PARAGON SOFTWARE

Data Loss Prevention Tools

Azure

A cloud-based for protecting documents and emails by applying labels.

Functionality:
• Data usage control
• Data flows analysis
• Risky behaviors detection
• Track access to documents and files

G Suite & Google Drive

G suit allows admins to set rules and permissions (including access) for working with company documentation on Google Drive.

Functionality:
• Detect sensitive content (via regular expressions, word lists, predefined detectors or more granular detection thresholds)
• Prevents users from sharing sensitive content

AWS

Fully managed data security and data privacy service via Amazon Macie AWS application. Automation of sensitive data identification and protection.

Functionality:
• Inventory
• Identification and alerting of any sensitive data in the selected list of Amazon S3 buckets
• Third-party apps integration
• A lot of sensitive data types preconfigured
• An option to create new sensitive data types

McAfee DLP suite

A sophisticated application that is created for the purposes of data loss prevention only.

Functionality:
• Identification of sensitive data or user activity
• Data classification
• Encryption, quarantine, redirection, and blocking of sensitive data transmissions
• Creation incidents of violations
• Automated reporting

Symantec Data Loss Prevention 15.7

A sophisticated application that is created for the purposes of data loss prevention only.

Functionality:
• Discover sensitive data in cloud storage repos, on file, web servers, in databases, and on endpoints
• Protect sensitive data through quarantine
• Monitor the use of sensitive data on endpoints
• Prevent transmission of sensitive data to unauthorized parties
• Enforce data security and encryption policies

FortiGate

A DLP solution from Fortinet. The main peculiarity is the protection of data on the internal company's network level.

Functionality:
• Preventing sensitive data from leaving the internal company's network
• Preventing unwanted data from entering the internal company's network
• Individual filters creation (type and size o files, regular expressions, advanced rules, compound rules)
• Applying digital watermarks to files

Forcepoint

A DLP solution, addressing the human-centric risk associated with data leakage and loss of sensitive data by controlling all environments where people work and data resides.

Functionality:
• Applying user-risk scoring to data
• A pre-packaged set of global regulations (350+ policies for 80+ countries) ready for implementation
• Optical Character Recognition (OCR)
• Identification for Personally Identifiable Information (PII)
• Custom encryption identification
• Cumulative analysis for drip DLP detection
• Integration with Microsoft Azure Information Protection

Sophos

The DLP functionality is included in the Sophos Endpoint and Email Appliance products.

Functionality:
• A set of sensitive data type definitions, created by SophosLabs
• An option to customize the data definitions
• Customizable DLP rule definitions (the rules, criteria, triggers and actions)
• DLP SDK is provided

Watchguard

Is a comprehensive DLP-focused solution, biased to keeping sensitive data private, preventing data breaches, and enforcing compliance.

Functionality:
• Library of 200+ rules for 18 countries (incl. PCI DSS & HIPAA)
• Automatic rule sets updates
• Integration with WatchGuard Dimension inspection tool
• Protection of sensitive data transmitted via email, web, and FTP
• Data parser, supporting 30+ files types
• Decompression of archived file

For state-of-the-art DLP guide visit
Data Loss Prevention Hub