IBM Security
Thought Leadership White Paper

July 2017

Reducing the cost and complexity of endpoint management

Discover how midsized organizations can improve endpoint security, patch compliance and lifecycle management on a limited budget

IBM

Contents

Introduction

While security attacks on big businesses dominate the headlines, midsized organizations are a highly attractive target for cybercriminals. Unlike large enterprises that have large IT departments with dedicated teams focused solely on security, midsized organizations must protect a growing amount of valuable information with limited IT staff and budgets. And the attackers are taking notice—targeted attacks aimed at small and midsized organizations are on the rise.

What is the true cost of these security breaches? It's not just the lost revenue, compromised data or inadequate compliance that is at stake. Security incidents can lead to a loss of trust among consumers, partners and suppliers, as well as damage to an organization's reputation for years to come.

At the same time, preventing security breaches is more challenging than ever. Today's organizations depend upon an ever-growing number of physical and virtual endpoints, including servers, laptops and desktops; tablets and smartphones; and point-of-sale (POS) devices, ATMs and self-service kiosks. These disparate devices run different operating systems and applications, and often access the network from remote locations. As a result, configuration errors, missing patches and compliance gaps are increasingly common. Traditional safeguards can no longer keep up with the latest threats.

This white paper examines the need for midsized organizations to combat the expanding sophistication of malicious attacks within the constraints of ever-shrinking IT budgets. It looks at ways to reduce the costs, complexity and resources required for administration. It will also explain how a single, cost-effective solution for endpoint management can help midsized organizations improve patch compliance, visibility and security—all within a limited IT budget.

Thwarting attacks with endpoint management

Traditionally, midsized organizations have turned to multiple products from multiple vendors to patch, manage and secure their diverse endpoints. Patches could be deployed from a USB drive, and compliance reports could be maintained within a few spreadsheets. However, these manual processes are hard to sustain as the organization grows, particularly in distributed environments.

Endpoints are increasingly becoming the weakest link in IT security, and the target of more sophisticated attacks. Security administrators need to guard against new types of malicious viruses, worms and spyware, and potential threats are often hidden within web pages and emails.

Another security challenge is that more and more employees are working remotely or in branch offices that have no IT staff onsite. These employees may be working off less secure Internet-based connections—not necessarily connecting to a corporate virtual private network (VPN). Effective endpoint management is critical in order to protect the entire organization, regardless of where the endpoint is located or how it is connected.

What business results can be achieved with IBM BigFix?

In real-world deployments of IBM BigFix, organizations in healthcare, banking and other sectors have achieved a wide range of positive business results.*

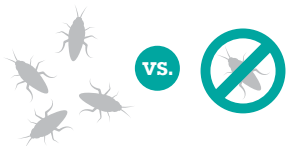
50% reduction in **labor costs**

98% **patch and update** compliance rate

50% reduction in **helpdesk calls**

80% reduction in patch **compliance times**

Increased first-pass **patch success rate** from **50%** to **99%**



No malware infections since solution implemented

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

Simplifying patch management

Whether employees work in the office or remotely, many exposures result from endpoints that lack critical patches or have configuration errors that leave them open to attack. But rapid deployment of security patches can be an overwhelming task for IT staff at midsized organizations.

Some organizations attempt to use free patch management products that end up costing them more overall. These free tools often require more infrastructure to use them and more IT staff to manage them, and they typically provide poor results in patch effectiveness and endpoint coverage. For example, Windows-only tools are not able to protect Linux, UNIX and Macintosh systems, or Android and iOS mobile devices. And free tools may not protect common third-party applications, such as Adobe applications, which puts organizations at even higher risk.

IBM provides a patch management solution designed to help midsized organizations manage the constant flow of patches, and it is available at a price to fit midsized budgets. The IBM solution enables IT administrators to easily apply the correct patches to the correct endpoints, and then verify that the patches are truly applied. By automatically enforcing patch policies, the solution supports continuous patch compliance.

With the IBM patch management solution, midsized organizations can:

- Automatically manage patches for multiple operating systems and applications across a wide range of endpoints, regardless of location, connection type or status
- Get greater visibility into patch compliance with flexible, near real-time monitoring and reporting
- See the patch status for all endpoints from a single console
- Help reduce security risk by streamlining remediation cycles from weeks to minutes or hours
- Patch online and offline virtual machines to improve security in virtual environments

- Patch endpoints on or off the network—including devices using Internet connections—with minimal endpoint impact, meaning laptops using a public Internet connection at a coffee shop and other "roaming" devices can still receive patches
- Improve audit readiness with simple and fast compliance reports

Improving lifecycle management

As the number and types of endpoints explode, tools for managing the lifecycle of these endpoints become more essential. Key lifecycle management capabilities—ranging from software distribution to automated asset discovery—are now more cost-effective and easy-to-deploy for midsized organizations.

IBM offers an affordable lifecycle management solution that is designed to help midsized organizations efficiently manage their endpoints. In addition to automating patch management, the IBM solution provides visibility into what exactly is connected to the network—including what software is installed. Administrators can use a single console to discover and inventory resources; distribute and manage applications for Windows, UNIX, Linux and Macintosh systems; and empower end users to deploy applications using a self-service portal.

Featuring high levels of automation combined with fine-grained configuration management, the IBM lifecycle management solution enables midsized organizations to:

- Run distributed scans of their entire network to identify all IP-addressable devices, including computing endpoints, network devices, and peripherals such as printers, routers and switches
- Automate software distribution across Windows, UNIX, Linux and Macintosh workstations and servers using a high-performance software package library
- Deploy approved and available software to end users utilizing a self-service portal
- Manage and enforce password policies, such as password length and complexity, to protect the security of local user accounts
- Create operator accounts based on group membership
- Address the full endpoint lifecycle with automated patching and system updates
- Reduce the clutter and expense of tools from multiple vendors
- Easily manage and enforce sophisticated power settings for all endpoints running Microsoft Windows and Mac OS X operating systems
- Reduce energy use and costs while avoiding disruptions in systems and security management

Helping ensure compliance

When it comes to security gaps in midsized organizations, cybercriminals are not the only concern. Regulatory agencies, suppliers and the general public are all demanding compliance with the latest security and privacy requirements.

Many midsized organizations need to establish, document and prove compliance with security policies in order to comply with governmental regulations. To operate as a supplier for a large enterprise, midsized organizations are now often required to show proof of compliance as part of the contracting process.

IBM provides an endpoint management solution to help midsized organizations enforce security policies and quickly report on compliance—helping improve their audit readiness. IT staff can use IBM BigFix to:

- Find and fix problems in real time regarding the health, compliance status, and currency of popular third-party anti-virus products from Symantec, Sophos, McAfee, Microsoft, CA, Proventia and Trend Micro, on a variety of operating systems
- Automate endpoint security configuration management
- Customize automatic quarantine rules to isolate malware attacks or out-of-compliance endpoints until remediation is complete

- Identify and respond to advanced persistent threats in minutes, regardless of endpoint type or location
- Simplify deployment of other security products
- Discover and report on all IP-enabled assets, even across heterogeneous operating systems

Taking control with the IBM BigFix family

IBM now offers simpler, more affordable solutions for improving endpoint security, patch compliance and lifecycle management—as well as power management—within midsized organizations. IBM® BigFix® provides continuous visibility, control and compliance of endpoints, while reducing costs and the burden on IT staffs.

Easy to deploy and manage, IBM BigFix can grow with your organization's needs. IBM Business Partners can help identify the right solutions for your organization, deploy them and provide ongoing support. And because all functions operate from the same console, management server and endpoint agent, adding more services is a simple matter of a license update.

IBM BigFix Patch: Deploy and manage patches across heterogeneous endpoints—physical or virtual, on or off the network—including Microsoft, UNIX, Linux and Mac OS systems, plus applications such as Adobe, Mozilla, Apple and Java. Compress patch cycles to minutes or hours with more than 99 percent first-pass success rates.

IBM BigFix Starterkit for Lifecycle: Complete administrator control over all endpoints, with visibility into the state of each endpoint from a centralized console. Manage updates with automated software distribution, patch management and self-service portals, and maintain visibility with asset discovery and inventory capabilities.

Conclusion

Today's midsized organizations are faced with the same security concerns as large enterprises—without the same budgets or IT resources. Many struggle to secure endpoints from attack using a complex mix of free tools and disparate point solutions. But now, there is an easier way.

Using IBM BigFix, midsized organizations can deploy a single, cost-effective solution for endpoint management—improving visibility and control within a limited budget. IBM can collaborate with your organization to understand the type of solution that's needed to help drive higher business results, and then help implement that solution to quickly deliver a fast return on investment. And, as your organization's needs change, you can easily extend the BigFix solution to include additional capabilities.

For more information

To learn more about IBM BigFix, please 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

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.

WGW03033-USEN-03