IBM Security
Thought Leadership White Paper

July 2015

Maintaining continuous compliance—a new best-practice approach

IBM BigFix provides endpoint auditing and management for distributed environments

Contents

Introduction

Organizations of all sizes and types put policies, processes and procedures in place to try to meet the endpoint compliance requirements of internal operations, industry bodies and government regulations.

But does a traditional endpoint management approach get them to the level of compliance they need? And more importantly, does it keep them there?

In most cases it doesn't do either. And the reason is simple. A traditional approach can't keep endpoints continuously compliant with regulations or protected from threats. To achieve continuous compliance, organizations need to replace traditional processes based on legacy technologies, outgrown assumptions and siloed IT operations with a new best-practice approach and new, innovative technology.

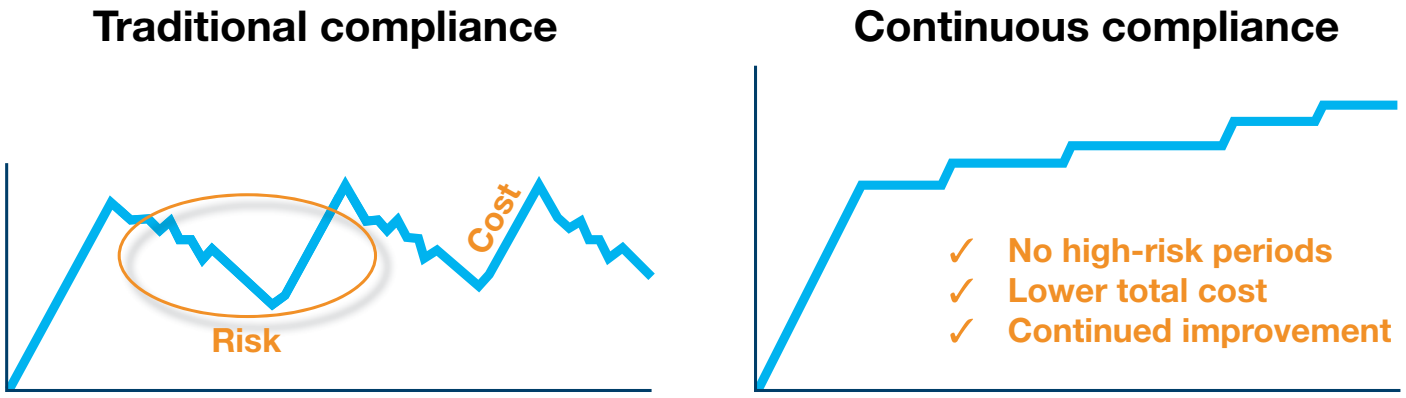
Organizations need to ensure that compliance assessment and remediation work together—because assessment without remediation, as often happens in traditional practice, is of limited or no value. They need to reduce the time they are exposed to vulnerabilities. And they need to conduct compliance operations in real time—compared to the weeks or even months that some processes take—so assessments are not obsolete before the remediation process has even begun.

An ever-changing landscape with valleys of vulnerability

For many organizations, the path to compliance is like hiking the peaks and valleys of a mountain. You walk up. You slide down. You walk up. And at the end of the day, you may or may not be any higher than where you started.

Achieving compliance should be more like climbing stairs. You step up. You stay level. You step up again. You don't lose ground. And with every step, you come closer to achieving or exceeding your goal.

Security and compliance are more important than ever today, as distributed environments constantly add new points of vulnerability. Mobile computing spreads vulnerability all over the map, and distributed endpoints have made simplified, centralized control more a wish than a reality. Slipping into a valley of noncompliance and vulnerability exposes organizations to both regulatory and security risks, with effects ranging from fines and sanctions levied by regulators to interrupted processes, compromised data and financial loss. What is needed is a best-practice approach that enables the organization to continuously demonstrate compliance while enhancing security.



A stair-step continuous-compliance model enables the organization to avoid the risks and cyclical costs of traditional techniques.

Protection and control at the organization's new perimeter

For many organizations, the quantities and varieties of endpoints—including servers, desktops, laptops, mobile devices, and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks—reach into the hundreds or even hundreds of thousands. Protecting and managing endpoints is a significant challenge because the perimeter of the organization, outside of which threats lurk, is no longer neatly defined by the corporate firewall. Organizational networks are becoming more porous all the time due to business demands for connectivity with external partners, suppliers and customers. The perimeter, therefore, is the endpoint itself, wherever it goes. And the endpoint's compliance status can change anywhere and at any time.

Organizations today have to meet country-specific data protection acts and data privacy laws, such as the EU Data Protection Directive. They have to comply with regulations such as Basel III, the Federal Information Security Management Act (FISMA) or the newer CyberScope, the Health Insurance Portability and Accountability Act (HIPAA) including the Health Information Technology for Economic and Clinical Health (HITECH) Act updates, the Payment Card Industry Data Security Standard (PCI DSS) or the Sarbanes-Oxley Act (SOX). Additionally, they have to keep up with internal security requirements. And as a result, many organizations often find themselves reactively addressing compliance requirements on a project-by-project basis instead of using an ongoing, strategic approach. When processes are reactive, compliance becomes a temporary achievement—not the continuous state that business and regulators require. As compliance requirements become more pervasive and computing environments become increasingly distributed, organizations need a way to become more efficient, effective and collaborative in their compliance efforts.

Disconnected processes for assessment and remediation

The challenge typically begins with the historical compliance model that divides management between two IT teams: security and operations. In the most common scenario, the security team sets policy, and then assesses the environment to determine if endpoints meet those policies. The operations team is responsible for implementing any changes necessary to bring endpoints into compliance, but this is typically secondary to ensuring that endpoints are up and running.

Challenges grow greater in the gaps that often occur between the assessment and remediation steps—particularly when each team operates within its own silo of processes and tools. Disconnected processes prevent organizations from breaking the cycle of peaks and valleys of compliance and vulnerability. Consider the typical compliance process:

1. The security team develops compliance policies.

2. The security team runs an assessment tool (or tools) against that policy.

3. The security team forwards discovered policy violations to the systems and desktop administration teams.

4. The operations team makes corrections as workload allows, typically covering one policy violation at a time, one endpoint at a time. Remediation of noncompliance may or may not be possible, particularly at scale. The operations team also typically uses remediation tools that are different from the tools used for assessment.

5. Following remediation, users often make changes to their machines, in some cases undoing corrections and causing endpoints to fall out of compliance again—a state known as "compliance drift."

6. The process begins again with Step 2 according to a predetermined assessment schedule. Due to the time and effort required, many organizations assess infrequently—monthly, quarterly or even yearly.

These disjointed steps make it clear that regardless of how effective individual assessment or remediation tools might be, operating them within silos makes it nearly impossible to address risk effectively. Even though the organization may be compliant with individual control requirements at a given point in time, the lack of unified processes may actually decrease security due to conflicting reports about how many endpoints an organization has, whether or not a particular endpoint is really patched, and conflicts between the tools' endpoint agents.

How do silos create problems?

Lack of coordination within the compliance process can cause significant challenges to achieving compliance in an efficient, timely and cost-effective manner. Here are just a few indicators that siloed assessment and remediation processes are operating ineffectively:

- Security and operations teams have different inventory counts for endpoints in the organization.
- There is a lag of weeks—or even months—between discovering a noncompliant endpoint and remediating or approving an exception request for that endpoint.
- The systems audit manager cannot name anyone who performs remediation work.
- The audit team is not confident that all in-scope endpoints are being assessed.
- The assessment team never receives requests for exceptions, indicating a communication breakdown or lack of follow-through on findings.
- The configuration baselines and standards have not been reviewed with the system administrators to identify potential conflicts.

Dangerous peaks and valleys on the path to compliance

The traditional approach for assessing, measuring, evaluating and remediating compliance issues by conducting a series of point-in-time audits can result in a number of issues, including:

- **Lack of visibility:** Siloed approaches that use different tools across server, desktop and operating system platforms lack comprehensive visibility. They produce results that must be reconciled and integrated in order to be useful. While legacy compliance efforts and tools focused primarily on centralized servers, today's focus must provide visibility across distributed endpoints, which are the most susceptible to attack.
- **Inconsistent information:** The different tools utilized in siloed processes often provide differing information about patching, malware signatures and configurations. The result? Accurate compliance reporting becomes a near-impossibility. Even if the information can be reconciled, putting it to use often takes so long that the original assessment data is obsolete by the time remediation occurs, requiring yet another assessment to address current compliance issues.
- **Increased costs:** At the simplest level, a siloed approach requires more tools and more staff to run tools, translating into higher costs. The frequent need for repeated audits in a siloed environment to ensure that findings are addressed adds still more cost, extends exposure times and increases the vulnerability of noncompliant endpoints.

Ultimately, point-in-time audits, siloed approaches and delays between assessment and remediation extend the "time to protection" during which endpoints are potentially at risk. An approach that enables continuous compliance, however, can reduce those times of risk so that the organization is more secure in its protection.

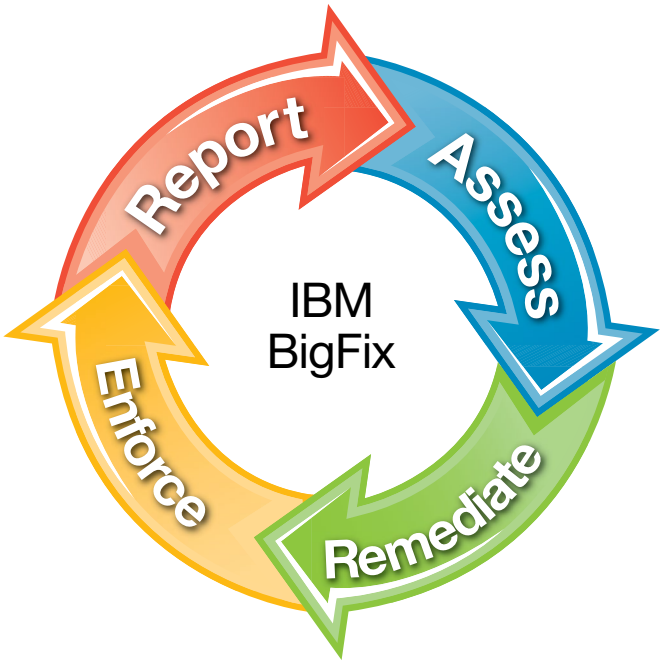
The pressing need for new processes and tools

The compliance challenges presented by siloed approaches demonstrate clearly that new processes and a unified solution are necessary to meet the distributed environment's compliance requirements and its operational need to maintain centralized visibility and control.

When a security breach occurs, organizations must be prepared with tools that not only rapidly determine which endpoints are at risk, but also rapidly address the vulnerabilities exposed. Even in a stable computing environment when disaster is not looming, the more tools an organization uses, the longer it takes to fix vulnerabilities discovered in the assessment phase, especially when the tools are disparate. A large number of tools slows down rather than facilitates the remediation process.

What organizations need is a single, unified approach to compliance. While many security tools are available for security teams to perform vulnerability and risk assessments, the assessment is only as good as the ability to implement remediation based on the findings. A unified solution that integrates and automates assessment and remediation not only addresses areas of risk, it can also eliminate them to a large extent, moving the organization closer to a state of continuous compliance while reducing costs.

Continuous compliance cycle



An effective continuous-compliance program provides an ongoing cycle of coordinated and uninterrupted processes.

A proactive approach that bridges disconnected silos

A unified approach that combines assessment and remediation to achieve compliance directly addresses weaknesses in the siloed approach, resulting in:

- **Real-time visibility:** To protect all endpoints, a unified approach should give security and operations teams the comprehensive, real-time visibility they need into the compliance state of endpoints, regardless of where the endpoints are physically located.
- **Consistent information:** A unified approach should ensure that reports and assessments provide the same up-to-date and accurate information to multiple teams.
- **Reduced costs:** A unified approach should not only minimize risk but also reduce the costs associated with managing compliance. A consolidated solution is much less expensive over the long term than performing compliance checks in the reactive, ad-hoc fashion that usually characterizes siloed management.

A unified compliance management approach should enable organizations to implement a proactive, policy-based approach, sharing and enforcing information across teams and defining policies based on accurate, real-time information.

A unified approach must provide coverage across all endpoints, pinpointing and remediating noncompliant endpoints while overcoming the challenge of manually managing every endpoint and requiring an enormous staff. It must provide support across multiple operating systems, including current and legacy versions of Microsoft Windows, Linux, UNIX, and Mac operating systems.

Continuous progress toward compliance goals

While a siloed approach results in peaks and valleys of compliance, a unified approach enables stair-step progress that allows organizations to move steadily toward compliance goals without sliding backward. Consider the steps that lead to continuous compliance:

1. Security and operations teams work together to formulate policies and service-level agreements for configuration baselines, patch management, anti-malware management and other aspects of endpoint security.

2. The operations team implements the baseline across all endpoints in the organization, regardless of the size or complexity of the environment—ideally in hours. It patches endpoints and monitors and manages endpoint anti-virus and firewall solutions as necessary.

3. An intelligent agent continuously monitors the endpoint for compliance with all security policies and keeps the endpoint continuously compliant.

4. The security team can check on the current state of endpoint security and compliance across the entire environment at any time without needing to initiate a new assessment.

5. Security and operations teams work together to continually strengthen security and adjust to evolving requirements.

Now security teams can “fix and forget.” Once the team has built policies that meet security, compliance and operations needs, the main task is to access reports to verify compliance

when needed. This continuous-compliance approach enables information security teams to take a more strategic approach with time to focus on continuous incremental improvements that will help ensure that they can meet or exceed today's compliance requirements and are ready for tomorrow's threats.

A best-practice approach for continuous compliance

IBM® BigFix® delivers a revolutionary solution that offers a unified approach to achieve and maintain continuous compliance, eliminating the need for separate, siloed assessment and remediation components by continuously assessing and enforcing policy-based compliance on each endpoint.

Designed for today's highly distributed public and private organizations, BigFix provides integrated, endpoint-centric assessment and remediation that ensures that all endpoints—even remote, roaming and mobile devices—stay in compliance regardless of operating system or location. It addresses the regulatory need for compliance and reporting as well as the operational need to maintain centralized visibility and enforce security configurations on endpoints, on or off the network, in real time.

Using a comprehensive policy-driven approach, BigFix consolidates multiple security and operations management functions into a single low-cost solution. This allows IT security and operations teams to quickly and easily measure their environment against defined compliance policies to assess and maintain compliance.

Now IT security and operations teams can finally break away from the traditional reactive compliance cycle by developing and delivering sustainable, cost-effective compliance best practices. By transforming the traditionally resource-intensive and repetitive compliance cycle into a state of continuous compliance, organizations can quickly and easily reduce risk and cost while increasing productivity.

Continuous compliance made possible by an intelligent agent

BigFix brings real-time visibility, automated remediation and global scalability to the compliance process. With a comprehensive library of technical controls and a flexible architecture that allows customization, it can adjust to support current and future compliance initiatives.

The continuous-compliance approach enabled by BigFix is made possible by a single-agent, single-infrastructure architecture that provides visibility into endpoints using a single management console. Powered by resilient, highly responsive intelligent agent technology, BigFix is purpose-built to support organizations of any size, including large, highly distributed environments.

A lightweight and intelligent agent placed on each endpoint continuously enforces security policies regardless of endpoint connectivity. Traditional endpoint management solutions utilize agents that depend on instructions they receive from a central command-and-control server to take any action. The intelligent agent built into BigFix automatically and autonomously initiates update and configuration actions to keep the endpoint current and compliant with organizational policies.

The agent identifies current patch and configuration levels, comparing them with defined policies. The agent then downloads only relevant patch, configuration and other content to the endpoint, quickly and accurately applying operating system and application updates. A key capability of the intelligent agent is its ability to close the compliance loop by transmitting status messages asynchronously to the management server, which always contains current endpoint compliance, configuration and change status, enabling real-time reporting.

With BigFix, operations and security teams have a real-time view of the infrastructure. Using this dynamic view of the configuration state, security and operations teams can immediately determine if the endpoints are in compliance. Discovery capabilities identify endpoints on the network that the organization may not know it has, including rogue devices that do not belong on the network. For endpoints not connected to the organizational network, it can also continuously enforce policy compliance via an Internet connection.

This unified approach offers the opportunity for teams to make policy-based assessments for reporting and measuring. It closes the loop on the remediation process as teams take advantage of the centralized view to immediately confirm that out-of-compliance endpoints are fixed. Everything BigFix can audit, it can remediate. Its real-time, automated process can shrink remediation windows from days or weeks to just hours or minutes—helping to ensure continuous compliance and strengthen security.

Addressing a full range of compliance needs

IBM BigFix deploys rapidly with a comprehensive set of capabilities, including:

- **Patch management:** Comprehensive capabilities for updating endpoints with patches from a wide range of operating system and application vendors
- **Security configuration management:** Information on the health and security of endpoints regardless of location, operating system, applications installed or connection
- **Lifecycle management:** A completely integrated approach for managing, securing and reporting on laptops, desktops, servers and even specialty devices such as point-of-sale terminals
- **Vulnerability management:** Assessment against standardized security vulnerability definitions with real-time reporting
- **Anti-virus protection:** Near real-time protection from malware and other malicious threats for both physical and virtual endpoints
- **Data loss prevention:** Security policy enforcement to block or allow data being copied to or sent to a variety of delivery channels, including network drives and USB storage
- **Multivendor anti-virus management:** A single point of control for managing third-party anti-virus products
- **Network self-quarantine:** Automatic assessment of endpoints against required compliance configurations and, if the endpoint is found to be out of compliance, optionally quarantining the endpoint until compliance is achieved
- **Endpoint firewall:** Enforcement of policies based on endpoint location, traffic control based on IP addresses, and regulation of communications
- **Asset discovery:** Visibility into changing conditions in the infrastructure, including identification of unmanaged and rogue devices
- **Software usage analysis:** The ability to track installations and usage of software on endpoints across the organization, reducing the cost of software license audits and decreasing the risk of fines from failing vendor license compliance audits

Broad-ranging benefits from a unified approach

BigFix offers a unified approach to achieving and maintaining continuous compliance, so organizations faced with internal policies and external security regulations can reduce their security exposure, minimize business risk and increase productivity through automation and control. With scalability that ranges to hundreds of thousands of endpoints, BigFix can provide critical endpoint visibility and control for organizations of any size.

Using BigFix, organizations can be confident that their endpoints are compliant as they mitigate risks and achieve benefits in critical areas, including:

- **Continuous compliance:** BigFix provides real-time, accurate compliance reporting and remediation through continuous assessment at the endpoint itself, helping to ensure a constant state of security and compliance.
- **Reliable security:** An intelligent agent provides instant notification of potential security issues—plus preventive management for software and operating system patching, anti-virus protection, data loss prevention, device control, firewalls, and network or device access.
- **Enhanced visibility:** Deep and wide visibility into all endpoints—including mobile and roaming endpoints—across Windows, Linux, UNIX and Mac operating systems—supports continuous enforcement of security configurations and the ability to answer questions, effect change, fix problems and report on compliance.
- **Effective IT operations:** A single, simplified, easy-to-manage console enables IT security and operations teams to coordinate efforts as they provide automated, streamlined, highly targeted and fast-to-respond processes.
- **Reduced costs:** Automation, task consolidation and scalability—all delivered by a single solution from a single vendor on a single infrastructure—help control the costs of providing effective vulnerability management and continuous compliance. Deployment in hours or days versus weeks or months enables rapid time to value.

BigFix enables organizations to combine assessment and remediation efforts with an automated solution that can reduce both cost and areas of risk. Its endpoint-centric, policy-based, intelligent agent approach automatically identifies noncompliant endpoints and brings them into compliance immediately.

A comprehensive endpoint security solution

The BigFix family of products operate from the same console, single management server and single intelligent agent, enabling organizations to consolidate tools, reduce the number of endpoint agents, and lower management costs.

BigFix is part of the comprehensive IBM security portfolio, designed to help address security challenges across the organization. IBM security solutions provide real-time visibility, centralized control and enhanced security for the entire IT infrastructure—including globally distributed endpoints—to facilitate the instrumented, interconnected and intelligent IT operations of a smarter planet.

Conclusion

To achieve the continuous compliance required by business operations and regulatory bodies today, organizations need to replace traditional processes based on legacy technologies, outgrown assumptions and siloed IT operations with a new best-practice approach and innovative technology.

IBM BigFix facilitates continuous compliance and risk reduction with distributed intelligence that enables organizations to see, change, enforce and report on security policies and endpoint compliance in real time, on a global scale. BigFix allows IT organizations to implement critical security and vulnerability management functions for endpoints from a single unified management console, with fine-grained reporting and an intuitive compliance dashboard.

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.

WGW03133-USEN-00