Managing Mobile Access to the Cloud

Published: 26 August 2013

Analyst(s): Song Chuang, Dionisio Zumerle

Use of mobile personal cloud services is proliferating on personal and enterprise-owned mobile devices. Organizations are considering controls that appear to conflict with the spirit of BYOD and wonder if their approach is correct. Use this framework to manage mobile access to the cloud.

Key Challenges

■ Enterprises are unsure how they should address data leakage concerns arising from the storage of enterprise data in personal cloud services, and they seek guidance on which of these services should be managed.

■ IT departments find it challenging to define and fund alternative solutions after they have blocked personal cloud services.

■ IT leaders with "bring your own device" (BYOD) environments would often prefer a more open approach but are unsure how to achieve both security and openness.

■ Enterprises also struggle with the need to secure enterprise data that is legitimately stored in SaaS services and to ensure that mobile access from personal devices and over public networks does not present a risk of data leakage, regulatory noncompliance and performance problems.

Recommendations

■ Isolate enterprise data on endpoints, and minimize data leakage to personal cloud services — for example, by using mobile device management (MDM) in conjunction with a containerization on mobile devices.

■ Block undesired personal cloud services and offer valid enterprise alternatives — for example, by providing enterprise file synchronization and sharing (EFSS) or standardizing on an enterprise-class cloud solution.

■ Secure enterprise data that is legitimately in the cloud with a cloud access security broker (CASB) that provides single sign-on (SSO) access and encrypts data stored in your SaaS-based ERP system. Ensure compliance with data residency regulations, and leverage content delivery networks for performance.
Implement network access control (NAC) solutions to block channels of data leakage that bypass your MDM’s mail server controls, such as unsanctioned computing devices.

Table of Contents

Introduction............................................................................................................................................2
Analysis..................................................................................................................................................3
    Contain Enterprise Data on Endpoints, and Minimize Data Leakage to Personal Cloud Services......3
    Block Undesired Personal Cloud Services and Offer Valid Enterprise Alternatives....................... 4
    Secure Enterprise Data That Is Legitimately in the Cloud................................................................. 6
    Close Gaps and Block Remaining Channels of Data Leakage.........................................................7
    The Need for Symmetry................................................................................................................. 7
Recommended Reading.........................................................................................................................7

Introduction

The growth of enterprise mobility has allowed users to access applications and data from multiple devices. Gartner refers to the collection of services accessible from multiple devices as the "personal cloud." The personal cloud introduces new risks of data leakage, and it must be addressed using new methods and technologies.

Enterprises have traditionally managed client computing devices by enforcing strict policies, which has been referred to as "lockdown." When consumer mobile devices first showed up, enterprises tried to manage them via these same strict policies that heavily restrict the devices’ capabilities.

However, this strategy won’t work with BYOD, because the devices do not belong to the enterprise. End users have rightfully begun to question what gives the enterprise the right to constrain their devices.

Complicating this is the fact that modern mobile OSs are by nature less manageable, both because of the immaturity of the platforms and for clear technological and commercial choices made by the vendors.

Enterprises also started asking themselves whether this kind of intrusive management can clash with privacy regulations. We believe a new approach for managing BYOD in the context of cloud services is emerging.

Rather than lock down personally owned devices, an alternative approach focuses on securing the enterprise apps and data. This approach consists of a three-prong approach:

- **Endpoint** — Enterprises should use a container (see Note 1) to isolate enterprise apps and data, and focus on protecting it rather than locking down the entire device.
- **Cloud** — Enterprises should consider providing new cloud services, such as EFSS, in-house so that enterprise content is created and stored in a trusted environment, on-premises or in the cloud, with a known acceptable assurance level. This should be complemented by cloud access gateways that ensure transparent encryption of enterprise data that is legitimately stored in the cloud by enterprise SaaS services.

- **Network** — Finally, to ensure that management efforts are complete, enterprises need to utilize NAC to ensure that unsanctioned and unmanaged devices are not allowed to connect to enterprise resources, because uncontrolled data leakage would follow.

This three-pronged approach allows users to access cloud services while minimizing the risk of data loss.

### Analysis

**Contain Enterprise Data on Endpoints, and Minimize Data Leakage to Personal Cloud Services**

Instead of potentially interfering with personal devices, apps and services, including personal cloud, enterprises should focus on isolating their data and protecting enterprise apps and data on personal and enterprise-owned devices. This isolation means that employees are free to use personal cloud apps in the personal space of their device and the enterprise can reduce the risk that enterprise apps will leak data into the personal space of the mobile device.

**This can be accomplished by using a container.** See "Technology Overview of Mobile Application Containers for Enterprise Data Management and Security."

Containers are not simply a new feature, but they really represent a new management paradigm. This is a critical development that will shape how enterprises manage mobile devices and the personal cloud. Any data leakage prevention on the mobile device needs to be complemented by equivalent controls on other endpoints (see the Close Gaps and Block Remaining Channels of Data Leakage section).

With containerization in use, it is much easier to protect enterprise data from leaking out of the enterprise container into personal cloud services. For example, users can be prevented from opening enterprise email attachments in Dropbox. Containers also typically include authentication, encryption, selective wipe and app-level VPN capabilities.

Gartner estimates that the attach rate of containerization with MDM solutions is at 30%, and projects it to grow rapidly. While heavyweight and invasive containment approaches like mobile hypervisors may be appropriate for a small percentage of organizations (for example, defense), many other organizations are likely to opt for lighter-weight container approaches.

One of the changes in containerization is that many of the newer products, such as AirWatch and MobileIron, allow users to use the native email while maintaining data leakage protection. There is
no need to use a separate third-party email client that implements a monolithic container (see Note 2). With these solutions, the user can continue to use the native email client, which is a substantial user experience win. Data leakage of email text is addressed by managing copy and paste. Data leakage for email attachments is addressed by encrypting attachments so that they can be opened only by an MDM component that can enforce a policy that determines which apps can be used to open the attachment (for example, blocking Dropbox). Some solutions completely strip attachments from email and force the users to retrieve the attachments from a MDM component on the network that enforces policies similarly. In these cases, there may be no monolithic container, but a virtual container around email has been logically implemented. This is similar to what is provided by Web browsers and hosted virtual desktop.

Leading solutions also support the containerization of third-party mobile applications via app-neutral or app-specific containers, also known as "app wrapping" and "software development kits (SDKs)," respectively. When a custom or commercial app is containerized this way, the app is now virtually in the same logical container.

If all mobile apps with enterprise data were containerized, it would be much more difficult for enterprise data to leak into personal cloud services that may be running on the same device. These data leakage controls must be complemented on all endpoints for control to be effective (also see Close Gaps and Block Remaining Channels of Data Leakage).

Enterprises that want even more security assurance — for example, from hardware-level isolation — can consider alternatives discussed in "An Update on Mobile Virtualization and Trusted Environments."

Gartner encourages clients to monitor changes in this area as vendors embrace new capabilities in iOS 7.

Block Undesired Personal Cloud Services and Offer Valid Enterprise Alternatives

There is a lot of discussion around whether the enterprise should allow personal cloud services (see Note 1), and if yes, which of the specific services. As was the case with device consumerization, personal clouds will eventually be accepted by enterprises. As in the case of BYOD, this will be driven by users, but will also be accommodated by app vendors adding enterprise features and versions of their tools. Examples are enterprise versions of file synchronization and sharing tools and productivity suites that offer corporate versions with accounts that can be controlled by enterprises. We expect this model to proliferate, which will reduce the need for users to obtain these services on their own.

Nevertheless, the current ecosystem of commercial apps and their terms of agreement does not fully accommodate enterprise needs yet. Undesired services may have policies that clash with the company policies, their cloud storage may reside in (and abide by regulations of) regions that are considered adverse to the enterprise’s interests, or they may simply have a hacking record that does not fit the enterprise’s risk appetite. Also, the ecosystem is far larger than the mobile operating system landscape, which consists of four major operating systems, making it harder to track and select acceptable apps. The enterprise needs to isolate corporate data through technical means, but also communicate this policy clearly to the workforce (via the mobile policy). Consumer
applications can be used for work only where no company information or intellectual property is used, which leaves a limited set of activities.

Application whitelisting/blacklisting solutions also fall into the "enterprise lockdown" philosophy and are difficult to implement with BYOD. However, the strict company policy currently must reign inside the enterprise container (or throughout the device if a container is not present). This approach will evolve, reducing the range of action of the mobile policy more and more toward the single application, but this will require a concerted effort of tech maturity, market maturity and mobile application development effort. There are several ways to block, including secure Web gateways (SWG — on-premises or cloud-based) and MDM agents. Some MDM agents partner with mobile application security testing services that can check applications for reputation and help approve or reject applications, to be put in the enterprise app store.

Blocking is only half of the exercise. The enterprise must also provide a valid alternative to the workforce. This is not done simply to "keep users happy," but also to avoid data leaks. Gartner has observed that users find a way to circumvent enterprise policies that are too strict. Enterprises cannot address consumerization by simply blocking services. Trying to stop consumerization is the wrong strategy. Pragmatism requires keeping up with consumerization by offering to the workforce attractive and user-friendly tools, to use instead of consumer applications for professional activities.

Let us consider some examples:

- **File sharing and synchronization** — The enterprise blocks the unauthorized services via an MDM tool. The enterprise must also offer a "legal alternative"; a list and rating of possible alternatives can be found in "MarketScope for Enterprise File Synchronization and Sharing."

- **Productivity tools** — The new tools that have become available through commercial app stores are very appealing to users, especially creative knowledge workers, because of the possibilities offered; most of these tools require registering a profile, storing work in the tool’s cloud, and agreeing to the terms of use proposed. A serious concern is that some of these tools claim intellectual property over anything produced via their use. It will be challenging for the enterprise to compete with this multitude of creative tools, but in the light of these issues, there is no alternative to banning them for work use. For organizations that have creative needs, purchasing professional creative tools is a (costlier) alternative. For regular productivity solutions, WatchDox Mobile Productivity & Collaboration and BoardVantage Backplane are two examples of tools that can be used.

- **Contacts** — A common issue encountered is how to simply load contacts from a PC or an older mobile device to a new smartphone. A typical situation is one where users need to migrate contacts from a BlackBerry device to an iPhone or Android device. Services that expose company contacts to third parties, such as iCloud or Gmail, should be avoided. In the case of iOS, the migration can be done with native tools, while for Android a third-party app will be necessary. The mobile policy should specify the modalities of the migration (unless the IT department takes care of this task) and provide any necessary third-party tools via the enterprise app catalog.
- **Backup** — Personal backups in the personal cloud (Google Drive, SkyDrive and iCloud) or on personal devices, should be prohibited by policy and blocked by technical means (for example, with a SWG). The difference between data stored on personal devices via BYOD and these personal backups is that there is no vetting process for the devices used and no control over their compromise (for example, via MDM agents) and the user has not agreed to any terms of use or signed any mobile policy. Currently, the possibilities to inhibit such backups are limited. Certain MDM tools can inhibit, for example, iCloud backups, but they cannot inhibit iTunes backups on personal devices — this can be done via command line via a Mac, but it can be reverted by the user via command line. Enterprises should forbid these types of backups explicitly in the policy, exercise the inhibiting controls that are available, but most of all, offer encrypted backup alternatives to users on corporate resources. It is essential that the backup tool is usable and efficient, offering fast retrieval to users.

**Secure Enterprise Data That Is Legitimately in the Cloud**

In contrast to the personal cloud services discussed above, an increasing number of SaaS enterprise applications are completely sanctioned by enterprise IT, a popular example being salesforce.com applications. The prolific use of personal mobile devices means that many of these services will be accessed from unmanaged devices over networks not controlled by IT. Enterprises are primarily concerned that there is an absence of auditing, demonstrable compliance, sensitive data monitoring, encryption, identity, policies, malware detection and/or control. In some cases, some of these capabilities may be in place but may be disparate as different solutions are in use. Increased visibility and control of enterprise data in these use cases is possible via CASBs that interject security controls between users and cloud-based services that they consume (see "The Growing Importance of Cloud Access Security Brokers").

Please note that CASBs are an emerging technology and current adoption rates are low, but we expect adoption to hit 25% by 2016 (see "Hype Cycle for Application Security, 2013," "Hype Cycle for Data and Collaboration Security, 2013" and "Cool Vendors in Security: Security Services, 2013"). Multiple types of providers offer solutions that will target the need for CASB services, including Symantec O3 and Intel Cloud SSO (see Note 3).

As a simple example, some of these products will allow users to have single-sign-on access to the entire set of enterprise SaaS applications while administrators have fine-grained control over what kind for access is acceptable; for example, iOS devices are not jailbroken, and connections occur only when the device is in the employee’s home country during working hours. These solutions can also transparently encrypt data that is stored in the SaaS application, so that it is secure from the SaaS provider. CASBs can also be used to provide comprehensive logging and auditing.

See "Five Cloud Data Residency Issues That Must Not Be Ignored" for more on the complex regulatory issues around data residency, encryption, national authority access and bilateral country agreements.

See "How to Accelerate Internet Websites and Applications" for more on content delivery networks, application delivery controllers and front-end optimization to ensure good-enough SaaS performance.
Close Gaps and Block Remaining Channels of Data Leakage

No matter how many controls are introduced, users always try to circumvent them. An example could be a user connected via wire to the enterprise network through his or her laptop, using a personal hot spot device to access unauthorized sites. When these unauthorized sites happen to be personal cloud applications, enterprise data can leak to these services.

Tools such as NAC can block personal hotspots and 3G dongles in the enterprise, while SWGs can inhibit the use of unauthorized personal clouds even when the user is not using the corporate connection. The ways to implement SWGs can vary; some enterprises choose to use SWGs only within certain times of the day, for example, so that users can use their personal devices as they wish outside of work time. While this enables productivity-driven URL filtering efficiently, it does not prevent data leakage. An alternative solution can be to use a container with enterprise data and filter the content that the user accesses through the browser that resides in the container.

Looking at mobility beyond cloud, NAC can be considered a useful complement of MDM and mobile application management, in that it provides granularity and visibility, ultimately enabling a more efficient and "elegant" enforcement of controls and policies. For instance, NAC coupled with MDM can limit the jailbreak detection checks to the moments when devices connect to the network with modified assets, instead of having periodic checks, which can be resource-intensive for the device's CPU and battery. A more thorough example of how NAC can contribute enterprise mobile security can be found in "Securing BYOD With Network Access Control, a Case Study."

The Need for Symmetry

This research focuses on access to sensitive data and personal clouds from mobile devices. However, it needs to be noted that breaches and uploads to personal clouds can occur from any type of device. The focus now is on the new mobile devices, in part because of the hype around them, in part because the industry is still trying to better understand how the devices work and how users use them, and in part because they are proliferating as personal devices.

The focus on mobile devices is an opportunity to run a concerted enterprise effort to set up proper protection measures. However, a correct mobile security strategy should take these findings and best practices and apply them to the rest of the endpoint fleet and infrastructure to achieve symmetry in protection.

Recommended Reading

Some documents may not be available as part of your current Gartner subscription.


"Managing the Mobile Personal Cloud at Work"

"Magic Quadrant for Mobile Device Management Software"
Evidence

1 Containerization is available from leading MDM vendors, including AirWatch, BlackBerry, Excitor, Good Technology, MobileIron, Soti, Symantec and Citrix. Stand-alone third-party vendors include Bitzer, MobileSpaces and Mocana. Samsung also uses containerization in its upcoming Knox product, and Apple has the Spaces capabilities in iOS 7.

2 An example is the creation of underground BYOD (or shadow IT) movements in enterprises that did not set up a BYOD program to accommodate user needs. Users managed to find ways to obtain access to corporate email (see "BYOD Doesn't Have to Be All or Nothing: Match Smartphone, Tablet and PC Rollouts to Organizational Readiness and Employee Demand").

3 "10 Steps to Transfer Contacts From BlackBerry to iPhone"

4 "How to Migrate and Import iPhone/Outlook Contacts Into Android Without Using GMail Using .vcf Files"

Note 1 Personal Cloud

Gartner defines the personal cloud as the individual’s collection of digital content, services and apps that are seamlessly accessible across any device. The personal cloud is not a tangible entity, but rather the realization of four different types of experience in which users store, synchronize, stream and share content on a contextual basis, moving from one platform, screen and location to another. Founded on interconnected services and applications, it both reflects and sets consumers' expectations for how next-generation computing services will work (see Gartner IT Glossary: Personal Cloud).

Note 2 New Style Containerization

One new approach to prevent data leakage of enterprise email is to have all email attachments encrypted by an in-line device, such as MobileIron Sentry. The attachments can then be decrypted
only by MobileIron, and policies can be enforced to ensure that the attachments cannot be "opened in" forbidden apps, such as Dropbox. The motivation for this approach is the desire by vendors to allow the use of the native email client — which is preferred by end users — while simultaneously providing the data leakage protection that enterprise IT desires. There is a risk that the text in the email body can be leaked, but some vendors have solved this problem as well by monitoring the copy-and-paste clipboard and effectively flushing it when the user attempts to copy and paste enterprise email text. This approach is likely to be further strengthened by new functionality in iOS 7.

Note 3 Examples of CASBs

Pure CASBs: SkyHigh Networks, Ionic Security, Symantec O3

Cloud desktop portal providers: Citrix Cloud Gateway, VMware Horizon

Providers of identity and access management as a service: Okta, Ping Identity, Symplified

On-premises identity bridge providers: Centrify, F5 Big-IP APM, Identropy Scuid, Radiant Logic RadiantOne

Cloud encryption gateways: CipherCloud, Concealium, PerspecSys, Vaultive

SWG vendors: Cisco IronPort SWG with cloud SSO