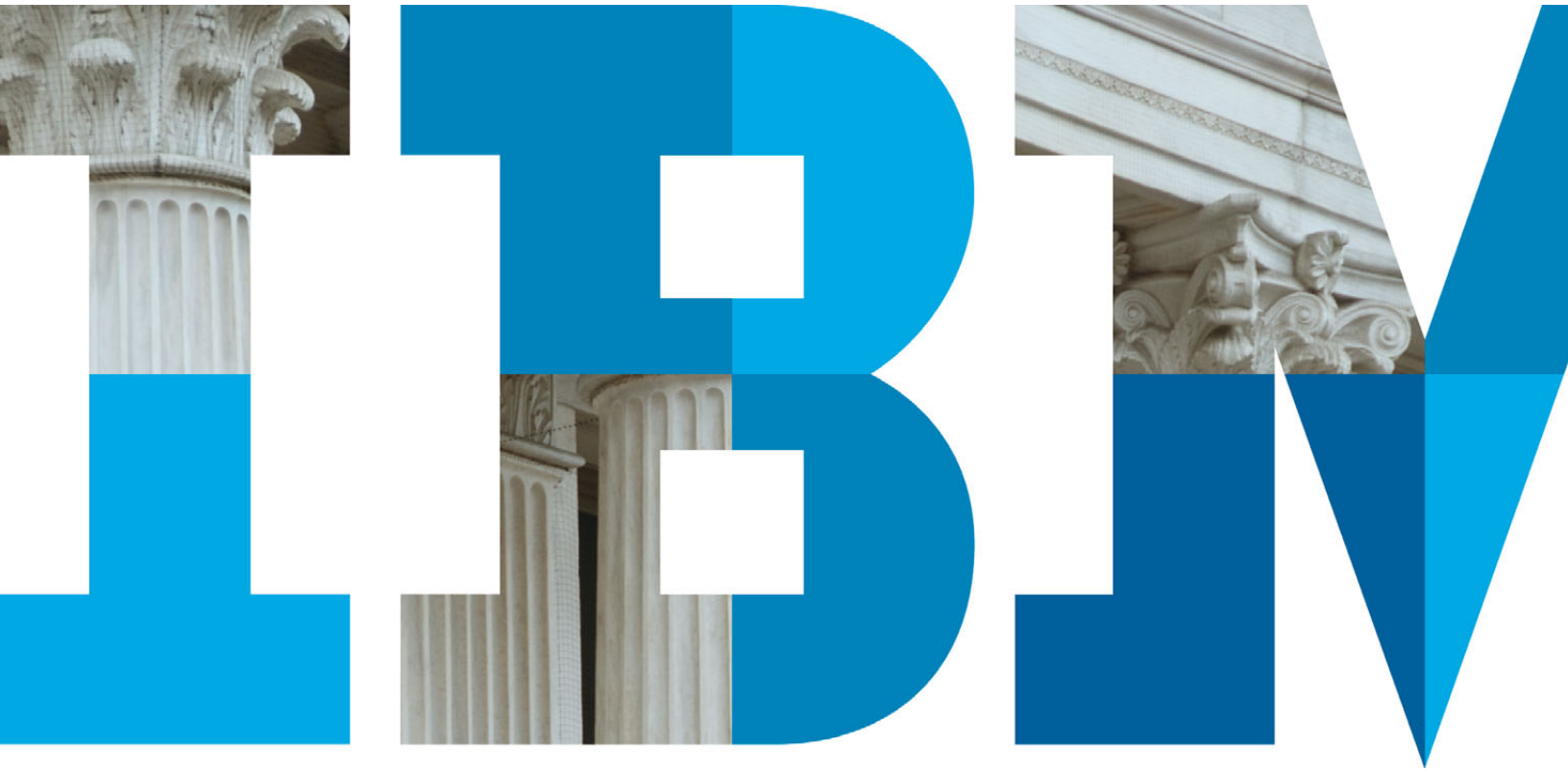
IBM Software
Thought Leadership White Paper

November 2011

Your network is the new battlefield

Combat cybersecurity threats with IBM Tivoli Endpoint Manager, built on BigFix technology



Contents

2 Introduction

2 The proven sentry: IBM Tivoli Endpoint Manager, built on BigFix technology

3 Continuous monitoring: Aspects that must be addressed

4 Meeting the increasing federal requirements for security compliance

4 The IBM Tivoli Endpoint Manager paradigm shift

7 Now is the time to act

8 For more information

Introduction

The United States is faced with an ever-increasing multitude and sophistication of cybersecurity threats. 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) and the Defense Information Systems Agency (DISA) to implement policies requiring more frequent submission of reports that demonstrate the effectiveness of department and agency cybersecurity operations.

Major initiatives 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 Tivoli Endpoint Manager, built on BigFix technology

IBM® Tivoli® 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 nonintegrated assessment and remediation systems from multiple vendors.

This solution:

- 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 two percent of the Central Processing Unit (CPU) on average, minimizing system impact.
- Delivers proven rapid time-to-value, a low cost of entry, and a low total cost of ownership—the minimal hardware, services, and human resources requirements, and potential power management and software license savings can provide an opportunity to self-fund the entire IBM Tivoli Endpoint Manager investment.
- Is the only CyberScope-ready solution on the market that provides a continuous compliance and management solution across operating systems (Microsoft Windows, UNIX, Linux, and Mac OS) and mobile devices, minimizing the need for future investment when reporting requirements become real-time.

Continuous monitoring: Aspects that must be addressed

Continuous monitoring is a common catch phrase within the industry and among agencies, which can result in misperceptions of the purpose of a continuous monitoring program.

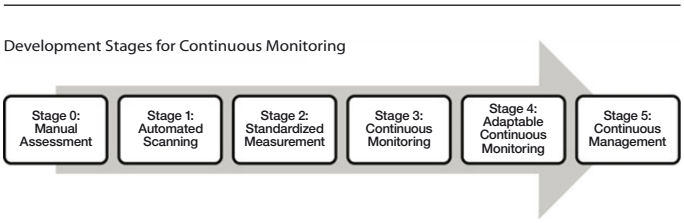
Major aspects of continuous monitoring addressed by IBM Tivoli Endpoint Manager are as follows:

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

Continuous management: Evolving beyond continuous monitoring

From a technical and standards-based perspective, NIST has proposed a maturity model for continuous monitoring consisting of five development stages. These stages illustrate the evolution from a manual to an automated approach, as well as a transition from static to adaptive activities. The most evolved stage is continuous management, or the continuous assessment and remediation of vulnerabilities and out-of-compliance configuration items.



Five development stages for continuous monitoring—the evolution from a manual to an automated approach (Source: NIST[1]).

IBM Tivoli Endpoint Manager provides comprehensive automation capabilities that streamline federal security compliance and scales to support continuous management of over 250,000 systems with minimal infrastructure investment. Its continuous management capabilities enable ongoing compliance assessment and enforcement with remediation first-pass success rates in the 95 percent range. This means administrators can patch and remediate configurations and deliver reporting that proves compliant with cybersecurity and data privacy regulations (under a number of directives and federal security standards) across 95 percent of their distributed computing networks. All this happens with the click of a mouse—significantly reducing workload which would traditionally net much lower success.

Situational awareness: Maximizing security posture and reducing risk

Continuous monitoring 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.[2]

IBM Tivoli Endpoint Manager is an industry-leading solution for achieving situational awareness at macro and micro levels across complex and distributed computing networks. Information reported by IBM Tivoli 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 to deal with an incident or exposure on the network.

At the micro level, IBM Tivoli 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 Tivoli Endpoint Manager to create granular situation-aware security policies, such as restricted network access, when systems are out of compliance, or by shutting down specific services when systems are connected to public Wi-Fi. 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 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, but the introduction of CyberScope has provided only partial relief. In fact, shortly before becoming the rule, a federal survey found that only 15 percent of CIOs at major federal agencies had even tried it.[3] 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. 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 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), formerly known as the Federal Desktop Core Configuration (FDCC).
  - 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 Tivoli 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 for

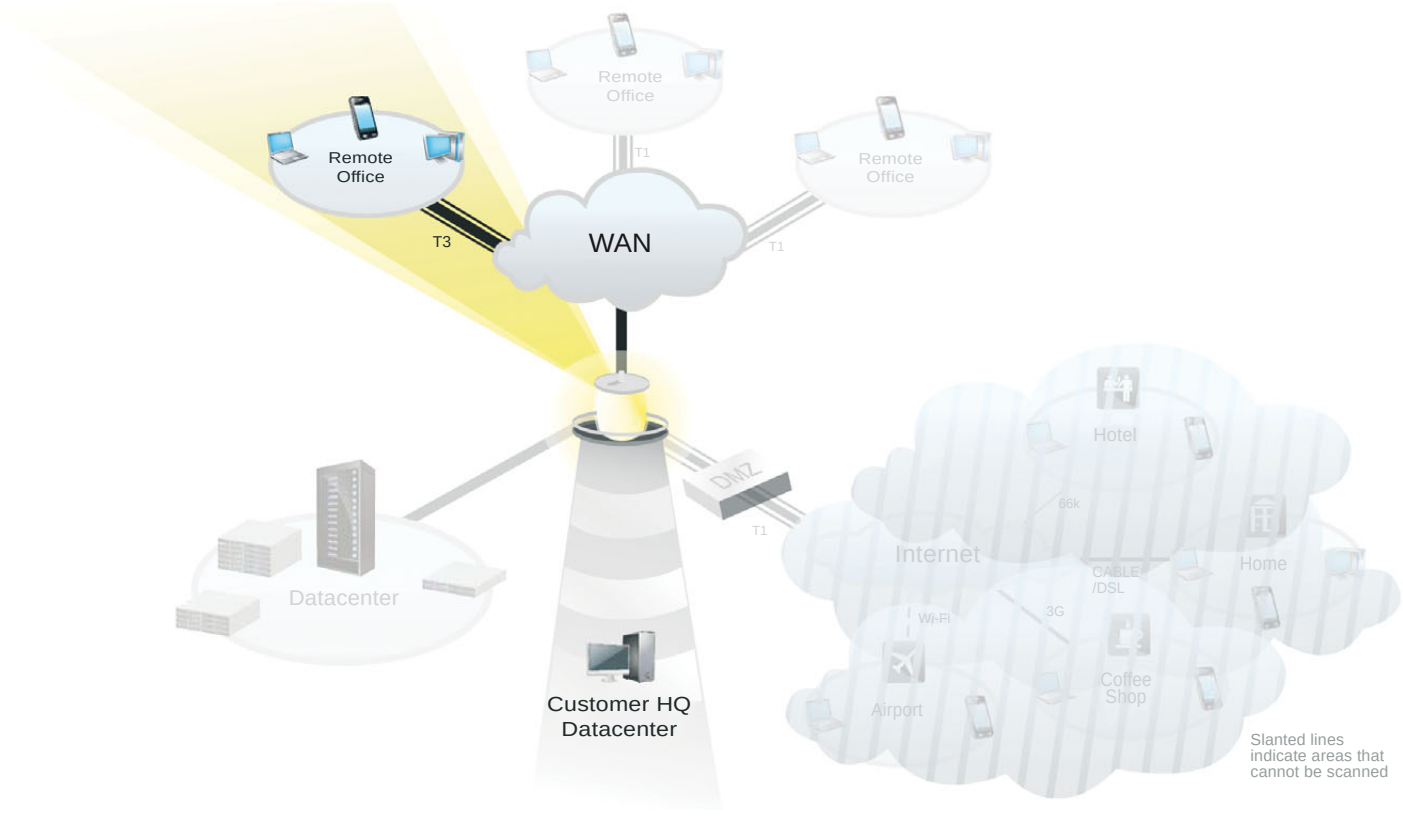
vulnerability assessment with results dumped into a spreadsheet and handed off to the system's administration team for remediation either manually or through a third-party tool. This repetitive scan-and-patch approach has left agencies with major compliance gaps and little time to investigate the implementation 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.

Traditional Vulnerability Assessment

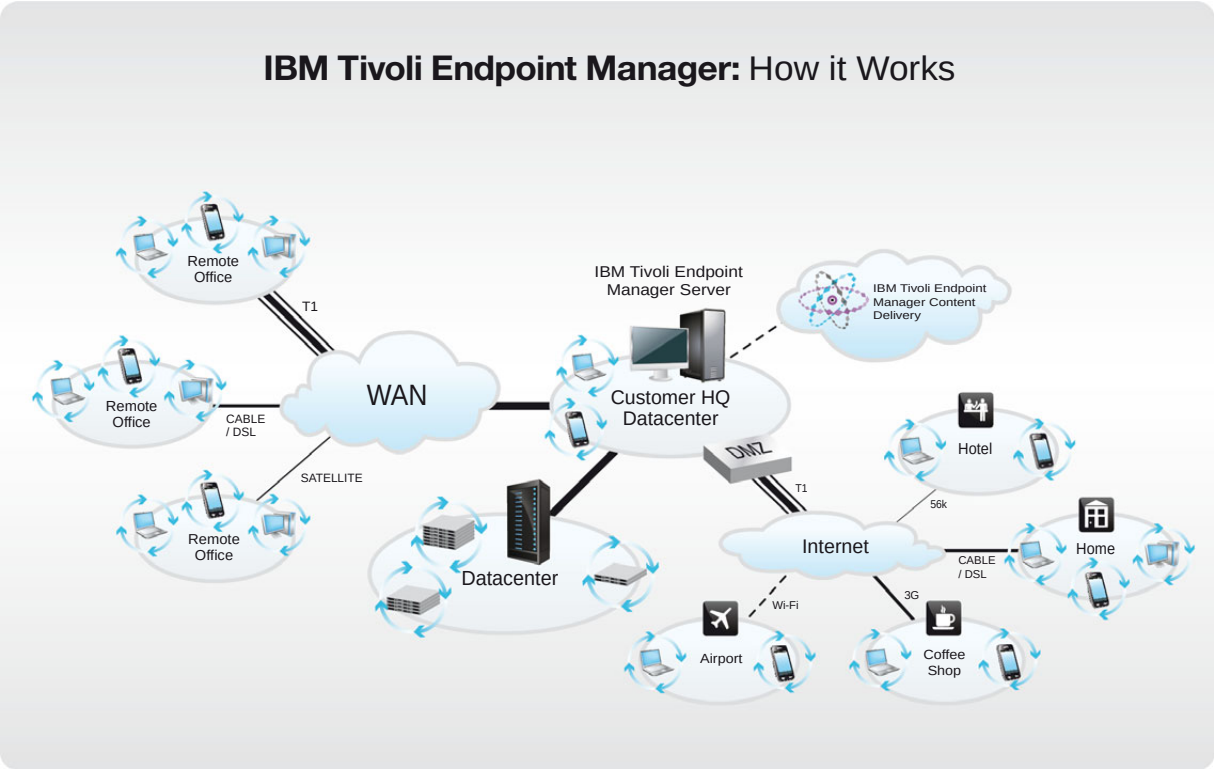
Vulnerabilities:

- Lighthouse vulnerability scans negatively impact networks while providing an outdated view of security posture.
- "Scan-and-patch, scan-and-patch" spreadsheet approach is inefficient and time consuming.
- Widespread vulnerability gaps exist leaving federal agencies and departments open to exposure.

Traditional Vulnerability Assessment



Legacy vulnerability management practices leave widespread gaps that open federal networks to exploitation.



Tivoli Endpoint Manager provides continuous compliance and real-time situational awareness, thereby eliminating threat vectors.

IBM Tivoli Endpoint Manager represents a change in this paradigm, by 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, 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.

Tivoli Endpoint Manager: How it works

Key Benefits:

- **Continuous assessment and enforcement of policies and mitigation of vulnerabilities.**
- **Threat vectors eliminated along with spreadsheet based patch management.**
- **Real-time situational awareness across complex global networks.**
- **Manage virtually any operating system while consolidating cybersecurity and systems administration functions into a single console.**

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.[4]

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 Tivoli Endpoint Manager, built on BigFix technology, is the clear solution for federal agencies—delivering real-time, continuous management across heterogeneous operating system environments. It enables situational awareness, simplifies federal security compliance requirements, and protects our nation's front lines throughout the cyber battlefield.

Reports from the field

More than 1.4 million endpoints are under management using IBM Tivoli Endpoint Manager in the civilian government alone; users include the Department of Agriculture, the Department of the Army, the Department of the Air Force, the Department of Energy, Independent Agencies, the Department of Justice, the Department of Labor, the Department of Veterans Affairs, and the Department of Health and Human Services.[5]

IBM Tivoli Endpoint Manager provides the cybersecurity technology necessary to thwart attackers and mitigate risks on the current battlefield. CyberScope reporting and the rapid installation time of days—not 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 from the Department of Justice CIO Office describe its use of IBM Tivoli Endpoint Manager, based on BigFix technology, for continuous monitoring:
https://www.ibm.com/services/forms/signup.do?source=swg-isms-DOJ-webcast-Fed

For more information

To learn more about the IBM Tivoli Endpoint Manager family of products, contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com**/tivoli/endpoint

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

Contributing Author

Joshua G. Stegall, CISSP, IBM Tivoli Endpoint Manager Technical Sales Specialist. Joshua Stegall has over ten years of information security and networking sales and consulting experience. Joshua has worked with multiple verticals including telecommunications, managed service providers, systems integrators and the US Federal government.

[1] National Institute of Standards and Technology (NIST), "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model," March 21, 2011. Available online at http://scap.nist.gov/events/2011/cm_workshop/presentations/pdf/MELL%20-%20CAESARS%20FE%20Ref%20Model%2020110318.pdf

[2] NIST Special Publication 800-137, December 2010, page 6. Available online at http://csrc.nist.gov/publications/drafts/800-137/draft-SP-800-137-IPD.pdf

[3] Waterman, Shaun, "Federal IT chiefs slow to try out CyberScope: Many wary about monitoring system," *The Washington Times*, October 3, 2010. Available online at http://www.washingtontimes.com/news/2010/oct/3/federal-it-chiefs-slow-to-try-out-cyberscope

[4] Government Technology Research Alliance (GTRA), "Cyber Security: Solving an Ever-Changing Equation," 2011. Available online at http://www.gtra.org/knowledge-center/1091-cyber-security-solving-an-ever-changing-equation

[5] BigFix, Inc., "BigFix FDCC Solution: 500,000 Federal Government Endpoints and Counting; Establishes Lead as Most Widely Adopted FDCC and Green IT Compliance Solutions," Press Release, June 29, 2009. Available online at http://www.marketwire.com/press-release/bigfix-fdcc-solution-500000-federal-government-endpoints-and-counting-1219667.htm

IBM Corporation
Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
November 2011

TIW14113-USEN-01