

Presenting the first mobile application platform that lets developers build secure, containerized iOS apps for leading consumer mobile devices.

**Good Dynamics** allows app developers to extend Good Technology's industry-leading security to their own mobile applications, giving you direct access to the licensed iOS software, tools, and support you need to incorporate Good's proven technology into your own app builds—speeding through security, management, and compliance issues. Good Dynamics provides the following native functionality for your iOS application:

- Secure connectivity through strong AES encryption
- Secure storage
- Application management and policies
- Push communication

#### ➔ **SECURE EVERY CONNECTION**

Good Dynamics provides support for strong end-to-end encrypted connectivity between your mobile application and application servers. Unlike other solutions, Good Dynamics does not require an enterprise application to open holes in your firewall or use a VPN for communications, which can create common security vulnerabilities.

#### ➔ **SAFEGUARD THE STORAGE OF APP DATA**

By providing encrypted on-device storage systems (file system, SQLite, and more), Good Dynamics ensures the complete privacy of data. This also allows app users to work securely, even in offline situations where there's no access to wireless.

#### ➔ **MANAGEABLE APPS AFTER DEPLOYMENT**

Using Good Dynamics' existing web-based mobile device management tools, enterprises can individually manage the security parameters of each enterprise application. They can monitor the state of the device, enforce policies, change the password

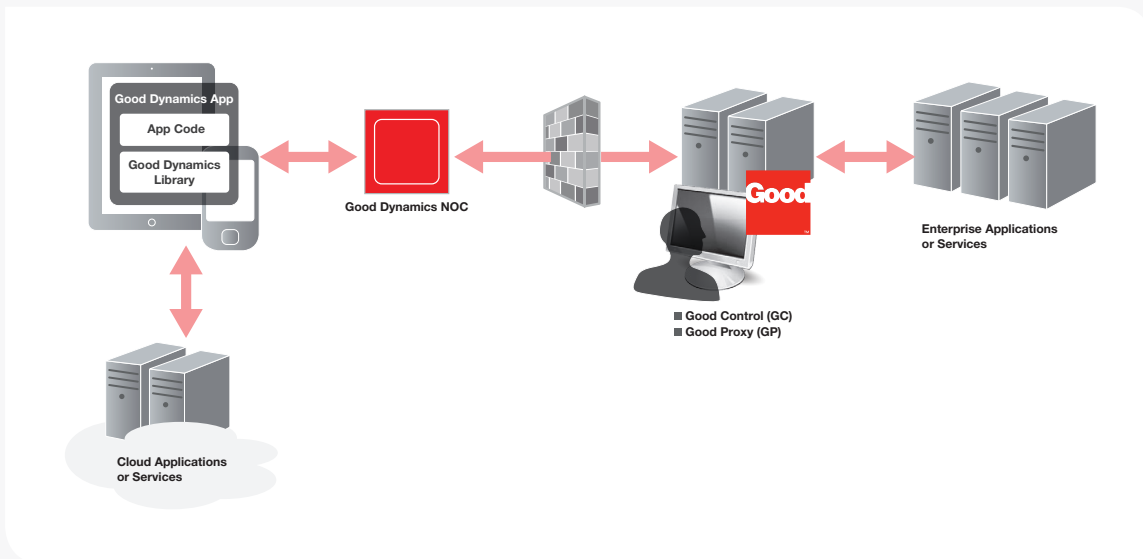
policy, and remotely lock or wipe the application. And they can do all of this at the application level without compromising security or breaching users' personal information.

#### ➔ **SAFELY PUSH DATA, POLICIES TO APPS**

The term "push communication" describes a system that offers an always-on capability—one in which any developer-specified event (e.g. database entry, appointment, document posting, application policy) is actively transferred by the Good Network Operations Center (NOC) to the mobile application. With this feature, enterprise servers and mobile apps can securely communicate with devices anytime.



## GOOD DYNAMICS ARCHITECTURE



## GOOD DYNAMICS SERVICES

SERVICE	DESCRIPTION
Push	<ul style="list-style-type: none"> <li>Push communication between enterprise servers and mobile devices</li> </ul>
Secure Communication	<ul style="list-style-type: none"> <li>Two types of secure communication: socket calls (TCP/IP) and web services calls (HTTP/HTTPS)</li> <li>Standards-based encryption (ex. AES 192)</li> </ul>
Secure Storage	<ul style="list-style-type: none"> <li>Two types of secure storage: encrypted file system (encryption of file content and names) and encrypted SQLite DB standards-based encryption (ex. AES 192)</li> </ul>
Management and Policies	<ul style="list-style-type: none"> <li>Set policies for each application (ex. password length, copy/cut/paste permission, etc.)</li> <li>Manage every application (e.g., jail-breaking detection, application version enforcement, etc.)</li> </ul>
Creation of Groups, Policies	<ul style="list-style-type: none"> <li>Initiate and secure user groups, application groups</li> <li>Apply policies at these levels</li> </ul>

To join the Good Dynamics Partner Program, visit [www.good.com/our\\_partners/index.php](http://www.good.com/our_partners/index.php).



**Good Technology**  
For more information visit [www.good.com](http://www.good.com).

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

**EMEA Headquarters**  
+44 (0) 20 7845 5300

**Asia/Pacific Headquarters**  
+61 (02) 92381953