Grayteq

Report and Audit

Complete your data loss prevention with insight

Every security solutions - even the best ones - are one-armed giants without proper reporting and audit features. Hundreds of thousands to multi-millions of activity logs are impossible to use and analyze efficiently without highly flexible, easy-to-setup reporting solutions with prebuilt report and audit templates to make log processing transparent, automated, schedule-able, fast and accurate. Considering that in case of a security investigation, reports made out of logs are the only available to prove one's innocence or guilt, reliability is definitely with one of the highest importance of all data loss prevention features. While DLP logs may prove the guilt of the perpetrator, it helps to separate malicious intentions from accidental actions, the harmful perpetrator from the large amount of loyal and truthful users without even letting the shadow of suspicion lay on them. And this is important!

Freely set activity reports

Finding a specific event, access, or action to a file by a given user on a device or devices or even-network-wise out of usually millions of log lines is impossible without sorting it somehow either manually or automatically. Grayteq DLP's reporting engine built in Security Orchestrator is powerful enough to make manual sorting of even the ever changing real-rime logs or the chain of as-long-as-you-please-in-time log archives for a specifically required result. Simply drag your angle of sorting interest on the SO over the logs and sorting immediately happens for as deep as your wish.

Automate your reports

Automated and scheduled setups for the provision of recurring and same angled reports is also part of the Grayteq DLP Report & Audit feature that makes it possible to read the same content, timely updated and automatically created, board-ready reports. And for the head of IT security, there is no more calming than reading professionally gathered reports every morning while drinking the day-starting coffee that ensures if no unhandled or worth to mention security breach has occurred since the last automated report.

Key Advantages

Evidential and Safe

- Create evidential reports using any viewpoints that pinpoint malicious activities and protect the innocent! Saving loyal and rule-abiding users from being accused is as important and finding the harmful ones.

Accurate and Reliable

- "Trust with your paycheck" on the report content. It will contain everything as it happened. In making reports, it's vital to make sure that there is no possibility to forge evidence about an action that did not happened, or delete about an action that did happen.

Automated and easy to use

- Automated, scheduled and easy to use, analyze, explain and understand. These are the properties of a well-made report.

Manual vs Automatic

- Setup various automated reports and schedule to execute recurrently, or "click-off" a manual one using a prebuilt report template or a live one with modifications is also a slight walk in the park.

Grayteq DLP Features

▶ DLP Monitor	⚙ Rights Management	🔒 Data Quarantine	🌐 App Management
Endpoint Protection	Encryption for DLP	Intrusion Prevention	**Report & Audit**

Grayteq

File Audit

Grayteq DLP File Audit feature is a one-of-a-kind set of features that enables organization's IT security professionals commence file audits from various angles, time-schedules, required results. By making purpose-built reports from either real-time logs or even from archives are essentials and by Grayteq DLP File Audit's preset reporting schemes, it's a single-click solution.

File Audit features

- **Standard File Audit about a file**
  Select a log entry and click Standard File Audit and Grayteq DLP automatically creates a tree-structured overview about what has happened to the file named in the log since the moment of the log till the current moment.

- **Standard File Audit about a file from its creation**
  Select a log entry and click Standard File Audit from Creation and Grayteq DLP automatically creates a tree-structured overview about what has happened to the file named in the log since the moment of it'd creation till the current moment.

- **Seek file origin**
  You can find the very origin of the selected file back in time as long as it appears Grayteq logs.

- **Seek file origin and generate Standard Audit Report**
  Find the very first existence of the selected file in Grayteq logs and draw its whole lifecycle in a report.

- **File existence history about a file**
  Find all storage location in your network, where the specific file exists.
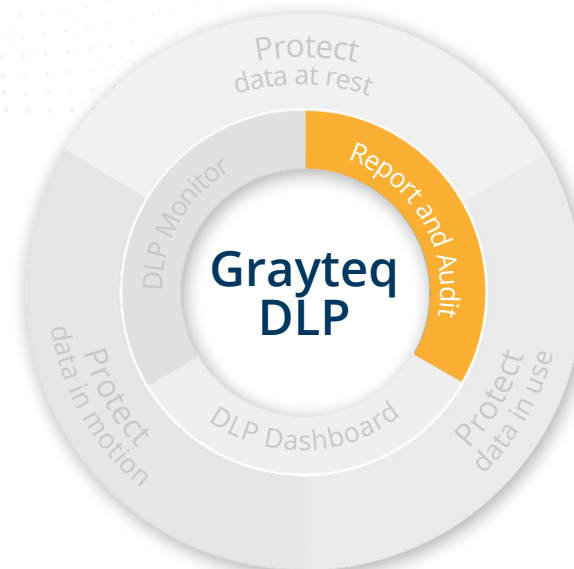
Next Step

For more information, visit www.grayteq.com/reportandaudit or contact us on www.grayteq.com/contact

Storage Audit

Besides of file audits, making reports of your corporate storages, where your sensitive data is brought by, who put these data to removable medias and moved from one location, from one device, from one subsystem to an other is also a must to properly follow-up with your data. Grayteq DLP's name, mount-point, serial and hardware ID based storage identification system allows you to create these storage usage audits in seconds, even at the absence of the specific device.

Storage Audit features

- **Storage Connectivity Report**
  Get all available log information about when and in which devices the specific storage device was connected. This report shows the time of connection and removal, the host name where the storage device was connected to and its current connection state (eg. If the storage device is currently connected to any Grayteq protected hosts)

- **File Operation Report**
  File Operation Report shows what file operations occurred during the selected connection session in details.

Protect data at rest
DLP Monitor
Report and Audit
Grayteq DLP
Protect data in motion
DLP Dashboard
Protect data in use

Supported systems

Grayteq DLP supports both 32- and 64-bit Microsoft Windows Desktop and Server operating system.

Desktop operating systems

- Windows 7 SP1 *
- Windows 8
- Windows 8.1
- Windows 10

Server operating systems

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

* All component of Grayteq DLP operate on Windows 7 SP1, but officially not supported and certain features may have limitations.

Get started

Grayteq data protection expert team will work with you to understand your unique data security requirements, help you define priorities and share industry best practices.

Email your questions or point of interest with contact details to support@grayteq.com

Grayteq

About us

Grayteq was born from a firm commitment to provide superior data security products to companies and people all over the world. Since its inception, our company has passed down and expanded on its traditional strengths as an IT security software manufacturing company. Grayteq's approach to data loss prevention massively differs from any other data loss prevention manufacturers' approach in numerous aspects. Our slogan well represents our way of thinking about data loss and applicable prevention measures to stop it.

Contact us

grayteq.com/contact

Grayteq on Web

Home
www.grayteq.com

DLP
www.grayteq.com/dlp

Classifier
www.grayteq.com/classifier

Encryption for DLP
www.grayteq.com/encryptions

DLP Dashboard
www.grayteq.com/dashboard

Prices
www.grayteq.com/prices

Services
www.grayteq.com/services

Think different
Do different

Your Grayteq Partner: