



Siber Varlık Risk Yönetimi



Jim Schwar
@jimiDFIR



@MalwareJake adlı kişiye yanıt olarak

CISO: How many windows hosts do we have?

AV Guy: 7864

Desktop Management: 6321

EDR Team: 6722

CMDB Team: 4848

SIEM Team: 9342

ÖS 4:55 · 8 Şub 2018 · Twitter for iPhone

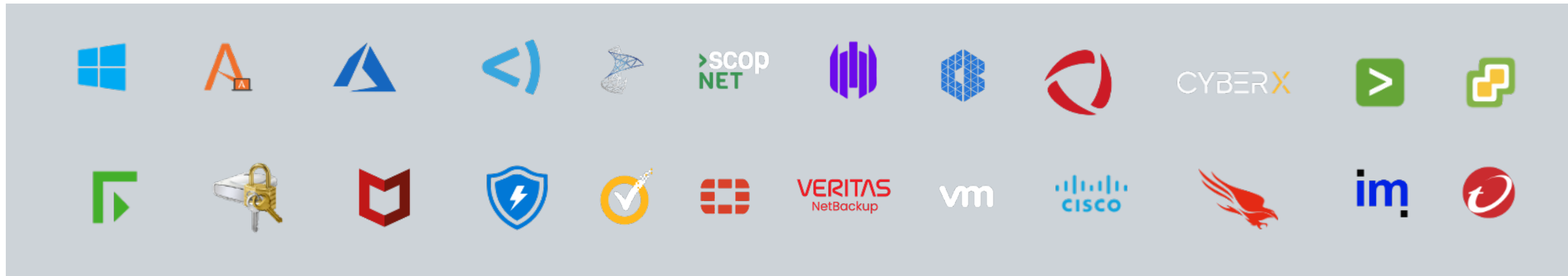
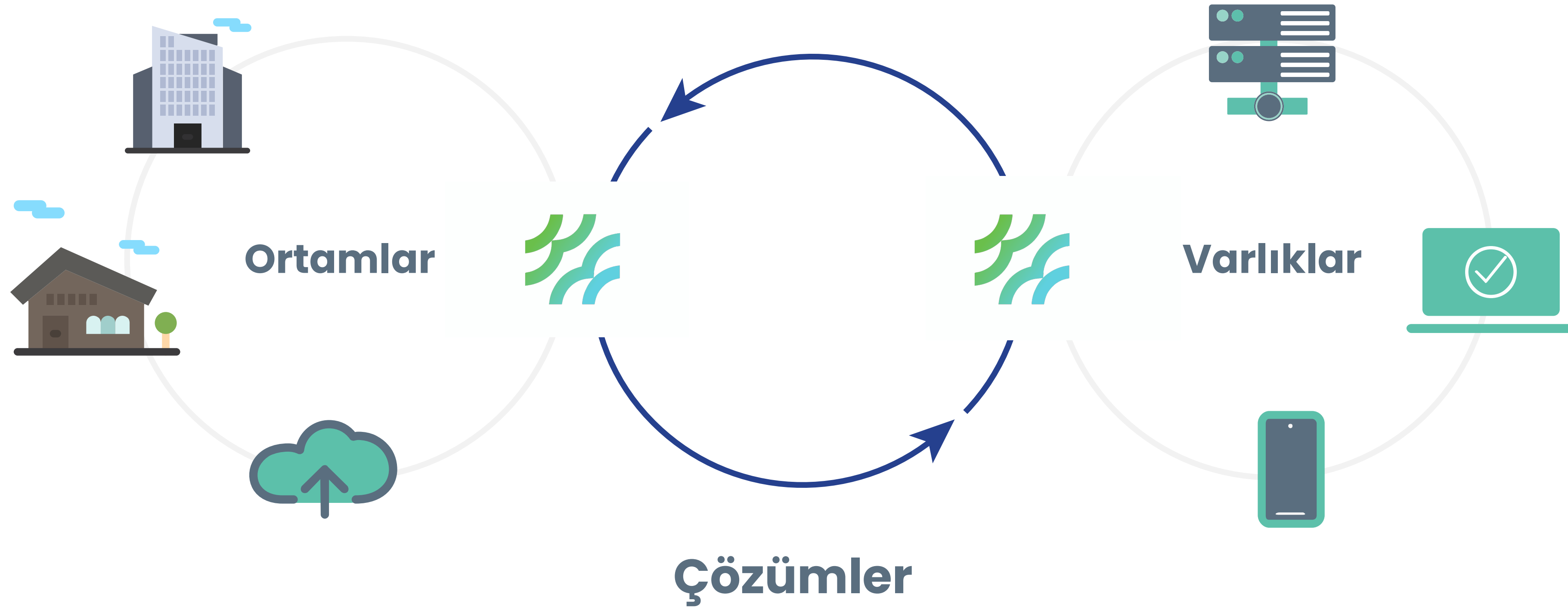
549 Retweet **82** Alıntı Tweetler **1.108** Beğeni



Siber Varlıkların Risk PROBLEMLERİ



Organizasyon



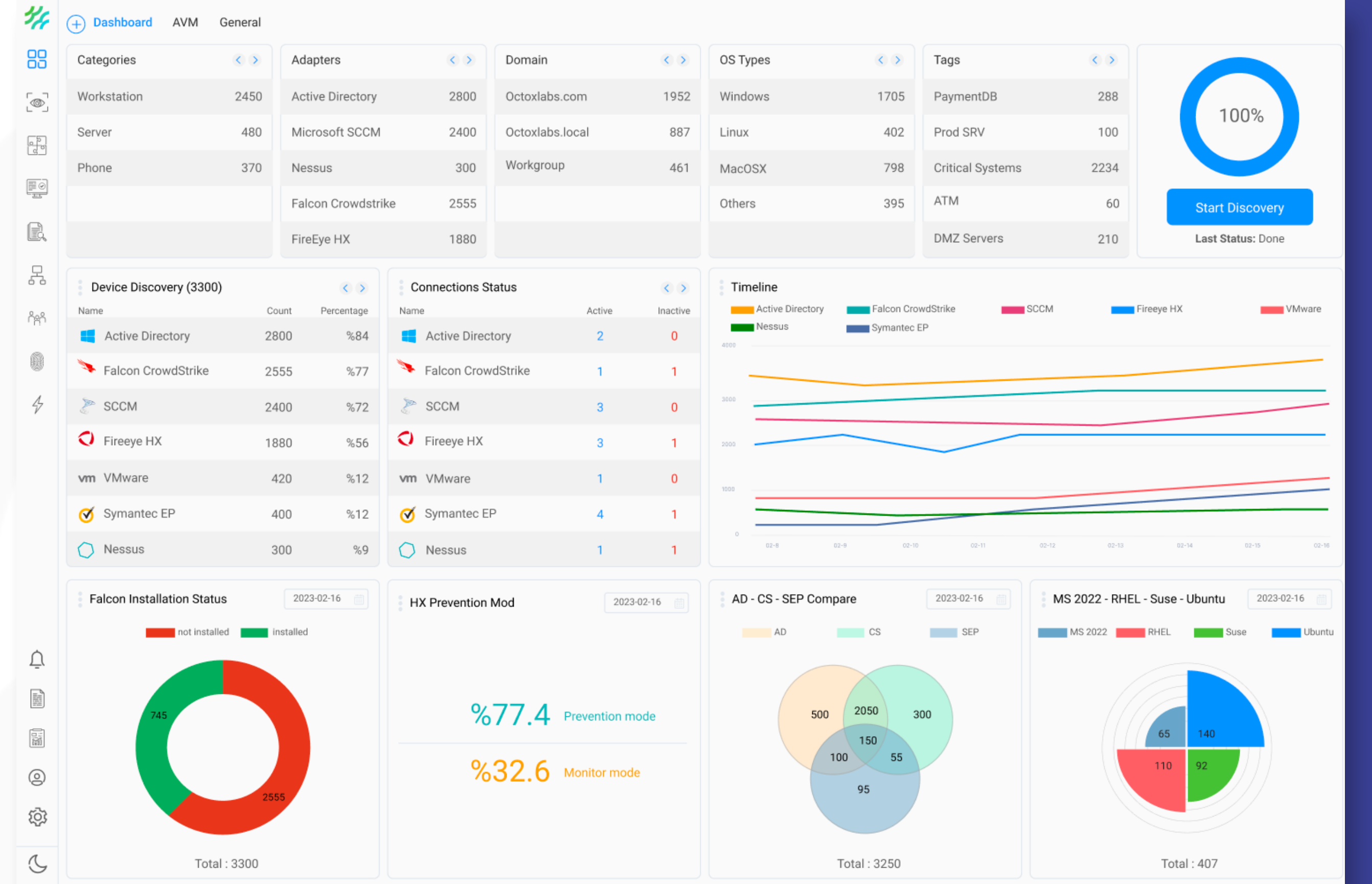
Organizasyonel	Hibrit BT ve güvenlik envanterlerini tutmak geleneksel yöntemlerle mümkün değil
Operasyonel	Görünürlük Eksikliği ve Boşluk Analizi
Raporlama	Ekiplerin zamanlarının %39'u raporlama ile geçmekte
Takip	Eksiklikleri gün geçtikçe takip etmek zorlaşmakta
Aksiyon	Otomatik aksiyonları gerçekleştirmek oldukça zor bir süreçtir

Yaşanılan Zorluklar



Göremediğini Yönetemezsin

- Tüm cihazların ve kullanıcıların güvenilir kapsamlı bir envanterine sahip olun
- Eksiklerinizi görün ve riskleri keşfedin
- Ajansız yapı
- 100'den fazla entegrasyon
- Dakikalar içinde devreye alın
- Politikaları doğrulayın ve hızlıca uygulayın



Modüller

SİBER ENVANTER YÖNETİMİ

Atak yüzeyini bulun
Ajan sağlık durumu

UYGULAMA/YAZILIM ENVANTERİ

Uygulama/Yazılım
Listesi

LİSANS YÖNETİMİ

Lisansları Takip Et

KULLANCILAR

Kullanıcı Hakları

VARLIK ZAAFİYET YÖNETİMİ

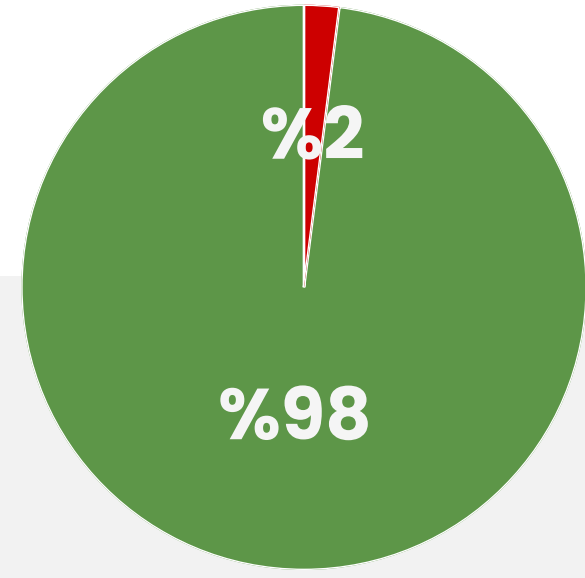
Tespit Et
Önceliklendir

AKSİYON MERKEZİ

İş Akışı Oluştur
Talep Oluştur
Bilgilendir

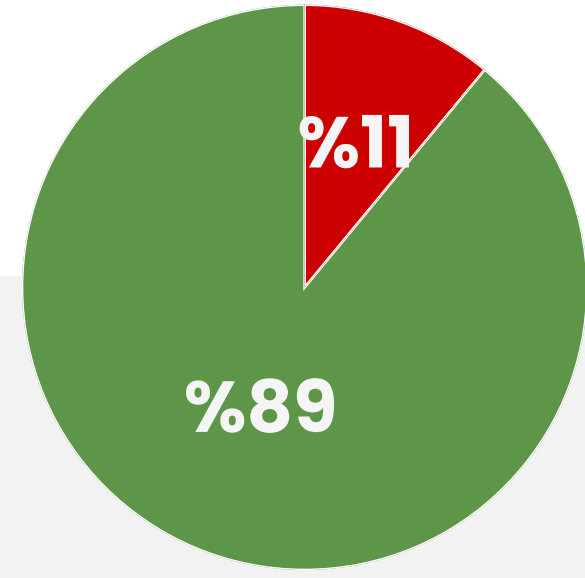


Bulgularımız



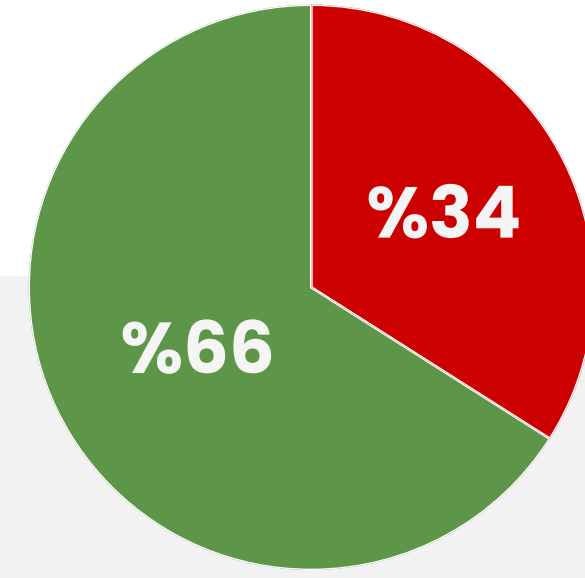
Microsoft Active Directory

• Kurulu • Eksik



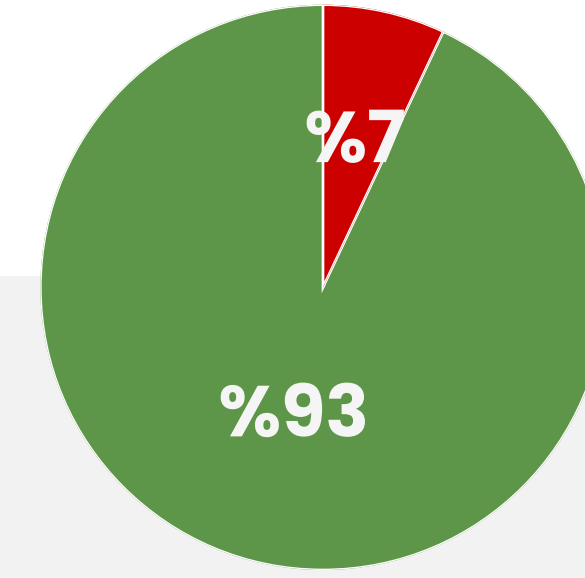
EDR

• Kurulu • Eksik



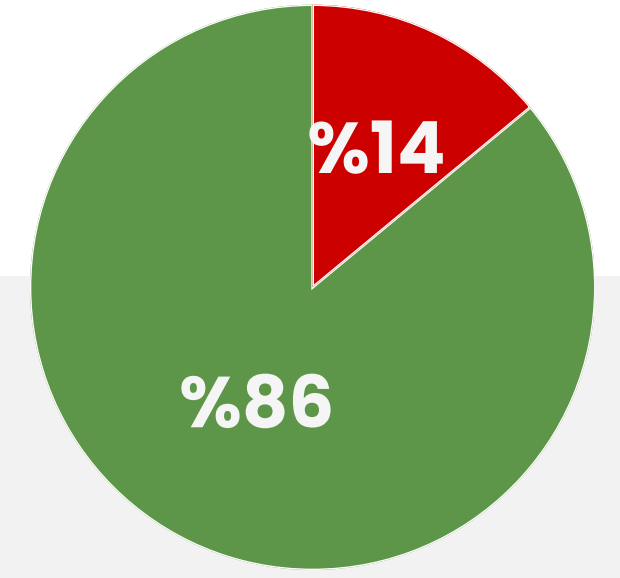
Zafiyet Yönetimi

• Kurulu • Eksik



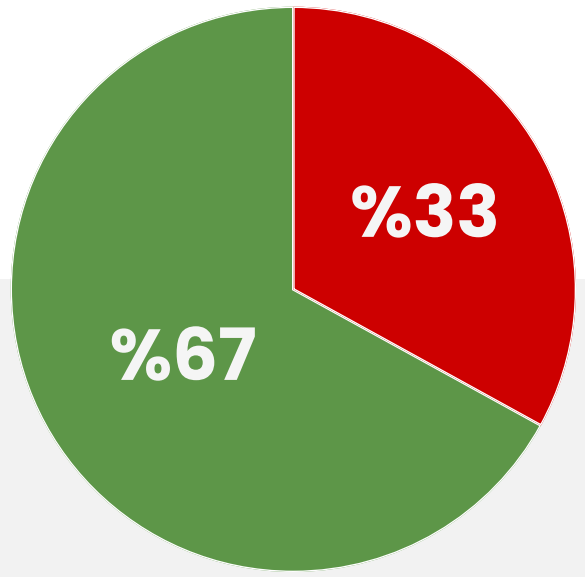
EPP

• Kurulu • Eksik



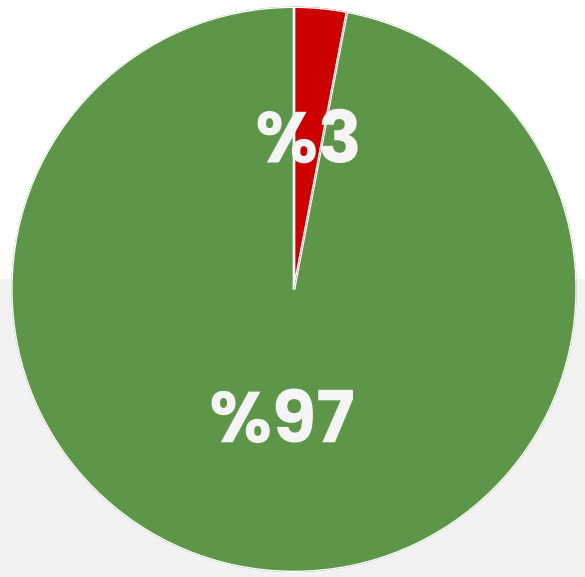
Veritabanı Aktivite İzleme

• Kurulu • Eksik



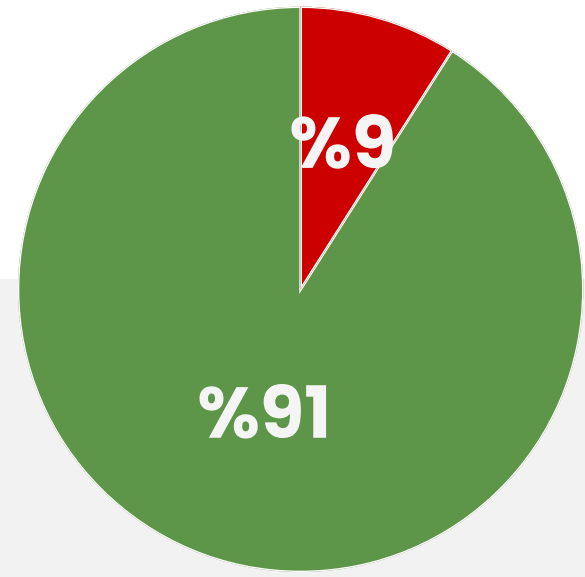
DLP

• Kurulu • Eksik



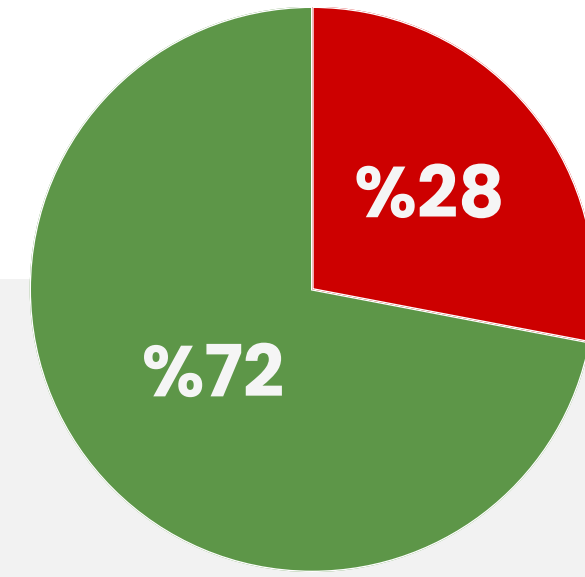
NAC

• Kurulu • Eksik



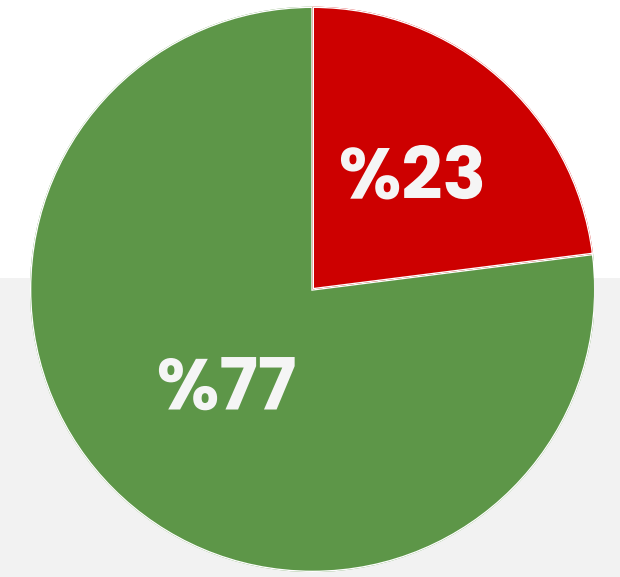
SIEM

• Kurulu • Eksik



Yazılım Dağıtım

• Kurulu • Eksik

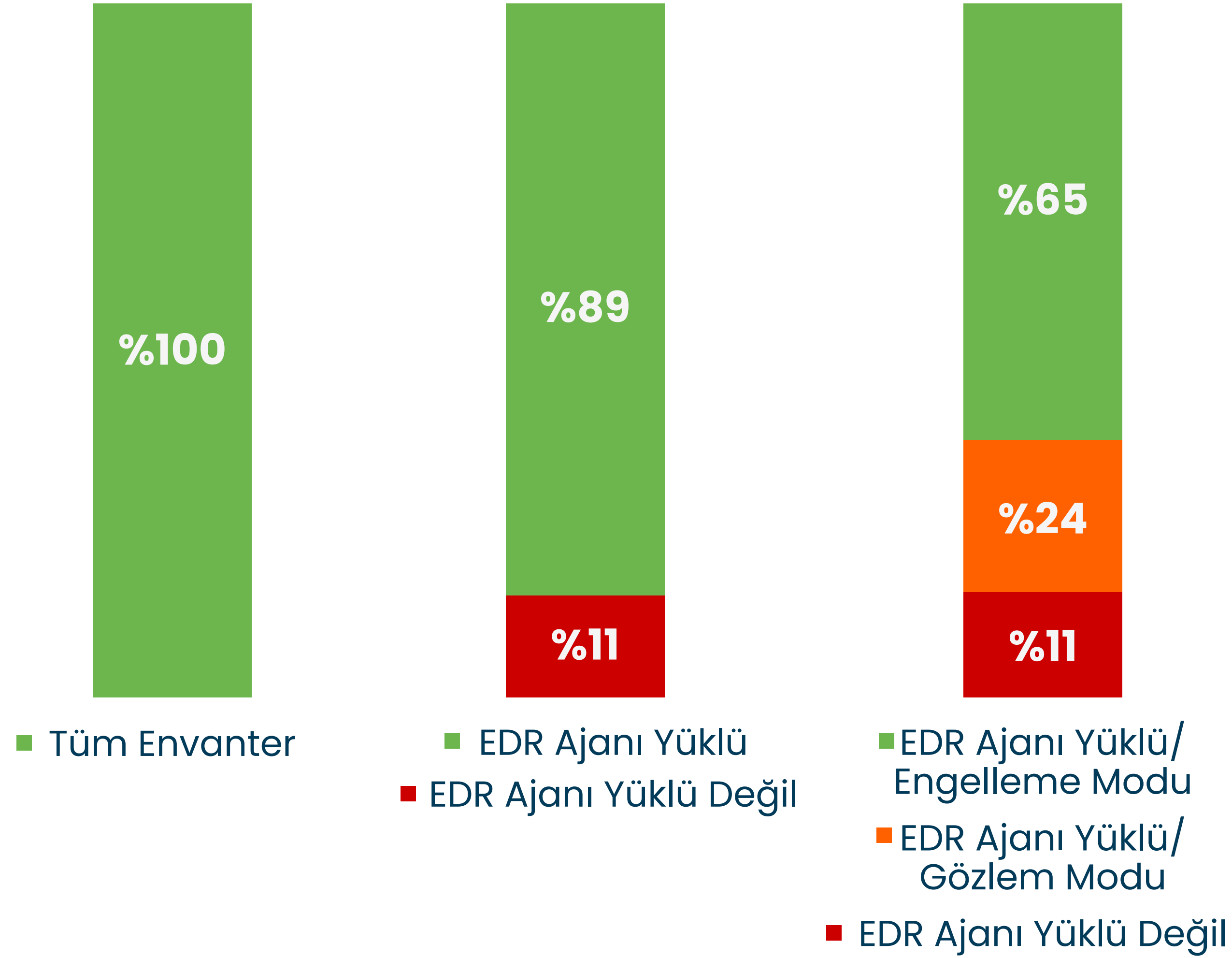


CMDB

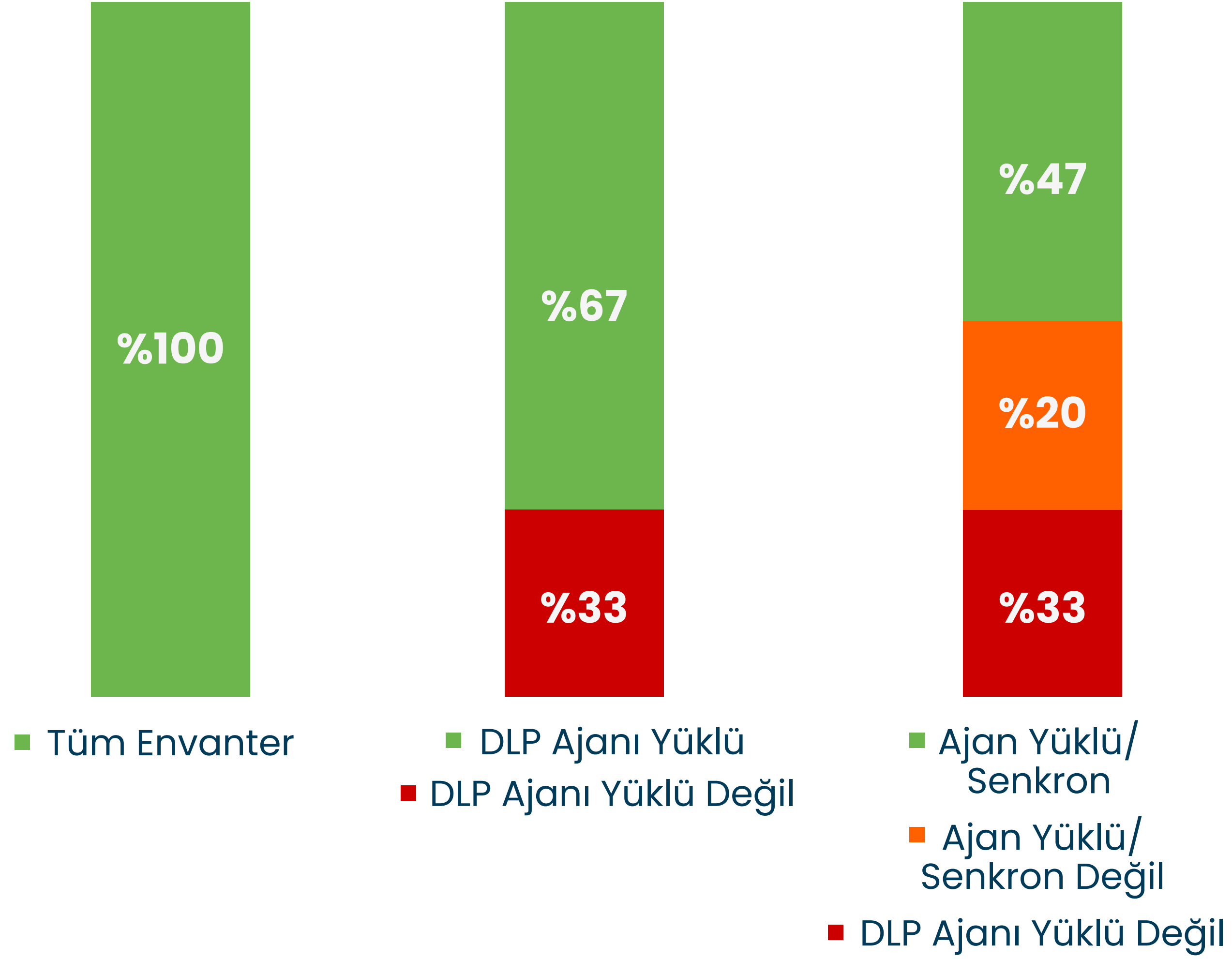
• Kurulu • Eksik



EDR DETAYI



DLP DETAYI





REFERANSLAR



ADAPTÖRLER



...



谢谢

gracias

merci

teşekkürler

grazie

thank you

danke

✉ ata.igdebeli@octoxlabs.com

☎ +90 542 202 2446