G00271435

How Digital Business Reshapes Mobile Security

Published: 11 February 2015

Analyst(s): Dionisio Zumerle, Nathan Hill

Enterprises need to drastically change their endpoint strategy to avoid the increasing disconnect between workforce enablement and security. We illustrate how enterprise approaches to protecting data evolve as mobility and consumer Internet of Things converge.

Impacts

- The increasing tendency to mix personal and business data on devices conflicts with and results in the bypass and breakdown of the legacy endpoint security models of enterprises.
- Management misinterpreting mobile risk and organizational structures that do not allow enterprise mobility projects to cater to security leads to growing security gaps for enterprises.
- Endpoint platforms become user-administered and application-centric, creating hurdles for enterprises attempting to enforce management and security policies on them.

Recommendations

- Focus your efforts on providing solutions that are tailored for mobile use and, therefore, obviate shadow IT practices, rather than forcing legacy toolsets to deliver functionality on mobile platforms that they were never designed for.
- Treat mobile security technology investments as tactical. The fast and uncertain evolution of mobility makes it necessary to stay flexible and avoid lock-in into long-term solutions.
- Abandon device-centric lockdown security models in favor of app-centric models. Trial data-centric solutions, but be aware of the limitations in terms of maturity and scalability.

Strategic Planning Assumptions

By 2020, 70% of enterprises will treat the entirety of their endpoints as untrusted platforms, regardless of whether they are enterprise or privately owned, up from 20% today.

By 2018, 50% of employees will be accessing enterprise data from devices for which there is currently no solution for enterprise management/visibility.

Analysis

Gartner defines digital business as the blurring of the physical and digital world to create new business opportunities. As one consequence of the advent of digital business, enterprise mobility is rapidly extending to cover an array of devices that have only recently started running mobile operating systems, such as connected cars, smart TVs, smart watches and other wearable devices.[1], [2] Since enterprise users adopted tablets and smartphones it became clear that protecting data with traditional endpoint management models, attempting to mimic laptop management, is incompatible with new OSs and use cases. In the light of these transformations, enterprises need to introduce new paradigms of endpoint management to avoid disconnect between enablement and security. How will enterprises protect data accessed from devices running mobile operating systems? This research illustrates enterprise approaches to protecting data on current and future mobile devices and how this is likely to evolve.

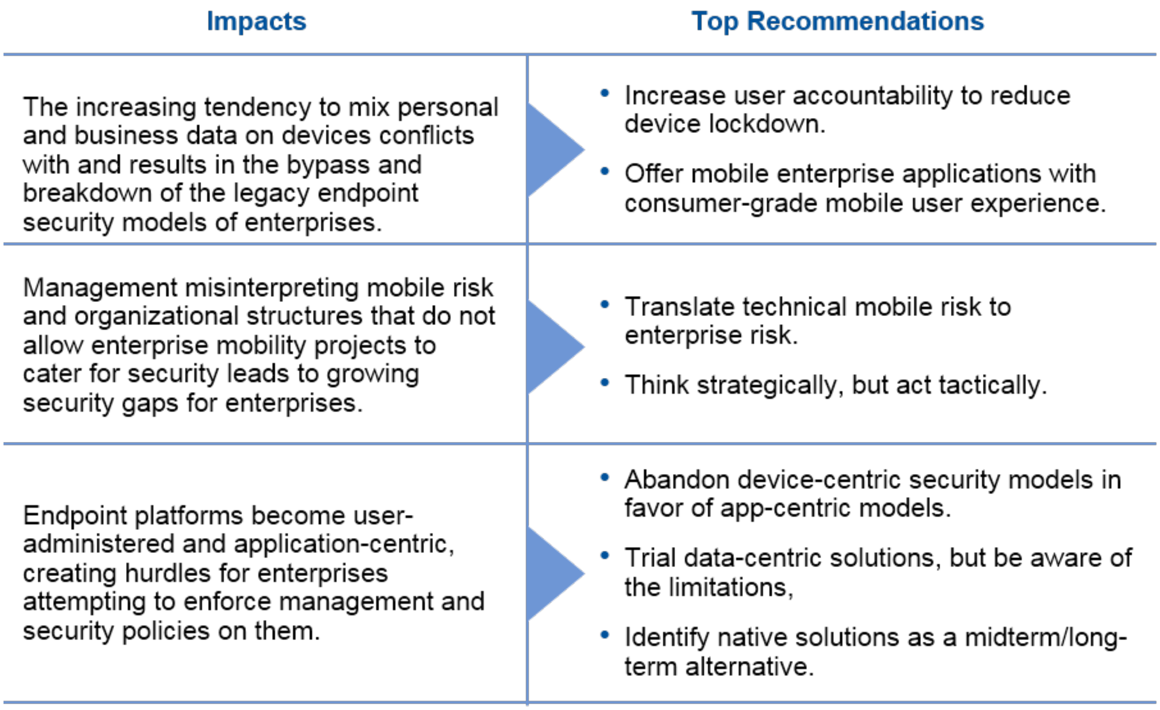
The Urge to Change a 30-Year-Old Endpoint Security Model

Two major phenomena are driving the need for change in security strategies for mobile endpoints. First is the aforementioned digital business. Consumerization, including the upcoming wave of consumer Internet of Things, makes it so that organizations' endpoint installed model shifts toward mobile, and the endpoint security model has to follow. As one example, in 2013 the Android installed base surpassed the Windows one.[3] Even traditional endpoints are turning into mobile platforms both in form factor and underlying platform (see for example "Windows 10 for PCs Will Let Organizations Choose How Often They Update"). Many of these platforms still need to mature in terms of the security they offer.[4], [5]

While the enterprise endpoint landscape changes passively with digital business, the second phenomenon, the creation of the digital workplace, actively brings change. Enterprises are responding to consumerization by proactively offering consumer-like enterprise IT environments and solutions. This change comes with new risks (see "Prepare for the Security Implications of the Digital Workplace").

The advent of the digital business and the digital workplace is increasing the speed at which mobility and security are disconnecting. Closing this gap requires a drastic shift in how enterprises tackle endpoint security. The conflict between traditional lockdown and enterprise mobility can be attributed to three main root causes: people, process and technology. It is under these three perspectives that it is analyzed in the first, second and third impacts, respectively. Enterprises should use the set of strategies illustrated to gradually introduce change in their endpoint security architecture. Initially the focus will be mobile devices. Gradually this set of strategies will become the norm for all endpoints.

Figure 1. Impacts and Top Recommendations for How Digital Business Reshapes Mobile Security



Impacts	Top Recommendations
The increasing tendency to mix personal and business data on devices conflicts with and results in the bypass and breakdown of the legacy endpoint security models of enterprises.	• Increase user accountability to reduce device lockdown. • Offer mobile enterprise applications with consumer-grade mobile user experience.
Management misinterpreting mobile risk and organizational structures that do not allow enterprise mobility projects to cater for security leads to growing security gaps for enterprises.	• Translate technical mobile risk to enterprise risk. • Think strategically, but act tactically.
Endpoint platforms become user-administered and application-centric, creating hurdles for enterprises attempting to enforce management and security policies on them.	• Abandon device-centric security models in favor of app-centric models. • Trial data-centric solutions, but be aware of the limitations, • Identify native solutions as a midterm/long-term alternative.

Source: Gartner (February 2015)

Impacts and Recommendations

The increasing tendency to mix personal and business data on devices conflicts with and results in the bypass and breakdown of the legacy endpoint security models of enterprises

Enterprise-owned devices, as well as bring your own device (BYOD) ones, are increasingly hosting both business and personal data. Form factors become more personal, and wearables' modern work styles require fast and easy switching between business and personal data. Therefore, modern endpoint models need to protect enterprise data without making the separation or protection evident to the user.

Secondly, IT does not have exclusivity over the provision of IT solutions. Therefore, solutions with a suboptimal user experience lead to users adopting privately owned devices and sometimes privately managed apps to work with enterprise data. This second practice is directly responsible for enterprise leaks.[6], [7] More often, these practices lead to silent enterprise leaks. These are incidents that often go unobserved when employees upload enterprise data to third-party clouds. Once leaked, the enterprise can neither track nor retrieve that data (see "Unprotected Cloud File Shares and Shadow IT Threaten Data Security").

Recommendations:

- **Increase user accountability to reduce device lockdown.**

  Device lockdown consists of the translation of security policies from logical to technical enforcement. Removing device lockdown is partly achieved by migrating many of these controls to the application layer, where the IT administrator has more freedom to act.

  However, complete lockdown, even on an application level, still conflicts with modern work styles, whereby users are accustomed to being able to work with data across multiple apps and transfer files between devices. The way modern endpoints are secured requires increasing the level of user freedom. Accommodating this need while maintaining the same level or risk acceptance requires holding users more accountable and responsible for their actions.

  This line of thought is tightly coupled to the concepts of people-centric security that Gartner has been developing (see "Consider a People-Centric Security Strategy").

  To increase accountability, organizations need to increase visibility on what occurs on mobile devices. A number of solutions offer varying amounts of monitoring (sample vendors include Adallom, Skyhigh Networks and Resolution1 Security — for a detailed description, see SaaS Platform Security Management in the "Hype Cycle for Cloud Security, 2014").

  However, this is currently limited for a combination of user-related reasons (for example, organizations have limitations in what they are allowed to monitor on privately owned devices, and those same difficulties sometimes extend to enterprise-owned devices). The other set of reasons has to do with the limitation platforms themselves (see the "Endpoint platforms become user-administered and application-centric, creating hurdles for enterprises attempting to enforce management and security policies on them" section below). For example, via passive monitoring, enterprises can see that a specific cloud storage app is used, but cannot identify which specific file is being uploaded.

  As highlighted in Figure 13 in "Bring Your Own Device: The Results and the Future," 7% of all users would not report mobile breaches, while 21% are unsure whether they would do so. Therefore, some level of lockdown, in the form of application containment, is still necessary — For example, forbidding copy-paste into nonbusiness applications, or usage of data from enterprise apps with nonbusiness apps. The right amount of policy enforcement will depend on a number of factors, such as enterprise risk appetite and regulatory constraints. The "Endpoint platforms become user-administered and application-centric, creating hurdles for enterprises attempting to enforce management and security policies on them" section below provides an overview of how to achieve application-level lockdown.

  Certain solutions enable users to run as "standard users" and self-elevate on an exception basis if, for example, a justification is provided. This strikes the right balance of security/responsibility with a logged event. Vendors such as BeyondTrust and Avecto provide this sort of solution for Windows. Even though this is an interesting concept that could extend to purely mobile platforms, an iOS or Android user is currently, by default, a "standard user" and cannot escalate his or her privileges unless he or she jailbreaks or roots the device.

- **Offer mobile enterprise applications with consumer-grade mobile user experience.**

Users turn to consumer devices and consumer apps because they offer a pleasant and efficient experience. To prevent shadow IT, rather than employing lockdown, it is much more productive to focus on offering the same quality of experience through enterprise solutions.

For example, an enterprise-offered alternative to a personal file synch-and-share app deters the workforce from using consumer apps with enterprise apps, avoiding data leakage by offering a path of least resistance (see "Magic Quadrant for Enterprise File Synchronization and Sharing").

One mistake many organizations make is trying to convert their legacy tools to work in mobile use cases. This makes for an awkward user experience, which leads users to employ shadow IT apps. The effort should be to deliver solutions that are tailored for mobile use and, therefore, deter shadow IT practices, rather than forcing legacy toolsets to deliver functionality on mobile platforms that they were never designed for.

For example, a VPN based on a one-time password derived from a hardware token may be employed for enterprise laptops. Migrating the same solution to smartphones — for instance, in the context of a sales associate in an airport — can prove to be challenging. Alternatively, a per-app VPN leveraging a certificate deployed via an EMM tool would activate when the app is opened, and deactivates when the app is closed, providing a much more pragmatic mobile experience. Admittedly, this is just user authentication to the device, rather than true user authentication, but many organizations find that level of security suitable.

Management misinterpreting mobile risk and organizational structures that do not allow enterprise mobility projects to cater for security leads to growing security gaps for enterprises

Mobile security remains one of the top concerns in IT departments, but the IT spending measured does not match the level of concern. In a recent Gartner survey, 71% of respondents said that mobile security is an area of high interest, but only 38% will invest significantly in 2015. While the invest interest is relatively high, 56% of respondents were also interested in network security, and 35% also want to invest in this technology, providing a much better ratio.

Top management typically expresses a generic concern about the uncertainty that comes with mobility, but the same management has observed enterprise data residing for years on mobile devices with basic security measures (such as Exchange ActiveSync) without having evidence of well-publicized breaches stemming from mobile.

From an organizational standpoint, enterprise mobility programs are run by IT operations. While this practice is logical, one side effect is that the selection of enterprise mobility management (EMM) tools is oriented toward workforce enablement. Often, security departments find their only hook to the device is the EMM agent, which, because of buying center considerations, does not support certain security functionalities or has reduced priority within the vendor's road map.

Recommendations:

- **Translate technical mobile risk to enterprise risk.**

Enterprise mobility managers and IT security leaders need to facilitate the translation of technical risk into enterprise risk.

For example, jailbroken iPhones can be unlocked, and files can be stolen. Organizations using Exchange ActiveSync alone for policy enforcement cannot detect jailbreak. An EMM or a mobile threat defense tool (see Mobile Advanced Threat Defense in "Hype Cycle for Enterprise Mobile Security, 2014") is required to monitor jailbreak detection on the devices.

Approximately 7.5% of today's iOS devices are jailbroken.[8] In inquiries with Gartner clients, it has been observed that a 1-000-user company loses 1.5 mobile devices per month on average. By putting this data together and quantifying a possible breach, an organization can calculate what the cost of a mobile breach is (see "Pay for Mobile Data Encryption Upfront, or Pay More Later" for a breakdown of this exercise).

IT leaders need to communicate the enterprise impact — this being the cost of a data breach and the cost of an EMM tool. Clearly, the data above is an example of a model, because EMM tools offer a variety of other functionalities.

IT leaders need to indicate a direction (for example, an EMM tool that offers containment) and obtain validation. Depending on the risk appetite of the organization, the direction may change. For example, a containment method may or may not be deemed necessary, depending on circumstances (industry vertical, regulatory environment and other factors).

Typically, the team managing mobility is decoupled from the team that traditionally manages the legacy endpoints. This is one of the challenges that organizational structures will have to face (see the "Management misinterpreting mobile risk and organizational structures that do not allow enterprise mobility projects to cater for security leads to growing security gaps for enterprises" section). One way to solve this issue is for the mobile people to involve the desktop and security team at the time the policy is written, so everyone is onboard (as much as they can be).

- **Think strategically, act tactically.**

  Mobile device and platform cycles are 12 to 18 months at the time of this writing. Each new major OS release offers new enterprise functionality. Enterprises need to have the flexibility to replace their solutions to be able to take advantage of new, native features with each cycle. The rate of refresh may slow down in the midterm, but the number of form factors and OS extensions (Android Wear, Apple CarPlay, Android Auto, for example) will increase, keeping the ratio similar.

  Allowing some time for testing and bug fixing, enterprises should introduce solutions that they are able to refresh or replace within 18 to 24 months from their introduction.

  For example, a software development kit (SDK)-based solution will prove to be less agile a solution than an app-wrapping solution to secure apps. An app-wrapping solution intervenes on the binary, rather than the source code, making it easier to replace the solution, should the organization choose to do so (see Note 1). There are important merits in SDK-based solutions, and not all organizations should always go with app wrapping (see "Debunking the Myths of App Wrapping"). However, IT leaders should ask, "In 18 months, can we swap out the solution we are putting in place today?" If the answer is negative, then selection of the technology has to be backed by specific reasons, such as a crucial strategic partnership, use case specificities or something else.

This approach matches the concept of bimodal IT, which foresees two distinct modes of operation: a mode with traditional long-term strategy that emphasizes reliability, safety, accuracy and steady progressions. Mode 2 strategies are about agility and speed (see "Bimodal IT: How to Be Digitally Agile Without Making a Mess"). Trialing solutions from smaller mobile security vendors proposing innovative solutions is a crucial part of this effort. Promoting continuous collaboration between the enterprise mobility program and the security department so that security requirements are taken into account early on in the enterprise mobility program is also paramount (well before the selection of a mobility tool).

Endpoint platforms become user-administered and application-centric, creating hurdles for enterprises attempting to enforce management and security policies on them

Mobile platforms are still relatively new. Without considering BlackBerry devices prior to 10, the first enterprise capabilities on modern mobile devices were observed in iOS 4 (released in 2010). Enterprise features are added with each major release, but this evolution is ongoing. In addition, mobile platforms are primarily consumer ones, meaning that many functions cannot be enforced from the IT administrator's side, but need to be driven by the user. A typical example is that, in the face of a major vulnerability, an organization cannot enforce an OS upgrade. It can only ask (for example, via email) its users to upgrade.

Mobile platforms are also application-centric. To access data, mobile UIs require the user to open an app. Similarly, for attackers to get hold of files, they need to attack mobile apps, which makes it necessary to protect apps so that the enterprise data is protected.

App stores provide basic review through an app approval process, which has contributed to limiting malware on mobile platforms (see"There Is Malware in Your Smartphone and Tablet Future, but Don't Panic Yet"). While this may change as new attacks are uncovered and as mobile devices become the primary device (see "Predicts 2014: Mobile Security Won't Just Be About the Device"),[9] app stores will continue to be the main way of delivering functionality to mobile and wearable devices for many reasons, some technical, but mainly commercial. App store delivery is already expanding to support a variety of other form factors and markets.[10], [11] Enterprises can use this to their advantage — for example, vetting untrusted apps using mobile app reputation solutions that scan commercial app stores, or using their own enterprise app store as a sort of a "walled garden."

The main implication of these two points is that enforcement, visibility and monitoring capabilities on mobile devices are limited. Therefore, it is paramount to move away from device lockdown as much as possible.

Recommendations:

- **Abandon device-centric security models in favor of app-centric models.**

BYOD is a precursor to a greater change in management strategies, in that organizations will treat all endpoints as untrusted ones. Because the intervention on a device level is extremely limited, to prevent data leakage, enterprises need to abstract from the device level and focus on the applications.

Modern mobile platforms require opening an app to access data (such as "Open In" in iOS), which means that, to attack data, attackers will try and target an app. Consequently, organizations need to protect their mobile apps. Solutions such as mobile workspaces and separating business from personal data (see Mobile Containers in "Hype Cycle for Enterprise Mobile Security, 2014") are essentially responding to this need.

- **Trial data-centric solutions, but be aware of the limitations in terms of maturity and scalability.**

  One alternative to securing applications is securing the enterprise data directly, either by skipping application security or adding to that protection. Current solutions achieve this through information rights management, or sometimes simple encryption, and come in a variety of flavors:

  - Solutions that perform file-level encryption
  - Solutions that, in addition to encrypting, take care of the key management, so that users can share files
  - Solutions that impose rights on email messages and attachments

  Some form of agent presence on the device will typically be required to perform this, either stand-alone or within a wrapped app. Some of these solutions will act more as content-based data leakage prevention solutions by watermarking files and monitoring their route via a proxy. As a means of reference, a sample set of vendors that offer different flavors and techniques along the lines described above include Bitglass, Fasoo and Nativeflow, Titus (for a detailed description, see Cloud Access Security Brokers in "Hype Cycle for Cloud Security, 2014").

  From a functional standpoint, many of these offerings provide solutions that are unique. For example, a common limitation in the industry is the ability to wrap commercial apps (see Note 1). A handful of vendors in the industry claim this ability (sample vendors: Bluebox, Nativeflow, MobileSpaces and Better Mobile Security). Many of these solutions solve problems for which there are no widespread solutions in the industry. The main caution is that the vendors offering these solutions are small, and therefore, the risks that come with small technology companies apply (for example, company stability and solution scalability concerns).

  One current challenge is that encryption limits searching and indexing possibilities on the device itself, unless the indexing is built to understand and access the proper keys for decryption. Another caution is that Information Rights Management (IRM)-based solutions typically require data-sensitivity classification on behalf of the user, which is something that impacts the user experience and somewhat conflicts with the whole concept of providing easy-to-use, attractive devices to workforce.

- **Identify native solutions that are the preferred midterm/long-term options for mainstream enterprises.**

Native solutions are also starting to come out from both device manufacturers and app vendors that can assist:

- Device manufacturers are offering dual-persona solutions to contain enterprise information: BlackBerry Balance, Samsung Knox and the solution that will be offered in Android Lollipop (see "Key Impacts of Google Android Lollipop on Enterprise Mobile App Development") are some examples. iOS is offering a managed Open In that allows the enterprise to select which apps and accounts are used to open documents and attachments, thus minimizing data leakage (see "iPhone and iPad Enterprise Security FAQ").
- Even though not entirely mature yet, these features have the advantage that they can offer native experience to users. EMM suites will still be required to manage these features. Organizations with higher-than-average security requirements will still need third-party solutions to cover specific needs.
- Enterprise apps are also starting to emerge. These are popular consumer apps that enter the enterprise and consequently have to offer enterprise features. An example is Evernote, which offers the possibility to have a personal Evernote account in which the enterprise adds a business workspace.[12] That space is administered and owned by the enterprise.

Organizations with average security requirements will find that leveraging a native approach provides the level of security they require, minimizing the impact on the user experience.

Gartner Recommended Reading

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

"Digital Business Forever Changes How Risk and Security Deliver Value"

"Introducing the Spectrum of Trust for Mobile Enterprise Design"

"Hype Cycle for Enterprise Mobile Security, 2014"

"Prepare for the Security Implications of the Digital Workplace"

"Global Security Futures: Architectural Implications of Gartner's Security 2020 Scenario"

"Debunking the Myths of App Wrapping"

"Use the Key Levers of Process to Ensure BYOD Success"

"BYOD vs CYOD: A Regional Best-Practice Guide"

"Connecting People and IoT Devices to the Wireless Network in the BYOD Era"

Evidence

[1] "Forecast Analysis: Internet of Things, Endpoints and Associated Services, Worldwide, 2014 Update."

[2] Gartner expects sales of fitness wearable devices to reach 200 million units per year in 2020 (see "Forecast: Wearable Electronic Devices for Fitness, Worldwide, 2014").

[3] "Forecast: PCs, Ultramobiles and Mobile Phones, Worldwide, 2010-2017, 4Q13 Update."

[4] E. Kovacs, "Communications Between Smartwatches and Phones Exposed to Hack Attacks," Securityweek, 11 December 2014.

[5] S. Margaritelli, "Nike+ FuelBand SE BLE Protocol Reversed," Simone Margaritelli, 29 January 2015.

[6] A system engineer allegedly copied corporate customer data onto a memory card in his smartphone on June 27 ("Benesse Suspect Gets Fresh Warrant Over Second Data Theft," The Japan Times, 11 August 2013).

[7] In a complaint filed by Lyft, the company claims that a former employee downloaded a number of nonpublic company documents to his personal Dropbox account in the lead-up to his departure, including confidential strategic product plans, financial information, forecasts and growth data (R. Lawler, "Lyft Accuses Former COO of Stealing Confidential Documents Before Joining Uber," TechCrunch, 5 November 2014).

[8] As many as 7.5% of iPhone users (30-34 million) globally have jailbroken their devices. In some regions such as China, this figure is somewhat higher than the global average (J. Mick, "'WireLurker' Malware May Have Infected 100,000+ iPhones, No Jailbreak Required," DailyTech, 6 November 2014).

[9] FireEye mobile security researchers have discovered that an iOS app installed using enterprise/ad hoc provisioning could replace another genuine app installed through the App Store, as long as both apps used the same bundle identifier (H. Xue and others, "Masque Attack: All Your iOS Apps Belong to Us," FireEye, 10 November 2014).

[10] HP launches software-defined networking app store (N. Heath, "HP Launches Software-Defined Networking App Store," ZDNet, 25 September 2014).

[11] E. Burns, "Salesforce Launch Appexchange Store Builder," Computer Business Review, 11 December 2014.

[12] Evernote Business.

Note 1 App Wrapping

App wrapping is a technique that applies policy enforcement on an app by intercepting its calls to the OS during runtime. Policy enforcement can, for example, disallow copying from the app and pasting content into other apps. It can also impose a passcode on the application, impose data encryption at rest or use a VPN when contacting the enterprise core network. Different app-wrapping vendors use slightly different techniques to intercept runtime calls. Usually, app wrapping involves some degree of code injection to the finalized app in binary format, meaning that commercial apps cannot be wrapped unless the independent software vendor publishes the commercial app with the injected code from the mobile application management or EMM embedded by the vendor.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."