

# Securing Business Mobility

Today's Best Practices: How smart business is protecting enterprise data integrity—and employee privacy—on popular mobile devices

Your  
Device  
Here.

Good supports  
hundreds of devices.



# Contents

- Mobility Is Shifting Terrain ..... 2**
- Enterprise Mobility: Security Level Red ..... 2**
- The Good Solution ..... 3**
  - Protect Enterprise Integrity, Employee Privacy ..... 3
  - Maintain Consistent, Centralized Control ..... 3
  - Prevent Rogue Device Network Access ..... 3
- Good Security Architecture ..... 4**
- Good Security Model ..... 4**
  - Authentication ..... 4
  - Data Protection ..... 4
  - Enforcing Access Controls ..... 4
  - Securing Network Access ..... 5
  - Securing the Platform ..... 5
- Good Assurance ..... 5**

## Mobility is shifting terrain

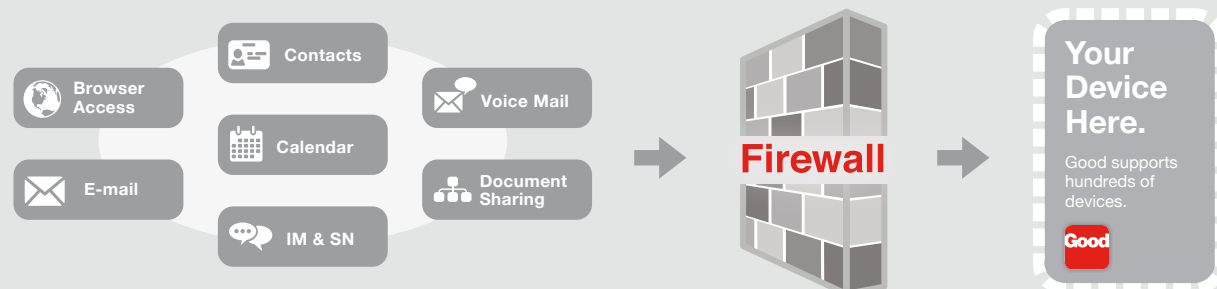
It's the price of portability. No longer does today's workforce simply require access to business email, calendar functions, and contacts while out of the office. Because work and life are now more fluid than ever, people are working at literally any hour of the day or night—and anywhere a smart device can pick up a signal. True employee collaboration requires a broader suite of mobile solutions.

Mobile phones have evolved into ultra-intelligent, and highly portable, mobile computers with sophisticated operating systems and the ability to connect to networks and applications. In the larger evolutionary picture, smart tablets are also now firmly entrenched in today's mobile business scenarios.

Agile businesses are now connecting employees, partners, and suppliers—no matter how remote—to Intranets, Web-enabled enterprise applications, document sharing, corporate instant messaging services, a broader range of collaboration tools, and, soon, custom, in-house-developed applications. All with appropriate security and control. At least, that's the hope.

Another key trend: Price points for both smart mobile devices and associated data plans continue to fall, so most employees are already equipped with the popular devices of their choice. What does this mean for CIOs and CFOs? The ability to shave millions from enterprise budgets that have traditionally been spent on devices and data plans.

While these trends represent an opportunity for smart businesses to rapidly accelerate the pace of business and reduce costs, they also represent significant security challenges.



## Enterprise mobility: Security level red

CIOs consistently rank security as one of their top IT priorities. As well they should. Today's heightened security conditions in both the analog and digital worlds add to the likelihood of mobile security threats. Misplaced devices. Lost devices. Stolen devices. But today's smart phones and tablets present additional challenges to IT administrators taxed with safeguarding enterprise infrastructure, applications, and data. As more employees buy their own devices and carrier plans, the consumerization of IT – or the access of corporate information by personal applications, Web services, and mobile hardware – is increasingly prevalent. To be more productive out of the office, employees frequently, and unwittingly, forward their email and documents to their personal Webmail accounts, inadvertently undermining IT security policies. In most

cases, employees are simply unaware of the potential risks of enterprise data loss. Or they may be naive as to IT's policies themselves. So while the IT consumerization trend presents businesses with the potential for tremendous cost savings, it has also introduced serious security risks for enterprises and government agencies alike, at the application level, the device level, the over-the-air level, and the enterprise network (perimeter) level. Before business mobility can be fully embraced, these obstacles must be overcome.

## The Good Solution

Good Technology recognizes that managing business data security in today's modern workplace is a huge undertaking—especially when it calls for securely providing employees with the information they need and the flexibility they want. To date, Good has satisfied the needs of the most demanding customers, including defense and intelligence agencies; companies in regulated industries such as financial services, healthcare, legal, and professional services; and many enterprises in high technology, retail, manufacturing, and other verticals. Good has developed a security model that addresses the safety of every part of the infrastructure.

The model is built on three main tenets:

- 1. Respect enterprise data integrity as well as employee privacy.** The sheer number of device types that combine a variety of untrusted consumer applications, personalization capabilities, and business data leads to tremendous challenges in maintaining the confidentiality and integrity of enterprise content. Good limits business risk associated with enterprise data on mobile devices by “containerizing” the data (which leaves employees' private information untouched) and enforcing policies and compliance at the application level.
- 2. Maintain consistent, centralized control.** Enterprises and government agencies are struggling to maintain centralization and enforce consistent security policies on all enterprise content in environments with different devices, different security approaches, and different operating systems. As your business expands to support personal devices and data plans, you must change the way you approach control.
- 3. Prevent rogue device network access.** The scope and number of mobile devices employees use today opens the possibility that devices may be replicated and rogue devices could potentially access the corporate network. Because these devices aren't authorized, they may or may not be following corporate security policies. Chances are, they're not. Without visibility into all the devices on the network, IT simply can't ensure the integrity of corporate data.



Good's security container separates company and personal information.

## Good Security Architecture

Good Technology's flagship product, Good for Enterprise, is a comprehensive platform providing secure end-to-end, wireless, real-time messaging, collaboration, and Intranet access supported by comprehensive device management and security. Good has developed a proven architecture that can help you overcome the challenges you face in embracing enterprise mobility. At the core of Good's architecture is a robust security model that helps you enable consumer-owned devices, and consequently increase employee productivity. You can also continue to deploy corporate-owned smart devices, while maintaining high levels of security and assurance in both device populations.

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

## Good Security Model

The growing use of smart devices extends the corporate network beyond the physical boundaries of the enterprise, and places the endpoint of the network outside the firewall. Using public and carrier networks to transmit data raises a multitude of security issues, some of which have already been described.

Good has developed an optimum security model, with five key elements:

- 1. Authentication.** Good provides you with the administration tools necessary to define strong authentication policies, enforced consistently across platforms. You have the flexibility to enforce passwords at the device level, for corporate-issued devices, or at the Good application level, for personally owned devices. Also, you can define policies to wipe the Good application and all its data (and on some device platforms, wipe the entire device), for an employee's failure to provide the correct password after a set number of failed attempts or if a device is lost or stolen. Strong policies let you disable sequential numbers in passwords, require special characters, and more. When you deploy strong over-the-air (OTA) policies, 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. It's possible because of the Good enterprise container, an encrypted cocoon that securely houses enterprise data and applications on the device, which encrypts all data with strong AES 192-bit encryption. The Good solution also encrypts any data that's in transit between the device and servers behind your firewall. So the 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.** The Good platform lets administrators restrict access to Good servers, based on a particular device OS and/or Good client version number. Additionally, Good provides the capacity to control access to networks from the device, including Bluetooth. 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 Good 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.** Good 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.** Good provides strong protections on each platform, with policy controls that include strong encryption of data (OTA and at rest), full device wipe, application white-listing/black-listing, preventing applications from being installed or registry settings from being changed, and detecting jailbroken or rooted devices. On some device platforms, Good can offer granular Bluetooth profile management, disabling transfers and LAN access through the Bluetooth network, while allowing devices (such as headsets) to pair with the device. On iOS devices, Good provides policies to prevent access to the App Store, YouTube, the Safari browser and more, if needed by your business.

## Good Assurance

Good for Enterprise leverages a FIPS 140-2 certified cryptographic module to protect data-at-rest and data-in-transit. Several security-conscious enterprises have approved the use of Good for Enterprise after rigorous internal or third party penetration testing. Additionally, Good helps the US Department of Defense and other US federal agencies comply with DoD Directive 8100.2, Homeland Security Presidential Directive 12 and the Federal Information Security Management Act.

When deployed securely, smart device and mobile application technologies can improve your business processes and yield substantial ROI with lower TCO. You can make your workforce more productive and responsive with the assurance that you're not compromising sensitive data or incurring unnecessary costs.

To learn more about Good solutions, visit [good.com/demos](http://good.com/demos) 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 may be claimed as the property of their respective owners. Good and Visto technology are protected by U.S. patents and various other foreign patents. Other patents pending.