


A background image showing a laptop on a desk with a speedometer overlay. The speedometer has numbers from 0 to 60 and a needle pointing towards 40. The scene is in a blurred office setting.

Trend Micro Data Protection

Trend Micro, Incorporated 

 **Addressing Compliance Requirements for Privacy, Data Retention, and e-Discovery**

A Trend Micro White Paper | March 2009

Trend Micro Data Protection: Addressing Compliance

➔ TABLE OF CONTENTS

I. PRIVACY, DATA RETENTION, AND E-DISCOVERY	3
II. IDENTIFYING SUSTAINABLE COMPLIANCE SOLUTIONS	4
III. THE TREND MICRO ADVANTAGE	6
IV. TRUST A SECURITY INDUSTRY LEADER	8

Trend Micro Data Protection: Addressing Compliance

Protecting individual and financial data, retaining data, and meeting e-discovery requirements are common compliance requirements across geographies and industries. Finding accurate, usable, and cost-effective solutions for meeting these requirements can make the difference between achieving compliance goals or leaving the organization vulnerable through unsecured use of sensitive data. Trend Micro security solutions for endpoint data leak protection, email encryption, and email archiving help organizations meet their compliance requirements – easily and cost-effectively.

I. PRIVACY, DATA RETENTION, AND E-DISCOVERY

At its simplest, “compliance” is the adherence to an accepted policy or set of requirements. Policies can range from those that help the business avoid worst-case scenarios – such as customer churn, litigation, and fines for noncompliance – to the “should haves,” including IT security standards and corporate mandates to protect its brand and stakeholder confidence.

Meeting compliance regulations requires protecting specific types of data and establishing controls to ensure that requirements are met on an ongoing basis. For more information about the regulatory landscape and specific requirements, please see *Protecting Information in an Increasingly Leaky World*, a Trend Micro white paper.

Figure 1: Protected data types and data requirements

Protected Data Types and Requirements	Description
PII: Personally Identifiable Information	Social security number/national identification number, drivers license number, address, phone number
PCI: Payment Card Industry	Credit card numbers, Card Verification Value (CVV), expiration date
PHI: Protected Health Information	Medical diagnosis codes, disease names, medication names, patient names
PFI: Personal Financial Information	Financial account number, credit score
PFI Access Control	Monitor privileged user access to company financial data, separation of duties for data and processes impacting financial reporting
Audit	Covers best practices to validate controls to address regulation

Trend Micro Data Protection: Addressing Compliance

Privacy Requirements

Privacy of an individual's personal, medical, and financial data is of utmost concern to enterprises for regulatory compliance. Regulations in place to protect individuals' privacy usually require that data associated with that individual is not visible to unauthorized users. This requires an ability to detect sensitive content, and report, block, or encrypt it. For example, protecting email and attachments from unwanted eavesdropping, tampering, and spoofing requires encryption, recently mandated by the state of Nevada to protect PII associated with Nevada residents. Solutions for Data Leak Prevention (DLP) that perform content monitoring and filtering can also be used for helping to meet a wide range of compliance requirements.

Data Retention Requirements

Data retention laws vary greatly, but many specify that certain types of data be stored for specific periods of time. For example, the European Union Directive 2006/24/EC requires Member States to ensure that communications providers retain data for anywhere from six months to two years. In addition, records must only be produced to entitled parties, and if they contain sensitive data, they should be kept confidential through encryption.

e-Discovery Requirements

Electronic discovery has become critical in a wide range of applications, such as litigation support, when evidence must be produced in a court of law to prove or refute a claim. Requirements include the ability to search for specific data in a timely manner and produce results that maintain chain of custody to prevent tampering with evidence.

II. IDENTIFYING SUSTAINABLE COMPLIANCE SOLUTIONS

In an ideal world, measures to assure privacy, data retention, and e-discovery would cover all networks and nodes where sensitive data is transported, stored, or used. This would include end-user systems, databases, file servers, email servers, and network gateways. However, this level of protection is unrealistic due to operational limitations. Enterprises must address compliance through people, enforced policies and procedures, and technology:

- **People:** employees and other authorized users of business data, such as partners or suppliers, require training and education on the organization's sensitive data use policies.
- **Procedures:** processes must be in place to facilitate secure data creation, modification, storage, transmission and destruction.
- **Technology solutions:** are deployed to automate as many of these processes as possible.

Technology must support business policies and enforce user training. Buying a product cannot ensure compliance, however, integrating sustainable controls into an existing infrastructure greatly increases likelihood of achieving and maintaining compliance.

Solution Requirements

Technology solutions that are designed to protect privacy, support data retention strategies, and facilitate e-discovery must be accurate, usable, and cost-effective.

Trend Micro Data Protection: Addressing Compliance

Accuracy is Critical

The core element of many regulations is the ability to detect sensitive content. Monitoring, scanning, and discovery capabilities must accurately detect content with few to no false positives. The goal is to successfully identify sensitive content without blocking legitimate business processes, such as emails to business partners. The solution must also be intelligent enough to catch pieces of restricted content in an otherwise approved communication. For example, users often copy and paste regulated content, such as a person's name, address, or social security number, or company-sensitive content, such as intellectual property or brand formulas, into emails or onto peripheral storage devices. Solutions should be able to detect and deal with restricted content in a manner consistent with the business's security policy.

Usability is Key to Achieving Desired Results

If the compliance solution is difficult to use, deploy, or manage, probability is high that it will:

- Not be used and therefore leave the organization vulnerable
- Be used incorrectly, placing the organization in danger of violation
- Be used inefficiently, requiring too much time or too many resources to manage, increasing total cost of ownership beyond the solution's value

In the case of e-discovery, relevant content must be produced in a timely manner to avoid fines. If data discovery is difficult for end users, it increases cost and extends timelines, likely resulting in e-discovery violations. For email encryption, requiring senders and recipients to use a complicated key management process can hamper routine business processes and cause undesirable escalations to senior management. For example, according to the IDC Encryption Usage Survey (August 2008, IDC #213646), approximately 70 percent of organizations say that cost/expense are critical to a choice of encryption product, and almost 80 percent agree that ease of use is critical.

Cost Effectiveness Results from Efficiency

Data protection solutions that integrate with existing infrastructure help eliminate costs associated with provisioning new technologies. For example, because most enterprises already have an email anti-spam solution deployed, a compatible email encryption solution can reduce hardware costs and improve application performance.

For cumbersome processes like encryption key management, a hosted solution may be more cost-effective than a premises-based solution, since hosted solutions do not require the same investment in hardware and IT resources for deployment and management. In the case of spam, large volumes continuously strain email servers and archive solutions, cluttering the archive with garbage emails and preventing efficient search of legitimate emails. A hosted anti-spam solution can block spam in the cloud, before it reaches the company network. By eliminating the need for the organization to purchase additional storage for coping with high spam volumes, a hosted anti-spam solution can also reduce archiving and storage costs while accelerating retrieval of emails required by data retention or e-discovery regulations.

III. THE TREND MICRO ADVANTAGE

Training employees and adapting processes to achieve compliance are essential elements of a compliance strategy. Success however, also depends on implementing proven, policy-based endpoint DLP, email encryption, and email archiving solutions – and ensuring that they are accurate, usable, and cost-effective. Trend Micro helps organizations address industry regulations with endpoint DLP, email encryption, and email archiving solutions. Trend Micro solutions also go beyond addressing compliance to help protect users and sensitive data from the growing threat of web-based attacks, such as viruses, malware, and malicious techniques used to steal data. The Trend Micro™ Smart Protection Network, a next-generation, cloud-client content security infrastructure helps detect and contain threats before they reach the business.

Figure 2: Trend Micro Protection Solutions

Business Need	Trend Micro Solutions
Protect sensitive data from insider threats Educate employees	<ul style="list-style-type: none"> • Trend Micro LeakProof™
Protect sensitive email and attachments	<ul style="list-style-type: none"> • Trend Micro Email Encryption for InterScan™ Messaging Hosted Security • Trend Micro Email Encryption Gateway • Trend Micro Email Encryption Client
Provide e-discovery capabilities Reduce email storage costs	<ul style="list-style-type: none"> • Trend Micro Message Archiver
Protect email with anti-spam, anti-virus, anti-spyware, anti-phishing, and content filtering	<ul style="list-style-type: none"> • Trend Micro InterScan Messaging Security • Trend Micro ScanMail™ for Exchange/Domino
Protect user endpoints with antivirus, anti-malware, anti-spyware, personal firewall, host intrusion prevention system	<ul style="list-style-type: none"> • Trend Micro OfficeScan™ • Trend Micro Endpoint Security Platform
Provide complete protection for messaging, endpoints, and web security against inappropriate content, spam and phishing, spyware, rootkits, bots, viruses and trojans, web threats, worms, and network attacks	<ul style="list-style-type: none"> • Trend Micro NeatSuite™ Advanced

Trend Micro Data Protection: Addressing Compliance

Data Leak Prevention: Trend Micro LeakProof

Data leak prevention solutions are designed to protect sensitive information such as customer, employee and patient data as well as intellectual property by monitoring and preventing information leaks across multiple threat vectors, including email, webmail, instant messaging, USB drives, and CD/DVDs. However, many solutions that are designed to monitor and block sensitive data:

- Scan data at endpoints too slowly
- Handle a limited number of documents
- Fail to detect data in multiple languages
- Do not support partial data matching
- Cannot identify and protect sensitive data when users are offline

LeakProof prevents data leaks with a unique approach that combines endpoint-based policy enforcement with highly accurate fingerprinting and content-matching technology. Pre-configured detection and validation modules for privacy data, such as those defined by PII, PHI, and PCI regulations, are included, making the process of detection and enforcement simple for IT and security staff. The Trend Micro LeakProof fingerprinting technology supports full or partial matches using a language-independent technology, with ultra-small, locally-stored signatures that enable policy enforcement for endpoints – whether they are on or off the network.

For data at rest, LeakProof performs data inventory across end-user systems, identifying sensitive data on employee endpoints. LeakProof also monitors data in motion across numerous communications channels – email, webmail, instant messaging, and FTP – as well as data in use on external devices such as USB-based removable storage, CDs, DVDs, and printers. Sensitive data can be blocked or encrypted, depending on company policy, preventing violations from occurring.

Demonstrating compliance requires validating data protection controls against the data protection policy. LeakProof provides tamper-proof activity logs and compliance reports that highlight violations and the actual content. To improve compliance over time, users are also educated at the point of the violation. A pop-up screen explains the organization's policy and prompts for justification of the prohibited action.

Secure Email with Trend Micro Email Encryption

Email encryption solutions enable organizations to enforce compliance requirements and to ensure that confidential information is delivered securely. However, protecting email and attachments from unwanted eavesdropping, tampering and spoofing using traditional encryption solutions is often complex, placing additional burdens on IT management.

Trend Micro Email Encryption solutions operate using the existing email infrastructure. They provide universal reach, allowing organizations to deliver private email to any address without pre-registering recipients.

Trend Micro Data Protection: Addressing Compliance

Trend Micro's hosted key management service manages public and private keys for businesses, allowing them to gain robust encryption capabilities for addressing compliance requirements without the cost and complexity associated with maintaining public keys, securing private keys, or managing certificate revocation lists. With Trend Micro, even small or medium-sized businesses can cost-effectively address encryption requirements. And businesses that choose Trend Micro Email Encryption can effortlessly deliver secure messages to people outside of their organizations, such as partners and customers. To support audit requirements, Trend Micro Email Encryption also provides tamper-proof activity logs and compliance reports that highlight any violations and the actual content in question.

Manage Data Retention and e-Discovery: Trend Micro Message Archiver

Many organizations required to comply with e-discovery and data retention laws find that most email archiving solutions come with high deployment and integration costs. In addition to ensuring timely delivery of content, the email archiving solution must also help enforce employee privacy policies. Trend Micro Message Archiver makes it far easier and more cost-effective to meet these requirements. As an easy-to-deploy, out-of-the-box solution, it provides:

- Clear chain of custody with encryption and fingerprinting of emails and access logs to protect against tampering, theft, and destruction.
- An unrivaled "Data Guardian" feature that provides complete and accurate disclosure and alerting to archive access by privileged users. The Data Guardian safeguards against archive search without cause or other abuse.
- Encryption of archived emails to protect employee privacy.
- Simplified deployment, with built-in configurations for integration with common email systems.
- Indexing for fast searches and compression for efficient storage
- Signed and encrypted activity logs

IV. TRUST A SECURITY INDUSTRY LEADER

As a global leader in Internet content security, Trend Micro focuses on securing the exchange of digital information. Based on extensive content security expertise, Trend Micro correlates threat data from more than 5 billion dynamically rated websites, spam sources, and files every day. Thousands of companies continue to put their trust in Trend Micro – a company with 20 years of experience dedicated to content security and expertise based on a history of innovation.

To learn more about Trend Micro solutions for addressing regulatory compliance, contact your Trend Micro representative or visit www.trendmicro.com.

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.

TREND MICRO INC.

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

