YANKEE GROUP REPORT

Application Infrastructure & Software Platforms
July 2005
by Laura DiDio, Application Infrastructure & Software Platforms Senior Analyst,
ldidio@yankeegroup.com, 617-880-0265

2005 North American Linux and Windows TCO Comparison Report, Part 2: Hardening Security Is Key to Reducing Risk and TCO

Executive Summary

Decision Point:	Best Practices: Making the Right Linux/Windows Migration Decisions
The Bottom Line:	Security is one of the fundamental components of the network infrastructure. Windows security has reached near parity with Linux security. Microsoft can never declare victory in the ongoing security wars and must maintain constant vigilance. At the same time, Linux shops should not be lulled into sense of false complacency.
Who Should Read:	SMBs, enterprises, business decision influencers and purchasing managers, vendors, CEOs, CIOs, CTOs

IT Global Practice Leader: *Brad Hecht*, *bhecht@yankeegroup.com*, 617-880-0306

Corporate enterprises rate Windows security nearly on par with comparable Linux networks, according to the findings of the Yankee Group 2005 North American Linux and Windows TCO Comparison Survey.

Our independent survey polled 550 IT managers and C-level executives at North American firms in the United States and Canada. The results for Microsoft are notable because of the dramatic improvement in its score compared to our 2004 Linux, UNIX and Windows TCO Comparison Survey *conducted 15 months ago.*

In 2005, using a scale of 1-to-10 (with 1 being the least secure and 10 being the most secure), respondents rated the overall security of Linux as 8.3, while Windows garnered an average score of 7.6 (see Exhibit 1). The 2005 survey reveals that users found a 100% improvement in Microsoft's security in the past 12 months. This is the clearest indication to date that Microsoft's Trustworthy Computing Initiative, improved patch management distribution schedule, along with inclusion of anti-spyware and anti-virus capabilities in its software, results in a noticeably increased perception that Windows now offers a more secure environment.

In the 2004 survey, the Windows operating system, which is under near constant assault from hackers, had a 3.5 security average, lagging far behind the relatively pristine Linux environment, which had a 9.2 security rating.

This year, Linux averaged a rating of 8.3, edging out Microsoft with a healthy and respectable score—but its slight slippage from the 9.2 rating posted in the 2004 poll is a warning to corporate users that Linux and open source networks are not immune to hackers and rogue code.

Security is one of the fundamental components of the network infrastructure that will negatively or positively impact a business' daily operations and total cost of ownership (TCO). No software code or hardware device—whether it's proprietary or open source—is invulnerable.

Other survey highlights include:

- ***Recovery time:*** *It takes network administrators 30% longer—or approximately 4 hours—to bring their Linux servers back online following a security attack, compared to a Windows server. In the majority of the cases, the fault lies not with the underlying Linux operating system but with poor documentation and support.*
- ***Patch management:*** *This is another area in which Microsoft's Windows scored high marks for improvement. Survey respondents reported they have reduced the time spent on applying and distributing Windows updates and patches by 50% to 80% since Microsoft went to a monthly schedule of patch management releases in the fall of 2004. Additionally, the availability of free Microsoft patch management utilities means there is no incremental cost to the user. Although patch management issues have eased for Windows networks, they are worsening for Linux servers. Linux IT administrators report they spend on average 15% to 23% longer—approximately 2 to 5 hours more per week—on patch management distribution compared to the same period in 2004.*

Exhibit 1.

Microsoft Security Improves, Users Rate Linux and Windows Server Security Nearly Equal

Source: Yankee Group 2005 North American Linux and Windows TCO Comparison Survey

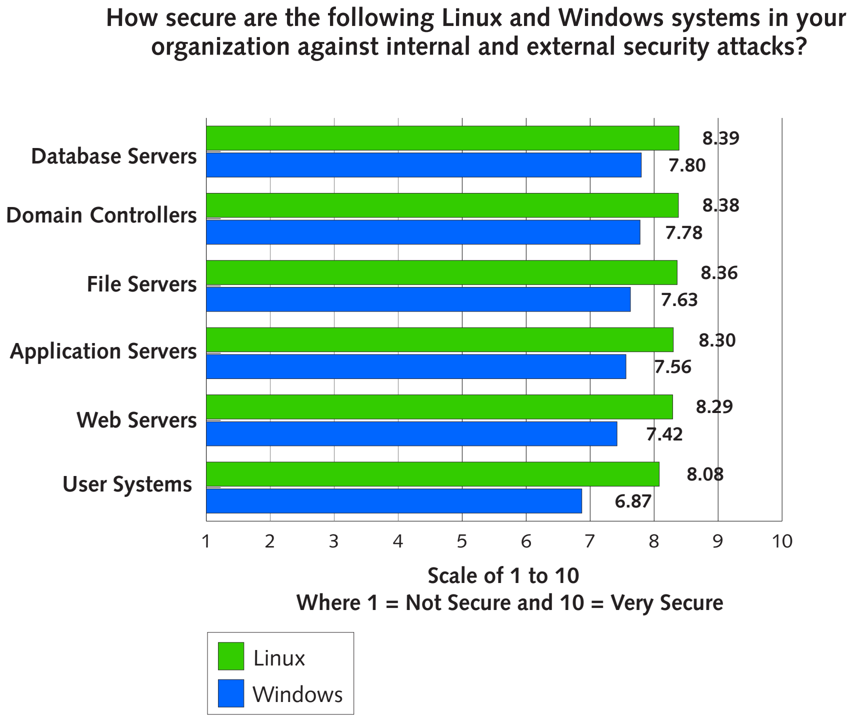


Table of Contents

I. Introduction

Vendors and corporate businesses bear equal responsibility for computer and network security. Microsoft must continue to invest in security; it cannot relax its vigilance for a moment. Linux distribution vendors are well advised to follow Microsoft's lead and invest heavily in security—paying particular attention to improving documentation and patch management. The number of Linux-specific hacks spiked sharply in the last year. This trend will continue as Linux gains more mainstream adoption.

Businesses must do their part. The most security-hardened operating systems can be undone in a moment of carelessness or disregard. Complacency is the biggest threat facing Linux users. Companies must implement and enforce computer and network security policies and procedures, regardless of whether or not a company runs Linux, Windows or a combination of both. Even the most secure code won't protect an organization whose administrators fail to take the appropriate security measures or whose end users don't adhere to corporate security policies.

Ironically, by virtue of the near-incessant assaults on the Windows, Internet Explorer and Office code, Microsoft now has some of the best security, documentation and fast comprehensive patch management in the industry.

Microsoft knows it is at war with hackers. In response, 2.5 ago, it launched an all-out offensive when it implemented the Trustworthy Computing Initiative. At the time, Microsoft and its corporate and consumer users took this unprecedented step and—although their Windows networks are most vulnerable to attack—they now boast some of the most hardened security code and computing practices.

II. Data/Analysis

Security and Patch Management

Specific security queries yielded the biggest surprises in our survey. Respondents gave Windows surprisingly high marks for security, patch management and recovery time. Users scored Microsoft security substantially higher in this year's survey than in the 2004 survey. In 2004, users gave Windows XP, Windows 2000 Server and Windows Server 2003 security an average rating of 3.5 on a scale of 1 to 10, with 1 being the least secure and 10 representing the most secure. In 2005, Windows achieved an average security rating of 7.6 and substantially narrowed the gap between itself and Linux, which had an average rating of 8.3.

No vendor—particularly Microsoft, which is the number-one target for hackers—can ever declare victory in the ongoing security war. Microsoft will always have to maintain its vigilance and continue to invest in security. Microsoft's security initiatives include: 1) the Trustworthy Computing Initiative to harden the core OS kernel; 2) the decision to release patches on a monthly rather than weekly basis (which is more manageable for IT administrators); and 3) the decision to provide the Windows Server Update Services (WSUS) for free. These initiatives are having a positive net impact.

Linux's security ranking slipped from an average 9.2 rating from last year's survey to a still very respectable 8.3 in the current poll. The slippage, although slight, is significant because it reflects the increasing number of Linux- and open-source-specific hacks in the past 12 months. These developments should warn corporations that they must apply and maintain the same computing practices in their Linux environments as they do in Windows and Unix networks.

Windows Systems Recover More Quickly from Security Attacks

Respondents indicated that network administrators were able to restore Windows servers approximately 30% more quickly following a security attack than their Linux counterparts (see Exhibit 2).

Yankee Group asked survey respondents to quantify the amount of time it took IT administrators to restore operations among Linux and Windows file servers, application servers, database servers, domain controllers, web servers and user systems. In every instance—except for one, domain controllers—the restoration process was quicker for Windows servers than for Linux servers. The disparity was most apparent in file servers and web servers.

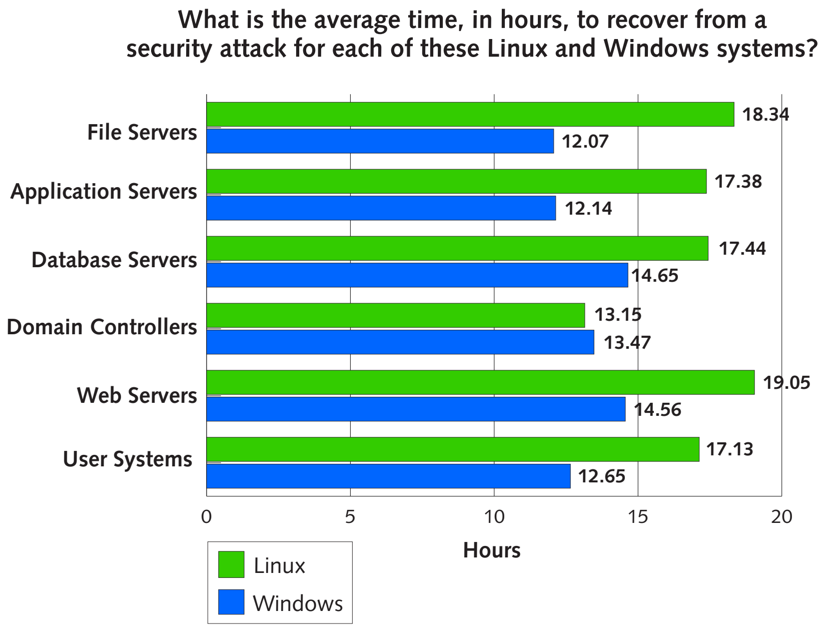
It took administrators 18.3 hours to restore a Linux file server following a security incident, compared to a recovery time of just more than 12 hours to bring a Windows server back online. On the client side, administrators needed 17.1 hours to restore Linux desktops versus 12.7 hours to fix a Windows desktop system. Domain controllers were the one device in which Linux servers came back more quickly than Windows—an average of 13.2 hours for Linux compared to 13.5 hours for Windows.

Time to recover from a security attack does not necessarily reflect inherent flaws in the core Linux kernel. Corporate customers said that, in many instances, the extra time needed to restore Linux servers was attributable to poor documentation of Linux security flaws. This shows that Linux administrators spend more time searching for the appropriate documentation and available security patches to restore a Linux server. By contrast, customers can check Microsoft's knowledge base and regularly updated list of security alerts and available patches.

Exhibit 2.

Windows Servers Recover from Security Attacks 30% Faster than Linux

Source: Yankee Group 2005 North American Linux and Windows TCO Comparison Survey



In the rare instance when it took a firm longer to restore a Windows file server from a security attack than from a Linux server, the primary reason was that the Linux server environment was newer and frequently contained more robust network equipment. One administrator told Yankee Group that his Linux file servers came online more quickly because of the NAS devices, while his Windows servers used the older tape backup equipment, which takes longer to restore than NAS.

Windows vs. Linux Security User Case Studies

Company A

Company A is media and entertainment corporation headquartered in New York City with 5,000-plus end users in more than 50 locations. The company has a mixture of Linux and Windows servers, a Windows PC desktop environment with a sprinkling of Apple Macintosh client machines. The corporation has 10 dedicated Windows administrators. Linux security and management issues are handled by Unix administrators.

Windows security TCO: Improvements to Windows patch management and free WSUS enabled Company A to cut patch management distribution time by 80% at no incremental cost to the organization. Additionally, enhancements to Active Directory security and management cut management time by an estimated 22% and tangibly improved overall security.

Linux security TCO: The relative newness of Linux, coupled with various Linux distributions and applications, constitute more of a security and patch management challenge and represent a higher TCO than the comparable Windows environment, according to Company A’s director of IT and security operations. The firm uses a variety of third-party security tools, including Sunbelt Software’s Security Scanner and eEye’s Retina Network Security Scanner to uncover any Linux vulnerabilities. In the event that any are discovered, the Unix administrators research the problem, then test and apply the fixes for the specific Linux distribution or application.

The administrators spend too much time—roughly 22 hours each quarter, or 88 additional hours annually—researching, testing and applying the appropriate patches for the Linux networks. Company A’s network administrators make approximately $85 per hour. That works out to $7,480 more each year, per administrator, to apply patches to the Linux environment compared to the Windows environment.

One major advantage of the Linux environment: the firm’s Linux servers can recover from a security attack on a Linux system in half the time that it takes to recover from a Windows system. This is not due to any inherent flaws in Windows; rather, it’s because the Linux servers are newer and they are in a NAS configuration. The older Windows servers use tape backup for storage, and the older technology is much slower than NAS, the IT director noted.

Company A’s overall security infrastructure: This firm recently completed a security audit and assessment review to determine the specific risks associated with numerous security issues in its Web server environment. Nearly two-thirds (65%) of Company A’s web servers are Linux; 35% are Windows. The audit revealed the company had “systemic web security issues.” Surprisingly, 90% of the security issues were related to the Linux server.

According to the director of IT and security operations, “Microsoft Windows servers are one-third of the environment and yet they represent only 10% of the problems. The bulk of the vulnerabilities are based *not* on the Linux kernel itself but on the applications running on Linux, such as Apache, PHP, eCommerce software and SSH.” The network manager was quick to point out that Apache and the open SSH organizations are “fairly responsive.” The company’s Linux security issues are directly attributable to poor documentation and resources to track and resolve multiplatform/application security issues in the Linux environment. “The most challenging [Linux/open source security] issue confronting us is that presently, there are few aggregate sites like Security Focus that we can go to check vulnerabilities across all platforms,” he said.

Like many Linux and open source users, this firm is confronted with an increasing array of open source offerings that have varying degrees of integration and interoperability. For example, the IT director noted that in his experience, there is close compatibility between Mandriva (formerly Mandrakesoft) and Red Hat. Similarly, Debian and Gentoo are closely aligned, while “Slackware is off on its own and is closer to BSD. Debian probably has the best software update management. Red Hat and SUSE come next. All in all, it can be very daunting to unravel the compatibilities or incompatibilities in various Linux and open source distributions and applications,” the IT director said. “And once you’ve gone down the customization path, maintenance and upgrade issues become more difficult.”

By contrast, the IT director said the firm realized tangible TCO economies of scale in Windows’ often-maligned proprietary architecture. He attributes the Windows TCO savings to the standardization inherent in the Windows code base.

The IT director gave Microsoft and its Windows Server 2003 and Active Directory security high marks across the board for their embedded security, configuration management, responsiveness, improved patch management distribution, superlative documentation and overall hardening of the core OS kernel.

“We’re spending a lot less time on patch management now. In the NT 4.0 time frame, it took us 2.5 days to patch 200 servers. Now the same process can be done in a half-day for the same number of systems, thanks to Group Policies—so we’ve got an 80% reduction in time at zero cost because WSUS is free,” the director said.

Windows reliability has likewise improved. “We only take our servers down when we choose to take them down,” the IT director said. Windows reliability is better “both in terms of a dramatic reduction in the number of unnecessary reboots and because a much higher percentage of patches in Windows Server 2003 do not require users to reboot [the server] to install a patch.”

Windows/Active Directory Security Enhancements Increase TCO and Flexibility

The media firm is running Active Directory version 1.1, which enhances overall security configuration management by adding an important TCO component: flexibility.

It now has a variety of options to configure and manage the security of local and remote sites and services. It has the option to designate that a single server act as domain controller to handle multiple zones. “This not only provides us with a higher degree of security but it eliminates multiple points of failure and saves me significant configuration time,” said the IT director. Once the company installs Windows XP Service Pack 1, it will further harden Windows’ native security based on the extra access to the enumeration facility. This enables administrators to block users from even seeing a file. “If they can’t see it, they won’t know it’s there and they won’t attempt to hack it.”

Overall, this IT director applauded Microsoft for hardening security, providing free update services and more convenient monthly patch management schedule. He noted that he’s equally wary of every software vendor’s security.

“Everyone’s software is equally buggy because of complexity of integration, and we’re also seeing hackers and legitimate researchers focusing on finding and exploiting security flaws in the application layer of the stack across all operating systems platforms, including Linux,” he noted. He’s disturbed by the sharp increase in the number of open source hacks in the last 8 months.

“Web servers are an important component of our business, and since the end of 2004, we’ve seen a ton of exploits directed against PHP [an open source Web scripting language.]” One such attack last December used a Google search engine to target a number of sites running the open source phpBB bulletin board. “That one open source hack took down 40,000 sites. And it was a wake up call for our organization: no operating system is immune,” the IT director said.

Company B

Company B is a small college in central Washington State with approximately 2,500 students. The college has an extremely proactive stance regarding implementing, adhering to and enforcing computer security policies and procedures. Its security policies and procedures are rigorous and are comparable to those of a leading-edge, security-conscious enterprise.

The IT administrator’s views on the TCO aspects of security challenge conventional wisdom about both Windows and Linux. He readily acknowledges that the college’s “Linux systems are less of a target [than Windows],” but says the college has no plans to do a wholesale switch from Windows to Linux.

As an academic institution, the college gets “significant educational discounts” from Microsoft. Surprisingly, the IT director believes that proprietary Windows software has a security advantage over open source.

“From a security standpoint, I think open source is a liability because of the nature of the code. It really is open and well published and ‘out there.’ It’s much easier for hackers and malicious users to write or create content that abuses Linux systems,” he asserted.

The college has had very few security attacks—only “three server incidents” in the last 5 years and approximately “50 desktop incidents” and those were relegated to a specific set of clients and one or two servers. The IT director said he maintains a constant state of vigilance for professional and personal reasons. “A significant security attack could be my job on the line. I take it very personally,” he said.

The traditionally tight academic IT budgets do not mean that a college or university has to sacrifice security. The college’s annual IT budget is $500,000 and server upgrades are done on a 4-year rotating basis.

The college has a 240-page security standards document that the IT director and his supervisor co-wrote in 2004. How did a small college manage to produce such exhaustive documentation, and how much did it cost? The answers are: “very easily” and “nothing.”

The college used simple ingenuity and initiative. “The State of Washington gave us a sample of their policies and procedures and we based our documentation on that,” he said. “We continually modify our security policies and procedures as needed.”

The document covers all areas of the college’s on-campus security and provides for actions—from warning to expulsions or firings—in the event that staff or students violate policies.

TCO of Microsoft Windows: The IT director noted that Microsoft’s Trustworthy Security Initiative is yielding tangible results. “The Microsoft products are definitely working more smoothly. I give them a higher average across the board for improved security, deployment, training and patching,” he said.

He especially praised the improvements in patch management. “We researched a lot of third-party tools and were not satisfied with the integration and distribution,” he said. The college settled on Microsoft’s WSUS and is very satisfied.

Currently, the college IT director spends about “20 minutes per month to configure and deploy client side patches” while on the more sensitive servers, he monitors every patch to each of the 35 servers, which consumes a total of “4 hours per month.” Although this is a significant time savings of about 60% compared to 18 months ago, he’d like to spend even less time applying updates, since he does it on his own time, after hours.

“The over-arching improvements Microsoft has made to security, Active Directory and manageability have lowered our TCO by about 25%. At this point, I’d give Microsoft a 9 out of 10 rating for security—it’s the best it’s ever been, and the Linux distribution vendors will be hard pressed to keep pace, when and if they are confronted with the same level of platform-specific hacks,” the IT director said. Microsoft products also deliver a cost-effective TCO because of the ready availability of skilled Windows administrators and embedded third-party tools and utilities, which allows the college to save on the cost of incremental third-party tools.

III. Conclusions

Security will remain one of the most fundamental components that positively or negatively impacts daily network operations and overall TCO and ROI.

To aggregate our survey findings:

- No software operating system, application or hardware device is hack-proof.
- Human error (i.e., failure to institute and adhere to computing security practices; failure to perform regular security checks, failure to install the latest patches and improper security configurations and settings) can negate even the best Windows or Linux security controls.
- Security is the responsibility of all. Vendors and corporate customers bear equal responsibility for the security of devices and networks.
- Microsoft's Trustworthy Security Initiative is reaping dividends. Windows XP and Windows Server security showed vast improvement in the last 12 months. This trend will continue as the Microsoft security team grows to more than 500 strong. Microsoft just completed its acquisition of anti-virus vendor Sybari.
- Windows and Linux security are nearly equal. Corporate customers—from micro-SMBs to the largest enterprises—now rate Windows security nearly equal to Linux. However, Yankee Group cautions that security is fluid, not static. An especially pernicious hack to either environment will cause either Windows or Linux' respective ratings to plummet in users' estimations.
- Windows servers recover approximately 30% faster (about 4 hours) from security attacks than Linux servers. This is mainly due to Microsoft's superior documentation, fast response time and enhanced patch management services. It underscores the need of both Linux vendors and users to quickly improve security documentation. They must work proactively and collaboratively to create aggregate cross-platform web sites that corporations and consumers can scan quickly and efficiently for known issues and patches affecting various Linux and open source distributions.
- Linux patch management is becoming more time-consuming and complex, particularly for businesses that have modified the core Linux OS kernel, but lack adequately trained skilled IT staff to administer upgrades. Based on our survey findings and anecdotal customer interviews, Yankee Group anticipates that Linux patch management issues will get worse before they get better.
- Linux documentation remains poor. Individual Linux distributors, such as Red Hat, Debian, Mandriva, Turbolinux and others, are responsive and proactive in issuing the appropriate security alerts and patches in a timely manner. Red Hat in particular has an extensive and growing knowledge base of known issues. However, there are few aggregate sites that identify cross-platform security issues that corporate Linux users can turn to for support. Companies like Novell, which offer subscription-based support services, can improve access to documentation, upgrades and ongoing maintenance.
- Linux does not appear ready for desktop primetime. In many ways, Linux's evolutionary stage—in terms of support—is where Windows was 10 years ago.

Recommendations

Vendors and corporate users must make Windows *and* Linux operating system security a top priority.

- **Windows is the top desktop and server operating system environment.** Therefore, it will continue to be the number-one target for hackers. Neither Microsoft nor its Windows users can relax their vigilance. Corporate users must perform regular security/risk assessment analyses at least annually, or more often if needed.
- **Linux-specific hacks are on the rise.** As in the Windows environment, the hackers and the hacks are more pernicious than ever. However, the biggest threat confronting Linux shops is *complacency***.** Corporate customers with Linux networks should adopt and maintain the same proactive security measures, security policies and enforcement as their Windows, Unix and Macintosh counterparts.

Corporations should take the following steps to remain secure:

- **Get training.** Corporations must not skimp on security. Make sure your internal IT staff has the appropriate training and certification. Organizations that cannot afford training for their entire staff should send the most experienced security professionals, who can then train their colleagues.
- **Keep up to date on latest patches and anti-virus releases.** All companies, regardless of operating system environment, should keep the latest anti-virus software up to date, download the latest patches to further secure their networks, and install the appropriate authentication, tracking and authorization mechanisms. This recommendation may seem obvious and intuitive; however, Yankee Group regularly consults with corporations that ignore these warnings and end up regretting it.
- **Perform regular security audits and risk assessments.** This is time consuming and expensive, but there's nothing more important than defending your firm's intellectual property assets and corporate data. IT administrators and security professionals who fear that their CTOs and CIOs will balk at the resources and expenditures required to perform these tasks should quantify the hourly downtime, staff hours, cost of data recovery and data losses the company could incur on an hourly basis if either the Windows or Linux systems fall prey to an internal or external hack.

No company can construct a 100% hack-proof network. But by strictly adhering to computer security best practices, imposing and enforcing security policies, and performing regular security audits and risk assessments, corporations can eliminate the vulnerabilities in their Windows and Linux networks and reduce the risk to an acceptable level.

IV. Further Reading

Yankee Group Reports

2005 North American Linux Windows TCO Comparison Report, Part 1, April 2005

Indemnification Becomes Open Source's Nightmare and Microsoft's Blessing, November 2004

Linux, Unix and Windows TCO Comparison, Part 2, June 2004

Linux, Unix and Windows TCO Comparison, Part 1, May 2004

Enterprises Worldwide Finally Plan to Increase IT Spending on Long-Overdue Software Upgrades, March 2004

Yankee Group DecisionNotes

Linux Is a Strong Contender, but Windows Is Still the Number-One Server OS, April 2005

How SMBs Should Choose Between Linux and Windows, March 2005

Think Before You Migrate: Due Diligence Required for OS Migration, March 2005

Windows Small Business Server 2003 Is Top Software Server Choice for SMBs, June 2004

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

Decision Services

Yankee Group Decision Service annual memberships offer clients access to research and one-on-one expert guidance.

Decision 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, published research and Online Decision Forums on relevant topics.

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

Decision Instruments

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

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

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 Decision 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 Yankee Group for consulting services to hone their corporate strategies and maximize overall return.

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. Yankee Group disclaims all implied warranties, including, without limitation, warranties of merchantability or fitness for a particular purpose. Yankee Group shall have no liability for any direct, incidental, special or consequential damages or lost profits. This publication was prepared by Yankee Group for use by our clients.