



 Grayteq
Data Security Solutions

Teljeskörű védelem érzékeny adatai számára

Napjainkban az adatok védelme egyértelműen a legfontosabb feladattá lépett elő, mely a vállalatok biztonsági és megfelelőségért felelős szakembereinek figyelmét igényli. A GDPR törvények az adatbiztonsági és a magánéletet érintő eseményeket felemelték a legfelső vezetés döntési szintjére, a nem-megfelelőség komoly következményei miatt, miközben az egyre terjedő felhő alapú szolgáltatások tovább emelik az IT biztonsági szakemberek kihívásait. És mindezt úgy, hogy az emelt szintű biztonság még véletlenül se fenyegetsen az engedélyezett adatáramlás vagy az üzleti folyamatok megbénításának kockázatával. Ahogy az emelt vállalati biztonság és megfelelés terhe emelkedik az IT vállán, az adatok védelme egy végeláthatatlan küzdelemnek tűnhet. Pedig nem kell annak lennie. Néhány adaszivárgás-megelőző megoldás (DLP) a bevezetése és üzemeltetése során egyaránt jelentős erőforrás-, és beruházási igénnyel bír. Néhány a "mely adatokat kell megvédeni" kérdését szegezi az üzleti oldalnak. Néhány pedig a védelmi funkciók mindegyikéhez külön felületet, szaktudást, alrendszer igényel. A Grayteq Data Security Solutions termékcsalád, egy közös felületről vezérelve, kezelhető léptékű erőforrás és beruházás igénnyel, megválaszolhatatlan kérdések nélkül oldja meg az adatvédelem valamennyi feladatát.

Fő Előnyök

Központi menedzsment

- A központi vezérlő konzolról valamennyi biztonsági politika, szabály, felhasználó, eszköz, riport, riasztás, incidens és annak kezelése vezérelhető.

Biztonsági politikák PC-ken, notebookokon és végponti eszközökön.

- A politikák betartatása független a védett eszközök kapcsolati állapotától lévén a szabályok a védett eszközökön kerülnek tárolásra.

Védelem a tárolt, továbbított és használt adatok számára.

- Az adat pillanatnyi helyétől függetlenül a védelem mindenkor fennáll.

Rugalmasság, minden területen.

- A Grayteq a legteljesebb rugalmasságot biztosítja a felhasználók, politikák, eszközök, fájl típusok, helyi-, hálózati és felhő tárolók kezelése terén.

Grayteq Termékcsalád



DLP Monitor

A Grayteq DLP Monitor valós időben folyamatosan figyeli a felhasználói tevékenységeket. A mélyreható - automatikus vagy kézi - klasszifikáció vagy a fájlok tárolási helye alapján azonnali áttekintést, szabály létrehozást és érvényesítést és a folyamatosan változó informatikai környezet mind pontosabb lekövetését biztosítja a védelmek alakítása érdekében. Ugyanakkor biztonsági incidens esetén gyors és hatékony felderítést, elemzést és ellenintézkedést biztosít valamennyi a nyomozáshoz szükséges releváns információ biztosításával. A Grayteq DLP Monitor ugyanakkor átfogó betekintést nyújt arról, hogy az érzékeny adatok hol találhatóak, ki és hogyan használja őket és hová kerülnek továbbításra. Ugyanakkor a nagyfokú rugalmasság érdekében fizikai szerverekre és munkaállomásokra csakúgy, mint virtuális környezetekre optimalizálásra került. Tudjon meg többet a [Grayteq DLP Monitorról](#)

DLP Policy enforcement

A Grayteq DLP Policy Enforcement motor a Grayteq Security Orchestrator (SO) integrálódva betartatja a hozzáférés vezérlési, végpont védelmi, adat karantén, tároló-, és eszköz kezelési, titkosítási, email-, webmail, instant üzenetküldési (IM) és egyéb biztonsági politikákat. A Politikák az SO-n keresztül - titkosított üzenetben - kerülnek kiterjesztésre a végpontokra telepített Grayteq Agentek számára, melyek - az eszköz csatlakozási állapotától függetlenül - betartatják azokat és közben valamennyi felhasználói cselekményről időbélyeggel ellátott, titkosított naplóbejegyzést készítenek. Valamennyi szabály és politika elkészíthető Teszt-módban, melynek segítségével a DLP szabályzások az élő környezeten kerülhetnek tesztelésre és finomhangolásra anélkül, hogy egy esetlegesen hibásan beállított szabály veszélyeztetné az üzletmenet-folytonosságát. Központi konzolja révén a Grayteq DLP megoldások egyenszilárd védelmet, teljeskörű áttekintést és egyszerű adminisztrációt biztosítanak, ezzel növelve az üzleti hatékonyságot és csökkentve az adminisztrációval járó terheket.

DLP Access Rights Management

Míg az adatvédelmi kihágások 73%-t külsős elkövetők hajtják végre, melyek 80%-a a kiemelt jogosultságok megsértése vagy nem megfelelő használata révén következik be, sosem volt fontosabb a szervezeti "bejáratok" őrzése és megfelelő zárva tartása, A kiemelt jogosultságok megfelelő kezelése és illetéktelenek előli elzárása, illetve a felhasználói és rendszer hozzáférések

monitorozása. Ugyanakkor ezen megközelítés gyakran több különböző eszköz kombinált használatát igényli, melyek nem állnak egymással kapcsolatban. Így viszont hogy lenne lehetséges szükségtelen bonyolítás nélkül megfelelő hozzáférés-ellenőrzést, védelmet és megelőzést biztosítani a munkafolyamatok megsértése nélkül? A Grayteq DLP Access Rights Management hatékonyan alkalmazza a hozzáférések szabályzását, a tárolók, folyamatok, alkalmazások és eszközök szabályzását, biztosítva a megfelelő jogosultságok birtokában az akadálytalan hozzáférést, míg megakadályozva az illetéktelen elérést és adat használatot.

További információk a [Grayteq DLP Access Rights Managementről](#)

DLP Reports, Alerts and Audit

A Grayteq DLP valós idejű riasztásokat, kézi-, automatikus és időzített riportokat és teljeskörű audit jelentéseket biztosít a fájlokkal, gépekkel és felhasználói tevékenységekkel kapcsolatban. Néhány kattintással a Grayteq SO-n különböző fókuszú, időintervallumú riportokat készíthet akár a valós idejű naplóból, akár egy önálló, vagy tetszőleges számú egymáshoz csatolt archív naplóállományból, akár egy gépről, akár gépek tetszőleges csoportjáról, egy felhasználóról, egy csoportról vagy egy szervezeti csoportról (OU). Szervezeti-, és rendszer-szintű analízisei révén a legmélyebb szinten nyomon követhető és átlátható, hogy hol kerülnek tárolásra az adatok, ki, mikor, mivel és milyen módon kerül velük kapcsolatba és használja azokat és hogy hová és hogyan továbbítja, ezzel tárva fel a szervezeti mozgások és változások okozta biztonsági réseket, miközben valós idejű riasztásokat készít biztonsági kihágási kísérlet esetén. Tudjon meg többet a [Grayteq DLP Reports, alerts and auditról](#)

DLP Endpoint Protection

Grayteq DLP Endpoint Protection teljeskörű védelmet biztosít a belső fenyegetésekkel szemben. Tároló-, eszköz-, protokoll-, nyomtató-, email-, és egyéb végponti biztonsági politikái jóvoltából átfogó, központosított védelmet nyújt, mindezt a Grayteq Security Orchestrator (SO) felügyeletével. A Grayteq DLP Endpoint Protection politikái biztosítják az adatszivárgás megelőzését úgy a cégen belül, mint otthon, útközben és a felhőben, ezzel csökkentve az alkalmazottak cselekményei által esetlegesen létrejövő adatvesztési, pénzügyi veszteséget illetve piaci pozíció veszteséget okozó veszélyektől. Hasonlóan az egyéb biztonsági politikáktól, a Grayteq DLP Endpoint Protection szabályrendszere valós időben kerül betartatásra, ezzel

Érdekesség

Az adatvesztés gyakorisága szempontjából a veszélyeztetett ügyfélrekordok kiszivárgása vezet a biztonsági incidensek listáját, és az alkalmazottak jelentik a biztonsági incidensek első számú forrását.

Tudja, hol vannak az adatai?

Egy harmadik fél adat-rezidencia jelentése szerint a szervezeteknek csak 47%-a van teljeskörűen tudatában annak, hol található adatai fizikailag – és csak 44%-uk ismeri alaposan a GDPR-szabályozást és annak hatását.

Kezdjük

A Grayteq szakértői csapata segít megfogalmazni cége adatvédelmi elvárásait, a prioritások kialakítását, a klasszifikációs rend kidolgozását és megosztja Önnel a legjobb iparági gyakorlatokat.

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

szabályozva a felhasználók adathasználatát és adat továbbítását. Bármely kihágási kísérletről valós idejű riasztás hozható létre, mellyel egyidőben az adott kísérlet megkadaályozásra kerül.

Tudjon meg többet a [Grayteq DLP Endpoint protectionról](#)

Encryption for DLP

A Grayteq Encryption for DLP különböző titkosítási megoldásokkal támogatja az adatszivárgás megelőzését. Iparági standar titkosítási technológiai kiterjeszthetők asztali PC-kre, laptopokra, hálóeati fájlokra, könyvtárakra és eltávolítható eszközökre. A megoldás AES, Serpent és DES titkosítási algoritmusok használatával biztosítja az erős titkosítást. A Grayteq Encryption for DLP megvédi az Ön adatait, függetlenül azok típusától, méretétől, tárolási helyétől, továbbításuk módjától és irányától.

Tudjon meg többet a [Grayteq Encryption for DLP-ről](#)

DLP Dashboard

Napjaink egyre összetettebb informatikai környezeteiben a korábban elkülönülő feladatok és szerepkörök kezdenek összemosódni, így a Grayteq DLP Dashboard használatával néhány kattintással lehetőség nyílik az összetett rendszerből teljesskörű áttekintést és különböző szempotok szerinti vezetői jelentések elkészítésére. Amellett, hogy a Grayteq Data Security Solutions teljes portfóliójának felügyeletét a Grayteq Security Orchestrator (SO) látja el, a Grayteq Dashboard betekintést és analitikákat biztosít a teljes rendszerről, ezzel emelve a beépített jelentések és betekintési képességeket egy új szintre.

Tudjon meg többet a [Grayteq Dashboardról](#)

Grayteq Email Security

A Grayteq Email Security, mint a Microsoft Outlook beépülő modulja lehetővé teszi a kifelé irányuló email forgalom hatékony és biztonságos szabályozását. A beépülő modul elérhető valamennyi Microsoft Outlook 2010 és újabb verziókra és teljesskörűen vezérelhető a Grayteq Security orchestraotr (SO) felületéről. Számos küldési paramméter és védelmi opció megadhatóvá válik csakúgy, mint biztonságos illetve veszélyes email címek, domainek, doain kiterjesztések. A Grayteq Email Security ugyanakkor képes értesíteni a felhasználót, amennyiben az email-ben küldeni kívánt dokumentum nem küldhető valamely címzettnek és a tiltott címzettet automatikusan el is távolítja, miközben a küldési kísérlet valamennyi részletét naplózza, ezzel

biztosítva bionyítékot a későbbi elemzések és értékelések számára. Ezek mellett valós idejű riasztások küldésére is lehetőség nyílik bármely kifelé irányuló email küldés vagy annak kísérlete alapján.

Grayteq Classifier

Az automatizált és a felhasználó által alkalmazott osztályozási támogatás megfelelő keverékével rendelkező osztályozási eszközök jelentősen növelhetik a végfelhasználók tudatosságát az adatok kezelése során. Mivel a vállalatokat egy nagy lépéssel közelebb kell vinni a GDPR-megfelelőséghez, a Grayteq Classifier a piacon elérhető legkifinomultabb fájlosztályozási megoldások egyikévé vált. Amellett, hogy lehetőséget ad a fájlok manuális besorolására a felhasználók számára, a beépített hely-alapú osztályozási képességei automatikusan is el tudja végezni a feladatot. További besorolási jelölési funkciói, mint például a színes, besorolási szinttől függő dokumentumfejléc, lábléc módosítás, szabadon beállítható szöveg vagy kép vízjelként történő használata, egyedi metacímkezés és egyedi fájltulajdonságok, illetve a fájl ikonok módosítása és még sok más teszi a Grayteq Classifier-t képessé arra, hogy a szervezeteket végig segítse értékes adataik sikeres és megfelelő osztályozásában.

Tudjon meg többet a [Grayteq Classifierről](#)

Grayteq Classifier for Office

A felhasználók bevonása a strukturálatlan adatok kontextusának és tartalmának azonosításába elengedhetetlen a valódi üzleti érték feltárásához és a szervezetben lévő adatok holisztikusabb képének feltárásához. Közvetlenül a Microsoft Office termékekbe beépülve a Grayteq Classifier intelligens módon irányítja a felhasználókat az adatok megfelelő üzleti címkékkel történő osztályozására a felhasználók által értett nyelven, majd előre formázható vizuális és metaadat-jelöléseket alkalmaz a dokumentumokon.

Tudjon meg többet a [Grayteq Classifier for Office-ről](#)

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.

Lépjön kapcsolatba velünk

grayteq.com/contact

Think different

Do different

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.

Az Ön Grayteq Partnere: