Information Management

IBM

Data Management

Veritabanı Risk ve Uyumluluk Yönetimi

Tansel ZENGİNLER

IBM InfoSphere Guardium Teknik Satis Uzmani / CEE

Telefon: 0530 317 1675

E-posta: tansel@tr.ibm.com

Guardium®

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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.

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

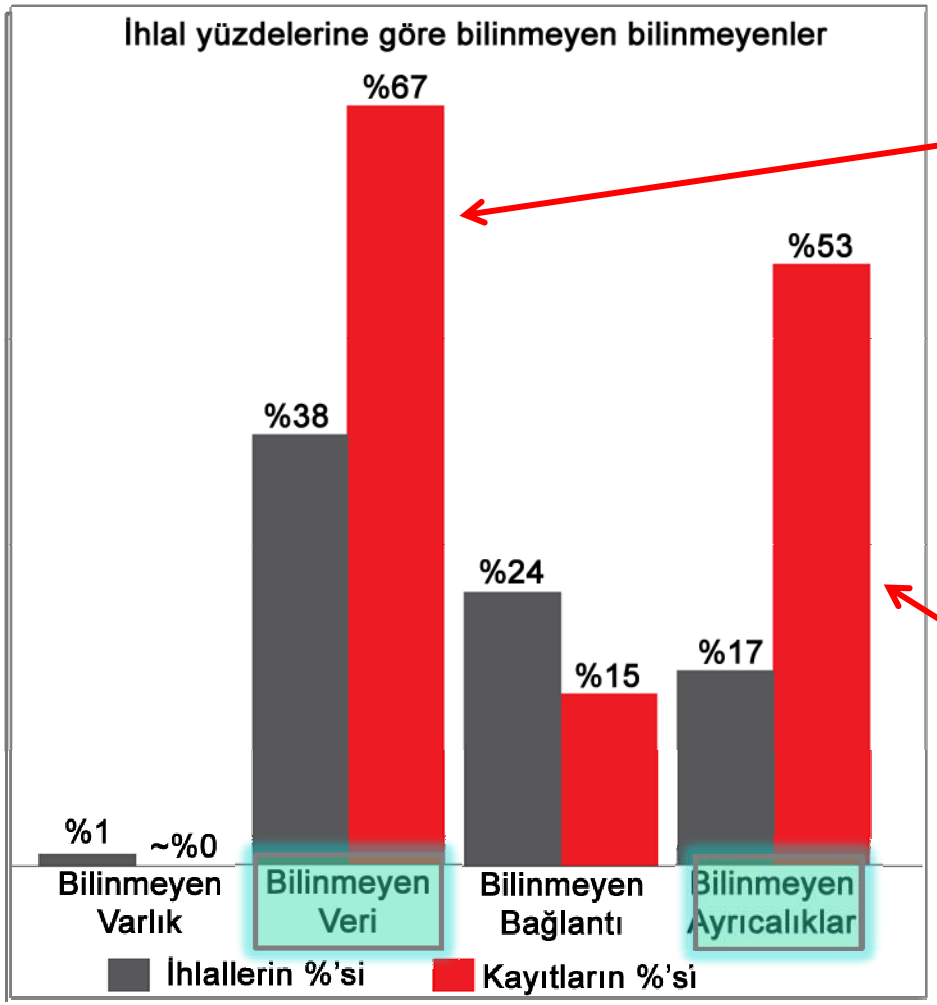
Verizon RISK Ekibi 2009 Veri İhlali Raporu

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

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

"Bilinmeyen Bilinmeyenler" Veri İhlallerinin En Önemli Nedenidir



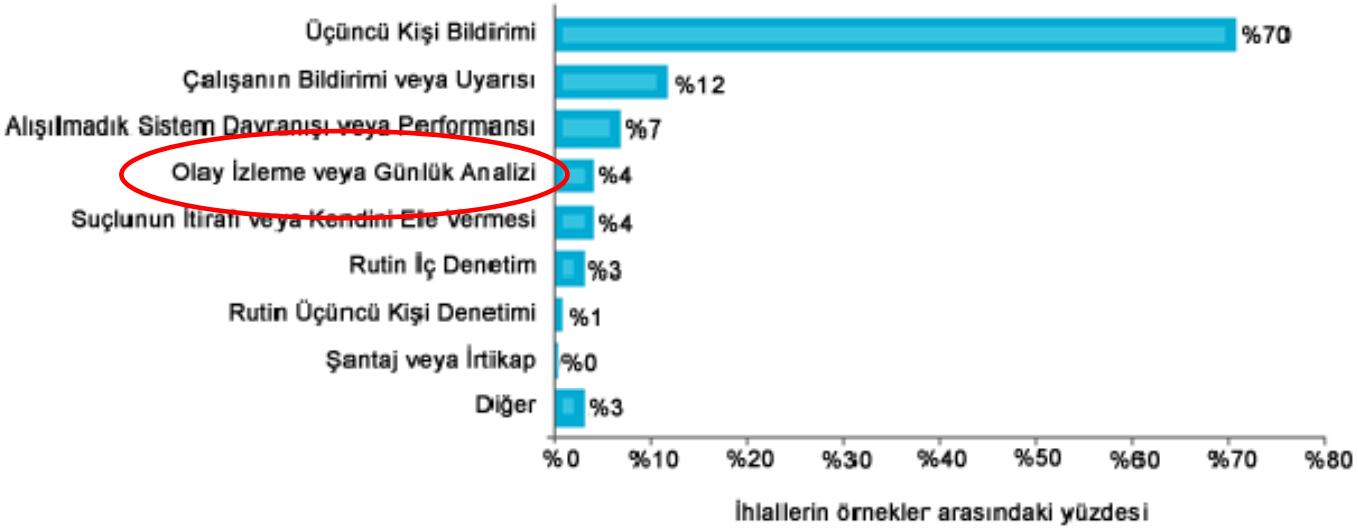
Bilinmeyen Veriler
"Burada hassas verilerin depolandığını bilmiyorduk bile"

Bilinmeyen Ayrıcalıklar
"Bu ayrıcalıkların bu şekilde yapılandırıldığını bilmiyorduk"

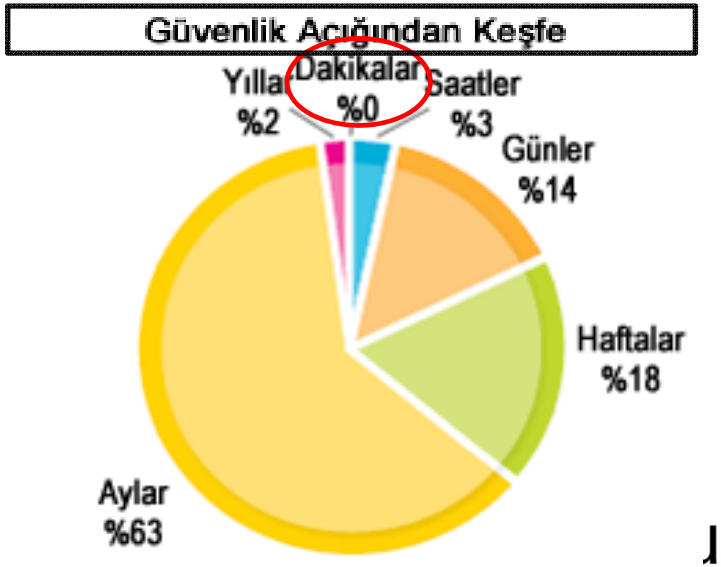
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Veri ihlalleri nasıl belirlenir?



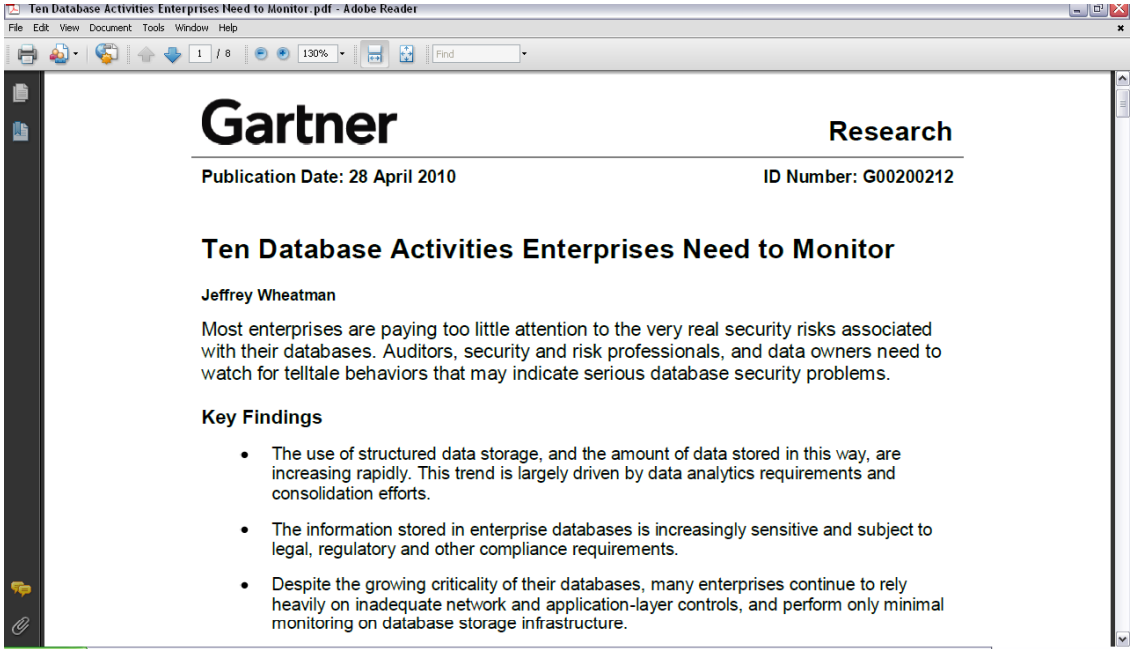
Veri İhlali Keşif Yöntemleri



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


Ten Database Activities Enterprises Need to Monitor.pdf - Adobe Reader

File Edit View Document Tools Window Help

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.

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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"

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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

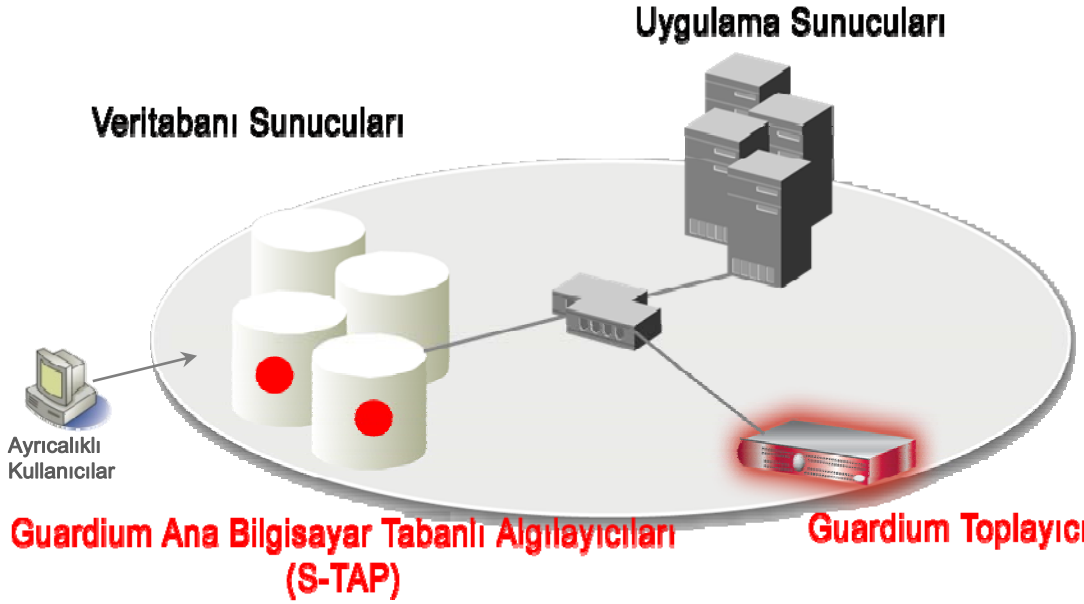
× Verimsiz ve yüksek maliyetli

- 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



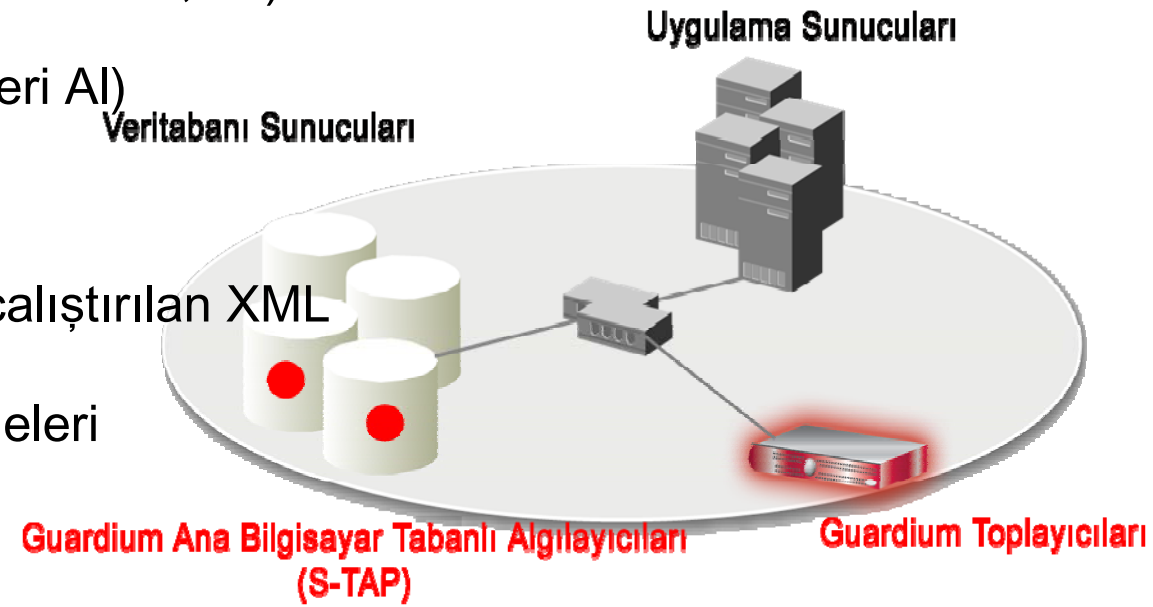
ORACLE
IBM DB2
Microsoft SQL Server
TERADATA
SYBASE
MySQL
Informix

- 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®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium ile Uygulama Kullanıcısı İzleme

Bağlantı Havuzu Oluşturma Uygulamalarındaki Kullanıcıları Tanımlayın

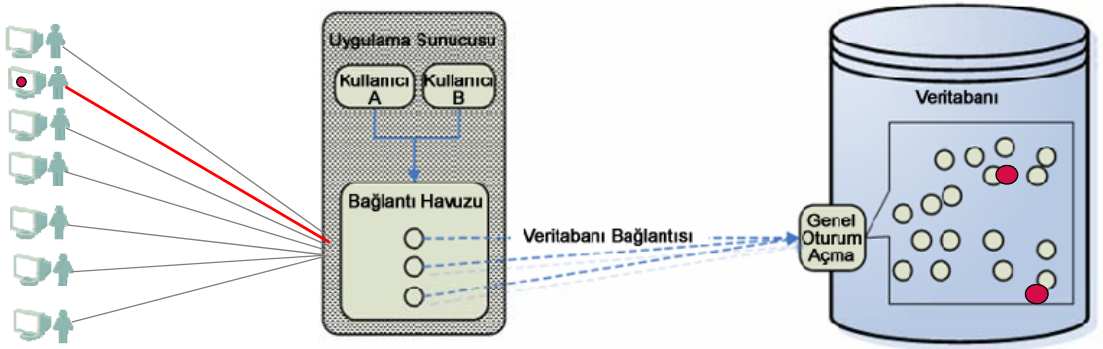
- Potansiyel dolandırıcılığı ortaya çıkarın
- Hassas tablolara kullanıcı erişimi için hatasız denetimler

Desteklenen Kurumsal Uygulamalar

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

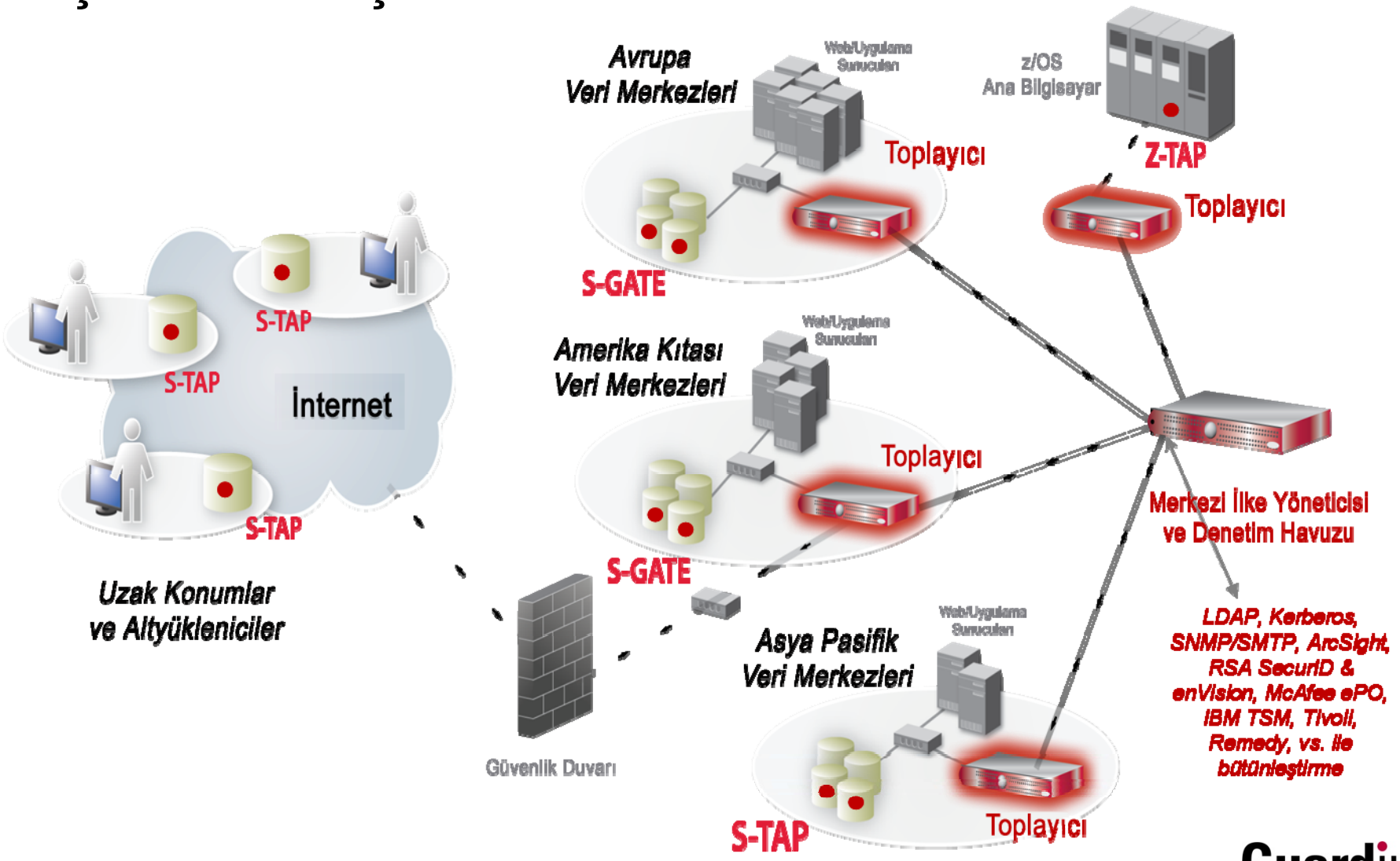
Uygulama Kullanıcı Kimliğinin Yakalanmasında Kullanılan Çeşitli Yöntemler

- 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



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Ölçeklenebilir Çok Katmanlı Mimari



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Kurumsal Ortamlar için Türdeş Olmayan Destek

Desteklenen DBMS Platformları

- Oracle 8i,9i,10g, 11g
- MS SQL Server 2000/05/08
- IBM DB2 UDB 9.1,9.5
- IBM DB2 z/OS 8.1, 9.1
- IBM DB2 UDB for iSeries
- IBM Informix 7, 8, 9, 10,11
- Sun MySQL 4.1,5,5.1
- Sybase ASE, IQ
- Teradata 6.01, 6.02

Desteklenen İşletim Sistemleri

- AIX
- HP-UX
- Red Hat Enterprise
- SUSE Linux
- Solaris SPARC
- Solaris – Intel/AMD
- Tru64
- Windows NT
- Windows 2000/03/08

Desteklenen Uygulamalar

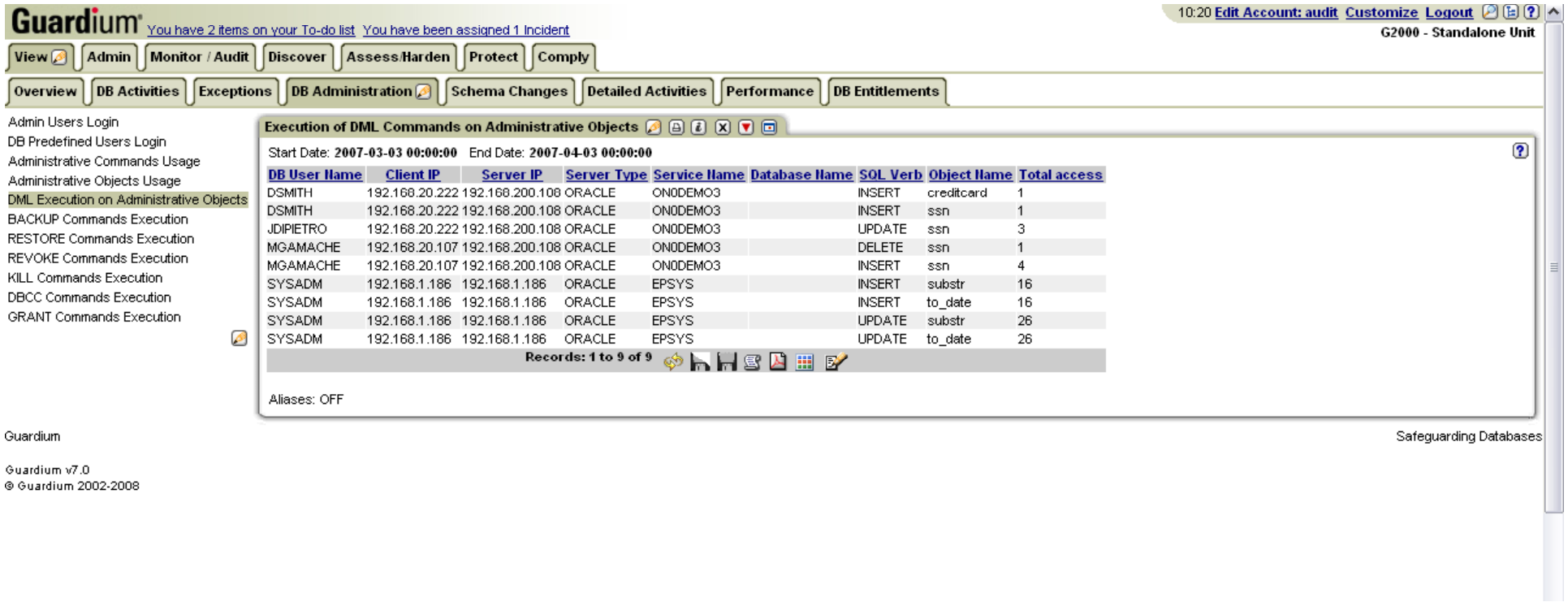
- Oracle E-Business Suite
- PeopleSoft, JDE
- Siebel
- SAP
- Business Objects Web Intel.
- Custom Applications

Desteklenen Uygulama Platformları

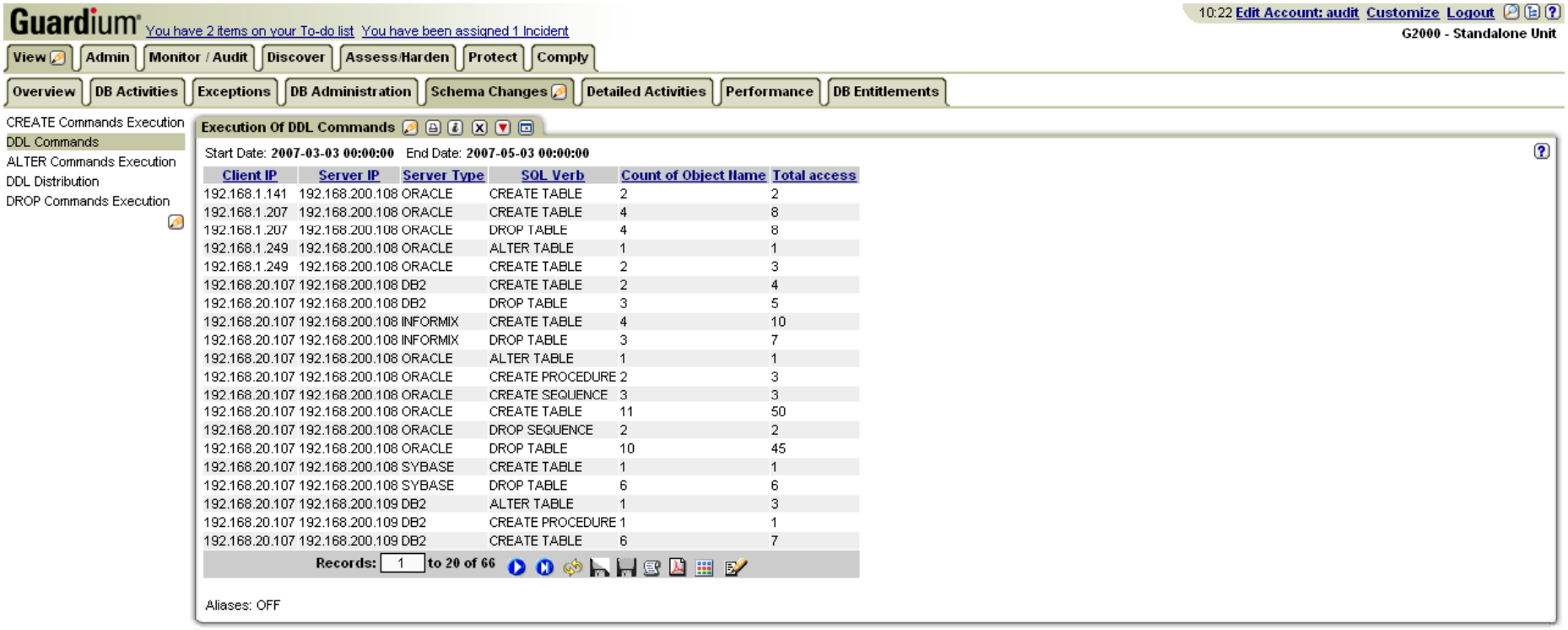
- IBM Websphere
- BEA WebLogic
- Oracle Application Server
- JBoss Enterprise App Platform

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Örnek Rapor - DML Komutları



Örnek Rapor - DDL Komutları



Guardium You have 2 items on your To-do list You have been assigned 1 Incident

10:22 Edit Account: audit Customize Logout

G2000 - Standalone Unit

View | Admin | Monitor / Audit | Discover | Assess/Harden | Protect | Comply

Overview | DB Activities | Exceptions | DB Administration | Schema Changes | Detailed Activities | Performance | DB Entitlements

- CREATE Commands Execution
- DDL Commands
- ALTER Commands Execution
- DDL Distribution
- DROP Commands Execution

Execution Of DDL Commands

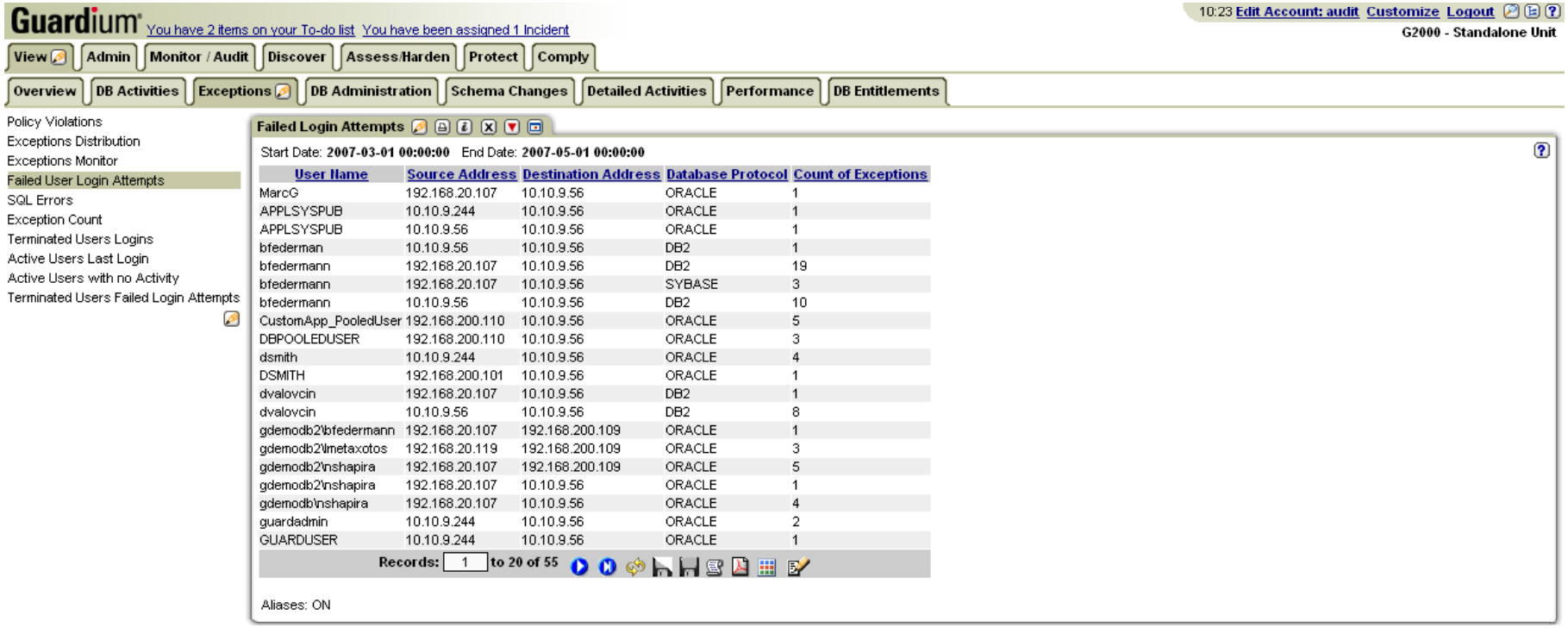
Start Date: 2007-03-03 00:00:00 End Date: 2007-05-03 00:00:00

Client IP	Server IP	Server Type	SQL Verb	Count of Object Name	Total access
192.168.1.141	192.168.200.108	ORACLE	CREATE TABLE	2	2
192.168.1.207	192.168.200.108	ORACLE	CREATE TABLE	4	8
192.168.1.207	192.168.200.108	ORACLE	DROP TABLE	4	8
192.168.1.249	192.168.200.108	ORACLE	ALTER TABLE	1	1
192.168.1.249	192.168.200.108	ORACLE	CREATE TABLE	2	3
192.168.20.107	192.168.200.108	DB2	CREATE TABLE	2	4
192.168.20.107	192.168.200.108	DB2	DROP TABLE	3	5
192.168.20.107	192.168.200.108	INFORMIX	CREATE TABLE	4	10
192.168.20.107	192.168.200.108	INFORMIX	DROP TABLE	3	7
192.168.20.107	192.168.200.108	ORACLE	ALTER TABLE	1	1
192.168.20.107	192.168.200.108	ORACLE	CREATE PROCEDURE	2	3
192.168.20.107	192.168.200.108	ORACLE	CREATE SEQUENCE	3	3
192.168.20.107	192.168.200.108	ORACLE	CREATE TABLE	11	50
192.168.20.107	192.168.200.108	ORACLE	DROP SEQUENCE	2	2
192.168.20.107	192.168.200.108	ORACLE	DROP TABLE	10	45
192.168.20.107	192.168.200.108	SYBASE	CREATE TABLE	1	1
192.168.20.107	192.168.200.108	SYBASE	DROP TABLE	6	6
192.168.20.107	192.168.200.109	DB2	ALTER TABLE	1	3
192.168.20.107	192.168.200.109	DB2	CREATE PROCEDURE	1	1
192.168.20.107	192.168.200.109	DB2	CREATE TABLE	6	7

Records: 1 to 20 of 66

Aliases: OFF

Örnek Rapor - Başarısız Oturum Açmalar



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

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

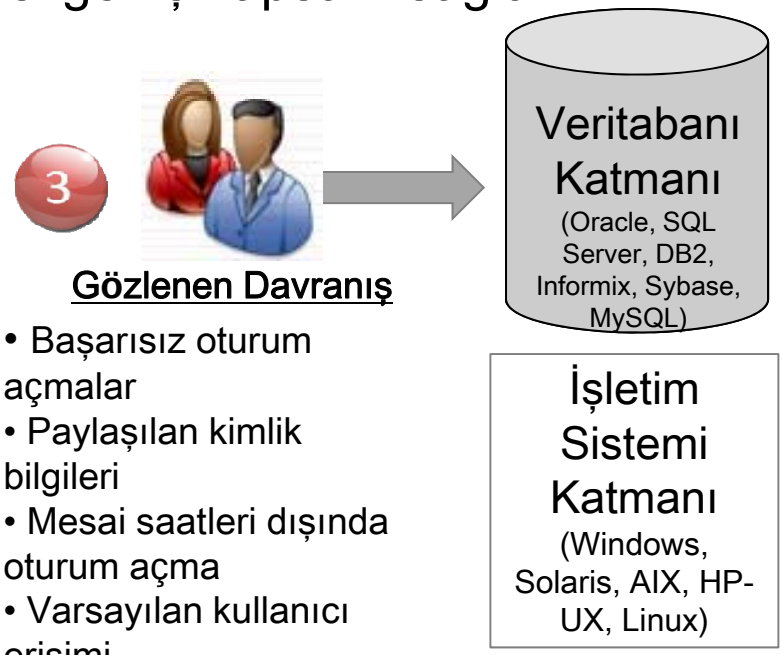
- Tüm veritabanlarının, uygulamaların ve istemcilerin keşfedilmesi
- Hassas verilerin keşfedilmesi ve sınıflandırılması

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

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

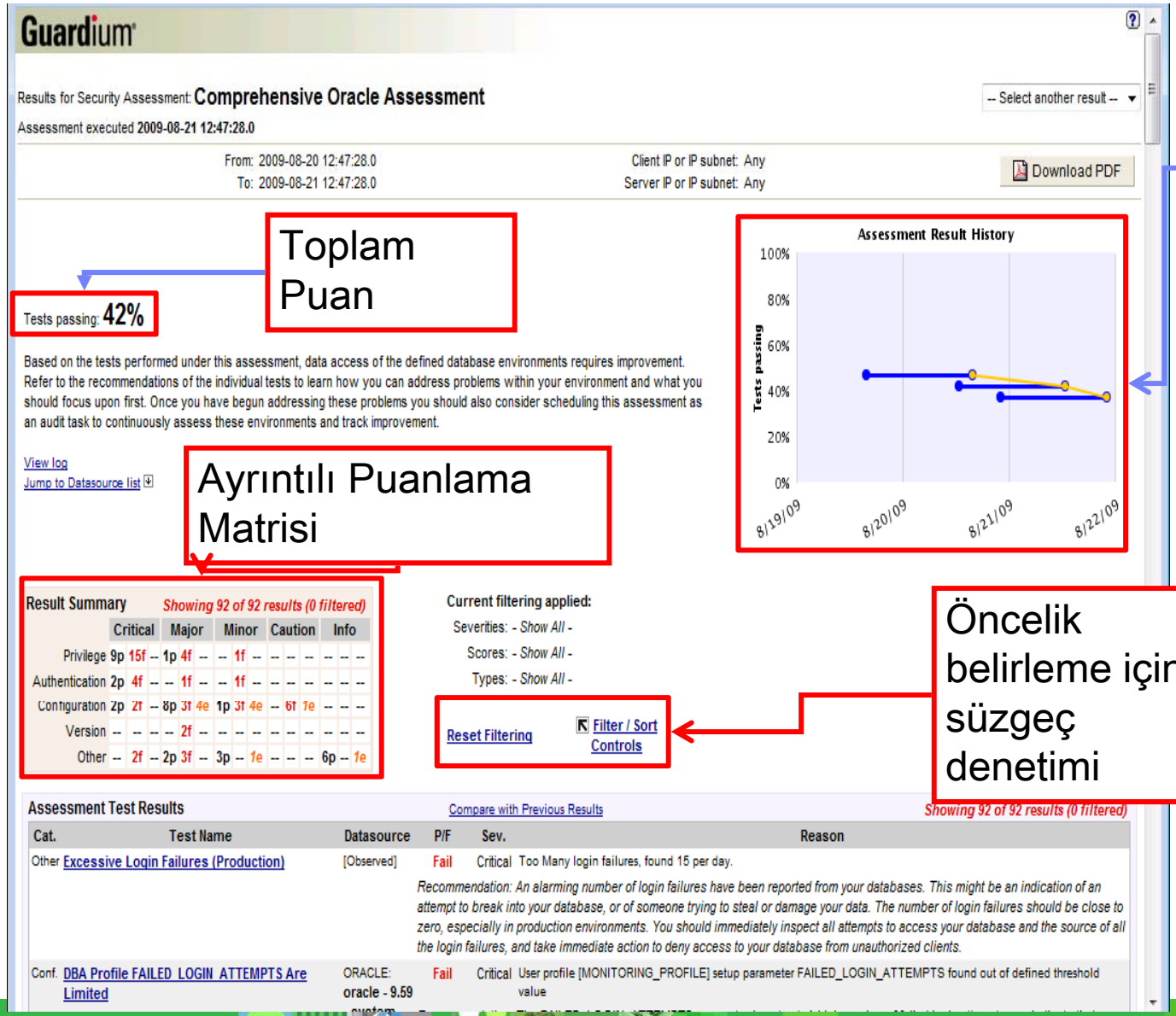
Güvenlik Açığı ve Yapılandırma Değerlendirmesi Mimarisi

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



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Basitleştirilmiş Güvenlik Açığı Yönetimi



Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

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

Topla
Puan

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 prob
an audit task to continuously assess these environments and track im

View log
Jump to Datasource list

Ayrıntılı Pu
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 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_PRI	058: oracle - 9.59 - system	Only DBA Access To ROLE_ROLE_PRIVS Fail
059: oracle - 9.59 - system	Only DBA Access To SYS.AUD$ P	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!

Assessment Test Results Compare with Previous Results

Cat.	Test Name	Datasource	P/F	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 r... attempt to break into your database, or of someone trying to steal or... zero, especially in production environments. You should immediatel... 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

Değerlendirmeler arasındaki farkların görüntülenmesi

Yapılması gerekenler

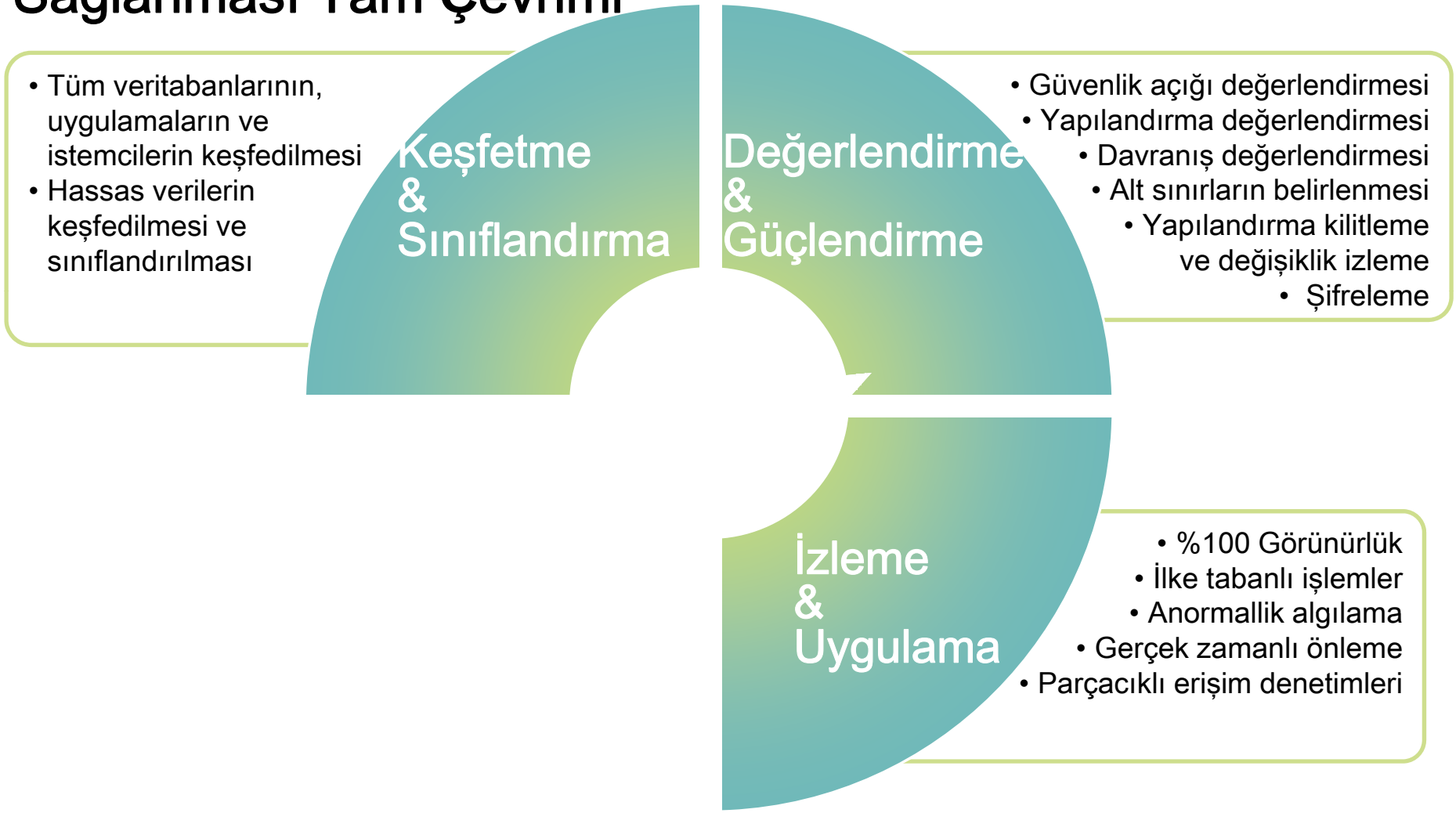
Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

- 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

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

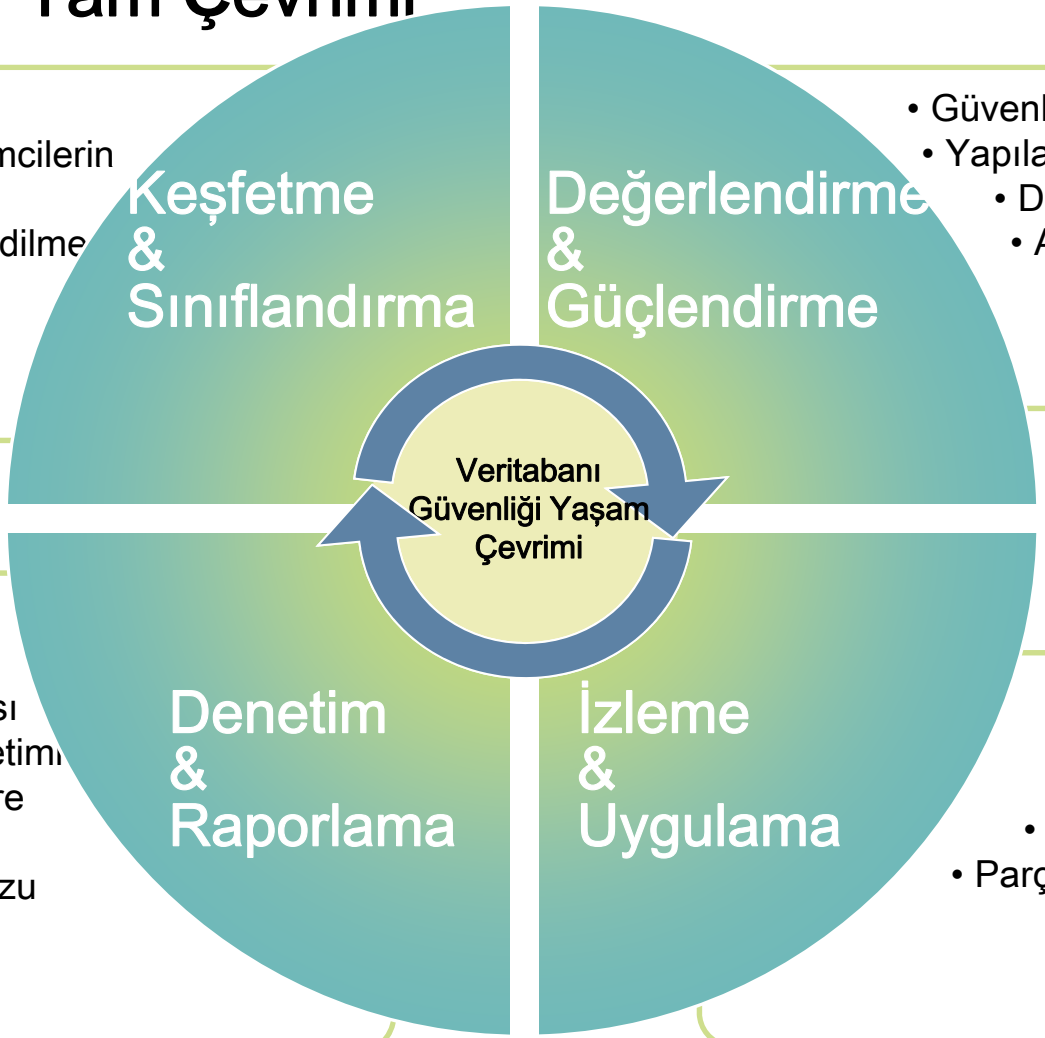
Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Kritik Önem Taşıyan Veri Altyapısının Güvenliğinin Sağlanması Tam Çevrimi

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



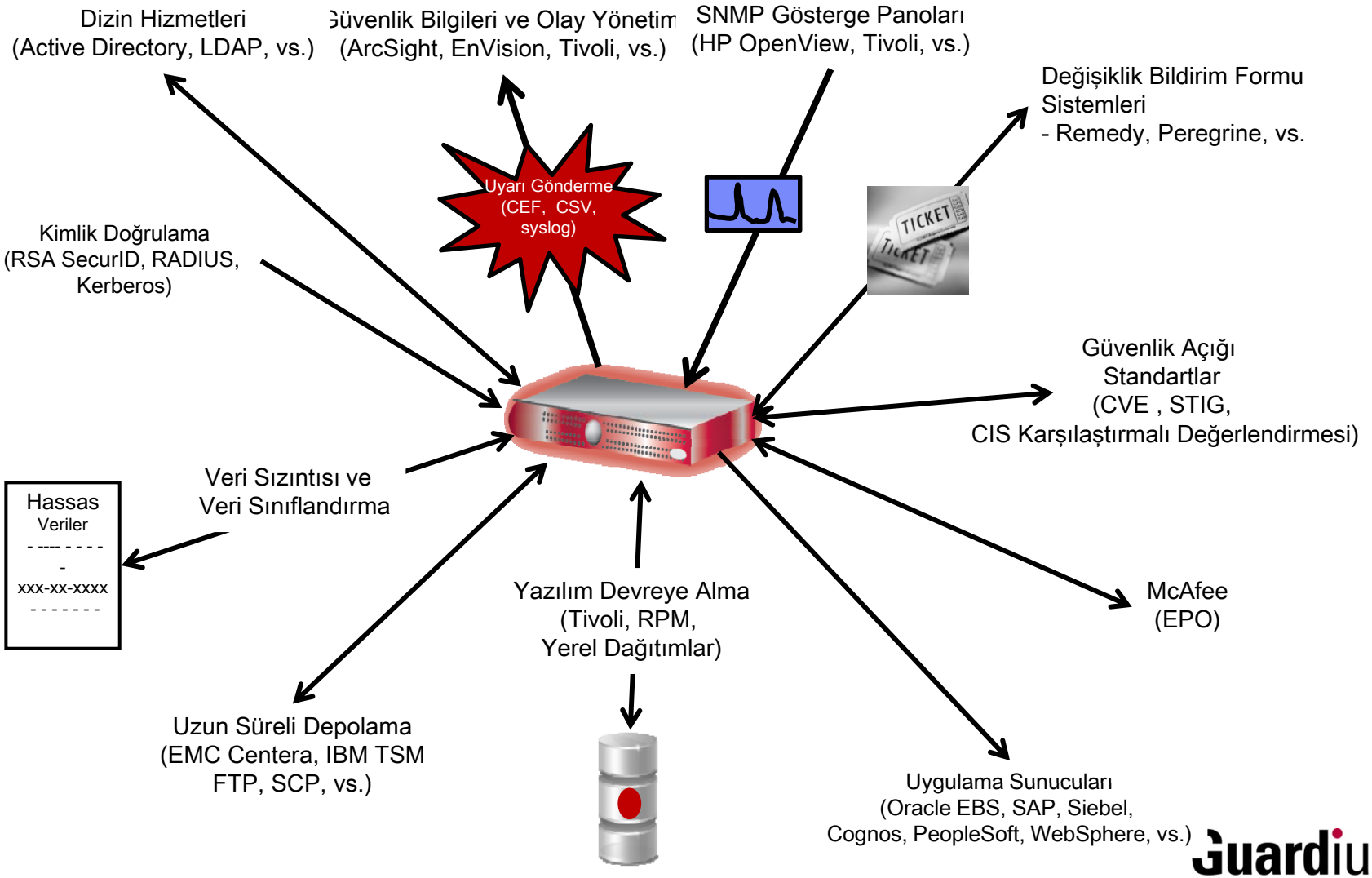
- Güvenlik açığı değerlendirmesi
- Yapılandırma değerlendirmesi
- Davranış değerlendirmesi
- Alt sınırların belirlenmesi
- Yapılandırma kilitleme ve değişiklik izleme
- Şifreleme

- Merkezileştirilmiş yönetişim
- Uyumluluk raporlaması
- Oturum kapatma yönetimi
- Otomatik üst seviyelere yükseltme
- Güvenli denetim havuzu
- Adli vakalar için veri madenciliği
- Uzun süreli saklama

- %100 Görünürlük
- İlke tabanlı işlemler
- Anormallik algılama
- Gerçek zamanlı önleme
- Parçacıklı erişim denetimleri

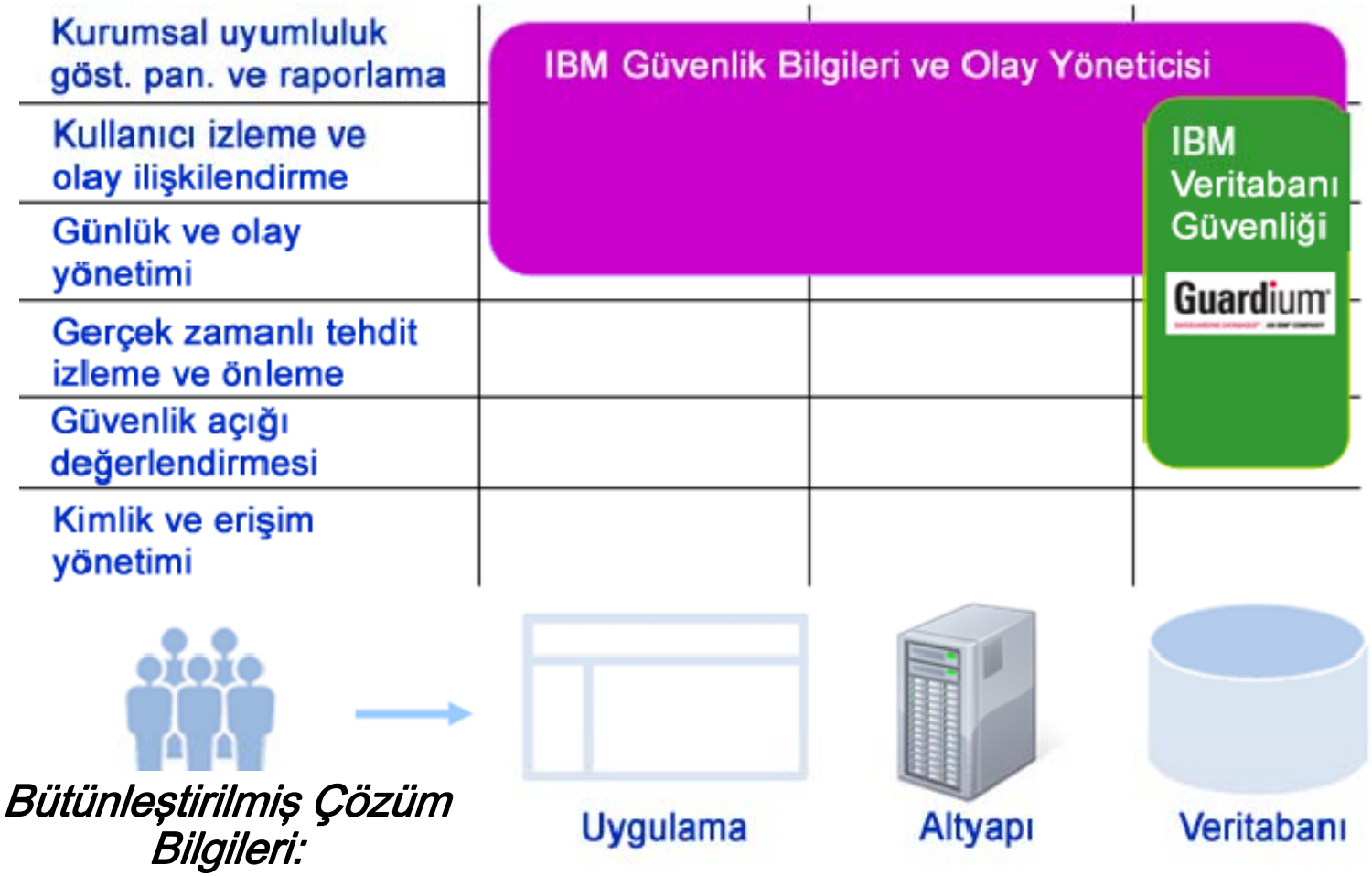
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Mevcut Altyapı ile Bütünleştirme Toplam Sahip Olma Maliyetini Düşürür



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium ve Tivoli

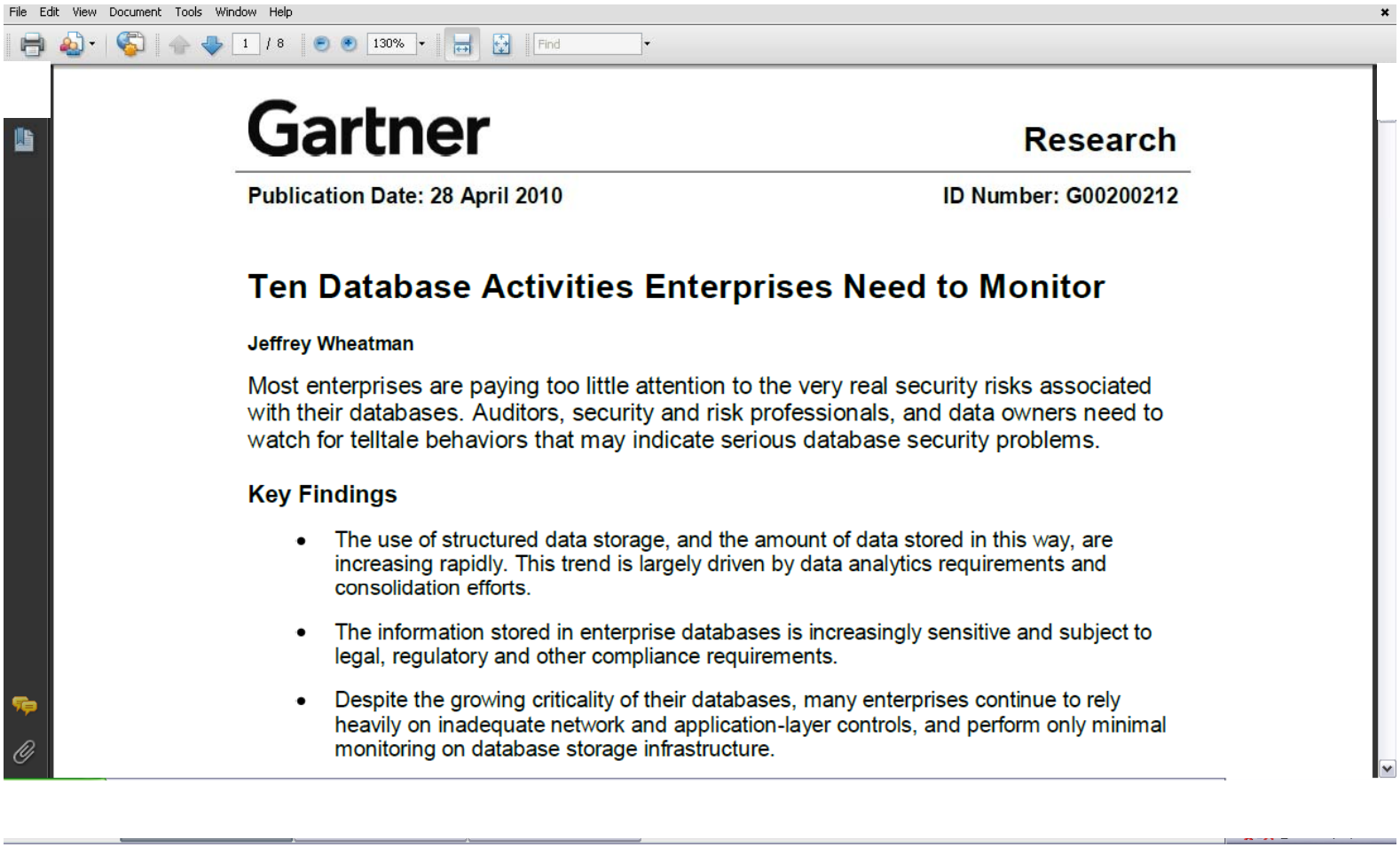


- TSIEM Kurumsal gösterge panosu ve uyumluluk raporları, Guardium olaylarını tam destekler

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium kullanmaya başlamak için

Nereden Başlanır



File Edit View Document Tools Window Help

1 / 8 130% Find

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.

Guardium® SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Gartner

"Kuruluşların Denetlemesi Gereken Kritik Önem Taşıyan Etkinlikler"

- Ayrıcalıklı Kullanıcılar
  - Kritik verilere Erişim/Değiştirme
  - 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®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

İlk DSM İlkesi Örneği

Örnek İlke

İlke	Ayrıntılar	Eylem
Yüksek ayrıcalıklı hesapların tüm oturum açma/kapatma olayları	Tüm üretim veritabanları için ayrıntılı bilgiler toplanır, ancak düşük riskli veritabanlarının raporları düzenli olarak incelenmez, ancak adli araştırmalar için gerekli olabilir	Eşik uyarıları
Sistem hesapları (uygulamalar için) sabit bir IP'den oluşturulmuş olmalıdır	Veritabanı Yöneticilerinin bu ayrıcalıklı hesapları uygulama sunucuları dışındaki IP adreslerinden kullanması durumunda, inceleme için bir özel durum raporu oluşturulacaktır.	Etkinlik uyarıları
Herhangi bir kullanıcının başarısız oturum açma girişimleri	Başarısız oturum açma girişimleri takip edilir ve herhangi bir kimliğin 3 dakika içinde 10 defadan fazla kullanılması durumunda bir ilke ihlali gerçekleşir.	Özet rapor günlük olarak güvenlik personeline gönderilir
Yüksek ayrıcalıklı hesapların DDL etkinlikleri.	Bu kategoriye yönetici olmayan personelin gerçekleştirdiği DDL komutlarının denetlenmesi dahildir.	Özet rapor günlük olarak uygulama/veri sahiplerine gönderilir
Veritabanı hataları ve yetkisiz erişim	Eksik tablolar, yapılandırma hataları, yetkisiz erişim, vs. Aşağıdakilerin rapor edilmesi gerekmektedir: kullanıcı adı, kaynak program, istemci IP/ana bilgisayar, tarih/saat ve veritabanı hatası iletisi ile veritabanı hata kodu.	Belirli kategorilerin özet raporu, çözüm için veritabanı veya güvenlik grubuna gönderilir
Tüm DCL, VERİLENLER ve GERİ ALINANLAR dahil olmak üzere ayrıcalıklarda, kullanıcı oturum açma tanımında değişiklikler	Kullanıcıların, oturum açma bilgilerinin ve görevlerin eklenmesi/silinmesi, kullanıcılar/görevler arasındaki eşlemin değiştirilmesi, parola değişiklikleri, nesnelerin güvenlik niteliklerinde değişiklikler.	Özet rapor günlük olarak uygun güvenlik personeline gönderilir
Hassas olarak sınıflandırılan verilerin DML'si	Herhangi bir DML etkinliğinin veya hassas verilere doğrudan erişimin (kullanıcı arabirimi kullanılmadan) aşağıdakileri içerip içermediği rapor edilmelidir: kullanıcı adı, istemci IP'si, kör değerler, kaynak program, oturum bilgileri, DML bildirimi ve tarih/saat.	Özet rapor günlük olarak uygulama sahipleri ile veri sahiplerine gönderilir
Denetim değişiklikleri/veritabanı bağlantılarının oluşturulması veya eşleme	Bağlantılarda veya eşlemelerde yapılan tüm değişikliklerin izlenmesi	Etkinlik uyarıları
Ayrıcalıklı bir hesabı kendi hesaplarıymış gibi kullanan bireysel kullanıcıların rapor edilmesi.	Ayrıcalıklı hesapları kullanan bireylerin izlenmesi	Etkinlik uyarıları
Üretim veritabanlarının uyumluluk durumunun rapor edilmesi	Eksik yamalar, zayıf parolalar, yatalı yapılandırılmış ayrıcalıklar, varsayılan satıcı firma hesapları ve diğer güvenlik yönergeleri için kritik önem taşıyan veritabanı sistemlerinin düzenli olarak taranması.	Özet rapor haftalık olarak uygun veritabanı ve güvenlik personeline gönderilir

Özet

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

Özet

- Veri gizliliğine ilişkin riskler daha önce hiç bu kadar fazla olmamıştır
- Veritabanı erişiminin küçük parçacıklar halinde izlenmesi, verilerin açığa çıkmasının önlenmesinin en iyi yoludur
- Veritabanı altyapısı çapında birleşik ve tutarlı bir yaklaşım, zamandan ve paradan tasarruf sağlarken güvenliği de artırır
- Guardium, kapsamlı işlevselliği ve uygulama kolaylığı aracılığıyla pazar liderliğini sürdürmektedir

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Teşekkürler