MOBOLIZE

DATA SHEET

MOBOLIZE | Secure

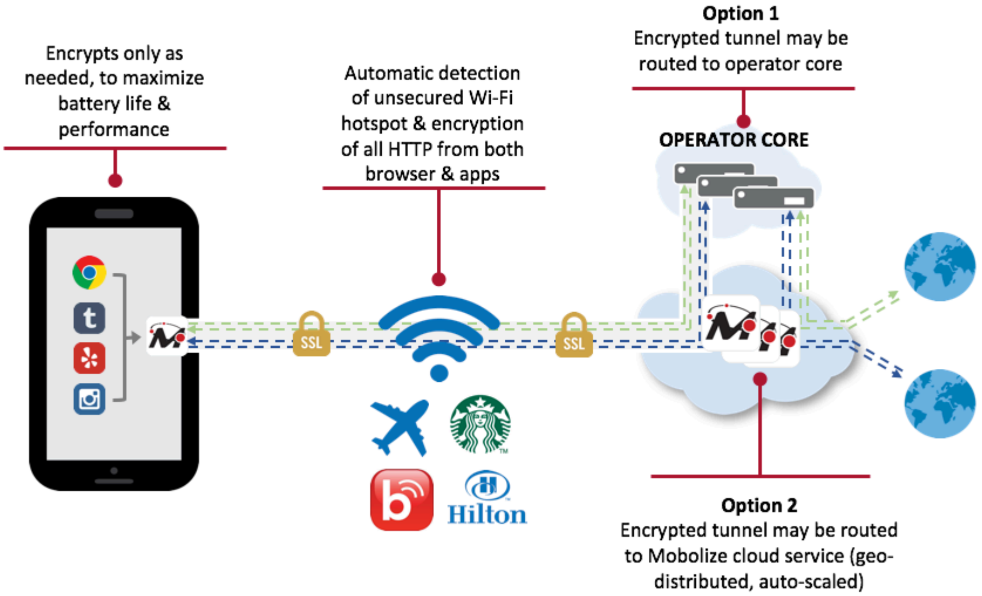
THE THREAT TO USERS

With as many as 70% of users connecting to an unsecured Wi-Fi hotspot every week, the majority of mobile users are vulnerable to a wide range of threats:

- Packet sniffers (e.g. AirPcap).
- Hotspot impersonation.
- Hacked AirBnB hotspots.
- Login session hijacking (e.g. Firesheep).
- Pervasive monitoring (e.g. NSA and GCHQ).

Give users the Wi-Fi security they need and expect on unsecured public hotspots.

- Automatic privacy protection that is easy to use.
- Encrypts unsecured traffic to ensure data is never vulnerable.
- The only SmartVPN™ solution that automatically turns itself on and off, making it faster and more efficient.



Encrypts only as needed, to maximize battery life & performance

Automatic detection of unsecured Wi-Fi hotspot & encryption of all HTTP from both browser & apps

Option 1
Encrypted tunnel may be routed to operator core

Option 2
Encrypted tunnel may be routed to Mobolize cloud service (geo-distributed, auto-scaled)

HOW IT WORKS

1. Whenever a user connects to a public hotspot, MOBOLIZE | SECURE automatically offers Secure Wi-Fi to the user (if not already purchased).
2. When MOBOLIZE | SECURE detects that the hotspot is open or unsecure, it automatically enables encryption for both web and application HTTP traffic before it leaves the device.
3. The encrypted HTTP traffic can be forwarded for termination at either the operator's infrastructure or at one of Mobolize's geographically distributed cloud servers.
4. When the original HTTP traffic is decrypted, it is then forwarded to the app/web server.

Benefits

- ❖ Increase ARPU – Wi-Fi security is a paid service that is in great demand today
- ❖ Bolsters your brand as a leader in security while tapping into subscriber trust
- ❖ Contextual sale means maximum conversions without minimal marketing investment
- ❖ Gain visibility/control into the mobile traffic that goes over Wi-Fi
- ❖ Ensure security for offload to public Wi-Fi

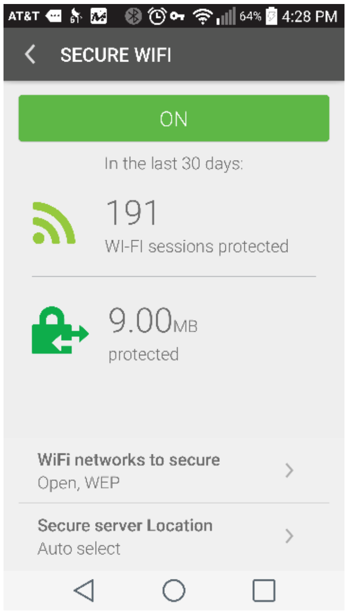
MOBOLIZE | System Requirements

- Android
  - 4.3 and above
  - Download or Preload
  - APK or SDK
- iOS
  - 9.0 and above
  - Download
  - IPA or SDK

5. On the return path, the response traffic is encrypted by Mobolize cloud servers (or the operator's infrastructure), and remains fully protected until it arrives on the device.
6. Whenever a user disconnects from the public hotspot, encryption is automatically disabled, maximizing performance and battery life.

BENEFITS FOR END-USERS

- Security
  - Protects both apps and web browsing.
  - Automatically activates whenever user is on an unsecured hotspot.
  - Provides indication when Secure Wi-Fi is active (configurable).
  - Does not alter HTTPS traffic.
- Ease of Use – Automatically encrypts traffic as soon as the phone connects to an unsecured network – no end user action required.
- Max performance and battery life – Encryption is only enabled when needed, so there's no unnecessary latency battery drain. When a user switches to a secure cellular or Wi-Fi network, it stops encrypting and redirecting. In markets like the US, where 50% of traffic is already encrypted (HTTPS) and about 40% of Wi-Fi connections are already secure, this means Mobolize Secure only has to process 30% of the traffic that traditional VPNs do.
- Compatibility – Works with all apps and browsers, and all unsecured Wi-Fi hotspots.



ON

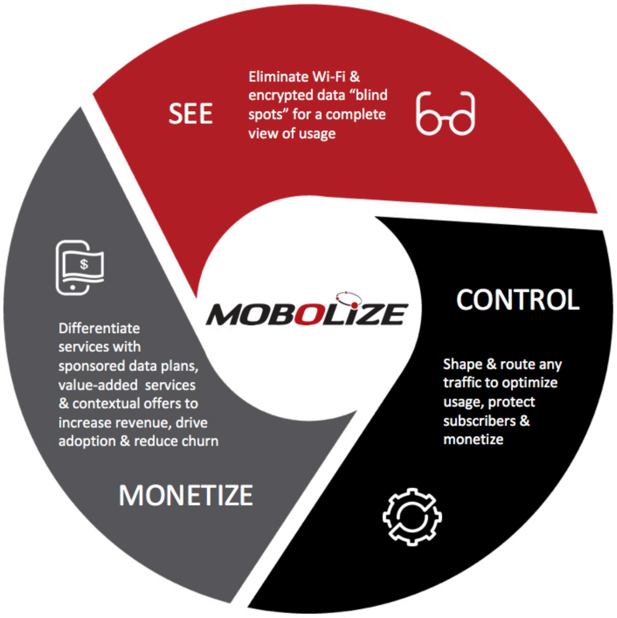
In the last 30 days:

191
WI-FI sessions protected

9.00MB
protected

WiFi networks to secure
Open, WEP

Secure server Location
Auto select


SEE
Eliminate Wi-Fi & encrypted data "blind spots" for a complete view of usage
CONTROL
Shape & route any traffic to optimize usage, protect subscribers & monetize
MONETIZE
Differentiate services with sponsored data plans, value-added services & contextual offers to increase revenue, drive adoption & reduce churn
MOBOLIZE

MOBOLIZE SECURE DELIVERS MORE BENEFITS TO OPERATORS

Feature	Mobolize	Competitors
Automatic operation	Yes. Automatically protects users when they connect to unsecured Wi-Fi for the best user experience	No. User has to remember to turn it on or leave on
Efficiently encrypts only traffic that needs it	Yes. SmartVPN™ avoids unnecessary overhead of redundantly encrypting traffic that doesn't need it, maximizing performance and battery life & minimizing cost	No. Redundantly encrypts all data, adding latency, slowing performance and killing battery life
Supports sending traffic to MNO's proxy servers	Yes. Enables low cost operation. Gives operator data visibility and system control.	No. Requires using proprietary VPN servers.
Provide MNO with usage data	Yes. Mobolize provides detailed Wi-Fi app and web usage data	No
Guaranteed to work with any firewall and NAT environment	Yes. Uses TLS on port 443, which is always open, for best reliability and user experience.	No. Uses IPsec ports, often blocked on firewalls
Contextual sale	Yes. App automatically notifies users of unsecured networks and makes sales offer. Provides highest conversion rates and zero-cost marketing.	No
Carrier Billing	Yes. Along with Contextual sale, removes friction from the purchase process, increasing conversion rates and maximizing revenues	No
White label app	Yes. MNO branding added to UI to increase user trust and loyalty	No
Carrier grade production software	Yes. Currently meeting rigorous requirements of a Tier 1 US operator	No
Easily embed into existing apps	Yes. Mobolize SDK can be integrated without any code changes for fast, efficient deployment	No

About Mobolize

Mobolize's software enables telecommunications operators to See, Control and Monetize all the data on users' mobile devices on any cellular or Wi-Fi network. Mobile Network Operators (MNOs), Mobile Virtual Network Operators (MVNOs), handset manufactures, and third-party developers use Mobolize's mobile data orchestration solutions to enhance customer experience and increase revenue.

Corporate Headquarters

2716 Ocean Park Blvd.
Suite 3055
Santa Monica, CA 90405
United States

Tel: +1-310-693-8340
Fax: +1-310-943-2155
www.mobolize.com
sales@mobolize.com