Android Management Redefined

Presenter:

Name inserted here

SOTI

Barriers to Android Entry in the Enterprise

SOTI

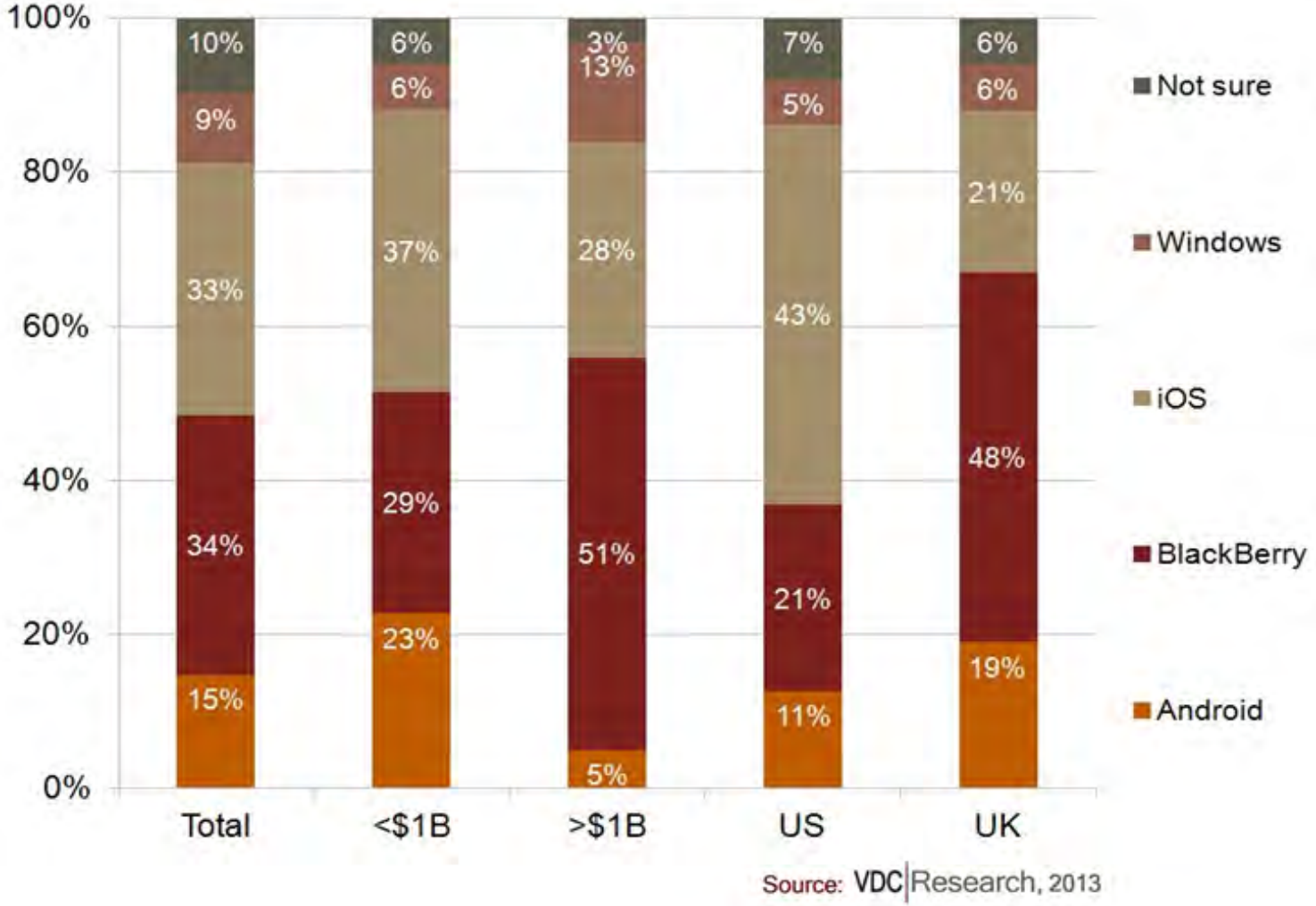
Android in the Enterprise

Top 3 hurdles to enterprise adoption:

1. Fear of OS compromise
2. Perceived lack of protection against data leakage
3. Limited policy controls and management

SOTI

Perceived Insecurity of Android



According to a VDC Research survey where CIOs were asked which platform they perceived as most secure, Android was rated as the most insecure mobile platform, especially among larger organizations (>$1B annual revenue).

SOTI

Third Party Android App Stores: A Cybercriminal's Dream

- Until recently, Google had been largely content to let Android developer community self-police validity of apps in Google Play
- Laissez-faire approach has played a key role in the amount of malicious code posing as legitimate apps in Google Play
- In 2003, 96% of all new mobile malware families or variants targeted the Android Platform
- Prevalence of viruses and malware has hugely contributed to Android's perception as an insecure OS in the market

security threats.

recent high profile cyberattacks.

1. **2013:** malware installed on PoS systems at Target compromised 40m credit and debit cards
2. **2014:** malware installed on PoS systems at Home Depot compromised 56m credit and debit cards in the US and Canada
3. **2015**: ~80m personal records from health insurance provider, Anthem, were stolen
4. **2016:** Dyn DNS suffered a DDoS attack that made impact several popular sites such as, Twitter, SoundCloud, and Spotify

rise of shadow IT.

- What is shadow IT? A term often used to describe information-technology systems and solutions built and used inside organizations without explicit organizational approval
- By 2020, 1/3 of successful attacks experienced by enterprises will be on their shadow IT resources.*
- By 2018, 25% of corporate data traffic will flow directly from mobile devices to the cloud, bypassing enterprise security controls*

Smarter with Gartner June 15, 2016

malware is evolving.

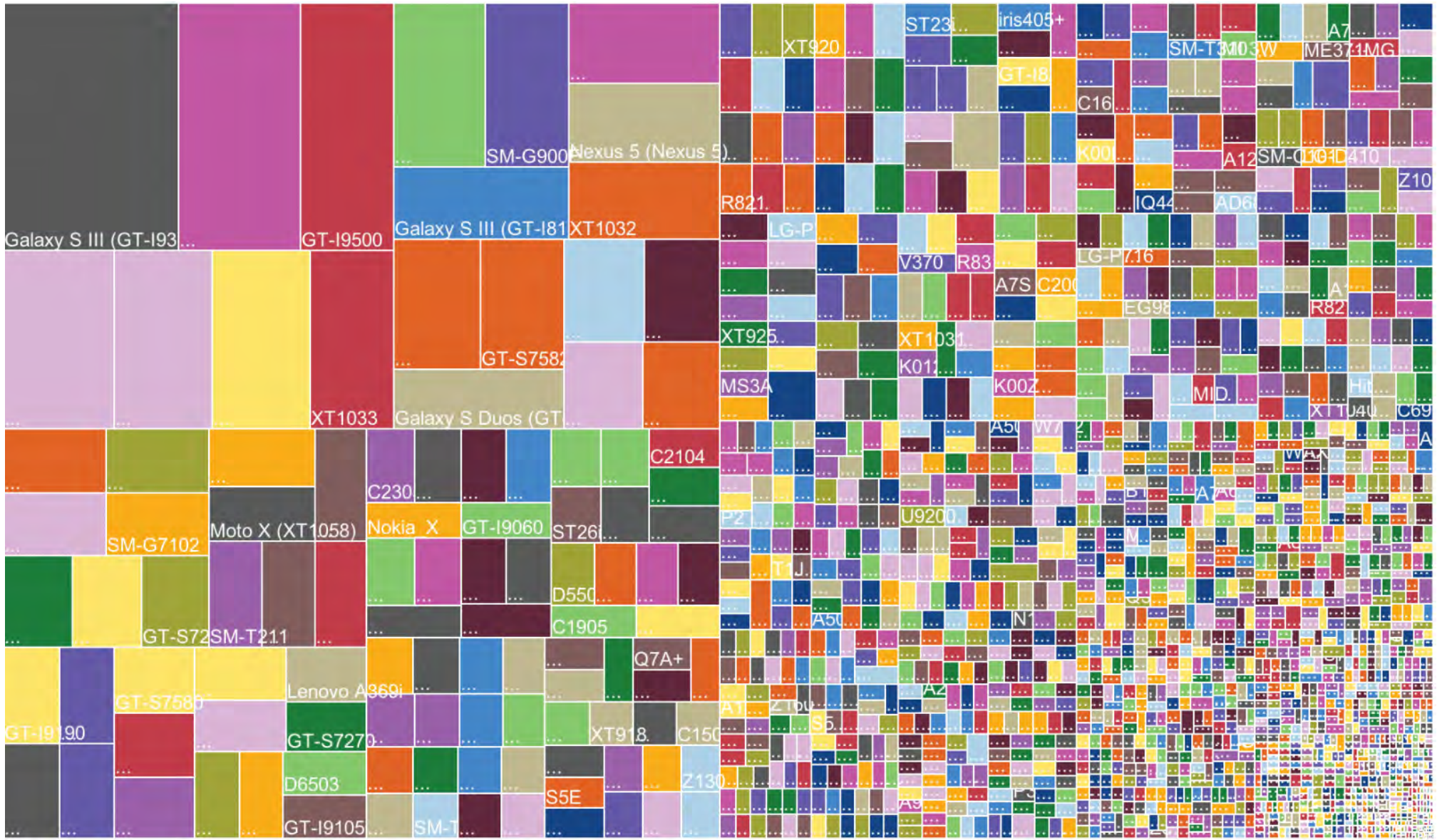
- Over 390k new malicious programs every day*
- 97% of malware is unique to a specific endpoint, rendering signature-based security virtually useless**
- Through 2020, 99% of vulnerabilities exploited will continue to be ones known by security and IT professionals for at least one year.***
- By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk***

*Source: AV Test – Independent IT-Security Institute
**Webroot 2015
***Smarter with Gartner June 15, 2016

Android Fragmentation: The Elephant in the Room

SOTI

Android OS Fragmentation Is Growing



2014

SOTI

Android Hardware Fragmentation Adds Complexity

- Processing power variances
- Different screens, different crashes
- Unpredictable application compatibility

SOTI

Android's Way Forward in the Enterprise

SOTI

Why Android Has a Future in the Enterprise

1. Gartner predicts that Android will top 1 billion shipments by the end of this year – 3 times the number of Apple devices expected to ship
2. The sheer number of Android devices in the hands of BYOD employees will force IT to fold Android into their enterprise mix
3. Android comes in all shapes - sizes , providing a larger flexibility to get use cases to business
4. Cost advantages enable leveraging low cost devices with faster retire cycles for business
5. Android+

RESULT: Android is starting to win over reluctant IT gatekeepers

SOTI

SOTI Changes the Game

SOTI

What's Needed for Android to become a good corporate citizen

1. Enterprises need to be able to set consistent management policies across broad range of Android devices (BYOD)
2. Enterprises need deep management policies to be able to customize the device to meet business needs (Corporate Liable)
3. Deep security policies to allow businesses to trust Android (Compliance)

SOTI

Focus on R&D: Android Challenges & Solution



OEM Challenges + EMM Vendor Issues = Result

- Google offers very few Management APIs for Android
- A few OEMs (e.g. Motorola, Samsung, LG) have added EMM API Stacks to fill the gap
- Most other OEMs add few or no EMM APIs (e.g. ZTE, Huawei, Panasonic, etc.)

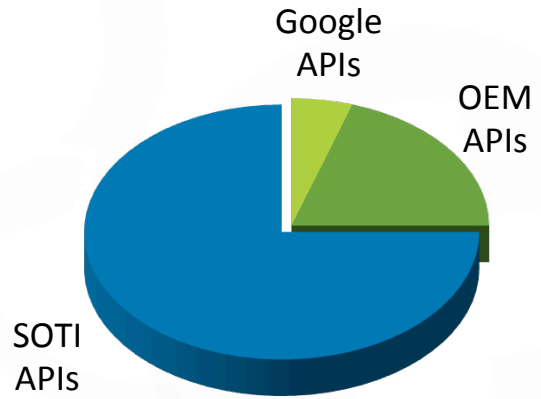
- Dependent on Google APIs + OEM APIs
- High cost & effort to develop and maintain APIs across all OEMs
- Most EMM Vendors focus on one Android manufacturers to save development costs

- **Fragmentation:** Hinders enterprise-grade mobility management
- **Inconsistency:** Impossible to set consistent corporate wide security or other policies across all devices
- **BYOD Not Possible:** Companies only allow employees to bring their own manageable devices (BYOMD)

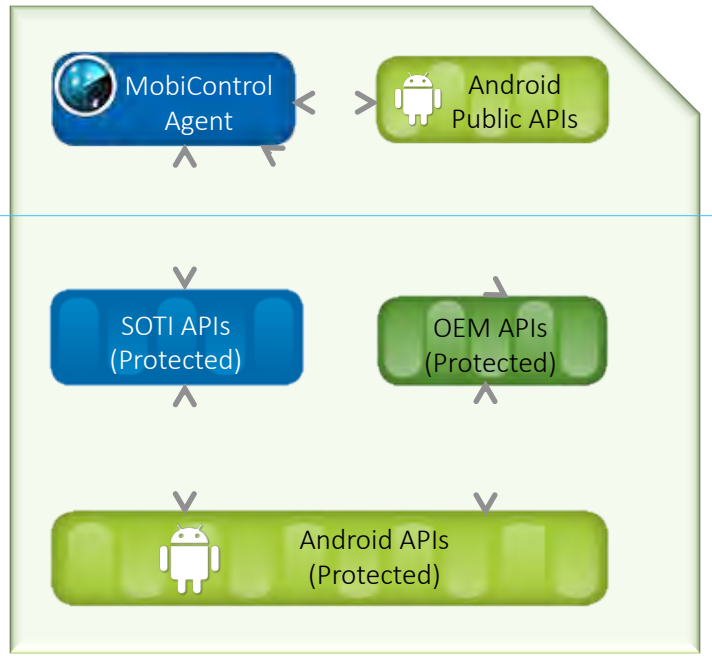
There is a solution: **Android+** Technology

SOTI

Focus on R&D: SOTI's Android + Technology

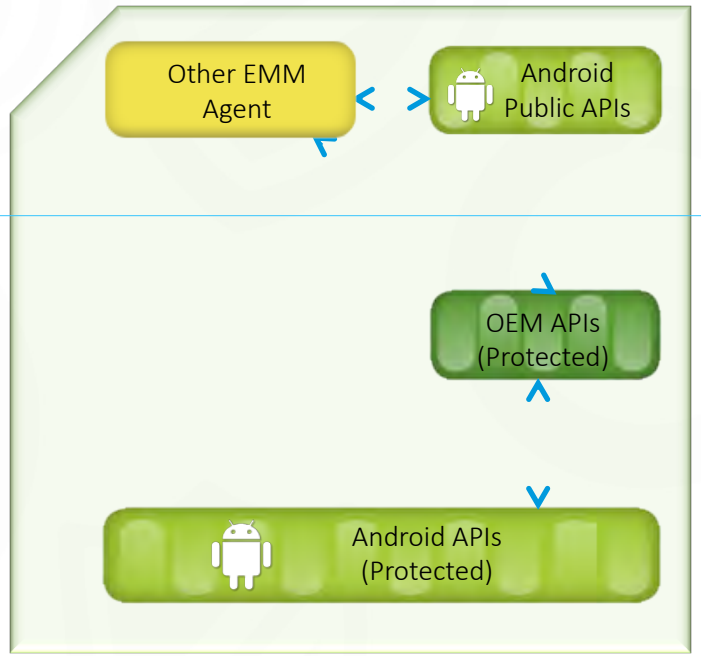


SOTI Android+ EMM Strategy



Full management

Other EMM Vendors Strategy



Management limited to functions provided by OEM

SOTI

SOTI Android+ Technology

- Advanced Remote Control
- Location Services/Geofencing
- Lockdown/'Kiosk' Mode
- Device Feature Control
- Speed Control
- Anti-Virus/Malware
- Web Filtering Protection
- Silent Software Deployment
- Advanced Policy Enforcement

Android+

SOTI

Android+ supports over 50 OEMs!

Accel	Caterpillar	Gadmei	Lava	Sonim	ZTE
Acer	Cipherlab	Getac	Lenovo	Sony	
Advantech	Coolpad	HCL	LG	Spectralink	
Alcatel	Coppernic	Honeywell	Mitac	Toshiba	
Amazon	Datalogic	HTC	Motorola	Toughphone	
Arcos	DRS	Huawei	Outform	Toughshield	
Askey	Exiom technology	iLeadsky	Panasonic	Trimble	
Asus	Extrem	Intermec	PAR technology	Unitech	
BQ	Filla	JCB	Pidion	Urovo	
Casio		Kyocera	Samsung	Winmate	

SOTI

SOTI MobiControl:

Android Management Redefined

SOTI

Unauthorized Access A Thing of the Past

Enforce strong authentication requirements

- Configure and enforce strong password requirements that end users must meet to secure their devices
- Prevent unauthorized device use and retain access to sensitive corporate data in the right hands with complex password enforcement

SOTI

Web Filtering



- Enforce and control web access policies to ensure secure, safe and authorized access to web content
- Configure web filtering policies to block access to specific URLs
- Specify a URL for device redirection
- Create a whitelist of acceptable URLs

SOTI

Antivirus/Malware Built in

- Monitor device file system and installed applications for malware and viruses
- Quarantine infected applications and files on devices
- Schedule antivirus scanning, virus definition updates, and quarantine management
- Configure antivirus whitelists

SOTI

Out of Contact Device Policy

Alert and take action on devices that have been out-of-contact for a period of time

- Enable out-of-contact policies based on last connection time and enforce device side actions
- Log events, show messages, wipe device, activate data connection
- Enable flexible script-based execution for IT administrators to specify any action currently supported by MobiControl

SOTI

Phone Call Policy

Whitelist or blacklist specific phone number for groups or individuals

- Enforce granular control over incoming and outgoing calls across device groups or on specific devices
- Import feature for large whitelists or blacklists
- Group blocking of phone numbers and long distance exchanges
- Configure device and server notifications for blocked calls

SOTI

When Employees Go Rogue or Devices Are Lost or Stolen

Remotely lock or wipe the entire device

SOTI MobiControl gives enterprises flexibility to take a phased approach depending on the situation:

a) Lock the device

b) Remotely unlock or reset device passwords for users who have forgotten them

c) Wipe the entire device; remove all data and settings back to factory default in real time

SOTI

Limiting the What & When of Device Usage

Lockdown / Kiosk Mode

- Create purpose-dedicated mobile devices that allow enterprises to limit applications, documents and web resources
- Decrease downtime and minimize unauthorized use of corporate devices
- Detect compromised or rooted Android devices and immediately force remote security actions to prohibit access to the corporate network or data

Speed Control

- Eliminate liability to the organization by enabling distracted driver controls to limit functionality when speed of movement is exceeded
- Device functionality is restored when no longer in motion.

SOTI

And What About the Where?

Real-Time Geo-Aware Policies

Beyond Simple Device Tracking Devices Tracked & Access Limited Based on Location

SOTI MobiControl provides accurate geo-location device tracking and user behavior monitoring that can be plotted on an interactive worldwide map.

Geofencing enables the creation of a virtual boundary around a geographical area to trigger alerts and pre-defined actions when devices enter or exit the boundary.

Geo-aware content access allows enterprises to restrict access to sensitive corporate content based on location while still giving employees access to their personal content and applications.

SOTI

Corporate Content: Protecting Your Assets

Secure Access to Corporate Content

- Securely distribute and manage corporate content to your mobile workforce
- Supporting all major formats, files can be delivered flexibly one-to-one, one-to-many or one-to-all
- Secure Content Library gives you fine-grained control over your content, allowing administrators to set priority levels, document expiry, and location based delivery.
- Data stored encrypted on device, for enhanced security.

SOTI

Applications:
It’s Not All Black & White

Application Management

SOTI provides the ability to:

- whitelist and blacklist apps within the container
- silently install approved corporate applications into the container without user intervention
- geo-awareness helps control usage of device apps (e.g. camera) when user is in the confines of a restricted work area.

Mobile Email Management

It’s About More Than Just Access

- Access, privacy, sharing, and forwarding don’t have to be taboo. All can be addressed with SOTI MobiControl management.
- Configure advanced compliance policies to manage user credentials
- Prevent data breaches by allowing, removing or blocking mobile devices accessing the network
- And for added protection, comprehensive Exchange Access Controls prevent unmanaged devices from accessing the corporate Exchange server.

SOTI

Email Privacy Made Easy

Use integrated Nitrodesk Touchdown to configure and manage a secure corporate email sandbox on Android devices

- Touchdown Email sandbox can be set up, managed, and removed by the MobiControl administrator to ensure corporate email is in the right hands at all times.
- Businesses can configure end user corporate email access and settings whilst monitoring policy compliance.
- Robust way of securing corporate email on Android devices.
- A seamless and easy to use MS Exchange email client.

SOTI

Enhanced Certificate Management

- Add, renew, revoke and deliver authentication certificates from a certificate authority to managed devices
- MobiControl integrates with Microsoft, VeriSign and Entrust
- Connects to corporate resources like Wi-Fi, VPN and email

SOTI®

File Synchronization

Manage device files and folders over the air

- MobiControl can synchronize files and folders between devices and servers on an ad hoc or scheduled basis
- Equip employees with up to date corporate resources with special read and write to device storage privileges

SOTI

Remote Help:
Happy User, Happy Admin

Remote Control for Live, Real-Time Support

- Fastest and most reliable interactive remote control of Android devices for optimal Helpdesk capability and troubleshooting

- Best-in-class remote helpdesk capabilities offer administrators the ability to support their growing mobile workforce effortlessly

SOTI

Put End Users In the Driver's Seat

"Manage Your Own Device"

With MobiControl's "Manage Your Own Device" End User Self-Service Portal, employees can:

- Enrol
- Lock
- Locate
- Wipe
- Reset password
- Send messages to their devices…
- And more

Your helpdesk employees will be grateful.

SOTI

Manage Enterprise Mobile Assets

Collect and store important device info for reporting purposes

- Enroll, provision and configure one or many devices simultaneously over the air
- Manage device inventory individually or by dynamic groups and communicate to end users proactively
- Access a wealth of live device information such as Device ID, Carrier, Phone Number, Signal Strength, Battery status, Memory (and many more) for live display, report, or auditing purposes
- Dashboard provides a quick and interactive overview of mobile asset status and system health in graphical displays
- Monitor the mobile fleet and communicate effectively using Android's native messaging system or MobiControl’s built in Messaging Service
- Wireless Device Configuration

SOTI

IT Visibility & Control

Audit Logs

Full device and network logging providing comprehensive analysis of device activities. KNOX Audit logs capture network traffic and statistics, as well as OS-level activity, to provide military grade auditable tracking.

Telecom Expense Management

The system provides Voice and Data overage alerts for administrators and device users, with automatic pre-defined actions. Also provides the ability to import large whitelists or blacklists, group blocking of phone numbers and long distance exchanges, and server notifications for blocked calls.

SOTI

SOTI provides the tools and solutions to make BYOD environments safe and productive ecosystems for today's IT administrators

SOTI is the proven leader in innovative technology solutions for enterprise mobility

SOTI's MobiControl is an award-winning EMM solution for mobile and desktop computing devices