

SÜRÜM 1.9 · 28 EKİM 2026

Colitu Güvenlik Teknik Belgesi

Güvenlik mimarisi, tehdit modeli ve gizlilik tasarımı

Colitu'yu kullanırken neye güvenmeniz gerektiği, kimin neyi görebildiği, Colitu'nun hangi saldırılara karşı koruma sağladığı, hangilerine karşı sağlamadığı ve iddialarımızı nasıl doğrulayabileceğiniz. Buradaki her ifade bugün yayımlanmış olanı anlatır. Eksik olan ya da olması gerekenden zayıf kalan bir şey varsa bunu açıkça belirtiyoruz.

SÜRÜM	SON GÜNCELLEME	GÜVENLİK İLETİŞİMİ
1.9	28 Ekim 2026	security@colitu.com

KAPSADIĞI SÜRÜMLER

Android 2.9.9 · Windows 3.0.5 · Linux 1.6.2 (beta) · iOS 5.9.7 (TestFlight) · 16 Ekim 2026 itibarıyla kontrol düzlemi, 7 Ekim 2026 itibarıyla node agent

KAYNAK KOD

Android, Windows ve Linux uygulamaları: github.com/colitu; iOS uygulaması: github.com/colitu/ios (tümü GPL-3.0). Sunucu yazılımı: kapalı kaynak.

0 Bir bakışta Colitu güvenliği

Aşağıdaki bölümlerin özeti. Yeşil: adı geçen her platformda anlatıldığı gibi çalışır. Sarı: kısmen ya da belirtilen sınırlarla. Kırmızı: henüz yok.

Açık kaynak uygulamalar	● Android, iOS, Windows ve Linux açık kaynaktır (GPL-3.0). Sunucu yazılımı kapalıdır.
Şifreli tünel	● Hysteria2, VLESS Reality, VLESS XHTTP, Trojan ve Shadowsocks 2022; yerleşik uygulamalarla (Xray-core, sing-box, Hysteria).
Trafik içeriği ve gezinme geçmişi	● Kaydedilmez. VPN sunucuları bağlantı başına log tutmaz.
Kullanıcı başına trafik hacmi	● Sunucu başına yaklaşık 15 saniyelik aralıklarla kaydedilir ve kota için 90 gün saklanır; sonrasında yalnızca dönem toplamları kalır.
Tünel üzerinden DNS	● Android ve iOS uygulamalarında ve TUN modunda evet. Sistem proxy modunda proxy dışında kalan uygulamalar için hayır (Linux'ta varsayılan; yeni Windows kurulumları TUN modunda başlar).
IPv6 sızıntı koruması	● Android ve iOS'ta, ayrıca Windows ve Linux'ta kill switch açıkken TUN modunda engellenir. Sistem proxy modunda kapsanmaz.
Kill switch	● Windows: kalıcı güvenlik duvarı kurallarıyla kendi hizmeti; Linux (TUN modu): nftables kuralları; ikisi de uygulama çökse bile engellemeyi sürdürür. Android, sistemin Always-on VPN ayarına dayanır; iOS'ta isteğe bağlı bir "VPN olmadan interneti engelle" anahtarı vardır (varsayılan olarak kapalı).
Bölgesel siteler VPN dışından yönlendirilir	● Yeni kurulumlarda varsayılan olarak kapalıdır (gizlilik modu açıktır): Windows ve Android 2.7.0, iOS 5.6.0 ve Linux 1.3.0'dan beri; daha önce kurulmuş olanlar önceki ayarını korur. Gizlilik modu kapatılırsa yerleşik bir listedeki siteler dört uygulamada da VPN dışından gider; o bölgedeki bir sunucuya bağlıyken uygulanmaz. §9 bölümünde açıklanmıştır.

Kullanıcılar için iki adımlı doğrulama	● Her hesap için isteğe bağlıdır (web sitesinden kurulur); dört uygulama da oturum açarken kodu ister. Yönetici hesapları için zorunludur.
Passkey'ler ve oturum denetimi	● Web sitesi için passkey'ler (hesap başına en fazla 10); güvenlik sayfası tarayıcı oturumlarını listeler ve sonlandırır; parola değişince diğer tüm oturumlar kapanır. Uygulamalar önceden olduğu gibi parolayla oturum açar.
Uygulamalarda sabitlenmiş API bağlantısı	● 10 Ekim 2026 uygulama sürümlerinden itibaren dört uygulama da API için Let's Encrypt (ISRG) ve Google Trust Services kök sertifika otoritelerini sabitler (pinning). Sınırlar: §12.
Bölünmüş tünel	● Windows, Android ve Linux'ta uygulamalar, siteler ve IP adresleri (Windows ve Linux'ta uygulamalar yalnızca TUN modunda); iOS'ta yalnızca siteler ve IP adresleri, çünkü iOS uygulama bazlı VPN'e yalnızca yönetilen profillerde izin verir.
Colitu Shield (DNS koruması)	● İsteğe bağlı. Reklam, izleyici, zararlı yazılım, kimlik avı, dolandırıcılık ve kripto madenciliği alan adlarını engeller (yaklaşık 380 bin kural). Çözümleyicilerinde sorgu kaydı ve istatistik yoktur.
Üçüncü taraf analitik	● Hiçbir uygulamada (Android, iOS, Windows, Linux) yok. iOS uygulamasından 5.4.1 sürümünde kaldırıldı.
İmzalı güncellemeler	● Android, Windows ve Linux'ta imzalı güncelleme manifesti (ECDSA P-256) ve SHA-256; iOS'ta App Store imzası.
Windows kod imzalama (Authenticode)	● Henüz yok.
Tekrarlanabilir derlemeler	● Android 2.9.3 ve Windows 2.9.8 sürümünden itibaren: etiketlenmiş kaynak kod, bayt bayt aynı dosyayı üretir. iOS ve Linux için henüz yok.
SBOM	● Her Android ve Windows GitHub sürümü için SPDX; Linux için henüz yok.
Bağımsız güvenlik denetimi	● Henüz tamamlanmadı.

Güvenlik açığı bildirimi	● security@colitu.com; politika §18 bölümünde ve security.txt dosyasında.
Kendi sunucunuzda barındırma	● Sunulmuyor. Tüm sunucuları Colitu kendisi işletir.

1 Yönetici özeti

Colitu; Android, Windows, Linux ve iOS uygulamaları olan bir VPN hizmetidir. Güvenilmeyen veya kararsız ağlar için tasarlanmıştır: her sunucu birden fazla taşıma protokolü sunar ve uygulamalar kullanıcının ağında çalışan birini seçer.

Tasarım hedefi, hassas verinin tek bir yerde biriken miktarını küçük tutmaktır. Hesaplar ve ödemeler, hiçbir zaman VPN trafiği taşımayan bir kontrol düzleminde tutulur. VPN sunucuları trafik taşır ancak e-posta adresi veya ödeme verisi barındırmaz. Uygulamalar kimlik bilgilerini her platformun güvenli depolama mekanizmasında saklar.

Bu belge mimariyi, tehdit modelini, protokolleri, anahtarların ve hesapların nasıl yönetildiğini, neyin loglandığını, güncellemelerin nasıl korunduğunu, bilinen sınırlamaları ve yapılması gereken işleri anlatır. İddialarımıza güvenmek yerine onları doğrulamak isteyen okuyucular için yazılmıştır.

İlkeler

- Olabildiğince az veri toplamak ve topladığımız veriyi tam olarak belirtmek.
- Uygulama ile VPN sunucusu arasındaki trafiği yerleşik protokollerle şifrelemek. Colitu'nun kendine ait bir kriptografisi yoktur.
- Hesapları ve ödemeleri trafik taşıyan sunuculardan ayrı tutmak.
- Geniş kapsamlı vaatler yerine belgelenmiş sınırlamaları tercih etmek.
- Uygulamaların davranışını doğrulanabilir kılmak: Android, Windows, Linux ve iOS uygulamalarının kaynak kodunu yayımlamak.

VPN sizi anonim yapmaz. Güveni yerel ağınızdan ve internet sağlayıcınızdan VPN işletmecisine taşır. Bu belge, bu güvenin neleri kapsadığını açıklar.

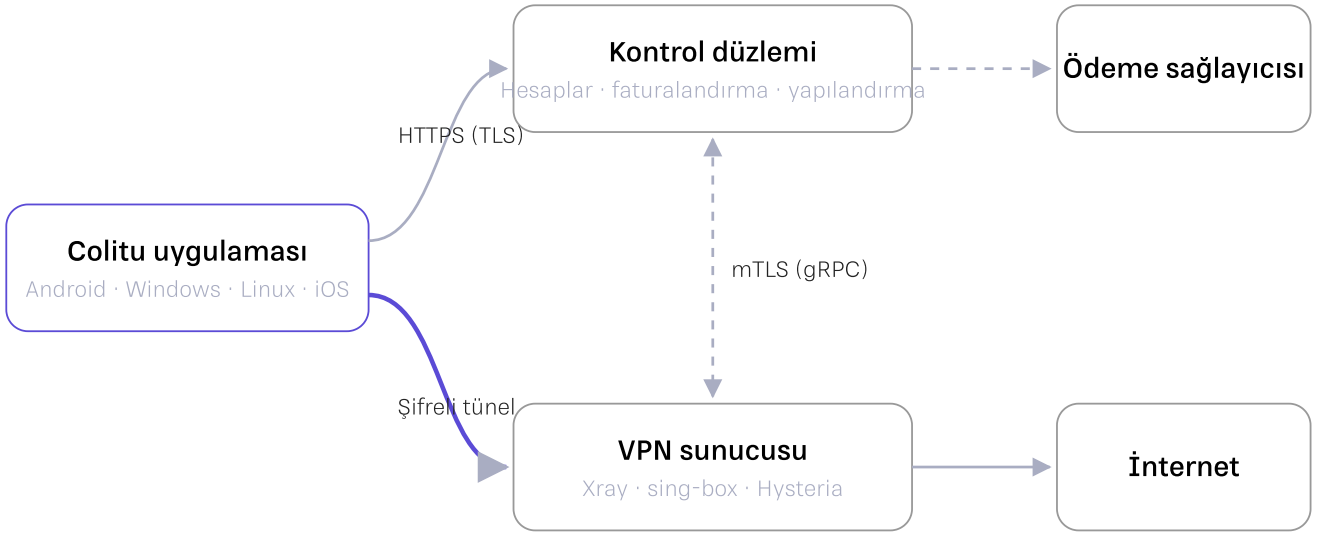
2 Kapsam

Kapsananlar: Android, Windows, Linux ve iOS için Colitu uygulamaları; kontrol düzlemi (hesap API'si, faturalandırma, yapılandırma, yönetim paneli); VPN sunucuları ve bunları yapılandıran node agent; Colitu Shield DNS sunucuları; güncelleme dağıtımı; colitu.com ve alt alan adları.

Kapsam dışında olanlar: kullanıcının işletim sisteminin ve cihazının güvenliği, tarayıcı eklentileri ve cihazdaki diğer yazılımlar, ödeme sağlayıcısının ve §11 bölümünde adı geçen diğer üçüncü tarafların iç güvenliği ve kullanıcının ziyaret ettiği web siteleri.

3 Mimari

Colitu, kullanıcıların kim olduğunu bilen kontrol düzlemini, onların trafiğini taşıyan veri düzleminden ayırır.



Kontrol düzlemi ve veri düzlemi. Kontrol düzlemi hiçbir zaman VPN trafiği taşımaz; VPN sunucuları e-posta veya ödeme verisi barındırmaz.

Bileşenler

Bileşen	Görevleri	Tuttuğu veriler
Uygulama	Oturum açma, sunucu seçimi, protokol seçimi ve yedeğe geçiş, tünelin kurulması, yönlendirme ve DNS ayarları, mevcut olduğu yerde kill switch, güncelleme denetimleri.	Oturum token'ları ve geçerli bağlantı ayarları (§12).
Kontrol düzlemi	Hesaplar, oturum açma, abonelikler ve ödemeler, cihaz kaydı, her sunucunun yapılandırmasının üretilmesi, yönetim paneli, destek.	Hesap ve faturalandırma verileri (§10). Tek bir sunucuda çalışır; veritabanına internetten erişilemez.

Bileşen	Görevleri	Tuttuğu veriler
Node agent	Her VPN sunucusunda çalışır. Yapılandırmasını karşılıklı kimlik doğrulamalı TLS üzerinden alır, VPN çekirdeklerini başlatır, kullanıcı başına trafik sayaçlarını ve sağlık durumunu raporlar.	O sunucunun protokol anahtarları ve onu kullanan kullanıcıların, dahili bir kullanıcı kimliğiyle tanımlanan bağlantı kimlik bilgileri. E-posta adresi yoktur.
VPN sunucusu (veri düzlemi)	Şifreli tüneli sonlandırır ve trafiği internete iletir.	Agent'ın verileri dışında hiçbir şey. Trafik veya bağlantı logu yoktur (§10).
Colitu Shield DNS	Üç VPN sunucusunda çalışan, tünelin içinden erişilen ve reklam, izleyici, zararlı yazılım, kimlik avı, dolandırıcılık ve kripto madenciliği alan adlarını engelleyen isteğe bağlı DNS-over-HTTPS çözümleyicisi (AdGuard Home): yaklaşık 380 bin kural, listeler her 24 saatte güncellenir. Yukarı akış çözümleyiciler DoH ile Cloudflare ve Quad9 dur, ECS kapalı.	Sorgu logu yok, istatistik yok.

Bağlantı nasıl kurulur

1. Uygulama HTTPS üzerinden oturum açar ve kısa ömürlü token'lar alır.
2. Kontrol düzleminden sunucu listesini ve seçilen sunucunun bağlantı ayarlarını ister.
3. Taşıma protokollerini sırayla dener ve bağlantı denetiminden geçen ilkini kullanır.
4. Bundan sonra trafik uygulama → VPN sunucusu → internet yolunu izler. Kontrol düzlemi bu yolun üzerinde değildir.

4 Güven modeli

Colitu'yu kullandığınızda şunlara güvenmeniz gerekir:

- yüklediğiniz Colitu uygulamasına ve onun çalıştığı cihaza ve işletim sistemine;
- bağlandığınız VPN sunucusuna ve onu işleten barındırma sağlayıcısına (VPN sunucuları disk şifrelemesi olmayan kiralık sanal makinelerdir, bu nedenle sağlayıcının bunlara teknik erişimi vardır);
- Colitu'nun kontrol düzlemine ve onu işleten kişilere;

- Colitu'nun kullandığı protokol uygulamalarına (Xray-core, sing-box, Hysteria) ve bunların altındaki kriptografi kütüphanelerine.

Tünelden geçen trafiğin içeriği ve hedefleri konusunda yerel ağınıza veya internet sağlayıcınıza güvenmeniz gerekmez. Ancak bunlar yine de şunları görebilir:

- bir Colitu sunucusuna bağlandığınızı, sunucunun IP adresini ve portunu;
- ne zaman bağlı olduğunuzu ve yaklaşık olarak ne kadar veri gönderip aldığınızı;
- protokole ve ağın inceleme araçlarına bağlı olarak, trafiğin VPN trafiği olduğunu;
- uygulamanın bilinçli olarak tünel dışından gönderdiği trafiği: bazı bölgesel siteler (§9), yerel ağ trafiği, güncelleme denetimleri ve gecikme ölçümleri.

Siz	Yerel ağ / İSS	VPN sunucusu	Web sitesi
	IP adresinizi, sunucunun IP adresini, zamanlamayı ve veri hacmini görür	IP adresinizi, hedefleri ve zamanlamayı görür; HTTPS içeriğini görmez	VPN sunucusunun IP adresini görür

Tünelden geçen trafikte kimin neyi gördüğü.

5 Tehdit modeli

Colitu, trafiği kötü niyetli veya güvenilmeyen yerel ağlara, yaptıklarınızı okuyan veya kaydeden internet sağlayıcılarına ve birçok ağ filtreleme türüne karşı korumak için tasarlanmıştır. VPN'e giren ve VPN'den çıkan trafiği aynı anda izleyebilen bir saldırgana karşı anonimlik sağlamak için tasarlanmamıştır.

Tehdit	Korunuyor mu?	Açıklama
Halka açık Wi-Fi'da dinleme	● Evet	Tünelden geçen trafik, uygulama ile VPN sunucusu arasında şifrelidir.
İnternet sağlayıcısının trafik içeriğini veya hedeflerini okuması	● Evet, tünelden geçen trafik için	Bilinçli olarak tünel dışına yönlendirilen trafik hariç (§9).
İnternet sağlayıcısının VPN kullanıldığını fark etmesi	● Bazen	Reality, XHTTP ve Hysteria2 sıradan TLS veya QUIC gibi görünecek şekilde tasarlanmıştır, ancak hiçbir taşıma protokolü tespit edilemez değildir.

Tehdit	Korunuyor mu?	Açıklama
DNS sızıntıları	🟡 Büyük ölçüde	Android, iOS ve Windows TUN modu tünel üzerinden çözümleme yapar. Windows proxy modu sistem çözümleyicisini kapsamaz.
IPv6 sızıntıları	🟡 Kısmen	Bkz. §9.
Tünel koptuğunda sızıntı	🟡 Kısmen	Windows ve Linux'ta uygulama çökse bile engellemeyi sürdüren bir kill switch vardır (aşağıda belgelenmiş boşluklar); Android'de sistem ayarı gerekir; iOS'ta isteğe bağlı, varsayılan olarak kapalı bir "VPN olmadan interneti engelle" anahtarı vardır.
Hesap API'sine ortadaki adam saldırısı	🟢 Evet	Sistem sertifika doğrulamalı TLS; 10 Ekim 2026 uygulama sürümlerinden itibaren dört uygulama da Let's Encrypt (ISRG) ve Google Trust Services kök sertifika otoritelerini sabitler (pinning); bu yüzden cihaza başkası tarafından kurulmuş bir kök sertifika API trafiğini okumak için kullanılamaz.
Kötü niyetli veya ele geçirilmiş VPN sunucusu	🔴 Hayır	Bir sunucu IP adresinizi ve trafiğinizin hedeflerini görür, ancak HTTPS bağlantılarının içeriğini görmez.
Ele geçirilmiş kontrol düzlemi	🟡 Kısmen	Saldırgan hesap ve faturalandırma verilerini elde eder ve sunuculara yapılandırma gönderebilir. Trafik içeriği hiçbir zaman orada bulunmaz.
Çalınmış hesap parolası	🟡 Kısmen	Hız sınırları tahmin denemelerini yavaşlatır ve cihazların oturumunu kapatabilirsiniz. İsteğe bağlı iki adımlı doğrulama (kimlik doğrulayıcı uygulama) sayesinde çalınmış bir parola tek başına oturum açamaz; ancak siz açana kadar kapalıdır. Passkey'ler web sitesinde alternatif bir oturum açma yoludur; parola değişikliği diğer tüm oturumları kapatır, parola sıfırlama ise hesap silmeyi ve iki adımlı doğrulamayı kapatmayı 24 saat kilitler.
Cihazınızdaki kötü amaçlı yazılım	🔴 Hayır	Hiçbir VPN'in kapsamında değildir.

Tehdit	Korunuyor mu?	Açıklama
Tarayıcı parmak izi, çerezler, oturum açılmış hesaplar	● Hayır	VPN, web sitelerindeki kimliğinizi değil IP adresinizi değiştirir.

Dikkate alınan saldırganlar

Sınıf	Örnek	Colitu'nun koruması
A1 Yerel ağ saldırganı	Aynı kafe Wi-Fi'ındaki biri	Tünelden geçen trafik için güçlü.
A2 İnternet sağlayıcısı	Kullanıcının İSS'si veya mobil operatörü	İçerik ve hedefler için güçlü; zamanlama ve veri hacmi görünür kalır.
A3 Sansürcü	DPI ve aktif yoklama ile ağ genelinde filtreleme	Birden fazla taşıma protokolü ve otomatik yedeğe geçiş; garanti yok (§14).
A4 Kötü niyetli VPN sunucusu veya barındırıcı	Ele geçirilmiş bir sunucu veya kötü niyetli bir barındırma sağlayıcısı	Sınırlı: sunucuyla aynı üst veriyi görür. Kimlik bilgileri her sunucuda ayrıdır, bu nedenle bir sunucu diğerlerine erişmek için kullanılamaz.
A5 Ele geçirilmiş kontrol düzlemi	Panele erişimi olan bir saldırgan	Sınırlı: hesap verileri açığa çıkar; ele geçirilecek trafik içeriği veya gezinme geçmişi yoktur.
A6 Uç nokta saldırganı	Kullanıcının cihazındaki kötü amaçlı yazılım	Yok.
A7 Küresel pasif saldırgan	Tünelin her iki ucunu da gözlemleyen biri	Yok.

6 Protokoller

Her sunucu aynı taşıma protokolü setini sunar. Colitu kriptografi icat etmez: şifreleme, kimlik doğrulama ve anahtar değişimi Xray-core, sing-box ve Hysteria ile bunların kullandığı

kütüphaneler tarafından sağlanır.

Taşıma protokolü	Nasıl çalışır	Sunucu kimlik doğrulaması	Notlar ve sınırlar
Hysteria2	TLS 1.3 ile QUIC (UDP)	Let's Encrypt (ACME) tarafından sunucuya verilen sertifika	Paket kaybı olan ağlarda hızlıdır. UDP'nin engellendiği veya yavaşlatıldığı yerlerde çalışmaz.
VLESS Reality	TCP; Reality, X25519 anahtarlarıyla gerçek bir web sitesini taklit eden bir TLS 1.3 el sıkışması yapar	Yapılandırmayla birlikte iletilen, sunucunun Reality açık anahtarı	DPI'a ve aktif yoklamaya karşı tasarlanmıştır. IP tabanlı engellemeye karşı garanti değildir.
VLESS XHTTP	Reality ile birlikte HTTP benzeri bir akış	Reality ile aynı, kendi anahtarlarıyla	Uzun ömürlü TCP bağlantılarını kesen ağlar için.
Trojan	TLS ile TCP (sürüm 1.2 veya 1.3; sunucu henüz 1.3'ü zorunlu kılmıyor)	Hysteria2 ile aynı sertifika	UDP'nin engellendiği yerlerde TLS yedeği.
Shadowsocks 2022	2022-blake3-aes-256-gcm (AEAD), her oturum için yeni anahtar	Önceden paylaşılmış anahtar	Hafif ve hızlı. İleri gizlilik (forward secrecy) yok: sızan bir anahtar kaydedilmiş oturumların şifresini çözebilir.

Bir taşıma protokolünü hangi çekirdeğin çalıştıracağı platforma bağlıdır. Android ve iOS, Hysteria2 dahil her taşıma protokolü için Xray-core kullanır. Windows ve Linux; VLESS, Trojan ve Shadowsocks için Xray-core, Hysteria2 için sing-box kullanır. Sunucularda VLESS'i Xray, Trojan ve Shadowsocks'u sing-box, Hysteria2'yi resmi Hysteria sunucusu çalıştırır.

Taşıma protokolleri arasında geçiş otomatiktir ancak kesintisiz değildir: uygulama başka bir taşıma protokolüne geçtiğinde tünel kapatılıp yeniden kurulur; bu yaklaşık bir saniye veya daha uzun sürer.

7 Kriptografi ve anahtar yönetimi

Amaç	Mekanizma
Uygulama ve web sitesinden API'ye	Sistem sertifika doğrulamalı TLS 1.2/1.3. 10 Ekim 2026 uygulama sürümlerinden itibaren Windows, Android, Linux ve iOS uygulamaları API için Let's Encrypt (ISRG) ve Google Trust Services kök anahtarlarını da sabitler. Sabitleme 31 Aralık 2027'de uygulanmaz hâle gelir; böylece eski uygulama sürümleri hiçbir zaman dışarıda kalmaz.
Parola saklama	Argon2id: 64 MiB bellek, 3 geçiş, 2 şerit, 16 baytlık rastgele salt, 32 baytlık hash. Parolalar hiçbir zaman düz metin olarak saklanmaz.
Erişim token'ları	Dönüşümlü bir anahtar halkasından HMAC-SHA256 ile imzalanan JWT, 15 dakika geçerli.
Yenileme token'ları	32 rastgele bayt, yalnızca SHA-256 hash'i olarak saklanır, 30 gün geçerlidir, her kullanımda yenisiyle değiştirilir. Eski bir token'ın yeniden kullanılması tüm token ailesini iptal eder.
Kontrol düzlemi ↔ VPN sunucuları	Karşılıklı TLS 1.3 (gRPC). ECDSA P-256 sertifika otoritesi; sunucu sertifikaları 30 gün geçerlidir ve otomatik yenilenir; iptal, parmak izi izin listesiyle yapılır.
Reality anahtarları	Her sunucuda her taşıma protokolü için ayrı X25519 anahtar çifti; kontrol düzleminde üretilir.
Sunucu TLS sertifikaları	Let's Encrypt; her sunucuda ayrı ayrı alınır; özel anahtar o sunucuda kalır.
Veritabanındaki gizli bilgiler	Ödeme, e-posta ve yapay zekâ sağlayıcılarının kimlik bilgileri AES-256-GCM ile şifrelenir.
Güncelleme manifestleri	Uygulamalar tarafından gömülü bir açık anahtara karşı doğrulanan ECDSA P-256 imzaları.
Yedekler	age ile bir açık anahtara şifrelenir; yedek almak için yalnızca bu anahtar gerekir. Şifre çözme anahtarı çevrimdışında tutulur, hiçbir sunucuda bulunmaz.
Kötüye kullanım ve taşıma parmak izleri	Ayarlar şifreleme anahtarından türetilen, veritabanında tutulmayan bir anahtarla HMAC-SHA256.

Anahtarlar nerede tutulur ve biri sızarsa ne olur

- Sertifika otoritesinin özel anahtarı kontrol düzleminde bir dosyadır. Bu anahtarı ele geçiren biri sunucu kimlikleri üretebilir; bu nedenle elimizdeki en hassas anahtardır.
- Her VPN sunucusu kendi Reality özel anahtarlarını, TLS sertifika anahtarını ve onu kullanmış kullanıcıların bağlantı kimlik bilgilerini tutar. Bu kimlik bilgileri rastgeledir ve her sunucuda farklıdır; bu nedenle ele geçirilen bir sunucu, diğer sunucularda geçerli kimlik bilgilerini açığa çıkarmaz.
- Reality özel anahtarları ve kullanıcıların bağlantı kimlik bilgileri kontrol düzlemi veritabanında şifrelenmeden saklanır. Bu değerlerin veritabanı düzeyinde şifrelenmesi yol haritasındadır.
- Reality anahtarları için henüz planlı bir rotasyon yoktur. Bir sunucunun ele geçirildiğinden şüphelenilirse sunucu uygulamalardan kaldırılır, anahtarları ve kimlik bilgileri değiştirilir.
- Kontrol düzlemi her gün şifreli bir yedek alır ve 3 gün saklar. Bir kopya, Object Lock ile Backblaze B2'ye (EU Central, Amsterdam) gönderilir: 30 gün boyunca Colitu dahil kimse onu silemez veya değiştiremez ve en geç 36 gün sonra otomatik olarak silinir. Şifre çözme anahtarı 16 Ekim 2026'dan beri çevrimdışında tutulur; bu yüzden yedekleri ne sunucu ne de Backblaze okuyabilir. Sunucu dışındaki kopyadan geri yükleme 16 Ekim 2026'da test edildi. Bir dağıtımdan önce alınan veritabanı anlık görüntüleri şifreli değildir ve kontrol düzlemi sunucusunda en fazla 7 gün kalır.

8 Hesaplar ve oturumlar

- Oturum açma e-posta ve parola ile yapılır. Bir TV, oturum açılmış bir telefonun onayladığı bir QR kod göstererek oturum açabilir (8 karakterlik kod, 10 dakika geçerli). Google, Telegram veya diğer üçüncü taraflar üzerinden oturum açma yoktur.
- Parolalar en az 10 karakter olmalıdır. Yeni bir hesap, e-postayla gönderilen 6 haneli bir kod onaylandıktan sonra VPN erişimi alır.
- Parola sıfırlama, 15 dakika geçerli, tek kullanımlık ve 5 denemeyle sınırlı 6 haneli bir kod kullanır. Adrese ait bir hesap olsa da olmasa da yanıt aynıdır. Parolanın sıfırlanması tüm cihazların ve web oturumlarının oturumunu kapatır. E-posta koduyla yapılan bir sıfırlamadan sonra hesap silme ve iki adımlı doğrulamayı kapatma 24 saat kilitlenir (RECOVERY_LOCKED hatası).
- Oturum açma, kayıt, parola sıfırlama ve promosyon kodları IP adresi başına hız sınırına tabidir. Web sitesinde oturum açma ve sıfırlama ayrıca e-posta adresi başına sınırlıdır; uygulamalarda oturum açma yalnızca IP başına sınırlıdır. Kullanıcı hesapları için hesap kilitleme yoktur.
- Oturumu kapatmak o cihazın yenileme token'ını iptal eder. Erişim token'ı süresi dolana kadar (en fazla 15 dakika) geçerli kalır.
- Cihazları hesap sayfanızdan kaldırabilirsiniz. Güvenlik sayfası tarayıcı oturumlarını cihaz etiketi (tarayıcı ve işletim sistemi), ülke, oturum açma yöntemi ve IP adresiyle listeler; tek bir oturumu, geçerli olan hariç diğer tüm oturumları veya her yerden çıkış yapabilirsiniz.

- Web sitesinde parolayı değiştirmek içinde bulunduğunuz tarayıcı oturumunu korur; diğer tüm web oturumlarını ve tüm uygulama yenileme token'larını sonlandırır. Değişiklikten önce verilmiş uygulama erişim token'ları hemen çalışmaz olur (AUTH_SESSION_REVOKED hatası).
- Parolayı yeniden isteyen işlemler (parola değiştirme, hesap silme, iki adımlı doğrulama değişiklikleri, passkey'ler) hesap başına 15 dakikada en fazla 10 denemeyle sınırlıdır.
- İki adımlı doğrulama (TOTP) her hesap için isteğe bağlıdır. colitu.com/account/security adresinde bir kimlik doğrulayıcı uygulamayla açarsınız ve 10 tek kullanımlık kurtarma kodu alırsınız; ardından uygulamalar parolanın ardından kodu ister (Windows 2.6.0, Android 2.6.0, Linux 1.2.0 ve iOS 5.5.0 sürümlerinden itibaren desteklenir; eski bir uygulama sizden güncelleme ister). Yalnızca web sitesinden kurulur.
- Passkey'ler: colitu.com'da Hesap → Güvenlik bölümünden (parola gerekir) en fazla 10 passkey ekleyebilir, her birine ad verebilir, parolanızla silebilir ve giriş sayfasında 'Passkey ile giriş yap' seçeneğini kullanabilirsiniz. Kullanıcı doğrulamalı bir passkey iki faktör sayıldığı için iki adımlı doğrulama kodunu atlar; son 90 günde görülmemiş bir ülkeden giriş yine e-posta kodu ister. Passkey'ler ayna alan adlarında çalışmaz. Uygulamalar önceden olduğu gibi ya da passkey ile giriş yapılmış bir tarayıcıda cihaz bağlama QR kodunu onaylayarak oturum açar.
- Colitu şu durumlarda güvenlik e-postası gönderir: yeni bir uygulama cihazı (ilk cihaz için değil), yeni bir ülkeden (90 gündür görülmemiş) oturum açma, iki adımlı doğrulamanın açılması veya kapatılması, kurtarma kodlarının yeniden üretilmesi, passkey eklenmesi veya kaldırılması ve parola değişikliği.
- Abonelik bağlantıları: ana bağlantıya ek olarak, isteğe bağlı 7, 30 veya 90 günlük süre sınırı olan, en fazla 5 adlandırılmış ek bağlantı oluşturabilir ve bunları tek tek iptal edebilirsiniz. Bir bağlantı kısa sürede çok sayıda farklı ağdan kullanılırsa uyarı görünür. Colitu bunun için IP adresi saklamaz; yalnızca günlük, anonim bir farklı ağ sayısı 48 saat tutulur.

Bağlantı kimlik bilgileri cihaz (ve abonelik bağlantısı) ve sunucu başına verilir. Bir cihazı kaldırmak veya abonelik bağlantısını yenilemek, kimlik bilgilerini tüm sunuculardan siler: o cihazdan gelen yeni bağlantılar yaklaşık 15 saniye içinde reddedilir, zaten açık olan bağlantılar kapandıklarında sona erer. Paketiniz daha az cihaza izin verdiği için duraklatılan bir cihaz da siz onu yeniden etkin yapana kadar aynı şekilde dışarıda kalır. Bir cihaz kaybolursa parolanızı da değiştirin.

Yönetici erişimi

Colitu çok küçük bir ekip tarafından işletilir. Yönetim paneli rol tabanlı yetkilerle ayrı bir adreste bulunur, yönetici uç noktaları genel API'de kapalıdır, yönetici hesapları 5 başarısız denemeden sonra 15 dakika kilitlenir ve yönetici işlemleri bir denetim loguna yazılır. Yönetici hesapları için iki adımlı doğrulama (TOTP) zorunludur: kurulmamışsa yönetici oturum açtıktan sonra yalnızca kurulumu yapabilir; sonraki her girişte kod veya tek kullanımlık bir kurtarma kodu gerekir (denemeler sınırlıdır). Yönetici ayrıca bir donanım güvenlik anahtarı (WebAuthn) kaydedebilir;

kaydedildiğinde giriş TOTP yerine parola ve anahtar ister, tek kullanımlık kurtarma kodu loglanan bir acil durum yolu olarak kalır. Kaybolan bir anahtar, kurtarma koduyla ya da kimlik bant dışı doğrulandıktan sonra sunucuda loglanan bir sıfırlama komutuyla değiştirilir. Erişim, hesabın devre dışı bırakılmasıyla bir sonraki istekte kaldırılır. Yönetici oturumları açıldıkları tarayıcıya ve ağa bağlıdır.

9 Trafik, DNS, IPv6 ve kill switch

VPN sunucusunun görebildikleri

Bir VPN sunucusu trafiğinizi nereye göndereceğini bilmek zorundadır; bu nedenle teknik olarak IP adresinizi, bağlandığınız sitelerin IP adreslerini ve çoğu zaman alan adlarını (TLS SNI) ve trafiğinizin zamanlamasını ve hacmini görür. Cihazınız ile web sitesi arasında şifreli kalan HTTPS bağlantılarının içeriğini okuyamaz. Colitu HTTPS trafiğinin şifresini çözmez ve onu incelemez.

Varsayılan yönlendirme

	Android	Windows	iOS	Linux (beta)
Trafiğin yakalanma şekli	Sistem VPN'i (tüm uygulamalar)	Yeni kurulumlarda TUN modu (tüm trafik); sistem proxy modunu kullanmış kurulumlar onu korur	Sistem VPN'i (tüm uygulamalar)	Varsayılan olarak sistem proxy'si; TUN modu isteğe bağlı
Varsayılan olarak kapsanmayanlar	Yerel ağ	Sistem proxy modunda: sistem proxy'sini yok sayan uygulamalar, Windows DNS çözümleyicisi, tarayıcı UDP trafiği (QUIC/WebRTC), IPv6. TUN modu bunları kapsar.	Yerel ağ	Sistem proxy modunda Windows ile aynı

	Android	Windows	iOS	Linux (beta)
Bölgesel siteler ve IP'ler (yerleşik liste)	Yalnızca gizlilik modu kapalıysa ve sunucu o bölgede değilse VPN dışından	Yalnızca gizlilik modu kapalıysa ve sunucu o bölgede değilse VPN dışından	Yalnızca gizlilik modu kapalıysa ve sunucu o bölgede değilse VPN dışından	Yalnızca gizlilik modu kapalıysa ve sunucu o bölgede değilse VPN dışından
DNS	Tünel üzerinden 1.1.1.1'e	TUN: tünel üzerinden Cloudflare DNS-over-HTTPS'e. Proxy modu: yalnızca proxy'ye ulaşan trafik için.	Tünel üzerinden (8.8.8.8 → Xray → 1.1.1.1)	Windows ile aynı
IPv6	● Engellenir	● TUN modunda kill switch ile engellenir; sistem proxy modunda kapsanmaz	● Sızıntı yapmaz: tünele yönlendirilir ve orada düşürülür	● Windows ile aynı
Kill switch	● Android'in Always-on VPN ve "VPN'siz bağlantıları engelle" ayarlarını kullanır; bunları kullanıcının açması gerekir	● Kalıcı Windows Filtering Platform kurallarıyla kendi Windows hizmeti, varsayılan olarak açık (aşağıya bakın)	● "VPN olmadan interneti engelle" (iOS includeAllNetworks), varsayılan olarak kapalı; açıkken Wi-Fi giriş sayfaları açılamaz. "Always-on" yalnızca yeniden bağlanır	● Uygulama çökse de kalan nftables kuralları; yalnızca TUN modunda

	Android	Windows	iOS	Linux (beta)
Bölünmüş tünel	● Uygulamalar (yalnızca siteler ve IP adresleri	● Uygulamalar (yalnızca TUN modunda), siteler ve IP adresleri	● Yalnızca siteler ve IP adresleri (iOS uygulama bazlı VPN'e yalnızca yönetilen profillerde izin verir)	● Uygulamalar (yalnızca TUN modunda), siteler ve IP adresleri
Multihop ve değişen IP	● Yalnızca VLESS	● Yalnızca VLESS	● Yalnızca VLESS	● Yalnızca VLESS

VPN dışından giden bölgesel siteler

Bazı bölgesel siteler (yerleşik bir listedeki alan adları ve IP aralıkları), yabancı IP adreslerini reddeden servislerin çalışmaya devam etmesi için tünelin dışından, doğrudan açılır. O bölgedeki bir sunucuya bağlıyken bu uygulanmaz. Bu trafikte site ve internet sağlayıcınız gerçek IP adresinizi görür. Kural yalnızca gizlilik modu kapalıyken uygulanır. Gizlilik modu yeni kurulumlarda varsayılan olarak açıktır (Windows ve Android 2.7.0, iOS 5.6.0, Linux 1.3.0 ve sonrası); yani varsayılan olarak tüm trafik VPN'den geçer, daha önce kurulmuş olanlar önceki ayarını korur. Kural etkinken ilk bağlandığınızda uygulama bunu açıklayan tek seferlik bir bildirim gösterir. İsterseniz o bölgedeki bir sunucuyu da seçebilirsiniz.

Windows kill switch ayrıntıları

- Loopback, yerel ağ (bir ayardır, varsayılan olarak açık), DHCP, VPN çekirdekleri, TUN bağdaştırıcısı ve Colitu uygulamasının kendisi dışındaki tüm IPv4 ve IPv6 trafiğini engeller.
- Oturum boyunca etkindir; hem TUN modunda hem sistem proxy modunda. Proxy modunda, proxy kullanmayan uygulamalar bağlıyken internete erişemez.
- Kurallar, ayrı bir Windows hizmeti (ColituKillSwitch, LocalSystem, otomatik başlatma) tarafından kalıcı Windows Filtering Platform kuralları olarak tutulur. Uygulama veya VPN çekirdeği çökerse ya da hizmet yeniden başlarsa kurallar yerinde kalır ve Colitu yeniden bağlanana kadar internet engelli kalır (fail-closed).
- Windows'un normal bir yeniden başlatılması veya kapatılması engellemeyi sonlandırır. Bu bilinçli bir tercihtir: internetin neden engellendiğini açıklayacak kimse olmazdı. İstisna, Otomatik bağlan ile Windows ile başlat birlikte açıkken görülür; bu durumda Colitu yeniden bağlanana kadar engelleme sürer. Bağlantıyı kendiniz keserseniz engelleme biter; kaldırma işlemi tüm kuralları siler.
- Hizmet yoksa (örneğin hasarlı bir kurulumdan sonra) uygulama sizi uyarır ve eski, uygulama içi kill switch'e döner. Onun filtreleri uygulamanın sürecine aittir: uygulama çökerse veya sonlandırılırsa Windows filtreleri kaldırır ve trafik akar (fail-open).
- Uygulamanın doğrudan yönlendirdiği trafik, örneğin yerleşik listedeki bölgesel siteler, tasarım gereği engellenmez.

Uygulamaların tünel dışından gönderdiği trafik

- Güncelleme denetimleri ve güncelleme indirmeleri (colitu.com).
- Sunuculara yapılan gecikme ölçümleri.
- Windows'ta, sunucuların alan adlarının Cloudflare veya Google DNS-over-HTTPS üzerinden çözümlenmesi.

Bağlantı denetimleri (örneğin Google'ın generate_204 adresi) tünel üzerinden gönderilir.

10 Loglama ve veri envanteri

Colitu'nun sakladığı verilerin tam listesi budur. Gizlilik politikası aynı listeyi hukuki biçimde içerir.

VPN hizmeti

Veri	Saklanıyor mu?	Saklama süresi ve amaç
Trafiğinizin içeriği	● Asla	—
Ziyaret ettiğiniz siteler ve IP adresleri	● Saklanmaz	Kaydedilmez.
DNS sorgularınız	● Saklanmaz	Colitu Shield çözümleyicilerinde sorgu loglama ve istatistikler kapalıdır. Uygulamalar varsayılan olarak genel çözümleyicileri (Cloudflare, Google) kullanır; bu çözümleyiciler sorguları sizin değil VPN sunucusunun IP adresinden alır.
VPN sunucularındaki IP adresiniz	● Saklanmaz	Yalnızca bağlantı için bellekte kullanılır.
Kullanıcı başına trafik hacmi	● Saklanır	Kullanıcı ve sunucu başına bayt miktarı, yaklaşık 15 saniyelik aralıklarla; kota ve adil kullanım için 90 gün saklanır, sonrasında yalnızca faturalandırma dönemi başına toplamlar kalır. Bu veri bir hesabın ne zaman aktif olduğunu ve ne kadar kullandığını gösterir, ancak trafiğin nereye gittiğini göstermez.

Hesap ve web sitesi

Passkey'ler, web oturumları ve abonelik bağlantıları aşağıdaki tabloda yer alır. Abonelik bağlantıları için IP adresi saklanmaz: bağlantı başına yalnızca günlük, anonim bir farklı ağ sayısı 48 saat tutulur.

Veri	Saklama süresi	Amaç
E-posta adresi, parola hash'i (Argon2id), dil, hesap tarihleri	Hesap silinene kadar; silmede adres bir yer tutucuyla değiştirilir ve parola kullanılamaz hale gelir	Hesap ve oturum açma
E-posta doğrulama ve parola sıfırlama kodları (adres, hash'lenmiş kod, IP adresi)	7 gün	E-posta adresinin doğrulanması, parola sıfırlama
Oturum açma olayları (IP adresi, ülke, tarayıcı veya uygulama)	180 gün	Hesap güvenliği, kötüye kullanımın önlenmesi
Kayıt sırasındaki ve son oturum açmadaki IP adresi ve ülke	Kayıt: 180 gün. Son oturum açma: 180 gün boyunca oturum açılmazsa silinir	Hesap güvenliği, bölgesel kurallar
Bölgesel kurallar nedeniyle reddedilen kayıt ve girişler (IP adresi, ülke)	90 gün	Bölgesel kuralların uygulanması
Web oturumları (IP adresi, ülke, tarayıcı, giriş yöntemi)	Oturum sona erdikten (çıkış, süre dolması veya iptal) 30 gün sonra silinir	Oturum açma, hesap sayfasındaki oturum listesi
Uygulama oturum token'ları (yalnızca hash olarak, bir cihaza bağlı)	Süresi dolduktan veya iptal edildikten 30 gün sonra silinir	Uygulamalarda oturumun açık kalması
İki adımlı doğrulama (şifrelenmiş doğrulayıcı anahtarı, tek kullanımlık kurtarma kodlarının hash'leri, 5 dakikalık giriş adımları)	Anahtar ve kurtarma kodları, siz kapatana veya hesap silinene kadar; giriş adımları süreleri dolduktan 1 gün sonra silinir	Hesap güvenliği

Veri	Saklama süresi	Amaç
Passkey'ler (genel anahtar, kimlik bilgisi kimliği, verdiğiniz ad, imza sayacı, oluşturulma ve son kullanım tarihi; özel anahtar ve biyometrik veri cihazınızdan hiç çıkmaz, 5 dakikalık tek kullanımlık doğrulama istekleri)	Siz passkey'i silene kadar veya hesap silinene kadar; doğrulama istekleri 5 dakika sonra kendiliğinden silinir	Parolasız giriş ve hesap güvenliği
VPN bağlantı kimlik bilgileri (sunucu başına, cihaza veya abonelik bağlantısına bağlı rastgele anahtarlar)	Cihaz veya bağlantı kullanımdayken; kaldırıldıktan veya yenilendikten 30 gün sonra silinir	VPN erişimi
Abonelik bağlantıları (verdiğiniz ad, oluşturulma, son kullanım ve bitiş tarihi, "paylaşılmış olabilir" işareti; bağlantının kendisi yalnızca hash olarak saklanır). Bağlantıyı kullanan IP adresleri saklanmaz; yalnızca bağlantı başına günlük, anonim, yaklaşık "kaç farklı ağdan kullanıldı" sayısı 48 saat tutulur	Bağlantıyı iptal edene veya hesabı silene kadar (süresi dolan bağlantı otomatik iptal edilir); ağ sayısı 48 saat sonra kendiliğinden silinir	Cihaz başına bağlantı ve paylaşılmış bağlantı uyarısı
TV ile giriş istekleri (cihaz adı, IP adresi, ülke)	10 dakikalık kodun süresi dolduktan 1 gün sonra silinir	QR ile giriş
Cihazlar (ad, platform, uygulama ve işletim sistemi sürümü, son IP adresi ve ülke, donanım kimliğinin anahtarlı hash'i)	Cihaz hesaptayken tutulur. Kaldırılan cihazın adı, IP adresi, ülkesi ve donanım hash'i 30 gün sonra silinir; 180 gündür görülmeyen cihazın IP adresi ve ülkesi silinir	Cihaz sınırları, hesap güvenliği
Reddedilen cihaz ekleme ve deneme girişimleri (IP adresi, cihaz bilgileri)	180 gün	Cihaz sınırları, kötüye kullanımın önlenmesi

Veri	Saklama süresi	Amaç
Ücretsiz plan ve deneme kötüye kullanım denetimleri (e-posta adresi, donanım kimliği ve ağın HMAC-SHA256 ile anahtarlanmış hash'i; anahtar veritabanında tutulmaz)	Ağ: 30 gün. E-posta ve donanım kimliği: hesap var olduğu sürece ve silindikten sonra 180 gün. Bu değişiklikten önce yazılmış anahtarsız SHA-256 hash'leri en geç yazıldıktan 180 gün sonra silinir	Tekrarlanan ücretsiz hesapların önlenmesi
Otomatik bot ve kötüye kullanım taraması: bekletilen veya engellenen hesaplarda puan, tetikleyen sinyaller, IP adresi, ülke, ağ (ASN) ve tarayıcı kimliği; kayıt aşamasında reddedilenlerde ayrıca e-posta adresi	Bekletilen veya engellenen hesaplar: hesap var olduğu sürece, hesap silinince silinir. Reddedilen kayıtlar: 30 gün	Botların, betiklerle hesap açılmasının ve sunucu adreslerinin toplanmasının önlenmesi
Promosyon kodlu deneme kötüye kullanım denetimleri (normalleştirilmiş e-posta adresi, cihazın donanım kimliği ve ağın — IPv4 /32 ve /24 veya IPv6 /64 ve /48 — HMAC-SHA256 ile anahtarlanmış hash'i; anahtar veritabanında tutulmaz)	Ağ: 35 gün. E-posta ve donanım kimliği: 365 gün, hesap silinse de	Deneme kodunun kişi başına bir kez kullanılması
Önceki hizmetten taşıma talepleri (Telegram kimliği ve adı, notlar, IP adresi)	Son değişiklikten 30 gün sonra silinir. Onaylanan bir talepten yalnızca Telegram kimliğinin anahtarlı hash'i 2 yıl kalır	Eski aboneliklerin taşınması; aynı aboneliğin iki kez taşınmasının önlenmesi
Kayıt kaynağı etiketi (örn. "github", "app:android"): sitenin giriş bağlantısındaki utm/ref etiketinden, sizi yönlendiren sitenin adından (örn. github.com) veya uygulamadan; çerez, takip pikseli ya da adres saklanmaz. İlk VPN bağlantısının zamanı.	Hesapla birlikte silinir	Hangi kanalların gerçek kullanıcı getirdiğini ve ilk bağlantının ne kadar sürdüğünü toplu olarak ölçmek

Veri	Saklama süresi	Amaç
Davet kodunuz; davet bağlantısıyla açılan hesaplarla davet edenin hesabı arasındaki bağ, davetin durumu (bekliyor, kazanıldı, geçersiz ve nedeni) ve verilen Premium gün sayısı. Davet edene davet edilenin adı veya e-postası gösterilmez.	İki hesaptan biri silinince silinir	Davet ödüllerini vermek; kötüye kullanımı (aynı IP adresi veya cihaz, geçici e-posta) engellemek; davetle gelen kayıtları toplu olarak ölçmek
Uygulamaların anonim kullanım istatistikleri: bağlantı denemelerinin sonucu ve başarısızlık türü, bağlanma ve kurtarma süreleri (aralık sayıları), beklenmedik kopmalar, Adaptive Connect'in protokol geçişleri, sunuculara ölçülen ping ve otomatik modun sunucu seçimi, kullanılan özellikler ve kill switch durumu; ağ türü ile bağlı olunan ağın ülkesi ve internet sağlayıcısı numarası (ASN, VPN kapalıyken alınan imzalı etiketten). Sunucuda yalnızca gün başına toplamlar, ağ (ülke + ASN) ve sunucu birbirinden ayrı tablolarda tutulur; hesap, cihaz, IP adresi veya ziyaret edilen siteler kaydedilmez. Uygulama ayarlarından kapatılabilir.	Toplamlar süresiz (kişiye bağlanamaz)	Bağlantı kalitesini, Adaptive Connect'in başarısını ve özelliklerin kullanımını ölçüp iyileştirmek

Veri	Saklama süresi	Amaç
Colitu Passport hesabına kaydedilir ve oturum açtığın her cihazda seninle gelir. Pulu açılan her ülke için açılış zamanı ve parça sayısı, başarımlar, koleksiyonlar, haftalık sefer ilerlemesi, takma ad, unvan, kapak, saat dilimi farkı ve koleksiyoncu numarası; günlük toplamlar (kullanım dakikası, parça, gece ve sabah erken dakikaları, o gün kullanılan ülkelerin listesi); süren seri (ülke, uzunluğu ve sayılan son dakika); uygulamalardaki açılış animasyonları için ödül olayları. Dakikaları sunucularımız bağlantı süresinden sayar: sunucularımızdan biri o dakikada hesabın için trafik bildirirse dakika sayılır (cihaz sayısı ne olursa olsun her dakika en fazla bir kez) ve ülke, sunucunun ülkesidir; uygulamalar dakika ekleyemez. Yalnızca gün ve ülke başına toplamlar tutulur; dakika dakika ya da oturum kaydı, site veya IP adresi tutulmaz. Eski sürümün cihazdaki ilerlemesi cihaz başına bir kez içe aktarılır (makul sınıra kadar, yüksek olan değer geçerli olur).	Günlük toplamlar 400 gün, ödül olayları 30 gün, geri kalanı hesap silinene kadar	Pasaportu hesabına kaydetmek, her cihazında göstermek ve ödülleri, haftalık seferleri hesaplamak
Colitu Passport'un isteğe bağlı anonim sayıları, günde en fazla bir rapor: açılmış pul sayısı, açık olan en yüksek bölüm, seviyelere göre pul sayıları, tamamlanan haftalık seferler, o gün kazanılan parça ve pasaportun o gün açılıp açılmadığı. Kimlik doğrulaması olmadan gönderilir; sunucu her raporu yalnızca gün başına toplamlara ekler, rapor satırı, hesap, cihaz veya IP adresi saklamaz. Pulların hangi ülkelerden ve ne zaman kazanıldığı gönderilmez. Yalnızca eski uygulama sürümleri gönderir; yeni sürümler göndermez, pasaport artık hesabında tutulur (aşağıdaki "Colitu Passport" satırı). Ayar kapalı başlar ve uygulamadan kapatılabilir.	Toplamlar süresiz (kişiye bağlanamaz)	Pasaportun ne kadar kullanıldığını ve kuralların dengesini (seviye ve parça hızı) toplu olarak görmek

Veri	Saklama süresi	Amaç
Uygulama içi anketlere verdiğiniz yanıtlar: tavsiye puanı (0–10), Colitu olmasa ne hissedeceğiniz, Premium'u yenilememe nedeni, isteğe bağlı yorum ve platform; kapattığınız anketler (30 günde en fazla bir anket sorulur)	Hesap silinince hesapla bağı ve yorum silinir; yalnızca anonim puan kalır	Memnuniyeti (NPS), ürün-pazar uyumunu ve ayrılma nedenlerini toplu olarak ölçmek
Çözülen destek talebine verdiğiniz 1–5 puan ve isteğe bağlı yorum; talebin ilk yanıt ve çözülme zamanı	Destek konuşmasıyla birlikte silinir	Destek kalitesini (memnuniyet, yanıt ve çözüm süresi) toplu olarak ölçmek
Bir cihaz için hangi taşıma protokollerinin hangi sunucuda ve ne hızda çalıştığı (IP yok)	Her raporla üzerine yazılır; son rapordan 35 gün sonra silinir	Çalışan protokollerin önce denenmesi
Plan, ödemeler ve siparişler (tutar, ödeme yöntemi türü, sağlayıcının işlem kimliği, sağlayıcının bildirimi; Rialit ile ödeyenler için hesaba bağlı sabit bir ödeyen numarası)	Muhasebe ve vergi mevzuatının gerektirdiği süre boyunca, hesap silindikten sonra da; bu sürenin sonunda otomatik silme henüz yok	Faturalandırma, iade, yasal yükümlülükler
Colitu Business şirket hesabı: şirket adı, fatura e-postası, ülke, vergi numarası, koltuk sayısı ve süresi; üyelik (rol, davet, katılım ve ayrılma tarihleri, ekleyen kişi); şirket faturaları ve şirket hareket kaydı. Şirketin sahibi ve yöneticileri üyelerin e-posta adresini, rolünü ve cihazlarının adını, platformunu, uygulama sürümünü ve son görülme zamanını görür; trafiği ve ziyaret edilen siteleri göremez	Şirket hesabı Colitu tarafından kapatılana kadar; şirket faturaları muhasebe ve vergi mevzuatının gerektirdiği süre boyunca; şifre kurma bağlantıları 7 gün geçerlidir. Hesabını silen üyenin üyeliği kapanır ve koltuk şirkete geri döner	Şirket koltuklarının yönetimi, şirket faturalandırması, süre hatırlatmaları

Veri	Saklama süresi	Amaç
Colitu Business iş birliği teklifi gönderdiğimiz firma ve içerik üreticileri: firma veya kanal adı, sitesinde ya da kanal açıklamasında iş iletişimi için yayımladığı e-posta adresi, ülke ve dil; gönderdiğimiz mailler ve tarihleri; gelen cevapların konusu ve ilk 300 karakteri, geri dönen mailler	Paneldeki gönderim ve cevap kayıtları 12 ay sonra silinir. İletişim listesi, kişi bizden yazmamamızı isteyene ya da adres artık gerekmeyene kadar tutulur; "bana yazmayın" cevabı gelen adrese bir daha yazılmaz	Colitu Business bayilik ve white label tekliflerini iletmek (meşru menfaat; her mailde itiraz yolu ve bu politika yazılıdır)
Destek yazışmaları ve ekleri, uygulamanın eklediği uygulama logları dahil (adresler, site adları ve gizli bilgiler maskelenir)	Kapatılan yazışmalar: son mesajdan 2 yıl sonra silinir	Destek, şikâyetlerin ele alınması
Güvenlik bildirimleri: bildirdiğiniz açığın metni (başlık, açıklama, adımlar, etki) ve ekiple yazışmalar; Hall of Fame'de anılmak ettiğiniz siteler gönderilmez	Hesap silinene kadar; hesap silindiğinde bildirimler, yazışmalar	Güvenlik açıklarını düzeltmek, ödülleri vermek (isteğe
Colitu Bot yazışmaları (metin, IP adresi, "yardımcı oldu mu" geri bildirimi)	180 gün	Soruların yanıtlanması
E-posta teslim kayıtları (alıcı adresi, e-posta türü)	90 gün	Teslim sorunlarının çözülmesi
Bülten aboneliği (e-posta adresi, dil, onay zamanı); yalnızca e-postadaki bağlantıyla onaylarsanız	Abonelikten çıkana kadar; onaylanmayan kayıtlar 7 gün sonra silinir	Duyuru, sürüm notu ve teklif e-postaları (açık rızayla)

Otomatik bir görev bu süreleri her saat uygular; hesap silme, gizlilik politikasında listelenenleri hemen siler. Kalan boşluklar: plan, ödeme ve sipariş kayıtları ile denetim logu için henüz otomatik silme yoktur ve silmeden önce alınmış şifreli yedekler verileri en fazla 36 gün, bir dağıtımdan önce alınmış şifrelenmemiş anlık görüntüler ise en fazla 7 gün tutar. Kötüye kullanım hash'leri bir sunucu anahtarıyla üretilir; bu değişiklikten önce yazılmış anahtarsız SHA-256 hash'leri silinene kadar, en geç yazıldıktan 180 gün sonrasına kadar eşleştirilebilir.

Veri	Saklama süresi	Amaç
Web sitesi ve API erişim logları (IP adresi, istenen adres, tarayıcı)	14 gün	Hizmetin işletilmesi ve korunması
Web sitemizdeki DNS sızıntı testi	Yalnızca bellekte, 10 dakika	Test sonucunun gösterilmesi
Denetim logu (yönetici işlemleri ve hesap kimliğiyle bazı hesap işlemleri, örneğin hesabın silinmesi)	Süresiz, hesabı silerken istege bağlı	İşlemlerin hesap verebilirliği

11 Telemetri ve üçüncü taraflar

Uygulamalardaki telemetri

- Hiçbir Colitu uygulaması (Android, iOS, Windows, Linux) analitik, reklam veya çökme raporlama kütüphanesi içermez; iOS uygulamasında 5.4.1 sürümünden beri bu tür bir kütüphane yoktur.
- Tüm uygulamalar, çalışan taşıma protokollerinin önce seçilebilmesi için hangi taşıma protokollerinin hangi sunucuda ve ne hızda çalıştığını cihaza bağlı olarak Colitu'ya raporlar.
- Destek talepleri, adresleri ve gizli bilgileri maskelenmiş son uygulama loglarını ekler.

Veri alan üçüncü taraflar

Taraf	Aldığı veriler
Bir ödeme sağlayıcısı (yalnızca ücretli plan satın almış müşteriler için)	Sipariş numarası, tutar, para birimi, plan açıklaması ve ödeme yöntemi; kart veya banka bilgileri sağlayıcının sayfasında girilir. Colitu e-posta adresinizi veya IP adresinizi göndermez.
Resend (e-posta)	E-posta adresiniz ve hesap e-postalarının içeriği (kodlar, makbuzlar).
Brevo (e-posta aktarımı)	Destek posta kutumuzdan gönderilen yanıtlar.
DeepSeek (Colitu Bot)	Soru ve bot yazışmasının son birkaç mesajı. Hesap bilgileri gönderilmez, ancak yazdığınız her şey iletilir.
Have I Been Pwned (Pwned Passwords)	Kayıt olurken veya yeni parola belirlerken: bilinen sızıntılarla karşılaştırmak için parolanın SHA-1 özetinin ilk 5 karakteri. Parolanın kendisi, tam özeti, e-posta veya IP adresiniz asla gönderilmez.
Cloudflare	DNS kayıtlarını barındırır ve docs.colitu.com ile map.colitu.com için proxy görevi görür. Ayrıca uygulamalardaki varsayılan DNS çözümleyicilerini ve iki sunucuda birkaç alan adı için çıkış noktasını sağlar (§17).
Backblaze B2 (EU Central, Amsterdam)	Günlük yedeğin şifreli kopyaları. Bunları okuyamaz: şifre çözme anahtarı çevrimdışında tutulur.
Barındırma sağlayıcıları	Sunucuları işletir ve bunlara teknik erişimi vardır.

Web sitesi üçüncü taraf betik, yazı tipi veya izleyici yüklemez.

12 Uygulama güvenliği

	Android	Windows	iOS	Linux (beta)
Oturum token'ları	Android Keystore anahtarıyla AES-256-GCM (Keystore başarısız olursa yazılım anahtarı)	DPAPI (geçerli kullanıcı)	Keychain (ilk kilit açılışından sonra erişilebilir)	Makineden ve kullanıcıdan türetilen anahtarla AES-GCM
Bağlantı kimlik bilgileri	Şifreli (AES-GCM)	Yalnızca yöneticilerin ve SYSTEM'in okuyabildiği bir veritabanında düz metin	Uygulamanın özel kapsayıcısında düz metin dosya	Korumalı dosyalar (0600)
API için sertifika sabitleme	● Evet	● Evet (10 Ekim 2026'dan itibaren)	● Evet (10 Ekim 2026'dan itibaren)	● Evet (10 Ekim 2026'dan itibaren)
Yetkiler	VPN izni olan normal uygulama	Her zaman yönetici olarak çalışır; kill switch kurallarını ayrı bir arka plan hizmeti (ColituKillSwitch, LocalSystem) tutar	Network extension	sudo ister; parola bellekte tutulur
Yerel VPN logları	Yalnızca uyarılar; erişim logu yok	Yalnızca uyarılar; adresler maskelenir; 7 gün sonra silinir	Yalnızca uyarılar; erişim logu yok	Yalnızca uyarılar

Android	Windows	iOS	Linux (beta)

Sabitleme, cihaza başkası tarafından kurulmuş bir kök sertifikanın uygulamaların API trafiğini okumak için kullanılamaması demektir. Kendi kök sertifikasını ekleyerek HTTPS'i denetleyen güvenlik yazılımları bu nedenle uygulamaların API bağlantısını engeller; bu tür yazılımlarda Colitu'yu hariç tutun.

13 Güncellemeler ve tedarik zinciri

Platform	Bir güncelleme nasıl doğrulanır
Android (indirilebilir sürüm)	Manifest ECDSA P-256 ile imzalanır ve uygulamaya gömülü bir anahtara karşı denetlenir. APK, colitu.com'dan HTTPS üzerinden gelmeli, manifestteki SHA-256 değeriyle eşleşmeli ve yüklü uygulamayla aynı sertifikayla imzalanmış olmalıdır. Daha eski sürümler reddedilir.
Android (Google Play)	Google Play üzerinden güncellenir.
Windows	Aynı imzalı manifest, colitu.com'dan HTTPS ile indirme, SHA-256 denetimi; yükseltilmiş yetkiyle çalışan kurulum adımında yeniden denetlenir. Kurulum dosyası henüz Authenticode ile imzalı değildir, bu nedenle Windows SmartScreen uyarı verebilir.
Linux	İmzalı manifest ve paketin SHA-256 değeri.
iOS	Apple TestFlight üzerinden dağıtılır; güncellemeleri Apple imzalar ve iletir.

Derleme ve kaynak kod

- Açık kaynak uygulamaların her sürümü GitHub'da etiketlenir. Sürüm sayfası SHA-256 sağlama toplamlarını ve SPDX biçiminde bir yazılım malzeme listesini (SBOM) içerir (Android ve Windows).
- Android ve Windows depolarında CodeQL kod taraması ve Dependabot bağımlılık güncellemeleri çalışır; GitHub Actions commit hash'lerine sabitlenmiştir.

- Android sürümü CI'da derlenir; Windows kurulum dosyası geliştiricinin bilgisayarında derlenir; Linux paketleri CI'da derlenir; iOS TestFlight sürümleri Codemagic'te derlenir.
- Android (2.9.3 sürümünden itibaren) ve Windows (2.9.8 sürümünden itibaren) derlemeleri tekrarlanabilirdir; bu nedenle herkes etiketlenmiş kaynak kodu yeniden derleyip sonucu yayımlanan dosyayla karşılaştırabilir. iOS ve Linux'ta bir sağlama toplamı hâlâ yalnızca elinizdeki dosyanın bizim yayımladığımız dosya olduğunu kanıtlar, etiketlenmiş kaynak koddan derlendiğini kanıtlamaz. Android Xray çekirdek kütüphanesi, SHA-256 ile sabitlenmiş resmî üst akış (upstream) ikili dosyasıdır; kaynaktan yeniden derlenmez.

Neyin açık, neyin kapalı olduğu

Bileşen	Kaynak kod
Android uygulaması	🟢 Açık (GPL-3.0)
Windows uygulaması	🟢 Açık (GPL-3.0)
Linux uygulaması	🟢 Açık (GPL-3.0)
iOS uygulaması	🟢 Açık (GPL-3.0)
Kontrol düzlemi ve node agent	🔴 Kapalı
Web sitesi	🔴 Kapalı

14 Sansüre karşı dayanıklılık

Hiçbir taşıma protokolünün her sansür sistemine karşı çalışmaya devam edeceği garanti edilemez. Colitu'nun yaklaşımı, farklı özelliklere sahip birden fazla taşıma protokolü sunmak ve uygulamanın otomatik olarak yedeğe geçmesini sağlamaktır.

Engelleme tekniği	Colitu'nun yanıtı
Sunucu IP adreslerinin engellenmesi	Farklı ağlarda birden fazla sunucu ve bir aktarma sunucusu (§17). Engellenen bir IP, sunucu değişene kadar engelli kalır.
Portların veya UDP'nin engellenmesi	UDP engellendiğinde TCP taşıma protokolleri (Reality, XHTTP, Trojan); TCP bozulduğunda Hysteria2.
DNS zehirlemesi	Uygulamalar sunucu adreslerini API'den alır ve gerektiğinde bunları şifreli DNS üzerinden çözümler.

Engelleme tekniği	Colitu'nun yanıtı
TLS parmak izi ve aktif yoklama	Reality, yoklamalara taklit ettiği gerçek web sitesi olarak yanıt verir.
Protokol parmak izi (DPI)	Reality ve XHTTP sıradan HTTPS'e, Hysteria2 ise QUIC'e benzer.
Yavaşlatma ve bağlantı sıfırlamaları	Başka bir taşıma protokolüne otomatik geçiş; uzun bağlantıları kesen ağlar için XHTTP.

15 Gizlilik sınırlamaları

VPN, trafiğinizi bulunduğunuz ağdan gizler. Her şeyi gizleyemez:

- Paket boyutları, zamanlama ve toplam veri hacmi görünür kalır ve her iki ucu da gören bir gözlemci tarafından eşleştirilebilir.
- Web siteleri sizi çerezler, tarayıcı parmak izi ve oturum açtığınız hesaplar aracılığıyla yine de tanıyabilir.
- VPN; kötü amaçlı yazılıma, oltalamaya veya ele geçirilmiş bir tarayıcıya karşı koruma sağlamaz.
- Tünel dışından yönlendirilen trafik (§9) korunmaz.

16 Olay müdahalesi ve olay kaydı

Bir VPN sunucusunun ele geçirildiğinden şüphelenirsek sunucuyu uygulamalardan gizler, anahtarlarını ve bağlantı kimlik bilgilerini değiştirir ve sunucuyu yeniden kurarız. Bir ihlal kişisel verileri etkilerse etkilenen kullanıcılara gereksiz gecikme olmadan e-posta gönderir ve ne olduğunu bu bölümde ve Güven Merkezi'nde yayımlarız. Hizmet durumu status.colitu.com adresinde herkese açıktır.

17 Altyapı

- Tüm sunucular, birbirinden bağımsız birkaç barındırma sağlayıcısından kiralanmış sanal makinelerdir. VPN sunucuları birkaç ülkeye dağılmıştır; güncel liste sunucular sayfasındadır. Hesap veritabanını tutan kontrol düzlemi Türkiye'deki bir sunucuda çalışır.
- Diskler şifreli değildir. Barındırma sağlayıcılarının kendi makinelerine teknik erişimi vardır.
- Yönetici erişimi yalnızca anahtarla SSH üzerinden yapılır; parolayla oturum açma devre dışıdır. Anahtarlar yalnızca Colitu ekibindedir.
- Sunucuların çoğunda otomatik güvenlik güncellemeleri etkindir; tümünde etkinleştirilmesi yol haritasındadır.

- Kontrol düzlemi ve bazı VPN sunucuları varsayılan olarak her şeyi reddeden (default-deny) bir güvenlik duvarı kullanır. Diğer VPN sunucularında yalnızca VPN hizmetleri, SSH ve ölçüm uç noktası dinler; her yerde default-deny güvenlik duvarı yol haritasındadır.
- Kontrol düzlemi veritabanına internetten erişilemez. VPN sunucularının ona erişimi yoktur.
- İki sunucu, küçük ve sabit bir alan adı kümesini (birinde Google hizmetleri, diğerinde Google'ın yapay zekâ hizmetleri) Cloudflare WARP üzerinden gönderir; böylece bu hizmetler Avrupa'da bir konum görür. Bu alan adları için çıkış noktası Cloudflare'dir ve bir VPN sunucusunun göreceği üst verinin aynısını görür.
- Bir röle giriş sunucusu, şifreli paketleri değiştirmeden Letonya'daki bir çıkış sunucusuna iletir. Giriş sunucusu trafiğin şifresini çözemez; herhangi bir ağın göreceği gibi IP adresinizi görür.

18 Güvenlik açığı bildirimi

Güvenlik sorunlarını security@colitu.com adresine gizli olarak bildirin (bu adres /.well-known/security.txt dosyasında da yer alır). Lütfen yeniden üretme adımlarını ve etkilenen sürümü ekleyin. Politikanın tamamı colitu.com/responsible-disclosure adresindedir.

- Bildirimlerin alındığını 3 iş günü içinde onaylar ve 10 iş günü içinde ilk değerlendirmeyi iletiriz.
- Ayrıntıları yayımlamadan önce lütfen sorunu düzeltmemiz için bize makul bir süre tanıyın.
- Diğer kullanıcıların verilerinden uzak duran, hizmeti aksatmayan ve gizli olarak bildirilen iyi niyetli araştırmalara karşı hukuki işlem başlatmayız.
- İsmi belirtilmek isteyen araştırmacıların ismini belirtiriz. Hata ödül programı (colitu.com/bug-bounty) kapsamında hesabınızdan gönderdiğiniz ve doğrulanan bildirimleri önem derecesine göre 1 ila 12 ay Plus ile, kritik açıkları nakit ödülle ödüllendiririz.
- Kapsamdakiler: uygulamalar, colitu.com ve alt alan adları, API ve VPN sunucuları. Kapsam dışındakiler: hizmet engelleme (DoS), spam, sosyal mühendislik ve §11 bölümündeki üçüncü taraflar.

19 Denetim durumu

Colitu henüz bağımsız bir üçüncü taraf güvenlik denetiminden veya sızma testinden geçmemiştir. Mevcut güvence şunlardan oluşur:

- Android, Windows, Linux ve iOS uygulamaları için herkese açık kaynak kod;
- otomatik kod taraması (CodeQL) ve bağımlılık güncellemeleri (Dependabot);
- uygulamaların iç güvenlik incelemeleri (Ekim 2026) ve bu belgenin dayandığı doğrulama çalışması;
- herkese açık bir güvenlik açığı bildirimi süreci.

Bağımsız bir denetim planlanmaktadır ancak henüz tarihi belirlenmemiştir.

20 Bilinen sınırlamalar

- Henüz bağımsız bir güvenlik denetimi yok.
- VPN sunucuları ve barındırma sağlayıcıları güvenmeniz gerekenlerin bir parçasıdır; sunucu diskleri şifreli değildir.
- Gizlilik modu kapatıldığında yerleşik listedeki bazı bölgesel siteler Windows, Android, iOS ve Linux uygulamalarında VPN dışından gider. Gizlilik modu Windows ve Android 2.7.0, iOS 5.6.0 ve Linux 1.3.0'dan beri yeni kurulumlarda varsayılan olarak açıktır; ancak daha önce kurulmuş olanlar önceki ayarını korur.
- Yeni Windows kurulumları TUN modunda başlar, ancak sistem proxy modunu kullanmış kurulumlar onu korur ve proxy modu her uygulamayı, sistem DNS çözümleyicisini veya IPv6'yı kapsamaz. Windows'un normal bir yeniden başlatılması, Colitu oturum açılırken yeniden bağlanacak şekilde ayarlı değilse kill switch engellemesini sonlandırır.
- Android'in kendine ait bir kill switch'i yoktur ve varsayılan olarak kapalı iki sistem ayarı gerektirir; iOS'taki "VPN olmadan interneti engelle" anahtarı varsayılan olarak kapalıdır ve açıkken Wi-Fi giriş sayfalarının açılmasını engeller.
- İki adımlı doğrulama yönetici hesapları için zorunludur, kullanıcılar için yalnızca isteğe bağlıdır.
- Faturalandırma kayıtları ve denetim logu için henüz otomatik silme yoktur (§10).
- Kendi kök sertifikasıyla HTTPS'i denetleyen güvenlik yazılımları, sertifika sabitleme nedeniyle uygulamaların API bağlantısını engeller; bunlarda Colitu'nun hariç tutulması gerekir. Passkey'ler yalnızca colitu.com'da çalışır: ayna alan adlarında ve uygulamaların içinde çalışmaz.
- Windows uygulaması Authenticode ile imzalı değildir ve iOS ile Linux derlemeleri henüz tekrarlanabilir değildir.
- Shadowsocks 2022'de ileri gizlilik yoktur; Trojan TLS 1.2'yi kabul eder.

21 1.4 ile 1.9 arasındaki sürümlerdeki değişiklikler

1.3 sürümü, uygulamaları son sürümlerden önceki hâliyle anlatıyordu. Bu sürüm bugün yayında olanı anlatır.

- İki adımlı doğrulama (TOTP) yalnızca yöneticiler için değil, her kullanıcı hesabı için kullanılabilir. Uygulamalar oturum açarken kodu ister.
- Windows: kill switch artık kalıcı güvenlik duvarı kuralları olan ayrı bir Windows hizmetidir. Uygulama veya VPN çekirdeği çökse bile engellemeyi sürdürür (artık fail-open değildir). Windows'un normal bir yeniden başlatılması, Colitu oturum açılırken yeniden bağlanacak şekilde ayarlı değilse engellemeyi yine sonlandırır. Yeni kurulumlar TUN modunda başlar.
- Bölünmüş tünel dört uygulamada da var: Windows, Android ve Linux'ta uygulamalar, siteler ve IP adresleri; iOS'ta siteler ve IP adresleri.

- iOS: IPv6 artık sızmaz ve isteğe bağlı bir "VPN olmadan interneti engelle" anahtarı (varsayılan olarak kapalı) tünel dışındaki trafiği engeller.
- Gizlilik modu (yeni kurulumlarda varsayılan olarak açık), Windows, Android, iOS ve Linux kullanıcılarının bazı bölgesel siteleri VPN dışına gönderen yerleşik kuralın etkin olup olmayacağına karar vermesini sağlar.
- Multihop (çift VPN) ve değişen IP, VLESS sunucularıyla kullanılabilir.
- Reklam engelleyici, 7 Ekim 2026'dan itibaren beş kategorili (reklam ve izleyiciler, zararlı yazılım, kimlik avı, dolandırıcılık, kripto madenciliği) isteğe bağlı DNS koruması Colitu Shield oldu. Çözümleyicileri sorgu kaydı ve istatistik tutmaz, yeni veri toplanmaz. İsteğe bağlı yetişkin içeriği filtresi, kişisel listeler, cihazda hesaplanan sayaç ve kategori başına anahtarlar yol haritasındadır, henüz yayında değildir.
- Bu belgedeki, indirme sayfalarındaki ve açık kaynak sayfasındaki sürümler, tarihler ve sağlama toplamları artık tek bir sürüm manifestosundan gelir.
- 1.5 sürümü (9 Ekim 2026): ücretli planlar (Kişisel, Plus ve Aile) satışta; ödeme bir ödeme sağlayıcısının sayfasında yapılır ve kart bilgileri Colitu'ya ulaşmaz. Ücretli planların sunulmadığı yönündeki ifade kaldırıldı. Bu belgede anlatılan başka bir uygulama değişmedi.
- 1.6 sürümü (10 Ekim 2026): web sitesi için passkey'ler, oturum denetimli bir oturum listesi, güvenlik e-postaları, parola sıfırlamadan sonra hesap silme ve iki adımlı doğrulamayı kapatma üzerinde 24 saatlik kilit, parola yeniden doğrulama denemelerine sınır, süre sınırlı adlandırılmış ek abonelik bağlantıları, yönetici hesapları için isteğe bağlı donanım güvenlik anahtarları ve dört uygulamada API bağlantısının Let's Encrypt (ISRG) ve Google Trust Services kök sertifika otoritelerine sabitlenmesi. Bu belgede anlatılan başka bir uygulama değişmedi.
- 1.7 sürümü (16 Ekim 2026): yedekler. Şifre çözme anahtarı çevrimdışına taşındı ve artık sunucuda saklanmıyor. Günlük şifreli bir kopya, 30 günlük silme kilidiyle Backblaze B2'de (EU Central) sunucu dışında tutuluyor ve en geç 36 gün sonra siliniyor. Dağıtımdan önce alınan şifrelenmemiş anlık görüntüler 7 gün sonra siliniyor. Backblaze üçüncü taraflar listesine eklendi. Bu belgede anlatılan başka bir uygulama değişmedi.
- 1.8 sürümü (20 Ekim 2026): Android (2.9.3 sürümünden itibaren) ve Windows (2.9.8 sürümünden itibaren) için tekrarlanabilir derlemeler. Bu belgede anlatılan başka bir uygulama değişmedi.
- 1.9 sürümü (28 Ekim 2026): hata ödül programı (1 ila 12 ay Plus, kritik açıklarda nakit ödül) bu belgeye eklendi; ücretli ödül sunulmadığını söyleyen ifade kaldırıldı. İç güvenlik değerlendirme raporu colitu.com/security-assessment adresinde yayımlandı. Bu belgede anlatılan başka hiçbir uygulama değişmedi.

22 Güvenlik yol haritası

Sıradakiler (2026 4. çeyrek)

- Yasal saklama süresi dolan faturalandırma kayıtlarının otomatik silinmesi.

- Tam IP adresi içermeyen, daha kısa süreli web sitesi erişim logları.
- Her sunucuda default-deny güvenlik duvarı ve otomatik güvenlik güncellemeleri.
- Trojan için TLS 1.3'ün zorunlu kılınması.

Daha sonra

- Windows için Authenticode imzalama.
- iOS ve Linux için tekrarlanabilir derlemeler ve her platform için SBOM.
- Harici bir sızma testi ve bağımsız bir denetim.
- Güvenlik bildirimleri için bir PGP anahtarı ve üç aylık şeffaflık raporları.

23 Yargı yetkisi

Colitu, İngiltere ve Galler'de tescilli COLITU LIMITED (kayıtlı adres: 128 City Road, London, Birleşik Krallık, EC1V 2NX; şirket numarası 17520342) tarafından işletilir ve İngiltere ve Galler hukukuna tabidir. Hesap veritabanı Türkiye'deki bir sunucudadır; VPN sunucuları sunucular sayfasında gösterilen ülkelerdedir ve bulundukları yerin yerel hukukuna tabidir. Yalnızca elimizde olan verileri teslim edebiliriz; bu verilerin tamamı §10 bölümünde listelenmiştir. Aldığımız talepler Güven Merkezi'ndeki şeffaflık raporlarında sayı olarak yer alır.

24 Kaynaklar

- Hysteria 2 protokolü: v2.hysteria.network
- Xray-core ve REALITY: github.com/XTLS
- sing-box: sing-box.sagernet.org
- TLS 1.3: RFC 8446 · QUIC: RFC 9000 · security.txt: RFC 9116
- Argon2: RFC 9106
- OWASP ASVS ve MASVS
- Android VpnService, Apple Network Extension ve Windows Filtering Platform belgeleri