

## WHITE PAPER

---

# Cost-Effectively Blocking Undesired Web and Email Traffic at the Gateway

Sponsored by: Trend Micro

---

Brian E. Burke

Gerry Pintal

Christian A. Christiansen

November 2006

## IDC OPINION

All businesses, large and small, face the same types of potential Internet security breaches. However, the manner in which small and medium-sized businesses (SMBs) protect themselves from these threats varies greatly.

Large enterprises are able to establish, fund, and staff security-specific groups whose charters are dedicated to architecting, managing, and maintaining secure corporate infrastructures. In many cases, tens of millions of dollars are allocated to ensure optimal service levels of corporate infrastructure security.

In sharp contrast, SMBs, by necessity, focus the lion's share of their financial and human resources on funding, managing, growing, and competing for market share in their respective industries. Consequently, the resources available on an ongoing basis to acquire, design, deploy, and support their security infrastructures are, in many cases, in short supply. As a result, information security among SMBs is primarily approached reactively rather than proactively.

IDC believes it is imperative for SMBs to seek security solutions that proactively address not only the emerging threat environment but also the management and operational cost issues facing them. In today's ebusiness environment, Internet security is an absolute necessity for conducting business.

## METHODOLOGY

To gain insights into the emerging security challenges and costs facing SMBs and to learn more about how organizations address these challenges, IDC conducted in-depth interviews with executives at companies in several industry sectors. These organizations operate in construction, mining, and managed security services. In addition, IDC met with Trend Micro's management team to review its goals and strategies for addressing customer challenges. This white paper uses all of these research perspectives to create a view of real-world challenges and solutions.

## IN THIS WHITE PAPER

This white paper provides line-of-business managers and midsize company executives with a deeper look at gateway security and the emerging threat environment. It offers a realistic view of the critical ingredients needed for optimizing a security architecture. The document presents perspectives on the evolving demands for gateway security solutions, including those essential to controlling spyware, viruses, worms, privacy, and compliance regulations. It also outlines emerging solutions to deal with the increasing complexity and sophistication of threats and emphasizes the need to minimize administration and labor costs.

## SITUATION OVERVIEW

---

### **The Challenges for SMB Information Technology**

#### ***Finding the Optimal Balance***

As discussed earlier, SMBs in many cases are faced with the ongoing challenge of establishing the highest levels of security while having to work with limited available human and capital resources.

Dedicating valuable technical staff to ensure the highest levels of 24 x 7 security for their businesses never seems to be feasible for SMBs. On the other hand, they face the risk that a single and unfortunate security breach can inflict severe damage to their companies.

Faced with ever-increasing numbers and types of security threats, SMBs are in a constant struggle to find the optimal balance between investing in human and capital resources for the growth and survival of the business and security.

As a consequence of the lack of resources, the security infrastructures of SMBs are virtually nonexistent, minimal, or outdated. In many cases, these businesses may simply have a central firewall and antivirus software installed on all or selected workstations and laptops.

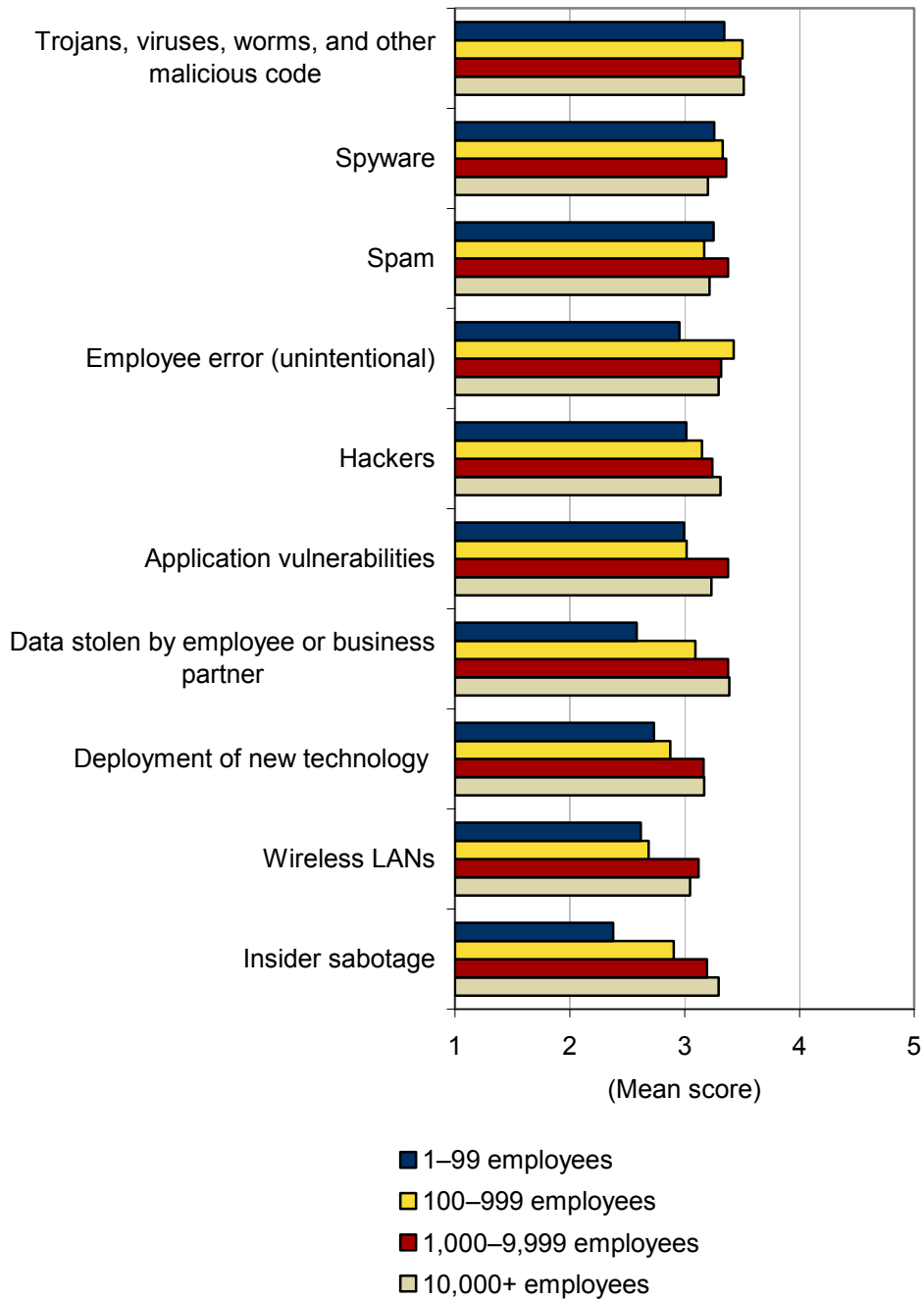
As these businesses grow, their minimal security infrastructures soon become inadequate in providing protection against the onslaught of Internet-borne threats that continue to attack in increasingly more diverse and sophisticated ways.

#### ***Security Concerns***

According to IDC's 2006 security survey, malicious code types top the list of leading concerns among IT management and administrators. Figure 1 contains a summary of the top responses given by IT managers who were asked to rate the threats that most concern them and their companies. As noted, spyware is now a leading threat to businesses. Spyware can expose businesses to theft of confidential data and degraded computing performance, and it can result in increased help desk call volumes.

**FIGURE 1**

Top Threats by Company Size



n = 430

Note: Threat sources are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC, 2006

### ***Go for the Money***

What compels hackers to do what they do? Their goals have changed significantly over the years. Malware developers and other mal-intentioned individuals previously competed solely for notoriety or to wreak havoc on computer systems just for the "fun of it." Today, a new generation of individuals and groups has emerged for whom financial gain is the primary driving force behind their developing spyware, phishing, worms, and other forms of malware.

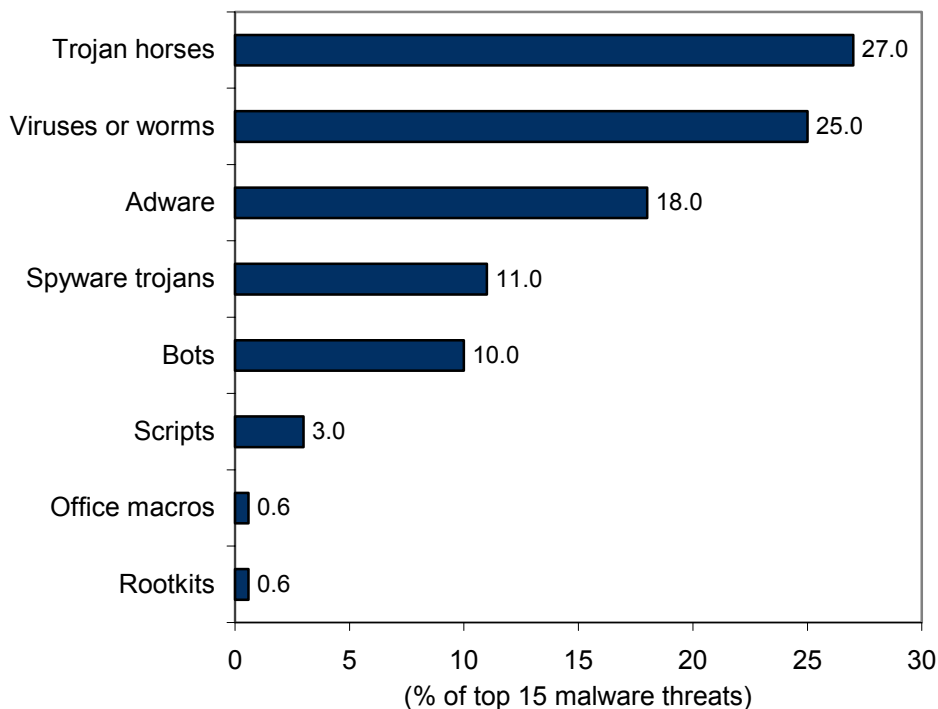
Much like a natural disaster, a security breach can be a very expensive business risk for companies of all sizes. A serious breach can damage a company's reputation and brand and consequently result in the loss of customers and revenues. Other business risks include loss of investor confidence, the potential for regulatory fines, and even litigation.

### ***Threat Protection***

Figure 2 provides a perspective on the eight prominent malware threat types in 2005 as a percentage of the top 15 malware threats.

**FIGURE 2**

Top Malware Threats



Source: Trend Micro, 2005

The following is a brief summary description of the most common methods of defense against the most common threat types.

### **Antivirus**

Viruses continue to plague businesses with outbreaks that sometimes inflict damages estimated in billions of dollars. When signatures are updated frequently, antivirus software that is implemented at the gateway will identify and eliminate malicious software — such as viruses, trojans, and worms — before it works its way onto a company's network and into exposed PCs and servers. Software that scans HTTP, FTP, POP3, and SMTP protocols for viruses and spyware at the gateway is an essential component of an antivirus system.

### **Antispyware**

Spyware was once considered just an annoying advertising mechanism that deluged users with pop-ups. Spyware developers can make a lot of money from selling or exploiting the data and passwords that they steal from individuals and businesses. Spyware is a particularly dangerous threat because it can monitor keystrokes, eavesdrop on email, and scan files on hard drives. More invasive spyware can crash the operating system, alter registry settings, and destroy the privacy of a company's most trusted information. IDC believes that 40% to 50% of all help desk calls are currently related to spyware.

Spyware is also a major threat to network and PC performance. When network and PC performance is affected by spyware, employee productivity suffers. Spyware can consume large amounts of system bandwidth. An effective antispyware system is absolutely essential in eliminating this form of threat.

### **Antispam**

Spam is an ever-increasing threat and an easy vehicle for hacker attacks. Antispam systems are able to significantly reduce the number of junk emails entering into a company's network. For a company without an antispam system in place, these messages can also carry undetected payloads such as worms, viruses, and any other form of spyware sent to infect a company's machines.

Emails have become an effective form of rapid communication for most business and private users. Unfortunately, emails have seriously eroded from being an efficient communication vehicle to plaguing users with a constant barrage of junk. It is estimated that in companies without spam filtering, more than 80% of emails received today are some form of spam. If left uncontrolled, spam can seriously congest networks, servers, and emailboxes with unsolicited content. After implementing Trend Micro™ InterScan™ Gateway Security, companies surveyed in this research reported an average 60% reduction in spam.

## **Web Filtering**

The Web has also become an effective tool for business and private users. Unfortunately, a mere visit to a Web site, whether intentional or unintentional, may expose the browsing system to dangerous viruses or code. A recent research project conducted by the University of Washington (Seattle) collected over 20,000 executables after a crawl of 2,500 domains. An examination of the executables determined that an alarming 1 in 20 contained spyware.

Bidirectional Web filtering is an important line of defense against such inbound and outbound Web traffic. Web filtering is used to enforce Internet use policies that prevent users from being exposed to Web pages containing "malware" and to suppress the further spreading of potentially infected Web traffic.

## **Antiphishing**

Phishing is a vehicle for attempting to trick personnel into revealing passwords as well as bank and credit card information. Aggressive email campaigns are driving unsuspecting Web users to counterfeit Web sites where they are duped into revealing their confidential information. Email phishing attacks now occur every day.

A study conducted by the Anti-Phishing Working Group during the 2005 holiday season uncovered several thousand new phishing sites in December alone.

When equipped with an antiphishing capability, companies can maintain a catalog of sites known to be counterfeit. When users visit such sites, they will be alerted to or prevented from interacting with them. Some antiphishing software looks at the reverse tracking information of an email or Web browser page to determine if the source of the request is legitimate.

## **Emerging Threats**

As a result of the increasing use of instant messaging (IM), blogs, file transfers, peer-to-peer messaging, and a host of other messaging forms of communication, hackers are now attempting to compromise computers through these means. All of these capabilities carry the risk of transmitting data that will either allow the theft of information from the infected systems or cause the infected computer to cease functioning correctly. Messaging security software is used to monitor, filter, and block messages from services that can also easily spread spam.

## ***Available Solutions***

Given the tight squeeze in which SMBs find themselves, it is obvious that an efficient, cost-effective, and comprehensive security solution is needed to address their unique situations.

SMBs that rely solely on firewalls with desktop- and server-level protection to secure their companies run the risk of being exposed to any or all of the previously discussed threat vectors.

An integrated security solution providing a high degree of protection for all of the aforementioned threats will yield cost savings as well as provide improved security. When an attempt to penetrate internal or external computing resources is sensed, an integrated system can trap the potential threat at the gateway and provide critical details in the form of a console alert and log entry, thereby providing forensics about capturing the nature of a suspected attack.

A comprehensive integrated security solution that provides at-the-gateway filtering of trojans, viruses, spyware, worms, and other malicious Internet traffic is easy to install, requires minimal ongoing maintenance, and will provide a cost-effective security approach for SMBs. A senior network administrator explained the installation process as follows: "I plugged in the Trend Micro [InterScan Gateway Security Appliance] box and turned it on. I liked the fact that there was not much tweaking required and that the equipment did the work instead of manpower."

A senior network administrator explained the installation process as follows: "I plugged in the Trend Micro [InterScan Gateway Security Appliance] box and turned it on. I liked the fact that there was not much tweaking required and that the equipment did the work instead of manpower."

An optimal solution for SMBs will provide the required security functionality in different form factors to meet their unique functional and budgetary requirements.

The most common types of security offerings for SMBs available today include:

- Software solution
- Appliance solution
- Hosted service

SMBs should seriously consider these optional security offerings. Trend Micro, which has historically led antivirus market share at the gateway, is a security vendor that provides the alternative choices mentioned above to meet the secure content management needs of SMBs.

## THE BUSINESS IMPACT

To assess the business and financial benefits that a comprehensive gateway solution offers SMBs, IDC interviewed several SMBs to gain a firsthand understanding of the primary issues involved in the decision process and the resulting economic benefits achieved from their implementations of a gateway system.

---

### The Decision Process

The primary drivers for the SMBs that are implementing a gateway solution ranged from updating legacy equipment to wanting to block significant volumes of spam and dangerous content such as viruses and worms before they entered their networks.

Participating SMBs (see the list on page 8) selected Trend Micro's gateway solutions on the basis of the extensive gateway functionality provided, overall effectiveness of spam reduction, ease of implementation, and low ongoing maintenance costs. "We should have changed to the Trend Micro gateway solution much sooner. We suffered for too long with solutions that did not work very well," explained an area service manager.

"We should have changed to the Trend Micro gateway solution much sooner. We suffered for too long with solutions that did not work very well," explained an area service manager.

## Considerations

The data presented in the following sections represents average benefits gained by participating SMBs. Because many variables and conditions are associated with these studies, quantitative results may vary considerably from the results presented in the following cost analysis model.

### ***Participating SMBs' Background Information***

- ☒ **Industries:** The businesses participating in this study included companies in construction, mining, and managed security services.
- ☒ **Employees:** The businesses represented in this research employed 40 to 5,000 people.
- ☒ **Budgets:** Overall IT budgets, including security line items for companies interviewed in this research, have remained flat over the previous and current years. IT budgets are expected to remain under pressure for the foreseeable future.
- ☒ **Security staff:** Dedicated security staffs in companies participating in this research ranged from 1 to 3 professional staff members.

Table 1 presents a summary of the average per-employee cost savings gained by the participants in this study.

**TABLE 1**

### Average Annual Security Cost Analysis

Security Event Type	Costs Before Trend Micro Gateway Solution (\$)	Costs with Trend Micro Gateway Solution (\$)	Average Security Cost Reductions with Trend Micro Gateway Solution (per Employee) (\$)
Malware (e.g., viruses, worms, bots)	364.00	14.00	350.00
Email spam	64.00	37.00	27.00
Help desk	64.00	45.00	19.00
Totals	492.00	96.00	396.00

Source: IDC, 2006

As can be seen in the preceding cost analysis model, significant per-employee savings, on an annualized basis, can be derived from the implementation of an effective and comprehensive gateway security solution.

## THE TREND MICRO SOLUTION

Trend Micro™ InterScan VirusWall™, InterScan Gateway Security Appliance, and Email Security Services offer SMBs a selection of cost-effective and comprehensive approaches to securing their businesses at the gateway.

As indicated earlier in this white paper, SMBs are confronted with unique and individualized issues where one-size-fits-all solutions completely miss the mark in providing cost-effective approaches to security.

To address these unique SMB security needs, Trend Micro has established a product set designed to provide cost-effective blocking of undesired Web and email traffic at the gateway. The three Trend Micro gateway options are:

- ☒ InterScan VirusWall
- ☒ InterScan Gateway Security Appliance
- ☒ Email Security Services

InterScan VirusWall and the InterScan Gateway Security Appliance provide cost-effective blocking of undesired Web and email traffic and embedded threats at the gateway. They intercept threats before they impact network traffic, employee productivity, uptime, or data confidentiality.

For organizations seeking a software solution, InterScan VirusWall provides an all-in-one Internet gateway content management solution. For organizations desiring an appliance approach to gateway content management, the InterScan appliance option will also meet their Internet gateway content management requirements.

For organizations seeking a hosted messaging solution, Email Security Services offer a hosted service for multilayered protection from email messaging threat vectors, including:

- ☒ Viruses
- ☒ Trojans
- ☒ Spyware
- ☒ Worms
- ☒ Bots

In addition, Email Security Services provide a highly flexible central management capability to facilitate the reduction of spam and other inappropriate email content.

The following sections provide a more detailed summary of the Trend Micro gateway solutions.

---

## **InterScan VirusWall**

Trend Micro InterScan VirusWall helps prevent viruses, spyware, spam, phishing, and bot attacks from entering a company's network through vulnerable Internet gateway access points. It reduces unwanted email using a combination of signatures and heuristics to provide high detection rates and fewer false positives. By scanning unprotected protocols — including SMTP, HTTP, FTP, and POP3 — it protects entry points exploited by attackers to carry malicious payloads.

InterScan VirusWall provides multilevel spyware, grayware, and phishing protection; blocks harmful Web and email downloads; protects privacy; and prevents the loss of company or personal information. The new antibot IntelliTrap capability feature defends PCs from being used as zombies to spread malware.

InterScan VirusWall's single Web-based remote console makes its multithreat protection easy to deploy and manage. In addition, the solution complements existing firewall and VPN solutions by providing an essential layer of front-line gateway defense.

InterScan VirusWall protects without intervention, resulting in reliable, timely responses and fewer infections. New and unique capabilities stop viruses earlier — before threat-specific detection signatures are available. IntelliTrap advances heuristic detection capabilities with technology to block malicious code that has not been encountered before. New Outbreak Prevention Services defend networks with rapid, automated responses when new outbreaks occur.

---

## **InterScan Gateway Security Appliance**

Trend Micro InterScan Gateway Security Appliance delivers all-in-one, comprehensive protection against security threats at the Internet gateway, before they can damage a company's network. This secure content management appliance saves time and money by reducing support calls, increasing the productivity of employees, and preserving the availability of network resources.

From a single Web-based console, InterScan Gateway Security Appliance automatically blocks threats — including viruses, spyware, spam, phishing, botnet attacks, harmful URLs, and inappropriate content — to provide a critical layer of security to complement desktop antivirus. The appliance blocks unwanted email and checks real-time blacklists to reduce inbox clutter, traffic, inappropriate content, and regulatory compliance costs.

InterScan Gateway Security Appliance comes preconfigured with software, making it easy to deploy. This secure content management appliance complements existing firewalls and VPNs to stop outbreaks early. Trend Micro Damage Cleanup Services eliminate virus and spyware infections automatically, saving administrative time and dramatically reducing downtime.

## Email Security Services

The majority of Internet threats enter a company's network through email traffic. Blended threats combine multiple tactics — spam, viruses, worms, trojans, and phishing (identity theft) — to penetrate a company's defenses. However, developing and managing an effective email security system can be complex and even costly, especially if a business has limited or no specialized IT security resources.

Trend Micro Email Security Services remove spam, viruses, and other Internet threats before they enter a company's gateway and stop denial of service (DOS) attacks and directory harvest attacks (DHAs) before they take down a network. Backed by experts in gateway secure content management, Email Security Services are designed to help protect available Internet bandwidth and email performance while reducing onsite storage requirements.

Trend Micro offers three levels of Email Security Services:

1. **Anti-Spam Service.** Anti-Spam Service offers an easy, cost-effective way to eliminate up to 80% of spam using advanced network-level connection controls without any administrator intervention. Using Trend Micro Network Reputation Services to evaluate the source of emails, this service protects against the most egregious spammers and highly dynamic sources such as zombie networks.

As a hosted service, Anti-Spam Service complements any existing mail system. It is easy to activate and simple to use and has immediate impact on spam levels. It also stops DOS attacks and DHAs before they stop business.

2. **Basic Email Security Service.** Basic Email Security Service delivers high-performance, cost-effective hosted security to protect a business against spam and threats such as viruses, worms, and trojans before they reach the network. This secure, fault-tolerant hosted service helps preserve available Internet bandwidth and mail performance while reducing onsite storage requirements.

Designed specifically for SMBs, Basic Email Security Service leverages Trend Micro's award-winning technology so there are no delays in obtaining patches or third parties required to maintain the systems. The result is a comprehensive, easy-to-use, and feature-rich system that is highly affordable and scales easily to meet a company's growing needs.

3. **Extended Email Security Service.** Extended Email Security Service delivers high-performance, cost-effective hosted security to protect a business against spam, viruses, worms, trojans, phishing, and inappropriate content. By blocking spam and other threats before they reach the network, Extended Email Security Service helps businesses protect available Internet bandwidth and mail performance while reducing onsite storage requirements.

Ideal for organizations that have specific information management requirements and overburdened IT resources, Extended Email Security Service eases the challenge of managing a complex messaging system. Detailed administrative reporting, easy-to-use policy management, and compliance enforcement allow the IT staff to focus on supporting the organization, not managing the technology.

Trend Micro's product set for SMBs includes integrated security solutions for the gateway, PCs, and servers with comprehensive management designed to set and forget.

More information is available at [www.trendmicro.com/gateway](http://www.trendmicro.com/gateway).

## **CONSIDERATIONS**

As with most important business decisions today, the cost of investing in any existing or new technology is a major consideration facing executives. Deciding where and how an organization can derive the biggest bang for the buck out of limited and often shrinking budgets is an ongoing balancing act that many CEOs and senior managers must deal with.

It is clear from current research that spam, spyware, phishing, worms, and other forms of malware are becoming more sophisticated. Establishing flexible and highly effective defenses to stay ahead of these increasingly complex and sophisticated threats must be among SMBs' top priorities.

## **CONCLUSION**

SMB business managers and executives face a variety of challenges every day. Many of these challenges require shoot-from-the-hip decision making if SMBs are to successfully compete in highly competitive markets and industries. At a minimum, the critical factors that must be included in SMBs' planning and decision-making processes are the profitability, efficiency, and security of their operations.

Planning, designing, and implementing a comprehensive security infrastructure that provides a high degree of protection from the various Internet threat vectors described earlier must be an essential part of an SMB's success-oriented business planning process.

Trend Micro's InterScan gateway products and services offer SMBs a comprehensive and cost-effective way to provide optimal protection from Internet-borne threats.

For more information, see [www.trendmicro.com](http://www.trendmicro.com).

---

## **Copyright Notice**

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2006 IDC. Reproduction without written permission is completely forbidden.