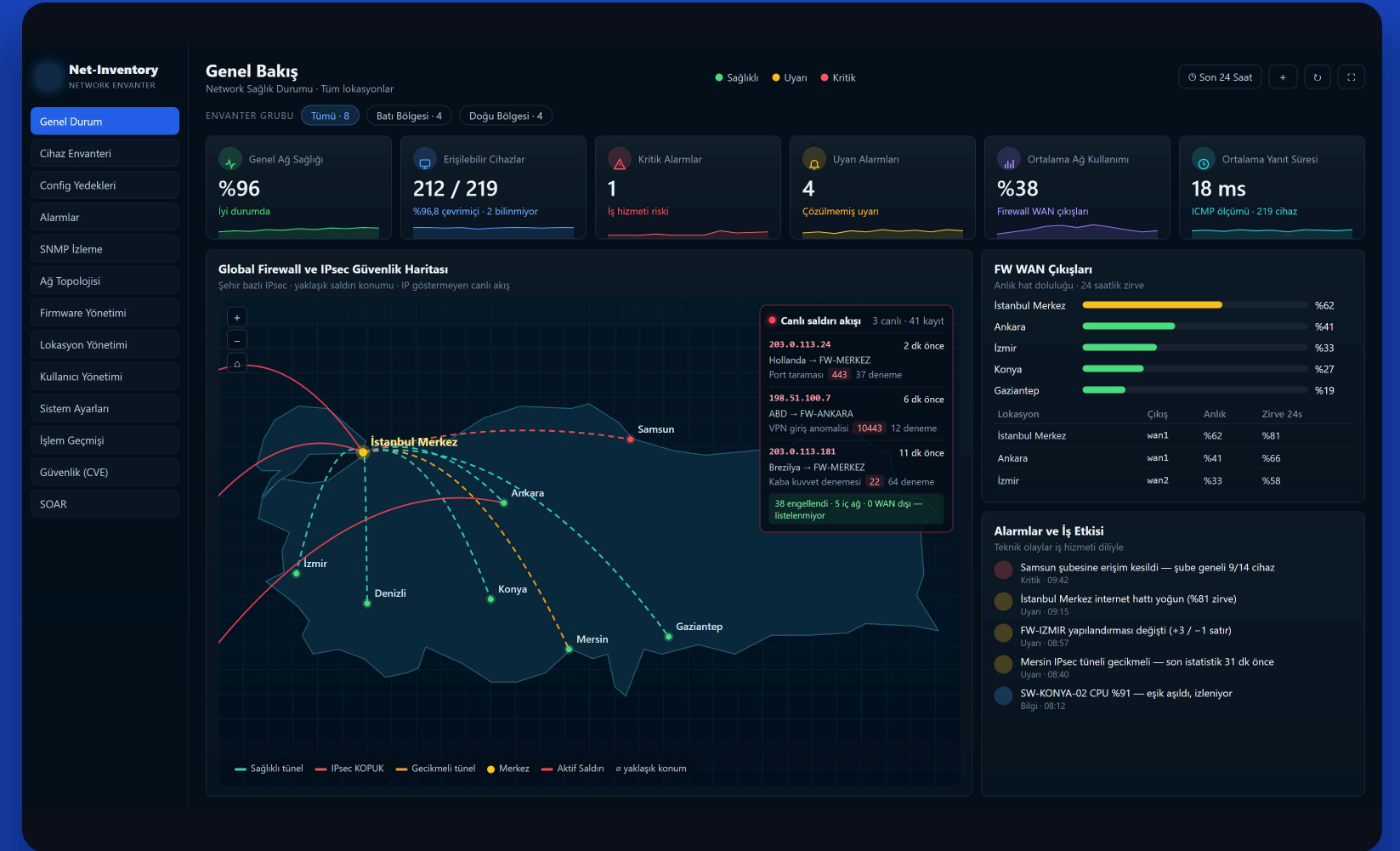


## Ürün Tanıtımı

# Net-Inventory

Çok lokasyonlu ağlar için envanter, izleme ve güvenlik olay yönetimi platformu



# Gündem

- |    |                            |                                                           |
|----|----------------------------|-----------------------------------------------------------|
| 01 | <b>MGMT Bilişim</b>        | Biz kimiz, hangi alanlarda çalışıyoruz                    |
| 02 | <b>İhtiyaç</b>             | Çok lokasyonlu ağların dört ortak sorunu                  |
| 03 | <b>Platform ve Mimari</b>  | Dokuz modül, merkez sunucu ve şube ajanı                  |
| 04 | <b>Ürün Ekranları</b>      | Pano, envanter, bildirimler, SOAR, yedek ve port yönetimi |
| 05 | <b>Güvenlik ve Kurulum</b> | Yetkilendirme, desteklenen cihazlar, devreye alma         |

# MGMT Biliřim Hakkında

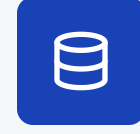
## 2019

Kuruluř yılı

MGMT Biliřim; sunucu, network, siber gvenlik, bulut, yazılım ve KVKK danıřmanlıęı alanlarında kurumlara hizmet verir.

🏠 Kocasinan / Kayseri

**Net-Inventory**, MGMT Biliřim tarafından geliřtirilen aę envanteri, izleme ve gvenlik olay ynetimi platformudur.



### Sunucu ve Storage

Sunucu ve depolama altyapısı



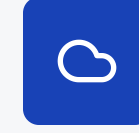
### Network ve Zayıf Akım

Aę ve zayıf akım altyapısı



### Siber Gvenlik

Aę ve sistem gvenlięi



### Cloud Hizmetleri

Bulut altyapı hizmetleri



### Yazılım Geliřtirme

Kurumsal yazılım zmleri



### KVKK Danıřmanlıęı

Kiřisel verilerin korunması

# Çok lokasyonlu ağların dört ortak sorunu



## Dağınık görünürlük

Her şubede farklı marka cihaz ve ayrı yönetim paneli. Hangi cihazın nerede ve ne durumda olduğu tek yerden görülmez.



## Geç fark edilen kesintiler

Bir şube ya da VPN tüneli koptuğunda haber çoğu zaman kullanıcı şikâyetiyle gelir.



## İzlenmeyen değişiklikler

Firewall ve switch yapılandırmasında kimin neyi değiştirdiği, bir sorun çıkana kadar fark edilmez.



## Kaybolan güvenlik olayları

Syslog kayıtları cihazlarda birikir; saldırı denemeleri ve şüpheli girişler incelenmeden kaybolur.

✓ **Net-Inventory** bu dört soruna tek panelden yanıt verir.

# Tek panelde dokuz modül



## Envanter ve keşif

Ağ taraması ve Excel aktarımı;  
marka, model, seri no, sürüm



## Durum izleme

Ping, TCP ve SNMP ile çevrimiçi  
/ çevrimdışı takibi



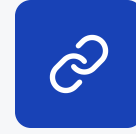
## Performans

CPU, RAM, çalışma süresi ve  
gecikme; eşik uyarısı



## Kesinti bildirimi

SMS ve e-posta; şube geneli  
kesintide tek alarm



## IPsec tünel izleme

Firewall syslog'undan kopma ve  
geri gelme bildirimi



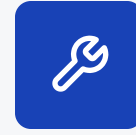
## Güvenlik olayları

SOAR: log toplama, kural, vaka  
ve onaylı müdahale önerisi



## Config yedekleme

Planlı yedek, satır satır fark,  
değişiklik e-postası



## Port, VLAN ve SSH

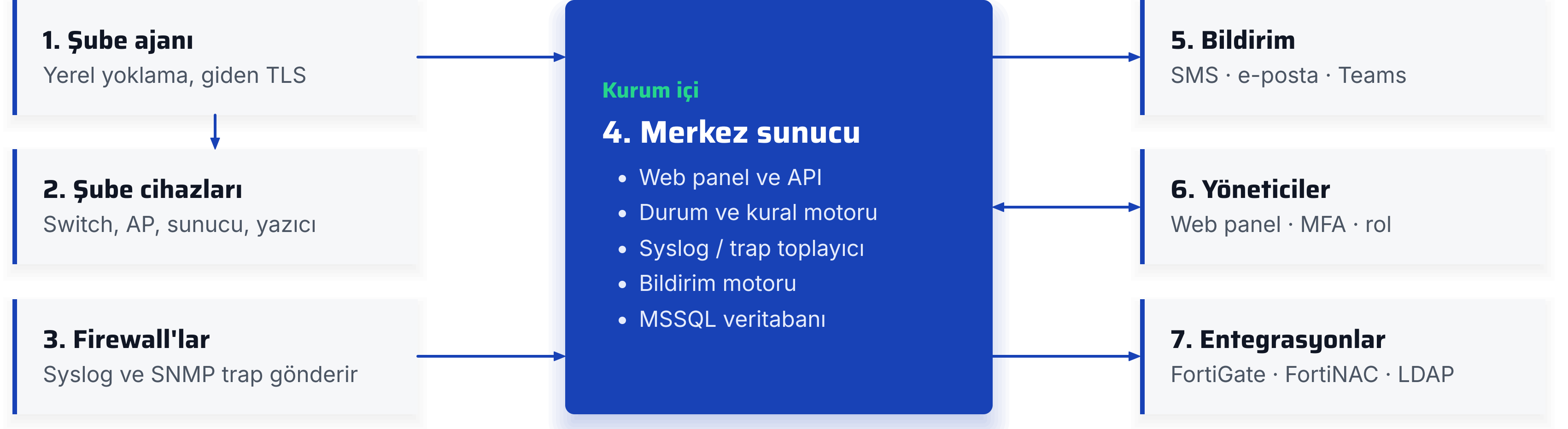
Port paneli, LLDP / MAC, onaylı  
VLAN değişikliği, web SSH



## Rapor ve güvenlik

Yönetici raporları, CVE takibi,  
MFA, rol ve denetim kaydı

# Kurum içi merkez sunucu, şubelerde hafif ajan



## Şubede port açmak gerekmez

Ajan merkeze kendisi bağlanır (giden TLS).

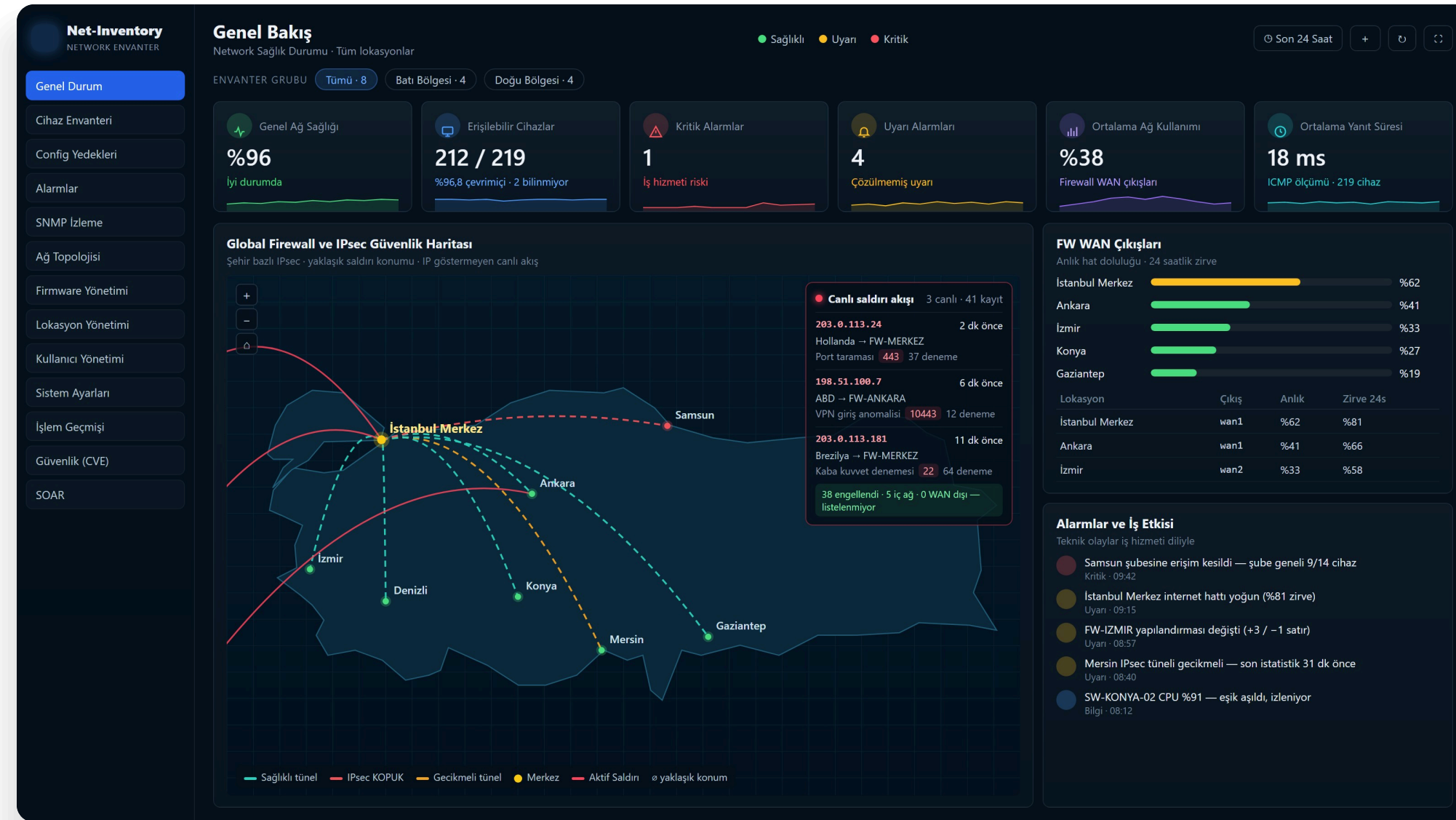
## Veriler kurum sunucusunda

Envanter, log ve yedekler kurumun kendi veritabanında.

## Ajansız izleme de mümkün

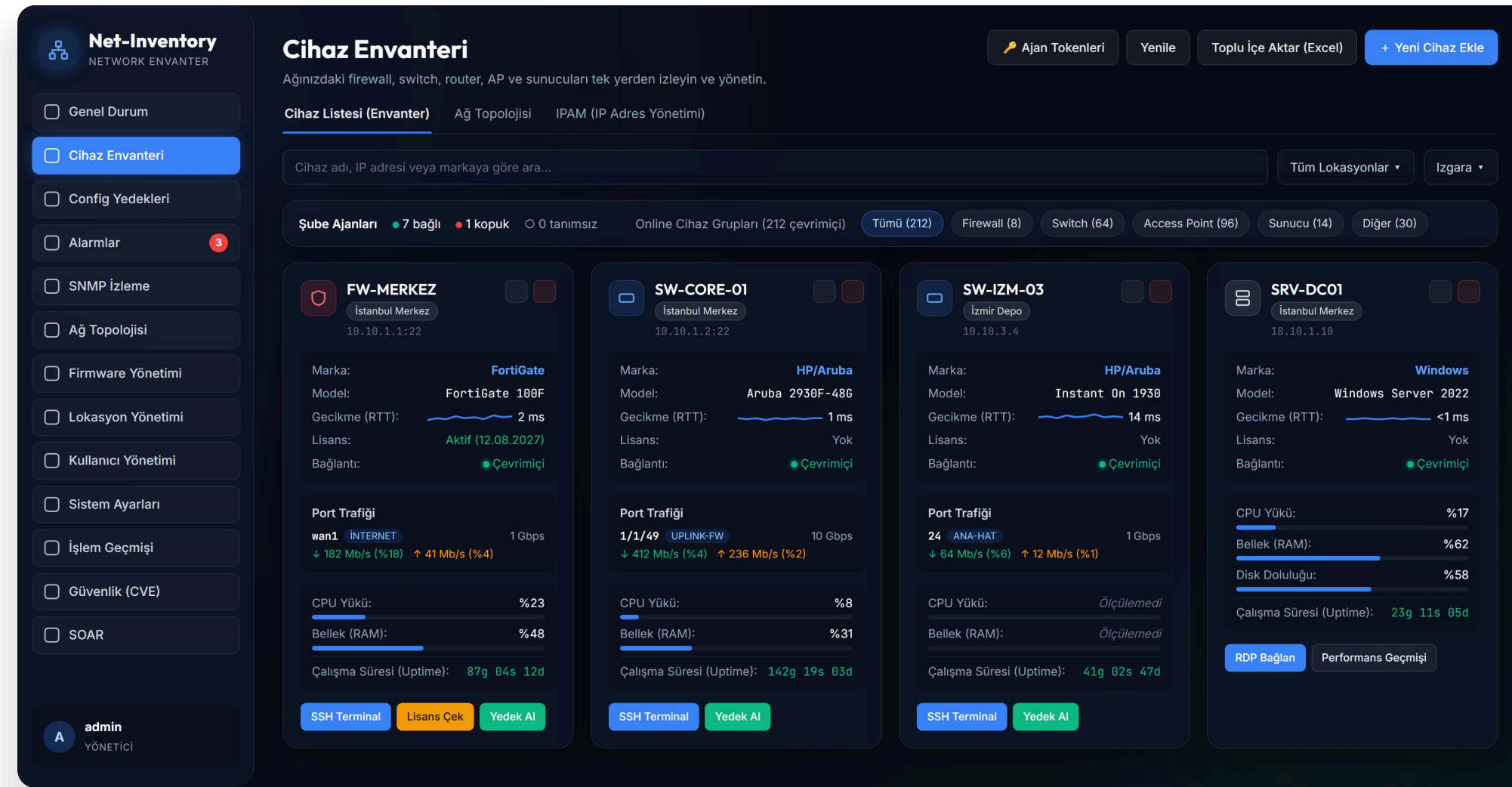
Merkezden erişilen cihazlar doğrudan izlenir.

# Genel Bakış: ağın sağlığı tek ekranda



- ✓ **Sağlık göstergeleri**  
Lokasyon, cihaz ve tünel durumu; açık alarm sayısı tek bakışta.
- ✓ **Güvenlik haritası**  
Firewall loglarındaki saldırı kaynakları ve şube tünelleri harita üzerinde.
- ✓ **Alarmlar iş diliyle**  
Teknik kod yerine: hangi şube, hangi cihaz, ne zamandan beri.

# Cihaz envanteri: tüm cihazlar ve canlı performans



- ✓ **Tüm markalar tek listede**  
FortiGate, HP/Aruba, Cisco, Huawei ve diğerleri; lokasyona göre gruplu.
- ✓ **Canlı kaynak kullanımı**  
CPU, RAM ve çalışma süresi SNMP ya da SSH ile ölçülür; eşik aşıldınca uyarı.
- ✓ **Dürüst ölçüm**  
Ölçülemeyen değer uydurulmaz; kartta "Ölçülemedi" yazar.

# Kesinti uyarısı: teyitli, sınırlı, tekrarsız

✓ 60 sn teyitli alarm

✓ 30 dk arayla en çok 3 bildirim

✓ Şube toptan düşerse tek alarm, tek SMS

**Net-Inventory**  
NETWORK ENVANTER

☐ Genel Durum
 ☐ Cihaz Envanteri
 ☐ Config Yedekleri
 ☒ Alarmlar 3
☐ SNMP İzleme
 ☐ Ağ Topolojisi
 ☐ Firmware Yönetimi
 ☐ Lokasyon Yönetimi
 ☐ Kullanıcı Yönetimi
 ☐ Sistem Ayarları
 ☐ İşlem Geçmişi
 ☐ Güvenlik (CVE)
 ☐ SOAR

**admin**  
YÖNETİCİ

**Sistem Alarmları**  
Ağ cihazlarındaki bağlantı kesintileri ve kritik sistem durum alarmları.

Aktif Alarmlar

3

Onaylanan Alarmlar

27

Toplam Kayıt

30

Aktif Alarmlar (3)

Onaylananlar (27)

Tüm Geçmiş (30)

Alarm filtrele — cihaz adı / IP / neden

☐ sadece kesinti 3 kayıt

| Durum   | Cihaz Bilgisi                             | Lokasyon          | Mesaj                                                                                                                 | Zaman                              | İşlemler                                        |
|---------|-------------------------------------------|-------------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------------------|
| • AKTİF | <b>Samsun — şube geneli</b><br>9/14 cihaz | 📍 Samsun Şube     | Samsun Şube: 9/14 cihaz aynı anda erişilemiyor (ilk düşüş 09:42) — tek lokasyon alarmı, cihaz alarmları bağlandı      | 12 dakika önce<br>14.10.2026 09:42 | <button>Onayla</button> <button>Sustur</button> |
| • AKTİF | <b>IPsec SAMSUN-VPN</b><br>10.10.1.1      | 📍 İstanbul Merkez | IPsec tüneli koptu: SAMSUN-VPN — FW-MERKEZ (başlangıç 14.10.2026 09:43; kaynak: firewall syslog)                      | 10 dakika önce<br>14.10.2026 09:46 | <button>Onayla</button> <button>Sustur</button> |
| • AKTİF | <b>FW-İZMİR</b><br>10.10.3.1              | 📍 İzmir Depo      | [CONFIG DEĞİŞTİ] FW-İZMİR: +3/-1 satır (önceki yedek #418) — firewall policy 14. Yetkisiz değişikse geri dönülebilir. | 57 dakika önce<br>14.10.2026 08:57 | <button>Onayla</button> <button>Sustur</button> |
| KAPANDI | <b>AP-KONYA-04</b><br>10.10.4.24          | 📍 Konya Fabrika   | AP-KONYA-04 bağlantısı geri geldi — kesinti 6 dk (ICMP + TCP yanıtız)                                                 | 2 saat önce<br>14.10.2026 07:31    | <button>Sil</button>                            |

09:46
 5G

NI
 NET-INVENTORY

Bugün 07:28

**KESİNTİ (1/3)**  
 Lokasyon: Konya Fabrika  
 Cihaz: AP-KONYA-04  
 IP: 10.10.4.24  
 Tür: Ping+TCP yanıtız  
 Suredir: 3 dk

**COZULDU**  
 Lokasyon: Konya Fabrika  
 Cihaz: AP-KONYA-04  
 IP: 10.10.4.24  
 Kesinti suresi: 6 dk  
 Durum: CEVRİMİCİ

Bugün 09:45

**LOKASYON OLAYI (1/3)**  
 Lokasyon: Samsun Şube  
 Etkilenen: 9/14 cihaz  
 SW-SAM-01, SW-SAM-02, AP-SAM-01, AP-SAM-02, AP-SAM-03, YAZ-SAM-01 ... (+3)  
 Suredir: 3 dk

# Tünel koptu, tünel geri geldi: ikisi de SMS

- ✓ Kaynak: firewall syslog'u
- ✓ 180 sn teyit
- ✓ Birlikte kopan tüneller tek mesaj
- ✓ Dönüşte kesinti süresi

SMTP Ayarları
Active Directory (DC/LDAP)
SMS Ayarları
Firma Bilgileri
Yedekleme Ayarları
Alarm Eşikleri
Bildirim Kanalları
SOAR Ayarları
Gelişmiş Ayarlar

### IPsec Tünel Bildirimi

Firewall syslog'undaki IPsec olaylarından: tünel **koptu** (teyit süresi kadar geri gelmezse) → panel alarmı + **admin rolündeki kişilere SMS; geri geldi** → kesinti süresiyle SMS. Birlikte kopan tüneller tek mesajda. Syslog hiç gelmiyorsa tünel durumu **bilinmez** — "koptu" denmez.

IPsec tünel bildirimi
etkin
ayarlı
ipsec\_bildirim

IPsec: bildirim yapılacak firewall
FW-MERKEZ
ayarlı
ipsec\_izlenen\_fw

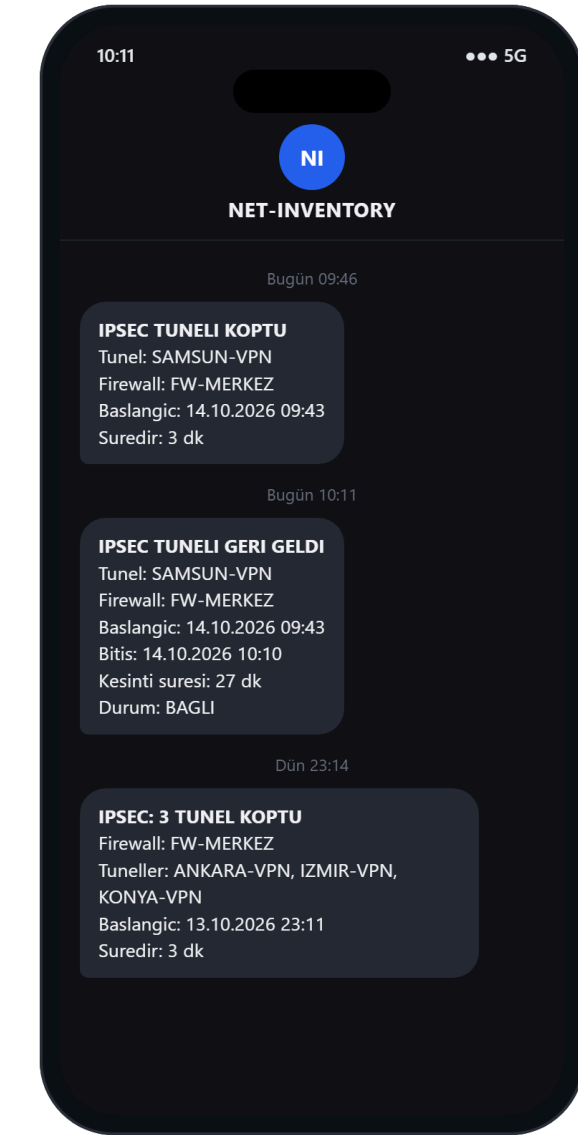
IPsec: kopma teyit süresi (sn)
180
varsayılan
ipsec\_kopma\_bekleme\_sn

IPsec SMS alıcıları
tum\_adminler
varsayılan
ipsec\_sms\_alici

Mod: etkin • kopma teyidi 180 sn • SMS alacak admin: 3

- FW-MERKEZ: 7 tünel • son IPsec olayı 1 dk önce • bildirim AÇIK
  - SAMSUN-VPN: **KOPIK** • başlangıç 14.10 09:43 • SMS: gönderildi
  - MERSIN-VPN: **koptu (teyit bekliyor)** • başlangıç 14.10 09:55
  - ANKARA-VPN: **ayakta** • son olay 14.10 09:54 (stats)
  - DENIZLI-VPN: **ayakta** • son olay 14.10 09:54 (stats)
  - GAZIANTEP-VPN: **ayakta** • son olay 14.10 09:53 (stats)
  - IZMIR-VPN: **ayakta** • son olay 14.10 09:54 (stats)
  - KONYA-VPN: **ayakta** • son olay 14.10 09:54 (stats)

Ayıklanan olay: SSL-VPN 214 • dial-up/dinamik örnek 9 • envantere eşlenmeyen kaynak 0



# Güvenlik olayları: loglardan onaylı aksiyona



## Log toplama

Syslog ve SNMP trap; FortiGate, Cisco ve HP/Aruba ayrıştırıcıları. Ham kayıt saklanır.



## Kural ve vaka

30 hazır kural şablonu ve 0–100 risk puanı; eşleşen olaylar vakaya dönüşür.



## Önce öneri, sonra onay

Cihaza kendiliğinden müdahale edilmez; öneri, yönetici onaylarsa uygulanır.

# Config yedekleme: değişiklik gözden kaçmaz

**Net-Inventory**  
NETWORK ENVANTER

**Cihaz Config Yedekleri**  
Cihazlarınızın yapılandırma dosyalarını yedekleyin, geçmiş sürümleri indirin ve karşılaştırın.

Cihaz Seçin: FW-IZMIR (10.10.3.1) | İzmir Depo | Firewall | [Şimdi Yedek Al](#) | [Oto Yedek Planları](#)

**Yedek Geçmişi**

| Tarih      | Saat  | Boyut         |
|------------|-------|---------------|
| 14.10.2026 | 09:00 | Boyut: 412 KB |
| 14.10.2026 | 07:00 | Boyut: 412 KB |
| 14.10.2026 | 05:00 | Boyut: 411 KB |
| 14.10.2026 | 03:00 | Boyut: 411 KB |

**Sürüm Karşılaştır (Diff)**

Eski Yedek: 14.10.2026 07:00

Yeni Yedek: 14.10.2026 09:00

[Karşılaştır](#)

**Karşılaştırma Sonuçları**

```
config firewall policy
edit 14
  set name "DEPO-MISAFIR-INTERNET"
  set srcintf "vlan40"
  set dstintf "wan1"
-  set action deny
+  set action accept
  set srcaddr "MISAFIR-AG"
  set dstaddr "all"
+  set schedule "always"
+  set service "HTTP" "HTTPS"
  set nat enable

next
end

config system admin
edit "operasyon"
  set accprofile "super_admin"
  set password ENC ***** (gizli değerler maskelenir)
next
end
```

**Config Değişikliği**  
FW-IZMIR: +3 / -1 satır · kullanıcı operasyon (GUI) · policy 14  
Yetkisiz değişikse önceki yedeğe dönülebilir — öneri, otomatik değil.

## Planlı otomatik yedek

SSH ile; desteklemeyen cihazda SNMP ya da web yolu. Geçmiş sürümler indirilebilir.

## Satır satır fark

Eklenen ve silinen satırlar renkli; parola gibi gizli değerler maskelenir.

## Anlık değişiklik uyarısı

Kim, nereden değiştirdi: dakikalar içinde e-posta. Geri dönüş yalnız öneridir.

# Port yönetimi: switch'e gitmeden port, VLAN ve SSH

The screenshot displays the Net-Inventory interface for switch SW-ANK-02. The left sidebar contains navigation options: Genel Durum, Cihaz Envanteri (selected), Config Yedekleri, Alarmlar (3), SNMP İzleme, Ağ Topolojisi, Firmware Yönetimi, Lokasyon Yönetimi, Kullanıcı Yönetimi, Sistem Ayarları, İşlem Geçmişi, Güvenlik (CVE), and SOAR. The main panel shows the switch's status (Ankara Bölge, 10.10.2.12:22) and hardware details (HP/Aruba, Aruba 2930F-24G, Çevrimiçi). It includes performance metrics (CPU %11, RAM %36, Uptime 63g 07s 41d) and buttons for SSH Terminal and Yedek Al. The Port Durumu section shows a grid of 24 ports, with port 12 highlighted. Below this, the VLAN (PVID) settings are shown: 1 YÖNETİM, 20 KULLANICI (selected), 30 KAMERA, and 40 MİSAFİR. The Port 12 configuration shows it is currently in VLAN 20 (KULLANICI) and can be changed to 30 (KAMERA). The Porttaki cihazlar section shows LLDP information for AP-ANK-07. The bottom section features a CANLI SSH PANELİ with a terminal window showing the command 'show interfaces brief 9-12' and its output, followed by 'show vlans ports 12' and its output.



## Port paneli

Port durumu, hız ve VLAN; LLDP komşuları ve MAC tablosu aynı ekranda.



## Onaylı VLAN değişikliği

Plan, onay, uygulama ve cihazdan yeniden okuma. Uplink portları kilitlidir.



## Tarayıcıdan SSH

Ajan üzerinden şube cihazına; oturum kaydı ve kapanışta döküm e-postası.

---

## Tasarım ilkesi

# Ölçemediğini uydurmaz.

Bir izleme aracının en büyük riski yanlış güven vermesidir.

---

Ölçülemeyen CPU/RAM boş kalır; kartta "Ölçülemedi" yazar.

---

Syslog gelmiyorsa tünel "koptu" sayılmaz; durumu "bilinmiyor" görünür.

---

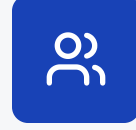
Çözülemeyen cihaz adı uydurulmaz; IP olarak kalır ve kaynağı yazılır.

# Ağ yönetim aracının kendisi de korunur



## Çok faktörlü giriş

E-posta ya da SMS koduyla MFA; Active Directory / LDAP ile giriş.



## Rol ve lokasyon kapsamı

Kullanıcı yalnız yetkili olduğu lokasyonları ve işlemleri görür.



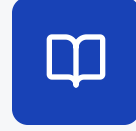
## Oturum güvenliği

30 dk hareketsizlikte otomatik çıkış; oturum en fazla 12 saat.



## Şifreli saklama

Cihaz parolaları ve erişim bilgileri AES-256 ile şifreli tutulur.



## Denetim kaydı

Kim, ne zaman, hangi işlemi yaptı: işlem geçmişinde kayıtlı.



## Kurum içi kurulum

Sunucu kurumun kendi ağında; CVE ve konum gibi dış servisler isteğe bağlı.

# Desteklenen cihazlar ve entegrasyonlar

| Marka / platform                                                            | Envanter ve durum | Config yedeđi | CPU / RAM | Port / VLAN | Syslog ayrıştırma |
|-----------------------------------------------------------------------------|-------------------|---------------|-----------|-------------|-------------------|
| FortiGate                                                                   | Var               | Var           | Var       | —           | Var               |
| HP / Aruba (ArubaOS-Switch, AOS-CX)                                         | Var               | Var           | Var       | Var         | Var               |
| Aruba Instant On                                                            | Var               | Web / SNMP    | —         | —           | —                 |
| Cisco IOS / Catalyst                                                        | Var               | Var           | Var       | —           | Var               |
| Huawei VRP                                                                  | Var               | Var           | SNMP      | Sınırlı     | —                 |
| Diđer: MikroTik, Juniper, pfSense, Allied Telesis, Cisco ASA / NX-OS, UniFi | Var               | Var           | Kısmen    | —           | —                 |
| Linux / Windows sunucu                                                      | Var               | —             | Var       | —           | —                 |

## Entegrasyonlar

FortiGate REST

FortiNAC

FortiAnalyzer

AD / LDAP

SMTP

SMS

Microsoft Teams

NVD CVE

# Dört adımda devreye alma

1

## Merkez kurulum

Tek kurulum dosyası ve sihirbaz; gerekirse SQL Server Express de kurulur.

2

## Web sihirbazı

Yönetici, firma, SMTP, lokasyonlar ve hazır SOAR kuralları.

3

## Şube ajanları

Lokasyona özel paket; şubeden yalnız giden bağlantı.

4

## Cihaz ve bildirim

Ağ taraması ya da Excel ile cihazlar; SMS ve e-posta alıcıları.

## Gereksinimler

- ✓ Windows Server 2016–2025
- ✓ Microsoft SQL Server (Express yeterli)
- ✓ Şube başına bir Windows makine (ajan)
- ✓ Cihazlara SSH / SNMP erişimi

## Güncelleme

İmzalı güncelleme paketleri; ayarlar ve veriler korunur.

# Teřekkürler

Kendi ađınızda canlı demo için bizimle iletişime geçin.

Telefon

**0543 656 89 98**

Web

**mgmtbilisim.com**

E-posta

**kenan.demirbilek@mgmtbilisim.com**

Adres

**Kocasinan / Kayseri**

