

Last update → Oct 23, 2025

X-VPN

Brief Intro

Press Releases → Sandra Mitchell

Sponsored Video Partnerships → Astrid Larsen

Editorial Reviews & Affiliate Collaboration → Luke Murphy

1. Jurisdiction and ownership

Headquartered in Singapore, independently operated.

	Owner	Based in (Country)	"Fourteen Eyes" Country
X-VPN	LIGHTNINGLINK NETWORKS PTE. LTD.	Singapore	No

2. No-logs policy and any independent audits

X-VPN enforces a **strict no-logs policy**, as clearly outlined in its [Privacy Policy](#).

To further demonstrate its commitment to privacy, X-VPN maintains a [Trust Center](#) with technical safeguards such as RAM-only servers, in-memory data handling, and a transparent Warrant Canary.

Although an independent audit has not yet been completed, X-VPN has initiated the process to engage a reputable third-party auditor.

	Audited	Proof	Audit company	No logs policy claims in ToS
X-VPN	No, independent third-party audit is in progress	Transparency report & warrant canary (2017–2025, no logs disclosed)	-	Yes: https://xvpn.io/policy ; https://xvpn.io/blog/xvpn-no-logs-policy-explained

3. Protocols and encryption standards

Protocol:

- Everest (proprietary):** X-VPN's own protocol, supporting multiple transport types: UDP, TCP, HTTP, TLS, TLS-2, TLS-3, TCP-2, HTTP-2, and HTTP-3. Designed for flexibility and obfuscation.
- OpenVPN-UDP:** Available on macOS (root), Windows (root), and OpenVPN-compatible routers.
- WireGuard:** Now supported on all platforms, though the protocol selection interface is currently only available on macOS and Windows. Display options for other platforms are being gradually rolled out.
- L2TP:** Currently supported on routers.
- QUIC:** Available on iOS, Android, Apple TV, and Amazon TV.

	OpenVPN/UDP	OpenVPN/TCP	L2TP/IPSec	L2TP	IPSec	IKEv2	IKEv2/IPSec	PPTP	WireGuard	Other protocols
X-VPN	Yes	No	No	Yes	No	No	No	No	Yes	Everest (proprietary)/QUIC

Encryption:

X-VPN uses **AES-256-GCM** as both the default and strongest encryption algorithm across our supported protocols. All VPN tunnels are protected using TLS 1.3 combined with ECDHE key exchange, ensuring confidentiality, integrity, and forward secrecy. These encryption standards are consistently applied across platforms.

	Default Provided	Strongest Provided	Handshake Encryption: Weakest	Handshake Encryption: Strongest
X-VPN	AES-256-GCM	AES-256-GCM	ECDHE	ECDHE

4. Server numbers, countries covered, RAM-only/owned servers

X-VPN operates a global network of over [10,000+ servers](#) across more than 80 countries, including key regions in the Americas, Europe, Asia-Pacific, Middle East, and Africa. **All servers run on RAM-only infrastructure, ensuring no data is written to disk.**

The **free tier includes 1,000+ servers**, with location access varying by platform:

- On **iOS and Android**, users can manually select from [26 server locations](#) in 15 countries, including up to 13 city-level options in the U.S.
- On **macOS, Windows, Chrome Extension, and Chromebook**, users are connected automatically to one of 50+ available locations, without manual selection.

	Number of servers	Number of different countries
X-VPN	10,000+	80+

	No Ram servers	In transition	Fully transitioned
X-VPN	-	-	√

5. Platform support (Windows, macOS, Linux, iOS, Android, extensions, SmartTVs)

X-VPN supports a wide range of platforms, ensuring users can protect their connection across virtually all major devices:

- **Fully Supported Platforms:** Windows, macOS, Android, iOS (iPhone & iPad), Linux, Chromebook, Chrome Extension, Routers, Game Consoles (PS4/PS5/Switch), Amazon Fire Stick, Apple TV, Android TV.
- **Free Plan Availability:** Available on Windows, macOS, Android, iOS, Chrome Extension, and Chromebook.

Platform	X-VPN (Paid)	X-VPN (Free)
Windows	Yes	Yes
macOS	Yes	Yes
Linux	Yes	No
iOS	Yes	Yes
Android	Yes	Yes
Chrome Extension	Yes	Yes
Firefox Extension	No	No
Chromebook	Yes	Yes
Smart TVs	Yes	No
Routers	Yes	No
Game Consoles	Yes	No

6. Leak protection (kill switch, DNS/WebRTC/IP)

X-VPN provides comprehensive leak protection across all tiers. Both free and paid users benefit from built-in DNS, IP, and WebRTC leak protection.

A Kill Switch is available on all paid platforms except Linux and routers. For free users, Kill Switch functionality is provided on Android and iOS.

	IP leak protection	DNS leak protection	WebRTC leak protection	Data leak protection
X-VPN	Yes	Yes	Yes	Yes

7. Features (ad blocker, split tunneling, SmartDNS, obfuscation, TOR support, etc.)

X-VPN provides a wide range of essential and advanced features:

Core VPN Features:

- **Obfuscation (Free & Paid)** (via HTTP/TLS domain-based disguise and built-in obfuscation in proprietary protocols)
- **Split Tunneling**
- **Double VPN**
- **Static IP**
- **Kill Switch (Free & Paid)**
- **Quick Connect (Free & Paid)**

Additional Tools & Privacy Enhancements:

- **Storage Cleanup**
- **Startup Management**
- **Dark Web Monitor**
- **Browser Protection**
- **Ad Blocker**
- **Private Browser** (with incognito mode and DuckDuckGo/Google search options)

	Quick-connect	SmartDNS	Active blog	Split-tunneling	Additional cybersecurity features
X-VPN	Yes	No	Yes	Yes	Yes (<i>Ad blocker, Dark Web Monitor, etc.</i>)

	Offers ad-blocker
X-VPN	Yes

	Shadowsocks Support	Integration with TOR	Obfuscated Servers	Dedicated IP Servers
X-VPN	No	No	Yes (<i>via built-in obfuscation and HTTP/TLS disguise</i>)	No (<i>Only shared static IPs on iOS/Android</i>)

8. Pricing, free plan limits, refund policy

Paid Plan Options:

We provide several paid plan options to suit different needs: a 1-month plan at \$11.99/month, a 12-month plan at \$3.99/month (billed annually at \$47.99), and a 24-month plan at \$2.99/month (billed every two years at \$69.99). All premium plans come with a 30-day money-back guarantee and a 7-day free trial.

	1 Month Price	1y Plan Price	2y Plan Price	3y Plan Price	Lifetime Plan	Free Trial	Money-Back Guarantee
X-VPN	\$11.99	\$47.99	\$69.99	-	-	Yes, 7 days	Yes, 30-day

Free Plan:Our free plan requires **no login and imposes no bandwidth**. However, it comes with certain limitations based on available features, server access, and the presence of ads.

Free Tier by Platform

Platform	Server Access	Ads	Kill Switch	Data Cap
iOS / Android	26 server locations in 15 countries (manual selection, incl. 13 US cities)	Yes (non-intrusive)	Yes	Unlimited
macOS / Windows/Chrome Extension/Chromebook	1000+ free servers (auto-connect only)	No	No	Unlimited

9. Payment methods supported

X-VPN supports multiple payment methods for user convenience. You can pay using major credit cards (Visa, MasterCard, American Express, Discover, JCB), PayPal, or cryptocurrencies via CoinPayments, including Bitcoin, Bitcoin Cash, and Ethereum.

	Crypto	Card	Cash	Online payments
X-VPN	Yes	Yes	No	Yes

10. Customer support channels

X-VPN offers standard customer support through the following channels:

- **24/7 Live Chat**

Real-time support with human agents is available around the clock.

- → **On website:** Click the green chat bubble in the bottom-right corner.
- → **In app:** Tap the **Help Center**, then select the **Live Chat** button.

- **Email Support**

Users can reach the team directly at support@xvpn.io.

- **In-App Help Center**

Available across all platforms with categorized FAQs.

- **Web Help Center**

The [X-VPN Help Center](#) offers searchable documentation and platform-specific guides.

- **Social Channels**

Official team members actively respond on [Reddit](#), [Facebook](#), [Twitter](#), [Instagram](#), and [YouTube](#).

	Chat	24/7?	Email / Ticket	Phone	FAQ / Help Center	Other
X-VPN	Yes (website & app live chat)	Yes	Yes	No	Yes	Reddit, Facebook, Twitter, Instagram, YouTube

11. Transparency (affiliate disclosure, bug bounty, etc.)

X-VPN maintains a [Trust Center](#) where it publishes transparency reports — as of mid-2025, **zero user data** has ever been disclosed in response to over **65 law enforcement** and **239,000+ DMCA requests**.

We also run a [bug bounty program](#), offering rewards from **\$50 to \$500** based on severity (using Bugcrowd's taxonomy). Researchers must follow a responsible disclosure policy, and all reports are reviewed by our security team.

In addition, users who help troubleshoot real-world connection issues may receive **\$20/hour** for testing, with bonuses up to **\$1000** if their input leads to a fix.