

版本 2.0 · 2026年11月21日

Colitu 安全白皮书

安全架构、威胁模型与隐私设计

使用 Colitu 时你需要信任什么、谁能看到什么、Colitu 能防御哪些攻击又不能防御哪些，以及你如何核实我们的说法。本文的每一项陈述描述的都是目前已经上线的内容。凡是缺失或不够完善之处，我们都会明确说明。

版本	最后更新	安全联系方式
2.0	2026年11月21日	security@colitu.com

适用范围

Android 3.2.2 · Windows 3.2.3 · Linux 1.9.2 (测试版) · iOS 5.10.0 (TestFlight) · 控制平面截至 2026 年 10 月 16 日，节点代理截至 2026 年 10 月 7 日

源代码

Android、Windows 和 Linux 应用：github.com/colitu；iOS 应用：github.com/colitu/ios（均为 GPL-3.0）。服务器软件：闭源。ColituGecko 协议代码为闭源；其在应用中的集成代码为开源。

Colitu 安全一览

以下各节的摘要。绿色：在所列的每个平台上均按所述工作。黄色：部分实现，或存在已说明的限制。红色：尚不可用。

开源应用	● Android、iOS、Windows 和 Linux 应用均为开源（GPL-3.0）。服务器软件为闭源。ColituGecko 协议代码同样闭源；应用中的集成代码开源。
加密隧道	● Hysteria2、VLESS Reality、VLESS XHTTP、Trojan 和 Shadowsocks 2022，使用成熟的实现（Xray-core、sing-box、Hysteria）。Android 3.2、Windows 3.2 和 Linux 1.8 及以上版本还提供 Colitu 自研协议 ColituGecko，采用结合 Noise NK 与 ML-KEM-768 的混合后量子握手。
流量内容与浏览历史	● 不记录。VPN 服务器不保存任何按连接的日志。
按用户统计的流量	● 在每台服务器上按约 15 秒的时间窗口记录，用于配额，保存 90 天，之后只保留各周期的合计。
通过隧道的 DNS	● Android 和 iOS 应用以及 TUN 模式下均通过隧道。在系统代理模式下（Linux 的默认模式；新安装的 Windows 以 TUN 模式启动），代理之外的应用不通过隧道。
IPv6 泄漏防护	● Android 和 iOS 上已阻止；Windows 和 Linux 在 TUN 模式且开启断网保护（kill switch）时已阻止。系统代理模式不在覆盖范围内。
断网保护 (kill switch)	● Windows：独立服务，带持久化防火墙规则；Linux（TUN 模式）：nftables 规则；两者在应用崩溃后仍会继续阻断。Android 依赖系统的“始终开启的 VPN”设置；iOS 有一个可选的“无 VPN 时阻止互联网”开关（默认关闭）。
绕过 VPN 的地区性网站	● 自 Windows 和 Android 2.7.0、iOS 5.6.0 和 Linux 1.3.0 起，新安装默认关闭（隐私模式处于开启状态）；此前的安装保留原有设置。关闭隐私模式后，四个应用中，内置列表上的网站会绕过 VPN，但你连接到该地区的服务器时除外。详见 §9。
用户的两步验证	● 每个账户均可选用（在网站上设置）；四个应用在登录时都会要求输入验证码。管理员账户为强制要求。

通行密钥与会话管理	● 网站支持通行密钥（每个账户最多 10 个）；安全页面列出并可结束浏览器会话；修改密码会结束所有其他会话。应用仍像以前一样使用密码登录。
应用中固定的 API 连接	● 自 2026 年 10 月 10 日的应用版本起，四个应用都为 API 固定（pinning）Let's Encrypt (ISRG) 和 Google Trust Services 根证书颁发机构。限制：§12。
分流	● Windows、Android 和 Linux 支持按应用、网站和 IP 地址分流（按应用分流仅在 Windows 和 Linux 的 TUN 模式下可用）；iOS 支持按网站和 IP 地址分流，因为 iOS 仅对受管理的配置文件允许按应用 VPN。
Colitu Shield（DNS 防护）	● 可选。拦截广告、跟踪器、恶意软件、网络钓鱼、诈骗和加密货币挖矿域名（约 38 万条规则）。其解析器不记录查询日志，也不做统计。
第三方分析	● 任何应用（Android、iOS、Windows、Linux）中均没有。iOS 应用已在 5.4.1 版本中移除。
签名更新	● Android、Windows 和 Linux 使用已签名的更新清单（ECDSA P-256）加 SHA-256；iOS 使用 App Store 签名。
Windows 代码签名 (Authenticode)	● 尚未实现。
可复现构建	● Android 自 2.9.3 起、Windows 自 2.9.8 起：从带标签的源代码构建出的文件与发布文件逐字节一致。iOS 和 Linux 尚未实现。
SBOM	● 每个 Android 和 Windows 的 GitHub 发布版本均提供 SPDX；Linux 尚未提供。
独立安全审计	● 尚未完成。
漏洞披露	● security@colitu.com，政策见 §18 和 security.txt。
自托管	● 不提供。所有服务器均由 Colitu 自行运行。

1 执行摘要

Colitu 是一项 VPN 服务，提供 Android、Windows、Linux 和 iOS 应用。它面向不受信任或不稳定的网络而设计：每台服务器提供多种传输方式，应用会选择在用户网络上可用的一种。

设计目标是让任何单一位置上的敏感数据量保持在较小水平。账户和支付位于控制平面上，而控制平面从不承载 VPN 流量。VPN 服务器承载流量，但不保存电子邮件地址或支付数据。应用使用各平台的安全存储来保存其凭据。

本文档介绍架构、威胁模型、协议、密钥和账户的处理方式、记录哪些日志、更新如何受到保护、已知的限制以及尚待完成的工作。它面向希望核实我们的说法、而不是一味轻信的读者。

原则

- 尽可能少地收集数据，并准确说明我们收集了什么。
- 应用与 VPN 服务器之间的流量使用成熟的协议加密。Colitu 不发明新的密码学原语：自研协议 ColituGecko 也是由成熟的构件（Noise 框架、X25519、ML-KEM-768、AEAD）组合而成。
- 将账户和支付与承载流量的服务器分开。
- 宁可写明已有的限制，也不做笼统的承诺。
- 让应用的行为可以被核查：公开 Android、Windows、Linux 和 iOS 应用的源代码。

> VPN 并不能让你匿名。它只是把信任从你的本地网络和互联网服务商转移到 VPN 运营方。本文档说明这种信任涵盖哪些内容。

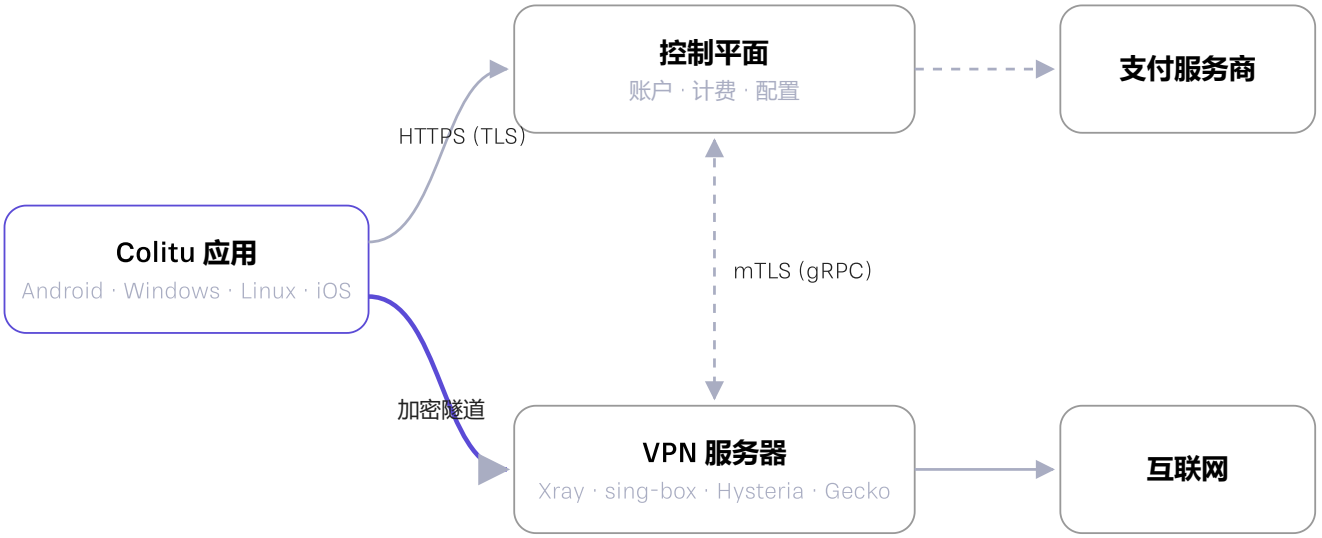
2 范围

涵盖：适用于 Android、Windows、Linux 和 iOS 的 Colitu 应用；控制平面（账户 API、计费、配置、管理面板）；VPN 服务器以及对其进行配置的节点代理；Colitu Shield DNS 服务器；更新分发；colitu.com 及其子域名。

不涵盖：用户操作系统和设备的安全、设备上的浏览器扩展及其他软件、支付服务商以及 §11 中列出的其他第三方的内部安全，以及用户访问的网站。

3 架构

Colitu 将知道用户身份的控制平面与承载其流量的数据平面分开。



控制平面与数据平面。控制平面从不承载 VPN 流量；VPN 服务器不保存电子邮件或支付数据。

组成部分

组件	职责	保存的内容
应用	登录、选择服务器、选择协议及回退、建立隧道、路由和 DNS 设置、在可用时提供断网保护 (kill switch)、检查更新。	会话令牌和当前的连接设置（§12）。
控制平面	账户、登录、订阅与支付、设备注册、生成每台服务器的配置、管理面板、支持。	账户和计费数据（§10）。运行在一台服务器上；数据库无法从互联网访问。
节点代理	运行在每台 VPN 服务器上。通过双向认证的 TLS 获取其配置，启动 VPN 内核，上报按用户的流量计数器和健康状态。	该服务器的协议密钥，以及使用该服务器的用户的连接凭据，以内部用户 ID 标识。不含电子邮件地址。
VPN 服务器（数据平面）	终止加密隧道并将流量转发到互联网。	除代理的数据外没有任何内容。没有流量日志或连接日志（§10）。

组件	职责	保存的内容
DNS	可选的 DNS-over-HTTPS 解析器（AdGuard Home），位于三台 VPN 服务器上，可从隧道内部访问，拦截广告、跟踪器、恶意软件、网络钓鱼、诈骗和加密货币挖矿域名，约 38 万条规则，列表每 24 小时刷新一次。上游解析器为 Cloudflare 和 Quad9（通过 DoH），ECS 已关闭。	没有查询日志，没有统计。

连接是如何建立的

1. 应用通过 HTTPS 登录并获得短期令牌。
2. 它向控制平面请求服务器列表以及所选服务器的连接设置。
3. 它按顺序尝试各种传输方式，并保留第一个通过连通性检查的方式。
4. 之后流量按 应用 → VPN 服务器 → 互联网 的路径传输。控制平面不在该路径上。

4 信任模型

使用 Colitu 时，你必须信任：

- 你安装的 Colitu 应用，以及它所运行的设备和操作系统；
- 你所连接的 VPN 服务器，以及运行它的托管服务商（VPN 服务器是未加密磁盘的租用虚拟机，因此托管服务商在技术上可以访问它们）；
- Colitu 的控制平面以及运营它的人员；
- Colitu 使用的协议实现（Xray-core、sing-box、Hysteria）以及其底层的密码学库；使用 ColituGecko 时，还包括 Colitu 自己的闭源 Gecko 实现。

你无需把隧道内流量的内容或目的地托付给你的本地网络或互联网服务商。他们仍然可以看到：

- 你连接到了 Colitu 服务器，及其 IP 地址和端口；
- 你何时处于连接状态，以及你收发的数据大致有多少；
- 也许还能看出该流量是 VPN 流量，这取决于协议和网络的检测工具；
- 应用有意发送到隧道之外的流量：部分地区性网站（§9）、本地网络流量、更新检查和延迟测量。

你	本地网络 / 互联网服务商	VPN 服务器	网站
	看到你的 IP、服务器的 IP、时间和流量大小	看到你的 IP、目的地和时间；看不到 HTTPS 内容	看到 VPN 服务器的 IP

对于经过隧道的流量，谁能看到什么。

5 威胁模型

Colitu 的设计目标是保护流量，使其免受敌对或不受信任的本地网络、读取或记录你行为的互联网服务商以及多种网络过滤手段的影响。它的设计目标不是针对能够同时观察进出 VPN 流量的对手提供匿名性。

威胁	是否防护?	说明
公共 Wi-Fi 上的窃听	● 是	隧道内的流量在应用与 VPN 服务器之间是加密的。
互联网服务商读取流量内容或目的地	● 是，针对隧道内流量	有意绕过隧道的流量除外（§9）。
互联网服务商察觉到正在使用 VPN	● 有时	Reality、XHTTP 和 Hysteria2 被设计成看起来像普通的 TLS 或 QUIC，但没有任何一种传输方式是不可被检测的。
DNS 泄漏	● 大多数情况	Android、iOS 和 Windows TUN 模式通过隧道解析。Windows 代理模式不覆盖系统解析器。
IPv6 泄漏	● 部分	参见 §9。
隧道中断时的泄漏	● 部分	Windows 和 Linux 有断网保护，应用崩溃后仍会继续阻断（下文有已记录的缺口）；Android 需要系统设置；iOS 有一个可选的“无 VPN 时阻止互联网”开关，默认关闭。
针对账户 API 的中间人攻击	● 是	使用 TLS 和系统证书验证；自 2026 年 10 月 10 日的应用版本起，四个应用还固定了 Let's Encrypt (ISRG) 和 Google Trust Services 根证书颁发机构，因此他人在设备上安装的根证书无法用于读取 API 流量。
恶意或被攻陷的 VPN 服务器	● 否	服务器能看到你的 IP 地址和流量的目的地，但看不到 HTTPS 连接的内容。

威胁	是否防护?	说明
被攻陷的控制平面	🟡 部分	攻击者将获得账户和计费数据，并可向服务器推送配置。流量内容从不在其中。
账户密码被盗	🟡 部分	速率限制会减缓猜测，你也可以让设备退出登录。可选的两步验证（验证器应用）意味着仅凭被盗的密码已无法登录，但在你开启之前它是关闭的。通行密钥是网站上的另一种登录方式；修改密码会结束所有其他会话，通过重置密码找回账户后，24 小时内会锁定账户删除和关闭两步验证。
你设备上的恶意软件	🔴 否	超出任何 VPN 的范围。
浏览器指纹、Cookie、已登录的账户	🔴 否	VPN 改变的是你的 IP 地址，而不是你在网站上的身份。
全局观察者的流量关	🔴 否	时间和流量大小可以在隧道与互联网之间进行匹配

所考虑的对手

类别	示例	Colitu 的防护
A1 本地网络攻击者	同一家咖啡馆 Wi-Fi 上的某个人	对隧道内流量防护较强。
A2 互联网服务商	用户的 ISP 或移动运营商	对内容和目的地防护较强；时间和流量大小仍可被看到。
A3 审查者	使用 DPI 和主动探测的全网络过滤	多种传输方式和自动回退；不作保证（§14）。
A4 恶意的 VPN 服务器或主机	被攻陷的服务器或敌对的托管服务商	有限：能看到与服务器相同的元数据。每台服务器的凭据各自独立，因此无法借助一台服务器访问其他服务器。
A5 被攻陷的控制平面	获得面板访问权限的攻击者	有限：账户数据会暴露；没有可窃取的流量内容或浏览历史。
A6 终端攻击者	用户设备上的恶意软件	无。
A7 全局被动对手	同时观察隧道两端的观察者	无。

6 协议

每台服务器提供同一组传输方式；ColituGecko 目前作为第六种模式在部分服务器上提供。Colitu 不发明新的密码学原语。在五种成熟模式中，加密、认证和密钥交换由 Xray-core、sing-box 和 Hysteria 以及它们所使用的库提供。ColituGecko 的会话与记录层以及握手由 Colitu 自行设计，但由成熟的构件组成：Noise 框架（NK 模式）、X25519 + ML-KEM-768 混合密钥协商，以及 AEAD 记录加密。

传输方式	工作原理	服务器认证	说明与限制
Hysteria2	基于 TLS 1.3 的 QUIC（UDP）	由 Let's Encrypt（ACME）为服务器签发的证书	在丢包网络上速度快。在 UDP 被阻断或限速的地方会失败。
VLESS Reality	TCP；Reality 使用 X25519 密钥执行模仿真实网站的 TLS 1.3 握手	随配置下发的服务器 Reality 公钥	针对 DPI 和主动探测而构建。不能保证不会被按 IP 封锁。
VLESS XHTTP	Reality 加上类 HTTP 的数据流	与 Reality 相同，使用其自己的密钥	适用于会切断长时间 TCP 连接的网络。
Trojan	带 TLS 的 TCP（1.2 或 1.3 版；服务器尚未强制使用 1.3）	与 Hysteria2 使用同一证书	UDP 被阻断时的 TLS 回退方案。
Shadowsocks 2022	2022-blake3-aes-256-gcm（AEAD），每个会话使用新密钥	预共享密钥	轻量快速。没有前向保密：泄漏的密钥可能解密已记录的会话。
ColituGecko（Android 3.2+、Windows 3.2+、Linux 1.8+）	Colitu 自己的会话与加密记录层，承载在 TLS、QUIC 或 WebSocket 等外层 skin 中。一个会话可以使用多条网络路径（grip）；入口服务器和终结会话的出口服务器（anchor）可以是不同的机器	Noise NK 握手：客户端用随配置下发的公钥验证 anchor；X25519 + ML-KEM-768 混合密钥协商。记录使用 ChaCha20-Poly1305 保护	默认使用后量子握手。协议较新且闭源，尚未经过独立的密码学审计。iOS 不提供。

由哪个内核运行某种传输方式取决于平台。Android 和 iOS 对所有传输方式（包括 Hysteria2）都使用 Xray-core。Windows 和 Linux 对 VLESS、Trojan 和 Shadowsocks 使用 Xray-core，对 Hysteria2 使

用 sing-box。在服务器端，Xray 运行 VLESS，sing-box 运行 Trojan 和 Shadowsocks，官方 Hysteria 服务器运行 Hysteria2。在 Android 3.2、Windows 3.2 和 Linux 1.8 及以上版本中，ColituGecko 由 Colitu 自己的 Gecko 客户端运行，服务器端运行 Colitu 自己的 Gecko 软件。Linux 没有协议菜单，Gecko 在 Adaptive Connect 中自动尝试。iOS 不提供 Gecko。

切换传输方式是自动的，但并非无缝：应用切换到另一种传输方式时，隧道会被拆除并重建，这大约需要一秒或更久。ColituGecko 内部的路径切换则不同：一条路径中断时，数据流在同一会话中转到另一条路径，对方未确认的字节会重新发送，隧道不会重建。所有路径都中断时流量暂停；如果在会话过期前恢复到同一 anchor 的路径，可以继续。anchor 本身故障时，已打开的目标连接会关闭。在 Gecko 与其他模式之间切换仍会重建隧道。

> ColituGecko 的详细技术说明：colitu.com/gecko/technical。

7 密码学与密钥管理

用途	机制
应用和网站到 API	TLS 1.2/1.3，使用系统证书验证。自 2026 年 10 月 10 日的应用版本起，Windows、Android、Linux 和 iOS 应用还为 API 固定 Let's Encrypt (ISRG) 和 Google Trust Services 的根密钥。这些固定将于 2027 年 12 月 31 日停止强制执行，因此旧版应用永远不会被拒之门外。
密码存储	Argon2id：64 MiB 内存、3 轮、2 条并行通道、16 字节随机盐、32 字节哈希。密码从不以明文存储。
访问令牌	使用轮换密钥环以 HMAC-SHA256 签名的 JWT，有效期 15 分钟。
刷新令牌	32 个随机字节，仅以 SHA-256 哈希形式存储，有效期 30 天，每次使用后即被替换。重复使用旧令牌会撤销整个令牌族。
控制平面 ↔ VPN 服务器	双向 TLS 1.3 (gRPC)。ECDSA P-256 证书颁发机构；服务器证书有效期 30 天并自动续期；通过指纹允许列表进行吊销。
Reality 密钥	每台服务器的每种传输方式一对 X25519 密钥，在控制平面上生成。
服务器 TLS 证书	Let's Encrypt，在每台服务器上签发；私钥保留在该服务器上。
数据库中的机密	支付、电子邮件和 AI 服务商的凭据使用 AES-256-GCM 加密。
更新清单	ECDSA P-256 签名，由应用对照内置公钥进行验证。

用途	机制
备份	使用 age 加密到一个公钥；制作备份只需要该公钥。解密密钥保存在离线环境，不在任何服务器上。

密钥存放在哪里，以及泄漏会怎样

- 证书颁发机构的私钥是控制平面上的一个文件。任何获得它的人都可以签发服务器身份，因此它是我们持有的最敏感的密钥。
- 每台 VPN 服务器持有自己的 Reality 私钥、TLS 证书密钥，以及使用过它的用户的连接凭据。这些凭据是随机的，并且在每台服务器上都不同，因此一台被攻陷的服务器不会暴露在其他服务器上有效的凭据。
- Reality 私钥和用户的连接凭据以未加密形式存储在控制平面数据库中。对这些值进行数据库级加密已列入路线图。
- 目前还没有定期轮换 Reality 密钥。如果怀疑某台服务器已被攻陷，它会从应用中移除，其密钥和凭据会被更换。
- 控制平面每天制作一份加密备份，并保留 3 天。一份副本会上传到启用 Object Lock 的 Backblaze B2（EU Central，阿姆斯特丹）：30 天内包括 Colitu 在内的任何人都无法删除或更改，最迟 36 天后自动删除。自 2026 年 10 月 16 日起解密密钥保存在离线环境，因此服务器和 Backblaze 都无法读取这些备份。已于 2026 年 10 月 16 日测试从异地副本恢复。部署前制作的数据库快照未加密，在控制平面服务器上最多保留 7 天。

8 账户与会话

- 使用电子邮件和密码登录。电视可以通过显示二维码、由已登录的手机批准来登录（8 位字符代码，有效期 10 分钟）。不支持通过 Google、Telegram 或其他第三方登录。
- 密码至少 10 个字符。新账户只有在确认通过电子邮件发送的 6 位验证码后才能使用 VPN。
- 重置密码使用 6 位验证码，有效期 15 分钟，只能使用一次，最多尝试 5 次。无论该地址是否有账户，返回的结果都相同。重置密码会让所有设备和网页会话退出登录。通过电子邮件验证码重置之后，删除账户和关闭两步验证会被锁定 24 小时（错误码 RECOVERY_LOCKED）。
- 登录、注册、重置密码和优惠码均按 IP 地址进行速率限制。在网站上，登录和重置还按电子邮件地址限制；在应用中，登录仅按 IP 限制。用户账户没有锁定机制。
- 退出登录会撤销该设备的刷新令牌。其访问令牌在过期前仍然有效（最长 15 分钟）。
- 你可以在账户页面移除设备。安全页面列出浏览器会话，包含设备标签（浏览器和操作系统）、国家/地区、登录方式和 IP 地址；你可以关闭一个会话、关闭其他所有会话（当前会话保留），或在所有位置退出登录。

- 在网站上修改密码会保留你当前所在的浏览器会话，并结束所有其他网页会话和所有应用刷新令牌。修改之前签发的应用访问令牌会立即失效（错误码 AUTH_SESSION_REVOKED）。
- 需要再次输入密码的操作（修改密码、删除账户、两步验证变更、通行密钥）限制为每个账户每 15 分钟最多 10 次尝试。
- 两步验证 (TOTP) 对每个账户均为可选。你可以在 colitu.com/account/security 使用验证器应用开启，并会获得 10 个一次性恢复码；之后应用会在输入密码后要求输入验证码（自 Windows 2.6.0, Android 2.6.0, Linux 1.2.0 和 iOS 5.5.0 起支持；较旧的应用会要求你更新）。它只能在网站上设置。
- 通行密钥：在 colitu.com 上，你可以在“账户 → 安全”下添加最多 10 个通行密钥（需要输入密码），为每个命名，并使用密码删除，然后在登录页面使用“使用通行密钥登录”。带用户验证的通行密钥相当于两个因素，因此会跳过两步验证码；但如果从过去 90 天内未出现过的国家/地区登录，仍会要求输入电子邮件验证码。通行密钥不适用于镜像域名。应用仍像以前一样登录，或者在已使用通行密钥登录的浏览器中批准设备关联二维码。
- Colitu 会在以下情况发送安全邮件：新的应用设备（第一台除外）、从新国家/地区登录（90 天内未出现过）、两步验证被开启或关闭、恢复码被重新生成、通行密钥被添加或移除，以及密码被修改。
- 订阅链接：除主链接外，你最多还可以创建 5 个额外的命名链接，每个可选择 7、30 或 90 天的有效期，并可逐个撤销。当某个链接在短时间内从许多不同的网络被使用时，会出现警告。Colitu 不为此存储任何 IP 地址，只保存每天不同网络数量的匿名计数，保留 48 小时。

连接凭据按设备（以及按订阅链接）和按服务器签发。移除设备或轮换订阅链接会从每台服务器删除其凭据：来自它的新连接会在约 15 秒内被拒绝，已打开的连接在关闭时结束。因你的套餐允许的设备数较少而被暂停的设备，也会以同样方式被排除在外，直到你将其重新设为活动状态。如果设备丢失，请同时修改你的密码。

管理员访问

Colitu 由一个非常小的团队运营。管理面板位于单独的地址，采用基于角色的权限，管理端点在公开 API 上已关闭，管理员账户在 5 次失败尝试后锁定 15 分钟，管理员操作会写入审计日志。管理员账户强制要求两步验证 (TOTP)：没有两步验证的管理员只能在登录后设置它，此后的每次登录都需要验证码或一次性恢复码（尝试受速率限制）。管理员还可以注册硬件安全密钥 (WebAuthn)；一旦注册，登录需要密码和该密钥而不是 TOTP，一次性恢复码仍作为有日志记录的紧急后备方案。丢失的密钥通过恢复码替换，或在经过带外身份核实后，由服务器上有日志记录的重置命令替换。通过禁用账户来撤销访问权限，在下一次请求时即生效。管理员会话绑定到其开启时所用的浏览器和网络。

9 流量、DNS、IPv6 与断网保护

VPN 服务器能看到什么

VPN 服务器必须知道把你的流量发往何处，因此在技术上它能看到你的 IP 地址、你所连接网站的 IP 地址以及通常还有主机名 (TLS SNI)，以及你流量的时间和大小。它无法读取 HTTPS 连接的内容，这些内容在你的设备与网站之间保持加密。Colitu 不会解密或检查 HTTPS 流量。

默认路由

	Android	Windows	iOS	Linux（测试版）
流量如何被捕获	系统 VPN（所有应用）	新安装使用 TUN 模式（所有流量）；使用过系统代理模式的安装保持该模式	系统 VPN（所有应用）	默认系统代理；TUN 模式可选
默认不覆盖的内容	本地网络	在系统代理模式下：忽略系统代理的应用、Windows DNS 解析器、浏览器 UDP（QUIC/WebRTC）、IPv6。TUN 模式则覆盖它们。	本地网络	与系统代理模式下的 Windows 相同
地区性网站和 IP（内置列表）	仅当隐私模式关闭时才绕过 VPN，除非服务器位于该地区	仅当隐私模式关闭时才绕过 VPN，除非服务器位于该地区	仅当隐私模式关闭时才绕过 VPN，除非服务器位于该地区	仅当隐私模式关闭时才绕过 VPN，除非服务器位于该地区
DNS	通过隧道发往 1.1.1.1	TUN：通过隧道发往 Cloudflare DNS-over-HTTPS。代理模式：仅针对到达代理的流量。	通过隧道（8.8.8.8 → Xray → 1.1.1.1）	与 Windows 相同
IPv6	● 已阻止	● 在 TUN 模式且开启断网保护时已阻止；系统代理模式不覆盖	● 不会泄漏：被路由进隧道并在那里丢弃	● 与 Windows 相同

	Android	Windows	iOS	Linux（测试版）
断网保护（kill switch）	● 使用 Android 的“始终开启的 VPN”和“阻止没有 VPN 的连接”设置，需要用户自行开启	● 独立的 Windows 服务，带持久化 Windows 筛选平台规则，默认开启（见下文）	● “无 VPN 时阻止互联网”（iOS includeAllNetworks），默认关闭；开启时 Wi-Fi 登录页面无法打开。“始终开启”仅负责重新连接	● nftables 规则，应用崩溃后仍然保留；仅限 TUN 模式
分流	● 应用、网站和 IP 地址	● 应用（仅限 TUN 模式）、网站和 IP 地址	● 仅限网站和 IP 地址（iOS 仅对受管理的配置文件允许按应用 VPN）	● 应用（仅限 TUN 模式）、网站和 IP 地址
多跳与轮换 IP	● 仅限 VLESS	● 仅限 VLESS	● 仅限 VLESS	● 仅限 VLESS

绕过 VPN 的地区性网站

部分地区性网站（内置列表上的域名和 IP 段）会直接打开，绕过隧道，以便拒绝外国 IP 地址的服务仍能正常使用。当你连接到该地区的服务器时，这不适用。对于这类流量，网站和你的互联网服务商看到的是你的真实 IP 地址。该规则仅在隐私模式关闭时适用。新安装默认开启隐私模式（Windows 和 Android 2.7.0、iOS 5.6.0、Linux 1.3.0 及更高版本），因此默认所有流量都经过 VPN；此前的安装保留原有设置。当该规则生效时，你首次连接时应用会显示一次性提示对此进行说明。你也可以选择该地区的服务器。

Windows 断网保护详解

- 它会阻止所有 IPv4 和 IPv6 流量，但回环、本地网络（一项设置，默认开启）、DHCP、VPN 内核、TUN 适配器以及 Colitu 应用本身除外。
- 它在整个会话期间都处于活动状态，无论是 TUN 模式还是系统代理模式。在代理模式下，不使用代理的应用在你连接期间无法访问互联网。
- 这些规则由一项独立的 Windows 服务（ColituKillSwitch，LocalSystem，自动启动）以持久化 Windows 筛选平台规则的形式持有。如果应用或 VPN 内核崩溃，或服务重启，规则仍然保留，互联网保持被阻断，直到 Colitu 重新连接（故障时关闭，fail-closed）。
- 正常的 Windows 重启或关机会结束阻断。这是有意为之：因为那时没有人在场解释为什么互联网被阻断。例外是“自动连接”和“随 Windows 启动”都已开启时；此时阻断会一直保持到 Colitu 重新连接。点

击“断开连接”会结束阻断，卸载会移除所有规则。

- 如果该服务缺失（例如安装损坏之后），应用会提醒你，并回退到较旧的应用内断网保护。其筛选器属于应用的进程：如果应用崩溃或被终止，Windows 会将其移除，流量随即放行（故障时开放，fail-open）。
- 应用直接路由的流量，例如内置列表上的地区性网站，按设计不会被阻断。

应用发送到隧道之外的流量

- 更新检查和更新下载 (colitu.com)。
- 对服务器的延迟测量。
- 在 Windows 上，通过 Cloudflare 或 Google 的 DNS-over-HTTPS 解析服务器主机名。

连通性检查（例如 Google 的 generate_204 地址）通过隧道发送。

10 日志与数据清单

这是 Colitu 所存储内容的完整清单。隐私政策以法律文本的形式包含相同的清单。

VPN 服务

数据	是否存储?	保留期限与用途
你的流量内容	● 从不	—
你访问的网站和 IP 地址	● 不存储	不记录。
你的 DNS 查询	● 不存储	Colitu Shield 的解析器已关闭查询日志和统计。默认情况下，应用使用公共解析器（Cloudflare、Google），它们收到的查询来自 VPN 服务器的 IP 地址，而不是你的。
你在 VPN 服务器上的 IP 地址	● 不存储	仅在内存中用于该连接。
按用户统计的流量	● 已存储	每台服务器上按用户的字节数，以约 15 秒为窗口，保存 90 天用于配额和公平使用；之后只保留每个计费周期的合计。这能显示账户何时活跃以及用了多少，但看不出流量去了哪里。

账户和网站

通行密钥、网页会话和订阅链接包含在下表中。对于订阅链接，不存储任何 IP 地址：每个链接只保留每天不同网络数量的匿名计数，保留 48 小时。

数据	保存期限	用途
电子邮件地址、密码哈希（Argon2id）、语言、账户日期	直到账户被删除；删除时，邮件地址会被占位符替换，密码也将无法再使用	账户与登录
电子邮件验证码和密码重置码（地址、验证码哈希、IP 地址）	7 天	验证电子邮件地址、重置密码
登录事件（IP 地址、国家、浏览器或应用）	180 天	账户安全、防止滥用
注册时和最近一次登录时的 IP 地址与国家	注册：180 天。最近一次登录：若 180 天内没有登录，则会被清除	账户安全、区域性规则
因区域性规则被拒绝的注册与登录（IP 地址、国家）	90 天	执行区域性规则
网页会话（IP 地址、国家、浏览器、登录方式）	会话结束（退出登录、过期或被撤销）30 天后删除	登录、账户页面上的会话列表
应用登录令牌（仅以哈希形式存储，与某台设备绑定）	过期或被撤销 30 天后删除	保持应用处于登录状态
两步验证（加密的验证器密钥、一次性恢复码的哈希、有效期 5 分钟的登录步骤）	密钥和恢复码保留到您关闭该功能或账户被删除为止；登录步骤在过期 1 天后删除	账户安全
通行密钥（公钥、凭据 ID、您设定的名称、签名计数器、创建日期和最近使用日期；私钥和任何生物特征数据从不离开您的设备；有效期 5 分钟的一次性验证请求）	直到您移除该通行密钥或账户被删除；验证请求在 5 分钟后过期并被删除	无密码登录与账户安全
VPN 连接凭据（每台服务器一份，与某台设备或某个订阅链接绑定的随机密钥）	设备或链接使用期间保留；被移除或替换 30 天后删除	VPN 访问

数据	保存期限	用途
订阅链接（您设定的名称、创建日期、最近使用日期和到期日期、“可能被共享”标记；链接本身仅以哈希形式存储）。使用链接的 IP 地址不会被存储；只保留每条链接每天使用过的不同网络数量的匿名近似计数，保留 48 小时	直到您撤销链接或删除账户（过期的链接会自动撤销）；网络数量计数在 48 小时后自动删除	每台设备一条链接，以及共享链接警告
电视登录请求（设备名称、IP 地址、国家）	有效期 10 分钟的验证码过期 1 天后删除	二维码登录
设备（名称、平台、应用和操作系统版本、最近的 IP 地址和国家、硬件标识符的带密钥哈希）	设备在账户中期间保留。已移除设备的名称、IP 地址、国家和硬件哈希在 30 天后清除；180 天未出现的设备的 IP 地址和国家会被清除	设备数量上限、账户安全
被拒绝的设备添加与试用尝试（IP 地址、设备详情）	180 天	设备数量上限、防止滥用
免费套餐与试用的滥用检查（电子邮件地址、硬件 ID 和网络的 HMAC-SHA256 带密钥哈希；密钥不存放在数据库中）	网络：30 天。电子邮件和硬件 ID：账户存在期间，以及账户删除后的 180 天。此项更改之前写入的无密钥 SHA-256 哈希最迟在写入 180 天后删除	防止重复创建免费账户
自动机器人与滥用筛查：对于被暂缓或封禁的账户，记录评分、触发的信号、IP 地址、国家、网络（ASN）和用户代理；对于在账户创建前被拒绝的注册，另记录电子邮件地址	被暂缓或封禁的账户：账户存在期间保留，随账户删除。被拒绝的注册：30 天	防止机器人、脚本注册和服务器地址收集
试用促销码的滥用检查（规范化后的电子邮件地址、设备硬件 ID 和网络——IPv4 /32 与 /24 或 IPv6 /64 与 /48——的 HMAC-SHA256 带密钥哈希；密钥不存放在数据库中）	网络：35 天。电子邮件和硬件 ID：365 天，账户删除后同样保留	每人只能使用一个试用码

数据	保存期限	用途
从原有服务迁移的请求（Telegram ID 和名称、备注、IP 地址）	最后一次变更 30 天后删除。已批准的请求只保留 Telegram ID 的带密钥哈希，保留 2 年	迁移旧订阅；防止同一订阅被迁移两次
注册来源标签（例如“github”、“app:android”），来自网站入口链接中的 utm/ref 标签、引导您来的网站名称（例如 github.com）或应用；不存储 cookie、跟踪像素或网址。首次 VPN 连接的时间。	随账户一同删除	以汇总方式衡量哪些渠道带来真实用户，以及首次连接需要多长时间
您的邀请码；通过邀请链接开通的账户与邀请人账户之间的关联、邀请状态（待定、已获得、无效及原因）以及已赠送的 Premium 天数。邀请人永远看不到被邀请人的姓名或电子邮件。	任一账户被删除时删除	发放邀请奖励；防止滥用（相同的 IP 地址或设备、一次性电子邮件）；以汇总方式衡量通过邀请产生的注册
应用的匿名使用统计：连接结果和失败类型、连接与恢复耗时（以区间计数表示）、意外断开、Adaptive Connect 的协议切换、测得的到服务器的延迟以及自动模式的服务器选择、所用功能和断网保护（kill switch）状态；当前所用网络的类型，以及该网络的国家和互联网服务提供商编号（ASN）（来自 VPN 关闭时收到的签名标签）。服务器只保存按日合计的数据，其中网络（国家 + ASN）和服务器分别存放在不同的表中；不存储账户、设备、IP 地址或所访问的网站。服务器事件还会附带城市级位置：城市在收到报告时根据其 IP 地址推断，地址不会保存；只有当天至少有五台不同设备从该城市报告时才会单独显示该城市（设备按每小时的化名计数，该化名在一小时结束时删除）。可在应用设置中关闭。	合计值无限期保留（无法关联到个人）；含城市的服务器合计保留 90 天	衡量并改进连接质量、Adaptive Connect 和功能使用情况

数据	保存期限	用途
Colitu Passport 保存在您的账户中，并跟随您到每一台登录的设备。按邮票所属国家：解锁时间和碎片数；成就、收藏、每周远征进度、昵称、称号、封面、时区偏移和收藏家编号；每日合计（使用分钟数、碎片、夜间和清晨分钟数，以及当天使用过的国家列表）；当前连续记录（国家、时长和最后计入的分钟）；供应用播放揭晓动画的奖励事件。分钟由我们的服务器根据连接时间计算：只要我们的某台服务器在该分钟内报告了您账户的流量，该分钟即计入（无论设备数量，每分钟最多计一次），国家即该服务器所在的国家；应用无法自行增加分钟。只保存按日和按国家的合计；没有逐分钟或逐会话的记录，也没有网站或 IP 地址。旧版本在设备上已有的进度会按设备导入一次（限制在合理范围内，取较高值）。	每日合计 400 天，奖励事件 30 天，其余数据保留至账户删除	将护照保存到您的账户、在每台设备上显示，并计算奖励和每周远征
Colitu Passport 的可选匿名计数，每天最多一份报告：已解锁的邮票数、已开启的最高篇章、各等级的邮票数、已完成的每周远征、当天获得的碎片，以及当天是否打开过护照。发送时无需身份验证；服务器只把每份报告加入按日合计，不保存报告行、账户、设备或 IP 地址。邮票来自哪些国家、何时获得均不发送。只有旧版应用会发送；新版不再发送，因为护照现在保存在您的账户中（见“Colitu Passport”一行）。此设置默认关闭，可在应用中关闭。	合计值无限期保留（无法关联到个人）	以汇总方式了解护照的使用程度及其规则是否平衡（等级和碎片的进度）
您对应用内问卷的回答：推荐评分（0–10）、如果没有 Colitu 您会有何感受、您未续订 Premium 的原因、可选的评论和平台；您关闭的问卷（30 天内最多询问一次问卷）	账户被删除时，与账户的关联和评论会被移除；只保留匿名评分	以汇总方式衡量满意度（NPS）、产品与市场的契合度以及离开的原因
您对已解决的支持会话给出的 1–5 分评分和可选评论；该会话首次回复和解决的时间	随支持会话一同删除	以汇总方式衡量支持质量（满意度、响应和解决时间）
某台设备在哪台服务器上哪些传输协议可用以及速度如何（不含 IP 地址）	每次报告都会覆盖；最后一次报告 35 天后删除	优先尝试可用的传输协议

数据	保存期限	用途
套餐、付款和订单（包括 Colitu Space 额外空间；金额、支付方式类型、服务商的交易 ID、服务商的通知；通过 Rialit 付款时，与账户绑定的固定付款人编号）	在会计和税法要求的期限内保留，账户删除后同样保留；该期限届满后的自动删除尚未实现	计费、退款、法定义务
Colitu Space 保险库：账户 ID、加密数据的大小、文件数量、创建和修改日期、文件夹结构（哪个项目位于哪个文件夹）、版本数量、收藏标记、旅行模式的结束时间、保险库设置（自动锁定时间）、加密的密钥材料（Argon2id 盐值和参数、由密码和恢复密钥分别包裹的主密钥）以及通行密钥记录。保险库密码不会发送到服务器	直到保险库或 Colitu 账户被删除	提供 Colitu Space：打开保险库、列出文件和文件夹、执行存储上限
您上传到 Colitu Space 的文件、缩略图、文件和文件夹名称、文件信息以及您的个人资料（名称和头像）：在您的浏览器中用您自己的密钥加密；Colitu 看不到内容、名称、个人资料和您的密钥。加密后的数据存放在 Backblaze B2 上 Colitu 的独立账户中	已删除的文件在回收站保留 30 天，之后永久删除；每个文件最多保留 10 个旧版本；删除保险库或文件时，其对象也会通过删除队列从存储中删除；删除保险库或 Colitu 账户时，全部数据都会被删除	以加密形式存储您的文件并将其提供给您
Colitu Space 共享（仅限 Colitu Space 用户之间，端到端加密）：谁与谁共享了什么，连同加密内容一起保存，但无法看到内容；共享日期；如果接收方举报某次共享，则包括举报理由（违法、骚扰、垃圾信息或其他）和可选备注	最迟保留到保险库或 Colitu 账户被删除	提供共享功能；通过审查举报来防止滥用
Colitu Space 文件请求链接：链接所有者填写的公开标签（不加密），以及收到的文件数量和大小。没有账户的人可以通过链接向保险库发送文件，文件在其浏览器中加密。上传者的 IP 地址仅保存在每日大小限制的计数器中，不会写入数据库	标签、文件数量和大小：最迟保留到保险库或 Colitu 账户被删除；上传者的 IP 地址：在计数器中最多 25 小时	提供文件请求功能；通过每日大小限制防止滥用
Colitu Space 紧急访问：保险库所有者选定的紧急访问联系人（另一位 Colitu Space 用户）、等待期（1–30 天）、请求和拒绝的日期，以及用该联系人的密钥密封的主密钥	最迟保留到保险库或 Colitu 账户被删除	在等待期内所有者未拒绝时，让选定的联系人能够访问保险库

数据	保存期限	用途
Colitu Business 企业账户：公司名称、账单邮箱、国家、税号、席位数量及其期限；成员资格（角色、邀请、加入和离开日期、添加该成员的人）；公司发票和公司操作记录。公司的所有者和管理员可以看到每位成员的电子邮件地址和角色，以及其设备的名称、平台、应用版本和最后在线时间；他们看不到流量或访问过的网站	直到 Colitu 关闭该企业账户；公司发票在会计和税法要求的期限内保留；设置密码的链接有效期为 7 天。成员删除自己的账户时，其成员资格会关闭，席位归还给公司	管理公司席位、公司计费、续期提醒
我们向其发送 Colitu Business 合作提议的企业和内容创作者：公司或频道名称、其在网站或频道简介中公开用于商务联系的电子邮件地址、国家和语言；我们发送的邮件及时间；回复的主题和前 300 个字符，以及退信	面板中的发送和回复记录在 12 个月后删除。联系人列表保留至对方要求我们停止联系或不再需要该地址为止；回复“不要再联系我”的地址不会再收到邮件	提供 Colitu Business 代理和白标合作（正当利益；每封邮件都说明如何拒绝并附有本政策链接）
支持会话及附件，包括应用附上的应用日志（地址、网站名称和机密信息已屏蔽）	已关闭的会话：最后一条消息 2 年后删除	支持、处理投诉
安全报告：您提交的漏洞报告文字（标题、描述、步骤、影响）以及与团队的往来消息；如果您希望在名人堂中署名，则包括您选择的名称（连同月份和严重程度公开发布）	直到账户被删除；删除账户时，报告、消息和名人堂条目都会被删除	修复漏洞并发放奖励（可选：在名人堂中署名）
一项自动任务每小时执行这些保留期限，删除账户会立即清除隐私政策所列的数据。仍存在的缺口：套餐、支付和订单记录以及审计日志尚无自动删除，并且在删除之前制作的加密备份最多会保留这些数据 36 天，部署前制作的未加密快照最多保留 7 天。滥用检查哈希使用服务器密钥进行带密钥处理；此变更之前写入的无密钥 SHA-256 哈希在被删除之前仍可被匹配，最迟在写入后 180 天。		
连接报告：支持团队排查连接问题时，您的应用会在下次打开时发送应用与设备信息、连接事件和应用日志；网站名称和地址在设备和服务器上均被屏蔽，不会发送您访问的网站。报告还包含 Adaptive Connect 最近决策的日志（候选服务器、测量、选择及结果、隐藏的服务器、白名单检查）；系统会根据已屏蔽的报告用 AI 为支持团队生成诊断	90 天后删除	解决连接问题（支持）

数据	保存期限	用途
Colitu Bot 对话（文本、IP 地址、“是否有帮助”反馈）	180 天	回答问题
电子邮件投递记录（收件人地址、邮件类型）	90 天	解决投递问题
新闻邮件订阅（电子邮件地址、语言、确认时间）；仅在您通过邮件中的链接确认后	直到您退订；未确认的注册在 7 天后删除	公告、发布说明和优惠邮件（经您同意）
网站和 API 访问日志（IP 地址、请求的地址、浏览器）	14 天	运行和保护本服务
我们网站上的 DNS 泄漏测试	仅在内存中，10 分钟	显示测试结果
审计日志（管理员操作，以及部分账户操作，例如按账户 ID 记录的账户删除）	永久，删除账户后	安全与问责

11 遥测与第三方

应用中的遥测

- 应用（Android、Windows、macOS、Linux）不包含分析、广告或崩溃报告库。Colitu 不会收集使用情况数据，旧版本也从来没有这些库。
- 所有应用都会向 Colitu 报告在哪台服务器上哪些传输方式可用以及速度如何，并与设备关联，以便优先选择可用的传输方式。
- 支持请求会附带最近的应用日志，其中的地址和机密已被屏蔽。

接收数据的第三方

第三方	接收的内容
支付服务商（仅限购买了付费套餐的客户）	订单号、金额、币种、套餐描述和支付方式；银行卡或银行详情在服务商的页面上输入。Colitu 不会发送你的电子邮件或 IP 地址。
Resend（电子邮件）	你的电子邮件地址以及账户邮件的内容（验证码、收据）。
Brevo（电子邮件中继）	从我们的支持邮箱发出的回复。
DeepSeek (Colitu Bot)	机器人对话中的问题和最近几条消息。不会发送账户详情，但你输入的任何内容都会被传递出去。
Have I Been Pwned (Pwned Passwords)	在你注册或设置新密码时：密码 SHA-1 哈希的前 5 个字符，用于对照已知泄漏进行检查。绝不发送密码、其完整哈希、你的电子邮件或 IP 地址。

第三方	接收的内容
Cloudflare	托管 DNS 记录，并代理 docs.colitu.com 和 map.colitu.com。它还提供应用中的默认 DNS 解析器，以及两台服务器上少数域名的出口（§17）。
Backblaze B2（EU Central，阿姆斯特丹）	每日备份的加密副本。它无法读取这些副本：解密密钥保存在离线环境。
托管服务商	运行服务器，并在技术上可以访问它们。

网站不加载任何第三方脚本、字体或跟踪器。

12 应用安全

	Android	Windows	iOS	Linux（测试版）
会话令牌	使用 Android Keystore 密钥的 AES-256-GCM（Keystore 失败时使用软件密钥）	DPAPI（当前用户）	钥匙串（首次解锁后可用）	AES-GCM，密钥派生自机器和用户
连接凭据	已加密（AES-GCM）	明文，存放在仅管理员和 SYSTEM 可读的数据库中	明文文件，位于应用的私有容器中	受保护的文件（0600）
API 证书固定	● 是	● 是（自 2026 年 10 月 10 日起）	● 是（自 2026 年 10 月 10 日起）	● 是（自 2026 年 10 月 10 日起）
权限	具有 VPN 权限的普通应用	始终以管理员身份运行；一项单独的后台服务（ColituKillSwitch，LocalSystem）持有断网保护规则	网络扩展	请求 sudo；密码保存在内存中

	Android	Windows	iOS	Linux（测试版）
本地 VPN 日志	仅警告；无访问日志	仅警告；地址已屏蔽；7 天后删除	仅警告；无访问日志	仅警告
应用数据备份	已禁用	—	钥匙串项目保留在设	—

固定（pinning）意味着他人安装在设备上的根证书无法用于读取应用的 API 流量。因此，通过插入自己的根证书来检查 HTTPS 的安全软件会阻断应用的 API 连接；请在此类软件中将 Colitu 排除在外。

13 更新与供应链

平台	更新如何验证
Android（下载版）	清单使用 ECDSA P-256 签名，并对照内置于应用中的密钥进行检查。APK 必须通过 HTTPS 从 colitu.com 获取，与清单中的 SHA-256 一致，并使用与已安装应用相同的证书签名。旧版本会被拒绝。
Android (Google Play)	通过 Google Play 更新。
Windows	相同的签名清单，从 colitu.com 通过 HTTPS 下载，SHA-256 检查，并由提权的安装程序步骤再次检查。安装程序尚未使用 Authenticode 签名，因此 Windows SmartScreen 可能会发出警告。
Linux	已签名的清单以及软件包的 SHA-256。
iOS	通过 Apple TestFlight 分发；由 Apple 签名并交付更新。

构建与源代码

- 开源应用的每个发布版本都在 GitHub 上打了标签。发布页面列出 SHA-256 校验和以及 SPDX 软件物料清单（Android 和 Windows）。

- Android 和 Windows 仓库运行 CodeQL 代码扫描和 Dependabot 依赖更新；GitHub Actions 固定到提交哈希。
- Android 发布版本在 CI 中构建；Windows 安装程序在开发者的机器上构建；Linux 软件包在 CI 中构建；iOS TestFlight 构建在 Codemagic 上进行。
- Android（自 2.9.3 起）和 Windows（自 2.9.8 起）的构建是可复现的，因此任何人都可以重新构建带标签的源代码，并将结果与发布的文件比对。在 iOS 和 Linux 上，校验和仍然只能证明你拿到的是我们发布的文件，而不能证明它是从带标签的源代码构建的。Android 的 Xray 内核库是通过 SHA-256 固定的官方上游二进制文件，并非从源代码重新构建。

哪些开源，哪些闭源

组件	源代码
Android 应用	🟢 开源 (GPL-3.0)
Windows 应用	🟢 开源 (GPL-3.0)
Linux 应用	🟢 开源 (GPL-3.0)
iOS 应用	🟢 开源 (GPL-3.0)
ColituGecko 协议	🔴 闭源；应用中的集成代码开源
控制平面和节点代理	🔴 闭源
网站	🔴 闭源

14 抗审查能力

没有任何传输方式能保证在所有审查系统面前持续可用。Colitu 的做法是提供多种特性各异的传输方式，并让应用自动回退。

封锁技术	Colitu 如何应对
封锁服务器 IP 地址	位于不同网络的多台服务器，外加一个中继（§17）。被封锁的 IP 在服务器更换之前会一直被封锁。
封锁端口或 UDP	UDP 被阻断时使用 TCP 传输方式（Reality、XHTTP、Trojan）；TCP 受到干扰时使用 Hysteria2。
DNS 污染	应用从 API 获取服务器地址，并在需要时通过加密 DNS 解析它们。

封锁技术	Colitu 如何应对
TLS 指纹识别与主动探测	Reality 会以其所模仿的真实网站的身份来响应探测。
协议指纹识别（DPI）	Reality 和 XHTTP 类似普通 HTTPS；Hysteria2 类似 QUIC。ColituGecko 可以承载在不同的 skin（TLS、QUIC、WebSocket）中。
限速与连接重置	自动回退到另一种传输方式；对会切断长连接的网络使用 XHTTP。

15 隐私方面的限制

VPN 可以对你所在的网络隐藏你的流量，但无法隐藏一切：

- 数据包大小、时间和总流量仍然可见，能够同时看到两端的观察者可以对它们进行匹配。
- 网站仍然可以通过 Cookie、浏览器指纹和你已登录的账户识别你。
- VPN 无法防御恶意软件、网络钓鱼或被攻陷的浏览器。
- 绕过隧道的流量（§9）不受保护。

16 事件响应与事件日志

如果我们怀疑某台 VPN 服务器已被攻陷，我们会将其从应用中隐藏、更换其密钥和连接凭据，并重建它。如果数据泄露涉及个人数据，我们会不无故拖延地向受影响的用户发送电子邮件，并在本节和信任中心公布事件经过。服务状态公开在 status.colitu.com。

17 基础设施

- 所有服务器都是从多家相互独立的托管服务商租用的虚拟机。VPN 服务器分布在多个国家/地区；实时列表见服务器页面。保存账户数据库的控制平面运行在位于土耳其的一台服务器上。
- 磁盘未加密。托管服务商在技术上可以访问其机器。
- 管理访问仅通过 SSH 密钥进行；密码登录已禁用。只有 Colitu 团队持有这些密钥。
- 大多数服务器已启用自动安全更新；在所有服务器上启用已列入路线图。
- 控制平面和部分 VPN 服务器使用默认拒绝的防火墙。在其他 VPN 服务器上，只有 VPN 服务、SSH 和测量端点在监听；在所有服务器上使用默认拒绝的防火墙已列入路线图。
- 控制平面数据库无法从互联网访问。VPN 服务器无法访问它。
- 两台服务器将一小组固定的域名（一台上是 Google 服务，另一台上是 Google 的 AI 服务）通过 Cloudflare WARP 发送，使这些服务看到的是欧洲的位置。对于这些域名，Cloudflare 是出口，看到的元数据与 VPN 服务器相同。

- 一台中继入口服务器将加密数据包原样转发到位于拉脱维亚的出口服务器。入口服务器无法解密流量；它看到你的 IP 地址，与任何网络一样。

18 漏洞披露

请将安全问题私下报告至 security@colitu.com（同时列在 /.well-known/security.txt 中）。请附上复现步骤和受影响的版本。完整政策见 colitu.com/responsible-disclosure。

- 我们会在 3 个工作日内确认收到报告，并在 10 个工作日内给出初步评估。
- 请在公布细节之前，给我们合理的时间来修复问题。
- 对于善意进行的研究，只要避免触及其他用户的数据、不干扰服务并且私下报告，我们不会采取法律行动。
- 我们会按研究人员的意愿署名致谢。通过漏洞赏金计划（colitu.com/bug-bounty），从账户提交并经确认的报告将按严重程度获得 1 至 12 个月的 Plus 奖励，严重漏洞可获得现金奖励。
- 范围内：应用、colitu.com 及其子域名、API 和 VPN 服务器。范围外：拒绝服务、垃圾信息、社会工程以及 §11 中列出的第三方。

19 审计状态

Colitu 尚未接受过独立第三方的安全审计或渗透测试。目前的保障包括：

- Android、Windows、Linux 和 iOS 应用的公开源代码；
- 自动化代码扫描（CodeQL）和依赖更新（Dependabot）；
- 对应用的内部安全审查（2026 年 10 月）以及本文档背后的核实工作；
- 公开的漏洞披露流程。

这同样适用于 Colitu 自研协议 ColituGecko：Gecko 较新，源代码闭源，尚未经过独立的密码学审计。目前其安全性依赖于 Colitu 的内部审查以及标准构件（Noise、X25519、ML-KEM-768、ChaCha20-Poly1305）的已知特性。

独立审计已在计划中，但尚未确定时间。

20 已知限制

- 尚无独立安全审计。
- ColituGecko 较新且闭源，尚未经过独立的密码学审计。目前仅在 Android 3.2、Windows 3.2 和 Linux 1.8 及以上版本中可用。
- VPN 服务器及其托管服务商是你必须信任的一部分；服务器磁盘未加密。
- 当隐私模式关闭时，内置列表上的部分地区性网站在 Windows、Android、iOS 和 Linux 应用中会绕过 VPN。自 Windows 和 Android 2.7.0、iOS 5.6.0 和 Linux 1.3.0 起，新安装默认开启隐私模式，但此前的安装保留原有设置。

- 新安装的 Windows 以 TUN 模式启动，但使用过系统代理模式的安装保持该模式，而代理模式不覆盖所有应用、系统 DNS 解析器或 IPv6。除非将 Colitu 设置为在登录时重新连接，否则正常的 Windows 重启会结束断网保护的阻断。
- Android 自身没有断网保护，需要两项默认关闭的系统设置；iOS 的“无 VPN 时阻止互联网”开关默认关闭，并且在开启时会导致 Wi-Fi 登录页面无法打开。
- 两步验证对管理员账户是强制的，但对用户只是可选的。
- 计费记录和审计日志尚无自动删除（§10）。
- 使用自身根证书检查 HTTPS 的安全软件会因证书固定而阻断应用的 API 连接；必须在其中将 Colitu 排除在外。通行密钥仅适用于 colitu.com：不适用于镜像域名，也不能在应用内使用。
- Windows 应用未使用 Authenticode 签名，iOS 和 Linux 的构建目前尚不可复现。
- Shadowsocks 2022 没有前向保密；Trojan 接受 TLS 1.2。

21 1.4 至 2.0 版的变更

1.3 版描述的是最新应用发布之前的应用状态。本版本描述的是目前已经上线的内容。

- 两步验证 (TOTP) 对每个用户账户开放，而不仅限于管理员。应用在登录时会要求输入验证码。
- Windows：断网保护现在是一项独立的 Windows 服务，带持久化防火墙规则。应用或 VPN 内核崩溃后它仍会继续阻断（不再故障时开放）。除非将 Colitu 设置为在登录时重新连接，否则正常的 Windows 重启仍会结束阻断。新安装以 TUN 模式启动。
- 四个应用都有分流功能：Windows、Android 和 Linux 支持按应用、网站和 IP 地址；iOS 支持按网站和 IP 地址。
- iOS：IPv6 不再泄漏，并新增一个可选的“无 VPN 时阻止互联网”开关（默认关闭），用于阻止隧道之外的流量。
- 隐私模式（新安装默认开启）让 Windows、Android、iOS 和 Linux 应用的用户可以决定是否启用内置的、让部分地区性网站绕过 VPN 的规则。
- 多跳（双重 VPN）和轮换 IP 可用于 VLESS 服务器。
- 自 2026 年 10 月 7 日起，广告拦截器变成了 Colitu Shield，即可选的 DNS 防护，分为五个类别（广告和跟踪器、恶意软件、网络钓鱼、诈骗、加密货币挖矿）。其解析器不保留查询日志，也不做统计，并且不收集任何新数据。可选的成人内容过滤器、个人列表、设备端计数器和按类别开关已列入路线图，尚未上线。
- 本文档、下载页面和开源页面中的版本、日期和校验和现在都来自同一份发布清单。
- 1.5 版（2026 年 10 月 9 日）：付费套餐（个人版、Plus 和家庭版）已开始销售；支付在支付服务商的页面上完成，银行卡信息不会到达 Colitu。此前关于不提供付费套餐的表述已删除。本文档所述的其他做法均未改变。
- 1.6 版（2026 年 10 月 10 日）：网站支持通行密钥、带会话控制的会话列表、安全邮件、重置密码后对删除账户和关闭两步验证实施 24 小时锁定、对密码再次验证尝试次数的限制、带有效期的额外命名订阅

链接、管理员账户可选的硬件安全密钥，以及四个应用中将 API 连接固定到 Let's Encrypt (ISRG) 和 Google Trust Services 根证书颁发机构。本文档所述的其他做法均未改变。

- 1.7 版（2026 年 10 月 16 日）：备份。解密密钥已移到离线环境，不再存放在服务器上。每日加密副本异地保存在 Backblaze B2（EU Central），带有 30 天删除锁定，最迟 36 天后删除。部署前制作的未加密快照 7 天后删除。Backblaze 已加入第三方列表。本文档所述的其他做法均未改变。
- 1.8 版（2026 年 10 月 20 日）：Android（自 2.9.3 起）和 Windows（自 2.9.8 起）的可复现构建。本文档所述的其他做法均未改变。
- 1.9 版（2026 年 10 月 28 日）：本文档加入了漏洞赏金计划（1 至 12 个月 Plus，严重漏洞给予现金奖励），删除了不提供付费赏金的说法。内部安全评估报告已发布于 colitu.com/security-assessment。本文档所述的其他做法均未改变。
- 2.0 版（2026 年 11 月 21 日）：Colitu 自研隧道协议 ColituGecko 作为第六种连接模式加入（Android 3.2、Windows 3.2 和 Linux 1.8 及以上）：自己的会话与记录层、结合 Noise NK 与 ML-KEM-768 的混合握手、一个会话使用多条网络路径。“Colitu 不自创密码学”的说法更正为“不发明新的密码学原语”，以涵盖 Gecko。Gecko 闭源且未经独立审计一事已加入已知限制。本文档描述的其他行为没有变化。

22 安全路线图

接下来（2026 年第四季度）

- 法定保留期限届满后自动删除计费记录。
- 不含完整 IP 地址的更短的网站访问日志。
- 在每台服务器上启用默认拒绝的防火墙和自动安全更新。
- 为 Trojan 强制使用 TLS 1.3。

之后

- Windows 的 Authenticode 签名。
- iOS 和 Linux 的可复现构建，以及所有平台的 SBOM。
- 外部渗透测试和独立审计。
- 用于安全报告的 PGP 密钥以及季度透明度报告。

23 司法管辖

Colitu 由 COLITU LIMITED 运营，该公司在英格兰和威尔士注册（注册地址：128 City Road, London, United Kingdom, EC1V 2NX；公司注册号 17520342），受英格兰和威尔士法律管辖。账户数据库位于土耳其的一台服务器上；VPN 服务器位于服务器页面所示的国家/地区，受所在地法律管辖。我们只能交出我们拥有的数据；§10 列出了全部数据。我们收到的请求会计入信任中心的透明度报告中。

24 参考资料

- Hysteria 2 协议：v2.hysteria.network
- Xray-core 和 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 和 MASVS
- Android VpnService、Apple Network Extension 和 Windows 筛选平台文档

Colitu 安全白皮书 · 版本 2.0 · 2026年11月21日 · security@colitu.com · colitu.com/security

