

Data Loss Prevention Whitepaper

When Mobile Device Management
Isn't Enough

Your
Device
Here.

Good supports
hundreds of devices.

Good





Contents

Shifting Security Landscapes 3

Security Challenges to Enterprise Mobility 3

Mobile Device Management 4

The Good Solution 5

■ Shifting Security Landscapes

Whether you're a government agency or an enterprise business, chances are your people are bringing their mobile devices to work and requesting that they be able to access parts of your infrastructure through them. IT may not even be aware of what devices are connecting to corporate resources. These devices run the gamut of popular smart handhelds, including the iPhone, iPod Touch, iPad, Android-enabled devices, and hundreds of other devices available now.

Some organizations are turning to mobile device management (MDM) solutions to better secure, monitor, manage and support the variety of mobile devices used by their employees. However, in many instances, MDM alone is not enough to prevent data loss.

This paper will explore common methods of data loss that cannot be prevented through MDM alone. In addition, this paper will introduce Good for Enterprise—and its unique approach to managing security on mobile devices, which does address some of the shortcomings of an MDM-only strategy.

■ Security Challenges to Enterprise Mobility

Critical business data, intellectual property, and sensitive information are now not only spread throughout your organization on servers and desktops—they're also being transmitted to mobiles via your network, and potentially from those mobile devices into public or private clouds.

So how does data intentionally or unintentionally escape from a smart handheld—and your network?

Unencrypted Information

Corporate email is the primary application employees want to use on their personal mobile devices. Unfortunately, many mobile devices do not support encryption. For example, today, existing Android phones cannot perform hardware encryption. As a result, confidential email and attachments sent to an Android phone can easily be viewed by anyone.

Consumer Applications

Let's say I'm an executive traveling on the road and I'm hard-pressed to finish my business plan within the next 12 hours, by order of the CEO. My assistant has just emailed me the plan and a straw man framework.

What do I do? From my mobile phone, I open and view the document using a 3rd party consumer viewer and editor.

The problem is that I can't possibly be sure that the 3rd party consumer viewer and editor is completely secure. Also, depending on the type of device I own, once I open the document I can't be sure that the document will be encrypted on my mobile device.

Weak Passwords

To keep confidential data stored on an employee's personal mobile device from falling into the wrong hands, many IT departments implement strong device passwords. However, most users simply don't want to enter a complex password every time they want to make a phone call, send a text message or update their Facebook status. As a result, IT often caves into employee pressure and compromises corporate security by allowing weak passwords.

Mobile Device Management

To address these common security challenges, organizations are turning to Mobile Device Management or MDM solutions to better secure, monitor, manage and support the variety of mobile devices used by their employees. MDM solutions enable IT to provide mobile users with access to corporate resources and applications (such as email), as well as to secure smartphones and tablets. To protect corporate applications and data, MDM solutions leverage platform security services provided by the mobile operating system or device manufacturer. IT organizations can then implement security controls such as passwords and remote wipe and lock. While MDM can provide some level of control, MDM is not enough to ensure security and prevent data loss, especially in increasingly “Bring Your Own Device” (BYOD) environments.

Mobile Device Management Shortcomings

MDM security controls are limited to device security services. As MDM solutions rely on the mobile operating system and each specific device manufacturer’s services, security controls can vary widely. Companies with an environment of mixed devices such as iOS and Android devices will find this especially challenging. For example, as previously discussed, Android devices do not support hardware data encryption. An MDM solution, no matter how robust, would not be able to add encryption to a device or application that doesn’t support it to begin with. Without a cross-platform standard that ensures consistent policies and/or control, IT will find it difficult to effectively protect corporate data in a consistent manner across a heterogeneous environment.

MDM policies are implemented at the device level, which interferes with personal use. As an example, in order to prevent unauthorized users from accessing an employee’s corporate email on the employee’s personal phone, MDM solutions require a password to the device itself rather than the email application. As a result, the employee must enter a password every time they use the device, whether they intend to use the device for work or personal communication and collaboration. As we discussed earlier, often IT will defer to users who find entering complex passwords a nuisance every time they use their devices, and allow weak passwords, thereby exposing corporate information to potential data loss.

Another example of an MDM policy implemented at the device level is remote wipe. Remote wipe allows IT to erase corporate data from a mobile device in the event a device is lost or stolen. However, for employees that use their personal phones for work, a remote wipe would erase personal apps and data in addition to the corporate data and applications. Employees may feel their personal privacy has been violated and inconvenienced if they have to re-create their personal information.

Consumer apps are especially challenging for most MDM solutions. Policy controls and data encryption cannot address potential security risks that lie within the applications themselves—and that can directly or indirectly access and share corporate data with other 3rd party apps and cloud services. Most corporate data leakage is due to the unintentional actions of the employee who uses these consumer applications, similar to our example of the traveling executive using his favorite mobile document reader to complete his business plan. Given that most MDM solutions are limited to security controls at the device level, most MDM functions are also unable to address potential security risks at the application level.

Addressing Mobile Device Management Shortcomings

To address MDM shortcomings, companies and government agencies need to adopt solutions that allow IT departments to set and manage security policies at both the application and the device level. By providing security and control at both levels, IT can further reduce the risk of data loss, more readily embrace BYOD, and ensure an uncompromised employee experience.

The Good Solution

Good for Enterprise (GFE) is the answer to MDM shortcomings. Unlike most MDM solutions, GFE provides a unique security approach that addresses the safety of every part of the infrastructure, including security at the mobile device and application level, while providing flexibility to the end user. To date, GFE has satisfied the needs of the most demanding customers, including defense and intelligence agencies; regulated industries such as Financial Services, Healthcare, Legal, and Defense Contracting; and many enterprises in high tech, retail, manufacturing, and other verticals.

GFE's Unique Security Approach

GFE limits business risk associated with enterprise data on mobile devices by containerizing the data (which leaves employees' private information untouched).

GFE's container or "sandbox" approach separates corporate and personal data—going well beyond basic MDM—by providing a separate, secure environment for corporate data. For example, attachments and other corporate documents accessed via GFE's email client or secure browser are stored within the container and cannot be accessed by 3rd party apps.

Users have open access to their personal applications, while enterprise data is secured within the GFE container.

This container-based approach secures corporate data and applications consistently, regardless of what is available natively, across a wide range of mobile platforms, including iOS and Android. By providing security and management at the application level, IT administrators can establish policies to prevent mobile data loss without interfering with personal use.

GFE's Benefits:

- *Consistent security across multiple platforms* - IT can rest assured that security policies are consistently applied, regardless of what is available in the underlying operating system or device. Users will not be limited to a single platform.
- *Respect employee privacy* - IT can manage corporate data on personally-owned devices while respecting employee privacy. By applying policies at an application level, IT can implement and enforce strong enterprise-grade policies for passwords, timeouts, and other security controls without impacting the employee's overall personal experience.
- *Freedom of choice* - Since GFE separates personal and work data and provides policy controls at an application level, IT can more readily embrace BYOD programs. IT manages only the corporate data. For example, rather than remote wiping the entire device, IT can wipe only the corporate data, leaving personal data and applications intact. Employees can use their own mobile devices without compromising their personal user experience, which increases employee satisfaction and productivity.

Good for Enterprise addresses common MDM shortcomings by:

- Going beyond basic platform security services
- Providing security at the device and application level
- Enabling consistent security policies across a heterogeneous environment

Good for Enterprise provides:

- Collaborative Applications (Email, Calendar, PIM)
- Secure Browser
- Mobile Device Management



Good's security container separates company and personal information.

Practical Application of GFE's Security Approach

Let's revisit a couple of our earlier examples to see how GFE goes beyond basic MDM capabilities:

With GFE, our corporate executive's assistant can send his business plan to him using GFE's secure email client. The business plan is encrypted over the wire while in transit from his company's email server to his mobile phone. In addition, when our executive opens the document in GFE's secure container, the document remains encrypted on his phone.

In the example of IT caving into employees' complaints about entering a complex password to use their personal devices, IT can now set the complex password at the application level rather than at the device level. As a result, IT can maintain as consistent password policies for smartphones and tablets as they do for desktops and laptops. Finally, with GFE's secure container that encrypts applications and documents, IT no longer has to worry about devices that may not natively provide encryption.

GFE's Unique Security Model

Good for Enterprise goes beyond most MDM solutions by providing end-to-end, wireless, real-time collaboration and enterprise application access supported by comprehensive security. GFE's security model helps IT overcome the shortcomings of other MDM solutions and embrace consumer-owned devices, and consequently increase employee productivity. IT can also continue to deploy corporate-owned smart devices, while maintaining high levels of security and assurance in both device populations.

GFE provides mobile professionals with up-to-date collaboration, connectivity, and applications when and where they need them, while giving IT the means to secure and manage a diverse fleet of smart devices. The data path through the GFE system is encrypted end-to-end: from the enterprise servers behind the firewall, all the way to wireless handhelds.

GFE's security model has five key elements:

1. **Authentication.** GFE provides IT with the administration tools necessary to define strong authentication policies, enforced consistently across platforms. Also, you can define policies to wipe the Good container and all its data (and on some device platforms, wipe the entire device), for failure to provide the correct password after a set number of failed attempts. Strong policies let IT disable sequential numbers in passwords, require special characters, and more. When strong over the air (OTA) policies are deployed, only employees that are authenticated can connect to the Good network operations center (NOC).
2. **Data Protection.** With Good for Enterprise, you can be confident your business data is protected even when your data shares the same device with any number of consumer applications from the Apple App Store or the Android Market. It's possible because of Good's Container—that encrypts enterprise data with strong AES 192-bit encryption. In addition to a secure container, GFE also separates and encrypts any data that's in transit between the device and servers behind your firewall. So data protection extends all the way from the firewall to the device — irrespective of whether the device is company-owned or employee-owned.
3. **Enforcing Access Controls.** GFE lets administrators restrict access to Good servers, based on a particular device OS and/or GFE client version number. On the server side, IT can distribute management tasks across a hierarchy of administrators using role-based administration that offers a set of roles—with varying permissions—for administering the GFE server and employee devices. Routine tasks, such as loading software, can be delegated to a wider group of administrators across multiple locations. More restricted tasks, such as setting global policies or remotely erasing a handheld when lost or stolen, can be limited to a smaller group.



4. **Securing Network Access.** GFE servers establish an outbound connection to the enterprise firewall, so there's no need to open inbound ports and expose the enterprise network to attack. In addition, network traffic between the device and the server is always encrypted with AES 192-bit encryption. The NOC only services encrypted packets, so it provides the additional functionality of authenticating devices to the network, granting access only to devices that have been provisioned to access their respective servers and services—thus preventing rogue devices from gaining access to the network.
5. **Securing the Platform.** GFE provides strong protections on each platform, with policy controls that include strong encryption of data (OTA and data at rest), remote wipe of only the Good container or full device wipe, and detecting jail-broken iPhones. For iOS devices, GFE provides policies to prevent access to the App Store, YouTube, and the Safari browser, if needed by your business.

Good for Enterprise Security Assurance

GFE's cryptography has been successfully tested by NIST-approved labs and certified to be compliant with FIPS 140-2 Level 1. Additionally, intelligence agencies and defense organizations such as the Defense Information Systems Agency (DISA), the US Army, the US Air Force, and the Department of Homeland Security (DHS) have tested the GFE and approved it for their most sensitive deployments.

Embracing Mobility with Confidence

While many MDM solutions have shortcomings that could potentially lead to corporate data loss, organizations can be confident that Good for Enterprise provides security beyond basic MDM capabilities while also respecting employee privacy.



To learn more about Good solutions, visit good.com or call 866-7-BE-GOOD.

©2011 VISTO Corporation and Good Technology, Inc. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for Government, Good for You, Good Mobile Messaging, Good Mobile Intranet, and Powered by Good are trademarks of Good Technology, Inc. ConstantSync, Constant Synchronization, Good Mobile Client, Good Mobile Portal, Good Mobile Exchange Access, Good Mobile Platform, Good Easy Setup, Good Social Networking and Good SmartIcon are either trademarks or registered trademarks of VISTO Corporation. All third-party trademarks, trade names, or service marks are the property of their respective owners and are used only to refer to the goods or services identified by those third-party marks. Good and VISTO technology are protected by U.S. Patents 6,085,192; 5,968,131; 6,023,708; 5,961,590; 6,131,116; 6,151,606; 6,233,341; 6,131,096, 6,708,221 and 6,766,454 and the following NTP U.S. Patents: 5,436,960, 5,438,611, 5,479,472, 5,625,670, 5,631,946, 5,819,172, 6,067,451, 6,317,592 and various other foreign patents. Other patents pending.