



Security Overview





Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

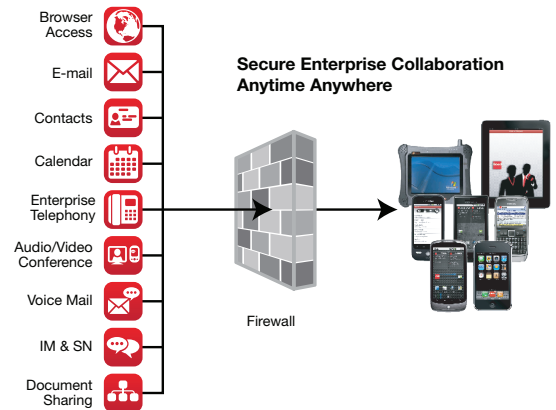
Contents

Changing Mobile Landscape	1
Security Challenges to Enterprise Mobility	1
Coexisting with Consumer Applications	1
Consistent Centralized Control	1
Prevent Rogue Devices from Accessing the Network	2
Good Security Architecture	2
Good Security Model	2
Authentication	3
Data Protection	3
Enforcing Access Controls	3
Securing Network Access	3
Securing the Platform	4
Good Assurance	4

Changing Mobile Landscape

Mobility in the enterprise is undergoing dramatic change, going beyond providing simple access to email, calendar, and contacts toward providing access to a broad suite of solutions that enable true mobile collaboration. Smartphones have become true platforms for connected applications, and enterprises are looking to connect employees, partners, and suppliers to their networks and applications from any location—with appropriate security and control. This includes browser access to intranets, corporate instant messaging, document sharing, collaboration, and enterprise telephony.

With falling prices for increasingly powerful smartphones, employees are purchasing mobile devices and associated data plans for their own personal use. This presents an opportunity for CIOs and CFOs to shave millions of dollars from enterprise budgets that have been traditionally spent on purchasing devices and data plans.



Security Challenges to Enterprise Mobility

CIOs consistently rank security as one of their top IT priorities. The unique nature of mobility outside the walls of the enterprise adds to heightened awareness of mobile security threats. In addition to the traditional risks to enterprise data from lost or stolen devices, today's smartphones present additional challenges to IT administrators entrusted with protecting enterprise infrastructure, applications, and data. The purchase of devices and data plans by employees is leading to the consumerization of IT infrastructure – that is, consumers are using personal devices to access corporate data. To be more productive with their smartphones, employees frequently forward their work—email and documents—to their personal email accounts, undermining enterprise security policies. In many cases, employees disregard IT organization standards and policies because they are not fully aware of the risks. While presenting opportunities for tremendous cost savings, this consumerization trend has introduced several challenges for enterprises. Each of these challenges present critical security issues IT organizations must overcome to fully embrace the benefits of enterprise mobility. Most important among these challenges are:

1. Coexisting with Consumer Applications:

The richness of device types that combine a variety of consumer applications and personalization capabilities leads to tremendous challenges in maintaining the confidentiality and integrity of enterprise data and content while coexisting with myriad untrusted consumer applications as well as respecting employees' private data and applications.

2. Consistent Centralized Control:

Enterprises are struggling to maintain centralized control and enforce consistent security policies on all enterprise content in environments with different devices, different security approaches, and different operating systems. Supporting personal devices and data plans changes the way organizations need to approach control.



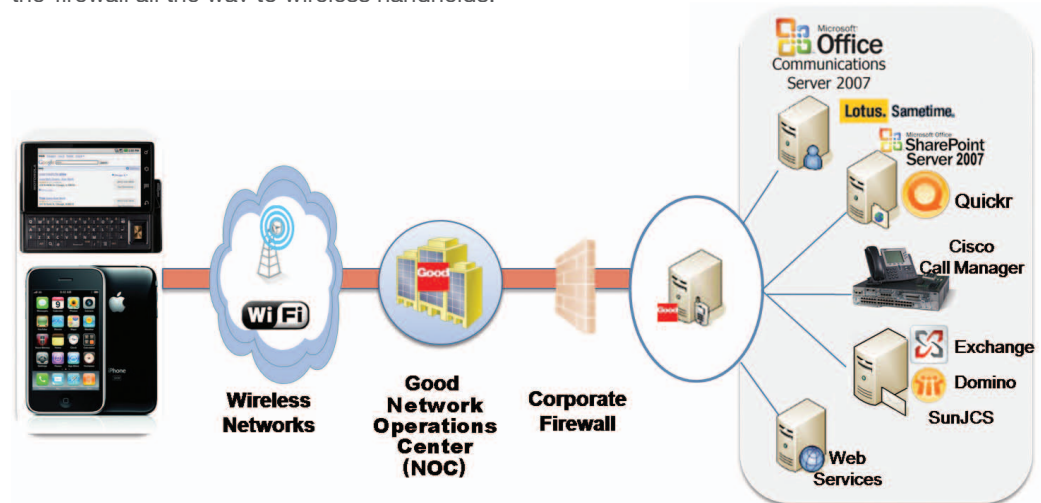
3. Prevent Rogue Devices from Accessing the Network:

The scope and number of mobile devices used today opens the possibility that devices may be replicated and rogue devices could potentially access the corporate network.

Good Security Architecture

Good for Enterprise is a comprehensive platform providing end-to-end, wireless, real-time collaboration and enterprise application access supported by comprehensive device management and security. Good has developed a proven architecture that can help enterprises overcome the challenges they face in embracing enterprise mobility. At the core of Good's architecture is a robust security model that helps enterprises embrace consumer-owned devices in addition to deploying corporate-owned smartphones, while maintaining the same levels of security and assurance.

Good for Enterprise provides mobile professionals with up-to-date information when and where they need it while giving IT the means to secure and manage a diverse fleet of smartphones. The data path through the Good system is encrypted end-to-end; from the enterprise servers behind-the-firewall all the way to wireless handhelds.



Good Security Model

The growing use of smartphones extends the corporate network beyond the physical boundaries of the enterprise and places the end point of the network outside the firewall while utilizing public and carrier networks to transmit data, which raises a multitude of security issues. Good recognizes that managing enterprise security in such an environment is a complex undertaking – especially when it requires providing mobile workers with anytime, anywhere access to the information they need. Good has satisfied the needs of some of the most demanding customers in government, including defense and intelligence agencies; in regulated industries such as financial services, health care, legal, and defense contractors; and in many enterprises in high tech, retail, manufacturing, and other industries. Good has developed a security model that addresses the security of every part of the infrastructure. This model has five key elements:

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com



1. Authentication

Good provides the administration tools necessary to define strong authentication policies that are enforced consistently across all device platforms. Additionally, you can define policies to wipe the Good application 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 authentication policies can include the ability to disable sequential numbers in passwords, require use of special characters, etc. Devices that connect to the Good network operations center (NOC) are authenticated and only users that are enabled by the IT administrator are allowed to authenticate to the NOC based on strong over the air (OTA) security and other policies.

2. Data Protection

With Good for Enterprise, CIOs can be confident that their enterprise data is protected even when their data shares the same device with any number of consumer applications from the iPhone App Store or the Android Market. This assurance comes from the Good Enterprise Container – which is an encrypted cocoon for the enterprise data and applications. This container not only encrypts all the data on the device with strong AES 192-bit encryption but also provides the same encryption for any data that is in transit between the device and the servers behind the enterprise firewall. This approach creates an enterprise container that extends from inside the firewall to the device – irrespective of whether the device is corporate owned or consumer owned. On some devices, Good also provides the ability to encrypt folders and SD cards.

3. Enforcing Access Controls

The Good platform allows administrators to restrict access to Good servers, based on the device OS and/or Good client version numbers. Additionally, Good provides capability to control access to networks from the device, including Bluetooth access.

On the server side, IT managers 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 users. By assigning appropriate roles to administrators, IT can better manage assets and increase security. 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. Administrators can create groups to organize and manage Good users. IT can manage all policies and software distribution at the global, group, or individual user level. This provides IT with more granular control and reduces the time it takes to manage users, especially in larger deployments.



4. Securing Network Access

Good servers establish an outbound connection to the enterprise firewall, so there is no need to open inbound ports and expose the enterprise network to a variety of attacks. In addition, all network traffic between the device and the server is always encrypted with AES 192-bit encryption. The Good NOC does not have access to the encryption keys that encrypt network traffic, so the NOC only services encrypted packets and does not see unencrypted data. The NOC 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 getting access to the network.

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com



5. Securing the Platform

Good provides strong protections on the platform with policy controls that include strong encryption of data (over the air [OTA] and data at rest), full device wipe, application white-listing/black-listing, preventing applications from being installed or registry settings being changed, and detecting jail-broken iPhones.* On some device platforms, Good can offer granular Bluetooth profile management, disabling file transfers and LAN access through the Bluetooth network, while allowing devices such as head-sets to pair with the device. On the iPhone, Good provides policies to prevent access to the App Store, YouTube, and the Safari Browser if needed by your organization.

Good Assurance

The cryptography employed by Good 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 Defense Information Systems Agency (DISA), US Army, US Air Force, and the Department of Homeland Security (DHS) have tested the Good product and approved it for their most sensitive deployments.

Good has deep understanding of enterprise security challenges gained over years of experience and thousands of enterprise and government deployments. The Good platform provides the most comprehensive security for mobile collaboration and data access deployments in the industry.

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

Good Technology
Phone: 866-7-BE-GOOD
Online: www.good.com

*Not all capabilities applicable on all platforms.

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

©2010 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 is 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.