Sicherheitskontrolle von Datenbanken in Echtzeit

Datenschutz, Compliance und Sicherheit in Echtzeit

Sprecher: Patrick Würl

Ein neues Bewusstsein

Fünf-Euro-Gutschein

Schlecker entschuldigt sich für Datenpanne

Drogeriemarktkette Schlecker: Nach Datenpanne An

WELT ONLINE

Nachrichten | Debatte | Schö

Politik | Wirtschaft | Geld | Sport | Wiss

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

01.09.10 | COMPUTERKRIMINALITÄT (14)

Datendiebe kosten deutsche Unternehmen Milliarden

Die deutsche Wirtschaft leidet unter den A

Immer häufiger kommt die Gefahr aus den

Mittwoch, 11. Februar 2009, 1

Einfacher Hackerangriff r

COMPUTER BIL atenleck

bei „Deutschlar uperstar"

Investigators Reveal 'Massive' World Cup Data Breach

By Chris Wright on September 6th, 2010 - 1 Comment

It should come as no surprise to any football fan with even a passing contempt for the game's governing body that FIFA have yet again dropped a sizeable bollock, a bollock that stands a very good chance of ruining many innocent supporters' lives.

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)

Branchenspezifische Anforderungen

- Fertigende Industrie
  - Entwicklungsdaten (z.B. CAD Pläne, Rezepturen..)
  - CRM & Forecast Daten

- Finanzinstitute
  - Compliance Auflagen durch z.B. BaFin oder PCI
  - Manipulationsmöglichkeiten

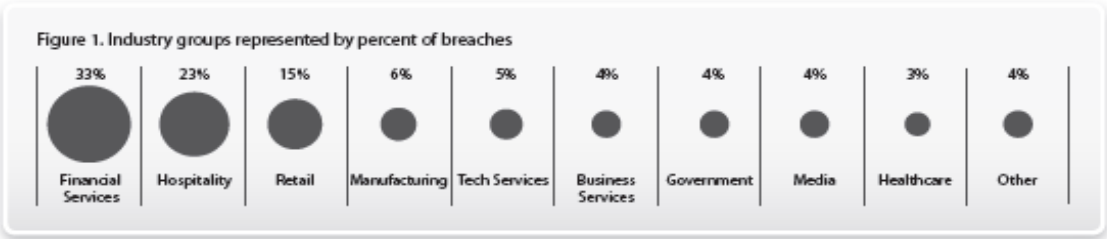
- Handel
  - PCI Compliance
  - Preismanipulationen (IT Mitarbeiter manipulieren Preis)

- Gesundheitswesen
  - Patientenschutz (insbes. von Prominenten)
  - Forschungs- und Patentschutz

- Öffentliche Auftraggeber
  - Schutz der Bürgerdaten
  - innere und äußere Sicherheit

- Telekommunikation
  - Call Data Records werden multipel verwendet
  - Vorratsdatenspeicherung

- Industrie-übergreifend
  - Finanzdaten
  - HR Daten
  - Unternehmensstrategien
  - Compliance



Quelle: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

Ergebnisse Data Breach Report des Verizon RISK Team (2010)

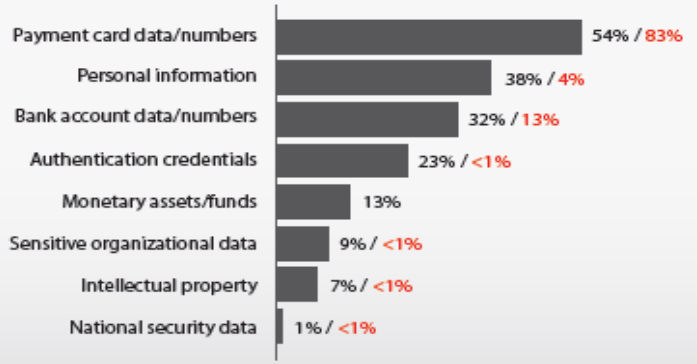
- 92% der mißbrauchten Datensätze kamen von Datenbankservern
- Kreditkarten Daten machen 83% aller attackierten Daten aus

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	
Documents	Offline Data	7%	
POS terminal	End-User Devices	6%	
File server	Servers & Applications	4%	
Automated Teller Machine (ATM)	End-User Devices	4%	
FTP server	Servers & Applications	2%	
Mail server	Servers & Applications	2%	
Customer (B2C)	People	2%	
Regular employee/end-user	People	2%	

* Only assets

Figure 31. Compromised data types by percent of breaches and percent of records



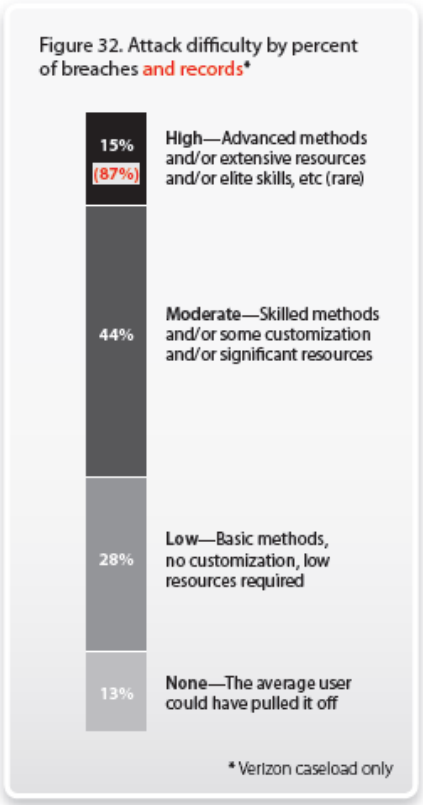
Nr. 1 Ursache aller veruntreuten Datensätze ist SQL Injection

- Über Cross-site Scripting 9% aller Hacks
- 11% aller Hacks über zu einfache oder Default Credentials
- Weiterer Top-Punkt: gestohlene Login Credentials

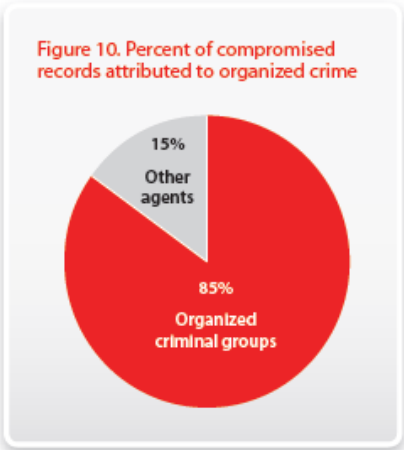
Weitere Erkenntnisse

	HOW DO BREACHES OCCUR?
Related to the larger proportion of insiders, Misuse sits atop the list of threat actions leading to breaches in 2009. That's not to say that Hacking and Malware have gone the way of the dinosaurs; they ranked #2 and #3 and were responsible for over 95% of all data comprised. Weak or stolen credentials, SQL injection, and data-capturing, customized malware continue to plague organizations trying to protect information assets. Cases involving the use of social tactics more than doubled and physical attacks like theft, tampering, and surveillance ticked up several notches.	48% involved privilege misuse (+26%)
	40% resulted from hacking (-24%)
	38% utilized malware (<>)
	28% employed social tactics (+16%)
	15% comprised physical attacks (+6%)

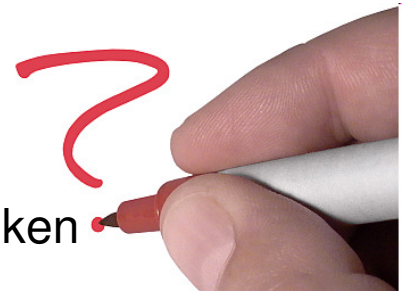
Der Missbrauch von privilegierten Nutzungsrechten sowie Hacking sind bevorzugte Wege an Daten zu kommen.



87% der Angriffe wurden über sehr fortschrittliche Methoden ausgeführt, 85% durch organisierte Kriminelle.



Sind Ihre Daten sicher ?



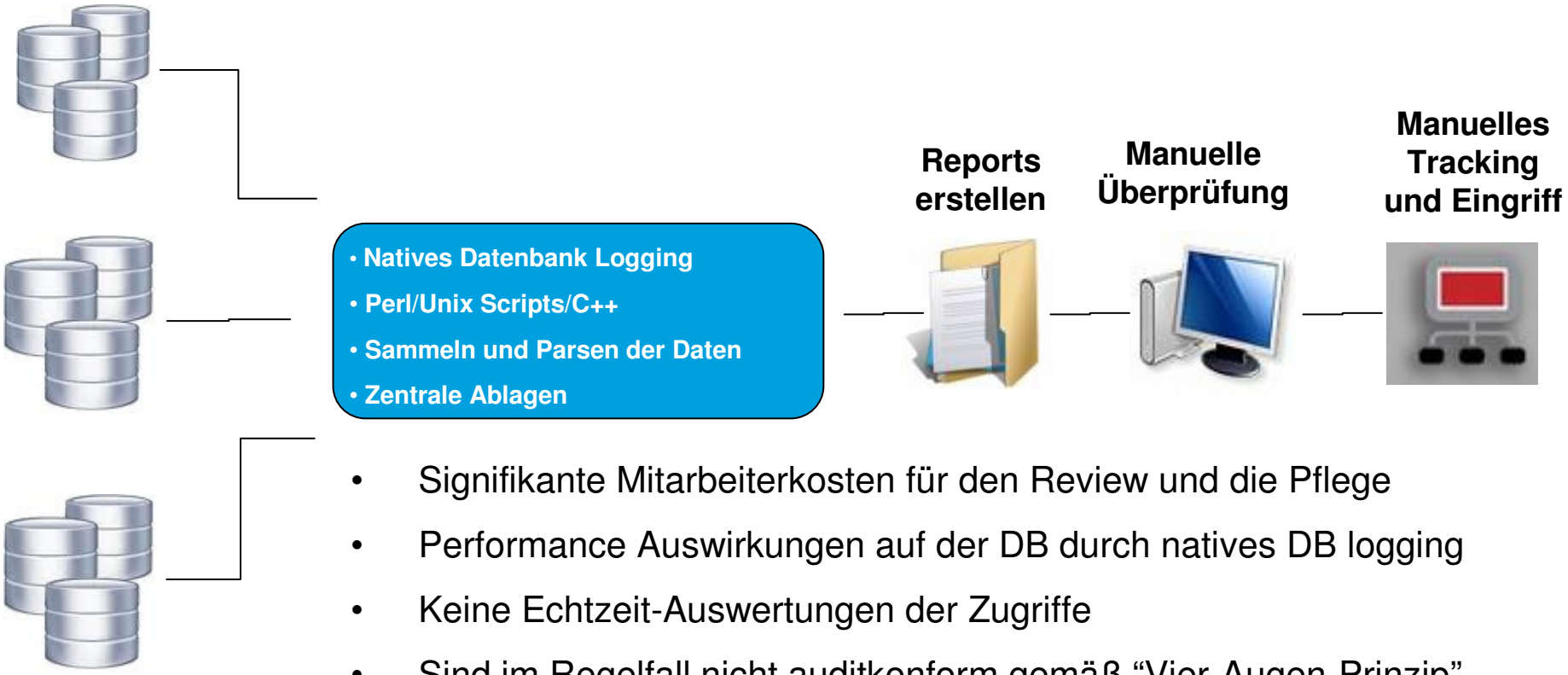
- Wie kann ich identifizieren und sicherstellen, ob meine Datenbanken sicher *konfiguriert* und kritische *Patches* eingespielt sind?

- Wo befinden sich unsere sensiblen Daten und wie vermeide ich, dass Dienstleister sensible Informationen sehen können?

- Wie können wir sicherstellen und überwachen, dass DBAs und andere privilegierte Nutzer ihre Zugriffsrechte nicht missbrauchen?

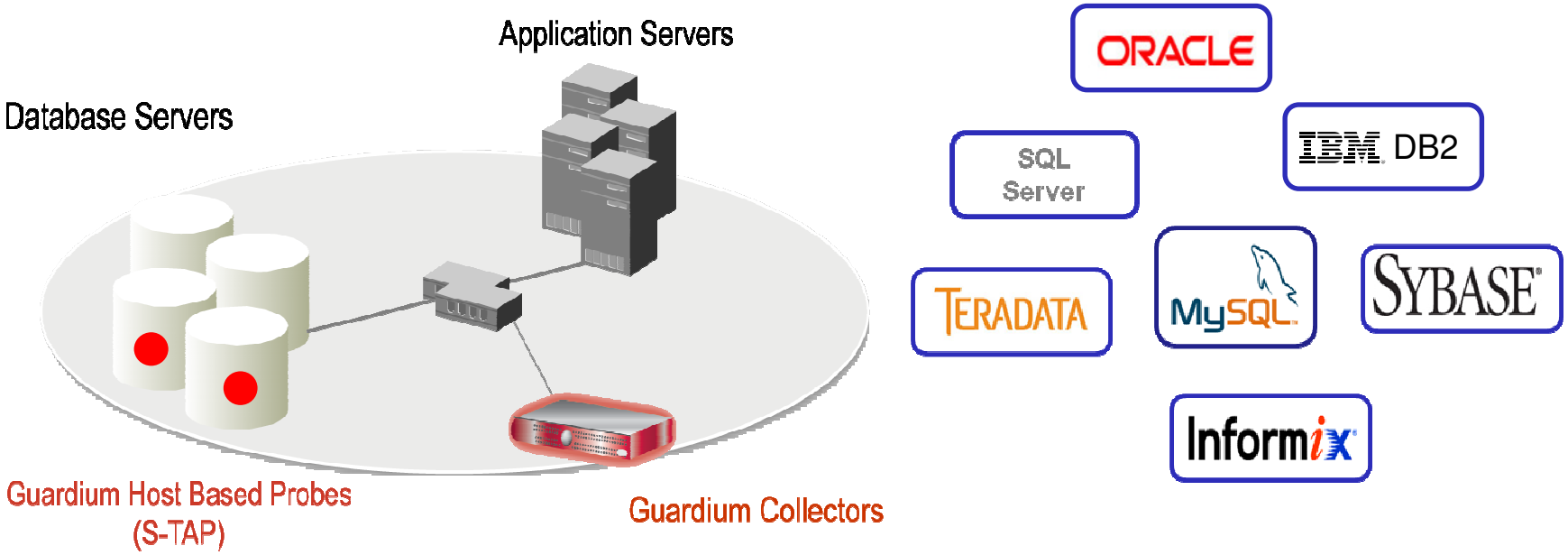
- Wie können wir in Echtzeit feststellen, wenn z.B.
  - Mehr als 3 fehlgeschlagene Loginversuche auftreten?
  - Jemand unautorisiert eine sicherheitsrelevante Tabelle z.B. in SAP ändert?
  - Verdächtige Zugriffe aus dem Anwendungsserver-Account auftreten?

Bisher verfügbare Lösungen sind teuer und arbeitsintensiv



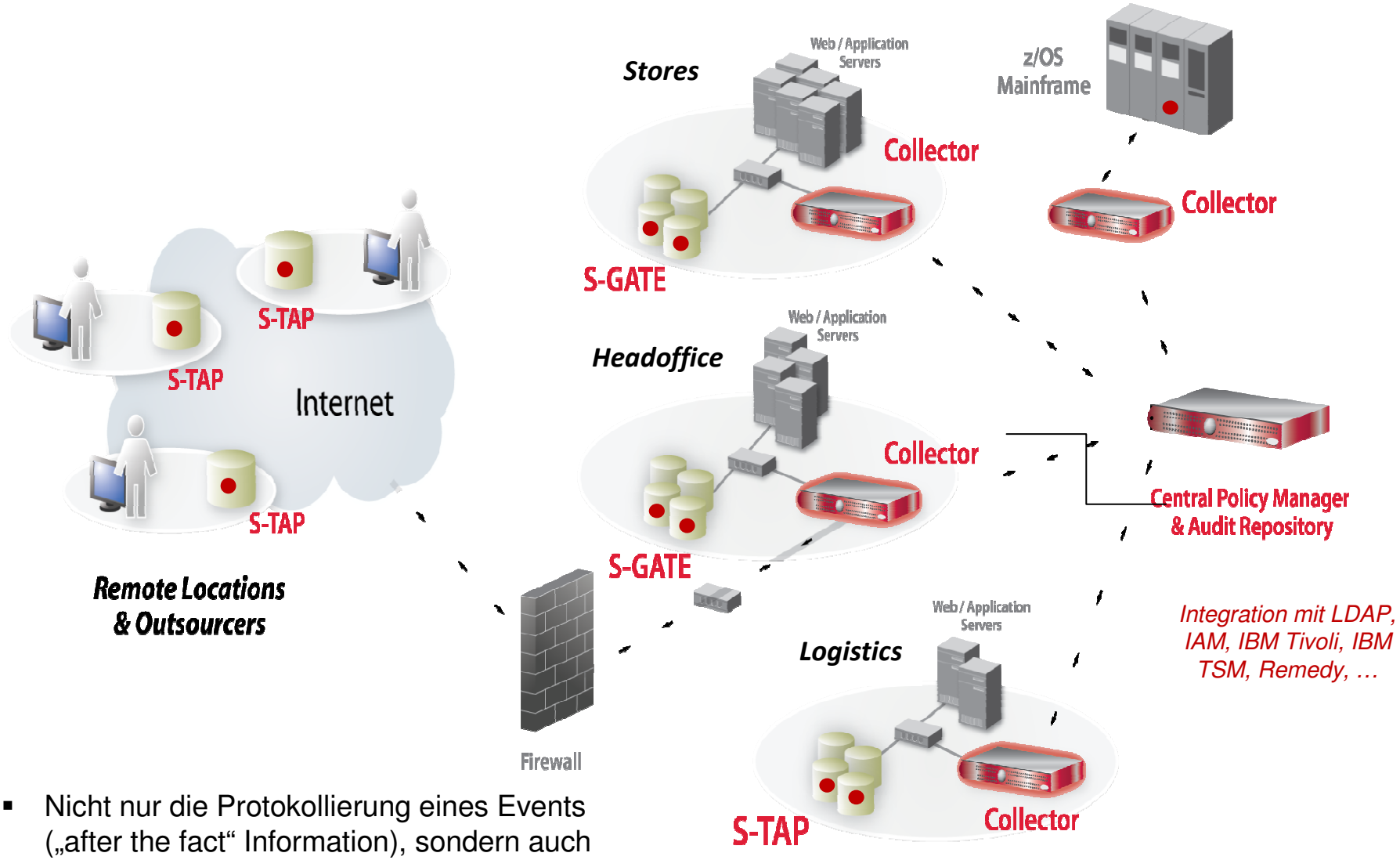
- Signifikante Mitarbeiterkosten für den Review und die Pflege
- Performance Auswirkungen auf der DB durch natives DB logging
- Keine Echtzeit-Auswertungen der Zugriffe
- Sind im Regelfall nicht auditkonform gemäß "Vier-Augen-Prinzip" (Separation of Duties)
- Der Audit-Trail ist vor Manipulationen nicht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

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.)

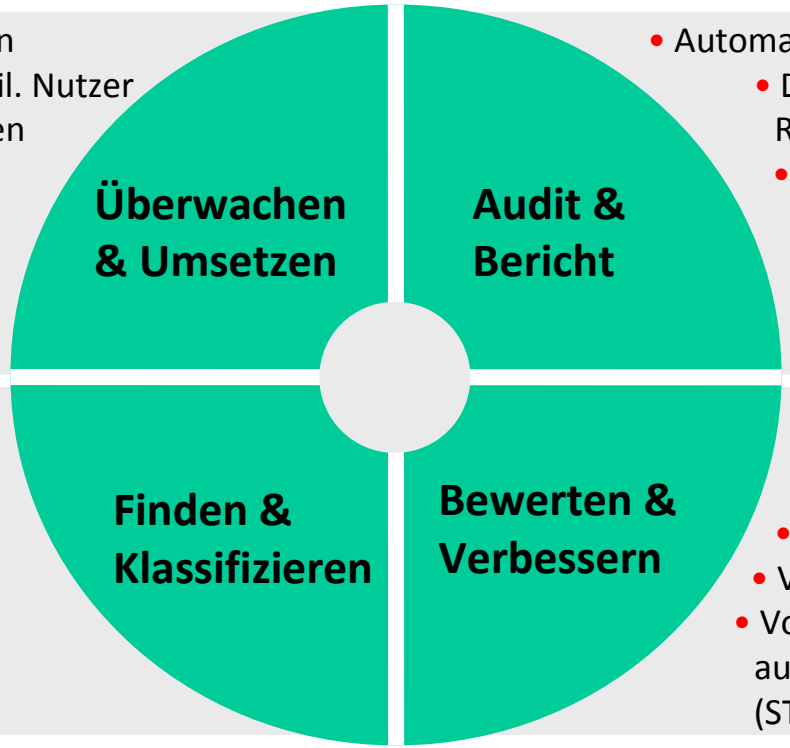
Skalierbare Multi-Tier Architektur



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

Guardium 8 - Funktionsübersicht

- Verhindern von Cyber-Attacken
- Überwachen & Blockieren privil. Nutzer
- Erkennen von Betrugsversuchen über die Anwendungsschicht
- Änderungskontrollen
- Real-time Alerts
- Forensische Datenanalyse
- SIEM Integration



- Automatisierte & zentralisierte Kontrollen
- Datenbankübergreifendes Audit-Repository
- Vorkonfigurierte Regeln/ Berichte
- Sign-off Verwaltung
- Archivierung (Retention)
- Keine Datenbankänderungen
- Keine Beeinflussung der Laufzeit

- Aufinden & Klassifizieren sensiblen Daten
- Kontinuierliche Aktualisierung der Regeln
- Erkennen von Schadsoftware

- Festellen von DB Schwachstellen (VA)
- Auditing von DB Konfigurationen
- Verhaltensbasierte Schwachstellen
- Vorkonfigurierte Tests basierend auf Best Practices & Standards (STIG, CIS)

Alle gängigen Plattformen & Anwendungen werden unterstützt

Unterstützte Plattform Platform	Unterstützte Versionen
Oracle	8i, 9i, 10g (r1, r2), 11g, 11gR2
Oracle Database (ASO ,SSL)	9i, 10g (r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, z/Linux)	9.1, 9.5, 9.7
IBM DB2 (Windows)	9.1, 9.2, 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
Sun MySQL und MySQL Cluster	4.1, 5.0, 5.1
Sybase ASE	12, 15, 15.5
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.x, 12, 13
FTP	unterstützt Netzwerk-Monitoring, und die Überwachung lokaler Aktivitäten via Enterprise Integrator

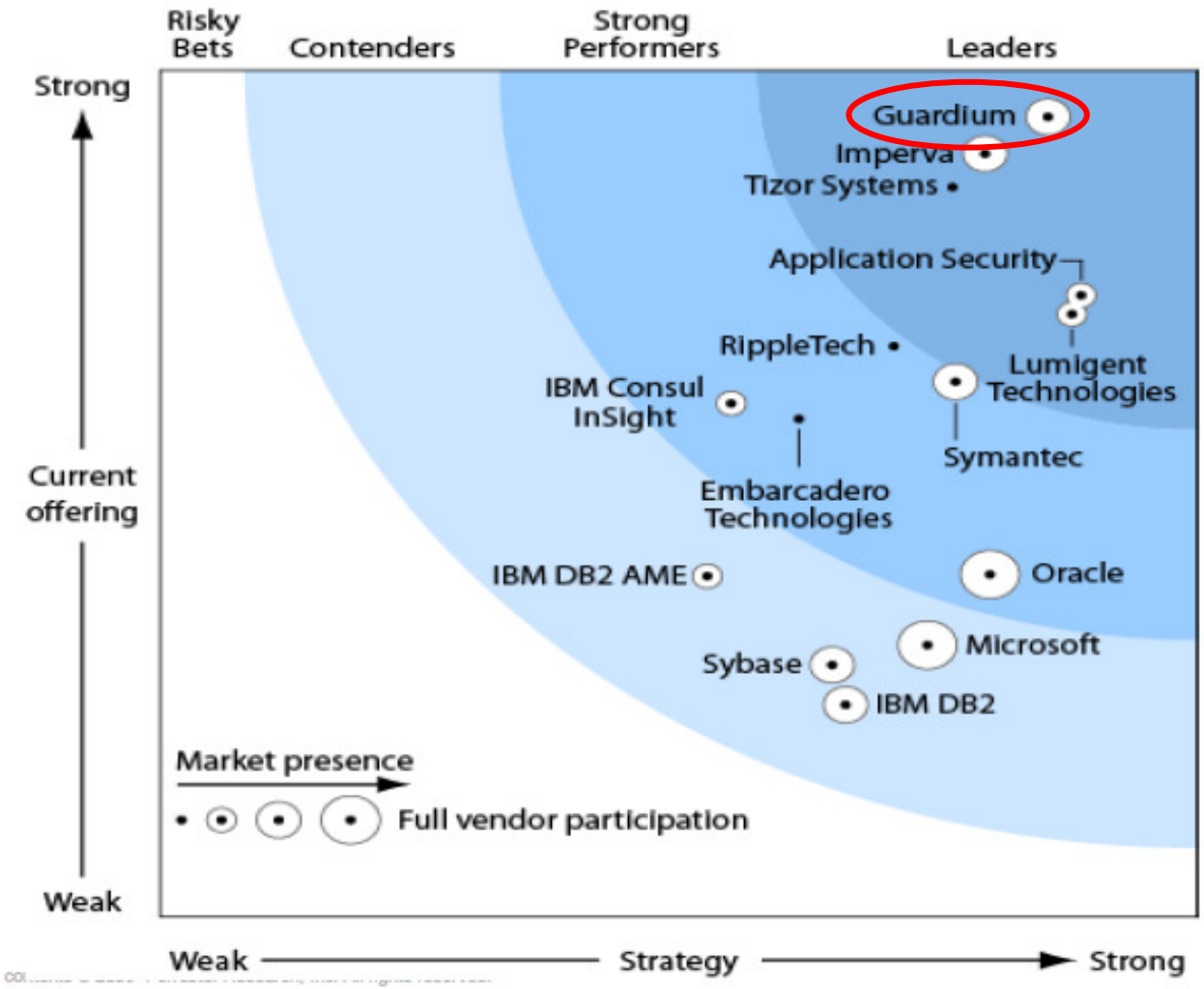
Betriebssystem	Version	32-Bit und 64-Bit
AIX	5.1, 5.2, 5.3	Beides
	6.1	64-Bit
HP-UX	11.00, 11.11, 11.23, 11.31	Beides
Red Hat Enterprise Linux	3, 4, 5	Beides
Red Hat Enterprise Linux for System z	5.4	
SUSE Enterprise Linux	9, 10, 11	Beides
SUSE Enterprise Linux For System z	9, 10, 11	
Solaris – SPARC	8, 9, 10	Beides
Solaris – Intel/AMD	10	Beides
Tru64	5.1A, 5.1B	64-Bit
Windows	2000, 2003, 2008	Beides
iSeries	i5/OS*	

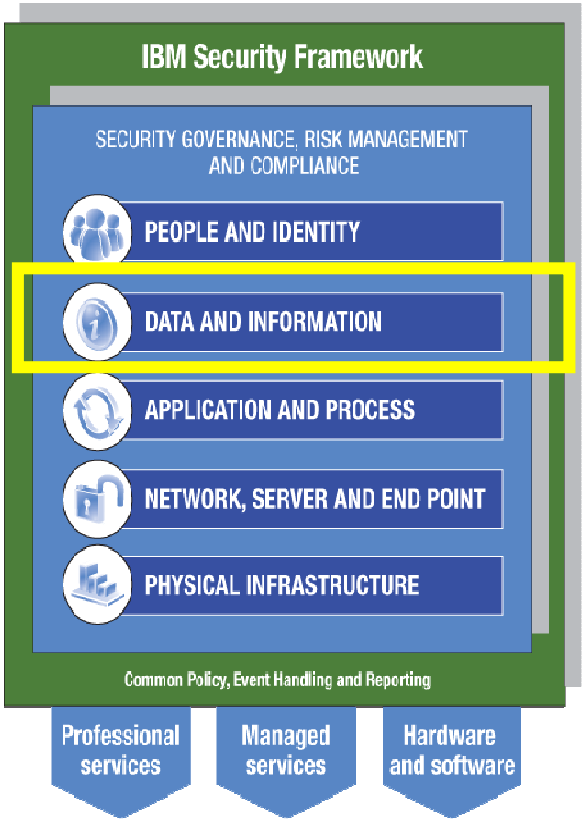
Unterstützte Unternehmensanwendungen	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
Unterstützte Anwendungs-server-plattformen	• IBM WebSphere • BEA WebLogic • Oracle Application Server (AS) • JBoss Enterprise Application Platform

Datenbank Sicherheit in Compliance Regularien

Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
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)	✓	✓	✓	✓	✓

InfoSphere Guardium ist führend im Database Security Markt





FORRESTER

Analysten- und Experten-Bewertungen

FORRESTER®

"Dominance in this space"
#1 Scores for Current Offering, Corporate & Product Strategy

INFORMATION SECURITY MAGAZINE

"Enterprise-class data security product that should be on every organization's radar."

SC MAGAZINE AWARDS 2008 FINALIST Honored in the U.S.

SC MAGAZINE

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security."

InformationWeek

"Top of DBEP Class"
"Practically every feature you'll need to lock down sensitive data."

INFORMATION SECURITY Hotpick

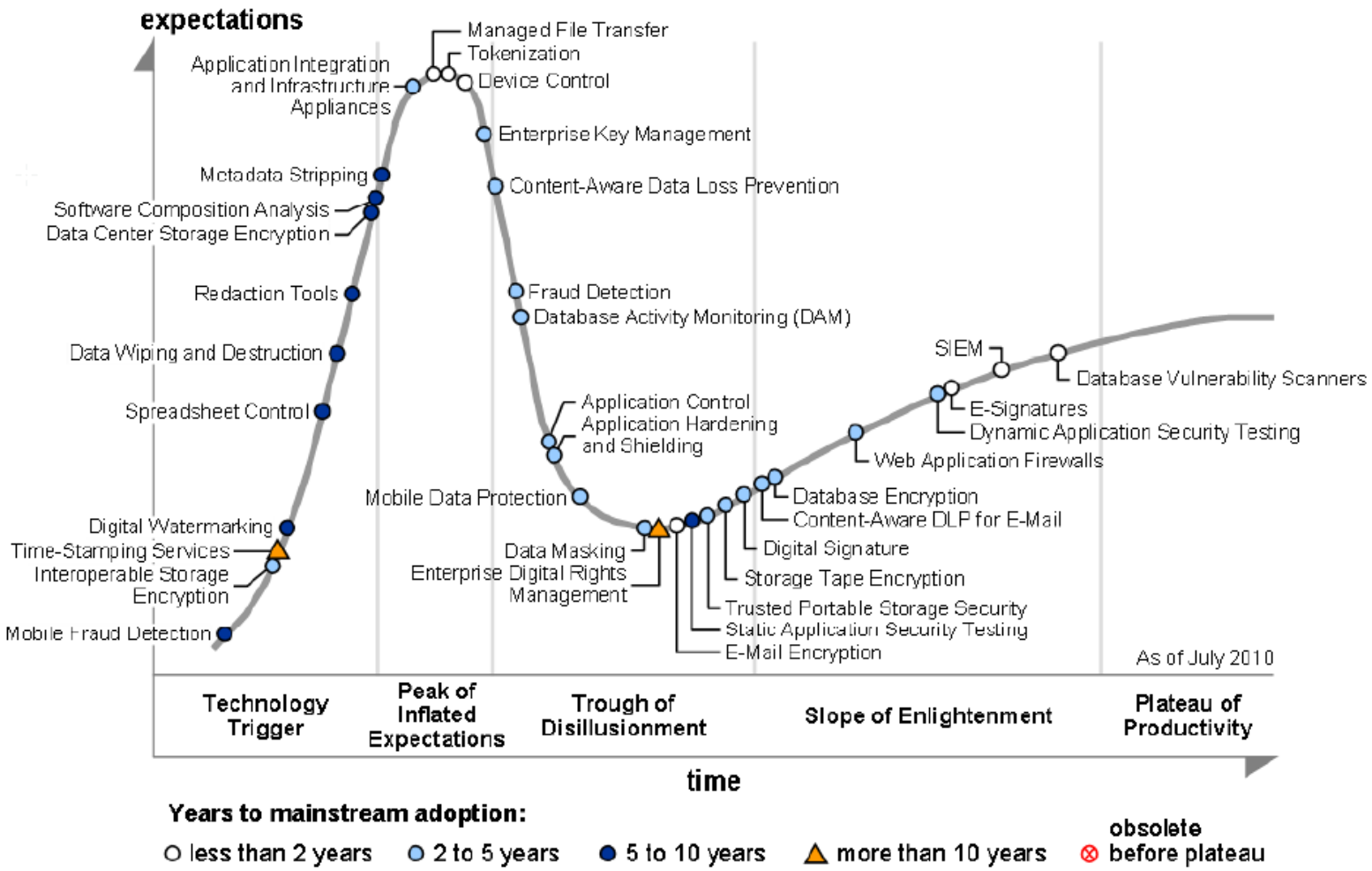
BANK TECHNOLOGY NEWS btn

"One of 10 technology companies to watch"

RED HERRING N. AMERICA WINNER 100

Gartner Hype Cycle

Figure 1. Hype Cycle for Data and Application Security, 2010



Source: Gartner (July 2010)

*Gartner, **Hype Cycle for Data and Application Security, 2010 (ID Number: G00201373**)

CASE STUDY:
SECURITY SOLUTIONS

HOW THE GUARDIUM PLATFORM HELPED DELL IT SIMPLIFY ENTERPRISE SECURITY

By Phil Neray
Addison Lawrence
David McMaster
Venugopal Nonavinakere

Safeguarding data is critical for many organizations, but auditing data access activity to comply with regulatory standards can be a complex undertaking. As part of its initiative to simplify IT, the Dell IT group implemented the Guardium platform and database activity monitoring technology to help protect its globally distributed database servers and streamline compliance processes.

Securely maintaining sensitive financial and customer information in enterprise data centers can be complex and challenging, and the heterogeneous global environment that stores enterprise data for Dell is no exception. The Dell IT infrastructure includes thousands of servers worldwide that run a diverse mix of enterprise applications such as Oracle® E-Business Suite, Oracle JD Edwards®, and Oracle Hyperion software as well as the Oracle Database and Microsoft® SQL Server® database platdesk—helps to ensure that a formal process is in place for tracking and addressing exceptions such as failed logins and unauthorized changes to database structures (schema modifications) through Data Definition Language (DDL) operations.[1]

Dell IT administrators are continually looking for new and innovative ways to safeguard critical data in these systems from both external and internal threats, including inadvertent or accidental changes that can affect the integrity of financial data governed

Guardium®

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Guardium Secures SAP and Siebel Data for F500 Global Consumer Products Manufacturer, Achieving 239% ROI

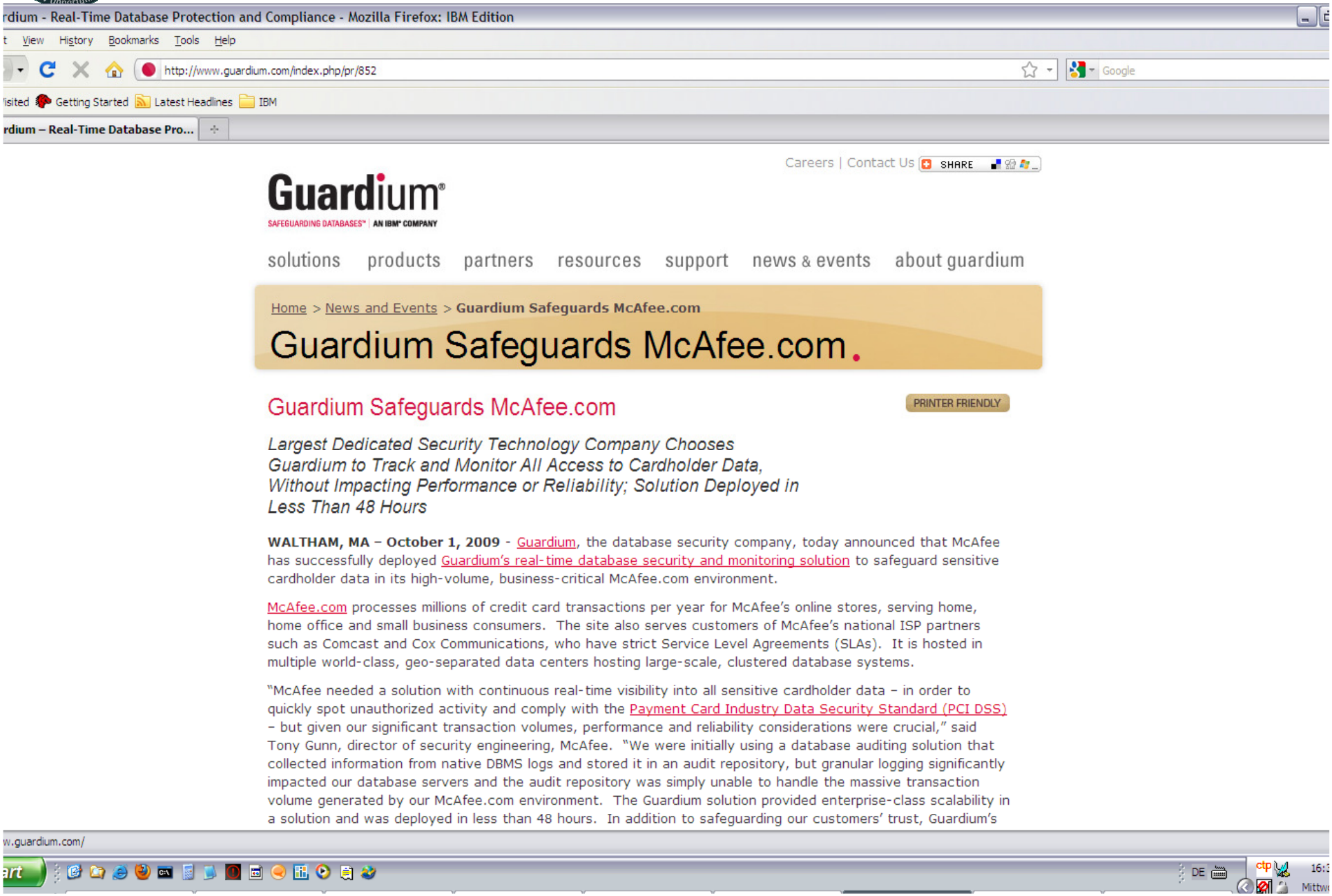
Guardium Database Monitoring and Security Solution Automates SOX Controls and Prevents Unauthorized Changes to Critical Databases, According to Case Study by Leading Analyst Firm

A commissioned case study by Forrester Consulting describing how a global manufacturer implemented Guardium's real-time monitoring technology to protect corporate data and enforce change controls for critical databases supporting SAP, Siebel and 22 other key financial systems. The detailed case study is now available at www.guardium.com/ForresterROI.

The customer is a Fortune 500 consumer food and beverage manufacturer whose brands are household names around the world. According to Forrester, the Guardium solution delivered a risk-adjusted ROI of 239 percent and payback period of less than 6 months compared to the "significant labor and capital costs" that would have otherwise been required using an in-house solution and traditional database logging utilities.

Proactive Security

In addition to economic benefits, the study found that Guardium "helps customers rapidly identify and proactively address security policy incidents." For example, the system's real-time alerting addresses a business requirement to immediately inform decision-makers of changes to certain database tables. The study adds that "an in-house solution would not have provided the real-time security controls provided by the Guardium product."



rdium - Real-Time Database Protection and Compliance - Mozilla Firefox: IBM Edition

t View History Bookmarks Tools Help

http://www.guardium.com/index.php/pr/852

Google

isited Getting Started Latest Headlines IBM

rdium – Real-Time Database Pro...

Careers | Contact Us SHARE

Guardium®

SAFEGUARDING DATABASES™ | AN IBM® COMPANY

solutions products partners resources support news & events about guardium

Home > News and Events > Guardium Safeguards McAfee.com

Guardium Safeguards McAfee.com.

Guardium Safeguards McAfee.com

PRINTER FRIENDLY

Largest Dedicated Security Technology Company Chooses Guardium to Track and Monitor All Access to Cardholder Data, Without Impacting Performance or Reliability; Solution Deployed in Less Than 48 Hours

WALTHAM, MA – October 1, 2009 - Guardium, the database security company, today announced that McAfee has successfully deployed Guardium's real-time database security and monitoring solution to safeguard sensitive cardholder data in its high-volume, business-critical McAfee.com environment.

McAfee.com processes millions of credit card transactions per year for McAfee's online stores, serving home, home office and small business consumers. The site also serves customers of McAfee's national ISP partners such as Comcast and Cox Communications, who have strict Service Level Agreements (SLAs). It is hosted in multiple world-class, geo-separated data centers hosting large-scale, clustered database systems.

"McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with the Payment Card Industry Data Security Standard (PCI DSS) – but given our significant transaction volumes, performance and reliability considerations were crucial," said Tony Gunn, director of security engineering, McAfee. "We were initially using a database auditing solution that collected information from native DBMS logs and stored it in an audit repository, but granular logging significantly impacted our database servers and the audit repository was simply unable to handle the massive transaction volume generated by our McAfee.com environment. The Guardium solution provided enterprise-class scalability in a solution and was deployed in less than 48 hours. In addition to safeguarding our customers' trust, Guardium's

w.guardium.com/

art DE

IBM Information On Demand 2010

Create Insight. Transform. Go Beyond.

Database Monitoring for Enterprise-Wide PCI and Data Privacy Compliance: Vodafone's Experience

vodafone

Corradino Corradi
Manager, ICT Security and Privacy
Vodafone Italy
Roma, May 19, 2010

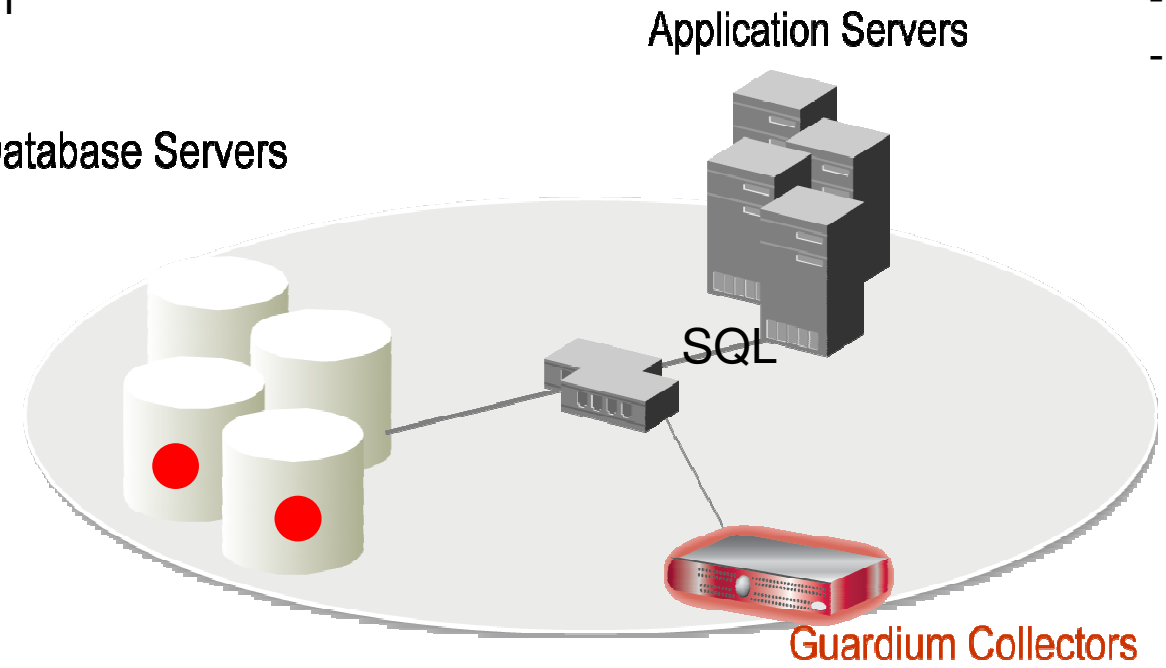
Zusammenfassung

Sicherheit

- proaktiv
- umfänglich
- SOD
- ...

Kosten

- Serverkosten
- Storagekosten
- Compliancekosten



Flexibilität

- fast alle Datenbanken
- jede gängige Middleware
- viele Applikationen

Akzeptanz

- bei IT
- im Business
- im Management

Q&A

Patrick Würl
Guardium Regional Sales Manager

Mobile 0151 1082 1388
Email patrick.wuerl@de.ibm.com

Thank you !