

ÜRÜN ÖZETİ

Tehdit görünmeden önce. Yapay zekâyı güvenle yönetin.

ScoutByt AI Security Ürün Özeti

Tarayıcı, geliştirici aracı, model trafiği ve yapay zekâ (YZ) ajanı gibi farklı kullanım yüzeylerini ortak görünürlük ve politika yaklaşımı altında birleştiren kurumsal güvenlik platformu.

YZ GÖRÜNÜRLÜĞÜ**İSTEM & VERİ KORUMASI****AJAN & ARAÇ KONTROLÜ****SOFTBYT LABS ÜRÜN AİLESİ • ÜRÜN ÖZETİ**

ÜRÜN ÖZETİ

Neden şimdi?

Kurumsal YZ kullanımı hızla büyürken risk, tek bir uygulamayla sınırlı kalmıyor.



Gölge YZ

Kurum onayı dışında kullanılan araçlar görünürlük ve sorumluluk boşluğu oluşturabilir.



Veri sızıntısı

İstem, dosya ve kopyala-yapıştır akışları hassas bilgiyi istemeden dışarı taşıyabilir.



Aşırı ajan yetkisi

Bir kullanıcının erişebildiği kaynağa YZ ajanının da erişmesi gerekmez.



Parçalı kontrol

Tarayıcı, masaüstü uygulaması, geliştirici aracı ve model trafiği farklı güvenlik yüzeyleridir.

Temel yaklaşım

Yapay zekâyı yasaklamak yerine; görünür, sınırlandırılmış ve politika odaklı hâle getirmek.

ÜRÜN ÖZETİ

Tek platformda katmanlı koruma

ScoutByt, her yüzeyi aynı yöntemle değil; o yüzeyin desteklediği güvenlik noktası üzerinden yönetir.

**Browser Guard**

Desteklenen tarayıcı yüzeylerinde istem, dosya ve veri hareketlerini politika ile değerlendirin.

**Prompt Guard**

Hassas içeriği desteklenen akıslarda sağlayıcıya ulaşmadan önce denetleyin.

**AI Gateway**

Desteklenen model trafiğini merkezî güvenlik ve veri politikalarından geçirin.

**Agent Guard**

Desteklenen YZ ajanlarını kontrollü oturumlar ve kaynak sınırlarıyla yönetin.

**MCP & Tool Control**

Onaylı araç ve entegrasyonları politika kapsamında tutun.

**Application Discovery / Policy Center**

Önce görünülük kazanın; ardından merkezî politikaları kademeli olarak uygulayın.

Kimlik + Politika + Kaynak + Ağ + Denetim

Ürün, insan yetkisi ile YZ ajan yetkisini ayrı güvenlik kararları olarak ele alır.

ÜRÜN ÖZETİ

Değer ve devreye alma

İş sürekliliğini koruyan, kademeli ve ölçülebilir bir uygulama yaklaşımı.

1

Keşfet

Kullanılan YZ yüzeylerini ve riskli davranışları görünür hâle getirin.

2

Politikayı Tanımla

Veri, kullanıcı, cihaz ve kullanım senaryosuna göre kuralları belirleyin.

3

Pilotla

Seçili kullanıcı ve uygulamalarda etkiyi kontrollü biçimde doğrulayın.

4

Kademeli Uygula

Doğrulan alanlarda politika uygulama seviyesini kontrollü olarak artırın.

Risk görünürlüğü

Gölge YZ ve dağınık kullanım yüzeylerini ortak bakışta değerlendirin.

Veri koruması

Hassas içeriğin istemeden model trafiğine çıkma riskini azaltın.

Ayrı YZ yetkisi

Kullanıcı erişimi ile ajan erişimini birbirinden ayırın.

Kurum içi öncelik

Merkezî yönetim ve veri egemenliği ihtiyaçlarına uygun kurgulayın.

Düşük operasyon yükü

İş akışına etkisini değerlendirerek kademeli ilerleyin.

Üreticiden bağımsız yaklaşım

Tek bir YZ sağlayıcısına bağlı kalmadan ortak güvenlik mantığı kurun.

Teknik değerlendirme ve pilot planı için Softbyt Labs ile iletişime geçin.