



## **Policy-Guided Message Networks Provide Solutions Approach to Reducing E-Mail Hazards**

### **Executive Summary**

*E-mail, arguably the most critical data communications function, continues to be overburdened and risky, even as improvements to messaging servers and antivirus and antispyware products proliferate.*

*Most e-mail systems rely on a patchwork of anachronistic security services, lack centralized management, and constantly need administrative crisis intervention to maintain baseline service levels. The consequence is more than lost productivity, inaccessible content, and scattered and unstructured intellectual property. The more acute penalty for e-mail's isolation from advanced and centralized network services is increased risk: security vulnerabilities, spam degradations, privacy issues, lack of policy enforcement, regulatory malfeasance, susceptibility to lawsuits and costly discovery demands, and under protected gateways in and out of an enterprise's essential systems and data assets.*

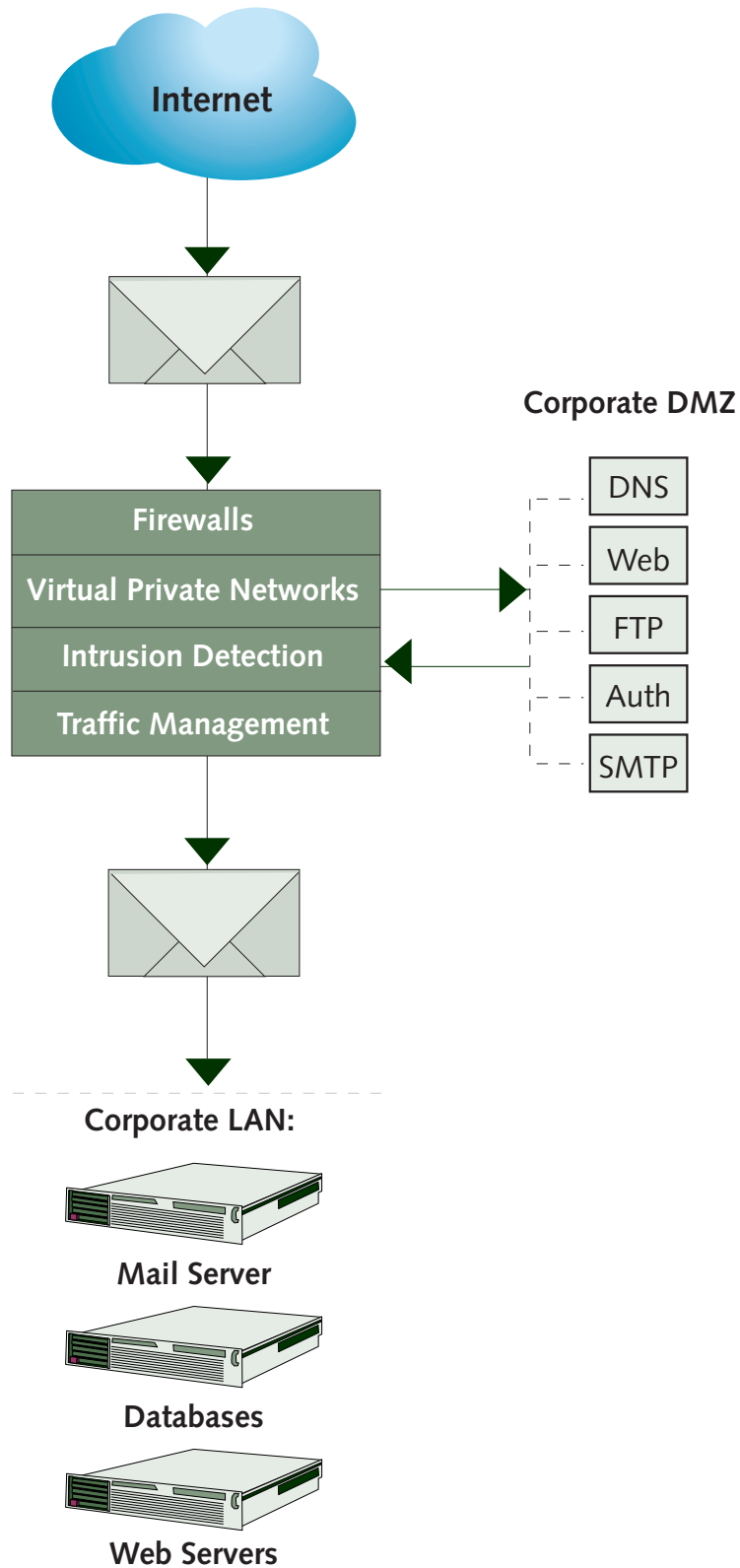
*What is needed is a collective message network infrastructure solution approach (see Exhibit 1), not additional piecemeal products from scores of vendors that fix weaknesses in individual servers but ignore the network and gateways.*

*The Yankee Group recommends enterprises, service providers, educational institutions, and government organizations take a network infrastructure approach to e-mail and related security and privacy issues.*

*Messaging-centric networks, built with network-based security technologies, allow appropriate automation and centralized control over the core components of messaging—directories, gateways, management, and storage—and set the stage for administrative and end-user policies. By seeking a network-based solution rather than a set of nonintegrated add-ons, users gain personalized control and administrators gain security, intellectual property protections, and significantly TCO.*

# Exhibit 1 E-mail's Isolation

Source: The Yankee Group, 2003



## Table of Contents

---

I.	Introduction . . . . .	3
II.	Unprotected E-Mail Means High-Stakes Poker . . . . .	4
	Spy vs. Spy . . . . .	5
	The Lingering Cost of Unprotected Systems . . . . .	5
	Centralized Control Strengthens the Perimeter . . . . .	6
III.	Seek a Message Network Solution . . . . .	6
	Network Control Extends to Messaging Hygiene . . . . .	7
	Market Needs a Best-of-Breed Message Network Vendor . . . . .	9
	A Glimpse at Future of Personalized Content Control . . . . .	10
IV.	Messages From the Field . . . . .	10
	Virginia Polytechnic Institute and State University . . . . .	10
	Illinois Tool Works, Inc. . . . .	11
V.	Conclusions . . . . .	11
	Recommendations . . . . .	12

---

### I. Introduction

Security and control over network content, especially content that moves through SMTP gateways and communications ports, has emerged as a top priority for enterprise, government, education, and hosting organizations. Increasingly, these organizations should seek reusable, network-based approaches to security that is multilayered and comprehensive, especially now that convergence between communications and data applications infrastructure is gaining momentum.

Gaining control of networks and communications applications is more critical to business operations than ever, yet is proving increasingly difficult to implement tactically. More applications and communications functions are open to more users, networks, and types of risks. Patches are hard to apply to every individual problem, and they ignore future risks and emerging threats. The Internet's permeable perimeters and messaging applications come at a price: corporate systems once shielded by a security perimeter are now exposed to the world of Internet users. E-mail borne spam is the most prevalent type of network intrusion in Microsoft Windows operating system environments.

These architectural changes contrast with the hard-perimeter techniques that dominated the security of the 1990s. Not long ago, network security focused on a hard perimeter of firewalls and authentication to lock out intruders, and an array of antivirus products to preserve host integrity. Most of these solutions were primarily geared toward analysis of IP packets moving in and out of a company's network, and were not geared specifically for critical e-mail-based communications (see Exhibit 1). Today, securing the wide area communications infrastructure requires gateway-level enforcement of security policy to analyze, identify, and filter messaging content.

Across corporate networks, the trusted security model of network intrusion-detection systems, which trigger alarms for IT action, has become overwhelmed. Consequently, network and communications application security is in a transition from a passive network intrusion detection model to an active network intrusion prevention model.

Active prevention means suspicious messages or attachments must be blocked in the network, quarantined with the possibility of retransmission, or transmitted along with a notification to IT. Active prevention takes immediate steps to prevent intrusions on systems and servers, and quell degradations early at or near the gateway. This approach requires rules, intelligence, and a message network to balance the needs of interconnectivity with the demands of security.

## II. Unprotected E-Mail Means High-Stakes Poker

The increased risk presented isolated e-mail systems was the reason most corporations maintained their security budgets from 2002 to 2003, even as they cut spending for other IT-related items, according to a joint Yankee Group/Sunbelt Software, Inc. security trends and spending poll of 400 IT managers worldwide. Yankee Group survey data also shows corporations in a holding pattern on network operating systems and evenly divided about security spending and the mechanisms used to defend their data.

The most dismaying—though not surprising—survey result is that an overwhelming 82 percent of organizations said spam adversely impacted their businesses (see Exhibit 2). By contrast, 74 percent of firms said they were victimized by computer viruses during the previous 12 months.

### Exhibit 2

#### Top Security Concerns for Enterprises

Source: Sunbelt Software and The Yankee Group, 2003

Choice	Count	Percent of Sample
Dealing with spam (unsolicited commercial e-mail)	230	82.4%
Software viruses	207	74.2%
Denial-of-service attacks	71	25.4%
Unauthorized use or modification of company data	29	10.4%
Hacking of company Web site	27	9.7%

E-mail risks also increasingly threaten such areas as intellectual property security, network boundary control, policy enforcement, and regulatory requirements. Companies must gain control over what takes place on their messaging systems, as well as what enters or leaves the organization. The risks on the reliability side of messaging are also high. Downtime is not an option. Many organizations depend on e-mail to function; without it, critical processes cease. Few organizations will tolerate an e-mail system that is not highly reliable.

## Spy vs. Spy

During the past several years, e-mail interactions have increasingly become the front end for many applications, portals, processes, and services—making any security or reliability flaws more apparent to an organization's many constituencies. IT faces viruses, spam, hacker attacks, DoS attacks, , mail bombs, directory harvests, password attacks, open relays, harassment, pornography, profanity, chain letters, e-mail floods, flames, leaks of sensitive corporate information, weak regulatory compliance—and the need to keep these systems running 99.999 percent of the time.

As e-mail's overall costs and risks continue to mount, administrators play *Spy vs. Spy*, implementing a series of defensive and offensive measures to deal with their messaging servers' vulnerabilities. However, security and reliability issues still grow, because many messaging-driven business processes extend beyond departments or enterprises to partners and sellers, directly exposed to mass consumers, students, and citizens via the Internet.

Many e-mail systems in use today were not designed for use in open and interconnected environments. Message networks, based on an infrastructure approach to security and policy enforcement, excel at providing a buffer and control layer between an organization's systems and the many different types of users accessing or attacking them.

## The Lingering Cost of Unprotected Systems

Unprotected and shoddily controlled messaging systems can cost organizations dearly. Consider these instances of high cost from insecure systems and an inability to enforce communications policy and procedures:

- More than 80 percent of computer viruses enter the network through e-mail, and the typical virus infection costs an organization up to \$500,000 per incident, according to Yankee Group analyst reports.
- Unnecessary e-mail costs the average U.S. business with 10,000 employees about \$16 million per year.
- During the mid-1990s, a Chevron subsidiary paid \$2.2 million to settle a sexual harassment lawsuit based on e-mail stored on its system.
- In a 1995 antitrust case, Ciba-Geigy was forced to search 30 million e-mails to produce required evidence. Ciba estimated the electronic discovery cost \$60,000.
- Five securities firms paid \$8.25 million in fines for failing to archive e-mails sought by regulators investigating analyst conflict of interest.

Inadequate and obsolete messaging systems and ill-managed networks cost billions of dollars annually. Moreover, the pressure on networks, applications, and e-mail administrators will build, not abate, during the next several years.

E-mail's vulnerabilities put entire business ecologies—webs of extra-enterprise commerce—at risk. Partner organizations must maintain the performance of their applications and services because service partners depend on them. The open, high-transaction environments leading to wide Web services adoption puts new pressure on

IT executives to play well and predictably in extended environments. These pressures require IT organizations to change the way they operate and seek a higher quality of service (QoS) for business-critical message networks, and focus on infrastructure as the strategic beachhead to implement the solution.

Many organizations continue to play high-stakes poker with their messaging infrastructure. The impact of not using a secure communications infrastructure can be severe. A new model of protection must evolve, because ad hoc controlled and managed messaging traffic cannot reliably secure business processes and assets.

## Centralized Control Strengthens the Perimeter

Enterprises once believed firewalls, content scanners, and intrusion-detection systems were sufficient to secure their networks. They believed e-mail server vendors had taken all the necessary precautions to guard them, their gateways, and their other systems from ill effects. The proliferation of Internet protocols such as HTTP, Secure Sockets Layer (SSL), and SMTP, however, left Internet-facing messaging applications vulnerable to attacks and has intensified awareness of perimeter security.

Yankee Group survey results make it clear that companies recognize the importance of computer security, and do act on it, particularly as it impacts e-mail. However, while the awareness of vulnerability is heightened, enterprises have just begun to take steps to address these weaknesses.

How can IT jibe the tactical need to quickly plug e-mail vulnerabilities and reduce the cost of spam with a longer-term strategic solution that controls entire networks? Organizations must increase efficiency by implementing security systems with more reach and more automation to respond to virus infections, spam, DoS attacks, and other losses of network integrity. Blind automation alone, however, comes with its own risks: Automated attack response can scale well, but can also block connections in a zero-sum way, without any balance or exception management. Spam detection false-positives are a high risk, because they are difficult to avoid and can cause wide-scale business disruption. The key is to implement automation that includes buffers against blind automation and unacceptable rates of false positives.

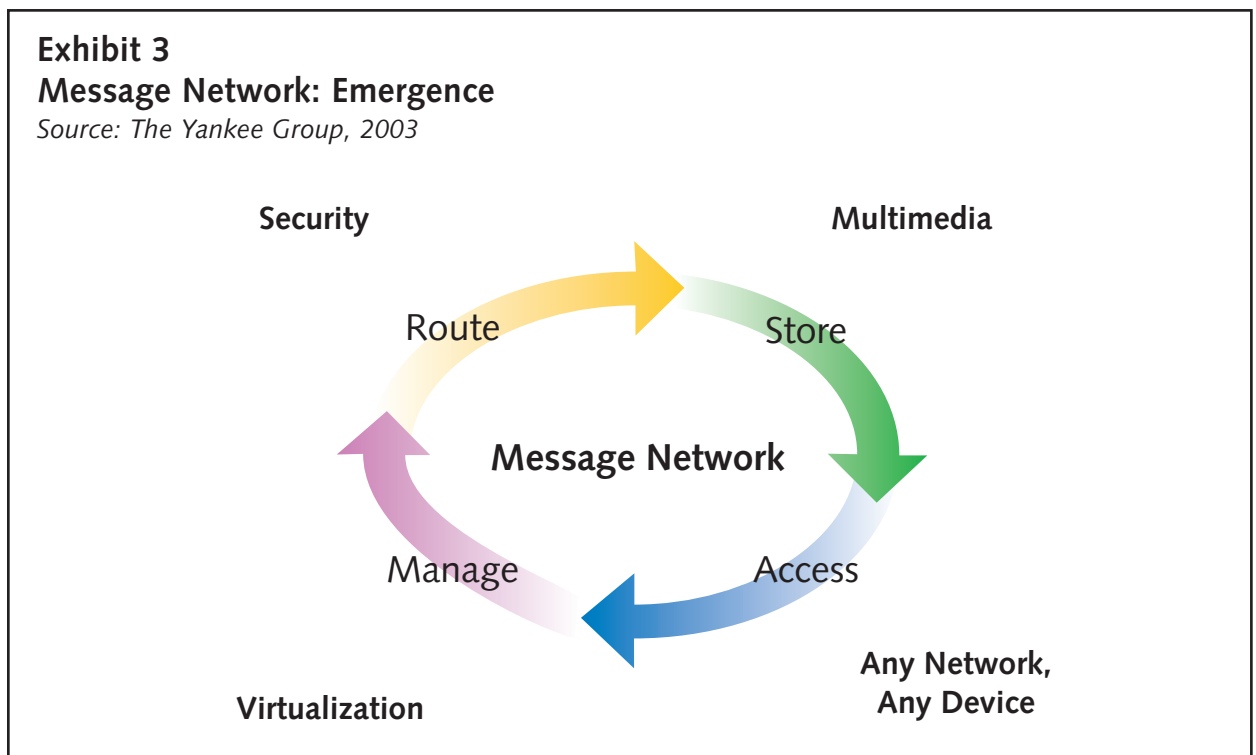
During the next 5 years, the Yankee Group predicts that intelligent message networks functionality—increasingly governed by user and administrator-driven policies—will join other security implementations such as firewalls, virtual private networks (VPNs), Web services security, security event management, and content filtering as an integrated approach to secure network connections. Organizations must disaster-proof their messaging systems and install what amounts to a 24/7 security watchtower. They must also set the stage for the invocation of policy-based management across their entire message network.

### III. Seek a Message Network Solution

A message network offers a strategic, integrated, holistic platform approach to messaging-oriented security vulnerabilities. Such an approach must join a secure, optimized messaging infrastructure with coordinated defenses against present and future viruses, attacks, and spam. The network must also manage resources, exploit ID management for policy enforcement, and support critical and often mandated messaging lifecycle services such as backup, disaster recovery and archiving.

These message network solutions, applied to all aspects of messaging traffic (routing, storage, access, archive, and lifecycle management), offer the dual benefit of personalized policy execution and enforcement, as well as a simplified and comprehensive approach to today's top-of-mind concerns for security and control over communications. The benefits also spill over in terms of lower TCO, and heightened levels of scaling and reliability. Shifting the security and policy burden to the network quickly realizes economies of scale. Furthermore, the network approach provides cost savings around executing and managing mobile device users and carriers in association with messaging and policy activities.

At their core, messaging servers consist of a switch, a gateway, a store, and an associated directory. However, messaging solutions that can solve today's issues of security, reliability, control, and contextual functionality require more than standalone components. There must be a balance between a high level of integration and flexibility to support open standards (see Exhibit 3).



This balance can be accomplished via a message network within a corporate network, where the essential functionality of reliable and secure messaging and policy enforcement are optimized and tightly packaged. This comprehensive message network should be simply deployed and maintained. Common management, the result of integration, should keep cost in check. Scaling the system should be a simple matter of adding additional server or appliance components.

### Network Control Extends to Messaging Hygiene

Message networks allow organizations to better control what takes place on their networks. They isolate the messaging and gateway functions from the general corporate networks until the security and content integrity work is complete. Message networks exploit directory and policy rules and apply them to traffic before the traffic hits the major systems.

The resulting demand on systems is relegated to delivering high-quality business-critical communications and data, not the miscellaneous items of the Internet. Message networks preserve the investments in infrastructure by intelligently brokering what should or should not tax these systems, and by protecting them from harmful executables. By doing so, message networks optimize what workers and resources are exposed to, reduce TCO, increase ROI, accelerate business processes, and enhance overall productivity.

Message networks offer additional productivity benefits by applying general policy conformity—best practices for security and regulatory issues and other governance patterns—across many other communications and application-management functions. By leveraging such networks, policies, regulatory compliance, and best practices can be continuously defined, instantiated, refined, managed, and enforced.

Consequently, the message network enables personalized and policy-driven service, regulatory and best-practices approaches across business processes. These benefits are directly tied to the primary way data, communications and processes are delivered: e-mail. Message networks can make a great deal of difference in how well a business operates.

Message networks should extend management and control to all e-mail traffic, incoming and outgoing, as well as internal messages and behaviors. Traffic management and delivery policy enforcement protects sensitive and confidential information, and helps prevent harassment and pornography dissemination. Best-practice enforcement methods include gateway-level blocking, tracking and logging e-mail to and from known threats or offenders, and sequestering messages for granular destinations such as competitors or nonpaying clients.

Furthermore, message networks can assist with timely and appropriate archiving of specific types of content, auto archiving confidential information and creating quarantine queues for questionable correspondence. They also help monitor traffic flow for network optimization and overall regulatory enforcement, can provide disaster recovery, and can adjust to changing regulatory requirements.

Directory and ID management (and an appropriate level of integration for the directory) is another critical element of message networks. Directories need higher levels of security today to prevent nefarious password and directory information harvesting.

Directory services management packages also extend the baseline capabilities of the underlying directory services mechanism. They perform tasks like domain migration and consolidation, user migration and directory-based policy management. The network helps automate many tasks that were done manually before directory services networks. The packages also deliver advanced features such as detailed statistical analysis and reporting.

A message network system should complement existing security investments such as firewalls and VPNs, and exploit improved architectures and systems. It should also work with the existing mail server. Message networks should be integrated, unified, and logical, and work well with other security approaches.

Message networks that optimize and extend protection will quickly remove e-mail vulnerabilities from the top concern list for IT administrators. When security issues are under control, there is higher reliability at a lower cost, and the additional productivity benefits of control and management can be exploited. Organizations that deal continuously with security breaches have difficulty moving to higher-order productivity benefits: Organizations that embrace message networks have a significant competitive advantage.

## Market Needs a Best-of-Breed Message Network Vendor

Mirapoint, Inc. of Sunnyvale, Calif., provides message network functionality that tackles security, reliability, and ease of deployment with the lower TCO and the operational efficiency of server appliances. Via its architecture, breadth of services, and the balance of standards-based interoperability with platform integration, Mirapoint is vying to become the best-of-breed provider of e-mail and security appliances designed for message networks.

Several aspects of Mirapoint's approach are unique. First, Mirapoint optimized the hardware and software of its leading appliances into packages specifically designed for message networks. The appliance packaging consists of integrated hardware, application software, operating system (a locked-down Unix-based kernel), and embedded integration to storage options such as SAN or NAS.

This optimization approach offers cost-effective reliability and high-scale messaging, especially from a long-term administration perspective. Tamper-proof kernels and other lock-down benefits reduce the likelihood of intrusion, error, and version or patch confusion. Appliance-based servers and networks also allow deployments to get and stay current on systems, computer security patches and fixes, since updates and enhancements are automatic and quickly and easily accessible over the network.

Mirapoint is also notable as a message network vendor because of its management and customization tools for gateway-level spam protection, specialized spam recognition and tagging intelligence, personalized end-user controls for spam management, powerful content filtering, and policy enforcement tools. These security benefits set the stage for the message network benefits of policy management and the accompanying productivity and process control solutions.

The Mirapoint appliance offerings consist of the Mirapoint Message Director, Message Server, and Directory Server.

Mirapoint's Message Director is a self-contained e-mail security appliance with boundary control over incoming message traffic to help defend against spam, virus and hacker attacks. It can process millions of messages per day, and provides policy enforcement and message tracking protection for outgoing traffic. The standards-based Message Director can also secure an existing e-mail server such as Microsoft Exchange Server.

Mirapoint's e-mail appliance brings together high-performance software, a contained operating system, and redundant hardware components to deliver an appliance specifically optimized for e-mail. Message Server can be deployed quickly compared to many of its competitors, to can provide rapid service-enablement for access to any standards-based e-mail client device, or value-added applications such as group calendars and address books.

Mirapoint's Lightweight Directory Access Protocol (LDAP)-based directory appliance provides a single point for user and system management of message networks. Capable of supporting tens of millions of entries, the Directory Server helps simplify management of large multitiered or distributed messaging environments. The Directory Server also integrates with other applications to provide centralized management and a single point of authentication.

## A Glimpse at Future of Personalized Content Control

In November 2003, Mirapoint introduced its Full-Spectrum e-mail security technology, which is designed to provide high spam containment with low false positives. Mirapoint claims 96 percent catch-rates with near-zero false positives. Full-Spectrum is a multilayered approach to addressing spam at the e-mail gateway, and provides personalized controls so end-users can individually identify spam to avoid lost messages and continually improve effectiveness.

The process analyzes messages based on information in the header, envelope, subject, and attachments, and scores the risk accordingly. If the score exceeds a defined threshold, the message is tagged as spam and the appropriate action is taken. Managers can elect to take appropriate action based on the magnitude of the filtering score, such as block, delete, forward, discard, remove attachments, or tag the message in the header or subject line.

Rules on how to best react to the scores can be set by end users themselves, or IT managers can create white lists, black lists, and filtering rules that essentially adjust the spam threshold for the message traffic. Managers can also develop unique domain or system-level white lists and black lists. The product can create new spam rules on an ongoing basis that are automatically provided to customers via network-based updates.

Mirapoint's approach to security includes quarantine queue and management tools for handling queued messages, comprehensive coverage and filtering of outbound traffic, and tools for addressing corporate liability such as policy-based message filters. The system applies the policy benefits of the message network capability to the vexing spam issue; the paradigm for spam containment can be applied to current, future, or unanticipated security breaches.

## IV. Messages From the Field

Mirapoint users find, regardless of their legacy messaging capabilities, the flexibility of Mirapoint products—used separately or in tandem—quickly brings the benefits of message networks home.

### Virginia Polytechnic Institute and State University

Virginia Polytechnic Institute and State University in Blacksburg, Va., messaging and security administrators have added Mirapoint Message Director to their Sun Microsystems Sun ONE POP e-mail system, which handles some 60,000 active user in-boxes.

Virginia Tech has used the Mirapoint Message Director for antivirus support since 2000, and for antispam protection since mid-2003. “We rode out many of the virus spikes that others went down for. We have not had to shut down our server for clean up or other virus problems once,” said William Dougherty, team leader of the telecommunications and client tools team at Virginia Tech.

Dougherty said he looks forward to new versions of Mirapoint products, such as Full-Spectrum, to gain even better control over spam, which he estimates at up to 60 percent of average daily e-mail. The Mirapoint Message Director-based antispam capability has eliminated all but 5 percent of spam with very low or no false positives. “We’re pleased, but we’re hoping to get even better performance [from Mirapoint Full-Spectrum],” he said.

## Illinois Tool Works, Inc.

Illinois Tool Works, Inc. (ITW), in Glenview, Ill., has its global business units direct their e-mail to the company's headquarters first, where Mirapoint's appliance checks it for spam and viruses, and then it is forwarded it back to the units over a VPN.

"We're very decentralized, so we were looking for an all-in-one appliance, instead of having to integrate products," said Marc Palano, IT director with ITW, a global manufacturing and components development conglomerate with 52,000 employees and about 10,000 corporate e-mail users.

Of the hundreds of thousands of e-mails the Full-Spectrum system sifts through per day, and catch about 50,000 spam e-mails, said Palano. Based on ITW's TCO analysis (for 5,000 users) during 2003, they experienced a 26 percent ROI by migrating users off third-party virus, spam, and messaging platforms and centralizing on the message network supported by Mirapoint products. ITW estimates that ROI will extrapolate to 118 percent by 2004, 177 percent by 2005, and 213 percent by 2006. This analysis takes into account the yearly recurring costs of hardware and software support, license fees, and administration costs.

## V. Conclusions

The Yankee Group recommends enterprises start now to develop messaging solutions based on the concept of a message network. These networks include several key elements working in technical harmony for high performance, security, control, manageability, and lower TCO.

The shift from uncoordinated standalone features to a network infrastructure or platform approach provides an opportunity for automation and efficiency, as well as the means to manage higher levels of complexity. The triad of business goals—reliability, better management, and lower TCO—must begin with the infrastructure. Messaging systems are low-hanging fruit administrators can improve upon using a network-within-a-network approach.

Enterprises, universities or government agencies that have portions of their user communities relying on portal-based e-mail such as Hotmail, or that use e-mail services from Internet service providers, should quickly consider delivering these services via an infrastructure that supports a protective message network. This can be done by bringing the e-mail function in-house via a message network: If this is not possible, they should make sure e-mail services providers employ best-practices message-network defenses and include these demands in future service-level agreements.

Service providers must quickly implement strategic defenses against bandwidth-consuming virus or DoS attacks and spam, and must address outgoing threats such as propagating viruses or spammers within their network. Service providers that guarantee greater availability and fewer security problems will be able to charge more for higher service levels, while cutting their internal operational costs. The policy and personalization features in message networks will also help the hosting organization to segment services, meter, and track various QoS levels.

Vendors entering the message networks space should cater to the problems enterprises face now, but should also prepare for the security, reliability, and cost issues that will occur during the next five or more years. Vendors should articulate a migration plan for customers based on how a flexible security platform can effectively anticipate future network integrity issues and provide the means to future-proof their systems.

Mirapoint's products and its flexible, integrated platform paradigm offer an alternative to the complexity, vulnerability, and expense of many messaging and ID management products. It also provides a coordinating network, unlike hundreds of ancillary security products on the market. Mirapoint's current and future offerings are geared toward a message network that balances the need for best-of-breed features with an optimized software and hardware foundation, and tight integration with third-party providers for a more secure and manageable messaging infrastructure. The products also exploit the unique benefits of the optimized appliance configuration.

Appliances that form these networks allow for unified policies that can be defined, instantiated, managed, and enforced. Consequently, the network enables personalized and policy-driven QoS, regulatory, and best-practices approaches across business processes. Tying these message networks to all aspects of messaging traffic (routing, storage, access, archiving, and management) reduces security vulnerability and eases the inclusion of security defenses as they mature and adapt.

A secure, optimized messaging infrastructure encompasses antivirus defense, antispam defense, management of resources, ID management, policy enforcement, and associated professional services. It also offers personalized policy execution and enforcement, as well as a simplified and comprehensive approach to today's top-of-mind security and communications control concerns. Appliance server architectures along with a message network approach bring simplicity, reliability, manageability and lower total costs due to reduced administration loads, compared to traditional general-purpose approaches.

A network services infrastructure optimized for messaging and security allows integration and reuse of components such as directory, management, storage, and policy enforcement. These are new benefits to end users and administrators. The move to a network infrastructure solution is in line with the advances that made Web applications and storage networks more robust. It is time for messaging systems to catch up to the rest of the IT infrastructure.

Large organizations that seek to secure and control messaging functions should evaluate a message network approach. The alternative is to continue to patch and upgrade point e-mail solutions that do little to address the security and policy enforcement needs from an infrastructure perspective.

## Recommendations

To evaluate the benefits of a personalized message network and the operational efficiencies of server appliance infrastructure, organizations should:

- **Find a holistic, platform approach to security.** This addresses the interwoven nature of these threats—i.e., hackers, spam, and viruses—and looks beyond short-term security threats by putting a strategic architecture in place for addressing future threats.

- **Begin examining the network from a network-messaging perspective—now.** The time to bring comprehensive security and lower administrative complexity to messaging systems is upon us, before security and regulatory demands become too burdensome.
- **Proceed with caution.** Although companies should begin immediately, it is a bad idea to rip-and-replace messaging systems without a well-conceived migration plan in place. Start with a departmental or division-level move to message networks, and incremental use of policy to drive messaging QoS. The advantages of these systems can then be applied more generally across the entire messaging infrastructure and content lifecycle.
- **Perform a thorough cost and performance analysis.** Make a realistic assessment of the current infrastructure and weigh it against future security and reliability needs. Map out a timetable for the migration and construct an organizational chart. Focus on year-two and year-three management and operations investment costs to ensure TCO declines over time.
- **Address budget issues.** Make sure the necessary funds are available to cover all aspects of message networks migration before proceeding.
- **Choose a vendor with a history of success delivering the solution.** When choosing a vendor for something as critical as message networks (and security in general), administrators should look to vendors that can act as a partner. This means the vendor can deliver a solution, not just a point product. Other factors include the vendor's ability to provide best practices with regard to deployment strategies, a demonstrated history of providing quality products, expertise in e-mail and messaging-specific security requirements, and experience working with enterprise-level customers.

## Did You Know The Yankee Group...

- Is a **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 offices and research staff in **North America, Latin America, Asia-Pacific, and Europe/Middle East/Africa (EMEA)**.
- 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 research reports and research notes** via the Internet and Lotus Notes.



ACCURATE RELIABLE TRUSTED

**The Yankee Group** is a global leader

in technology research and consulting.

Our customers, which include technology

vendors and users, benefit from our

accurate, reliable, and trusted research,

consulting, and personalized one-to-one client interaction

covering communications and IT products and services.

Now in our fourth decade, the company is headquartered

in Boston and maintains offices throughout

North America, Europe, Latin America, and the Pacific Rim.



ACCURATE RELIABLE TRUSTED



# 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

### Asia-Pacific

Itochu Enex Bldg., 6F 1-24-12  
Meguro, Meguro-Ku  
**TOKYO 153-8655 JAPAN**  
T 81.3.5740.8081  
F 81.3.5436.5057  
asiainfo@yankeegroup.com

### EMEA

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

### Latin America

Alameda Santos  
234, 7º Andar, 01418-000  
**SÃO PAULO, SP, BRASIL**  
T 55.11.3145.3855  
F 55.11.3145.3892  
info@yankeegroup.com.br

## Advisory Services

Yankee Group AnalystDirect 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 40 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.

---

## For More Information . . .

Phone: 617.956.5000, Fax: 617.956.5005. E-mail: [info@yankeegroup.com](mailto:info@yankeegroup.com). Web site: [www.yankeegroup.com](http://www.yankeegroup.com).

## ACCURATE • RELIABLE • TRUSTED

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.