

MARKET ANALYSIS

Worldwide Security Software 2004–2008 Forecast: April 2004 Forecast

Brian E. Burke

Charles J. Kolodgy

Christian A. Christiansen

IDC OPINION

2003 was a year of major virus and worm outbreaks, explosive growth in spam, and corporate deadlines for compliance with government regulations. These factors fueled the strong growth of the security software market, and in light of these industry trends and the recovering economy, IDC is providing a top-down estimate of security software revenue for 2003 and an updated forecast for the security software market for 2004–2008. IDC now expects the worldwide revenue for security software to be \$8.05 billion in 2003. The market is now forecast to increase to \$16 billion in 2008, a 14.7% compound annual growth rate (CAGR) for the period from 2003 through 2008. Important trends in the security software market include the following:

- ☒ Organizations continue to look for 3A vendors that provide reduced complexity and cost through consolidation of identity information from across the enterprise, such as preferences, policies, and processes. To provide a more comprehensive solution, security 3A vendors are quickly repositioning themselves as identity management vendors.
- ☒ 2003 was a very busy year for antivirus vendors. SoBig, Slammer, Nachi, Bugbear, and Blaster wreaked havoc on consumer and corporate users alike. The attacks in 2003 were a mix of worms that targeted known vulnerabilities and traditional mass-mailing viruses.
- ☒ Spam has become a major driver for messaging security implementation. Many vendors in the SCM market have developed, partnered with, or acquired an antispam technology. Internet service providers (ISPs) and antispam solution vendors report that spam currently represents 45–80% of all inbound Internet email, way up from 2002 levels closer to 15–30%.
- ☒ Firewalls are quickly becoming the key application where centralized security policy is enforced. Increasingly, firewalls are tightly integrated with other security software, such as antivirus, intrusion detection, intrusion prevention, anti-denial of service, and access control.
- ☒ Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and various SEC regulations have caused unprecedented pressure on corporations to secure customer information. These regulations are forcing companies to meet minimum levels of security for their systems and the information in their databases.

TABLE OF CONTENTS

	P
In This Study	1
Methodology	1
Security Software Market Definition	2
Situation Overview	5
Security 3A Software	5
Secure Content Management Software	7
Firewall/VPN Software	9
Intrusion Detection and Vulnerability Assessment Software	10
Future Outlook	13
Forecast and Assumptions	13
Essential Guidance	21
Secure Content Management	21
Intrusion Detection and Vulnerability Assessment	22
Firewall/VPN	23
Security 3A	23
Learn More	24
Related Research	24

LIST OF TABLES

P

- 1 Worldwide Security Software Revenue by Market Segment, 2003–2008 14
- 2 Worldwide Security Software Revenue by Region and Operating Environment, 2003–2008 15
- 3 Key Forecast Assumptions for the Worldwide Security Software Market, 2004–2008 16

LIST OF FIGURES

	P
1 Worldwide Security Software Revenue by Region, 2003 and 2008	20
2 Worldwide Security Software Revenue by Operating Environment, 2003 and 2008.....	21

IN THIS STUDY

This study provides a top-down sizing of the security software market in 2003 and a 2004–2008 forecast for this market. Historical and forecast revenue data is shown for the total worldwide market and by geographic region and operating environment. This study does not contain vendor-specific revenue, market shares, or vendor profiles, all of which will be published in a separate study in 2Q04.

Methodology

The software revenue forecasts presented in this study represent IDC's best estimates and projections based on the following:

- ☒ Reported and observed trends and financial activity in 2003 as of the end of January 2004, including reported revenue data for public companies trading on North American stock exchanges (1Q03–3Q03 in nearly all cases, plus 4Q03 where available)
- ☒ Additional modeling to fill in any information gaps using a top-down/market-level approach to estimate overall 2003 market sizing
- ☒ Bottom-up regional forecast growth rates provided by IDC analysts in each geographic region

Bottom-up/company-level data collection began in March 2004 with in-depth vendor surveys and analysis to develop detailed 2003 company models by market, geographic region, and operating environment. This activity will form the basis of vendor share, updated forecast, and competitive analysis studies that will appear later in the year.

The IDC Software Research Group (SRG) market sizing and forecasts are presented in terms of "packaged software revenue." Packaged software is defined as programs or codesets of any type commercially available through sale, lease, or rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately as software maintenance. Upgrades may be included in the continuing right of use or may be priced separately.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license but *includes* the implicit value of software included in a service that offers software functionality by a different pricing scheme (e.g., the implicit or stated value of software included in an application service provider's [ASP's] or other hosted software arrangement). It is the total packaged software revenue that is further allocated to markets, geographic areas, and operating environments.

In addition, please note the following:

- ☒ The information contained in this study was derived from the IDC Software Market Forecaster database as of March 9, 2004.
- ☒ All numbers in this document may not be exact due to rounding.
- ☒ For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2004* (IDC #30838, February 2004).

Security Software Market Definition

Secure Content Management

Secure content management (SCM) is a market that reflects corporate customers' need for policy-based Internet management tools that manage Web content, messaging security, virus protection, and malicious code. SCM is a superset of three specific product areas:

- ☒ **Antivirus software.** This identifies and/or eliminates harmful software and macros. Antivirus software scans hard drives, email attachments, floppy disks, Web pages, and other types of electronic traffic (e.g., instant messages and short message service [SMS]) for any known or potential viruses, malicious code, or Trojan horses.
- ☒ **Web filtering software.** This is used to screen and exclude from access or availability Web pages that are deemed objectionable or not business related. Web filtering is used by corporations to enforce corporate policy as well as by schools and universities and home computer owners (for parental controls).
- ☒ **Messaging security software.** This is used to monitor, filter, and/or block messages from different messaging applications (e.g., email, instant messaging, SMS, and peer to peer) containing spam, confidential company information, and objectionable content. Messaging security is also used by certain industries to enforce compliance with privacy regulations (e.g., HIPAA, Gramm-Leach-Bliley, and SEC) by monitoring electronic messages for compliance violations. This market also includes secure email.

Firewall/VPN Software

The firewall/virtual private network (VPN) market consists of software that identifies and blocks access to certain applications and data. These products may also include VPN encryption as an option. Software firewalls fall into two distinct categories: enterprise and personal. The personal firewall category is divided into corporate and consumer categories. In more detail:

- ☒ **Enterprise firewall/VPN software.** This is robust enterprise-class software that inspects IP packets as they enter a network. The inspection is to determine if the packet conforms to a policy (i.e., an acceptable protocol). The result of the inspection will be to allow the packet or to reject the packet.

- ☒ **Personal firewalls.** These cost less than \$100 and are used to determine if a given IP packet should be passed to the desktop device. Generally the products are used to control what desktop applications can communicate with the Internet. They are also evolving to control the functionality of the Web browser. The personal firewall market is divided into those sold to corporate customers and those sold to consumers.
- ☒ **Corporate personal firewalls.** These are generally used to maintain the corporate desktop security policy. Many of the corporate personal firewalls incorporate remote management and policy. Through the use of a central management console, enterprises or service providers can manage the firewall to ensure that it remains within a stated policy, receives software updates, and has virtual VPN management. Revenue in this market includes any management servers used to serve the corporate policy.
- ☒ **Consumer personal firewalls.** These are generally used to protect home and small business offices that have a high-speed, always-on connection through cable or DSL modem. These products have the same technology as that of the corporate personal firewall, but remote management of these products is not possible.

Security 3A Software

Security 3A software (i.e., administration, authorization, and authentication) is used to administer security on a computer system or systems or in an enterprise. Security 3A includes the process of authenticating, authorizing, defining, creating, changing, deleting, and auditing users. In more detail:

- ☒ **Authentication software.** At its simplest level, this is just a way of identifying the user. This means the software (and associated hardware) determines that users are who they say they are. The authentication software market contains two submarkets: public key infrastructure (PKI) and advanced authentication software. Both of these technologies play key roles in verifying users' identities and avoiding repudiation.
- ☒ **Authorization software.** This is used to determine resource access in conjunction with business policy. The authorization software market includes three submarkets: Web single sign-on (SSO), host SSO, and legacy authorization.
- ☒ **Administration software.** This includes solutions that focus on increasing end-user productivity, reducing administrative errors, providing management of various security technologies from a single point of control, enforcing user access security policies, and reducing potential security breaches from internal and external parties.

Intrusion Detection and Vulnerability Assessment Software

Intrusion detection products include the subset intrusion prevention products, and vulnerability assessment products include the subset vulnerability management products. In more detail:

- ☒ **Intrusion detection products.** These products provide continuous monitoring of devices or networks and react to malicious activity. A device or agent on a network or a system, respectively, will compare current activity with a list of signatures known to represent malicious activity, or it will use other detection methods such as protocol analysis, anomaly, behavioral, or heuristics to discover unauthorized network activity. Intrusion detection products are passive systems that do not interact directly with the datastream or application calls. They can direct other security products, such as firewalls, to activate a preestablished automated response to policy-violating activities. A subset of these products is:
 - ☐ **Intrusion prevention products.** This is a subset of intrusion detection because one must be able to detect before one can prevent. Prevention products perform the same tasks as detection products; however, to qualify as prevention products, they must be inline (have direct access to traffic and commands) and have the ability to proactively prohibit malicious activity. Although prevention products are considerably different in function than pure intrusion detection, the two categories are being tracked together because they compete for the same budget.

- ☒ **Vulnerability assessment (VA) products.** These are batch-level products that determine the configuration, structure, and security attributes of network user accounts, directories, servers, workstations, and other devices. Some products also deal with vulnerabilities of applications. This information is compared with a database of known security holes and best practices for security configuration management. More sophisticated VA products can test for both known and unknown vulnerabilities by looking at both the common Web vulnerabilities and application-specific vulnerabilities or those defects that exist in the actual business logic of the site. Many products also run actual attacks to determine the strength of various systems and networks. A subset of these products is:
 - ☐ **Vulnerability management products.** These expand upon vulnerability scanning by integrating additional features to provide risk management and policy compliance.

Other Security Software

Other security software covers emerging security functions that do not fit well into an existing category. It also covers some of the underlying functions, such as encryption tools and algorithms, that are the basis for many security capabilities found in other software and hardware products. Also included in this category will be products that fit a specific need but have yet to become established in the marketplace.

Products in this category will grow into their own categories or eventually be incorporated into the other market segments. For 2003, areas covered by other

security software include, but are not restricted to, encryption toolkits, file encryption products, database security, storage security, standalone VPN and VPN clients, wireless security, Web services security, and secure operating systems. In addition, readers should be aware that the products that are covered here (especially for wireless and Web services) are only those that do not qualify for one of the more established categories.

SITUATION OVERVIEW

Security 3A Software

The identity management transition that IDC previously forecast is certainly rolling along. Almost every vendor in the security 3A market is clearly positioning itself as an identity management vendor. The OASIS and SAML standards seem to be well accepted among the vendors, and customers increasingly view these standards as a way to reduce the cost of integration. In fact, one of the dominant themes this year seems to be that customers are demanding modular tested and integrated solutions from a smaller number of vendors.

Even though they are outside the scope of IDC's 3A definition, we believe directories and their reconciliation are an increasingly important benefit for customers. However, IDC believes directories will also represent a major challenge for vendors to overcome. Consider that most companies have anywhere from tens to hundreds of directories across geographic locations and business units. Moreover, each individual user may have 10 or 20 different identities (user names/accounts) in an average corporate environment. Reconciling all of these different user names to common understanding of an individual user's rights and access privileges can be extremely difficult. Simply finding all the instances of that particular user and coming to the realization that they are, indeed, the same individual is often a very complex, tedious, and costly manual process.

Regulatory Compliance

We believe that directory reconciliation and consolidating is crucial to the success of identity management because it has a direct bearing on regulatory compliance. Regulatory compliance at its very heart requires that systems know who users are and make reasonable efforts to tightly authenticate those users. Once a system knows who a user is, it must then know what the user is permitted to do online. After that, the system has to be able to record what the user has done and to provide an auditable record that reconciles the user's privileges with the user's actions.

The critical part is for a company to have an enforcement process in place that incorporates access policies and ensures that no unauthorized access or actions take place. For example, should a low-level hospital clerk have full access to a patient's previous medical history? Does the physical therapist need to know about the blood work? Should an HR person have access to an employee's complete medical history? Should there be a guarantee that the financial records of a company are reviewed and verified (signed off on) by a company officer? Is there a guarantee that those records will not be changed prior to publication? Can a corporate whistle-blower be

assured that complaints and/or charges of improper governance are recorded and that those records are protected from unauthorized deletion or modification? These are just a few examples of what customers face in the challenge of complying with various privacy regulations.

New Players in the Identity Management Market

We fully expect that the major enterprise software vendors will also enter the identity management market. In some cases, they will develop their own solutions; in other cases, they will partner. For example, Oracle recently announced an identity management solution largely based on its own products.

We still believe that identity management must be a core component of Web services. The next major challenge, still several years off, is getting identity management to deal with the problem of authenticating and authorizing machine-to-machine in addition to people-to-people and people-to-machine interactions and transactions.

IDC expects to see more and more hardware in the identity management area. Tokens, smart cards, and biometrics, to a lesser extent, will become parts of comprehensive identity management solutions. Identity management solutions from vendors like RSA, Secure Computing, Aladdin, and SafeNet, as well as other hardware authentication vendors, will see significant benefits from the reduction of password reset requests and an increase in security, especially for remote users on VPN connections.

We also believe there will be an emergence of security appliances in the 3A market. Improvada is an example of a single sign-on security appliance that is targeted at the middle tier and is designed with tokens so customers can extend their current hardware authentication environments to identity management. Security appliances and activity will increase in the midtier market, which has been largely ignored by most enterprises focused on identity management vendors.

Public Key Infrastructure

The market for public key infrastructure certificate authorities and certificates has not lived up to the hype heaped on it. However, the market remains of interest and has a number of vendors that provide many components for the successful deployment of public key certificates and applications. PKI remains a market in the doldrums for a number of factors, including a weak economy that has limited how much enterprises are willing to invest in the technology and confusion on how to measure return on the PKI investment.

Although many enterprises have been slow to roll out large-scale PKI deployment, there are many encouraging signs that the technology and the vendors that provide it will rebound. The technology, including PKI-enabled applications, is advancing to the point at which PKI deployment makes great sense. One strong sector for PKI has been government. Many nations, including Denmark, Italy, and Singapore, and U.S. states such as Illinois have adopted PKI in order to allow citizens, businesses, and others to easily and securely exchange digital information with government authorities via the Internet.

PKI is also being considered by the healthcare, financial, and insurance sectors as the mechanism to deal with government privacy regulations. With the utilization of PKI, customer information and sensitive data can now be processed and distributed securely to appropriate individuals. There are now many PKI solutions that can aid healthcare and insurance providers in meeting the authentication, authorization, and encryption required by the HIPAA.

The future of PKI will be driven by its ability to support Web services and enterprise identity management deployments. As enterprises add smart cards and USB tokens, there will be an opportunity to deploy PKI with those hardware solutions. Many applications (email, SSO, and digital signatures) that can utilize certificates already exist.

PKI's ability to support Web services was enhanced when the OASIS global standard consortium took over the PKI Forum. Now PKI will be included within the other OASIS XML-based standards activities. This move strengthens IDC's position that PKI will be baked into the infrastructure. PKI will exist and be used by many, although they will not realize that the technology is being utilized.

Last, the main reason the PKI market, as measured by dollars, hasn't been as strong as many thought is because PKI can be implemented using open source methods; thus, usage of the technology is higher than the dollar amounts indicate. The use of open source works for smaller deployments or when the certificates are used within a closed system (such as the authentication of devices to a management console). As the requirements for PKI become more sophisticated, the use of open source should be replaced by purchased solutions that can scale to enterprisewide levels.

Secure Content Management Software

August 2003: Month of Malicious Code

After a quiet start, 2003 turned out to be a very big year for viruses, worms, and malicious code. In fact, August 2003 is widely regarded as the worst month in the history of virus outbreaks. Blaster and SoBig came within eight days of each other in August and were two very different types of attacks. The Blaster attack was a perfect example of a worm, spreading to other computers and networks automatically and without the action of humans. The worm targeted a known vulnerability in Microsoft's Windows operating system called the Distributed Component Object Model (DCOM) interface, which handles messages sent using the Remote Procedure Call (RPC) protocol. RPC is a common protocol that software programs use to request services from other programs running on servers in a networked environment. SoBig, on the other hand, was a mass-mailing virus that collected email addresses from several different locations on a computer and sent emails containing the virus to each address. There is widespread belief the SoBig virus was created by a spammer as a proof of concept for delivering spam messages.

The Convergence of Spam and Virus

In the past, spammers traditionally sent spam from their own ISP accounts. When corporate IT departments and antispam solutions first started to block messages from certain domains and ISP accounts, spammers turned to new methods to conceal their identity. We believe spammers are starting to resort to outright criminality in their efforts to conceal the sources of their spam messages, using Trojan horses to turn the computers of innocent consumers and corporate users into secret spam engines. The explosive growth of cable modems and broadband connections has left consumers and remote employees open to attack. In many cases, their computers are being used as a relay for sending spam to thousands of other people. There is also very little chance that PC owners will have any idea their systems are being used by a third party. The SoBig virus, described above, is a good example of the convergence of spam and viruses.

The Need for Speed

Viruses remain constant; however, worms and malicious code are now the more significant threat to organizations. With a constant stream of new threats, antivirus companies are producing and distributing signature files faster than ever. However, the speed with which new worms and malicious code are spreading has caused the effectiveness of traditional signature-based antivirus solutions to suffer. Recent malicious code incidents have achieved widespread propagation at rates significantly faster than many previous viruses. Worm propagation times have dropped from hours to minutes.

Show Me the Money

In addition to it being a big year for viruses, worms, and malicious code, the motive and intention of virus writers has changed. In the past, worms and viruses were typically created to destroy data by amateurs seeking notoriety. Today, more sophisticated attackers, often in organized crime, are increasingly using worms and viruses to obtain credit card numbers, bank account information, and other personal information to perpetrate identity theft. The sophistication and scale of online frauds and identity thefts are increasing at a rapid pace. The recent incidents of "phishing attacks" on banks and their online customers have opened both consumer and corporate eyes to the increasing dangers of corporate identity theft. Phishing is clearly motivated by financial fraud and gain, and thus criminals are most often behind these attacks (rather than teenagers just trying to cause havoc).

Spam Not Slowing Down

Spam has become a major driver for messaging security implementation. The majority of vendors in the SCM market have developed, partnered with, or acquired an antispam technology. Internet service providers and antispam solution vendors report that spam currently represents 45–80% of all inbound Internet email, way up from 2002 levels closer to 15–30%. When internal email is included in the calculation, IDC estimates that spam represents 32% of all email sent on an average day in North America in 2003 (see *Worldwide Email Usage Forecast, 2003–2007: Spam and Instant Messaging Take a Bite out of Email*, IDC #30195, October 2003).

Regulatory Compliance

The challenge of controlling electronic communications as they flow into and out of an organization is becoming increasingly more critical. Government and industry regulations such as HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley, and SEC have caused unprecedented pressure on corporations to secure the use of their electronic communications. In many cases in which the original intent was to address a regulatory issue, the security aspect represents part of the solution. Organizations are faced with the complex task of complying with various regulations and making sure that employees do not inadvertently, or deliberately, break the law. Each of these regulations can carry criminal penalties and/or civil penalties. Criminal means criminal prosecution of individuals as well as substantial fines. Successful criminal convictions generally lead to civil lawsuits. Civil lawsuits (especially in class-action situations) can carry substantial financial penalties and damage a company's reputation with its customers. Although many regulations only fall into the civil area and would seem "toothless," the fact that they permit class-action suits creates major opportunities for the legal community, especially in today's litigious society.

Productivity, Liability, and Network Resources

Web filtering solutions continue to evolve into more comprehensive employee Internet management (EIM) solutions to meet ever-expanding threats of non-business related Internet use. Instant messaging, peer-to-peer, and streaming media have joined non-business related Web surfing as a growing productivity, legal liability, and network resource concern in many organizations. The impact of streaming media is clearly on bandwidth; however, streaming media has also affected employee productivity because employees waste time watching concert highlights or clips from their favorite TV show. Driven by peer-to-peer networks, which allow employees to swap digital files using corporate high-speed connections, the problem of illegal content in corporate networks is quickly becoming a significant legal issue for corporations. Public instant messaging use is putting companies at greater risk to security vulnerabilities, breaches of confidentiality, virus infection, legal liability, and violation of privacy regulations. Last but not least, employees surfing the Web for pornography or racist, hate, and other non-business related sites affect productivity, liability, and network resources for any corporation.

Firewall/VPN Software

The software firewall/VPN has been growing, but with the challenges posed by appliances and new infrastructures and technologies, the market will need to transform to maintain stable growth. Developments that will shape this market in the future include the following:

- ☒ **Firewalls as gateway security platforms.** Firewalls will become the key application where centralized security policy will be enforced. They will have increased responsibility to host and interact with other security solutions targeted directly at gateway protection.

- ☒ **Firewall specialization.** The firewall market is becoming increasingly fragmented as it matures and products are designed to meet specific needs, such as dedicated email server firewalls or other specific application-protection mechanisms. These specialized firewalls will sit behind a gateway firewall.
- ☒ **Continued integration with other security and performance software.** Firewalls will continue to work tightly with other security software, such as antivirus, intrusion detection, intrusion prevention, anti-denial of service, and access control. Firewalls will also be more active in protecting applications at layers higher up the stack than normally handled by firewalls. Non-security functionality, such as load balancing and high availability, will continue to be incorporated.
- ☒ **Strategies to handle appliances and keep the software relevant.** Software vendors will need to remain vigilant regarding the activities of the hardware firewall/VPN vendors and to work with OEMs to ensure there are offerings that can meet all customer needs.
- ☒ **Addressing other untapped opportunities, such as mobile, wireless, Web services, and storage networks.** As acceptance of the mobile Internet grows, there will need to be firewall solutions to connect the wired gateways with the mobile access points. The case is the same for wireless networking. With firewall and VPN, vendors will be able to deploy wireless local area networks with improved confidence. In addition, software firewall vendors should investigate emerging opportunities, including Web services and storage networks.
- ☒ **Handling open-port applications, such as instant messaging.** New communication activities, such as instant messaging and SSL-encrypted communications, leverage the HTTP protocols to easily pass through the firewall. However, by allowing instant messaging programs and uncontrolled SSL through the gateway, corporations are putting enterprise systems at risk. Offering enterprises additional control of the gateway will be required for firewalls to remain the paramount security product.
- ☒ **Increased government scrutiny.** Government regulations, such as Sarbanes-Oxley, and other pressures on enterprises to increase their security posture will require organizations to expand the security infrastructure. Firewalls are the first line of defense; they will be relied upon to cover more areas, and enterprises will be expected to deploy more within the internal network and at the desktop to meet compliance requirements.

Intrusion Detection and Vulnerability Assessment Software

Intrusion Detection and Prevention

The intrusion detection and prevention (ID&P) market has had strong growth, but with the challenges posed by appliances and new infrastructures and technologies, the market will need to transform to maintain stable growth. Developments that will shape this market in the future include the following:

- ☒ **Wireless and mobile intrusion detection.** Wireless and mobile IDS, like its wired cousins, provides automated detection, security analysis, and device discovery, and it monitors for policy compliance. However, due to the nature of the wireless and mobile environment, it must do so efficiently and with reduced bandwidth consumption. Products already associated with this market include Wireless Scanner by ISS, Border Guard by StillSecure, and AirDefense IDS.
- ☒ **Moving from a defensive to a proactive security technology.** Intrusion detection is considered a defensive security technology; its primary function is to watch the traffic on the network and/or watch for commands calling an operating system. However, intrusion detection is taking a more proactive approach to prevent intrusions before they can do any damage. This approach ranges from sending policy changes to the firewall to directly preventing traffic to pass through the network or calls to be dropped at the host level.
- ☒ **Improved detection methods to reduce false positives.** The greatest complaint about ID&P systems is that they generate huge amounts of data that can't easily be monitored. As a result, vendors are working to improve the processing of this data. ID&P will need to integrate better with vulnerability assessment products to determine the risk of an attack based on the assessment of a system or network. ISS' SecurityFusion module already has this feature, in that it can correlate events against known vulnerabilities and assets to prioritize events. Cisco's Threat Response technology performs "just-in-time" event validation to remove spurious alerts. Many more products are expected to have this capability and similar ones in the future.
- ☒ **Cooperative ID&P solutions for network, server, and host.** The major security vendors (in this case, ISS, Symantec, Cisco, and Network Associates) appear to be headed toward a strategy that offers enterprises consistency with their ID&P solutions for network, server, and host.
- ☒ **Increasing use of appliances for network intrusion prevention.** To increase ID&P performance and manageability, vendors and customers are turning to appliance-based network ID&P products. With the release of ISS' Proventia line of network security appliances, network ID&P is destined to be delivered in an appliance format. All of the large enterprise vendors, including Cisco, Symantec, Network Associates, ISS, NetScreen, and Enterasys, can offer their ID&P in appliance format. These are in addition to appliances offered by Top Layer, Lancope, SourceFire, NFR, DeepNines, and Vsecure.

- ☒ **IDS as a forensics and policy-compliance tool.** If for nothing else, intrusion detection will continue to be valued for its forensics abilities — that is, being able to provide insight into how a system was exploited and what might have been compromised. Also included in this category is the ability to audit whether the gateway firewall and intrusion prevention systems are performing well.
- ☒ **Continued market competition.** There has been some consolidation in the ID&P market; however, for every company that has been purchased, three more have appeared to take its place. The established security vendors have made purchases in the past year. (Symantec bought Recourse and NetScreen acquired OneSecure in 2002, while 2003 saw Cisco buy Okena and Network Associates add intrusion prevention vendors IntruVert and Enterscept.) However, there continues to be increasing interest in start-ups doing XML, host-based intrusion prevention, and network-based intrusion prevention. Given this trend, it does not appear that there will be considerable consolidation in this market for the next three years.

Vulnerability Assessment and Management

The vulnerability assessment and management (VA&M) market has seen decent growth, but IDC believes the market will experience increasing growth over the next few years. There are new challenges, technologies, and opportunities that will shape this market in the future, including the following:

- ☒ **Increased availability of VA appliances.** IDC believes that by 2007, 80% of all security solutions will be delivered via an appliance. One reason for this prediction has been the continuous expansion of appliances into areas where appliances would not be expected. VA&M is one of those areas. Appliances that can perform remotes scans, especially behind firewalls, and send the data to a central server for final processing is the area where VA&M appliances are cropping up. Qualys, Foundstone, Computer Associates, nCircle, and newcomer PredatorWatch all have appliances that support their VA&M software products. Preventsys has gone the CD-appliance route, which allows suppliers or customers to create dedicated appliances.
- ☒ **Compliance assessment/positive security model.** Security efforts to date have been focused on keeping the bad guys at bay. Traditionally, this has been accomplished by trying to outsmart hackers by creating barriers or providing defensive mechanisms once a vulnerability was identified. This is a reactive approach to security that is being replaced by a proactive one geared to prevention and the management of risk. Under this model, only intended actions specified by policy are allowed. To make the positive security model work well, enterprises must be able to ascertain their existing security posture and measure it against a policy. VA&M vendors such as BindView, Foundstone, NetIQ, Preventsys, and Qualys are developing products that can assist enterprises in measuring their compliance against the security policy.

- ☒ **Tie to event correlation.** VA&M assessments can be valuable tools in making other security products better. By using the output from vulnerability scans, intrusion detection and intrusion prevention products can reduce false positives. By correlating a potential attack against the vulnerability posture, the intrusion detection device can determine if a real threat exists. The vulnerability results can also be used by security event management programs to better tune their correlation data, to improve accuracy, and to provide a better threat determination.

- ☒ **VA for applications and application development.** As security becomes more important at the application level, there will be new products that are designed to assess the status of individual applications. ISS, Symantec, NetIQ, and Application Security have scanner modules that can perform assessments on databases and other applications. Vendors such as Sanctum have been providing assessment tools for Web applications. The next step in this evolution is to utilize vulnerability discover testing throughout the application life-cycle development so that vulnerabilities can be eliminated before software is operational. Application security will be a hot topic as more organizations improve software quality. Organizations are going to demand software that is less vulnerable to attack, thus application level security needs to be a fundamental component for software development and quality assurance. Sanctum is out in front of this development, as are SPI Dynamics and @Stake.

- ☒ **Patch management.** The vast majority of attacks, including automated worms, are performed against known vulnerabilities that have patches available. However, ensuring that patches are up to date is a very difficult task. VA&M software will be asked to discover the existing patch level and to determine what vulnerabilities exist at that patch level. The software may also be asked to track the status of patch remediation, including workflow and opening help tickets, but in most cases the specific patching will be done using separate products that do not fall under the VA&M market.

- ☒ **Increased deployment of VA&M for the small and medium-sized enterprise.** Small to medium-sized enterprises will need be able to demonstrate that they are meeting government-mandated security requirements; they will also be asked by larger enterprises to provide a status of their security posture to connect directly to the larger companies systems. These developments will increase the need for VA&M that can meet the specific needs of this sector.

- ☒ **Open source.** One competitive component of the VA&M market that does not register in a market sizing based on vendor revenue is the use of open source or freeware products. Many enterprises use free tools that have come out of academia or as the result of government projects. In the VA&M category, freeware NESSUS is included in many products as a baseline vulnerability scanner. Additionally, other products can use data collected from NESSUS scans. This open source product sets the baseline against which all commercial products are evaluated.

- ☒ **New vendors.** As in so many of the security markets, new vendors continue to emerge. In the VA&M space, the new vendors are involved with advancing the concepts of risk management, policy compliance, and the other trends mentioned above. Some of the fastest-growing new vendors include SPI Dynamics (380%), Qualys (133%), and Foundstone (100%). In addition to those vendors, there are other companies, such as @Stake and Visionael, that are adding VA&M software to their already-existing product lines, or new players like Preventsys and Core Security, which emerged in 2002. All of these vendors will help to redefine this market.

FUTURE OUTLOOK

Forecast and Assumptions

Security Software Forecast, 2004–2008

Worldwide

IDC's estimate of the growth of the security software market through 2008 is presented in Table 1. Worldwide revenue for the security software market reached \$8.05 billion in 2003. The security software is forecast to increase to \$16 billion in 2008, a 14.7% CAGR for the period from 2003 through 2008. Additionally:

- ☒ Secure content management software will increase from \$3.3 billion in 2003 to \$7.2 billion in 2008, representing a 17% CAGR for the period from 2003 through 2008.
- ☒ Security 3A software will increase from \$2.7 billion in 2003 to \$5.3 billion in 2008, representing a 14.4% CAGR for the period from 2003 through 2008.
- ☒ Firewall/VPN software will increase from \$934 million in 2003 to \$1.3 billion in 2008, representing a 6.4% CAGR for the period from 2003 through 2008.
- ☒ Intrusion detection and vulnerability assessment software will increase from \$828 million in 2003 to \$1.6 billion in 2008, representing a 13.8% CAGR for the period from 2003 through 2008.
- ☒ Other security software will increase from \$307 million in 2003 to \$623 million in 2008, representing a 15.2% CAGR for the period from 2003 through 2008.

A more detailed analysis of the security software market in 2003 including vendor revenue and shares will be published in 2Q04.

Table 2 shows the market forecast by region and platform.

Table 3 shows the key assumptions underlying this forecast.

TABLE 1

Worldwide Security Software Revenue by Market Segment, 2003–2008 (\$M)

	2003	2004	2005	2006	2007	2008	2003 Share (%)	2003– 2008 CAGR (%)	2008 Share (%)
Security 3A	2,694	3,087	3,549	4,077	4,666	5,284	33.5	14.4	33.1
Secure content management	3,289	3,972	4,707	5,486	6,332	7,214	40.8	17.0	45.2
Firewall/VPN	934	1,000	1,070	1,135	1,204	1,271	11.6	6.4	8.0
Intrusion detection and vulnerability assessment	828	962	1,102	1,257	1,414	1,577	10.3	13.8	9.9
Other	307	354	412	476	548	623	3.8	15.2	3.9
Total	8,051	9,375	10,841	12,430	14,163	15,969	100.0	14.7	100.0

Note: See Table 3 for key forecast assumptions.

Source: IDC, March 2004

TABLE 2

Worldwide Security Software Revenue by Region and Operating Environment, 2003–2008 (\$M)

	2003	2004	2005	2006	2007	2008	2003 Share (%)	2003–2008 CAGR (%)	2008 Share (%)
Geographic region									
North America	3,852	4,411	5,046	5,745	6,508	7,336	47.8	13.8	45.9
Western Europe	2,489	2,937	3,434	3,957	4,539	5,108	30.9	15.5	32.0
Asia/Pacific	1,320	1,571	1,823	2,099	2,386	2,679	16.4	15.2	16.8
ROW	390	456	537	629	731	847	4.8	16.8	5.3
Total	8,051	9,375	10,841	12,430	14,163	15,969	100.0	14.7	100.0
Operating environment									
Mainframe	654	684	711	733	750	756	8.1	2.9	4.7
OS/400	73	73	73	72	71	69	0.9	-1.2	0.4
Unix	2,333	2,590	2,857	3,131	3,408	3,670	29.0	9.5	23.0
Linux/other open source	213	307	441	625	864	1,154	2.7	40.2	7.2
Other host/server	346	370	394	415	435	449	4.3	5.4	2.8
Windows 32 and 64	3,860	4,687	5,599	6,581	7,646	8,752	47.9	17.8	54.8
Embedded	38	45	54	64	76	90	0.5	18.6	0.6
Other single user	424	491	559	625	691	757	5.3	12.3	4.7
Platform independent	109	129	153	183	222	273	1.4	20.1	1.7
Total	8,051	9,375	10,841	12,430	14,163	15,969	100.0	14.7	100.0
Growth (%)	NA	16.4	15.6	14.7	13.9	12.8			

Note: See Table 3 for key forecast assumptions.

Source: IDC, March 2004

TABLE 3

Key Forecast Assumptions for the Worldwide Security Software Market, 2004–2008

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Macroeconomics				
Economy	Worldwide economic growth will continue to recover slowly from 2001 levels to traditional levels. There will be no double-dip recession. Consensus Economics' March 2003 forecast holds.	High. Economic growth will begin to be a positive impact for IT spending.	↑	★★★★☆
Iraq	The war in Iraq will be over by summer, Saddam Hussein will be deposed and discredited, and NATO allies will patch up their differences. Travel restrictions will be lifted, and the aura of uncertainty affecting business decisions will dissipate.	Moderate. There will be little reason for economic uncertainty over Iraq to impact IT spending.	↔	★★★★☆
Other geopolitics	The threat of terrorism at home and other potential armed political conflicts will not escalate or abate. No events as drastic as those of September 11 will occur during the forecast period.	Moderate. Business decisions and project initiations will begin in line with a better economic outlook.	↔	★★★★☆
Inflation	Inflation will remain under control. Over the next three years (according to Consensus Economics) expectations for the United States, Western Europe, and Asia/Pacific are that consumer prices will rise less than 2%. Eastern Europe and Latin America, however, will see double-digit inflation in 2003. There will be no deflation.	Moderate. Business confidence will be unaffected.	↔	★★★★☆
Telecom	The telecom industry will begin to recover. Capital expenditure (capex) and operating expenditure (opex) spending, which in 2003 mirrored 2002, will slowly pick up. European governments will help rebuild after the 3G licensing fiasco.	Moderate. The IT industry has already factored the recovery of the telecom industry in.	↔	★★★★☆

TABLE 3

Key Forecast Assumptions for the Worldwide Security Software Market, 2004–2008

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Compliance	Increased compliance legislation within the United States and Western Europe will increase transparency in many industries with Sarbanes-Oxley, Basel II, HIPAA, and so forth.	High. Compliance regulations will begin to have an effect on software spending in 2005 and beyond. Compliance will affect areas of infrastructure software like security, storage, and applications areas such as records management, content management, and business performance management, to name a few.	↑	★★★★☆
Technology/ service developments				
Software complexity	Software systems will continue to increase in complexity, but demand for higher quality and productivity will be unabated.	Moderate. The complexity crisis will maintain the need for integration, but the demand for high quality and productivity could deter skeptical buyers from existing product offerings. Increasingly, this functionality may be delivered as an IT or business service.	↔	★★★★☆
Growth in security appliances	Security appliances will continue to grow in popularity as an easy way to distribute software security solutions to customers.	High. With more software available in appliance form, customers will be able to field solutions quickly and at less cost.	↑	★★★★★
Communication	There will be a doubling of the number of Internet users in five years as well as a tenfold increase in Internet commerce. There will be rapid growth of wireless LANs, communicating handhelds, and IP telephony. Supply chain automation will remain a long-term growth area.	High. All of these factors will create demand for new security solutions.	↑	★★★★★

TABLE 3

Key Forecast Assumptions for the Worldwide Security Software Market, 2004–2008

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Killer apps	New technology (e.g., Web services, wireless LANs, storage area networks, clustering, and high-growth software areas) will help drive price performance to attractive levels that support new IT spending growth.	Moderate. No "killer apps" or new technologies will drive overall industry growth in the same way Windows and Office suites did in the 1980s or the Internet did in the late 1990s. Web services will continue to be mostly a software development technique.	↔	★★★★☆
Market ecosystem				
Security: SCM consolidation	Antivirus companies are building, acquiring, or partnering with antispam companies, giving organizations fewer vendors to deal with and an easier time managing their messaging security architecture.	Moderate. We believe customers will continue to buy point-solutions, but this will be the exception, not the rule. Antispam will continue to be an important adoption driver in the messaging security section; however, IDC believes it will become a feature of messaging security and not a distinct market.	↔	★★★★☆
Capitalization				
Venture	Venture funding, now at 1998 levels, will pick up slowly year by year. New companies will begin to find some funds available.	Moderate. This will have a moderate impact on increasing software revenue growth.	↔	★★★★☆
Stocks	The world stock market will come back to 2002 peak levels by the end of 2003 but not to March 2000 levels until after 2006.	Moderate. Business confidence and market liquidity will increase.	↑	★★☆☆☆
Labor supply				
Productivity management	During the economic downturn, companies learned to do more with less. Potentially, there will be less of an uptick in employment as more processes are automated.	Moderate. The impact on increasing software revenue growth will be moderate.	↑	★★★☆☆

TABLE 3

Key Forecast Assumptions for the Worldwide Security Software Market, 2004–2008

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Offshoring	Offshore software development will fill out the skill supply.	Low. The impact on overall software growth will be low.	↔	★★★★☆
Consumption				
Buying sentiment	IT buyers will begin to spend again as the economy improves; CIOs will begin to replace hardware and operating systems, begin to spend on mobility, and regain attitudes that IT spending is critical to their companies' well-being. IT spending as a percentage of revenue (or income) will go up.	High. Security will be a primary area of IT spending.	↑	★★★★☆

Legend: ★☆☆☆☆ very low, ★★☆☆☆ low, ★★★☆☆ moderate, ★★★★☆ high, ★★★★★ very high

Source: IDC, 2004

By Geographic Region

IDC analysts around the globe supplied regional input and insight into the security software market forecast. The worldwide forecast is the aggregation of this regional data (refer back to Table 1).

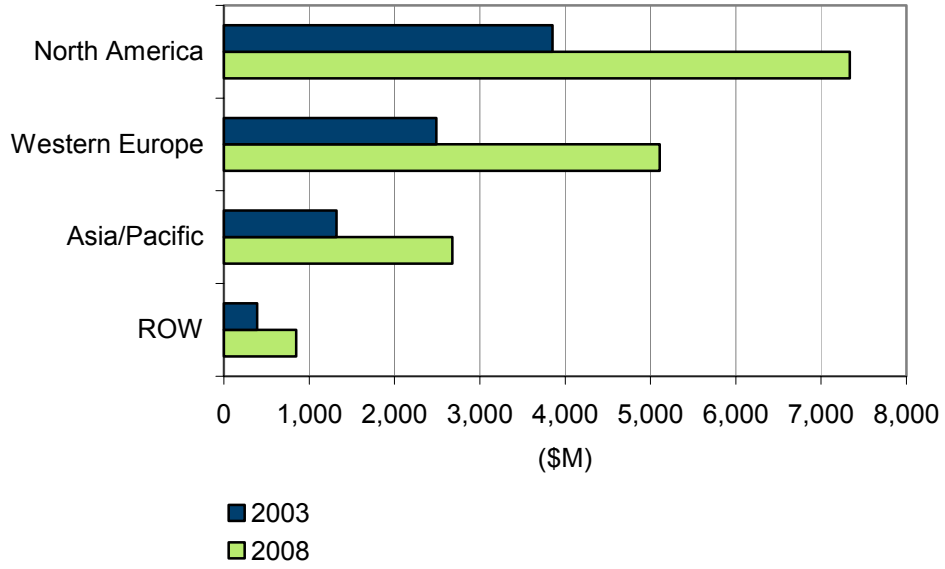
Revenue for 2003 and 2008 is shown graphically in Figure 1.

By Operating Environment

This study represents IDC's operating environment forecast for the security software market through 2008. The revenue forecast for the security software market, segmented by operating environment is also shown (refer back to Table 1); revenue for 2003 and 2008 is shown in Figure 2.

FIGURE 1

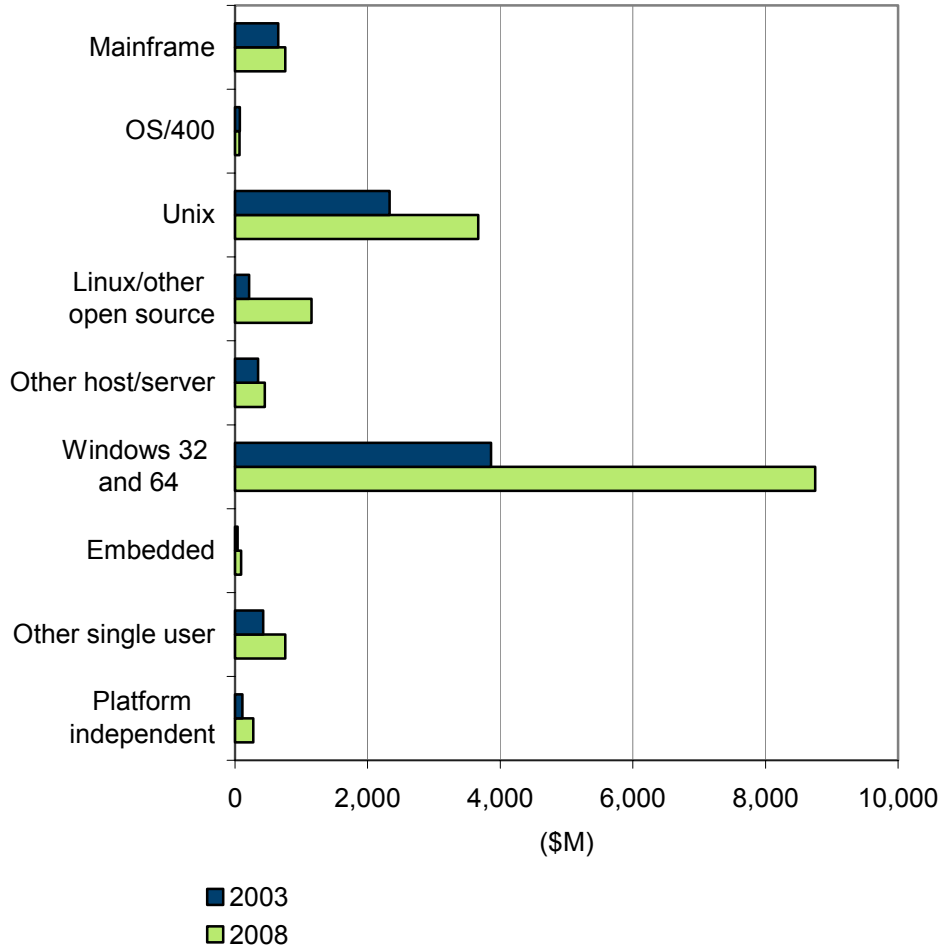
Worldwide Security Software Revenue by Region,
2003 and 2008



Source: IDC, March 2004

FIGURE 2

Worldwide Security Software Revenue by Operating Environment, 2003 and 2008



Source: IDC, March 2004

ESSENTIAL GUIDANCE

Secure Content Management

The recent onslaught of viruses and worms such as Blaster, Nachi, and SoBig not only highlights the importance of keeping security solutions up to date, but it also shines a spotlight on the growing need for more proactive security products and services. While corporate customers have long realized that antivirus software is only as good as its last update, consumers and small business customers are realizing the necessity of subscription-based updates. Consumers and small businesses are finally recognizing the fact that antivirus software is more of a service than a product.

Furthermore, the rapid infection by these new worm and virus attacks means that slow responses will cripple most customer environments because they will not be able to get ahead of the initial infection and the far more serious reinfections. Malicious hackers are getting much more sophisticated and faster at exploiting application vulnerabilities. The threat of zero-day attacks that take advantage of software vulnerabilities for which there are no available fixes are starting to be viewed as a major threat to data security.

IDC believes that a multilayered approach to the security infrastructure is necessary to thwart the threats outlined in this document. This approach could include some or all of the following: secure content management software, identity management software, antispam filtering products, firewall/VPNs, network forensic software, management and monitoring software, security appliances, and secured application server technology. Finally, it is essential that enterprise IT departments outline and implement security policies that are strictly enforced throughout the organization. IDC advocates awareness, strictly enforced security policies corporatewide, and a multilayered approach to building and maintaining the security infrastructure.

Intrusion Detection and Vulnerability Assessment

Intrusion Detection and Prevention

The ID&P market will experience considerable change over the next few years, especially with the increasing inclusion of ID&P features in gateway firewalls. The line between a firewall and a network intrusion prevention product will continue to blur. However, IDC firmly believes that intrusion detection technology and its subset, intrusion prevention, will not be obsolete by 2005, as others have predicted. The ability to monitor and respond to incidents at the network gateway, within the network, and at the device level remain critical to a defense-in-depth security infrastructure.

While acknowledging that there are problems with performance, false positives/negatives, and the overhead required for monitoring, IDC believes that the technology will grow to meet the needs of the customers. It will evolve. In environments where there will be improved gateway defenses, ID&P will be smarter. It will be used to monitor network, server, and host activities within the perimeter as much as a problem-finding and -audit tool as a full security tool. It is the only technology that can really tell you what is going on within the network and alert you to possible security problems. Within the network, you don't want to be blocking everything, but you do want to see what is taking place and be able to check for malicious activity.

Vendors that can best address existing IDS shortcomings while growing the capabilities with the technology (as outlined above) will have the most success. Major enterprises will probably migrate to the larger vendors that can offer consistent network, server, and host ID&P solutions. Small vendors will need to concentrate on meeting specific needs such as wireless, Web security, and application security. In these areas, their specialization and innovation will provide enterprises with added value.

Vulnerability Assessment and Management

It isn't just about discovering vulnerabilities anymore. Enterprises are looking for much more from VA&M software. They still need to know about their vulnerabilities, but those must now be put into context. The vulnerabilities must be viewed as part of an overall security management infrastructure that takes into account security policy and compliance and risk management. VA&M software will need to have many more features available. The VA&M software will be expected to tell the enterprise why the vulnerability is a concern and how each specific vulnerability is ranked so that remediation can be performed in a consistent manner instead of handled in a chaotic manner.

One untapped segment for VA&M products is the small to medium-sized enterprise. In the past, this segment has been overlooked because the cost associated with vulnerability assessment has been so high. However, as government requirements for security and privacy proliferate, organizations of all sizes are beginning to be concerned about their ability to measure their compliance to security requirements. As these companies expand their use of additional security products and services, they will also be looking for ways to measure their risk. Vendors that can provide small and medium-sized enterprises with simple, easy-to-use, and affordable products for policy compliance and risk management should have considerable success.

Firewall/VPN

To take advantage of the forecast growth, IDC recommends that vendors expand the capabilities of firewalls. Vendors will need to look at emerging technologies to find ways to ensure that firewall software is optimized to protect wireless networks, Web services, and storage area networks — all growth areas in which improved performance and different protocol inspection will be required.

Firewall/VPN software products must be able to have smooth integration with complementary security products, such as intrusion detection and content security. Vendors should also look closely at partnering with managed service providers. These service providers will eventually provide firewalls as an embedded service; to succeed, the software vendor must capture some of this market. Software vendors must also offer options that can compete with the faster-growing firewall/VPN security appliance market. Licensing and partnerships will be required for vendors to remain strong in this market.

Security 3A

The 3A market will continue to undergo significant changes over the next few years. IDC believes that point products and utilities will find less and less acceptance because of the systems integration costs. Customers are already starting to reject 3A products that are 3 to 10 times more expensive to install and operate than to purchase. In other words, products that may cost \$100,000 in licenses and annualized support but require \$500,000–700,000 in systems integration work are just not acceptable anymore to most midtier and large enterprises. However, very large enterprises will continue to view systems integration as a necessary component of building custom 3A and identity management solutions in order to gain a competitive advantage.

Increasingly, we believe that identity management will become a superset of 3A. Identity management will embrace all 3A software technologies and extend into directory services and hardware authentication devices as well. Granted, only a portion or percentage of 3A markets and submarkets can currently be attributed to identity management. However, over the course of our forecast, we expect many of these markets, such as Web SSO and provisioning, to be almost entirely consumed by or assimilated into the identity management market.

LEARN MORE

Related Research

- ☒ *Worldwide Firewall/VPN Software 2004–2008 Forecast: April 2004 Forecast* (forthcoming)
- ☒ *Worldwide Security 3A Software 2004–2008 Forecast: April 2004 Forecast* (forthcoming)
- ☒ *Worldwide Intrusion Detection and Vulnerability Assessment Software 2004–2008 Forecast: April 2004 Forecast* (forthcoming)
- ☒ *Worldwide Secure Content Management Software 2004–2008 Forecast: March 2004 Forecast* (IDC #30964, March 2004)
- ☒ *IDC's Enterprise Security Survey, 2003* (IDC #30653, December 2003)
- ☒ *North America Messaging Security Competitive Analysis, 2003: Regulatory Compliance and Spam Drive Spending* (IDC #30397, November 2003)
- ☒ *Worldwide Security Software Forecast Update and Analysis, 2002–2007* (IDC #30254, October 2003)
- ☒ *Worldwide Antivirus Software Forecast and Analysis, 2003–2007: Return of the Consumer* (IDC #29953, August 2003)
- ☒ *Worldwide Secure Content Management Forecast Update and Competitive Vendor Shares, 2002–2007* (IDC #29635, July 2003)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2004 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services: Security Products; Secure Content Management; 3As Security; Firewalls and Security Appliances; Intrusion Detection and Vulnerability Assessment