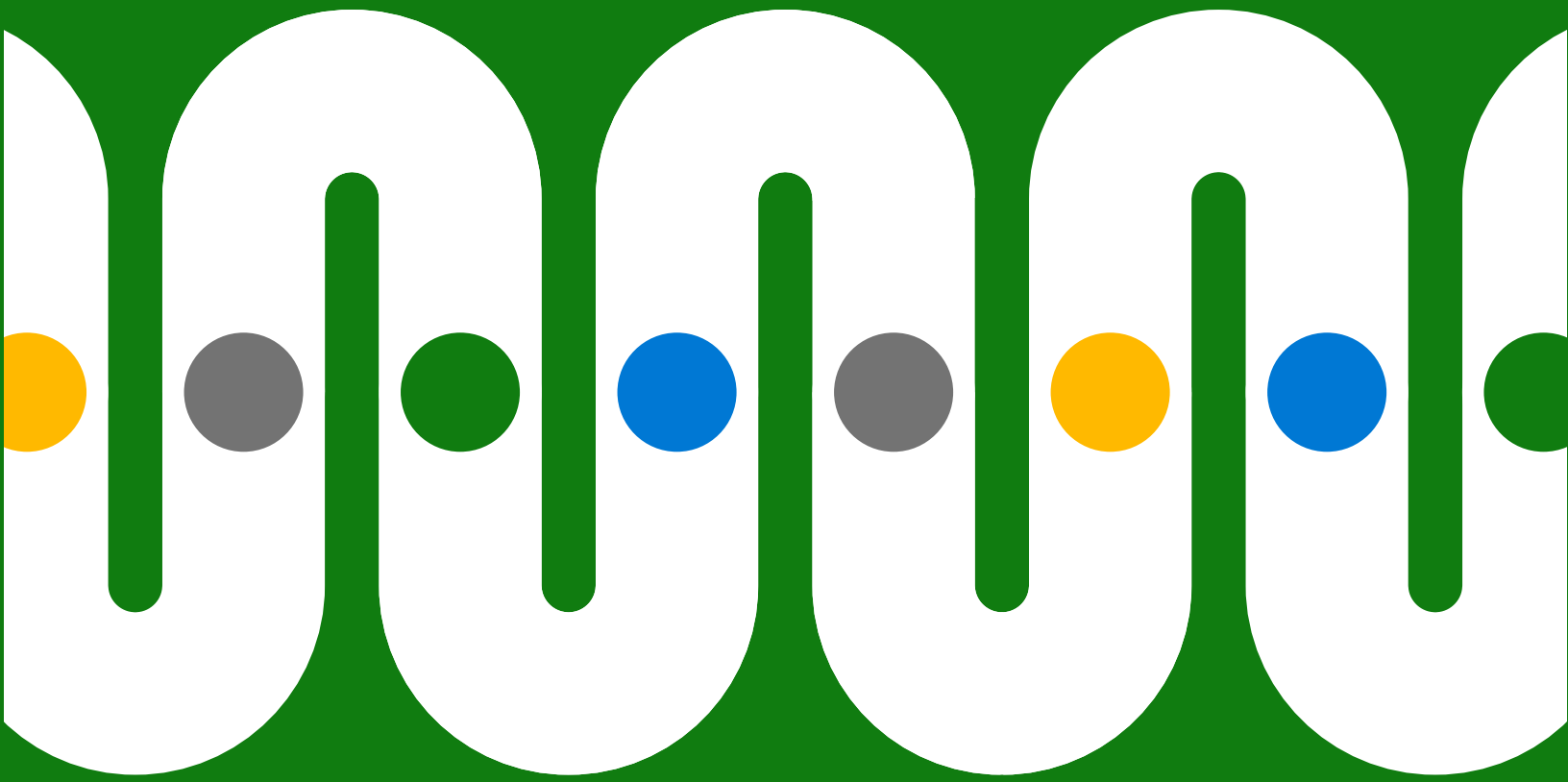
Microsoft Security

Verilerinizi Uçtan Uca Korumak İçin 3 Adım



İçindekiler

Uyumluluk karar alıcılarıyla yapılan bir ankette katılımcıların %95'inin veri koruma zorlukları hakkında endişe duydukları görülmüştür.[2]

Giriş

Kurumlar, hibrit işler sayesinde dijital ayak izlerinde büyük bir artış gördü ve geleneksel ofisin çok ötesine geçti.

Bu da daha fazla veri parçalanması ve sızmasına neden oldu. Çok sayıda uygulama, cihaz ve konumun hızla büyümesiyle bu süreç karmaşıklaştı. Ayrıca birçok çalışan daha iyi performans veya esneklik arayışıyla rol değiştirmiştir ve bu da bu zorluklara ek olarak sürekli büyüyen veri varlıklarında yeni kör noktalar oluşturmuştur.[1]

Tüm bu faktörler, CIO ve CISO'ların bilgi koruma yaklaşımlarını yeniden düşünmesine yol açmıştır. ABD'de uyumluluk konusunda karar alıcıların yer aldığı 500'den fazla kişiden oluşan izleme anketinde katılımcıların neredeyse tamamının (yüzde 95) veri korumanın zorluklarıyla ilgilendiği görülmüştür.[2]

[1] "Microsoft, Büyük Değişiklik süresince iç tehdit riskini azaltmaya nasıl yardımcı olabilir? Alym Rayani", Microsoft Güvenlik. 28 Şubat 2022.

[2] "ABD'de 512 uyumluluk karar alıcısıyla yapılan Eylül 2021 tarihli anket, Microsoft'un isteğiyle Vital Findings tarafından yapılmıştır".

BT ve güvenlik ekipleri, çoklu bulut, hibrit bulut ve kurum içi ortamlardaki tüm veri yaşam döngüsünü daha iyi yönetmenin yollarını arıyor. Bu uçtan uca yaklaşım üç temel adımdan oluşur:

1. Adım: Verileri tanımlama

Verilerinizin bulunduğu yeri, bunların ne tür veriler olduğunu ve nasıl kullanıldığını veya paylaşıldığını belirleyin

2. Adım: Verileri sınıflandırma

Doğru kuralların ve risk azaltmayı uygulayabilmek için verilerinizi sınıflandırın ve etiketleyin

3. Adım: Veri kaybını önleme

Akıllı algılama ve kontrol ile çalışanlarınız için risk azaltma ve esneklik arasında bir denge kurun

Bu yaklaşımın amacı nedir? Verimlilikten ödün vermeden boşlukları kapatmak ve riski en aza indirmek.

1. Adım

Verileri tanımlama

Verilerinin ne kadarının "karanlık" olduğu sorulduğunda, kurumların %42'si en az yarısının "karanlık" olduğunu söylemiştir.[3]

Bu "gizli" veriler, e-posta ekleri, müşteri çağrı kayıtları, makine günlükleri ve video görüntüleri gibi birçok farklı şekilde olabilir.

Tüm verilerinizin nerede olduğunu, ne tür veriler olduğunu veya nasıl kullanıldığını veya nasıl paylaşıldığını tanımlayamıyorsanız bu verilere doğru koruma kuralları veya korumayı uygulamak mümkün değildir.

Modern kurumlar sürekli olarak büyük miktarlarda veri üretir. Yalnızca belgeler, e-postalar ve mesajlar değil, güvenlik görüntülerinden coğrafi konum verilerine kadar her şey, uygulamalarda, cihazlarda ve depolamada, kurum içinde ve bulutta yaygınlaşarak birleşmiştir.

Tüm bu verileri tanımlamak zor olabilir. Kurumların yüzde 42'si verilerinin en az yarısının "karanlık" olduğunu söylüyor.[3] Bunlar, toplanan ancak bilinmeyen veya kurumsal amaçlar için kullanılmayan bilgilerdir. Bazen verileri oluşturan çalışan, projeleri veya rolleri değiştirdiğinde veriler kararır. Genellikle oluşturma veya değiştirme sırasında verileri tanımlayan sistem yoktur.

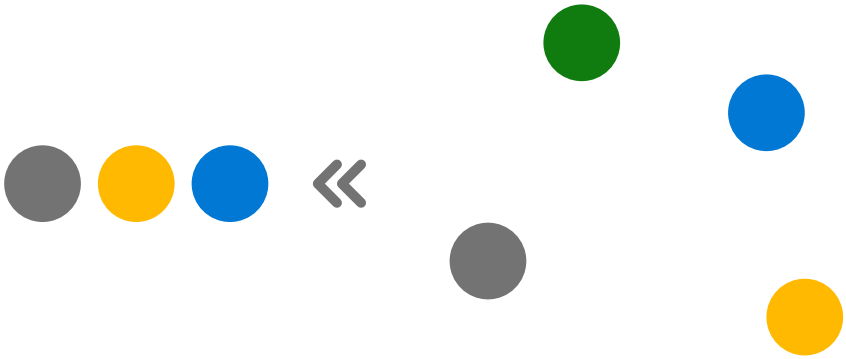
[3] "2022 State of Data Governance and Empowerment Report", Enterprise Strategy Group. Temmuz 2022.

Tek bir platformda uçtan uca keşif iş akışı mı oluşturmak istiyorsunuz?

Microsoft.com adresinden Microsoft Purview'da veri keşfi hakkında daha fazla bilgi edinin.

Bu zorluk gittikçe büyüyecek. Oluşturulan, yakalanan, çoğaltılan ve tüketilen yeni veri miktarının 2026 yılına kadar mevcut oranın iki katından fazla olması ve kurumsal verilerin tüketici verilerinin iki katından daha hızlı artması beklenmektedir.[4]

Yapay zeka (AI) ve makine öğrenimi (ML), e-posta adresleri, sağlık verileri, kredi kartı numaraları veya fikri mülkiyet gibi hassas verileri tanıma ve otomatik olarak sınıflandırmada yardımcı olabilir. Yapay zeka ve makine öğrenimi ayrıca sınıflandırma doğruluğunu artırabilir ve verileri geriye dönük olarak inceleyebilir. Bu tanımlama işlemleri, tüm veri mülkünüze yayılabilir; içeriği bulunduğu bulutta tüm bulutlarda koruyabilir, toplayabilir, analiz edebilir, gözden geçirebilir ve dışa aktarabilir.



[4] "Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth", John Rydning, IDC. Mayıs 2022.

2. Adım

Verileri sınıflandırma

Hem sınıflandırmalar hem de kurallar yer değiştiren verileri takip etmelidir.

Örneğin, bir çalışan kredi kartı numaralarını Microsoft Word belgesinden bir Excel'e kopyalarsa sınıflandırma ve kurallar belgelere otomatik olarak uygulanmalıdır.

Hassas verileri ortamınızda daha iyi yönetmek ve korumak mı istiyorsunuz?

Microsoft.com adresinden Microsoft'taki veri sınıflandırması ve koruması hakkında daha fazla bilgi edinin.

Uygun veri sınıflandırması, farklı veri türlerinin hatayla veya bilinçli olarak kötüye kullanılmasını veya yetkisiz olarak erişilmesini önlemek için doğru kuralları ve risk azaltma önlemlerini belirlemenize yardımcı olur. Şifreleme ve filigran ekleme, veriyi beklemede, taşınırken veya kullanımdayken daha iyi koruyabilir.

Ancak sınıflandırma ve kuralların kurumda dolaşan verileri izlemesi gerekir. Etiketleme ve koruma kuralları ayrı belgelerle sınırlı kalamaz, tüm dijital mülklerinizi, yani kurum içindeki depoları, bulut tabanlı depoları, hizmet olarak yazılım (SaaS) uygulamalarını ve işletim sistemine özgü uygulamaları kapsaması gerekir.

Geleneksel sınıflandırma yaklaşımları arasında tüm önemli manuel çalışmalar bulunur ve bu da hata yapma veya kazara kritik verilerin gözden kaçması riskini taşır. Yerleşik ve eğitilebilir sınıflandırıcılar bu işlemi otomatikleştirmeye yardımcı olabilir ve tümleşik bir çözüm, yöneticilerin kuralları tüm sistemlerde merkezi olarak yönetmesine olanak tanır.

3. Adım

Veri kaybını önleme

DLP kuralı uyumsuzluk eylemlerini önleyebilir.

Örneğin, bir çalışan bir flash sürücüye kredi kartı numarası içeren bir elektronik tablo indirmeye veya bunu bulut depolamaya yüklemeye çalışırsa, DLP kuralı etkinliği uyumsuz olarak belirleyebilir ve bu etkinliği önleyebilir.

Hassas bilgilerin akıllıca algılanmasını ve kontrol edilmesini mi istiyorsunuz?

Microsoft.com adresinden Microsoft Purview'da veri kaybı önleme hakkında daha fazla bilgi edinin.

Verilerinizi belirleyip sınıflandırdıktan sonra, veri kaybı önleme (DLP) çözümleri, karanlık veri ve veri sızması gibi tehditleri azaltan uçtan uca koruma kuralları uygulayabilir, böylece mevcut ve eski çalışanlar (bilinçli olarak veya kazayla) hassas verileri paylaşamaz, kullanıma sunamaz veya aktaramaz.

Akıllı DLP çözümleri, esneklik sağlama ve yüksek riskli eylemleri engelleme arasında bir denge oluşturmak için bağlamı kullanır. Örneğin, bireyler olası riskler ve uygulanabilir kurallar hakkında hatırlatma yapıldıktan sonra ilgili eyleme devam edebilir. Bu çözüm, hassas verilerin korunmasına yardımcı olurken aynı zamanda kullanıcıları riski daha iyi anlamaları için eğitir.

DLP çözümleri, fikri mülkiyet ve diğer kritik kurum verilerini korumaya yardımcı olur ve ayrıca Genel Veri Koruma Yönetmeliği (GDPR), Sağlık Bilgileri Taşınabilirliği ve Sorumluluk Yasası (HIPAA) ve California Tüketici Gizliliği Yasası (CCPA) gibi düzenlemelerle uyumluluğu iyileştirir.

DLP'ye yönelik kapsamlı bir yaklaşım, kuralları kurumunuz genelinde tutarlı bir şekilde uygulayarak veri yaşam döngüsündeki "en zayıf bağlantı" noktalarını korur.

Veri korumasını takviye etmeyin. Yerleştirin.

Bir uyum karar alıcıları anketinde, katılımcıların %79'unun birden fazla uyumluluk ve veri koruma ürünü satın aldığı görülmüştür.

Çoğunluk üç adet veya daha fazla ürün satın almıştır.[5]

Birçok kurum, veri yaşam döngüsünün farklı bölümlerini yönetmek üzere birden çok çözüm kullanarak, bilgi korumasına yönelik "takviye edilen" bir yaklaşımda bulunmayı denemiştir. Ancak bu, güvenlik, veri yönetimi, uyumluluk ve yasal ekiplerinizi genellikle etkisiz olan ve kaynakları zorlayan karmaşık işler yapmaya zorlar.

"Yerleşik" bir yaklaşım, veri tanımlama, veri sınıflandırma ve DLP'yi bir araya getirerek boşlukları kapatabilir. Kuralları merkezi olarak yönetmek ve uygulamak tümleşik bir çözümle daha kolaydır. Ayrıca uygulamalar içinde bildikleri yollardan kural bildirimleri alan kullanıcıların eğitim süresini azaltır.

[5] "ABD'de 200 uyumluluk karar alıcısının katıldığı Şubat 2022 tarihli anket (n=100 599-999 çalışan, n=100 1.000+ çalışan) Microsoft'un isteğiyle MDC Research tarafından yapılmıştır."

Yerleşik, tümleşik bir çözüm: Microsoft Purview

Microsoft Purview, veri varlığınızın tamamını yönetmenize, korumanıza ve yönetmenize yardımcı olan kapsamlı bir dizi çözümle günümüz dünyasındaki merkezi olmayan, veri açısından zengin işyeri zorluklarını çözmenize yardımcı olur.

Yönetimin ötesine geçin.

Microsoft Purview ile verilerinizi koruma hakkında daha fazla bilgi edinin >

Belirli bir veri koruma alanıyla mı ilgileniyorsunuz? Microsoft Purview'ın şu konu hakkında size nasıl yardımcı olabileceği hakkında daha ayrıntılı bilgi edinin:

Veri keşfi >

Veri sınıflandırması ve koruması >

Veri kaybı önleme >

Microsoft Security