MULLVAD PRIVACY THREAT MODEL

NAME Mullvad VPN — user perspective

DESCRIPTION Level-0 privacy threat model of a person using the Mullvad VPN app, covering the numbered account, control plane, VPN relays, DNS, destination traffic, payments, updates, diagnostics and support. Assessments are as-is and reflect Mullvad's published policies and audits available in 2024–2026; optional multihop, DAITA, Lockdown mode, split tunneling and custom DNS materially change individual risk.

// ASSESSMENT SUMMARY

EXTREME	12
HIGH	20
MEDIUM	13
LOW	4

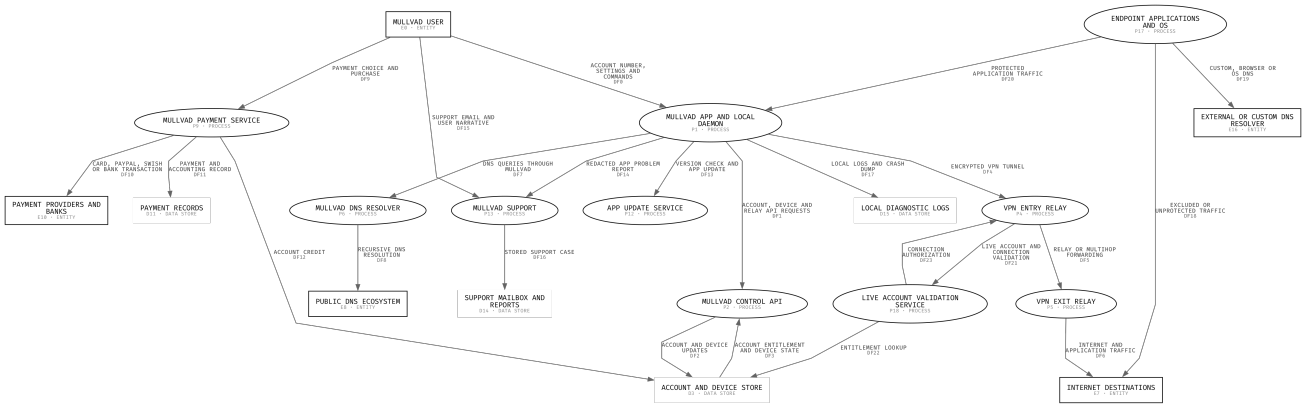
Risk matrix (impact x likelihood)

IMPACT ↓ / LIKELIHOOD →	L	M	H
H	7	10	12
M	1	5	10
L	0	3	1

[L] LINKING 13 [I] IDENTIFYING 7 [NR] NON-REPUDIATION 2 [D] DETECTING 5 [DD] DATA DISCLOSURE 16 [U] UNAWARENESS 4 [NC] NON-COMPLIANCE 2

TOTAL: 54 · open: 49 · mitigated by design: 5 · not applicable: 0

// DATA FLOW DIAGRAM



DF0 · ACCOUNT NUMBER, SETTINGS AND COMMANDS

E0 MULLVAD USER → P1 MULLVAD APP AND LOCAL DAEMON · 3 THREATS

T-01 ONE ACCOUNT NUMBER LINKS DEVICES AND SESSIONS

[L · SOURCE · I:M × L:H → H]

L.1.1 UNIQUE IDENTIFIER

The random 16-digit account number is the user's sole Mullvad identifier and is reused when the same account is entered on up to five devices. Disclosure or deliberate sharing therefore links those devices and their account state even though Mullvad requests no name, email, username or password (https://mullvad.net/en/help/no-logging-data-policy).

// MITIGATION: Mullvad minimizes identity collection and permits users to create fresh numbered accounts. Users needing compartmentalization should use separate accounts and store each number like a password.

T-03 USER MAY MISTAKE PSEUDONYMITY FOR ANONYMITY

[U · SOURCE · I:M × L:M → M]

U.1.1 UNAWARENESS AS DATA SUBJECT

A numbered account avoids direct identity fields but remains a stable pseudonym that can be connected to payment, device, support or network observations. The low-friction login UI does not remove those external linkage paths.

// MITIGATION: Mullvad documents the exact stored account fields and payment consequences. Users should choose payment and support channels consistent with their threat model.

T-02 EXPOSED ACCOUNT NUMBER LINKS UNAUTHORIZED USE

[L · DESTINATION · I:M × L:M → M]

L.1.1 UNIQUE IDENTIFIER

The account number is both identifier and bearer credential. Anyone who obtains it from the app screen, clipboard, storage or correspondence can use the same account, linking their devices and service use to the user's account state (https://mullvad.net/en/help/using-mullvad-vpn-app).

// MITIGATION: Keep the number in an encrypted password manager, never include it in support text, and replace the account when compromise is suspected.

DF1 · ACCOUNT, DEVICE AND RELAY API REQUESTS

P1 MULLVAD APP AND LOCAL DAEMON → P2 MULLVAD CONTROL API · 2 THREATS

T-04 CONTROL API CONTACT REVEALS MULLVAD USE

[D · FLOW · I:M × L:H → H]

D.1 OBSERVED COMMUNICATIONS

The app must contact Mullvad's API for account, device and relay functions, including when no tunnel is established. A local ISP, network censor or endpoint observer can therefore detect contact with Mullvad infrastructure even though request contents use TLS (https://github.com/mullvad/mullvadvpn-app/blob/main/docs/architecture.md).

// MITIGATION: The app supports API access methods and anti-censorship transports, but endpoint and timing observability cannot be eliminated for a direct network observer.

T-05 PRE-TUNNEL API LINKS SOURCE IP TO ACCOUNT

[L · DESTINATION · I:H × L:M → H]

L.2.1.1 QUASI-IDENTIFIER COMBINING DATA OF A SINGLE INDIVIDUAL

When an authenticated account/device request occurs before the VPN is up, the receiving service necessarily handles the ordinary source IP while processing a stable account or device reference. Mullvad states it does not log IP addresses or account activity, but live co-observation remains technically possible (https://mullvad.net/en/help/no-logging-data-policy).

// MITIGATION: No source-IP or connection logging, short web logs without IPs, RAM-only validation state, and optional API access obfuscation reduce persistence and detectability.

DF2 · ACCOUNT AND DEVICE UPDATES

P2 MULLVAD CONTROL API → D3 ACCOUNT AND DEVICE STORE · 3 THREATS

T-08 ACCOUNT PSEUDONYM CAN BECOME IDENTIFYING

[I · FLOW · I:H × L:M → H]

I.2.1.1 IDENTIFIER

The account number is a pseudonym. Conventional payment records, a bank-wire message, a support disclosure or a captured device can map it to a person, turning otherwise pseudonymous device state into identified information.

// MITIGATION: Use cash or an anonymously purchased voucher, avoid entering the account number in correspondence, and separate accounts for separate identities.

T-06 ACCOUNT STORE LINKS ACCOUNT TO DEVICE KEYS

[L · DESTINATION · I:M × L:H → H]

L.1.1 UNIQUE IDENTIFIER

Mullvad documents storage of account number and expiry plus WireGuard public key and tunnel address where used. These stable identifiers link all registered devices to the numbered account even without civil identity (https://mullvad.net/en/help/no-logging-data-policy).

// MITIGATION: The records contain no required name or email, and device keys/tunnel addresses can be replaced by removing and re-adding devices.

T-07 ACCOUNT-STORE COMPROMISE EXPOSES PSEUDONYMOUS USERS

[DD · DESTINATION · I:H × L:L → M]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

Unauthorized access to account and device records would disclose account numbers, expiry, public keys and tunnel addresses. Correlation with payment records, seized devices or live network observations could then identify or profile users.

// MITIGATION: Data minimization, no activity history, and independently audited infrastructure limit the value of the store; they do not make the required account store non-sensitive.

DF3 · ACCOUNT ENTITLEMENT AND DEVICE STATE

D3 ACCOUNT AND DEVICE STORE → P2 MULLVAD CONTROL API · 1 THREATS

T-09 ACCOUNT VALIDITY CAN BE DETECTED

[D · DESTINATION · I:L × L:M → L]

D.3 SYSTEM RESPONSES

Login and device-management responses necessarily distinguish usable, expired, invalid and connection-limited accounts. Possession of a candidate number can therefore reveal account existence and state.

// MITIGATION: Random 16-digit numbers provide a large search space; rate limiting and uniform unauthenticated errors should be maintained.

DF4 · ENCRYPTED VPN TUNNEL

P1 MULLVAD APP AND LOCAL DAEMON → P4 VPN ENTRY RELAY · 6 THREATS

T-11 ISP AND LOCAL NETWORK DETECT VPN USE

[D · FLOW · I:M × L:H → H]

D.1 OBSERVED COMMUNICATIONS

A direct WireGuard connection goes to recognizable Mullvad relay addresses and exposes connection timing and volume to the user’s ISP or local network. Encryption hides payloads, not the existence of communication.

// MITIGATION: Mullvad provides anti-censorship/obfuscation options, but direct endpoint detection remains likely unless an appropriate transport is enabled.

T-13 TUNNEL PATTERNS PROFILE USER ACTIVITY

[L · FLOW · I:H × L:M → H]

L.2.2.1 PROFILING AN INDIVIDUAL

Packet size, timing and volume can support website fingerprinting and correlation even though the tunnel content is encrypted. X41’s 2024 audit described MTU/timing manipulation and traffic-correlation heuristics (https://github.com/mullvad/mullvadvpn-app/blob/main/audits/2024-12-10-X41-D-Sec.md).

// MITIGATION: Enable DAITA and multihop for sensitive use. These raise cost but do not guarantee anonymity against a global observer.

T-15 HOSTING AND TRANSIT PROVIDERS OBSERVE METADATA

[DD · FLOW · I:H × L:M → H]

DD.3.3 IMPLICIT DATA DISCLOSURE

Data-center and transit networks can observe incoming encrypted packet metadata such as source/destination addresses, timing and volume even when they lack login access to the relay. Mullvad itself warns that provider-side monitoring can support correlation (https://mullvad.net/en/help/multihop-wireguard).

// MITIGATION: Filter relay selection by ownership/provider and use multihop with different providers and jurisdictions.

T-12 ENTRY RELAY OBSERVES THE REAL SOURCE IP

[I · DESTINATION · I:H × L:H → E]

I.2.1.1 IDENTIFIER

The first VPN relay necessarily handles the user's public source IP and a WireGuard peer/tunnel identifier while the session is active. In single-hop operation the same host also forwards destination-side traffic.

// MITIGATION: Mullvad states that relays keep no IP or connection logs, run from RAM, and use dedicated servers; multihop separates source-side and destination-side views.

T-48 NO-LOGS ASSURANCE IS POINT-IN-TIME AND SCOPED

[NC · DESTINATION · I:H × L:L → M]

Nc.3 INSUFFICIENT CYBERSECURITY RISK MANAGEMENT

Privacy depends on continuing operational enforcement across Mullvad, administrators, rented hosts and software releases. Cure53's June 2024 relay audit was positive but tested two staging relays; X41's 2024 app audit found six vulnerabilities before fixes.

// MITIGATION: Open source, repeated independent audits, RAM-only relays, published findings/fixes and transparent incident reporting provide strong assurance, but users with exceptional risk should reassess current audits and releases periodically.

T-14 RELAY LOGS WOULD MAKE SESSIONS ATTRIBUTABLE

[NR · DESTINATION · I:H × L:L → M · MITIGATED]

Nr.1.3 METADATA

Source-IP, account and timestamp logs at the entry relay would provide evidence that a person used Mullvad at a particular time. Mullvad's published policy prohibits these logs, and its RAM-only relays have no persistent storage.

// MITIGATION: No activity, DNS, IP, connection or per-user bandwidth logs; RAM-only deployment; repeated independent audits; and the 18 April 2023 search-warrant outcome.

DF5 · RELAY OR MULTIHOP FORWARDING

P4 VPN ENTRY RELAY → P5 VPN EXIT RELAY · 2 THREATS

T-16 ENTRY AND EXIT TRAFFIC CAN BE CORRELATED

[L · FLOW · I:H × L:M → H]

L.2.2.1 PROFILING AN INDIVIDUAL

An observer with visibility near both sides can match timing and volume between entry and exit. A single-hop relay collapses both views onto one host; multihop only raises the observation cost.

// MITIGATION: Use multihop across different hosting providers and countries plus DAITA. For a global passive adversary, a VPN alone is not a complete anonymity system.

T-17 COMPROMISED RELAY CAN INSPECT LIVE TRAFFIC

[DD · DESTINATION · I:H × L:L → M]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

RAM-only operation prevents durable disk evidence but does not prevent a compromised runtime or privileged administrator from capturing live metadata or plaintext leaving the exit. The 2023 infrastructure audit noted that production administrators could technically tap traffic.

// MITIGATION: Dedicated controlled servers, access controls, audit logging, reduced administrative access, app-layer TLS and independent infrastructure audits reduce but do not eliminate live compromise risk.

DF6 · INTERNET AND APPLICATION TRAFFIC

P5 VPN EXIT RELAY → E7 INTERNET DESTINATIONS · 4 THREATS

T-18 EXIT RELAY SEES DESTINATIONS AND PLAINTEXT

[DD · SOURCE · I:H × L:M → H]

DD.3.3 IMPLICIT DATA DISCLOSURE

The exit relay handles destination IPs, ports, timing and volume and can read application payloads not protected end-to-end. This exposure is inherent to VPN egress, regardless of relay logging policy.

// MITIGATION: Use HTTPS/TLS or another end-to-end encrypted protocol. Mullvad states it records no traffic or DNS content.

T-21 SHARED EXIT TRAFFIC REMAINS LINKABLE

[L · FLOW · I:M × L:H → H]

L.2.1.1 QUASI-IDENTIFIER COMBINING DATA OF A SINGLE INDIVIDUAL

Cookies, browser fingerprints, authentication tokens and timing can link multiple requests made through changing or shared exit addresses. Shared IP addresses prevent simple IP attribution but do not break application identifiers.

// MITIGATION: Use privacy-hardened applications and fresh identities; Mullvad cannot remove identifiers embedded above the network layer.

T-19 DESTINATION LOGIN RE-IDENTIFIES THE USER

[I · DESTINATION · I:H × L:H → E]

I.1.1 PROCESSING OF IDENTIFIED DATA

Logging into a personal website account, sending identifying content or accepting persistent application trackers identifies the user to that destination regardless of the VPN exit IP.

// MITIGATION: Separate browser profiles and identities, minimize trackers, and do not treat a changed IP address as application-layer anonymity.

T-20 DESTINATION RECORDS MAKE ACTIONS ATTRIBUTABLE

[NR · DESTINATION · I:M × L:H → H]

Nr.2 ATTRIBUTABLE ACTION SIDE-EFFECT EVIDENCE

Destination services may retain account events, cookies, request contents and timestamps. Those records can prove user actions even though they show a shared Mullvad exit address rather than the user's residential address.

// MITIGATION: This is outside Mullvad's control; users must rely on destination privacy controls and avoid identified sessions when deniability matters.

DF7 · DNS QUERIES THROUGH MULLVAD

P1 MULLVAD APP AND LOCAL DAEMON → P6 MULLVAD DNS RESOLVER · 2 THREATS

T-22 DNS QUERIES REVEAL BROWSING INTERESTS

[DD · DESTINATION · I:H × L:H → E]

DD.3.3 IMPLICIT DATA DISCLOSURE

The Mullvad resolver necessarily handles queried domain names during resolution, which can reveal health, political, sexual or other sensitive interests. The privacy benefit depends on the stated no-DNS-log policy.

// MITIGATION: Mullvad routes app DNS through its resolver and states that it keeps no DNS request logs (https://mullvad.net/en/help/no-logging-data-policy).

T-24 MULLVAD DOES NOT RETAIN DNS HISTORY

[NR · DESTINATION · I:H × L:L → M · MITIGATED]

Nr.1.1 DATA

A retained query history would make domains attributable to sessions or accounts. Mullvad's no-logging policy explicitly excludes DNS request logging.

// MITIGATION: No DNS request logs are stored; this does not cover leaks to an ISP or a user-selected external resolver.

DF8 · RECURSIVE DNS RESOLUTION

P6 MULLVAD DNS RESOLVER → E8 PUBLIC DNS ECOSYSTEM · 1 THREATS

T-25 AUTHORITATIVE DNS PARTIES PROFILE RESOLVER TRAFFIC

[L · DESTINATION · I:L × L:M → L]

L.2.2.1 PROFILING AN INDIVIDUAL

Authoritative servers and upstream DNS infrastructure can profile aggregate queries originating from Mullvad's resolver. They generally see the resolver rather than the individual user, but rare names and timing may reduce the anonymity set.

// MITIGATION: Recursive resolution separates the user's source IP from authoritative DNS. Query minimization, caching and broad shared use further reduce individual linkage.

DF9 · PAYMENT CHOICE AND PURCHASE

E0 MULLVAD USER → P9 MULLVAD PAYMENT SERVICE · 1 THREATS

T-28 USERS MAY NOT DISTINGUISH PAYMENT PRIVACY LEVELS

[U · SOURCE · I:M × L:M → M]

U.1.1 UNAWARENESS AS DATA SUBJECT

All payment options buy the same service but expose very different identifiers and retention. Bitcoin and Bitcoin Cash are public-chain payments, a reseller can know the purchaser, and bank wire may place the account number in the message.

// MITIGATION: Mullvad publishes method-specific fields and retention. Payment UI should continue to make identity and third-party consequences prominent before purchase.

DF10 · CARD, PAYPAL, SWISH OR BANK TRANSACTION

P9 MULLVAD PAYMENT SERVICE → E10 PAYMENT PROVIDERS AND BANKS · 4 THREATS

T-27 PAYMENT RAILS COLLECT UNNECESSARY IDENTITY FOR VPN USE

[DD · FLOW · I:H × L:H → E]

DD.1.1 DATA TYPE SENSITIVITY

Billing names, addresses, bank accounts, phone numbers and email addresses are not functionally necessary to route VPN traffic but are required or collected by conventional payment rails and accounting rules.

// MITIGATION: Mullvad offers multiple lower-data payment methods and does not require a subscription or email account.

T-26 PAYMENT PROVIDER DIRECTLY IDENTIFIES THE BUYER

[I · DESTINATION · I:H × L:H → E]

I.1.1 PROCESSING OF IDENTIFIED DATA

Card, PayPal, Swish and bank wire process direct identifiers. Mullvad lists sender name/address/account, PayPal name/email/country, Swish name/phone and Stripe card metadata among accessible data (https://mullvad.net/en/help/privacy-policy).

// MITIGATION: Choose carefully handled cash, Monero, or an anonymously purchased voucher when purchase identity is outside the acceptable threat model.

T-29 PROCESSOR LINKS LEGAL IDENTITY TO MULLVAD PURCHASE

[L · DESTINATION · I:H × L:H → E]

L.2.1.1 QUASI-IDENTIFIER COMBINING DATA OF A SINGLE INDIVIDUAL

Stripe, PayPal and SEB/Swish can link a named customer, amount and time to a Mullvad purchase. Mullvad states that these companies log everything; their records are outside the VPN no-activity-log scope.

// MITIGATION: Payment processors normally receive a temporary token rather than the Mullvad account number. Avoid bank wire and identifying rails when purchase linkage matters.

T-30 FINANCIAL RECORDS DEFEAT PURCHASE DENIABILITY

[NR · DESTINATION · I:M × L:H → H]

Nr.1.3 METADATA

Bank and processor receipts create durable metadata proving that the payer purchased Mullvad service, even when they do not prove who later used the numbered account.

// MITIGATION: Cash without sender details or an anonymously purchased voucher offers stronger purchase deniability; public-chain cryptocurrency still leaves transaction evidence.

DF11 · PAYMENT AND ACCOUNTING RECORD

P9 MULLVAD PAYMENT SERVICE → D11 PAYMENT RECORDS · 2 THREATS

T-31 ACCOUNTING RETENTION PRESERVES PAYMENT LINKAGE

[DD · DESTINATION · I:H × L:H → E]

DD.3.4 DURATION/RETENTION

Mullvad generally deletes transaction IDs and precise timestamp portions after 20 days, but Swedish accounting obligations require some payment data for seven years from the end of the fiscal year. The remaining record outlives the VPN session by design.

// MITIGATION: Method-specific minimization and deletion are documented; statutory records cannot be erased on ordinary user request while retention law applies.

T-32 PAYMENT-STORE BREACH EXPOSES BUYERS

[DD · DESTINATION · I:H × L:L → M]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

Unauthorized access to payment and accounting records could disclose account references, payment method, amount, date and method-specific identifiers, enabling identity linkage despite the absence of VPN activity logs.

// MITIGATION: Separate payment tokens, 20-day deletion of high-resolution linkage fields, access controls and anonymous payment alternatives reduce exposure.

DF12 · ACCOUNT CREDIT

P9 MULLVAD PAYMENT SERVICE → D3 ACCOUNT AND DEVICE STORE · 1 THREATS

T-33 CREDIT TIMING LINKS PAYMENT TO ACCOUNT

[L · FLOW · I:H × L:M → H]

L.2.1.1 QUASI-IDENTIFIER COMBINING DATA OF A SINGLE INDIVIDUAL

The account-credit event links a payment or temporary token to a numbered account. During the documented token window, internal records or correlated timestamps can connect an identifying payment to that account; bank wire can expose the account number directly.

// MITIGATION: Most processor-linking tokens and transaction details expire after 20 days and processors normally do not receive the account number. Exceptions include unaccounted cash tokens retained for 120 days and Monero transaction hashes retained longer to prevent double-crediting.

DF13 · VERSION CHECK AND APP UPDATE

P1 MULLVAD APP AND LOCAL DAEMON → P12 APP UPDATE SERVICE · 4 THREATS

T-34 UPDATE CHECK FINGERPRINTS APP AND PLATFORM

[L · FLOW · I:L × L:M → L]

L.2.1.1 QUASI-IDENTIFIER COMBINING DATA OF A SINGLE INDIVIDUAL

The app sends its version and a coarse platform version about once per 24 hours. Combined with request time and source network metadata, uncommon versions may narrow a user population even though no account or device identifier is sent (https://github.com/mullvad/mullvadvpn-app/blob/main/docs/logging-and-telemetry.md).

// MITIGATION: Mullvad retains only aggregate version counters and excludes account/device identifiers from the update request.

T-35 UPDATE CONTACT REVEALS MULLVAD INSTALLATION

[D · FLOW · I:M × L:H → H]

D.1 OBSERVED COMMUNICATIONS

A network observer can detect periodic communication with Mullvad’s update service, including before the tunnel exists. This can expose installation or continued use in environments where VPN software is sensitive.

// MITIGATION: Route checks through the tunnel where available and use anti-censorship transports; endpoint contact remains observable to sufficiently positioned parties.

T-36 COMPROMISED UPDATE CHAIN DEFEATS VPN PRIVACY

[NC · DESTINATION · I:H × L:L → M]

Nc.3 INSUFFICIENT CYBERSECURITY RISK MANAGEMENT

A compromised build, signing key, update service, phishing site or stale vulnerable client could install privileged code able to read account secrets, traffic and local data. Signature verification reduces distribution risk but does not eliminate upstream build or key compromise.

// MITIGATION: Mullvad uses signed and verified packages, publishes its signing fingerprint and source code, commissions independent audits, and prompts users to update.

T-54 FIXED WINDOWS INSTALLER FLAW WAS REMEDIATED

[NC · DESTINATION · I:H × L:L → M · MITIGATED]

Nc.3 INSUFFICIENT CYBERSECURITY RISK MANAGEMENT

X41 found that the Windows installer could execute an adjacent malicious taskkill.exe with administrator privileges. Mullvad fixed the issue in version 2024.8 and the remediation was retested in the 2024 audit.

// MITIGATION: Use version 2024.8 or later and obtain installers through the verified in-app or official signed distribution path.

DF14 · REDACTED APP PROBLEM REPORT

P1 MULLVAD APP AND LOCAL DAEMON → P13 MULLVAD SUPPORT · 2 THREATS

T-37 PROBLEM REPORT MAY CONTAIN REVEALING FREE TEXT

[I · SOURCE · I:M × L:M → M]

I.2.2 REVEALING ATTRIBUTES

Automated redaction cannot remove identity or sensitive context that the user voluntarily types into a problem description. App/OS versions and unusual error details can also form a quasi-identifier.

// MITIGATION: The report is opt-in, can be reviewed before sending, needs no email if no reply is wanted, and documented redaction removes account-like numbers, IP/MAC addresses, UUIDs and home paths.

T-38 AUTOMATIC TELEMETRY IS NOT SENT

[U · SOURCE · I:M × L:L → L · MITIGATED]

U.1.1 UNAWARENESS AS DATA SUBJECT

Silent crash or usage telemetry would process data without a deliberate user action. Mullvad documents that local logs and Windows crash dumps are never automatically sent; submitting a report is manual and inspectable.

// MITIGATION: No automatic diagnostic upload; manual opt-in; report preview; redaction; certificate-pinned TLS.

DF15 · SUPPORT EMAIL AND USER NARRATIVE

E0 MULLVAD USER → P13 MULLVAD SUPPORT · 2 THREATS

T-39 SUPPORT EMAIL DIRECTLY IDENTIFIES THE USER

[I · SOURCE · I:M × L:H → H]

I.1.1 PROCESSING OF IDENTIFIED DATA

Ordinary support email exposes the sender address and any name, account number, location or narrative they include to Mullvad and its email service provider. Mullvad warns that plain email is not safe for sensitive communication.

// MITIGATION: Use the in-app report without an email when no reply is needed, omit account/PII, or use Mullvad’s published PGP procedure.

T-40 EMAIL PROPAGATES DATA TO A SERVICE PROVIDER

[DD · FLOW · I:M × L:H → H]

DD.3.2 PROPAGATION

Support correspondence is processed by a third-party email supplier acting for Mullvad. Plain email also traverses mail infrastructure outside the VPN service's relay and no-activity-log guarantees (https://mullvad.net/en/help/privacy-policy).

// MITIGATION: PGP protects message content; users can avoid email entirely for reports that do not require a response.

DF16 · STORED SUPPORT CASE

P13 MULLVAD SUPPORT → D14 SUPPORT MAILBOX AND REPORTS · 1 THREATS

T-41 SUPPORT CASES PERSIST FOR UP TO 70 DAYS

[DD · DESTINATION · I:M × L:M → M]

DD.3.4 DURATION/RETENTION

Closed support emails and problem reports are archived and automatically erased after 70 days. During that period, their identifiers, narrative and diagnostics remain accessible for support purposes.

// MITIGATION: Automatic permanent deletion after 70 days bounds retention; users should still minimize what they submit.

DF17 · LOCAL LOGS AND CRASH DUMP

P1 MULLVAD APP AND LOCAL DAEMON → D15 LOCAL DIAGNOSTIC LOGS · 1 THREATS

T-42 LOCAL COMPROMISE EXPOSES DIAGNOSTIC ARTIFACTS

[DD · DESTINATION · I:M × L:L → L]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

Local logs and the Windows crash dump remain on the device until removed and are not automatically uploaded. Malware or a person with sufficient filesystem access can inspect those artifacts for app state and operational details (https://github.com/mullvad/mullvadvpn-app/blob/main/docs/logging-and-telemetry.md).

// MITIGATION: Logs exclude account numbers and key material and redact sensitive fields for reports. Use full-disk encryption, trusted local accounts and normal device access controls.

DF18 · EXCLUDED OR UNPROTECTED TRAFFIC

P17 ENDPOINT APPLICATIONS AND OS → E7 INTERNET DESTINATIONS · 3 THREATS

T-44 DISCONNECT AND QUIT CAN SILENTLY END PROTECTION

[U · SOURCE · I:H × L:M → H]

U.1.1 UNAWARENESS AS DATA SUBJECT

The built-in kill switch blocks accidental failures only while connecting or connected. Without optional Lockdown mode, a deliberate Disconnect or Quit restores ordinary networking, which users may confuse with permanent kill-switch protection.

// MITIGATION: Enable Lockdown mode, auto-connect and launch-on-startup when all traffic must remain protected; keep the app's connection status visible.

T-43 SPLIT TUNNELING EXPOSES THE REAL IP

[DD · FLOW · I:H × L:H → E]

DD.3.3 IMPLICIT DATA DISCLOSURE

An excluded application deliberately bypasses the VPN and sends traffic from the user's ordinary address. Mullvad documents Windows cases where installers or child applications launched by an excluded process can inherit exclusion unexpectedly (https://mullvad.net/en/help/split-tunneling-with-the-mullvad-app).

// MITIGATION: Avoid split tunneling for sensitive sessions, review exclusions, launch sensitive child processes separately, and verify the observed address with Connection Check.

T-45 DESTINATION IDENTIFIES BYPASSED APPLICATIONS

[I · DESTINATION · I:H × L:H → E]

I.2.1.1 IDENTIFIER

A destination receiving excluded or post-disconnect traffic sees the user's ordinary public IP and can connect it with cookies or accounts previously used through the VPN.

// MITIGATION: Do not mix identified and compartmentalized activity; disable exclusions and use Lockdown mode where real-IP disclosure is unacceptable.

DF19 · CUSTOM, BROWSER OR OS DNS

P17 ENDPOINT APPLICATIONS AND OS → E16 EXTERNAL OR CUSTOM DNS RESOLVER · 3 THREATS

T-47 DNS BYPASS IS EASY TO OVERLOOK

[U · SOURCE · I:H × L:M → H]

U.1.1 UNAWARENESS AS DATA SUBJECT

Browser Secure DNS, Android Private DNS and security products can override the DNS path independently of the Mullvad app. Users may believe all names use Mullvad merely because the VPN status is green.

// MITIGATION: Mullvad documents common bypass causes and provides Connection Check. Test each browser/device configuration after changes.

T-23 ANDROID TUNNEL CHANGES CAN LEAK DNS

[DD · FLOW · I:H × L:M → H]

DD.3.3 IMPLICIT DATA DISCLOSURE

Mullvad disclosed on 3 May 2024 that Android could emit plaintext DNS during tunnel reconfiguration or app force-stop/crash, including with Always-on VPN and blocking enabled (CVE-2024-34446). Queried domains and the user's ordinary network location may reach the ISP resolver.

// MITIGATION: Keep app and OS updated, avoid relay changes during sensitive activity, test for leaks, and avoid Android where this platform residual exceeds the user's risk tolerance.

T-46 CUSTOM RESOLVER RECEIVES BROWSING INTERESTS

[DD · DESTINATION · I:H × L:H → E]

DD.3.2 PROPAGATION

Enabling custom DNS or application/browser DoH moves queried domains to an external resolver with its own logging, jurisdiction and identity linkage. The resolver may receive a direct source IP or a Mullvad exit IP depending on routing.

// MITIGATION: Keep Mullvad's default DNS unless a separately trusted resolver is an explicit requirement; disable unintended browser Secure DNS/DoH and Android Private DNS.

DF20 · PROTECTED APPLICATION TRAFFIC

P17 ENDPOINT APPLICATIONS AND OS → P1 MULLVAD APP AND LOCAL DAEMON · 1 THREATS

T-49 PROTECTED APPS ENTRUST ALL TRAFFIC TO THE DAEMON

[DD · DESTINATION · I:H × L:L → M]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

Endpoint applications hand DNS and application traffic to a privileged local daemon that controls routing and tunnel enforcement. A compromised or outdated daemon could observe plaintext before encryption or misroute it outside the tunnel.

// MITIGATION: The app is open source, uses platform firewall controls, is independently audited, and includes an always-on connection-failure kill switch. Keep it updated and protect the endpoint from local compromise.

DF21 · LIVE ACCOUNT AND CONNECTION VALIDATION

P4 VPN ENTRY RELAY → P18 LIVE ACCOUNT VALIDATION SERVICE · 3 THREATS

T-50 LIVE VALIDATION LINKS ACCOUNT TO AN ACTIVE RELAY

[L · FLOW · I:H × L:H → E]

L.1.1 UNIQUE IDENTIFIER

When a customer connects, the VPN server asks a central service to validate the numbered account, remaining time and connection limit. During that request, the stable account identifier is linked to an active relay/session even though Mullvad says the state is temporary memory only (https://mullvad.net/en/help/no-logging-data-policy).

// MITIGATION: Validation state and simultaneous-connection counts are not written to disk or retained as history. Separate accounts reduce cross-device linkage.

T-51 COMPROMISED VALIDATION SERVICE EXPOSES ACTIVE ACCOUNTS

[DD · DESTINATION · I:H × L:L → M]

DD.4.2 AVAILABILITY/ACCESSIBILITY OF DATA

A compromise of the central validation service could reveal which numbered accounts are active and at which relay in real time, enabling correlation with network observation despite the absence of historical connection logs.

// MITIGATION: Memory-only state, no source-IP/connection history, short data lifetime and infrastructure access controls constrain retrospective exposure.

T-10 HISTORICAL CONNECTION EVIDENCE IS NOT RETAINED

[NR · DESTINATION · I:M × L:L → L · MITIGATED]

Nr.2 ATTRIBUTABLE ACTION SIDE-EFFECT EVIDENCE

Stored connection history would let an observer attribute account activity and defeat deniability. Mullvad says simultaneous-connection validation exists only in temporary memory and it cannot report how many connections an account had five minutes earlier (https://mullvad.net/en/help/no-logging-data-policy).

// MITIGATION: No connection timestamps, duration, source IP, bandwidth or account-activity history is persisted; the April 2023 police search obtained no customer activity data.

DF22 · ENTITLEMENT LOOKUP

P18 LIVE ACCOUNT VALIDATION SERVICE → D3 ACCOUNT AND DEVICE STORE · 1 THREATS

T-52 ENTITLEMENT LOOKUP JOINS LIVE AND STORED IDENTIFIERS

[L · DESTINATION · I:H × L:H → E]

L.1.1 UNIQUE IDENTIFIER

The validation service looks up the active account against stored expiry and device state. This is a necessary join between a live session pseudonym and its durable account record.

// MITIGATION: The durable record is minimized to account, expiry and device/tunnel fields and contains no required civil identity or traffic history.

DF23 · CONNECTION AUTHORIZATION

P18 LIVE ACCOUNT VALIDATION SERVICE → P4 VPN ENTRY RELAY · 1 THREATS

T-53 AUTHORIZATION RESPONSE REVEALS ACCOUNT STATE

[D · DESTINATION · I:L × L:H → M]

D.3 SYSTEM RESPONSES

The relay receives enough authorization state to accept or reject a connection based on expiry and simultaneous-device limits. Those distinct outcomes reveal current entitlement and connection-limit status to the relay process.

// MITIGATION: Only the state needed to authorize the connection is returned and Mullvad states that it is not persistently logged.

// THREAT TREE REFERENCE

[L] LINKING

L.1 Linked data
  L.1.1 Unique identifier — Data items share an identifier that is unique (globally, or within the system/session), making linking trivial.
L.2 Linkable data
  L.2.1 Through combination
    L.2.1.1 Quasi-identifier combining data of a single individual — A set of attributes serves as a quasi-identifier linking data of a single individual.
    L.2.1.2 Combining data of different individuals — Joining datasets or records of different individuals reveals additional information about them.
  L.2.2 Through profiling, derivation, or inference
    L.2.2.1 Profiling an individual — Patterns derived from data or user actions link data to an individual.
    L.2.2.2 Profiling a group of individuals — Data of one individual yields insights about a larger group (family, household).
    L.2.2.3 Profiling an individual through (dis)similarity — Uniqueness or similarity assessment (clustering) predicts properties of an individual.

[I] IDENTIFYING

I.1 Identified information
  I.1.1 Processing of identified data — The system requests or processes data that directly contains identity information.
  I.1.2 Identified information in metadata — Metadata of files or communication contains identified information.
I.2 Identifiable information
  I.2.1 Pseudonym
    I.2.1.1 Identifier — The data contains a unique reference (pseudonym) to the data subject's identity.
    I.2.1.2 Quasi-identifier — A combination of attributes is unique to a data subject and serves as a pseudonym.
  I.2.2 Revealing attributes — Collected or free-form attributes, combined, reveal the identity.
  I.2.3 The data subject is distinguishable from others — The anonymity set is too small; the data subject can be singled out.

[NR] NON-REPUDIATION

Nr.1 Attributable data evidence
  Nr.1.1 Data — Recorded data can be used as evidence against deniability claims.
  Nr.1.2 Signed data — Digital signatures or immutable storage prevent deniability.
  Nr.1.3 Metadata — Metadata (authorship, revisions, receipts) impacts deniability claims.
  Nr.1.4 Embedded/hidden data — Watermarks, tracking resources or per-recipient secrets attribute data to an individual.
Nr.2 Attributable action side-effect evidence — Action side effects (read receipts, logs, history) make actions attributable.

[D] DETECTING

D.1 Observed communications — Detecting involvement by observing communications, their existence or patterns.
D.2 Application side effect — Detecting involvement through (trans)action side effects (files, logs, transmissions).
D.3 System responses — System responses reveal the existence of an item of interest.

[DD] DATA DISCLOSURE

DD.1 Unnecessary data types
  DD.1.1 Data type sensitivity — More sensitive data types are collected than functionally required.
  DD.1.2 Data type granularity — Data is disclosed at a more fine-grained level than needed.
  DD.1.3 Data type encoding — The data encoding carries additional personal data (e.g. EXIF location).
DD.2 Excessive volume
  DD.2.1 Amount — An excessive amount of personal data is processed beyond functional need.
  DD.2.2 Frequency — Personal data is processed more frequently than functionally needed.
  DD.2.3 Involved data subjects — Personal data of more data subjects is processed than needed.
DD.3 Unnecessary processing
  DD.3.1 Treatment, analysis, enrichment, transformation — Data is treated, analyzed or enriched beyond functional need.
  DD.3.2 Propagation — Data propagates to, or is accessible by, services where it is not needed.
  DD.3.3 Implicit data disclosure — Data is implicitly disclosed as a side effect of flows or usage patterns.
  DD.3.4 Duration/retention — Data is processed or kept longer than functionally needed.
DD.4 Involved parties and exposure
  DD.4.1 Involved parties
    DD.4.1.1 Predetermined set of parties — Personal data is shared with more parties than functionally necessary (fixed set).
    DD.4.1.2 Dynamic set of parties — Personal data is shared with a dynamically determined set of parties.
  DD.4.2 Availability/accessibility of data — Personal data is published or made accessible more broadly than necessary.

[U] UNAWARENESS

U.1 Unawareness of processing
  U.1.1 Unawareness as data subject — Data subjects are insufficiently informed about the processing of their data.
  U.1.2 Unawareness as a user sharing personal data — Users sharing personal data of others are unaware of the further processing.

U.2 Lack of data subject control
  U.2.1 Preferences — Data subjects cannot set or alter preferences/consent for the processing.
  U.2.2 Access — Data subjects cannot access their personal data held by the system.
  U.2.3 Rectification/erasure — Data subjects cannot rectify or erase their personal data.

[NC] NON-COMPLIANCE

Nc.1 Regulatory non-compliance
  Nc.1.1 GDPR
    Nc.1.1.1 Insufficient data subject controls — Support for the data subject rights codified in GDPR Chapter 3 is lacking.
    Nc.1.1.2 Violation of data minimization principle — More personal data is processed than necessary (GDPR Art. 5.1(c)).
    Nc.1.1.3 Unlawful processing of personal data
      Nc.1.1.3.1 Invalid consent — Consent is not freely given, informed, specific, unambiguous, withdrawable and demonstrable (Art. 7).
      Nc.1.1.3.2 Lawfulness problems not related to consent — Lawfulness problems beyond consent (Art. 6.1(b-f), automated decision making).
    Nc.1.1.4 Violation of storage limitation principle — Data is stored longer than legally necessary (GDPR Art. 5.1(e)).
  Nc.1.2 Generic regulatory non-compliance — Non-compliance with applicable privacy regulations (fines, sanctions, reputational damage).
Nc.2 Improper personal data management — Personal data management falls short: no lifecycle policy, retention rules or responsibilities.
Nc.3 Insufficient cybersecurity risk management — Cybersecurity risk management is insufficient, with privacy consequences.
Nc.4 Non-compliance with privacy standards and best practices — The system does not implement applicable privacy standards and best practices.