MyDLP Enterprise Edition

Data Leak Prevention

MyDLP Enterprise Edition is a feature-rich, scalable and affordable all-in-one data leakage prevention solution with blazing fast performance.

Almost all indispensable office applications and devices are potential data leakage sources. Organizations struggle to achieve security without hindering performance. On one side restrictive policies on web, e-mail, removable memory devices, smart-phones, printers , laptops removes almost all advantages of today's unified office environment. On the other side, compliance requirements, unmitigated risks, real-life horror stories occurring everyday pressures IT management.

MyDLP allows you to monitor, inspect and prevent all outgoing confidential data without the hassle. With painless deployment and configuration, easy to use policy interface and great performance IT administrators and security officers are able to combat data leakage.

All-in-One DLP Solution

*You don't need to buy several modules or products to **Monitor, Discover and Prevent data leakage** on your company network and endpoints.*

MyDLP proposed as an All-in-One solution with a single subscription license. You will never need to acquire more licenses to use any features, including the ones will be available in future releases.

One Month Free Trial & Easy Deployment

Contrary to conventional DLP solutions, MyDLP deployed and start to protect you in a few hours. You can define your basic policy in minutes and tailor it according to needs without any hassle. Using MyDLP Virtual Machine images you can start to try MyDLP without waiting and with literally zero investment.

Common Use Cases

» Block or quarantine outgoing confidential data from your organization network via mail and web. Archive suspicious files.

» 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.

Centralized Management

» Manage all MyDLP components with user friendly interface.

» Define a single rule for all or define different rules for different sources (AD Group, TCP Network Rage etc.) and

MyDLP Network Protection

- Enforces DLP policy on all organizational network.
- Almost linearly scaling performance.
- Freedom to run on a virtual machine or on any hardware meeting minimum requirements.
- Analyze large files in few seconds.
- Seamlessly integrate with any ICAP supporting proxy or content filtering solution.
- Integrate with Microsoft
- Exchange or any other mail
- Remote/agent-less data discovery.
- Ability to monitor / block emails with external BCC address
- Integrates with custom applications with REST API.

MyDLP Endpoint Protection

- Control removable devices and printers connected to laptops and workstations.
- Easy deployment with available deployment infrastructure such as Microsoft Active Directory or SCCM
- Off-line protection outside the organization network.
- Endpoint data discovery.
- Supports all printer drivers without exception.
- Minimal resource usage, does not bothers the user with unnecessary messages and popup.
- Domain encryption for removable storage devices.

different destinations (Web sites, Email domains etc.).

» Administer DLP policy effecting thousands of agents and all network traffic with a few clicks.

» Monitor all events in logs, in your dashboard and collect reports.

» Make Google-like full text search in quarantined or archived suspicious files, see related event details and users.

» Restrict different management roles for configuration and audit functions for users and groups with Microsoft Active Directory integration.

» Allow executives and other non- technical staff with classifier management role to mark documents as confidential without alerting IT staff or breaking DLP policy easily.

Complete DLP Solution

» MyDLP is designed as a complete solution for data leakage problems in corporate environments from the start. It provides state of the art abilities to help you battle the information leakage risks.

» MyDLP support service is ready to help you to mitigate risks and to resolve emergencies.

Find Out More

For more information visit **http://www.mydlp.com**

To speak with a specialist contact s**ales@mydlp.com**

Technical Specifications

MyDLP Network Server System Minimum Requirements:

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

MyDLP Endpoint Agent Minimum Requirements:

- Windows XP, Windows 7, Windows 8, Windows 10, Windows Server 2003, Window Server 2008 operating systems (64 bit /32 bit)
- 1GB RAM
- Minimal 200 MB free hard drive space

Inspection Channels

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

Integration Capabilities

- Microsoft Active Directory: Enables you to use domain users and groups in policies.
- Database Servers: Enables you to use database content in DLP policies.
- Syslog, HP ArcSight and other log collection, correlation systems.
- and more...

Comodo Group Inc.
1255 Broad Street
Clifton, NJ 07013
United States
+1 (888) 256 2608

Comodo Security Solutions Limited
159 Praed street
W2 1RL London, United Kingdom
Tel: +44 207 402 7278
Email: emeasales@comodo.com