Windows Mobile Device Management and Security Solutions Guide

White Paper

Published: October 2006

For the latest information, please see http://www.microsoft.com/windowsmobile/

Abstract

As mobile devices have become increasingly common and powerful, companies have come to rely on them more and more. Because mobile devices share many of the same characteristics of desktop systems, there is growing interest in management solutions that can provide the same degree of assurance for asset management, inventory, and protection for mobile devices. Microsoft's partners offer a wide range of solutions that provide device management and security functionality for Windows Mobile devices. This guide describes and categorizes these solutions.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Microsoft, Active Sync, Outlook, Windows, Windows Mobile, Windows Server, and the Windows logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

Introduction

As mobile devices have become increasingly common and powerful, companies have come to rely on them more and more. At the same time, companies also face a much broader landscape of security threats than they did in the past. Because mobile devices combine powerful capabilities with small form factors that are easily stolen or lost, protecting the information on these devices has become a priority for many organizations. In addition, efforts to reduce IT management costs have led to widespread deployment of desktop management solutions. Because mobile devices share many of the same characteristics of desktop systems, there is growing interest in management solutions that can provide the same degree of assurance for asset management, inventory, and protection for mobile devices.

This paper describes some of the key device management and security challenges that organizations face; highlights individual technology areas that can help meet these challenges; and describes solutions from Microsoft partners to provide improved device management and security functionality.

Device Management and Security Challenges

The power and capability of mobile devices is steadily increasing, powered both by improvements in semiconductor technology and enhancements to the operating system software that these devices run. These increases have been matched by business pressures to encourage individual workers to use mobile devices as an alternate means of getting work done. In the past, mobile devices have had limited capacity for doing “office-style” work like editing documents, giving presentations, and working with complex e-mail messages. Now these activities have become commonplace, leading to a steady rise in the number of devices deployed, the volume of data stored on them, and the sensitivity and importance of these data.

Organizations that use mobile devices as part of their computing infrastructure face some specific challenges:

- Mobile devices are small and easy to lose. Because these devices are small, they are often lost, misplaced, or stolen. For example, the London Underground estimates that approximately 100,000 mobile devices are found in tube trains each year. Some of these devices are returned to their rightful owners, many are not.
- Mobile devices can hold large amounts of data. It’s now common for mobile devices to have at least 64 MB of RAM. That’s enough to store several dozen e-mail messages, several hundred contacts, and several hundred calendar appointments. Most devices now have some sort of expansion slot that can accommodate removable storage cards. These cards come in capacities up to 8 GB, meaning a single lost mobile device can potentially expose as much data as a lost laptop would have four or five years ago.
- Mobile devices may not participate in the organization’s security management infrastructure. At many organizations, the initial deployment of mobile devices was to executives or other business decision-makers who had sufficient influence to push such deployments through. This led to fairly small deployments and correspondingly little reason to push for separate mobile device management solutions. As mobile devices have increased in power and decreased in cost, they have become much more common. This has compelled organizations to seek management solutions that incorporate mobile devices as well as desktop systems and servers.
- Users may co-mingle personal and corporate data on their mobile devices. For devices that act as mobile phones, users often want to access corporate e-mail systems while still retaining access to their personal contact and calendar data. This creates difficulties in separating corporate information, which must be protected

according to one set of rules, and users’ personal data, which may have different protection requirements.

While Microsoft has built functionality into the Windows Mobile operating system family to address some of these concerns, third-party vendors have introduced solutions that provide broader device security and management capabilities that address these challenges in varying ways. We can broadly separate these capabilities into two categories: device management and security. Device management capabilities include the ability to see which devices are connected; control which devices may connect and synchronize data with servers; track individual devices; maintain an inventory of existing devices; and provide other management capabilities including remote device control and monitoring. Security capabilities include the ability to set and enforce password policies; encrypt some or all data on the device (including removable storage); restrict the use of device peripherals like Bluetooth connections and onboard cameras; and restrict users from modifying or subverting security policies. Some of the products described in this paper provide both device management and security capabilities, while others focus on one area or the other.

Device Management Capabilities

Device management usually refers to the process of inventorying, monitoring, and managing computing devices. Historically these management tasks have primarily been directed at servers and desktop or laptop computers. Increasing mobile device deployment has led to a corresponding rise in interest about device management for mobile computing devices. The features of mobile device management solutions correspond fairly well to the capabilities of traditional device management products. However, there are some key differences caused by the nature of mobile devices, their connections to the network, and the difference in operating system permissions and privileges between desktop and mobile products.

Network Usage and Support

Mobile devices can commonly be connected in one of two ways: they can be tethered to a desktop computer, or they can connect using a wireless network. Different types of devices may be connected differently, and even within one company it's common for different users to use different connection methods. For example, a company with operations both in North America and Europe will probably have a mix of users using CDMA cell phones from US carriers like Verizon and Sprint and GSM carriers like T-Mobile, Orange, and Cingular. The speed, reliability, latency, and availability of carrier-provided wireless networks will vary from location to location. In addition, the wireless coverage plans purchased by the company for their devices may dictate how often employees are able to use data connections with their devices.

These factors influence the capabilities of device management packages. Most device management solutions assume a permanent existence of connectivity; that is, they assume that the device can contact a centralized policy server at any time to receive policy updates, software updates, or diagnostic or remote control commands or information. Some solutions offer full functionality through wireless over-the-air (OTA) connections, while others reserve some functionality for use only with managed devices connected by a cradle or cable to a desktop computer. An increasingly common approach is to allow offline management actions to take place, with results of operations like configuration changes, application installation, or changes to files or folders recorded in a log that is played back to the management software when the device is reconnected. Most device management products assume the existence of IP network connectivity between the management server and the device, although some can communicate using SMS messages. Most products use proprietary network protocols, sometimes tunneled over HTTP+SSL connections. An emerging class of products uses Web services and XML-based protocols, allowing integration with other management solutions, line of business applications, and other infrastructure components.

Server Deployment

Almost all mobile device management solutions require the deployment of at least one centralized server to run management software. While scalability varies, most products can handle thousands of devices from a single server, although additional servers may be required for high availability, load balancing, load distribution, or complicated topologies. In general, device management products use Microsoft SQL Server for logging, and some also use it for policy storage. Organizations that already have SQL Server deployed may be able to use existing database resources to host databases required for device management.

The number, configuration, and roles of servers required for device management can vary widely between products. As part of your evaluation process, you should consider not only the per-device cost of the solution but also what cost server requirements will add to the deployment. A few products rely only on agents installed on the mobile device, with no centralized server required. These may be appropriate for environments where centralized server deployment is not possible or is too expensive.

Directory Access

There are two prevailing models for mobile device deployment based on user identity. In the most common model, a device “belongs” to an individual user, and should be associated with that user’s identity so that policies can correctly be applied based on that identity. The other model decouples user identity from specific devices with a “pool” model, in which devices are assigned to specific locations or job roles.

Much of the value of device management comes from being able to associate a user account (and the permissions associated with it) with a specific device. This association lets administrators control what software is installed, what device features are enabled, and what the device user can do, based on who the user is. There are several ways that mobile device management applications can use information from an enterprise directory like Windows Active Directory:

- Users can be required to log on to their mobile device using their directory credentials. This enforces the strong binding between an individual user and a specific device.
- The management suite can import from or synchronize with the enterprise directory. This gives the suite updated information about which users exist, what groups they belong to, and what roles they occupy.
- Users may be granted or denied access to individual features or software applications on the mobile device based on their directory identity or group membership.
- Users may be granted or denied access to synchronization, control, or management services (like remote password resets, remote software installation, or backup services) based on their account identity.

Some management products support Active Directory, allowing administrators to define policies in terms of which Active Directory groups should receive them, and to dynamically update policies when group memberships change. However, most device management products rely on Active Directory for authenticating the device management administrators and providing a list of users and groups to whom policies may be assigned.

Inventory

Hardware inventory has been a major feature of desktop management systems for some time. IT administrators welcome the ability to automatically discover connected devices and keep track of their configuration and software loads. Some of the same capabilities exist in mobile device management solutions. Generally, the inventory process begins when the management agent is installed on the mobile device; the agent provides information (usually including a unique device ID and a list of installed software packages) to the management server’s inventory component. Some inventory systems include the ability to track devices by class. Administrators can define classes of devices and apply policy by class of device.

There are some useful mobile device-specific features offered by vendors in this space, including the ability to inventory specific Subscriber Identity Modules (SIMs) in wireless devices, the ability to use the device’s mobile network identifier as a unique key, and the ability to remotely back up and restore device contents over the air.

Device Provisioning

For small numbers of devices, mobile device deployment may seem simple. However, for larger deployments, the logistics of provisioning new devices can quickly become complicated and costly. The process of provisioning new devices can include setting up the device with a synchronization relationship, pre-loading software, creating an entry in the management system for the new device, and loading the correct set of policies for the device and user.

Some device management tools allow complete over-the-air provisioning, so a user with a new device has only to visit a Web page to have their device provisioned. More commonly, companies use the features of their device management suite to create a set of packages that install the device management client and other software applications that have to be preloaded. Users can obtain these packages by downloading them over the air, installing them over a tethered synchronization connection, or installing them from a removable storage card. In either case, provisioning usually requires the installation of the device management client, which then downloads software, settings, and policy information.

A related step is linking the device to a particular user in Active Directory. Device management products that uses Active Directory for device provisioning can automatically choose the policy and software to be applied based on the user’s identity. Some solutions that require the user to log in to the device using Active Directory credentials can also automatically register an association between the device and the user, although generally this must be done manually by the device management administrator.

Software Installation

One persistent challenge for both desktop and mobile device management is ensuring that the correct software is loaded, and that users don’t install or run unwanted or unauthorized programs. Mobile device management solutions usually address this challenge by providing a way to couple the inventory of what software items are installed with controls for restricting software installation.

Some solutions add the ability to create lists of approved or blocked applications. Alternately, they may create standardized software images (either as true images or sets of installation packages) that can be used to install a uniform set of software on devices according to policy definitions. Besides installing entire software packages, it is often useful to push scripts or registry settings to devices using the same tools as for software distribution. Some device management tools offer this capability.

Another valuable capability is the ability to utilize mobile devices with Microsoft Systems Management Server (SMS). This allows administrators to use the same monitoring, control, and reporting tools for desktop, server, and mobile computing resources.

Image Distribution and Updating

A few packages offer the ability to clone the contents and configuration of one device to other identical hardware. This is a useful capability for recovering a failed or lost device, and it’s also useful for quickly rolling out a standardized device image. Device management solutions usually support one of two approaches:

- Creating and managing complete device images that replace the entire contents of a device with a cloned image (much like desktop tools such as Symantec Ghost and Acronis True Image do).
- Building and managing a prepackaged set of files, settings, and policies that brings the device contents to a standardized level when installed.

It is important to note that some solutions have the ability to send and apply an image to a device completely over the air, while others require the user to initiate a device restore.

Cloning and imaging operations support backup and recovery functionality so that a device's precise state can be captured as a backup, then restored in case of a lost or failed device. However, some products separate these functions.

Troubleshooting and Diagnostic Tools

Remote diagnostics are particularly useful for mobile devices because the devices are often inaccessible to traditional support channels. Diagnostic tools can be used to gather data about the remote device's configuration, performance, and status. This information is very valuable for identifying problems, particularly when combined with strong logging and reporting functionality.

Troubleshooting tools may include the ability to remotely monitor device parameters, including battery life, memory usage, running processes, and installed programs, either instantaneously or over a set time period. These tools may create their own logs on the device, or they may send logs to a centralized collection point on the management server.

The on-device management agent may be able to respond to log requests from the management server, in which case an administrator can ask for logs from a specific device when needed. Agents that don't support this functionality usually require the user or administrator to manually enable logging.

Policy Application

The ability to define a policy that controls what a user can do with a given device is an important part of device management. Policies may govern all the device management features discussed earlier in this section, and they may extend to additional areas. For example, some device management tools enable administrators to create policies that control which users can receive remote-control support or even which users can override or turn off policy application on their devices.

The key policy-related items to look for in a device management suite are:

- The granularity with which policies can be defined; by user, by Active Directory group membership, and by device type are common granularities.
- Whether policies are automatically pushed to the device and refreshed periodically.
- Whether there is a way to identify (and potentially block) devices that have not accepted policy updates or don't have the correct policy applied.
- Whether administrators or users can exempt devices or users from policy applications.

Logging and Reporting

Administrators often depend on logging and reporting functionality in their desktop/server management solutions to keep track of what changes have been, or are being, made to managed systems. Logging and reporting functionality is one area where mobile device management packages can vary significantly in capability. Almost every package has the ability to log management actions (like device provisioning, software installation, and policy changes) to a log file of some kind. Some products allow administrators to choose where logs are kept, and some are expressly designed to have their log file data imported into, and managed by, third-party logging products.

Reporting tools may have both the ability to create ad-hoc, on-demand reports and to run scheduled reports. A few device management solutions provide real-time reporting, although this is fairly unusual. Most device management tools provide a way to view graphical reports, if only through exporting data to external tools.

Report data aggregation is an important feature for large enterprises. The ability to “roll up” data and view summaries of data collected by arbitrary grouping is very useful in such environments.

Remote Control and Administration

Desktop support has been eased by the existence of tools that let a support professional remotely view, and control, the end user’s machine. This greatly reduces the difficulty of figuring out what’s wrong and how to effectively fix it. Some device management solutions include similar functionality so that a support technician can take control over a device and operate it remotely, using a local screen and keyboard to control the device as though they had it locally.

In addition to traditional remote control functionality, many device management solutions include tools for remotely sending files, scripts, or registry keys to a remote device. These tools may be used for remote device control or provisioning, or as part of troubleshooting and repair efforts.

Security Capabilities

Physical security is probably the most important single security aspect of mobile devices. Because it's difficult to ensure continuous physical security of most mobile devices, software-based security measures are gaining in importance. Security capabilities can be broadly separated into three areas: confidentiality, integrity, and availability. Most existing mobile device security solutions focus on providing integrity and confidentiality. Availability provision is usually included as a device management capability.

Confidentiality includes the ability to encrypt data on the device, and to recover encryption keys if they're lost or damaged. It also includes measures that protect against inadvertent disclosure of confidential information, including features that limit access to or destroy data when it is at risk of compromise. Integrity functions for mobile devices are mostly limited to the application of digital signatures to ensure the integrity of software or policies being pushed to the device. (Windows Mobile 5.0 includes the ability to send and receive e-mail messages protected with the S/MIME encryption standard, which provides both confidentiality and integrity protection.)

Device Encryption

The ability to encrypt data stored on mobile devices is an often-requested feature. Companies rightly worry that when sensitive data is placed on these devices the data becomes more vulnerable to loss or disclosure. There are several interrelated issues that affect the usefulness of on-device encryption:

- Whether encryption applies only to data items in the device's internal storage, or whether removable storage cards can be encrypted too. For products that support encryption of removable storage, it's also important to consider whether the card can be read or recovered in another device (including desktop or laptop computers) or whether it's bound irrevocably to the device where it was encrypted.
- Whether data can be encrypted on the user's device without user intervention, and whether users can opt out of encryption policies.
- Whether the user or the administrator can select which data items are encrypted; some organizations want to encrypt all data on the device, while others might wish to allow personal contacts or other information to remain unencrypted.
- Which data encryption algorithms can be used to protect data. Some algorithms are stronger, more mature, or more widely deployed than others.
- Whether the algorithm implementations have been certified or tested by an independent body. The Federal Information Processing Standard (FIPS) 140-2 certification is widely accepted in the security community because it indicates that a cryptographic implementation has been rigorously tested for security and correct implementation.

Key Escrow and Recovery

Many organizations have resisted the use of computer and device encryption because they are concerned that they might lose access to critical data if the encryption keys are lost or compromised. Key escrow and recovery systems address this concern by storing an additional copy of the keys used to encrypt data in a manner that allow the keys (and thus the data) to be recovered by authorized administrators. Implementations of this feature can vary widely in ease of use, security, and capability. Some mobile device security products provide tools that allow users to recover their own encryption keys, but most require an administrator to participate in the recovery. A hybrid approach is to provide a challenge/response system, where the device user contacts the administrator and receives a challenge string generated by the security tool, and then runs a program on the device that produces a response. If the proper response is generated, the key can be recovered from storage on the server.

Windows Mobile Messaging and Security Feature Pack

Devices based on the Windows Mobile 5.0 operating system with the Messaging and Security Feature Pack (MSFP) support security policies that can be pushed from an Exchange 2003 or Exchange 2007 server to the device. These policies can control whether the device locks itself after a period of inactivity, whether the user must use a PIN to unlock the device, and what the length and composition of the PIN must be. The MSFP also provides a way for administrators to remotely erase a lost or stolen device that is still connected to a wireless network. However, some device management and security solutions either replace or extend the MSFP policy mechanism to add extended security policy capabilities.

Lockout

Many organizations want to be able to lock devices after a set period of inactivity or after a preset number of incorrect PIN attempts. This helps protect sensitive data if a device is lost or stolen. Besides specifying lockout-related settings like whether a PIN is required and how long the device can remain inactive before it's automatically locked, many security software manufacturers provide additional controls that govern what happens when the device is locked. Some tools restrict access to all applications on the device, while others allow unauthenticated users to make and/or receive calls or run specified applications on the device.

Lockout recovery is the flip side of this feature set: once a device is locked, legitimate users need a way to unlock it. Some systems support remote unlocking either using an additional "super" PIN or a challenge/response protocol similar to those used for key recovery. A few require the locked device to be cradled or tethered to be unlocked.

Data Destruction

Under some circumstances, it may be desirable to erase data from a device. For example, if a device is confirmed as lost or stolen, it's probably best to erase its contents to prevent an attacker from gaining access to sensitive data. Some organizations also prefer to have devices erased after a preset number of consecutive incorrect PIN entries. Windows Mobile with the MSFP supports both remote and local device erasure. However, the contents of removable storage cards aren't erased.

Third-party solutions can extend this behavior to ensure that either all or selected data are erased from the device. For example, some products have a means for administrators to erase only unencrypted data, while others allow a remote "fading" operation that restricts access to data on a suspect device without completely erasing it.

Partner Profiles

The summary material in this section was provided by each vendor. Microsoft does not recommend or endorse particular solutions.

B2M

B2M's (www.b2m-solutions.com) mprodigy product line provides facilities that enable administrators to minimize their support costs, keep mobile devices operational, and understand where and how mobile assets are being used. mprodigy combines device management, asset management, communications management, supplier management, and application monitoring functionality that ensures that mobile equipment requires the absolute minimum of operational maintenance. With mprodigy's recovery functionality, mprodigy-equipped devices can often recover from situations in the field that would normally require a return to base.

mprodigy is designed for blue collar and industrial markets. Typical customers include Lynx Express, one of the largest parcel carriers in the UK. They have over 1000 devices managed by mprodigy, both within their depots and used by their delivery agents "on the road".

Unlike most competing products, mprodigy has been designed from the ground up to scale to enterprise size deployments of tens of thousands of mobile devices. mprodigy manages Windows CE based devices only. We do not attempt to manage Windows laptops or desktops, and consequently have not had to shoehorn facilities and capabilities that are really designed for fixed LAN environments into mobile operations. Our competitors' products are often designed for the SME market, where issues or scalability and robustness are less critical.

BeCrypt

BeCrypt (www.becrypt.com) specializes in producing security products for laptops, Tablet PCs, and desktops, as well as for Pocket PC/Windows Mobile 5 PDA devices. Our products include full-volume disk encryption for Windows 2000, Windows XP, and Windows Server 2003, and encryption, security-enhanced erasure, and device control of wireless devices and their peripherals. BeCrypt's products are accredited for government use. Major customers include BAe Systems, Thales, the United Kingdom Ministry of Defense, Bechtel, and Bombardier.

BeCrypt's products are designed to offer simple solutions to specific threats, and they're designed for security first. BeCrypt's products focus on providing government-accredited security for data "at rest", relying on device management solutions like iAnywhere's Afaria and Microsoft Systems Management Server for distribution and installation. Unique features of BeCrypt's solution include its ability to encrypt data on removable storage cards and to provide robust, security-enhanced tools to let authorized administrators recover encrypted data when needed.

Bluefire Security Technologies, Inc.

The Bluefire (www.bluefiresecurity.com) Mobile Security Suite is a comprehensive suite of products that work together to help secure mobile devices. This patented technology allows the implementation of a rich set of security features with a single solution. The features , include: On-device firewall, intrusion prevention and detection, managed authentication, data encryption, integrity management, and centralized policy management and reporting. Major customers include Bank of America, the US Federal Government, Motorola, and Johns Hopkins Medical Center.

The Bluefire Security Suite was developed on the premise that CIO's want to enforce the same level of security policy currently mandated on desktops and laptops, on mobile devices connected to the network. With Bluefire Mobile Security Suite this goal is achieved. Enterprise data is protected on multiple levels:

- Authentication: Enforces power-on PIN or strong password requirements.
- Data Encryption protects data stored in security-enhanced folders on the device and on removable storage cards with AES 128-bit encryption that complies with Federal Information Processing Standards (FIPS) 140-2 policy. A "logout and encrypt" feature can be invoked to automatically encrypt data at power-off.
- Integrity Manager monitors core system assets and automatically alerts the user of an integrity violation on the device. The Integrity Manager can be set to actively alert and log events, and/or to quarantine the device by blocking all incoming and outgoing network communication.
- Intrusion Detection scans inbound network packets to identify and prohibit electronic attacks such as LAND.
- Real-time Logging captures and retains detailed logs of security events such as successful and invalid login attempts, password resets, quarantine overrides, port scans, firewall security level changes and integrity violations. Controllable at the administrator level, administrators can determine device usage by choosing to log all network traffic to the device.
- The on-device firewall filters traffic to the device in compliance with administrator-controlled port and protocol policies via an integrated LAN/WAN firewall.
- Bluefire is tested for compatibility with all Major AntiVirus solutions, and device management consoles..
- The Bluefire IPsec VPN client allows mobile devices secure access to corporate data protected by thew company VPN Network. The Bluefire VPN client is certified for use with both Cisco and Nortel VPN equipment.

Credant

Credant's Mobile Guardian line of products provides enterprise-grade centralized security policy management for access control and data encryption for desktops, laptops, tablets and mobile devices. Credant's major customers include the International Monetary Fund, the US Department of Homeland Security, the US Army, and large financial, manufacturing and healthcare companies.

CMG provides granular control of access, encryption policy, application whitelisting and blacklisting, and key device control. Other products in the encryption space have an "all or nothing" approach to encryption, which makes them difficult to manage and use. Credant's CMG is transparent to the end user and won't interfere with how users interact with their data. Administrators can specify file types and locations, such as the SD card, that should always (or never) be encrypted. The encryption keys are automatically escrowed on the management server for recoverability in case of data or device loss.

CMG also allows security administrators to restrict which programs can run on the device and which device types (including Bluetooth devices, removable storage cards, infrared, and network connections) are available. By blocking unapproved applications, organizations can block the use of on-device cameras or other hardware devices. Additionally, organizations can restrict rouge devices from accessing the Exchange server, through an optional over-the –air sync control feature.

Credant's server-based management console can handle over 100,000 mixed devices (including Windows Mobile, Windows 2000/XP, BlackBerry, Palm, and Symbian) from a single management server.

Access control and policy settings can be driven by Active Directory so that software installation and policy updates are based on user identity. Administrators have access to a flexible role-based security toolset that allows delegation of administrative access to allow large-scale management while still retaining separation of duties.

CMG's protective functions are combined with software installation, automatic policy updates, Web-based reporting, and support for multiple device types from a single set of policies.

iAnywhere

iAnywhere (www.ianywhere.com) is a subsidiary of Sybase. Their primary product, the Afaria management suite, provides comprehensive management capabilities that overcome the challenges of maintaining the reliability and security of data and devices that are widely dispersed in remote locations. Acknowledged as a market leader in mobile device management by leading industry analysts such as IDC and Gartner, iAnywhere's Afaria technology has been proven in hundreds of large mobile enterprise deployments throughout the world.

With Afaria, administrators gain the level of control and visibility required to proactively manage and apply security to multiple device types, applications, data and communications critical to frontline success, regardless of the bandwidth available. Afaria uniquely combines management and security into a single console, providing the best protection against security threats and compliance issues. Unlike competing products, Afaria combines security and management to deliver an overall device management framework with an easy-to-use, wizard-based interface that makes devices "self-managing" without extensive helpdesk assistance.

Afaria's policy management engine extends beyond software management to manage business policies; for example, Afaria can verify and enforce that certain business forms or content are present on devices that are authorized to use that content. In addition, Afaria supports Microsoft SMS so that it can be used to manage Windows desktop and server platforms, as well as handheld devices on non-Windows platforms.

Odyssey

Odyssey's (www.odysseysoftware.com) Athena product is a device management solution that provides comprehensive management for Windows Mobile, Windows CE, Win32 and Windows XP embedded devices. Athena takes full advantage of the Windows platform to provide complete device management without requiring a centralized server, using an extensible set of open, standards-based interfaces that can easily be used with other line-of-business and management applications. Athena allows administrators to remotely manage devices from any browser-equipped Internet workstation, or work with preexisting consoles such as Microsoft SMS 2003.

Odyssey's focus on the Windows platform results in better functionality and capability with lower device resource usage than competing solutions. Among Athena's unique features are its Messenger service, which allows helpdesk personnel or administrators to send messages that users must acknowledge; its open architecture, which makes it possible to consume Athena data through almost any XML-aware application; its extensive Windows-based feature set; and its custom plug-in architecture, which provides XML-based remote access to any on-device function or API.

Perlego

The Perlego Mobile Device Lifecycle Management (MDLM) suite provides remote control, data assurance, and content distribution tools to protect and manage devices and their data throughout their lifecycle, from deployment through service to termination/transfer. The MDLM suite includes a centralized web-based management console, wireless remote control (including device wipe), backup and restore, and customized, policy-based content distribution.

Perlego's architecture allows multiple delegations of authority, giving both mobile carriers and enterprises an effective way to deliver multi-tier device management. MDLM is agnostic to device, operating system and carrier network, providing an economical per-device subscription plan that comprises the software and service cost. In addition, Perlego is available as a hosted service that requires no customer deployment; managed mobile devices can be provisioned over the air and managed by Perlego's administrative staff. For more information, please visit www.perlego.com

Pointsec

Pointsec (www.pointsec.com) produces a full line of disk and data encryption products for Windows-based computers, Windows Mobile handheld devices, removable media, Symbian- and Palm-based handhelds, and Linux systems. The Pointsec Wireless product provides full-device encryption for Windows Mobile-based handhelds. Pointsec has been a long and consistent player in the data protection market, having been placed in the leader quadrant of Gartner's Mobile Data Protection Magic Quadrant for over six years.

Pointsec features encryption algorithm implementations that are certified to the US FIPS 140-2 standards, with complete on-the-fly encryption to protect data on the device at all times. Encrypted data is only decrypted when it's read by an application, and as soon as data is written by any application on the device it's encrypted. Administrators can choose whether removable storage cards are encrypted; if there is no central policy requiring such encryption, users can still enable it. Any encrypted storage card can be read on a Pointsec protected PC. Key recovery uses a challenge/response system that requires cooperation between the user and the helpdesk or administrative staff. Helpdesk personnel are able to support password reset operations through the Pointsec webRH web-based remote help system.

Pointsec extends the native Windows Mobile authentication mechanism to use Picture PINs, a unique method of specifying PINs using images rather than text or keyboard input. Administrators can also choose to allow a shortened PIN entry when a device has only been inactive for a short time, allowing easier use of long PINs for longer periods.

Pointsec's solution takes advantage of third-party software distribution and installation tools to deliver the client application to the device; Pointsec supports the OMA device management standard and provides an API that on-device applications can use to ensure seamless interoperability.

SOTI

SOTI's (www.soti.com) MobiControl product provides centralized management, full support and helpdesk capabilities, and software/data distribution through OTA, wired and WiFi connections. These capabilities are controlled by an integrated, role-based security system that allows administrators to remotely control, manage and apply security to remote devices from a single centralized management interface.

MobiControl also offers a broad range of remote control and diagnostic functionality, including full-fidelity remote screen interface, remote command-line capability, remote registry editing, device image differencing, messaging and extensive logging capabilities. MobiControl's device lockdown functionality can be used to restrict user access on mobile devices and effectively manage access rights on an individual or group level. Built-in reporting tools facilitate asset tracking through standard and customizable reports. The solution has a scalable and fault tolerant architecture, equally adept to small and large deployments of mobile devices.

MobiControl supports all Windows Mobile devices, including Pocket PC, Smartphone, CE .NET, as well as Windows 2000/2003/XP/Tablet PC operating systems. These features are combined in a powerful, easy-to-use interface. SOTI makes a full version of the product available as a trial download from their website (www.soti.net).

Synchronica

Synchronica (www.synchronica.com) is focused on mobile device management and synchronization solutions. Its product portfolio covers over-the-air device management, firmware update, push e-mail, and personal information management (PIM) synchronization for a wide range of mobile devices. Synchronica is a key participant in the Open Mobile Alliance (OMA) and has millions of devices in service with customers including Nextel, Orange, Cingular, Motorola, and Siemens, as well as hundreds of SMEs and large corporates.

Synchronica’s flagship product, Mobile Manager, is a widely deployed and proven Enterprise Device Management (EDM) solution that has been designed exclusively for managing mobile devices in the enterprise. Its feature-set spans the entire life-cycle, including device provisioning, monitoring, configuration backup & restore, diagnostics and repair as well as security with a number of unique features, such as the “Scream” capability for lost or stolen devices.

Enterprises can use Mobile Manager to assist the rollout of Smartphones, with provisioning of ActiveSync, GPRS, and VPN connectivity as well as certificates and registry settings. It supports the installation and removal of applications, as well as distribution of documents to individuals or a group of devices. Mobile Manager addresses support issues with remote diagnosis and monitoring features enabling the help desk to inspect and repair device configuration issues, even if the user is out of the office. For securing mobile devices in the event they get lost or stolen, Mobile Manager enables an administrator to erase all data (internal memory and removable media), lock the device and SIM card to prevent unauthorized usage and activate a “Scream” alerting of the device theft.

Mobile Manager supports remote device management of individual devices, as well as query and rollout to groups of devices. A set of applications, documents, certificates, and settings can be saved as a pre-canned “Package” enabling efficient activation of new devices, bringing them to a standardized state. Packages can be applied over-the-air or saved on a removable memory card for offline installation. Mobile Manager’s advanced device management and security capabilities require a small, invisible, client (100 kB footprint) on the device, but it also supports basic device management without a client (by using the industry standard OMA DM supported by major device manufacturers).

Device management sessions are initiated over-the-air by SMS trigger, enabling support for GPRS and CDMA networks as well as always-on UMTS and WiFi networks. Communication between client and server is based on efficient and secure HTTP/S communication, with a unique support for fall-back to SMS-based communication in case the device is unable to establish a data connection.

Mobile Manager is built on a mature codebase developed since Synchronica’s founding in 1996. It is based on the latest Microsoft technologies including C# and ASP .NET, incorporating a completely AJAX-based management console, with an easy-to-use web interface that enables remote device management from any PC using a web browser. Thanks to Mobile Manager’s multi-domain support and carrier-grade scalability, it can serve multiple companies with multiple subsidiaries, from a single installation. This is supported by a role-based permission schema with fine-grained access control covering every single application feature. Mobile Manager was designed for use as a hosted service offered by mobile operators and ASPs, but it can also be deployed behind the firewall of an enterprise including support for Active Directory integration.

Trust Digital

Trust Digital offers mobile device and perimeter security solutions. It provides policy-based security for PDAs and smartphones, enabling corporations to reduce the regulatory and financial risks associated with the accidental or malicious disclosure of data as well as ensuring the security of these endpoints accessing the enterprise network. Major customers include Verizon Wireless, the US Air Force, and the US Internal Revenue Service.

Rather than a loose collection of components, the Trust Digital solution provides managed security capabilities for mobile devices, giving enterprises the same security protection for desktops, laptops, and mobile devices. Trust Digital's encryption solutions provide complete on-the-fly encryption with total user transparency. Administrators can create policies to restrict user access to various device resources (including cameras and Bluetooth connections), and the US Department of Defense Common Access Card (CAC) and RSA SecurID are both supported for two-factor authentication systems.