Kaspersky® Embedded Systems Security

Gömülü sistemler için tasarlanan hepsi bir arada güvenlik teknolojisi

Tehdit ortamı sürekli gelişerek; kritik iş süreçlerini, gizli verileri ve finansal kaynakları sıfır saniye açıklarından dolayı daha fazla riske sokmaktadır. İşletmenizdeki riski azaltmak için sizi hedef alan siber suçlulardan daha akıllı, daha iyi donanımlı ve daha bilgili olmanız gerekir.

Günümüzde bilet makineleri, ATM'ler, kiosklar, Satış Noktası (POS) sistemleri ve medikal ekipmanlar gibi birçok alanda Gömülü sistemler kullanılmaktadır. Gömülü sistemler genellikle coğrafi olarak farklı bölgelerde bulunduğu, yönetimi zor olduğu ve nadiren güncellendiği için güvenlik açısından özel bir önem taşır. Ayrıca nakit para ve kredi kartı bilgileriyle çalıştıkları için hataya karşı son derece dayanıklı ve dirençli olmaları gerekir. Gömülü sistemlerin yalnızca tehditlere karşı korunuyor olması yeterli değildir. Aynı zamanda siber suçlular ve içerideki saldırganlar tarafından kurumsal ağa giriş noktası olarak kullanılamaz olmalıdır.

Gömülü cihazlar için standart güvenlik düzenlemeleri, genellikle yalnızca virüsten koruma tabanlı güvenlik ve sistem güçlendirmesini kapsar, bu da yeterli değildir. Tamamen virüsten koruma tabanlı bir yaklaşım, mevcut gömülü sistem tehditleri karşısında yeterince etkili değildir. Yakın zamanda gerçekleştirilen saldırılarda da bu durum fazlasıyla görülmüştür. Artık Cihaz Kontrolü ve Baştan Yasaklı gibi başarısını kanıtlamış teknolojilerin yanı sıra gerektiğinde kritik sistemlere ek antivirüs koruması uygulanmalıdır.

Çözümün Öne Çıkan Özellikleri

Uygun Maliyetli Donanım

Kaspersky Embedded Systems Security, uygun maliyetli donanımlarda bile etkili bir şekilde çalışması için özel olarak tasarlanmıştır. Verimli tasarımı sayesinde sistemlerde aşırı yüklenme olmadan güçlü koruma sağlanır. "Default Deny only" (Yalnızca Baştan Yasaklı) modunda çalışırken Windows XP ailesi için 256 Mb RAM ve sistem hard diskinde 50 Mb boş alan yeterlidir.

Windows XP İçin Optimize Edilmiştir

Gömülü sistemlerin çoğu artık desteklenmeyen Windows® XP ailesi işletim sisteminde çalışır. Kaspersky Embedded Systems Security, Windows XP platformunun yanı sıra Windows 7, Windows 2009 ve Windows 10 ailelerinin tam işlevselliğiyle çalışacak şekilde optimize edilmiştir.

Lider birçok uç nokta güvenliği tedarikçisi Windows XP'ye destek vermeyi sonlandırırken Kaspersky Embedded Systems Security, öngörülebilir geleceğe yönelik olarak Windows XP ailesi için %100 destek sağlamaya devam etmektedir.

Varsayılan Olarak Reddet

Son 10 yılda Tyupkin, Skimer, Carbanak ve aileleri dahil olmak üzere özellikle Gömülü sistemlere saldırmak için geliştirilen kötü amaçlı yazılımların sayısı artmıştır. Geleneksel antivirüs çözümlerinin çoğu bu tür gelişmiş ve hedefli kötü amaçlı yazılım tehditlerine karşı tam koruma sağlayamaz. Klasik bir kötü amaçlı yazılıma karşı koruma çözümü, kötü amaçlı yazılımlara dayalı olmayan ve bunun yerine farklı bir saldırı yaklaşımıyla ara yazılım kullanan birçok hedefli tehdidi önleme konusunda yetersizdir. Baştan Yasaklı işlevi, yazılım koruması haricinde hiçbir yürütülebilir dosya, sürücü ve kitaplığın Güvenlik Yöneticisi'nin onayı olmadan çalıştırılamayacağı anlamına gelir.

Cihaz Kontrolü

Kaspersky Lab'in Cihaz Kontrolü özelliği, sistem donanımına fiziksel olarak bağlı veya bağlanmaya çalışan USB depolama cihazlarını kontrol etme olanağı sunar. Yetkisiz cihazların erişiminin önlenmesi, siber suçlular tarafından kötü amaçlı yazılım saldırısının ilk aşaması olarak sıklıkla kullanılan önemli bir giriş noktasını engellemenizi sağlar.

SIEM entegrasyonu

Kaspersky Embedded Systems Security, artık uygulama günlüklerindeki olayları syslog sunucusu tarafından desteklenen formatlara dönüştürebilir. Böylece bu olaylar tüm SIEM sistemlerine iletilebilir ve başarılı bir şekilde tanımlanabilir.

Bellek koruması

Kaspersky Embedded Systems Security, belleği açıklardan yararlanan yazılımlara karşı korur. Dinamik yüklü bir Süreç Koruma aracı korumalı süreçlere yerleştirilir. Bu aracı, süreçlerin bütünlüğünü izler ve güvenlik açıklarından yararlanma riskini azaltır.

Merkezi Yönetim

Güvenlik ilkeleri, imza güncellemeleri, antivirüs taramaları ve sonuç derlemesi Kaspersky Security Center adlı tek bir merkezi yönetim konsolu aracılığıyla kolaylıkla yönetilebilir. Yerel ağdaki tüm aracılar, her türlü yerel konsolla yönetilebilir. Bu özellik, Gömülü sistemlerde sıklıkla karşılaşılan izole ve bölünmüş ağlar için son derece önemlidir.

Bakım ve destek

Dünya genelinde 200'den fazla ülkede, 34 ofisimizle hizmet veriyoruz. 24/7/365 global destek anlayışımız Maintenance Service Agreement (MSA) destek paketlerine de yansımıştır.

Profesyonel Hizmetler ekibimiz, Kaspersky Lab güvenlik kurulumunuzdan maksimum düzeyde yararlanmanız için sürekli nöbettedir.

Gömülü sistemlerinizi daha etkili bir şekilde korumakla ilgili daha fazla bilgi edinmek için lütfen www.kaspersky.com/enterprise adresini ziyaret edin

Tüm USB cihaz bağlantıları izlenir ve analiz edilir. Bu sayede uygun olmayan USB kullanımı, olay soruşturması ve yanıt süreçlerinde olası bir saldırı kaynağı olarak tanımlanabilir.

Koruma Duvarı ve CD/DVD yönetimi

Bazı gömülü sistem saldırılarının yapısı nedeniyle içerideki kötü niyetli kişilerin faaliyetlerine karşı koruma sağlama kritik önem taşır. Etki alanı dışından çalışan yerleşik sistemler her zaman hem dahili CD/DVD hem de USB depolama sürücüleri için merkezi olarak yönetilen Cihaz Denetimleri ve bir güvenlik duvarı tarafından korunmalıdır.

Dosya Bütünlüğünü İzleme

Dosya Bütünlüğünü İzleme, belirtilen dosyalar ve klasörler kapsamında gerçekleştirilen eylemleri izler. Ayrıca izleme kesintiye uğradığı dönemlerde dosya değişikliklerinin takip edilmesini sağlayabilirsiniz.

Günlük Denetimi

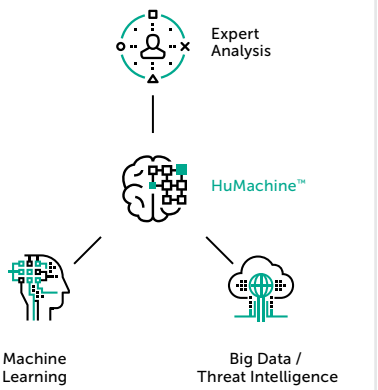
Kaspersky Embedded Systems Security, korunan ortamın bütünlüğünü Windows Olay Günlükleri'nin denetimine dayalı olarak izler. Uygulama, siber saldırı girişiminin belirtisi olabilecek anormal davranışlar konusunda yöneticiyi uyarır.

Çözüm, Windows olay günlüklerini inceleyerek kullanıcı veya Sezgisel Analiz Aracı ayarları tarafından belirtilen kurallara bağlı olarak güvenlik ihlâllerini tespit eder.

Virüsten Koruma Yazılımı ve Kaspersky Security Network

Antivirüs, isteğe bağlı bir modül olarak sunulur. Uygun maliyetli sistemlerin kısıtlamaları nedeniyle klasik bir "kötü amaçlı yazılıma karşı koruma yaklaşımı" kullanmak mümkün değildir ve bu özel tehdit ortamında büyük ölçüde etkisizdir. Kaspersky Embedded Systems Security, Cihaz Kontrolü ve Baştan Yasaklı modunda kurulduğunda genellikle ek antivirüse gerek kalmaz. Ancak ihtiyaç duyarsanız ek güvenlik düzeyi olarak sisteme ilave edebilirsiniz.

Ayrıca Kaspersky Lab, açıklardan yararlanan yazılım tabanlı güvenlik risklerini önlemek ve reaksiyon süresini en aza indirmek için Kaspersky Security [illegible] tabanı gibi akıllı bir güvenlik çözümünün kullanılmasını önerir.



Kaspersky Lab
Kurumsal Güvenlik: **www.kaspersky.com.tr/enterprise**
Siber Tehdit Haberleri: **www.securelist.com**
BT Güvenliğiyle İlgili Haberler: **business.kaspersky.com.tr/**

#truecybersecurity
#HuMachine

www.kaspersky.com.tr