## Limitations of the Walled Garden

This is the second part in a series designed to help organizations develop their "BYOD" (bring-your-own-device) strategies for personally-owned smartphones and tablets in the enterprise. Chapter 1 of the series, "Building Bring Your Own Device Strategies," introduced core components of a BYOD program. This chapter compares two technical approaches to BYOD: the walled garden vs. the enterprise workspace.

### *Summary*

The "enterprise workspace" approach to BYOD is secure, cost-effective, extends to apps, and drives user satisfaction. It allows IT to configure, monitor, and control enterprise data and access across the mobile device without compromising the native user experience. This is the approach MobileIron takes to BYOD. We will describe this approach in detail in Chapter 3 of this series.

The "walled garden", or container, approach to BYOD focuses heavily on security, but compromises the user experience which is the foundation of a BYOD program. End-users are not allowed to use the native email, PIM, or browser experience of the device and must, instead, download a separate app that tries to replicate those capabilities.

This is the approach Good Technology takes to BYOD and it can have several limitations:

- *Low user satisfaction because it forces use of an email app the end-user doesn't want*
- *Limited incremental risk management, especially after Apple's iOS 5 release*
- *Limited ability to support mobile apps*
- *High cost of ownership due to upgrade, scale, and maintenance overhead*

Walled gardens can be attractive in the early generations of a mobile operating system before the native email experience is fully secured and before the mobile device is being used for apps. However, the security capabilities of mobile operating systems like iOS 5 have evolved rapidly. As a result, a BYOD program built around a walled garden email experience is neither required nor sustainable for most enterprises.

### *User Satisfaction*

The underlying principle of BYOD is that professionals are more productive on technologies of their own choosing. Allowing employees to bring their personal devices to work, but forcing them to use a different email app or browser than the one they want, puts the entire program at risk.

But user experience is subjective, so we recommend testing with a pilot group of users:

- Give half the group the native email experience with ActiveSync and MobileIron.
- Give the other half the walled garden experience.
- Let them run for one week then have them switch to the other approach.
- Survey them on:

- Overall satisfaction
- Quality of email and PIM interface
- Speed of email delivery, especially download
- Integration with other on-device services, like voice commands

Walled gardens like Good compete head-on with Apple, Google, Android device manufacturers, and Microsoft, who are all building integrated native email experiences for their devices. These companies, especially Apple, invest heavily in design. Third-party email providers have difficulty competing with Apple on user experience, and the native email experience inevitably becomes the end-user's preferred option.

**User experience is the litmus test for the sustainability of a BYOD program.** If control trumps user experience, adoption will suffer.

### *Risk Management*

Corporate security programs leverage technology and education to drive appropriate behavior and reduce the risk of corporate data loss. BYOD programs introduce new variables for IT and, therefore, new types of risk.

Traditionally, the primary selling point of the walled garden has been to minimize this risk by putting all enterprise data into a single container on the device. But does that actually reduce risk? There are several security requirements to consider:

- Encryption
  - Walled gardens encrypt email.
  - But in 2009, Apple encrypted all new iOS devices and, in 2010, added even an extra layer of data protection for iOS native email content. Apple has also submitted their encryption for FIPS 140-2 certification.
  - Note that some walled gardens do not use the hardware-based cryptography of iOS, so the only factor used for encryption is the PIN code of the app itself. Such approaches cannot get the same strength of encryption as iOS native email, which can use both hardware cryptography and the device PIN. The only option for increasing strength in this case is to force the user to an unsustainable, extremely long PIN (20+ characters).
  - Android also now offers encryption, starting with version 3.0 of the operating system for tablets and with version 4.0 for smartphones.
  - MobileIron monitors all these encryption states and enforces action if the device is non-compliant.
- Identity
  - Walled gardens can set passwords for the email client.
  - But because the device has capabilities beyond email as well, a password also needs to be set at the device level. Having two passwords is a poor user experience.

- MobileIron enforces password policy at the device level, plus secures identity for native email, Wi-Fi, and VPN services through the use of digital certificates.
- MobileIron's lifecycle management of certificates from enrollment through renewal is a foundational capability necessary for both app security and user experience.

- Selective wipe of corporate data
  - Walled gardens wipe corporate email in their own app but have no control over the native email on the device
  - But MobileIron can wipe corporate email in the **native** email app without touching the personal email in the same app. So users get the native email experience they want, and IT still gets the data separation it needs.
  - MobileIron also manages the enterprise apps and connectivity (Wi-Fi, VPN) of the device. As a result, the entire enterprise workspace on that device can be wiped at once, even though it is not located in one specific container.
  - This is the core value of the enterprise workspace: It preserves the native experience and can be secured and managed through MobileIron without forcing end-users to use apps they don't want.
- Privacy
  - The walled garden approach to privacy is: *"If it's not in the container, I don't have to worry about it."* The assumption is that there will be no other apps on the device used for business purposes.
  - However the reality is more complex and there will actually be multiple apps used for business purposes on the same device.
  - As a result, IT needs to be able to monitor the device broadly but, at the same time, focus that monitoring on only those aspects of the device that truly impact security.
  - MobileIron's granular privacy policy gives IT the ability to monitor selectively. For example, IT may decide to track the location of corporate devices, but never do so for personal devices. IT can set MobileIron privacy policy to match company compliance requirements.
- Mail forwarding
  - Walled gardens prevent the forwarding of corporate email from a personal email account.
  - But MobileIron also prevents the forwarding of corporate email from a personal email account. The advantage is that MobileIron does this using the **native** email experience.
  - MobileIron also prevents moving email across inboxes and triggering an email from a third-party app.
  - These data loss prevention functions are available starting in iOS 5.

- Saved attachments:
    - Walled gardens prevent users from storing email attachments on the device.
    - This restriction is not yet available within native email clients, though given Apple's investments in enterprise security over the last two versions of iOS, it could well be added to future releases.
    - MobileIron's compensating control is to monitor apps that might access attachments and take automated action to block email flow if the risk is deemed too high.
    - Note also that all email to the device flows first through MobileIron (specifically, the MobileIron Sentry inline proxy) for enforcement of access control. As a result, future versions of Sentry could include policy-based content filtering as well as integration with existing Data Loss Prevention (DLP) systems for risk assessment.
- Malicious action:
    - There are a handful of other possible ways to misappropriate email content, like copy/paste. However these are generally acts of the malicious, not well-intentioned, user and in most organizations this information can also be accessed from the desktop or web. Mobile isn't the only potential source of such data leaks, though this is an area that will resolve over time.
- User cooperation
    - When you put a person in a straitjacket, they try to get out. An unfortunate side effect of the walled garden is that well-intentioned users try to go around the system to get the experience they want. They actively undermine the BYOD security program, not because of any malicious intent, but because they just want to get their work done efficiently.

In every release of iOS, Apple has consistently improved the security of the native email experience on iPhones and iPads. We expect this to continue. We see this same movement in Android, as well. As native email security increases, the additional risk management value of the walled garden diminishes, while the cost to the organization remains constant: **low user satisfaction, limited apps expansion, and high operational overhead.**

### *Moving to Apps*

Email is the first mobile function, after voice, that most organizations deploy. But as Forrester says, "*Corporate app stores will become the intranet of the future*." (from Forrester Research's "Mobile Management Takes a 180-Degree Turn" August 2011). In other words, the true value of mobile as a computing platform will be realized as companies move beyond email to apps. Mobile apps, whether native or web, will become the employee's window into his or her company's business processes.

**Walled gardens limit an organization's ability to use mobile apps because these apps almost always fall outside the boundaries of that walled garden.** The stronger the business demand for apps, the faster an organization moves away from a walled garden toward an approach that can include enterprise app store and security capabilities for both internal and public apps.

### *Cost of Ownership*

Walled gardens, especially Good Technology, have a high total cost of ownership.

- Upgradeability
  - Core changes in the underlying operating system can break the Good security solution and require a re-registration of **every** deployed device.
  - When iOS 5 was released in Fall 2011, customers of Good Technology faced a serious helpdesk and user issue: Every mobile device using Good Technology's email app had to be re-registered. In other words, each end-user had to manually delete and reinstall Good Technology's email app.
  - The burden of this upgrade fell directly on the helpdesk and the end-user community.
  - This indicates a basic architectural issue with the product that increases the total cost of ownership with every major operating system upgrade.
  - The native iOS email experience, on the other hand, has no interruption in service and no incremental operating cost when the mobile operating system is upgraded.
- Scalability
  - Our customers tell us that each Good Technology server can only support 1000-2000 devices, and even fewer (600) if using the Good browser. Therefore, large deployments incur substantial infrastructure and ongoing operational costs, primarily excess staff.
  - MobileIron, on the other hand, supports 20,000+ devices per server.
  - Our customers have also told us that operational costs for ongoing management of Good are three times those for ongoing management of MobileIron plus ActiveSync.
- Single point of failure
  - Good Technology has the same external NOC-based architecture as RIM.
  - Therefore, email performance and availability is dependent on Good's infrastructure and is outside the control of IT.
  - Maintaining service levels will require additional monitoring of the Good infrastructure and investment in the tools to do so.
- Legacy technology
  - Good does not use ActiveSync, which is the de facto standard for mobilization of email.
  - Third-party email apps with proprietary protocols are expensive for the vendor to maintain and customers to buy, while native email apps are free.

- Device support
  - Because email is a complex app, each new device make and model needs to be certified by the third-party email vendor.
  - If you are considering a walled garden email app, check the devices supported and the historical time lag between device introduction and email app certification.
  - For example, there was a seven month lag between the U.S. launch of the original iPad in April 2010 and first availability of Good Technology's iPad-optimized email app that November.
  - In a BYOD world, device diversity grows over time. Users become frustrated when they cannot get corporate email because the walled garden email app does not yet support the make and model of their mobile devices.
  - This is not an issue for the native email experience, because it is always certified by the manufacturer before device launch.

### *Conclusion*

We concluded Chapter 1 of this series with the statement "BYOD seems simple, but it's often not." That is the case with the walled garden approach for BYOD, as well. At first, it seems like a good fit for the security needs of an organization. However, any incremental risk management the walled garden may offer for BYOD is countered by the low user satisfaction, limited apps expansion, and high operational overhead that results.