Gartner | Press Release

Gartner Says Through 2016, Federated Single Sign-On Will Be the Predominant SSO Technology, Needed by 80 Per Cent of Organisations

Mobile Devices Pose Latest Challenge to Authentication and SSO
Analysts to Share Best Practices for Identity and Access Management Programmes at Gartner Identity and Access Management Summit 2013, 11-13 March, in London

STAMFORD, Conn., January 31, 2013 — A well-executed single sign-on (SSO) strategy reduces password-related support incidents and provides users with improved convenience and more-efficient authentication processes, according to Gartner, Inc. A sound SSO strategy will give users fewer reasons to write down passwords. However, one password providing access to all in-scope systems can lead to compromised access to those systems.

"Organisations implementing SSO, particularly to systems that hold sensitive data, should implement risk-appropriate authentication methods with the SSO system," said Gregg Kreizman, research vice president at Gartner. "Solutions are not 'one size fits all,' and solutions that provide SSO to all target systems may be deemed too expensive. Therefore, a best practice is to identify the tactical and strategic approaches that reduce enough of the problem space over time and within budget."

Mobile devices can pose further challenges for SSO. "The proliferation of mobile phones and tablets with a variety of operating systems has created the latest and greatest challenges to authentication and SSO," said Mr Kreizman. "Web-architected applications can often be supported with existing access management tools, such as web access management (WAM) and federation, because smartphones and tablets have web browsers. Native mobile resident applications can create a gap in SSO support, and market offerings to resolve the issues are currently immature, proprietary, or not comprehensive enough to support multiple device and operating system variants."

Gartner has identified the following steps and framework that should be used to appropriately scope the target solution set.

Assess the Current Environment and Pain Points
The first step is to scope the problem space by identifying the user population and use cases that require a solution, and to inventory the target systems, their architectures and the anticipated lifetimes.

- User population: Identify whether a solution set should cover employees, contractors, external business partners or consumers/constituents.
- Use cases and applications: Identify the logical location of users and the target systems that must be accessed — for example, internal users accessing internally managed applications and software as a service (SaaS) applications, or external consumers and business partners accessing internally managed applications. Identify the applications and use cases that are currently used the most and generating the most calls to the help desk for authentication-related issues.
- Applications and their architectures: Determine the application architecture for each application deemed to be in scope for an SSO initiative.

Evaluate Anticipated Changes to In-Scope Applications
It's important to determine whether the applications used today will still be in scope over the next few years. If an application is retired or replaced or has its user base significantly reduced within one to two years, then it can possibly be removed from consideration and, therefore, reduce the problem space.

Approaching commercial application vendors to ask whether there are any plans to provide authentication options that can leverage the enterprise standards is also a good idea. A matrix with the inventory results should be drawn up to help identify common architecture and use case patterns.

Leverage Currently Owned Services or Solutions to Reduce the In-Scope Applications
Identifying existing tools that could help reduce the problem is essential. Their use may be isolated to one business unit or application set when they could be more broadly deployed. Sometimes reduced sign-on (RSO), enabled by an established password synchronisation tool or authentication to a common LDAP-accessible directory, will provide good-enough reduction in the problem space. When multiple directories are used for authentication, directory synchronisation or virtual directories may be brought to bear to join disparate identity sources and to expose one standardised view of identity to multiple applications or authentication services, such as a WAM tool. This can provide RSO or SSO, depending on the configuration.

Select Solutions to Resolve the Remaining Requirements
Application designs are moving toward web architectures. As soon as currently owned directories, Kerberos and password synchronization tools have been leveraged, it is likely that tool or service selection will be based on the need to support SSO to web-architected applications. Furthermore, SaaS adoption has been driving the need for federated Web SSO. Therefore, the solutions that support these needs should be presented first, with less prevalently needed solutions following.

More detailed analysis is available in the report "How to Get Single Sign-On" The report is available on Gartner's web site at http://www.gartner.com/resId=2310115.

Additional details on identity management will be presented at the Gartner Identity and Access Management Summit 2013 taking place 11-13 March in London, UK. The Summit will provide the must-have information for retooling an IAM strategy to meet the challenges brought on by the nexus of cloud, social, mobile and the information revolution and to seize the opportunities ahead.

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.

Information from the Gartner IAM Summit 2013 will be shared on Twitter at http://twitter.com/Gartner_inc using #GartnerIAM.

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.

# # #