

## WHITE PAPER

---

# Secure Enterprise Threat Management Through an Integrated Security Framework

Sponsored by: Trend Micro Inc.

---

Gerry Pinal  
August 2006

Charles J. Kolodgy

## IDC OPINION

Enterprise stakeholders and IT executives are involved in a constant battle to establish an optimal and often delicate balance between maintaining highly secure and effective security infrastructures, providing high-quality IT services, and more recently, satisfying the requirements of government mandates.

At the same time, they are aggressively seeking ways to improve IT productivity within limited and too-often diminishing human capital and funding.

In 2005, IDC's research determined that security-related expenditures for hardware, software, and services reached \$32.6 billion. This already staggering figure is expected to continue to rise to \$60 billion by 2009.

Secure content management is a critical component of an overall threat protection strategy for enterprises. This segment of the security market is also projected to grow. IDC forecasts expenditures in this market segment to be \$6.2 billion in 2006 and to rise to \$11 billion by 2009.

To successfully meet their challenges, IT executives need to take proactive steps toward achieving the highest levels of threat protection for their enterprises and at the same time maintain their human and capital expenditures within tight budgetary constraints.

## METHODOLOGY

This white paper is based on current and historical IDC research. As part of this research, IDC conducted interviews with IT executives who have successfully achieved improved threat management and content protection at a lower cost by implementing highly integrated security frameworks. Summary results of these experiences are presented in this white paper.

Enterprise executives surveyed in this research reported that Trend Micro's Enterprise Protection Strategy provides comprehensive protection against sophisticated new threats.

## IN THIS WHITE PAPER

In this white paper, we discuss some of the pressing issues facing IT executives today and review a brief history of the complexities and challenges of staying ahead of today's existing, emerging, and evolving content threat types and sources.

In addition, we discuss some specific cases in which IT executives have significantly improved their overall content threat protection and at the same time reduced overall demands on IT resources.

## SITUATION OVERVIEW

---

### The Big Picture

IT executives are constantly striving to maintain the highest levels of organizational performance by striking an optimal balance between the following priorities:

- ☒ Providing continuous high levels of system availability and performance to maintain organizational productivity
- ☒ Establishing and maintaining a secure enterprise infrastructure to defend against any and all forms of security breaches, including securing both inbound and outbound content
- ☒ Rolling out and maintaining new and updated hardware, software, and business applications
- ☒ Providing responsive technical support to ensure consistent individual, business unit, and company performance

In many cases, because of the changing nature of these priorities, situations arise that require organizations that are already dealing with tight resource availability to make tough choices. These choices often involve decisions to make compromises between meeting the demands of securing the enterprise from security breaches, providing quality IT services, and now, satisfying IT requirements imposed by established government mandates.

Government mandates such as HIPAA and Sarbanes-Oxley, and many more, add even more complexity to the already difficult task of effectively balancing priorities. These established mandates require IT to divert already stressed resources. To effectively deal with these mandates, IT has had to launch new projects to ensure conformance and, ultimately, to receive passing grades when undergoing periodic company audits.

Obviously, these compliance-oriented projects further exacerbate the IT resource availability problem. IDC estimates that regulation-related projects will cost enterprises an estimated \$2 million or more in the first year if they are outsourced. Enterprises deciding to undertake these projects internally may have to invest as much as \$600,000 or more in the first year. Even worse, neither of these approaches includes the missed opportunity costs in diverting IT resources from other planned and critical internal business-related priorities.

It is clear from the preceding discussion that the challenges for IT executives continue unabated. More than ever, IT executives are seeking ways to continue providing and maintaining high levels of security as well as quality IT services.

In short, the name of the game for IT today is to find ways to "do more with less."

---

## **The Secure Enterprise**

Today's challenges in establishing impenetrable defenses for enterprises have become progressively more complex as the nature of threats to enterprises has become increasingly more sophisticated.

To compete in the global market, enterprises have readily adopted more sophisticated IT technologies. For many, these technologies have become the driving forces behind attaining the desired higher levels of productivity and profitability.

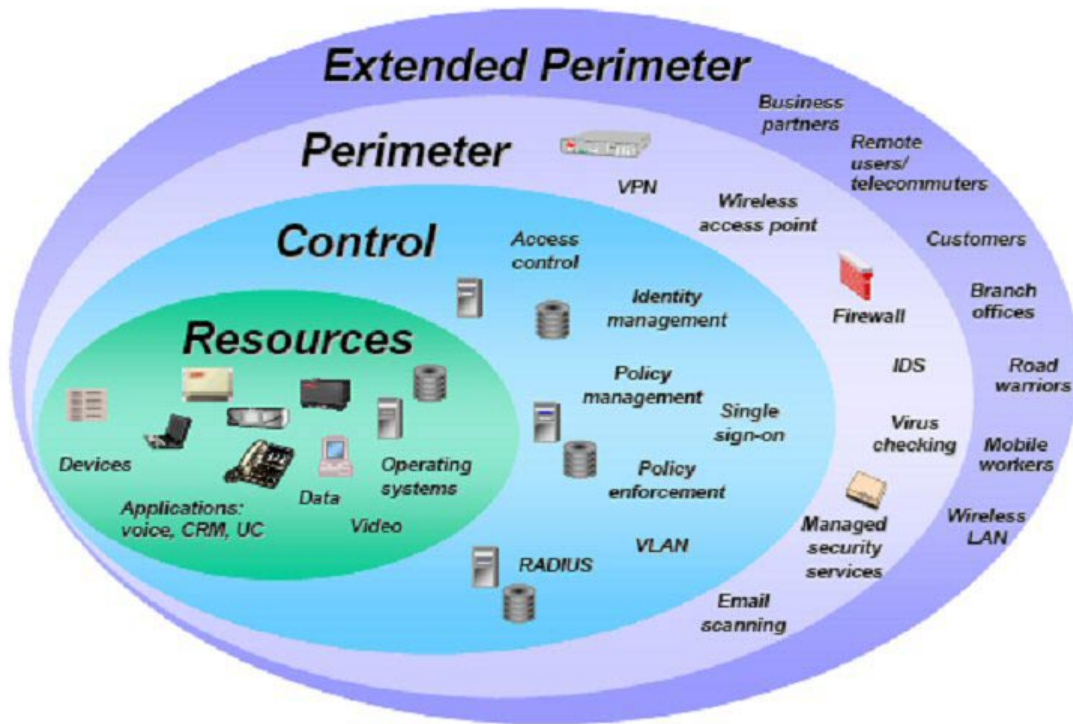
The adoption and use of the Internet for commerce throughout the world have completely changed the dynamics of doing business in an ecommerce-oriented world. On the one hand, the speed of transactions and communications has been the driving force behind higher levels of productivity and margin performance. On the other hand, the downside risks of opening up the enterprise to the cyberworld has also opened the door to people with malicious, criminal, and egregious intent.

For valid business reasons, providing remote access to business, customer, and internal company information has made it necessary to open portals into the IT infrastructure. Providing remote access to corporate data and information to employees and others has added to already "leaky" corporate infrastructures. Confidential company information is now accessible via the Internet by employees, partners, consultants, and customers. Unfortunately, these opened portals have also increased the risk of potential security breaches.

Figure 1 provides a high-level graphical overview of the functional layers of a typical corporate computing infrastructure.

**FIGURE 1**

The Porous Enterprise Infrastructure



Source: IDC, 2006

In our conceptual overview, the architecture comprises four layers:

- Resources
- Control
- Perimeter
- Extended perimeter

Centrally positioned in this conceptual enterprise architecture (the resources layer) are the corporate computing and networking resources. This core comprises central computing systems managing data storage and execution of centrally managed applications. Also included in this core are voice and other centrally located computing, network, and infrastructure devices.

The control layer implements and manages functions such as access control, identity management, policy management, auditing, and single sign-on methodology.

The perimeter layer comprises security-related devices and security functions. It includes the implementation of firewall, IDS/IPS, antispam, antivirus, managed security services, email scanning, wireless access, and VPN access.

The extended perimeter (or perforated perimeter) layer provides screened access to selected applications and core data and is dependent on the access privileges defined by the control layer. The perforated perimeter deals with the unmanaged user community. This is where business partners, remote users/telecommuters, customers, suppliers, and mobile workers are identified, authenticated, and allowed access to selected specific enterprise information resources.

Attacks directed at the extended perimeter and perimeter are everyday nonstop occurrences, and effectively implementing and maintaining the perimeter functionality in a secure way present significant challenges for IT.

It is important to note at this point that many of the IT infrastructure components are vulnerable to attacks as a result of security deficiencies in equipment and software components as well as errors in configurations or deficient or incomplete security policies. Tracking and maintaining current knowledge of vulnerabilities in all equipment and software, coupled with establishing sound security policies, present added challenges for management and IT professionals.

Until recently, the ability to thwart attacks at the enterprise perimeter, or within the enterprise infrastructure, has been achieved to a large degree through knowledge of existing and past known vulnerabilities.

Now, however, these various access portals into the enterprise have created opportunities for individuals with malicious or criminal intent, or both. The dynamics of these threat vectors have evolved into a situation in which not only are corporate assets at risk from a mischievous few, but threats are now driven by individuals who are seeking vulnerabilities in established defenses for illegal purposes. These threats exist both outside and within the enterprise.

A recent surge in thefts of high-value corporate and personal content has underscored the critical need for enterprises to establish strict policies and systems to defend against intruders seeking to steal content for profit. As a result, a new category of products and solutions called network access control (NAC) has emerged recently and is becoming increasingly popular with IT administrators.

---

## **Evolution of Defenses Against Enterprise Attacks**

As gateways into and out of the enterprise became a necessity, IT management began to define policies and implement security infrastructures. Firewalls were, for the most part, the initial appliances needed to protect against attacks from unwanted intruders.

With the extensive use and wide acceptance of email and the Web as communications vehicles, intruders began to use email and the Web as vehicles for penetrating the enterprise. Email was effectively being used to infect and spread viruses throughout and across enterprise systems. Email scanners and desktop antivirus systems were developed and utilized as a defensive move against these types of infecting vectors.

More recently, rootkits have become a popular threat mechanism for would-be criminals to gain access to enterprise systems and are being used to gain access to highly confidential enterprise data and information.

The aforementioned evolution is not meant to be a full treatise on the development of all the attack mechanisms currently in use; however, the progressively sophisticated ways in which exploits are being developed require a more comprehensive and equally sophisticated approach to defending against these various forms of intrusion, no matter how subtle or sophisticated.

As a result of the changing source and attack types over the past several years, enterprise IT organizations have had to incrementally build into their IT infrastructures point solutions directed at defending against the "popular threat" of the day, week, month, or even year.

From a systems perspective, as these threats have become increasingly more sophisticated, defense strategies have had to evolve in sophistication and complexity to keep pace. Because no single technology solution addresses all these various forms of attacks, by necessity, organizations have had to develop or implement incremental or "piecemeal" defense strategies to deal with these forms of intrusion.

In many cases, the search for the best-of-breed solution in each area of vulnerability at the time has resulted in enterprises' being protected by several point solutions with support provided by an equal number of vendors. Some IT managers now find themselves, for historical reasons, dealing with multiple point security solutions supported by an equal number of security vendors.

IDC believes that often point solutions are not an effective approach to building a secure enterprise infrastructure. If these point solutions and their accompanying support mechanisms are not completely compatible, the overall effectiveness and potential added cost of supporting and maintaining these independent systems are, to some extent, diverting valuable and limited IT resources.

## **THE IDEAL SECURITY ARCHITECTURE IS MULTILAYERED**

Experience has shown that the overall effectiveness of a highly secure and cost-effective security infrastructure is achieved when all of the security components are tightly integrated and are able to interact and support each other.

Conceptually, the ideal architectural approach to establishing a highly secure enterprise infrastructure is to have the components of the security architecture provide secure coverage at all levels.

The ideal security infrastructure provides protection for the four layers illustrated in the conceptual enterprise architecture in Figure 1: resources, control, perimeter, and extended perimeter. Introducing a central monitoring and control component to the security infrastructure creates a truly integrated and secure enterprise by providing protection from all forms of attack at all layers of the infrastructure and managing the process through a single central command component.

Further advantages to implementing an integrated architecture are achieved when all unusual incidents can be forensically analyzed through a single centralized management capability.

When respondents in our survey were asked about the benefits of having an integrated security architecture with a single vendor supporting them, common responses were "It is much more efficient to be able to call a single number and discuss a complex critical security issue with someone you have developed a trusted relationship with and who understands your architecture and configuration" and "Generally we get the rapid support we need when it is crucial that we have all the answers."

---

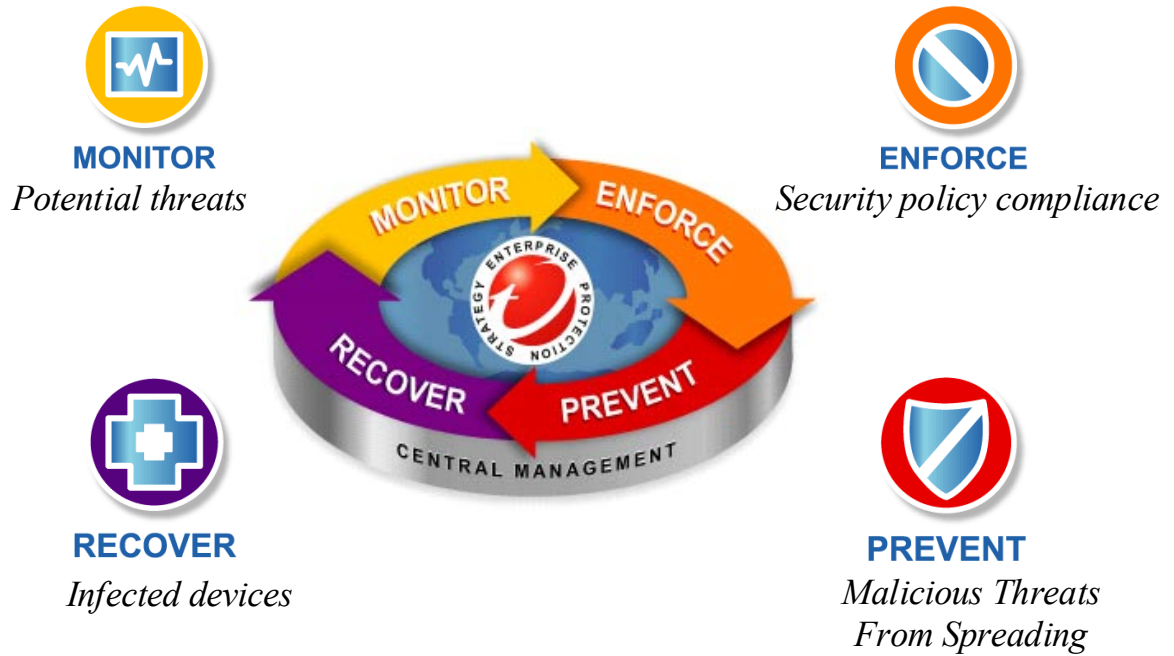
## **The Trend Micro Solution**

Trend Micro Enterprise Protection Strategy (EPS) provides a unique approach to threat management for the porous enterprise infrastructure. EPS is a security framework that combines multiple layers of products and services for comprehensive, intelligent protection against known and unknown threats. Tightly integrated, centrally managed security enables seamless interproduct collaboration that helps reduce overall threat exposure.

Intelligent threat life-cycle management, shown in Figure 2, is a phased approach to comprehensive threat protection that consists of four primary stages — monitoring for potential threats, enforcing security policy compliance, preventing the spread of malicious threats, and recovering infected devices. A centralized management console helps coordinate the response to new threats and provides consolidated administration and reporting. EPS incorporates the delivery of timely updates and attack-specific outbreak policy recommendations from TrendLabs to all Trend Micro products and services. During these stages, Trend Micro's global network of security experts helps manage the time, costs, and system damage associated with new threats.

**FIGURE 2**

Intelligent Threat Life-Cycle Management



Source: Trend Micro Inc., 2006

***Monitors for Potential Threats***

This first proactive stage of EPS continuously monitors the global Internet and the corporate network for potential threats. New technologies under development will accurately detect known and unknown threats in real time. Trend Micro Expert Services, a managed service, offers 24 x 7 monitoring of the environment from a remote location so the new threats are detected irrespective of where and when they enter the network. Trend Micro Network Reputation Services detects and stops email-bound threats in the service provider network even before they reach the enterprise. The IntelliTrap feature in InterScan Messaging Security Suite detects unknown variants of email threats in real time. With advanced endpoint security, EPS will be able to stop known and unknown threats at the endpoint device itself — even when the device is not connected to the enterprise network.

***Enforces Security Policy Compliance***

This second proactive stage of EPS enforces access controls to ensure that only compliant user devices are allowed to connect to the enterprise network. It incorporates a cost-effective, turnkey NAC solution for corporate security policy enforcement on every device that tries to access the network. In the process, it blocks devices with known threats or outdated security profiles until they go through automatic remediation. In addition, this enforcement stage also incorporates a future migration path to comprehensive NAC solutions. Trend Micro also supports industry-standard NAC frameworks, such as Cisco NAC and Microsoft NAP, with its OfficeScan products.

### ***Prevents Malicious Threats from Spreading***

This first reactive stage of EPS stops all malware, including viruses, spyware, spam, bots, rootkits, phishing, and hybrid threats as soon as they are detected at the endpoints. Multiple layers of security guard every network entry point: clients, servers, gateway, firewall, network infrastructure, and IP layer. In the rare event of a virus outbreak, this EPS stage delivers a rapid response to all Trend Micro security products through outbreak prevention policies.

"Our email volume is about 20 million messages per year. Prior to Trend Micro's spam blocking, 67% of these messages were spam. At an estimated 4.2 seconds per message, we estimate that we save \$500,000 in staff time dealing with spam," said a project manager at a local government agency.

"Our email volume is about 20 million messages per year. Prior to Trend Micro's spam blocking, 67% of these messages were spam. At an estimated 4.2 seconds per message, we estimate that we save \$500,000 in staff time dealing with spam," said a project manager at a local government agency.

### ***Recovers Infected Devices***

This second reactive stage of EPS automatically recovers infected devices to ensure businesses are quickly brought back to normal. Automated cleanup removes viruses, worms, trojans, and spyware from managed as well as unmanaged clients, whether the infected devices are local or remote.

### ***Provides Central Management***

The most critical component of EPS is its centralized management of all Trend Micro products and services through a single, Web-based management console. Trend Micro Control Manager simplifies and consolidates enterprisewide administration, reporting, updates, and coordination.

Further augmenting the EPS framework, Trend Micro's product, solutions, and services neatly fit into four key security threat management categories — messaging, Web, endpoint, and network security — to offer comprehensive coverage across every critical network entry point. A close partnership with Cisco Systems enables Trend Micro to extend the comprehensive, intelligent threat protection beyond traditional network entry points to nodes inside the Cisco network infrastructure.

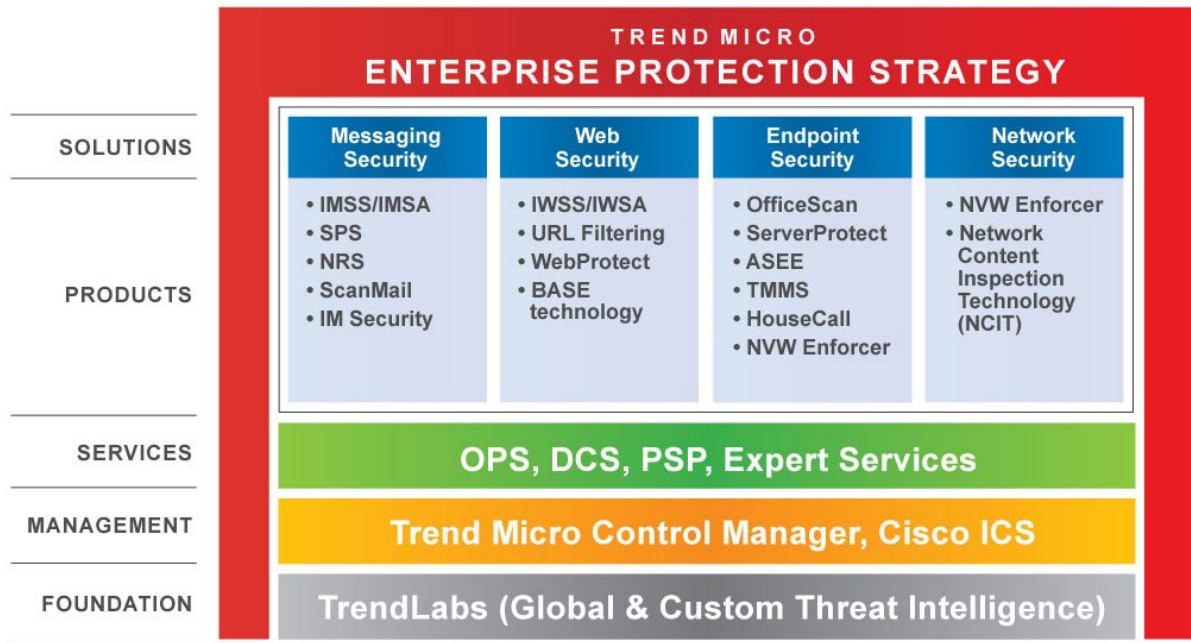
---

## **Trend Micro Enterprise Protection Strategy**

Enterprise Protection Strategy provides a holistic framework in which Trend Micro products, services, and capabilities work together to deliver intelligent threat protection (see Figure 3). TrendLabs provides the foundation for global and customer-specific threat intelligence for all products and services. Trend Micro Control Manager provides a central management console to deliver up-to-date threat intelligence as well as common administration, reporting, and deployment for all products and services. Common services such as Trend Micro Outbreak Prevention Services, Trend Micro Damage Cleanup Services, and Trend Micro Expert Services enhance the capabilities of all Trend Micro products, irrespective of whether the product is for a desktop, server, gateway, network, or mobile device. The integrated components of EPS enable a proactive offense that prevents threats from gaining entry to enterprises.

**FIGURE 3**

Trend Micro Enterprise Protection Strategy



Notes:

- IMSS:** InterScan Messaging Security Suite
- IMSA:** InterScan Messaging Security Appliance
- SPS:** Spam Prevention Services
- NRS:** Network Reputation Services
- IWSS:** InterScan Web Security Suite
- IWSA:** InterScan Web Security Appliance
- BASE:** Behavioral Analysis Security Engine
- ASEE:** Anti-Spyware Enterprise Edition
- TMMS:** Trend Micro Mobile Security
- NVW:** Network VirusWall
- OPS:** Outbreak Prevention Services
- DCS:** Damage Cleanup Services
- PSP:** Premium Support Program
- CISCO ICS:** Cisco Incident Control System

Source: Trend Micro Inc., 2006

**Benefits**

***Comprehensive: Supports Managed and Unmanaged Users***

Trend Micro EPS incorporates support for both managed and unmanaged users in the enforce and recover stages of the framework. This support leads to a more complete solution for security policy compliance and savings in IT administrative costs to support remote users with devices that may be infected.

***Intelligent: Accurately Detects Potential Threats in Real Time***

EPS features advanced network content inspection capabilities to detect known and unknown threats in real time. Backed by a broad range of intelligent rules and over 15 years of threat management experience, Trend Micro products are capable of identifying and stopping potential threats at the network layer itself before they reach the endpoints.

***Reliable: Provides Reliable Protection by Combining Proactive and Reactive Defenses***

EPS combines proactive and reactive defenses to offer reliable protection for the enterprise. Because reactive defenses (signature files) are no longer enough to protect against today's sophisticated new threats, Trend Micro is introducing several proactive defenses in the monitor and enforce stages that help keep new threats out of the enterprise environment in the first place.

***Flexible: Lowers Overall Threat Exposure***

EPS comes with the flexibility to deploy Trend Micro products and services gradually to manage the acceptable level of risk at any point in time. This flexibility enables IT administrators to start small and phase in new products over time to achieve increasingly lower overall threat exposure. For example, reactive defenses can be combined with the proactive enforce stage initially to achieve a certain level of risk exposure. Advanced network content inspection technologies can be introduced at a later stage to further reduce the overall exposure to new threats.

**INTERVIEW SUMMARIES**

As discussed earlier, IDC undertook this research project to help gain a clearer picture of the direct and quantifiable improvements achieved when IT organizations instituted security-related programs to:

- Reduce the overall IT staff workload for security-oriented tasks
- Reduce the number and frequency of security calls
- Establish a single point of contact for security issues
- Improve effectiveness of security-related remote repair activities

The following sections provide valuable insights into the types of success realized by a selected group of customers as a result of working with a single security vendor and an integrated security framework such as Trend Micro's.

Participating enterprises ranged in size from 1,000 to 17,000 employees. IT headcounts supporting these numbers ranged from 5 to 280. IT budgets for these enterprises ranged from \$1 million to \$50 million.

With regard to overall IT budgets, a consistent trend among the participants was the continuing tight squeeze on overall IT and security budgets. Overall IT budgets for 2006 range from being reduced by as much as 10% to tracking the inflation rate at a mere 3%.

---

## **Reduction in Overall IT Staff Workload for Security-Oriented Tasks**

A trend that became evident in our research is that as the effectiveness of enterprise security systems increases, the first responders in dealing with security-related calls are members of the help desk.

This trend has been driven by:

- An overall enhanced effectiveness of security policies and security products and services
- A reduced number of serious breaches or infections encountered over the past year
- Improved security-related automation capabilities

As a direct result of implementing an integrated security framework such as Trend Micro's EPS, enterprises reduced the number of security staff hours expended in repairing the effects of virus infections by 60% to 80%. Further, with advanced security automation functionality in place, enterprises reported that the total time expended in dealing with signature updates ranges from 0 to 10 hours per year.

"We have implemented Trend Micro's desktop, gateway, and server security products, and since our full implementation has been completed, we have significantly improved our security-related automation capabilities," said a systems security manager in the insurance industry.

---

## **Reduction in the Number and Frequency of Security Calls Due to Centrally Managed Security**

Since deciding to designate members of the help desk as first responders to all security-related calls, enterprises reported that they have realized a significant reduction in the number of calls related to escalated security issues and that escalated calls are becoming rare occurrences.

The following anecdotal comment describes the overall improvement in security-related call frequencies: "Since the Trend Micro software was installed, the security staff don't need to be involved. All it usually takes is a reboot, and the help desk provides direction to complete the repair. The only issues we have to deal with today are spam and blocked attachments. Everything else requires minimal intervention on our part," said a system manager at a state agency.

"The only issues we have to deal with today are spam and blocked attachments. Everything else requires minimal intervention on our part," said a system manager at a state agency.

---

## **Establishing of a Single Point of Contact for Security Issues**

A main reason given for partnering with a single security vendor was to simplify the procurement/contract process. One respondent sought multiyear contracts, whenever possible, to get better pricing and to reduce the amount of work that goes into procurement and purchasing process.

On the technical side, dealing with a vendor as a single point of contact, with which this firm has developed a relationship, has made it easier to function when help was needed. Given the small number of dedicated security staff members available, this has become a crucial issue.

---

## **Improvement in Effectiveness of Security-Related Remote Repair Activities**

The typical response of survey respondents is that the number of hours spent by their security staffs in dealing with remote security-related fixes has been significantly reduced. As one respondent noted, "The only time the help desk is called for security issues is when something doesn't work. This is rare."

## **CHALLENGES/OPPORTUNITIES**

Enterprise security challenges facing today's IT management and professionals are becoming increasingly more complex. Attackers are becoming more serious in their targeting of critical enterprise data and in their use of more advanced malware. Because more enterprise value resides in the information, stronger defenses are required. Thus, sound management, technical, and auditable policy decisions must be made to ensure compliance with governing regulations.

Trend Micro is addressing the heightened threat environment with its Enterprise Protection Strategy, which provides enterprise IT with the opportunity to arrest sophisticated new threats with a comprehensive end-to-end solution that is both scalable and cost-effective.

## **CONCLUSION**

IT executives participating in this research were successful in attaining a return on their security investments while, in an increasingly complex threat environment, establishing the highest levels of protection for their enterprises. In addition, by achieving significant reductions in spam, they demonstrated network performance and user productivity gains. By implementing Trend Micro's integrated and centrally managed security framework, these IT executives have achieved their security solution objectives, and at the same time, they have maintained costs within their static or, in some cases, decreasing IT security budgets.

---

## **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.