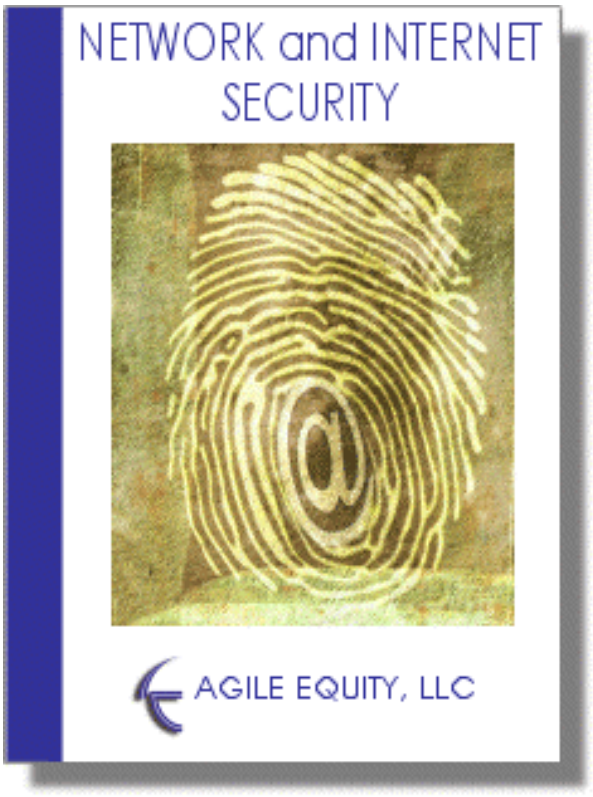


AGILE EQUITY

611 Broadway, Suite 725 New York, NY 10012

Network and Internet Security

I. Executive Summary

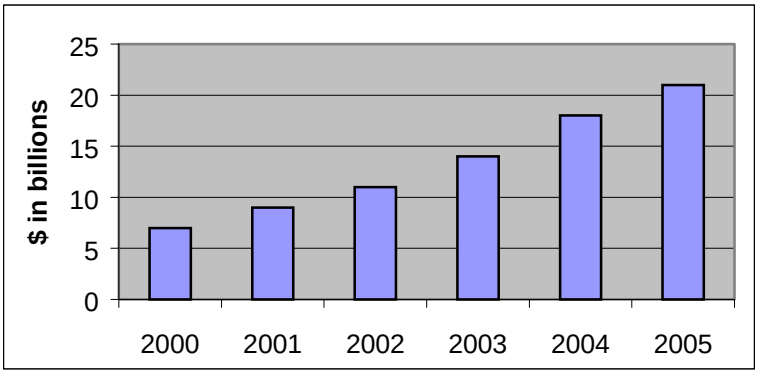
Security is now a top priority for all corporations, private and public, large and small. Over the last two years, we have seen thousands of companies post Web sites and provide employees with e-mail and Internet access. As a result, the risk of an intrusion is many times greater than it was before. Once inside, an intruder can find ways to snoop around; destroy, change, or steal data; and wreak havoc of various sorts. Companies, government agencies, and individuals have all seen the effects of a security breach.

The growth of the Internet has increased the risks faced by owners of private networks. By definition, the Internet is a public, cooperative, and self-sustaining system accessible to hundreds of millions of people worldwide. It was not developed to transmit confidential data. As businesses inevitably move more and more of their data onto the Net, they also inevitably increase their exposure to risk. Organizations have been so focused on getting new customers and getting "big fast," they have devoted little time and effort to securing their data.

The technology industry as a whole has been hit by the economic downfall, but security has held up reasonably well compared to many of the other tech sectors. While other technology initiatives have been put on hold, security is now considered a necessity in order to do business. Companies are poised to make the investments in security that they had previously made in Internet infrastructure and e-commerce. This is not to say the entire security market is immune from an economic slump. Technologies that have a proven track record, solve mission-critical problems, and offer a high return on investment (ROI) remain attractive. Internet security spending is estimated to grow at a compound annual growth rate (CAGR) of 29 percent, from $6 billion in 2000 to over $20 billion in 2005.

The network security market is responding quickly to the challenge by adapting existing authentication and encryption technologies to Internet connections and by developing new security products. However, the current state of the market is characterized by a myriad of evolving standards, technologies, and products that solve one piece of the security puzzle or another, but do not yet interoperate well. This report will attempt to discuss the security industry as a whole, with an eye towards the wave of corporate consolidation that has already begun. We will break the market down into sub-markets, provide an overview of a selection of companies in each sector, and discuss some of the technologies available or under development.

Internet Security Spending Estimates[1]



[1] IDC estimates

II. Consolidation Trends

A. Increased Fragmentation Leading to Further Consolidation

The steady stream of venture capital (VC) money into the security sector over the past few years has created a plethora of similar companies. Not all of them will succeed and become profitable. Much like the hype surrounding other technology sectors in recent years, the real need for security products does not justify the number of new companies that have formed. Without additional funding, the only possible outcome is for them to go bankrupt, merge, or be acquired. As a result, mergers and acquisitions (M&A) activity will increase as VC firms and institutional investors stem new investments and remaining security firms seek acquisitions that will help them build the market and product breadth needed to compete with the more established players. One such company is Vigilante, which already made one acquisition this year. According to CEO Eric Fullerton, Vigilante is looking for other deals, as well, either for new technologies or for a consulting practice that would give Vigilante direct access to additional customers. In addition to Vigilante's transaction, 18 other mergers or acquisitions were completed by the end of July 2001. Altogether, the deals are worth in excess of $765 million.

Many of the companies in the security market have formed partnerships to create an end-to-end solution – the Holy Grail for security providers. This indicates that many companies' software or services are interconnected. Customers seek vendors with numerous partners to ensure credibility and interoperability. The next logical step for vendors, then, is to bolster their offerings by acquiring or merging with their partners. We expect a convergence in the security industry with all kinds of permutations. The security industry is so fragmented that the players involved need to work with others to create economies of scale and economies of scope if they want to emerge as a formidable player.

In an extremely fragmented market such as the security sector, three types of companies emerge: Leaders, Contenders, and Pretenders. As the Leaders gain additional market share, they use their increased size to acquire other companies – the Contenders – to complement their existing business. In doing so, the Leaders are able to further increase their market share by selling additional products and services to an expanded customer base. As the consolidation between the Leaders and the Contenders takes place, the Pretenders continue to lose market share and find it difficult to raise additional funding from investors or find a merger partner. The ultimate result is that the Pretenders go out of business and a handful of established players remain. Within the next five years, a similar consolidation scenario is expected to transpire among the 500 or so current companies in the security sector. In fact, it has already begun. RSA Security, a company with a market cap of $1.4 billion, has already made three acquisitions in 2001, with a combined value of $216 million. Additional acquisitions will occur by similar-sized companies, such as Avaya Communication, Internet Security Systems, Network Associates, and SonicWALL, as they seek to gain scale in specific elements of their business by expanding their product and service offerings and customer bases.

B. Recent Mergers and Acquisitions Transactions

The security market has become very fragmented, with over 500 companies fighting for market share in the approximately 46 categories and subcategories tracked by International Data Corp. (IDC). Additionally, the market is characterized by a dichotomy between the established, public companies and the smaller upstarts that have recently received funding. As a result, consolidation is accelerating among private and public companies as the industry moves from adolescence to a state of rapid growth and increased competition.

The following table presents the M&A transactions that have occurred between January 2001 and July 2001:

Date Closed	Buyer	Target	Ownership (Buyer/Target)	Deal Size ($000's)
Jul-01	**RSA Security**	Securant Technologies	Public/Private	**$136,500**
Jul-01	Cisco Systems	Allegro Systems	Public/Private	181,000
Jul-01	RedSiren Technologies	Secure360	Private/NFP	N/D
Jul-01	Cyota	Auripay	Private/Private	N/D
Jul-01	Universal Domains Inc	Cavio Corp	Public/Private	N/D
Jun-01	**Internet Security Systems**	Network ICE Corp	Public/Private	**228,500**
Jun-01	**RSA Security**	3G International (3GI)	Public/Private	**12,000**
May-01	Guardent	DefendNet	Private/Private	N/D
May-01	AtomicTangerine Inc	SecurityPortal Inc	Private/Private	N/D
May-01	Pearson PLC	Kajax Engineering Inc	Public/Private	N/D
Apr-01	**VASCO Data Security Int'l**	Identikey Pty Ltd	Public/Private	**2,000**
Apr-01	BIZ Interative Zone Inc	Litronic Inc	Private/Public	N/D
Apr-01	Net Tel International Inc	zTrace Inc	Private/Private	N/D
Apr-01	Vigilante	Networks Vigilance	Private/Private	N/D
Mar-01	SonicWALL	Ignyte Technology	Public/Private	10,200
Feb-01	Phoenix Technologies Ltd	Integrity Sciences Inc	Public/Private	3,800
Feb-01	Vigilinx	LogiKeep	Private/Private	N/D
Feb-01	**RSA Security**	Xcert International	Public/Private	**67,500**
Jan-01	Avaya Communication	VPNet Technologies	Public/Private	126,000
Total				**$767,500**

Source: Mergerstat and VentureWire.

N/D = Not Disclosed

Since the beginning of 2001, approximately 19 M&A transactions have been completed in the security industry, totaling in excess of $765 million. Of the 19 transactions, 11 were acquisitions of a private company by a public company, six were transactions between private companies, one was an acquisition of a public company by a private company, and one was an acquisition of a university's research center by a private company.

C. Active Acquirers

The highlighted companies in the above chart, Internet Security Systems, RSA Security, and VASCO Data Security, represent the companies that have been the most acquisitive since January 2000. All three of these companies are public with market caps ranging from $60 million to $1.4 billion, with a median market cap of $963.5 million. Five of the acquisitions completed since January 2001 accounted for 46 percent of the 19 transactions' total value. In addition, two additional acquisitions by Internet Security Systems and VASCO Data Security for undisclosed amounts occurred in the latter half of 2000. These two acquisitions were also of private companies.

D. Strategy and Tactics

The majority of this year's acquisitions have involved companies seeking both to fill a hole in their product line or service offerings and to become end-to-end security providers. Several of these acquisitions were initiated by service companies that wanted to add a technology component to their product offerings and, vice versa, by pure play technology companies that wanted to add a service component to their offerings. These vertical acquisitions usually involved large public companies that purchased smaller private companies. Additionally, there have been a number of horizontal acquisitions, mainly among private companies seeking to gain product depth and market breadth in order to compete with the larger, more established players. Lastly, several acquisitions have occurred among Internet companies in the e-commerce and Web spaces seeking to build highly related adjacencies by adding a security component to complement their current product offering.

A well-defined strategic rationale is imperative for capturing shareholder value through acquisitions. To date, we have seen three primary motivations for consummating a transaction:

1. *Growing Scale* – Increasing scale in specific elements of the business and using these elements to become more competitive overall. Understanding the business and market definitions of scale-based initiatives can be difficult, since they will continue to change in the security industry over time.
2. *Broadening Scope* – Systematically acquiring specific areas of expertise to accelerate new business development and technology. Many companies are lacking product and/or services depth and breadth.
3. *Related Businesses* – Expanding into related business to create pull-through revenue synergies. Companies are looking to acquire new products and services that are tangential to their core business, since organic development is too slow and dilutes focus.

In our view, the security industry is ripe for consolidation. Many clients are confused by the abundance of products and services from numerous vendors. Clients are demanding integrated solutions, product suites and wireless capabilities from one provider. In addition, the market is too fragmented, with many companies lacking the size and capital necessary to remain competitive.

We are surprised that the M&A function has not been a more important tool in implementing the core business strategy for companies. To date, many security companies lack an effective merger and acquisition program within their organizations. Building a solid M&A process would provide these companies with the ability to identify, value and assess strategic targets and successfully integrate targets. A poor process can lead to those disastrous deals in which a company fails to get the vision, culture and strategic rationale properly aligned before executing. More importantly, the primary risk we see is the inability to acquire strategically important and possibly industry-transforming targets, thereby being left behind and becoming bait for the stronger, more acquisitive leaders.

In our view, smart companies make their greatest strategic moves during periods of financially difficult times. Successful companies place counterintuitive bets in a downturn in order to dramatically transform their market positions. If the core business is worth holding and growing, focused acquisitions during downturns should reduce risk, not increase it.
In summary, we believe an effective M&A process is interconnected with – not separate from – corporate strategic planning. A clear strategic vision that considers changing markets and business models and is linked to rigorous valuation will be a strong predictor of M&A success.

III. Industry Overview

A. Background

The rise of network computing in recent years has created a need for connectivity across not only Local Area Networks (LANs), but also enterprise-wide networks that span multiple LANs and Wide Area Networks (WANs). Concurrently, with the shift to distributed computing architectures, Internet use by organizations has grown dramatically, driven largely by the development of the Web and graphical browsers, the proliferation of personal computers, and the emergence of compelling Web-based content and commerce applications.

The increase in email use, information browsing, and the exchange of non-sensitive data has fueled the growth of the Internet. However, business and government organizations are increasingly connecting their enterprise networks to the Internet to move beyond these limited uses, thus facilitating and supporting a number of more valuable and sensitive activities, including B2B transactions, Web-based electronic data interchange (EDI), Web-based access to account and benefits information, and secure messaging and transaction processing. The proliferation of client/server architectures and the growth of the Internet as a business tool has also led to the use of Internet Protocol (IP)-based communications on intranets and private enterprise systems that share information and services both within and outside the enterprise network.

Although open computing environments and connections to the Internet have many business advantages, their accessibility and the relative anonymity of Internet users make the systems and networks vulnerable to security breaches and employee misuse. The Internet is inherently insecure. Internet Open Protocol is a connectionless protocol, and one of the resulting implications is that the transmission of data is less secure than a point-to-point connection-based protocol.

Any party that has an Internet connection can view data that travels across or is connected to the Internet (assuming the data is unencrypted). With the unforeseen, explosive growth of distributed computing, security has emerged as a primary concern. The conflicts between the benefits of the Internet connection and the need to protect information and applications from unauthorized access, misuse, and business disruption requires solutions that allow organizations to monitor activity, authenticate users, encrypt data, block unwanted activities, and easily implement and enforce security policy.

To adequately secure a network, IT managers must have the resources to not only correctly configure the security components in each system, but also to understand the risks created by any change to existing systems on the network. As a consequence, Internet security may be one of the most daunting tasks facing IT managers over the next decade. Given the substantial capital commitment required to establish an e-commerce presence and the larger transaction value of most B2B exchanges, the stakes are high. There can be no downtime on the supply chain. Trade secrets and business confidences must be kept private and safe from unauthorized use.

It will be critical for clients to establish a two-way, end-to-end security solution. To operate a full-scale e-commerce business, companies need assurance that online transactions are secure as they make their way from the enterprise to the end user. In a recent *Wall Street Journal* article, some Web merchants reported that nearly half of their Web-based credit card transactions were fraudulent. Intranets or internal networks within the same organization are not safe either. Industry studies show that roughly 70 percent of security breaches are internal. However, investments in security solutions remain low today despite the security risk companies increasingly face. Findings from Forrester Research reveal that, on average, *Fortune* 1000 companies spend less than $1 million annually on network security, even though many have invested aggressively in e-commerce initiatives. In a recent survey of IT managers, *Information Week* magazine found that network security tops the agenda of IT managers for 2002.

Evolving Beyond Protecting the Network

In addition to blocking access to a computer network and safeguarding data, information security services need to replicate the types of functions normally associated with physical documents as e-commerce continues to emerge. Documents may require signatures and dates; they may need to be protected from disclosure, tampering, or destruction; they may be notarized or witnessed; or they may be recorded and licensed. As electronic information becomes more pervasive and important, many of the roles traditionally performed by paper documents have been surpassed by electronic data. With the rise in the importance of e-commerce, security functionality needs to expand beyond its traditional role.

Security Requirements

To provide complete and total security for Internet and Intranet based communications and transactions, an effective Internet security solution must include these critical security measures:

1. *Authentication* – This identifies and verifies the sender of the data.
2. *Access Control* – This protects clients from unauthorized access to any resource (computers, communications, or information). Access control is the primary means for enforcing authorization.
3. *Data Confidentiality* – This protects information from being disclosed or revealed to parties not intended or authorized to have the information.
4. *Data Integrity* – This protects data from being altered or compromised by unauthorized manipulation.
5. *Non-repudiation* – This creates a system ensuring that the bona fide sender of a transmission cannot deny or repudiate the transmission.

There is no single mechanism or method that provides all of the services above. Instead, a variety of security technologies and protocols have emerged that, in combination, can provide these needed services.

B. Growth Drivers

Several trends are taking off in the network and Internet computing markets are fueling an increase in security spending. These trends follow:

1. *The "Virtual Corporation" and the "Extended Enterprise"* - Companies are rapidly integrating Internet-based communications into their business models, enabling employees, suppliers, and customers to access highly sensitive data through browser interfaces.

With the growing acceptance and use of the Internet as a communications and sales tool, companies continue to expand their Internet-based, enterprise-wide networks to conduct B2B and B2C e-commerce, as well as to communicate with a mobile workforce. As these companies offer access to confidential or proprietary information through the Internet, security becomes of paramount concern. This openness of the corporate network is one of the main factors driving security spending.

2. *Increase in External Traffic* – The growth of the Internet has dramatically increased the amount of external traffic running across corporate LANs. This increase has significantly heightened the potential for a serious security breach, including a virus infection and an attack from hackers and other unauthorized users. In addition, with the growth of B2B and B2C e-commerce, companies must install leading-edge security solutions to protect their Web commerce franchises.
3. *Security Spending Viewed as a Business Enabler* – The return on invested capital (ROIC) on a network security investment is no longer the net present value (NPV) of potential fraud expenses, but the NPV of opportunity costs for business initiatives that would otherwise never get off the ground because of security concerns. Security spending has traditionally been viewed as a cost of doing business. Now, security-based solutions that can eliminate the high cost of leased lines, such as virtual private networks (VPNs), have positioned security spending as an NPV-positive investment.
4. *Growth of Broadband Access* – Emerging broadband technologies such as DSL provide affordable, high-speed Internet access to small and medium-sized enterprises, telecommuters, and employees working at branch offices. These technologies create an "always on" connection that leaves the network wide open to hackers and other unauthorized users.

   Additionally, a fundamental change in network architecture is occurring. Due to local capacity constraints, data storage is being transitioned from local hard drives to Web site servers, increasing transmission speeds and reducing costs. As companies store more of their sensitive information on remote sites, keeping this information secure and safe becomes a priority.
5. *The Threat of Cyber Terrorism Grows* – According to a United States government report on Cyber Terrorism, the U.S. is the world's most technologically vulnerable nation. Cyber Terrorism could cripple the U.S. by disrupting its power systems, telecommunications networks, air traffic control systems, financial data transmissions, government information systems, and even military command systems. Additionally, billions of dollars in proprietary information have already been stolen electronically from U.S. high-tech companies. The FBI estimates this type of crime costs U.S. companies $10 billion annually.

Security Growth is Perpetual – Hackers will always be a fact of life and, as a result, new security threats and holes will constantly appear. Many of today's security products need to be continually updated to remain effective. This need for continual updating presents an attractive business model. In many cases, a product is already outdated the day after it is sold.

Privacy Legislation

The U.S. Congress recently enacted two laws that will serve as near-term catalysts for Security Industry growth. The Gramm-Leach-Bliley Act (GLBA, also known as the Financial Services Modernization Act of 1999) and the Healthcare Insurance Portability and Accounting Act (HIPAA) mandate a new set of privacy and security standards for the financial services and healthcare industries.

GLBA became effective July 2001 and requires that financial institutions be able to display that they have secured and protected customer data. HIPAA becomes effective over the next two to three years and is designed to streamline the administrative functions of healthcare while encouraging healthcare entities to electronically exchange and access information. Another bill is the Electronic Signatures in Global and National Commerce Act, often referred to as the e-signature bill. In effect since October 1, 2000, this act specifies that the use of a digital signature in the United States is as legally valid as a traditional signature. This, however, has not yet taken off because organizations have the right to reject digital signatures and because a technology standard has not been specified.

C. Keys to Success

In general terms, there are three keys to success for a company in the security sector:

1. *Broad Product Lines* – In the past, companies have gone with a best-of-breed approach, choosing different vendors for different security needs. Companies were forced into this because vendors did not offer a complete suite of products, and if they did, one or more of the products were not as secure or manageable as those of another vendor. As the number of products increased, so too did product complexity, and IT managers became more confused than ever. Now, what companies really want is the option to buy more products from fewer vendors. The leaders of the future security market will provide a true end-to-end solution and require the least amount of work from a company's IT staff to implement it.
2. *Solving Business Problems* – The problem with many technology companies is they are more concerned about building the best technology, without considering its business use. An old adage is "build it and they will come." In the case of security, this could not be further from the truth. Vendors must think ahead. For example, it is easy to forecast that authentication, authorization, and administration will be large markets because they address real business needs, enabling companies to share data within and across networks in a secure environment.
3. *Scalability and Interoperability* – Networks are in a constant state of flux and security products and solutions need to be flexible enough to manage change without creating new vulnerabilities. New types of attacks are devised everyday as technology becomes more advanced, and security is only as strong as its weakest component. Companies want products and services that can safely accommodate network growth. In this regard, it is also important that vendor solutions are able to work in conjunction with one another to prevent potential security breaches.

D. Relative Immunity from Spending Cuts

Whether or not the U.S. economy goes into a prolonged recession, the cost of not having security will exceed the cost of security solutions. Security concerns are permanent, and with more and more at risk, security solutions are quickly becoming mission-critical. Investments in these solutions will be among the last expenses cut when companies tighten their belts, and among the first to be implemented when companies have cash to spend.

While spending on network and Internet security is relatively sheltered from cost cuts, it is not immune to them. Perimeter-based security solutions should be the safest segment – most enterprise customers see firewalls and virtual private networks (VPNs) as must-haves, and these will typically be among the last areas targeted for budget reduction among customers. Authentication and encryption products, the key building blocks of privacy and remote access, are just behind perimeter-based solutions as must-haves for customers, regardless of the economic outlook. Additionally, content-based security products such as antivirus solutions will be sheltered from IT spending cuts.

Return on investment (ROI) is key with the current state of IT budgets. Sub-markets such as managed security services (MSS) that can save companies money by outsourcing, rather than investing in, equipment and capital are areas that will be relatively safe.

Segments of the security industry facing greater risks include vendors of Public Key Infrastructure (PKI) products, which could become the basis for distributed networking in the future, but are difficult to deploy and typically have a longer period of cost recovery. In addition, PKI products have a limited penetration in the market at this time. Likewise, operations-security products such as intrusion detection and vulnerability assessment systems are very valuable to most networks, but it is difficult to quantify the amount of money they can save a customer by detecting attacks. Additionally, authorization solutions may see slower demand owing to the slowdown in e-business initiatives, such as exchanges. Digital-rights management solutions offer compelling long-term value propositions to customers, but suffer in the near-term because they have relatively few existing deployments.

E. Continued Funding for Security Companies

Between January 1 and September 1, 2001, over $550 million was raised by security companies from venture capital firms and strategic partners. The following chart lists some of the companies that have received funding:

Date	Company	Security Category	Amount
Sep-01	Arcot Systems	Digital Security	$20,000,000
Sep-01	nCircle Network Security	Network Security	11,000,000
Sep-01	Vordel	XML Security	10,000,000
Aug-01	ForeScout Technologies	Network Security	12,000,000
Aug-01	Conclusive Logic	Infrastructure Management	6,000,000
Aug-01	KaVaDo	Application Security	3,700,000
Jul-01	Sanctum	Web-application Control & Security	30,000,000
Jun-01	OneSecure	Managed Security Services	67,000,000
May-01	Foundstone	Security Assessment	9,000,000
May-01	Guardent	Digital Security	20,000,000
May-01	Atomic Tangerine	Information Security Consulting	12,600,000
May-01	Captus Networks	Network Security	16,100,000
May-01	CertCo	Risk Management & Security Infrastructure	20,000,000
May-01	**Vigilante**	Automated Security Assessment	**4,300,000**
Apr-01	Top Layer Networks	Network Security	8,300,000
Apr-01	Qualys	Network Assessment & Monitoring	20,000,000
Apr-01	**e-Security**	Security Monitoring	**7,000,000**
Apr-01	NFR Security	Information Security	22,300,000
Mar-01	SHYM Technology	Security & Trust Management	17,750,000
Mar-01	NetForensics	Security Information Management	7,000,000
Mar-01	TruSecure	Electronic Security	22,000,000
Feb-01	Gilian Technologies	Web Security	14,000,000
Jan-01	Vigilinx	Digital Security Services	75,000,000
Jan-01	Cyota	Web Payment	11,000,000
Jan-01	Niksun, Inc.	Network Security	27,000,000
Jan-01	**e-Security**	Security Monitoring	**13,000,000**
Jan-01	**Vigilante**	Net Security	**11,300,000**
Jan-01	Entercept Security Technologies	Server Security	33,000,000
Jan-01	CyberSafe	Transaction Security	20,000,000

Source: Venture Wire

The highlighted firms in the above chart represent those that have received more than one round of funding in the first half of 2001. The remaining firms are those that have received a large round of funding, are profiled in this report for receiving funding, or both.

IV. Security Sub-markets

Numerous sub-markets characterize Internet and network security. Most of them are complementary, and vendors don't necessarily compete with one another. There are many large companies in the security sector, but none of them offers an end-to-end security solution for the enterprise market. Even if they did, companies will still choose security products a la carte if any of the products in the suite are substandard.

We have divided the security market into eight sub-markets: encryption, Public Key Infrastructure (PKI), firewalls, virtual private networks (VPNs), authentication and authorization, antivirus, intrusion detection, and managed security services.

Keep in mind that the security industry is constantly evolving. The lines between the sub-markets may blur or new sub-markets may appear. Even now, analysts divide the security industry into different sub-markets. The players in this space are also changing. New companies appear each day with a potential revolutionary technology and larger companies acquire or develop technologies to add functionality to their current line of products.

A. Encryption Market

When one thinks about Internet security, encryption is most likely the first term to come to mind. The use of encryption and decryption is as old as the art of communication and the technology is considered a relatively mature one in the security industry. While it is widely used and a key building block for security, it is ironic that this market is relatively small ($166 million in 2000) compared to the rest of the security industry.

Encryption companies such as RSA Security do not sell their algorithms to customers. Rather, they sell a package that allows vendors to incorporate encryption technologies into their own applications. Some of the applications include Web browsers, commerce servers, e-mail systems, and virtual private network products.

There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption. Public-key encryption is a cryptographic system that uses two keys – a public key known to everyone and a private or secret key known only to the recipient of the message. Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt the message. (This differs from public-key encryption, which uses one key to encrypt a message and another to decrypt the message.) In the context of Internet security, public-key encryption is much more important. It allows two parties that have no prior reason to trust each other to exchange information securely over the Internet.

Competitive Landscape

RSA dominates the encryption sector with a 39 percent market share, while several others occupy certain niches. F-Secure, with a nine percent market share, has a leading line of file encryption applications. Certicom, also with a nine percent share, has developed an elliptic-based cryptography that will be used in wireless devices.

RSA has maintained its dominance due to its leading group of partners and customers, as well as its establishment as the de facto standard in authentication and communications infrastructure. There is little danger that RSA will lose market share, as there is little demand for stronger encryption than what is already in the market.

Any hacker will tell you that it is much easier to enter a network through other points of entry rather than try to break an encryption algorithm. Furthermore, while companies such as Certicom and NTRU Cryptosystems have more technologically advanced encryption, there is little buzz or use for these improvements in the near future.

According to IDC estimates, the worldwide encryption market was worth $185 million in 2000 and is only expected to grow at a compound annual growth rate (CAGR) of 15 percent to over $300 million in 2004. Because this sub-market is small compared to the rest of the security industry, and dominated by one vendor, it often receives little attention.

B. Public Key Infrastructure (PKI) Market

Of all the security sub-markets, public key infrastructure (PKI) is perhaps the one that could emerge as the largest. PKI leverages the core capabilities of encryption technology to enable the management of public keys and digital certificates and to reliably identify parties on a network. The three main components of a PKI solution follow:

1. *Public and Private Keys* – An important element to the public key system is the pairing of public and private keys. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key, even if you know the public key.
2. *Digital Certificates* – An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be, and to provide the receiver with the means to encode a reply.
3. *Certificate Authority (CA)* – The cornerstone of a PKI system, a certificate authority (CA) is a trusted third-party that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity.

Obviously, being able to trust another party on the Internet has been an issue since the Internet's inception. As the amount of Internet traffic and e-commerce grows, so will the need for PKI services. According to IDC, e-commerce revenues could explode to $5 trillion by 2005 as compared to $354 billion in 2000. If this holds true, the PKI market should grow at a compound annual growth rate (CAGR) of 50 percent.

Market Analysis

While there are many growth drivers in this market, the PKI sector has not expanded as fast as many thought it would. PKI solutions are extremely robust and technically advanced, but often serve as a "sledgehammer trying to swat a fly." Their uses are often too complex for commercial use. Today, most e-commerce transactions include small-ticket items such as a book purchased on Amazon.com. These types of transactions do not warrant PKI solutions. At the height of the B2B e-commerce boom, PKI was poised for tremendous growth. But with the current state of the economy, companies have reduced or eliminated spending on B2B e-commerce solutions. The annual PKI product sales are expected to top $1.2 billion by 2003, according to IDC, up from a mere $125 million in 1998.

We believe that customer-demands as well as the PKI solutions will evolve over time. Large companies will reassess their e-commerce strategies and deploy projects that require PKI solutions. PKI companies will continue to modify their offerings. Currently, the management and cost of deploying a PKI solution are considerable and can take several months. PKI companies will have to develop a solution that is simpler and has a lower total cost of ownership (TCO). Once all of these pieces fall into place, application developers will start to produce more software that utilizes PKI.

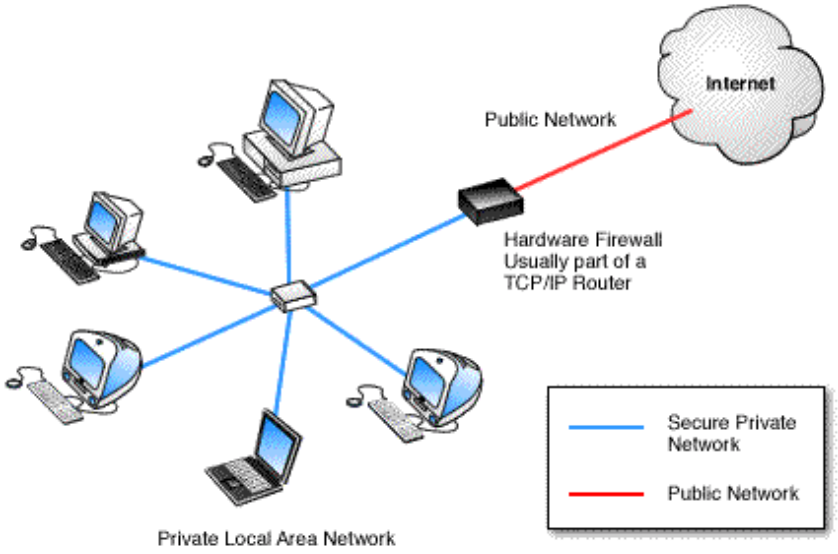
Competitive Landscape

There are three main players in the PKI market. Entrust is the clear leader in software product revenue, providing an integrated PKI and authorization software solution. Its products enable secure communications and transactions in extranets and intranets. Verisign is the clear leader in Certificate Authority services. It provides full offerings needed in Internet transactions, including digital certificates, authorization, payment processing, time stamping, and domain name registration. Baltimore Technologies offers similar solutions to Entrust, and has been gaining market share recently. The wildcard is RSA, which is new to the PKI space and may be able to leverage its brand name and encryption technology to become a formidable player in this sub-market.

C. Perimeter-Based Security Market

1. Firewalls

Firewalls are the bedrock of Internet security – their role is well described by their name. A firewall protects networked computers from a hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It may be a hardware device or a software program running on a secure host computer. A firewall sits at the gateway between two networks, usually a private network and a public network such as the Internet. The earliest firewalls were simply routers. Here is an example of a typical hardware firewall.[2]



[2] SANS Institute

Firewalls fall into three broad categories: packet filters, application level gateways, and stateful multilayer inspection firewalls. A description of each follows:

1. Packet filtering firewalls are usually part of a router. Each packet is compared to a set of criteria at the network level before it is forwarded. Depending on the packet and the criteria, the firewall can drop the packet, forward it, or send a message to the originator. Rules can include a source and destination IP address, a source and destination port number, and the protocol used. The advantage of packet filtering firewalls is their low cost and low impact on network performance.
2. Application level gateways, also called proxies, offer a high level of security, but have a significant impact on network performance. This is because each entire packet is inspected at the application level. Proxies are not transparent to end-users and require the manual configuration of each client computer.
3. Stateful multilayer inspection firewalls combine the aspects of the other types of firewalls. They filter packets at the network layer, determine whether session packets are legitimate, and evaluate the contents of packets at the application layer. Stateful multilayer inspection firewalls offer a high level of security, good performance, and transparency to end-users. They are expensive, however, and, due to their complexity, potentially less secure than simpler types of firewalls if not administered by highly competent personnel.

Market Analysis

The firewall market has grown steadily over the last several years due to the need for front-end security. This growth has been driven by an increase in the number of networks and thus a need for firewalls. Also, companies are installing more and more firewalls in their network. It is typical for a large company to have one hundred firewalls in its network. According to Bear Stearns estimates, firewall software revenue reached $1.2 billion in 2000 and could reach over $3 billion in 2005.

Firewalls have evolved in the last decade. They were originally designed to simply block all external traffic from entering a network. Now, firewalls are expected to provide intelligent access control and be an all-in-one security solution. Recently, this demand has caused the nascent firewall appliance market to boom.

Firewall Appliances

Like other firewall systems, firewall appliances protect an internal network from an external network, but that is where the similarity ends. Firewall appliances are self-contained, stand-alone devices. They usually work in conjunction with enterprise firewalls to protect a smaller sub-network. As these appliances continue to evolve, they also become increasingly more functional, offering VPN support, content filtering, load balancing, anti-virus protection, and PKI encryption. In addition to all these functionalities, firewall appliances are simpler, more scalable, easier to manage, and higher in performance than other firewall systems.

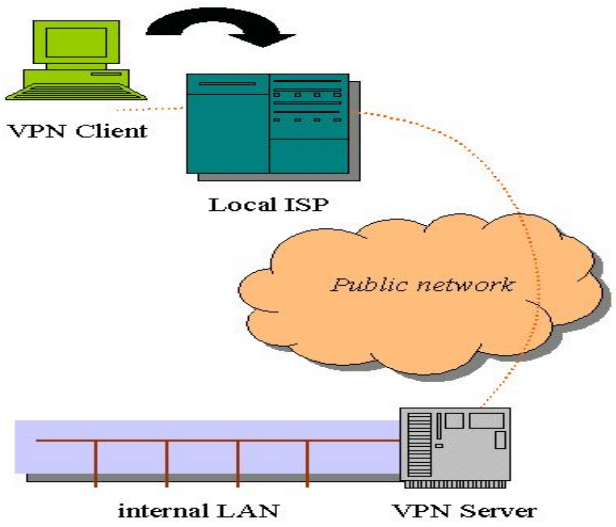
Competitive Landscape

In the enterprise firewall software market, Checkpoint is clearly the market leader with Computer Associates, Microsoft, and Network Associates a distant second. In the security appliance sector, SonicWall is the industry leader with a 39 percent market share, while other players such as Cisco, WatchGuard, NetScreen, and Nokia also enjoy a large piece of this growing market.

2. Virtual Private Networks (VPNs)

A virtual private network (VPN) is essentially a private connection between two machines or networks over a shared or public network. In practical terms, VPN technology lets an organization securely extend its network services over the Internet to remote users, branch offices, and partner companies. In other words, VPNs turn the Internet into a simulated private WAN.

VPNs do this by using a process called tunneling. Instead of crossing the Internet out in the open, data packets are first encrypted for security, and then encapsulated in an IP package by the VPN before being tunneled through the Internet. A VPN uses a combination of authentication, tunneling, access control, and encryption technology. The following shows a basic VPN configuration.



Market Analysis

Analysts have been saying for years that VPNs are the next “big thing.” With companies becoming more global, more employees working from home, and all parties in the value chain utilizing the Internet, VPNs would seem to be an ideal solution for remote-access needs. In addition, the weak economy serves as another factor that may spur growth in this market, as VPN players claim to save companies money by eliminating the costs of the leased lines between remote locations. This large potential market has attracted over 50 companies to enter the industry, each of them offering a variety of VPN solutions and possibly emerging as the dominant leader.

The main reason VPNs have yet to gain widespread acceptance is the confusion among customers. Historically, “bleeding-edge” VPN products came with implementation and management issues that offset the cost-savings that fuel VPN growth. While the technology has improved, customers are now confused by the overwhelming amount of choices, none of which are proven.

For VPNs to become a successful networking solution, VPN providers must focus on four features:

1. *Security* – This is a given in the VPN space. Any company that does not meet the basic security requirements will not survive. A differentiating factor will be offering additional services, such as support for PKI.

2. *Manageability* – This has been VPNs' Achilles' heel since the technology came into existence. The majority of customers require simple installation, configuration, and user management.
3. *Scalability* – Customers do not want to invest in a networking solution that can only support a certain number of users. Extranets seem to find a way to multiply and VPNs need to be able to multiply in conjunction with them.
4. *Performance* – Perhaps the least important of the four characteristics, faster performance becomes a strong selling point when all of the other traits meet or exceed customer requirements.

VPNs are often linked with firewalls, not because they are the same, but because VPN users must enter and exit through firewalls. There are firewall vendors that do not have VPN solutions and vice versa, but companies now want to buy both technologies from one vendor. It is important that they are interoperable.

Competitive Landscape

There are dozens of companies targeting various segments of the VPN market, including service providers, gateway vendors, firewall vendors, and equipment providers. Companies like Cisco and Nortel may control the service provider network. Check Point and SonicWALL currently sell end-to-end VPN solutions. As for service providers, players include Fiber Link, MCI, and AT&T. There are many small companies in the gateway provider space, including Fortress, NetScreen, and RedCreek. We expect larger companies to acquire some of these smaller outfits to offer end-to-end solutions. This trend can already be seen through the Cisco and Efficient Networks acquisitions in this space.

D. Authentication and Authorization Market

Authentication

There are basically three different ways to authenticate users:

1. *Through something users know* – Passwords
2. *Through something users have* – Tokens and Smart Cards
3. *Through something users are* – Biometrics

The four technologies mentioned are described below:

Passwords

Any computer user is familiar with the most basic form of authentication, passwords. This provides the lowest level of security. As more and more systems are deployed, a user may generate several passwords and the level of security required by a company becomes higher than that which authentication can provide. The problems with passwords are that they are often forgotten, stolen, or figured out by potential intruders. Several companies now offer products that enhance passwords, such as tokens, smart cards, or biometrics.

Tokens

Tokens are small devices the size of a credit card that display a constantly changing ID code. A user first enters a password and then the card displays an ID that can be used to log into a network. Tokens add a high level of security because the user has to physically possess the token in order to gain access to the network. The problem with tokens is the potential to lose the token. The industry leader in tokens is RSA with its SecurID product.

Smart Cards

Smart cards are small electronic devices about the size of a credit card that contain electronic memory, and possibly an embedded integrated circuit (IC). They are used for a variety of purposes, including storing a patient's medical records, storing digital cash, and generating network IDs. While smart card technology has been around for years, it is just beginning to take off in the U.S. Credit card companies are using smart card chips on their cards and large software companies are endorsing smart cards as a key component of secure information.

Smart cards provide many benefits over other alternatives, including ease-of-use, durability, and simplicity. They are cheaper to implement than biometric authentication. Although they do not provide the same amount of security, they do satisfy the requirements for commercial uses, such as building authorization, phone cards, and identification.

Biometrics

Biometrics refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked. Examples include computer analysis of fingerprints, retinal scans, and speech. Though the field is still in its infancy, many people believe that biometrics will play a critical role in future computers, and especially in electronic commerce. Personal computers of the future might include a fingerprint scanner on which you could place your index finger. The computer would analyze your fingerprint to determine who you are and, based on your identity, authorize different levels of access.

The advantage over other authentication methods is that a physical ID cannot be lost or stolen. But biometrics' strength is also its weakness. Unlike a stolen password, biometric data cannot be altered. Thus, if biometric data is compromised, it has lost its security. Since biometrics is still in its infant state, there is no dominant leader in the industry. Some of the players include AuthenTec, Precise Biometrics, and UniSecurity.

Authorization

Authorization is usually blended in with authentication, but they are two separate sub-markets that work in conjunction. Most computer security systems are based on a two-step process. The first stage is authentication, which ensures that a user is who he or she claims to be. The second stage is authorization, which allows the user access to various resources based on the user's identity. According to IDC estimates, authentication and authorization together represent nearly a $3 billion industry and are predicted to surpass $7 billion in 2004. Combined, they create not only one of the largest sectors of the security market, but with a 28 percent CAGR, one of the fastest growing ones.

There are generally three subsectors of authorization: Secure Portal Management (SPM), Access Management, and Web Access Control. SPM provides shared services for the authentication, authorization, and personalization of portals. The players include Netegrity, IBM, Oblix, Securant, and Entrust. Access Management provides the back-end integration that controls many types of network resources. It works in conjunction with SPM. The leaders of this market include Cylink, IBM, Vasco, and Secure Computing. Web Access Control solutions allow companies to manage productivity, protect themselves against fraud, and prevent illegal activities. Companies in this space include SurfControl, Symantec, Unisys, and Ubizen. Currently, all three sub-sectors are far from maturity and have room for dozens of companies. Any one of these may emerge as the dominant market leader several years from now.

One of the latest buzzwords in the industry is single sign-on (SSO) because of the significant return on investment (ROI) the technology offers companies. The proliferation of network systems has resulted in multiple usernames, passwords, and access levels – a daunting amount of information for security systems to track. Companies need to properly authenticate the users as well as grant access to the authorized data and applications. SSO solutions make this easier by integrating user sign-on functions and user account management functions. They typically collect user credential and identification information when the user first signs on and check for the correct credentials when accessed later.

1. Digital Rights Management (DRM)

Digital Rights Management (DRM) gained publicity through the Napster case, which popularized the concern that copyrighted content may be illegally distributed. DRM is a type of server software developed to enable secure distribution and disable the illegal distribution of paid content over the Web. Although copyright laws protect online content, policing the Web is impossible. DRM technology focuses on making it impossible to steal Web content in the first place.

With this type of technology, it is hard to believe that it is not ubiquitous. There are two main reasons DRM has not become prevalent. First, the owners of the content have not reached a consensus on how to price their product. Should a downloaded song be charged by the amount of times it is listened to or by a flat rate for the download itself? These are the types of questions facing content providers. The second reason is customer-focused. If there are too many restrictions on the material, it may become an annoyance and deter users from embracing the content.

DRM is still in its infancy. We are at least a year or two away from broad adoption. Some say it is impossible to stop the distribution of material in the Internet age. While this is a definite possibility, we feel there will be an explosion in this market at some point depending on when more businesses start selling copyrighted content online. The more content a business puts online, the more a business will want to protect its content. Both the businesses and the users will see the economic benefits of gaining access to more content and will deal with the security issues accordingly.

E. Antivirus Market

Antivirus software is the only segment of the network security market to gain widespread acceptance in both the enterprise and consumer markets. This is indicative of the potential dangers of viruses. We have all heard of the Code Red, Melissa, and ILOVEYOU viruses, which have paralyzed the networks of major companies around the world.

Antivirus software is a class of programs that search your hard drive, floppy disks, or e-mail for any known or potential viruses. For simplicity's sake, a virus is defined as a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event, and is often designed to automatically spread to other computer users. The market for antivirus software has expanded because of Internet growth and the increasing use of the Internet by businesses concerned about protecting their computer assets.

Antivirus software serves three primary functions:

1. *Detection* – It determines when a virus is present and where it is located on the system.
2. *Identification* – After a virus is detected, it is compared to a database of known viruses to determine the type and name of the destructive code.
3. *Removal* – It removes the virus so that it does not harm the system.

Most antivirus software blocks the virus by scanning for its signature, which is located in the scanning engine database. As new viruses are created, more signatures are added to the database, requiring the antivirus software to be updated, as well. The next generation of antivirus software, known as heuristic or generic detection software, sifts through files to search for codes that display similarities to other known viruses. Because of the number of constantly mutating viruses, this will be an improvement over current methods.

Market Analysis

While antivirus software has been around since the invention of the disk drive, it is far from antiquated. In fact, it is one market that can expect to see constant growth. According to IDC estimates, the antivirus market should grow at a CAGR of over 15 percent per year, from $1.4 billion in 2000 to over $2.7 billion in 2005. The reason for this growth in such a mature industry is the creation of new and more dangerous viruses. About 150 to 200 viruses are created each month, making regular updates to antivirus software a necessity. There is also the new possibility of wireless viruses, which may pose a serious threat in the near future.

Competitive Landscape

There are large barriers to entry in the antivirus market because a large customer base is required. The top four companies (Network Associates, Symantec, Computer Associates, and Trend Micro) own close to 90 percent of the market. All of these companies offer similar antivirus protection, but are differentiated by their administrative tools.

F. Intrusion Detection Market and Vulnerability Assessment Market

Intrusion detection systems (IDS) are perceived as the next layer of defense after the firewall in a corporate network. They monitor packets on the network wire and attempt to discover if a hacker is attempting to break into a system (or cause a denial-of-service attack). A typical example is a system that watches for a large number of TCP connection requests to many different ports on one specific machine. It can preempt denial-of-service attacks that have attracted major headlines for bringing sites such as Amazon.com and Yahoo down.

There are two types of intrusion detection systems: those that are network-based and host-based. In a host-based system, a specific machine watches its own traffic (usually integrated with the server stack and services themselves). In a network-based system, an independent machine simultaneously watches all of the network traffic (that of the hub, router, and probe). Note that a network-based system monitors many machines, whereas a host-based system monitors only a single machine (the one it is installed on).

There are two main requirements for an IDS solution. First, it must perform at network speeds so that it does not slow down network traffic. Second, it must have a comprehensive and current database of attack signatures. This is similar to antivirus software, where an old database will allow newer viruses to wreak havoc.

Also included in this section is vulnerability assessment, which is often uttered in the same breath as IDS, but is slightly different. Vulnerability analysis is a preventive measure deployed by an organization in order to detect any deficiencies in the security structure. While an IDS analyzes a network in real-time, vulnerability assessment products examine log files and configurations in the network to determine if there are certain setups that pose a potential security risk.

Limitations

Intrusion detection systems do not provide real-time prevention of attacks. In addition, increasing evidence shows that IDS products have limited detection capabilities and inherent difficulties properly identifying attack attempts. As a result, many attacks are left undetected and false alarms are sometimes generated. The major drawbacks of IDS follow:

1. Intrusion detection systems cannot prevent attacks in real-time. They listen to packets on the wire, but do not block their transfer. More often than not, the packet reaches its destination and is processed prior to interpretation by the IDS. As a result, it is common for an attack to be successful before it is identified by the IDS.
2. Intrusion detection systems cannot detect unknown attacks. Any signature-based system can only handle signatures that exist in the product database.
3. Intrusion detection systems create a false sense of security. A company should never be too comfortable with its security system. As mentioned previously, attacks may go undetected because a virus is not in the database or because the data is encrypted.

Competitive Landscape

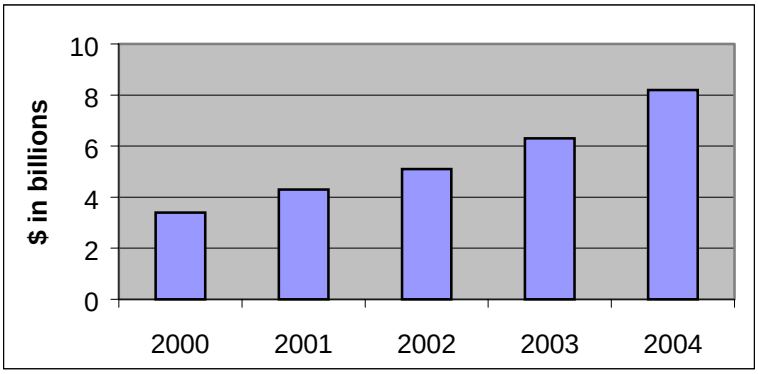
The competition becomes increasingly intense in this industry as more companies try to offer a fully integrated security solution. This trend can be seen through the rapid consolidation of players in the last 12 months. These transactions include the Symantec acquisition of Axent, the Cabletron acquisition of Network Security Wizards, and the ISS acquisition of Network ICE. ISS is still the leader in the combined intrusion detection and vulnerability assessment market, though the combination of Network and ICE may prove to be a formidable one. In vulnerability assessment alone, BindView is the market leader.

G. Services Market

Undoubtedly, implementing and administering a complete security solution is a large task for any organization. In the past, companies have deployed the best security systems that were available at the time. But times have changed. The attacks have evolved, the types of defenses have multiplied, and the potential for loss has increased. Comprehensive security policies and multi-faceted technology solutions are required to secure valuable assets. Yet, as no one vendor dominates all areas of security, there is mass confusion among IT managers about how to implement such solutions. Security requires constant vigilance and industry specialists – it is becoming a responsibility that a typical network administrator cannot handle. These factors have contributed to the emergence of security services.

Security services do not receive as many headlines as hardware or software, but the sector is a large part of the security market. Services represent approximately 50 percent of the security spending market, garnering $3.4 billion in revenue in 2000. According to IDC estimates, that number is expected to grow at a CAGR of 24.2 percent, reaching over $8 billion in 2004. Although, this growth-rate is slightly lower than the rate of the entire security industry, it still represents over 45 percent of the spending in 2004.

Security Services Spending Estimates[3]



1. Managed Security Services

There are many factors driving the growth of the security management market. First, as intruders become savvier, IT managers need to react more quickly. Centralized management solutions that collect, monitor, and respond to events allow a company to accomplish this goal. In addition, the multitude of security products makes interoperability a challenge. Companies often choose a best-of-breed approach rather than purchase a suite of products from one vendor, because they are unwilling to compromise security for a uniform product. This, however, requires additional management.

Outsourcing the security management function to an outside vendor is the future for both large and small organizations. With large organizations, it is critical that any security breaches be monitored, understood, and responded to in real-time. Such a security solution is often too complicated for in-house IT staff to manage. This has already been seen in network management, which is often outsourced because of the same reasons. Smaller firms are even more likely to use managed security services because of the large investment in security products that would otherwise need to be made. A comparison can be drawn to Web-hosting companies that enable small outfits to minimize capital expenditures and back-end monitoring so that they can focus on growing their business.

Those who outsource their security management function can often anticipate a tremendous return on investment. Companies can save money by reducing staff and cutting installation and maintenance costs associated with deploying security hardware and software. The demand for these services will continue to rise as service providers establish themselves and as clients become more comfortable outsourcing this important function to a third party. According to the Yankee Group, the MSS market will grow to nearly $1.7 billion by 2005, up from $140 million in 2000.

Market Analysis

In the last two years, over 100 MSS companies have popped up to provide outsourced security services. A close look at the funding shows that MSS has dominated the recent private equity investments in the security sector. Yet the MSS business model has yet to be proven. Almost none of the players in this space are profitable and potential customers are still wary of outsourcing such an important function to a company that has only been around for two years or less.

[3] IDC estimates

As companies prove themselves, they will gain momentum, emerging as leaders in this crowded space. Some of the differentiating factors will include cutting-edge detection capabilities, filtering technologies, back-end forensics, and response capabilities. There will undoubtedly be consolidation in this industry once funding begins to slow down and companies are forced to merge or be acquired to survive. Although MSS is a service, it is not people-intensive and thus scales well. MSS will eventually become a commodity once the pretenders are weeded out of the market. The key to success will be efficiency, measured by the number of people per device and revenue dollars per device.

Competitive Landscape

This is probably the most fragmented sub-market in the security industry. Outside the company ISS, this market is filled with relatively small private companies. This is not to say that ISS dominates managed security. Although venture capital funding has been limited overall, companies in this sector have been receiving their fair share. Each of these new companies offers a unique area of expertise. RipTech offers a complete, collaborative services solution. Open Service targets corporate IT departments. NetForensics is well suited for Cisco environments.

While this sub-market is continuing to evolve, our prediction is that there will be a shakeout. The many smaller players will be forced to merge and sell themselves to a larger company, possibly a traditional network manager such as IBM, HP, or Micromuse. It will also be interesting what ISS does in this space. It already has a firm foot in the door but may need to bolster its offerings by acquiring or merging with one of the smaller players.

2. Other Services

Although managed security services have received most of the attention in the services space, there are other sectors that will play a large role in security and also warrant consideration. There is no standardized way to segment this sector, but three broad elements include security consulting, security implementation, and security training. These are not mutually exclusive and service companies may perform one or all of the service elements.

Security consulting includes an enterprise-wide assessment of a customer's vulnerabilities and policies to assist in determining the client's overall state of preparedness. Security implementation is the act of installing, configuring, and integrating a customer's firewall and then testing the firewall to ensure proper protection. Security knowledge transfer is the formal or informal process by which information is passed from the service company to the customer.

There are several aspects of security services including strategy, privacy, policy and standards, risk assessment, attack and penetration testing, architectural design review, implementation, and education and training. This is not an exhaustive list and the range and level of services is constantly increasing. Consultants may provide some or all of these services to a company, including MSS.

Market Analysis

The "other services" market is very similar to MSS. It is a fragmented market with no dominant leader. There are hundreds of companies that occupy a niche in this market, many of which have been around for less than two years. We predict that consolidation will occur in the near future as companies try to expand their current capabilities and reach critical mass. Meanwhile, software companies are becoming more hybrid, leveraging their software expertise to provide services, as well.

We expect that software companies will also acquire service companies with a solid customer base and revenue stream.

H. Wireless Security Market

Wireless is one of the fastest growing areas in technology. According to the Strategis Group, the number of professional mobile data users in the United States is upwards of 32 million, and growing. Ericsson predicts that there will be approximately 600 million mobile Internet subscribers worldwide by 2004. With the number of wireless devices in use, hackers no longer need to physically tap into a line; they can steal information through the air without anyone knowing.

Wireless security is not that different from wired security. In security, you authenticate the person you are talking to, secure the data as it travels from the handheld device to the destination host, and ensure that the traffic has not been altered en route. However, wireless has some unique difficulties, such as limited bandwidth, high latency, and unstable connections. Wireless implementations must be smaller and simpler, due to wireless terminal technology, and faster, due to wireless network limitations. There is no one wireless security solution. Rather, solutions utilize all the areas of security previously mentioned:

1. *Encryption* – The information transmitted over the wireless connection from terminal to base station will most likely be encrypted through standard digital transmission protocols. It is also important that this data remain encrypted as it travels through the network from the base station to whichever server it must go to. Encryption from end-to-end (terminal-to-server) maintains confidentiality at all stages of transport.
2. *PKI* – Public key infrastructure provides a trusted system for verifying digital signatures. All carriers of digital signatures agree to trust the authority of the public key registrars. This is the cornerstone of maintaining a secure transaction environment. The merchant and the customer need a common basis for trusting each other's digital signatures.
3. *Authentication* – Once the confidential information arrives at the server, it needs to be authenticated. Authentication is required to identify the user, to authorize the user to complete the transaction, and to verify that the data that has come in is actually valid.
4. *Digital Signatures* – For authentication, both the user and the server must use some sort of digital key to ensure that the parties are authorized and trusted members of a transaction. This allows the server or the user to repudiate any invalid interaction before it happens. Before a secure purchase can be initiated, the user must be verified and the merchant must be certified.

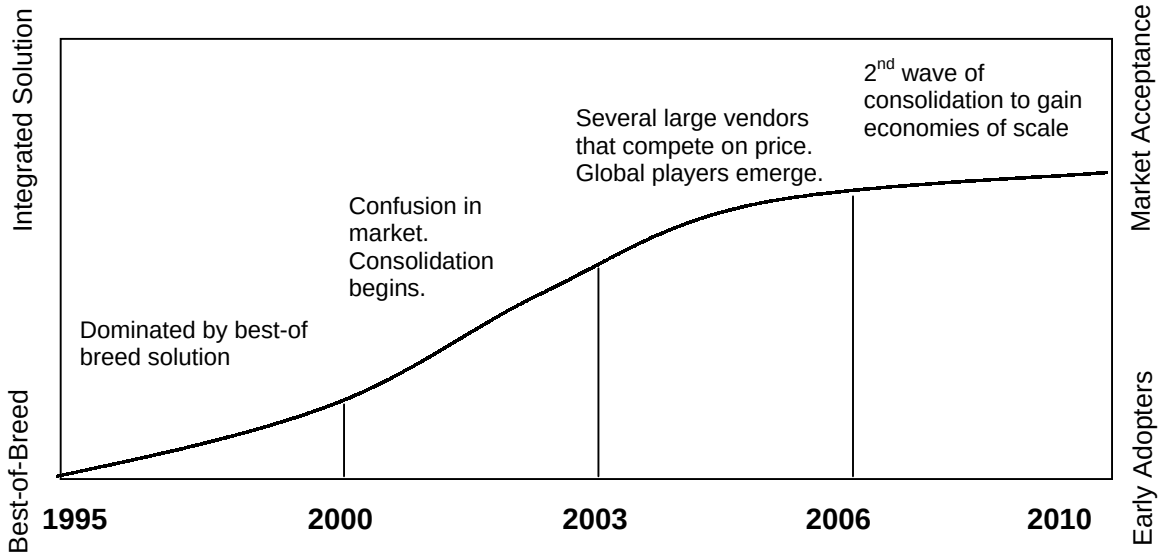
Competitive Landscape

Although wireless security serves the same purpose as network security, there are limitations that make wireless security more complicated. Physical limitations include limited battery life, limited memory, and unstable connections. Two of the major players in wireless security are Certicom and NTRU, although the sector is filled with both large and small niche players. Because of the fragmentation of the sector, wireless consulting companies play a large role in putting all the pieces together.

V. Conclusion

A. 2001 and Beyond

The following is a graph showing the evolution of the Internet security industry. From 1995 (or even earlier) to the year 2000, the security industry was dominated by best-of-breed solutions. As the industry progressed to the point where it is today, the number of companies in this space has ballooned to a point where customers are confused with what product is best for their needs. In the past 12 months, consolidation has already begun and should continue for the next few years, as companies seek to expand their suite of products and offer an end-to-end security solution. Eventually, there will be a few large players that dominate the industry, and then further consolidate to gain economies of scale.



The second evolutionary stage has lasted longer that expected. Just a year or two ago, many thought that security would become a mature industry within a few years, especially considering the investments and the attention given to the industry. But, in fact, what we have seen are companies not meeting customer needs, thus opening the door for smaller players to establish a foothold in the industry. The current market can best be described as extremely fragmented. Companies will continue to fight to achieve critical mass and vie to become king of the security market.

However, security solutions still have a long way to go before complete market acceptance. Here's why:

1. First, there is an ever-growing need for security services managers. As the variety of choices and the complexity of the products increase, it becomes increasingly difficult for companies to manage security in-house. Instead, businesses are turning outward for help.
2. Second, security solutions need to be interoperable and scalable. A corporate network is in a constant state of flux and security systems need to change in conjunction with the network. Since companies choose best-of-breed products, those products need to be able to work with each other. In addition, as a network grows, there is a need for more probes and firewalls, opening up new loopholes in the network. For example, it is not uncommon for a developer to put test machines in the network. If not properly secured, it serves as an entry point into the system.

3. Third, application security needs to improve. Ask any IT manager what he or she fears more, external or internal attacks, and the answer will be clear: internal attacks. So much emphasis and so many resources have been dedicated to fortifying the outer perimeter, but little has been done to protect mission-critical applications and data.

There is no doubt that the previous problems will be addressed and new problems will arrive, such as the recent issue of individual privacy. Through the use of new and advanced technologies, people are exchanging or releasing even more information that can potentially be accessed by intruders. While users enjoy customized services, for example, the convenience may come at the price of privacy. There are already technologies out there that can track individuals within a few feet if the person is carrying a wireless device. The passage of HIPAA mandates strict confidentiality of the online medical records that have raised security concerns. There are products that monitor every mouse click and Web site you visit. With all these potential "invasions" of privacy, security solution will play a role in protecting your identity.

The year 2004 will present another interesting situation as cable television pipes become open for competitive use, as mandated by the OpenCable consortium. This will increase the need to safeguard public switched telephone networks and video media over cable networks. In addition, security will become even more important as hackers attempt to get free cable and phone calls.

Another area that is ripe for growth is biometrics. Biometric security vendors have been trying to make the leap from science fiction to enterprise functionality for years. With the most recent developments, they may soon reach their goal. Banks, healthcare providers, and government agencies are increasingly turning to iris scanners, voice recognition software, and fingerprint scanners as simple and cost-effective means of securing networks against attackers and forgetful employees. The potential for this market is difficult to predict due to privacy issues.

VI. Security Company Profiles

A. Application Security

Private Companies

Entercept Security Technologies — Application Security
www.entercept.com — San Jose, California

Entercept™ Security Technologies is dedicated to providing award-winning products that deliver superior security. The company's patented technology provides companies with a security solution that stops hackers from penetrating Internet servers, Web servers, and Web applications. Since the introduction of its security solutions, Entercept™ has received awards and praise from both technology analysts and the press. Most recently, the company's server security product, Entercept™, won the InfoWorld "Technology of the Year Business Impact Award." Entercept™ is quickly becoming a standard for server security and is the only security solution that proactively protects e-business servers, Web servers, and Web applications from known and unknown security breaches.

KaVaDo, Inc. — Application Security
www.kavado.com — New York, New York

KaVaDo is an application-layer, security-solutions company dedicated to protecting the applications that make business on the Web possible. The company's patent-pending technology is the first in a new breed of safeguards designed to protect each application individually, delivering comprehensive and adaptable security against known and emerging threats. The highly scalable platform requires minimal installation effort and can accommodate numerous applications, making it a long-term solution for growing businesses.

Tripwire, Inc. — Application Security
www.tripwire.com — Portland, Oregon

Tripwire is the leading provider of data and network integrity (DNI) solutions and assures the integrity of "data at rest" at all points in a network. The company's software is one of the most widely deployed and trusted DNI solutions in the world. Today's Tripwire software provides the most comprehensive prevention, detection, and recovery capabilities available. In addition, Tripwire solutions provide a platform and a foundation for an organization's security, network management, and risk management architecture. Tripwire software has earned the trust of the world's leading organizations such as Lloyd's of London. Lloyd's recently entered into an agreement with Tripwire that provides a ten percent premium discount to clients of Lloyd's e-Comprehensive cyber insurance policy who have properly deployed Tripwire software on their systems.

Public Companies

BindView — Application
www.bindview.com — Houston, Texas

BindView Development Corp. provides software solutions that enhance business performance by helping to ensure the integrity of the information technology infrastructure. Its two core product suites are its bv-Admin and bv-Control lines. The bv-Admin software is a comprehensive directory and systems administration solution for effective security and efficient migration that helps organizations proactively manage the transition from Windows NT, Exchange 5.5, and Novell environments to Windows 2000, Active Directory, and Exchange 2000 environments.

Bv-Control software offers a complete security and configuration management solution for protecting complex and distributed enterprises by providing in-depth security and administrative analysis to mission-critical systems enterprise-wide. More than 10 million licenses of the company's solutions have been shipped worldwide to approximately 5,000 companies.

Market Cap – $68.3 million NASD: BVEW
FY 2000 Sales – $86.1 million
FY 2000 Net Income – $(3.8) million

Computer Associates Application
www.ca.com Islandia, New York

Computer Associates International Inc. is an e-business software company. The company's solutions address all aspects of e-business process management, information management, and infrastructure management in six focus areas: enterprise management, e-business security, e-business storage, e-business transformation and integration, portal and knowledge management, and predictive analysis and visualization. With its portfolio of software products and a professional services organization dedicated to understanding the needs of its customers, the company is committed to meeting the technology requirements of e-businesses in every sector of the economy. The company's global business is principally in a single industry segment: the design, development, marketing, licensing, and support of integrated computer software products operating on a diverse range of hardware platforms and operating systems.

Computer Associates' security component is delivered through eTrust, a security suite designed to protect against malicious attacks. Security Integrity Solutions (SIS) covers a series of assessments that analyze your organization's current level of protection and recommends means to further safeguard information assets. These include base lining, risk assessment, and penetration study. The other aspects of eTrusts' end-to-end solution include intrusion detection, policy compliance, access control, and single sign-on.

Market Cap – $20.2 billion NASD: CA
FY 2000 Sales – $4.2 billion
FY 2000 Net Income – $(591) million

B. Authentication and Authorization Market and Digital Rights Management

Private Companies

Arcot Systems, Inc. Authentication
www.arcot.com Santa Clara, California

Arcot Systems is the leading provider of authentication and access control solutions for securing e-business in Internet-scale and wireless environments. The company is responding to the e-business market demand for solutions that secure the deployment of higher-value services with a "frictionless" end-user experience. Arcot Systems is meeting this demand with a new Internet-class of solutions based on architectures that scale for the Internet, while delivering the ease-of-use and economies of Web solutions. The company offers a complete, affordable solution for strong authentication of users and transactions that deliver smart card-level security with all the cost and implementation benefits of a software-only solution.

Authentica — Digital Rights Management
www.authentica.com — Waltham, Massachusetts

Authentica is the premier provider of information security software that allows enterprises to protect and actively control intellectual property and sensitive digital information after it's distributed across the Internet. Based on the company's patented Active Rights Management technology, Authentica's Recall™ product suite provides real-time control and management of digital information. Users can expire content; establish whether recipients have the right to forward, print, or copy information; and track the availability of information no matter where it is located. Authentica's customers include large manufacturers, law firms, government agencies, and pharmaceutical companies.

CertCo — Authentication/Authorization
www.certco.com — New York, New York

CertCo's vision extends beyond technology to assure the creation of e-business solutions that manage risk as a critical business process. To that end, the company has developed the first complete technology and business solution that allows individual companies to build the trustworthy infrastructures needed to support large-scale, globally secure e-businesses. CertCo's customers include corporations, financial institutions, online exchanges, and governments. They rely on the company for its one-source business solutions, which allow them to safely conduct and complete high-value transactions over open networks with trading partners anywhere in the world.

Oblix — Authentication/Authorization
www.oblix.com — Cupertino, California

Oblix enables companies to secure and manage e-business. The Oblix model enables administrators to delegate the management of each element of information to the user who is most knowledgeable about it. Oblix solutions provide the security infrastructure for complex enterprise environments. Its customer services will get e-businesses up and running quickly and securely. An extensive partnership network ensures smooth integration into any e-business infrastructure. Its market-proven Web access management solution, Oblix NetPoint, provides global enterprises with a unified security infrastructure that scales with growing e-businesses. Global companies such as Amdahl, i2 Technologies, Charles Schwab & Co., Norsk Hydro, National Australia Bank, and Xerox have relied on Oblix solutions for their leading-edge e-business networks.

Reciprocal, Inc. — Digital Rights Management
www.reciprocal.com — New York, New York

Reciprocal provides transaction-processing services that deliver e-commerce to all kinds of digital content providers, ensuring product security as well as an enjoyable customer experience. Since 1996, the company has focused its business on Digital Rights Management solutions and enabling content owners to maximize d-commerce in the following areas: global coverage, multiple platform capabilities, multiple types of digital content, strategic consulting, and end-to-end outsourcing solutions.

Securify, Inc. Authentication/Authorization
www.securify.com Mountain View, California

Securify is a leading provider of cost-effective, e-Security technologies and solutions. The company combines its own unique technology and expert services to provide customers with the ability to achieve business objectives and maximize their network security investments. Securify offers two complementary suites of solutions SecurVantage and Access Management Services.

SecurVantage is a cost-effective service that provides security metrics for managing the overall quality of security in business networks, enabling decreased operating costs and improved efficiency of security efforts. SecurVantage manages security across Intranets as well as between e-business partners by providing visibility into network traffic, device operation, applications, and processes that impact network security. With patent-pending technology and a range of security services, SecurVantage is flexible and is customized for each unique network environment.

Securify Access Management services make it easier for companies to implement cost-effective authentication and access management solutions. The company provides vendor-neutral recommendations to organizations on leading-edge security technologies such as PKI, smart cards, and access control products. Securify will act as an advocate through the selection and implementation of authentication and access management systems. The company's expert consultants have extensive expertise and can help identify the best security solution to suit its customers' business applications, requirements, and budget.

Veridicom, Inc. Authentication/Authorization
www.veridicom.com Santa Clara, California

Veridicom was created to take state-of-the-art technologies first developed at Lucent/Bell Labs and turn them into products that enable simple, authenticated Web access, e-commerce, user privacy, and business security. The company has taken powerful fingerprint sensor and imaging algorithm technologies and turned them into personal authentication products that enable e-business to be conducted securely. Veridicom's solutions replace PINs and passwords with personal authentication based on individual fingerprints, which provide dramatically stronger security.

VIGILANTe Authentication/Authorization/IDS
www.vigilante.com Melville, New York

VIGILANTe specializes in providing security assurance through assessment. Its offerings include SecureScan™, which identifies potential security vulnerabilities around a network's Internet perimeter, and SecureScan™ NX, which detects vulnerabilities within the network. Both solutions encapsulate the company's core experience and expertise in automated security testing.

VIGILANTe's philosophy revolves around the concept that true security consists of assessing the network, determining acceptable risk, and prescribing corrective action where necessary. With that in mind, VIGILANTe operates under the guiding principle that impartiality is crucial to winning the trust of its business partners and, ultimately, its clients. Therefore, it does not sell hardware or software, security-related or otherwise.

VIGILANTe understands that marketing firewalls while providing services to find holes in firewalls could lead to conflicts of interest. Its tests culminate in the recommendation of actions, not products. Accordingly, it leaves decisions about product selection in the hands of its clients or its business partners.

Public Companies

RSA Security, Inc. — Authentication
www.rsasecurity.com — Bedford, Massachusetts

RSA Security, the most trusted name in e-security, helps organizations build secure, trusted foundations for e-business through its two-factor authentication, encryption, and public key management systems. As the global integration of Security Dynamics and RSA Data Security, RSA Security has the market reach, proven leadership, and unrivaled technical and systems experience to address the changing security needs of e-business and bring trust to the new, online economy.

A truly global company with more than 5,000 customers, RSA Security is renowned for providing technologies that help organizations conduct e-business with confidence. The company's RSA SecurID enterprise authentication products are protecting information in the majority of the Fortune 100 companies today, addressing the important need for easy, hacker-proof user authentication both inside and outside the corporate network. These same products are similarly used by leading e-commerce businesses, including securities trading and banking applications, to protect against external attacks and fraudulent activity. The company's RSA BSAFE line of encryption-based security technologies are embedded in over 450 million copies of today's most successful Internet applications, including Web browsers, commerce servers, e-mail systems, and virtual private network products. The majority of todays secure electronic commerce transactions and communications on the Internet are conducted using RSA Security technologies. Both RSA SecurID and RSA BSAFE are considered de facto standards worldwide.

RSA Security now offers its customers the RSA Keon family of PKI products, a solution for enabling, managing, and simplifying the public key authentication and encryption security in today's leading e-mail, Web browser, Web server, and VPN applications. Elements of RSA Keon are available on an OEM basis to allow application designers to build many core RSA Keon benefits into new applications, and other options are available to adapt existing, installed applications to gain RSA Keon security and management benefits. RSA Keon is the first product to combine the expertise of the entire company, from public key technology to large-system scalability and management.

Market Cap – $1.4 billion — NASD: RSAS
FY 2000 Sales – $280.2 million
FY 2000 Net Income – $205.8 million

VASCO Data Security International, Inc. — Authentication, Authorization
www.vasco.com — Oakbrook Terrace, Illinois

VASCO designs, develops, markets, and supports security products and services, which manage and secure access to computer systems of corporate and governmental clients. The company's Digipass product line provides greater flexibility and more affordable options than competing products authenticating users on any network, including the Internet. The Digipass family of user-authentication devices, all of which incorporate an electronic digital signature capability to guarantee the integrity of electronic transactions and data transmissions, are commonly referred to as security tokens.

The company's SnareWorks product line provides enterprise-wide solutions to secure Internet, client/server, and mainframe applications.

Market Cap – $59.6 million NASD: VDSI
FY 2000 Sales – $28.1 million
FY 2000 Net Income – $(4.2) million

C. Encryption

Private Companies

NTRU Encryption
www.ntru.com Burlington, Massachusetts

NTRU, a critical enabling technology for emerging digital infrastructures, delivers the fastest and smallest public key cryptography solutions for wireless services, such as m-commerce, streaming media, interactive banking, and mobile enterprise applications. The company is based on a fundamental mathematical innovation, which for the first time makes efficient public key cryptography practical on a scale necessary for consumer and embedded applications. Supporting a wide range of devices in wired and wireless environments, NTRU delivers strong security for any application, while eliminating traditional speed, size, cost, and security tradeoffs. NTRU operates at speeds up to 2,000 times faster than alternatives, while using as little as 1/50 the footprint, and enables new security paradigms impractical with older cryptography technology, bringing security to a new breed of connected consumer devices and highly scalable servers.

SSP Solutions Encryption
www.bizssp.com Irvine, California

SSP Solutions is a leading provider of authentication and encryption security technology and a developer of Internet security solutions. The SSP Solution empowers a secure Internet for e-commerce, communications, and network access while protecting the integrity of digital transmissions and stored data. Combining a wide range of technologies and intellectual properties, SSP develops custom-made solutions for the digital economy, including: digital rights management, financial services, government, entertainment, healthcare, and education.

Public Companies

Baltimore Technologies Encryption
www.baltimore.com Needham Heights, Massachusetts

Baltimore Technologies develops and markets security products and services to enable companies to develop trusted, secure systems for e-business, the Internet, and mobile commerce. The company's offerings include a wide range of PKI products and hosting services, wireless e-security solutions, cryptographic toolkits, security applications, and hardware cryptographic devices. Baltimore Technologies' global professional services organization offers a wide variety of consulting, training, and deployment support to its customers worldwide. The company markets and sells its solutions worldwide directly and also through the TrustedWorld channel program, which includes many of the world's leading technology companies and a wide variety of global, regional, and local business alliance partners.

Cap – $194.1 million NASD: BALT
FY 2000 Sales – $126.3 million
FY 2000 Net Income – $(224) million

Certicom Corp. Encryption
www.certicom.com Hayward, California

Certicom is an encryption technology company specializing in security solutions for mobile computing and wireless data markets, including mobile e-commerce, or mobile commerce. The company's product line includes cryptographic toolkits, information security protocol toolkits, and PKI products. Certicom announced certificate authority (CA) services and a VPN client application, both available later this year. In addition to licensing its security products, the company provides consulting and systems integration services to assist its customers in designing and implementing efficient security solutions. Certicom's customers incorporate its patented technology into their applications for handheld computers, mobile phones, two-way pagers, and other Internet information appliances.

Market Cap – $46.9 million NASD: CERT
FY 2000 Sales – $12 million
FY 2000 Net Income – $(17.9) million

Cylink Corporation Encryption
www.cylink.com Santa Clara, California

Cylink develops, markets, and supports a comprehensive family of secure e-business solutions. The company's cryptographically based products provide a secure, flexible, and easily managed solution for expanding its customers' businesses. Cylink creates trust in customers' networks by securing the access, privacy, and integrity of information when it is transmitted over their LANs, as well as globally over WANs and public networks, such as the Internet. These solutions enable the company's customers to merge their operations and transactions systems with their existing networks, maximize their use, reduce the costs of their operations, and expand their businesses. The company's customers include Fortune 500 companies, multi-national financial institutions, and agencies within the United States government.

Market Cap – $17.3 million NASD: CYLK
FY 2000 Sales – $68.1 million
FY 2000 Net Income – $(35.4) million

D. Intrusion Detection and Vulnerability Assessment

Private Companies

Asta Networks Intrusion Detection System
www.astanetworks.com Seattle, Washington

Asta Networks develops software and services that increase the reliability, predictability and manageability of networks. This is done through a distributed, scalable system that bridges the gap between network providers and their customers to provide insight into, and control over, network traffic. The company's initial product is the first proven solution to automatically detect and respond to denial-of-service attacks. Worldwide leaders in the fields of distributed networking, security, and Internet reliability founded Asta Networks.

Captus Networks — Intrusion Detection System
www.captusnetworks.com — Woodland, California

Captus Networks designs and manufactures network security devices that provide immediate and automatic protection from denial-of-service and distributed denial-of-service attacks. The CaptIO™ protects networks and systems from the crippling effects of these attacks, allowing only legitimate traffic to traverse an e-commerce company's mission-critical network. The primary mission of the company is to provide network security solutions for the e-business economy.

Intellitactics — Intrusion Detection System
www.itactics.com — Kitchener, Ontario, Canada

Intellitactics is a leading innovator of security management software solutions. The company's sophisticated information security technology allows corporations to take a proactive approach to protecting their mission-critical assets. Intellitactics developed two critical platforms for enterprise security management. The first product disseminates and enforces policies and procedures within large enterprises. The second product integrates the monitoring and analysis of events from network, system, and disparate security devices.

nCircle Network Security, Inc. — Intrusion Detection System
www.ncircle.com — Emeryville, California

nCircle develops and offers innovative, intelligent, and adaptive network security solutions. The recent integration of nCircle technology and services into the IP360 System forms a unique architecture that completely envelops and protects networks. The components share intelligence learned throughout the cycle to provide highly efficient, highly accurate network security.

nCircle's IP360 is the first comprehensive, automated security solution that provides true, continuous network protection. Installed at nCircle's Secure Operations Center (SOC) as well as on the customer's network, IP360 incorporates hardware, software, and service components that work in concert to provide true wire speed intrusion detection and intrusion prevention. IP360 continuously scans the network to map its configuration and detect potential vulnerabilities. The intrusion detection system knows when an attack poses an actual threat, because it is integrated with the scanning sensors, giving IP360 the unique ability to all but eliminate false alarms.

netForensics.com — Intrusion Detection System
www.netforensics.com — Edison, New Jersey

netForensics.com, a spin-off from NetCom Systems, Inc., is a security information management (SIM) company focused on providing valuable and actionable information to support security management, operations, architecture, and reporting. The company's Web-based security information management (SIM) platform provides cross-device relationship analysis between security devices. By integrating industry-leading point-solutions, netForensics.com provides an extensive view of all security events in a centralized environment with an easy-to-use interface and multidimensional reporting features.

Network ICE — Intrusion Detection System
www.networkice.com — San Mateo, California

Network ICE offers advanced, third-generation global intrusion detection and protection for enterprise customers who understand the significance of “Zero Tolerance” infrastructure security. The company goes beyond traditional second-generation, discrete IDS techniques that can only approximate true security due to reliance on failure-prone, pattern-matching algorithms and patchwork coverage. The BlackICE Global-IDS product family blankets an entire infrastructure, including remote sites and workers, at every point of potential compromise by using a patent-pending Active Protocol™ protection technique that can deliver up to 10 times the protection of any other IDS system, regardless of network complexity or speed.

NFR Security, Inc. — Intrusion Detection System
www.nfr.com — Rockville, Maryland

NFR's mission is to provide customers with best-of-breed solutions for detecting attacks, misuses, and anomalies associated with their IT resources. The company’s intrusion detection portfolio encompasses networks, host-servers, and workstations. Products include NFR Network Intrusion Detection (NID) and NFR Secure Log Repository (SLR), which are offered through an extensive worldwide network of channel partners. NFR's technology direction is to offer a comprehensive portfolio that protects all IT resources by providing both reactive and proactive intrusion detection.

NIKSUN, Inc. — Intrusion Detection System
www.niksun.com — Monmouth Junction, New Jersey

NIKSUN is the recognized worldwide leader in developing and deploying a complete range of network performance monitoring, security surveillance, and forensic analysis tools serving a wide range of protocols and interfaces, ranging from Ethernet and Gigabit Ethernet to OC-3. The company’s products are the only network appliances that continuously capture and analyze LAN, MAN, and WAN traffic at Gigabit rates in a single platform. NIKSUN's product line delivers unprecedented flexibility, scalability, and real-time response. The company's patent-pending, real-time data analysis and recording technology enables enterprises, ASPs, ISPs, and carriers to provide secure and reliable network infrastructures and services.

PentaSafe Security Technologies, Inc. — Intrusion Detection System
www.pentasafe.com — Houston, Texas

PentaSafe Security Technologies helps companies safely grow their businesses by providing complete security policy and infrastructure solutions that address security from a people, policy, and technology perspective. The company offers security solutions for companies of all sizes. Its services include policy management, auditing, vulnerability assessment, host-based intrusion detection, and best-practice security publications. Additionally, PentaSafe offers security management solutions for operating systems, databases, Web servers, firewalls, and applications including Windows 2000/NT, AS/400 or iSeries, UNIX, NetWare, JDEdwards WorldSoftware, Microsoft IIS, Apache, iPlanet, BEA WebLogic, CheckPoint FireWall-1, Cisco's NetRanger, Oracle, Sybase, and SQL.

Qualys — Intrusion Detection System
www.qualys.com — Sunnyvale, California

Qualys' flagship service, QualysGuard, is a security auditing service that continuously detects Internet network vulnerabilities, assesses the severity risk of each vulnerability, and provides alerts in a summarized graphical report. While other security monitoring products require companies to buy, develop, and manage solutions internally, QualysGuard is easy to implement and provides immediate and continuous security auditing and risk assessment of a company's network. QualysGuard provides comprehensive, on-demand security audits that identify, analyze, and report on network security threats. By focusing on networks from a "hacker's eye view" perspective, Qualys identifies real-world weaknesses that would elude traditional security solutions.

Recourse Technologies, Inc. — Intrusion Detection System
www.recourse.com — Redwood City, California

Recourse Technologies™ is the leading provider of threat management solutions that contain, control, and respond to malicious computer attacks, enabling secure and uninterrupted business operations. The company's threat-management products, including ManHunt™ and ManTrap®, can protect large, complex networks from a wide range of threats. Manhunt, the first comprehensive threat management system, goes beyond existing intrusion detection techniques to provide a scalable and effective solution for detecting, analyzing, and responding to attacks. ManTrap®, the industry's leading secure detection system based on honeypot technology, provides a realistic and flexible environment in which to catch and identify both internal and external security threats.

SHYM Technology — Intrusion Detection System
www.shym.com — Needham, Massachusetts

SHYM Technology produces plug-in security and trust management solutions for a company's critical business applications. The company quickly and cost-effectively delivers new levels of security, authentication, and assurance to e-business applications. SHYM works with leading vendors, including VeriSign, Entrust, Baltimore, Xcert/RSA, Netscape, and Microsoft, as well as leading application makers such as Microsoft, IBM/Lotus, SAP, PeopleSoft, and Eudora.

Public Companies

Internet Security Systems, Inc. — Intrusion Detection System
www.iss.net — Atlanta, Georgia

Internet Security Systems is a global provider of security management solutions that protect digital business assets. The company's continuous-lifecycle approach to information security protects distributed computing environments, such as internal corporate networks, inter-company networks, and electronic commerce environments, from attacks, misuse, and security policy violations, while ensuring the confidentiality, privacy, integrity, and availability of proprietary information. The company delivers an end-to-end security management solution through its SAFEsuite platform of software products, its around-the-clock remote security monitoring, and its professional services, comprised of both consulting and education services.

As of year-end 2000, the company's lifecycle security management solutions protected more than 8,000 customers worldwide. The company also has established strategic relationships with companies including BellSouth, Check Point, GTE, IBM, MCI WorldCom (Embratel), Microsoft, and Nokia to enable worldwide distribution of its core monitoring technology.

Market Cap – $963.5 million NASD: ISSX
FY 2000 Sales – $195 million
FY 2000 Net Income – $18.3 million

Websense Intrusion Detection System
www.websense.com San Diego, California

Websense, Inc. provides employee Internet management products that enable businesses to monitor, report, and manage how their employees use the Internet. The company's primary product, Websense Enterprise, gives businesses the ability to rapidly implement and configure Internet access policies in support of their efforts to improve employee productivity, conserve network bandwidth, and mitigate potential legal liability. The company's flexible and easy-to-use software applications operate in conjunction with its proprietary database, which is available for daily incremental downloads.

Market Cap – $313.6 million NASD: WBSN
FY 2000 Sales – $17.4 million
FY 2000 Net Income – $(5.9) million

E. Perimeter-Based Security (Firewalls and VPNs)

Private Companies

Asita Technologies, Inc. VPN
www.asitatechnologies.com Irvine, California

Asita Technologies provides high-speed, high-performance VPN solutions that integrate firewalls, networking, policy routing, load balancing and a network management system into a single network device. The Asita LineSpeed product range features hardware based encryption that ensures true wire speed performance and delivers the highest level of security for international standards (IPSec using 3DES-CBC mode). The Asita LineSpeed is scalable and flexible, and also easy to configure and manage. The Asita LineSpeed family is based on one of the world’s fastest multi-functional cryptographic accelerator chips. The chip features a true random number generator supporting key generation, a secure key store, and tamper-proof circuitry for ultimate security even during power down mode.

Gilian Technologies, Inc. Firewall Appliance
www.gilian.com Redwood Shores, California

Gilian Technologies is a global technology leader in Web security, protecting companies against the critical epidemic of Web site vandalism and sabotage. The company’s G-Server is an exit control solution that keeps Web sites accurate and available regardless of the origin of a security breach. Gilian’s solution saves time and money, while preserving the reputation of customers, including industry leaders in banking, finance, publishing, media, retailing, and technology.

Top Layer Networks Inc. Firewall/IDS
www.toplayer.com Westboro, Massachusetts

Top Layer Networks designs and produces security hardware and software products that thwart a wide range of network threats, including denial-of-service floods and criminal intrusions into corporate systems. The Company's ASIC-based security devices orchestrate and strengthen critical security features surrounding firewall and intrusion detection system functionalities. Companies using the AppSwitch™ and AppSafe™ from the AS 3500 family of security products, along with Top Layer's custom security software modules, dramatically increase the efficiency of their network defenses and have access to detailed network information that is otherwise unattainable.

Public Companies

Check Point Software Technologies Ltd. Firewall/VPN
www.checkpoint.com Ramat Gan, Israel

Check Point develops, markets, and supports Internet security solutions for enterprise networks and service providers (Telcos, ISPs, ASPs and MSPs). Its solutions include VPNs, firewalls, intranet and extranet security, and Managed Service Providers (MSP). The company delivers solutions that enable secure, reliable, and manageable B2B communications over any IP network – including the Internet, intranets, and extranets. Check Point product offerings also include traffic control/quality of service (QoS) and IP address management. Check Point products are fully integrated as a part of the company's Secure Virtual Network (SVN) architecture and provide centralized management, distributed deployment, and comprehensive policy administration. The capabilities of Check Point products can be extended with the Open Platform for Security (OPSEC), enabling integration with best-of-breed hardware, security applications, and enterprise software applications.

Check Point's product lines offer a broad range of policy-based solutions for securing and managing networks. The company's security product line includes its FireWall-1 family of products, its VPN-1 family of virtual private networking solutions, and some associated products. The company's traffic control product line includes its FloodGate-1 bandwidth management solution. The management product line includes Meta IP address management solutions.

Market Cap – $9.2 billion NASD: CHKP
FY 2000 Sales – $425.3 million
FY 2000 Net Income – $221.2 million

Network Associates, Inc. Antivirus
www.nai.com Santa Clara, California

Networks Associates is a supplier of security and availability solutions for e-business. The company's products focus on two important areas of e-business: network security and network management. The majority of the company's revenue has historically been derived from its McAfee anti-virus product group and its Sniffer network availability and performance management product group. These two flagship product groups form the customer base and product base from which the balance of the company's product line has developed.

Market Cap – $1.5 billion NASD: NETA
FY 2000 Sales – $745.7 million
FY 2000 Net Income – $(124) million

SonicWALL, Inc. Firewall Appliance
www.sonicwall.com Sunnyvale, California

SonicWALL designs, develops, and manufactures a complete line of Internet security solutions that provide access security, security services, and transaction security for small, medium, and large enterprises. The company's Internet security appliances have a worldwide installed base of more than 117,000 units. By integrating its line of high-performance, solid-state firewalls with value-added security services, such as network antivirus systems, virtual private networking (VPN), strong authentication using digital certificates, and content filtering, SonicWALL Internet security appliances deliver complete security solutions.

SonicWALL continues to extend its leadership position in security solutions with the acquisition in Q4, 2000 of Phobos Corporation, a leader in secure transaction and high-availability technologies. These products, now part of the SonicWALL family of security solutions, include secure transaction accelerators and load balancers. Together, secure transaction accelerators and load balancers deliver speed, reliability, and high availability to enterprises, e-commerce outfits, and service providers.

Market Cap – $1.3 billion NASD: SNWL
FY 2000 Sales – $69.5 million
FY 2000 Net Income – $8.8 million

Symantec Corporation Antivirus/IDS/MSS
www.symantec.com Cupertino, California

Symantec is a world leader in Internet security technology, providing a broad range of content and network security solutions to individuals and enterprises. The company is a leading provider of virus protection, vulnerability assessment, intrusion prevention, Internet content and e-mail filtering, remote management technologies, and security services to enterprises around the world. Symantec's Norton brand of consumer security products leads the market in worldwide retail sales and industry awards. The company has worldwide operations in 37 countries.

Market Cap – $3.3 billion NASD: SYMC
FY 2001 Sales – $853.6 million
FY 2001 Net Income – $63.9 million

WatchGuard Technologies, Inc. Firewall Appliance
www.watchguard.com Seattle, Washington

WatchGuard Technologies is a provider of Internet security solutions designed to protect enterprises that use the Internet for electronic commerce and secure communications. Thousands of large and small companies worldwide use the company's products and services, which include firewalls for access control, VPNs for secure communications, and the ServerLock products for server content and application security. The company's core market includes small to mid-sized enterprises (SMEs); large, Internet-distributed enterprises (IDEs) with ultra-high-speed connections that support VPNs between the IDEs and their geographically dispersed branch offices and telecommuters; small and home offices (SOHOs) with broadband connections; and telecommuters.

Market Cap – $269.1 million NASD: WGRD
FY 2000 Sales – $60.7 million
FY 2000 Net Income – $(15.7) million

Public Key Infrastructure (PKI)
Public Companies

Entrust, Inc. PKI
www.entrust.com Plano, Texas

Entrust, formerly known as Entrust Technologies, Inc., is a global provider of PKI products and services to e-businesses and other organizations. The company's solution is a comprehensive, end-to-end PKI framework designed to assure the security of electronic transactions and communications over advanced networks, including the Internet. Its open, scalable software solution operates across multiple platforms, network devices, and applications. The products that constitute the core of the company's PKI solution include Entrust/Authority, Entrust/RA, Entrust/AutoRA, Entrust/Roaming, Entrust/Timestamp, and Entrust Electronic Identities.

The company's PKI infrastructure comprises software that manages and administers life cycles of keys and digital certificates throughout an organization and across multiple applications. The PKI infrastructure also includes a directory compliant with the lightweight directory access protocol (LDAP) for the storage and retrieval of certificates and software that enable applications and users to access the functionality provided by the PKI. The company's software supports a wide variety of encryption algorithms, including RSA, as well as symmetric and hashing algorithms, allowing customers to select those algorithms best-suited for their requirements.

Market Cap – $302.8 million NASD: ENTU
FY 2000 Sales – $148.4 million
FY 2000 Net Income – $(79.9) million

VeriSign, Inc. PKI
www.verisign.com Mountain View, California

VeriSign provides infrastructure services to Web site owners, enterprises, e-commerce service providers, and individuals. The company's domain name registration, digital certificate, global registry, and payment services provide the critical Web identity, authentication, and transaction infrastructure that online businesses need to establish their identities and to conduct secure e-commerce and communications. The company's services support businesses and consumers from the moment they establish an Internet presence through the entire lifecycle of e-commerce activities. In May 2001, the company acquired the Internet payment services assets of CyberCash, Inc.

Effective January 1, 2001, the company was organized into two customer-focused lines of business. The mass markets division focuses on delivering all of its products and services to small and medium-size enterprises, as well as to consumers that wish to establish a presence on the Web. The enterprise and service provider division focuses on delivering all of its products and services to larger enterprises and service providers around the world that want to establish and deliver secure Internet-based services to their customers in both B2C and B2B environments.

Market Cap – $10 billion NASD: VRSN
FY 2000 Sales – $474.8 million
FY 2000 Net Income – $(3.2) billion

F. Management Security Services and Other Services

Private Companies

@stake, Inc. — Other Services
www.atstake.com — Cambridge, Massachusetts

@stake offers a comprehensive set of professional services spanning security strategy, design, and implementation. These services prepare large enterprises for the increased risks and rewards of moving their businesses on-line. @stake's technical expertise includes extensive knowledge of secure networks, applications, hardware, and policies. Specialty areas include firewalls, data encryption, digital certificates, intrusion detection systems, digital forensics, wireless devices, and SANs.

AtomicTangerine, Inc. — Other Services
www.atomictangerine.com — Menlo Park, California

AtomicTangerine, a spin-off of SRI International, is a leading worldwide provider of information security services that help companies continuously adapt to the changing risks of the connected economy. The company has a solid record of delivering high-quality, customizable solutions uniquely tailored to each client. No other company offers the depth of security experience, the business focus, and the technical expertise organizations need stay ahead of rapidly evolving business risks, both internal and external. AtomicTangerine provides options for those who want to work with a company that was instrumental in defining and evolving the discipline of information security, and with a staff that includes the founding fathers of the information security profession, as well as today's leading practitioners.

Cigital — Managed Security Services
www.cigital.com — Dulles, Virginia

Cigital is the leading authority on Software Risk Management (SRM) that ensures reliability, safety, and security on essential software. Cigital helps companies identify, analyze, and reduce the risks of software failure. Cigital's uses Cigital Advantage, a methodical approach to full-lifecycle SRM that is grounded in research and proven practice.

Cigital has received numerous awards including: *Inc. Magazine*'s list of the country's 500 fastest-growing companies and Deloitte & Touche's "Technology Fast 500." Cigital is committed to cutting-edge research and technical excellence to solve the problems that affect businesses and to anticipate future areas of trouble.

Counterpane Internet Security — Managed Security Services
www.counterpane.com — Cupertino, California

Counterpane's Managed Security Monitoring (MSM) service monitors and protects corporate networks in cyberspace through the continuous, broad, product-independent, and non-invasive surveillance of the network and the Internet, and also provides an immediate defense against internal and external attacks to information assets. MSM watches a company's entire network, providing a comprehensive view of a company's security in real-time – even when it is constantly changing in the face of new attacks, new threats, new hardware or software, and day-to-day network reconfigurations.

CyberSafe Corporation — Managed Security Services
www.cybersafe.com — Issaquah, Washington

CyberSafe Corporation is a leading provider of e-business security solutions and services. The company's comprehensive portfolio includes security services and software offerings that, when combined, provide a full suite of security solutions. These solutions are designed to meet the needs of the global 1000 marketplace – from managed services to software products that provide a set of infrastructure solutions for transactional security, network and host-based intrusion detection, and strong authentication from the Web to the mainframe.

Cyber Security, Inc. — Managed Security Services
www.cyber-security.com — Chantilly, Virginia

Cyber Security is a security solutions provider, offering a wide range of products and services to meet today and tomorrow's Internet security needs. The company's managed services include: managed firewalls, managed VPNs, intrusion detection systems, antivirus gateways, and vulnerability scanning. The company's professional services include: vulnerability assessments, PKI and consulting services. The company's subscription services include: the Rapid Incident Response Service™, Autoscan, and the Intrusion Protection Service™.

Cyota — Managed Security Services
www.cyota.com — New York, New York

Cyota is an innovative technology company that is dedicated to helping financial institutions strengthen their customer relationships through reliable, flexible, easy-to-use online security, payment, and transaction products. The company develops advanced technology products that can be easily understood, adopted, and used by financial institutions to increase their brand awareness and strengthen cardholder relationships. Current products include Cyota SecureClick™, Cyota SecureMobile™, and Cyota PayMatch™.

DOLFIN.COM, Inc. — Other Services
www.dolfin.com — Manassas, Virginia

DOLFIN.COM is a leader in the field of e-security. The company's focus is to provide a full range of professional services in the five critical areas of a company's secure information architecture: policies and administration, internal and external threats, support systems and business applications, network integrity and architecture, and disaster prevention and recovery. DOLFIN.COM also develops and supports custom security solutions designed to provide comprehensive security to computer networks, Internet-based systems and global computing resources. The company provides e-security services and products to business, government, and institutional customers.

e-Security, Inc. — Managed Security Services
www.esecurityinc.com — Rockledge, Florida

e-Security is a leading provider of security software solutions for today's e-business environment, with deep roots in distributed security management. The company was founded by security professionals with many years of experience in building and managing security systems for Fortune 500 companies.

By researching the market and listening to the concerns of CIO's, security administrators, and network managers, e-Security has introduced the first and only integrated, automated, and centralized security-management system on the market.

Through the Open e-Security Platform™, companies can integrate all sources of security information in their enterprise-wide security environment, enabling them to actually see and respond to network abuse, attacks, or intrusions, as well as identify, assess, and minimize vulnerabilities associated with their security. E-Security is passionately dedicated to providing software solutions that address the crucial security issues that e-businesses face every day in "Internet time."

Foundstone — Managed Security Services
www.foundstone.com — Irvine, California

Foundstone is a provider of managed and professional security assessment services and education. Its consulting services include:

1. Attack and penetration testing
2. E-commerce application testing
3. Incident response/Computer forensics
4. Product testing

Foundstone's Managed Vulnerability Assessment Services use FoundScan technology to footprint a network's infrastructure and regularly evaluate and probe its vulnerabilities. These focused assessments provide a complete, accurate picture of an organization's security posture at any time.

Guardent — Managed Security Services
www.guardent.com — Waltham, Massachusetts

Guardent provides security and privacy programs for Global 2000 organizations. Integrating consulting and managed services, Guardent helps financial services, life sciences, manufacturing, government, and technology clients achieve their business objectives through the use of appropriate security and privacy measures.

NETSEC — Managed Security Service
www.netsec.net — Herndon, Virginia

NETSEC enables secure business by providing comprehensive and thorough proactive management of intrusion detection systems (IDS), firewalls, and virtual private networks (VPNs), offering complete network information assurance and security intelligence 24x7, 365 days a year. Based in part on practices developed for the National Security Agency, NETSEC's methods and its technology are regarded as state-of-the-art by its customers, who include Fortune 1000 companies, international companies, and government agencies. NETSEC is a privately held company headquartered in Herndon, Va., and backed by leading investors, including Softbank Venture Capital and E*Trade Venture Capital.

OneSecure, Inc. Managed Security Services
www.onesecure.com Denver, Colorado

OneSecure is a leading managed security services provider (MSSP) offering customers the only co-managed network security service based on a complete lifecycle approach. The company offers a comprehensive suite of managed security services for businesses including: managed firewall services, managed VPN services, intrusion detection services, vulnerability scanning services, and URL filtering services. OneSecure's co-management system allows customers to retain control of their networks by offering a complete view of their network security information and easy communication with OneSecure's Security Operations Center (SOC). The company's dedicated, certified (CERT), and experienced SOC engineers are focused solely on providing the best network security and incident response 24x7x365.

OpenService, Inc. Managed Security Services
www.open.com Westborough, Massachusetts

OpenService is focused on managing mission-critical, diverse security applications and architectures via software that is fast to implement, easy-to-use, and cost-effective in both purchase price and overall deployment. The company's SystemWatch is the only Web-enabled technology that automates the management of all security applications and appliances within an enterprise. SystemWatch's platform-neutral, intelligent security agents provide the consistency necessary for total coverage. The software's rules-based profile enables it to take corrective action anywhere in the security network, and its patented event reduction and correlation technology manages both custom security applications and commercial software through a Web-based interface.

Ponte Communications Managed Security Services
www.ponte.com Mountain View, California

Ponte provides network security-control software that allows enterprises and managed service providers to centrally control network security policy across all network devices, regardless of vendor or device type. Developed in partnership with a major Wall Street financial services firm, the Ponte nsControl™ platform automates the implementation of security policy through the translation of policy to device configurations, followed by the deployment of configurations, firmware, and passwords to network devices.

Riptech, Inc. Managed Security Services
www.riptech.com Alexandria, Virginia

Riptech, the premier provider of scalable, real-time managed security services, protects clients through advanced, outsourced security monitoring and professional services. The company's unique Caltarian technology platform provides real-time information protection through around-the-clock monitoring, analysis, and response. Riptech offers the only technology capable of processing large volumes of network security data to separate security threats from false-positives in real-time, with carrier-class scalability. Additionally, the company's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response.

Telenisus Corp. Managed Security Services
www.telenisus.com Rolling Meadows, Illinois

Telenisus has quickly advanced to become a leading provider of highly secure and reliable managed Internet infrastructure services that power and protect your Web-reliant business initiatives. The company's WebStructure by Telenisus suite of managed Internet infrastructure services integrate Web hosting, information security, and VPNs and are delivered through the Telenisus Built for e-Business™ platform. Telenisus also provides information protection consulting with the following professional services: application security testing, assessment services, strategy and architecture services, implementation and management services, incident and response planning and support services, and security awareness services.

TruSecure Corporation Managed Security Services
www.trusecure.com Herndon, Virginia

TruSecure® Corporation is a worldwide leader in managed security solutions for Internet-connected organizations. Hundreds of leading companies rely on TruSecure® to help them identify, correct, and continuously manage risks to critical systems and information. The company's cost-effective programs generate improved returns on security investments, and provide the assurance that organizations can confidently and safely pursue their Internet-based initiatives.

TruSecure® Corporation pioneered the security assurance market with its innovative TruSecure® Solutions – comprehensive, multi-disciplined programs that help companies achieve and maintain sound information security using the people and products already in place. TruSecure® Solutions include TruSecure® Enterprise 2001, which helps organizations secure their critical information and systems, and TruSecure® Service Provider 2001, which provides validation of the security posture of ASPs, ISPs, and other managed service providers.

TruSecure® brings its customers an unparalleled body of expertise through its ICSA Labs division – the security industry's central authority for research, intelligence, and product certification for over a decade. The ICSA Labs set performance standards for information security products and certify over 95 percent of the installed base of firewall, antivirus, cryptography, and IPSec products. The ICSA Labs also lead security consortia that provide a forum for intelligence-sharing among the leading vendors of security products.

TruSecure® Publications include input from the leading providers of information, intelligence, and perspective in the Internet security field. *Information Security Magazine*, published monthly by TruSecure® Corporation, is the security industry's leading publication, with more than 49,000 subscribers. The magazine includes in-depth features, case studies, timely news coverage, authoritative commentary, and product reviews authored by recognized experts. *Security Digest* is a bi-weekly e-letter with over 36,000 subscribers, covering breaking news in the information security world.

Vanguard Integrity Professionals — Managed Security Services
www.go2vanguard.com — Las Vegas, Nevada

Vanguard Integrity Professionals is a pioneer and world leader in information security software, services, and solutions. Since 1986, customers have looked to Vanguard as the single-source solution for increased enterprise security through robust software solutions, comprehensive support, in-depth training, expert consulting, security system migrations, and world-class conferences. The company's products and services improve enterprise security, save time and money, reduce human errors, and increase user and help-desk productivity.

Vigilinx — Managed Security Services
www.vigilinx.com — Parsippany, New Jersey

Vigilinx is a security solutions provider that offers unique security solutions to solve specific business problems and reduce security costs. Its approach is vendor neutral, so working with its clients' existing infrastructure is seamless. Some of the products offered by Vigilinx include business security consulting, integration, managed security solutions, and emergency response and forensics. Informing all the work the company does is the Vigilinx Security Intelligence Service (VSIS™) – a product that warns about threats in real-time.

Public Companies

Acxiom — Managed Security Services
www.acxiom.com — Little Rock, Arkansas

Acxiom Corporation is involved in the business of customer data integration and customer recognition infrastructure. This enables businesses to develop and deepen customer relationships by creating a single, accurate view of their customers across the enterprise. Acxiom achieves this by providing customer data integration software, database management services, and premier customer data content through its AbiliTec, Solvitur, and InfoBase products, while also offering a broad range of information technology outsourcing services. The company's products and services enable its clients to use information to improve their business decision-making processes and to effectively manage existing and prospective customer relationships. Acxiom has three business segments: Services, Data and Software Products, and Information Technology (IT) Management.

Market Cap – $984.9 million — NASD: ACXM
FY 2000 Sales – $1,009.9 billion
FY 2000 Net Income – $6.4 million

Predictive Systems, Inc. — Managed Security Services
www.predictive.com — New York, New York

Predictive Systems is an independent, network infrastructure consulting company focused on helping service providers and global enterprises harness the power of network technology. Specifically, the company designs, manages, and secures network and technology infrastructures that continuously deliver measurable business results for its clients. The company uses two complementary approaches to network infrastructure solutions.

The company's consulting services give clients a comprehensive range of offerings that delivers breadth and depth of expertise across six practices. The company delivers managed security services to clients through its global integrity managed services division, which allows clients to outsource their network security needs and which is generally provided on an annual subscription basis.

Market Cap – $104.4 million NASD: PRDS
FY 2000 Sales – $88.3 million
FY 2000 Net Income – $(3.9) million

G. Wireless Security

Public Companies

Avaya, Inc. Wireless Security
www.avaya.com Basking Ridge, New Jersey

Avaya is a provider of communications systems and software for enterprises, including businesses, government agencies, and other organizations. The company offers voice, converged voice and data, customer relationship management, messaging, multi-service networking, and structured cabling products and services. The company supports its customers with comprehensive global service offerings, including remote diagnostics testing of its advanced systems, installation of its products, on-site repair, and maintenance. The company also offers professional services for customer relationship management and unified communications, and value-added services for the outsourcing of messaging and other portions of an enterprise's communications system.

The company was incorporated under the name Lucent EN Corp. in February 2000 as a wholly owned subsidiary of Lucent Technologies Inc. On June 27, 2000, its name was changed to Avaya, Inc. In September 2000, Lucent contributed its enterprise networking business to the company and distributed all of the outstanding shares of the company's capital stock to its shareowners. Prior to this distribution, the company operated as part of Lucent. The company operates in three business segments: communications solutions, services, and connectivity solutions.

Market Cap – $3.7 billion NYSE: AV
FY 2000 Sales – $7.7 billion
FY 2000 Net Income – $(375) million

VII. Technology Primer

Encryption

How Encryption Works:[4]

1. 

A pre hash code is derived mathematically from the message to be sent.

2. 

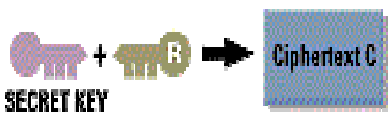
The pre hash code is encrypted using the sender's private key.

3. 

The encrypted pre hash code and the message are encrypted using the secret key.

4. 

The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

5. 

The sender encrypts the secret key with the recipient's public key, so only the recipient can decrypt it with his or her private key.

A cryptographic system uses two keys: a public key known to everyone and a private or secret key known only to the recipient of the message. An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

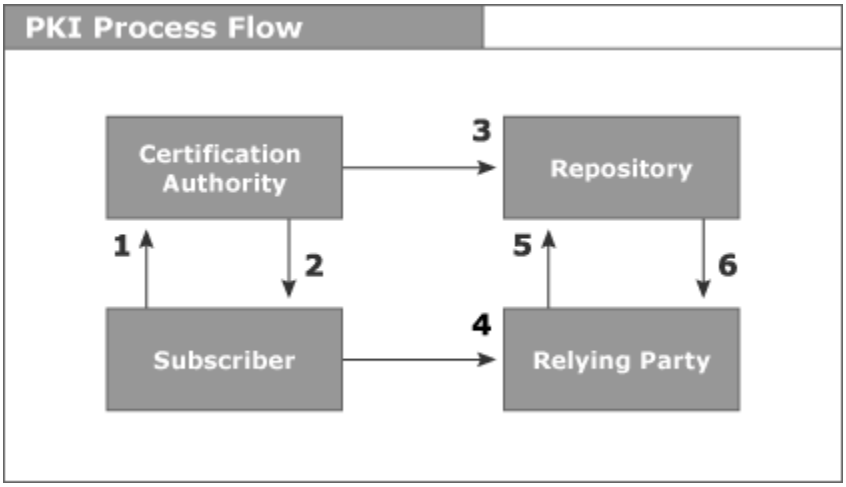
[4] PC Magazine, "How Encryption Works"

Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use. The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her. What's needed, therefore, is a global registry of public keys, which is one of the promises of the new LDAP technology.

Many different types of encryption algorithms are available, but the most widely used are DES, a symmetric or secret key algorithm, and RSA, an asymmetric or public key algorithm. DES can be used with 40- or 56-bit keys. RSA's key lengths are generally anywhere from 512 to 2,048 bits. A more recent algorithm called Triple DES is a stronger version of DES that uses more than one key. S/MIME is an up-and-coming standard for securing e-mail that uses RSA encryption. Microsoft, Netscape, Novell, and Sun all either presently support or have plans to support S/MIME in their messaging systems. This will allow the messaging systems to send secure e-mail to each other. They can also address several desktop e-mail encryption packages, including ConnectSoft's E-Mail Connection, OpenSoft's ExpressMail, and Deming Internet Security's Secure Messenger, support S/MIME.

Public Key Infrastructure (PKI)

How PKI Works:[5]



Step 1. Subscriber applies to Certification Authority (CA) for Digital Certificate.

Step 2. CA verifies identity of Subscriber and issues Digital Certificate.

Step 3. CA publishes Certificate to Repository.

Step 4. Subscriber digitally signs electronic message with Private Key to ensure Sender Authenticity, Message Integrity, and Non-Repudiation and sends to Relying Party.

Step 5. Relying Party receives message, verifies Digital Signature with Subscriber's Public Key, and goes to Repository to check status and validity of Subscriber's Certificate.

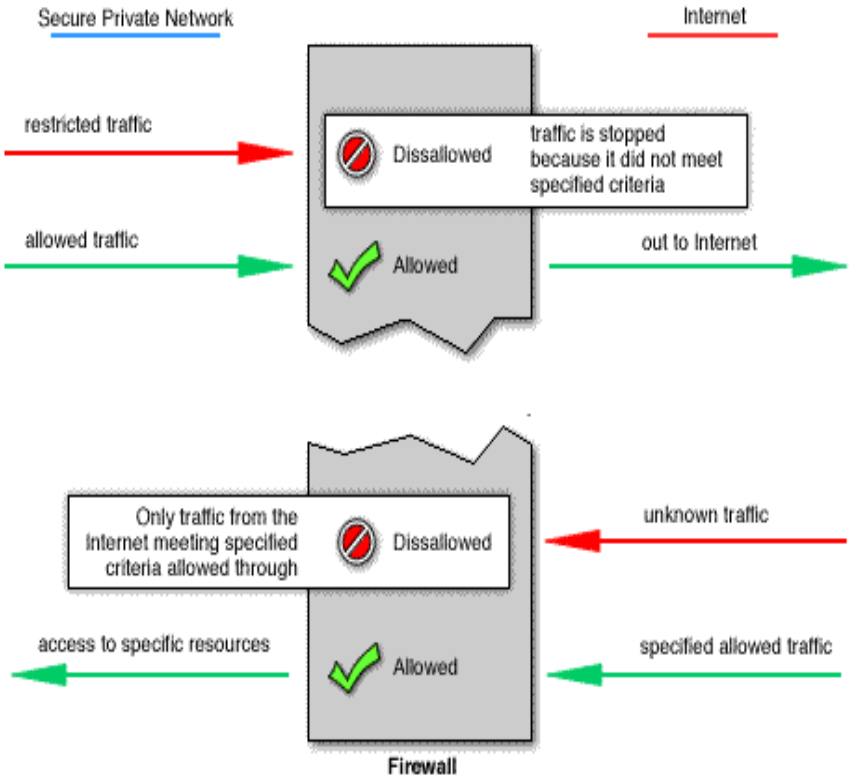
Step 6. Repository returns results of status check on Subscriber's Certificate to Relying Party.

[5] Digital Signature Trust

Firewalls

How does a firewall work?

There are two access denial methodologies used by firewalls. A firewall may allow all traffic through unless it meets certain criteria, or it may deny all traffic unless it meets certain criteria. The type of criteria used to determine whether traffic should be allowed through varies from one type of firewall to another. Firewalls may be concerned with the type of traffic, or with source or destination addresses and ports. They may also use complex rule bases that analyze the application data to determine if the traffic should be allowed through. How a firewall determines what traffic to let through depends on which network layer it operates at. A discussion on network layers and architecture follows.[6]



Packet filters inspect each packet and check it against a set of rules. They can also match each client request with its corresponding server response. Packets that are allowed are passed through unaltered. Application proxy firewalls work at the application layer and, acting as a server, accept packets from a client. The server must run a proxy of the application (HTTP, FTP, or Real Audio, for example) used by the client in order to accept a packet. If the connection is allowed, the firewall then recreates the packet and resends it, acting as a client. It then returns the results to the original requesting client.

[6] Vicomsoft Web site

How Firewalls Handle Packets:[7]

Application proxy and packet filter firewalls inspect packets at the IP layer. Packet filter firewalls also look at the TCP layer. Newer content-scanning servers go deeper still by checking the data portions of packets for viruses and rogue Java and Active X applets.

Firewalls typically ignore most of the data portion of the packet. Some can examine URLs within HTTP or FTP requests. Newer content scanning add-ons look for viruses or misbehaving Java and ActiveX applets within files that are downloaded by users.	Packet filter firewalls use the TCP portion of the packet to identify client-to-server sessions, only allowing server responses to permitted client requests.	Both types of firewalls extract the source address, destination address, and service type from the IP portion of the packet.	Firewalls typically ignore the data link information, though some firewalls use this instead of the IP address to identify local addresses.

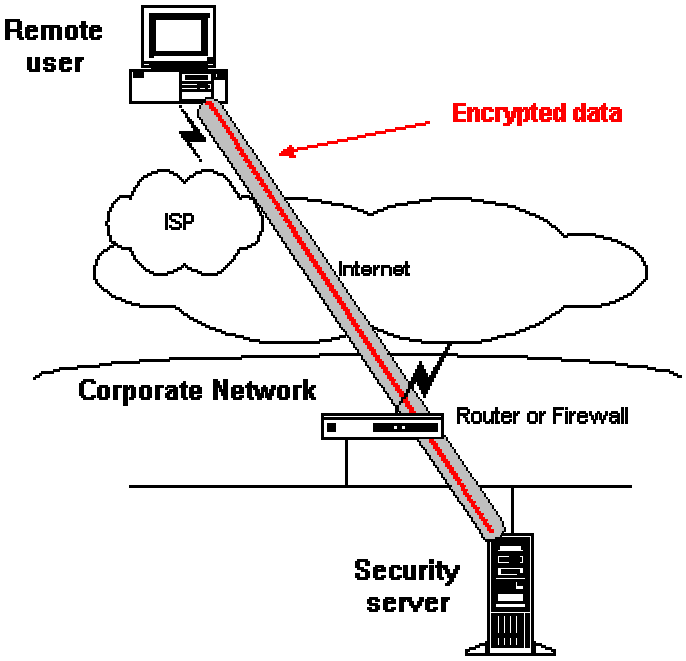
[7] PC Magazine, "How Firewalls Work" by Paul Dwyer, November 18, 1997

Virtual Private Networks (VPNs)

How VPNs work:

The remote user calls the local ISP and connects to the central network over the Internet. When a VPN device receives instructions to transmit a packet over the Internet, it negotiates encryption with the VPN device on the destination network, and encrypts the packet accordingly. Next, it encapsulates the encrypted packet in an IP packet and sends it over the Internet to the destination network. Once the packet arrives, the receiving VPN termination device reverses the process and lets the packet continue to its destination on the internal network.

Two industry standards have recently become interoperable to make remote access and connections over VPNs a viable strategy: Point-to-Point Tunneling protocol and Two Forwarding (L2F), now combined by the IETF to form the Layer Two Tunneling Protocol (L2TP). This standard essentially allows the authentication and authorization process to be forwarded from the ISP to a server located elsewhere on the Internet.

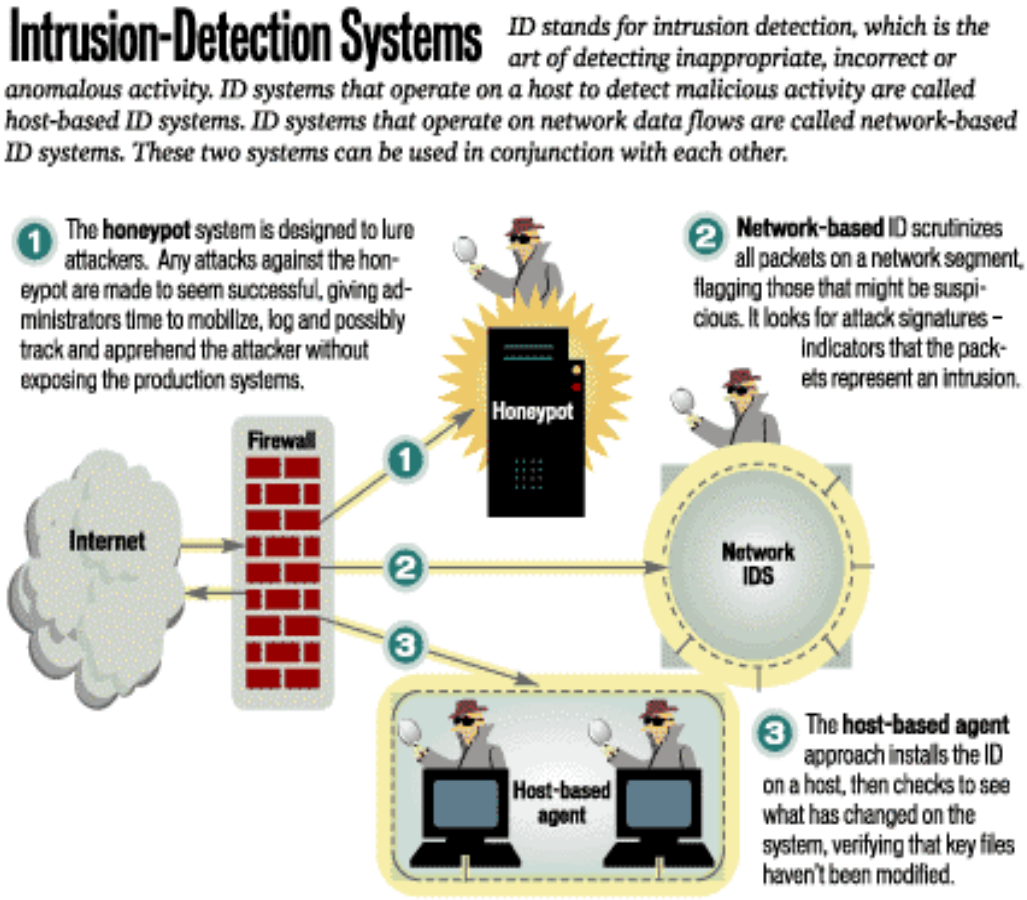


Intrusion Detection Systems

The IDS Solution:[8]

There are 3 steps involved in an IDS:

1. *Assessment* – Just like securing a home, when a security system is put into place, all potential points of vulnerability need to be determined.
2. *Deployment* – After the network is assessed, the next step is to deploy the system.
3. *Monitoring* – Now that the system is working, human factors are important. IT Staff must create a management policy so that the appropriate people find out about potential problems. The IT staff must also monitor logs to properly identify attacks. And lastly, IT staff must react to alerts to limit or prevent damage.



[8] Computer World, "Intrusion Detection" by Peter Loshin, April 16, 2001