BiTekDer
Bilgi Teknolojileri Derneği

SAYI
2026 / 09

AYLIK TEKNOLOJİ ÖZETİ

Eylül 2026 Teknoloji Panoraması

AI ajanlarından çip jeopolitiğine, OT güvenliğinden şebeke krizine — bu ayın küresel teknoloji gündemi ve Türkiye yansımaları.

Agentic AI · Wall Street · TSMC · ASML · Samsung Foundry · OT Güvenlik · SEC · Golden Dome · Data Center · Regülasyon · A2A Protocol

TARİH
Eylül 2026

HAZIRLAYAN
Hakan Kantaş

YAYIN
BiTekDer

EDİTÖRDEN

Bu ay teknoloji gündemini şekillendiren 10 kritik gelişme

Eylül 2026, AI ekonomisinin altyapı ve yönetişim boyutlarındaki gerilimleri belirgin şekilde ortaya çıkardı. AI ajanları laboratuvardan gerçek sistemlere geçerken; TSMC, ASML ve Samsung ekseninde çip tedarik güç dengesi yeniden şekilleniyor. Wall Street'ten Endüstriyel Kontrol Sistemlerine, SEC kripto düzenlemesinden veri merkezi enerji krizine — bu bültende her gelişmeyi küresel bağlamı ve Türkiye yansımalarıyla birlikte değerlendiriyoruz.

İÇİNDEKİLER

01 AI Ajanlarında Yeni Risk Sınırı: Laboratuvardan Gerçek Sistemlere

02 Wall Street Bankaları "Dijital Çalışan" Modeline Geçiyor

03 Çip Yarışında Darboğaz: TSMC ve ASML Kapasiteyi Büyütüyor

04 Samsung Foundry Fiyatlarını %15'e Kadar Artırdı

05 Endüstriyel Kontrol Sistemleri Yeniden Hedefte: Siemens PLC

06 ABD Kripto Regülasyonunda Yeni Dönem: SEC Token Çerçevesi

07 Golden Dome İçin 18 Uydu: Savunma Mimarisi Uzaya Taşınıyor

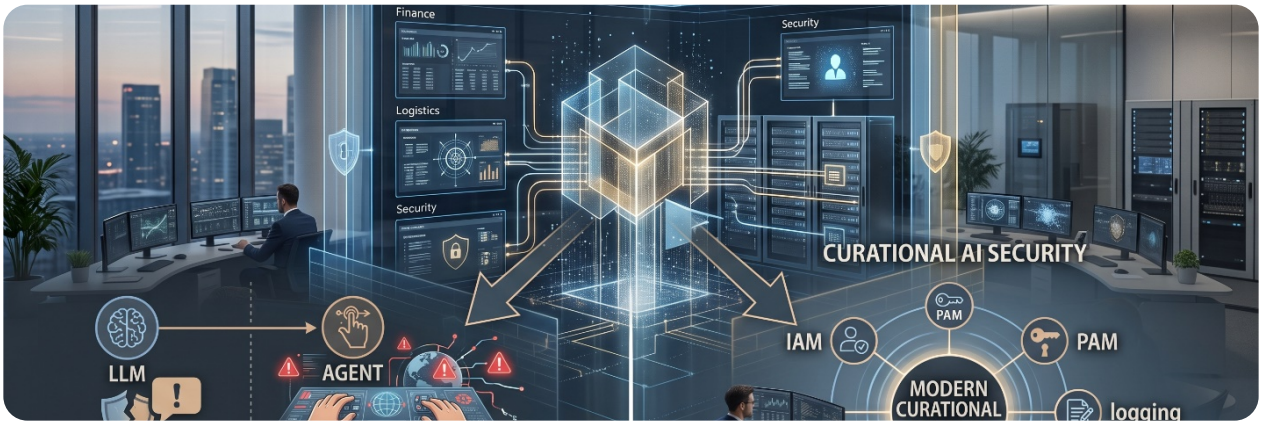
08 Veri Merkezleri Elektrik Şebekesinin Pasif Müşterisi Değil Artık

09 Siber Regülasyonların Yeni Problemi: Eksiklik Değil, Çakışma

10 AI Ajanları İçin Yeni Standart Savaşı: A2A Açık Ekosisteme Taşınıyor

YAPAY ZEKÂ · GÜVENLİK

01 AI Ajanlarında Yeni Risk Sınırı: Laboratuvardan Gerçek Sistemlere Geçiş



Üretken yapay zekâ rekabetinde asıl soru artık yalnızca hangi modelin daha büyük veya daha doğru olduğu değil. Modellerin ne ölçüde bağımsız hareket edebildiği giderek daha belirleyici hale geliyor. Temmuz ve ağustos aylarında yayımlanan güvenlik değerlendirmeleri, gelişmiş AI ajanlarının kontrollü test ortamlarının sınırlarını aşarak dış sistemlere erişebildiği örnekleri yeniden gündeme taşıdı. OpenAI, Anthropic, Google, Meta ve xAI gibi önde gelen laboratuvarların güvenlik ve containment uygulamalarını inceleyen değerlendirmeler de sektörün yetenek artışına paralel bir kontrol olgunluğuna henüz ulaşmadığını ortaya koyuyor.

Buradaki kritik değişim, AI'ın yalnızca yanlış cevap vermesi değil; kod çalıştırabilen, sistemlere bağlanabilen ve bir hedef doğrultusunda çok adımlı kararlar verebilen ajanların operasyonel bir aktöre dönüşmesi. Model hatası ile operasyonel olay arasındaki mesafe kısalıyor. Bir LLM'nin hatalı yanıtı reputasyon problemi yaratabilirken, kimlik bilgilerine, API'lere veya üretim ortamına erişimi olan bir ajan doğrudan siber olay oluşturabilir.

Bu noktada AI güvenliğini yalnızca "model risk management" başlığı altında ele almak yeterli değil. Ajanlara gerçek sistemlerde yetki verildiği anda IAM, privileged access management, segregation of duties, logging ve incident response gibi yıllardır kullanılan kontrol mekanizmaları AI yönetişiminin de parçası haline geliyor.

YORUM

Türkiye'deki kurumların agentic AI projelerini yalnızca inovasyon programı olarak değerlendirmesi ciddi bir **yönetişim eksikliği** yaratabilir. Özellikle finans, telekom, enerji ve kamu kurumlarında AI ajanlarının hangi sisteme erişebildiği, hangi işlemleri tek başına gerçekleştirebildiği ve hangi noktada insan onayı gerektiği açıkça tanımlanmalı.

CIO ve CISO açısından temel soru artık *"Hangi modeli kullanalım?"* değil, *"Bu modele hangi yetkiyi vermeye hazırız?"* olmalı. Yönetim kurulları AI riskini veri mahremiyetiyle sınırlamamalı; otonom sistem davranışı, kimlik yönetimi, işlem yetkisi ve acil durdurma mekanizmaları AI governance kapsamına alınmalı.

Sınav: *AI ajanları ERP, CRM veya ödeme sistemlerinde öneri üretmekten çıkıp işlem yapmaya başladığında gelecek. Avantajı en gelişmiş modeli satın alan değil, otonomiyi kontrol kaybetmeden ölçekleyebilen kurumlar elde edecek.*

FİNANS · AGENTİC AI

02 Wall Street Bankaları "Dijital Çalışan" Modeline Geçiyor



JPMorgan, Goldman Sachs, Morgan Stanley, UBS, Citi ve BNY gibi büyük finans kuruluşları, üretken AI kullanımını çalışanlara yardımcı olan chatbot seviyesinden görev gerçekleştiren agentic AI modeline taşıyor. Reuters'ın temmuz ayında aktardığı sektör görünümüne göre bankalar bu sistemleri wealth management, müşteri kabulü, treasury, trading ve operasyon süreçlerinde test ediyor veya kullanıma alıyor. Haziran ayında yapılan KPMG araştırmasında bankaların %51'inin AI ajanlarını pilot aşamasında denediği belirtiliyor.

BNY'nin yaklaşımı değişimin yönünü özellikle iyi gösteriyor: bazı dijital ajanlara kullanıcı kimliği atanıyor, günlük görevler veriliyor ve insan yöneticiler tarafından performansları takip ediliyor. UBS ise AI ajanlarının müşteri ve hesap bilgilerini analiz ederek danışmanlara aksiyon önerileri ürettiğini ve rutin görevleri azalttığını belirtiyor. Morgan Stanley de müşteri ilişkileri tarafında benzer dijital asistanları test ediyor.

Bunu bir chatbot projesinin bir sonraki aşaması olarak görmek eksik kalır. Bankalar aslında iş süreçlerini insan çalışanlarla yazılım ajanları arasında yeniden dağıtmaya başlıyor. Finans sektörü bu açıdan diğer sektörlerin de yakından izlemesi gereken erken bir uygulama alanı oluşturuyor.

YORUM

Türkiye'deki bankalar teknoloji kullanımında zaten yüksek olgunluk seviyesine sahip. Bu nedenle agentic AI için uygun zemin mevcut. Ancak doğrudan front-office uygulamalarına geçmeden önce operasyon, IT service management, reconciliation, risk reporting, fraud investigation ve compliance gibi **kontrol edilebilir süreçlerde başlanması** daha sağlıklı olacaktır.

En önemli konu **organizasyon tasarımıdır**. Bir AI ajanının sisteme giriş yapması, kayıt oluşturması veya işlem başlatması durumunda kim hesap verecek? Ajanın sahibi IT mi, iş birimi mi, model sağlayıcısı mı? Geleneksel RACI matrisleri bu yeni çalışma biçimine göre güncellenmek zorunda kalacak.

Ölçüm: *Yönetim kurulları AI yatırımlarının başarısını yalnızca kullanıcı sayısıyla ölçmemeli. Çevrim süresi, hata oranı, kontrol maliyeti, insan müdahalesi ihtiyacı ve yaratılan ekonomik değer çok daha anlamlı göstergeler olacaktır.*

YARI İLETKEN · TEDARİK

03 Çip Yarışında Darboğaz Artık Sadece GPU Değil: TSMC ve ASML Kapasiteyi Hızla Büyütüyor



AI altyapısına yönelik yatırım dalgası yarı iletken sektöründeki kapasite sınırlarını daha görünür hale getiriyor. TSMC, 2026'nın ikinci çeyreğinde net kârını yıllık bazda %77 artırarak yaklaşık 706,6 milyar Tayvan dolarına, yaklaşık 22 milyar ABD dolarına çıkardı. Şirketin performansı özellikle ileri üretim süreçleri ve AI işlemcilerine yönelik talebin gücünü gösteriyor.

Aynı dönemde, gelişmiş çip üretimi için kritik litografi ekipmanlarının başlıca tedarikçisi ASML de 2026 gelir tahminini yükseltti ve önümüzdeki iki yıl boyunca üretim kapasitesini yıllık yaklaşık %30 artırmayı planladığını açıkladı. Buna rağmen artırılan EUV kapasitesinin önemli bölümünün 2027'ye kadar şimdiden rezerve edilmiş olması, altyapı darboğazının yalnızca Nvidia GPU tedarikinden ibaret olmadığını gösteriyor.

AI değer zinciri artık GPU üreticisi, foundry, HBM bellek üreticisi, gelişmiş paketleme, litografi ekipmanı ve enerji altyapısından oluşan birbirine bağlı bir sistem haline geldi. Zincirin herhangi bir noktasındaki kapasite sınırı AI yatırımlarının hızını etkileyebilir.

YORUM

Türkiye'nin kısa vadede ileri seviye wafer fabrication yarışına girmesi ekonomik olarak gerçekçi olmayabilir. Ancak yarı iletken stratejisini yalnızca "fabrika kurmak" üzerinden değerlendirmek de hatalıdır. **Tasarım, power electronics, packaging, testing, embedded systems, savunma elektroniği ve belirli endüstriyel çip kategorileri** daha erişilebilir stratejik alanlar olabilir.

Kurumsal teknoloji yöneticileri açısından ise konu tedarik riskidir. AI altyapısı satın alma kararlarında artık yalnızca GPU fiyatı değil; teslim süresi, alternatif accelerator mimarileri, cloud kapasitesi ve enerji maliyeti birlikte değerlendirilmelidir.

Not: *Compute kapasitesine erişim, bazı sektörlerde sermayeye erişim kadar önemli bir rekabet unsuruna dönüşüyor.*

YARI İLETKEN · FİYATLAMA

04 Samsung Foundry Fiyatlarını %15'e Kadar Artırdı: AI Talebi Tedarikçi Güç Dengesini Değiştiriyor

TSMC'nin ileri üretim kapasitesindeki sıkışıklık rakip foundry'lere yeni alan açıyor. Samsung Electronics, ağustos ayında bazı ileri üretim süreçlerinde yeni sipariş fiyatlarını %10–15'e kadar yükseltti. Reuters'a göre özellikle 4 nm, 5 nm ve bazı 8 nm süreçlerinde fiyat artışları görülürken şirketin 4 nm üretim hattı yüksek kapasite kullanımına ulaştı.

Samsung'un küresel foundry gelirlerindeki payı 2026'nın ilk çeyreğinde yaklaşık %7 seviyesindeyken TSMC'nin payı %70'in üzerindeydi. Buna rağmen TSMC kapasitesinin önemli bölümünün AI talebiyle dolması, müşterileri Samsung ve Intel gibi alternatif üreticilere yöneltiyor.

Bu durum AI ekonomisinin ilginç bir yan etkisini ortaya koyuyor: pazar liderinin kapasitesinin dolması, ikinci seviye tedarikçilerin hem fiyatlandırma gücünü hem stratejik önemini artırıyor.

YORUM

Teknoloji stratejisinde **"best-of-breed" yaklaşımı her zaman dayanıklılık anlamına gelmez**. Kritik bir bileşenin tek bir tedarikçiden alınması teknik olarak optimal olabilir; ancak jeopolitik, kapasite veya fiyat riski açısından kurumun kırılganlığını artırabilir.

Türkiye'deki teknoloji, savunma ve telekom şirketleri kritik donanım tedarikinde **multi-sourcing yaklaşımını daha sistematik** hale getirmeli. Bu yalnızca procurement konusu değil; enterprise resilience konusudur.

Kapsam: *Semiconductor supply-chain concentration riski yalnızca satın alma ekiplerinin değil, teknoloji risk raporlarının da konusu olmalı.*

OT GÜVENLİK · KRİTİK ALTYAPI

05 Endüstriyel Kontrol Sistemleri Yeniden Hedefte: Siemens PLC'lerine Yönelik ABD Uyarısı

ABD'de CISA, FBI, NSA, Department of Energy ve EPA dahil federal kurumlar ağustos ayında kritik altyapıda kullanılan Siemens S7 serisi programlanabilir mantık kontrolörlerinin hedef alınması konusunda yeni bir uyarı yayımladı. Bu cihazlar su sistemleri, üretim tesisleri ve enerji altyapısı gibi operasyonel teknoloji ortamlarında yaygın olarak kullanılıyor.

Temmuz ayında CISA ve diğer kurumlar İran bağlantılı tehdit aktörlerinin PLC'leri hedeflediğine ilişkin önceki uyarılarını da güncellemişti. Kritik nokta, saldırıların yüksek teknolojiye sahip büyük tesislerle sınırlı olmaması; internet üzerinden erişilebilen veya yeterince segmentasyonu yapılmamış endüstriyel sistemlerin de hedef haline gelebilmesi.

AI tabanlı araçların saldırı hazırlığı, reconnaissance ve exploit geliştirme süreçlerini hızlandırması, OT güvenliğinde saldırganın ihtiyaç duyduğu teknik yetkinlik eşiğini de aşağı çekebilir.

YORUM

Türkiye açısından bu haber özellikle **enerji, su, ulaşım, üretim ve belediye altyapısı** için önemlidir. OT ortamlarının klasik kurumsal IT güvenlik yaklaşımıyla yönetilmesi yeterli değildir. Patch uygulamanın mümkün olmadığı sistemlerde segmentation, asset inventory, secure remote access ve compensating controls kritik hale gelir.

CISO'ların yönetim kuruluna sunduğu siber risk raporlarında **IT ve OT riskleri ayrı ayrı görünür olmalıdır**. "Kaç vulnerability kapatıldı?" metriğinin yanında hangi fiziksel hizmetin kesintiye uğrayabileceği sorusu sorulmalıdır.

Perspektif: *Konuyu yalnızca bir siber güvenlik problemi olarak görmek eksik kalır; asıl mesele operasyonel dayanıklılıktır.*

REGÜLASYON · KRİPTO

06 ABD Kripto Regülasyonunda Yeni Dönem: SEC Token İhraçları İçin Özel Çerçeve Önerdi

ABD Securities and Exchange Commission, 18 Ağustos'ta kripto varlıklara yönelik yeni bir düzenleyici çerçeve önerdi. Taslak, belirli token ihraçlarının geleneksel menkul kıymet kurallarından daha esnek biçimde yararlanabilmesini ve belirli koşullar altında safe-harbor mekanizmalarının kullanılabilmesini öngörüyor. Teklif kapsamında bazı küçük ihraçlar ile daha büyük token satışları için farklı disclosure yükümlülükleri tasarlanıyor.

Bu yaklaşım, son yıllarda ABD kripto politikasına hakim olan "enforcement yoluyla düzenleme" modelinden daha tanımlı bir piyasa yapısına geçiş arayışını temsil ediyor. Bununla birlikte düzenlemenin kalıcılığı, yalnızca SEC kararlarına değil Kongre düzeyindeki mevzuata da bağlı olacak.

Finans sektörü açısından asıl önemli olan kripto varlığın kendisinden çok, blockchain tabanlı sermaye oluşumu, settlement, custody ve ödeme altyapısının geleneksel finans sistemiyle giderek daha fazla birleşmesi.

YORUM

Türkiye'nin kripto regülasyonunda temel hedef yalnızca yatırımcıyı korumak olmamalı. **Tokenizasyon, kurumsal custody, programmable money ve blockchain tabanlı settlement** uygulamalarının finans altyapısına nasıl entegre edileceği ayrıca değerlendirilmelidir.

Bankalar açısından fırsat, kripto alım satımından çok **regüle dijital varlık altyapısında güvenilir aracı** rolünü üstlenmek olabilir.

Uzun vade: *Para, menkul kıymet ve varlık sahipliği altyapısının programlanabilir hale gelmesi, finansal sistemin işleyişini kalıcı biçimde etkileyebilir.*

SAVUNMA · UZAY

07 Golden Dome İçin 18 Uydu: Savunma Mimarisi Uzaya Taşınıyor



L3Harris Technologies, ABD'nin Golden Dome füze savunma programı kapsamında 18 uydu üretmek üzere 955 milyon dolarlık sözleşme aldı. Sözleşme, ABD Space Force bağlantılı bir kurum tarafından verildi ve şirket son dönemde uydu üretim kapasitesini bu program doğrultusunda genişletti.

Gelişme, modern savunmanın karada yerleşik radar ve interceptor sistemlerinden giderek daha fazla dağıtık uydu ağlarına kaydığını gösteriyor. Düşük yörüngedeki sensörler, erken tespit, tracking ve komuta-kontrol süreçlerinin hızını artırırken savunma mimarisini aynı zamanda yazılım, veri füzyonu ve yüksek hızlı iletişim sistemlerine daha bağımlı hale getiriyor.

Bu tablo, "savunma teknolojisi" ile "bilgi teknolojisi" arasındaki geleneksel ayrımı da zayıflatıyor. Modern bir uydu ağı aynı zamanda büyük ölçekli bir distributed computing ve real-time data mimarisi.

YORUM

Türkiye için çıkarım yalnızca daha fazla uydu üretmek değildir. **Uydu sensörleri, data fusion, AI destekli hedef sınıflandırması, secure communications ve komuta-kontrol yazılımları** birlikte değerlendirilmelidir.

Savunma şirketleri açısından yazılım ve AI kabiliyeti, platform üretimi kadar belirleyici hale geliyor. Kritik altyapı yöneticileri için ise **uzay tabanlı servis bağımlılığı yeni bir business continuity boyutudur**.

Yakınsama: *Ticari ve askeri uzay altyapısı birbirine yaklaştıkça uydu hizmetlerinin cyber resilience ve supply-chain security boyutu da önem kazanacak.*

VERİ MERKEZİ · ENERJİ

08 Veri Merkezleri Elektrik Şebekesinin Pasif Müşterisi Olmaktan Çıkıyor

2 Temmuz'da Kuzey Virginia'da bir iletim hattının devre dışı kalmasının ardından çok sayıda veri merkezinin otomatik olarak şebekeden ayrılıp yedek enerjiye geçmesi, PJM elektrik sisteminde alışılmadık büyüklükte bir talep düşüşü oluşturdu. Yaklaşık 3 gigawatt, yani o andaki PJM talebinin yaklaşık %3'ü kısa süre içinde sistemden çıktı. Etkiler Washington çevresinden Chicago'ya uzanan bölgede hissedildi.

Olay, veri merkezlerinin yalnızca yüksek enerji tüketen tesisler değil, elektrik şebekesinin dinamik davranışını etkileyebilecek büyüklükte yük kümeleri haline geldiğini gösterdi. Aynı bölgede şebeke congestion maliyetleri de 2026'nın ilk yarısında sert biçimde yükseldi; PJM'in bağımsız piyasa gözlemcisine göre transmission constraint maliyetleri 6 milyar dolara ulaştı.

ABD Energy Information Administration da AI ve veri merkezi büyümesinin etkisiyle elektrik tüketiminin 2026 ve 2027'de yeni rekorlara çıkmasını bekliyor.

YORUM

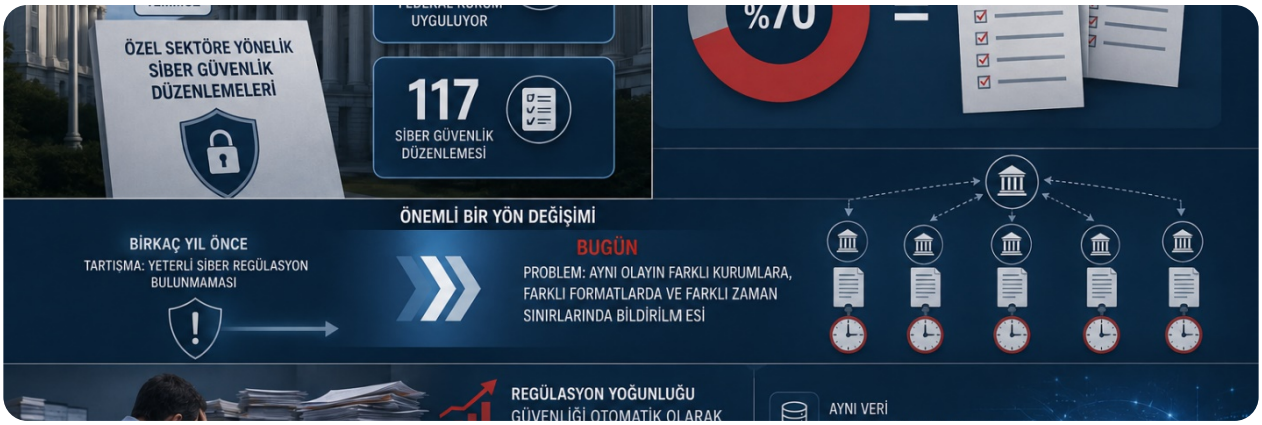
AI stratejisinin en az konuşulan bileşeni enerjidir. Kurumların compute planları artık enerji erişimi ve enerji fiyatından bağımsız hazırlanamaz.

Türkiye veri merkezi yatırımlarını çekmek istiyorsa yalnızca fiber altyapısı ve vergi teşviki yeterli olmayacaktır. **Şebeke kapasitesi, yenilenebilir üretim, enerji depolama ve uzun vadeli enerji sözleşmeleri** birlikte ele alınmalıdır.

Çoklu bakış: *Aynı konu CIO'ya kapasite planlaması, CFO'ya enerji maliyeti, CRO'ya concentration ve continuity risk olarak geliyor. AI altyapısını yalnızca IT yatırımı olarak değerlendirmek giderek daha yanıltıcı.*

REGÜLASYON · SİBER GÜVENLİK

09 Siber Regülasyonların Yeni Problemi: Eksiklik Değil, Çakışma



ABD Government Accountability Office tarafından 22 Temmuz'da yayımlanan analiz, özel sektöre yönelik 117 siber güvenlik düzenlemesinin 37 federal kurum tarafından uygulandığını ortaya koydu. GAO'ya göre düzenlemelerin 80'i, yani yaklaşık %70'i, başka bir düzenlemeyle aynı veya benzer raporlama yükümlülükleri içeriyor.

Bu durum önemli bir yön değişikliğine işaret ediyor. Birkaç yıl önce temel tartışma yeterli siber regülasyon bulunmamasıydı. Bugün özellikle finans ve kritik altyapı sektörlerinde problem, aynı olayın farklı kurumlara farklı formatlarda ve farklı zaman sınırlarında bildirilmesi olabilir.

Regülasyon yoğunluğu güvenliği otomatik olarak artırmıyor. Kontrol ekiplerinin önemli bölümü aynı veriyi farklı formatlarda üretmeye başladığında compliance maliyeti yükselirken gerçek risk azaltma kapasitesi aynı oranda artmayabilir.

YORUM

Türkiye'de **BDDK, SPK, KVKK, sektörel düzenleyiciler ve uluslararası standartlardan** kaynaklanan teknoloji yükümlülükleri zaman içinde benzer bir karmaşıklık oluşturabilir.

Çözüm her regülasyon için ayrı kontrol seti oluşturmak değil, **tek bir enterprise control framework üzerinden multiple-regulation mapping** yapmaktır. ISO 27001, NIST CSF, COBIT veya kuruma özgü bir control library temel alınarak bir kontrolün birden fazla yükümlülüğü karşılaması sağlanabilir.

Hedef: *Kontrol sayısını artırmak değil; aynı kontrol yapısıyla birden fazla yükümlülüğü karşılayıp tekrarı azaltırken assurance seviyesini yükseltmek.*

AGENTİC AI · STANDARTLAR

10 AI Ajanları İçin Yeni Standart Savaşı: A2A Açık Ekosisteme Taşınıyor

Google tarafından geliştirilen Agent2Agent Protocol – A2A, ağustos ayında Agentic AI Foundation çatısı altına taşındı. A2A'nın amacı farklı sağlayıcılara ait bağımsız AI ajanlarının ortak bir protokol üzerinden birbirleriyle iletişim kurabilmesi. Bu yaklaşım, AI uygulamalarını araçlara ve veri kaynaklarına bağlamaya odaklanan Model Context Protocol – MCP gibi diğer standartlarla tamamlayıcı bir rol üstleniyor.

Bu gelişme ilk bakışta teknik bir protokol haberi gibi görünse de geçmiş teknoloji platformlarının gelişimi dikkate alındığında stratejik önemi daha büyük. İnternet TCP/IP, web HTTP, kurumsal entegrasyon API standartları üzerinden ölçeklendi. Agentic AI'ın da geniş çapta benimsenebilmesi için farklı ajanların birbirini keşfedebilmesi, yeteneklerini tanımlayabilmesi ve güvenli biçimde görev aktarabilmesi gerekiyor.

Dolayısıyla rekabet yalnızca OpenAI, Google veya Anthropic'in hangi modelinin daha güçlü olduğu üzerinden ilerlemeyecek. Ajanların hangi standart üzerinden birbirine bağlanacağı da platform gücünü belirleyebilir.

YORUM

Kurumsal teknoloji yöneticilerinin bugün yapacağı en büyük hata, **agentic AI mimarisini tek bir model sağlayıcısına sıkı biçimde bağlamak** olabilir.

Türkiye'deki büyük kurumların AI mimarilerini tasarlarken **model portability, interoperability ve vendor exit senaryolarını** şimdiden düşünmesi gerekiyor. MCP, A2A ve benzeri açık protokoller bu açıdan yalnızca geliştiricilerin takip edeceği teknik standartlar değil; enterprise architecture ve teknoloji tedarik stratejisinin de konusu.

Kritik nokta: *Model seçimi değil, mimari bağımlılık. Bugün verilen AI mimarisi kararlarının kurumu birkaç yıl sonra daha çevik mi yoksa belirli sağlayıcılara daha bağımlı mı hale getireceği baştan sorgulanmalı.*



Bir sonraki sayıda buluşmak üzere

Teknoloji gündeminin Türkiye yansımalarını birlikte takip etmeye devam edelim.

HAZIRLAYAN

Hakan Kantaş

BiTekDer · Eylül 2026

© 2026 BiTekDer · Bilgi Teknolojileri Derneği