Microsoft Security Copilot

Microsoft 365 E5 Kullanım, Onboarding ve SCU Kapasite Rehberi

Hazırlayan

Mustafa Emre SONER

Modern Work & Security Manager

TWORKS

Sürüm 1.0 | 13 Ağustos 2026

İçindekiler

1. Yönetici Özeti ... 3
Kararı etkileyen beş kritik bulgu ... 3
2. Kapsam, Yöntem ve Doğrulama ... 4
Belgenin kapsamı ... 4
Kapsam dışı ... 4
Yöntem ve doğrulama ... 4
3. Security Copilot ve Microsoft 365 E5 İlişkisi ... 5
Lisans modelleri: Inclusion ve Provisioned ... 5
Deneyimler: Standalone, Embedded ve Ajanlar ... 5
Inclusion kapsamı dışında kalanlar ... 6
4. Onboarding: Adım Adım Devreye Alma ... 7
Portal ve erişim adresleri ... 7
Akış A — Microsoft 365 E5 / E7 sahibi kurumlar ... 7
Akış B — Microsoft 365 E5 / E7 dışı kurumlar ... 9
Rol ve yetkilendirme (RBAC) modeli ... 10
Ajan devreye alma akışı ... 11
Ajan bazlı ön koşullar ve kurulum yolları ... 12
Kullanımın izlemeye alınması ... 12
Onboarding kontrol listesi ... 12
5. SCU Hesaplaması ve Kapasite Yönetimi ... 14
SCU nedir, neyi tüketir ... 14
E5 dahil kapasite formülü ... 14
Dokümante edilmiş tüketim referansları ... 15
Örnek kapasite planı (2.500 kullanıcı) ... 15
İzleme, eşik ve aşım davranışı ... 16
6. Örnek Kullanım Senaryoları ... 17
Otomasyon ve entegrasyon seçenekleri ... 20
7. Güvenlik Uzmanı Gözüyle Kontrol: Sık Yapılan Hatalar ... 21
Lisans ve kapasite ... 21
Devreye alma ve yapılandırma ... 21
Dil, uyum ve operasyon ... 22
8. Veri Koruma, Veri Yerleşimi ve KVKK Değerlendirmesi ... 23
Müşteri verisi ve sistem günlükleri ... 23
Veri saklama konumu ve prompt değerlendirme konumu ... 23
Veri paylaşımı tercihleri ... 23
Saklama ve silme ... 24
9. Öneriler ve 30-60-90 Gün Yol Haritası ... 25
10. Ekler ... 27

1. Yönetici Özeti

Bu belge, Microsoft 365 E5 lisansına sahip bir kurumun Microsoft Security Copilot'ı hangi koşullarda ek ücret ödemeden kullanabileceğini, devreye alma (onboarding) adımlarını, Security Compute Unit (SCU) kapasitesinin nasıl hesaplandığını ve hangi senaryolarda somut değer ürettiğini tek bir referansta toplar. Tüm teknik iddialar Microsoft Learn üzerinden doğrulanmış, ürün dokümantasyonunda karşılığı olmayan hiçbir rakam belgeye alınmamıştır.

Temel tespit: **Microsoft 365 E5 ve E7 müşterileri için Security Copilot lisansa dahildir; her 1.000 ücretli kullanıcı lisansı başına ayda 400 SCU, aylık 10.000 SCU tavanına kadar ek ücret olmaksızın sağlanır.** Ancak "lisansa dahil olmak" ile "tenant'ta kullanılabilir olmak" aynı şey değildir; etkinleştirme kademeli dağıtımla yapılır ve doğrulanması gerekir.

Kararı etkileyen beş kritik bulgu

1. **Uygunluk otomatik erişim anlamına gelmez.** Rollout 18 Kasım 2025'te başlamıştır ve kademelidir. Tenant'ın etkin olup olmadığı Microsoft 365 Message Center bildirimi veya ürün içi banner ile doğrulanır.
2. **Dahil kapasite aylık havuzdur, saatlik provizyon değildir.** Kullanılmayan SCU devretmez, her ay sıfırlanır. Bu, klasik "provisioned + overage" modelinden farklı bir planlama disiplini gerektirir.
3. **Ajanlar kendiliğinden çalışmaz.** Her ajanın ayrı ön koşulu, ayrı RBAC gereksinimi ve ayrı devreye alma adımı vardır. Bazılarında yapılandırma eksikse ajan sessizce hiçbir uyarıyı işlemez.
4. **Türkçe, model dili değil yalnızca arayüz dilidir.** Prompt yazımı ve yanıt üretimi sekiz dilde desteklenir ve Türkçe bu sekiz dilin içinde değildir. Analist ekiplerinin prompt dili İngilizce olarak planlanmalıdır.
5. **Veri yerleşimi ayrı bir değerlendirme başlığıdır.** Security Copilot tarafından erişilen Microsoft 365 verisi, erişimden önceki EU Data Boundary taahhütlerinden bağımsız olarak Security Copilot'ın kendi veri işleme koşullarına tabi olur. KVKK/GDPR değerlendirmesi bu farkı dikkate almalıdır.

> **Yönetici için tek cümlelik sonuç**
>
> Microsoft 365 E5 sahibi bir kurum için Security Copilot'ın ek lisans maliyeti yoktur; asıl maliyet kalemi devreye alma disiplini, rol tasarımı ve SCU tüketiminin ölçülerek yönetilmesidir. Doğru kurgulandığında ilk 30 günde ölçülebilir değer üreten üç senaryo mevcuttur: kimlik avı triyajı, Koşullu Erişim politika optimizasyonu ve olay özetleme.

2. Kapsam, Yöntem ve Doğrulama

Belgenin kapsamı

- Microsoft 365 E5 / E7 lisansı ile Security Copilot kullanım modeli ve hak edilen kapasite.
- Onboarding: uygunluk doğrulaması, otomatik provizyon davranışı, rol/yetki tasarımı, kontrol listesi.
- SCU kavramı, hesaplama formülü, dokümante edilmiş tüketim referansları ve örnek kapasite planı.
- Defender, Entra, Intune ve Purview üzerinde uygulanabilir örnek kullanım senaryoları ve ön koşulları.
- Güvenlik uzmanı gözüyle yapılan doğrulama: sahada sık karşılaşılan yanlış varsayımlar ve düzeltmeleri.

Kapsam dışı

- Microsoft Sentinel data lake işlem/depolama maliyetleri ve Sentinel mimarisi tasarımı.
- Partner (üçüncü taraf) ajanlarının lisans ve ticari koşulları.
- Kurum özelinde ölçülmüş gerçek SCU tüketim verisi. Belgedeki tüketim değerleri, Microsoft dokümantasyonundaki örnek değerlerdir; kurumun kendi ölçümü esastır.
- ABD kamu bulutları (GCC, GCC High, DoD, Azure Government). Security Copilot bu bulutlar için tasarlanmamıştır; belge ticari bulut varsayımıyla yazılmıştır.

Yöntem ve doğrulama

Belgedeki her teknik iddia Microsoft Learn resmi dokümantasyonundan doğrulanmıştır. Kaynak listesi Ek B'de verilmiştir. Doğrulama tarihi 13 Ağustos 2026'dır. Security Copilot ayda bir güncellenen bir üründür; kritik kararlar öncesinde "What's new in Microsoft Security Copilot" sayfasının tekrar kontrol edilmesi önerilir.

> **İddia disiplini notu**
>
> Fiyat bilgileri hızlı değişen veridir. Bu belgede yalnızca Microsoft dokümantasyonunda açıkça yer alan tek bir fiyat referansı kullanılmıştır (dahil kapasite aşımı için SCU başına 6 USD kullandıkça-öde). Provisioned SCU birim fiyatı için resmî fiyatlandırma sayfası esas alınmalı, teklif öncesi teyit edilmelidir.

3. Security Copilot ve Microsoft 365 E5 İlişkisi

Microsoft Security Copilot, güvenlik ve BT ekiplerinin tehditlere yanıt vermesini, sinyalleri işlemesini ve risk maruziyetini değerlendirmesini hızlandıran üretken yapay zeka tabanlı bir güvenlik ürünüdür. Microsoft 365 E5/E7 tarafında ürünün konumu 2025 sonunda değişmiştir: Security Copilot artık ayrı satın alınması zorunlu bir ürün olmaktan çıkmış, uygun E5 ve E7 müşterileri için lisansa dahil hale gelmiştir.

Lisans modelleri: Inclusion ve Provisioned

Bugün iki farklı kapasite modeli bir arada mevcuttur. Hangi modelde olduğunuz, onboarding adımlarınızı ve maliyet yapınızı doğrudan belirler.

Kriter	Inclusion modeli (M365 E5 / E7)	Provisioned modeli (E5/E7 dışı)
Kapasite kaynağı	Aylık dahil SCU havuzu (Default Security Copilot Capacity)	Önceden provizyonlanan saatlik SCU + isteğe bağlı overage
Hak ediş	Her 1.000 ücretli kullanıcı lisansı için ayda 400 SCU; tavan ayda 10.000 SCU	En az 1, en fazla 100 provisioned SCU; overage 0–999
Faturalama	Ek ücret yok. Arayüzdeki maliyet değerleri yalnızca bilgilendirme amaçlıdır	Provisioned saatlik, overage tüketildiği kadar (ondalık hassasiyetle)
Yenilenme	Aylık sıfırlanır, kullanılmayan SCU devretmez	Her tam saat başında yenilenir, saat sonunda devretmez
Azure kurulumu	Gerekmez; sıfır tıklama ile provizyonlanır	Azure aboneliği ve kaynak grubu üzerinde kapasite oluşturulması gerekir
Kapasite değiştirme	Varsayılan kapasite değiştirilemez, tenant genelinde paylaşılır	Azure veya Security Copilot portalından artırılıp azaltılabilir

> **Kritik ayrım**
>
> Inclusion modelinde "saatlik provizyon" kavramı yoktur. Provisioned modelde 5 SCU provizyonlayan bir müşteri, o saat içinde 3,5 SCU tüketse bile 5 SCU üzerinden faturalanır. Inclusion modelinde ise aynı senaryoda aylık havuzdan yalnızca gerçekleşen 3,5 SCU düşülür. Bu fark, kapasite planlamasının mantığını tamamen değiştirir.

Mevcut Security Copilot müşterileri için not: E5 kapsamına girmiş olsanız bile daha önce provizyonladığınız kapasiteyi silmemeniz önerilir. Microsoft, ürünü kesintisiz kullanabilmek adına mevcut kapasitenin korunmasını tavsiye etmektedir.

Deneyimler: Standalone, Embedded ve Ajanlar

Security Copilot üç farklı yüzeyde kullanılır. Kullanıcı deneyimi ve SCU tüketimi bu yüzeylere göre farklılaşır; kullanım senaryosu tasarımında doğru yüzeyi seçmek önemlidir.

Standalone deneyim

securitycopilot.microsoft.com adresinden erişilen bağımsız portaldır. Serbest prompt, promptbook çalıştırma, oturum paylaşımı, ajan kütüphanesi ve kullanım panosu bu yüzeyde bulunur. Yeni onboard olan E5/E7 müşterilerinde ajan öncelikli (agents-first) bir açılış deneyimi görülebilir; bu durumda sohbet oturumu "All history" bölümünden başlatılır.

Embedded (gömülü) deneyim

Security Copilot'ın diğer Microsoft güvenlik ürünlerinin içinden kullanılmasıdır. Analistin araç değiştirmeden çalışmasını sağladığı için benimsenmesi en yüksek yüzeydir.

Ürün	Gömülü yetenekler (seçilmiş)
Microsoft Defender XDR	Olay özetleme, kılavuzlu yanıt, olay raporu oluşturma, betik/kod analizi, dosya analizi, cihaz ve kimlik özeti, doğal dilden KQL sorgusu üretme
Microsoft Entra	Riskli kullanıcı araştırması, riskli uygulama araştırması, olay araştırması, yaşam döngüsü iş akışlarının yönetimi
Microsoft Intune	Cihaz sorgulama (device query), politika ve ayar yönetimi, cihaz sorun giderme
Microsoft Purview	DLP uyarısı araştırma, insider risk etkinlikleri, iletişim uyumluluğu mesaj özeti, eDiscovery mesaj özeti
Microsoft Sentinel	Sentinel olaylarının özetlenmesi
Defender for Cloud / Azure Firewall / Defender TI	Öneri özetleme ve düzeltme, IDPS imza zenginleştirme, tehdit istihbaratı sorgulama

Gömülü deneyimlerde Copilot panelini kapatmak SCU tüketimini durdurmaz; örneğin Defender XDR olay özeti panel kapalıyken de arka planda üretilmeye devam eder. Bu, tüketim planlamasında dikkate alınması gereken bir davranıştır.

Ajanlar (agents)

Ajanlar, yönetici tarafından tanımlanan tetikleyici, kimlik ve izinler çerçevesinde otonom çalışan bileşenlerdir. Microsoft 365 E5/E7 inclusion kapsamında Defender, Entra, Intune ve Purview ajanları ile geliştirici araçları (Agent Builder, MCP ve Graph API üzerinden özel ajan geliştirme) yer alır. Partner ajanlarının SCU maliyeti de şimdilik dahildir; ancak partner ajanının kendi lisansı Security Store üzerinden ayrıca ücretlendirilebilir.

Önemli: Ajanlar otomatik olarak etkinleştirilmez. Her ajanın ilgili ürün konsolunda ayrıca kurulması, kimliğinin ve izinlerinin yapılandırılması gerekir.

Inclusion kapsamı dışında kalanlar

E5/E7 kapsamındaki dahil kapasite, "çekirdek Security Copilot değeri" ile sınırlıdır. Aşağıdaki kalemler ayrı maliyet doğurur ve teklif/bütçe çalışmasında ayrıca ele alınmalıdır.

- Microsoft Sentinel data lake işlem (compute) ve depolama maliyetleri.
- Microsoft Purview tarafındaki ajan tabanlı olmayan Data Security Investigations deneyimi.
- Security Copilot ile birlikte kullanılan Azure Logic Apps çalıştırma ücretleri.
- Security Store üzerinden satın alınan partner ajanlarının lisans bedelleri.
- Bazı ajanların ön koşulu olan ve Microsoft 365 E5/E7 kapsamı dışında kalan ürünler.

Bir açıklama gerektiren nokta: Microsoft Sentinel kullanan ancak Microsoft 365 E5/E7 lisansı olmayan müşteriler inclusion kapsamına girmez. Buna karşılık E5/E7 sahibi ve aynı zamanda Sentinel kullanan müşteriler, dahil SCU tahsisatlarını Sentinel senaryolarında da kullanabilir.

4. Onboarding: Adım Adım Devreye Alma

Bu bölüm, Security Copilot'ın sıfırdan devreye alınmasını tıklama düzeyinde anlatır. Akış, kurumun lisans durumuna göre ikiye ayrılır: Microsoft 365 E5/E7 sahibi kurumlar Akış A'yı, diğerleri Akış B'yi izler. Yanlış akıştan başlamak gereksiz Azure kaynağı ve gereksiz maliyet doğurur; bu nedenle her iki akış da aynı doğrulama adımıyla başlar.

Portal ve erişim adresleri

Onboarding boyunca kullanılacak adreslerin tamamı aşağıdadır. Tüm portallara aynı kurumsal hesapla, uygun rol atanmış olarak giriş yapılır.

Amaç	Adres
Security Copilot bağımsız portalı (ana çalışma alanı)	https://securitycopilot.microsoft.com
SCU kapasite hesaplayıcısı (Cost Estimator)	https://securitycopilot.microsoft.com/calculator
Microsoft 365 yönetim merkezi (Message Center bildirimi)	https://admin.microsoft.com
Azure portalı (yalnızca manuel SCU provizyonu için)	https://portal.azure.com
Microsoft Defender portalı (SOC senaryoları ve ajanları)	https://security.microsoft.com
Microsoft Entra yönetim merkezi (kimlik senaryoları ve ajanları)	https://entra.microsoft.com
Microsoft Intune yönetim merkezi (uç nokta ajanları)	https://intune.microsoft.com
Microsoft Purview portalı (veri güvenliği ajanları)	https://purview.microsoft.com
Microsoft Security Store (partner ajanları)	https://securitystore.microsoft.com

> **Giriş yaparken dikkat**
>
> Birden fazla tenant'a erişimi olan kullanıcılar (MSSP, danışman, çoklu tenant yapıları) Security Copilot portalında sağ üstteki tenant değiştirme menüsünü kullanmalıdır. Yanlış tenant'ta yapılan yapılandırma sessizce doğru görünür ancak hedef tenant'ı etkilemez. Aktif tenant, adres satırındaki tenantId parametresinden de doğrulanabilir.

Akış A — Microsoft 365 E5 / E7 sahibi kurumlar

Bu akışta Azure tarafında hiçbir işlem yapılmaz. Microsoft, uygun ve etkinleştirilmiş tenant'lar için kapasiteyi ve çalışma alanını otomatik oluşturur. Yapılacak iş, otomatik gelen yapılandırmayı doğrulamak ve kurumsal politikaya göre ayarlamaktır.

A1. Uygunluk ve etkinleştirmenin doğrulanması

Lisansa sahip olmak tek başına erişim vermez; tenant'ın kademeli dağıtım kapsamına alınmış olması gerekir. Doğrulama iki yoldan yapılır:

1. **https://admin.microsoft.com** adresine girin, sol menüden **Health > Message center** bölümünü açın ve Security Copilot ile ilgili duyuruyu arayın. Bu bildirimi Global Administrator, Message Center Reader, Security Admin, Purview Compliance Admin ve Intune Admin rolleri alır.

2. Alternatif olarak **https://securitycopilot.microsoft.com** adresine giriş yapın. Tenant etkinleştirilmişse portal açılır ve ürün içi bilgilendirme banner'ı görünür. Defender, Entra, Intune veya Purview portallarında da aynı banner görüntülenir.

> **Bu adım atlanırsa**
>
> En pahalı hata burada yapılır: "E5'imiz var, o zaman açıktır" varsayımıyla doğrudan Azure portalına gidip SCU kapasitesi oluşturmak. Bu, dahil kapasiteye ek olarak faturalandırılan ayrı bir provisioned kapasite yaratır ve kapasite bir ortama bağlanmamış olsa bile faturalama anında başlar.

A2. Portala ilk giriş ve açılış deneyiminin tanınması

Adres: **https://securitycopilot.microsoft.com**

İlk girişte iki farklı açılış ekranından biri karşılaşır. Hangisiyle karşılaştığınız, sohbet oturumunu nereden başlatacağınızı belirler:

- Ajan öncelikli (agents-first) deneyim: Yeni onboard olan E5/E7 tenant'larında görülür. Ana sayfa doğrudan **Agents** alanıdır ve genel sohbet çubuğu ana sayfada bulunmaz. Sohbet başlatmak için sol menüden **All history > New session** izlenir.
- Sohbet öncelikli (chat-first) deneyim: Mevcut müşterilerde görülür. Ana sayfa doğrudan prompt çubuğuyla açılır; **Agents** alanına sol menüden erişilir.

A3. Sahip ayarlarının gözden geçirilmesi

Yol: Security Copilot portalı > sol üstteki **ana menü (hamburger) simgesi** > **Owner > Owner settings**

Bu sayfa yalnızca Security Copilot owner rolüne sahip kullanıcılara görünür. Otomatik provizyonla gelen varsayılanlar burada doğrulanır ve kurumsal politikaya göre ayarlanır:

Ayar	Otomatik gelen varsayılan	Yapılacak
Manage capacity	Default Security Copilot Capacity atanmıştır; değiştirilemez ve tenant genelinde paylaşılır	Kapasitenin bağlı olduğunu doğrulayın. Arayüzdeki maliyet değerleri yalnızca bilgilendirme amaçlıdır, fatura oluşturmaz
Müşteri verisi saklama konumu	Microsoft Entra coğrafyanız; tenant'ta M365 geo override varsa o eşlenir	Konumu görüntüleyip kayıt altına alın. Çalışma alanı oluşturulduktan sonra değiştirilemez
Prompt değerlendirme konumu	Veri saklama konumu AB ise AB; değilse yük ve GPU müsaitliğine göre küresel	Uyum gereksinimi varsa konumu bilinçli seçin
Help improve Copilot (iki veri paylaşımı ayarı)	Otomatik provizyonda her ikisi de kapalı (Off)	Kurumsal politikaya göre teyit edin ve kararı gerekçesiyle belgeleyin
M365 servis verilerine erişim	Açık (On)	Purview verisinin işlenmesini istemiyorsanız kapatın; kapatmak Purview senaryolarını devre dışı bırakır
Logging audit data in Microsoft Purview	Yönetici ve kullanıcı eylemlerinin Purview'da denetim kaydına yazılması	Etkinleştirin. Purview kullanılmıyorsa ücretsiz sınırlı deneyimin sağlanması gerekir; kayıtlar genelde 24 saat içinde görünür
Manage who can upload files	Dosya yükleme izni	Dosya yüklemenin kimlere açık olacağını karara bağlayın (hiç kimse / contributor ve owner)

A4. Rol atamalarının yapılandırılması

Yol: **ana menü > Owner > Role assignment**. Kullanıcı veya grup eklemek için **Add members** seçilir, ad yazılarak kişi/grup bulunur, **Copilot owner** veya **Copilot contributor** rolü seçilip **Add** ile kaydedilir.

- Rolleri tek tek kullanıcılara değil, rol atanabilir (role-assignable) Entra güvenlik gruplarına atayın — Security Copilot yalnızca rol atanabilir grupları destekler.

- Contributor tarafında "Everyone" grubu atanmışsa kaldırın ve yerine "Recommended Microsoft Security roles" grubunu ekleyin. Everyone grubu bir kez kaldırıldıktan sonra tekrar atanamaz.
- Yalnızca Copilot erişimi için kullanıcıya Security Administrator gibi ayrıcalıklı bir rol vermeyin; güvenlik grubu oluşturup grubu Copilot rolüne ekleyin.
- Sahipsiz kalmayı önlemek için Security Copilot her zaman en az iki owner tutar; bu iki owner kaldırılamaz.

A5. Eklentilerin (plugin) yapılandırılması

Yol: Sohbet ekranında prompt çubuğunun yanındaki **Sources** düğmesi > **Manage sources**. Kurum geneli kısıtlamalar için **ana menü > Owner > Plugin settings** kullanılır.

Eklenti ayarları çalışma alanı veya kurum düzeyinde yapılandırılabilir; bu, her kullanıcı için ayrı kurulum ihtiyacını ortadan kaldırır. Dişli simgesi veya "Set up" düğmesi taşıyan önceden yüklü eklentiler (örneğin Microsoft Sentinel) kullanıcı başına ayrıca yapılandırılır.

A6. Dil tercihinin ayarlanması

Yol: **ana menü > Settings > Preferences** > tercih edilen dil seçilir.

- Türkçe yalnızca ürün arayüzü dili olarak seçilebilir. Prompt yazımı ve yanıt üretimi sekiz dilde desteklenir (İngilizce, Almanca, Japonca, İspanyolca, Fransızca, İtalyanca, Portekizce, Çince) ve Türkçe bu listede yoktur.
- Desteklenmeyen bir dilde yazılan prompt hata döndürür. Bu nedenle arayüz Türkçe seçilse dahi prompt dili İngilizce olarak standartlaştırılmalıdır.
- Tercihlerde bir dil seçili olsa bile, prompt farklı bir desteklenen dilde yazılırsa yanıt promptun dilinde döner; prompt içinde açıkça istenen dil her ikisini de geçersiz kılar.

Akış B — Microsoft 365 E5 / E7 dışı kurumlar

Bu akışta kapasite manuel olarak provizyonlanır. İki yol vardır; Microsoft, Security Copilot portalı üzerinden ilerlemeyi önermektedir. Her iki yolda da Azure abonelik veya kaynak grubu düzeyinde Contributor ya da Owner rolü ve tenant tarafında en az Security Administrator rolü gereklidir.

B1. Yöntem 1 (önerilen) — Security Copilot portalı üzerinden

1. **https://securitycopilot.microsoft.com** adresine giriş yapın; ilk çalıştırma (first run) sihirbazı açılır.
2. Çalışma alanı adı girin. Ad, Azure kaynak adlandırma kurallarına uymalıdır. **Continue** ile ilerleyin.
3. Güvenlik kapasitesini kurun: Azure aboneliğini seçin, kapasiteyi bir kaynak grubuyla ilişkilendirin, kapasiteye ad verin, prompt değerlendirme konumunu seçin ve SCU sayısı ile overage miktarını girin. SCU saatlik provizyonlanır ve tahmini aylık maliyet ekranda gösterilir.
4. Veri paylaşımı seçeneklerini belirleyin ve **Continue** ile ilerleyin.
5. Koşulları okuyup onaylayın. Arka planda Azure kaynağının oluşturulması birkaç dakika sürer.
6. Security Copilot'ın yönetici eylemlerini, kullanıcı eylemlerini ve sistem yanıtlarını yakalayıp saklamasını isteyip istemediğinizi seçin.
7. Security Copilot'a erişebilecek rolleri gözden geçirin; önerilen owner rollerini seçebilir veya contributor ekleyebilirsiniz.
8. Onay sayfasında **Finish** ile kurulumu tamamlayın.

B2. Yöntem 2 — Azure portalı üzerinden

1. **https://portal.azure.com** adresine giriş yapın.
2. Hizmet arama kutusuna **Security compute** yazın ve **Microsoft Security compute capacities** hizmetini seçin.
3. **Resource groups** bölümünü seçin.

4. **Plan** altında **Microsoft Security Copilot** seçeneğini işaretleyin ve **Create** düğmesine basın.
5. Abonelik ve kaynak grubunu seçin, kapasiteye ad verin, prompt değerlendirme konumunu ve SCU sayısını belirleyin. İsterseniz overage birim sayısını da girin. Veri her zaman kendi coğrafyanızda saklanır.
6. Koşulları okuduğunuzu onaylayın ve **Review + create** ile devam edin.
7. Bilgileri doğrulayıp **Create** düğmesine basın.
8. **Finish setup in the Security Copilot portal** bağlantısıyla kurulumu Security Copilot portalında tamamlayın.

Faturalama uyarısı

Azure tarafında kapasite oluşturulduğu anda faturalama başlar — SCU bir ortama bağlanmamış olsa bile. Ayrıca faturalama saatlik bloklar hâlinde hesaplanır: aynı saat içinde kapasite açıp kapatıp tekrar açmak, o saat için iki birim ücretlendirme doğurur. Kapasite değişikliklerini saat başında yapmak en verimli yaklaşımdır ve değişikliklerin etkili olması 30 dakikayı bulabilir.

- Asgari 1, azami 100 provisioned SCU satın alınabilir. Overage 0–999 aralığında ayarlanabilir veya sınırsız bırakılabilir.
- Microsoft, tanışma amaçlı ilk keşif için 3 provisioned SCU ve sınırsız overage yapılandırmasını önermektedir.
- Kapasite ihtiyacını tahmin etmek için **https://securitycopilot.microsoft.com/calculator** adresindeki hesaplayıcı kullanılabilir (Azure hesabı gerekir).

Rol ve yetkilendirme (RBAC) modeli

Security Copilot rolleri Microsoft Entra rolleri değildir. Yalnızca platform yeteneklerine erişimi kontrol ederler ve tek başlarına hiçbir güvenlik verisine erişim vermezler. Bu ayrımın doğru anlaşılması hem güvenlik hem de kullanıcı deneyimi açısından belirleyicidir.

Katman	Ne kontrol eder	Nerede yönetilir
Security Copilot RBAC	Platforma erişim, ayar yönetimi, kapasite yönetimi, kullanım panosu, eklenti yönetimi	Security Copilot portalı > Owner > Role assignment
Microsoft Entra RBAC	Microsoft ürün portföyüne ve güvenlik verisine erişim	entra.microsoft.com
Azure RBAC	Azure kaynakları: SCU kapasitesi, Sentinel çalışma alanları	portal.azure.com
Servis bazlı RBAC	Defender XDR Unified RBAC, Intune RBAC, Purview rolleri, Sentinel rolleri	İlgili ürün konsolu

Temel ilke: Security Copilot kullanıcı adına (on-behalf-of) çalışır ve kullanıcının sahip olduğu erişimin ötesine geçmez. Bir analiste Copilot contributor rolü vermek, ona Sentinel veya Intune verisine erişim vermez; bunun için ilgili servis rolü (örneğin Microsoft Sentinel Reader, Endpoint Security Manager) ayrıca atanmalıdır. Eksik servis rolü, "Copilot çalışmıyor" şikayetinin en yaygın nedenidir.

Rol atama yaklaşımları

Yaklaşım	Avantaj	Zayıf yön
Recommended Microsoft Security roles (varsayılan)	Güvenlik verisine zaten erişimi olan kullanıcılara hızlı ve kontrollü platform erişimi	Ya hep ya hiç: gruptaki tek bir rolü istemiyorsanız grubun tamamını kaldırmanız gerekir
Everyone	Provizyonu basitleştirir	Güvenlik verisine erişimi olmayan kullanıcılar için anlamsız bir deneyim yaratır. Kaldırıldıktan sonra tekrar atanamaz
Custom (güvenlik grupları)	Erişim üzerinde tam kontrol; en az ayrıcalık ilkesine uygun	Daha fazla yönetim eforu gerektirir

- **Paylaşılan oturum riski:** Bir oturum paylaşıldığında alıcı, oturumda kullanılan eklentinin verisine erişim yetkisine sahip olmasa bile tüm sonuçları görebilir ve dışa aktarabilir. Oturum paylaşımı bir veri paylaşımı kararıdır ve süreç olarak ele alınmalıdır.

Ajan devreye alma akışı

Her iki akışta da ortak olan adımdır. Ajanlar otomatik etkinleştirilmez; her ajan ayrıca kurulur. Kurulum, ajanın Microsoft tarafından mı yoksa partner tarafından mı geliştirildiğine göre farklılaşır.

Microsoft tarafından geliştirilen ajanlar

1. **https://securitycopilot.microsoft.com** adresine giriş yapın.
2. Sol gezinme bölmesinden **Agents** seçin; ajan kütüphanesi açılır.
3. Kullanmak istediğiniz ajanı seçip **Set up** ile ajan detay sayfasına geçin.
4. Ajan için kimlik seçin: **ajan kimliği oluşturma** (Microsoft Entra Agent ID — önerilen) veya **mevcut bir kullanıcı hesabına bağlama**. Kullanıcı hesabı seçilirse ajan o kullanıcının tüm erişimini devralır.
5. Kurulum talimatlarını izleyin ve gerekli giriş parametrelerini girin. Parametreler ajana göre değişir: tetikleyici (trigger), izinler, kimlik, eklentiler, gerekli ürünler ve rol tabanlı erişim.
6. Kurulum tamamlandığında ajan sayfasına yönlendirilirsiniz. **Run** ile ilk çalıştırmayı yapıp çıktıyı doğrulayın.

Partner tarafından geliştirilen ajanlar

Microsoft ürünlerinden veri erişen partner ajanlarında, kurulumdan önce tenant içinde bir Global Administrator onayı gerekir.

1. Owner veya contributor kurulumu başlattığında, Global Administrator onayı gerektiğini belirten bir banner görünür ve **Set up** düğmesi devre dışı kalır.
2. **Copy Link** ile bağlantı kopyalanır ve Global Administrator ile paylaşılır.
3. Global Administrator bağlantıyı açar (veya **Active agents > Set up** yolunu izler), gerekli izinleri inceler ve **Start approval** ile onay sürecini başlatır.
4. Onay tamamlandıktan sonra owner/contributor kurulumu bitirir: mevcut bir kullanıcı hesabı atanır, giriş yapılır ve **Next** ile parametreler girilir.

- Ajanı geçici olarak durdurmak için ajan sayfasında **Pause**; elle çalıştırmak için **One time** seçeneği kullanılır. Tetikleyici açıksa ajan zamanlandığı gibi otomatik çalışır.
- Ajan çıktısına geri bildirim vermek için sonuç bölmesindeki geri bildirim düğmesi kullanılır; geri bildirim ajanın hafızasında saklanır. Hafızayı yönetmek için ajan sayfasında **… > Manage memory** izlenir ve gerekirse **Reject feedback** ile kayıt kaldırılır.

- Ek ajanlar için **Browse more agents** veya menüden **Security Store** seçilir.

Ajan bazlı ön koşullar ve kurulum yolları

Aşağıdaki tablo, E5 kapsamında en sık devreye alınan ajanların nereden kurulduğunu ve kurulum öncesinde tamamlanması gereken yapılandırmaları özetler. Ön koşulların eksik olması, ajanın hata vermeden hiçbir iş üretmemesine yol açan en yaygın nedendir.

Ajan	Kurulum yolu	Kurulum öncesi tamamlanacaklar
Phishing Triage / Security Alert Triage Agent	security.microsoft.com veya Security Copilot > Agents	Defender for Office 365 için Unified RBAC etkinleştirilir (Defender XDR ayarlarından iş yükü aktive edilir); "Monitor reported messages in Outlook" kullanıcı bildirim ayarı açılır ve bildirim hedefi seçilir; "Email reported by user as malware or phish" uyarı politikası açılır; "Auto-Resolve – Email reported by user as malware or phish" uyarı ayarlama kuralı ve bu uyarıyı çözen özel kurallar devre dışı bırakılır
Conditional Access Optimization Agent	entra.microsoft.com > Copilot / ajan sayfası	İlk etkinleştirme için Security Administrator rolü; kullanım için en az Conditional Access Administrator; ajan kimliği için ajan ayarlarında "Create agent identity" seçilir (bu geçiş tek yönlüdür); kademeli dağıtım planı için tenant'ta Koşullu Erişim politikalarında kullanılan en az beş grup bulunmalıdır
Vulnerability Remediation Agent	intune.microsoft.com > Agents > Vulnerability Remediation Agent > Overview > Set up Agent > Start agent	Intune ve Defender eklentileri etkin olmalı; kurulum sırasında oluşan ajan kullanıcısına izinler ajan akışının dışında Entra ve Defender konsollarından delege edilmeli (Intune okuma izinleri + Defender tarafında Unified RBAC Security Reader eşdeğeri); "Run Readiness Check" ile izinler çalıştırmadan önce doğrulanmalı
Purview triyaj ajanları (DLP ve Insider Risk)	purview.microsoft.com > Agents > Explore agents > View agent > Edit agent	İlgili çözüm lisansı ve rolleri; DLP politikalarının aktif modda olması (simülasyon modundaki politikaların uyarıları triyaj edilmez); cihaz uyarıları için dosya etkinliklerinde kanıt toplama etkinleştirilmeli; tetikleyicide uyarı zaman aralığı seçilmeli. SCU tüketimi aynı sayfadaki "Usage monitoring" bölümünden izlenir
Threat Intelligence Briefing Agent	Security Copilot > Agents	Tehdit istihbaratı eklentilerinin etkin olması; varsayılan olarak yedi günlük zamanlanmış çalışma tetikleyicisi yapılandırılır

Kullanımın izlemeye alınması

Yol: **ana menü > Owner > Usage monitoring**. Aynı ekrana Owner settings üzerinden de erişilebilir.

- Pano 90 güne kadar veri sunar ve tüketimi oturum düzeyinde gösterir: oturum kimliği, tarih, tüketilen SCU, oturumu başlatan kullanıcı, kategori (prompt/promptbook/agent/primitive), tür (manuel/otomatik), kullanılan yüzey ve eklenti.
- Veriler **Export** düğmesiyle Excel olarak dışa aktarılabilir. Aylık kapasite gözden geçirme toplantısı bu ihracata dayandırılmalıdır.
- Filtreler yalnızca tabloya uygulanır, çubuk grafiğe uygulanmaz; rapor hazırlarken bu ayrım gözden kaçırılmamalıdır.
- Provisioned modelde SCU sayısı **Owner settings > Security compute units > Change** veya kullanım panosundaki **Change units** ile güncellenir. Bu işlem için Azure kapasite owner/contributor rolü ve Security Copilot owner rolü birlikte gerekir.

Onboarding kontrol listesi

#	Adım	Nerede	Doğrulama
1	E5/E7 lisans durumu ve tenant etkinleştirmesi doğrulanır	admin.microsoft.com > Message center	Bildirim veya ürün içi banner görülür
2	Security Copilot portalına ilk giriş yapılır, açılış deneyimi tespit edilir	securitycopilot.microsoft.com	Portal açılır; agents-first / chat-first ayrımı not edilir

#	Adım	Nerede	Doğrulama
3	Varsayılan çalışma alanı ve kapasite doğrulanır	Owner > Owner settings > Manage capacity	Default Security Copilot Capacity bağlı görünür
4	Veri saklama ve prompt değerlendirme konumu kayıt altına alınır	Owner > Owner settings	Ekran kaydı uyum dosyasına eklenir
5	Veri paylaşımı tercihleri kurumsal politikaya göre teyit edilir	Owner settings > Help improve Copilot	İki ayarın durumu belgelenir
6	M365 servis verisi (Purview) erişimi karara bağlanır	Owner settings	Karar gerekçesiyle kayıt altına alınır
7	Purview denetim kaydı etkinleştirilir	Owner settings > Logging audit data	Kayıtlar 24 saat içinde Purview'da görünür
8	Dosya yükleme izni karara bağlanır	Owner settings > Manage who can upload files	Seçim belgelenir
9	Rol atamaları düzenlenir; Everyone kaldırılır	Owner > Role assignment	Rol atanabilir güvenlik grupları kullanılır
10	Copilot erişimi Koşullu Erişim politikasıyla korunur	entra.microsoft.com	Politika raporlama modunda test edilip devreye alınır
11	Eklentiler çalışma alanı düzeyinde yapılandırılır	Sources / Owner > Plugin settings	Kullanıcı başına kurulum ihtiyacı kalmaz
12	Dil tercihi ayarlanır, prompt dili İngilizce standartlaştırılır	Settings > Preferences	Analist ekibine duyurulur
13	Pilot ajan seçilir, ön koşulları tamamlanır, kimliği yapılandırılır	Agents > Set up	İlk çalıştırma çıktı üretir
14	Kullanım panosu izlemeye alınır	Owner > Usage monitoring	İlk 30 gün haftalık gözden geçirme yapılır
15	Ajan yönetim denetimi doğrulanır	Purview Unified Audit Log	Ajan oluşturma/güncelleme/silme olayları görünür

5. SCU Hesaplaması ve Kapasite Yönetimi

SCU nedir, neyi tüketir

Security Compute Unit (SCU), Security Copilot iş yüklerini çalıştırmak için gereken hesaplama kapasitesinin birimidir. Aşağıdaki beş senaryoda SCU tüketilir:

- Security Copilot bağımsız (standalone) portalının kullanılması.
- Gömülü (embedded) Security Copilot deneyimlerinin çalıştırılması.
- Microsoft tarafından geliştirilen ajanların çağrılması.
- Partner tarafından geliştirilen ajanların çağrılması.
- Diğer Security Copilot özellik ve yeteneklerinin çalıştırılması.

Sık gözden kaçan iki kural

Genel kullanıma açık (GA) ve genel önizleme (public preview) aşamasındaki yetenekler SCU tüketir ve ücretlendirilir. Yalnızca özel önizleme (private preview) yetenekleri ücretlendirilmez.

SCU'lar workspace'ler arasında paylaşılmaz. Workspace A kendi kapasitesini tükettiğinde Workspace B'nin kapasitesini kullanamaz. Çok bölgeli veya çok ekipli tasarımlarda bu kısıt planlamayı doğrudan etkiler.

E5 dahil kapasite formülü

Microsoft 365 E5 ve E7 müşterileri için hak edilen aylık kapasite doğrusal bir formülle hesaplanır ve 1.000 lisanstan az kullanıcıya sahip kurumlar için de orantılı olarak uygulanır.

Formül

Aylık dahil SCU = (Ücretli M365 E5/E7 kullanıcı lisansı sayısı ÷ 1.000) × 400

Üst sınır: ayda 10.000 SCU. Tahsisat her ay sıfırlanır; kullanılmayan SCU bir sonraki aya devretmez.

Ücretli E5/E7 kullanıcı lisansı	Aylık dahil SCU	Not
250	100	Orantılı uygulanır; asgari lisans taahhüdü yoktur
400	160	Microsoft dokümantasyonundaki örnek
1.000	400	Referans oran
2.500	1.000	Bu belgedeki örnek kapasite planının temeli
4.000	1.600	Microsoft dokümantasyonundaki örnek
10.000	4.000	
25.000	10.000	Tavana ulaşılan lisans sayısı
50.000	10.000	Tavan nedeniyle artış durur; aşım planlaması gerekir

Planlama sonucu: 25.000 ücretli lisanstan sonra dahil kapasite artmaz. Bu ölçekteki kurumlarda SCU tüketiminin ölçülmesi ve önceliklendirilmesi bir tercih değil, zorunluluktur.

Dokümante edilmiş tüketim referansları

Microsoft, SCU tüketiminin sabit olmadığını, her prompt ve iş akışının karmaşıklığına göre değiştiğini açıkça belirtmektedir. Aşağıdaki değerler resmî dokümantasyonda geçen örnek değerlerdir; garanti edilen birim maliyet değildir. Kurumun kendi ölçümü esas alınmalıdır.

İşlem	Dokümante edilmiş örnek tüketim	Kaynak bağlamı
Tek prompt çalıştırma	3,0 SCU	Faturalama örneği senaryosu
Defender olay özetleme (incident summarization)	0,5 SCU	Faturalama örneği senaryosu
Promptbook çalıştırma	3,7 SCU	Faturalama örneği senaryosu
Koşullu Erişim Optimizasyon Ajanı — tek çalışma	Ortalama 1 SCU'dan az	Ajan dokümantasyonu
Koşullu Erişim Ajanı — tarama adımları	0 SCU	Politika taraması, boşluk kontrolü ve önceki öneri gözden geçirmesi tüketmez
Phishing / Alert Triage Ajanı	Dokümante edilmemiş	Uyarı sayısı ve türüne göre değişir; ölçülmelidir
Purview triyaj ajanları	Dokümante edilmemiş	İşlenen uyarı sayısı ve türüne göre değişir

- Tahmin için Microsoft'un SCU kapasite hesaplayıcısı kullanılabilir. Hesaplayıcı, deneyim başına aylık kullanıcı sayısı ile Logic Apps ve promptbook otomasyonlarını girdi alarak saatlik azami SCU ihtiyacını verir.
- Hesaplayıcının gösterdiği en yüksek aylık maliyet, kapasitenin 7/24 kesintisiz kullanıldığı varsayımına dayanır. Gerçekçi bir bütçe için bu üst sınır değil, ölçülen tüketim esas alınmalıdır.

Örnek kapasite planı (2.500 kullanıcı)

Aşağıdaki plan, 2.500 ücretli E5 lisansına sahip ve ayda 1.000 SCU hak eden bir kurum için hazırlanmış bir planlama şablonudur. Yalnızca yukarıdaki dokümante edilmiş örnek değerler kullanılmış, dokümante edilmemiş kalemler açıkça "rezerv" olarak ayrılmıştır.

Kullanım kalemi	Aylık hacim varsayımı	Birim (örnek)	Aylık SCU
Defender olay özetleme	400 olay	0,5	200
Standalone analist promptları	20 analist × 5 prompt	3,0	300
Promptbook çalıştırma	20 çalışma	3,7	74
Koşullu Erişim Optimizasyon Ajanı	Günlük 1 çalışma (30)	≤1,0	30
Kimlik avı triyaj ajanı ve diğer ajanlar	Ölçülecek	Bilinmiyor	250 (rezerv)
TOPLAM (planlanan)			854
DAHİL KAPASİTE			1.000
TAMPON			146 (%14,6)

Bu tabloyu nasıl kullanmalı

Bu bir tahmin şablonudur, taahhüt değildir. Doğru yaklaşım: ilk ay dar kapsamlı bir pilotla başlayın, kullanım panosundan gerçek tüketimi haftalık okuyun, 30. günün sonunda tablodaki birim değerleri

kurumun ölçülmüş değerleriyle değiştirin ve planı yeniden kurun. Microsoft'un önerisi de aynı yöndedir: küçük başla, ölç, kullanıma göre iyileştir.

İzleme, eşik ve aşım davranışı

Security Copilot portalındaki kullanım izleme panosu (Owner settings > Usage monitoring) 90 güne kadar veri sunar ve tüketimi oturum düzeyinde ayrıştırır.

Boyut	Ne gösterir
Session ID / Date / Units used	Oturum kimliği, tarih ve o oturumda tüketilen SCU miktarı
Initiated by	Oturumu başlatan kullanıcı — kişi bazlı tüketim analizi için temel veri
Category	Prompt, Promptbook, Agent veya Primitive (kullanıcı etkileşimi olmadan yapılan çıkarım çağrısı)
Type	Manual Action (kullanıcı tetikli) veya Automated Action (zamanlanmış/otomatik)
Copilot experience	Standalone portal, gömülü deneyim veya Azure Logic Apps
Plugin used	Oturumda kullanılan eklenti — hangi ürünün tüketimi sürüklediğini gösterir

- Veriler Excel olarak dışa aktarılabilir. Aylık kapasite gözden geçirme toplantısı için bu ihracat temel alınmalıdır.
- Filtreler yalnızca tabloya uygulanır, çubuk grafiğe uygulanmaz. Rapor hazırlarken bu ayrım gözden kaçırılmamalıdır.

Kapasite sınırına yaklaşıldığında

- Kullanım sınıra yaklaştığında analistler prompt gönderirken uyarı bildirimi görür; bu bildirim gömülü deneyimlerde de gösterilir.
- Kapasitenin %100'üne ulaşıldığında yeni prompt gönderilemez ve hata mesajı görüntülenir. Provisioned modelde kapasite bir sonraki saatte yenilenir.
- Inclusion modelinde dahil SCU tahsisatının aşılması durumunda kullanım ileride kısıtlanacaktır (throttling). Microsoft, bu seçenek devreye girmeden önce 30 gün önceden bildirim yapacağını ve SCU başına 6 USD kullandıkça-öde ile ölçeklenebileceğini belirtmektedir.

6. Örnek Kullanım Senaryoları

Aşağıdaki senaryolar, Microsoft 365 E5 lisansı ile ek ürün satın almadan devreye alınabilecek, dokümantasyonla doğrulanmış kullanım örnekleridir. Her senaryoda ön koşullar ayrıca belirtilmiştir; E5 kapsamına giren bir ön koşul "E5 ile karşılanır" olarak işaretlenmiştir. Ön koşulların yapılandırılmaması, ajanın hata vermeden hiçbir iş üretmemesine yol açan en yaygın nedendir.

Senaryo 1 — Kullanıcı bildirimli kimlik avı triyajı

Boyut	Açıklama
Kime	SOC Seviye 1 analistleri, e-posta güvenliği ekibi
Yüzey	Microsoft Defender portalı — Phishing Triage Agent / Security Alert Triage Agent
Ön koşullar	Defender for Office 365 Plan 2 (E5 ile karşılanır); Defender for Office 365 için Unified RBAC (URBAC) etkin; "Monitor reported messages in Outlook" kullanıcı bildirim ayarı açık; "Email reported by user as malware or phish" uyarı politikası açık
Kritik yapılandırma	"Auto-Resolve – Email reported by user as malware or phish" yerleşik uyarı ayarlama (alert tuning) kuralı ve bu uyarıyı çözen özel kurallar devre dışı bırakılmalıdır. Ajan, ayarlama kurallarıyla çözülmüş uyarıları triyaj etmez
Nasıl çalışır	Kullanıcı bildirimli e-postalar geldikçe otonom olarak değerlendirilir. E-posta içeriği analizi, dosya ve URL detonasyonu, ekran görüntüsü analizi, tehdit istihbaratı ve veri kaynakları arası gelişmiş av (advanced hunting) birlikte kullanılır
Çıktı	Gerçek tehdit / yanlış alarm sınıflandırması, doğal dilde gerekçe ve görsel karar haritası. Analist geri bildirimi zamanla ajanın davranışını kurumsal bağlama göre iyileştirir
Ölçüm önerisi	Devreye almadan önce 30 günlük manuel triyaj süresini ölçün; ajan sonrası aynı metriği tekrarlayın. Bu, yatırımın geri dönüşünü gösteren en somut veridir

Senaryo 2 — Olay özetleme ve kılavuzlu yanıt

Boyut	Açıklama
Kime	SOC analistleri, vardiya devri yapan ekipler
Yüzey	Microsoft Defender XDR — gömülü Copilot paneli
Ön koşullar	Defender XDR erişimi ve ilgili Unified RBAC rolleri (E5 ile karşılanır)
Nasıl çalışır	Olay açıldığında Copilot paneli otomatik olarak olay özetini üretir; analist kılavuzlu yanıt (guided response) adımlarını takip eder ve olay raporunu tek adımda oluşturur
Çıktı	Olay özeti, önerilen yanıt adımları, paydaşa gönderilebilir olay raporu
Dikkat	Copilot paneli kapatılsa dahi olay özeti arka planda üretilmeye devam eder ve SCU tüketir. Yoğun olay hacmi olan ortamlarda bu kalem tüketimin en büyük bileşeni olabilir
Tüketim referansı	Dokümantasyondaki örnek değer olay başına 0,5 SCU

Senaryo 3 — Doğal dilden KQL üretimi ve tehdit avı

Boyut	Açıklama
Kime	KQL deneyimi sınırlı seviye 1–2 analistler, tehdit avcıları
Yüzey	Defender XDR gelişmiş av (advanced hunting) — Query Assistant; standalone tarafta Threat Hunting Assistant
Ön koşullar	Defender XDR gelişmiş av erişimi (E5 ile karşılanır)
Nasıl çalışır	Analist avlamak istediği davranışı doğal dilde tanımlar; Copilot KQL sorgusunu üretir ve sorgunun mantığını adım adım açıklar

Boyut	Açıklama
Çıktı	Çalıştırılabilir KQL sorgusu ve sorgunun açıklaması. Açıklama özelliği, analistin sorgunun niyetiyle örtüştüğünü doğrulamasını ve zamanla KQL yetkinliği kazanmasını sağlar
Kurumsal değer	Seviye 1 ekibin seviye 2 işlerine erişimini açar; ekip içi bilgi asimetrisini azaltır

Senaryo 4 — Koşullu Erişim politika optimizasyonu

Boyut	Açıklama
Kime	Kimlik yöneticileri, Zero Trust programı sahipleri
Yüzey	Microsoft Entra yönetim merkezi — Conditional Access Optimization Agent
Ön koşullar	En az Microsoft Entra ID P1 (E5 ile karşılanır, E5 P2 içerir); ilk etkinleştirme için Security Administrator rolü; cihaz tabanlı denetimler için Intune lisansı (E5 ile karşılanır); riskli kullanıcı ve riskli oturum açma önerileri için Entra ID P2 (E5 ile karşılanır)
Nasıl çalışır	Ajan son 24 saatte eklenen kullanıcı, uygulama ve ajan kimliklerini tarar; politika kapsamı dışında kalanları ve birleştirilebilecek politika çiftlerini tespit eder. Tarama adımları SCU tüketmez; yalnızca yeni bir öneri üretildiğinde tüketim olur
Çıktı	Rapor-only modda oluşturulmuş yeni politika önerileri veya mevcut politikada değişiklik önerisi: MFA zorunluluğu, cihaz tabanlı denetim, eski kimlik doğrulamanın engellenmesi, device code flow engelleme, riskli kullanıcı ve riskli oturum açma politikaları
Sınırlar	Tek çalışmada en fazla 300 kullanıcı ve 150 uygulama incelenir; politika birleştirmede 40 benzer politika çifti değerlendirilir. Tarama 24 saatlik pencereyle sınırlıdır. Başlatılan çalışma durdurulamaz; öneriler özelleştirilemez veya geçersiz kılınamaz
Kimlik tasarımı	Yeni kurulumlar varsayılan olarak Microsoft Entra Agent ID ile ajan kimliği kullanır. Mevcut kurulumlar kullanıcı bağlamından ajan kimliğine geçebilir; ancak bu geçiş tek yönlüdür, geri dönüş yoktur

Senaryo 5 — Riskli kullanıcı ve uygulama araştırması

Boyut	Açıklama
Kime	Kimlik güvenliği ekibi, SOC
Yüzey	Microsoft Entra yönetim merkezi — gömülü Copilot
Ön koşullar	Senaryoya göre değişir: denetim günlükleri ücretsiz Entra ID ile, sağlama günlükleri 7 gün sonrasında Entra ID P1 ile, kimlik koruma senaryoları P2 ile kullanılabilir (E5 ile karşılanır)
Nasıl çalışır	Yönetici doğal dilde soru sorar: oturum açma sorunlarının nedeni, rol atamalarının analizi, riskli kullanıcının risk gerekçesi, riskli uygulama araştırması. Copilot, Microsoft Graph API üzerinde çok aşamalı akıl yürütme yapar ve kullanılan sorguyu gösterir
Çıktı	Risk gerekçesi özeti, ilgili oturum açma ve denetim kayıtları, önerilen sonraki adımlar
Dikkat	Kullanılan sorgunun görünür olması, yanıtın doğrulanabilirliği açısından önemlidir. Analistin çıktıyı doğrulamadan aksiyon almaması bir süreç kuralı olarak tanımlanmalıdır

Senaryo 6 — Zafiyet düzeltme önceliklendirmesi

Boyut	Açıklama
Kime	Uç nokta yönetimi ve BT operasyon ekipleri
Yüzey	Microsoft Intune yönetim merkezi — Vulnerability Remediation Agent
Ön koşullar	Microsoft Intune Plan 1 (E5 ile karşılanır); Microsoft Defender Vulnerability Management — Defender for Endpoint P2 ile gelir (E5 ile karşılanır) veya bağımsız MDVM; Intune ve Defender eklentileri etkin

Boyut	Açıklama
Roller	Kurulum ve yönetim için Intune Read Only Operator (veya Security Tasks / Mobile apps / Device configurations / Organization okuma izinli özel rol) ve Security Copilot owner. Ajanın çalışması için ajan kullanıcısına Intune okuma izinleri ile Defender tarafında Unified RBAC Security Reader eşdeğeri izinler ayrıca delege edilmelidir
Nasıl çalışır	Ajan Defender verisini kullanarak zafiyetleri izler ve yapay zeka destekli risk değerlendirmesiyle önceliklendirir; Intune yönetim merkezinde adım adım düzeltme rehberliği sunar
Kapsam	Windows platformu ve Intune uygulamaları için değerlendirme ve öneri üretir. Yalnızca genel bulutu destekler
Dikkat	Kurulum sırasında tenant'ta bir ajan kimliği oluşur; izinler ajan akışının dışında Entra ve Defender konsollarından delege edilmelidir. "Run Readiness Check" ile izinlerin doğru delege edildiği çalıştırmadan önce doğrulanmalıdır

Senaryo 7 — DLP uyarı triyajı

Boyut	Açıklama
Kime	Veri güvenliği yöneticileri, uyum ekipleri
Yüzey	Microsoft Purview — Alert Triage Agent in Data Loss Prevention
Ön koşullar	Microsoft Purview DLP lisansı (E5 ile karşılanır); cihaz uyarılarının triyajı için "evidence collection for file activities on devices" etkin olmalıdır
Nasıl çalışır	Uyarılar hassasiyet riski, sızdırma riski ve politika riski üzerinden değerlendirilir; Needs attention / Less urgent / Not categorized kategorilerine ayrılır. Exchange, cihazlar, SharePoint, OneDrive ve Teams kaynaklı uyarılar kapsamdadır
Kritik sınır	Yalnızca aktif moddaki DLP politikalarının uyarıları triyaj edilir; simülasyon modundaki politikaların uyarıları işlenmez. Yalnızca hassas bilgi türü veya eğitilebilir sınıflandırıcı dışındaki koşullara dayanan uyarılar (örneğin yalnızca e-posta konusu eşleşmesi) değerlendirilmez
Geriye dönük kapsam	Yeterli SCU varsa ajan etkinleştirmeden önceki 30 güne kadar üretilmiş uyarılar da incelenebilir; 30 günden eski uyarılar kapsam dışıdır
Süreç kuralı	Ajanın değerlendirmediği uyarılar için manuel analiz süreci korunmalıdır. Ajan, triyaj kapasitesini artırır; triyaj sorumluluğunu ortadan kaldırmaz

Senaryo 8 — Kuruma özel tehdit istihbaratı brifingi

Boyut	Açıklama
Kime	Tehdit istihbaratı analistleri, CISO ve yönetim raporlaması
Yüzey	Security Copilot standalone portalı — Threat Intelligence Briefing Agent
Ön koşullar	Security Copilot erişimi ve ilgili tehdit istihbaratı eklentileri
Nasıl çalışır	Ajan; sektör, coğrafya ve kurumun saldırı yüzeyi gibi nitelikleri kullanarak Defender Threat Intelligence, Defender External Attack Surface Management sinyalleri ve gerçek zamanlı kurum bağlamını ilişkilendirir. Varsayılan olarak yedi günde bir zamanlanmış çalışabilir
Çıktı	Kuruma özgü, dakikalar içinde üretilen tehdit istihbaratı brifingi
Kurumsal değer	Saatler veya günler süren manuel istihbarat derleme ve ilişkilendirme işini yapılandırılmış bir çıktıya dönüştürür; yönetim raporlamasında tekrarlanabilir bir kaynak sağlar

Otomasyon ve entegrasyon seçenekleri

- Promptbook: sırayla çalışan prompt dizileridir; olay müdahalesi ve araştırma gibi tekrar eden adımları şablonlaştırır. Paylaşılan kütüphaneden çalıştırılabilir veya kurum içi promptbook oluşturulup tenant genelinde yayımlanabilir.
- Azure Logic Apps konnektörü: iş akışından Security Copilot prompt'u veya promptbook'u çağırıp sonucu akışa döndürür. Logic Apps çalıştırma ücretleri E5 inclusion kapsamı dışındadır.
- Copilot Studio konnektörü: doğal dil prompt'u göndererek yeni bir araştırma başlatır ve sonucu iş akışına döndürür.
- Özel ajanlar: kod gerektirmeyen agent builder veya geliştirici araçları (MCP ve Graph API) ile kuruma özgü iş akışları otomatikleştirilebilir. Geliştirici deneyimleri E5 inclusion kapsamındadır.

7. Güvenlik Uzmanı Gözüyle Kontrol: Sık Yapılan Hatalar

Bu bölüm, belgenin bağımsız bir güvenlik uzmanı gözüyle yeniden okunması sonucunda hazırlanmıştır. Sahada ve ilk taslak dokümanlarda en sık karşılaşılan yanlış varsayımlar, doğrulanmış karşılıkları ve alınması gereken aksiyonla birlikte listelenmiştir. Her satır Microsoft Learn üzerinden teyit edilmiştir.

Lisans ve kapasite

Yaygın varsayım	Doğrusu	Aksiyon
"E5 lisansımız var, Security Copilot açıktır"	Uygunluk erişim anlamına gelmez. Etkinleştirme kademeli dağıtımla yapılır ve tenant'ın kapsama alınmış olması gerekir	Message Center bildirimini ve ürün içi banner'ı doğrulayın; doğrulamadan proje planı vermeyin
"E5 ile sınırsız kullanım"	Her 1.000 ücretli lisans için ayda 400 SCU, tavan ayda 10.000 SCU	Lisans sayısından hak edişi hesaplayın; 25.000 lisans üzerinde tavan planlaması yapın
"Kullanmadığımız SCU birikir"	Tahsisat aylık sıfırlanır, devretmez	Aylık kullanım hedefi belirleyin; ay sonuna doğru düşük kullanım varsa değer üretmeyen kapasite kaybı vardır
"E5 varsa Azure'da kapasite oluşturmalıyız"	Inclusion modelinde Azure kurulumu gerekmez; kapasite sıfır tıklama ile oluşur. Azure'da kapasite oluşturulduğu anda faturalama başlar	Uygunluk doğrulanmadan Azure tarafında SCU kapasitesi oluşturmayın
"E5 kapsamına girdik, eski provisioned kapasiteyi silelim"	Microsoft, mevcut kapasitenin silinmemesini önermektedir	Mevcut kapasiteyi koruyun; silme kararını Microsoft hesap ekibiyle teyit edin
"Preview özellikler ücretsizdir"	Genel önizleme (public preview) yetenekleri SCU tüketir ve ücretlendirilir; yalnızca özel önizleme (private preview) ücretlendirilmez	Önizleme özelliklerini bütçe dışında bırakmayın
"Kapasite tenant genelinde ortak kullanılır"	SCU'lar workspace'ler arasında paylaşılmaz	Çok workspace'li tasarımlarda her workspace için ayrı kapasite planı yapın
"Sentinel kullanıyoruz, kapsamdayız"	M365 E5/E7 lisansı olmayan Sentinel müşterileri inclusion kapsamında değildir. E5/E7 sahibi Sentinel müşterileri dahil SCU'yu Sentinel senaryolarında kullanabilir; ancak data lake işlem ve depolama maliyetleri dahil değildir	Sentinel maliyetlerini ayrı kalem olarak modelleyin

Devreye alma ve yapılandırma

Yaygın varsayım	Doğrusu	Aksiyon
"Ajanlar otomatik çalışmaya başlar"	Ajanlar otomatik etkinleştirilmez; her biri ayrıca kurulmalı, kimliği ve izinleri yapılandırılmalıdır	Ajan başına devreye alma planı yapın; ön koşul listesi çıkarın
"Ajan kuruldu, çalışıyor demektir"	Ön koşul eksikse ajan sessizce hiçbir iş üretmeyebilir. Örneğin kimlik avı ajanı, Auto-Resolve uyarı ayarlama kuralı açıkken hiçbir uyarıyı triyaj etmez	Kurulum sonrası ilk çalışmayı doğrulayın; ajanın gerçekten çıktı ürettiğini kontrol edin
"Ajanı kullanıcı hesabıyla çalıştırmak pratik"	Kullanıcı hesabıyla çalışan ajan o kullanıcının tüm erişimini devralır. Microsoft Entra Agent ID ile ajana özel kimlik, erişimi kapsamlı ve yönetilebilir tutar	Mümkün olan her ajanda ajan kimliği kullanın; kullanıcı bağlamını istisna olarak ele alın
"Kimlik seçimi geri alınabilir"	Koşullu Erişim Optimizasyon Ajanı'nda kullanıcı bağlamından ajan kimliğine geçiş tek yönlüdür	Kararı geçişten önce verin; test tenant'ında doğrulayın
"Ajan kimliği bir kez kurulur, unutulur"	Purview Insider Risk triyaj ajanında ajan kimlik doğrulaması 90 günde sona erer ve yenilenmelidir	Takvime yenileme hatırlatıcısı ekleyin; operasyon runbook'una alın

Yaygın varsayım	Doğrusu	Aksiyon
"Copilot rolü veren analist veriye erişir"	Security Copilot rolleri Entra rolü değildir ve tek başına güvenlik verisine erişim vermez. Copilot kullanıcı adına çalışır, kullanıcının erişiminin ötesine geçmez	Platform rolü ile servis rolünü ayrı planlayın; eksik servis rolü "Copilot çalışmıyor" şikayetinin en yaygın nedenidir
"Everyone grubu pratik bir başlangıçtır"	Güvenlik verisine erişimi olmayan kullanıcılar için kafa karıştırıcı bir deneyim üretir ve kaldırıldıktan sonra tekrar atanamaz	Recommended Microsoft Security roles veya rol atanabilir güvenlik grupları kullanın
"Oturum paylaşımı zararsızdır"	Paylaşılan oturumu görüntüleyen kullanıcı, ilgili eklentinin verisine erişim yetkisi olmasa bile tüm sonuçları görebilir	Oturum paylaşımını veri paylaşımı kararı olarak ele alın; kural tanımlayın
"Panel kapalıysa tüketim durur"	Gömülü deneyimlerde panel kapatılsa da olay özeti arka planda üretilmeye devam eder	Tüketim modelinde otomatik özetlemeyi ayrı kalem olarak hesaplayın

Dil, uyum ve operasyon

Yaygın varsayım	Doğrusu	Aksiyon
"Türkçe prompt yazabiliriz"	Türkçe yalnızca ürün arayüzü dilidir. Prompt yazımı ve yanıt üretimi sekiz dilde desteklenir (İngilizce, Almanca, Japonca, İspanyolca, Fransızca, İtalyanca, Portekizce, Çince) ve Türkçe bu listede yoktur. Desteklenmeyen dilde yazılan prompt hata döndürür	Prompt dilini İngilizce olarak standartlaştırın; promptbook ve özel ajan talimatlarını İngilizce yazın; analist eğitimini buna göre planlayın
"Veri yerleşimi M365 ile aynı"	Security Copilot tarafından erişilen M365 verisi, erişimden önceki EU Data Boundary ve Product Terms veri yerleşimi taahhütlerinden bağımsız olarak Security Copilot koşullarına göre işlenir ve saklanır	Uyum ekibiyle ayrı değerlendirme yapın; kararı gerekçesiyle kayıt altına alın
"Workspace konumu sonradan düzeltilir"	Workspace oluşturulduktan sonra veri saklama konumu değiştirilemez	Konumu ilk kurulumda bilinçli seçin
"Veri paylaşımı varsayılanı her yerde aynı"	Otomatik provizyonda veri paylaşımı kapalı gelir; manuel onboarding dokümantasyonunda açık olarak tanımlanmıştır	Owner settings üzerinden fiili durumu doğrulayın, varsayıma dayanmayın
"Ajan değişiklikleri izlenmiyor"	Ajan oluşturma, güncelleme ve silme işlemleri Microsoft Purview Unified Audit Log'a ayrı olaylar olarak yazılır	Denetim sorgularını hazırlayın; değişiklik izlenebilirliğini uyum dosyasına ekleyin
"Copilot erişimi ayrıca korunmalı değil"	Security Copilot platformuna erişim Koşullu Erişim politikalarıyla katmanlanabilir	Copilot erişimi için ayrı bir Koşullu Erişim politikası tanımlayın
"Kamu bulutunda da kullanılabilir"	Security Copilot şu an ABD kamu bulutları (GCC, GCC High, DoD, Azure Government) için tasarlanmamıştır	Ticari bulut varsayımını belgede açıkça belirtin

Üründeki değişim hızı

Security Copilot ayda bir güncellenen bir üründür ve ajan portföyü hızla genişlemektedir. Bu belgedeki bilgiler 13 Ağustos 2026 itibarıyla doğrulanmıştır. Müşteriye taahhüt içeren bir teklif veya proje planı üretilmeden önce "What's new in Microsoft Security Copilot" sayfası ve ilgili ajanın kendi ön koşul bölümü tekrar kontrol edilmelidir.

8. Veri Koruma, Veri Yerleşimi ve KVKK Değerlendirmesi

Security Copilot bir üretken yapay zeka hizmetidir ve müşteri verisini işler. Türkiye'de faaliyet gösteren kurumlar için KVKK, uluslararası operasyonu olanlar için GDPR açısından aşağıdaki başlıkların onboarding öncesinde değerlendirilmesi ve karara bağlanması önerilir.

Müşteri verisi ve sistem günlükleri

Müşteri Verisi (Customer Data)	Sistem tarafından üretilen günlükler
Kullanıcıların gönderdiği promptlar Yanıt üretmek için alınan bilgiler Yanıtların kendisi Sabitlenmiş (pinned) öğelerin içeriği Yüklenen dosyalar	Hesap bilgileri (tenant kimliği, hesap kimliği, lisans vb.) Kullanım verisi Performans bilgisi Sistem davranışına ilişkin dahili bilgiler

Veri saklama konumu ve prompt değerlendirme konumu

- Veri, workspace oluşturulurken seçilen konumda saklanır. Otomatik provizyonda bu konum Microsoft Entra coğrafyanızdır; tenant'ta M365 coğrafya geçersiz kılma (Preferred Data Location, Advanced Data Residency vb.) varsa o eşlenir.
- Workspace oluşturulduktan sonra veri saklama konumu değiştirilemez.
- Prompt değerlendirme konumu, promptların GPU üzerinde işlendiği yerdir. Veri saklama konumu AB ise promptlar AB'de işlenir; değilse yük ve GPU müsaitliğine göre ABD, İngiltere, AB veya ANZ arasında dağıtılır.
- Veri paylaşımına onay verilmesi durumunda müşteri verisi (yüklenen dosyalar hariç) seçilen workspace coğrafyası dışında saklanabilir. Yüklenen dosyalar workspace'te saklanır; ancak dosya içeriğinden yanıt üretmek için alınan bilgiler workspace dışında saklanabilir.
- Ajanların e-posta veya Microsoft Teams üzerinden sonuç ilettiği durumlarda iletim küresel Microsoft ağ altyapısı üzerinden geçebilir; veri saklama konumu değişmese de aktarım coğrafi sınırları aşabilir.

> **KVKK/GDPR açısından en kritik madde**
>
> Security Copilot tarafından erişilen Microsoft 365 verisi — Purview tarafından üretilen müşteri verisi dahil — erişimden önce hangi veri yerleşimi taahhüdüne tabi olursa olsun, erişildikten sonra Security Copilot'ın veri işleme, saklama ve güvenlik uygulamalarına tabi olur. Kurum, EU Data Boundary veya benzeri bir taahhüde dayanıyorsa bu farkın veri işleme envanterine ve aydınlatma metnine yansıtılması gerekir.

Veri paylaşımı tercihleri

İki ayrı veri paylaşımı ayarı vardır ve her ikisi de Copilot owner tarafından yönetilir:

- Ürün performansının insan incelemesiyle doğrulanması için Microsoft'un Security Copilot verisini yakalamasına izin verilmesi.
- Microsoft'un güvenlik yapay zeka modelini geliştirmesi ve doğrulaması için verinin yakalanmasına ve insan incelemesine izin verilmesi.

Her iki durumda da Microsoft'un açık taahhüdü: veri OpenAI ile paylaşılmaz, satış amacıyla kullanılmaz, üçüncü taraflarla paylaşılmaz ve Azure OpenAI temel modellerinin eğitiminde kullanılmaz. Otomatik provizyonlanan E5/E7 tenant'larında her iki ayar da varsayılan olarak kapalıdır.

Saklama ve silme

Durum	Süre
Tüm provizyonlanan kapasite silindiğinde müşteri verisinin silinmesi	180 gün içinde
180 günden uzun süre işlem görmeyen oturum verisi	180 gün sonunda silinir
Portal veya destek üzerinden silme talebi	Talepten sonra 30 gün içinde
Veri paylaşımına onay verilen durumda paylaşılan verinin saklanması	Değerlendiren ekip tarafından 90 gün
Veri paylaşımından çıkıldığında paylaşılmış verinin silinmesi	30 gün içinde; önceden paylaşılan veri en fazla 180 gün saklanır

- GDPR kapsamındaki veri sahibi talepleri (DSR) için Security Copilot destek ekibiyle iletişime geçilir.
- Azure'da saklanan tüm veriler AES-256 ile beklemede şifrelenir.
- Security Copilot ISO 42001 sertifikasına sahiptir ve Azure Ticari ortamında FedRAMP High yetkilendirmesi kapsamına alınmıştır.

9. Öneriler ve 30-60-90 Gün Yol Haritası

Aşağıdaki yol haritası, Microsoft 365 E5 lisansına sahip ve Security Copilot'ı ilk kez devreye alacak bir kurum için hazırlanmıştır. Amaç, ilk 30 günde ölçülebilir bir kazanım üretmek ve kapasite tüketimini varsayım yerine ölçüm üzerine kurmaktır.

İlk 30 gün — Temel ve ölçüm

Alan	Yapılacak	Çıktı
Doğrulama	Lisans uygunluğu ve tenant etkinleştirmesinin teyidi	Ekran kayıtlı doğrulama notu
Yönetişim	Owner settings gözden geçirmesi: veri saklama konumu, prompt değerlendirme konumu, veri paylaşımı, M365 servis verisi erişimi	Karara bağlanmış ve gerekçelendirilmiş yapılandırma kaydı
Kimlik	Rol tasarımı: Everyone kaldırılır, rol atanabilir güvenlik grupları kurulur, Copilot erişimi için Koşullu Erişim politikası devreye alınır	RBAC matrisi ve devreye alınmış politika
Pilot	Tek bir yüksek değerli senaryo: Defender olay özetleme veya kimlik avı triyajı	Öncesi/sonrası triyaj süresi ölçümü
Ölçüm	Kullanım panosunun haftalık okunması ve Excel ihracatı	İlk gerçek SCU tüketim tabanı

31-60 gün — Genişleme

Alan	Yapılacak	Çıktı
Kimlik güvenliği	Koşullu Erişim Optimizasyon Ajanı devreye alınır; öneriler rapor-only modda değerlendirilir	Kapatılmış politika boşlukları listesi
Uç nokta	Zafiyet Düzeltme Ajanı için ön koşullar tamamlanır ve readiness check çalıştırılır	Önceliklendirilmiş zafiyet düzeltme planı
Veri güvenliği	DLP triyaj ajanı için politika modu (aktif/simülasyon) ve kanıt toplama ayarları gözden geçirilir	Triyaj kapsamı netleştirilmiş DLP uyarı akışı
Kapasite	İlk 30 günün ölçümüyle kapasite planının yeniden kurulması	Gerçek veriye dayalı SCU bütçesi
Yetkinlik	Analist eğitimi: İngilizce prompt disiplini, promptbook kullanımı, çıktı doğrulama kuralı	Eğitim tamamlanma kaydı ve kurum içi prompt kütüphanesi

61-90 gün — Olgunlaşma

Alan	Yapılacak	Çıktı
Otomasyon	Kuruma özel promptbook'lar ve gerekirse özel ajan geliştirme	Tekrarlanabilir iş akışı kütüphanesi
Raporlama	Tehdit İstihbaratı Brifing Ajanı ile düzenli yönetim raporlaması	Aylık CISO brifing formatı
Yönetişim	Purview Unified Audit Log üzerinden ajan değişiklik denetiminin kurumsallaştırılması	Denetim sorguları ve periyodik gözden geçirme takvimi
Kapasite	Aylık kapasite gözden geçirme toplantısının rutine alınması	Tüketim trendi ve tavan riski değerlendirmesi
Değer	Kazanım ölçümü: triyaj süresi, kapatılan politika boşluğu, düzeltilen zafiyet sayısı	Yönetime sunulabilir fayda raporu

Kalıcı operasyon kuralları

1. Prompt dili İngilizce standardı korunur; Türkçe yalnızca arayüz dili olarak kullanılır.
2. Copilot çıktısı doğrulanmadan aksiyon alınmaz; üretken yapay zeka çıktısı kanıt değil, hızlandırıcıdır.

3. Yeni bir ajan devreye alınmadan önce ön koşul listesi çıkarılır, kimlik ve izin tasarımı yapılır, ilk çalışma doğrulanır.
4. Kapasite tüketimi aylık gözden geçirilir; tavan riskine yaklaşıldığında önceliklendirme yapılır.
5. Ürün güncellemeleri aylık takip edilir; ajan ön koşulları değişebilir.

10. Ekler

Ek A — Terim sözlüğü

Terim	Açıklama
SCU (Security Compute Unit)	Security Copilot iş yüklerini çalıştırmak için gereken hesaplama kapasitesinin birimi
Inclusion modeli	Microsoft 365 E5/E7 lisansına dahil edilen, aylık havuz esaslı kapasite modeli
Provisioned kapasite	Önceden satın alınan ve saatlik faturalanan taban SCU kapasitesi
Overage kapasite	Provisioned kapasite tükendiğinde devreye giren, kullanıldıkça faturalanan ek kapasite
Workspace	Verinin nerede saklandığını, hangi kapasitenin kullanıldığını ve kimin erişebileceğini tanımlayan mantıksal kapsayıcı
Default Security Copilot Capacity	E5/E7 inclusion etkinleştiğinde otomatik oluşan, değiştirilemeyen ve tenant genelinde paylaşılan kapasite
Standalone deneyim	securitycopilot.microsoft.com üzerinden erişilen bağımsız portal
Embedded deneyim	Copilot'ın Defender, Entra, Intune, Purview gibi ürünlerin içinden kullanılması
Ajan (agent)	Tanımlı tetikleyici, kimlik ve izinler çerçevesinde otonom çalışan bileşen
Tetikleyici (trigger)	Ajanı başlatan olay veya koşul; zamanlanmış veya manuel olabilir
Microsoft Entra Agent ID	Yapay zeka ajanları için oluşturulan, kullanıcı hesabından bağımsız kimlik
Promptbook	Belirli bir görevi tamamlamak için sırayla çalışan prompt dizisi
Eklenti (plugin)	Copilot'ın Microsoft ve Microsoft dışı servislerin yeteneklerine API üzerinden erişmesini sağlayan bileşen
Primitive	Kullanıcı etkileşimi olmadan bir servis, uygulama veya iş akışı tarafından yapılan yapay zeka çıkarım çağrısı
On-behalf-of kimlik doğrulama	Copilot'ın kullanıcı adına çalışması; kullanıcının erişiminin ötesine geçmemesi ilkesi

Ek B — Kaynaklar

Aşağıdaki Microsoft Learn kaynakları 13 Ağustos 2026 tarihinde doğrulanmıştır.

- Learn about Security Copilot for Microsoft 365 E5 and E7 included customers — learn.microsoft.com/copilot/security/security-copilot-inclusion
- Understand how Security Copilot is auto provisioned for eligible Microsoft 365 E5 and E7 customers — learn.microsoft.com/copilot/security/auto-provisioning-security-copilot
- Microsoft Security Copilot Security Compute Units and capacity — learn.microsoft.com/copilot/security/security-compute-units-capacity
- Get started with onboarding to Microsoft Security Copilot — learn.microsoft.com/copilot/security/get-started-security-copilot
- Onboarding to Security Copilot for non-Microsoft 365 E5 and E7 customers — learn.microsoft.com/copilot/security/manual-onboarding
- Manage security compute unit usage in Security Copilot — learn.microsoft.com/copilot/security/manage-usage
- Understand authentication in Microsoft Security Copilot — learn.microsoft.com/copilot/security/authentication
- Microsoft Security Copilot experiences — learn.microsoft.com/copilot/security/experiences-security-copilot
- Privacy and data security in Microsoft Security Copilot — learn.microsoft.com/copilot/security/privacy-data-security

- Supported languages in Microsoft Security Copilot — learn.microsoft.com/copilot/security/supported-languages
- Microsoft Security Copilot Frequently Asked Questions — learn.microsoft.com/copilot/security/faq-security-copilot
- What's new in Microsoft Security Copilot — learn.microsoft.com/copilot/security/whats-new-copilot-security
- Microsoft Security Copilot agents overview — learn.microsoft.com/copilot/security/agents-overview
- Application card: Microsoft Security Copilot agents — learn.microsoft.com/copilot/security/security-copilot-application-card-agents
- Microsoft Security Copilot Phishing Triage Agent in Microsoft Defender — learn.microsoft.com/defender-xdr/phishing-triage-agent
- Microsoft Entra Conditional Access Optimization Agent — learn.microsoft.com/entra/security-copilot/conditional-access-agent-optimization
- Vulnerability Remediation Agent in Microsoft Intune — learn.microsoft.com/intune/copilot/agents/vulnerability-remediation-agent
- Get started with the Microsoft Purview Triage Agent in Data Loss Prevention — learn.microsoft.com/purview/copilot-in-purview-triage-dlp-agent-get-started
- Security Copilot agents in Microsoft Purview overview — learn.microsoft.com/purview/copilot-in-purview-agents-overview
- Microsoft Security Copilot in Microsoft Entra proof-of-concept guide — learn.microsoft.com/entra/architecture/security-copilot-entra-proof-of-concept

Ek C — Belge bilgileri

Alan	Değer
Belge adı	Microsoft Security Copilot – Microsoft 365 E5 Kullanım, Onboarding ve SCU Kapasite Rehberi
Sürüm	1.0
Tarih	13 Ağustos 2026
Sınıflandırma	HERKESE ACIK – PUBLIC
Hazırlayan	Mustafa Emre SONER, Modern Work & Security Manager, Tworks
Kurum	Tworks Bilişim Hizmetleri — Microsoft Solutions Partner
Kaynak doğrulama	Microsoft Learn, 13 Ağustos 2026

Tworks Bilişim Hizmetleri
Quasar İstanbul, Fulya Mah. Büyükdere Cad. No:76 Kat:1 İç Kapı No:104, 34394 Mecidiyeköy/Şişli/İstanbul
VKN: 8591464631 | MERSİS: 0859 1464 6310 0001
info@tworks.com.tr | Microsoft Solutions Partner