



A megfelelő adattörlési megoldás kiválasztása

használt adathordozók,
merevlemezek, mobiltelefonok
és logikai adattárolók fertőtlenítéséhez

www.blancco.hu

A Blanco termékeit Magyarországon
a V-Detect Antivírus Kft. képviseli,
amely viszonteladói segítségével
szolgálja ki a végfelhasználókat.

Bevezetés

Legyen szó akár szerverekről, munkaállomásokról vagy mobiltelefonokról, a vállalatok IT eszközei időről időre elavulnak és lecserélésre kerülnek. Az ezredfordulóig a mágneses adathordozók (HDD) jelentették az elsődleges tárolási megoldást, és a fizikai megsemmisítésük volt az elsődleges módszer a leselejtezésükre. Ez mára megváltozott, és a szoftveres fertőtlenítés, vagy másképpen: a minősített adattörlés került előtérbe.

A gyorsabb, megbízható SSD meghajtók elterjedésével az adattörlési és megsemmisítési eljárások is megváltoztak. Sok esetben a korábbi eljárások nem voltak megfelelőek: a fizikai darabolás például nem bontotta elég kis részekre a meghajtókat, így akár egész adattárolási egységek maradtak sértetlenek. A demagnetizálás (degaussing) egyszerűen nem működik az SSD technológia esetében.

Emellett folyamatosan szaporodnak az adatvédelmi szabályok és előírások, szigorodnak a szabványok, és mára elengedhetlenné vált, hogy minden egyes fertőtlenítésről és fertőtlenített adathordozóról egyedi törlési jegyzőkönyv kerüljön kiállításra. A jegyzőkönyvezés Magyarországon is kötelező mind az EU GDPR, mind a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) vonatkozó iránymutatása alapján.

A törlési jegyzőkönyvek hiányát és az adattörlés elmulasztását a hatóságok büntetik, de ennél fontosabb, hogy elemi érdeke minden vállalatnak, hogy ne veszítsen el üzleti titkokat és megakadályozza az adatvédelmi incidenseket.

Mára a vezető vállalatok felismerték az adattörlés fontosságát, és tudják, hogy az adathordozók fertőtlenítését megbízható, ellenőrizhető és auditálható módszerrel kell elvégezniük.

Mindez olyan szoftveres adattörlési megoldás alkalmazását jelenti, amely alkalmas mind a mágneses, mind a flashalapú adathordozók fertőtlenítésére, és az adattörlés folyamatát visszaellenőrzi (verifikálja), majd részletes, lehetőleg a hamisítás ellen védett jegyzőkönyvvel is tanúsítja.

A vállalatoknak azonban körültekintően kell eljárniuk az adattörlési megoldásuk beszerzése során: hasonlóan hangzó eljárások nagymértékben különböző eredményekhez vezethetnek. Használja ezt az útmutatót ahhoz, hogy:

- ✓ Megértse, hogy mi teszi az egyes adattörlési megoldásokat teljessé és a szabályozásnak megfelelővé.
- ✓ Megértse a hatékony, innovatív eljárások előnyeit a mai informatikai környezetekben.
- ✓ Tisztába kerüljön a verifikálás és a jegyzőkönyvezés fontosságával.
- ✓ Tudja, hogy milyen kérdéseket tegyen fel, amikor adattörlésre kap ajánlatot.
- ✓ A megfelelő megoldás kiválasztásával megfeleljen a jogszabályoknak és hatósági előírásoknak, és elkerülje a büntetéseket.

Adathordozók fertőtlenítése, az adatok törlése vagy titkosítás?

Amikor egy adat vagy egy adathordozó életciklusa véget ér, az adatot olyan módon kell megsemmisíteni, hogy az soha többé ne legyen hozzáférhető.

Közismert tény, hogy az adatok egyszerű törlése valójában nem teszi elérhetetlenné az adatokat, azok egyszerű módszerekkel visszaállíthatóak. Hiba azonban az is, ha a titkosítást egyenértékűnek tekintjük az adathordozó fertőtlenítésével. Az adathordozók titkosítása jó módszer a biztonság növelésére, de a titkosítás idővel feloldhatóvá válhat, például ha a titkosításra használt eljárásban sérülékenységet fedeznek fel, márpedig ez időről időre megtörténik.

Az adathordozók fertőtlenítése ezzel szemben olyan fizikai vagy szoftveres eljárást jelent, amely garantálja, hogy az adatok soha, semmilyen módszerrel nem állíthatók vissza.

Szoftveres módszer esetében ez a megfelelő adattörlési algoritmus alkalmazásával az adathordozó teljes területének az egyszeres vagy többszörös felülírását jelenti, mégpedig úgy, hogy az adattörlésre használt szoftver az adathordozó teljes területére rálát, beleértve az elmaszkolt, elrejtett területeket is.

Az adathordozók szoftveres fertőtlenítése – a teljes felülírásnak köszönhetően – időt vesz igénybe, ezért egyáltalán nem mindegy, hogy az alkalmazott megoldás milyen mértékben képes a törlések párhuzamosítására és az adminisztrációs teher csökkentésére, és mennyire egyszerűen kezelhető.

A minősített adattörlés meghatározása

Az adathordozók fertőtlenítése olyan szoftveres eljárást jelent, amelynek során a szoftver egyesekkel és nullákkal felülírja az adathordozó felületét, és ennek köszönhetően az eredeti adat visszaállíthatatlanná válik.

A megfelelő adattörléshez az alábbi három követelménynek mindenképpen teljesülnie kell. A szoftver:

Ha ezek közül a komponensek közül akár csak egy is hiányzik, az adathordozó fertőtlenítése NEM történt megfelelően.

- ✓ engedje meg a kívánt törlési algoritmus használatát,
- ✓ ellenőrizze, verifikálja az adatok törlését a különböző szektorok visszaellenőrzésével,
- ✓ állítson elő egy hamisítás ellen védett jegyzőkönyvet, amely azonosítja a törölt adathordozót, a használt adattörlési eljárást és az adattörlés eredményét is.

Ha a fenti követelmények nem teljesülnek, fennáll az adatszivárgás veszélye, és a hatósági büntetésektől is tartania kell a vállalatnak.

FONTOS, hogy néhány adattörlési megoldás nem támogatja az olyan rejtett területek felülírását, mint a host protected area (HPA) és a device configuration overlay (DCO), amelyet az operációs rendszer vagy a merevlemez gyártója maszkol el a lemezen.

Ezért az egyik legmegbízhatóbb módszer, ha megvizsgáljuk, hogy az adott adattörlési megoldás milyen külső minősítésekkel és ajánlásokkal rendelkezik. Amennyiben a megoldást több nemzeti hatóság, biztonsági felügyelet minősítette, és rendelkezik olyan ajánlásokkal, mint a NATO vagy a Common Criteria, úgy biztosak lehetünk abban, hogy az adott megoldás teljesíteni fogja az adattörlés feladatát. Ezalatt más, hasonlóan hangzó, de nem minősített megoldások használata veszélynek teheti ki a vállalatot.

Nem megfelelő adattörlési eljárások

Gyakori, hogy a vállalatok nem megfelelő adattörlési eljárást használnak, amely után az adatok egyszerű vagy laboratóriumi eljárással visszaállíthatóak maradnak.

Az alábbi eljárások nem felelnek meg a technikai követelményeknek és a hatósági előírásoknak:

- ✗ **Törlés** – egyszerűen elégtelen eljárás, még a nem érzékeny adatok esetében is. Az operációs rendszeren belül végzett törlés csak az adatokra mutató „tartalomjegyzéket” törli, de magukat az adatokat nem. Azok könnyen visszaállíthatóak maradnak, még nem hozzáértő felhasználók számára is.
- ✗ **Wiping** – a nem teljes felülírás megsemmisíti a felülírt adatokat, de érintetlenül hagyja a merevlemez vagy SSD meghajtó rejtett területein tárolt adatokat. Az SSD meghajtók BIOS freeze lock védelmi mechanizmusa meggátolhatja néhány firmware-alapú eljárás sikeres lefutását, és így a törlés meghiúsul.
- ✗ **Újraformázás** – a formázás (teljes formázás, deep format) szintén kérdéses eljárás. Néhány gyártó a deep format eljárásra tévesen törlési eljárásként hivatkozik. A valóságban a formázással nem jár visszaigazolás, törlési jegyzőkönyv, és így nem lehet meggyőződni arról, hogy a kezelő a gyorsformázását vagy a teljes formázását választotta ki. A Windows formázási eljárása nem biztos, hogy helyesen detektálja a merevlemez méretét (HPA és DCO területeket), ezért nem írja felül a lemez teljes területét teljes formázás esetében sem.

✗ **Titkosítás** – a titkosítás jellemzően egy titkosítási kulcs birtokában oldható fel. A cryptographic erasure (crypto erase) eljárás csak a titkosításhoz használt kulcsot törli, és így meggátolja az adatok visszanyerését, mialatt magukat az adatokat ott hagyja a merevlemezben. Ez növeli a biztonságot, főként azon adathordozók esetében, amelyeket magasabb biztonsági protokoll szerint kell kezelni. A titkosítással kapcsolatban azonban implementálási problémák merülhetnek fel, főként egy SED (self-encrypting disk) esetében. A titkosításra használt algoritmusok ezenkívül idővel gyengülhetnek, a titkosításhoz használt kulcsok helytelen kezelése pedig további sérülékenységet rejt magában. Az is jellemző, hogy a különböző titkosítási eljárásokkal kapcsolatban időről időre sérülékenységek válnak ismertté. Az eljárás emellett nem felel meg a jegyzőkönyvezés jogszabályi kötelezettségének, hiszen nem áll elő törlési jegyzőkönyv. A titkosításhoz képest a minősített adattörlés további biztonságot nyújt a szervezetek számára.

✗ **Töredezettségmentesítés** – noha nem tipikus eljárás, a töredezettségmentesítésre néha úgy gondolnak a vállalatok, mint amely alkalmas a törölt adatok végleges megsemmisítésére. Az eljárást azonban nem erre tervezték, és ugyan alkalmas az adatok újrendezésére, de nem a törlésre.

A fenti eljárások egyike sem felel meg a minősített adattörlés összes követelményének, ezért rendkívül fontos, hogy egész pontosan megismerjük, hogy a kiválasztott módszer vagy beszállító milyen eljárást alkalmaz az adatok törlésére.



Megfelelni az adattörlés területén jelentkező kihívásoknak

Megfelelő megoldás:

- ✓ Zökkenőmentesen illeszthető a meglévő informatikai környezethez
- ✓ Lokálisan vagy a hálózaton keresztül használható
- ✓ Párhuzamosan tud törölni több HDD és SSD lemezről
- ✓ Képes a különböző meghajtók széles körű kezelésére
- ✓ Képes a különböző biztonsági szabványok és törlési algoritmusok kezelésére
- ✓ Lehetővé teszi a folyamatok automatizálását
- ✓ 100 százalékban a hamisítás ellen védett jegyzőkönyveket generál

A vállalatoknak hatékony, rugalmas megoldásokra van szükségük

A vállalatok egyre több adatot tárolnak az adathordozók egyre szélesebb körén. A kis méretű adathordozók – például memóriakártyák és mobiltelefonok – kapacitása folyamatosan növekszik, az adatközpontokban pedig lemezek ezrei szolgálnak.

Az adattörlések érvényesítése ebben a környezetben megterhelő lehet, ha az adattörlések nem egy egységes rendszerben kerülnek megvalósításra és nyilvántartásra. Ezzel együtt a biztonságra törekvő vállalatok nem engedhetik meg, hogy akár egyetlen adathordozót fertőtlenítés nélkül selejtezzenek le.

A felméréseink azt mutatják, hogy a vállalatok jelentős része tárol adathordozókat anélkül, hogy azokat fertőtlenítette volna a korábban rajtuk tárolt adatoktól. Ezek egyaránt tartalmazhatnak üzleti adatokat, de a munkavállalók és üzleti partnerek személyes adatait is.

Az egyik indoka annak, hogy az adathordozók nem kerülnek időben fertőtlenítésre, az, hogy a vállalatnál bevezetett adattörlési megoldás nem képes rugalmasan és nagy volumenben kezelni az adathordozók leselejtezését. A biztonság fenntartásához ezért rugalmas és könnyen használható adattörlési megoldásra van szükség. Idetartozik a jogosultságkezeléstől a távoli törlést lehetővé tevő hálózatos felépítésig sok minden, és nem utolsósorban az is, hogy a kiválasztott megoldás az adathordozók lehető legszélesebb körét kezelje a memóriakártyáktól kezdve az SSD, PCIe és NVMe meghajtókon keresztül a mobiltelefonokig és tabletekig, de ideértve a logikai egységek törlését, a fájlok és mappák törlését, valamint a virtuális környezetek támogatását is.

A kiválasztott megoldás emellett működjön annyira automatikusan, amennyire ez csak lehetséges, beleértve a BIOS Freeze Lock eltávolítását, a RAID tömbök kezelését, az automatikus adattörlést, valamint a hamisítás ellen védett törlési jegyzőkönyv automatikus beküldését a központi nyilvántartási rendszerbe.

A vállalkozásoknak innovatív megoldásokra van szükségük

A felhőalapú technológiák, az 5G hálózatok és a folyamatos technikai fejlődés megváltoztatja az adatok tárolásának módját. Az önmagukat titkosító meghajtók, a gyártóspecifikus biztonsági fejlesztések és a felülírási követelmények kihívást jelentenek az adatok törlésében. A kiválasztott megoldás gyártójának tapasztalattal kell rendelkeznie ezeken a területeken.



A következő években:

- ✓ Az adathordozók gyártói várhatóan további védelmi technológiákat vezetnek be, amelyek megnehezíthetik az adatok törlését.
- ✓ A hatóságok emelni fogják az adatvédelmi incidensekhez kapcsolódó bírságok mértékét.
- ✓ Az IT-csapatoknak egyre gyorsabban és rugalmasabban kell reagálniuk az üzleti igényekre.

A fenti okok miatt a jó döntés, ha az adatok törlésére olyan megoldást választunk, amelynek gyártója lépést tart a fejlődéssel, követi a jogszabályok és a technológiai sztenderdek változását, emellett jelentős pénzügyi és emberi erőforrást fordít a kutatásra és fejlesztésre, hogy az adathordozók gyártóinak fejlesztéseire a megfelelő technológiai válaszokat tudja adni.

A felügyeleti lánc sérülékenységei

A felügyeleti lánc sérülékenységeiből fakadó adatvédelmi incidensek kivédésére az egyik legjobb módszer, ha olyan adattörlési megoldást választunk, amely a vállalat telephelyein, helyben kerül megvalósításra. Az adattörlési megoldást beépíthetjük a mindennapos munkafolyamatokba is. A helyi adattörlések megvalósításával a vállalat elkerülheti a szállítás során bekövetkező adatvédelmi incidenseket, és azokat is, amelyek az alvállalkozó esetleges hanyagságából erednek.

Kedvező gyakorlatot jelent, ha az adatokat tartalmazó adathordozókat még helyben sem tároljuk hetekig, hónapokig vagy évekig, mert ez ismét lehetőséget ad a hibázásra. A legbiztosabb módszer a helyben, azonnal megtörténő adattörlés.

Az adattörlés felgyorsításával csökkentjük a hanyagságból vagy lopásból, illetéktelen hozzáférésből eredő adatvédelmi incidenseket, azokat is, amelyeket belső ügynök követne el.

Ha külső vállalkozást szeretnénk megbízni az adattörlésekkel, akkor győződjünk meg arról, hogy a teljes folyamat minden lépése megfelelően biztosítva van, a szállítástól az adattörlésben részt vevő munkavállalók feddhetetlenségéig. Emellett követeljük meg az adattörlések elvégzésének egyértelmű bizonyítékát, a törlési jegyzőkönyvet.

Mire terjedjen ki a törlési jegyzőkönyv

A fertőtlenítés eredményét részletesen jegyzőkönyvben kell rögzíteni minden egyes adathordozó esetében, amely fertőtlenítésre kerül. Ez a jegyzőkönyv lehet nyomtatott vagy elektronikus, de ellenőrizhetőnek kell lennie annak, hogy a jegyzőkönyvben foglalt adatokat senki sem változtatta meg.

A megfelelő törlési jegyzőkönyv tartalmazza:

- ✓ Az adathordozó fizikai azonosítóit (sorozatszámát, IMEI számát)
- ✓ Az adattörlési eljárás típusát (és algoritmusát)
- ✓ Az adattörlési eljárás eredményét és idejét
- ✓ Az adathordozó méretét
- ✓ Az adattörlést végző szervezet és személy megnevezését
- ✓ Az adattörlés egyéb azonosítóit (például projektszám)
- ✓ A jegyzőkönyv védelmét szolgáló digitális aláírást vagy más hitelesítési módszert

A jegyzőkönyveket visszakereshető módon kell tárolni, és hatósági ellenőrzés során bemutatni.

A legjobb mód az adattörlések biztonságának növelésére, ha olyan szoftveres megoldást választunk, amelyet számos kormányzati biztonsági szervezet és külső minősítő laboratórium tesztelt.

A minősítéssel nem rendelkező adattörlési megoldások bár sokszor ugyanolyannak tűnnek, mégis veszélynek teszik ki a vállalatokat.

Milyen kérdéseket tegyünk fel, amikor beszállítót választunk?

Hatékony fertőtlenítés, robusztus kapacitás, auditálható dokumentáció. Ha a vállalatnak adattörlési megoldásra van szüksége, egy megbízható és minősített gyártótól beszerzett megoldás biztosítja a hatósági előírásoknak történő megfelelést és a kellő biztonságot.

**A következő kérdőívet használhatja a beszállító
alkalmasságának megítélésére!**

Általános adattörlési kérdések

- ✓ Hitelesítette a gyártó megoldását több független laboratórium és nemzetvédelmi hatóság?
- ✓ A gyártó megoldása támogatja a nemzetközi adattörlési sztenderdek széles körét?
- ✓ A gyártó megoldása megfelel az iparági követelményeknek, és a segítségével megfelelhet a vállalat a hatóságok és felügyeleti szervek előírásainak?
- ✓ A gyártó megoldásával az adathordozók széles körét lehet törölni – beleértve a szervereket, adatközpontokat, laptopokat, SSD meghajtókat, mobiltelefonokat, tableteket, USB kulcsokat és memóriakártyákat?
- ✓ A gyártó hatékony megoldást kínál, amely párhuzamosan valósítja meg több merevlemez, mobiltelefon és memóriakártya törlését?
- ✓ Támogatja a gyártó a merevlemezek széles körét (SATA, SCSI, SAS, USB, PCIe, NVMe), beleértve az önmagukat titkosító meghajtókat?
- ✓ Ellenőrzi és eltávolítja a gyártó a BIOS Freeze Lock mechanizmust?
- ✓ Alkalmazható a törlési megoldás a saját telephelyen, vagy van olyan megbízható felelősségi lánc, amely lehetővé teszi alvállalkozó alkalmazását?
- ✓ Figyelmet fordít a gyártó a kutatásra és fejlesztésre, és naprakészen tartja a megoldásait?

Adatközpont-specifikus képességek

- ✓ Képes a szoftver egyszerre több száz vagy több ezer szerver törlésére?
- ✓ Képes a szoftver a szerverek törlésére a rack szekrényekből történő kiserelés nélkül?
- ✓ Képes a szoftver tömbök megcélzására és teljes tömbök törlésére?
- ✓ Biztosít a gyártó lehetőséget a törlésre élő környezetben is?

Automatizálás és hatékonyság

- ✓ Lehet a megoldást automatizálni és távolról futtatni?
- ✓ Egyszerűen illeszthető a megoldás a meglévő informatikai környezethez?
- ✓ Támogatja a szoftver a különböző bootolási lehetőségeket?
- ✓ Képes a szoftver a false positive események azonosítására a törlés során?
- ✓ Képes a szoftver automatizálni a BIOS Freeze Lock eltávolítását?
- ✓ Képes a szoftver felismerni és kezelni a RAID tömböket?

Jegyzőkönyvezési képességek

- ✓ Biztosítja a szoftver a jegyzőkönyvek testre szabásának lehetőségét, hogy megfeleljen a speciális igényeknek?
- ✓ Védi a szoftver a jegyzőkönyveket a hamisítás ellen valamilyen elektronikus eljárással vagy aláírással?
- ✓ Biztosítja a gyártó a törlési eljárás sikerének visszaellenőrzését, valamint előállít a hamisítás ellen védett, a hatósági előírásoknak megfelelő jegyzőkönyvet?
- ✓ Biztosítja a megoldás a hozzáféréssel rendelkező szakemberek számára a jegyzőkönyvek visszakeresését, megtekintését, mentését?

Terméktámogatásra vonatkozó kérdések

- ✓ Van lehetőség oktatásra?
- ✓ Ad hozzáférést a gyártó online tudásbázishoz?
- ✓ A nagyvállalatok igényeinek megfelelő, többcsatornás terméktámogatást is nyújt a gyártó?
- ✓ Van a gyártónak nemzetközi terméktámogatási háttere?
- ✓ Tudja támogatni a gyártó a többnyelvű kommunikációt?
- ✓ Van a gyártónak technikai tréning programja?

A Blancco

Menedzselt, minősített adattörlés és diagnosztika

A Blancco a világ vezető gyártója a menedzselt, megbízható és minősített adattörlés területén. A nemzetbiztonsági szervezetek, a rendőrség, a pénzügyi szolgáltatók és a számítógép újrahasznosításával foglalkozó szervezetek első számú választása. 1997-ben alapított vállalatunk a legtöbb szakmai minősítéssel rendelkező adattörlési megoldásokat kínálja a világon.

Cégünk 14 saját irodát tart fent Európában, Észak- és Dél-Amerikában, Ázsiában és Ausztráliában. Szoftvereink és hardveres megoldásaink segítségével ügyfeink mindennap több tízezer számítógépről törlik az adatokat; a Blancco Asset Manager használatával pedig minden egyes nap több tízezer hardver- és szoftverleltárt készítenek. Mobil diagnosztikai szoftverünk lehetővé teszi a mobilkészülékek hatékony kezelését és a velük kapcsolatos problémák feltárását.

A Blancco előnyei

- ✓ Az automatizálható és irányított folyamatok segítségével a lehető leggyorsabb és legbiztonságosabb módon valósítható meg az adattörlés.
- ✓ Tanúsítható, auditálható jegyzőkönyv készül minden sikeres törlésről.
- ✓ A törölt adatok semmilyen technológiával nem állíthatók helyre.
- ✓ Csökken a szervezet jogi mulasztásának kockázata, a hírnév sérülésének veszélye, valamint a vállalat számára értéket jelentő adatok kiszivárgásának esélye.

A Blancco termékei teljes mértékben eleget tesznek a biztonsági és titoktartási előírásoknak. A Blancco adattörlési rendszere többek között NATO-, Common Criteria-, TÜV-Süd- és CESG-ajánlással vagy -minősítéssel rendelkezik. Magyarországi ügyfeink közé tartozik több nemzetvédelmi szervezet, pénzügyi intézet, gyártással foglalkozó vállalat és tanácsadó cég.

A Blancco segítségével elvégzett törléseket széles körben elfogadják a biztonsági auditok (pl. ISO 27001) során. Mivel a Blancco lehetővé teszi a leselejtezni kívánt adathordozók újraértékesítését vagy ismételt felhasználását, így lényegesen javítja az informatikai eszközök megtérülését.

A Blancco magyarországi disztribúcióját és képviselőjét a V-Detect Antivírus Kft. látja el elkötelezett viszonteladói segítségével.

További információ: blancco.hu