Guard data in government environments by implementing continuous diagnostics and mitigation

IBM Security offerings and services can help ensure federal compliance and reduce risks to sensitive—and often classified—information
Introduction

As government agencies continue to face increasingly hazardous IT security threats, they are constantly challenged to keep these threats at bay while protecting sensitive—and often classified—data. To help them address these challenges, the US Department of Homeland Security (DHS) has been developing a process for implementing continuous diagnostics and mitigation, an automated approach to evolving computer network and systems cyber security. This approach is designed to help government organizations understand the threats, data and assets that reside within their networks, relevant risks, and real-time mitigation techniques. The goal of continuous diagnostics and mitigation is to find and repair computer and network vulnerabilities in order to better secure systems to meet directives from the US Office of Management and Budget to follow National Institutes of Standards and Technology (NIST) Special Publications (SP) 800-137 and 800-53—requirements that enable government systems to be accredited to security controls across the enterprise. IBM Security Systems provides a security framework that outlines the domains within federal organizations’ environments and eases integration with NIST security requirements. This framework integration also enables the security and compliance automation required under the Federal Information Security Management Act (FISMA). In any case, the tighter, more automated security enabled by offerings found within the IBM Security Framework can ultimately enable federal organizations to more efficiently prioritize their IT resources.

Implementing continuous diagnostics and mitigation can end the practice of manual compliance reporting and combat system vulnerabilities and threats on a real-time basis. The US government envisions that employing the continuous diagnostics and mitigation approach will help enhance and automate existing continuous network monitoring capabilities; correlate and analyze critical security-related information; and improve risk-based decision-making at the federal enterprise level.

Assessing the federal security landscape

Although the number of security incidents reported by federal agencies continues to rise, the actual number of incidents is almost certainly greater because a large number of them go undetected. According to John Streufert, director of Federal Network Resilience, US Department of Homeland Security, malicious code attacks within federal agencies increased by 47 percent between 2008 and 2010. Moreover, since then the variety and sophistication of the threats and attacks have grown. Attackers have become smarter and more experienced, and are devoting ever-increasing resources to their efforts.

Compounding the growing numbers and types of threats are significant deficiencies in the security controls of federal information systems, which have resulted in pervasive vulnerabilities, undetected breaches, and unknown amounts of damage and theft. These vulnerabilities, identified by the federal Government Accountability Office (GAO) and other federal agencies, include weaknesses in the security of both financial and non-financial critical systems and data.
“Our success will be measured by how well we can articulate risk vulnerabilities and reduce our risks. Right now we have no way to measure this. Congress spends billions of dollars on cyber issues, and cannot currently measure the results.”


These deficiencies continue to place federal assets at risk for inadvertent or deliberate misuse; financial information at risk for unauthorized exposure, modification or destruction; sensitive intellectual property at risk for theft or vulnerable to espionage; and critical operations at risk for disruption.

Continuous Monitoring as a Service
The federal government Continuous-Monitoring-as-a-Service (CMaaS) strategy calls for expert services to implement, maintain and operate continuous diagnostics and mitigation tools within government organizations. CMaaS tasks are broken down into 11 task areas (TAs):

- TA-1: Provide order project management support
- TA-2: Continuous diagnostics and mitigation order planning
- TA-3: Support continuous diagnostics and mitigation dashboards
- TA-4: Provide specified tools and sensors
- TA-5: Configure and customize tools and sensors
- TA-6: Maintain data on desired state for continuous diagnostics and mitigation tools and sensors
- TA-7: Operate continuous diagnostics and mitigation tools and sensors
- TA-8: Integrate and maintain interoperability between continuous diagnostics and mitigation tools and legacy applications and data
- TA-9: Operate data feeds to and from installed dashboards
- TA-10: Training and consulting in continuous diagnostics and mitigation governance for departments, agencies and other requesting organizations
- TA-11: Support independent verification and validation and system certification

To align with CMaaS, IBM® Global Business Services® provides functional, strategic and managerial business consulting and support services to help execute the overall program aligned to four functional work areas

1. Tools architecture and integration
2. Tools configuration and customization
3. Tools operations and maintenance
4. CMaaS consulting and support

These four work areas are designed to help government agencies create or enhance their continuous diagnostics and mitigation/CMaaS capabilities guided by risk considerations. Effective continuous monitoring can be achieved by applying these four work areas— with consulting and governance-shaping continuous diagnostics and mitigation capabilities—in a manner that improves overall security posture. Without continuous improvement to the security architecture, the static architecture becomes more vulnerable as threats evolve. Continuous diagnostics and mitigation capabilities must be integrated into a continuous improvement program to keep pace with the evolving threat landscape. Continuous monitoring of security architecture provided through a continuous diagnostics and mitigation/CMaaS approach can support the cyber security oversight goal as described by the presidential cyber security coordinator. The presidential cyber security coordinator has also named continuous monitoring as one of three administration priorities to improve cyber security and the security of federal information systems.

1

2
FISMA 2.0 and continuous monitoring

The federal government is implementing FISMA 2.0 to help agencies develop risk-based IT security strategies that can better handle the threat of attacks. Instead of the annual, paper-based FISMA 1.0 exercises that yield instantly obsolete deliverables, FISMA 2.0—in the form of the Continuous Asset Evaluation, Situational Awareness and Risk Scoring (CAESARS) Reference Architecture released by the DHS in September 2010, NIST SP 800-37, and NIST SP 800-53—will require agencies to move beyond a checkbox approach to compliance by deploying continuous-monitoring enterprise solutions.

Exploring continuous diagnostics and mitigation

Continuous diagnostics and mitigation entails knowing one's environment—including hardware, software and their configurations—and finding known vulnerabilities and/or weaknesses in the government systems with the goal of dramatically lowering the number of incidents that currently result in data exfiltration. Further, this process enables organizations to centralize and automate their methods for discovering these flaws, thus allowing them to assign risk and remediation strategies across the federal enterprise. New technologies on today's smarter planet—where instrumented, interconnected and intelligent businesses collect, process, use and store more information than ever before—are designed to mitigate, upon discovery, many of these flaws and weaknesses to help improve governmental organizations' security postures.

Efforts to achieve continuous diagnostics and mitigation can also enable agencies to more efficiently gather information for their FISMA reporting requirements using deployed sensors and tools, which provide more accurate and timely results.

Three distinct phases of implementing information security continuous diagnostics and mitigation are currently being developed and considered by the DHS. While the first phase has tentatively been adopted and is already in use by some agencies, the other two are still in development and have not yet been enacted.

The DHS continuous diagnostics and mitigation/CMaaS implementation of tool functional areas (TFAs) is divided into three phases. Following is a list of their contents and expected deployment dates:

- **Phase 1: Current scope**
  - TFA-1: Hardware asset management
  - TFA-2: Software asset management
  - TFA-3: Configuration management
  - TFA-4: Vulnerability management

- **Phase 2: Expected Q2/government fiscal year (GFY) 2014**
  - TFA-5: Manage network access controls
  - TFA-6: Manage trust in people granted access
  - TFA-7: Manage security-related behavior
  - TFA-8: Manage credentialed authentication
  - TFA-9: Manage account access

- **Phase 3: Expected Q2/GFY 2015**
  - TFA-10: Prepare for contingencies and incidents
  - TFA-11: Respond to contingencies and incidents
  - TFA-12: Design and build in requirements
  - TFA-13: Design and build in requirements and policy in planning
  - TFA-14: Design and build in quality
  - TFA-15: Manage operations security

**Phase 1**

The first phase of continuous diagnostics and mitigation focuses on endpoint integrity of local computing devices and addresses four functional areas: hardware asset management, software asset management, vulnerability asset management and configuration management.

In Phase 1, the current scope of continuous diagnostics and mitigation aims to establish good cyber habits, essentially requiring users to perform basic functions to help keep their systems secure. These include maintaining an accurate inventory of both hardware and software, knowing their configurations, and managing vulnerabilities found in the organization's environment. These functions form the foundation of a strong security program, and these TFAs directly align to the activities...
IBM tools, including IBM Endpoint Manager, IBM Security QRadar® and IBM Security AppScan®, form the core of an approach that can be used to address these issues. The Endpoint Manager distributed architecture allows security teams and administrators to quickly understand what is on their network and what is under management (authorized), versus what is not (unauthorized). Unauthorized systems can be quickly identified and brought under management. Managed systems will be continuously assessed for compliance against agency policies for software, configuration settings and security posture. The ability for agents to automatically repair user changes to the desired state means that systems are continuously diagnosed and issues are mitigated automatically.

The IBM Security QRadar vulnerability management tool enables the rapid assessment of vulnerabilities in the environment. Distributed scanning minimizes impact to network resources while results are directly integrated into IBM QRadar Security Intelligence Platform. When combined with IBM X-Force® Threat Intelligence, legitimate vulnerabilities and exploited systems are quickly targeted for mitigation activities. One particular challenge is reducing the noise generated by endpoints and vulnerability tools, which is why it is critical to include security intelligence capabilities as part of Phase 1. The unique ability of QRadar to collect data streams from more than 500 security point products, and to normalize, categorize and correlate data, transforms noise into actionable intelligence that can be used by security teams and system administrators to quickly fix what is broken.

Security AppScan can assist with the vulnerability management aspect of Phase 1 through automated application security testing. By scanning applications, identifying vulnerabilities and generating reports with intelligent fix recommendations, Security AppScan helps government organizations efficiently discover and support remediation of application vulnerabilities.

Phase 2
During the second phase of continuous diagnostics and mitigation, government organizations will concentrate on the least privileges of employees associated with local computing environments and the infrastructure integrity of network and other devices. This includes identity management and links into information technology operations, especially as it relates to system access for data and applications.

Phase 2 moves from the basics, to managing identity and access, to networks and information systems in order to address the NIST SP 800-53r4 control areas of access control, identification and authentication, and system and communications protection. IBM continues to evolve its technology to meet the challenges of the ever-evolving threat landscape. The IBM Security portfolio provides a holistic strategy for managing information security with products and services ranging from its identity and access management suite to identity assessment, strategy, implementation and management services. For example, IBM Security Privileged Identity Manager is designed to secure, automate and audit the use of privileged identities to help reduce the overall number of privileged accounts. In addition, IBM Security intrusion prevention systems can help provide unmatched levels of performance, providing a wider breadth and depth of security. An agency’s investment in QRadar can be further realized as a part of this phase to help bring additional data into focus, forming a more complete perspective of security intelligence for government organizations.

Phase 3
The intent of the third phase of continuous diagnostics and mitigation will be to enable enclave boundary protection for devices and events, as well as event management for local computing environments, network environments and other infrastructure events.

Phase 3 will complete the implementation of all 15 TFAs by addressing the NIST SP 800-53r4 control areas of contingency planning, incident response, planning, system and services acquisition, and managing operations security. The holistic
IBM approach to security continues to provide tools and services to address these remaining areas, offering services that include assessment, architecture development, implementation and management. IBM Public Sector Cyber Security Assessment and Response specifically addresses contingency planning and incident response activities called out in this phase, including security infrastructure testing, application testing and source code analysis.

Recognizing that the security perimeter continues to collapse and that applications continue to grow in size, scope and complexity—with attackers continuing to match security strategies—government organizations must be able to prepare for, detect, contain, eradicate and recover from incidents. It is no longer a matter of if, but rather, when they will experience a security incident.

**Creating a business case for continuous monitoring**
Since January 2011, federal agencies have been required to report continuous-monitoring data to CyberScope on a monthly basis. However, continuous monitoring is not just another onerous compliance mandate for agencies to deal with. Rather, it can yield real benefits for both security and business managers. As Allan Paller, research director at the SANS Institute, noted in testimony to the US Senate Committee on Homeland Security and Governmental Affairs in June 2010, continuous monitoring, as already in place at the US Department of State, “causes rapid risk reduction with low overhead.”

Moreover, continuous monitoring makes IT security solutions more relevant to senior agency executives. The notion of scoring makes security more easily understandable—and makes it easy to compare the security status of one department unit or agency with another. It can help system managers and information-assurance managers have understandable, security-focused conversations with their executive management instead of the
mutually incomprehensible discussions that have so often occurred. Scoring also can resonate with senior executives more readily than the pleas of security managers clamoring for greater security investments.

Continuous monitoring can also enable agencies to gain the same operating efficiencies from IT investments that Fortune 500 companies have realized—something that is particularly relevant when agency budgets are trending downward.

One of the biggest criticisms of FISMA 1.0 has been that an agency could receive an “A” security rating but actually have significant security vulnerabilities and experience breaches. It could even have foreign adversaries actively penetrating its network and exploiting its assets. At the same time, an agency could get an “F” or “D” but possess a security posture superior to the agency that received an “A”—because of actions the failing agency had taken to identify and reduce its security vulnerabilities.

The scoring employed by FISMA 2.0 is designed to more accurately reflect the actual security environment of an agency. However, security is a process, not a destination, especially when the attackers from without and within are increasing, evolving and improving in sophistication. Likewise, the metrics for continuous monitoring will need improvement to better reflect the true state of the enterprise—which was not possible under FISMA 1.0.

**Understanding the IBM Security Framework**

The IBM approach to security is tailored to meet security requirements across multiple domains that integrate with one another. The IBM Security Framework is designed to ensure the right people have access to the right resources at the right times, while protecting critical data in transit and at rest; identifying emerging threats to support breach prevention, internal threats and remediation; and providing protection across all IT resources. This integrated approach to federal security includes appliances, software products and managed services, including technical, risk consultation and implementation services.
The IBM Security Framework aims to identify, combine and automate security controls across four risk domains—people, data, applications and infrastructure—to more effectively govern data. This framework increases security awareness and accuracy by detecting and preventing advanced and increasingly sophisticated threats, increasing visibility and awareness, and conducting comprehensive incident investigations. An interoperable framework eases the burden on administrators by simplifying risk management and decision-making, and by enhancing auditing and access capabilities. Effective risk management and an infrastructure governed by automated security controls are paramount to addressing governance, risk and compliance. The framework reduces cost and complexity by enabling fast deployment, increased value and lower total cost of ownership. These world-class capabilities are especially valuable in highly targeted government environments.

The IBM Security Systems division is based on three main tenets—intelligence, integration and expertise.

- **Intelligence:** Intelligence requires knowledge, information and the ability to analyze this information to reach conclusions. In the realm of organizational security, this translates to needing relevant network, infrastructure and external threat intelligence visibility, plus real-time correlation and security analytics to flag and remediate suspicious activities.
- **Integration:** Integrating the comprehensive IBM portfolio of security intelligence, X-Force research and asset core protection reduces vulnerability compromises and attackable weaknesses arising from cobbled-together security point products. It also eases deployment, collapses data silos for easier compliance reporting and improved security intelligence, reduces complexity, and lowers the cost of maintaining a strong security posture.
- **Expertise:** With more than 6,000 researchers, developers and subject-matter experts engaged in security initiatives, IBM operates one of the world’s broadest enterprise security research, development and delivery organizations. This powerful combination of expertise is made up of the award-winning X-Force research and development team—with one of the largest vulnerability databases in the industry—and includes 10 security operations centers, 10 IBM research centers, 17 software security development labs and the IBM Institute for Advanced Security with chapters in the United States, Europe and the Asia-Pacific region.

The IBM Security Framework offers an infrastructure that can help federal agencies dynamically manage the network while driving down costs, increasing security and risk posture, and automating compliance reporting. Information security groups within these agencies can increase their security management capabilities by:

- Identifying hardware assets attached to their networks
- Cataloging and managing software installed on hardware assets
- Enforcing department configuration management policies on these assets
- Scanning the network for vulnerabilities on the hardware and software attached to their network
- Managing endpoint and patch management of machines for security compliance
- Increasing visibility and situational awareness within multi-tenant environments

**Taking the IBM approach to continuous diagnostics and mitigation**

Based on many years of expertise in the industry and its comprehensive line of trusted security solutions, IBM can offer a measured and effective approach to helping government organizations implement continuous diagnostics and mitigation.
Phase 1—the one fully developed and partially adopted phase thus far—focuses on strengthening architecture effectiveness, enhancing critical data protection and bridging compliance gaps:

- **Security architecture effectiveness**: Focuses on rapidly assessing the vulnerabilities of the security architecture and the development of a prioritized roadmap to strengthen cyber protection; near-term activities plug security gaps and help meet congressional expectations; long-term activities integrate with the enterprise architecture and cyber analysis strategies.

- **Critical data protection**: Focuses on rapidly assessing the critical data architecture and the shortfalls in tracking and protecting critical data; helps improve continuous monitoring.

- **Compliance gaps**: Focuses on reducing IT security risk by rapidly assessing and remediating compliance gaps and establishing a roadmap to achieve continuous compliance; unsatisfactory inspector general reports and congressional reviews can impact budget situations and mission readiness.

The IBM Security Framework promotes effective results with full-scope government compliance coverage for Phase 1 of the continuous diagnostics and mitigation implementation, delivered through a variety of security solutions.

The IBM Security Framework maps to government controls to achieve effective security and compliance.
IBM QRadar Security Intelligence Platform
QRadar Security Intelligence Platform provides comprehensive and in-depth continuous monitoring of an organization's security status, and monitors and provides advanced security analytics for any changes that occur in order to help determine vulnerabilities, threats and breaches. It integrates previously disparate functions—including security information and event management (SIEM), risk management, log management, network behavior analytics, and vulnerability management—into a comprehensive security intelligence solution that fits the constrained budgets and resources of government agencies. By providing agencies with more intelligence, reduced complexity, high scalability, more automation, and out-of-the-box rules and reports, QRadar Security Intelligence Platform delivers a quick return on investment while meeting and exceeding the requirements of FISMA.

IBM Endpoint Manager
Endpoint Manager, built on IBM BigFix® technology, is a platform that can be used to help federal agencies achieve and maintain continuous diagnostics and mitigation. It enables federal IT organizations to continuously assess, remediate and enforce policy-based security compliance on all endpoints—even remote, roaming and mobile devices—regardless of operating system or location. This way, federal agencies can proactively mitigate vulnerabilities and secure critical assets from attack.

Endpoint Manager provides a single, unified approach to security compliance that enables federal agencies not only to rapidly determine which endpoints are at risk, but also to rapidly address exposed vulnerabilities. Using a comprehensive library of compliance settings, security teams can establish the baseline security configurations for all endpoints—and patch endpoints, as needed—without requiring multiple iterations for the patch to succeed. An intelligent agent placed on each endpoint continuously enforces security policies regardless of endpoint connectivity. And security teams use a central console to check on the compliance status of endpoints at any time.
IBM Endpoint Manager for Software Use Analysis addresses the DHS continuous diagnostics and mitigation hardware and software asset management requirements with network discovery, hardware and software inventory, and software use analysis capabilities. These capabilities integrate with and leverage the same platform and agent as those included in IBM Endpoint Manager for Security and Compliance. In fact, the entire Endpoint Manager family is designed to integrate and work together.

**IBM InfoSphere Guardium**

IBM InfoSphere® Guardium® provides proactive automated compliance capabilities in addition to complete continuous monitoring. This solution non-intrusively monitors, inspects and audits all SQL command activity for real-time data security and regulatory compliance. It enables users to deploy centralized controls for real-time data security and monitoring, fine-grained database auditing, automated compliance reporting, data-level access control, database vulnerability management, automatic discovery of sensitive data, and static and dynamic masking on demand.

**IBM Security AppScan**

Security AppScan is designed to quickly identify and repair application vulnerabilities early in the development lifecycle, improve communication across the organization, and save considerable time and costs throughout an organization’s journey to application security. It does so by combining static and dynamic analyses with hybrid analyses in order to more accurately correlate application security results.

Static analysis capabilities examine source code for potential vulnerabilities, and can be used earlier in the development cycle because they do not require a running application. Dynamic analysis capabilities test running applications by probing them in the same ways that hackers would. Using dynamic analysis results, it is easier to connect vulnerabilities to potential exploits. Hybrid analysis brings together dynamic and static analyses to correlate and verify the results. Issues identified using dynamic analysis can be traced to the offending line of code, while issues identified in static analysis can be validated with an external test. Additional AppScan features include client-side and run-time analysis. Client-side analysis analyzes code downloaded to the client, while run-time analysis places a run-time agent on the application machine and analyzes the application as it is being tested.

As the DHS continues to develop Phases 2 and 3 of implementing continuous diagnostics and mitigation, IBM has the experience and solutions necessary, and is prepared to also address these phases.

**Conclusion**

For years, federal agencies have complained that FISMA was a paper exercise that wasted scarce resources while producing a misleading and instantly outdated picture of an agency’s IT security state of affairs. FISMA 2.0 now requires agencies to carry out risk-based assessments on the basis of continuous monitoring of their IT infrastructures. Unlike many other mandates issued to government agencies, FISMA 2.0 goes a long way toward answering complaints and providing a framework for the agencies to measure, compare, assess and act upon their actual security conditions on an ongoing basis.

With continuous monitoring as a mandate, agencies need a solution that best meets federal requirements while meeting increasingly tight budgets, enabling them to do more with less. Now, agencies that already use IBM Security solutions such as Endpoint Manager or QRadar Security Intelligence Platform can easily leverage their existing assets to comply with the new mandates and cost-effectively implement continuous monitoring. Other agencies can adopt these capabilities, which easily integrate with other systems, applications and devices to meet the new mandates and stay within budget.
For more information
To learn more about IBM Security solutions, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

© Copyright IBM Corporation 2013
IBM Corporation
Software Group
Route 100
Somers, NY 10589
Produced in the United States of America
December 2013

IBM, the IBM logo, ibm.com, AppScan, BigFix, Global Business Services, Guardium, InfoSphere, QRadar, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.