

SECURING THE MOBILE WORKER



CONTACT

Prem Iyer, CISSP/PMP
Practice Director
Information Security
infosec@ironbow.com

Consumerization, telework and Bring Your Own (BYO) device trends are quickly shaping a mobile, energetic workforce, empowered to work anywhere on computing devices of their choice. Whether using personal or corporate supplied devices, these workers need access to their organization's network, applications and services.

This blend of corporate and personal equipment makes for a complex combination of technologies to secure. They consistently carry company data and interact with the company network, but may touch content that is not trustworthy.

With a loss of visibility and control, what is the best way to keep your data, devices and enterprise secure? How can you support mobility with easy access to corporate IT resources without compromising security?

EMPOWER MOBILE WORKERS WITHOUT SACRIFICING INFORMATION SECURITY

Iron Bow's secure mobile computing solution combines Citrix virtualization and McAfee security technologies into a single comprehensive solution that will empower mobile workers without sacrificing security. Allow employees to compute securely anywhere, on any mobile device and on a virtual desktop that accesses corporate resources as needed. At the same time, get the visibility and management control you need. Iron Bow's secure mobile computing solution will:

- Secure any device, it's data and applications
- Support employee owned smartphones, netbooks, tablets, hybrids and laptops
- Enable virtual desktops that allow users ubiquitous access to familiar business applications
- Facilitate centralized IT and lower TCO with automated configuration, administration and compliance reporting
- Allow remote management of devices, including security
- Enable secure access to new mobile applications

"Government could achieve an estimated \$37M in productivity gains by enabling employees with connected smart phones [mobile computing capability]."
- *Telework Exchange*



SECURE ACCESS TO CORPORATE RESOURCES FROM ANY DEVICE

Connect securely to enterprise services, including VPN, Wi-Fi, messaging and line of business applications, utilizing strong authentication and role based access.

Utilize any device – smartphone, tablet, hybrid/convertible, netbook or laptop.

Utilize any platform – Windows XP/7, MAC OSX, Linux, Apple iOS (iPhone & iPad), Nokia Symbian, Webos, Windows Mobile, Android, Java and Blackberry.

[Only] 16% of federal employees rate their agency with a 'A' for equipping them with mobile tools. Workers with agency enabled 'smart phones' gain almost 1 hour per day in productivity.
- *eWeek*

VIRTUAL DESKTOPS AND BUSINESS APPS ON DEMAND

Self-provisioning allows users to access a full catalog of desktops, applications and business services from a personalized enterprise storefront, as well as utilizing Bring Your Own (BYO) programs.

Desktops and applications are available on demand for any device in any location, providing a rich "high-definition" experience.

Automatic updates and plug-ins are pushed to desktops based upon the policies set up by IT and preferences chosen by the user.

ENTERPRISE MANAGEMENT MAINTAINS VIRTUAL VISIBILITY AND CONTROL

Comprehensive management and compliance tools enable you to effectively secure a mobile workforce, ensure that policies and configurations are persistent, and deliver automatic and real-time compliance management.

Automated configuration and connectivity of VPN, Wi-Fi and native email sync makes self-provisioning easy. The user's unique credentials can personalize the device allowing access to user-specific application services and the enforcement of role-based policies.

A scalable mobile architecture enables you to seamlessly manage thousands of mobile devices over a geographically dispersed data network, while efficiently assisting users when problems arise.

DEVICE SECURITY PROTECTS DATA AND PRIVACY IN CASE OF THEFT OR LOSS

Remotely lock and wipe out important data stored on a mobile device to protect privacy or sensitive information.

Back up data from a phone or remotely on the web. Users can access data online from anywhere, or restore data to a new phone.

SIM tracking can locate a lost phone and plot the locations on a map. Track SIM cards inserted and phone calls made to help get a lost phone back.

Contact our experts today to see how we can empower and fortify your mobile workforce at infosec@ironbow.com.