Grayteq

Adat Karantén

Tartsa cégen belül érzékeny adatait és szabályozza kijutásukat

Széles körben elfogadott tévhit, hogy az adat karanténok csak a gyanús fájlok megsemmisítés-, vagy ártalmatlannak minősítés előtti tárolására használhatók. A Grayteq DLP Data Quarantine funkciójával Ön felépíthet egy több-szintű védelmi falat érzékeny adatai köré mellyel akadálytalan adat-elérést biztosíthat az authentikált felhasználóknak, eszközöknek, alkalmazásoknak, míg kívül tarthatja az engedéllyel nem rendelkezőket miközben erős és áthághatatlan végponti védelmet és szabályzást biztosíthat a mozgatás, másolás, nyomtatás, küldés, fel-, és letöltés számára. Nevezze meg érzékeny adatait, védendő tárolási helyeit, könyvtárait, desktop, laptop vagy szerver gépeit és a Grayteq DLP Data Quarantine megvédi őket az ön számára.

A jól ismert cél, egy csavarral

A Grayteq DLP Data Quarantine fejlesztésének célja egy erős, Grayteq felhasználói authentikáción alapuló, szabadon konfigurálható védelmi képesség biztosítása volt az érzékeny adatokat tartalmazó tároló területek számára, melyek akár néhány kattintással menedzselhetők a szervezet IT szakemberei által, és amelyek a Grayteq Biztonsági Központ (SO) drag-n-drop politika-alkalmazási megoldásával és a Grayteq DLP Agentek erős, jól felépített és könnyen betartatható politikái révén megbízható és egyenszilárd adatvédelmi réteget képeznek.

Akár alapszintű felhasználói jogokkal is kezelhető

A karantén politikák konfigurálhatók akár úgy is, hogy azok használata, alkalmazása és kezelése az átlagos felhasználók által is lehetségessé váljon bármely előzetes IT biztonsági képzés nélkül. Amint egy biztonsági politika alkalmazását és betartatását egyszerű, az előképzettséggel nem rendelkező felhasználók számára is biztonságosan elérhetővé lehet tenni, a biztonság-menedzsment IT biztonsági személyzet vállára nehezedő felelősségét és súlyát jelentősen lehet csökkenteni. A felhasználók számára elérhető politikákat a Grayteq DLP adminisztrátori jogaival felül lehet bírálni.

Grayteq DLP Funkciók

- DLP Monitor
- Jogosultság Kezelés
- **Adat Karantén**
- Alkalmazás Szabályzás
- Végpont Védelem
- DLP Titkosítás
- Behatolás Megelőzés
- Riport és Audit

Fő előnyök

- Elkülönített védelem valamennyi érzékeny adat számára a védett területen belül, a hozzáférés, használat, továbbítás és nyomtatás sza-bályzásával a felhasználók, felhasználói csoportok és alkalmazások számára;
- Erősítse meg adatai védelmét a Grayteq Encryption karanténon belüli alkalmazásával;
- Szabályozza a karanténok alkalmazását a fizikai hely alapján;
- Szabályozza, hogy ki “léphet be” a karantén területére, mely alkalmazásokkal, mit tehessen a karanténos adatokkal és hová és mily módon juttathassa ki azokat a karanténon kívülre;
- Védje a karantéban található adatokat a képernyőfelvételek ellen;
- Kapjon valós idejű riasztásokat a karantén-sértési kísérletekről;

Önmagában is erőteljes, de könnyen társítható

A Grayteq DLP Data Quarantine funkcionalitása önmagában is képes az érzékeny céges adatok vétlen vagy szándékos kiszivárgásának megakadályozására. Ugyanakkor kombinálva a Grayteq DLP egyéb védelmi funkcióival mint a végpont védelem (Endpoint Protection), a titkosítás (Encryption for DLP), a behatolás megelőzés (Host Intrusion Prevention) és a jogosultság kezelés (Access Rights Management), a szervezet IT biztonsága egy jelentős lépést tesz a teljes és egyenszilárd adatvédelem felé, a Grayteq Biztonsági Központjából (SO) vezérelve.

Az általános használattól a legspeciálisabb helyzetekig

Egy adat karantén szabály, más karanténekkel vagy egyéb Grayteq DLP szabályokkal kombinálva lehetővé teszi akár a legösszetettebb és legspeciálisabb adatvédelmi igények leképzését egy finom-hangolt és célzott politikába, mely akár a legbonyolultabb munkafolyamatokat is lépésről-lépésre követni tudja. Ez a részletes, ugyanakkor nagyfokú rugalmasság képessé teszi a Grayteq DLP Data Quarantine szabályzását arra, hogy a lehető legnagyobb mértékben alkalmazkodjon a felhasználók napi munkafolyamataihoz és a biztonsági politikák betartatása mellett a legkevésbé változtassa meg azokat, ezzel is jelentősen csökkentve a felhasználók "fenntartásait".

Bizonyíték, jelentés és valós idejű riasztás, néhány kattintással

Bármely, az érzékeny adatait célzó támadás megakadályozása csak a fele a védelemnek, míg az azonnal jelentés és valós idejű riasztás teszi azt teljessé. A Grayteq DLP Data Quarantine funkciója beállítható oly módon, hogy valós idében értesítse az IT biztonsági kollégákat a kihágási kísérlet összes részletével, a támadó tevékenység megakadálíozásáva egyidőben. Emellett a Grayteq DLP Agent beépített felhasználó-értesítési rendszere segítségével a vétlen vagy szándékos elkövető is értesíthető, hogy az általa megkísérelt tevékenység beleütközött egy használatban lévő Grayteq DLP szabályba vagy politikába. További előnye a Grayteq DLP Agent által készített naplónak, hogy az elkövetés pillanatában akár képernyőfelvételt is készíthet az elkövető képernyőiről, melyel képi bizonyítékot csatol a bizonyító erejű naplóhoz.

Központosított kezelés a Grayteq SO használatával

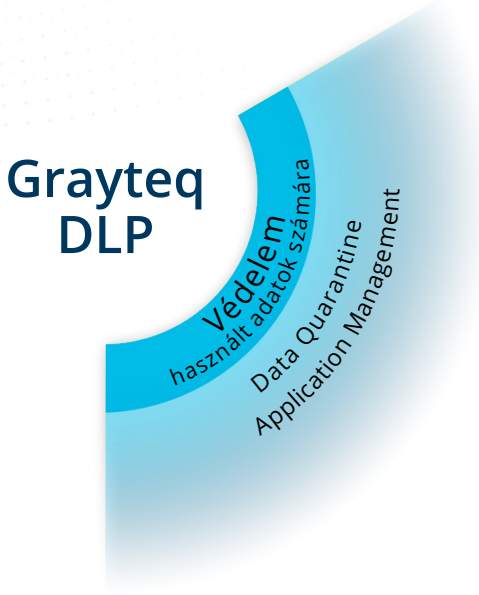
A Grayteq DLP központi, menedzsment szoftvere, a Biztonsági Központ (Security Orchestrator, SO) egyesíti és központosítja valamennyi jogosultság kezelését, ezzel nyújtva átfogó képet a szervezet adatvédelméről. Ezen menedzsment platform integrálja a Grayteq DLP Data Quarantine funkciót a többi Grayteq DLP védelmi komponenssel és funkcióval.

Konklúzió

Rugalmasság, célzott felhasználhatóság, erőteljes politika érvényesítő motor, minden szempontból védett infrastruktúra, központosított menedzsment, könnyű kombinálhatóság a fejlett biztonsági politika kialakítás érdekében, felhasználó kezelhetőség, automatikus riasztás és még sok más teszi a Grayteq DLP Data Quarantine funkciót az egyik legjobb védelmi réteggé, mellyel megvédheti értékes céges adatait.

A következő lépés

További információkért látogasson el a www.grayteq.com/quarantine weboldalra vagy lépjen kapcsolatba velünk a www.grayteq.com/contact oldalon.



Támogatott rendszerek

A Grayteq DLP valamennyi 32- és 64-bites Microsoft Windows Desktop és Server operációs rendszert támogat az alábbiak szerint.

Desktop operációs rendszerek

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

Server operációs rendszerek

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

* A Grayteq DLP valamennyi komponense működik Windows 7 SP1 alatt is, azonban hivatalosan nem támogatott, így néhány funkció működésében lehetnek limitációk.

Kezdjük

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

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

Grayteq

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

Grayteq a Weben

Honlap
www.grayteq.com/hu-hu/

DLP
www.grayteq.com/hu-hu/dlp

Classifier
www.grayteq.com/hu-hu/classifier

DLP Titkosítások
www.grayteq.com/hu-hu/encryptions

DLP Dashboard
www.grayteq.com/hu-hu/dashboard

Árak
www.grayteq.com/hu-hu/prices

Szolgáltatások
www.grayteq.com/hu-hu/services

Az Ön Grayteq Partnere: