



Best Practices for Securing the Mobile Enterprise

February 2004

**CREDANT Technologies
Security Solutions
White Paper**



The Mobile Enterprise

It is no secret that laptop computers improve employee effectiveness. With a simple connection to your network, employees stay in touch and are more productive while on the road. Now, the introduction of smaller “wireless-ready” handheld computers and smartphones has further fueled interest in mobility. Powerful enough to run major corporate applications, these affordable and portable devices allow on-the-go professionals to improve responsiveness, increase productivity and enhance customer relationships.

But increased mobility also means increased risk. Today the majority of mobile devices come “wireless-ready” with built-in support for WLANs, Bluetooth and wireless WAN (WWAN). No longer encumbered by the complexity of connecting to corporate networks and resources, mobile users can more easily access and exchange business information anywhere on a corporate campus, in the field or while traveling. As a result, valuable enterprise data which was once tightly secured within the networked perimeter now resides unprotected on mobile end points, including smartphones, laptops, tablet PCs, and PDAs. Left unsecured, mobile devices are an open door to one of your most valuable corporate assets — information. And because of their size, these devices are easily misplaced, lost or stolen — exposing your organization to legal liability, financial loss and brand damage.

Security threats introduced by mobile devices are forcing organizations to fundamentally change their philosophy of what a secured perimeter is. When organizations only had to worry about protecting physically connected computers from unauthorized access, they quickly added firewalls, anti-virus software, VPNs, and strong authentication to protect their perimeter. However, when you add computing devices that are even smaller than laptops that work completely independent of the network, the job of securing the perimeter becomes more complex. Because these devices are used outside the network’s span of control, they require their own security strategy. To adequately protect your digital assets, you need to expand your secured perimeter to include mobile devices and their wired or wireless connection to your network.

If you think this isn’t a big problem, think again. Companies are adopting mobile and wireless devices into their organization faster than any other platform. Industry analyst firm Gartner predicts that by the year 2007, there will be nearly 120,000 WLAN “hot spot” gateways worldwide, providing access to private and public networks for over 200 million mobile devices used in business. Gartner also predicts that more than 60% of staff in Global 2000 companies will have mobile access to corporate applications and that 40% of corporate data will reside on handheld devices by 2005.

Managing mobility is no longer an option — it is a required component of network security. Your challenge is to determine who is accessing your network, how they are accessing it, and with what type of mobile device. Then you’ll need to figure out how to secure and effectively manage these devices and connectivity options for potentially thousands of users — while keeping costs in line.

Best Practices for Securing the Mobile Enterprise

The best approach is a proactive one. The following strategies will help you develop a plan that includes sound practices, adequate training and the implementation of a security and management framework to expand your secured network perimeter to include mobile devices.

Perform a Risk Assessment

Sound security practices are dictated by the business you are in and the risks you face. And, information security planning begins with understanding the value and sensitivity of the information you store today. Identify where sensitive data is located, who controls it, who and what has access to it, how it is stored and how it is protected. From a mobile device perspective, it is important to understand what information can be stored on mobile devices, even if the organization doesn't officially support them.

Implement a Security Policy for Mobile Devices

Once you have performed a risk assessment, you'll need to implement a security policy for mobile devices. The policy should cover reasonable and prudent security controls that include items such as the types of information that is to be placed on the device; the security configuration of the device, including all software that is to be used to protect enterprise data; and permissible modes of operation, including acceptable wireless connectivity options and use of removable media. In most cases, this will be an extension of your existing security policies to include mobile devices rather than a completely new policy.

Train and Educate Employees

Employees should be made aware of the vulnerabilities of mobile devices and the implications to the company if they fall into the wrong hands. Training should include awareness of the physical security of the device, the mobile device security policy, a review of the types of information that can be stored on the device, and the procedure to follow if a device is lost or stolen.

Implement Strong On-device Security

Many times, sensitive information, such as customer account information, order history, pricing, and product roadmaps, as well as critical access and network credentials, are stored unprotected on mobile devices. To maximize the protection of enterprise data, security should be enforced at all times to ensure the mobile device is protected whether online or off. At the very least, start with a policy that requires user authentication to prevent unauthorized users from obtaining access to the device's functions, applications or network access from the device. Enable fail-safe options that can automatically lock-out access privileges when a user exceeds a certain number of access attempts, as well as more aggressive measures that automatically destroy all applications and data stored on the device.

Unauthorized users can also easily circumvent security by simply removing the device's hard drive or removable media and inserting it in an unprotected device to gain access to the data. To prevent this, encryption policies should be enforced which make the data unreadable and inaccessible by an unauthorized user.

Anti-virus software is commonplace on notebooks and tablet PCs, but should also be used for other mobile devices such as smartphones and PDAs, especially for devices with network connectivity. Note that it is important to check for viruses and update anti-virus definitions whenever a device attempts to connect to an organization's network.

Personal firewall software is also being used more frequently on notebooks and tablets, but should also be required for ALL mobile devices with network connectivity. Even though many mobile devices are not always connected to public networks such as 802.11 hot spots or wireless WAN services from telecommunications carriers, they are susceptible to attacks via open communications ports when they *are* connected and should be protected by a personal firewall.

Control the Use of Employee-Owned Devices

The inexpensive nature of mobile devices enables and encourages staff to bring personal devices into the office and onto the network. This compromises many of the basic assumptions of a sound enterprise security foundation. Control the use of employee-owned devices and the flow of enterprise data to them by detecting and blocking the use of personal devices or auto-provisioning security software and user policies to ensure they are protected at all times.

Authenticate Users and Devices Prior to Granting Access to Enterprise Data

Synchronization software can be used to easily transfer large amounts of sensitive data from an unattended desktop computer to a mobile device. To prevent malicious synchronization, manage synchronization activities through security policies that enforce authentication and control where users can synchronize.

To prevent rogue attacks at points of entry to corporate LANs behind the firewall, network authentication should be enforced for all connectivity to the network. It is increasingly important to authenticate that it is an authorized user AND an authorized device which includes up-to-date security software before granting access to the network. The check for an authorized user and an authorized device needs to be done for all devices which connect to the corporate network, including those connecting via a VPN from outside the organization as well as those connecting via a WLAN within the organization.

Centralize Policy Administration and Enforce with Software

When it comes to policy enforcement, compliance remains the responsibility of the security office. Many times, security safeguards such as passwords and data encryption are circumvented by a hard reset of PDAs and smartphones; this action automatically resets the device to the factory default settings, which do not include security. Implement policy-based software to ensure that the measures you put in place to safeguard the privacy of sensitive information is not defeated. Be sure the

security software can monitor, audit and report vital statistics about each user's network access to validate compliance with security policies.

To ease the burden and costs of administering potentially thousands of mobile devices across multiple mobile operating systems, policy administration should be centralized and automated. Use software that will automate the distribution of security software and policies as they are defined for new users or updated to ensure ongoing compliance — even in the event of an intended hard reset. Ideally, mobile security policies should be integrated with an enterprise directory, such as Microsoft Active Directory, allowing consistency across all corporate systems. These best practices ensure a base level of security on all systems and greatly simplify administration by eliminating the need to update multiple systems each time a change in employment status is made.

Control the Flow and Secure Information in Flight

Many mobile devices are shipped “wireless-ready” and support communication options such as infrared beaming, Bluetooth, WLAN and wireless WAN. Be sure that only safe, authorized communication mechanisms are used. Establish controls as to when, where and how an employee can communicate when using mobile devices.

Given the security risks associated with information traveling over the public Internet, be sure to protect enterprise data as it is transmitted to and from the enterprise network using link-level encryption such as Secure Socket Layer (SSL) or Virtual Private Network (VPN) technology.

Balance Accessibility of Information with Security

User acceptance of security policies for mobile devices requires a delicate balance of security and accessibility of information. To allow continuity of business functions, on-device security controls should be transparent to the user and should not hinder productivity. For example, encryption and decryption of databases or folders containing sensitive information should occur in real-time and when requested to reduce the impact on the user. And, be sure an authorized administrator can recover encrypted databases or files in the event an employee leaves the company. Users who forget his/her password should not have to depend on a call to the Help Desk or connectivity to the network to obtain access to the device's functions. Use software that ensures business continuity, as well as eases Help Desk calls by allowing an authorized user to reset his/her PIN and/or password, whether connected to the network or not.

Ensuring that a user can always be productive, even in the event of a catastrophic failure, is especially important for mobile devices that are used by remote workers. While notebooks and tablets are very reliable, PDAs and smartphones can become useless to an employee if their battery runs down and important enterprise-specific applications and data are lost. Automated backup and recovery solutions should be in place to enable workers to continue to work with a minimum of disruption if their battery runs down or if the device locks up and a hard reset is required.

Conclusion

Mobility marks the next new wave of computing. The demand is real, the technology is here and the benefits are great. However, new security threats introduced by mobile devices and anytime, anywhere access to corporate networks are eroding the secured networked perimeter, dictating a change in the fundamental philosophy of enterprise security and how you protect your digital assets. As you mobilize employees, address this new computing paradigm by effectively extending your networked perimeter to include mobile devices and their wired or wireless connections to your network. With 120,000 WLAN "hot spots" predicted to provide network access to more than 200 million mobile business devices by 2007, managing and securing mobility is no longer an option. To adequately protect your most important business asset – information – expand your secured perimeter to include mobile and wireless devices.

CREDANT Technologies is the market leader in providing software that enables you to control security enterprise-wide for your mobile and wireless workers. Supporting notebooks, tablet PCs, PDAs and smartphones, CREDANT's award-winning security and management software platform provides end-to-end security for the mobile ecosystem, making it safe for you to use mobile and wireless technologies to increase employee productivity. If you're looking to secure your most valuable business asset – information – on the device, over-the-air, and/or into the network from rogue mobile devices, CREDANT can help.

Contact us

For more information on how CREDANT can help meet your mobile security and management needs, please contact us:

1-866-CREDANT (273-3268) or 972-458-5400

www.credant.com

info@CREDANT.com

Disclaimer: This white paper is not intended to take the place of informed legal counsel. The information and recommendations contained herein are for informational purposes only, and should be expanded upon by trusted legal sources. For specific advice about formulating an information security policy that is compliant with current laws and regulations, or for further information about complying with information security laws, it is recommended that you seek professional counsel.

Copyright © 2004 CREDANT Technologies, Inc. All rights reserved.

CREDANT, CREDANT Technologies, Be mobile. Be secure., and the CREDANT logo are registered trademarks of CREDANT Technologies, Inc. All other trademarks used herein are the property of their respective owners and are used for identification purposes only.