Grayteq

Grayteq DLP

Comprehensive and strong. The protection your corporate data needs.

Loss or leakage of valuable corporate information that resides on PCs, laptops, shared file servers and in cloud storage may be putting your organization into grave danger from various aspects. The task of their protection is especially difficult because sensitive information isn't always properly identified, classified or stored. The more employees work with the information, the greater the likelihood that someone will deliberately or intentionally leak sensitive data to an unauthorized recipient. There are several path available for information to leave the corporate perimeter — email, file share, web, instant messaging (IM) or FTP. Enforcing the right policies real-time is essential to ensuring data security, regulatory compliance and intellectual property protection Grayteq DLP helps you locate, classify and protect your sensitive corporate data, monitor how it is being used and protect it against loss or leakage.

Key Advantages

Identification of data leakage risks

- Monitor the use of information stored on premise or in the cloud.
- Identify where sensitive data is stored and who the content owner is.
- Search and view all activity data from an intuitive interface.

Policies and customized reports

- Use prebuilt compliance, corporate governance and intellectual property policies.
- Create ad-hoc, manual and automated reports from any aspect.

Alerts

- Create automatic alerts about policy violation attempts and notify security administrators in real-time.

Deliver data traffic enforcement

- By Data Quarantine feature, it's easy to determine to and from which path data can move, who can move it, by which application, to whom and where it must be stored afterwards.

Grayteq

Policy enforcement for data at rest

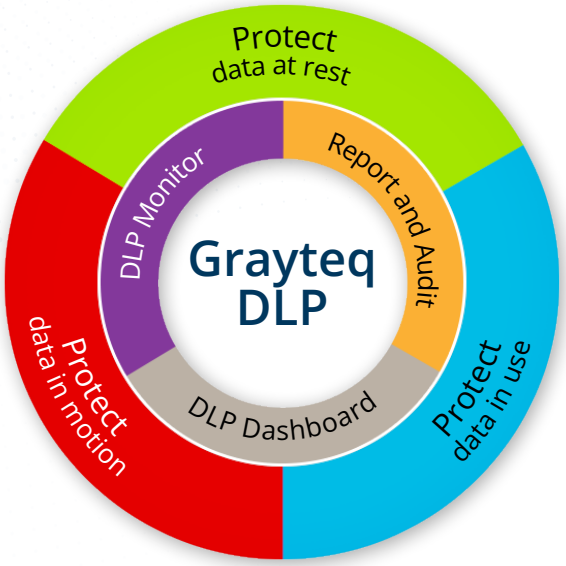
Stationery data protection features of Grayteq DLP, Access Rights Management and Encryption for DLP are specifically designed to provide efficient and easy-to-manage protection for your corporate data at rest wherever its resided. In addition to constantly monitoring all data access to detect policy violations, Grayteq DLP automatically overrule Microsoft Active Directory (AD) provided access rights to data if those might breach Grayteq access rights policies. This operating methodology empowers your organization to protect all kinds of sensitive data—from common, fixed-format data to complex, highly variable intellectual property, wherever its stored. Combining Encryption for DLP feature with Grayteq Classifier's data classification capabilities, every occurrence of the specific data can be automatically protected.

Policy enforcement for data in use

Grayteq DLP continuously monitor every activity that access data within the protected system and enforce policies on every interaction that might put data at the risk of being leaked or lost automatically. Data Quarantine and Application Management allow you to setup a proper protective fence surrounding your data while in use, blocking any action taken by any authorized or unauthorized user or application that might result the improper usage or leakage of the specific data. Alerts - after the blocking of the security breaching attempt - automatically and real-time notify the security administrators about the incident, providing them with all details that necessary for the decision of the required counter-actions. Grayteq DLP's endpoint agent can inform the user that the intended action was against the upholding data security policies and in certain cases - depending on the security classification of the user - offer justification for the user. By using this special right, the user may initiate a temporary policy overruling sequence that lets the previous rejected action to complete, but notifying the user that the fact of the user overrule and the action taken afterwards are sole responsibilities of the user and are logged as intentional policy violating actions.

Policy enforcement for data in motion

Enforcement of Security Policies for Data in Motion across each department of every company, individuals share data using multiple applications and a variety of protocols is the cornerstone of every data protection system. Save data from being deliberately or intentionally leaked requires proactive protection of valuable information from leaving the network or the specific device. Grayteq DLP automatically enforces policies for information intended to leave the network in any traditional ways while Grayteq DLP for Outlook is integrated with Microsoft Outlook, using simple mail transfer protocol (SMTP) or ICAP-compliant web proxies to control the outbound email delivery of protected information. Upon encountering a policy violation, Grayteq DLP automatically denies the specific action, log all details of the intended breaching attempt and either create an automatic report for the security personnel or alerts them in real-time. By these counter-actions you can ensure compliance with regulations governing the privacy of sensitive information and reduce the risk of security threats.



Trivia

Prevalence of Data Loss
Compromized customer records top the list of security incidents, and employees are the number one source of security incidents.

Do You Know Where Your Data Is?

According to a third party data residency report, only 47% of organizations are completely confident that they know where their data is physically located—and only 44% have a thorough understanding of the GDPR regulation and how it impacts them.

Get started

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

Email your questions or point of interest with contact details to

support@grayteq.com

Grayteq

Protection for data at rest

Access Rights Management

Grayteq DLP's Data Quarantine provides unprecedented protection for your stored data by combining the enforcement of storing policies for your valuable data with the protection of Access Rights Management. Data Quarantine allows you to setup complex policies to determine and control who can work with the quarantined data, by what application, where are the allowed outbound paths of the quarantine, if the data can be transferred in email within the organization or outside of it. The possibility of stacking quarantines with different protection settings enables data handling workflow setups by dynamically protecting data at every step of the way within the quarantine and with Grayteq Encryption for DLP, outside of it.

Encryption for DLP

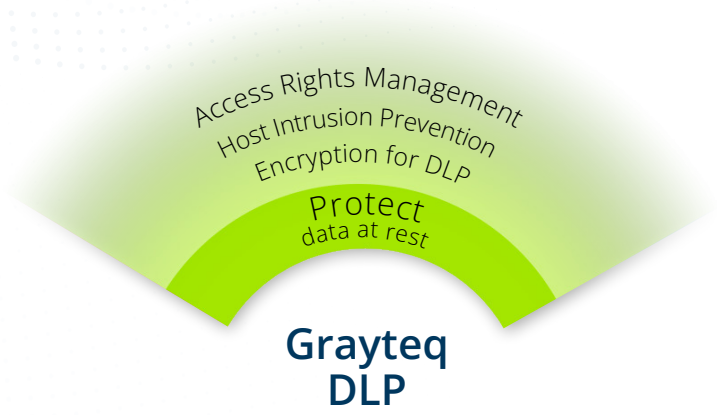
Removable Media, File and Folder, and Cloud Share Encryption ensure that specific files and folders are always encrypted, regardless of where data is edited, copied or saved. All encryptions and decryptions are fully user transparent and automatically enforced on-the-fly, based on the data using user's credentials. You can create and enforce central policies based on users and user groups for specific files and folders without any user interaction. Grayteq Encryption for DLP empowers your data protection system with various, centrally managed, industry standard encryption methodologies that efficiently save your corporate data against being decrypted by any unauthorized party, even if the data or the whole storage is stolen or lost. Read more about Encryption for DLP

Host Intrusion Prevention

With Grayteq DLP's patent protected, unique Host Intrusion Prevention (HIP) technology, you can setup unlimited separated and overlapping protection zones within your network, that provides you with software-based separation between different network segments, departments, groups of devices and more. This technology initiates a sequence of question-response communication between the "caller" device and the "called" one and enables seamless and user-transparent connection between the devices if both meet at least one of the upholding HIP policies. All incoming connection attempts are logged and in case of a security breach, a real-time alert is triggered.

Classifier, Classifier for Office

Data protection goes way more reliable when appended with a proper classification. Grayteq Classifier is a best-of-breed file classification engine for Grayteq DLP that enables the users to manually classify file based on their data content and automatically apply security policies related to the specific type of content. Classifier also provides users with storage location-based automatic file classification that auto-classifies any file that is moved, copied or saved into a specific storage area, a folder or even a partition. Glassifier's user module automatically adds a colored sign to the classified file's icon with its classification color that visually notifies the user about the classification level of the file without opening the file itself. Gratyeq Classifier's addin module Classifier for Microsoft Office embeds into the members of Microsoft Office, providing a ribbon for the users to make classification a single-click event. Optionally, file classification can be made mandatory for newly created file, just as for the old - unclassified- ones when opened. Mandatory classification may force the user to classifiy the file before closing or saving it. Read more about Grayteq Classifier



Key Advantages

Real-time

- Act in real time to fix vulnerabilities and stop threats in their tracks.

Efficient

- Efficiency is important in both policy enforcement and seamless embedment into the infrastructure.

Comprehensive

- Anything less than a full-cover is not enough. Cover the whole and you are safe.

Fast

- Get fast, software enhanced protection against today's toughest and stealthiest threats.

Unified

- Unify management across all your endpoints, from virtual machines and servers to PCs and laptops.

Protection for data in use

Application Management

There are gazillions of applications out there. Some of them are useful tools, some of them are simply irrelevant from security perspective and some of them are designed to cause harm on your data. Games, unauthorized browsers, instant messengers, social media tools and other unwelcome applications may impact your business with their drain on employee productivity. Scan your network for all applications and executables, then classify them into trusted and blocked lists and set automatically enforceable policy for those that are unknown. All is set in an instant and application management and the threat unknown or harmful applications may pose on your infrastructure are not issues anymore.

Data Quarantine

Grayteq DLP's Data Quarantine provides unprecedented protection for your stored data by combining the enforcement of storing policies for your valuable data with the protection of Access Rights Management. Data Quarantine allows you to setup complex policies to determine and control who can work with the quarantined data, by what application, where are the allowed outbound paths of the quarantine, if the data can be transferred in email within the organization or outside of it. The possibility of stacking quarantines with different protection settings enables data handling workflow setups by dynamically protecting data at every step of the way within the quarantine and by using Grayteq Encryption for DLP, outside of it.

Key Advantages

Layered protection

- Strengthen your security with various layers of protection over your data in use

Flexibility

- Get the utmost flexibility in expanding your protection as your system and needs change.

Keep the flow

- Information-flow across the organization is one of the most important for operation. The internal data flow is uninterfered, while the outbound is strictly controlled.

Focus on business

- Elevate your productivity with central management console and the lowest impact to system resources in the industry.

Grayteq

Protection for data in motion

Endpoint Protection

Defend all your endpoint devices, from traditional PCs and laptops to in-house and in the cloud storage servers with Grayteq DLP's single console managed Endpoint Protection. As integrated part of Grayteq DLP, Endpoint Protection is fully manageable from the Grayteq Security Orchestrator, enabling 24/7 monitored and protected endpoints for all of your Windows-based devices. You can control data flow thru any and every devices and protocols in real-time. Single-console management eases the day-to-day burden on your IT security staff and empowers them to act fast when threats strike. Get proactive about protecting your data by using Grayteq Endpoint Protection as another layers of your data security infrastructure.

Encrypted Data Transmission

While Grayteq Encryption for DLP is originally designed to provide strong encryption for data at rest, Encrypted Data Transmission (EDT) feature protects your corporate data on the road, providing industry standard, centrally managed, strong encryption for the period of travel and ensures that your data can only be decrypted on a Grayteq protected device wherein pre-distributed policies protect your data after decryption is done. EDT's encryption and decryption authorization is user based and embedded into the Windows Explorer context (right-click) menu for easy accessibility for the users
Read more about Encryption for DLP

Key Advantages

Safe endpoints

- No matter which endpoints are in use, uninerfered protection for all of them streghtens your data safety.
  Safe endpoint is a must!

Share protection

- Secure confidential data on all devices and removable media while you share files securely.
  Share protection is a must!

Encryption

- No data is safe while being transferred without proper, industry standard and strong encryption.
  Encryption is a must!

Grayteq DLP
IS A MUST

Grayteq

DLP Monitor

Real-time monitor, track, log and alert

No matter which business your company is, you need a proper real-time monitoring, tracking, logging and alert to keep posted what happens to your sensitive information over any application, any protocol, any endpoint, and in any form. And it has to be done with a highest accuracy with no false positive results. With Grayteq DLP Monitor, you can real-time monitor, track and log every interactions to your data across your entire network to find what and how information travels between users inside the organization and on which path it leaves the perimeter. With Grayteq DLP's real-time Alert capabilities you easily can setup action-triggered alerts for any and every circumstances that strengthen your data loss prevention infrastructure by automatically notifying your IT security personnel about the breaching attempt with all necessary details that help to make counter-actions with the fastest response time. A high-performance, purpose-built, Windows kernel embedding monitoring agent Grayteq DLP Monitor uncovers threats to your data and stop them to protect your organization against data loss. In addition, through its enhanced user notification system, Grayteq DLP Monitor educates your users on data loss violations to change behaviors with no effort.

Forensic and Rule Tuning Capability

Grayteq DLP's unique logging technology and its built-in Test Mode for policies - that let's you test your security settings on your live system without risking any wrong policy-caused breakdown, enables you to leverage historical data to implement a much faster and way more efficient protection by minimising the possibility of business disruption. This makes it easy to tailor-made your DLP policies on your all-time-changing business needs. DLP Monitor's built-in drill-down type forensic technology enables you to dig down to the deepest depth of your business workflows and find out how could they've been made more secure without significantly changing users' everyday working habits.

Easy Deployment

You may not have security experts in every office— that's why we keep Grayteq DLP's whole agent and policy deployment as simple as can. System and security management is centralized and easy with Grayteq DLP SO software—a single pane of glass where you can view security and manage policies from and for all supported devices.

Strong and Effective Performance

Grayteq DLP's lowest-in-the-industry hardware requirements and power consumption help you to improve your IT operational efficiency. Policy enforcement and logging is optimized for performance.

Centralized Management and Advanced Reporting

Security Orchestrator software is the heart and mind of the whole Grayteq security environment. Use the centralized SO console to implement and enforce mandatory, company-wide security policies that control how data is accessed, used by the users and how it's encrypted, monitored and protected from loss. Centrally define, deploy, manage and update security policies that monitor, manage, allow or block, report and alert all authorized and unauthorized access to your sensitive and valuable corporate data.

Grayteq DLP Dashboard

For heads of IT, IT security or even for the highest boards, there is no need for all security operating details to make strategic decisions. Grayteq DLP Dashboard is made to create management level insights, reports, analytics about the current security status of your whole corporate network and help decision makers to clearly see the present and figure out the future from the aspect of IT security.
Read more about Grayteq DLP Dashboard

Compatibility

Operating System

- Grayteq DLP supports every 32- and 64-bit Microsoft Windows Desktop and Server operating system up from Windows 8 and Windows Server 2012 R2.

Database & SYSLOG

- Grayteq DLP is shipped with its own built-in database engine, so you don't have to buy any third-party database licenses solution to enjoy the benefits of Grayteq DLP, however if you use either Oracle Database Server (up to Oracle 11G R2) or Microsoft SQL Server (up to SQL Server 2019) or PostgreSQL (in ANSI or Unicode mode) database, you can use them as Grayteq DLP databases also.
- You can use your existing SYSLOG system on industry-standard network protocol and port (UDP-512) also.

Anti-Virus

- In opposition to certain other data loss prevention systems, Grayteq DLP doesn't require any specific third-party anti-virus and content-indexing solution on client side and is 100% compatible with your existing software park.

Report and audit

Reports and Audit

With Grayteq Security Orchestrator (SO), you can customize summary views of security incidents and subsequent actions based on any two contextual pivot points. List and detail views, as well as summary views with trending, are available at your fingertips. Grayteq SO also includes a large number of pre-built reports, each of which can be viewed, saved for later use, or scheduled for periodic delivery.

File Audit

Grayteq DLP SO has a built-in, one-in-the-industry File Audit feature that enables you to dig down deep into user file activity logs to automatically build up a file audit that provides you with wide range of information about the lifecycle of the specific file. When, where, under what name it was created by which user. Where it was moved, copied, sent, by which application and which user. Which versions of this file existed and which versions still exist at which locations. Seek for origin, file lifecycle tree and many more. This is File Audit.

Storage Audit

With file audit, a half of a comprehensive data security audit is done. But the other half is still missing. That's why we created Storage Audit. With Storage Audit, it's easy to build-up the storage and file activity history of a storage. Either it is a removable media or a fixed drive. With removable media, you can draw the whole list of data moves, copies and erases, the connections to hosts, the file activity details during a specific connection session and the list of users who have done these actions with a couple of clicks.

Review and Remediate Violations

Grayteq DLP eliminates or minimizes proliferation of sensitive material through integrated incident workflow and case management. If DLP Monitor finds an action that violates protection policies, it generates incidents and sends notifications as to the perpetrator as to the IT security administrators. Incidents created by Grayteq SO can be added to the case management framework, which allows you to involve specialists from numerous organizations within the company to take action on the violation. Additionally, risk dashboards provide easy ways for security personnel to see the profile of policy violations and generate reports.

Customizable Views and Incident Reports

Grayteq SO provides you with numerous options for customizing the view fo the activity logs, the incidents, all rules and policies, users, hosts and groups and allows you to easily rearrange every view to fit your current searching and analytics needs. It's completely up to you to figure out what and how you want to see and Grayteq SO will meet your expectations..

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

Think different

Do different

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

Your Grayteq Partner: