



نسخه 1.6 · 10 اکتبر 2026

سند فنی امنیت Colitu

معماری امنیتی، مدل تهدید و طراحی حریم خصوصی

اینکه هنگام استفاده از Colitu باید به چه چیزی اعتماد کنید، چه کسی چه چیزی را می بیند، Colitu در برابر کدام حمله ها محافظت می کند و در برابر کدام نه، و چگونه می توانید ادعاهای ما را بررسی کنید. هر عبارت این سند آنچه را که امروز عرضه می شود توصیف می کند. هر جا چیزی وجود ندارد یا ضعیف تر از حد لازم است، آن را می گوئیم.

تماس امنیتی

security@colitu.com

آخرین به روزرسانی

10 اکتبر 2026

نسخه

1.6

محدوده کاربرد

2026، عامل گره تا 7 اکتبر 2026
Linux 1.5.0 · Windows 2.9.0 · Android 2.9.0 (بتا) · iOS 5.8.0 (TestFlight) · صفحه کنترل تا 10 اکتبر

کد منبع

برنامه های Android و Windows و Linux: github.com/colitu؛ برنامه iOS: github.com/colitu/ios
(همه تحت GPL-3.0). نرم افزار سرور: کد بسته.

امنیت Colitu در یک نگاه

خلاصه‌ای از بخش‌های زیر. سبز: روی همه پلتفرم‌های نام‌برده همان‌طور که توضیح داده شده کار می‌کند. زرد: به‌طور جزئی یا با محدودیت‌های مستند. قرمز: هنوز در دسترس نیست.

برنامه‌های متن‌باز	● برنامه‌های Android و iOS و Windows و Linux متن‌باز هستند (GPL-3.0). نرم‌افزار سرور بسته است.
تونل رمزگذاری‌شده	● Hysteria2 و VLESS Reality و VLESS XHTTP و Trojan و Shadowsocks 2022 با پیاده‌سازی‌های شناخته‌شده (Xray-core و sing-box و Hysteria).
محتوای ترافیک و سابقه مرور	● ثبت نمی‌شود. سرورهای VPN هیچ گزارش اتصالی به‌ازای هر اتصال نگه نمی‌دارند.
حجم ترافیک به‌ازای هر کاربر	● روی هر سرور در بازه‌های تقریباً 15 ثانیه‌ای ثبت می‌شود و برای سهمیه‌ها 90 روز نگه داشته می‌شود؛ پس از آن فقط جمع هر دوره.
DNS از طریق تونل	● در برنامه‌های Android و iOS و در حالت TUN بله. در حالت پروکسی سیستمی (پیش‌فرض Linux؛ نصب‌های جدید Windows در حالت TUN شروع می‌شوند) برای برنامه‌هایی که خارج از پروکسی هستند نه.
محافظت در برابر نشت IPv6	● در Android و iOS مسدود است، و در Windows و Linux در حالت TUN با روشن بودن قطع‌کن اضطراری (Kill Switch). حالت پروکسی سیستمی را پوشش نمی‌دهد.
قطع‌کن اضطراری (Kill Switch)	● Windows: سرویس مستقل با قوانین دائمی دیوار آتش؛ Linux (حالت TUN): قوانین nftables؛ هر دو در صورت از کار افتادن برنامه به مسدودسازی ادامه می‌دهند. Android به تنظیم «VPN همیشه روشن» سیستم متکی است؛ iOS یک گزینه اختیاری «مسدود کردن اینترنت بدون VPN» دارد (به‌صورت پیش‌فرض خاموش).
سایت‌های منطقه‌ای که خارج از VPN مسیریابی می‌شوند	● از Windows و Android نسخه 2.7.0 و iOS نسخه 5.6.0 و Linux نسخه 1.3.0 برای نصب‌های جدید به‌صورت پیش‌فرض خاموش است (حالت حریم خصوصی روشن است)؛ نصب‌های قبلی تنظیم قبلی خود را حفظ می‌کنند. وقتی حالت حریم خصوصی خاموش شود، در هر چهار برنامه سایت‌های فهرست داخلی خارج از VPN می‌روند، مگر زمانی که به سروری در همان منطقه وصل باشید. شرح آن در 9S آمده است.
تأیید دومرحله‌ای برای کاربران	● برای هر حساب اختیاری است (در وب‌سایت تنظیم می‌شود)؛ هر چهار برنامه هنگام ورود کد را می‌پرسند. برای حساب‌های مدیر اجباری است.

● کلید عبور برای وبسایت (تا 10 عدد برای هر حساب)؛ صفحه امنیت نشست‌های مرورگر را فهرست می‌کند و پایان می‌دهد؛ تغییر رمز عبور همه نشست‌های دیگر را پایان می‌دهد. برنامه‌ها مثل قبل با رمز عبور وارد می‌شوند.	کلیدهای عبور (passkey) و کنترل نشست
● از نسخه‌های برنامه در 10 اکتبر 2026، هر چهار برنامه مراجع صدور گواهی ریشه Let's Encrypt (ISRG) و Google Trust Services را برای API سنجاق (pinning) می‌کنند. محدودیت‌ها: 12S.	اتصال API سنجاق شده در برنامه‌ها
● برنامه‌ها، سایت‌ها و نشانی‌های IP در Windows و Android و Linux (برنامه‌ها در حالت TUN فقط در Windows و Linux)؛ سایت‌ها و نشانی‌های IP در iOS، که VPN به‌ازای هر برنامه را فقط برای پروفایل‌های مدیریت شده مجاز می‌کند.	تونل‌زنی تقسیم شده
● اختیاری. دامنه‌های تبلیغات، ردیاب‌ها، بدافزار، فیشینگ، کلاهبرداری و استخراج رمزارز را مسدود می‌کند (حدود 380 هزار قانون). هیچ گزارش پرس‌وجو و هیچ آماری روی حل‌کننده‌های آن نیست.	Colitu Shield (محافظت DNS)
● در هیچ برنامه‌ای (Android، iOS، Windows، Linux) وجود ندارد. از برنامه iOS در نسخه 5.4.1 حذف شد.	تحلیل‌گر شخص ثالث
● مانیفست به‌روزرسانی امضا شده (ECDSA P-256) به‌علاوه SHA-256 در Android و Windows و Linux؛ امضای App Store در iOS.	به‌روزرسانی‌های امضا شده
● هنوز نه.	امضای کد Windows (Authenticode)
● هنوز نه.	ساخت‌های بازتولیدپذیر
● SPDX برای هر انتشار GitHub برنامه‌های Android و Windows؛ Linux هنوز نه.	SBOM
● هنوز انجام نشده است.	ممیزی امنیتی مستقل
● security@colitu.com، سیاست در 18S و security.txt.	افشای مسئولانه آسیب‌پذیری
● ارائه نمی‌شود. Colitu همه سرورها را خودش اجرا می‌کند.	میزبانی شخصی

1 خلاصه اجرایی

Colitu یک سرویس VPN با برنامه‌هایی برای Android و Windows و Linux و iOS است. این سرویس برای شبکه‌های محدود یا ناپایدار ساخته شده است؛ هر سرور چند روش انتقال ارائه می‌دهد و برنامه روشی را برمی‌گزیند که

روی شبکه کاربر کار می‌کند.

هدف طراحی این است که حجم داده‌های حساس در هر نقطه واحد کم بماند. حساب‌ها و پرداخت‌ها روی یک صفحه کنترل قرار دارند که هرگز ترافیک VPN را حمل نمی‌کند. سرورهای VPN ترافیک را حمل می‌کنند اما نشانی ایمیل یا داده‌های پرداخت ندارند. برنامه‌ها اعتبارنامه‌های خود را در فضای ذخیره‌سازی امن هر پلتفرم نگه می‌دارند.

این سند معماری، مدل تهدید، پروتکل‌ها، نحوه مدیریت کلیدها و حساب‌ها، آنچه ثبت می‌شود، نحوه محافظت از به‌روزرسانی‌ها، محدودیت‌های شناخته‌شده و کارهای باقی‌مانده را شرح می‌دهد. برای خوانندگانی نوشته شده است که می‌خواهند ادعاهای ما را بررسی کنند، نه اینکه صرفاً به آن‌ها اعتماد کنند.

اصول

- تا حد امکان کم جمع‌آوری کنیم و دقیقاً بگوییم چه چیزی جمع‌آوری می‌کنیم.
- ترافیک بین برنامه و سرور VPN را با پروتکل‌های شناخته‌شده رمزگذاری کنیم. Colitu رمزنگاری اختصاصی خودش را ندارد.
- حساب‌ها و پرداخت‌ها را از سرورهایی که ترافیک را حمل می‌کنند جدا نگه داریم.
- محدودیت‌های مستند را به وعده‌های کلی ترجیح دهیم.
- رفتار برنامه‌ها را قابل بررسی کنیم: کد منبع برنامه‌های Android و Windows و Linux و iOS را منتشر کنیم.

VPN شما را ناشناس نمی‌کند. VPN اعتماد را از شبکه محلی و ارائه‌دهنده اینترنت شما به اپراتور VPN منتقل می‌کند. این سند توضیح می‌دهد که این اعتماد چه چیزهایی را در بر می‌گیرد.

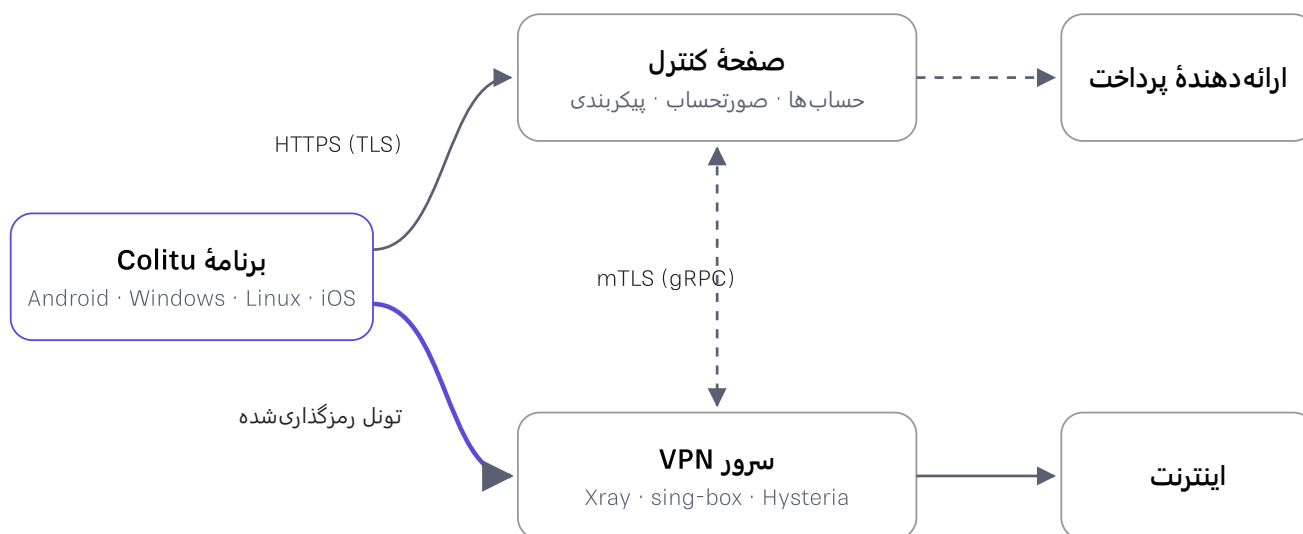
2 دامنه

شامل می‌شود: برنامه‌های Colitu برای Android و Windows و Linux و iOS؛ صفحه کنترل (API حساب، صورتحساب، پیکربندی، پنل مدیریت)؛ سرورهای VPN و عامل گره که آن‌ها را پیکربندی می‌کند؛ سرورهای DNS مربوط به Colitu Shield؛ توزیع به‌روزرسانی‌ها؛ colitu.com و زیردامنه‌های آن.

شامل نمی‌شود: امنیت سیستم عامل و دستگاه کاربر، افزونه‌های مرورگر و سایر نرم‌افزارهای روی دستگاه، امنیت داخلی ارائه‌دهنده پرداخت و سایر اشخاص ثالث نامبرده در §11، و وبسایت‌هایی که کاربر بازدید می‌کند.

3 معماری

Colitu صفحه کنترل را، که می‌داند کاربران چه کسانی هستند، از صفحه داده، که ترافیک آن‌ها را حمل می‌کند، جدا می‌کند.



صفحه کنترل و صفحه داده. صفحه کنترل هرگز ترافیک VPN را حمل نمی‌کند؛ سرورهای VPN ایمیل یا داده‌های پرداخت ندارند.

اجزا

جزء	مسئولیت‌ها	آنچه نگه می‌دارد
برنامه	ورود، انتخاب سرور، انتخاب پروتکل و بازگشت به روش دیگر، برپایی تونل، تنظیمات مسیریابی و DNS، قطع‌کن اضطراری (Kill Switch) در جاهایی که وجود دارد، بررسی به‌روزرسانی.	توکن‌های نشست و تنظیمات اتصال فعلی (12§).
صفحه کنترل	حساب‌ها، ورود، اشتراک‌ها و پرداخت‌ها، ثبت دستگاه، تولید پیکربندی هر سرور، پنل مدیریت، پشتیبانی.	داده‌های حساب و صورتحساب (10§). روی یک سرور اجرا می‌شود؛ پایگاه داده از اینترنت قابل دسترسی نیست.
عامل گره	روی هر سرور VPN اجرا می‌شود. پیکربندی خود را از طریق TLS دوطرفه احرازهویت شده می‌گیرد، هسته‌های VPN را راه می‌اندازد و شمارنده‌های ترافیک به‌ازای هر کاربر و وضعیت سلامت را گزارش می‌کند.	کلیدهای پروتکل آن سرور و اعتبارنامه‌های اتصال کاربرانی که از آن استفاده می‌کنند، با شناسه داخلی کاربر. بدون نشانی ایمیل.
سرور VPN (صفحه داده)	تونل رمزگذاری شده را خاتمه می‌دهد و ترافیک را به اینترنت می‌فرستد.	چیزی فراتر از داده‌های عامل نیست. بدون گزارش ترافیک یا اتصال (10§).

جزء	مسئولیت‌ها	آنچه نگه می‌دارد
Colitu Shield DNS	حل‌کنندهٔ اختیاری (AdGuard Home) روی سه سرور VPN که از داخل تونل در دسترس است و دامنه‌های تبلیغات، ردیاب‌ها، بدافزار، فیشینگ، استخراج رمزارز را مسدود می‌کند: حدود 380 هزار قانون، فهرست‌ها هر 24 ساعت به روزرسانی می‌شوند. حل‌کننده‌های بالادستی Cloudflare و Quad9 از طریق HTTPS وارد می‌شود و توکن‌های کوتاه مدت دریافت می‌کند.	بدون گزارش پرس‌وجو، بدون آمار.

اتصال چگونه برقرار می‌شود

1. برنامه از طریق HTTPS وارد می‌شود و توکن‌های کوتاه مدت دریافت می‌کند. حل‌کننده‌های بالادستی Cloudflare و Quad9 از طریق HTTPS وارد می‌شود و توکن‌های کوتاه مدت دریافت می‌کند.
2. فهرست سرورها و تنظیمات اتصال سرور انتخاب می‌شود و صفحهٔ کنترل می‌خواهد.
3. روش‌های انتقال را به ترتیب امتحان می‌کند و اولین روشی را که بررسی اتصال را بگذراند نگه می‌دارد.
4. سپس ترافیک از برنامه ← سرور VPN ← اینترنت جریان می‌یابد. صفحهٔ کنترل در این مسیر نیست.

4 مدل اعتماد

هنگام استفاده از Colitu باید به این موارد اعتماد کنید:

- برنامهٔ Colitu که نصب کرده‌اید، و دستگاه و سیستم‌عاملی که روی آن اجرا می‌شود؛
 - سرور VPN که به آن وصل می‌شوید، و ارائه‌دهندهٔ میزبانی که آن را اجرا می‌کند (سرورهای VPN ماشین‌های مجازی اجاره‌ای بدون رمزگذاری دیسک هستند، بنابراین ارائه‌دهندهٔ میزبانی از نظر فنی به آن‌ها دسترسی دارد)؛
 - صفحهٔ کنترل Colitu و افرادی که آن را اداره می‌کنند؛
 - پیاده‌سازی‌های پروتکل که Colitu به کار می‌برد (Xray-core و sing-box و Hysteria) و کتابخانه‌های رمزنگاری زیر آن‌ها.
- لازم نیست برای محتوا یا مقصد ترافیک تونل‌شده به شبکهٔ محلی یا ارائه‌دهندهٔ اینترنت خود اعتماد کنید. آن‌ها همچنان می‌توانند این‌ها را ببینند:
- اینکه به یک سرور Colitu وصل می‌شوید، و نشانی IP و درگاه آن را؛
 - اینکه چه زمانی وصل هستید و تقریباً چه مقدار داده می‌فرستید و دریافت می‌کنید؛
 - شاید اینکه ترافیک، ترافیک VPN است، بسته به پروتکل و ابزارهای بازرسی شبکه؛
 - ترافیکی که برنامه عمداً خارج از تونل می‌فرستد: برخی سایت‌های منطقه‌ای (9S)، ترافیک شبکهٔ محلی، بررسی به روزرسانی و اندازه‌گیری تأخیر.

شما	شبکه محلی / ارائه‌دهنده اینترنت	سرور VPN	وبسایت
IP شما، IP سرور، زمان‌بندی و حجم را می‌بیند	IP شما، مقصدها و زمان‌بندی را می‌بیند؛ محتوای HTTPS را نه	IP سرور VPN را می‌بیند	

اینکه برای ترافیکی که از تونل می‌گذرد چه کسی چه چیزی را می‌بیند.

5 مدل تهدید

Colitu برای محافظت از ترافیک در برابر شبکه‌های محلی خصمانه یا غیرقابل اعتماد، ارائه‌دهندگان اینترنتی که آنچه انجام می‌دهید را می‌خوانند یا ثبت می‌کنند، و بسیاری از انواع فیلترینگ شبکه طراحی شده است. برای ایجاد ناشناسی در برابر مهاجمی که می‌تواند ورود و خروج ترافیک VPN را هم‌زمان مشاهده کند طراحی نشده است.

توضیح	محافظت می‌شود؟	تهدید
ترافیک تونل‌شده بین برنامه و سرور VPN رمزگذاری می‌شود.	بله ●	شنود در Wi-Fi عمومی
به‌جز ترافیکی که عمداً خارج از تونل مسیریابی می‌شود (9§).	بله، برای ترافیک تونل‌شده ●	ارائه‌دهنده اینترنت که محتوا یا مقصد ترافیک را می‌خواند
Reality و XHTTP و Hysteria2 طوری طراحی شده‌اند که شبیه TLS یا QUIC معمولی به نظر برسند، اما هیچ روش انتقالی غیرقابل تشخیص نیست.	گاهی ●	ارائه‌دهنده اینترنت که متوجه استفاده از VPN می‌شود
iOS و Android و حالت TUN در Windows از طریق تونل حل می‌کنند. حالت پروکسی Windows حل‌کننده سیستم را پوشش نمی‌دهد.	بیشتر اوقات ●	نشت DNS
به 9§ نگاه کنید.	تا حدی ●	نشت IPv6
Windows و Linux قطع‌کن اضطراری (Kill Switch) دارند که اگر برنامه از کار بیفتد مسدودسازی را ادامه می‌دهد (شکاف‌های مستند در ادامه)؛ Android به تنظیم سیستم نیاز دارد؛ iOS گزینه اختیاری «مسدود کردن اینترنت بدون VPN» دارد که به‌صورت پیش‌فرض خاموش است.	تا حدی ●	نشت هنگام قطع شدن تونل

توضیح	محافظة می شود؟	تهدید
TLS با اعتبارسنجی گواهی سیستم؛ از نسخه های برنامه در 10 اکتبر 2026، هر چهار برنامه مراجع صدور گواهی ریشه Let's Encrypt (ISRG) و Google Trust Services را نیز سنجاق می کنند، بنابراین گواهی ریشه ای که کسی روی دستگاه نصب کرده باشد برای خواندن ترافیک API قابل استفاده نیست.	بله ●	حمله مرد میانی روی API حساب
سرور نشانی IP شما و مقصد ترافیکتان را می بیند، هرچند محتوای اتصال های HTTPS را نه.	خیر ●	سرور VPN مخرب یا نفوذ شده
مهاجم به داده های حساب و صورتحساب دست می یابد و می تواند پیکربندی ها را به سرورها بفرستد. محتوای ترافیک هرگز آنجا نیست.	تا حدی ●	صفحه کنترل نفوذ شده
محدودیت نرخ حدس زدن را کند می کند و می توانید دستگاه ها را از حساب خارج کنید. تأیید دومرحله ای اختیاری (برنامه احراز هویت) یعنی رمز عبور سرقت شده به تنهایی دیگر وارد نمی شود، اما تا زمانی که روشنش نکنید خاموش است. کلیدهای عبور (passkey) روش ورود جایگزین در وبسایت هستند؛ تغییر رمز عبور همه نشست های دیگر را پایان می دهد، و بازنشانی رمز عبور حذف حساب و خاموش کردن تأیید دومرحله ای را 24 ساعت قفل می کند.	تا حدی ●	رمز عبور حساب به سرقت رفته
خارج از دامنه هر VPN.	خیر ●	بدافزار روی دستگاه شما
VPN نشانی IP شما را تغییر می دهد، نه هویتتان را در وبسایت ها.	خیر ●	اثر انگشت مرورگر، کوکی ها، حساب های وارد شده
زمان بندی و حجم را می توان بین تونل و اینترنت تطبیق داد.	خیر ●	همبستگی ترافیک توسط ناظر سراسری

مهاجمان بررسی شده

دسته	مثال	محافظة Colitu
A1 مهاجم شبکه محلی	کسی که روی همان Wi-Fi کافه است	قوی برای ترافیک تونل شده.
A2 ارائه دهنده اینترنت	ISP یا اپراتور همراه کاربر	قوی برای محتوا و مقصدها؛ زمان بندی و حجم همچنان قابل مشاهده می مانند.

دسته	مثال	محافظت Colitu
A3 سانسورگر	فیلترینگ سراسری شبکه با DPI و کاوش فعال	چند روش انتقال و بازگشت خودکار به روش دیگر؛ بدون تضمین (§14).
A4 سرور یا میزبان VPN مخرب	یک سرور نفوذ شده یا ارائه دهنده میزبانی خصمانه	محدود؛ همان فراداده‌ای را می‌بیند که سرور می‌بیند. اعتبارنامه‌ها برای هر سرور جدا هستند، بنابراین نمی‌توان از یک سرور برای دسترسی به بقیه استفاده کرد.
A5 صفحه کنترل نفوذ شده	مهاجمی با دسترسی به پنل	محدود؛ داده‌های حساب افشا می‌شود؛ محتوای ترافیک یا سابقه مروری برای برداشتن وجود ندارد.
A6 مهاجم نقطه انتهایی	بدافزار روی دستگاه کاربر	هیچ.
A7 مهاجم منفعل سراسری	ناظری که هر دو سر تونل را می‌بیند	هیچ.

6 پروتکل‌ها

هر سرور همین مجموعه روش‌های انتقال را ارائه می‌دهد. Colitu رمزنگاری ابداع نمی‌کند؛ رمزگذاری، احراز هویت و تبادل کلید را Xray-core و sing-box و Hysteria و کتابخانه‌هایی که به کار می‌برند فراهم می‌کنند.

روش انتقال	نحوه کار	احراز هویت سرور	نکات و محدودیت‌ها
Hysteria2	TLS 1.3 با QUIC (UDP)	گواهی صادر شده برای سرور توسط Let's Encrypt (ACME)	در شبکه‌های دارای افت بسته سریع است. جایی که UDP مسدود یا کند شده باشد شکست می‌خورد.
VLESS Reality	TCP؛ Reality یک دست‌دهی TLS 1.3 انجام می‌دهد که از یک وب‌سایت واقعی تقلید می‌کند و از کلیدهای X25519 استفاده می‌کند	کلید عمومی Reality سرور که همراه پیکربندی تحویل داده می‌شود	علیه DPI و کاوش فعال ساخته شده است. تضمینی در برابر مسدودسازی بر پایه IP نیست.
VLESS XHTTP	Reality به علاوه یک جریان شبیه HTTP	مانند Reality، با کلیدهای خودش	برای شبکه‌هایی که اتصال‌های TCP طولانی مدت را قطع می‌کنند.

روش انتقال	نحوه کار	احراز هویت سرور	نکات و محدودیت‌ها
Trojan	TCP یا TLS (نسخه 1.2 یا 1.3؛ سرور هنوز 1.3 را الزامی نمی‌کند)	همان گواهی Hysteria2	جایگزین TLS در جایی که UDP مسدود است.
Shadowsocks 2022	blake3-aes-256--2022 gcm (AEAD)، کلید جدید برای هر نشست	کلید از پیش به اشتراک گذاشته شده	سبک و سریع. بدون محرمانگی رو به جلو (forward secrecy): کلید فاش شده می‌تواند همهٔ نشست‌های ضبط شده را رمزگشایی کند.

اینکه کدام هسته یک روش انتقال را اجرا می‌کند به پلتفرم بستگی دارد. iOS و Android برای همهٔ روش‌های انتقال، از جمله Hysteria2، از Xray-core استفاده می‌کنند. Windows و Linux برای VLESS و Trojan و Shadowsocks از Xray-core و برای Hysteria2 از sing-box استفاده می‌کنند. روی سرورها، Xray پروتکل VLESS را اجرا می‌کند، sing-box پروتکل‌های Trojan و Shadowsocks را اجرا می‌کند و سرور رسمی Hysteria پروتکل Hysteria2 را اجرا می‌کند.

تعویض روش انتقال خودکار است اما بدون وقفه نیست؛ وقتی برنامه به روش انتقال دیگری می‌رود تونل بسته و دوباره ساخته می‌شود که حدود یک ثانیه یا بیشتر طول می‌کشد.

7 رمزنگاری و مدیریت کلید

هدف	سازوکار
برنامه و وبسایت به API	TLS 1.2/1.3 با اعتبارسنجی گواهی سیستم. از نسخه‌های برنامه در 10 اکتبر 2026، برنامه‌های Windows و Android و Linux و iOS کلیدهای ریشه Let's Encrypt (ISRG) و Google Trust Services را نیز برای API سنجاق می‌کنند. اجرای این سنجاق‌ها در 31 دسامبر 2027 متوقف می‌شود، بنابراین نسخه‌های قدیمی برنامه هرگز قفل نمی‌شوند.
ذخیره رمز عبور	Argon2id: حافظه 64 MiB، گذر، 2 مسیر، نمک تصادفی 16 بایتی، هش 32 بایتی. رمزهای عبور هرگز به صورت متن ساده ذخیره نمی‌شوند.
توکن‌های دسترسی	JWT امضا شده با HMAC-SHA256 از یک حلقه کلید چرخان، با اعتبار 15 دقیقه.
توکن‌های تازه‌سازی	32 بایت تصادفی، فقط به صورت هش SHA-256 ذخیره می‌شود، با اعتبار 30 روز، در هر استفاده جایگزین می‌شود. استفاده‌ی مجدد از توکن قدیمی کل خانواده توکن را باطل می‌کند.
صفحه کنترل → سرورهای VPN	TLS 1.3 دوطرفه (gRPC). مرجع صدور گواهی ECDSA P-256؛ گواهی‌های سرور 30 روز اعتبار دارند و خودکار تمدید می‌شوند؛ ابطال با فهرست مجاز اثر انگشت.

هدف	سازوکار
کلیدهای Reality	یک جفت کلید X25519 برای هر روش انتقال در هر سرور، تولیدشده روی صفحه کنترل.
گواهی‌های TLS سرور	Let's Encrypt، روی هر سرور صادر می‌شود؛ کلید خصوصی روی همان سرور می‌ماند.
رازها در پایگاه داده	اعتبارنامه‌های ارائه‌دهنده پرداخت، ایمیل و هوش مصنوعی با AES-256-GCM رمزگذاری می‌شوند.
مانیفست‌های به‌روزرسانی	امضاها ECDSA P-256 که برنامه‌ها در برابر یک کلید عمومی تعبیه‌شده راستی‌آزمایی می‌کنند.
پشتیبان‌ها	با age به یک کلید عمومی رمزگذاری می‌شوند؛ تهیه پشتیبان فقط به همان کلید نیاز دارد.
کلیدها و نگهداری آنها می‌شوند و اگر یکی فاش شود چه می‌شود	

اثر انگشت‌های بررسی HMAC-SHA256 زیر کلیدی که از کلید رمزگذاری تنظیمات مشتق شده و در پایگاه داده ذخیره نمی‌شود.

- کلید خصوصی مرجع صدور گواهی یک فایل روی صفحه کنترل است. هر کسی که آن را به دست آورد می‌تواند هویت سرور صادر کند، بنابراین حساس‌ترین کلیدی است که نگه می‌داریم.
- هر سرور VPN کلیدهای خصوصی Reality خودش، کلید گواهی TLS خودش و اعتبارنامه‌های اتصال کاربرانی را که از آن استفاده کرده‌اند نگه می‌دارد. این اعتبارنامه‌ها تصادفی و روی هر سرور متفاوت هستند، بنابراین سرور نفوذشده اعتبارنامه‌هایی را که روی سرورهای دیگر معتبرند افشا نمی‌کند.
- کلیدهای خصوصی Reality و اعتبارنامه‌های اتصال کاربران به‌صورت رمزگذاری‌نشده در پایگاه داده صفحه کنترل ذخیره می‌شوند. رمزگذاری این مقادیر در سطح پایگاه داده در نقشه راه است.
- هنوز چرخش زمان‌بندی‌شده کلیدهای Reality وجود ندارد. اگر به نفوذ به یک سرور مشکوک شویم، آن سرور از برنامه‌ها برداشته می‌شود و کلیدها و اعتبارنامه‌هایش تعویض می‌شوند.
- پشتیبان‌ها به یک کلید عمومی رمزگذاری می‌شوند و روی سرور صفحه کنترل نگه داشته می‌شوند. کلید رمزگشایی متناظر فعلاً هنوز روی همان سرور ذخیره است؛ انتقال آن به بیرون از خط و نگهداری یک نسخه خارج از محل در نقشه راه است.

8 حساب‌ها و نشست‌ها

- ورود با ایمیل و رمز عبور است. تلویزیون می‌تواند با نمایش یک QR که گوشی واردشده آن را تأیید می‌کند وارد شود (کد 8 نویسه‌ای، با اعتبار 10 دقیقه). ورود از طریق Google یا Telegram یا اشخاص ثالث دیگر وجود ندارد.
- رمز عبور باید دست‌کم 10 نویسه باشد. حساب جدید فقط پس از تأیید یک کد 6 رقمی که با ایمیل ارسال می‌شود به VPN دسترسی پیدا می‌کند.

- بازنشانی رمز عبور از یک کد 6 رقمی با اعتبار 15 دقیقه استفاده می‌کند که یک‌بار مصرف است و حداکثر 5 تلاش دارد. پاسخ چه برای نشانی‌ای که حساب دارد و چه برای نشانی‌ای که ندارد یکسان است. بازنشانی رمز عبور همه دستگاه‌ها و نشست‌های وب را خارج می‌کند. پس از بازنشانی با کد ایمیل، حذف حساب و خاموش کردن تأیید دومارحله‌ای به مدت 24 ساعت قفل می‌شوند (خطای RECOVERY_LOCKED).
- ورود، ثبت‌نام، بازنشانی رمز عبور و کدهای تبلیغاتی برای هر نشانی IP محدودیت نرخ دارند. در وب‌سایت، ورود و بازنشانی برای هر نشانی ایمیل هم محدود می‌شوند؛ در برنامه‌ها ورود فقط برای هر IP محدود می‌شود. برای حساب‌های کاربران قفل‌شدن وجود ندارد.
- خروج، توکن تازه‌سازی آن دستگاه را باطل می‌کند. توکن دسترسی آن تا زمان انقضا معتبر می‌ماند (حداکثر 15 دقیقه).
- می‌توانید دستگاه‌ها را از صفحه حساب خود حذف کنید. صفحه امنیت نشست‌های مرورگر را با برچسب دستگاه (مرورگر و سیستم‌عامل)، کشور، روش ورود و نشانی IP فهرست می‌کند؛ می‌توانید یک نشست را ببندید، همه نشست‌های دیگر را ببندید (نشست فعلی می‌ماند) یا از همه‌جا خارج شوید.
- تغییر رمز عبور در وب‌سایت نشست مرورگری را که در آن هستید نگه می‌دارد و همه نشست‌های وب دیگر و همه توکن‌های تازه‌سازی برنامه را پایان می‌دهد. توکن‌های دسترسی برنامه که پیش از تغییر صادر شده‌اند بلافاصله از کار می‌افتند (خطای AUTH_SESSION_REVOKED).
- اقداماتی که دوباره رمز عبور می‌خواهند (تغییر رمز عبور، حذف حساب، تغییرات تأیید دومارحله‌ای، کلیدهای عبور) به 10 تلاش در هر 15 دقیقه برای هر حساب محدود هستند.
- تأیید دومارحله‌ای (TOTP) برای هر حساب اختیاری است. آن را در colitu.com/account/security با یک برنامه احراز هویت روشن می‌کنید و 10 کد بازیابی یک‌بار مصرف دریافت می‌کنید؛ پس از آن برنامه‌ها پس از رمز عبور کد را می‌پرسند (پشتیبانی از Windows 2.6.0, Android 2.6.0, Linux 1.2.0 و iOS 5.5.0؛ برنامه قدیمی‌تر از شما می‌خواهد به‌روزرسانی کنید). فقط در وب‌سایت تنظیم می‌شود.
- کلیدهای عبور (passkey): در colitu.com می‌توانید در بخش حساب ← امنیت تا 10 کلید عبور اضافه کنید (نیازمند رمز عبور)، برای هر کدام نام بگذارید و با رمز عبور حذف کنید، و سپس در صفحه ورود از «ورود با کلید عبور» استفاده کنید. کلید عبور دارای تأیید کاربر دو عامل به حساب می‌آید، بنابراین از کد تأیید دومارحله‌ای عبور می‌کند؛ ورود از کشوری که در 90 روز گذشته دیده نشده همچنان کد ایمیل می‌خواهد. کلیدهای عبور روی دامنه‌های آینه کار نمی‌کنند. برنامه‌ها مثل قبل وارد می‌شوند، یا با تأیید یک کد QR اتصال دستگاه در مرورگری که با کلید عبور وارد شده است.
- Colitu برای این موارد ایمیل امنیتی می‌فرستد: دستگاه جدید برنامه (نه برای اولین دستگاه)، ورود از کشور جدید (در 90 روز دیده نشده)، روشن یا خاموش شدن تأیید دومارحله‌ای، ساخت مجدد کدهای بازیابی، افزودن یا حذف کلید عبور، و تغییر رمز عبور.
- پیوندهای اشتراک: علاوه بر پیوند اصلی، می‌توانید تا 5 پیوند اضافی نام‌دار بسازید، هر کدام با انقضای اختیاری 7 یا 30 یا 90 روز، و آن‌ها را یکی‌یکی باطل کنید. وقتی پیوندی در مدت کوتاه از شبکه‌های متفاوت بسیاری استفاده شود هشدار ظاهر می‌شود. Colitu برای این کار هیچ نشانی IP ذخیره نمی‌کند، فقط شمارش ناشناس روزانه شبکه‌های متمایز را که 48 ساعت نگه داشته می‌شود.

اعتبارنامه‌های اتصال به‌ازای هر دستگاه (و هر پیوند اشتراک) و هر سرور صادر می‌شوند. حذف یک دستگاه یا چرخاندن پیوند اشتراک، اعتبارنامه‌هایش را از همه سرورها حذف می‌کند: اتصال‌های جدید از آن ظرف حدود 15 ثانیه رد می‌شوند و اتصال‌های از قبل باز با بسته شدنشان پایان می‌یابند. دستگاهی که به این دلیل متوقف شده که طرح شما دستگاه کمتری مجاز می‌داند، تا زمانی که دوباره فعالش کنید به همین شکل کنار گذاشته می‌شود. اگر دستگاهی گم شد، رمز عبور خود را هم تغییر دهید.

دسترسی مدیران

Colitu را تیمی بسیار کوچک اداره می‌کند. پنل مدیریت در نشانی جداگانه و با مجوزهای مبتنی بر نقش قرار دارد، نقاط پایانی مدیریتی روی API عمومی بسته‌اند، حساب‌های مدیر پس از 5 تلاش ناموفق 15 دقیقه قفل می‌شوند و اقدامات مدیر در یک گزارش ممیزی نوشته می‌شود. تأیید دومرحله‌ای (TOTP) برای حساب‌های مدیر اجباری است: مدیری که آن را ندارد فقط پس از ورود می‌تواند آن را تنظیم کند و هر ورود بعدی به کد یا یک کد بازیابی یک‌بار مصرف نیاز دارد (تلاش‌ها محدودیت نرخ دارند). مدیر همچنین می‌تواند یک کلید امنیتی سخت‌افزاری (WebAuthn) ثبت کند؛ پس از ثبت، ورود به‌جای TOTP به رمز عبور و کلید نیاز دارد و یک کد بازیابی یک‌بار مصرف به‌عنوان جایگزین اضطراری ثبت‌شده در گزارش باقی می‌ماند. کلید گم‌شده با کد بازیابی یا، پس از بررسی هویت خارج از کانال، با یک فرمان بازنشانی ثبت‌شده در گزارش روی سرور جایگزین می‌شود. دسترسی با غیرفعال کردن حساب لغو می‌شود که از درخواست بعدی اثر می‌کند. نشست‌های مدیر به مرورگر و شبکه‌ای که از آن باز شده‌اند گره خورده‌اند.

9 ترافیک، DNS، IPv6 و قطع‌کن اضطراری

سرور VPN چه چیزی را می‌تواند ببیند

سرور VPN باید بداند ترافیک شما را کجا بفرستد، بنابراین از نظر فنی نشانی IP شما، نشانی‌های IP و اغلب نام میزبان (TLS SNI) سایت‌هایی که به آن‌ها وصل می‌شوید، و زمان‌بندی و حجم ترافیک شما را می‌بیند. نمی‌تواند محتوای اتصال‌های HTTPS را بخواند، که بین دستگاه شما و وب‌سایت رمزگذاری شده می‌ماند. Colitu ترافیک HTTPS را رمزگشایی یا بازرسی نمی‌کند.

پیش‌فرض‌های مسیریابی

Linux (بتا)	iOS	Windows	Android	ترافیک چگونه گرفته می‌شود
پروکسی سیستمی به‌صورت پیش‌فرض؛ حالت TUN اختیاری	VPN سیستمی (همه برنامه‌ها)	حالت TUN (همه ترافیک) برای نصب‌های جدید؛ نصب‌هایی که از حالت پروکسی سیستمی استفاده می‌کردند آن را نگه می‌دارند	VPN سیستمی (همه برنامه‌ها)	

Android	Windows	iOS	Linux (بتا)
به طور پیش فرض پوشش داده نمی شود	در حالت پروکسی سیستمی: برنامه هایی که پروکسی سیستم را نادیده می گیرند، حل کننده DNS ویندوز، UDP مرورگر (QUIC/WebRTC)، IPv6. حالت TUN آن ها را پوشش می دهد.	شبکه محلی	مانند Windows در حالت پروکسی سیستمی
سایت ها و IP های منطقه ای (فهرست داخلی)	فقط اگر حالت حریم خصوصی خاموش باشد، مگر اینکه سرور در آن منطقه باشد	فقط اگر حالت حریم خصوصی خاموش باشد	فقط اگر حالت حریم خصوصی خاموش باشد خارج از VPN است، مگر اینکه سرور در آن منطقه باشد
DNS	TUN: از طریق تونل به DNS-over-HTTPS مربوط به Cloudflare. حالت پروکسی: فقط برای ترافیکی که به پروکسی می رسد.	از طریق تونل (8.8.8.8 ← Xray ← 1.1.1.1)	مانند Windows
IPv6	در حالت TUN با قطع کن اضطراری مسدود است؛ در حالت پروکسی سیستمی پوشش داده نمی شود	نشت نمی کند: به تونل هدایت می شود و همان جا حذف می شود	مانند Windows

Android	Windows	iOS	Linux (بتا)
● از تنظیمات VPN» همیشه روشن» و «مسدود کردن اتصال‌های بدون VPN» در Android استفاده می‌کند که کاربر باید روشنشان کند	● سرویس مستقل Windows با قوانین دائمی Windows Filtering Platform، به صورت پیش فرض روشن (در ادامه ببینید)	● «مسدود کردن اینترنت بدون iOS» (VPN، includeAllNetworks)، به صورت پیش فرض خاموش؛ تا وقتی روشن است صفحات ورود Wi-Fi باز نمی‌شوند. «همیشه روشن» فقط دوباره وصل می‌کند	● قوانین nftables که با از کار افتادن برنامه باقی می‌مانند؛ فقط حالت TUN
● برنامه‌ها، سایت‌ها و نشانی‌های IP	● برنامه‌ها (فقط حالت TUN)، سایت‌ها و نشانی‌های IP	● فقط سایت‌ها و نشانی‌های IP فقط برای پروفایل‌های مدیریت شده VPN به ازای هر برنامه را مجاز می‌کند	● برنامه‌ها (فقط حالت TUN)، سایت‌ها و نشانی‌های IP
● فقط VLESS	● فقط VLESS	● فقط VLESS	● فقط VLESS
چندجهشی IP و (MultiHop) چرخان			

سایت‌های منطقه‌ای خارج از VPN

برخی سایت‌های منطقه‌ای (دامنه‌ها و بازه‌های IP در یک فهرست داخلی) مستقیم و خارج از تونل باز می‌شوند تا سرویس‌هایی که نشانی‌های IP خارجی را نمی‌پذیرند به کار خود ادامه دهند. وقتی به سروری در همان منطقه وصل هستید این مورد اعمال نمی‌شود. برای این ترافیک، سایت و ارائه‌دهنده اینترنت شما نشانی IP واقعی شما را می‌بینند. این قاعده فقط زمانی اعمال می‌شود که حالت حریم خصوصی خاموش باشد. حالت حریم خصوصی برای نصب‌های جدید به صورت پیش فرض روشن است (Windows و نسخه 2.7.0، iOS نسخه 5.6.0، Linux نسخه 1.3.0 و بعدتر)، بنابراین به طور پیش فرض همه ترافیک از VPN می‌گذرد؛ نصب‌های قبلی تنظیم قبلی خود را حفظ می‌کنند. وقتی این قاعده فعال است، اولین باری که وصل می‌شوید برنامه یک اعلان یک‌باره نشان می‌دهد که این موضوع را توضیح می‌دهد. می‌توانید سروری در همان منطقه هم انتخاب کنید.

قطع‌کن اضطراری Windows به تفصیل

- همه ترافیک IPv4 و IPv6 را مسدود می‌کند، به جز loopback، شبکه محلی (یک تنظیم، به صورت پیش فرض روشن)، DHCP، هسته‌های VPN، مبدل TUN و خود برنامه Colitu.

- در کل نشست فعال است، هم در حالت TUN و هم در حالت پروکسی سیستمی. در حالت پروکسی، برنامه‌هایی که از پروکسی استفاده نمی‌کنند تا زمانی که وصل هستید اینترنت ندارند.
- قوانین توسط یک سرویس جداگانه Windows (ColituKillSwitch، LocalSystem، شروع خودکار) به صورت قوانین دائمی Windows Filtering Platform نگه داشته می‌شوند. اگر برنامه یا هسته VPN از کار بیفتد، یا سرویس دوباره راه‌اندازی شود، قوانین سر جایشان می‌مانند و اینترنت تا زمانی که Colitu دوباره وصل شود مسدود می‌ماند (fail-closed).
- راه‌اندازی مجدد یا خاموش شدن عادی Windows مسدودسازی را پایان می‌دهد. این عمدی است: کسی آنجا نخواهد بود تا توضیح دهد چرا اینترنت مسدود است. استثنا زمانی است که هم اتصال خودکار و هم شروع با Windows روشن باشند؛ در این صورت مسدودسازی تا زمانی که Colitu دوباره وصل شود می‌ماند. زدن «قطع اتصال» مسدودسازی را پایان می‌دهد و حذف برنامه همه قوانین را برمی‌دارد.
- اگر سرویس وجود نداشته باشد (مثلاً پس از یک نصب آسیب‌دیده)، برنامه به شما هشدار می‌دهد و به قطع‌کن اضطراری قدیمی‌تر درون برنامه برمی‌گردد. فیلترهای آن به فرایند برنامه تعلق دارند: اگر برنامه از کار بیفتد یا متوقف شود، Windows آن‌ها را برمی‌دارد و ترافیک جریان می‌یابد (fail-open).
- ترافیکی که برنامه مستقیم مسیریابی می‌کند، مانند سایت‌های منطقه‌ای فهرست داخلی، طبق طراحی مسدود نمی‌شود.

ترافیکی که برنامه‌ها خارج از تونل می‌فرستند

- بررسی به روزرسانی و دانلود به روزرسانی (colitu.com).
- اندازه‌گیری تأخیر تا سرورها.
- در Windows، حل نام میزبان سرورها از طریق DNS-over-HTTPS مربوط به Google یا Cloudflare.

بررسی‌های اتصال (مثلاً نشانی generate_204 از Google) از طریق تونل فرستاده می‌شوند.

10 ثبت وقایع و فهرست داده‌ها

این فهرست کامل آن چیزی است که Colitu ذخیره می‌کند. سیاست حریم خصوصی همین فهرست را به شکل حقوقی دربر دارد.

سرویس VPN

نگهداری و هدف	ذخیره می‌شود؟	داده
—	● هرگز	محتوای ترافیک شما
ثبت نمی‌شود.	● ذخیره نمی‌شود	سایت‌ها و نشانی‌های IP که بازدید می‌کنید

نگهداری و هدف	ذخیره می‌شود؟	داده
حل‌کننده‌های Colitu Shield ثبت پرس‌وجو و آمار را خاموش دارند. برنامه‌ها به صورت پیش‌فرض از حل‌کننده‌های عمومی (Cloudflare، Google) استفاده می‌کنند که پرس‌وجوها را از نشانی IP سرور VPN دریافت می‌کنند، نه از نشانی شما.	● ذخیره نمی‌شود	پرس‌وجوهای DNS شما
فقط در حافظه و فقط برای خود اتصال استفاده می‌شود.	● ذخیره نمی‌شود	نشانی IP شما روی سرورهای VPN
بایت‌ها به ازای هر کاربر در هر سرور در بازه‌های حدود 15 ثانیه‌ای، برای سهمیه‌ها و استفاده منصفانه 90 روز نگه داشته می‌شود؛ پس از آن فقط جمع هر دوره صورت‌حساب. این نشان می‌دهد حساب چه زمانی فعال بوده و چقدر مصرف کرده، اما نه اینکه ترافیک به کجا رفته است.	● ذخیره می‌شود	حجم ترافیک به ازای هر کاربر

حساب و وب‌سایت

کلیدهای عبور، نشست‌های وب و پیوندهای اشتراک در جدول زیر آمده‌اند. برای پیوندهای اشتراک هیچ نشانی IP ذخیره نمی‌شود: فقط یک شمارش ناشناس روزانه شبکه‌های متمایز برای هر پیوند، به مدت 48 ساعت نگه داشته می‌شود.

هدف	مدت نگهداری	داده
حساب و ورود	تا زمان حذف حساب؛ در هنگام حذف، نشانی با یک مقدار جایگزین می‌شود و رمز عبور غیرقابل استفاده می‌گردد	نشانی ایمیل، هش رمز عبور (Argon2id)، زبان، تاریخ‌های حساب
تأیید نشانی ایمیل، بازنشانی رمز عبور	7 روز	کدهای تأیید ایمیل و بازنشانی رمز عبور (نشانی، هش کد، نشانی IP)
امنیت حساب، جلوگیری از سوءاستفاده	180 روز	رویدادهای ورود (نشانی IP، کشور، مرورگر یا برنامه)
امنیت حساب، قواعد منطقه‌ای	ثبت‌نام: 180 روز. آخرین ورود: اگر 180 روز ورودی انجام نشود پاک می‌شود	نشانی IP و کشور هنگام ثبت‌نام و در آخرین ورود
اجرای قواعد منطقه‌ای	90 روز	ثبت‌نام‌ها و ورودهای رد شده بر اساس قواعد منطقه‌ای (نشانی IP، کشور)

هدف	مدت نگهداری	داده
ورود، فهرست نشست‌ها در صفحه حساب	30 روز پس از پایان نشست (خروج، انقضا یا ابطال) حذف می‌شود	نشست‌های وب (نشانی IP، کشور، مرورگر، روش ورود)
حفظ ورود در برنامه‌ها	30 روز پس از انقضا یا ابطال حذف می‌شوند	توکن‌های ورود برنامه (فقط به صورت هش ذخیره می‌شوند و به یک دستگاه متصل‌اند)
امنیت حساب	کلید و کدهای بازیابی تا زمانی که آن را خاموش کنید یا حساب حذف شود؛ مراحل ورود 1 روز پس از انقضا حذف می‌شوند	تأیید دومرحله‌ای (کلید رمزگذاری شده برنامه احراز هویت، هش کدهای بازیابی یک‌بارمصرف، مراحل ورود 5 دقیقه‌ای)
ورود بدون رمز عبور و امنیت حساب	تا زمانی که کلید عبور را حذف کنید یا حساب حذف شود؛ درخواست‌های تأیید پس از 5 دقیقه منقضی و حذف می‌شوند	کلیدهای عبور (passkey) (کلید عمومی، شناسه اعتبارنامه، نامی که می‌دهید، شمارنده امضا، تاریخ ایجاد و آخرین استفاده؛ کلید خصوصی و هرگونه داده زیستی هرگز از دستگاه شما خارج نمی‌شود؛ درخواست‌های تأیید یک‌بارمصرف 5 دقیقه‌ای)
دسترسی به VPN	تا زمانی که دستگاه یا پیوند در حال استفاده است؛ 30 روز پس از حذف یا جایگزینی حذف می‌شود	اطلاعات اتصال VPN (کلیدهای تصادفی به‌ازای هر سرور، متصل به یک دستگاه یا یک پیوند اشتراک)
یک پیوند به‌ازای هر دستگاه و هشدار پیوند اشتراکی	تا زمانی که پیوند را باطل کنید یا حساب را حذف کنید (پیوند منقضی شده خودکار باطل می‌شود)؛ شمارش شبکه‌ها پس از 48 ساعت خودبه‌خود حذف می‌شود	پیوندهای اشتراک (نامی که می‌دهید، تاریخ ایجاد، آخرین استفاده و انقضا، نشانه «احتمالاً به اشتراک گذاشته شده»؛ خود پیوند فقط به صورت هش ذخیره می‌شود). نشانی‌های IP که از پیوند استفاده می‌کنند ذخیره نمی‌شوند؛ فقط یک شمارش روزانه، ناشناس و تقریبی از اینکه هر پیوند از چند شبکه مختلف استفاده شده به مدت 48 ساعت نگه داشته می‌شود
QR ورود با کد	1 روز پس از انقضای کد 10 دقیقه‌ای حذف می‌شود	درخواست‌های ورود تلویزیون (نام دستگاه، نشانی IP، کشور)

هدف	مدت نگهداری	داده
سقف دستگاه‌ها، امنیت حساب	تا زمانی که دستگاه در حساب است نگه داشته می‌شود. نام، نشانی IP، کشور و هش سخت‌افزار دستگاه حذف شده پس از 30 روز پاک می‌شود؛ نشانی IP و کشور دستگاهی که 180 روز دیده نشده پاک می‌شود	دستگاه‌ها (نام، پلتفرم، نسخه برنامه و سیستم عامل، آخرین نشانی IP و کشور، هش کلیددار شناسه سخت‌افزار)
سقف دستگاه‌ها، جلوگیری از سوءاستفاده	180 روز	تلاش‌های رد شده افزودن دستگاه و دوره آزمایشی (نشانی IP، جزئیات دستگاه)
جلوگیری از ایجاد مکرر حساب رایگان	شبکه: 30 روز. ایمیل و شناسه سخت‌افزار: تا زمانی که حساب وجود دارد و تا 180 روز پس از حذف آن. هش‌های SHA-256 بدون کلید که پیش از این تغییر نوشته شده‌اند، حداکثر 180 روز پس از نوشته شدن حذف می‌شوند	بررسی‌های سوءاستفاده از طرح رایگان و دوره آزمایشی (هش‌های کلیددار HMAC-SHA256 از نشانی ایمیل، شناسه سخت‌افزار و شبکه؛ کلید در پایگاه داده ذخیره نمی‌شود)
هر نفر فقط یک کد آزمایشی	شبکه: 35 روز. ایمیل و شناسه سخت‌افزار: 365 روز، حتی پس از حذف حساب	بررسی‌های سوءاستفاده از کد تبلیغاتی دوره آزمایشی (هش‌های کلیددار HMAC-SHA256 از نشانی ایمیل نرمال سازی شده، شناسه سخت‌افزار دستگاه و شبکه – IPv4 با 32/ و 24/ یا IPv6 با 64/ و 48؛ کلید در پایگاه داده ذخیره نمی‌شود)
انتقال اشتراک‌های قدیمی؛ جلوگیری از انتقال دوباره یک اشتراک	30 روز پس از آخرین تغییر حذف می‌شود. از درخواست تأیید شده فقط هش کلیددار شناسه Telegram به مدت 2 سال می‌ماند	درخواست‌های انتقال از سرویس قبلی (شناسه و نام Telegram، یادداشت‌ها، نشانی IP)

هدف	مدت نگهداری	داده
اندازه‌گیری تجمیعی اینکه کدام کانال‌ها کاربران واقعی می‌آورند و اولین اتصال چقدر طول می‌کشد	همراه حساب حذف می‌شود	برچسب منبع ثبت نام (مثلاً «app:android»، «github») از برچسب utm/ref در پیوند ورودی سایت، نام سایتی که شما را به اینجا فرستاده (مثلاً github.com) یا برنامه؛ هیچ کوکی، پیکسل ردیابی یا نشانی اینترنتی ذخیره نمی‌شود. زمان اولین اتصال VPN.
اعطای پاداش دعوت؛ جلوگیری از سوءاستفاده (نشانی IP یا دستگاه یکسان، ایمیل یک‌بار مصرف)؛ اندازه‌گیری تجمیعی ثبت‌نام‌های ناشی از دعوت	با حذف هر یک از دو حساب حذف می‌شود	کد دعوت شما؛ پیوند میان حسابی که با پیوند دعوت باز شده و حساب دعوت‌کننده، وضعیت دعوت (در انتظار، کسب‌شده، نامعتبر و دلیل آن) و تعداد روزهای Premium اعطاشده. نام یا ایمیل دعوت‌شده هرگز به دعوت‌کننده نشان داده نمی‌شود.
اندازه‌گیری و بهبود کیفیت اتصال، Adaptive Connect و استفاده از قابلیت‌ها	جمع‌های کل بدون محدودیت زمانی نگه داشته می‌شوند (غیرقابل ارتباط با یک فرد)	آمار استفاده ناشناس برنامه‌ها: نتیجه اتصال‌ها و نوع خطا، زمان اتصال و بازیابی (به صورت شمارش در بازه‌ها)، قطع‌های غیرمنتظره، تغییر پروتکل‌های Adaptive Connect، تأخیر اندازه‌گیری‌شده تا سرورها و انتخاب سرور در حالت خودکار، قابلیت‌های استفاده‌شده و وضعیت قطع‌کن اضطراری (Kill Switch)؛ نوع شبکه و کشور و شماره ارائه‌دهنده اینترنت (ASN) شبکه در حال استفاده (از یک برچسب امضاشده که هنگام خاموش بودن VPN دریافت می‌شود). سرور فقط جمع کل روزانه را نگه می‌دارد و شبکه‌ها (کشور + ASN) و سرورها در جدول‌های جداگانه‌اند؛ هیچ حساب، دستگاه، نشانی IP یا وبسایت بازدیدشده‌ای ذخیره نمی‌شود. در تنظیمات برنامه قابل خاموش کردن است.
اندازه‌گیری تجمیعی رضایت (NPS)، تناسب محصول با بازار و دلایل ترک	با حذف حساب، پیوند با آن و نظر حذف می‌شود؛ فقط امتیاز ناشناس باقی می‌ماند	پاسخ‌های شما به نظرسنجی‌های درون برنامه: امتیاز توصیه (0-10)، اینکه بدون Colitu چه احساسی خواهید داشت، دلیل تمدید نکردن Premium، یک نظر اختیاری و پلتفرم؛ نظرسنجی‌هایی که بسته‌اید (حداکثر یک نظرسنجی در 30 روز)
اندازه‌گیری تجمیعی کیفیت پشتیبانی (رضایت، زمان پاسخ و حل)	همراه گفتگوی پشتیبانی حذف می‌شود	امتیاز 1-5 و نظر اختیاری که به یک گفتگوی پشتیبانی حل‌شده می‌دهید؛ زمان اولین پاسخ و زمان حل آن

هدف	مدت نگهداری	داده
امتحان کردن ابتدایی پروتکل‌های انتقال کارآمد	با هر گزارش بازنویسی می‌شود	اینکه برای یک دستگاه کدام پروتکل‌های انتقال روی کدام سرور و با چه سرعتی کار کرده‌اند (بدون نشانی IP)
صورتحساب، بازپرداخت، تعهدات قانونی	تا مدتی که قانون حسابداری و مالیات الزام می‌کند، حتی پس از حذف حساب؛ حذف خودکار در پایان آن مدت هنوز پیاده‌سازی نشده است	طرح، پرداخت‌ها و سفارش‌ها (مبلغ، نوع روش پرداخت، شناسه تراکنش ارائه‌دهنده، اعلان ارائه‌دهنده)
پشتیبانی، رسیدگی به	گفتگوهای بسته‌شده: 2	گفتگوهای پشتیبانی و پیوست‌ها، از جمله گزارش‌های برنامه
یک کار خودکار هر ساعت این مدت‌ها را اعمال می‌کند و حذف حساب بلافاصله هر آنچه سیاست حریم خصوصی فهرست کرده را پاک می‌کند. شکاف‌های باقی‌مانده: سوابق طرح، پرداخت و سفارش و گزارش ممیزی هنوز حذف خودکار ندارند، و پشتیبان‌های رمزگذاری‌شده‌ای که پیش از یک حذف تهیه شده‌اند تا زمانی که خودشان حذف شوند داده‌ها را نگه می‌دارند (حذف خودکار پشتیبان‌ها پس از 35 روز در حال معرفی است). هش‌های بررسی سوءاستفاده با یک راز سرور کلیددار می‌شوند؛ هش‌های SHA-256 بدون کلید که پیش از این تغییر نوشته شده‌اند تا زمانی که حذف شوند قابل تطبیق می‌مانند، حداکثر 180 روز پس از نوشته شدنشان.		
ایمیل‌های اعلان، یادداشت انتشار و پیشنهاد (با رضایت شما)	تا زمانی که لغو اشتراک کنید؛ ثبت‌نام‌های تأییدنشده پس از 7 روز حذف می‌شوند	اشتراک خبرنامه (نشانی ایمیل، زبان، زمان تأیید)؛ فقط اگر از طریق پیوند داخل ایمیل تأیید کنید
اداره و حفاظت از سرویس	14 روز	گزارش‌های دسترسی وب‌سایت و API (نشانی IP، نشانی درخواستی، مرورگر)
نمایش نتیجه آزمون	فقط در حافظه، 10 دقیقه	آزمون نشت DNS در وب‌سایت ما
پاسخگویی در قبال اقدامات	بدون محدودیت زمانی؛ دلیل اختیاری که هنگام حذف حساب می‌نویسید: 180 روز	گزارش ممیزی (اقدامات مدیران و برخی اقدامات حساب مانند حذف حساب، بر اساس شناسه حساب)

11 تله‌متری و اشخاص ثالث

تله‌متری در برنامه‌ها

- هیچ‌یک از برنامه‌های Colitu (Android، iOS، Windows، Linux) کتابخانه تحلیل، تبلیغات یا گزارش خرابی ندارد؛ برنامه iOS از نسخه 5.4.1 چنین کتابخانه‌ای ندارد.
- همه برنامه‌ها به Colitu گزارش می‌دهند کدام روش‌های انتقال روی کدام سرور کار کرده و با چه سرعتی، به‌صورت وابسته به دستگاه، تا روش‌های انتقال کارآمد ابتدا انتخاب شوند.
- درخواست‌های پشتیبانی گزارش‌های اخیر برنامه را پیوست می‌کنند، با نشانی‌ها و رازهای پنهان‌شده.

اشخاص ثالثی که داده دریافت می‌کنند

طرف	آنچه دریافت می‌کند
ارائه‌دهنده پرداخت (فقط برای مشتریانی که طرح پولی خریده‌اند)	شماره سفارش، مبلغ، ارز، توضیح طرح و روش پرداخت؛ اطلاعات کارت یا بانک در صفحه ارائه‌دهنده وارد می‌شود. Colitu ایمیل یا نشانی IP شما را نمی‌فرستد.
Resend (ایمیل)	نشانی ایمیل شما و محتوای ایمیل‌های حساب (کدها، رسیدها).
Brevo (رله ایمیل)	پاسخ‌هایی که از صندوق پشتیبانی ما فرستاده می‌شوند.
DeepSeek (Colitu Bot)	پرسش و چند پیام آخر یک گفتگوی ربات. جزئیات حساب فرستاده نمی‌شود، اما هر چیزی که تایپ کنید منتقل می‌شود.
Have I Been Pwned (Pwned Passwords)	هنگام ثبت‌نام یا تعیین رمز عبور جدید: 5 نویسه اول هش SHA-1 رمز عبور، برای مقایسه با نشتهای شناخته‌شده. هرگز رمز عبور، هش کامل آن، ایمیل یا نشانی IP شما.
Cloudflare	رکوردهای DNS را میزبانی می‌کند و docs.colitu.com و map.colitu.com را پروکسی می‌کند. همچنین حل‌کننده‌های DNS پیش‌فرض در برنامه‌ها و خروجی چند دامنه روی دو سرور را فراهم می‌کند (17§).
ارائه‌دهندگان میزبانی	سرورها را اجرا می‌کنند و از نظر فنی به آن‌ها دسترسی دارند.

وبسایت هیچ اسکرپیت، فونت یا ردیاب شخص ثالثی بارگذاری نمی‌کند.

12 امنیت برنامه

Linux (بتا)	iOS	Windows	Android	
با AES-GCM کلیدی مشتق شده از ماشین و کاربر	Keychain (پس از اولین بازگشایی قفل در دسترس است)	DPAPI (کاربر فعلی)	AES-256-GCM با کلید Android Keystore (کلید نرم افزاری اگر Keystore شکست بخورد)	توکن های نشست
فایل های محافظت شده (0600)	فایل متن ساده در محفظه خصوصی برنامه	متن ساده در یک پایگاه داده که فقط مدیران و SYSTEM می توانند بخوانند	رمزگذاری شده (AES-GCM)	اعتبارنامه های اتصال
● بله (از 10 اکتبر 2026)	● بله (از 10 اکتبر 2026)	● بله (از 10 اکتبر 2026)	● بله	سنجاق کردن گواهی برای API
sudo می خواهد؛ رمز عبور در حافظه نگه داشته می شود	افزونه شبکه	همیشه با دسترسی مدیر اجرا می شود؛ یک سرویس پس زمینه جداگانه (ColituKillSwitch، LocalSystem) قوانین قطع کن اضطراری را نگه می دارد	برنامه عادی با مجوز VPN	سطح دسترسی
فقط هشدارها	فقط هشدارها؛ بدون گزارش دسترسی	فقط هشدارها؛ نشانی ها پنهان؛ پس از 7 روز حذف می شود	فقط هشدارها؛ بدون گزارش دسترسی	گزارش های محلی VPN
—	موارد Keychain روی دستگاه می مانند	—	غیرفعال	پشتیبان گیری از داده های برنامه

سنجاق کردن (pinning) یعنی گواهی ریشه ای که شخص دیگری روی دستگاه نصب کرده برای خواندن ترافیک API برنامه ها قابل استفاده نیست. بنابراین نرم افزارهای امنیتی که با درج گواهی ریشه خودشان HTTPS را بازرسی می کنند اتصال API برنامه ها را مسدود می کنند؛ در چنین نرم افزارهایی Colitu را مستثنا کنید.

13 به روزرسانی ها و زنجیره تأمین

پلتفرم	نحوه راستی‌آزمایی به‌روزرسانی
Android (نسخه داندودی)	مانیفست با ECDSA P-256 امضا شده و در برابر کلیدی که در برنامه تعبیه شده بررسی می‌شود. APK باید از طریق HTTPS از colitu.com بیاید، با SHA-256 مانیفست مطابقت داشته باشد و با همان گواهی برنامه نصب‌شده امضا شده باشد. نسخه‌های قدیمی‌تر رد می‌شوند.
Android (Google Play)	از طریق Google Play به‌روزرسانی می‌شود.
Windows	همان مانیفست امضا شده، داندود HTTPS از colitu.com، بررسی SHA-256، که دوباره توسط مرحله نصب‌کننده با دسترسی بالا بررسی می‌شود. نصب‌کننده هنوز با Authenticode امضا نشده است، بنابراین Windows SmartScreen ممکن است هشدار دهد.
Linux	مانیفست امضا شده و SHA-256 بسته.
iOS	از طریق Apple TestFlight توزیع می‌شود؛ Apple به‌روزرسانی‌ها را امضا و تحویل می‌دهد.

ساخت و کد منبع

- هر انتشار برنامه‌های متن‌باز روی GitHub برچسب‌گذاری می‌شود. صفحه انتشار مجموع‌های کنترلی SHA-256 و یک صورت‌حساب مواد نرم‌افزار (SBOM) به قالب SPDX را فهرست می‌کند (Android و Windows).
- اسکن کد CodeQL و به‌روزرسانی وابستگی‌ها با Dependabot روی مخازن Android و Windows اجرا می‌شوند؛ GitHub Actions به هش کامیت‌ها سنجاق شده‌اند.
- انتشار Android در CI ساخته می‌شود؛ نصب‌کننده Windows روی دستگاه توسعه‌دهنده ساخته می‌شود؛ بسته‌های Linux در CI ساخته می‌شوند؛ ساخت‌های iOS TestFlight روی Codemagic انجام می‌شوند.
- ساخت‌ها هنوز بازتولیدپذیر نیستند، بنابراین یک مجموع کنترلی ثابت می‌کند فایلی که منتشر کرده‌ایم را دارید، نه اینکه از کد منبع برچسب‌خورده ساخته شده است. نسخه کد منبع خود کتابخانه هسته VPN در Android هنوز سنجاق نشده است.

چه چیزی باز است و چه چیزی بسته

کد منبع	جزء
● باز (GPL-3.0)	برنامه Android
● باز (GPL-3.0)	برنامه Windows

جزء	کد منبع
برنامه Linux	● باز (GPL-3.0)
برنامه iOS	● باز (GPL-3.0)
صفحه کنترل و عامل گره	● بسته
وبسایت	● بسته

14 مقاومت در برابر سانسور

نمی‌توان تضمین کرد که هیچ روش انتقالی در برابر هر سامانه سانسوری به کار خود ادامه دهد. رویکرد Colitu این است که چند روش انتقال با ویژگی‌های متفاوت ارائه دهد و بگذارد برنامه به‌طور خودکار به روش دیگر برگردد.

شیوه مسدودسازی	پاسخ Colitu
مسدود کردن نشانی‌های IP سرور	چند سرور در شبکه‌های مختلف، به‌علاوه یک رله (17S). IP مسدودشده تا زمانی که سرور تغییر کند مسدود می‌ماند.
مسدود کردن درگاه‌ها یا UDP	روش‌های انتقال (Reality، XHTTP، Trojan) وقتی UDP مسدود است؛ Hysteria2 وقتی TCP مختل شده است.
مسموم‌سازی DNS	برنامه‌ها نشانی سرورها را از API دریافت می‌کنند و در صورت نیاز آن‌ها را با DNS رمزگذاری‌شده حل می‌کنند.
اثر انگشت TLS و کاوش فعال	Reality به کاوش‌ها همچون وبسایت واقعی‌ای که از آن تقلید می‌کند پاسخ می‌دهد.
اثر انگشت پروتکل (DPI)	Reality و XHTTP شبیه HTTPS معمولی‌اند؛ Hysteria2 شبیه QUIC است.
کند کردن و ریست اتصال‌ها	بازگشت خودکار به روش انتقال دیگر؛ XHTTP برای شبکه‌هایی که اتصال‌های طولانی را قطع می‌کنند.

15 محدودیت‌های حریم خصوصی

VPN ترافیک شما را از شبکه‌ای که روی آن هستید پنهان می‌کند. نمی‌تواند همه‌چیز را پنهان کند:

- اندازه بسته‌ها، زمان‌بندی و حجم کل همچنان قابل مشاهده‌اند و ناظری که هر دو سر را می‌بیند می‌تواند آن‌ها را تطبیق دهد.

- وبسایت‌ها همچنان می‌توانند شما را از طریق کوکی‌ها، اثر انگشت مرورگر و حساب‌هایی که در آن‌ها وارد شده‌اید شناسایی کنند.
- VPN در برابر بدافزار، فیشینگ یا مرورگر نفوذشده محافظت نمی‌کند.
- ترافیکی که خارج از تونل مسیریابی می‌شود (9§) محافظت‌شده نیست.

16 واکنش به رخداد و گزارش رخدادها

اگر به نفوذ به یک سرور VPN مشکوک شویم، آن را از برنامه‌ها پنهان می‌کنیم، کلیدها و اعتبارنامه‌های اتصال آن را تعویض می‌کنیم و آن را از نو می‌سازیم. اگر نقض امنیتی بر داده‌های شخصی اثر بگذارد، بدون تأخیر ناروا به کاربران آسیب‌دیده ایمیل می‌فرستیم و آنچه رخ داده را در همین بخش و در مرکز اعتماد منتشر می‌کنیم. وضعیت سرویس در status.colitu.com عمومی است.

17 زیرساخت

- همه سرورها ماشین‌های مجازی اجاره‌ای از چند ارائه‌دهنده میزبانی مستقل هستند. سرورهای VPN در چند کشور پخش شده‌اند؛ فهرست زنده در صفحه سرورها است. صفحه کنترل، که پایگاه داده حساب‌ها را نگه می‌دارد، روی یک سرور در ترکیه اجرا می‌شود.
- دیسک‌ها رمزگذاری نشده‌اند. ارائه‌دهندگان میزبانی از نظر فنی به ماشین‌های خود دسترسی دارند.
- دسترسی مدیریتی فقط با SSH و کلید است؛ ورود با رمز عبور غیرفعال است. فقط تیم Colitu کلیدها را در اختیار دارد.
- به‌روزرسانی‌های امنیتی خودکار روی بیشتر سرورها فعال است؛ فعال کردن آن‌ها در همه‌جا در نقشه راه است.
- صفحه کنترل و برخی سرورهای VPN از دیوار آتش با پیش‌فرض مسدودسازی استفاده می‌کنند. روی سرورهای VPN دیگر فقط سرویس‌های SSH، VPN و نقطه پایانی اندازه‌گیری گوش می‌دهند؛ دیوار آتش با پیش‌فرض مسدودسازی در همه‌جا در نقشه راه است.
- پایگاه داده صفحه کنترل از اینترنت قابل دسترسی نیست. سرورهای VPN به آن دسترسی ندارند.
- دو سرور مجموعه‌ای کوچک و ثابت از دامنه‌ها (روی یکی سرویس‌های Google و روی دیگری سرویس‌های هوش مصنوعی Google) را از طریق Cloudflare WARP می‌فرستند تا این سرویس‌ها یک موقعیت اروپایی ببینند. برای آن دامنه‌ها Cloudflare خروجی است و همان فراداده‌ای را می‌بیند که یک سرور VPN می‌دید.
- یک سرور ورودی رله بسته‌های رمزگذاری‌شده را بدون تغییر به یک سرور خروجی در لتونی می‌فرستد. سرور ورودی نمی‌تواند ترافیک را رمزگشایی کند؛ نشانی IP شما را همان‌طور که هر شبکه‌ای می‌بیند، می‌بیند.

18 افشای مسئولانه آسیب‌پذیری

مسائل امنیتی را به‌صورت خصوصی به security@colitu.com گزارش دهید (در well-known/security.txt هم آمده است). لطفاً مراحل بازتولید و نسخه آسیب‌دیده را بنویسید. سیاست کامل در colitu.com/responsible-disclosure است.

- دریافت گزارش‌ها را ظرف 3 روز کاری تأیید می‌کنیم و ظرف 10 روز کاری ارزیابی اولیه می‌دهیم.
- لطفاً پیش از انتشار جزئیات، زمان معقولی برای رفع مشکل به ما بدهید.

- علیه پژوهشی که با حسن نیت انجام شده، از داده‌های کاربران دیگر دوری می‌کند، سرویس را مختل نمی‌کند و به‌صورت خصوصی گزارش می‌شود اقدام قانونی نخواهیم کرد.
- از پژوهشگرانی که بخواهند از آن‌ها نام ببریم قدردانی می‌کنیم. در حال حاضر پاداش مالی نمی‌دهیم.
- در محدوده: برنامه‌ها، colitu.com و زیردامنه‌های آن، API و سرورهای VPN. خارج از محدوده: ازکارانداختن سرویس (DoS)، هرزنامه، مهندسی اجتماعی و اشخاص ثالث ذکرشده در §11.

19 وضعیت ممیزی

Colitu هنوز ممیزی امنیتی یا آزمون نفوذ مستقل از شخص ثالث نداشته است. اطمینان فعلی شامل این موارد است:

- کد منبع عمومی برنامه‌های Android و Windows و Linux و iOS؛
- اسکن خودکار کد (CodeQL) و به‌روزرسانی وابستگی‌ها (Dependabot)؛
- بازبینی‌های امنیتی داخلی برنامه‌ها (اکتبر 2026) و راستی‌آزمایی پشت این سند؛
- فرایند عمومی افشای مسئولانه آسیب‌پذیری.

ممیزی مستقل برنامه‌ریزی شده اما هنوز زمان‌بندی نشده است.

20 محدودیت‌های شناخته‌شده

- هنوز ممیزی امنیتی مستقل وجود ندارد.
- سرورهای VPN و ارائه‌دهندگان میزبانی آن‌ها بخشی از چیزی هستند که باید به آن اعتماد کنید؛ دیسک‌های سرور رمزگذاری نشده‌اند.
- وقتی حالت حریم خصوصی خاموش شود، برخی سایت‌های منطقه‌ای در یک فهرست داخلی در برنامه‌های Windows و Android و iOS و Linux خارج از VPN می‌روند. از Windows و Android نسخه 2.7.0، iOS نسخه 5.6.0 و Linux نسخه 1.3.0 حالت حریم خصوصی برای نصب‌های جدید به‌صورت پیش‌فرض روشن است، اما نصب‌های قبلی تنظیم قبلی خود را حفظ می‌کنند.
- نصب‌های جدید Windows در حالت TUN شروع می‌شوند، اما نصب‌هایی که از حالت پروکسی سیستمی استفاده می‌کردند آن را نگه می‌دارند، و حالت پروکسی همه برنامه‌ها، حل‌کننده DNS سیستم یا IPv6 را پوشش نمی‌دهد. راه‌اندازی مجدد عادی Windows مسدودسازی قطع‌کن اضطراری را پایان می‌دهد، مگر اینکه Colitu برای اتصال مجدد هنگام ورود تنظیم شده باشد.
- Android قطع‌کن اضطراری مخصوص خودش را ندارد و به دو تنظیم سیستمی نیاز دارد که به‌صورت پیش‌فرض خاموش‌اند؛ گزینه «مسدود کردن اینترنت بدون VPN» در iOS به‌صورت پیش‌فرض خاموش است و تا وقتی روشن است مانع باز شدن صفحات ورود Wi-Fi می‌شود.
- تأیید دومرحله‌ای برای حساب‌های مدیر اجباری است اما برای کاربران فقط اختیاری.
- سوابق صورتحساب و گزارش ممیزی هنوز حذف خودکار ندارند (§10)، و پشتیبان‌ها روی همان سرور نگه داشته می‌شوند، فعلاً همراه با کلید رمزگشایی‌شان.
- نرم‌افزارهای امنیتی که HTTPS را با گواهی ریشه خودشان بازرسی می‌کنند به‌دلیل سنجاق کردن گواهی اتصال API برنامه‌ها را مسدود می‌کنند؛ باید Colitu در آن‌ها مستثنا شود. کلیدهای عبور فقط روی colitu.com کار می‌کنند؛ نه روی دامنه‌های آینه و نه درون برنامه‌ها.

- برنامه Windows با Authenticode امضا نشده است و هنوز هیچ ساختی بازتولیدپذیر نیست.
- Shadowsocks 2022 محرمانگی رو به جلو ندارد؛ Trojan نسخه 1.2 TLS را می‌پذیرد.

21 تغییرات در نسخه‌های 1.4 و 1.5 و 1.6

- نسخه 1.3 برنامه‌ها را همان‌طور که پیش از آخرین انتشارهای برنامه بودند توصیف می‌کرد. این نسخه آنچه را که امروز عرضه می‌شود توصیف می‌کند.
- تأیید دومرحله‌ای (TOTP) برای هر حساب کاربری در دسترس است، نه فقط برای مدیران. برنامه‌ها هنگام ورود کد را می‌پرسند.
- Windows: قطع‌کن اضطراری اکنون یک سرویس جداگانه Windows با قوانین دائمی دیوار آتش است. اگر برنامه یا هسته VPN از کار بیفتد مسدودسازی را ادامه می‌دهد (دیگر fail-open نیست). راه‌اندازی مجدد عادی Windows هنوز مسدودسازی را پایان می‌دهد، مگر اینکه Colitu برای اتصال مجدد هنگام ورود تنظیم شده باشد. نصب‌های جدید در حالت TUN شروع می‌شوند.
- تونل‌زنی تقسیم‌شده در هر چهار برنامه وجود دارد: برنامه‌ها، سایت‌ها و نشانی‌های IP در Windows و Android و Linux؛ سایت‌ها و نشانی‌های IP در iOS.
- iOS: IPv6 دیگر نشت نمی‌کند و یک گزینه اختیاری «مسدود کردن اینترنت بدون VPN» (به صورت پیش‌فرض خاموش) ترافیک خارج از تونل را مسدود می‌کند.
- حالت حریم خصوصی (برای نصب‌های جدید به صورت پیش‌فرض روشن) به کاربران برنامه‌های Windows و Android و iOS و Linux اجازه می‌دهد تصمیم بگیرند قاعده داخلی که برخی سایت‌های منطقه‌ای را خارج از VPN می‌فرستد فعال باشد یا نه.
- چندجهشی (VPN، Multihop، دوگانه) و IP چرخان با سرورهای VLESS در دسترس هستند.
- مسدودکننده تبلیغات از 7 اکتبر 2026 به Colitu Shield تبدیل شد، محافظت DNS اختیاری با پنج دسته (تبلیغات و ردیاب‌ها، بدافزار، فیشینگ، کلاهبرداری، استخراج رمزارز). حل‌کننده‌های آن گزارش پرس‌وجو و آمار نگه نمی‌دارند و هیچ داده جدیدی جمع‌آوری نمی‌شود. فیلتر اختیاری محتوای بزرگسالان، فهرست‌های شخصی، شمارنده روی دستگاه و کلیدهای هر دسته در نقشه راه هستند، نه فعال.
- نسخه‌ها، تاریخ‌ها و مجموع‌های کنترلی در این سند، صفحه‌های دانلود و صفحه متن‌باز اکنون از یک مانیفست انتشار می‌آیند.
- نسخه 1.5 (9 اکتبر 2026): طرح‌های پولی (شخصی، Plus و خانوادگی) در دسترس فروش هستند؛ پرداخت‌ها در صفحه یک ارائه‌دهنده پرداخت انجام می‌شود و اطلاعات کارت هرگز به Colitu نمی‌رسد. این عبارت که طرح‌های پولی ارائه نمی‌شوند حذف شده است. هیچ رویه دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخه 1.6 (10 اکتبر 2026): کلیدهای عبور برای وب‌سایت، فهرست نشست‌ها با کنترل نشست، ایمیل‌های امنیتی، قفل 24 ساعته برای حذف حساب و خاموش کردن تأیید دومرحله‌ای پس از بازنشانی رمز عبور، محدودیت تعداد تلاش‌های تأیید مجدد رمز عبور، پیوندهای اشتراک نام‌دار اضافی با انقضا، کلیدهای امنیتی سخت‌افزاری اختیاری برای حساب‌های مدیر، و سنجاق کردن اتصال API به مراجع صدور گواهی ریشه Let's Encrypt (ISRG) و Google Trust Services در هر چهار برنامه. هیچ رویه دیگر توصیف‌شده در این سند تغییر نکرده است.

22 نقشه راه امنیتی

بعدی (سه ماهه چهارم 2026)

- حذف خودکار سوابق صورتحساب پس از پایان دوره نگهداری قانونی.
- گزارش‌های دسترسی کوتاه‌تر وب‌سایت بدون نشانی‌های IP کامل.
- دیوار آتش با پیش‌فرض مسدودسازی و به‌روزرسانی‌های امنیتی خودکار روی هر سرور.
- پشتیبان‌های رمزگذاری شده خارج از محل با کلید رمزگشایی نگه‌داشته شده در حالت آفلاین.
- الزامی کردن TLS 1.3 برای Trojan.

بعدتر

- امضای Authenticode برای Windows.
- ساخت‌های بازتولیدپذیر و SBOM برای هر پلتفرم.
- آزمون نفوذ خارجی و ممیزی مستقل.
- یک کلید PGP برای گزارش‌های امنیتی و گزارش‌های شفافیت فصلی.

23 صلاحیت قضایی

Colitu را COLITU LIMITED اداره می‌کند، شرکتی ثبت شده در انگلستان و ولز (نشانی ثبتی: City Road, 128 London EC1V 2NX, United Kingdom)، و تابع قانون انگلستان و ولز است. پایگاه داده حساب‌ها روی یک سرور در ترکیه است؛ سرورهای VPN در کشورهای نشان داده شده در صفحه سرورها هستند و تابع قانون محلی همان‌جا هستند. ما فقط می‌توانیم داده‌ای را که داریم تحویل دهیم؛ **10S** همه آن را فهرست می‌کند. درخواست‌هایی که دریافت می‌کنیم در گزارش‌های شفافیت در مرکز اعتماد شمارش می‌شوند.

24 منابع

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

سند فنی امنیت Colitu · نسخه 1.6 · 10 اکتبر 2026 · colitu.com/security · security@colitu.com

