

Encryption for DLP

Erős és iparági sztenderd titkosítás az érzékeny adatai védelmére.

Az átfogó adatbiztonság egyik kulcs tényezője az, hogy a szervezet mennyire tudja adatait megvédeni az illetéktelen kezekbe jutástól vagy, amennyiben mégis rossz kezekbe kerülnek, úgy azok mennyire védettek a jogtalan felhasználás ellen. A Grayteq Encryption for DLP állandó, erős titkosítások különböző vállfajaival védi érzékeny céges adatait munkaállomásain, laptopjain és szerverein, miközben átfogó tevékenység monitorozást, központosított kulcs és titkosítási szabály kiterjesztést, valós idejű riasztást, teljeskörű audit funkcionalitást és riportot biztosít.

Titkosítás, minden körülmény esetére

Többszintű védelemmel az egyszerű, automatizált, teljesen felhasználó-transzparens tároló-, és eltávolítható média titkosítástól a megosztott könyvtárak és meghajtók védelmén keresztül a továbbított adatok erős, iparági sztenderd titkosításáig a Grayteq Encryption for DLP valamennyi felhasználási igényhez, környezethez és helyzethez tud alkalmazkodni.

Fő Előnyök

- Védje érzékeny fájljait a PC-ken, laptopokon, virtuális desktop infrastruktúráiban (VDI), megosztott könyvtárakban, USB és egyéb eltávolítható eszközein és a felhőben.
- Biztosítson erős és egyenszilárd adattitkosítást a céges eszközök teljes palettáján.
- Védje a céges szellemi tulajdont és támogassa a törvényi megfelelést.
- Egyszerűsítse biztonsági menedzsmentjét és biztosítson átfogó kezelést, auditot és jelentést a titkosító kulcsok, politikák és szabályok számára.
- Egyszerűen és hatékonyan terjessze kis titkosítási politikáit a teljes szervezetre.
- Csökkentse a TCO-t és a rendszer összetettségét, központosított biztonsági menedzsment és átfogó védelmi megoldás révén.

Grayteq Data Security Solutions Termékcsalád



DLP



DLP Dashboard



DLP Titkosítás



Classifier



Classifier for Office

Funkciók

Védje helyi adatait

A Grayteq Encryption for DLP valós idejű, felhasználó-transzparens titkosítást és visszafejtést biztosít a PC-ken és laptopokon tárolt adatok számára, ezzel alkalmazva egy újabb védelmi réteget a Grayteq DLP egyéb védelmein túl, legyen az eszköz akár a védett hálózatban vagy azon kívül.

Védje adatait a hálózaton

Az érzékeny fájlok hálózati elérése során a fájlok és könyvtárak elkülönített titkosítása biztosíthatja, hogy a védett adatok olvashatatlanok és felhasználhatatlanok legyenek az engedélyezetlen elérést használók számára. A Grayteq Encryption for DLP használatával különböző kulcsokkal titkosított fájlokat tárolhat egy azoktól eltérő titkosítású könyvtárban, ezzel is növelve a védelmi rétegek számát.

Védje adatait a felhőben

A Grayteq Cloud Share Encryption funkció használatával biztonságosan tárolhat titkosított fájlokat olyan felhő-tároló szolgáltatóknál, mint az Apple iCloud, JustCloud, ZipCloud, Dropbox, MyPCBackup, SugarSync, Backup Genie, CrashPlan, Google Drive vagy a Microsoft OneDrive.

Védje adatait az eltávolítható eszközökön

Bár a hétköznapi USB eszközök kis méretük ellenére igen nagy adattárolási kapacitással bírhatnak, igen könnyen kerülhetnek rossz kezekbe. Az ezen eszközökön tárolt adatok felhasználó-transzparens, automatikus fájl-, és könyvtár titkosítással láthatók el, függetlenül az eszközök gyártójától, méretétől és típusától.

A Grayteq név, logó, a Grayteq DLP és más, a jelen dokumentumban nevesített Grayteq termékek a Sealar, Inc. védjegyei vagy bejegyzett védjegyei az Egyesült Államokban és/vagy más országokban. Az egyéb nevek a tulajdonosaik védjegyei lehetnek.

A közölt információk előzetes értesítés nélküli megváltoztatásának jogát fenntartjuk. Hibák és elírások előfordulhatnak.

A biztonsági politika-alapú titkosítás segítségével egyszerűen és hatékonyan terjesztheti ki a titkosítást a teljes szervezetre, jelentősen csökkentve az adatvesztés kockázatát. A titkosított eszközök akadálytalan használhatóak a szervezet védett gépein kívül is, míg a rajtuk tárolt adatok erős védelmet élvezhetnek.

Észrevétlen felhasználói élmény

A Grayteq Encryption for DLP által titkosított fájlok megtartják eredeti megjelenésüket a felhasználók fel, miközben tartalmuk erős titkosítással védett. A felhasználói visszafejtési jog autentikációja teljes mértékben integrált a Microsoft Windows bejelentkező autentikációval, így bármely Windows bejelentkezési mód, jelszó, token, stb. automatikusan támogatott a fájl és eltávolítható média titkosításokhoz, szükségtelenné téve bármely további autentikációs eljárást.

Rólunk

A Grayteq márka azon szilárd elhatározásból jött létre, hogy az ügyfelek számára kimagasló adatvédelmi megoldásokat szállítson világszerte. A Grayteq termékek megközelítése az adatvédelemhez számos ponton gyökeresen eltér más adatszivárgás megelőző rendszerek gyártói megközelítésétől. Jelmondatunk jól érzékelteti az adatszivárgás és adatvesztés és annak megelőzésére nyújtott megoldásaink gondolatvilágát.

Lépjen kapcsolatba velünk

grayteq.com/contact

Think different

Do different

Teljeskörű rugalmasság

- A dokumentumok, könyvtárak, meghajtók, eszközök és tárterületek egyedi titkosításával a Grayteq DLP Titkosítás széleskörű lehetőségek tárházát biztosítja az érzékeny adatok biztonsági politika-alapú védelmére csakúgy, mint a felhasználók általi, igény-alapú egyedi fájltitkosítás megvalósítására.

Titkosítás. Maga a

BIZTONSÁG

Kezdjük

A Grayteq adatvédelmi csapata segít kialakítani cégének adatvédelmi elvárásait, a prioritásokat és a klasszifikációs rendet és megosztja Önnel a legjobb iparági gyakorlatokat.

Küldje el kérdéseit és elérhetőségét a support@grayteq.com címre.