Continuous Diagnostics and Mitigation demands, CyberScope and beyond

IBM BigFix streamlines federal security compliance with real-time insights and remediation

Highlights

- Meet Continuous Diagnostics and Mitigation (CDM) requirements with industry-leading technology
- Purchase with a CDM tools and continuous-monitoring-as-a-service (CMaaS) blanket purchase agreement (BPA)
- Deliver automatic reporting feeds to the CyberScope application
- Transition from CyberScope to CDM reporting systems when available
- Simplify compliance with FISMA reporting and data calls
- Support infrastructure compliance with SCAP, UCCGB/FDCC, DISA STIG, NIST directives and other federal security standards

While the Federal Information Security Management Act (FISMA) has been in place since 2002—requiring federal agencies not only to implement programs for securing IT infrastructures and information but also to report on the progress of their efforts—the compliance status and security posture of government networks are still in flux. The National Institute for Standards and Technology (NIST) has provided high-level guidance through various special publications, but agencies have struggled to implement this guidance in a cost-effective manner. Reporting, in particular, has largely remained a cumbersome, manual process, relying on spreadsheets and paper copies, requiring full-time staff months to assemble and analyze, and typically becoming out of date and obsolete before it is complete.

Today, the processes and standards for FISMA compliance have evolved. The Department of Homeland Security and the Department of Justice together have developed a reporting specification and application called CyberScope to handle manual and automated inputs of agency data for FISMA reporting. The use of CyberScope, which was intended as a way to provide the Office of Management and Budget and the White House with visibility into agency progress in moving from a paper-based system to one of continuous monitoring, became mandatory in November 2010 for IT operations across all federal agencies.

One challenge with CyberScope reporting, however, is that many agencies have visibility gaps in their infrastructure. Gathering accurate information and reporting on the security status of tens or hundreds of thousands of endpoints—from servers to desktops, laptops and specialized devices—can be an impossible task without the proper processes and tools. In addition, agencies also need a way to act on the data, rather than just gathering it to meet the mandate of FISMA compliance. That's why CDM programs have now put the emphasis on using the data gathered to help improve government-wide security and eliminate risk.

IBM® BigFix® can help. Already a significant provider of CyberScope data feeds, the solution delivers the infrastructure insight necessary to successfully conduct an endpoint security compliance initiative, automation to speed data gathering and reporting, and remediation capabilities to help agencies attain and remain in compliance with federal IT security and data privacy requirements. Currently, more than 1.4 million endpoints are under management using BigFix in the civilian government alone. BigFix is the industry-leading, real-time continuous monitoring and remediation solution that enables agencies to support real-time feeds of compliance status and risk—and meet the demands of current and future security regulations.

Delivering automated capabilities for continuous monitoring

The introduction of CyberScope is closely tied to a directive by NIST requiring that FISMA compliance be supported by agency-level programs for continuous infrastructure monitoring. NIST Special Publication 800-137 established a goal of near real-time insight into the security status of IT infrastructures so corrections can be made quickly when systems fall out of compliance. NIST data models use the underlying Security Content Automation Protocol (SCAP) primitives including common vulnerabilities and exposures (CVE), common configuration enumeration (CCE) and common platform enumeration (CPE) to produce data feeds from security management tools that can be sent directly into CyberScope.

BigFix delivers streamlined, automated capabilities for continuously monitoring and remediating security compliance. A BigFix deployment can deliver insight and control for an agency's endpoints, and it can feed data on endpoint configurations and compliance status directly into CyberScope and future applications such as the CDM Dashboard. The solution's ability to speed the migration from spreadsheet-based reporting to CyberScope reporting and beyond, along with its ability to reduce the time required for collecting and compiling data into reports, can yield rapid time to value and return on investment.

Now agencies can have a better understanding of the endpoints in their infrastructure coupled with an enhanced ability to protect them. BigFix provides visibility into endpoints across distributed infrastructures—including devices and software that might be in use without IT's permission, licensing that may need a true-up, and roaming devices that are only intermittently connected to the network. The ability of BigFix to continuously monitor devices, automatically bring them into compliance when needed and instantly report on status represents a major step toward reducing or eliminating security vulnerabilities in an agency's environment while simultaneously enhancing and simplifying compliance reporting.

Meeting federal requirements for security compliance

In an era in which federal agencies need to know about possible threats in minutes, not weeks, real-time knowledge of each endpoint's status and the infrastructure's overall security posture is invaluable. Putting together a program of comprehensive insight, remediation and reporting, however, can present significant challenges. An agency must:

- Initiate capabilities for insight, control and remediation of endpoints regardless of their type or location
- Provide continuous monitoring of the infrastructure to identify security issues as they occur—and remediate as funded in the federal IT budget
- Deliver reporting that proves compliance with cyber security and data privacy regulations under a number of standards, including not only FISMA and SCAP but also:
  - The US Government Configuration Baseline (USGCB), formerly known as the Federal Desktop Core Configuration (FDCC)
  - The Defense Systems Information Agency (DISA) Security Technical Implementation Guide (STIG)
  - Technical security controls in NIST Special Publication 800-53
  - The risk management framework described in NIST Special Publication 800-137
  - The patch management framework described in NIST Special Publication 800-40
  - Network inventory reports to satisfy FISMA data calls
- Determine processes and deploy solutions for helping ensure timely and accurate compliance and reporting
- Fund compliance operations in a way that delivers rapid time to value while leveraging existing infrastructure investments
- Achieve compliance in an efficient, modernized environment that supports both cost savings and environmental awareness

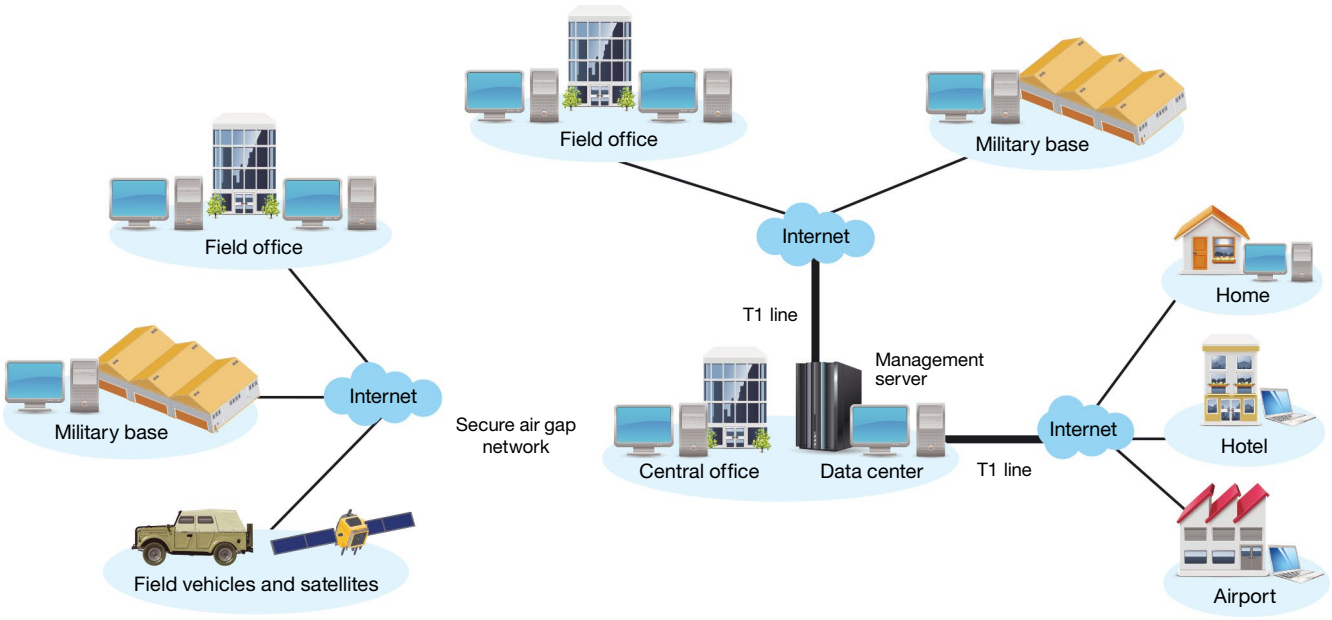
Addressing the challenges of ensuring security

The IT infrastructures that support government agencies today are large and complex, with ever-increasing demands for public access and transparency. Providing secure environments for information, as a result, requires a combination of flexibility, insight and power—the ability to adapt to varied and changing requirements, the knowledge of what needs protecting, and the ability to quickly remediate vulnerabilities that threats might otherwise exploit.

Cyber-attacks or any advanced persistent threats are a major concern for government agencies. In a recent Senate hearing, the current FBI director warned that cyber-attacks were likely to eclipse terrorism as the gravest domestic threat over the next decade.[1] At the same time, agencies are faced with threats from negligent or even malicious employees. With the increase of wireless endpoints and workers who expect anywhere, anytime access, the security of devices and software carried by mobile employees is in constant danger.

As a result, the cost and complexity for providing security and proving compliance have risen. Laptop computers, for example, must be patched just as thoroughly as computers in the office, despite being only occasionally connected to the agency network. Lack of insight and action can lead to major vulnerabilities and potential entry points into the agency for attackers.

IBM BigFix for government agencies



IBM BigFix delivers capabilities for continuous diagnostics, mitigation and compliance reporting across the entire federal infrastructure.

Delivering continuous diagnostics and mitigation

BigFix can meet these challenges. It provides targeted capabilities such as agnostic anti-malware management that supports security compliance by ensuring that solutions from a wide variety of vendors are supported, patched and maintained.

It also enables comprehensive automation capabilities with an intelligent agent-based approach that streamlines compliance management. The agent requires minimal system resources, eliminates manual processes and reduces IT staff workload. A unified approach to management that provides IT staff with only one console to learn further simplifies the solution and reduces costs.

With BigFix, a broad range of functions—from continuous monitoring, to compliance assessment, to endpoint remediation and regulatory reporting—all work in concert to ensure continuous enforcement of standards. The solution provides a comprehensive approach across diverse endpoints—spanning Microsoft Windows, UNIX, Linux and Mac OS platforms. Its management functions include asset discovery and inventory, software distribution, patch management, remote desktop control, software usage analysis and power management.

In an era in which situational awareness is critical, BigFix supports the modernization of computing environments, as new, more efficient systems are integrated into the infrastructure. And at a time when the federal government is focused on consolidating or eliminating redundant business applications, systems and services, BigFix can help rein in costs. The ability to manage hundreds of thousands of endpoints from a single server, automation that can reduce the need to expand IT staffs, agent-based remediation that reduces or eliminates system issues and help-desk calls, low network impact that reduces the need for upgrades, and the elimination of redundant management tools all contribute to a lower total cost of ownership, including overall reduction in IT and security management costs.

BigFix can provide savings that significantly offset the cost of the implementation. Support for asset and power management, coupled with tool consolidation, can reduce expenditures on license fees and power. Third-party tools for asset scanning, many of which only provide visibility without remediation capabilities, can be eliminated by BigFix. Reduction in power usage averaging between USD30 and USD50 per year per desktop computer, based on the experience of IBM clients, can save millions of dollars annually for a large agency. Software usage monitoring, or software metering, allows the agency to determine exactly how many copies of an application are being used and how often, to better control and save money on licensing agreements.

Why IBM?

With IBM BigFix, federal agencies have the insight and control they need to implement a robust Continuous Diagnostics and Mitigation program. Streamlined, automated capabilities for continuously monitoring and remediating endpoint security compliance can simplify compliance with FISMA reporting requirements. With more than 1.4 million endpoints in civilian government alone currently running IBM BigFix, the solution is a proven answer for enforcing compliance and proactively minimizing risk.

For more information

To learn more about IBM BigFix, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security/bigfix

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

Please Recycle

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, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, 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 ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

[1] Spencer Ackerman, "Cyber-attacks eclipsing terrorism as gravest domestic threat—FBI," *The Guardian*, November 14, 2013. http://www.theguardian.com/world/2013/nov/14/cyber-attacks-terrorism-domestic-threat-fbi

WGS03061-USEN-00