

September 21, 2005

The State Of Security In SMBs And Enterprises

by Natalie Lambert and Michael Speyer

DATA OVERVIEW

**by Natalie Lambert and
Michael Speyer**
with Laura Koetzle,
Robert Whiteley, and
Sarah Bernhardt

September 21, 2005

The State Of Security In SMBs And Enterprises

Business Technographics North America

EXECUTIVE SUMMARY

Forrester surveyed 798 technology decision-makers at US small and medium-size businesses (SMBs) and 1,402 IT decision-makers at North American enterprises to understand the state of IT security. Seventy-one percent of SMBs will invest in additional security technologies by the end of 2005. Viruses, worms, spyware, and spam are SMBs' top IT security concerns. Furthermore, enterprises list upgrading their security environment as their No. 2 overall priority, so it's no surprise that 62% will spend more on IT security in 2005 than they did in 2004. In 2005, enterprises will continue adopting network quarantine — most notably, 39% of finance and insurance firms have already deployed it. Symantec is both SMBs' and enterprises' top vendor for desktop and security software, but Cisco heads enterprises' shortlists for network-centric security technologies.

TABLE OF CONTENTS

2 IT Security Concerns And Adoption In US SMBs

3 SMBs — Threats And Adoption Trends

5 Enterprise Security Spending And Technology Adoption

6 Security Priorities And Spending

7 Drivers And Obstacles When Adopting Security

8 Security Adoption Across The Network

9 Appliance-Based Security Adoption And Drivers

10 Enterprise Vendor Preferences For Security Technologies

11 Enterprise Vendor Preferences

12 Supplemental Material

IT SECURITY CONCERNS AND ADOPTION IN US SMBs

Recently, Forrester collected data on security concerns and security technology adoption trends from 798 US small and medium-size businesses.¹ Forty percent of respondents work for companies with six to 99 employees, 43% have 100 to 499 employees, and the remaining 18% represent firms with 500 to 999 employees. We found that:

- **SMBs will purchase a broad range of security technologies.** SMB IT groups consider viruses, worms, and spyware to be their most dangerous security threats. For that reason, 59% of them will purchase network firewalls, 57% will purchase antispymware software, and 45% will purchase host antivirus software in 2005. However, only 21% of SMBs will purchase host-based IPS, and only 13% will buy patch management — key technologies used to prevent viruses and worms. Because only 20% of SMBs consider internal hackers a top security issue, SMBs are not adequately protecting themselves against internal attacks. Unfortunately, their concerns are misguided; the recent CSI/FBI Computer Crime And Security Survey states that internal attacks are occurring as often as external attacks.²
- **Symantec is SMBs' top security vendor.** Symantec was a preferred vendor for 66% of SMBs. More than one-third of SMBs will also consider McAfee for security software.
- **SMBs need IT security consulting services.** Security assessment and planning made SMBs' lists of the top three consulting services they will buy in 2005.³ Thirty-seven percent of SMBs will purchase IT security assessment and planning consulting services, and the number grows to 43% for companies with 500 to 999 employees. Increasingly sophisticated security threats and increasingly complex threat prevention technologies are forcing SMBs to seek outside expertise to help with their security issues.
- **Utilities and telecom and manufacturing will buy the most security software.** Overall, 71% of US SMBs will purchase security software in 2005. The biggest spenders will be utilities and telecom firms and manufacturers, with 77% of each planning to purchase security software. Why do only 65% of media, entertainment, and leisure firms and 58% of finance and insurance firms intend to buy security software? Because more than 80% of each went shopping in 2004. Today, they're busy deploying what they bought.⁴

SMBs — THREATS AND ADOPTION TRENDS

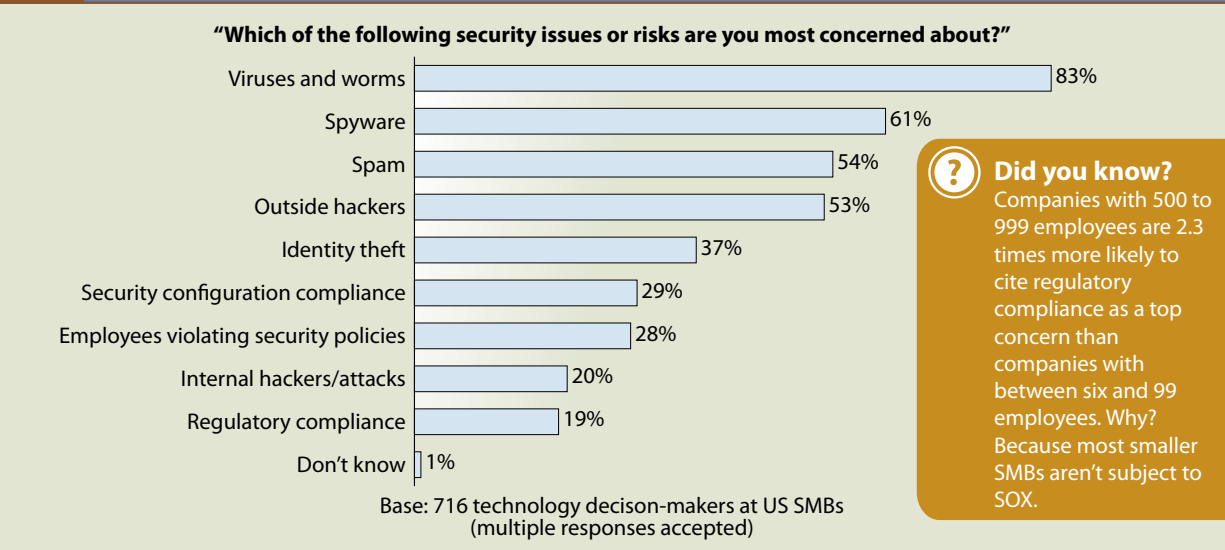
Viruses and worms are a top concern for SMBs — 83% of respondents see them as a risk to their IT organization. Spyware, the category of malicious code that includes key loggers and trojans, takes second place on the most-wanted list. Considering that insiders perpetrate about 50% of all attacks, it's worrisome that only 20% of SMBs are on the alert.⁵ SMBs are deploying a wide variety of client- and network-based technologies to combat these threats. Fifty-nine percent of SMBs will invest

in network firewalls in 2005; and close behind are the 57% of SMBs that will invest in antispyware technologies. However, with spam as the No. 3 threat to SMBs, it is surprising that only 37% of them will invest in spam filtering technologies this year.

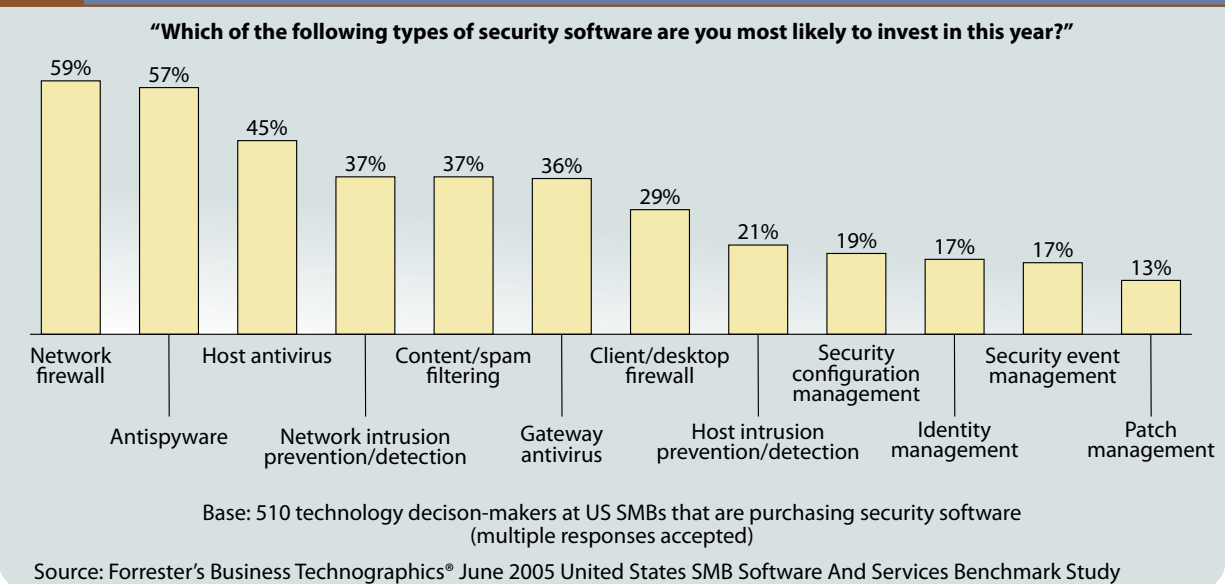


Related Research:
 "What To Do About Spyware"
 November 9, 2004, Best Practices

1 - 1 Viruses And Worms Top The List Of Risks; Regulatory Compliance Is Not Seen As An Issue



1 - 2 Technology Adoption Is Slightly Out Of Sync With Current Threats



Symantec dominates the SMB security software market. Nearly two-thirds of SMBs will consider Symantec, while only 35% put competitor McAfee on their shortlists. Seventy-one percent of SMBs will purchase security software in 2005. Although there is little variance by company size, only 58% of finance and insurance firms will purchase security software. However, three-fourths of

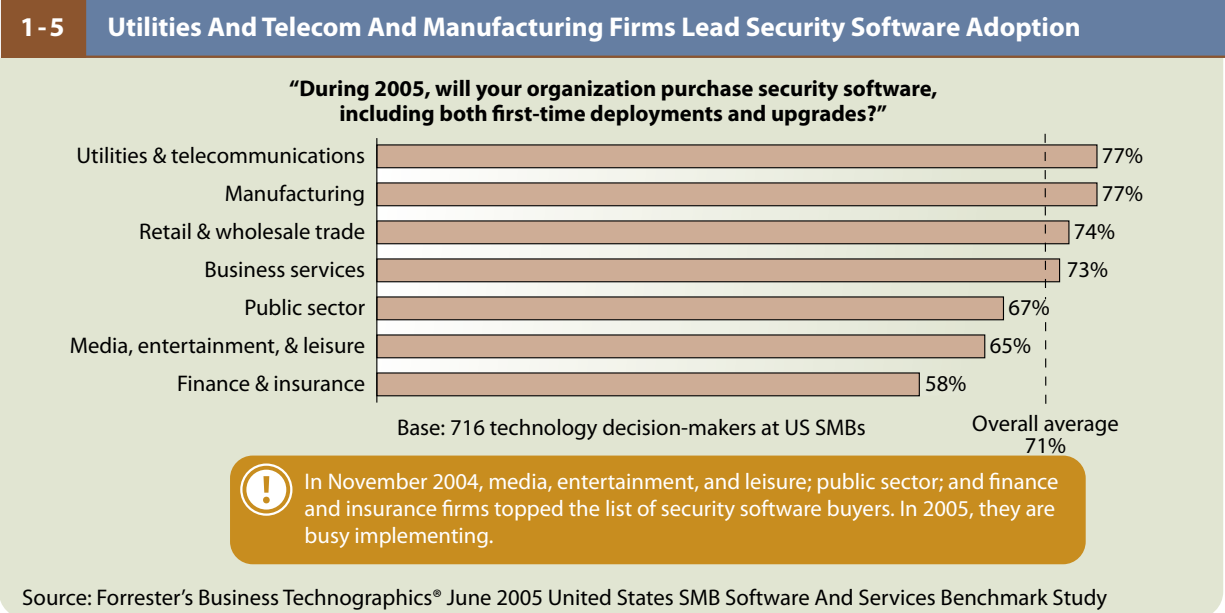
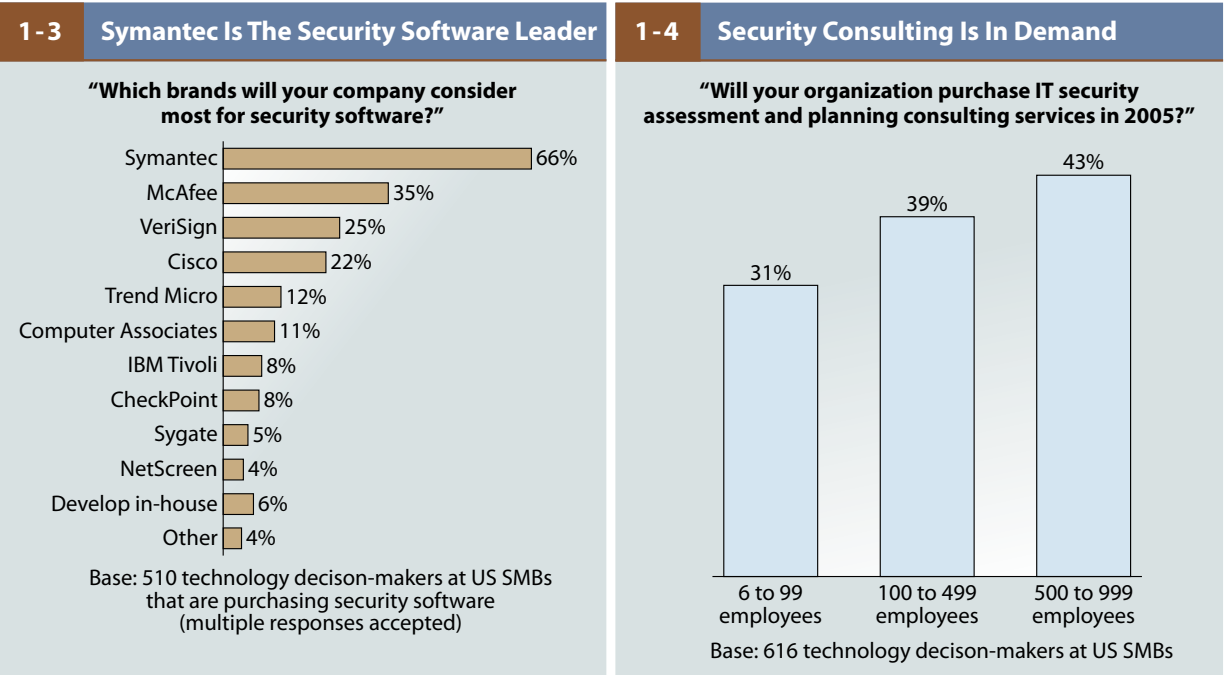
utilities and telecom and manufacturing firms will purchase security software.



Related Research:

“The State Of IT Spending In SMBs: Business Technographics United States”

November 18, 2004, Data Overview



ENTERPRISE SECURITY SPENDING AND TECHNOLOGY ADOPTION

Forrester recently surveyed 702 network and telecom decision-makers and 700 infrastructure decision-makers at North American enterprises to gain insight into their 2005 IT security spending and technology adoption.⁶ We found that:

- **Upgrading security is a top IT priority this year.** Over the past three years, security upgrades have remained a top priority for enterprises: This year, respondents cited it as their No. 2 priority behind supporting regulatory compliance efforts. In addition, 63% of enterprises will spend more on IT security in 2005 than in 2004, making IT security the No. 1 IT spending growth area.⁷ Rising tides lift all boats, including IT security — public sector entities' IT budgets will grow by 4.9%, and 80% of them will have larger IT security budgets in 2005 than they had in 2004. Similarly, manufacturing firms' IT budgets will grow by 3.5%, and 70% of them will have larger IT security budgets.⁸
- **Cost overruns present the biggest challenge to security implementations.** Vendors largely satisfy customers' demands for reliability, availability, and scalability. But 35% of users run into significant deployment costs, and 18% struggle to manage their new security technologies. Simple manageability and infrastructure integration are important to 82% of enterprises when selecting a security product.
- **Network quarantine is gaining momentum.** Thirty-one percent of enterprises tell us that they are already using network quarantine, which Forrester defines as the dynamic restriction of network access based on compliance to security policy. This demonstrates that enterprises are integrating security into networking gear like switches and routers.⁹ An additional 16% of those aware of network quarantine will pilot the technology in the next 12 months as solutions mature and as vendors like Cisco and Microsoft ship more complete offerings. The uptake of network quarantine indicates a shift from traditional perimeter security that relies on network firewalls to a more distributed environment that emphasizes secure authentication coupled with endpoint security.¹⁰
- **Appliance-based security will experience modest adoption rates.** Nearly 20% of enterprises currently use appliance-based security technologies. Why? Because they're easier to manage and users believe they're more secure. Thus, enterprises will deploy multiple functions including intrusion prevention, network firewalls, and email security on both standalone and integrated all-in-one security appliances.¹¹

SECURITY PRIORITIES AND SPENDING

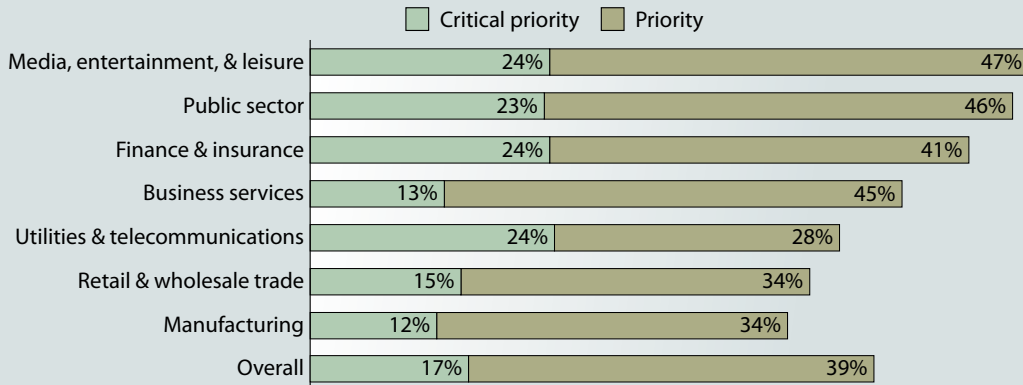
Security upgrades remain a top priority for North American enterprises. During the past two years, upgrading the security environment has not dropped below No. 4 on enterprises' lists of major IT themes. However, increased IT spending does not necessarily come with this priority. Seventy-one percent of media, entertainment, and leisure firms consider upgrading their


security environment a priority, yet only 57% will spend more on IT security than they did in 2004. Overall, 63% of enterprises will spend more on IT security than they did in 2004.

 **Related Research:**
 "IT Spending Continues To Focus On Security"
 June 29, 2004, Trends

2-1 Security Upgrades Are A Top Priority For The Third Year In A Row

"Will significantly upgrading your security environment be one of your IT organization's major themes for 2005?"



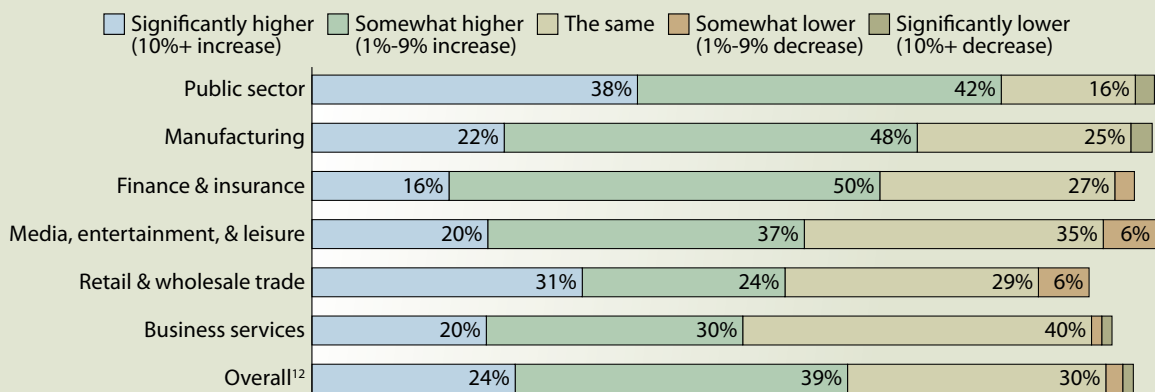
 In November 2003, upgrading the security environment ranked No. 1 on a list of 13 themes for IT spending; in November 2004, it dropped to No. 4.* In July of 2005, it was back up to No. 2.

Base: 700 infrastructure decision-makers at North American enterprises

Source: Business Technographics® July 2005 North American And European Infrastructure And Data Center Survey
 *Source: Forrester's Business Technographics November 2004 North American And European Benchmark Study and Forrester's Business Technographics November 2003 North American Benchmark Study

2-2 Enterprises Will See An Increase In IT Security Spending In 2005

"How will your IT security spending in 2005 compare to last year?"



Base: 407 telecom decision-makers at North American enterprises

Note: "Don't know" and "not applicable" responses have been excluded.
 Source: Forrester's Business Technographics May 2005 North American And European Network And Telecommunications Benchmark Study

DRIVERS AND OBSTACLES WHEN ADOPTING SECURITY

While 82% of enterprises overall state that infrastructure integration is an important driver, an overwhelming 95% of financial services companies tell us that this integration is important for their security technology purchases. Enterprises also want to simplify the task on managing their security environments. In addition, when enterprises are investigating technologies, 53% tell us that reliability is the most important factor they consider.

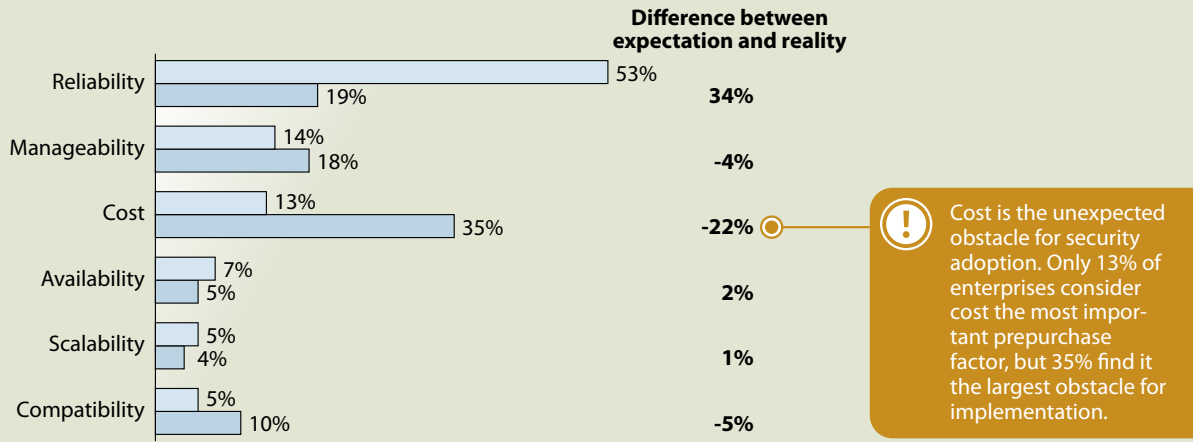
However, upon deployment, cost is the major obstacle that enterprises face. Surprisingly, firms don't consider scalability and compatibility to be terribly important factors either before buying or during deployment.



Related Research:
 "What Security Buyers Want From Technology"
 November 19, 2004, Trends

3-1 Cost Is The Unexpected Obstacle When Adopting A Security Technology

- "What is the most important factor you consider when acquiring security technologies?"
- "What is the largest obstacle you face when implementing security technologies?"



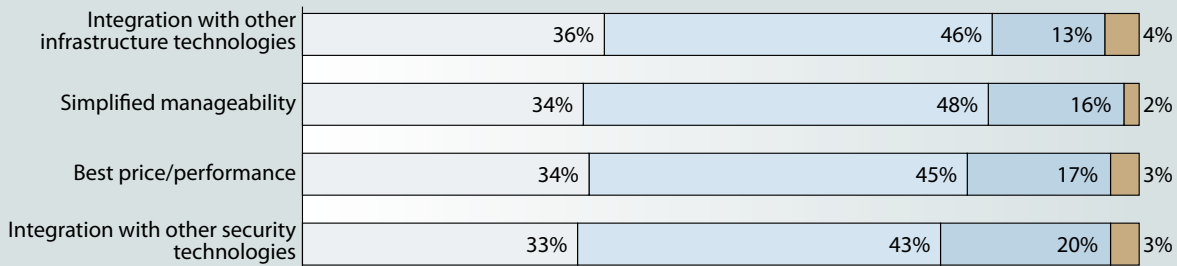
Base: 438 telecom decision-makers at North American enterprises

Source: Forrester's Business Technographics May 2005 North American And European Network And Telecommunications Benchmark Study

3-2 Integration And Simplified Manageability Are Important Drivers When Purchasing Security

"How important are the following drivers when purchasing enterprise security technologies?"

□ 4 — Very important □ 3 □ 2 □ 1 — Not important



Base: 438 infrastructure decision-makers at North American enterprises (percentages may not total 100 because of rounding)

Source: Business Technographics July 2005 North American And European Infrastructure And Data Center Survey

SECURITY ADOPTION ACROSS THE NETWORK

Network quarantine has already moved beyond the early adopter stage — 31% of enterprises are already using it, at least in pilot projects. Of the remaining 42% of enterprises that are aware of network quarantine, 16% plan to pilot it in the next 12 months. In addition, 41% of business services firms and 39% of finance and insurance firms are already deploying network quarantine solutions.

On the flip side, storage security applications have stagnated. Currently, only 20% of firms have implemented storage security, and only another 6% are planning to pilot the technology in the next 12 months. Today's adopters

include the business services industry, where 31% of firms are already using storage security applications.

XML security gateways, from vendors like DataPower Technology and Forum Systems, offer customers protection from unauthorized and malformed XML requests that may constitute an attack. However, only 26% of enterprises have already deployed such technology.



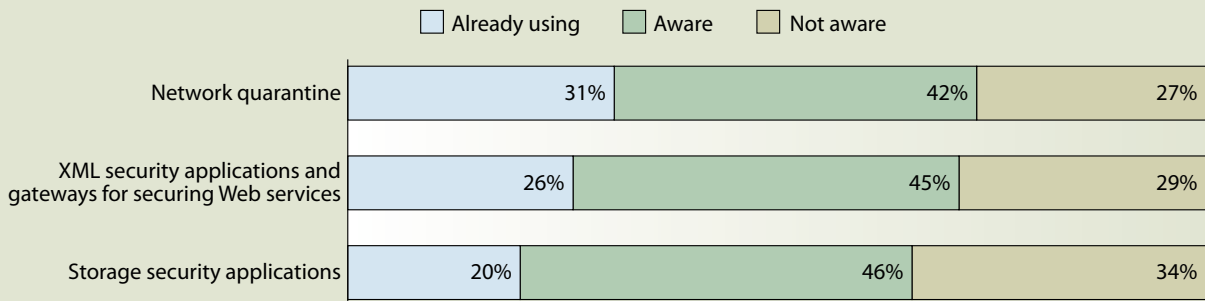
Related Research:

"Choosing The Right Network Quarantine Solution" June 28, 2005, Tech Choices

"Forrester Wave™: XML Security Gateways" March 29, 2004, Tech Choices

4-1 Almost One-Third Of Enterprises Are Already Using Network Quarantine

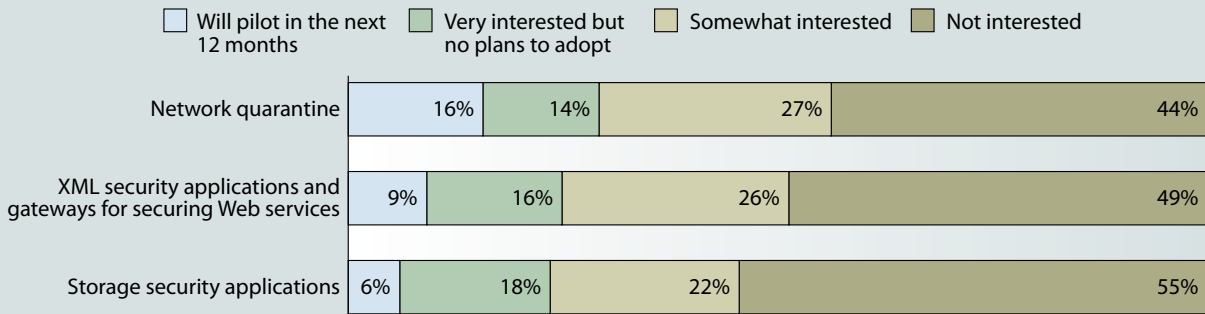
"For the following technologies, please indicate if you are 'aware,' 'not aware,' or 'already using' them."



Base: 438 infrastructure decision-makers at North American enterprises

4-2 Network Quarantine Will Start Its Growth Phase In 2005

"What is your level of interest in the following technologies?"



Base: infrastructure decision-makers at North American enterprises that indicated they were "aware" of each technology (percentages may not total 100 because of rounding)

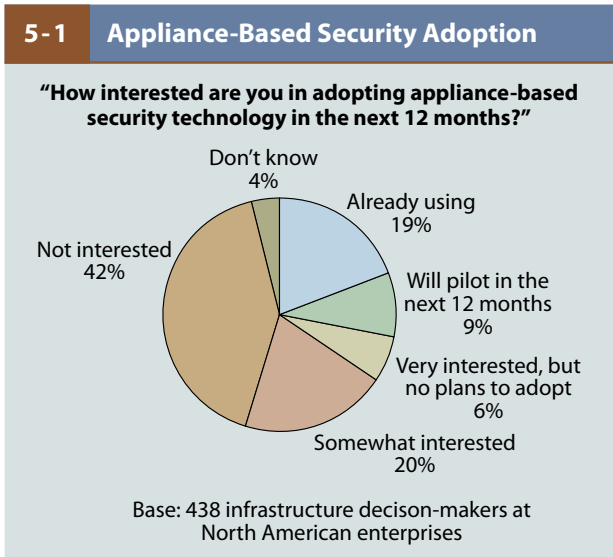
Source: Business Technographics® July 2005 North American And European Infrastructure And Data Center Survey

APPLIANCE-BASED SECURITY ADOPTION AND DRIVERS

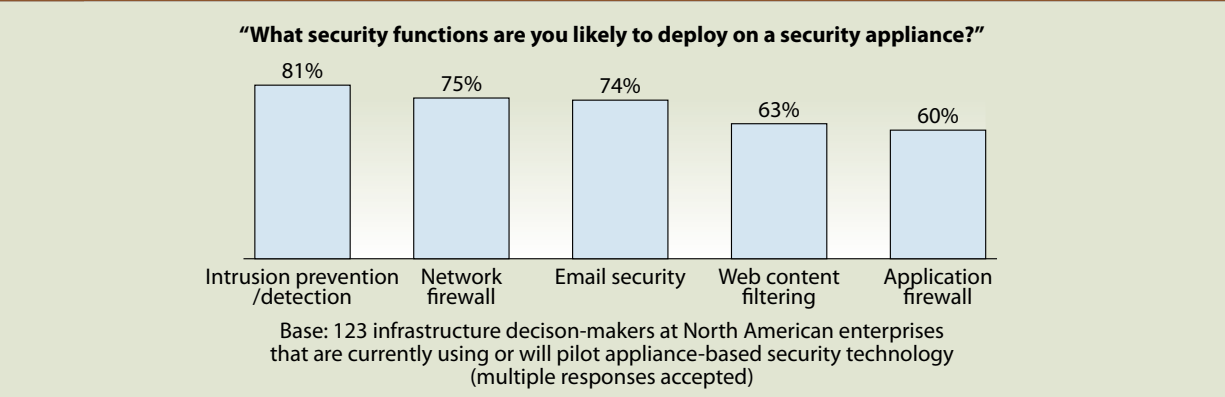
Despite compelling reasons to purchase security products as appliances, only 9% of respondents plan to pilot this type of technology in the next 12 months. Surprisingly, 42% have no interest in adopting appliances.

Of the enterprises that are using or will pilot appliances, 81% intend to deploy IPS or IDS on appliances. Other top functions that enterprises will deploy on appliances include network firewalls and email security. Appliance believers see obvious benefits, with 79% ranking simpler manageability as important, followed by 73% for improved security. Price/performance and functional convergence rank as less important, at 58% and 52%, respectively.

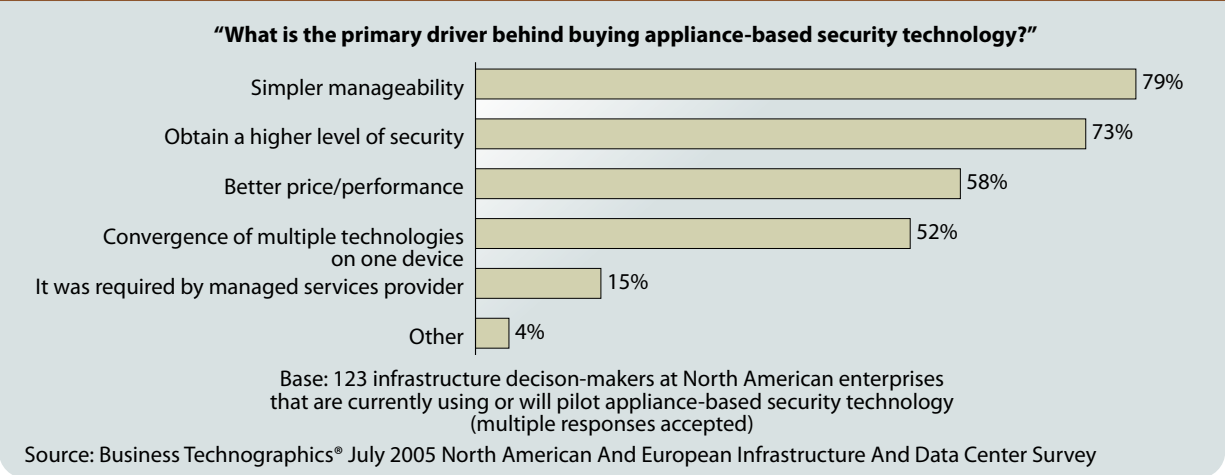
 **Related Research:**
 "Building A Security Architecture Around Appliances"
 June 24, 2005, Tech Choices



5-2 Enterprises Will Put Multiple Security Technologies On Appliances



5-3 Manageability Is A Key Driver In Appliance-Based Security Adoption



ENTERPRISE VENDOR PREFERENCES FOR SECURITY TECHNOLOGIES

Forrester also asked infrastructure decision-makers who are buying network quarantine, desktop security, data center and network security, and identity management technologies which vendors they will consider most for those solutions. We learned that:


- **Enterprises prefer Cisco for network-centric security technologies.** One-third of enterprises look to Cisco for data center and network security, and 44% choose Cisco for network quarantine solutions. This makes sense: Thanks to its Network Admission Control (NAC) campaign and recent acquisitions like Perfigo, Cisco has the most complete network quarantine portfolio. Check Point ranks a distant second behind Cisco, but its InterSpect and Integrity product lines are gaining traction as standalone network quarantine solutions. Absent for now is Microsoft, whose Network Access Protection (NAP) solution doesn't ship until it releases Longhorn (now called Vista) at the end of 2007, at which point the software giant will gain traction with midsize enterprises. Enterasys Networks, which has been shipping a switch-based solution longer than any vendor, garnered only 4% of enterprises' attention, a reflection of the company's small overall share of the enterprise network hardware market. The bottom line? If enterprises are going to buy a network hardware solution, Cisco is the vendor of choice.
- **Like SMBs, enterprises choose desktop security technologies from Symantec.** Symantec is enterprises' top choice for desktop security software, once again followed by McAfee at No. 2. Because Cisco is primarily a network gear vendor, it's a surprise to see it at No. 3 in client security. Are customers confused? No — they're responding to Cisco's NAC programs, its host-based IPS (CSA), and its general self-defending network strategy.
- **Nearly a quarter of enterprises buying identity management choose Microsoft.** Because of its robust directories and single sign-on (SSO) capabilities, 23% of enterprises consider Microsoft to be the strongest identity management player. IBM follows thanks to its broad portfolio and its strong Web single sign-on product, Tivoli Access Manager.¹³ Because identity management is a broad category that covers many technologies including directories, SSO, user provisioning, and access rights, customers also consider RSA Security, Computer Associates (thanks in part to its acquisition of specialist Netegrity), and Novell to be preferred suppliers for identity management.

ENTERPRISE VENDOR PREFERENCES

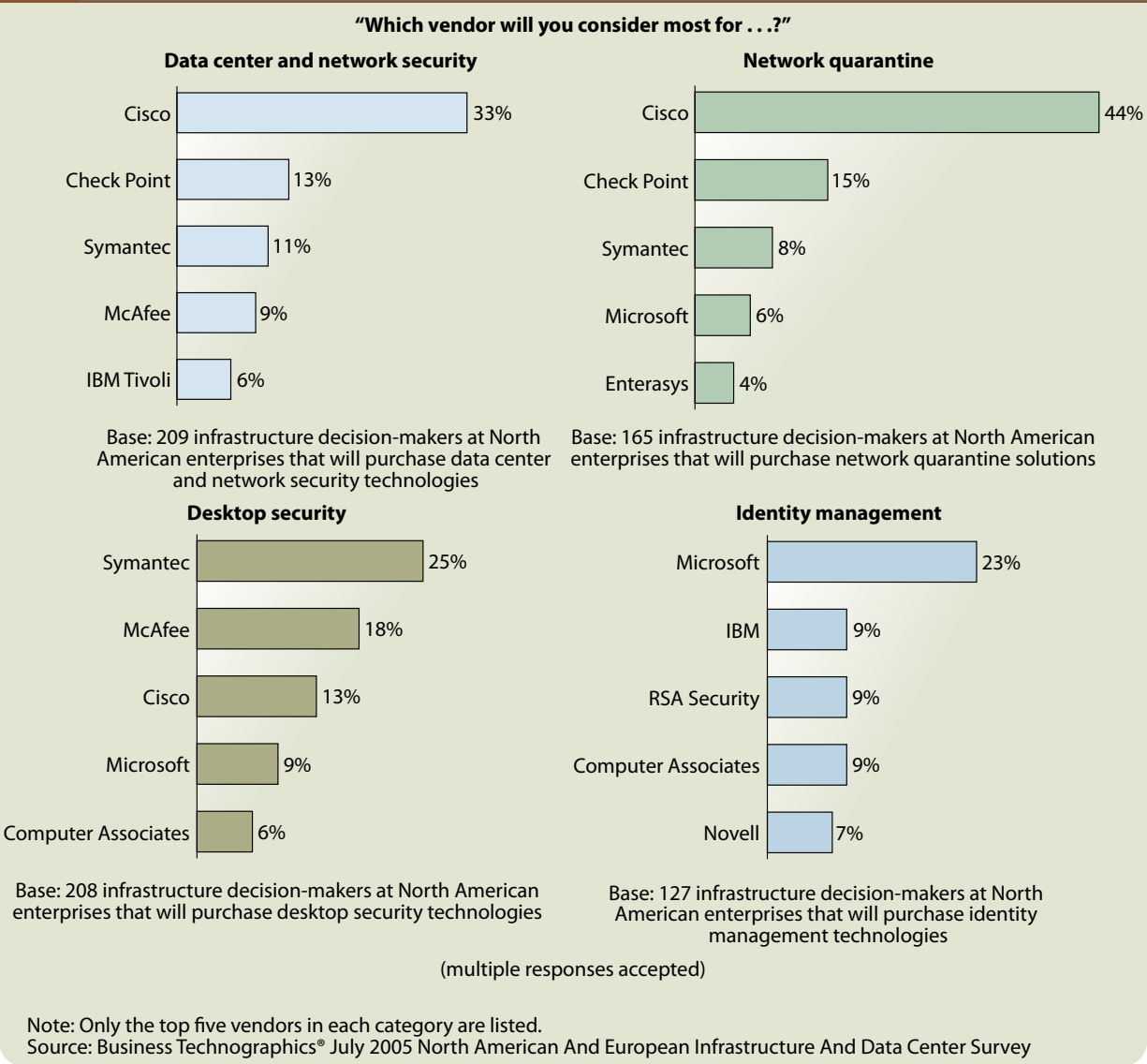
Enterprises prefer large IT security vendors. Cisco and Check Point head enterprises' shortlists for overall data center and network security, at 33% and 13%, respectively. Respondents display similar preferences for network quarantine — 44% of enterprises will consider Cisco, and 15% will look to Check Point. Cisco's strong showing reflects the increasing integration of security features into network gear.

Symantec still dominates enterprise desktop security, but less decisively than it does the SMB desktop market.

The identity management market includes a completely different set of vendors. Here, Microsoft takes the top slot with 23% of firms, followed by IBM and RSA Security, each with 9%.

 **Related Research:**
 "The Forrester Wave™: Client Security Suites, Q2 2005"
 June 22, 2005, Tech Choices

6-1 Enterprise Vendor Preferences For Security Technologies



SUPPLEMENTAL MATERIAL

Methodology

Forrester surveyed 1,005 infrastructure and data center decision-makers at North American and European enterprises. Of these, 700 are from North American enterprises, and 305 are from European enterprises. The sample is composed of 26% senior-most IT decision-makers, 39% executives reporting directly to the senior-most IT decision-maker, and 35% directors and managers in IT reporting directly to an executive. Fifty-one percent represent enterprises with 1,000 to 4,999 employees, 28% have 5,000 to 19,999 employees, and the remaining 21% have 20,000 or more employees. We screened all respondents for significant involvement in the purchasing process of infrastructure and/or data center technologies.

Evalueserve fielded the telephone-based survey in May and June 2005 and motivated the respondents by offering them a summary of the results.

We also drew from Forrester's Business Technographics June 2005 United States SMB Software And Services Benchmark Study and Forrester's Business Technographics May 2005 North American And European Network And Telecommunications Benchmark Study.

In addition to sampling error, one should bear in mind that the practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls. Other possible sources of error in polls are probably more serious than theoretical calculations of sampling error. These other potential sources of error include question wording, question ordering, and nonresponse. As with all survey research, it is impossible to quantify the errors that may result from these factors without an experimental control group, so we strongly caution against using the words "margin of error" in reporting any survey data.

These statements conform to the principles of disclosure of the National Council on Public Polls.

You can find more information about the data on the Survey & Data page online. From this page, you will be able to download the Survey Instrument.

ENDNOTES

- ¹ Forrester surveyed 798 technology decision-makers at small and medium-size businesses (SMBs) in the US to understand their software and associated services priorities for 2005. Source: Forrester's Business Technographics June 2005 United States SMB Software And Services Benchmark Study. See the July 7, 2005, Data Overview "Software And Services In The SMB Market: Business Technographics United States."
- ² Source: 2005 CSI/FBI Computer Crime And Security Survey (<http://www.gocsi.com>).
- ³ IT consulting services are in demand for US SMBs. The top three services that SMBs need are Web site design, application development, and IT security assessment. See the July 7, 2005, Data Overview "Software And Services In The SMB Market: Business Technographics United States."

- ⁴ In 2004, 75% of SMBs, led by finance and insurance firms, said that they would purchase new security technology. See the April 22, 2004, Data Overview “The State Of IT In The SMB Market: Business Technographics North America.”
- ⁵ Source: 2005 CSI/FBI Computer Crime And Security Survey (<http://www.gocsi.com>).
- ⁶ Forrester surveyed 1,007 network and telecom decision-makers and 1,005 technology decision-makers at North American and European enterprises to better understand their technology adoption. Sources: Forrester’s Business Technographics May 2005 North American And European Network And Telecommunications Benchmark Study and Business Technographics July 2005 North American And European Infrastructure And Data Center Survey. See the June 23, 2005, Data Overview “The State Of Network And Telecom Adoption: Business Technographics North America And Europe.”
- ⁷ Forrester asked respondents how their spending in 2005 would compare to last year in 10 different functional areas. IT security spending will grow the most, IP telephony came in second, and VoIP on the WAN came in third. See the June 23, 2005, Data Overview “The State Of Network And Telecom Adoption: Business Technographics North America And Europe.”
- ⁸ In November 2004, Forrester asked respondents how their company’s 2005 IT budget would compare to their actual spend in 2004. See the December 15, 2004, Data Overview “2005 Enterprise IT Outlook.”
- ⁹ Adoption of network quarantine will surge in the second half of 2005. Although Cisco will dominate this space in the long run, its solution for the LAN will not be ready for prime time until late 2005. As a result, many firms that need solutions now will purchase standalone appliances and software-only solutions. See the June 28, 2005, Tech Choices “Choosing The Right Network Quarantine Solution.”
- ¹⁰ The Jericho Forum, a powerful and vocal security user group that includes organizations like BP, Procter & Gamble, and the UK’s Royal Mail, aims to change the way we think about IT and network security. The Jericho Forum claims that current security models that concentrate on the network perimeter just don’t cut it in today’s business environment. The Jericho members introduce the concept of “deperimeterization” and encourage organizations to look at securing the data rather than the infrastructure that supports it. See the July 8, 2005, Quick Take “Jericho Forum Looks To Bring Network Walls Tumbling Down.”
- ¹¹ Fifty percent of enterprises prefer separate, stand alone appliances for security functions; 14% prefer all-in-one integrated security appliances; and 28% prefer security functions integrated into other networking equipment. See the June 23, 2005, Data Overview “The State Of Network And Telecom Adoption: Business Technographics North America And Europe.”
- ¹² This “overall” number includes the utilities industry, which has been left out of the industry breakouts because it does not have a statistically significant number of relevant responses.
- ¹³ IBM has been a major player in the identity management jungle and is the company against which all other vendors must compete. See the September 19, 2003, Idea Byte “Brace For Acquisition And Consolidation In The Identity Management Market.”

FORRESTER®

Helping Business Thrive On Technology Change

Headquarters

Forrester Research, Inc.
400 Technology Square
Cambridge, MA 02139 USA
Tel: +1 617/613-6000
Fax: +1 617/613-5000
Email: forrester@forrester.com
Nasdaq symbol: FORR
www.forrester.com

Research and Sales Offices

Australia	Israel
Brazil	Japan
Canada	Korea
Denmark	The Netherlands
France	Switzerland
Germany	United Kingdom
Hong Kong	United States
India	

*For a complete list of worldwide locations
visit www.forrester.com/about.*

For information on hard-copy or electronic reprints, please contact the Client Resource Center at +1 866/367-7378, +1 617/617-5730, or resourcecenter@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Forrester Research (Nasdaq: FORR) is an independent technology and market research company that provides pragmatic and forward-thinking advice about technology's impact on business and consumers. For 22 years, Forrester has been a thought leader and trusted advisor, helping global clients lead in their markets through its research, consulting, events, and peer-to-peer executive programs. For more information, visit www.forrester.com.