

Prevent Information Leaks:

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

Benefits

- Protect Intellectual Property
- Prevent Identity Theft
- Comply with Privacy Regulations
- Discover Leakage Activity Quickly
- Extend Protection Beyond Headquarters

Competitive Advantages

- Most comprehensive protection, lowest risk
- Real-time enforcement, even offline
- Lowest false positives, highest accuracy
- Fast, scalable, unobtrusive

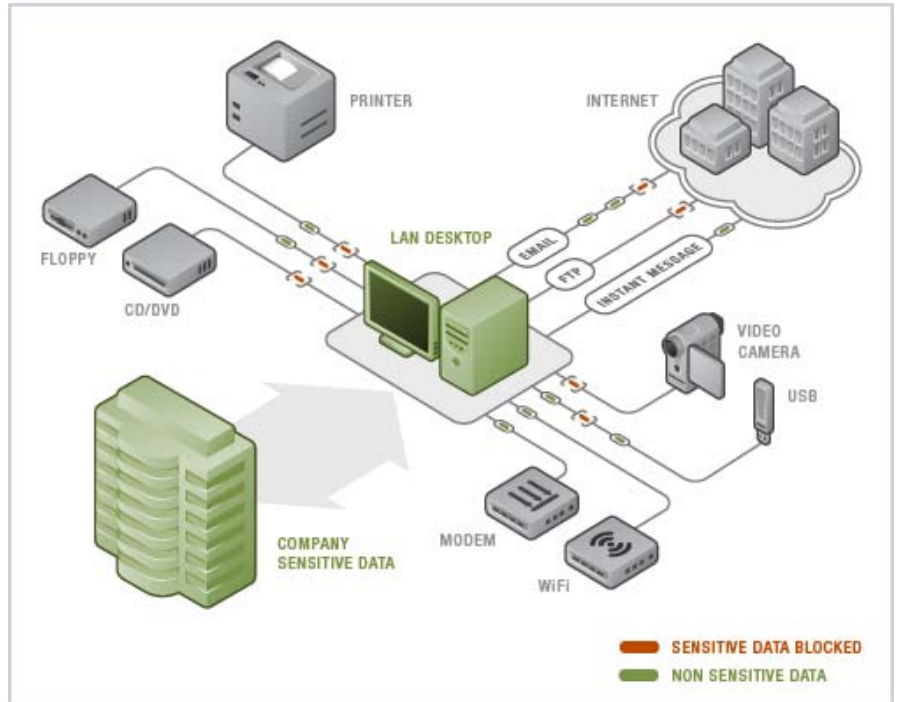
Information Leaks

Proprietary information and intellectual property assets are critical to the success of most leading businesses. Loss of this property can trigger litigation, loss of competitive advantage, brand damage and tough PR problems.

Existing security solutions (firewall, VPN, IDS/IPS, anti-virus, etc.) are designed to secure the perimeter of the organization, but they do little about the more serious threat which is from within. Fine-grained access control (ACLs) tried to address the information leak problem, but was never up to the task of preventing illegal copying or accidental leakage of critical data.

With the explosion of messaging systems, wireless networking and cheap removable I/O devices, the opportunities to leak critical enterprise data have multiplied. As a result, enterprises increasingly experience theft of critical company data - often by legitimately authorized network users.

Furthermore, compliance with business governance and privacy regulations (HIPAA, SB-1386, GLBA, EU DPD, Sarbanes-Oxley) require comprehensive company wide security policies to keep information confidential, protect customer privacy, and ensure tight management of corporate governance.



The LeakProof™ Solution

Provilla prevents information leakage of sensitive data with a unique approach that combines endpoint-based enforcement with highly accurate fingerprinting called DataDNA™. Provilla's Information Leak Prevention (ILP) solution is comprised of two components:

- **Anti-leak (A/L) Agent.** The A/L Agent is a non-intrusive, powerful monitoring and enforcement agent which detects and prevents information leaks at each endpoint. It communicates with the DataDNA Server to receive signature and policy updates and to escalate analysis of suspicious data to the Server. Because the A/L Agent resides at the endpoint and contains its own policy matching capability and signature snapshot, it provides the unique capability to:
 - ✓ Operate even when offline, when no connection to the server is available
 - ✓ Perform rapid detection of sensitive data using its own signature snapshot
 - ✓ Monitor local devices such as USB ports, applications such as Web mail, and network interfaces such as wireless and Bluetooth
- **DataDNA™ Server.** The DataDNA™ Server provides a central point for visibility, configuration of policies, and extraction of signatures from content sources. The server works with the A/L agents to identify and prevent information leakage. Key functions provided by the server include:
 - ✓ Identifies and fingerprints protected assets and sensitive content
 - ✓ Provides a management Dashboard to view real-time summaries
 - ✓ Provides a console for viewing and editing security policies
 - ✓ Monitors status and health of agent endpoints

Comprehensive Protection: Data, Ports, Channels, Networks

An effective Information Leak Prevention solution must monitor potential information leak at the point of use. This is the only way to prevent information leakage from within.

LeakProof™ is the only comprehensive and integrated data protection solution that covers both the network perimeter and endpoints – internal PCs and corporate laptops, even when they're disconnected. It can protect all information exits including network channels (such as HTTP Post,

SMTP, Web-based email, FTP, IM) and endpoint I/O (such as file transfers to USB drives or CD/DVD burners). It even prevents encryption of sensitive data, closing that “back door” to your network.

Real-time Enforcement and Complete Reporting

LeakProof provides flexible security enforcement policies including violation logging, alerting and real-time blocking. The system captures details for each violation such as user, endpoint computer, time, violation activity, file name, etc. LeakProof also provides reporting and alerting capabilities including: executive summaries, customized, ad-hoc and scheduled reports, and real time alerts. It also has strong data analysis including violation trend analysis, violation channel break down, and network protocol analysis.

Agent-based / Device Security Control

- Real-time monitoring and filtering online/offline
- Control of all I/O devices (USB, CD/DVD, Floppy, Bluetooth, IrDA, Imaging devices, COM & IPT Ports etc)
- Centralized agent status monitoring and management
- Detection and prevention of sensitive information encryption at endpoint
- Control all network protocols and messaging applications

Sensitive Information Detection/Matching

- Detection/matching of structured and unstructured data; partial matching of text files and exact matching of binary files; language independent match
- Data crawling to update signatures, automated or manual
- Keyword based content detection/matching
- Entity-based content detection/matching; entity validation

Endpoint Topology Discovery/Management

- Enterprise endpoint computer discovery
- Real-time map display of endpoint status
- Detailed display of endpoints status

Simple and Effective Security Policy

- Endpoint I/O device access (read/write) control
- Flexible security policies including logging, alert (client & server) and blocking, forensic data capturing
- Endpoint domain and group based security policies
- Content-based and metadata-based sensitive information control

Security Scanning

- Discovery of unauthorized sensitive information residing at endpoints
- Discovery of unauthorized I/O devices at endpoints

Content Security Report and Data Analysis

- Real-time Dashboard and security violation reports summarized by endpoints, users, etc.
- Trend analysis and violation channel breakdown
- Scheduled and ad-hoc reports of security violations
- Endpoint security risk assessment

System Administration

- Web-based system management interface
- Role-based administration and sensitive content access control
- Integration with LDAP and Active Directory for user and groups

File Types Supported

- Recognizes and processes 300+ file types
- Office files: Microsoft Word, Excel, Power-Point, 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, etc.

Network/Applications Controlled

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

Endpoint Devices Controlled

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

A/L Agent Supported Platforms

Windows 2000, Windows XP (SP1, SP2), Windows 2003 Server

DataDNA™ Server

- Purpose-built rack-mountable appliance
- Security hardened and service reduced Linux
- Gigabit NIC

Model	LeakProof™-100	LeakProof™-500
CPU	Single	Dual
Memory	2GB	4GB
Storage	160GB	300GB RAID Hot Swappable

