TREND MICRO™ Securing Your Web World

Trend Micro™

LeakProof™ 3.0

Comprehensive Protection of Sensitive Data At-Rest, In-Use, and In-Motion

Loss of proprietary information and intellectual property can trigger fines, litigation, brand damage, and bad press. To protect sensitive data, enterprises need an effective data leak prevention (DLP) solution that monitors potential information leaks at the point of use. However, the explosion of messaging systems, wireless networking, and USB storage devices has made the protection of critical enterprise data difficult. As a result, enterprises are experiencing an increase in the loss and even theft of data assets by employees or contractors who maliciously or accidentally leak data.

Furthermore, achieving regulatory compliance with business governance and privacy regulations such as SB-1386, GLBA, EU DPD, Sarbanes-Oxley, and HIPAA requires comprehensive security policies to keep information confidential and protect customer privacy. Meeting these challenges requires intelligent content filtering solutions that enforce security policies and educate employees about the proper handling of information.

Trend Micro™ LeakProof™ prevents data leaks with a unique approach that combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology. A software client and an appliance comprise the complete LeakProof solution:

- **LeakProof Anti-Leak Client**—includes non-intrusive, powerful monitoring and enforcement software that detects and prevents data leaks at each endpoint. The client communicates with the DataDNA™ Server to receive policy and fingerprint updates and report violations to the server.
- **LeakProof DataDNA™ Server**—is an appliance that provides a central point for visibility, policy configuration, and fingerprint extraction from content sources. A web-based interface supports an administrative workflow for discovery, classification, policy setting, monitoring, and reporting.

COMPREHENSIVE PROTECTION: DATA, PORTS, CHANNELS, NETWORKS

LeakProof provides the broadest coverage available for the network perimeter and endpoints. Coverage includes network channels such as HTTP/S, SMTP, Webmail, FTP, and IM, plus endpoint input/output such as file transfers to USB drives or CD/DVD burners. Built-in filtering modules inspect content before it is encrypted to protect activity through Web browser and email applications. IT managers can disable specific devices easily.

ACCURATE DETECTION WITH DATADNA™ TECHNOLOGY

Patent-pending technology detects sensitive data with the highest levels of accuracy and performance. Multiple matching engines provide real-time filtering using fingerprinting, regular expressions, keywords, and metadata. Powerful algorithms extract information from content to create a unique DNA sequence or "fingerprint" for each document. This "fingerprint" enables endpoint-based enforcement on or offline.

NEW! INTERACTIVE EMPLOYEE EDUCATION, ENCRYPTION, AND WORKFLOW

Interactive "alerts" enable IT managers to define content-sensitive dialog boxes that appear directly on an employee's computer screen. These dialog boxes contain custom URL links that educate employees on the appropriate handling of confidential information. Unauthorized transfers are blocked, or employees can be required to use the built-in data encryption module to copy data onto USB devices.

DATA DISCOVERY AND SECURITY SCANNING

Through continuous monitoring, LeakProof™ provides corporate security and compliance officers with a radar-like capability to locate sensitive information and decrease the risk of data breaches. LeakProof discovers unauthorized information residing at endpoints, including laptops, desktops, and servers.

PREVENT DATA LEAKS

- Mobile, Branch, Corporate
- Endpoints Online, Offline
- Corporate Networks
- Public Networks
- USB, Bluetooth, WiFi, Email
- Data in Motion, at Rest, in Use

THREAT PROTECTION

- Data Leaks
- Data Loss
- Insider Threats

KEY BENEFITS

- **Protect Privacy** - Monitor and prevent improper use of customer and employee information
- **Protect Intellectual Property** - Discover, classify, and protect critical company assets
- **Comply with Privacy Regulations** - Monitor usage, scan endpoints, and educate employees to reduce risk
- **Educate Employees** - Customize interactive dialogs for employee education and workflows
- **Discover Sensitive Data** - Find sensitive data on laptops, desktops, and servers

"Trend Micro LeakProof™ is giving administrators greater control over what employees see and what they are allowed to do through interactive dialogs that are informative and helpful in resolving security issues."

Martin Hodgett, CIO
Orchard Supply Hardware (OSH)

LEAKPROOF DATA LEAK PREVENTION FEATURE SUMMARY

Sensitive Information Matching

- Fingerprint, regular expression, keyword, metadata matching
- Structured and unstructured data
- Partial matching of text files and exact matching of binary files
- Language independent

Granular Security Policies

- Logging, server-side alerts, client-side alerts, blocking, encryption, justification
- Separate policies for online and offline violations
- Endpoint domain and group-based security policies
- Configurable security boundaries–LAN, PC, trusted/not trusted email domains

Endpoint Topology Discovery and Management

- Enterprise endpoint computer discovery
- Real-time map display of endpoint status
- Centralized client status monitoring and management
- Detailed display of endpoints status
- Discovery of unauthorized I/O devices at endpoints

Device and Application Control

- Control of all I/O devices: USB, CD/DVD, floppy, Bluetooth, IrDA, imaging devices, COM and LPT ports etc
- PrintScreen (PrtSc) function blocking

Monitoring and Reporting

- Real-time dashboard and security violation reports summarized by endpoints, users, etc.
- Trend analysis and violation channel breakdown
- Scheduled and on-demand reports of security violations
- Optional forensic capture feature logs the actual file violation on the DataDNA server for later inspection

Compliance Templates

- Preconfigured classifications and policies supporting regulatory compliance such as PCI, GLBA, SB-1386, and SOX
- Built-in rules with validation modules for entities such as social security, credit card, ABA routing, Canadian and Chinese National ID, and American name recognition

System Administration and Scalability

- Web browser management interface
- Role-based administration and sensitive content access control
- Integration with LDAP and Active Directory
- Management server clustering for enterprise scalability
- Secure communication between endpoint and server via SSL

MINIMUM SYSTEM REQUIREMENTS

LeakProof Anti-Leak Client Software

- **Supported Platforms:** Microsoft Vista, Windows XP, Windows 2000, Windows 2003 Server

LeakProof DataDNA Server Appliance

- Purpose-built 1U rack-mountable appliance
- Security hardened
- Gigabit NIC
- Available in Single/Dual CPU
- Memory: 2GB/4GB
- Storage: Dual 160GB/500GB RAID
- Power: Single/Dual PSU

LeakProof DataDNA Server Virtual Appliance—VMWare

- CPU: Intel XEON or AMD Opteron dual-core
- Memory: 2GB
- Storage: 160GB

COMPREHENSIVE COVERAGE OF FILE TYPES, APPLICATIONS, AND DEVICES

LeakProof DataDNA Server

The LeakProof DataDNA Server appliance coordinates with the LeakProof Anti-Leak Client software to protect sensitive information assets from data loss, data theft, and insider threats.

File Types Supported

- Recognizes and processes 300+ file types
- Microsoft™ Office files including Office 2007: Microsoft Word, Excel, PowerPoint, Outlook™ email; Lotus™ 1-2-3, OpenOffice, RTF, Wordpad, Text, etc.
- Graphics files: Visio, Postscript, PDF, TIFF, etc.
- Software/engineering files: C/C++, JAVA, Verilog, AutoCAD, etc.
- Archived/compressed files: Win ZIP, RAR, TAR, JAR, ARJ, 7Z, RPM, CPIO, GZIP, BZIP2, Unix/Linux ZIP, LZH, etc.

Network/Applications Controlled

- Email: Microsoft Outlook, Lotus Notes, and SMTP Email
- Web mail: MSN/Hotmail, Yahoo, GMail, AOL Mail, and more
- Instant Messaging: MSN, AIM, Yahoo, and more
- Network Protocols: FTP, HTTP/HTTPS, and SMTP

Endpoint Devices Controlled

- USB, SCSI, (S)ATA, EIDE, PCMCIA, CD/DVD, floppy, Bluetooth, IrDA, WiFi, printers, imaging devices, COM port, LPT port, etc.