



Gizli bilgilere içeriden ya da dışarıdan yapılan yetkisiz erişimlere karşı özel koruma

Birçok veri koruma ölçütü bir şirketin dışındaki tehlikelerle karşılaşmak üzere tasarlanmış olup, içerideki pek çok risk göz ardı edilir. Oysa gizli şirket bilgilerinin kötüye kullanımının neden olduğu potansiyel zarar tamamen aynıdır. Hemen her kuruluşta iş raporları, İK belgeleri, müşteri verileri ve araştırma sonuçları gibi değerli bilgiler koruma olmadan elektronik ortama kaydedilir. Halihazırdaki; bilgileri merkezi olarak sunucularda saklama, çok siteli işyeri ağları ve gezici veri kayıt ortamlarının kullanımı pratiklerinin anlamı, güvenlik risklerinin giderek artmasıdır. Giderek artan sayıda kuruluş maliyetleri azaltmak için, BT bölümlerinin işlevlerini dış kaynaklardan karşılarken, gizlilik konusundaki kaygıları da buna paralel biçimde artmaktadır.

Asıl gereken, bir kuruluştaki duyarlı bilgilere yalnızca yetkili kullanıcı gruplarının erişimine izin veren bir güvenlik çözümüdür. Kurum personeli olan sistem yöneticileri ya da dış kaynak şirketinin elemanlarının dahi gizli bilgileri görmelerine izin verilmemelidir. İşte **SafeGuard LAN Crypt** tam olarak bu güvenlik sorununu çözmek üzere tasarlanmıştır.

SafeGuard LAN Crypt gizli dosyaların etkin biçimde korunması için tam otomatik dosya şifrelemesinden yararlanır. **SafeGuard LAN Crypt**'te Sistem Yöneticisi ile Güvenlik Yöneticisi'nin rolleri kesin olarak tanımlanmıştır. Bu özellik ona veri güvenliğini ele alma konusunda özgün bir avantaj sağlar. Sistem Yöneticisi sistemi her zaman olduğu gibi yönetebilir ancak elinde herhangi bir dosyayı deşifre edecek araç bulunmaz. Bunun nedeni, anahtarların kendi adına, saklanmış, şifreli dosyalara erişemeyen Güvenlik Yöneticisi tarafından yönetilmesidir.

Güvenlik Yöneticisi çalışma grupları ya da kişisel kullanıcıların bireysel erişim haklarını şirket güvenlik ilkeleriyle uyum içinde tanımlar. Sonra bu erişim hakları şifreleme profilleri içinde bir araya getirilir. Bunun anlamı her kullanıcıya, serbest bırakılmış dosyaları normal biçimde ve düz metin halinde okuyabileceği, profiline bağlı, tekil bir "anahtar grubunun" atanmasıdır. Yetkisiz kişiler yalnızca şifrelenmiş, okunamayacak bir karakter katmanı görür.

SafeGuard LAN Crypt kullanıcıları çalışma biçimlerini değiştirmeye zorlamaz. Şifreleme süreci şeffaf olup, arka planda görünmez olarak çalışır. SafeGuard LAN Crypt değişik türden bellek ortamları, ağ sürücülerini ya da dosya sunucuları, sabit diskler ve çıkarılabilir ortamlarla uç nokta hizmeti sunucularında kullanılabilir.

SafeGuard LAN Crypt bir şirketin tüm verileri için kapsamlı koruma sağlar. Ölçeklenebilir, dolayısıyla küçük geçici ekiplerde, bölümlerde ve proje gruplarında ya da kurumların tamamında kullanılabilir.

SafeGuard PrivateDisk – Akıllı dosya şifreleme.

Utimaco – Veri Güvenliği Şirketi –Hakkında

Utimaco lider bir veri güvenliği çözümleri sağlayıcısıdır. Veri Güvenliği Şirketi olarak, orta ve büyük boydaki kuruluşların bilgi varlıklarını saldırılardan korumalarına ve mahremiyetleri ile bütünlüklerini bozmadan, gizlilik yasalarına uymalarına olanak verir. Utimaco'nun çözüm yelpazesinin tamamı, yalnızca özel güvenlik gereksinimlerini karşılayan, ücretsiz, uç nokta ya da dahili şifreleme çözümlerinin aksine, 360°'lik tam koruma sağlar. Gelişkin SafeGuard Çözümleri verileri her koşulda (saklanan/durağan veriler, aktarımdaki/hareket halindeki veriler ya da işlenen/kullanılan veriler) yönetmeye ve güvence altına almaya yardımcı olurlar. Utimaco Avrupa, ABD ve Asya'da, dünya çapında bir iş ortakları ve bayiler ağı üzerinden, müşterilerine kapsamlı yerinde destek sunmaktadır. Daha fazla bilgi için www.utimaco.com adresini ziyaret ediniz.

Yararları

Geliştirilmiş güvenlik

- ✓ Kullanıcı grupları ve bireysel kullanıcılar için şeffaf veri güvenliği
- ✓ Tüm standart ortamlarda ve heterojen platformlarda şifreleme
- ✓ Sistem ve güvenlik yönetimi arasında güç bölüşümü
- ✓ Şirket genelinde bir güvenlik politikasının kolayca gerçekleştirilmesi
- ✓ Kullanıcı grupları için esnek şifreleme kurallarının tanımlanması
- ✓ Karmaşık olmayan PKI entegrasyonu ve sertifikalar, akıllı kartlar ve USB işaretleri (token) için destek

Uygulaması kolay

- ✓ Heterojen BT altyapılarında sorunsuz entegrasyon
- ✓ Mevcut izin ya da etki alanları kullanılarak, karmaşık olmayan, merkezi yönetim
- ✓ Mevcut BT altyapısı için ek yükseltmeler gerekmez
- ✓ Bireysel kullanıcıların gruplarından şirket boyutunda kullanıma varana dek ölçeklenebilirlik

Kullanımı kolay

- ✓ Alışılmış çalışma ortamlarına entegrasyon sayesinde kolay kullanım
- ✓ Kullanıcılar açısından şeffaf
- ✓ Kendini açıklayan işlevsellik, yüksek düzeylerde kullanıcı kabulü anlamına gelir

Anahtar Özellikler/İşlevsellik

Güvenlik

- ✓ Yetkisiz veri erişimini önlemek için kapsamlı güvenlik çözümü
- ✓ Değerli şirket verilerini ve gizli kişisel bilgileri korur
- ✓ Sistem ve güvenlik yöneticilerinin sorumluluklarını kesin olarak ayırır
- ✓ BT'nin dış kaynaktan sağlanması durumunda, olası en iyi korumadır, zira dış kaynaktan gelen elemanlar dosyaları yönetseler dahi, onları düz metin halinde okuyamazlar
- ✓ Denenmiş ve sınanmış güvenlik algoritmalarını kullanır
- ✓ Arka planda otomatik şifreleme ve şifre çözme
- ✓ Sabit diskler, ağ sürücüler ve disketler, CD-ROMlar, DVDler, USB ve flaş bellek kartları gibi taşınabilir ortamlardaki verileri korur
- ✓ X.509 sertifikaları aracılığıyla kullanıcı kimliği doğrulama
- ✓ Akıllı kartlar ve USB işaretlerini (token) destekler
- ✓ **Sistem Yönetimi**
- ✓ Mevcut BT ortamlarına entegrasyon ve mevcut dizin hizmetlerinin (LDAP, Active Directory) ya da etki alanlarının kullanımı aracılığıyla kolay, merkezi kurulum, ayarlama ve yönetim
- ✓ Mevcut PKI sistemleri ile karmaşık olmayan entegrasyon
- ✓ Sunucu verimliliği azalmaz. Şifreleme ve şifre çözme işlemi yalnızca cihazların üzerindeki bir filtre sürücüsü tarafından yapılır
- ✓ Fazladan altyapı gerektirmeyen maliyet-etkin, hızlı geliştirilen çözüm
- ✓ Yardım masası hizmetleri için daha az zaman ve para gerekir
- ✓ Kurtarma stratejisi sayesinde, acil bir durumda da şifrelenmiş verilere erişilebilir

Kullanımı kolay

- ✓ Yetkili kullanıcılar, dışarıdan yetkisiz bir kişinin erişimi riski olmaksızın, paylaşımlı bilgilerini, alıştıkları bellek ortamına güvenle kaydedebilir
- ✓ Sürekli şifreleme
- ✓ Alıştıkları çalışma ortam ve adetlerini değiştirmek gerekmez
- ✓ Yüksek kullanıcı kabulü düzeyleri – ek eğitim gerekmez

Sistem Gereksinimleri

Donanım

- ✓ Intel Pentium ya da uyumlu işlemci taşıyan kişisel bilgisayar

İşletim Sistemi

- ✓ Microsoft Windows XP
- ✓ Microsoft Windows 2000

Desteklenen dosya sunucusu işletim sistemleri

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

Sertifikalar

- ✓ FIPS 140-2
- ✓ Aladdin eToken Enabled

Birlikte çalışabildikleri

- ✓ Microsoft Crypto API entegrasyonu: Kriptografik Hizmet Sağlayıcıların (CSPlar) kullanımı, kullanıcı kimliğinin doğrulanması için, üçüncü parti sağlayıcılardan gelen RSA niteliğindeki her tür ögenin (akıllı kartlar ya da USB işaretleri gibi) uygulanabileceği anlamına gelmektedir
- ✓ Oracle ve Microsoft SQL Server veritabanı arayüzü
- ✓ Microsoft Active Directory ve Novel eDirectory entegrasyonu

Desteklenen ortamlar

- ✓ Sabit diskler, ağ sürücüler, disketler, CD, DVD, USB sürücüler ve daha pek çoğu

Arayüzler

- ✓ ODBC (Veritabanı)
- ✓ Crypto API
- ✓ Microsoft Kriptografik Hizmet Sağlayıcı (CSP – İşaret ve akıllı kartlar)

Standartlar/Protokoller

- ✓ Kimlik doğrulama: X.509 sertifikaları aracılığıyla kullanıcı kimliği doğrulama
- ✓ PKCS#12
- ✓ LDAP
- ✓ Şifreleme: 3DES 168 ikil, IDEA 128 ikil, AES – 128 ve 256 ikil
- ✓ Karıştırma: MD5, SHA-256
- ✓ İşaretler: Akıllı kartlar ve Crypto API aracılığıyla USB işaretleri

Dil Sürümleri

- ✓ İngilizce, Almanca, Fransızca

Bağlantılar

AVRUPA ORTADOĞU AFRİKA

Utimaco Safeware AG
Hohemarkstrasse 22
DE-61440 Oberursel
Germany
Phone +49 (61 71) 88-14 44
info@utimaco.com

ASYA PASİFİK

Utimaco Safeware Asia Ltd.
Unit 602, Stanhope House
734 King's Road, Quarry Bay
Hong Kong
Phone +8 52 25 20 26 08
info@utimaco-asia.com

KUZEY & GÜNEY AMERİKA

Utimaco Safeware Inc.
10 Lincoln Road
Foxboro, MA 02035
USA
Phone +1 (508) 543-10 08
sales.us@utimaco.com

JAPONYA

Utimaco Safeware K.K.
Nisso 16 Building, 3F
3-8-8 Shin Yokohama, Kohoku-ku
Yokohama 222-0033
Japan
Phone +81 (0) 45 470-1430
info.jp@utimaco.jp