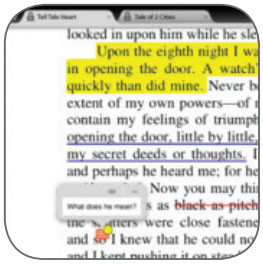
Good™

Secure Mobile Workflows

A Technical Whitepaper



Contents

Secure Mobile Workflows

The majority of employees now demand their choice of apps, collaboration spaces, and cloud storage. Each personalized, consumer-grade workspace enables productive collaboration: employees can efficiently navigate around their workdays and a host of smartphones and tablets.

Collaboration is different from traditional business process workflows that can be automated. Collaboration is dynamic and unpredictable—well, the kinds of things people want to do can be predicted, but the ways, sequences, tools, and interactions are always changing.

For the user, the chief requirements are effectiveness (can I get the apps and data access to do my job?) and convenience (can I do my job on the device I have wherever I am?), which together equal productivity. Collaborations depend on gaining consensus among people who aren't in the same place or time zone. Teams need to share, debate, and edit data and imagery in a natural and speedy way.

Employees will not be denied
Employees aren't waiting for IT. Employees are downloading off-the-shelf, consumer-grade mobile productivity apps from their favorite app stores, then forwarding, storing, editing, and sharing freely—within, beyond, and through the protective policies of the enterprise firewall.

> *Common declarations:*
> *"I do whatever it takes to get my job done."*
> *"It's easier to ask forgiveness than to get permission."*
> *"My boss said it was OK."*

The path to perceived productivity is for a good cause—the success of the business. But the consumer-grade approach places a major, generally unquantified, tax on user efficiency due to the lack of process synergies among the unrestricted apps that users want.

For example, users must purchase, download, and sign-in to each app separately; log into separate websites; and create and store separate passwords. They launch VPNs, navigate to SharePoint, and invite others to a cloud file repository like Box, where the recipient may need to register to gain access. It's not a workflow. It's a series of disconnected tasks: effective (eventually), but hardly efficient.

IT takes the hit
Well-intentioned users generate unintended consequences. Although most users think the cost of an app is its purchase price, each app adds to the management and support burden. Support emergencies spring from lost files and confused users.

Policy management is an ongoing hurdle, since apps weren't built to work together. Policy options are different for each app and IT must juggle and oversee access and policies for hundreds of user-chosen apps. Often, companies that have only deployed basic Mobile Device Management (MDM) systems are stuck with software that wraps each corporate app in separate policies, rather than managing apps in a consistent, unified way.

Many collaboration apps—including instant messaging and email—require server-side components. IT typically tries to find economies of scale by consolidating and standardizing these server elements in managed file repositories. This is a mostly hidden extra IT cost required for mobile collaboration.

Plus, the "consumer grade" approach provides zero protection for business data. In fact, this approach increases enterprise risk by necessitating servers in the DMZ and holes in the firewall that can lead to compliance violations and data breaches.

Tablets force a confrontation
Time is up for adopting an "enterprise grade" solution. New devices have accelerated the need for a solution that achieves all these goals. Although smartphones are a bit too small to be the perfect device for mainstream enterprise use, tablets are a very reasonable and rapidly proliferating productivity tool. The capabilities and broad adoption of tablets make it extremely likely that confidential information is being downloaded, stored, shared, and exposed in your organization right now.

A Good Workflow is a Flexible, Manageable Workflow

Good offers a complete and open end-to-end app ecosystem that enables fluid, flexible collaboration workflows within a manageable and secure framework. It provides a satisfying compromise between the environment IT must have to say "yes" to users and the experience users need to be productive.

The Good Mobile Collaboration solution does three things to enhance collaborative workflows. First, it manages the sign-on and authentication processes for the different required apps in a single repository, with policies managed from a single console. That brings the convenience of just one fast but strongly authenticated single sign in to users and one full-featured, policy-based identity management environment for IT to navigate.

Secondly, the workflow includes a full set of collaboration features with no interdependencies. Apps can be used in any order, permitting organic and spontaneous collaboration according to each user's preferences. Maybe a user collaborates by email, maybe by IM, maybe by uploading a file to a shared repository, then emailing or IMing out a link to the eager recipient, following up with a text message. Whatever the workflow, Good lets users work naturally.

Finally, data and process security are integrated into the collaboration workflow to be effective but unobtrusive. Communications between the apps (both within the device and through the cloud) are isolated and secured with encryption, and communications over the network are encrypted and processed through the highly secure Good Network Operations Center. Data used by the collaboration apps is stored in the Good for Enterprise repository, an encrypted and managed container on the device.

These strengths add up to a much more productive and predictable experience for both users and administrators. Let's compare the Good solution to the typical ad hoc, consumer grade approach in a merger scenario:

> *Company A's board of directors is contemplating a merger with Company B. The CFO schedules a review meeting and attaches the revised merger proposal as a PDF to the board members' invitations. The board members need to review the new paragraph and initial their approvals of a higher asking price.*

Action	Good "Enterprise Grade"	"Consumer Grade"
Setup	Administrators define policies for Good apps as well as approved third-party editing apps. They then associate apps with the users in the corporate directory and publish the apps to either a custom storefront or an approved app store (Apple App Store or Google Play). Users download new versions as needed, and IT can push mandatory app updates as required.	Users download whatever they want from any app store, or request the desired app from IT and wait a week for it to be "wrapped" and released for consumption. IT wraps the apps in policies as best they can to make them work with the MDM software and comply with corporate rules. Password length and complexity options vary, so users have different passwords of differing strength for each app.
PDF viewing	Board members receive a file in email and open the PDF file in an annotation app on their various smartphones and tablets. Single sign-on means no one has to enter extra credentials.	Users receive the file in their personal email accounts on their devices. Several board members have to download a PDF editing app from their preferred app stores and create a login. Then all users sign in to their apps, open the file, and review.
Email with attachments	In one "reply to all" message, he is able to send both the marked up document and the spreadsheet back to the full board.	The CTO uses native email for his personal mail, which doesn't permit attachment of multiple messages, so he has to send the two files separately. These corporate confidential messages are stored in the native email system.
IM	The CFO sends a secure IM to the CTO, saying he received the docs, he agrees, and that he will be posting a revised acquisition PDF in the finance SharePoint repository.	Board members message each other using Facebook, Yahoo! or SMS, exposing confidential ideas and information through these public consumer channels.
SharePoint access and file editing	The CTO checks out the latest version of the acquisition PDF from SharePoint, opens in his PDF annotation app, signs the doc, and checks the doc back in for the next signature.	The CTO boots up the VPN on his tablet and logs into SharePoint to download the updated file. He opens in his editor app, signs the doc, and checks the doc back in for the next signature.

Inside the Good Solution

The cross-device Good Mobile Collaboration solution includes core apps that Good has engineered for user productivity and IT convenience. The Good software is deployed and managed from a highly scalable management console, streamlining mundane software distribution, monitoring, reporting, and help desk tasks. In addition, Good partners with third parties whose capabilities cover the collaboration spectrum to support complete and open-ended workflows.

Here, the components of a Good solution are:

- **Good Share—**Without the hassle of a VPN, users can access, sync, and share files located on file servers behind the corporate firewall. For instance, salespeople can get the latest versions of presentations from marketing SharePoint servers, upload proposals for approval by sales management, and distribute forecasts securely.

- **Good Connect—**Instant messaging goes mobile with this secure extension of corporate IM platforms including Microsoft Lync and OCS. Integrated with the corporate directory, users can see who is online, communicate via IM, email, or a call, and look up colleagues, all without logging into a VPN or resorting to consumer tools. IT can offer users this convenience without increasing the risk to the enterprise caused by encrypted VPN traffic coming in through open ports in the firewall. IT also avoids the management complexity and expense of deploying special IM servers in the DMZ. Corporate and personal data remain separate for privacy and security.

- **Good for Enterprise—**Intuitive for any enterprise email user, this app offers email, contacts, calendar, tasks, and browsing for easy access to corporate and Internet content and communications.

- **Good Dynamics Platform—**Enterprises use this platform to leverage third party apps and develop and support custom apps that implement security at the application level, with each app's data protected from rogue applications, malware, and device loss.

- **Third Party Partners—**Dozens of Good Dynamics partners offer spreadsheets, PDF markup, cloud storage, social media, dashboarding, printing, and vertical BI solutions through the convenience of public app stores. These apps are pre-integrated with the Good solution for single sign on and data security. Any of these apps can be used in any combination with the Good apps to create on-the-fly workflows.

Tested integrations among Good apps and these partner solutions are an important way that IT can accelerate policy development and application deployment compared to the "consumer grade" experience. In addition, Good offers app wrapping, so that internally developed and third party apps can be added to the "approved" list and distributed, controlled, and managed through the application lifecycle. Internally developed apps can integrate Good libraries into their code to permit app-specific policies, such as controlling file access based on file size. Third-party apps can gain an application security "wrapper" without IT having to write or integrate code.

IT can regain control
IT can enforce fundamental security controls like requiring a single strong password across all apps and blocking jailbroken devices from accessing the corporate network. To restrict data loss, app capabilities can be constrained by disabling features like cut, copy, and paste between apps. Should the device be lost or stolen, IT can remotely lock or wipe the device.

Behind the scenes, the Good framework provides secure data storage and secure policy-based transmission between workflow components. This framework permits users to enjoy the apps and the processes that make sense to them while adhering to data security policies. Unlike alternative enterprise offerings that redistribute risk, Good goes beyond simple encryption and point security efforts to create an integrated security environment that reduces overall risk to the enterprise.

The Good solution builds on the Good for Enterprise container, a secure repository on the device that protects corporate data and enforces centrally managed policies, including policies for off the shelf, Good, and custom developed app usage. The data in the container is separate from any personal data stored on the device. This model preserves the privacy of the user and permits storage of personal contacts, music, apps, and other content where it won't be wiped when enterprise data is deleted from a personally-owned device.

Data security throughout the workflow
As data travels between apps on the device itself, the data is isolated from the operating system so it can't be sniffed by malware or exposed to unapproved apps. Any data or file stored by the apps is safely held in the secure Good container. And only specified and approved apps can join the workflow.

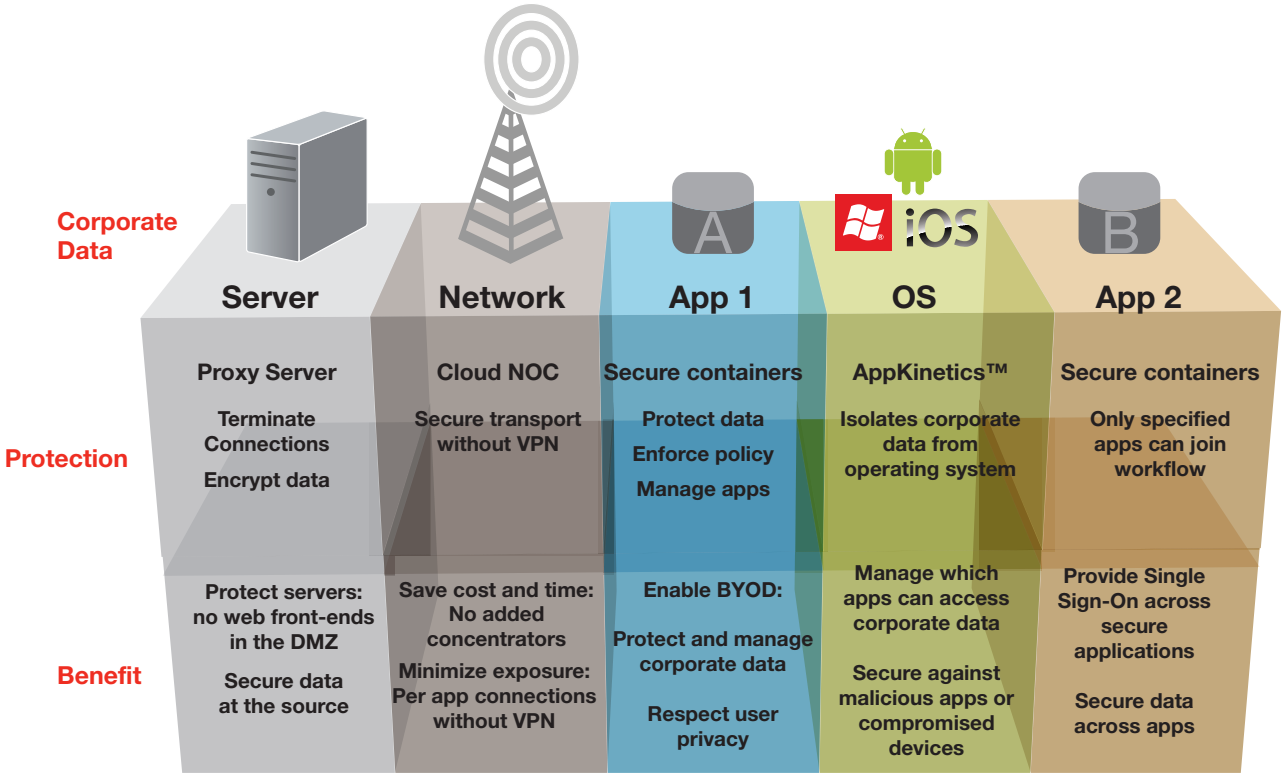


Figure 1: The Good framework incorporates manageability and security into each component of the collaboration workflow.

Mobile Collaboration that Works

Consumer technology is freeing enterprise users to work when, where, and how they want to. To regain control, IT must offer, manage, and support the full range of compelling features required by different user communities while remaining compliant with corporate and regulatory policies for privacy and data protection. Performing this feat within constrained human resources means finding and creating efficiencies in day-to-day management of mobile app operations.

Good and its enterprise-class partners provide a technology framework that encourages collaboration within manageable boundaries. As devices, app capabilities, and user expectations grow, IT can use this system to say “yes” to users without compromising needlessly on cost and security.

About Good Technology

Good Technology is on a mission to create a world where mobile device users can travel freely, access web servers, exchange files and messages, engage with applications, collaborate with others, and never put sensitive personal or business data at risk. We’re building the industry’s best platform for mobile security because we see a digital world where important information can go anywhere securely.

Joining us in this vision are thousands of enterprise customers in 90+ countries. They are Fortune 100 leaders in financial services, healthcare, retail, telecommunications, manufacturing, legal, and government agencies. They are leading device manufacturers (including Apple, LG, HTC, Microsoft, and Nokia), leading systems integrators, global carriers, and government agencies worldwide.

Learn more about Good Mobile Collaboration Solutions by visiting www.good.com.

©2012 Good Technology Corporation and its related entities. All rights reserved. Good, Good Technology, the Good logo, Good for Enterprise, Good for You, Good Dynamics, Secured by Good, Good Connect, Good Mobile Manager, Good Share and Good Dynamics AppKinetics are trademarks of Good Technology Corporation and its related entities. All third-party trademarks, trade names, or service marks may be claimed as the property of their respective owners. Good’s products and technology are protected by U.S. patents and various other foreign patents. Other patents pending.