Equity Research
North America

Industry

Security Software

Peter Kuper
+1 (1)617 856 8751
Peter.Kuper@morganstanley.com
Brian Essex, CFA
+1 (1)617 856 8753
Brian.Essex@morganstanley.com

Industry Overview

May 25, 2005

Spyware — The AV Replacement Killer

GICS SECTOR INFORMATION TECHNOLOGY	
US Strategist Weight	12.9%
S&P 500 Weight	15.1%

COMPANIES FEATURED	
McAfee (MFE, $27.18)	Equal-weight
Microsoft* (MSFT, $25.71)	Overweight
Check Point Software (CHKP,$22.89)	Underweight
RSA Security (RSAS, $12.11)	Overweight-V
Symantec (SYMC, $22.13)	Equal-weight
Websense (WBSN, $51.92)	Equal-weight

** Covered by Mary Meeker.*

- **Conclusion: Spyware replacing viruses as greatest security threat**
  Low and slow is the new preferred attack vector and spyware is rapidly replacing classic viruses as the main threat. As a result, we expect additional pricing pressure for antivirus products. In the consumer market, antispyware (AS) products are available at low cost or for free providing less opportunity for vendors to capitalize on the segment. On the enterprise side, there are meaningful opportunities given the complexity of removal and the higher value of assets at risk.
- **What's new: The power of the privates driving bifurcation of the market**
  In our view, larger antivirus (AV) vendors have been slow and reactionary, giving privates a strong head start in AS. The market appears to be experiencing 'barbell' pricing with best of breed vendors with pricing leverage on one end and commodity products on the other. We anticipate that AV suite providers will offer AS as an enhancement to consumer security suites for little or no extra cost. Enterprises will likely be more profitable but again private companies should grab share.
- **Implication: Playing the spyware trend**
  In our view, Microsoft is clearly the best-positioned vendor to tackle AS, especially for the consumer. Yet an enterprise-worthy product may prove more of a challenge. Within our coverage universe, Websense may be the unrecognized best able to capitalize in spyware. McAfee and Symantec are already bundling or rebating AS, making it less a profit center and more a share protector, hence no upside in our models. Checkpoint has less opportunity here in our view as its strength is isolated to the firewall but could respond in part via Zone. In this report, we have also examined some of the leading private companies — Sunbelt, Tenebril, and Webroot.
- **Embedding, convergence and layered security**
  As we have indicated for other segments of the security software market, we consider AS yet another candidate for technology embedded within other software security solutions. Larger vendors are already increasing functionality within their suites, partly to augment AV pricing issues. We expect AS to continue to evolve beyond the desktop, becoming widely available at the gateway and within the network.
- **Industry View: In-Line**
  Because the problem of ongoing, evolving threats likely will never be fully countered, we expect continued demand independent of economic factors — but with a focus on specific sub-segments as security efforts shift to protection of the network and data.

Please see analyst certification and other important disclosures starting on page 16.

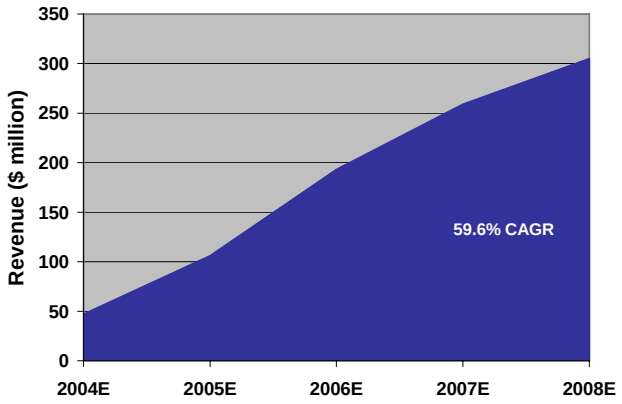
Spyware — The AV Replacement Killer

Summary and Investment Conclusion

Antispyware is the 'new' new thing for the security software industry. With commoditization and maturity facing more perimeter-focused segments of the security market, many companies are targeting what we see as the next major threat to data integrity. In the first quarter of 2005, Webroot found that 55% of the PCs it scanned had at least one form of unwanted programs — and this excludes potentially harmless cookies. Throw in those biscuits and the infection rate leaps to 87%. This contagion is causing serious concerns in the market. A recent survey of IT managers commissioned by Trend Micro and performed by TechRepublic indicated that 78% identified spyware among their top three priorities for 2005 and 87% of those surveyed thought that spyware would get worse before it gets better. These staggering statistics make it easy to accept that spyware, for security vendors, is a rapidly growing opportunity.

Exhibit 1

2004E - 2008E Spyware Market Forecast



Source: IDC

However, as spyware is becoming the preferred attack vector, we believe antivirus solutions offer less protection and hence less value to end users. The net affect is we see spyware spend as largely ablative, not incremental to total security software spend especially in the consumer market. Here we expect AV pricing to continue its decline with spyware solutions used to help offset further price compression. Within enterprises, we also see further commoditization of AV but there will be appreciable spend in AS products given the complexities and pressing needs of enterprise computing environments. Removal of spyware is a far greater undertaking in a 40,000 desktop environment than for one Windows XP home computer.

Given this, we have not upped our consumer revenue forecasts for either Symantec or McAfee. We have left them unchanged even in light of the Microsoft offering. We had expected the Microsoft move (although we did not a product so comprehensive as to expand beyond pure security tools via its OneCare offering) and see the spyware additions as a hedge against any accelerating price declines or market share erosion via the Redmond presence. Our expectations for timing of the Microsoft entry, which we had accounted for in our models, appears to have been right on track. For Websense, we have already seen the suite benefiting from the spyware abilities as enterprises upgrade and/or renew to add this extra layer of defense. For RSA, authentication should remain a key focus area but spyware is more an indirect play for them, in our view. Finally, for Checkpoint, we see limited opportunity given their traditional "slow to react" posture and the Microsoft offering limiting Zone upside in the consumer market.

Overview

Why the huge focus on spyware? It started in 2004 as the industry grappled with yet another attack vector. According to a study performed by Webroot Software and Earthlink ISP, a scan of 4.6 million computers in 2004 yielded an average of 25 instances of potential spyware per PC found (116.5 million total instances). Public awareness reached a peak when a *New York Times* editorial called for legislation, followed up by a Federal Trade Commission discussion of potential regulations to combat this pervasive IT security issue. IDC has estimated that the antispyware market will grow at a near 60% CAGR through 2008 to a $305 million market. Given IDC's relatively low starting point and our view of the potential for spyware as an ongoing threat, we believe that these projections are on the light side and that, long term, spyware threats will become more invasive and prevalent than antivirus threats. The financial rewards of antispyware could, in our view, power an opportunity as large as the antivirus market. Anyone questioning the last comment need only consider perhaps the most blatant example of the potential threat from spyware. Earlier this year Sumitomo Mitsui bank almost lost over £220 million due to a very well targeted spyware attack. From our

Please see analyst certification and other important disclosures starting on page 16.

industry sources, we understand it was stopped at the very last minute as traditional security software products were largely blind to this attack. Losses of that size would be devastating to any organization and a key reason why we expect the enterprise market for spyware to be very lucrative indeed.

For investors, however, we caution that in the consumer market we believe spyware is not an incremental spend — it will, over time, grow at the expense of the AV market. The easy example here is Microsoft, which has already indicated its spyware tool will be free to consumers (along with the firewall and other tools). We discuss the Microsoft implications, including its most recent announcement around OneCare, later in this report.

From our perspective, most of the larger public vendors are finally addressing the spyware market. We say "finally" as Symantec only had its product ready earlier this year (2005). Yet even as the market is seeing only increased attention, already we are seeing the largest suite vendors bundling in spyware as part of the antivirus suites — certainly in the consumer market. This is a primary driver behind our thesis that spyware will grow in large part from inclusion in a security suite that will over time not experience pricing power but will be recognized more as a pricing-pressure relief valve in the rapidly commoditizing AV market as more vendors offer security as a functionality or tool.

The following are a few key factors shaping the antispyware market today:

1. **Is antispyware the next generation of antivirus?** Spyware differs from viruses in that spyware seeks to use and exploit hosts whereas viruses typically seek to destroy them. However, a primary method to combat spyware is to develop signatures through research and block threats, just as antivirus technology does. As a result, we see spyware as a natural fit for antivirus vendors and vice versa. We will even go as far as to say that soon antivirus software will not be needed at the desktop level. If the enterprises have strong desktop firewalls and good (active) antispyware software at the gateway and client levels, AV should become largely irrelevant. The nature of this concept dictates that suite vendors will need to carry antispyware capability in order to sustain their security suite models. From an investment perspective, we believe antispyware will become the new AV, replacing it as the key value proposition. After all, antispyware blocking technology blocks unwanted executable files. This is just what AV does, but AV does it on a simpler and more commoditized level. When the .dat signature file is uploaded, we suspect it will be more targeted towards the spyware engine and less to the AV filter. Therefore, we see no reason why antispyware cannot ultimately handle the vast majority if not all of AV threats.

2. **Privates lead the segment**. We are seeing more of the larger public vendors racing to catch up to the privates which, according to field contacts and published independent reviews, currently have more comprehensive signature libraries, more complete removal capabilities, lower false positive rates and faster turnaround times for signature development. The markets have recognized the value of privates over the past nine months or so. Activity in the private market has been robust - kicked off with the acquisition of Pest Patrol by Computer Associates. Momentum remains strong, as indicated by the recent $108 million round of financing obtained by Webroot. Although larger vendors have dabbled behind the scenes in spyware, only as recently as February did Symantec and McAfee announce the release of comprehensive (not just blocking but removal as well) antispyware software. This is reflected in IDC's estimates, which indicate that 82% of 2004 antispyware revenue was generated by standalone solutions as opposed to suite-based products.

3. **Consumer and enterprise markets should be viewed in a very different manner**. The consumer market is mostly focused on privacy issues while the enterprise market is focused on preventing corporate espionage, monetary loss, and damage to goodwill. Vendors can also be more aggressive with remediation efforts in the consumer market where they need to be more careful about removing sensitive code in the enterprise market. Enterprise solutions need to be more complex and scalable with heterogeneous operability, careful remediation, centralized management, and low (preferably zero) false positives. Although spyware is the latest buzz in the press, the threats have been around for a while and vendors in the private market, such as Webroot, have built a very rapidly growing business.

4. **Antispyware technology is currently focused on endpoint security.** We expect the trend to follow the development of antivirus technology and become an increasingly layered system of defense with expansion to include gateway and network defense. In the antivirus segment, Trend Micro is already targeting this approach promoting solutions for the gateway, server, and client.

Please see analyst certification and other important disclosures starting on page 16.

Privates are also building out layered functionality from platforms based on best-of-breed antispyware software.

5. **Spyware will likely be fought in the marketplace, not in the legislature**. While spyware certainly has the ears and support of the Capitol Hill gang (the I-SPY act passed 415-0 in the US House of Representatives) the legislation will be ornamental, in our view, considering the volume of threats emerging from clandestine foreign locations. While a few domestic adware companies may fizzle as a result of legislative focus, we expect the markets to dictate the pace of protection against spyware. As threats continue to grow, simple economics will drive demand.

Spyware — a virus or not a virus?

Some industry professionals argue that spyware is not a virus as the intent and method of the two classifications of threats are different in some ways. Where viruses are engineered to take over, disable and destroy their hosts, spyware and its associated malware is designed as a more covert and pervasive threat. Contrary to viruses, spyware is created with the intention of running hidden in the background and exploiting the host for its own purposes. Destruction of the host would undermine the purpose of the malware. Security software vendors, fully aware of these differences, have been quick to create a new category to capitalize on what they are touting as a different type of threat.

A critical point, however, is the realization that the underlying technology for combating spyware is strikingly similar to antivirus technology — at least the detection component. Signatures emerge again as the core technology for identification of the presence of unwanted code. Further, the threat isn't exactly foreign to AV classifications. Although the buzz around spyware is relatively new, spyware has been around for quite a while. Trojans, zombies, and bots have been recognized as the first generation of spyware.

As spyware has increasingly become recognized as a more efficient way for hackers to make money, it has emerged as a derivative, and thus distinctive segment of blended threats in the computing environment. The more sophisticated embedded attacks that we are now experiencing is a mere evolution of the technology that propagated viruses.

Spyware vs. Adware

Although some will debate on the definition of adware as malicious software, we include adware in our definition. The reason for our inclusion involves the frequency with which adware spreads when the user does not want it and the damage that even adware is capable of. Adware is typically found in connection with freeware (as the providers of freeware use the advertisements to fund the sites) and is run with the users 'consent' but this often pushes the limits of acceptable practices. Although seemingly innocuous, adware can carry with it several unforeseen problems. At the very least, adware can increase latency by using available memory and slowing processing speeds on a computer. According to the TechRepublic survey, 90% of the managers surveyed noted lower computer performance as their greatest spyware-related concern. Microsoft has said it believes that up to one-third of all PC crashes are caused by spyware. To take this to a further extreme, for any enterprise with grid computing applications, cycle-stealing adware will greatly compromise that effort.

Adware typically involves agreement to an end user licensing agreement (EULA) but these agreements are typically glossed over if read at all. Unread EULAs can also allow many more adware programs than the user thinks are authorized. Research performed by PestPatrol on Grokster, a P2P file-sharing service, found that the 25,254 word EULA included authorization language for at least 11 other bundled products to be run and installed on users' PCs. As if this was not enough, some of these EULAs also provide for the storage of the vendors' advertisements on users' hard drives, using valuable memory. EULAs are very seldom read by users. To illustrate this dynamic, PC pitstop last year inserted a 'special consideration' clause in a EULA offering money to anyone who sent an email to an address contained in the license. It took 3,000 downloads and four months before someone actually read the EULA and sent the email. The respondent received a $1,000 check in the mail.

Consumer versus enterprise markets

We view the consumer and enterprise markets very differently when considering spyware. For starters, the most malicious and hence threatening forms of spyware are focused on stealing valuable information. For instance, knocking over a bank for $400 million is far more lucrative than stealing Grandma's credit card number. Obviously, personal information theft is a real issue that can drive consumer spend, even considering the multiple free spyware tools out there, but we see a far more concentrated and profitable opportunity in the bigger "bank-for-the-buck" enterprise investments. Enterprises also demand a far more

Please see analyst certification and other important disclosures starting on page 16.

robust and scalable solution, rendering many of the free products irrelevant and thus removing this commodity pressure driver from our assessments.

Consumer. Approaches in the consumer market have a very different focus than enterprise markets. In large part, the consumer markets are primarily focused on identity theft issues and employ a different distribution model. A recent example of consumer threat is the installation of keyloggers in 13 Kinko's stores in New York by JuJu Jiang. The hacker was able to obtain more than 450 banking passwords and usernames from the attempt. While revealing the consumer threat from spyware, this example also shows how the solution is more enterprise focused — the hacker targeted a large enterprise to gain scale and effectiveness in his theft of consumer information.

As with antivirus technology, two of the most significant factors in the consumer market remain Microsoft and the Internet service providers. Consumers may well expect the Microsofts and AOLs of the world to protect them for no incremental money — a trend we expect to build throughout the next few years. With these two channels offering spyware protection for free, the larger antivirus vendors are starting off in the market with a very low pricing base. Even McAfee has offered its standalone antispyware product for free, after an online discount and mail-in rebate, in the retail channel — and this is a brand new product. As a result, we do not feel as though there is a significant opportunity here for larger suite providers on the consumer side. They will instead wind up including spyware protection as part of existing security suites and here too this trend is becoming prevalent.

In fact, the market may soon realize that this is a technology that is essentially an evolved virus, which begs the question: Should AV vendors be protecting against spyware in the first place through advanced antivirus technology? The limited utility of AV will force persistent pricing pressure. Reference checks to a dated .dat file simply do not cut it in the ever-evolving threat landscape.

Enterprise. In addition to requiring more centrally managed solutions, the enterprise market is focused on monetary loss, corporate espionage, and damage to reputation. The recent keylogging attack on Sumitomo Mitsui Bank is a good example. Thieves used the keylogging software to relay passwords and access information so that funds could be transferred electronically. Here the stakes are much higher on a per-incident level than in the consumer market. The distribution methods are also much different and the remediation technology is more complex. As such, antispyware products may currently be able to command some economics in terms of pricing on the enterprise level but it may be here that enterprises soon question investment in antivirus technology if antispyware technology proves an ability to effectively protect against viruses as well.

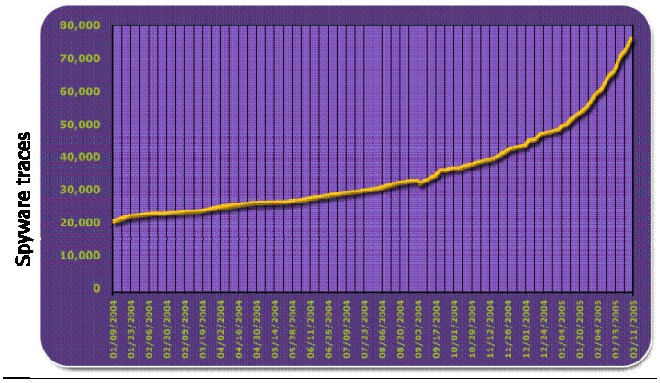
Overall, however, we expect progress in the enterprise market to be made with a higher degree of caution than the consumer market. This may be a reason why larger public vendors seemed slow to attack the spyware problem. There are a number of programs critical to operations that enterprises may employ which mimic the characteristics of spyware. For example, a remote access string in the registry could be perceived to be a spyware attempt to set up an unauthorized connection. Loosely jumping into "regedit" and removing the suspected code would mean the road warrior (or an entire sales force) is cut off from company data sources. A false positive identification and subsequent improper removal at any level of these applications can have a major impact across an effected enterprise beyond just the inconvenienced traveling employee.

Growth potential

Although we have not yet experienced a truly 'big' spyware hit of the magnitude of a Sasser or Blaster, spyware tends to be a more discreet ('low and slow') problem and is a threat that is certainly growing exponentially, just as traditional viruses did.

Exhibit 2

Spyware Traces Shipped



Source: Webroot.

Webroot has indicated that cumulative spyware traces scanned by the company have grown from approximately 20,000 traces in January 2004 to over 70,000 traces for

Please see analyst certification and other important disclosures starting on page 16.

February 2005. Cumulative numbers are significant because, unlike traditional viruses that are less harmful once a signature is sufficiently distributed, spyware can continue to cause damage if not removed from a computer. As mentioned in our industry report in January 2005, attacks are evolving into threats that are more sophisticated, with the programmers' motivation moving from fame to fortune. As it is difficult for hackers to directly extort infrastructures from more destructive viral programs, spyware offers the ability to covertly gain information that can be exploited for financial gain. This is another factor behind our thesis that the opportunity lies more in the enterprise market. The rewards are far more substantial.

Blended threats

Malicious software (malware) threats continue to grow in the form of blended attacks. Most malware is installed on a computer without a user's knowledge. The variance, pervasiveness and blended nature of installation methods for spyware and other threats make this problem particularly troublesome and difficult to defend against. Malware can be acquired by using peer-to-peer software (such as Kazaa and Morpheus), visiting a website (a drive-by download), opening spam, acquiring a separate virus or clicking on a pop-up.

Types of malware can include spyware, keyloggers, system monitors, and hijackers or remote-control programs for establishing zombie computers (bots). There are even ways to lure or trick a user into agreeing to or activating a spyware download through user interaction. In addition to the lengthy or deceptive EULAs which go the 'legal' route, these methods can range from a pop-up that notes a particular type of software must be downloaded in order to properly view a website, to a similar prompt with misleading text reading "click 'NO' to install". In more covert instances, spyware can be embedded in a different type of file so that, when run, the desired file loads but so does the spyware. This may leave some users thinking, "why does this file take so long to download?".

To illustrate how bad things have become and how covert the software can be, a large number of website owners have even discovered that their websites are being used to distribute spyware to those visiting the sites. In some cases, the websites were found to have been infected for some time before the owners ever discovered the threats. Websense's 2004 Web@Work Survey noted, "Only 6% of employees who access the Internet at work said they have ever visited any Web sites that contain spyware; however, 92% of IT managers estimate that their organization has been infected by spyware at some point." As recently noted by Kaspersky, spyware authors are also creating 'made to order' malware for specific rates of infection and purpose. These limited edition programs make them even harder to detect as the virus writers only infect the number of computers they need at a given time. When only 5,000 or 10,000 unique copies of a program are in the wild, there is less of a chance they will be detected and less of a chance a signature file will be created for it. Even if a signature file is created, a new version of the program will quickly follow which will go undetected (zero day threat problem).

As blended threats expand, it becomes more difficult to trace the origins of spyware and more difficult to stop it. A particularly troubling method of spreading spyware is the ubiquity of bot nets throughout the Internet. The Honeynet Project report, released on March 14, 2005, summarized the seriousness of bots as they exponentially increase the number of infected computers on the Internet. The Honeynet Project is run by an international organization made up of 30 members throughout the security community. The report found that bot nets, collections of compromised computers (zombies), have become more pervasive and have increasingly focused on identity theft and installing spyware. The project was able to track over 100 bot nets, some as large as 50,000 hosts, in a four-month period. Any computer infected with bot software is prone to having sensitive information, such as account number and password combinations or credit card numbers, sent to the controller of the bot network. One of the issues with bot or zombie networks is that very few users are aware that their computers are affected at all. As such, remediation of the network in its entirety is nearly impossible. The very nature of these networks perpetuate themselves and spread more malicious code throughout the Internet.

Remediation

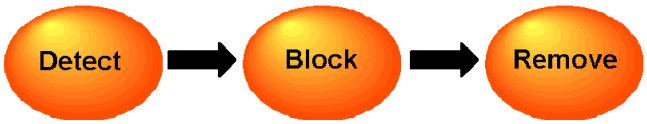
As with viruses, the most efficient way to avoid a spyware threat is to block it. In fact, technology very similar to antivirus technology is often used for spyware. Once a spyware threat is identified, a signature or fingerprint is created and sent to subscribers so that the software can recognize the pattern of code as malicious. However, antispyware software must be more sophisticated than traditional antivirus software as it must also identify malware that has slipped through the system (or was previously installed) and remove the code that has embedded itself in the operating system. Remediation is more complex in the enterprise than in consumer

Please see analyst certification and other important disclosures starting on page 16.

environment, hence our belief that enterprise applications could yield economic benefit for antispyware vendors.

Exhibit 3

Remediation Process



Source: Morgan Stanley Research

The detection of malware starts with signatures. However, the problem with a signature-only platform is the lack of protection of new or unknown ("day zero") threats. Therefore, the next step is behavioral or active protection. This is the direction we are seeing some of the leading vendors take, such as Webroot, Tenebril, and Sunbelt, heading. Currently, antispyware vendors are attempting to reach the 90%+ effectiveness level but none appear to have hit the mark yet with a meaningfully low false positive rate. While larger vendors are trying to get close to that benchmark, the privates appear to be close and are moving on to deeper functionality.

Detection and removal of embedded spyware is difficult because of the complexity of the malware. Examples of complex installations include randomizing files or breaking parts of the program up into several pieces and installing it in different places on the computer. Malicious files can replace or embed into parts of existing executable programs so that removal of the files would disable the valid application. Some programs can embed themselves in registry files. Other executable programs can be installed in groups that check the status of associated segments of the program on a regular basis. In this case, if one segment of the malware detects that another segment is disabled or removed, it may automatically reinstall that segment.

Consumer spyware solutions appear to be well ahead of enterprise solutions in the development process for several reasons. First, spyware embeds itself deep into some files. Removal of these files, particularly registry files, can cause problems running applications. This is where Microsoft has an advantage. Other vendors must reverse engineer the code in order to determine which parts of files to remove while Microsoft owns the code to its applications. This is not a big deal for a few consumer machines but can carry very serious implications for enterprise customers where one instance of removing the incorrect registry file can have a much more serious operational impact than the same error on a few consumer desktops. Second, much of the initial press regarding spyware involved the impact to consumers. Therefore, the resulting spend in the consumer market made this a natural initial area of focus for vendors.

Power of the privates

If the larger suite providers have so many research and development engineers, why didn't antivirus vendors address this threat? Many spyware threats have been around for quite a while and the smaller private companies have been able to react. In our view, the spyware threats have evolved quickly while most of the larger suite providers have built their products in a slow and reactive manner. Most larger suite providers have only recently developed complete solutions (and we have yet to see tests for them) while many private companies have had solutions around for over a year and have developed and tested them more extensively.

Private companies also appear to be well-funded. Software tends to draw a substantial amount of investment in general with over $5 billion in venture-backed funding in 2004, according to PriceWaterhouseCooper's Money Tree Survey. As antispyware software is one of the fastest growing software segments, it tends to be a natural draw for a significant amount of this investment, as evidenced by Webroot's recent $108 million round of financing. The privates' momentum, along with significant funding, has allowed the group to release substantial products with effective marketing to the point where one can walk into a retail store and see Webroot's product displayed just as prominently as Symantec's shrink-wrapped product.

As we have written before, private companies tend to move more quickly due to their ability to attract and retain talent and to commit to a project that can become delayed by bureaucracy at a larger company, and the lean effectiveness with which they are able to convert research into practice due to more flexible architecture. In general, several private companies appear to have a head start on the larger public suite vendors. As noted above, IDC estimates that 82% of 2004 spyware revenue went to standalone spyware products, compared to suite-based products. Most stand-alone antispyware solutions are provided by privately held vendors.

Relative to vendors that only recently entered the antispyware space, the lead should (at least temporarily) benefit the more established private vendors. These

Please see analyst certification and other important disclosures starting on page 16.

vendors tend to have comprehensive (not necessarily larger) signature libraries to detect threats, the experience of deployment in a real environment, the development of lower false positive rates, and the ability to offer reduced response time for signature development.

In response to the required learning curve, we have also seen a number of transactions where larger companies acquire the necessary technology to achieve scale right away. Although antivirus databases can be had relatively cheap while yielding high rates of success, antispyware databases are still very proprietary, so there is real value there. In the past nine months, we have seen Computer Associates acquire Pest Patrol, Microsoft acquire Giant Software and Surf Control acquire antispyware technology from Apreo. We believe there are more acquisitions to come. Any large security vendor must have AS protection in our view and time to market is essential. Wait too long to develop internally and enterprises likely pick someone else as the immediacy of the spyware threat severely weakens the "GA next year" promises. As acquisitions continue and larger suite-oriented vendors recognize the need to offer comprehensive antispyware solutions, we expect to see suite-based antispyware products increase in functionality, competitiveness and share.

And then there's Microsoft…

An intriguing thought is the reach of the Microsoft platform and its effect on market penetration — at least at the consumer level. If consumers can get leading (or at least average) antispyware technology, with automatic signature updates (as well as the potential for faster signature generations since the tool is reporting incidents back immediately to Microsoft) and it won't cost them anything, how to compete? Given this, it will be very difficult to convince home users that they need to pay a different vendor for a similar level of effectiveness. In addition to antispyware, Microsoft's Beta has some very firewall-like characteristics to it, implying that the vendor may slip in extra functionality while safeguarding code that it owns against external threats. Sure there may be better technology out there but what is that incremental performance worth? While Microsoft faces greater challenges in the enterprise market with heterogeneous platforms, it certainly can make quite an impact directly in the consumer market and the inside information that Microsoft has on the code being attacked should warrant serious consideration from IT managers.

Many believe that Microsoft security is an oxymoron - particularly in the enterprise market. However, we believe that Microsoft can deliver when it gets serious about addressing an issue. We saw this with market share threat from Netscape. The fact that CEO Bill Gates has announced an approximately $2 billion budget for security R&D is a statement in itself. Consider that this figure is more than twice McAfee's total 2004 *revenue*. With that level of commitment to security, the chances of success are substantial.

The Microsoft OneCare model will entirely mask the security part of the service versus the other tools — quite literally, security will become a transparent feature of a utility set.

To further debunk the "Microsoft won't compete in security" myth (again, in the consumer market), look at its latest offering OneCare. We think this announcement is very significant for a number of reasons. For starters, consumers now have a direct, always available suite of tools to keep their PC running effectively. As we have stated prior, we see security more as a function of technology, not a standalone industry (please see our industry report January 5, 2005). By including security protections such as AV, firewall, and antispyware along with disk defragmentation, Microsoft is rapidly driving this model of utility solutions in a simple to use, consumer friendly package. The Microsoft OneCare model will entirely mask the security part of the service versus the other tools — quite literally, security will become a transparent feature of a utility set.

In a few recent reviews of consumer-focused antispyware products, the Microsoft Beta release has been favorably received for the most part. Consistently ranking at least in the middle of its class (and often at the top), the Microsoft Beta not only exhibits relatively strong performance versus its peers but it carries with it deeper implications for the spyware segment as well as the antivirus segment, in our view. As the software provider with the deepest understanding of the most commonly deployed operating system, spyware really is Microsoft's opportunity to lose. We took issue with the *Wall Street Journal* review, which, while headlining "serious flaws" with the tool, made mostly political complaints about the spyware solution setting the home page default to MSN.com. While a matter of taste, this is in no way a technological deficiency, in our view. The Microsoft product may not be as solid as other

Please see analyst certification and other important disclosures starting on page 16.

solutions, as some test results have suggested, but it is a start and given the Microsoft security development budget, we think the company must be taken seriously.

As much as some may eschew the notion of a competitive and comprehensive Microsoft product, the spyware beta offers telling functionality with perhaps a foreshadowing of what the Redmond software giant is capable of. When referring to the antispyware technology that Microsoft purchased in December of 2004, we have heard comments from knowledgeable industry professionals (even some from a few of the big three antivirus vendors) that were very positive on the capabilities of the technology. We heard some mixed testing results from the product but we point out that recent articles in *PC World* and *PC Magazine* are very bullish on its functionality. Keeping in mind that this product is still in beta, it appears as though the test for Microsoft will be, as the spyware segment and its solutions evolve, thoughtful and progressive evolution of the antispyware product. In our view, Microsoft is getting plenty of candid feedback from the industry on what is expected from the antispyware product.

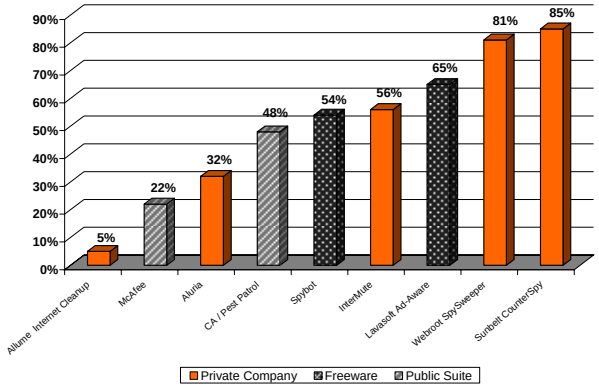
Track record of delivering on time aside, we see Microsoft as uniquely positioned to carry a significant amount of weight in the security software market. Because there are many consumers that place the cost/benefit breakeven of security software below current product prices, there is a limit to the penetration of a large addressable market by vendors. Based on the proposed functionality of OneCare, if Microsoft can deliver on this antivirus, antispyware, PC maintenance bundle, the company could shift the breakeven point in the market and potentially affect the penetration and renewal rates of the security software vendors.

Where they stand

Many larger public vendors now claim to offer complete solutions to the new spyware threats but we do not see a clear indication from the market that these solutions are effective enough. Meanwhile, we are seeing the smaller private antispyware vendors build out suite functionality around the better performing spyware platforms and starting to claim their share of the pie.

Exhibit 4

Recent Test Results
Antispyware Detection Rates



Source: PC World, April, 2005.

While we expect vendors such as Symantec, McAfee and Trend to catch up with truly enterprise-class antispyware product relatively quickly, they do not appear to be there yet and smaller best of breed vendors have the opportunity to do some damage to the few high-growth security software segments left in the meantime. Specifically, Sunbelt and Webroot, already with arguably the most effective antispyware solutions, are moving into security suite territory with moves toward firewall and antivirus functionality. Tenebril also has the potential to gain meaningful share as the company ramps up its engineering staff, bolsters its balance sheet with a healthy round of financing, and tees up a very successful team of seasoned marketing executives from Zone Labs. With complimentary technologies more of a commodity now, development of meaningful security software suites may come relatively inexpensively.

Positioning of the publics

Websense. Websense offers a layered approach by helping to block access to websites that are known to distribute malicious code. Although the company does not have a solution to remove spyware, Websense can also block a serious spread of malicious code throughout the network with its Client Policy Manager (CPM). CPM has the ability to block malicious applications from running or, at a minimum, can block communication with other nodes within a network essentially quarantining an infected computer. Although only for the enterprise, the Websense approach offers protection against DNS redirection, bot network infiltration, malicious websites and unauthorized outbound port 80 traffic. The software also offers protection against keylogging, which has become one of the

most dangerous and widespread spyware threats on the Internet. Considering that Websense can use a whitelisting approach to enforce approved applications blocking malicious content and protects at several layers of the network, the vendor could essentially eliminate the need for installing signature-based antispyware at the client level.

RSA Security. We expect to see more emphasis on authentication as a result of increased spyware activity. Strong two-factor authentication is an effective way to protect against keylogging. Keylogging is the primary method of obtaining personal and confidential information in both the consumer and enterprise environments. Even if a keylogger were to obtain sensitive password information, since the SecurID codes (hence passwords) change every 60 seconds, the passwords are not valid for long. Additionally, the user account does not permit multiple logins. In addition to RSA Security, Verisign *(VRSN, $29.50, Equal-weight-V, covered by Mary Meeker)* is also well positioned to protect against keylogging with an effective authentication offering.

Symantec and McAfee. Both of these larger security suite providers offered spyware that only blocked until February 2005, when each also announced removal technology as well. In our view, although they have the ability to build a product quickly, each of these vendors has some ground to make up to build signature libraries and to develop the effectiveness of their products in existing IT environments. While consumer products have been released quickly, these products are facing commoditization right away, as indicated by the ability to get both McAfee Antispyware and Virusscan for free after rebate at Staples. Enterprise products appear to be considerably behind the consumer market due to the complicated remediation issues discussed previously.

Microsoft. As noted above, Microsoft made a significant splash in the market with the purchase of Giant antispyware software in December 2004. Contrary to its track record, the company quickly turned the acquired technology into a beta product for the market to experience. Without losing any momentum, at the RSA Conference in February 2005, Bill Gates announced that the antispyware product would be available to the public for free after the beta period. Going forward, we think the Giant technology may be significant if Microsoft can manage the development of this software with the fast pace of emerging spyware threats. The offering of this technology to the consumer market for free also creates a rift in the consumer pricing structure alongside the Internet Service Providers offering strong antispyware technology for free.

Drivers for continued growth

Given the immediacy and severity of the spyware threat, we believe that the standalone market opportunity is very significant. Longer-term, however, as the spyware market matures, we see the standalone spyware models absorbing additional functionality. First, we still see suites and appliances as dominant industry drivers. Enterprise buyers are looking for more capability from fewer vendors. This is a trend that we expect to continue. If antivirus vendors should have (arguably) been offering a solution for spyware long ago, we see it as necessary for them to include it in their suites now. In fact, we are finally seeing movement from Symantec and McAfee offering real antispyware technology instead of just spyware blocking technology as they have in the past. They will likely not be able to justify a price for it (as noted above, McAfee antispyware has already been offered for free to consumers after rebates — along with Virusscan by the way) but they will need to provide it in support of suite platforms in order to provide truly comprehensive security. As a threat to the big boys, some of the private antispyware vendors actually have a chance to take share currently held by the big three security vendors (four if you count Microsoft).

Second, we still see blended threats and embedded technology driving the market. This is, in part, what caused the spyware problem in the first place. Antispyware technology will eventually be convergent technology that becomes embedded, we believe, as antivirus and antispam technology is now.

In addition to the above, we also expect opportunity in a layered defense model — just as we have seen antivirus and firewall technology reach the gateway, network and desktop. By the viral nature of the threat and the increasingly porous nature of networks today, antispyware variants will need to be present in each network layer in order to effectively protect the networks.

Lastly, we see growing legislative drivers. As we've commented in several notes over the past few weeks, data theft and identity fraud continue to be hot issues, not just for individuals and enterprises assessing damages to their data and reputations but also to legislators now that these issues are starting to effect them personally. Spyware is beginning to receive an elevated level of attention to the point where it will become a critical, if not mandated, area of spend for

Please see analyst certification and other important disclosures starting on page 16.

consumers and enterprises over the next four years. There will be opportunity in the markets on a broad basis but right now, it appears to be primarily in the private markets.

Private company profiles

Following are one-page profiles of Sunbelt Software, Tenebril, and Webroot, three private companies that we think are likely to gain share in the antispyware space within the software security industry.

Please see analyst certification and other important disclosures starting on page 16.

Sunbelt Software

Not Rated

Business Overview

With its US office located in Tampa Bay (Clearwater), Florida, Sunbelt Software, Inc. is a provider of enterprise system infrastructure software, including security, anti-spam and system management tools. The company was founded in 1994 and offers product solutions that enable companies to protect and secure their infrastructure from costly inefficiencies including spam, Windows system downtime and network security vulnerabilities.

Products and Services

CounterSpy Enterprise — allows enterprises to scan and remove spyware. CounterSpy features a central management console that gives administrators the ability to access and control agent deployment, update threat databases, quarantine spyware, push agent policies, and schedule scans. Deployment throughout an organization is accomplished via a policy-based interface. Agents can be deployed using a silent push install (using either WMI or RPC and admin shares) as an MSI file or as a self-extracting executable. The new version 1.5, slated for a summer release, will add real-time protection to help reduce against recurring spyware infestation.

iHateSpam for Exchange — removes unwanted email and protects against phishing. Currently available for Exchange v5.5, 2000 and 2003, the product has high spam detection rates ,low false positives, and filters at the server level to eliminate the need for client software.

Network Security Inspector — network vulnerability assessment tool and scanner. Security Inspector enables the identification of security holes on a wide array of platforms and includes remediation instructions.

LanHound — enables the user to troubleshoot NT/2000/2003 LAN, WAN or Internet segments.

ServerVision — ServerVision is a system monitor product that enables monitoring of the status and health of all network servers on a single screen.

Directory Inspector — enables analysis and reporting of Active Directory information. With support of all the major industry standard directories (IBM, Microsoft, Netscape, Novell and all LDAP-based directories), this product provides analysis for directory structure, security, integrity, and standards and policy compliance.

Sunbelt Remote Administrator — a fast and secure remote control tool that supports NT security, file transfer, and telnet access with multilanguage support.

Positioning

With offices in five countries (Europe is handled through Sunbelt's French sister company, Sunbelt Software Systems), and a focus on antispyware, Sunbelt offers an array of security software products centred on antispyware, antispam, server monitoring and vulnerability assessment. The company also has two products adapted for consumer use, iHateSpam 4 and CounterSpy Consumer.

Funding History

Date	Round	Amt Raised ($MM)	Post $ Valuation ($MM)
Company is self-funded.			

Partners

ASAP Software	SoftChoice Corp.
Insight	Softmart
PC Connection	Software House Int.
PlanetGov	Software Plus Computers
Programmers Paradise	Software Shelf
Sandbox Technologies	

Management

Jo Murciano — Founder, Chairman
Alex Eckelberry — President
Stu Sjouwerman — Founder, COO
Sam Licciardi — Executive Vice President
Laurie Green — Chief Financial Officer
Greg Kras — VP, Product Management
Eric Sites — VP, Research & Development

Recent Company News Releases

5/12/05 — Announced upgrade to ServerVision
4/25/05 — Acquired Web Spidering technology to help identify new spyware threats.
3/22/05 — CounterSpy Enterprise added to the Air Force NETCENTS contract.
3/2/05 — Announced upgrade to CounterSpy Enterprise.
2/7/05 — Announced upgrade to iHateSpam for Exchange.
1/20/05 — Announced upgrade to Security Vulnerabilty Scanner.
1/12/05 — Announced Antispyware Software Developer Kit (SDK).
1/12/05 — Sunbelt and Cloudmark partner to fight spam.

Please see analyst certification and other important disclosures starting on page 16.

Tenebril

Not Rated

Business Overview

Tenebril is a provider of antispyware and privacy software. The company operates worldwide with headquarters split between Boston, MA and San Mateo, CA. The company was founded in 1998 and is led by a team of software industry veterans. Tenebril's product lines are distributed worldwide via e-commerce, retail security experts and a direct sales force.

Products and Services

SpyCatcher 3.5 — SpyCatcher is Tenebril's best selling antispyware software. Partial-matching search algorithms, multiple boot level search functionality, antiphishing capability, and hosts file analyzer, enable the user to employ broad antispyware protection.

TracksCleaner 3.0 — removes surfing and computer use. With deletion technology meeting Department of Defense standards, TracksCleaner prevents undelete tools and hardware recovery systems from retrieving wiped data.

GhostSurf — provides anonymous, encrypted connection to the Internet, hiding the user from Web sites, and ISP. GhostSurf Standard Edition comes with TracksCleaner, and the Platinum Edition includes TracksCleaner, AdArmor, Personal Data Vault and SpyCatcher.

AdArmor 3.0 — blocks pop-ups, banner ads, flashing text, and paid search engine results.

Personal Data Vault 1.0 — locks documents, passwords and favorites in a safe location.

Lifeguard 3.0 — all-in-one data backup product. The product combines an easy interface with powerful compression and encryption features.

StickyNote 9.0 — enables users to create attractive, photo-realistic three-dimensional notes on the desktop and send them to other parties instantly.

Slingshot 1.2 — speeds up downloads and automatically checks for new versions of software.

Uninstaller 1.2 — enables removal of broken files, cleaning of the start menu and repair of the system registry.

MemoryBoost Pro 2.6 — speeds up computer processes and improves reliability.

Positioning

Tenebril is a provider of anti-spyware solutions for businesses and is concentrated on providing protection against mutating threats as well as traditional solutions. As spyware threats continue to grow, vendors in this space could see a disproportionate amount of spending and funding by investors looking to put money to work.

Funding History

Date	Round	Amt Raised ($MM)	Post $ Valuation ($MM)
4/25/05	A	$6.5	N/A

Selected Investors

Investment Firm	Participating Rounds
Sierra Ventures	Series A

Selected Customers and Partners

Partners	
Best Buy	Walmart
CompUSA	PC Mall
Circuit City	Target
Office Depot	Micro Center
Amazon.com	Costco
Officemax	

Management

Irfan Salim —CEO
Fred Felman— VP, Business Development
Te Smith — VP, Communications

Recent Company News Releases

4/25/05 — Announced $6.5 million Series A funding from Sierra Ventures.

Please see analyst certification and other important disclosures starting on page 16.

Webroot

Not Rated

Business Overview

Webroot is a provider of privacy, protection and performance solutions for Internet users. The company operates in North America, Europe, and Asia and sells on both a direct and indirect basis across all markets and geographies. Webroot has deployed solutions to over 2,500 businesses and six million consumers worldwide.

Products and Services

Spy Sweeper — This product includes spyware detection, spyware quarantine, proactive protection, spyware definitions updates, spyware education, software updates, and customer support.

Spy Sweeper Enterprise — Using a client/server architecture, it detects and removes spyware and malware.

Window Washer 5.5 — cleans on and off line activities. Window Washer 5.5 is an Internet washer, system cleaner, registry cleaner, and privacy protector.

Pop Up Washer — includes an "allow list", transparent removal, messenger service spam window blocking, audio notification, and log files of all ads stopped.

Spam Shredder — detects and configures Outlook, Outlook Express, and Eudora email accounts. Currently works with other POP3 mail clients.

My Firewall Plus — provides a multi-layered shield for Internet users, including network connection control, content protection, application verification, and operating system security.

Private Surfing — protects personal information, including shopping, banking, and online chat. It also prevents marketers from profiling personal activities and hides e-mail addresses.

Phish Net — uses a black list of known "phisher" websites to warn users when they attempt to access a site on that list and refuses any Web navigation that originates from or has a destination to one of these sources on the black list.

Accelerate — boosts connection speed and works with existing modem and network connections.

My Personal Favorites — securely stores an organizes favorite sites, user names and passwords.

MacWasher & MacWasherX — cleans online and offline tracks, and wipes out data to protect Internet privacy.

Positioning

Webroot is a provider of anti-spyware solutions for businesses and consumers designed to provide best-in-class, easy-to-administer software solutions to protect sensitive information on corporate networks and personal computers from security threats on the Internet. As security threats continue to grow, vendors in this space could see demand for their products rise over the next few years and a greater amount of funding as other products in the security space slow in growth.

Funding History

Date	Round	Amt Raised ($MM)	Post $ Valuation ($MM)
2/7/05	A	$108MM	N/A

Selected Investors

Investment Firm	Participating Rounds
TCV, Accel & Mayfield	

Selected Customers and Partners

Partners	
Best Buy	Fry's
CompUSA	Staples
Circuit City	MicroCenter

Management

C. David Moll —CEO
Mike Irwin — CFO

Recent Company News Releases

5/16/05 — Former Check Point Software senior exectutive to lead worldwide marketing for Webroot.
5/10/05 — Webroot CEO to testify before Senate Committee on combating growing spyware problem.
5/3/05 — Webroot releases industry's first comprehensive report on Spyware.
3/22/05 — Quarterly Webroot Report Identifies the Ten Most Significant Emerging Spyware and Adware Threats.
3/1/05 —Michael D. Conner, former Symantec and Brightmail Executive, will join company as SVP of Sales
2/7/05 — Webroot Secures $108 Million Investment from TCV, Accel and Mayfield
2/4/05 — Webroot Resigns from Consortium of Anti-Spyware Technology Vendors (COAST)
1/24/05 — Webroot Spy Sweeper Enterprise Surpasses One Million Seat Milestone

Please see analyst certification and other important disclosures starting on page 16.

Appendix A

Top Spyware Threats

Name: PurityScan

Description: PurityScan frequently displays pop-up advertisements onto your computer whenever you are online. It induces you to install it by claiming to find and delete pornographic images.

Name: n-CASE

Description: (msbb.exe) **–** n-CASE is an adware program that delivers targeted pop-up advertisements to your computer. This program is usually bundled with freeware applications.

Name: Gator

Description: Gator (GAIN) – is an adware program that has the ability to display banner advertisements based on your Web surfing habits. Gator is usually bundled with numerous free software programs, including the popular file-sharing program Kazaa.

Name: CoolWebSearch

Description: CoolWebSearch (CWS) – CoolWebSearch has the ability to hijack your Web searches, home page, and Internet Explorer settings. Recent variants of CoolWebSearch install using malicious HTML applications or security flaws, such as exploits in the HTML Help format and Microsoft Java Virtual machines.

Name: Transponder

Description: Transponder (vx2) – Transponder is an IE Browser Helper Object that monitors requested web pages and data entered into online forms, then delivers targeted advertisements.

Name: ISTbar/AUpdate

Description: ISTbar/AUpdate – ISTbar is a toolbar used for searching pornographic web sites that has been reported to display pornographic pop-ups and to hijack your homepage and Internet searches.

Name: KeenValue

Description: KeenValue – KeenValue is an adware program that collects personal information and delivers advertisements to your computer.

Name: Internet Optimizer

Description: Bargain Buddy delivers targeted pop-up advertisements to your computer based on key words you might enter while surfing the Web.

Method of Infection: Internet Optimizer – Internet Optimizer hijacks error pages and redirects them to its own controlling server at http://www.internet-optimizer.com.

Name: Perfect Keylogger

Description: Perfect Keylogger – Perfect Keylogger is a monitoring tool that records all visited web sites, keystrokes and mouse clicks. For example, it can log passwords, account numbers and other sensitive information. It is usually installed manually.

Name: TIBS Dialer

Description: TIBS Dialer – TIBS Dialer is a dialer program that hijacks your modem and dials toll numbers, usually to access pornographic "pay" Web sites.

Source: Webroot.

Analyst Certification

The following analysts hereby certify that their views about the companies and their securities discussed in this report are accurately expressed and that they have not received and will not receive direct or indirect compensation in exchange for expressing specific recommendations or views in this report: Peter Kuper.

Important US Regulatory Disclosures on Subject Companies

The information and opinions in this report were prepared by Morgan Stanley & Co. Incorporated and its affiliates (collectively, "Morgan Stanley").

As of April 29, 2005, Morgan Stanley beneficially owned 1% or more of a class of common equity securities of the following companies covered in this report: Check Point Software, RSA Security, Symantec and Websense.

Within the last 12 months, Morgan Stanley has received compensation for investment banking services from McAfee and Microsoft.

In the next 3 months, Morgan Stanley expects to receive or intends to seek compensation for investment banking services from Check Point Software, Symantec, Websense and Microsoft.

Within the last 12 months, Morgan Stanley has received compensation for products and services other than investment banking services from Microsoft.

Within the last 12 months, Morgan Stanley has provided or is providing investment banking services to, or has an investment banking client relationship with, the following companies covered in this report: Check Point Software, McAfee, Symantec, Websense and Microsoft.

Within the last 12 months, Morgan Stanley has either provided or is providing non-investment banking, securities-related services to and/or in the past has entered into an agreement to provide services or has a client relationship with the following companies covered in this report: Check Point Software and Microsoft.

The research analysts, strategists, or research associates principally responsible for the preparation of this research report have received compensation based upon various factors, including quality of research, investor client feedback, stock picking, competitive factors, firm revenues and overall investment banking revenues.

Morgan Stanley & Co. Incorporated makes a market in the securities of Check Point Software, RSA Security, Symantec, Websense and Microsoft.

Stock Ratings

Different securities firms use a variety of rating terms as well as different rating systems to describe their recommendations. For example, Morgan Stanley uses a relative rating system including terms such as Overweight, Equal-weight or Underweight (see definitions below). A rating system using terms such as buy, hold and sell is not equivalent to our rating system. Investors should carefully read the definitions of all ratings used in each research report. In addition, since the research report contains more complete information concerning the analyst's views, investors should carefully read the entire research report and not infer its contents from the rating alone. In any case, ratings (or research) should not be used or relied upon as investment advice. An investor's decision to buy or sell a stock should depend on individual circumstances (such as the investor's existing holdings) and other considerations.

Global Stock Ratings Distribution

(as of April 30, 2005)

	Coverage Universe		Investment Banking Clients (IBC)		
Stock Rating Category	Count	% of Total	Count	% of Total IBC	% of Rating Category
Overweight/Buy	686	36%	275	41%	40%
Equal-weight/Hold	852	45%	294	44%	35%
Underweight/Sell	367	19%	98	15%	27%
Total	1,905		667		

Data include common stock and ADRs currently assigned ratings. For disclosure purposes (in accordance with NASD and NYSE requirements), we note that Overweight, our most positive stock rating, most closely corresponds to a buy recommendation; Equal-weight and Underweight most closely correspond to neutral and sell recommendations, respectively. However, Overweight, Equal-weight, and Underweight are not the equivalent of buy, neutral, and sell but represent recommended relative weightings (see definitions below). An investor's decision to buy or sell a stock should depend on individual circumstances (such as the investor's existing holdings) and other considerations. Investment Banking Clients are companies from whom Morgan Stanley or an affiliate received investment banking compensation in the last 12 months.

Analyst Stock Ratings

Overweight (O). The stock's total return is expected to exceed the average total return of the analyst's industry (or industry team's) coverage universe, on a risk-adjusted basis, over the next 12-18 months.

Equal-weight (E). The stock's total return is expected to be in line with the average total return of the analyst's industry (or industry team's) coverage universe, on a risk-adjusted basis, over the next 12-18 months.

Underweight (U). The stock's total return is expected to be below the average total return of the analyst's industry (or industry team's) coverage universe, on a risk-adjusted basis, over the next 12-18 months.

More volatile (V). We estimate that this stock has more than a 25% chance of a price move (up or down) of more than 25% in a month, based on a quantitative assessment of historical data, or in the analyst's view, it is likely to become materially more volatile over the next 1-12 months compared with the past three years. Stocks with less than one year of trading history are automatically rated as more volatile (unless otherwise noted). We note that securities that we do not currently consider "more volatile" can still perform in that manner.

Unless otherwise specified, the time frame for price targets included in this report is 12 to 18 months. Ratings prior to March 18, 2002: SB=Strong Buy; OP=Outperform; N=Neutral; UP=Underperform. For definitions, please go to www.morganstanley.com/companycharts.

Analyst Industry Views

Attractive (A). The analyst expects the performance of his or her industry coverage universe over the next 12-18 months to be attractive vs. the relevant broad market benchmark named on the cover of this report.

In-Line (I). The analyst expects the performance of his or her industry coverage universe over the next 12-18 months to be in line with the relevant broad market benchmark named on the cover of this report.

Cautious (C). The analyst views the performance of his or her industry coverage universe over the next 12-18 months with caution vs. the relevant broad market benchmark named on the cover of this report.

Stock price charts and rating histories for companies discussed in this report are also available at www.morganstanley.com/companycharts. You may also request this information by writing to Morgan Stanley at 1585 Broadway, 14th Floor (Attention: Research Disclosures), New York, NY, 10036 USA.

Other Important Disclosures

This research report has been published in accordance with our conflict management policy, which is available at www.morganstanley.com/institutional/research/conflictpolicies.

For a discussion, if applicable, of the valuation methods used to determine the price targets included in this summary and the risks related to achieving these targets, please refer to the latest relevant published research on these stocks. Research is available through your sales representative or on Client Link at www.morganstanley.com and other electronic systems.

This report does not provide individually tailored investment advice. It has been prepared without regard to the individual financial circumstances and objectives of persons who receive it. The securities discussed in this report may not be suitable for all investors. Morgan Stanley recommends that investors independently evaluate particular investments and strategies, and encourages investors to seek the advice of a financial adviser. The appropriateness of a particular investment or strategy will depend on an investor's individual circumstances and objectives.

This report is not an offer to buy or sell any security or to participate in any trading strategy. In addition to any holdings disclosed in the section entitled "Important US Regulatory Disclosures on Subject Companies", Morgan Stanley and/or its employees not involved in the preparation of this report may have investments in securities or derivatives of securities of companies mentioned in this report, and may trade them in ways different from those discussed in this report. Derivatives may be issued by Morgan Stanley or associated persons.

Morgan Stanley & Co. Incorporated and its affiliate companies do business that relates to companies covered in its research reports, including market making and specialized trading, risk arbitrage and other proprietary trading, fund management, investment services and investment banking. Morgan Stanley sells to and buys from customers the equity securities of companies covered in its research reports on a principal basis.

Morgan Stanley makes every effort to use reliable, comprehensive information, but we make no representation that it is accurate or complete. We have no obligation to tell you when opinions or information in this report change apart from when we intend to discontinue research coverage of a subject company.

With the exception of information regarding Morgan Stanley, reports prepared by Morgan Stanley research personnel are based on public information. Facts and views presented in this report have not been reviewed by, and may not reflect information known to, professionals in other Morgan Stanley business areas, including investment banking personnel.

Morgan Stanley research personnel conduct site visits from time to time but are prohibited from accepting payment or reimbursement by the company of travel expenses for such visits.

The value of and income from your investments may vary because of changes in interest rates or foreign exchange rates, securities prices or market indexes, operational or financial conditions of companies or other factors. There may be time limitations on the exercise of options or other rights in your securities transactions. Past performance is not necessarily a guide to future performance. Estimates of future performance are based on assumptions that may not be realized.

This publication is disseminated in Japan by Morgan Stanley Japan Limited; in Hong Kong by Morgan Stanley Dean Witter Asia Limited; in Singapore by Morgan Stanley Dean Witter Asia (Singapore) Pte. (Registration number 199206298Z) and/or Morgan Stanley Asia (Singapore) Securities Pte Ltd (Registration number 200008434H), regulated by the Monetary Authority of Singapore, which accepts responsibility for its contents; in Australia by Morgan Stanley Dean Witter Australia Limited A.B.N. 67 003 734 576, holder of Australian financial services licence No. 233742, which accepts responsibility for its contents; in Taiwan by Morgan Stanley & Co. International Limited, Taipei Branch; in Korea by Morgan Stanley & Co. International Limited, Seoul Branch; in India by JM Morgan Stanley Securities Private Limited; in Canada by Morgan Stanley Canada Limited, which has approved of, and has agreed to take responsibility for, the contents of this publication in Canada; in Spain by Morgan Stanley, S.V., S.A., a Morgan Stanley group company, which is supervised by the Spanish Securities Markets Commission (CNMV) and states that this document has been written and distributed in accordance with the rules of conduct applicable to financial research as established under Spanish regulations; in the United States by Morgan Stanley & Co. Incorporated and Morgan Stanley DW Inc., which accept responsibility for its contents. Morgan Stanley & Co. International Limited, authorized and regulated by Financial Services Authority, disseminates in the UK research that it has prepared, and approves solely for the purposes of section 21 of the Financial Services and Markets Act 2000, research which has been prepared by any of its affiliates. Private U.K. investors should obtain the advice of their Morgan Stanley & Co. International Limited representative about the investments concerned. In Australia, this report, and any access to it, is intended only for "wholesale clients" within the meaning of the Australian Corporations Act.

Additional information on recommended securities is available on request.

Morgan Stanley

The Americas
1585 Broadway
New York, NY 10036-8293
United States
Tel: +1 (1)212 761 4000

Europe
25 Cabot Square, Canary Wharf
London E14 4QA
United Kingdom
Tel: +44 (0)20 7513 8000

Japan
20-3, Ebisu 4-chome
Shibuya-ku,
Tokyo 150-6008, Japan
Tel: +81 (0)3 5424 5000

Asia/Pacific
Three Exchange Square
Central
Hong Kong
Tel: +852 2848 5200