

نسخه 2.0 · 21 نوامبر 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 می‌بیند، Colitu در برابر کدام حمله‌ها محافظت می‌کند و در برابر کدام نه، و چگونه می‌توانید ادعاهای ما را بررسی کنید. هر عبارت این سند آنچه را که امروز عرضه می‌شود توصیف می‌کند. هر جا چیزی وجود ندارد یا ضعیف‌تر از حد لازم است، آن را می‌گوییم.

نسخه	آخرین به‌روزرسانی	تماس امنیتی
2.0	21 نوامبر 2026	security@colitu.com

محدودهٔ کاربرد

Linux 1.9.2 · Windows 3.2.3 · Android 3.2.2 (بتا) · iOS 5.10.0 (TestFlight) · صفحهٔ کنترل تا 16 اکتبر 2026، عامل گره تا 7 اکتبر 2026

کد منبع

برنامه‌های Android و Windows و Linux: github.com/colitu؛ برنامهٔ iOS: github.com/colitu/ios (همه تحت GPL-3.0). نرم‌افزار سرور: کد بسته. کد پروتکل ColituGecko بسته است؛ یکپارچه‌سازی آن در برنامه‌ها متن‌باز است.

امنیت Colitu در یک نگاه

خلاصه‌ای از بخش‌های زیر. سبز: روی همهٔ 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. کد پروتکل ColituGecko نیز بسته است؛ یکپارچه‌سازی آن در برنامه‌ها باز 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). در Android 3.2 و Windows 3.2 و Linux 1.8 و بالاتر همچنین ColituGecko، پروتکل اختصاصی Colitu، با دست‌دهی ترکیبی پساکوانتومی که Noise NK و ML-KEM-768 را با هم ترکیب می‌کند.
محتوای ترافیک و سابقهٔ 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 گزینهٔ اختیاری «مسدود کردن اینترنت بدون VPN» دارد (به‌صورت پیش‌فرض خاموش).
سایت‌های منطقه‌ای که خارج از VPN مسیریابی می‌شوند	● از Windows و Android نسخهٔ 2.7.0 و iOS نسخهٔ 5.6.0 و Linux نسخهٔ 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 §9 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.
کلیدهای عبور (passkey) و کنترل نشست	🟢کلید عبور برای وب‌سایت (تا 10 عدد برای هر حساب)؛ صفحهٔ امنیت نشست‌های مرورگر را فهرست می‌کند و پایان می‌دهد؛ تغییر رمز عبور همهٔ نشست‌های دیگر را پایان می‌دهد. برنامه‌ها مثل قبل با رمز عبور وارد می‌شوند.
اتصال API سنجاق‌شده در برنامه‌ها	🟢از نسخه‌های برنامه در 10 اکتبر 2026، هر چهار برنامه مراجع صدور گواهی ریشهٔ Let's Encrypt (ISRG) و Google Trust Services را برای سنجاق API (pinning) می‌کنند. محدودیت‌ها: §12.
تونل‌زنی تقسیم‌شده	🟢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 مدیریت‌شده مجاز می‌کند.
Colitu Shield (محافظت DNS)	🟢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.
تحلیل‌گر شخص ثالث	🟢در هیچ برنامه‌ای (Android، iOS، Windows، Linux) وجود ندارد. از برنامهٔ iOS در نسخهٔ 5.4.1 حذف شد.
به‌روزرسانی‌های امضاشده	🟢مانیفست به‌روزرسانی امضاشده (ECDSA P-256) به‌علاوهٔ SHA-256 در Android و Windows و Linux؛ امضای App Store در iOS.
امضای کد Windows (Authenticode)	🔴هنوز نه.
ساخت‌های بازتولیدپذیر	🟡Android از 2.9.3 و Windows از 2.9.8: کد منبع برچسب‌خورده فایلی بایت‌به‌بایت یکسان می‌سازد. iOS و Linux هنوز نه.
SBOM	🟡SPDX برای هر انتشار GitHub برنامه‌های Android و Windows؛ Linux هنوز نه.
ممیزی امنیتی مستقل	🔴هنوز انجام نشده است.
افشای مسئولانهٔ آسیب‌پذیری	🟢security@colitu.com، سیاست در §18 و security.txt.
میزبانی شخصی	🔴ارائه نمی‌شود. Colitu همهٔ سرورها را خودش اجرا می‌کند.

1 خلاصهٔ اجرایی

Colitu یک سرویس VPN با برنامه‌هایی برای Android و Windows و Linux و iOS است. این سرویس برای شبکه‌های نامطمئن یا ناپایدار ساخته شده است: هر سرور چند روش انتقال ارائه می‌دهد و برنامه روشی را برمی‌گزیند که روی شبکهٔ کاربر کار می‌کند.

هدف طراحی این است که حجم داده‌های حساس در هر نقطهٔ واحد کم بماند. حساب‌ها و پرداخت‌ها روی یک صفحهٔ 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، نحوهٔ مدیریت کلیدها و حساب‌ها، آنچه ثبت می‌شود، نحوهٔ 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 اجزای اولیهٔ رمزنگاری جدید ابداع نمی‌کند: پروتکل اختصاصی آن، ColituGecko، نیز از اجزای شناخته‌شده (چارچوب Noise، AEAD، ML-KEM-768، X25519) ساخته شده است.
- 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 شبکهٔ محلی و ارائه‌دهندهٔ اینترنت شما به اپراتور VPN منتقل می‌کند. این سند توضیح می‌دهد که این اعتماد چه چیزهایی را در بر می‌گیرد.

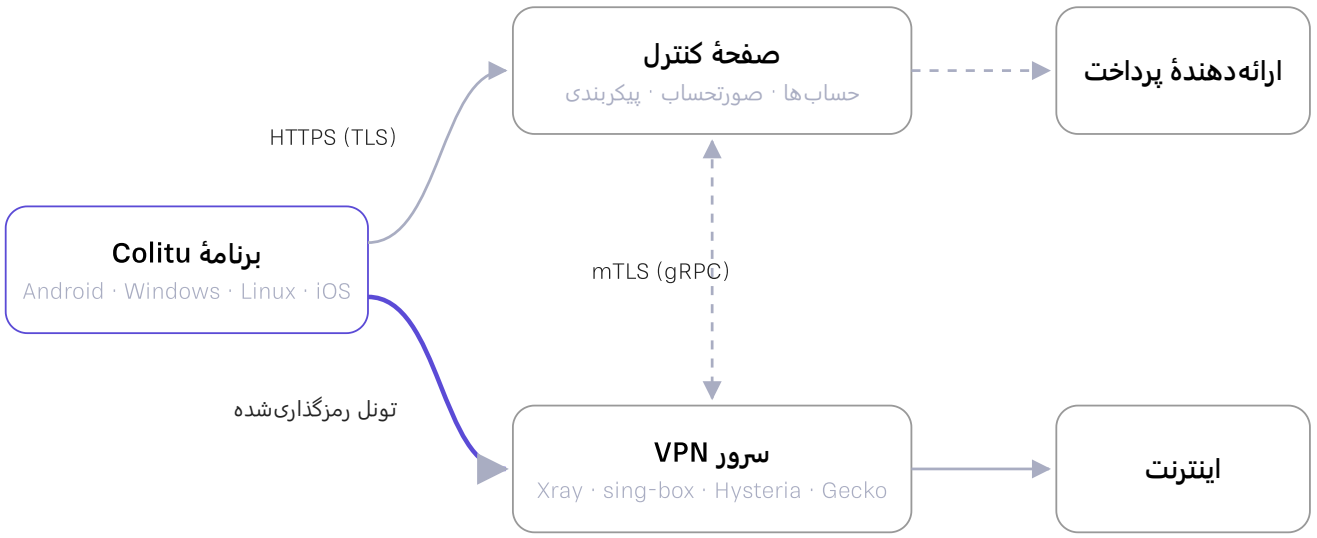
2 دامنه

شامل می‌شود: برنامه‌های Colitu برای Android و Windows و Linux و iOS؛ صفحهٔ 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 سیستم‌عامل و دستگاه کاربر، افزونه‌های مرورگر و سایر نرم‌افزارهای روی دستگاه، امنیت داخلی ارائه‌دهندهٔ پرداخت و سایر اشخاص ثالث نام‌برده در §11، و وب‌سایت‌هایی که کاربر بازدید می‌کند.

3 معماری

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



صفحهٔ کنترل و صفحهٔ داده. صفحهٔ 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).
صفحهٔ 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 احرازهویت‌شده 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 شناسهٔ داخلی کاربر. بدون نشانی ایمیل.
سرور VPN (صفحهٔ داده)	تونل رمزگذاری‌شده 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 DNS-over-HTTPS (AdGuard Home) روی سه سرور VPN که از داخل تونل در دسترس است و دامنه‌های تبلیغات، ردیاب‌ها، بدافزار، فیشینگ، کلاهبرداری و استخراج رمزارز را مسدود می‌کند: حدود 380 هزار قانون، فهرست‌ها هر 24 ساعت به‌روزرسانی می‌شوند. حل‌کننده‌های بالادستی Cloudflare و Quad9 از طریق DoH، همتای ECS غیرفعال است.	بدون گزارش پرس‌وجو، بدون آمار.

اتصال چگونه برقرار می‌شود

1. برنامه از طریق HTTPS وارد می‌شود و توکن‌های کوتاه‌مدت دریافت می‌کند.
2. فهرست سرورها و تنظیمات اتصال سرور انتخاب‌شده را از 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؛ و هنگام استفاده از ColituGecko، پیاده‌سازی اختصاصی و کد بستهٔ Gecko از Colitu.

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 (§9)، ترافیک شبکهٔ محلی، بررسی به‌روزرسانی و اندازه‌گیری تأخیر.

شما	شبکهٔ محلی / ارائه‌دهندهٔ 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.

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

تهدید	محافظت می‌شود؟	توضیح
حملهٔ مرد میانی روی API حساب	🟢بله	TLS با اعتبارسنجی گواهی سیستم؛ از نسخه‌های برنامه در 10 اکتبر 2026، هر چهار برنامه مراجع صدور گواهی ریشهٔ Let's Encrypt (ISRG) و Google Trust Services را نیز سنجاق می‌کنند، بنابراین گواهی ریشه‌ای که کسی روی دستگاه نصب کرده باشد برای خواندن ترافیک API قابل استفاده نیست.
سرور VPN مخرب یا نفوذشده	🔴خیر	سرور نشانی IP شما و مقصد ترافیکتان را می‌بیند، هرچند محتوای اتصال‌های HTTPS را نه.
صفحهٔ کنترل نفوذشده	🟡تا حدی	مهاجم به داده‌های حساب و صورتحساب دست می‌یابد و می‌تواند پیکربندی‌ها را به سرورها بفرستد. محتوای ترافیک هرگز آنجا نیست.
رمز عبور حساب به سرقت رفته	🟡تا حدی	محدودیت نرخ حدس زدن را کند می‌کند و می‌توانید دستگاه‌ها را از حساب خارج کنید. تأیید دومرحله‌ای اختیاری (برنامهٔ احرازهویت) یعنی رمز عبور سرقت‌شده به‌تنهایی دیگر وارد نمی‌شود، اما تا زمانی که روشنش نکنید خاموش است. کلیدهای عبور (passkey) روش ورود جایگزین در وب‌سایت هستند؛ تغییر رمز عبور همهٔ نشست‌های دیگر را پایان می‌دهد، و بازنشانی رمز عبور حذف حساب و خاموش کردن تأیید دومرحله‌ای را 24 ساعت قفل می‌کند.
بدافزار روی دستگاه شما	🔴خیر	خارج از دامنهٔ هر VPN.
اثر انگشت مرورگر، کوکی‌ها، حساب‌های واردشده	🔴خیر	VPN نشانی IP شما را تغییر می‌دهد، نه هویتتان را در وب‌سایت‌ها.
همبستگی ترافیک توسط ناظر سراسری	🔴خیر	زمان‌بندی و حجم را می‌توان بین تونل و اینترنت تطبیق داد.

مهاجمان بررسی‌شده

دسته	مثال	محافظت Colitu
A1 مهاجم شبکهٔ محلی	کسی که روی همان Wi-Fi کافه است	قوی برای ترافیک تونل‌شده.
A2 ارائه‌دهندهٔ اینترنت	ISP یا اپراتور همراه کاربر	قوی برای محتوا و مقصدها؛ زمان‌بندی و حجم همچنان قابل مشاهده می‌مانند.

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 نفوذشده یا ارائه‌دهندهٔ 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 صفحهٔ کنترل نفوذشده	مهاجمی با دسترسی به پنل	محدود: داده‌های حساب افشا می‌شود؛ محتوای ترافیک یا سابقهٔ مروری برای برداشتن وجود ندارد.
A6 مهاجم نقطهٔ انتهایی	بدافزار روی دستگاه کاربر	هیچ.
A7 مهاجم منفعل سراسری	ناظری که هر دو سر تونل را می‌بیند	هیچ.

6 پروتکل‌ها

هر سرور همین مجموعهٔ روش‌های انتقال را ارائه می‌دهد؛ ColituGecko فعلاً به‌عنوان حالت ششم روی بخشی از سرورها ارائه می‌شود. Colitu اجزای اولیهٔ رمزنگاری جدید ابداع نمی‌کند. در پنج حالت شناخته‌شده، رمزگذاری، احراز هویت و تبادل کلید را Xray-core و sing-box و Hysteria و کتابخانه‌هایی که به کار می‌برند فراهم می‌کنند. در ColituGecko لایهٔ نشست و رکورد و دست‌دهی را خود Colitu طراحی کرده، اما از اجزای شناخته‌شده ساخته شده‌اند: چارچوب Noise (الگوی NK)، توافق کلید ترکیبی X25519 + ML-KEM-768 و رمزگذاری AEAD رکوردها.

روش انتقال	نحوهٔ کار	احرازهویت سرور	نکات و محدودیت‌ها
Hysteria2	QUIC (UDP) با TLS 1.3	گواهی صادرشده 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 پایهٔ IP نیست.

روش انتقال	نحوهٔ کار	احرازهویت سرور	نکات و محدودیت‌ها
VLESS XHTTP	Reality به‌علاوهٔ یک جریان شبیه HTTP	Reality مانند، با کلیدهای خودش	برای شبکه‌هایی که اتصال‌های TCP طولانی‌مدت را قطع می‌کنند.
Trojan	TCP با TLS (نسخهٔ 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 گذاشته‌شده	سبک و سریع. بدون محرمانگی رو به جلو (forward secrecy): کلید فاش‌شده می‌تواند نشست‌های ضبط‌شده را رمزگشایی کند.
ColituGecko (Android 3.2+ و Windows 3.2+ و Linux 1.8+)	لایهٔ نشست و رکورد رمزگذاری‌شدهٔ اختصاصی Colitu که درون یک پوستهٔ بیرونی (skin) مانند TLS، QUIC یا WebSocket منتقل می‌شود. یک نشست می‌تواند از چند مسیر شبکه (grip) استفاده کند؛ سرور ورودی و سرور خروجی که نشست را پایان می‌دهد (anchor) می‌توانند جدا باشند	دست‌دهی Noise NK: کارخواه هویت anchor را با کلید عمومی‌ای که همراه پیکربندی می‌رسد تأیید می‌کند؛ توافق کلید ترکیبی X25519 + ML-KEM-768. رکوردها با ChaCha20-Poly1305 محافظت می‌شوند	دست‌دهی پساکوانتومی به‌صورت پیش‌فرض. جدید و کد بسته؛ هنوز ممیزی رمزنگاری مستقل نداشته است. در iOS موجود نیست.

اینکه کدام هسته یک روش انتقال را اجرا می‌کند به پلتفرم بستگی دارد. Android و iOS 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. در Android 3.2 و Windows 3.2 و Linux 1.8 و بالاتر، ColituGecko با کارخواه اختصاصی Gecko از Colitu اجرا می‌شود و روی سرورها نرم‌افزار اختصاصی Gecko از Colitu اجرا می‌شود. در Linux منوی پروتکل وجود ندارد؛ Gecko در Adaptive Connect به‌صورت خودکار آزموده می‌شود. Gecko در iOS موجود نیست.

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. تغییر مسیر درون ColituGecko متفاوت است: وقتی یک مسیر قطع می‌شود، جریان در همان نشست به مسیر دیگری می‌رود، بایت‌هایی که طرف مقابل تأیید نکرده دوباره فرستاده می‌شوند و تونل از نو ساخته نمی‌شود. اگر همهٔ مسیرها قطع شوند ترافیک متوقف می‌شود و اگر پیش از

انقضای نشست مسیری به همان anchor برگردد، می‌تواند ادامه یابد. اگر خود anchor از کار بیفتد، اتصال‌های باز به

شرح فنی کامل ColituGecko: colitu.com/gecko/technical.

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 ریشهٔ 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.
ذخیرهٔ رمز عبور	Argon2id: حافظهٔ 64 MiB، 3 گذر، 2 مسیر، نمک تصادفی 16 بایتی، هش 32 بایتی. رمزهای عبور هرگز به‌صورت متن ساده ذخیره نمی‌شوند.
توکن‌های دسترسی	JWT امضاشده با HMAC-SHA256 از یک حلقهٔ کلید چرخان، با اعتبار 15 دقیقه.
توکن‌های تازه‌سازی	32 بایت تصادفی، فقط به‌صورت هش SHA-256 ذخیره می‌شود، با اعتبار 30 روز، در هر استفاده جایگزین می‌شود. استفاده‌ی مجدد از توکن قدیمی کل خانوادهٔ توکن را باطل می‌کند.
صفحهٔ 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.
کلیدهای Reality	یک جفت کلید X25519 برای هر روش انتقال در هر سرور، تولیدشده روی صفحهٔ کنترل.
گواهی‌های TLS سرور	Let's Encrypt، روی هر سرور صادر می‌شود؛ کلید خصوصی روی همان سرور می‌ماند.
رازها در پایگاه داده	اعتبارنامه‌های ارائه‌دهندهٔ پرداخت، ایمیل و هوش مصنوعی با AES-256-GCM رمزگذاری می‌شوند.
مانیفست‌های به‌روزرسانی	امضاهای ECDSA P-256 که برنامه‌ها در برابر یک کلید عمومی تعبیه‌شده راستی‌آزمایی می‌کنند.
پشتیبان‌ها	با age به یک کلید عمومی رمزگذاری می‌شوند؛ تهیهٔ پشتیبان فقط به همان کلید نیاز دارد. کلید رمزگشایی آفلاین نگه داشته می‌شود و روی هیچ سروری نیست.

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

کلیدها کجا نگهداری می‌شوند و اگر یکی فاش شود چه می‌شود

- کلید خصوصی مرجع صدور گواهی یک فایل روی صفحهٔ 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 دادهٔ صفحهٔ کنترل ذخیره می‌شوند. رمزگذاری این مقادیر در سطح پایگاه داده در نقشهٔ راه است.
- هنوز چرخش زمان‌بندی‌شدهٔ کلیدهای Reality وجود ندارد. اگر به نفوذ به یک سرور مشکوک شویم، آن سرور از برنامه‌ها برداشته می‌شود و کلیدها و اعتبارنامه‌هایش تعویض می‌شوند.
- صفحهٔ کنترل هر روز یک پشتیبان رمزگذاری‌شده می‌گیرد و آن را 3 روز نگه می‌دارد. یک نسخه با Object Lock به Backblaze B2 (EU Central، آمستردام) می‌رود: تا 30 روز هیچ‌کس، از جمله Colitu، نمی‌تواند آن را حذف یا تغییر دهد و حداکثر پس از 36 روز خودکار حذف می‌شود. کلید رمزگشایی از 16 اکتبر 2026 آفلاین نگه داشته می‌شود، بنابراین نه سرور می‌تواند پشتیبان‌ها را بخواند و نه Backblaze. بازیابی از نسخهٔ خارج از محل در 16 اکتبر 2026 آزمایش شد. تصاویر لحظه‌ای پایگاه داده که پیش از استقرار گرفته می‌شوند رمزگذاری نشده‌اند و حداکثر 7 روز روی سرور صفحهٔ کنترل می‌مانند.

8 حساب‌ها و نشست‌ها

- ورود با ایمیل و رمز عبور است. تلویزیون می‌تواند با نمایش یک کد 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 همهٔ دستگاه‌ها و نشست‌های وب را خارج می‌کند. پس از بازنشانی با کد ایمیل، حذف حساب و خاموش کردن تأیید دومرحله‌ای 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 صفحهٔ حساب خود حذف کنید. صفحهٔ امنیت نشست‌های مرورگر را با برچسب دستگاه (مرورگر و سیستم‌عامل)، کشور، روش ورود و نشانی IP فهرست می‌کند؛ می‌توانید یک نشست را ببندید، همهٔ 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 همهٔ نشست‌های وب دیگر و همهٔ 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 دومرحله‌ای، کلیدهای عبور) به 10 تلاش در هر 15 دقیقه برای هر حساب محدود هستند.
- تأیید دومرحله‌ای (TOTP) برای هر حساب اختیاری است. آن را در colitu.com/account/security با یک برنامهٔ احرازهویت 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؛ برنامهٔ 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 حذفش کنید، و سپس در صفحهٔ ورود از «ورود با کلید عبور» استفاده کنید. کلید عبور دارای تأیید کاربر دو عامل به حساب می‌آید، بنابراین از کد تأیید دومرحله‌ای 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 دومرحله‌ای، 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 هشداری ظاهر می‌شود. Colitu برای این کار هیچ نشانی IP ذخیره نمی‌کند، فقط شمارش ناشناس روزانهٔ 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 همهٔ 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، IPv6، DNS 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 رمزگذاری‌شده می‌ماند. Colitu ترافیک HTTPS را رمزگشایی یا بازرسی نمی‌کند.

پیش‌فرض‌های مسیریابی

	Android	Windows	iOS	Linux (بتا)
ترافیک چگونه گرفته می‌شود	VPN سیستمی (همهٔ برنامه‌ها)	حالت TUN (همهٔ ترافیک) برای نصب‌های جدید؛ نصب‌هایی که از حالت پروکسی سیستمی استفاده می‌کردند آن را نگه می‌دارند	VPN سیستمی (همهٔ برنامه‌ها)	پروکسی سیستمی به‌صورت پیش‌فرض؛ حالت TUN اختیاری
به‌طور پیش‌فرض پوشش داده نمی‌شود	شبکهٔ محلی	در حالت پروکسی سیستمی: برنامه‌هایی که پروکسی سیستم را نادیده می‌گیرند، حل‌کنندهٔ DNS ویندوز، مرورگر UDP (QUIC/WebRTC)، IPv6. حالت TUN آن‌ها را پوشش می‌دهد.	شبکهٔ محلی	مانند Windows در حالت پروکسی سیستمی

	Android	Windows	iOS	Linux (بتا)
سایت‌ها و IPهای منطقه‌ای (فهرست داخلی)	فقط اگر حالت حریم خصوصی خاموش باشد خارج از VPN است، مگر اینکه سرور در آن منطقه باشد	فقط اگر حالت حریم خصوصی خاموش باشد خارج از VPN است، مگر اینکه سرور در آن منطقه باشد	فقط اگر حالت حریم خصوصی خاموش باشد خارج از VPN است، مگر اینکه سرور در آن منطقه باشد	فقط اگر حالت حریم خصوصی خاموش باشد خارج از VPN است، مگر اینکه سرور در آن منطقه باشد
DNS	از طریق تونل به 1.1.1.1	TUN: از طریق تونل به DNS-over-HTTPS مربوط به Cloudflare. حالت پروکسی: فقط برای ترافیکی که به پروکسی می‌رسد.	از طریق تونل (8.8.8.8 ← Xray ← 1.1.1.1)	مانند Windows
IPv6	🟢مسدود	🟡در حالت TUN با قطع‌کن اضطراری مسدود است؛ در حالت پروکسی سیستمی پوشش داده نمی‌شود	🟢نشت نمی‌کند: به تونل هدایت می‌شود و همان‌جا حذف می‌شود	🟡مانند Windows
قطع‌کن اضطراری (Kill Switch)	🟡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، به‌صورت پیش‌فرض روشن (در ادامه ببینید)	🟡«مسدود کردن اینترنت بدون VPN» (iOS includeAllNetworks)، به‌صورت پیش‌فرض 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

سایت‌های منطقه‌ای خارج از VPN

	Android	Windows	iOS	Linux (بتا)
تونل‌زنی تقسیم‌شده	● برنامه‌ها و سایت‌ها و نشانی‌های IP	● برنامه‌ها (فقط حالت TUN)	● فقط سایت‌ها و نشانی‌های IP	● برنامه‌ها و سایت‌ها و نشانی‌های IP (فقط حالت TUN)
چندجهشی (Multihop) و IP چرخان	● فقط VLESS	● فقط VLESS	● فقط VLESS	● فقط VLESS

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 ارائه‌دهندهٔ 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 به‌صورت پیش‌فرض روشن است (Windows و Android نسخهٔ 2.7.0، iOS نسخهٔ 5.6.0، Linux نسخهٔ 1.3.0 و بعدتر)، بنابراین به‌طور پیش‌فرض همهٔ 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 به‌تفصیل

- همهٔ ترافیک IPv4 و IPv6 را مسدود می‌کند، به‌جز loopback، شبکهٔ محلی (یک تنظیم، به‌صورت پیش‌فرض روشن)، DHCP، هسته‌های VPN، مبدل TUN و خود برنامهٔ 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 جداگانهٔ Windows (LocalSystem، ColituKillSwitch، شروع خودکار) به‌صورت قوانین دائمی Windows Filtering Platform نگه داشته می‌شوند. اگر برنامه یا هستهٔ 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 همهٔ 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 به‌روزرسانی و دانلود به‌روزرسانی (colitu.com).
- اندازه‌گیری تأخیر تا سرورها.
- در Windows، حل نام میزبان سرورها از طریق DNS-over-HTTPS مربوط به Cloudflare یا Google.

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

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

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 روزانهٔ شبکه‌های متمایز برای هر پیوند، به مدت 48 ساعت نگه داشته می‌شود.

داده	مدت نگهداری	هدف
نشانی ایمیل، هش رمز عبور (Argon2id)، زبان، تاریخ‌های حساب	تا زمان حذف حساب؛ در هنگام حذف، نشانی با یک مقدار جایگزین می‌شود و رمز عبور غیرقابل استفاده می‌گردد	حساب و ورود

داده	مدت نگهداری	هدف
کدهای تأیید ایمیل و بازنشانی رمز عبور (نشانی، هش کد، نشانی IP)	7 روز	تأیید نشانی ایمیل، بازنشانی رمز عبور
رویدادهای ورود (نشانی IP، کشور، مرورگر یا برنامه)	180 روز	امنیت حساب، جلوگیری از سوءاستفاده
نشانی IP و کشور هنگام ثبت‌نام و در آخرین ورود	ثبت‌نام: 180 روز. آخرین ورود: اگر 180 روز ورودی انجام نشود پاک می‌شود	امنیت حساب، قواعد منطقه‌ای
ثبت‌نام‌ها و ورودهای ردشده بر اساس قواعد منطقه‌ای (نشانی IP، کشور)	90 روز	اجرای قواعد منطقه‌ای
نشست‌های وب (نشانی IP، کشور، مرورگر، روش ورود)	30 روز پس از پایان نشست (خروج، انقضا یا ابطال) حذف می‌شود	ورود، فهرست نشست‌ها در صفحهٔ حساب
توکن‌های ورود برنامه (فقط به‌صورت هش ذخیره می‌شوند و به یک دستگاه متصل‌اند)	30 روز پس از انقضا یا ابطال حذف می‌شوند	حفظ ورود در برنامه‌ها
تأیید دومرحله‌ای (کلید رمزگذاری‌شدهٔ برنامهٔ احراز هویت، هش کدهای بازیابی یک‌بارمصرف، مراحل ورود 5 دقیقه‌ای)	کلید و کدهای بازیابی تا زمانی که آن را خاموش کنید یا حساب حذف شود؛ مراحل ورود 1 روز پس از انقضا حذف می‌شوند	امنیت حساب
کلیدهای عبور (passkey) (کلید عمومی، شناسهٔ اعتبارنامه، نامی که می‌دهید، شمارندهٔ امضا، تاریخ ایجاد و آخرین استفاده؛ کلید خصوصی و هرگونه داده زیستی هرگز از دستگاه شما خارج نمی‌شود؛ درخواست‌های تأیید یک‌بارمصرف 5 دقیقه‌ای)	تا زمانی که کلید عبور را حذف کنید یا حساب حذف شود؛ درخواست‌های تأیید پس از 5 دقیقه منقضی و حذف می‌شوند	ورود بدون رمز عبور و امنیت حساب
اطلاعات اتصال VPN (کلیدهای تصادفی به‌ازای هر سرور، متصل به یک دستگاه یا یک پیوند اشتراک)	تا زمانی که دستگاه یا پیوند در حال استفاده است؛ 30 روز پس از حذف یا جایگزینی حذف می‌شود	دسترسی به VPN

داده	مدت نگهداری	هدف
پیوندهای اشتراک (نامی که می‌دهید، تاریخ ایجاد، آخرین استفاده و انقضا، نشانهٔ «احتمالاً به اشتراک گذاشته شده»؛ خود پیوند فقط به‌صورت 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 شبکهٔ مختلف استفاده شده به مدت 48 ساعت نگه داشته می‌شود	تا زمانی که پیوند را باطل کنید یا حساب را حذف کنید (پیوند منقضی‌شده خودکار باطل می‌شود)؛ شمارش شبکه‌ها پس از 48 ساعت خودبه‌خود حذف می‌شود	یک پیوند به‌ازای هر دستگاه و هشدار پیوند اشتراکی
درخواست‌های ورود تلویزیون (نام دستگاه، نشانی IP، کشور)	1 روز پس از انقضای کد 10 دقیقه‌ای حذف می‌شود	ورود با کد QR
دستگاه‌ها (نام، پلتفرم، نسخهٔ برنامه و سیستم‌عامل، آخرین نشانی IP و کشور، هش کلیددار شناسهٔ سخت‌افزار)	تا زمانی که دستگاه در حساب است نگه داشته می‌شود. نام، نشانی IP، کشور و هش سخت‌افزار دستگاه حذف‌شده پس از 30 روز پاک می‌شود؛ نشانی IP و کشور دستگاهی که 180 روز دیده نشده پاک می‌شود	سقف دستگاه‌ها، امنیت حساب
تلاش‌های ردشدهٔ افزودن دستگاه و دورهٔ آزمایشی (نشانی IP، جزئیات دستگاه)	180 روز	سقف دستگاه‌ها، جلوگیری از سوءاستفاده
بررسی‌های سوءاستفاده از طرح رایگان و دورهٔ آزمایشی (هش‌های کلیددار HMAC-SHA256 از نشانی ایمیل، شناسهٔ سخت‌افزار و شبکه؛ کلید در پایگاه داده ذخیره نمی‌شود)	شبکه: 30 روز. ایمیل و شناسهٔ 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	جلوگیری از ایجاد مکرر حساب رایگان
بررسی خودکار ربات و سوءاستفاده: برای حساب‌های معلق‌شده یا مسدودشده امتیاز، نشانه‌های برانگیزاننده، نشانی IP، کشور، شبکه (ASN) و شناسهٔ مرورگر؛ برای ثبت‌نام‌هایی که پیش از ساخت حساب رد شده‌اند، نشانی ایمیل نیز	حساب‌های معلق‌شده یا مسدودشده: تا زمانی که حساب وجود دارد و همراه آن حذف می‌شود. ثبت‌نام‌های ردشده: 30 روز	جلوگیری از ربات‌ها، ثبت‌نام خودکار و جمع‌آوری نشانی سرورها

داده	مدت نگهداری	هدف
بررسی‌های سوءاستفاده از کد تبلیغاتی دورهٔ آزمایشی (هش‌های کلیددار HMAC-SHA256 از نشانی ایمیل نرمال‌سازی‌شده، شناسهٔ سخت‌افزار دستگاه و شبکه — IPv4 با /32 و /24 یا IPv6 با /64 و /48؛ کلید در پایگاه داده ذخیره نمی‌شود)	شبکه: 35 روز. ایمیل و شناسهٔ سخت‌افزار: 365 روز، حتی پس از حذف حساب	هر نفر فقط یک کد آزمایشی
درخواست‌های انتقال از سرویس قبلی (شناسه و نام Telegram، یادداشت‌ها، نشانی IP)	30 روز پس از آخرین تغییر حذف می‌شود. از درخواست تأییدشده فقط هش کلیددار شناسهٔ Telegram به مدت 2 سال می‌ماند	انتقال اشتراک‌های قدیمی؛ جلوگیری از انتقال دوبارهٔ یک اشتراک
برچسب منبع ثبت‌نام (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.	همراه حساب حذف می‌شود	اندازه‌گیری تجمیعی اینکه کدام کانال‌ها کاربران واقعی می‌آورند و اولین اتصال چقدر طول می‌کشد
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.	با حذف هر یک از دو حساب حذف می‌شود	اعطای پاداش دعوت؛ جلوگیری از سوءاستفاده (نشانی IP یا دستگاه یکسان، ایمیل یک‌بارمصرف)؛ اندازه‌گیری تجمیعی ثبت‌نام‌های ناشی از دعوت

داده	مدت نگهداری	هدف
آمار استفادهٔ ناشناس برنامه‌ها: نتیجهٔ اتصال‌ها و نوع خطا، زمان اتصال و بازیابی (به‌صورت 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 شمارهٔ ارائه‌دهندهٔ اینترنت (ASN) شبکهٔ 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. به رویدادهای سرور موقعیتی در سطح شهر نیز افزوده می‌شود: شهر هنگام دریافت گزارش از نشانی IP آن تشخیص داده می‌شود و نشانی نگه داشته نمی‌شود؛ یک شهر فقط وقتی جداگانه نشان داده می‌شود که در آن روز دست‌کم پنج دستگاه مختلف از آن گزارش داده باشند (دستگاه‌ها با یک نام مستعار ساعتی شمرده می‌شوند که با پایان ساعت حذف می‌شود). در تنظیمات برنامه قابل خاموش کردن است.	جمع‌های کل بدون محدودیت زمانی نگه داشته می‌شوند (غیرقابل ارتباط با یک فرد)؛ جمع‌های سرور همراه با شهر 90 روز	اندازه‌گیری و بهبود کیفیت اتصال، Adaptive Connect و استفاده از قابلیت‌ها
Colitu Passport در حساب شما ذخیره می‌شود و در هر دستگاهی که وارد شوید همراهتان است. برای هر کشور تمبر: زمان بازشدن و تعداد قطعه‌ها؛ دستاوردها، مجموعه‌ها، پیشرفت سفرهای هفتگی، نام مستعار، عنوان، جلد، اختلاف منطقهٔ زمانی و شمارهٔ کلکسیونر؛ جمع‌های روزانه (دقیقه‌های استفاده، قطعه‌ها، دقیقه‌های شب و صبح زود و فهرست کشورهای استفاده‌شده در آن روز)؛ سری جاری (کشور، طول آن و آخرین دقیقهٔ شمرده‌شده)؛ رویدادهای پاداش برای انیمیشن‌های نمایش در برنامه‌ها. دقیقه‌ها را سرورهای ما از روی زمان اتصال می‌شمارند: اگر یکی از سرورهای ما در آن دقیقه ترافیک حساب شما را گزارش کند، آن دقیقه شمرده می‌شود (هر دقیقه حداکثر یک بار، به هر تعداد دستگاه) و کشور همان کشور سرور است؛ برنامه‌ها نمی‌توانند دقیقه اضافه کنند. فقط جمع‌های روزانه و به‌ازای هر کشور نگه داشته می‌شود؛ هیچ گزارش دقیقه‌به‌دقیقه یا نشستی، وب‌سایت یا نشانی IP ثبت نمی‌شود. پیشرفتی که از نسخهٔ قدیمی روی دستگاه بوده، برای هر دستگاه یک بار وارد می‌شود (در حد معقول و مقدار بالاتر معتبر است).	جمع‌های روزانه 400 روز، رویدادهای پاداش 30 روز، بقیه تا زمان حذف حساب	ذخیرهٔ گذرنامه در حساب شما، نمایش آن در هر دستگاه و محاسبهٔ پاداش‌ها و سفرهای هفتگی

داده	مدت نگهداری	هدف
شمارنده‌های ناشناس و اختیاری Colitu Passport، حداکثر یک گزارش در روز: تعداد تمبرهای بازشده، بالاترین فصل باز، تعداد تمبرها در هر سطح، سفرهای هفتگی تکمیل‌شده، قطعه‌های به‌دست‌آمده در آن روز و اینکه گذرنامه در آن روز باز شده است یا نه. بدون احراز هویت فرستاده می‌شود؛ سرور هر گزارش را فقط به جمع‌های روزانه اضافه می‌کند و هیچ ردیف گزارش، حساب، دستگاه یا نشانی IP ذخیره نمی‌کند. اینکه تمبرها از کدام کشورها و چه زمانی به دست آمده‌اند فرستاده نمی‌شود. فقط نسخه‌های قدیمی برنامه آن را می‌فرستند؛ نسخه‌های جدید نمی‌فرستند، چون گذرنامه اکنون در حساب شما نگه داشته می‌شود (ردیف «Colitu Passport» را ببینید). این تنظیم در ابتدا خاموش است و در برنامه قابل خاموش کردن است.	جمع‌های کل بدون محدودیت زمانی نگه داشته می‌شوند (غیرقابل ارتباط با یک فرد)	دیدن تجمیعی میزان استفاده از گذرنامه و متعادل بودن قواعد آن (سرعت سطح‌ها و قطعه‌ها)
پاسخ‌های شما به نظرسنجی‌های درون‌برنامه: 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)	با حذف حساب، پیوند با آن و نظر حذف می‌شود؛ فقط امتیاز ناشناس باقی می‌ماند	اندازه‌گیری تجمیعی رضایت (NPS)، تناسب محصول با بازار و دلایل ترک
امتیاز 1–5 و نظر اختیاری که به یک گفتگوی پشتیبانی حل‌شده می‌دهید؛ زمان اولین پاسخ و زمان حل آن	همراه گفتگوی پشتیبانی حذف می‌شود	اندازه‌گیری تجمیعی کیفیت پشتیبانی (رضایت، زمان پاسخ و حل)
اینکه برای یک دستگاه کدام پروتکل‌های انتقال روی کدام سرور و با چه سرعتی کار کرده‌اند (بدون نشانی IP)	با هر گزارش بازنویسی می‌شود؛ ۳۵ روز پس از آخرین گزارش حذف می‌شود	امتحان کردن ابتدایی پروتکل‌های انتقال کارآمد
طرح، پرداخت‌ها و سفارش‌ها (از جمله فضای اضافهٔ Colitu Space؛ مبلغ، نوع روش پرداخت، شناسهٔ تراکنش ارائه‌دهنده، اعلان ارائه‌دهنده؛ برای پرداخت‌های ریالیت، یک شمارهٔ ثابت پرداخت‌کننده متصل به حساب)	تا مدتی که قانون حسابداری و مالیات الزام می‌کند، حتی پس از حذف حساب؛ حذف خودکار در پایان آن مدت هنوز پیاده‌سازی نشده است	صورتحساب، بازپرداخت، تعهدات قانونی

داده	مدت نگهداری	هدف
گاوصندوق Colitu Space: شناسهٔ حساب، اندازهٔ داده‌های رمزگذاری‌شده، تعداد فایل‌ها، تاریخ‌های ایجاد و تغییر، ساختار پوشه‌ها (هر مورد در کدام پوشه است)، تعداد نسخه‌ها، علامت مورد علاقه، زمان پایان حالت سفر، تنظیمات گاوصندوق (مدت قفل خودکار)، مواد کلید رمزگذاری‌شده (نمک و پارامترهای Argon2id، کلید اصلی بسته‌بندی‌شده با رمز عبور و با کلید بازیابی) و سوابق کلید عبور. رمز عبور گاوصندوق هرگز به سرور فرستاده نمی‌شود	تا زمان حذف گاوصندوق یا حساب Colitu	ارائهٔ Colitu Space: باز کردن گاوصندوق، فهرست‌کردن فایل‌ها و پوشه‌ها، اعمال سقف فضای ذخیره‌سازی
فایل‌هایی که در Colitu Space بارگذاری می‌کنید، تصاویر بندانگشتی، نام فایل‌ها و پوشه‌ها، اطلاعات فایل‌ها و نمایهٔ شما (نام و تصویر نمایه): در مرورگر شما با کلید خودتان رمزگذاری می‌شوند؛ Colitu محتوا، نام‌ها، نمایه و کلید شما را نمی‌بیند. داده‌های رمزگذاری‌شده در Backblaze B2 و در یک حساب جداگانهٔ Colitu نگهداری می‌شوند	فایل‌های حذف‌شده 30 روز در سطل زباله می‌مانند و سپس برای همیشه حذف می‌شوند؛ از هر فایل حداکثر 10 نسخهٔ قدیمی نگه داشته می‌شود؛ با حذف گاوصندوق یا فایل، اشیای آن از طریق صف حذف از محل ذخیره‌سازی هم پاک می‌شوند؛ با حذف گاوصندوق یا حساب Colitu همه چیز حذف می‌شود	نگهداری رمزگذاری‌شدهٔ فایل‌های شما و ارائهٔ آن‌ها به شما
اشتراک‌گذاری‌های Colitu Space (فقط میان کاربران Colitu Space و با رمزگذاری سرتاسری): اینکه چه کسی چه چیزی را با چه کسی به اشتراک گذاشته، همراه با محتوای رمزگذاری‌شده اما بدون دیدن محتوا؛ تاریخ‌های اشتراک‌گذاری؛ اگر گیرنده‌ای اشتراک‌گذاری را گزارش کند، دلیل (غیرقانونی، آزار، هرزنامه یا سایر) و یادداشت اختیاری	حداکثر تا زمان حذف گاوصندوق یا حساب Colitu	ارائهٔ اشتراک‌گذاری؛ جلوگیری از سوءاستفاده با بررسی گزارش‌ها
پیوندهای درخواست فایل در Colitu Space: برچسب عمومی‌ای که صاحب پیوند می‌نویسد (رمزگذاری نمی‌شود) و تعداد و اندازهٔ فایل‌های دریافتی. کسی که حساب ندارد می‌تواند با پیوند به گاوصندوق فایل بفرستد؛ فایل در مرورگر خودش رمزگذاری می‌شود. نشانی IP بارگذارنده فقط در شمارنده‌ای برای سقف اندازهٔ روزانه نگه داشته می‌شود و در پایگاه داده نوشته نمی‌شود	برچسب، تعداد و اندازهٔ فایل‌ها: حداکثر تا زمان حذف گاوصندوق یا حساب Colitu؛ نشانی IP بارگذارنده: در شمارنده حداکثر 25 ساعت	ارائهٔ قابلیت درخواست فایل؛ جلوگیری از سوءاستفاده با سقف اندازهٔ روزانه

داده	مدت نگهداری	هدف
دسترسی اضطراری Colitu Space: مخاطب دسترسی اضطراری که صاحب گاوصندوق برمی‌گزیند (کاربر دیگری از Colitu Space)، مدت انتظار (1 تا 30 روز)، تاریخ‌های درخواست و رد، و کلید اصلی مهروموم‌شده با کلید آن مخاطب	حداکثر تا زمان حذف گاوصندوق یا حساب Colitu	امکان دسترسی مخاطب انتخاب‌شده به گاوصندوق در صورتی که صاحب آن در مدت انتظار رد نکند
حساب شرکتی Colitu Business: نام شرکت، ایمیل صورتحساب، کشور، شمارهٔ مالیاتی، تعداد صندلی‌ها و مدت آن‌ها؛ عضویت (نقش، تاریخ‌های دعوت، پیوستن و خروج، کسی که عضو را افزوده است)؛ صورتحساب‌های شرکت و گزارش فعالیت شرکت. مالک و مدیران شرکت نشانی ایمیل و نقش هر عضو و نام، پلتفرم، نسخهٔ برنامه و آخرین زمان فعالیت دستگاه‌های او را می‌بینند؛ ترافیک و سایت‌های بازدیدشده را نمی‌بینند	تا زمانی که Colitu حساب شرکت را ببندد؛ صورتحساب‌های شرکت تا مدتی که قانون حسابداری و مالیات الزام می‌کند؛ پیوندهای تنظیم رمز عبور 7 روز معتبرند. وقتی عضوی حساب خود را حذف کند، عضویتش بسته می‌شود و صندلی به شرکت بازمی‌گردد	مدیریت صندلی‌های شرکت، صورتحساب شرکت، یادآوری‌های تمدید
کسب‌وکارها و تولیدکنندگان محتوایی که پیشنهاد همکاری Colitu Business برایشان می‌فرستیم: نام شرکت یا کانال، نشانی ایمیلی که برای تماس تجاری در وب‌سایت یا توضیحات کانال خود منتشر کرده‌اند، کشور و زبان؛ ایمیل‌هایی که فرستاده‌ایم و زمان آن‌ها؛ موضوع و ۳۰۰ نویسهٔ نخست پاسخ‌ها، و ایمیل‌های برگشتی	سوابق ارسال و پاسخ در پنل پس از ۱۲ ماه حذف می‌شوند. فهرست تماس تا زمانی نگه داشته می‌شود که مخاطب بخواهد دیگر برایش ننویسیم یا نشانی دیگر لازم نباشد؛ به نشانی‌ای که پاسخ «برایم ننویسید» بدهد دیگر ایمیل فرستاده نمی‌شود	ارائهٔ همکاری نمایندگی و برچسب سفید Colitu Business (منافع مشروع؛ در هر ایمیل راه اعتراض و پیوند این سیاست آمده است)
گفتگوهای پشتیبانی و پیوست‌ها، از جمله گزارش‌های برنامه که برنامه پیوست می‌کند (نشانی‌ها، نام سایت‌ها و اطلاعات محرمانه پوشانده شده‌اند)	گفتگوهای بسته‌شده: 2 سال پس از آخرین پیام حذف می‌شوند	پشتیبانی، رسیدگی به شکایات

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 داده‌ها را حداکثر 36 روز نگه می‌دارند، و تصاویر لحظه‌ای رمزگذاری‌نشده‌ای که پیش از یک استقرار گرفته شده‌اند حداکثر 7 روز. 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.

داده	مدت نگهداری	هدف
گزارش‌های خطای اتصال ColituGecko (نسخهٔ آزمایشی): کدام ورودی سرور و کدام پوشش ناموفق بوده، نوع خطا، مقدار بایت‌هایی که تا آن لحظه عبور کرده (به‌صورت بازه) و زمان آن؛ ثبت یک اتصال سالم با بازه‌های کلی تأخیر، سرعت و مدت اتصال (بدون مقدار خام) و نسخهٔ برنامه؛ سرور فقط مجموع‌های ساعتی را به ازای هر ورودی و هر شبکه (کشور + ASN که هنگام دریافت درخواست استخراج می‌شود؛ نشانی IP نگهداری نمی‌شود) نگه می‌دارد؛ دستگاه‌ها با یک نام مستعار ساعتی شمرده می‌شوند. حساب، دستگاه یا سایت‌های بازدیدشده ذخیره نمی‌شوند	مجموع‌های ساعتی ۹۰ روز؛ نام‌های مستعار دستگاه ۴۸ ساعت	یافتن ورودی‌هایی که یک شبکه مسدود می‌کند و کنار گذاشتن موقت آن‌ها برای همان شبکه
گزارش اتصال: وقتی پشتیبانی مشکل اتصالی را بررسی می‌کند، برنامه شما در اجرای بعدی اطلاعات برنامه و دستگاه، رویدادهای اتصال و گزارش‌های برنامه را می‌فرستد؛ نام سایت‌ها و نشانی‌ها در دستگاه و روی سرور پوشانده می‌شوند و سایت‌هایی که بازدید می‌کنید فرستاده نمی‌شوند. گزارش همچنین گزارش آخرین تصمیم‌های Adaptive Connect را دارد (سرورهای نامزد، اندازه‌گیری‌ها، انتخاب و نتیجه، سرورهای پنهان‌شده، بررسی‌های فهرست سفید)؛ از گزارش پوشانده‌شده با هوش مصنوعی یک تشخیص برای پشتیبانی نوشته می‌شود	پس از 90 روز حذف می‌شود	رفع مشکلات اتصال (پشتیبانی)
گفتگوهای Colitu Bot (متن، نشانی IP، بازخورد «آیا مفید بود»)	180 روز	پاسخ دادن به پرسش‌ها
سوابق تحویل ایمیل (نشانی گیرنده، نوع ایمیل)	90 روز	حل مشکلات تحویل
اشتراک خبرنامه (نشانی ایمیل، زبان، زمان تأیید)؛ فقط اگر از طریق پیوند داخل ایمیل تأیید کنید	تا زمانی که لغو اشتراک کنید؛ ثبت‌نام‌های تأییدنشده پس از 7 روز حذف می‌شوند	ایمیل‌های اعلان، یادداشت انتشار و پیشنهاد (با رضایت شما)
گزارش‌های دسترسی وب‌سایت و API (نشانی IP، نشانی درخواستی، مرورگر)	14 روز	اداره و حفاظت از سرویس
آزمون نشت DNS در وب‌سایت ما	فقط در حافظه، 10 دقیقه	نمایش نتیجهٔ آزمون
گزارش ممیزی (اقدامات مدیران و برخی اقدامات حساب مانند حذف حساب، بر اساس شناسهٔ حساب)	بدون محدودیت زمانی؛ دلیل اختیاری که هنگام حذف حساب می‌نویسید: 180 روز	پاسخگویی در قبال اقدامات

11 تله‌متری و اشخاص ثالث

تله‌متری در برنامه‌ها

- هیچ‌یک از برنامه‌های Colitu (Android، iOS، Windows، Linux) کتابخانهٔ تحلیل، تبلیغات یا گزارش خرابی ندارد؛ برنامهٔ iOS از نسخهٔ 5.4.1 چنین کتابخانه‌ای ندارد.
- همهٔ 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
ارائه‌دهندهٔ پرداخت (فقط برای مشتریانی که طرح پولی خریده‌اند)	شمارهٔ سفارش، مبلغ، ارز، توضیح طرح و روش پرداخت؛ اطلاعات کارت یا بانک در صفحهٔ 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 نویسهٔ 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).
Backblaze B2 (EU Central، آمستردام)	نسخه‌های رمزگذاری‌شدهٔ پشتیبان روزانه. این شرکت نمی‌تواند آن‌ها را بخواند: کلید رمزگشایی آفلاین نگه داشته می‌شود.
ارائه‌دهندگان میزبانی	سرورها را اجرا می‌کنند و از نظر فنی به آن‌ها دسترسی دارند.

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

امنیت برنامه

	Android	Windows	iOS	Linux (بتا)
توکن‌های نشست	AES-256-GCM با کلید Android Keystore (کلید نرم‌افزاری اگر Keystore شکست بخورد)	DPAPI (کاربر فعلی)	Keychain (پس از اولین بازگشایی قفل در دسترس است)	AES-GCM با کلیدی مشتق‌شده از ماشین و کاربر
اعتبارنامه‌های اتصال	رمزگذاری‌شده (AES-GCM)	متن ساده در یک پایگاه داده که فقط مدیران و SYSTEM می‌توانند بخوانند	فایل متن ساده در محفظهٔ خصوصی برنامه	فایل‌های محافظت‌شده (0600)
سنجاق کردن گواهی برای API	● بله	● بله (از 10 اکتبر 2026)	● بله (از 10 اکتبر 2026)	● بله (از 10 اکتبر 2026)
سطح دسترسی	برنامهٔ عادی با مجوز VPN	همیشه با دسترسی مدیر اجرا می‌شود؛ یک سرویس پس‌زمینهٔ جداگانه (ColituKillSwitch، LocalSystem) قوانین قطع‌کن اضطراری را نگه می‌دارد	افزونهٔ شبکه	sudo می‌خواهد؛ رمز عبور در حافظه نگه داشته می‌شود
گزارش‌های محلی VPN	فقط هشدارها؛ بدون گزارش دسترسی	فقط هشدارها؛ نشانی‌ها پنهان؛ پس از 7 روز حذف می‌شود	فقط هشدارها؛ بدون گزارش دسترسی	فقط هشدارها
پشتیبان‌گیری از داده‌های برنامه	غیرفعال	—	موارد Keychain روی دستگاه می‌مانند	—

سنجاق کردن (pinning) یعنی گواهی ریشه‌ای که شخص دیگری روی دستگاه نصب کرده برای خواندن ترافیک API برنامه‌ها قابل استفاده نیست. بنابراین نرم‌افزارهای امنیتی که با درج گواهی ریشهٔ خودشان HTTPS را بازرسی می‌کنند اتصال API برنامه‌ها را مسدود می‌کنند؛ در چنین نرم‌افزارهایی Colitu را مستثنا کنید.

13 به‌روزرسانی‌ها و زنجیرهٔ تأمین

پلتفرم	نحوهٔ راستی‌آزمایی به‌روزرسانی
Android (نسخهٔ دانلودی)	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 برنامهٔ نصب‌شده امضا شده باشد. نسخه‌های قدیمی‌تر رد می‌شوند.
Android (Google Play)	از طریق Google Play به‌روزرسانی می‌شود.
Windows	همان مانیفست امضاشده، دانلود HTTPS از colitu.com، بررسی SHA-256، که دوباره توسط مرحلهٔ نصب‌کنندهٔ با دسترسی بالا بررسی می‌شود. نصب‌کننده هنوز با Authenticode امضا نشده است، بنابراین Windows SmartScreen ممکن است هشدار دهد.
Linux	مانیفست امضاشده 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. صفحهٔ 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؛ نصب‌کنندهٔ Windows روی دستگاه توسعه‌دهنده ساخته می‌شود؛ بسته‌های Linux در CI ساخته می‌شوند؛ ساخت‌های iOS TestFlight روی Codemagic انجام می‌شوند.
- ساخت‌های Android (از 2.9.3) و Windows (از 2.9.8) بازتولیدپذیر هستند، بنابراین هر کسی می‌تواند کد منبع برچسب‌خورده را دوباره بسازد و نتیجه را با فایل منتشرشده مقایسه کند. در iOS و Linux یک مجموع کنترلی هنوز فقط ثابت می‌کند فایلی که منتشر کرده‌ایم را دارید، نه اینکه از کد منبع برچسب‌خورده ساخته شده است. کتابخانهٔ هستهٔ Xray در Android همان فایل باینری رسمی بالادستی (upstream) است که با SHA-256 سنجاق شده و از روی کد منبع دوباره ساخته نمی‌شود.

چه چیزی باز است و چه چیزی بسته

جزء	کد منبع
برنامهٔ Android	باز (GPL-3.0)●
برنامهٔ Windows	باز (GPL-3.0)●
برنامهٔ Linux	باز (GPL-3.0)●
برنامهٔ iOS	باز (GPL-3.0)●
پروتکل ColituGecko	بسته؛ کد یکپارچه‌سازی در برنامه‌ها باز است●
صفحهٔ کنترل و عامل گره	بسته●
وب‌سایت	بسته●

14 مقاومت در برابر سانسور

نمی‌توان تضمین کرد که هیچ روش انتقالی در برابر هر سامانهٔ 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.

شیوهٔ مسدودسازی	پاسخ Colitu
مسدود کردن نشانی‌های IP سرور	چند سرور در شبکه‌های مختلف، به‌علاوهٔ یک رله (§17). IP مسدودشده تا زمانی که سرور تغییر کند مسدود می‌ماند.
مسدود کردن درگاه‌ها یا UDP	روش‌های انتقال TCP (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. ColituGecko می‌تواند درون پوسته‌های مختلف (TLS، QUIC، WebSocket) منتقل شود.

شیوهٔ مسدودسازی	پاسخ Colitu
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:

- اندازهٔ 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

- همهٔ سرورها ماشین‌های مجازی اجاره‌ای از چند ارائه‌دهندهٔ میزبانی مستقل هستند. سرورهای VPN در چند کشور پخش شده‌اند؛ فهرست زنده در صفحهٔ سرورها است. صفحهٔ کنترل، که پایگاه دادهٔ 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 نقشهٔ راه است.
- صفحهٔ کنترل و برخی سرورهای VPN از دیوار آتش با پیش‌فرض مسدودسازی استفاده می‌کنند. روی سرورهای VPN دیگر فقط سرویس‌های SSH، VPN و نقطهٔ پایانی اندازه‌گیری گوش می‌دهند؛ دیوار آتش با پیش‌فرض مسدودسازی در همه‌جا در نقشهٔ راه است.
- پایگاه دادهٔ صفحهٔ 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 مسئولانهٔ آسیب‌پذیری

مسائل امنیتی را به‌صورت خصوصی به security@colitu.com گزارش دهید (در /.well-known/security.txt هم آمده است). لطفاً مراحل بازتولید و نسخهٔ 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 برنامهٔ پاداش باگ (colitu.com/bug-bounty)، گزارش‌های تأییدشده‌ای که از حساب کاربری فرستاده شوند بسته به شدت با ۱ تا ۱۲ ماه Plus و آسیب‌پذیری‌های بحرانی با پاداش نقدی جبران می‌شوند.
- 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 مسئولانهٔ آسیب‌پذیری.

این موضوع دربارهٔ پروتکل اختصاصی Colitu، یعنی ColituGecko، نیز صدق می‌کند: Gecko جدید است، کد منبع آن بسته است و هنوز ممیزی رمزنگاری مستقل نداشته است. فعلاً امنیت آن بر بازبینی‌های داخلی Colitu و ویژگی‌های شناخته‌شدهٔ اجزای استاندارد (Noise، X25519، ML-KEM-768، ChaCha20-Poly1305) تکیه دارد.

ممیزی مستقل برنامه‌ریزی شده اما هنوز زمان‌بندی نشده است.

20 محدودیت‌های شناخته‌شده

- هنوز ممیزی امنیتی مستقل وجود ندارد.
- ColituGecko جدید و کد بسته است و هنوز ممیزی رمزنگاری مستقل نداشته است. فعلاً فقط در Android 3.2 و Windows 3.2 و Linux 1.8 و بالاتر در دسترس است.
- 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 نسخهٔ 2.7.0، iOS نسخهٔ 5.6.0 و Linux نسخهٔ 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 همهٔ برنامه‌ها، حل‌کنندهٔ 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؛ گزینهٔ «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).
- نرم‌افزارهای امنیتی که HTTPS را با گواهی ریشهٔ 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.
- برنامهٔ Windows با Authenticode امضا نشده است و ساخت‌های iOS و Linux هنوز بازتولیدپذیر نیستند.
- Shadowsocks 2022 محرمانگی رو به جلو ندارد؛ Trojan نسخهٔ TLS 1.2 را می‌پذیرد.

21 تغییرات در نسخه‌های 1.4 تا 2.0

نسخهٔ 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 جداگانهٔ Windows با قوانین دائمی دیوار آتش است. اگر برنامه یا هستهٔ 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 گزینهٔ اختیاری «مسدود کردن اینترنت بدون VPN» (به‌صورت پیش‌فرض خاموش) ترافیک خارج از تونل را مسدود می‌کند.
- حالت حریم خصوصی (برای نصب‌های جدید به‌صورت پیش‌فرض روشن) به کاربران برنامه‌های Windows و Android و iOS و Linux اجازه می‌دهد تصمیم بگیرند قاعدهٔ 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.

- مسدودکنندهٔ 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، شمارندهٔ روی دستگاه و کلیدهای هر دسته در نقشهٔ راه هستند، نه فعال.
- نسخه‌ها، تاریخ‌ها و مجموع‌های کنترلی در این سند، صفحه‌های دانلود و صفحهٔ متن‌باز اکنون از یک مانیفست انتشار می‌آیند.
- نسخهٔ 1.5 (9 اکتبر 2026): طرح‌های پولی (شخصی، Plus و خانوادگی) در دسترس فروش هستند؛ پرداخت‌ها در صفحهٔ یک ارائه‌دهندهٔ پرداخت انجام می‌شود و اطلاعات کارت هرگز به Colitu نمی‌رسد. این عبارت که طرح‌های پولی ارائه نمی‌شوند حذف شده است. هیچ رویهٔ دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخهٔ 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 ریشهٔ Let's Encrypt (ISRG) و Google Trust Services در هر چهار برنامه. هیچ رویهٔ دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخهٔ 1.7 (16 اکتبر 2026): پشتیبان‌ها. کلید رمزگشایی به حالت آفلاین منتقل شد و دیگر روی سرور ذخیره نمی‌شود. یک نسخهٔ رمزگذاری‌شدهٔ روزانه خارج از محل در Backblaze B2 (EU Central) با قفل حذف 30 روزه نگه داشته می‌شود و حداکثر پس از 36 روز حذف می‌شود. تصاویر لحظه‌ای رمزگذاری‌نشده که پیش از استقرار گرفته می‌شوند پس از 7 روز حذف می‌شوند. Backblaze به فهرست اشخاص ثالث افزوده شد. هیچ رویهٔ دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخهٔ 1.8 (20 اکتبر 2026): ساخت‌های بازتولیدپذیر برای Android (از 2.9.3) و Windows (از 2.9.8). هیچ رویهٔ دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخهٔ 1.9 (28 اکتبر 2026): برنامهٔ پاداش باگ (۱ تا ۱۲ ماه Plus و پاداش نقدی برای آسیب‌پذیری‌های بحرانی) به این سند افزوده شد و جملهٔ مربوط به نبود پاداش مالی حذف شد. گزارش ارزیابی امنیتی داخلی در colitu.com/security-assessment منتشر شد. هیچ رویهٔ دیگر توصیف‌شده در این سند تغییر نکرده است.
- نسخهٔ 2.0 (21 نوامبر 2026): ColituGecko، پروتکل تونل اختصاصی Colitu، به‌عنوان حالت اتصال ششم اضافه شد (Android 3.2 و Windows 3.2 و Linux 1.8 و بالاتر): لایهٔ نشست و رکورد اختصاصی، دست‌دهی ترکیبی Noise NK و ML-KEM-768 و چند مسیر شبکه در یک نشست. این گزاره که Colitu رمزنگاری ابداع نمی‌کند اصلاح شد: Colitu اجزای اولیهٔ رمزنگاری جدید ابداع نمی‌کند، و این دربارهٔ Gecko هم صدق می‌کند. بسته بودن کد Gecko و نبود ممیزی مستقل به محدودیت‌های شناخته‌شده افزوده شد. هیچ رفتار دیگری که در این سند شرح داده شده تغییر نکرد.

22 نقشهٔ راه امنیتی

بعدی (سه‌ماههٔ چهارم 2026)

- حذف خودکار سوابق صورتحساب پس از پایان دورهٔ نگهداری قانونی.
- گزارش‌های دسترسی کوتاه‌تر وب‌سایت بدون نشانی‌های IP کامل.
- دیوار آتش با پیش‌فرض مسدودسازی و به‌روزرسانی‌های امنیتی خودکار روی هر سرور.

- الزامی کردن TLS 1.3 برای Trojan.

بعدتر

- امضای Authenticode برای Windows.
- ساخت‌های بازتولیدپذیر برای iOS و Linux 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 ثبت‌شده در انگلستان و ولز (نشانی ثبتی: 128 City Road, London, United Kingdom, EC1V 2NX؛ شمارهٔ ثبت شرکت 17520342)، و تابع قانون انگلستان و ولز است. پایگاه دادهٔ حساب‌ها روی یک سرور در ترکیه است؛ سرورهای VPN در کشورهای نشان‌داده‌شده در صفحهٔ سرورها هستند و تابع قانون محلی همان‌جا هستند. ما فقط می‌توانیم داده‌ای را که داریم تحویل دهیم؛ §10 همهٔ آن را فهرست می‌کند. درخواست‌هایی که دریافت می‌کنیم در گزارش‌های شفافیت در مرکز اعتماد شمارش می‌شوند.

24 منابع

- پروتکل Hysteria 2: v2.hysteria.network
- Xray-core و REALITY: github.com/XTLS
- sing-box: sing-box.sagernet.org
- Noise Protocol Framework: noiseprotocol.org · ML-KEM: NIST FIPS 203
- ColituGecko: colitu.com/gecko/technical
- TLS 1.3: RFC 8446 · QUIC: RFC 9000 · security.txt: RFC 9116
- Argon2: RFC 9106
- OWASP ASVS و MASVS
- مستندات Android VpnService، Apple Network Extension و Windows Filtering Platform

0
1
Insight