

Endpoint Protection

Keep your borders safe!

With the rapid spreading of various mobile devices, the everyday use of connected devices with large data storing capabilities are now an integral part of your business, your employees' digital lives and pose as potential risk to your valuable data. Your time is valuable and your security shouldn't slow you down. Whether you are a government organization, run your company if a competitive market segment or own a PR agency, a law firm or any other type of business, protecting your data from being leaked or lost via endpoints should be simple and affordable. Grayteq DLP Endpoint Protection provides advanced and real-time protection for your data, your devices, your business.

Removable media protection

Risking your corporate valuables to leak deliberately through any removable medias or accidentally go lost with the USB device itself by an unharmed employee may put your organization into a situation that has way more grave consequences. It may risk your business, your market position, leak your data to a business competitor, breach a GDPR law that causes enormous financial losses and a lot more. That's why we created the industry's most enhanced, fully automated, user-transparent and centrally managed removable media protection packed with unique features.

Known versus unknown

One of the greatest questions in life is how we can separate right from wrong. The base of every endpoint device management is the same with the addition of how accurately we can do it. In Grayteq DLP Endpoint Protection, the New Storage Action feature is designed to make this difference at the very moment of a storage gets connected. You can setup how an unknown connected device should be handled. Grayteq DLP blocks the mounting of the new storage device if New Storage Action is Denied, allow only incoming data transfer from them when in Read-Only mode or allows full, bidirectional data movement when set to Normal mode.

Key Advantages

- Normal, Read only and Blocked modes for any endpoint storage devices.
- Automatic endpoint storage recognition by mount-point, serial number and hardware ID.
- Automated endpoint device and storage inventory creation.
- Unique protection can be assigned to even a single endpoint device.
- Database automatically created and maintained about every connected endpoint devices.
- Device-absent protection rules with pop-up notifications for users.
- Endpoint protection rules are assignable to hosts, users and groups.
- Session-based reports and action-dependant alerts can be generated automatically.

Grayteq DLP Features



DLP Monitor



Rights Management



Data Quarantine



App Management



Endpoint Protection



Encryption for DLP



Intrusion Prevention



Report & Audit

Device management

Grayteq DLP Endpoint Protection engine is capable of uniquely identify every connected storage devices and learn and store the following unique properties - if any - in its internal database:

- Name
- Mount point
- Serial number
- Hardware ID
- Manufacturer ID

It's enough to connect the specific USB device into any Grayteq DLP protected PC, laptop or server once and all of the above details are available about the device and ready to use for the creation of a removable media rule of policy. By using these unique identifiers, you easily can setup a removable media rule and assign it to any specific user, a user group, an Active Director (AD) organizational unit, a specific PC or laptop, a group of computers, or even to all users or devices.

Device assignment

With Grayteq DLP Endpoint Protection, you can single-click assign any endpoint device or storage to a user, a PC, a laptop, or a group of any, making it available for Standard or Read-Only usage. Every Endpoint device is uniquely identified when assigned to a uniquely identified user or computer in order to make security breaching perpetrators fully accountable for their actions. General, corporate-wise used devices can be assigned to All Users or All Hosts making them use able for everyone on every device.

Monitoring and reporting

Data leakage protection for your data on removable devices or in an outgoing email is just a part of your data loss prevention, while combined with the comprehensive monitoring, logging, reporting and real-time alerting capabilities of Grayteq DLP Monitor, you can always keep posted about where your data are, on which endpoint devices, how it is used, on which removable medias are there copies, if those are encrypted or plain, if sent to an unauthorized recipient and where do these data move within your organization and out.

Protected endpoints and devices

Grayteq DLP Endpoint Protection is available for

- Email messaging with Microsoft Outlook
- Email messaging via Web browsers
- Disc type devices
- Infrared & Bluetooth devices
- IEEE 1394 Firewire devices
- Wireless adapters (Microsoft Wireless Zero)
- Serial & parallel port connected devices
- Network devices (Microsoft and Novell network)
- PCMCIA devices
- USB storage devices



Comprehensiveness

- Secure all your endpoints against harmful data leakage. External drives, disc writer, connection port, shares, hardware adapters and other devices. Any of them may pose threat to your data security or integrity. Decide which ones shall be used and the ones shall be rejected and Grayteq DLP will make it happen your way.

Devices, Media, Email.
ALL SAFE

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

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

The Grayteq name, logo, Grayteq DLP and all other Grayteq products named herein are either registered trademarks or trademarks of Sealar Incorporated in the United States and/or other countries. Other names may be trademarks of their respective owners.

All information provided is subject to change without notice. Errors and omissions excepted.

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: