Keeping distributed endpoints safe and compliant

IBM BigFix provides real-time visibility and control over globally distributed endpoints

Highlights

- Identify, manage and report on policy exceptions and deviations with security and compliance analytics
- Leverage a single infrastructure and console to manage all devices—smartphones, tablets, desktops, laptops and servers
- Deliver real-time endpoint protection against viruses, Trojan horses, spyware, rootkits and other malware
- Automatically manage patches for multiple operating systems and applications
- Enforce security policies using integrated data-loss prevention and device control

In today's far-reaching environments, where the numbers and varieties of servers, desktops, laptops, mobile devices and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks—known collectively as "endpoints"—are growing at unprecedented rates, traditional protection schemes such as firewalls and anti-virus agents are no longer sufficient on their own. With rapidly increasing numbers of remote workers and mobile devices, there is no well-defined perimeter. The perimeter, by necessity, must be the endpoint itself.

Endpoints, by their very nature, are highly vulnerable to attack—including system damage inflicted by malware, theft by phishing, privacy infringements through social networking, or loss of productivity due to spam, interruptions and system instabilities. These vulnerabilities can represent significant risk—including loss of control over the endpoint and the risk of losing valuable data. And they are likely present to some degree on every endpoint in your organization.

Many exposures are simply the result of endpoints that lack critical patches or have configuration errors that leave them open to attack. The Stuxnet virus outbreak, for example, exploited well-known vulnerabilities tied to the use of USB drives and the Microsoft Windows "autoplay" feature as an attack vector, both of which could have been eliminated through the consistent application of configuration and update policies organization-wide.

The pains caused by security issues, however, are not only in the attacks, but also in the way organizations protect themselves. Protection can be costly, complex and time consuming, stretching IT staff thin and driving costs even higher. After security is in place, many organizations have to prove compliance with internal policies, security standards and government regulations. In addition to the pain involved in achieving initial compliance, "compliance drift" is another key concern, as is the substantial effort it takes to produce an internal audit. Once compliance levels are attained, organizations must ensure that they are continuously maintained.

IBM® BigFix® can meet all of these needs, scaling from small to large organizations using the same easily deployed technology. It provides real-time visibility and control over each endpoint's status, remediating issues to enforce continuous security and compliance.

Visibility and control are the foundation of security

Organizations can have as few as one hundred or as many as several hundred thousand endpoints that must be kept secure in order to effectively manage risk, contain costs and maintain compliance. The challenges in managing such a large, diverse collection of technology lie in knowing how many and what types of endpoints you have, verifying and updating patch and security policies across all endpoints, and confirming compliance with internal IT and external regulatory policies—and doing it all fast enough to make a real difference in your security posture.

In a large and complex environment where threats come from multiple directions and individual endpoints are frequently targeted, where do you turn? How do you manage thousands of moving targets that are so diverse, they seem unmanageable?

The answer is to deploy a single, unified solution that not only addresses the risks associated with security threats, but also controls cost, complexity and IT staff burden while meeting compliance mandates. This solution must be able to provide organization-wide compliance reports instantly without the need to poll systems over days or weeks to assess the organization's security posture. Organizations need a simplified, streamlined, highly scalable visibility and enforcement solution that delivers continuous protection designed for today's distributed environments.

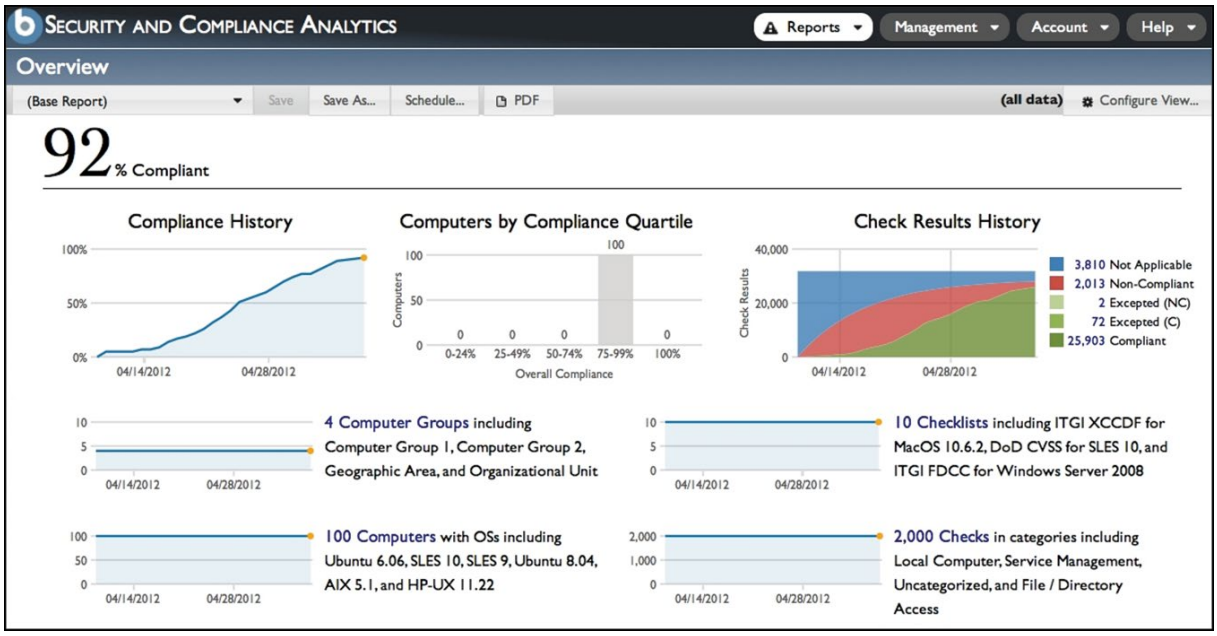
The ideal endpoint management solution provides smarter, faster, automated management capabilities that leverage the opportunities available in today's interconnected world while adapting to the inherent challenges presented by this environment. With the right solution, you can see and protect all of your organization's physical and virtual endpoints, whether they are smartphones; tablets; desktop PCs; roaming, Internet-connected laptops; servers or specialized equipment such as point-of-sale devices, ATMs and self-service kiosks. You can help ensure security for your environment whether it is based on Microsoft Windows, UNIX, Linux or Mac operating systems—or any combination—from the same console, utilizing the same management infrastructure.

IBM BigFix delivers rapid results

BigFix deploys in hours or days, depending on the complexity of your infrastructure, to deliver comprehensive endpoint security capabilities across the organization. This unified solution delivers endpoint management for hundreds of thousands of endpoints via a single console and single management server, rapidly addressing security risks by identifying and remediating vulnerabilities in real time.

The solution's discovery capabilities identify endpoints on the network that you may not know you have, including rogue endpoints that do not belong on your network and other endpoints that are not currently under management. The BigFix solution's intelligent agent deploys quickly and identifies current patch and configuration levels, comparing them against defined policies. It then quickly and accurately applies operating system and application updates regardless of the endpoint's location, connection type or status, and continuously enforces policy compliance, even if endpoints are not connected to the network. Vulnerability management capabilities quickly identify vulnerabilities, assessing and remediating managed endpoints using predefined policies.

The BigFix solution's unique intelligent agent continuously enforces security policies regardless of endpoint connectivity. Traditional endpoint management solutions utilize agents that depend entirely on instructions received from a central command-and-control server. The intelligent agent built into the IBM solution autonomously initiates update and configuration actions to keep the endpoint current and compliant with organizational policies, which are encapsulated in IBM Fixlet® messages. The agent downloads relevant patch, configuration or other content to the endpoint only when needed, while also continuously monitoring policy compliance and sending status updates to the management console as changes are detected. The centralized console always contains current endpoint compliance, configuration and change status, enabling real-time reporting.



Reporting via a centralized console provides real-time visibility into configuration and compliance status in a variety of easy-to-understand formats.

BigFix addresses a full range of security needs

BigFix provides key security capabilities, including:

- **Security standards support**: Supports Center for Internet Security (CIS) security benchmarks, which are consensus-based, best-practice security configuration guides both developed and accepted by government, business, industry and academia. Provides out-of-box capabilities for best practices that implement the U.S. Federal Desktop Configuration Control (FDCC) and U.S. Government Configuration Baseline (USGCB) standards. The solution has been certified by the National Institute of Standards and Technology (NIST) under the Secure Content Automation Protocol (SCAP) and has been deployed to that purpose at government agencies since 2008. The solution supports security checklists across multiple operating system platforms using the SCAP, USGCB, and Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) guidance documents. It can receive and act on vulnerability and security risk alerts published by the SANS Institute and from the National Vulnerability Database.
- **Patch management**: Provides unified, real-time visibility and enforcement to deploy and manage patches to all endpoints from a single console. Supports Microsoft, UNIX, Linux and Mac OS, plus applications such as Adobe, Mozilla, Apple and Java. Compresses patch cycles to minutes or hours with up to 99 percent first-pass success.
- **Security configuration management**: Provides a comprehensive library of technical controls that can help you achieve security compliance by detecting and enforcing security configurations. Policy libraries support continuous enforcement of configuration baselines; report, remediate and confirm remediation of noncompliant endpoints in real time; and ensure a verified real-time view of all endpoints.
- **Vulnerability management**: Assesses endpoints against standardized, Open Vulnerability and Assessment Language (OVAL)-based security vulnerability definitions and reports on noncompliance in real time to support the elimination of known vulnerabilities across endpoints.
- **Security and compliance analytics**: Provides analytics for insight and reporting to meet compliance regulations and IT security objectives, including determining progress and historical trends toward continuous security configuration policy compliance; quickly identifying endpoint security exposures and risks; providing detailed reports on security configuration policy compliance; and identifying, managing and reporting on policy exceptions and deviations.
- **Mobile device security**: Secures and manages mobile devices, including Apple iOS, Android, Symbian and Microsoft Windows Phone devices. Safeguards data by selectively wiping data when devices are lost or stolen and configuring and enforcing passcode policies, encryption, virtual private networks (VPNs) and more. Maintains compliance by automatically identifying noncompliant devices and taking action by denying email access or by issuing user notifications until corrective actions are implemented.
- **Multivendor endpoint protection management**: Provides a single point of control for managing third-party anti-virus and firewall products from vendors, including Computer Associates, McAfee, Sophos, Symantec, Microsoft and Trend Micro, enabling organizations to enhance the scalability, speed and thoroughness of protection solutions. In addition to ensuring that endpoint security clients are always running and virus signatures are updated, it facilitates migrating endpoints from one solution to another with one-click software removal and reinstall.

- **Network self-quarantine**: Automatically assesses the endpoint against required compliance configurations—and if the endpoint is found to be out of compliance, the solution can automatically configure the endpoint to be placed in network quarantine until compliance is obtained. The BigFix server is provided with management access, but all other access is disabled.
- **Endpoint firewall**: Enables administrators to enforce policies based on endpoint location, control network traffic based on source and destination IP addresses, regulate inbound and outbound endpoint communications, and quarantine endpoints when necessary.
- **Asset discovery**: Creates dynamic visibility into changing conditions in the infrastructure, with the ability to deliver pervasive visibility and control, including quick identification of unmanaged network devices for further investigation or to support automatic agent installations to rapidly bring rogue endpoints under management.
- **Superior malware protection**: Guards against the full range of malware and scans POP3 email and Microsoft Outlook folders for threats. It automatically cleans endpoints of malware, including rootkits, spyware, processes and registry entries that are hidden or locked.
- **Data-loss prevention**: Provides integrated data-loss prevention to enforce security policies in a manner that allows users to access sensitive data for their jobs but not misuse or lose that data, and to leverage predefined templates to help comply with data privacy regulations.
- **Granular device control**: Monitors and controls physical ports on endpoints, and can enable or disable these ports based on device type and content-aware scanning restrictions. Additional protections can be applied to restrict removable USB storage device access.
- **File reputation**: Queries up-to-the second data in a cloud-based database to determine the safety of a file and prevent users from opening infected documents.
- **Web reputation**: Automatically determines the safety of millions of dynamically-rated websites to protect endpoints against web-based malware, data theft, lost productivity and reputation damage.

A unified solution is the key to endpoint management success

BigFix can dramatically shrink gaps in security exposures by quickly and accurately effecting changes across the infrastructure. It eliminates the clutter of multiple management tools that make comprehensive visibility and control difficult or impossible, providing a single management infrastructure that coordinates efficiently among IT, security, desktop, mobile and server operations; effecting change; fixing problems; answering questions and reporting on compliance throughout the organization.

BigFix helps reduce security risks, management costs and management complexity as it increases the speed and accuracy of remediation while improving the productivity and satisfaction of end users. The single agent, single console and single management server approach streamlines processes and increases reliability. The solution delivers rapid time-to-value through functions such as patch management and asset discovery as well as long-term ROI by increasing operational efficiencies, enabling management infrastructure consolidation and improving IT productivity.

For more information

To learn more about IBM BigFix, contact your IBM sales 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

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.

WGS03060-USEN-00