**IBM Security**
Thought Leadership White Paper

July 2017

# Ensuring progress toward risk management and continuous configuration compliance

*Get continuous compliance, real-time analytics and insight with IBM BigFix*

IBM

## Contents



## Introduction

Soon after putting monitoring, configuration and remediation capabilities into place to help ensure compliance with IT security objectives, an organization will have questions. Are we secure? Where are we exposed? Are our initiatives working? Have we met our targets? What progress are we making toward achieving continuous compliance? How do we prove our progress to security officers, regulatory agencies or auditors?

IBM® BigFix® Compliance helps apply, enforce and manage endpoint security and risk. In addition to continuous IT security configuration enforcement and remediation, it provides leading analytics capabilities to collect and archive automated security-check results to help identify configuration issues and report levels of IT security-related compliance.

With libraries of best-practice technical checks and compliance reporting tools for endpoint and server security configuration included, the solution is designed to provide critical management capabilities for supporting continuous, automated detection and remediation of security configuration issues and vulnerabilities. Its analytics capabilities further support enforcement of the organization's technical and configuration policies by monitoring, reporting and tracking progress, and determining success of security initiatives.

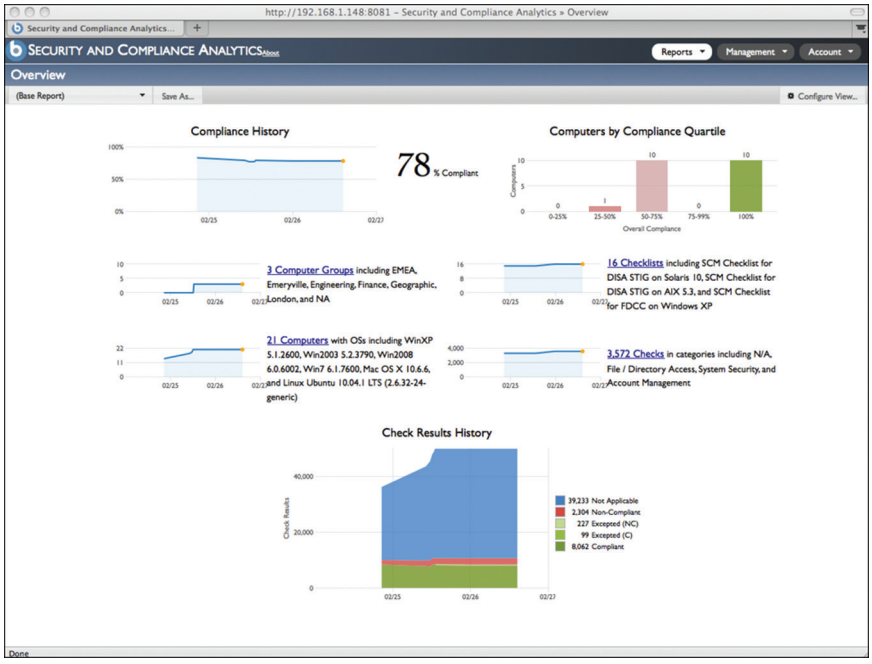
Analytics tools built into BigFix Compliance provide a variety of views on compliance status and security exposure, from high-level aggregate roll-up views to the identification of hot spots to drill-downs for detailed information. Analyses are based on infrastructure views that can be defined in multiple ways, from an individual device to groups of devices to the entire infrastructure. The results provide both technical and non-technical staff with the insights and tools necessary to strengthen the infrastructure against attacks to their network, servers and endpoints.

## Compliance for small to large distributed environments

BigFix Compliance helps meet organizations' specific policy-management needs by delivering analytics capabilities that utilize included libraries and by providing a platform for creating custom policies. This comprehensive endpoint security management solution can quickly and easily assess an organization's security and vulnerability posture, and can provide needed analytics capabilities for further insights. It supports security and compliance in small and midsized organizations up through large and complex distributed environments with management for up to 250,000 endpoints with a single management server.

The analytics capabilities of BigFix Compliance directly address an organization's need for insight and reporting to meet compliance regulations and IT security objectives, including:

- Determining progress and historical trends toward continuous compliance with security policies
- Quickly identifying endpoint security exposures and risks
- Easily creating and sharing summary and detailed reports about security policy compliance
- Identifying, managing and reporting on policy exceptions and deviations




Overview reports aggregate pass/fail automated security-check results across endpoints and graphically demonstrate compliance history.

## Clear visibility into endpoint compliance status

An organization with IT security policies typically has between 100 and 5,000 security checks that it must apply to ensure policies are being followed. Larger, more complex organizations, especially those with high regulatory reporting requirements, may have significantly more. The complexity of policies and infrastructure, coupled with the huge workload required to manually perform checks, can result in lack of infrastructure visibility and control, lack of standards enforcement, poor success rates and lack of overall security. Failure to enforce policies can result in endpoints that are highly susceptible to internal error or abuse and to external attacks.

The library of more than 8,500 automated checks included in BigFix Compliance supports virtually any IT security policy or benchmark to ensure that best practices are followed for security configuration compliance and that corporate and regulatory

governance requirements are met. For example, the library includes checklists based on benchmarks from the Center for Internet Security (CIS), the US Government Configuration Baseline (USGCB) and the US Federal Desktop Core Configuration (FDCC), as well as guides published by the US Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) and the US National Institute of Standards and Technology (NIST). Organizations that employ this solution can improve the detection, remediation and continuous enforcement of technical controls that help ensure risks are properly managed and security objectives are met.

### Compliance with standards and security checklists

**IBM BigFix Compliance provides out-of-box support for enforcing compliance with an ever-growing list of standards and security checklists, such as those published by CIS, DISA and NIST, including:**

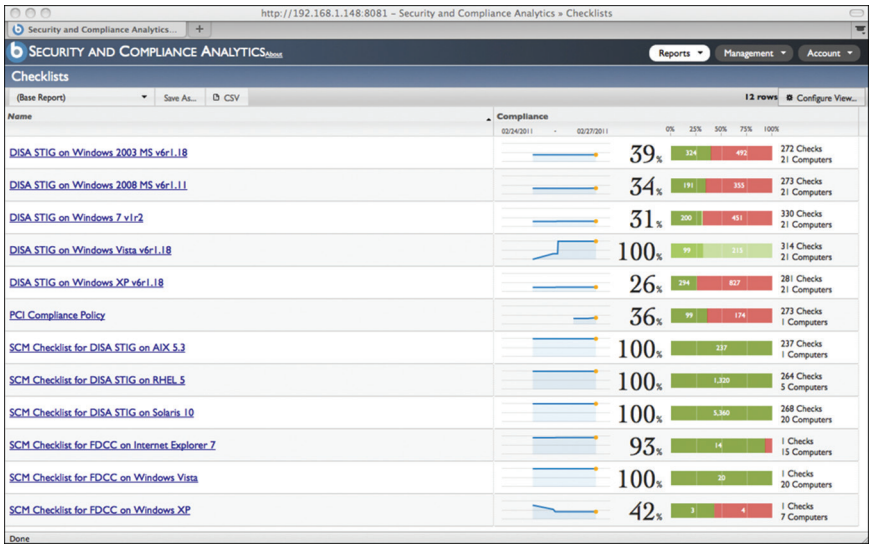
- **CIS checklists for Apple iOS, Google Android, Mac OS X, IBM AIX®, Solaris, Red Hat Enterprise Linux and Microsoft Windows**
- **DISA STIG checklists for AIX, HP-UX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server and Windows**
- **USGCB checklists for Microsoft Internet Explorer, Windows, Windows Firewall and Windows Energy**
- **FDCC checklists for Internet Explorer, Windows and Windows Firewall**

**For more detailed information about the supported standards and security checklists, visit:** http://tinyurl.com/m3rtwjs

BigFix Compliance extends capabilities with reporting and analytics functions to audit and evaluate an organization's progress toward achieving continuous compliance. It helps to detect, enforce and report on security configuration policies in centralized and distributed environments. The solution also enables customized, integrated reporting with other enterprise governance, risk and compliance management solutions, including those on the IBM OpenPages® platform.

## Targeted reports for effective management

It is common for an organization to need compliance information on a particular platform or type of endpoint, on a particular organizational or geographical segment, or on a specific regulatory or governance objective across all endpoints. It may, for example, need insight and remediation for its Windows environment or its Red Hat Linux platform, its finance or public Internet-facing endpoints, specific data centers, or its Payment Card Industry (PCI) or Control Objectives for Information and Related Technology (COBIT) objectives across all applicable endpoints. BigFix Compliance meets this need by producing reports with a variety of standardized and customized views. It does this by warehousing analytics and asset data in its database, then aggregating that data to help ensure rapid, timely and easy-to-use visualizations. Dashboards provide reporting and exceptions management with confirmation of compliance posture and system changes.




Checklist reports can show aggregate and detailed compliance status across checklists, endpoints and computer groups.

User permissions and roles can be defined to ensure each report user has access to only those endpoints and reports to which he or she is entitled according to the user's responsibilities. Report filters and analysis groups can use any combination of the thousands of asset attributes available through the BigFix solution to enable aggregated—as well as detailed—views into historical compliance, metadata for endpoints, checklists and the IT security checks themselves. Reports can be generated to compare actual measured results with the desired or required values for the security settings.

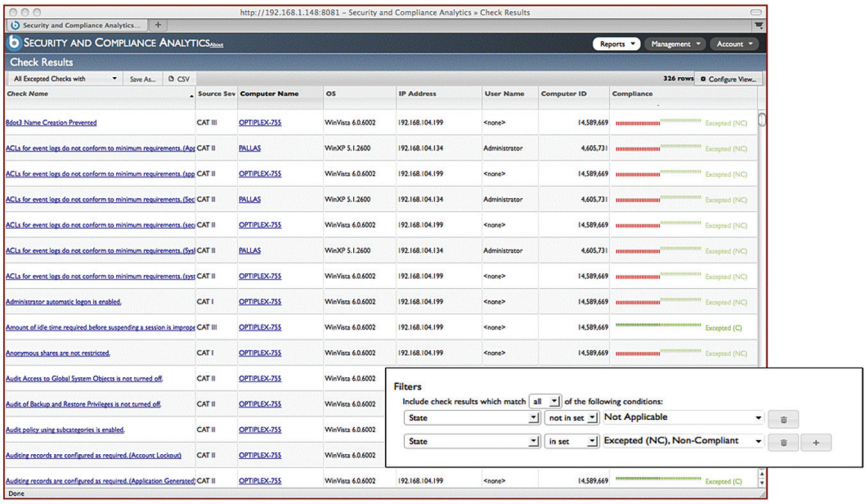
## Required compliance reports

**IBM BigFix Compliance delivers a full range of reports for managing IT policy checks. Reports can be filtered, sorted, grouped and customized using any set of BigFix properties. All can be exported, and then printed and emailed. Core reports include:**

- **Overviews: compliance status and history**
- **Checklists: compliance status and history**
- **Checks: compliance status, values and history**
- **Computers: compliance status, values and history**
- **Computer groups: compliance status and history**
- **Exceptions: management, compliance status and history**

Drill-down views provide a variety of perspectives on security and compliance issues such as configurations, security, health and compliance—for a business intelligence-like approach to managing IT.

Overview reports examine compliance history, aggregating pass/fail check results across endpoints, checks and checklists and providing graphic representation of groups according to compliance. List reports show pass/fail check results across endpoints, checks and checklists within a current scope, organized by check result compliance status. Check result reports show lists of the individual checks on each endpoint. Exceptions reports show checks and endpoints that have been excluded from compliance measures, with detailed information also provided on each exception. Each report type can be sorted, filtered and configured using an easy-to-use settings panel.




Check result reports show a list of individual checks on each endpoint. Users then leverage this rich metadata about endpoints, checks and compliance to filter, sort and customize report views.

## Historical views for ongoing improvement

Historical visibility into the state of compliance can be a particularly powerful tool in assessing the progress the organization is making toward achieving its goals—or to discover a past status that led to an issue. An organization that was the victim of a cyber-attack, for example, can examine its compliance status at the time of the attack to discover where vulnerabilities existed. This ability to drill down into specific details of both compliant and noncompliant endpoints can help identify critical gaps and provide insights that can be used to bring endpoints into compliance and strengthen an organization's overall security posture.

BigFix Compliance provides archiving and reporting capabilities that can also produce historical reports quickly and with a reduced IT workload. With this solution, it is no longer necessary to manually compile reports and chain them together to achieve the desired view. Each time a report user logs in, the solution automatically provides continuous reporting views that include a status history. For nontechnical staff charged with directing but not implementing compliance, BigFix Compliance provides web-based executive reporting.

Today, a host of compliance requirements—ranging from an organization's own security policies to country-specific data protection acts and privacy laws including the EU Data Protection Directive, to regulatory mandates such as Basel III, the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), PCI and Sarbanes-Oxley (SOX) standards—continue to reinforce the importance of security compliance management capabilities. The dangers of failed audits or operational failures along with the complexity brought on by reductions in force or mergers and acquisitions makes a streamlined, automated analytics tool a valuable asset in determining risk posture as well as in measuring success and progress toward compliance.

## For more information

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

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. For credit-qualified clients we can customize a financing solution to suit your business and development requirements, enable effective cash management, and improve your total cost of ownership. Fund your critical IT investment and propel your business forward with IBM Global Financing. For more information, visit: **ibm.com**/financing



IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2017



Please Recycle

WGW03130-USEN-01