AN END-TO-END FRAMEWORK FOR MOBILE SECURITY
A GOOD TECHNOLOGY TECHNICAL WHITE PAPER

TODAY’S MOBILE ENTERPRISE
It’s clear that mobility is driving the next wave of business growth, innovation and productivity. Benefits can be realized in many parts of business operations, from staff through executive levels.

With almost 80%¹ of organizations having achieved the first wave of productivity by providing mobile access to email, employees are now demanding access to enterprise resources and collaboration tools on their chosen mobile devices. They need access to their documents in SharePoint® or other file servers or clouds, intranets/portals, the corporate IM, and web applications from their devices. Lines of business want to transform themselves through the use of mobile technology, requiring that multiple apps share data to create processes that better serve their employees, partners, and customers. To meet expectations for convenient mobile apps and data, IT and application development departments face ever-increasing and evolving requirements for mobility enablement. They’re also confronted with a persistent challenge – securing the corporate data.

Changing Mobile Landscape
There are three broad categories that capture the changing landscape in enterprise mobility:

Consumerization of IT Infrastructure
Smartphones and tablets are “must-have” gadgets among consumers. By the end of 2014, the number of mobile-connected devices had exceeded the number of people on earth, and by the end of 2019 North America will have nearly 90% of its installed base converted to smart devices and connections, followed by Western Europe with 78% smart devices and connections.²

As this consumer adoption proliferates, so does the use of these devices in the enterprise. In fact, according to IDC, 1.29 billion mobile devices were in use at work worldwide by the end of 2014, and that number is expected to reach 1.87 billion by 2018³. By 2020, organizations expect over half of their employees to participate in a BYOD program with no resistance, according to a recent Gartner survey.⁴ With employees willing to bear the cost of these mobile devices and associated data plans, IT will continue to face demands for new mobility initiatives and added risks that must be managed.

¹Forrsights Workforce Employee Survey, Forrester Research, Q4 2013
²Visual Networking Index Study Update, Cisco, May 2015
⁴Bring Your Own Device: The Results and the Future, David Willis, May 2014
Device Diversity
The richness of device types, now including wearables such as smart watches and fitness bands, with capabilities to offer more entertainment, personalization, and applications for increased productivity is driving the adoption of a wide variety of devices. This is leading organizations to move away from supporting a standardized set of devices from one device maker to satisfy employee demands for broader diversity while still protecting sensitive data.

The Cybersecurity Risk has Expanded to Include Mobile
Cybercriminals are expending significant resources to exploit sensitive intellectual property and personal data, causing financial and reputational damage while nation states are pursuing cyber espionage that could threaten national security. In 2014, there were many large and pervasive incidents that affected retailers, financial institutions, governments and others.

PwC’s The Global State of Information Security Survey 2015 reported that global security incidents increased by 48% from 2013 to 2014. Furthermore, in the same report, respondents from companies with greater than $1 billion in revenue reported an average of 13,138 incidents in 2014, an increase of 44% year over year. Compounding cybersecurity challenges, criminals and nation states are increasingly targeting mobile devices and leveraging personal applications as a conduit for malware designed to steal corporate data. As both mobility and cybercrime continue to grow, the need for robust security solutions on mobile devices becomes increasingly critical to the enterprise.

The Security Challenge
For all the promise of these new technologies, security remains the Achilles’ heel of mobility deployments. Organizations must address security issues to reap the benefits of mobilizing the enterprise.

CIOs consistently rank security as one of their top IT priorities, and the unique nature of mobility outside the walls of the enterprise adds heightened awareness of the threat.

Security breaches put companies’ valuable assets and information at risk. An enterprise cannot compromise intellectual property, proprietary business processes, business intelligence, and customer data in order to mobilize. As a result, CIOs and CSOs demand stringent security standards to ensure that mobile users are allowed access to key enterprise data only as authorized; that such data is safeguarded both during transmission to and while resident on the devices; and that the core IT infrastructure is not jeopardized.
THE END OF THE PERIMETER

In the not so distant past, IT provided a company issued laptop for work, and perhaps provided VPN access for remote work. IT provided certain sets of security and information management tools on that laptop including full disk encryption, firewalls, virtual private networks, intrusion detection or protection software and of course anti-virus.

Now fast forward to the present. With near ubiquitous high speed wireless data access and powerful mobile devices, there is no real enterprise perimeter anymore and a PC centric model for security doesn’t work. The corporate network now extends beyond the physical boundaries of the enterprise wherever mobile devices and their users go. In today’s world, protecting corporate data requires a multi-layered approach to security.
Good recognizes that managing enterprise security is a complex undertaking and requires a comprehensive approach—especially when it requires providing mobile workers with anytime, anywhere access to the information they need. As the pioneer and leader in Secure Mobility, Good today is installed in more than 50% of the F100, including 100% of F100 Commercial Banks and F100 Aerospace and Defense firms as well as some of the most demanding customers in government, healthcare, legal, high tech, retail, manufacturing, and other sectors.

THE GOOD MOBILE SECURITY ARCHITECTURE

Understanding that a PC-centric approach to mobile security is heavyweight and not user friendly, Good has developed a modern, extensible layered security model that addresses the unique needs of a mobile, always connected enterprise. This model has eight key elements:

Authentication
The first step in security is ascertaining the user is who they say they are. For initial activation, Good establishes the correct EMM Server and the user’s identity for the application/container via an account/access-key and the subsequent exchange of encryption keys, authentication tokens, and certificates. This identity is preserved or protected thereafter via frequent key/token rotation between each activated container and its Good EMM Server.

This unique capability of the Good architecture to activate a user’s app without the user having to enter the EMM server address ensures there is no possibility of phishing due to a mistyped address. Further, Active Directory (AD) credentials are not used in activation or onboarding thus averting the potential for DOS attacks due to AD exposure at the enterprise edge.

For subsequent user log in, Good provides administrators with tools to define strong authentication policies that are enforced consistently across all device platforms. Strong authentication policies can include disabling sequential numbers in passwords, requiring use of special characters, and more. Additionally, policies can be defined to wipe the Good application(s) and all its data (or optionally wipe the entire device) for failure to provide the correct password after a set number of attempts.

As well as supporting strong password-based authentication, Good is unique in providing an extensible authentication framework that supports a variety of multi-factor authentication mechanisms provided by third parties. These include smart-card based authentication (compatible with US Government CAC and PIV standards), biometric authentication using factors such as eye blood vessel recognition and Bluetooth-connected crypto tokens, as well as seamlessly supporting future authentication methods that have yet to come.
Identity and Access Management

Once the user is ascertained to be who they are, they should be spared the inconvenience of verifying it again and again. I.e. first to an application, and then secondly to an enterprise service that the application uses. This requires translating the users identity on mobile and verifying it with existing back end systems such as AD, web applications, CRM systems, etc. The alternative route - IT changing existing identity and access management solutions to adapt to mobile - is too costly and disruptive.

Good solves this dilemma by allowing organizations to use their existing identity and access management solution for mobile applications. Through the above user activation process, Good establishes a permanent and canonical identity of the user associated with each and every activated container/application. This ability of Good to authoritatively attest to the user’s identity of an inbound container connection makes it an Identity Service Provider (IDP) within the enterprise and therefore an accepted Kerberos Constrained Delegate (KCD) candidate. The Good unique support for KCD (including multi-realm KCD) allows the Good Control server to obtain and issue Kerberos service tickets on behalf of the container/user. As a result, users are not required to enter their AD credentials to gain access to business systems (email, intranet, etc.) enabling a truly delightful yet completely secure no-sign-on solution. The Good identity architecture is designed to be extended in the future to support other types of Single Sign-On system including SAML, OAuth or similar as customers require.

Managing the Device Platform

IT managers must meet the growing demand for mobile devices while ensuring mobile devices comply with their organization-specific IT policies and that proper configurations are pushed to devices. However, unlike traditional PC management, mobile environments are highly heterogeneous. Good Mobile Device Management provides the control and visibility IT needs with the flexibility to support multiple mobile devices, ownership models and use cases.

For most device platforms, mobile device management (MDM) allows the owner of a mobile device (or some authority to whom the owner has ceded control) to push specific configuration settings, known as profiles, to the device. The settings available vary from device to device and OS to OS. IT can streamline help desk costs by allowing users to quickly self-enroll for MDM over-the-air. In addition to automatically configuring corporate policies and controls, IT can automatically setup WiFi, VPN and Exchange ActiveSync configurations on user devices. Streamlining the enrollment process increases user satisfaction while driving down mobile support costs.

Good provides a rich set of policy controls over password, device encryption, camera, Wi-Fi, VPN, app whitelisting and blacklisting, detecting jailbroken iPhone or rooted Android devices, and preventing certain applications from being installed. In addition, should a device be lost, stolen, retired or replaced, Good MDM can wipe the whole device or just the application data within Good-secured apps. IT can also enable a policy that disables the Good application or wipes its data in the event that the device is offline for a defined period of time. This helps prevent an attacker from turning off the device radio in order to block the command from the server to wipe the device.

Data Protection

Managing the device and securing the data are different activities and it’s important to understand those differences. Good limits business risk associated with having corporate data on mobile devices by using the patented Good secure app container to encrypt and provide policy control over the organization’s data on a mobile device. Only Good has received the highest level of security certification for cross-platform mobile collaboration, Common Criteria EAL 4+ for iOS and Android.

To protect the app data at rest and in use, the Good secure container uses FIPS-validated cryptographic libraries that are independent
of the device. This means that even if the device pin code is compromised, corporate data within a Good secure container remains encrypted. The Good secure container uniquely protects content as well as user credentials and application configuration data that may be used by the app/container. Content can be protected against falling outside of enterprise control via Open In to personal clouds, cut and paste and other leakage methods. Content stored in a Good-secure application/container is always obfuscated in the file system and encrypted even if a user does not explicitly save the file to the container. It protects credentials such as usernames and passwords, tokens and certificates for both the container and backend systems. Finally it protects configuration information for applications that could be used to access backend systems. Because the Good secure container is not reliant on a MDM profile, app-level security can be applied to non-employee devices such as those used by business partners, contractors or even customers.

All application data protected by the container is secured using AES encryption before it's written to the file system and as it moves from app to app, either during cut and paste or when files are in motion between applications. This assures the confidentiality of data at all times. Container AES encryption keys are derived using the industry standard Password-Based Derivation Function (PBKDF2) protocol and are generated from the passwords provided by the user unless the administrator has configured multi-factor authentication, in which case the keys are stored using the second factor. Further encryption and authentication keys are stored securely on the device protected by these container keys.

If a user’s mobile device is lost or stolen, the IT administrator can remotely disable the device and remove all Good application data. If a device is recovered, the Good applications can be restored over the air (OTA). IT can also initiate a remote wipe of the Good data stored on the device if it is lost or stolen. In the event that the lost or stolen device is out of contact with the Good server for a predetermined period, the Good application can either be disabled or the data can be wiped.

In summary the Good Secure Container protects all key enterprise data. And, because of the app-level controls enabled by app containerization, IT can now require more complex passwords only at the corporate application level – where it matters most – rather than at the device level. Users will not be inconvenienced when they want to use their smart device for personal reasons – e.g., a phone call, a Facebook update or personal email.

Securing Network Access
Once the applications are authenticated to the back end systems, an application must access the services it needs. Ideally, this is done in a way to limit network exposure and provide access only to required services. The Good solution does this by forming an end-to-end encrypted channel between that application on the device and only those specific services that it needs behind the firewall or in a cloud service. The Good Secure Cloud provides a single, tightly controlled access point between the apps on the device and enterprise back-end or cloud systems with secure over-the-air encryption and data protection. Other solutions have multiple access points, multiple ports in the firewall and even multiple gateways, each of which add risk to network security.
Good establishes an outbound connection through the enterprise firewall, which means there is no need to open inbound ports and expose the enterprise networks to a variety of potential attacks. Additionally, all network traffic between the device and the server is protected using AES encryption. Since Good does not have access to the encryption keys that encrypt network traffic, the Good Secure Cloud only services encrypted packets and does not see unencrypted data. The Good Secure Cloud provides the additional functionality of authenticating devices to the network, granting access only to devices that have been provisioned to access their respective services – thus preventing rogue devices from getting onto the corporate network and protecting the enterprise from resource-hogging Distributed Denial of Service (DDoS) attacks. IT administrators also have the flexibility of using Direct Connect after device authentication, to allow direct connection between the device and enterprise back end systems for regulatory compliance or low latency reasons.

The Good solution allows administrators to control the types of devices and versions of operating systems that may connect to the enterprise network, and install and run Good-secured applications. For management simplicity or security reasons, IT managers can standardize on devices running a certain operating system and prohibit all other devices if they wish. When this is the case, IT managers can prohibit use of Good-secured applications on devices with a particular operating system or a specific version of an OS. This enables the IT administrator to ensure that devices are running with software that includes specific security features that are deemed required for the enterprise. For these reasons, integration with traditional network access control (NAC) solutions is less imperative. Good prevents the common security concerns from occurring – devices attaching without the proper OS or app level, or devices and apps accessing unauthorized data via the corporate network. However, some organizations may wish to implement contextual or proximity based authentication for certain corporate resources and data. In these cases, Good partners with leading providers such as Cisco and AirPatrol to explicitly allow or deny the features, apps and content available through Good-secured apps by policy.

Additionally, Good provides the optional capability to control access to various networks from the device, including Bluetooth and Wi-Fi access. On some devices, Good can offer granular Bluetooth profile management, disabling file transfers and LAN access through the Bluetooth network from taking place while allowing devices such as headsets to pair with the device.

The Role of VPNs
The Good approach of enabling per-app secure connections without requiring VPN to be used or inbound ports to be opened allows applications and devices to operate on both public cellular networks and public WiFi networks as securely as on private corporate WiFi networks. Good supports this mode of operation seamlessly without having to expose or scale up existing costly VPN infrastructure, without the use of corporate credentials and without the use of complex certificate management systems. Because of its unique approach, organizations do not have to apply policies that block access from cellular or public WiFi networks for security reasons. This approach also has the benefit of being transparent to the user, removing the inconvenience of starting a VPN on a mobile device. Good-secured applications operate as if they are connecting directly from the private network, irrespective of the connectivity employed and they do so without risk of data, network, or application infrastructure exposure. Because the containerized per-app approach does not rely on local APIs, keys or certificates, it also defends against local and network-borne man in the middle (MITM) attacks. Split or closed tunnel mode is configurable on an individual app basis, as is proxy forwarding to third party secure web gateways. Third party VPN client and VPN gateways can be used as an additional layer of protection when deployment is configured for Direct Connect, although this extra layer of security may be superfluous. However Good does not recommend device level VPN for security and privacy reasons because it potentially allows on-device malware to access the organizations’ corporate intranet and has been subject to numerous operating system level vulnerabilities. IT should carefully evaluate the associated risks before implementing device level VPN.

AntiMalware, AntiVirus and App Reputation Services
In 2014, there were 5 malware events every second. And on mobile, 96% of all mobile malware is directed at Android systems, creating a potential for exploits of personal and corporate information.

\(^5\)2015 Data Breach Investigation Report, Verizon, April 2015
Half of organizations discovered malware events during 35 or fewer days in 2014. Financial Services, Insurance, Retail, Utilities, and Education.

However, iOS and Android are sandboxed OS’s meaning that apps cannot share data amongst each other, so traditional reactive anti-malware built for the PC environment are not very effective. Although there are a few anti-virus and anti-malware solutions for Android, they cannot remedy a situation, but rather just alert to it. However, the Good solution provides preventative defense in depth ahead of deployment. That coupled with integration of app reputation services provides a strong solution.

First, Good ensures mobile apps do not accidentally or intentionally engage in risky behavior. In partnership with Veracode, both Good-developed and ISV apps built on the Good Dynamics platform are put through Veracode’s world class testing. Leveraging Veracode’s static and behavioral analysis, all apps that are published with the Good lock are tested to verify that no security vulnerabilities exist that may endanger the data being managed by the application or exhibit risky or unintended behaviors such as indiscriminate sharing of data with third parties or cloud services.

Second, Good recommends organizations only utilize trusted app stores from Apple, Google and Microsoft. For BYOD and COPE devices, this helps mitigate against personally downloaded apps that contain malware. If the enterprise is developing their own applications, Good recommends distribution through an enterprise app store.

Third, as described above, the Good secure container protects corporate data, and IT has the ability to implement policies to prevent data sharing to other 3rd party apps or cloud services. For iOS and Android platforms, Good also provides the ability to restrict access to the enterprise data or remote wipe enterprise data if the compliance rules put in place by IT have been broken. This includes the ability to detect whether the device has been jailbroken or rooted, the last time the device connected to the enterprise, the OS version, device type and the Good-secured app version allowed to access the enterprise data. Furthermore, integration of third party app reputation analytics can also trigger various actions including device wipe, device lock, app wipe, etc. In addition to actions triggered by third party app reputation analytics, Good enables the following compliance rules to be enforced:
1. **Jailbreak or Rooted Detection:** A jailbreak or rooting of a device is essentially a modification of the underlying OS to behave in a way that it was not originally designed to do. It opens up opportunities for numerous security vulnerabilities. Enterprises can further secure their infrastructure and content by preventing Good-secured apps from running on jailbroken or rooted devices. Although jailbreaking and rooting in and of itself does not expose any data in the Good container, they do enable an environment where malware, spyware and viruses can be installed on a device that could ultimately compromise enterprise data. Jailbreak and root detection is not an exact science. Hackers continue to find new ways to bypass detection mechanisms. Good continuously updates detection processes to provide optimal protection.

2. **Device Type:** Some organizations may wish to standardize on specific device types. For example, a healthcare organization may wish to allow iPads for access to collaboration and intranet applications, but prevent iPhones or iPod Touch devices from doing the same. With Good, the IT administrator can enforce a compliance rule that allows only specific device types to access enterprise data.

3. **OS Version:** The iOS and Android operating systems continue to evolve. With Good, the IT administrator can enforce a compliance rule that allows only devices with a specific OS to access enterprise data. This enforcement can also be used to ensure that OS versions that contain security vulnerability patches are being employed by users. This is key as the recent Verizon Data Breach Investigation Report noted that 99.9% of exploited vulnerabilities had been compromised more than a year after the associated common vulnerability and exposure (CVE) had been published.

4. **Client Version Number:** Frequent upgrades to apps on iOS and Android devices are a reality. These upgrades are either due to enhanced functionality or resolving problems in previous versions. IT administrators may desire that all their users use a specific version number of a Good-secured app, either for support reasons or because a specific version offers a security feature or usability feature that they wish to manage. With Good, IT administrators can force users to upgrade to a specific app version number by setting a policy that refuses to allow older clients to connect.

**Enforcing IT Access Controls**

Not all administrative tasks are equal and ensuring that the most sensitive operations are restricted is smart. IT managers can distribute management tasks across a hierarchy of administrators by using role-based administration that offers a set of roles, with varying permissions, for administering the Good solution 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 device when lost or stolen, can be limited to a smaller group. Administrators can create groups to organize and manage Good users. All policies and software distribution can be managed 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. IT administrators can also enable the self-service option, allowing users to manage a few policies on their own devices.

**GOOD RISK AND COMPLIANCE FRAMEWORK**

Security is not a one-time event. With the ongoing rapidly changing mobile landscape, maintaining vigilance is key to mitigating security vulnerabilities. For this reason, Good employs a combination of people, processes, and tools that form a Risk and Compliance framework.

This reduces the risk of data leakage from any Good-secured app as a result of a compromise of the underlying mobile device operating system. Two independent teams proactively discover new threats and possible attack vectors while the other is tasked with ensuring that these new findings are properly prioritized and integrated into Good software. These teams employ a continuous security enhancement process and use a combination of internal and external research and analysis to keep on the cutting edge. For more details, read the Good Risk and Compliance Framework.
SUMMARY

Mobile devices are the new computing fabric in the enterprise. They bring great opportunity for new innovation and productivity in business processes, however, they also bring new challenges for securing corporate data. Mobile security cannot be addressed through point solutions nor through PC-centric solutions as they do not provide the usability and extensibility needed in a heterogeneous world of device platforms and OS's. The Good Mobile Security framework delivers a holistic end to end approach designed specifically for the new risks in a mobile era protecting corporate data, preserving end user usability and privacy, and allowing for extensibility to new authentication methods, new devices and OS’s as well as to business to partner and business to consumer models.

ABOUT GOOD

Good Technology is the leader in secure mobility, delivering solutions across all stages of the mobility lifecycle for enterprises and governments worldwide. Good offers a comprehensive, end-to-end solutions portfolio, consisting of a suite of collaboration applications, a secure mobility platform, mobile device management, unified monitoring, management and analytics, and a third-party application and partner ecosystem. More than 6,200 organizations in 189 countries use Good Technology, and we are trusted and deployed in 100% of the FORTUNE® 100 commercial banks and aerospace and defense firms as well as leaders across healthcare, manufacturing and retail. Learn more at www.good.com.