



## Ofiste çalışan ve gezici elemanlar için, politika tabanlı erişim denetimine yönelik, uyarlanabilen güvenlik süiti

Günümüzün ağ yapısındaki işletme ortamı ve gezici bilgi-işlemin engellenemeyen ve hızlı çıkışı, bir işletmenin BT altyapısını, başarı için anahtar bir bileşene dönüştürmüştür. Öte yandan, BT altyapısının birçok potansiyel zayıf noktası vardır. Sunucular ve kişisel cihazlarda tutulan duyarlı bilgiler anında koruma gerektirir ve sistemin devrede kalması için sürekliliği için ön koşullardan biridir.

Demek ki, BT altyapısına yapılan yetkisiz erişim önemli bir sorundur. Güvenlik konuları arasında cihazlara, uygulamalara ve şirket ağına yetkisiz erişimi yasaklamak ve kullanıcıların yetkisiz yazılım ve donanım kurmasını engellemek bulunmaktadır.

Kuruluşlar güvenlik politikalarını kurmak için ciddi çabalar gösterseler de, politikayı zorlayacak araçlardan genellikle yoksundurlar. **SafeGuard Advanced Security** bu boşluğu doldurmaktadır. **SafeGuard Advanced Security**'nin yedi modülü, kullanıcıların değişik platformlarda çalışmasından ya da değişik cihazlara (kişisel bilgisayarlar, dizüstü bilgisayarlar ya da uç hizmeti veren sunucular) erişmesinden bağımsız olarak, gereksinimlere göre uyarlanmış bir güvenlik çözümü sağlamaktadır.

- ⇒ Advanced Security base (BASE) güçlü kimlik doğrulama özelliği ile, sisteme giriş işleminin yerini almaktadır.
- ⇒ Application Specific Access Rights (ASAR) kullanıcılar, uygulamalar ve bilgilerin üç boyutlu erişim hakları getirmektedir.
- ⇒ Plug and Play Management (PnP) Tak-Çalıştır niteliğindeki cihazların merkezi denetimine olanak sağlar.

Kapsamlı güvenlik özellikleri, kolay yönetimi ve kullanım kolaylığı **SafeGuard Advanced Security**'i doğru seçenek haline getirmektedir.

## Yararları

### Geliştirilmiş güvenlik

- Heterojen ortamlarda (çoklu işletim sistemleri, çoklu cihazlar – kişisel bilgisayarlar, dizüstü bilgisayarlar, uç hizmeti veren sunucular) şirket geneline yayılan bir güvenlik politikasının kolayca yürütülmesi
- Gelişkin sistem kullanılabilirliği/dengesi ve böylelikle yetkisiz program kurulumuna karşı etkin koruma ile garantili iş sürekliliği
- Yetkisiz erişim ve yanlış kullanıma karşı koruma
- Yetkisiz çevre birimlerinin bağlanması karşı koruma
- Sistemden içeri/dışarı yetkisiz veri aktarımına karşı kapsamlı koruma

### Uygulaması kolay

- Active Directory için Microsoft Yönetim Konsolu (MMC) ve Novell yönetim araçları ile entegre yönetim
- Artan sistem bütünlüğü / kullanılabilirliği ile, yardım masasının iş yükünün azalması ve kullanıcılar için parola yönetiminin kolaylaşması
- Modüler mimari aracılığıyla, gereksinimlere uyarlanmış güvenlik

### Kullanımı kolay

- Tüm kullanıcı birimlerinin şeffaf olarak uygulanması sayesinde eğitim çabası gerekmez
- Removable Media Management (Çıkarılabilir Ortam Yönetimi) sayesinde, artık kullanılmayan dosya sürümlerinin yüklenmesinin kesin olarak engellenmesi
- Güvenli ve etkin istemci paylaşımı ile artan üretkenlik ve/ya da varlık kullanımı
- Tak-Çalıştır cihazları tüm hakları ile sınırsız olarak kullanılabilir

## 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](http://www.utimaco.com) adresini ziyaret ediniz.

## Anahtar Özellikler/işlevsellik

### Temel modül

- ✓ Geliştirilmiş parola kuralları ve akıllı kartlar ve/ya da PIN üzerinden, ayrıntılı kimlik doğrulama
- ✓ Etki alanı kullanıcıları arasında hızlı ve güvenli istemci paylaşımı: akıllı kartın çıkarılması ve takılması yinelenen çıkış/giriş işlemleri olmaksızın, kişisel masaüstünü güvenle kapatıp yeniden açar
- ✓ Güvenlik olay kayıtlarının kapsamlı olarak tutulmasıZ
- ✓ Windows Installer (MSI) tabanlı kurulum
- ✓ Microsoft Yönetim Konsolu (Microsoft Management Console-MMC) ve Novell yönetim araçları ile tam entegrasyon
- ✓ Mevcut ayarların tam olarak sunumu için Configuration Viewer (Ayar İzleyici)

### Tak-Çalıştır (Plug and Play-PnP) Yönetimi

- ✓ Tak-Çalıştır niteliğindeki cihazlar için kullanım denetimi
  - ✓ Kullanım izni cihaz sınıfına (sürücüler, yazıcılar, vb.) ya da belirli cihazların cihaz kimliğine bağlı olarak verilebilir ya da verilemeyebilir
  - ✓ ASAR modülü ile bağlantılı zorlayıcı sürücü adreslemesi cihaza özgü erişim ve dışarıya veri aktarma haklarının tanımlanmasına olanak sağlar
  - ✓ SafeGuard LAN Crypt ile bağlantılı zorlayıcı sürücü adreslemesi cihaza özgü şifreleme kurallarının tanımlanmasına olanak sağlar

### Uygulamaya Özgü Erişim Hakları (Application Specific Access Rights-ASAR)

- ✓ Kullanıcılar, veriler ve uygulamalar arasındaki etkileşimi denetlemek için erişim haklarının 3 boyutlu yönetimi

## Sistem Gereksinimleri

### Donanım

- ✓ Intel Pentium ya da benzer işlemcili kişisel bilgisayar
- ✓ (Tüm modüllerin tam kurulumu için) En az 35 MB boş disk alanı

### İşletim Sistemi

- ✓ Microsoft Windows XP / 2000
- ✓ Microsoft Windows 2003 Server Standard Edition
- ✓ (Yönetim için) Novell Server 5.1 / 6.0
- ✓ Citrix istemci, 6.31 Citrix Metaframe XP FR2
- ✓ IBM CSS 5.20 ya da üzeri

### Ağ

- ✓ Microsoft tarafından desteklenen tüm ağlar

## Tamamlayıcı SafeGuard® ürünleri

- ✓ Tüm sabit diskin ya da çıkarılabilir ortamın temel olarak şifrenmesi için SafeGuard Easy
- ✓ Cep bilgisayarlarını korumak için SafeGuard PDA
- ✓ Dosyaların/klasörlerin şeffaf olarak şifrenmesi için SafeGuard LAN Crypt

## Birlikte çalışabildikleri

- ✓ İstemcinin sisteme girişinde Novell-Client ve diğer ürünler desteklenmektedir
- ✓ Novell ZENWorks
- ✓ Uç Nokta Hizmet Sunucusu (Terminal Server) dahil, Citrix Metaframe
- ✓ IBM Client Security Yazılımı (CSS ve ESS)
- ✓ PKCS#11 üzerinden akıllı kart ya da USB işaretleri (token)



## Arayüzler

- ✓ MS GINA istemci arayüzü
- ✓ Novell IntranetWare istemci arayüzü
- ✓ Biyometrik kimlik doğrulama arayüzü (PKCS#11 PAP)
- ✓ PKCS#11

## Standartlar/Protokoller

- ✓ PC/SC



## Dil Sürümleri

- ✓ İngilizce, Almanca, Fransızca (Temel modül)

## Standartlar/Protokoller

- ✓ PKCS#11, AES (256 and 128 bit), Rijndael (256 bit), IDEA (128 bit), DES (56 bit), 3DES (168 bit), Blowfish-8/16 (256 bit), Stealth-40 (40 bit)

## 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](mailto: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](mailto: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](mailto: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](mailto:info.jp@utimaco.jp)