ABOUT SYMANTEC

Symantec, a world leader in Internet security technology, provides a broad range of content and network security solutions to individuals and enterprises. The company is a leading provider of virus protection, risk management, Internet content and email filtering, remote management, and mobile code detection technologies to customers. Headquartered in Cupertino, Calif., Symantec has worldwide operations in more than 33 countries.

WORLD HEADQUARTERS

20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 (800) 441-7234
1 (541) 334-6054
World Wide Web site:
http://www.symantec.com

Argentina: +(54) 11 4811 7526
Australia (Sydney): +(61) 2 9850 1000
Australia (Melbourne): +(61) 3 9864 2600
Austria: +43 150 137 5020
Belgium: +32 2 713 1700
Brazil: +(55) 11 5561 0284
Canada: +1 (416) 441-3676
Caribbean/Central America: +305 662 5899
China (Beijing): +86 10 6264 8866
China (Hong Kong): +(852) 2528 6206
Denmark: +45 35 44 57 00
Eastern Europe Sales Office (Munich): +49 89 9458 3000
Finland: +358 9 61507 465
France: +33 (0) 1 41 38 57 00
Germany: +49 (0) 2102 7453 0
India: +91 22 2880698
Italy: +39 (0) 2 6955 21
Ireland: +353 (0)1 811 8032
Japan: +81 3 5457 5300
Korea: +82-2-3420 8600
Luxembourg: +352 29 8479 5020
Malaysia: +(603) 705 4910
Mexico: +(52) 5 481 2600
New Zealand: +64 9 309 5620
Netherlands: +31 (0) 71 408 3111
Norway: +47 23 05 3300
Poland: +48 22 528 91 00
Russia: +(7095) 238 3822
Singapore: +65 239 2000
South Africa: +27 (0) 11 804 4670
Spain: +34 (9) 1662 4413
Sweden: +46 (0) 8 457 34 00
Switzerland: +41 (0) 52 244 39 39
Taiwan: +(886) 2 2739 9506
UK: +44 1628 592 222

SYMANTEC.™

02-71-00012

Internet Security for the Web:

Protecting Enterprise Networks from Malicious and Inappropriate Web-based Content

A SYMANTEC ENTERPRISE SECURITY SOLUTION

SYMANTEC.™

Table of Contents

Executive Summary 1

Introduction 1

Understanding content security 2

Why Internet content security solutions are needed 2

Security starts with effective policies 3

The importance of gateway-based solutions 3

Why firewalls are not enough 3

The hidden costs of Internet access 4

Productivity losses 4

Network performance costs 5

Corporate liability 5

Liability due to inappropriate content. 5

Could your company be convicted by employees' Web browser cache files? 6

Copyright infringement 6

Unknown losses 6

Emerging threats—the many faces of viruses and other malicious code 7

A brief history of the evolution of viruses and other malicious code 7

Viruses 7

Early viruses 7

Encrypted viruses 7

Polymorphic viruses 7

Trojan Horses 7

Mobile code attacks and vulnerabilities 8

Worms 8

Malicious code hybrids 9

Viruses and the Internet 9

A growing problem 9

Essential components of an effective solution 10

Enterprise-wide security and acceptable use policies 10

Effective, granular content and URL filtering and anti-virus tools, deployed at Internet gateways 11

Symantec Internet security for the Web 11

The importance of modular deployment 11

Symantec I-Gear 12

Symantec AntiVirus for Firewalls with Mobile Code Filtering Module 14

Norton AntiVirus Extensible Engine Technology (NAVEX™) provides industry leading fast antidotes to known and unknown viruses 14

Symantec's Striker™ patented detection system patrols the enterprise, seeking out known and unknown threats 14

Bloodhound™ 15

Symantec AntiVirus for Firewalls Mobile Code Extension 15

World class support and customer service 15

Summary 15

About Symantec 16

Executive Summary

The wide proliferation of Internet computing is raising new concerns for business enterprises. The World Wide Web has become an essential business communications tool. It supports intra- and inter-enterprise research and collaboration, and accelerated business processes. The productivity gains that Web-enabled enterprises may enjoy, however, are tempered by new concerns. Acceptable use policies notwithstanding, employees with Internet access may waste time and precious bandwidth accessing subject matter that has no bearing on business. In addition, certain subject matter may in fact be inappropriate for use or distribution within an enterprise, and may leave the corporation liable for a variety of lawsuits. Finally, enterprise networks may become vulnerable to infection, intrusion, and tampering via files such as cookies or other active content, which can be downloaded via the Web, often without the user's knowledge.

Enterprises now need strong protection and enforceable policies regarding Internet security and acceptable Internet use. While protection must be strong, it should not nullify essential business productivity gains. Automated, centrally managed, policy-based, Internet security tools implemented at Internet gateways can provide an answer to this dilemma. Ideally, these tools should permit the fine-grained control that is needed to allow maximum Web-based productivity while also implementing strong security. For maximum protection, they should include both essential content filtering technology and also strong anti-virus and malicious code prevention, detection, and repair measures.

This white paper explores the potential enterprise liabilities and network vulnerabilities associated with Internet access, as well as the characteristics of effective solutions. It further describes the steps that enterprises can take to deploy stable, scalable, efficient, and effective content-filtering and anti-virus measures at the Internet gateway. Finally, it illustrates how Symantec products provide the high-performance, comprehensive, flexible control and monitoring necessary for enterprises to achieve strong security while maximizing Web-based productivity and performance gains.

Introduction

In just the few short years that the Internet has been open to commercial use, it has fundamentally changed the nature of doing business across the globe. The business productivity gains offered by the World Wide Web and its ubiquitous, user-friendly interface (the browser) are undisputable. Through intranet, extranet, and Internet access, the Web has escalated intra-business and business-to-business (B2B) processes to new, previously unimagined, levels of speed and efficiency. Integrated supply chain product-to-market cycle times that once took months are being reduced to weeks—or even days. Real-time, virtually instant, communications and information exchange are now possible on a global basis.

The ubiquity of the Web and Web-based applications can open new back doors to corporate access. The connectivity that provides a basis for shared information with industry allies can also be a conduit for unauthorized access and the leaking of confidential information to unauthorized persons, either willfully or by neglect.

Employees may also expose enterprise networked computers to rapidly spreading viruses or other malicious or harmful code by accessing or downloading files of unknown origin. And, unlike earlier viruses, which were designed to infect single computers, the latest generation of viruses has been specifically designed to take advantage of the rapid propagation environments of networked computers and the World Wide Web. Proof-of-concept viruses, such as Melissa, Explore.zip, and LoveLetter have clearly demonstrated the potential of these threats to spread through entire networks within minutes.

In addition, the same virtual workspace that yields enormous business productivity gains has the potential to diminish worker productivity when used for the wrong purposes—or when placed in the wrong hands. The Web is alluring...and provides an easy distraction from business-related tasks.

Recent industry statistics indicate that employees squander both meaningful work hours and precious (and expensive) network bandwidth on Web-based activities that have nothing to do with business. In addition to incurring lost work hours, and negatively affecting network performance, these activities also leave the enterprise vulnerable to a variety of lawsuits. Enterprises may be held accountable for the information that resides in their networked computers, even when that information has no bearing on business and has been downloaded or accessed by an employee strictly for that employee's use.

To protect themselves from these threats, enterprises will need to implement a comprehensive Internet security program.

Understanding Internet security

Internet security is becoming an essential tool for doing business in the 21st century. While earlier vectors of delivering harmful content to an enterprise, such as physical access and file sharing via diskettes, are still a concern, the primary vectors for the introduction of harmful content into an enterprise have now shifted. Today, the two primary vectors for the delivery of harmful content to an enterprise are: Internet access and email. Protecting the enterprise from harmful content vulnerabilities due to Internet access is the topic of this white paper. Email content security, while still a primary area of concern, will not be discussed in any detail in this white paper, as it is the topic of another Symantec white paper.

Why Internet content security solutions are needed

The following highlights of the Computer Security Institute (CSI)/FBI 1999 Computer Crime and Security Survey are revealing:

- System penetration by outsiders increased for the third year in a row; 30% of respondents report intrusions.
- Those reporting their Internet connection as a frequent point of attack rose for the third straight year: from 37% of respondents in 1996 to 57% in 1999.
- Insider abuse of Internet access privileges (for example, downloading pornography or pirated software or engaging in inappropriate use of email systems) was reported by 97% of respondents.
- 26% of respondents reported theft of proprietary information.

Security starts with effective policies

Security breaches can occur from both within and outside of an organization. All good security efforts start with developing reasonable and effective policies. These policies are a critical first step in protecting vital enterprise information assets. They can also be used as a defense against potential legal liabilities. Today, enterprises must define or redefine their security policies to include rules regarding Internet access and acceptable use.

Even with these policies in place, however, some means of enforcing them must be available. Manual enforcement methods are easily defeated. And because Internet/intranet/extranet access is a necessary prerequisite for business in the 21st century, there is a danger of too much security constraining the business—in effect throwing out the baby with the bath water.

The importance of gateway-based solutions

Appropriate, gateway-based solutions can provide a needed answer to this dilemma. Automated, granular, policy-based solutions can assist the enterprise in providing an effective means to administer and enforce Internet access and appropriate content rules, while still allowing Web-based productivity. Deployment of this technology at Internet gateways allows enterprises to control threats before they have a chance to spread to essential network data and applications behind the firewall.

Centrally managed, granular, policy based solutions provide the enterprise with maximum control and maximum flexibility. In addition, such solutions are highly scalable and can greatly reduce administrative overhead. These measures, when combined with other network security measures, such as email, desktop, and server security, constitute the total Internet security solution that doing business in the 21st century will increasingly require.

Why firewalls are not enough

It's important to note that in today's Internet-enabled business environment, firewalls alone are no longer sufficient to provide all of the levels of security that are needed. Firewalls are generally very effective at keeping unwanted people out of enterprise networks. They do this by establishing what types of network connections will be allowed and what session services will be supported. This works well when the boundaries of the network are clearly defined, and when there is either limited or no need for collaborative computing.

Today's Web-based business processes, however, have changed the rules for enterprise computing. Enterprises increasingly need to be able to allow and control more applications. With each new application allowed, the risk of security holes is multiplied. With each new user, there is also an increased risk of tampering, misuse, and information falling into the wrong hands, either willfully or by neglect. With access being extended to enterprise partners, customers, and suppliers, a centrally managed solution is needed to control system complexity. Policy-based granular controls are also needed to enable the many levels of limited access that will now be required.

In addition to being able to control *who gets in* to view sensitive information residing behind enterprise firewalls, enterprises must also be able to control *what information gets out*. Attacks or intrusion may originate from within or without conventional enterprise

boundaries. Statistics now show that a great many security breaches originate from behind the firewall—from within the enterprise itself. To protect confidential enterprise information from falling into the wrong hands, the ability to monitor the content of files leaving the network is just as important as the ability to monitor files coming in. This is an area where firewalls typically fall short.

Although firewalls may be able to impose some constraints on exporting information via protocol blocking (such as disallowing Internet Chat through IRC connections), these efforts could still be defeated through the use of other protocols. And firewalls, in general, are incapable of exercising the fine-grained content controls needed to monitor and block unauthorized exporting of information as well as unauthorized access. Finally, firewalls don't natively support anti-virus measures or granular monitoring and control of today's mobile code files, such as Java applets or ActiveX com files. However, these files can contain harmful content capable of crippling enterprise networks.

Gateway-based content filtering and strong gateway-based anti-virus measures will both be required to ensure adequate enterprise protection.

The hidden costs of Internet access

Unauthorized and inappropriate use of the Internet by employees, and exposure to viruses or harmful code, can impact the enterprise in a number of different areas.

These include: 1) Productivity, 2) Network performance, 3) Corporate liability, and 4) Unknown losses.

Let's examine each of these, in turn.

Productivity losses

The lure of the Web is undeniable. Its potential for distracting employees is immeasurable. When employees access subject matter that has no bearing on business, they waste both valuable work hours and precious network bandwidth. Unfortunately, this practice is very widespread. In the 1999 CSI/FBI Computer Crime and Security Survey listed above, fully ninety-seven percent (97%) of companies reported that their employees abused Internet access. And a recent survey conducted by the Saratoga Institute of Human Resources revealed the following statistics:

- Nearly 70 percent of companies surveyed had more than half of their employees online.
- Almost all companies had Internet access policies (IAP) in place (82.6 percent), outlining appropriate and inappropriate use of the Internet in the workplace.
- Despite IAPs, more than 60 percent of American companies have disciplined—and more than 30 percent have terminated—employees for inappropriate use of the Internet.
- Accessing pornography, chatting online, gaming, investing, or shopping at work are the leading causes for disciplinary action or termination.

In other surveys, employees have admitted to surfing the Web during work hours.

Nielsen-NetRatings offer remarkably consistent statistics: employees spend more than one hour per workday surfing the Web for personal reasons.

The Saratoga Institute of Human Resources estimates that a company with 1,000 employees who use company Internet access one hour per day for personal surfing can cost a company upwards of $35 million each year in lost productivity. Extrapolate this figure to the Fortune 1000 and you have a multi-billion dollar issue.

Network performance costs

According to the Gartner Group, "Bandwidth consumption within organizations is doubling every 90 to 180 days." Yet, according to industry statistics and employees' own reports, an alarming percentage of expensive Internet access bandwidth carries Web traffic that serves no useful purpose for the corporation. This unauthorized bandwidth usage may result in business network slowdowns and bottlenecks that choke legitimate network traffic and cause the productivity levels of employees engaged in meaningful business activities to suffer. In addition, the business may end up investing critical business dollars in adding still more bandwidth which is not necessary to support the business.

Applications that make *sustained* use of company Internet access also negatively impact business performance. Consider streaming media: Internet Radio, Pointcast/EntryPoint, and stock ticker agents are applications that have been carefully designed to operate in the consumer (modem) environment, so individually use relatively small amounts of bandwidth. Now multiply the 20-30 kilobits per second for Internet Radio broadcasts delivered to even 10% of employee desktops through a Windows Media Player over enterprise LANs in a large corporation. It's easy to demonstrate how megabits per second can be sapped away from productive and mission-critical applications.

According to ZDNet, "The cost to businesses from Internet broadcasts of the October 1998 Starr report alone was in excess of $450 million."

Corporate liability

Liability due to inappropriate content

Increasingly, the receipt, mishandling, re-posting, or forwarding of subject matter that is considered inappropriate for consumption or distribution within an enterprise—from religion to pornography to sites promoting hate, violence, and ethnic-cleansing—may leave a company liable to expensive lawsuits and/or expose the company to embarrassing and costly publicity.

Employers may be held accountable for failure to enforce federal, state, and local laws regarding sexual harassment, discrimination, child pornography, as well as corporate policies that are enforced for other media (postal mail, broadcast radio, and telephone use). An employee who downloads and displays child pornography on a monitor is just as much in violation of a federal law prohibiting possession of the same vile material. An employee who tunes into an Internet Radio hate-station that debases women or minorities is similarly in violation of a company policy against harassment and discrimination.

Could your company be convicted by employees' Web browser cache files?

As the Microsoft trials have illustrated, companies are liable for content that exists in their databases. In Microsoft's case, the damaging files were in the company's email. However, this same liability may be extended to cached HTML pages and images, if these files can serve as evidence of threats and abuse. While this is still a legal gray area, there have been a number of cases in which, based on allegations or suspicion of activities involving child pornography, computers were seized by federal agents. Cache files were used to prove access and storage of the pictures, and later as evidence of criminal activities. In one international child-pornography sting operation called Operation Ripcord, computer servers owned and operated by two Internet Service Providers (ISPs) were seized. Although neither ISP was ultimately convicted, both incurred costs for legal fees, equipment replacement, service interruption, and negative publicity. Even in the absence of criminal charges, stored files can be used as the basis for costly civil litigation by employees, customers, and third parties.

Copyright infringement

Employers may be liable for actions of employees who download illegal copies of MP3 files or software from piracy sites over corporate networks. United States law, based on Constitutional Article I, Section 8, protects a person's right to control the reproduction and distribution of his or her creative works like books, songs, and movies. The law describing these rights and their limitations is included in Title 17 of the U.S. Code. Recently, Temple University paid the Business Software Alliance (BSA) $100,000 to settle claims related to unlicensed software programs on its computers. In addition to the settlement, Temple University has agreed to destroy all unlicensed software, purchase replacement software, and strengthen its software management policies. The City of Issaquah, Washington, also agreed to pay the BSA $80,000 to settle claims related to unlicensed software installed on its computers.

Unknown losses

Since the origin of content downloaded from the Internet cannot always be verified, there is an increased risk of infection through network-borne viruses, worms, Trojan Horses, and other forms of malicious code. In addition, with the widespread availability and ease of programming provided by today's mobile code languages, such as Java or ActiveX, it is now more likely than ever that employees surfing the Web may unknowingly download cookies or applets (small programs) containing self-executable active programming onto business networks. This programming could be aimed at rendering enterprise networks useless—or it could be used to make the business network more vulnerable to hackers and information thieves.

Programming code authorizing various aspects of remote access and control of business networks by hackers may reside unnoticed in cookies or applets, which can be downloaded in a process that is transparent to the average user. Although Web browsers contain some built-in safeguards in the form of warnings to protect against this, these safeguards may be disabled at the desktop, or warnings may go unheeded by employees who do not know how to interpret them. Employees may also download what appears to be a legitimate program. However, this program may carry within it a hidden intent (Trojan Horse program) to make the network or its confidential business information more available to hackers. In these cases, the potential loss to business enterprises is inestimable.

How likely is this scenario? According to John Christensen, reporting for CNN on April 6, 1999, "There are about 30,000 hacker-oriented sites on the Internet, bringing hacking—and terrorism—within the reach of even the technically challenged."

Emerging threats—the many faces of viruses and other malicious code

The Internet poses the most daunting environment yet for anti-virus measures. To appreciate just how daunting, let's take a brief look at the history of viruses, how they have evolved to date, and what anti-virus experts predict the future of viruses portends.

A brief history of the evolution of viruses and other malicious code

Viruses

A computer virus is a small program designed to replicate and spread, generally without the user's knowledge. Computer viruses spread by attaching themselves to other programs (e.g., word processor or spreadsheet application files) or to the boot sector of a disk. When an infected file is activated—or executed—or when the computer is started from an infected disk, the virus itself is also executed.

Early viruses

The earliest viruses were and are relatively easy to detect. Each virus contains unique, identifiable, strands of programming code. Anti-virus researchers recognized this, and called these unique identifiers the virus's "signature." Once a virus's signature is detected by an anti-virus scanning engine, the virus can be identified and eliminated from the system.

Encrypted viruses

Virus writers responded to the defeat of simple viruses by encrypting new viruses—hiding their signatures by writing them in indecipherable code. These viruses need to return to their original state, however, in order to replicate. So the writers of these viruses needed to attach a decryption routine to the viruses. Eventually, anti-virus researchers found they could use the decryption routine itself as a virus signature. This feature allowed a virus to be detected by an anti-virus scanning engine.

Polymorphic viruses

Polymorphic virus writers still encrypted the virus, but now they introduced a mutation engine: code that generated a randomized decryption routine. This raised the detection bar for anti-virus researchers, who now had to contend with a randomly generated decryption routine in each new infected program. Ultimately, anti-virus writers devised various methods to trick a polymorphic virus into decrypting itself. Symantec's Striker System is an example of one of these methods.

Trojan Horses

The Trojan Horse virus typically masquerades as something desirable—for example, a legitimate software program. Like its classical namesake, however, it delivers a hidden payload. The Trojan Horse generally does not replicate (although researchers have

discovered replicating Trojan Horses). It waits until its trigger event and then displays a message or destroys files or disks. Because it generally does not replicate, some researchers do not classify Trojan Horses as viruses—but that is of little comfort to the victims of these malicious strains of software. Recently, the incidence of Trojan Horses has been increasing.

Mobile code attacks and vulnerabilities

Mobile code, as defined by the World Wide Web consortium, is "(programming)[1] code that can be transmitted across the network and executed on the other end." Mobile code may be created using one of numerous mobile code systems, including Java, ActiveX, safe Tcl, Visual Basic, Visual Basic for Applications (VBA), and scripting. All of these systems can be used by developers to create small self-executable programs (dynamic content) that can be embedded in Web documents.

When used for a positive purpose, mobile code provides valuable content and time-saving features to applications and Web pages. These same features, however, can be used for negative purposes. Because of this, mobile code attacks in the making are difficult to detect. Companies could protect themselves by unilaterally banning any programs that use these languages from the network—but they would pay a high price in terms of lost productivity. In addition, these programs are becoming such an important part of Web-based business processes, that it may be impossible for companies to maintain a sustained competitive advantage without them. Instead, enterprises need a discerning set of finely grained, behavior-based policies and controls that can isolate suspicious mobile code files while allowing legitimate programs to run as needed.

Worms

The *computer worm* is a program that is designed to rapidly copy itself from one computer to another, leveraging some network medium: email, TCP/IP, etc. According to Cary Nachenburg, Chief Researcher at the Symantec AntiVirus Research Center (SARC), "Worms are insidious because they rely less (or not at all) upon human behavior in order to spread themselves from one computer to others."

"Most viruses," Nachenberg says, "rely on some type of user trigger, such as opening an attachment, rebooting a machine, or launching a program. Worms, however, may be able to operate more independently. An example of this is the Explore.zip virus, which can identify widely used group email programs, such as MS Outlook, that may exist on a client's computer, and systematically start sending itself to everyone on the user's email list."

"In addition," Nachenberg says, "The worm is more interested in infecting as many machines as possible on the network, and less interested in spreading many copies of itself on individual computers (like earlier computer viruses)."

Worms are generally classified as either email worms or protocol worms, depending on the primary vector by which they spread. Either type may be knowingly or unknowingly downloaded via the Web.

"Computer viruses have progressed from urban myth to annoyance to major threat," says Nachenberg, "Yet, even with all the damage that computer viruses have done, they pale in comparison to what we have seen and have yet to see from the computer worm."

Malicious code hybrids

Virus and malicious code developers have already succeeded in developing new virus hybrids, that combine the best (or worst, depending on your point of view) features of several types of malicious code into one exponentially more lethal product. Explore.zip, Melissa, and Babylonia 95 are all examples of the hybrid virus types that are likely to become more prevalent in the future. What is most sinister about these viruses is the speed at which they can spread throughout entire networks.

Once a virus infects a single networked computer, the average time required to infect another workstation is 10 to 20 minutes—meaning a virus can paralyze an entire enterprise in just a few hours.

Viruses and the Internet

With information now travelling quickly over the information superhighway, the problem becomes even more pronounced. Viruses can travel across the world with a single mouse click. Over intranets, extranets, and the Internet, viruses from one enterprise can travel to thousands of others. Entire groups of networks can be instantaneously affected.

The Internet was designed for the rapid propagation of data. It makes no distinction between good or bad data. Viruses and other forms of malicious code can be transported across it just as effectively as other information.

While most attention is focused on email-borne viruses and worms—and statistics corroborate this is currently the primary area of concern—malicious code is increasingly finding its way into the enterprise through Web browsing and Internet downloads.

A growing problem

In addition to the speed at which computer networks can now become infected with a virus, the number of different viruses in existence is increasing at an unprecedented rate. In 1986, there was one known computer virus; three years later, that number had increased to six. By 1990, however, the total had jumped to 80. Today, between 10 and 15 new viruses appear every day.

In a press release issued in June of 1999, Adam Harriss and Catherine Huneke of *Computer Economics, Inc.*, a research firm in Carlsbad, California, stated, "The economic impact of virus and worm attacks on information systems has increased significantly this year, with businesses losing a total of $7.6 billion in the first two quarters of 1999 as a result of disabled computers."

And a survey of 2700 information technology professionals in 49 countries, conducted by *Information Week* in June of 1999, revealed the following statistics:

- Globally, about 64% of companies were hit by at least one virus in the past 12 months, up from 53% the year before. In the United States, viruses affected 69% of companies.
- A year ago, half of the companies surveyed said they suffered no system downtime as a result of security breaches. This year, only 36% could make that claim.
- Viruses hit 69% of companies with revenue of more than $500 million.

Essential components of an effective solution

Enterprise-wide security and acceptable use policies

In order to protect themselves against potential losses and liabilities, enterprises must establish security policies that define acceptable use of Internet/intranet/extranet access privileges and require virus countermeasures. The policies should also determine at a fine-grained level any variations in access privileges and appropriate use, which may depend upon various combined factors such as: job title, current work projects, need to know, and level of trust within the organization.

Policies must be sufficiently granular to protect resources at the highest risk without adversely impacting employee productivity. Different rules may be needed at organization, server, group, and even user levels. Such policies may dictate enterprise-wide deployment of measures like firewall port blocking, disabling execution of active Web content (mobile code), and anti-virus detection at the desktop, server, and firewall. Policies may also prohibit employee access to pornographic or hate Web sites, online shopping, or MP3 music file download sites, and define penalties for inappropriate use. Policies will need to be based on an assessment of business needs and risks within the organization.

Security is based on limiting access, while collaborative computing requires that access to certain information be shared. Enterprises will need to define the rules needed to establish the most appropriate balance within their organization.

Once established, security policies must be monitored and enforced. Yet, a poll conducted by Network Computing indicates that more than a quarter of respondents do not use any tool to enforce security policy. Another quarter simply spot-check employee activity. Such practices leave the door wide open for non-conformance. Monitoring by managerial oversight is not only inefficient but wholly inadequate as protection against litigation. Desktop security measures can be ignored, misconfigured, or disabled. A single unprotected PC, exploited by a self-propagating worm, exposes the entire enterprise to risk. Policy enforcement can only be assured through software automation.

Robust, cost-effective, policy implementation is best accomplished by applying a company's written security policy to software solutions designed to monitor and enforce Internet content security measures at every level: on the desktop, at key servers, and at every Internet gateway. Although desktop and server security continue to be important, countermeasures against unauthorized content and malicious code are most effectively and efficiently deployed at Internet gateways, through the firewalls operating as the first and last entry to the enterprise network.

Content filtering and monitoring tools applied at Internet gateways can also help the enterprise to proactively identify both potential threats. Monitoring enterprise Internet usage at baseline without filtering can help network administrators to determine where filters need to be applied and where policies need to be developed.

Effective, granular content and URL filtering and anti-virus tools, deployed at Internet gateways

These tools should have as many as possible of the following characteristics:

- Minimal or no performance degradation
- Flexibility, granularity
- Reliability and efficiency
- Scalability
- Ease of integration
- Automated updating
- Strong logging and auditing capabilities
- Rapid response
- Centralized management, ease of administration
- Uninterruptable service

Symantec Internet security for the Web

Symantec AntiVirus for Firewalls™ and Symantec I-Gear™ are part of Symantec's multi-layered approach to total Internet security. Symantec offers a complete suite of products that enable consistent, enterprise-wide, policy-based security for both Web and mail traffic. To maximize performance and allow flexible deployment, Symantec's solution is highly modular.

Symantec's Internet Security for the Web solution comprises the following components:

- **Symantec I-Gear** controls Web-delivered content through both a list-based and dynamic, multilingual, context-sensitive filtering and monitoring technology that enables safe use of search engines, anthology sites, and Web pages.
- **Symantec AntiVirus for Firewalls (includes Mobile Code security)** applies Symantec's award-winning, market-leading, intelligent virus protection solution to Web-borne threats detected at any firewall.

The importance of modular deployment

Symantec Internet Security products may be used singly or in combination to offer high-performance security for real-time Web traffic. Other solutions tightly couple Web and email security within a single platform, creating a choke point that causes unacceptable delay for Web traffic. Symantec provides email content security filtering via separate email software components within its total enterprise security solution. Not only is performance degradation minimized, but through intelligent caching, enterprises may realize enhanced network performance.

Symantec I-Gear™

Flexible, granular, dynamic Internet access and content controls

Extensive logging and reporting, with automated policy enforcement tools and transparent auditing

I-Gear provides user-transparent auditing of Internet usage and detailed reporting on user, client, and group activity. Extensive logging and reporting features are key to protecting your company from litigation brought on by those offended or sensitive to discriminatory material introduced through the Internet. I-Gear's activity logging provides the reliable audit trail required to identify problem employees and take corrective action.

With AutoLock and AutoAlert, violation thresholds can be set for automatic lockout after repeated blocking of the same user or client, and automatic policy violation email notification can be sent to designated recipients.

Logging functions can also assist an enterprise in developing acceptable use policies. An organization can start out with just the monitoring function to develop a baseline view of Internet use patterns. Appropriate policies can then be developed taking into consideration both needed access and key violation areas.

Policy-based management

Finely grained policies are configured through an object-oriented interface whereby rulesets are defined for clients, users, groups of users or clients, or the entire system. Each ruleset includes a prioritized set of URL-based control lists, dictionaries, and context rules that allow or deny access. Policies can be scheduled or associated with repeated or one-time events.

Access control, context sensitive keyword and URL filtering

I-Gear provides customizable access permissions and granular content and URL filters for individual users, client computers, and groups. Group policies can be specified for a quick solution, while exceptions allow for complete customization to accommodate special needs.

These controls can implement policies that permit legitimate URL access for departments that need this—for example, comptroller access to finance sites or marketing access to strategic news—while blocking inappropriate access to these same sites by others. I-Gear even permits selective blocking of inappropriate keywords within legitimate sites.

Dynamic Document Review (DDR)—Symantec's patented, context-based, dynamic content filter

Intelligent context-based content scanning allows I-Gear's Dynamic Document Review (DDR) to go beyond the capacity of static list-based filters. DDR not only scans pages, searching for objectionable words and phrases, it also scans the *context* in which these words or phrases are used, dynamically blocking material based on configured policies. Dynamic Document Review helps to provide the most accurate and comprehensive filtering *where*, for *whom,* and even *when* filtering is desired in an organization.

Flexible scheduling

I-Gear policies can also incorporate time of day and day of week for single or recurring events. For example, an enterprise can block all Internet access during non-working hours to avoid liability due to unsupervised, unauthorized, desktop use. Or if there is a need to selectively permit access during non-work hours, the corporation can configure policies that require passwords for Internet access, and apply reasonable timeouts to protect against unattended use.

Comprehensive—and growing—pre-defined content lists, with selective permissions and customization/exception options

I-Gear uses an extensive set of predefined Content Category Lists and an unlimited set of locally-defined lists. I-Gear's comprehensive database identifies hundreds of thousands of Internet sites. Content is divided into Super- and Sub-Categories that make it easy to implement acceptable use policies. Top-level categories include Crime, Drugs, Entertainment, Interactive (Mail and Chat), Intolerance, Job Search, News, Sex, Sex Education, Violence, and Weapons. The pre-defined lists are totally customizable allowing administrators to override Web sites or add sites locally without contacting Symantec. Local administrators can also create their own categories and populate them with URLs to meet their organization's policies. The lists are updated automatically each night and Symantec is constantly expanding the number of categories.

Ability to scan both HTTP and FTP traffic

I-Gear incorporates both HTTP and FTP scanning. Many content filtering products only block HTTP traffic. With these products, potentially harmful software downloaded by employees via FTP would be ignored.

Deployment flexibility—multi-platform high performance proxy/caching server

For maximum deployment flexibility, I-Gear includes a built-in, high-performance transparent proxy/caching server for Windows NT™ Server 4.0, Windows™ 2000, or Solaris™ operating systems.

Ability to restrict downloads/scan for viruses

I-Gear also allows administrators to selectively restrict the ability to download files such as executables, movies, sound, and more via HTTP and FTP. When Symantec Anti-Virus for Firewalls is used in conjunction with I-Gear, permitted file downloads can also be scanned for viruses.

Dynamic caching speeds performance, reduces bandwidth consumption

When operating as a proxy server, I-Gear not only provides content filtering as an Internet gateway, but it can also store (cache) retrieved content. Caching reduces Internet bandwidth consumption, allowing local users to share stored copies of popular content. According to caching.com, as a rule of thumb, caches have a "hit" rate of 35%, which means they reduce upstream traffic on the network by that same percentage. I-Gear also supports hierarchical proxy chaining for more efficient distribution of stored content across the network.

Symantec AntiVirus for Firewalls with Mobile Code Filtering Module

Award-winning, market-leading continuous detection, prevention, and repair of known and unknown virus and other malicious code activity
Symantec AntiVirus for Firewalls, built on Norton technology, operates as a company's first and last line of defense against Web-borne viruses, worms, and malicious code. Its efficiencies work together with Symantec desktop AntiVirus products, and server solutions such as Norton AntiVirus for NetWare® and Notes to inoculate the enterprise from virus threats at every possible port of entry.

Quarantine Console, with Digital Immune System™ technology provides the fastest anti-virus turnaround in the industry
Once suspicious activity has been detected, Symantec AntiVirus for Firewalls employs Symantec's Digital Immune System technologies—Quarantine Console and Scan and Deliver—to provide the fastest turnaround in the industry.

Before they can do any damage, the suspect files are deflected to the Symantec System Center's Central Quarantine, where they are safely stored until further notice. IT administrators are notified of the event and have an opportunity to test and check the suspected files before emailing them to the Symantec AntiVirus Research Center (SARC™).

Upon receipt, SARC emails a confirmation, with tracking number, back to the submitter. Engineers at SARC analyze the virus with Symantec AntiVirus Research Automation (SARA™) technology, producing a cure (a virus definition). The definition is mailed back to the IT administrator, who may test the cure on the suspect files held in Quarantine. Once the cure has been proven safe and effective, the virus definition is made available by the Symantec Centralized Management Console for enterprise-wide deployment.

Norton AntiVirus Extensible Engine Technology (NAVEX) provides industry leading fast antidotes to known and unknown viruses

Norton AntiVirus Extensible Engine Technology (NAVEX) is a modular virus-scanning engine that lets engineers in the Symantec AntiVirus Research Center (SARC) quickly formulate and distribute antidotes efficiently and effectively. You not only get virus fixes faster, you get them in a form that's smaller and easier to deploy enterprise-wide. And all Symantec AntiVirus products can be upgraded with new NAVEX engines or virus definitions without the application update, scanner shutdown, or system reboot required by other products—which results in savings in time and money.

Symantec's Striker patented detection system patrols the enterprise, seeking out known and unknown threats

Symantec's Striker detection system is highly effective at finding known and unknown threats, including worms, malicious code, and even mobile code. Striker offers multi-level detection, based on signatures, static and dynamic heuristics, and generic decryption of polymorphic viruses. But unlike other products, Striker speeds detection and resolution by applying profiles—rules that can identify entire classes of viruses.

With LiveUpdate™, your network and Symantec AntiVirus are always "on"
Scheduled or one-button LiveUpdates—a component of every Symantec AntiVirus product—assure up-to-date protection without interruption of daily activities. This automated workflow allows Symantec to provide the industry's most cost effective mechanisms for incident response. Over 90% of viruses submitted to SARC since August 1998 were cured in under 9 hours—even with a submission rate averaging over 5000 events per month.

Scans and disinfects compressed and uncompressed files
Symantec AntiVirus for Firewalls scans and disinfects both compressed and uncompressed files.

Bloodhound
Symantec's patent-pending Bloodhound hybrid technology is capable of detecting 80% of new and unknown executable file viruses.

Symantec AntiVirus for Firewalls Mobile Code Extension
The Mobile Code Extension adds a new level of protection against malicious software by combining Symantec's anti-virus engine, which automatically detects any known Java or ActiveX threat, with a Digital Signature Verification (DSV) engine allowing security administrators to manage Internet-borne code based on its signature. The DSV engine checks the presence and integrity of a digital signature on any incoming code (ActiveX, Java classes, CAB files, etc.), allowing administrators to block unsigned code or code that has potentially been tampered with.

World class support and customer service
All of this is backed with Symantec's "customer first" vision and commitment: your enterprise gets unbeatable support, backed by industry leading consultation and risk assessment capabilities, as well as vulnerability testing capabilities and highly available onsite or Web-based training.

In addition, Symantec is able to provide:

- Security and acceptable use policy development assistance
- Enterprise-quality installation and operations support
- Network performance consultation (in relationship to the installation and customization of its Web Security tools)
- Multi-language, multinational support from locations in more than 24 countries, worldwide
- Additional content security tools, including solutions for desktops, file servers, and email gateways

Summary

Web-based business processes and Internet connectivity bring with them many business advantages. However, Web-based productivity advantages may be tempered by

new concerns about enterprise network security. Desktop security solutions, while necessary, will not protect the enterprise from the latest wave of Internet-based threats. Firewalls, while effective at protecting the enterprise from a number of threats, can be enhanced, with the addition of new, finely tuned, proactive content security and virus control measures.

Today there is a compelling need for enterprises to implement a multi-layered, complete content security solution for the entire organization. This should include both fine-grained content and URL filtering; monitoring and reporting solutions; and strong anti-virus solutions; all capable of being deployed at Internet gateways.

Symantec is uniquely positioned to assist the enterprise in achieving the best possible solution to protect the enterprise against today's—and tomorrow's—Internet-based threats. Symantec AntiVirus for Firewalls and Symantec I-Gear content and URL filtering software constitute a leading edge, highly scalable solution that is always on, eliminating system downtime due to upgrades and maintenance. Updates are provided automatically—and in Internet time. Symantec also backs this product expertise with world-class support and consultation capabilities, including a full spectrum of multinational support, available in more than 24 countries.

About Symantec

Symantec, a world leader in Internet security technology, provides a broad range of content and network security solutions to individuals and enterprises. The company is a leading provider of virus protection, risk management, Internet content and email filtering, remote management, and mobile code detection technologies to customers. Headquartered in Cupertino, Calif., Symantec has worldwide operations in more than 33 countries.

Symantec serves more than 50 million customers around the world, including some of the world's largest corporate enterprises, government agencies, and higher education institutions. Ninety-eight of the Fortune 100 companies rely on Symantec solutions every day. The company holds numerous patents and awards, establishing it as a world leader in the product areas it represents.

Symantec is committed to providing uncompromising quality in everything it does. This includes providing best in class service and support to customers. Its products and solutions are available in over 15 languages.