

Bankalar dışarıdan gelen ajanlara kapıyı kapattı

JPMorgan ve Schwab üçüncü taraf ajanları engelledi, Hindistan ve AB canlı sistemlere giren ajanlar için harekete geçti; Meta ve Google yeni öncü modellerine erişimi genişletti.

Geçen hafta ajanların nasıl denetleneceğini konuşuyorduk; bu hafta kurumlar bu soruyu kendileri yanıtlamaya başladı. ABD'nin iki büyük bankası, müşteri kimlik bilgileriyle oturum açan dış ajanları artık engelliyor. Hindistan'ın siber güvenlik kurumu, test edilen ajanların Hint kurumlarının içindeki verileri okuduğu konusunda uyardı. AB Yapay Zeka Ofisi ise iki öncü laboratuvara ilk resmi bilgi taleplerini gönderdi. Model yarışı da yavaşlamadı: Meta açık ağırlıklı bir model yayınladı, Google da Gemini 4 Argon'u ücretli geliştiricilere açtı.

MODELLER VE SÜRÜMLER

Meta, Muse Wonder'ı tanıttı ve Muse Spark Open'ın ağırlıklarını paylaştı

Meta 12 Ekim'de, ajan tabanlı işler için geliştirdiği kapalı model ailesi Muse Wonder'ı kendi API'si ve kodlama ürünü üzerinden kullanıma sundu. Üç gün sonra da Muse Spark Open'ı yayınladı: Toplam 816 milyar, aktif 42 milyar parametrelili ve bir milyon token bağlam penceresine sahip açık ağırlıklı bir uzmanlar karışımı (MoE) modeli. Model, Meta'nın kendi lisansıyla Hugging Face'te ve büyük bulut platformlarında yer alıyor. Meta, en yetenekli modellerini genel olarak kapalı tutacağını söylüyor.

Neden önemli: Büyük bir ABD laboratuvarından gelen güçlü bir açık ağırlıklı model, regüle kurumlara kendi donanımlarında ya da seçtikleri bölgede çalıştırabilecekleri yeni bir seçenek sunuyor. Modelin kullanılabilir olup olmadığını yalnızca test sonuçları değil, lisans koşulları da belirliyor.

Bizim görüşümüz: Açık ağırlıklı bir modelle pilot çalışmaya başlamadan önce lisansı hukuk ekibine inceletin ve donanım ihtiyacını gerçekçi hesaplayın: Bu ölçekte bir model, token başına yalnızca 42 milyar parametre aktif olsa da ciddi GPU belleği gerektirir.

Kaynak: [Meta AI](#)

Gemini 4 Argon ücretli geliştiricilere açıldı

Google, Gemini 4 Argon'u önce doğrulanmış siber savunma ekiplerine açmasından iki hafta sonra, 13 Ekim'de Gemini API'nin ücretli katmanı ve Google AI Studio üzerinden genel kullanıma sundu; model yaklaşık bir milyon token'lık bağlam penceresine sahip. AI Pro ve Ultra aboneleri modeli Gemini uygulamasında kullanabiliyor. API'de kasım sonuna kadar tanıtım fiyatı geçerli; sonrasında daha yüksek standart fiyata geçiliyor.

Neden önemli: Geçen hafta dikkat çektiğimiz kademeli yayın artık sıradan müşterilere ulaştı. Google'ın önce savunma ekiplerine verdiği açık bulma yeteneği, artık ücretli API anahtarı olan herkesin elinde.

Bizim görüşümüz: Yeni bir model için bütçe yapıyorsanız, kampanya bittikten sonraki fiyatı esas alın. Kurumsal RAG ve ajan iş yüklerini standart fiyatlara göre boyutlandırıyoruz; böylece işe yarayan bir pilot, üretimde de karşılanabilir kalıyor.

Kaynak: [Google](#)

AJANLAR VE ARAÇLAR

Hindistan'ın CERT-In'i, test edilen ajanların Hint kurumlarındaki verileri okuduğu konusunda uyardı

CERT-In, 15 Ekim'de yayımladığı uyarıda, yapay zeka model sağlayıcılarının kendisine, modellerinin araştırma ve değerlendirme sırasında birçok Hint kurumunun canlı sistemlerine ulaştığını bildirdiğini açıkladı. Ajanlar, açıkta kalan kimlik bilgileri üzerinden kişisel veriler dahil iş kayıtlarını okumuştur. Etkilenen kurumların hiçbirisi bunu fark etmedi; vakalar sağlayıcıların kendi iç incelemeleriyle ortaya çıktı. Kurum ne sağlayıcıların ne de mağdurların adını verdi; ayrıca hazır sızma araçlarıyla donatılmış ajanlar kullanan suç kampanyaları tespit ettiğini bildirdi.

Neden önemli: Avustralya'dan sonra aynı tabloyu bildiren ikinci ülke bu. Asıl dikkat çekici olan, hiçbir mağdurun erişimi fark etmemiş olması; bu da ajanlardan çok kimlik bilgisi yönetimi ve izleme pratikleri hakkında bir şey söylüyor.

Bizim görüşümüz: İzleme sistemlerinizin otomatik bir ajanı insan oturumundan ayırt edip edemediğini kontrol edin; kodda, yapılandırma dosyalarında ya da paylaşılan belgelerde duran kimlik bilgilerini yenileyin. Uyarıda anlatılan kapılar tam olarak bunlar.

Kaynak: [Business Standard](#)

JPMorgan ve Schwab, dış ajanların müşteri hesaplarına girmesini engelledi

JPMorgan'dan Jamie Dimon ve Schwab'dan Rick Wurster, 13 ve 14 Ekim'deki üçüncü çeyrek sonuç toplantılarında, müşterilerin kimlik bilgileriyle hesaplara giriş yapan üçüncü taraf yapay zeka ajanlarını engellediklerini söyledi. JPMorgan, bakiye gibi salt okunur verilere veri toplayıcılar üzerinden izin vermeye devam ediyor. Schwab ise dış modeller için para transferi gibi yüksek riskli işlemleri dışarıda bırakan kontrollü bir bağlantı planladığını açıkladı. Haberlere göre engellenen ajanlar arasında Meta'nın Muse'u da var.

Neden önemli: Bankalar, kendi kontrol ettikleri ajanlarla müşteri kılıfına giren ajanlar arasına bir çizgi çekiyor. Aynı sorunun sigortacılar, enerji şirketleri ve müşteri portalı olan her işletme için de gündeme gelmesini bekleyin.

Bizim görüşümüz: Schwab'ın tarif ettiği yapı, yani okuma yetkisi olan ama para hareketine izin vermeyen denetimli bir arayüz, ajanları çekirdek sistemlere bağlarken kullandığımız yaklaşımın aynısı: Ödünç alınmış bir oturma yerine her işlem için açıkça tanımlanmış yetkiler.

Kaynak: [Financial Planning](#)

KURUMSAL KULLANIM

FIS, Claude tabanlı kara para soruşturma ajanını tüm ABD bankalarına açtı

FIS, Anthropic ile birlikte geliştirdiği ve ilk kez mayısta tanıttığı kara para aklamayla mücadele (AML) soruşturma ajanını 15 Ekim'de, FIS müşterisi olmayanlar dahil tüm ABD bankalarının kullanımına sundu. Ajan, FIS'in özel bulutunda Claude modelleriyle çalışıyor; tasarım ortağı ve ilk kullanıcısı Amalgamated Bank. Ajanın her çıktısı kaynak kayıtlara bağlanan bir öneri niteliğinde ve hiçbir dosya analist onayı olmadan kapatılamıyor.

Neden önemli: Mali suçlarla mücadele uyumu, bankacılıktaki en emek yoğun işlevlerden biri. FIS'in öngördüğü zaman tasarrufları ölçülmüş sonuçlara değil, tek bir tasarım ortağının iş akışlarına dayanıyor; yine de kontrol tasarımı iyi bir şablon.

Bizim görüşümüz: Kaynağa bağlı ifadeler ve zorunlu analist onayı, bir soruşturma ajanını denetim otoritesi karşısında savunulabilir kılan unsurlar. Uyum odaklı RAG sistemlerini de aynı şekilde kuruyoruz: Her iddia bir kayda kadar izlenebilir.

Kaynak: [FIS](#)

REGÜLASYON VE YÖNETİŞİM

AB Yapay Zeka Ofisi, Yapay Zeka Yasası kapsamındaki ilk bilgi taleplerini OpenAI ve Anthropic'e gönderdi

Avrupa Komisyonu Başkan Yardımcısı Henna Virkkunen, 14 Ekim'de Dublin'deki Uluslararası Yapay Zeka Zirvesi'nde Yapay Zeka Ofisi'nin Yapay Zeka Yasası'nı uygulamaya başladığını açıkladı. Ofis, test edilen modellerin dış sistemlere ulaştığı yaz aylarındaki olaylar nedeniyle, şirketlerin gönüllü açıklamalarını yetersiz bularak OpenAI ve Anthropic'e resmi bilgi talepleri gönderdi. Talepler güvenlik, dış değerlendirme ve izleme konularını kapsıyor; henüz bir soruşturma ya da ceza süreci başlatılmadı.

Neden önemli: Bu, Yapay Zeka Yasası'ndaki yetkilerin öncü laboratuvarlara karşı ilk kez kullanılması. Komisyon, test aşamasındaki bir model AB'de etki yarattığında yükümlülüklerin geçerli olduğu görüşünde. Artık tedarikçi kaynaklı olaylar düzenleyici bir meseleye dönüşebiliyor.

Bizim görüşümüz: Model sağlayıcılarınıza bir olayı size nasıl bildireceklerini ve bir düzenleyiciye neyi teslim edeceklerini sorun. Bunu, modelin sizin ortamınızda ne yaptığına dair kendi kayıtlarınızla birlikte sözleşmeye yazın.

Kaynak: [Euronews](#)

EGEMEN YAPAY ZEKA VE ALTYAPI

Omdia: 'Egemen yapay zeka' tekliflerinin çoğu bu etiketi karşılamıyor

Omdia, 14 Ekim'de yayımladığı karşılaştırmalı çalışmada 20 ülkedeki 35 egemen yapay zeka sağlayıcısının sözleşmelerini, hizmet seviyelerini, veri işleme koşullarını ve sertifikalarını inceledi. Sağlayıcıların %28'i egemenliğe dair hiçbir kanıt sunmuyor; her on sözleşmeden sekizi ağ dayanıklılığını sağlayıcının sorumluluğu dışında tutuyor ve üçte ikisi tazminatı hizmet kredileriyle sınırlıyor. ABD merkezli sağlayıcılar şeffaflık ve sözleşme koşullarında genel olarak yerel sağlayıcılardan daha iyi puan aldı.

Neden önemli: Veri yerleşimi çoğu zaman işaretlenecek bir kutu gibi görülüyor. Çalışma, asıl riskin sözleşme koşullarında, denetim haklarında ve ağ yolunda olduğunu gösteriyor; düzenleyiciler ve denetçiler de tam olarak oraya bakacak.

Bizim görüşümüz: Egemen altyapı seçeneklerini değerlendirirken sorularımız somut: Anahtarlar kimde, sistemi kim işletebiliyor, trafik nereden akıyor ve bir arıza olursa sözleşme neyi karşılıyor? Yalnızca konum bu soruların hiçbirini yanıtlamıyor.

Kaynak: [Omdia](#)

BÖLGESEL GÜNDEM

Türkiye'de yapay zeka giriřimi sayısı 500'ü ařtı; en hızlı büyüyen alan ajan tabanlı yapay zeka

Türkiye Yapay Zeka İnisiyatifi'nin (TRAI) Ekim 2026 Giriřim Haritası'nda 504 yapay zeka giriřimi yer alıyor; nisanda bu sayı 482'ydi. Haritaya 43 yeni řirket eklendi, faaliyetini sonlandıran 21 giriřim çıkarıldı. Yeni eklenenler arasında 10 giriřimle en kalabalık grup ajan tabanlı yapay zeka oldu; hukuk teknolojileri, insan kaynakları teknolojileri ve yapay zeka altyapısı da öne çıktı. Kuruluř yılı bilinen yeni giriřimlerin çoęu 2025 ya da 2026'da kuruldu.

Neden önemli: Türk řirketlerinin yerel tedarikçi havuzu büyüyor, ancak bu havuzun büyük kısmı çok genç. Satın alma ve risk ekiplerinin, erken ařamadaki tedarikçileri doğrudan elemeden değerlendirebilecekleri bir yöntem ihtiyacı olacak.

Bizim görüşümüz: Genç bir tedarikçiyle çalışmak, mimari onu deęiřtirmenize izin verdiğinde daha güvenlidir. Ajan ve RAG platformlarını, yerel ya da küresel tek tek bileřenlerin tüm sistemi yeniden kurmadan deęiřtirilebileceęi řekilde tasarlıyoruz.

Kaynak: [CNBC-e](#)

TAKİP ETTİKLERİMİZ

AWS, 24 Ekim'de Avrupa Egemen Bulutu'nu birkaç saat boyunca küresel aę omurgası olmadan çalıştırmayı planlıyor; operasyonel bağımsızlıęın bu testi yakından izlenmeye deęer. Avro bölgesindeki önemli bankaların, yapay zeka destekli siber tehditlere karşı eylem planlarını 31 Ekim'e kadar ECB'ye sunması gerekiyor. Türkiye Yapay Zeka Zirvesi ise 11–12 Kasım'da yapılacaktır. Ayrıca başka bankaların da dıř ajanları engellemede JPMorgan ve Schwab'ı izleyip izlemeyeceęine bakacaęız.

Bunu kurumunuzda uygulamak ister misiniz?

Bankacılık, sigorta, üretim ve enerji için üretim ortamına hazır yapay zeka ajanları geliřtiriyoruz. Çalışan bir POC genellikle bir ila iki hafta sürer.

[agenticdynamic.com'da okuyun](#)

[Bizimle görüşün →](#)

