

# [SafeGuard® LAN Crypt]



## A bizalmas adatok egyedülálló védelme az illetéktelen külső, illetve belső hozzáférésekkel szemben

Az adatbiztonsággal foglalkozó termékek a vállalatokat "kívülről" fenyegető kockázatok ellen nyújtanak megoldást, míg a "belső" támadásokat általában figyelmen kívül hagyják- annak ellenére, hogy a vállalat bizalmas adataival való visszaélés kockázata megegyezik. Szinte minden vállalatnál igaz az, hogy az értékes adatok (üzleti jelentések, HR adatok, ügyfelek adatai, felmérési eredmények...) elektronikus módon kerülnek tárolásra, minden védelem nélkül. Jelenleg az adatok mentését általában központi szervereken oldják meg. Az internet, a hordozható adattárolók használata mind-mind a biztonsági kockázatok növekedését eredményezik.

Amire szükség van, az egy olyan biztonsági megoldás, mely csak az engedéllyel rendelkező felhasználói csoportoknak teszi lehetővé a védeni kívánt adatokhoz való hozzáférést. Sem a rendszer adminisztrátor, sem a külső dolgozók nem olvashatják a bizalmas adatokat. Pontosan ezek azok a biztonsági követelmények, melyek megvalósítására létrehozták a **SafeGuard LAN Crypt**-et.

A teljesen automatizált fájl titkosítás eredményeként hatékony megoldást nyújt a bizalmas adatok védelmére. A **SafeGuard LAN Crypt**-ben a rendszer adminisztrátori és biztonsági adminisztrátori szerepek élesen elkülönülnek egymástól, mely egyedülálló előnye a bizalmas adatok kezelésében. A rendszer adminisztrátor továbbra is úgy képes kezelni a rendszert, mint korábban, de nincs lehetősége, arra, hogy visszafejtse a titkosított fájlokat. Ez úgy lehetséges, hogy a kulcsokat a biztonsági adminisztrátor kezeli, aki viszont nem rendelkezik hozzáféréssel a titkosított fájlokhoz.

A biztonsági adminisztrátor definiálja az egyéni hozzáférési jogokat csoportok, illetve egyéni felhasználók számára a vállalat biztonsági irányelveinek megfelelően. A hozzáférési jogok profilokba tárolódnak. Minden felhasználó rendelkezik egy „kulcs csoporttal”, a profiljának megfelelően, így a felhasználó a megszokott módon olvashatja a fájlok neveit, illetve tartalmukat. Illetéktelen személyek csak egy titkosított, olvashatatlan karakter sorozatot látnak.

**SafeGuard LAN Crypt** nem kényszeríti a felhasználókat arra, hogy megváltoztassák megszokott munkafolyamataikat. A titkosítási folyamat észrevétlenül, a háttérben fut. A **SafeGuard LAN Crypt**-tel kezelhető, különböző típusú adathordozók, hálózati meghajtók, fájl szerverek, merevlemezek, eltávolítható adathordozók és terminál szerver is.

**SafeGuard LAN Crypt** teljes körű adatbiztonság eredményez a vállalat minden adatára.

Rugalmaságának köszönhetően használható kis rövid átmeneti csoportok, egyes részlegek, vagy project csoportok illetve egy egész vállalatra kiterjedően.

**SafeGuard LAN Crypt –Inteligens fájl titkosítás.**

## Utimaco Safeware

Az Utimaco Safeware az első IT szoftverét 1983-ban fejlesztette ki. Napjainkban az Utimaco piacvezető a vállalati információk biztonság területén. A legfejlettebb technikák használatának köszönhetően az Utimaco szoftverek egyedülálló biztonságot valósítanak meg. Az Utimaco termékek összköltsége alacsony, nagy megbízhatóságuk, könnyű használatuk, és adminisztrációjuk eredményeként. További részletekért látogasson el a [www.utimaco.hu](http://www.utimaco.hu) oldalra.

## Előnyök

### Megerősített biztonság

- Átlátszó adat védelem a felhasználói csoportok és egyéni felhasználók számára
- Tikosítás minden szokványos adathordozó
- Jogok szétosztása a rendszer-, és a biztonság adminisztrátor között
- Egyszerű implementálhatóság, a vállalat biztonsági házirendjébe
- A titkosítási szabályok rugalmas kezelése a felhasználói csoportok részére.
- Egyszerű PKI implementációs lehetőség. Támogatja a tanúsítványok, smart kártyák, USB tokenek használatát.

### Egyszerű alkalmazás

- Egyszerű központi adminisztráció a létező könyvtárak és domain-ek használatával.
- Nem szükséges módosítani a jelenlegi IT infrastruktúrát
- Skálázható az egyéni felhasználóktól a teljes vállalatot átölelő rendszerig

### Egyszerű használat

- Egyszerűen integrálható a népszerű munkakörnyezetbe
- A felhasználók számára átlátszó
- Magától értetődő funkcióinak köszönhetően, népszerű a felhasználók körében.

**utimaco**<sup>®</sup>  
safe ware

## Funkciók

### Biztonság

- Minden részletre kiterjedő biztonsági megoldás, az illetéktelen adat hozzáférés megakadályozására.
- Megvédi a vállalat értékes adatait, és a bizalmas személyes adatokat
- Élesen elkülöníti a rendszer- és biztonsági adminisztratori feladatköröket
- A legjobb elérhető megoldás, ha IT dolgozók nem alkalmazottai a vállalatnak, mivel annak ellenére, hogy el tudják végezni a munkájukhoz szükséges műveleteket, az adatokat nem képesek olvasni.
- Kipróbált és tesztelt titkosítási algoritmusokat használ
- Automatikus titkosítás és visszaféjtés a háttérben
- Megvédi az adatokat a merevlemezen, hálózati meghajtón egyéb adathordozókon, mint például CD-ROM-ok, DVD-k, ZIP-, JAZ drive-ok USB és flash memória kártyák...
- Felhasználó azonosítása X.509 tanúsítvánnyal
- Támogatja a smartcard-okat és USB token-eket

### Rendszer adminisztráció

- Egyszerű központi installáció, konfiguráció és adminisztráció, a jelenlegi IT eszközökbe való beépüléssel, és a jelenlegi könyvtárak, és szolgáltatások használatával (LDAP, Active Directory, domain)
- Egyszerű integráció a kialakított PKI rendszerhez
- Nem csökken a szerver teljesítménye.
- Költség hatékony és gyorsan implementálható megoldás, melynek nincs szüksége semmilyen új struktúra kialakításra
- Kevesebb idő és pénz kell a helpdesk szolgáltatásokra
- Visszaállítási lehetőség, így a titkosított adatokhoz biztosított a hozzáférés probléma felmerülése esetén.

### Könnyen használható

- Jogosult felhasználók biztonságosan menthetik le megosztott adataikat az általuk használni kívánt adathordozóra, annak kockázat nélkül, hogy illetéktelen személy hozzájuk férne.
- Nem szükséges a megszokott munkafolyamatokon-, és eszközökön változtatni.
- A felhasználók könnyen elfogadják, hiszen nincs szükség semmilyen oktatásra a használatához

## Rendszerkövetelmény

### Hardware

- PC Intel Pentium, vagy azzal kompatibilis processzorral

### Operációs rendszer

- Microsoft Windows XP
- Microsoft Windows 2000

### Támogatott file server-ek, operációs rendszerek

- Microsoft Windows
- Novell Netware
- Linux, Unix (Samba)

### Támogatott Terminál szerverek

- Microsoft Windows 2000 Terminal Server
- Microsoft Windows 2003 Terminal Server
- Citrix MetaFrame

## Tanúsítványok

- FIPS 140-2 (cryptographic library in evaluation)
- Aladdin eToken certified



## Kiegészítő SafeGuard® termékek

- Ez a termék együtt használható a SafeGuard® Advanced Security modulokkal, más kiegészítő megoldások megvalósítás érdekében. Ezek lehetnek például: Multi-Desktop alkalmazások, Single Sign On, Plug & Play Management és alkalmazás specifikus hozzáférési jogok (ASAI)

## Együtműködés

- Microsoft Crypto API integráció: Cryptographic Service Providers (CSPs) használata azt jelenti, hogy a "third-party suppliers"-ek (pl: smartcard, USB token) által elérhető bármely RSA komponens használható felhasználó azonosítására

## Támogatott adathordozók

- Hard disks, hálózati meghajtók, disket, CD-ROM, ZIP drive, USB drive és számos egyéb adathordozó

## Interfészek

- ODBC (Database)
- Crypto API
- Microsoft cryptographic service provider (CSP – Token és smart cards)

## Szabványok/protokollok

- Azonosítás: Felhasználó azonosítása X.509v3 tanúsítványokkal
- PKCS#12
- LDAP
- Rejtjelezés: 3DES 168-bit, IDEA 128-bit, AES 128-bit and 256-bit
- Hash: MD5, SHA-1, SHA-256
- Token-ek: smart kártyák, USB token-ek Crypto API-val



## Nyelvi verziók

- Angol, német

## Kapcsolat

### Utimaco Safeware AG

- info@utimaco.hu
- info@safesoft.hu



### Copyright Information

© 2004 – Utimaco Safeware AG  
SafeGuard® LAN Crypt Version 3.11

All SafeGuard products are registered trademarks of Utimaco Safeware AG. All other named trademarks are trademarks of the particular copyright holder.