Gartner | Press Release

FOR IMMEDIATE RELEASE

CONTACTS:
Janessa Rivera
Gartner
+ 1 408 709 8220
janessa.rivera@gartner.com

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

Gartner Says 30 Per Cent of Organisations Will Use Biometric Authentication for Mobile Devices by 2016

Proliferation of Devices in the Workplace Will Require Trade-Offs Between Security and Usability

London, UK, 4 February, 2014 — The consumerisation of IT and business bring your own device (BYOD) programmes have resulted in potential security problems for IT leaders, according to Gartner Inc. User expectations of a clean and simple mobile user experience often outweigh security concerns, and the same valuable data guarded by complex passwords and security measures on PCs can be left vulnerable on mobile devices. Gartner predicts that, by 2016, 30 per cent of organisations will use biometric authentication on mobile devices, up from five per cent today.

"Mobile users staunchly resist authentication methods that were tolerable on PCs and are still needed to bolster secure access on mobile devices," said Ant Allan, research vice president at Gartner. "Security leaders must manage users' expectations and take into account the user experience without comprising security."

Gartner has identified some potential security impacts of the consumerisation of IT, and has made some recommendations for IT security leaders.

User experience trumps security concerns

While most organisations require robust passwords on laptops, smartphones and tablet devices often have access to the same applications and critical data but not the same levels of security. The increased number of devices in play also exacerbates the exposure of critical information. Implementing standard power-on password policies is made much more complex by the acceptance of BYOD practices, with the inevitable clash over user rights and privacy.

While complex passwords can be especially problematic for users to type on mobile devices, if these devices hold corporate data or provide access to corporate systems such as email without further login — even a default four-digit password is inappropriate. However, support for more robust power-on authentication is patchy — with only a few mobile operating systems and devices supporting biometric authentication. Even in cases that do offer this support, the implementation may not be good enough for business use.

"An eight-digit numeric password will require hours to recover, and that will discourage casual hackers with toolkits," said John Girard, vice president and distinguished analyst at Gartner. "However, even a six-character lowercase alphanumeric password can provide billions of values. For most practical purposes, hackers are not prepared to pursue this large a set of combinations due to the relatively slow speeds involved in brute force attacks against smartphones and tablets."

-more-

Gartner recommends that a password policy requiring use of at least six alphanumeric characters, and prohibiting dictionary words, is enforced on devices with access to corporate information via mobile device management (MDM) tools.

Wipe the slate clean

Some organisations attempt to counter the risks from a lost or stolen device by implementing controls that wipe a device after a limited number of incorrect password entries, or by remote command. "This practice does not wholly mitigate the risk because solid-state memory is nearly impossible to overwrite," said Mr Girard. "The best practice is to use encryption that is not tied to the primary power-on authentication, meaning the key cannot be recovered from the device after a soft wipe operation has been performed."

In addition, Gartner recommends that a further authentication method — at a minimum, another password — should be used for access to sensitive corporate applications and data. In this way, even if a hacker breaches the power-on defences, each additional app or store of data presents an additional challenge that will, collectively, present too much of a hurdle to be worthwhile.

In some cases, higher-assurance authentication is required. In PCs (traditionally), a standalone device may be used to provide a hardware token that might be used to provide additional authentication. "Traditional authentication of this kind is often spurned in mobile use cases, because of the poor user experience with most kinds of hardware tokens," said Mr Allan. "Juggling the token in one hand, the phone in another and a latte in the third is increasingly resisted by mobile device users."

Software tokens, such as X.509 credentials on the endpoint, provide options in this case, but often need MDM tools to be implemented properly and still require additional controls to provide the higher-assurance authentication necessary in some organisations.

Biometric options offer compromise

Gartner recommends that security leaders evaluate biometric authentication methods where higher-assurance authentication is required. Suitable authentication modes include interface interactivity, voice recognition, face topography and iris structure. These modes can be used in conjunction with passwords to provide higher-assurance authentication without requiring any significant change in user behaviour.

Moreover, as a mobile device itself provides a rich node of identity-relevant contextual data, this information can also be used to increase the trust in the claimed identity. It is possible that the combination of passive biometric authentication and contextual authentication will provide sufficient assurance in medium-risk scenarios without the need for "gateway" authentication events using passwords or tokens.

It is also important, when planning a comprehensive authentication policy that includes mobile devices, to consider the burden on organisations and users alike — so that the policy is sustainable. "Adopting significantly different authentication methods for different devices will eventually be unsustainable," said Mr Allan, "Mobile-apt authentication methods must also be PC apt. Combinations of X.509 credentials on the endpoint, low-friction biometric modes and contextual authentication will likely fit the bill."

Additional information is available in the report "Good Choices for Mobile Authentication Must Balance Conflicting Security, Technical and User Experience Needs." The report can be found on Gartner's web site at http://www.gartner.com/doc/2595417.

This topic will also be discussed in more detail at the Gartner Identity & Access Management Summit 2014, held from 17 to 18 March in London, UK For more information about the Summit, please visit

europe.gartner.com/iam.. Members of the press can register by contacting Rob van der Meulen at rob.van.dermeulen@gartner.com. You can also follow the event on Twitter at http://twitter.com/Gartner_inc using #GartnerIAM.

About Gartner Identity and Access Management Summit 2014
The Gartner Identity and Access Management Summit is the only IT event dedicated to the issues faced by identity and access management (IAM) professionals. It will lay out the key trends and strategies that will define successful IAM programmes. It will also examine the technology, tools and techniques needed to establish effective IAM programmes at a time when IT architectures and the regulatory landscape are rapidly changing in response to the Nexus of Forces — mobile, cloud, information and social.

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 more than 13,000 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 5,800 associates, including more than 1,450 research analysts and consultants, and clients in 85 countries. For more information, visit www.gartner.com.

# # #