

The Evolving Need for Security Risk Management and Comprehensive, Integrated Security Solutions



www.yankeegroup.com

by Sandra Palumbo and Lauren Cotes | October 2006

Executive Summary

Security threats are becoming increasingly sophisticated and destructive and continue to disrupt businesses of all sizes and industries (see Exhibit 1). Enterprises have to stay abreast of the latest network, application and security technology while balancing the needs of their business and customers.

For many businesses, these tasks are difficult to accomplish—especially with the challenges of managing multiple, disparate point solutions. With an abundance of security point solutions required to support a complete corporate security environment, managing, maintaining and integrating these solutions can be too complex for a business to handle internally.

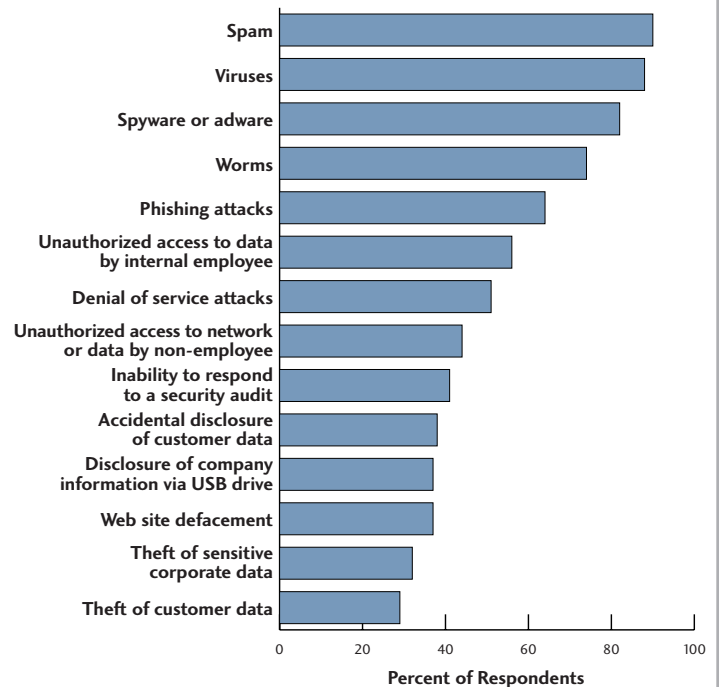
Enterprises continue to experience business disruptions as a direct result of security breaches, often in spite of several independent security point solutions already in place. Whether these incidents affect a single business unit or an entire corporate organization, the damage can still be catastrophic to a company. Risks include lost revenue, tarnished brands and customer dissatisfaction. Enterprises cannot afford to ignore or take a haphazard approach to corporate security.

Therefore, enterprises are increasingly considering adopting integrated security solutions along with security risk management solutions that enable them to more easily manage and maintain a secure environment. This Yankee Group Report examines the drivers for adopting comprehensive, integrated “security-as-a-service” solutions. In addition, we discuss how businesses should plan to complement this approach with security risk management solutions to provide maximum protection and minimize their exposure to security risks.

Exhibit 1

Spam, Spyware, Viruses and Worms Continue to Affect Enterprises

Source: Yankee Group 2005 Security Leaders and Laggards Survey



This custom publication has been funded by McAfee.

© Copyright 1997-2006. 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.

Table of Contents

I. Comprehensive Security Solutions Ease Complexity	2
II. Market Overview	2
Understanding the Need for Desktop Security Consolidation.....	3
The Growing Importance of Security Risk Management in Business Protection	4
Enterprise Security Risk Management	5
Security Risk Management Metrics.....	5
III. Enterprise Drivers	6
The Value of Adopting an Integrated Solution	6
IV. Conclusions and Recommendations	7
Recommendations for Businesses.....	7

I. Comprehensive Security Solutions Ease Complexity

Securing data, networks and applications is an enormous task for all enterprises, particularly in the rapidly changing world of security threats. Many businesses lack the expertise, funds or rapid response capabilities necessary to deal effectively with this problem.

Not only must businesses have the expertise to install anti-virus, anti-spyware, firewall and intrusion detection and prevention solutions, but also they must make them interoperate, maintain patches and updates, and monitor and manage these solutions. The cost associated with deploying several point security solutions or managing multiple anti-virus, anti-spyware, firewall and host intrusion prevention systems can be overwhelming for many businesses. Additionally, the management of a security environment consisting of point solutions can be challenging to manage, maintain and keep up to date.

As the complexities and costs of securing businesses increase, organizations should consider adopting comprehensive security solutions that fully integrate previously multiple independent solutions, enabling organizations to monitor and manage all the security functions from a single web-based security console. This approach maximizes a business' ability to respond to, protect against and repair damage from malware.

In addition, companies want to adopt new security solutions that help them assess the overall risk exposure of their network and its assets and also help them proactively mitigate the security risk and reduce their business exposure to all known vulnerabilities. In this way, businesses are able to reduce many of the costs and headaches associated with maintaining individual point solutions, while proactively securing their business networks against future attacks.

II. Market Overview

With employees' near-total reliance on their PCs, laptops and e-mail, keeping desktops up and running securely and efficiently is a top priority for businesses. Equally important is ensuring that the business applications are constantly available and functioning; this is done by securing and protecting the network and its assets, including file servers, databases, routers and internet gateways. Enterprises also have to ensure that legitimate remote workers are allowed to safely connect to the corporate network and that communication with external business partners is secure and safe.

When planning security strategies, enterprises must do their best to assess business risks as well as the costs associated with achieving the required level of network and business protection. There are many factors businesses must consider when evaluating their budget for implementing the required security policy:

- The cost to the business of employee downtime resulting from a successful attack
- The financial impact of the inability to conduct business due to an attack
- The financial impact of and required resources for desktop support and virus cleanup when an incident occurs
- The result of information leaks arising from successful spyware attacks (e.g., personal employee data loss, loss of intellectual property and corporate data and damage to image and integrity)
- Management costs (e.g., resources and assets) to monitor and manage multiple security solutions
- The total cost of purchasing and implementing multiple independent security solutions (e.g., software licenses, yearly contracts, support contracts)

Businesses must try to strike the correct balance when budgeting for the security of business operations and network systems without overspending—either in actual dollars or in the time and materials it takes to manage and maintain multiple security solutions. It’s not surprising that many companies prefer a single vendor source for their security agents as a way to better control their security solutions and spending (see Exhibit 2).

Understanding the Need for Desktop Security Consolidation

Computer security issues caused by viruses, worms, spyware and adware have created significant problems for businesses and consumer users of technology. Anti-virus software, personal firewalls and anti-spyware protection must coexist on PCs because alone they do not provide sufficient protection from threats. Desktop and server security point solutions add an increasing level of complexity to the management and control of these solutions and the policies that they are designed to affect.

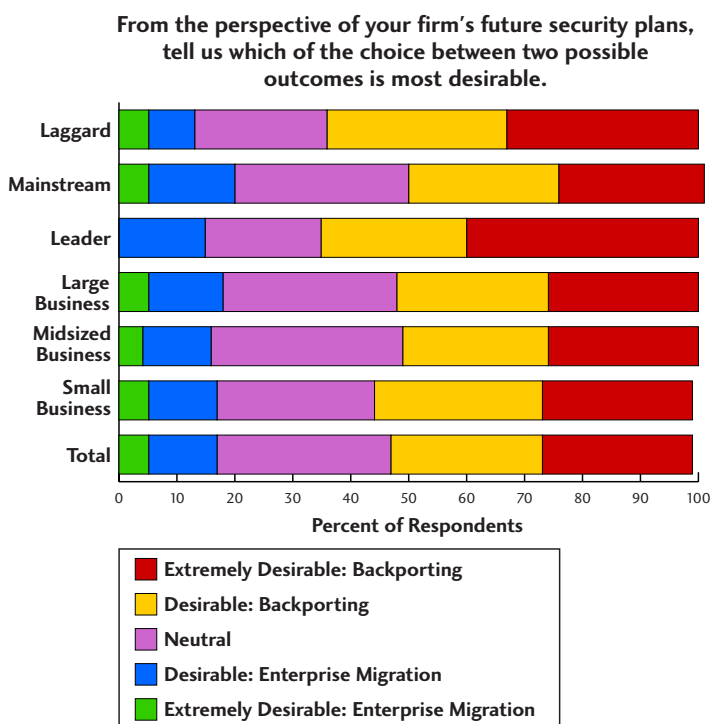
Enterprises have installed multiple layers of security defense, including firewalls, VPNs, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), anti-virus and anti-spyware solutions. These additional layers can make the management of security much more difficult and add to a business’ operational costs.

However, the weakness for most businesses is the potentially exploitable vulnerabilities that these measures do not address. No matter what solution businesses choose to adopt, it is critical they take a holistic approach to security policy and security architecture.

Interestingly, the threat to network security is often perceived as originating from external targeted hacker attacks. It’s not so well-known that vulnerabilities within unpatched, outdated and misconfigured software are commonly exploited by malware from dangerous e-mail attachments inadvertently downloaded by unsuspecting employees. When activated, this malware propagates throughout the network. Employee behavior represents the largest threat to enterprises; a total of 31% of enterprise threats comes from in-office and remote employees (see Exhibit 3 on next page).

The notion that employees play a large role in disruptive attacks emphasizes the need to ensure the secure protection of employee desktops, which minimizes the risk of employee-initiated attacks. Unfortunately, keeping different point security solutions updated and performing optimally requires a great deal of time and attention, which many businesses struggle to achieve.

Exhibit 2
Enterprises Prefer a More Complete Package for Security Agents
Source: Yankee Group 2005 Security Leaders and Laggards Survey



When a business has multiple point solutions, it loses a communal holistic view, which can create holes in the protection of its environment. Ambiguity is introduced if point solutions compete against each other in the remediation of threats and vulnerabilities. Hence the desire to have one integrated solution that provides comprehensive protection from a single desktop agent, can be managed from a communal manager and kept up to date with automated downloads. Such a solution alleviates the pains associated with managing multiple security solutions.

The Growing Importance of Security Risk Management in Business Protection

Desktop security continues to be a key area of enterprise security spending—in terms of both time and dollars. Two primary areas often require multiple products and management capabilities:

- **Threat mitigation:** Enterprises need desktop threat mitigation security. This typically includes anti-virus, anti-spyware, anti-phishing, desktop firewall capabilities and host intrusion prevention systems. Additionally, with increasingly smarter and more diverse threats for the desktop, standard threat mitigation solutions may not be enough to protect business endpoints.
- **Command and control:** Protecting against threats requires constant updating and fine-tuning—even at the desktop level. Command and control functions include patch management, systems management, policy management and connectivity (VPN).

Large enterprises have many priorities to balance. With compliance, improving operational efficiencies and aligning business strategy with security and technology all competing for resources and attention within an organization, businesses can lose sight of the impact of these initiatives on potential business risks.

In addition, businesses seek other methodologies to proactively help them assess the risk and identify possible vulnerabilities within their business systems that could be targeted in any attack, enabling them to mitigate their risk and minimize their exposure before an attack is launched. Security risk management is a challenge even for the most adept companies, because it requires correlating, evaluating and assessing the mountains of security data and information that businesses produce. In addition, business must be aware of what is occurring in the world in terms of new and emerging threats.

Based on business priorities, enterprises need to provide their security teams with the ability to detect, predict and respond to threats through assessing, prioritizing and then coordinating their response to threats. In addition, enterprises need to measure compliance, control network access and manage the ever-evolving risks threatening their business.

Security risk management tools can:

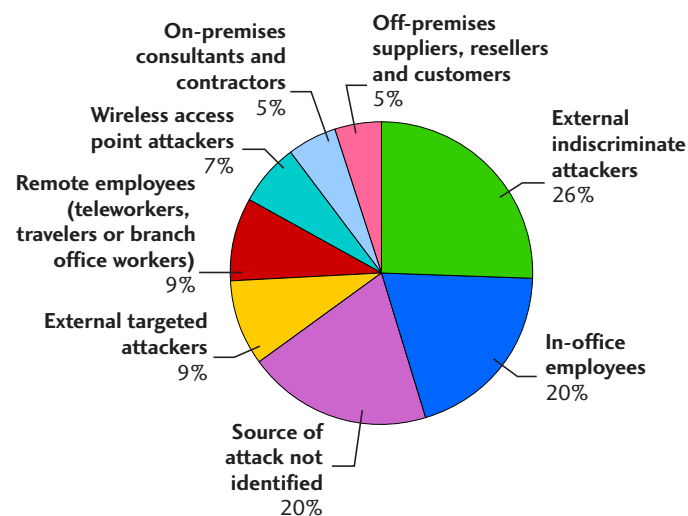
- Provide security administrators with the ability to respond to threats by:
 - Assessing the risk to the network and its assets
 - Prioritizing assets and business processes that need protection
 - Coordinating a system of network mitigation and remediation response based on business priority
- Provide an organization's administrators with the necessary solutions for:
 - Measuring device policy compliance
 - Controlling network access
 - Staying informed of new threats
 - Efficiently managing the security risk management lifecycle

Exhibit 3

What Are the Biggest Enterprise Threats?

Source: Yankee Group 2005 Security Leaders and Laggards Survey

For attacks rated as disruptive to the business, allocate a percentage impact to the following attack sources.



Note: Totals do not equal 100% due to rounding

It is difficult for a business to evaluate all of these areas when determining the actual impact on the business. In an evolving and dynamic marketplace, the question of just how much a company should spend on security risk management and mitigation is uppermost in the minds of most IT and security leaders today. Security risk management continues to be an area of great frustration for many businesses because metrics and benchmarks are lacking and corporations want some help and guidance in making sense of risk and their business. Businesses are challenged to simultaneously address security concerns and implement federal compliance policies. In addition, any security spending must be quantifiably justified.

Exhibit 4
Enterprise Use of Security Risk Management

Source: Yankee Group 2005 Security Leaders and Laggards Survey

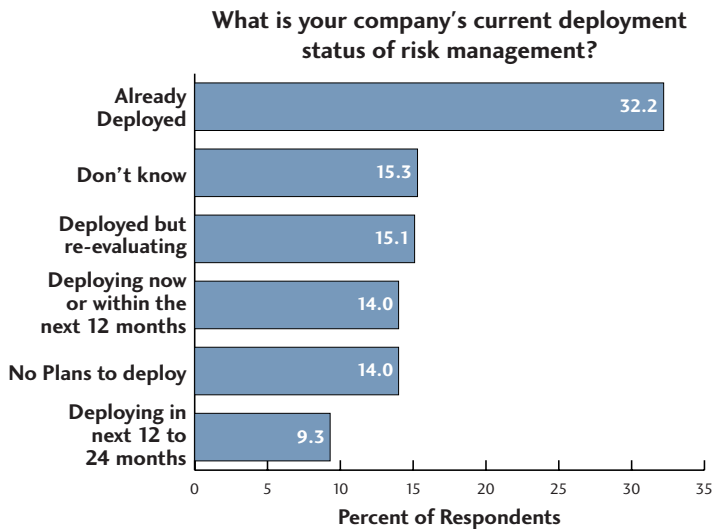


Exhibit 5
Security Risk Management Deployment by Industry Vertical

Source: Yankee Group 2005 Security Leaders and Laggards Survey

	Average	Construction	Education	Finance	Healthcare	Information Technology
Already Deployed	32%	42%	21%	33%	33%	39%
Deploying Now or Within Next 24 Months	23%	32%		28%	24%	25%
Deployed but Reevaluating	15%	16%		24%		15%
No Plans to Deploy	14%		21%		19%	
Don't Know	15%		24%			

Note: Average does not equal 100% due to rounding. Industry verticals do not equal 100% because they represent the top three responses.

Enterprise Security Risk Management

Enterprises use security risk management tools to better prioritize which vulnerabilities and security incidents to repair first, based on their threat level and impact on the business. Security risk management solutions include additional features such as tracking, monitoring, auditing and reporting capabilities.

Desired outputs vary from enterprise to enterprise, and even business unit to business unit within enterprises. Therefore, security risk management tools must be customizable. Because of this, most enterprises use ad hoc databases created internally or security management consoles from security event and security incident management vendors as security risk management solutions. Additionally, some enterprises rely on consultants to establish a security risk management metric for tracking security breaches.

Security Risk Management Metrics

For the most part, enterprise adoption of security risk management and asset classification tools is growing steadily. Thirty-two percent of enterprises have deployed some type of security risk management solution (see Exhibit 4). Additionally, approximately 23% of enterprises plan to deploy security risk management now or within the next 24 months. Although more than 70% of enterprises have already deployed or plan to deploy security risk management in the future (includes “deployed but reevaluating”), the remaining enterprises don’t know or have no plans to deploy security risk management—which could ultimately hinder the performance of IT departments.

The construction, finance and information technology industries are among the leaders in security risk management deployment (see Exhibit 5 on previous page). These verticals outpace the average respondent by current and future deployment.

Although approximately the same percentage of the healthcare industry and the average enterprise have deployed security risk management, 19% of businesses in the healthcare industry are not planning to deploy security risk management, which is 5% higher than the average.

The education industry is also underperforming the average, with almost one-half (45%) of respondents stating that they either have no plans to deploy security risk management or don't know their security risk management plans.

III. Enterprise Drivers

The day-to-day security issues that enterprises face are as commonplace as e-mail spam and viruses. In fact, 90% of enterprises experienced incidents of spam, 88% experienced viruses and 82% experienced incidents of spyware in the past 12 months (see Exhibit 1). Ninety-nine percent of enterprises have desktop anti-virus solutions, 96% have anti-spam solutions and 95% use desktop anti-spyware software.

What's more alarming is the number of enterprises that have security solutions in place and still experienced security breaches. There are a number of possible reasons for this:

- The company deployed protection for one form of malware but not for another (e.g., for anti-virus but not for anti-spyware).
- The company deployed point solutions for different forms of malware, but they did not work together to provide holistic protection for the network.
- The deployed solutions were not kept up to date.

The Yankee Group *2005 Security Leaders and Laggards Survey* shows that when it comes to deploying security solutions, 63% of enterprises now prefer to use a single vendor over best-of-breed endpoint policy enforcement and anti-malware agents. However, although most enterprises would like to deploy a single console rather than several best-of-breed vendors, most have not yet done so.

Exhibit 6 illustrates what providers those 63% of enterprise respondents that prefer to use a single vendor endpoint security solution are actually using today. Even though these enterprises

would like a single, integrated solution, they don't feel they have many options other than using point solutions. McAfee and Symantec are the only vendors that offer all three security solutions (i.e., anti-spam, desktop anti-virus and desktop anti-spyware), leaving the majority of enterprises to rely on multiple vendors for protection against malware.

Single-vendor security solutions do a lot to ease the burdens of management throughout the entire lifecycle—from fielding RFPs to deploying the software. With integrated security solutions on a single console, IT departments only need to familiarize themselves with one user interface, which improves operational efficiency and reduces training costs. Additionally, all-in-one solutions eliminate compatibility issues that can occur with multiple best-of-breed solutions on a single endpoint.

The Value of Adopting an Integrated Solution

If the world was a simple place, securing a business would just require deploying a single product, device or service that would be simple to manage and update. But the world today is not a “set it and forget it” kind of place. Instead, companies need layers and layers of products and services to successfully secure

Exhibit 6

Even Enterprises That Prefer a Single Vendor Solution Are Still Reliant on Multiple Vendors and Products

Source: Yankee Group 2005 Security Leaders and Laggards Survey

	Anti-Spam	Desktop Anti-Virus	Desktop Anti-Spyware
Symantec	22%	25%	24%
McAfee	22%	29%	24%
Microsoft		15%	19%
CA		7%	4%
Trend Micro	3%	4%	
Lavasoft Ad-Aware			17%
IBM	14%		
McAfee Managed	7%		
Outlook 2003	6%		
Spybot Search & Destroy			6%
Barracuda Networks	4%		
F-Secure		4%	

their business. Integrated security solutions go a long way in providing businesses of all sizes with some help in simplifying endpoint security.

The security and applications markets are now moving to the software-as-a-service model. This model helps alleviate many of the nightmares traditionally associated with deploying software in a business environment. This service model provides businesses with:

- Reduced upfront capital expenditure for security appliances or software
- Reduced ongoing operating expenditure
- More predictable costs and charges relating to security provisioning
- More effective protection resulting from comprehensive integrated protection and automated updating options
- Less IT involvement and support costs, especially those relating to cleaning up after a security incident has occurred
- Shorter time to get software running and security protection in place
- Ease of scaling as the business changes

The advantages of moving to the software-as-a-service model are particularly attractive to those businesses where the economics can be significant—instead of purchasing security software or appliances upfront, many businesses can now turn to local telecommunications companies and service providers to obtain comprehensive security as a value-added service that is charged on a monthly basis along with their existing invoices for the provision of broadband or telephone services. Businesses will be better able to manage and secure their environments through these flexible and scalable service models.

IV. Conclusions and Recommendations

Security threats are becoming more sophisticated and widespread. To counter the growing threat, enterprises must take action to secure their networks, data and business applications. However, managing a series of point security solutions can be expensive, complex and challenging, given the complexity of business infrastructures and the number of point solutions required to secure the corporate environment effectively and adequately. With limited resources for training on these devices and technologies, managing multiple security solutions, ensuring individual point solutions are up to date with the most recent patches and enforcing company security policies, the task of managing security internally is a daunting and difficult task for many companies.

Fortunately, vendors have recognized the need to provide greater integration of security point solutions. They are now beginning to provide comprehensive, integrated security solutions that may be offered to companies as a security service.

At the same time, companies are becoming more risk-aware. They are increasingly looking at adopting security risk management solutions that help identify security risk within their organizations and proactively help companies take guided action to reduce this risk before an attack is successful.

Recommendations for Businesses

- **Evaluate desktop security solutions based on scalability, accuracy and management overhead.** Many desktop security solutions—whether point solutions or integrated solutions—require regular tuning, and do not scale easily to larger environments. Businesses need to evaluate how well a solution will meet their needs and capabilities before making a decision.
- **Consider the benefits of a service model when selecting security solutions.** Gone are the days when businesses only had the options of buying shrink-wrapped, point security solutions. An increasing number of security vendors also offer products in a security-as-a-service model, where many of the management headaches are built into the solution and monthly charges.
- **Evaluate security management consoles on how well they aid risk, policy and compliance management objectives.** When adopting a solution that includes a portal console for management, look at what additional functions the portal will enable your company to manage, such as security risk management, compliance management and policy management.
- **Investigate security risk management security solutions that identify business risks and vulnerabilities.** Security risk management can be a frustrating topic for businesses, but it must be a critical aspect to your security approach and can be a valuable exercise if you can find the right tools and partners.

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
T 617-956-5000
F 617-956-5005
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

North America

200-260 Terence Matthews Crescent
OTTAWA, ONTARIO K2M 2C7
CANADA
T 613-591-0087
F 613-591-0035
canadainfo@yankeegroup.com

Decision Services

Yankee Group Decision Service annual memberships offer clients access to research and one-to-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, research reports, forecasts, DecisionNotes and regular Webinars 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 in order to hone their corporate strategies and maximize overall return.

www.yankeegroup.com

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.