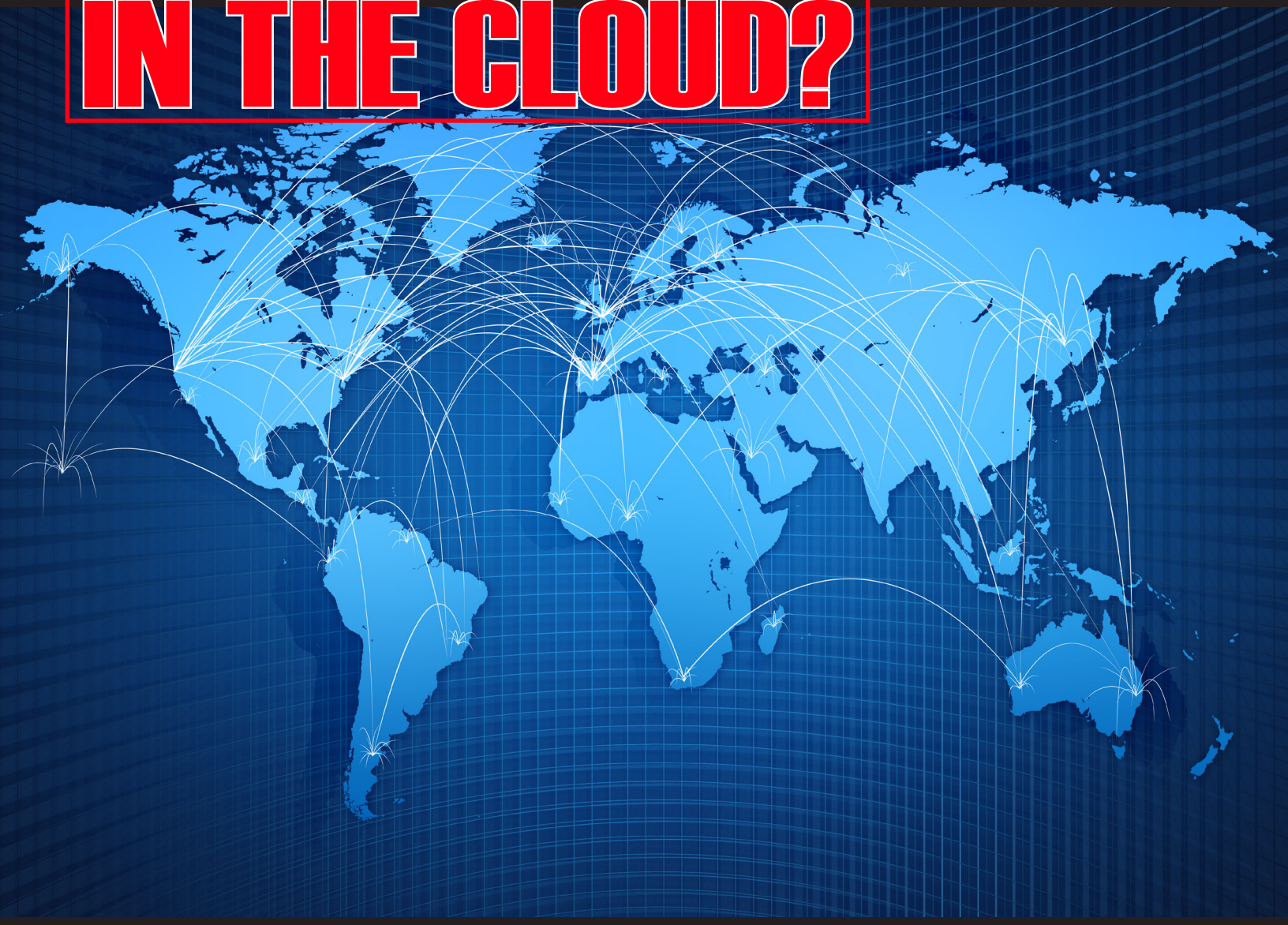
IS THERE AUDITABLE SECURITY IN THE CLOUD?



by Preston Williams III

CLOUD COMPUTING IN POLITICAL CAMPAIGNS

I recently watched the CSPAN coverage of cloud computing in political campaigns held at the Graduate School of Political Management at George Washington University. Participants shared their views about cloud computing in campaigns, but the issue of "auditing through the cloud" appeared problematic. I put on my "auditor" hat and began to question a number of issues related to the performance of a reliable audit in a private, public, or hybrid cloud environment.

An extensive discussion about various platforms, architectures, and application layers as well as corporate protocols and policies provides a lot of food for thought as we consider how, when, and if we should deploy a public or private cloud in our enterprise.

The ability to establish standards for auditing through the cloud is captured in ISO/IEC 27001 "Information Security Management," which replaces BS7799-2. The standard applies Organization for Economic Cooperation and Development (OECD) principles governing security of information and network systems to the process of developing "best practices," which will ensure that providers and customers are satisfied with the level of transparency, security, and verifiability of both the process and the results of an audit review. The standard is intended to provide a foundation for third-party audits.

An engaging discussion about the role of the internal auditor in the cloud is discussed here: (http://tinyurl.com/CC-Internal-Audit), and I found this article about "simplifying cloud computing security audit procedures" quite informative.

Another interesting follow-up discussion that I have seen related to this matter is the quality of the audit report generated from a cloud audit review.

The notion that this issue is considered both substantive and complex enough to have garnered the import of IBM, Cisco, SAP, EMC, and several other technology companies to create an 'open cloud manifesto' is quite encouraging. Their clarion call for more consistent security and monitoring of cloud services is captured in the "Cloud Computing Use Cases" white paper.

The following issues are considered quite important in the ongoing discussion:

Endpoint Security: Customers should secure endpoints to their cloud resources. This includes the ability to restrict endpoints by network protocol and device type.

Event Auditing and Reporting: Customers should be able to access data about events that happen in the cloud, including system failures and security breaches. Their access to events should include the ability to learn about past events and reporting of new events as they occur.

Identity, Roles, Access Control, and Attributes: The solution should also address identity, roles, entitlements, and any other attributes of individuals and services in a consistent, machine-readable way. Customers should be able to effectively implement access-control and enforce security policy against cloud-based resources.

Network Security: Customers and providers should be able to secure network traffic at the switch, router, and packet level (i.e., The IP stack itself should be secure).

Security Policies: It must be possible to define, resolve, and enforce security policies in support of access control, resource allocation, and any other decisions in a consistent, machine-readable way.

Audit and Compliance: There should be the ability to collect audit and compliance data spread across multiple domains, including hybrid clouds.
Beyond XaaS and PaaS, there is a radical view about the value proposition for extending to the cloud in the article titled "Don't buy cloud computing hype: Business model will evaporate."

Given all of the preceding points, is there "auditable security" in the cloud? ■