Essential Trends and Dynamics of the Endpoint Security Industry

Lenny Zeltser wrote this paper together with a co-author who chose to remain anonymous.

May 2005

This paper examines trends and dynamics of the endpoint security industry, and shows how business strategies of market leaders such as Symantec exemplify these factors. When exploring current developments in the information security marketplace, we stipulate that this sector is beginning to converge with the general IT software industry in response to factors such as the evolution of the industry structure, competitive dynamics, regulatory compliance efforts, and the maturing state of security products.

Table of Contents

Introduction

This paper examines trends and dynamics of the endpoint security industry and evaluates the performance of market leaders such as Symantec in the context of these factors. We begin by defining the scope of the industry and explore the evolution of its structural characteristics and the value chain. Next, we highlight Symantec as a case study exemplifying the trends we've identified in the industry. We then discuss the company's acquisition of VERITAS, which we believe is a response to the emerging shift from security as a product to security as a feature; namely, the transition away from stand-alone security products and toward more general IT products with embedded security features. In the final section of the paper, we explain how the emerging shift in value creation that we've identified in the endpoint security segment is indicative of changes sweeping the larger security industry as a whole.

Characteristics of the Endpoint Security Industry

Scope of the Industry

Established in the early 1990's as the *anti-virus* software industry, it has evolved to encompass *endpoint security* software. This industry includes companies that develop information security software for protecting endpoint systems such as laptops, desktops, and servers.

A list of endpoint security software categories includes:

- Anti-virus software
- Personal (host-centric) firewall software
- Personal (host-centric) intrusion detection software
- Anti-spyware software
- Behavior-blocking software

The general trend in the endpoint security industry has been to consolidate disparate applications listed above into a unified product or a suit of integrated products.

Industry Size Estimates

Even though the endpoint security industry encompasses several product categories, the driving factor behind its growth has been the anti-virus sector, which focuses on threats associated with malicious software (malware). In fact, according to Gartner, anti-virus software has been the fastest growing category among security software for several years, growing at more than 30% in 2004.[1] Therefore, to get a sense for the minimum size of the endpoint security software industry, we can look at the size of the anti-virus software sector.

The anti-virus sector is a $3 billion market, according to 2004 IDC estimates.[2] The market is split between consumer ($1 billion) and enterprise ($2 billion) segments. McAfee and Symantec each hold about 25% each of the corporate segment, with competitor Trend Micro trailing at 15%.[3] The four largest players—Symantec, McAfee, Trend Micro and Computer Associates—comprise 78% of the total antivirus market.

Structural Characteristics of the Industry

The endpoint security industry is characterized by strong competition, fueled by relatively high technology spillover and economies of scale. The industry's heterogeneous customer segments are often faced with significant switching costs, and pay attention to the brand of the security product's vendor. These structural characteristics are explored in greater detail in the following listing:

- **Spillover.** Technology spillover in the endpoint security industry is fairly high. Although competition between firms is significant, security professionals have strong ties across companies, and share information via conferences and industry associations. Additionally, because many technological innovations in this industry are based on extremely high-level concepts (for example, behavior-based instead of

---

[1] Norma Schroder, "Forecast: Security Software, Worldwide, 2005-2009 (Executive Summary)," Gartner. March 30, 2005.

[2] Ellen Messmer, "Security Titans Intensify Rivalry," *ComputerWorld*. June 16, 2004 URL: http://www.computerworld.com/printthis/2004/0,4814,93869,00.html.

[3] Zeus Kerravala, "Ubiquitous but Not Mature: Antivirus Needs to Grow Up," Yankee Group. April 12, 2005, URL: http://www.yankeegroup.com/public/products/decision_note.jsp?ID=13023.

signature-based malware identification), once a company has introduced a new concept-based product into the market, it is fairly easy for rival firms to design around any patents or copyrights.

- **Switching Costs.** Switching costs vary across industry segments. Consumer switching costs are notable but not excessively high, requiring only the installation of a new anti-virus software product and a switch to the corresponding anti-virus update service. However, as with most other enterprise software, switching costs in the corporate segment are very high: companies must re-train IT staff, test the new product, and engage in a costly firm-wide roll-out. Additionally, as the market has matured, security vendors have bundled anti-virus software into larger endpoint security suites: in this case, switching from one product to another may require replacing the entire security suite.

- **Demand Heterogeneity.** Although the early anti-virus market was characterized by little heterogeneity of demand, the modern endpoint security market has broadened the scope of the industry and now must cater to a variety of changing user needs.

- **Economies of Scale.** Successful firms in the endpoint security industry must shoulder considerable operational R&D and marketing expenses, so economies of scale are important in this sector.

- **Brand.** Endpoint security products, such as anti-virus software, are difficult and risky to evaluate. As a result, brand is very important in this industry. Both consumer and corporate segments of the industry rely heavily on brand as a signal of quality.

Competitive Dynamics

Two firms, Symantec and McAfee (formerly Network Associates), have dominated the endpoint security industry since the early 1990s. Although majority market shares have periodically shifted between the two firms over time, the industry has generally been divided between the two market leaders, who combined have comprised between 60% and 85% of the market since 1993. Since its beginning, the industry has been marked by frequent acquisitions of smaller rivals by the two industry leaders. In fact, Symantec had negligible anti-virus capabilities until its acquisition of Peter Norton Computing in 1990.

One of the reasons Symantec and McAfee have been able to defend their market positions so successfully is that they entered the endpoint security software industry relatively early and benefited from the reinforcing forces within the industry. Enjoying the position of early market leaders, the two companies chose to invest the resources gained from this success into developing complementary assets such as strong brands, R&D labs, and channel relationships. These resources proved invaluable in the rapidly expanding industry and, in turn, solidified the companies' positions as market leaders.

Additionally, the two companies have managed to compete via product differentiation instead of price. Although smaller competitors have reduced prices to attempt to gain market share, Symantec and McAfee have always maintained similar pricing. In fact, by expanding product SKUs and entering into a service payment model, the vendors have actually considerably increased the prices they command for their products. For example, Symantec has managed to increase average product prices by approximately 25% for the last several years.[4]

The discussion of competitive forces in the industry wouldn't be complete without addressing Microsoft's activities in this market. Perhaps the first credible signal that Microsoft will participate in the endpoint security industry appeared with the release of a personal firewall product that is available without extra fees as part of Windows XP operating system. With the release of an enhanced version of the personal firewall in Windows XP Service Pack 2, Microsoft introduced features that made the product friendlier to enterprise environments than it was before. Microsoft's perusal of this market became more apparent after it acquired several companies in the endpoint security and anti-virus space: the anti-virus software vendor GeCad in 2003, the anti-spyware maker Giant Software in 2004, and the maker of anti-virus gateway products Sybari in 2005.

In early 2005 Microsoft released the beta version of its anti-spyware tool, based on the technology acquired with the purchase of Giant Software. Undercutting margins of numerous commercial anti-spyware products, Microsoft announced that its anti-spyware

[4] Peter Kuper & Brian Essex, "Symantec," *Morgan Stanley Investment Report*. January 5, 2005, p. 1.

tool will be provided free of charge for all licensed Windows users.[5] Microsoft is expected to also release a more general anti-virus product by the end of 2005, although the company is unlikely to offer it for free or at a significant discount, in part to prevent potential anti-trust issues, and in part to take advantage of this revenue source.

Microsoft's current and upcoming endpoint security products—personal firewall, anti-spyware tool, and anti-virus software—are focused on consumer markets, and are unlikely to gain significant presence in the enterprise market for at least several years. Larger enterprises will still be willing to pay for the piece of mind of established security vendors, and for the enterprise-level security management tools that they offer. This gives existing endpoint security vendors some time to establish strategies that balance Microsoft's activities in this market.

Industry Evolution: From 1990 to 2005

Technological and Cultural Influences

Over the 15-year span of its existence to date, the endpoint security industry has been shaped by the evolution of malicious software, from the development of the first boot virus in the mid-1980s, to the more recent phenomena of macro viruses, network worms, and spyware. Figure 1 shows a timeline of the evolution of malicious software, which drove the development of the corresponding protective technologies. For example, when macro viruses appeared in the mid-to-late- 90s, anti-virus vendors needed to rewrite their malware detection software almost completely to address a threat that was application- rather than operating system- specific. As polymorphic viruses began to appear, the vendors were again required to re-draft their systems to detect malicious code using behavioral techniques instead of signatures. (Malware prevalence data presented in Figure 1 is based largely on the table included in Appendix C, *Popular Viral Malware Specimens, 1995-2005*.)

[5] Robert Lemos & Dawn Kawamoto, "Windows Anti-Spyware to Come Free of Charge," CNET News.com. February 15, 2005. URL: http://news.com.com/2100-7355_3-5577202.html.

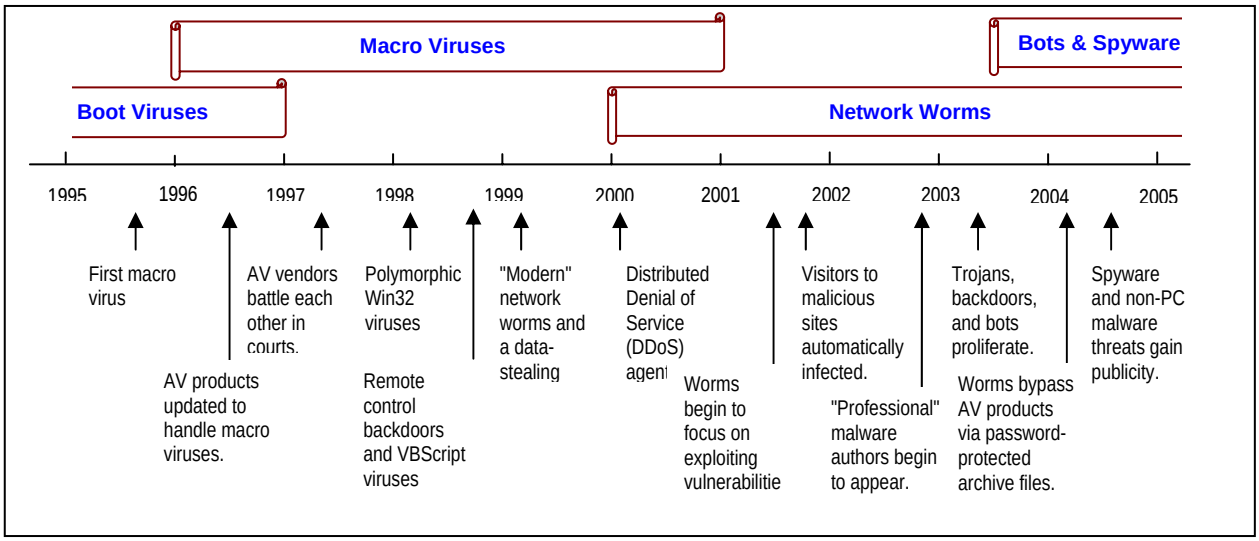

Figure 1: Timeline of Malicious Software Technology, 1995-2005

Additionally, the industry has been affected by the changing nature of Internet connectivity. The growing adoption of Internet-connected devices has affected mainly the scope of the industry: the potential anti-virus user base increases as more and more people are connected to the Internet, and the need for anti-virus products increases as users connect more frequently and for longer periods.

Over time, the risk of malware infections has increased; at the same time, the increased Internet connectivity has drastically hastened the transmission rate of infection. These forces have caused security software to change from a low-priority niche application to a mission-critical enterprise and consumer product. The scope of the industry has also broadened to include complementary technologies, such as host-centric firewalls and intrusion detection systems, and the very definition of end-point security has expanded to address issues such as maintaining personal privacy (anti-spyware), and protecting users from intrusive annoyances (unwanted pop-up ads).

The Evolution of the Industry Structure

The nature of corporate resources need to excel in the endpoint security industry has changed dramatically since its era of ferment in the early 1990s. Figure 2 illustrates the evolution of the general industry structure between 1990 and 2005, capturing the significant

increase in the industry's barriers to entry and the decrease in buyer power. Appendix A, *Evolving Forces in the Endpoint Security Industry*, describes these forces in greater detail.

Industry Force	**1990**	**1997**	**2005**
Barriers to Entry	Low	Medium	High
Supplier Power	Low	Low	Low
Buyer Power	High	High	Low
Substitutes	Low	Low	Medium

Figure 2: Evolving Forces of the Endpoint Security Industry Structure, 1990-2005

The path to success in the endpoint security industry has shifted from an emphasis on uniqueness (effective anti-virus technologies) to complementary assets such as brand, customer support capabilities, R&D competencies, and channel relationships.

More specifically, the industry in the early 1990s possessed the following characteristics:

- **Uniqueness is very important.** The industry is new, and firms are competing to establish a dominant design in technology as well as a standard business model. Success is determined primarily by the effectiveness of the firm's anti-virus technology. It is during this early period that the market leaders emerge.

- **Complementary assets are somewhat important.** *Brand* is not very important, since most users are early adopters, who are well-informed and make educated purchasing decisions based on product quality. Since the market is still very small and limited to highly knowledgeable IT specialists, the difficulty of evaluation, which makes brand so important in the general consumer market, is not a significant factor. Early adopters buy products direct from vendors; *channel* relationships are not yet critical to success. Because products are initially stand-alone applications that do not require updating, they don't yet require the extensive *support* capabilities that vendors must posses to defend against the rapidly-changing threats that characterize the later market.

In contrast, the industry in 2005 has different properties:

- **Uniqueness is moderately important.** Because the nature of security threats is constantly evolving, new technologies are constantly required to maintain security. However, uniqueness has become less important relative to complementary assets

- **Complementary assets are very important.** *Brand* is very important. Consumers find the effectiveness of security products difficult and risky to evaluate, and rely on brand as a signal of quality. *Channel* relationships are critical to reaching enterprise and retail consumers; now that the anti-virus industry is a mass software market, vendors rely on OEMs, VARs, systems integrators, and retail distributors to reach customers. *Support capabilities* are particularly relevant in the enterprise segment, though important across the industry. Threats change rapidly, and vendors must establish R&D facilities to constantly identify and eliminate new threats; they must also develop extensive support procedures to customers on day-to-day basis. Timing is critical in this industry, so vendors must maintain a considerable support and distribution infrastructure to deal with threats in a timely manner.

The Value Chain of the Endpoint Security Industry

The Evolution of the Industry Value Chain

A number of factors mentioned in the *Technological and Cultural Influences* section have caused the endpoint security industry to change drastically since early 1990s. Such significant changes in technology and market scope have overhauled the structure of the industry value chain. Customers, customer needs, channels, and the value proposition of end-point security products in this industry in 2005 bear little similarity to their counterparts in the early 1990s. As a result, companies have had to develop an entirely different set of resources to meet customer needs in this new environment. Appendix B, *Industry Factors Comparison*, summarizes key aspects of the endpoint security industry, which helped shape the value chain in the early 1990s and 2005.

The technical and structural changes in the industry have completely overhauled the industry's value chain. As illustrated in Figure 3, the structure of the value chain has become more complex, with several channels reaching different customer categories. Some of the most interesting aspects of the 2005 version of the value chain are the roles that ISPs and security start-ups play in it, as we discuss in the next two sections.

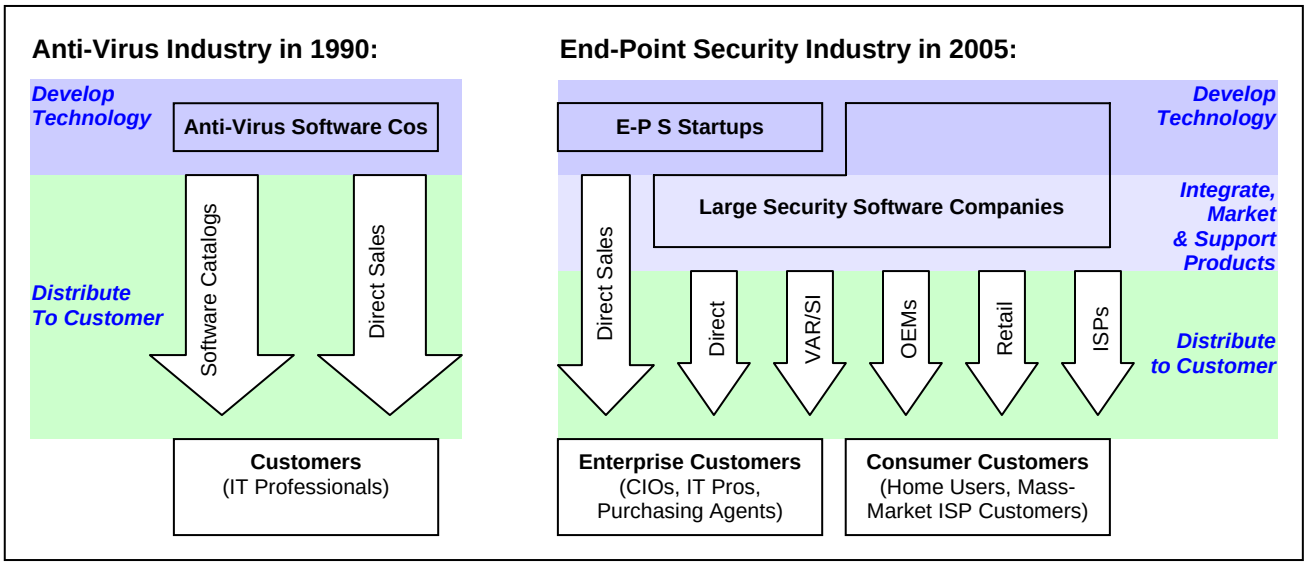

Figure 3: The Evolution of the Industry Value Chain, 1990-2005

The ISP Enters the Value Chain: Outsourcing Mass-Market Sales

Several trends have contributed to the growing adoption of endpoint security software by home users: the increasing number of people who access the internet, the increasing reliance on always-on broadband connections, and the increasing awareness of threats associated with malicious software infections. As a result, the number of consumers that end-point security vendors need to reach is approaching the population of the Internet-connected world.

Reaching the growing home-user market may be too costly even for leading endpoint security vendors. The emerging trend among these vendors involves partnering with ISPs and other companies that have a direct relationship with consumers: in essence, "outsourcing" mass marketing to the ISP channel. For example, McAfee signed a distribution deal with AOL in 2004 that provides McAfee VirusScan anti-virus software to AOL subscribers at a substantial discount to typical VirusScan annual service fees. In another example of an increased importance of such partnerships to reaching mass-market consumers, MasterCard agreed in 2004 to provide BitDefender anti-virus software to select small business customers in Europe.

The trend of outsourcing mass-market consumer anti-virus sales to other companies is likely to decrease endpoint security vendors' profit margins in this segment, while

encouraging them to focus their marketing efforts on the enterprise customer segment. Moreover, this trend reflects a key change in the long-term value of endpoint security: anti-virus functionality is changing from a stand-alone product to an embedded feature. As the ISP channel captures more of the value provided by anti-virus software, endpoint security vendors are faced with decreasing profit margins.

Outsourcing Technology Development: Exploiters vs. Explorers

Responding to the changes in the industry's landscape, leading endpoint security firms are relying on more nimble start-up companies for developing innovative technologies to address customer needs. This trend is a response to the greater need for industry incumbents to focus on nurturing their complementary assets. As a result of the evolution in the industry, a new layer emerged in its value chain to address the need for marketing, integration, and support of products. For example, as endpoint security applications became mission-critical enterprise software, customer requirements changed. Enterprise customers required stable applications that were thoroughly tested for compatibility with other software, and required guarantees for fast updates and reliable support.

To succeed, vendors needed to develop the resources to meet these new requirements: support infrastructure and processes, channel relationships, a strong brand, marketing skills, and so on. On the one hand, customers demanded integrated functionality for ease-of-use and support; on the other hand, the rapid evolution of malware required that vendors quickly integrate new—and often vastly different—technologies into their product portfolios. These factors have contributed to the greater involvement of the leading endpoint security vendors at the marketing level of the channel, with the increasing reliance on start-up companies to develop innovative technologies.

In 2005, the ability to quickly integrate new technology into product suites is an absolute requirement for endpoint security vendors. Customers want a comprehensive solution, and the scope of their requirements has been rapidly broadening: from anti-virus, to personal firewalls, to host-centric intrusion detection, to spyware blocking, and so forth. As the industry has placed more of an emphasis on the resources common to exploitative companies (for example, tightly-coupled complementary assets such as support processes, channel relationships, brand, and centralized control systems), dominant players such as Symantec and McAfee have prioritized the development of these resources. Although this

process has positioned them well to capture the value from their technologies, the "exploitative" corporate structure has left them less able to develop new and innovative security technologies. This weakness is exacerbated by the rapidly-changing technical requirements and scope of the end-point security industry: the next "hot" technology may well require an entirely different set of technical strengths than a company has today.

A Case Study of Industry Evolution: Symantec

Symantec's M&A Core Competency

Symantec is a major player in the information security industry, reporting revenues of US$2.6 billion in fiscal year 2005,[6] and maintaining a portfolio of products that spans most segments of the market. Sharing the spotlight with McAfee, Symantec has been a leading force in the anti-virus market since the early 1990s. Symantec successfully addressed strategic requirements outlined in the *Outsourcing Technology Development* section, by developing a complementary asset essential to maintaining a leading position in this industry: merger and acquisition (M&A) capabilities. Since 1990, the company has made 39 acquisitions, 17 of which occurred between 2000 and 2005. (For details regarding this M&A activity, please see Appendix D, *Symantec's Acquisition History*.)

Mark W. Bailey, a Vice President of business development at Symantec in 1990s, justified the company's reliance on acquisitions to help fuel its product development funnel by pointing out that acquisitions "generate instant revenues against which to fund expenses. … Instead of investing for 12 to 18 months in the internal development of a product, during which time the market window may have closed without providing revenues to offset the development expenses, a merger offers the opportunity for a neutral to positive impact on earnings within a brief period, if not immediately."[7]

---

[6] Symantec Press Release, "Symantec Closes Fiscal Year 2005 with Record Revenue and Earnings." May 4, 2005. URL: http://enterprisesecurity.symantec.com/content.cfm?articleid=5643.

[7] Mark W. Bailey, "New-Age Challenges To Acquirers in High Technology," *Mergers & Acquisitions*, Volume 29, Number 5. March/April 1995. URL: http://web.archive.org/web/19960101-20001231re_/http://www.symantec.com/corporate/mergers/newage.html.

John Thompson, Symantec's Chief Executive Officer (CEO), confirmed that the company uses acquisitions to expand its market presence, while devoting internal development resources to integrate products into unified suites. He further explained, "We launched the first set of integrated security appliances that hit the market in the spring of 2002. Those were organically developed products, not products that came through acquisition."[8]

The flurry of Symantec's acquisitions between 2000 and 2005 has coincided with the broadening definition of end-point security: as incumbents are pressured to incorporate new and increasingly different technologies into their security suites at a faster rate than they can develop them internally, they must look outside the firm to develop technologies quickly enough to meet market demands. The diversification of end-point security requirements can be seen clearly via Symantec's post-2000 acquisitions, which included notable acquisitions outside Symantec's core technologies, including anti-spam functionality (Brightmail, TurnTide), and intrusion detection (Recourse). The merger with VERITAS, a provider of data management software, exemplifies and broadens this trend, as we discuss in the *Symantec's Merger with VERITAS* section.

McAfee, Symantec's main competitor, has followed Symantec's pattern, acquiring, for example, anti-spam (DeerSoft), and intrusion-detection (IntruVert) companies in 2003. However, unlike Symantec, McAfee has not been able to develop a strong complementary asset of acquisition integration, the lack of which has resulted in a string of unsuccessful acquisitions. McAfee's poor acquisition strategy has hurt its performance in the endpoint security sector; because the company was not able to develop the type of complementary assets that the changing industry structure required, their competitiveness has suffered.

Judging by Symantec's success at maintaining a leading role in the industry, we believe the company's strategy of outsourcing much of its new technology development has been an effective one. This is mainly due to the fact that success in the end-point security space is so dependent on the complementary assets of industry incumbents. Because brand, channel relationships, and support processes are so critical to sales in this sector, small explorer firms with new technologies are at a huge disadvantage. The proliferation of explorer firms adds to this market power inequality: there are many, many small companies

[8] "Q&A with Symantec's John Thompson," *BusinessWeek Online*. June 21, 2004. URL: http://www.businessweek.com/magazine/content/04_25/b3888620.htm.

developing new technologies to choose from, which provides Symantec with negotiating leverage. Given this competitive landscape, Symantec is likely to be able to exact favorable pricing from its acquisitions.

Symantec's Merger with VERITAS

In December 2004, Symantec announced its plans to purchase VERITAS, a provider of data management software for $13.5 billion. Symantec justified the merger as a mechanism for providing "enterprise customers with a more effective way to secure and manage their most valuable asset, their information."[9] Mr. Thompson, Symantec's CEO explained that the deal is a strategic move to address a trend of "convergence between securing the infrastructure and ensuring information availability," which, he believes, is the result of the current regulatory environment and the business need to make information available to a greater number of people.[10] Gary Bloom, the CEO of VERITAS agreed with this vision, explaining that the combined company will focus its strategy on performance, availability, and security of IT environments.[11] (We take a closer look at this trend in the *Convergence of Security and IT* section.)

In addition to positioning Symantec to address the changing landscape of the information security industry, the VERITAS acquisition helps the company address the competitive threats that we outlined in the *Competitive Dynamics* section. In particular, by introducing products focused on the enterprise market, Symantec is mitigating the risks of relying too much on revenues from the consumer segment. This segment, comprised mainly of home user and Small Office/Home Office (SOHO) users is most likely to suffer from decreasing profit margins due to difficulties of reaching mass-market consumers, and from the potential market share contraction due to Microsoft's entry into the industry.

---

[9] Symantec Press Release, "Software Industry Leaders Symantec and VERITAS Software to Merge." December 16, 2004. URL: http://www.symantec.com/press/2004/n041216.html.

[10] Ellen Messmer & Deni Connor, "Symantec-Veritas Deal Blends Security, Storage Mgmt. Well, Analysts Say, *Network World Fusion*. December 16, 2004. URL: http://www.networkworld.com/news/2004/1216symanwill.html.

[11] Stephen Shankland, "Veritas CEO Defends Symantec Acquisition," CNET News.com. April 25, 2005. URL: http://news.com.com/2100-1014_3-5683677.html.

Although Symantec's acquisition of VERITAS makes sense from the tactical perspective, it is unclear whether the companies will be able to integrate their operations into a cohesive whole that is necessary to implement the companies' strategic vision. On the one hand, Symantec has built up considerable expertise in acquiring startups to expand its market presence. On the other hand, its acquisition history has been focused on engulfing companies that were significantly smaller than an industry giant such as VERITAS.

Another challenge to the success of the merger is the resulting company's ability to offer a suite of products that holistically address their customers' infrastructure management needs. Although the new and improved Symantec will have products in security and data management sectors, it will not have the ability to manage enterprise networks in the way IBM's Tivoli or HP's OpenView products can. Time will tell whether Symantec will succeed in capturing the market that results from the convergence of security and IT management products. If it does, its old-time rivals such as McAfee and its new competitors such as EMC are likely to find themselves at a significant disadvantage, unless they consider some forms of product consolidation strategies.

The Convergence of Security and IT

In the preceding sections, we have mentioned several findings that point to a long-term shift in the structure and dynamics of the end-point security market: end-point security functionality has started to change from a stand-alone product requirement to an embedded feature. In this conclusive section, we argue that this trend of *security convergence* in the end-point security market is indicative of a larger trend, which in the long-term will change the structure and dynamics of the information security industry as a whole. We believe security features will be gradually integrated with more general IT products. As a result, aside from niche applications, the stand-alone security product market as we know it today will significantly diminish in size and might eventually cease to exist. We are beginning to observe the trends that lead the industry in this direction in both consumer and enterprise customer segments.

Consumer Anti-Virus: A Model of Future Change

The consumer anti-virus segment, one of the most mature and profitable segments in the end-point security industry, most clearly illustrates the trend of security convergence. As

changes in Internet connectivity and malicious software have made end-point security a ubiquitous requirement, non-security companies have started to respond to this consumer demand by offering security functionality. Recent developments, such as AOL's decision to offer subscribers free anti-virus protection and Microsoft's entry into the endpoint security market are exerting a downward pressure on consumer end-point security prices. Additionally, this end-point security integration has disrupted the segment's value chain (see *The ISP Enters the Value Chain: Outsourcing Mass-Market Sales)*, lessening the security vendors' importance to and contact with the customer. Non-power user consumers demand security, but they don't particularly care how they get it, and have a relatively low willingness to pay. In fact, in Juniper survey conducted in 2005, as many as 35% of broadband users were interested in an ISP-supplied security package only if it was free.[12]

Traditional complementary assets that differentiated leaders such as Symantec and McAfee from smaller rivals are less compelling when competing with reaching to mass-market consumers, and when competing against companies such as Microsoft, who has very strong brand, channel, and support capabilities. Market leaders such as Symantec must look for growth outside historically profitable segments. (Prior to the Veritas acquisition, consumer segment sales comprised 52% of Symantec's revenue). It's clear that in order to create value in this new environment, security vendors must find a way to sustain their position in the value chain. Currently, information security firms are attempting to do this via security convergence; they hope to create value by integrating their security products with more general IT utilities the customers *do* value.

Security Convergence in the Enterprise

The trend of security convergence is beginning to manifest itself in the enterprise segment. New regulations, such as HIPAA, the Gramm-Leach-Bliley Act, and Sarbanes-Oxley, have forced companies to examine the effectiveness of their internal controls and, as a result, to invest in their security systems and processes. This trend has broadened the base of enterprise security customers and requirements. As the enterprise customer base and security requirements increase, companies who in the past did not regard security as a high priority and did not have dedicated security teams must find ways to address their security

---

[12] Juniper Data. "Consumer Willingness to Pay for Security and Entertainment VAS Bundles." January 26, 2005. URL: http://www.jupiterresearch.com/bin/item.pl/data:quickchart/59/id=93243.

needs. Like in the consumer segment, we've seen a demand among this expanded set of enterprise customers for simpler, more integrated products, which has led to the development of "one-stop-shop" security suites. A report by the Meta Group confirms this trend, suggesting that "there is an increasing realization that traditional operational disciplines (that is, configuration management, patching, software maintenance, secure disposal, acceptable usage, and so on) can have a significant impact on overall security posture."[13]

This maturing of security products is leading to the delegation of more security functions to IT departments. As products require less specialized knowledge, security responsibilities, historically restricted to security specialists, can be delegated to general IT staff. In a personal conversation with us, a Chief Security Officer (CSO) of a major financial institution has confirmed that his firm is laying the groundwork for integrating many of its security and IT functions into a unified operation.

Like in the consumer endpoint security segment, where we see security functionality integrated into ISP offerings, security as a *general requirement* will become integrated into other, more general, IT products. The slough of recent security mergers supports this assertion. For instance, networking vendors have been actively acquiring security companies in the recent years; most notably, 3Com purchased the maker of intrusion prevention systems TippingPoint in 2005, Juniper purchased firewall vendor NetScreeen in 2004, and Cisco bought the anti-denial-of-service vendor Riverhead and the maker of Virtual Private Network (VPN) technology in 2005. Security features, such as intrusion detection and prevention, which have traditionally been provided by stand-alone products, are being integrated into the actual network. We outlined other manifestations of security converging with IT in the discussion of Symantec's and Microsoft's M&A activities earlier in this paper.

Outlook on the Future of Convergence

How much will the convergence trends, discussed in the previous two sections, affect the information security industry? Although it is unlikely to disappear completely, due to the

---

[13] Peter Firstbrook, "The Changing Threat Landscape," Meta Group. March 24, 2005. URL: http://www.csoonline.com/analyst/report3427.html.

presence of niche markets that will value best-of-breed security technologies, we believe this industry will eventually merge with the general IT sector. Ultimately, the outcome of this thesis will depend upon the long-term success of major acquisitions that attempt to integrate security and IT technologies into unified product offerings—deals such as Symantec's purchase of VERITAS, which we discussed in the *Symantec's Merger with VERITAS* section.

Appendix A: Evolving Forces in the Endpoint Security Industry

Barriers to Entry

- **1990.** In 1990, it's very easy to enter the endpoint security industry. The core requirements are human capital (programmers who develop anti-virus software) and a means of distributing the software (diskettes via mail).

- **1997.** By 1997, entry has become more difficult. Incumbent market leaders, such as McAfee and Symantec, have established powerful complementary assets, which include brand, support infrastructure, R&D knowledge and process, and channel relationships, which have become critical to success in this market. However, malware threats are constantly changing, so companies with effective new defensive technologies can still enter the market.

- **2005.** By 2005, the endpoint security market is very difficult to enter credibly. To effectively compete in this industry, a firm must invest heavily in marketing to make consumers aware of and willing to try the firm's product. Additionally, customers demand extensive support capabilities, which are expensive and difficult for a firm to develop. Lastly, an entrant must develop the channel relationships required to reach enterprise and retail customers.

Supplier Power

Suppliers have never had much market power in this industry, since the only inputs required to produce antivirus software are commodity inputs (CDs, packaging, etc.) and human capital.

Buyer Power

In the early days of the endpoint security industry, the consumer, whether individual or enterprise, enjoyed considerable buyer power: a relatively small set of customers were served by a wide variety of anti-virus vendors. In the mid-90s, consumers benefited from increased competition between the vendors; however, prices remained stable for the most part, the range and availability of products increased dramatically. As the software market

underwent consolidation, consumers lost much of their buyer power. Prices rose after the late-1990s, as the market leaders were able to extract more surplus than before.

Substitutes

In the early days of the industry, the main substitute for anti-virus software was none at all. By 2005, endpoint security software, namely anti-virus products, has become an essential component of an IT infrastructure. Potential substitutes to this software include "hardening" procedures that lockdown the system's base configuration, and gateway security devices positioned at the network's perimeter, rather than individual systems; however, these technologies are more often used as supplementary products, rather than as substitutes.

Appendix B: Industry Factors Comparison

Security Risks

Anti-Virus Industry in 1990	**Endpoint Security Industry in 2005**
Risk Level = LOW. Viruses are spread mainly via diskettes. Manual transmission of viruses means the threat is machine-specific and therefore easy-to-contain. Anti-Virus Software = OPTIONAL Deployment = LIMITED Customers need anti-virus software only for machines with high-diskette traffic – this could be only 1-2 machines in an organization	Risk Level = HIGH. Worms spread quickly via internet connections, and can completely disable a corporate network and disrupt operations. End-Point Security Software = REQUIRED Deployment = WIDESPREAD Enterprise customers must deploy anti-virus software to every desktop

Customers

Anti-Virus Industry in 1990	**Endpoint Security Industry in 2005**
IT Professionals Technical Knowledge = HIGH	Enterprise Customers (IT Pros, CIOs, Corporate Purchasing Agents) Home Customers Technical Knowledge = VARIED (both high & low)

Customer Needs

Anti-Virus Industry in 1990	**Endpoint Security Industry in 2005**
Anti-Virus Functionality	The definition of "security" has broadened to include various technologies (firewalls, intrusion detection systems, etc.) as well as a wider scope of protection, such as maintaining personal privacy (anti-spyware) and protecting users from intrusive annoyances (e. g., blocking unwanted pop-up ads). Enterprise User Needs: Ease-of-installation, guaranteed effectiveness, reliable support, thorough application testing (to avoid conflicts with other software), ease-of-use. Home User Needs: Ease-of-use, guaranteed effectiveness.

Value Channel

Anti-Virus Industry in 1990	**Endpoint Security Industry in 2005**
Direct Sales to Customers (shipment of diskettes from company to customer)	Enterprise Channels (VARs, Systems Integrators, Direct Licensing) Home Customers (OEM, Retail, Direct Downloads)

Complementary vs. Unique Assets

Anti-Virus Industry in 1990	**Endpoint Security Industry in 2005**
Resources for Effective Software: Good Programmer, Thorough Testing Resources for Sales: Direct Sales Force	Resources for Effective Software: Good Programming Team, Good R&D Lab, Thorough Testing, Relationships with major software vendors, M&A Know-How Resources for Effective Support: Good threat updating processes, Large, well-trained support team, Good support communication systems Sales & Marketing Resources: Strong brand, Channel Relationships, Large, well-trained sales force

Appendix C: Popular Viral Malware Specimens, 1995-2005

Popularity figures in the following table are based on data published as part of Virus Bulletin prevalence archives at http://www.virusbtn.com/resources/malwareDirectory/prevalence.

Year	Specimen	Popularity	Key Characteristic	Comments
1995	Form	11%	Boot sector, memory resident	May corrupt disks
1995	AntiEXE.A	9%	Boot sector, memory resident	Stealth capabilities
1995	Parity_Boot	7%	Boot sector, memory resident	Stealth capabilities
1995	Empire.Monkey.B	6%	Boot sector, memory resident	Stealth capabilities
1995	AntiCMOS	5%	Boot sector, memory resident	CMOS-erasing capabilities
1995	Ripper	5%	Boot sector, memory resident	Stealth capabilities; may corrupt disks
1996	Concept	16%	Macro virus	Infects Word docs
1996	Form.A	7%	Boot sector, memory resident	May corrupt disks
1996	AntiEXE.A	5%	Boot sector, memory resident	Stealth capabilities
1996	AntiCMOS.A	5%	Boot sector, memory resident	Does not replicate well
1996	Parity_Boot.B	5%	Boot sector, memory resident	Stealth capabilities
1997	Concept	11%	Macro virus	Infects Word docs
1997	Cap	8%	Macro virus	Infects Word docs
1997	Npad	6%	Macro virus	Infects Word docs
1998	Cap	15%	Macro virus	Infects Word docs
1998	XM/Laroux	8%	Macro virus	Infects Excel spreadsheets
1998	Class	8%	Macro virus	Infects Word docs; uses polymorphism
1999	ColdApe	23%	Macro virus	Infects Word docs; drops a WSH script
1999	Class	10%	Macro virus	Infects Word docs; uses polymorphism
1999	Ethan	9%	Macro virus	Infects Word docs; can mix with other viruses
1999	W32/Ska	8%	Mail worm	Spreads via SMTP and NNTP; patches WSOCK32.DLL.
1999	Cap	6%	Macro virus	Infects Word docs
1999	W95/CIH	6%	File and boot virus	Damages hardware
1999	Marker	6%	Macro virus	Infects Word docs
2000	LoveLetter	12%	Mail and network worm	
2000	W32/MTX	12%	Mail and network worm	Includes a backdoor
2000	Stages	10%	Network worm	Spreads via 4 distinct mechanisms
2000	JS/Kak	10%	Mail worm	Exploits Outlook Express
2000	W32/Ska	5%	Mail worm	Spreads via SMTP and NNTP; patches WSOCK32.DLL.

2000	W32/Navidad	5%	Mail worm	Spreads via Outlook
2000	Marker	5%	Macro virus	Infects Word docs
2001	W32/SirCam	59%	Mail worm	
2001	W32/Naked	9%	Mail worm	Masquerades as a Flash movie
2001	W32/BadTrans	8%	Mail worm	Exploits Windows; installs key logger
2001	W32/Magistr	5%	Mail worm	Includes viral polymorphic code with anti-debug capabilities
2002	W32/Klez	45%	Mail worm	Exploits Outlook; drops W32/Elkern virus; disables AV software
2002	W32/Bugbear	14%	Mail and network worm	Targets Outlook and Internet Explorer; installs a backdoor and key logger; disables anti-virus software
2002	W32/SirCam	8%	Mail worm	
2002	W32/Opaserv	7%	Network worm	Spreads via file shares
2002	W32/Magistr	6%	Mail worm	Includes viral polymorphic code with anti-debug capabilities
2002	W32/BadTrans	5%	Mail worm	Exploits Outlook; drops W32/Elkern virus; disables AV software
2003	W32/Sobig	38%	Mail and network worm	Installs a mail proxy; auto-updates itself
2003	W32/Opaserv	20%	Network worm	Spreads via file shares
2003	W32/Mimail	8%	Mail worm	
2003	W32/Klez	7%	Mail worm	Exploits Outlook; drops W32/Elkern virus; disables AV software
2003	W32/Dumaru	6%	Mail worm	Installs a password-stealing trojan
2004	W32/Netsky	72%	Mail and network worm	Disables security software and the W32/Beagle worm
2004	W32/Bagle	15%	Mail and P2P worm	Exploits Windows; disables security software
2004	W32/Sober	5%	Mail and P2P worm	

Appendix D: Symantec's Acquisition History

Date	Acquired Company	Cost (mil)	Description
Jan-05	Veritas	$1,350	Storage & backup
Dec-04	@Stake		Security Auditing & Analysis, Digital Security Consulting
Dec-04	Lyric		Consulting for Risk Assessment & Secure Design
Jul-04	TurnTide	$28	Anti-Spam (Network Level)
May-04	Brightmail	$370	Anti-Spam
Feb-04	ON Technology	$100	Enterprise Infrastructure Management Software Provider
Oct-03	SafeWeb	$26	SSL, VPN Security Appliances
Sep-03	PowerQuest	$150	Storage Management Software Provider
May-03	Nexland	$20	Internet Security Solutions for Corporate Remote Offices
Aug-02	Security Focus	$75	Threat & Vulnerability Data Provider
Aug-02	Recourse Technologies	$135	Intrusion Detection Systems
Aug-02	RipTech	$145	Managed Security Provider
Jul-02	Mountain Wave	$20	Enterprise Security & Software Management Services
Jul-01	Foster Melliar Security Mgt Division		Enterprise Security Management
2001	Linder & Pelc		Network & Information Enterprise Security Consulting
Dec-00	Axent Technologies		Information Security Technology
Feb-00	L3 Network Security Unit		Computer Security Products & Security Consulting
Jul-99	URLabs	$42	Content Security Software
Nov-98	Quarterdeck	$65	Utilities Software / Remote Control/Access Software
Sep-98	Intel's Anti-Virus Business	$16.5	Anti-Virus Technology
Jun-98	Binary Research (Ghost)	$27.5	Disk Cloning Software
May-98	IBM's Anti-Virus Immune System Technology	$20.3	Anti-Virus Technology
Mar-96	FastTrack	$7.2	Network Management Utilities
Nov-95	Delrina (WinFax)	$415	Fax Management Software
Jun-94	CentralPoint	$60	Utilities Software
Aug-94	Intec Systems	$1.9	Contact Management Software
May-94	SLR	$2.3	Application Development Tools
Jun-93	Contact Software	$40	Contact Management Software
Oct-93	Fifth Generation	$48	Utilities Software (incl. Anti-Virus)
Oct-93	Rapid Enterprises	$7.5	
Oct-93	Distributor Pro	$0.8	Utilities Software
Apr-92	Symantec UK Ltd	$25	Utilities Software (incl. Anti-Virus)
Sep-92	Whitewater Group	$3	Development Tools
Sep-92	MultiScope	$6.6	Development Tools
Nov-92	Certus International	$5	Utilities Software (incl. Anti-Virus)
Aug-91	DMA	$20	Utilities Software
Aug-91	Zortech	$10	Development Tools
Aug-91	Leonard Development Group	$3	Applications
Aug-90	Peter Norton Computing	$70	Utilities Software (incl. Anti-Virus)
Aug-87	Living VideoText	$1.6	Personal Information Management Software
Oct-87	Think Technologies	$2.1	Language Development Tools, System Utilities Software
Jan-87	Breakthrough Software	$2.6	Project Management Software
Jan-84	Merger w/ CE Software		
1982	Company Founded		