IBM yazılım zirvesi '10

KAOSTAN FIRSATA

VERİTABANI RİSK VE UYUMLULUK YÖNETİMİ

Mesut Ünal
Turkcell İletişim Hizmetleri - Information Technologies / Service Security

İbrahim Arslan
Bilişimcim Limited

Tansel Zenginler
IBM InfoSphere Guardium Teknik Satis Uzmani / CEE

İçindekiler

- Giriş
- Gereksinimler
- Geleneksel Yöntemler
- Optim Çözümü
- Guardium Çözümü
- Turkcell Veritabanı İzleme Projesi

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.

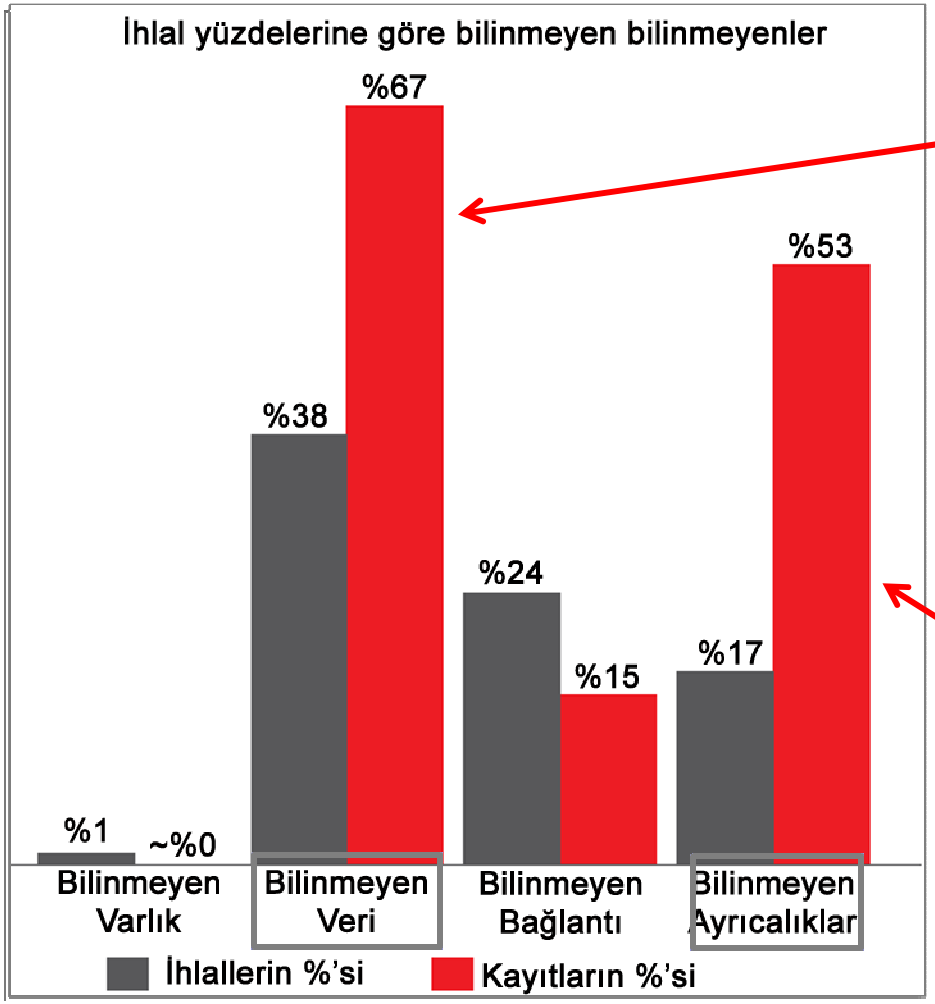
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

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

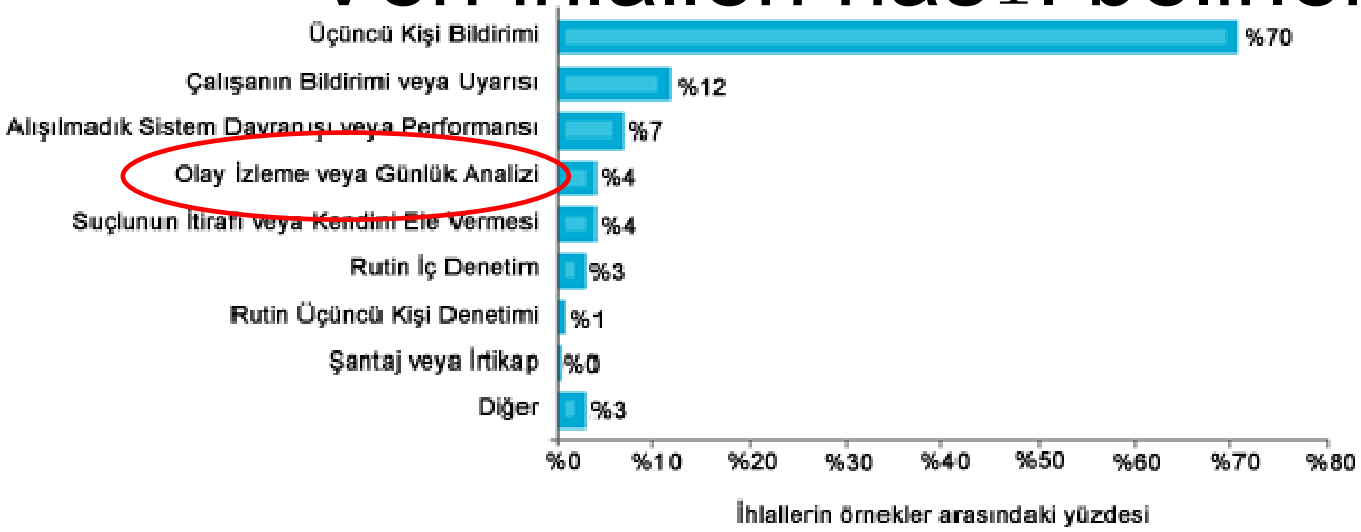


Bilinmeyen Veriler
"Burada hassas verilerin depolandığını bilmiyorduk bile"

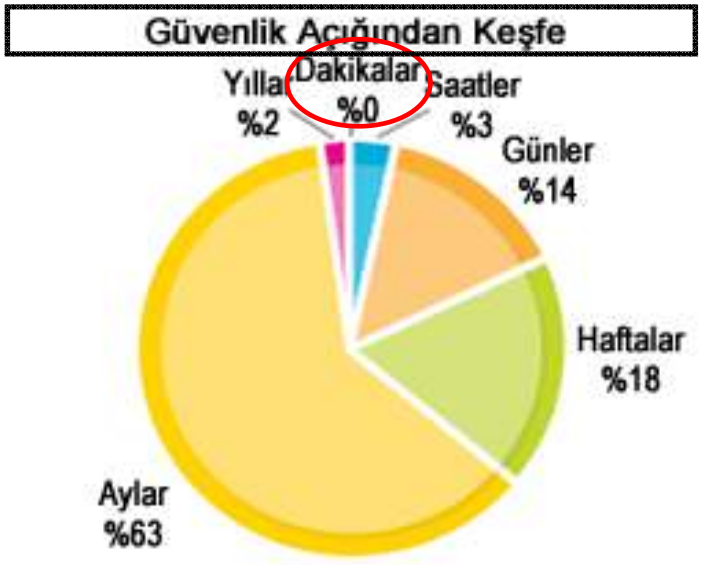
Bilinmeyen Ayrıcalıklar
"Bu ayrıcalıkların bu şekilde yapılandırıldığını bilmiyorduk"

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 Research

Publication Date: 28 April 2010 ID Number: G00208212

Ten Database Activities Enterprises Need to Monitor

Jeffrey Wheatman

Most enterprises are paying too little attention to the very real security risks associated with their databases. Auditors, security and risk professionals, and data owners need to watch for telltale behaviors that may indicate serious database security problems.

Key Findings

- The use of structured data storage, and the amount of data stored in this way, are increasing rapidly. This trend is largely driven by data analytics requirements and consolidation efforts.
- The information stored in enterprise databases is increasingly sensitive and subject to legal, regulatory and other compliance requirements.
- Despite the growing criticality of their databases, many enterprises continue to rely heavily on inadequate network and application-layer controls, and perform only minimal monitoring on database storage infrastructure.

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"

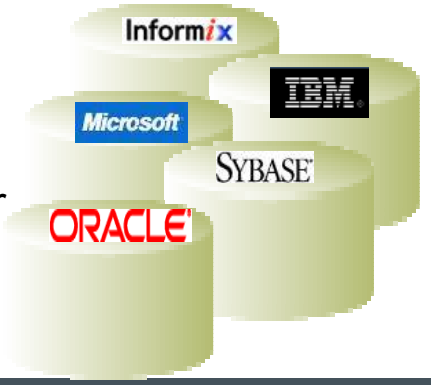
• Pek çok kuruluş, ağırlıklı olarak yetersiz ağ ve uygulama katmanı denetimlerine güvenmektedir ve veritabanlarını çok düşük seviyede izlemektedir"

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



Üçü Bir Arada:

Verinizi Arşivleyin,

Test Verinizi Yaratın,

Maskeleyin

Optim

THE POWER OF ENTERPRISE DATA MANAGEMENT

IBM yazılım zirvesi '10

KAOSTAN FIRSATA

- Kurumsal Veri Yönetiminde (EDM) Lider:
  - Veri Büyümesi
  - Veri Saklama & Sunma
  - Veri Güvenliği
  - Test Verisi Yönetimi
  - Uygulama Güncellemeleri
  - Uygulama Emekliliği
- 1989'dan beri karmaşık veri sorunlarına çözümler getirir
- Altyapı ve uygulama sağlayacıları ile partner çalışmaları yapmıştır: IBM, Oracle, EMC, Symantec, Hitachi ve diğerleri
- 2400 müşterisi; 50%'si Fortune 500
- 46% Pazar payı ile rakiplerinden en az iki kat önde(Gartner)
- Deloitte'un 2006 Technology Fast 500 araştırmasında "Yükselen Yıldız Firma" olarak adlandırılmıştır

Kurumsal Veri Yönetimi Daha Güçlü İş Sonuçları Getirir

Performans İyileştirmesi

- Geçmişe dönük sık kullanılmayan verilerin süzülerek, güvenli bir arşiv ortamına aktarılması ile Uygulama performansının arttırılması
- Hizmet Seviyesi Anlaşmaların (SLA) gereklerinin sürekli olarak sağlanması

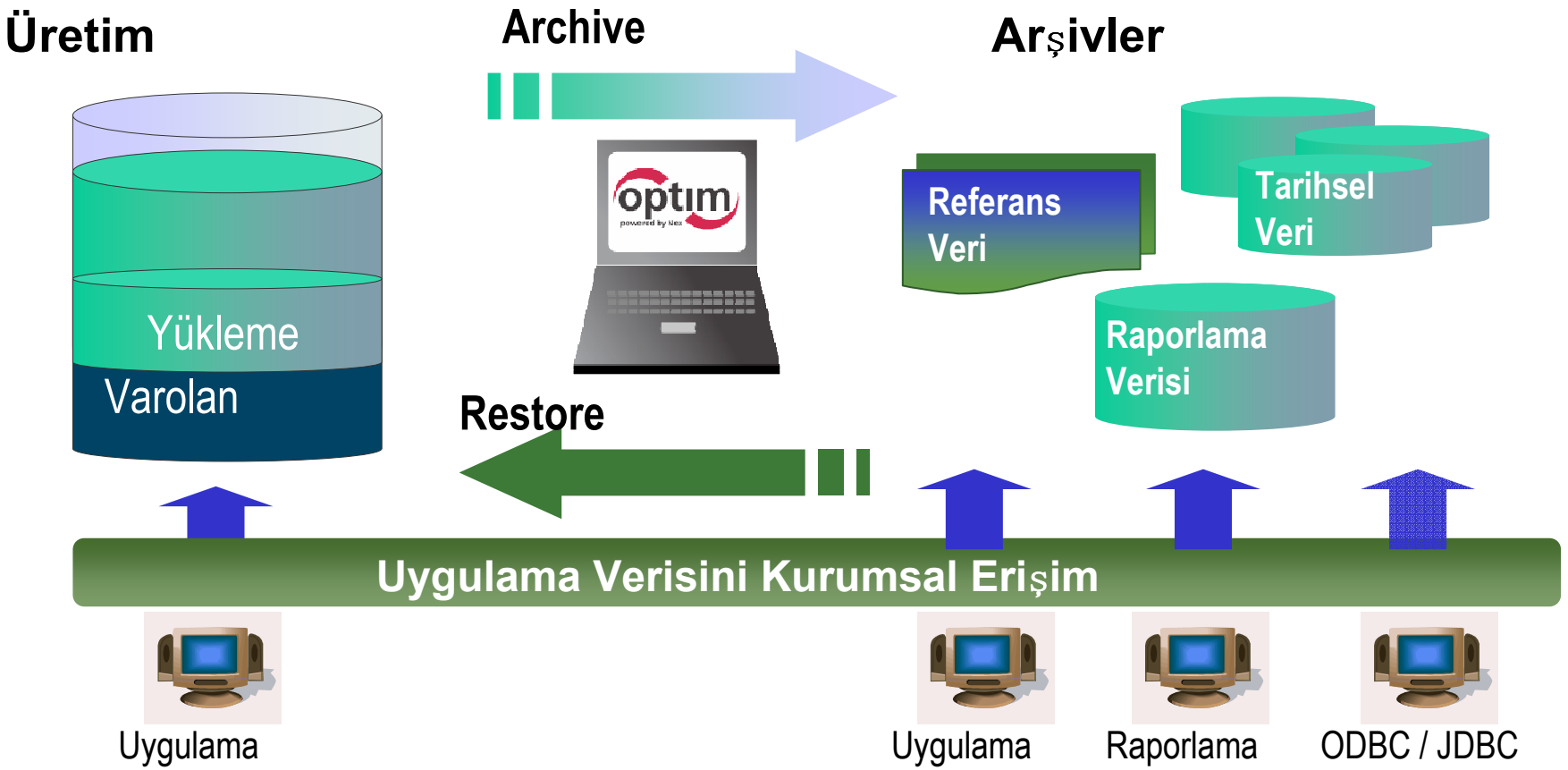
Riskin Azaltılması

- Endüstriye yönelik kuralların gerçeklenmesi (SOX, HIPPA, PII)
- Veri Saklama/Tutma – Arşiv Verisi erişim ve yönetimi; İstekleri karşılanabilir kılma, Audit/e-discovery isteklerine doğru ve tam sonuç oluşturma
- Veri gizliliği gereksinimlerinin sağlanması

Masraf Kontrolü

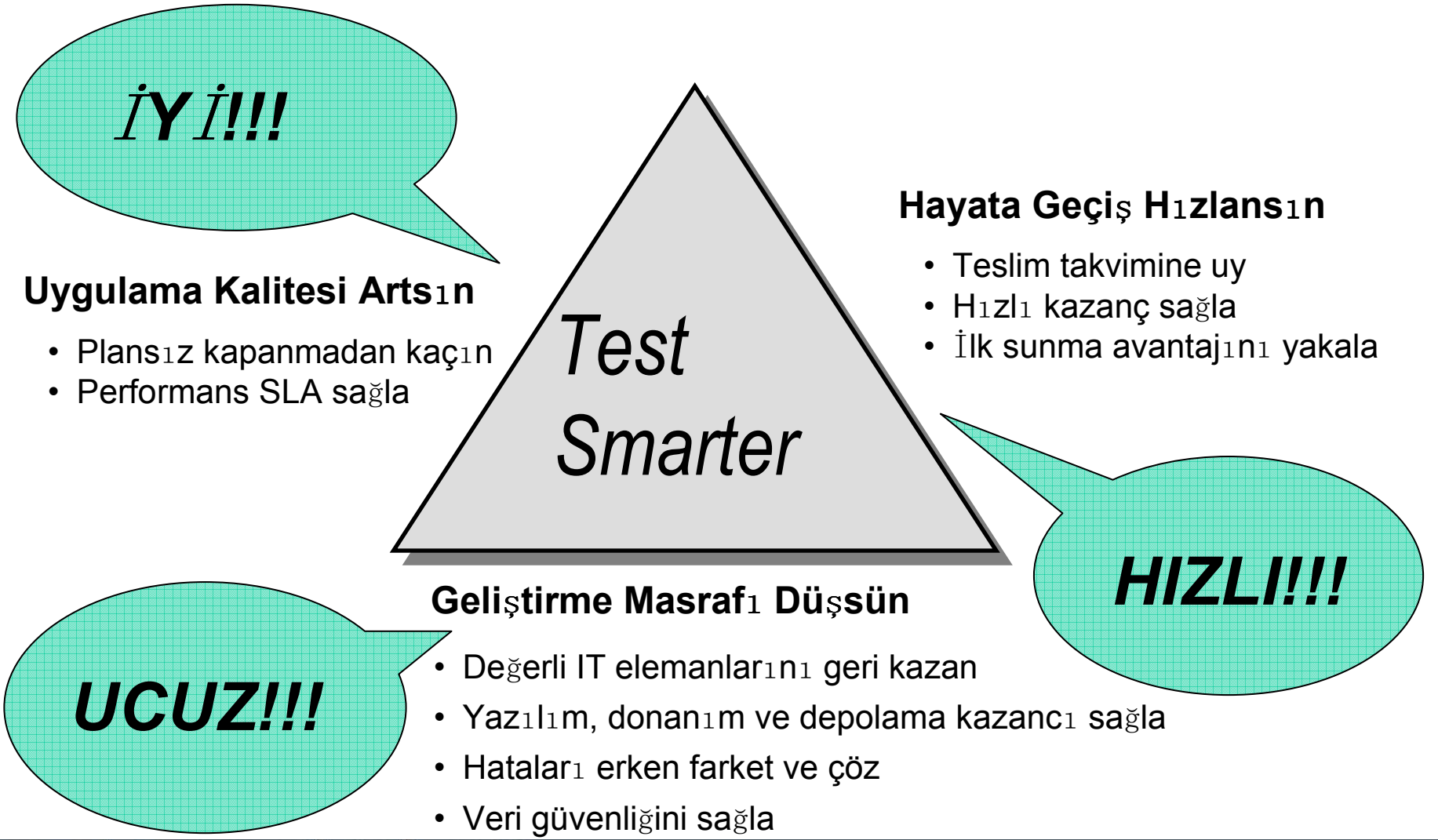
- Altyapı (Storage) maliyeti azaltılır
- Ortalama Veri büyümesi %40
- Uyumluluk masrafları düşer (Ceza lar karşısında ödenmesi gereken)
- Test/Geliştirme Veri Yönetimi altyapısı

IBM Optim Veri Büyümesi Çözümü: Arşivleme

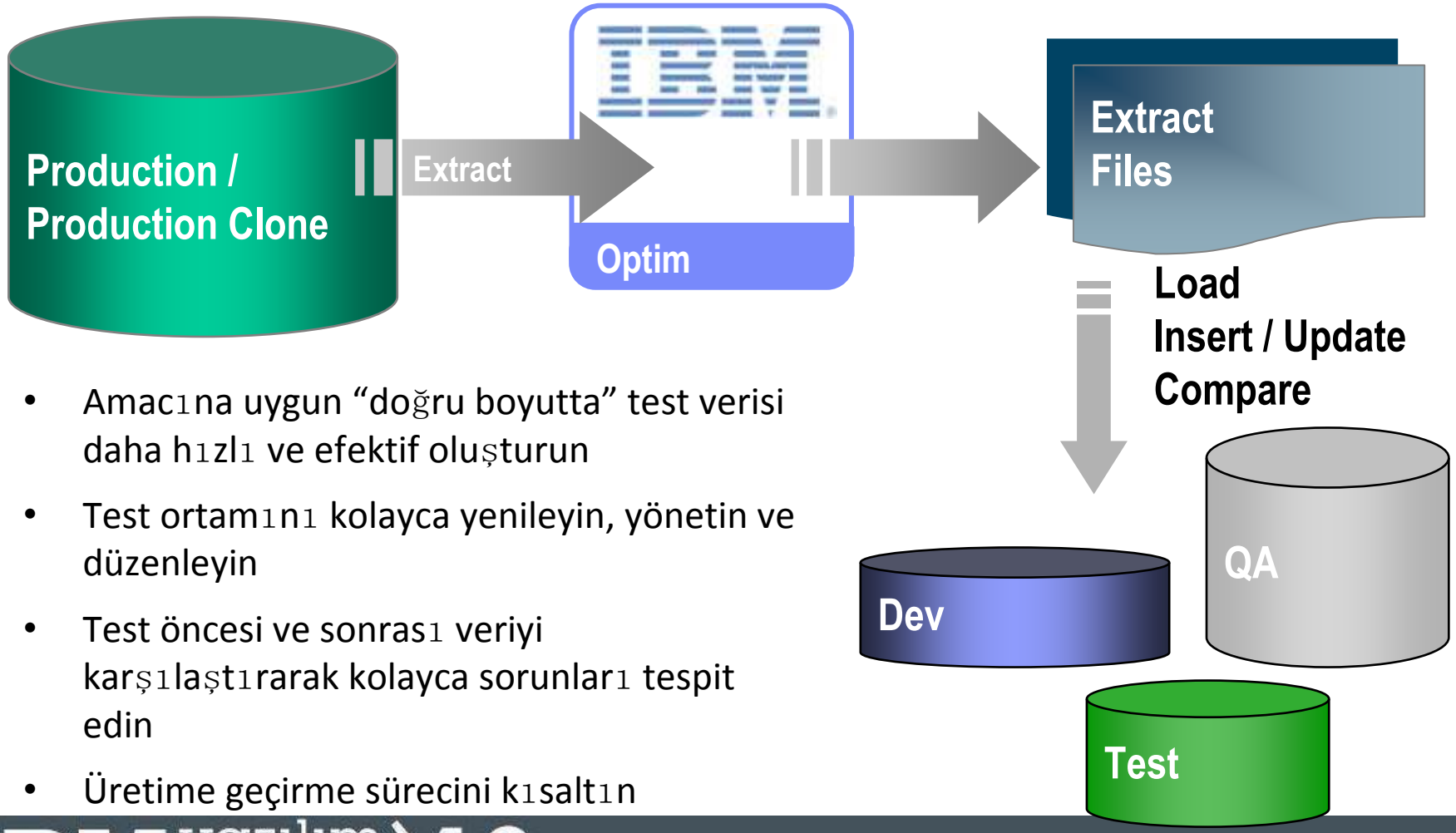


- Tümleşik İş Nesnesi özelliği ile Verinin Tarihsel Resmini üretebilirsiniz
- Veri Saklama Ünitelerinden bağımsızlık ile ILM
- Değişmezliği kesin dosya formatı ile veri saklama yönetmeliklerine uyum sağlanır.

Test Veri Yönetimi



IBM Optim Test Veri Yönetimi Çözümü



- Amacına uygun "doğru boyutta" test verisi daha hızlı ve efektif oluşturun
- Test ortamını kolayca yenileyin, yönetin ve düzenleyin
- Test öncesi ve sonrası veriyi karşılaştırarak kolayca sorunları tespit edin
- Üretime geçirme sürecini kısaltın

Veri Gizliliği

- **Hassas verilerin**
  - Üretim dışı ortamlarda korunmasını sağlar
  - Gerçek verileri hayali ama anlamli veriler ile değiştirme imkanı sağlar
  - Bir takım hazır maskeleme algoritmaları sunar
  - Özel amaçlara yönelik maskeleme fonksiyonları oluşturma ve kullanma imkanı sağlar

Enterprise Challenge: Data Privacy

Optim™ Data Privacy Solution

Veri maskeleme yöntemleri:

- String literal values
- Character substrings
- Random or sequential numbers
- Arithmetic expressions
- Concatenated expressions
- Date aging
- Lookup values
- Intelligence

Örnek 1

Patient Information

Patient No.	123456	**SSN**	333-22-4444
Name	Erica Schafer		
Address	12 Murray Court		
City	Austin	TX	78704

Anlamsal olarak bütünlüğü bozulmayacak şekilde maskelenmiş veri

Örnek 2

Personal Info Table

PersNbr	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	Pablo	Picasso

Anahtar Yayma (Key Propogation) ile veri bütünlüğü korunur

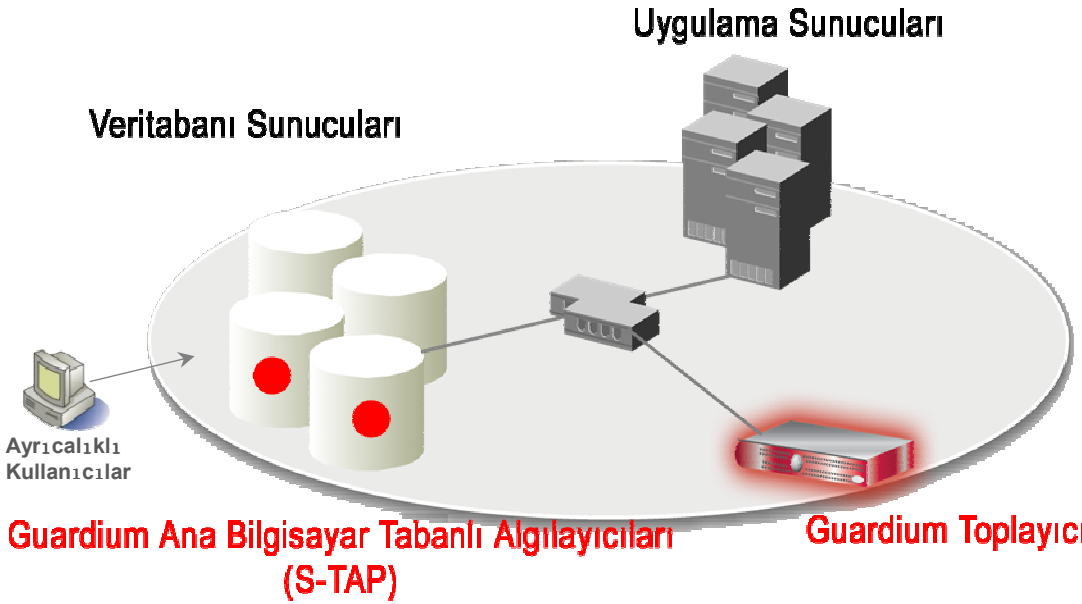
Event Table

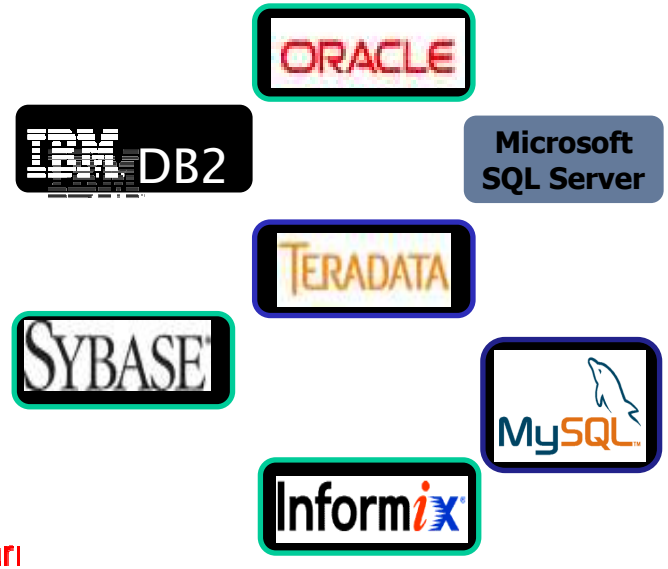
PersNbr	FstNEvtOwn	LstNEvtOwn
10002	Pablo	Picasso
10002	Pablo	Picasso

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 müşteri
- Aralık 2009'dan bu yana, IBM'in Bütünleştirilmiş Veri Yönetimi portföyünün bir parçasıdır.

Gerçek Zamanlı Veritabanı Güvenliği ve İzleme

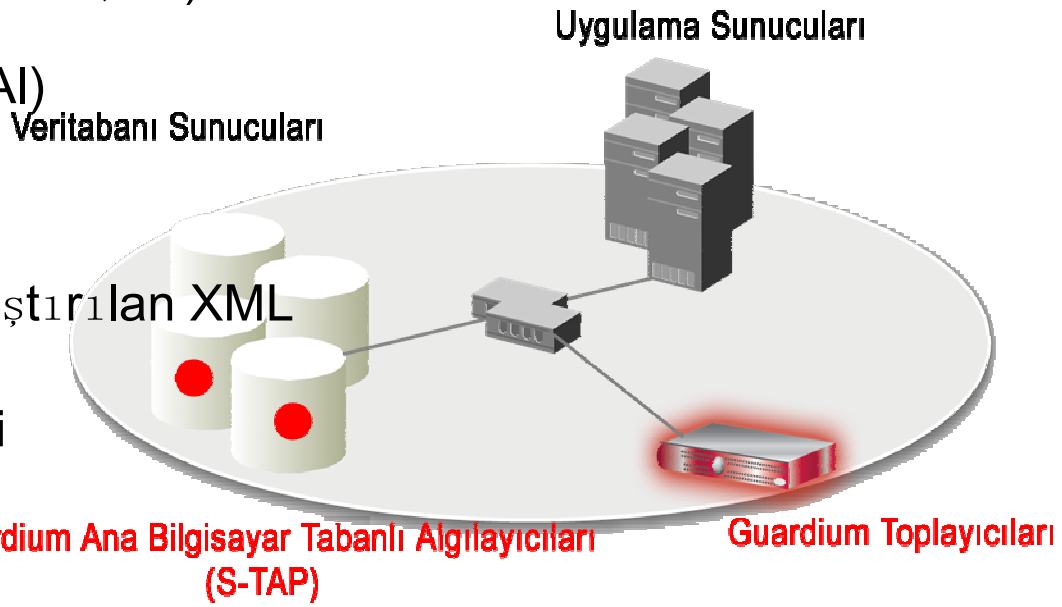




- Yerel veritabanı yöneticisi erişimi dahil %100 görünürlük
- DBMS veya uygulama değişikliği yoktur
- Veritabanı performansı üzerinde en düşük seviyede etki
- Müdahale edilmesi mümkün olmayan denetim havuzu ile görevlerin ayrılmasını sağlar
- Parçacıklı ilkeler, izleme ve denetim, Kimi, Neyi, Nedeni 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



Guardium ile Uygulama Kullanıcısı İzleme

Bağlantı Havuzu Oluşturma Uygulamalarındaki Kullanıcıları Tanımlayın

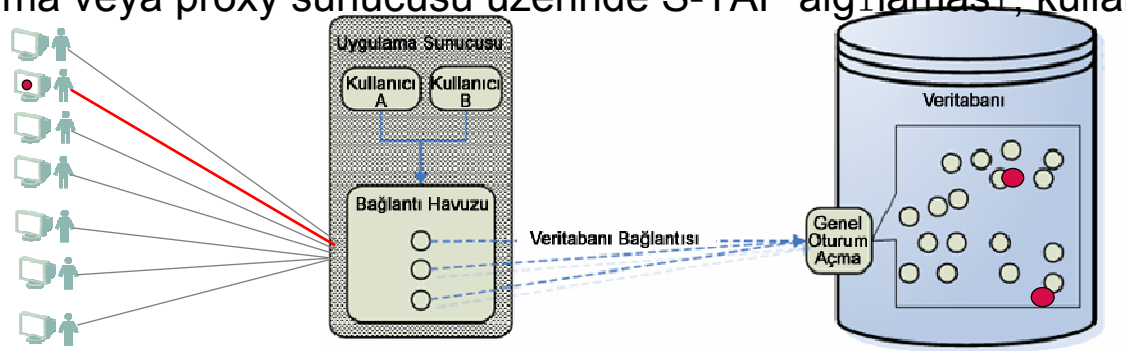
- Potansiyel dolandırıcılığı ortaya çıkarın
- Hassas tablolara kullanıcı erişimi için hatasız denetimler

Desteklenen Kurumsal Uygulamalar

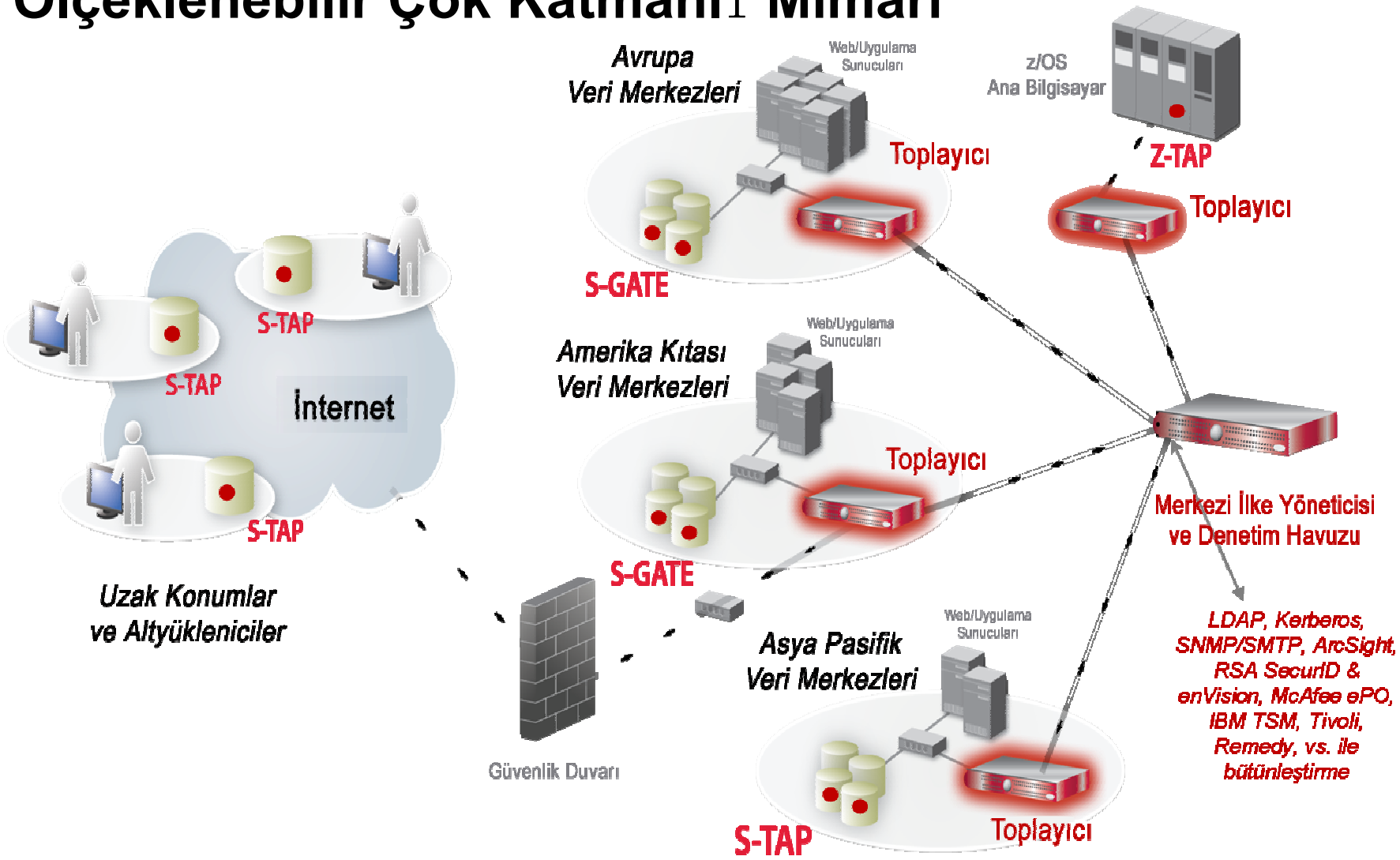
- Oracle E-Business Suite, PeopleSoft, Business Objects Web Intelligence, JD Edwards, SAP, Siebel, şirket içinde oluşturulan özel uygulamalar

Uygulama Kullanıcı Kimliğinin Yakalanmasında Kullanılan Çeşitli Yöntemler

- Tablo, tetik, vs. aracılığıyla altta yatan veritabanından özgün kimliği alır
- Prosedürlere olan çağrıları izler ve parametrelerinden bilgi alır
- Uygulama veya proxy sunucusu üzerinde S-TAP algılaması, kullanıcı kimliğini alır



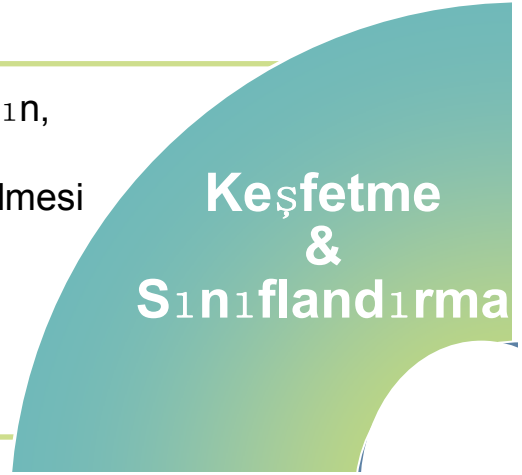
Ölçeklenebilir Çok Katmanlı Mimari



Veritaban1 Risk ve Uyumluluk Yönetimi Tam Çevrimi

Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

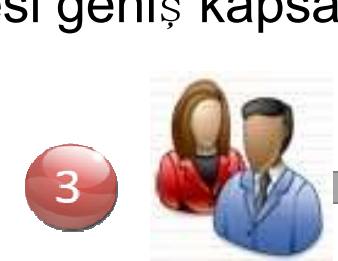
- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilmesi ve sınıflandırılması



Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

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:



Gözlenen Davranış

- Başarısız oturum açmalar
- Paylaşılan kimlik bilgileri
- Mesai saatleri dışında oturum açma
- Varsayılan kullanıcı erişimi

Veritabanı Katmanı
(Oracle, SQL Server, DB2, Informix, Sybase, MySQL)

İşletim Sistemi Katmanı
(Windows, Solaris, AIX, HP-UX, Linux)

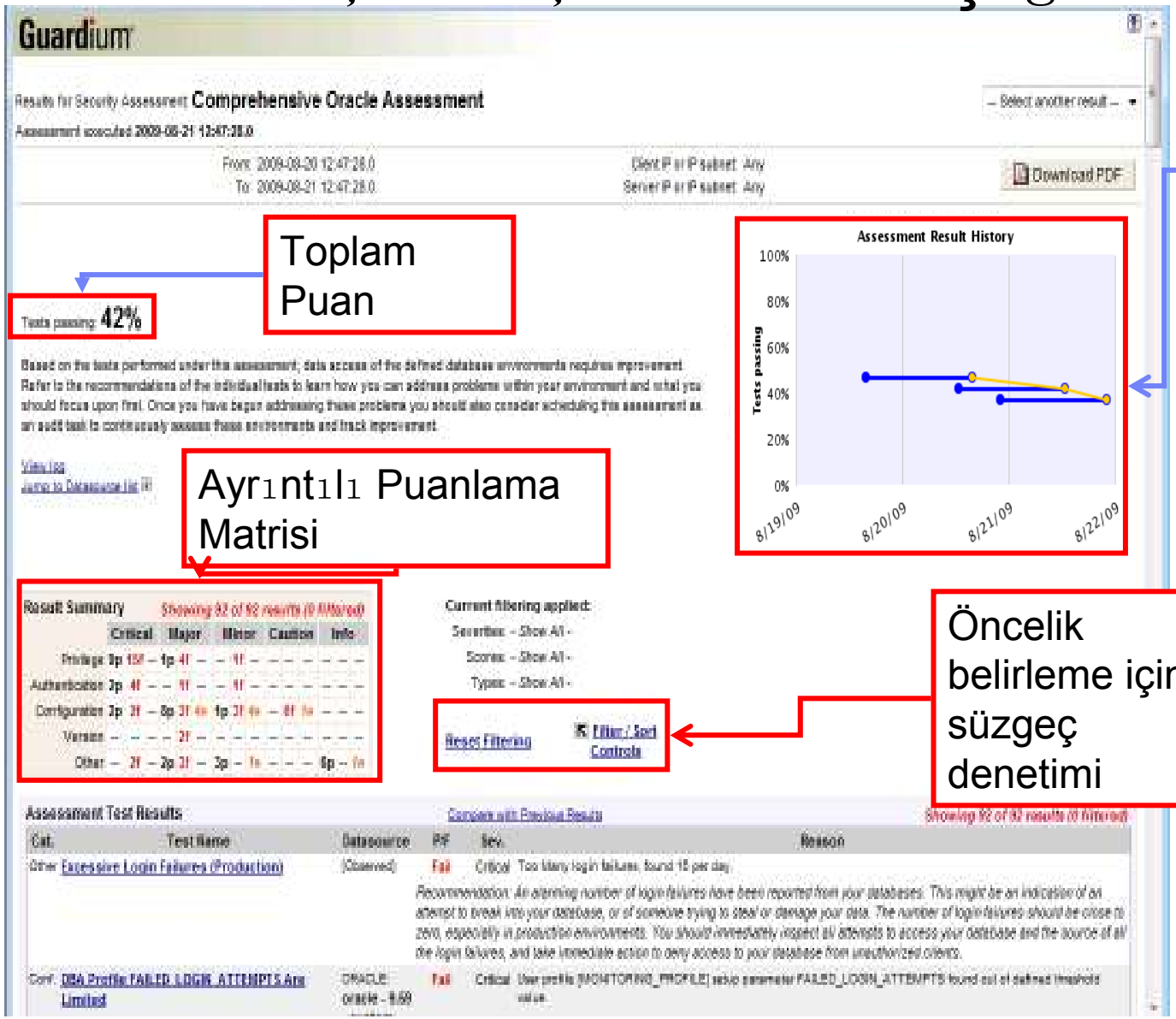
Veritabanı Ayarları

- Görevler
- Yapılandırmalar
- Sürümler
- Özel testler

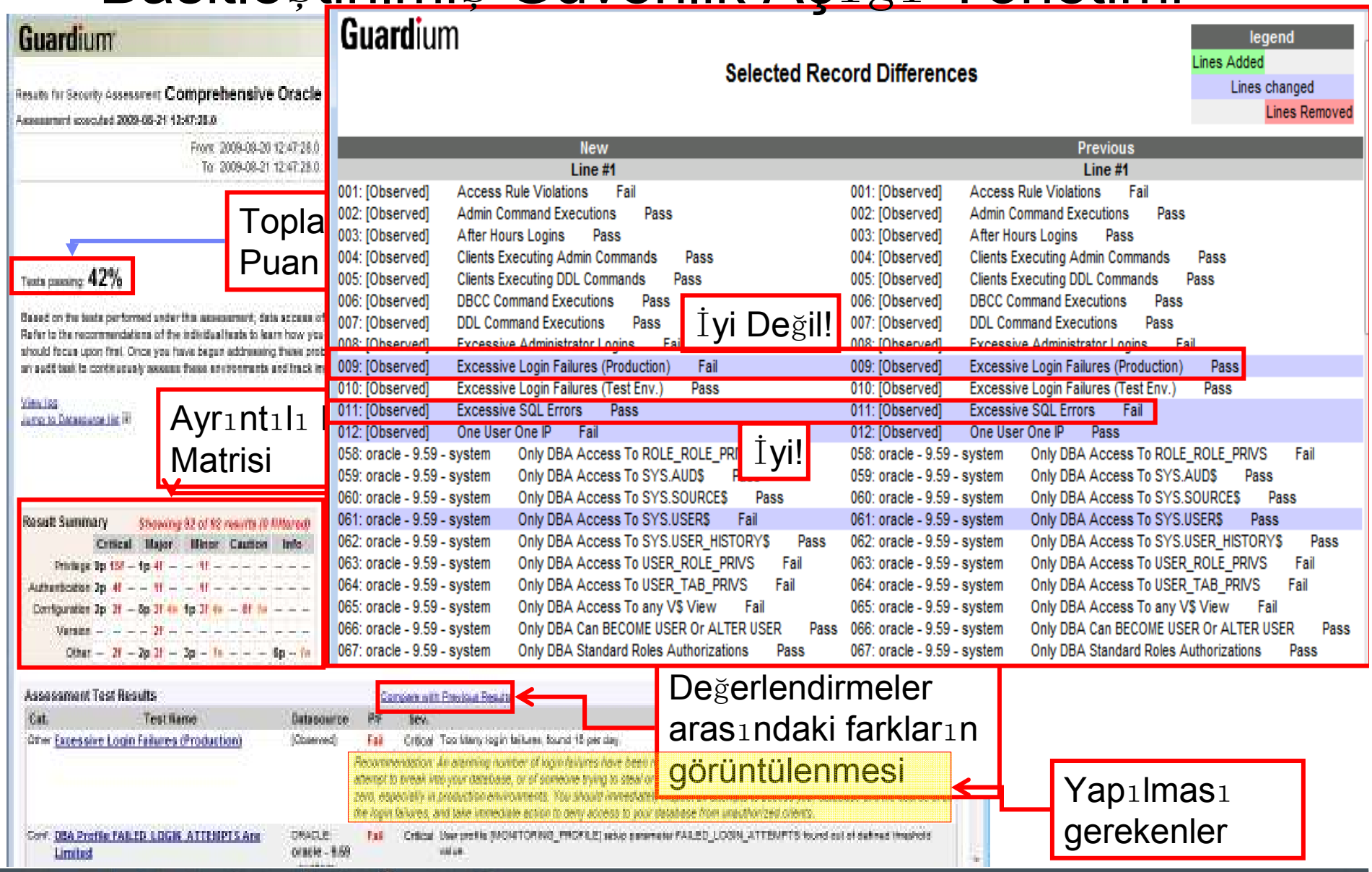
İşletim Sistemi Ayarları

- Yapılandırma dosyaları
- Ortam değişkenleri
- Kayıt dosyası ayarları
- Özel testler

Basitleştirilmiş Güvenlik Açığı Yönetimi



Basitleştirilmiş Güvenlik Açığı Yönetimi

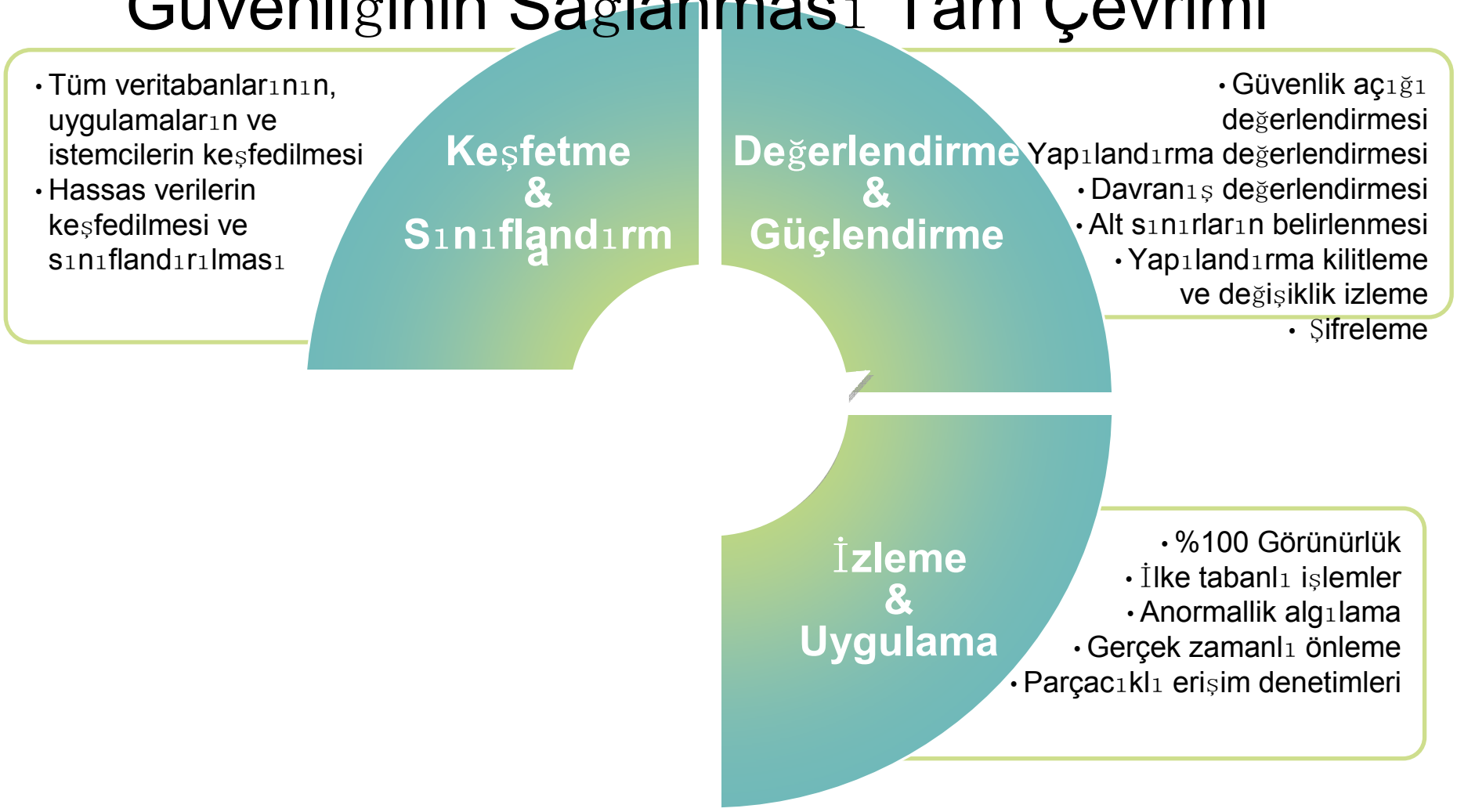


Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

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

Guardium kullanmaya başlamak için

Nereden Başlanır

Gartner Research

Publication Date: 28 April 2010 ID Number: G00200212

Ten Database Activities Enterprises Need to Monitor

Jeffrey Wheatman

Most enterprises are paying too little attention to the very real security risks associated with their databases. Auditors, security and risk professionals, and data owners need to watch for telltale behaviors that may indicate serious database security problems.

Key Findings

- The use of structured data storage, and the amount of data stored in this way, are increasing rapidly. This trend is largely driven by data analytics requirements and consolidation efforts.
- The information stored in enterprise databases is increasingly sensitive and subject to legal, regulatory and other compliance requirements.
- Despite the growing criticality of their databases, many enterprises continue to rely heavily on inadequate network and application-layer controls, and perform only minimal monitoring on database storage infrastructure.

Gartner

"Kurulu?lar?n Denetlemesi Gereken Kritik Önem Ta??yan Etkinlikler"

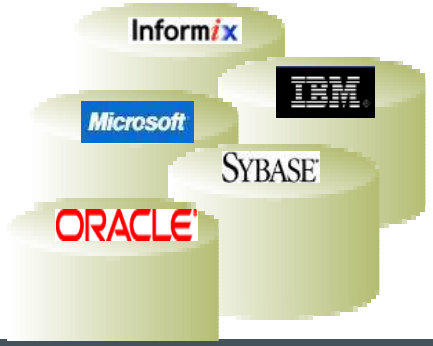
- Ayr?cal?kl? Kullan?c?lar
  - Kritik verilere Eri?im/De?i?tirme/Silme
  - Uygun olmayan kanallar kullan?larak eri?im
  - ?ema de?i?iklikleri
  - Yetkisiz kullan?c? hesab? ekleme
- Son Kullan?c?lar
  - Normalde gerekli olmayan a??r? miktarda veriye eri?im
  - Standart mesai saatleri d???nda verilere eri?im
  - Uygun olmayan kanallar arac?l???yla verilere eri?im
- Geli?tiriciler, Analistler ve Sistem Yöneticileri
  - Etkin üretim sistemlerine eri?im
- BT Operasyonlar?
  - Veritabanlar?nda veya veritaban?na eri?en uygulamalarda onaylanmam?? de?i?iklikler

Guardium'un işiniz için sağladıkları :

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



TURKCELL

- İhtiyaçlarımız
- Test Süreci
- Kriterlerimiz
- Turkcell Veritabanı İzleme Yapısı
- Sonuç

İhtiyaçlarımız

- Veritabanı izleme yapısının oluşturulması
- Vaka takip yapısının esnek, devamlı raporlanabilir bir hale getirilmesi
- SoX

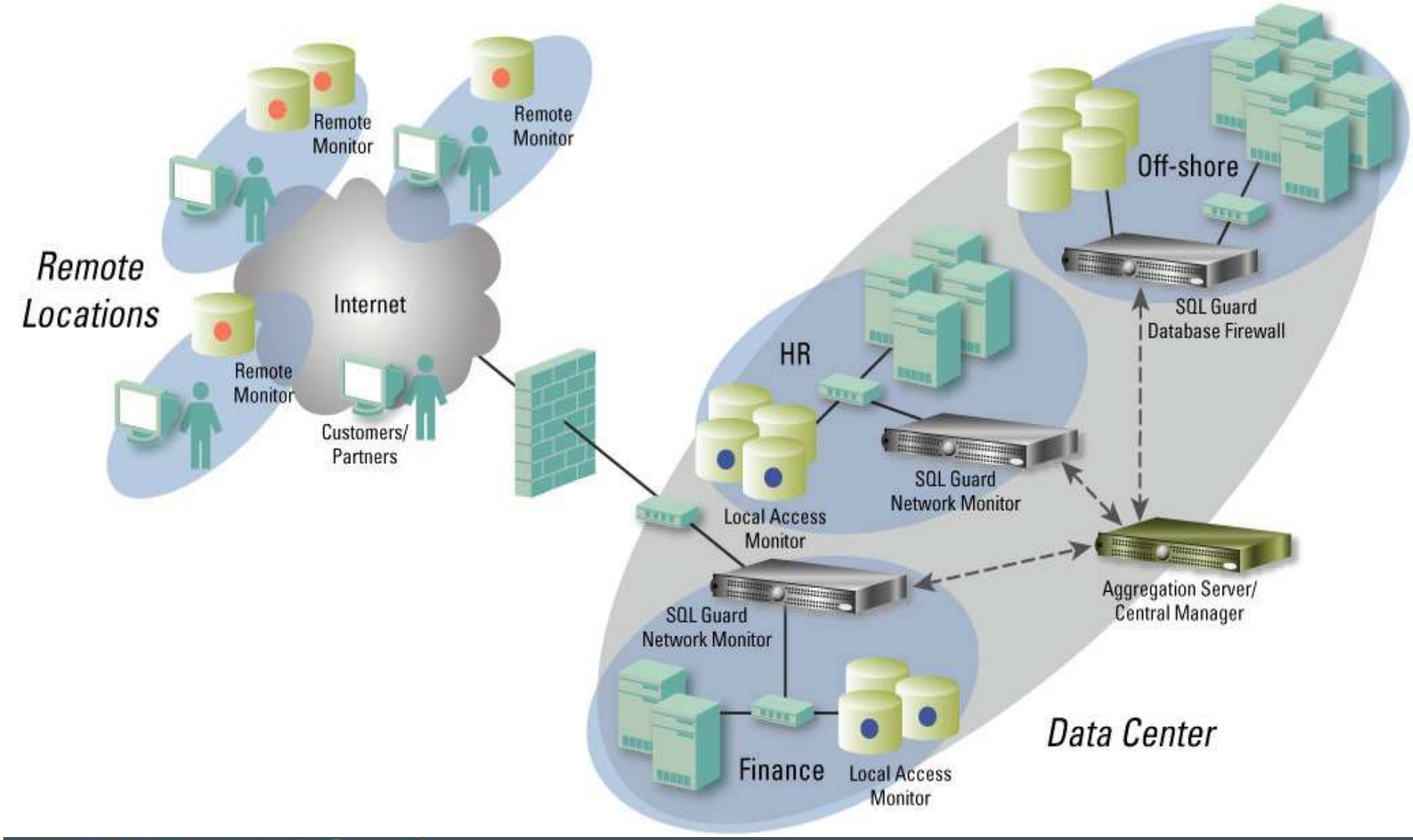
Test Süreci

- İhtiyaçlarımıza uygun dört ürünü belirledik.
- İki ürün üzerinde uzun bir test süreci gerçekleştirdik.
- İşlem hacmi en büyük sistemlerimizde test ettik.
- Farklı implemetasyon kurguları ile testler yaptık (Agent, Span vb.).

Kriterlerimiz

- Sistemlere olan performans etkisinin az olmasıdır.
- Log toplama konusunda esnek çözümler üretebiliyor olması.
- Yönetiminin kolay olması.
- Raporlama ekranlarının ihtiyaçlarımıza en yakın ürün olması.
- Ürünün Türkiye desteğinin olması.
- Loglara en az müdahale edilebilen bir yapının kurulması.
- Lokalde yapılan işlemleri loglayabiliyor olması.

Turkcell Veritabanı İzleme Yapısı



Sonuç

- SOX uyumluluğunda veritabanı konusunda çözüm üretme
- Veritabanı güvenliğini merkezi yönetme
- Güvenlik riski yüksek seviyeli senaryolar için real-time alarm üretme
- Riskli operasyonel işlemleri periyodik raporlama
- Otomatik çağrı süreci

TESEKKURLER