IBM Security
Thought Leadership White Paper

July 2015

Rewriting the rules of patch management

IBM BigFix shifts the patching paradigm

IBM

Contents

Introduction

Malware attacks are in a race against time to exploit vulnerable computer systems before software vendors publish patches and their customers can apply them. When malware wins the race, organizations lose productivity and risk loss of sensitive data, potential litigation and regulatory fines. The sheer enormity of the problem is alarming—the cost of cybercrime and cyber espionage to the global economy can be measured in the hundreds of billions of dollars, according to the security firm McAfee and the Center for Strategic and International Studies. In the US alone, hacking costs the overall economy as much as USD100 billion each year.[1]

To combat these threats, more and more software vendors are issuing more and more patches in attempts to keep pace with the frenzy of malware exploits. Unfortunately, most organizations are not equipped to handle this onslaught of patches in a time- and cost-effective manner. Because of organizational processes, it takes most IT departments weeks or even months to deploy patches throughout their environments. In fact, it can take organizations several months to even come close to achieving complete patch compliance. By then, countless additional patches have been issued, meaning that organizations are perpetually at high risk and out of compliance—and the situation only compounds over time.

Patch management has always been an uphill climb because of the massive complexity involved. Despite the risks, some organizations are reluctant to patch because of the time and labor required, plus the potential of disrupting business operations.

In an organization with a heterogeneous hardware and software environment, staying on top of the multitude of patches—and issuing them in a timely manner—can overextend IT staff and budgets. What is needed is a rapidly deployable, cost-effective, policy-based patch management solution that:

- Easily scales to manage all endpoints in organizations of all sizes—even the very largest—with minimal infrastructure
- Supports multiple vendors, operating systems (including Microsoft Windows, Linux and UNIX), applications and platforms
- Works over low-speed connections and supports devices that roam outside of the organizational network
- Minimizes the demand on IT staff
- Operates in real time, deploying patches organization-wide in hours
- Manages even offline virtual machines

IBM® BigFix® combines the separate pieces of the patch management puzzle into an intelligent, simplified solution that streamlines and optimizes the process of researching, assessing, remediating, confirming, enforcing and reporting on patches.

Addressing the patch management conundrum

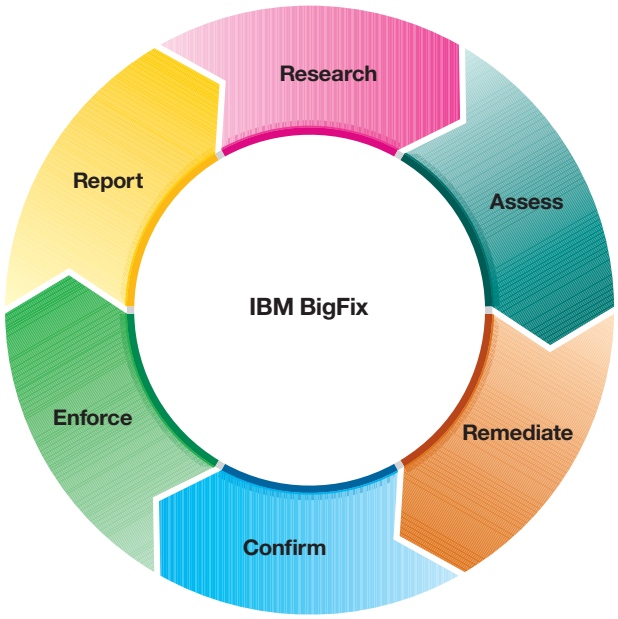
While patch management may seem straightforward, it is one of the most complex and critical challenges an organization faces. The nuances of effective patch management run much deeper than simply having a system administrator push out patches or relying on vendor-supplied patch mechanisms, hoping that they will be successfully applied—but never knowing for sure. The patch management conundrum raises questions that many organizations may find difficult, if not impossible, to answer. For example:

- How should an organization deploy critical "out-of-band" patches that arrive urgently and off the routine patch schedule?
- How can system administrators keep track of patches in an environment with hundreds or hundreds of thousands of endpoints running a variety of operating systems (OSs) and applications?
- How are system administrators supposed to monitor the status of roaming laptops and other mobile devices?
- How long will the patching process take from start to finish, and how will system administrators confirm (and prove) that every endpoint in their infrastructure has been properly patched—and stays that way?
- How can system administrators quickly test patches before deploying them—and roll them back if they cause problems?
- How can patches be deployed without interfering with end-user experience and productivity?
- How can patches be applied to business applications during strict maintenance windows, and can this be done with minimal downtime?

While it is clear that patch management is one of the most important security priorities for organizations, these questions indicate just how many barriers organizations face when implementing effective patch management practices. Between a lack of visibility and personnel, potential business impact, network-bandwidth limitations, lack of manageability, long remediation times, scalability issues, and coverage for different platforms, third-party applications, and roaming endpoints, the hurdles are many.

Fortunately, these hurdles are surmountable. BigFix removes these obstacles with a comprehensive solution that is purpose-built for highly distributed, heterogeneous environments. With this solution, organizations can finally see, change, enforce and report on patch compliance status in real time, on a global scale, through a single console.

Patch management process



With BigFix, patch management becomes a fully unified, closed-loop process that helps enhance security and save money.

Changing the patch management paradigm

While there is no single, official patch management best practice, the general approach involves a closed-loop process with six basic steps: research, assess, remediate, confirm, enforce and report. Historically, many of these steps were implemented via separate, non-integrated technologies, making it virtually impossible to create a closed-loop, real-time patch management process. BigFix provides all of these steps as part of a unified, fully integrated process that can help enhance security and save money, time and resources.

Here is a before-and-after look at how this solution changes the rules for patch management.

Step 1: Research

Before: The first step in the patch management process involves discovering which patches are available. This often includes researching patch availability through vendor email messages, application pop-up notifications, websites, blogs and a variety of other sources. This process must be repeated weekly—or even daily—for hundreds of patches, across scores of OS, application and anti-malware vendors. One alternative—relying on default vendor auto-updates—may lead to mistakes that can have negative consequences. Automating acceptance of patches without testing them can put organizations at huge risk, because there is no enterprise control over timing or reporting—and relying on users to apply updates is risky and unreliable.

A better approach is to have a patch management vendor provide a consolidated stream of the most common patches so that the organization only needs to evaluate each load of patches as it comes in, test the patches for compatibility with the organizational environment, and then deploy them via highly granular policies targeted to specific machine profiles. This allows specific patches to be applied only to the endpoints that need them. The problem, however, is that if this approach is not automated, it requires significant time and resources that organizations may not have.

After: IBM tracks patch releases from OS, anti-malware and common third-party application vendors and makes them available to users, helping to eliminate the need for time-consuming patch research processes. Patches and updates are wrapped in logic to help ensure accurate vulnerability and remediation assessments, then tested extensively. This results in patch policies called IBM Fixlet® messages. These Fixlet messages are then automatically sent to BigFix customer servers. Users can simply open up their BigFix consoles to view the latest updates and select patches for deployment. They can also create their own custom Fixlet messages through an easy-to-use, wizard-driven interface. This process works for virtually any update, including internal application patches.

Step 2: Assess

Before: For each identified patch, the IT organization must determine the applicability and criticality of the update, identifying which endpoints need patching across the organization. In the case of security updates, this critical data translates directly into risk, as business risk increases with the number of unpatched endpoints. Many organizations do not have access to the complete, current asset and configuration data set required to quantify the scope and impact of patches across the organization. There are tools that can help acquire this data, but many require days or weeks to collect and collate this information by scanning every endpoint on the network—and many roaming endpoints are rarely connected to the network. This information needs to be immediately available to system administrators at the time of patch release since many patches are time-critical, and the process of risk assessment and patch prioritization must take place as quickly as possible.

After: With BigFix, a single intelligent software agent is installed on all managed endpoints to continuously monitor and report endpoint state, including patch levels, to a management server. The agent also compares endpoint compliance against defined policies, such as mandatory patch levels and standard configurations. This information is especially critical during emergency patch scenarios when a vendor releases a highly critical, out-of-band patch, and organizations must rapidly quantify the overall magnitude and risk from the related exploit(s). In one example, a customer using BigFix installed agents on 5,100 endpoints and discovered that more than 1,500 (30 percent) of their endpoints were missing at least one critical patch. Taken as a whole, endpoints across the institution were missing 20,033 "critical" patches—an average of 13 patches per endpoint.

Once the total number of patches is mapped to the endpoints that need them, and the business criticality is defined, the IT organization can proceed to the remediation step.

Step 3: Remediate

Before: After a patch is assessed and a determination is made to distribute it across the organization, it must be packaged and tested to ensure that it will not conflict with other patches or third-party software installed on the target endpoints. Patch prerequisites and dependencies, such as minimum service-pack levels, must also be determined. This is usually accomplished by applying and testing the update on a select number of endpoints before a general release—a process that can take days or weeks to complete using manual tools. Once testing indicates that the patch is probably safe for organization-wide deployment, it is applied to affected endpoints, typically in batches, further extending the patch window. Long remediation times are primarily due to the inability to rely on patch quality, and secondarily due to unreliable distribution mechanisms, both of which result in low first-pass patch rates. Most organizations are therefore forced to proceed slowly in case a patch causes an unforeseen problem, as well as to ensure that network links are not overwhelmed by the patch distribution process. As a result, remediation is often difficult to accomplish quickly and effectively on an organizational scale.

Many tools also require deep platform expertise and highly trained personnel to operate them, or do not work until endpoints are connected to a high-speed corporate network—leaving roaming laptops and other mobile endpoints out of the update cycle for long periods. Many do not provide the fine-grained, policy-based controls that operators need to effectively deploy patches to all affected endpoints in the organization. Controls such as patch installation time windows—whether or not a user must be present—reboot options, method of distribution (including bandwidth and CPU throttles), system type and user notification options must be available inputs into the automated update processes.

After: Since BigFix customer servers automatically download the latest patch updates, endpoints can immediately begin to assess whether a particular patch is needed, without the need for operator intervention. The patch Fixlet messages include distribution instructions, including OS, version and prerequisite requirements, eliminating the need for IT to "package" and thoroughly test the patch. Operators can then spend a few minutes determining when the patch should go out, what notification should be displayed to end users (if any), whether or not to allow users to delay a patch implementation and for how long, and whether to force (or delay) reboots. The endpoint agent receives the new policy and immediately evaluates the endpoint to determine if the patch is applicable—and if so, it downloads and applies the patch, reporting back success or failure within minutes. This approach, combined with the BigFix relay structure and ability to reach Internet-connected devices, significantly reduces network load and can improve first-pass success rates to greater than 95 percent.

The solution also provides a highly secure mechanism that employs cryptographic identities, ensuring that only authorized administrators can create and distribute policies. The solution stores audit information that tracks who ordered which policies to be applied to which endpoints, and does not require specific OS expertise for operators that initiate the remediation process. Any BigFix operator with a few hours of basic training can safely and rapidly patch Windows, Linux, UNIX and Mac OSs, as well as Windows and Mac applications, with no domain-specific knowledge or expertise.

Step 4: Confirm

Before: After patches are scheduled for application, successful installation must be confirmed. This lets IT know when the patch cycle is complete and helps to support compliance reporting requirements. This data should be communicated back to a central reporting system that updates personnel on the process, including exceptions, in real time. However, many patch management technologies do not effectively perform this process, requiring weeks to re-scan all endpoints and even longer to correct exceptions. This lag time introduces significant uncertainty regarding the organization's overall business risk and compliance posture.

Many products do not provide confirmation that patches are applied—or if they do, it can take days or even weeks to obtain an organization-wide report. Even worse, some tools incorrectly report that patches are applied, when in fact the files were downloaded but the patch was not actually applied. With this amount of delay and uncertainty, some endpoints are often left exposed, leaving a significant window of vulnerability.

After: Once a patch is deployed, the BigFix agent automatically and continuously reassesses the endpoint status to confirm successful installation, immediately updating the management server in real time (or in the case of roaming devices, at the earliest opportunity). This step is critical in supporting compliance requirements, which require definitive proof of continuous patch installation. With this solution, operators can watch the patch deployment process in real time via a centralized management console, receiving confirmation of patch installation within minutes of initiating the patch process. Closing the loop on patch deployment enables organizations to ensure patch compliance in a way that is smarter, faster and much more reliable.

Step 5: Enforce

Before: After the initial application, many updates do not always "stick." Users intentionally or accidentally uninstall patches, new applications or patches may corrupt existing updates, malware may deliberately remove patches, or problems created by the update may necessitate a rollback. Patch management technologies must continuously monitor machines to ensure compliance

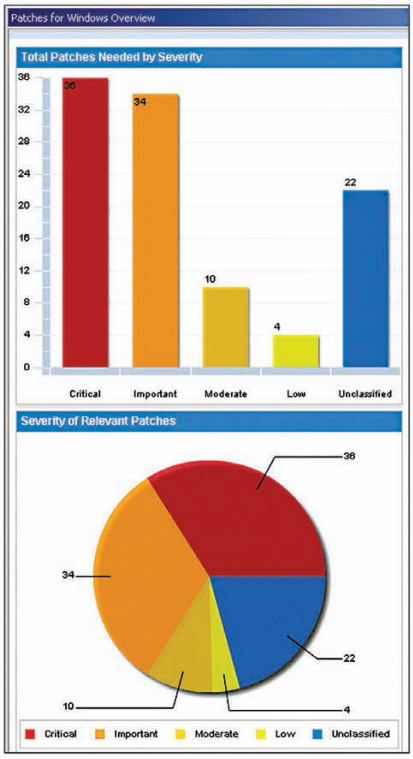
with update policies, providing rapid, policy-based rollback capabilities in the event of a major patch problem. If a patch is removed contrary to security policy, it must be immediately reinstalled, and if a patch creates a major problem after application, organizations must also be able to issue a rapid mass rollback. Without the proper tools, this step becomes next to impossible.

After: The BigFix intelligent agent continuously enforces patch policy compliance, helping to ensure that endpoints remain updated. If a patch is uninstalled for any reason, the policy can specify that the agent should automatically reapply it to the endpoint as needed. In the event of problems with a patch, BigFix administrators can quickly and easily issue a rollback to endpoints—either en masse or to a select few. Through the same centralized console, endpoint compliance status is reported in real time, allowing IT administrators to easily monitor the state of all managed endpoints in the organization. Administrators enjoy full control of their endpoints, enabling them to handle significantly more work than other products that require a lot of manual intervention and introduce significant time lags into the reporting process.

Step 6: Report

Before: Compliance and corporate policies require highly detailed, up-to-date dashboards and reports that indicate the organization's risk position and patch management status for a variety of consumers, including compliance auditors, executives, management and even end users. Without an overall solution, there is no clear-cut way to report on patch status organization-wide.

After: The integrated web-reporting capabilities of BigFix allow end users, administrators, executives, management and others to view up-to-the-minute dashboards and reports that 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.



Dashboard reports in BigFix show patch management progress in real time.

Understanding why it works

Traditional patch management approaches that utilize manual processes and cumbersome scan- and poll-based mechanisms are no longer fast enough or cost-effective enough to meet business and regulatory requirements, leaving organizations with unacceptably high risk and costs. Many organizations that try to utilize "free" or low-cost vendor tools quickly realize that these solutions are not enterprise-class. Most are limited to a single vendor, do not provide organizational control over what patches go where and when, are disruptive to the end user, and offer poor reporting that does not reflect real-time status.

Endpoints not immediately patched become a window of opportunity for cybercriminals—and a window of organizational risk. Moreover, organizations need to manage updates for a wide variety of vendor products and hardware form factors.

BigFix is a market leader in terms of breadth of coverage, speed, automation and cost effectiveness, providing comprehensive OS and third-party application patches. The solution, which includes deploying a single multipurpose, lightweight intelligent agent to all endpoints, supports a wide variety of device types ranging from servers to desktop PCs, "roaming" Internet-connected laptops, and specialized equipment such as point-of-sale devices, ATMs and self-service kiosks.

A single management server can support up to 250,000 endpoints, regardless of their location, connection type, speed or status, and additional servers can provide virtually unlimited scalability. Policy-based controls provide IT administrators with fine-grained, highly automated patch management capabilities, and comprehensive reports support compliance requirements. Policy compliance is continuously assessed and enforced by the intelligent agent, regardless of endpoint connectivity to the network. Competing products can be backend heavy, requiring massive amounts of hardware and personnel to support deployments. In many cases, they require dozens or even hundreds of servers, multiple agents per endpoint, and an army of operators to support the same environment that BigFix handles with one management server, one endpoint agent, and as little as 1/20th of the personnel.

Another key aspect of the BigFix architecture is support for endpoints that are on and off the corporate network. Roaming devices like laptops, for example, can receive patches via any Internet connection, including WiFi or even dialup. The patch management process is virtually transparent to the user, and Fixlet messages control the total amount of bandwidth and CPU consumed by the endpoint agent, which is location- and connection-aware to optimize network usage.

Achieving 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) and corporate policies. Regulations such as Sarbanes-Oxley (SOX), Payment Card Industry (PCI) Data Security Standard (DSS) and Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act require that a regular, fully documented patch management process be in place—with proof of continuous compliance necessary in order to pass audits. Unfortunately, many organizations spend an enormous amount of time and resources on patch management, yet still cannot meet compliance requirements. The ability of BigFix to enforce policies and quickly report on compliance can help improve an organization's audit readiness and pass rates.

Using IBM BigFix

Organizations are meeting the challenges of patch management head-on using BigFix. For customers, the results have included faster deployment, better compliance, reduced IT costs and shorter management cycles.

Offering a comprehensive endpoint management and security portfolio

IBM offers patch management capabilities through a standalone product—IBM BigFix Patch—or as an integral part of two larger endpoint management solutions—IBM BigFix Lifecycle and IBM BigFix Compliance. The BigFix family all operates from the same console, management server and endpoint agent, enabling organizations to consolidate tools, reduce the number of endpoint agents, and lower management costs.

BigFix is part of a comprehensive IBM security portfolio, helping organizations address security challenges for users and identities, data and information, applications and processes, networks, servers and endpoints, and physical infrastructures. By enhancing real-time visibility and control and improving endpoint security and management, the IBM portfolio supports today's ever-expanding, smarter data centers to facilitate the instrumented, interconnected and intelligent IT operations of a smarter planet.

BigFix technology provides:

- **A single intelligent agent—**BigFix leverages an industry-leading approach that places a single intelligent agent on each endpoint. This agent performs multiple functions, including continuous self-assessment and policy enforcement—yet it has minimal impact on system performance, using less than two percent of the endpoint CPU, on average. The agent initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations or other information to the endpoint when necessary to comply with relevant policies. As a result of the agent's intelligence and speed, the central management server always knows the compliance and change status of endpoints, enabling faster and more up-to-date compliance reporting.
- **Instant answers—**Whether it's finding out how many instances of Adobe Acrobat are installed or validating which laptops are impacted by a manufacturer recall, BigFix provides answers, across the organization, within minutes. Thanks to the intelligent agent, there is no need to wait for lengthy scans to complete, a centralized server to churn on the details, or thousands of SQL queries to finish running before dashboards and reports are generated. Each agent evaluates the relevance of the question, analyzes the information, reports back, and even takes action based on the analyses, if desired.
- **Roaming endpoint coverage—**The corporate-owned laptop has moved well beyond the confines of a corporate office. Users are connecting from home, hotels, airports and even airplanes. Always staying a step ahead, BigFix provides the unique ability to manage endpoints in real time—even for roaming devices.
- **Broad platform coverage—**It's hard enough to keep up with OS security updates, much less non-critical and non-security-related updates and a wide variety of application updates—but the challenge is intensified further when extended to offline virtual machines. However, a well-run BigFix environment with continuously delivered new content and features makes it a lot simpler, minimizing the downtime associated with putting off updates.

IBM BIGFIX ADDRESSES

PATCH MANAGEMENT CHALLENGES

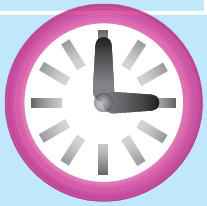
See how real-world clients in a wide range of business sectors—from banking, to retail, to healthcare—have achieved significant business improvements using IBM BigFix.*

Challenge: Speeding patch management deployment

Reduced software update and patch cycle times from **3 weeks to 3 days**

80%
reduction in patch deployment times

90%
reduction in time to deploy new patches and software upgrades



Challenge: Achieving compliance with licensing, corporate policies and regulations

99.99%
patch compliance rate

33%
increase in patch compliance, from 60 to 93 percent

USD 1 million
in license noncompliance fees avoided

Challenge: Reducing IT costs

75%
reduction in staff needed to support endpoint management

EUR 3.2 million
saved in labor, software licensing and hardware costs

USD 500,000
saved on software licensing costs

* Read the customer case studies at:
http://www-03.ibm.com/software/products/en/ibmendpmanaforpatcmana

Conclusion

BigFix addresses key challenges that many organizations currently face, providing a centralized, organization-wide server, desktop and mobile device patch management solution that automates and helps to alleviate much of the patch testing process from IT. BigFix deploys in days, and a single management server supports up to 250,000 endpoints, helping to drastically increase patch success rates, improve regulatory compliance and reduce expenditures.

In a world where seconds matter, BigFix can be the difference between a successful patch management strategy and one that leaves the organization at risk.

For more information

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

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by the world-renowned IBM X-Force® research and development team, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

Additionally, IBM Global Financing can help you acquire the software capabilities that your business needs in the most cost-effective and strategic way possible. We'll partner with credit-qualified clients to customize a financing solution to suit your business and development goals, 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 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.

[1] James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage," *Center for Strategic and International Studies (CSIS) and McAfee*, July 2013. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

WGW03137-USEN-00