

# Need to Free Critical IT Resources Propels Patch Management

## Executive Summary

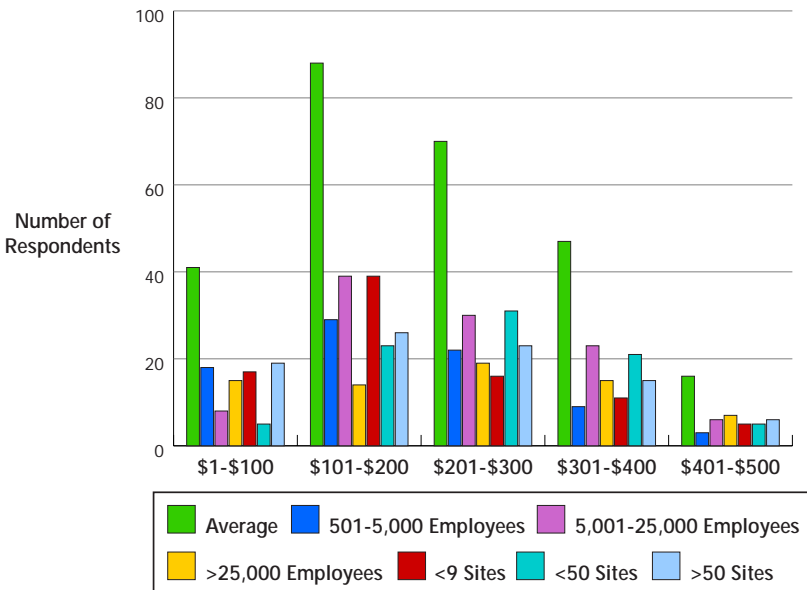
*The cost of patching is a greatly debated subject among network administrators, analysts and patch-management vendors. How enterprises patch today varies from doing the job manually to highly automated processes, thus explaining the disparity between reported costs for patching.*

*An entirely manual process can cost up to \$300 per patch, per machine. Exhibit 1 illustrates the results of the Yankee Group's 2003 Enterprise Security Spending Survey, where the overall average cost to patch a desktop was reported as \$254.*

*Some truths are universally accepted: There are on average 40 Windows patches per year—a third of them critical and a great many more related to applications and other operating systems. Any network greater than 500 seats that is patched in response to a vulnerability release consumes 100 to 120 hours of human resources in testing, installation and problem resolution. This costs the enterprise \$3,000 to \$4,000 in salary and diverts resources from vital business development.*

**Exhibit 1.**  
**Average Patching Costs by Size and Number of Sites**

Source: The Yankee Group 2003 Enterprise Security Spending Survey



n = 404 decision-makers

THE YANKEE GROUP REPORT

*The availability of desktops affects productivity at the most personal level of the enterprise; the work of employees is disrupted. If a desktop is not available for an hour or two while it is disinfected or repaired, how much it costs the enterprise depends largely on the individuals affected.*

*Traditional solutions to software maintenance—software distribution tools—are better suited to software installation than patching and upgrades. Patch management should include features necessary to manage an upgrade process. For example, identify new code versions, aid testing, installation and rollback. Technologies from Shavlik, BigFix and PatchLink are meeting these needs.*

*The need for tighter control over both desktops and servers creates opportunities for audit and compliance vendors such as BindView and configuration and network management plays LANDesk, AlterPoint, Altiris and Goldwire. Vulnerability management and scanning vendors offering passive intelligence will enter this market to extend their reach from perimeter to LAN, enabling enterprises to make better decisions about configuration and patch levels.*

*Antivirus vendors with presence on enterprise desktops and servers are recognizing the value that can be added with patching and configuration management. Remote endpoint security vendors and services providers iPass, Fiberlink and GRIC see an opportunity to expand their presence from remote office to enterprise-wide deployment. Software vendors have a stake in maintaining control over the maintenance of their application. These factors are making this a turbulent but exciting year in patch and configuration management markets.*

*This Yankee Group report looks at the market for next-generation patch- and configuration-management products. We profile some of the solutions available and discuss market drivers and future directions. We also examine the benefits of combining patch and configuration control to raise awareness of the costs of inconsistent configurations.*

## Table of Contents

---

<b>I. Introduction .....</b>	<b>3</b>
Challenges.....	3
<b>II. Endpoint Security and Management.....</b>	<b>4</b>
Patch Management .....	4
Configuration Management.....	4
Vulnerability Management .....	5
Host Intrusion Prevention .....	5
Policy Compliance and Enforcement .....	5
Patch- and Configuration-Management Product Features.....	6
Market Forecast.....	8
Winners and Challengers .....	8
<b>III. Conclusions and Recommendations.....</b>	<b>13</b>
Vendor Recommendations.....	14
Enterprise Recommendations .....	14
<b>IV. Further Reading.....</b>	<b>15</b>

---

## I. Introduction

The core driver of patching, software maintenance and configuration control is desktop availability and integrity. We all rely heavily on our workstations and servers; enterprises recognize the need to maintain these assets. Demand for new patching solutions is driven by the continued need to prevent the spread of viruses and worms and to free critical IT resources. Trends in business development, increased regulation, and acceptance of and reliance on IT follow patch management to its logical conclusion: host policy enforcement.

### Challenges

The impact of lost productivity and revenue related to desktop or server security is difficult to measure so the overall costs of patching or not patching are poorly articulated by the industry. According to the Yankee Group's *2003 Enterprise Security Spending Survey* of 404 decision-makers, 16 percent cannot identify their patching costs. Without a clear ROI, enterprises look to other solutions to mitigate risks. Network perimeter defense and antivirus are the mainstays of this protection.

Greenfield players dominate the patch- and configuration-management market, making them less attractive to large enterprises. Stuck without a viable alternative to SMS—and with the misconception that patch distribution is the same as software distribution—large enterprises are slow to recognize the benefits of this new technology.

## II. Endpoint Security and Management

Patch management is part of a larger market for endpoint security currently dominated by antivirus players offering threat mitigation. Patch management, configuration control, vulnerability management, host intrusion prevention systems (HIPSs) and firewalls underpinned by policy-compliance features will be major technology contributors to the endpoint security market in the next 3 to 5 years. The combination of technologies from each of these segments is forming the future host security solution, as illustrated by the entrance of many large security players (Microsoft, Symantec, Cisco) into patch management, policy compliance and HIPSs through partnerships and product enhancements.

### Patch Management

Vulnerability management systems (VMSs) emerged to help enterprises prioritize patching to the most critical issues and assets. However, these systems fall short of handling patching for the enterprise. Enterprises cannot apply patches or software upgrades as soon as the vendor releases them without diverting resources from vital business development.

The question for enterprises is not *if* the patches are applied, only *when*. The response ranges from immediately to protect against a serious threat such as a new worm or virus, to waiting for a quarterly service pack or patch rollout. The former allows less time for planning resource allocations and costs the business more. Patch-management solutions costing around \$20 per desktop and \$500 to \$1,500 per server offer the ability to reduce the costs and disruption associated with urgent patching—a significant driver for large enterprises that want to focus on the core business, not on updating software.

Reducing the known costs of patching—payroll—is a core driver, but enterprises must also consider the unknown costs of patching: the potluck nature of problems resulting from a patch. A patch can bring a server down or affect the desktop of a top revenue-producer. These unpredictable risks are major concerns for system administrators. The effort involved in a rollout of the latest patch is largely due to the small number of patches that fail to install correctly.

### Configuration Management

There is significant variation in desktops and servers: Each can report several hundred issues during a scan. Configuration changes occur when users change something or when software is installed, configured or upgraded. Most changes have no impact on security or other areas, but a few can cause problems such as a virus infection, software incompatibility or violation of corporate security policy.

Today, most enterprises use vulnerability scanners and audit tools—or, at a minimum, built-in administrative tools such as Windows Group Policy—to see how desktops and servers are configured. The fact that a configuration is being audited does not mean it is being managed. Most configuration changes on desktops and servers are performed manually. The human cost of identifying and fixing configuration discrepancies manually is such that it is almost never done, except when critical and obvious security issues are identified. Configuration management solutions such as those offered by Altiris, AlterPoint and Goldwire are helping the desktop and server administrators automate this task and finally gain control over host configuration.

## Vulnerability Management

Vulnerability scanners and security intelligence services (real-time vulnerability and threat information) are a popular solution to the “to patch or not to patch” dilemma facing enterprises. Scanning tools have found their place at the perimeter as an audit requirement for many business-to-business relationships and a cheap way to make sure the front door is locked. Inside the network, the role of vulnerability management is more complex, requiring asset management and risk analysis to apply vulnerability mitigation strategically. Vulnerability management must become a business process, of which these tools are only one part.

Vulnerability scanning is combined with intelligence by vendors such as iDefense, Symantec, TruSecure, Solutionary, Qualys and Foundstone. Players are likely to partner with or acquire patch- and configuration-management vendors that can form part of the end-to-end solution enterprises are seeking.

## Host Intrusion Prevention

Intrusion detection and prevention device vendors have introduced the concept of virtual patching: terminating suspect network connections before they can affect the network. The main benefit is the ability to block attacks without prior knowledge of it, avoiding the inevitable delays while security products are updated.

Entercept, ForeScout, Symantec and Cisco offer host intrusion prevention solutions. These players should partner with signature vendors and focus on threat mitigation. The Yankee Group recommends separating the command and control aspect of endpoint security offered by patch- and configuration-management solutions from threat mitigation. Integration between threat and control systems is desirable but security controls should ensure the two components are logically separate.

## Policy Compliance and Enforcement

Audit tools are needed for internal and external audits—even more so today with new regulations such as HIPAA and the Sarbanes-Oxley Act. Vendors like BindView, NetIQ and Polivec offer audit tools; it is an easy leap to combine the two needs for audit and enforcement. These vendors are leaving behind a passive role to a more intrusive security presence on the endpoint. Vendors InfoExpress, ENDFORCE, Sygate, Symantec and Cisco are also offering some policy-enforcement features as part of their endpoint security suites.

## Patch- and Configuration-Management Product Features

### Architecture

Systems architecture uses either agents or remote procedure calls. Using an agentless system limits the extent to which the architecture can manipulate the target device. For example, continual monitoring and enforcement of a policy is impossible without agents. If an agentless architecture is preferred, understand its limitations and verify that the remote procedure calls use a secure mechanism.

When evaluating agents, criteria such as size, CPU and memory use are key. Verify that the agent cannot be circumvented, removed or disabled, and that the solution provides easy ways to distribute and update the agent component.

Distributed architectures are more scalable. Features for load balancing and caching across multiple servers enable management tools to scale to more than 100,000 nodes.

### Accuracy

There are several means for verifying a patch is installed: Examining the size, timestamp and version of program files is the most reliable method. Examining the registry is known to cause false positives and negatives. Patch-management vendors should work with target-system vendors to find reliable methods for checking code version. Using two separate systems to double check system configuration and software level is one option. Given the added complexity, this is not a desirable method of control, except where extremely high levels of host policy compliance are needed.

Patch-management vendors that provide a testing service and deliver tested patches add value by improving accuracy. Determine how the vendor carries out its tests. Verify that patches are delivered over a secure communications channel that ensures patch confidentiality and integrity.

Additional features that help are those that keep track of software incompatibilities (e.g., some patches create problems when applied in the wrong order) and perform rollbacks to recover systems.

### Support for Platforms

Verify the solution supports all the organization's platforms and applications that you want to manage.

### Asset Inventory

The solution should include features for managing assets or be capable of integrating with technology that automatically discovers network assets. The reliability of the method used for asset discovery is a big consideration; assets that are undiscovered and unmanaged represent the biggest risks to the network. Look for features that allow you to prioritize and group assets according to policy and criticality so you can treat patch and configuration management as part of the overall asset-management process.

### Policy Compliance

The solution should allow you to define a corporate policy and report machines that are out of compliance with regard to patch level or configuration.

## Policy Enforcement

It is important to have the ability to automatically enforce a defined policy. For example, Microsoft Active Directory Group Policies enforce policies at the desktop and server level. Remote endpoint vendors excel at performing policy enforcement at the network perimeter including antivirus, firewall, service and process inspection.

Consider how the solution behaves when a machine is off the network for a period and reconnects needing a virus or patch update. When policy noncompliance is identified, quarantining until the machine is corrected is desirable.

## Configuration Control

It is valuable to have features for monitoring and making configuration changes—for example, the services that are running, the software that is installed and how the operating system is configured.

## Patch Management Road Map

Patch management, as a process separate from software distribution, is currently implemented in one-tenth of *Fortune 1000* companies. Combined patch, configuration and policy-compliance tools can significantly reduce the risk of virus infection, configuration issues and patching costs. However, large investments in existing technology and ignorance of the costs of maintaining outmoded methods for software distribution are to blame for the industry's inability to show ROI for patch management.

The decision of BindView, Microsoft, Symantec and Mobile Automation to partner with Shavlik and add features for patch management creates a clear path for other software vendors to follow. Their entry into the market does not imply absorption of patch- and configuration-management markets by larger software vendors as many industry followers believe.

## Configuration Management Road Map

The current market for configuration control is healthiest in the public sector, where the Federal Information Security Management Act has created strong drivers for desktop and server control. The existence of P2P file-sharing applications, spyware and incorrect versions of software is tolerated less by many government organizations than by those in the private sector. The benefit of controlling software deployed on the network is not a sufficient driver for wide-scale adoption in the private sector. A clearer understanding of the costs of configuration issues is needed in addition to solutions that scale to the desktop. The benefits of configuration control in the enterprise exist in a holistic host-management solution, combining build management, configuration, patching, software distribution and policy enforcement.

Configuration control features will eventually enable us to track configuration and version changes, automate testing and reduce the likelihood of failed patches, failed installations or applications that do not work because of a configuration issue. Other more subtle benefits include automated software installation routines. A manual installation tracked using a configuration control system is easily replicated by that system without requiring any package to be created or image built as we do today.

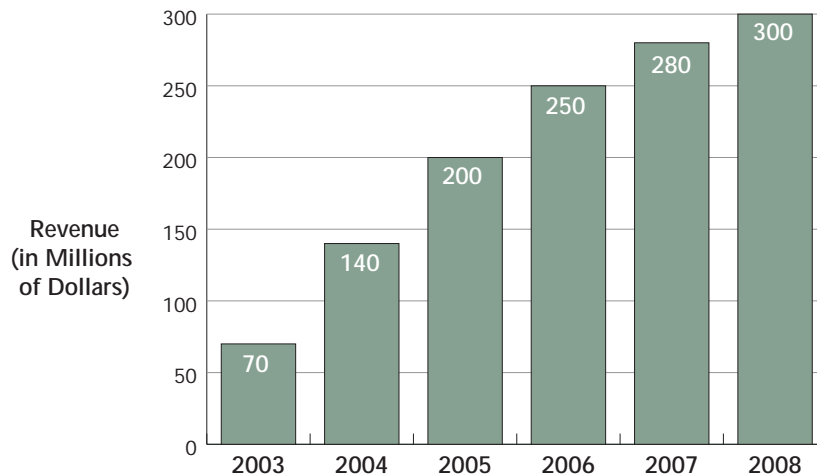
## Market Forecast

The Yankee Group forecasts the global patch-management market will grow from \$70 million in 2003 to \$300 million in 2008 (see Exhibit 2). Patch-management, configuration and policy-compliance features form part of the market for systems and network management and will consolidate with this larger space by 2006.

### Exhibit 2.

#### Global Patch-Management Forecast

Source: The Yankee Group, 2004



## Winners and Challengers

Exhibit 3 places prominent vendors according to the breadth of the solution offered and their ability to execute in the market. To determine solution breadth, we used criteria such as product features, clarity of messaging and customer references. The ability to execute in the market reflects financial stability and brand quality, and takes into consideration the core competencies of the vendor with regard to patch and configuration control.

**Exhibit 3.****Summary of Patch and Configuration Management Solutions***Source: The Yankee Group, 2004*

Vendor	Platforms Supported	Patching	Configuration Control	Policy Compliance
Shavlik	Windows, IIS, SQL, Exchange, MDAC, Internet Explorer, Linux	Yes	Limited	Yes
BigFix	Windows, UNIX, Linux	Yes	Limited	Yes
LANDesk	Windows, UNIX, Linux, Cisco, Macintosh	Yes	Yes	Yes
Altiris	Windows, UNIX, Linux	Yes	Limited	Yes
BindView	Windows, UNIX, Linux, Netware	Yes	Limited	Excellent
Microsoft	Windows, IIS, SQL, Exchange, MDAC, Internet Explorer	Yes	Limited	Limited
Pedestal	Windows, UNIX, Linux	No	Yes	Yes
St. Bernard	Windows	Yes	Limited	Yes
AlterPoint	Cisco, Checkpoint, VPN, VoIP	Limited	Yes	Yes
Goldwire	Extensive	Limited	Yes	Yes
Marimba	Windows, UNIX, Linux	Yes	Limited	Yes
Mobile Automation	Windows, SQL, Sybase, Oracle, Palm OS, Pocket PC	Yes	Yes	Yes
IBM/Tivoli	Extensive	No	Yes	Yes
PatchLink	Windows, UNIX, Linux, Macintosh	Yes	Yes	Yes
Novadigm	Extensive	Yes	Yes	Yes
NetIQ	Extensive	No	Yes	Yes
Polivec	Extensive	No	Yes	Yes
Citadel	Windows, UNIX, Linux, Macintosh	Yes	Yes	Yes
Authentium	Windows, UNIX, Linux, Macintosh	Yes	Limited	Limited
Ecora	Windows, Solaris, Cisco	Yes	Yes	Yes
Sygate	Windows	Yes	Limited	Yes
Opware Inc	Windows, UNIX, Linux	Yes	Yes	Yes
Symantec	Windows, Office, Apache, SQL, Lotus Notes/ Domino	Yes	Yes	Yes

Based on these criteria, BindView, PatchLink, Ecora and Shavlik are currently best positioned to lead the patch-management market. Configuration-management vendors Goldwire and AlterPoint are struggling, but moving toward patch management is the right move to improve the ROI for these solutions. Citadel and LANDesk are the ones to watch in 2004—they will challenge the leaders for market share in patch management.

### **PatchLink**

PatchLink plans to open offices in Europe and Asia in 2004. PatchLink Update, an automated enterprise patch-management solution, was first developed in 1996 and is the sole product of this highly profitable company. Version 6.0—released in the fourth quarter of 2003—added active configuration management features such as monitoring the authorized service processes and quarantining noncompliant machines.

Extensive platform support including Macintosh, Netware, Solaris, HP-UX, AIX and Windows has attracted customers such as the U.S. Navy and Army, Ernst & Young, IBM and Motorola. More recently, partner PricewaterhouseCoopers aligned with PatchLink to meet the increased demand for patch-management solutions and services. PatchLink offers a highly scalable solution coupled with thorough patch-testing services—patches are applied to machines in PatchLink labs, effectively minimizing the risk of patches causing a problem. In 2004, PatchLink should focus on market awareness and fostering a brand image. Behind the scenes, PatchLink should invest in infrastructure that is capable of supporting an aggressive partnership and sales strategy.

### **Shavlik**

Shavlik markets HFNetChkPro, EnterpriseInspector and AccountInspector as a suite of products. The strengths of the solution are speed and accuracy in Windows environments. BindView, Microsoft, Symantec, Marimba and Mobile Automation have deployed Shavlik's HFNetChkPro technology. Awareness of the Shavlik brand will skyrocket with the co-branding and reselling opportunities created by these partnerships. This will encourage new partners and makes Shavlik an attractive acquisition target. However, Shavlik needs to catch up on features to compete with the other pure-play patch vendors and their own partners. Support was recently added for Linux and will be available for other flavors of UNIX later in 2004.

### **BigFix**

BigFix offers a scalable architecture for patch management within a large enterprise. It provides the value-added service of prepackaged, pretested patches for all Windows, major UNIX and Linux platforms. Vulnerability information is integrated into the console, enabling administrators to identify the most critically needed updates. Policy-enforcement features in BigFix include monitoring of antivirus versions and other software such as SMS. Third-party reviews show some problems with accuracy, but this has not discouraged potential partners. For example, remote endpoint security service provider Fiberlink has announced integration of BigFix into its solution.

## Ecora

Ecora provides configuration- and patch-management solutions to 2,000 customers worldwide. LANDesk's selection of Ecora patch-management solutions extends its reach to 10 million more nodes in 4,000 new customers. Ecora provides a policy-management approach to patch and configuration management spanning servers, desktops, routers and databases. Despite early bias toward Windows platforms, the latest release adds a Solaris agent to meet the needs of *Fortune 1000* enterprise customers. Ecora will extend platform support to Linux and other flavors of UNIX in 2004. Ecora's solution allows users to apply patches within a sandbox to minimize the risks associated with patching. Ecora has a recognized brand image and can leverage it to gain traction in this market in 2004. The company's vision for the future of patch management is sound, but it is unclear whether Ecora has the resources to execute the strategy.

## LANDesk

LANDesk software manages 10 million enterprise network nodes for performance and availability. The solution scales to 200,000 nodes and integrates tightly with asset- and change-management systems such as Remedy. LANDesk partnered to offer a patch-management solution as part of the LANDesk Suite. This recent move brings a new competitor to this budding market. If LANDesk produces a patch solution with the same high quality as its successful management system, the company is sure to do well. Quickly gaining expertise in the technology of patching—far more invasive than traditional systems management—is key to its success. The evaluation criteria outlined above are enhancements that LANDesk should seriously consider for the product road map.

## BindView

BindView based in Houston, Tex., is an established public company providing audit solutions to *Fortune 500* customers. With more than 5,000 customers worldwide, its excellent reputation among security and audit professionals is well deserved. Early entry into the patch-management space through a partnership with Shavlik is a smart strategy, keeping internal resources free to focus on the audit and compliance technology that BindView excels at. Caution is advisable for BindView and other vendors in the position of moving from passive auditing to proactive control. The Yankee Group recommends more proactive features for policy compliance—but this is a challenging technical problem that warrants the expertise of a focused pure-play vendor.

## Microsoft

Microsoft first offered SMS software distribution system as a free tool for system administrators. It is the dominant patch distribution platform of *Fortune 1000* companies. SMS provides centralized software distribution capability and enterprise reporting. It is scalable to networks of more than 100,000 nodes but limited to Windows platform support.

The SMS system’s suitability for patch management is questionable because it was designed for software distribution. Testing and packaging the software delays the application of a patch for hours, when critical security updates are needed immediately to minimize network outages. The introduction of Windows update in 2002 simplified the problem of identifying which patches are needed. The tool is a lifeline for consumers and small businesses trying to secure their Windows desktops and servers, but does not scale to the enterprise. Similarly, SUS and WUS are tools designed specifically to patch Windows systems, but these do not yet scale to the large enterprise network.

Microsoft’s platform bias excludes it from competing with enterprise patch-management vendors. However, offering a scalable enterprise-class solution designed for patch management of Windows platforms is a strategy that can only benefit Microsoft in the long term. It serves to increase customer loyalty in single-platform enterprises.

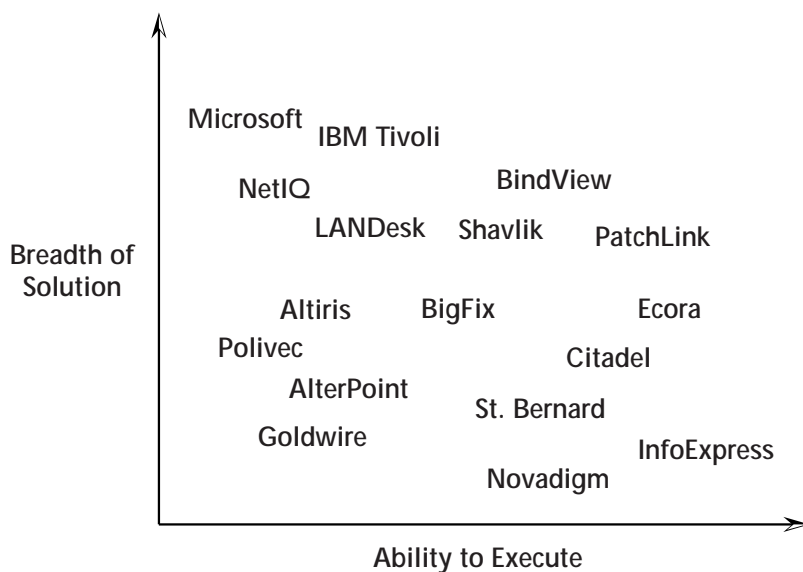
### Citadel

Citadel markets a patch- and configuration-management solution called Hercules to an installed base of public-sector customers. The breadth of product features and platform support is excellent. The focus on vulnerability remediation—rather than just applying patches and managing the configuration—appeals to security and market analysts seeing success in the vulnerability management space. The Yankee Group recommends against a strong vulnerability mitigation message because customers equate that with technology they have already invested in, and have not delivered on promises of actually managing the vulnerabilities.

#### Exhibit 4.

#### Patch Management Competitive Positioning

Source: The Yankee Group, 2004



### III. Conclusions and Recommendations

Soon we will quickly, cheaply and automatically patch and resolve problems. It will become less important to risk-assess each patch—although the cost of a software upgrade will go down, it will never be zero. It always will be advisable to apply patches where they are needed, rather than indiscriminately. Patch management is an extension of change control and asset management; vendors with expertise in these heavily process-oriented areas are the ones to watch.

Integrating patching into software so that each application takes care of its own patching is an obvious end state, although not the most desirable. There are several drawbacks or vulnerabilities related to this approach:

- Enterprises have less control over code deployment.
- Multiple applications are performing the same job of checking for updates and installing them.
- Auditing patch levels across multiple applications is complicated and time-consuming.
- Vendor monopolies are encouraged.
- Server and desktop software listens to and communicates with the Internet.
- Server and desktop software has agents running and consuming resources.
- A third party is unlikely to test new code.
- There is no central unbiased repository of incompatibilities between software versions.

The approach will help software vendors further penetrate a customer's network, but it is less beneficial for customers. Independent patch-management services add a lot of value to the enterprise in the form of vendor neutrality, layered defense and efficient use of computing resources.

It is difficult to prove that configuration control is a recipe for network insecurity. Mismanaged configurations are tolerated for want of proof or a better alternative. Until enterprises recognize configuration errors as a security risk, demand for these solutions will remain low. A high level of consistency in endpoint configuration also limits end users' ability to customize a PDA or desktop. We need to recognize that a high degree of consistency in endpoint configuration is unrealistic.

The only desirable result is a process for managing hosts that reduces the number of outages and virus infections in a measurable way. Achieving this is not trivial; it warrants a unique set of core technologies and vendor competencies in two distinct areas: threat mitigation and command and control.

## Vendor Recommendations

- **Software vendors should actively support the efforts of platform-neutral patching service providers.** Software vendors will benefit from the extra help testing patches offer and will gain the freedom to concentrate on creating software rather than distributing it. Customers gain added assurance that patches are thoroughly tested by more than one organization.
- **Managed security service providers should use patch management to diversify and increase LAN penetration.** Partnerships between patch-management vendors and large service providers IBM, ISS, Solutionary and Symantec; vulnerability management vendors Counterpane, iDefense, NetSec, TruSecure, Qualys and Foundstone; and desktop support providers Dell, Sony and Hewlett-Packard add value on all sides.
- **Deliver a marketing message focused on patch management and policy compliance.** These are stronger enterprise purchase drivers than configuration control. Enterprises do not yet feel the pain or the necessity to tightly control desktop configurations and will struggle to cost-justify microcontrol over desktops, in particular. More data is needed to prove that the root cause of network problems is split between software version and software configuration.
- **Patch management vendors should focus on adding platform and application support, fostering open relationships with each vendor with regard to the patch release process.** Enterprises need to patch more than just the operating system. Wide platform and application support is a key feature of leading vendors in this market.

## Enterprise Recommendations

- **Look further than your platform and application vendors for patch-management solutions.** The free patch and software distribution capabilities that come bundled with platforms are not necessarily cheap to run. For example, SUS has fewer centralized management features and you will need to run more than SUS to cover all your platforms.
- **Use patch and configuration management to reduce IT costs and improve host security.** Audio files, P2P file-sharing programs, unauthorized network protocols and services are indicators of loosely enforced host security policies. Vendors such as Citadel and PatchLink control these and many other aspects of the desktop and server, acting as an effective mitigator of network integrity and availability risks.
- **Roll out patch and configuration management using a phased approach.** A pilot and subsequent phases allow time for testing agents, patch process and configuration control features with each platform.
- **Integrate patch and configuration management with asset management, software distribution and workflow processes.** Patching and managing configurations is more about process than technology. Consider how to integrate with these processes to avoid redesigning them down the road.

## IV. Further Reading

### **Yankee Group Security Solutions & Services Reports**

*Vulnerability Management: Processes Strengthen IT's Security Performance*,  
November 2003

*Preventive Steps for Securing Corporate Networks*, July 2003

*The Three Phases of Security: Product, Pervasive and Persistence*, June 2003

## The Yankee Group

### World Headquarters

31 St. James Avenue  
**BOSTON, MASSACHUSETTS** 02116-4114  
T 617.956.5000  
F 617.956.5005  
info@yankeegroup.com

### Regional Headquarters

#### North America

31 St. James Avenue  
**BOSTON, MASSACHUSETTS** 02116-4114  
T 617.956.5000  
F 617.956.5005  
info@yankeegroup.com

951 Mariner's Island Boulevard, Suite 260  
**SAN MATEO, CALIFORNIA** 94404-5023  
T 650.522.3600  
F 650.522.3666  
info@yankeegroup.com

#### EMEA

55 Russell Square  
**LONDON WC1B 4HP**  
**UNITED KINGDOM**  
T 44.20.7307.1050  
F 44.20.7323.3747  
euroinfo@yankeegroup.com

### For More Information

T 617.956.5000  
F 617.956.5005  
E-mail: info@yankeegroup.com  
Web site: www.yankeegroup.com

### Advisory Services

Yankee Group advisory service annual memberships offer clients direct, easy and frequent analyst access and one-to-one expert guidance.

Advisory services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, research reports, forecasts, research notes and regular audioconferences on relevant topics.

We offer advisory services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

### Decision Instruments

The Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

#### Trackers

Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

#### Surveys

Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

#### Forecasts

Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

### Signature Events

The Yankee Group's signature events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

### Consulting Services

The Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine advisory service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged the Yankee Group for consulting services in order to hone their corporate strategies and maximize overall return.

The Yankee Group believes the statements contained in this publication are based on accurate and reliable information. However, because our information is provided from various sources, including third parties, we cannot warrant that this publication is complete and error-free. The Yankee Group disclaims all implied warranties, including, without limitation, warranties of merchantability or fitness for a particular purpose. The Yankee Group shall have no liability for any direct, incidental, special, or consequential damages or lost profits. This publication was prepared by the Yankee Group for use by our clients.