Protect Your Valuable Data with MyDLP

MY DLP
DATA SECURED BY COMODO

MyDLP from Comodo is the fastest, most scalable and feature-rich solution for Data Loss Prevention

COMODO
ENTERPRISE™

MyDLP Enterprise Edition

Data Leak Prevention

MyDLP is a feature-rich data leak prevention solution that allows businesses to discover, monitor and control the movement of con-fidential data across networks of any size.

Intellectual property is sent out of organizations on a daily basis. But did you know that well meaning employees and trusted insiders are often the biggest culprits?

Sound familiar?

If so, it's because almost every commonly used office application and hardware device is a potential source of data leakage. This presents organizations with an unenviable balancing act of trying to protect corporate data without affecting daily business workflows.

On the one hand, placing overly restrictive policies on email, removable devices, printers and laptops can hinder productivity and remove many of the advantages of today's modern office. On the other hand, too lax a policy can lead to the theft or loss of Important company data. This leads to financial and reputational loss, operational disruption, exposure of company secrets and non-compliance with data privacy laws.

The good news is that data loss is almost entirely preventable if organizations implement strong, intelligent polices to control its movement.

MyDLP - All in One Data Loss Prevention

MyDLP allows you quickly discover all sensitive data stored on your network then create policies to dynamically monitor, inspect and control its movement. Real time reports and event logs let you see who, how and where your sensitive data is being accessed.

Managed through a single, centralized console, MyDLP is a cost-effective solution which is easy to setup, does not require expensive new hardware and has little to no impact on network resources.

Full integration with Active Directory means businesses can import users and implement identity based security policies with immediate effect.

Key Benefits

- Detect and prevent any confidential data from exiting your organization network via mail and web channels.
- Monitor removable device usage in your organization and block or quarantine confidential files copied into these devices such as USB memory sticks or smart phones.
- Block or quarantine print jobs which contain confidential information.
- Discover confidential data on network storages, databases, workstations and laptops in your organization.

MYDLP DATA PROTECTION

- Build an inventory of sensitive data stored on company networks and deploy policies to control its movement and use
- Automatically implement re-strictions when sensitive infor-mation types are discovered in newly created documents and data sources
- Control which data can be sent to removable devices and printers connected to laptops and work-stations
- Enforce policy on laptops and other endpoints even when they are outside the network
- Implement identity based data policies via full integration with Active Directory
- Set rules to block emails with ex-ternal BCC addresses, automatically encrypt the usb devices and prevent screenshots when certain applications are running
- Real-time monitoring and reports provide a live feed of attempted policy infringements and areas of potential concern
- Fast, lightweight solution analyzes large files in seconds and can run on any server or virtual machine
- Fully compatible with Microsoft Exchange, SCCM and other major office suite
- Standalone, installable ISO which does not require licenses for any other 3rd party product

Powerful, Centralized Management

- Coordinate and manage an enterprise-wide, data protection strategy through a single, user friendly console
- Define multiple rules to cover a diverse range of data sources (AD Groups, Network Ranges etc.) and destinations (Web sites, Email domains, Print jobs etc.).
- Real-time dashboards and reporting allow you to you see what sensitive information has been prevented from leaving and where.
- Specify multiple tiers of administrator with different permission levels for configuration, execution and auditing.
- Allow executives and other non-technical staff to mark documents as confidential without alerting IT staff or breaking DLP policy

Complete DLP Solution

MyDLP is designed to provide your company with panoramic insight and control over data in motion, data at rest and data on endpoints.

It's single, centralized console allows administrators to quickly scan their network for confidential information then configure and deploy custom policies based on data type, location, destination, traffic type or user group. Real-time reports let you analyze data movement on your network and identify new areas for action.

As with all Comodo enterprise solutions, MyDLP is fully supported by a dedicated team of product experts and is available in a range of competitively priced and flexible licensing options.

Getting MyDLP

For more information and try out a demo, go to www.mydlp.com

If you have a business inquiry and would like to speak directly with a sales representative about Comodo products and services, please contact us at:

Tel: US +U.S. +1-888-256-2608
UK & Europe +44(0)-161-874-7070
International +1-703-637-9361
Email: **sales@mydlp.com**

About Comodo

Comodo is a leading provider of trust-based, Internet security products for organizations of every size. Comodo's offerings range from SSL certificates and antivirus software to endpoint security, mobile device management, and PCI compliance. Clients utilizing Comodo security products include Morgan Stanley, Comcast, Sears, Time Warner and Merck among others.

Comodo Security Solutions, Inc.
1255 Broad Street
Clifton, NJ 07013
United States
Tel: +1 (888) 256 2608

Comodo CA Limited
3rd Floor, 26 Office Village
Exchange Quay, Trafford Road
Salford, Manchester, M5 3EQ
United Kingdom
Tel: +44 (0) 161 874 7070

MyDLP Network Server

System Minimum Requirements:

- Dual or quad core Intel Xeon processors
- 8 GB or more RAM
- 256 GB or more Hard drive
- NIC 1000/100,
- Or equivalent virtual resources

MyDLP Endpoint Agent

System Minimum Requirements:

- Operating Systems:Windows XP / 7 / 8 / 8.1 / 10 Windows Server 2003 / 2008 (64 bit and 32 bit supported)
- 1GB RAM
- 400 MB free hard drive space

Inspection Channels

- Web (HTTP, HTTPS, FTP, SFTP)
- Email (POP, SMTP)
- Printers (local printers, print servers)
- Removable devices (USB memory sticks, smart phones,etc.)
- Discovery on data storages and endpoints

Integration Highlights

- Microsoft Active Directory: Ena-bles you to use domain users and groups in policies.
- Major Database Servers: Ena-bles you to use database con-tent in DLP policies.
- ICAP proxy or content filtering solution and with custom appli-cations via the REST API
- Syslog, HP ArcSight and other log collection, correlation systems.