Mobility in the Federal Government
White paper series on how to deliver secure, mobile access anywhere in the world.

The Top Three Requirements for Safe Mobile Computing

by Jacob Vargis

Jacob Vargis is the Chief Mobility Architect for Sybase Federal and has been architecting enterprise information systems for federal agency clients for over 24 years. For the last seven years he has focused on the secure and reliable mobilization of enterprise systems, providing the most remote mobile users with access to information and applications, irrespective of network connectivity, bandwidth or location.

Introduction

Mobile devices are quickly becoming the primary enterprise computing interface. Although this is especially true for the mobile workforce, every user who accesses company emails on a smart phone, or who works from home or on the road, is accessing enterprise resources, retrieving and storing information on mobile devices, and sending or uploading files to enterprise systems.

With advances in wireless technology, smart phones and PDAs are now able to operate on multiple networks, ranging from cellular carrier networks to WiFi hotspots, and they are able to communicate with other devices via peer-to-peer communication, such as Bluetooth.

In addition, the proliferation and convergence of technologies, such as business process automation, mobile application deployment, mobile commerce, mobile banking, and push email, have generated widespread adoption of smart phones and PDAs across virtually all industries. As a result, threats to mobile operating systems are on the increase.

These threats have escalated beyond the inconvenience of a lost or stolen device scenario to more sophisticated, invisible attacks that can intercept sensitive data and cause irreparable harm to mobile devices.

Comprehensive mobile device management and security

Enterprise IT management has become even more complicated as mobile computing has evolved into a plethora of access devices that offer significantly larger storage capacity, support for multiple network connections, and plenty of computing power. Devices like the iPhone and Android, and more recently the extremely popular iPad, are changing the mobile computing landscape in ways that were unimagined just a few years ago.

To further complicate matters, users insist on using their latest "cool" personal device to access enterprise systems and information. This has placed an unusual and increasingly overwhelming burden on IT organizations that typically established standardized configurations for antivirus and firewall protection on a manageable range of approved mobile computers. However, the benefits of supporting personal mobile devices within the enterprise outweigh the infrastructure requirements.

Policies must be deployed to control and manage the secure and reliable use of this broad spectrum of mobile devices that run on a variety of hardware and operating systems. Ensuring that proprietary information is kept secure and isolated from users' personal applications and content, such as music, pictures and contacts, is now a priority.

> *"Enterprises should consider mobile antivirus and firewall protection, for all enterprise-supported mobile operating systems, as part of a holistic mobility security offering that puts IT in central control of all mobile devices and information."*
>
> Sean Ryan
> Research Analyst,
> Mobile Enterprise
> IDC

The top three requirements for safe mobile computing

As IT organizations consider policies for secure mobile computing and remote access to enterprise resources, three general areas of focus for the management and security of enterprise assets emerge:

1. **Securing mobile devices and data**
   - Apply strong authentication to ensure authorized access to devices, applications and data
   - Use antivirus software, firewall, and encryption to protect all data and information
   - Issue and enforce timely updates of OS patches and virus definition files to every device
   - Continuously monitor, detect, block and log new threats or any malicious use of a device
   - Manage and maintain all configuration settings and security modules
   - Review firewall logs for intrusions
2. **Controlling mobile access to enterprise resources**
   - Register all mobile users on the enterprise directory servers
   - Authenticate all devices and mobile users prior to allowing access to enterprise systems and resources
   - Apply, enforce and activate secure network protocols such as VPN, port management, etc.
   - Ensure that all enterprise information is encrypted while in transit
3. **Enabling centralized enterprise IT management of all mobile devices**
   - Deploy and enforce enterprise IT policies and mechanisms
   - Continuously monitor, manage and maintain (update) mobile devices
   - Perform comprehensive enterprise device and application lifecycle management
     - Provision devices centrally and manage all devices from a unified console
     - Manage and apply a common and streamlined set of IT policies for all mobile users
   - Remotely control and assist mobile users
   - Clean devices of all sensitive information if lost or decommissioned

Sybase delivers safe mobile computing

Afaria Antivirus protection secures mobile devices by scanning for malicious content on-demand and on-access. The on-access feature continuously monitors the device and scans all data received by the device. Once harmful content is detected, it alerts the user and offers the option to delete the data or save it. The user may also initiate a scan, using the on-demand feature.

Administrators can control the frequency of updates via a simple menu option. Virus definition files are easily, securely and efficiently downloaded over-the-air to protect mobile devices from the latest threats. And all activity is logged in the application's log files, recording the date and time of any scan, along with any virus activity detected and resolved during a scan, so as to adhere to corporate security policies.

Afaria Antivirus & Firewall protects users from current and future threats by providing filtering and blocking of TCP/IP traffic. Afaria offers a bi-directional port and IP-based packet filtering option that protects the mobile device from accessing harmful or questionable content and prevents malicious content from being transferred to the device.

The firewall monitors cellular data connections, WiFi, and all TCP/IP traffic, blocking and allowing incoming and outgoing data packets. The firewall can also be configured to block/accept traffic from a specific IP address or a range of IP addresses, providing control over all data traffic on all devices. For security audit purposes, the firewall has an activity log that keeps track of changes to the firewall security level and information about any packets that are filtered.

Summary

As mobile devices become pervasive, the benefits for government workers are apparent in immediate user access to information, faster situation response and decision making, and more reactive supply chains. At the same time, risks to security increase dramatically as more information is available to more users in more places. In this rapidly-growing environment, it only makes sense to adopt a comprehensive mobile device management and security solution administered by a central IT organization.

For more information

Go to http://mobilegov.sybase.com

About Sybase

Sybase delivers mission-critical enterprise software to manage, analyze, and mobilize information. Sybase is the first vendor to offer antivirus and firewall protection for handheld devices as part of a comprehensive mobility software suite. Ranked in three Gartner Magic Quadrants for mobile leadership and as the market share leader by IDC, Sybase mobile computing solutions enable a more efficient and secure government.

Sybase Federal

For over 20 years, Sybase has supported the diverse missions of federal government departments and agencies, helping them maximize the value of their data and increase the effectiveness of their services. Government organizations have used Sybase solutions to mobilize supply-management systems, reduce ship inspection times by half, and cut data capture time from days to hours.