Damage

- Damaged brand and trust
- Economic damage
- Risks to life and health

HOLM SECURITY

Lack of proactive cyber defense



Source: NIST Cybersecurity Framework

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

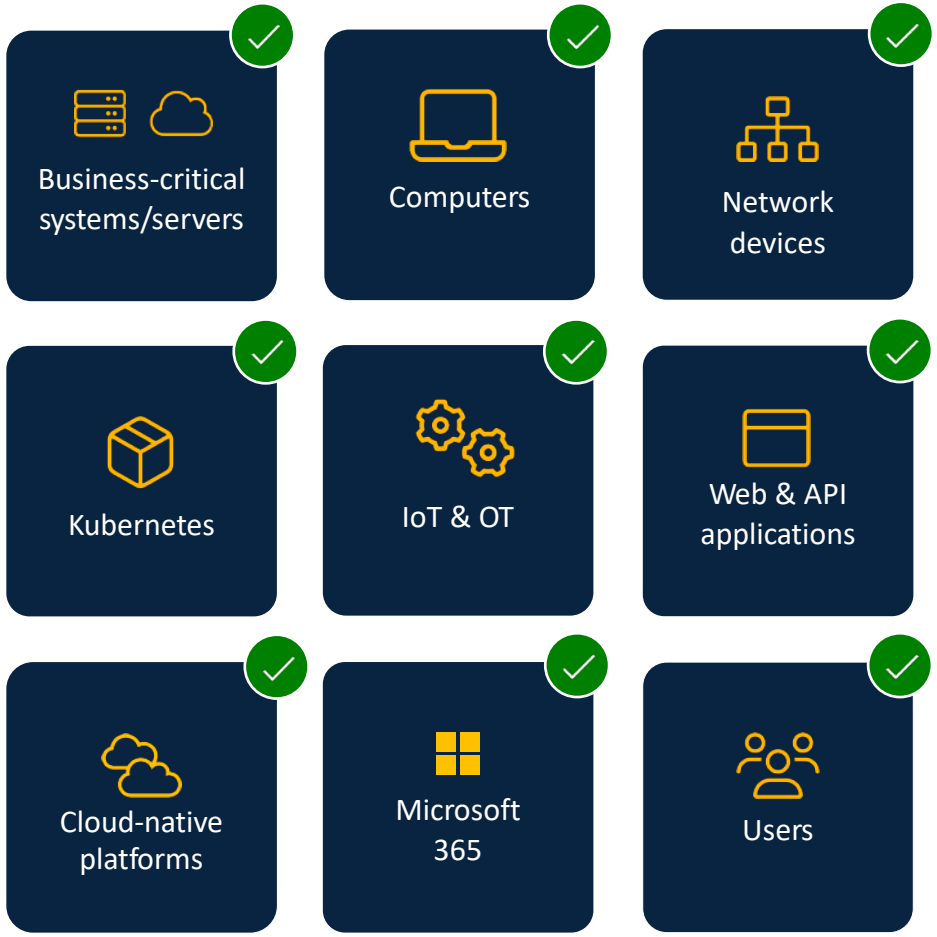
Get the hacker's perspective

How secure is your organization if cybercriminals actively try to hack into your systems, target you with a phishing attack, or try to spread ransomware?

HOLM SECURITY

Protects all important attack vectors

Our all-in-one platform detects vulnerabilities in all critical attack vectors - including unmanaged systems.



Integrated & automated Attack Surface Management

Integrated Attack Surface Management (ASM) and External Attack Surface Management (EASM) for asset discovery and monitoring of asset changes in systems, web, domains, and cloud-native platforms.

HOLM SECURITY

1

Platform
Workflow
Risk model

→

Time-efficient
Cost effective
Stronger cyber defense

OTD BİLİŞİM
GLOBAL VAD

Perfect preparation for future efforts

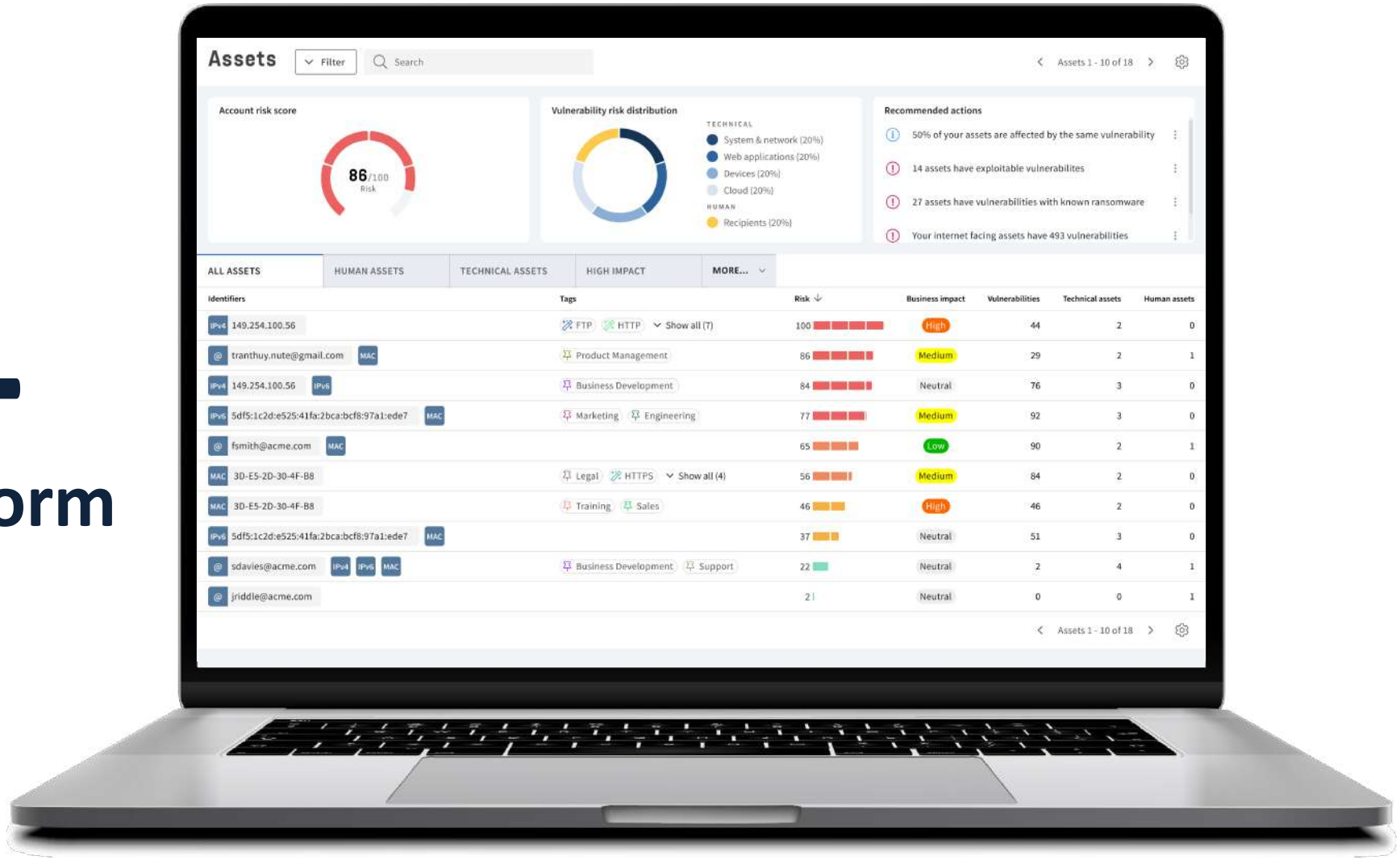
Makes other cyber security efforts, such as penetration testing and implementation of a SOC, time- and cost effective.

HOLM SECURITY

TRUE UNIFICATION

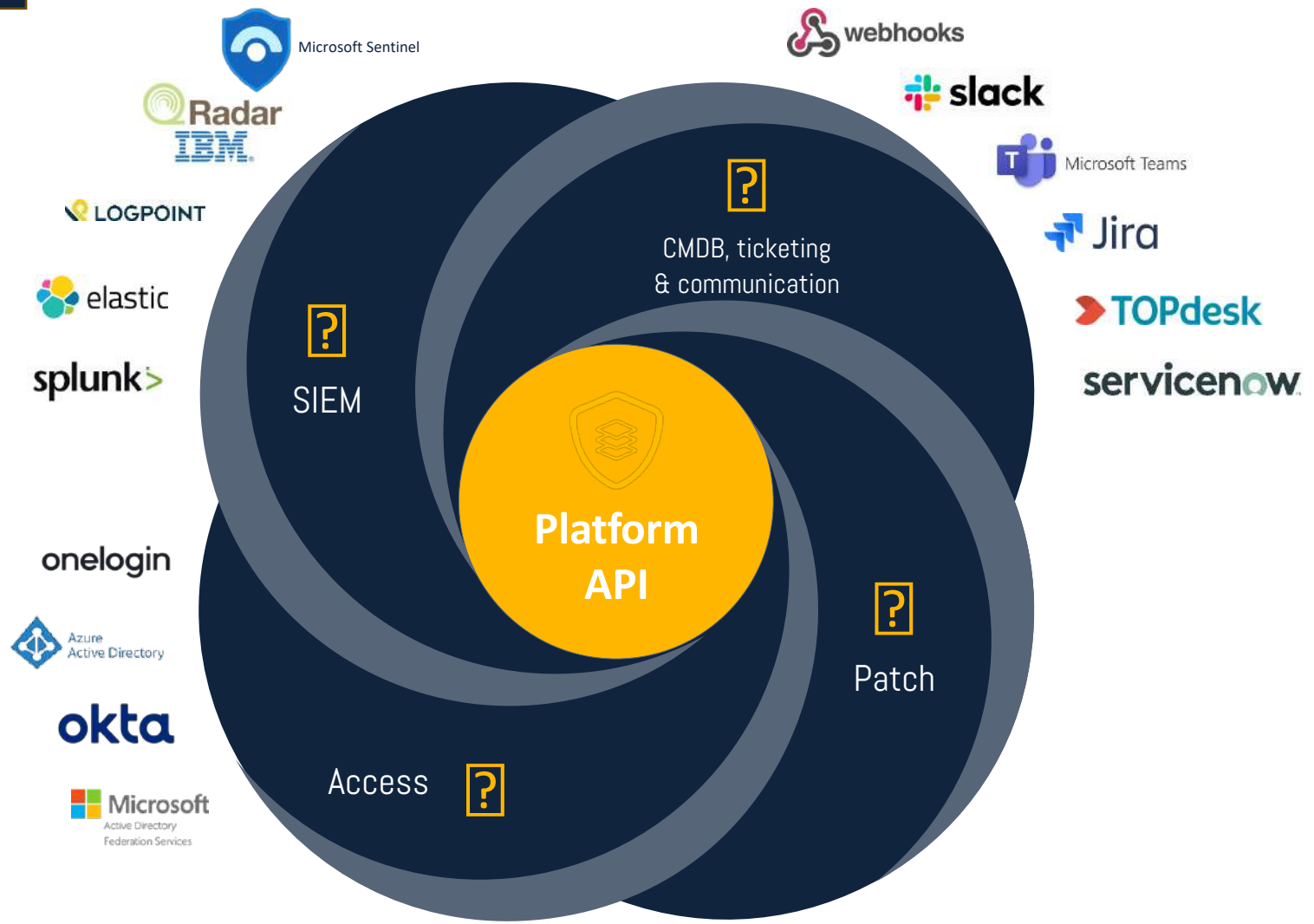
4 → 1

products platform



OTD BİLİŞİM GLOBAL VAD

READY-MADE INTEGRATIONS



PROFESSIONAL SERVICES

Have our experts help you achieve your goals.

Training Center

Success Programs

HOLM SECURITY

Supports your work to meet regulatory demands

A major leap towards a systematic and risk-based cyber defense for compliance with NIS/NIS2, DORA, GDPR, CRA, ISO 27001, among others.

OTD BİLİŞİM
GLOBAL VAD


Do you have the operational capabilities NIS2 requires?
Incident response
Continuity and recovery
Secure system development
Vulnerability Management
Monitoring and testing
Cyber Hygiene and Training
Access Control
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
Enisa recommends vulnerability management for NIS2 compliance.
enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
NIS2
TECHNICAL IMPLEMENTATION GUIDANCE
On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures
JUNE 2025, VERSION 1.0

Source:

HOLM SECURITY

Work together with your outsourcing partner

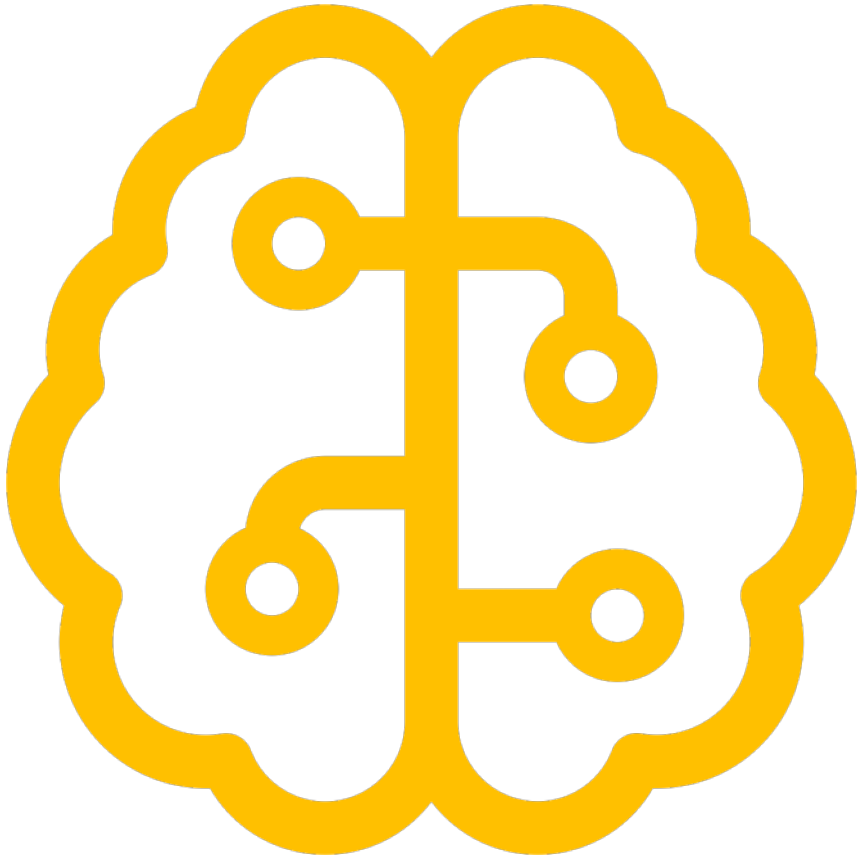
Benchmark your outsourcing partner’s SLA and cooperate to remediate vulnerabilities and reduce risk exposure.

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

AI-driven threat intelligence

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



OTD BİLİŞİM
GLOBAL VAD

Efficiently measure & communicate risk

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

Benchmark risk exposure

Understand your organizations' risk exposure compared to others in the same industry.

HOLM SECURITY

Automation for IT departments of all sizes

A platform that suits smaller organizations as well as larger ones.

Get started in just a couple of hours

Be up and running within hours with agentless implementation.

Professional support every step of the way

Ensuring your vulnerability management program is successfully strengthening your cyber defenses.

OTD BİLİŞİM GLOBAL VAD

Get proactive

Creates a systematic, risk-based, and proactive approach to cyber security.

Established technology
Recognized established technology that provides value for your organization.

All-in-one platform
Covers all important attack vectors – one workflow, and one risk model.

Automated
Automated platform adding minimal workload to your team.

Supports compliance
An important component in meeting existing and upcoming regulatory demands.

Measure, compare & report
Effectively measure, report internally, and compare how secure your organization is compared to others.

Expert support
Our expert support ensures progress and a worthwhile investment.

Get started instantly
Get started in just a couple of hours with instant results.

A perfect preparation
Makes other cyber security efforts more efficient and cost effective.

A reliable partner
A European supplier for the highest level of security, data privacy, and reliability.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Next-Gen Vulnerability Management

CERTIFIED ISO 27001 SVENSK CERTIFIERING
NIS2 Directive Compliant
MADE IN EUROPE Stability — Reliability — Unity

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Next-Gen Vulnerability Management

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Next-Gen Vulnerability Management

CERTIFIED ISO 27001 SVENSK CERTIFIERING
NIS2 Directive Compliant
MADE IN EUROPE Stability — Reliability — Unity

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

Finance, insurance & banking

Medtech & healthcare

Government agencies

Critical infrastructure

Food & beverage production

Manufacturing & production

Next-Gen Vulnerability Management

Minimize your attack surface

Monitor and minimize your attack surface and find blank spots.

All attack vectors in one place

A complete solution that finds risks in all important attack vectors.

All risks in one place with true unification

A single pane of glass with all risks for efficient prioritization and remediation.

AI-driven threat intelligence

AI for faster and broader coverage of risks, and data enrichment for better risk prioritization.

HOLM SECURITY

Next-Gen Vulnerability Management Platform

Attack surface

External Attack Surface (EASM)

Third party (suppliers)

Attack vectors

- Business-critical systems /servers
- Computers & office equipment
- Network devices
- IoT
- Kubernetes
- OT
- Web apps
- APIs
- Cloud-native platforms
- Microsoft 365
- Users

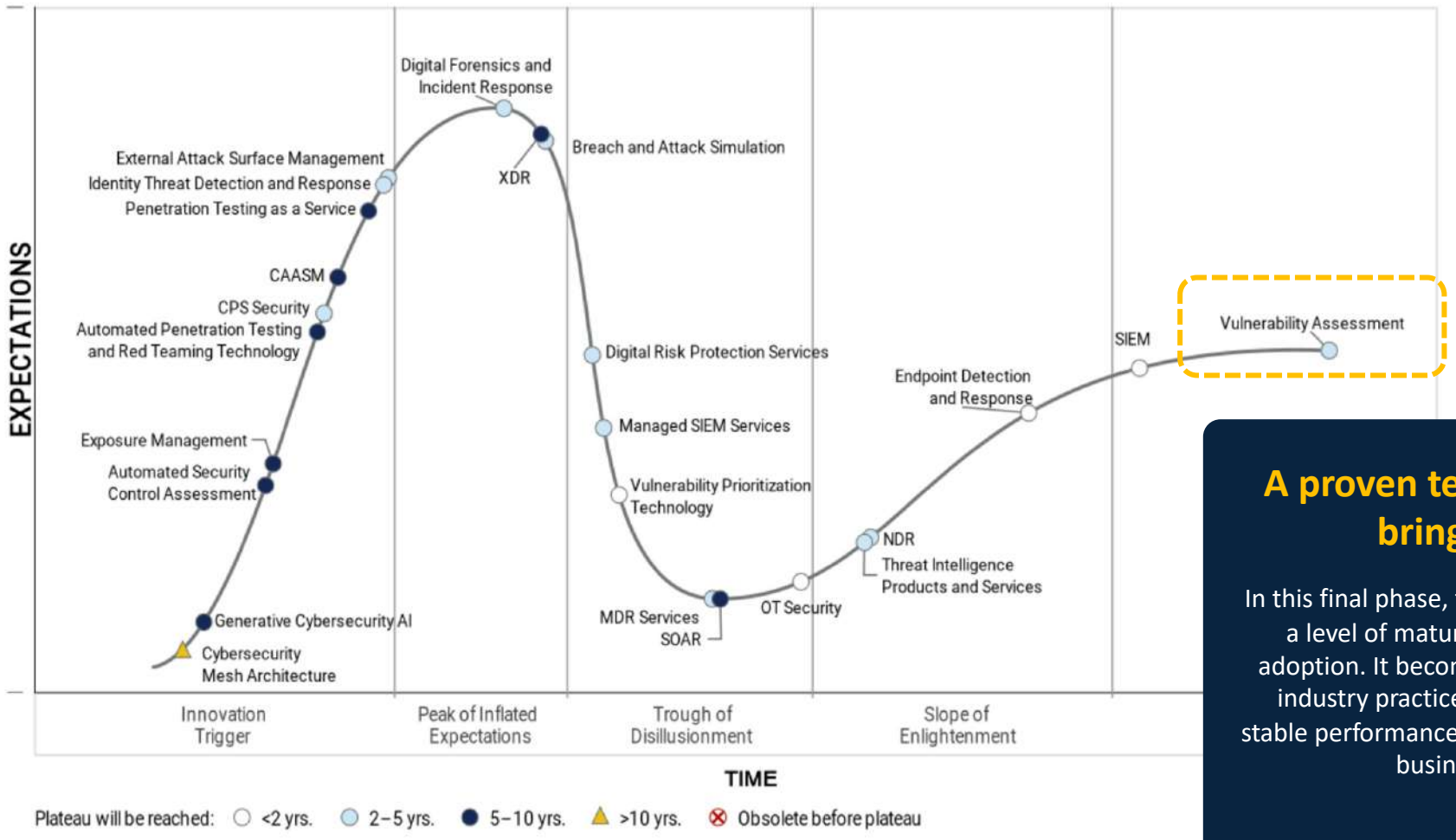
Products

- System & Network Security
- Web Application Security
- API Security
- Cloud Security
- Phishing Simulation & Awareness Training

Gartner

HOLM SECURITY

Hype Cycle for Security Operations, 2023



A proven technology that brings value

In this final phase, the technology reaches a level of maturity and widespread adoption. It becomes an integral part of industry practices and demonstrates stable performance, delivering measurable business value.

Gartner

Gartner

HOLM SECURITY

Holm Security VMP Reviews

by Holm Security in Vulnerability Assessment

4.4 ★★★★½ 42 Ratings

5.0 ★★★★★ Aug 4, 2021

Easy to use, capable, and constantly improved Vulnerability Management platform

Reviewer Function: IT Security and Risk Management | Company Size: 50M - 250M USD | Industry: Manufacturing Industry

The Holm Security platform is a great fit for our organisation and has helped us to better control vulnerabilities and phishing awareness. Premium support is a valuable addition for us, because it enabled us to reduce some of the work required to set up and improve the platform.

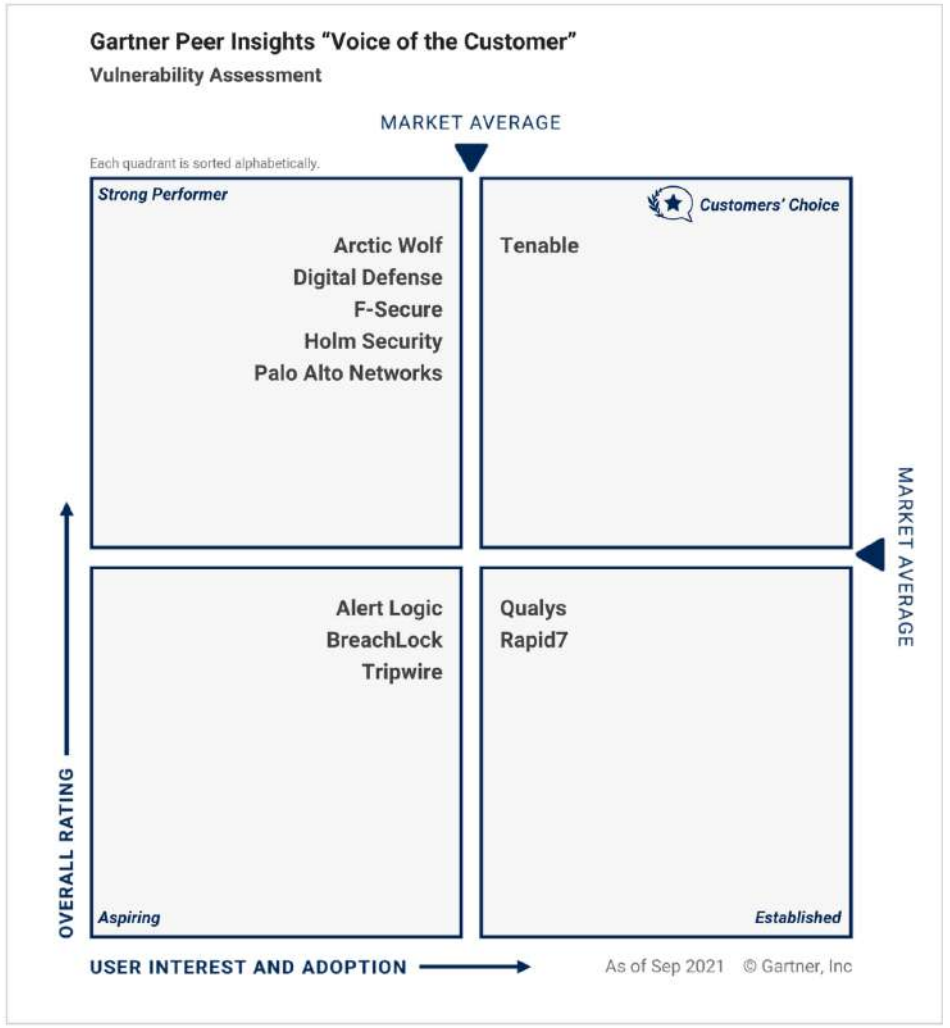
5.0 ★★★★★ Jun 7, 2022

Helps to learn about potential threats .

Reviewer Role: Analyst | Company Size: 30B + USD | Industry: Finance Industry

Holm security offers security with genuine information into dangers then they react quickly and resist their growth. It also equips staff with the knowledge to spot and respond to assaults when they occur. The whole platform is self contained by saving time.

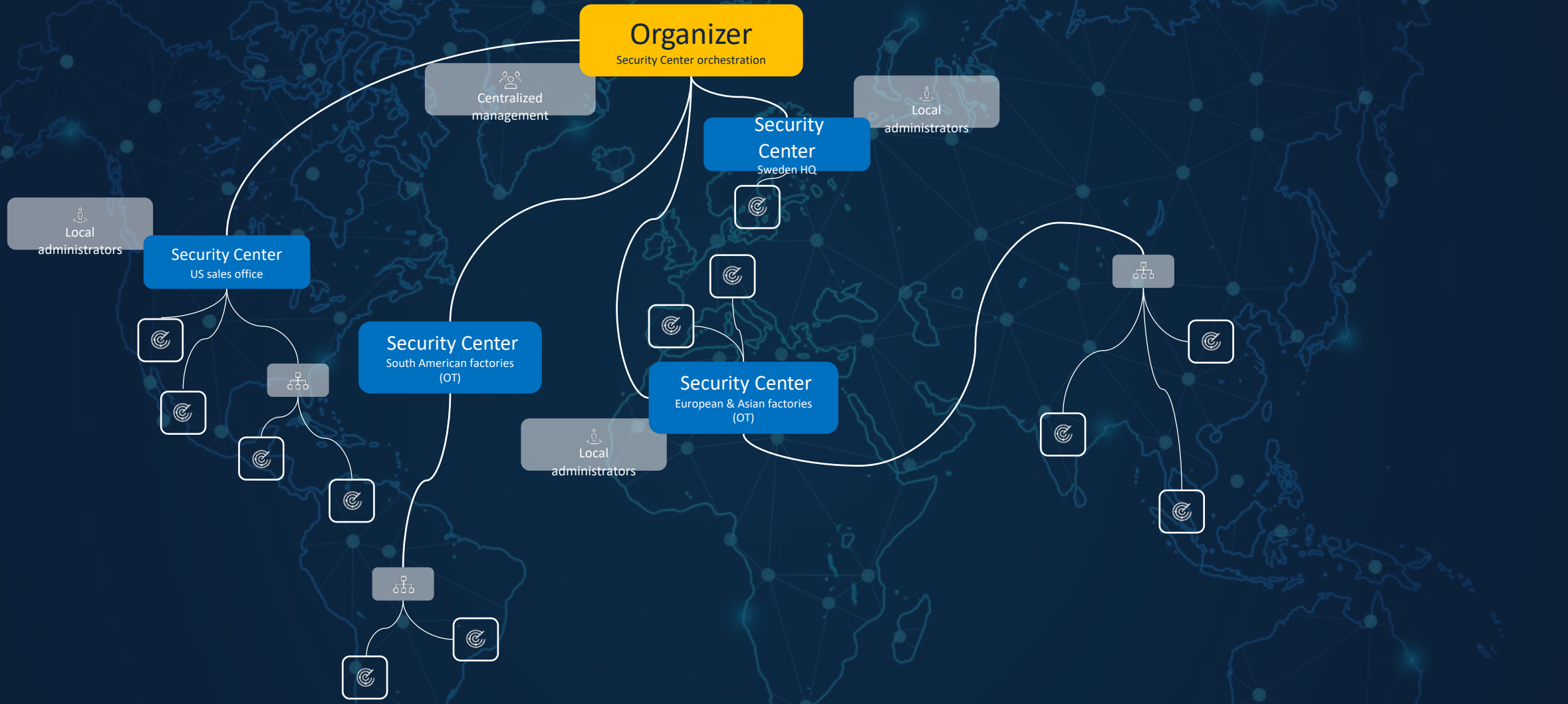
Click here to read more reviews at the Gartner Peer Insight website



Gartner

OTD BİLİŞİM GLOBAL VAD

EXAMPLE: ENTERPRISE SETUP



Local scanners & data collectors

Local proxy

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Cloud VMP

PREPARATION CHECKLIST

HOLM SECURITY

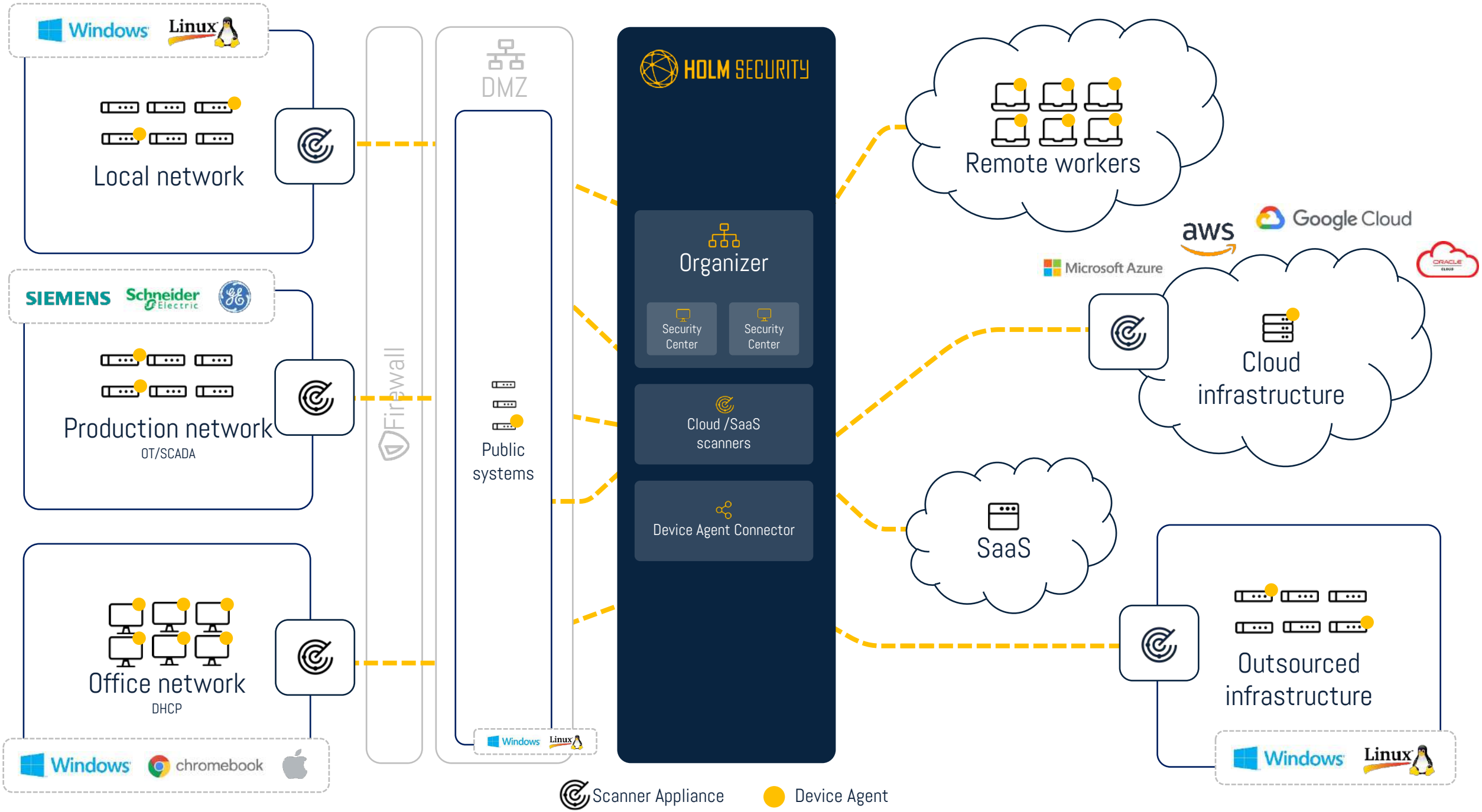
Customer

- **Virtualization Platform**
  - VM ESXi, VM Workstation, VM Player, Oracle VirtualBox, KVM, etc for Virtual Scanner Appliance
- **Images Download**
  - Virtual Scanner Appliance
- **Networking**
  - Edge Firewall Policy (Outbound)
  - Internal Firewall Policy (Between Core Engine and Virtual Scanner Appliance), if any
  - Private static IP for Virtual Scanner Appliance

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Architecture

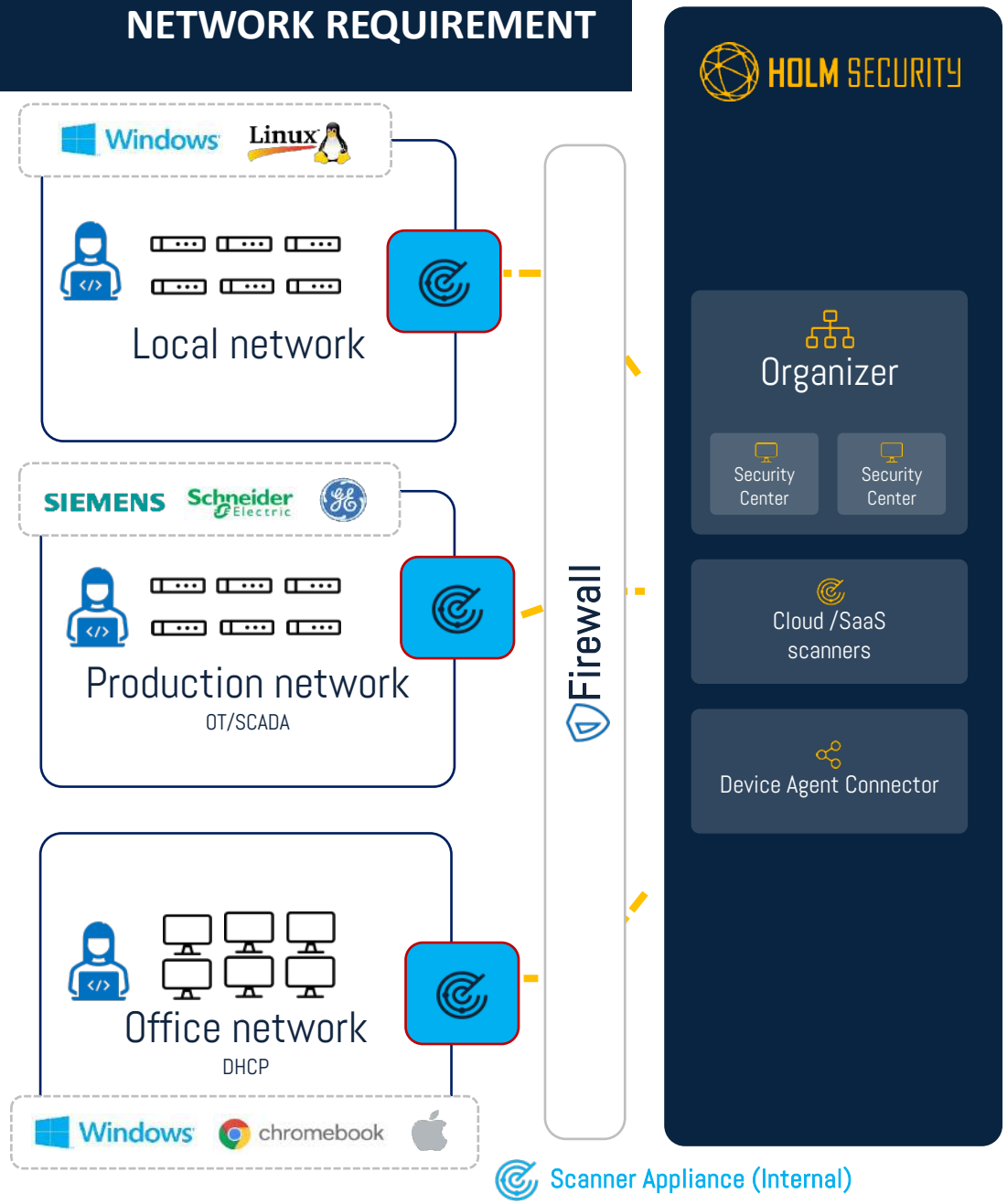

Windows
Linux
Local network
SIEMENS
Schneider Electric
Production network
OT/SCADA
Office network
DHCP
Windows
chromebook
Firewall
DMZ
Public systems
Windows
Linux
HOLM SECURITY
Organizer
Security Center
Security Center
Cloud /SaaS scanners
Device Agent Connector
Remote workers
aws
Google Cloud
Microsoft Azure
Cloud infrastructure
SaaS
Outsourced infrastructure
Windows
Linux
Scanner Appliance
Device Agent

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Network Requirement

NETWORK REQUIREMENT



- The virtual Scanner Appliance is to connect to the Holm Security with the following outgoing TCP Ports via internal firewall policy: -
  - TCP Port: 443 and 8022
  - IPv4: 185.163.84.0/22

If a /22 network is too extensive to grant access to, please use the following: 185.163.84.0/24 and 185.163.85.0/24

Link: https://support.holmsecurity.com/knowledge/what-are-the-firewall-settings-for-scanner-appliance

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Images Download

IMAGES DOWNLOAD: DIRECT

HOLM SECURITY

Virtual Scanner Appliance

OVA

https://swift-kna1.citycloud.com/swift/v1/AUTH_b86ff371e25f443fb8161f2f56143a3f/scanner-appliance/ova_public_3-19-2_07137bb1.ova?temp_url_sig=86486711088d7209fea60c14894ea96ae20f76bb&temp_url_expires=2078138795

Hyper-V

https://swift-kna1.citycloud.com/swift/v1/AUTH_b86ff371e25f443fb8161f2f56143a3f/scanner-appliance/vhdx_public_3-19-2_07137bb1.vhdx.gz?temp_url_sig=54a51a17d366dd753a4e73c4ba8d5328b9b9e645&temp_url_expires=2078139685

Note: Inform your representative if the links above has expired

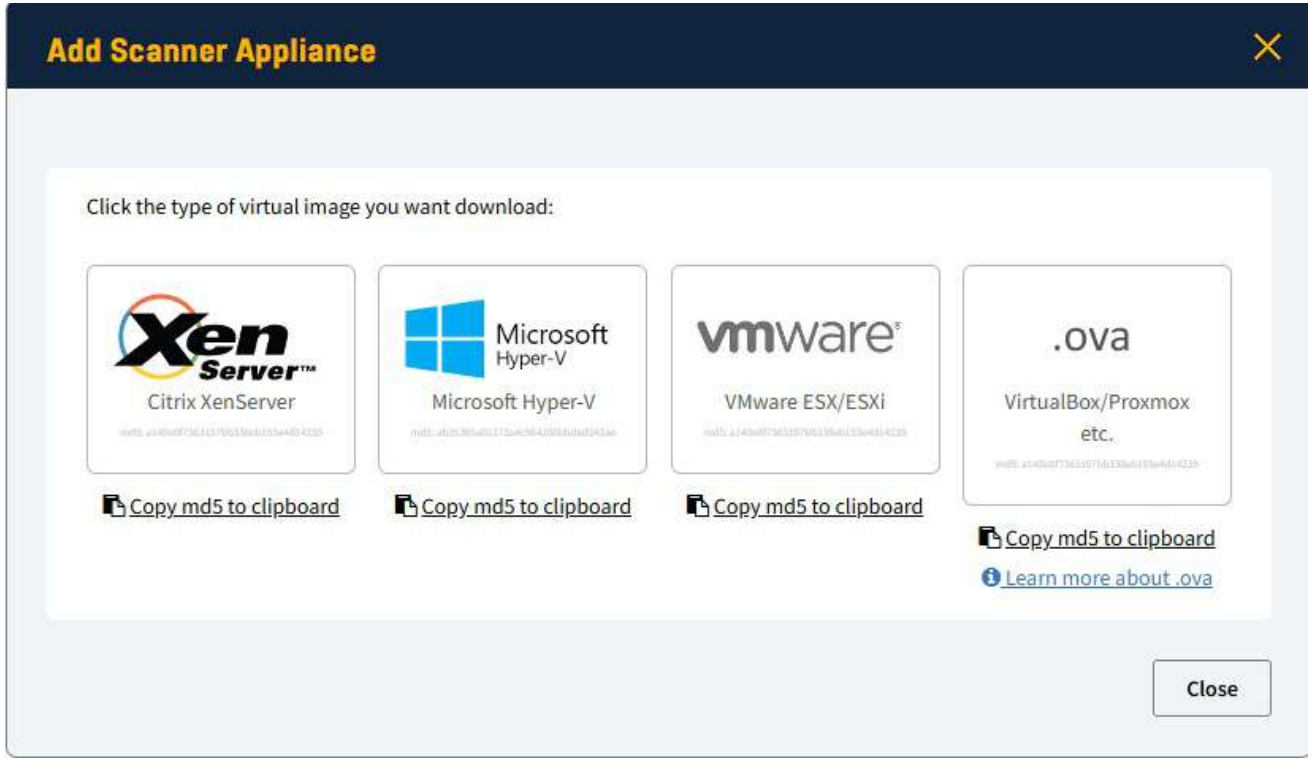
Link: https://support.holmsecurity.com/knowledge/what-are-the-system-requirements-for-the-scanner-appliance

IMAGES DOWNLOAD: SECURITY CENTER

HOLM SECURITY

Virtual Scanner Appliance

VMware ESXi™
VirtualBox
Xen Server™
vmware Workstation
PROXMOX
KVM
Microsoft Hyper-V
Microsoft Hyper-V



Link: https://support.holmsecurity.com/knowledge/which-virtualization-platforms-does-the-general-ova-image-support

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

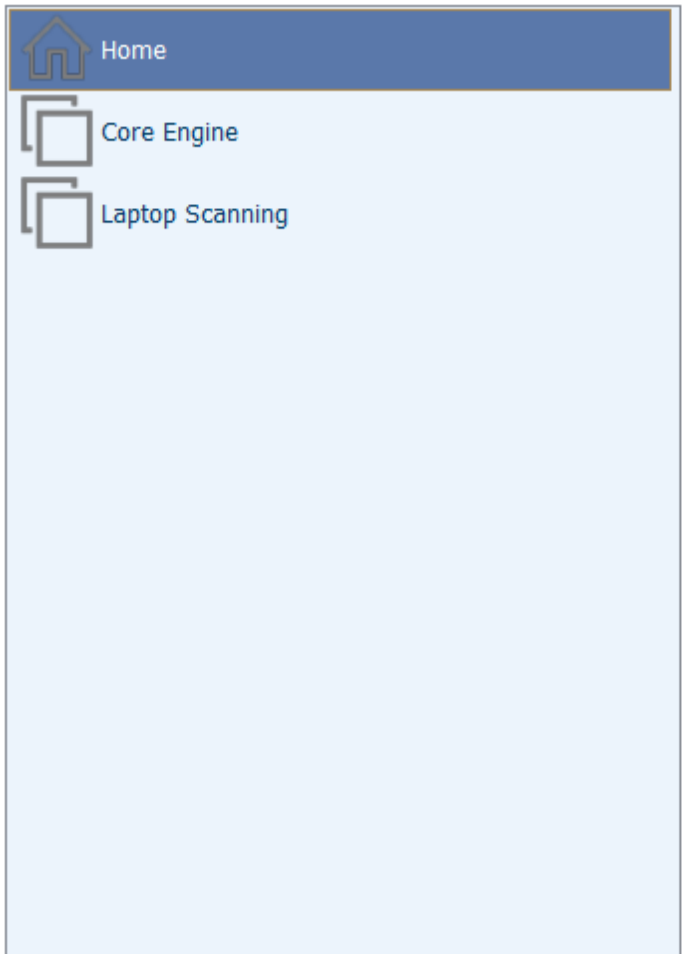
Deployment

SCANNER APPLIANCE: IMPORT

Link: https://support.holmsecurity.com/knowledge/how-do-i-install-a-scanner-appliance-1

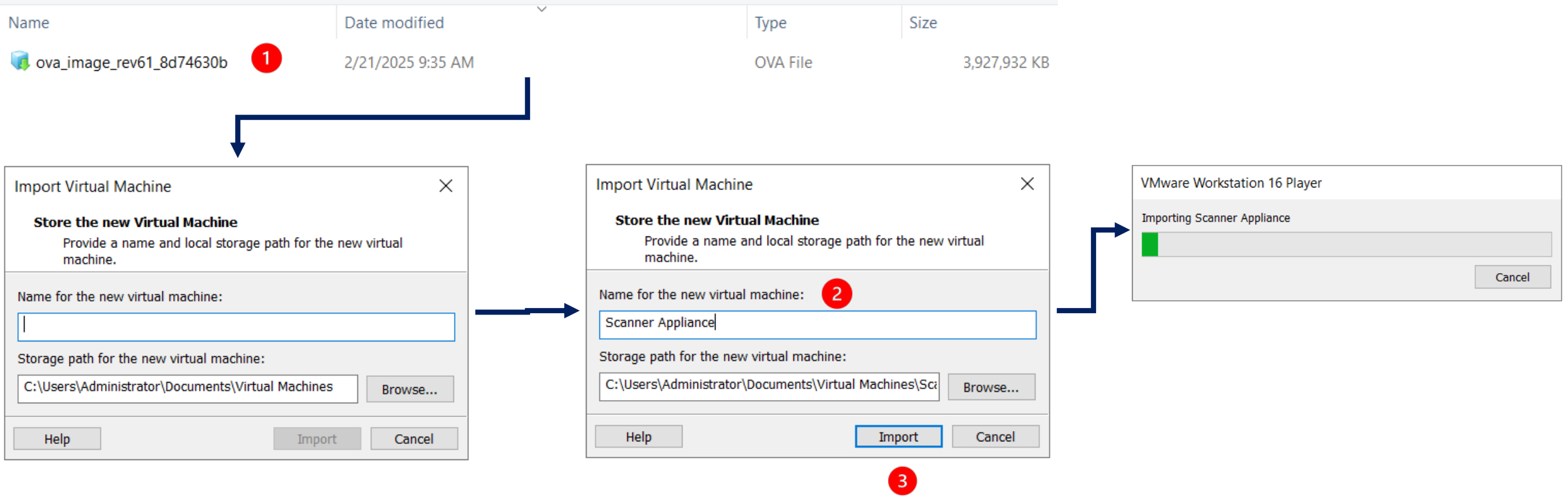
Virtual Scanner Appliance

Note: Simulating an import process of the Core Engine image using VMWare Workstation Player 16



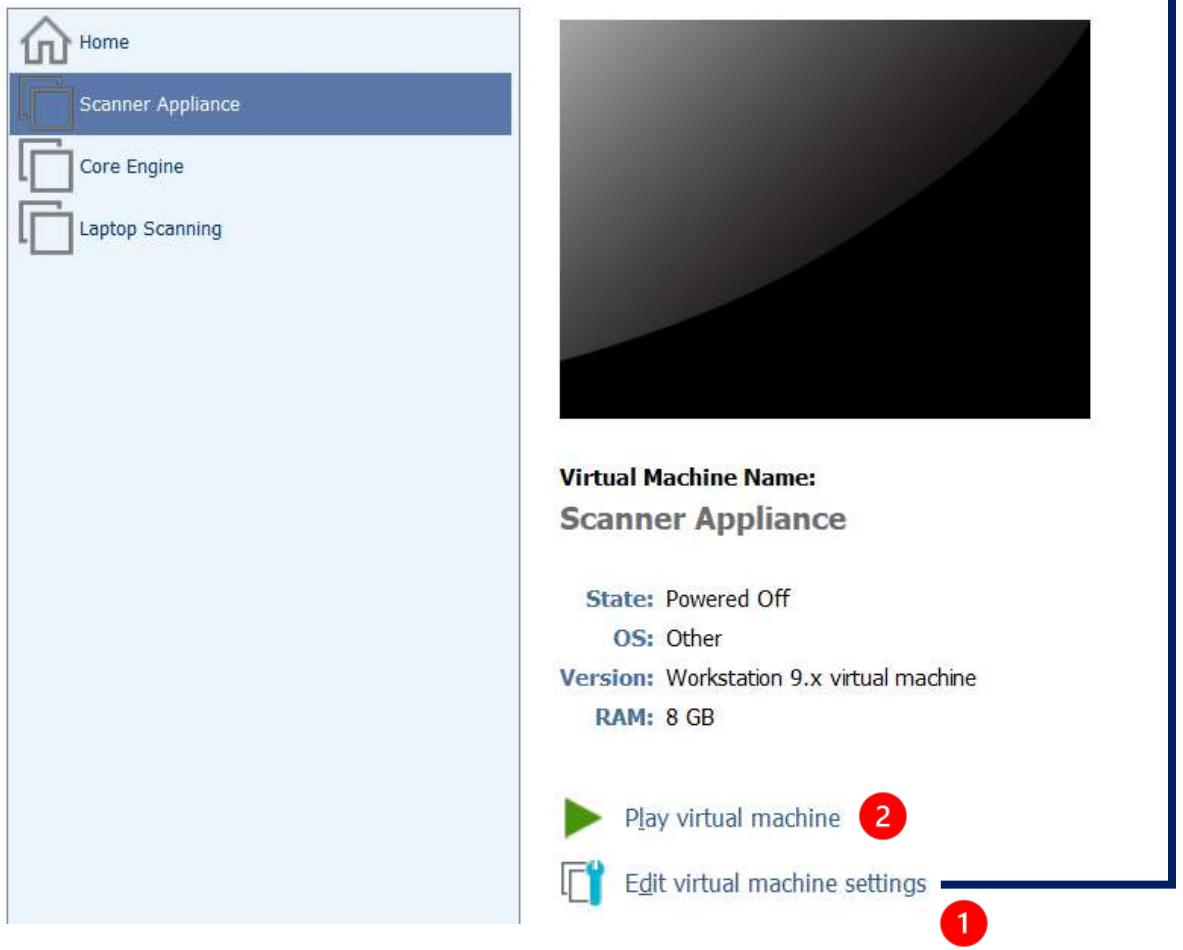
Open a Virtual Machine

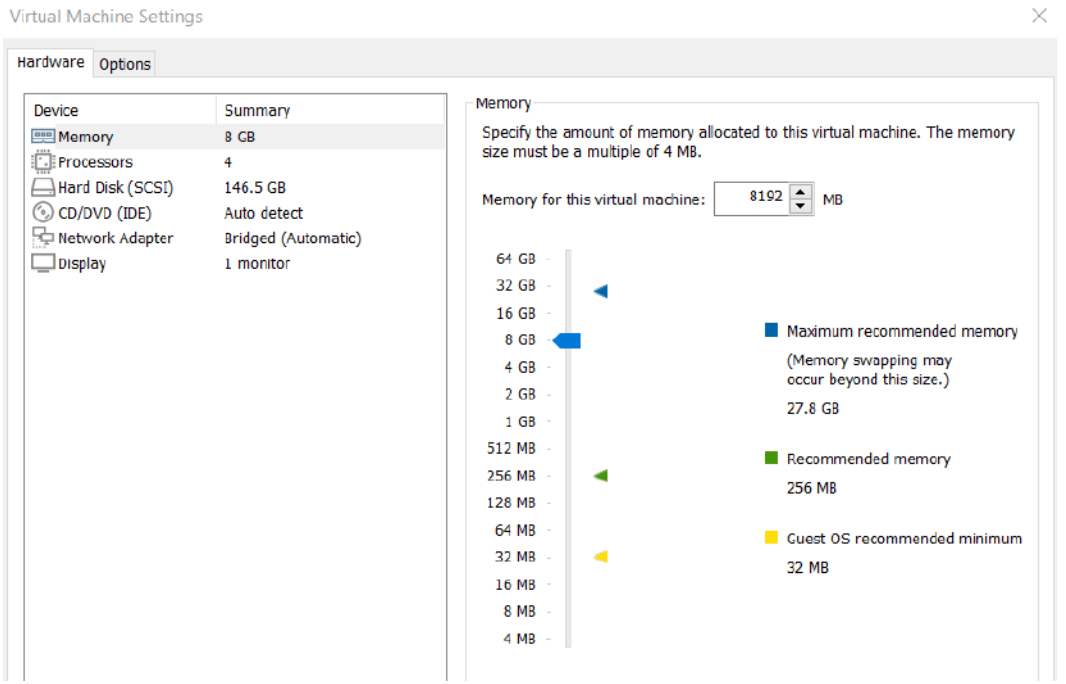
SCANNER APPLIANCE: IMPORT



Importing Image

SCANNER APPLIANCE: RESOURCES



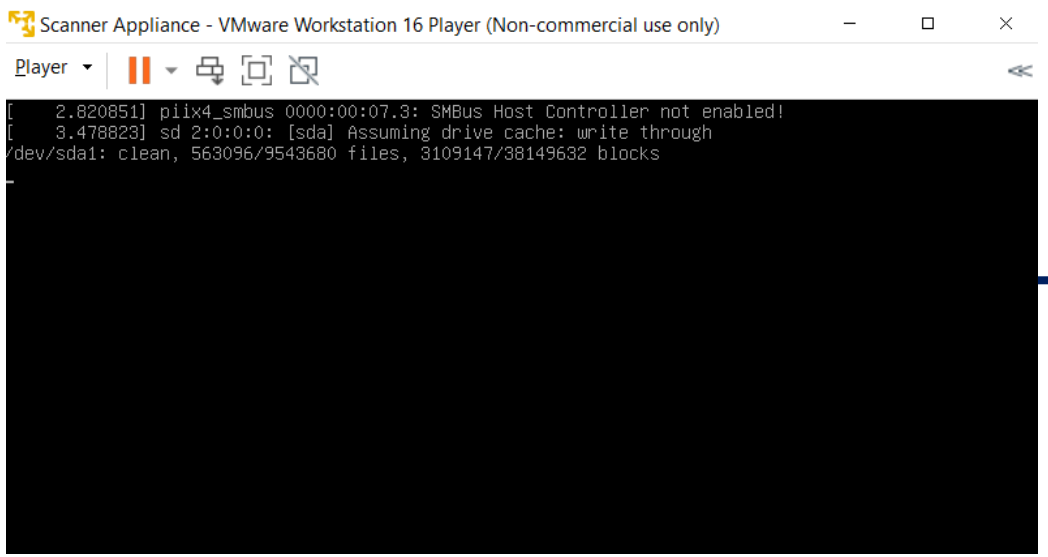


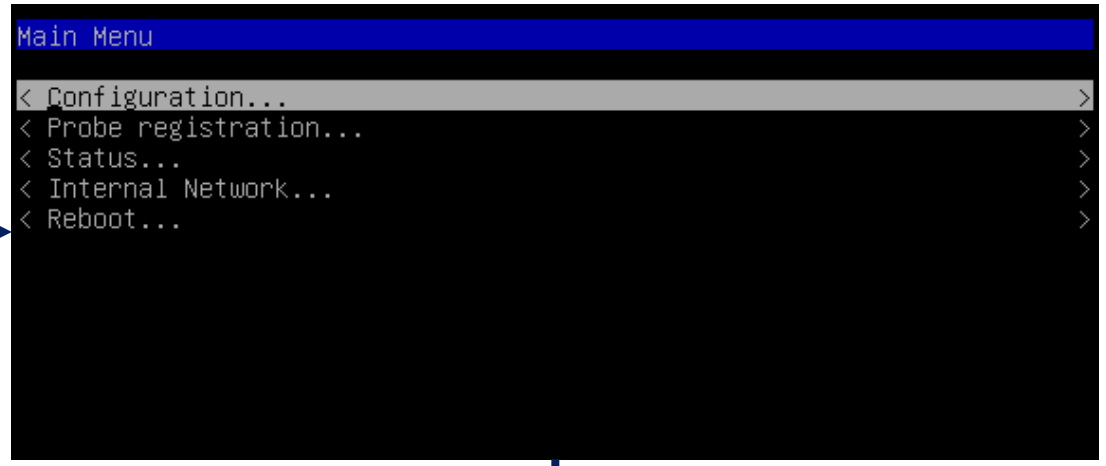
Ensure the Network Adapter selection is valid

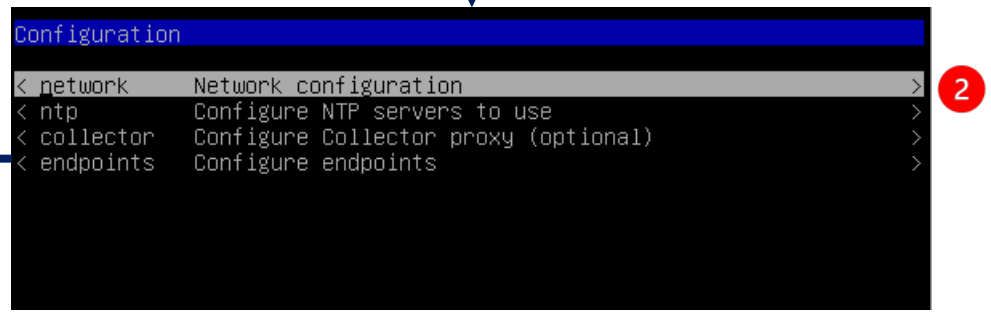
Virtualization resources check

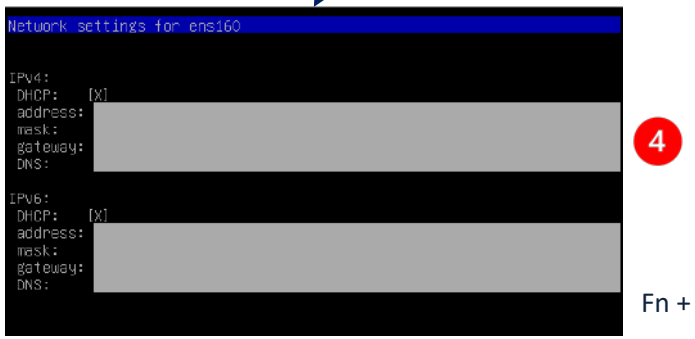
SCANNER APPLIANCE:
IP SETUP

HOLM SECURITY







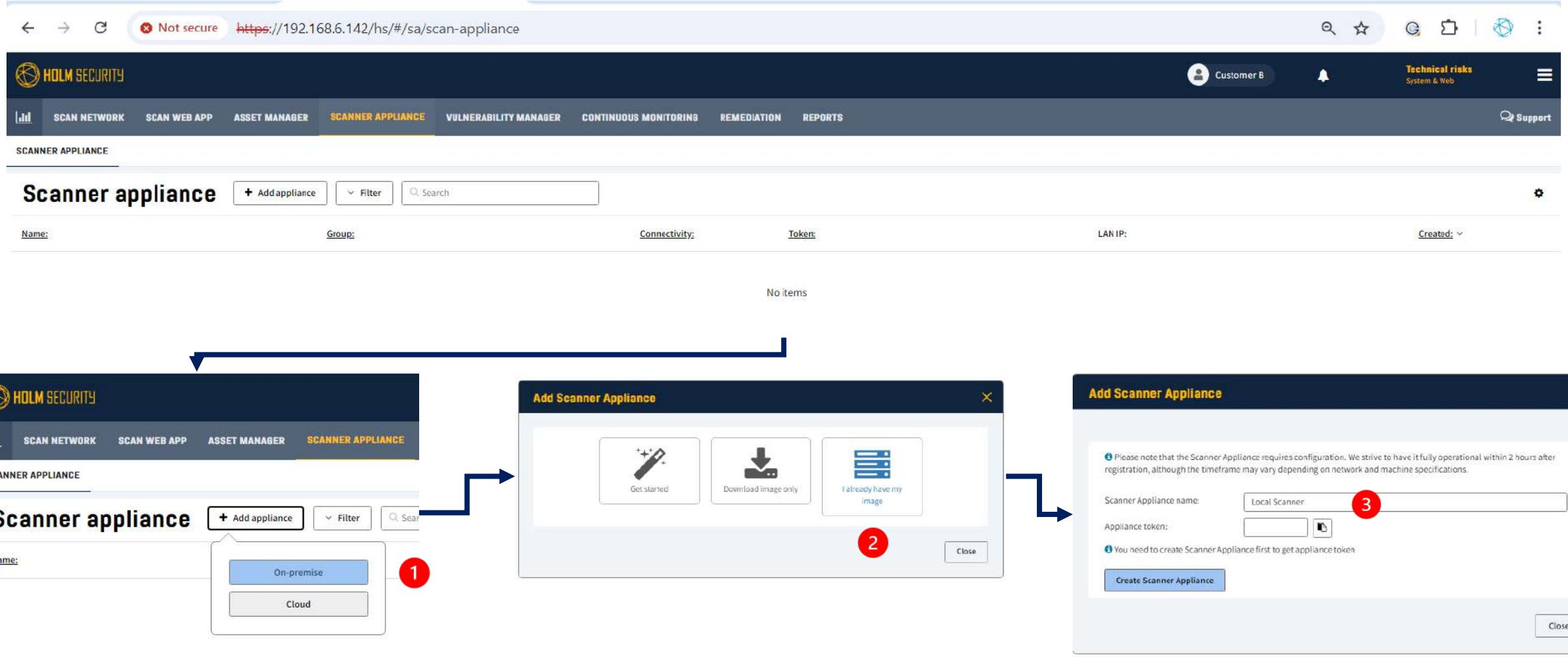


Fn + F11 to Save

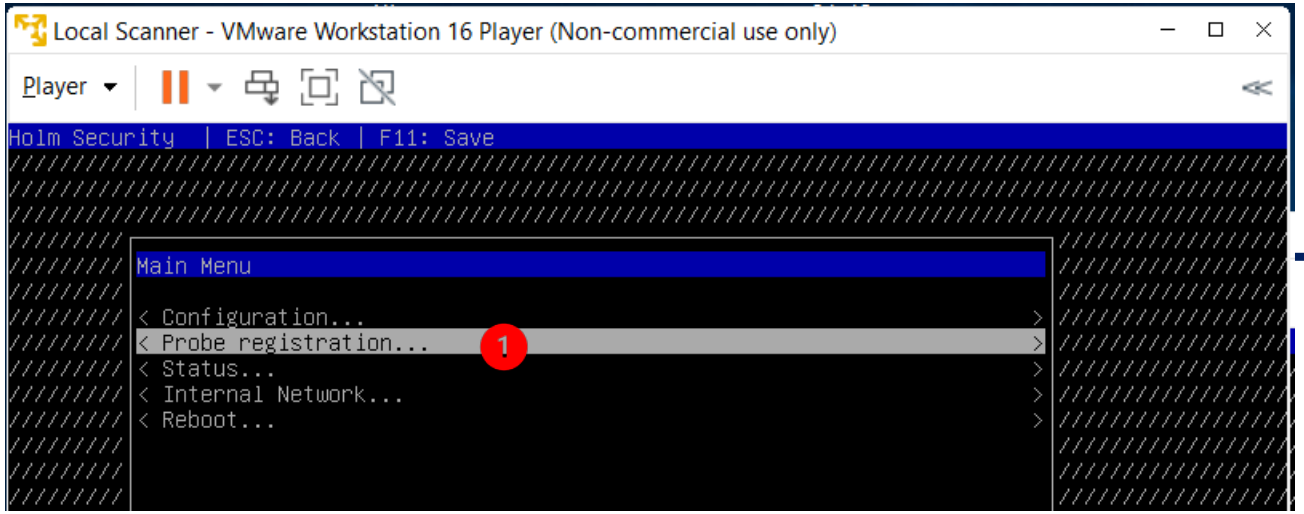
Note: This simulation is based on DHCP for the IP

SECURITY CENTER:
TOKEN KEY CREATION

- You need to generate the Scanner Appliance's token key for the Probe Registration



SCANNER APPLIANCE:
PROBE REGISTRATION



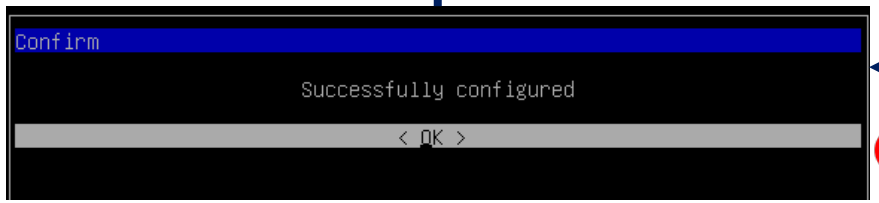
2

Enter the Token Key

3

4

5



6

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

On-Premise VMP

HOLM SECURITY

Next-Gen Vulnerability Management Platform

Attack surface

External Attack Surface (EASM)

Third party (suppliers)

Attack vectors

- Business-critical systems /servers
- Computers & office equipment
- Network devices
- IoT
- Kubernetes
- OT
- Web apps
- APIs
- Cloud-native platforms
- Microsoft 365
- Users

Products

- System & Network Security
- Web Application Security
- API Security
- Cloud Security
- Phishing Simulation & Awareness Training

PREPARATION CHECKLIST

HOLM SECURITY

Customer

- **Virtualization Platform**
  - VM ESXi for Core Engine (or VMWare Workstation, if you are on demo purposes)
  - VM ESXi, VM Workstation, VM Player, Oracle VirtualBox, KVM, etc for Scanner Appliance

- **Images Download**
  - Core Engine
  - Virtual Scanner Appliance

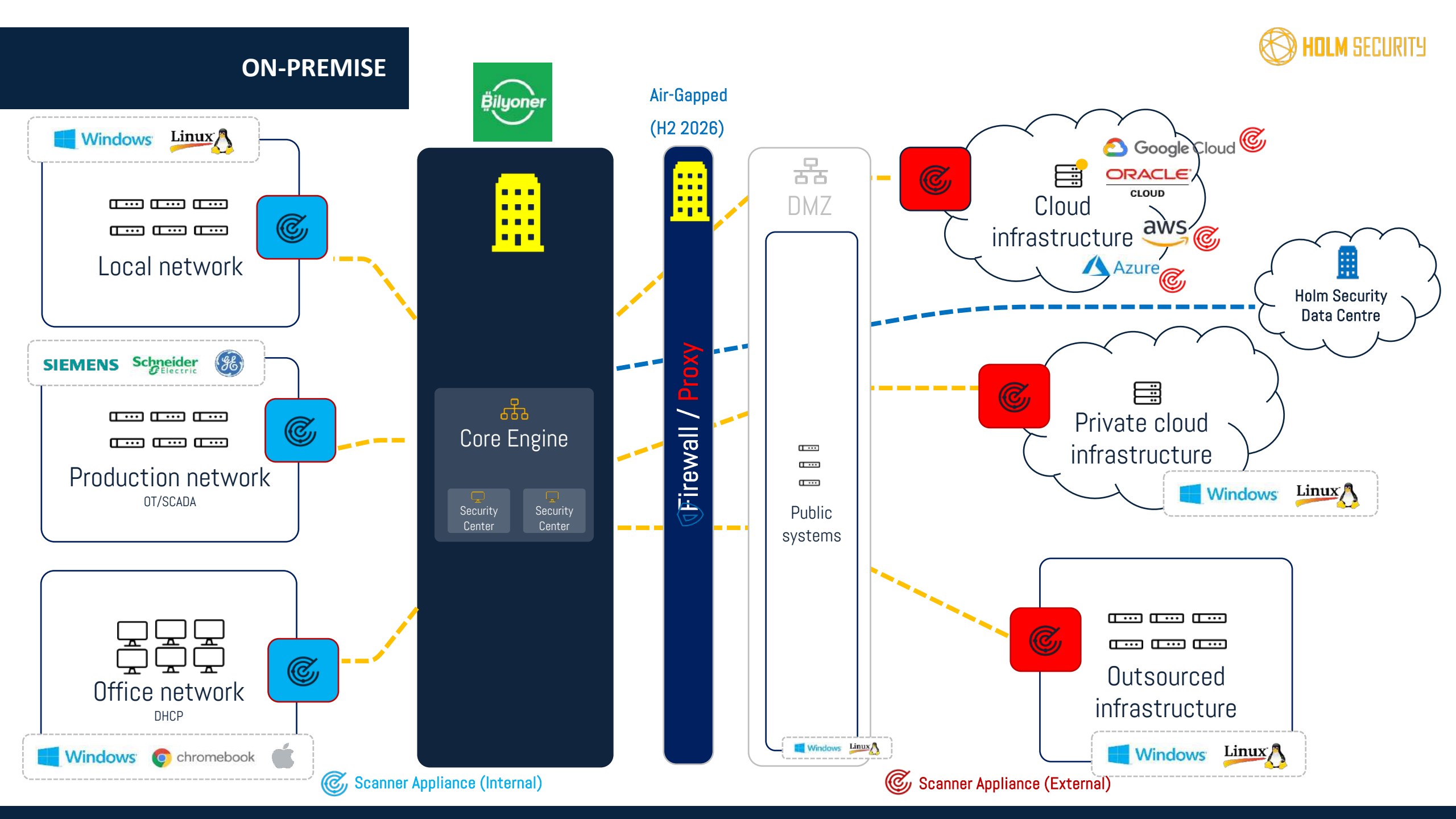
- **Networking**
  - Edge Firewall Policy (Outbound)
  - Internal Firewall Policy (Between Core Engine and Virtual Scanner Appliance), if any
  - Private static IP for Core Engine and Virtual Scanner Appliance

OTD BİLİŞİM
GLOBAL VAD

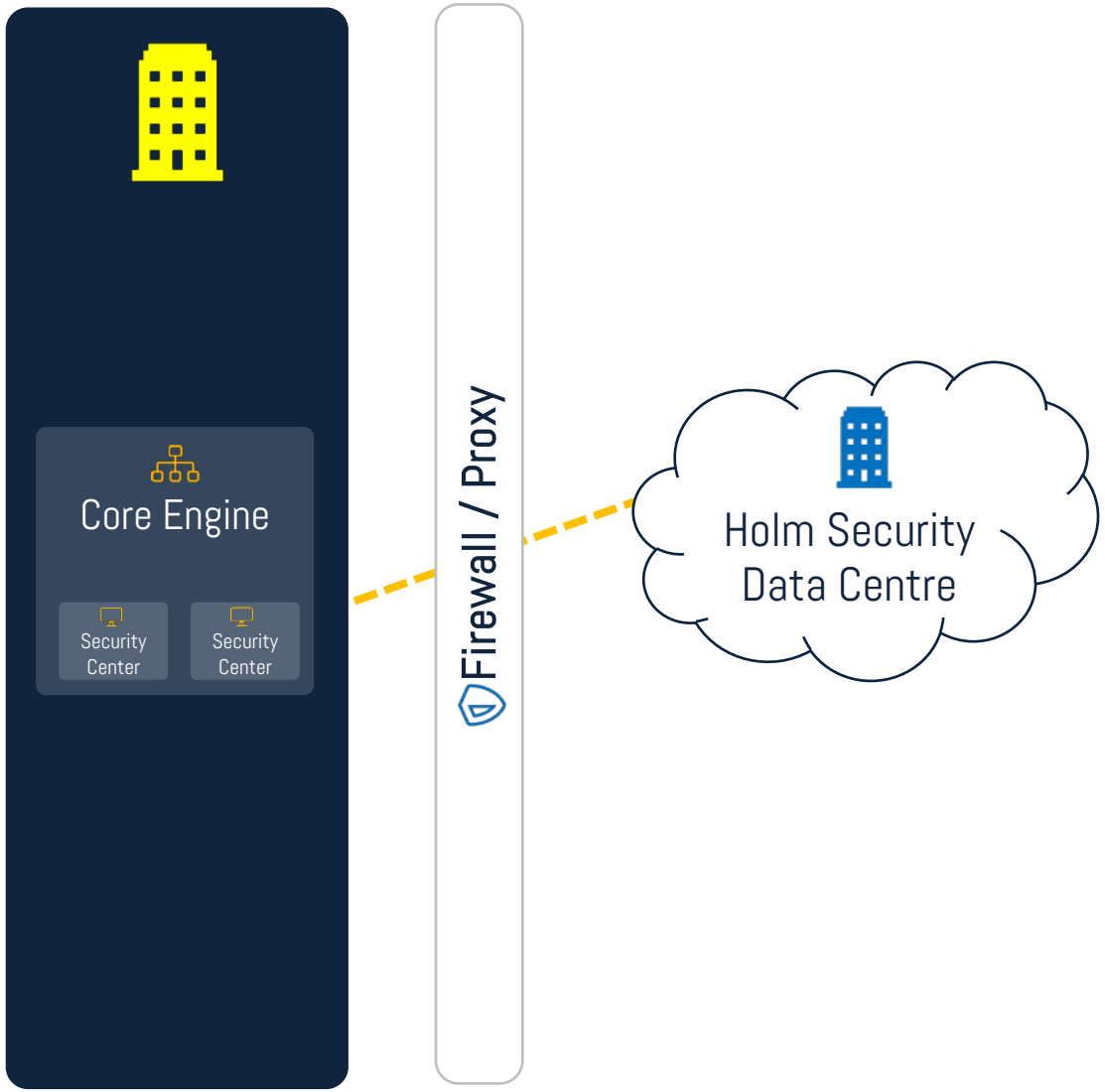
HOLM SECURITY

Architecture

ON-PREMISE

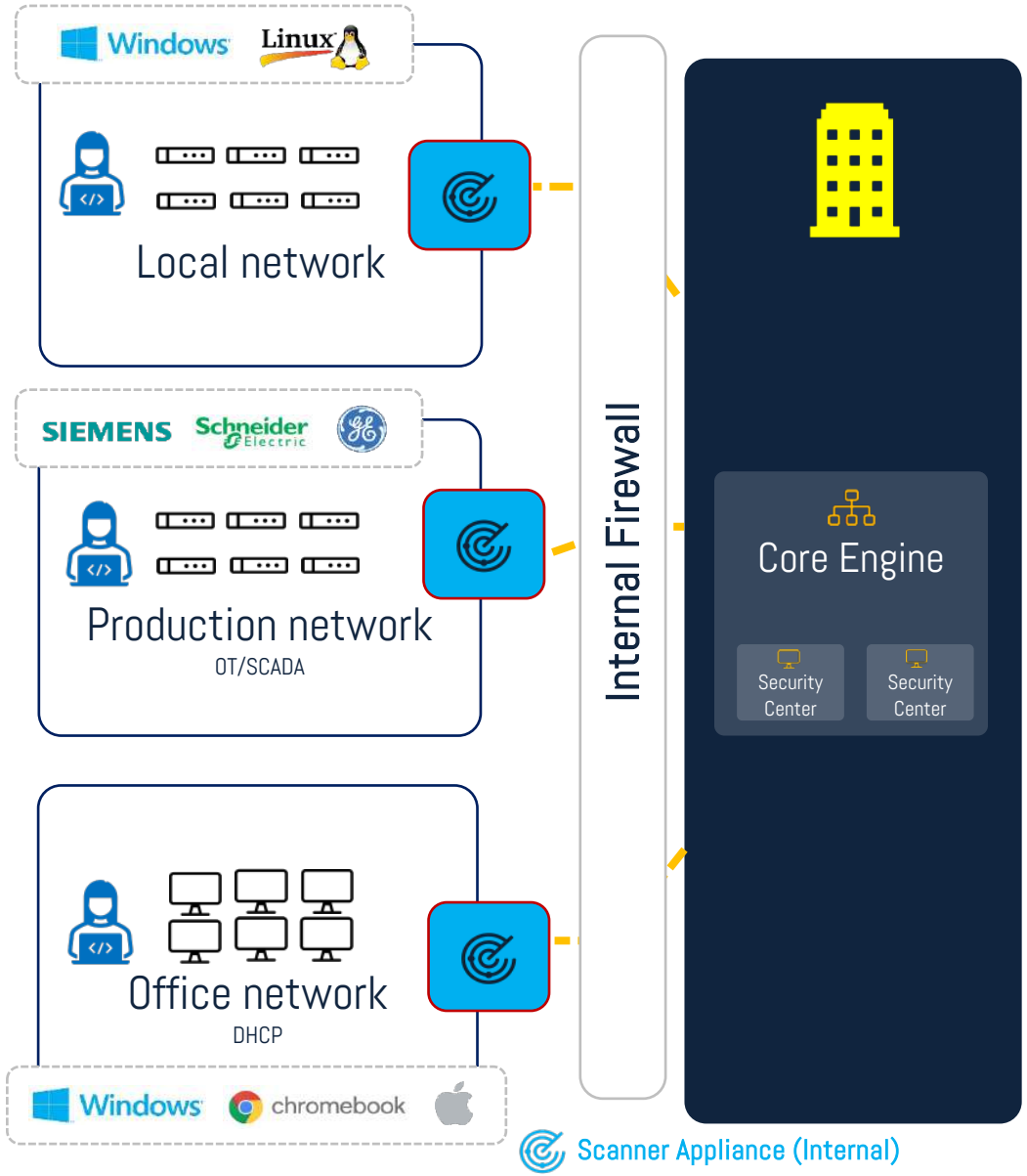

Bilyoner
Air-Gapped
(H2 2026)
Windows
Linux
Local network
SIEMENS
Schneider Electric
Production network
OT/SCADA
Office network
DHCP
Windows
chromebook
Core Engine
Security Center
Security Center
Firewall / Proxy
DMZ
Public systems
Windows
Linux
Google Cloud
ORACLE CLOUD
Cloud infrastructure
aws
Azure
Holm Security Data Centre
Private cloud infrastructure
Windows
Linux
Outsourced infrastructure
Windows
Linux
Scanner Appliance (Internal)
Scanner Appliance (External)

CORE ENGINE



- F/W - outbound rule to allow Core Engine to be connected to Holm Security DC for software patches and vulnerability database updates: -
  - TCP: 443 and 8022
  - IPv4: 185.163.84.0/22 **or** IPv6: 2a0b:6800::/29
  - NTP: UDP 123
  - DNS: TCP/UDP 53

ON-PREMISE: INTERNAL

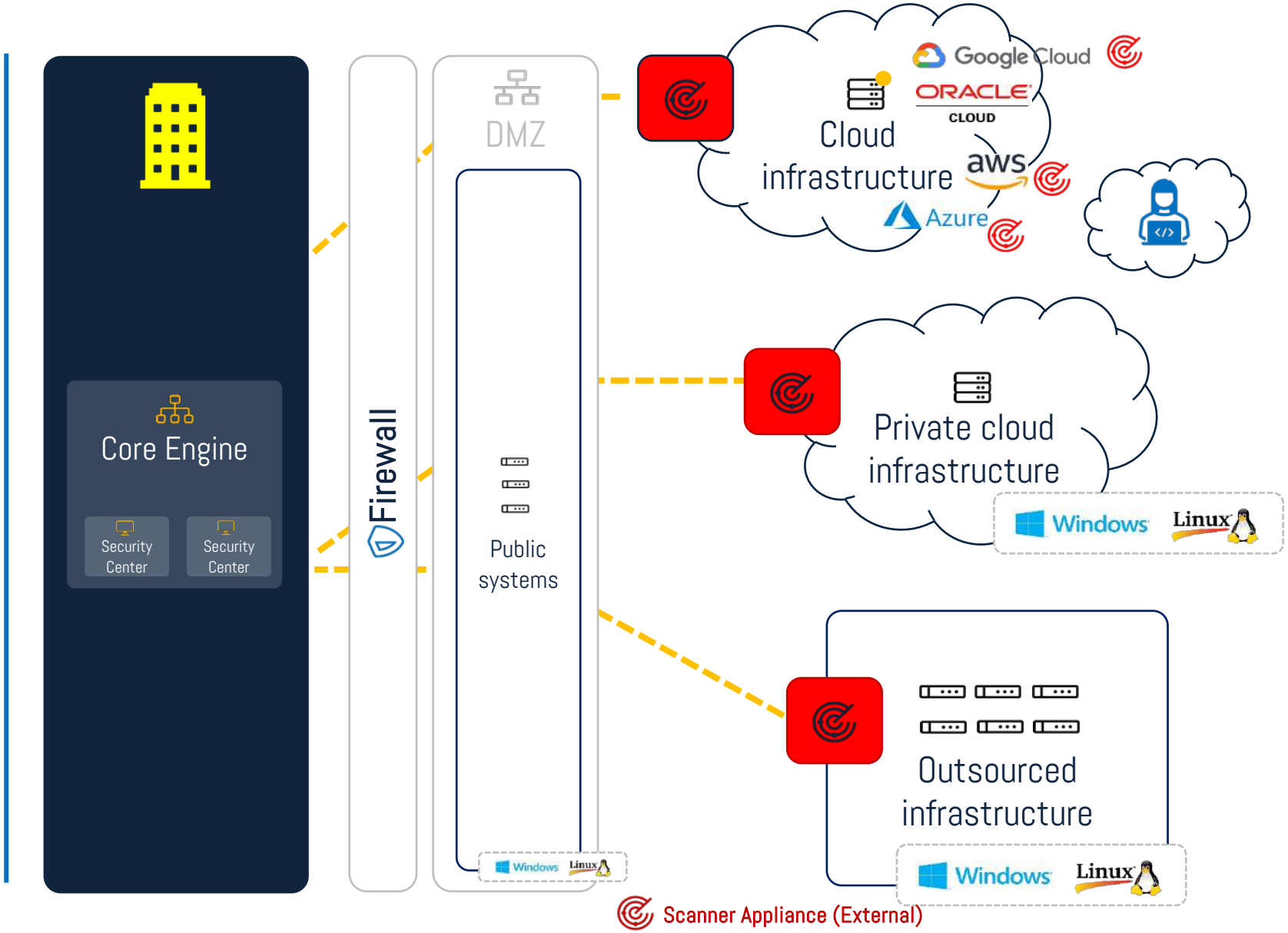


- The internal Scanner Appliance is to connect to the Core Engine with the following TCP Ports: -
  - 8004, 8007, 8044 and 8022
- The following TCP Ports are for access of the system administrator: -
  - Web Portal Admin: 8001
  - Multi Tenant Organizer: 8002
  - REST API: 8005

ON-PREMISE: EXTERNAL

- The **external** Scanner Appliance is to connect to the Core Engine with the following TCP Ports: -
  - 8004, 8007, 8044 and 8022
- The following TCP Ports are for access from the system administrator: -
  - Web Portal Admin: 8001
  - Multi Tenant Organizer: 8002
  - REST API: 8005

Note: The SSL Certificate must bind both Root and Intermediate



OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Services and Ports

SERVICES AND PORTS

HOLM SECURITY

No	Service	Ports	Protocol	Notes
1	Security Center*	443	HTTPS	Main Portal
2	Web Admin*	8001	HTTPS	Web admin interface for core settings of On-Prem system
3	Organizer*	8002	HTTPS	Multi-tenant Portal
4	Platform API*	8005	HTTPS	Security Center REST API
5	Back Office	8003	HTTPS	Internal to Holm Security only
6	Scanner Appliance API**	8004	HTTPS	Internal for Scanner Appliance
7	Feed Updates**	8007	HTTPS	Signature and scanner appliance updates
8	APT**	8044	HTTP	Signed OS package updates for scanner appliance
9	Scanner Appliance**	8022	SSH	Management port with unique key for each scanner appliance

*To be used by the Customer

**To be used by Virtual Scanner Appliance

OTD BİLİŞİM
GLOBAL VAD

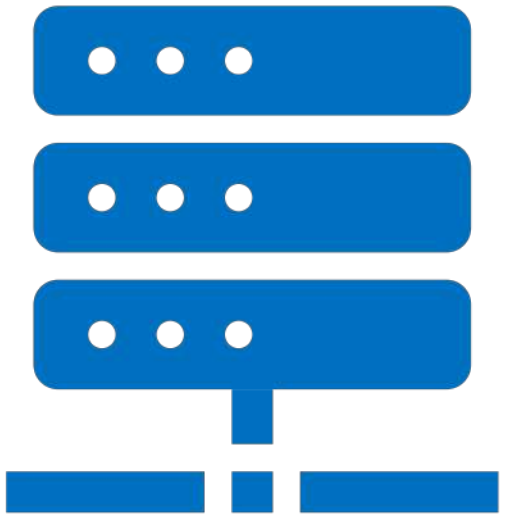
HOLM SECURITY

Components of On-Premise

CORE ENGINE & VIRTUAL SCANNER APPLIANCE

HOLM SECURITY

Core Engine



VMware ESXi™

- Static IP (and Subnet Mask, Gateway and DNS)
- SMTP Settings
- License File (contact your Holm Security representative to obtain this license key)

Virtual Scanner Appliance

- Static IP (and Subnet Mask, Gateway and DNS)

VMware ESXi™ · vmware Workstation · VirtualBox · KVM · PROXMOX · Xen Server™ · Microsoft Hyper-V

Link: https://support.holmsecurity.com/knowledge/which-virtualization-platforms-does-the-general-ova-image-support
Link: https://support.holmsecurity.com/knowledge/what-are-the-requirements-to-run-onprem

OTD BİLİŞİM GLOBAL VAD

SYSTEM REQUIREMENTS

HOLM SECURITY

Proof of Concept (200 IPs / 5 Web Applications)

Server	Description	CPU	RAM (GB)	HDD (GB)	Quantity
Server A	Core Engine	4	16	100	1
Server B	Scanner Appliance	2	8	150	1

Small (>1000 IPs / 5 Web Applications)

Server	Description	CPU	RAM (GB)	HDD (GB)	Quantity
Server A	Core Engine	8	24	100	1
Server B	Scanner Appliance	2	8	150	2

Medium (1000 – 10000 IPs / 5 – 30 Web Applications)

Server	Description	CPU	RAM (GB)	HDD (GB)	Quantity
Server A	Core Engine	12	32	100	1
Server B	Scanner Appliance	2	8	150	4

Large (> 10000 IPs / > 30 Web Applications)

Server	Description	CPU	RAM (GB)	HDD (GB)	Quantity
Server A	Core Engine	24	48	100	1
Server B	Scanner Appliance	2	8	150	8

Link: https://support.holmsecurity.com/knowledge/what-are-the-requirements-to-run-onprem

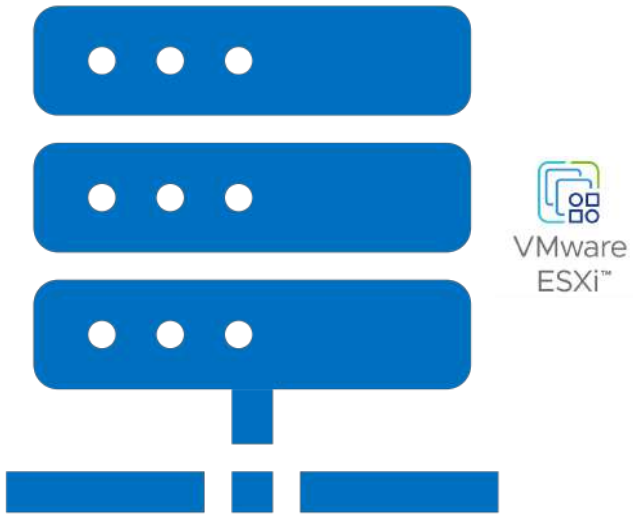
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Images Download

IMAGES DOWNLOAD

Core Engine



https://s3-kna1.citycloud.com:8080/8bc8ec85d2074ca7b282d0fab0f79f75:onprem/onprem-public-058e31b8.ova

Virtual Scanner Appliance

OVA

https://swift-kna1.citycloud.com/swift/v1/AUTH_b86ff371e25f443fb8161f2f56143a3f/scanner-appliance/ova_public_3-19-2_07137bb1.ova?temp_url_sig=86486711088d7209fea60c14894ea96ae20f76bb&temp_url_expires=2078138795

Hyper-V

https://swift-kna1.citycloud.com/swift/v1/AUTH_b86ff371e25f443fb8161f2f56143a3f/scanner-appliance/vhdx_public_3-19-2_07137bb1.vhdx.gz?temp_url_sig=54a51a17d366dd753a4e73c4ba8d5328b9b9e645&temp_url_expires=2078139685

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

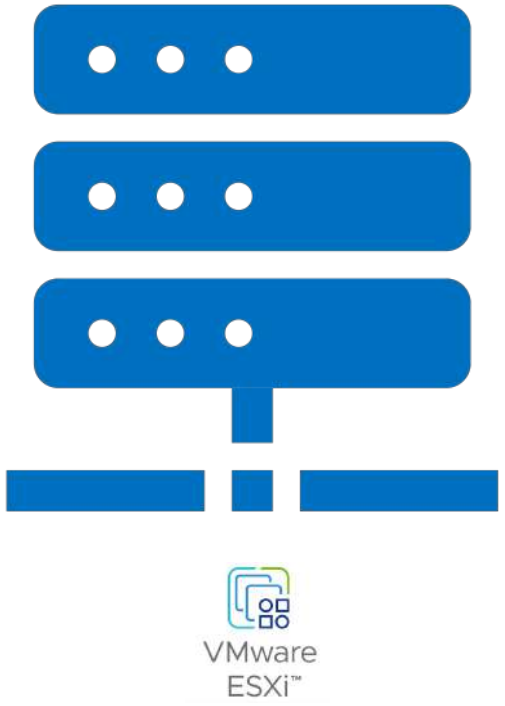
Core Engine

Deployment and Configuration

CORE ENGINE: IMPORT

HOLM SECURITY

Core Engine

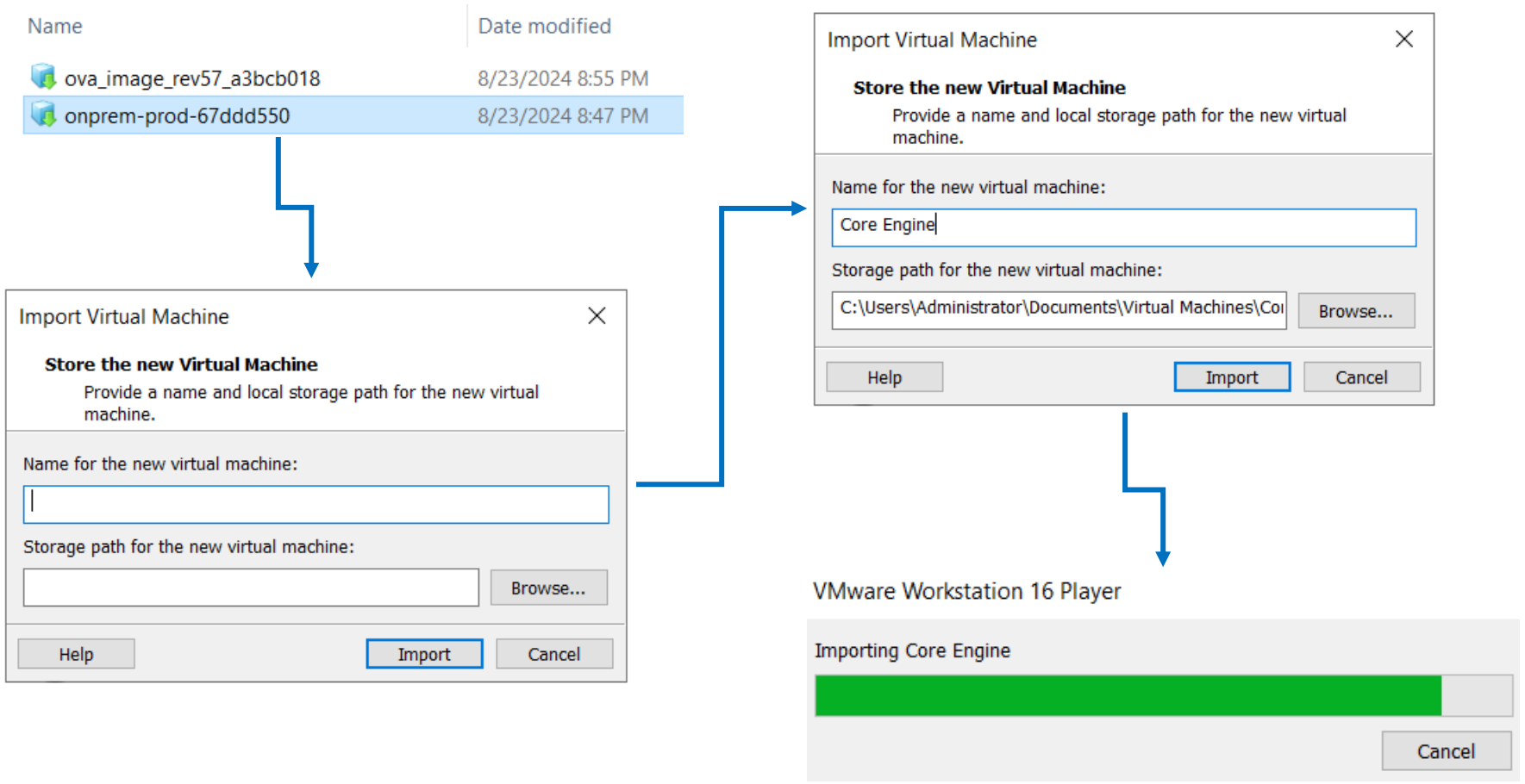


Open a Virtual Machine

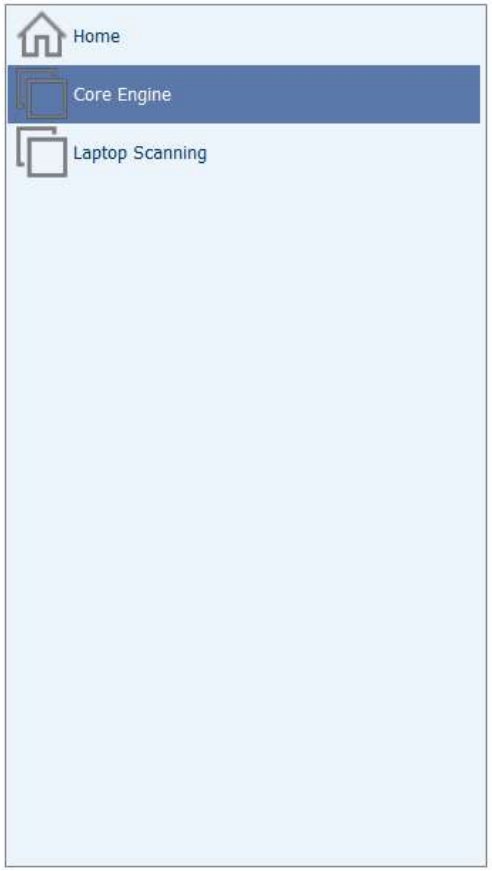
Note: Simulating an import process of the Core Engine image using VMWare Workstation Player 16

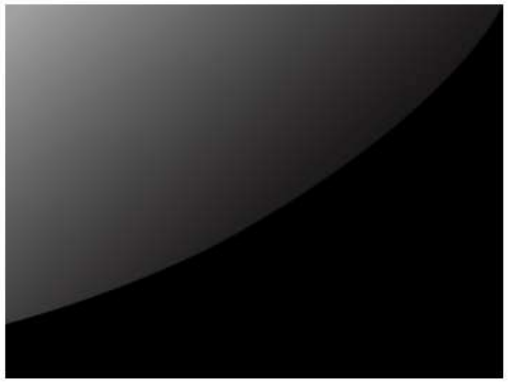
OTD BİLİŞİM GLOBAL VAD

CORE ENGINE: IMPORT



CORE ENGINE: IMPORT





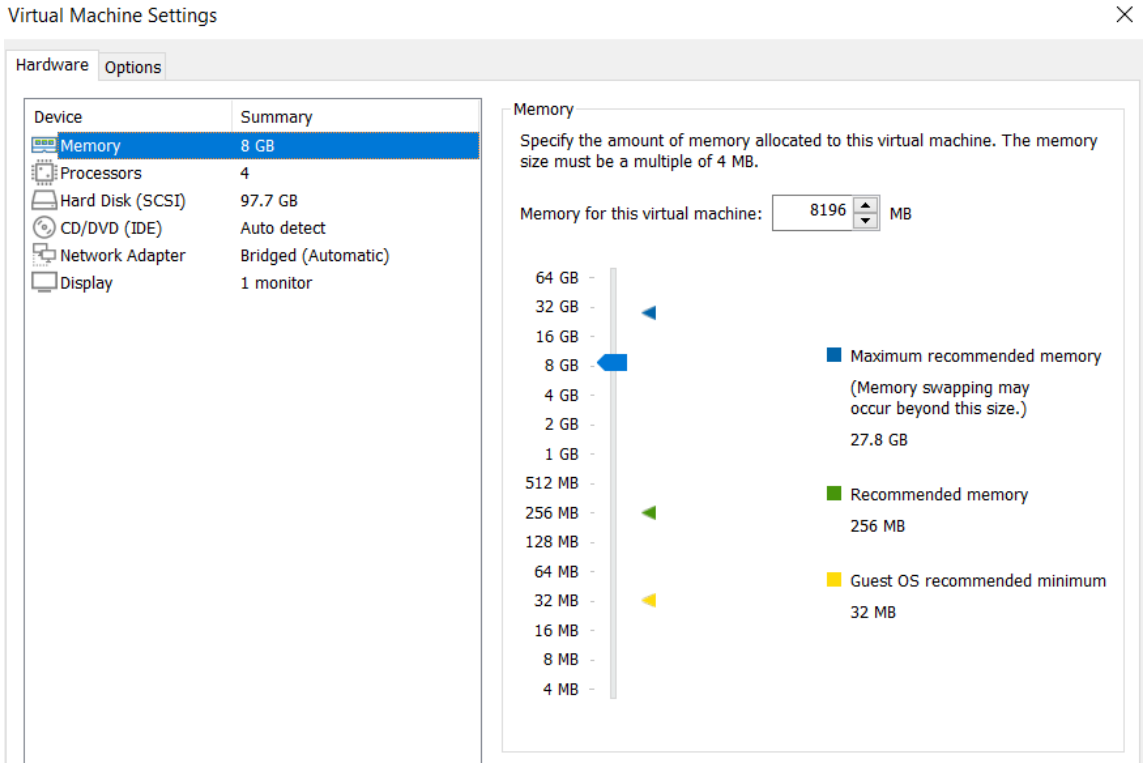
Virtual Machine Name:

Core Engine

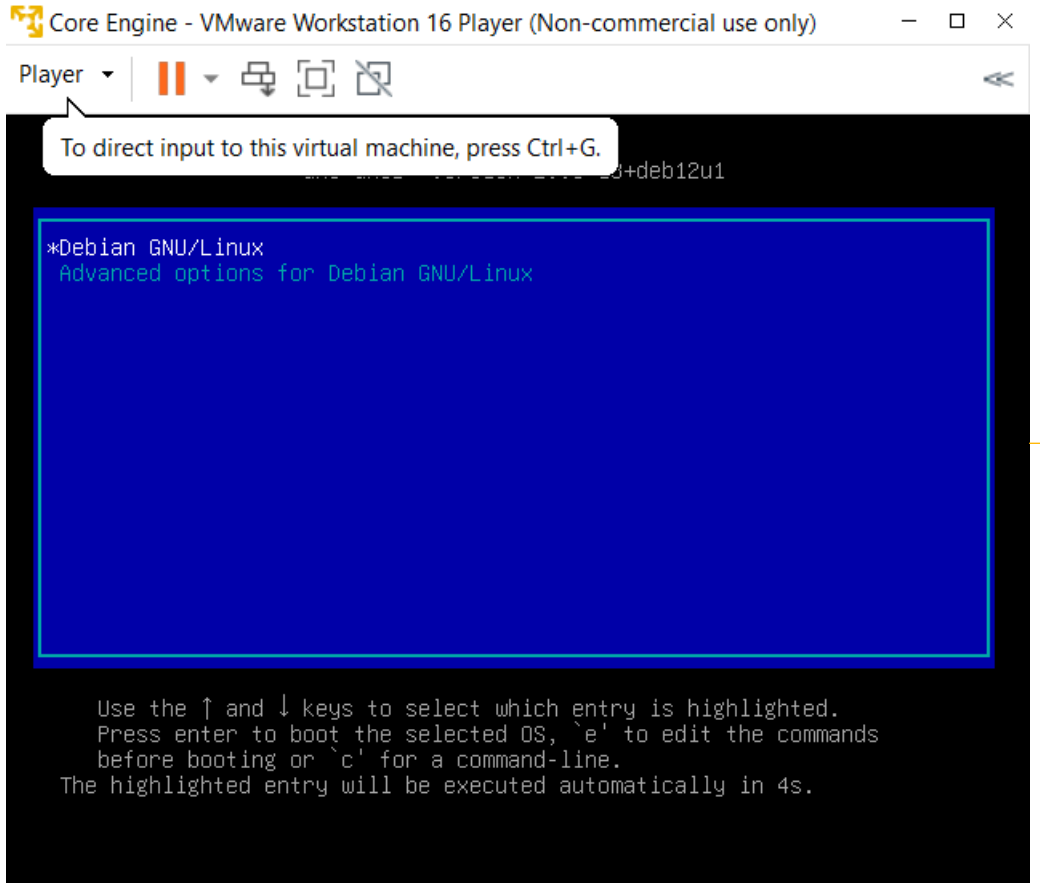
State: Powered On
OS: Other
Version: ESXi 6.5 virtual machine
RAM: 8 GB

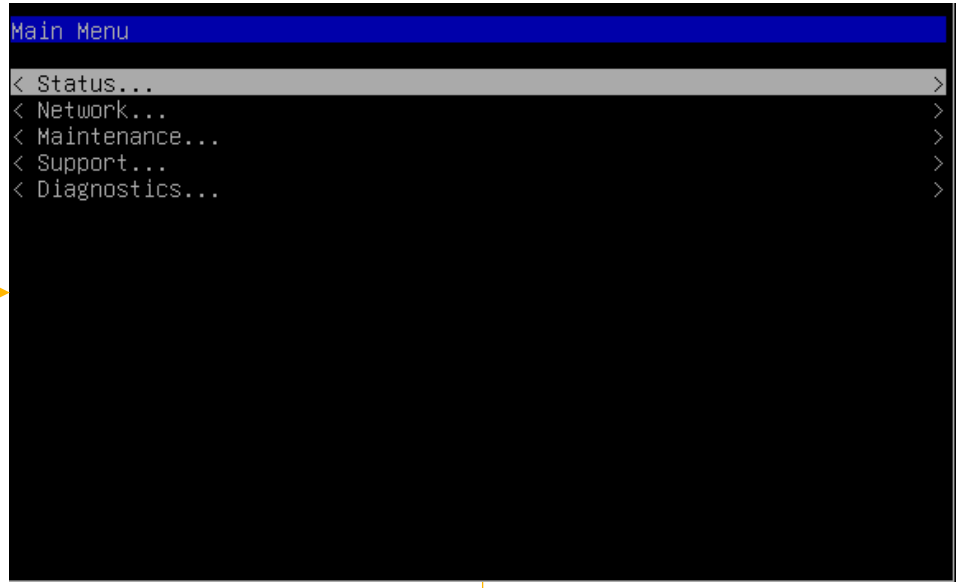
Play virtual machine

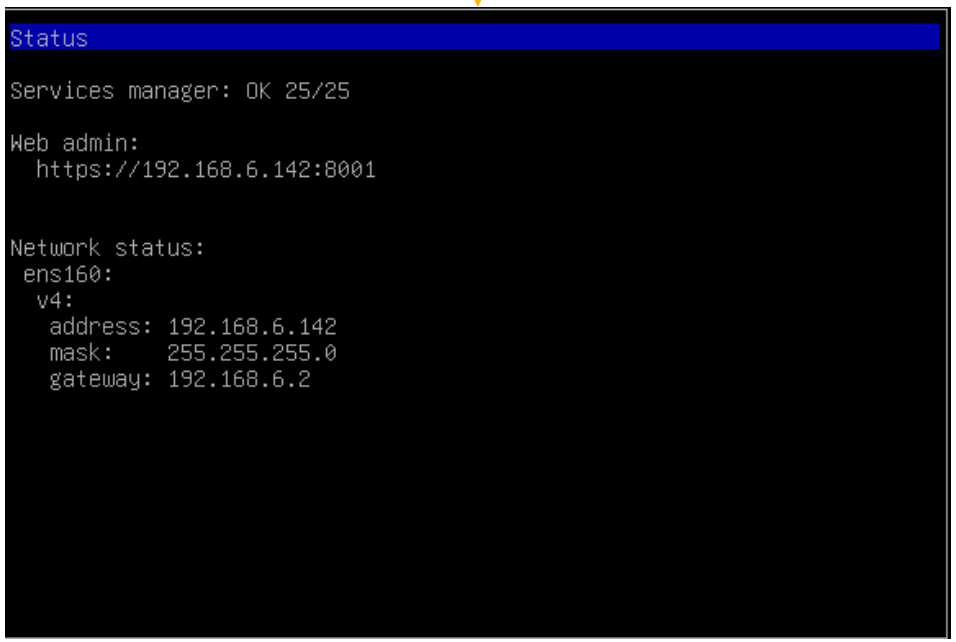
Edit virtual machine settings



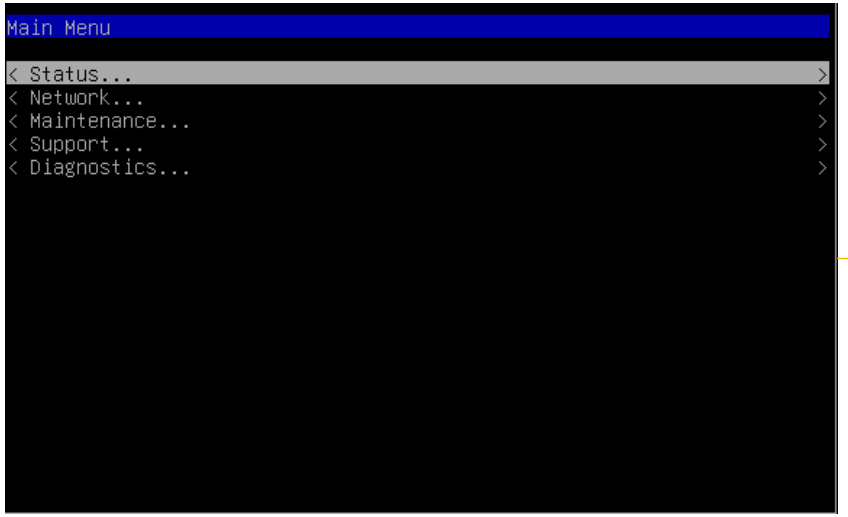
CORE ENGINE: SETUP

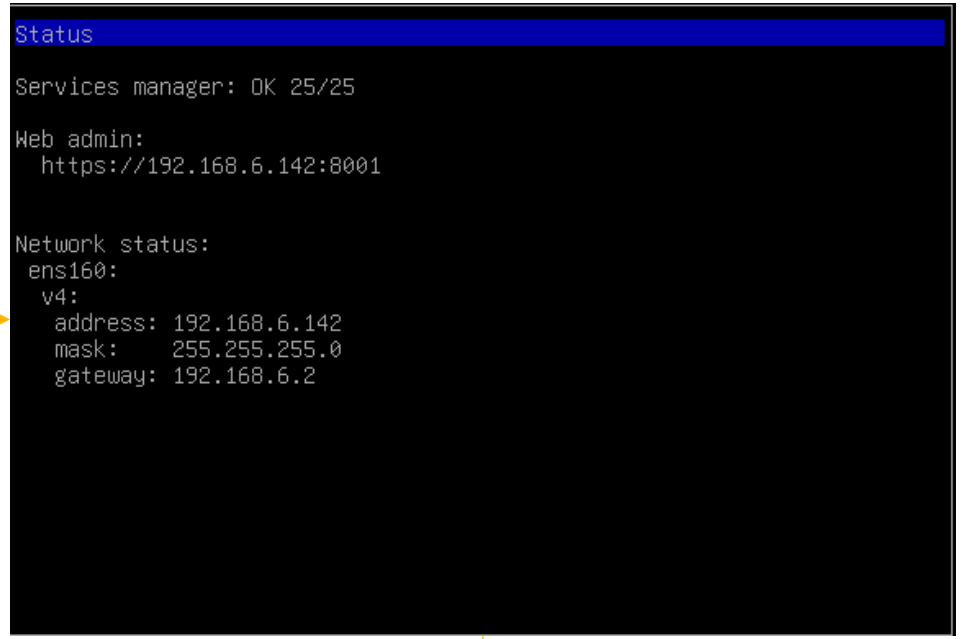


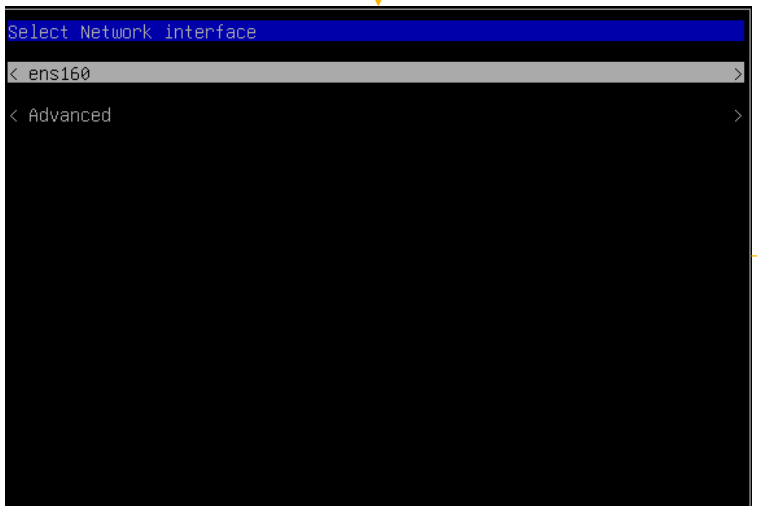


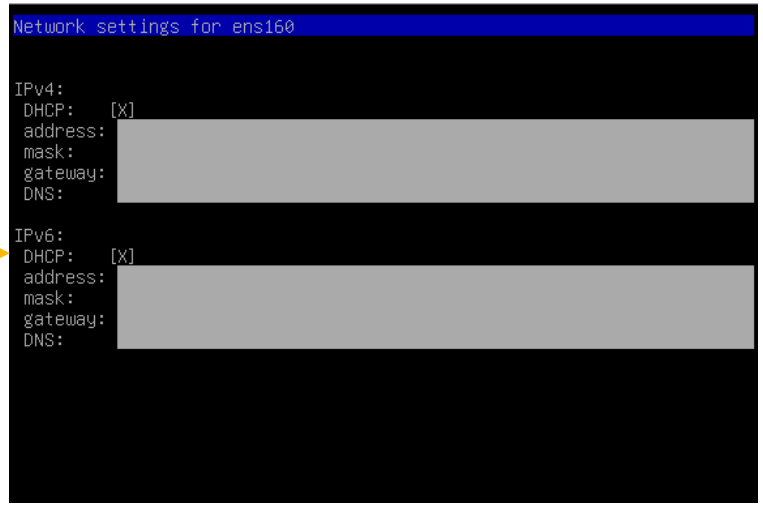


CORE ENGINE: IMPORT









Note: This simulation is based on DHCP for the IP

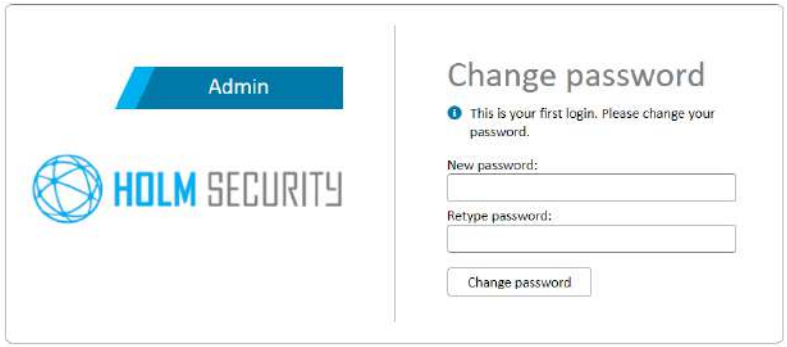
OTD BİLİŞİM
GLOBAL VAD

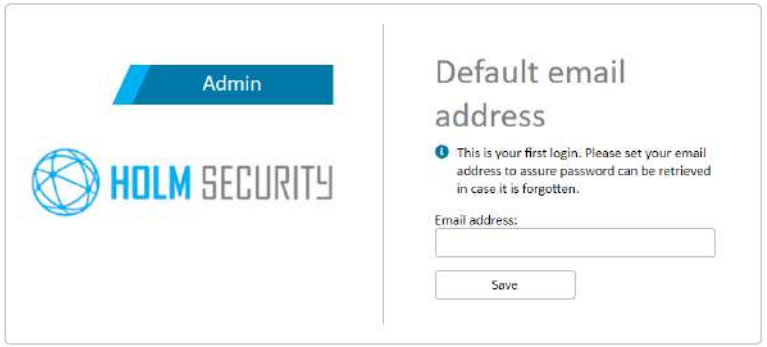
HOLM SECURITY

Web Admin Portal

Setup and Configuration

WEB ADMIN: CONFIGURATION





- Launch the web admin portal, i.e.; https://ip-address-of-core-engine:8001
- The default credential: -
  - Username: admin
  - Password: holmsecurity
- You will be prompted to change to a new password and specify a new email address

WEB ADMIN: CONFIGURATION

HOLM SECURITY

E-mail

SMTP Hostname/IP:*

SMTP port:*

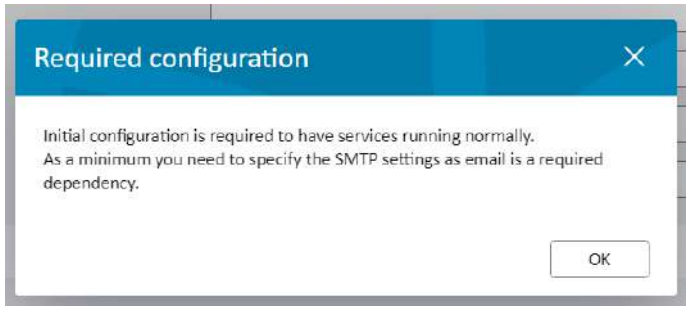
Use TLS: Yes No

SMTP username:

SMTP password:

SMTP sender email:*

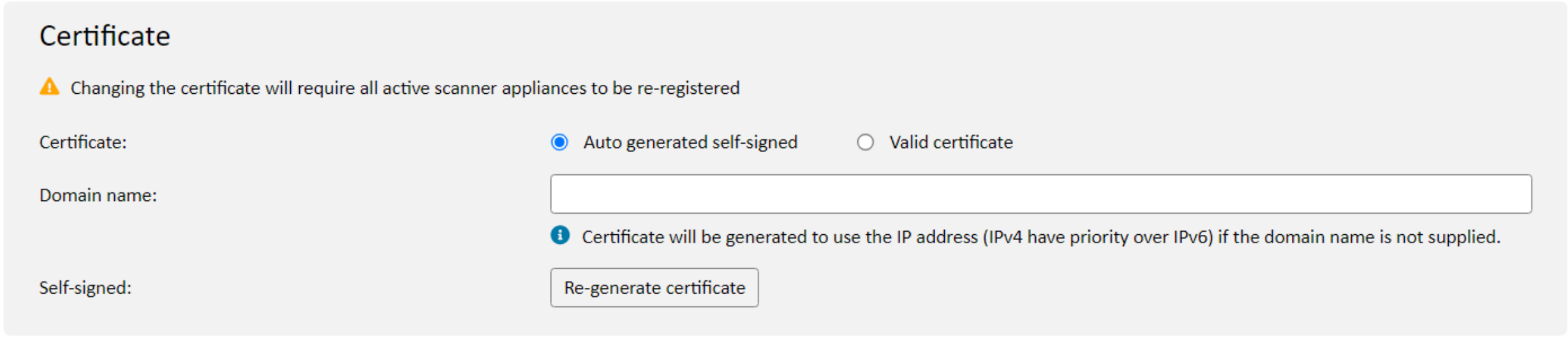
SMTP sender name:*



- The following settings are required for the SMTP configuration: -
  - SMTP Hostname / IP
  - SMTP port: Choose either 25, 465, 587
  - TLS: Yes or No
  - SMTP - Username, Password, Sender email and Sender name

OTD BİLİŞİM GLOBAL VAD

WEB ADMIN: CONFIGURATION



You can opt for a self-signed certificate based on the IP address configured for the Core Engine or……(next page)

WEB ADMIN: CONFIGURATION

HOLM SECURITY

Certificate

⚠ Changing the domain name will require all active scanner appliances to be re-registered

Certificate: ○ Auto generated self-signed ◉ Valid certificate

Domain name:*

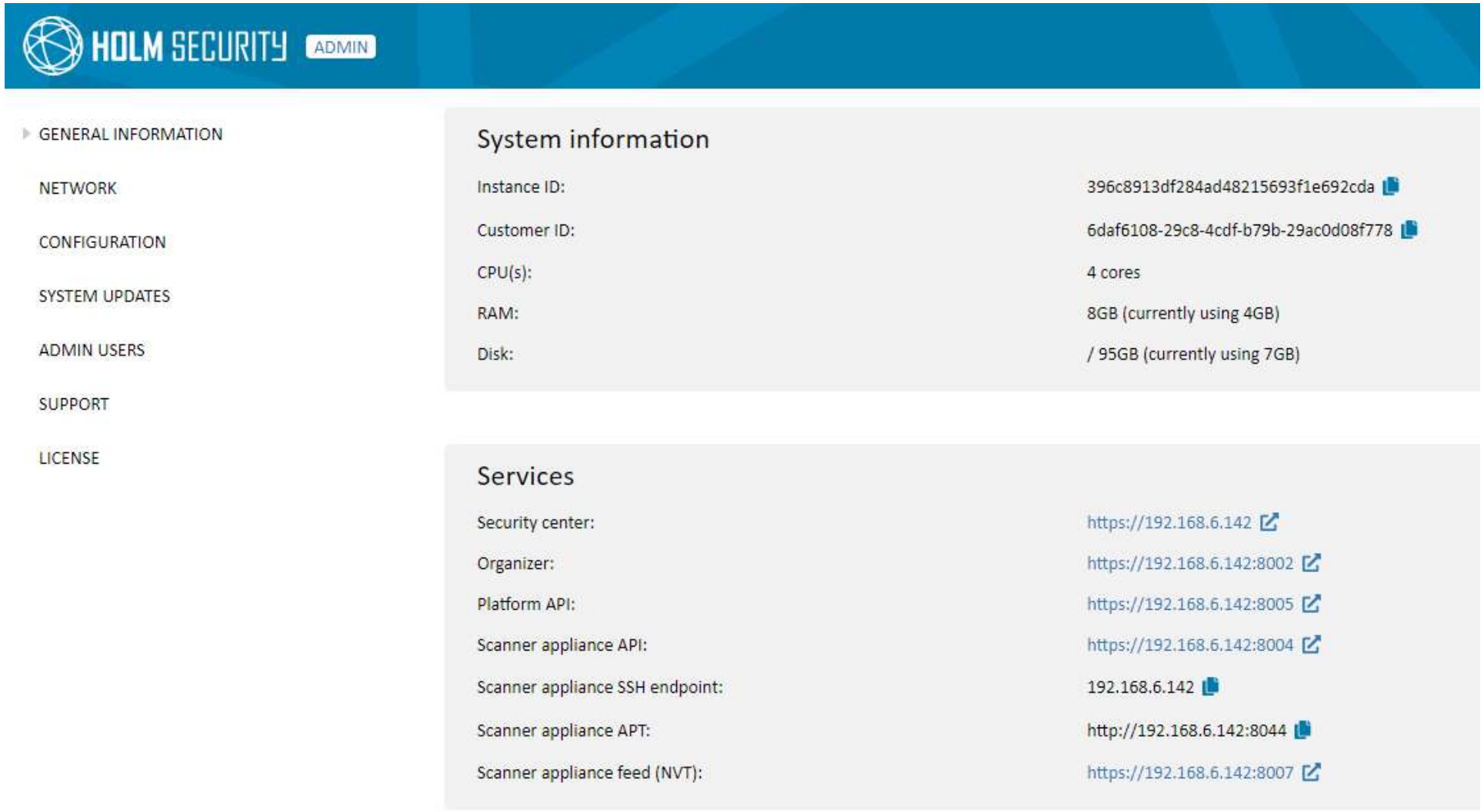
ℹ Domain name must match the certificate exactly. If a wildcard certificate is used it needs to match witin the subdomain.

Upload certificate:* Select PEM certificate

Upload key:* Select PEM key

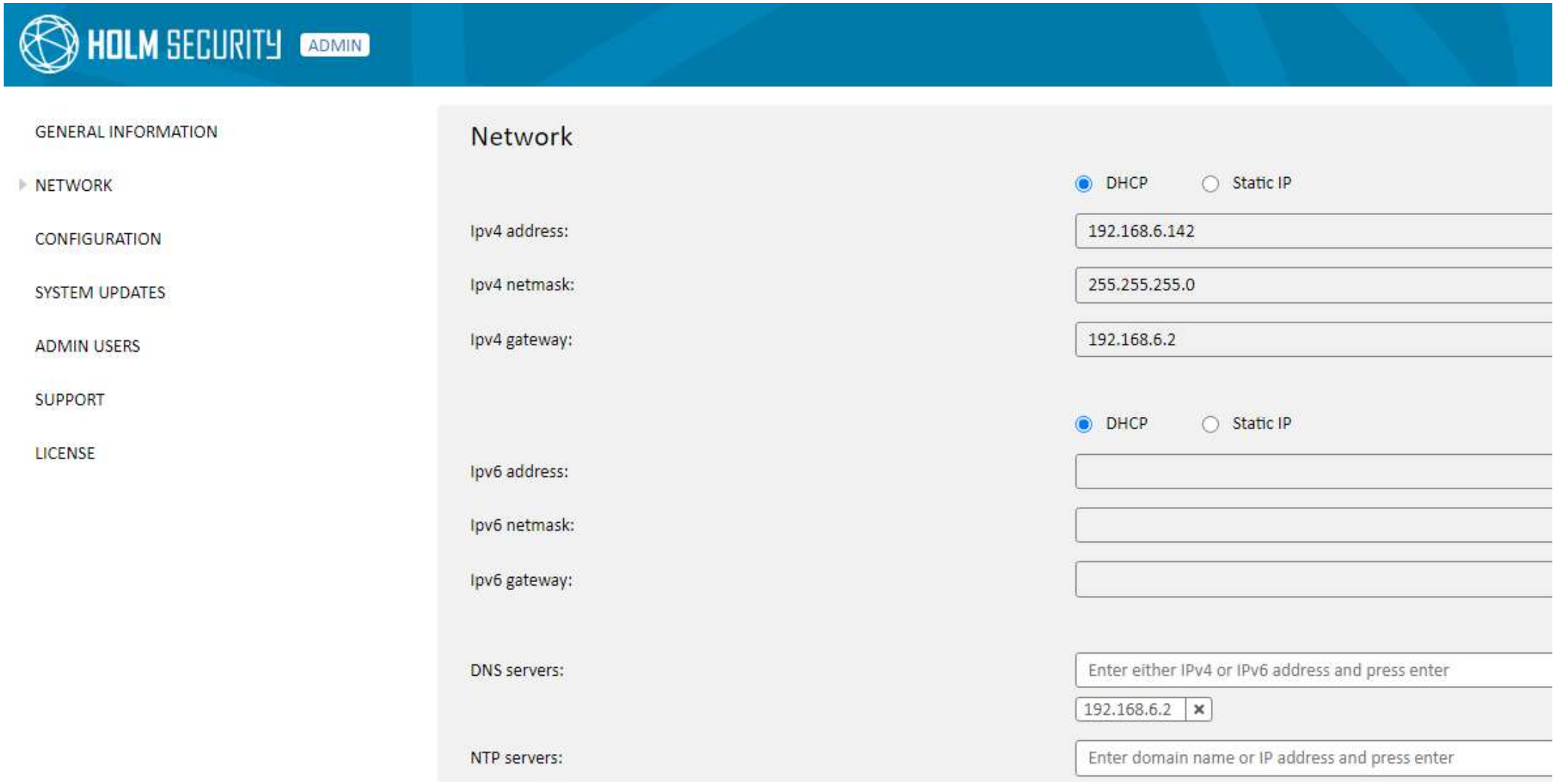
You can opt for a valid certificate where both Root and Intermediate are binded together

WEB ADMIN: CONFIGURATION



General Information: The IP addresses take into effect. Take note of the Services and its TCP Ports

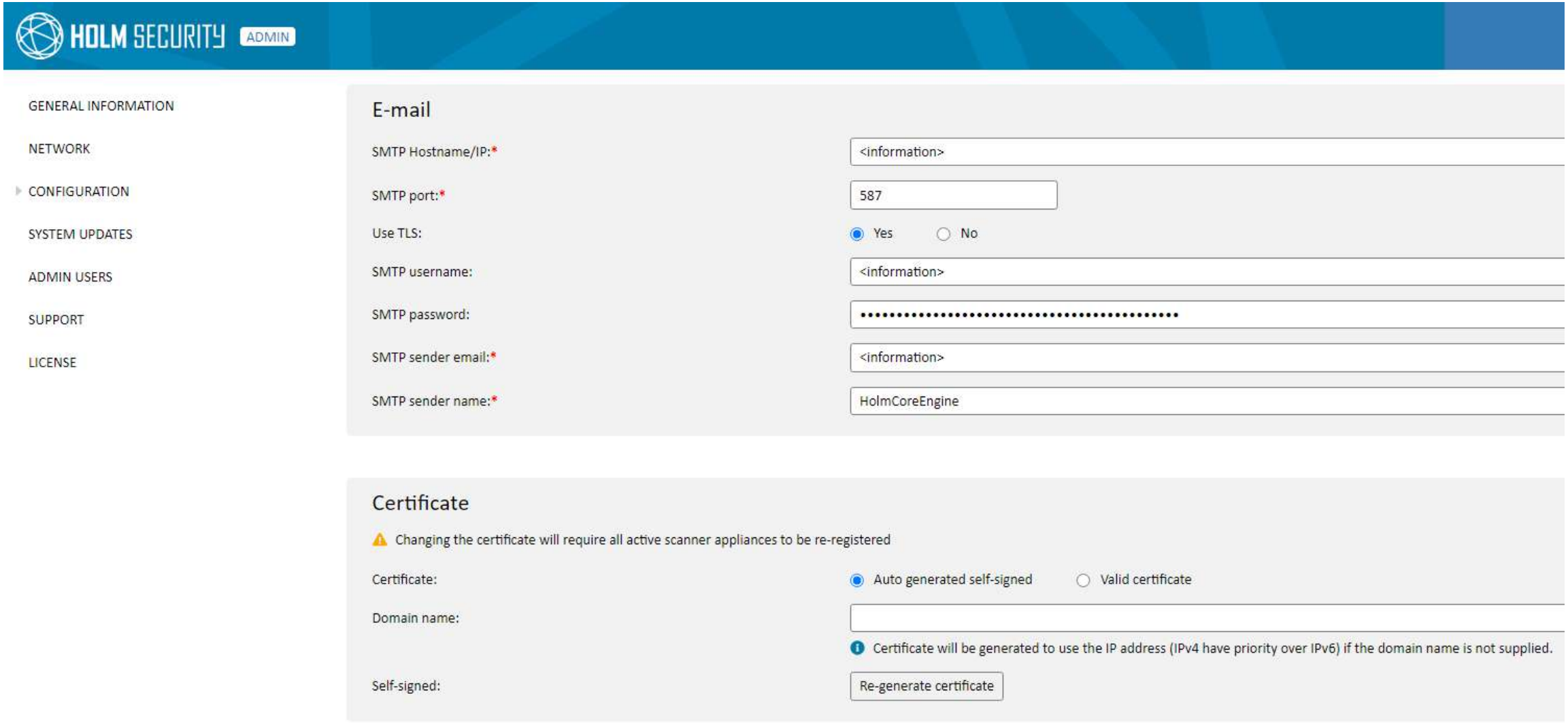
WEB ADMIN: CONFIGURATION



Network: The display of the IP settings (DHCP or Static IP)

WEB ADMIN: CONFIGURATION

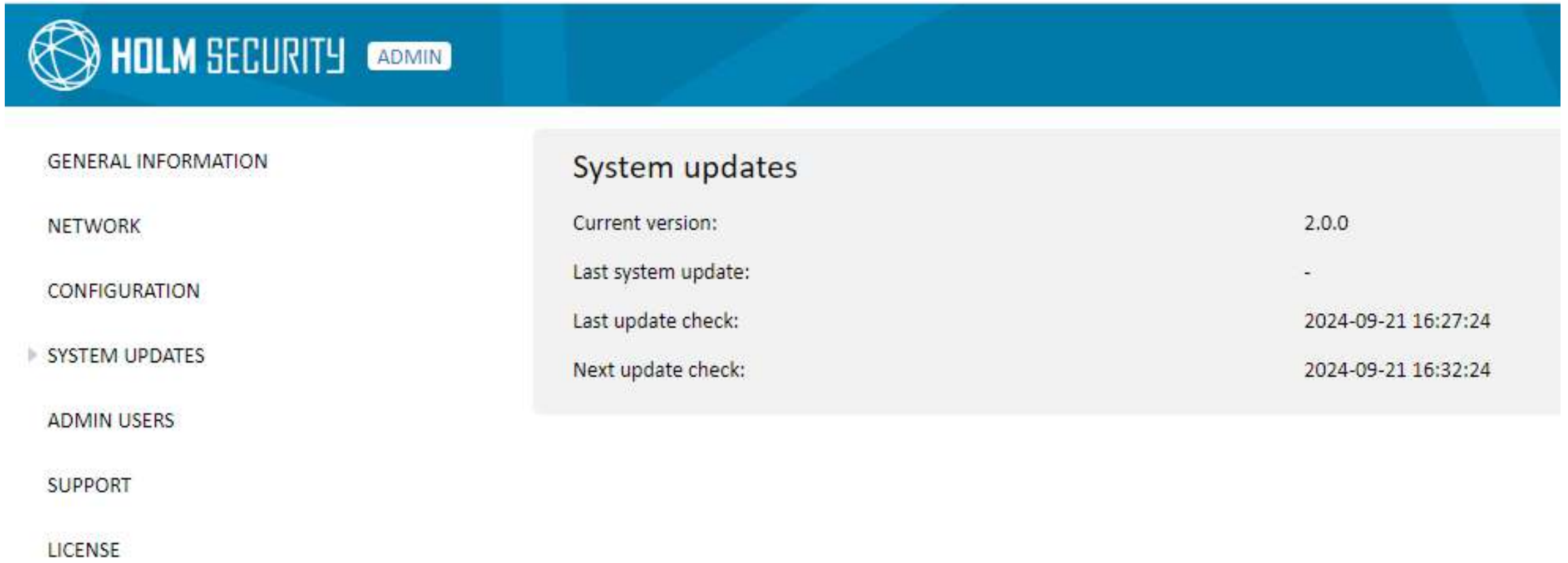
HOLM SECURITY



Configuration: A re-cap of the SMTP and Certificate inputs

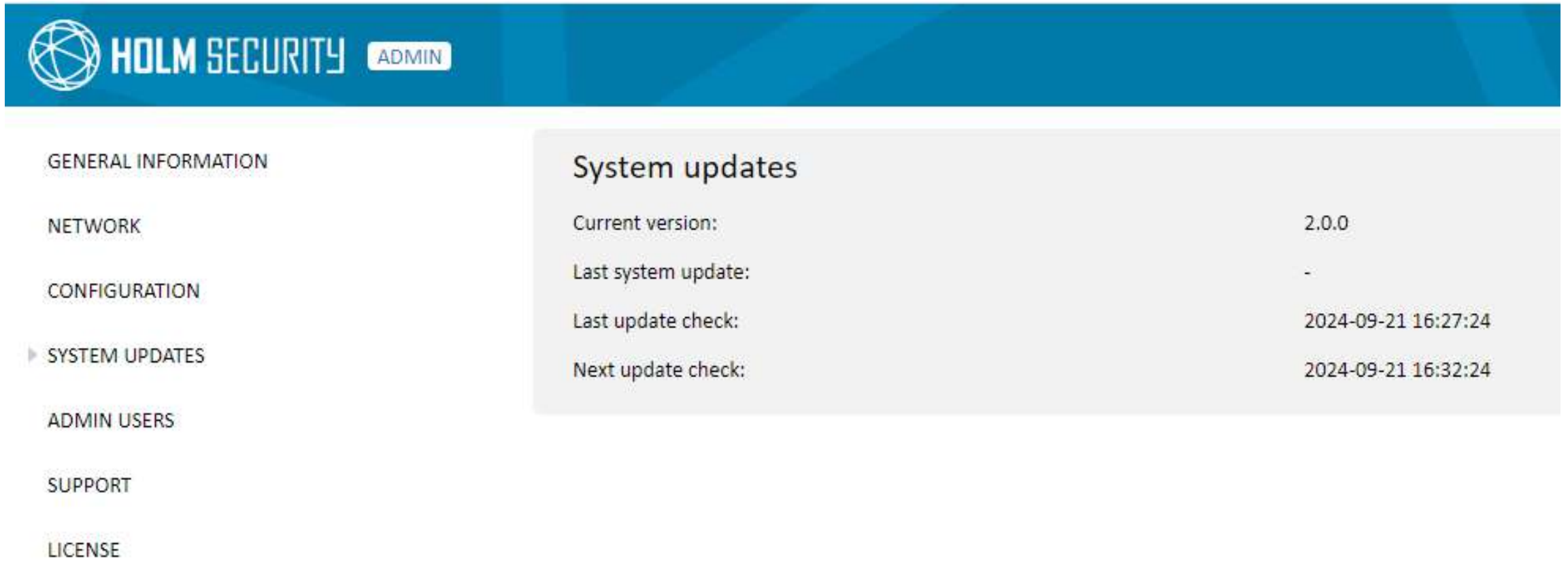
OTD BİLİŞİM GLOBAL VAD

WEB ADMIN: CONFIGURATION



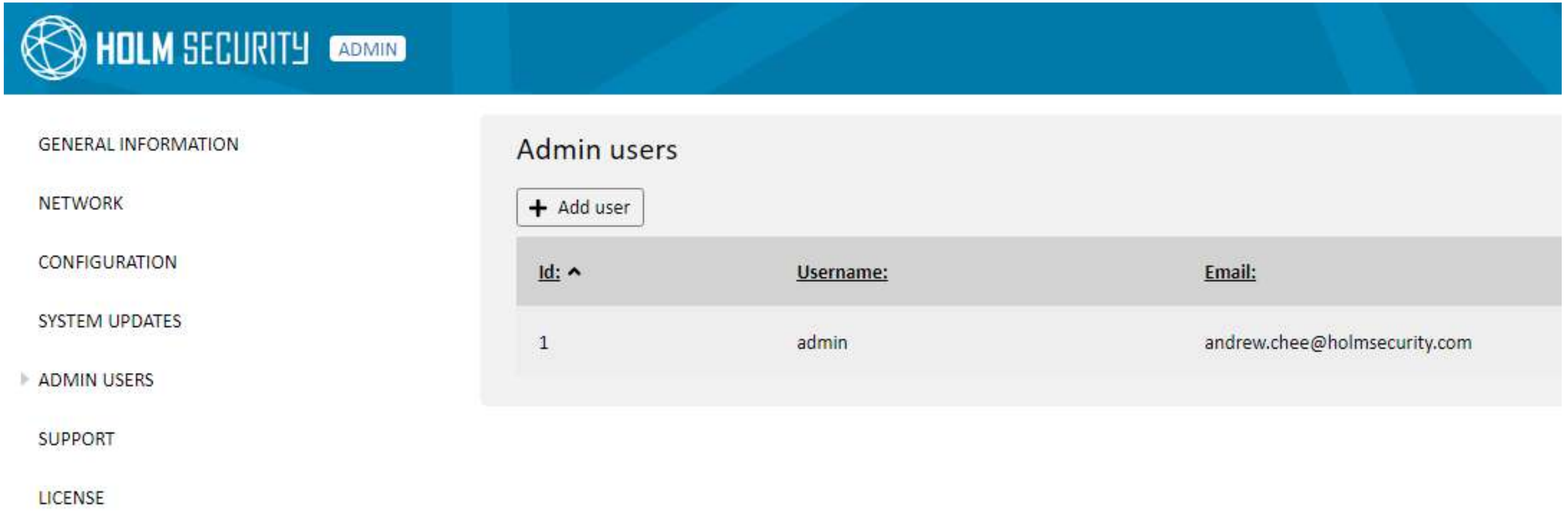
System Updates: The current version of the On-Premise Core Engine – 2.0.0

WEB ADMIN: CONFIGURATION



System Updates: The current version of the On-Premise Core Engine – 2.0.0

WEB ADMIN: CONFIGURATION

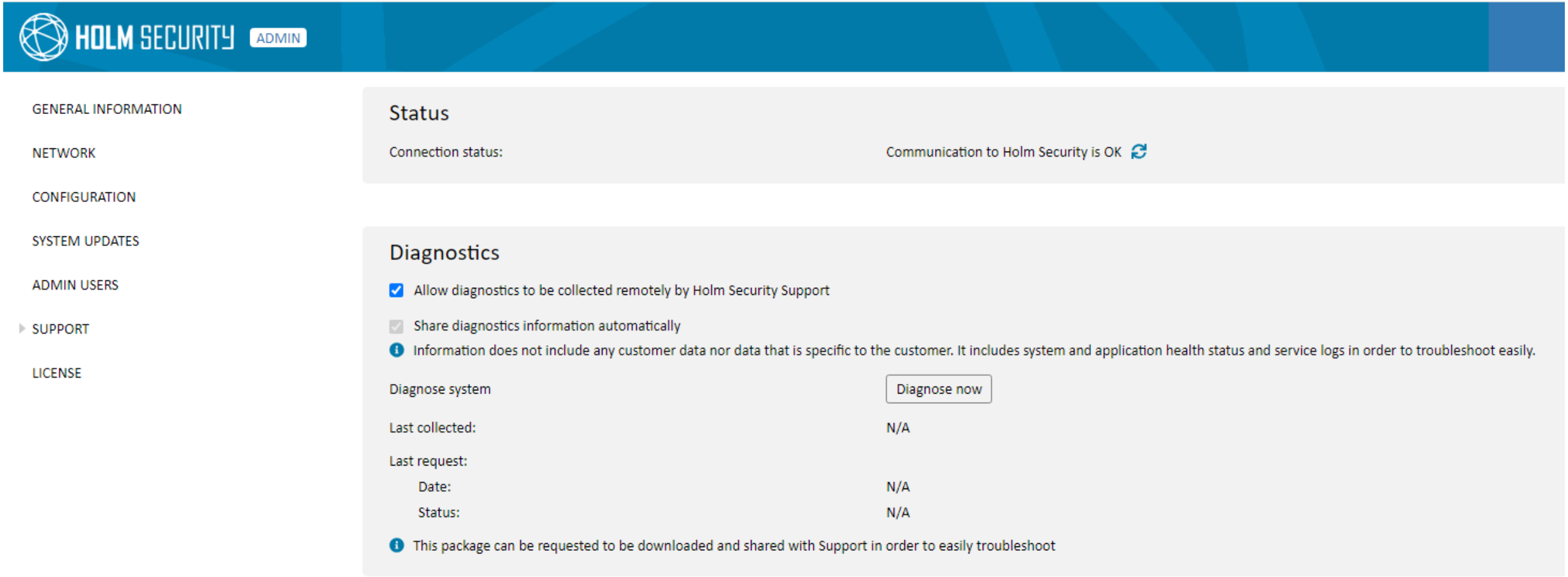


Admin Users: The email ID of the admin user(s)

WEB ADMIN: CONFIGURATION

License: Upload the license key provided by your Holm Security representative

WEB ADMIN: CONFIGURATION



Support

- Status: The communication to the Holm Security Data Center upon successful license is validated
- Diagnostics: Allow diagnostics log to be collected remotely by Holm Security Support (to be enabled upon needed). Click Diagnose Now to have the log generated

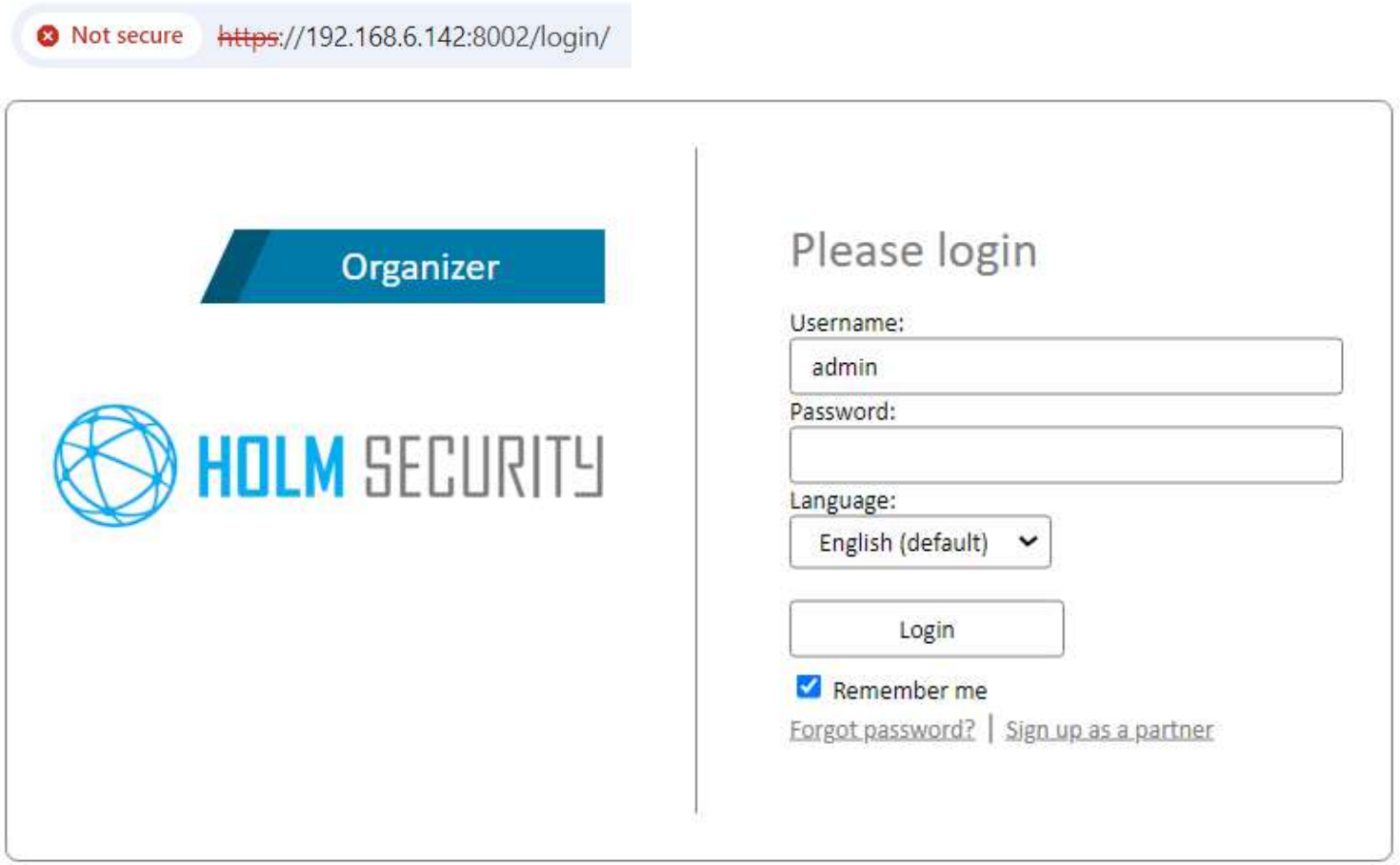
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Organizer Portal

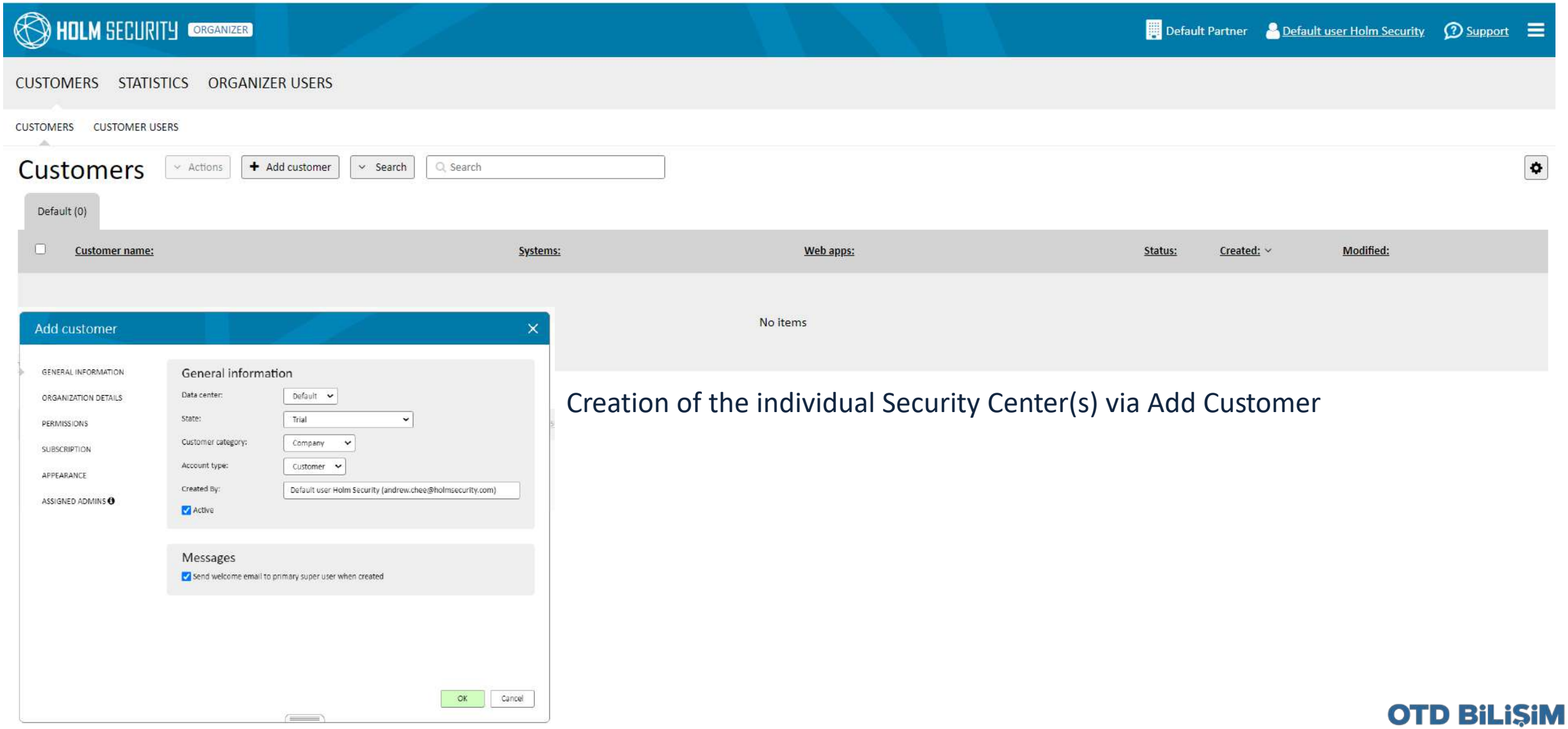
Creation of Multi-Tenants

ORGANIZER: INITIAL LOGIN



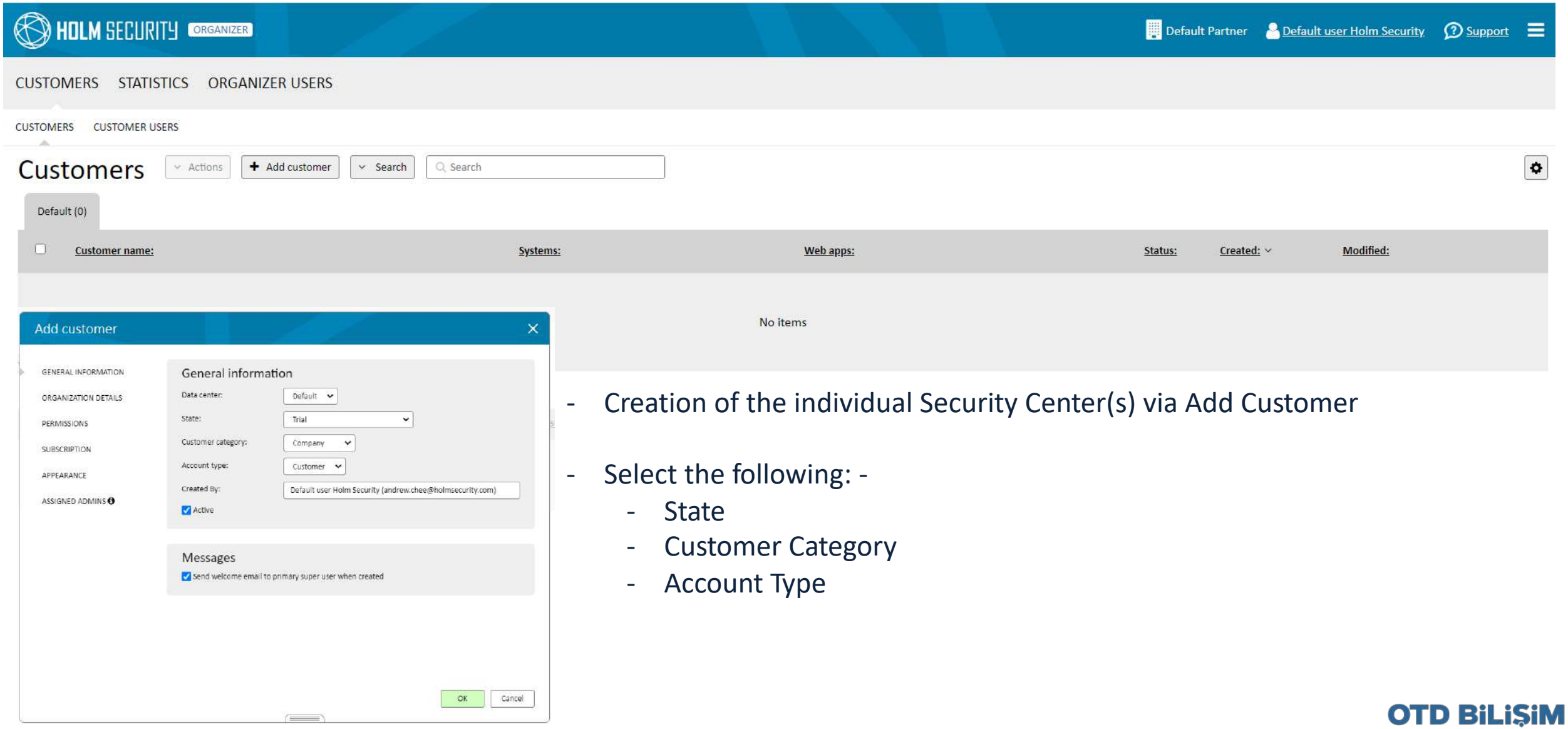
- Launch the Organizer portal, i.e., https://ip-address-of-core-engine:8002
- The default credential: -
  - Username: admin
  - Password: holmsecurity

ORGANIZER: SECURITY CENTER CREATION



Creation of the individual Security Center(s) via Add Customer

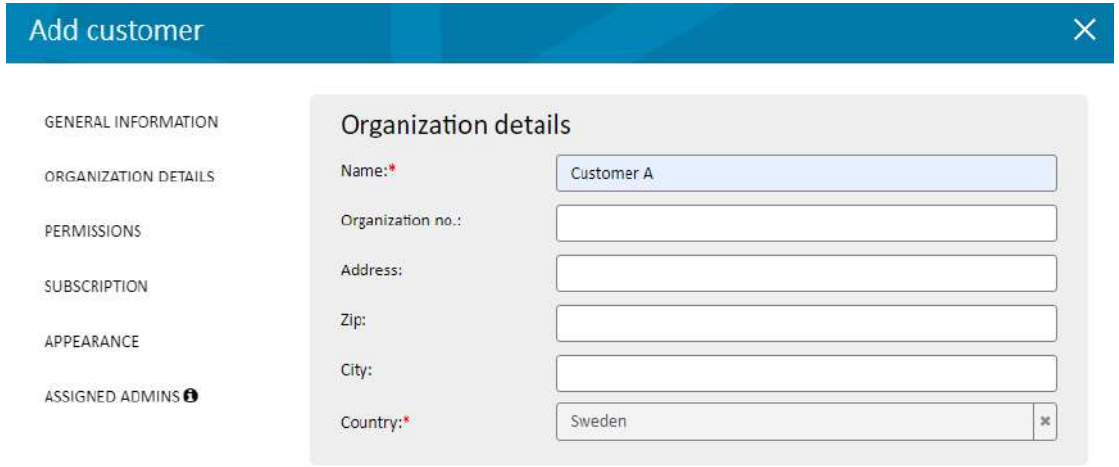
ORGANIZER: SECURITY CENTER CREATION

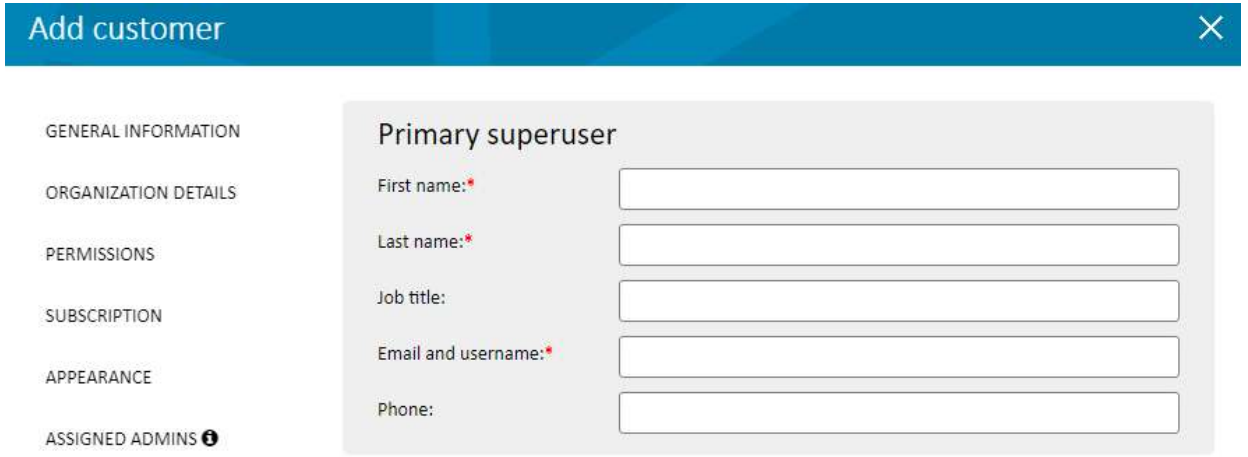


- Creation of the individual Security Center(s) via Add Customer

- Select the following: -
  - State
  - Customer Category
  - Account Type

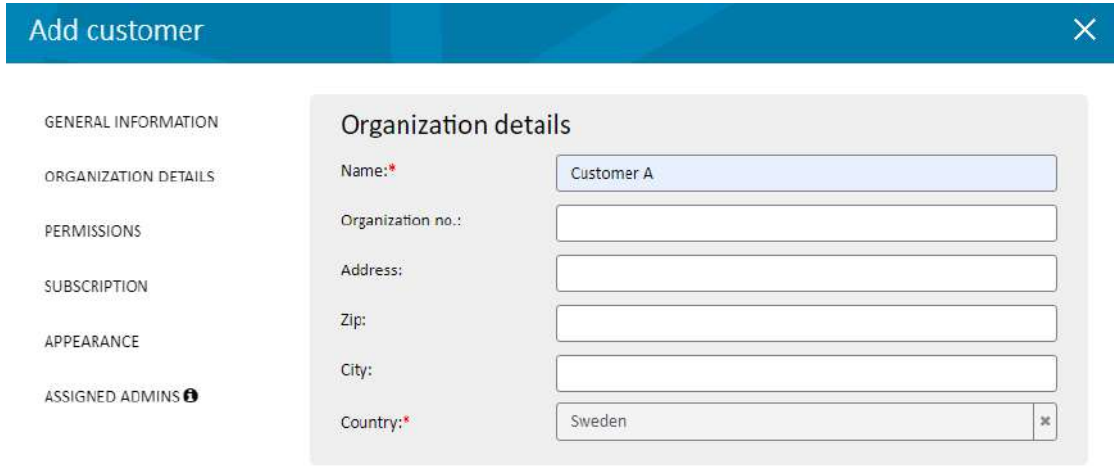
ORGANIZER: SECURITY CENTER CREATION

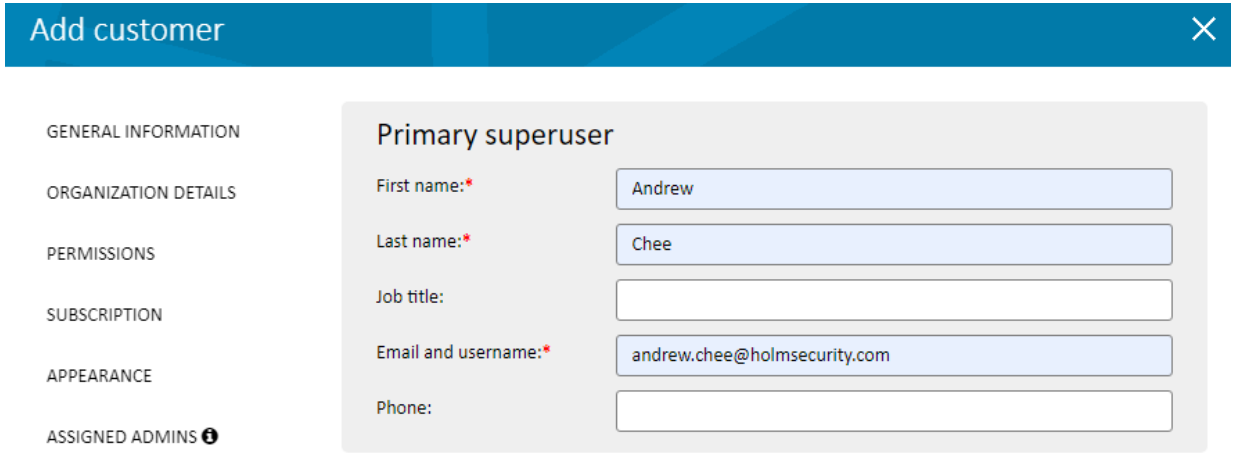




- Organization Details: -
  - Name and Country is mandatory
- Primary Superuser
  - First / Last Name, Email ID is mandatory

ORGANIZER: SECURITY CENTER CREATION

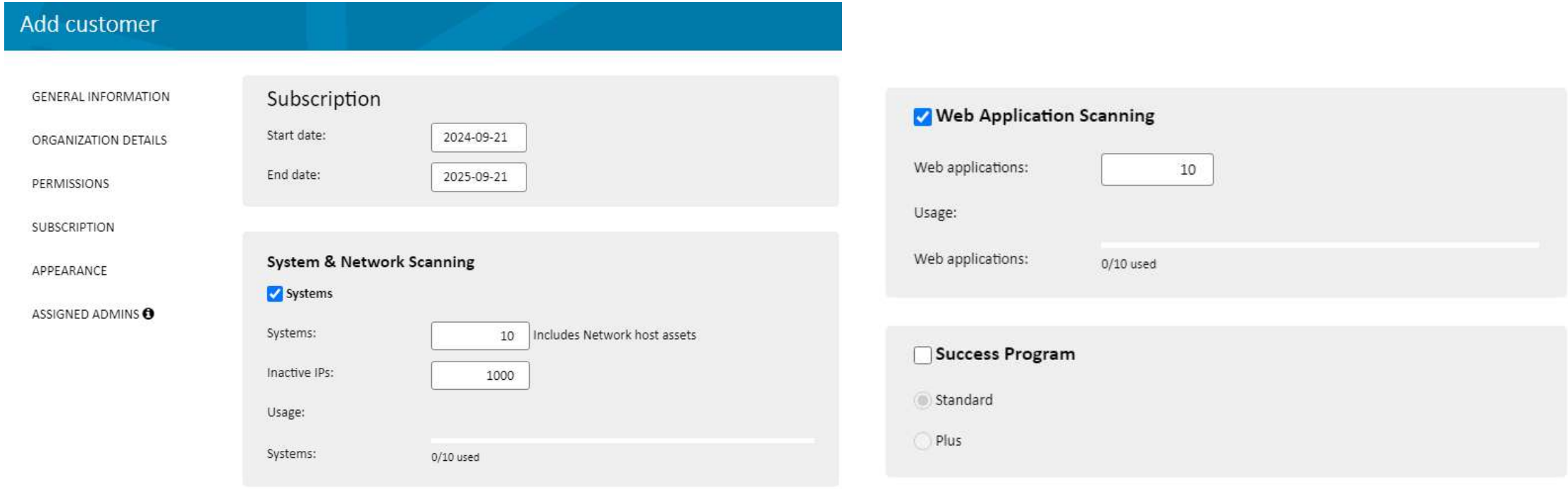




- Organization Details: -
  - Name and Country is mandatory

- Primary Superuser
  - First / Last Name, Email ID is mandatory

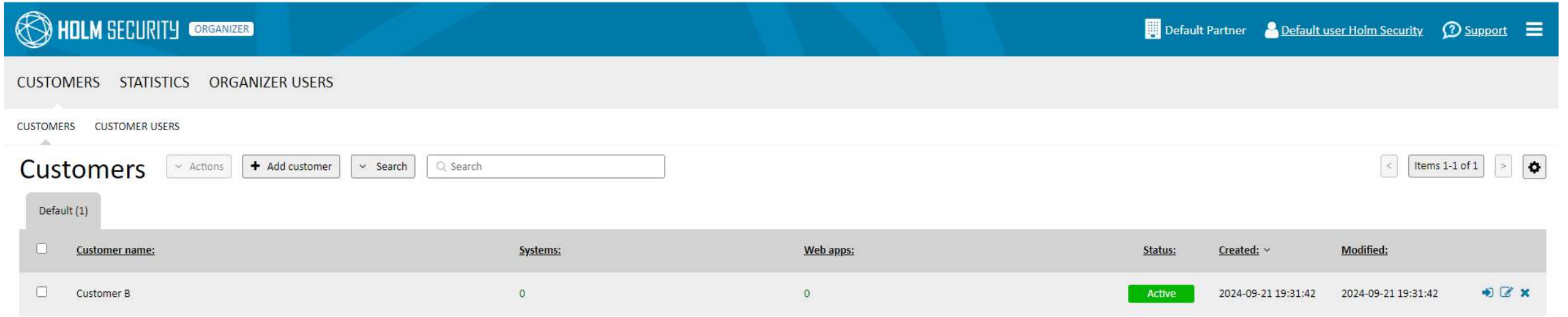
ORGANIZER: SECURITY CENTER CREATION



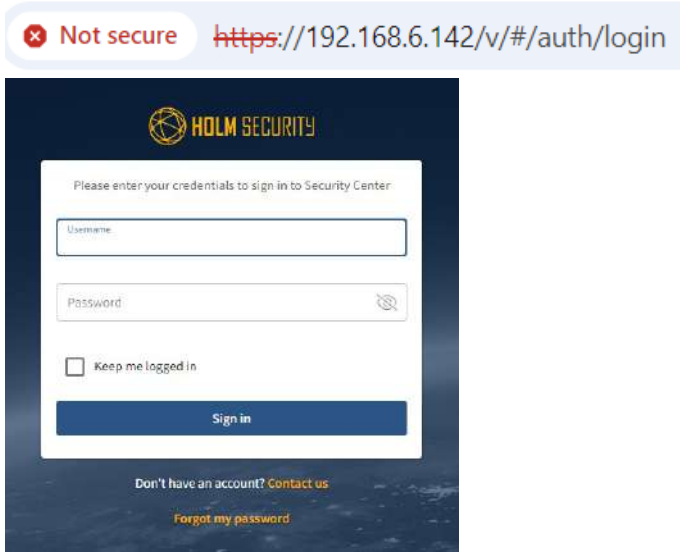
- Subscription
  - Determine the subscription date for Start and End
- System and Network Scanning
  - Specify the number of Active hosts
  - Specify the number of Inactive hosts (To allow sufficient room for a larger count)
- Web Application Scanning
  - Specify the number of web applications

ORGANIZER: SECURITY CENTER CREATION

HOLM SECURITY



- Your 1st Security Center customer / account is ready



OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Virtual Scanner Appliance

Deployment and Configuration

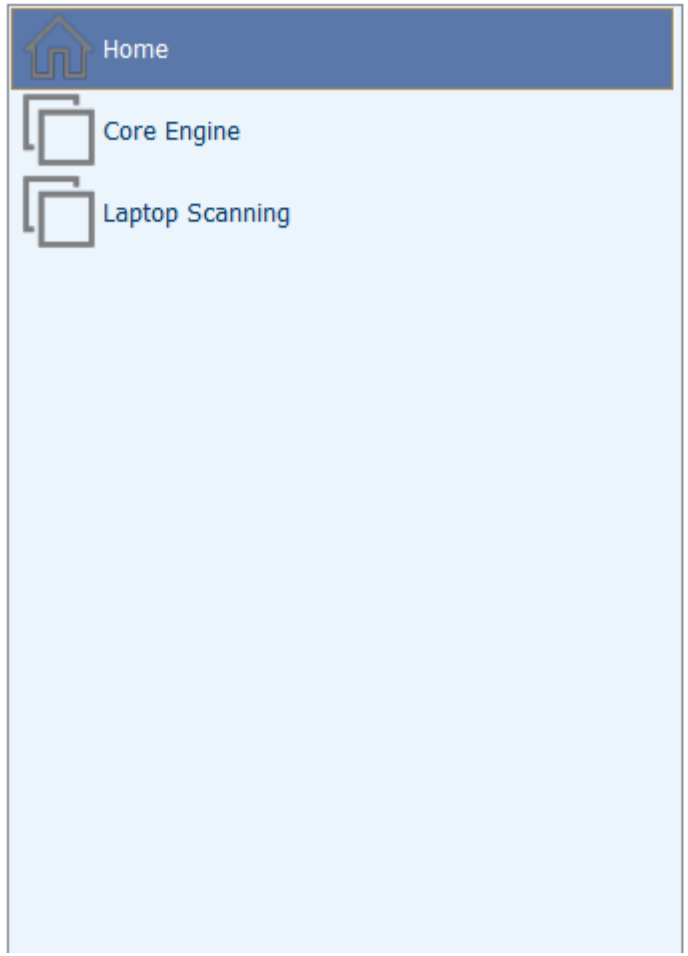
SCANNER APPLIANCE: IMPORT

HOLM SECURITY

Virtual Scanner Appliance

vmware Workstation

VMware ESXi™ PROXMOX VirtualBox KVM Xen Server™

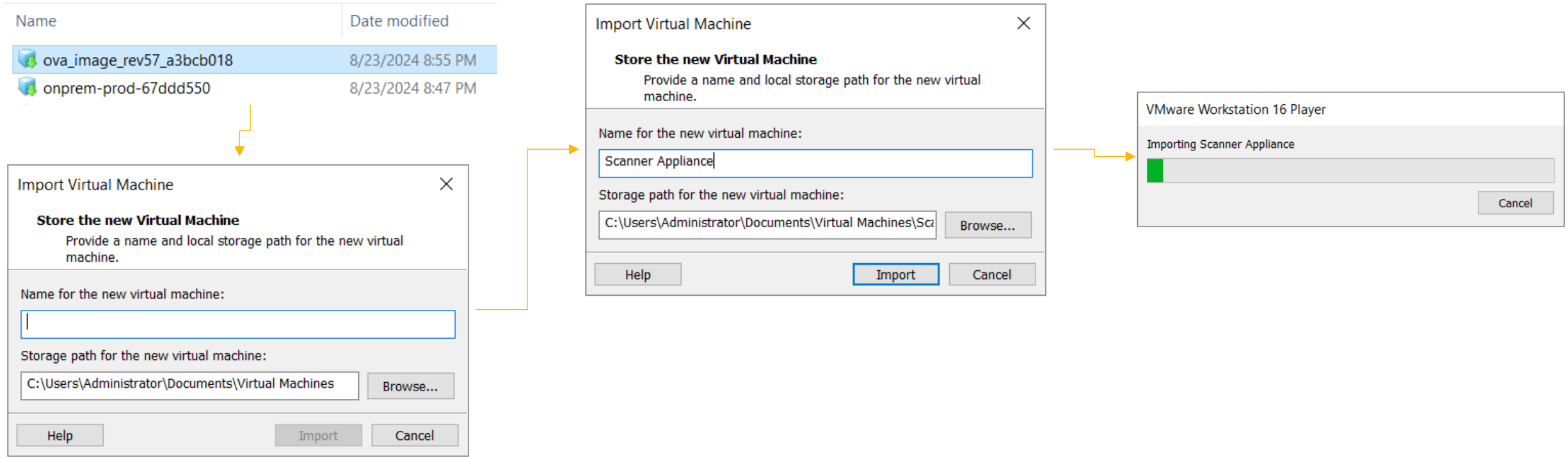


Note: Simulating an import process of the Core Engine image using VMWare Workstation Player 16

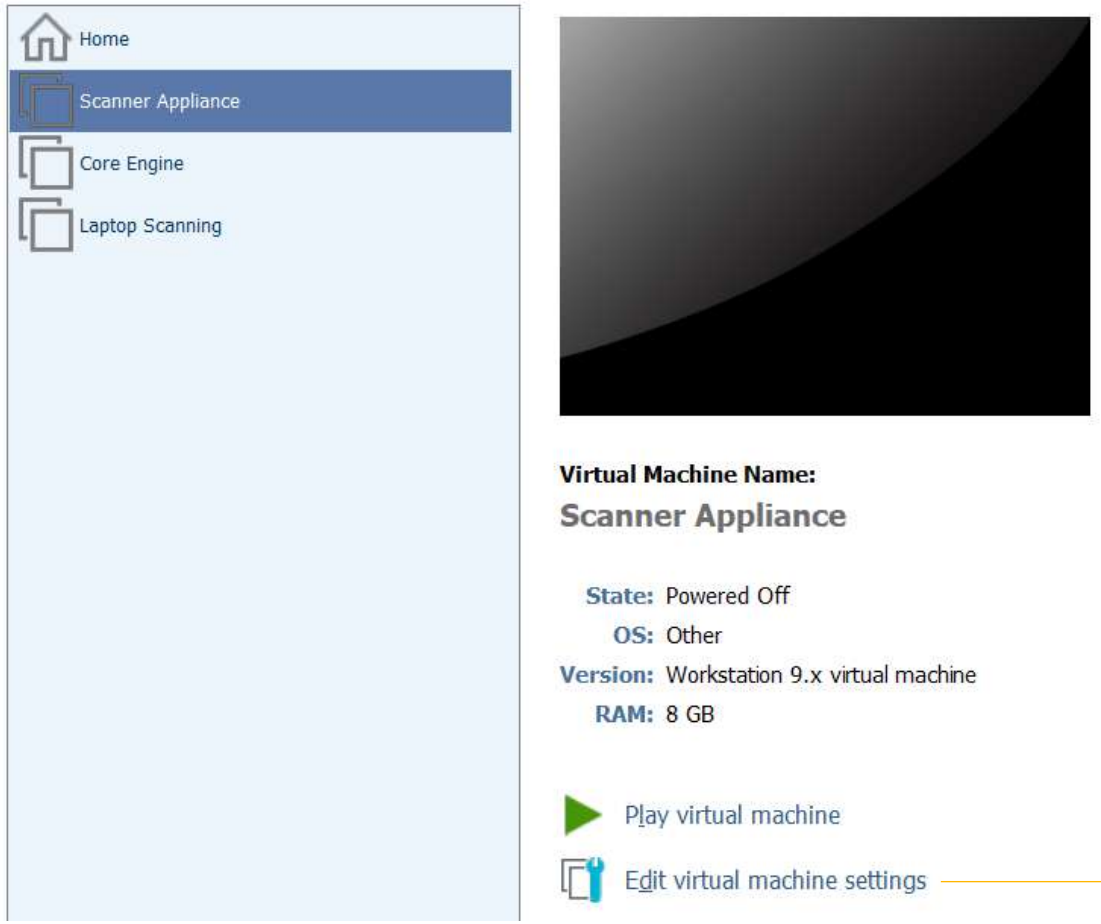
Open a Virtual Machine

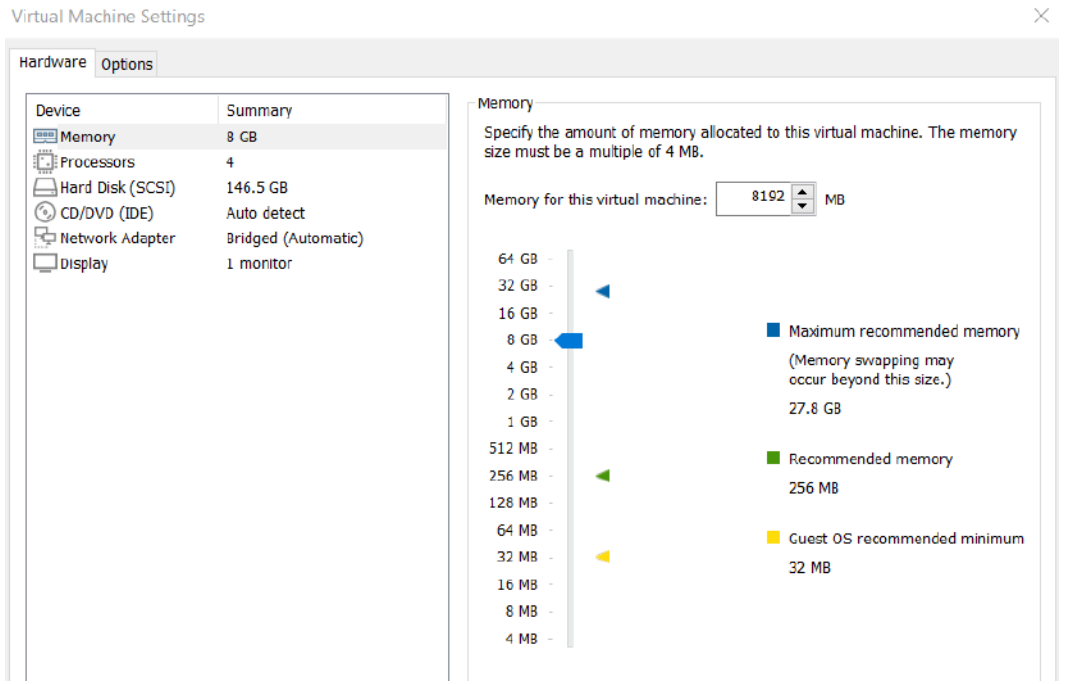
OTD BİLİŞİM GLOBAL VAD

SCANNER APPLIANCE: IMPORT

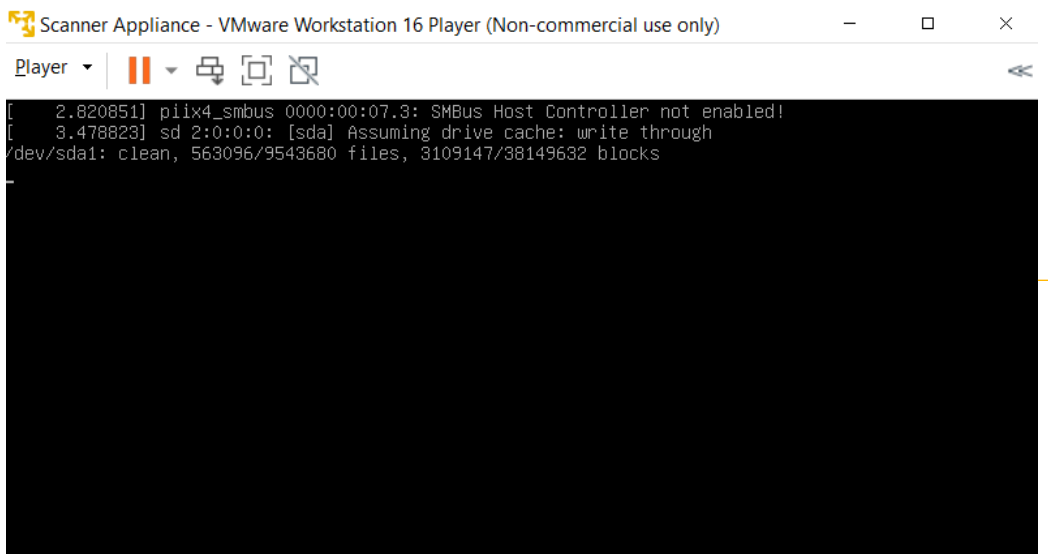


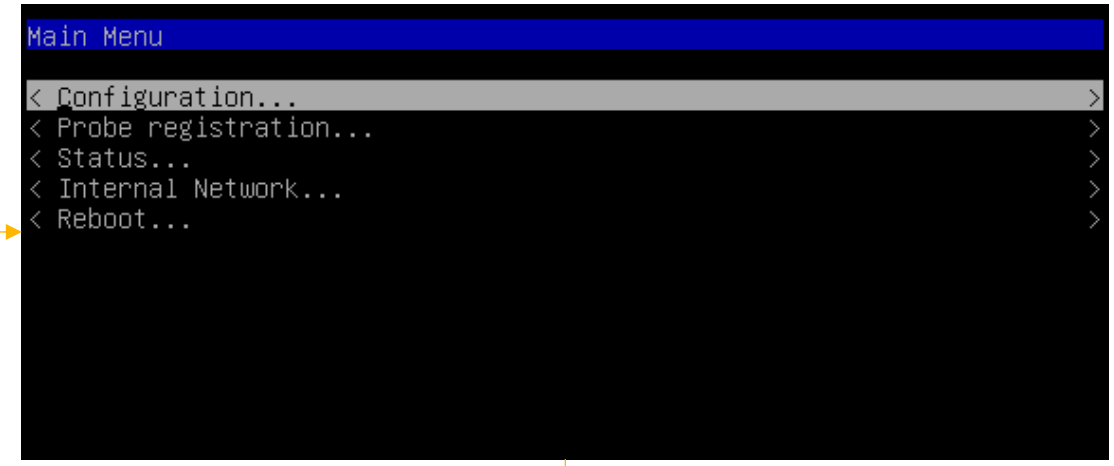
SCANNER APPLIANCE: SETUP

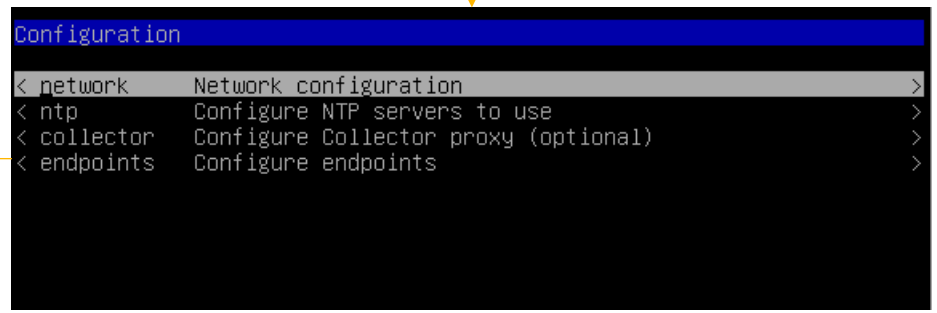


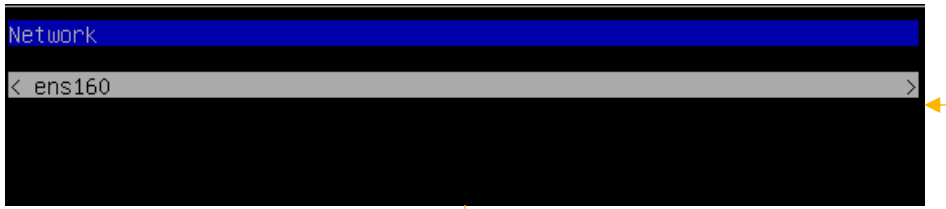


SCANNER APPLIANCE: NETWORK SETUP



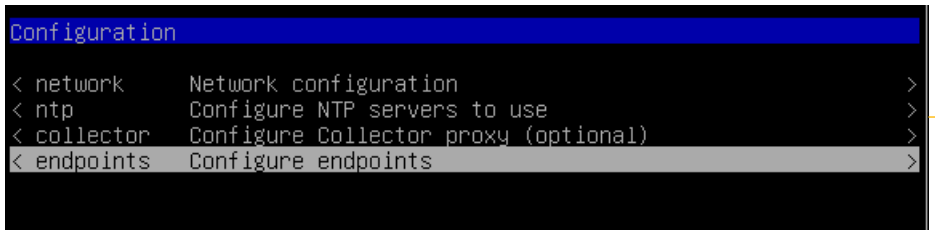


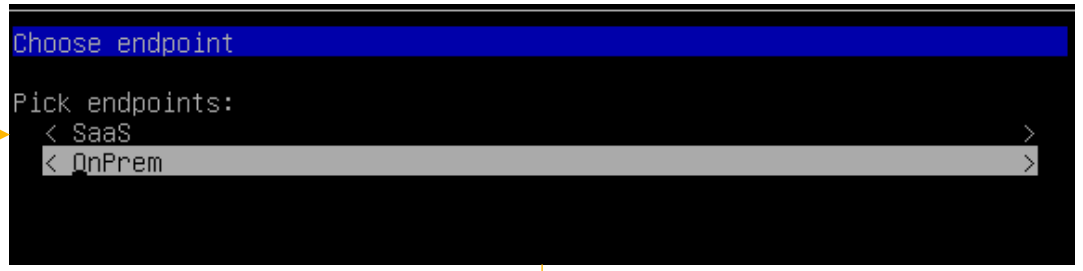


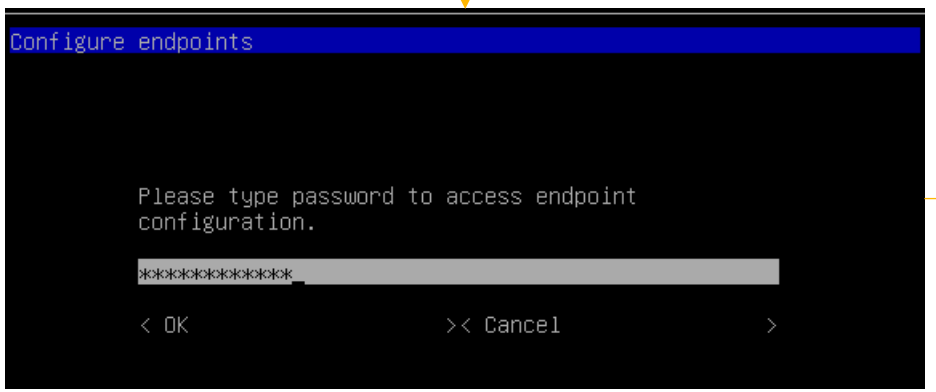


Note: This simulation is based on DHCP for the IP

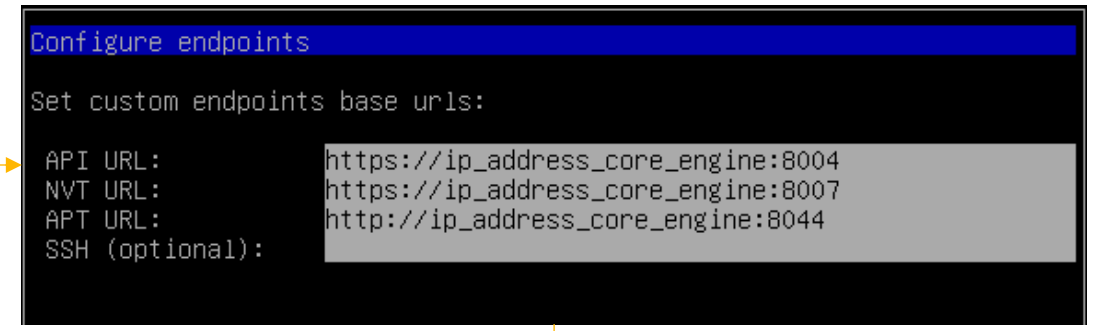
SCANNER APPLIANCE: ENDPOINT SETUP

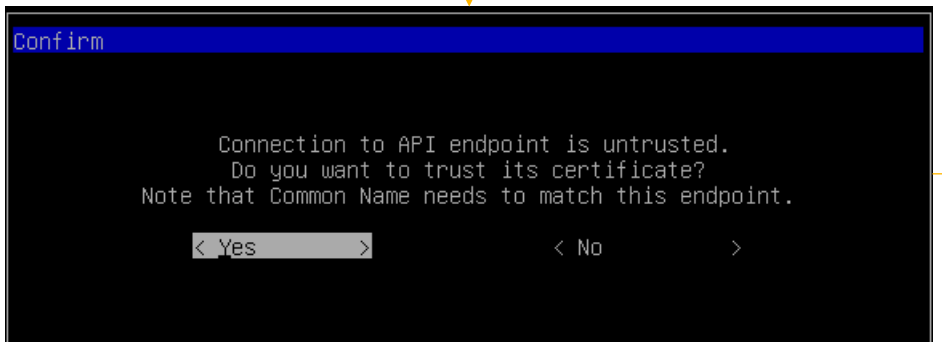






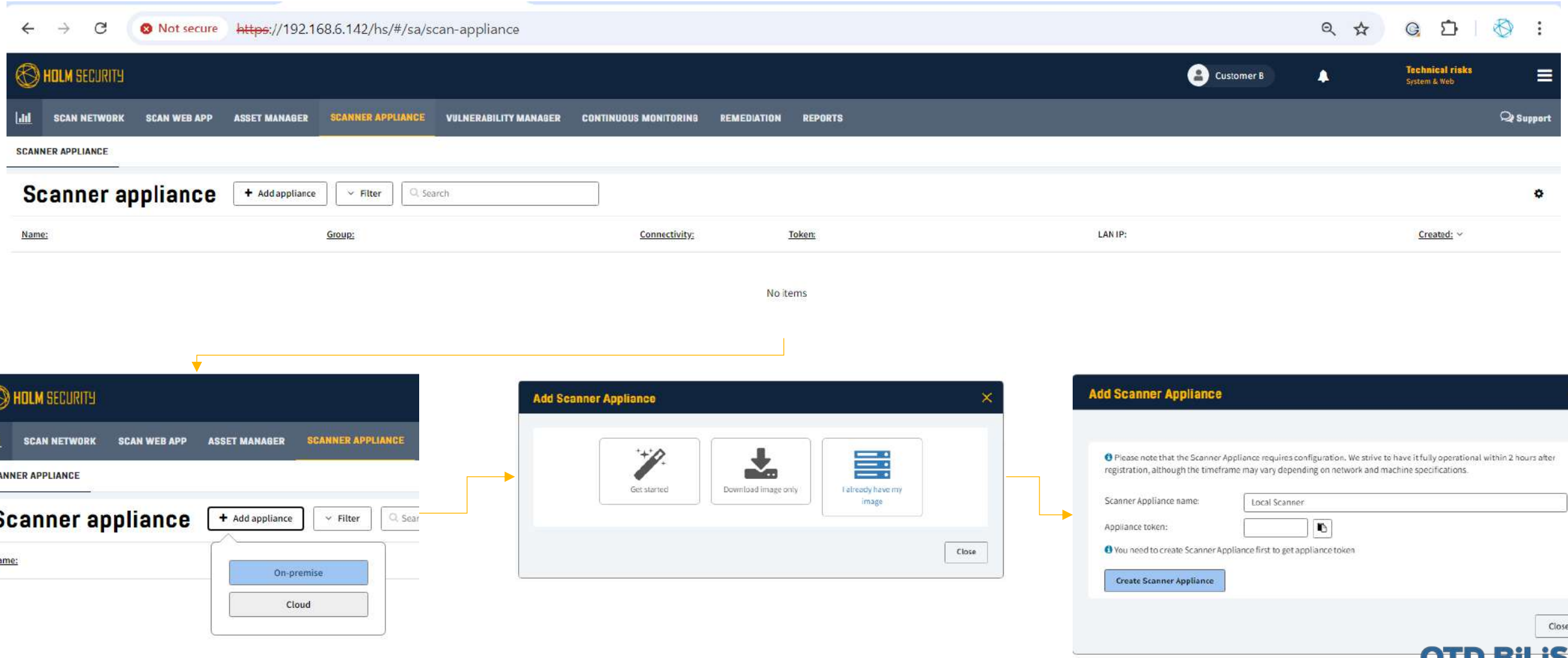
Password:
appliancebox



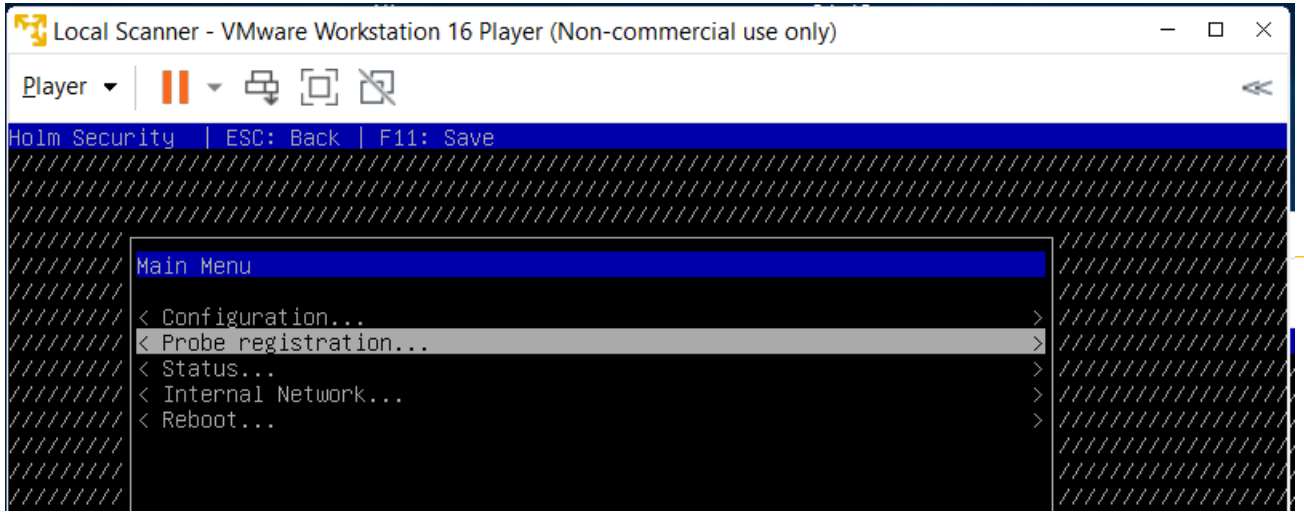


SECURITY CENTER: TOKEN KEY CREATION

- You need to generate the Scanner Appliance token key for the Probe Registration



SCANNER APPLIANCE: PROBE REGISTRATION



OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Next-Gen Vulnerability Management

We help you stay one step ahead of cybercriminals by identifying vulnerabilities across your cyber security defenses by covering all your technical and human assets.

Thank You
Q&A

Andrew Chee
andrew.chee@holmsecurity.com

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

System & Network Security

Finds over 200,000 vulnerabilities across all your technical assets, using a wide range of assessment capabilities.

Asset discovery & monitoring

Integrated ASM and EASM that automatically discover assets to identify blank spots and shadow IT.

Covers your entire infrastructure

Supports asset discovery and monitoring, as well as finding vulnerabilities in both internet-facing and local networks.

Finds outdated software & misconfigurations

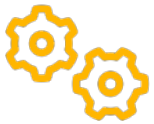
Finds vulnerabilities, outdated software, and much more.

Comprehensive assessment capabilities

Supports multiple assessment capabilities, such as unauthenticated and authenticated scanning, CIS Benchmarks, and local scanners for cloud-native platforms.

Supports the entire workflow

Our Security Center provides one pane of glass for discovery, prioritization, remediation, and reporting.

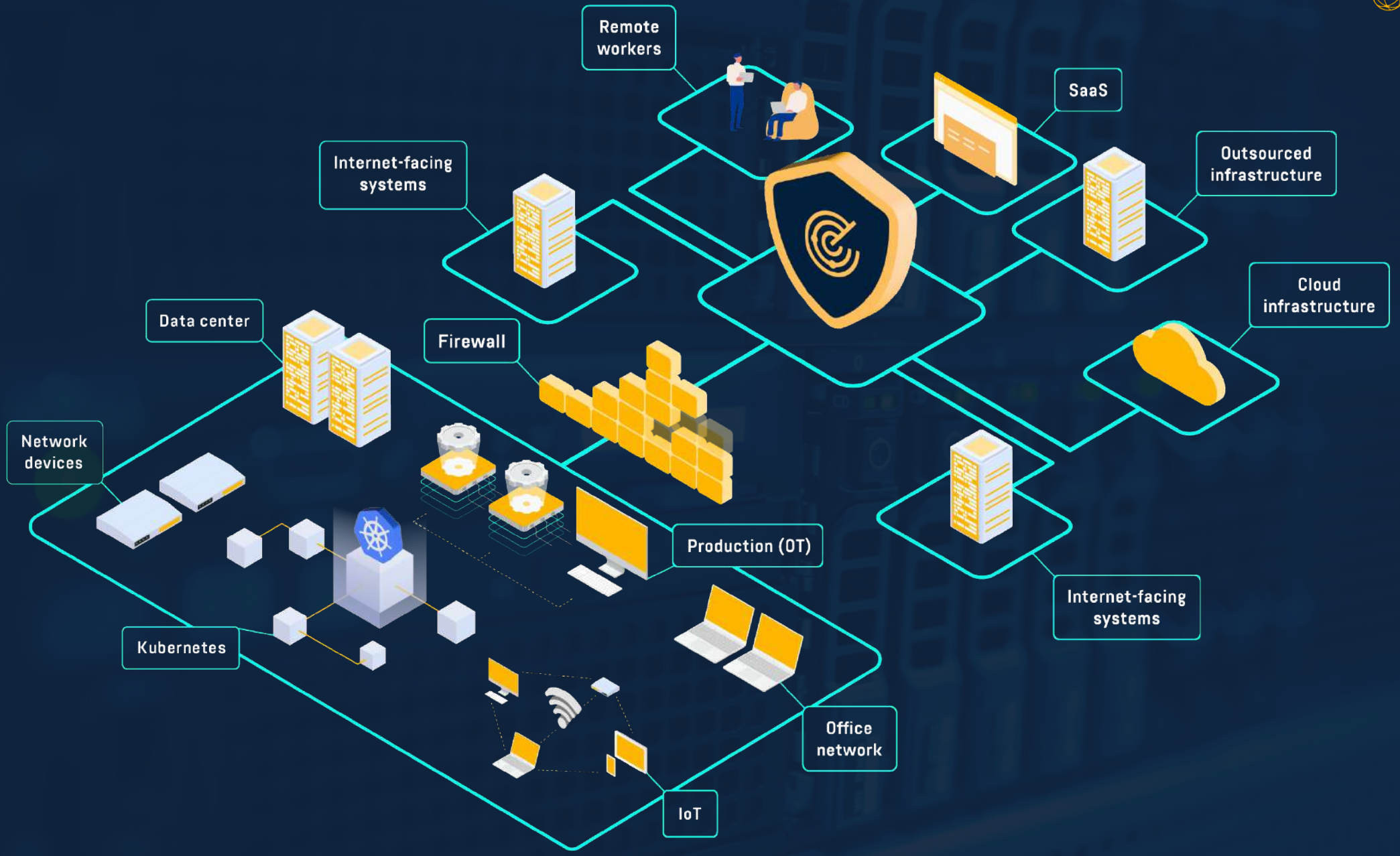


Fully automated

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

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY



Attack vector coverage

HOLM SECURITY

Vectors:	Description:
Systems/servers	OSs, software, and services for Microsoft, Linux, Unix, Mac, and other platforms.
Computers	Personal computers inside your office network and remote computers.
Network devices	Network equipment, such as firewalls, routers, and switches.
OT	Supervisory layer for Operational Technology systems within production and manufacturing.
IoT	Sensors, diagnostics, monitoring, and alarm systems.
Kubernetes	Cloud and on-prem orchestration platform for containers.
Cloud-native platforms	Cloud-native infrastructure in Azure, AWS, Google, and Oracle Cloud.
Office equipment	Printers, webcams, and other office devices.

Assessment technologies

Technologies:	Description:	Deployment method:	
		Cloud/SaaS:	On-premise:
Discovery scanning	Automated and continuous discovery and monitoring of assets running within a network.	✓	✓
Unauthenticated scanning	Scanning from the outside without access to the system, computer, or device.	✓	✓
Authenticated scanning	Authenticates against scanned targets and performs deeper analysis of vulnerabilities from installed applications and packages.	✓	✓
Cloud-native scanner	Local scanner (Scanner Appliance) for cloud-native platforms AWS, Azure, and Google Cloud.	✓	✓
CIS Benchmarks (policy scanning)	CIS Benchmarks best practices for the secure configuration of a target system. Holm Security is certified by Center for Internet Security (CIS).	✓	✓
Agent-based assessments	Windows-based lightweight endpoint extracting all software installed on a server or computer to find vulnerabilities.	✓	✗
Operational Technology (OT)	Assessment of mission-critical infrastructure and industrial systems.	✓	✓
PCI DSS ASV	Compliance scans according to the Payment Card Industry Data Security Standard (PCI DSS). Holm Security's platform is certified by PCI as an Approved Scanning Vendor (ASV).	✓	✓

Infrastructure capabilities

HOLM SECURITY

Capabilities:	Description:	Deployment method:	
		Cloud/SaaS:	On-premise:
Internet-facing/public networks	Perimeter scanning of systems and networks without any requirement for software, hardware or credentials.	✓	✓
Local networks	Scanner (Scanner Appliance) installed as a virtual appliance making it possible to simultaneously scan any number of local networks.	✓	✓
Cloud-native infrastructure	Scanning of cloud-based infrastructure with a local scanner (Scanner Appliance) for AWS, Azure, and Google Cloud.	✓	×
Remote computers	Agent-based assessment of Windows systems using our lightweight endpoint software agent (Device Agent).	✓	×

Vulnerability-finding capabilities

HOLM SECURITY

Capabilities:	Description:
Outdated software	Finds outdated operating systems, software, and services.
Weak passwords	Brute force logins using common usernames and passwords.
Misconfigurations	Finds misconfigurations, exposed ports, and services.
Blank spots & shadow IT	Gain instant visibility into your networks and systems.
Malware	Find known malware on scanned systems.
Exposed system information	Detect exposure of system and application information, such as php.info and system configs.
Faulty SSL certificates	Detects SSL certificates that are about to expire, have expired, or are vulnerable.
Weak encryption	Finds weak encryptions, including ciphers, versions, and protocols.

Deployment options

Options:	Description:
Cloud	Safe and secure management and storage in the cloud as SaaS.
On-premise	Installed and operating within your own infrastructure, with local data storage. No data is communicated over the internet.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Web Application Security

Find a wide range of vulnerabilities, such as OWASP Top 10, in your websites and web apps.

HOLM SECURITY

Comprehensive assessment capabilities

Finding vulnerabilities like CSR and 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 to scan web apps “behind” a login.

Modern web app support

Support scanning of modern JavaScript-empowered web applications.

Supports the entire workflow

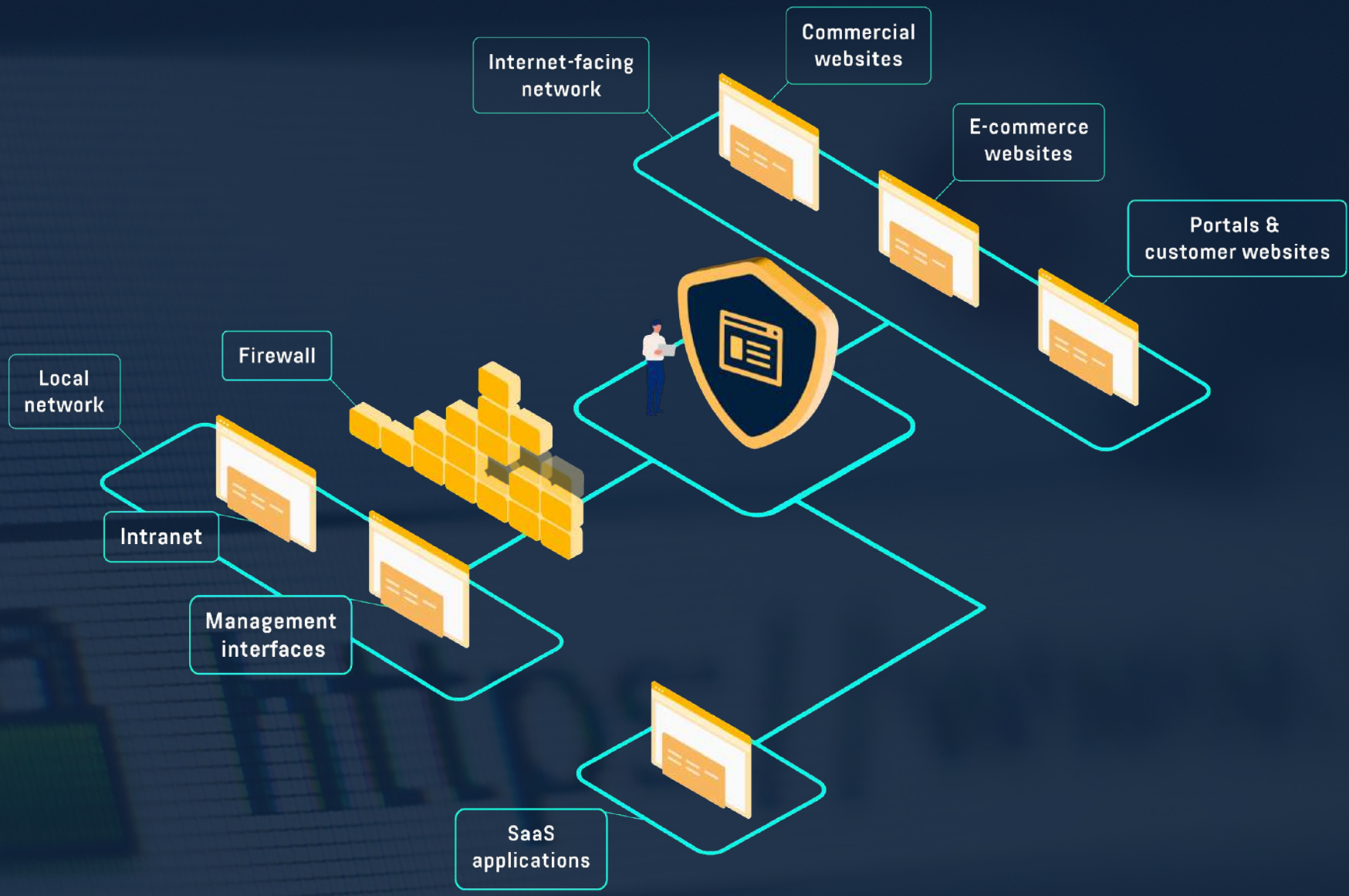
Our Security Center provides one pane of glass for discovery, prioritization, remediation, and reporting.

Fully automated

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

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY



Assessment technologies

HOLM SECURITY

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 popular frameworks such as AngularJS, VueJS, ReactJS, and more.
API vulnerabilities	Automatically detects SOAP API's and supports scanning REST API's such as those using OpenAPI v2 and v3.
CMS vulnerabilities	Finds vulnerabilities in CMSs such as WordPress and WordPress plug-ins.
Standard authentication support	Authenticate using Basic authentication, 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

HOLM SECURITY

Capabilities:	Description:
Misconfigured web servers	Find vulnerabilities like exposed directory listings 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

HOLM SECURITY

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 on 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.

Deployment options

Options:	Description:
Cloud	Safe and secure management and storage in the cloud as SaaS.
On-premise	Installed and operating within your own infrastructure, with local data storage. No data is communicated over the internet.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

API Security

Find vulnerabilities, such as OWASP API Top 10, in your APIs.

HOLM SECURITY

Comprehensive API technology coverage

Scan for threats across all your APIs including REST/OpenAPI, GraphQL, and SOAP.

Comprehensive vulnerability detection

Identify SQL injections, parameter, and type injection flaws in your API caused by improper validation of data.

Detect misconfigured servers

Finds misconfigurations in the server hosting the API.

OWASP API Top 10

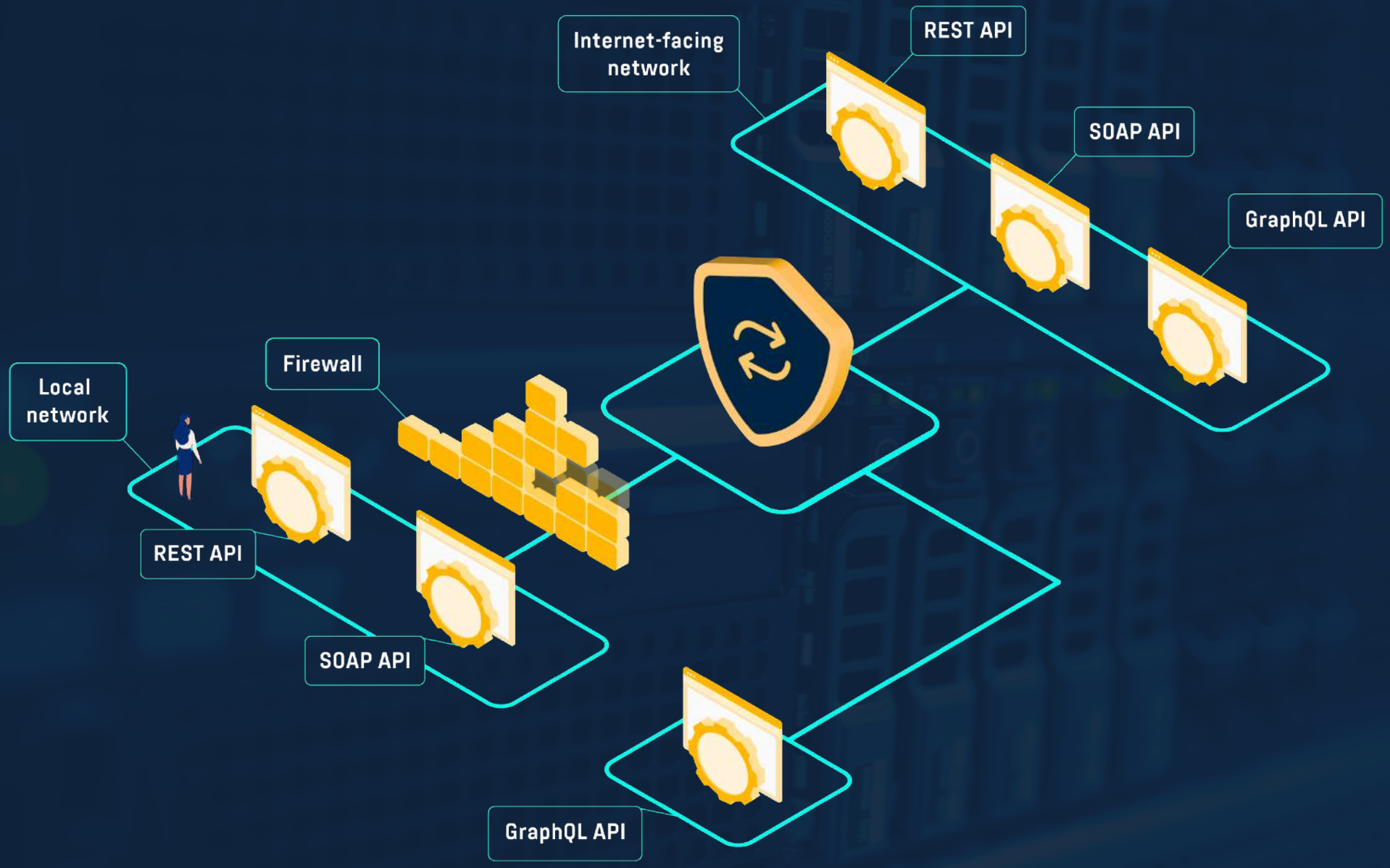
Find the most common API vulnerabilities with the most powerful compliance framework.

Supports the entire workflow

Our Security Center provides one pane of glass for discovery, prioritization, remediation, and reporting.

Fully automated

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


Internet-facing network
REST API
SOAP API
GraphQL API
Local network
Firewall
REST API
SOAP API
GraphQL API

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Cloud Security

Identify vulnerabilities across your cloud-native platforms with Cloud Security Posture Management (CSPM).

HOLM SECURITY

Cloud asset discovery & monitoring

Automatically discovers cloud assets with integrated ASM.

Multi-cloud support

Supports all major cloud-native platforms and Microsoft 365, providing a single pane of glass.

Detects cloud misconfigurations

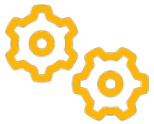
Gain complete visibility and actionable context related to misconfigurations in your cloud-native platforms.

Agentless

Assessment carried out by integrating with the cloud-native platforms. No software is required.

Supports the entire workflow

Our Security Center provides one pane of glass for discovery, prioritization remediation, and reporting.



Fully automated

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

OTD BİLİŞİM
GLOBAL VAD


OTD BİLİŞİM
GLOBAL VAD
HOLM SECURITY
ORACLE
Google Cloud
aws
Microsoft 365
Microsoft Azure

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Phishing Simulation & Awareness Training

Build your own human firewall to protect against phishing, ransomware, and other user-targeted attacks.

HOLM SECURITY

Fully automated sequences

Sequences of simulations, awareness training, and follow-up quizzes.

Modern awareness training

Automated and tailored nano-learning based on user behavior in phishing simulations.

Phishing simulation

Realistic out-of-the-box phishing scenarios and customizable templates.

Video material & quizzes

Built-in awareness videos and support to embed your own visual material. Ready-made interactive questionnaires for awareness verification.

Individual & team risk scoring

Follow the individual and team risk score over time to help plan additional efforts.

Out-of-the-box

Ready-made and customizable templates for simulations, awareness training, and questionnaires.

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Vulnerability management program

HOLM SECURITY

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

COMPLIANCE

ISO 27001

HOLM SECURITY

Requirements

Our solution

Risk assessment (§6.1.2)
ISO 27001 requires organizations to perform a risk assessment to identify and assess information security risks.

A market-leading platform for systematic, automated, and continuous risk assessments using Attack Surface Management (ASM) and vulnerability management. Our platform creates a foundation for proactive cyber defense for compliance.

Risk treatment (§6.1.2)
Once risks are identified, ISO 27001 mandates that organizations develop a risk treatment plan. Part of this plan may involve vulnerability management.

We support our customers in implementing a long-term risk treatment plan with our vulnerability management program.

Control selection (§6.1.3)
ISO 27001 provides a list of control objectives and controls in Annex A of the standard. Some of these controls are directly related to vulnerability assessment and management, such as:

- A.12.6.1 - Management of technical vulnerabilities
- A.14.2.7 - System vulnerability assessments
- A.14.2.8 - Remediation of technical vulnerabilities

We support finding technical vulnerabilities, as well as establishing a vulnerability management program, and supporting the process of remediating vulnerabilities.

Continuous improvement (§10.1)
ISO 27001 promotes a cycle of continuous improvement. Organizations are required to regularly review and update their risk assessment, risk treatment plan, and information security controls.

Vulnerability management plays a crucial role in this ongoing process by helping organizations stay informed about emerging vulnerabilities and adapting their security measures accordingly.

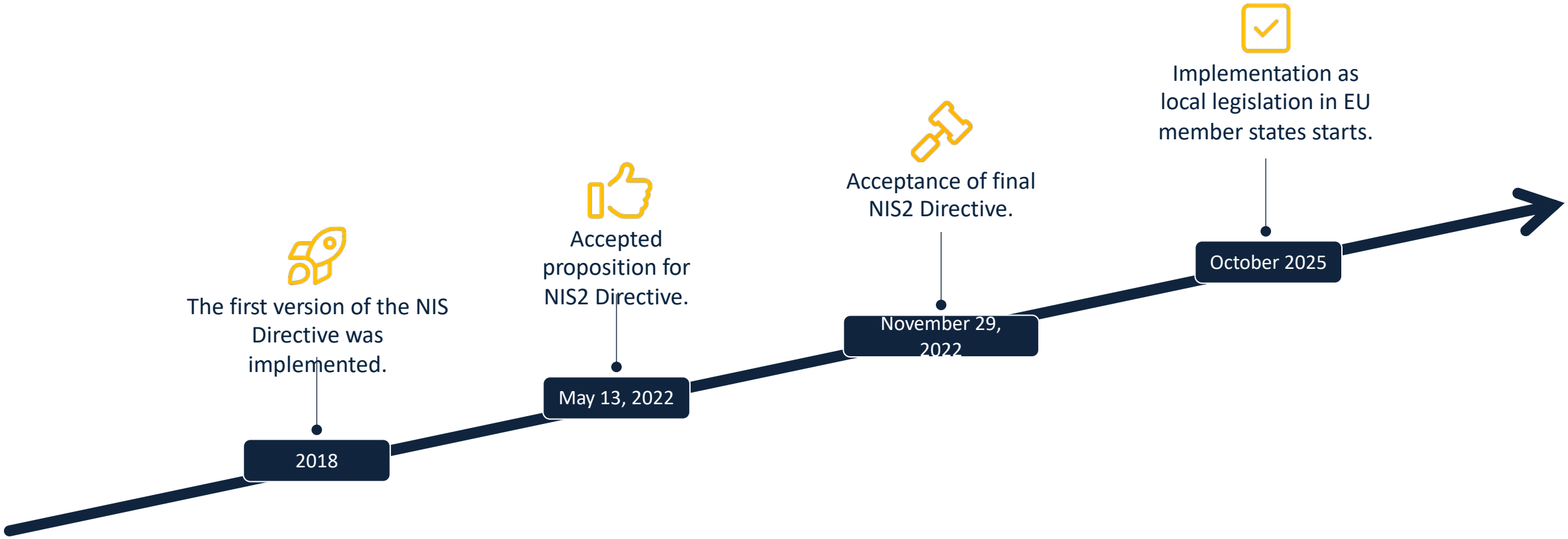
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

COMPLIANCE

NIS & NIS2

NIS MILESTONES



NIS2 SECTORS

HOLM SECURITY

Proactively monitored sectors report to designated supervisory authorities. Reactively monitored sectors report to the regulator on request.

Essential entities

Proactive supervision

- Energy
- Wastewater
- Healthcare
- Drinking water supply & distribution
- Banking
- Financial market
- Digital infrastructure
- Transportation
- Space
- Public administration

Important entities

Reactive supervision

- Waste management
- Digital distributors
- Postal & courier services
- Chemicals production, processing & distribution
- Production & manufacturing
  - Medtech products
  - Computers, electronics, and optics
  - Electrical appliances
  - Industrial machines
  - Motor vehicles
  - Other transports
- Food production, processing & distribution

OTD BİLİŞİM GLOBAL VAD

Requirements

Our solution

HOLM SECURITY

Requirements	Our solution
Systematic and risk-based Take systematic, analytical, and risk-based steps within information security and perform risk assessments.	A market-leading platform for systematic, automated, and continuous risk assessments using Attack Surface Management (ASM) and vulnerability management. Our platform creates a foundation for proactive cyber defense and NIS2 compliance.
Risk assessments Perform risk assessments during the implementation phase as well as during daily maintenance work.	Automated risk assessments in the initial phase of NIS2 compliance and continuously thereafter.
Cyber hygiene Implement basic cyber hygiene practices and cyber security training.	Strengthen the human defense against phishing attacks using phishing simulation in combination with tailored and automated awareness training.
Supply chain assessments As risk assessments are a key factor of NIS2 compliance, it will be a requirement for your suppliers to conduct such assessments.	Our platform allows our customers, as well as their suppliers, to perform continuous risk assessments.
Demonstrate compliance Be able to demonstrate compliance today and in the future.	An unlimited archive of reports and vulnerability data shows compliance historically and today.

More solutions

Requirements

Our solution

HOLM SECURITY

Supervise
Management supervises the implementation of risk management.

Fully automated process for management to supervise continuous risk assessments based on easy-to-consume statistics and data, as well as automated reporting. Our platform describes in detail how your organization's exposure develops over time.

Avoid penalties
Avoid administrative sanctions, lost permits, certifications, and penalties.

Protect your most business-critical assets by proactively and automatically identifying vulnerabilities and blank spots.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

NIS2 applies directly and indirectly

Essential and Important entities must secure their entire supply chain.

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

USE CASES

Operational Technology

The Stuxnet worm sabotage

- The malicious computer worm was first officially uncovered in 2010.
- Used to attack a uranium enrichment facility at Iran’s nuclear site.
- Destroyed almost one-fifth of Iran's nuclear centrifuges.
- The worm infected over 200,000 computers and caused 1,000 machines to physically degrade.

Ukrainian power grid hack

- In 2015 and 2016, cyberattacks on the power grid cut electricity to nearly a quarter million Ukrainians.
- Shut off power to 30 substations, leaving around 230,000 people without electricity for up to six hours.
- SCADA equipment wasn't working and power restoration had to be done manually.

OPERATIONAL TECHNOLOGY

Market-leading coverage for the supervisory layer

OPERATIONAL TECHNOLOGY

HOLM SECURITY

Supervisory layer

Computers (software), network data communications, and Human-Machine Interface (HMI).

Full coverage for the supervisory layer and all layers above.

Control layer

PLCs/RTUs, PIDs, and DCS.

Partial coverage for the control layer.

Field layer

Sensors, pumps, actuators, valves, engines, and other peripherical devices.

OTD BİLİŞİM GLOBAL VAD

OPERATIONAL TECHNOLOGY

HOLM SECURITY

Schneider Electric
ABB
SIEMENS
Honeywell
General Electric
westermo
MITSUBISHI ELECTRIC
Circutor
Rockwell Automation
YOKOGAWA

75+ vendors covered

Major coverage of OT vendors.

3,650+ vulnerabilities covered

Comprehensive OT vulnerability test coverage.

OTD BİLİŞİM GLOBAL VAD