



WHITEPAPER · 2026-07-11

Güvenlik & KVKK Mimarisi

Satır düzeyi yetki, denetim izi, AI guardrail ve veri yerleşimi — tek dokümanda.

CISO / BT / HUKUK

4+1

guardrail detektörü + pipeline

100%

RLS kapsamı — AI dahil

0

localOnly modunda dışarı çıkan istek

Kurumsal alıcının üç sorusu vardır: Verime kim erişiyor? AI verimle ne yapıyor? Denetimde ne göstereceğim? Bu doküman 361 Platform'un güvenlik mimarisini bu üç soru üzerinden anlatır.

Katman 1 — Erişim: Satır Düzeyi Güvenlik (RLS)

Her sorgu, kullanıcının rol ve sahiplik bağlamına göre **satır düzeyinde** filtrelenir; yetki modeli tüm görünümelerde (liste, rapor, BI, AI cevabı) aynı motorla uygulanır. AI da dahil hiçbir tüketici yetki filtresinin dışına çıkamaz.

Katman 2 — İzlenebilirlik: Değiştirilemez Denetim İzi

Kayıt geçmişi alan düzeyinde tutulur (kim, ne zaman, hangi değerden hangisine). Denetim kayıtları hash-zincirli tutulabilir; geri almalar da yeni sürüm olarak denetlenebilir şekilde işlenir. Son kullanıcı geçmişi görebilir, tek tıkla geri alabilir — BT eforu olmadan.

Katman 3 — AI Guardrail: 4 Detektör + Pipeline



PII maskesi — kişisel veri modele gitmeden maskelenir



Halüsinasyon denetimi — cevaplar kaynak veriyle doğrulanır



Prompt-injection koruması — kötü niyetli talimat kalıpları reddedilir



Maliyet limiti — kullanım kotaları aşımı otomatik keser



Tümü **GuardrailPipeline** üzerinde tek hatta koşar; denetim izi compliance modülünde tutulur

AI agent'ları uygulamayı doğrudan yapmaz; öneriler **Agent Inbox**'ta insan onayına düşer, her onay geri alınabilir, her öneri gerekçe ve güven skoru taşır.

Katman 4 — Veri Yerleşimi: Yerel AI ve Air-Gap

AI iş yükü tamamen tesis içinde çalışabilir: gömülü yerel çalışma zamanı (LLM + embedding + OCR + TTS) token maliyeti olmadan yereldedir. **localOnly** modu bulut modellerini kategorik reddeder — "veri makineden çıkamaz" sözleşme diline yazılabilir. İnternetsiz (air-gap) kurulum desteklenir.

Katman 5 — KVKK Operasyonları



Saklama/imha politikaları ve veri sahibi hakları (erişim/taşıma/silme) platform süreçleriyle yönetilir



Elektronik ileti onayları İYS ile senkron; izinsiz gönderim kanal katmanında engellenir (fail-closed seçenek)



Nitelikli e-imza: PAdES + HSM + üç GSM operatörüyle mobil imza platform içinde — belge dışarı çıkmadan imzalanır

Sayılarla

Denetim günü

Denetçiye tek ekrandan: kim erişti (RLS + oturum kayıtları), ne değişti (alan düzeyi geçmiş), AI ne yaptı (guardrail + Agent Inbox onay izi), veri nerede işlendi (yerel çalışma zamanı).

Kimler İçin?

Rol	Bu dokümandan çıkaracağı
CISO	RLS + guardrail + denetim izinin tek mimaride olduğu
KVKK / Hukuk	Veri yerleşimi garantisi ve veri sahibi hakları operasyonu
BT Müdürü	Air-gap dahil kurulum seçenekleri ve İYS/e-imza entegrasyonu

SONRAKİ ADIM

361'i kendi verinizde görün

2 haftalık ücretsiz POC — gerçek süreçlerinizde, sıfır risk. Kurulum yok, mevcut sisteminize dokunmadan; beğenmezseniz hiçbir şey değişmez.

Hemen başlayın

17 sağlayıcı · 52 tool · 8 kanal ailesi/44 adaptör · 200+ modül



361.com.tr · info@361.com.tr