Real time endpoint compliance for Continuous Diagnostics and Mitigation

IBM Endpoint Manager, built on BigFix Technology, is the leading enterprise cybersecurity solution helping governments combat threats and eliminate vulnerabilities.
How do you secure your network?

Major initiatives such as DHS Continuous Diagnostics and Mitigation (CDM) and developing National Institute of Standards and Technology (NIST) guidelines, including continuous monitoring and CyberScope, support the acquisition and deployment of solutions that will continuously monitor, manage and mitigate vulnerabilities. With current budgetary constraints in mind, it's crucial that these solutions provide a rapid return on investment with substantial resource recovery.

The proven sentry: IBM Endpoint Manager, built on BigFix technology
IBM Endpoint Manager, built on BigFix® technology, has been validated by NIST as conforming to the Security Content Automation Protocol (SCAP) and its component standards. It provides a flexible automation framework for effective continuous monitoring and management that advances the current paradigm of disparate and non-integrated assessment and remediation systems from multiple vendors.

This solution:
- Is currently available through the GSA/DHS CDM CMaaS BPA
- Offers a breadth of functionality that plugs the gaps of older legacy security tools that weren't designed to keep up with the frequency, complexity and volume of evolving threats
- Continuously scans and enforces policies against security configurations and vulnerabilities
- Reduces vulnerability management and patching cycles to less than a day
- Enables the detection and mitigation of zero-day exploits across complex distributed networks in minutes
- Is massively scalable—controls up to 250,000 endpoints with a single management server
- Uses less than 2 percent of the central processing unit (CPU) on average, minimizing system impact

The United States is fighting a continuous cyber war against adversaries of all types, including nation states, terrorist groups, criminal organizations, and other nefarious actors. The US is faced with an ever-increasing multitude and sophistication of cybersecurity threats, which was demonstrated when foreign adversaries compromised US Federal Weapons System programs during 2013. Federal departments and agencies, along with elements of the national critical infrastructure, must take a proactive approach to information and network security. Continuously emerging threats have prompted federal oversight organizations such as the White House Office of Management and Budget (OMB), the Defense Information Systems Agency (DISA), and the US Cyber Command (USCYBERCOM) to implement policies requiring more frequent submission of reports that demonstrate the effectiveness of department and agency cybersecurity operations.
Major aspects of continuous monitoring addressed by IBM Endpoint Manager are as follows:

- Continuous monitoring requirements will evolve to continuous compliance and management.
- Continuous monitoring requires 24/7 real-time knowledge and situational awareness of network security posture.
- Federal Information Security Management Act (FISMA) reporting is advancing, requiring automated digital reporting through CyberScope with ever-increasing report frequency.

IBM Endpoint Manager fully supports implementation and integration of these aspects of continuous monitoring into IT policies and operational processes.

Continuous monitoring: Aspects that must be addressed

Continuous monitoring is a common catchphrase within the industry and among agencies, which can lead to misperceptions of the purpose of a continuous monitoring program.

Figure 1: Development Stages for Continuous Monitoring.

How do you secure your network?

locally on managed systems, tying specific actions to measurable qualities of the system, such as network range and connectivity type, software loads, or currently logged-in users.

With over 600 properties measured out of the box and the ability to easily create custom properties, network managers can use IBM Endpoint Manager to create granular situation-aware security policies, such as restricting network access when systems are out of compliance, or shutting down specific services when systems are connected to public WiFi. This capability ensures enforcement of security policies both on and off of government networks, maximizing security posture and reducing risk as IT becomes increasingly mobile.

CyberScope reporting: Ever-increasing requirements.
The Department of Homeland Security and the Department of Justice have co-developed a reporting specification and application called CyberScope to handle manual and automated inputs of agency data for FISMA reporting. The use of CyberScope was intended as a way to provide the OMB

“Continuous management helps ensure ongoing situational awareness and control of the security of systems across the organization and ongoing knowledge of associated threats and vulnerabilities, despite inevitable changes to organizational information systems and their environments of operation.”

— NIST Special Publication 800-137, December 2010

Situational awareness: Maximizing security posture and reducing risk
IBM Endpoint Manager is the industry-leading solution for achieving situational awareness at macro and micro levels across complex and distributed computing networks. Information reported by IBM Endpoint Manager agents to administrators and analysts is current within 15 minutes, ensuring network-wide awareness of security posture and risk. Current and accurate information enables network managers to make proper and informed decisions to support normal operations and deal with incidents or exposures on the network.

At the micro level, IBM Endpoint Manager agents also enable situational awareness by enforcing policies and taking actions locally on managed systems, tying specific actions to measurable qualities of the system, such as network range and connectivity type, software loads, or currently logged-in users. With over 600 properties measured out of the box and the ability to easily create custom properties, network managers can use IBM Endpoint Manager to create granular situation-aware security policies, such as restricting network access when systems are out of compliance, or shutting down specific services when systems are connected to public WiFi. This capability ensures enforcement of security policies both on and off of government networks, maximizing security posture and reducing risk as IT becomes increasingly mobile.
and the White House with visibility into agency progress in moving from a paper-based system to one of continuous monitoring. It became mandatory in November 2010 for IT operations across all federal agencies. However, the introduction of CyberScope has provided only partial relief. In fact, shortly before becoming a rule, a federal survey found that only 15 percent of CIOs at major federal agencies had even tried it. Due to visibility and technology gaps, the rate of CyberScope adoption may be understandable.

**Meeting the increasing 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. However, putting together a program of comprehensive insight, remediation and reporting 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 them as funded by the federal IT budget.
- Deliver reporting that proves compliance with cybersecurity and data privacy regulations under a number of standards, including not only FISMA and SCAP, but also:
  - The U.S. Government Configuration Baseline (USGCB)
  - The DISA Security Technical Implementation Guide (STIG)
  - Technical security controls in NIST Special Publication 800-53
  - The Risk Management Framework (RMF) described in NIST Special Publication 800-37
- Determine processes and deploy solutions for ensuring 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

**The IBM Endpoint Manager paradigm shift**

Many solutions that lay claim to continuous monitoring support are based on the old paradigm for vulnerability management that implements disparate technologies for assessment and remediation. Typically, this involves a lighthouse scanning approach to vulnerability assessment, with results dumped into a spreadsheet and handed off to the system’s administration team for remediation either manually or through a third-party tool. This repetitive scan-and-patch approach has left agencies with major compliance gaps and little time to investigate the implementation of a true continuous monitoring solution to feed CyberScope. Considering today’s threat environment and the amount of malware released, this approach to security management falls dangerously short.

IBM Endpoint Manager represents a change in this paradigm, eliminating the antiquated manual scan-and-patch approach and integrating the assessment and remediation processes into a single solution. Already a significant provider of CyberScope data feeds, the solution delivers the infrastructure insight necessary to successfully conduct an endpoint security compliance initiative, the automation needed to speed data gathering and reporting, and the remediation capabilities required to help agencies attain and remain in compliance with federal IT security and data privacy requirements.
How do you secure your network?

Now is the time to act

Continuous monitoring is not simply the latest Federal trend or catch phrase—it is a necessary mandate to ensure business continuity and federal IT security compliance within the government and national critical infrastructure. Ultimately, federal agencies need to implement a continuous management solution to meet the requirements of future and current mandates, but more importantly, to secure our nation’s networks from cyber threats compromising national security.

IBM Endpoint Manager, built on BigFix technology, is the clear solution for federal agencies, delivering real-time, continuous management across heterogeneous operating system environments, enabling situational awareness, simplifying federal security compliance requirements, and protecting our nation’s front lines throughout the cyber battlefield.

Reports from the field

More than 1.4 million endpoints are under management using IBM Endpoint Manager in the civilian government alone; users include the Department of Justice, the Department of Agriculture, the Department of Veterans Affairs, the Department of Homeland Security, NASA, the Department of Energy, the National Institutes of Health, and federal courts.

IBM Endpoint Manager provides the cyber-security technology necessary to thwart attackers and mitigate risks on the current battlefield. CyberScope reporting and rapid installation times (days instead of weeks or months) provide immediate value and return on investment.

Continuous Monitoring From the Front Lines of Cybersecurity: A Department of Justice Case Study

Hear Dave Otto, formerly of the Department of Justice CIO Office, describe their use of IBM Endpoint Manager, built on BigFix technology, for continuous monitoring. [http://event.on24.com/r.htm?e=312918&s=1&k=9A92D941188F6109EF63656F14F5BE2E](http://event.on24.com/r.htm?e=312918&s=1&k=9A92D941188F6109EF63656F14F5BE2E)

“In one survey, 74 percent of government IT executives said they expected a foreign-based cyber attack, including viruses, malware or hacking, in the next 12 months.”


Now is the time to act

Continuous monitoring is not simply the latest Federal trend or catch phrase—it is a necessary mandate to ensure business continuity and federal IT security compliance within the government and national critical infrastructure. Ultimately, federal agencies need to implement a continuous management solution to meet the requirements of future and current mandates, but more importantly, to secure our nation’s networks from cyber threats compromising national security.

IBM Endpoint Manager, built on BigFix technology, is the clear solution for federal agencies, delivering real-time, continuous management across heterogeneous operating system environments, enabling situational awareness, simplifying federal security compliance requirements, and protecting our nation’s front lines throughout the cyber battlefield.
References

1. Most organizations deploy IBM Endpoint Manager with only 1-4 dedicated servers.


