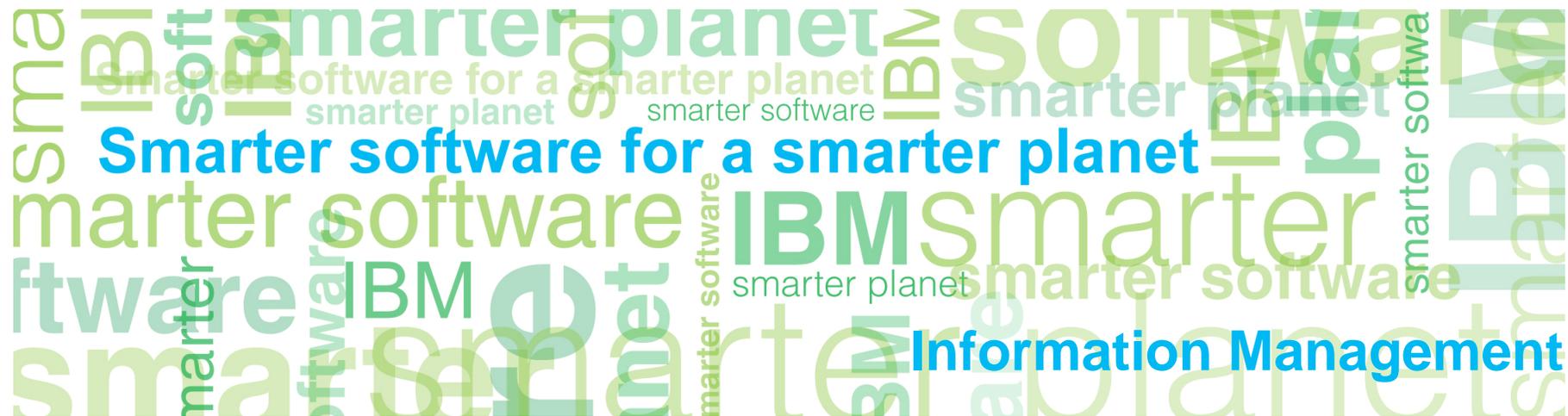


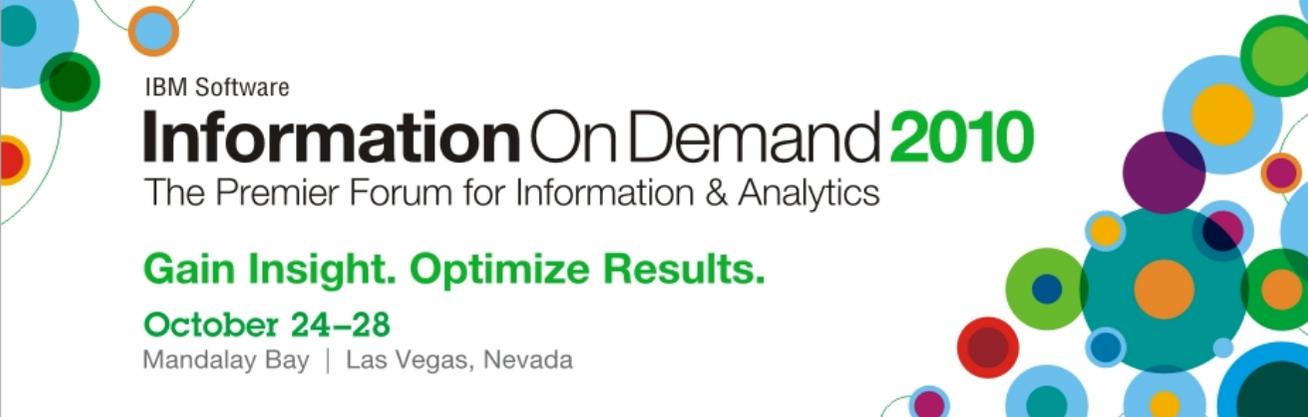


# IBM InfoSphere Guardium **Guardium**<sup>®</sup>

Sicherheitkontrolle(n) von Datenbanken in Echtzeit



## Information On Demand 2010 Las Vegas



IBM Software  
**Information On Demand 2010**  
The Premier Forum for Information & Analytics

**Gain Insight. Optimize Results.**  
**October 24–28**  
Mandalay Bay | Las Vegas, Nevada

Conference Overview **Business Analytics Forum**

Innovate and optimize with the best technical and business education. Two industry-leading IBM conferences become one powerhouse global event.



Registration  
Early Bird ends August 31!

### • Technical Track und Business Leadership Sessionstrack

§ Kunden, Partner und IBM Experten präsentieren Produktneuheiten und Einblicke in das Lösungsportfolio von Information Management

### § Business Partner Development

### § NEU! Business Analytic Forum

§ Industriespezifische Sessions (Industry Roadmaps) für ausgewählte Branchen

§ Möglichkeit von Einzelmeetings mit IBM Executives

§ „Meet the Expert“ Sessions zur individuellen Vertiefung/kundenspezifischen Diskussion

# Das ist das PROBLEM !

Fünf-Euro-Gutschein

## Schlecker entschuldigt sich für Datenpanne



Drogeriemarktkette Schlecker: Nach Datenpanne An:

Der Drogeriemarkt Schlecker will seine Kund bietet allen, deren Daten ungeschützt im Inte über fünf Euro an. Die Schuld an der Panne tr Dienstleister.

WELT ONLINE

Nachrichten | Debatte | Schö  
Politik | Wirtschaft | Geld | Sport | Wiss

In den Nachrichten: Thilo Sarrazin | Karstadt | Lottozahlen | Apple

01.09.10 | COMPUTERKRIMINALITÄT

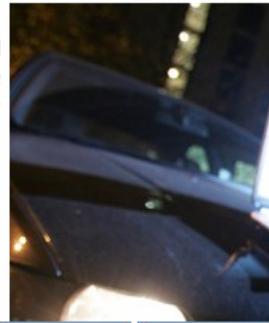
**Datendiebe kosten deutsche Unternehmen Milliarden**

Mittwoch, 11. Februar 2009, 15:50 Uhr

Die deutsche Wirtschaft Immer häufiger kommt d

### COMPUTER BILD deckt auf: Datenleck bei „Deutschland sucht den Superstar“

Grobe Patzer und Skandälchen sind bei der Casting-Show „Deutschland sucht den Superstar“ (DSDS) an der Tagesordnung. Doch bisher betrafen sie mehr die Gesangstalente der Bewerber



sowie di  
COMPUT  
sechste  
genüge

### Datenpanne bei Werder Bremen

Eine Datenpanne im Internet macht dem SV Werder Bremen zu schaffen: Zwei Stunden lang waren am 28. Juni die gespeicherten Daten von 34700 Mitgliedern und Werder-Kunden einsehbar - Namen, Adressen, Geburtsdaten und auch Kontonummern.

Quelle: Weser Kurier ([Link](#))

## IBM InfoSphere Guardium

### § **Guard** (engl. für Wachposten, Wächter )

- ist die ursprüngliche Berufsbezeichnung eines Bewachenden. Als Bewachung wird dabei hauptsächlich die Sicherung eines Objektes verstanden.
- Bewachungsobjekt kann z. B. ein Gegenstand, ein Gebäude, eine Stadt oder auch ein [Subjekt](#), d. h. eine Person sein. Heutige rechtliche Grundlage für das Tätigwerden von Wächtern und Wachleuten sind die [Gewerbeordnung](#) und die Bewachungsverordnung

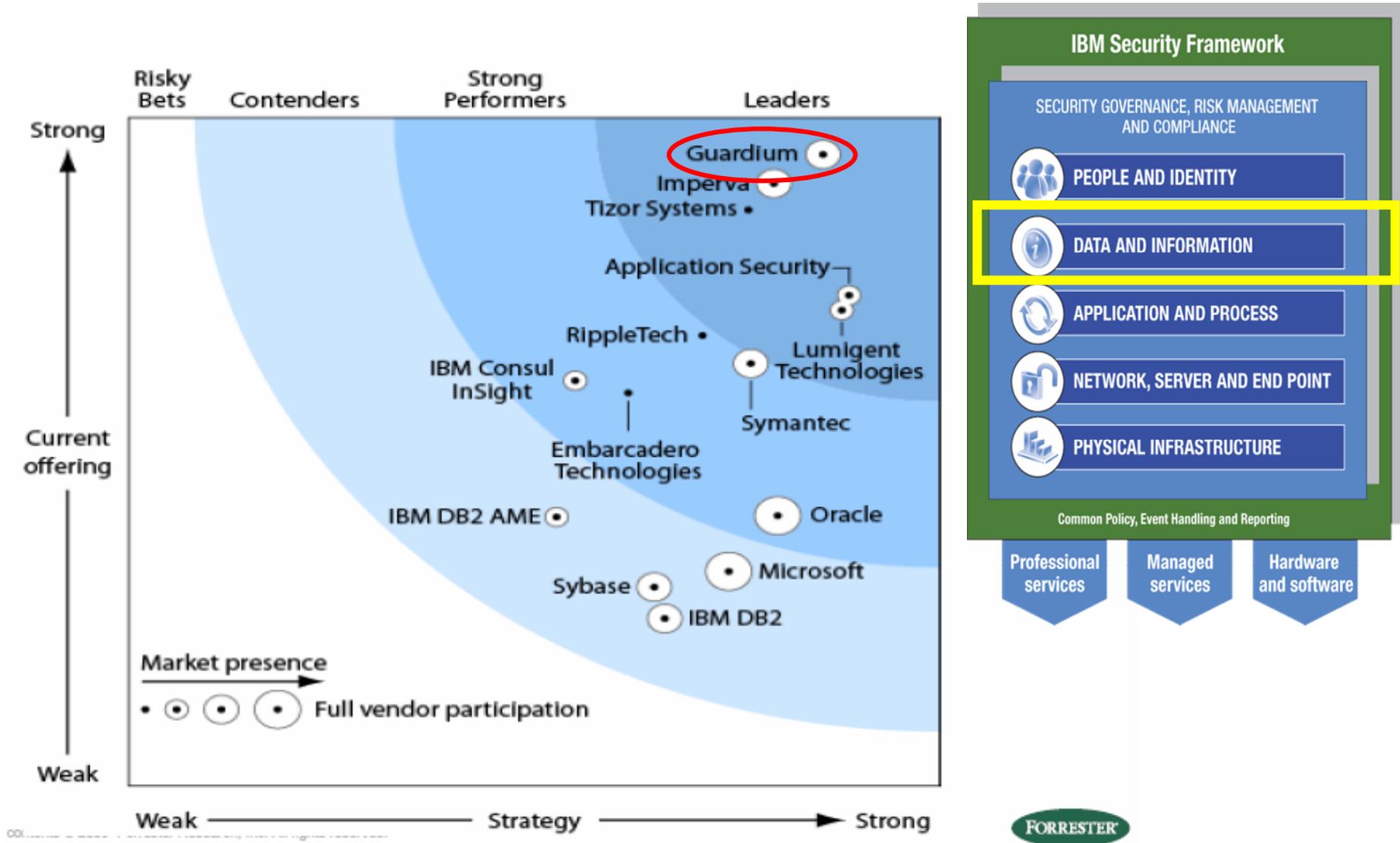
aus Wikipedia

### § **Guardium Corp.**

- gegründet 2002 in USA
- Database Activity Monitoring Markt
- Erste Industrielösung für Database Security am Markt (Oracle)
- 600+ Kunden
- 120+ Mitarbeiter weltweit
- Aquisition durch IBM im November 2009

# Guardium®

# InfoSphere Guardium ist führend im Database Security Markt



## Aussagen des Data Breach Report vom Verizon RISK Team (2009)

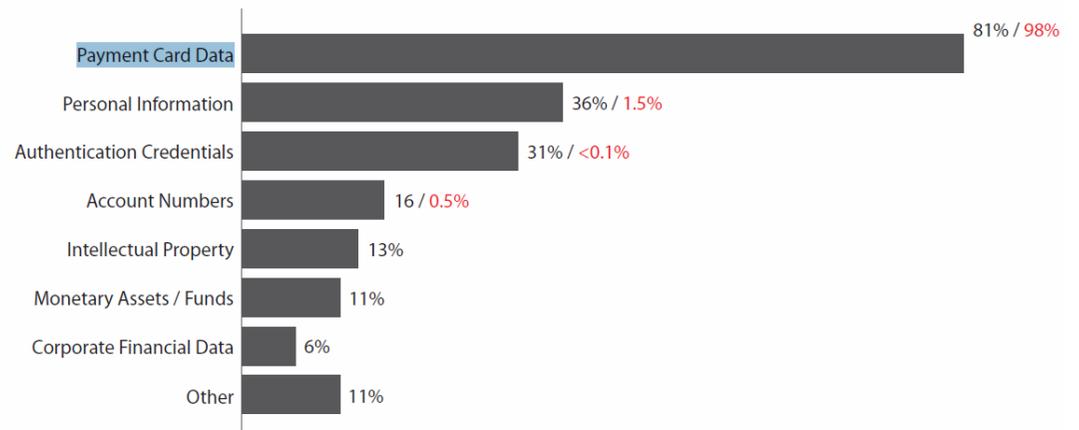
[http://www.verizonbusiness.com/resources/security/reports/2009\\_databreach\\_rp.pdf](http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf)

- § 2008 wurden mehr Datensätze attackiert als in den vorherigen 4 Jahren zusammen
- § **Datenbank** Server machen **75%** der kompromittierten Datensätze aus
- § **Kreditkarten** Daten machen **98%** aller attackierten Daten aus
- § Nur **5%** der attackierten Organisationen sind PCI Reqt. 10 konform

Table 9. Detailed listing of compromised assets by percentage of breaches and records

Asset	Asset Group	% of Breaches	% of Records
POS system	Online Data	32%	6%
Database server	Online Data	30%	75%
Application server	Online Data	12%	19%
Web server	Online Data	10%	
File server	Online Data	8%	
Public kiosk system	Online Data	2%	
Authentication / Directory server	Online Data	2%	
Backup tapes	Offline Data	1%	
Documents	Offline Data	1%	
Workstation	End-User System	8%	
Laptop	End-User System	4%	
PIN Entry Device	End-User System	2%	

Figure 29. Compromised data types by percent of breaches (black) and records (red)\*

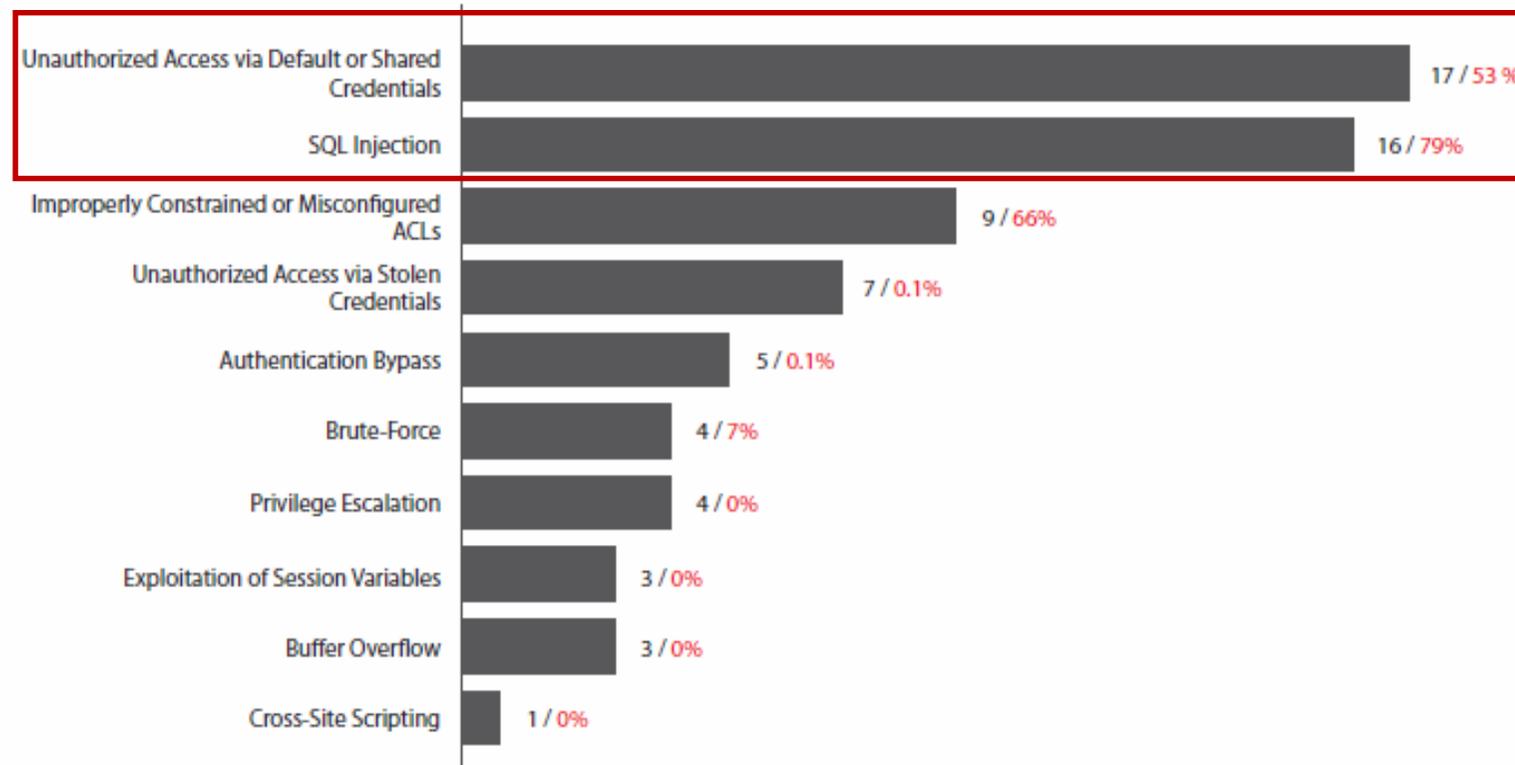


## Nr. 1 aller Angriffe: SQL Injection! - Zugriff über gemeinsame Berechtigungen -

§ Top 2 externe Einbruchsversuche sind “*unauthorized access via default or shared credentials*” & „*SQL injection*“

§ Die überwiegende Art von Web Attacken sind SQL injections

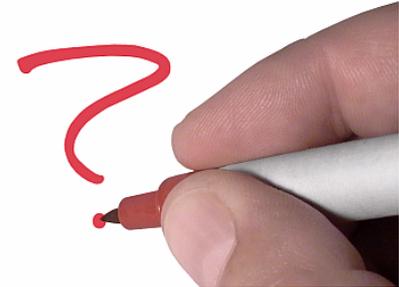
Figure 15. Types of hacking by number of breaches (black) and percent of records (red)



## Datenbank Sicherheit ist in Compliance Regularien festgelegt !

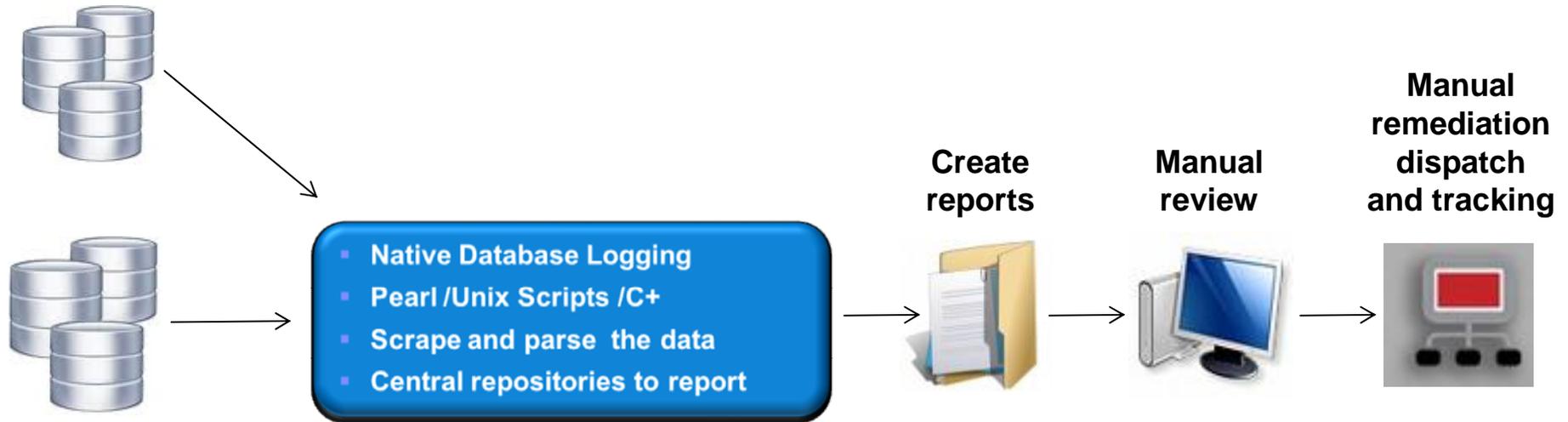
<b>Audit Requirements</b>	<b>CobiT (SOX)</b>	<b>PCI DSS</b>	<b>HIPAA</b>	<b>CMS ARS</b>	<b>GLBA</b>	<b>ISO 17799 (Basel II)</b>	<b>NERC</b>	<b>NIST 800-53 (FISMA)</b>
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓	✓		✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓		✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓			✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓	✓	✓	✓

## Sind sich Ihre Kunden sicher ??



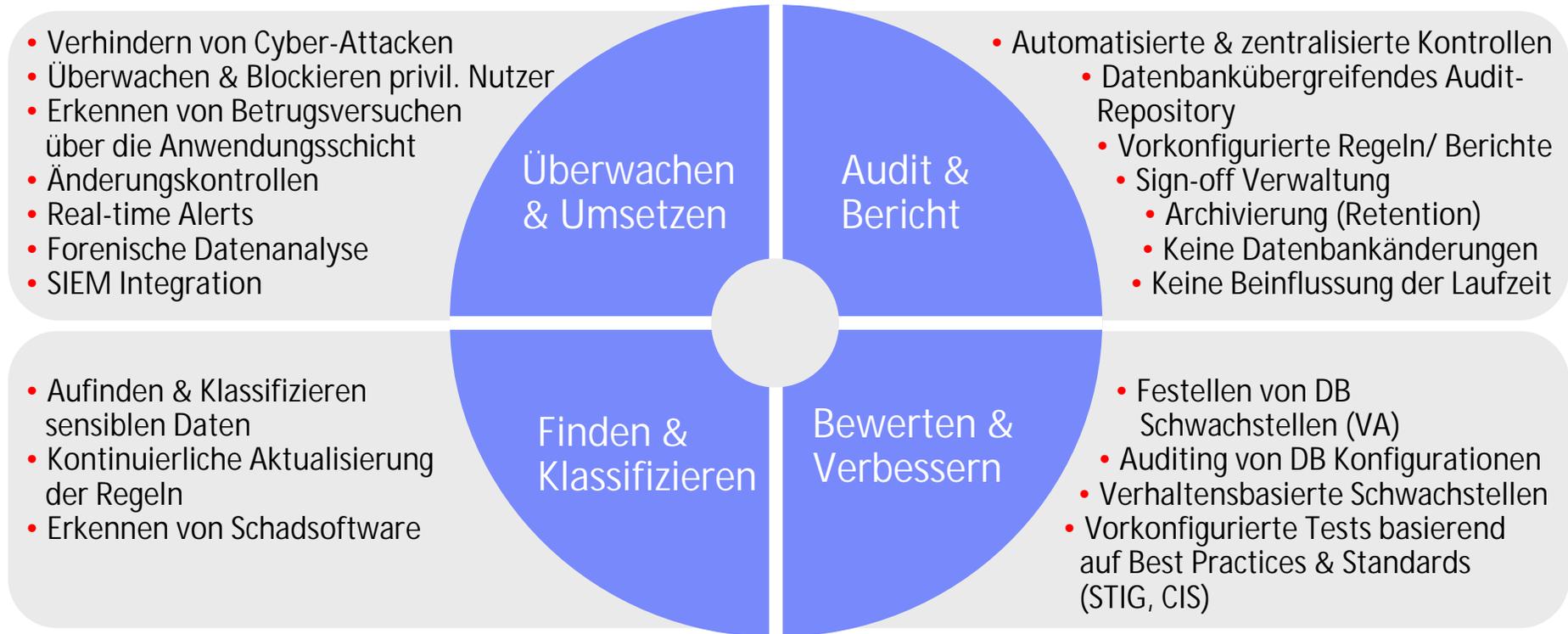
- § Wie sicher ist mein interner Datenschutz?
- § Wie kann ich identifizieren und sicherstellen, ob meine Datenbanken sicher *konfiguriert* und kritische *Patches* eingespielt sind?
- § Wir haben einige Unternehmenszusammenschlüsse/ Reorganisationen – wo befinden sich unsere sensiblen Daten?
- § Wie vermeide ich, dass Dienstleister sensible Informationen sehen können?
- § Wie können wir sicherstellen und monitoren, dass DBAs und andere privilegierte Nutzer ihre Zugriffsrechte nicht missbrauchen?
- § Wie können wir in Echtzeit feststellen, wenn z.B.:
  - Mehr als 3 fehlgeschlagene Loginversuche auftreten?
  - Jemand unauthorisiert eine sicherheitsrelevante Tabelle in SAP ändert?
  - Verdächtige Zugriffe aus dem Anwendungsserver Account auftreten?
- § Wie generiere ich Compliance/ Auditing/ PCI Berichte?
- § Datenbankeigene Auditmechanismen können einen hohen negativen Einfluss auf das Laufzeitverhalten haben
- § Datenbank-Logs generieren massiv Daten - Lösungen zum Speichern & Analysieren, zur Berichterstellung & Archivierung werden benötigt
- § Nativer Zugriff auf die Logs liefert nicht alle benötigten Informationen um zu wissen *wer wann wie auf welche* Daten zugegriffen hat

## Bisher verfügbare Lösungen sind teuer oder arbeitsintensiv

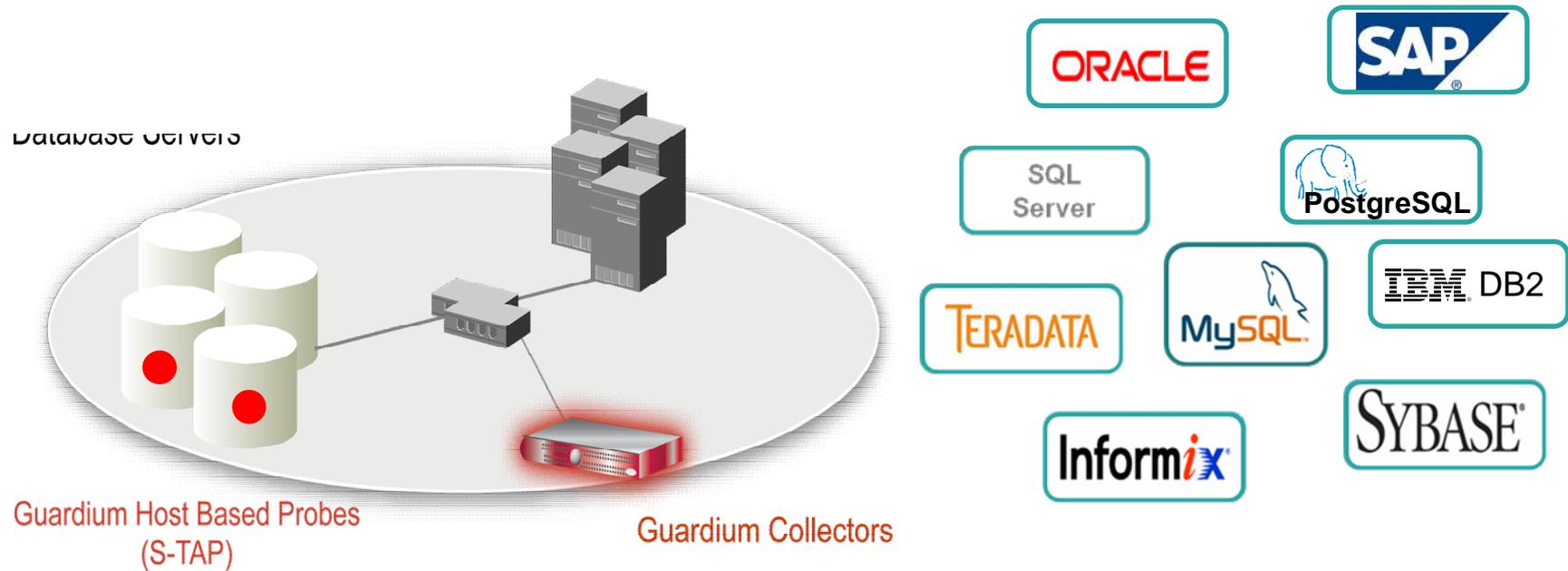


- Signifikante Mitarbeiterkosten für den Review und die Pflege
- Performance Auswirkungen auf der DB durch natives DB logging
- Keine Echtzeit-Auswertungen der Zugriffe
- Sind im Regelfall nicht Auditkonform gemäß "Vier-Augen-Prinzip" (Separation of Duties)
- Der Audit-Trail ist vor Manipulationen nicht geschützt
- Auditing kann nicht regelbasierend durchgeführt werden

## Wir haben die Lösung: IBM InfoSphere Guardium



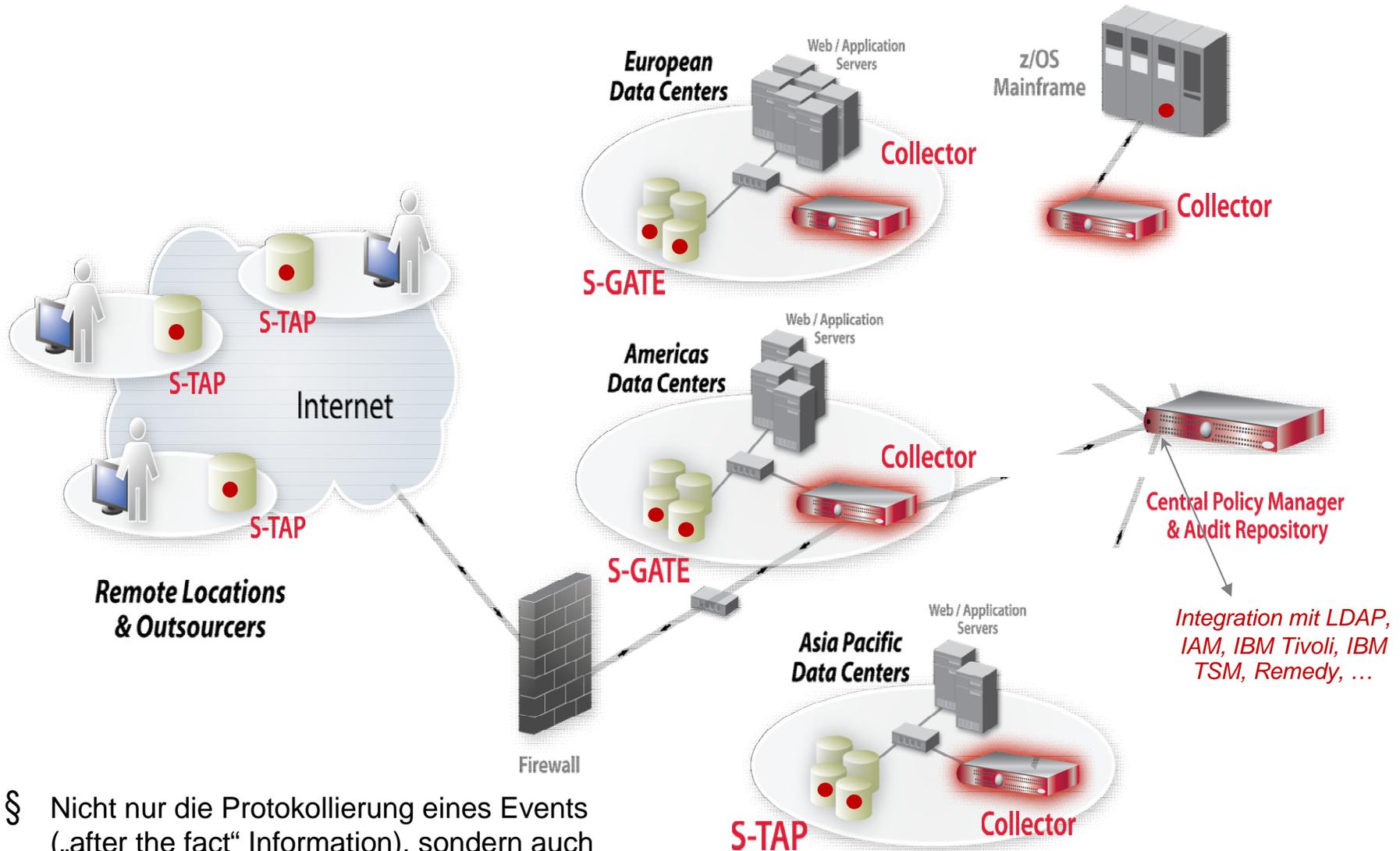
## Das ist Datenbanküberwachung in Echtzeit



- § Nicht-invasive Architektur
  - Außerhalb der Datenbanken
  - Minimaler Einfluß auf Performance (2-3%)
  - Keine Änderungen der DBMS oder Anwendungen
- § Unterstützung heterogener Systemlandschaften
- § Zentralisiertes Auditing im Guardium Collector
- § 100% Transparenz, inkl. Zugriffe lokaler DBAs

- § Realisiert Vier-Augen-Prinzip (Separation of Duties)
- § Verläßt sich nicht nur auf lokale DBMS logs die von Angreifern gelöscht werden können
- § Granulare Regeln & Echtzeit Auditing
  - *Wer, Was, Wann, Wie*
- § Automatisiertes Compliance Reporting, sign-offs & Eskalationen (SOX, PCI, NIST, etc.)

# Wie funktioniert eine Skalierbare Multi-Tier Architektur



§ Nicht nur die Protokollierung eines Events („after the fact“ Information), sondern auch eine aktive Zugriffsbeschränkung in Echtzeit

## Am Beispiel: Was kann InfoSphere Guardium?

1. **Finden & Klassifizieren**
  - Transparenz: „Access Map“ der Datenbankzugriffe
  - Angriffe erkennen und verhindern
2. **Überwachen & Umsetzen**
  - Granulare Regeldefinition
  - Auffälliges Nutzerverhalten feststellen
  - Nicht bevollmächtigte Zugriffe identifizieren und verhindern
  - Betrugsversuche in der Anwendungsschicht erkennen (Connection Pooling)
3. **Audit & Bericht**
  - Definition von Workflows (Sign-off / Eskalationen / Kommentare)
  - Erstellen von Audit-Berichten (auf Basis von Templates)
4. **Bewerten & Verbessern**
  - Schwachstellen-Analyse



# Database Discovery

**Guardium**

View Monitor/Audit Discover Assess/Harden Comply Protect Nir

Classification DB Discovery

- Auto-discovery Configuration
- Auto-discovery Query Builder
- Databases Discovered
- Data Sources
- Data Source Version History

**Auto-discovery Configuration**

**Auto-discovery Process Builder**

**Configuration:**

Process name

This process is not running. Progress/Summary

---

Run probe automatically after scan

**Current tasks:**

Note: This process scans up to 257 host(s) and 240352 ports.

	Host(s)	Ports
✘	<input type="text" value="192.168.2.*"/>	<input type="text" value="1521-2000"/>
✘	<input type="text" value="192.168.3.12 192.168.3.15"/>	<input type="text" value="1025-60000"/>

Revert Apply

---

**Add a new task:**

List of hosts to Auto-discover:

Add

---

**Scheduling:**

**Scan for open ports:**

Scanning is currently not scheduled for execution.

Modify Schedule...

**Databases Discovered**

**Start Date:** 2008-06-26 14:48:49 **End Date:** 2008-06-26 15:48:49

Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp

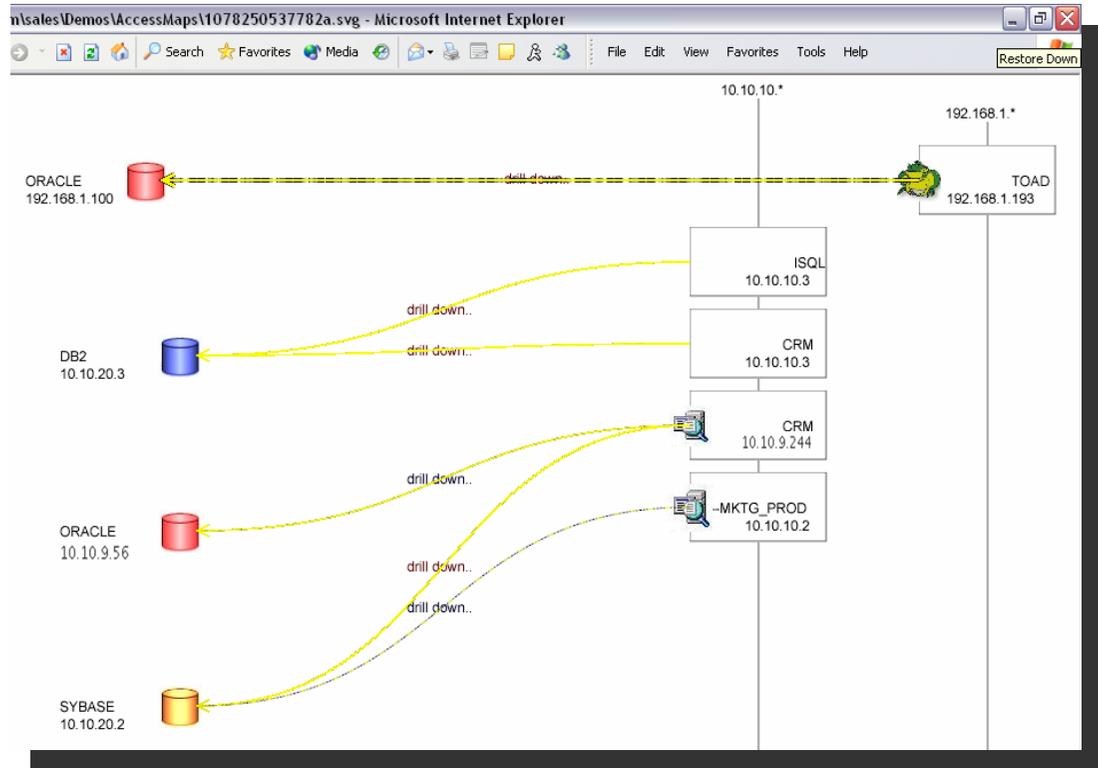
# 100% Sichtbarkeit



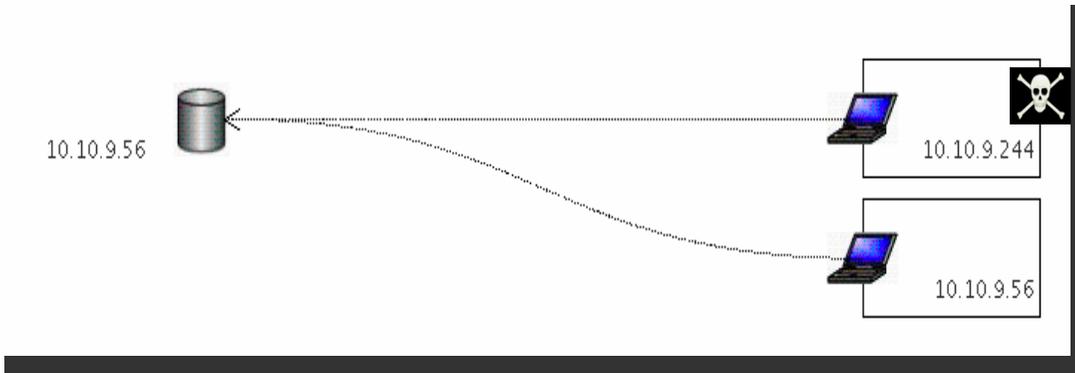
Anwendungs Server  
10.10.9.244



Datenbank Server  
10.10.9.56



## Angriffe identifizieren



Interne Angreifer wissen wonach sie suchen, aber ...

Sie wissen nicht immer wo die Informationen zu finden sind!

SQL injection führt zu **SQL Fehlern!**

Returned SQL Errors

Start Date: 2007-03-01 00:00:00 End Date: 2007-04-15 00:00:00

Client IP	Server IP	Server Type	DB User Name	Database Error Text
10.10.9.244	10.10.9.56	ORACLE	APPLSYSUB	ORA-00942: table or view does not exist

Failed Login Attempts

Start Date: 2007-03-01 00:00:00 End Date: 2007-05-01 00:00:00

User Name	Source Address	Destination Address	Database
MarcG	192.168.20.107	10.10.9.56	ORACLE
APPLSYSUB	10.10.9.244	10.10.9.56	ORACLE
APPLSYSUB	10.10.9.56	10.10.9.56	ORACLE

Brute force Angriffe resultieren in **failed logins!**

Guardium: 100% Sichtbarkeit mit real-time alerts ...



# Granulare Regeln mit Real-Time Alerts

**Rule #5 Description** Login Failures to Production Database Server

**Category** Security **Classification** Breach **Severity** HIGH

**Hot**  **Server IP** / and/or Group **Production Servers**

**Hot**  **Client IP** / and/or Group

**Hot**  **Client MAC** **Net. Protocol** and/or Group

**DB Type** **Hot**  **Service Name** and/or Group

**Hot**  **DB Name** and/or Group

**Hot**  **DB User** APPUSER and/or Group

**Hot**  **Error Code** and/or Group

**Hot**  **Exception Type** LOGIN\_FAILED

**Min. Ct.** 0 **Reset Interval (minutes)** 0

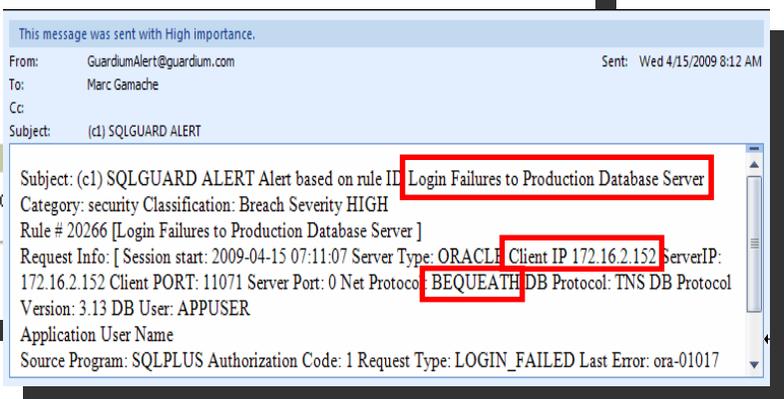
**Continue to next Rule**  **Rec. Vals.**

**Action** ALERT PER MATCH

**Notification**

**Notification Type** MAIL **Mail User** marc\_gamache@guardium.c...

**Notification Type** MAIL  
SNMP  
CUSTM  
SYSLOG



Fokus auf Produktionssysteme

Identifizieren von fehlgeschlagenen Anmeldungen mit dem Anwendungs-Nutzer (technischer User sowie End-User)!

**Aktion ausführen:** Alarm via Email, SYSLOG, SNMP oder eigener Java class senden

Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

## Auffälliges Verhalten feststellen

Sollte mein Kundenservice Mitarbeiter 99 Datensätze die Stunde bearbeiten?

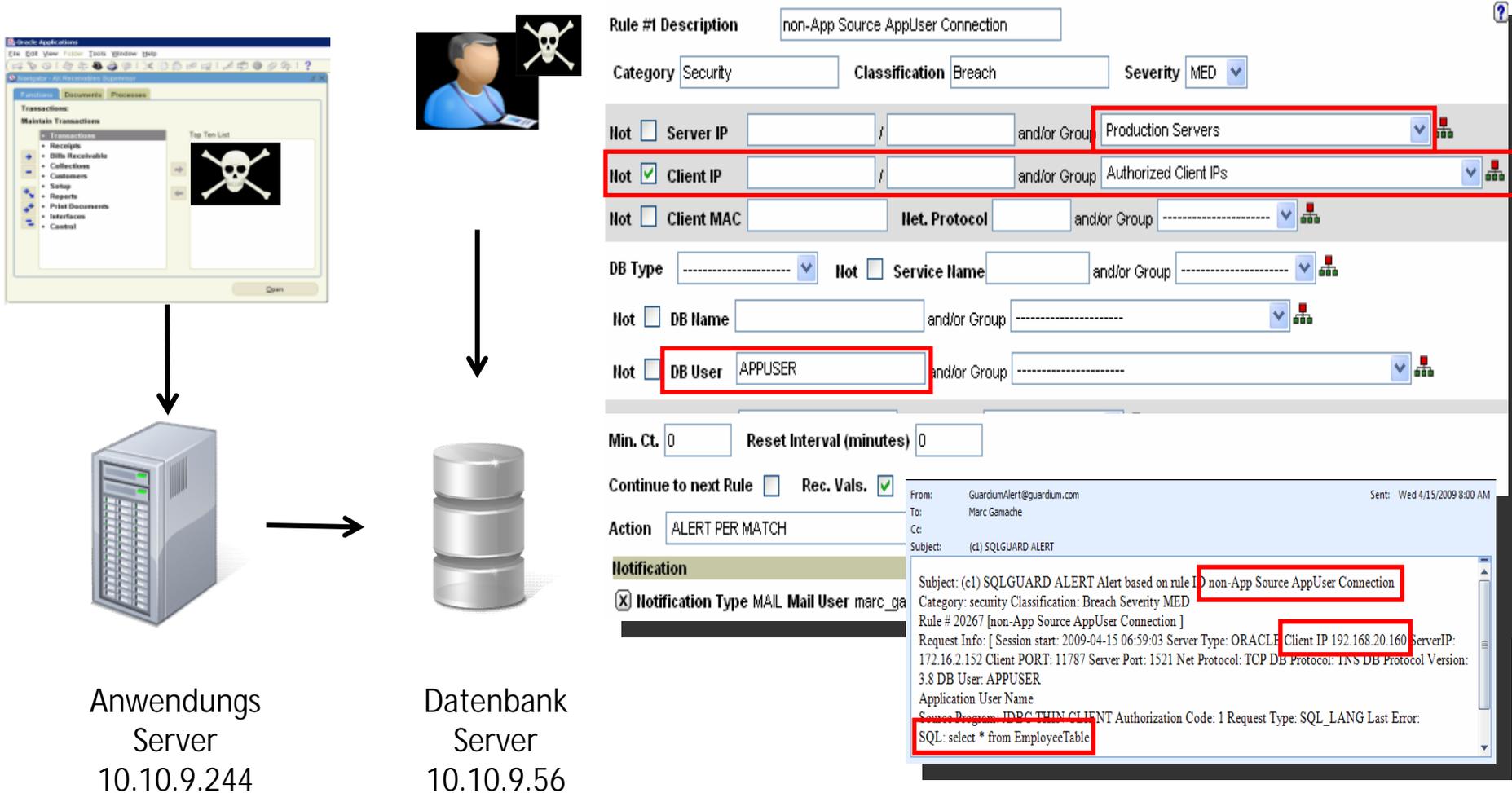
**Ist das normal?**

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<? 4	
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

**Was hat er angeschaut?**

HARRY	select * from ar.creditcard where i<?	*****0002, *****0003, *****0004
JOE	select * from ar.creditcard where i<?	*****0001
JOE	select * from ar.creditcard where i<?	*****0002, *****0003, *****0004, *****0005, *****0006, *****0007, *****0008, *****0009, *****0010, *****0011, *****0012, *****0013, *****0014, *****0015, *****0016
JOE	select * from ar.creditcard where i<?	*****0017, *****0018, *****0019, *****0020, *****0021, *****0022, *****0023, *****0024, *****0025, *****0026, *****0027, *****0028, *****0029, *****0030, *****0031
JOE	select * from ar.creditcard where i<?	*****0032, *****0033, *****0034, *****0035, *****0036, *****0037, *****0038, *****0039, *****0040, *****0041, *****0042, *****0043, *****0044, *****0045, *****0046
JOE	select * from ar.creditcard where i<?	*****0047, *****0048, *****0049, *****0050, *****0051, *****0052, *****0053, *****0054, *****0055, *****0056, *****0057, *****0058, *****0059, *****0060, *****0061
JOE	select * from ar.creditcard where i<?	*****0062, *****0063, *****0064, *****0065, *****0066, *****0067, *****0068, *****0069, *****0070, *****0071, *****0072, *****0073, *****0074, *****0075, *****0076
JOE	select * from ar.creditcard where i<?	*****0077, *****0078, *****0079, *****0080, *****0081, *****0082, *****0083, *****0084, *****0085, *****0086, *****0087, *****0088, *****0089, *****0090, *****0091
JOE	select * from ar.creditcard where i<?	*****0092, *****0093, *****0094, *****0095, *****0096, *****0097, *****0098, *****0099

# ALERTs für unberechtigte Zugriffe & Credential Sharing



**Alarm** für jeden Login der den technischen Benutzer von einem anderen System als dem Anwendungsserver nutzt!

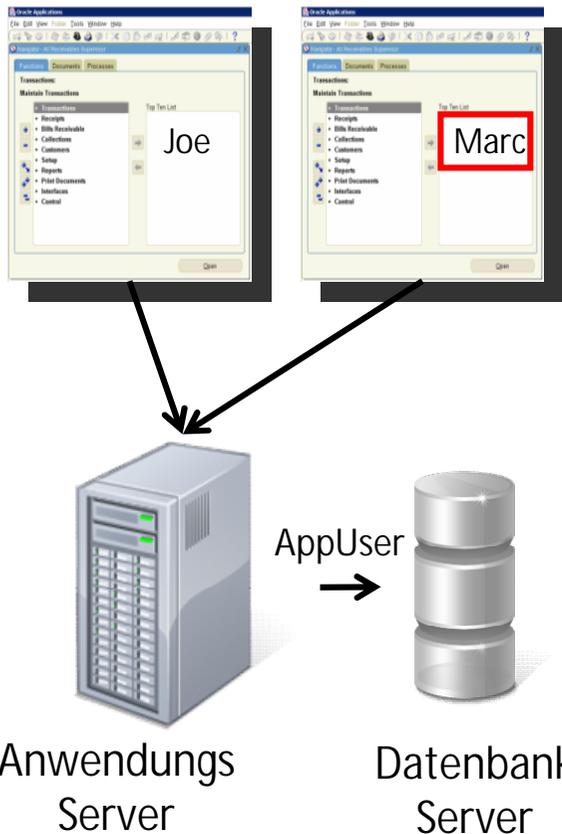
# Application Layer Monitoring

DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?)

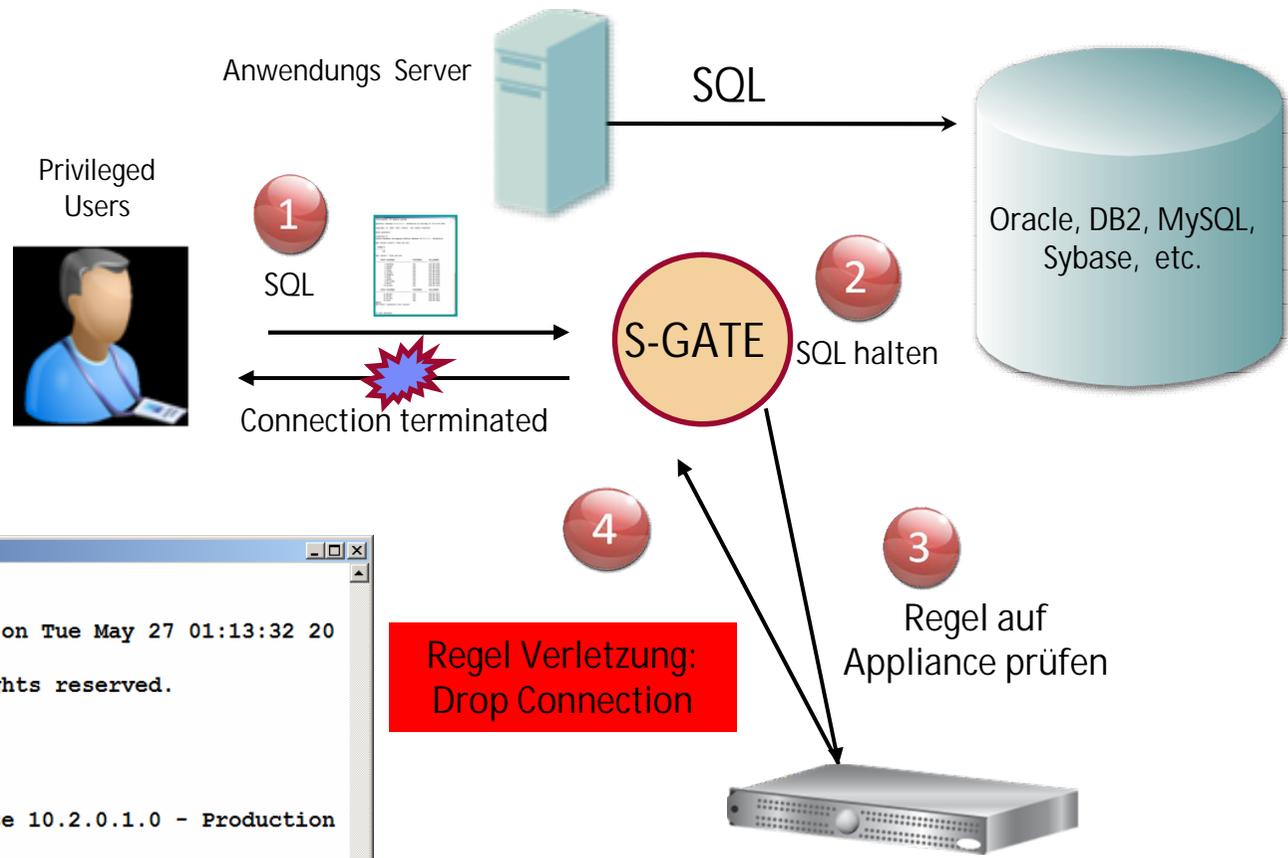
§ **Problem:** *Anwendungs Server nutzt generischen Account um auf die DB zuzugreifen – es ist nicht ersichtlich welcher Endbenutzer hinter dem DB Zugriff steht (connection pooling)*

§ **Lösung:** Zuordnung von Anwendungsnutzern mittels spezieller SQL Befehle

- Deterministische Identifizierung und kein zeitbasierter “best guess”
- Out-of-the-box Unterstützung für gängige Unternehmensanwendungen (Oracle Applications, PeopleSoft, SAP, Siebel, Business Objects, Cognos, etc.)
- Plus eigene Anwendungen (WebLogic, WebSphere, Oracle AS, etc.)
- Keine Änderungen der Anwendungen nötig



# S-GATE: Unberechtigte Zugriffe blockieren



```

root@osprey:~
[root@osprey ~]# sqlplus system
SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Enter password:
Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production
SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel
SQL>
    
```

Session Terminated

# S-GATE: Granulares Regelwerk

Rule #4 Description: Terminate Connection

Category: Policy Classification: Violation Severity: HIGH

Hot  Server IP [ ] / [ ] and/or Group: **Production Servers**

Hot  Client IP [ ] / [ ] and/or Group [ ]

Hot  Client MAC [ ] Net. Protocol [ ] and/or Group [ ]

DB Type: **Oracle** Hot  Service Name [ ] and/or Group [ ]

Hot  DB Name [ ] and/or Group [ ]

Hot  DB User [ ] and/or Group: **(Public) Admin Users**

Hot  App. User [ ] and/or Group: **Oracle EBS AppUser Group**

Hot  OS User [ ] and/or Group: **Unauthorized OS Users**

Hot  Src App. [ ] and/or Group [ ]

Hot  Field Name [ ] and/or Group: **Sensitive Columns**

Hot  Object [ ] and/or Group: **Financial Objects**

Hot  Command [ ] and/or Group: **(Public) DML Commands**

Min. Ct. 0 Reset Interval (minutes) 0

Continue to next Rule  Rec. Vals.

Action: S-GATE TERMINATE

ALERT DAILY

ALERT ONCE PER SESSION

ALERT PER MATCH

ALERT PER TIME GRANULARITY

ALLOW

IGNORE RESPONSES PER SESSION

IGNORE SESSION

IGNORE SQL PER SESSION

LOG FULL DETAILS

LOG FULL DETAILS PER SESSION

LOG FULL DETAILS WITH VALUES

LOG FULL DETAILS WITH VALUES PER SESSION

LOG MASKED DETAILS

LOG ONLY

RESET

**S-GATE ATTACH**

S-GATE DETACH

S-GATE TERMINATE

S-TAP TERMINATE

SKIP LOGGING

Welche Server

Welche Datenbanken

Welche Nutzer

Welche Felder

Welche Tabellen

Welche SQL Ausdrücke

Mit der Möglichkeit die Verbindung zu terminieren und einen Datenverlust zu verhindern!

## Audit Workflow mit Sign-Off & Eskalationen



### Weekly Database Change Management Process

Audit process execution began 4/16/09 12:24 AM

Other Results For This Process

Sign Results
 Continue
 Escalate
 Comment
 Download PDF

Distribution Status:

Receiver	Status	Action Required
Marc(Marc Gamache)	Viewed not Signed	Review and Sign
Role dba	Not Distributed	Review Only
Role infosec	Not Distributed	Review and Sign
Role audit	Not Distributed	Review and Sign

Comments:

- [Report: Database Changes Report \[-ChangeRequest Report\] Overall Value: 3](#)

---

- [Security Assessment: Security Assessment \[-Assessment\] Overall Value: 36](#)

---

- [Classification Process: Classification Process \[Search for CreditCard Accounts - CreditCard Accounts\]](#)

---

- [Report: Failed DB Logins Report \[Failed User Login Attempts\] Overall Value: 1](#)

---

- [Report: SQL Errors Report \[SQL Errors\] Overall Value: 56](#)

[Close this window](#)



# Vulnerability Assessment

- § Basierend auf Industry Best Practices
- § Betrachtet das gesamte Datenbankumfeld unter Berücksichtigung vom Betriebssystem
- § Assessment Tests beinhalten:
  - § Configuration Assessment
  - § Vulnerability Assessment
  - § Behavioral Assessment
- § Assessment Report beinhalten
  - § Testresultate in diversen Ansichten
  - § Remediation Plan

**Assessment Test Selections**

Tests for Security Assessment: Health Assessment Test 1

Select All | Unselect All | Remove Selected

Type	Test Name	Tuning
<input type="checkbox"/> [Observed]	Clients Executing DDL Commands	Other Informational 2: Maximum Number of clients executing DDL commands allowed
<input type="checkbox"/> [Observed]	DDL Command Executions	Other Informational 20: Maximum Number of DDL commands executions allowed per day (after factoring the assessed period)
<input type="checkbox"/> [Observed]	One User One IP	Other Informational 2: Maximum Number of Different IP's Allowed per user
<input type="checkbox"/> ORACLE	DBLINK_ENCRYPT_LOGIN Is True	Configuration Informational (n/a) :
<input type="checkbox"/> ORACLE	No Authorizations To System	Configuration Informational (n/a) :

Tests available for addition

predefined | custom | query based | All

[Observed] | ORACLE | DB2 | SYBASE | MS SQL S... | INFO

Select multiple items using Shift- or Ctrl-click

Configuration: \_TRACE\_FILES\_PUBLIC Is False  
 Configuration: ADMIN\_RESTRICTIONS Is On  
 Configuration: CONNECT\_TIME limited  
 Configuration: CPU\_PER\_SESSION limited  
 Configuration: DBA Profile FAILED\_LOGIN\_ATTEMPTS Are Limited  
 Configuration: DBA Profile PASSWORD\_LIFE\_TIME Is Limited  
 Configuration: DBA Profile PASSWORD\_VERIFY\_FUNCTION Is Implemented  
 Authentication: Default Accounts Password Changed  
 Other: File permissions  
 Other: File scanning

Back | Groups

**Guardium Security Assessment Results - Internet Explorer**

Results for Security Assessment: VA test for production servers  
 Assessment executed 2008-10-20 23:27:13.0  
 From: 2008-10-13 23:27:13.0 To: 2008-10-20 23:27:13.0  
 Client IP or IP subnet: Any Server IP or IP subnet: Any

Download PDF

Assessment Result History

Tests passing: 38%

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

Result Summary Showing 93 of 93 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	8p	16f	2p	3f	2f
Authentication	6f	1f	1f	1f	
Configuration	2p	2f	5p	6f	4e
Version			2f		
Other	1p	3p	2f	3p	1f

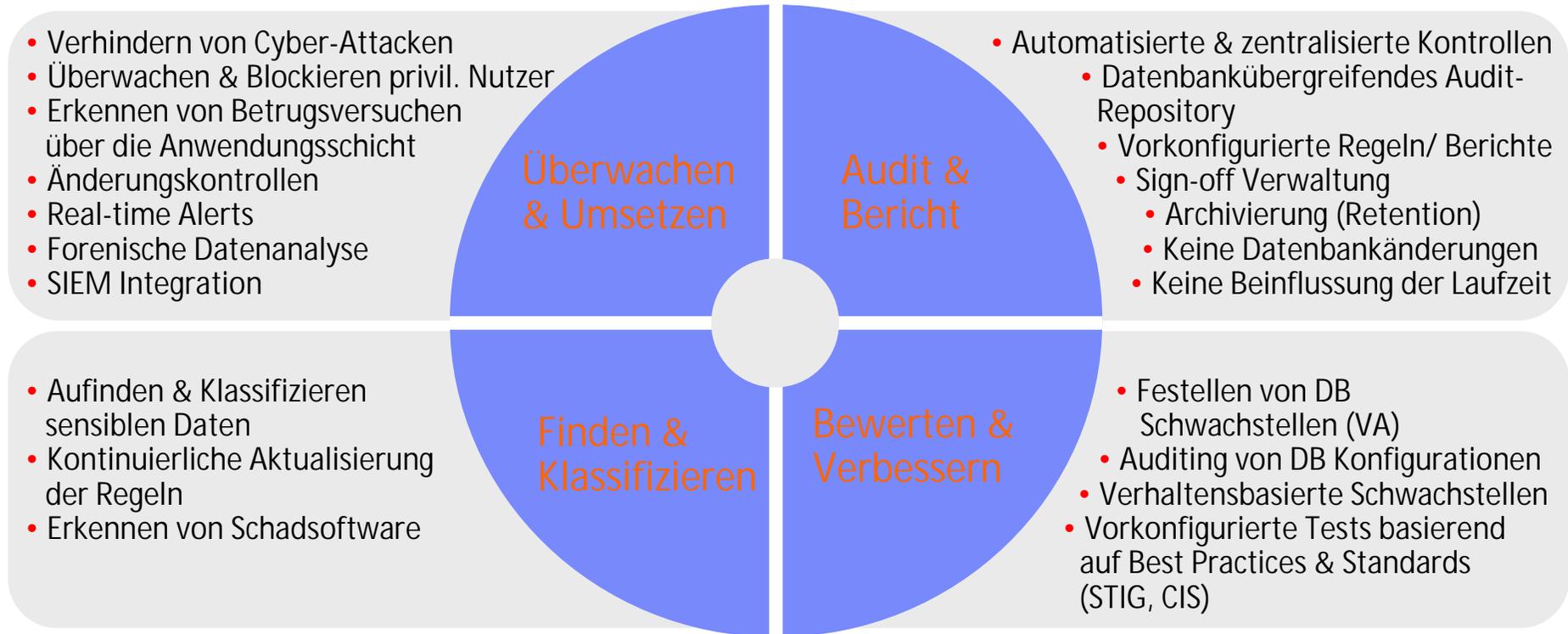
Current filtering applied:  
 Severities: - Show All -  
 Scores: - Show All -  
 Types: - Show All -

Reset Filtering | Filter / Sort Controls

Assessment Test Results

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Conf.	DBA Profile PASSWORD_LIFE_TIME Is Limited	ORACLE Oracle on Ocean	Fail	Critical	User profile [DEFAULT] setup parameter PASSWORD_LIFE_TIME found out of defined threshold value. <b>Recommendation:</b> The PASSWORD_LIFE_TIME parameter is not set, allowing users to retain the same password indefinitely. Passwords that have been in use for long periods of time are likely to become known to unauthorized users. We recommend that you set this parameter in order to limit the lifetime of users' passwords.
Conf.	DBA Profile PASSWORD_VERIFY_FUNCTION Is Implemented	ORACLE Oracle on Ocean	Fail	Critical	Found active profile 'APPL_PROFILE_DEFAULT' with PASSWORD_VERIFY_FUNCTION not implemented. <b>Recommendation:</b> No Password Verification Routine has been implemented. We recommend that you implement a password function to prevent the use of weak passwords.
Auth.	Default Accounts Password Changed	ORACLE Oracle on Ocean	Fail	Critical	2 active pre-defined users have default passwords. <b>Recommendation:</b> Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that you remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.
Priv.	No Access To 'Users' Catalog Tables	ORACLE Oracle on Ocean	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <b>Recommendation:</b> Access to the DBA_USERS or ALL_USERS tables has been granted to users other than DBA or SELECT_CATALOG_ROLE. We recommend restricting access to these tables for security reasons.
Priv.	No Authorizations To System Level	ORACLE	Fail	Critical	Users or roles, other than DBAs, were found with access to EXECUTE ANY PROCEDURE, GRANT

## Zusammenfassend: Das sind die Funktionen von InfoSphere Guardium



## Alle gängigen Plattformen & Anwendungen werden unterstützt

Unterstützte Datenbanken	Unterstützte Versionen
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle (ASO, SSL)	9i, 10g (r1,r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Windows)	9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10,11, 11.50
MySQL und MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
PostgreSQL	8
Oracle Enterprise Application Server	
IBM Websphere	
SAP	
IBM Cognos	
Teradata	6.x, 12, 13
FTP	

## Wie lizensiere ich Guardium & Wie groß ist ein typ. Projekt

### § Lizensiert wird

- InfoSphere DB Activity Monitor (Appliance Server & Software) nach PVU
- Agent je DB Server der überwacht wird (IBM, Oracle, Microsoft, etc.) nach PVU
  
- Alternativ: virtuelle Lizensierung (SW only) nach PVU

### § Sales Cycle

- 6 - 8 Monate, ggf. auch kürzer

### § HEUTE: FCT Vertrag mit PA Nummern

### § MORGEN: Software ValueNet (SWVN)

- Akkreditierung notwendig

### § **Typ. Projekte**

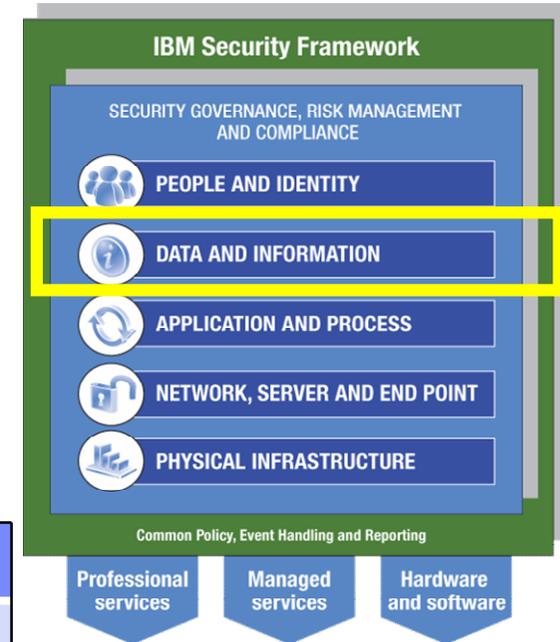
- Kleine Instanz für 1 -5 Datenbanken
  - Appliance, SW, Service (3-10 MT) 30- 50 k€ (Listpreis)
- Große Instanz für 10- 100 Datenbanken
  - Appliance, SW, Service (ca. 50 MT) 200-250 k€ (Listpreis)

## Warum Buy und nicht Build – Vorteile einer gekauften Lösung -

- § Unabhängigkeit von Personen die Systeme erstellt haben. → Erhöhung der Flexibilität → **Sicherheit (der Dieb der sein Schloss selber baut)**
- § Integrität des Systems an sich muss in einem Audit nicht mehr nachgewiesen werden. → **Kostenreduktion**
- § Gesicherte Wiederverwendbarkeit und Interoperabilität → **Kostenreduktion & Erhöhung der Flexibilität**
- § Hohe Betriebseffizienz, ohne versteckte Folgekosten → **Kostenreduktion**
- § Mögliche Verrechnung von Services an Kostenverursacher → **Bedarfsgerechte Abrechnung**
- § Unabhängigkeit von Applikations- und Datenbankherstellern → **Erhöhung der Flexibilität**
- § Zusätzliche Funktionalität out of the Box (z.B. PCI Compliance) → **Kostenreduktion & Erhöhung der Flexibilität**
- § Native Logs manuel überprüfen - vs. **Automatisierte Kontrolle**
- § Admin kann seine eigenen Logs manipulieren - **der Täter verschafft sich seine eigene „Freiheiten“**

## Das Zusammenspiel von Guardium & Tivoli

- § Guardium adressiert die “Data and Information” Schicht des IBM Security Framework
- § Integriert sich mit dem Tivoli Compliance Insight Manager (TCIM) zum Austausch von Regelverletzungen (Alerts) und Log Informationen



	Guardium	Tivoli TCIM
Addresses security & compliance for database environments	√	√
Monitors privileged users	√	√
Collects & correlates native logs from OS servers, applications, etc.	x	√
Monitors all database transactions – in real-time – without overhead and SoD issues of native logs	√	x
Provides database-focused analytics, reporting, vulnerability assessment & data-level access control	√	x

## Zusammenfassung: Welche Zielgruppe hat erhöhte Sicherheitsanforderungen

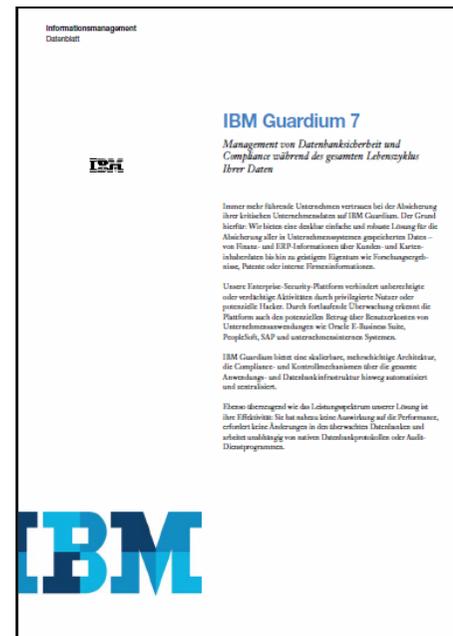
- § Unternehmen oder Organisationen, welche **sensitive Daten speichern und verarbeiten** und/oder erhöhte Anforderungen an die Einhaltung von Datenschutzrichtlinien erfüllen müssen.
- § Unternehmen die den Zugriff von „**geistigen**“ **Informationen gegenüber Dritten** verhindern müssen
- § Beispiele für sensitive & unternehmenswichtige Daten
  - Kreditkarten Daten
    - PCI - Payment Card Industry Data Security Standard
    - Einhalten zahlreicher Sicherheitsbestimmungen, vielfache Audits
    - Banken, Versicherungen, eCommerce
  - Gesundheitsdaten
  - Krankenkassen, Verbände, Behörden
  - Finanzdaten
  - Unternehmensberatungen, (Finanz und Steuer)-Behörden
  - Unternehmen mit „geistiger“ Entwicklung (Automobilindustrie, etc.)
  - Telekom, Internet Communities, ...
  - der Vertrieb....
  - Typische „Datensammler“

## Zusammenfassung: Die Vorteile von InfoSphere Guardium

- § Unterstützung der gängigsten Datenbankhersteller und Anwendungsanbieter
  - Guardium Standard im Unternehmen
- § Datenbankeigene Werkzeuge können **nicht**
  - die notwendige Zugriffstransparenz schaffen
  - unauthorisierte Zugriffe verhindern
  - minimalen Performance-Overhead generieren
- § Guardium ist nicht nur reine Event-Monitoring Lösung, sondern auch eine **Prevention** Lösung
- § Mit Guardium zentralisiert ein Unternehmen die **Daten- Auditing- und Compliance- Verfahren**
- § Guardium ist die industrieführende Lösung am Markt:
  - Granulare Visibilität und Echtzeit Regeln
  - Automatisierung
  - Skalierbare Architektur
- § Für den Kunden ist die Cost of Compliance kalkulierbar

## Unterstützung durch Marketing & Schulungen

§ Flyer, Whitepaper in dt. Sprache



§ Guardium Bootcamp 05.-08.10.2010 in Ehningen

– <http://www.ibm.com/developerworks/wikis/display/im/Guardium+Bootcamp>

## Referenzen



## Links & Weitere Infos

- § Guardium Homepage <http://www.guardium.com/>
- § IBM InfoSphere Guardium <http://www-01.ibm.com/software/data/guardium/>
- § Data Governance Blueprint <http://www-01.ibm.com/software/data/db2imstools/solutions/security-blueprint.html>
- § PCI Security Standards Council for Gaaadium <http://www.guardium.com/index.php/pr/90>
- § PCI Security Standards Council <https://www.pcisecuritystandards.org/>

