

# A mobilszolgáltatók és a használt mobileszközök piaca

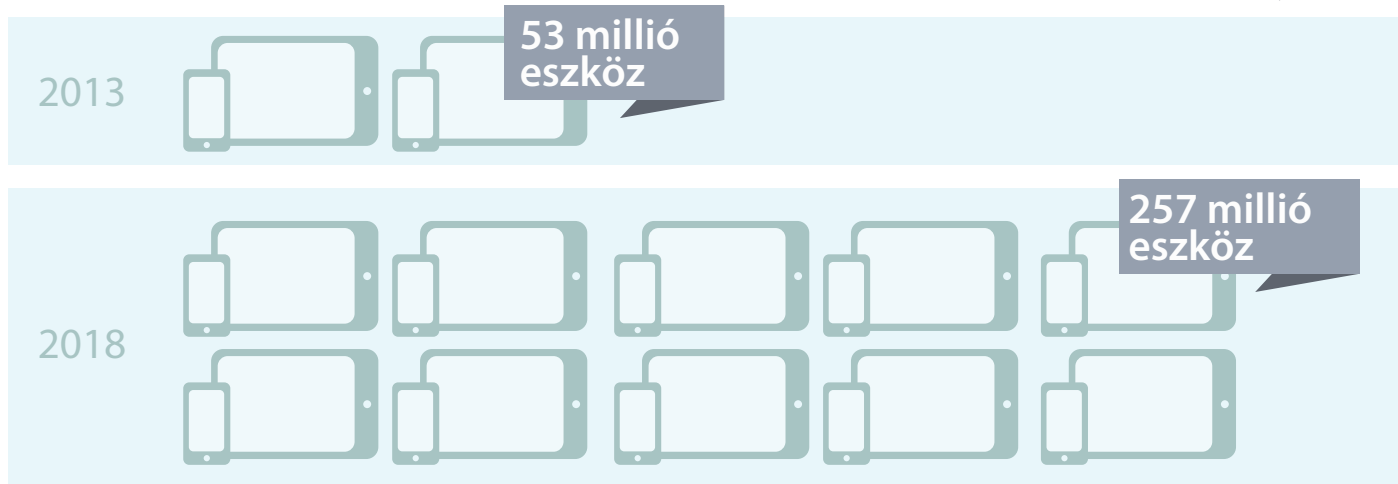


Biztonságos értékteremtés az adattörlés segítségével

# Tartalomjegyzék

<b>Bevezetés</b>	<b>3</b>
<b>A mobileszközök teljes törlésének indokai</b>	<b>4</b>
Az ügyfeladatok és a márka hírneve	4
A gyári állapot visszaállítása maradványadatokat hagyhat	5
Kis eszközök, nagy kockázat	5
Folyamatos kihívás a jogalkotás számára	5
Az üzleti élet nélkülözi az erős mobileszköz-politikát	6
<b>A hatékony adattörlési technológia felismerése</b>	<b>7</b>
A fejlett technológia választ ad a biztonsági kihívásokra	8
Termelékenységi előnyök a mobil-ökoszisztémák számára	8
<b>A fejlett adattörlés előnye a teljes mobil-ökoszisztéma számára</b>	<b>9</b>
A márka hírnevének védelme	9
Bevonzani és megtartani az ügyfeleket	9
A személyes és üzleti adatok biztonsága	9
Értékteremtés a fordított logisztikai láncolaton keresztül	9
<b>Összefoglalás</b>	<b>10</b>

## A HASZNÁLT MOBILTELEFONOK PIACÁNAK NÖVEKEDÉSE



## Bevezetés

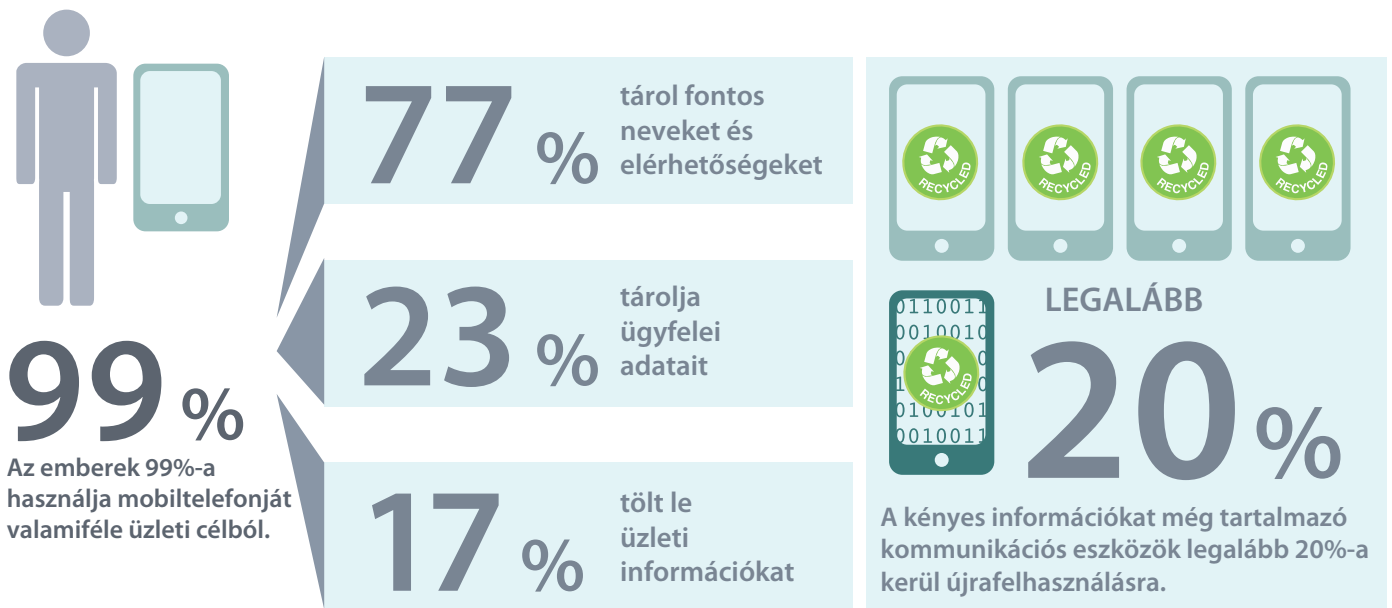
Az értéknövelt szolgáltatások számának bővítése nem az egyetlen módja annak, hogy a mobilszolgáltatók fokozatosan növeljék az egy felhasználóra eső átlagos bevételüket. A használt okostelefonok és tabletek értékesítésének előre jelzett emelkedése alapján jelentős bevételi potenciál van a korábban használt mobil eszközök újraértékesítésében.

A használt okostelefonok piaca jelentős növekedés határán áll, amelyet a „cseréld be és vásárolj vissza” típusú programok fűtenek. Az elemzők úgy becsülik, hogy a piac 53 millióról 257 millió darabra fog nőni a következő 5 évben. Becslések szerint 2018-ra a használt telefonok 8 százalékát kannibalizálják a teljes új okostelefon-értékesítéseknek, ami meg lehetőséges növekedés a 2012-es 3 százalékhoz képest.

Mivel az okostelefon-piac gyors ütemben bővül, egy új, támogatásra váró mobil-ökoszisztéma formálódik. Amíg a mobilszolgáltatók és a kiskereskedők a korábban említett programokat ajánlják, addig más partnerek azt biztosítják, hogy a telefonok készen álljanak az újraértékesítésre. A szolgáltatók megvásárolhatják a használt telefonokat a különböző mobilszolgáltatóktól, aztán eladják őket az IT eszköz megsemmisítő specialistáknak vagy mobiltelefon-újrahasznosítóknak feljavításra, ezután pedig különböző outleteken keresztül kerülnek értékesítésre.

Ezen fordított logisztikai lánc mellett nagyon jó lehetőség a mobilis ökoszisztéma szereplői számára lecsapni a használt mobil eszközökből (okostelefonok, tabletek) származó fennmaradó értékekre. Azonban megvan ennek a negatív oldala is, hiszen ha nem megfelelően végzik el a törlésüket, veszélybe kerülhet az egyre növekvő mennyiségű személyes és üzleti adat is, melyeket az ilyen eszközökön tárolnak. A mobil eszközök teljes adattörlése nélkül a mobilszolgáltatók körülbelül olyan kockázatnak teszik ki a hírnevüket, mintha egy ügyféladatokkal teli laptopot véletlenül elveszítenének.

A márkának okozott lehetséges károk mellett számos más tényező miatt is fontos a mobil eszközök törlése. Ilyen például a növekvő számú szabály és előírás, amelyek kihatnak az üzleti adatokra. Az eszközök hatékony és teljes körű törlése azonban nem azonos az egyszerű gyári visszaállítással. A hitelesített, fejlett adattörlő szoftverek olyan technológiát és jegyzőkönyvezési képességet biztosítanak, amellyel biztonságosan el lehet távolítani az összes adatot, illetve bizonyítékot is szolgáltatnak arról, hogy ez valóban meg is történt, miközben elősegítik a bevételek növekedését a mobil-ökoszisztémán keresztül.



## A mobileszközök teljes törlésének indokai

A Gartner becslése szerint 2014-ben mintegy 2,2 milliárd okostelefont és tabletet fognak leszállítani. A mobiltelefonoknak magas a fennmaradó értéke, és ez a mobilszolgáltatókat arra ösztönzi, hogy megváltoztassák a felhasználókkal kapcsolatos terveiket úgy, hogy lehetővé tegyék a gyorsabb mobiltelefon-lecserélési ciklusokat.

A technológia gyorsabb fejlődése és a fogyasztói készülék-becserélés lehetősége ugyanakkor megnöveli a mobil-eszközök életciklusát. Ezáltal nagy mennyiségű okostelefon és „adatforgalom” kerül a használt piacra, utóbbi főleg amiatt, hogy a felhasználóktól származó átlagos bevétel egyre inkább az adatforgalomból fog keletkezni a hang alapú szolgáltatások rovására. Amennyiben a mobilszolgáltatók meg akarnak jelenni a használt eszközök másodlagos piacán, illetve olyan szervizszolgáltatásokat kívánnak nyújtani, melyek nem veszélyeztetik a márka hírnevét, be kell vezetniük a teljes körű adattörlést.

### AZ ÜGYFÉLADATOK ÉS A BRAND HÍRNEVE

Az üzleti világban az adatvesztés veszélye folyamatos fejfájást okoz a vállalatok biztonsági csapatai számára. A legtöbb adatvesztés a kiskereskedelmi szektorban történik, de a mobilszolgáltatók hírnevét is csorbítják a kiberbűnözők. A tanulmányok azt mutatják, hogy az adatvesztések összköltsége 184 millió és 330 millió dollár között lehet, és az ügyfelek 15-30%-a megszüntetné a szolgáltatást, ha adatvesztésről értesülne. Az adatvesztés a jelentős pénzügyi hátrány mellett – jogi szakértők szerint – hosszabb távon a hírnévben okozná a legnagyobb kárt.

A Gartner becslése szerint 2014-ben a cégek 90%-a támogatni fogja a vállalati alkalmazásokat a személyi eszközökön, ezáltal pedig sokszorosára növekszik az adatvesztések esélye, negatív kihatással az egyénekre és cégekre is.

## A GYÁRI ÁLLAPOT VISSZAÁLLÍTÁSA MARADVÁNYADATOKAT HAGYHAT

A mobilhálózat-üzemeltetők és -szolgáltatók gyakran még mindig azt gondolják, hogy a gyári állapot visszaállítása egy okostelefonon, vagy az eszköz törlő funkciójának alkalmazása minden adatot megsemmisít a belső memóriában, azonban sok esetben ezek az adatok továbbra is léteznek. Téves az a feltételezés is, hogy a visszaállítás után maradt adatokhoz történő hozzáférés szakértőt igényel. Az androidos telefonok esetében, amelyek a globális piac több mint 79%-át teszik ki, csak egy gyors látogatást kell tenni a Youtube-ra, hogy megtudjuk, hogyan kell visszanyerni az adatokat a készülékekről a gyári állapot visszaállítása után, pusztán úgy, hogy lemezmeghajtóként érzük el a telefont egy PC-ről.

Azok, akik újraértékesítés előtt mindössze a gyári visszaállítást végzik el, hamis biztonság tudatban vannak. Egy egyesült királyságbeli felmérésben a megkérdezettek 81%-a nyilatkozott úgy, hogy letörölte a telefonját az eladás előtt, és tízből hat biztos volt benne, hogy az adatok véglegesen eltűntek. A legtöbben a gyári visszaállítást alkalmazták.

## KIS ESZKÖZÖK, NAGY KOCKÁZAT

Több számítási teljesítménnyel, mint amennyi az Apollo 11-nek volt a Holdra szálláskor, a mobil eszközök rengeteg információt képesek hordozni kis méretük ellenére, hiszen némely okostelefonnak vagy tabletnek csak a belső memóriája 64 GB adatot tud tárolni. Ehhez az adatmennyiséghez hozzáadódnak a mobil eszközök által elérhető adatok olyan felhő alapú alkalmazásokból, mint a Facebook, Outlook és egyéb vállalati alkalmazásokból, mint a Salesforce, Yammer. Ahogy ezek a memóriában bővelkedő eszközök egyre okosabbá és népszerűbbé válnak, segítve az embereket abban, hogy még produktívabbak legyenek a munkában és személyes tevékenységeikben, egyre valószínűbb, hogy e-maileket, ügyféladatokat, jelszavakat és más érzékeny információt tárolnak, amelyek azután könnyen idegenek kezébe kerülhetnek, ha teljes körű adattörlés nélkül selejtezik le őket.

Egy 2009-es felmérés azt mutatta, az emberek 99%-a különböző üzleti célú feladatokra is használja telefonját. A megkérdezettek 77%-a üzleti célú neveket és címeteket, 23%-a ügyféladatokat, 17%-a pedig letöltött vállalati információkat is tárolt telefonján.

Ahogy a mobil eszközök technológiája egyre jobban fejlődik, az adatvesztés esélye is egyre nagyobb lesz. Egy tanulmány azt mutatja, hogy az okostelefonokon és tableteken tárolt személyes és üzleti adatok megtalálják útjukat a használt piac irányába. Már egy 2008-as kutatás is úgy találta, hogy öt mobilkommunikációs eszközből egy az újrhasználó piacon még mindig tartalmazott érzékeny információt, míg más nem hivatalos felmérések szerint ez az arány 66%-tól egészen 99%-ig is terjedhet. Sok eszköz a fejlődő országokban végzi, hozzájárulva az adatbiztonsággal kapcsolatos aggodalmakhoz.

## FOLYAMATOS KIHÍVÁS A JOGALKOTÁS SZÁMÁRA

Az adatvesztéssel kapcsolatos jogszabályok és szabványok, beleértve a digitális eszközök törlési követelményeit is, folyamatosan alakulnak ki világszerte, hatást gyakorolva a mobilszolgáltatók ügyfeleire. Míg ez régióként más és más, a kialakuló trend a szigorúbb intézkedések és büntetések felé halad. A „hozd a saját eszközöd” kapcsán elszennvedett adatvesztés iparág-specifikus büntetéseket eredményezhet, mint ahogy történt azokban az esetekben is, amikor hitelkártya- és más személyes adatok kerültek nyilvánosságra, és a Payment Card Industry Data Security Standard (PCI DSS) alapján, vagy védett személyes egészségügyi információk kerültek ki, és a HIPPA alapján szabták ki a büntetéseket az Egyesült Államokban.

Európában változtatásokat javasoltak az Európai Unió 1995-ös Adatvédelmi Direktívájának adatvédelmi szabályozásában. Az EU-s tagállamok a friss javaslatok kivonatait vizsgálják, amelyek tartalmazzák az online adatok törlésének és a személyes adatokat feldolgozó cégek számára az ellenőrizhető eljárások követelményeit, továbbá buzdítást a hitelesített eszközök és eljárások használatára. Az új követelmények megszegése miatti büntetés mértéke 250 000 eurótól a teljes éves forgalom 0,5%-áig terjedhet kisebb kihágás esetén, de komolyabbaknál már 1 millió eurótól a forgalom 2%-áig is felmehet a bírság.

Az Európai Hálózati és Információ Biztonsági Ügynökség (ENISA) is felismerte, hogy az okostelefonok komplett adattörlés nélküli forgalomból kivonása jelenti a legnagyobb veszélyt az információbiztonságra, ennek ellenére ezek az eszközök nem tartoznak semmilyen kötelező törlési eljárás hatálya alá, mint amelyek a használt merevlemezekre vonatkoznak. Ez különösen problémás, tekintve, hogy évente kb. 170 millió mobiltelefon kerül újrhasználásra.

## **AZ ÜZLETI ÉLET NÉLKÜLÖZI AZ ERŐS MOBILESZKÖZ-POLITIKÁT**

Az okostelefonokról és tabletekről történő adatvesztések következményei pont olyan súlyosak lehetnek, mint ha egy szerverről vagy laptopról történne ugyanez. Ez különösen igaz akkor, ha a mobileszközt üzleti célra is használták, hiszen akár ügyfelek ezreinek az adatai is veszélybe kerülhetnek. Míg egy vállalat saját maga felelős a mobileszközökről kiszivárgott adatok miatt biztonsági és szabályozási szempontból, addig egy mobilszolgáltatónak figyelembe kell vennie, hogy egy a forgalomból nem megfelelően kivont mobileszközről történt jelentős adatvesztés negatív hatásai őt is elérhetik.

Egy tanulmány szerint a cégek mindössze 14%-a rendelkezik részletesen kidolgozott, mobileszközökre vonatkozó előírásokkal. Míg a megkérdezettek 65%-a elismerte, hogy a „hozd magaddal a saját eszközöd”-féle környezet növekvő biztonsági kockázatot jelent, majdnem 64%-uknak nincs semmilyen tervük bármilyen szigorúbb mobileszköz-szabályozást bevezetni, legtöbb esetben nyilvánvalóan ennek költségei miatt.

Betartani a biztonsági követelményeket egy olyan környezetben, ahol a költségvetés és az IT-források limitáltak, a kisebb cégek számára valódi kihívást jelenthet.



# A hatékony adattörlési technológia felismerése

A mobilszolgáltatóknak (vagy IT eszközöket megsemmisítő partnereiknek) olyan technológiát kell használniuk, amely teljes körűen megvédi az adatokat a mobileszköz becserélése, visszavásárlása során. Olyan technológiát kell alkalmazniuk, amivel a mobileszközök külső és belső memóriájából eltávolíthatóak az adatok, mielőtt újrafelhasználják, újfeldolgozzák, tárolják vagy megsemmisítik őket. Ez a SIM kártya pusztán megsemmisítésén túl magába kell, hogy foglalja a nem mindig könnyen hozzáférhető belső memória és külső memóriakártyák törlését is. Nem elég csupán a mobileszközök fizikai megsemmisítése, hiszen a töredezett digitális médiából visszaállíthatóak az adatok, és ez az eljárás a környezetet is szennyezi.

Ismert az az adateltávolítási módszer is, amikor szoftverrel teljesen felülírják az eszköz memóriáját. Ennek az eljárásnak azonban van egy fontos hiányossága: nem tud olyan elektronikus sorozatszámokkal és egyéb hardveradatokkal ellátott ellenőrizhető jelentést produkálni, amely bizonyítja, hogy az adatok eltűntek. Ez pedig szükséges az emberi

hibázás kockázatának megszüntetéséhez, az előírások betartásához és a készülék kockázatmentes újraértékesítéséhez vagy újrafelhasználáshoz. Mindemellett ez az alkalmazás csak bizonyos eszközök operációs rendszereivel működik, és manuálisan kell alkalmazni.

## A FEJLETT TECHNOLÓGIA VÁLASZT AD BIZTONSÁGI KIHÍVÁSOKRA

A minősített, fejlett adattörlés is a felülírás egyik típusa több biztonsági és technikai előnnyel. Nem csupán eltávolítja az adatokat a mobilszekőről, de részletes jelentést is szolgáltat mintegy bizonyítékként, hogy a telefon megfelelően lett kivonva a forgalomból. Fejlett funkcionalitása miatt az adattörlés számos előnyt kínál:

**Részletes riportolás** – A mobilos ökoszisztémák számára a teljes körű törlési jelentések kritikus információt szolgáltatnak az auditokhoz, újraértékesítéshez és biztonsági célokhoz, tartalmazzák a hardver állapotát, a fontos szériaszámokat és eszközcímkéket, szoftverrészeleteket a licenck begyűjtéséhez és azt, hogy hogyan és ki végezte az adattörlést. A szériaszámok összevethetőek az adatbázisokkal, hogy azonosíthatóak a lopott telefonokat. Ez a hamisítás-biztos és ellenőrizhető riportolás alapvető része a törvényi ellenőrzési követelményeknek, enélkül a mobilszolgáltatók nem képesek bizonyítani a magánszemélyeknek és cégeknek, hogy adataik teljesen biztonságban vannak.

### **Ragaszkodás a törvényekhez és szabványokhoz** –

A fejlett adattörlési technológia ragaszkodik a legszigorúbb adatfelülírási szabványokhoz, mint a HMG Infosec és a DoD 5220.22-M, amelyeket sok kormány és cég is szükségesnek tart az adateltávolításhoz. A fejlett adattörlés különböző nemzetközi szabványokhoz is világszerte hitelesítve van, olyan kereskedőktől, mint például a Blancco.

Mai napig nincs kialakítva egy közös törlési szabvány az összes okostelefonhoz és tablethez. A Nemzeti Szabvány és Technológiai Intézet (NIST) jelenleg is frissíti az útmutatóit a mobilszeközök és az SSD-k törléséhez, míg az Eszköz Megújító Fórum (DRF) egy egyedi hitelesítési eljárás dolgozik a felújított okostelefonok, „buta telefonok”, USB modemek és más vezeték nélküli eszközök teszteléséhez és hitelesítéséhez, hogy biztosítsák, azok megfelelnek a szigorú termékminőségi és teljesítménybeli szabványoknak.

A Blancco együttműködik a DRF-tagokkal, hogy hozzájáruljanak a biztonságos adattisztítási eljárásokhoz, hogy biztosíthatóak az adateltávolítást a felújított mobilszeközökről.

**Külsős jóváhagyások** – A mobilszolgáltatóknak és a mobilszeköz-újrafeldolgozóknak olyan fejlett adattörlési eszközt kell alkalmazniuk, amelyet egy nemzetközileg elismert tesztelőügynökség, mint például a TÜV SÜD is jóváhagyott.

## TERMELÉKENYSÉGI ELŐNYÖK A MOBIL-ÖKOSZISZTÉMÁK SZÁMÁRA

**Automatizált törlési eljárás** – A fejlett adattörléssel automatizálható és végrehajtható ugyanaz a törlési eljárás számtalan mobilszeköz esetében egy normál laptopról vagy asztali számítógépről. Az automatikus törlési eljárás néhány perc alatt beállítható, és lehetővé teszi egyetlen operátor számára okostelefonok százainak letörlését egy nap alatt.

A törlőszoftver automatikusan küldi a törlési jelentést egy központi konzol számára, így segítve elő az egyszerű jelentésmegosztást a mobilszolgáltatókkal.

**Széles platformtámogatás** – A hatékonysága mellett a fejlett adattörlési szoftver detektálja és egyszerre törli az adatot különböző típusú mobil- és tabletplatformokról, mert közvetlenül kommunikál az operációs rendszerükkel. Ezek az eszközök lehetnek akár iOS, Nokia Symbian, Android, Windows és Blackberry rendszerűek. Ez a rugalmasság a platformok terén különösen fontos, mivel a különböző típusú eszközök mind más és más törlési eljárást igényelnek.



# A fejlett adattörlés előnye a teljes mobil-ökoszisztéma számára

A fejlett adattörlés használatának előnyei közé tartozik, hogy az adatok teljes eltávolítása az okostelefonokról és tabletekről az ügyfélnél kezdődik, és a teljes mobil-ökoszisztémán keresztül kiterjed a logisztikai láncolatra is. A márka hírneve, biztonság, ügyféllojalítás és műveleti hatékonyság csak néhány az előnyök közül.

## A MÁRKA HÍRNEVÉNEK VÉDELME

Tekintve azt az óriási költséget, ami az ügyféladatok nem szándékolt kiszivárgásával járhat, a minősített adattörlés csak egy minimális beruházás a brand hírnevének megóvása érdekében, hatalmas biztonsági haszonnal. A mobilszolgáltatók e technológia használatával elkerülhetik azt a hamis biztonságérzetet, amit a gyári beállítások visszaállítása nyújt, ráadásul részletes, ellenőrizhető jelentést is kapnak bizonyítékul.

A biztonságos adattörléssel a mobilszolgáltatók és újrafeldolgozók biztonságosan emelhetik a márka hírnevét okostelefonok és tabletek adományozásával különböző jótékonyági célokra. Ugyanez vonatkozik arra, ha biztonságos, zöld alternatívát nyújtanak a használt mobilkészülékek forgalomból való kivonására.

## BEVONZANI ÉS MEGTARTANI AZ ÜGYFELEKET

Azok a mobilszolgáltatók, melyek minősített adattörlő szoftvert használnak, nem csupán elkerülik az adatvesztések miatti negatív publicitást, de értéknövelt megkülönböztető jegyeket nyújthatnak szolgáltatásaikhoz és visszavásárlási programjaikhoz, a pénzbeli vagy becserélési kompenzáción kívül.

## A SZEMÉLYES ÉS ÜZLETI ADATOK BIZTONSÁGA

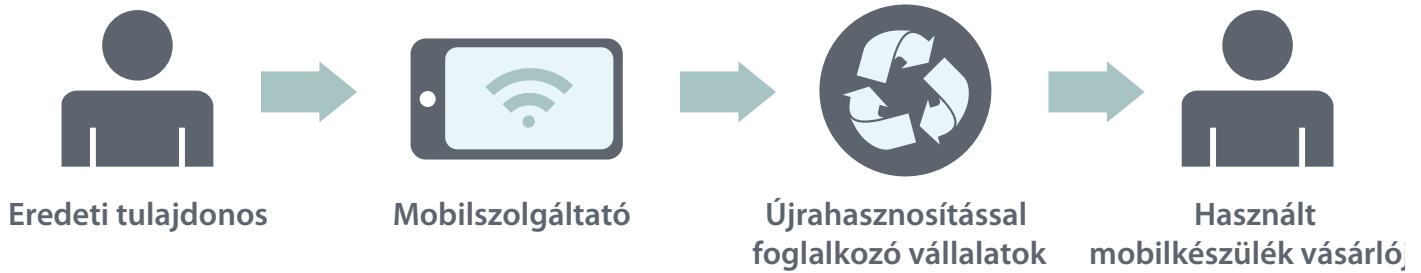
A nem megfelelően leselejtezett okostelefonok és tabletek könnyen rossz kezekbe juttathatják valakinek a teljes digitális ujjlenyomatát, nem beszélve ezernyi érzékeny ügyféladatról, ha ez egy „hozd a saját eszközödet” készülék. A fejlett adattörlő szoftver alkalmazásával a mobilszolgáltató biztonságban tarthatja a személyes fotókat, kontaktlistákat, e-maileket és a vállalati alkalmazásokból származó információkat is az ügyfelei számára.

A minősített adattörlés ragaszkodik a legszigorúbb technológiához és felülírási szabványokhoz, beleértve a részletes törlési jelentések készítését is.

## ÉRTÉKTEREMTÉS A FORDÍTOTT LOGISZTIKAI LÁNCOLATON KERESZTÜL

A mobilszolgáltatók nem az egyedüli szereplők a mobil-ökoszisztéma fordított logisztikai láncolatában, amelyek bevételre tehetnek szert a fejlett adattörlés használatából. Az egyéb szolgáltatóknak, IT eszköz megsemmisítőknak és mobiltelefon-újrahasznosítóknak szintén van erre lehetőségük. Egyrészt az értéknövelt szolgáltatások révén, teljes adattörlési szolgáltatás nyújtásával a mobilszolgáltatóknak, másrészt azzal a potenciállal, amellyel nagyobb mennyiségű mobilkészüléket képesek feldolgozni, ahogy a fogyasztók és a vállalatok egyre jobban megbarátkoznak a biztonságos okostelefon- és tabletbecseréléssel.

## ÉRTÉKTEREMTÉSI LÁNC A HASZNÁLT MOBILESZKÖZÖK PIACÁN



## Összefoglalás

A használt mobilkészülékek piacának küszöbönálló növekedése növekvő kockázatokat is rejt. Elengedhetetlen ezért egy olyan technológia használata, mely garantálja, hogy nem marad semmiféle adat a mobilkészülékeken azok újraértékelése előtt. Ezt a biztonságot nyújtja a fejlett adattörölő szoftver. A minősített adattörölés segítségével az eredeti felhasználótól és a mobilszolgáltatóktól az IT eszköz megsemmisítői és a használt eszközöket vásárló magánszemélyekig mindenki értékhez és megnövelt biztonsághoz jut.

Emellett, mivel a fejlett adattörölés automatikusan nyújt részletes törlési jelentést, több platformot is támogat és egyszerre számos eszközt képes letörölni, ez egy praktikus választás az IT eszköz megsemmisítőknél és újrahasznosítóknál, akik biztosítani akarják az adatokat az időigényes kézzelvezérelt eljárások nélkül, és fel kívánják készíteni arra, hogy megfeleljenek a szigorodó jogi szabályozásnak.

# Hivatkozások

- 1 Forbes.com, "Used Smartphone Market 'Poised to Explode,' Apple iPhone Holding up Better than Samsung Galaxy," 7 August 2013, [www.forbes.com/sites/connieguglielmo/2013/08/07/used-smartphone-market-poised-to-explode-apple-iphone-holding-up-better-than-samsung-galaxy/](http://www.forbes.com/sites/connieguglielmo/2013/08/07/used-smartphone-market-poised-to-explode-apple-iphone-holding-up-better-than-samsung-galaxy/)
- 2 Gartner.com, "Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 4.5 Percent in 2013 as Lower-Priced Devices Drive Growth," 21 October 2013, [www.gartner.com/newsroom/id/2610015](http://www.gartner.com/newsroom/id/2610015).
- 3 NBC News, "Target estimates breach affected up to 110 million," 10 January 2014, [www.nbcnews.com/business/target-says-stolen-infodata-breach-hit-70-million-people-2D11894083](http://www.nbcnews.com/business/target-says-stolen-infodata-breach-hit-70-million-people-2D11894083)
- 4 Infosecurity-magazine.com, "Massive Data Breach Hits Millions of Vodafone Germany Customers," 12 September 2013, [www.infosecurity-magazine.com/view/34504/massive-data-breach-hits-millions-of-vodafone-germany-customers/](http://www.infosecurity-magazine.com/view/34504/massive-data-breach-hits-millions-of-vodafone-germany-customers/)
- 5 Ponemon Institute—Experian Study 2011, [www.prnewswire.com/news-releases/new-survey-by-the-ponemon-institute-finds-that-databreaches-can-cause-lasting-and-costly-damage-to-the-reputation-of-affected-organizations-132682688.html](http://www.prnewswire.com/news-releases/new-survey-by-the-ponemon-institute-finds-that-databreaches-can-cause-lasting-and-costly-damage-to-the-reputation-of-affected-organizations-132682688.html)
- 6 Ponemon Institute—Experian, 2012 Consumer Study on Data Breach Notification, [www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf](http://www.experian.com/assets/data-breach/brochures/ponemon-notification-study-2012.pdf)
- 7 Javelin Strategy & Research—DEBIX, Consumer Survey on Data Breach Notification, June 2008, [mortstern.net/PDFSArticles/consumersurvey.pdf](http://mortstern.net/PDFSArticles/consumersurvey.pdf)
- 8 Law Technology News, "Reputational Damage Is the Lingering Data Breach Injury," 21 November, 2013, [www.lawtechnologynews.com/id=1202629029759/Reputational-Damage-Is-the-Lingering-Data-Breach-Injury#ixzz2r9pBZLYG](http://www.lawtechnologynews.com/id=1202629029759/Reputational-Damage-Is-the-Lingering-Data-Breach-Injury#ixzz2r9pBZLYG)
- 9 The Guardian, "Vodafone rings up complaints selling my old iPhone and data as new," 23 November 2013, [www.theguardian.com/money/2013/nov/24/consumer-rights-money-internetphonesbroadband?CMP=tw\\_t\\_gu](http://www.theguardian.com/money/2013/nov/24/consumer-rights-money-internetphonesbroadband?CMP=tw_t_gu)
- 10 Gartner, "Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond," 2010, [www.gartner.com/it/page.jsp?id=1480514](http://www.gartner.com/it/page.jsp?id=1480514)
- 11 thenextweb.com, "Canalys: Android on 79% of the 998 million smartphones shipped in 2013, Windows Phone fastest growing platform," 30 January 2014, <http://thenextweb.com/insider/2014/01/30/canalys-android-80-998-million-smartphones-shipped-2013-windowsphone-fastest-growing-platform/#luosKX>
- 12 CPPGroup plc, "Second Hand Mobiles Contain Personal Data," 22 March 2011, [www.prnewswire.com/news-releases/second-hand-mobiles-contain-personal-data-118434314.html](http://www.prnewswire.com/news-releases/second-hand-mobiles-contain-personal-data-118434314.html)
- 13 NBC News, "Why you should never sell your old cell phone," 8 May 2012, [www.nbcnews.com/business/why-you-should-never-sell-your-old-cell-phone-759723](http://www.nbcnews.com/business/why-you-should-never-sell-your-old-cell-phone-759723)
- 14 Government Technology, "4.2 Million Cell Phone Users Leave Sensitive Data Unprotected," 19 March 2009, [www.govtech.com/security/42-Million-Cell-Phone.html](http://www.govtech.com/security/42-Million-Cell-Phone.html)
- 15 Businessweek, "The Recycled Cell-Phone Trap," 3 November 2008, [www.businessweek.com/technology/content/nov2008/tc2008113\\_981236.htm](http://www.businessweek.com/technology/content/nov2008/tc2008113_981236.htm)
- 16 PC World, "Your Old Smartphone's Data Can Come Back to Haunt You," 10 July 2011, [www.pcworld.com/article/235276/your\\_old\\_smartphones\\_data\\_can\\_come\\_back\\_to\\_haunt\\_you.html](http://www.pcworld.com/article/235276/your_old_smartphones_data_can_come_back_to_haunt_you.html)
- 17 Dark Reading, "Old Smartphones Leave Tons Of Data For Digital Dumpster Divers," 15 December 2011, [www.darkreading.com/mobilesecurity/167901113/security/news/232300628/old-smartphones-leave-tons-of-data-for-digital-dumpster-divers.html](http://www.darkreading.com/mobilesecurity/167901113/security/news/232300628/old-smartphones-leave-tons-of-data-for-digital-dumpster-divers.html)
- 18 New York Times, "Where do old cellphones go to die?," 4 May 2013, [www.nytimes.com/2013/05/05/opinion/sunday/where-do-old-cellphones-go-to-die.html?\\_r=0](http://www.nytimes.com/2013/05/05/opinion/sunday/where-do-old-cellphones-go-to-die.html?_r=0)
- 19 ENISA, [www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/](http://www.enisa.europa.eu/act/application-security/smartphone-security-1/top-ten-risks/) top-ten-smartphone-risks?searchterm=Top+Ten+Smartphone+
- 20 CNET, "Your smartphone's secret afterlife (Smartphones Unlocked)," 19 August 2013, [www.cnet.com/8301-17918\\_1-57556225-85/your-smartphones-secret-afterlife-smartphones-unlocked/](http://www.cnet.com/8301-17918_1-57556225-85/your-smartphones-secret-afterlife-smartphones-unlocked/)
- 21 National Conference of State Legislatures, 14 November 2013, [www.ncsl.org/research/telecommunications-and-information-technology/2013-security-breach-legislation635200257.aspx](http://www.ncsl.org/research/telecommunications-and-information-technology/2013-security-breach-legislation635200257.aspx)
- 22 Kaspersky Lab-B2B International, "Global Corporate IT Security Risks: 2013," May 2013, [media.kaspersky.com/en/business-security/Kaspersky\\_Global\\_IT\\_Security\\_Risks\\_Survey\\_report\\_Eng\\_final.pdf](http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf)
- 23 Healthcare Technology Online, "Bracing For Healthcare's Mobile Explosion," 6 January 2012, [www.healthcaretechnologyonline.com/article.mvc/Bracing-For-Healthcares-Mobile-Explosion-0001?sectionCode=Welcome&templateCode=EnhancedStandard&user=2431702&source=nl:32854](http://www.healthcaretechnologyonline.com/article.mvc/Bracing-For-Healthcares-Mobile-Explosion-0001?sectionCode=Welcome&templateCode=EnhancedStandard&user=2431702&source=nl:32854)
- 24 Health Information Trust Alliance, "HITRUST's Analysis of U.S. Breach Data Finds Little Progress and Concern for Un-reported Breaches," 5 December 2012, [www.hitrustalliance.net/news/index.php?a=119](http://www.hitrustalliance.net/news/index.php?a=119)



**blancco**

MINŐSÍTETT ADATTÖRLÉS

További információ a Blanco termékeiről: <http://torles.hu>

---

A Blanco termékek kizárólagos magyarországi képviselője a V-Detect Antivírus Kft.



[www.v-detect.hu](http://www.v-detect.hu)

A Blanco termékek magyarországi Disztribútora a Kvarzar-Micro CEE Kft.



[hsw@kvarzar-micro.hu](mailto:hsw@kvarzar-micro.hu)