IBM Connected 2013

Her Deneyim Bir Kazanım

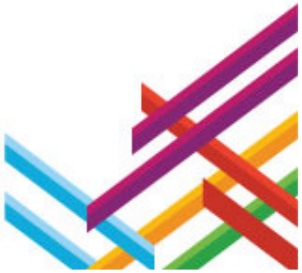
Veritabanı Risk ve Uyumluluk Yönetimi

Tansel ZENGİNLER
IBM Veri Yönetimi Çözüm Mimarı
Telefon: 0530 317 1675
E-posta: tansel@tr.ibm.com

#connected

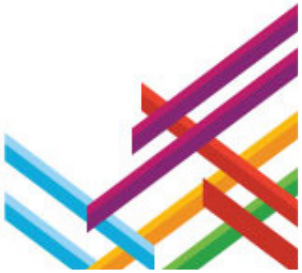
İçindekiler

- Giriş
- Veritabanı Denetim Gereksinimi
- Geleneksel Veritabanı Denetim Yöntemleri
- Guardium Çözümü
- Devreye Alma
- Özet

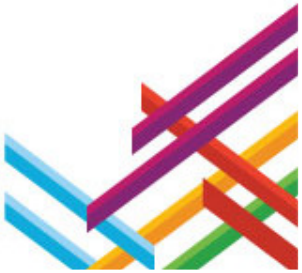


Guardium kimdir?

- Guardium, 2002 yılından bu yana Veritabanı Etkinliği İzleme pazarının açık farkla lideridir.
- %100 oranında veritabanı denetimine ve güvenliğine odaklıdır.
- Tüm dünyada her tür endüstriden 400'den fazla musteri
- Aralık 2009'dan bu yana, IBM'in Bütünleştirilmiş Veri Yönetimi portföyünün bir parçasıdır.



Veritabanları, her kuruluş için hayati önem taşır,
buna bağlı olarak zaten iyi korunuyor olmalıdır?



2009 Veri İhlali Araştırmaları Raporu

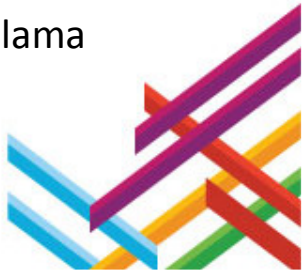
Verizon Business RISK ekibi tarafından gerçekleştirilen bir araştırma

Yönetici Özeti

2008 yılı, muhtemelen hem kuruluşlar hem de tüketiciler için karışık bir yıl olarak hatırlanacaktır. Korku, belirsizlik ve şüphe küresel finans piyasalarını ele geçirmiştir; rahatsız edici sayıda dev kuruluş batmıştır; daha önce bolluk içinde olan pek çokları ise temel ihtiyaçlarını karşılamakta bile zorlanır hale gelmiştir. Ekonomik sıkıntılara ek olarak tarihin en büyük veri ihlallerinden bazıları da bu dönemde bildirilmiştir. Bu olaylar, piyasalar gibi bilgilerimizin emniyetinin ve güvenliğinin de kesin olduğunun varsayılamayacağını hatırlatmıştır.

2009 Veri İhlali Araştırmaları Raporu, tarihin bu çalkantılı dönemini adli araştırmacıların bakış açısından ele almaktadır. 2008 yılı olay örnekleri arasındaki 90 doğrulanmış ihlal, tam 285 milyon kaydın açığa çıktığı anlamına gelmektedir. Bu kayıtların anlatacağı ilgi çekici bir hikaye bulunmaktadır ve bu raporun sayfaları bu hikayenin anlatılmasına ayrılmıştır. Amacımız, geçtiğimiz yıl olduğu gibi, bu raporda sunulan verilerin ve analizin okuyucularımızın planlama ve güvenlik çalışmalarında yararlı olmasıdır.

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

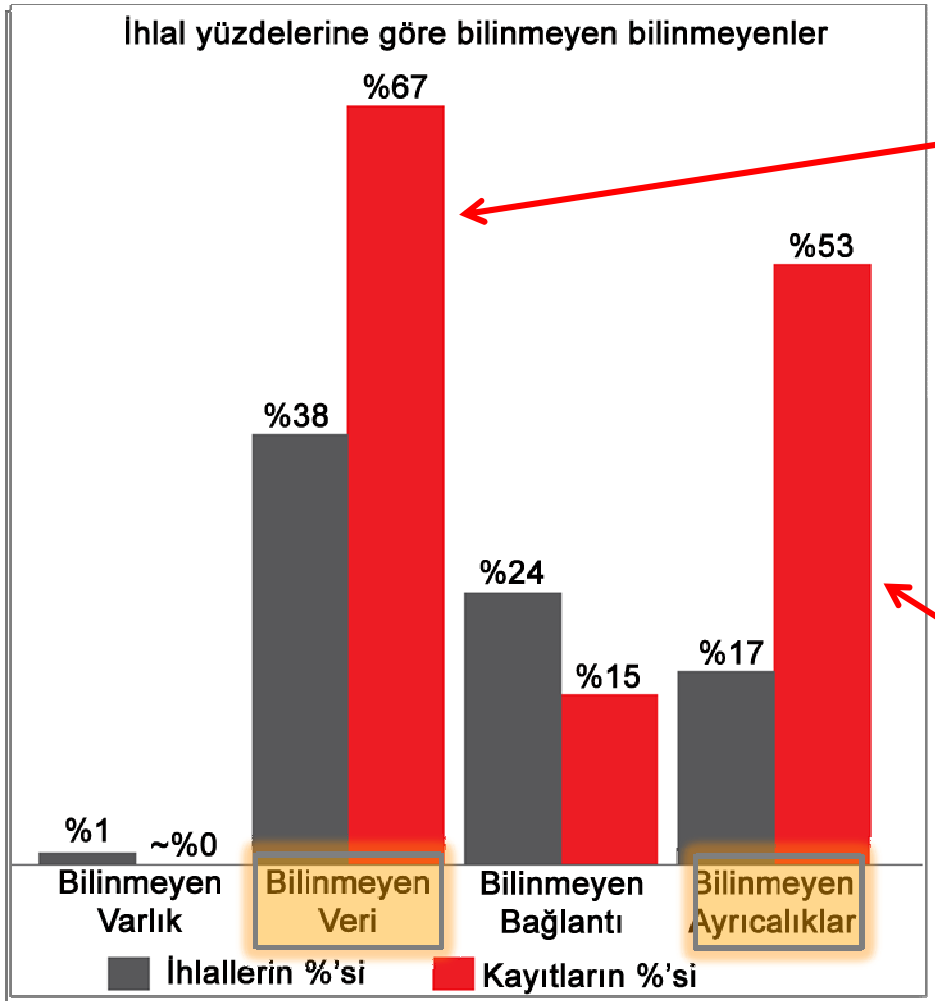


Verizon RISK Ekibi 2009 Veri İhlali Raporu

Varlık	Varlık Grubu	İhlallerin %'si	Kayıtların %'si
POS sistemi	Çevrimiçi Veri	%32	%6
Veritabanı sunucusu	Çevrimiçi Veri	%30	%75
Uygulama sunucusu	Çevrimiçi Veri	%12	%19
Web sunucusu	Çevrimiçi Veri	%10	%0.004
Dosya sunucusu	Çevrimiçi Veri	%8	%0.1
Genel kiosk sistemi	Çevrimiçi Veri	%2	%0.4
Kimlik doğrulama/Dizin sunucusu	Çevrimiçi Veri	%2	%0.1
Yedekleme manyetik bantları	Çevrimiçi Veri	%1	%0.04
Belgeler	Çevrimiçi Veri	%1	%0.000
İş istasyonu	Son Kullanıcı Sistemi	%8	%0.01
Dizüstü bilgisayar	Son Kullanıcı Sistemi	%4	%0.000
PIN Giriş Aygıtı	Son Kullanıcı Sistemi	%2	%0.004

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

"Bilinmeyen Bilinmeyenler" Veri İhlallerinin En Önemli Nedenidir

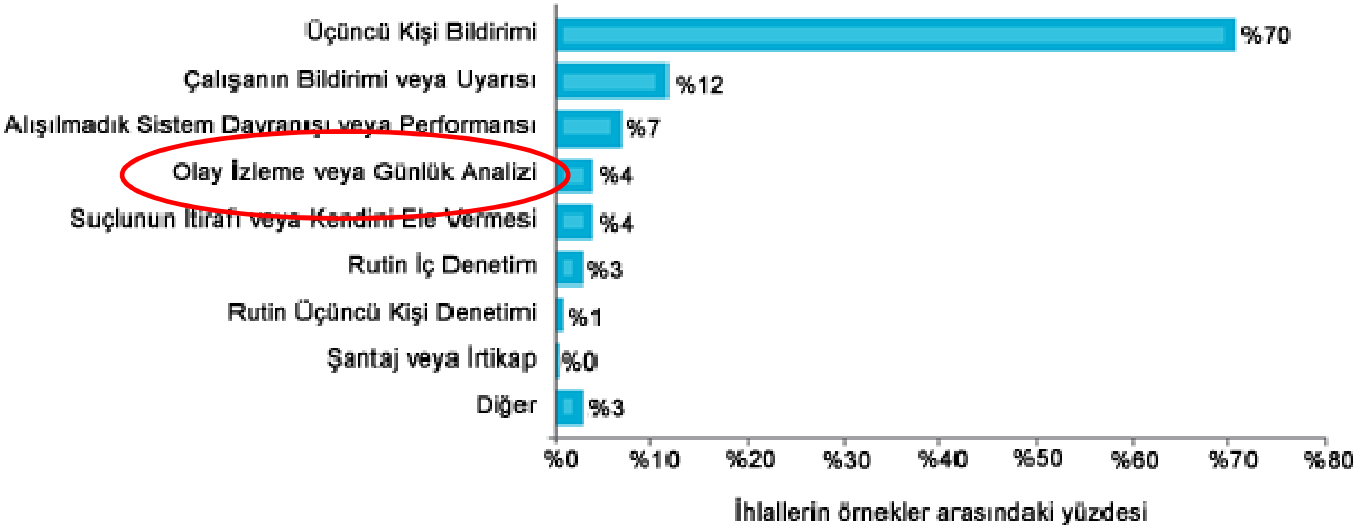


Bilinmeyen Veriler
"Burada hassas verilerin depolandığını bilmiyorduk bile"

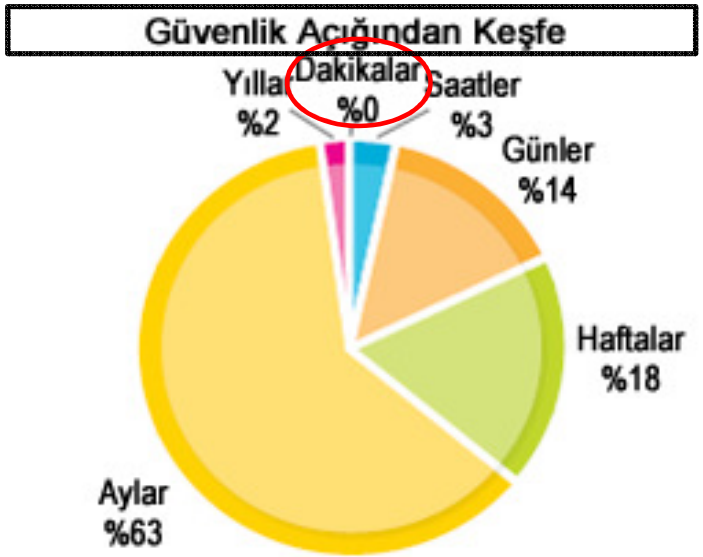
Bilinmeyen Ayrıcalıklar
"Bu ayrıcalıkların bu şekilde yapılandırıldığını bilmiyorduk"

http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Veri ihlalleri nasıl belirlenir?



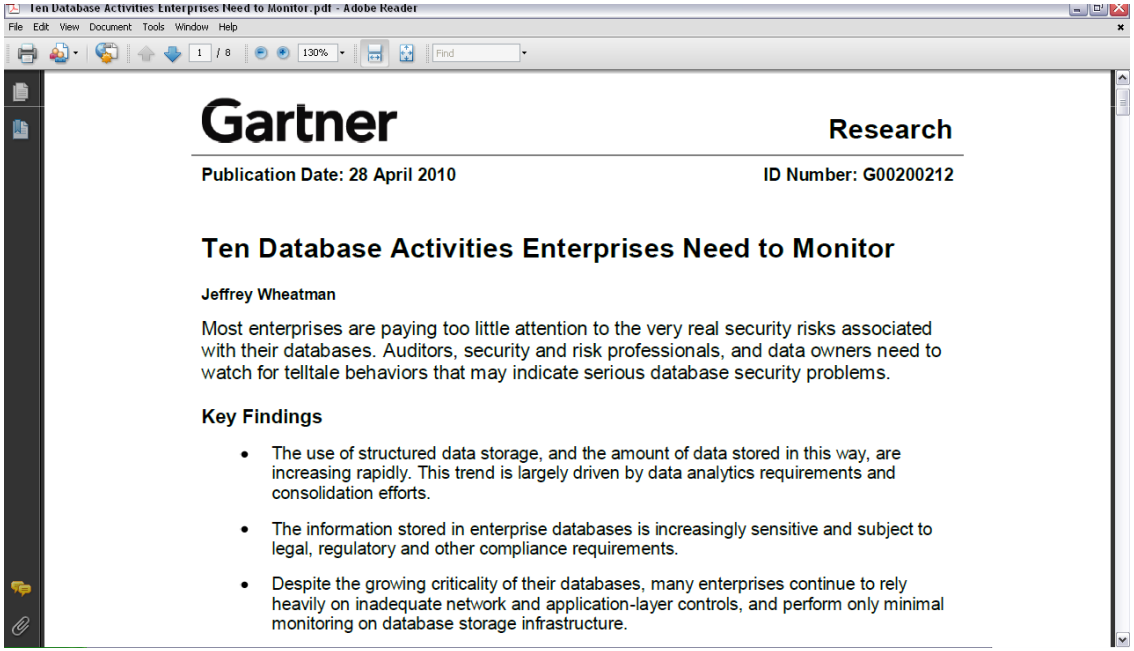
Veri İhlali Keşif Yöntemleri



Analistler veritabanı güvenliği hakkında ne düşünüyor?

"Pek çok kuruluş, veritabanları ile bağlantılı çok gerçek güvenlik risklerine çok az önem vermektedir."

- Gartner Research, 28 Nisan 2010



Gartner

Veritabanı Etkinliği İzleme

- "İlişkisel veritabanlarında depolanan veriler giderek daha hassas hale gelmektedir ve yasa, yönetmelik ve uyumluluk gereksinimlerine tabidir"

- "Güvenlik profesyonellerinin ve veri sahiplerinin, kuruluşlarının veritabanı etkinlikleri konusunda şimdi olduğundan çok daha fazlasını bilmesi gerekmektedir"

- Pek çok kuruluş, ağırlıklı olarak yetersiz ağ ve uygulama katmanı denetimlerine güvenmektedir ve veritabanlarını çok düşük seviyede izlemektedir"

Veritabanı denetimi neden bu kadar zor?

Günümüzde veritabanlarının çoğu nasıl denetleniyor?

DBMS içindeki yerel denetim günlüklerine bağımlılık

× Görünürlüğü ve parçacıklı yapısı yoktur

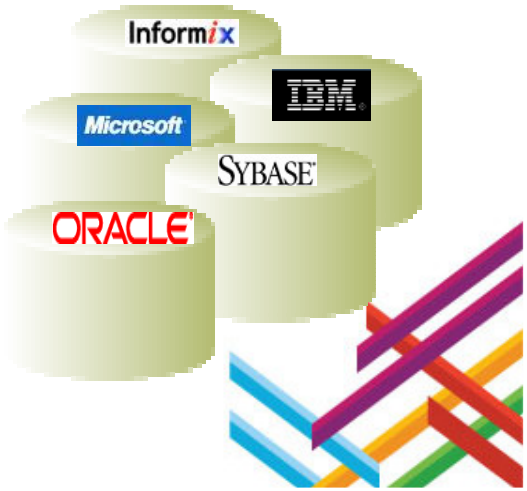
- » Ayrıcalıklı kullanıcıların izlenmesi zordur
- » Uygulamanın "gerçek kullanıcısının" takip edilmesi zordur
- » Denetimin ayrıntı düzeyi yetersizdir

× Verimsiz ve yüksek maliyetli

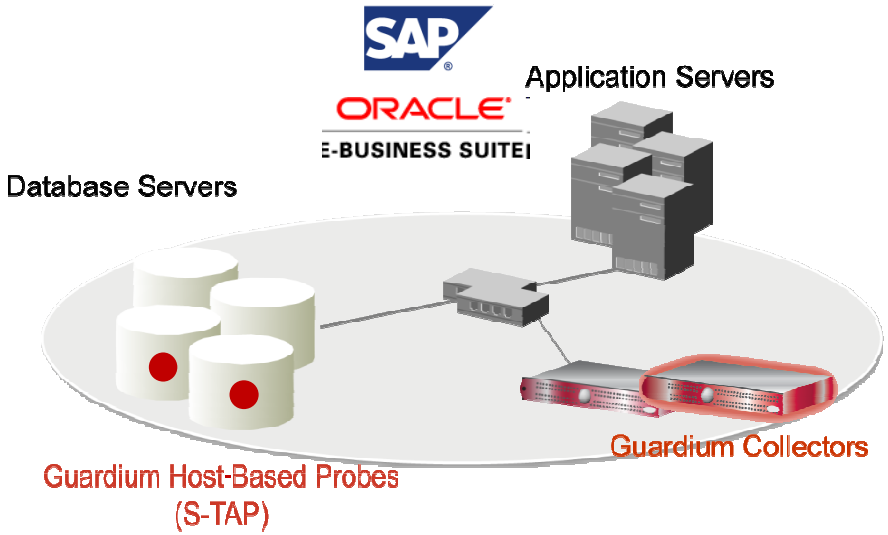
- » Veritabanı performansını etkiler
- » Büyük günlük dosyaları düşük değer sağlar
- » Her veritabanı tipi için farklı yöntemler

× Görev ayrılığı yoktur

- » İzleme sistemini veritabanı yöneticileri yönetir
- » Ayrıcalıklı kullanıcılar sistemi atlayabilir
- » Denetim yolu güvenli değildir



Gerçek Zamanlı Veritabanı Güvenliği ve İzleme

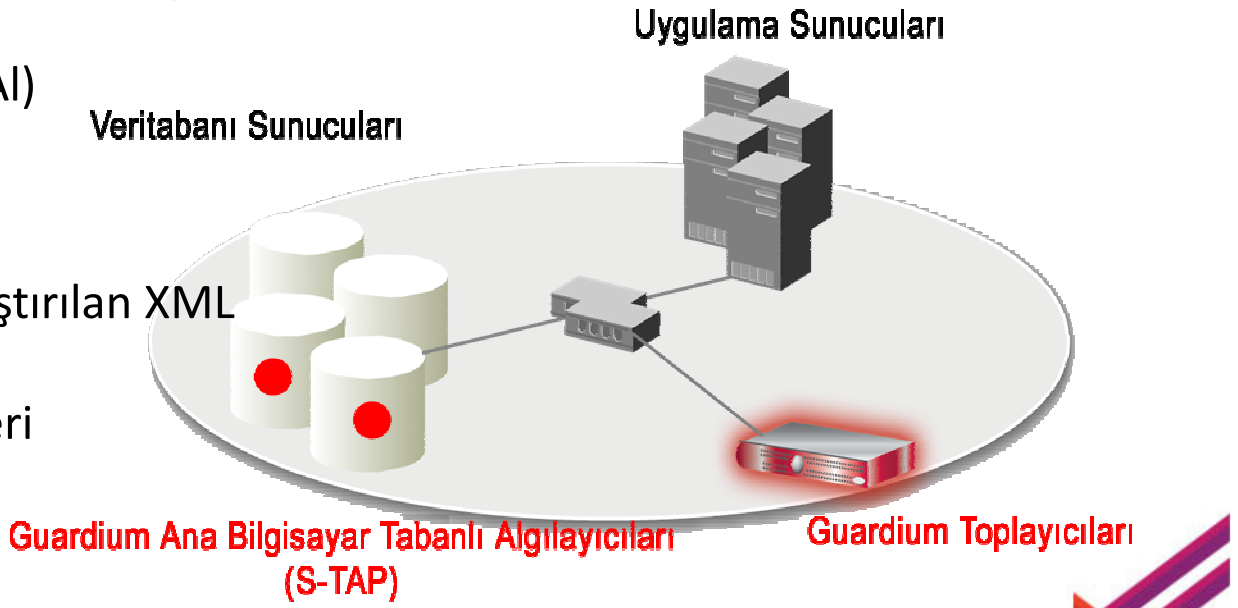


- Yerel veritabanı yöneticisi erişimi dahil %100 görünürlük
- DBMS veya uygulama değişikliği yoktur
- Veritabanı performansı üzerinde en düşük seviyede etki
- Müdahale edilmesi mümkün olmayan denetim havuzu ile görevlerin ayrılmasını sağlar

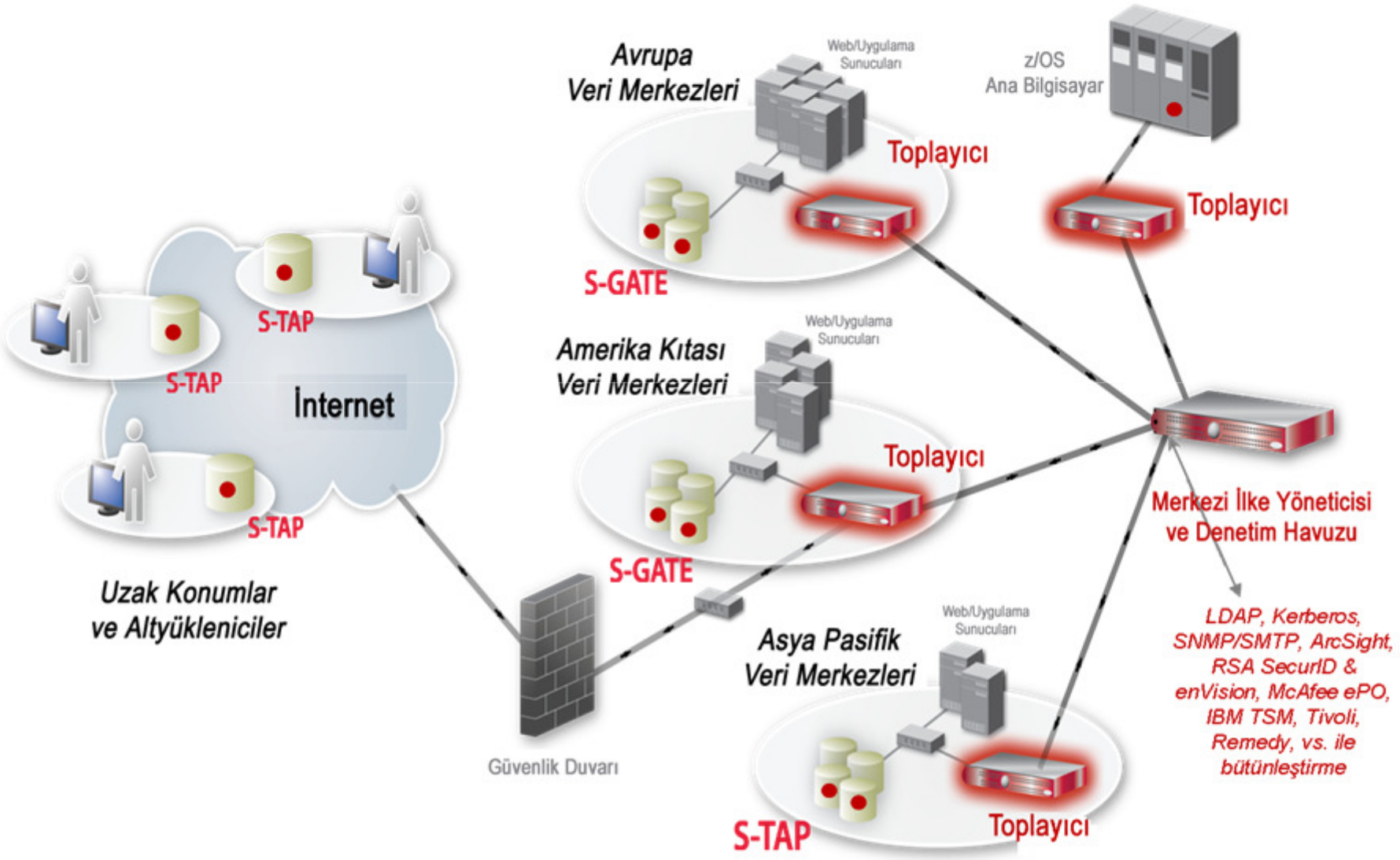
- Parçacıklı ilkeler, izleme ve denetim, Kimi, Neyi, Nedeni ve Nasılı sağlar
- Gerçek zamanlı, ilke tabanlı uyarılar
- 3-6 aylık denetim verilerini aygıtın kendisinde depolayabilir ve arşivleme sistemleri ile bütünleşir

Guardium neyi izler?

- SQL hataları ve başarısız oturum açmalar
- DDL komutları (Tablo Oluştur/Bırak/Değiştir)
- SELECT sorgulamaları
- DML komutları (Ekle, Güncelle, Sil)
- DCL komutları (Ver, Geri Al)
- Prosedür dilleri
- Veritabanı tarafından çalıştırılan XML
- Geri dönen sonuç kümeleri



Ölçeklenebilir Çok Katmanlı Mimari



Veritabanı Risk ve Uyumluluk Yönetimi Tam Çevrimi

Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilme ve sınıflandırılması

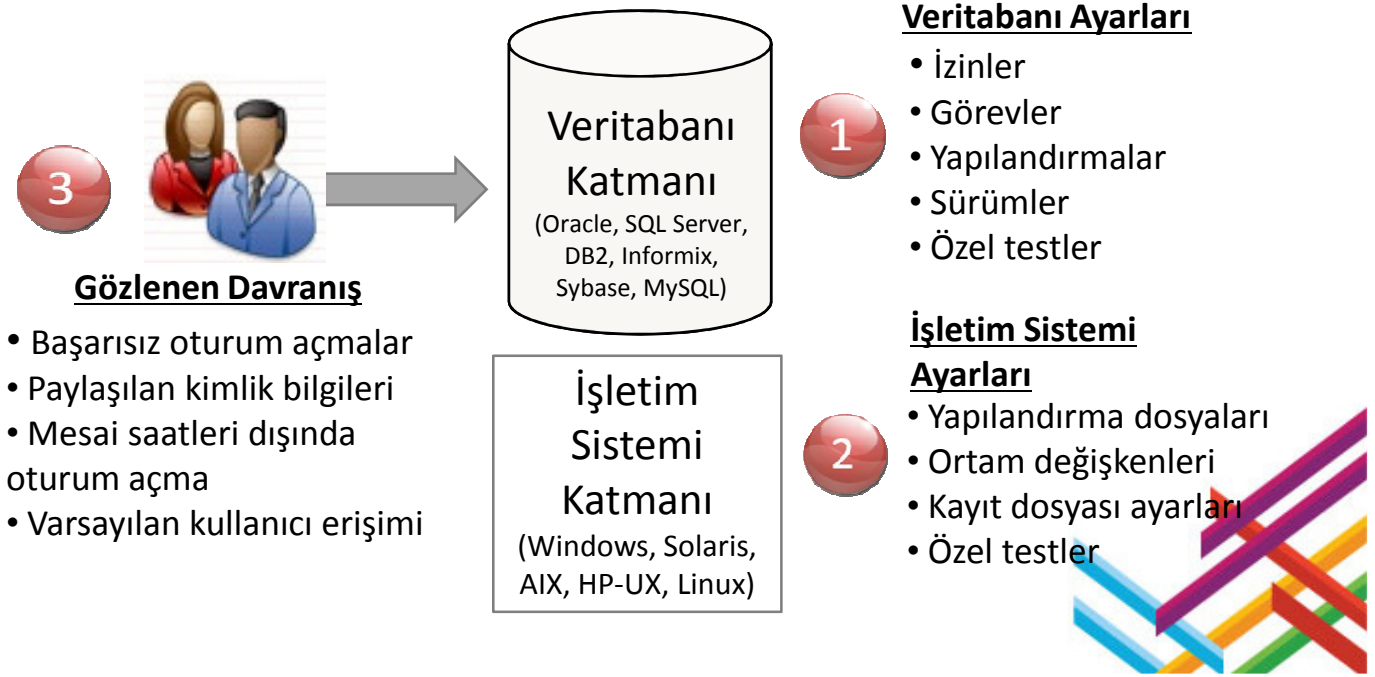
Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilme ve sınıflandırılması

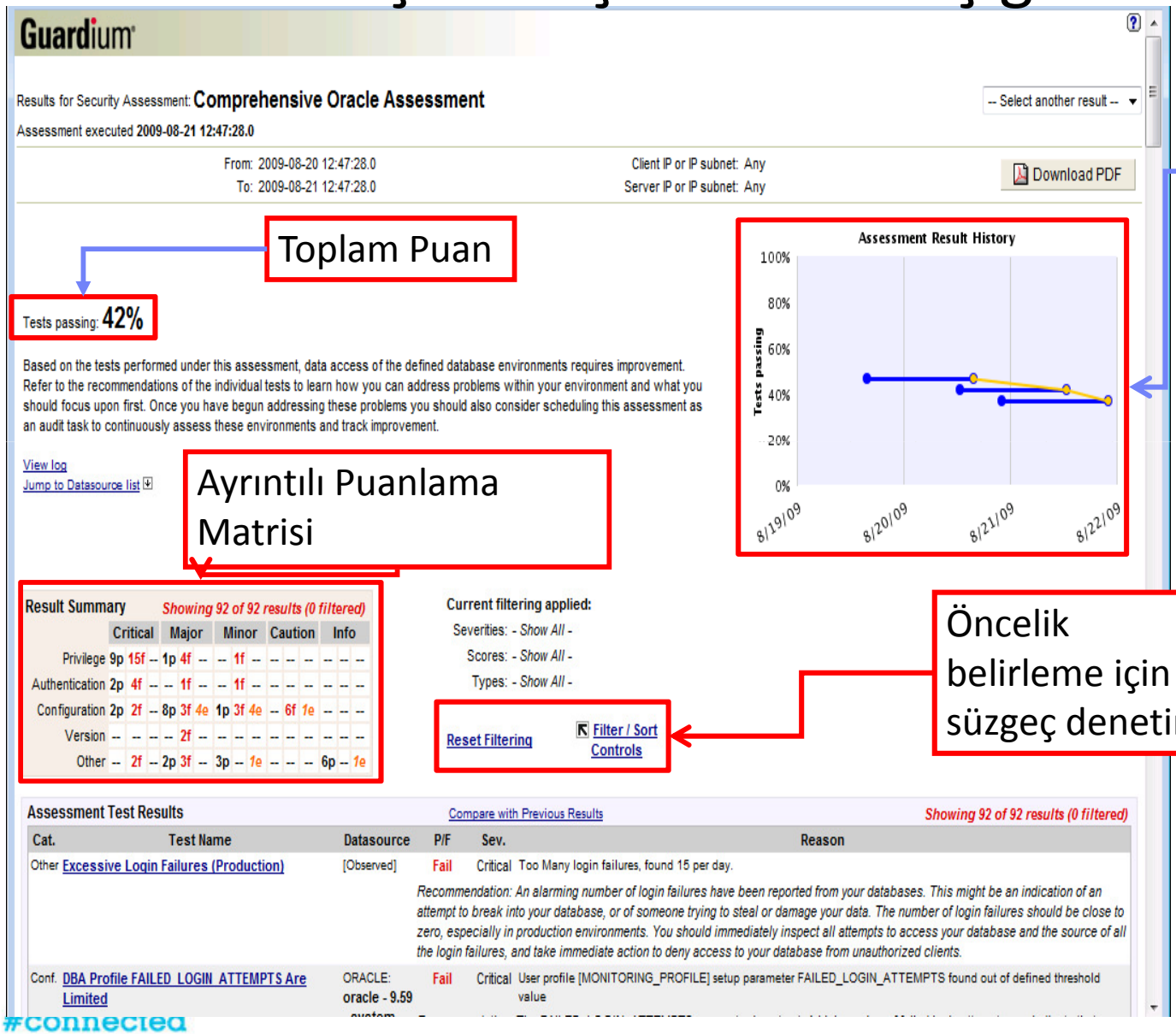
- Güvenlik açığı değerlendirmesi
- Yapılandırma değerlendirmesi
- Davranış değerlendirmesi
- Alt sınırların belirlenmesi
- Yapılandırma kilitleme ve değişiklik izleme
- Şifreleme

Güvenlik Açığı ve Yapılandırma Değerlendirmesi Mimarisi

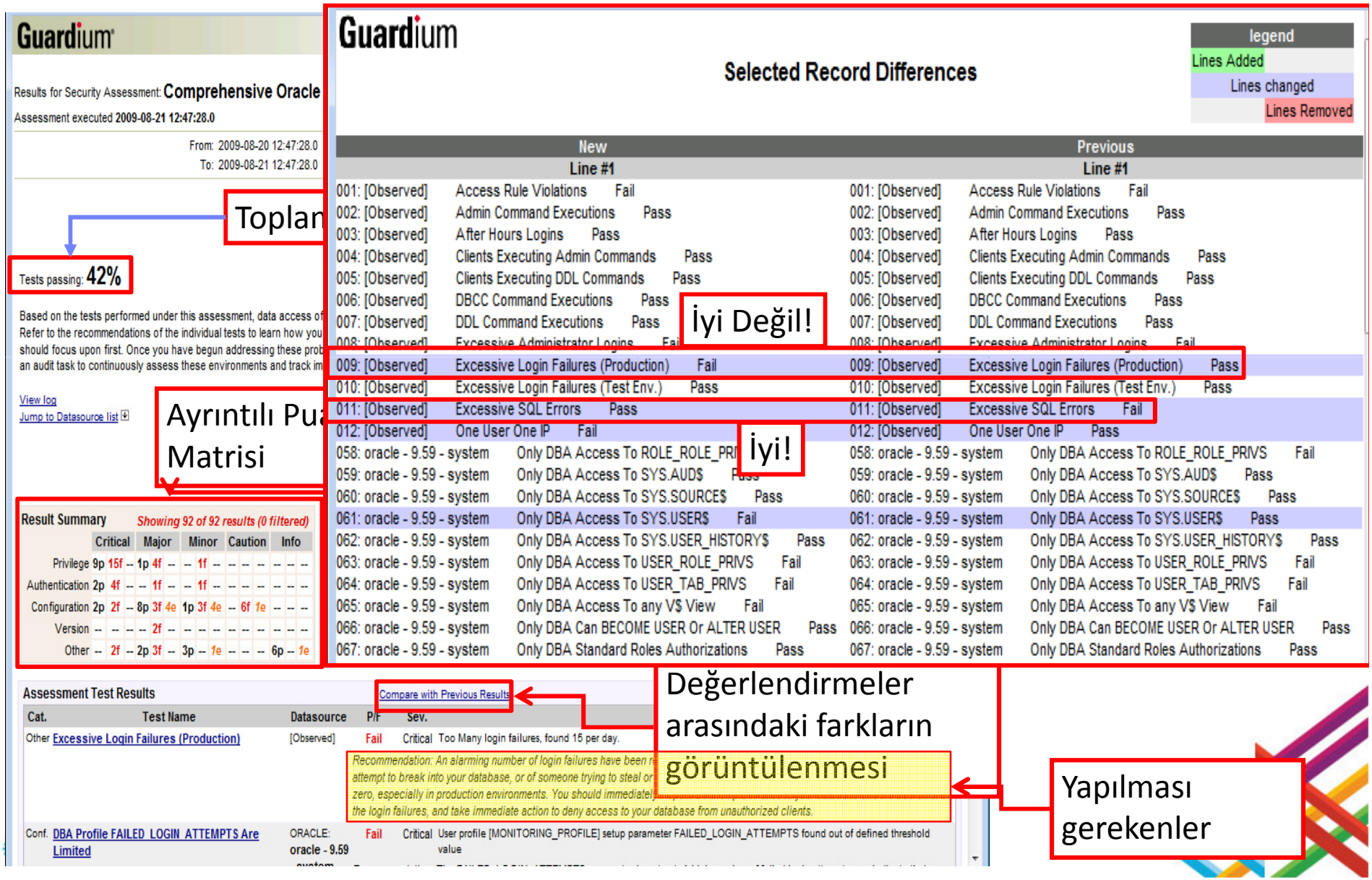
- Endüstri standartları tabanlıdır: DISA STIG & CIS Karşılaştırmalı Değerlendirmesi
- Belirli kurumsal güvenlik ilkelerinizin karşılanması için özelleştirilebilir testler
- Tam test yelpazesi geniş kapsam sağlar:



Basitleştirilmiş Güvenlik Açığı Yönetimi



Basitleştirilmiş Güvenlik Açığı Yönetimi

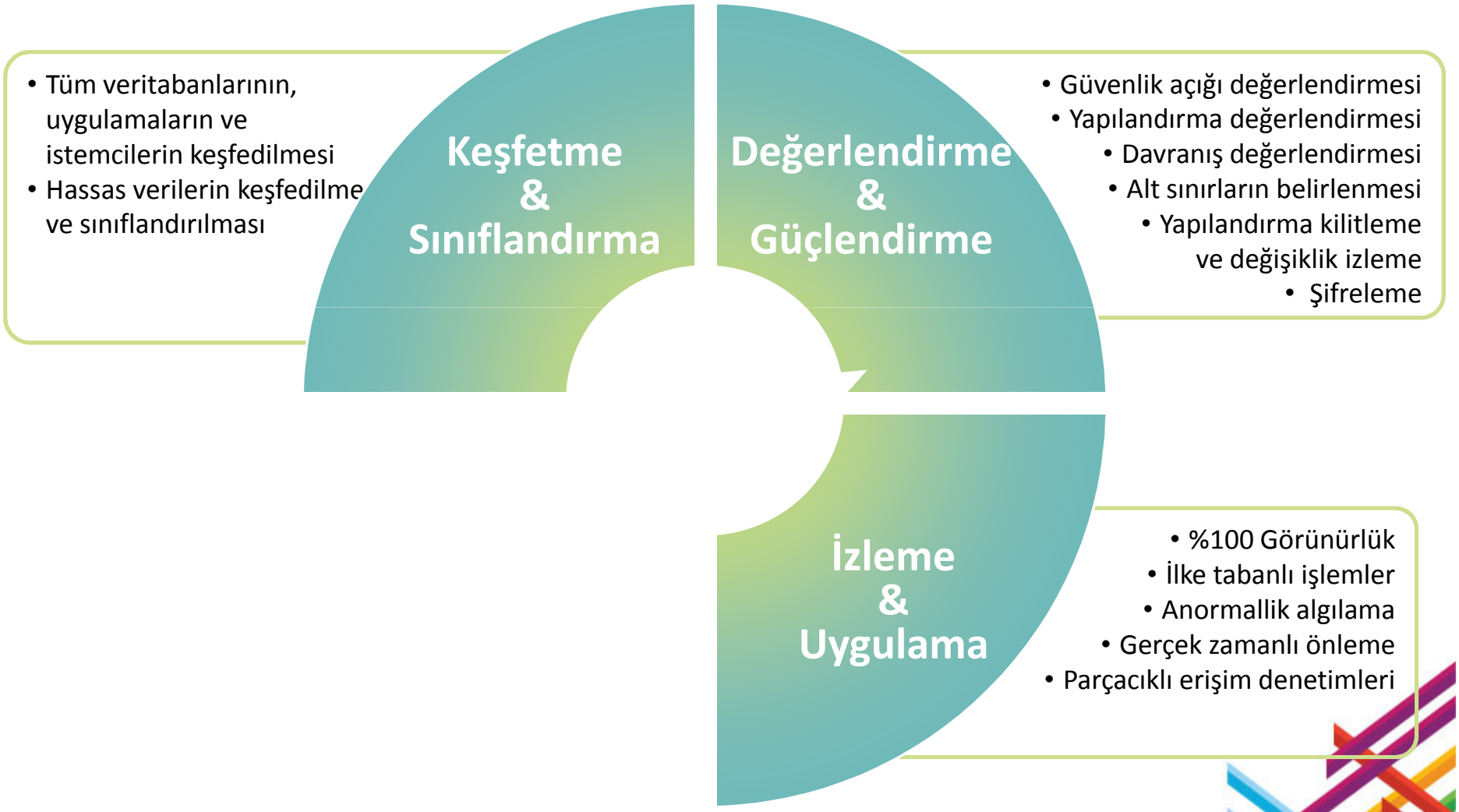


Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

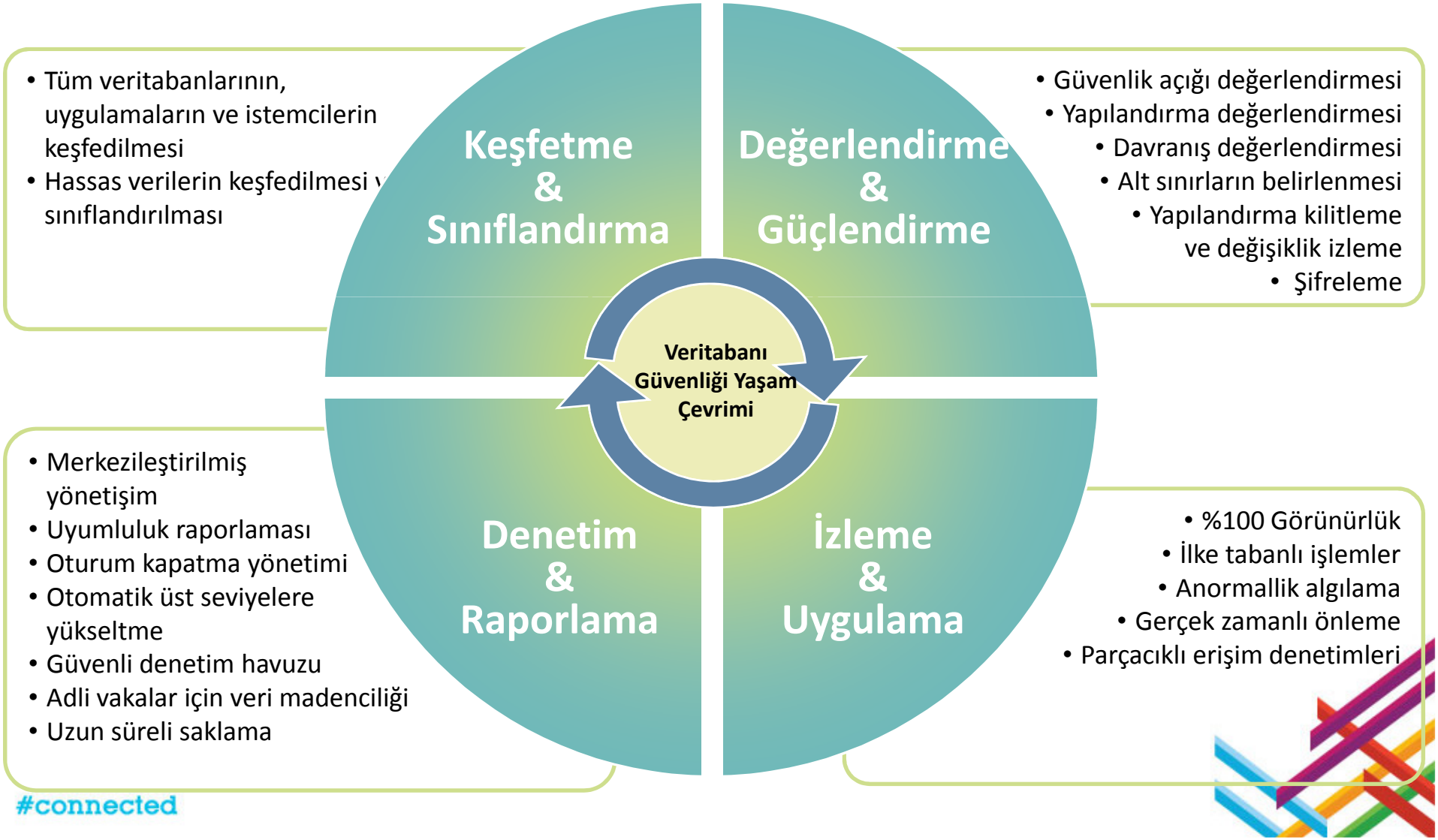
- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilme ve sınıflandırılması

- Güvenlik açığı değerlendirmesi
- Yapılandırma değerlendirmesi
- Davranış değerlendirmesi
- Alt sınırların belirlenmesi
- Yapılandırma kilitleme ve değişiklik izleme
- Şifreleme

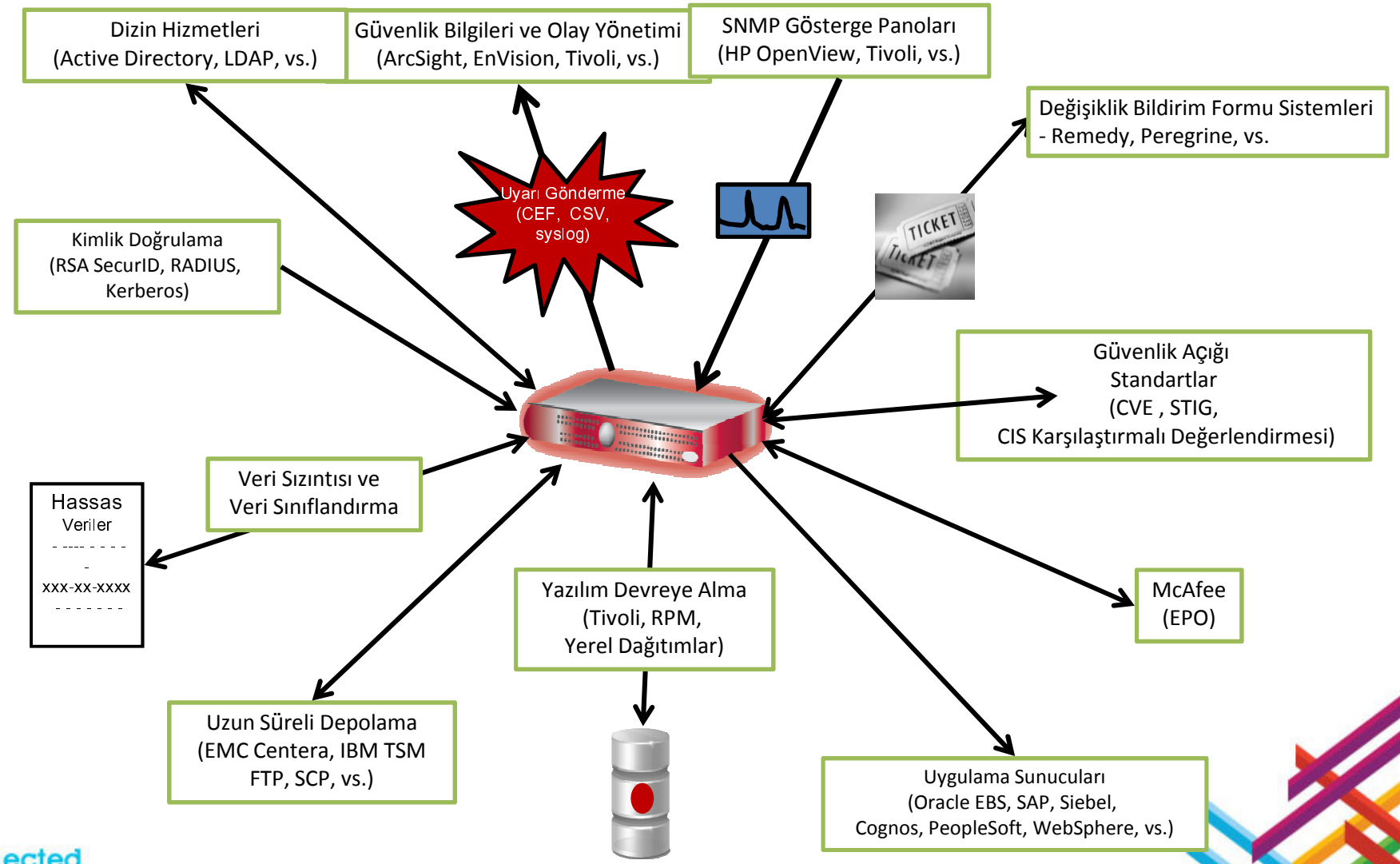
Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi



Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi



Mevcut Altyapı ile Bütünleştirme Toplam Sahip Olma Maliyetini Düşürür

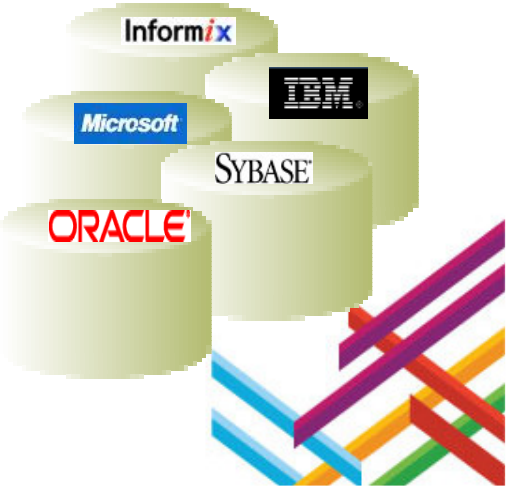


Guardium için İş Örneği

1. Veri İhlallerini Önler
   - İç ve dış güvenlik açıklarını azaltır
   - Gerçek zamanlı ve proaktif denetimler

2. Veri Yönetişimi Sağlar
   - Hassas verilerde yetkisiz değişiklik yapılmasını önler
   - Denetçilere uyumluluğu kanıtlar

3. Uyumluluk Maliyetini Düşürür
   - Denetimleri basitleştirir, otomatikleştirir ve merkezileştirir
   - Sabit giderleri ve sistemler üzerindeki etkiyi azaltır



IBM

IBM Connected 2013

Her Deneyim Bir Kazanım

Teşekkürler

#connected