IBM BigFix Patch

Continuous patch compliance, visibility and enforcement

Highlights

- Automatically manage patches for multiple operating systems and applications across hundreds of thousands of endpoints—regardless of location, connection type or status
- Reduce security and compliance risk by slashing remediation cycles from weeks to days or hours
- Gain greater visibility into patch compliance with flexible, real-time monitoring and reporting
- Patch online and offline virtual machines to improve security in virtual environments

With software—and the threats against that software—constantly evolving, organizations need an effective way to assess, deploy and manage a constant flow of patches for the myriad operating systems and applications in their heterogeneous environments. For system administrators responsible for potentially tens or hundreds of thousands of endpoints running various operating systems and software applications, patch management can easily overwhelm already strained budgets and staff. IBM® BigFix® Patch balances the need for fast deployment and high availability with an automated, simplified patching process that is administered from a single console.

BigFix Patch gives organizations access to comprehensive capabilities for delivering patches for Microsoft Windows, UNIX, Linux and Apple Macintosh operating systems; third-party applications from vendors including Adobe, Mozilla, Apple and Java; and customer-supplied patches to endpoints—regardless of their location, connection type or status. Endpoints can include servers, laptops, desktops and specialized equipment such as point-of-sale (POS) devices, ATMs and self-service kiosks. In addition, online and offline virtual machines can be patched so that virtual and cloud environments have the same level of security as physical systems. The offline virtual machines are brought online in a secure environment where only BigFix has access to them, ensuring that patches can be applied before the endpoints are made available for use.

Apply the correct patches to the correct endpoints

One approach to patch management is to create large patch files with a large update "payload" and distribute them to all of the endpoints, regardless of whether they already have all of the patches. BigFix Patch

takes a different approach, automatically creating patch policies, called IBM Fixlet® messages, which wrap the update with policy information such as patch dependencies, applicable systems and severity level. An intelligent endpoint agent recognizes which patches are required for the machine on which it is installed based on the endpoint's unique hardware, operating system, configuration settings, applications and installed patches. The agent then automatically retrieves and applies only the relevant updates for that specific endpoint.

Accelerate and automate the patch management process

BigFix Patch automates the entire patch management process and enhances security while saving organizations money, time and effort.

Research—BigFix acquires, tests, packages and distributes many patch policies directly for users, removing considerable patch management overhead. This largely automated process provides a consistent, high-quality patch in a timely manner.

Assess—The BigFix intelligent agent continuously monitors and reports the endpoint status, including patch levels, to a management server. This intelligent agent also compares endpoint compliance against defined policies, such as mandatory patch levels.

Remediate—An organization can quickly create a report showing which endpoints need updates and then distribute those updates to the endpoints within minutes. IT administrators can safely and rapidly patch Windows, Linux, UNIX and Mac operating systems with no domain-specific knowledge or expertise, and the solution stores audit information that tracks who ordered which updates to be applied to which endpoints.

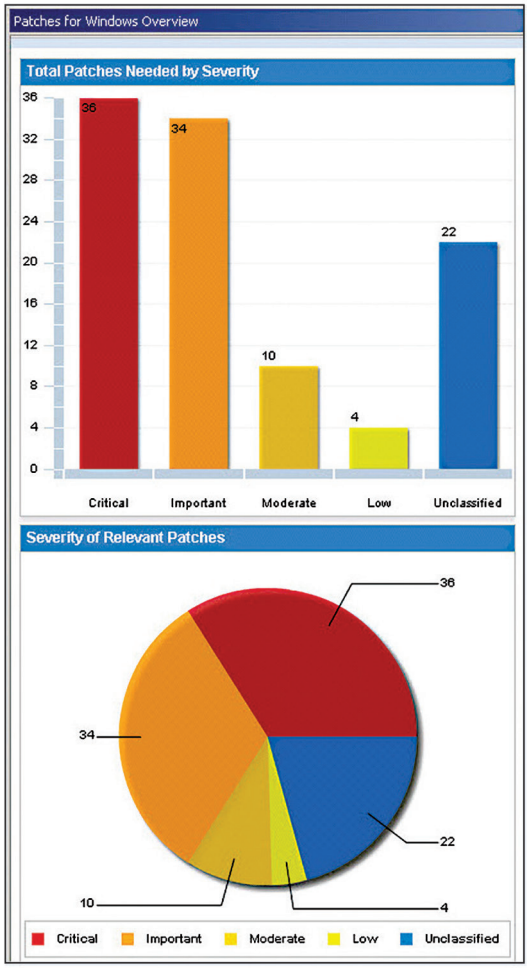
Confirm—Once a patch is deployed, BigFix automatically reassesses the endpoint status to confirm successful installation and immediately updates the management server in real time. This step is critical in supporting compliance requirements, which require definitive proof of patch installation. With this solution, operators can watch the patch deployment process in real time via a centralized management console to receive installation confirmation within minutes of initiating the patch process. By closing the loop on patch times, organizations can ensure patch compliance in a way that is smarter and faster.

Enforce—The BigFix intelligent agent provides continuous endpoint enforcement and ensures that endpoints remain updated. If a patch is uninstalled for any reason, the agent can be configured to automatically reapply it to the endpoint as needed.

Report—Integrated web reporting capabilities allow end users, administrators, executives, management and others to view dashboards and receive up-to-the-minute reports. Dashboards and reports indicate which patches were deployed, when they were deployed, who deployed them, and to which endpoints. Special "click-through" dashboards show patch management progress in real time.

Achieve continuous compliance

Many organizations need to establish, document and prove compliance with patch management processes in order to comply with governmental regulations, service level agreements (SLAs) with other organizations and internal constituents, and corporate policies. Regulations such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS) and Health Insurance Portability and Accountability Act (HIPAA) require that a regular, fully documented patch management process be in place, and proof of continuous compliance is necessary in order to pass audits. This solution's ability to enforce policies and quickly report on compliance can help improve an organization's audit readiness.



IBM BigFix Patch dashboards and reports show patch management progress in real time.

Simple to use, vast in scope

A single patch management server can support up to 250,000 endpoints, shortening patch times and updates with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks. The solution features patented bandwidth-throttling technology that manages network traffic and minimizes congestion.

IBM customers have achieved 95+ percent first-pass success rates—up from the conventional 60 to 75 percent rate—not only increasing the effectiveness of the patch process, but cutting operational costs and reducing staff workloads by as much as 20 to one. BigFix can patch endpoints on or off the network—including devices using Internet connections—with minimal endpoint impact. This means laptops using a public Internet connection at a coffee shop and other "roaming" devices can still receive patches.

IBM BigFix family at a glance

Server requirements:

- Microsoft SQL Server 2005/2008
- Microsoft Windows Server 2003/2008/2008 R2

Console requirements:

- Microsoft Windows XP/2003/Vista/2008/2008 R2/7

Supported platforms for the agent:

- Microsoft Windows, including XP, 2000, 2003, Vista, 2008, 2008 R2, 7, 8, Server 2012, CE, Mobile, XP Embedded and Embedded Point-of-Sale
- Mac OS X
- Solaris
- IBM AIX®
- Linux on IBM z Systems™
- HP-UX
- VMware ESX Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise
- CentOS Linux
- Debian Linux
- Ubuntu Linux

Why IBM?

Organizations can realize significant value by deploying additional solutions from the IBM BigFix family. The broad BigFix family addresses the convergence of system management and security requirements by delivering capabilities for vulnerability management, security configuration management, mobile device management, asset discovery, inventory, software distribution, operating system deployment, software usage analysis, compliance reporting and more. Because IBM has designed all functions to operate from the same console, management server and single intelligent agent, adding more services is a simple matter of a license key change.

For more information

To learn more about IBM BigFix Patch, 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

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.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2015

WGD03071-USEN-00