



Microsoft 365
Copilot

Yapay Zeka Çağında Veri Güvenliğini Sağlama

BT Liderlerine Yönelik Kılavuz

E-kitap



Bu kılavuz, kurumlarının verilerini güvende tutarken yapay zekayı benimsemeyi artırması gereken BT liderleri için hazırlanmıştır. Kurumunuzun yapay zeka dönüşümüne güvenle liderlik etmenizi sağlayacak bilgileri sunarken, yapay zekanın veri güvenliği ve gizliliğine sunduğu riskleri anlamanıza yardımcı olur.

İçindekiler

01

Yapay zeka destekli işin
yeni kuralları

03

Gölge yapay zeka
sorunu

05

Düzenleyici labirent

07

Microsoft 365 Copilot:
Güvenebileceğiniz
yapay zeka

02

Yapay zekanın veri
güvenliği üzerindeki
etkisini anlama

04

BYOAI gerçekliği

06

Yapay zeka çözümlerini
değerlendirmek için
güvenlik öncelikli
çerçeve

08

Yapay zeka
dönüşümünün
güvenli yolu

01

Yapay zeka destekli işin yeni kuralları

Üretici AI, yenilik için yeni kapılar açıyor ve ekiplerin her zamankinden daha hızlı ve daha akıllı şekilde çalışmasına yardımcı oluyor. İleri görüşlü kurumlar için yapay zeka yalnızca başka bir teknoloji trendi değildir; aynı zamanda işleyiş biçimleri, değer sunma yöntemleri ve rekabet avantajını sürdürmeleri açısından vazgeçilmez bir iş zorunluluğudur.

Ancak bu hızlı benimseme, BT liderlerinin proaktif olarak ele alması ve kontrol etmesi gereken yeni ve güçlendirilmiş zorlukları beraberinde getirir. Yapay zeka sistemleri, tüm veri ekosisteminde aktif olarak bilgi arayabilir ve bilgileri birleştirebilir, bu da geleneksel araçların ötesinde güvenlik risklerini artırır. Yapay zekanın hızlı bir şekilde genişlemesine rağmen, kurumların yalnızca **%1**'i yapay zekayı uygun güvenlik protokolleri ile iş akışlarına tam olarak entegre ettiklerini bildirmektedir.¹ Ekibiniz, yapay zeka yolculuğunuzun başlangıcından itibaren sağlam güvenlik ve yönetim önlemleri uygulayarak, hassas verileri etkili bir şekilde koruyabilir, uyumluluk gereksinimlerini karşılayabilir ve yeniliklerin gelişmesini sağlarken kurumunuzun bilgilerini koruyabilir.

Yapay zeka benimseme dalgası şimdiden burada



02

Yapay zekanın veri güvenliği üzerindeki etkisini anlama

Belirli zorluklara dalmadan önce, yapay zekanın veri güvenliği ortamını nasıl temelden değiştirdiğini anlamak önemlidir. Verilere yalnızca özel olarak talimat verildiğinde erişen geleneksel yazılımların aksine üretici AI, aldığı tüm bilgilere dayanarak aktif olarak işler, analiz eder ve içerik oluşturur.

Bu fark çeşitli nedenlerle önemlidir:

- Yapay zeka araçları, insanların gözden kaçırabileceği veriler arasındaki bağlantıları keşfedebilir
- Birden çok kaynak arasında otomatik olarak bilgi sentezleyebilirler
- Hassas girdilerden öğeler içeren yeni içerik oluşturabilirler

Geleneksel güvenlik araçlarınız büyük olasılıkla bu özellikler dikkate alınmadan tasarlanmıştır. Geleneksel yazılım verilere erişirken öngörülebilir yollar izlese de yapay zeka, bilgi ekosistemi aracılığıyla beklenmedik rotaları izleyerek hassas verileri beklenmedik şekillerde açığa çıkarabilir.

Bu temel geçiş, yapay zekanın kurumunuzun bilgi varlıklarıyla nasıl etkileşime girdiğini ele alan güvenlik ve veri yönetimine yönelik yeni yaklaşımlar gerektirmektedir.

03

Gölge yapay zeka sorunu

Yapay zeka benimseme yolculuğunuzda nerede olursanız olun, çalışanlarınız zaten kendi çözümlerini bularak "gölge yapay zeka" olarak bilinen şeyleri oluşturuyor.

Bu yetkisiz kullanım, güvenlik duruşunuzda önemli kör noktalar oluşturur. Çalışanlar kurum verilerini harici yapay zeka sistemleri ile paylaştıklarında, mevcut güvenlik denetimlerini atlar ve çoğu kurumun ele almaya hazır olmadığı güvenlik açıkları oluşturur.

Gölge yapay zeka yalnızca bir güvenlik sorunu değildir, aynı zamanda kurumunuzdaki karşılanmamış üretkenlik gereksinimlerinin bir belirtisi olabilir. Çalışanlar onaylanmamış araçlara başvurduğunda bu, resmi sistemlerinizin gereksinimlerini karşılamadığı noktaları işaret eder. Gölge yapay zekayı ele almak için hem daha güçlü yönetim hem de gelişmiş üretkenlik çözümleri gerekir.

%64

işlerini yapmak için gereken zamana ve enerjiye sahip olmada zorlanan çalışanların oranı.³
Üretkenliklerini önemli ölçüde artıran yapay zeka araçlarını keşfettiklerinde BT onayı olsun ya da olmasın kullanırlar.

Gölge yapay zekanın ortaya çıkma nedeni:

- Çalışanlar, yapay zekanın etkileyici özellikleriyle üretkenliği artırmaya isteklidir
- Günlük iş yükleri mevcut zamanı ve enerjiyi giderek daha fazla aşıyor
- Ekipler aynı kaynaklarla daha fazlasını sunmak için artan baskılarla karşı karşıyadır
- Tüketici yapay zeka araçları, onay engelleri olmadan anında çözümler sunar
- Resmi BT tedarik süreçleri yeniliğin hızıyla eşleşemez

Gölge yapay zekanın riskleri:

- Harici yapay zeka sistemleri tarafından hangi kurum verilerinin işlendiğine dair hiçbir görünürlük yoktur
- Gizli bilgilerin saklanmayacağına garanti yoktur
- Farklı yapay zeka platformlarında tutarlı güvenlik standartları yoktur
- Uyumluluk amacıyla denetim imkanı yoktur
- Mevcut güvenlik altyapınızla entegrasyon yoktur

Şu senaryoyu göz önünde bulundurun:

Karmaşık bir elektronik tabloyla mücadele eden bir finansal analist, yardım almak için bunu yetkisiz bir yapay zeka aracına yükler. Bu elektronik tabloda müşteri finansal verileri, dahili ölçümler ve tahminler yer alır. Analist ihtiyaç duyduğu yardımı alırken, kurumunuzun hassas finansal verileri artık güvenlik çevrenizin dışındadır ve izleme sistemleriniz tarafından tamamen görünmez haldedir.



04

BYOAI gerçekliği

Çalışanlar, liderlik konusunda açık bir rehberlik olmadan giderek daha fazla yapay zeka benimsemeyi kendi ellerine alıyorlar. **%78** oranında yapay zeka kullanıcısı "kendi yapay zekanı getir" (BYOAI) yaklaşımını işyerinde uyguluyor.² Bu trend, çalışanların **%80**'inin BYOAI uygulamalarını kullandığı küçük ve orta ölçekli kurumlarda daha da belirgindir.²

Bu onaylanmamış yaklaşım, önemli dezavantajlar içerir. Çalışanlar genellikle yapay zeka kullanımlarını gizli tutuyorlar. **%52**'si, önemli görevler için yapay zeka kullandığını kabul etmekte isteksizdir ve **%53**'ü yapay zeka kullanımının işlerini yapay zekaya kaybedilebilir gösterdiğinden endişe ediyor.² Bu gizlilik, kurumların yalnızca stratejik yapay zeka uygulamasının tüm avantajlarından yararlanmasını önlemekle kalmıyor, aynı zamanda liderlerin siber güvenlik ve veri gizliliğini **1 numaralı** endişeleri olarak belirttikleri bir ortamda ciddi güvenlik açıkları oluşturuyor.²

Yapay zekanın yaygın kullanımı ve kaçınılmaz büyümesi göz önüne alındığında yapılacak şey kurumunuzda yapay zekaya izin verilip verilmeyeceğini sorgulamak değil; çalışanlarınızın ihtiyaçlarını karşılayan ve kurumunuzun verilerini güvenli tutan bir çözüm sağlamaktır.

05

Düzenleyici labirent

Veri gizliliği ve güvenliği ile ilgili çerçeveler ve yasalar, yapay zeka benimsenirken başka bir karmaşıklık katmanı oluşturur. Bazı çerçeveler yapay zeka yönetimi için özel olarak tasarlanmışken, diğerleri daha geniş uygulamalara sahiptir ve yine de bilgileri nasıl işlediğinizi etkiler. İhlallere yönelik cezalar ise ciddi olmaya devam eder.

Çalışanlarınız yapay zeka araçlarını uygun bir gözetim olmadan kullandığında yanlışlıkla uyumluluk ihlalleri oluşturabilirler. Yapay zeka, geleneksel teknolojilerin yapamayacağı şekillerde düzenlenmiş bilgilere erişebildiği, bunları birleştirebildiği ve ifşa edebildiği için bu riski daha büyük hale getirir.

Yapay zeka kullanımınızı etkileyen temel düzenlemeler:

GDPR

Avrupa Birliği'nin Genel Veri Koruma Yönetmeliği, kişilere kişisel verileri üzerinde kontrol imkanı verir ve verilerin işlenmesi için açık bir onay gerektirir.

AB Yapay Zeka Yasası:

Avrupa Birliği'nin yapay zeka sistemlerini risk düzeylerine göre düzenlemek için özel olarak tasarlanmış kapsamlı çerçevesi

HIPAA

Bu ABD sağlık hizmetleri federal yasası, güvenli sağlık bilgilerinin işlenmesi için sıkı standartlar belirler

NIST Yapay Zeka Risk Yönetimi Çerçevesi

Bu gönüllü ABD rehberi, kurumların yapay zeka sistemlerinin tasarımı, geliştirilmesi ve dağıtımındaki riskleri ele almasına yardımcı olur

Yapay zeka ile uyumluluk riskleri:

- Müşteri verilerinin, onaylanan bölgeler dışındaki sunucularda işlenmesi
- Kişisel bilgilerin uygun onay olmadan kullanılması
- Hassas verilerin uygun saklama kontrolleri olmadan sistemlerde kalıcı hale gelmesi
- Güvenli bilgilere nasıl erişildiğine ve kullanıldığına dair denetim izi olmaması
- Yapay zeka tarafından oluşturulan içeriklerin sektöre özgü uyumluluk gereksinimlerini ihlal etmesi

Bu ihlaller ciddi sonuçlara yol açabilir:

- Büyük finansal cezalar (GDPR para cezaları genel gelirinizin **%4**'üne ulaşabilir)⁴
- Etkilenen taraflara veri ihlallerini bildirme gereksinimleri
- Etkilenen kişilerin yasal işlem başlatması
- Kurumunuzun itibarının ve müşteri güveninin zarar görmesi

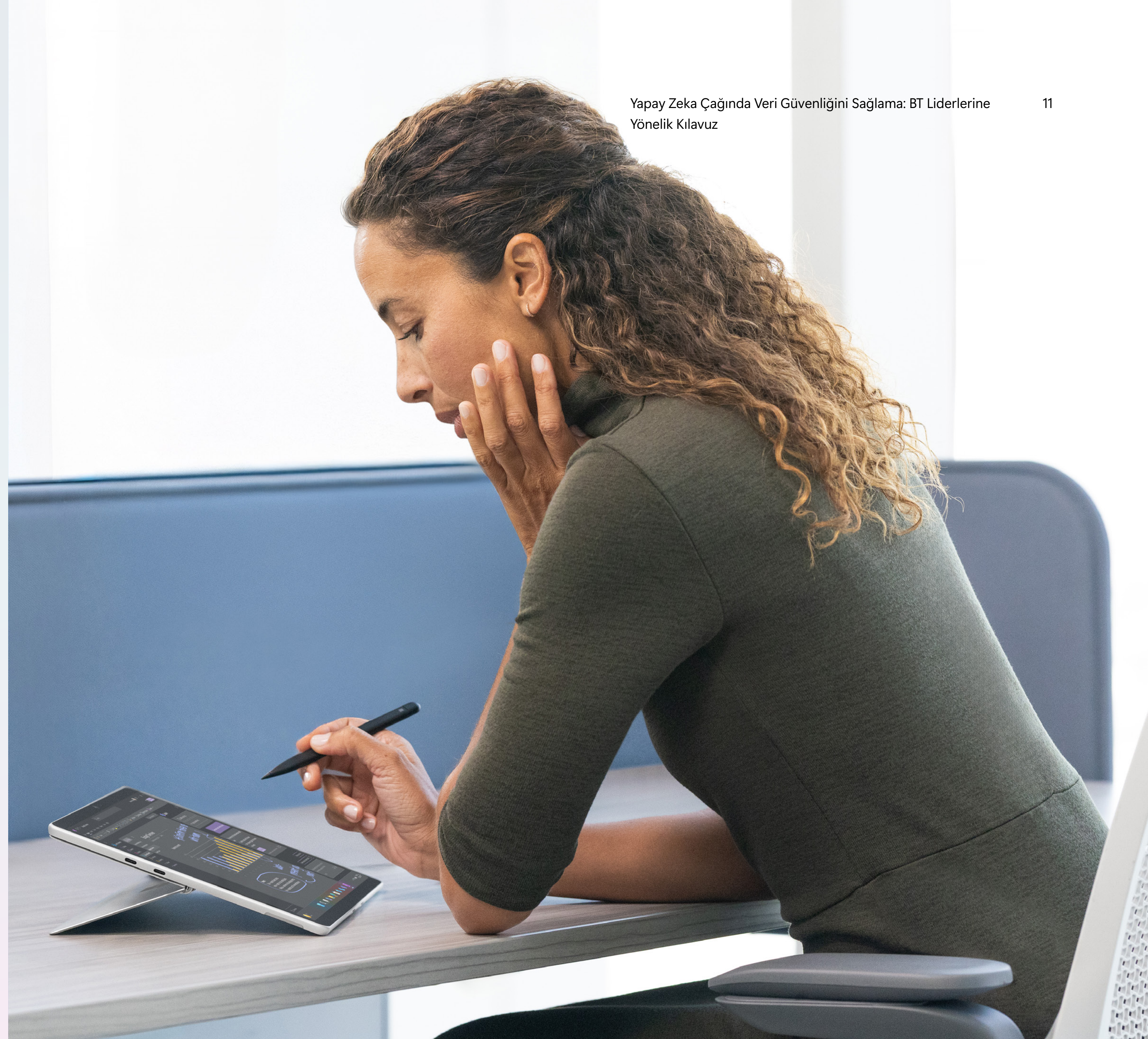
Yapay zeka kullanımı kurumunuz genelinde büyüdükçe, kurumunuzu ve müşterilerinizi etkileyen düzenlemelere uyumlu kalmasını sağlarken, çalışanların verimli bir şekilde çalışmasına yardımcı olan bir yönetime ihtiyacı duyarsınız.

06

Yapay zeka çözümlerini değerlendirmek için güvenlik öncelikli çerçeve

Gölge yapay zeka, BYOAI ve önemli riskler oluşturan yönetmeliklerle; hassas verileri koruyup gelişen düzenleyici gereksinimlere uyum sağlarken ve yapay zeka çözümlerini değerlendirirken kurumunuzun yenilikleri desteklemelerine yardımcı olan yapılandırılmış bir yaklaşıma ihtiyacınız vardır.

Aşağıdaki çerçeve, bir yapay zeka platformunun her iki açıdan da beklentileri karşılayıp karşılamadığını değerlendirmek için altı basit soru sunmaktadır.



1. Soru

Baştan sona kurumsal düzeyde güvenlik sunuyor mu?

Doğru çözümle, güvenliğiniz sorunlara sadece ortaya çıktıktan sonra tepki vermekle kalmayıp, kurumunuzun verilerindeki zayıflıkları daha büyük sorunlar haline gelmeden önce proaktif bir şekilde arayacak şekilde dönüşür.

Şu çözümleri arayın:

- Tüm veri ekosisteminizde gerçek zamanlı görünürlük sağlayan
- Olası veri risklerini olay haline gelmeden önce otomatik olarak belirleyen
- Hassas bilgileri her düzeyde koruyan

2. Soru

Mevcut güvenlik denetimlerini kolayca benimseyip geliştirebilir mi?

Kurumunuzun güvenlik kuralları yapay zeka ile sorunsuz bir şekilde çalışmalıdır. Yapay zeka çözüm sağlayıcınız mevcut güvenlik çerçevelerinize saygı göstermeli ve bunlara entegre olmalıdır, tamamen yeni çerçeveler oluşturmanızı gerektirmemelidir.

Şu çözümleri arayın:

- Mevcut güvenlik kurallarınızı, hassasiyet etiketlerinizi ve bilgi koruma ayarlarınızı sorunsuz bir şekilde benimseyen
- Ayrıntılı erişim denetimlerini bireysel düzeyde uygulayarak hiçbir kullanıcının erişmemesi gereken verilere erişimi olmamasını sağlayan
- Erişim denetimlerini bozma girişimlerini aktif olarak işaretleyen

3. Soru

Yerleşik yönetim ve gizlilik denetimleri içeriyor mu?

Yapay zeka araçları daha proaktif bir şekilde çalıştığından güvenlik önlemlerinizin de proaktif olması gerekir. Güçlü veri yönetimi uygulamak, çalışanlarınızın hassas bilgileri riske atmadan güvenle yenilik yapabileceği açık sınırlar oluşturur.

Şu çözümleri arayın:

- Tüm faaliyetlerde otomatik kural uygulama ile yapay zeka yönetimini merkezileştiren
- Potansiyel aşırı veri paylaşımının erken tespiti dahil eden
- Uyumlu yapay zeka kullanımını sağlamak için düzenleyici çerçevelere uyum sağlayan

4. Soru

Tüm kurum genelinde tutarlı bir şekilde kurulabilir mi?

Çalışanlarınızın kendi çalışma stilleri, kendi programları vardır ve dünyanın her yerinden çalışabilirler. Yapay zeka herkese fayda sağlamalıdır.

Şu çözümleri arayın:

- Günlük iş akışlarında sorunsuz kurulum ve kolay yapay zeka benimsemesi sunan
- Ücretsiz yapay zeka sohbetinden ölçeklenebilir aracı çözümlerine kadar esnek erişim sağlayan
- Çalışanların yapay zeka akıcılığı kazanmasına ve bunu çalışmalarına entegre etmesine yardımcı olan

5. Soru

Mevcut çerçevelere sorunsuz bir şekilde entegre oluyor mu?

Kurumunuz şu anda kendi dijital yazılım programları, uygulamaları ve daha fazlası altyapısıyla çalışıyor.

Şu çözümleri arayın:

- Kesintiyi en aza indirmek için araçlarınız ve programlarınızla sorunsuz bir şekilde ağ oluşturan
- İşin araçlar arasında sorunsuz bir şekilde akabilmesi için tüm uygulamalarda sürekli bir yapay zeka deneyimi sağlayan
- Mevcut iş akışları içindeki görevleri otomatikleştiren ve iyileştiren

6. Soru

Kullanıcıların yenilik yapma yetkisi var mı?

Yapay zeka, özünde işin yapılma şeklini dönüştürmelidir. Sadece otomasyon sağlamamalı, üretkenliği artırmalı ve yeniliği teşvik etmelidir.

Şu çözümleri arayın:

- Zaman kayıplarını kolaylaştırılmış işlemlere dönüştüren
- Tekrarlayan görevleri otomatikleştiren
- Çalışanları zamanı geri kazanmaları ve önceliklere odaklanmaları için güçlendiren

07

Microsoft 365 Copilot: Güvenebileceğiniz yapay zeka

Microsoft 365 Copilot; sağlam güvenlik, yönetim ve erişim kontrolleri sunarak güvenli kurulum ve sürekli yenilik sağlayan bir üretici AI çözümüdür. Copilot Sohbet'in çalıştığınız yerde çalıştığı ve ekibinizin kodlama becerilerine ihtiyaç duymadan özel yapay zeka araçları oluşturabildiği Copilot Studio gibi sezgisel araçlarla üretkenliği artırır.

Copilot, Microsoft 365 ortamınızda sorunsuz bir şekilde entegre olur ve ekstra yapılandırmalar olmadan kullanıcı izinlerini, hassasiyet etiketlerini, veri kaybı önleme kurallarını ve coğrafi veri yerleşikliği gereksinimlerini devralır. Copilot, çalışanlarınızın zaten kullandığı araçlara yapay zekayı entegre ederek, verileri güvenilir Microsoft 365 ortamınızda tutarken güvenlik risklerini azaltır.

Microsoft'un taahhütleri kurumunuzun kontrol altında kalmasını sağlar:

- Verileriniz beklemede ve taşınırken güvendedir
- Verileriniz, yapay zeka modellerini eğitmek için kullanılmaz
- Buluta hangi bilgilerin gireceğini siz seçersiniz
- Yapay zeka güvenliği ve telif hakkı risklerine karşı güvende olursunuz

Copilot Denetim Sistemi ve SharePoint Gelişmiş Yönetim gibi amaca yönelik oluşturulan yönetim araçları, BT ekiplerine uyumluluğu sürdürmek için gereken görünürlük, kontroller ve denetim loglarını sağlar.

Microsoft 365 Copilot ile yenilik ve güvenlik arasında seçim yapmak zorunda değilsiniz; ikisine de sahip olabilirsiniz.

Yapay zeka dönüşümünün güvenli yolu

Her şeyi kökten değiştiren yapay zeka, BT liderlerine yenilik ve güvenliği dengeleyerek stratejik değer sunmaları için eşsiz bir fırsat sunuyor.

Microsoft 365 Copilot gibi güvenli yapay zeka araçlarını uygulayarak, gölge yapay zeka risklerini ortadan kaldırırken çalışanlarınızı daha fazla üretkenlik için güçlendireceksiniz. Geleceğe doğru giden yol, yenilikleri güvenli bir şekilde sağlamaktan geçer. Güvenli yapay zekayı benimseme konusundaki liderliğiniz, BT'nin bir dönüşüm sağlayıcısı olmasını sağlayacak ve verilerinizin güvenli ve uyumlu kalmasına olanak tanıırken kurumunuzun bu yeni dönemde başarılı olmasına yardımcı olacaktır.



Microsoft 365 Copilot'ı kullanmaya başlayın

Kaynaklar:

¹"Superagency in the workplace: Empowering people to unlock AI's full potential", McKinsey & Company, 28 Ocak 2025. <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

²"İşyerinde Yapay Zeka Burada. İşte Şimdi Zor Kısma Geldik", Microsoft Çalışma Trendi Endeksi, 8 Mayıs 2024. <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>.

³"Yapay Zeka Çalışma Şeklini Düzeltebilir mi?" Microsoft Çalışma Trendi Endeksi, 9 Mayıs 2023. <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>.

⁴"95/46/AT sayılı Direktif'i yürürlükten kaldıran, gerçek kişilerin kişisel verilerin işlenmesi bakımından korunması ve bu tür verilerin serbest dolaşımı hakkında 27 Nisan 2016 tarihli ve (AB) 2016/679 sayılı Avrupa Parlamentosu ve Konsey Tüzüğü (Genel Veri Koruma Tüzüğü)", Avrupa Parlamentosu ve Avrupa Birliği Konseyi, 27 Nisan 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.