AVEPOINT COMPLIANCE GUARDIAN
FOR DATA LOSS PROTECTION (DLP)

PROTECTING YOUR CONTENT EVERY STEP OF THE WAY

KEY BENEFITS

| DATA IDENTIFICATION	DATA ANALYSIS	FILE ANALYSIS	DATA AT REST	DATA LEAKAGE PREVENTION
Set the right level of protection for the right data with context-aware reporting, notification, and classification – preventing regulatory violations within your data. Real-time scans promptly and accurately identify regulated and sensitive data to help you mitigate harmful leaks before they become costly fines.	Define the scope of data and a schedule for data analysis, and get a full assessment to pinpoint potential violations in privacy, operational security, accessibility, and site quality policies. With detailed reporting and flexible corrective options, prioritize risks to address your biggest threats first to minimize your vulnerability.	Analyze and define unstructured data across multiple platforms to prioritize and declutter your data. Identify and eliminate redundant, obsolete, and trivial (ROT) data to improve performance and reduce risk. Determine service level agreements (SLAs) for backing up critical documents and establish rules for record retention.	Discover dark data wherever it lives in your current repositories with Compliance Guardian's extensible APIs. Scan across SharePoint, Exchange, file shares, databases, websites, cloud platforms – including Office 365, Exchange Online, and Box, Dropbox and Slack – as well as social platforms including Skype for Business and Yammer.	Centrally monitor the status of any incident as well as its associated risk levels to ensure violations are dealt with based on criticality and time of occurrence. With trend reports and detailed historical analysis, track and manage risk level throughout the entire lifecycle of your data.

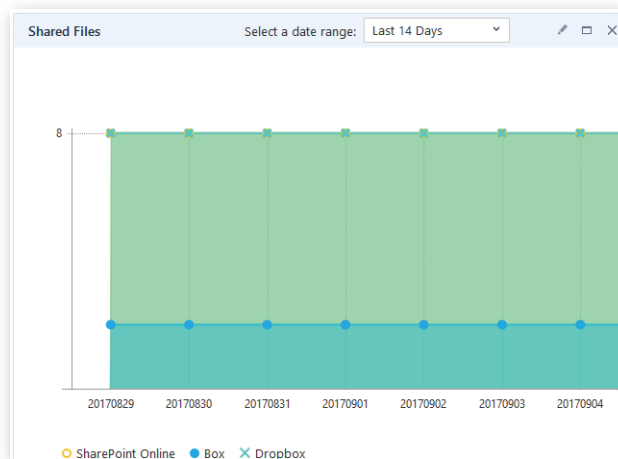## PROACTIVELY MONITOR AND SECURE YOUR DATA

Implement a plan of action that empowers a collaborative working environment for end users while protecting your most valuable assets. By integrating content level scans with automated tagging, classification, securing of potentially sensitive documents, permissions, and policy enforcement. With location-based mobile access control, you can secure your information while allowing users to work the way they naturally do.

TECHNICAL FEATURES

- Real-time and scheduled scans identify and analyze files and their content so you can map out data upon your queries with multiple filter conditions including file type, age, size, ownership, location, and sensitivity level.

- Classify data with user-assisted or automated tagging via a Metadata Classification Engine

- Identify privacy or information security violations in files and assign by role and ownership so issues can be resolved by the right people.

- Security-trimmed and heat-mapped reports prioritize by criticality and concentration.

- Report on access levels to ensure the right people are able to see, edit, download, and share specific information and file types.

- File history reports show all access and modification to pinpoint leaks.
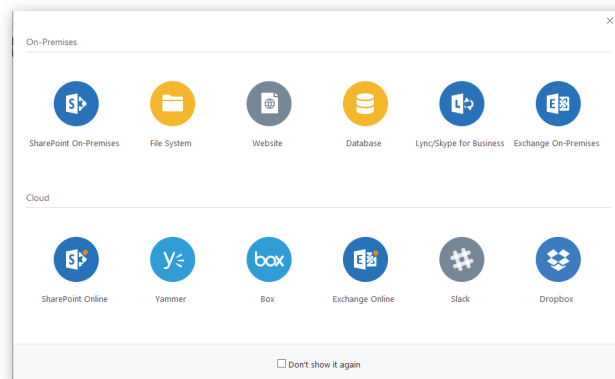
Supported Data Sources

Shared Files Trend