



Matrix42 İşbirliği ile En İyi Uç Nokta Güvenliği Açıklandı ve İncelendi

MATRIX42

#KingstonIsWithYou

Matrix42 İşbirliği ile En İyi Uç Nokta Güvenliği Açıklandı ve İncelendi



Giriş

Bilgi ve veri güvenliği, günümüz dünyasında işletmeler, devletler ve bireyler için en temel gereksinimlerden biridir.

Veri ihlalleri, bilgisayar korsanlığı (hacking) ve insan unsuru, dünya çapında tehdit ve risklerin sürekli gündemde kalmasına neden olmaktadır. Veri ihlallerinin neden olduğu hem parasal hem de itibar kaybı maliyetleri astronomik düzeyde olabilir. Gelişmiş siber güvenlik gereksinimleri ve uç nokta DLP (data loss protection - veri kaybı koruması) stratejileri, güvenilir ve etkili veri saklama ve bellek sistemlerine dayanmaktadır.

Şifreleme, hızlı veri saklama sistemleri ve belleğin, en iyi uygulamalar, standartlar ve politikalar ile kullanılması önemli bir adımdır. Kaybedilen dizüstü bilgisayarlar ve USB bellekler, hem bireyleri hem de şirketleri, kişisel ve özel bilgilerinin ifşa olması riskiyle karşı karşıya bırakmaktadır. Kingston, mevcut ya da geliştirilmekte olan bir güvenlik planı oluştururken risklerin azaltılmasına yardımcı olacak tehdit önleme çözümleri sunmaktadır.



Matrix42 İşbirliği ile En İyi Uç Nokta Güvenliği Açıklandı ve İncelendi

İçindekiler

Bu kısa e-Kitap'ta uç nokta çözümleri ve Kingston'ın şifrelenmiş USB belleklerinin, özelleştirme programının ve Matrix42 EgoSecure Data Protection yazılımının, altı farklı endüstri sektörünün karşı karşıya olduğu sorunların çözümüne ve onlara kendi iş gereksinimlerine uygun bir çözüm sunulmasına nasıl yardımcı olduğu anlatılmaktadır.

Bu altı sektörü derinlemesine inceledik ve uç nokta güvenliğinde karşı karşıya kaldıkları zorluklarla nasıl baş ettiklerini öğrendik.

İçindekiler

Bölüm 1	Endüstride Kullanım Örneği – Kamu Sektörü	4
Bölüm 2	Endüstride Kullanım Örneği – Sağlık	5
Bölüm 3	Endüstride Kullanım Örneği – Finans	6
Bölüm 4	Endüstride Kullanım Örneği – Otomotiv	7
Bölüm 5	Endüstride Kullanım Örneği – Telekomünikasyon	8
Bölüm 6	Endüstride Kullanım Örneği – Üretim	9
Bölüm 7	Kingston ve Matrix42 Çözümleri	10
	Özet	11
	Kingston hakkında	12



Bölüm 1: Endüstride Kullanım Örneği

Kamu Sektörü



Durum:

Kamu sektöründe, USB bellekler yaygın biçimde kullanılıyor. Örneğin kamu düzeni birimlerinin, park ihlali yapanların ve idari suçlar işleyenlerin görevliler tarafından çekilen fotoğraflarını USB kablo üzerinden kurumların sistemlerine kopyalaması gerekiyor. Polis yetkilileri inceleme verilerini harici veri saklama cihazlarında alıyorlar. Bu verilerin yeniden yazılması gerekirken aynı zamanda yetkisiz kişilerce erişime karşı korunması gerekiyor.

Zorluk:

USB cihazlara olan yoğun talepler nedeniyle çalışanlar düzenli olarak USB bellekler istiyorlar. Özel ve yetkisiz veri saklama cihazlarının kullanımının, güvenlik nedenlerinden dolayı engellenmesi gerekiyor. Bir çalışanın, yeni bir USB veri saklama cihazına ihtiyacı varsa, çalışanların işinin aksamaması için bu cihaz, Kullanıcı Yardım Masası tarafından en kısa zamanda sağlanmalıdır. Uygun USB cihazların kullanılmasından hiçbir güvenlik sorunu çıkmadığını belirtmek önemlidir.

Çözüm:

Cihaz kontrolünü, veri filtrelemesini bir araya getirerek aşağıdaki senaryo uygulanabilir:

Bilinmeyen cihazlar genellikle bilgisayar uç noktalarında engellenir. Dijital kameralar gibi veri saklama cihazlarına yalnızca görüntü dosyalarının okunması gibi belirli işlevler için izin verilir. Yazma işlemleri genellikle şifrelenir ve yalnızca yetkilendirilmiş USB cihazlarında bulunmasına izin verilir. Tüm veri erişimleri günlüklere kaydedilir. Yetkilendirilmiş cihazların yönetimi, özelleştirilmiş seri numaraları ve donanım kimlikleri ile basitleştirilebilir. Dolayısıyla Matrix42 Service Management, kullanıcının Self-Servis Portal'da kişiselleştirilmiş bir Kingston Technology USB Bellek talebinde bulunmasını sağlar. Onay sürecinden sonra USB cihazına, EgoSecure Data Protection'da kullanılmak için otomatik olarak izin verilir.

“Çalışanlarımız, yeni USB cihazlarının kısa bir onay sürecinden sonraki kolayca ve hızlıca sağlanmasından dolayı heyecanlılar. Kingston Technology'nin özelleştirme programından ve Matrix42'nin hizmet yönetimi ve uç nokta güvenliği kombinasyonunun kolay yönetiliyor olmasından dolayı çok memnunuz.”

Yardım Masası Müdürü, Kamu Sektörü

Bölüm 2: Endüstride Kullanım Örneği Sağlık



Durum:

Harici veri depolama cihazları, çalışanlar ve diğer kurumlarla veri alışverişinde sık kullanılan bir yöntem olmaya devam ediyor.

Örneğin Almanya'daki hastanelerin, Kanseri Sicili'ne geçerli kanser vakaları ve onların ilerlemesi ile ilgili bilgiler sağlaması gerekiyor. Kolaylık açısından bu veriler genellikle mobil veri saklama cihazlarında aktarılıyor.

Doktorlar da araştırma verileri gibi belgeleri derslerine USB belleklerle götürüyor.

Zorluk:

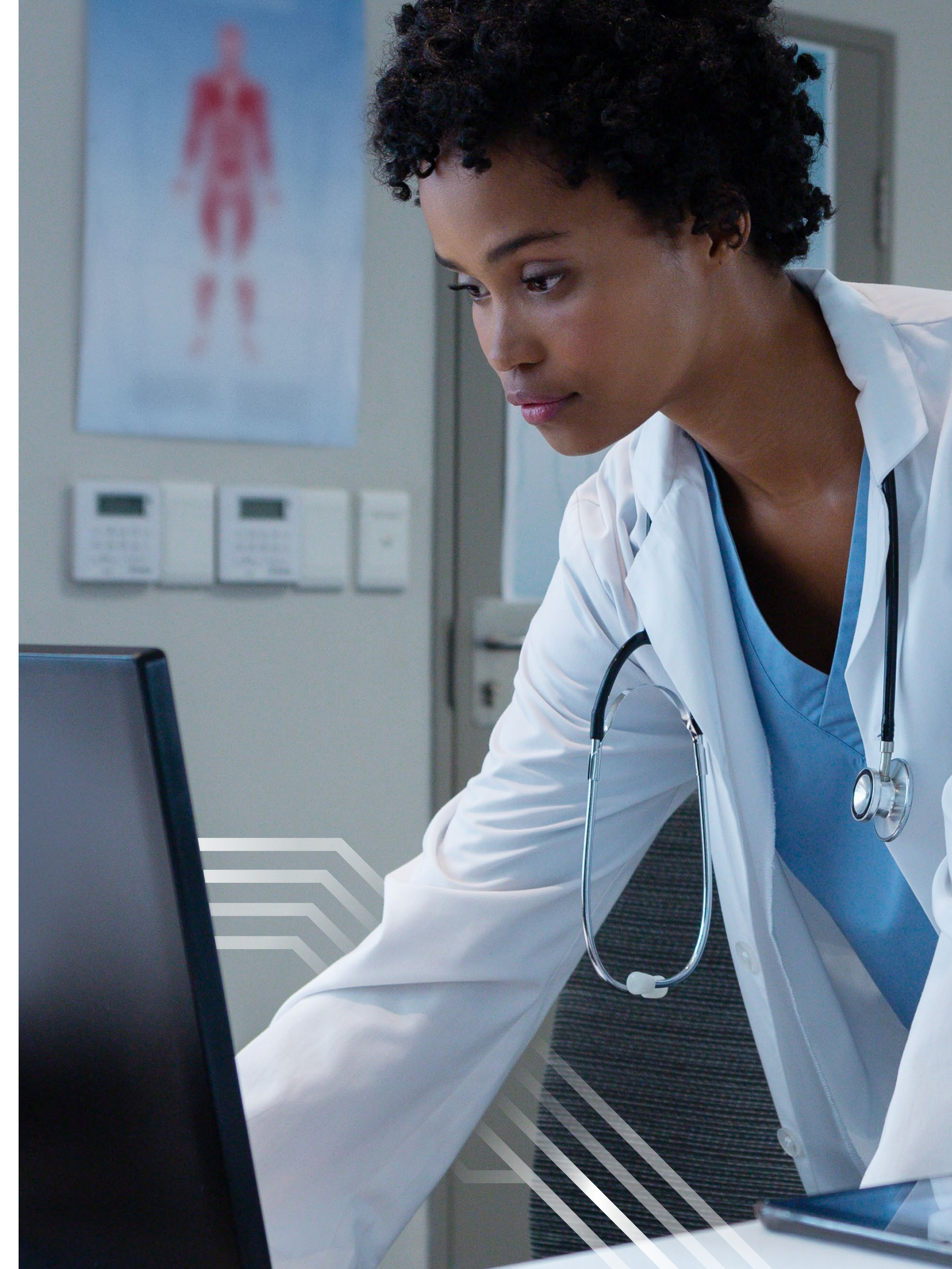
Hasta verileri çok hassastır ve yetkisiz kişilerin ellerine düşmemelidir. Dolayısıyla veri koruması artırılmalı ve güçlendirilmelidir. Verinin taşındığı birim kaybolursa, sadece GDPR açısından değil hastaların iyiliği açısından da büyük sorunlar ortaya çıkabilir. Bu nedenle, USB veri saklama birimlerine erişimin kontrollü, izlemeli ve şifrelemeli olması önemlidir.

Çözüm:

EgoSecure Data Protection, erişim kontrolü, veri denetimi, filtreleme ve şifreleme gibi çeşitli koruma önlemlerini tek çözüm altında bir araya getiriyor. IT yöneticileri, hangi çalışanların hangi cihazlara erişebileceğini belirleyebiliyor. Örneğin seri numarasına ya da donanım kimliğine göre istisnalar yapılabilir. Bu tanımlayıcılar, Kingston Technology'nin özelleştirme programıyla tanımlanabildiğinden EgoSecure Data Protection yönetiminde sadece şirket tarafından onaylanmış cihazların kullanılmasına izin vermek için yalnızca bir değer yapılandırılması yeterli oluyor. Bu durum, idari işleri önemli miktarda azaltıyor ve erişimin şifreli ve izlemeli olması dolayısıyla veri güvenliğini (GDPR, CCPA, HIPAA, vb.) artırıyor.

“ Zaten Kingston şifrelenmiş USB bellekler kullanıyorduk. Artık EgoSecure Data Protection sayesinde hasta verilerinin aktarılmasının izlenebilirliğinin EU-GDPR'ye uygun olduğundan da emin olabiliyoruz. ”

CISO, Üniversite Hastanesi



Bölüm 3: Endüstride Kullanım Örneği

Finans



Durum:

Bankalar, çeşitli uyum gereksinimlerine tabidir. Bu gereksinimlerden bir tanesi PCI-DSS (Payment Card Industry Data Security Standard - Ödeme Kartları Endüstrisi Veri Güvenliği Standardı) uyumudur. PCI-DSS gereksinimleri arasında veri şifreleme gereksinimi, saldırıya açıklık analizi ve veri filtreleme gösterilebilir. Hedef, tehditleri ve IT güvenlik risklerini en aza indirmek ya da tamamen önlemektir.

Zorluk:

Uç noktada IT güvenliği açısından birçok risk bulunuyor. Çalışanların her gün tüketiciler ve işletmelerden ödeme kartı bilgileriyle çalışması ve finansal kurumlardan gelen hassas verileri işlemesi gerekiyor. Dolayısıyla bulut, e-posta, USB ve web'den gelen verilerin, kötü amaçlı yazılımlar tarafından tehlikeye atılması ya da verilerin, yeterli düzeyde korunmadığında yanlışlıkla üçüncü şahısların ellerine geçmesi tehdidiyle karşı karşıyadırlar. Bu tür bir olay bir banka açısından, GDRP, PCI-DSS ve Sarbanes-oxley yasası kapsamında finansal sonuçlar doğurma riski ortaya koyuyor. Ayrıca siber suçlular, bankacılık sistemlerini çeşitli şekillerde etkilemeye ya

da manipüle etmeye çalışıyor ve bu konuda her geçen gün daha yaratıcı hale geliyorlar. Örneğin yakın zamanda paraları çalmak için ATM'lerin güç beslemesinin kesildiği ve sistemin açılış yapılabilir bir USB cihaz ile başlatıldığı bir siber suç işlendi.

Çözüm:

IT sistemleri, çok katmanlı koruyucu önlemlerle korunmalıdır. Bu koruma, uygulama kontrolü, cihaz kontrolü, anormallik tespiti, UEBA (User and Entity Behaviour Analytics - Kullanıcı ve Varlık Davranışı Analizi), izleme ve Açılış Öncesi Kimlik Doğrulama tam disk şifreleme ile sağlanabilir. Matrix42, sadece yetkilendirilmiş uygulamalara ve şifrelenmiş USB cihazlara izin verilmesi için bunu bir otomatik ve entegre ekosistemde sunabilir. Ayrıca şüpheli ya da kötü amaçlı etkinlikler otomatik olarak tespit edilir ve otomatik olarak daha ileri tedbirler başlatılır. Konu USB belleklerin kullanılması olduğunda, Kingston Technology'nin özelleştirilmiş USB bellekleri, cihazların minimum çaba ile beyaz listeye eklenmesine ve verilerin izlenebilir şekilde şifrelenmesine yardımcı olur. Bu durum uyumu, ekstra bir çalışma yapmadan önemli ölçüde artırır.

“ EgoSecure Data Protection ve beyaz listeye ekleme işlevi ile sadece Kingston'ın şifrelenmiş USB belleklerinin onaylanmasına izin veriyoruz. Kişiselleştirilmiş donanım kimliğine sahip Kingston şifrelenmiş USB bellekleri beyaz listeye alıyoruz. Diğer cihazlara izin verilmiyor. Bu durum hem idari işleri önemli ölçüde azaltıyor hem de güvenliği artırıyor! ”

IT Müdürü, Finans Şirketi



Bölüm 4: Endüstride Kullanım Örneği Otomotiv

Durum:

Otomotiv sektöründe USB cihazları çeşitli alanlarda kullanılıyor. Örneğin, araştırma verileri, harici veri saklama cihazlarına kaydediliyor ve şirketteki ilgili mühendisler arasında alınıp veriliyor. Üretim makinelerini yapılandırmak için dosyalar IT ortamından otomasyon teknolojileri ortamına aktarılıyor. Tüm bu veriler çok hassastır ve endüstriyel casusluk ve veri hırsızlığına karşı korunmalıdır. Aksi takdirde elde edilmiş olan bilgi birikimi yanlış ellere geçebilir.

Zorluk:

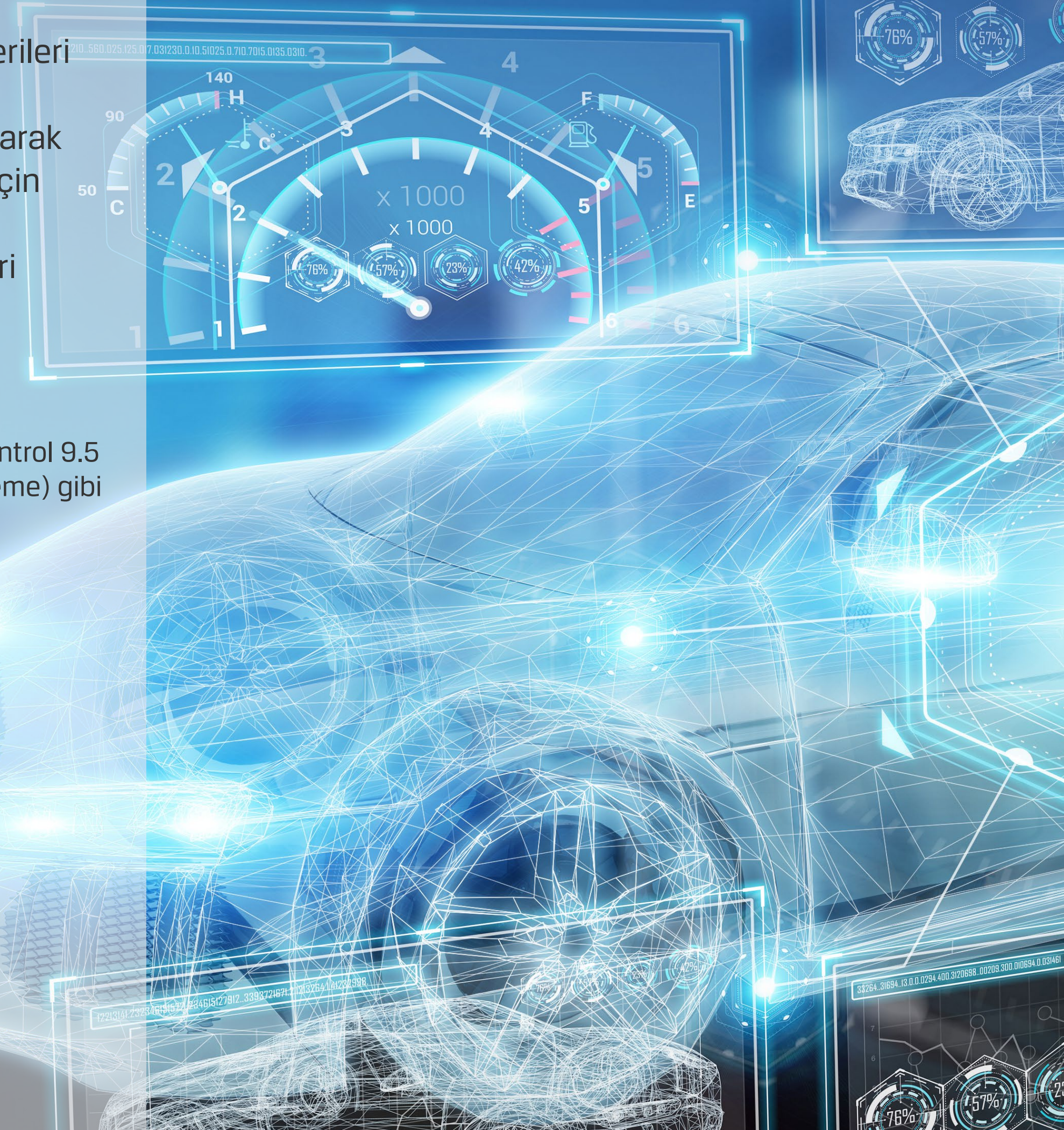
Otomotiv endüstrisi, TISAX, prototip koruması, ENX, ISO27001, "üçüncü şahıs bağlantı" ve GDPR gibi uyum gereksinimlerine tabidir. TISAX'da, Kontrol 9.1, 9.5 ve 10.1 maddeleri, veri erişiminin kontrollü, izlemeli, filtrelenmiş ve şifrelenmiş olmasını gerektiriyor. Bu önlemler, otomotiv şirketlerinin her alanında GDPR ve ISO27001 gibi diğer uyum gereksinimleri için de uygulanmalıdır.

Çözüm:

Kingston Technology şifrelenmiş USB bellekleri, verileri donanım tabanlı şifreleme ile koruyor. Bu cihazlar, EgoSecure Data Protection tarafından otomatik olarak belirli bir veri kullanımı için beyaz listeye alınmak için kullanılabilecek bir kişiselleştirilmiş seri numarası ve donanım kimliği alabiliyor. Ayrıca veri hareketleri izlenebiliyor ve şüpheli bir etkinlik olduğundan analiz edilebiliyor.

“Matrix42 ve Kingston Technology sayesinde kullanıcı davranışından önemli bir değişiklik olmadan TISAX'ın Kontrol 9.5 (bilgilere ve uygulamalara erişim) ve Kontrol 10.1 (şifreleme) gibi gereksinimlerine uygun hale geldik.”

CTO, otomotiv tedarikçisi



Bölüm 5: Endüstride Kullanım Örneği Telekomünikasyon

Durum:

Telekomünikasyon sağlayıcılarının elinde müşterileriyle ilgili çok miktarda bilgi bulunuyor. Bu bilgiler özellikle GDPR açısından çok hassastır. Dolayısıyla veri kaybı ya da veri çalınmasını önlemek için yeterli önlemler alınmalıdır.

Zorluk:

Telekomünikasyon şirketlerinin çalışanları, her gün müşteri verileri üzerinde çalışıyorlar. Verilerin çoğu iş uygulamalarında saklanıyor. Ancak, müşteri kontratlarının, hatta veri tabanı dışarı aktarma dosyalarının uç noktalarda ve bunlara bağlı harici cihazlarda saklanması riski bulunuyor. Kullanıcılar, veri alışverişi için genellikle harici veri saklama cihazlarını kullanıyor. Dolayısıyla yanlış veri saklama uygulamalarının tespit edilmesi ve düzeltilmesi ya da koruma sağlanması çok önemlidir.

Çözüm:

Satın alma sürecini kolaylaştırmak için kişiselleştirilmiş Ürün Kimliğine sahip Kingston Technology şifrelenmiş USB bellekleri, EgoSecure Data Protection'da önceden tanımlanmış beyaz liste üzerinden kolayca satın

alınabilir ve Matrix42 Service Catalog üzerinden teslim edilebilir. Hassas bilgilerin yer alabileceği veri saklama ve dışarı aktarma işlemleri, ve "kullanılan veri" ve "saklanan" taramalarını temel alan derinlemesine içerik incelemesi ile otomatik olarak tespit edilebilir ve düzeltilebilir. Veri hareketleri merkezi olarak günlüklere kaydedilir. Dolayısıyla çalışan, yeni veri saklama donanımına talepte bulunduktan ve talebi onaylandıktan kısa bir süre sonra alabilir. Bu durum GDPR ile uyumlu olmasını garanti edebilir.

“ Matrix42'in self-servis portalı sayesinde kullanıcılarımız ihtiyaçları olan veri saklama ortamını talep edebiliyorlar. Sipariş onaylandığında ve teslim edildiğinde cihaza, EgoSecure'un cihaz kontrolü tarafından izin veriliyor. Matrix42 ve Kingston Technology'nin birlikte kullanılması şirketimizde üretkenliği ve güvenliği artırıyor. ”

CTO, Telekomünikasyon Sağlayıcısı



Bölüm 6: Endüstride Kullanım Örneği Üretim Endüstrisi



Durum:

Geleceğin altını dijital verilerdir. Üretim endüstrisinde bu değerli veriler arasında üretim planları, müşteriler ve tedarikçilerle ilgili bilgiler ve şirket bilgi birikimi sayılabilir. Bu verilerin kaybolması hem GDPR'den dolayı çok ciddi cezalara hem de dolaylı sorunlara ve itibar kaybına neden olabilir. Maalesef her gün taksilerde, çamaşırhanelerde, havalimanlarında, tren istasyonlarında ya da otoparklarda USB bellekler bulunuyor.

Zorluk:

Veri saklama cihazlarında genellikle yüksek düzeyde hassas veriler bulunuyor ve maalesef bu veriler genellikle şifrelenmemiş oluyor. Aynı zamanda servis teknisyenlerinin üretim makinelerine güncellemeleri yüklemek için harici veri taşıma cihazları kullanma riski de bulunuyor. Bu harici cihazlar, ağa kötü amaçlı yazılımların girmesi riskini taşıyor.

Çözüm:

Kingston Technology şifrelenmiş USB bellekleri, verileri donanım tabanlı şifreleme ile koruyor. Bu cihazlar, EgoSecure Data Protection tarafından otomatik olarak belirli bir veri kullanımı için beyaz listeye alınmak için kullanılabilecek bir kişiselleştirilmiş seri numarası ve donanım kimliği ile teslim edilebiliyor. Ayrıca veri hareketleri izlenebiliyor ve şüpheli bir etkinlik olduğundan analiz edilebiliyor.

“ Üretim verilerimizin şifrelemesi, kendimizi veri hırsızlığına karşı korumak için çok önemlidir. Bu yüksek düzeyde hassas verilerin, EgoSecure Data Protection tarafından uygulanan dosya filtrelemesi sayesinde sadece onaylı Kingston şifrelenmiş USB belleklerde bulunmasına izin veriliyor. Tüm diğer USB cihazlarında üretim verileri engelleniyor ve harici veri cihazlarına yazma erişimi, EgoSecure'ın anında şifrelemesi ve günlüğe kaydedilmesi için korumaya alınıyor. ”

IT Güvenlik Müdürü, Üretim Endüstrisi



Şifreleme, hızlı veri saklama sistemleri ve belleğin, en iyi uygulamalar, standartlar ve politikalar ile kullanılması önemli bir adımdır. Kaybedilen dizüstü bilgisayarlar ve USB bellekler, hem bireyleri hem de şirketleri, kişisel ve özel bilgilerinin ifşa olması riskiyle karşı karşıya bırakmaktadır. Kingston Technology, mevcut ya da geliştirilmekte olan bir güvenlik planı oluştururken risklerin azaltılmasına yardımcı olacak tehdit önleme çözümleri sunmaktadır.

Kingston Technology Şifrelenmiş USB Bellekler

Kingston Technology'nin donanım tabanlı şifrelemeli USB belleklerinde, bir kuruluşun güvenlik duvarının içinde ve dışındaki mobil veriler için veri koruma çözümleri bulunmaktadır. Çok yüksek güvenlik gerektiren verilerinizi korumak için tasarlanan bu bellekler, endüstri standartlarının, direktiflerinin ve yönetmeliklerinin gereksinimlerini karşılamaya yardımcı olurlar. Ürünler TAA uyumludur, FIPS sertifikalıdır ve 128GB'a varan kapasitelerde sunulmaktadır. Bu sayede hem kurumsal hem de devlet kurumları için ideal bir tercihtir.



Güvenli Özelleştirme Programı

Kingston'in şifrelenmiş USB belleklerini, organizasyonunuzun gereksinimlerini karşılayacak çeşitli şekillerde özelleştirebilirsiniz. Benzersiz, vazgeçilmez bellekler oluşturmak için seçilen özellikleri ekleyin. Kingston Technology, tercih ettiğiniz satıcı ya da dağıtıcı üzerinden size özel şifrelenmiş USB belleği kolayca ve rahatça sipariş etmenizi sağlar. Kingston Technology'nin şifrelenmiş USB bellekleri serisinde DTVP30, DT4000G2 ve IKD300S yer almaktadır. Bu program, seri numaralandırma, çift parola ve özel logolar dahil olmak üzere müşteriler tarafından sık sık istenen seçenekleri sunmaktadır. En az 50 parça sipariş ve 25 parça yeniden sipariş edilmesinin gerektiği program, kuruluşunuzun gereksinimlerini tam olarak karşılar.

Matrix42 EgoSecure Data Protection

Matrix42 EgoSecure Data Protection, şirketlere cihazların, sistemlerin ve verilerin önlenmesi ve korunması için 360° güvenlik yönetimi olanağı sunmaktadır. Çözüm, önleme ve tespitten hasar durumunda üretim kaybı olmadan karşı tedbirlerin uygulanmasına kadar her alanda otomasyon sağlamaktadır.

Veri koruması ve siber güvenlik, göz korkutucu bir sorumluluk gibi düşünülebilir. Dijital çalışmanın gereksinimleri, çalışanların ne zaman, nerede ve hangi cihazlarla çalışacağına kendilerinin karar verebilmesiyle önemli ölçüde değişti. Donanım tabanlı şifrelenmiş USB belleklerin ve uç nokta yazılım yönetiminin doğru biçimde birlikte kullanılması, kuruluşların cihazlarının kontrolünü ele geçirmesine yardımcı olabilir. Dolayısıyla veri ihlali riski azaltılabilir ve devam etmekte olan GDPR uyumu stratejileri desteklenebilir.





Kingston hakkında

Kingston Technology 30 yılı aşkın deneyimiyle, kuruluşunuzu tehlikeye atmadan uç nokta güvenliği ile ilgili zorluklarınızı belirleyecek ve çözecek bilgiye sahiptir.

©2021 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. All rights reserved.
Tüm ticari markalar ve kayıtlı ticari markalar, ilgili sahiplerinin mülküdür.

#KingstonIsWithYou