Product Information | SDK for VPN and Wi-Fi Security

AnchorFree's SDK delivers a critical layer of security and privacy for consumers and businesses. End point security companies, XSPs, consumer app developers, and hardware manufacturers use our SDK to secure their customers, accelerate time to market and deliver premium performance around the globe.

Overview

AnchorFree is a global leader in secure communication

AnchorFreeVPN technology is run by 100's of millions of monthly connected users

AnchorFree's patented Hydra technology delivers the fastest speeds on the market

Key features

Security

Protects identity and sensitive data when connected to public Wi-Fi

Privacy

Protects IP address from spammers, snoopers and hackers

Protection

Alerts/blocks suspicious websites and protects against dangerous sites.

Proven technology

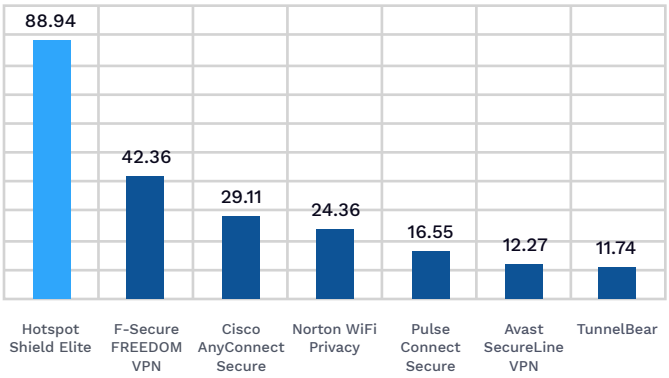
With more than 650 million downloads AnchorFree technology has been proven to perform globally. Our technology now drives VPN/Wi-Fi security for the most popular app developers and Fortune 500 companies including:

verizon SAMSUNG Bitdefender McAfee KDDI KASPERSKY lab

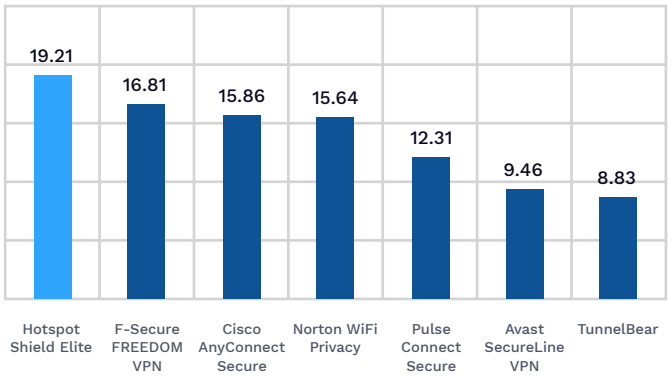
Powerful performance

Our performance leadership was documented in AVTest.org's recent VPN comparison. Hotspot Shield – AnchorFree's consumer product built on our proprietary Hydra technology – dominated consumer and enterprise competitors.

Download speed in MB/s



Upload speed in MB/s



- Up to 2x faster downloading large files from remote servers
- Faster downloads of small files due to the removal of DNS overhead
- Works for all traffic that requires DNS resolution
- Decreases time to start download of websites, small, and large files

Flexible implementation

Our turnkey service delivers server and client components and easily integrates into Windows, Mac, Android and iOS applications. Our flexible implementation allows our partners to control:

- when the service engages (at user prompt, launch of app, connection to unprotected Wi-Fi)
- length of trial (if any)
- end user messaging
- band with limitation (if any)
- choice of global server locations

Advantages

Client-side plug-in framework

Ability to integrate partner's code inside the VPN client's data path for real-timeinspection. Use case: A company may deploy mobile anti-virus solution that performs deep traffic inspection or signature analysis and blocks or allows the traffic based on its own set of rules, independently updated from partner's servers

Selectivity

- Split traffic sending specific traffic through the VPN tunnel; sends other traffic directly
- Application-specific rulesfor mobile devices. Implementation on iOS is unique to AnchorFree
- System-wide VPN intercepts all traffic from the client
- Can run through app-specific local proxy or network module

Multi-server

VPN client can connect to multiple VPN servers in different locations during the same session and route traffic between them based on domain, IP, port, protocol, or app name. This allows the technology to select the best path for each content provider

Client-side traffic analysis and blocking

- Block traffic by pattern on the client device, even if VPN operates in bypass mode
- Detect and measure amounts of traffic by domain, IP, port, protocol or app name
- Option to throttle specific traffic (e.g. video on cell connection) even if VPN operates in bypass mode

Censorship bypass

Extensive ability to make VPN traffic indistinguishable from other traffic over the Internet (includes eliminating the need to maintain the same persistent connection during long VPN session)

Anti-phishing

Protect mobile users in real time from malicious domains and IPs

Key VPN features

1. Flexible initiation options:
    a. autoconnect to trusted Wi-Fi networks
    b. notifications upon Wi-Fi detection (all Wi-Fi networks or only notify on unsafe networks)
2. Autoconnection on application start
    a. Automatically triggers VPN connection for specific applications
    b. option to create a rule to connect to a specific location for the application (e.g. connect to UK location for bbc.co.uk)
3. Autoconnection on accessing a specific URL
    a. Triggers VPN connection on banking\social\e-commerce sites
    b. Rule-based connection to a specific location for the URL (e.g. connect via USA location for Zillow.com)
4. Connect to multiple VPN locations simultaneously and route traffic based on rules
6. Option to create dedicated IP address
7. Route certain traffic in bypass of the VPN tunnel (e.g. ride share apps)
8. Manually change a location for connection (~30 locations supported around the world). Additional locations are available upon request
9. Option to enable periodic end user messaging (service capabilities, problems solved, etc.)

Key anti-phishing features

1. Integrate with partner's own definition databases to detect threats
2. Define specific actions by threat type: do nothing, show a warning page (HTTP only), send a notification, turn on VPN, block the traffic
3. Block online trackers
4. Block malware
5. Block untrusted sites
6. Block known phishing/fraud destinations
7. Enable autostart or manual protection
8. Manual protection pause
9. Notifications about threats detected and blocked
10. Daily summary of the threats detected and blocked

For more information contact: Chris Weltzien, VP Business Development, AnchorFree Inc.

c.weltzien@anchorfree.com