Gartner | Press Release

CONTACTS:
Janessa Rivera
Gartner
+ 1 408 468 8312
janessa.rivera@gartner.com

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

Gartner Says Hosted Virtual Desktops Can Increase Security and Help Organisations Meet Compliance Standards

Analysts to Discuss Security Trends at Gartner's 2013 Security and Risk Management Summits, 10-13 June in National Harbor, Maryland, 19-20 August in Sydney and 18-20 September in London

STAMFORD, Conn., April 23, 2013 — One of the most commonly cited motivations for implementing hosted virtual desktops (HVDs) is to increase the security of end-user computing, according to Gartner, Inc. Gartner said that properly implemented HVDs can increase security, and help organisations and infrastructure leaders meet compliance requirements. However, before assuming HVD is the right answer to all security and compliance concerns, security professionals need to consider the alternatives available.

"Having the organisation's data spread across hundreds or thousands of devices, many of which leave the physical security of office locations, presents a significant risk of data loss," said Neil MacDonald, vice president and Gartner Fellow. "HVDs can help improve the security standing of the client computing environment by centralising sensitive information and applications in the data centre, giving IT system and security stakeholders the opportunity not only to improve support efficiency, but also security."

HVD is a technology that enables client computing to shift from a device-centric to a user-centric workspace, application and data delivery technology while providing an endpoint-agnostic access solution where the user's workspace can be accessed from many different locations using many different devices.

Although HVD architecture holds the promise of a more secure environment, it can only do so if carefully planned, deployed and configured, then managed consistently on an ongoing basis. Security may be a native strength of the HVD architecture, but any solution under consideration must be cost-effective and compatible with the applications user's need, must be sized appropriately for capacity and performance and, most importantly, must deliver a good end-user experience.

"An HVD architecture is complex, and infrastructure and security stakeholders must consider multiple facets, such as device form factors, access methods and data security, to avoid potential issues," said Nathan Hill, research director at Gartner. "Chief among the concerns of organisations is how they capitalise on the opportunity to use HVDs and ensure that the environment is secure, and which areas of the architecture represent a change in risk profile from traditional client computing architectures.

Many traditional PC security considerations remain with the HVD architecture, including desktop OS antivirus protection, but the complex nature of the HVD architecture also introduces new areas where security must be considered. Security stakeholders must ensure that they address the security requirements of the access device and remote connectivity, in addition to the virtualisation platform.

Emerging HVD security solutions promise enterprises and users more efficient and secure platforms tailored for the architecture's needs. Over the past four to five years, there has been an improvement in platform architecture, with the evolution of software and hardware tailored to the workload, including HVD appliances, reference architectures, storage virtualisation and personalisation software. The same is true

for security solutions that are evolving to meet the demands of the platform, and to offer increased security and/or performance.

"Centralising workloads gives organizations the potential to improve security, but because risk is aggregated in the data centre and network with HVD, strong security controls are required to protect the infrastructure," said Mr MacDonald. "As a result it's important to address data and HVD security requirements, and leverage the security capabilities of the Citrix and VMware product sets, when required."

More detailed analysis is available in the report "Know the Security Implications of Adopting Hosted Virtual Desktops." The report is available on Gartner's web site at http://www.gartner.com/resId=2414215.

Gartner analysts will take a deeper look at the outlook for security solutions at the Gartner Security & Risk Management Summits 2013 taking place 10-13 June in National Harbor, Maryland, 19-20 August in Sydney, Australia and 18-20 September in London, UK. More information on the US event can be found at www.gartner.com/us/securityrisk. Details on the Australia event are at http://www.gartner.com/technology/summits/apac/security/. More information on the UK event is at http://www.gartner.com/technology/summits/emea/security/.

Members of the media can register for press passes to the Summits by contacting christy.pettey@gartner.com (US), susan.moore@gartner.com (Sydney) or laurence.goasduff@gartner.com (London).

Information from the Gartner Security & Risk Management Summits 2013 will be shared on Twitter at http://twitter.com/Gartner_inc using #GartnerSEC.

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 5,500 associates, including 1,400 research analysts and consultants, and clients in 85 countries. For more information, visit www.gartner.com.

# # #