



# 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](mailto:tansel@tr.ibm.com)

[#connected](https://twitter.com/connected)

# İçindekiler

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



# Guardium kimdir?

- Guardium, 2002 yılından bu yana Veritabanı Etkinliđi 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.



Veritabanları, her kuruluş için hayati önem taşır,  
buna bağılı 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 varsayılmayacağını 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](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)



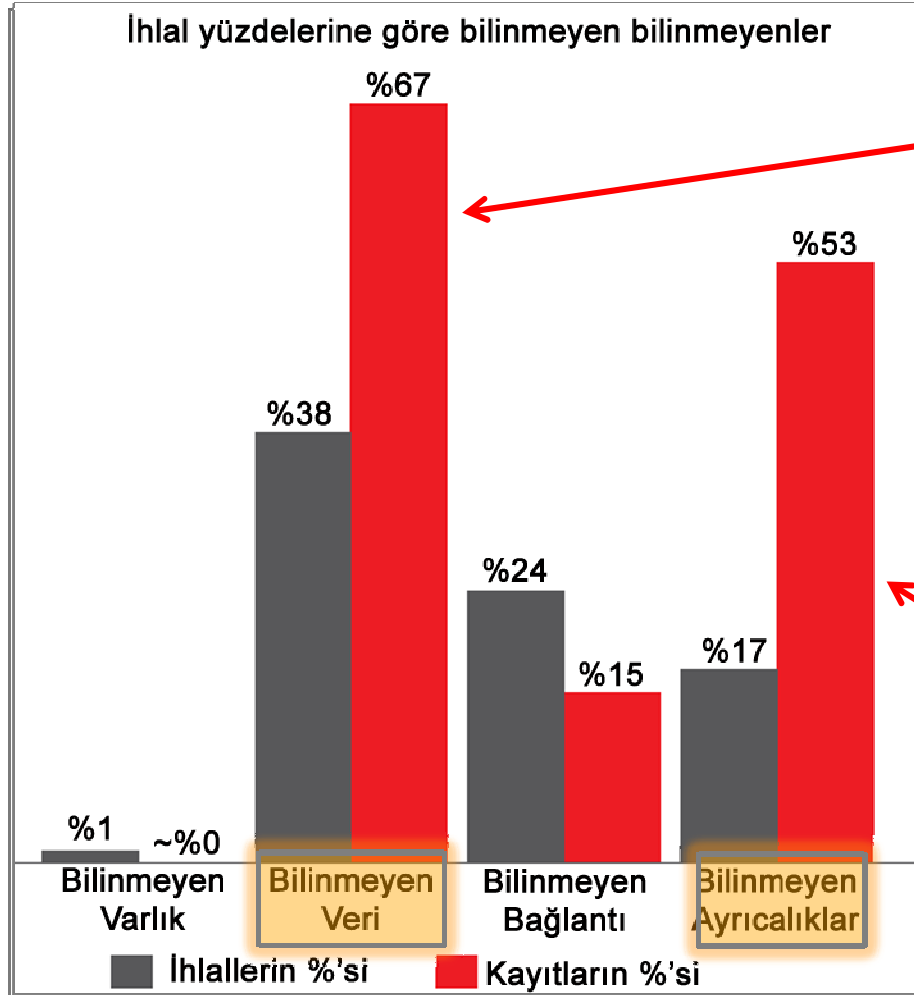
## Verizon RISK Ekibi 2009 Veri İhlali Raporu

Varlık	Varlık Grubu	İhlallerin %'si	Kayıtların %'si
POS sistemi	Çevrimiçi Veri	%32	%6
<b>Veritabanı sunucusu</b>	<b>Çevrimiçi Veri</b>	<b>%30</b>	<b>%75</b>
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](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"

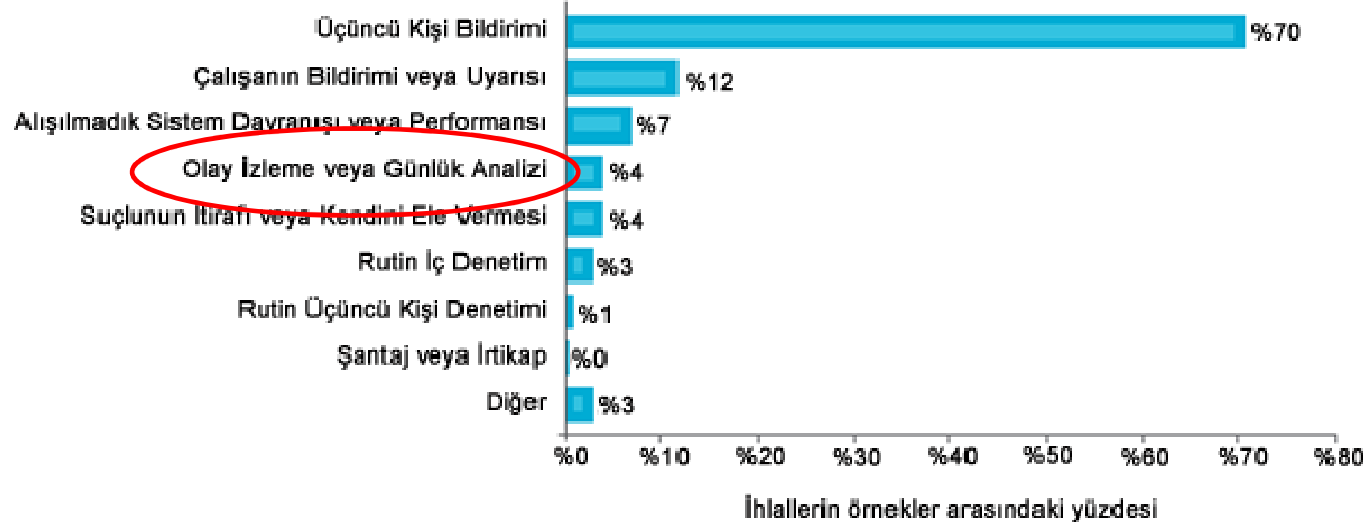
## Bilinmeyen Ayrıcalıklar

"Bu ayrıcalıkların bu şekilde yapılandırıldığını bilmiyorduk"

[http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)

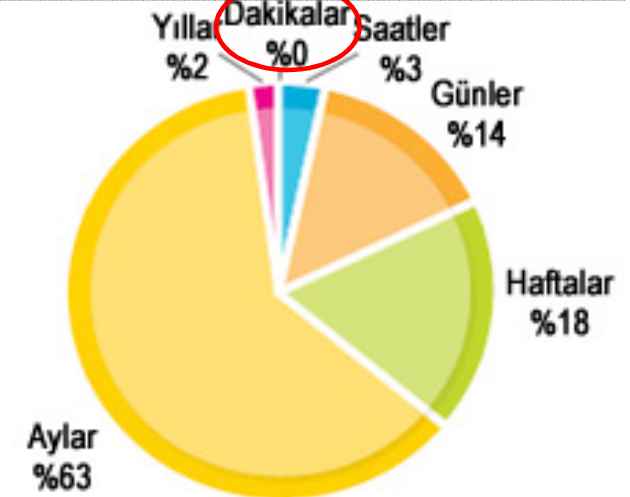


## Veri ihlalleri nasıl belirlenir?



### Veri İhlali Keşif Yöntemleri

### Güvenlik Açısından Keşfe



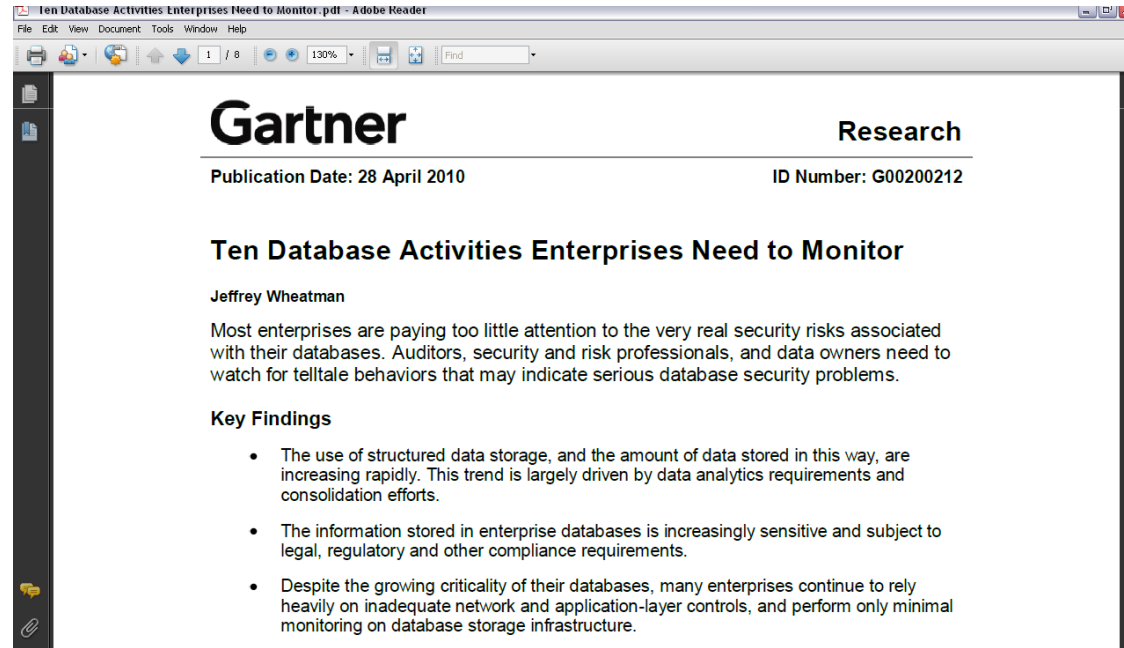


Analistler veritabanı güvenliđi hakkında ne düşünüyor?



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

*- Gartner Research, 28 Nisan 2010*



The screenshot shows a PDF document viewer displaying a Gartner research report. The document is titled "Ten Database Activities Enterprises Need to Monitor" and is authored by Jeffrey Wheatman. The report is dated 28 April 2010 and has an ID number of G00200212. The main text states: "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." The report includes a section titled "Key Findings" with three bullet points: 1. 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. 2. The information stored in enterprise databases is increasingly sensitive and subject to legal, regulatory and other compliance requirements. 3. 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.



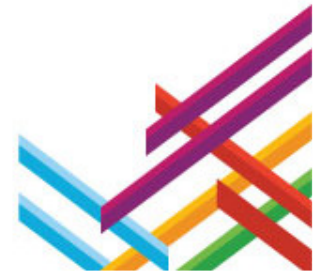
Gartner

## Veritabanı Etkinliđi 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 ađ 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

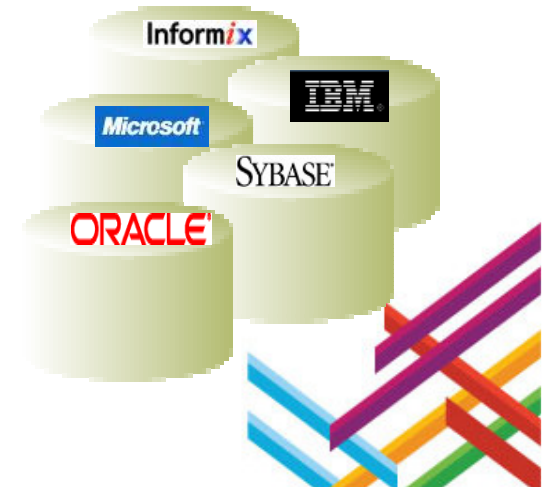
- » Ayrıcalıklı kullanıcıların izlenmesi zordur
- » Uygulamanın "gerçek kullanıcısının" takip edilmesi zordur
- » Denetimin ayrıntı düzeyi yetersizdir

## × Verimsiz ve yüksek maliyetli

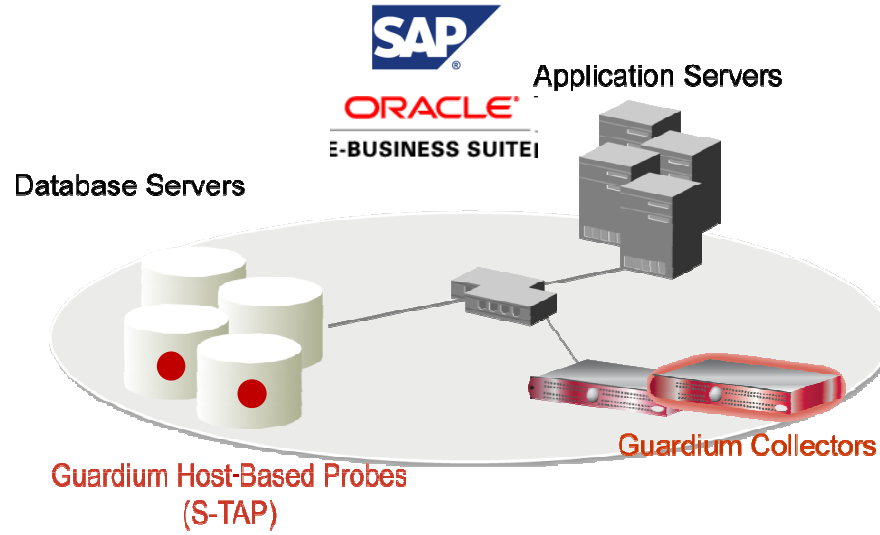
- » Veritabanı performansını etkiler
- » Büyük günlük dosyaları düşük değer sağlar
- » Her veritabanı tipi için farklı yöntemler

## × Görev ayrılığı yoktur

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



# Gerçek Zamanlı Veritabanı Güvenliği ve İzleme



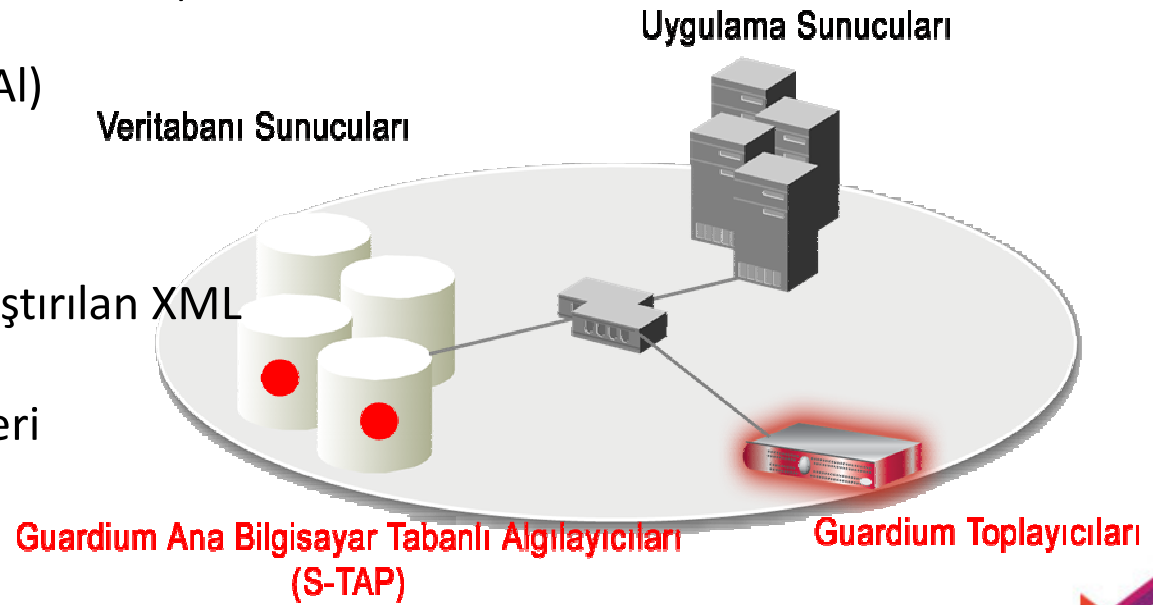
- Yerel veritabanı yöneticisi erişimi dahil %100 görünürlük
- DBMS veya uygulama değişikliği yoktur
- Veritabanı performansı üzerinde en düşük seviyede etki
- Müdahale edilmesi mümkün olmayan denetim havuzu ile görevlerin ayrılmasını sağlar

- 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

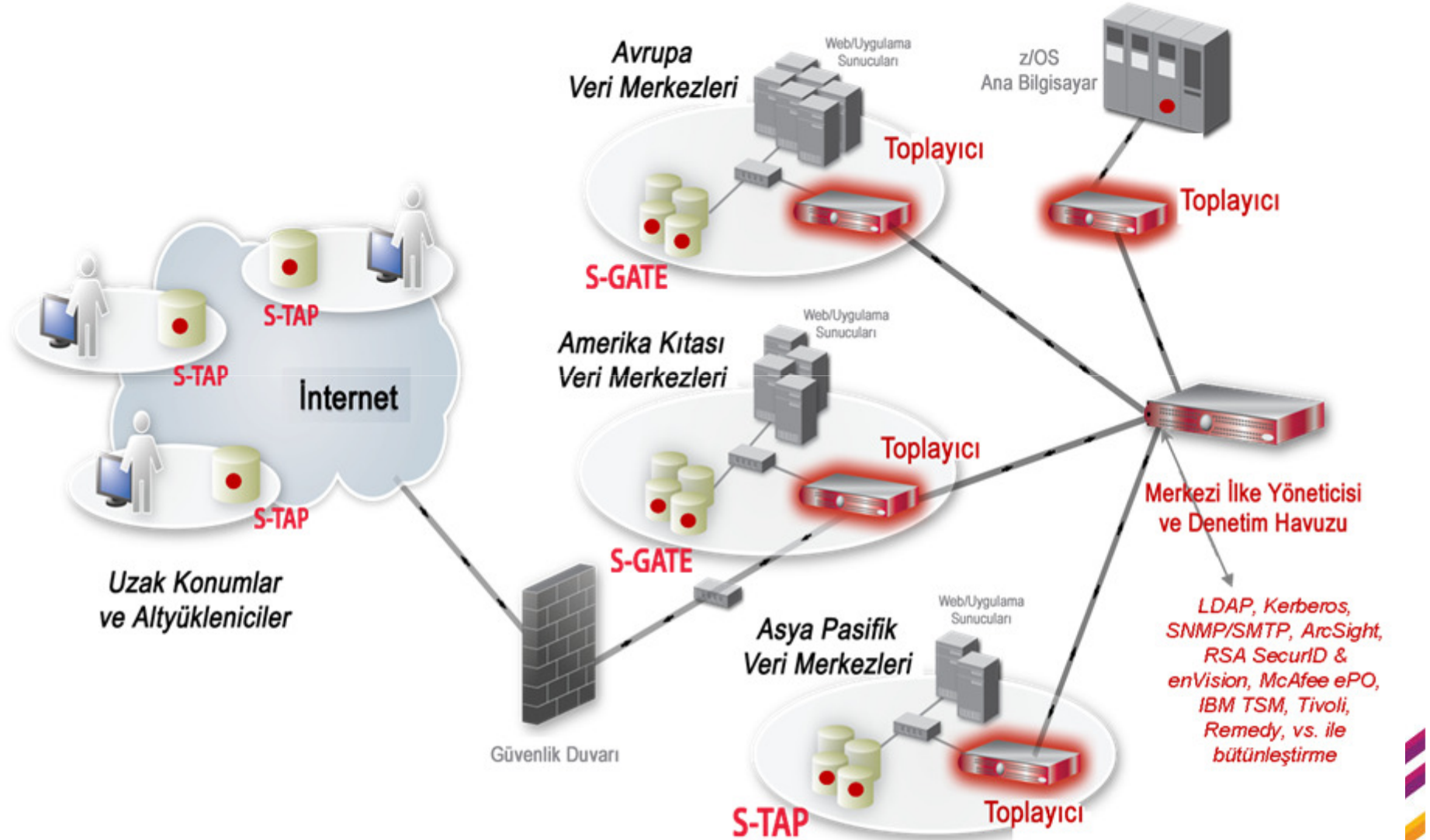


# Guardium neyi izler?

- 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

Keşfetme  
&  
Sınıflandırma



# Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

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

Keşfetme  
&  
Sınıflandırma

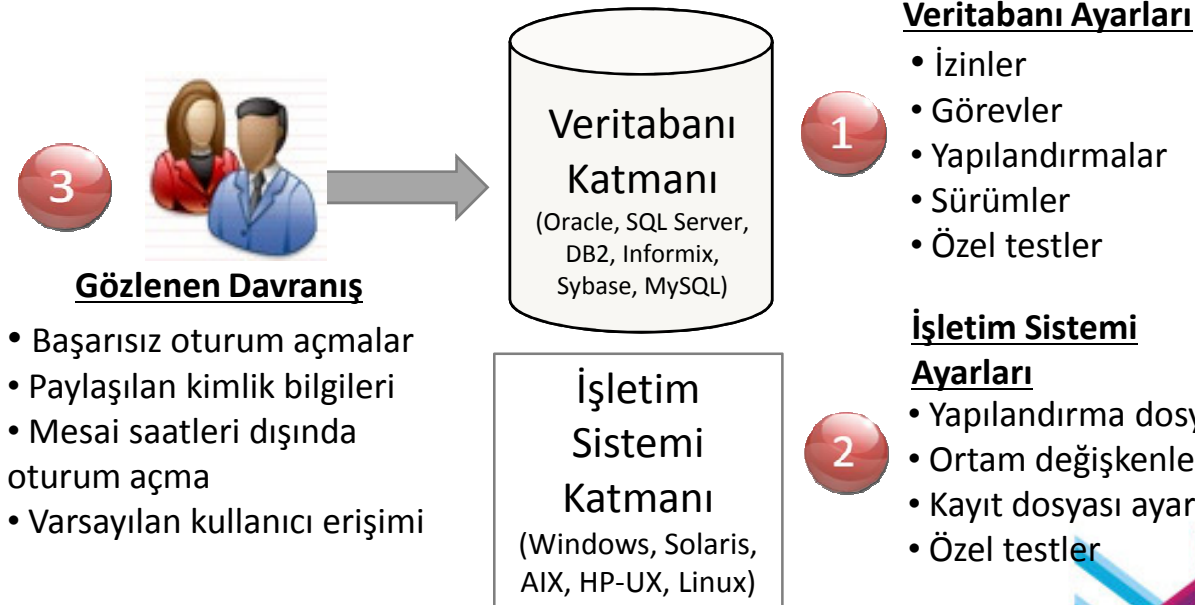
Değerlendirme  
&  
Güçlendirme

- 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

**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 subnet: Any Server IP or IP subnet: Any

Download PDF

Tests passing: **42%**

Based on the tests performed under this assessment, data access 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 Datasource list

**Ayrıntılı Puanlama Matrisi**

**Result Summary** Showing 92 of 92 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	9p 15f	1p 4f	-- 1f	-- --	-- --
Authentication	2p 4f	-- 1f	-- 1f	-- --	-- --
Configuration	2p 2f	-- 8p 3f 4e	1p 3f 4e	-- 6f 1e	-- --
Version	-- --	-- 2f	-- --	-- --	-- --
Other	-- 2f	-- 2p 3f	-- 3p	-- 1e	-- 6p -- 1e

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

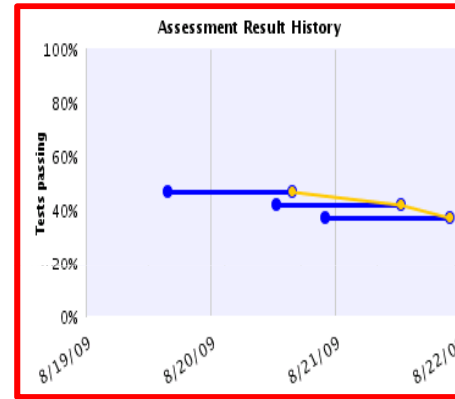
Reset Filtering  Filter / Sort Controls

**Assessment Test Results** Compare with Previous Results Showing 92 of 92 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	<a href="#">Excessive Login Failures (Production)</a>	[Observed]	Fail	Critical	Too Many login failures, found 15 per day.  <i>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.</i>
Conf.	<a href="#">DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited</a>	ORACLE: oracle - 9.59 custom	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

Toplam Puan

Geçmiş Dönük İlerleme 😊 veya Gerileme ☹️



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: Severity  
Second: Score  
Third: Datasource

Apply



# Basitleştirilmiş Güvenlik Açığı Yönetimi

**Guardium**

Results for Security Assessment: **Comprehensive Oracle**

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

Tests passing: **42%**

Based on the tests performed under this assessment, data access of... Refer to the recommendations of the individual tests to learn how you should focus upon first. Once you have begun addressing these problems, you should audit task to continuously assess these environments and track im...

[View log](#)  
[Jump to Datasource list](#)

**Ayrıntılı Puantaj Matrisi**

Result Summary	Showing 92 of 92 results (0 filtered)												
	Critical	Major	Minor	Caution	Info								
Privilege	9p	15f	1p	4f	--	1f	--	--	--	--			
Authentication	2p	4f	--	1f	--	1f	--	--	--	--			
Configuration	2p	2f	--	8p	3f	4e	1p	3f	4e	6f	1e		
Version	--	--	--	2f	--	--	--	--	--	--			
Other	--	2f	--	2p	3f	--	3p	--	1e	--	6p	--	1e

**Guardium**

**Selected Record Differences**

legend  
Lines Added  
Lines changed  
Lines Removed

New			Previous		
Line #1			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\$ Pass	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

Assessment Test Results

[Compare with Previous Results](#)

Cat.	Test Name	Datasource	P/F	Sev.	
Other	<a href="#">Excessive Login Failures (Production)</a>	[Observed]	Fail	Critical	Too Many login failures, found 15 per day.
Conf.	<a href="#">DBA Profile FAILED_LOGIN_ATTEMPTS Are Limited</a>	ORACLE: oracle - 9.59	Fail	Critical	User profile [MONITORING_PROFILE] setup parameter FAILED_LOGIN_ATTEMPTS found out of defined threshold value

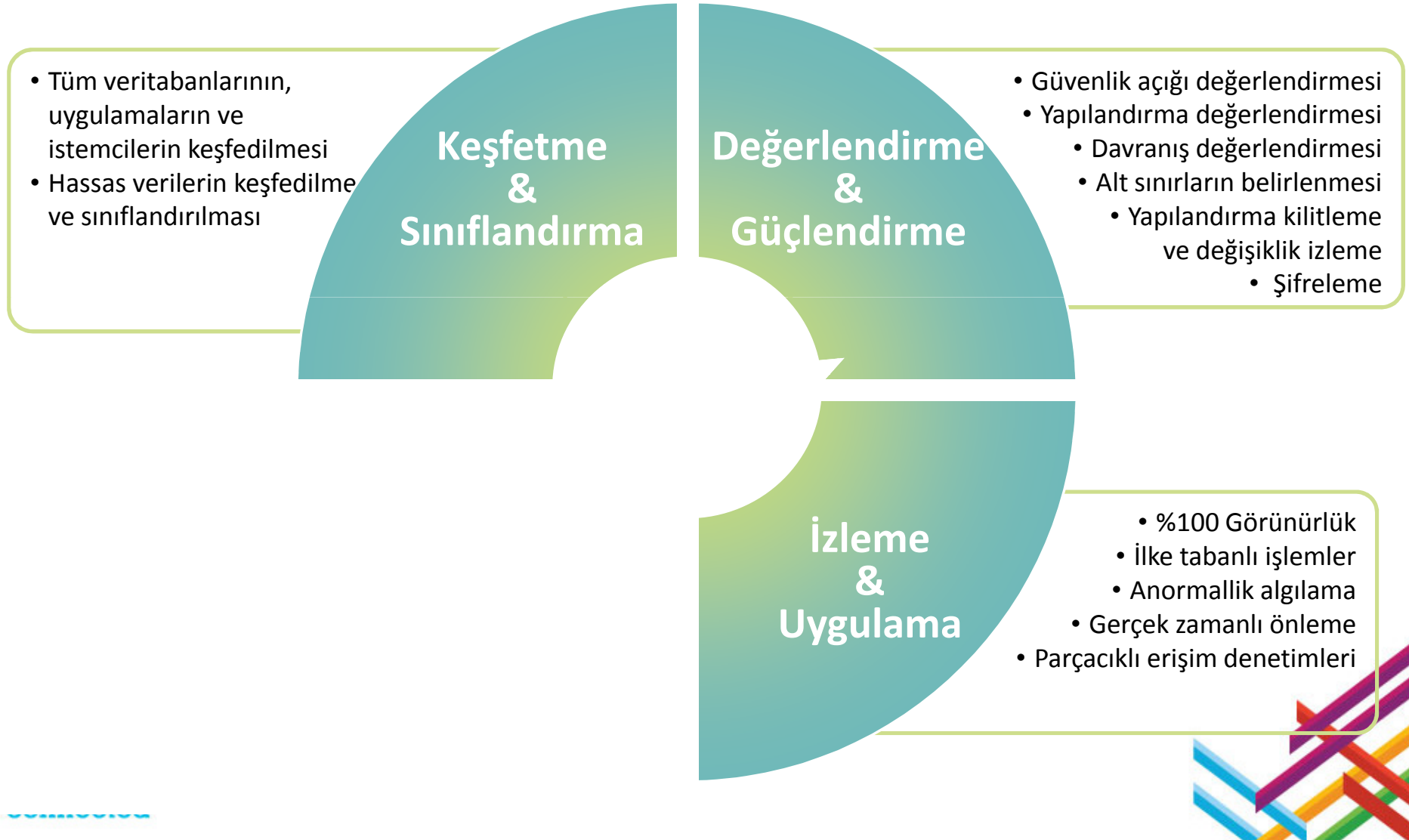
**Değerlendirmeler arasındaki farkların görüntülenmesi**

**Yapılması gerekenler**

# Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

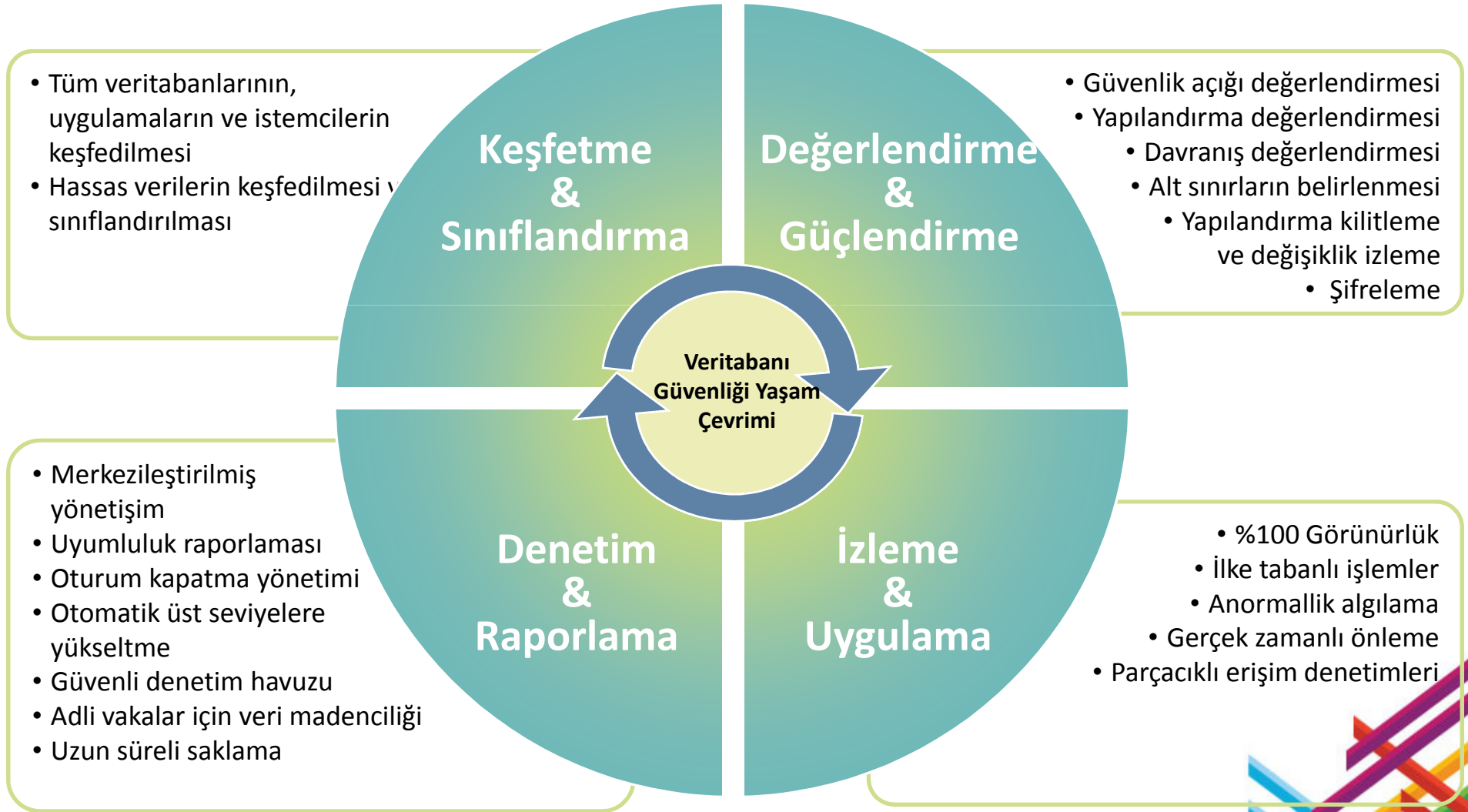


# Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

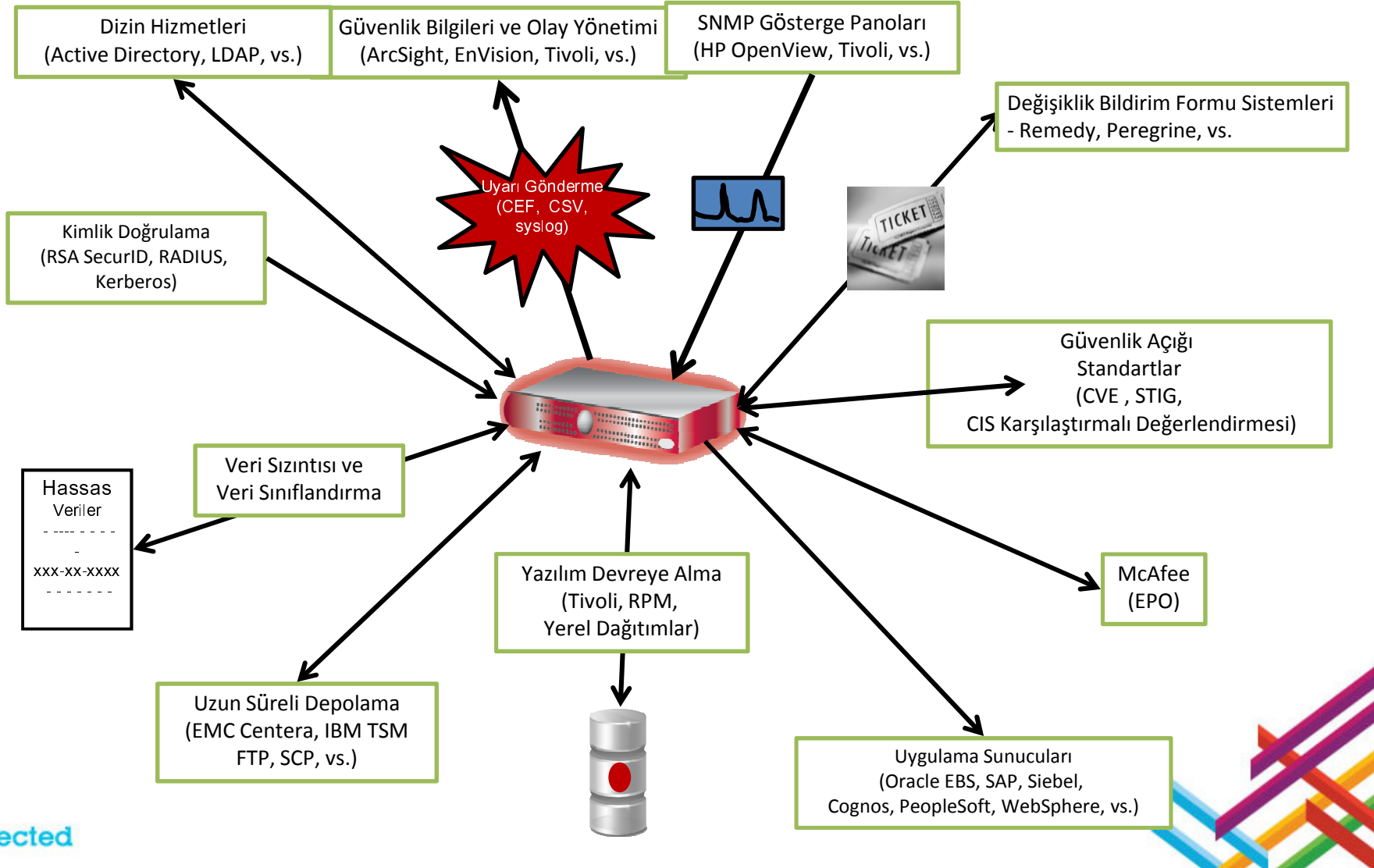




# Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi



# Mevcut Altyapı ile Bütünleştirme Toplam Sahip Olma Maliyetini Düşürür



# Guardium için İş Örneği

## 1. Veri İhlallerini Önler

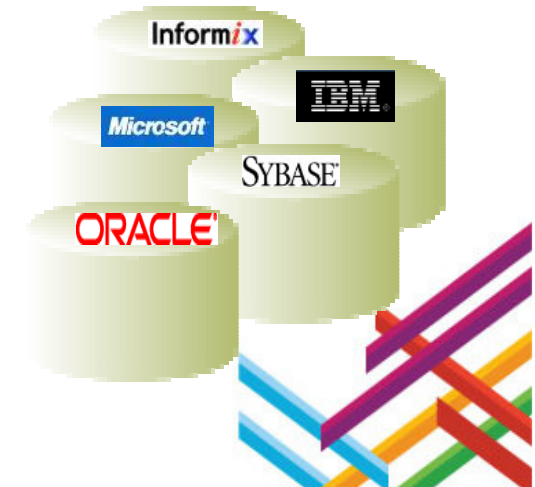
- İç ve dış güvenlik açıklarını azaltır
- Gerçek zamanlı ve proaktif denetimler

## 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

