Gartner | Press Release

CONTACTS:
Christy Pettey
Gartner
+ 1 408 468 8312
christy.pettey@gartner.com

Robert van der Meulen
Gartner
+ 44 (0) 1784 267 738
rob.vandermeulen@gartner.com

Gartner Identifies Three Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD

STAMFORD, Conn., December 4, 2012 — Seventy per cent of respondents in a recent survey by Gartner, Inc. said that they have or are planning to have "bring your own device" (BYOD) policies within the next 12 months to allow employees to use personal mobile devices to connect to enterprise applications. Thirty-three per cent of all organisations surveyed currently have BYOD policies in place for mobile devices, such as smartphones and tablets.

“Shifting from an enterprise-owned mobile device fleet to having employees bringing their own devices has a major impact on the way of thinking and acting about mobile security,” said Dionisio Zumerle, principal research analyst at Gartner. “Policies and tools initially put in place to deal with mobile devices offering consumer-grade security must be revised to deal with these devices being under the ultimate control of a private user, rather than the organisation.”

Gartner said that organisations must consider and take action on three major impacts when moving to a BYOD policy:

Impact 1 - The right of users to leverage the capabilities of their personal devices conflicts with enterprise mobile security policies and increases the risk of data leakage and the exploiting of vulnerabilities.
Outside the organisation's premises, employees may define their own usage policy for personal devices. Users can, therefore, install apps and visit URLs of their choice, whereas enterprises can limit applications and web access on enterprise-owned devices. Users can also decide the level of protection for their personally owned devices. When enterprise data is allowed on these devices, the risk of leakage increases for the organisation, not just because of the rise of mobile malware, but also because legitimate but unsupported apps may inadvertently create security risks for the organization and, most importantly, because of device loss.

Using mobile device management (MDM) software is one way to enforce policy on mobile devices. Users should obtain access to enterprise information only after having accepted an MDM agent on their personal devices, and possibly a URL filtering tool, such as a cloud-based secure web gateway (SWG) service, to safeguard and enforce enterprise policy on Internet traffic. Businesses should consider using application white listing, blacklisting and containerisation, as well as setting up an enterprise app store, or app catalogue, for apps that are supported.

Impact 2 - User freedom of choice of device and the proliferation of devices with inadequate security make it difficult to properly secure certain devices, as well as keep track of vulnerabilities and updates.

-more-

Allowing users, rather than the IT department, to select operating systems (OS) and versions of mobile devices opens the door to devices that are inadequate from a security standpoint. An essential security baseline should require enhanced password controls, lock timeout period enforcement, lock device after password retry limit, data encryption, remote lock and/or wipe. The enterprise mobility baseline must also express minimum requirements on hardware — OS versions will not be sufficient.

In alignment with the mobile security policy, network access control policies should be used — for example, to deny access to enterprise resources such as email and apps from devices that cannot support the security baseline. Preventive action should be taken to ban noncompliant devices or create an alert for them by using tools such as MDM software.

Nevertheless, excessively limiting the types of allowed devices eliminates the benefits of BYOD for users. There should be no compromise of security for the sake of device variety, but where it is possible to manage and secure a new device model, it should be done. The policies that are enforced will depend on the risk appetite of the organisation and the sensitivity of data allowed to reside on the device.

Impact 3 - The user's ownership of device and data raises privacy concerns and stands in the way of taking corrective action for compromised devices.
Most people consider data on their personal devices as their property, and would strongly object to having it manipulated by the organisation without their explicit consent. When shifting from enterprise to user-owned devices, "remote wipe," which is a fundamental security feature in a mobile security policy, becomes complicated from a legal and cultural point of view. Thus, sufficient attention should be paid to this issue to avoid repercussions. In practice, "selective wipe" is proving to be difficult in ensuring that all business data, and only business data, has been deleted from the device.

In this situation, it is recommended to liaise with the legal department to obtain advice, because there may be legal implications related to device wiping. Problems may arise if the user refuses a remote wipe. Time is of the essence when performing this task, and asking the user for permission after the compromise, when a remote wipe is considered necessary, will be impacted by message exchange delays that can be critical. It is therefore advisable to obtain the explicit, written consent of users to delete their data in case of compromises, or the loss or theft of devices, at the time of the user's initiation to the BYOD programme.

Additional information is available in the report "Three Crucial Security Hurdles to Overcome When Shifting From Enterprise-Owned Devices to BYOD". The report is available on Gartner's web site at http://www.gartner.com/resId=2237715.

About Gartner
Gartner, Inc. (NYSE: IT) is the world's leading information technology research and advisory company. Gartner delivers the technology-related insight necessary for its clients to make the right decisions, every day. From CIOs and senior IT leaders in corporations and government agencies, to business leaders in high-tech and telecom enterprises and professional services firms, to technology investors, Gartner is a valuable partner in 12,400 distinct organizations. Through the resources of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events, Gartner works with every client to research, analyze and interpret the business of IT within the context of their individual role. Founded in 1979, Gartner is headquartered in Stamford, Connecticut, USA, and has 5,300 associates, including 1,390 research analysts and consultants, and clients in 85 countries. For more information, visit www.gartner.com.

# # #