

FOR IMMEDIATE RELEASE

CONTACTS:

Christy Pettey

Gartner

+ 1 408 468 8312

[christy.pettey@gartner.com](mailto:christy.pettey@gartner.com)

Robert van der Meulen

Gartner

+ 44 (0) 1784 267 738

[rob.vandermeulen@gartner.com](mailto:rob.vandermeulen@gartner.com)

## **Gartner Predicts Cloud as a Delivery Model to Shape Buying and Prioritisation of Security**

### ***Analysts Identify Key Security Solution Predictions for 2013 and Beyond***

STAMFORD, Conn., January 22, 2013 — Increased adoption of cloud-based computing is expected to impact the way security is consumed as well as how key government agencies will prioritise security of public cloud infrastructures, according to Gartner, Inc. The growing importance of public clouds, along with the ever-persistent threat on private and public sectors' infrastructures, is expected to result in the US government declaring them a critical national infrastructure.

"The popularity and increased adoption of cloud-based security services, albeit at different degrees, will influence the shape of future security marketplaces," said Ruggero Contu, research director at Gartner. "Deployments of virtualisation, and its replacing of traditional physical hardware platforms, are expected to impact the deployment model of future network security capabilities, which are expected to be based increasingly on virtual security appliances."

Gartner has made three predictions about the security solutions industry for 2013 and beyond:

#### **By 2016, public cloud infrastructure will include and be mandated to critical national infrastructure regulations by the US.**

In lieu of poor economic and debt conditions globally, governments continue to seek ways to reduce their IT operating expenditures, eliminate duplication across their IT organisations and optimise their compute resources. Several key governments have created initiatives for the adoption of cloud-based services but have yet to experience significant negative impacts due to their cloud services adoption in the form of disruptions or attacks on cloud services providers. As the economy becomes heavily reliant on public cloud infrastructure for everyday computing activities, cloud services disruptions will pose greater risks to the overall economy and eventually become a threat to national security in the form of economic disruption.

"Public cloud services providers will need to comply with critical infrastructure protection mandates for systems outside of the scope of just federal government use under the FedRAMP programme (Federal Risk and Authorization Management Programme)," said Lawrence Pingree, research director at Gartner. "Security technology providers will need to prepare their technologies in order to address potential mandates for critical infrastructure protection of public cloud environments. Providers that lack the ability to offer compliant security controls to address critical infrastructure protection mandates will likely face sales difficulties in cloud environments and may be filtered from shortlists based on emerging critical infrastructure protection requirements."

#### **By 2015, 10 per cent of overall IT security enterprise product capabilities will be delivered in the cloud.**

Growth rates for cloud-based security services are set to overtake those of traditional on-premises

security equipment over the next three years with operational cost reduction, flexibility of deployment across multiple IT environments, and fast implementation and product updates among major factors driving demand. A number of factors will inhibit higher adoption of cloud-based security services as not all businesses will be able to benefit from this delivery model in equal measure. Those organisations located in geographies where internet connectivity is unreliable or that require high levels of product customisation will be at a disadvantage in utilising this form factor.

Growth opportunities are present across different regions and countries, but Gartner expects North America to provide the majority of spending.

"The biggest opportunities currently centre on areas such as messaging and web security as well as remote vulnerability assessment," said Mr Contu. "However, as maturity evolves a wide variety of security offerings will emerge, such as data loss prevention (DLP), encryption and authentication, to be increasingly available in the cloud. As new start-up players establish themselves with innovative offerings, established players will look to acquire them to expand their portfolios with new capabilities and remain competitive."

**By 2015, 20 per cent of the VPN/firewall market will be deployed in a virtual switch on a hypervisor rather than a physical security appliance.**

Physical network security appliances, such as server mobility and simplified architecture, can inhibit key virtual server benefits customers seek. Partnering with hypervisor providers has become critical to offering network security on the virtual switch. Virtual switches allow for new firewall players such as host-based security software companies to enter the network firewall market. Since a virtual switch is one level of abstraction away from the physical data switch ports, providing network security is no longer just for physical network providers. Hypervisor providers are moving firewall offerings from the data centre to the network edge. This could be key for new network firewall players leveraging hypervisor technologies to gain firewall market share outside of the data centre.

"Growth in the firewall market could come from virtual players," said Eric Ahlm, research director at Gartner. "To date, the virtual firewall market has been limited to data-centre-class firewalls, which make up the minority of the total firewall market. A push from the virtual providers to bring their technology to the edge could be a key accelerator to the virtual switch market growth. Enabling the key benefits of virtualised servers, while not compromising security, is becoming a key requirement for network data-centre-class firewalls while transportability of network firewall controls outside of a customer's data centre to a third-party provider is essential to customers using these providers for more critical systems."

More detailed analysis is available in the report "Predicts 2013: Security Solutions." The report is available on Gartner's web site at <http://www.gartner.com/resId=2246015>.

More information on Gartner's top predictions for 2013 will be presented in the webinar "Top Technology Predictions for 2013 and Beyond" taking place 27 February at 1pm and 4pm UK time. To register for this complimentary webinar, please visit <http://my.gartner.com/webinardetail/resId=2297221?srclId=1-2994690285>.

More information on security solutions and management will be presented at the Gartner Identity and Access Management Summit 2013 taking place 11-13 March in London, UK. More information can be found at <http://www.gartner.com/technology/summits/emea/identity-access/>. Members of the media can register to attend the event by contact Rob van der Meulen at [rob.vandermeulen@gartner.com](mailto:rob.vandermeulen@gartner.com).

Information from the Gartner IAM Summit 2013 will be shared on Twitter at [http://twitter.com/Gartner\\_inc](http://twitter.com/Gartner_inc) using #GartnerIAM.

Gartner analysts will also look at the outlook for security solutions at the Gartner Security & Risk Management Summit 2013 taking place 10-13 June in National Harbor, MD, 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/security](http://www.gartner.com/us/security). Details on the UK event are at <http://www.gartner.com/technology/summits/emea/security/>. Members of the media can register for press passes to the Summit by contacting [christy.pettey@gartner.com](mailto:christy.pettey@gartner.com) (US), [susan.moore@gartner.com](mailto:susan.moore@gartner.com) (Sydney) or [laurence.goasduff@gartner.com](mailto:laurence.goasduff@gartner.com) (UK).

Information from the Gartner Security & Risk Management Summits 2013 will be shared on Twitter at [http://twitter.com/Gartner\\_inc](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 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](http://www.gartner.com).

# # #