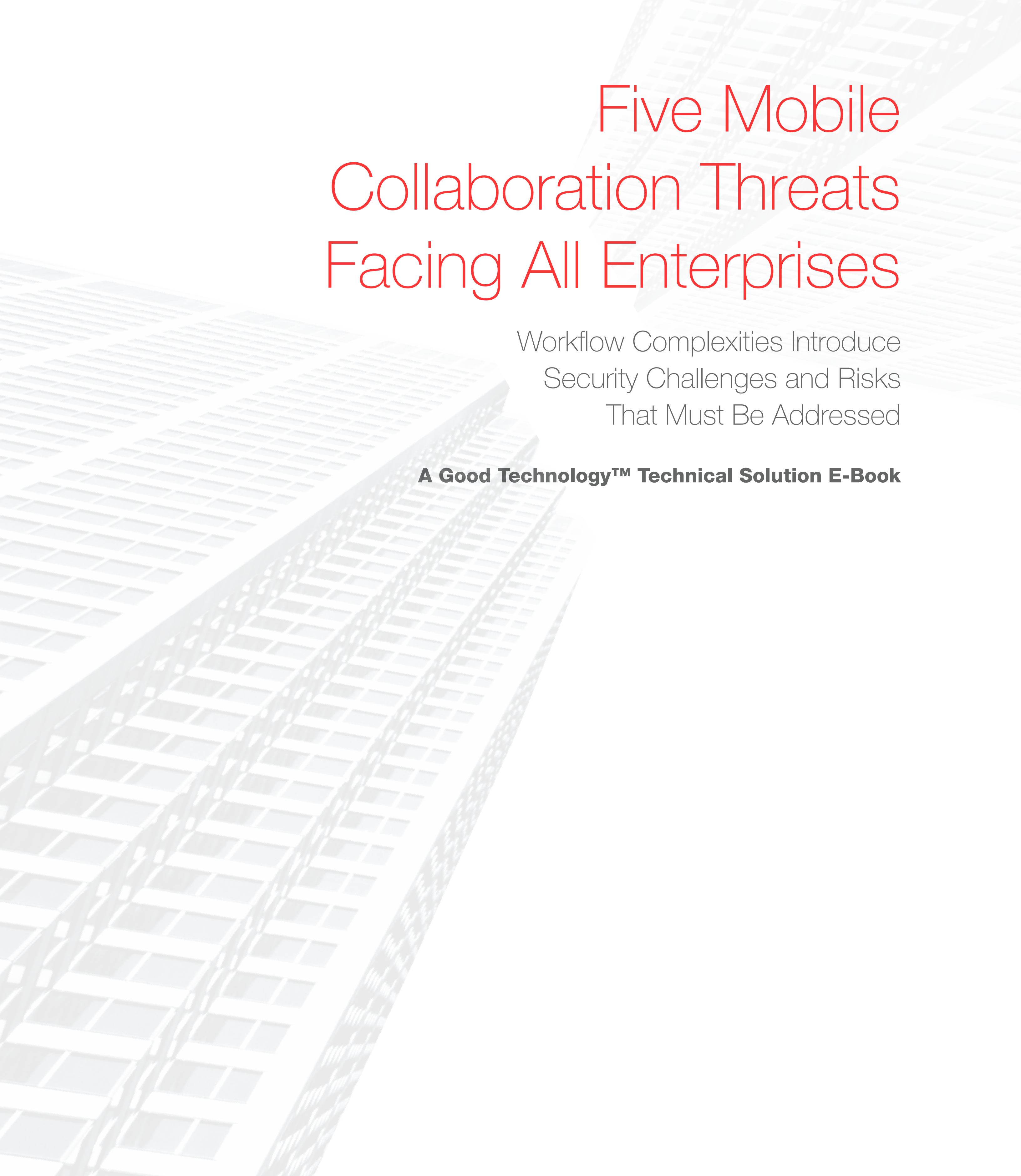


Five Mobile Collaboration Threats Facing All Enterprises

Workflow Complexities Introduce Security Challenges and Risks That Must Be Addressed

A Good Technology™ Technical Solution E-Book

Table of Contents

Executive Overview

Mobile collaboration—the ability for end users to work together and deliver greater business value from any place in the world at any time—presents a tremendous opportunity for businesses. The consumerization of IT leverages the unprecedented growth of smartphones and tablets in the workplace to make mobile collaboration a competitive necessity.

Nearly 50% of enterprises have developed or are currently developing mobile apps, while nearly 80% of US enterprises practice the Bring-Your-Own-Device (BYOD) approach.[1] Employees and senior executives alike demand the freedom of BYOD so they can accomplish more at work, and even work more often when not in the office. In return, enterprise businesses and public-sector agencies benefit from the ability for teams to collaborate effectively at any time from any place—at the office, at home, on the road, or even in the air. According to a report from the Aberdeen Group, IT departments must now include enterprise mobility—along with public clouds, private clouds and social media sites—as essential components of their corporate infrastructures if corporations are to compete effectively.[2]

Along with the great productivity benefits that mobile collaboration promises, there are also risks that must be addressed and mitigated. Organizations face several types of threats that could lead to stolen corporate data. This not only threatens competitive advantages but also runs the risk of regulatory compliance violations that could lead to large fines.

Taking steps to protect information in the mobile world is particularly critical, since the latest mobile technology makes it possible for end users to utilize their own personal devices to access corporate information and collaborate with colleagues, potentially exposing corporate information outside the corporate perimeter. While the use of these technologies improves efficiencies and drives up productivity, organizations must apply extra security measures to protect their electronic information—not just at the device management level, but also across applications and the data itself.

This white paper examines five primary risks that enterprises face when deploying and supporting mobile applications. Individually, each threat may not pose significant risks. However, considering all five threats are in play 24x7, organizations must rely on a comprehensive mobile application platform to ensure data security at all times on all popular device platforms.

This paper also presents use-cases illustrating how mobile collaboration has a positive impact on various industries. The paper then presents the benefits of an integrated enterprise-ready secure mobility platform and the various process efficiencies gained by adopting business-enabling mobility.

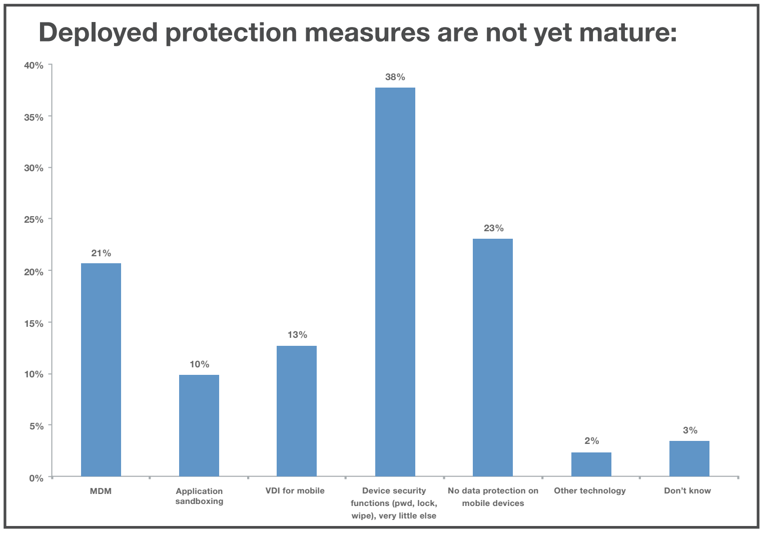
Security and convenience should not be a zero-sum game. Security must not block progress to transform businesses.

The Five Common Mobile Collaboration Risk Categories

Enterprises are keenly aware of the benefits mobile collaboration technologies provide as executives and users interact with applications more easily and efficiently—both individually and as a team. Whether using smartphones, tablets or laptops, users can share and process information in ways that not only improve products and services delivered to customers, but also streamline administrative tasks such as invoicing and data exchanges with business partners across the supply chain.

When selecting mobile technology, businesses face a significant road block: the missing or limited security features and controls that mobile devices and mobile applications introduce. All organizations must protect their data and comply with government and industry regulations that enforce strict guidelines on the handling of electronic data.

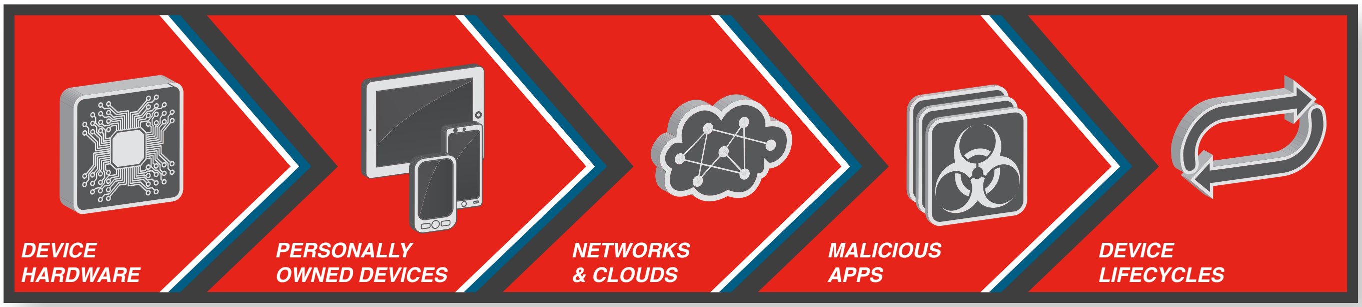
Without applying the proper technology safeguards, mobile devices and applications will not meet compliance standards and may subject businesses to significant fines. This is particularly true when users exchange electronic information with their peers and business partners without applying a level of due care for the data. In some cases, employees may act maliciously; more often, they simply just make expensive mistakes.



Deployed protection measures are not yet mature:

Source: "Mobile Security," presentation by Chenxi Wang, Ph.D. Vice President & Principal Analyst Forrester Research – March 2013

Mobile Environments Contain 5 Primary Threat Elements



Mismanaged Device Lifecycles

These threats include data loss that occurs when users lose their mobile devices as well as when devices are stolen or decommissioned. In addition to data owned by the company, users can also potentially lose their personal data if an entire device is wiped by the organization. Wiping an employee's personal data could place the company in a potentially costly legal situation.[3] Consider, for example, the deletion of a personal portrait that can never be recovered; this could upset the employee. Companies are not responsible for personal data, but it is in the organization's best interest to protect personal information on behalf of the staff—especially if staff members agree to use their personal devices for business purposes.

The device lifecycle threat is one of the most difficult to thwart because people literally carry their devices 24x7 everywhere they go, and lost/stolen devices occur frequently. In addition, many people choose weak passwords or fail to use any password at all. When combining these factors with the lack of device data-encryption, companies leave themselves wide open to data theft. Organizations and end-users may also decommission (sell or discard) devices without realizing corporate data must be wiped first, which begs the question: In whose hands did the corporate data land?

Potential Mismanaged Device Lifecycle Risks

- Lost devices
- Stolen devices
- Devices that go unused or get discarded when users upgrade to a new device
- De-provisioned devices the company or end users give to another user or sell to the general public
- Transfer of data from corporate apps to personal apps

In all of these cases, businesses risk the possibility of unexpected device access by someone with the potential to view and extract sensitive corporate or personal data.

Uncontrolled Personally-Owned Devices

Many businesses support Bring-Your-Own-Device (BYOD) policies which help increase staff productivity by giving users the freedom to use their personal devices for business purposes. Familiarity with their own devices—and the tendency to carry devices on their person at all times—prompts users to interact with applications more often.

Unfortunately, bring-your-own devices also carry a higher level of risk than devices owned by the company which are typically directly managed and controlled by IT. Some devices in BYOD environments have limited or non-existent data protection, as users often disable the encryption functionality, set weak passwords, and re-use the same passwords across personal/corporate log-ins. These "user-friendly shortcuts" make it easy to access the then-decrypted corporate data.

In some cases, users even turn off passwords, bypassing the encryption altogether. Users also sometimes refuse to enter complex device passwords and may demand the removal of such restrictions. This can lead to corporate data no longer being encrypted. Users may also not understand how to use devices in conjunction with company security and regulatory policies—often connecting their devices to and sharing data with other devices they own via cables and networks.

Additionally, while bouncing back and forth from personal to business applications, users may inadvertently transfer corporate information into a personal application, thereby exposing that data to others who have access to that application. Finally, a number of personal applications obtained from app stores often gain access to contacts, calendars, storage media, and other elements on the device—leaving corporate data wide open to theft.

Potential Uncontrolled Personally-Owned Device Risks

- Limited encryption
- Mixture of corporate and personal data
- Weak passwords
- No passwords
- Access to corporate systems, repositories, and data by personal applications
- Lost and stolen devices

Given these conditions, devices in BYOD environments that are misused—either intentionally or by unsophisticated users—could give malicious hackers access to corporate data via shared devices or by the cracking of inadequate passwords.

Vulnerable Device Hardware and Software

Mobile hardware devices and their operating system software contain vulnerabilities susceptible to breaches that could allow hackers to gain access to data. Furthermore, malware attacks could degrade system performance or shut down services, applications, or even the entire device. Just because devices haven't been exploited yet doesn't mean the risks are not there.

Additionally, operating system developers, device manufacturers and carriers all apply their own hardware and software configuration changes to create a unique ecosystem. The devices must be protected to the same degree as desktops—with the added challenge of defending against threats for which cellular networks are susceptible, such as spoofed/fake cellular towers and other wireless access points created by malicious actors.

Equally troubling is the fact that carriers and manufacturers work together to apply updates to devices over the air—oftentimes without user approval or acknowledgement. On the other end of the spectrum, even though carriers control a large part of the update process, they do not always deploy updates associated with protecting smartphones against malware.[5]

In addition to verifying that all appropriate updates have been uploaded by carriers, businesses should also consider whether their IT teams have approved the use of the latest social networking app or instant messaging app that a carrier installed. These apps can automatically access corporate contact lists and meeting details, which could allow an outsider to access the confidential information. The apps may also automatically access enterprise data, such as client lists, which could create an even bigger problem for the breached enterprise.

Potential Vulnerable Device Hardware and Software Risks

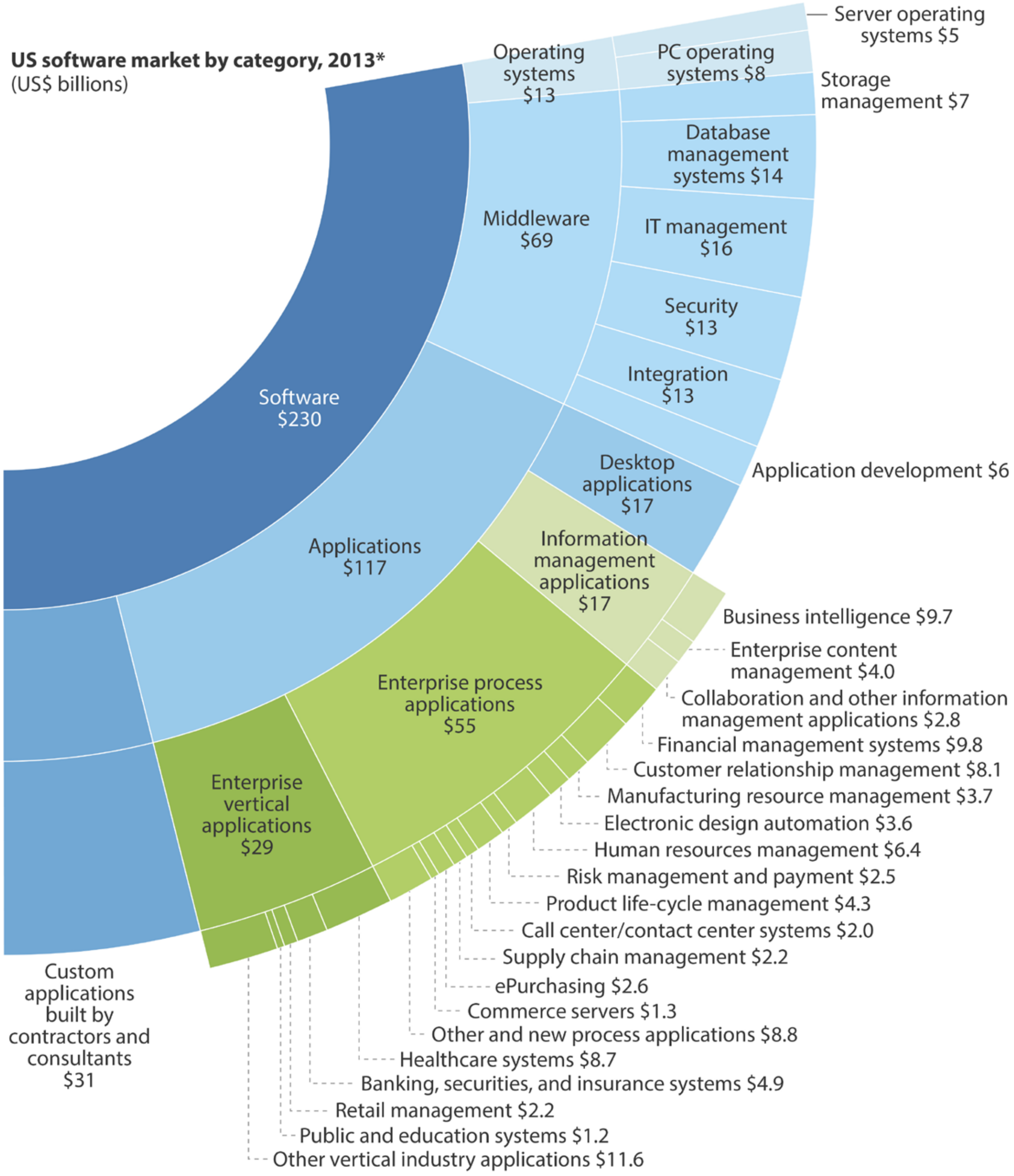
- Hardware vulnerabilities that vary by manufacturer and by carrier
- Operating system vulnerabilities that also vary by manufacturer and carrier

These conditions have proven particularly challenging for personal devices running on Android and Windows operating systems that feature open source application coding. But even Apple devices running on iOS have come under recent attacks, driven in part by the popularity of "jail-broken" devices—which allow any application to run, even if not from the approved Apple App Store. iOS apps can pose just as great a risk to users as Android apps. No device is bulletproof.

Malicious and Poorly-Designed Apps/App Stores

A recent report from Forrester[6] forecasts software purchases will grow by 6% in 2013, with commercial software expanding by 8%. Within this space, mobile, collaboration, business intelligence, and analytical apps are expected to be the hottest growth areas—with construction, transportation, education, and healthcare leading the charge from an industry perspective. Continued investments are expected in the financial services, insurance, manufacturing, and public sector verticals.

It's also interesting to note that, in addition to the commercial app forecasts, the Forrester report projects that custom applications built for organizations by contractors and consultants are expected to reach $31B in 2013 as illustrated by the graph below:



*Forrester forecast

83003

Source: Forrester Research, Inc.

Although the leading application marketplaces such as the Apple App Store have built-in application security checks, the level of access required by each application and the level of security that each application provides vary widely. For example, many data collection processes used by mobile applications are not necessary—either asking for too much data access or gathering more data than they need. This creates more ways for malware to succeed in an attempted breach and data extraction.

Consider for a moment an app store receiving tens of thousands of submissions per week. It is nearly impossible to vet every application for every aspect of security. Even with automation, threats can be missed, even if only because the threats change. Some malicious application developers even understand how the vetting system works and build their applications to bypass the checks. They turn off the malicious code segments while running within the automated environment and turn on the malicious code segment when running in production—well after the app store has let it out into the wild.

Even vetted apps have weaknesses; clear-text passwords used by consumer apps allow hackers and other malicious apps to view user password lists. Because users often re-use the same username and password across a number of applications, attackers can easily gain access to corporate systems and resources.

Potential Malicious and Poorly-Designed Application/App Store Risks

- User-installed apps
- Clear-text passwords
- Insecure (non-SSL) HTTP communications

Facing these conditions, poorly-designed apps and apps written with malicious intent are left open to a wide variety of malware and spyware. Users who download such apps become targets of click-jacking, vishing and phishing campaigns that may cause systems to malfunction or even worse, provide access to corporate data. Multiple open ports across a variety of apps not only impact performance but also introduce configuration and policy enforcement complexities, which could leave weaknesses exposed.

Exposed Public Clouds and Open Network Access

As the number of mobile users increases, and as carrier data-access costs remain high, users access the Internet more frequently via free, public-access Wi-Fi hot spots. The exponential number of hot spots that have emerged in recent years adds to the amount of time end users spend on these networks, which are often left wide open to attack.

Devices connected at all times to an open network present a core risk: Corporate data residing on the device and data accessible to the device are often shared through and stored on networks and storage areas beyond the control of IT. Individuals and teams want access to their content and often need to share content with colleagues, peers, and partners. Where IT is unable or unwilling to provide the ability to share this content via mobile devices, employees will find a way. The corporate data then finds its way outside of the organization.

Businesses that rely on a Virtual Private Network (VPN) for mobile-device access face additional network access risks. Deploying a VPN for each user and each of their devices requires IT to create multiple ports for each application. Each port thus provides a potential entry point through the security perimeter for hackers. For businesses with hundreds of mobile apps connecting to the enterprise network, the management of security policies through the firewall also leaves the network vulnerable to human error due to the many users, their many roles and their multiple devices.

If a device with access to a VPN is compromised, the person who breached the device gains authenticated access into the entire corporate network. VPN solutions do work well in the PC world, but they can negatively impact mobile-device user experiences and drain battery life. Also of concern is the possibility of some network traffic operating outside of the VPN—even when configured not to do so. This can expose company data outside the enterprise network either deliberately or accidentally.[7]

Potential Exposed Cloud and Network Access Risks

- Public cloud storage (the “drop box” effect)
- Cellular network connectivity
- Public/private cloud mixture
- Device-level VPN for all apps (network complexities and battery drain)

These risk developments have dramatically increased the number of opportunities hackers have to gain access to corporate networks and the information they host. When content from corporate resources finds its way onto devices, users often share the content with others inside and outside the corporate network. They often choose to use commercial public cloud storage apps, which presents the potential for the content to leak from the organization. When hackers gain shared network-access via a vulnerable device connected through an insecure Wi-Fi hot spot, a cellular network, or a VPN, they can establish rogue access points that enable eavesdropping, the compromising of mobile devices, or even malicious code injection on a network.

Mobile Collaboration Workflows: Balancing Productivity with Risk

Mobile technology provides all industries with the ability to enable their workforces to operate more efficiently and share information more immediately. These capabilities in turn lead to improved customer service levels and reduced operational costs. Following are a few sample use cases:

Industry	Mobile Collaboration Benefit Example	Possible Risk
Healthcare	As doctors and nurses move throughout medical facilities, they can use tablets and smartphones to quickly access patient information, leverage visual aids while communicating with patients, and collaborate with colleagues.	When information flows slow down or fail to deliver critical data on time, patient health can suffer, and lives can even be placed at risk. HIPAA requirements to protect patient data place healthcare facilities at risk if data is exposed.
Manufacturing	As users move across large plant facilities and campuses with multiple buildings, they can easily communicate on equipment performance, production levels, system maintenance/repair issues, and general logistics coordination.	External data breaches or internal leakage could lead to competitors gaining access to intellectual property.
Financial Services	Advisors and brokers can more easily stay connected with clients and colleagues to discuss financial strategies and to act on security buy/sell decisions before market conditions change.	Information leakage through lost and stolen devices as well as data breaches from external attacks could provide competitors with key information that leads to an unfair advantage.

Industry	Mobile Collaboration Benefit Example	Possible Risk
Legal	Legal teams can collaborate with colleagues whether in court, at the office, at home, or on the road.	Mishandled information could violate client confidentiality.
Utilities	Service managers and field users can communicate immediately on the status of maintenance and repair orders.	Confidential consumer information could be accessed by malware.

When deploying mobile technology, enterprises must ensure they employ a security platform that prevents external attacks that exfiltrate data. Enterprises should also establish Internet systems that block denial-of-service attacks while also protecting against internal data leakage that can occur when mobile devices are stolen, lost, or misused.

Every industry needs to be concerned with security when enabling mobile collaboration. Sensitive business data could be lost, such as company financials, and intellectual property could be stolen. Private customer data could also be at risk, which could create a loss of customer faith in the company. In addition, malicious access to systems could bring company business processes down through denial-of-service attacks or could be used to control systems to cause mass destruction.

Building Secure Mobility From The Ground Up

Relying on disparate mobility security components typically forces enterprises to spend too much on managing their environment and mitigating too much risk. Multiple components can also lead to an increase in end-user calls looking for exceptions to their business workflows that cater to their individual preferences.

To take on the mobility security challenges presented previously, deploy a secure platform that provides the ability to select and build apps that enable any mobile workflow imaginable—but in a secure and scalable way with complete enterprise-grade management. The platform should provide all of the following capabilities:

- Management of BYOD devices and corporate-liable devices
- Secure communications and storage
- Global, multi-user/multi-app scalability
- Online and offline consumer-like performance
- Operations center with high availability and redundancy
- Fine-grained policy control supporting line-of-business workflows, internal requirements, and external regulations

Equally important, the platform should tie together multiple mobility management functions into a single enterprise-grade, mobile-first solution:

- Mobile Device Management (MDM)
- Mobile Application Management (MAM)
- Enterprise App Store
- Secure App Wrapping and App Development
- App-to-App Integration

Achieving Mobile Maturity With "Mobile First" Best Practices

When starting any long journey, it is important to keep the end goal in mind. It may be tempting to conclude that the first enterprise mobility management issues to arise—such as controlling corporate and personal devices—can be resolved through mobile device management (MDM), and that MDM is all that will ever be needed.

However, achieving mobile maturity requires a long-term view, a comprehensive plan, and a solid foundation. Enterprises should consider three stages when moving to mobile maturity, and while each stage addresses certain risks, the stages must work together as part of a comprehensive strategy to preclude a "weak-link" vulnerability in the corporate mobility strategy.

Gain Control: Properly Manage Personal and Corporate-Liable Devices

Adopting MDM is a necessary first stage to enable secure mobile users, but deploying an MDM solution alone is not a sufficient step. MDM allows a company to control many aspects of a mobile device and is the tool to use when devices have been lost or stolen.

However, MDM does nothing to secure data used by apps, nor does it allow corporations to develop and deploy secure apps. As an example, many apps—especially BYOD apps—have "connectors" to allow data sharing with social networks and in cloud storage. MDM does little to nothing to prevent secure corporate data from being accessed by these apps, Thus, "leaking" data can occur as these connectors can then be shared with the public.

Embrace Mobility: Select, Wrap, Develop, and Deploy Secure Mobile Apps

After a company has addressed the problems addressed by MDM, it can move to the second stage, which focuses on issues related to apps. A mobile application management solution (MAM) is the next step, but this too must be seen in the context of a larger mobility management perspective.

MAM solutions allow a company to reduce, and in some cases remove, the threat of data loss or theft from applications. Corporate-developed apps can be built utilizing a software development kit that controls data flows and access. Existing apps can also be "wrapped" to redirect data flows into approved apps and containers.

An approach of note is the use of a secure container for the app and its data. While "wrapping" an app offers some control over data flows, the app still stores data locally. The data should thus be encrypted. If the app and its data are in a secure container, the data is theoretically protected.

Unfortunately, some container solutions rely solely on the native encryption of mobile devices while others support levels of security and encryption approved for use in government, regulated, and high-value industries. The former approach is vulnerable when device passcodes are broken while the latter can ensure constant data integrity.

A side note: in BYOD environments, the native-encryption container approach often leads companies to enforce lengthy passcodes, which has the unfortunate side effect of forcing BYOD users to enter the lengthy passcodes merely to listen to music or view photos. The highly-secure container approach functions independently of the passcode, so users may choose shorter passcodes without threatening corporate data security.

Advanced MAM solutions allow corporations to set up their own app store that provides these corporate-written and security-wrapped apps to employees and customers. Some of these private-branded app stores have the capability to support searches, user reviews and feedback as well as revision history; others are merely catalogs listing available apps.

Another approach of note is to test the wrapped and the corporate-developed apps for security holes and data leaks. It makes little sense to wrap or build an app and publish it to your employees or customers if that app is not proven to be secure. Independent third-parties can review, test, and certify apps. At least one platform vendor provides this capability to ensure the integrity of any wrapped or corporate-built apps.

MAM alone, though, does not address the needs of most line-of-business mobility deployments.

Transform With Mobile First: Deliver Secure Mobile Workflows for Each Line-of-Business

The third stage in the mobile maturity growth path enables a company's lines-of-business to embrace mobile workflows as a means to drive revenue and operating efficiencies. This means that on a secure device (MDM), using secure apps (MAM) and secure containers (enterprise mobility platform), organizations can enable a secure method for employees, agents, representatives, partners, customers, and others to interact with the business on their mobile devices.

When securely containerized apps can share secure data with each other on a secure platform, the company can set up a secure end-to-end workflow that allows an entire process comprising multiple tasks to be accomplished. With this level of integration, organizations can begin automating processes that have never been automated before, taking full advantage of the capabilities introduced by mobility. The benefit to the business by using this multi-stage model is that this can be accomplished while addressing risk and security in front of the curve.

Of course, this level of secure workflow can only be achieved when all of the preceding steps have been deployed, and this marks the last step in mobile maturity—transforming the way business is conducted by providing a secure mobility platform with centrally managed devices, apps, and communications.

Mobile collaboration means that organizations can compete more effectively while they also reduce time and cost and as they approach and open up new markets. Embracing security-first mobile collaboration also means IT can build and deploy a BYOD strategy while remaining confident in the security of the devices, corporate data, and workflow management.

Enabling Secure Mobile Workflows with the Good Dynamics Secure Mobility Platform

To enable line-of-business workflows while preventing data loss, many global enterprises and top government agencies around the world have turned to the Good Dynamics Secure Mobility Platform as it enables them to deliver on the mobile-first productivity premise while adhering to mobile-first best practices. The selection is typically based on the fact that Good Technology has leveraged more than a decade of experience in secure enterprise mobility, enabling the company to offer the Good Dynamics Secure Mobility Platform that supports organizations regardless of where they are on their mobile journey.

The containerized capabilities of the Good Dynamics Secure Mobility Platform allow enterprises to establish multiple controls at the app level:

- Encrypting data on devices
- Segregating corporate data from personal data
- Requiring application passwords
- Applying shared authentication

Part of the Good Secure Mobility Solution, the Good Dynamics Secure Mobility Platform also minimizes data loss even if devices are compromised. This lets IT say ‘yes’ to user application usage requests while also ensuring secure workflows. For securing data at the application level, Good Secure Mobility Solution app containers essentially allow enterprises to separate corporate data from personal data on the device and apply controls and policies at the application level.

The containers also provide an extra level of protection should devices become compromised. For example, even if a device is jail-broken, the application data will continue to remain encrypted if the application is encrypted using the application password/key and not the device password/key.

The following capabilities allow organizations to deploy enterprise-class mobility solutions that secure and distribute apps while also providing control of the apps on any device:

- **Shared Authentication:** After authenticating into a Good Dynamics enabled app, users do not have to authenticate to other Good Dynamics enabled apps because they are checked against the master app.

- **Secure Document Collaboration:** Secure exchange of documents (such as trapping Open In/Open With/Save In) between Good Dynamics enabled apps ensures documents remain secure throughout entire workflows. Corporate data never spills into personal applications, even if both corporate and personal apps co-exist on the same device.

- **Shared Services:** Enables creation of apps that provide a secure print app that is published as a shared service. For example, if an iPad-based CAD design editor needs the ability to print, rather than write code for printing in the CAD-design editing doc, the shared print service published from the secure print app could be used instead.

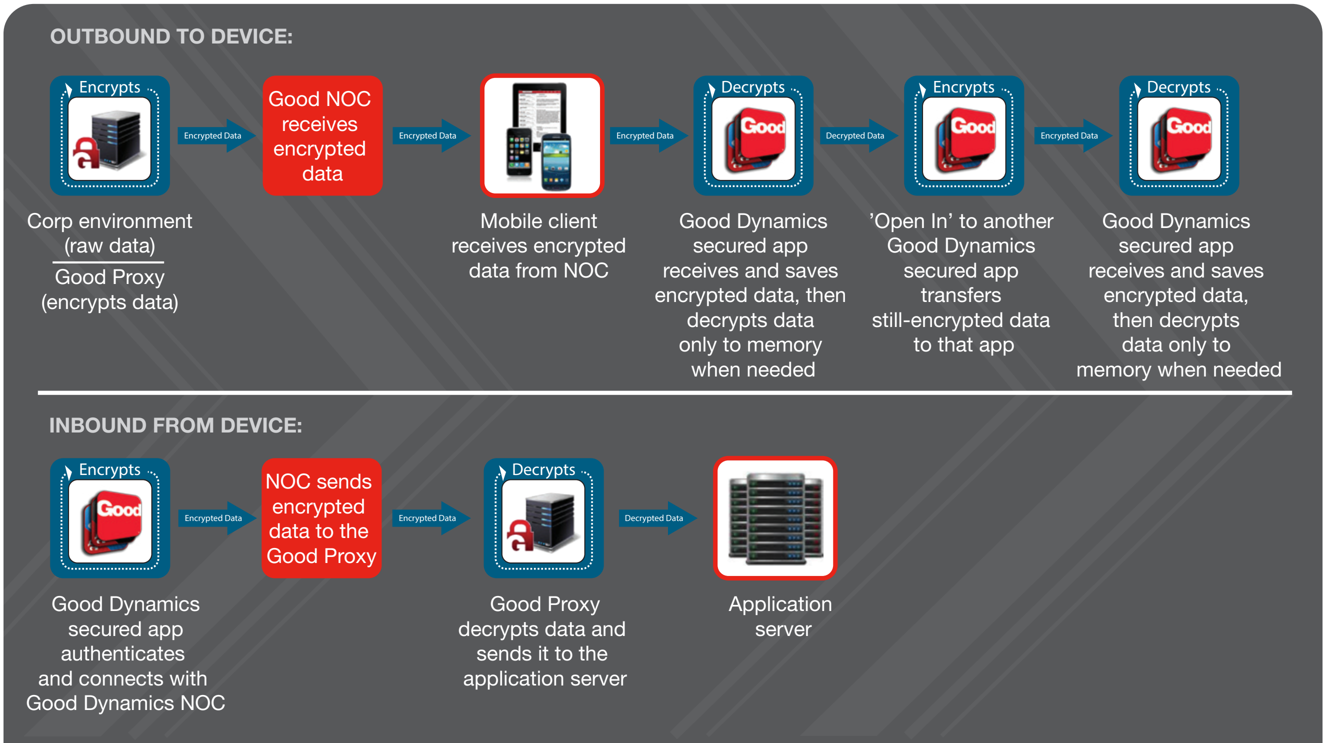
- **Custom App-Specific Policies:** Gives developers the ability to define app-specific controls in an XML file and manage the policy through the same console as the default Good Dynamics policies to eliminate the need for another management console. For example, if a human resources app makes tabs visible depending on the Active Directory membership of users, a director might see the admin tab while an employee might only see the view tab.

Mapping of Controls to Overcome Mobile Collaboration Risks

Mobile Collaboration Risk	Mitigation Strategies	Good Technology Control
Mismanaged Device Lifecycles	• Policy-driven mobile lifecycle management • Remote device management capabilities to enforce compliance	• Mobile Device Management
Uncontrolled Personally-Owned Devices	• Encrypt corporate data at rest, in memory, and in transit regardless of whether the user disables the device passcode or selects weak device security • Separation of personal/corporate apps and data using secure containers • Encrypt data at the application level using secure containers • Selective remote wipe of corporate data only	• Mobile Device Management • Containerization via Secure App Wrapping and App Dev
Vulnerable Device Hardware and Software	• For corporate liable devices, enable strong device passwords • For corporate liable and BYOD devices, require strong passwords at the app level with shared app-based authentication • Encrypt corporate data at rest, in memory, and in transit at the application level using secure containers • Prevent access to corporate data by personal apps seeking to share data with other apps on the device or services located off the device • Selective remote wipe of corporate data only	• Mobile Device Management • Containerization via Secure App Wrapping and App Dev
Malicious and Poorly-Designed Apps/App Stores	• Encrypt corporate data at rest, in memory, and in transit • For BYOD devices, encrypt data at the application level • Selective remote wipe of corporate data only • Control unsecured communications and instant messaging just as email is managed • Select secure workflow-enabling apps from trusted and proven providers	• Mobile Device Management • Containerization via Secure App Wrapping and App Dev • Enterprise App Store
Exposed Public Clouds and Open Network Access	• Securely read, write, update and store files behind the corporate firewall; enable “check-in” and “check-out” access for programs or platforms (e.g., Sharepoint) that require this • Secure remote access without having to implement a VPN or series of Micro-VPNs • Leverage a secure, highly-available, redundant network operations center (NOC) • Enable secure file access/synchronization of corporate assets without placing systems in the demilitarized zone (DMZ)	• Secure File Access/Sync via Good for Enterprise and Good Share • Good Secure Proxy via the Good Network Operations Center (NOC)

How It Works: The Good Dynamics Secure Mobility Platform Architecture

The Good Dynamics Secure Mobility Platform is built on industry standards to provide organizations with maximum flexibility when mobilizing their enterprise and allowing employees to select their own devices. The platform also supports devices running the current iOS, Android, and Windows Phone operating systems.


OUTBOUND TO DEVICE:
Encrypts
Encrypted Data
Good NOC receives encrypted data
Encrypted Data
Encrypted Data
Decrypts
Decrypted Data
Encrypts
Encrypted Data
Decrypts
Corp environment (raw data)
Good Proxy (encrypts data)
Mobile client receives encrypted data from NOC
Good Dynamics secured app receives and saves encrypted data, then decrypts data only to memory when needed
'Open In' to another Good Dynamics secured app transfers still-encrypted data to that app
Good Dynamics secured app receives and saves encrypted data, then decrypts data only to memory when needed
INBOUND FROM DEVICE:
Encrypts
Encrypted Data
NOC sends encrypted data to the Good Proxy
Encrypted Data
Decrypts
Decrypted Data
Good Dynamics secured app authenticates and connects with Good Dynamics NOC
Good Proxy decrypts data and sends it to the application server
Application server

For controlling data sharing at the app level, policies can be set by IT to allow a Good Dynamics secured app to share data only with other specific Good Dynamics secured apps through whitelisting and blacklisting. Good Dynamics secured data can be shared among Good Dynamics secured apps whether the apps are built by Good, an ISV, or an internal development team using the Good Dynamics SDK and Good Dynamics app-wrapping technology.

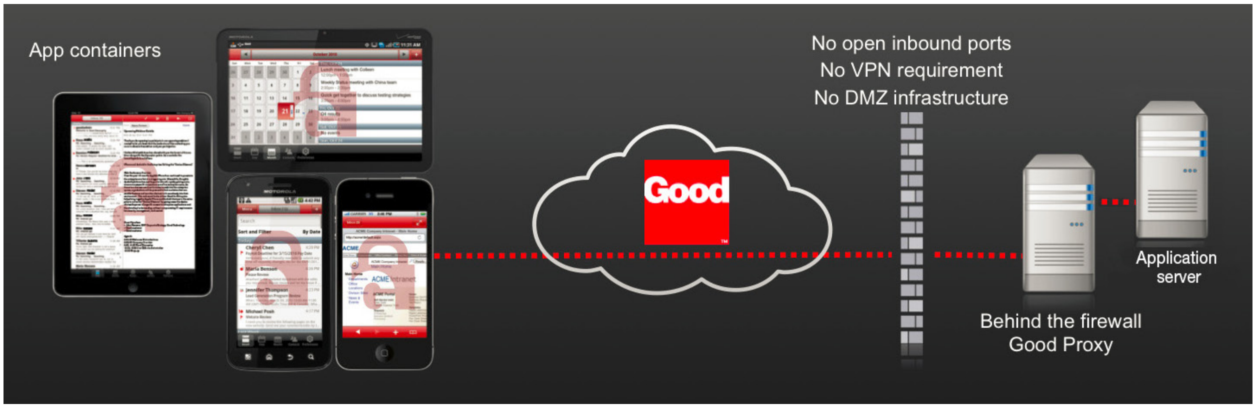
While note represented in this diagram, a Good Dynamics secured app can also “Open In” to a non-Good Dynamics secured app IF permitted by IT policy, including whitelist and blacklist app-specific granularity. If such an action is permitted, then the Good proxy server decrypts the data and sends the data to the non-secured app. At this point, the data could be at risk for loss since the app is now out of Good Dynamics control. This model falls outside of data loss prevention (DLP) best practices and is not recommended due to the obvious risk of potential data loss.

In real time, users can easily access their email, contacts, calendar, and other enterprise applications required to collaborate with their colleagues and other business partners. Users can also view, edit and share documents, including graphics, PDFs, Word and Excel files. Using either the file repository or integrated Microsoft SharePoint® access, users can access and share documents securely within the Good Dynamics application ecosystem and then send the documents via email and instant messaging.

Policy settings allow these features to be enabled or disabled. File-handling policies allow administrators to control which file types can be saved, which third-party applications are permitted to save the files, and which applications can be exported to either inclusive whitelists or exclusive blacklists.

The Good Dynamics Secure Mobility Platform also uses a Secure Socket Layer (SSL) encrypted tunnel, which allows Good-enabled applications to communicate and share data while protecting the content. The platform replaces the native “Open In” communication channel with an authenticated app-to-app SSL tunnel that secures the communication between Good Dynamics enabled apps so the content cannot be sniffed in transit by malicious software.

The Good Network Operations Center (NOC) serves as the core of the Good Dynamics Secure Mobility Platform architecture. Servers register and authenticate with the NOC using industry-standard security procedures. When a mobile device is activated, it authenticates to the NOC, and the NOC then manages the routing of the device data to the appropriate servers while ensuring only authorized devices are allowed to connect to enterprise servers.



Once authenticated, the mobile device and the servers establish an end-to-end secure communications channel. The NOC does not have access to the security keys for this communications channel, so unencrypted data is never exposed in the NOC. Those keys are kept by the mobile device and the Good Dynamics servers located behind the enterprise firewall.

Building Workflows With Secure Mobile Applications

In addition to employing the Good Dynamics Secure Mobility Platform, organizations also need to recognize that off-the shelf apps may not be available to complete every workflow their users require. Therefore, organizations should consider the development of enterprise-ready applications to utilize the platform properly:

- Business Intelligence
- Cloud Storage
- Document Editing/Annotation
- Enterprise Resource Planning
- Customer Relationship Management
- Finance
- Healthcare
- Instant Messaging/Presence
- Remote Desktop
- Document Management: SharePoint/File Access/ Sync
- Social Business
- e-Printing/Cloud Printing

Common Lines-of-Business Using Mobile Technology:

- Field service teams
- Healthcare professionals
- Manufacturing supply chain
- Legal war rooms
- Financial service advisors
- Emergency response first responders
- And more…

Mobile apps within these categories and others, including apps that have been commercially developed or custom-built by an organization, facilitate the process flows that enable mobile workforce collaboration while following corporate security policies.

The Role of Security in App-to-App Workflows

Good Dynamics enabled apps can securely access information—such as a PDF—and open this information in an image annotator such that users can draw on the image/document. They can then save notes and the drawing before sending the annotated image via a secure email application to other users.

In the world of collaboration, the multiple parties that work together multiply the number of applications running across multiple devices. Data thus becomes ubiquitous throughout the environment so that keeping track of and securing all data is critical. As business partners continue to shift to a BYOD approach—so devices, applications, and cloud services can enable mobility—meeting the IT need for security and control thus becomes increasingly complex.

The Good Dynamics Secure Mobility Platform helps meet this secure data-chain challenge by managing and securing applications and data on every device, between apps, and throughout the network. Simply put, Good Dynamics can instantaneously embed military-grade encryption and policy-control capabilities into any application without significant development work. This approach allows enterprises to securely manage confidential business applications and data—even on devices and within data stores beyond enterprise control.

In addition, Good Technology's unique inter-app communication capability enables app-to-app secure workflows and the sharing of document-centric services. This component of the Good Dynamics Secure Mobility Platform, called Good Dynamics AppKinetics, lets IT control which apps can talk to each other and for what purposes. Good Dynamics AppKinetics also allows IT to establish specific security policies, such as whether or not users can open a PDF received via email and print it wirelessly. By leveraging the built-in user authentication and authorization capabilities powered by the Good Dynamics Secure Mobility Platform, IT can also eliminate multiple logins and the potential exposure of data loss as the content moves between the apps.

With Good Dynamics enabled applications, businesses gain several capabilities so they can focus on managing their apps and data, without having to manage devices they don't own:

- **Share Information Safely:** Enables access to confidential business information from any device with out risking data loss.

- **Collaborate Securely:** Ensures constant information protection in collaborative workflows with app-to-app secure data exchange.

- **Enable Policy Controls:** Enforces application-level security controls for jailbreaks, root detection, passwords, OS requirements, application-specific custom policies, and data leak prevention.

- **Leverage Extensive Application Ecosystem:** Selects from a variety of off-the-shelf applications built for the Good Dynamics Secure Mobility Platform to enable secure healthcare mobility.

- **Containerize Any Application:** Embeds policy controls within in-house custom applications using Good Dynamics app wrapping technology.

Ensuring Data Security While Users Focus on Running the Business

Executives and users at all levels are leveraging tablets and other mobile devices to improve business efficiencies via improved workflows. End users can access the computing environment right at their fingertips, improving the level of services they can offer customers by saving time collaborating with associates through simplified workflows that would otherwise be complex if managed separately.

But along with these business benefits come many mobile collaboration risks. These include mismanaged device lifecycles and uncontrolled devices owned by employees as well as vulnerable device hardware and software. Enterprises also need to consider risks such as malicious and poorly-designed apps and app stores along with exposed public clouds that can create open network access

With Good Dynamics, the mobile collaboration data chain is sure to be secure—closing the gaps in protection regardless of which apps and how many apps are used. By relying on an enterprise mobility management platform such as Good Dynamics, organizations can secure the productivity-enhancing applications they develop without investing in and building their own security infrastructure—or worse, opening their existing infrastructure to risk by exposing mobility-enabling ports on the firewall or adding complexity by setting up mobility-enabling VPNs.

The Good Secure Mobility Solution offers the tools, VPN-eliminating infrastructures, and APIs that ensure software developers meet the highest standards of security in applications across all devices and operating systems. By utilizing proven technologies and methods such as FIPS 140-2 encryption, centralized app-level controls, and Web-based monitoring tools, organizations can leverage Good Dynamics to dramatically speed the delivery of application development projects to include industry-leading levels of protection and compliance.

This approach offers a unique level of security: By providing protection beyond the device level, developers can rapidly incorporate technology that containerizes data within mobile applications by wrapping a layer of protection around a variety IT-approved field-deployed apps.

Doing so ensures data security while enabling users to focus more time on what matters most—their customers.

About The Good Secure Mobility Solution

The Good Secure Mobility Solution comprises the Good Dynamics Secure Mobility Platform, the Good Collaboration Suite, and a rich ecosystem of custom mobile apps. These technologies combine to provide the market's first comprehensive solution for secure enterprise-wide mobility while supporting user demands for robust and interoperable enterprise-grade mobile apps. The technologies also give IT the required data security, service visibility, and infrastructure control to meet both regulatory requirements and service level agreements.

The Good Secure Mobility Solution also provides the security and application services that enterprise developers need to build transformative mobile apps on the most extensive, integrated framework. This capability allows enterprises to protect and manage apps, data, and devices while also enabling business productivity, collaboration, and workflow transformation.

About Good Technology™

Good Technology™ is the innovation leader in secure mobility solutions enabling business to move freely. Good's comprehensive solution consists of a secure mobility platform, a suite of collaboration applications, and a broad third-party application and partner ecosystem that unlocks mobile potential. More than 5,000 organizations in 130 countries use Good Technology™ solutions, including FORTUNE 100™ leaders in commercial banking, insurance, healthcare, retail, government, and aerospace and defense. Learn more at www.good.com.

Citations

1. *2013 Mobile Security Predictions* by Chenxi Wang, Ph.D. Vice President & Principal Analyst-Forrester Research, March 2013. www.forrester.com/2013+Forrester+Mobile+Security+Predictions/fulltext/-/E-RES92061

2. *Enterprise Mobility Management 2012* by Andrew Borg-Aberdeen Group, April 2012. www.aberdeen.com/Aberdeen-Library/7616/RA-enterprise-mobility-management.aspx

3. *The Security, Privacy and Legal Implications of BYOD (Bring Your Own Device)* by David Navetta, InfoLawGroup.com, March 28, 2012. http://www.infolawgroup.com/2012/03/articles/byod/the-security-privacy-and-legal-implications-of-byod-bring-your-own-device/

4. *SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones* by Parmy Olson, Forbes Staff, July 21, 2013. http://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/

5. *How Android users can overcome LeNa malware, slow carrier updates* by Nick Lewis of Enterprise Threats, SearchSecurity. http://searchsecurity.techtarget.com/answer/How-Android-users-can-overcome-LeNa-malware-slow-carrier-updates

6. *Forrester: $2.1 Trillion Will Go Into IT Spend In 2013; Apps And The U.S. Lead The Charge,* by Ingrid Lunden, TechCrunch, July 15, 2013. http://techcrunch.com/2013/07/15/forrester-2-1-trillion-will-go-into-it-spend-in-2013-apps-and-the-u-s-lead-the-charge/

7. *TCO & Security of Enterprise Grade Mobility* by Andrew Brown-Strategy Analytics, November 2012. http://www.strategyanalytics.com/default.aspx?mod=reportabstractviewer&a0=7919

Global Headquarters
+1 408 212 7500 (main)
+1 866 7 BE GOOD (sales)

EMEA Headquarters
+44 (0) 20 7845 5300

Asia/Pacific Headquarters
+1 300 BE GOOD

good.com