

Trend Micro™

LeakProof™ 3.1

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, customer churn and bad press. Yet managing the explosion of messaging systems, wireless networking, and USB storage devices has led to an increase in the loss and 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.

Trend Micro™ LeakProof™ is a data leak prevention (DLP) solution that protects customer and employee privacy, and intellectual property. Its unique approach combines endpoint-based enforcement with highly accurate fingerprinting and content matching technology. LeakProof provides the broadest protection of any endpoint client including email, Webmail, USB, IM, FTP and HTTPS—whether on or offline. The LeakProof solution includes both client and server components, as described below.

- LeakProof Client—Non-intrusive, powerful monitoring and enforcement software detects and prevents data leaks at each endpoint. Communicates with the LeakProof Server to receive policy and fingerprint updates and report violations.
- LeakProof Server—Centralized visibility streamlines policy configuration and fingerprint extraction from content sources. Appliance web-based interface supports workflow for discovery, classification, policy setting, monitoring, and reporting.

LEAKPROOF BENEFITS

Comprehensive Protection

- Provides the broadest coverage available for the network perimeter and endpoints
- Defends network channels such as HTTP/S, SMTP, Webmail, FTP, and IM
- Safeguards endpoint input/output such as file transfers to USB drives or CD/DVD burners
- Protects web browser and email with built-in filtering to inspect content before it's encrypted

Accurate Detection

- Detects sensitive data using DataDNA™ technology for the highest levels of accuracy and performance
- Employs multiple matching engines for real-time filtering
- Creates a unique DNA sequence for each document using a powerful algorithm
- Uses low-impact fingerprints for endpoint-based enforcement on or offline

Interactive Education and Encryption

- Enables content-sensitive alerts to appear directly on an employee's computer screen
- Uses dialog boxes to educate employees on appropriate handling of confidential information
- Blocks unauthorized transfers
- Enforces use of built-in data encryption module to copy data onto USB devices (optional)

Data Discovery and Security Scanning

- Continuously monitors to decrease the risk of data breaches
- Gives compliance officers radar-like capability to locate sensitive information
- Discovers unauthorized data residing at endpoints, including laptops, desktops, and servers

Granular Administration

- Empowers IT managers to easily disable specific devices
- Improves productivity for large file transfers with bulk encryption
- Dramatically reduces scan time with incremental fingerprint scanning

PREVENT DATA LEAKS

- Mobile, branch, corporate
- Endpoints online, offline
- Corporate networks
- Public networks
- USB, Bluetooth, Wi-Fi, 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 FEATURES**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

- Endpoint computer discovery
- Real-time map display of endpoint status
- Centralized client status monitoring and management
- Detailed display of endpoints status
- Discovery of unauthorized input/output devices at endpoints

Device and Application Control

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

Monitoring and Reporting

- Real-time dashboard and security violation reports summarized by endpoints, users, and more
- 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 LeakProof 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 for delegated administration and endpoint discovery
- Secure communication between endpoint and server via SSL

COMPREHENSIVE COVERAGE OF FILE TYPES, APPLICATIONS, AND DEVICES**LeakProof Server**

The LeakProof Server coordinates with the LeakProof Client to protect sensitive information assets from data loss, data theft, and other 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.

MINIMUM SYSTEM REQUIREMENTS**LeakProof Client (Software)**

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

LeakProof 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 Server (Virtual Appliance)—VMWare

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



©2008 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro i-ball logo, DataDNA, and LeakProof are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. [DS01LeakProof3-1_081124US]

www.trendmicro.com