There's Nothing Like the Real Thing: Genuine Software Is a Win-Win for Customers, Microsoft and Partners

yankee group
www.yankeegroup.com

by Laura DiDio | January 22, 2007

Executive Summary

There is no more pervasive or pernicious problem plaguing the software industry than that of counterfeit or pirated software operating systems and applications.

Microsoft's genuine software programs—which are now more than a year old—enable customers to quickly and easily verify if they are running an authentic version of Microsoft Windows or Office, using a validation mechanism through the Windows Genuine Advantage (WGA) and Office Genuine Advantage (OGA) web sites. And at the same time, these programs enable Microsoft to responsibly protect its own intellectual property.

However, the issue of genuine software—that is, customers running legitimately licensed software operating systems and applications as opposed to pirated or purloined software—is frequently miscast and misunderstood.

It is an issue that engenders fear and loathing among customers and software vendors alike. Corporate and consumer customers rightfully fear that, if caught, they may be subject to costs and other penalties by their respective vendors and the Business Software Alliance (BSA), which tracks illegal software trafficking on behalf of the vendor community. Vendors are equally fearful and outraged—not just for the obvious lost revenue, but also for violations of intellectual property rights, incompatibility problems and the service and support issues that arise as a direct consequence of unlicensed and illegal software.

What is not in dispute is the well-documented and publicized fact that illegal or pirated software costs software vendors—particularly the largest vendors such as Microsoft, Oracle, SAP and others—billions in lost revenue each year.

As Exhibit 1 indicates, the use of counterfeit and pirated software is pervasive. According to Yankee Group survey data, over half—55%—report they have had some instances of counterfeit or pirated software in their organization at some time. Of that figure, 15% acknowledge that the situation was severe enough to cause them to delay contract negotiations and product upgrades to address the situation.

According to the BSA, 35% of the world's software is pirated. Of the 97 countries worldwide that the BSA tracks, more than one-half—51 nations—have a median piracy rate of 64%. This means that, particularly in emerging and developing nations, two-thirds of all software in use either is pirated or is a faulty facsimile of the original package. Or to put it in monetary terms, the BSA states: "for every 2 dollars worth of PC software purchased legitimately, 1 dollars worth was obtained illegally." In sheer numbers, the BSA estimates that software vendors and the associated service and support organizations lose a staggering $50 billion or more annually to software piracy.

This custom publication has been funded by Microsoft.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

This Yankee Group Consulting Report is published for the sole use of Yankee Group clients. It may not be duplicated, reproduced or transmitted in whole or in part without the express permission of Yankee Group, 31 St. James Avenue, Boston, MA 02116. For more information, contact Yankee Group: info@yankeegroup.com; Phone: 617-956-5005. All rights reserved. All opinions and estimates herein constitute our judgment as of this date and are subject to change without notice.

Executive Summary (continued)

However, software vendors are not the only losers. Consumer and corporate users also suffer the consequences of using purloined or illegal software, although this fact is much less publicized. Consumers and businesses that deploy counterfeit software put themselves, their end users, business partners and suppliers at serious risk for:

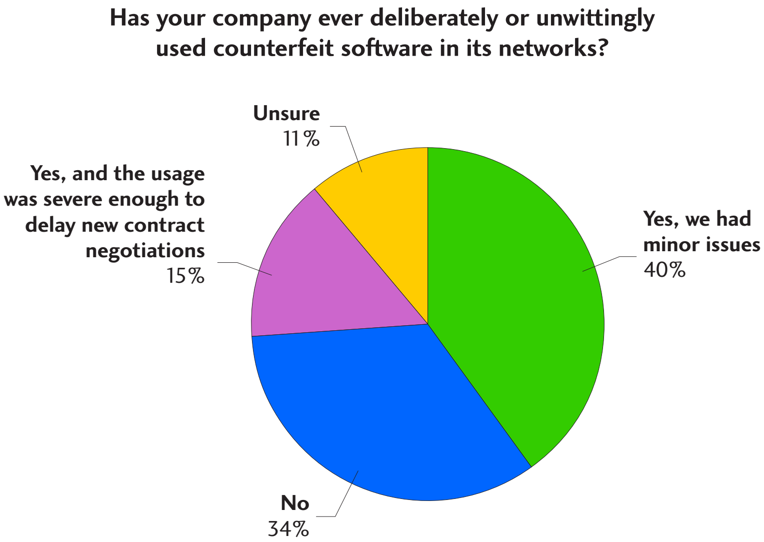
- Network downtime and lost data increases when the counterfeit software malfunctions.
- Technical service and support and interoperability issues involving counterfeit software typically take longer to resolve because either the gray market source is long gone or the legitimate software vendor will spend more time trying to troubleshoot.
- Businesses that knowingly or unwittingly use counterfeit software are at increased risk of litigation from business partners, suppliers and customers in the event their network operations are adversely affected when something goes awry with the pirated software.
- Non-genuine software also raises the risk of incompatibility with legitimate Windows and Office patches, fixes and updates.
- The Yankee Group 2005 North American Linux Windows TCO Comparison Survey and subsequent customer interviews indicate that when problems arise with counterfeit software, IT administrators typically require 20% to 30% more time and labor to identify and resolve the problems—at a monetary premium to the business.

In summary, using legal software is a win-win for customers, vendors, OEMs, resellers and service and support providers. Microsoft's Genuine Software Initiative program provides the framework, mechanism and documentation to help consumers and businesses become legal, stay legal and realize optimal performance. In turn, this will keep their Windows desktop operating systems, server operating systems and Office productivity applications running at peak efficiency. Every organization should avail itself of the WGA and OGA program web sites to become legal and stay legal.

Exhibit 1

Counterfeit Software Plagues Many Corporations

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



© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

Table of Contents

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

I. Genuine Software Initiative Fights Piracy

Software piracy and the use of counterfeit software—whether knowingly or unwittingly—are illegal activities. They are not victimless crimes.

Anytime a consumer or a corporation deploys unlicensed or counterfeit software, they cheat proprietary software vendors out of their rightful royalties. However, such customers may also ultimately find that they victimize themselves. Counterfeit and pirated software puts PCs, laptops and networks at a higher risk for malfunctions, increases downtime and heightens security threats from viruses and other forms of malware.

Proprietary vendors such as Microsoft have every right to protect their intellectual property and the millions of research and development (R&D) dollars by taking measures to protect their investments and their shareholders' investments by ensuring that customers use only legitimate, properly licensed software.

The mechanism by which Microsoft chose to battle piracy was its Genuine Software Initiative.

Genuine Software Initiative Evolves

The Genuine Software Initiative is an ongoing work in progress. Microsoft has continually refined, enhanced and expanded the program as needed since it first launched 18 months ago.

The Genuine Software Initiative focuses the company's many activities and investments directed at combating software counterfeiting and other forms of software piracy into a singular initiative with a common goal. The initiative concentrates on increasing investments across three strategic areas: education, engineering and enforcement. For example, WGA, OGA, legal enforcement and various channel and consumer programs are under the Genuine Software Initiative umbrella.

Windows Genuine Advantage and Office Genuine Advantage

Microsoft can quickly create a match between the PC or laptop's hardware profile and the 25-character product key (located on the Certificate of Authenticity), which Microsoft stores and checks against future activation and validation attempts. Microsoft does this to ensure that no one else—whether it's a coworker or a malicious hacker—can use the legitimate product key to activate a counterfeit or non-genuine copy of Windows or Office.

WGA and OGA notifications display alerts to inform users in the event they are running pirated copies of Windows or Office. In addition, these notifications provide users with a mechanism to pay for a legitimate copy of Microsoft software.

Starting on October 27, 2006, Microsoft's Download Center began requiring mandatory validation of certain Office downloads. Office Online templates downloaded from within the Office 2007 applications will also require validations. In addition, as with Windows Update, Office Update will also require validation beginning in January 2007.

If consumers find that they are using a non-genuine version of Office, they have several choices on how to proceed. Qualifying customers who fill out a counterfeit report, provide proof of purchase and send in their counterfeit CDs may receive a genuine copy at no cost. Customers who learn through the OGA validation process that they unknowingly acquired a counterfeit version of Office (and do not qualify or chose not to take advantage of the complimentary offer) have a few options. They can license an OGA kit for Microsoft Office Professional Edition 2003 at $359, for Microsoft Office Small Business Edition 2003 at $269 or for Microsoft Office Student and Teacher Edition 2003 for $139. (These are US prices only and do not include taxes. International prices will vary.) This legalization offer became available in November 2006.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

It is true that the words “Microsoft,” “mandatory,” “validation,” “privacy,” and “piracy” used in the same sentence can raise the eyebrows of some skeptics.

In fact, Microsoft’s Genuine Software Initiative programs (i.e., WGA and OGA) are open and straightforward. Microsoft encourages customer feedback via its web site and technical support lines for anyone who has questions or encounters problems with the validation process.

Such was the case in June 2006 when Microsoft issued a software update to quell users’ concerns about privacy aspects of the validation process. The test version of the validation tool became the subject of controversy when users discovered that the tool essentially “phoned home” and—unbeknownst to them—made daily contact with Microsoft servers, checking for a new update for WGA, irrespective of whether or not their software was legitimate.

In response, Microsoft issued a software update to the Windows Genuine Advantage tool in late June; the finished software no longer makes daily contact with Microsoft’s servers. Windows Genuine Advantage is installed with the consent of the user and only notifies the user if a proper license is not in place.

That is also the case with the newly released Office Genuine Advantage program, which is currently available in 26 languages worldwide. As of October 27, 2006, OGA requires all users to validate the legitimacy of their Office system applications. And beginning in January, Microsoft will ask users of Office Update to complete the validation process to ensure that their Office software is legitimate.

Customers who utilize the Genuine Software Initiative program can log onto the web site and participate in and access forums that are specifically tailored to address any technical problems users may experience. Microsoft designed the validation process to be quick and simple. But as with any software tool or application, it is not perfect. Should users encounter problems, Microsoft has several methods for customers to provide feedback and resolve their specific issues.

Microsoft’s WGA validation problems forum provides a venue for customers to voice their complaints directly to Microsoft and to seek help for any problems they encounter with the validation process. Not surprisingly, with such a new software initiative, some IT administrators have found the process challenging. And there have been some technical glitches.

Microsoft engineers work diligently to address technical problems as they arrive.

For example, some users have received false-positive notifications that their software was counterfeit, when in fact it was legitimate. However, the actual number and percentage of false positives is very small, given that more than 500 million individual consumers have visited the WGA site.

Microsoft engineers report that some of the false positives stem from cryptographic errors related to digital signatures. Some users also reported false positives that occurred due to a specific issue—which has since been fixed—related to the QuickClean utility contained in McAfee’s Internet Security Suite.

McAfee’s QuickClean frees disk space by eliminating unnecessary cached files, temp files and other things that slow system performance. Unfortunately, this particular utility also eliminated the information the Windows Genuine Advantage tools used to identify genuine, licensed copies of Windows XP, resulting in some users receiving a false-positive notification of counterfeit software this past summer. McAfee issued a patch on August 30, 2006. Consumers or corporations that use the McAfee utility should download the patch before running the Microsoft WGA or OGA notification tool.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

II. Piracy Is a Worldwide Problem

Legitimate, legally licensed software benefits everyone. By deploying genuine software, consumer and corporate users and the OEM and reseller partners can:

- Access the latest product updates and enhancements.
- Gain the ability to get the best deals and discounts when they upgrade or renegotiate their existing software licensing contracts.
- Ensure that they are not leaving "money on the table" or paying additional costs and penalties at contract negotiation or upgrade time.
- Maintain backward and forward compatibility and interoperability with other legitimate software applications and updates.
- Improve system and network reliability and uptime.
- Accelerate technical troubleshooting and problem resolution.
- Improve and maintain system and network security.

Don't Be Fooled

There are myriad reasons—ranging from the sublime to the ridiculous—for how consumers and corporations end up with counterfeit software. The percentage of counterfeit software is lowest in developed geographic regions such as North America and Western Europe, which have 22% and 35% pirated software, respectively, according to the latest BSA estimates.

In emerging regions, the use of counterfeit and pirated software has been raised to the status of art form, with individual consumers and corporations deliberately seeking out pirated or counterfeit software programs.

Central and Eastern Europe and Latin America have the dubious distinction of being tied for first place as the regions with the highest totals of pirated software: 69% and 68%, respectively, according to the BSA. Asia-Pacific rim countries currently have a piracy rate of 54%, the BSA says.

Corporate executives at many firms in developing or emerging nations often take great pride in the fact that such a high percentage of their software is unlicensed or counterfeit. They feel it saves them money and are often unabashedly delighted at the thought of getting something for nothing.

One of the chief reasons for the lower percentage of pirated software in developed geographic regions such as North America, Western Europe and the European Union is that intellectual property protection against copyright infringement, patent infringement and theft of trade secrets is much stronger than in developing nations. And more significantly, intellectual property laws that are already on the books are enforced in these developed areas.

However, central governments in countries in emerging regions—most notably China—are working closely with software vendors such as Microsoft and cracking down and enforcing compliance. But as the BSA notes in its 2006 Global Software Piracy Study, there are limitations to enforcement—even in China. "There is a large heterogeneous market in rural areas outside the central Chinese government's immediate reach in large cities. In the more remote areas, piracy is very high," the BSA study notes. Although most countries have intellectual property laws, the actual enforcement or degree of penalty makes software piracy less of a legal risk in outlying areas of China.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

III. Unwitting Piracy Dupes

Not all instances of software piracy are deliberate. Some users—particularly consumers and small and midsized businesses—are often unwittingly hoodwinked into purchasing what they believe to be genuine software at a discount from online sources ranging from eBay to various web sites that specialize in counterfeit software and malware.

In fact, many of these sites are fronts for gray market outfits which advertise just long enough to stay ahead of law enforcement. Gray market is a term that refers to secondary and unauthorized resellers. Their "products" often look like the real thing, but caveat emptor: There are certain telltale signs that the software is counterfeit. One blatant indication that you don't have a genuine Microsoft product is if there is a label that literally peels off the CD. These online predators typically want to make a quick score from unsuspecting consumers and smaller firms anxious for bigger discounts than what they might normally receive from legitimate resellers, but they conveniently are unavailable when problems arise with their software.

There are also multiple sites that contain bad malware that will actively infect PCs, laptops and servers, resulting in widespread havoc and damage. A partial list follows. However, Yankee Group strongly recommends that you only access these sites using a test system that is isolated from other PCs or servers on the network to avoid infection.

Sites with Reported Bad Malware

Yankee Group does not advise customers to access the following web sites on any production systems. It is advisable that you only access them while using a test system.

http://www.crackfind.com
http://www.mscracks.com
http://www.cracks.thebugs.us
http://www.crackspider.com
http://www.anycracks.com
http://www.serialsbox.com
http://www.newcracks.net
http://www.cracks4all.com
http://www.cracks.spb.ru
http://www.crackportal.com
http://www.seriall.com
http://www.crack-cd.com
http://windows.crack-cd.com

IV. User Case Studies

Organizations and individuals that routinely use counterfeit software give little thought to the potential consequences—unless or until they believe discovery is imminent. Individuals and corporations that deploy counterfeit software do not neatly fit into any singular profile. Counterfeiters are found in every geographic region and in every vertical market. The offenders encompass companies of all sizes, ranging from the smallest small home and offices (SOHOs) to the largest enterprises.

Consider the following case studies compiled by Yankee Group. The offenders range from a large European telecommunications firm, to a midsized bank in Canada, to a midsized US firm, to a US SMB printing company.

© Copyright 1997-2007 Yankee Group Research, Inc. All rights reserved.

Large European Telecommunications Firm: Living Dangerously

Some organizations thumb their noses at rules, believing that the end justifies the means. Such was the case with an executive at a large European telecommunications firm. Yankee Group spoke with the executive when he sought information on the best deal he could expect for Windows and Office per-seat pricing pursuant to renegotiating his Microsoft licensing contract.

"First thing's first: What percentage of your software is illegal, pirated or unlicensed?" we asked. "About 55%," the executive responded unhesitatingly. "You know, of course, that your company is asking for big trouble if you get caught. You may have to pay true-up costs, plus penalties, not to mention that pirated software can wreak havoc with network operations," we persisted.

The executive remained nonplussed. "Well, we've never had any problems. And we intend to get around the issue of the unlicensed and counterfeit software by just upgrading from a Microsoft Select License to an Enterprise Agreement."

In this instance, the telecommunications provider rolled the dice and won. But not everyone will be so lucky.

Midsized Canadian Bank: Day of Reckoning

This is an example of a firm that did not tend to its housekeeping chores—namely performing regular asset management checks to ensure that only licensed and genuine copies of Microsoft software were in use at its 2,000 person financial institution.

Yankee Group received an urgent call from a senior IT administrator at the bank, seeking advice on how to deal with a Microsoft audit scheduled for the next day. Unfortunately, such eleventh-hour panic calls are all too commonplace.

The IT administrator nervously admitted that at least one-quarter (he wasn't sure of the exact amount) of the bank's software was either unlicensed or pirated. He was extremely fearful that the Microsoft auditors would find out and come down hard. The administrator's fears were well-founded. Many organizations would be surprised to learn just how much information their software vendors possess based on a working knowledge of their customers' environments and whether or not there is unlicensed or pirated software in use.

In this case, Yankee Group advised the bank that the only correct and practical course of action was to tell the truth. The bank had let matters spiral out of control and waited until it was too late to rectify its counterfeit and unlicensed software problem.

Any company that finds itself in a similar situation should likewise be truthful with Microsoft or any of its software vendors. Software manufacturers want to retain you as a loyal customer. Never under any circumstances should a company try to destroy evidence—such a deliberate act will make you doubly guilty and will destroy whatever chance it has for leniency.

In the case of the Canadian bank, honesty was the best policy. By volunteering the truth—including the fact that a single individual had inserted the counterfeit software into the organization—the company avoided paying additional costs and Microsoft waived the penalty. However, because of the acknowledged transgression, the bank's contract discount was not as favorable as it could have been. Additionally, it was subject to regular audits for the term of its 3-year licensing contract.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

Small US Printing Firm: Too Good to Be True

This company is a family-owned business with 60 employees that wanted to save money on its software licenses. So when the opportunity arose to purchase counterfeit copies of Office at a 90% discount from a gray market reseller in Flushing, Queens, the company jumped at the chance. Unfortunately, Flushing, Queens is home to large illegal immigrant populations—many of whom hail from the Asia-Pacific region and have ties to highly organized counterfeit rings that operate in China, Hong Kong and San Francisco. Such was the case with this gray marketer.

Along with the company's big discount came big problems. The software behaved erratically, crashes were frequent and there were huge interoperability problems. The printing firm struggled for a month, racking up large amounts of downtime that caused it to delay shipping orders to several key customers. Finally, fed up and frustrated, the head of the company went back to his gray market source to complain—only to find that his contact had vacated the premises and left no forwarding address.

The printing company learned its lesson the hard way, but the company president vows "never to make that mistake again." "I've learned my lesson; it was not worth the time or trouble. Fortunately, there was no lasting damage to our reputation, though we did have to give some of our customers some hefty discounts to compensate for the inconvenience."

Overall, the experience cost the company approximately $10,000 to rectify (including the discounts to its customers and overtime to its network administrator) and a lot of unnecessary downtime.

Midsized US Firm: The Counterfeit Package That Wouldn't Stop Singing

This is a case of the ridiculous, and it illustrates just how problematic it is to troubleshoot counterfeit software.

Despite an explicit corporate policy forbidding the use of unapproved software at its site, one of the company's software developers just couldn't resist downloading what he was assured was a turbocharged version of Windows. However, he and his colleagues got more than they bargained for.

The pirated Windows XP contained a virus that caused the PCs and notebooks in the developers' network to begin playing a badly written and off-key version of "Yankee Doodle Dandy" every afternoon at 3:00 p.m. No amount of troubleshooting would rid the systems of the offending tune, which played for about 20 minutes. The only solution: Wipe the systems and do a clean install.

V. Conclusions and Recommendations

In summary, genuine software benefits everyone. Counterfeit or pirated software works to everyone's detriment.

The fortunes and economic bottom lines of corporate and consumer users, software vendors, OEM and reseller partners as well as the aftermarket technical service and support organizations are materially affected in a positive or negative way by the use of genuine versus counterfeit software. It is wise to take precautions to become legal and stay legal. Using genuine software offers users the best and most comprehensive means to do so.

© Copyright 1997-2007 Yankee Group Research, Inc. All rights reserved.

To reiterate, counterfeit software can:

- Adversely affect PC and network operations, increasing network downtime and the potential for lost data.
- Subject businesses and consumers that knowingly or unwittingly use pirated software to penalties, if caught.
- Cause incompatibility and interoperability issues with legitimate software and heighten the risk that vendor software updates, patches and fixes will not work with the counterfeit copies.
- Require more time and labor to troubleshoot and resolve network problems.
- Commensurately increase PC and network security risks, including instances of viruses, worms, malware and spyware.
- Leave the business vulnerable to lost business and legal action in the event that the counterfeit software affects business partners, suppliers and customers in the course of doing business.

The use of counterfeit software is not a victimless crime. As the above examples and the first-person user accounts indicate, the use of pirated software is risky and wrong on many levels. Individuals and organizations that engage in such activities deprive software vendors such as Microsoft of their rightful revenue and royalties.

At the same time, these consumers and organizations victimize and cheat themselves. If and when problems arise—as they invariably do—with sloppy, ill-constructed counterfeit programs, the users will have no one to blame but themselves.

It's also highly likely that their counterfeit sources will be long gone and unavailable when trouble arises, leaving the hapless users and software vendors to clean up the mess.

In the end, the price and payback for using counterfeit software will far exceed the cost of purchasing genuine software.

Therefore, every organization should ask themselves: "What have we got to lose?" and "Is it really worth the risk?"

Recommendations for Enterprises

Yankee Group strongly advises organizations to be proactive on their own behalf. That means becoming legal and staying legal. The Microsoft Genuine Software Initiative for Windows and Office provides a ready-made mechanism and framework for doing so. In addition, we make the following recommendations.

- **Manage assets.** All individual consumers and corporations should perform regular asset management checks. In other words, be proactive in policing yourself. This is the best defense against pirated software. This will enable you to get a comprehensive overview as to the state of your company's compliance or lack thereof.
- **Only purchase software from Microsoft or approved, legitimate resellers and OEM partners.** If you're surfing the internet and come across a site that's advertising phenomenal, unbelievable discounts, then it probably is too good to be true. Pass. Ultimately, the money, time, effort and energy you save will be your own.
- **Understand licensing contract conditions.** Everyone should also thoroughly review the terms and conditions (T&Cs) of their licensing contracts. If you don't understand something, run it by your firm's corporate counsel. Alternatively, ask Microsoft, your reseller or OEM hardware vendor to explain nebulous phrases. Don't be embarrassed. Volume licensing agreements are notoriously complex and confound even so-called experts. Businesses that engage in merger and acquisition activity should ascertain whether or not and under what circumstances their existing licensing agreements are affected by acquisitions, divestitures and personnel layoffs.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.

- **Check with Microsoft and third-party software vendors for known incompatibility issues with the WGA and OGA notification tool.** Also, if your firm uncovers a bug, immediately notify Microsoft's WGA validation problems forum of the issue as well as any other appropriate third-party software or tools vendor.
- **Notify Microsoft immediately if you receive a false positive during the validation process when you are certain that your software is legal.** There may be several reasons this is happening, but Microsoft needs to know so it can resolve the matter as expeditiously as possible. Don't be afraid to escalate if the problem persists or if your firm feels the response or the response time is inadequate.
- **Frankly discuss any concerns about the Genuine Software Initiative program** with Microsoft, your Microsoft sales representative, reseller or OEM hardware vendor. It is always better to ask questions and raise issues than to listen to rumor and innuendos or suffer in silence.
- **Get educated via forums and user groups.** These are excellent sources of information on known issues and can often provide expert guidance on whether or not a fix is available and where to find it. One cautionary note: Although forums and user groups are very good supplemental resources, businesses should not rely on them as their sole source to resolve technical issues. It is absolutely crucial for businesses to ensure that their internal IT administrators receive the appropriate amount of training on the WGA and OGA validation process.

VI. Further Reading

Yankee Group Link Research:

- *Server Virtualization Part 1: Technology Goes Mainstream, Nets Corporations Big TCO Gains, Fast ROI,* Report, July 2006
- *Unix, Windows and Custom Linux Score Well on Yankee Group 2006 Global Server Reliability Survey,* Report, March 2006
- *Virtualization, Multicore Hardware Technologies Spark Debate on Software License Price Models,* Report, January 2006
- *2005 North American Linux and Windows TCO Comparison Report, Part 2: Hardening Security Is Key to Reducing Risk and TCO,* Report, July 2005
- *2005 North American Linux and Windows TCO Comparison Report, Part 1,* Report, April 2005
- *Indemnification Becomes Open Source's Nightmare and Microsoft's Blessing,* Report, November 2004
- *Linux, UNIX and Windows TCO Comparison, Part 2,* Report, June 2004
- *Linux, UNIX and Windows TCO Comparison, Part 1,* Report, May 2004
- *Enterprises Worldwide Finally Plan to Increase IT Spending on Long-Overdue Software Upgrades,* Report, March 2004
- *Linux Is a Strong Contender, but Windows Is Still the Number-One Server OS,* Note, April 2005
- *How SMBs Should Choose Between Linux and Windows,* Note, March 2005
- Think Before You Migrate: Due Diligence Required for OS Migration, Note, March 2005

© Copyright 1997-2007 Yankee Group Research, Inc. All rights reserved.

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
617-956-5000 phone
617-956-5005 fax
info@yankeegroup.com

EMEA

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
44-20-7307-1050 phone
44-20-7323-3747 fax
euroinfo@yankeegroup.com

North America

Terence Matthews Crescent, Suite 200
KANATA, ONTARIO K2M 2C7
CANADA
613-591-0087 phone
613-591-0035 fax
canadainfo@yankeegroup.com

Yankee Group | the global connectivity experts™

A global connectivity revolution is under way, transforming the way that businesses and consumers interact beyond anything we have experienced to date. The stakes are high, and there are new needs to be met while power shifts among traditional and new market entrants. Advice about technology change is everywhere—in the clamor of the media, the boardroom approaches of management consultants and the technology research community. Among these sources, Yankee Group stands out as the original and most respected source of deep insight and counsel for the builders, operators and users of connectivity solutions.

For 35 years, we have conducted primary research on the fundamental questions that chart the pace and nature of technology changes on networks, consumers and enterprises. Coupling professional expertise in communications development and deployment with hundreds of interviews and tens of thousands of data points each year, we provide qualitative and quantitative information to our clients in an insightful, timely, flexible and economic offering.

Yankee Group Link

As technology connects more people, places and things, players must confront challenging questions to benefit from the changes: which technologies, what economic models, which partners and what offerings? Yankee Group Link™ is the research membership uniquely positioned to bring you the focus, the depth, the history and the flexibility you need to answer these questions.

Yankee Group Link membership connects you to our qualitative analysis of the technologies, services and industries we assess in our research agenda charting global connectivity change. It also connects you to unique quantitative data from the dozens of annual surveys we conduct with thousands of enterprises and consumers, along with market adoption data, comprehensive forecasts and global regulatory dashboards.

Yankee Group Link Research

As a Link member, you have access to more than 500 research reports and notes that Yankee Group publishes each year. Link Research examines current business issues with a unique combination of knowledge and services. We explore topics in an easy-to-read, solutions-oriented format. With the combination of market-driven research and built-in direct access to Yankee Group analysts, you benefit from the interpretation and application of our research to your individual business requirements.

Yankee Group Link Interaction

Our analysts are at your further disposal with data, information or advice on a particular topic at the core of a Link membership. We encourage you to have direct interaction with analysts through ongoing conversations, conference calls and briefings.

Yankee Group Link Data

Yankee Group Link Data modules provide a comprehensive, quantitative perspective of global connectivity markets, technologies and the competitive landscape. Together with Link Research, data modules connect you to the information you need to make the most informed strategic and tactical business decisions.

Yankee Group Consulting

Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization's readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and survey results to your specific needs to produce expert, timely, custom results.

Yankee Group Live!

The global connectivity revolution won't wait. Join our live debates to discuss the impact ubiquitous connectivity will have on your future. Yankee Group's signature events—conferences, webinars and speaking engagements—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this connectivity revolution.

www.yankeegroup.com

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel for builders, operators and users of connectivity solutions. For more than 35 years, Yankee Group has conducted primary research that charts the pace of technology change and its effect on networks, consumers and enterprises. Headquartered in Boston, Yankee Group has a global presence including operations in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific.

© Copyright 1997-2007. Yankee Group Research, Inc. All rights reserved.