Grayteq

Host Intrusion Prevention

Átfogó védelem az engedélyezetlen kapcsolódások ellen.

A Grayteq DLP Host Intrusion Prevention (HIP) az iparágban egyedülálló, jogvédett, következő generációs behatolás érzékelő és megelőző funkció, mely felismeri és blokkolja az engedély nélküli behatolási és tallózási kísérleteket a Grayteq-védett hálózatban. Fejlett kérdés-válasz alapú értékelő és authorizáló technológiája használatával, messze meghaladja az egyszerű, mintavételes védelmi rendszereket, 100%-os hatékonyságot biztosítva. Az integrált Grayteq Security Solutions portfólió leegyszerűsíti az adatbiztonsági eljárásokat, míg a végpontokon telepített Grayteq DLP Agentek a valós idejű felismerés-elemzés-döntés-cselekvés négyesével védik a felhasználókat, eszközöket, fájlokat és alkalmazásokat a támadásokra adott gyors és pontos válaszokkal.

Védelem a legrejtettebb fenyegetésekkel szemben

A digitalizáció drámaian megváltoztatt az üzlet képét szinte minden területen. Csakúgy az biztonság terén. távoli elérés, VPN, felhő, mobilok és Iot mind új szinten hozott a "határok nélküli" kapcsolódások védelme szintjén. A kockázatok mennyisége és súlyossága egyik napról a másikra ugrásszerűen megnőtt. A cégek fókusza az erős hálózati védelem révén megvalósuló adatvédelem felé tolódott el. Minden hálózatnak szembe kell néznie a legrejtettebb fenyegetésekkel, melyek csak a legfejlettebb felismerő megoldások révén állíthatók meg. Azonban a szervezetek egy részénél hiányzik a pénzügyi erőforrás vagy a szervezeti érettség komplex védelmi rendszerek implementálására és használatára melyek révén megfelelő védelmet élvezhetnének. A Grayteq DLP HIP ezt próbálja oly módon enyhíteni, hogy csökkenti az It vállára nehezedő nyomást egy fejlett, felhasználó-transzparens, központilag menedzselt és bizonyítottan működő behatolás megelőzést biztosít. Egyetlen más behatolás-megelőző rendszer sem képes az engedélyezetlen behatolások és tallózások olyan hatékonyságú megelőzésére, melyet a Grayteq DLP HIP kérdés-válasz rendszerű authentikációja valósít meg.

Grayteq DLP Funkciók

- DLP Monitor
- Rights Management
- Data Quarantine
- Application Management
- **Endpoint Protection**
- Encryption for DLP
- **Host Intrusion Prevention**
- Report & Audit

Fő Előnyök

Detektálás

- Az engedélyezetlen csatlakozási kísérletek hatékony detektálása és blokkolása.

Hatásfok

- Magas hatásfokú, skálázható megoldás a dinakimusan változó környezetekhez.

Átfedő vagy elkülönülő

- Elkülönülő, átfedő vagy kombinált védelmi zónák alakíthatók ki eltérő HIP Azonosítókkal a különböző bejövő kapcsolati kérések különböző kezelésére.

Központi menedzsment

- Központosított kezelés az átláthatóság és a kontroll érdekében.

Monitorozás és Elérhetőség

- Naplózás, riasztás és monitorozás valamennyi bejövő kapcsolati kérésre a hálózati forgalom ellenőrzése érdekében Magas elérhetőség és katasztrófa-elhárítási védettség.

Integráció

- A HIP teljeskörűen integrált valamennyi további Grayteq DLP funkcióval.

Grayteq

Valós idejű detektálás és riasztás

A végpontokra telepített Grayteq DLP Agentek révén a Host Intrusion Prevention valós időben végzi a kapcsolódási kísérletek detektálását és egyedi és hamisíthatatlan kódot küld a "hívó" gép számára, mely csatlakozását a megfelelő válasz kód megérkeztéig várakoztatja. Ezen válasz kódot csak a hívó gép Grayteq DLP Agentje képes létrehozni, így a Grayteq DLP nélküli gépek eleve nem képesek csatlakozni a védett környezethez, így biztosítva, hogy védett adat ne kerülhessen továbbításra védetlen gépekre és hogy engedélyezetlen tallózás se történhessen a védett hálózat gépein. Miközben a Grayteq DLP Agentek blokkolják a bejövő kapcsolatot, egy bizonyító erejű napló és riasztás készül a kísérletről, mely valós időben továbbításra került a biztonsági adminisztrátorok felé, ezzel téve lehetővé az azonnali beavatkozásukat.

Láthatóság és Kezelés

A bejövő kapcsolati kérések megfelelő elbírálása létfontosságú kérdés. A Grayteq DLP kombinálja a HIP detektálás és megelőzés funkcióját az alkalmazás és fájl kezelés valamint a tevékenység monitorozó biztonsági döntéshozó motort, mely kapcsolatba hozza a fenyegetést jelentő tevékenységet az adott alkalmazás használatával, lehetővé teszi az IT biztonsági adminisztrátorok számára az eszköz és alkalmazás engedélyezés megfelelő kezelését. Az eszköz és alkalmazás beazonosításon felül a Grayteq DLP HIP felhasználói és eszköz rendszerezést is megvalósít, priorizálva a veszélyes gépeket és felhasználókat.

Teljesítmény és Elérhetőség

A Grayteq DLP a beépített Host Intrusion Prevention technológiája mindkét világból a legjobbat ötvözi - biztonságot és nagy teljesítményt. Kombinálja az egyszeri, kérdés-válasz alapú védelmi architektúrát egy erre a célra kifejlesztett végponti szoftver ügynökkel a legmagasabb szintű felismerési rátával és szó szerint kimutathatalanul alacsony performacia-igénnyel. A HIP egyszerű és hatékony architektúrája fenntartja a céges IT rendszer működési sebességét és hatékonyságát elkerülve, hogy a behatolás-megelőzés legyen az IT rendszer szűk keresztmetszete adatátviteli szempontból.

Központosított kezelés a Grayteq SO használatával

A Grayteq DLP központi, menedzsment szoftvere, a Security Orchestrator (SO) egyesíti és központosítja valamennyi behatolás megelőzés kezelését. Ezen menedzsment platform integrálja a Grayteq DLP Host Intrusion Prevention funkciót a többi Grayteq DLP védelmi komponenssel és funkcióval.

A következő lépés

További információkért látogasson el a https://www.grayteq.com/hu-hu/dlp/hip.aspx 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 8.1
- Windows 10
- Windows 11

Server operációs rendszerek

- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

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.

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

Home
www.grayteq.com/hu-hu

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

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

Encryption for DLP
www.grayteq.com/hu-hu/encryptions

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

Prices
www.grayteq.com/hu-hu/prices

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

Az Ön Grayteq Partnere: