



# Enterprise Instant Messaging: Reducing Security Risks and Maintaining Regulatory Compliance

## Executive Summary

During the next 3 years, the adoption of enterprise instant messaging (IM) will increase threefold. Already, businesses find that they must strike a balance between mitigating security risks and maintaining regulatory compliance while not adversely affecting the productivity of users or the financial benefits of the technology. To temper the myriad security risks posed by IM (e.g., loss of confidential data, sending sensitive customer data over public IM networks, misusing company IT resources, exposure to malicious code and noncompliance with government regulations), businesses must invest in IM security and compliance solutions that can provide content filtering, access controls, encryption, auditing and archiving.

Various federal regulations, federal regulatory authorities and industry practices mandate archiving to mitigate risks of sensitive data transferred over all IM networks. Examples of regulations include the Securities and Exchange Commission (SEC) rules 17a-3 and 4, which affect the financial industry; the Sarbanes-Oxley Act, which affects all publicly traded companies; and the Health Insurance Portability and Accountability Act (HIPAA), which affects healthcare services industries. Examples of regulatory authorities include the Federal Energy Regulatory Commission (FERC), which oversees the energy and utility industry, the Food and Drug Administration (FDA), which oversees the medical technology and pharmaceutical industries; and the Internal Revenue Service (IRS), whose record retention requirements cover both individuals and corporations.

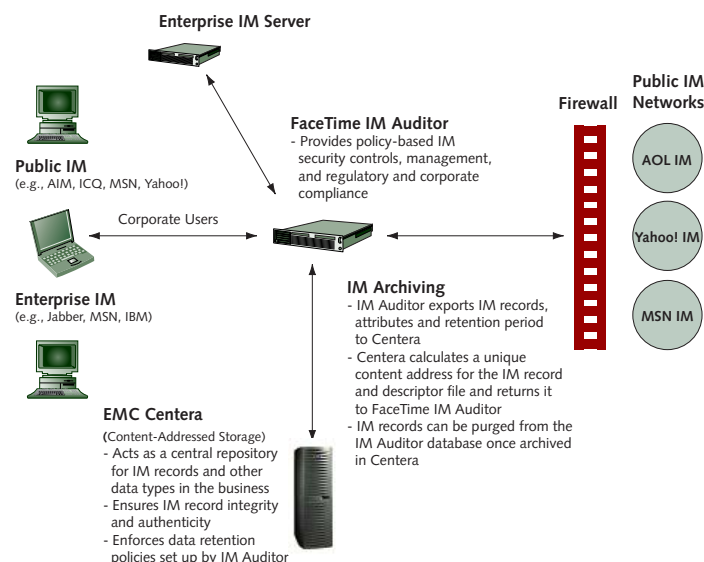
Industry best practices necessitate improved record retention policies to facilitate litigation support, which is affected by general corporate records discovery requirements. Increasingly, even in unregulated sectors, general corporate policy requires companies to conduct the same level of record retention diligence for IM as for e-mail. According to the Yankee Group 2004 *Enterprise Storage Survey*, businesses typically archive instant messages for 4.6 years (the same as e-mail). A complete archiving solution must provide policy-based archiving and a storage medium that ensures the stored data cannot be overwritten or altered. Optical CDs/DVDs, tape and disk are all common storage options for archiving, but the most appropriate option is determined by its ability to ensure data integrity over long periods of time, access requirements, scalability, manageability and cost. Historically, disk was a cost-prohibitive option for archiving. Today, low-cost drive

options and easy-to-manage disk systems, which are purpose-built for storing fixed or archived content, have made disk a popular option—especially in environments where online access is important and the business also must store several other data types.

To offer end-to-end IM management, security and archiving, FaceTime Communications (a provider of IM security, management and compliance solution software) and EMC (a provider of information storage and management) have partnered to deliver an integrated end-to-end solution. The joint offering integrates FaceTime's IM Auditor software with EMC's content addressed storage system, Centera. IM Auditor provides businesses with policy-based logging, auditing, content blocking and filtering, antivirus and archiving (100% of all IM conversations logged and audited) plus a real-time alerting and reporting infrastructure. Archived conversations are exported to EMC Centera; Centera enforces IM Auditor's policies while providing online access to archived messages (see Exhibit 1).

## Exhibit 1 FaceTime and EMC Joint Solution Offer IM Compliance, Security and Archiving

Source: EMC and FaceTime, 2005



## Table of Contents

I. Introduction . . . . .	2
II. Enterprise IM Market Overview . . . . .	2
IM Risks and Controls . . . . .	3
III. Product/Service Profile . . . . .	4
FaceTime Communications . . . . .	4
EMC . . . . .	6
IV. Joint Offering Differentiation . . . . .	7
Joint Product Applications . . . . .	8
V. Conclusions . . . . .	9
VI. Enterprise Recommendations . . . . .	10

### I. Introduction

Until recently, security risks and concerns regarding management and control were major barriers to enterprises' adoption of IM. Early adopters included industries where the need for faster communication among employees (e.g., stock traders) and the ability to reduce communication costs to partners and customers (e.g., service-oriented industries) outweighed the risks and concerns. The advent of IM security and compliance software reduced the risks and accelerated adoption. As adoption has increased and IM has become a primary communication technology, it has become subject to the same IT requirements and regulations as other communication technology such as e-mail. IM must integrate with software, storage and other IT components for high availability, data protection and archiving capabilities to meet corporate and regulatory compliance, privacy and security concerns.

In this report, we focus on an integrated offering of IM security, management and compliance software and storage from FaceTime and EMC. We examine the synergies between FaceTime's IM software offerings, particularly IM Auditor, and EMC's content addressed storage system, Centera.

### II. Enterprise IM Market Overview

Yankee Group estimates that the 2005 worldwide enterprise market for IM will consist of 45 million enterprise seats and \$56 million in revenue. We expect the number of enterprise IM seats to grow to approximately 140 million by 2008 (see Exhibit 2 on next page). Consumer use has outpaced enterprise use as businesses have struggled with security concerns and a quantifiable return on investment (ROI). However, advantages over e-mail (e.g., real-time communication among employees, partners and customers; telephony cost reductions; the ability to view user availability and status; and storage cost reductions), coupled with IM security, management and compliance software, have accelerated enterprise adoption. Adoption will further accelerate as the following technologies combine to form the new online collaboration suite:

- E-mail and IM integration
- Webcasting and webconferencing
- Application and document sharing
- Telephony, audio and videoconferencing

## IM Risks and Controls

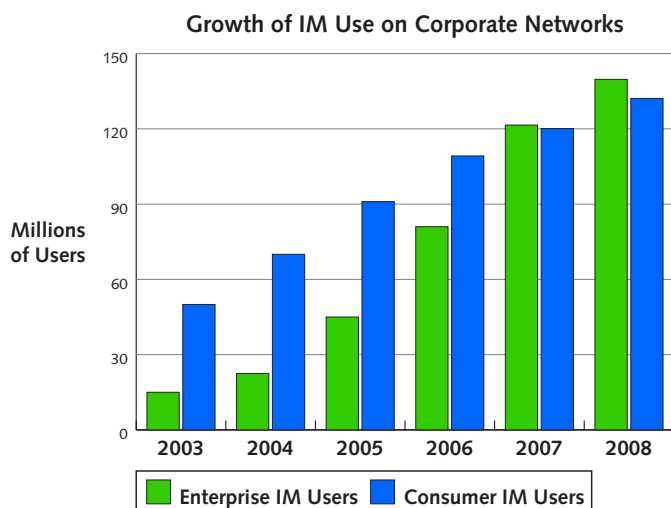
IM risks include the loss of intellectual property and confidentiality, legal liabilities, data security and privacy risks, lapses in regulatory compliance and virus attacks. One of the most prevalent threats today is IM spam or “spim” (e.g., a link that when clicked on potentially infects the computer with a virus or Trojan). Many businesses use IM without encountering information leakage, viruses or spim; but as IM’s popularity grows, so does the frequency of these threats. The following are common risks of IM:

- **Information leakage and confidentiality:** The risk that intellectual property and sensitive information can be read by or distributed to unauthorized users. This is especially the case when employees use public IM clients to communicate among themselves and with individuals outside the business.
- **Message integrity:** The risk that unauthorized users will alter communications.
- **Network security:** The risk that malicious code will spread to the network.
- **Network availability and performance:** The risk that excessive messaging traffic will adversely affect more critical business communication.

### Exhibit 2

The Growth of Enterprise Instant Messaging Is on the Fast Track

Source: Yankee Group, 2005



- **Timeliness:** The risk that messages will not be received in a timely manner.
- **Accountability:** The risk that the identity of the message sender/receiver cannot be verified.
- **Regulatory requirements:** The need to retain, archive and ensure the authenticity of communications affected by regulations, such as:
  - **Finance:** SEC rules 17a-3 and 17a-4; National Association of Securities Dealers (NASD) rules 2210 and 3010; New York Stock Exchange (NYSE) rules 440, 372 and 342; Investment Company Act of 1940 as amended (affecting asset, hedge fund and mutual fund managers); Investment Advisers Act of 1940, as amended (affecting investment advisors); in the European Union (EU), Basel II; and in Japan, Banking Reform Act
  - **Commodities and futures:** Commodity Exchange Act (CEA), National Futures Association (NFA) rules 1.31 and 4.23, NFA rules 2.9, 2.10 and 2.29 (f)
  - **Banking:** Gramm-Leach-Bliley Act, U.S. Patriot Act and the Federal Deposit Insurance Corporation (FDIC) (data privacy and guidance on IM logging and auditing)
  - **Insurance:** Varying state regulations with guidance on messaging retention with likely federal regulation looming
  - **Healthcare services (providers and payers):** HIPAA (data privacy and security provisions)
  - **Medical technology and pharmaceuticals:** FDA 21 CFR Part 11 and HIPAA
  - **Energy and utilities:** FERC
  - **U.S. publicly traded companies and accounting firms auditing public companies:** Sarbanes-Oxley Act
  - **U.S. government:** Department of Defense 5015.2 and other departments
  - **General:**
    - » U.S. legal discovery requirement
    - » General privacy laws (e.g., California SB 1386)
    - » IRS record retention

Given the risks enumerated above, it's critical that businesses implement controls for their IM system. Businesses should consider implementing the following basic controls as part of the IM ecosystem:

- **Content filtering:** Filter content to block unwanted messages (spim), viruses and offensive material.
- **Access controls:** Limit access to messaging systems using authentication and authorization, mapping public instant messaging "buddy names" to an authenticated corporate identity.
- **Threat prevention (antivirus, antispim):** The existing antivirus infrastructure doesn't scan files transferred over IM. Keep all messaging clients up-to-date with patches to reduce code vulnerabilities. Integrate and run threat prevention software or antivirus to reduce the risk of viruses, worms, spyware and Trojans.
- **Network safeguard:** Prioritize and block unauthorized messaging traffic (including internal and external users) to prevent network overload and enforce corporate policies.
- **Encryption:** Encrypt sensitive information sent through IM.
- **Logging, auditing and archiving:** Implement an archiving solution to log, retain and maintain the authenticity of messages to meet regulatory requirements and corporate policy.
- **Support standardization:** Ensure that employees adhere to a network standardization policy.

### III. Product and Service Profile

A complete IM security and archiving solution requires not only policy-based software to provide IM controls and archive messages, but also a storage medium to act as the long-term repository. To meet most regulatory requirements, the storage medium must ensure that the stored data cannot be overwritten or altered in any fashion. This section profiles the complementary pairing of an IM solutions provider, FaceTime Communications, and an information storage and management provider, EMC.

#### FaceTime Communications

Founded in 1998, FaceTime Communications ([www.facetime.com](http://www.facetime.com)) provides software to secure, manage and extend the use of IM networks and other real-time communication in the enterprise. It's a leader in market share, revenue and growth for IM security and compliance software solutions with more than 400 customers, including 50 of the 100 largest financial services institutions worldwide. Its solution suite consists of two main offerings that constitute a tightly integrated IM security solution:

- **IM Auditor:** A software application designed to manage and control IM throughout the enterprise. It also logs and archives IM for regulatory compliance and corporate policy enforcement.
- **RTG500:** A hardened appliance that detects and controls all IM and peer-to-peer (P2P) network traffic, protects against sophisticated workarounds and enforces compliant and authorized use. It provides detailed network traffic reports and is also available as a software application.

FaceTime designed its IM solutions to operate across enterprise and public IM clients, such as AOL AIM, Yahoo! Messenger, Microsoft MSN Messenger, Microsoft MSN Messenger Connect for Enterprises, Jabber, Microsoft Office Live Communications Server, IBM Lotus IM (Sametime) and Reuters Messaging.

## FaceTime IM Auditor

IM Auditor provides IM security, management, regulatory compliance and corporate policy enforcement across enterprise and public IM clients. The goal is to implement the controls and management capabilities necessary to reduce the risk to the business without affecting or limiting the productivity and financial benefits of the technology.

IM Auditor's security features specifically address many of the risks and threats outlined in Section II of this report, such as policy-based access controls, the ability to restrict inter-organization contact, antivirus scanning and the ability to block spam from public IM networks or federated enterprises. Restricting inter-organization communication is particularly helpful in enterprises that are required to keep specific business functions separate due to regulatory requirements. A good example is a financial institution that must keep its research and trading functions separate. Businesses also can use their existing antivirus application with IM Auditor; there are no additional software costs. The ability to block spam is a critical feature because it's one of the most common IM security risks. The IM Auditor uses a combination of allow/block lists, rich content filtering (including full regular expression capabilities) and a patent-pending challenge-response mechanism to eliminate spam bots.

IM Auditor provides businesses with policy-based management of all IM controls as well as real-time enforcement, monitoring and reporting. Enterprises can set policies at the global, group and employee levels. IM Auditor offers granular control of capabilities and access across all enterprise and public IM clients. Its real-time capabilities—including enforcement of policy changes, usage reports and graphical statistics monitoring—are an additional advantage.

FaceTime optimized IM Auditor for strict regulatory compliance and corporate policy enforcement. This is critical because the same government regulations (detailed in the "IM Risks and Controls" subsection of Section II) that govern e-mail communication govern IM communication. Increasingly, both regulated and unregulated industries audit and retain IM according to their own corporate/HR policies. The following are a few of IM Auditor's compliance features:

- Group-specific legal audit disclosure notices
- Extended logging and 100% auditing of all IM conversations, including encrypted conversations (IM Auditor can recreate IM conversations with 100% accuracy because the messages are stored in a binary format and in the order they were exchanged and it provides time stamps for all messages and events.)
- Real-time restriction of inter-organization contact, flagging of inappropriate content and prevention of policy breaches with alerts
- Message-level data integrity and anti-tampering
- 360-degree audit of all users, including the actions of administrators and reviewers themselves
- Integration with e-mail compliance, document management and write-once, read many (WORM) storage systems such as EMC Centera

The IM Auditor software application is available on Windows 2000 Server, Windows 2003 Server and Red Hat Enterprise Linux Operating System with either a Microsoft SQL Server or Oracle 9i database.

## EMC

Yankee Group estimates that EMC ([www.emc.com](http://www.emc.com)) is the leader in both networked storage systems (the aggregate of SAN-attached, NAS-attached and content storage) and storage management software. The company has a broad lineup from entry-level to high-performance storage systems. During the past 2 years, EMC has transformed itself into a software company with a series of acquisitions (Documentum, Legato and VMware) to complement its own storage management software, such as ControlCenter, and its data protection software, such as TimeFinder and Symmetrix Remote Data Facility (SRDF).

Its broad portfolio of storage systems and storage software for infrastructure management, data management and protection, enterprise resource management, and workflow enable EMC to provide end-to-end solutions for information lifecycle management (ILM). ILM is a deployment model that matches the appropriate storage class to content and manages the content through its lifecycle of relative value from one storage class to another. EMC's content-addressed storage (CAS) system, Centera, is an example of a storage system purpose-built for storing fixed or archived content.

## EMC Centera

The EMC Centera CAS system is a bundled software and disk platform that targets the storage requirements of fixed content. Yankee Group defines fixed content as content that must remain unchanged and preserved for compliance and other business retention reasons. Electronic bank statements, digital images of stock transactions, e-mail and IM messages, Microsoft Office files, patient medical records, digital x-rays, blueprints and mechanical drawings are some examples of fixed content.

The Centera storage system includes a redundant array of independent nodes (RAIN) interconnected via a private LAN. Each node executes the Centera software and has processing power and storage capacity. Each node acts as either an access node or storage node. Access nodes are the conduits between the applications and the storage nodes. Applications write to the Centera application programming interface (API) and access the Centera nodes via the LAN.

Centera offers the following benefits to enterprises:

- **Integration:** Centera provides an API to enable independent software developers to integrate their solutions with Centera.
- **Data integrity, authenticity and long-term retention:** Centera ensures the authenticity of the object to be stored. When an application sends a request to Centera to store an object, the Centera software calculates a content address for that object and then stores the object and a mirror copy in the Centera repository. The content address is globally unique and acts like a digital fingerprint for the object. This ensures the object is stored uniquely and is not modified. A change to the object generates a new copy of the object with a new unique content address. In addition, the object cannot be deleted before the parameters are specified by the application to Centera.

Centera simultaneously records the object's content address in a metadata file, which EMC calls a C-Clip Descriptor File (CDF). The C-Clip is in XML format and contains the content address for the object and

standard application-defined attributes of the object, such as date, time, creator, size and file name. A content address for the C-Clip is calculated and that address is then returned to the application. Authenticity is crucial for business requirements but also for compliance requirements for SEC 17a-4, HIPAA, Sarbanes-Oxley and others.

- **Data protection:** Centera offers two options for local content protection: content mirroring and content parity protection. For disaster recovery, information from one Centera cluster can be mirrored asynchronously to a remote Centera cluster. The process is transparent to users once implemented and read failover is automated.
- **Manageability and scalability:** Content addressing reduces storage complexity. Because Centera determines the physical placement of objects, system administrators don't have to specify and manage the underlying file or logical unit number structure. They can add nodes as capacity is needed and Centera self-configures the additional capacity. Each cabinet can accommodate up to 32 nodes and four cabinets can be clustered together. An application can access multiple Centera clusters (up to 1 petabyte) through the Centera API.
- **Online accessibility:** Unlike tape or optical storage media, Centera provides fast, online access to data via the LAN.

## IV. Joint Offering Differentiation

A complete IM security archiving solution requires an application to implement controls and set policies, and an appropriate storage medium that can physically store the IM conversations and enforce the policies set by the application. The joint offering of FaceTime's IM Auditor and EMC's Centera provides a number of key differentiators:

- **API-based integration:** There are several capabilities between the two product offerings that are only possible through API (as opposed to SMTP export) integration:
  - **IM records are treated as first-class data.** They are treated with the same importance and priority as other data types, such as e-mail. This is important because all electronic conversations are subject to the same regulations. It also makes it easier for customers to manage all their content media uniformly in the same storage system.
  - **IM Auditor programmatically sets the retention policies in EMC Centera.** The appropriate business/industry-specific data retention policies set using the IM Auditor UI are automatically carried over and strictly enforced by Centera.
  - **After IM records are written from the IM Auditor internal database to EMC Centera, enterprises can purge these records from the IM Auditor internal database.** This reduces storage requirements and helps to manage database growth on the IM Auditor server.
  - **Real-time access to and reporting on IM records already archived to EMC Centera are preserved on the same IM Auditor Reviewer UI.** Even if the data has been purged from the IM Auditor SQL database, the API allows real-time search retrieval of the relevant records from EMC Centera via their content address.

- **Secure and compliant IM collaboration:** Through IM Auditor's IM controls and policies and EMC Centera's content-based addressing and authenticity, businesses have an integrated solution to address IM risk and regulatory requirements. An added benefit is IM Auditor's integration with additional FaceTime offerings, such as RTG500, a network perimeter security solution for IM and P2P.
- **Online access:** Tape, optical CD/DVD and disk are all common options for archiving. Tape is the least expensive, but access to archived messages is slow. Optical CDs/DVDs are known for their long-term reliability but also offer slow access. Disk provides online access and purpose-built content storage systems such as Centera provide not only online access but also advanced data integrity and data authenticity capabilities.

## Joint Product Applications

Yankee Group research shows that both regulated and nonregulated industries will need IM security and archiving solutions. According to the Yankee Group *2004 Enterprise Storage Survey*, enterprises (i.e., businesses with more than 500 employees) indicated that internal corporate policies influenced their business and how they managed storage more than any government regulation (see Exhibit 3). In the same Yankee Group survey, enterprises also indicated that aside from backup and recovery, data retention was their next highest priority during the next 12 months. Businesses clearly have internal needs to reduce risk and archive content in ways that meet or exceed any regulatory requirements.

The federal government—particularly the military—is influenced most heavily by its own corporate policies (approximately 86% of government respondents). Archiving with message-level integrity and authenticity is a major priority for this industry. The finance industry is most influenced by SEC 17a-3 and SEC 17a-4, and the medical industry is most influenced by HIPAA and FDA CFR Part 21. However, both are still significantly influenced by their own corporate policies. Regardless of whether an industry shapes its response to archiving and security from a regulatory perspective or a business-policy perspective, C-level executives are realizing that good governance and superior business performance require a robust, rigorous, methodical and transparent approach to IM compliance, management, security and archiving.

The joint product offering of FaceTime IM Auditor and EMC Centera enables businesses to meet the requirements of their own corporate policies and adhere to government regulations for IM compliance, management and archiving. In addition, because data retention is such a high priority for most businesses during 2005, it's likely that they are

### Exhibit 3

#### Corporate Policy and Government Regulations

Source: Yankee Group 2004 Enterprise Storage Survey

Which regulations have the most impact on your business and the way you manage your storage infrastructure?

	Our Own Internal Policies	HIPAA	U.S. Patriot Act	Sarbanes-Oxley Act	SEC17a-3 and SEC17a4	21 CFR Part 11	NASD 3010 and 3110
<b>Total</b>	50.85%	25.42%	16.61%	16.27%	14.92%	11.86%	10.85%
<b>Manufacturing</b>	52.17%	13.04%	20.29%	20.29%	13.04%	15.94%	10.14%
<b>Finance, Banking and Accounting</b>	25.45%	14.55%	27.27%	12.73%	34.55%	16.36%	20.00%
<b>Insurance, Real Estate and Legal</b>	44.44%	25.93%	14.81%	29.63%	14.81%	18.52%	7.41%
<b>Federal Government (Including Military)</b>	65.00%	25.00%	5.00%	10.00%	15.00%	5.00%	0.00%
<b>Medical, Dental and Healthcare</b>	46.34%	75.61%	12.20%	12.20%	4.88%	14.63%	9.76%
<b>Wholesale Retail and Distribution</b>	50.00%	18.18%	4.55%	22.73%	9.09%	0.00%	31.82%
<b>Transportation/Utilities</b>	52.38%	19.05%	19.05%	23.81%	14.29%	9.52%	4.76%
<b>Education</b>	85.00%	17.50%	12.50%	5.00%	5.00%	2.50%	0.00%

Note: Shading indicates the top two highest regulations for each industry.

retaining other types of data as well—from e-mail to office documents to financial statements. A benefit of deploying EMC Centera as the storage repository for IM records is that it can simultaneously act as the repository for other data types in the corporate environment and integrate with other types of applications. This integration ensures that corporate policies for archiving and storage are enforced consistently across multiple systems.

## V. Conclusions

As enterprise adoption of IM continues to rise and IM begins to overtake e-mail as the preferred form of electronic communication, it's inevitable that businesses must develop a plan to manage IM use and address security risks, threats, regulatory requirements and corporate policies. Businesses governed by regulations and nonregulated businesses will need to invest in IM software solutions. IM software must provide archiving in addition to controls such as content filtering, access controls, encryption and auditing. A complete archiving solution must comprise both policy-based software and a storage medium that ensures the integrity and authenticity of the content. For businesses that are retaining different data types, having a scalable, easy-to-manage storage offering that can act as a single repository and integrate with several types of applications is beneficial.

A FaceTime IM Auditor and EMC Centera joint offering satisfies many of these requirements. IM Auditor provides policy-based security controls, management and enhanced functions for regulatory and corporate compliance. It has the added benefit of tightly integrating with other FaceTime IM solutions such as RTG500 for compliance. When integrated with EMC Centera, businesses have a storage repository that can strictly enforce retention policies, provide online access to archived content and simultaneously act as a repository for other data types.

## VII. Enterprise Recommendations

- **Many businesses are either unaware or choose to ignore public and enterprise system IM use by employees.** This is a dangerous situation given the security risks and threats described in this report. The cost of noncompliance with regulations concerning record retention can be very high. Assume that employees are using IM, and determine how your business should embrace enterprise IM use and deploy the proper controls.
- **Determine ROI measures for enterprise IM.** Many businesses have been slow to adopt enterprise IM, because they cannot quantify the ROI and are concerned about the security risks. Quantifying the ROI will help them make a more educated decision about enterprise IM use. Enterprises have successfully adopted IM to increase productivity among employees, partners and customers and to reduce telephony costs.
- **Build a highly scalable storage solution.** Businesses should consider the storage requirements of e-mail and IM simultaneously. Both forms of electronic communication are governed by the same regulations and are archived for the same period of time (4.6 years). Yankee Group estimates that a company of about 5,000 employees will need 4 terabytes of storage per year. The ability to add and manage capacity cost-effectively in the future will determine the true total cost of ownership for a business.

# Did You Know ? The Yankee Group...



Is the **world's most trusted** name for communications and networking research and consulting, focusing on strategic planning assistance, technology forecasting and industry analysis.

Has **unmatched expertise** across telecommunications, wireless/mobile communications, IT business applications and consumer technologies.

Was **founded in 1970** as the first research and advisory services firm.

Maintains research staff in **North America, Latin America, Asia-Pacific, and Europe/Middle East/Africa.**

Employs approximately **200 skilled professionals.**

Offers a portfolio comprising nearly **100 service offerings**—advisory services, decision instruments, signature events and consulting.

Provides **complete** technology and management consulting capabilities.

Showcases a **full calendar of technology-related conferences and seminars** held around the globe.

Delivers a **full line of reports and research notes** via the Internet.

## The Yankee Group

### World Headquarters

31 St. James Avenue

**BOSTON, MASSACHUSETTS** 02116-4114

T 617.956.5000

F 617.956.5005

info@yankeegroup.com

### Regional Headquarters

#### North America

31 St. James Avenue

**BOSTON, MASSACHUSETTS** 02116-4114

T 617.956.5000

F 617.956.5005

info@yankeegroup.com

951 Mariner's Island Boulevard, Suite 260

**SAN MATEO, CALIFORNIA** 94404-5023

T 650.522.3600

F 650.522.3666

info@yankeegroup.com

#### EMEA

55 Russell Square

**LONDON WC1B 4HP**

**UNITED KINGDOM**

T 44.20.7307.1050

F 44.20.7323.3747

euroinfo@yankeegroup.com

### For More Information

T 617.956.5000

F 617.956.5005

E-mail: info@yankeegroup.com

Web site: www.yankeegroup.com

### Advisory Services

Yankee Group advisory service annual memberships offer clients access to research and one-to-one expert guidance.

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

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

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

### Decision Instruments

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

#### Trackers

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

#### Surveys

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

#### Forecasts

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

### Signature Events

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

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

### Consulting Services

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

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

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

### www.yankeegroup.com

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