X-VPN

X-VPN SPEED UPGRADE

Technical overview

How X-VPN rebuilt network capacity, routing, packet processing, and transport around our new Talaria protocol.



200%+ **Overall** Speed Improvement*

*Aggregate download and upload improvement across 10 Gbps internal test configurations versus previous X-VPN protocols. Individual results vary.

2026

At a Glance



200%+ Overall Speed Improvement

Across 10 Gbps internal tests on Windows, macOS, iOS, and Android, Talaria delivered an aggregate download and upload improvement of over 200% versus previous X-VPN protocols.



≤5% Download Speed Loss

In 1 Gbps and 100 Mbps internal tests, Talaria kept download speed loss within 5% across local, near-distance, and long-distance routes on Windows and macOS.



End-to-End Speed Stack

The upgrade spans higher-bandwidth infrastructure, client and server data paths, smarter routing, and Talaria transport, improving the whole connection rather than a single component.

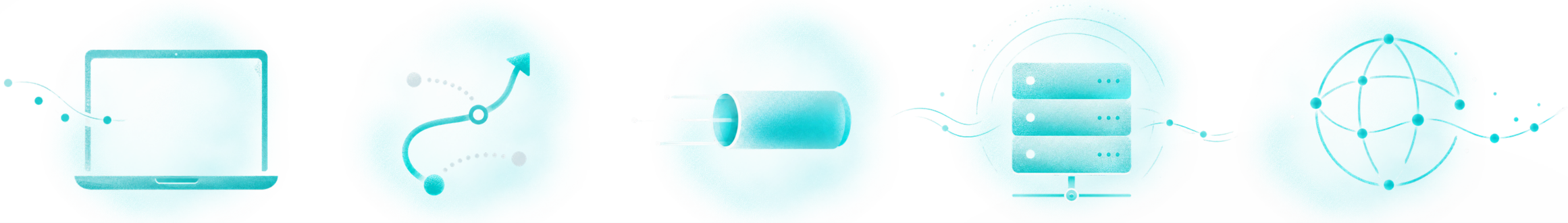


Security Held Constant

Talaria combines TLS 1.3, hybrid post-quantum key exchange, and replay protection. An independent security assessment by Vantage Point Security identified no vulnerabilities in the reviewed scope.

Speed Is End-To-End

X-VPN improved the whole VPN path — from device-side processing and route selection to transport efficiency and server capacity.



Device

Less work on the device

Path

Find a faster route

Talaria

Move more data efficiently

VPN Server

More processing headroom

Internet

Destination reached

NETWORK FOUNDATION

More bandwidth and compute supporting the whole path

CONTENTS

01 | Network Foundation

02 | Client Data Path

03 | Platform Optimizations

04 | AI Routing

05 | Talaria Transport

06 | Server Data Plane

07 | Measured Performance

08 | How We Tested

09 | Security & Audit

10 | Verification & Scope

NETWORK FOUNDATION

More Capacity to Work With

Higher-bandwidth infrastructure and stronger bare-metal configurations give the rest of X-VPN's speed stack more room to perform.

10–25 Gbps

Server port capacity



More than 90% of X-VPN traffic in the U.S. and Europe can be served by 10 Gbps or 25 Gbps infrastructure, extending high-bandwidth capacity across major demand regions.

64 Cores

Bare-metal compute



Current bare-metal configurations run 64 CPU cores. More compute headroom allows more traffic to be processed before CPU becomes the bottleneck.

128–256 GB

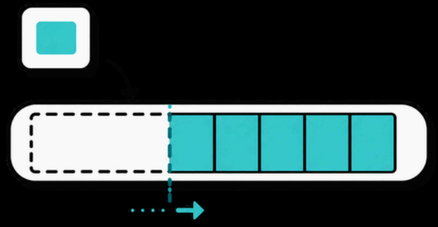
Server memory



Current bare-metal configurations use 128–256 GB of memory, up from 4 GB in the previous generation. More memory headroom supports higher-volume packet processing under load.

CLIENT DATA PATH

Less copying, less repeated work. X-VPN streamlines the client data path to reduce unnecessary copying, rebuilding, and handoffs for outgoing and incoming traffic.



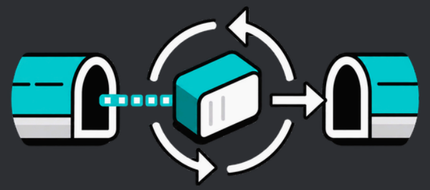
In-Place Framing

Outbound buffers reserve room for framing in advance, allowing headers to be written directly into the existing buffer instead of rebuilding the packet.



Platform-Native Paths

Rather than forcing every operating system through the same generic path, X-VPN uses an optimized data path supported by each platform.



Buffer Reuse & Direct Write

Where supported, X-VPN reuses buffers from the system tunnel instead of allocating and copying data into another buffer. Qualifying inbound traffic can be written directly back to the tunnel interface, avoiding an additional object-building and handoff step.

PLATFORM OPTIMIZATIONS

iOS

Larger Batches, Lower Memory Use

On supported iOS paths, X-VPN processes larger data batches while keeping memory overhead low, reducing repeated work in the client data path.

01

Android

More Data per Processing Cycle

X-VPN processes larger chunks of data per cycle, reducing repeated packet handling and CPU work on supported Android paths.

02

macOS

Balanced Multicore Scheduling

X-VPN controls how much work runs in parallel on macOS, keeping CPU cores productive while reducing competition for shared resources.

03

Windows

Efficient Driver-Based Processing

On Windows, X-VPN uses an upgraded kernel data driver to improve data processing efficiency and stability.

04

Optimized for Each Operating System

X-VPN tailors data processing to each platform, using batching, multicore scheduling, and driver-level optimizations to reduce unnecessary data movement and resource contention.



AI ROUTING

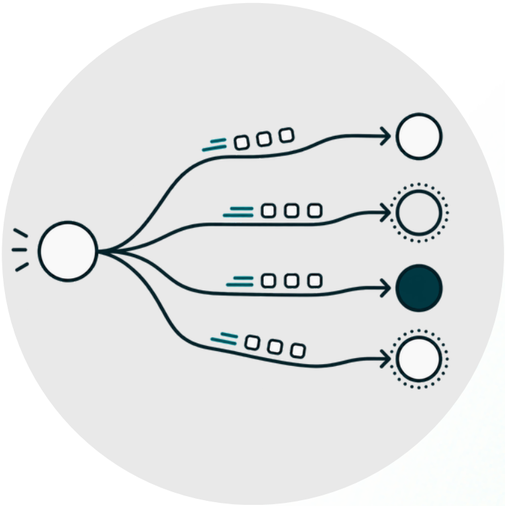
Choose a better path. Connect with less waiting.



SmartEntry Adaptive Mesh

Choose a Better Path

The client tests available high-capacity entry nodes while X-VPN evaluates available bandwidth, helping select a route suited to current network conditions.



PrivacyRoute Fabric

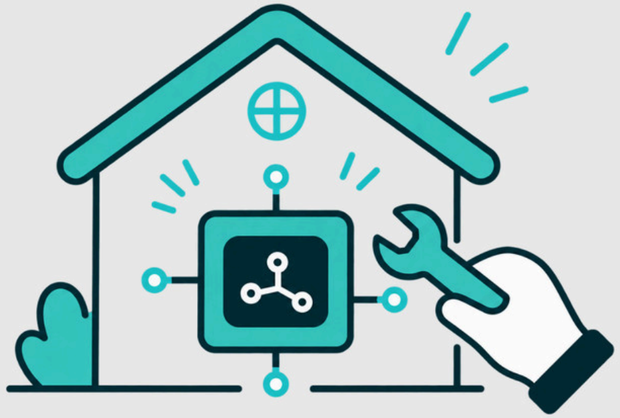
Connect Through Promising Routes First

Promising candidates are tried in time-limited batches. Once one completes authentication, the remaining attempts stop, reducing unnecessary connection attempts.

Talaria Transport

Meet Talaria

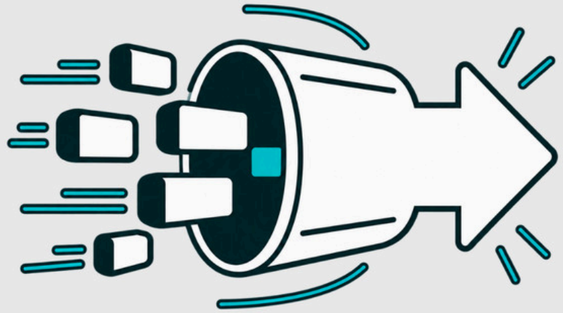
Talaria is X-VPN's new in-house protocol, designed for higher transport efficiency and now open source on GitHub.



Built In House

A new protocol developed by X-VPN

Talaria is designed and implemented in house around X-VPN's own performance, security, and network requirements.



Built for Speed

Make better use of available bandwidth

Built to reduce avoidable transport overhead and move data efficiently across everyday and high-bandwidth connections.



Open Source

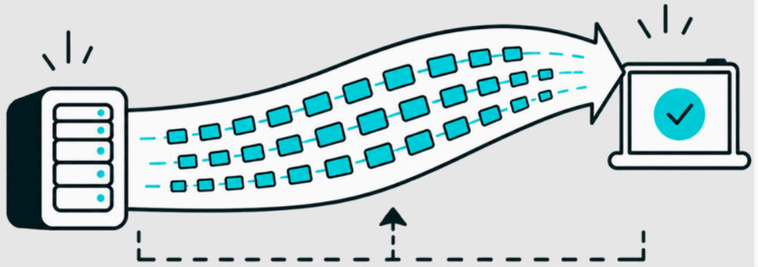
Inspect the implementation directly

Published on GitHub under the AGPL v3 license, Talaria's source code is now available for researchers and developers to inspect.

Talaria Transport

Built for Efficient Data Movement

Talaria combines parallel transport, pipeline acceleration, and flow-level forwarding to reduce repeated work and keep more data moving.



Multi-Channel Parallelism

Process Concurrent Flows Independently

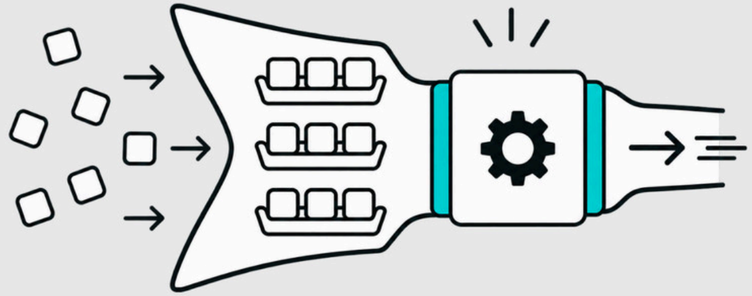
Each application connection gets its own transport channel. Concurrent flows can be processed independently across CPU cores, reducing contention in a single shared processing path.



Offload & Pipeline Acceleration

Batch More Work, Repeat Less

Batched I/O handles multiple packets per system call, while supported kernel offload paths reduce repeated packet work. Receiving, authenticated decryption, and writing data back run as a pipeline.



Flow-Level Forwarding

Forward Flows with Less Packet Work

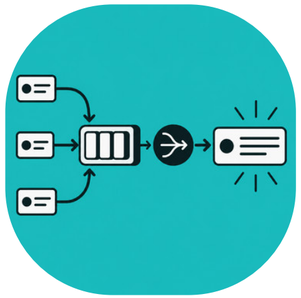
On supported paths, a userspace network stack reconstructs connection flows from IP packets and forwards their data toward the destination, reducing repeated packet-level processing.

SERVER DATA PLANE

Built to Keep Up

X-VPN redesigned the server data path to skip unnecessary processing, handle traffic more efficiently, and keep data moving smoothly under load.

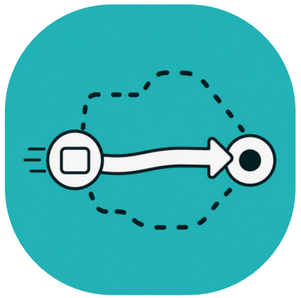
Prefetch and Recombine



Decouple reads, combine writes

We use a single-producer, single-consumer (SPSC) prefetch queue to separate data reads from later processing, allowing each stage to keep moving independently. Adjacent data batches can then be combined before they are written out, reducing repeated write operations.

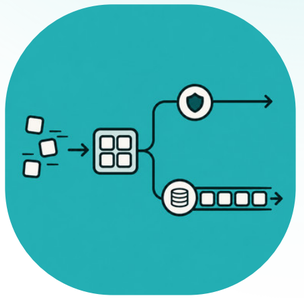
Take the Faster Path



Skip general processing when possible

Qualifying long-lived IPv4 TCP flows can move onto an optional fast path. When address fields are rewritten, RFC 1624 incremental checksum updates avoid recalculating the checksum from scratch.

Batch and Prioritize



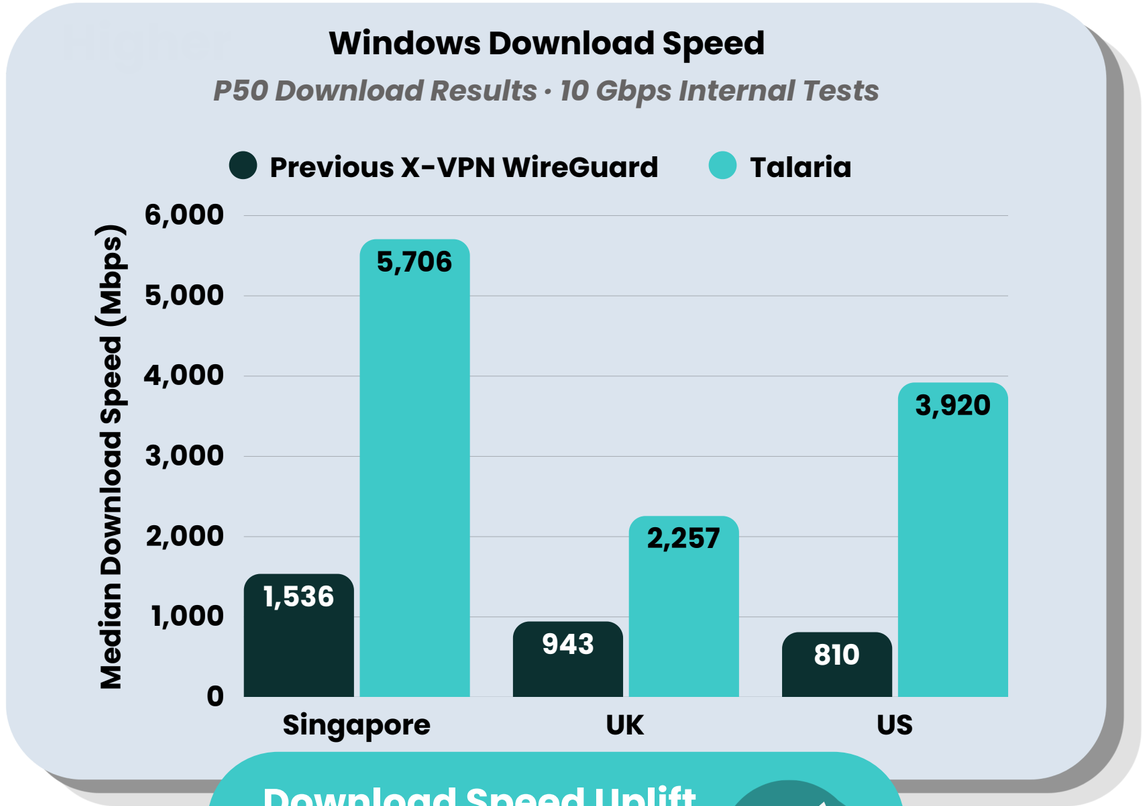
Do more work with fewer handoffs

Sustained traffic can be briefly grouped before writing, while small packets are sent promptly. Control and data traffic use separate queues, and bounded queues keep memory use and backlog within defined limits.

MEASURED PERFORMANCE

Higher Download Speeds Across Regions

In 10 Gbps internal tests initiated in Singapore, Talaria achieved higher median download speeds than previous X-VPN protocols when connecting to Singapore, the UK, and the US.

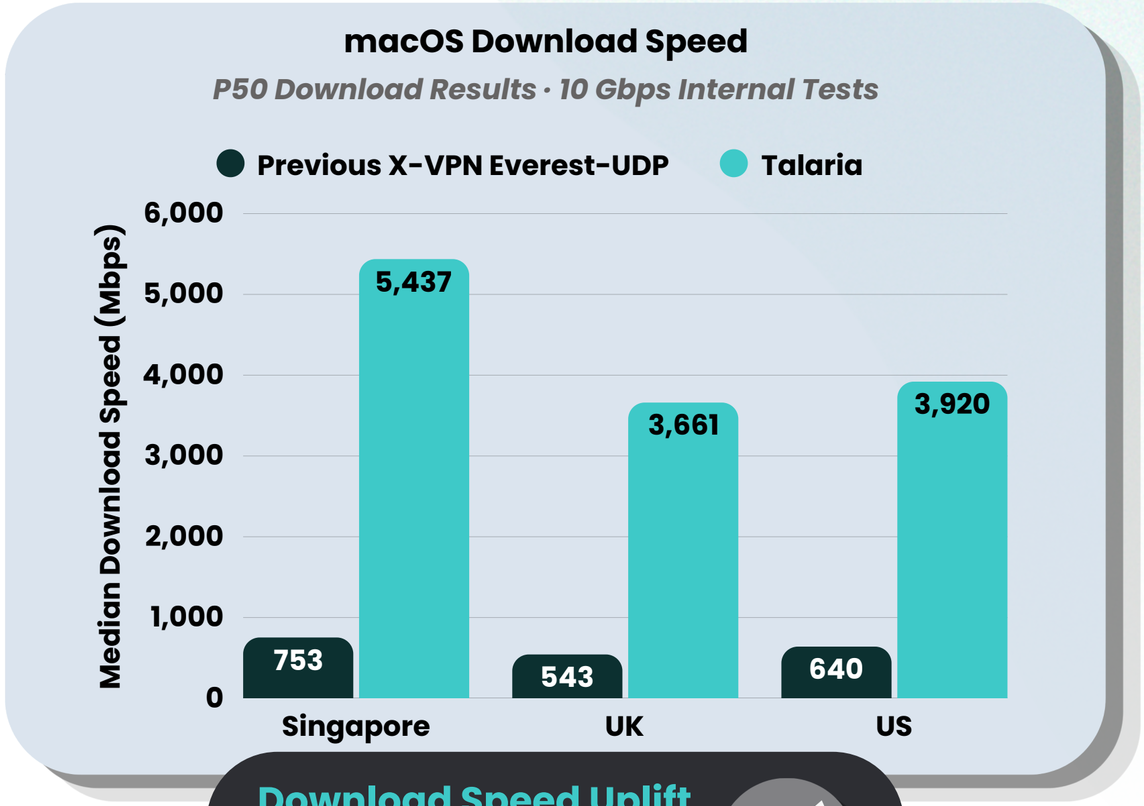


Download Speed Uplift

Singapore + 271.5%

UK + 139.3%

US + 383.9%



Download Speed Uplift

Singapore + 621.8%

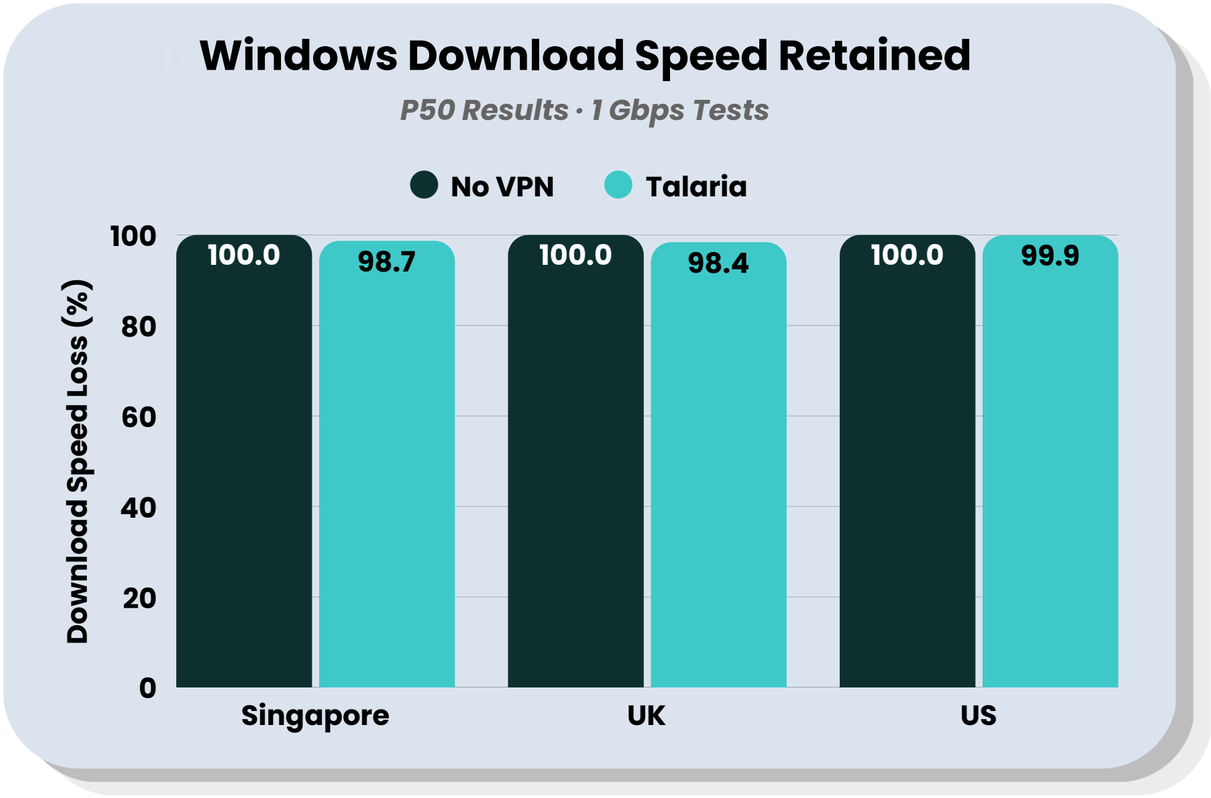
UK + 573.7%

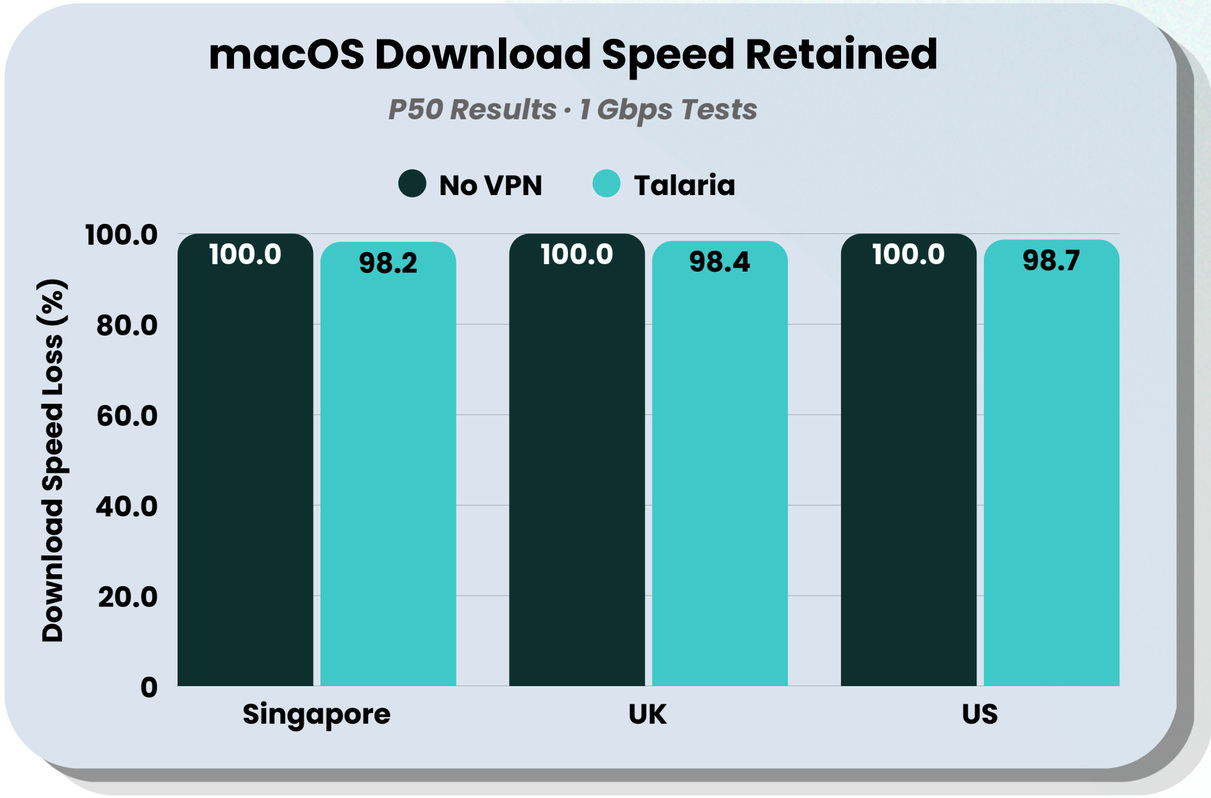
US + 512.6%

MEASURED PERFORMANCE

5% or Less Download Speed Loss

In 1 Gbps internal tests on Windows and macOS, Talaria kept download speed loss below 5% across the three tested VPN locations.





Windows

0.1–1.6% download speed loss

macOS

1.3–1.8% download speed loss

HOW WE TESTED

Internal Tests, Defined Conditions

**Results apply to the tested configurations and vary by device, server, route, and network conditions.*

01 Test Period

X-VPN conducted internal tests from August 22 to September 8, 2026, using configurations across different platforms, bandwidth tiers, protocols, and routes.

02 Test Locations

Tests started in Singapore and connected to VPN servers in Singapore, the UK, and the US.

03 Platforms & Connections

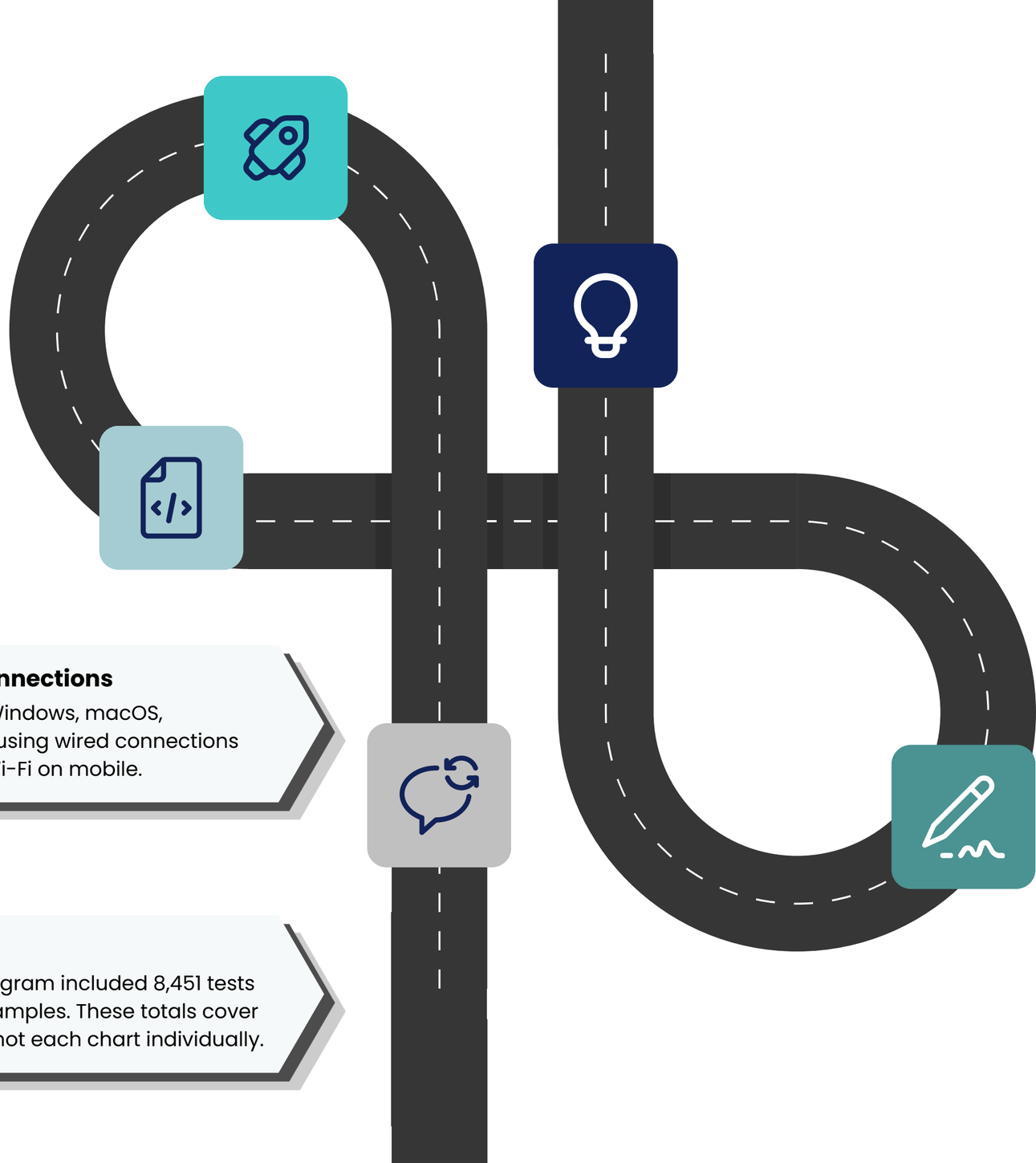
Testing covered Windows, macOS, Android, and iOS, using wired connections on desktop and Wi-Fi on mobile.

04 Test Tools

Desktop tests used Speedtest CLI 1.2.0.8. Mobile tests used Speedtest for Android 7.0.7 and Speedtest for iOS 7.0.5.

05 Sample Size

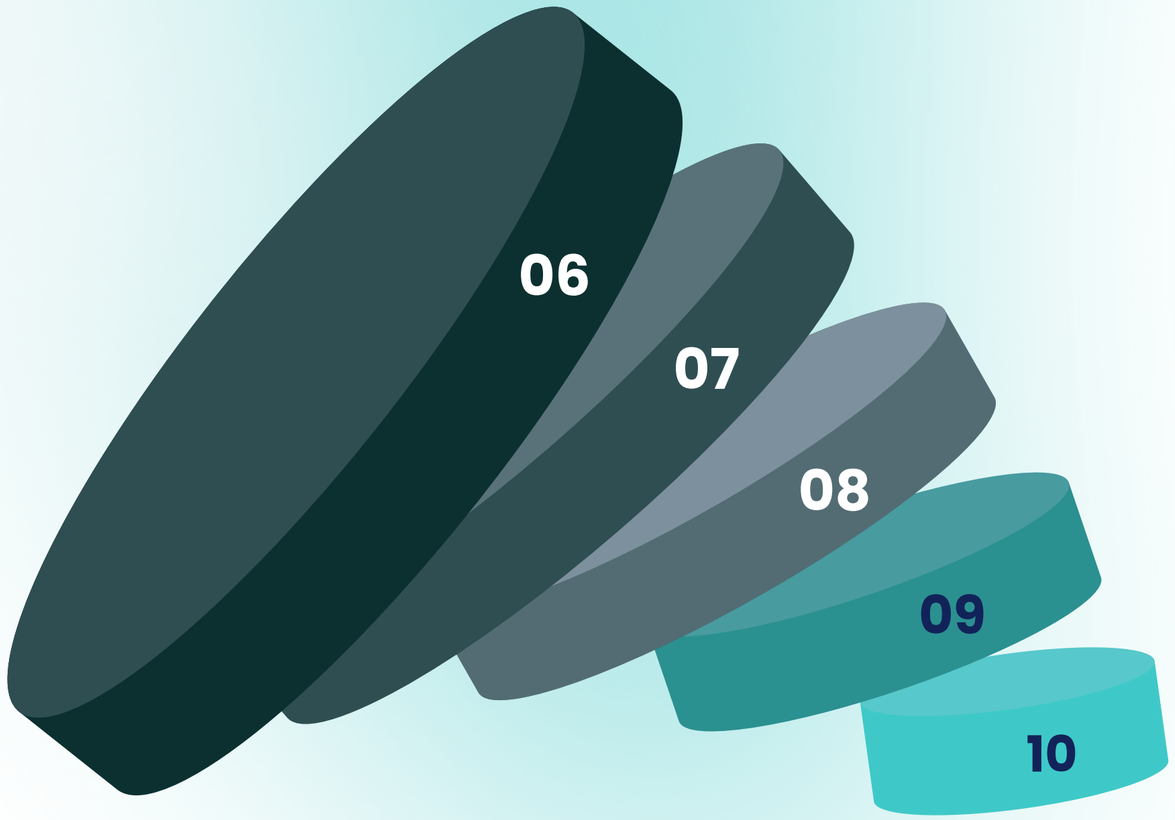
The wider test program included 8,451 tests and 6,590 valid samples. These totals cover the full program, not each chart individually.



HOW WE TESTED

Internal Tests, Defined Conditions

**Results apply to the tested configurations and vary by device, server, route, and network conditions.*



macOS Hardware

macOS tests used an Apple M4 Mac mini with 10 Gbps Ethernet, 24 GB of memory, and 256 GB of storage.

Windows Hardware

Windows tests used a system with an AMD Ryzen 7 processor running Windows 11 Pro, connected over a wired network.

Repeated Tests & Filtering

Each platform, bandwidth, protocol, and route combination was tested repeatedly. Only successful connections with download speeds above zero were included in the statistics.

No-VPN Baseline

Download speed loss is measured against the no-VPN baseline, showing the percentage of baseline download speed lost when the VPN is connected.

Results & Comparisons

Charts show median (P50) desktop download results. The overall improvement headline averages combined download and upload percentage improvements across the wider test set.

SECURITY

Speed Without Cutting Security

Talaria requires TLS 1.3 and combines hybrid post-quantum key exchange, isolated session keys, authenticated encryption, and replay protection.

**Post-quantum protection here applies to hybrid key exchange. It does not mean every cryptographic component is post-quantum.*



Hybrid Post-Quantum Key Exchange

TLS 1.3 with X25519 + ML-KEM-768

Talaria uses TLS 1.3 only, with a hybrid X25519 + ML-KEM-768 key exchange to protect session key establishment while retaining the security of the classical component.



Isolated Session Keys

Separate keys per connection and direction

Traffic keys are derived independently for each connection through TLS Exporter/HKDF, with separate keys for each direction. Server identity is verified through X-VPN's private trust chain.



Authenticated and Replay-Protected

Protect confidentiality, integrity & freshness

AEAD authenticated encryption protects traffic from being read or altered in transit, while a sliding replay window rejects duplicate or expired packets.

INDEPENDENT SECURITY AUDIT

Security Reviewed by an Independent Firm

Singapore-based Vantage Point Security independently assessed Talaria's security through a white-box source code review and protocol-level penetration test. The assessment identified no vulnerabilities in the reviewed scope.

Read the Full Security Report →



Six Security Objectives

Comprehensive Security Coverage

Testing covered tunnel establishment, traffic protection, session security, forwarding isolation, adversarial inputs, and resilience.



0 Vulnerabilities Identified

No critical, high, medium, or low vulnerabilities identified

The assessment identified no security vulnerabilities. It noted only four observations, all of which were addressed and verified by Vantage Point Security during retesting.



Security Best Practices

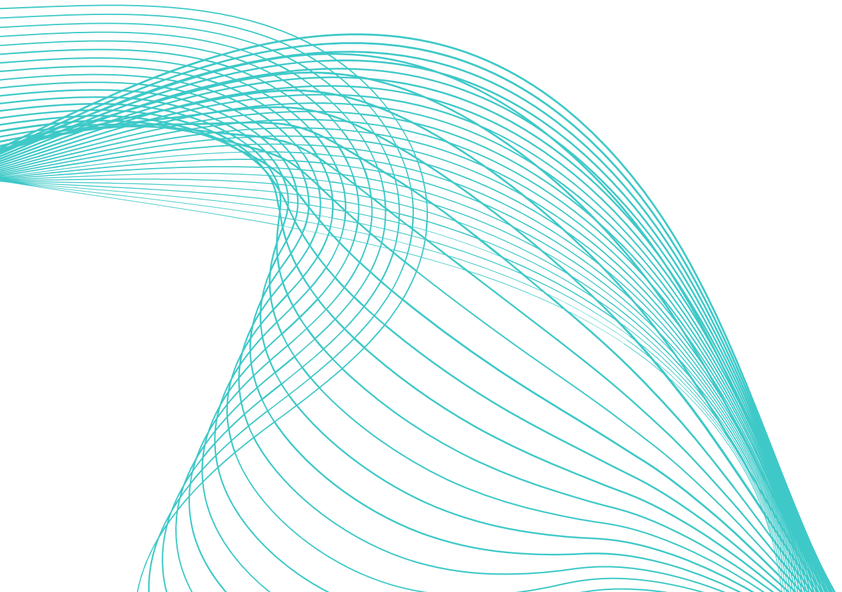
Secure Cryptographic Design and Use

Talaria's reviewed cryptographic design and use align with security best practices, with no demonstrated flaws undermining its cryptographic primitives.

VERIFICATION & SCOPE

Clear About What Applies
Performance claims matter most when their scope is clear. X-VPN explains where optimizations apply and how availability and performance vary across platforms and plans.

For users, the result is simple: faster path selection, better use of available bandwidth, and more efficient processing across the connection.



01

Open Source on GitHub

Public code, open to inspection

Talaria was released on GitHub on October 16, 2026, under the AGPL v3 license. Its published source code is available for public review.
View Talaria on GitHub

02

Platform-optimized paths

Use the best path available

Support varies by operating system, build configuration, and server capability. Not every optimization applies to every platform or data path.

03

Talaria and Everest

Built for different conditions

Talaria focuses on speed and transport efficiency, while Everest remains better suited to restrictive networks where VPN traffic needs obfuscation.

04

Plan Availability

Talaria is available on the free plan

Talaria is available to free users, bringing its efficiency improvements to the free plan as well. Performance varies by plan, platform, and connection.



Media Contact
sandramitchell@media.xvpn.io