SECURITY MUST "TRUST BUT VERIFY"

Security solutions must enforce the true spirit of security policy.

JOHN DE SANTIS
CHAIRMAN AND CEO,
HYTRUST

GOVERNMENT AGENCIES often have a tough time moving to the cloud. The Obama administration gave federal CIOs a mandate with its "Cloud First" policy, yet agencies and departments at all levels of government perceive great risks, and many remain reluctant. What's needed is a new, more strategic approach to cloud security to help government proceed with confidence.

Compared to commercial organizations, public sector organizations are under a microscope when it comes to compliance. Scrutiny comes from all sides: from internal auditors, external auditors, regulators, Congress, and even politically motivated independent actors. There's little wonder they're hesitant to shake up their IT. Depending on the agency, a data breach could affect not just personal privacy, but also national security.

The need for data security is nothing new in government. Many standards have been drafted by the National Institute of Standards and Technology (NIST) and others to help guide the way. This is actually considered trustworthy behavior in a highly virtualized or cloud environment from an operational perspective.

The problem is that organizations too often take a tactical approach to security. The controls they put in place are designed to mitigate threats, not enforce policy. As a result, policies can too easily be subverted, either through malice or simple negligence.

For example, security audits are only beneficial if compliance is based on not just the letter, but the spirit of security standards and policies. Bad behavior hidden from auditors is still bad behavior. In some cases, an organization can start drifting into noncompliance within hours after completing an audit.

Most often, a bad actor can simply gain access to privileged credentials and take actions that are outside policy but nevertheless possible due to elevated account privilege. This was the case in a massive data breach in 2014, for example, where bad actors were able to harvest sensitive data from databases for more than a year.

Moving to the cloud adds more wrinkles to the security challenges facing government CIOs. It means relinquishing some modicum of control. The old adage of "trust but verify" must now apply.

A more strategic approach would be to implement security controls that don't just monitor and guard against potential threats, but actively enforce security policy. By deploying software to continuously enforce policies in real time, agencies can truly automate good behavior on their networks.

For example, it should not have been possible for the attackers to export sensitive databases to external sites. If there are indeed legitimate use cases for such actions, they should trigger red flags that require approval by a second or third person. A secondary benefit of this type of automation is that it eases the pain of the compliance auditing and investigation process. Instead of answering endless questions, an agency can generate reports to demonstrate policies are automatically and continuously enforced.

HyTrust has already seen this strategic approach deliver benefits for the commercial sector. The need in government is even greater. We believe automated security policy enforcement is the key—not just to more reliable data protection, but to cutting the red tape of the audit process so agencies can proceed to the cloud with confidence.

***John De Santis** is the chairman and CEO of HyTrust.*

Enable trustworthy infrastructure and eliminate security gaps.

Secure data in the cloud and automate private cloud compliance with HyTrust Workload Security.

Visit www.carahsoft.com/innovation/HYTRUST-cloud.

HYTRUST