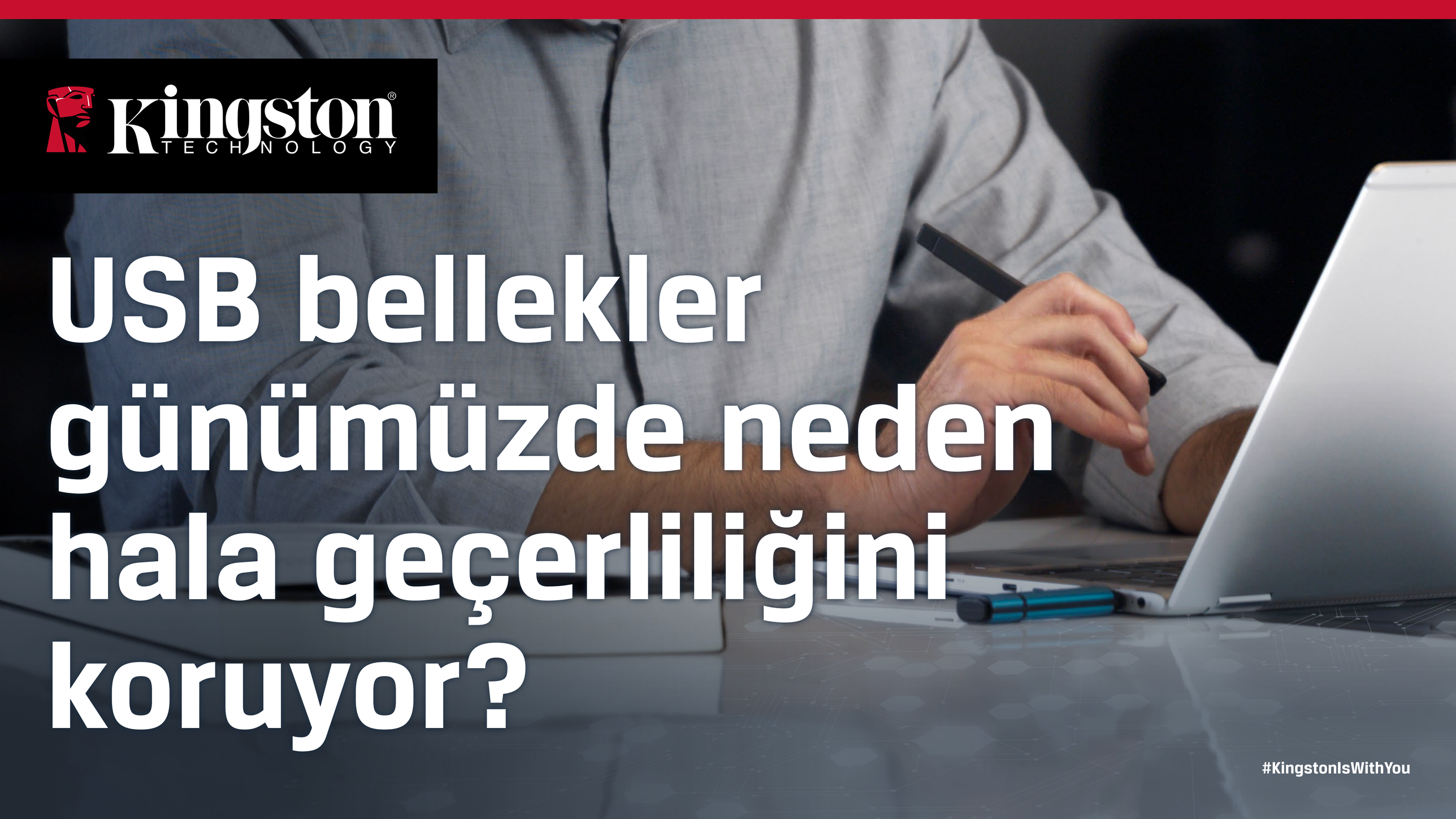

Kingston
TECHNOLOGY
USB bellekler günümüzde neden hala geçerliliğini koruyor?
#KingstonIsWithYou

USB bellekler günümüzde neden hala geçerliliğini koruyor?

Önsöz ve içindekiler

Tüm küresel kurumsal verilerin %60'ının bulutta[1] saklandığı günümüzün dijital çağında, otuz yaşına yaklaşan bir veri saklama teknolojisinin geçerliliğini korumasını tartışmak biraz tuhaf görünebilir. Bununla birlikte, piyasaya sürülmesinden bu yana, veri saklama sistemlerinin temel ürünlerinden bir olan bu ürün, gelişti ve gelişmeye devam ediyor.

USB belleklerin dosyaları, sürücüleri ve uygulamaları aktarmak için standart bir araç olduğu günler çoktan geride kaldı. Günümüzün çözümleri büyük ölçüde artırılmış aktarım hızına sahip olmanın yanı sıra birçok durumda zorunlu olan güvenilir ve güvenli taşınabilir medya da sağlıyor. Peki bulut veri saklama çözümleri görünüşte aynı avantajların çoğunu sunabiliyorken USB bellekler nasıl hala geçerliliğini koruyabiliyor?

Bu e-kitapta USB flash belleklerin, bulut sistemlerin hakim olduğu bir ortamda nasıl konumlandırıldığını ele alacağız. Sektörün önde gelen uzmanlarından bazılarının önemli görüşleriyle desteklenen bu yazıda, günümüz kuruluşlarının USB bellekleri nasıl kullandıklarını inceleyecek ve yazılım tabanlı şifreleme, bağımsız veri saklama ortamları ve uç nokta veri güvenliği açısından yerlerini tartışacağız.

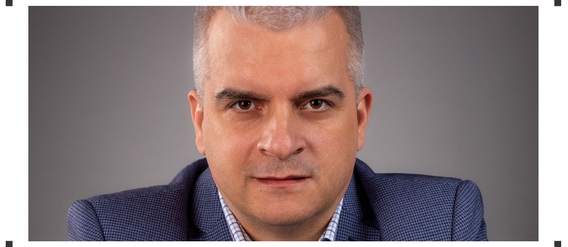
İçindekiler	Sayfalar
Katılımcılar	3
Usb flash belleklerin yükselişi	4
Değişen talebin gereklerini karşılayan taşınabilir veri saklama ortamı	5-6
Şifreleme: Donanım tabanlıya karşı yazılım tabanlı	7-8
Hassas verileri koruma konusunda artan gereksinim	9
Hassas finansal verilerin güvenceye alınması	10
Hasta sağlık verilerine güvenli erişim	11
Bulut veri saklamanın geleceğinde USB bellek	12-13
Özet ve Kingston hakkında	14

Katılımcılar

Bu eKitap, IT ve gelişmekte olan teknolojiler alanında dört endüstri uzmanıyla birlikte hazırlanmıştır.

Rafael Bloom

Rafael, kariyeri boyunca üst düzey Teknoloji Ürünleri, Pazarlama İletişimi ve İş Geliştirme rollerinde görev yaptı. Danışmanlık uygulamaları, teknolojik ve yasal değişikliklerin yarattığı yeni organizasyonel, ürün ve iletişim zorluklarına odaklanmaktadır. Bu çok kapsamlı çalışma, bilgi yönetişimi ve tasarımsal uyum, veri gizliliği ve AdTech, Mobil ve 5G, Yapay Zeka ve Makine Öğrenmesi gibi gelişmekte olan teknolojiler konusunda uzmanlık gerektirmektedir.



Tomasz Surdyk

Tomasz, devletlerde IT güvenliği alanında 24 yılı aşkın deneyimi ile bilgi güvenliği, kişisel veriler ve siber güvenlik konusunda önemli isimlerden biridir. Geçmişte devlet idaresinin yanı sıra NATO ve AB'de gizli bilgileri ve kişisel verileri işleyen ICT sistemlerini ve ağlarını inceledi. Yıllardır ticari bilgilerin ve kişisel verilerin güvenliğini artıran güvenli çözümlerin uygulamaya alınması konusunda uzman bir şirketin sahibi olarak çalışıyor.

David Clarke

David, Thompson Reuter'ın "Birleşik Krallık'ta, risk yönetimi, uyum ve yasal teknolojiler alanında sosyal medyanın en etkili 30 kanaat önderi ve düşünürü" listesinde en etkili 10 kişi arasında ve Kingston Technology'nin En Etkili 50 Global Uzman listesinde yer almaktadır. Geçmişte David Küresel FTSE 100 şirketlerinde Güvenlik Hizmeti Sunumu Küresel Başkanı ve Güvenlik Altyapısı Başkanı gibi güvenlikle ilgili birçok yöneticilik görevini yürüttü.

Usb flash belleklerin yükselişi

İlk Evrensel Seri Veri Yolu (Universal Serial Bus - USB) sürücüsü yirmi yılı aşkın bir süre önce piyasaya çıktığında, genel uyumluluğu, bilgisayar teknolojisi alanında oyunun kurallarını değiştirdi. Birçok cihaz işlemini geniş kitleler için erişilebilir hale getirme yeteneğiyle USB, kısa sürede gelişti ve önemli ölçüde daha hızlı veri aktarımı, USB 3.0 bağlantı noktası ve 2000 yılında ilk USB flash sürücünün piyasaya sürüldüğü zamandakine kıyasla daha da fazla yetenek sunar hale geldi.

O zamandan bu yana teknoloji, mobil veri depolama ve güvenlik ihtiyaçları açısından önemli bir mesafe kat etti. Ana odak noktası, çok özel kullanım durumları göz önünde bulundurularak tasarlanan günümüzün USB bellek neslidir. Kurumsal açıdan bakıldığında, yaygınlaşan uzaktan ve hibrit çalışma, bulut hizmetlerinin kullanımı ve siber güvenlik kaygıları daha etkili çözümlere ihtiyaç duyulmasına neden oluyor. Bunun yanı sıra, yasal zorunluluklar, verilerin yasalara uyumlu bir şekilde saklanmasını gerektiriyor. Bu baskılar "şirket tesisinde" ve bulutta çalışıyor olabilen dağıtık ve karmaşık sistemlerle genellikle daha da artırmaktadır.

Ayrıca belgeler, e-postalar, fotoğraflar, videolar ve meta veriler gibi yapılandırılmış ve yapılandırılmamış veri hacimlerinin artması durumu var. Tüm bunlar değişen kurumsal veri saklama ihtiyaçlarının karmaşıklığını artmasına neden oluyor.

Ancak bulut saklama, bu zorlukların çoğuna cevap verebiliyorsa, USB belleklerin günümüz iş dünyasında geçerliliğini koruyor olmasının nedeni nedir?

> **Birçok kişi USB belleklerin geçmişte biraz tek kullanımlık, düşük performanslı, düşük güvenlikli cihazlar olarak kullanılmaları nedeniyle eski moda ya da önemsiz olduğunu düşünmektedir. - Rafael Bloom**

Değişen talebin gereklerini karşılayan taşınabilir veri saklama ortamı

USB belleklerin, taşınabilir veri saklama aracı olarak kullanıldığı eski kullanım şekilleri kaybolurken, yüksek performanslı USB sürücüler, kişisel, ekstra bir veri koruma ve gizlilik katmanı ile güvenli yerel yedekleme için kullanılmaya başlanmıştır. Bu, İK kayıtları, finansal veriler, sağlık kayıtları, fikri mülkiyet (Intellectual Property - IP) ve tüm kişisel olarak tanımlanabilir bilgiler (Personally Identifiable Information - PII) gibi uyumluluk açısından hassas veriler için son derece önemli olabilir. Ayrıca bu nesildeki cihazlar, hızlı veri aktarımı, saklama, yedekleme ve güvenlik için kullanılabilecek becerilere sahiptir:

- Elden teslim edilmesi gereken düzenlemelere tabi bilgiler
- Tesis içinde ya da dışında teslim edilmesi ve bastırılması gereken Yasal ve Finansal belgeler
- Fidye yazılımlarının bir tehdit olabileceği her türlü tehlikeli olabilecek ortam
- Ağ erişimine izin verilmeyen yerlerde baskı sistemlerine aktarım

Önde gelen şifrelenmiş USB sağlayıcısı olan Kingston Technology, Kingston IronKey™ S1000 gibi çözümleri çıkararak değişen taleplere ayak uydurdu. Sınıfının en iyisi bu şifrelenmiş USB bellek, XTS-AES 256-bit şifrelemenin sunmanın yanı sıra üzerinde oynama yapılmasına karşı güçlü korumalara sahip ayrı bir kripto çipi ile gizli verileri koruma becerisiyle en katı standartları karşılar. Ayrıca FIPS 140-2 3. Seviye Onaylıdır. Bu onay, bir kriptografik donanım parçası olarak etkinliği açısından ABD hükümeti tarafından resmi olarak onaylandığını gösterir ve bu sayede veri koruması söz konusu olduğunda daha fazla iç rahatlığına ihtiyaç duyan kuruluşlar için idealdir.

Bu tür donanımsal şifrelemeli USB bellekler, verileri ister bulut tabanlı ister şirket içinde olsun, merkezi güvenli cihaz yönetimi çözümleri sunar. Yazılım gerektirmemesiyle kullanımı kolay uyumlu şifrelenmiş veri saklama, hızlı ve verimli dağıtım için tasarlanmış çözümler sunarak IT açısından değerli zamanın da serbest kalmasını sağlar.

Değişen talebin gereklerini karşılayan taşınabilir veri saklama ortamı

Yedekleme ve arşivleme, USB belleklerin dijital varlıkları uzun vadede ve 3. taraf Bulut hizmetlerinden bağımsız olarak korumak için kullanılabileceği bir diğer örnektir. Büyük veri aktarımlarının Bulut'ta kolayca gerçekleştirilebildiği doğru olsa da tescilli fikri mülkiyetler, hala internetten uzakta ve güvenli bir şekilde saklanabilen şifrelenmiş, güvenli bir USB bellekte saklanmaya değecek kadar hassas olabilir.

Ayrıca, kuruluşların, özellikle şifrelenmiş sürücüler kullanılarak, verilerin mantıksal ve fiziksel olarak kendi kontrolleri altında olmasını gerektirdiği durumlar her zaman olacaktır. Bunun yanı sıra bir HDD/SSD'de saklanan verilerin şifrelenemeyeceği durumlar vardır. Kingston IronKey D300S gibi harici şifrelenmiş USB belleklerin kullanılması bu sorunu çözmektedir. Bu USB flash bellekte, 128 bit veri bloklarını şifreleyebilen bir tür blok şifreleyici olan XTS 256 bit Advanced Encryption Standard (AES) donanımsal şifreleme bulunur. Ayrıca bundan daha ileri veri şifreleme ihtiyacı doğduğunda AES, önceki modlara göre daha iyi ve daha güçlü veri koruması sağlayabilen XTS blok şifreleyici modunu kullanır.

> Bana göre USB flash bellekler hala kullanılıyor ve veri güvenliğinin ayrılmaz bir parçası. Bu bellekler, bilgilerin cihazlar arasında hızlı bir şekilde aktarılması ve uygun şekilde saklanması ve korunması gibi birçok alanda kullanılmaktadır. - Tomasz Surdyk

Şifreleme: Donanım tabanlıya karşı yazılım tabanlı

Verilerin nasıl şifrelendiğine bakıldığında, donanım şifrelemesinin yazılım şifrelemesine göre daha kolay yönetilebilir ve daha güvenli olduğu söylenebilir. Bunun nedeni şifreleme işleminin ana sistemin geri kalanından ayrı tutulması sayesinde işleme müdahale edilmesinin ve işlemin durdurulmasının daha zor olmasıdır. Merkezi cihaz seviyesi yönetim yazılımı, intranet LAN ve İnternet bağlantıları üzerinden sürücü kontrolüne olanak tanır ve aşağıdakiler için ideal araçlar olabilir:

- Şifrelenmiş bireysel ve/veya grup USB kullanım politikalarının belirlenmesi ve zorunlu olarak uygulanması
- Kuruluşunuza giren ve kuruluşunuzdan çıkan verileri daha iyi takip etmek için dosya etkinliğinin denetlenmesi
- Kritik verilerin taşınması için uzaktan içerik yedekleme imkanının sağlanması
- USB kaybolduğunda ya da güvenlik açığı verdiğinde cihazların uzaktan devre dışı bırakılması
- Unutulduğunda uzaktan parola sıfırlaması yapılması

Yetkili belleklerin bu şekilde doğru yönetilmesi, hassas verilerin kopyalanması ve paylaşılması riskini en aza indirir. Ayrıca günümüzün donanımsal şifrelemeli USB bellekleri, dosyaların ve mesajların amaçlanan alıcı dışında herhangi biri tarafından ulaşılmasının veya okunmasının önlenmesine yardımcı olan çok sayıda ekstra güvenlik özelliği sunmaktadır.

> **Donanımsal şifrelemenin yazılımsal şifrelemeden daha iyi olduğuna inanıyorum. Donanımsal ve yazılımsal şifreleme yöntemleri arasındaki farklar, kaba güç (brute force) saldırılarına karşı kırılganlık açısından çok büyüktür. Donanımsal şifrelemeli cihazlarda, bu tür saldırılardan etkilenmemek daha kolaydır.**
>
> - Tomasz Surdyk

Şifreleme: Donanım tabanlıya karşı yazılım tabanlı

İşletmeler, maliyet nedeniyle yazılım tabanlı şifrelemeyi tercih edebilirler ancak bu biraz öngörüsüz bir yaklaşım olabilir. Yazılım tabanlı çözümler, ana cihazın şifreleme kaynaklarını diğer programlarla paylaşırlar. Dolayısıyla yalnızca bilgisayar kadar güvenlidir ve genellikle uygulanmadığında kırılgan hale gelmenize neden olabilecek yazılım güncellemeleri gerektirir. Yazılım tabanlı şifrelemeli USB bellekler, şifreyi bulmak için sınırsız kaba kuvvet saldırılarına maruz kalabilir ve kısa sürede milyonlarca karakter kombinasyonunu test edebilen yazılım tabanlı sözlük saldırılarına karşı koyacak hiçbir araçları yoktur.

Ayrıca yazılım tabanlı şifreleme, kaldırılabilir bir şifrelemedir. Yazılım şifrelemeli bir belleğe sahip herhangi bir çalışan, verileri kopyalayabilir, USB belleği formatlayabilir ve böylece şifrelemeyi kaldırabilir. Daha sonra veri dosyalarını tekrar kopyalayabilir ve belleği, farklı platformlar ve işletim sistemlerinde doğrulama zahmeti olmadan kullanabilir.

Daha önce de belirttiğimiz gibi donanım tabanlı şifrelemede fiziksel "şifreleme" ve verilerin daha sonraki saklanmaları ana sistemden bağımsız olarak gerçekleşir. Bu durum, sistemlerin herhangi bir şekilde tehlikeye girmesi durumunda ekstra bir savunma katmanı sunar.

Bu, özellikle finansa, sağlık ve devlet gibi sektörlerde faaliyet gösterenler için göz ardı edilemeyecek bir özelliktir. Bunun nedeni Sağlık Sigortası Taşınabilirliği ve Güvenilirliği Yasası (HIPAA) ve Ödeme Kartı Sektörü Veri Güvenliği Standartları (PCI DSS) gibi düzenlemelerin, hassas bilgilerin şifrelenmesiyle ilgili katı gereksinimlere sahip olmasıdır.

Güçlü donanım tabanlı şifrelemeli cihazlar kullanarak bu düzenlemelere uygun hareket edilmesi kuruluşların yüksek cezalar, davalar ve itibar zedelenmesi gibi olumsuz durumlardan kaçınmasına yardımcı olacaktır. Donanım tabanlı şifrelemeli bellekler daha ucuz standart USB belleklerden daha pahalı olabilmesine karşın ihlallerin yasal maliyetleri yüksektir ve sadece birkaç saatlik hukuki danışmanlık ücreti karşılığında rahatlıkla yüzlerce bellek satın alınabilir.

Hassas verileri koruma konusunda artan gereksinim

> Tüm verileri mümkün olduğunca hızlı biçimde şifreleyin, 321 Yöntemini kullanarak yedekleyin (USB, halihazırda mevcut olduğundan bir seçenek olabilir) ve hızlı mikro-segmentasyon olanakları uygulayın. - David Clarke

Hassas verilerin kayıp ve hırsızlığa karşı korunması söz konusu olduğunda, her kuruluşun cihazlarının yeterli güvenlik özelliklerine sahip olmasını sağlama yükümlülüğü vardır. Sürekli gelişen sayısız siber tehdit varken, dijital olgunluk seviyesinin ve kullanıcıların kendi uç nokta veri yönetimi becerilerinin, dikkate alınmadığı takdirde önemli bir risk faktörü olmaya devam ettiğini göz önünde bulundurmak da önemlidir. Veri kontrolü veya USB veri saklama cihazlarının kaybı, verilerin güvenli bir ortam dışında aktarılması, şifrelenmemiş USB sürücülerin kullanılması ve parolaların paylaşılması gibi içeriden gelen tehditler, son kullanıcının gerekli dikkati göstermemesinin bir sonucu olabilir. Bunların hepsi yeterli eğitim, öğretim ve doğru USB bellek çözümleri ile önlenebilir.

> Kuruluşlar, tüm veri gruplarının önem ve/veya hassasiyet seviyeleri de dahil olmak üzere verilerinin net bir haritasına ve verilere fiziksel olarak bağlantıyı keserek veya bu veri kaynağını dışarıya kapatarak en önemli verileri ilk olarak ele alan bir plana sahip olmalıdır. Etkilenen sistemleri hızlı bir şekilde izole edebilmek çok önemlidir ve yine, uyguladığınız belgelenmiş bir plana sahip olmak kesinlikle hayati öneme sahiptir. - Rafael Bloom

Önceden planlama ve iyi denenmiş iletişim yapısı da var olabilecek tehditleri ele almada önemli bir faktördür. Günümüzün siber tehditleri, kuruluşların zayıf noktalarını hedefleme amacını taşımaktadır.

Bir şifrelenmiş USB planı oluşturmak için en iyi zamanlama, şifrelenmiş USB bellekleri ve politikaları kuruluşunuzun genel güvenlik stratejisine dahil ederek gerçekten ihtiyaç duyulmasından öncedir. Şifrelenmiş USB'ler için herhangi bir planınızın ve kurallarınızın olmaması, elinizde hiçbir şey olmamasına ve kuruluşunuzun her düzeyde riske açık olmasına neden olur. Bu riskler arasında hassas verilerin şifrelenmesi gerektiğini açıkça belirten 32. maddesiyle Genel Veri Koruma Yönetmeliği (GDPR) gibi düzenlemelere uyulmaması da yer almaktadır.

> Kullanıcılar hassas verileri işler. Bunların kaybedilmesi, sorumluluğu artırır ve şirketin imajını ve güvenliğini önemli ölçüde etkiler. Hassas verileri korumak için veri şifreleme dahil olmak üzere çeşitli güvenlik çözümleri kullanılmalıdır. - Tomasz Surdyk

Hassas finansal verilerin güvenceye alınması

Güvenlik sonuçlarının yanı sıra, veri saklama ve yedekleme çözümlerinin uyması gereken uyumluluk standartları da vardır. Veri tutma programlarını yönetme ve zorunlu olarak uygulama ihtiyacı gibi bu uygulamalardan bazıları tüm sektörlerde yaygınken, kurumsal verilerin buluta taşınması gibi diğerleri çok farklı şekilde ele alınmaktadır.

Finansal hizmetler gibi birçok sektörde, düzgün veri yönetimini zorunlu hale getiren düzenlemeler yürürlüğe alınmıştır. Özellikle bankalar, eskiden veri saklama ve yedekleme için 3. tarafları kullanma konusunda oldukça çekingendi ve birçoğu hala tüm veri altyapılarına kendisi sahip olmakta ısrar ediyor.

Finans kurumları ayrıca Sarbanes-Oxley Yasası (SOX) ve Genel Veri Koruma Yönetmeliği (GDPR) gibi giderek uzayan veri güvenliği yönetmelikleri ve standartları listesine uymakla yükümlüdür. Ancak mobil çalışanların ve yüklenicilerin sayısı arttıkça, veri sızıntısı ve bu tür yasa ve standartların getirdiği zorunluluklara uyulmaması riski de artmaktadır.

Aslında mobil çalışanlar dijital kimliklerini, taşınabilir çalışma alanlarını, taşıdıkları müşteri kayıtlarını ve finansal verileri koruyamazlarsa uyumluluk çabaları korkutucu bir kolaylıkla tehlikeye girebilir. İşte bu nedenle daha fazla kuruluş, dijital kimliklerini ve uygulamalarını, çalışanları nereye götürürse götürsün korumak için Kingston IronKey şifrelenmiş USB bellekler gibi mobil güvenlik çözümlerine kayıyor.

> **Genel eğilimin daha dağıtık bir IT ayak izine doğru kaydığını ve Bulut altyapısının geniş ölçeklenebilirliğini göz önünde bulundurduğunuzda, çoğu endüstrinin ve KOBİ'lerin çoğunluğunun artık soğutulmuş sunucu odalarını yönetmekle kendileri ilgilenmemesinin nedeni kolayca görülebilir. - Rafael Bloom**

Hasta sağlık verilerine güvenli erişim

Sağlık hizmetleri, veri güvenliğinin hiç olmadığı kadar önemli olduğu bir diğer sektördür. Hasta bilgilerinin çalınma riski daha da yüksektir. 2021'de 45,67 milyon hasta kaydının ifşa eden ihlaller yaşandı. Bu, 2015'ten bu yana görülen en büyük yıllık toplam ihlal sayısıdır[2]. Konu veri saklama ve yedekleme olduğunda hasta verileri, sağlık hizmeti sağlayıcılarının hastalarını güvenli bir şekilde tedavi etmelerini sağlayan kritik ve kapsamlı tıbbi bilgilerdir.

Bunlar, sağlık geçmişleri, testler, fotoğraflar ve radyografik görüntüleri içeren hasta Elektronik Sağlık Kaydı (EHR) dosyalarından bordro kayıtları, hasta sigortası ve alacaklılar hesapları gibi idari dosyalara kadar her şeyi içerebilir. Artan mobil iş gücü ve büyük bir değişim ve dönüşüm geçiren küresel sağlık hizmetleri pazarıyla karşı karşıya kalan günümüz sağlık hizmeti sağlayıcılarının veri güvenliği konusunda endişe duyması şaşırtıcı değildir.

> **Özellikle fidye yazılımlarının giderek büyüyen bir sektör haline gelmesiyle, hassas verileri işleyen tüm kuruluşların aşırı baskı altında nasıl çalışacağını düşünmesi gerekiyor. - Rafael Bloom**

Ayrıca, riskleri öngörememek ve Sağlık Sigortası Taşınabilirliği ve Güvenilirliği Yasası (HIPAA) veya Ekonomik ve Klinik Sağlık için Sağlık Bilgi Teknolojisi Yasası (HITECH) gibi sıkı zorunlulukların gereklerini karşılayamamak, yüksek maliyetli sağlık hizmeti veri ihlalleriyle sonuçlanabilir ve bu da hastaların, iş ortaklarının veya düzenleyicilerin güvenini daha da sarsabilir.

Kingston IronKey şifrelenmiş USB bellek ürün serisi gibi çözümlerle sağlık kuruluşları, tek bir konsoldan ister az sayıda isterse binlerce bellek için parola, uygulama kullanımı, kurtarma ve diğer konularda politikalar belirleyebilir. Mobil ve ön saflardaki çalışanların, sakladıkları verilere güvenle erişmesi için sürücüler ya da diğer yazılımlar yüklemesi gereksinimini ortadan kaldıran kullanıcı dostu çözümlerle daha fazla hastayı desteklemesi sağlanabilir. Kullanıcılar ve yöneticiler, nereye giderse gitsin verileri kolayca ve hızlı bir şekilde kilitleyebilirler.

Bulut veri saklamanın geleceğinde USB bellek

> **Bulut veri saklama günümüzün ve geleceğin çözümüdür. Örneğin şifrelenmiş USB bellekler kullanarak verilerin fiziksel olarak güvenceye alınmasının en hızlı yöntem olduğunu düşünüyorum. Kullanıcılar bulutta neler olacağı konusunda tam kontrole sahip değildir. Ancak kendimizin güvenceye aldığı ve sakladığı şifrelenmiş USB belleklerdeki veriler üzerinde kontrole sahibiz. Bu ortamlara, bizim dışımızda kimse erişemez.**
>
> **- Tomasz Surdyk**

USB belleklerin avantajlarının açıkça ortaya konmasıyla bunların bulut veri saklama sistemlerinin geleceğindeki rolü tam olarak nedir?

On yıl önce verilerin rahatça saklanması ve aktarılması için ana araç olarak büyük talep görüyordu. Ancak yeni hibrit çalışma modellerinin ve daha dağıtık hale gelen ekiplerin etkisiyle bulut artık saklanan bilgilere birçok cihazdan hızlı ve kolay erişim olanağı sunuyor. Flash bellekler dosyaların taşınması için sundukları benzersiz rahatlık nedeniyle bir zamanlar çok popülerdi. Günümüzde bulut veri saklama hizmetleri, daha yüksek dosya taşınabilirliği hizmetleri sunmaktadır.

Bununla birlikte konu bulut veri saklama olduğunda hala birçok sınırlama bulunuyor. Ağ bağlantısının gerekli olması yalnızca dosyaların nasıl ve ne zaman yedeklenebileceğini veya aktarılabileceğini belirlemekle kalmıyor, aynı zamanda ekstra bir güvenlik endişesi de ekliyor. Bir şirket bulut kullanımını zorunlu kıldığında verilere nereden erişildiğini kontrol edemeyebilir. Dolayısıyla bir VPN'e kişisel ya da halka açık Wi-Fi bağlantı üzerinden erişmek gibi basit bir eylem bile bilgisayar korsanlığı saldırısına uğrama riskini ortaya çıkarır. Ayrıca Bulut hizmetleri, tüm kötü amaçlı saldırıların büyük bir bölümünün (%61) bulut uygulamaları üzerinden yapılmasıyla korsanlar için çok çekicidir[3].

> **Bulut kullanılamadığında ne olacağını, verilerin %100 kullanılabilir olması gereken senaryoları ve uzun süreli veri saklamanın bir güvenlik açığı yaratabileceği durumları göz önünde bulundurmak akıllıca olabilir.**
>
> **- David Clarke**

Bulut veri saklamanın geleceğinde USB bellek

Diğer yandan USB şifrelemesi, cihazın donanımı ya da bir yazılım üzerinden yapılabilir. Donanım odaklı, yazılımsız şifreleme, siber saldırılara karşı koruma sağlamanın en etkili yöntemidir. Bu yöntem veri ihlallerine karşı koruma sağlamak için mükemmel, karmaşık olmayan bir çözümdür ve kuruluşların tehditleri güvenle yönetmesine ve riskleri azaltmasına yardımcı olmak için veri korumada en üst düzey güvenlik ile zorlu uyumluluk standartlarının gereklerini karşılayabilir.

Donanım şifrelemeli USB bellekler, bağımsız ürünler olmaları sayesinde ana bilgisayarda yazılım kullanımını gerektirmezler. Hiçbir yazılım kırılganlığı olmaması, kaba güç, dinleme ve bellek karma (hash) saldırıları olasılığını ortadan kaldırır. Yazılım şifrelemeli USB bellekler aynı zamanda herhangi bir kullanıcının belleği herhangi bir bilgisayarda formatlayarak şifrelemeyi devre dışı bırakması ve sürücüyü, hassas verileri korunmasız şekilde saklamak için kullanması riskiyle karşı karşıyadır.

Donanım şifrelemeli USB bellekler, verilerin güvende tutulmasında olağanüstü bir fiziksel olanak da sunmaktadır. Bilgi erişim kriterlerinin bir kullanıcı veya yönetici tarafından belirlenmesine olanak tanırlar ve mevcut yerel uç nokta çözümlerine entegre edilebilirler. Bu da onları bulut veri saklamanın işe yaramayacağı veya etkili bir çözüm olmayacağı birçok senaryo için uygun ve maliyet açısından verimli bir çözüm haline getirmektedir. Bu, verilerin ağa bağlı olmayan cihazlardan saklanması, özel olması gerektiğinde veya çevrimdışıyken erişim gerektirdiğinde olabilir.

> **Verileri, bir kuruluş için günlük esasta fayda düzeyine bağlı olarak 'sıcak' veya 'soğuk' olarak düşünürsek, operasyonel süreklilik ve yüksek performans kuruluş için veya belirli bir iş açısından kritik işlev veya süreç için daha önemliyse, 'soğuk' verileri buluta koymak ve 'sıcak' veriler için yerelleştirilmiş USB veri saklamaya yönelmek daha verimli olabilir. - Rafael Bloom**

Özet

Gelecekte yeniliklerin ne zaman geleceğini tahmin edemesek de mobil veri koruma gereksinimlerinin her seviyesi için dinamik bir şifrelenmiş çözüm yelpazesi sunan ödüllü bir USB bellek portföyü sunabiliriz. Kingston IronKey ürünleri, kolay kullanımlı PIN koruması için alfanümerik tuş takımına sahip USB belleklerden, üzerinde oynama yapılmasına karşı koruma ile birlikte en yüksek düzeyde şifreleme için FIPS 140-2-Seviye 3 sertifikasına ve güvenlikten ödün vermeyen SuperSpeed USB 3.1 teknolojisine kadar; güçlü ve etkili veri taşıma ve mobil veri saklama çözümleri vaat eden USB bellekler ile veri ile ilgili zorluklarınızı karşılamak için tasarlanmıştır.

Konuyla ilgili uzmanlardan oluşan ekibimiz, ihtiyaçlarınızı karşılayacak doğru veri saklama çözümünü bulmanızda yardım sunarak veri saklama yolculuğunuzun her adımında sizi desteklemeye hazırdır.

İster şifrelenmiş USB planı oluşturmak, ister işletmeniz için en iyi USB bellekleri belirlemek isterse güvenlik politikaları oluşturmak ve bunların zorunlu olarak uygulanmasını istiyor olun, gizli bilgileri güvende tutmanıza ve yeni düzenlemelere uymanıza yardımcı olacak becerilere ve teknik kapasiteye sahibiz. Yüksek düzeyde kişiselleştirilmiş hizmetler sunarak, veri saklama önceliklerinizi destekleyecek ve iş dünyasının beklenmedik hareket hızına ayak uydurmanızı sağlayacak ürünler sağlamak konusunda kararlıyız.

Kingston hakkında

Kingston 35 yıllık deneyimi ile mobil veriyle ilgili zorluklarınızı belirlemek ve çözmek, bu sayede iş gücünüzün kuruluşunuzu tehlikeye atmadan güvenli biçimde çalışmasını kolaylaştıracak bilgiye sahiptir.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou