



# Server and Application Protection—Behind the Lines

Data Security 

 Trend Micro/Third Brigade

A Trend Micro White Paper | March 2009

# Server and Application Protection— Behind the Lines



## TABLE OF CONTENTS

A GROWING THREAT, A BETTER RESPONSE.....	3
BRAND EQUITY, MARKET CAPITALIZATION, AND LITIGATION.....	4
CLOSING THE PATCH MANAGEMENT VULNERABILITY GAP.....	4
CODE FIXES AND COMPLEMENTING SECURE CODE INITIATIVES .....	6
IMPROVING INCIDENT RESPONSE.....	7
CUSTOMER SERVICE AND COMMUNICATIONS .....	8
EMPLOYEE PRODUCTIVITY: THE HIDDEN COST.....	8
COMPLIANCE AT REDUCED COST.....	8
SAFETY AND CRITICAL INFRASTRUCTURE PROTECTION .....	10
REVENUE AND BUSINESS CONTINUITY .....	11
THE TREND MICRO/THIRD BRIGADE ALLIANCE .....	11

# Server and Application Protection— Behind the Lines

## A GROWING THREAT, A BETTER RESPONSE

Cyber attacks can bypass or penetrate even top-of-the-line perimeter security, and it's increasingly recognized as a security best practice to provide server and application protection to detect and prevent these attacks as an integral part of a defense-in-depth strategy. A comprehensive server and application protection system will include: firewall, IDS/IPS, integrity monitoring, and log inspection technologies that enable systems to become self-defending. Driven by the growing awareness of targeted attacks and the insider threat—as well as by virtualization security concerns and pressures from PCI and other regulations and standards, and by high-profile security breaches—many organizations now actively evaluate the merits of investing in a server and application protection system to complement their existing IT security systems.

One of the other drivers of this trend is the need to cost-effectively stop or prevent loss, as the costs of prevention are usually far less than the price of fixing a system that has been breached. According to SearchSecurity.com, retailer TJX Companies announced that it will spend \$256 million responding to a data breach that compromised up to 100 million accounts.

For organizations evaluating the benefits of server and application protection systems and making a case for incorporating them into the IT infrastructure, Trend Micro and Third Brigade recommend examining these nine different areas of business interest:

- Brand equity and market capitalization
- Code fixes
- Compliance
- Customer service and communications
- Employee productivity
- Incident response
- Patch management
- Revenue
- Safety

Trend Micro and Third Brigade are working together to offer solutions that can help organizations address all of these concerns.

Third Brigade Deep Security Solution™ is a server and application protection software that enables systems to protect themselves. It provides comprehensive, manageable protection for datacenters—including physical and virtualized servers, and cloud computing environments—through these software modules:

- Deep Packet Inspection
  - Intrusion Detection and Prevention (IDS/IPS)
  - Web application protection
  - Application control
- Firewall
- Integrity Monitoring (files, directories, and system)
- Log Inspection

This comprehensive security helps customers prevent data breaches and business disruptions, enables compliance, and supports operational cost reductions for organizations that recognize that perimeter defenses alone are no longer sufficient.

# Server and Application Protection— Behind the Lines

## BRAND EQUITY, MARKET CAPITALIZATION, AND LITIGATION

A high-profile attack can have a significant impact on the perceived value and quality of a brand, and the loyalty and trust that stakeholders have in the enterprise. Imagine being the head of alumni relations at a school that depends heavily on donations, and having to notify 50,000 alumni that their personal data was stolen because a system was inadvertently left exposed. Or being a senior government official that has to explain how a security breach to a citizen-facing application—e.g., tax, immigration, passports, social security—will impact trust, confidence, and the continued adoption of reduced-cost online channels.

A security breach that compromises confidential data can also have a material impact on a company's market capitalization. ChoicePoint, Inc.'s market capitalization fell by \$720 million following news that identity thieves had gained access to personal consumer information. CardSystems Solutions, Inc., was a billion-dollar company before a security breach compromised 40 million consumer accounts. The data security breach occurred because intruders were able to exploit software security vulnerabilities to install a rogue program on the network of CardSystems Solutions. After the breach, the company was acquired by Pay By Touch™ Payment Solutions, LLC, for \$47 million.

Class action lawsuits also are being filed increasingly following breaches, particularly those that involve medical and personal financial information. For example, the *New York Law Journal* reported on May 15, 2008: "On March 17, 2008, Hannaford announced that cyberbandits had breached its system, obtaining access to personal financial information of nearly 4.2 million customers. Just three days after the announcement, plaintiffs' lawyers filed four class actions against Hannaford. Since then, lawyers have filed an additional 12 complaints, requiring Hannaford to defend litigation from Florida to Maine."

By preventing attacks resulting in security breaches that compromise confidential data or service availability, customers, partners, suppliers, and even employees will have increased confidence, which builds trust in a brand. It also helps prevent drops in share price and/or costs of litigation that could result from a breach of confidential data. According to a 2003 article from the *Journal of Computer Security*, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market," "A firm suffering a breach of 'confidential information' saw a 5 percent drop in stock price, while firms suffering a nonconfidential breach saw no impact."

## CLOSING THE PATCH MANAGEMENT VULNERABILITY GAP

Patch management involves properly acquiring, testing, installing, and documenting code changes—or "patches"—to an administered computer system. Although regularly scheduled patching is unavoidable, it can be disruptive and expensive to carry out emergency patching in response to the discovery of newly disclosed critical vulnerabilities. A vulnerability gap exists between the time when vulnerabilities are first discovered and the time when they are patched or shielded.

According to *The Laws of Vulnerabilities: Six Axioms for Understanding Risk—Global Data from 40 Million Security Scans over 40 Months Define Behavior of Vulnerabilities for Insight on Protecting Networks* (Qualys, 2006), there are six relevant factors to consider about patching vulnerabilities:

# Server and Application Protection— Behind the Lines

## Half-life

Half-life identifies the length of time it takes users to patch half of their systems, reducing their window of exposure. In the last year, the half-life of critical vulnerabilities for external systems has been reduced from 21 days to 19 days, and from 62 days to 48 days for internal systems.

## Prevalence

Prevalence is the frequency with which vulnerabilities are created. On an annual basis, 50 percent of the most prevalent and critical vulnerabilities are replaced by new ones.

## Persistence

Persistence is the durability of system vulnerabilities. Four percent of critical vulnerabilities remain persistent, and their lifespan is unlimited.

## Focus

The focus of system security is extremely important. Ninety percent of vulnerability exposure is caused by 10 percent of critical vulnerabilities. Early detection and awareness of suspicious activity occurring within your organization is a key element in effectively dealing with data breaches. Integrity Monitoring and automated inspection of logging events provide visibility into suspicious behavior and enable organizations to remediate issues before they lead to embarrassing and business-critical disclosures.

## Window of Exposure

The window of exposure for your systems is crucial. The time-to-exploit cycle is shrinking faster than the remediation cycle—80 percent of exploits are available within the first half-life period of critical vulnerabilities.

## Exploitation

Exploitation of these vulnerabilities is the point of greatest concern. Automated attacks create 85 percent of their damage within the first 15 days of the outbreak, and they have an unlimited lifespan.

According to the *2007 CSI Computer Crime & Security Survey*, almost 18 percent—approximately one-fifth—of those respondents who reported they suffered one or more kinds of security incident further said they'd suffered a "targeted attack," defined as a malware attack aimed exclusively at their organization or at organizations within a small subset of the general population. In many cases, this gap can extend for weeks or months before appropriate patches are deployed to all production systems. Additionally, SANS reported 4,396 total vulnerabilities disclosed for commercial and open-source Web applications from November 2006 to October 2007—and according to the 2008 Web Application Security Consortium, 15 percent of the incidents in the 2007 Web Hacking Incident Database (WHID) exploited known vulnerabilities.

Using filters that monitor for attacks targeting known vulnerabilities in applications and operating systems, a server and application protection system acts as a "virtual patch" to shield systems before vendor-issued patches can be applied. This enables organizations to avoid emergency, event-driven patching costs by shielding newly discovered vulnerabilities until the appropriate patch is developed, tested, and deployed. Patching costs can be considerable. In a study sponsored by Microsoft and audited by Meta Group (*The Total Cost of Security Patch Management*, WiPro, 2005), WiPro determined that a patching event can take from 0.6 to 2.4 hours of labor per system, depending on the type of server—whether it's a Windows server, Windows database server, or open-source server.

# Server and Application Protection— Behind the Lines

Most server and application protection companies have corresponding security labs that monitor industry sources to create and automatically deliver vulnerability filters within hours of a known existence of vulnerabilities. These filters should be able to be pushed out and applied automatically to thousands of hosts in minutes, without requiring systems to be rebooted. As such, they can dramatically reduce or shrink the duration of the vulnerability gap. A virtual patch does not require changes to the OS or the application, protects immediately before the patch is applied, works even when there is no patch available, and can be configured to shield proprietary applications.

Additionally, because the server and application protection agents reside on the server itself, the status of patch deployments can be monitored automatically, per system. Vulnerability filters can be added or removed, depending on the patches currently applied to unique applications and operating systems. The severity of the vulnerability can also be used to determine the appropriate security action: either detect only or attack prevention. These capabilities improve the overall performance and effectiveness of the server and application protection system.

## CODE FIXES AND COMPLEMENTING SECURE CODE INITIATIVES

According to *Software Assessments, Benchmarks, and Best Practices* (Jones, 2000), most software has from 1,000 to 1,500 security defects per million lines of code. Gartner concurs, noting in a 2005 report that 60 percent of customer-facing Web applications have an exploitable vulnerability. Vulnerabilities or flaws that are discovered in custom-built and legacy Web applications require code fixes. But there is another hurdle for the organization: In many cases, developers with the necessary subject matter expertise are not available to fix the application. They might be busy with other projects or no longer with the company. This can be a common occurrence within organizations that have grown through acquisition. Custom and legacy Web applications are vulnerable to varying degrees of cross-site scripting, remote code execution, command injections, denial of service, and other attacks.

Server and application protection provides virtual patch capabilities for these applications, enabling organizations to avoid the costs associated with code fixes, or to schedule these development efforts when resources are available, thereby minimizing disruption and staying better in line with business objectives. This can also be vital to regulatory compliance. Requirement 6.6 of the *PCI Data Security Standard* states that organizations must: “Ensure that all Web-facing applications are protected against known attacks by applying either of the following methods: Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security, or installing an application-layer firewall in front of Web-facing applications.”

Best practices demand that proactive solutions are made a part of the IT security infrastructure. Gartner’s 2008 report *Web Server Security Hierarchy*, concurs: “Host-based Intrusion Prevention software can be installed on high-value Web servers to provide a means of blocking execution of malicious software on the Web server” and “File integrity monitoring and nonblocking host-based intrusion detection capabilities may be considered for the detection of events after the fact.”

# Server and Application Protection— Behind the Lines

## IMPROVING INCIDENT RESPONSE

An organization's computer incident (or emergency) response team (CIRT or CERT) typically follows the incident response lifecycle when preparing for and managing a security incident. The costs associated with this lifecycle can be significant, and security technologies for server and application protection can shorten this cycle and help reduce or avoid costs.

In early 2007, a Canadian federal government agency fell victim to a worm that nearly brought operations to a halt. The infection began with just a few computers but spread like a prairie grass fire, eventually knocking out 1,308 workstations in three cities while taking more than a month to be eradicated. The worm also spread to another department when infected agency computers tapped into the bigger department's data network, disabling 543 additional workstations in five offices. The attack is estimated to have cost the agency up to \$1.5 million, including downtime for employees made idle by their ailing workstations. More than 50 technicians and other experts struggled for weeks to contain the damage.

Server and application protection systems provide significant value at the identification, containment, eradication, and recovery stages of the incident response lifecycle.

### Identification

A server and application protection system proactively detects and prevents Web threats, hacking attempts, and vulnerability exploits that target vulnerabilities in operating systems, as well as enterprise applications and Web applications. It provides detailed information on who attacked, when they attacked, and what they attempted to exploit, which enables analysts to take appropriate, timely, informed action. Integrity monitoring and log inspection provide another vital element for gaining insight into suspicious activity occurring within the environment, supplying the controls and audit trail necessary for achieving and maintaining compliance.

### Containment/Mitigation

A server and application protection system intercepts malicious network communication right at the host, before it has a chance to intrude into networks and disrupt users, and it can stop outbound attacks.

### Eradication/Remediation

A server and application protection system enables organizations to avoid remediation costs—reimaging or rebuilding—by detecting and preventing attacks before they cause damage. In addition, corporate services and end users remain online, ensuring that corporate SLAs are met with no impact to revenue and efficiencies.

### Recovery

It can take one to two days to restore a single mission-critical server by reinstalling the OS, applying the system state information from backup, restoring the data and user accounts, and configuring the system. An application server might take a day or less. By narrowing the scope and impact of an incident, reducing endpoint downtime, and providing incremental protection against zero-day attacks, server and application protection systems expedite the recovery phase. In situations where an attack was not the cause of a failure, industry statistics point to a system change (patch, service pack, or configuration change) as being responsible for 80 percent of system outages. Furthermore, 80 percent of the mean-time-to-repair involves identifying the change that caused the problem. Integrity monitoring and log inspection provide visibility into changes and enable administrators to quickly identify and remediate changes related to system outages, significantly reducing interruptions to services and the costs associated with those service interruptions.

# Server and Application Protection— Behind the Lines

## CUSTOMER SERVICE AND COMMUNICATIONS

Regulations in more than half of all U.S. states, as well as in many other countries, require that customers be notified if their confidential or personal data has been lost, stolen, or compromised. The only “safe harbor” exception exempting organizations from these notification requirements is for data held in an encrypted form when lost. In addition, in the event of a security breach that results in the theft of personal data, new credit, health, SSN, and other cards might need to be issued to customers and citizens. This can be costly: The American Bankers Association reports that the cost to reissue a credit card is between \$10 and \$25 per card.

The costs to the organization can be greater still. According to the Ponemon Institute’s *2006 Annual Study: Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventative Solutions*, “Direct incremental costs for incremental, out-of-pocket, unbudgeted spending for outside legal counsel, mail notification letters, calls to individual customers, increased call center costs, and discounted product offers are \$54 per record.” Forrester’s 2007 report *Calculating the Cost of a Security Breach* concludes that the average security breach can cost a company between \$90 and \$305 per lost record: “Although studies may not be able to determine the exact cost of a security breach in your organization, the loss of sensitive data can have a crippling impact on an organization’s bottom line, especially if it is ill-equipped, and it’s important to be able to make an educated estimate of its cost.”

Preventing a security breach from occurring enables organizations to avoid customer notification costs, including direct costs associated with telephone, email, direct mail, or other general notice and advertising costs, as well as the costs of replacing cards or, worse, replacing customers lost due to brand damage.

## EMPLOYEE PRODUCTIVITY: THE HIDDEN COST

Lost productivity resulting from a security incident can have a serious impact on the bottom line. For many organizations, the cost of lost productivity associated with a security incident is far greater than the cost of data recovery or system repair, since a security breach can result in computers not being available for normal daily labor. As a result, worker productivity is reduced. The Ponemon Institute has estimated that indirect productivity costs for lost employee productivity are \$30 per record. By preventing attacks that result in downtime, or containing and minimizing the impact or spread of an attack, server and application protection software enables organizations to better maintain productivity of people and systems.

## COMPLIANCE AT REDUCED COST

Lawmakers and regulatory agencies have made it clear that confidential data must be protected in today’s environment. Individuals and organizations have no alternative. In fact, as of February 2008, at least 37 states in the U.S. have passed laws requiring organizations and government agencies to notify customers, employees, and other affected individuals when a breach of protected personal information occurs due to human error, technology problems, or malicious acts. The penalties for failure are often severe and not strictly financial, as they might also include criminal, class action, and civil legal actions against the organization and its directors. As a result of one security breach, identification and credential verification services provider ChoicePoint was ordered by the Federal Trade Commission to pay a \$10 million federal fine, contribute \$5 million to a fund to compensate consumers who suffered from the breach, and submit to external security audits for 20 years.

# Server and Application Protection— Behind the Lines

Some of the regulatory factors for an organization to consider are:

## **PCI Security Standards Protocols**

If a member, merchant, or service provider fails to comply with the security requirements or fails to rectify a security issue, they might face fines of up to \$500,000 per incident, or restrictions imposed by the credit card companies, including denying their ability to accept or process credit card transactions.

## **Statement on Auditing Standards (SAS) 70**

Technology-related service providers—such as SaaS, ASPs, and MSPs—rely on accounting firms to report on internal controls, including security, using SAS 70, an auditing standard developed by the American Institute of Certified Public Accountants that focuses on controls and control objectives.

## **Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA mandates civil fines as high as \$25,000 per person for every violation of a single standard in a given year. Violations leading to gain or harm can bring fines up to \$250,000 and 10 years in prison.

## **Sarbanes-Oxley (SOX) Legislation**

Penalties under SOX are even harsher—as much as \$5 million in fines or 20 years in prison.

## **Gramm-Leach-Bliley Act (GLBA)**

Violations of GLBA, which requires banks and financial institutions to protect consumer information, can lead to fines of up to \$100,000 per violation for officers and directors, and prison terms of up to five years.

## **Federal Information Security Management Act (FISMA)**

According to FISMA, federal departments and agencies are required to implement “risk-based, cost-effective approaches to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats.”

Larger organizations generally have more auditors, and auditors can charge more than \$250/hour. In many cases, roughly half of the auditor’s time will be spent assessing internal controls, including IT security. In some industries, such as banking, there can be internal and external auditors. Server and application protection systems can help organizations avoid these costs in three ways:

- First, these solutions help reduce audit-related costs across numerous compliance initiatives by addressing multiple compliance requirements with a single universal agent. This reduces the need to audit multiple standalone management and agent architectures and implementations. It also reduces the need to review multiple task-specific consoles, log files, etc. A comprehensive server and application protection system provides centralized security management and reporting capability, reducing the time spent by internal and external auditors—and by compliance and IT staff—before, during, and after an audit. By having the necessary controls in place and using automated scheduling of common administrative tasks, a server and application protection system can reduce the time and costs associated with addressing any issues discovered during the audit process.
- Second, host-based firewalls can be used to segment a network more cost-effectively than using hardware-based appliances and to reduce the scope of a PCI audit. If not already implemented, full physical segmentation—for example, through the use of a UTM to perform firewalling, virtual patch protection, and intrusion prevention at each site—is often prohibitive to purchase, deploy, and manage. This impact is even greater in highly distributed cardholder data environments, such as retail outlets and branch offices.

# Server and Application Protection— Behind the Lines

Host-based segmentation eliminates the need for additional physical firewalls, complements a single perimeter firewall, works at the network layer to provide network-level protection, and normalizes host segmentation control, regardless of network architecture.

- And third, server and application protection systems help organizations avoid penalties and fines associated with a security breach or noncompliance.

## SAFETY AND CRITICAL INFRASTRUCTURE PROTECTION

There have been a number of cases that highlight the potential safety risks to sectors that are directly linked to critical infrastructure: public health and safety, including food and water; energy and utilities; transportation; healthcare; and telecommunications. These sectors increasingly rely on networked systems and applications. Some examples include:

“On June 10, 1999, a 16-in.-diameter steel pipeline operated by the now-defunct Olympic Pipeline Company ruptured near Bellingham, Washington, flooding two local creeks with 237,000 gallons of gasoline. The gas ignited into a mile-and-a-half river of fire that claimed the lives of two 10-year-old boys and an 18-year-old man, and injured eight others. Computer security experts who recently reexamined the Bellingham incident called its victims the first verified human casualties of a control-system computer incident. They argue that government cyber security standards currently under debate might have prevented the tragedy.”

—Wired.com, April 2008

“In 2005, a hacker was able to remotely access the systems of a hospital in the U.S. As a result, they were able to lock the operating room doors, and turn off pagers and other critical systems.”

—Computerworld, February 13, 2006

“Researchers have discovered a rare bug in a Windows-based control software package used by as many as one-third of the world’s industrial plants.... According to the National Vulnerability Database, the flaw earns a 7.5 CVSS score, out of 10. A successful exploit could permit unauthorized access, information disclosure, and service disruption.”

—Dan Kaplan, “Rare SCADA Vulnerability Discovered,” *SC Magazine*, May 2008

“We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet.”

—CIA analyst Tom Donahue, on a statement posted by the SANS Institute

A comprehensive server and application protection system provides targeted protection for the platforms used to run mission-critical applications, including Windows, Solaris, Linux, and other UNIX platforms, as well as virtualized servers. It detects and prevents attacks that target these systems, and alerts staff the moment an attack has been attempted, enabling preemptive measures to be taken. It shields software vulnerabilities commonly found in operating systems, as well as enterprise and industry applications that organizations rely on, such as electronic health records (EHR) or supervisory control and data acquisition (SCADA), helping ensure the availability and integrity of these systems. It detects changes to critical system and application files, and monitors system and application log files for important security events that require attention, significantly increasing the level of protection provided.

# Server and Application Protection— Behind the Lines

## REVENUE AND BUSINESS CONTINUITY

Server and application protection is integral to business continuity. By preventing attacks and detecting changes that result in downtime to systems, it enables organizations to protect or maintain their revenues and to avoid costs related to acquiring new customers to offset lost customers. According to the Ponemon Institute, lost business continues to dominate the cost of a data breach, accounting for 65 percent of breach costs. The Yankee Group's 2004 report *Host Intrusion Prevention Systems Are Here to Stay* calculated the reported revenue loss related to downtime to be \$90,000/hour (transportation and retail), \$100,000/hour (e-commerce), \$1,200,000/hour (media), \$2,600,000/hour (banking), and \$4,500,000/hour (brokerage).

An attack that disrupts operations—for example, to a customer-facing application or an e-commerce server—can result in lost sales as frustrated customers shop or go elsewhere. A 2005 EDS survey found that almost one-third of North American consumers would close all accounts and move to another bank if their personal data were compromised. In the event that an incident results in the permanent loss of a customer, then the lifetime value of a customer relationship, along with the costs to acquire a new customer, have to be factored in. The Ponemon Institute's *2005 National Consumer Survey on Data Security Breach Notification* offers this sobering observation: "In a national survey of more than 1,000 victims of personal data security breaches, nearly 20 percent said they had already terminated their relationships with companies that maintained their data, while another 40 percent said they might do so. And nearly 5 percent of those surveyed said they had hired lawyers to seek legal recourse after their data was put at risk."

An April 2007 report from Javelin Strategy & Research, *Data Breaches and Buyer Behavior*, further supports this assessment. It stated that three in four consumers indicated they will stop shopping a merchant if a data breach occurs. Further, it indicates that "when little is known about a data breach, half of all consumers automatically consider the merchants where they shop to be at fault. However, 85 percent will reward merchants who are perceived as security leaders with increased purchases."

Equally, in the event of a security breach that exposes customer or personal information, customer churn or turnover rates often increase. The Ponemon Institute's *2007 Annual Study: Cost of a Data Breach* indicated that following a data breach, organizations suffered an average increased customer churn rate of 2.67 percent.

The potential cost of a data breach is a serious concern for any organization, and a powerful consideration in selecting protective IT measures.

## THE TREND MICRO/THIRD BRIGADE ALLIANCE

Trend Micro is working with industry leaders such as Third Brigade to create powerful, effective solutions for business IT security. Server and application protection for dynamic datacenters is only part of the equation in Trend Micro's ongoing efforts to provide the best in information security for your organization.

Trend Micro, Incorporated, is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).



# Server and Application Protection— Behind the Lines

Third Brigade specializes in server and application protection for dynamic datacenters. Its advanced software and vulnerability response service enables virtual machines and physical servers to become self-defending—safe from the latest online threats. This comprehensive, proven protection helps customers prevent data breaches and business disruptions. It enables compliance, supports operational cost reductions, and addresses the dynamic nature of datacenters, including virtualization and consolidation, new service delivery models, and cloud computing. Third Brigade also owns and maintains OSSEC, the Open Source Host Intrusion Detection Project, actively used in 50 countries around the world.

## TREND MICRO™

Trend Micro, Incorporated, is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at [www.trendmicro.com](http://www.trendmicro.com).

## TREND MICRO, INCORPORATED

10101 N. De Anza Blvd.  
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651  
phone: 1 +408.257.1500  
fax: 1 +408.257.2003

[www.trendmicro.com](http://www.trendmicro.com)

