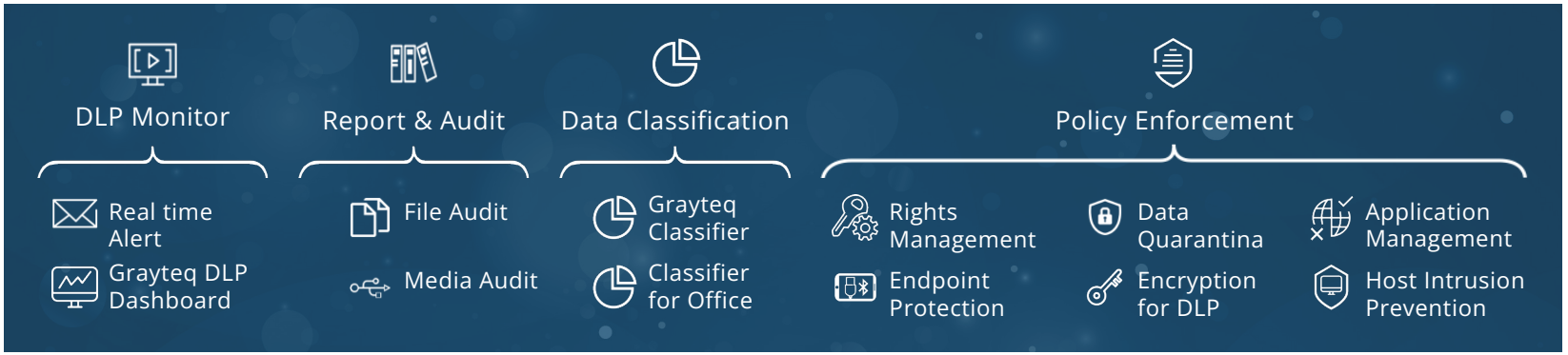
MEGOLDÁS ISMERTETŐ

Grayteq DLP

Átfogó és erős. A védelem amelyre céges adatainak szüksége van.

A céges asztali számítógépeken, laptopok, megosztott szervereken és felhő tárolókon tárolt érzékeny adatok kiszivárgása több szempontból is komoly veszlynek teheti a szervezetet. A védelmük feladata különösen azért bonyolult, mert az érzékeny adatok nem mindig kerülnek megfelelően azonosításra, klasszifikálásra vagy éppen tárolásra. Minél több alkalmazott dolgozik az információkkal, annál nagyobb a valószínűsége annak, hogy valaki vétlenül vagy szándéko-san érzékeny adatot szivárogtat ki illetéktelenek számára. Jópár különböző útvonal és mód áll az információk rendelkezésére, melyeken át elhagyhatják a védett céges környezetet - email, fájl megosztás, web, azonnali üzenetküldők (IM), FTP és még sok más. A megfelelő védelmi poli-tikák érvényesítése alapvető az adatok védelme, az adatvédelmi rendelkezéseknek történő megfelelés és a szellemio tulajdon védelme érdekében, melyeket a Grayteq DLP fellel, klasszifikál és megvéd, miközben naplózza azok használatát, ezzel erősítve a kiszivárgás és elvesztés elleni védelmüket.



Fő Előnyök

Kockázatok beazonosítása

- Az információk felhasználásának monitorozása helyileg és a felhőben
- Az adatok tárolásái helyének és a hozzájuk tartozó adatgazdák beazonosítása.
- Valamennyi tevékenység egyetlen, intuitív felületen elérhető és kereshető.

Politikák és Jelentések

- Használja az előre elkészített, a céges szellemi tulajdont védő biztonsági politikákat.
- Készítsen eseti, kézi és automatikus jelentéseket, bármely nézőpontból.
- Készítsen automatikus riasztásokat a biztonsági kihágásokról és értesítse a biztonsági kollégáit valós időben.

Irányítsa az adatáramlást

- Az Adat Karantén funkció révén egyszerűvé válik az adatutak meghatározása, hogy mely adatok honnan hová mozognak, ki mozgatja őket, milyen alkalmazások használatával, kinek a részére és hogy hol kerülnek tárolásra ezt követően.

Biztonsági Politika a tárolt adatok számára

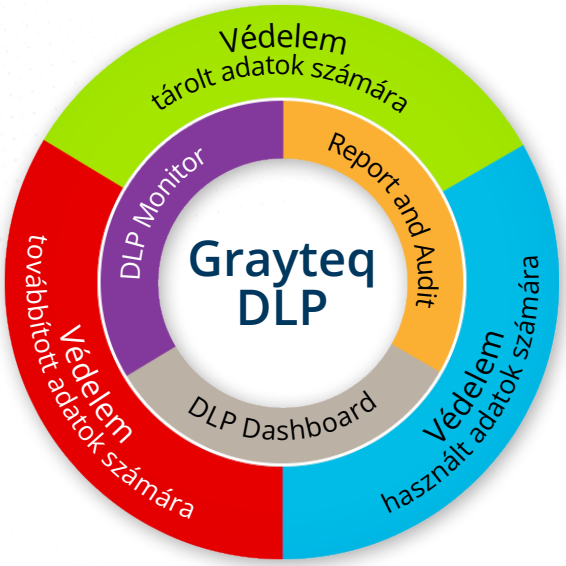
A Grayteq DLP tárolt adatok védelmét biztosító Rights Management és Encryption for DLP kifejezett úgy került kialakításra, hogy hatékony és könnyen menedzselhető védelmet nyújtson az Ön vállalkozása tárolt adatai számára, függetlenül azok tárolási helyétől. Az adat hozzáférések és biztonsági politika megsértési kísérletek folyamatos monitorozása és naplózása mellett a Grayteq DLP automatikusan felülbírálja a Microsoft Címtár (AD) által biztosított adat elérési jogosultságokat, amennyiben azok megsértenék a Grayteq rendszerben beállított jogosultsági politikákat. Ezen működési modell lehetővé teszi az Ön cége számára, hogy valamennyi érzékeny adata számára megfelelő védelmet tudjon biztosítani, kezdve az általánosan használt, rögzített formátumadatoktól az összetett, erősen változó szellemi tulajdonig, bárhol is legyenek tárolva. Az Encryption for DLP funkciókkal, valamint a Grayteq Classifier által nyújtott fájl-besorolási lehetőségekkel párosítva az adott adat bármely előfordulása automatikus védelmet élvezhet.

Biztonsági Politika a használt adatok számára

A Grayteq DLP folyamatosan monitoroz valamennyi adat-elérést az általa védett rendszerben és betartat minden biztonsági politikát annak érdekében, hogy hogy megvédje az Ön érzékeny adatait a kiszivárgástól illetve az elvesztéstől. A Data Qurantineés az Application Management funkciói egy “védelmi kerítést” hoznak létre a használatban lévő adatai köré, megakadályozva az adott adat nem megfelelő használatát vagy kijuttatását bármely engedéllyel rendelkező vagy nem engedélyezett felhasználó illetve alkalmazás számára. Az adott biztonságsértési kísérlet blokkolását követően automatikus, valós idejű riasztás révén értesíti a biztonsági adminisztrátorokat az adott incidensről, valamennyi olyan részletet tudatva velük, mellyel a megfelelő válaszlépés kialakíthatóvá válik. A Grayteq DLP végponti “ügynöke” ezzel párhuzamosan felúszó ablakban értesítheti a felhasználót, hogy az általa megkísérelt művelet megsértette valamely biztonsági politikát és bizonyos esetekben - függően a felhasználó biztonsági besorolásától - akár az adott politika felülbírálatát is felajánlhatja a felhasználónak. Ezen különleges jog használata révén a felhasználó egy időszakos politika-felülbírálatot kezdeményezhet, mely a korábban tiltott művelet végrehajtását lehetővé teszi, de előzőleg tudatja a felhasználóval, hogy a felülbírálat, mint tudatos biztonsági politika felülbírálat kerül naplózásra és az azt követő cselekmény teljes egészében a felhasználó felelőssége.

Biztonsági Politika a továbbított adatok számára

A cégen belül, részlegek között, az egyes felhasználók által alkalmazásokon és protokollokon keresztül megosztott fájok védelme valamennyi adatvédelmi rendszer sarokköve. Az adatok adathordozón vagy hálózati úton történő vétlen vagy szándékos kiszivárogtatása elleni védekezés proaktív megközelítést igényel. A Grayteq DLP automatikusan alkalmazza a biztonsági szabályzásokat valamennyi, a rendszert elhagyni szándékozó fájlra, míg az emailben történő kiküldés ellen a Microsoft Outlook alkalmazásba integrált Grayteq Email Security nyújt védelmet. Biztonsági kihágási kísérlet észlelése esetén a Grayteq DLP automatikusan blokkolja a műveletet, valamennyi részletéről időbélyeggel ellátott naplót készít és akár automatikus jelentés, akár riasztás útján valós időben értesíti a biztonsági személyzetet. Ezen ellenlépések révén az ön vállalkozása megfelelhet a személyes adatok védelmére előírt követelményeknek és jelentősen csökkentheti a biztonsági kihágásoknak való kitettségét.



Alapvetés

A biztonsági incidensek listájának abszolút első helyezettje az ügyféladatok elvesztése és az adatbiztonsági kihágások első számú forrásai a felhasználók.

Tudja Ön, hogy hol vannak az adatai?

Független, haramdik féltől származó jelentés szerint a szervezetek csupán 47%-a teljesen biztos abban, hogy adatai fizikailag hol vannak tárolva és csak 44%-a rendelkezik megfelelő szintű rálátással a GDPR szabályozásokra és azok a cégre gyakorolt hatásaival.

Kezdjük

A Grayteq adatvédelmi szakértői csapata Önnel együtt segít megfogalmazni cégének adatvédelmi elvárásait, a prioritások kialakításában, az információk klasszifikációs rendjének kidolgozásában és megosztja Önnel a legjobb iparági gyakorlatokat.

Küldje el kérdéseit vagy érdeklődésének irányát emailben, elérhetőségeivel a support@grayteq.com email címre.

Grayteq

Védelem a tárolt adatok számára

Rights Management

A Grayteq DLP Data Quarantine korábban nem látott szintű védelmet biztosít tárolt adatai számára, a tároló biztonsági politikák ötvözését a Rights Management beállításaival. A Data Quarantine komplex biztonsági politikák kialakítást teszi lehetővé, melyek révén szabályozható, hogy ki férhet hozzá a karantéban tárolt fájlokhoz, mely alkalmazások használatával és mely útvonalakra, illetve email küldés esetén csak belső email címekre vagy külsőkre is kijuttathatóak legyenek-e. A különböző beállítású szabályok rétegzése lehetővé teszi a legösszetettebb munkafolyamatok leképzését is, mely dinamikusan tudja követni a különféle szcenáriókat és a Grayteq Encryption for DLP révén akár a rendszeren kívülre juttatott fájlokat is.

Encryption for DLP

Eltávolítható eszköz-, Fájl és könyvtár-, valamint Cloud Share Encryption egyaránt rendelkezésre áll az érzékeny adatok tárolási helyétől független titkosítása érdekében. Valamennyi titkosítási illetve visszafejtési művelet teljesen felhasználó-transzparens módon, valós időben, a felhasználói azonosító adatok használatával biztosított. Alkalmazhat központilag menedzselt biztonsági szabályokat akár felhasználókra, akár felhasználói csoportokra, egyes fájlokra, de akár teljes könyvtárakra vagy eszközökre is, bárminemű felhasználói közreműködés nélkül. A Grayteq Encryption for DLP tovább erősíti az Ön védelmi rendszerét korlátlan számú, egyedileg beállítható, központilag menedzselt, iparági sztenderd titkosításai révén, ezzel akadályozva meg a fájlok illetéktelenek általi visszafejtését és használatát.

További információk az Encryption for DLP termékről.

Host Intrusion Prevention

A Grayteq DLP szabadalmi bejegyzés alatt álló, egyedi Host Intrusion Prevention (HIP) technológiája segítségével korlátlan számú elkülönített vagy éppen egymást részben vagy egészében átfedő védelmi zóna alakítható ki a céges hálózaton belül, mely szoftveres elkülönülést biztosít az egyes hálózati szegmensek, részlegek vagy számítógép csoportok között. A technológia egy adott csatlakozási kísérlet során egy kérdés-válasz alapú authentikációt biztosít a "hívó" és a "hívott" gépek között, ezzel - a megfelelő HIP politikához kötött authentikációt követően - biztosítva az akadálytalan és felhasználó-transzparens kommunikációt az eszközök között. Valamennyi "bejövő" kapcsolati kísérlet naplózásra és valós idejű riasztásra kerül.

Classifier, Classifier for Office

Az érzékeny adatok védelme sokkal megbízhatóbbá válik, amennyiben a védendő adatok felismerése és osztályzása egy megfelelő klasszifikációs alkalmazás révén valósul meg. A Grayteq Classifier a Grayteq DLP rendszerhez legjobban illeszkedő adatklasszifikációs alkalmazás, melynek használatával a felhasználók, az adott fájl tartalma alapján saját maguk is feljogosítottá válnak a fájl manuális klasszifikációjára, melynek alapján a Grayteq DLP rendszer a megfelelő védelmi szabályokat és politikákat automatikusan alkalmazni tudja. A Classifier a fentieken túl, a fájlok tárolási helye alapján történő automatitikus klasszifikációt is képes elvégezni, mely a fájl az adott területre történő bemozgatása, bemásolása vagy mentése során megtörténik. A Classifier felhasználói modulja automatikus, a klasszifikációs szintnek megfelelő színű jelzéssel látja el a fájlok ikonjait, ezzel is tudatva a felhasználókkal az adott fájl besorolását, míg a Classifier for Microsoft Office a Microsoft Office programcsalád tagjainak szalagjában (ribbon bar) biztosítja a felhasználók egy kattintással történő fájl klasszifikációját.

További információk a Grayteq Classifierről

Fő Előnyök

Valós időben

- Valós idejűsége révén a Grayteq DLP azonnal kijavítja a sérülékenységeket és megállítja a fenyegetéseket.

Hatékony

- A hatékonyság a politikák alkalmazása és a meglévő infrastruktúrába történő akadálytalan beépülés szintjén egyaránt fontos.

Átfogó

- A teljes lefedettségnél kevesebb egyszerűen nem elég. Fedje le az egészet és biztonságban lesz!

Gyors

- Szerezzen gyors, szoftveresen javított védelmet napjaink legkeményebb és legrejtettebb fenyegetései ellen.

Egyesített

- Egyesítse végpontjai kezelését a virtuális-gépektől és szerverektől az asztali gépekig és laptopokig.

Grayteq

Védelem a használt adatok számára

Application management

Alkalmazások milliárdjai léteznek mindenfelé. Némelyik hasznos eszköz, egy részük biztonsági szempontból teljesen lényegtelen, míg egy részük kimondottan azzal a céllal készült, hogy kárt okozzon a felhasználók számára. A játékok, az engedélyezetlen böngészők, az azonnali üzenetküldők (IM), a közösségi média eszközök és egyéb, céges szempontból nemkívánatos alkalmazások pusztán figyelemelterelő képességük révén is jelentősen ronthatják a munkavállalók hatékonyságát. A Grayteq DLP automatikus alkalmazás felismerő szkennelési képessége révén ön könnyedén fellelheti valamennyi, a hálózatán található futtatható fájlt, melyeket "Engedélyezett", "Tiltott" illetve "Elbírálás alatt álló" alkalmazás-listákba történő rendezésével egy csapásra megoldhatja az alkalmazások központosított menedzsmentjének problémáját.

Data Quarantine

A Grayteq DLP Data Quarantine funkciója a Rights Management funkcióval kombinálva teljeskörű, központilag menedzselt, folyamatosan naplózott és bármely Windows jogosultság számára szabályozható védelmet jelent az ön érzékeny adatai számára. A Data Quarantine az adat hozzáférési kísérlet legelső lépésétől, az engedélyezett hozzáférést követően a fájlokkal történő valamennyi műveleten át azok mentését, küldését, másolását, törlését és bármely a fájlokkal kapcsolatos műveletet egyaránt képes vezérelni, míg a "kijárati útvonalak" és alkalmazások kezelésével az adatok - védett területről történő - kimozgatását is képes teljes egészében az ellenőrzése alatt tartani. Természetesen a Karanténsértési kísérletekről a többi Grayteq DLP védelmi funkcióval megegyezően naplók, jelentések és valós idejű riasztások készülhetnek.

Fő Előnyök

Réteges védelem

- Erősítse meg adatai védelmét a védelem különböző rétegeinek egymásra helyezésével.

Rugalmasság

- Élvezze a legmagasabb szintű rugalmasságot, adatai védelme és a folyamatosan változó környezethez történő alkalmazkodás terén.

Tartsa fenn az adatáramlást

- A céges működés egyértelműen legfontosabb eleme a belső adatáramlás fenntartása, miközben a kifelé irányuló adatáramlást tartsa a kezében.

Koncentráljon az üzletre

- Emelje üzleti hatékonyságát a Grayteq központi menedzsment konzolja és az iparág legalacsonyabb erőforrás-igénye révén.

Grayteq

Védelem a továbbított adatok számára

Endpoint Protection

Védje valamennyi hagyományos asztali gépét és laptopját, saját szervereit és felhőben tárolt adatait a Grayteq DLP központi menedzsment konzoljáról vezérelhető Végpont Védelemmel. A Grayteq DLP integrált részeként az Endpoint Protection teljeskörű, 7/24-es monitorozást és védelmet biztosít az ön összes Windows alapú eszközének. Szabályozza az eszközökön tárolt és azokra továbbított adatok kiáramlását valamennyi protokollon, valós időben. Míg a központosított, egy konzolról történő vezérlés jelentősen csökkenti a szervezet informatikusai vállára nehezedő terhet és egyben azonnali reakcióra ad lehetőséget bármely biztonsági fenyegetés esetén. Legyen pro-aktív ha adatai védelméről van szó és használja a Grayteq endpoint Protection-t mint a biztonsági infrastruktúra egy újabb rétegét.

Encrypted Data Transmission

Miközben z Encryption for DLP eredetileg a tárolt adatok erős titkosítására készült, Az Encrypted Data Transmission(EDT) az úton lévő fájlok titkosított védelmét hivatott ellátni, a továbbítás teljes tartama alatt, valamint azt, hogy a továbbított adatok csak egy Grayteq DLP-vel védett gépen legyenek visszafejthetők és hogy az előzetesen a fogadó kliensre disztributált biztonsági szabályok megvédjék a visszafejtett adatokat. Az EDT titkosító és visszafejtő motorja a Windows authentikációját használja és a felhasználók számára a Windows Explorer jobb-klikkes menüjébe beépülve érhető el.
Tudjon meg többet a Encryption for DLP termékről.

Fő Előnyök

Védett végpontok

- Függetlenül attól, hogy melyik végpont van éppen használatban, biztosítjuk az Ön zavartalan védelmét.
  A védett végpont fontos!

Megosztás védelem

- Védje megosztott érzékeny adatait valamennyi eszközén és eltávolítható médiáján.
  A megosztás védelem fontos!

Titkosítás

- Az adatok továbbításakor a megfelelő, iparági sztenderd, erős titkosítás nélkül a védelem nem lehet teljes.
  A titkosítás fontos!

A Grayteq DLP FONTOS

Grayteq

DLP Monitor

Valós idejű monitorozás, nyomon követés, logolás és riasztás

Nem számít, melyik iparágban működik az Ön cége, szüksége van monitorozásra, nyomon követésre, logolásra és riasztásra ahhoz, hogy tudja, mi történik érzékeny adataival, mely alkalmazások, protokollok, végpontok használatával. A Grayteq DLP Monitor valós idejű tevékenység monitorozást, nyomon követést és naplózást biztosít valamennyi fájlműveletre a teljes hálózaton annak érdekében, hogy láthatóvá váljon, hogy milyen információk és milyen módon kerülnek továbbításra a felhasználók között a szervezeten belül és hogy mely útvonalakon keresztül kerülnek kijuttatásra. A Grayteq DLP riasztása révén egyszerűen hozhat létre bármely tevékenység által kiváltott riasztást az informatikai biztonsági személyzet automatikus értesítésével. A riasztások valamennyi részletet tartalmaznak, melyek elősegítik a minél gyorsabb és hatékonyabb incidens kezelést és az azok további előfordulását megelőző politikák kidolgozását. A Grayteq DLP Monitor által használt, nagy hatékonyságú, a Windows magjába (kernel) beépülő Grayteq Agent felfedi valamennyi, az Ön adatait fenyegető veszélyt és megakadályozza azokat, ezzel véde meg az ön szervezetét az adatvesztéstől. Ugyanakkor fejlett felhasználói értesítő rendszere révén a Grayteq DLP Monitor egyben alkalmas a felhasználói magatartás és adatbiztonsági tudatosság fejlesztésére.

Analízis és szabály hangolási lehetőségek

A Grayteq DLP egyedi naplózási technológiája és a biztonsági politikákba beépített Test Mode révén a szabályok és politikák az élő rendszeren kerülhetnek tesztelésre annak veszélye nélkül, hogy egy esetlegesen hibásan beállított szabály bármilyen fennakadást okozhatna a működésben. Ezen metódus lehetővé teszi a DLP szabályok egyszerű testre szabását, melyek így a legjobban tudnak alkalmazkodni a folyamatosan változó üzleti igényekhez. A DLP Monitor beépített "lefúrásos" technológiájú elemző rendszere révén a folyamatok legmélye is felderíthető és ezen adatok birtokában olyan szabályok és politikák alakíthatók ki, melyek a tökéletesen alkalmazkodnak a mindennapi munka menetéhez és amelyek a legkevésbé kívánják meg ezen folyamatok bármilyen szintű megváltoztatását. Ez pedig egyértelműen segíti a felhasználói "ellenállás" minél alacsonyabb szinten tartását.

Egyszerű terítés

Nem biztos, hogy minden irodában biztonsági szakemberek ülnek - épp ezért készítettük a Grayteq DLP teljes ügynök-, és biztonsági politika terítési rendszerét a lehető legegyszerűbbre. A Grayteq rendszer és a biztonság-kezelése teljes mértékben központosított a Grayteq DLP Security Orchestrator (SO) keresztül - mely használatával a naplók és politikák átfogó kezelése valamennyi támogatott eszközön egyszerűen megvalósítható.

Központosított Menedzsment és Emelt szintű Jelentés

A Grayteq SO a Grayteq biztonsági környezet szíve és lelke. Használja a központosított SO konzolt a kötelező érvényű, cég szinten alkalmazandó és betartatandó biztonsági politikák elkészítéséhez és terítéséhez és kövesse nyomon az adat-hozzáféréseket, hogy ki és hogyan használja azokat, hogy hogyan történik a védendő adatok titkosítása, nyomon követése és megvédése a kiszivárgástól. Központilag határozza meg, terítse, kezelje és frissítse a monitorozásra, kezelésre, engedélyezésre vagy blokkolásra, jelentésre és valamennyi engedélyezett és nem engedélyezett adatelérésre vonatkozó szabályait, ezzel védve érzékeny és értékes céges adatait.

Grayteq DLP Dashboard

IT és IT biztonsági vezetőknek de akár a legfelső vezetésnek alapvetően nincs szüksége valamennyi biztonsági működési részletre a megfelelő döntések meghozatalához. Ugyanakkor a vezetői szintű betekintés elengedhetetlen a biztonsági kérdések és politikák megfelelő megértéséhez és naprakészen tartásához. A Grayteq DLP Dashboard ezen alapvetés szerint került kifejlesztésre, hogy menedzsment szintű áttekintést, jelentéseket, analítikákat készítsen az aktuális biztonsági helyzetről és segítsen a szervezet egészét érintő jelenlegi és jövőbeni IT biztonsági stratégia kialakításában.

További infrmációk a Grayteq DLP Dashboard termékről.

Kompatibilitás

Operációs Rendszer

- A Grayteq DLP valamennyi 32- és 64-bites Microsoft Windows Desktop és Server operációs rendszert támogat Windows 8 és Windows Server 2012 R2-től.

Adatbázis és SYSLOG

- A Grayteq DLP a saját, beépített adatbázisával kerül leszállításra, úgyhogy Önnek nincs szüksége harmadik féltől származó adatbázis licencre a Grayteq DLP előnyeinek használatához, mivel a meglévő Oracle Database Server (Oracle 11G R2-ig) vagy a Microsoft SQL Server (SQL Server 2019-ig) vagy PostgreSQL (ANSI vagy Unicode módban) adatbázisát is használhatja.
- A meglévő SYSLOG rendszer az ipari sztender hálózati protokollokon és az UDP-512-es porton szintén használható.

Anti-Vírus

- Más adatszivárgás megelőző rendszerekkel ellentétben a Grayteq DLP nem igényli bármely specifikus antivírus vagy tartalom-indexelési szoftver kliens-oldali alkalmazását és 100%-ban kompatibilis az ön jelenlegi szoftver parkjával.

Report and Audit

Report and Audit

A Grayteq Security Orchestrator (SO) használatával, testre szabhatja a biztonsági incidensek és az azokhoz kapcsolódó intézkedések nézetét és azok egymásra gyakorolt hatását. Lista és részletes nézetek csakúgy, mint a trendek áttekintő nézetei egyaránt elérhetőek néhány kattintással. A Grayteq SO ugyanakkor jelentős számú előre kialakított jelentést is tartalmaz, melyek mindegyike megnézhető, későbbi használatra menthető, módosítható de akár automatizálható is a periódikus használathoz.

File Audit

A Grayteq DLP SO beépített, az ipargában egyedülálló File Audit funkcióval rendelkezik, melynek segítségével lehetővé válik a lefúrás a felhasználói tevékenységeket rögzítő naplók legmélyére, így hozva létre az adott fájl teljes életciklusát átfogó fájl audit jelentést. Hol, mikor, milyen néven, mely felhasználó készített a fájlt. Hová került mozgatásra, másolásra, átnevezésre, elküldésre és mindezt mely felhasználó, milyen alkalmazások használatával tette. Mely verziói léteztek vagy léteznek és hol találhatók a hálózaton. Keresse meg a fájl eredetijét, a teljes életciklusát és még sok mást. Ez a File Audit.

Media Audit

A File Audit csupán az egyik fele egy átfogó adatvédelmi audit rendszernek. De a másik fele is fontos. Ezért készítettük a Media Audit funkciót, melynek segítségével a adott tároló teljes használati életútja és a tárolón történt fájl műveletek életútja ábrázolható. Legyen az akár eltávolítható, akár rögzített tároló. Az eltávolítható eszközökön a teljes fájlműveleti, másolási és törlési életút mellett a különböző számítógépekhez történt csatlakozások, eltávolítások és a csatlakozások alatt történt fájlműveletek csakúgy, mint az azokat végrehajtó felhasználók listája néhány kattintással megjeleníthető.

Kihágások Áttekintése és Kijavítása

A Grayteq DLP a beépített incidens-munkafolyamat-, és eset menedzsmentje révén csökkenti vagy akár meg is szünteti az érzékeny adatok ellenőrizetlen terjesztését. Amennyiben a DLP Monitor felismer egy biztonsági kihágási kísérletet azonnal incidenst készít és értesíti úgy az elkövetőt, mind a biztonsági személyzetet. A Grayteq DLP Monitor által készített incidensek az értesítési rendszeren keresztül lehetővé teszi a biztonsági szakértők számára, hogy azonnal felléphessenek a kihágás ellen. Ezen felül a Grayteq DLP Dashboard egyszerűen áttekinthető és részletekbe menő menedzsment kimutatást nyújt az adminisztrátorok és vezetők számára.

Testreszabható Nézetek és Incidens Jelentések

A Grayteq Biztonsági Központja (SO) számos lehetőséget biztosít ahhoz, hogy egyedi nézetekben kerüljenek megjelenítésre a tevékenység naplók, az incidensek, valamennyi szabály és politika, a felhasználók, a számítógépek és csoportjaik annak érdekében, hogy minél jobban megfeleljenek az ön keresési és elemzési elvárásainak. Teljes mértékben önön múlik, hogy mit és hogyan szeretne látni és a Grayteq SO megjelenítő rendszere meg fog felelni az elvárásainak.

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 velünk kapcsolatba

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: