Sparta Siber Güvenlik

Forensic Horizon
CYBER EVIDENCE ASSURANCE

SPARTA TEKNİK REHBER / YAPAY ZEKÂ ORTAMLARINDA DFIR

Yapay Zekâ Adli Bilişim Konsolide Rehberi

ChatGPT | Google Gemini | Claude

Kanıt kaynakları, kayıtlar, saklama süreleri, ajan davranışı ve adli görünürlük sınırları için pratik bir DFIR saha başvuru kaynağı.

HIZLA DEĞİŞEN PLATFORM UYARISI

Yapay zekâ servisleri çok hızlı değişir. Bu Türkçe sürüm, 28-29 Ağustos 2026 tarihlerinde doğrulanmış Forensic Horizon kaynak çalışmasının çevirisidir. Ürün adları, plan yetkileri, olay şemaları, API'ler, saklama kuralları, yerel artefaktlar ve bağlı uygulama davranışları değişebilir. Gerçek bir incelemede güncel üretici dokümantasyonu ile canlı kiracı/ortam mutlaka yeniden doğrulanmalıdır.

Türkçe Konsolide Sürüm 1.0
Ağustos 2026
TLP:CLEAR

Yönetici Özeti

Bu konsolide Forensic Horizon Horizon Series rehberi; **ChatGPT, Google Gemini ve Claude** için hazırlanmış platforma özgü üç adli bilişim kılavuzunu tek belgede bir araya getirir. İncelemeciler, olay müdahale ekipleri, güvenlik ekipleri, hukuk/eDiscovery paydaşları ve hızla gelişen yapay zekâ servisleri için adli bilişim hazırlığı oluşturan kurumlar açısından pratik bir DFIR saha başvuru kaynağı olarak tasarlanmıştır.

Yapay zekâ adli bilişimi neden önemlidir? Yapay zekâ sistemleri artık günlük iş akışlarının parçasıdır; ancak oluşturdukları delil izi kimlik sistemleri, konuşmalar, istemler ve yanıtlar, yüklenen dosyalar, uç nokta artefaktları, bulut denetim akışları, bağlı uygulamalar, ajanlar ve aşağı akış SaaS/API kayıtları arasında parçalanır. Bir olay sırasında "yapay zekâ platformu kullanıldı" demek; platformun hangi veriyi aldığı, modelin ne döndürdüğü, hangi araç/ajan eyleminin istendiği veya başka bir sistemde nihayetinde neyin değiştiğini ispatlamakla aynı değildir. Bu ayrımlar atıf, veri ifşası analizi, içeriden kötüye kullanım, prompt injection, ajan kötüye kullanımı ve savunulabilir olay rekonstrüksiyonu açısından doğrudan önem taşır.

FORENSIC HORIZON İLKESİ

Kullanışlı adli görünürlük ufku yalnızca platformun neyi kaydettiğiyle değil, her bir kanıt kaynağının ne kadar süre **aranabilir, geri getirilebilir, bir kimliğe/oturuma bağlanabilir ve savunulabilir** kaldığıyla belirlenir. Yerel saklama pencereleri kısa olabilir, içerik ve denetim kayıtları farklı yaşam döngülerine sahip olabilir ve aşağı akışta gerçekten neyin çalıştığını göstermek çoğu zaman yapay zekâ platformu dışındaki kaynaklarla doğrulama gerektirir.

Platformlar arası ortak temalar

- **Birden fazla kanıt düzlemini koruyun.** Yapay zekâ platformu kayıt ve içeriğini kimlik, uç nokta, tarayıcı, ağ, DLP, depo, bulut ve üçüncü taraf sağlayıcı kanıtlarıyla korele edin.
- **Saklama bir mimari kontroldür.** Kısa ufuklu kayıtlar veya isteğe bağlı payload kaydı sunan platformlarda sürekli dışa aktarma ve planlı muhafaza, inceleme erişimini ciddi ölçüde uzatır.
- **Ajanlar nedensellik zinciri problemi yaratır.** Güvenilmeyen girdiyi, model bağlamını, karar/araç isteğini, yetkilendirmeyi, aşağı akış yürütmeyi ve oluşan etkiyi birbirinden ayırın.
- **Kesinliği abartmayın.** Kullanım telemetrisi otomatik olarak konuşma dökümü değildir; saklanan bir konuşma da bağlı servisin istenen eylemi gerçekten yürüttüğünü tek başına kanıtlamaz.
- **Canlı davranışı doğrulayın.** Yetkiler, şemalar, API yolları, varsayılan ayarlar ve saklama davranışları klasik adli bilişim kaynaklarından çok daha hızlı değişebilir.

İçindekiler ve Rehberin Kullanımı

Kaynak üç kılavuz, platforma özgü uyarılar, tablolar, taktik akışlar ve kanıt eşleştirmeleri korunacak şekilde Türkçeleştirilerek bu belgede birleştirilmiştir. Ürün ve API adları teknik doğruluk için mümkün olduğunca özgün biçimiyle bırakılmıştır.

Önerilen inceleme akışı

1. Tam kiracı/tenant, hesap türü, plan, rol, etkin özellikler ve olay zaman aralığını belirleyin.
2. Containment veya hesap değişiklikleri durumu değiştirmeden önce volatil veya kısa saklama süreli kaynakları koruyun.
3. Yerel denetim/uyumluluk telemetrisini dışa aktarın ve normalizasyondan önce ham olayları saklayın.
4. Hukuken yetkili olduğunuz ölçüde içerikleri, dosyaları, yerel artefaktları ve özelliğe özgü kanıtları toplayın.
5. Atfı güçlendirmek için kimlik ve uç nokta bağlamını korele edin.
6. Bağlı uygulamalar veya ajanlar için yürütme ve etkiyi kanıtlamak üzere aşağı akış sağlayıcı kayıtlarını edinin.
7. Kullanım metadatasından eksik içerik uydurmak yerine kanıt boşluklarını açıkça kayıt altına alın.

Horizon Series:

ChatGPT

ChatGPT Enterprise, Edu, Business, uygulamalar ve workspace ajanları genelinde kanıt kaynakları, kayıtlar, saklama ve adli görünürlük ufku sınırlayıcıları için pratik bir kılavuz.

HIZLA DEĞİŞEN PLATFORM UYARISI

Yapay zekâ platformları, ürün adları, plan yetkileri, olay şemaları, API'ler, saklama kuralları, yerel artefaktlar ve bağlı uygulama davranışları hızla değişebilir. Bu bölüm **29 Ağustos 2026** tarihinde doğrulanan kaynak çalışmayı temel alır. Bir soruşturmada herhangi bir yol, alan, izin, saklama süresi veya davranışa güvenmeden önce güncel üretici dokümantasyonunu ve canlı ortamı yeniden doğrulayın.

Sürüm: 1.0
Tarih: Ağustos 2026
TLP: CLEAR

Forensic Horizon × Sparta Siber Güvenlik

Yönetici Özeti

DOĞRULAMA UYARISI - KULLANMADAN ÖNCE OKUYUN

OpenAI; ChatGPT planlarını, Compliance Platform şemalarını, uygulama davranışını, izinleri, saklama davranışını ve idari kontrolleri sık değiştirir. Bu bölüm 29 Ağustos 2026 tarihinde gözden geçirilen kamuya açık OpenAI dokümantasyonunu temel alır. Delil niteliğinde bir iddia oluşturmadan önce kesin workspace, plan, rol ve etkin özellikleri doğrulayın.

- **Önce plan ve kanıt sınırlarını ayırın:** Enterprise/Edu, Compliance Platform üzerinden en güçlü yerel adli görünürlüğü sunar. Business ve kişisel hesapların idari görünürlük ve dışa aktarma yolları ciddi biçimde farklıdır.
- **Compliance Logs Platform dışa aktarılmadıkça kısa ufuklu bir kaynaktır:** OpenAI, uyumluluk log verisinin 30 gün saklandığını belirtir. Bu nedenle bağımsız kontrol edilen SIEM/veri gölüne sürekli dışa aktarma temel hazırlık kontrolüdür.
- **Konuşma içeriği ile denetim faaliyeti farklı kanıt sınıflarıdır:** değiştirilemez/zaman pencereli olaylar aktivite ve atfa yardımcı olur; conversation-message verisi ise gerekli izin ve endpoint kapsamı mevcutsa desteklenen kayıtlı mesaj içeriğini yeniden kurabilir.
- **Silme, geri getirilebilirliği hızla çökertir:** içerik silindiğinde veya süresi dolduğunda, iç yedekler geçici olarak kalsa bile Compliance API üzerinden hemen erişilemez hale gelebilir.
- **Uygulamalar ve ajanlar ikinci bir kanıt düzlemi yaratır:** ChatGPT kaydı bir uygulamaya istek yapıldığını gösterebilir; ancak hangi eylemin gerçekten çalıştığını ve neyin değiştiğini kanıtlamak için çoğu zaman aşağı akış sağlayıcı logları gerekir.

Forensic Horizon ilkesi

“ChatGPT kullanıldı” ile “kullanıcının, modelin, uygulamanın ve aşağı akış servisin tam olarak ne yaptığını yeniden kurabiliyoruz” farklı delil ifadeleridir. Aradaki boşluğu açıkça kaydedin.

Kapsam ve İnceleme Sınırları

Bu bölüm, en zengin yerel uyumluluk telemetrisini sundukları için öncelikle ChatGPT Enterprise ve Edu ortamlarına odaklanır. Kanıt mevcudiyetini etkilediği ölçüde Business ve kişisel hesap sınırlamaları, Temporary Chat, dosyalar/Library, GPT’ler, uygulamalar/plug-in’ler, Record Mode ve workspace ajanları da kapsanır.

Ortam	Birincil kanıt	Önemli sınırlama
ChatGPT Enterprise / Edu	Compliance Logs Platform, stateful Compliance API, admin/tenant audit, conversation-message verisi	Kapsam; izinlara, özellik türüne, saklama süresine ve dışa aktarma sıklığına bağlıdır.
ChatGPT Business	Workspace/admin ayarları, analitik, uç nokta/tarayıcı kanıtı, uygulama/sağlayıcı logları	Yöneticiler sıradan özel konuşmalara otomatik olarak erişmez.
Kişisel ChatGPT	Kullanıcı veri dışa aktarımı, hesap/oturum kanıtı, uç nokta/tarayıcı artefaktları	Kurumsal tenant çapında uyumluluk toplaması yoktur.
Uygulamalar / plug-in’ler / ajanlar	Varsa ChatGPT uygulama aktivitesi/kimlik doğrulama logları + üçüncü taraf audit logları	ChatGPT tarafındaki kanıt aşağı akış yürütme/etkisini kanıtlamayabilir.

Temel Tehdit Soruları

- **Hesap ele geçirilmesi:** Ele geçirilme sonrasında yönetilen bir kimlik ChatGPT'ye erişmek, önceki konuşmaları okumak, veri yüklemek, GPT/ajan oluşturmak veya uygulama çağırmak için kullanıldı mı?
- **Veri ifşası:** Hangi gizli içerik yapıştırıldı, yüklendi, Library/projelerden referanslandı, bağlı bir uygulamadan getirildi veya model tarafından döndürüldü?
- **Ajan / uygulama kötüye kullanımı:** Hangi güvenilmeyen girdi model bağlamına girdi, hangi app/tool çağrısı istendi, hangi kimlik bunu yetkilendirdi ve aşağı akışta gerçekte ne çalıştı?
- **İçeriden kötüye kullanım:** Kullanıcı ChatGPT'yi kısıtlı bilgiyi özetlemek, dönüştürmek, hazırlamak veya taşımak amacıyla bilerek kullandı mı?
- **Savunmadan kaçınma:** Sohbetler silindi mi, Temporary Chat kullanıldı mı, saklama/ayarlar değiştirildi mi, uygulamalar bağlantıdan çıkarıldı mı veya kanıt dışa aktarma hatları devre dışı bırakıldı mı?

Kanıt Düzlemleri

Düzlem	Neyi ortaya koyabilir	Tek başına genellikle neyi ortaya koyamaz
Kimlik / kimlik doğrulama	Kimin, ne zaman ve kaydedildiği ölçüde hangi tenant/güvenlik bağlamından kimlik doğruladığını.	Kesin prompt, yanıt veya aşağı akış eylemi.
Uyumluluk aktivite logları	Yönetim, kimlik doğrulama, uygulama, konuşma ve desteklenen diğer olay kategorileri.	İlgili içerik/mesaj kaydı yoksa her özelliğin tam içeriğini.
Konuşma / içerik durumu	Mesajlar, saklanan konuşma verisi, dosya/GPT/proje durumu.	Harici bir servisin istenen eylemi gerçekten gerçekleştirdiğini.
Uygulama / ajan telemetrisi	Uygulama istekleri, bağlantı olayları, mevcutsa ajan kullanım/yapılandırma verisi.	Sağlayıcı audit kanıtı olmadan sağlayıcı tarafındaki nesne değişikliklerini.
Uç nokta / tarayıcı kanıtı	Yerel erişim bağlamı, zaman damgaları, indirilen dışa aktarımlar, cache parçaları, tarayıcı geçmişi.	Garanti edilmiş kanonik bir konuşma dökümü deposunu.

KORELASYON KURALI Kullanım metadatasına konuşma-dökümü düzeyinde kesinlik atamayın. Tersine, saklanan bir konuşmanın tüm bağlı-uygulama işlemlerinin tamamlandığını kanıtladığını da varsaymayın. Kimlik, ChatGPT log/içeriği, uç nokta kanıtı ve aşağı akış SaaS/bulut audit loglarından tek bir zaman çizelgesi oluşturun.

Compliance Platform: Gerçekte Neler Mevcut?

Uygun Enterprise ve Edu workspace'leri için OpenAI iki tamamlayıcı yapı tanımlar: audit olayları için değiştirilemez, append-only **Compliance Logs Platform** ve mevcut durum ile desteklenen legacy/content birleştirmeleri için stateful **Compliance API** endpoint'leri. Erişim, workspace kapsamlı Admin anahtarları ve izinlarla kontrol edilir.

Kaynak / kontrol	Adli değer	Ufuk / uyarı
Compliance Logs Platform	SIEM, eDiscovery ve DLP alımı için uygun append-only/zaman pencereli audit kanıtı.	OpenAI 30 günlük saklama penceresi belirtir; daha uzun geçmiş için sürekli dışa aktarın.

Kaynak / kontrol	Adli değer	Ufuk / uyarı
Conversation-message logları	Gerekli izinlarla desteklenen mesaj aktivitesi ve içeriğini yeniden kurar.	Eski stateful conversation rotası Haziran 2026'da kaldırılmıştır; güncel logs şemasını doğrulayın.
Admin audit logları	Workspace/tenant idari aktiviteleri ve güvenlik kontrolü değişiklikleri.	Tenant çapında audit ile workspace compliance kapsamları farklıdır; görünürlük rol, olay türü ve özellik mevcudiyetine bağlıdır.
Authentication logları	Kimlik/oturum erişimi ve bağlantı aktivitesini destekler.	Güçlü atıf için yine de IdP/cihaz/ağ kanıtı gerekir.
App activity / authentication logları	Varsa uygulamalara istekleri ve bağlantı/bağlantı kesme aktivitesini kaydedebilir.	Aşağı akış etkisini kesin biçimde ispatlamak için sağlayıcı tarafı logları gerekir.

Saklama Bir Yapılandırma ve Toplama Problemidir

- **30 günlük compliance log penceresi:** platformu arşiv değil, besleme akışı olarak görün. Bir toplama döngüsünü kaçırmak kalıcı boşluk yaratabilir.
- **Workspace içerik saklama:** Enterprise/Edu yöneticileri workspace retention'ını kontrol eder; silinen konuşmalar, yasal/güvenlik istisnaları yoksa genel olarak 30 gün içinde OpenAI sistemlerinden kaldırılır.
- **Silinmiş/süresi dolmuş içerik:** erişilemeyen iç yedek kopyalar geçici olarak kalırken bile içerik silme/süre dolumu sonrasında Compliance API'den hemen kaybolabilir.

Hazırlık sonucu

En güçlü ChatGPT adli görünürlük ufku çoğu zaman yerel 30 günlük log penceresi değil, kurumun kendi sürekli dışa aktarılan compliance veri kümesinin ufkudur.

Konuşmalar, Dosyalar, Library, GPT'ler ve Projeler

ChatGPT kanıtı artık yalnızca bir sohbet dökümü değildir. İncelemeler; mesajları, yüklenen dosyaları, Library nesnelerini, proje bağlamını, GPT yapılandırması/bilgisini, memories ve özelliğe özgü artefaktları korumayı gerektirebilir.

Kanıt kaynağı	En iyi kullanım	Önemli saklama davranışı
Konuşma mesajları	Kullanıcının ne sorduğunu ve modelin ne döndürdüğünü belirlemek.	Mevcudiyet, workspace/içerik saklama ayarlarını ve desteklenen Compliance Platform kapsamını izler.
Library'ye kaydedilen dosyalar	Kaynak belgeleri geri kazanmak ve referanslar izin verdiğinde sohbetler arası dosya tekrar kullanım korelasyonu yapmak.	Aktifken workspace retention'ını izler; silme/süre dolumu sonrasında Compliance API'den erişilemez hale gelir.
Geçici / Library dışı yüklemeler	Tek seferlik yükleme veya geçici dosya akışlarını kanıtlamak.	OpenAI, başka bir saklama kuralı geçerli değilse bazı Enterprise dosyalarının 48 saat sonra süresinin dolabileceğini belirtir.
Özel GPT'ler / projeler	Yapılandırma, bilgi dosyaları, proje içeriği ve provenance.	Dosyalar GPT/proje ile birlikte silmeye kadar tutulur; ardından belirtilen silme penceresine tabi olarak kaldırılır.

Kanıt kaynağı	En iyi kullanım	Önemli saklama davranışı
Memory	Memory etkin olduğunda konuşmalar arasında taşınan kişiselleştirilmiş bağlamı açıklamaya yardımcı olabilir.	Compliance kapsamı evrensel değildir; memory özetini eksiksiz kabul etmeyin. Varsa alttaki konuşmalarla korele edin.

DOSYA-UFKU UYARISI Sohbet saklama ve dosya saklama her zaman aynı değildir. Konuşma kalırken yüklenmiş bir dosya Compliance API üzerinden artık geri getirilemeyebilir. Yüksek değerli dosyaları hukuken ve operasyonel olarak mümkün olan en erken anda koruyun.

Record Mode ve Özelliğe Özgü Diğer Kanıtlar

OpenAI'ye göre Enterprise/Edu için Record Mode konuşma dökümleri ve canvases Compliance API tarafından yakalanır; ses, transkripsiyondan hemen sonra silinir; transkriptler ve özetler ise workspace retention'ını devralır. Bunu klasik bir volatil kaynak problemi olarak değerlendirin: orijinal ses artık yokken transkript kalabilir.

Uygulamalar, Plug-in'ler ve Workspace Ajanları

Modern ChatGPT, bağlı servislerden veri alabilir ve etkinleştirildiği durumlarda bu sistemlerde eylem gerçekleştirebilir. Bu da diğer ajan tabanlı platformlarda görülen nedensellik zinciri problemini yaratır.

Aşama	ChatGPT tarafı kanıt	Doğrulayıcı kanıt
1. Girdi / bağlam	Konuşma mesajı, dosya, uygulamadan alınan içerik, memory/context.	Kaynak sistem nesnesi, e-posta/belge provenance, DLP.
2. Model / ajan kararı	Konuşma/ajan aktivitesi, app request kaydı, varsa yapılandırma/sürüm.	Ajan yapılandırma geçmişi, prompt/instruction kaynağı.
3. Yetkilendirme	App authentication/connection durumu, workspace izinleri.	OAuth/IdP logları, sağlayıcı hesap izinleri.
4. Eylem isteği	App-activity kaydı istek ve ilgili yanıt bilgisini içerebilir.	Sağlayıcı API/audit logları.
5. Yürütme / etki	Dönen uygulama yanıtında kısmen görünebilir.	Kesin aşağı akış logları: dosya değişimi, mesaj gönderimi, issue güncellemesi, DB write vb.

Temel Adli Uyarılar

- **İzinler önemlidir:** Enterprise/Edu yöneticileri uygun Compliance Platform izinlerine ihtiyaç duyar; geniş conversation-message erişimi sıradan log kategorilerinden daha kısıtlıdır.
- **Üçüncü taraf saklama bağımsızdır:** bağlı uygulamaya gönderilen veri ayrıca o sağlayıcının politikalarına tabidir. Sağlayıcı kanıtı ChatGPT'den daha uzun veya daha kısa saklayabilir.
- **Ajanın sahip olduğu/paylaşılan kimlik bilgileri atfı zorlaştırır:** etkili dış kimlik, çalıştırmayı başlatan insan yerine paylaşılan/servis hesabı olabilir.
- **Write approval ve kısıtlar kanıttır:** yapılandırılmış onay modunu ve app/action kısıtlarını koruyun; bunlar eylemin insan onayı olmaksızın yürüyüp yürüyemeyeceğini etkiler.

Nedensellik ayrımı

Bir model tool-call'ı **eylem isteğidir**. Sağlayıcı audit olayı **yürütmeyi** ortaya koyabilir. Ortaya çıkan nesne/durum değişikliği ise **etkidir**. "Ajan gerçekte ne yaptı?" sorusu için üçünü de koruyun.

Temporary Chat, Business ve Kişisel Hesaplar

İncelemeciler, sıradan sohbet geçmişinde görünmemenin platform tarafında kanıt olmadığı anlamına geldiğini varsaymamalıdır.

Temporary Chat

- Temporary Chat'ler sıradan geçmiş değildir: genellikle chat history'de görünmez ve geçici oldukları sürece memory oluşturmazlar.
- Enterprise adli görünürlüğü açıktır: OpenAI, Temporary Chat'lerin özel workspace retention süresinden bağımsız olarak Compliance API üzerinden 30 gün kullanılabilir olduğunu belirtir.
- Üçüncü taraf eylemleri sohbetten daha uzun yaşayabilir: bir GPT/plug-in/app veriyi dışarı gönderirse alıcının kendi retention politikası geçerlidir.

ChatGPT Business

Business güçlü workspace kontrollerine sahiptir ancak adli toplama açısından Enterprise/Edu ile eşdeğer sayılmamalıdır. Business yöneticileri varsayılan olarak sıradan workspace UI veya bir Business Compliance API aracılığıyla tüm üyelerin özel sohbetlerine transcript düzeyinde erişmez. Data export yetenekleri de kişisel/Edu senaryolarından farklıdır. Bu nedenle uç nokta, kimlik, DLP, proxy/SASE ve bağlı sağlayıcı kanıtları daha önemli hale gelir.

Kişisel Hesaplar

Kullanıcının talep ettiği ChatGPT data export, sohbet geçmişi ve ilgili hesap verisini içerebilir; ancak bu noktasal, kullanıcı kontrollü bir kaynaktır ve önceden silinmiş sohbetleri geri getiremez. Varsa tarayıcı/oturum, cihaz, e-posta bildirimi, kimlik ve ağ kanıtıyla destekleyin.

UÇ NOKTA KANITI UYARISI Tarayıcı geçmişi, indirmeler, cookie/session artefaktları, cache içerik ve masaüstü/mobil uygulama verisi zamanlama ve erişim sorularını destekleyebilir; ancak OpenAI bunları kararlı bir forensic API olarak dokümante etmez. Yerel yol ve şemaları sürüme özgü kabul edin ve edinilen uç noktada doğrulayın.

Taktik Playbook'lar

1. Şüpheli Yönetilen-Hesap Ele Geçirilmesi

- Containment oturum durumunu yok etmeden önce IdP/SSO, authentication, tenant/workspace audit, cihaz, browser/session ve ağ kanıtını koruyun.
- İlgili 30 günlük Compliance Logs penceresini derhal dışa aktarın ve ham dosyaları hash'leriyle koruyun.
- İzin verildiği ve mevcut olduğu ölçüde kapsam içi conversation-message/content kayıtlarını, GPT/proje durumunu, Library dosyalarını, memories ve app activity verisini çekin.
- Yürütme iddiasında bulunmadan önce tüm app/tool isteklerini aşağı akış sağlayıcı loglarıyla korele edin.

- Olay etkisini ciddi biçimde artırmıyor veya gerekli containment'ı geciktirmiyorsa volatil/oturum kanıtını mümkün olan en erken zamanda koruyun. Ardından hukuki ve olay müdahale yetkisine uygun biçimde oturum/token iptali, hesap devre dışı bırakma, secret rotasyonu veya retention/ayar değişikliklerini yapın.

2. Şüpheli Hassas Veri İfşası

- Kapsamdaki kesin konuşma, dosya, proje, GPT, app retrieval veya agent run'ını belirleyin.
- Kaynak veriyi koruyun ve kullanıcının bunu yapıştırıp/yükleyip yüklemediğini, ChatGPT'nin bir app'den getirip getirmediğini veya ajanın paylaşılan bağlantı üzerinden alıp almadığını belirleyin.
- Verinin nereye gittiğini belirleyin: yalnızca model yanıtı, shared link, indirilen dosya, dış app action, Slack/channel deployment veya başka bir aşağı akış sistemi.
- İfşanın ChatGPT dışına uzanıp uzanmadığını belirlemek için DLP, file-access, SaaS audit, e-posta, repository ve endpoint telemetrisini kullanın.

3. Şüpheli Ajan / Bağlı Uygulama Kötüye Kullanımı

- Ajan/GPT yapılandırmasını, etkin uygulamaları, scope'ları, authentication modelini, approval ayarlarını, action kısıtlarını, schedule/trigger'ları ve varsa ilgili sürüm geçmişini yakalayın.
- Zinciri yeniden kurun: güvenilmeyen girdi -> model/ajan kararı -> app request -> provider execution -> ortaya çıkan change/egress.
- Hem ChatGPT kanıtını hem dış servisin audit trail'ini koruyun; ikisini tek bir anlatı kaynağı gibi birleştirmeyin.

Hazırlık Kontrol Listesi

- **Dışa aktarma:** Compliance Logs Platform verisini ayrı korunan SIEM/veri gölüne sürekli alın; alım durursa alarm üretin.
- **İzinler:** uygun scope'lu Admin anahtarlarını önceden oluşturun ve conversation-message ile audit/auth/app kategorilerine kimin erişebildiğini dokümante edin.
- **Saklama:** workspace retention, deletion davranışı, Temporary Chat, file/Library davranışı ve özelliğe özgü istisnaları dokümante edin.
- **Kimlik:** IdP/SSO, SCIM, cihaz posture, VPN/proxy/SASE ve EDR telemetrisini ChatGPT olay ufkundan daha uzun tutun.
- **Uygulamalar:** etkin app/plug-in'leri, OAuth scope'larını, shared/agent-owned bağlantıları, write approval'ları ve provider-side audit log retention'ını envanterleyin.
- **Ajanlar:** agent configuration/versioning, schedule/trigger, app constraints ve varsa analytics verisini koruyun.
- **Test:** 30/90/180 günlük bir rekonstrüksiyon egzersizi yapın ve kanıtın gerçekten geri getirilebilir ve atfedilebilir olduğunu ispatlayın.

Ufuk Sınırlayıcıları

Sınırlayıcı	Adli sonuç
Compliance loglarının sürekli dışa aktarılmaması	Yerel 30 günlük pencere yaşlanır; tarihsel audit olayları kalıcı olarak kaybolabilir.
Konuşma/dosya retention süresinin kısa olması	Daha üst düzey aktivite kalsa bile prompt, yanıt ve kaynak belge rekonstrüksiyonu başarısız olabilir.

Sınırlayıcı	Adli sonuç
Temporary Chat	Sıradan geçmiş olmayabilir; Enterprise Compliance API ufku 30 gün olarak dokümante edilmiştir.
Geçici dosya süresinin dolması	Sohbet kalırken yüklenen nesne Compliance API'den geri getirilemeyebilir.
App/provider loglarının kısa olması	ChatGPT'nin eylem istediği bilinebilir ama aşağı akış yürütme veya etki kanıtlanamayabilir.
Shared / agent-owned credentials	Dış eylem, başlatan insandan ziyade servis/paylaşılan kimliğe atfedilebilir.
Zayıf endpoint/IdP retention	ChatGPT kayıtları kalsa bile kullanıcı atfı ve session-context rekonstrüksiyonu bozulur.

Hızlı Referans

Kaynak	En iyi soru	Öncelik
Compliance Logs Platform	Son 30 günde hangi desteklenen aktivite gerçekleşti?	Kritik - sürekli dışa aktarın
Conversation-message/content data	Kullanıcı/model gerçekte ne söyledi veya ne sakladı?	Yüksek
Authentication / admin logs	Ortama kim erişti veya neyi değiştirdi?	Yüksek
Files / Library / GPT / project evidence	Hangi kaynak materyal veya kalıcı bağlam devredeydi?	Yüksek
App + provider logs	Dış eylem gerçekten yürütüldü mü?	Ajan vakalarında kritik
Endpoint / IdP / EDR	Aktivitenin arkasında hangi insan/oturum/cihaz vardı?	Temel doğrulayıcı

Kaynaklar ve Doğrulama Notları

OpenAI dokümantasyonu 29 Ağustos 2026 tarihinde gözden geçirilmiştir. Plan yetkileri, şemalar, ürün adları ve saklama davranışı hızla değiştiğinden her vakada bu kaynakları yeniden açın.

1. OpenAI - Enterprise privacy
   https://openai.com/enterprise-privacy/
2. OpenAI Help - Compliance Platform for Enterprise and Edu
   https://help.openai.com/en/articles/9261474-openai-compliance-platform-for-enterprise-and-edu-customers
3. OpenAI - New compliance and administrative tools for ChatGPT Enterprise
   https://openai.com/index/new-tools-for-chatgpt-enterprise/
4. OpenAI Help - Chat and File Retention Policies in ChatGPT
   https://help.openai.com/en/articles/8983778-chat-and-file-retention-policies-in-chatgpt
5. OpenAI Help - Temporary Chat FAQ
   https://help.openai.com/en/articles/8914046-temporary-chat-faq
6. OpenAI Help - Data sharing and privacy for apps in ChatGPT
   https://help.openai.com/en/articles/20001496-data-sharing-and-privacy-for-apps-in-chatgpt
7. OpenAI Help - Admin controls, security, and compliance for apps
   https://help.openai.com/en/articles/11509118-admin-controls-security-and-compliance-in-apps-enterprise-edu-and-business
8. OpenAI Help - ChatGPT Workspace Agents for Enterprise and Business
   https://help.openai.com/en/articles/20001143-chatgpt-workspace-agents-for-enterprise-and-business
9. OpenAI Help - Enterprise compliance information for ChatGPT record mode
   https://help.openai.com/en/articles/11664471-enterprise-compliance-information-for-chatgpt-record-mode

10. OpenAI Help - ChatGPT Enterprise admin quickstart
https://help.openai.com/en/articles/20001264-chatgpt-enterprise-admin-quickstart
11. OpenAI Help - Exporting your ChatGPT history and data
https://help.openai.com/en/articles/7260999-how-do-i-export-my-chat-history-and-data

Yayın notu

Bu bölüm, bağımsız bir Forensic Horizon çalışmasının Türkçe çevirisidir. OpenAI ile bağlantılı değildir ve OpenAI tarafından onaylanmamıştır. ChatGPT, OpenAI ve ilgili ürün adları ilgili hak sahiplerinin ticari markalarıdır.

Forensic Horizon Hakkında

Forensic Horizon, bir kurumun bir siber olayı ne kadar geriye doğru güvenilir ve savunulabilir biçimde yeniden kurabileceğini ölçen bir Cyber Evidence Assurance yaklaşımıdır. Kimlik, uç nokta, ağ, bulut, SaaS, e-posta, yedek ve güvenlik telemetrisi genelinde kanıtı değerlendirerek aranabilir, geri getirilebilir, savunulabilir ve senaryoya özgü rekonstrüksiyon ufuklarını belirler.

Horizon Series:

Google Gemini

Gemini for Google Workspace ve Vertex AI genelinde kanıt kaynakları, logging, retention ve adli görünürlük ufku sınırlayıcıları için pratik bir kılavuz.

HIZLA DEĞİŞEN PLATFORM UYARISI

Yapay zekâ platformları, ürün adları, plan yetkileri, olay şemaları, API'ler, saklama kuralları, yerel artefaktlar ve bağlı uygulama davranışları hızla değişebilir. Bu bölüm **28 Ağustos 2026** tarihinde doğrulanan kaynak çalışmayı temel alır. Bir soruşturmada herhangi bir yol, alan, izin, saklama süresi veya davranışa güvenmeden önce güncel üretici dokümantasyonunu ve canlı ortamı yeniden doğrulayın.

Sürüm: 1.0
Tarih: Ağustos 2026
TLP: CLEAR

Forensic Horizon × Sparta Siber Güvenlik

Yönetici Özeti

DOĞRULAMA UYARISI - KULLANMADAN ÖNCE OKUYUN

Google; Gemini ürün adlarını, Workspace yetkilerini, logging şemalarını, Vault desteğini, Cloud Audit Log kapsamını, ajan servislerini ve request/response logging özelliklerini sık değiştirir. Kaynak çalışma 28 Ağustos 2026 tarihinde Google dokümantasyonuyla doğrulanmıştır. Gerçek incelemede her event adı, retention süresi, API metodu ve logging yapılandırmasını yeniden doğrulayın.

- **Kanıt düzlemlerini hemen ayırın:** Workspace uygulamalarındaki Gemini, yönetilen Workspace hesabındaki Gemini app, Gemini for Google Cloud/Code Assist ve Vertex AI/ajan platformları üzerinden kullanılan Gemini modelleri farklı loglar üretir.
- **Workspace artık Gemini'ye özgü utilization loglarına sahiptir:** Admin Reports API uygulaması `gemini_in_workspace_apps`, 180 güne kadar dönen geçmişle Gemini kullanım olaylarını kaydeder. Bu kullanım telemetrisidir; transcript deposu değildir.
- **Gemini kullanımından belge erişimi çıkarsamayın:** sıradan Drive, Gmail, login, device ve Admin logları destekleyici kanıttır. Belirli event şeması bunu ispatlamadıkça Gemini'nin bağlam olarak kullandığı her öğenin garantili kaydı şeklinde yorumlanmamalıdır.
- **Gemini app konuşmaları eDiscovery kaynağı olabilir:** Google Vault, desteklenen Workspace yapılandırmalarında Gemini app prompt ve yanıtları için retention ve hold destekler.
- **Vertex AI adli görünürlüğü yapılandırmaya bağlıdır:** Cloud Audit Logs idari ve erişim aktivitesini gösterir; inference düzeyinde kalıcı kanıt için Data Access logging ve request/response logging desteklendiği yerde özellikle etkinleştirilmelidir.

Forensic Horizon ilkesi

"Gemini kullanıldı" ile "Gemini'nin tam olarak ne gördüğünü ve ne döndürdüğünü yeniden kurabiliyoruz" farklı delil ifadeleridir. Boşluğu açıkça belgeleyin.

Mimari ve Kapsam

Gemini yüzeyi	Tipik kullanım	Birincil kanıt
Workspace uygulamalarında Gemini	Gmail, Docs, Drive, Sheets, Slides, Meet vb. içindeki side panel/AI özellikleri	Gemini-in-Workspace kullanım audit event'leri + destekleyici Workspace logları
Yönetilen hesapta Gemini app	Workspace core service olarak gemini.google.com / mobil	Gemini activity, desteklendiği yerde Vault-retained conversations, admin/login evidence
Gemini for Google Cloud / Code Assist	Google Cloud araçlarında geliştirici yardımı	Gemini for Google Cloud audit logları; opsiyonel prompt/response logging to Cloud Logging
Vertex AI Gemini	Google Cloud üzerinden Gemini modellerini çağıran uygulamalar	Cloud Audit Logs, Data Access logs, request/response logging, application traces
Agent platformları / reasoning engines	Tool kullanan kurumsal ajanlar ve orchestration	Agent-platform audit/usage logları + downstream tool/service logları

Tehdit Soruları

- **Hesap ele geçirilmesi:** Yönetilen bir kimlik, ele geçirilmeden sonra Gemini çağırmak veya Workspace verisine erişmek için kullanıldı mı?

- **Veri ifşası:** Hangi içerik Gemini konuşmasına kondu, grounding/context olarak kullanıldı veya model tarafından döndürüldü?
- **Prompt injection / ajan kötüye kullanımı:** Hangi güvenilmeyen girdi model bağlamına girdi, hangi tool call istendi ve aşağı akışta hangi eylem gerçekten yürüdü?
- **API kötüye kullanımı:** Hangi principal/service account, nereden, hangi project/model'e ve hangi hacimde Gemini çağrısı yaptı?
- **Savunmadan kaçınma:** Audit ayarları, sink'ler, retention kuralları veya service-account izinleri olay öncesinde ya da sırasında değiştirildi mi?

Google Workspace İçinde Gemini: Gerçekte Ne Loglanıyor?

En güçlü yerel Workspace kanıtı, Admin Reports API üzerinden sunulan Gemini'ye özgü aktivite akışıdır. Google uygulama adını `gemini_in_workspace_apps` olarak dokümante eder. Loglar 20 Haziran 2025'ten itibaren ve 180 güne kadar dönen geçmişle kullanılabilir.

Alan / kavram	Adli değer	Önemli sınırlama
feature_utilization event	Kullanıcının bir Workspace app içinde Gemini kullanarak işlem yaptığını gösterir.	Kullanım telemetrisidir; kelimesi kelimesine prompt/response transcript değildir.
action / app name	Workspace yüzeyini tanımlar (ör. Gmail, Docs, Drive, Sheets, Slides).	Tek başına tam olarak hangi alttaki öğenin bağlam olarak okunduğunu ispatlamaz.
event_category	summarize, generate, active conversation gibi geniş kullanım sınıflarını ayırır.	Kategori semantiği değişebilir; ham event JSON'unu koruyun.
feature_source	side panel, help me write, AI function vb. UI kökenini gösterir.	Scope belirlemek için ipucudur; uygulamaya özgü loglarla korele edin.
actor/timestamp context	Kullanımı yönetilen hesap ve zamanla ilişkilendirir.	Atıf yine identity/session/device kanıtına bağlıdır.

YAYGIN ADLİ VARSAYIMLARA DÜZELTME Standart Drive veya Gmail audit olayları, Gemini'nin iç bağlam olarak tükettiği her dosya veya mesajın garantili logu gibi sunulmamalıdır. Invocation'ı göstermek için Gemini'ye özgü usage event'lerini; Drive/Gmail/application loglarını ise yalnızca dokümante edilmiş event semantiğinin desteklediği iddialar için kullanın. Event şeması doğrudan erişilen nesneyi tanımlamıyorsa sonuçları "... ile tutarlı" şeklinde ifade edin.

Gemini App Konuşmaları ve Vault

Desteklenen Workspace dağıtımlarında Google Vault, kullanıcı prompt'ları ve Gemini yanıtlarından oluşan Gemini app konuşmalarını saklayabilir. Vault retention rules ve holds sıradan conversation-history görünürlüğünü aşabilir. Bu, Gemini-in-Workspace utilization loglarından farklı bir kanıt kaynağıdır ve chat içeriğinin geri getirilebilir ufkunu ciddi biçimde uzatabilir.

Kaynak	Neyi gösterir	Retention / uyarı
Gemini app activity / conversation history	Yönetilen kullanıcı için hangi konuşmaların mevcut olduğunu ve ne zaman gerçekleştiğini.	Admin kontrollü history 3, 18 veya 36 ay olabilir; güncel politikayı doğrulayın.
Google Vault - Gemini app	Desteklenen sürümlerde eDiscovery için prompt/response search/export/hold.	Custom/default Vault retention mesajları belirli süreler veya süresiz tutabilir.

Kaynak	Neyi gösterir	Retention / uyarı
Workspace Gemini usage logs	Hangi Workspace AI özelliğinin kim tarafından, hangi app/category içinde kullanıldığını.	180 güne kadar dönen geçmiş.
Admin / Login / Device logs	Policy değişiklikleri, authentication ve device context.	Destekleyici atıf kanıtı; retention log türü/sürüme göre değişir.

Vertex AI ve Gemini API Adli Bilişimi

Geliştirici iş yüklerinde kanıt Google Cloud'a taşınır. Temel sorular şunlardır: hangi principal servisi çağırdı, hangi project/location/model hedeflendi, request ve response gövdeleri korunmuş muydu ve hangi aşağı akış tool/application action izledi?

Cloud Audit Logs

- **Admin Activity**, Google Cloud servisleri için idari değişiklikleri kaydeder ve desteklenen işlemlerde varsayılan olarak etkindir.
- **Data Access**, desteklenen metotlarda user-provided data'ya read/write erişimini kaydeder; ancak incelemeciler bunu genel olarak etkin varsaymamalıdır. Vertex AI / ilgili Gemini servisi için gerçek audit yapılandırmasını doğrulayın.
- Vertex AI aktivitesi için servis adı yaygın olarak `aiplatform.googleapis.com`'dur. Gemini for Google Cloud / Code Assist için Google `cloudaicompanion.googleapis.com` adını dokümante eder.
- Base Gemini modellerinde inference metotları `GenerateContent` ve `StreamGenerateContent` kullanır. Legacy `Predict` / `RawPredict` filtrelerini evrensel Gemini sorgusu olarak kullanmayın.

Örnek Logs Explorer filtreleri

```
protoPayload.serviceName="aiplatform.googleapis.com"
protoPayload.methodName:"GenerateContent"
```

Projenizde yakalanan gerçek log şemasına göre substring/exact method matching kullanın. Detection kuralını standardize etmeden önce örnek bir ham event'i koruyun.

Request / Response Logging

Desteklendiği yerde Google, Gemini model çağrıları için request-response logging sunar. Güncel dokümantasyon `generateContent` veya `streamGenerateContent` kullanan Gemini modellerini; BigQuery'ye yönlendirilen logları ve bazı ürün varyantlarında opsiyonel OpenTelemetry entegrasyonunu açıklar. Bu kaynak, incelemeyi "bir model çağrıldı" düzeyinden "loglanan prompt/response payload budur" düzeyine taşıyabilir.

> **GİZLİLİK VE MALİYET DENGESİ** Payload logging; hassas prompt'ları, retrieved context'i, model output'larını ve potansiyel secret'ları yakalayabilir. Full payload capture açılmadan önce retention, erişim kontrolü, sampling, encryption, DLP ve legal basis tasarlanmalıdır. Forensic readiness kontrolsüz ikincil bir data lake yaratmamalıdır.

Gemini for Google Cloud / Code Assist

Google, Gemini for Google Cloud için ayrı logging destekler. Prompt/response logging etkinleştirildiğinde user input, contextual information ve responses Cloud Logging'e gönderilebilir. Google bunu Vertex AI içindeki Gemini'den açıkça ayırır; logging kontrolleri ürüne özgüdür. Her Gemini yüzeyini ayrı bir evidence pipeline olarak ele alın.

Ajan ve Prompt-Injection İncelemeleri

Prompt injection bir nedensellik zinciri problemidir. Savunulabilir bir rekonstrüksiyon; güvenilmeyen kaynağı, model bağlamını, model/tool kararını, aşağı akış yürütmeyi ve oluşan veri değişikliği veya egress'i ayırmalıdır.

Aşama	Kanıt / örnek	Soru
1. Güvenilmeyen girdi	E-posta/belge/web/RAG kaynağı, attachment hash, database row, URL	Ajan bağlamına hangi içerik girdi?
2. Model invocation	Gemini usage event, Cloud Audit Log, application trace	Modeli kim/ne çağırdı ve ne zaman?
3. Prompt/ response	Vault conversation, request-response log, varsa application trace	Model hangi kesin instruction/context'i aldı ve ne döndürdü?
4. Tool decision	Agent trace, function-call payload, orchestration logs	Model hangi tool/function'ı istedi?
5. Execution	Cloud Run/Functions/GKE logs, DB audit, SaaS audit, endpoint telemetry	Gerçekte ne çalıştı ve hangi kimlikle?
6. Effect	File/data changes, outbound network, IAM changes, exfil destination	Ne değişti veya ortamdan ne çıktı?

Taktik Playbook: Yönetilen Workspace Hesabı Ele Geçirilmesi

- Containment session state'i değiştirmeden önce olay penceresine ait login, token, device, admin-policy ve Gemini-specific usage loglarını koruyun.
- Gemini özelliklerinin ne zaman ve nerede kullanıldığını belirlemek için `gemini_in_workspace_apps` event'lerini export/query edin.
- Gemini app kapsamdaysa hukuken yetkili olunan durumda uygun Vault hold uygulayın / saklanan konuşmaları koruyun.
- Drive/Gmail/Docs event'leriyle yalnızca şemalarının object access/modification'ı gerçekten ortaya koyduğu ölçüde korele edin; görünmez internal context fetch'leri varsaymayın.
- Koruma adımlarından sonra olayın ciddiyetine uygun şekilde session/token iptali ve account containment uygulayın.

Taktik Playbook: Vertex AI / Ajan Kötüye Kullanımı

- Resource'ları devre dışı bırakmadan önce Cloud Audit Logs, mevcut sink'ler, request-response logs, application traces ve downstream service logs'u koruyun.
- Principal, service account, project, region, model, API method, source network context ve request volume'u belirleyin.
- Payload logging varsa prompt ve response'u yeniden kurun; yoksa metadatadan anlatı üretmek yerine içerik boşluğunu belgeleyin.
- Her function/tool call'ı gerçekte çalıştıran sisteme kadar takip edin; model request execution ile aynı şey değildir.
- Kanıt koruma gereksinimleri karşılandıktan sonra ele geçirilmiş credential'ları rotate edin, IAM scope'u azaltın ve agent/runtime'ı izole edin.

Hazırlık Kontrol Listesi

- **Workspace:** Gemini'ye özgü audit event'lerinin Admin Reports/Security tooling üzerinden erişilebilir olduğunu ve 180 günlük pencere dolmadan dışa aktarıldığını doğrulayın.
- **Vault:** Gemini app konuşmaları için retention rule veya hold gerekip gerekmediğine karar verin; olay olmadan search/export test edin.
- **Cloud:** Vertex AI ve kullandığınız tüm Gemini/agent servislerinde Data Access audit yapılandırmasını özellikle inceleyin.
- **Payloads:** request-response logging'in gerekçesini değerlendirin; etkinse least-privilege erişimli kontrollü uzun dönem depoya yönlendirin.
- **Log sinks:** kritik audit logları bağımsız korunan proje/SIEM'e aktarın; ele geçirilen workload identity tek kopyayı silememelidir.
- **Identity:** mümkünse long-lived service-account key kullanmayın; IAM değişiklikleri ve credential creation'ı izleyin.
- **Agents:** tool call'ları ve downstream execution'ı ayrı ayrı loglayın. MCP, Cloud Run, Functions, database, SaaS ve network evidence'ı koruyun.
- **Test:** geçmiş verinin gerçekten retrievable ve attributable olduğunu kanıtlamak için 90/180 günlük rekonstrüksiyon egzersizi yapın.

Ufuk Sınırlayıcıları

Sınırlayıcı	Sonuç
180 günlük Workspace Gemini kullanım penceresi	Daha eski feature-use metadatası dışa aktarılmazsa yaşlanır.
Vault retention yok / desteklenmeyen edition	Prompt/response içeriği yönetilen Workspace servisinden geri getirilemeyebilir.
Data Access audit devre dışı	Inference-level access metadata eksik olabilir.
Request-response logging etkin değil	Cloud-native loglardan tam prompt/output rekonstrüksiyonu imkânsız olabilir.
Uygulama trace saklamıyor	Model call görünse bile tool/function kararları eksik olabilir.
Downstream service logları kısa	Ajanın ne istediği bilinir, fakat neyin gerçekten çalıştığı ispatlanamayabilir.
Shared / zayıf service-account attribution	Aktivite workload identity'ye bağlanır ancak başlatan insan/session güvenilir biçimde belirlenemez.

Hızlı Referans

Kaynak	En iyi kullanım	Sınırlama
gemini_in_workspace_apps	Workspace Gemini feature usage'ı belirlemek	180 günlük rolling history; verbatim transcript değil
Google Vault - Gemini app	Prompt/response koruma ve arama	Edition/configuration dependent
Admin/Login/Device logs	Attribution ve policy timeline	Destekleyici kanıt; Gemini content değildir
Vertex AI Cloud Audit Logs	Principal, method, resource, admin/data access	Data Access configuration önemlidir

Kaynak	En iyi kullanım	Sınırlama
Request-response logging	Yapılandırıldıysa prompt/output payload	Hassas; sampled veya absent olabilir
Gemini for Google Cloud logs	Logging etkinse Code Assist/Cloud-assistant prompt, response ve metadata	Vertex AI kontrollerinden ayrıdır
Application/agent traces	Tool decision ve orchestration	Olay öncesi instrumentation kalitesi kadar iyidir
Downstream service logs	Gerçek execution/effect'i ispatlamak	Retention çoğu zaman asıl horizon limiter'dır

Kaynaklar ve Doğrulama Notları

Google dokümantasyonu 28 Ağustos 2026 tarihinde incelenmiştir. Şemalar ve ürün adları hızlı değiştiği için her vakada yeniden açın.

1. Google Workspace Admin Reports API - Gemini in Workspace Apps Activity Events
   https://developers.google.com/workspace/admin/reports/v1/appendix/activity/gemini-in-workspace-apps
2. Admin Reports API - activities.list
   https://developers.google.com/workspace/admin/reports/reference/rest/v1/activities/list
3. Google Vault - Retain Gemini app messages
   https://support.google.com/vault/answer/16677125
4. Google Workspace - Turn Gemini app on/off and conversation history
   https://support.google.com/a/answer/14571493
5. Google Cloud - Gemini for Google Cloud logs
   https://docs.cloud.google.com/gemini/docs/log-gemini
6. Google Cloud - Gemini for Google Cloud audit logging
   https://docs.cloud.google.com/gemini/docs/audit-logging
7. Google Cloud - Enable Data Access audit logs
   https://docs.cloud.google.com/logging/docs/audit/configure-data-access
8. Vertex AI - Request-response logging
   https://docs.cloud.google.com/gemini-enterprise-agent-platform/models/capabilities/request-response-logging
9. Vertex AI RPC - PredictionService / GenerateContent
   https://docs.cloud.google.com/vertex-ai/generative-ai/docs/reference/rpc/google.cloud.aiplatform.v1

Yayın notu

Bu bölüm, bağımsız bir Forensic Horizon çalışmasının Türkçe çevirisidir. Google ile bağlantılı değildir ve Google tarafından onaylanmamıştır. Google, Google Workspace, Gemini ve Google Cloud ilgili hak sahiplerinin ticari markalarıdır.

Forensic Horizon Hakkında

Forensic Horizon, bir kurumun bir siber olayı ne kadar geriye doğru güvenilir ve savunulabilir biçimde yeniden kurabileceğini ölçen bir Cyber Evidence Assurance yaklaşımıdır. Kimlik, uç nokta, ağ, bulut, SaaS, e-posta, yedek ve güvenlik telemetrisi genelinde kanıtı değerlendirerek aranabilir, geri getirilebilir, savunulabilir ve senaryoya özgü rekonstrüksiyon ufuklarını belirler.

Horizon Series:

Claude

Claude Enterprise ve Claude Code genelinde kanıt kaynakları, logging, retention ve adli görünürlük ufku sınırlayıcıları için pratik bir kılavuz.

HIZLA DEĞİŞEN PLATFORM UYARISI

Yapay zekâ platformları, ürün adları, plan yetkileri, olay şemaları, API'ler, saklama kuralları, yerel artefaktlar ve bağlı uygulama davranışları hızla değişebilir. Bu bölüm **28 Ağustos 2026** tarihinde doğrulanan kaynak çalışmayı temel alır. Bir soruşturmada herhangi bir yol, alan, izin, saklama süresi veya davranışa güvenmeden önce güncel üretici dokümantasyonunu ve canlı ortamı yeniden doğrulayın.

Sürüm: 1.1
Tarih: Ağustos 2026
TLP: CLEAR

Forensic Horizon × Sparta Siber Güvenlik

Yönetici Özeti

DOĞRULAMA UYARISI - KULLANMADAN ÖNCE OKUYUN

Anthropic; Claude ürünlerini, plan yetkilerini, API'leri, varsayılan ayarları, yerel dosya düzenlerini ve retention davranışını hızla değiştirir. Kaynak çalışma, 28 Ağustos 2026 tarihinde gözden geçirilen vendor dokümantasyonu ve sağlanan endpoint araştırmasını temel alır. Her path, retention değeri, event type ve API davranışını gerçek soruşturma sırasında canlı tenant ve güncel Anthropic dokümantasyonuna karşı doğrulanması gereken bir hipotez olarak ele alın.

- **İki kanıt düzlemi önemlidir:** yönetilen Claude Enterprise / claude.ai kanıtı ile Claude Code / Desktop uç nokta kanıtı. Hiçbiri tek başına yeterli değildir.
- **Enterprise audit-log CSV'leri kısa ufuklu kaynaktır:** UI export son 180 günü birleştirir ve chat/project content'i dışarıda bırakır.
- **Compliance API ufku ciddi biçimde değiştirir:** Activity Feed API etkinleştirildikten sonra 6 yıl saklanır; toplama retroaktif değildir. Content/session endpoint'leri, ürün retention ve availability koşullarına tabi olarak chats, files, projects ve managed Claude Code/Cowork transcripts sunar.
- **Claude Code uç noktaları zengin ama değiştirilebilirdir:** `~/.claude` altındaki local transcript'ler messages, tool calls, tool results ve çoğu zaman hassas içerik taşır; automatic cleanup yapılandırılabilir ve managed setting override etmezse yaygın olarak 30 gündür.
- **Yapılandırma kanıttır:** custom retention, history suppression, telemetry, tenant restrictions, managed settings ve user account context nelerin yeniden kurulabileceğini doğrudan etkiler.

Forensic Horizon ilkesi

Yalnızca hangi kanıtın var olduğunu değil, her kaynağın hangi tarihte **aranabilir, geri getirilebilir, atfedilebilir veya savunulabilir** olmaktan çıktığını da kaydedin.

Kapsam ve İnceleme Sınırları

Bu bölüm Claude.ai Team/Enterprise workspace'leri, Claude Code ve Claude Desktop endpoint artefaktlarına odaklanır. Workspace içeriğini ve managed local-session transcript'lerini sunduğu ölçüde Claude Compliance API de kapsanır. Yalnızca API kullanan iş yükleri, third-party hosting platformları ve olası her MCP server ayrıntılı olarak kataloglanmamıştır.

ASSISTANT KANITI İLE HOST KANITINI KARIŞTIRMAYIN Claude Code transcript'i Claude Code içinden ne geçtiğini kanıtlar; başka hiçbir process'in aynı veriye erişmediğini, değiştirmediğini veya dışarı çıkarmadığını kanıtlamaz. EDR, shell history, identity, repository, network, cloud ve MCP-server telemetry ile korele edin.

Kapsam Soruları

Soru	Birincil Claude kanıtı	Doğrulayıcı kanıt
Hesap ele geçirilmesi	Enterprise audit logs / Compliance Activity Feed; directory state	IdP, device posture, EDR, browser/session evidence
Hangi veri Claude'a ulaştı?	Compliance content/session endpoint'leri; local transcripts ve caches	DLP, file access, repository, endpoint telemetry

Soru	Birincil Claude kanıtı	Doğrulayıcı kanıt
Savunmadan kaçınma	Retention-setting event'leri; managed settings; missing/suppressed local artifacts	Change management, MDM, EDR, SIEM
Agentic coding abuse	Claude Code transcript, file-history, OTel etkinse, Compliance session transcript	Shell/process telemetry, Git, CI/CD, MCP logs

Kanıt Mimarisi ve Saklama

Anthropic, farklı lookback karakteristiklerine sahip birkaç kanıt sınıfı sunar. 180 günlük CSV export ile Compliance Activity Feed arasındaki fark operasyonel olarak önemlidir.

Kanıt kaynağı	Neyi içerir	Adli görünürlük ufku / uyarı
Audit log CSV export	Authentication, organization, project, conversation ve file events; content yerine identifiers/metadata	Yalnızca Enterprise; export anında önceki 180 gün.
Compliance API Activity Feed	Authentication, chat, file, project, admin ve platform activity	Vendor docs: enablement sonrası 6 yıl retention; retroactive değil.
Compliance content endpoints	Chats, file uploads, projects, attachments	Enterprise; retained content ve permissions'a tabidir.
Compliance session endpoints	Managed Claude Code ve Cowork session transcripts	Uygun managed session'lar yakalanır; personal-account use tenant visibility dışındadır.
Organization data export	Removed user data dahil, tutulduğu yerde bulk chat/project holdings	Point-in-time preservation; retention'a tabidir.
Claude Code local data	Session JSONL, file-history, caches, task/plan data, history	User-writable plaintext. Birçok path'e auto-cleanup uygulanır; effective value kontrol edilmelidir.
OpenTelemetry	Yapılandırılmışsa centralized usage/event telemetry	Birçok deployment'ta off by default; content fields settings'e bağlıdır.
Desktop app data	Application state, logs, MCP config ve product-specific local state	OS/version dependent; acquired image üzerinde path doğrulayın.

Claude Code: Yüksek Değerli Yerel Artefaktlar

Güncel Claude Code dokümantasyonu application data'yı `~/.claude` altında tanımlar. Dosyalar plaintext olduğundan değerli, volatil ve integrity-sensitive'dir.

Path / artefakt	Adli değer	Cleanup davranışı
projects/…/*.jsonl	Tam conversation transcript: messages, tool calls ve tool results. Hassas file content veya command output burada görünebilir.	`cleanupPeriodDays` değerinden eskiyse startup sırasında silinebilir.
projects/…/tool-results/	Ana transcript'ten taşan büyük tool output'ları.	Cleanup'ı izler.
file-history/	Checkpoint restore için pre-edit snapshot'lar.	Cleanup'ı izler.

Path / artefakt	Adli değer	Cleanup davranışı
paste-cache/ / image-cache/	Büyük pasted content ve attached images.	Cleanup'ı izler.
plans/ / tasks/ / session-env/	Agent plans, task state ve session metadata.	Cleanup'ı izler.
shell-snapshots/	Captured shell environment; crash leftovers yararlı olabilir.	Clean exit'te kaldırılır; sweep leftovers'ı temizler.
history.jsonl	Yazılan prompt'lar, timestamp ve project path.	Güncel docs automatic cleanup kapsamı dışında listeler; silinene/purge edilene kadar kalabilir.
stats-cache.json	Aggregate token/cost usage.	Silinene kadar kalır.
backups/	Config migration'lar çevresinde `~/.claude.json` kopyaları.	Güncel docs cleanup-managed data arasında listeler; gerçek sürüm davranışını doğrulayın.

BÜTÜNLÜK UYARISI Yerel Claude Code kanıtı kullanıcı tarafından yazılabilir/değiştirilebilir. Transcript eksik, düzenlenmiş, silinmiş veya bastırılmış olabilir. Yalnızca varlığına dayanarak evidentiary weight vermeyin; timestamps/events'i centralized telemetry, EDR, shell/process logs, repository history ve varsa Compliance API ile doğrulayın.

Kurumsal Kanıt Kaynakları

1. Audit log export

Organization Owners ve Primary Owners, Claude.ai üzerinden organization audit loglarını dışa aktarabilir. İncelenen Anthropic dokümantasyonuna göre export önceki 180 günün event'lerini birleştirir. Chat/project titles ve content hariç tutulur; identifiers ve contextual metadata sağlanır. CMEK-enabled organizations UI export düğmesini kullanamaz ve bunun yerine API üzerinden erişilebilen audit event'leri kullanmalıdır.

2. Compliance API Activity Feed

Etkin olduğunda tercih edilen kalıcı event kaynağı Activity Feed'dir. Bu sürüm için incelenen Anthropic dokümantasyonu, activity'lerin olaydan kısa süre sonra query edilebilir olduğunu ve 6 yıl saklandığını belirtir. Recording, Compliance API enable edildiğinde başlar ve retroactive değildir. Bu ayrım, feed'in workspace-content retention'ı yalnızca aynaladığı yönündeki yaygın yanlış algıyı düzeltir.

3. Compliance content ve session endpoint'leri

Enterprise Compliance Access Keys; claude.ai chats, files, projects, project attachments ve uygun Cowork/Claude Code session transcript'lerini açabilir. Audit identifiers'ı content'e çözmek ve user deletion/offboarding availability'yi değiştirmeden önce centrally captured managed-session evidence'ı korumak için kullanın.

4. Organization exports

Primary Owner export'ları bulk conversation ve project content'i koruyabilir. Removed users verisi organization policy altında hâlâ retained ise dahil kalabilir. Export çalıştırılmasını hassas bir administrative action olarak değerlendirin ve audit event'lerle korele edin.

Kanıt Ufku Değiştiren Kontroller

Kontrol	Neden önemlidir
Custom Enterprise retention	Varsayılan workspace data retention custom policy yoksa indefinite'tır; minimum custom retention 30 gündür. Süreyi kısaltmak out-of-window data'yı hemen silebilir.
Compliance API enablement	Activity Feed retention uzundur ancak logging yalnızca enablement sonrası başlar. Retroactive backfill yoktur.
CMEK	Collection procedures'ı değiştirir ve key availability'yi kanıt erişimi için pratik önkoşul haline getirebilir.
cleanupPeriodDays	Local Claude Code application-data cleanup'ını kontrol eder. Nominal default yerine effective managed settings'i kontrol edin.
CLAUDE_CODE_SKIP_PROMPT_HISTORY / no-session-persistence	Local transcript/history creation'ı bastırabilir. Yerel dosya yokluğu kullanım olmadığına kanıt değildir.
OpenTelemetry settings	Centralized event telemetry'nin olup olmadığını ve hangi content/details taşıdığını belirler.
Personal vs managed accounts	Kurumsal host üzerindeki personal-account Claude kullanımı enterprise tenant evidence'da görünmeyebilir; endpoint collection kritik hale gelir.
Incognito chats	Normal chat history'de görünmez; Anthropic Enterprise incognito chats'in en az 30 gün veya custom retention'a göre daha uzun saklandığını ve Compliance API/org exports'a dahil olduğunu belirtir.

Zaman Baskısı Altında Toplama

- **Önce control state'i koruyun.** Effective retention, Compliance API status, managed settings, telemetry settings, tenant/account context ve current time zone'u kaydedin.
- **180 günlük audit-log window'u hemen export edin.** Bu sabit kayan bir penceredir.
- **Compliance Activity Feed ve kapsam içi content/session data'yı çekin.** Hukuken uygun olduğu ölçüde IDs, timestamps, actor metadata ve raw API responses'ı koruyun.
- **Cleanup veya user action'dan önce endpoint evidence edinin.** `~/.claude`, Desktop application data, logs ve ilgili MCP-server evidence'ı copy/image edin; file metadata ve hashes'i koruyun.
- **Korele edin.** IdP, EDR, shell, filesystem, Git, cloud, network, DLP ve application evidence ile timeline oluşturun.
- **Yalnızca bundan sonra disruptive actions uygulayın.** Offboarding, purge commands, retention changes veya application uninstall kanıtı yok edebilir.

Ufuk Sınırlayıcı Kontrol Listesi

Sınırlayıcı	Sonuç
180 günlük UI audit export	Pencere dışındaki administrative/access event'leri bu export üzerinden kullanılamaz.
Compliance API geç etkinleştirildi	Enablement öncesi activity için Activity Feed backfill yoktur.
Local cleanup	Endpoint transcript/cache geçmişi enterprise incident discovery'den çok önce kaybolabilir.

Sınırlayıcı	Sonuç
Suppressed persistence	Meşru bir configuration çok az veya hiç local transcript evidence üretebilir.
Personal account use	Enterprise tenant evidence personal account altında yapılan aktiviteyi kapsamayabilir.
Missing centralized telemetry	Local files mutable kalır ve tek başına defensibility gereksinimlerini karşılamayabilir.

Hızlı Referans

Kaynak	En iyi soru	Öncelik
Audit CSV	Son 180 günde kim sign-in yaptı / neyi değiştirdi?	Yüksek - erken export edin
Compliance Activity Feed	Enablement sonrası uzun ufuklu enterprise activity neydi?	Yüksek
Compliance content/ session	Retained chats ve managed sessions içinde model ne aldı/ döndürdü?	Yüksek
Claude Code transcript	Ajan bu endpoint'te ne istedi/yaptı/aldı?	Kritik ve volatil
history.jsonl	Session transcript aged out olsa bile hangi prompt'lar yazıldı?	Yüksek
file-history/caches	Hangi içerik geçti veya değiştirildi?	Yüksek ve volatil
OTel	Hangi centrally observed Claude Code event'leri endpoint'i doğrulayabilir?	Yapılandırıldıysa yüksek
EDR / shell / Git / MCP	Eylemler gerçekten çalıştı mı ve downstream ne değişti?	Temel doğrulayıcı

Kaynaklar ve Doğrulama Notları

Vendor dokümantasyonu 28 Ağustos 2026 tarihinde gözden geçirilmiştir. Ürün davranışı hızlı değiştiği için URL'ler yeniden doğrulama amacıyla verilmiştir.

1. Anthropic - Compliance API
   https://platform.claude.com/docs/en/manage-claude/compliance-api
2. Anthropic - Query the Activity Feed
   https://platform.claude.com/docs/en/manage-claude/compliance-activity-feed
3. Anthropic - Compliance API content/session data
   https://platform.claude.com/docs/en/manage-claude/compliance-content-data
4. Anthropic - Access audit logs
   https://support.claude.com/en/articles/9970975-access-audit-logs
5. Anthropic - Custom Enterprise retention
   https://support.claude.com/en/articles/10440198-configure-custom-data-retention-controls-for-enterprise-plans
6. Claude Code - Explore the .claude directory
   https://code.claude.com/docs/en/claude-directory
7. Claude Code - Manage sessions
   https://code.claude.com/docs/en/sessions
8. Anthropic - Incognito chats
   https://support.claude.com/en/articles/12260368-use-incognito-chats

Yayın notu

Bu bölüm, bağımsız bir Forensic Horizon çalışmasının Türkçe çevirisidir. Anthropic ile bağlantılı değildir ve Anthropic tarafından onaylanmamıştır. Claude ve Anthropic ilgili hak sahiplerinin ticari markalarıdır.

Forensic Horizon Hakkında

Forensic Horizon, bir kurumun bir siber olayı ne kadar geriye doğru güvenilir ve savunulabilir biçimde yeniden kurabileceğini ölçen bir Cyber Evidence Assurance yaklaşımıdır. Kimlik, uç nokta, ağ, bulut, SaaS, e-posta, yedek ve güvenlik telemetrisi genelinde kanıtı değerlendirerek aranabilir, geri getirilebilir, savunulabilir ve senaryoya özgü rekonstrüksiyon ufuklarını belirler.

KAYNAK VE ÇEVİRİ NOTU

Bu Türkçe Sürüm Hakkında

Bu belge, **Forensic Horizon tarafından hazırlanmış “AI Forensics Consolidated Guide” özgün İngilizce çalışmasının Türkçe çevirisi ve Sparta Siber Güvenlik ile ortak markalı yayın sürümüdür.**

Türkçe sürüm, kaynak metnin teknik içeriğini Türkçe okuyucu için erişilebilir kılmayı amaçlar; kaynak metnin 28-29 Ağustos 2026 doğrulama tarihlerini değiştirmez ve ayrı bir teknik güncelleme anlamına gelmez. Yapay zekâ platformları, ürün adları, yetkiler, API’ler, olay şemaları, saklama davranışları ve yerel artefaktlar hızla değişebildiğinden gerçek incelemelerde güncel vendor dokümantasyonu ve canlı ortam yeniden doğrulanmalıdır.

Özgün çalışma: **Forensic Horizon** - Cyber Evidence Assurance
Türkçe ortak markalı yayın: **Forensic Horizon × Sparta Siber Güvenlik**
www.forensichorizon.com | www.sparta.com.tr

Marka ve üretici bağımsızlığı

ChatGPT/OpenAI, Google/Gemini/Google Cloud ve Claude/Anthropic adları ilgili hak sahiplerinin ticari markalarıdır. Bu yayın söz konusu üreticilerle bağlantılı değildir ve onlar tarafından onaylanmış bir üretici dokümanı değildir.