VANGUARD
INTEGRITY PROFESSIONALS
CYBERSECURITY EXPERTS

FOR IMMEDIATE RELEASE

FOR MORE INFORMATION:
Roxane Rosberg
Vanguard Integrity Professionals
roxane.rosberg@go2vanguard.com
(702) 794-0014

VANGUARD INTEGRITY PROFESSIONALS ANNOUNCE WEBINAR
Leading Cybersecurity Experts to host IBM Systems Magazine Webinar
Securing Cloud with Multifactor Authentication

LAS VEGAS, NEVADA – October 04, 2016 – Vanguard Integrity Professionals, Inc., cybersecurity experts for networks, distributed systems and enterprises, announces the date and time of an IBM Systems Magazine webinar entitled Securing Cloud with Multifactor Authentication. The Vanguard Webinar will be hosted on Thursday, October 20, 2016 12:00 p.m. CDT.

The hour-long webinar will feature Brian Marshall, vp of research and development. Vanguard's executive will discuss how to stay protected with Vanguard Cloud based Authentication.

Enterprises today are looking for ways to outsource email and other applications to the cloud. A critical requirement for making cloud outsourcing migration a success is to ensure that security exposures are not increased. While cloud based services provide many benefits, they can also significantly increase an organization's security risks and vulnerabilities, especially if proper processes to safeguard corporate data are not implemented.

The Vanguard solution works with either IBM® z/OS® Security Server, or standard Windows® Active Directory®. Vanguard Enterprise Cloud Authentication also includes comprehensive options for Multifactor Authentication including Token, Tokenless and PIV Card Authentication. Data is maintained in the Cloud where you benefit from high performance processing and access that cloud solutions deliver. Access is through standard access and authentication from the likes of Google, Yahoo, Sales Force etc. however; control is administered remotely. Data and passwords are separated and never in the same place. If data is breached, no password or credentials are associated.

To minimize risk, enterprises using cloud computing must ensure that their systems are secure and control is centrally managed. Only authorized and authenticated, users should be allowed to access sensitive cloud based data and applications. Securing the cloud is complex, but no more difficult than many of the security challenges that Vanguard has been solving for customers for more than 30 years.

Make plans to attend the IBM Systems Magazine webinar "Securing Cloud with Multifactor Authentication" in order to learn the latest most current information on Cloud based Authentication.

Click on the link below to register.

https://ibmsystemsmag.webex.com/mw3100/mywebex/default.do?siteurl=ibmsystemsmag

For the latest information and training on Cybersecurity, make plans to attend the Vanguard Security & Compliance™ 2016 Conference held at The Westin Hotel in Las Vegas, Nevada, Monday, November 14 through Thursday, November 17, 2016.   www.go2vsc.com

** MORE **

About Vanguard Integrity Professionals

Vanguard Integrity Professionals provides enterprise security software and services that solve complex security and regulatory compliance challenges for financial, insurance, healthcare, education, transportation and government agencies around the world. Vanguard provides automated solutions for Audit and Compliance, Operational Security, and Intrusion Management. The world's largest Financial, Insurance, Government Agencies and Retailers entrust their security to Vanguard Integrity Professionals. Vanguard is committed to protecting and securing the Cloud, z/OS Security Server and any Enterprise environments. Vanguard proudly provides 24/7/365 live customer support from the United States of America.

IBM and z/OS are trademarks of International Business Machines Corporation in the United States and/or other countries.

Windows and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Vanguard Security & Compliance is a trademark of Vanguard Integrity Professionals in the United States and other countries. All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

END##