Adatbiztonsági megoldások

A Micro Focus® adatbiztonsági megoldásai fejlett, formátumtartó titkosítást, biztonságos állapottartó tokenizálást és állapottartó kulcskezelést biztosítanak a nagyvállalati adatok, az adatfeldolgozó infrastruktúra, a hibrid IT/felhő, a fizetési ökoszisztémák, a kritikus rendszerek, a tárolók, valamint a Big Data/IoT-platformok védelméhez.

- **Főbb megoldások:**
  - Big Data biztonság
  - A nagy megfelelési költség csökkentése
  - A felhőben használt szolgáltatások védelme
  - Biztonságos nagyvállalati üzenetküldés
- **Képességek:**
  - Formátumtartó titkosítás
  - Biztonságos állapottartó tokenizálás
  - Állapottartó kulcskezelés
- **Támogatott folyamatok:**
  - Az adatok anonimizálásával semlegesíti a biztonsági incidensek hatását
  - Jól használható, de mégis védett adatokat bocsát az alkalmazások és az analitika rendelkezésére
  - Teljes körű lefedettséggel kiterjeszti az adatbiztonságot a régi rendszerekről a hibrid IT-re

A Micro Focus Data Security titkosítási és tokenizáló megoldásai ösztönzik a biztonsággal kapcsolatos innovációt az adatközpontban. A kényes adatok anonimizálásával segítséget nyújtunk a világ vezető cégeinek a biztonsági incidensek hatásának semlegesítéséhez a tárolt, a mozgásban és a használatban lévő adatoknál. A Data Security a komplex régi és modern IT adatvédelmének egyszerűsítésével megoldja az iparág előtt álló legnagyobb kihívást.

Megoldások

Skálázható Big Data biztonság

A Hyper FPE funkció nagy teljesítménnyel védi az adatközpontokba irányuló adatáramlást, lehetővé teszi az analitikai elemzések készítését, miközben az adatok nem rendeltetésszerű felhasználásának és az incidensek felmerülésének kockázatát is mérsékli. Így szélesebb körű hozzáférés biztosítható a vállalatvezetők és az operatív csapatok számára a biztonságosabb, anonimizált adatokhoz. Anélkül gyorsul az értékteremtés és az IT optimalizálása, hogy megnövekedne a nagyobb adatvolumennel járó kockázat.

A nagy megfelelési költség csökkentése

Az adatok pszeudonimizálása és anonimizálása a GDPR és más szabályok előírásainak megfelelő, kipróbált, szabványos módszerekkel történik. A formátumtartó titkosítás és a „hash" használata nem zavarja az alkalmazások és a folyamatok futását, és egyszerre fedi le a régebbi és a hibrid IT-t. A biztonságos állapottartó tokenizálásnak köszönhetően szűkíthető az auditok hatásköre, és könnyebben megvalósítható a piacvezető bankok, kiskereskedelmi vállalatok és fizetésfeldolgozók számára kötelező PCI DSS előírás teljesítése.

A felhőben futtatott szolgáltatások védelme

A SecureData teljes körű adatbiztonságot nyújt a felhős alkalmazásokhoz, és egyúttal a hibrid IT támogatás révén a régebbi helyben telepített rendszereket is lefedi – egy következetes, egységes rendszerrel. A SecureData platformsemleges szemlélettel támogatja az IT-rendszerek határokon átívelő bevezetését, a SecureData Sentry által biztosított állapottartó infrastruktúra és átlátható átjárók segítségével.

Biztonságos nagyvállalati üzenetküldés

Végponttól végpontig terjedő titkosítás asztali gépes, mobil- és felhőalkalmazásokhoz, akár több millió felhasználó számára, a kényes adatok védelmével (PII, ePHI stb.) A biztonságos kommunikáció révén a szervezetek magabiztosan teljesíthetik adatvédelmi kötelezettségeiket, és mérsékelhetik az adatvesztéssel, bírságokkal és helyreállítással járó visszaélések és adatvédelmi incidensek kockázatát.

Termékek

Voltage SecureData Enterprise

Végponttól végpontig terjedő védelem a teljes körű adatközponti biztonság érdekében a Hyper FPE és a tokenizálás alkalmazásával, az adatkezelési incidensek hatásának semlegesítésére az adatok létrehozásától kezdve a teljes adatéletciklusban (a használatban és mozgásban lévő, illetve a tárolt adatoknál).

- Jól skálázható tranzakciós teljesítményt biztosít a biztonságos adatbeviteli, -feldolgozó, -tároló és egyéb megoldásokhoz.
- Megfelel a hatókörcsökkentésre vonatkozó hatósági megfelelőségi követelményeknek, miközben a megvalósítás és az üzemeltetés költségeit is csökkenti.
- A régi és a modern környezeteket egyaránt kezelő hibrid IT-megoldásokat is lefedi, és gördülékenyen kiterjeszthető új alkalmazásokra.

Voltage SecureData Payments

Point to point titkosítás (P2PE) és tokenizálás a PCI-megfelelés és a biztonságos fizetés érdekében, a POS-adatrögzítéstől kezdve a kártyafeldolgozásig.

- Végponttól végpontig védi a tárolt és mozgásban lévő hitelkártya-adatokat a digitális fizetési ökoszisztémában.
- A kritikus üzleti folyamatok és workflowk megváltoztatása nélkül mérsékli a PCI-hatókört.
- Teljes körű point to point titkosítást (P2PE) és tokenizálást biztosít a kiskereskedelmi fizetési tranzakciókhoz.

Voltage SecureData for Hadoop and IoT

Lehetővé teszi a Hadoop és IoT alkalmazásoknál (Kylo, Apache NiFi) használt kényes adatok védelmét.

- Védi az adatokat a hálózat peremén az adattavakba és -tárházakba való biztonságos, nagy tömegű bevitelhez.
- Anonimizálja az adatokat miközben fenntartja használhatóságukat a Big Data és az analitikai alkalmazásoknál.
- Konkrét adatmezőkre, alkalmazásokra és felhasználókra korlátozza az elérhetőséget a kockázatok mérséklése és az incidensek hatásának semlegesítése érdekében.

Voltage SecureData Cloud

Felhőnatív módszer az alkalmazások által használt adatok védelméhez, következetes átállással a régi rendszerekről a hibrid IT-re.

- Bevezeti az adatvédelmet a felhőben a felhő alapú szolgáltatások biztonságának gyorsabb megteremtéséhez.
- A kulcsok adathelytől független, platformsemleges felügyeletével támogatja a hibrid (felhők közötti) felhőanalitikát.
- Átlátható átjárókkal a teljes hibrid IT-t lefedi az egységes felügyeleti szemlélet megvalósításához.

Voltage SecureData Sentry

Átlátható titkosítás fejlett CASB-szemlélettel, a biztonsági megoldások bevezetésének egyszerűsítésére és gyorsabb használatba vételére.

- Átlátható módszer a régi környezetekben fellépő zavarok és kockázatok minimumra szorítására.
- Az API-hoz képest gyorsabban megvalósítja az alkalmazásbiztonságot, sokféle alkalmazás esetében egyszerűsítve ezzel a fejlesztést.
- Kiterjeszti a használati forgatókönyvek következő generációs CASB-támogatását többek között az alábbi környezetekre: SaaS/felhő, nagyvállalat, COTS, régi rendszerek.

A hálózat peremének védelme a SecureData segítségével

A Voltage SecureData Mobile védi az eszközök végpontjain rögzített adatokat, a Voltage SecureData Web pedig a Voltage Page Integrated Encryption (PIE) használatával védi a böngészők felől érkező kényes adatokat.

- Többcsatornás védelmet és egységes biztonságot nyújt a különböző digitális fizetési rendszerek e-kereskedelmi alkalmazásaihoz
- Segít a kereskedőknek csökkenteni a PCI DSS hatókörét a mobil és webes végponti tranzakcióknál
- Az iOS- és Android-alkalmazásokhoz egyszerű natív könyvtárakat használva gyorsítja a fejlesztést

Voltage SecureMail

Globális nagyvállalati levéltitkosítás dolgozók és mobilfelhasználók számára, az ügyfelekre és a partnerekre is kiterjesztve.

- Egységes szemléletet valósít meg az asztali számítógépekről, a felhőn keresztül a mobil eszközökről küldött e-mailek és mellékletek védelme terén
- Állapottartó kulcskezeléssel, szabványos személyazonosság-alapú titkosítás (IBE) mellett skálázható
- Lehetővé teszi a rugalmas hibrid IT megvalósítását a helyszínen vagy SaaS-megoldásokon keresztül a felhőben

Kapcsolatfelvétel:
www.microfocus.com

További információ:
https://software.microfocus.com/software/data-security-encryption