AgenticObjects

AGENTİCOBJECTS · GÜVENLİK VE DENETİM NOTU

Dil modeline güvenmeniz gerekmez. Mimari, onu doğrulamak üzerine kurulu.

Bu not, AgenticObjects'i kurumunda değerlendiren bilgi teknolojileri, bilgi güvenliği ve iç denetim ekipleri için hazırlandı. Büyük dil modellerinin (LLM) hata yapabileceğini, uydurabileceğini ve yanlış yorumlayabileceğini varsayar. Bu risklerin ürün içinde hangi mekanizmayla karşılandığını, kanıtının nerede görüldüğünü ve her mekanizmanın sınırını anlatır.

Sürüm 1.0 · Ekim 2026 · D-CAT Technologies

ÖZET

Altı temel güvence

01

Rakamı model üretmez

Her rakam, veri ambarınızda çalışan sorgudan gelir. Motor, cevaptaki her rakamı yayından önce sorgu sonucuyla karşılaştırır.

02

Model veriye dokunmaz

Model sorgu yazmaz, ambara bağlanmaz. Yapılandırılmış bir istek gönderir; sorguyu ürünün motoru üretir ve salt-okunur bir geçitten çalıştırır.

03

Modele giden sınırlıdır

Soru, ölçü ve boyut adları ve sınırlı sayıda özet satır. Kişisel veri alanları maskelenir. Ambarın kopyası gönderilmez.

04

Her adım kayıt altındadır

Model çağrıları, sorgular, yetki ve ayar değişiklikleri kayda geçer. Kayıtlar yalnız eklenebilir; sonradan değiştirilemez.

05

Model kendiliğinden değişmez

Otomatik yedek modele geçiş yoktur. Model seçimi bir insan kararıdır ve kayda geçer.

06

Her şey sizin sunucunuzda

Uygulama, kayıtlar ve yedekler kurumunuzun sunucusunda çalışır. Model çağrıları istenirse Türkiye'deki altyapıda kalır.

MİMARİ

Verinin yolu: model nerede durur?

Ürünün temel tasarım kararı, dil modelini veri hattının **dışında** tutmaktır. Model soruyu anlar ve cevabı yazar; aradaki her şeyi deterministik bileşenler yapar.



Model hiçbir zaman veri ambarına bağlanmaz ve sorgu yazmaz. Sorguyu, veri modelindeki resmî ölçü tanımlarıyla ürünün motoru üretir; sorgu, yalnız okuma sorgularını geçiren bir veri geçidinden çalışır.

RİSK VE KONTROL HARİTASI

Denetimin soracağı riskler ve ürünün cevabı

Risk	Üründeki kontrol	Kanıtı nerede görülür
Model rakam uydurur ya da yanlış hesaplar	Cevaptaki her rakam, o cevap için çalışan sorgunun sonucuna bağlanmak zorundadır. Bağlanamayan rakam düzeltilir, çıkarılır ya da "doğrulanmadı" işaretiyle gösterilir.	Cevaptaki her rakamın kanıt kartı: ölçü, dönem, filtre, satır kapsamı, verinin tarihi.
Değişimin yönü ya da oran yanlış yorumlanır	"Arttı / azaldı" gibi yön ifadeleri kurala göre üretilir. Oranlar paydasını açıkça söyler. Para birimi uyuşmazlığı yayından önce reddedilir.	Kanıt kartı ve cevabın doğrulama durumu.
Model yetkisiz veriye ulaşır	Model ambara erişemez. Sorgu, soruyu soran kullanıcının yetkisiyle çalışır; satır bazında yetki sorguya motor tarafından eklenir.	Koşum kaydındaki yetki kapsamı; denetim kaydı.
Ambarda veri değiştirilir ya da silinir	Veri geçidi yalnız okuma sorgularını geçirir; birden fazla komut, dosyaya yazma ve tanınmayan her ifade reddedilir. Bağlantı ayrıca salt-okunur bir ambar hesabıyla kurulur.	Sorgu kaydı; yetkili kişiler için çalışan sorgunun metni.
Hassas veri dış modele gider	Modele sorgu başına sınırlı sayıda özet satır gider (sohbette en fazla 40, zamanlanmış analizlerde 80). Kişisel veri olarak işaretlenen alanların değerleri baş harflerine indirilir. Model çağrıları istenirse Türkiye'de kalır.	Model çağrısı kaydında modele giden metnin tamamı.
Model sessizce değişir	Model her koşumun başında belirlenir ve koşum boyunca değişmez. Otomatik yedek modele ya da kaliteye göre geçiş yoktur.	Her koşum kaydında kullanılan model; model seçimi denetim kaydında.

Risk	Üründeki kontrol	Kanıtı nerede görülür
Maliyet kontrolden çıkar	Her analizin adım, süre ve maliyet tavanı başlamadan önce sabitlenir; tavan aşılınca analiz durur ve "kesildi" olarak işaretlenir. Aylık bütçede %80 ve %100 uyarısı, günlük harcamada olağandışı artış uyarısı vardır.	Harcama ekranı: kullanıcı, model ve ajan kırılımı.
Kaynak bağlantısı ya da model sağlayıcısı kesilir	Yarım kalan analiz tamamlanmış gibi sunulmaz; hata olarak kapanır ve ilgililere bildirim gider. Tamamlanmış adımlar yeniden çalıştırılmaz, analiz kaldığı yerden sürer.	Koşum sayfası: adımlar, hata nedeni, bildirimler.
Kontrol katmanı devre dışı bırakılır	Rakam denetimi ayrı bir servis değildir; motorun içinde her cevapta çalışır ve ürün ayarlarıyla kapatılamaz. Yöneticinin seçebildiği tek şey, doğrulanamayan rakamın gizlenmesi ya da işaretlenmesidir.	Ayar değişiklikleri denetim kaydında.
Arayüz atlanarak yetkisiz işlem yapılır	Yetki sunucu tarafında uygulanır: oturum, siteler arası istek sahteciliği (CSRF) koruması, işlem yetkisi ve kaynak kapsamı her istekte denetlenir. Varsayılan cevap rettir.	Reddedilen istekler; denetim kaydı.
Kaynak veri geriye dönük değişir	Her cevap üretildiği anda dondurulur: sorgu, filtreler, verinin uzandığı tarih ve model. Eski cevabın dayanağı her zaman görülür. Tekrarlayan bulgular "tekrar" ya da "süregelen" olarak işaretlenir.	Cevabın kalıcı kaydı ve kanıt kartı.

DİL MODELİ HATALARI

"Model saçmalarsa ne olur?"

AgenticObjects, modelin hata yapmayacağını varsaymaz; hata yapacağını varsayar ve her rakamı kullanıcıya ulaşmadan sınar. Bu yaklaşımın etkisini ölçüyoruz. 5 Eylül 2026 itibarıyla geliştirme ve deneme ortamlarımızda teslim edilen 845 cevabın dağılımı:

845	663	129	53
teslim edilen cevap	temiz: düzeltme gerekmedi	hatalı rakam kullanıcıya ulaşmadan motor tarafından düzeltildi	rakam "doğrulanmadı" işaretiyle gösterildi

Bu sayılar bir zayıflığı değil, mekanizmanın çalıştığını gösterir: modelin yaptığı hatalar kayıtta görünür ve hiçbiri doğrulanmış gibi kullanıcıya ulaşmaz.

Geliştirme sürecinde yakalanan ve kalıcı korumaya dönüşen durumlar

- **Ters yön ifadesi:** Rakamlar doğruyken değişimin yönünü anlatan kelimelerin ters yazıldığı görüldü. Yön ifadeleri artık kurala göre üretiliyor.
- **Yanlış para birimi:** Bir tutarın yanlış para birimi işaretiyle doğrulanmış sayıldığı görüldü. Bu durum artık yayından önce reddediliyor; ajanın ekrandaki satırları kendi topladığı tutarlar da reddediliyor.
- **Okuma denetimini aşma denemesi:** Özel bir boşluk karakteriyle okuma denetiminin atlatılabildiği görüldü. Bu biçimler artık reddediliyor ve benzer saldırı kalıpları sürekli çalışan test setine eklendi.
- **Sessiz başarısızlık:** Zamanlanmış bir brifingin başarısız olduğunda kimseye haber vermediği görüldü. Artık analizin sahibine, sahibi yoksa yöneticilere bildirim gidiyor.

> SINIR Ürün, cümledeki rakamların **nereden geldiğini** açıklar; modelin cümleyi **neden böyle kurduğunu** açıklamaz. Zamanlanmış keşif analizlerinde hangi bulgunun öne çıkarılacağını model seçer; bu yüzden iki koşum farklı bulgular öne çıkarabilir. Her bulgudaki rakamlar ise her koşumda aynı denetimden geçer.

VERİ GÜVENLİĞİ

Veriniz nerede, kim görür, modele ne gider?

Kurulum ve veri yeri

Uygulama, ajan çalışma ortamı, sorgu motoru ve kayıt veritabanı kurumunuzun Linux sunucusunda Docker kapları olarak çalışır. Veri ambarınız kendi sunucusunda kalır; ürün verinin kopyasını tutmaz, yalnız toplu sonuç alır. Dışarıya yalnız model çağrıları ve e-posta bildirimleri için çıkış gerekir; içeriye doğru bağlantı gerekmez.

Modele giden içerik

Sorulan soru, veri modelinin yapısı (ölçü ve boyut adları) ve sorgu başına sınırlı sayıda özet satır. Kişisel veri olarak işaretlenen boyutların değerleri "A*** K***" biçiminde maskelenir; örnek değer listelerinde kişisel alanlar hiç yer almaz.

Verinin yurt içinde kalması

Model, kurumunuzun yöneticisinin onayladığı katalogdan seçilir. Yurt içi seçenekler: Bulutistan dil modeli hizmeti ve EVREN. İki seçenekte de model çağrıları Türkiye'deki altyapıda kalır.

Salt-okunur erişim, iki katman

Ürünün veri geçidi yalnız okuma sorgularını geçirir; tanımadığı her ifadeyi reddeder. Küp kaynaklarında da yalnız okuma sorguları kabul edilir. Buna ek olarak ambar bağlantısının salt-okunur bir hesapla kurulmasını şart koşarız.

Satır bazında yetki

Satır yetkisi açık bir modelde her kullanıcı yalnız görmeye yetkili olduğu satırlar üzerinden cevap alır. Yetki tanımı olmayan kullanıcı hiçbir satır görmez. Her koşumun yetki kapsamı kayda geçer.

Bağlantı sırları

Ambar bağlantı şifreleri veritabanında AES-256-GCM ile şifreli saklanır. Şifreyi çözen anahtar veritabanının dışında, sunucunun ayar dosyasında durur; veritabanı yedeği tek başına şifreleri açamaz.

DENETİM VE KAYIT

Neler kayda geçer, kim görür?

Ürünün yaptığı her iş, birbirine bağlı kayıtlarla izlenir. Cevaptaki bir rakamdan, onu üreten sorguya ve o koşumdaki model çağrılarına kadar inilebilir.

Kayıt	Ne tutulur	Kim görür
Model çağrıları	Cevap üreten her model çağrısında modele giden metnin ve dönen cevabın tam içeriği; model, işlenen metin miktarı, maliyet, süre. Her çağrının hangi kullanıcının sorusu ya da hangi zamanlanmış analiz için yapıldığı görülür.	Ayrı yetkiyle. Her görüntüleme denetim kaydına yazılır.
Sorgu kaydı	Ambarda çalışan her sorgunun amacı, gittiği bağlantı, bekleme ve çalışma süreleri, döndürdüğü satır sayısı. 90 gün sonra arşive taşınır, silinmez.	Analiz sorumluları ve yöneticiler.
Çalışan sorgunun metni	Veritabanında fiilen çalışan SQL (küplerde DAX/MDX) sorgusu.	Yalnız bu yetki ayrıca verilen kişiler.
Koşum kaydı	Her analizin adımları, kullanılan model, sabitlenen ayarlar ve tavanlar, yetki kapsamı, sonuç ya da hata nedeni. Koşum JSON olarak dışa aktarılabilir; her dışa aktarım da kayda geçer.	Yönetim konsolu, yetkiye göre.
Denetim kaydı	Kim, ne zaman, neyi değiştirdi: yetki verme ve geri alma, "tüm satırları görme" yetkisi, model seçimi, ayar değişiklikleri, kanıt katmanının açılması.	Yöneticiler; ayrıntılı oturum bilgisi ayrı yetkiyle.
Harcama	Model kullanım maliyeti; kullanıcı, model ve ajan kırılımı; bütçe uyarıları.	Yöneticiler.

İLKE Kayıtlar yalnız eklenebilir; ürünün hiçbir işlemi kayıt silmez ya da değiştirmez. Tüm kayıtlar kurumunuzun sunucusunda tutulur. Saklama sürelerini, Kişisel Verilerin Korunması Kanunu (KVKK) ve kurumunuzun politikalarıyla birlikte belirleriz.

OPERASYON VE DAYANIKLILIK

Sistem nasıl ayakta kalır, nasıl izlenir?

Sağlık kontrolü

Her 5 dakikada bir: servisler ve kapasiteleri, iş kuyruğu ve takılı kalan analizler, zamanlayıcı, veritabanı, veri geçidi, sürüm tutarlılığı, güvenli bağlantı sertifikasının bitişine kalan süre, yedeklerin tazeliği ve verinin uzandığı tarih. Bir madde sorunlu duruma geçtiğinde ya da düzeldiğinde e-posta gönderilir; uyarılarda veri bulunmaz.

Yedek ve güncelleme

Ürün veritabanı her gece otomatik yedeklenir ve yedek, geri yükleme denemesiyle doğrulanır. Güncelleme, yedek alınmadan başlamaz; gerektiğinde önceki sürüme dönülür. Sunucunun kendisinin yedeklenmesi kurumunuzun mevcut düzeninde kalır.

Kesintide davranış

Geçici hatalarda adım 3 kez yeniden denenir; kalıcı hatalarda denenmez. Model sağlayıcısına ulaşılamazsa zamanlanmış analizler 4 saate kadar bekler, sonra kapanır ve bildirim gider. Durmuş bir iş süreci tespit edilir ve iş başka bir sürece devredilir.

Yönetim konsolu

Genel bakış ekranında başarısız analizler, harcama, duran servisler, zamanlama sorunları, bağlantı test durumu ve veri tazeliği. Servis ekranından durum izlenir ve servis yeniden başlatılır.

Kurumunuzun ekibinin izlemesi gerekenler

- Alarm e-postaları ve izleme ekranları
- Haftada bir yönetim konsolunun genel bakış ekranı
- Ambara bağlanan salt-okunur hesabın yönetimi
- Şifreleme anahtarı dosyasının kurumun şifre kasasında ayrıca saklanması
- Model harcaması ve bütçe uyarıları

Bu not, AgenticObjects'in mevcut sürümünü tanımlar. Sorularınız için: hello@agenticobjects.ai