



# Regulatory Compliance Drives the Need for an Enterprise Security Framework

A Trend Micro White Paper



# REGULATORY COMPLIANCE



## CONTENT

### I. REGULATORY COMPLIANCE AND GOVERNANCE TAKE CENTER STAGE

- The Challenges Mount
- IT Feels the Heat
- Unexpected Benefits of Compliance

### II. SURVEY OF REGULATIONS

#### • Financial Accounting Regulations

- The Basel Accords (Europe)
- Check 21 (United States)
- Sarbanes-Oxley (United States)

#### • Information Privacy Regulations

- California SB 1386 (United States)
- Data Protection Act of 1998 (United Kingdom)
- Electronic Funds Transfer Act (United States)
- European Union Directive 95/46/EC (Europe)
- Fair Credit Reporting Act (United States)
- Federal Privacy Act (Australia)
- Gramm-Leach-Bliley Act (United States)
- Habeas Data Bill (Argentina)<sup>2</sup>
- HIPAA (United States)
- Law for the Protection of Private Life (Chile)<sup>1</sup>
- Personal Information Protection and Electronic Documents Act (Canada)
- Personal Information Protection Law (Japan)

### III. THE CHANGING FACE OF ENTERPRISE SECURITY

- The Threat Landscape is Changing—And Not for the Better
- Balancing Risk/Reward in Enterprise Security
- The Rewards of Enterprise Security
- The Dynamics of Enterprise Security

### IV. THE ROLE OF INFRASTRUCTURE STANDARDS

- IT Controls Essential to Security
- Control Objectives for Information and Related Technology (COBIT)
- The Information Technology Infrastructure Library (ITIL)
- ISO/IEC 17799 (BS 7799 in Europe)

### V. THE ENTERPRISE SECURITY FRAMEWORK

- Trend Micro Enterprise Protection Strategy Solution Summary

---

<sup>1</sup> Argentina and Chile were the first Latin American countries to adopt data protection laws. Although weaker than their European and American counterparts, the laws nevertheless pose new challenges to organizations operating in either country.

# REGULATORY COMPLIANCE



## Executive Summary

Information is vital to compliance. Reports that demonstrate compliance to regulatory bodies are generated from information about a company's processes and activities. But the growing wave of regulations has placed new demands on how that enterprise information is safeguarded and accessed. Privacy statutes and other regulations dictate how personal information is to be used and disseminated.

This enhanced scrutiny of information has created demands for more rigorous security measures. The foundation of good corporate governance is a well-designed and executed security strategy. In order to truly protect the company, security must incorporate the processes and safeguards necessary to ensure regulatory compliance and prevent disclosures of sensitive personal information as well as corporate intellectual property.

In the quest for a more cost-effective, flexible and holistic approach to security, enterprises are turning to a comprehensive security framework. Solutions integrated within this framework enhance an enterprise's ability to comply with external regulations and internal governance requirements, while reducing the overall cost of compliance and ongoing security operations.

## I. REGULATORY COMPLIANCE AND GOVERNANCE TAKE CENTER STAGE

### ➔ The Challenges Mount

Security imperatives in the enterprise are affected by both regulatory compliance and governance considerations. While they have different driving forces, compliance and governance have similar effects on the modern enterprise.

In one case, a company in a particular industry such as healthcare can be required to comply with regulations concerning protection of patient health information. Another company in a different industry may be compelled to protect client information for governance reasons because it is demanded by the corporation's board of directors. Whether the policy mandates are regulatory or imposed by the internal standards of the corporation, corporations have increased pressure to comply.

### ➔ Compliance challenges

The proliferation of regulations is making compliance tougher. The U.S. Office of Management and Budget reports that nearly 114,000 regulations have been introduced since 1981 in the United States alone.<sup>2</sup> Organizations must comply—or face fines, sanctions, competitive disadvantage or loss of reputation. For some regulations, the corporate entity does not provide protection for individuals: Executives themselves can be fined or even imprisoned for noncompliance.

### ➔ Governance challenges:

At the same time, corporate governance is becoming more complex. High-profile collapses of companies such as Enron and WorldCom have thrust governance into the spotlight. In response, boards of directors are beginning to exercise much-needed oversight, demanding more detailed reports and raising expectations for corporate officers. Auditors challenge accounting statements and require access to detailed records for backup and verification. Investors are more vocal and involved. And a subpoena is always as close as the daily mail.

<sup>2</sup> Regulatory Simplification in the United States: Modest Progress, Large Unfinished Business, Dr. John D. Graham, Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, Executive Office of the President, October 27, 2005.

# REGULATORY COMPLIANCE



## ⊕ IT Feels the Heat

Information technology (IT) is the focal point for the enterprise's compliance and governance strategies. Regulations almost always include restrictions on information—how it is stored, used, and disseminated. In the modern enterprise, IT owns not only the information, but also the infrastructure that manages that information.

Compliance is expensive. These initiatives can siphon vast amounts of time and money from other projects, delaying or shortcutting needed IT infrastructure improvements. Every dollar that goes to compliance may appear to be a dollar that is not being used to acquire customers, deliver products and services, and improve the efficiency of other operations—in short, a dollar wasted.

## ⊕ Unexpected Benefits of Compliance

Yet it doesn't have to be either-or. As IT departments begin to address compliance and governance requirements, they put into place more rigorous IT and security controls. Many companies are finding significant value in those controls—in fact, the benefits to the organization frequently outweigh the costs.

For example, protecting information ensures that regulatory information will not be compromised, and also safeguards vital intellectual property such as product designs and roadmaps, software, customer lists and strategic plans, thereby reducing risk to the enterprise's "crown jewels." Avoiding embarrassing publicity for noncompliance avoids damage to the corporate image and brand equity.

When an enterprise retools key internal processes in response to regulations and governance initiatives, that effort creates opportunities to streamline and rationalize those processes, enhancing productivity and boosting competitiveness. Simply put, better compliance requires better governance, and a properly governed company can compete and deliver more effectively.



## II. SURVEY OF REGULATIONS

While no list of regulations can be comprehensive, this section summarizes some of the more common ones affecting today's enterprise, both in the United States and other countries and explains how they impact an enterprise's security requirements. Two areas of particular interest to many enterprises are regulations concerning financial accounting and information privacy.

### FINANCIAL ACCOUNTING REGULATIONS

#### ➔ **The Basel Accords (Europe)**

The Basel Accords—Basel I and Basel II—are banking supervision recommendations issued by the Basel Committee on Banking Supervision, which is named for Basel, the Swiss city in which the committee meets. Among the provisions of the Basel Accords is capital adequacy, a requirement to maintain a minimum level of capital to protect against unexpected losses. Institutions subject to the Basel Accords are required to retain transaction records for as long as seven years, which imposes a strong information archiving burden on the enterprise IT group. That necessarily impacts the organization's security posture, requiring effective security measures to safeguard the information over its lifecycle.

#### ➔ **Check 21 (United States)**

This act, formally known as the "Check Clearing in the Twenty-First Century Act," revised the rules governing the exchange of checks among financial institutions, creating a more automated check collection system. By eliminating the cost and delays associated with the movement and processing of paper checks, Check 21 has streamlined the check-clearing process and increased profits.

Complying with Check 21 involves implementing a completely digital imaging system to replace the paper-based legacy processes. At the same time, the security measures developed for paper systems are no longer workable in an all-digital age. Moving to digital imaging of checks moves the burden for overall security into the IT department.

#### ➔ **Sarbanes-Oxley (United States)**

The Sarbanes-Oxley Act of 2002 (known also as the Public Company Accounting Reform and Investor Protection Act of 2002), brought about one of the most significant changes to United States securities laws since the 1930s.

Of particular interest to IT professionals is that Sarbanes-Oxley, commonly referred to as SOX, holds corporate officers "responsible for establishing and maintaining internal controls," which necessarily includes controls on how information is protected and disseminated. Sarbanes-Oxley requires an annual internal control report that documents control procedures related to information technology.

# REGULATORY COMPLIANCE



## INFORMATION PRIVACY REGULATIONS

### ➔ California SB 1386 (United States)

California Senate Bill 1386, which took effect on July 1, 2003, requires that financial institutions, insurance companies and other enterprises disclose breaches of security of personal data. A number of recent episodes have brought this problem to public attention. For example, an auditor left a diskette containing thousands of names, social security numbers and account information in the seat pocket of an airplane. Because of SB 1386, that institution had to notify each person, by certified mail, of the breach.

### ➔ Data Protection Act of 1998 (United Kingdom)

The Data Protection Act (DPA) of 1998 is an implementation of EU Directive 95/46/EC and provides for the protection of personal data of citizens and residents of the United Kingdom. Under this act, personal information can only be used for the specific purpose for which it was collected. Furthermore, the act places restrictions on how long such data can be retained. Information covered by DPA includes names, birthday and anniversary dates, addresses and telephone numbers. The enterprise's security measures must be strong to ensure compliance with this regulation.

### ➔ Electronic Funds Transfer Act (United States)

The Electronic Funds Transfer Act, enacted in 1996, requires the federal government to make payments electronically, rather than through traditional paper-based checking methods. These payments represent enormous amounts of money and therefore require secure methods of authentication.

This act also requires financial institutions to enact certain consumer protections, including the prompt investigation and resolution of consumer-reported errors. Consumers have the right to obtain copies of documents used in the investigation.

### ➔ European Union Directive 95/46/EC (Europe)

The member states of the European Union are also signatories of the European Convention on Human Rights (ECHR). ECHR Article 8 articulates a right to respect for one's private and family life, home and correspondence. Historically, the ECHR has interpreted this provision quite broadly.

In an effort to rationalize legislation across EU member countries, the European Commission recently proposed European Union (EU) Directive 95/46/EC, dealing with the protection of personal data. This directive regulates the processing of personal data, whether or not that processing is automated. The responsibility for protecting the data applies to any person or organization using equipment situated within the EU in order to process data. As an example, Yahoo!, eBay and other online businesses process some personal data when trading with EU citizens and, therefore, must comply with the European data protection rules.

### ➔ Fair Credit Reporting Act (United States)

The Fair Credit Reporting Act (FCRA), enforced by the Federal Trade Commission (FTC), is designed to promote the accuracy of information used in consumer and credit reports. It also ensures the privacy of the information gathered for these reports, requiring a robust and effective security infrastructure. Companies that provide information to consumer reporting agencies also have specific legal obligations, including the duty to investigate disputed information.

# REGULATORY COMPLIANCE



## ➔ **Federal Privacy Act (Australia)**

The Federal Privacy Act provides protections for customers' personal financial information that are similar to those enacted in other countries. It affects both public and private organizations, including financial institutions and healthcare providers.

## ➔ **Gramm-Leach-Bliley Act (United States)**

Banks, credit card companies and other financial institutions routinely buy and sell customer information that is private, including bank balances and account numbers. The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, provides limited privacy protections against the sale of consumers' private financial information. Additionally, GLBA offers protections against obtaining personal information through false pretenses, so-called "pretexting."

GLBA includes provisions that affect IT groups directly. Financial institutions are required to securely store personal financial information. In addition, they have to make consumers aware of their policies on sharing personal information, and offer the possibility to opt out. All of these requirements affect the way enterprises handle and disseminate their information, and therefore must be considered in IT infrastructure planning.

## ➔ **Habeas Data Bill (Argentina)<sup>3</sup>**

Argentina's bill prohibits data transfers to countries that do not provide an adequate level of data protection. There are some exemptions to this rule with regard to banking and medical data, and data transfers to international intelligence agencies fighting against terrorism, organized crime and drugs.

## ➔ **HIPAA (United States)**

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996 to allow workers and their families to retain health insurance coverage if they leave or lose their jobs, and to establish national standards for electronic health care transactions and national identifiers for providers, health insurance plans and employers.

Under HIPAA, individuals must be able to access their own health records and request corrections of errors. HIPAA places restrictions on how personal health information can be used, to whom it can be disseminated and under what conditions. Organizations must document their privacy procedures carefully, a task that includes IT procedures related to information security.

## ➔ **Law for the Protection of Private Life (Chile)<sup>3</sup>**

Adopted in October 1999, this law applies to automated and manually stored (?) personal data in the private and public sectors. The law includes some elements of EU Directive 95/46/EC (see above), such as restrictions on the processing of sensitive data. The law allows the processing of personal data without consent when the data is collected from public registers; however the data can only be used internally or shared with associates.

Organizations are obliged to inform individuals about the purposes for which data is collected and whether it is disclosed to third parties. Individuals have the right to access their data without fees, which the institution must produce within two days. They can also request that inaccurate data be corrected or deleted, and can elect to have their information excluded from advertising purposes, market surveys or opinion polls. Civil and criminal penalties may apply for noncompliance.

# REGULATORY COMPLIANCE



## ➔ **Personal Information Protection and Electronic Documents Act (Canada)**

The Personal Information Protection and Electronic Documents Act (PIPEDA) limits trade with nations unless they provide privacy protection equivalent to the EU directives. Under this act, individuals must explicitly authorize and provide specific reasons for the disclosure of personal information. Noncompliance can involve monetary damages and legal sanctions.

## ➔ **Personal Information Protection Law (Japan)**

Taking effect on April 1, 2005, the Personal Information Protection Law provides data privacy regulations covering any company or organization operating in Japan holding personal data on 5,000 or more individuals, including employees. Compliance is regulated by Japan's Ministry of Economy Trade and Industry (METI), which has issued a set of guidelines. Companies must designate a corporate privacy office to oversee compliance. Potential penalties under the law are severe, including a possible six-month jail sentences for managers who fail to adequately protect data.

---

<sup>3</sup> Argentina and Chile were the first Latin American countries to adopt data protection laws. Although weaker than their European and American counterparts, the laws nevertheless pose new challenges to organizations operating in either country.



## III. THE CHANGING FACE OF ENTERPRISE SECURITY

The growing wave of regulations and the push to improve corporate governance has created demands for more rigorous security measures. As government agencies and standards organizations are focusing more on how information is obtained, handled, secured and delivered, the importance of information security grows. If a hacker penetration or malicious threat, such as spyware, compromises private or regulated information, the corporation will not be able to demonstrate compliance. Unintentionally revealing personal information about a company's customers has always been a public relations disaster, but now the stakes are much higher—companies face lawsuits and their officers can be prosecuted.

### THE THREAT LANDSCAPE IS CHANGING—AND NOT FOR THE BETTER

What about the nature of the security threats themselves? On that front, there's both good news and bad news. The good news is that the number and intensity of the more traditional malicious agents such as viruses, worms and Trojans—attacks intended solely to disrupt operations and destroy information—have decreased in recent years. According to research conducted by Trend Labs, these threats combined represented just 52 percent of the total threat landscape.<sup>4</sup> Combine that fact with the high efficiency of the antivirus and other security solutions from tier-one vendors, and the overall danger posed by this class of threat can fairly be said to be trending down.

The bad news is that another class of threat—so-called “grayware”—is on the rise. BOTs, spyware, adware and scripts, once annoyances, now constitute major threats to enterprise networks. Motives have changed, too: “In 2005, the vast majority of threats were inspired by financial gain, rather than the apparent desire for notoriety or bragging rights that influenced malicious behavior in prior years.”<sup>4</sup>

Phishing<sup>5</sup> and pharming<sup>6</sup> attacks are also a major trend as attackers shift to profit-motivated threats. The potential gains for the “bad guys” are substantial. Thieves deploy spyware to capture sensitive information such as bank account information, credit card numbers and passwords, then use that information to steal the assets of individuals and corporations. Luring a single unsuspecting consumer to a phishing or pharming site can result in a payoff of thousands of dollars through credit card fraud. Multiply this by attackers using mass phishing and pharming techniques, and the profit motives via fraud increase tremendously.

Alarming, the profile of the attacker has changed as dramatically as the attack itself. Yesterday's worm or virus writer was a computer whiz, operating solo or with a small group of like-minded hackers, selecting victims more or less by whim. Modern threats come from organized groups, targeting high-worth individuals and organizations where their efforts are most likely to pay off financially. Furthermore, the skill barriers to entry for those with malicious intent are lower, with sample code and other hacking resources easily accessible through the Internet.

One factor working in favor of the attackers is the increasing vulnerability of the global enterprise. The typical enterprise infrastructure is structurally more vulnerable, as mobile workforces and connections throughout the supply and partner chains offer multiple entry points to the enterprise network with varying levels of security.

*“In 2005, the vast majority of threats were inspired by financial gain, rather than the apparent desire for notoriety or bragging rights that influenced malicious behavior in prior years.”*

*– The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast, Trend Micro*

# REGULATORY COMPLIANCE



## BALANCING RISK/REWARD IN ENTERPRISE SECURITY

The challenge for corporate decision-makers looking at an enterprise security solution is to weigh the potential risks (How will this affect my organization?) against potential rewards (How will this bring value to my bottom line?).

The risks of inadequate enterprise security are substantial. When customer data is compromised, the outcome can be highly visible negative publicity, threatening investor and consumer confidence and loyalty. Sensitive intellectual property can be stolen by a competitor or made public. There are potential legal liabilities as well, both civil and criminal. Fines and penalties from regulating organizations and network downtime can cost the organization thousands of dollars. Some recent examples of high-profile security breaches include:

- ④ “Personal electronic information on up to 26.5 million military veterans, including their Social Security numbers and birth dates, was stolen from the residence of a **Department of Veterans Affairs** employee who had taken the data home without authorization.” The New York Times, May 23, 2006
- ④ “Sensitive documents about a Japanese thermal power plant operated by **Chubu Electric Power in central Japan**—including a list of the names and home addresses of the plant’s security personnel—were uploaded to an Internet file-sharing network by a program an employee installed on his computer.” [www.Security.ithub.com](http://www.Security.ithub.com), May 18, 2006
- ④ “A **U.K.-based online retailer** has been identified as the source of a security breach that has resulted in thousands of MasterCard and Visa holders having their credit cards cancelled this week. At least 4,000 U.K. MasterCard holders are believed to have been affected by the breach, which occurred after hackers gained access to credit card details via the retailer.” [www.silicon.com](http://www.silicon.com), April 28, 2006
- ④ “**Time Warner Inc.** said Monday that data on 600,000 current and former employees stored on computer backup tapes was lost by an outside storage company and that the Secret Service is now investigating.” [www.CNNMoney.com](http://www.CNNMoney.com), May 3, 2005

The Privacy Rights Clearinghouse ([www.privacyrights.org](http://www.privacyrights.org)) has documented at least 180 security breaches at corporations, educational institutions and government agency from February 2005 to May 2006, potentially affecting more than 83 million individuals.

<sup>4</sup> “The Trend of Threats Today: 2005 Annual Roundup and 2006 Forecast,” by Trend Micro International

<sup>5</sup> “Phishing” refers to a fraudulent attempt to acquire sensitive information, such as passwords and credit card details, by masquerading as a legitimate business in an e-mail message or other apparently official electronic communication.

<sup>6</sup> “Pharming” attacks features programs, worms, or other virus technologies and are more sophisticated than phishing schemes. When users type a valid URL into browser’s address bar, the pharming program redirects the browser to a fraudulent site, in essence hijacking the browser. Pharming attacks are almost always carried out for criminal purposes such as credit card fraud.

# REGULATORY COMPLIANCE



## THE REWARDS OF ENTERPRISE SECURITY

Beyond protecting the enterprise from fines, prosecution and negative publicity, a well-executed enterprise security solution offers both tangible and intangible rewards. It can allow the enterprise to reclaim IT resources—both staff and management time—for use in more strategic ways. Through effective use of automation, an enterprise security solution reduces the overall cost of compliance and security operations.

The ability to ensure the integrity and privacy of information opens the door to a host of profitable new business opportunities with customers and suppliers and others who could directly help to optimize or enhance the value of the supply chain, simply given access. Enabling new types of products and services opens new channels and markets. Effective security creates opportunities to increase revenue while maintaining reliable, cost-effective and timely communication with customers.

## THE DYNAMICS OF ENTERPRISE SECURITY

Enterprises are changing the way they think about—and approach—security from a number of perspectives, including governance, business and technology.

### ➔ Governance

Because of the dramatic growth in regulatory requirements and the increasingly serious consequences of noncompliance, the need to comply is a key driver for enterprise security. But making companies compliant has come to occupy only part of the thinking that determines how information is handled and what level of security is needed. Good governance is also good business.

### ➔ Business

Like any investment, the corporation's investments in security must be assessed in a risk/reward framework. In other words, security—like other IT solutions—must be linked to the overall business goals. The prime directive is to keep the business running by preventing attacks and remediating problems as quickly as possible. And businesses want to link their security investments to investments that are netting improvements by providing stronger marketing capabilities, more profitable financial management and other business initiatives that can realize actual dollar benefits.

### ➔ Technology

The cost and complexity of the IT infrastructure has a profound impact on the enterprise. If the network and data centers can be consolidated and rationalized while meeting the corporate security requirements, then the enterprise can gain competitive advantage and enhance the bottom line. At the same time, companies want their IT investments to work together with security policies and demonstrate that they are, or can be made secure. There is a high degree of security awareness today. Companies want to know that everything they buy is secure and will stand up to the most well-conceived attacks.



## IV. THE ROLE OF INFRASTRUCTURE STANDARDS

### IT CONTROLS ESSENTIAL TO SECURITY

As IT groups work to deploy effective security measures, they realize the need for an internal control framework that features integration across multiple entry points and centralized management. Without a well-organized and designed infrastructure, IT managers cannot ensure that security measures are applied across the entire enterprise and cover all the possible entry and transit points. In addition, addressing compliance requirements in a fragmented way can multiply costs and increase the complexity of the IT infrastructure, making it harder to respond to changes in the regulatory climate, not to mention the competitive environment.

Fortunately, the IT world has established best-practices standards for IT infrastructures, the most significant ones being COBIT, ISO/IEC 17799 (BS 7799 in Europe) and ITIL.

#### ➔ **Control Objectives for Information and Related Technology (COBIT)**

A set of best practices for information (IT) management, COBIT was created in 1992 by the Information Systems Audit and Control Association and the IT Governance Institute. COBIT provides managers, auditors and IT users with a set of generally accepted processes and best practices to maximize the benefits derived through the use of information technology. COBIT also helps enterprises develop IT governance and control internally.

#### ➔ **The Information Technology Infrastructure Library (ITIL)**

A customizable framework of best practices that promote quality computing services in the information technology (IT) sector, ITIL was developed in the late 1980s by the Central Computer and Telecommunications Agency (CCTA). ITIL addresses the organizational structure and skill requirements for an IT organization by presenting a comprehensive set of management procedures with which an organization can manage its IT operations. ITIL is built on a process-model view of controlling and managing operations.

#### ➔ **ISO/IEC 17799 (BS 7799 in Europe)**

An information security standard published in 2005 by the International Organization for Standardization and the International Electrotechnical Commission, ISO/IEC 17799 deals specifically with security, offering recommendations for best practices in information security management. ISO 17799 breaks down its recommendations into:

- *Preservation of confidentiality*—Ensuring that information is accessible only to those authorized to have access
- *Integrity*—Safeguarding the accuracy and completeness of information and processing methods
- *Availability*—Ensuring that authorized users have access to information and associated assets when required



## V. THE ENTERPRISE SECURITY FRAMEWORK

In recent years, many companies have seen a proliferation in the number of point solutions for specific security needs. This approach inevitably creates gaps, which increases risk, and adds to complexity, which increases cost.

Security officers and other IT professionals—including those focusing on compliance—need a comprehensive, integrated solution that reduces risk and complexity while offering even greater levels of security. To help organizations align with business objectives, meet key compliance and governance needs, and be flexible enough to adapt to changing regulations, Trend Micro offers the Enterprise Protection Strategy (EPS).

### THE TREND MICRO ENTERPRISE PROTECTION STRATEGY SOLUTION: INTELLIGENT THREAT PROTECTION

Trend Micro offers integrated, centrally managed solutions designed to provide intelligent threat protection against known and unknown threats in real time. Intelligent rules accurately profile how potential threats spread in the environment and collaborate with other products and services in real time to provide the most comprehensive, reliable threat protection. Trend Micro industry solutions based on Enterprise Protection Strategy are centrally managed to ensure tighter security, lower administration costs and raise IT productivity.

EPS offers product solutions that support four key security functions of a well-defined and comprehensive security strategy beginning with the ability to monitor for potential threats, **enforce** security policy compliance, **prevent** threats from spreading and **recover** infected devices. It also offers central management for efficiency and ease of administration.

#### MONITOR FOR POTENTIAL THREATS

IT staffs frequently lack the resources they need to continuously monitor their networks and systems. They are particularly at risk from zero-day threats, that can fly “under the radar” of existing security measures and disrupt operations before signature updates and other defenses are deployed.

An effective monitoring system collects, analyzes, detects and identifies threats. Automating monitoring increases the effectiveness of IT resources. Real-time detection and intrusion prevention solutions stop known and unknown threats before they interfere with operations or compromise information. Identifying the source of threats helps prevent future outbreaks. Real-time monitoring of the environment helps ensure potential threats—known and unknown—are detected as soon as the first infection occurs.

#### ENFORCE SECURITY POLICY COMPLIANCE

Creating and enforcing enterprise-wide security policies is a necessity, but can be hard to accomplish in enterprises that include thousands of employees and multiple locations. Without effective enforcement, the risk of compromised data is high and regulatory compliance is difficult to achieve. Effective enforcement facilitates regulatory compliance while blocking network access to devices that cannot demonstrate conformance to security policies. Strict enforcement of corporate security policies helps limit network access to compliant users.

# REGULATORY COMPLIANCE



## PREVENT MALICIOUS THREATS FROM SPREADING

To avoid productivity losses and business costs of downtime from threat outbreaks, prevention is key. Without a comprehensive approach to prevention, gaps in coverage create network vulnerabilities and allow threats to penetrate the enterprise.

A sound prevention process must protect all possible network entry points and eliminate the threats that can disrupt business continuity. The solution must also include intelligent outbreak response and isolation of infected segments, decreasing downtime and generating significant ROI. Preventing the spread of malicious threats helps ensure that corporate digital assets are always secure

## RECOVER INFECTED DEVICES

Even the best prevention system cannot ensure 100 percent safety against every possible attack. The enterprise must have a proactive strategy for responding to outbreaks. Effective recovery procedures are necessary to ensure business continuity. Automated recovery for managed and unmanaged devices eliminates the need for dedicated resources, and prevents data corruption and business disruption. Infected devices can be recovered back to the original state to ensure business continuity.

## CENTRAL MANAGEMENT OF ENTERPRISE-WIDE SECURITY POLICY DEPLOYMENT

In many companies, security measures have been added in a piecemeal fashion, creating a complex environment that is costly and difficult to manage. This approach can appear to management as a resource sinkhole instead of a sound investment that enables business growth.

Central management can turn that perception around. A customizable security console that provides an enterprise-wide view of all threats streamlines administration and provides a high level of control for responding to attacks. The result is that security comes to be seen internally as an investment, not a necessary evil.

## SUMMARY

As this paper shows, regulatory compliance and good governance are requiring more and more attention from corporate IT managers. That in turn raises the need to ensure the security and integrity of corporate information. The days are gone when IT groups could get away with point security solutions deployed to specific parts of the infrastructure. Today's more stringent requirements demand a comprehensive security approach.

New threats such as spyware, spam and phishing enter the environment at any time from anywhere and are not tied to specific virus outbreaks. Trend Micro Enterprise Protection Strategy provides around-the-clock protection to prevent threats from spreading and disrupting operations.

For more information on Trend Micro Enterprise Protection Strategy:

- Visit [www.trendmicro.com/en/products/eps](http://www.trendmicro.com/en/products/eps)

### TREND MICRO™

Trend Micro, Inc. is a global leader in network antivirus and Internet content security products and services. The company is focused on providing customers with customized and comprehensive security strategies to manage the impacts of known and unknown threats. Trend Micro has offices in 30 countries and its stock trades on the Tokyo Stock Exchange (4704) and on NASDAQ (TMIC).

### TREND MICRO INC.

10101 N. De Anza Blvd.  
Cupertino, CA 95014  
USA toll free: 1+800-228-5651  
phone: 1+408-257-1500  
fax: 1+408-257-2003  
[www.trendmicro.com](http://www.trendmicro.com)

