

TKMT RISK MANAGEMENT

(MODULE: DATA LOSS PREVENTION)

Protect your organization from confidential information leaks by controlling data at rest and in motion. Monitor all channels of sensitive data transfer, analyze information flows, detect and prevent violations, and deliver actionable reports to responsible stakeholders.

69,19%

Local Content Component

HOW TKMT RISK MANAGEMENT SUPPORT YOUR BUSINESS

- Safeguards confidential information during storage, usage, and transfer.
- Facilitates inventory for software and hardware assets.
- Encrypts sensitive data to prevent unauthorized use outside the organization.
- Detects suspicious activities such as copying data to USB drives or deleting large volumes of files.

ALWAYS KEEP CRITICAL DATA IN SIGHT

TKMT Risk Management Module: Data Loss Prevention uses Data-Centric Audit & Protection (DCAP) to automatically audit storage, detect unauthorized access, and track changes to sensitive files.

Key Functions:

1. Data Classification

Identify files containing sensitive information (e.g., personal data, secrets information data, credit card numbers, bank number) and assign specific categories.

2. Document Archiving

Create shadow copies of critical files stored on PCs, servers, or network folders, and maintaining revision history for incident investigation and recovery of lost information

3. Access Rights Audit

Automatically monitoring who has access to sensitive files and privileged accounts.

4. User Activity Monitoring

Audit user operations to mitigate risks by tracking file changes such as creation, editing, movement, or deletion

The average volume of data stored by organizations is substantial, and every data contains sensitive information such as personal and financial records, specifications, images, and more. Each category of sensitive data must be stored, processed, and distributed in accordance with appropriate policies and controls.

DATA ANALYSIS AND VISUALIZATION

TKMT Risk Management DLP provides file system scans clear visualization based on defined rules:

1. Directories are mapped with understandable access rights.
2. File activities (creation, modification) are logged for easier monitoring.
3. Files are labeled by type (e.g., confidential agreements, personal data, financial reports) for efficient management.
4. The number of critical files is calculated by disk or folder, offering insights into stored sensitive information.

Contacts:

www.tkm-teknologi.id

Email : support@tkm-teknologi.com

Phone: +62 811-1552-270



TKMT RISK MANAGEMENT

(MODULE: DATA LOSS PREVENTION)

TECHNICAL SPECIFICATIONS

Application Feature	Description
Automatic Classification	Data Classification based on file attributes such as content, name, and size.
Manual Classification	Allows users to create manual files classification.
Data Backup	Sensitive files secure backup .
Version Control	Stores up to 99 versions of file changes, before and after modifications.
File Monitoring	Records file changes, including renaming or deletion.
Keylogger	Records keyboard activity, including typed passwords.
Camera Control	Captures or records camera activity when risky sites are accessed or under security policy.
Screen Control	Automaticly screenshots or records user activity under security policies.
Microphone Control	Records audio automatically when risky sites are accessed.
Program Control	Monitoring program usage and blocking unauthorized applications.
Cloud Control	Monitoring and preventing data leaks via cloud services (Google Drive, OneDrive, etc.).
Print Control	Preventing sensitive data leaks from physical document printing.
HTTP/S Control	Monitoring and restricts risky web activity to prevent sensitive data transfer.
Email Control	Monitoring email activity to prevent leaks via Gmail, Outlook, etc.
Instant Messenger Control	Instant messaging platforms monitoring (WhatsApp, Telegram, etc.) to prevent leaks.
Device Control	Monitors and encrypts data transferred via external devices (USB, HDD, mobile).
FTP Control	Records all file transfers via FTP protocol.
OCR (Optical Character Recognition)	Detects and prevents sensitive data leaks via scanned documents or images.
Security Alerts	Provides warnings when users violate security policies.
Audit Detailed	Comprehensive audit for hardware installation and software.
Reporting	Generates reports for security violations, KPIs, and employee device usage efficiency.

Contacts:

www.tkm-teknologi.id

Email : support@tkm-teknologi.com

Phone: +62 811-1552-270

