



OnEdge Wireless Data Sheet

Controlling Wireless Connections

Wi-Fi is now part of your network whether you wanted wireless or not. Every laptop now has wireless built in and is creating a wide-open hole in the security of your network. The fact that your employees will use Wi-Fi at work, home, and on the road intensifies the security threats of the wireless laptop.

If you have wireless laptops behind your firewall they will compromise the data on your endpoint devices and punch holes in your network perimeter defenses.

OnEdge Wireless ensures all endpoint devices, including desktops, notebooks, and tablet PCs comply with corporate security policies governing Wi-Fi network connectivity and security. With advanced, patent-pending smart agent technology, MobileSecure enforces highly-customizable system connectivity policies that are centrally managed, automatically distributed to end-users, and continuously enforced-always and everywhere-without user intervention.

What can OnEdge Wireless do for you?

1. Prevents connections to rogue access points, ad hoc connections, or 'evil twin' / man-in-the-middle attacks
2. Secure users working at public access Wi-Fi hotspots, making them virtually invisible to hackers and enforcing security measures such as VPN usage
3. Automate the creation and enforcement of security policies, monitoring compliance via a central management console
4. Control unwitting or malicious employee behavior
5. Use existing Wi-Fi infrastructure, with no need to purchase, install or manage additional Wi-Fi hardware on every floor (sensors, gateways, etc.)

About MobileSecure

MobileSecure enforces compliance at the "Mobile Edge". With more than 1 billion mobile devices (PDAs, smartphones, iPods, thumb drives, Zip disks, and more) currently in the market, business users are connecting these devices to corporate PCs and networks on a daily basis.

MobileSecure brings business continuity to companies looking to both meet compliance and to continue to allow their workforce to leverage the power of mobile technologies.

Top Wireless Threats

Rogue Access Points

What is preventing your mobile users from connecting to rogue access points? OnEdge Wireless can restrict users from connecting to unauthorized access points inside and outside the office.

Dual Homing and Bridging

One of the most feared vulnerabilities is a wireless laptop connected to both the wired network and a wireless network at the same time.

Peer-to-Peer Networks

Ad Hoc Networks can be a serious threat to the protected network and its data. A malicious user can connect to an open peer-to-peer connection and access the computer, its data and the wired network.

Accidental Associations

Wireless networks are present everywhere. Whether a user is in the office, at home or on the road there is a good chance they will associate with an unsecured access point.

Contact us Today

MobileSecure, Inc.
2 Dundee Park
Andover, MA 01810

Phone: (978) 470-8770
Email: info@mobilesecure.com
Web: www.mobilesecure.com