

Overcoming Mobile Enterprise Security Challenges

WHITE PAPER



TABLE OF CONTENTS

Executive Summary	2
Protecting the corporate network and firewall	3
Managing and Limiting access to sensitive corporate data	3
Enabling and Disabling Access to Exchange ActiveSync	3
User Authentication with Active Directory credentials	4
Securing stored data on device and storage media	4
File Encryption for Device Memory and Removable Storage	4
Automatic Time-based Data Fading	4
Multiple Delivery Options for Remote Device Wipe	4
Securing over-the-air communication to protect data in transit	5
Secure and Encrypted File Transfers	5
Virus and malware protection	5
Intrusion Detection	5
Disabling Internet Downloads and Unauthorized Software Installation	6
Limiting end user access to the mobile device	6
Disabling Communication Modules and Hardware Features	6
Device Lockdown and Controlled Web Browsing	6
Securing lost or stolen devices	6
Remote Control functionality for Instant Device Take-over	6
Real-time Device Location Tracking	7
Managing Security for Remote Out-of-Contact devices	7
Cellular Device Management via SMS / Text Messages	7
Auditing and monitoring administrator(s) activity	7
Roles Based Access Control for Securing the Helpdesk Console	7
Conclusion	8

EXECUTIVE SUMMARY

Increasingly powerful feature sets and rich functionality are driving the wide-spread use of mobile devices by banks, security and law enforcement agencies, government authorities and other security conscious organizations. Mobile workforces are taking advantage of mobile devices to remotely access confidential emails, spreadsheets, databases, customer data, order information, credit card data, medical history and patient information among other sensitive corporate data. Mobile devices are now the most vulnerable entry points for malware and other threats to the corporate network to which they are connected. Additionally, mobile devices are increasingly more dispersed geographically and at the forefront of operations in the field. So is sensitive corporate data!

The potential security loopholes are increasing – as are the associated costs and liability! Will the next leak of sensitive information in your organization result from a stolen SD card? Or data transferred out of the device through USB or Bluetooth? Can you ensure that corporate email is being accessed only on authorized mobile devices protected by security policies and not just any device the end user can buy? How quickly can you disable email access for a missing mobile device?

Do you have a strategy to deal with lost or stolen devices? Can you reliably “wipe” the information from a lost device if it does not connect to your server? Will your data be protected in the interim, if device theft is not detected for 24 hours? Can you proactively detect an attempt to install unauthorized software on a device? Can you respond in real-time and take control of the device if it is in the wrong hands? Can you track the location of a stolen device to retrieve it?

Most importantly, can you manage security for all these – and unforeseen – scenarios using only ONE solution, without incurring the cost and hassle of purchasing, deploying and supporting four or five security applications, and making them work well together?

This document helps you answer these questions and examines how to manage end-to-end security by:

- Protecting corporate data in transit over public Wi-Fi and cellular networks
- Encrypting data stored on device, making it available only to authenticated users on your domain
- Disabling device communication modules and hardware features (e.g. camera, Bluetooth)
- Authenticating device users using Active Directory (Domain Security) credentials
- Authenticating mobile device hardware using certificates
- Enabling malware protection and intrusion detection
- Limiting end user’s access, preventing harmful Internet downloads and unauthorized software installation
- Proactively mitigating risk of data loss with efficient strategies for dealing with lost and stolen devices

“Gartner estimates the cost of each unrecovered mobile phone or PDA to be at least \$2,500 because of compromised data.”¹

¹ Gartner’s analyst Jack Heine, cited in “What’s the Cost of Lost Phones and PDAs?” <http://www.techweb.com/wire/story/TWB20010425S0006>

PROTECTING THE CORPORATE NETWORK AND FIREWALL

With mobile users on the go, it is necessary to remotely manage mobile devices as they connect to various public networks (Wi-Fi ‘hot-spots’, cellular networks like GPRS, IDEN, EVDO, etc.) to access email, business information and data. Legacy solutions, designed for managing devices within the four walls, are not equipped to manage these remote devices while protecting the corporate network in an efficient, cost-effective and secure way.

The security goals are:

- Minimizing modification of corporate firewall configuration and integrating with existing security technologies.
- Preventing devices from having unlimited access to the corporate network.
- Ensuring secure, encrypted communication without incurring the overhead of resource-intensive VPN clients.

SOTI MobiControl meets these goals by integrating with existing firewall and security technologies seamlessly, including the Internet Security and Acceleration (ISA) server. The firewall configuration is minimal, requiring only one administrator-selectable TCP port to be forwarded to the server. The server can reside in the demilitarized zone (DMZ) thus limiting access to the corporate network from mobile devices.

To further safeguard the network, the communication between mobile devices and the SOTI MobiControl server utilizes SSL certificates for encrypted and secure end-to-end communication. SOTI MobiControl utilizes the TLS v1.0 Cipher Suites of the Secure Channel (SChannel) Microsoft Security Support Provider (SSP) and SSL Certificates installed on the mobile devices are used for physical device identification and encryption.

SOTI MobiControl meets all these security goals, without the additional expense of purchasing private APNs or static IP addresses from cellular companies and ISPs, due to its superior architecture that does not require the use of static, public IP addresses on mobile devices to manage them. Unlike VPN-based solutions, SOTI MobiControl’s SSL communication does not draw heavily on the mobile device’s limited processing power, battery and memory resources. By eliminating the network traffic overhead associated with VPN, MobiControl maximizes savings due to lower data usage costs over cellular networks.

MANAGING AND LIMITING ACCESS TO SENSITIVE CORPORATE DATA

Wireless ActiveSync – information nightmare? Your IT department has enabled cellular access to corporate email, contacts and calendar through Microsoft Exchange ActiveSync and assured you that IT policies are protecting your mobile device and all emails on the device will be wiped if it is stolen. Your end user walked into the neighborhood electronics store to shop for a new device, and entered their Exchange settings into 3 new devices to compare the attachment viewing capabilities...Stop! Those 3 devices are not covered by IT policies – and cannot be wiped!

Possible solution? Forego the benefits of wireless email? Not acceptable! Hope that those 3 devices will not be bought by malicious users? Not realistic!

Enabling and Disabling Access to Exchange ActiveSync

SOTI MobiControl can remotely and automatically configure the Exchange ActiveSync settings on a mobile device for each user. It has the capability to deliver and install Exchange SSL certificates over-the-air on devices (without the need to physically touch each device) as well as removing certificates from stolen devices to instantly disable cellular email access. The labor and time resources saved due to the automatic configuration (instead of helping each user configure settings individually) are an added bonus!

By making MobiControl-delivered SSL certificates a “pre-requisite” before a device can be configured to receive email, you can ensure that corporate data and emails can be accessed only on devices secured by SOTI MobiControl’s policies.

User Authentication with Active Directory credentials

Most security solutions implement mobile device security using a PIN, which is not linked to your existing Domain Security (i.e. LDAP directory). This makes “one-window” centralized security management difficult as different passwords and multiple user profiles have to be managed, resulting in delays compromising security.

Tracking User Activity. With SOTI MobiControl you can identify mobile users and track user activity by verifying network credentials on a mobile device to ensure that only legitimate users (active and valid on your domain) can gain access to the device. SOTI MobiControl uses a read-only Active Directory lookup to verify the identity of the end user before allowing access to the device. The need for security is balanced against usability by providing an optional user-friendly ‘simplified’ PIN (after successful AD authentication). User credentials are cached in encrypted form on the device to allow working in ‘offline’ mode, when disconnected from the data network.

Using SOTI MobiControl, disabling the end user’s account in Active Directory automatically disables the user’s access to the mobile device as well, allowing unified and centralized management.



SECURING STORED DATA ON DEVICE AND STORAGE MEDIA

The prevalence of removable SD memory cards for storing information means that setting a basic “wipe” policy is no longer adequate protection for corporate data – especially when the wipe delivery is not assured! Data needs to be protected at all times, including the interval that elapses before the loss / theft of a device is detected and reported to IT.

File Encryption for Device Memory and Removable Storage

SOTI MobiControl utilizes FIPS 140-2 validated AES 256-bit algorithms for File Encryption for both on-board storage as well as removable storage cards. On-the-fly encryption is implemented in a transparent manner without impacting the end user’s experience. Encrypted data on a lost or stolen SD card cannot be read by an unauthorized device, thus securing corporate data stored on a card. Real-time key escrow at the time of key generation provides an emergency recovery mechanism (to retrieve data from SD cards in the event of hardware failure).

Automatic Time-based Data Fading

Programming “self-destroy” policies on the device serves as a safeguard against the unforeseen. In the event that a device theft is not detected promptly or the device does not report to the server for an extended interval (e.g. 24 hours), SOTI MobiControl’s device-side policies can automatically encrypt or remove data from specified directories as a precaution.

Multiple Delivery Options for Remote Device Wipe

A false sense of security has been created by numerous solutions claiming to have the ability to ‘wipe’ a stolen device. It is important to evaluate the wipe delivery mechanisms, especially in cases where the missing device may be in a disconnected or ‘offline’ state. Administrators should be wary of solutions that can execute a remote wipe only “when the device is **online** and connected to the VPN”. Such a convenient stolen device scenario is not typical!

Real-world wipe.

MobiControl’s multi-pronged strategy combines multiple wipe delivery modes to ensure success.

Wipe Delivery Options Checklist (for device & storage card)	SOTI MobiControl	Other Solution
On-demand. Deliver instantaneous wipe command for an online device	✓	----
Scheduled. Request a 'wipe-on-sight' action the next time the device appears online	✓	----
Event-based. Multiple incorrect password entry attempts result in wipe of offline device	✓	----
Time-based. Wipe clean 'out-of-contact' offline device if it does not appear online for X hours	✓	----
Conditional. Trigger a wipe of an online / offline device if a particular condition is satisfied	✓	----
SMS / Text Message. Send encrypted SMS message to offline device to 'wake-up' & wipe it	✓	----

SECURING OVER-THE-AIR COMMUNICATION TO PROTECT DATA IN TRANSIT

With Wi-Fi and 3G / HSDPA data capabilities becoming standard fare, a mobile user can connect to a non-secure Internet connection at home, a public Wi-Fi hot-spot at a trade-show, airport or a café during business travel, or a cellular data network while on the road. How can you protect the corporate data which is susceptible to interception and hacking when being transferred over these networks?

Secure and Encrypted File Transfers

SOTI MobiControl uses server-distributed SSL Certificates for secure, encrypted data transfer using SSL / TLS communication. The SOTI MobiControl server limits communication and data transfer only to devices that have a valid certificate installed. This protects sensitive documents and corporate data over-the-air, on any network. Remote delivery and installation of 3rd party security certificates can also be achieved through SOTI MobiControl (e.g. Exchange SSL certificates, WLAN encryption certificates, etc.) to secure communication with other applications.

VIRUS AND MALWARE PROTECTION

Mobile devices without malware safeguards are a vulnerable entry point into the corporate network for viruses and malicious applications. Conventional anti-virus solutions designed for PCs are not suited for mobile devices due to the reliance on a sizable database of virus definitions stored on the device that needs to be constantly updated, causing excessive network traffic. The frequent scanning of the memory, necessary to detect viruses, adversely affects the performance of the device's low power processor and battery life.

Smarter Malware Protection. Using "Black-lists" (restricted applications) or "White-Lists" (approved applications), SOTI MobiControl's Process Run Control provides effective protection with a negligible memory footprint. Unlike other solutions that scan the memory to 'shoot-down' a black-listed process **after** it has started running in the memory, MobiControl's low-level memory management prevents black-listed processes from running **before** they even get a chance to load into the memory. The difference is critical!

A virus launched – even momentarily – has a chance to cause damage!

Intrusion Detection

In addition to preventing restricted or black-listed processes from launching on the device, SOTI MobiControl alerts the administrators through warnings and event logs, if an attempt to launch a restricted application is detected or an unauthorized process is disabled on a device. This allows administrators to take proactive measures against malicious attempts to hack into the device and/or the network the mobile device is connected to.

Disabling Internet Downloads and Unauthorized Software Installation

With a process “White-list” in effect, SOTI MobiControl prevents the installation or execution of any software application that is not on the approved list, whether it is being downloaded from the Internet or installed using the SD card auto-run functionality. The installation attempt is logged and reported to administrators, with the option to also send an SMS alert.

LIMITING END USER ACCESS TO THE MOBILE DEVICE

Disabling Communication Modules and Hardware Features

To prevent the transfer of sensitive information out of the device and to limit access to features for curious end users, SOTI MobiControl provides remote one-click disabling of device communication modules to prevent data transfer through Bluetooth, Infra-Red beam or through the USB port. Device features like the Camera and Phone can be disabled completely or restricted (e.g. limiting calls to and from specific phone numbers only).

Device Lockdown and Controlled Web Browsing

To provide a higher level of security for the device, SOTI MobiControl provides a locked-down ‘kiosk’ mode of operation, which limits the user’s access on the device to administrator-approved applications and Intranet / Internet sites only. Access to all other applications and device settings in the control panel is disabled to limit user activity and regulate usage of the device.

The Lockdown appearance can be customized and modified over-the-air. For example, on a stolen device the kiosk screen may display a “Stolen Device” message prompting the device-user to contact a Device Recovery Hotline.

By restricting the user’s browsing experience to corporate intranets and portals only, the device can be protected from the security hazards of unrestricted Internet surfing, **without** sacrificing the benefits of mobile web-browsing.



MobiControl Lockdown Screen

SECURING LOST OR STOLEN DEVICES

Devices roaming nation-wide over different cellular networks pose unique security challenges. Unfettered from corporate LANs, the geographical spread of cellular-enabled mobile hardware is truly global and security-conscious administrators need to plan – and equip – for the unforeseen.

SOTI MobiControl offers an arsenal of unique features for developing an effective multi-pronged strategy for securing and attempting retrieval of lost or stolen devices. SOTI MobiControl provides multiple options of connecting to remote devices and controlling them in different conditions and situations.

Remote Control functionality for Instant Device Take-over

Administrators now have the power to remotely take-over a mobile device, over any network type, including ActiveSync / Windows Mobile Device Center (WMDC) and all cellular networks (including GPRS, CDMA, 3G, HSDPA,

IDEN, etc.). SOTI MobiControl's Remote Control functionality facilitates remotely viewing and controlling the device, using the mouse as a stylus and using the device 'skin' to access the device's keypad – without requiring static public IP addresses for the device or any VPN connectivity! The capability to take over control of a lost device remotely can allow a real-time response to unforeseen situations and allows real-time monitoring of the usage of the device by any unauthorized users.

Real-time Device Location Tracking

For GPS-enabled devices, real-time GPS data can be retrieved from the device and the geographical location of the device can be automatically tracked on a map within the SOTI MobiControl management console. In addition to tracking the last known location of the device, SOTI MobiControl also records 'bread-crumbs' information to display the location history of a device. Real-time location-tracking allows better asset management and tracking and in the event of a device being lost or stolen, the capability to track the exact location is a valuable first step towards retrieving and securing the device and data.

Managing Security for Remote Out-of-Contact devices

When devices fail to connect to the data network to report back to the server for an extended time interval, SOTI MobiControl's time-based security mechanisms are triggered as a fail-safe last line of defense for a lost or stolen device. The actions that can be triggered include forced attempts to connect to the data network, auto-dial a phone number, warning the end-user, encrypting and / or wiping the information on the device.

Cellular Device Management via SMS / Text Messages

Even if a cellular device is not connected to any data network, SOTI MobiControl has the ability to send an encrypted SMS message (i.e. a simple text message) to the device to execute any command, including device-wipe, wake-up-and-connect to data network and other commands. SMS messages can 'wake-up' most devices even from a sleep or power standby mode, providing last-resort connectivity to take control of a remote device that is lost or stolen.

AUDITING AND MONITORING ADMINISTRATOR(S) ACTIVITY

Network-wide security cannot be achieved if there is no way to regulate who can access the device – and what level of control they have on the device.

Common security pitfalls. Unfortunately, some security solutions do not limit access to the devices and open security loopholes to compensate for architectural weaknesses. One example is the use of static public IP addresses on the device in order to provide remote control functionality (unlike SOTI MobiControl's Remote Control which is capable of NAT / firewall traversal and can connect to devices that have a dynamic or a private IP address). However, mobile devices typically do not have the networking safeguards that are common for computers on a LAN (e.g. defense mechanisms like firewall protection, private addresses, proxy servers, etc.). Exposing the devices to the world with public IPs, places the devices, and the data residing on them, at a risk of hacking and intrusion.

Some solutions go to the extent of installing a web-server on the device to remotely control it. This opens up unlimited access to the device for the intended helpdesk administrators – and for anyone else with a web browser!

Roles Based Access Control for Securing the Helpdesk Console

SOTI MobiControl ensures that administrator and helpdesk personnel's access to the devices can be restricted by integrating with the existing enterprise security infrastructure. SOTI MobiControl's domain-based security integrates with the Active Directory to implement roles-based security permissions which can be assigned to groups and users in the Active Directory. Granular group-level and device level permissions ensure that different

levels of access can be configured to implement a tiered support model. For example, a helpdesk user with fewer privileges can be limited to basic diagnostics only and access to the data stored on the device can be restricted.

Detailed audit logs allow administrators to monitor the system and identify problems or critical events using different criteria including time-stamp, helpdesk user ID, device name, event type and priority.

CONCLUSION

Effective mobile security for the enterprise must provide safeguards not only for the device but also for the data stored on the device and removable media, the communication channels through which the data flows when in transit, the end-users who have physical access to the device and the helpdesk or administrators who have remote access to the device. The security solution should be designed specifically for mobile devices instead of porting over inefficient solutions from a desktop environment. The solution should have the capability to communicate through multiple network topologies, cellular technologies and deliver security-related commands in different ways to provide fail-over in predictable or unforeseen circumstances. These goals should be met with technologies that are suited for the limited processing power, memory and battery resources on the mobile devices instead of relying on resource-intensive technologies like VPN, locally installed web-server on each mobile device, etc.

SOTI MobiControl is the only solution that achieves all of these objectives efficiently, by combining an architecture designed specifically for mobile devices, with unique features like:

- Verification of Active Directory domain credentials for remote user login on device
- Real-time location tracking of GPS-enabled devices
- Instant device-take over with the Remote Control functionality
- Device Rescue via SMS text messages with remote device 'wake-up'
- Encryption of data in transit as well as information stored on device and removable media
- Automatic data-fading and multiple delivery options for device 'wipe'
- Virus and malware protection through smart memory management
- Device lockdown with intrusion detection to protect from unauthorized usage and applications

ABOUT SOTI

SOTI Inc. develops industry leading technology that solves the unique challenges involved in deploying, managing, securing and supporting remote mobile and desktop computing devices. Today over 55,000 customers around the world ranging from retail, manufacturing, health care, government, logistics and other industries rely on SOTI products to reduce costs by allowing them to centrally manage and secure their remote mobile field forces.

To learn more about how MobiControl can help you manage the security for your mobile enterprise and fulfill the device management requirements for your organization visit our website at www.soti.net, contact us directly at +1 905 624 9828, or email us:

support@soti.net for technical information.

sales@soti.net to schedule a **live online demo** and technical discussion for your team.