

Trend Micro™

Data Loss Prevention

Comprehensive Data Loss Prevention with Lower Cost and Complexity

Data loss prevention (DLP) is critical to stop accidental and malicious data leaks—whether it's customer information, financial data, intellectual property or trade secrets. One incident could cost millions in brand damage, lost business, fines, and litigation.

The challenge for data loss prevention is identifying, tracking, and securing all confidential data at rest, in use, and in motion. This is increasingly difficult due to growing risk factors, including distressed employees in fear of layoffs, mobile workers, and leakage points like USB drives, webmail, IM, and CDs/DVDs.

Trend Micro™ Data Loss Prevention (DLP) is a family of solutions that secure your private data and intellectual property, while reducing complexity and costs. You'll gain broad coverage, high performance, and deployment flexibility needed to comply with regulatory mandates that protect employee and customer data. Trend Micro DLP solutions also offer advanced DataDNA™ fingerprinting to secure unstructured data and intellectual property and protect all data modalities: data at rest, data in use and data in motion.

- **Trend Micro™ DLP for Endpoint** – non-intrusive monitoring and enforcement client software detects and prevents data loss at each endpoint, across the broadest variety of threat vectors—whether online or off.
- **Trend Micro™ DLP for Network*** – powered by the Trend Micro Smart Protection Network™, monitors your network 24x7 to identify and document data loss of sensitive information and intellectual property across a variety of threat vectors. **Expected Q2 2010*
- **Trend Micro™ DLP Management Server** – provides a central point of visibility and control for discovery, fingerprint extraction, policy enforcement, and reporting violations. The server is available as a hardware appliance or software virtual appliance—for greater flexibility and lower costs.

DATA LOSS PREVENTION FEATURES

Lower Cost and Complexity

- Provides faster time to protection with new push-button compliance templates
- Saves time with new UI, Active Directory integration, and user/group policies
- Streamlines IT with delegated administration plus end user device and access control
- Offers pricing options and flexibility with two versions and multiple form factors

Expanded Privacy Protection

- Helps ensure compliance with more inspection points—for the broadest coverage
- Offers new filters for Skype, P2P, Windows File Share, ActiveSync, clipboard, and network printers
- Defends other network channels including email, webmail, HTTP/S, FTP, and IM
- Secures endpoint input/output such as file transfers to USB drives and CD/DVDs

Data Discovery and Scanning

- Locates sensitive data stored on laptops, desktops, and servers with radar-like precision
- Employs policy enforcement and multiple matching engines for real-time protection
- Continuously monitors data at rest, in use, and in motion to prevent data loss
- Blocks unauthorised data transfers

Advanced Intellectual Property Protection

- Protects unstructured proprietary data using DataDNA™ fingerprinting technology—for superior accuracy
- Reduces fingerprint size by over 90%, increasing scalability without sacrificing accuracy
- Improves performance with new endpoint fingerprint crawler for real-time identification

Interactive Employee Education and Remediation

- Alerts employees to sensitive content and risky behavior with options to block or allow with proper justification
- Uses dialog boxes to educate employees on appropriate handling of confidential information
- Does not impact business processes

DATA LOSS PREVENTION

- Data in motion, at rest, in use
- Mobile, branch, corporate
- Endpoints online, offline
- Corporate networks
- Public networks
- P2P, Skype, Active Sync and more

THREAT PROTECTION

Internal Threats

- Accidental data loss
- Malicious data loss

External Threats

- Data-stealing malware
- Hackers

KEY BENEFITS

- **Protect Privacy** - Discover, monitor and prevent confidential data loss—on or off network
- **Secure Intellectual Property** - Identify, monitor, and protect trade secrets
- **Comply with Regulations** - Implement controls for protection, visibility, and enforcement
- **Educate and Remediate** - Customise interactive dialogs to stop risky employee behavior and data loss
- **Discover Sensitive Data** - Find sensitive data on laptops, desktops, and servers

Customers Recommend It

“ Even with established procedures for checking out data, it wasn't until we had the visibility offered by Trend Micro [DLP] that we could be assured—and prove—that we were achieving the desired level of data protection. ”

Lucia Johnson

Information Systems Manager
Associated Fuel Pump Systems Corporation

Trend Micro DLP		
Key DLP Features	for Endpoint	for Network
Discover, monitor, block and encrypt private data with real-time view of endpoint status	✓	Discover and monitor only
High-performance, low-impact filtering based on keywords, meta data and regular expressions	✓	✓
Granular policy enforcement by ActiveDirectory user or group, Windows domain, and endpoint groups	✓	✓
Control of input/output devices: USB, CD/DVD, IrDA, Bluetooth, COM and LPT ports, and more	✓	
Broad coverage of communication systems: email, webmail, IM, P2P, FTP, Skype, Windows File Share, ActiveSync, and more	✓	✓
Low administration and TCO with new UI, alerts, 10xs faster deployment, compliance templates, encryption, and more	✓	✓
Intellectual property protection using DataDNA™ technology with 90% smaller fingerprint for higher performance, scalability and accuracy	✓	Monitor only

MINIMUM SYSTEM REQUIREMENTS

Supported Microsoft Platforms

- Windows 2008
- Windows 2003
- Windows Vista
- Windows XP

Trend Micro DLP for Endpoint Software

- **CPU:** 300MHz Intel™ Pentium™ or equivalent
- **RAM:** 512MB
- **Storage:** 300MB

Trend Micro DLP Management Server Virtual Appliance

- **CPU:** Intel XEON or AMD Opteron dual-core or equivalent
- **Memory:** 2GB
- **Storage:** 30GB
- VMWare ESX and ESXi 3.5

Trend Micro DLP Management Server Hardware Appliance

- Purpose-built 1U rack-mountable appliance
- Security hardened
- **CPU:** Quad Core Xeon E5410 Processor 2x6MB Cache, 2.33GHz, 1333MHz FSB, PE1950,OEM (223-5027)
- **Memory:** 4GB 667MHz (4X1GB), Single Ranked Fully Buffered DIMMs
- **Storage:** 250GB 7.2K RPM Serial ATA 3Gbps 3.5-in HotPlug Hard Drive
- **NIC:** Dual Embedded Broadcom NetXtreme II 5708 Gigabit Ethernet NIC

WIDE COVERAGE OF FILE TYPES, APPLICATIONS, AND DEVICES

File Types Supported

- Recognises 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, CD/DVD, COM & LPT ports, removable disks, floppy, infrared and imaging devices, print screen, modems, PCMCIA



©2010 by Trend Micro, Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and DataDNA are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners. [DS01_DLP_091217GB]

www.trendmicro.com