Government Business Council
Industry Insights

A Briefing
by GBC:
Industry Insights
December 2011

Cloud Computing:
The Need for Continuous Monitoring

Cloud computing, a process which provides users with access to scalable, on-demand capabilities through internet-based technologies, is still relatively new to federal agencies. While cloud has the potential for great benefits, especially in cost-savings and convenience, many federal managers hesitate because of the security risks involved. Agencies can reduce this risk through the use of continuous monitoring.

Defining Continuous Monitoring

Continuous monitoring refers to the ongoing observation of an organization's networks, information, and systems. It allows for responses that accept, transfer, or mitigate risk as situations change. Continuous monitoring is not new; The National Institute of Science and Technology (NIST) first introduced the concept in 1995.[2]

While often associated with cloud computing, continuous monitoring can assist other agency operations. The Central Intelligence Agency uses continuous monitoring for their security infrastructure, ensuring that firewalls and other network access controls continue to function during infrastructure changes. Continuous monitoring can be leveraged in any situation in which information technology administrators want to remain up-to-date on the security status of their agency's network.

Continuous monitoring has three cyclical objectives:

- **Prevent.** Continuous monitoring seeks to minimize agency data loss to known cyber threats.
- **Predict.** Analyzing usage patterns can help an agency to accurately forecast future threats. By breaking the chain of events leading to an outbreak, continuous monitoring may be able to stop an incident from occurring.
- **Respond.** Since it is acknowledged that not all threats can be prevented, continuous monitoring enables an agency to respond within minutes of the breach. This assures that vital government services remain available, while decreasing the costs associated with damage remediation.

> “Continuous monitoring is the backbone of true security – security that moves beyond compliance and paperwork. The threats to our nation‘s information security continue to evolve and therefore our approach to cybersecurity must confront these new realities on a real time basis.
>
> -Vivek Kundra
> former Federal Chief
> Information Officer [1]”

Agency Requirements

Real-time data. Current federal regulations require infrequent security checks of agency networks, but these scans are often wasteful. While “point-in-time” monitoring tests the security of the agency network at that moment, they are mere snapshots in time. These scans leave many blind spots, telling nothing about what has transpired since the last test.

> “Organizations need a comprehensive approach to manage risk—an approach that recognizes the balance between the organization’s mission and business functions and its day-to-day operations...
>
> - National Institute of Science and Technology [8]”

“Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient condition to demonstrate security due diligence,” Kundra testified to the House Committee on Oversight and Government Reform in March 2010. “An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle.”[3]

Cost-savings. This “culture of compliance” is extremely costly. Results must be reported to the Office of Management and Budget, Congress, and the Government Accountability Office, demanding large amounts of time, paper and money. From 2004 to 2010, the Department of State spent $133 million amassing a total of 50 shelf feet, or 95 thousand pages, of security documentation for about 150 major IT systems. Each page cost the federal government about $1,400.[4]

Agencies also incur costs after a security breach, including notification and credit-monitoring services if personal information is leaked. The Department of Energy paid more than $2 million to recover from infrastructure attacks in FY2011.[5] Energy Inspector General Gregory Friedman noted in the agency’s audit that the agency “did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place.” Through automated support tools like vulnerability and network scanning devices, security can become more cost-effective, consistent, and efficient.

Collaboration. The “silo-ed” or “stovepiped” approach of traditional risk management strategies is no longer effective in today’s environment. A collaborative effort within agencies is necessary to block threats to data security. Decision makers must know how their actions affect other parts of the organization. A robust continuous monitoring program requires the active involvement of many people, including information system owners and common control providers, mission and business owners, and agency leadership.

Federal applications cannot afford to depend on trial and error. The collaborative strategy should include cloud provider oversight; when developing contracts, agencies should build continuous monitoring into the original agreement.

“A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved from the agency heads to those charged with oversight. It entails employees, contractors, and the American people working together to create a culture of vigilance and security to enable us to continue to efficiently leverage the power of technology while respecting the privacy and civil liberties of the American people,” Kundra testified in 2010.[6]

Improving Your Risk Management Strategy

Agency decision makers must be aware of missing patches, known vulnerabilities, cases of noncompliance with approved configurations, and any violations of security control policies before a risk management strategy can be developed. After conducting a thorough security assessment, agencies should engage in the following activities: [7]

1. **Categorize information systems.** Define the sensitivity of agency data based upon the negative impact a breach would have on the agency’s mission.
2. **Select security controls.** Select baseline controls and supplement them as needed based on continued analysis.
3. **Implement security controls.** Implement an enterprise-wide approach that focuses on the total life cycle of systems. Controls should be executed across the agency’s three hierarchical tiers: at the mission and governance level; the business process level; and the information systems level.

4. **Assess security controls.** Determine if security controls are effective and assess if the risk level is acceptable to the agency's requirements.

5. **Authorize information system.** If risk is acceptable, the ...[add. Text to come].

6. **Monitor security state.** Continuously track changes to the system and reassess the system's effectiveness. These steps should be repeated as new agency data is created or additional threats become known.

"Organizations need a comprehensive approach to manage risk—an approach that recognizes the balance between the organization's mission and business functions and its day-to-day operations—including the use of information systems to achieve their missions and accomplish their business goals," says NIST.[8]

While continuous monitoring alone does not provide a comprehensive, enterprise-wide security solution, it is a key component in the federal risk management strategy.

[1] Vivek Kundra, OMB Chief Information Officer Memorandum, Subject: Security Testing for Agency Systems, April 5, 2010.
[2] NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, 1995, http://csrc.nist.gov/publications/nistpubs/800-12.
[3] Vivek Kundra, *Federal Information Security: Current Challenges and Future Policy Considerations, Testimony before the House Committee on Oversight and Government Reform*, March 24, 2010, http://www.cio.gov/pages.cfm/page/Vivek-Kundra-Testimony-Federal-Information-Security.
[4] Kundra, March 24, 2010.
[5] Gregory Friedman, *Evaluation Report on the Department's Unclassified Cyber Security Program 2011*, Department of Energy, October 20, 2011, http://energy.gov/sites/prod/files/IG-0856_0.pdf.
[6] Kundra, March 24, 2010.
[7] NIST, "Risk Management Framework Overview," 2010, http://csrc.nist.gov/groups/SMA/fisma/framework.html.
[8] NIST, "Select Step - Management Perspective," January 18, 2011, http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/select/qsg_select_management-perspective.pdf.

About CDW-G

CDW is a leading provider of technology solutions for business, government, education and healthcare in the US and Canada.

We're a 6,000-plus-member team with dedicated solution architects who help customers choose the right technology products and services to best meet their unique needs.

We offer expertise in designing customized solutions and assisting customers with the implementation and long-term management of those solutions such as virtualization, collaboration, security, mobility, data center optimization and cloud computing.

To learn more about security solutions from CDW-G, visit: http://www.cdwg.com/content/solutions/security

About McAfee

McAfee is the world's largest dedicated security company. Since our founding in 1987, we have had just one mission: to help our customers stay safe. We achieve this by creating proactive security solutions for securing your digital world.

Through our vigilance, we allow organizations to work, play and shop online more securely, no matter where they are or how they connect.

About the Government Business Council: Industry Insights

GBC: Industry Insights, a division of the Government Business Council and Government Executive Media Group, is dedicated to advancing the business of government through analysis and insight. GBC: Industry Insights partners with industry to share best practices with top government decision-makers, understanding the deep value inherent in industry's experience engaging and supporting federal agencies.

Contact Bryan Klopack, Director, at bklopack@govexec.com.