

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 Arařtırmalar Raporu

Verizon Business RISK ekibi tarafından gerekleřtirilen bir arařtırma

Yönetici Özeti

2008 yılı, muhtemelen hem kuruluşlar hem de tüketiciler için karışık bir yıl olarak hatırlanacaktır. Korku, belirsizlik ve şüphe küresel finans piyasalarının 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 varsayılmayacağını hatırlatmıştır.

2009 Veri İhlali Arařtırmalar Raporu, tarihin bu çalkantılı dönemini adli arařtırmacıların 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.

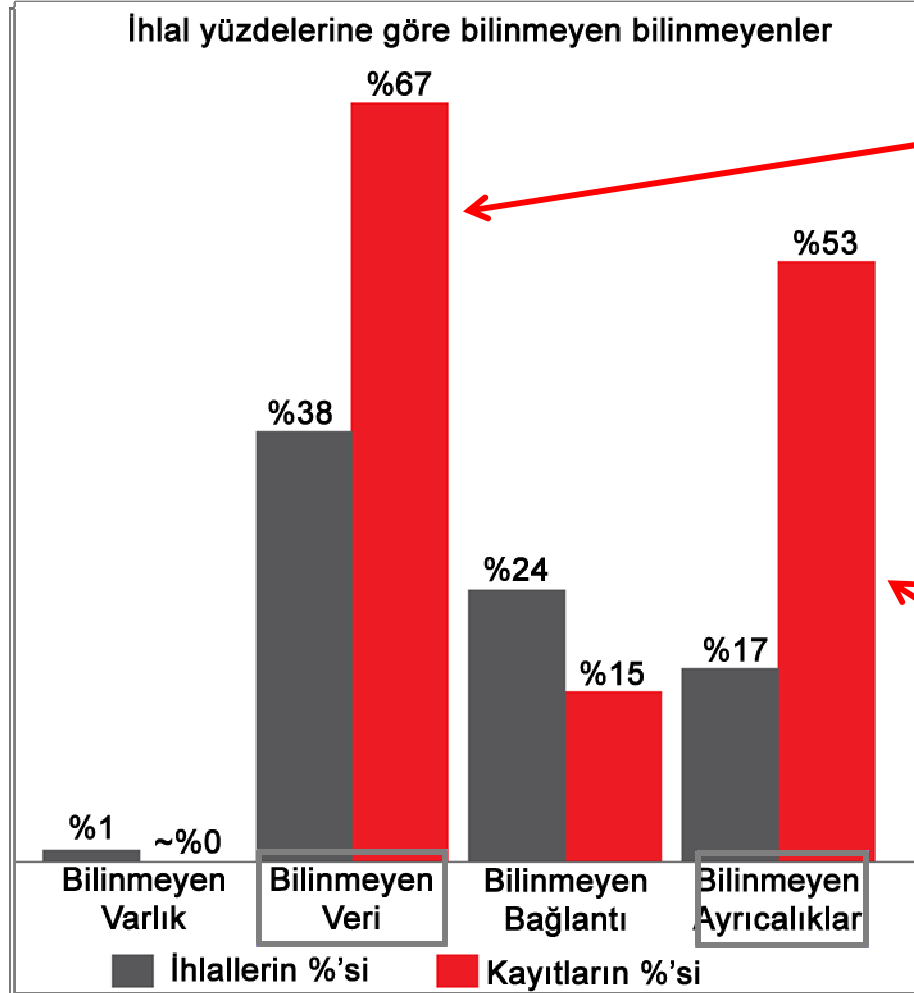
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

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

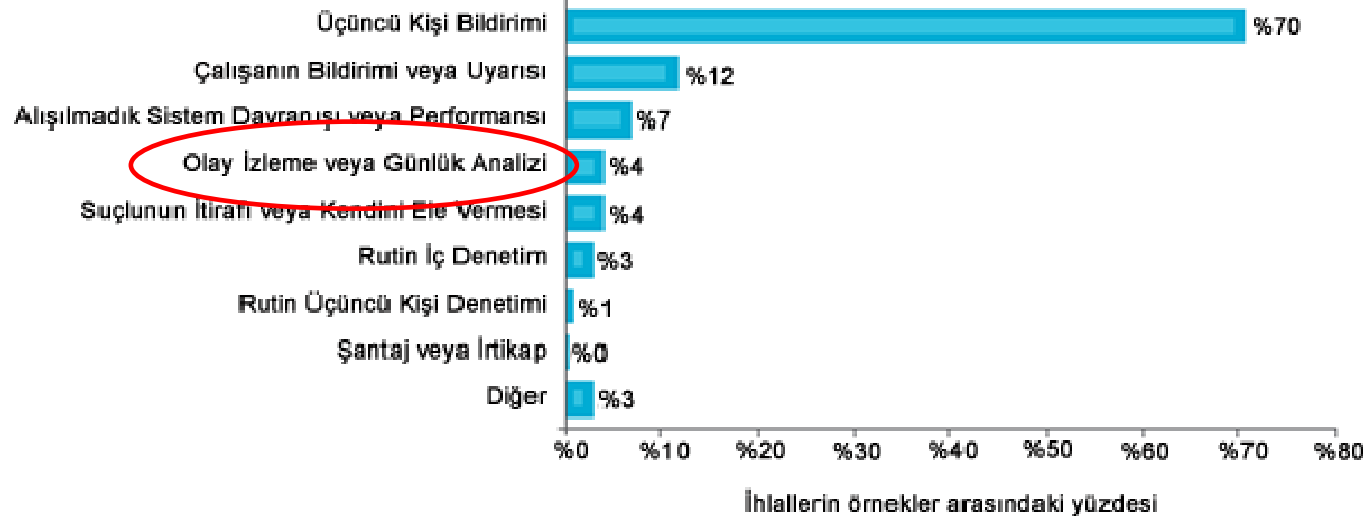
"Burada hassas verilerin depolandığını bilmiyorduk bile"

Bilinmeyen Ayrıcalıklar

"Bu ayrıcalıkların bu şekilde yapılandırıldığını bilmiyorduk"

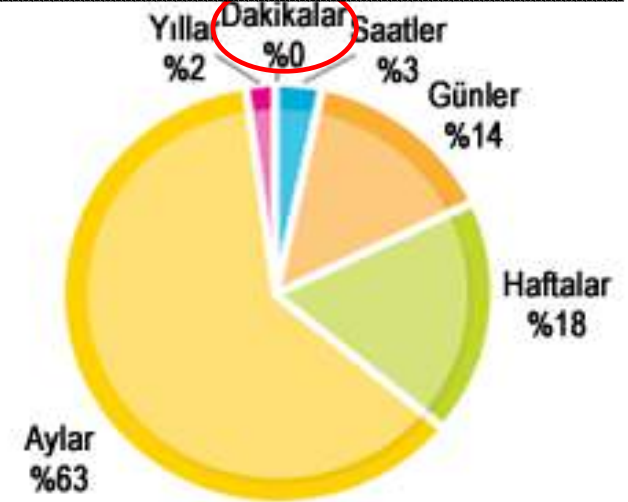
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Veri ihlalleri nasıl belirlenir?



Veri İhlali Keşif Yöntemleri

Güvenlik Açısından Keşfe



Analistler veritabanı güvenliđi hakkında ne düşünüyor?

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

- Gartner Research, 28 Nisan 2010





Veritabanı Etkinliđi İzleme

- "İlişkişel 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 ađ ve uygulama katmanı denetimlerine güvenmektedir ve veritabanlarının çok düşük seviyede izlemektedir"

Veritabanı denetimi neden bu kadar zor?

Günümüzde veritabanlarının çoğu nasıl denetleniyor?

DBMS içindeki yerel denetim günlüklerine bağımlılık

× Görünürlüğü ve parçalı yapısı yoktur

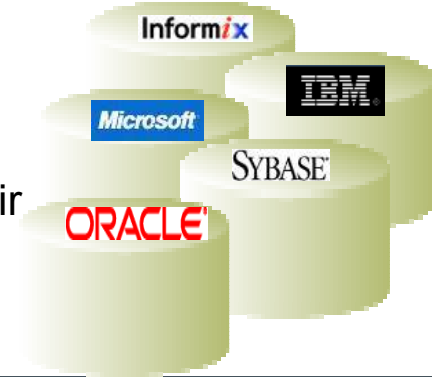
- » Ayrıcalıklı kullanıcıların izlenmesi zordur
- » Uygulamanın "gerçek kullanıcılarının" takip edilmesi zordur
- » Denetimin ayrıntı düzeyi yetersizdir

× 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



IBM yazılım
zirvesi 10

THE POWER OF
ENTERPRISE DATA
MANAGEMENT

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 sağlayıcıları 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 gerçekleşmesi (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

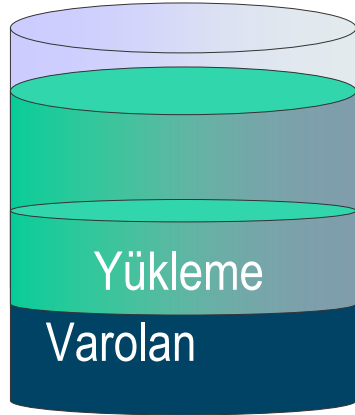
- Altyapı (Storage) maliyeti azaltılır
- Ortalama Veri büyümesi %40
- Uyumluluk masrafları düşer (Ceza lar karşısında ödenmesi gereken)
- Test/Geliştirme Veri Yönetimi altyapısı

IBM Optim Veri Büyümesi Çözümü: Arşivleme

Üretim

Archive

Arşivler



Restore



Uygulama Verisini Kurumsal Erişim



Uygulama



Uygulama



Raporlama



ODBC / JDBC

- Tümlerik 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

İYİ!!!

Uygulama Kalitesi Artsın

- Plansız kapanmadan kaçın
- Performans SLA sağla

***Test
Smarter***

Hayata Geçiş Hızlansın

- Teslim takvimine uy
- Hızlı kazanç sağla
- İlk sunma avantajını yakala

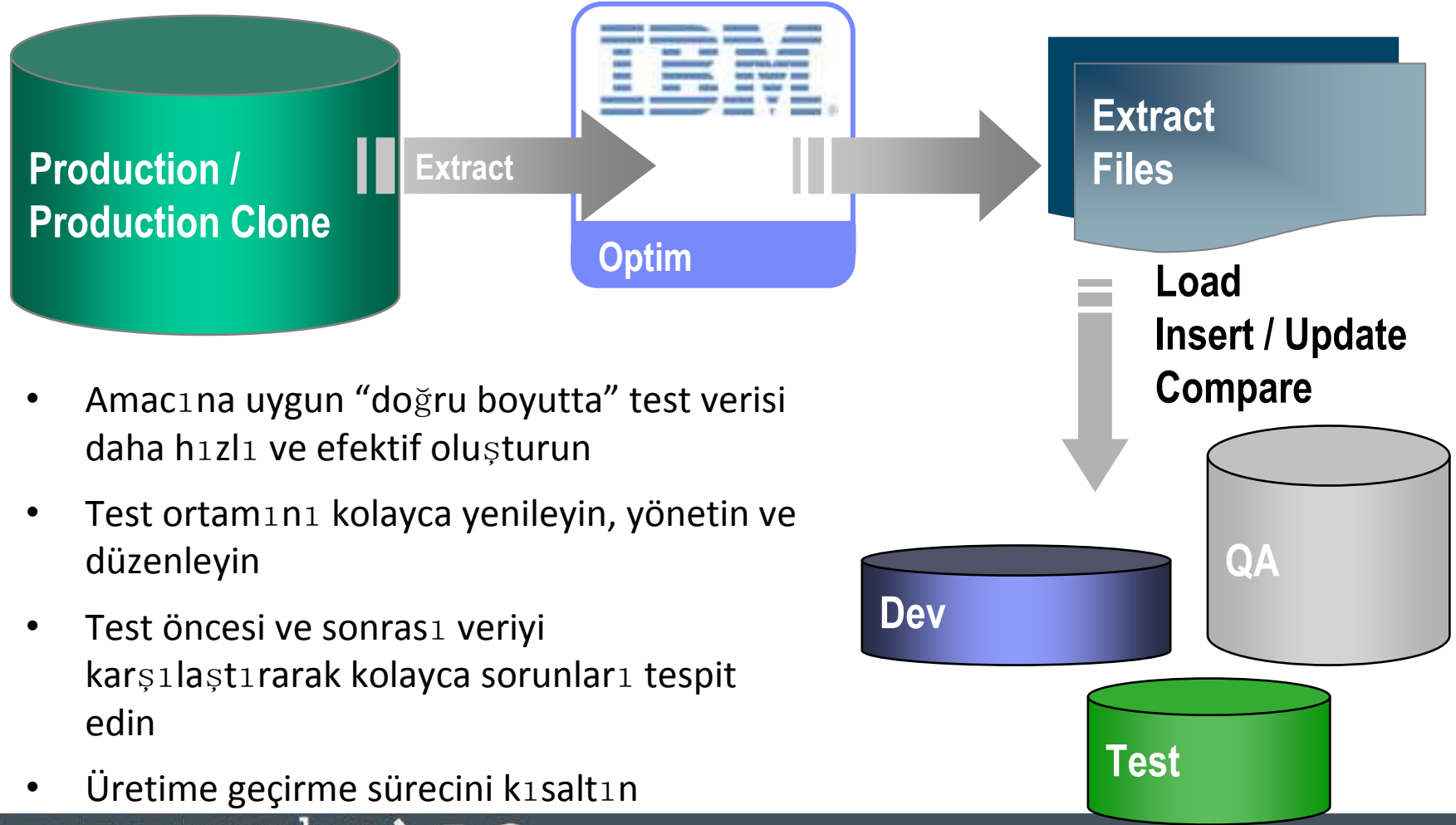
HIZLI!!!

UCUZ!!!

Geliştirme Masrafı Düşsün

- Değerli IT elemanlarını geri kazan
- Yazılım, donanım ve depolama kazancı sağla
- Hataları erken farket ve çöz
- Veri güvenliğini sağla

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



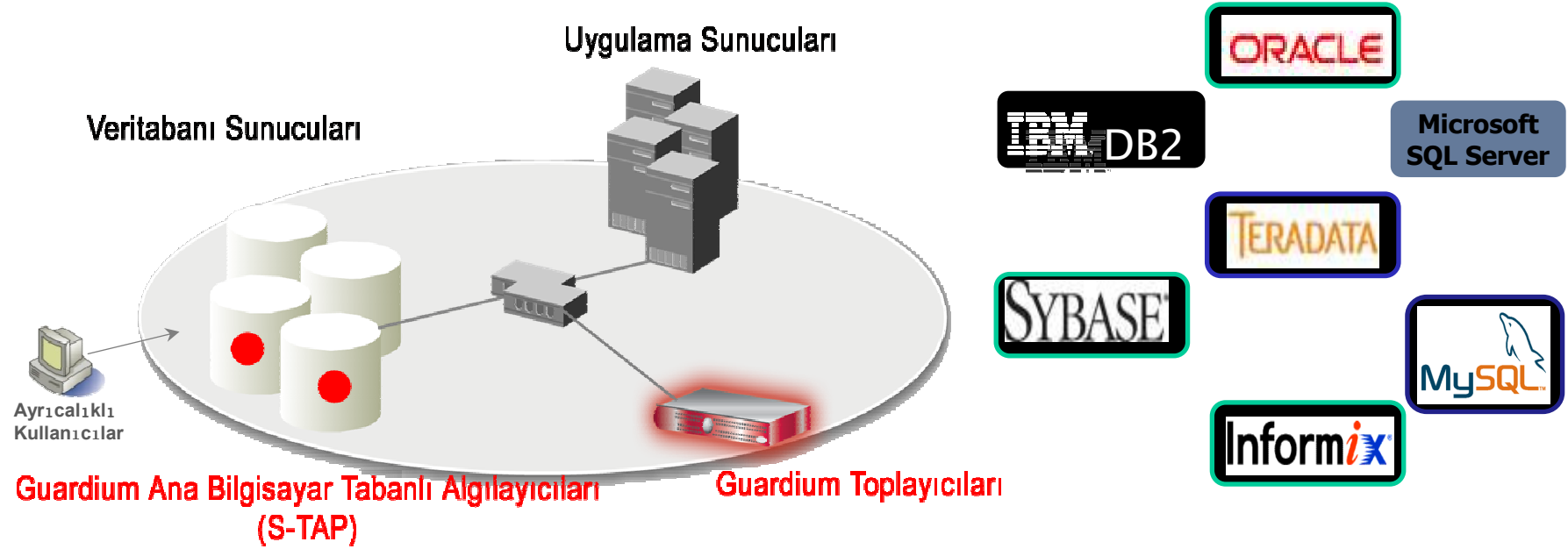
- **Hassas verilerin**

- Üretim dışı ortamlarda korunmasını sağlar
- Gerçek verileri hayali ama anlamlı veriler ile değiştirme imkanı sağlar
- Bir takım hazır maskeleyme algoritmaları sunar
- Özel amaçlara yönelik maskeleyme fonksiyonları oluşturma ve kullanma imkanı sağlar

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.

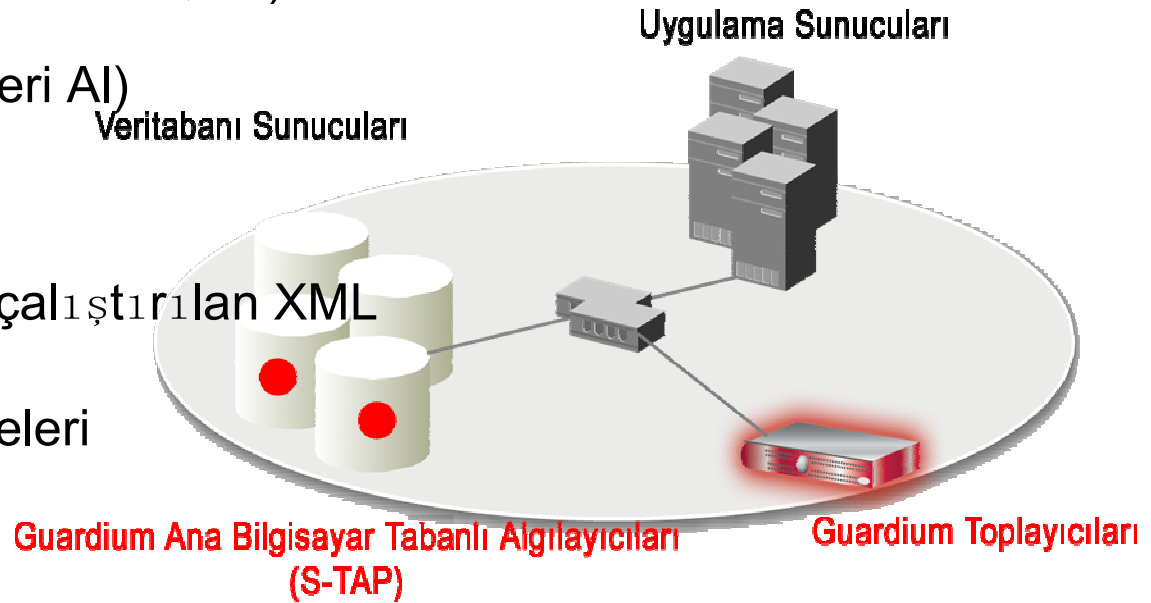
Gerçek Zamanlı Veritabanı Güvenliği ve İzleme



- Yerel veritabanı yöneticisi erişimi dahil %100 görünürlük
- DBMS veya uygulama değişikliği yoktur
- Veritabanı performans üzerinde en düşük seviyede etki
- Müdahale edilmesi mümkün olmayan denetim havuzu ile görevlerin ayrılmasını sağlar
- Parçalı ilkeler, izleme ve denetim, Kimi, Neyi, Nedeni ve Nasıl sağlar
- Gerçek zamanlı, ilke tabanlı uyarılar
- 3-6 aylık denetim verilerini aygıtın kendisinde depolayabilir ve arşivleme sistemleri ile bütünleşir

Guardium neyi izler?

- SQL hatalar₁ ve başarısız oturum açmalar
- DDL komutlar₁ (Tablo Oluştur/Bırak/Değiştir)
- SELECT sorgulamalar₁
- DML komutlar₁ (Ekle, Güncelle, Sil)
- DCL komutlar₁ (Ver, Geri Al)
- Prosedür dilleri
- Veritabanı tarafından çalıştırılan XML
- Geri dönen sonuç kümeleri



Guardium ile Uygulama Kullanıcısı İzleme

Bağlantı Havuzu Oluşturma Uygulamalarındaki Kullanıcıları Tanımlayın

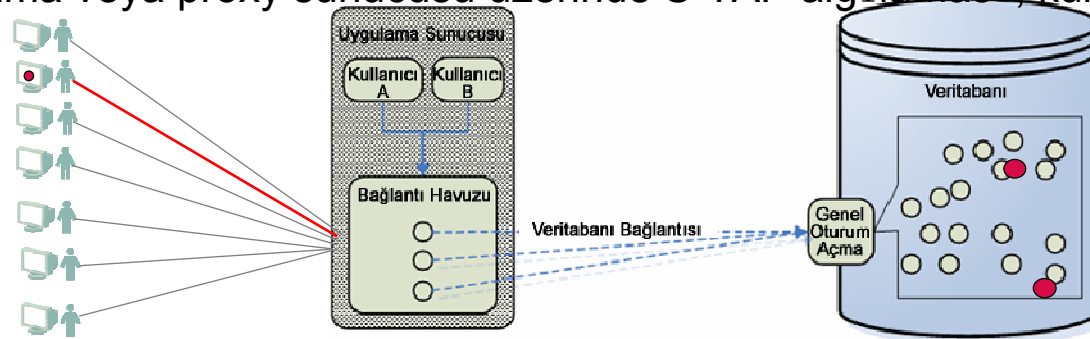
- Potansiyel dolandırıcılığı ortaya çıkarın
- Hassas tablolara kullanıcı erişimi için hatasız denetimler

Desteklenen Kurumsal Uygulamalar

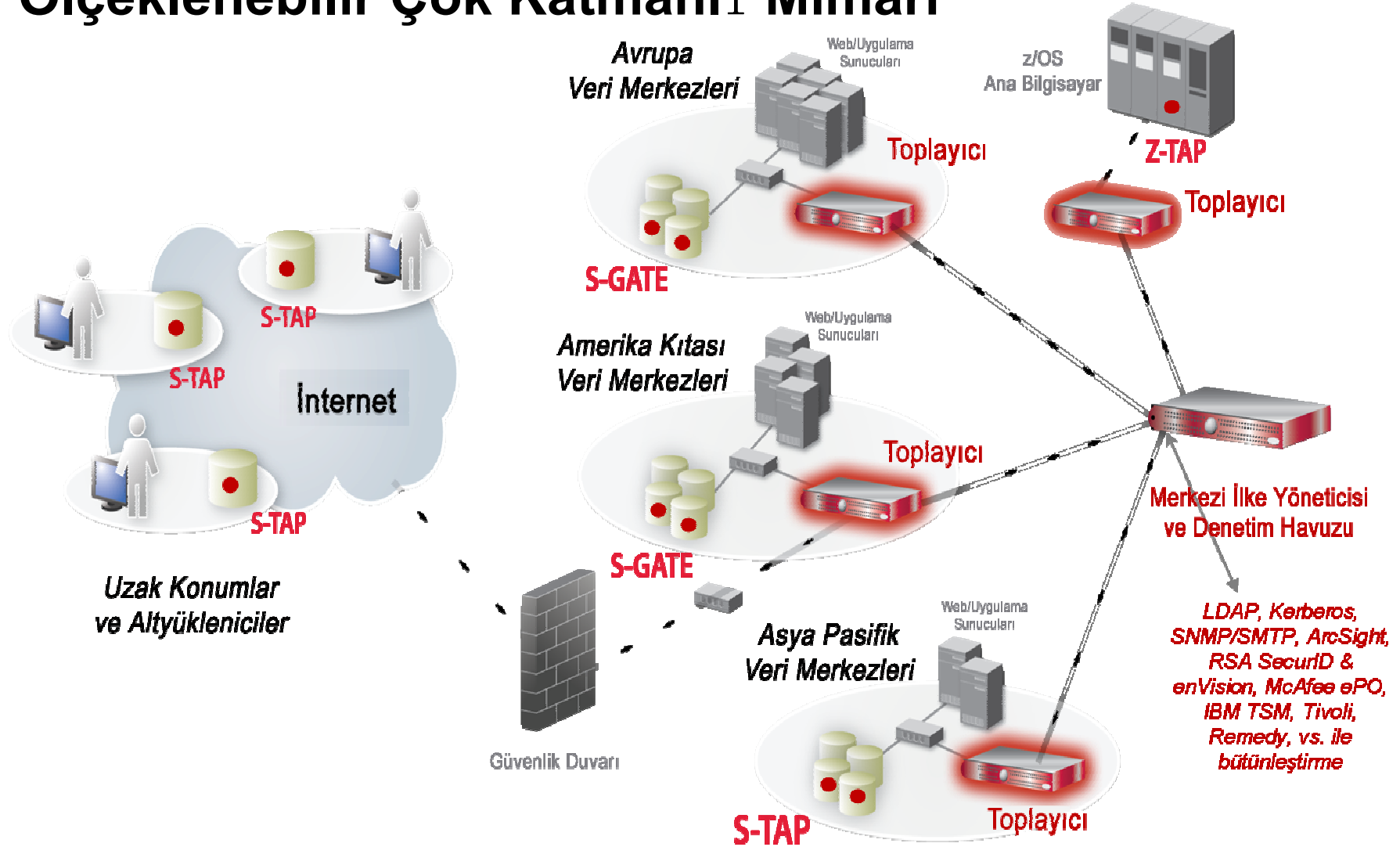
- Oracle E-Business Suite, PeopleSoft, Business Objects Web Intelligence, JD Edwards, SAP, Siebel, şirket içinde oluşturulan özel uygulamalar

Uygulama Kullanıcı Kimliğinin Yakalanmasında Kullanılan Çeşitli Yöntemler

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



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 keşfedilmesi ve sınıflandırılması

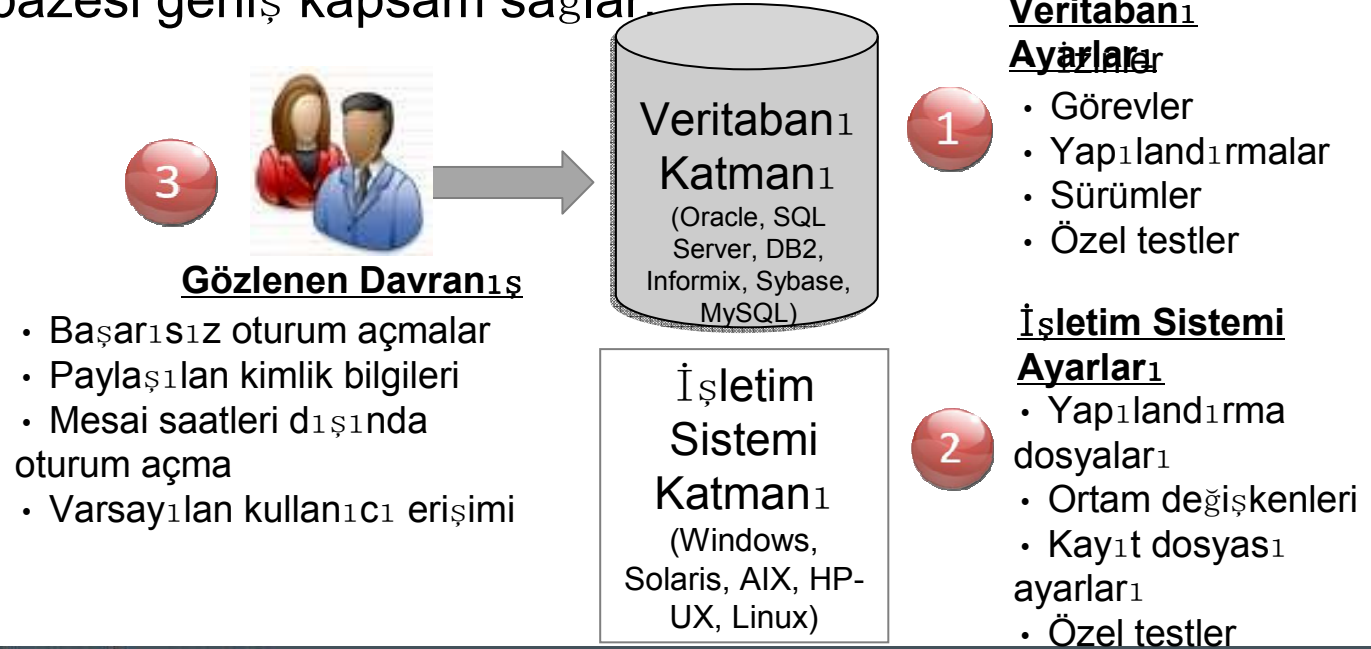
Keşfetme
&
Sınıflandırma

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:



Basitleştirilmiş Güvenlik Açığı Yönetimi

Guardium

Results for Security Assessment: **Comprehensive Oracle Assessment**

Assessment executed: 2009-08-21 12:47:28.0

From: 2009-08-20 12:47:28.0 To: 2009-08-21 12:47:28.0

Client IP or IP subset: Any Server IP or IP subset: Any

Download PDF

Tests passing: **42%**

Based on the tests performed under this assessment, this success of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

View Log
Jump to Database List (R)

Ayrıntılı Puanlama Matrisi

Result Summary Showing 82 of 82 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege 3p	15F	1p	4I	--	1I
Authentication 2p	4I	--	1I	--	1I
Configuration 2p	3I	8p	3I	4p	8I
Version	--	--	2I	--	--
Other	2I	3p	2I	3p	1p

Current filtering applied:
Severities: Show All
Scores: Show All
Types: Show All

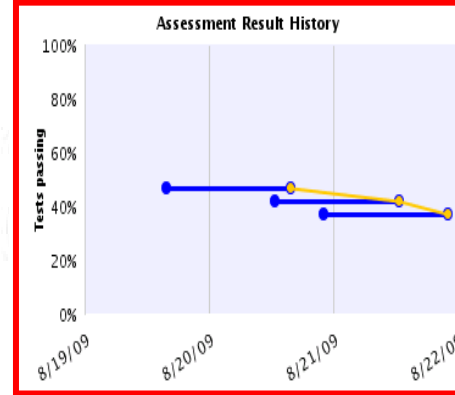
Reset Filtering Filtered/Sort Controls

Assessment Test Results Showing 82 of 82 results (0 filtered)

Cat.	Test Name	Datasource	PF	Sev.	Reason
Other	Excessive Login Failures (Production)	(Observed)	Fail	Critical	Too many login failures, found 18 per day. Recommendation: An alarming number of login failures have been reported from your databases. This might be an indication of an attempt to break into your database, or of someone trying to steal or damage your data. The number of login failures should be close to zero, especially in production environments. You should immediately inspect all attempts to access your database and the source of all the login failures, and take immediate action to deny access to your database from unauthorized clients.
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.99	Fail	Critical	User profile (MONITORING_PROFILE) setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value.

Geçmişe Dönük İlerleme 😊 veya Gerileme ☹️

Toplam Puan



Öncelik belirleme için süzgeç denetimi

Show only: [Reset Filtering](#)

Severities	Scores	Test Types
Critical	Fail	SYBASE
Major	Pass	MS SQL SERVER
Minor	Error	INFORMIX
Cautionary		MYSQL

Sort by:

First	Second	Third
Severity	Score	Datasource

Apply

Basitleştirilmiş Güvenlik Açığı Yönetimi

Guardium

Results for Security Assessment: **Comprehensive Oracle**

Assessment executed: 2009-08-21 13:47:28.0

From: 2009-08-20 12:47:28.0
To: 2009-08-21 12:47:28.0

Tests passing: **42%**

Based on the tests performed under this assessment, this score of 42% is a good starting point. Refer to the recommendations of the individual tests to learn how you should focus upon first. Once you have begun addressing these problems, it is an added task to continuously assess these environments and track improvements.

[View Test](#)
[Jump to Database List \(1\)](#)

Topla Puan

Ayrıntılı Matrisi

Result Summary Showing 82 of 92 results (0 Hidden)

Critical	Major	Minor	Caution	Info
Privilege 3p 15f	1p 4f	1f	1f	1f
Authentication 2p 4f	1f	1f	1f	1f
Configuration 2p 2f	3p 2f	1p 2f	4f	8f 1f
Version	1f	2f	1f	1f
Other	2f	2p 2f	3p	1f 1f 1f 1f 1f

Guardium

Selected Record Differences

Legend
Lines Added
Lines changed
Lines Removed

New Line #1	Previous Line #1
001: [Observed] Access Rule Violations Fail	001: [Observed] Access Rule Violations Fail
002: [Observed] Admin Command Executions Pass	002: [Observed] Admin Command Executions Pass
003: [Observed] After Hours Logins Pass	003: [Observed] After Hours Logins Pass
004: [Observed] Clients Executing Admin Commands Pass	004: [Observed] Clients Executing Admin Commands Pass
005: [Observed] Clients Executing DDL Commands Pass	005: [Observed] Clients Executing DDL Commands Pass
006: [Observed] DBCC Command Executions Pass	006: [Observed] DBCC Command Executions Pass
007: [Observed] DDL Command Executions Pass	007: [Observed] DDL Command Executions Pass
008: [Observed] Excessive Administrator Logins Fail	008: [Observed] Excessive Administrator Logins Fail
009: [Observed] Excessive Login Failures (Production) Fail	009: [Observed] Excessive Login Failures (Production) Pass
010: [Observed] Excessive Login Failures (Test Env.) Pass	010: [Observed] Excessive Login Failures (Test Env.) Pass
011: [Observed] Excessive SQL Errors Pass	011: [Observed] Excessive SQL Errors Fail
012: [Observed] One User One IP Fail	012: [Observed] One User One IP Pass
058: oracle - 9.59 - system Only DBA Access To ROLE_ROLE_PRIVS Fail	058: oracle - 9.59 - system Only DBA Access To ROLE_ROLE_PRIVS Fail
059: oracle - 9.59 - system Only DBA Access To SYS.AUD\$ Fail	059: oracle - 9.59 - system Only DBA Access To SYS.AUD\$ Pass
060: oracle - 9.59 - system Only DBA Access To SYS.SOURCE\$ Pass	060: oracle - 9.59 - system Only DBA Access To SYS.SOURCE\$ Pass
061: oracle - 9.59 - system Only DBA Access To SYS.USER\$ Fail	061: oracle - 9.59 - system Only DBA Access To SYS.USER\$ Pass
062: oracle - 9.59 - system Only DBA Access To SYS.USER_HISTORY\$ Pass	062: oracle - 9.59 - system Only DBA Access To SYS.USER_HISTORY\$ Pass
063: oracle - 9.59 - system Only DBA Access To USER_ROLE_PRIVS Fail	063: oracle - 9.59 - system Only DBA Access To USER_ROLE_PRIVS Fail
064: oracle - 9.59 - system Only DBA Access To USER_TAB_PRIVS Fail	064: oracle - 9.59 - system Only DBA Access To USER_TAB_PRIVS Fail
065: oracle - 9.59 - system Only DBA Access To any V\$ View Fail	065: oracle - 9.59 - system Only DBA Access To any V\$ View Fail
066: oracle - 9.59 - system Only DBA Can BECOME USER Or ALTER USER Pass	066: oracle - 9.59 - system Only DBA Can BECOME USER Or ALTER USER Pass
067: oracle - 9.59 - system Only DBA Standard Roles Authorizations Pass	067: oracle - 9.59 - system Only DBA Standard Roles Authorizations Pass

İyi Değil!

İyi!

Değerlendirmeler arasındaki farkların görüntülenmesi

Yapılması gerekenler

Assessment Test Results

Cat.	Test Name	Database	PP	SEV.
Other	Excessive Login Failures (Production)	(Observed)	Fail	Critical
				Too many login failures, found 15 per day.
				Recommendation: An alarming number of login failures have been observed to break into your database, or if someone trying to steal or deny, especially in production environments. You should investigate the login failures, and take immediate action to deny access to your database from unauthorized clients.
Conf.	DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited	ORACLE: oracle - 9.59	Fail	Critical
				User profile (MONITORING_PROFILE) setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value.

Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

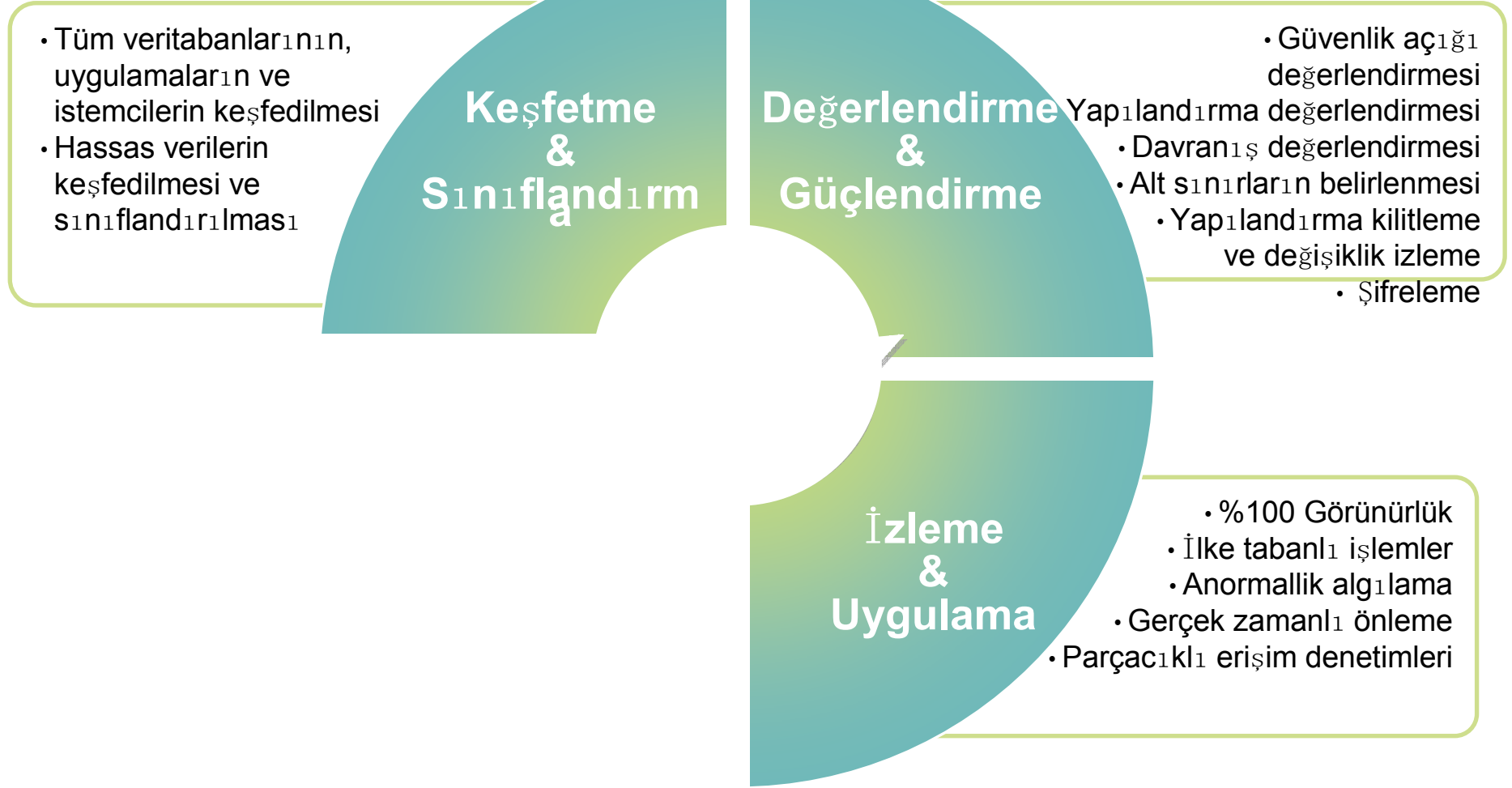
- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilmesi ve sınıflandırılması

Keşfetme
&
Sınıflandırma

Değerlendirme
&
Güçlendirme

- Güvenlik açığı değerlendirmesi
- Yapılandırma değerlendirme
- Davranış değerlendirme
- Alt sınıfların 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



The image shows a screenshot of a Gartner research report. The Gartner logo is in the top left, and the word 'Research' is in the top right. Below the logo, the publication date is '28 April 2010' and the ID number is 'G00200212'. The title of the report is 'Ten Database Activities Enterprises Need to Monitor' by Jeffrey Wheatman. The abstract states that most enterprises are paying too little attention to database security risks. The key findings are listed in a bulleted format.

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.



"Kuruluşların Denetlenmesi Gereken Kritik Önem Taşıyan Etkinlikler"

•Ayrıcalıklı Kullanıcılar

- Kritik verilere Erişim/Değiştirme/Silme
- Uygun olmayan kanallar kullanılarak erişim
- Şema değişiklikleri
- Yetkisiz kullanıcı hesabı ekleme

•Son Kullanıcılar

- Normalde gerekli olmayan aşırı miktarda veriye erişim
- Standart mesai saatleri dışında verilere erişim
- Uygun olmayan kanallar aracılığıyla verilere erişim

•Geliştiriciler, Analistler ve Sistem Yöneticileri

- Etkin üretim sistemlerine erişim

•BT Operasyonları

- Veritabanlarında veya veritabanına erişen uygulamalarda onaylanmamış değişiklikler

Guardium'un iřiniz iin sađladıkları :

1. Veri İhlallerini Öner

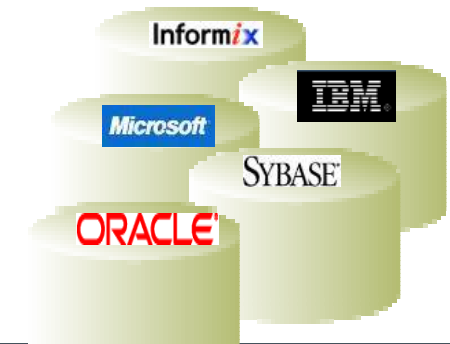
- İ ve dış güvenlik açıklarını azaltır
- Gerek zamanlı ve proaktif denetimler

2. Veri Yönetişimi Sađlar

- Hassas verilerde yetkisiz deđişiklik yapılmasını öner
- Denetçilere uyumluluđu 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

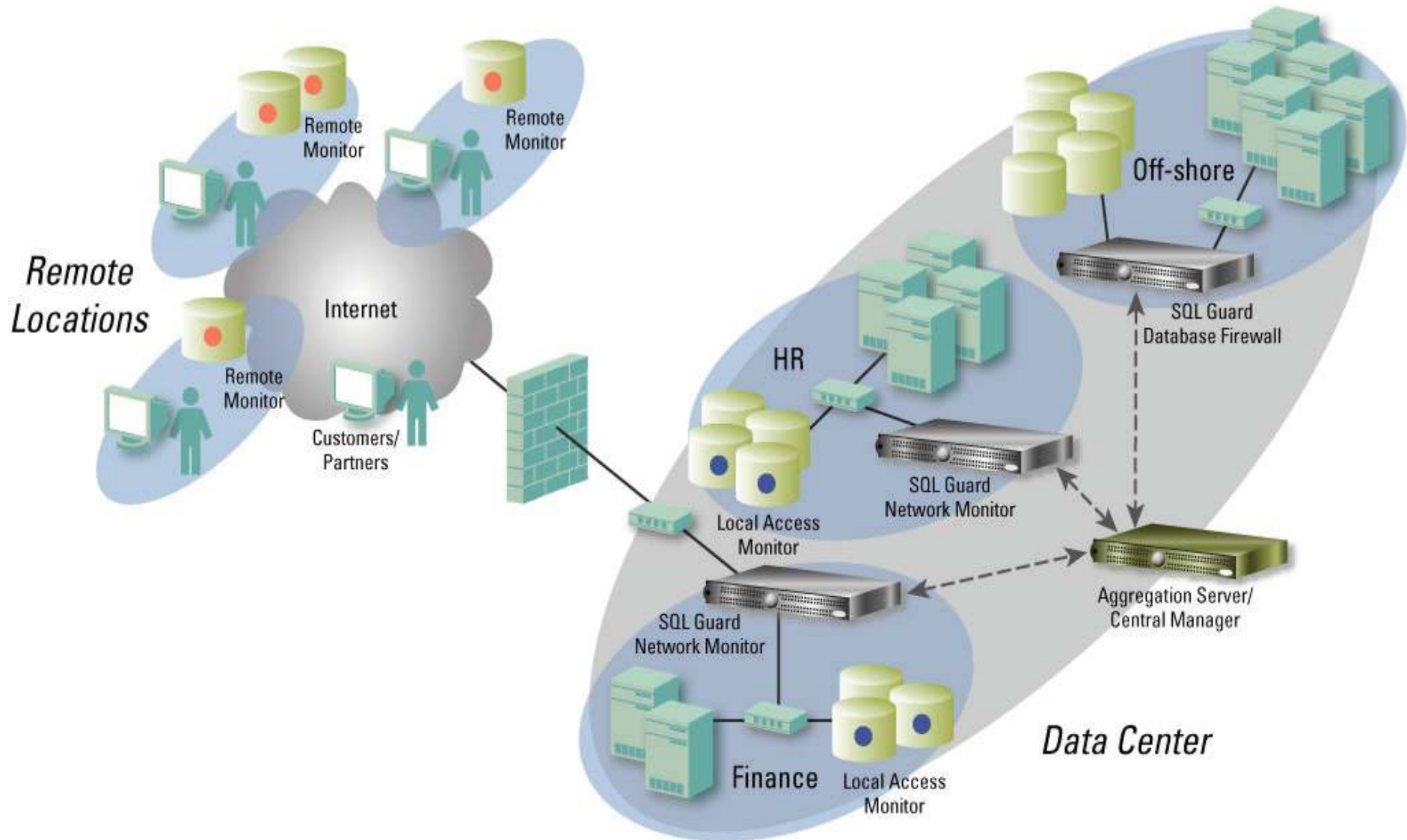
Test Süreci

- 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.

Turkcell Veritabanı İzleme Yapısı



Sonu



- SOX uyumluluęunda veritabanı konusunda özüm üretme
- Veritabanı güvenlięini merkezi yönetme
- Güvenlik riski yüksek seviyeli senaryolar için real-time alarm üretme
- Riskli operasyonel işlemleri periyodik raporlama
- Otomatik çağrı süreci

TESEKKURLER