Veri Korumanın Keyfini Çıkarın

EGOSECURE
ENJOY DATA PROTECTION

KVKK
Kişisel Verilerin Korunması Kanunu

Veri Koruması

Veri akışını analiz ettikten ve Insight & IntellAct ile zayıf bağlantıları belirledikten sonra , koruyucu önlemler 20 koruma fonksiyonu ile ayrı ayrı yapılandırılabilir. Bu koruma işlevleri i.C.A.F.E. PRENSİBİ' ne dayanmaktadır.

Tüm fonksiyonlar tek bir çözüme entegre edilmiştir, sadece bir veritabanına erişir ve merkezi bir yönetim konsolu ile kontrol edilir. Sadece bir kurulum vardır, bundan sonra modüller koruma gereksinimlerine göre etkinleştirilebilir. Koruma ihtiyaçlarının daha sonra ayarlanması yeni kurulum gerektirmez.

Çözümümüz, kapsamlı çalışma ve maliyetli danışmanlık desteği olmadan kurulumu kolay ve hızlıdır. **EgoSecure Data Protection** esas olarak kurum içi gelişmelerden oluşur ve bu nedenle tek tip bir kurulum, yönetim ve işletim konseptine sahiptir.

Tüm koruma fonksiyonları, EgoSecure Veri Koruması kullanımını mümkün olduğunca kolay ve güvenli hale getirmeye odaklanır. Biz buna **“mükemmel BT güvenliği”** diyoruz.

Sağladığı Artı Değerler

- ✓ **Veri güvenliğiniz için hepsi bir arada çözüm**
- ✓ **Çok düşük yönetim çabası**
- ✓ **EU-DSGVO, CCPA ve Co.'ya uygunluk**
- ✓ **Arka planda güvenilir sistem koruması**
- ✓ **Müşterilerle diyalog içinde sürekli gelişim**
- ✓ **Gerçek zamanlı raporlama ve gösterge tabloları sayesinde daha fazla şeffaflık**
- ✓ **İş gereksinimlerinize uyarlanmış**
- ✓ **Basit ve hızlı kurulum, sezgisel yönetim**
- ✓ **Birleşik Uç Nokta Yönetimi, Hizmet Yönetimi ve Yazılım Varlık Yönetimine Entegrasyonlar**

INTELLACT

Insight Analizi (Insight Analysis)

Koruyucu önlemlerin en iyi şekilde alınmasını sağlamak için, INSIGHT modülü önce işletme ağında veri güvenliği ile ilgili genel durumu belirler.
Bu analizin sonuçları daha sonra yönetime uygun bir şekilde işlenir ve grafik ve tablolarda sunulur. Bu şekilde INSIGHT, her bir işletme ve kuruluş için veri güvenliği hakkında genel bir tablo çizen gerçekleri sağlar. Sunum kümülatiftir, bu nedenle bireysel kullanıcıların faaliyetleri hakkında sonuçları görmek mümkün değildir. Bu formdaki veriler, gerçekten gerekli olan koruyucu önlemleri ayarlamak için idealdir.
INSIGHT hakkında daha fazla bilgiyi buradan edinebilirsiniz.

IntellAct Otomasyonu (IntellAct Automation)

IntellAct modülü, Modul Insight'ın önceden belirlenmiş kurallara göre koruyucu önlemleri belirlediği ve tetiklediği gerçeğini analiz eder. Ayrıca anormallikleri veya kritik durumları otomatik olarak tespit etmek ve uygun koruyucu yanıtı tetiklemek için normal değerlerle karşılaştırma imkanı sunar. Bu otomatizm, yöneticilerin çalışmasını muazzam bir şekilde kolaylaştırır ve reaksiyon süresini önemli ölçüde azaltır.

Araçlar (Tools)

Envanter (Inventory)

Her şeyden önce, Envanter ile işltme ağındaki bilgisayarda hangi donanım ve yazılım ürünlerinin yüklü olduğunu görebilirsiniz. Ancak çok daha önemli olan, Envanter'deki değişiklikleri görmenize, analiz etmenize ve bir şey değiştiğinde uyarı almanıza izin veren özelliklerdir. Donanımın durumu da görüntülenebilir ve bu nedenle güvenilir bir şekilde sorunları gösterir.

Parola Yöneticisi (Password Manager)

Çalışanların artık kimliklerini (e-posta adresi, kullanıcı adları, oturum açma bilgileri) ve şifrelerini Post-It'e, dosyalara veya benzer yardım dosyalarına yazmasına gerek yoktur - güvenli Parola Yöneticisi bununla ilgilenir. Karmaşık şifreler oluştururken bile, Parola Yöneticisi akıllı bir prosedürle sizi destekleyebilir. Ayrıca, korunan Parola Yöneticisi dosyalarını ağ üzerinde depolayarak oturum açma bilgilerinin iş arkadaşlarınızla paylaşılması da mümkündür.

Güvenli Silme (Secure Erase)

Güvenli Silme, dosya dahili sabit sürücüde veya harici depolama aygıtında olsun, silinen dosyaların kurtarılamayacağını garanti eder. Bu amaç için çok çeşitli silme seçenekleri mevcuttur. Donanımı satsanız veya son olarak kullanımdan kaldırsanız bile, Güvenli Silme, donanımdan tamamen kurtulmanızı sağlar.

Yeşil-BT (Green-IT)

Akıllı güç yönetimi, yalnızca bilgisayar kullanımdayken enerji tüketerek son aygıtların verimli bir şekilde çalışmasına yardımcı olur. Yeşil BT, BT'nin işletim maliyetlerinin düşürülmesini, BT'nin çevre dengesine önemli bir katkıda bulunmasını ve EgoSecure Data Protection' ın başlatılması için hızlı bir yatırım getirisinin elde edilmesini sağlar.

KONTROL (CONTROL)

Cihaz Yönetimi (Device Management)

Cihaz Yönetimi, kimin hangi cihazları (örneğin USB çubukları, CD'ler, TV tarayıcısı) veya arayüzleri (örneğin WLAN, Firewire, USB) kullanmasına izin verildiğine ve ne ölçüde kullanıldığına dair net bir tanım sağlar. Bu, tüm bu cihazların yanlış kullanım veya veri kaybı riski olmadan kullanılabileceği anlamına gelir. Ayrıca, kötü amaçlı yazılımların arabirimler aracılığıyla işletme ağına girmesini önler. Cihaz Yönetimi (Device Management) "içeriden gelen saldırganlara" karşı etkin koruma sağlar.

Bulut Erişim Kontrolü (Cloud Access Control)

Her yerde verilere erişilebildiğinden, bulutun kullanılmasının iş esnekliği açısından birçok avantajı vardır. Bununla birlikte, özellikle hassas verilerin bulutta yeri yoktur ve bazı verilerin üçüncü ülkelerdeki bulut depolama alanında yasal olarak depolanmasına bile izin verilmez. Bulut Erişim Kontrolü hangi çalışanın hangi bulut hizmetlerini ve ne ölçüde kullanabileceğini kontrol eder.

Bağlantı Erişim Kontrolü (Connection Access Control)

Bugün, kurumsal ağ üzerindeki resmi rotalara ek olarak, en yaygın olanları adlandırmak için Bluetooth, WiFi, modem gibi diğer birçok yolla veri iletimi mümkündür. Ancak, bir işletme verilerin hangi rotalardan ayrıldığını kontrol etmelidir. Bağlantı Erişim Kontrolü hangi çalışanın hangi veri aktarım cihazlarına erişebileceğini kontrol eder.

DENETİM (AUDIT)

Güvenli Denetim (Secure Audit)

Denetim, veri akışlarını ayrıntılı olarak görünür hale getirir, koruma ayarlarındaki olası zayıflıkları gösterir ve adli bilgilerin tanımlanmasını sağlar. Bu bilgileri üretme yeteneği BT uyumluluğuna önemli bir katkıdır ve yasaların ve endüstri düzenlemelerinin gerekliliklerini karşılar. Örneğin, Federal Veri Koruma Yasası (Federal Data Protection Act) günlüğe kaydetmeyi zorunlu kılar. EgoSecure INSIGHT-Audit, 4 veya 6 göz prensibi ile kayıt verilerine erişimi koruyarak çalışanların kişisel haklarını ihlal etmeyi de imkansız hale getirir.

FİLTRE (FILTER)

İçerik Analizi ve Filtre (Content Analysis & Filter)

İçeriğin analizi ve işletmeden ayrılan verilerden gizli bilgilerin filtrelenmesi ve gelen verilerde zararlı bilgilerin engellenmesi bütüncül bir güvenlik kavramının bileşenleridir. İçerik Analizi ve Filtre, iş süreçlerini ve istenen veri aktarımını engellemeden veri iletişimi için ayrıntılı ve güvenilir koruma sağlar.

Antivirüs (Antivirus)

Virüsten koruma çözümü, Internet'ten gelen anonim saldırganlara karşı kanıtlanmış koruma sağlar. Tespit hızının olabildiğince yüksek olması, yani yeni virüslere ve Truva atlarına çok hızlı tepki vermesi önemlidir. EGOSECURE DATA PROTECTION, birçok test raporuna göre, piyasadaki en iyi çözüm olan ve tanınan yüksek algılama oranına sahip bir çözümü entegre eder.

Uygulama Kontrolü (Application Control)

Uygulama Kontrolü hangi kullanıcının hangi programları başlatabileceğini denetler. Bu, örneğin sorumluluk risklerine ve ekonomik hasara neden olabilecek oyunların veya lisanssız yazılım ürünlerinin kullanımını önler. Birçok virüs de engellenebilir, genellikle anti-virüs çözümlerinin tespit edebileceğinden daha hızlıdır.

Veri Kaybı Önleme (Data Loss Prevention)

DLP (Veri Kaybını Önleme), belirli içerik için bilgisayara bırakılan veya bilgisayara kopyalanan metin dosyalarını tarar. Bu, kredi kartı numaraları veya diğer kesinlikle gizli bilgiler gibi bilgilerin dış dünyaya iletilmemesini sağlar. Gizli bir bilgi bulunduğunda, işlemi günlüğe kaydetme veya engelleme gibi seçili eylemler gerçekleştirilebilir.

ŞİFRELEME (ENCRYPTION)

Çıkarılabilir Cihaz Şifrelemesi (Removable Device Encryption)

USB çubukları gibi mobil veri taşıyıcıları gittikçe küçülüyor ve daha güçlü hale geliyor, ancak kaybedilmesi veya çalınması da giderek daha kolay hale geliyor. Çıkarılabilir Aygıt Şifrelemesi, verilerin yetkisiz kişiler tarafından kullanılmamasını sağlar. Şifreleme dosya tabanlıdır ve bir ortam üzerinde paralel olarak kullanılabilen farklı şifreleme türleri mümkündür.

Tam Disk Şifrelemesi (Full Disk Encryption)

Dizüstü bilgisayarlar kaybolabilir veya çalınabilir ve üzerlerinde hassas kurumsal veriler olabilir. Tam Disk Şifrelemesi, aygıta ve verilere yalnızca yetkili kullanıcıların erişmesini sağlar. Daha iyi güvenlik için akıllı kartlar ve eToken, 2 faktörlü kullanıcı kimlik doğrulaması için kullanılabilir. EgoSecure FDE, yazılımda FIPS 140-2 Seviye 1 sertifikalıdır. EgoSecure FDE'de Gelişmiş Şifreleme Standardı Yeni Yönetmelik (AES-NI) desteği, şifreleme performansını artırır

Önyükleme Öncesi Kimlik Doğrulaması (Pre-Boot Authentication)

ÖNYÜKLEME ÖNCESİ DOĞRULAMA, Windows ve bağlantılı örneğin harddisk şifrelemesi gibi şifrelemelerin, sabit diskleri yeniden yapılandırarak, USB/CD'yi başlatarak veya işletim sistemini değiştirme yoluyla değiştirilemez veya atlatılamaz olmasını sağlar. İlgili terminale kayıt BIOS yükleme işleminden hemen sonra, ancak işletim sisteminin başlatılmasından önce yapılacaktır. Parolaların yanı sıra birçok akıllı kart da giriş güvenliği olarak desteklenir. Yardım masası, kendi kendine başlatma ve daha fazlası gibi kurumsal özellikler de mevcuttur. Oturum açma maskelemesi her çalışan için özelleştirilebilir.

Yerel Klasör Şifrelemesi (Local Folder Encryption)

Klasör Şifrelemesi, kaybolan dizüstü bilgisayarlardaki veya sabit disklerdeki verileri korur ve ayrıca birden çok kullanıcı tarafından erişilebilen sistemlerde ayrı ayrı tanımlanan hassas verileri korur. Örneğin, son derece hassas yönetim verileri, BT personeli gibi birçok ayrıcalığa sahip çalışanlar aracılığıyla erişime karşı korunabilir.

Bulut Depolama / Ağ Paylaşımı Şifrelemesi (Cloud Storage / Network Share Encryption)

Bulut ve Ağ Şifrelemesi, buluttaki veya herhangi bir ağdaki klasörleri şifrelemek için kullanılabilir. Şifreleme anahtarları işletme içinde kalır ve asla bulutta depolanmaz - bulut depolama sağlayıcılarının sağladığı şifreleme çözümlerine göre açık bir avantaj.

Kalıcı Şifreleme (Permanent Encryption)

Kalıcı Şifreleme, hangi veri taşıyıcılarında depolandıklarına bakılmaksızın dosyaları şifreler. Bu şifreli veri paketleri, diğer veri taşıyıcılarına aktarım sırasında da şifreli kalır. Böylece, şifrelenmiş bir dosya kalıcı olarak şifrelenirken bir e-posta ekine kopyalanabilir veya web tabanlı bir buluta yüklenebilir. Harici bilgisayarlarda ve mobil cihazlarda, dosya bir parola girilerek veya bir PKI belirteci kullanılarak açılabilir.

Android / iOS Şifrelemesi (Android / iOS Encryption)

İOS ve Android cihazlar için şifreleme, uygulama yoluyla mobil cihazların dahili depolarında, bellek kartlarında ve bulut hesaplarında dosya tabanlı koruma sağlar. Bir şifre girilerek dosyaların şifresi çözülür.

Otomatik Uç Nokta Algılama & Yanıtlama

Gücünü enSilo' dan almaktadır

Yazılım, uç nokta güvenlik önlemleri işlevlerini uç nokta algılama ve yanıt (EDR) işlevleriyle birleştiren ve uygulamaların iletişiminin denetimini sağlayan bir veri koruma platformudur. Ve bunu gerçek zamanlı olarak yapıyor.

Buradan fonksiyonel tanımlarla ilgili broşürü indirebilirsiniz.

Uç cihazları otomatik olarak güvenli hale getirin ve saldırılara karşı koyun

Bugün, EgoSecure Uç Nokta Güvenlik Yazılımı fidye yazılımlarına ve diğer saldırılara karşı önemli bir koruma faktörüdür. Yazılım, virüsten koruma çözümlerinin ve güvenlik duvarlarının sunabileceğinin çok ötesine geçen kötü amaçlı yazılımlara karşı ek bir koruma katmanı sağlar. Güvenlik politikalarını uygulamanıza ve sürdürmenize de yardımcı olur.Uç cihazlarınızı bir ajanla güvence altına alıyoruz. Yazılım, çok kademeli bir savunma sistemi ile fidye yazılımı ve bilinmeyen saldırılara karşı savunmaya yardımcı olur. Gelişmiş makine öğrenimi teknolojileri ve davranış analizi içeren çözüm, korumayı en üst düzeye çıkarır ve yanlış pozitifleri en aza indirir. Örneğin, ortak uygulamalardaki bellek tabanlı güvenlik açıklarından yararlanan sıfır gün saldırılarını engellemenize yardımcı olur.

Sağladığı artı değerler

Kötü amaçlı yazılımların girmesi her zaman önlenemez. EgoSecure, başlangıç noktalarını yetkisiz veri aktarımına karşı korur. Bu, BT'nize olası güvenlik açıkları için giriş kapılarını analiz etmek ve karşı stratejiler geliştirmek için yeterli zaman sağlar.

✓ Gerçek zamanlı veri hırsızlığının önlenmesi

EgoSecure, işletim sistemi düzeyinde çalıştığı için verileri gerçek zamanlı olarak hırsızlığa karşı korur. Bu, verilerin çalınmasını önler.

✓ Fidye yazılımlarına karşı gerçek zamanlı koruma

EgoSecure, veriler şifrelenmeden önce Bad Rabbit gibi saldırganları durdurur. İşletim sistemi düzeyinde çalışır ve bu nedenle tek evrensel çözümdür.

✓ Sorunsuz güvenlik, gerçek zamanlı veri hırsızlığını önler

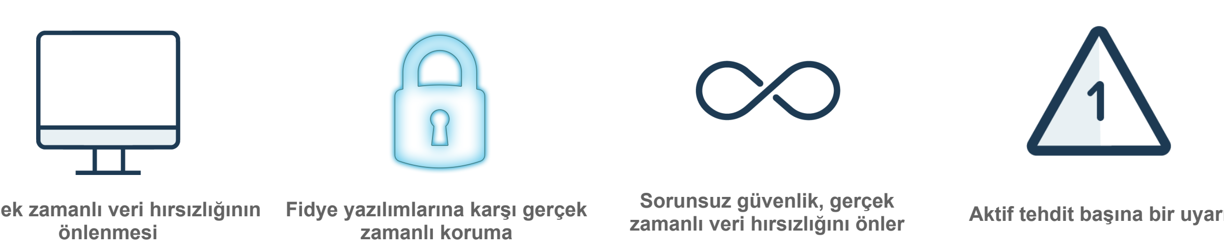
Güvenliğin iş süreçleri üzerinde olumsuz bir etkisi olmamalıdır. Sıkıştırılmış bir sistemde bile çalışmaya devam edebilmelisiniz.

✓ Aktif tehdit başına bir uyarı

EgoSecure, yalnızca kötü niyetli giden iletişimi, veri manipülasyonunu veya yetkisiz şifrelemeyi önledikten sonra sizi uyarır.

İşlevsellik

Yazılım, uç nokta güvenlik önlemleri işlevlerini uç nokta algılama ve yanıt (EDR) işlevleriyle birleştiren ve uygulamaların iletişiminin denetimini sağlayan bir veri koruma platformudur. Ve bunu gerçek zamanlı olarak yapıyor.



ENSILO TOPLAYICI

Aşama 1:
Toplayıcı kaydedilmiş İşletim sistemi meta verileri.

TUTARLILIKLA İLİŞKİN FAALİYETLER

Aşama 2:
Bağlantı kurulumu veya dosya değişikliği sırasında çekirdeğe bir anlık görüntü gönderilir.

ENSILO CORE

Aşama 3:
Çekirdek meta verileri analiz eder ve veri hırsızlığı veya fidye yazılımı saldırısını önler.

Aşama 4:
Yalnızca yasal bağlantılar veya dosya değişiklikleri onaylanır.

Yazılım videosunu izleyin

Gerçek zamanlı veri hırsızlığının önlenmesi

enSilo, işletim sistemi düzeyinde çalıştığı için verileri gerçek zamanlı olarak hırsızlığa karşı korur. Bu, verilerin çalınmasını önler.

Fidye yazılımlarına karşı gerçek zamanlı koruma

enSilo, veriler şifrelenmeden önce Bad Rabbit gibi saldırganları durdurur. İşletim sistemi düzeyinde çalışır ve bu nedenle tek evrensel çözümdür.

Sorunsuz güvenlik, gerçek zamanlı veri hırsızlığını önler

Güvenliğin iş süreçleri üzerinde olumsuz bir etkisi olmamalıdır. Sıkıştırılmış bir sistemde bile çalışmaya devam edebilmelisiniz.

Aktif tehdit başına bir uyarı

enSilo sizi ancak zararlı dışa bağımlı iletişimi, veri işlemeyi veya yetkisiz şifrelemeyi önledikten sonra uyarır.

SİSTEM GEREKSİNİMLERİ

Donanım Gereksinimleri

EgoSecure ürünlerini kullanmak için sisteminizin aşağıdaki minimum donanım gereksinimlerini karşılaması gerekir:

EgoSecure Server

Bileşenler	Minimum	Tavsiye Edilen
RAM	2 GB	4 GB
Boş hard disk alanı	20 GB	50 GB
İşlemci	Dual core	Quad core

EgoSecure Agent (İstemci Bilgisayar)

Bileşenler	Minimum	Tavsiye Edilen
RAM	2 GB	4 GB
Boş hard disk alanı	20 GB	50 GB
İşlemci	Dual core	Quad core

Veritabanı (Database)

EgoSecure Data Protection kullanmak için bir SQL veritabanı gereklidir. Gerekli sabit disk alanı, ürün kullanımına bağlı olarak büyük ölçüde değişir.
Veritabanının varsayılan otomatik büyüme ve maksimum boyut parametrelerini değiştirmemenizi öneririz.
Secure Audit (Güvenli Denetim) modülü, özellikle diğer modüllerle birlikte büyük miktarlarda veri üretebilir.

Yazılım Gereksinimleri

EgoSecure ürünlerini kullanmak için sistemin aşağıdaki gereksinimleri karşılaması gerekir. **EgoSecure Data Protection** 13.1'den başlayarak, **EgoSecure Sunucusu** yalnızca 64 bit sistemlere yüklenebilir, ancak **EgoSecure Console**, **Program Files/EgoSecure/EgoSecure Server** altında hem 32 hem de 64 bit sürümlerinde kullanılabilir.

Sunucu (Server)

İşletim sistemi
Windows Server Version 2008 R2, 2012, 2012 R2, 2016 veya 2019
Windows Vista, 7, 8, 8.1 veya 10

Varolan bir SQL Server'ı kullanabilir veya ayrı bir SQL Server yükleyebilirsiniz.

SQL Sunucu (SQL Server)
Microsoft SQL Server: 2008 R2 Express Edition, 2008 R2, 2012 Express Edition, 2012, 2014 Express Edition, 2014, 2016 Express Edition, 2016, 2017 Express Edition, 2017, 2019
MySQL Community Server 5 ve üstü

İstemci (Client)

İşletim sistemi
Windows XP (limitli), Vista, 7, 8, 8.1 veya 10
Mac OS

Destekledikleri
Windows Terminal Server
Citrix XenApp®
Citrix XenDesktop®

Windows XP için sınırlı destek

EgoSecure Server' ın yüklenmesi Windows XP'de desteklenmez.
EgoSecure Agent' ların Windows XP'ye yüklenmesi yalnızca kısmen desteklenmektedir.
Aşağıdaki işlevler desteklenmez veya düzgün çalışmaz:

» Secure Audit (Güvenli Denetim): İnternet denetimi
» BitLocker Encryption
» Windows Çevrimdışı dosyaları devre dışı bırakma
» External media (Harici ortam) gibi sabit diskleri denetleme
» Mobil cihazların tanınması

EGOSECURE GmbH
Pforzheimer Straße 128a
76275 Ettlingen
Germany

Phone +49 (0)7243 354 95 - 0
Mail contact@egosecure.com
www.egosecure.com

EGOSECURE
ENJOY DATA PROTECTION

Türkiye Distribütörü

IMPEKS IT GROUP
Impeks Bilgisayar
+90 212 909 10 23
http://www.impeks.com

MATRIX42 EGOSECURE
A MATRIX42 COMPANY