



HOLM SECURITY

Siber Güvenlik Risklerinizi Proaktif ve Kolay bir Şekilde Önceliklendirir

WATERSCHAP ZUIDERZEELAND

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

MÜŞTERİ ÖRNEKLERİ

1.000+
Müşteri

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

Platformumuz en önemli varlıklarınızı korur

Riskler	Olaylar	Zarar
Phishing saldırıları	Üretim kesintileri / azalan verimlilik	Zedelenmiş marka itibarı ve güven
Fidye Yazılımı	Veri sızıntısı ve veri kaybı	Ekonomik zarar
Sızma	Yasal düzenlemelere ve mevzuata uyumsuzluk	Yaşam ve sağlık için riskler
İzinsiz giriş Operasyonel aksaklıklar ve sabotaj		

Proaktif siber savunma eksikliği

Tespit Et	Koru	Tespit Et	Müdahale Et	Geri Yükle
Penetrasyon Testi	Antivirüs			Yedekleme ve Kurtarma
Güvenlik Açığı Yönetimi	Firewalls	SIEM Güvenlik Bilgisi ve Olay Yönetimi		
	Phishing ve Güvenlik Farkındalığı		SOC Siber Güvenlik Operasyon Merkezi	
	EDR/XDR/MDR			

Kaynak: NIST Siber Güvenlik Çerçevesi

HOLM SECURITY

Saldırganın bakış açısını elde edin

Siber suçlular sistemlerinize aktif olarak sızmaya çalışsa, sizi bir phishing saldırısıyla hedef alsa veya ransomware yaymaya çalışsa, kuruluşunuz ne kadar güvende?

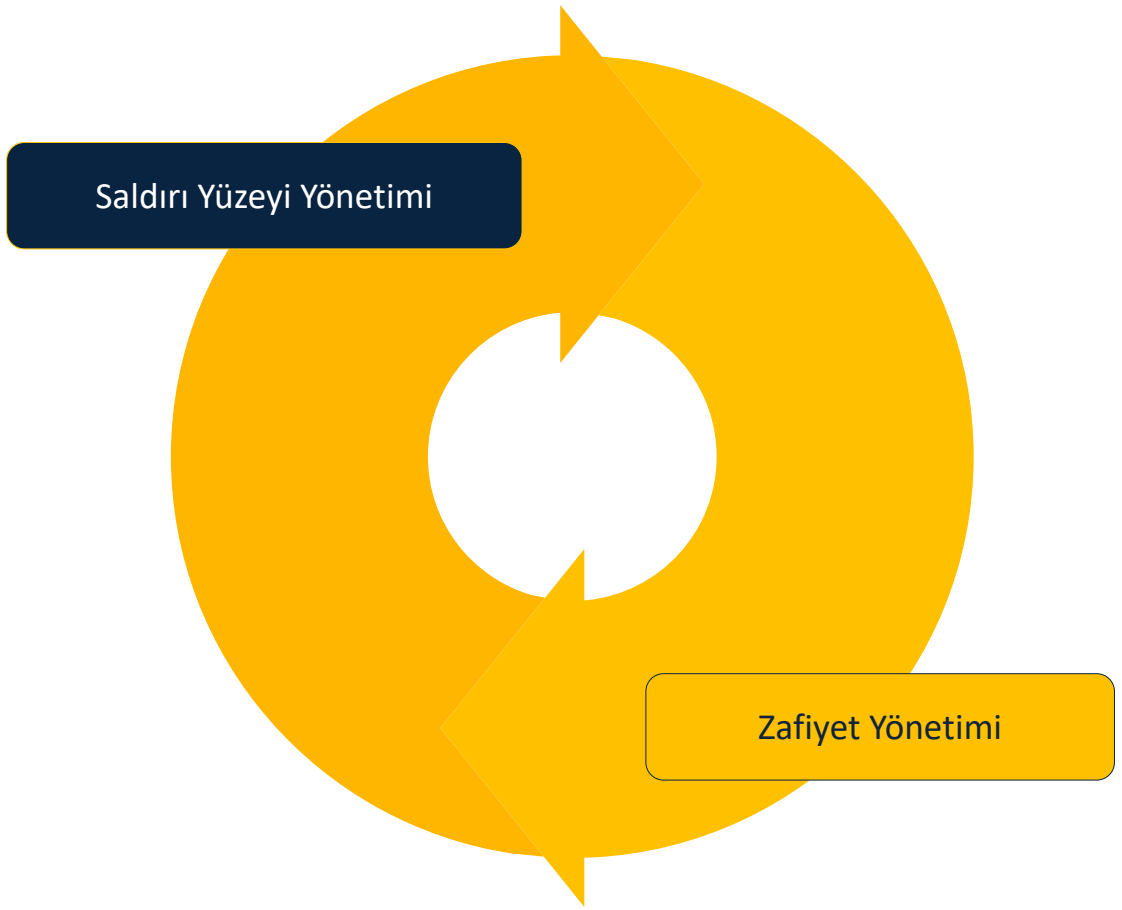
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Tüm önemli saldırı vektörlerini korur

Hepsi bir arada platformumuz, tüm kritik saldırı vektörlerindeki zafiyetleri tespit eder - yönetilmeyen sistemler dahil.

OTD BİLİŞİM GLOBAL VAD



Entegre ve otomatik Saldırı Yüzeyi Yönetimi

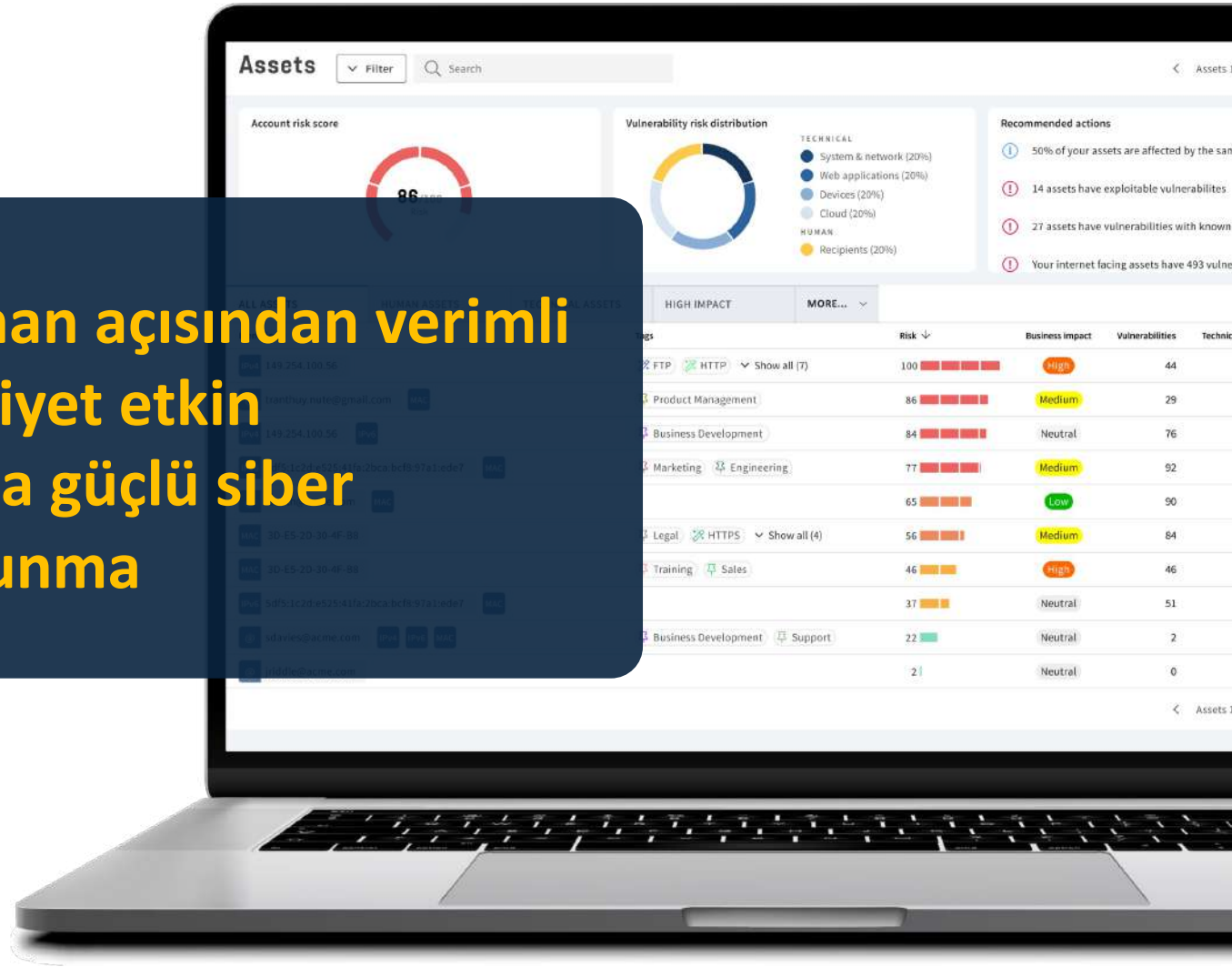
Sistemler, web, alan adları ve bulut yerel platformlardaki varlık keşfi ve varlık değişikliklerinin izlenmesi için Entegre Saldırı Yüzeyi Yönetimi (ASM) ve Harici Saldırı Yüzeyi Yönetimi (EASM)

HOLM SECURITY

1 Platform
İş Akışı
Risk modeli

→

Zaman açısından verimli
Maliyet etkin
Daha güçlü siber savunma



OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Gelecekteki çalışmalar için mükemmel hazırlık

Sızma testi ve SOC kurulumu gibi diğer siber güvenlik çalışmalarını zaman ve maliyet açısından daha verimli hale getirir.

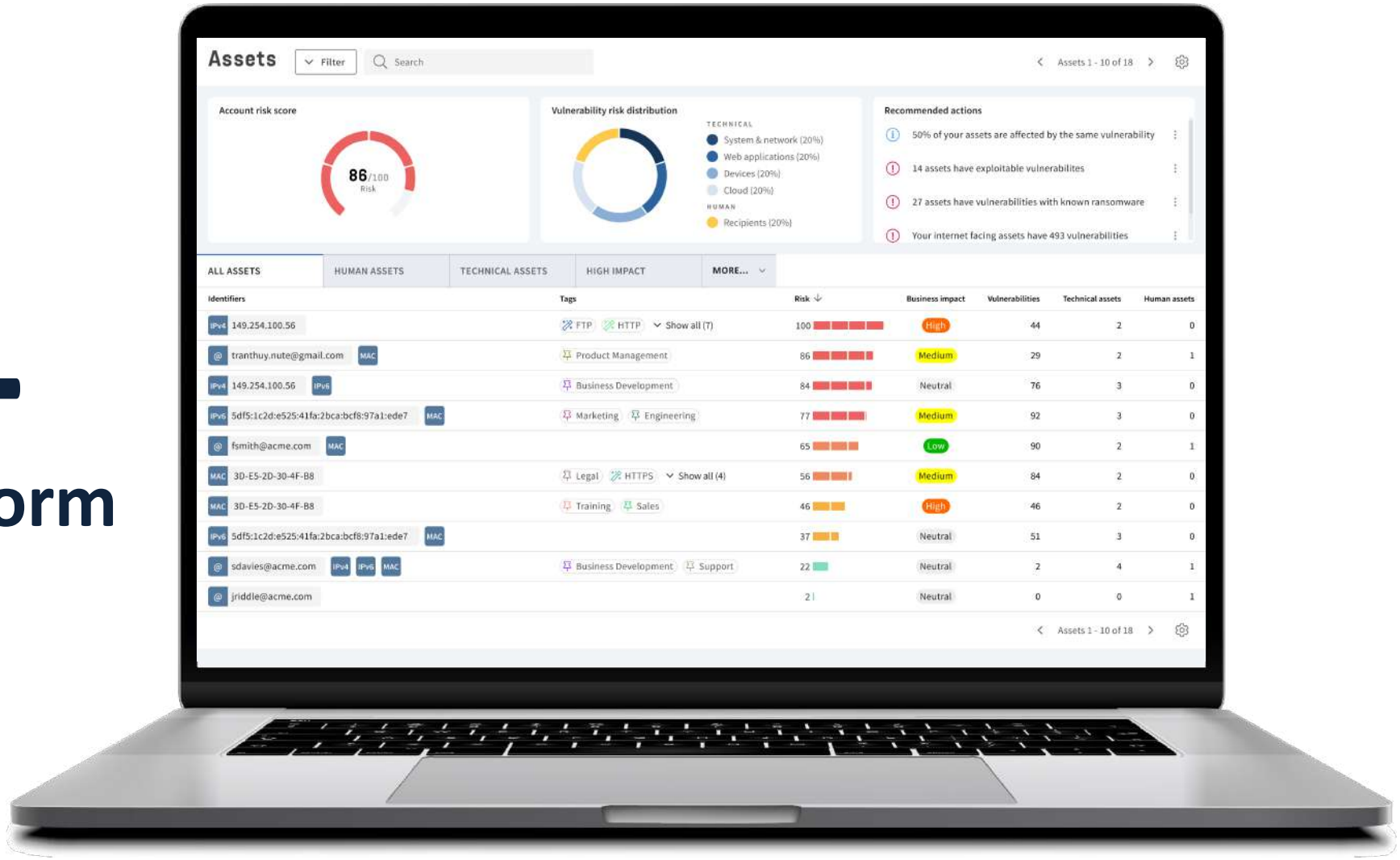
OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

TAM ENTEGRASYON

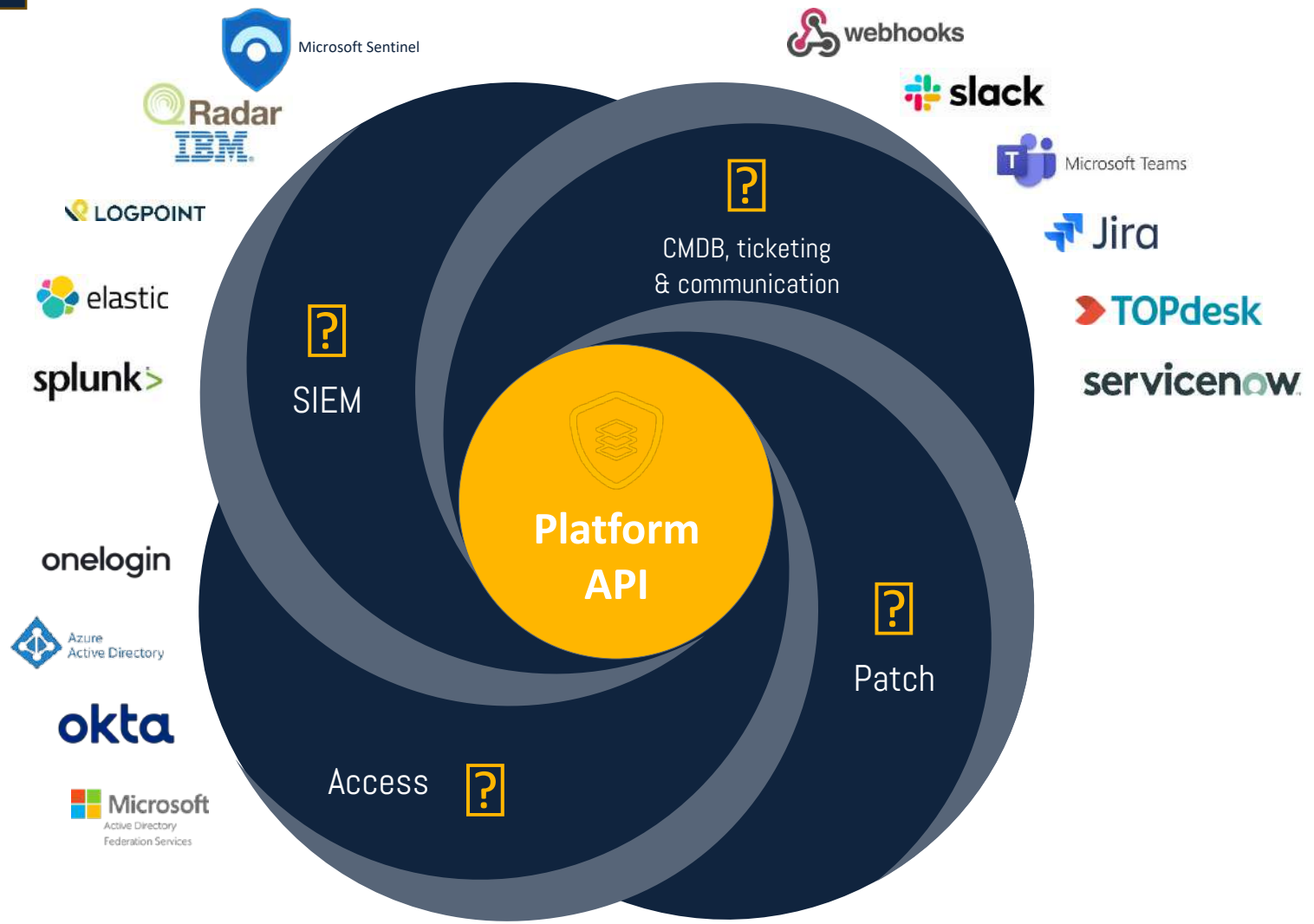
4 → 1

ürünler **platform**



OTD BİLİŞİM GLOBAL VAD

HAZIR ENTEGRASYONLAR



HOLM SECURITY

PROFESYONEL SERVİSLER

Uzmanlarımızla hedeflerinize hızlı ve güvenli şekilde ulaşın.

Eğitim Merkezi

Başarı Programları

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

Yasal gereksinimleri karşılamaya yönelik çalışmalarınızı destekler

NIS/NIS2, DORA, GDPR, CRA, ISO 27001 gibi standartlara uyum için sistematik ve risk odaklı bir siber savunmaya doğru büyük bir adım.

OTD BİLİŞİM GLOBAL VAD

NIS2'nin gerektirdiği **operasyonel yetkinliklere** sahip misiniz?

ENISA, NIS2 uyumluluğu için zafiyet yönetimini önermektedir

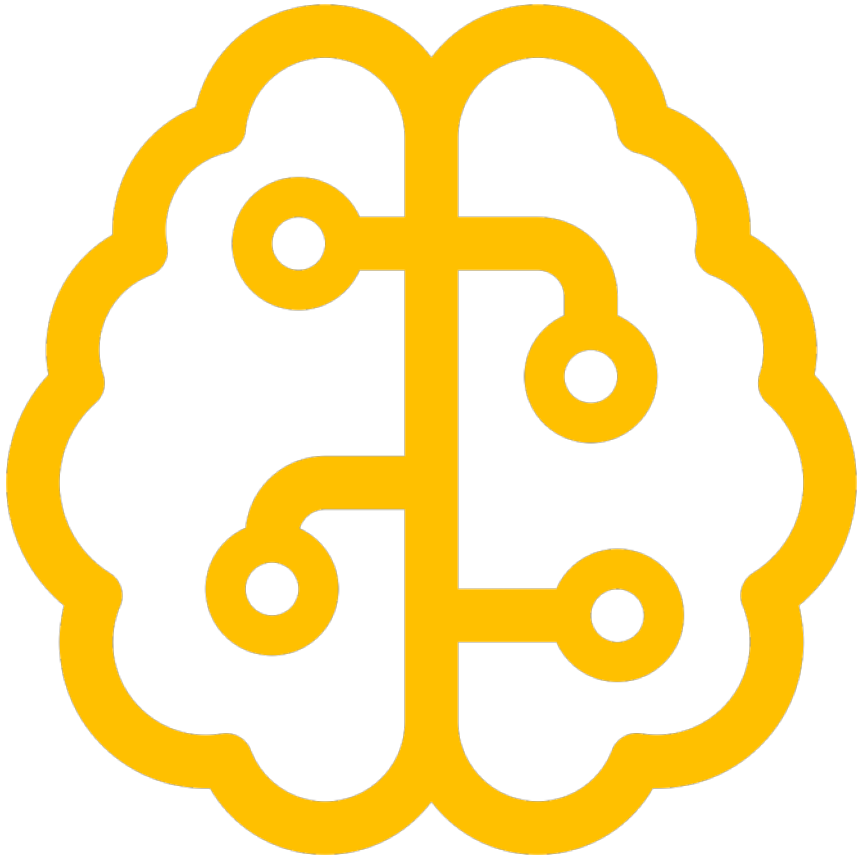
Dış kaynak iş ortağınızla **birlikte çalışın**

Dış kaynak iş ortağınızın SLA'sını kıyaslayın ve zafiyetleri gidermek ile risk maruziyetini azaltmak için birlikte çalışın.

HOLM SECURITY

Yapay zeka destekli tehdit istihbaratı

Yapay Zeka Destekli Güvenlik Araştırma Ekibimiz, en güncel güvenlik açıkları hakkında sizi güncel tutar – 7/24, yıl boyunca.



OTD BİLİŞİM GLOBAL VAD

Riski etkin şekilde ölçün ve iletin

Riski hem kurum içinde hem de kurum dışında ölçmek ve iletmek için ihtiyaç duyduğunuz tüm araçları sunuyoruz.

Risk maruziyetini kıyaslayın

Kuruluşunuzun risk maruziyetini, aynı sektördeki diğer kuruluşlarla karşılaştırarak anlayın.

HOLM SECURITY

Her ölçekteki IT departmanları için otomasyon

Küçük ölçekli kuruluşlardan büyük ölçekli kuruluşlara kadar uyum sağlayan bir platform.

Sadece birkaç saat içinde kullanmaya başlayın

Ajan gerektirmeyen kurulum ile saatler içinde kullanıma hazır hale gelin.

Her adımda profesyonel destek

Zafiyet yönetimi programınızın siber savunmanızı başarıyla güçlendirmesini sağlar.

OTD BİLİŞİM GLOBAL VAD

Proaktif olun

Siber güvenliğe sistematik, risk odaklı ve proaktif bir yaklaşım oluşturur.

HOLM SECURITY

Kanıtlanmış teknoloji
Kuruluşunuza değer sağlayan, tanınmış ve kanıtlanmış bir teknoloji.

Hepsi bir arada platform
Tüm önemli saldırı vektörlerini kapsar – tek bir iş akışı ve tek bir risk modeli.

Otomatik
Ekibinize minimum iş yükü ekleyen otomatik platform.

Uyumluluğu destekler
Mevcut ve yaklaşan yasal gereksinimleri karşılamada önemli bir bileşen.

Ölçün, karşılaştırın ve raporlayın
Kuruluşunuzun güvenlik seviyesini etkin şekilde ölçün, kurum içinde raporlayın ve diğer kuruluşlarla karşılaştırın.

Uzman desteği
Uzman desteğimiz, ilerleme sağlamanızı ve yaptığınız yatırımın değerli olmasını garanti eder.

Anında başlayın
Sadece birkaç saat içinde anında sonuçlarla kullanmaya başlayın.

Mükemmel bir hazırlık
Diğer siber güvenlik çalışmalarını daha verimli ve maliyet etkin hale getirir.

Güvenilir bir iş ortağı
En yüksek seviyede güvenlik, veri gizliliği ve güvenilirlik sunan Avrupalı bir sağlayıcı.

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi

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

1,400+ customers

70 FTEs

100% recommendations in 2024
Gartner

HOLM SECURITY

Finans, Sigorta ve Bankacılık

Medikal teknoloji ve sağlık hizmetleri

Kamu kurumları

Kritik altyapı

Gıda ve içecek üretimi

Üretim ve imalat

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi

Saldırı yüzeyinizi minimize edin

Saldırı yüzeyinizi izleyin ve minimize edin, kör noktaları tespit edin.

Tüm saldırı vektörleri tek bir platformda

Tüm önemli saldırı vektörlerindeki riskleri tespit eden kapsamlı bir çözüm.

Gerçek birleşik yapı ile tüm riskler tek bir platformda

Etkin önceliklendirme ve iyileştirme için tüm riskleri tek bir ekranda sunan merkezi bir görünüm.

Yapay zeka destekli tehdit istihbaratı

Daha hızlı ve geniş kapsamlı risk kapsaması için yapay zeka ve daha iyi risk önceliklendirmesi için veri zenginleştirme.

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi Platformu

Saldırı yüzeyi

Harici Saldırı Yüzeyi (EASM)

Üçüncü taraf (tedarikçiler)

Saldırı vektörleri

- İş açısından kritik sistemler / sunucular
- Bilgisayarlar ve ofis ekipmanları
- Ağ cihazları
- IoT
- Kubernetes
- OT
- Web uygulamaları
- APIs
- Bulut yerel platformlar
- Microsoft 365
- Kullanıcılar

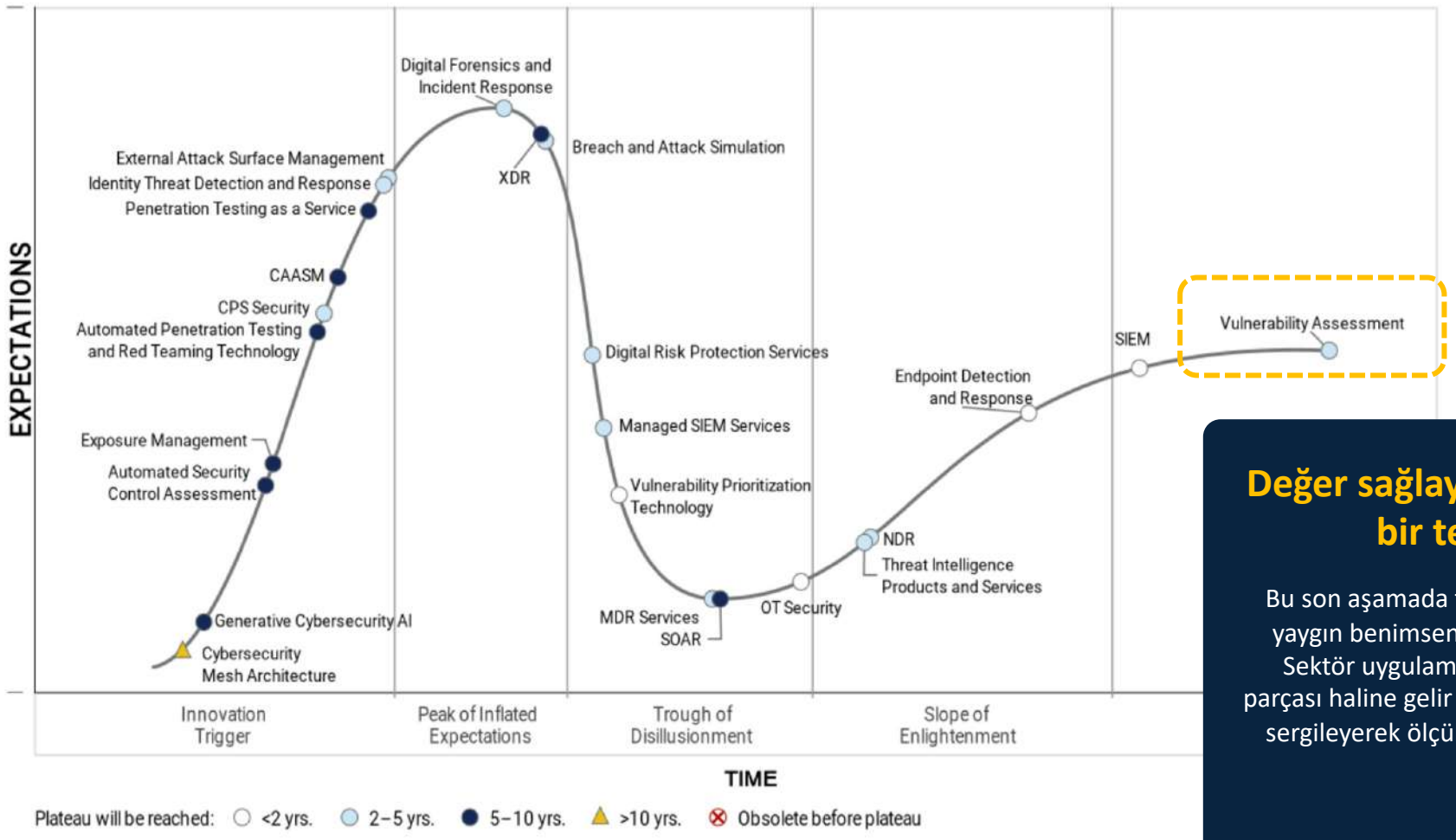
Ürünler

- **Sistem ve ağ güvenliği**
- **Web uygulama güvenliği**
- **API Güvenliği**
- **Bulut Güvenliği**
- **Phishing simülasyonu ve farkındalık eğitimi**

Gartner

HOLM SECURITY

Hype Cycle for Security Operations, 2023



Değer sağlayan kanıtlanmış bir teknoloji

Bu son aşamada teknoloji, olgunluk ve yaygın benimsenme seviyesine ulaşır. Sektör uygulamalarının ayrılmaz bir parçası haline gelir ve istikrarlı performans sergileyerek ölçülebilir iş değeri sağlar.

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

ÖRNEK: KURUMSAL KURULUM

Yerel tarayıcılar ve veri toplayıcılar

Yerel proxy

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Bulut VMP

HAZIRLIK KONTROL LİSTESİ

HOLM SECURITY

Müşteri

- **Sanallaştırma Platformu**
  - Sanal Tarayıcı Cihazı için VM ESXi, VM Workstation, VM Player, Oracle VirtualBox, KVM vb.

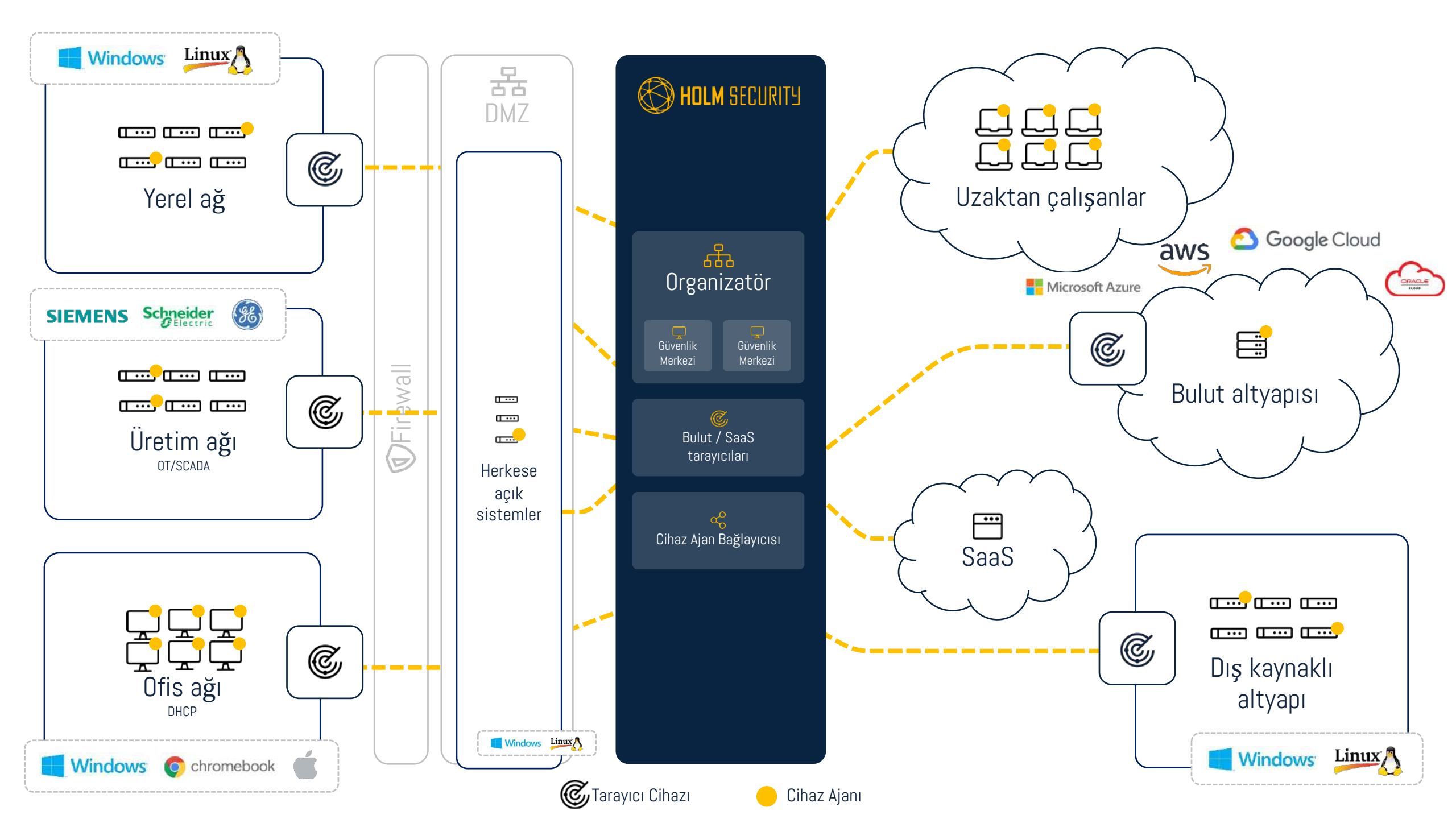
- **İmajları indirin**
  - Sanal Tarayıcı Cihazı

- **Ağ yapılandırması**
  - Edge Firewall Politikası (Giden Trafik)
  - İç Firewall Politikası (Core Engine ile Sanal Tarayıcı Cihazı arasında), varsa
  - Sanal Tarayıcı Cihazı için özel statik IP

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Mimari

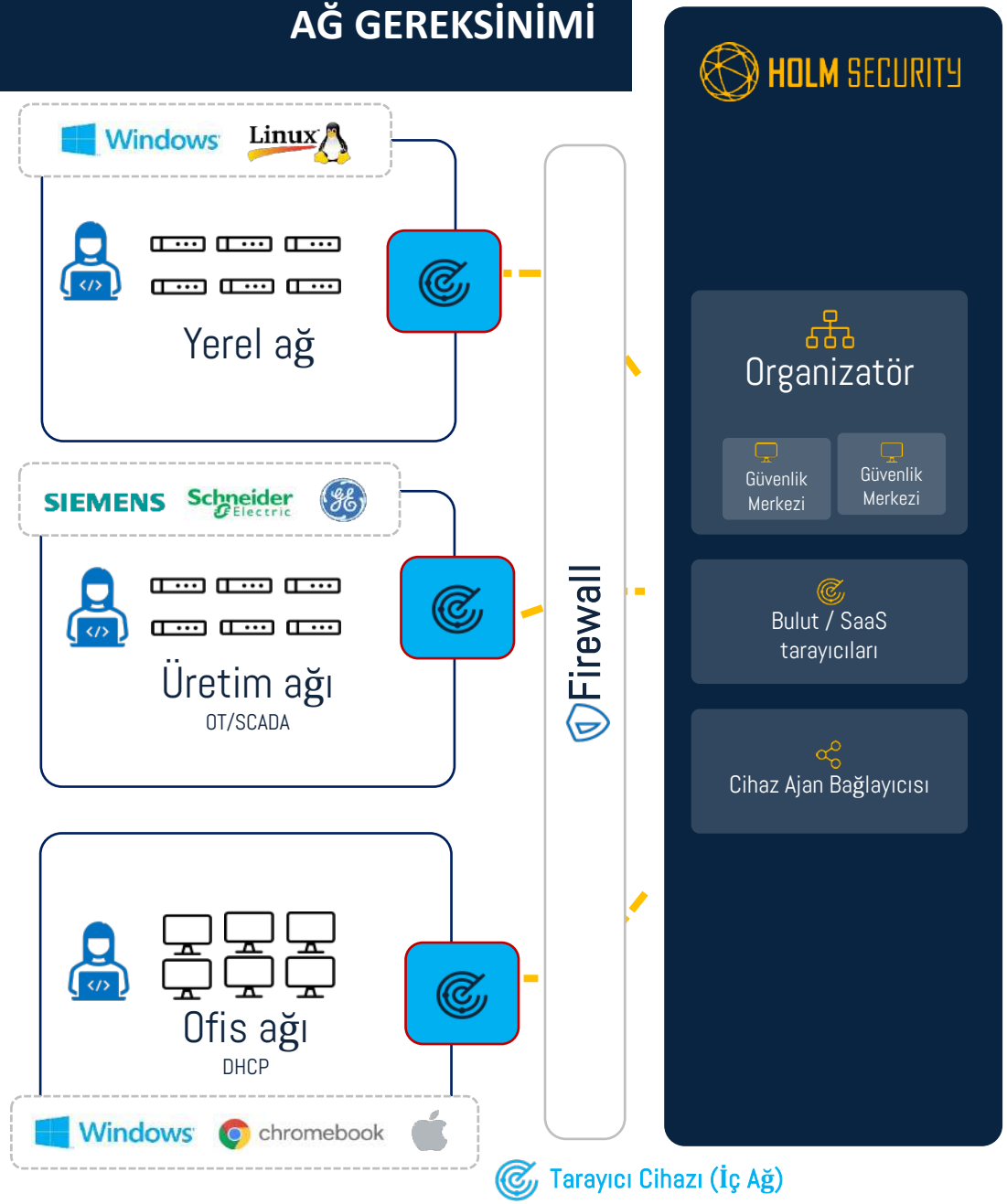

Windows
Linux
Yerel ağ
SIEMENS
Schneider Electric
Üretim ağı
OT/SCADA
Ofis ağı
DHCP
Windows
chromebook
Firewall
DMZ
Herkese açık sistemler
Windows
Linux
HOLM SECURITY
Organizatör
Güvenlik Merkezi
Güvenlik Merkezi
Bulut / SaaS tarayıcıları
Cihaz Ajan Bağlayıcısı
Uzaktan çalışanlar
aws
Google Cloud
Microsoft Azure
ORACLE CLOUD
Bulut altyapısı
SaaS
Dış kaynaklı altyapı
Windows
Linux
Tarayıcı Cihazı
Cihaz Ajanı

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Ağ Gereksinimi

AĞ GEREKSİNİMİ



- Sanal Tarayıcı Cihazı, iç firewall politikası üzerinden aşağıdaki giden TCP portları aracılığıyla Holm Security'ye bağlanmalıdır: -
  - TCP Portu: 443 ve 8022
  - IPv4: 185.163.84.0/22

22 ağının erişim vermek için fazla geniş olması durumunda, aşağıdaki ağları kullanabilirsiniz: 185.163.84.0/24 ve 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

İmajları indirin

İMAJ İNDİRME: DOĞRUDAN

HOLM SECURITY

Sanal Tarayıcı Cihazı

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

Microsoft Hyper-V

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

Not: Yukarıdaki bağlantıların süresi dolmuşsa temsilcinizi bilgilendirin

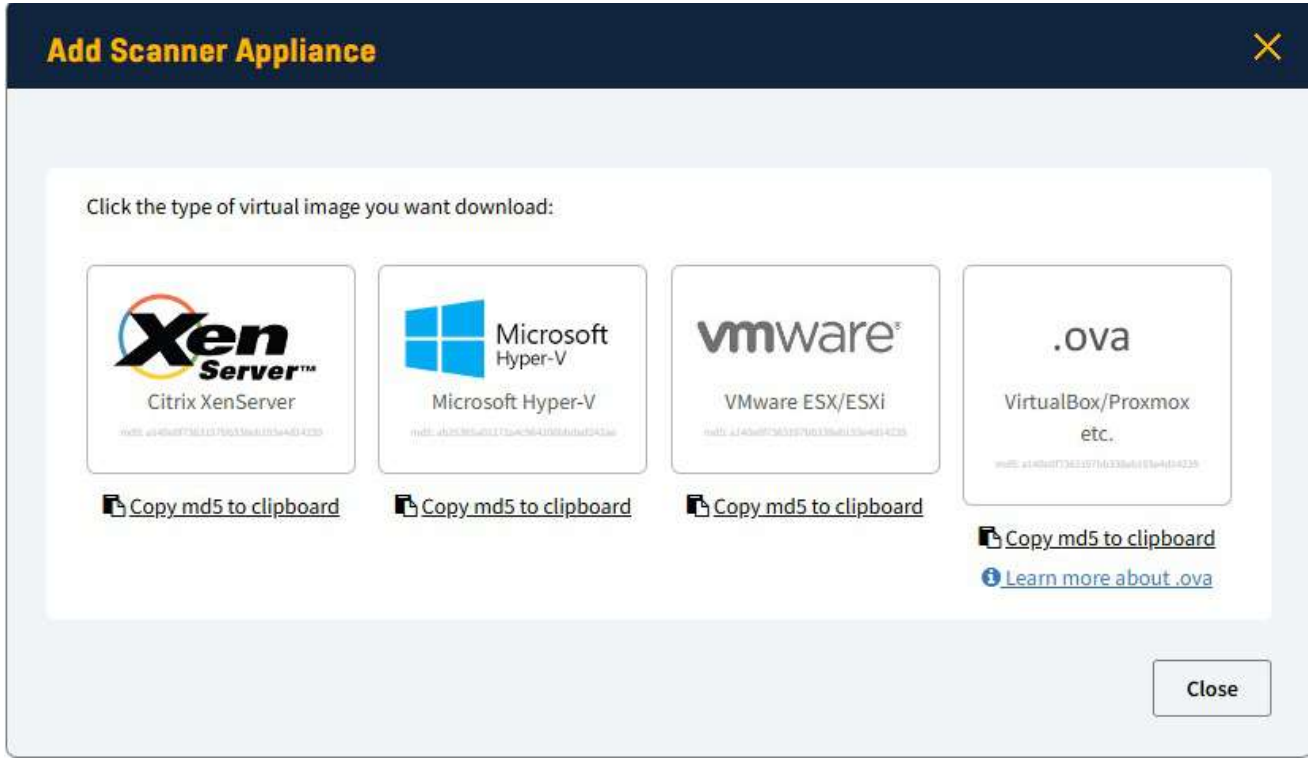
Link: https://support.holmsecurity.com/knowledge/what-are-the-system-requirements-for-the-scanner-appliance

İMAJ İNDİRME:
GÜVENLİK MERKEZİ

HOLM SECURITY

Sanal Tarayıcı Cihazı

VMware ESXi™ · VirtualBox · Xen Server™ · vmware Workstation · PROXMOX · KVM · 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

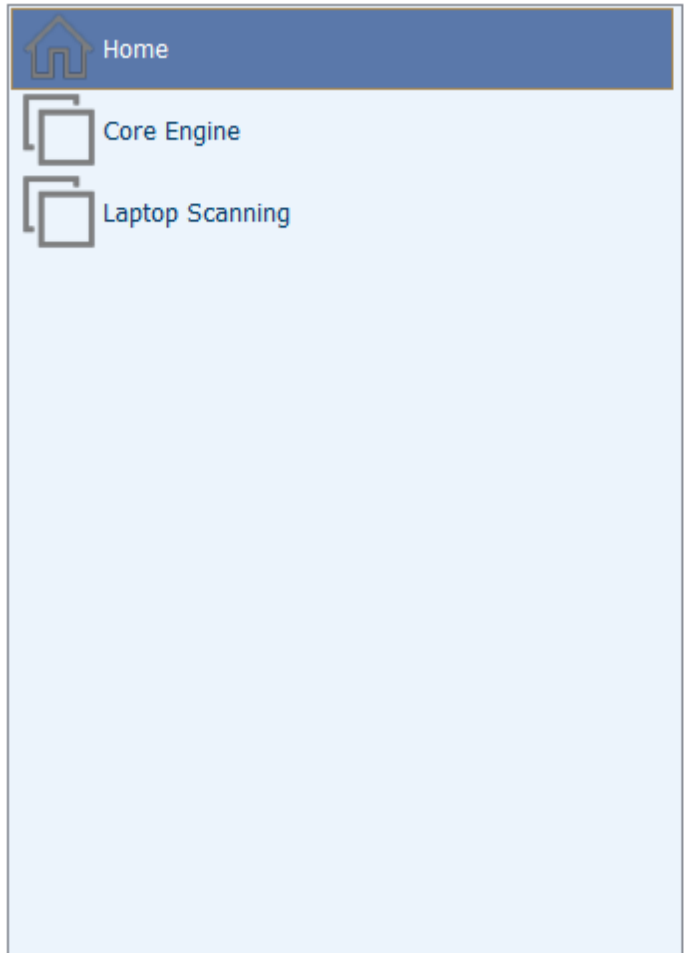
Kurulum

TARAYICI CİHAZI: İÇE AKTAR

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

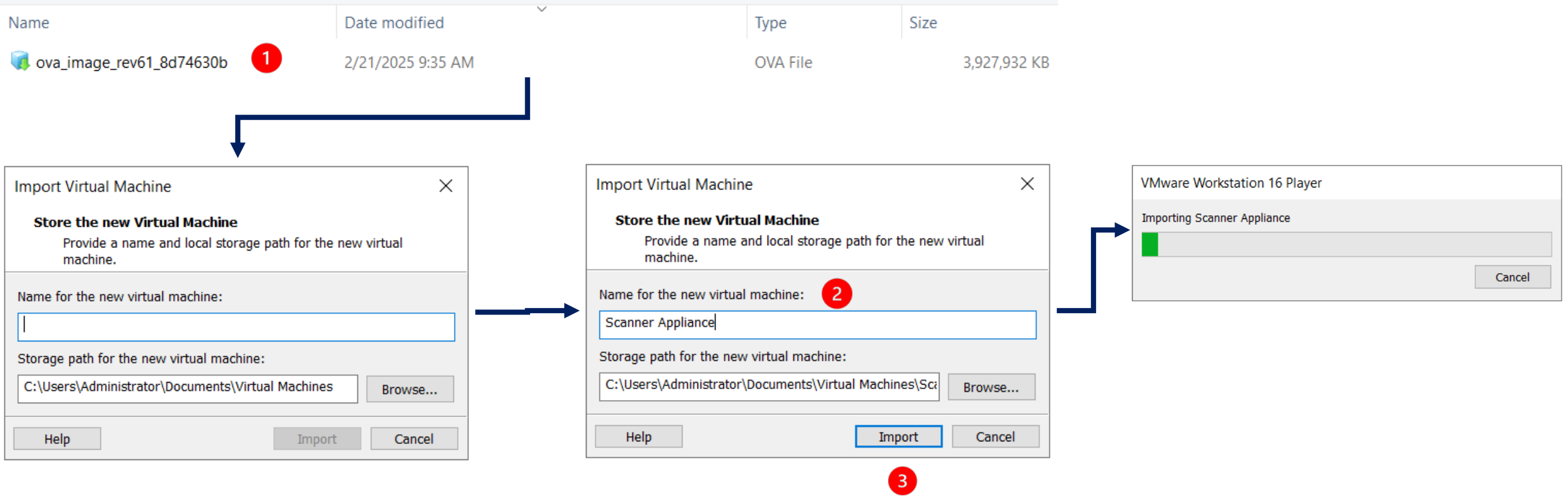
Sanal Tarayıcı Cihazı

Not: VMWare Workstation Player 16 kullanılarak Core Engine imajının içe aktarım süreci simüle edilmektedir



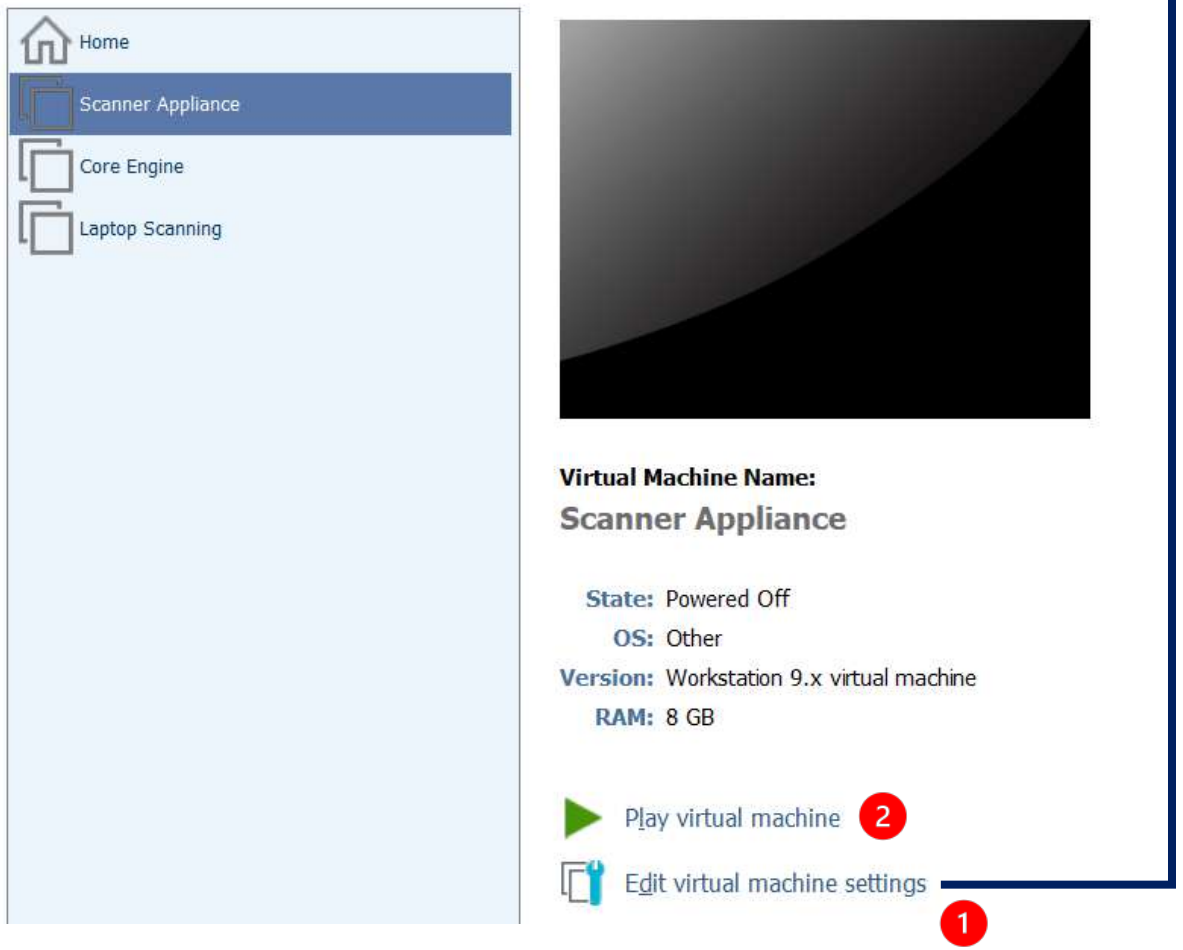
Bir Sanal Makine açın

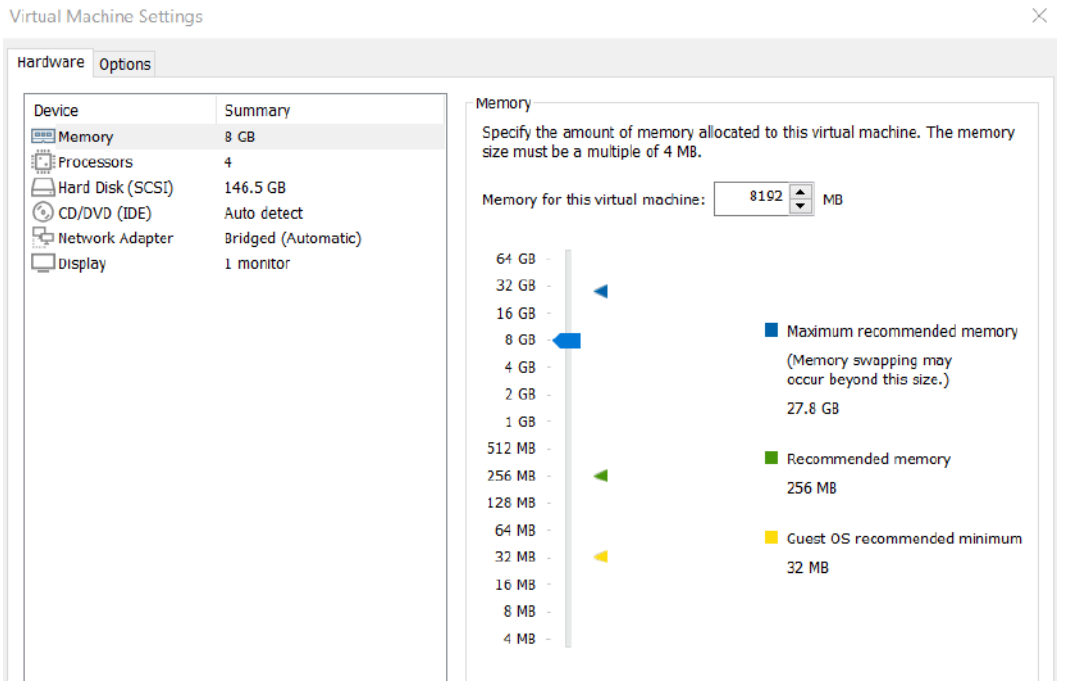
TARAYICI CİHAZI:
İÇE AKTAR



İmajın içe aktarılması

TARAYICI CİHAZI:
KAYNAKLAR

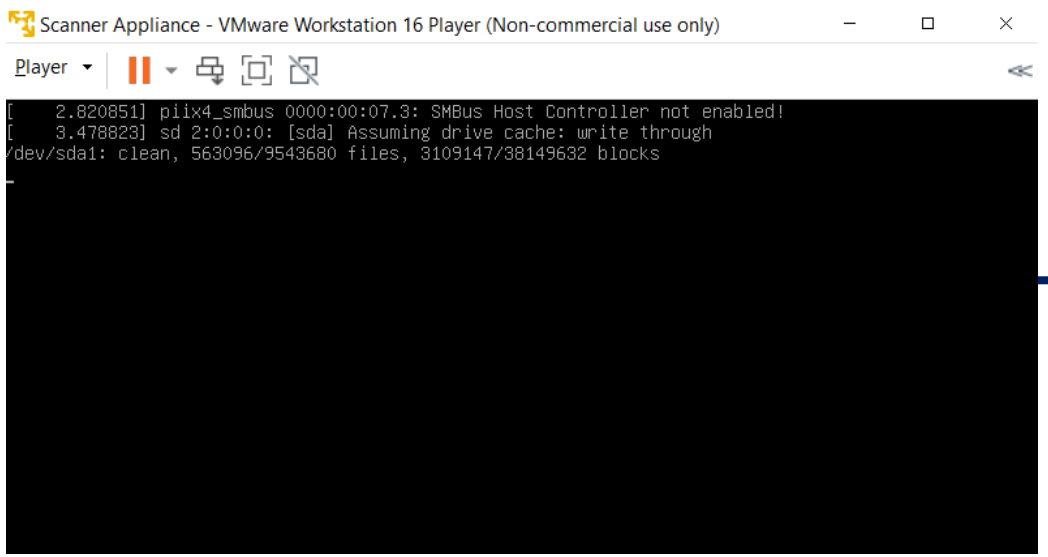


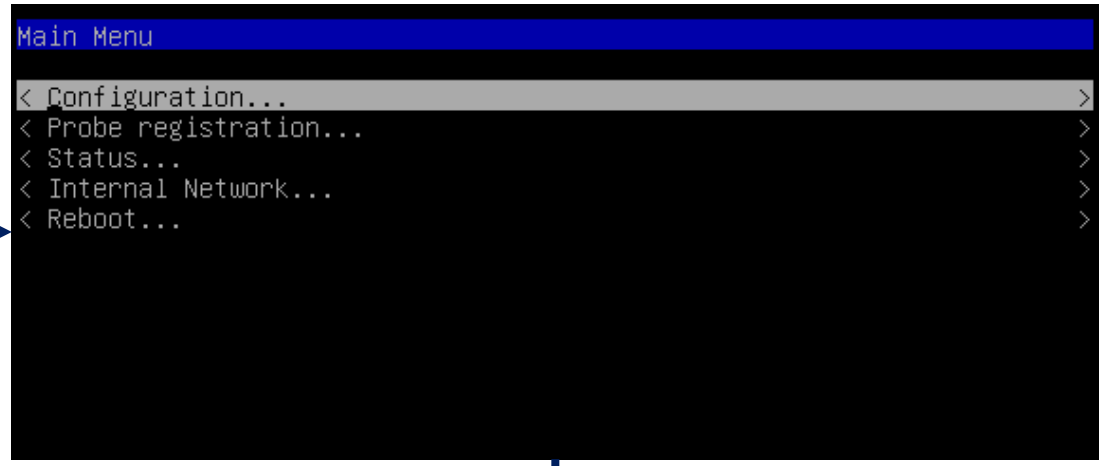


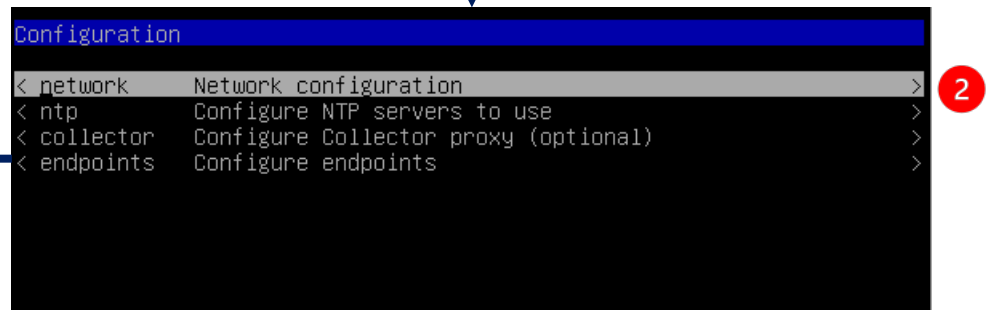
Ağ Adaptörü seçiminin doğru olduğundan emin olun

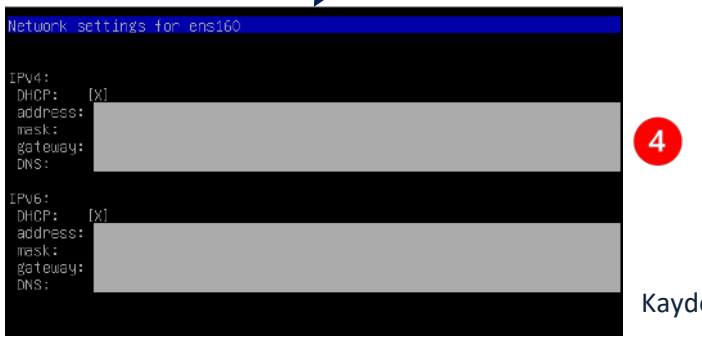
Sanallaştırma kaynak kontrolü

TARAYICI CİHAZI:
IP YAPILANDIRMASI







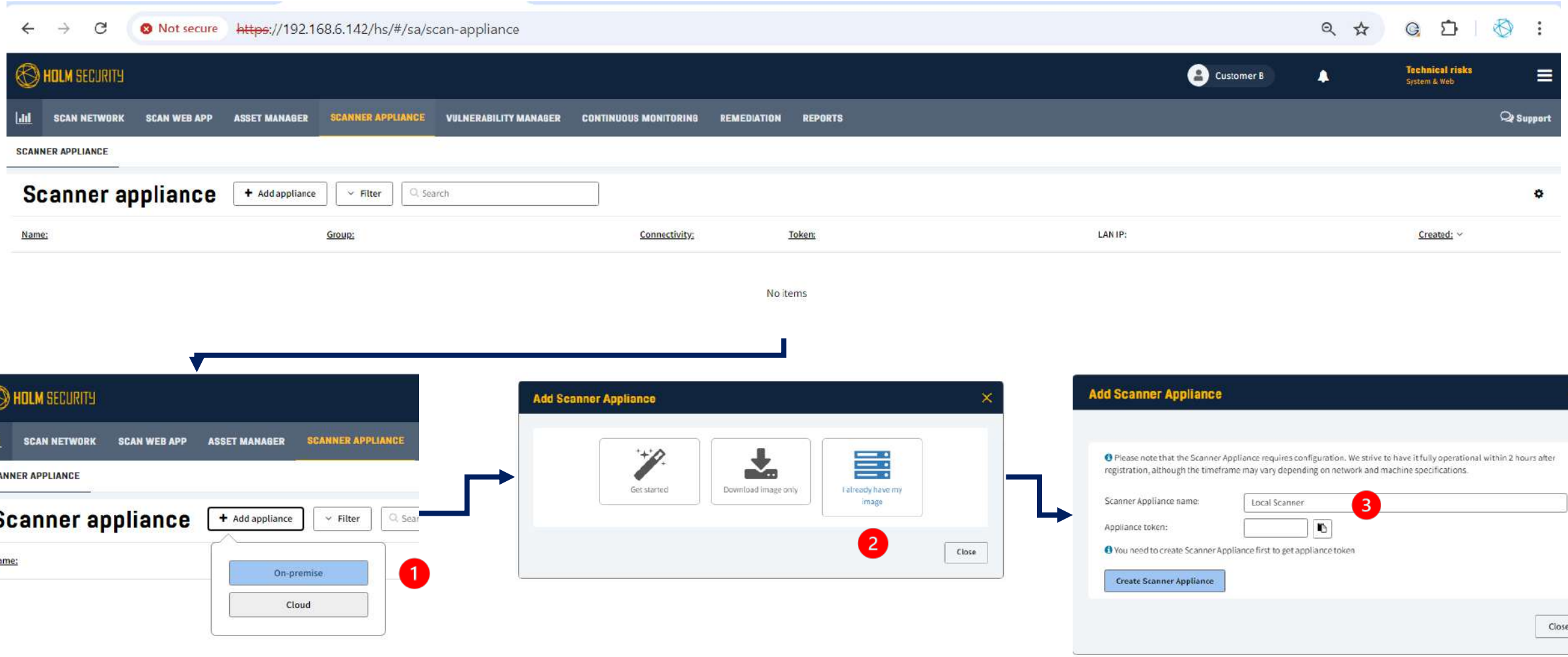


Kaydetmek için Fn + F11

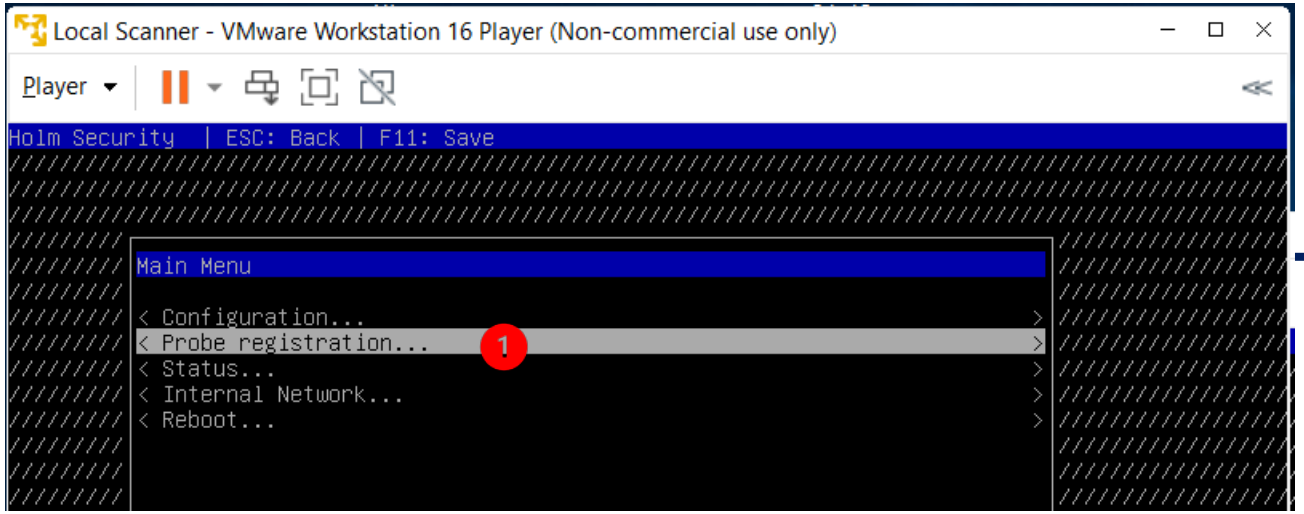
Not: Bu simülasyon, IP adresi için DHCP'ye dayanmaktadır

GÜVENLİK MERKEZİ:
TOKEN ANAHTARI OLUŞTURMA

- Probe kaydı için Tarayıcı Cihazının token anahtarını oluşturmanız gerekmektedir



TARAYICI CİHAZI:
PROBE KAYDI



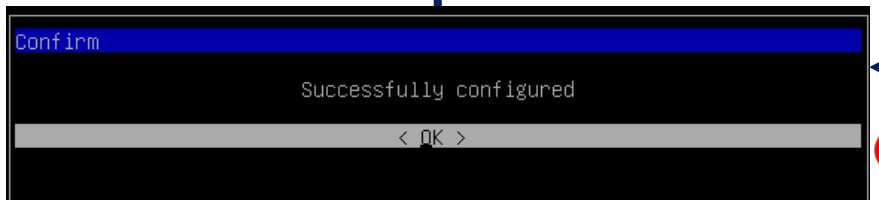
2

Token anahtarını girin

3

4

5



6

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

On-Premise VMP

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi Platformu

Saldırı yüzeyi

Harici Saldırı Yüzeyi (EASM)

Üçüncü taraf (tedarikçiler)

Saldırı vektörleri

- İş açısından kritik sistemler / sunucular
- Bilgisayarlar ve ofis ekipmanları
- Ağ cihazları
- IoT
- Kubernetes
- OT
- Web uygulamaları
- APIs
- Bulut yerel platformlar
- Microsoft 365
- Kullanıcılar

Ürünler

- **Sistem ve ağ güvenliği**
- **Web uygulama güvenliği**
- **API güvenliği**
- **Bulut güvenliği**
- **Phishing simülasyonu ve farkındalık eğitimi**

HAZIRLIK KONTROL LİSTESİ

HOLM SECURITY

Müşteri

- **Sanallaştırma platformu**
  - Core Engine için VM ESXi (veya demo amaçlıysa VMWare Workstation)
  - Tarayıcı Cihazı için VM ESXi, VM Workstation, VM Player, Oracle VirtualBox, KVM vb.

- **İmajları indirin**
  - Core Engine
  - Sanal Tarayıcı Cihazı

- **Ağ yapılandırması**
  - Edge Firewall Politikası (Giden Trafik)
  - İç Firewall Politikası (Core Engine ile Sanal Tarayıcı Cihazı arasında), varsa
  - Core Engine ve Sanal Tarayıcı Cihazı için özel statik IP

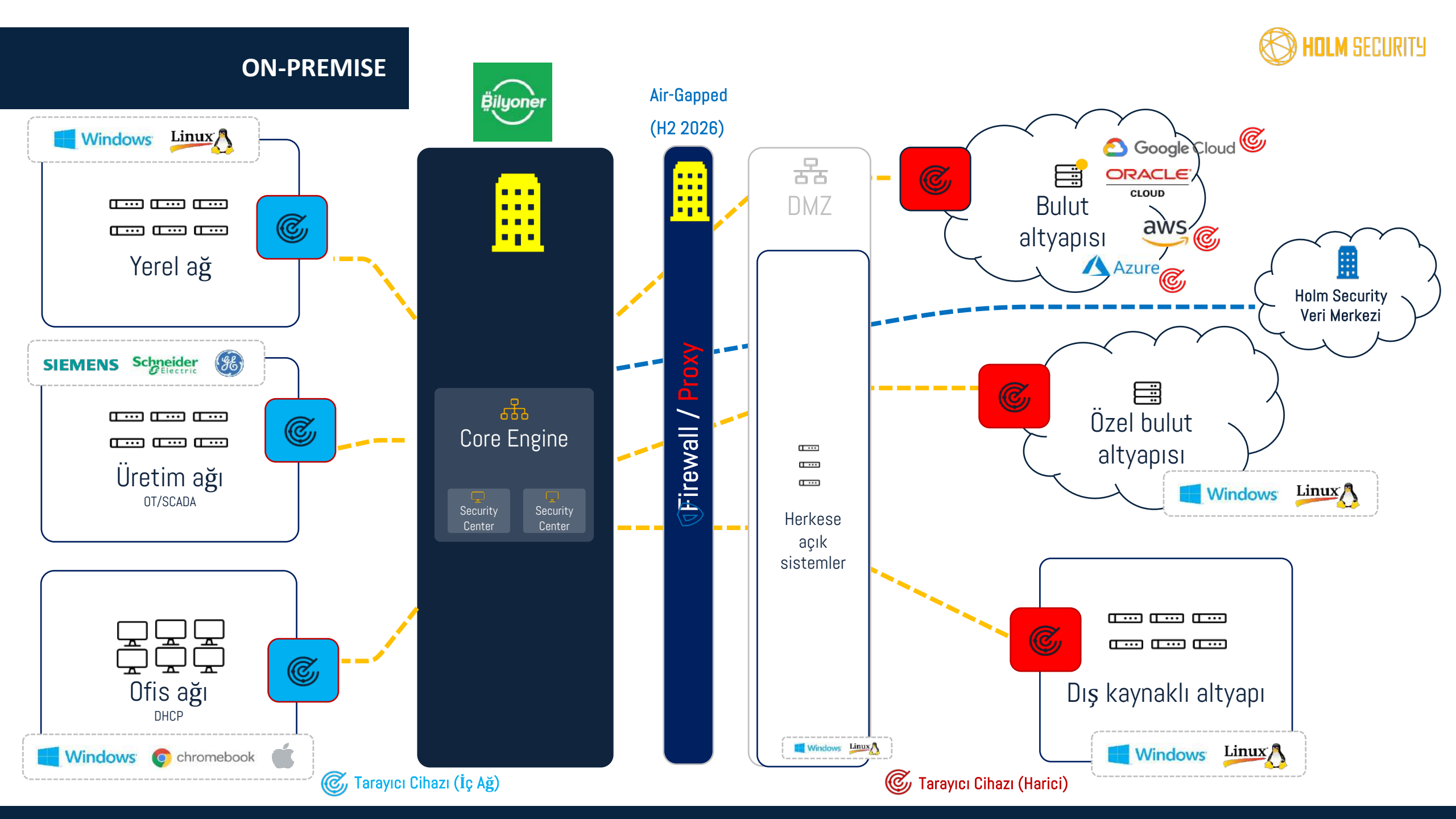
OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

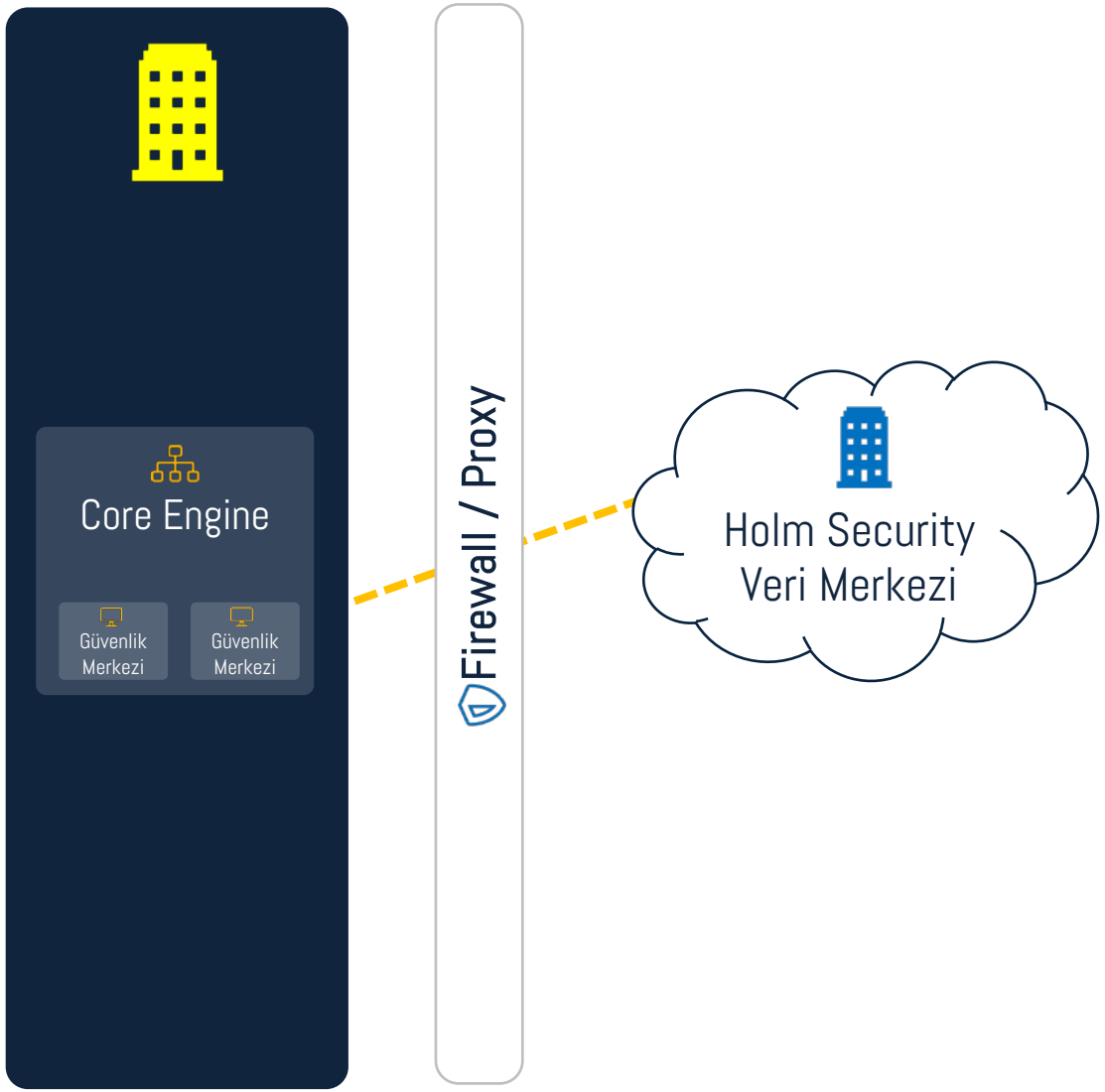
HOLM SECURITY

Mimari

ON-PREMISE

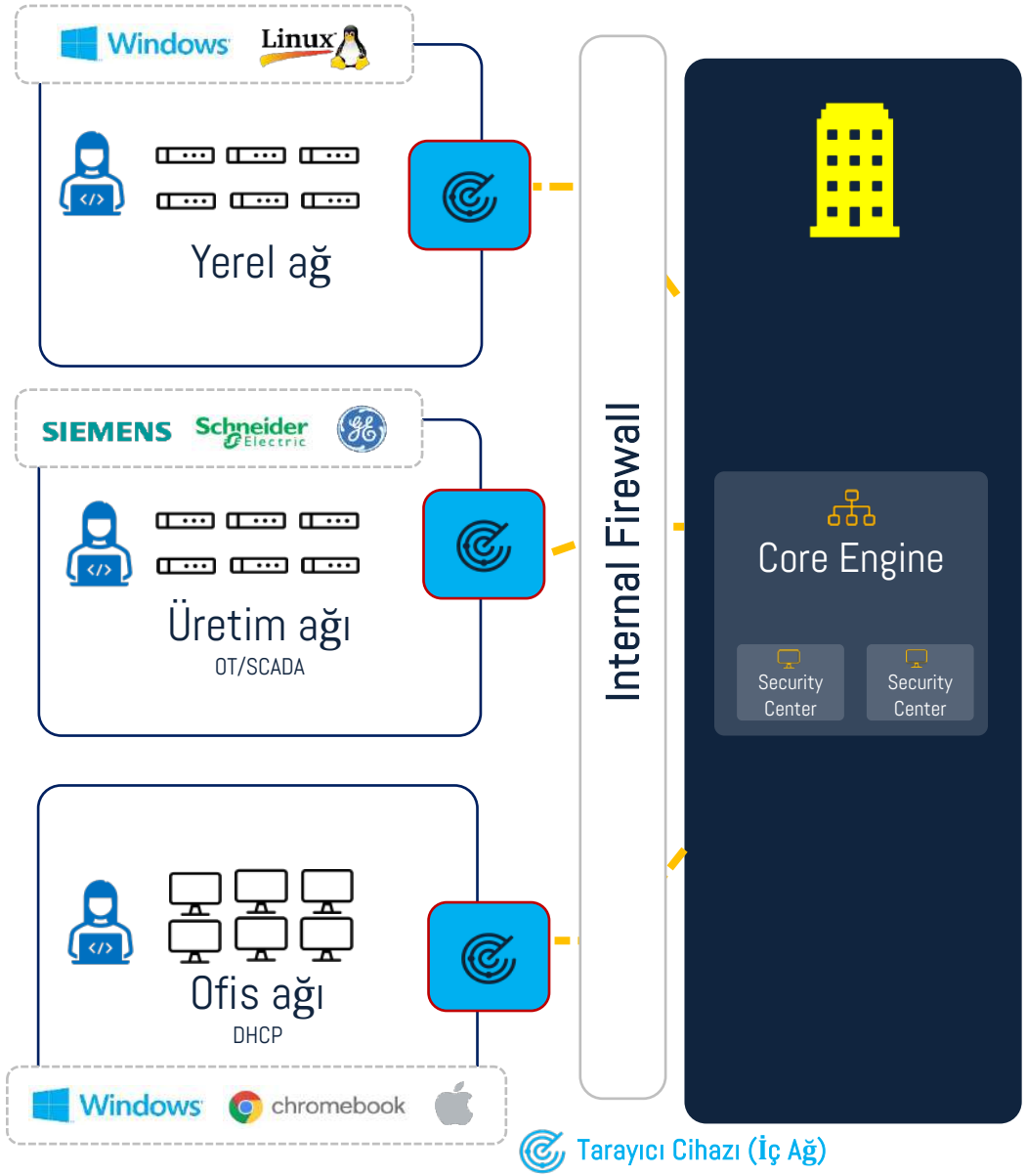

Bilyoner
Air-Gapped
(H2 2026)
Windows
Linux
Yerel ağ
SIEMENS
Schneider Electric
Üretim ağı
OT/SCADA
Ofis ağı
DHCP
Windows
chromebook
Core Engine
Security Center
Security Center
Firewall / Proxy
DMZ
Herkese açık sistemler
Windows
Linux
Google Cloud
ORACLE CLOUD
Bulut altyapısı
aws
Azure
Holm Security Veri Merkezi
Özel bulut altyapısı
Windows
Linux
Dış kaynaklı altyapı
Windows
Linux
Tarayıcı Cihazı (İç Ağ)
Tarayıcı Cihazı (Harici)

CORE ENGINE



- F/W – Core Engine'in yazılım güncellemeleri ve zafiyet veritabanı güncellemeleri için Holm Security Veri Merkezi'ne bağlanmasına izin verecek giden kural: -
  - TCP: 443 ve 8022
  - IPv4: 185.163.84.0/22 veya IPv6: 2a0b:6800::/29
  - NTP: UDP 123
  - DNS: TCP/UDP 53

ON-PREMISE: İÇ ORTAM

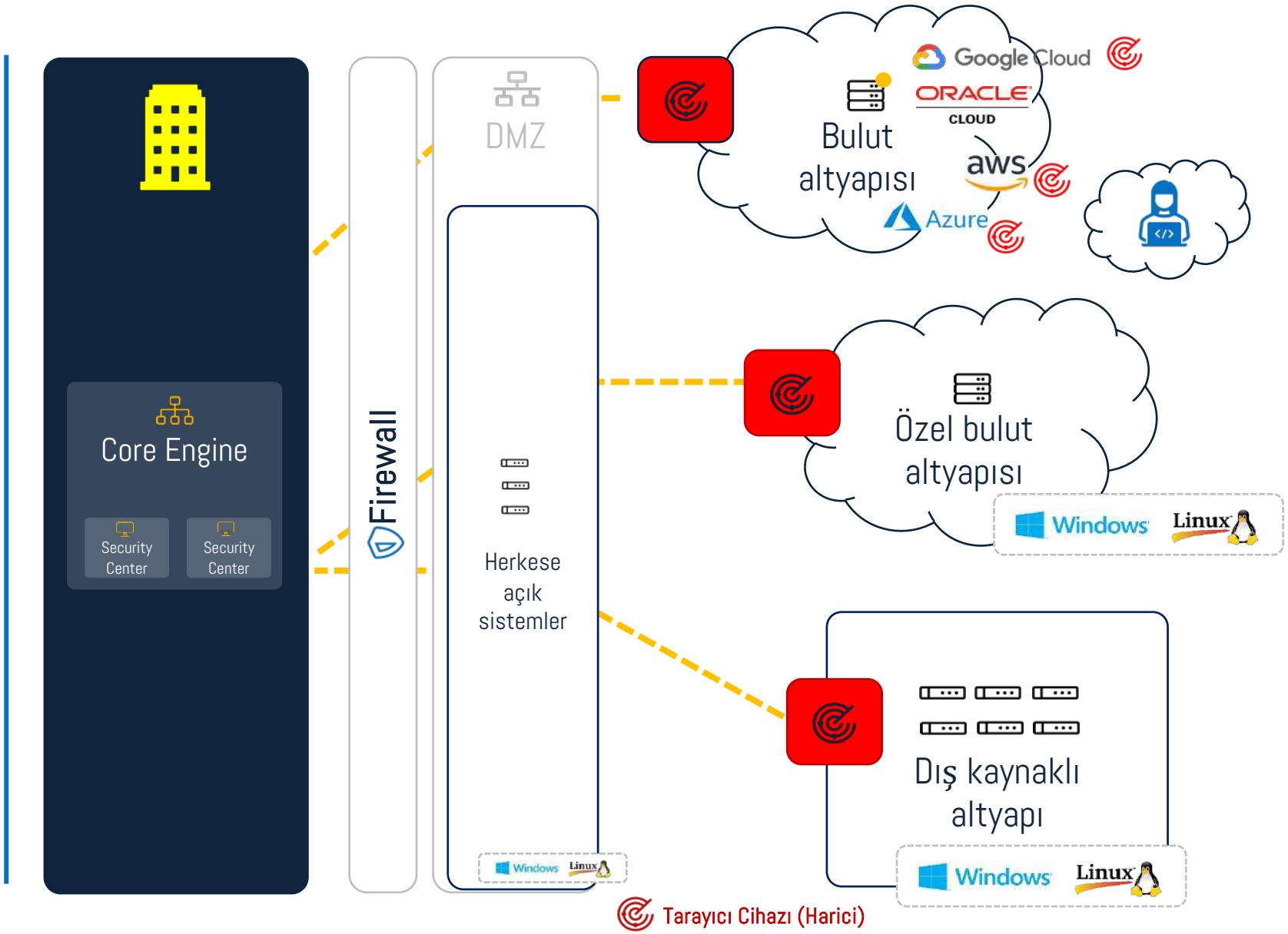


- İç Tarayıcı Cihazı, aşağıdaki TCP portları üzerinden Core Engine'e bağlanmalıdır: -
  - 8004, 8007, 8044 ve 8022
- Aşağıdaki TCP portları, sistem yöneticisinin erişimi içindir: -
  - Web Portal Admin: 8001
  - Multi Tenant Organizer: 8002
  - REST API: 8005

ON-PREMISE: İÇ ORTAM

- Harici Tarayıcı Cihazı, aşağıdaki TCP portları üzerinden Core Engine'e bağlanmalıdır: -
  - 8004, 8007, 8044 ve 8022
- Aşağıdaki TCP portları, sistem yöneticisinin erişimi içindir: -
  - Web Portal Admin: 8001
  - Multi Tenant Organizer: 8002
  - REST API: 8005

Not: SSL Sertifikası hem Root hem de Intermediate sertifikalarını içermelidir



OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Servisler ve Portlar

SERVİSLER VE PORTLAR

No	Servis	Portlar	Protokol	Notlar
1	Güvenlik Merkezi*	443	HTTPS	Ana Portal
2	Web Yönetim Paneli*	8001	HTTPS	On-Prem sistemin temel ayarları için web yönetim arayüzü
3	Organizatör*	8002	HTTPS	Multi-tenant Portal
4	Platform API*	8005	HTTPS	Security Center REST API
5	Back Office	8003	HTTPS	Yalnızca Holm Security iç kullanımı içindir
6	Tarayıcı Cihazı API**	8004	HTTPS	Tarayıcı Cihazı için dahili kullanım
7	Besleme Güncellemeleri**	8007	HTTPS	İmza ve tarayıcı cihazı güncellemeleri
8	APT**	8044	HTTP	Tarayıcı cihazı için imzalı işletim sistemi paket güncellemeleri
9	Tarayıcı Cihazı**	8022	SSH	Her bir tarayıcı cihazı için benzersiz anahtara sahip yönetim portu

* Müşteri tarafından kullanılacaktır
* Sanal Tarayıcı Cihazı tarafından kullanılacaktır

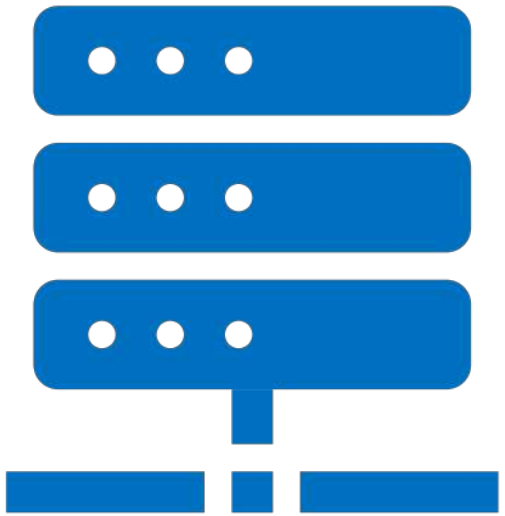
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

On-Premise Bileşenleri

CORE ENGINE VE SANAL TARAYICI CİHAZI

Core Engine



- Statik IP (ve Alt Ağ Maskesi, Ağ Geçidi ve DNS)
- SMTP Ayarları
- Lisans Dosyası (bu lisans anahtarını temin etmek için Holm Security temsilcinizle iletişime geçin)

Sanal Tarayıcı Cihazı

- Statik IP (ve Alt Ağ Maskesi, Ağ Geçidi ve DNS)

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

SİSTEM GEREKSİNİMLERİ

HOLM SECURITY

Kavram Kanıtı (200 IP / 5 Web Uygulaması)

Sunucu	Açıklama	CPU	RAM (GB)	HDD (GB)	Adet
Sunucu A	Core Engine	4	16	100	1
Sunucu B	Scanner Appliance	2	8	150	1

Küçük (>1000 IP / 5 Web Uygulaması)

Sunucu	Açıklama	CPU	RAM (GB)	HDD (GB)	Adet
Sunucu A	Core Engine	8	24	100	1
Sunucu B	Scanner Appliance	2	8	150	2

Orta (1000 – 10000 IP / 5 – 30 Web Uygulaması)

Sunucu	Açıklama	CPU	RAM (GB)	HDD (GB)	Adet
Sunucu A	Core Engine	12	32	100	1
Sunucu B	Scanner Appliance	2	8	150	4

Büyük (> 10000 IP / > 30 Web Uygulaması)

Sunucu	Açıklama	CPU	RAM (GB)	HDD (GB)	Adet
Sunucu A	Core Engine	24	48	100	1
Sunucu B	Scanner Appliance	2	8	150	8

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

OTD BİLİŞİM
GLOBAL VAD

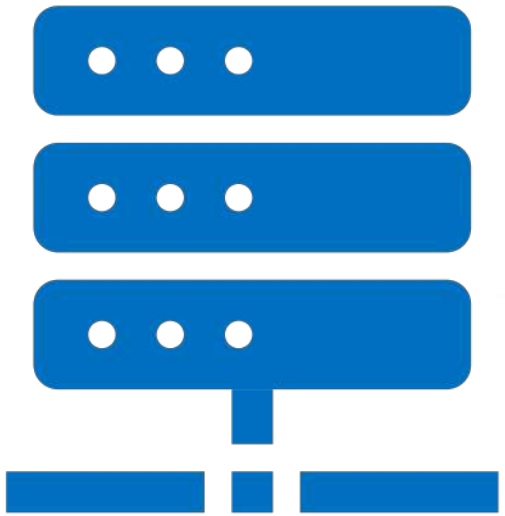
HOLM SECURITY

Tarayıcı Cihazı

İMAJ İNDİRME

HOLM SECURITY

Core Engine



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

Sanal Tarayıcı Cihazı

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

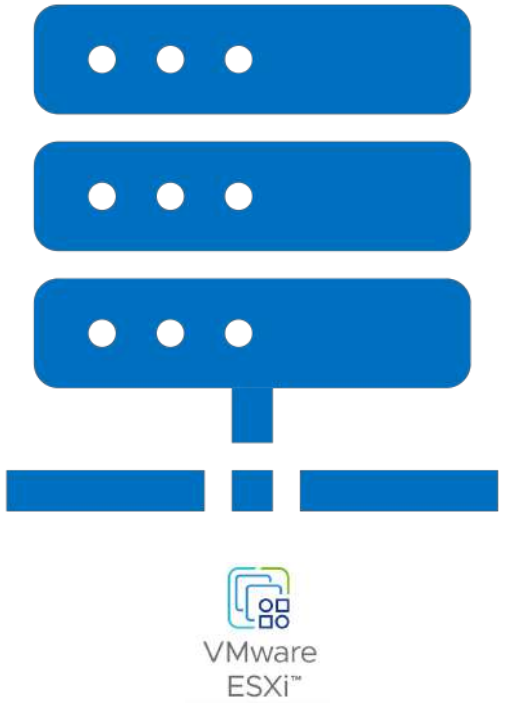
Core Engine

Kurulum ve Yapılandırma

CORE ENGINE: İÇE AKTAR

HOLM SECURITY

Core Engine

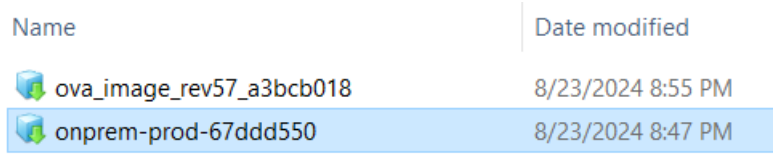


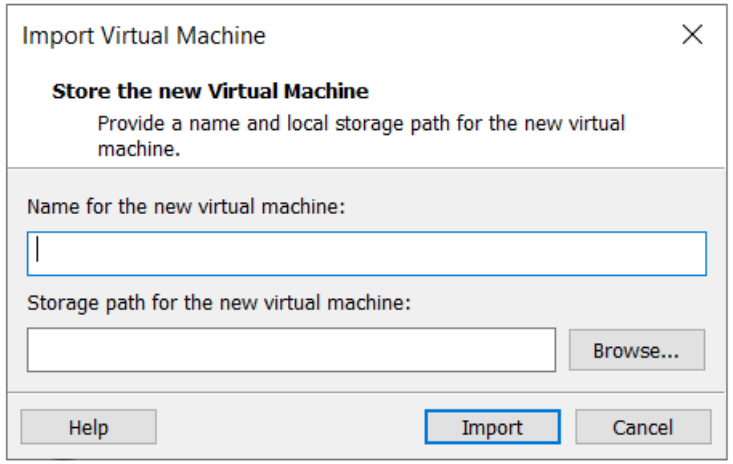
Bir Sanal Makine açın

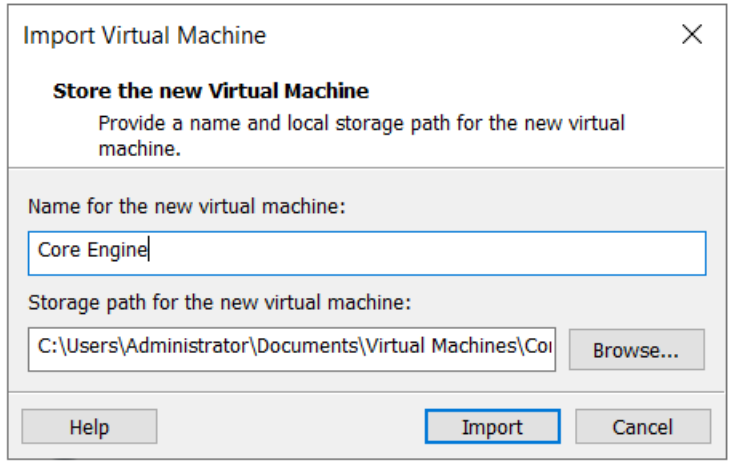
Not: VMWare Workstation Player 16 kullanılarak Core Engine imajının içe aktarım sürecinin simüle edilmesi

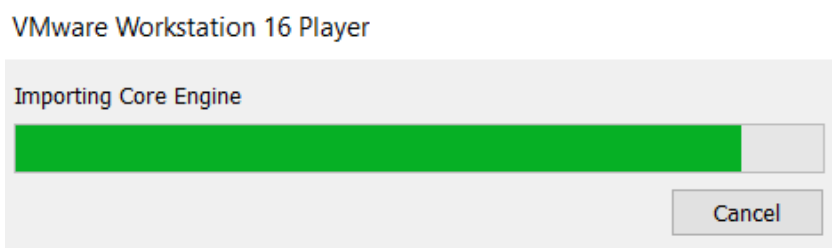
OTD BİLİŞİM GLOBAL VAD

CORE ENGINE: İÇE AKTAR

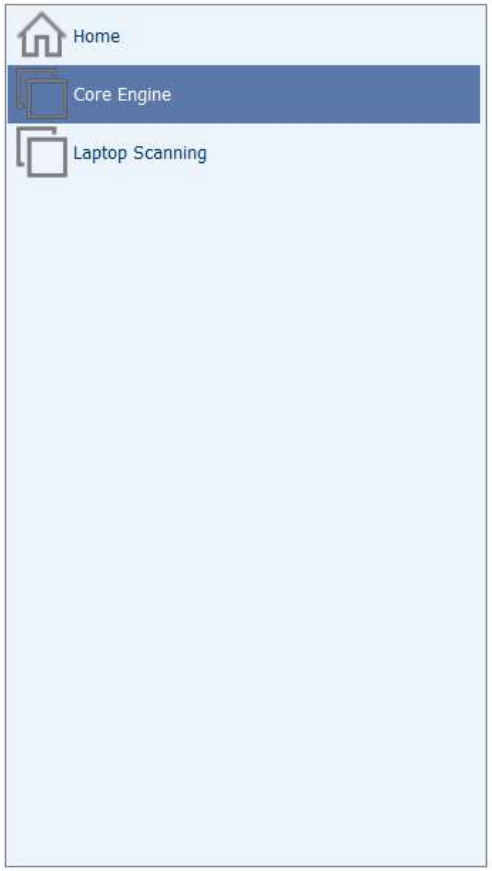


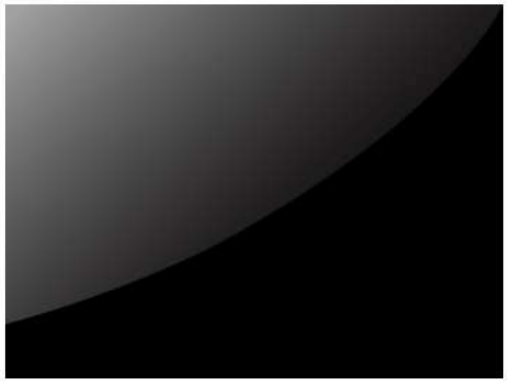






CORE ENGINE: İÇE AKTAR





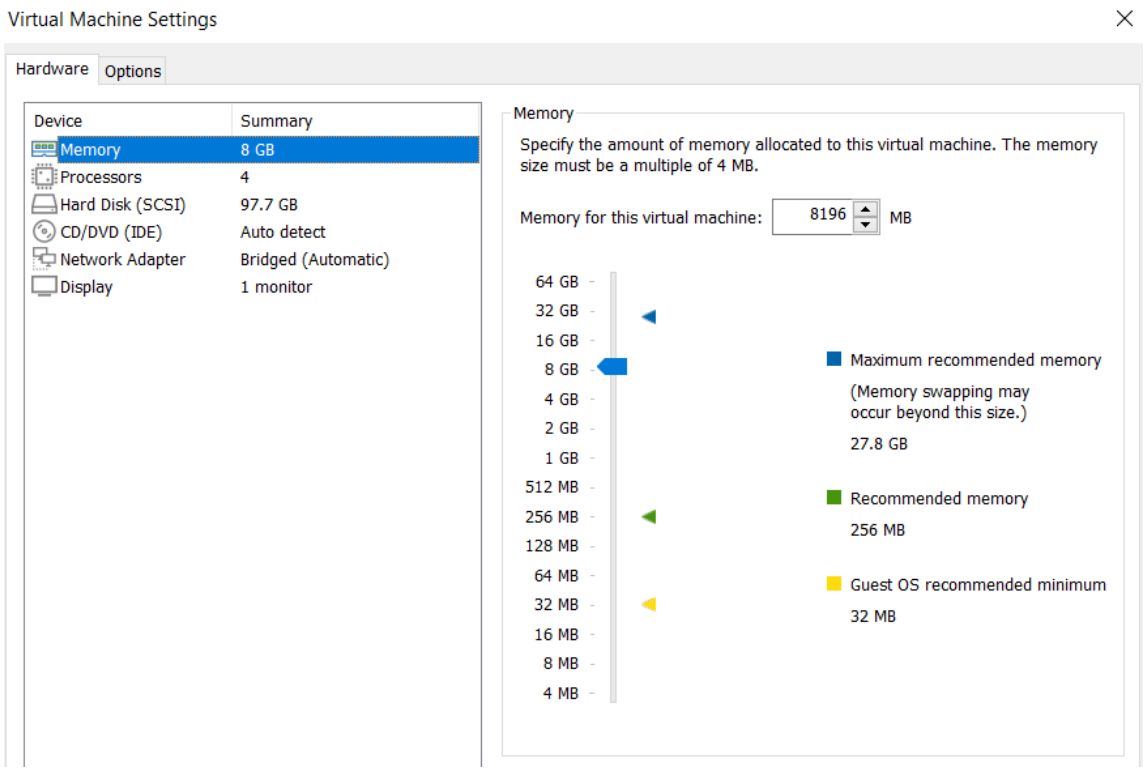
Virtual Machine Name:

Core Engine

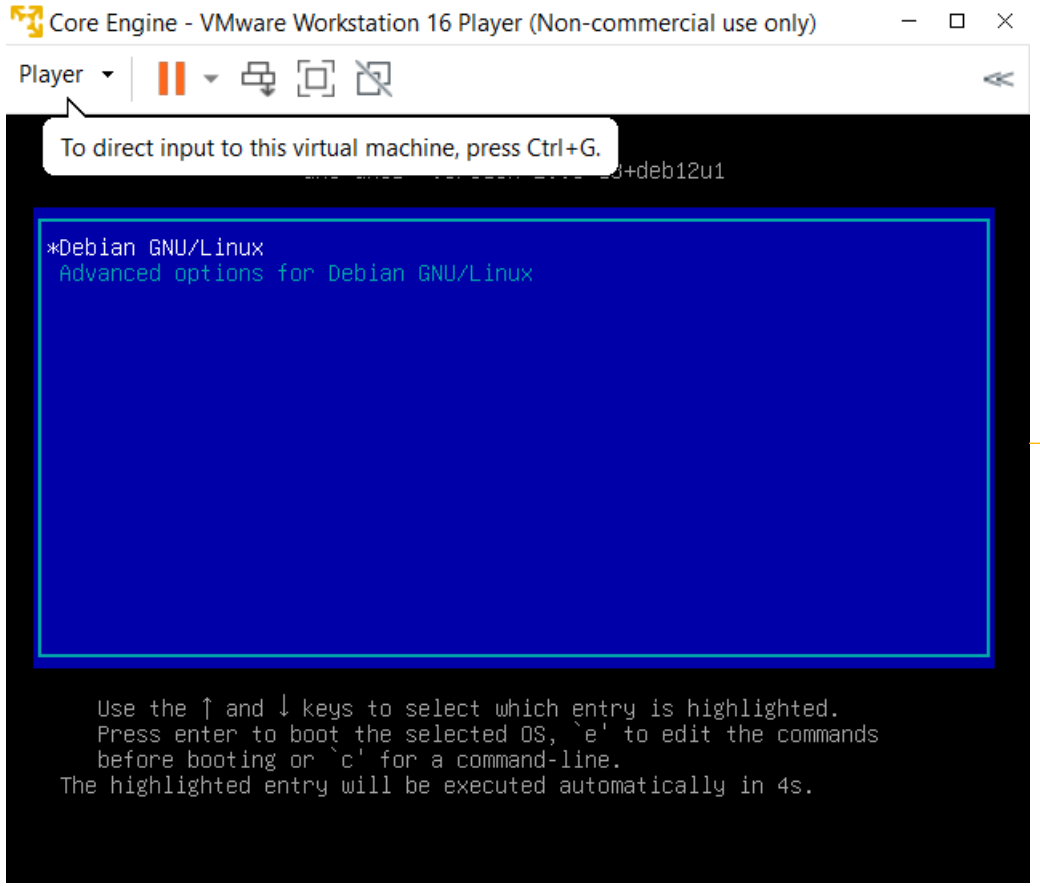
State: Powered On
OS: Other
Version: ESXi 6.5 virtual machine
RAM: 8 GB

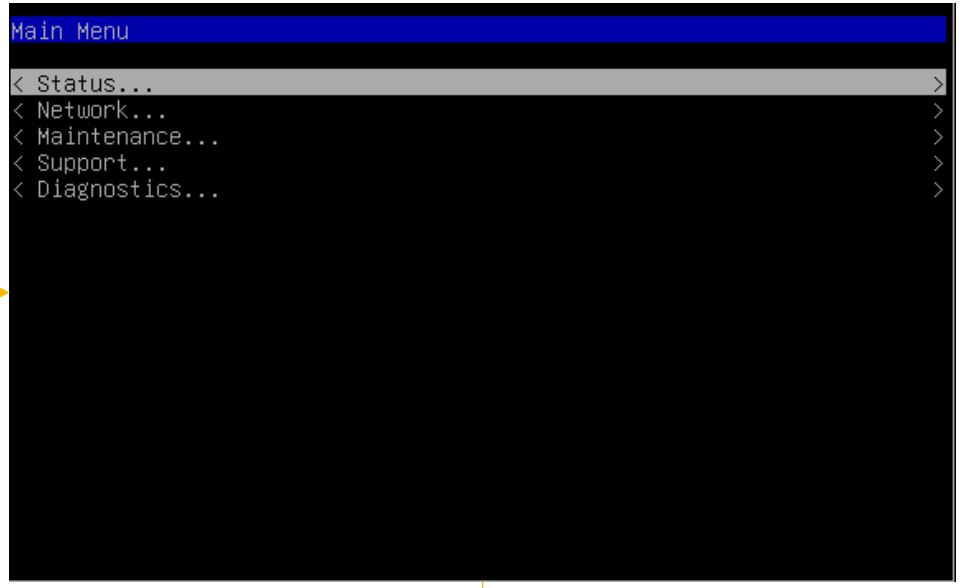
Play virtual machine

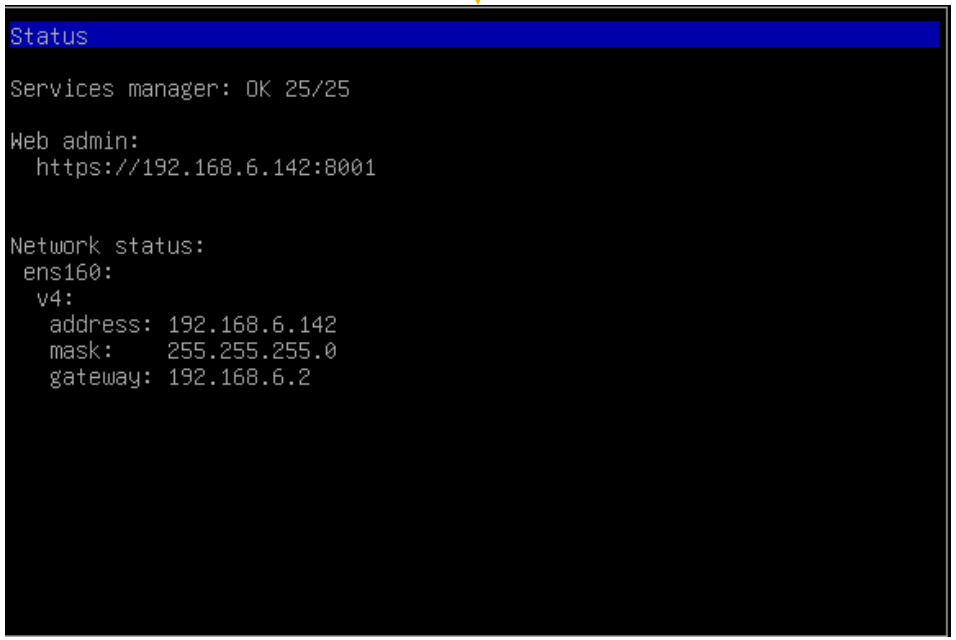
Edit virtual machine settings



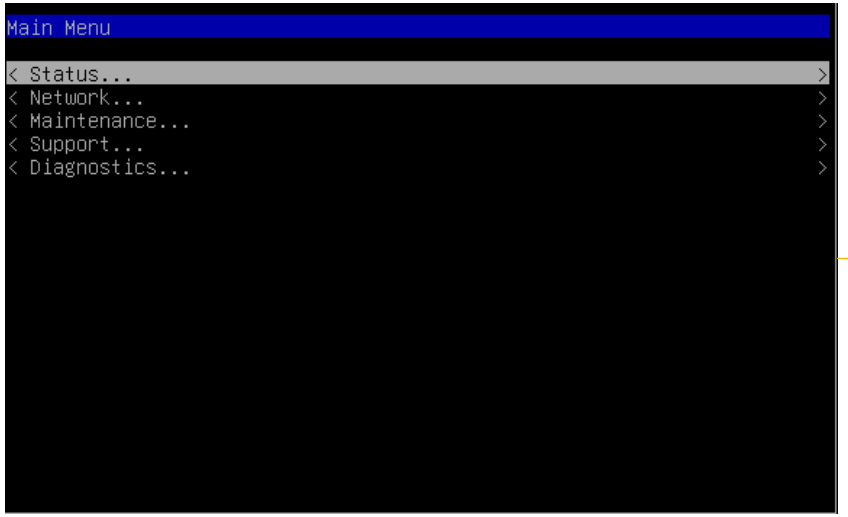
CORE ENGINE: KURULUM

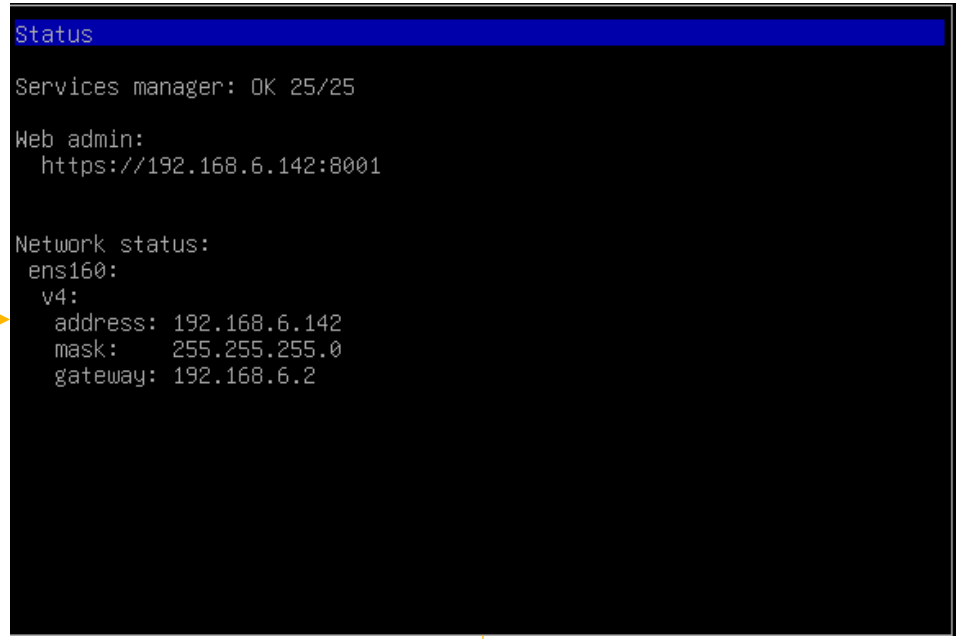


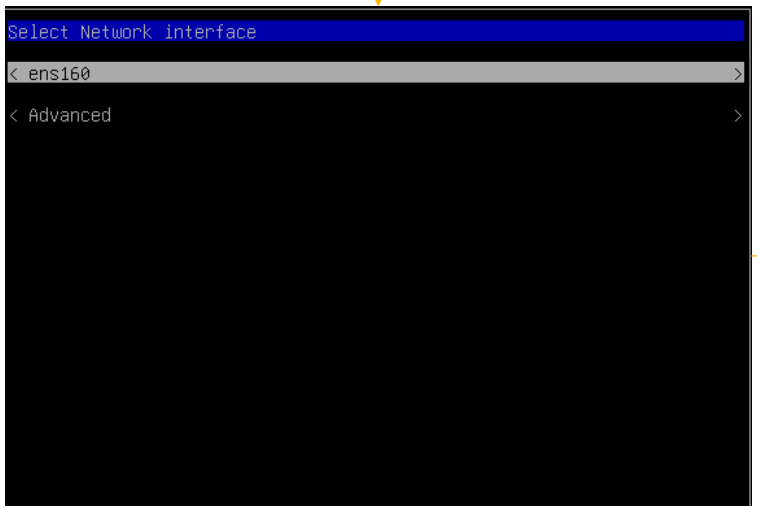


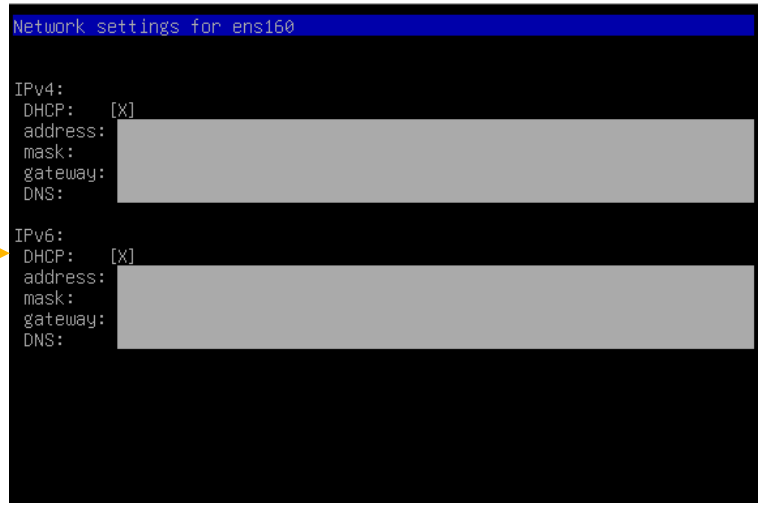


CORE ENGINE: İÇE AKTAR









Not: Bu simülasyon, IP adresi için DHCP'ye dayanmaktadır.

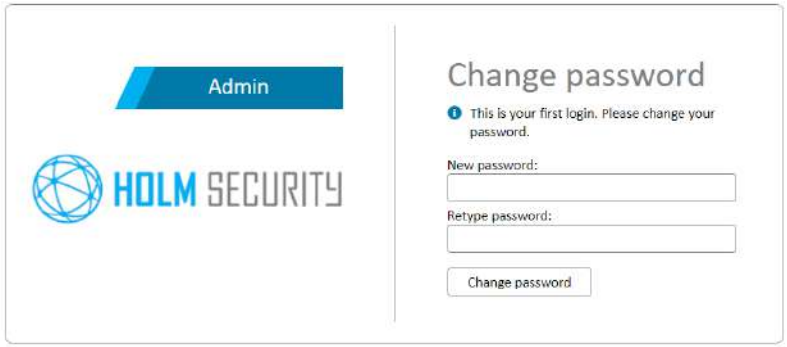
OTD BİLİŞİM
GLOBAL VAD

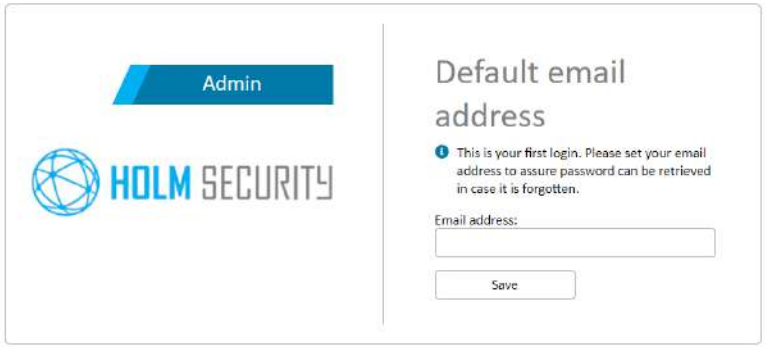
HOLM SECURITY

Web Yönetim Portalı

Kurulum ve yapılandırma

WEB YÖNETİM PANELİ: YAPILANDIRMA

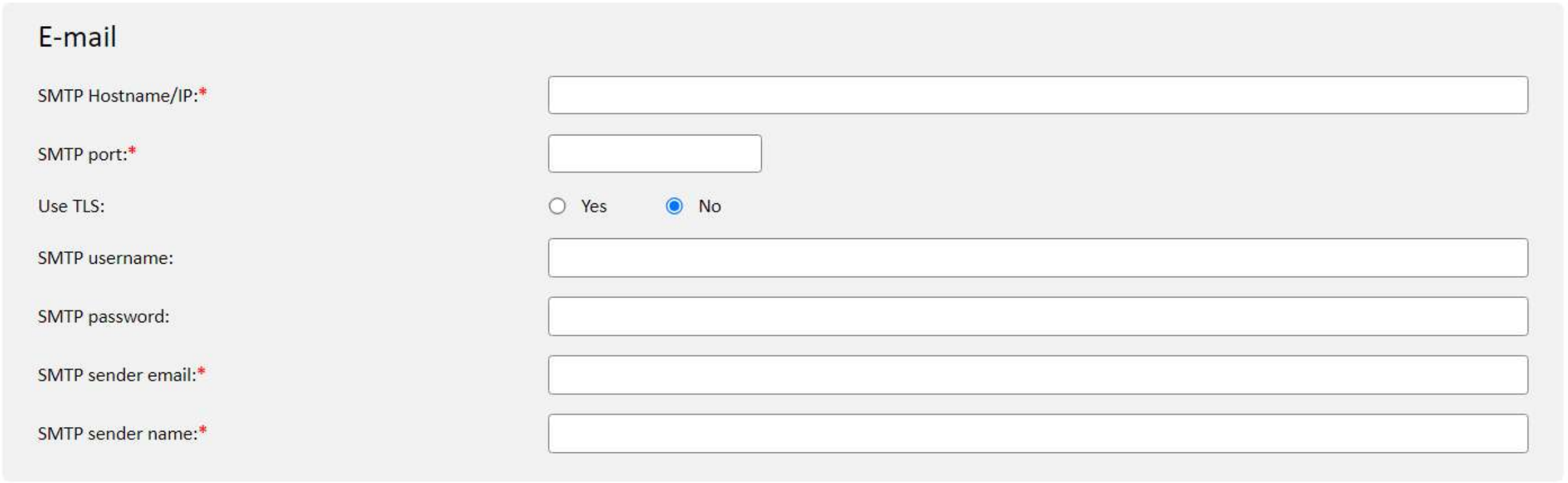




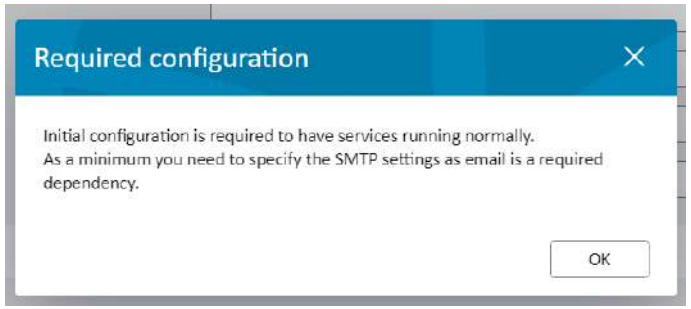
- Web yönetim portalını başlatın, örn.: https://core-engine-ip-adresi:8001
- Varsayılan kimlik bilgileri: -
  - Kullanıcı adı: admin
  - Şifre: holmsecurity
- Yeni bir şifre belirlemeniz ve yeni bir e-posta adresi tanımlamanız istenecektir

WEB YÖNETİM PANELİ: YAPILANDIRMA

HOLM SECURITY



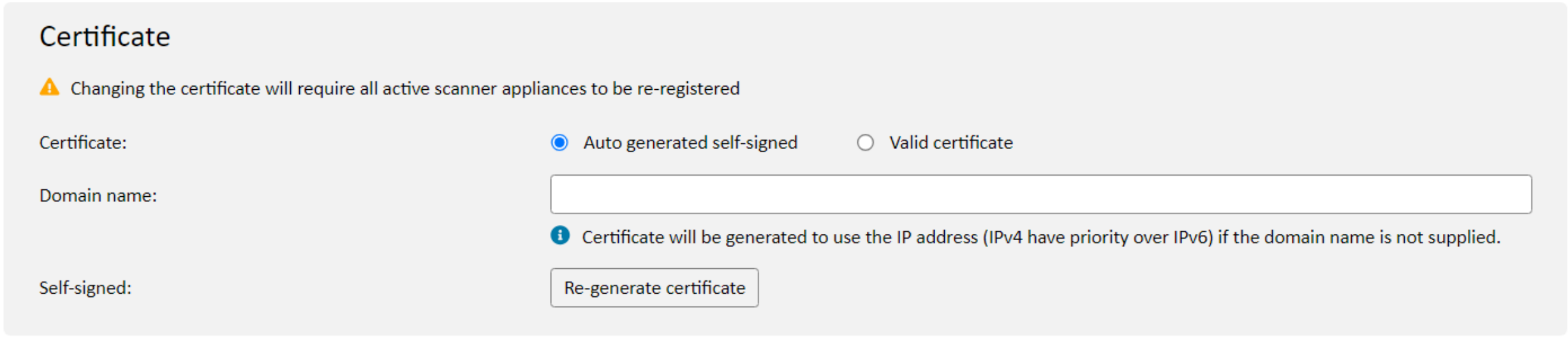
- SMTP yapılandırması için aşağıdaki ayarlar gereklidir: -
  - SMTP Hostname / IP
  - SMTP portu: 25, 465 veya 587 seçeneklerinden biri
  - TLS: Evet veya Hayır
  - SMTP – Kullanıcı adı, şifre, gönderici e-posta adresi ve gönderici adı



OTD BİLİŞİM GLOBAL VAD

WEB YÖNETİM PANELİ: YAPILANDIRMA

HOLM SECURITY



Core Engine için yapılandırılan IP adresine bağlı olarak self-signed bir sertifika tercih edebilirsiniz veya……(sonraki sayfa)

OTD BİLİŞİM GLOBAL VAD

WEB YÖNETİM PANELİ: YAPILANDIRMA

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.

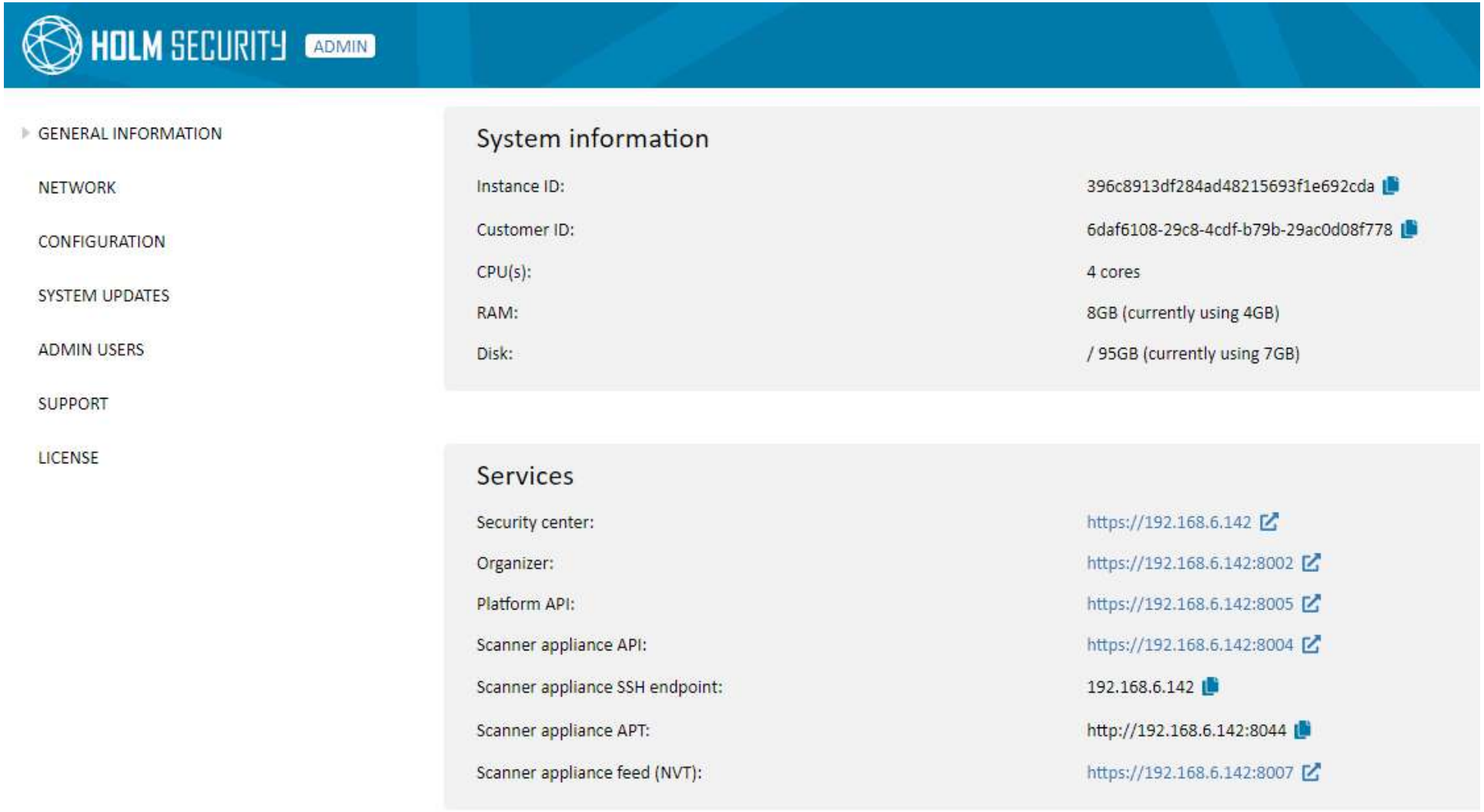
Upload certificate:* Select PEM certificate

Upload key:* Select PEM key

Root ve Intermediate sertifikalarının birlikte tanımlandığı geçerli bir sertifika tercih edebilirsiniz

WEB YÖNETİM PANELİ: YAPILANDIRMA

HOLM SECURITY

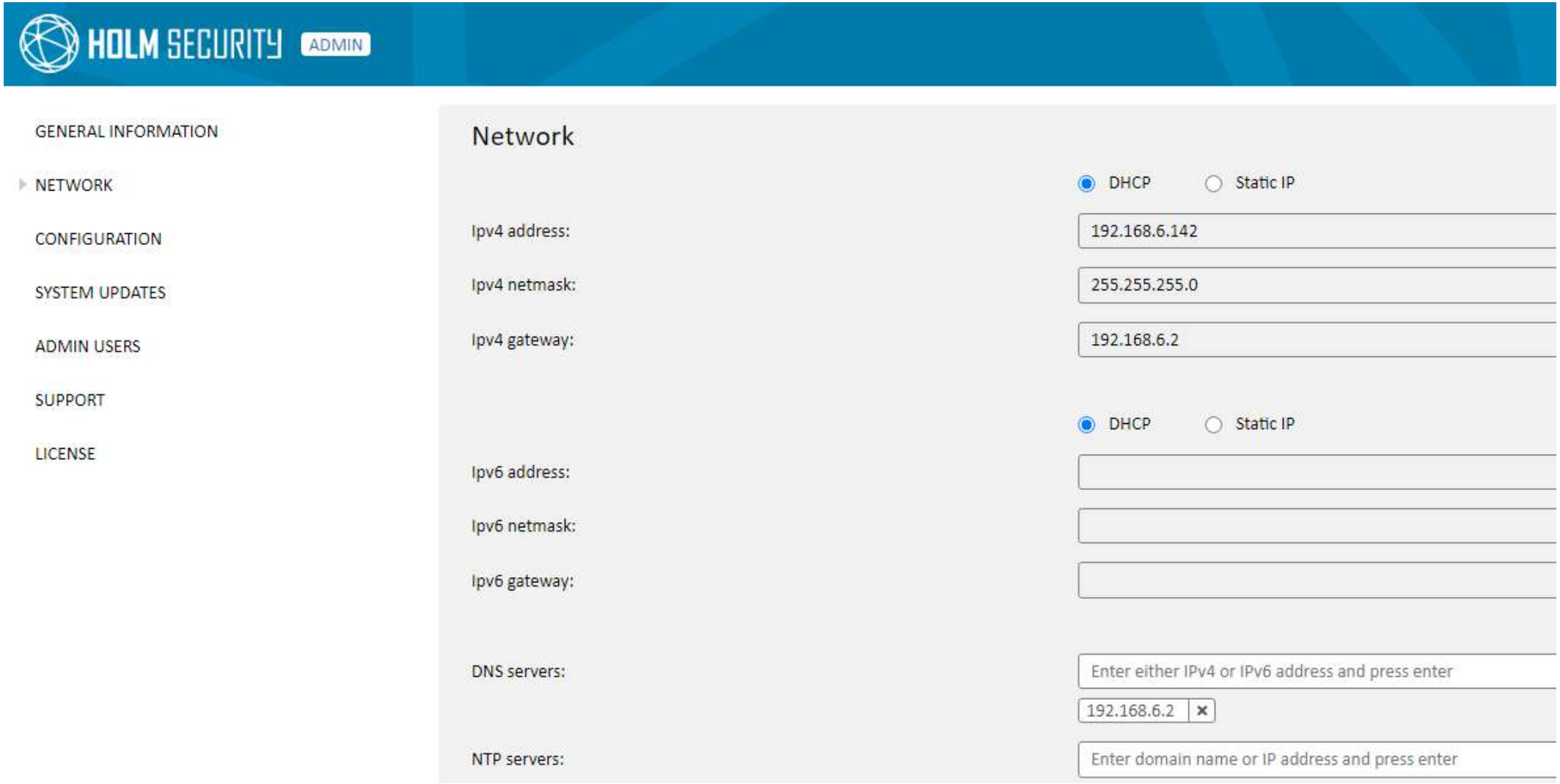


Genel Bilgi: IP adresleri aktif hale gelir. Servisleri ve ilgili TCP portlarını dikkate alın

OTD BİLİŞİM GLOBAL VAD

WEB YÖNETİM PANELİ: YAPILANDIRMA

HOLM SECURITY

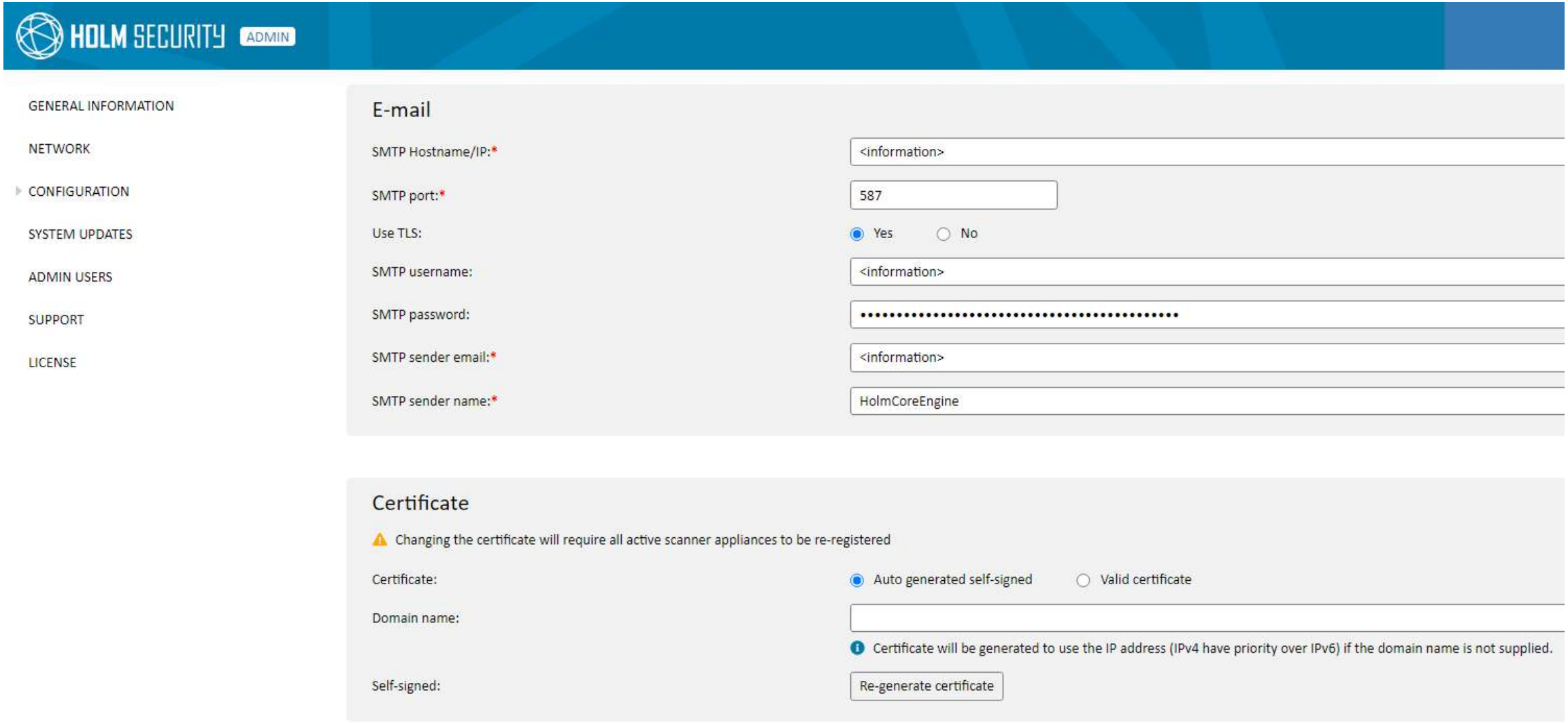


Ağ: IP ayarlarının görüntülenmesi (DHCP veya Statik IP)

OTD BİLİŞİM GLOBAL VAD

WEB YÖNETİM PANELİ: YAPILANDIRMA

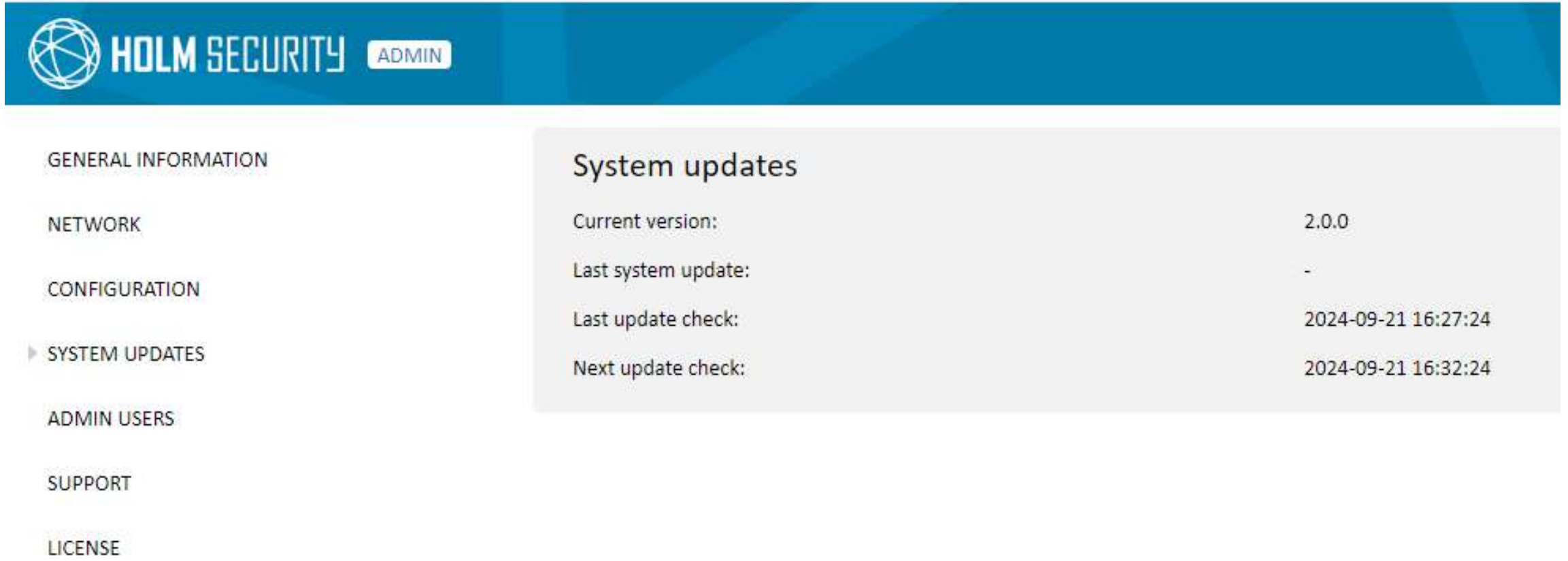
HOLM SECURITY



Yapılandırma: SMTP ve Sertifika girişlerinin özeti

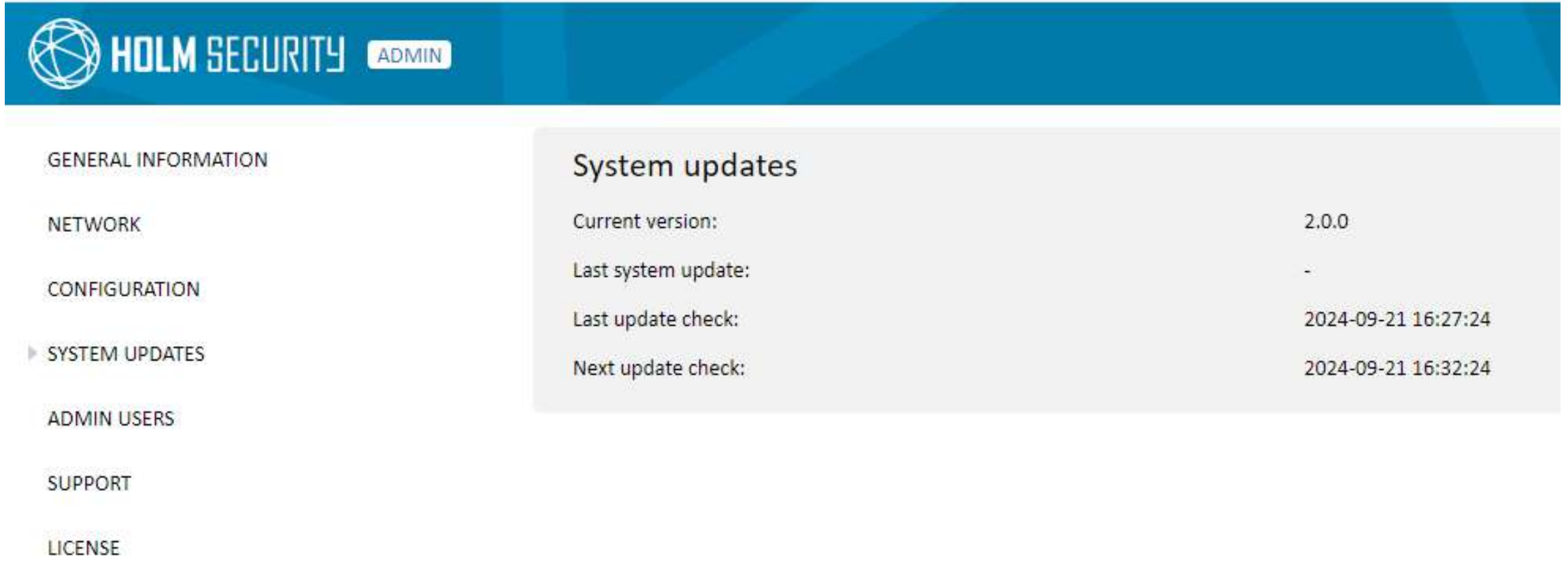
OTD BİLİŞİM GLOBAL VAD

WEB YÖNETİM PANELİ: YAPILANDIRMA



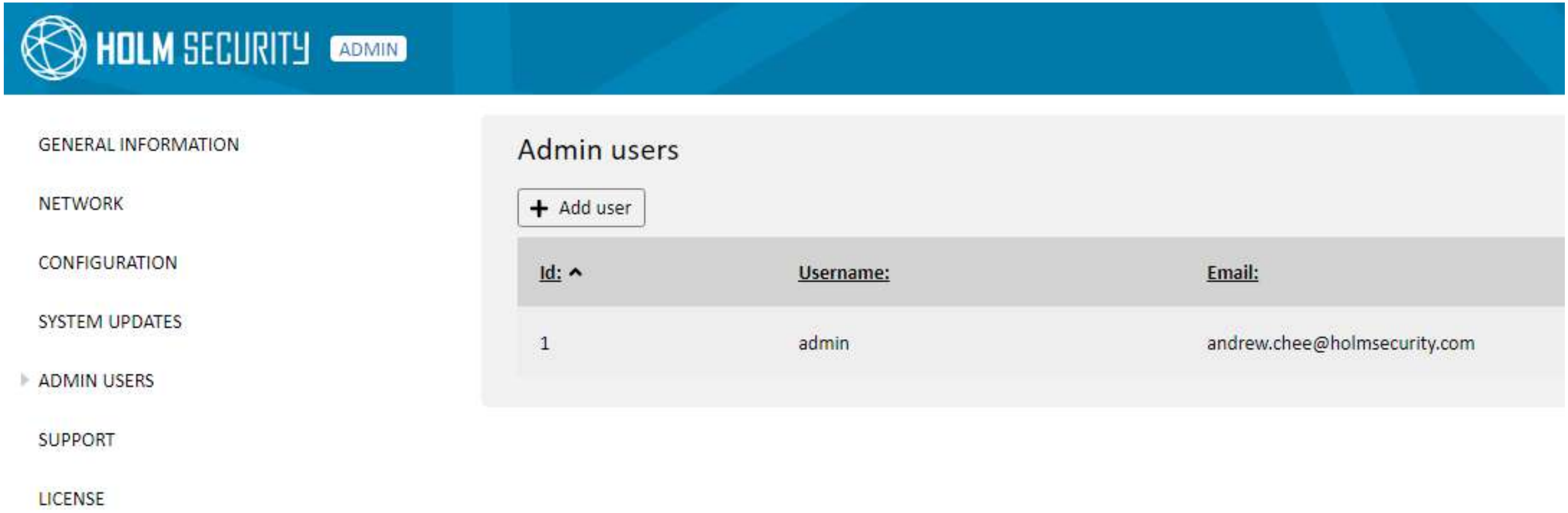
Sistem Güncellemeleri: On-Premise Core Engine'in mevcut sürümü – 2.0.0

WEB YÖNETİM PANELİ: YAPILANDIRMA



Sistem Güncellemeleri: On-Premise Core Engine'in mevcut sürümü – 2.0.0

WEB YÖNETİM PANELİ: YAPILANDIRMA

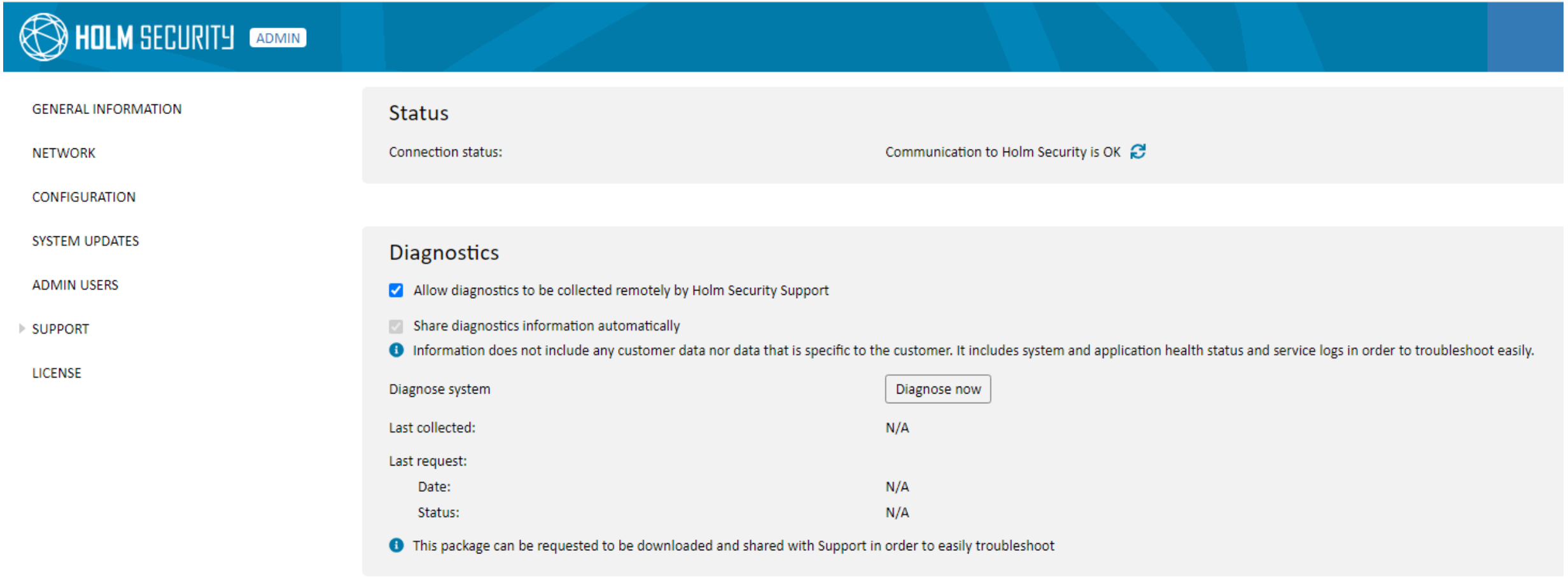


Yönetici Kullanıcılar: Yönetici kullanıcı(lar)ın e-posta adresi

WEB YÖNETİM PANELİ: YAPILANDIRMA

Lisans: Holm Security temsilciniz tarafından sağlanan lisans anahtarını yükleyin

WEB YÖNETİM PANELİ: YAPILANDIRMA



Destek

Durum: Lisans doğrulandıktan sonra Holm Security Veri Merkezi ile iletişim sağlanır

Tanılama: Tanılama loglarının Holm Security Destek ekibi tarafından uzaktan toplanmasına izin verir (gerektiğinde etkinleştirilir).

Log oluşturmak için “Diagnose Now” seçeneğine tıklayın

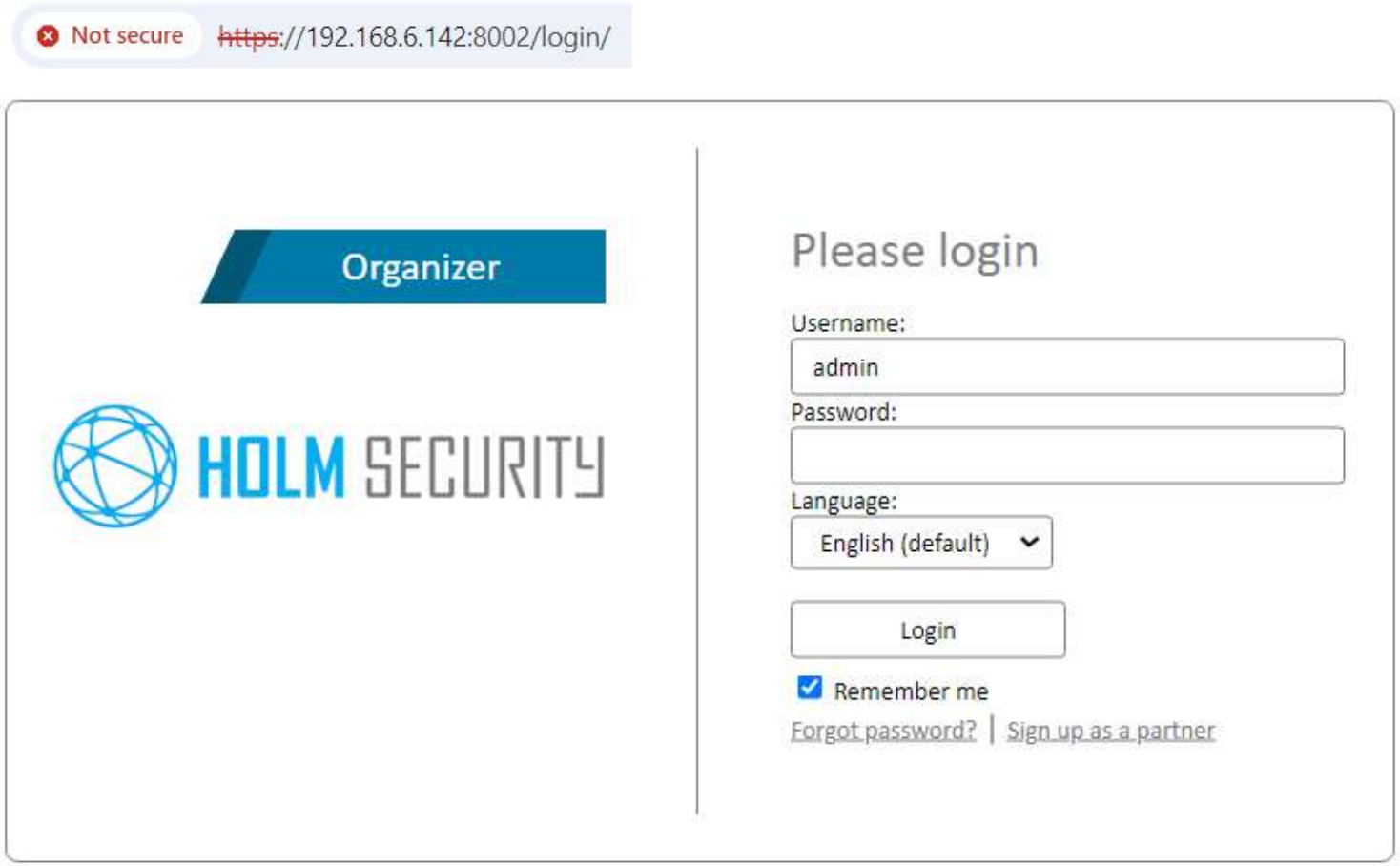
OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Organizatör Portalı

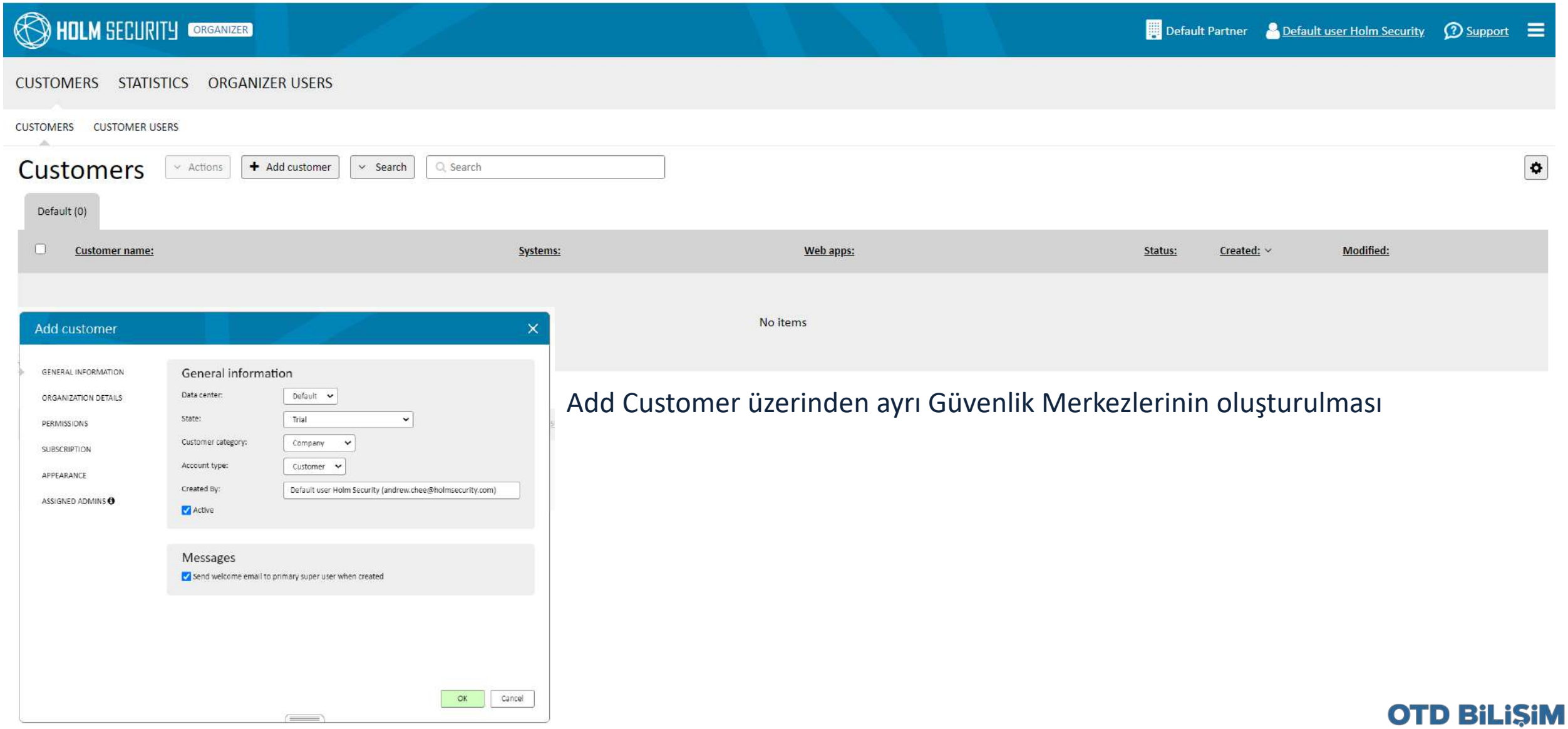
Multi-Tenant oluşturulması

ORGANİZATÖR: İLK GİRİŞ



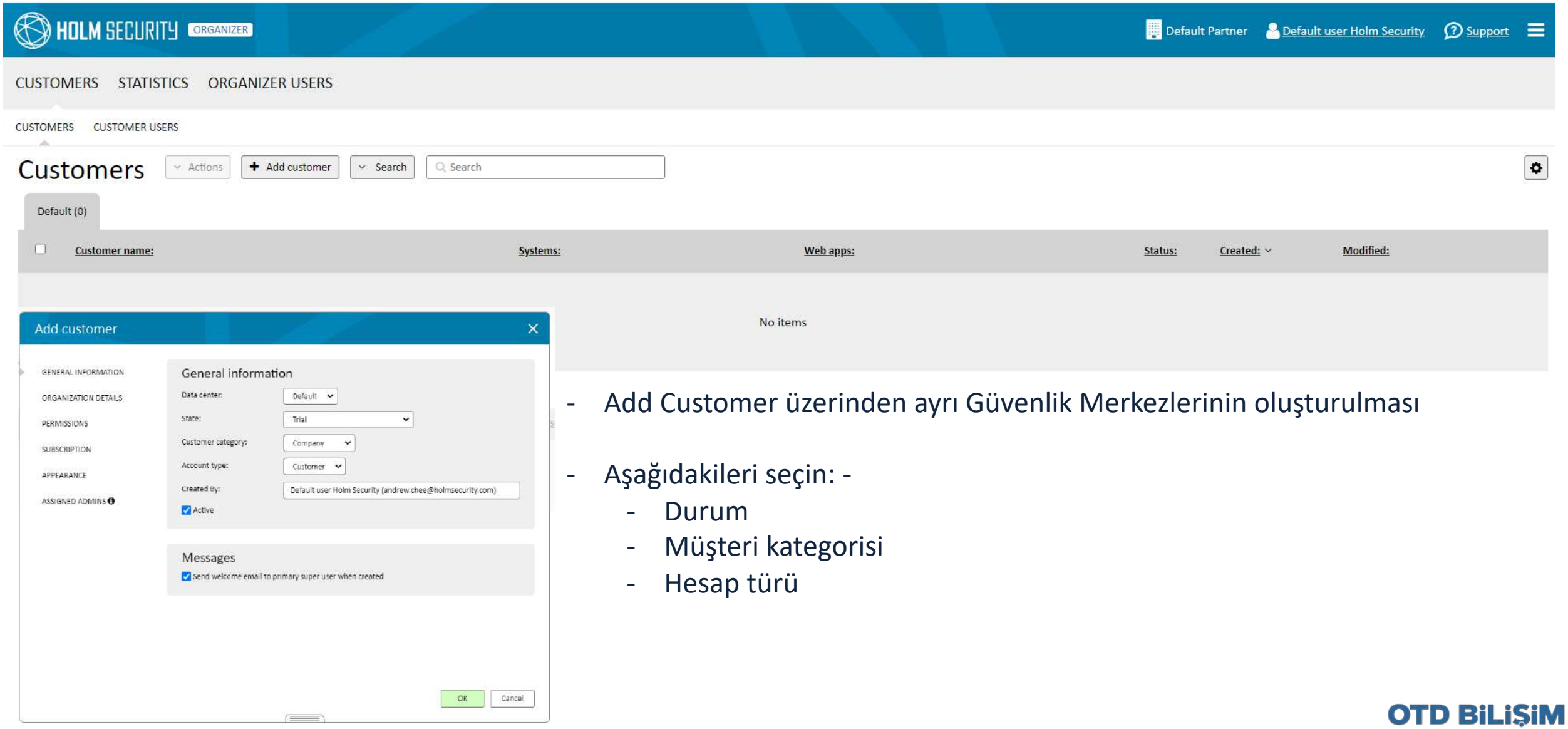
- Organizatör portalını başlatın, örn.: https://core-engine-ip-adresi:8002
- Varsayılan kimlik bilgileri: -
  - Kullanıcı adı: admin
  - Şifre: holmsecurity

ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA



Add Customer üzerinden ayrı Güvenlik Merkezlerinin oluşturulması

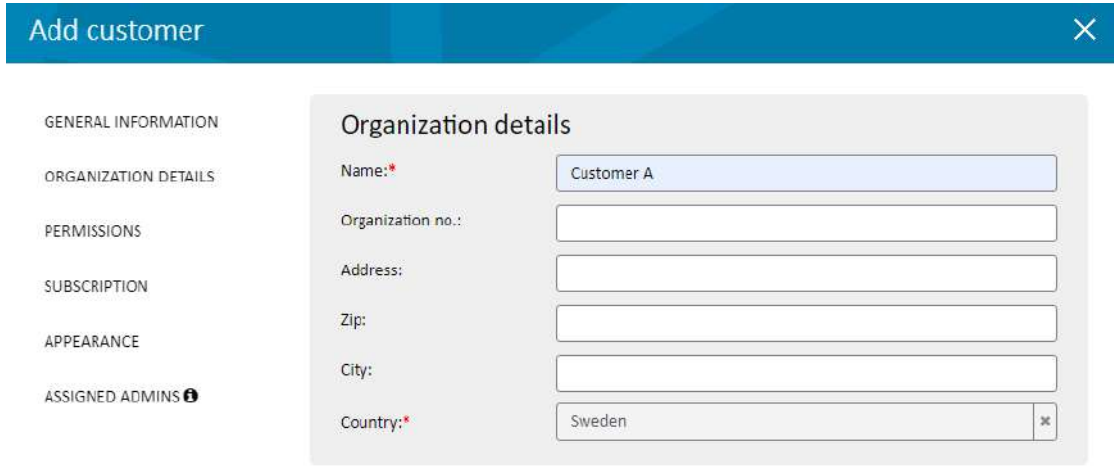
ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA

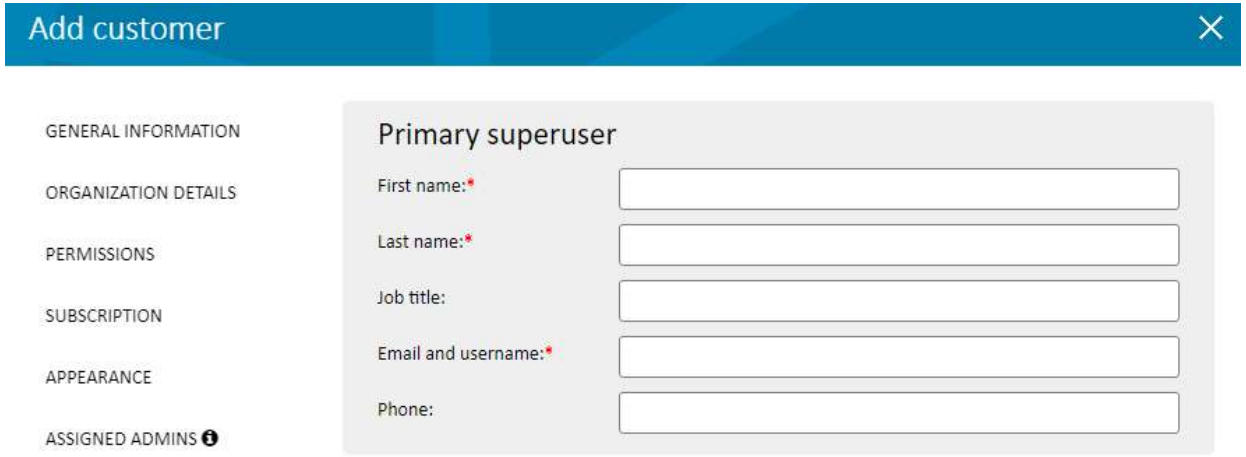


- Add Customer üzerinden ayrı Güvenlik Merkezlerinin oluşturulması

- Aşağıdakileri seçin: -
  - Durum
  - Müşteri kategorisi
  - Hesap türü

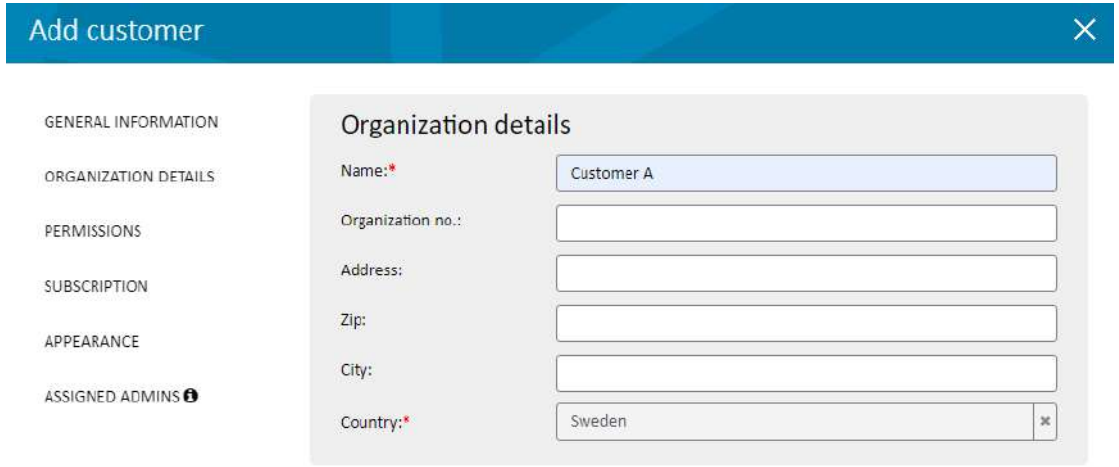
ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA

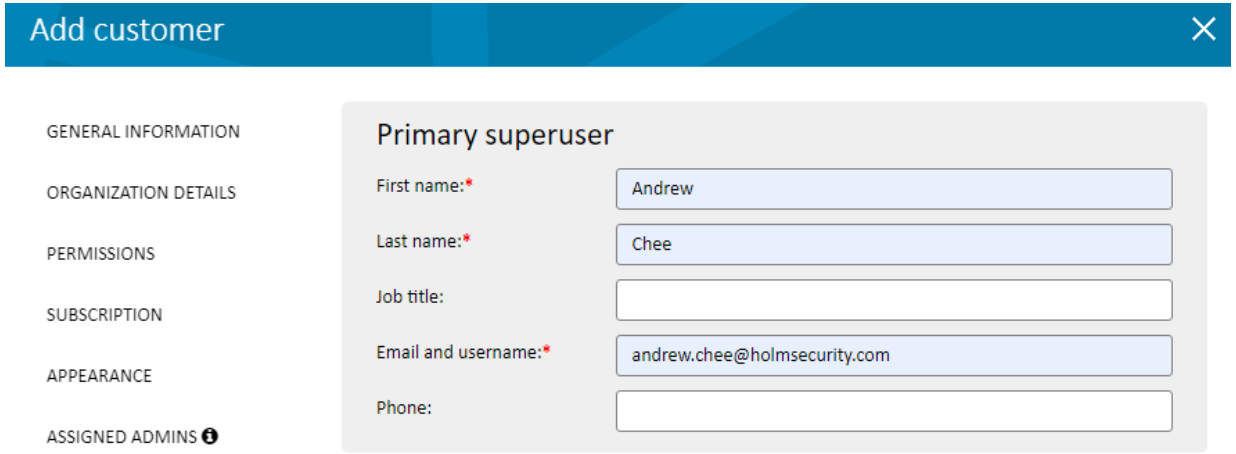




- Organizasyon Bilgileri: -
  - Ad ve ülke zorunludur
- Birincil Süper Kullanıcı
  - Ad / Soyad, e-posta adresi zorunludur

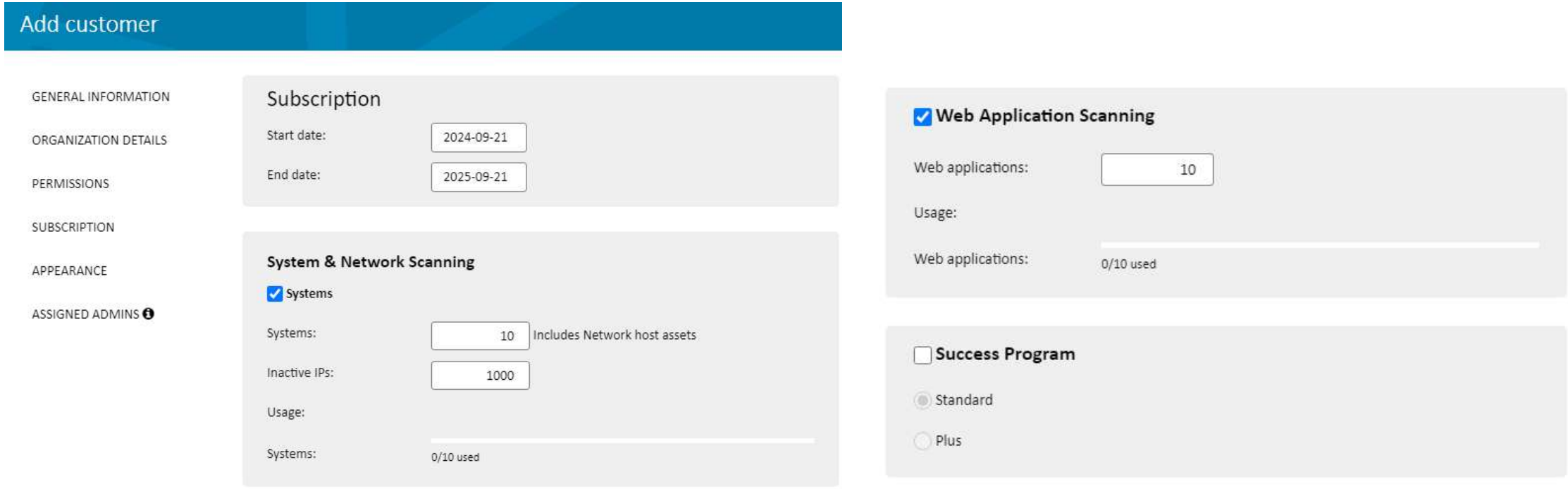
ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA





- Organizasyon Bilgileri: -
  - Ad ve ülke zorunludur
- Birincil Süper Kullanıcı
  - Ad / Soyad, e-posta adresi zorunludur

ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA



- Abonelik
  - Başlangıç ve bitiş için abonelik tarihlerini belirleyin
- Sistem ve Ağ Tarama
  - Aktif host sayısını belirtin
  - İnaktif host sayısını belirtin (daha yüksek bir kapasite için yeterli alan sağlamak amacıyla)
- Web Uygulama Tarama
  - Web uygulaması sayısını belirtin

ORGANİZATÖR: GÜVENLİK MERKEZİ OLUŞTURMA

HOLM SECURITY

HOLM SECURITY ORGANIZER

Default Partner | Default user Holm Security | Support

CUSTOMERS STATISTICS ORGANIZER USERS

CUSTOMERS CUSTOMER USERS

Customers

Actions | + Add customer | Search | Search

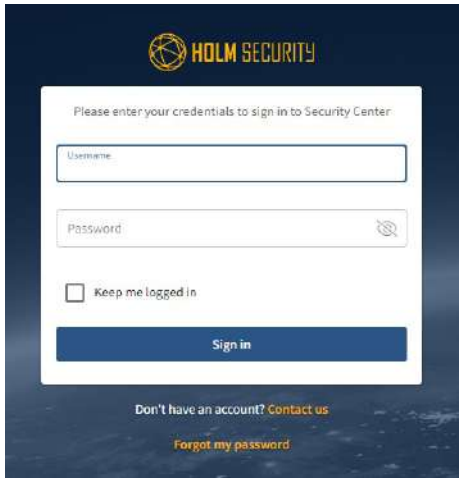
Items 1-1 of 1

Default (1)

Customer name:	Systems:	Web apps:	Status:	Created:	Modified:
Customer B	0	0	Active	2024-09-21 19:31:42	2024-09-21 19:31:42

- İlk Güvenlik Merkezi müşteriniz / hesabınız hazır

Not secure https://192.168.6.142/v/#/auth/login



OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

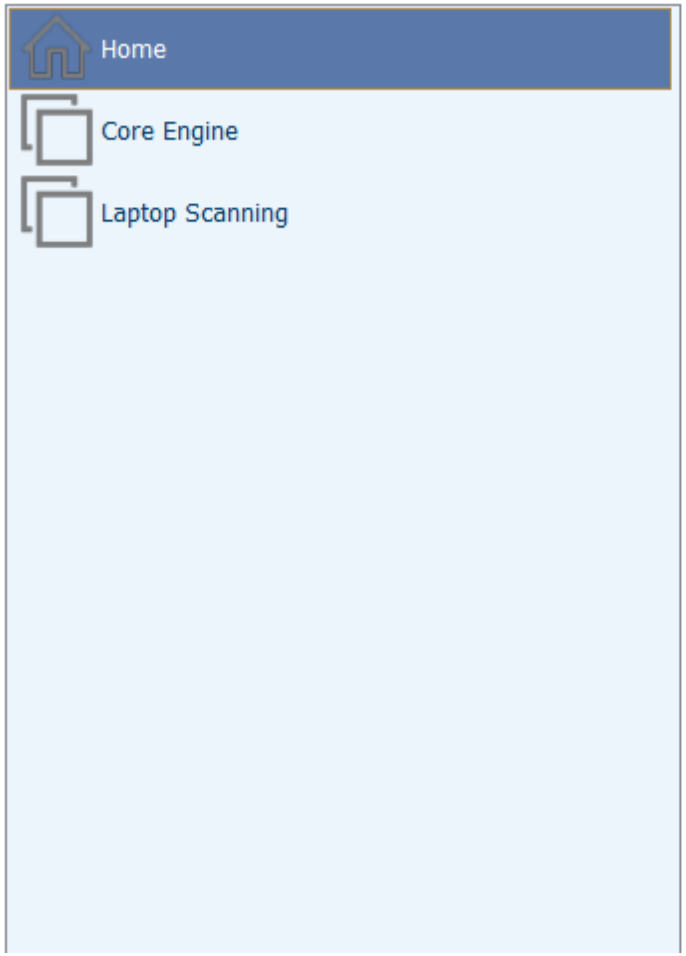
Sanal Tarayıcı Cihazı

Kurulum ve Yapılandırma

TARAYICI CİHAZI: İÇE AKTAR

HOLM SECURITY

Sanal Tarayıcı Cihazı

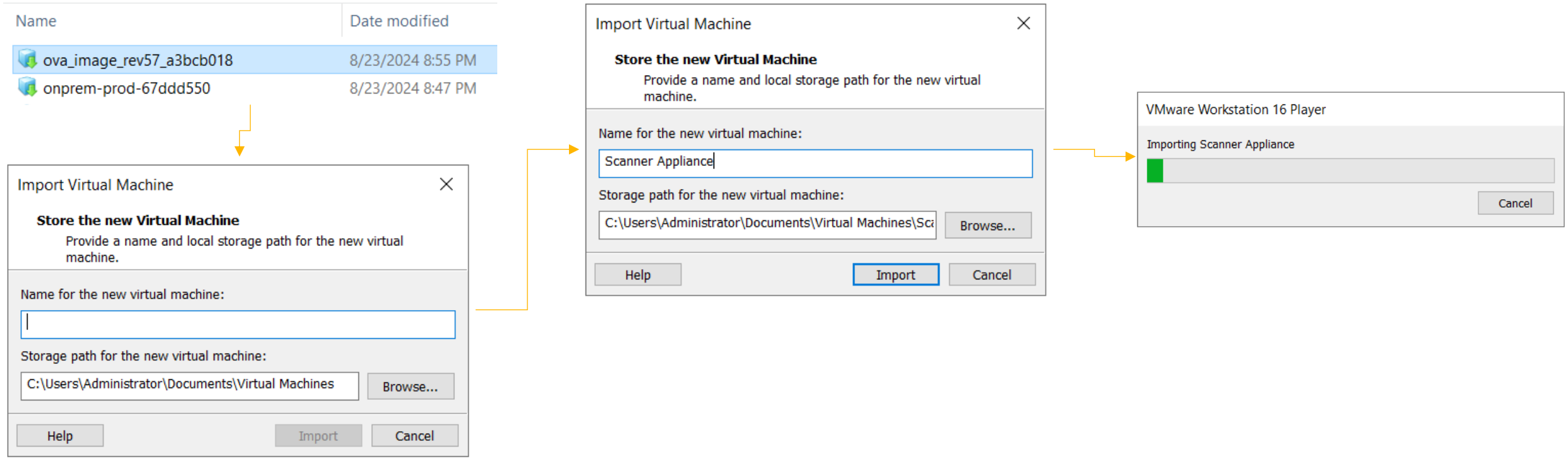


Not: VMWare Workstation Player 16 kullanılarak Core Engine imajının içe aktarım sürecinin simüle edilmesi

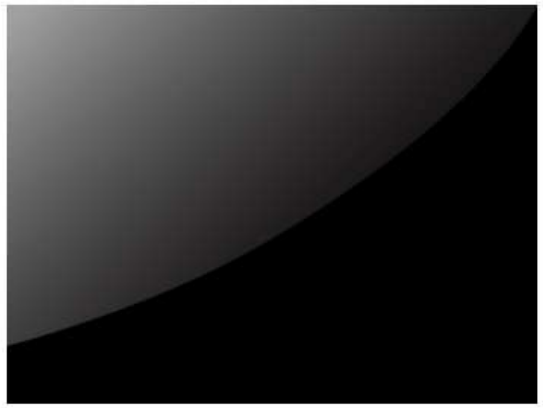
Bir Sanal Makine açın

OTD BİLİŞİM GLOBAL VAD

TARAYICI CİHAZI: İÇE AKTAR



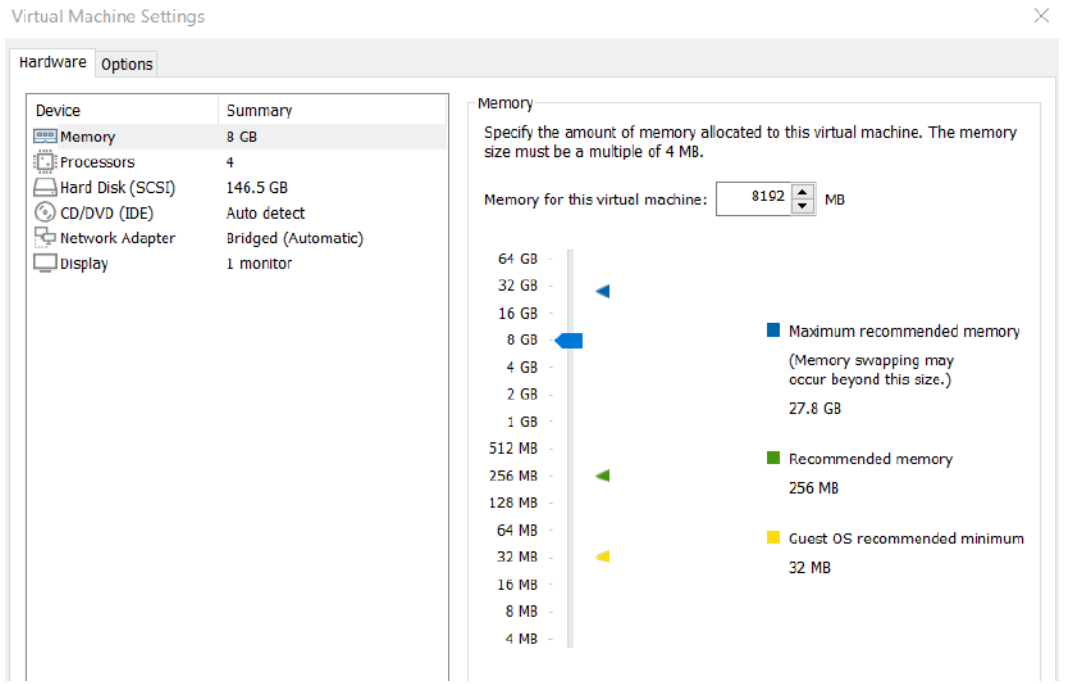
TARAYICI CİHAZI: KURULUM



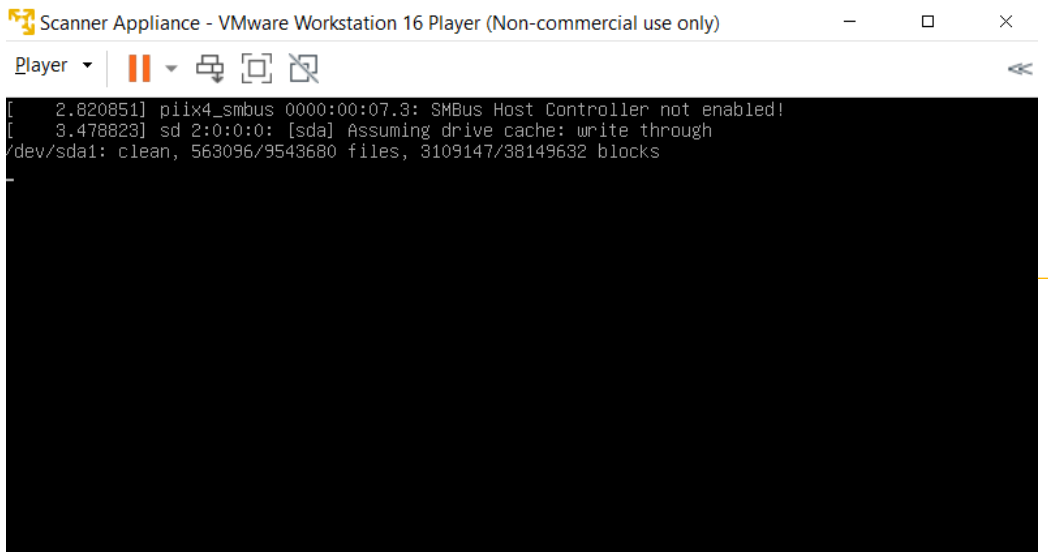
Virtual Machine Name:
Scanner Appliance

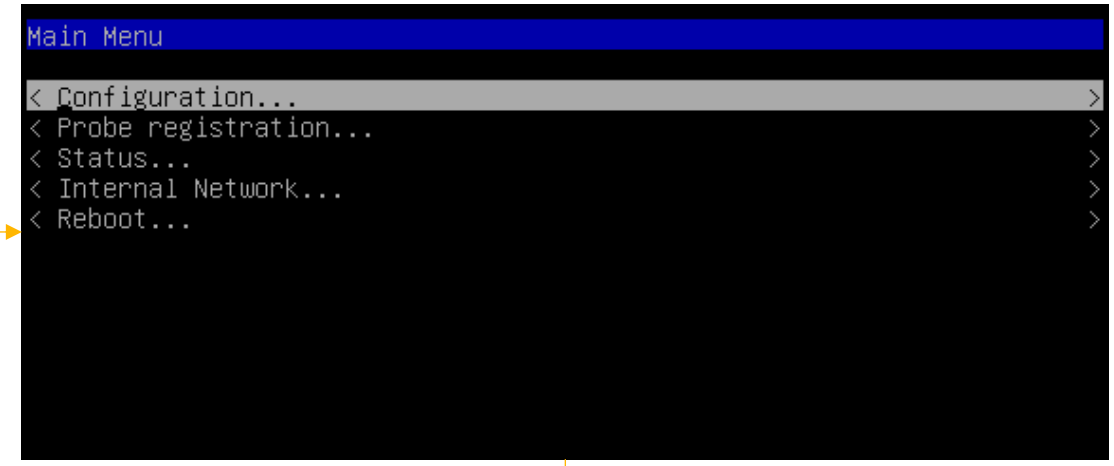
State: Powered Off
OS: Other
Version: Workstation 9.x virtual machine
RAM: 8 GB

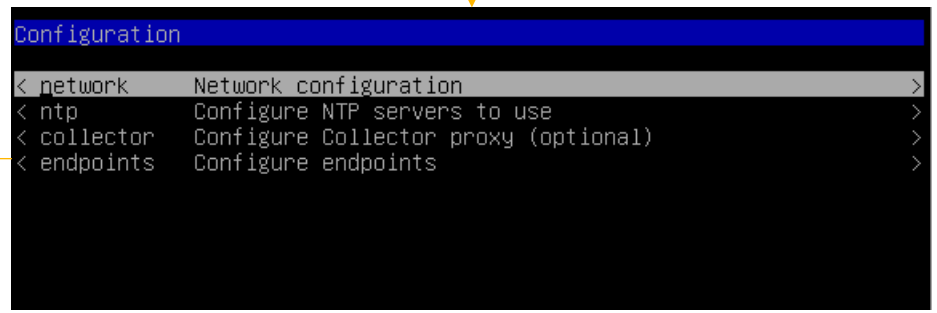
Play virtual machine
Edit virtual machine settings

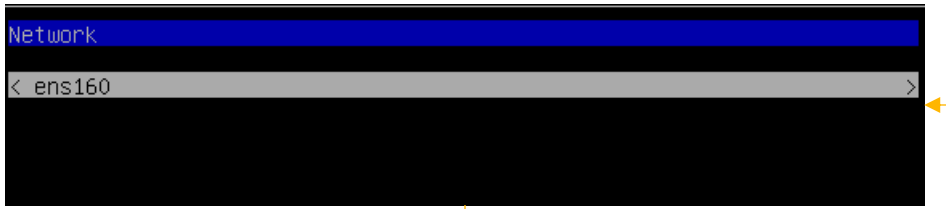


TARAYICI CİHAZI: AĞ YAPILANDIRMASI



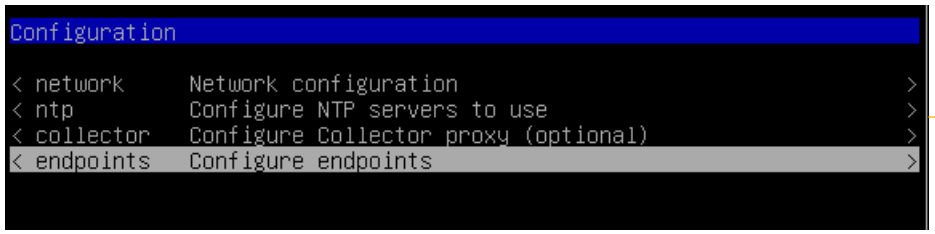


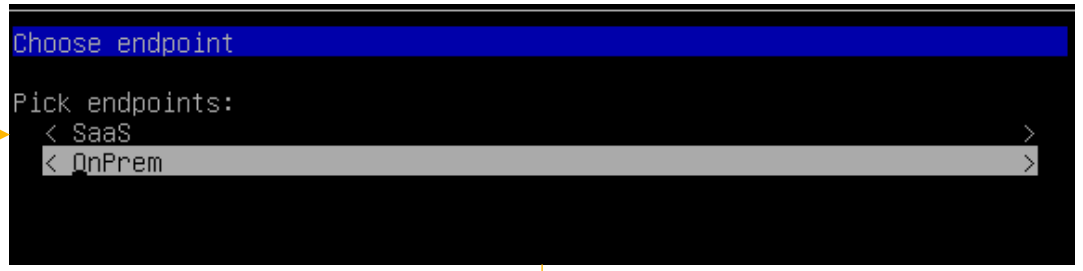


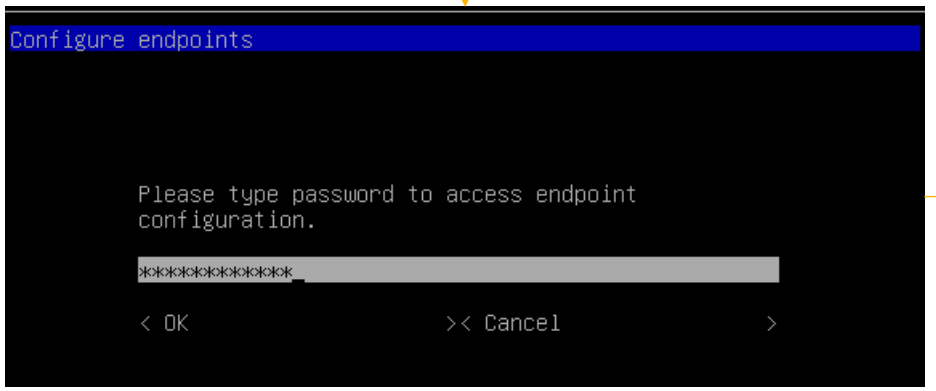


Not: Bu simülasyon, IP adresi için DHCP'ye dayanmaktadır

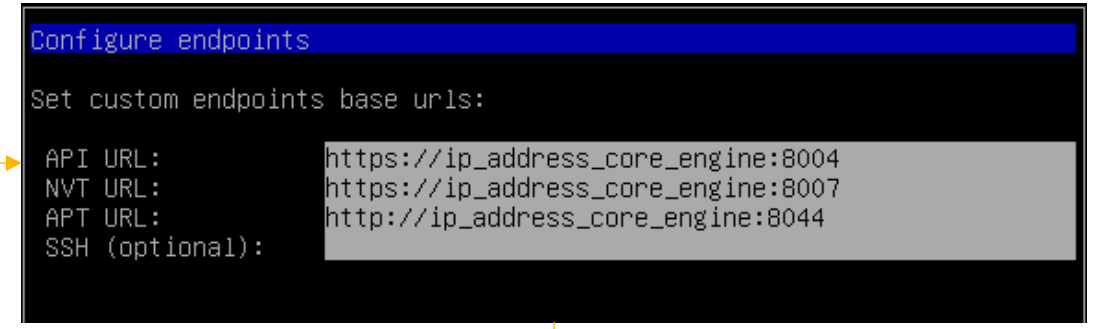
TARAYICI CİHAZI: UÇ NOKTA YAPILANDIRMASI

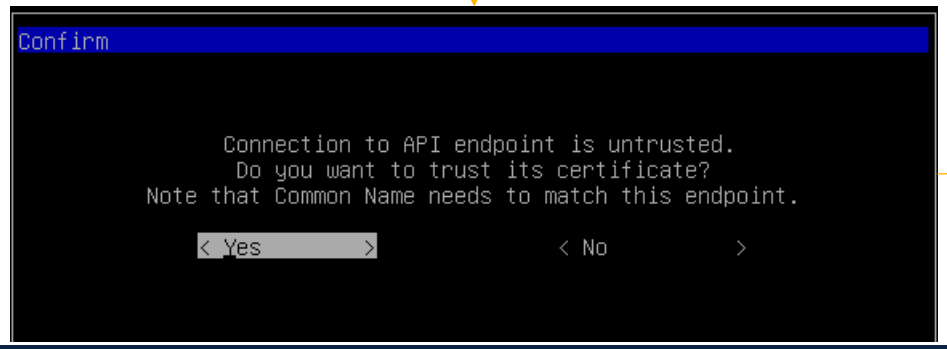






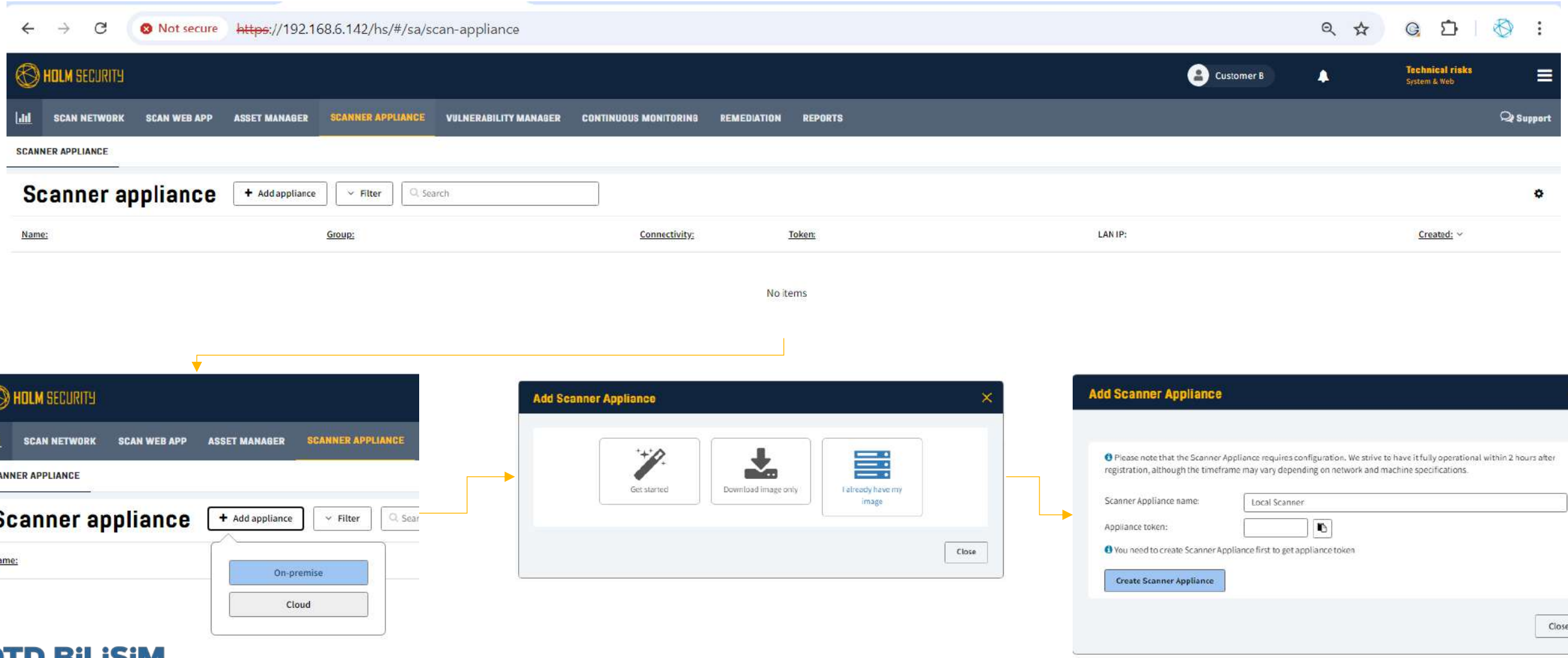
Şifre: appliancebox



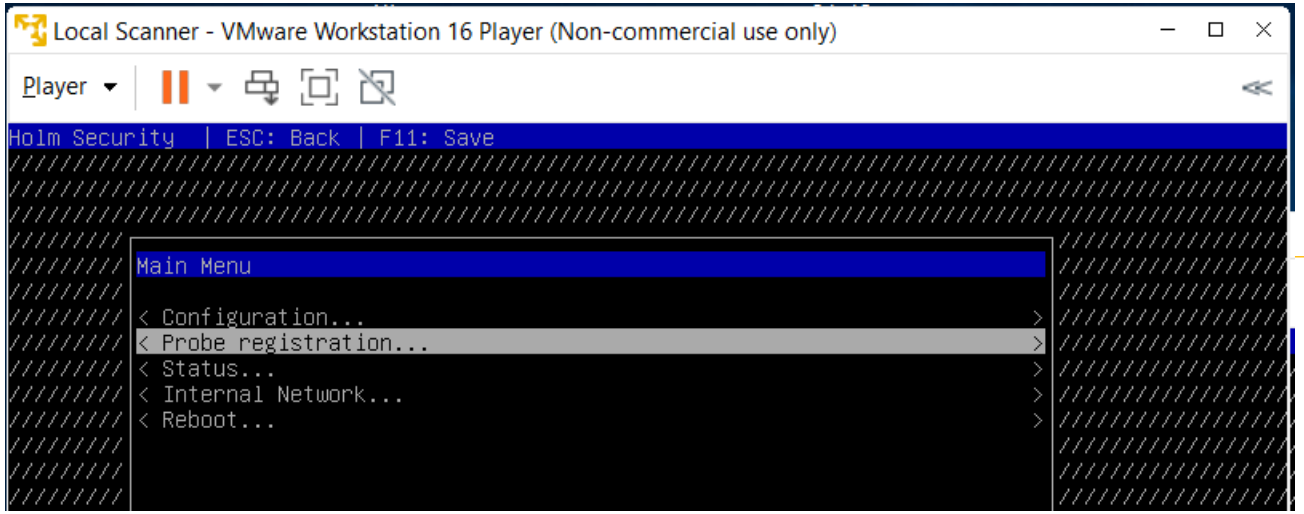


GÜVENLİK MERKEZİ: TOKEN ANAHTARI OLUŞTURMA

- Probe kaydı için Tarayıcı Cihazı token anahtarını oluşturmanız gerekmektedir



TARAYICI CİHAZI: PROBE KAYDI



OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Yeni Nesil Zafiyet Yönetimi

Tüm teknik ve insan varlıklarınızı kapsayarak siber güvenlik savunmalarınızdaki zafiyetleri tespit eder ve siber suçluların bir adım önünde olmanıza yardımcı olur.

Teşekkürler
Q&A

Andrew Chee
andrew.chee@holmsecurity.com

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Sistem ve Ağ Güvenliği

Geniş kapsamlı değerlendirme yetenekleri kullanarak tüm teknik varlıklarınız genelinde 200.000'den fazla zafiyeti tespit eder.

HOLM SECURITY

Varlık keşfi ve izleme

Kör noktaları ve gölge BT'yi tespit etmek için varlıkları otomatik olarak keşfeden entegre ASM ve EASM.

Tüm altyapınızı kapsar

Varlık keşfi ve izlemeyi destekler; ayrıca hem internete açık sistemlerde hem de yerel ağlarda zafiyetleri tespit eder.

Güncel olmayan yazılımları ve yanlış yapılandırmaları tespit eder

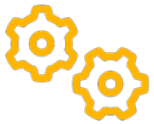
Zafiyetleri, güncel olmayan yazılımları ve çok daha fazlasını tespit eder.

Kapsamlı değerlendirme yetenekleri

Kimlik doğrulamasız ve kimlik doğrulamalı tarama, CIS Benchmark'ları ve bulut yerel platformlar için yerel tarayıcılar gibi birden fazla değerlendirme yeteneğini destekler.

Tüm iş akışını destekler

Güvenlik Merkezimiz; keşif, önceliklendirme, iyileştirme ve raporlama için tek bir merkezi görünüm sunar.



Tamamen otomatik

Otomatik ve sürekli varlık keşfi ve izleme, zafiyet değerlendirmeleri, önceliklendirme, raporlama ve takip.

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Saldırı vektörü kapsamı

HOLM SECURITY

Vektörler:	Açıklama:
Sistemler / sunucular	Microsoft, Linux, Unix, Mac ve diğer platformlar için işletim sistemleri, yazılımlar ve servisler.
Bilgisayarlar	Ofis ağınızdaki kişisel bilgisayarlar ve uzaktaki bilgisayarlar.
Network devices	Firewall, router ve switch gibi ağ ekipmanları.
OT	Üretim ve imalat ortamlarındaki Operasyonel Teknoloji sistemleri için denetim katmanı.
IoT	Sensörler, teşhis, izleme ve alarm sistemleri.
Kubernetes	Container'lar için bulut ve on-prem orkestrasyon platformu.
Bulut yerel platformlar	Azure, AWS, Google ve Oracle Cloud üzerindeki bulut yerel altyapı.
Bulut yerel platformlar	Yazıcılar, web kameraları ve diğer ofis cihazları.

Değerlendirme teknolojileri

HOLM SECURITY

Teknolojiler:	Açıklama:	Kurulum yöntemi:	
		Cloud/SaaS:	On-premise:
Keşif taraması	Bir ağ içerisinde çalışan varlıkların otomatik ve sürekli keşfi ve izlenmesi.	✓	✓
Kimlik doğrulamasız tarama	Sistem, bilgisayar veya cihaza erişim olmadan dışarıdan gerçekleştirilen tarama.	✓	✓
Kimlik doğrulamalı tarama	Taranan hedeflere kimlik doğrulaması yaparak, kurulu uygulama ve paketler üzerinden zafiyetlerin daha derinlemesine analiz edilmesi.	✓	✓
Bulut yerel tarayıcı	AWS, Azure ve Google Cloud gibi bulut yerel platformlar için yerel tarayıcı (Tarayıcı Cihazı).	✓	✓
CIS Benchmark'ları (politika taraması)	Hedef sistemin güvenli yapılandırılması için CIS Benchmark en iyi uygulamaları. Holm Security, Center for Internet Security (CIS) tarafından sertifikalandırılmıştır.	✓	✓
Ajan tabanlı değerlendirmeler	Sunucu veya bilgisayarda yüklü tüm yazılımları çıkararak zafiyetleri tespit eden Windows tabanlı hafif ajan.	✓	✗
Operasyonel Teknoloji (OT)	Görev açısından kritik altyapı ve endüstriyel sistemlerin değerlendirilmesi.	✓	✓
PCI DSS ASV	Payment Card Industry Data Security Standard (PCI DSS) kapsamında uyumluluk taramaları. Holm Security platformu, PCI tarafından Onaylı Tarama Sağlayıcısı (ASV) olarak sertifikalandırılmıştır.	✓	✓

Altyapı yetenekleri

Yetenekler:	Açıklama:	Kurulum yöntemi:	
		Cloud/SaaS:	On-premise:
İnternete açık / herkese açık ağlar	Herhangi bir yazılım, donanım veya kimlik bilgisi gerektirmeden sistemlerin ve ağların çevresel (perimeter) taranması.	✓	✓
Yerel ağlar	Sanal cihaz olarak kurulan tarayıcı (Tarayıcı Cihazı) sayesinde birden fazla yerel ağın eş zamanlı olarak taranabilmesi.	✓	✓
Bulut yerel altyapı	AWS, Azure ve Google Cloud için yerel tarayıcı (Tarayıcı Cihazı) ile bulut tabanlı altyapının taranması.	✓	×
Uzaktaki bilgisayarlar	Hafif uç nokta yazılım ajanımız (Cihaz Ajanı) kullanılarak Windows sistemlerin ajan tabanlı değerlendirilmesi.	✓	×

Zafiyet tespit yetenekleri

HOLM SECURITY

Yetenekler:	Açıklama:
Güncel olmayan yazılımlar	Güncel olmayan işletim sistemlerini, yazılımları ve servisleri tespit eder.
Zayıf parolalar	Yaygın kullanıcı adı ve parolalar ile brute force giriş denemeleri gerçekleştirir.
Yanlış yapılandırmalar	Yanlış yapılandırmaları, açık portları ve servisleri tespit eder.
BYanlış yapılandırmalar	Ağlarınız ve sistemleriniz üzerinde anında görünürlük sağlar.
Zararlı yazılımlar	Taranan sistemlerde bilinen zararlı yazılımları tespit eder.
Açığa çıkan sistem bilgileri	php.info ve sistem yapılandırmaları gibi sistem ve uygulama bilgilerinin açığa çıkmasını tespit eder.
Hatalı SSL sertifikaları	Süresi dolmak üzere olan, süresi dolmuş veya zafiyet içeren SSL sertifikalarını tespit eder.
Zayıf şifreleme	Şifreleme algoritmaları, sürümler ve protokoller dahil olmak üzere zayıf şifrelemeleri tespit eder.

Kurulum seçenekleri

Seçenekler:	Açıklama:
Cloud	Bulut üzerinde SaaS olarak güvenli yönetim ve veri saklama.
On-premise	Kendi altyapınızda kurulu ve çalışan, yerel veri depolama ile. İnternet üzerinden veri aktarımı yapılmaz.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Web Uygulama Güvenliği

Web sitelerinizde ve web uygulamalarınızda OWASP Top 10 gibi geniş bir zafiyet yelpazesini tespit eder.

HOLM SECURITY

Kapsamlı değerlendirme yetenekleri

Finding vulnerabilities CSR ve RFI gibi zafiyetlerin yanı sıra güncel olmayan JavaScript bileşenlerini, zayıf parolaları ve web sunucusu ile web framework yanlış yapılandırmalarını tespit eder.

OWASP Top 10 uyumluluğu

En güçlü uyumluluk çerçevesi ile en yaygın web uygulama zafiyetlerini tespit edin.

Gelişmiş kimlik doğrulama özellikleri

Giriş (login) arkasındaki web uygulamalarını taramak için geniş bir kimlik doğrulama yöntemi yelpazesini destekler.

Modern web uygulama desteği

Modern JavaScript tabanlı web uygulamalarının taranmasını destekler.

Tüm iş akışını destekler

Güvenlik Merkezimiz; keşif, önceliklendirme, iyileştirme ve raporlama için tek bir merkezi görünüm sunar.

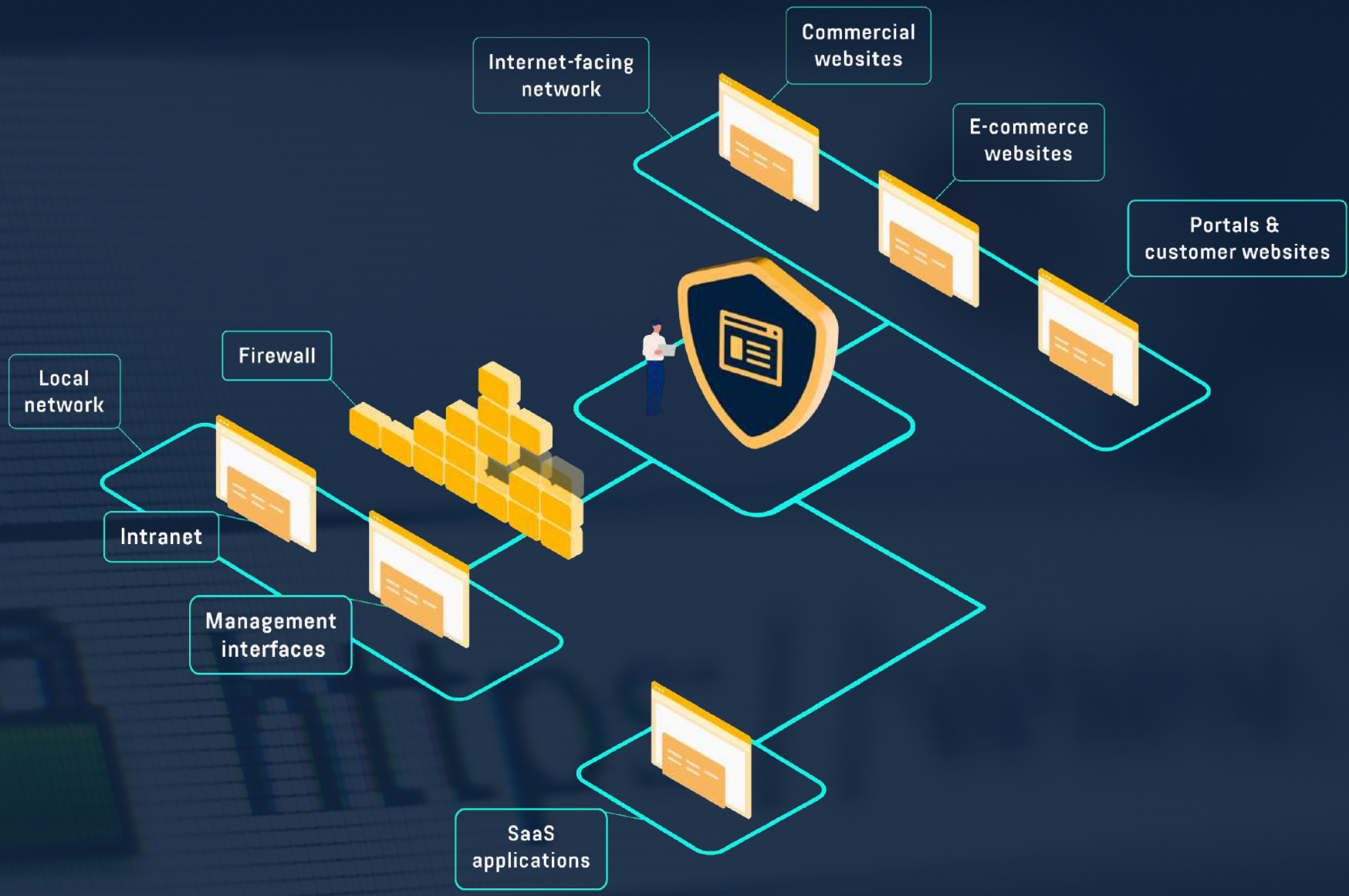
Tamamen otomatik

Otomatik ve sürekli varlık keşfi ve izleme, zafiyet değerlendirmeleri, önceliklendirme, raporlama ve takip.

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY



Değerlendirme teknolojileri

HOLM SECURITY

Teknolojiler:	Açıklama:
Teknolojiler: DAST ve SCA teknolojisi	Web uygulama tarayıcımız, Dinamik Uygulama Güvenliği Testi (DAST) ve Yazılım Bileşen Analizi (SCA) teknolojilerine dayanmaktadır.
İnternete açık ve yerel web uygulamaları	İnternete açık ve yerel web uygulamalarını tarar.
Otomatik tespit	Web sunucularını, programlama dillerini ve veritabanlarını otomatik olarak tanımlar.
JavaScript desteği	AngularJS, VueJS, ReactJS gibi popüler framework'lerle geliştirilen JavaScript tabanlı web sayfalarının taranmasını destekler.
API zafiyetleri	SOAP API'lerini otomatik olarak tespit eder ve OpenAPI v2 ve v3 kullanan REST API'lerin taranmasını destekler.
CMS zafiyetleri	WordPress ve WordPress eklentileri gibi CMS'lerdeki zafiyetleri tespit eder.
Standart kimlik doğrulama desteği	Basic authentication, statik formlar, dinamik JavaScript formları veya özel header'lar kullanarak yetkili kullanıcı olarak zafiyet taraması yapılmasını sağlar.
Gelişmiş kimlik doğrulama desteği	Single sign-on veya çok adımlı kimlik doğrulama gibi gelişmiş senaryolar için, web tarayıcısı üzerinden giriş (login) süreci kaydedilerek login arkasındaki zafiyetlerin taranmasını mümkün kılar.

Zafiyet tespit yetenekleri

HOLM SECURITY

Yetenekler:	Açıklama:
Yanlış yapılandırılmış web sunucuları	Açığa açık dizin listeleme veya herkese açık erişim gibi zafiyetleri tespit eder.
Zayıf parolalar	Yaygın kullanıcı adı ve parolalar ile brute force giriş denemeleri gerçekleştirir.
Güncel olmayan JavaScript bileşenleri	Güncel olmayan ve zafiyet içeren JavaScript bileşenlerini tespit eder.
Açığa çıkan kişisel veriler ve finansal bilgiler	Kişisel kimlik bilgileri ve kredi kartı verileri gibi açığa çıkan hassas bilgileri tespit eder.
OWASP Top 10	OWASP Top 10'un hem 2017 hem de 2021 sürümleri için tam destek sağlar.
Açığa çıkan hassas bilgiler	Kaynak kodu veya yapılandırma değerleri gibi açığa çıkan sistem ve uygulama bilgilerini tespit eder.
Hatalı SSL sertifikaları	Süresi dolmak üzere olan, süresi dolmuş, kullanım dışı kalmış veya zafiyet içeren SSL sertifikalarını tespit eder.
Fuzz testi	Bir web uygulamasının beklenmeyen veya anormal davranışlar sergileyip sergilemediğini tespit eder.

Daha fazlası →

Zafiyet tespit yetenekleri

Yetenekler:	Açıklama:
SQL enjeksiyonu	SQL Injection ve blind SQL Injection zafiyetlerini tespit eder.
Cross-Site Request Forgery (CSRF)	CSRF, son kullanıcının hâlihazırda kimlik doğrulaması yaptığı bir web uygulamasında istenmeyen işlemleri gerçekleştirmeye zorlayan bir saldırıdır.
Remote File Inclusion (RFI)	RFI zafiyeti, saldırganın bir dosyayı indirip çalıştırmasına olanak tanır.
PHP misconfiguration	Yaygın PHP yanlış yapılandırma zafiyetlerini tespit eder.
Sanal host tespiti	Web sunucusunda yapılandırılmış açık sanal hostları tespit eder.
Server-side Include (SSI)	SSI enjeksiyonları, kullanıcı kontrollü girdilerin sunucu taraflı şablonlara gömülmesiyle oluşur ve saldırganların şablon direktifleri enjekte etmesine olanak tanır.
Açığa çıkan e-posta adresleri	Sosyal mühendislik saldırılarında (phishing, spear phishing ve ransomware gibi) kullanılabilecek açık e-posta adreslerini tespit eder.

Kurulum seçenekleri

Seçenekler:	Açıklama:
Cloud	Bulut üzerinde SaaS olarak güvenli yönetim ve veri saklama.
On-premise	Kendi altyapınızda kurulu ve çalışan, yerel veri depolama ile. İnternet üzerinden veri aktarımı yapılmaz.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

API Güvenliği

API’lerinizde OWASP API Top 10 gibi zafiyetleri tespit eder.

HOLM SECURITY

Kapsamlı API teknoloji kapsamı

ScaREST/OpenAPI, GraphQL ve SOAP dahil tüm API'leriniz genelinde tehditleri tarar.

Kapsamlı zafiyet tespiti

Veri doğrulamasının hatalı yapılmasından kaynaklanan SQL enjeksiyonları, parametre ve tip enjeksiyonu zafiyetlerini API'lerinizde tespit eder.

Yanlış yapılandırılmış sunucuları tespit eder

API'yi barındıran sunucudaki yanlış yapılandırmaları tespit eder.

OWASP API Top 10

En güçlü uyumluluk çerçevesi ile en yaygın API zafiyetlerini tespit edin.

Tüm iş akışını destekler

Güvenlik Merkezimiz; keşif, önceliklendirme, iyileştirme ve raporlama için tek bir merkezi görünüm sunar.

Tamamen otomatik

Otomatik ve sürekli varlık keşfi ve izleme, zafiyet değerlendirmeleri, önceliklendirme, raporlama ve takip.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Bulut Güvenliği

Cloud Security Posture Management (CSPM) ile bulut yerel platformlarınız genelinde zafiyetleri tespit edin.

HOLM SECURITY

Bulut varlık keşfi ve izleme

Entegre ASM ile bulut varlıklarını otomatik olarak keşfeder.

Çoklu bulut desteği

Tüm büyük bulut yerel platformları ve Microsoft 365'i destekler, tek bir merkezi görünüm sunar.

Bulut yanlış yapılandırmalarını tespit eder

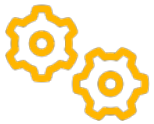
Bulut yerel platformlarınızdaki yanlış yapılandırmalarla ilgili tam görünürlük ve aksiyon alınabilir bağlam sağlar.

Ajan gerektirmeyen

Değerlendirme, bulut yerel platformlarla entegrasyon yoluyla gerçekleştirilir. Herhangi bir yazılım gerektirmez.

Tüm iş akışını destekler

Güvenlik Merkezimiz; keşif, önceliklendirme, iyileştirme ve raporlama için tek bir merkezi görünüm sunar.



Tamamen otomatik

Otomatik ve sürekli varlık keşfi ve izleme, zafiyet değerlendirmeleri, önceliklendirme, raporlama ve takip.

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 Simülasyonu ve Farkındalık Eğitimi

Phishing, ransomware ve diğer kullanıcı hedefli saldırılara karşı korunmak için kendi insan güvenlik duvarınızı oluşturun.

HOLM SECURITY

Tamamen otomatik senaryolar

Simülasyonlar, farkındalık eğitimleri ve takip testlerinden oluşan senaryolar.

Modern farkındalık eğitimi

Phishing simülasyonlarındaki kullanıcı davranışlarına göre otomatik ve özelleştirilmiş nano öğrenme.

Phishing simülasyonu

Gerçekçi, hazır phishing senaryoları ve özelleştirilebilir şablonlar.

Video materyalleri ve testler

Yerleşik farkındalık videoları ve kendi görsel materyallerinizi ekleme desteği. Farkındalık doğrulaması için hazır interaktif anketler.

Bireysel ve ekip risk skorlama

Ek aksiyonları planlamaya yardımcı olmak için bireysel ve ekip risk skorlarını zaman içinde takip edin.

Hazır kullanım

Simülasyonlar, farkındalık eğitimleri ve anketler için hazır ve özelleştirilebilir şablonlar.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

Zafiyet yönetimi programı

HOLM SECURITY

OTD BİLİŞİM GLOBAL VAD

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

UYUMLULUK

ISO 27001

Gereksinimler

Çözümlerimiz

Risk değerlendirmesi (§6.1.2)
ISO 27001, kuruluşların bilgi güvenliği risklerini belirlemek ve değerlendirmek için risk değerlendirmesi yapmasını gerektirir.

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 işleme (§6.1.2)
Riskler belirlendikten sonra, ISO 27001 kuruluşların bir risk işleme planı oluşturmasını zorunlu kılar. Bu planın bir parçası zafiyet yönetimini içerebilir.

Saldırı Yüzeyi Yönetimi (ASM) ve zafiyet yönetimi kullanarak sistematik, otomatik ve sürekli risk değerlendirmeleri sağlayan pazar lideri bir platform. Platformumuz, uyumluluk için proaktif siber savunmaya temel oluşturur.

Kontrol seçimi (§6.1.3)
ISO 27001, standardın Ek A bölümünde kontrol hedefleri ve kontrollerin bir listesini sunar. Bu kontrollerden bazıları doğrudan zafiyet değerlendirme ve yönetimi ile ilgilidir, örneğin:

- A.12.6.1 – Teknik zafiyetlerin yönetimi
- A.14.2.7 – Sistem zafiyet değerlendirmeleri
- A.14.2.8 – Teknik zafiyetlerin giderilmesi

Zafiyet yönetimi programımız ile müşterilerimizin uzun vadeli bir risk işleme planı uygulamasını destekliyoruz.

Sürekli iyileştirme (§10.1)
ISISO 27001, sürekli iyileştirme döngüsünü teşvik eder. Kuruluşların risk değerlendirmelerini, risk işleme planlarını ve bilgi güvenliği kontrollerini düzenli olarak gözden geçirmesi ve güncellemesi gerekmektedir.

Zafiyet yönetimi, kuruluşların ortaya çıkan yeni zafiyetler hakkında bilgi sahibi olmasını ve güvenlik önlemlerini buna göre uyarlamasını sağlayarak bu sürekli süreçte kritik bir rol oynar.

OTD BİLİŞİM
GLOBAL VAD

HOLM SECURITY

UYUMLULUK

NIS & NIS2

NIS DÖNÜM NOKTALARI

NIS2 SEKTÖRLER

Proaktif olarak izlenen sektörler, belirlenmiş denetleyici otoritelere raporlama yapar.
Reaktif olarak izlenen sektörler ise talep üzerine düzenleyici kuruma rapor sunar.

Temel kuruluşlar

Proaktif denetim

- Enerji
- Atık su
- Sağlık hizmetleri
- Drinking water supply & distribution
- Bankacılık
- Finansal piyasa
- Dijital altyapı
- Ulaşım
- Uzay
- Kamu yönetimi

Önemli kuruluşlar

Reaktif denetim

- Atık yönetimi
- Digital distributors
- Postal & courier services
- Kimyasal üretim, işleme ve dağıtım
- Üretim ve imalat
  - Medikal teknoloji ürünleri
  - Bilgisayarlar, elektronik ve optik
  - Elektrikli cihazlar
  - Endüstriyel makineler
  - Motorlu araçlar
  - Diğer ulaşım araçları
- Food production, processing & distribution

Gereksinimler

Çözümlerimiz

HOLM SECURITY

Gereksinimler	Çözümlerimiz
Sistematik ve risk odaklı Bilgi güvenliği kapsamında sistematik, analitik ve risk odaklı adımlar atın ve risk değerlendirmeleri gerçekleştirin.	Saldırı Yüzeyi Yönetimi (ASM) ve zafiyet yönetimi kullanarak sistematik, otomatik ve sürekli risk değerlendirmeleri sağlayan pazar lideri bir platform. Platformumuz, proaktif siber savunma ve NIS2 uyumluluğu için güçlü bir temel oluşturur.
Risk değerlendirmeleri Hem uygulama aşamasında hem de günlük bakım çalışmaları sırasında risk değerlendirmeleri gerçekleştirin.	NIS2 uyumluluğunun ilk aşamasında ve sonrasında sürekli olarak otomatik risk değerlendirmeleri.
Siber hijyen Temel siber hijyen uygulamalarını hayata geçirin ve siber güvenlik eğitimleri uygulayın.	Phishing saldırılarına karşı insan savunmasını, phishing simülasyonu ile birlikte özelleştirilmiş ve otomatik farkındalık eğitimi kullanarak güçlendirin.
Tedarik zinciri değerlendirmeleri Risk değerlendirmeleri NIS2 uyumluluğunun temel bir unsuru olduğundan, tedarikçilerinizin de bu değerlendirmeleri gerçekleştirmesi bir gereklilik olacaktır.	Platformumuz, müşterilerimizin yanı sıra onların tedarikçilerinin de sürekli risk değerlendirmeleri gerçekleştirmesine olanak tanır.
Uyumluluğu gösterin Bugün ve gelecekte uyumluluğu gösterebilir durumda olun.	Sınırsız rapor ve zafiyet verisi arşivi, uyumluluğu hem geçmişte hem de günümüzde gösterir.

Daha fazla çözüm →

Gereksinimler

Çözümlerimiz

HOLM SECURITY

Denetleme
Yönetim, risk yönetiminin uygulanmasını denetler.

Yönetimin; kolay anlaşılır istatistikler ve veriler ile otomatik raporlama üzerinden sürekli risk değerlendirmelerini denetlemesini sağlayan tamamen otomatik bir süreç. Platformumuz, kuruluşunuzun risk maruziyetinin zaman içinde nasıl geliştiğini detaylı şekilde açıklar.

Cezalardan kaçının
İdari yaptırımlardan, kaybedilen izinlerden, sertifikalardan ve cezalardan kaçının.

En kritik iş varlıklarınızı, zafiyetleri ve kör noktaları proaktif ve otomatik olarak tespit ederek koruyun.

OTD BİLİŞİM
GLOBAL VAD

TEDARİK ZİNCİRİ

NIS2 doğrudan ve dolaylı olarak uygulanır

NIS2 doğrudan ve dolaylı olarak uygulanır.

OTD BİLİŞİM GLOBAL VAD

HOLM SECURITY

KULLANIM SENARYOLARI

Operasyonel Teknoloji

Stuxnet zararlı yazılım sabotajı

Kötü amaçlı yazılım ilk olarak 2010 yılında ortaya çıkarıldı.

- İran'daki bir nükleer tesiste uranyum zenginleştirme tesisine saldırmak için kullanıldı.
- İran'ın nükleer santrifüjlerinin yaklaşık beşte birini yok etti.
- 200.000'den fazla bilgisayara bulaştı ve yaklaşık 1.000 makinenin fiziksel olarak zarar görmesine neden oldu.

Ukrayna elektrik şebekesi saldırısı

2015 ve 2016 yıllarında, elektrik şebekesine yönelik siber saldırılar yaklaşık çeyrek milyon Ukraynalının elektriksiz kalmasına neden oldu.

- 30 trafo merkezinin elektriği kesildi ve yaklaşık 230.000 kişi altı saate kadar elektriksiz kaldı.
- SCADA ekipmanları çalışmadı ve elektrik yeniden sağlama işlemi manuel olarak yapılmak zorunda kaldı.

OPERASYONEL TEKNOLOJİ

Denetim katmanı için pazar lideri kapsama

OPERASYONEL TEKNOLOJİ

HOLM SECURITY

Denetim katmanı

Bilgisayarlar (yazılım), ağ veri iletişimi ve İnsan-Makine Arayüzü (HMI).

Denetim katmanı ve üzerindeki tüm katmanlar için tam kapsama sağlar.

Kontrol katmanı

PLCs/RTUs, PIDs, ve DCS.

Kontrol katmanı için kısmi kapsama sağlar.

Saha katmanı

Sensörler, pompalar, aktüatörler, vanalar, motorlar ve diğer çevresel cihazlar.

OTD BİLİŞİM GLOBAL VAD

OPERASYONEL TEKNOLOJİ

HOLM SECURITY

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

75’ten fazla üretici kapsanır

OT üreticilerinin büyük bir kısmı kapsanmaktadır.

3.650+ zafiyet kapsanmaktadır

Kapsamlı OT zafiyet test kapsamı.

OTD BİLİŞİM GLOBAL VAD