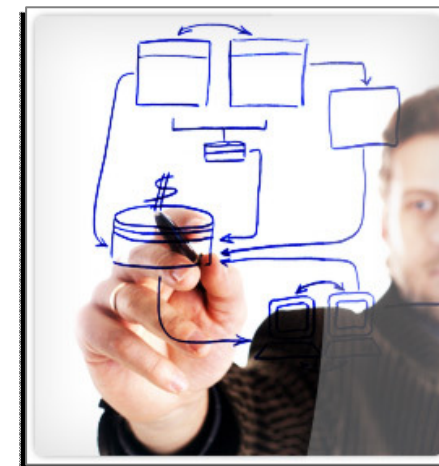


Cómo Proteger la Seguridad y la Privacidad de los Datos de Manera Inteligente



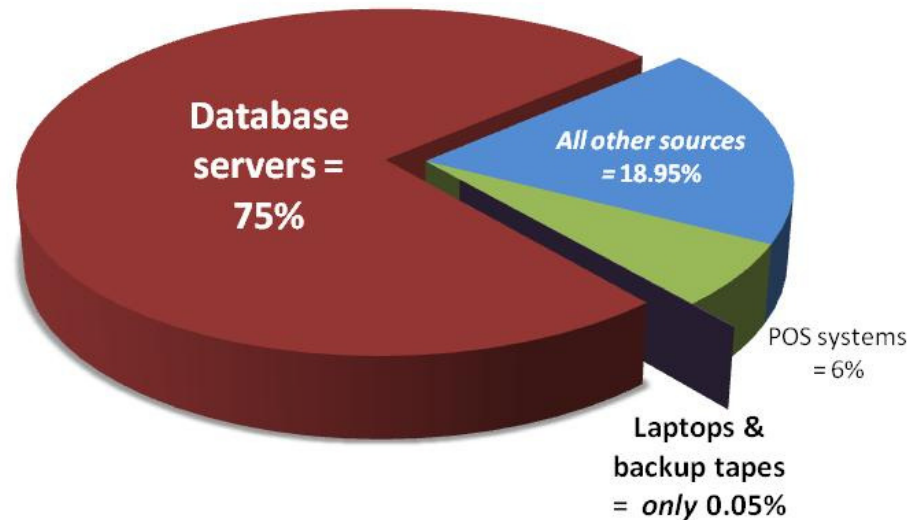
Phil Neray,
Vice-President of Data Security
IBM Data Governance

22 de Septiembre
TORRE ESPACIO
Madrid



Database Servers Are The Primary Source of Breached Data

% of Records Breached (2009)



2009 Data Breach Report from Verizon Business RISK Team

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

“Although much angst and security funding is given to **mobile devices and end-user systems**, these assets are simply not a major point of compromise.”

Perimeter Defenses No Longer Sufficient

“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”

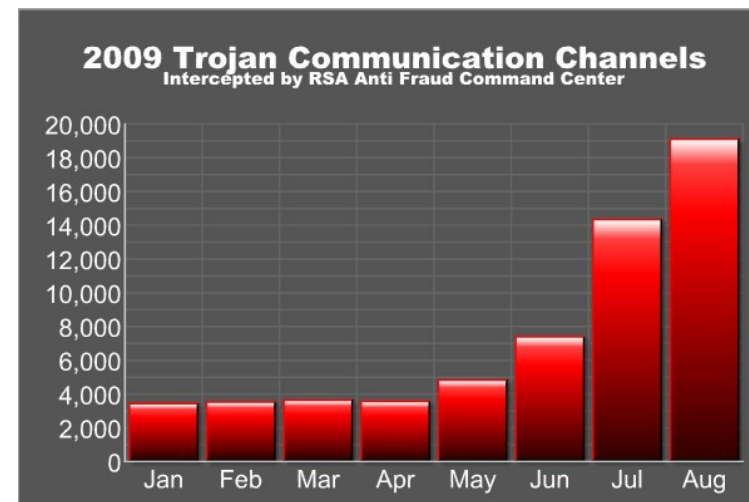
- William J. Lynn III,
U.S. Deputy Defense Secretary



Battlefield Moves from Networks to Employee PCs

- Nearly all F500 companies affected
 - Corporate credentials already in wrong hands
- Kneber Botnet example (*source: NetWitness*)
 - 68,000 credentials stolen
 - 75,000 PCs owned
 - 2,411 organizations penetrated
 - 196 countries
- Commercial-grade “crimeware”
 - QA team
 - Documentation
 - Phone support
 - License keys
 - \$4K + add-ons up to \$10K
 - *Re-encrypts each install*

- **Relying on IAM alone is no longer sufficient**



CP :: Summary statistics

Information	
Current user:	root
GMT date:	12.07.2009
GMT time:	11:35:10

Statistics:	
→ Summary	
OS	

Botnet:	
Bots	
Scripts	

Reports:	
Search in database	
Search in files	

System:	
Information	
Options	

Information	
Total reports in database:	11 590 693
Time of first activity:	12.06.2009 13:12:47
Total bots:	36 638
Total active bots in 24 hours:	16.46% - 6 032
Minimal version of bot:	1.2.5.1
Maximal version of bot:	1.2.5.1

Botnet: [All] >>

Actions: Reset Installs

Installs (1 665)		Online (2 122)	
US	609	US	634
RU	253	RU	427
IN	127	IN	88
MA	57	UA	84
PE	53	RO	67

Qué es?



FEATURES

Hackers Gone Wild

Sex! Drugs! Software code!
How three young computer
geeks went gangster and
pulled off the biggest
cybercrime of all time.

By Sabrina Rubin Erdely... 64



Rolling Stone



Operation Get Rich began in Miami. Hackers recruited by Albert would drive up and down U.S. 1, a busy artery of strip malls and traffic lights, with their laptops open, searching for retail stores with open wireless networks, a technique called "wardriving." When they found an open network, they would park in a nearby lot or rent a hotel room close by and swiftly hack into the store's payment database. Then they would bide their time. From that point on, each time the store swiped a card, the hackers could capture its data and send it on to Albert. Albert

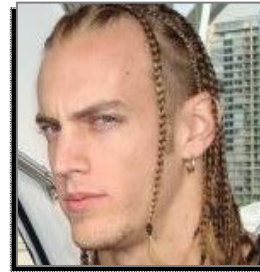


Maksym Yastremskiy

then transfer the data onto servers that Patrick had set up in Latvia, Singapore, China and Ukraine, where associates Albert had recruited online would use the information to drain bank accounts and ATMs worldwide. By late 2005, the money being FedExed to Albert's drop box in Miami was arriving in stacks of up to \$370,000. Operation Get Rich was paying off.

about getting the cash. So Albert enlisted the services of Maksym Yastremskiy, a 22-year-old Ukrainian cybercrime lord. ("The card 'dumps' are all run by Russians," says Patrick, "so they have the most clientele.") Yastremskiy arranged to have the payment data encoded onto bank cards, which were then sold at nightclubs all over the world for \$300 a pop, of which Albert got half. To launder the money before wiring it to Miami, Albert used the offshore Internet-based payment systems WebMoney and E-gold. He had

Operation Get Rich or Die Tryin'



Stephen Watt, author of "blabla" sniffer: 2 years in prison & \$170M in restitution



"Maksik" Yastremskiy: 30 years in Turkish prison

- Gonzalez sentenced to 20 years ("Largest Hacking Case Ever Prosecuted")
- Heartland, 7-Eleven, Hannaford: Stole 130M cards via SQL injection, network reconnaissance, malware, sniffers
- Dave & Buster's Restaurants: Stole admin password file from POS service provider
- TJX, OfficeMax + 6 other retailers: Stole 40M cards via SQL injection & war driving
- San Diego case: International ring (Ukraine, Estonia, PRC, Philippines, Thailand)
 - "Maksik" Yastremskiy earned \$11 million from stolen credit cards
 - Hacked 11 Turkish banks; sentenced to 30 years in Turkish prison
- ***"Our most formidable challenge is getting companies to detect they have been compromised ..."*** Kimberly Kiefer Peretti, senior counsel, DoJ



From Latvia to Amsterdam (to Montana)

- 192,000 records stolen from broker-dealer in Montana
- Online extortion scheme by Latvians in Netherlands
- Used SQL injection to compromise database
 - Default blank password
 - Never reviewed logs
 - Only alerted to breach by extortion email
- Company fined \$375,000 by regulators (FINRA)
- FBI-USSS Advisory (Feb. 2009)
 - Disable harmful stored procedure calls
 - Require password for “sa” account
 - “Attackers generally create tables into which they store malware or data collected from the enterprise ... Restrict the capabilities of accounts used to modify databases.”

http://usa.visa.com/download/merchants/20090212-ussf_fbi_advisory.pdf



UNITED STATES OF AMERICA,
 Plaintiff,
 vs.
 JOHN DOE, *aka Robert Borko*,
 ALEKSANDRS HOHOLKO,
 JEVGENIJS KUZMENKO, and
 VITALIJS DROZDOVS,
 Defendants.

MICHAEL S. LAHR
 Assistant U.S. Attorney
 U.S. Attorney's Office
 301 Front Street, Suite 1100
 Helena, MT 59626
 Phone: (406) 457-5270
 FAX: (406) 457-5130
 ATTORNEY FOR PLAINTIFF
 UNITED STATES OF AMERICA

"I have news from people working in Western Union: they are increasing measures against money laundering (sic) now, many transfers are being (sic) locked as suspicious. That was the reason of our problems in Netherlands. So, we can't use WU now - it becomes very unreliable."

Real-World Insider Threat Examples



- Unauthorized changes to financial/ERP data
 - DBA accidentally deleted critical financial table during production hours (was doing a favor for application developer, bypassing change process)
 - Outsourcer erased logs showing he made changes during the day (because it was more convenient than during the night)
- Theft of sensitive data
 - Departing employees stealing design information & other intellectual property
 - DBAs and outsourcers selling customer information to competitors, crime syndicates and tax authorities
- Internal fraud
 - Mortgage processor: Insider changed credit scores to make loans look better
 - Mobile telecom: Insider created & sold pre-paid phone cards
 - Electric utility: Insider gave free service to friends and family as part of low-income assistance program
 - Health provider: Insider sold medical identities for insurance fraud

An Insider Tale



- Certegy – public company (Jacksonville, Fla.)
 - Check authorization & check cashing services
- Senior DBA sold 8.5 million customer records to data broker
 - Names, addresses, birth dates, bank account & credit card info – was paid \$580K
- Data theft came to light after retailer reported correlation between transactions and receipt of external marketing offers by its customers
 - U.S. Secret Service found data came from separate company owned by Certegy DBA
 - “Why did it take Certegy more than five years to find out that confidential consumer information was being sucked out of its database?” (*St. Petersburg Times*)
- Settled class-action suit for \$4 million
 - Plus \$975,000 in fines from Attorney General
 - Plus mandatory security audit every year
 - Plus 2 years of credit monitoring services (\$180 per customer)
- Rogue DBA sentenced to nearly 6 years in prison

Cost of a Data Breach

- Forrester survey of 305 IT decision makers
- Secrets (e.g., strategic plans) are twice as valuable as custodial data (personal information, credit card data, etc.)
 - 2/3 of value in corporate information portfolio from non-regulated data (secrets)
- Companies focus mainly on preventing accidents (email, etc.)
 - But deliberate theft of information by employees is much more costly
 - Damage caused by rogue IT administrator = \$482K (average)
 - Average cost of accidental leakage = \$12K
- Most CISOs don't really know if their controls really work
- Note: Survey does not address other costs such as fines
 - Australian bank was fined \$500K by VISA
 - Heartland breach cost = \$140M

A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC

The Value Of Corporate Secrets

How Compliance And Collaboration Affect Enterprise Perceptions Of Risk

March 2010

Key Business Drivers for Database Activity Monitoring (DAM)

Continuously Monitor All Access to Sensitive Data:

1. Prevent data breaches

- Cybercriminals & rogue insiders
- Protect customer data & corporate secrets (IP)



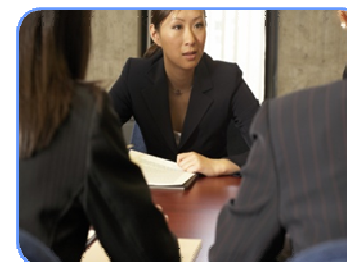
2. Assure data governance

- Prevent unauthorized changes to sensitive data by privileged users

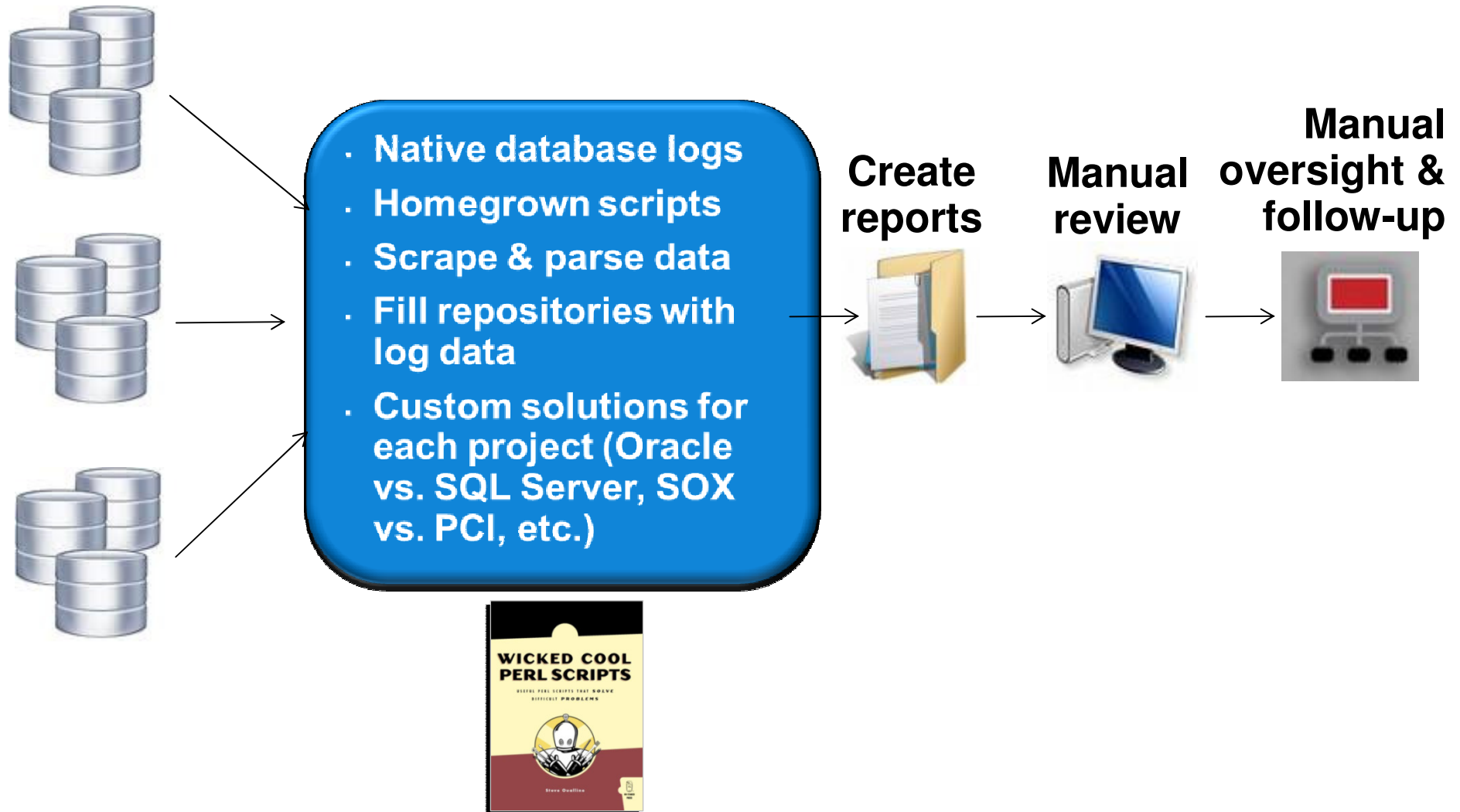


3. Reduce audit costs

- Automated, continuous controls
- Simplified processes



What Database Audit Tools are Enterprises Using Today?

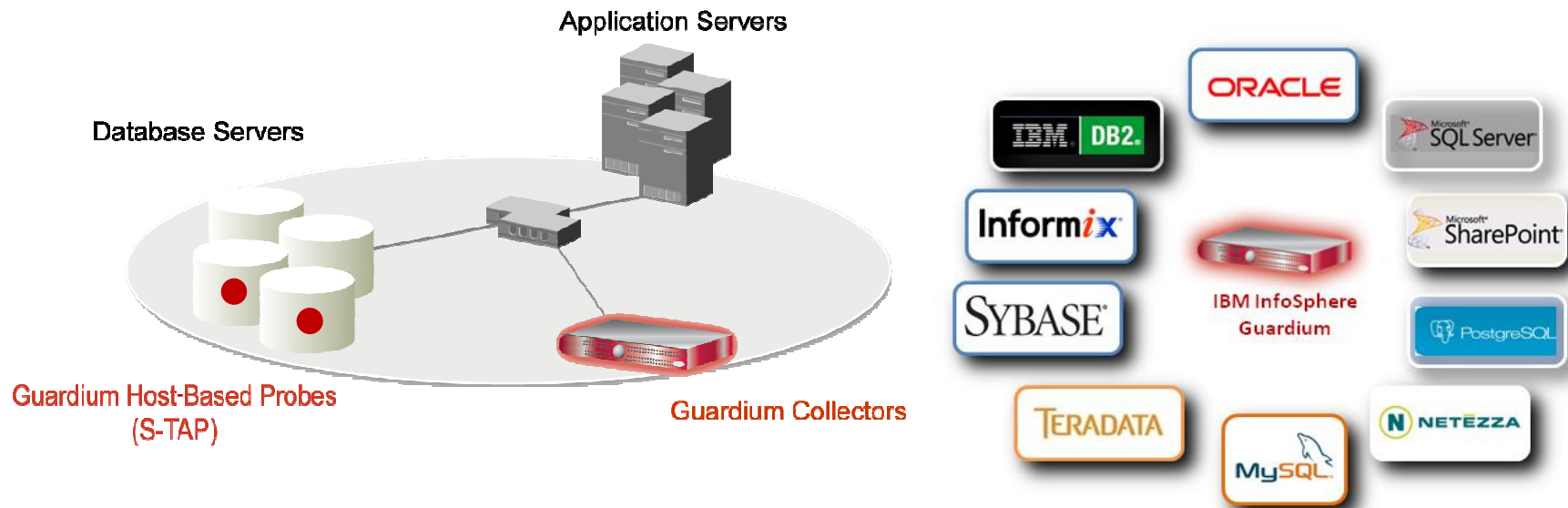


What Are the Challenges with Current Approaches?



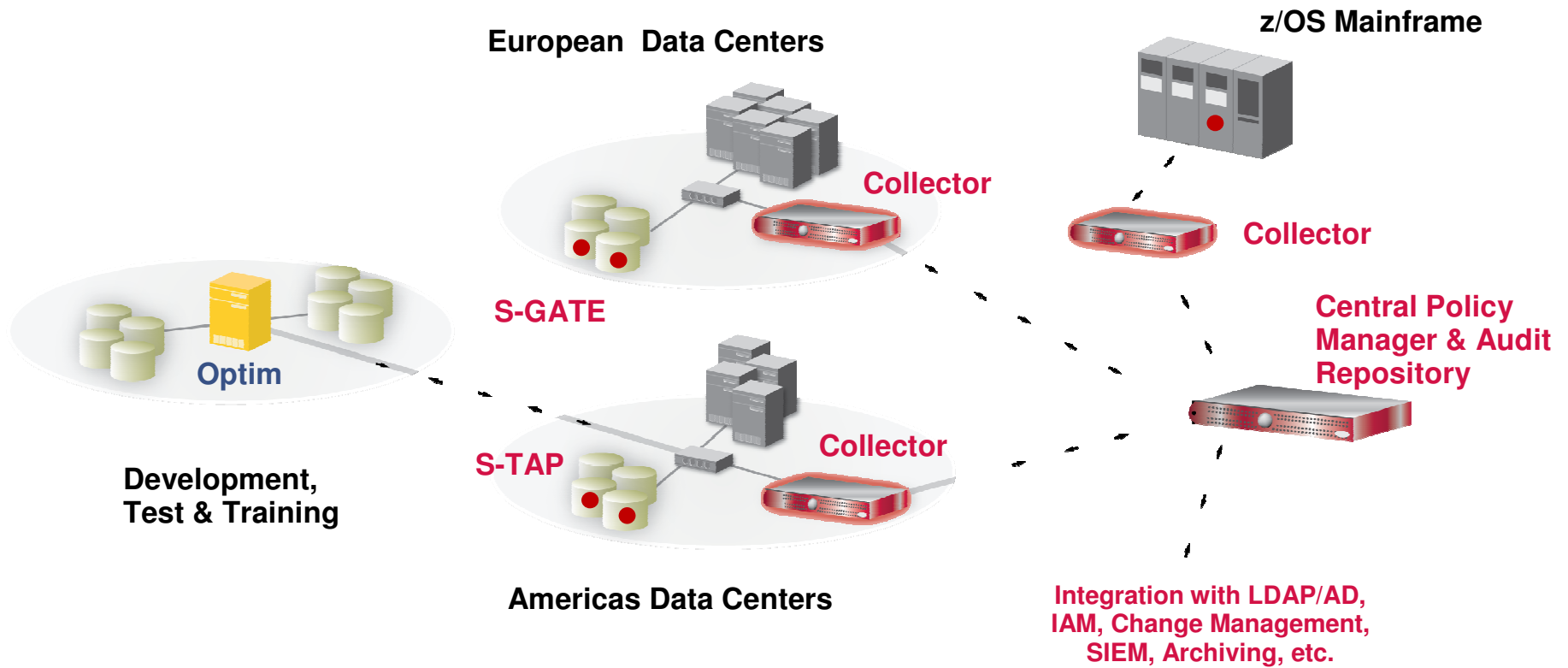
- No separation of duties -- DBAs & hackers can easily modify logs
- Performance impact of native logging on the DBMS
- Limited scope & granularity of log data
- Not real-time
- No preventive controls
- Another data store to secure and manage (\$\$\$)
- Inconsistent policies across applications, DBMS platforms, compliance initiatives
- Can't identify end-user fraud for connection-pooled applications that use generic service accounts (SAP, PeopleSoft, etc.)
- Lack of DBMS expertise on security teams
- Significant labor cost to clean & review data, maintain processes

Non-Invasive, Real-Time Database Security & Monitoring

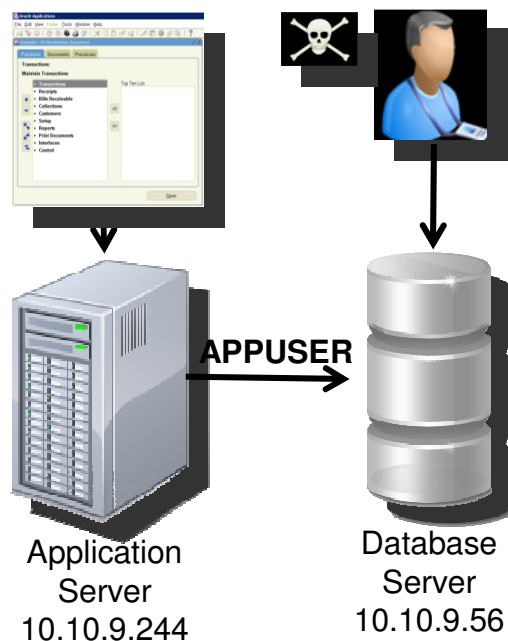


- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS logs
- Minimal performance impact (2-3%)
- No DBMS or application changes
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
 - *Who, what, when, where, how*

Scalable Multi-Tier Architecture



Granular Policies with Detective & Preventive Controls



Rule #1 Description non-App Source AppUser Connection

Category Security **Classification** Breach **Severity** MED

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

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

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

Hot **DB Name**

Hot **DB User** APPUSER

Field Name

Object INVENTORY

Command DROP TABLE

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.com

- 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

Sample Alert

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM

To: Marc Gamache

Cc:

Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection

Category: security Classification: Breach Severity: MED

Rule # 20267 [non-App Source AppUser Connection]

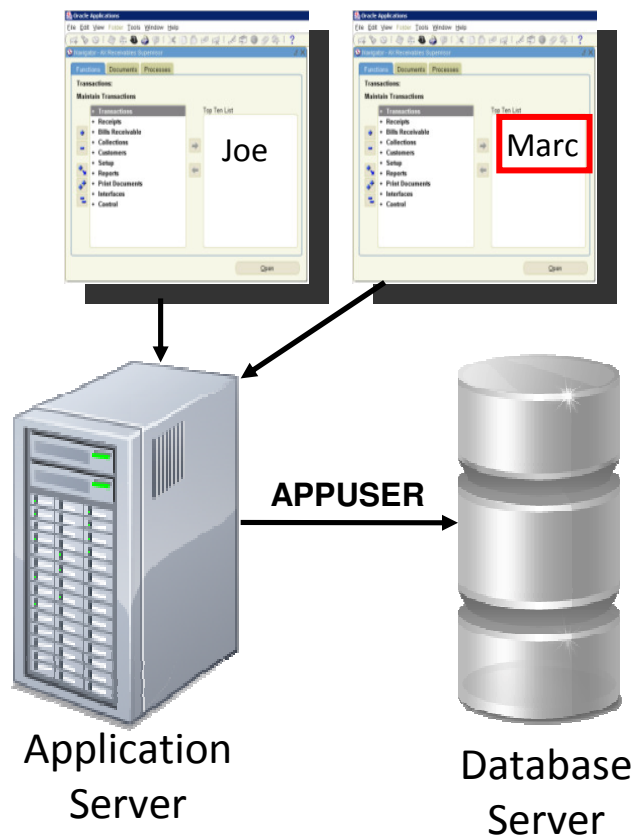
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER

Application User Name

Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:

SQL: select * from EmployeeTable

Identifying Fraud at the Application Layer



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

- **Issue:** Application server uses generic service account to access DB
 - Doesn't identify *who* initiated transaction (connection pooling)
- **Solution:** Guardium tracks access to **application user associated with specific SQL commands**
 - Out-of-the-box support for all major enterprise applications (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos...) and custom applications (WebSphere ...)
 - No changes required to applications
 - Deterministic tracking of user IDs
 - Does not rely on time-based "best-guess"

Access To Excessive or Unneeded Data

Should my customer service rep view 99 records in an hour when average is 4?

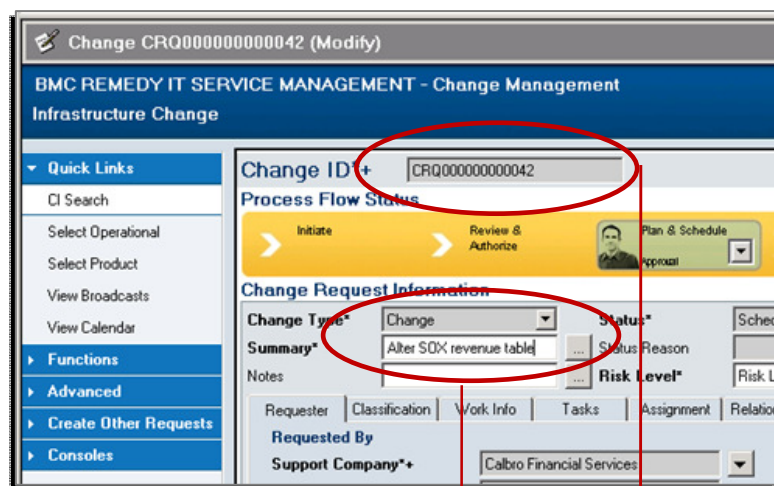
<u>DB User Name</u>	<u>Sql</u>	<u>Records</u>
STEVE	select * from ar.creditcard where i>? and i<? 4	
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

Is this normal?

What did he see?

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

Enforcing Change Control Policies



Tag DBA actions with ticket IDs










Compare observed changes to approved changes

Identify unauthorized changes (red) or changes with invalid ticket IDs

Start Date: 2009-01-22 15:00:00 End Date: 2009-01-22 16:00:00

Timestamp	Server Type	risk level	priority	description	change id	change id entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:41:55.0	ORACLE	0	0			crq0000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,,?)

Auditing Database Configuration Changes

 SORACLE_HOME/soap/bin/.*	File Pattern	12h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 SORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 SORACLE_HOME/sysman/config/.*.properties	File Pattern	12h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 SORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
 ORACLE_BASE	Environment Variable	12h	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 ORACLE_HOME	Environment Variable	12h	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 ORACLE_SID	Environment Variable	12h	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 TNS_ADMIN	Environment Variable	12h	<input checked="" type="checkbox"/>	<input type="checkbox"/>
 select * from dba_db_links	SQL Script	12h	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- Track changes to files, environment variables, registry settings, scripts, etc. that can affect security posture
- 200+ pre-configured, customizable templates for all major OS/DBMS configurations

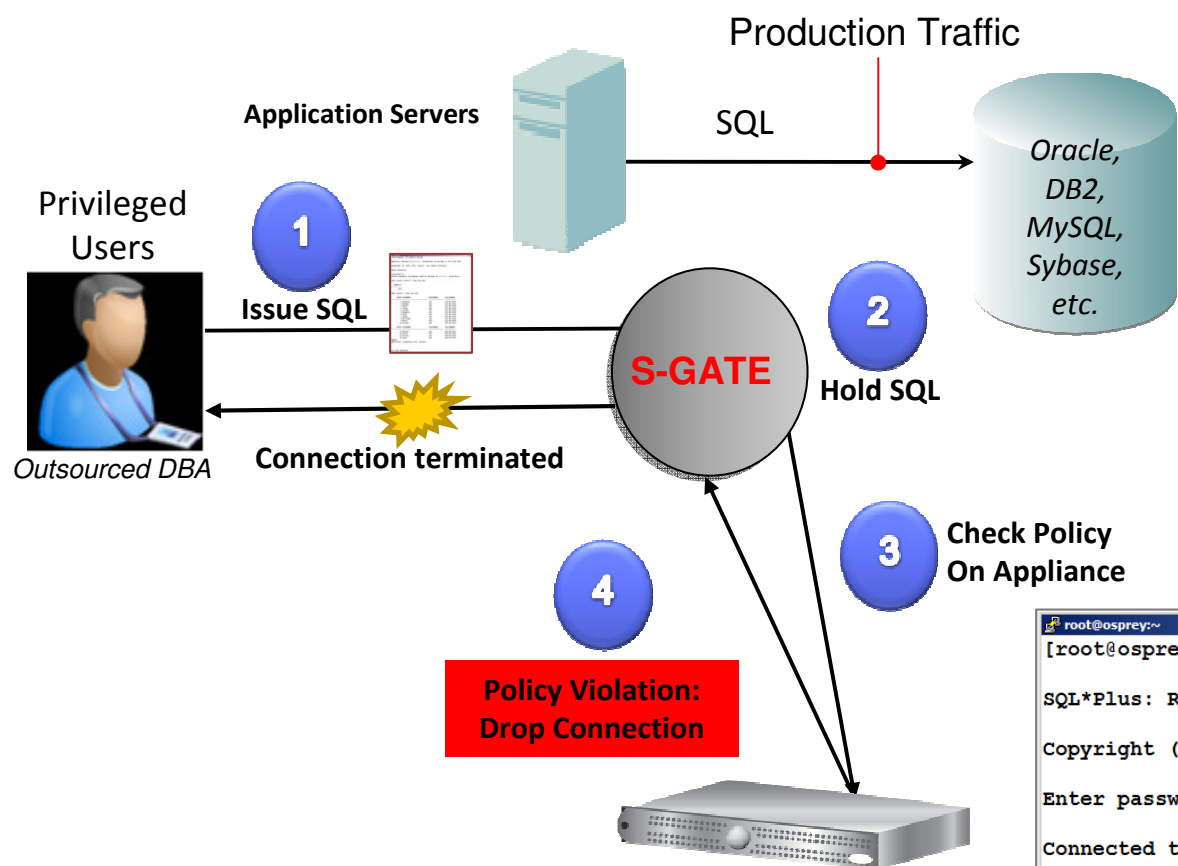
Discovering & Classifying Sensitive Data

Administration Console						
Administration Console	Access Management	Tools	Daily Monitor	SQL Guard Monitor	Tap Monitor	Incidents
SQL Count	Databases Discovered					
Session Count	Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49					
Logged Threshold Alerts	<u>Time Probed</u>	<u>Server IP</u>	<u>Server Host Name</u>	<u>DB Type</u>	<u>Port</u>	<u>Port Type</u>
Logged R/T Alerts	2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp
Exception Count	2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp
Dropped Requests	2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp
TCP Exceptions	2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp
Admin User Logins	2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp
Databases by Type	2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp
Databases Discovered						
Retrospective Report Requests						
Values Changed						
Throughput						

- ✓ Discover databases
- ✓ Discover sensitive data
- ✓ Policy-based actions
 - ✓ Alerts
 - ✓ Add to group of sensitive objects

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
<input type="checkbox"/>	BANKAPP	CREDITCARD	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:07 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE BANKAPP.CREDITCARD VARCHAR2 (20) CARDNUMBER Category: 'PCI' Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE=TABLE,VIEW, DATA_TYPE=TEXT, SEARCH_VALUE_PATTERN='[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-system

Proactively Preventing Policy Violations in Real-time



- ✓ No database changes
- ✓ No application changes
- ✓ Without risk of inline appliances that can interfere with application traffic

**Policy Violation:
Drop Connection**

```

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
Session Terminated
SQL>
    
```

Automated Sign-offs & Escalations for Compliance



Guardium

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:

Comments:

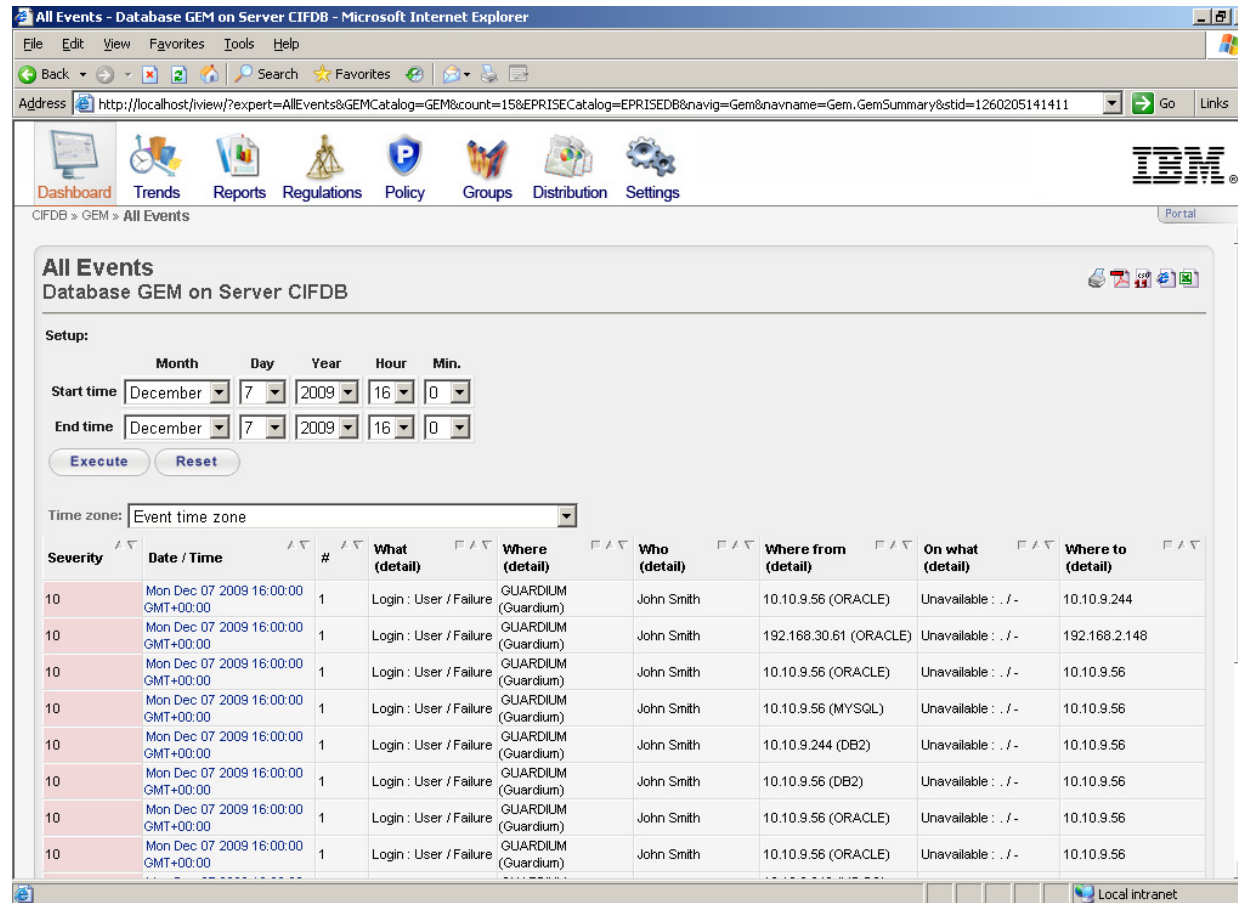
Timestamp	User	Comment for Result
2009-04-16 00:42:37.0	Marc	Need to review the DB login failure more closely! App User account should not fail a login.

[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](#) View

- Automates entire compliance workflow
 - Report distribution to oversight team
 - Electronic sign-offs
 - Escalations
 - Comments & exception handling
- Addresses auditors' requirements to document oversight processes
- Results of audit process stored with audit data in secure audit repository
- Streamlines and simplifies compliance processes

Optimizing Operations With TSIEM Integration



All Events - Database GEM on Server CIFDB - Microsoft Internet Explorer

Address: <http://localhost/view/?expert=AllEvents&GEMCatalog=GEM&count=15&EPRISECatalog=EPRISED&nav=Gem&navname=Gem.GemSummary&stid=1260205141411>

Navigation: Dashboard Trends Reports Regulations Policy Groups Distribution Settings

CFDB > GEM > All Events

All Events
Database GEM on Server CIFDB

Setup:

Start time: Month: December, Day: 7, Year: 2009, Hour: 16, Min: 0
End time: Month: December, Day: 7, Year: 2009, Hour: 16, Min: 0

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : / -	10.10.9.244
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	192.168.30.61 (ORACLE)	Unavailable : / -	192.168.2.148
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (MYSQL)	Unavailable : / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.244 (DB2)	Unavailable : / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (DB2)	Unavailable : / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : / -	10.10.9.56
10	Mon Dec 07 2009 16:00:00 GMT+00:00	1	Login : User / Failure	GUARDIUM (Guardium)	John Smith	10.10.9.56 (ORACLE)	Unavailable : / -	10.10.9.56

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

De-identify Data in Test/Dev Environments

- Mask or de-identify sensitive data elements that could be used to identify an individual
- Ensure masked data is contextually appropriate to the data it replaced, so as not to impede testing
 - Data is realistic but fictional
 - Masked data is within permissible range of values
- Support referential integrity of the masked data elements to prevent errors in testing



Personal identifiable information is masked with realistic but fictional data for testing & development purposes.

Financial Services Firm with 1M+ Sessions/Day



- **Who:** Global NYSE-traded company with 75M customers
- **Need:** Enhance SOX compliance & data governance
 - *Phase 1:* Monitor privileged user activities, especially DB changes.
 - *Phase 2:* Focus on data privacy.
- **Environment:** 4 data centers managed by IBM Global Services
 - 122 database instances on 100+ servers
 - Oracle, IBM DB2, Sybase, SQL Server on AIX, HP-UX, Solaris, Windows
 - PeopleSoft plus 75 in-house applications
- **Alternatives considered:** Native auditing
 - Not practical because of overhead; DB servers at 99% capacity
- **Results:** Now auditing 1M+ sessions per day (GRANTs, DDL, etc.)
 - Caught DBAs accessing databases with Excel & shared credentials
 - Producing daily automated reports with sign-off by oversight teams
 - Automated change control reconciliation using ticket IDs
 - Passed multiple external audits

PCI Compliance for McAfee.com

- **Who:** Global security company
- **Need:** Safeguard millions of PCI transactions
 - Maintain strict SLAs with ISP customers (Comcast, COX, etc.)
 - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
 - Multiple data centers; clustered databases
 - Integrated with ArcSight SIEM
 - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
 - Massive data volumes; performance & reliability issues
 - Separation of Duties (SOD) issues
- **Results**
 - *“McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial.”*



How Guardium Addresses PCI-DSS



- Req. 10: Track & monitor all access to cardholder data
 - Guardium creates secure audit trail with granular audit data (including SELECTs) with minimal performance impact, including logging all access by privileged users

- Req. 3: Protect stored cardholder data
 - Real-time controls based on client IP, application, OS user, DB user, ...
 - Compensating control for column-level encryption

- Req. 7: Restrict access to cardholder data
 - Provides granular access control via real-time alerts and/or blocking
 - Compensating control for unsegmented networks

- Req. 6: Maintain secure systems
 - Identifies vulnerabilities and configuration changes at database tier

- Req. 2: Do not use vendor defaults for system passwords
 - Checks for default passwords, unpatched systems, ...

Securing SAP & Siebel: 239% ROI and <6 Months Payback

- **Who:** F500 manufacturer (\$15B revenue)
- **Need:** Secure SAP & Siebel data for SOX
 - Enforce change controls & consistent auditing across platforms
- **Environment**
 - SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems
 - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results: 239% ROI & 5.9 months payback, plus:**
 - **Proactive security:** Real-time alert when changes made to critical tables
 - **Simplified compliance:** Passed 4 audits (internal & external)
 - *“The ability to associate changes with a ticket number makes our job a lot easier ... which is something the auditors ask about.”*
 - **Strategic focus on data security**
 - *“There’s a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers.”*



Commissioned
Forrester Consulting
Case Study

Protecting Data Privacy in Test Environments

Leading Global Household Goods Manufacturer

Challenge

- This leading household goods manufacturer needed to consolidate multiple worldwide instances of the SAP Human Capital Management application.
- As they created their testing environment, the client wanted to “de-identify” their SAP HCM data so that developers were not using confidential employee HR data in their test environments.

Solution

- IBM Optim Data Privacy Solution for SAP Applications

Business Benefits

- Reduced time to manually code the data scrambling routines.
- Implemented data masking solution, as part of overall support data governance strategy
- Protected confidential employee information within the testing and development environments, ensuring privacy of HR and payroll information
- Deployed data masking solution quickly and efficiently, using both out-of-box definitions as well as custom de-identification routines

Guardium 8 -- Announcement Summary (September 13)

The Industry's Broadest Platform Support for Data Security & Compliance

- New & enhanced platforms

- SharePoint
- System z
- SAP
- PostgreSQL
- Netezza



IBM System z



- New access control capabilities

- Quarantine & Fire-ID
- Entitlement reporting

- New audit & compliance oversight capabilities

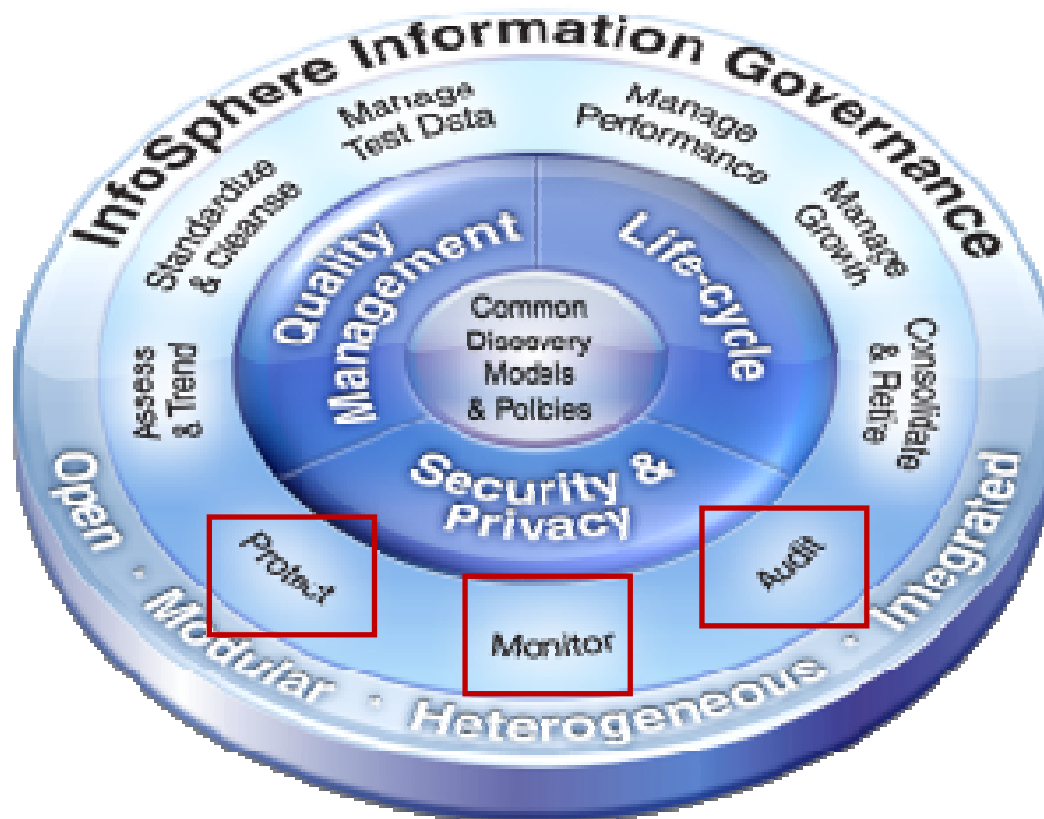
- Advanced compliance workflow automation

- 500 new VA tests

- Integration with Tivoli (TSIEM)

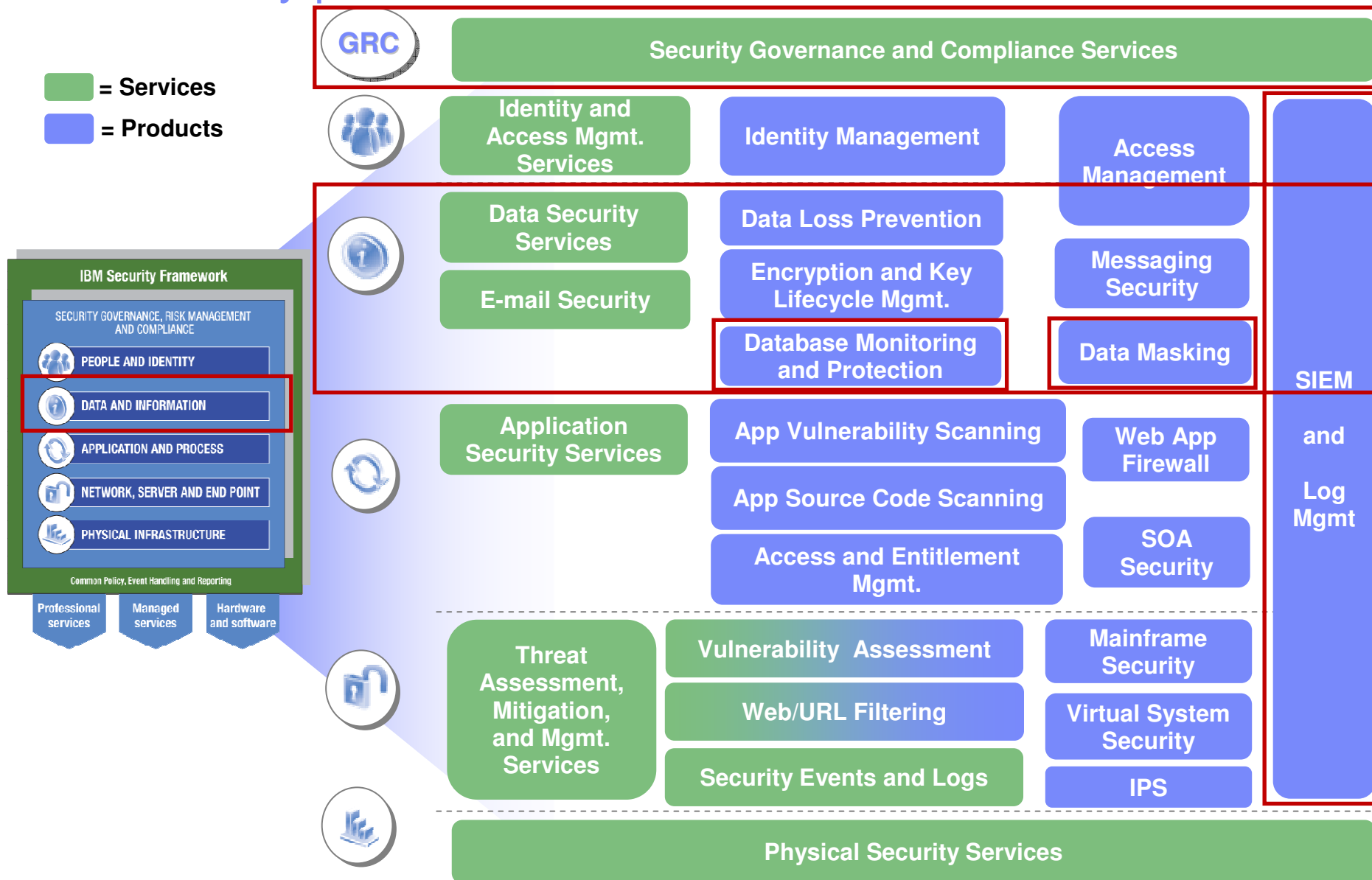
- Numerous scalability & usability enhancements based on ongoing customer feedback from large-scale installations

InfoSphere Guardium: Enabling Information Governance



IBM Security portfolio

= Services
 = Products



What The Analysts Are Saying

Gartner



Jeff Wheatman

“Most enterprises are paying too little attention to the very real security risks associated with their databases ... Native logging isn’t the answer [lack of granularity, separation of duties not supported, high overhead].”

FORRESTER



Noel Yuhanna

“Basic database security is no longer sufficient to protect private data ... Critical databases have hundreds or even thousands of connections per second, so it is humanly impossible to view and detect security anomalies.”

ESG



Jon Oltsik

“Databases house a higher percentage of confidential data than any other type of repository ... In most organizations (63%), database security depends primarily on manual or ad hoc processes ... no match for well-organized cybercriminals, malicious insiders and accidental events.”

Forrester: The Truth About Database Security!

- Most attacks on databases are difficult to detect.
- 75% of attacks are internal.
- 80% don't have a database security plan.
- 20% of enterprises take advanced security measures.
- 70% behind in security patches.
- DBAs spend less than 5% on database security.
- Most don't implement data security policies.

**Creating a Database Security Plan
– Why Basic Database Security Is
No Longer Sufficient.**

Noel Yuhanna
Principal Analyst
Forrester Research

Addressing the Full Lifecycle of Database Security

Real-time Database Security & Monitoring



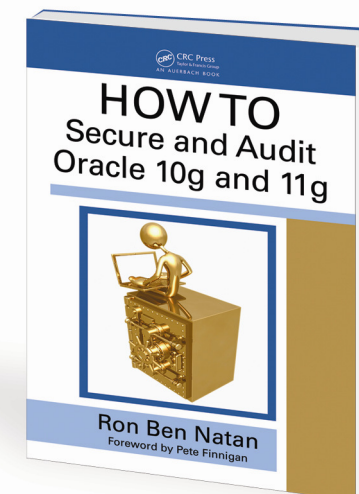
Summary & Conclusions

- Basic database security is insufficient to secure high-value databases
 - Ineffective against privileged users or end-users violating corporate policies
 - No real-time monitoring to immediately detect or block unauthorized access
 - Inability to detect fraud at application layer (SAP, PeopleSoft, etc.)
 - No VA, data discovery, leakage detection, file integrity monitoring, ...
 - No data masking to de-identify data in test/dev environments
- IBM/Guardium is the most widely-deployed solution, with ongoing feedback from the most demanding data center environments worldwide
 - Scalable enterprise architecture
 - Broad heterogeneous support
 - Deep automation to reduce workload
 - Holistic (comprehensive) approach
 - Available as virtual appliance for cloud environments



For More Information

- Download complementary analyst reports from www.guardium.com/resources
 - Forrester: “Your Enterprise Database Security Strategy 2010”
 - Gartner: “10 Database Activities Enterprises Need to Monitor”
- Check out *HOWTO Secure and Audit Oracle 10g and 11g*
 - Definitive 454-page text for security, risk management & database professionals
 - Written by database security expert & IBM/Guardium CTO, Ron Ben Natan, Ph.D.
 - Free chapter download available from www.guardium.com/index.php/landing/642
- See "Resources" section for case studies, ROI examples, white papers, reviews, Webcasts
- Check out the *Database Security TechCenter*
 - Latest news, tips & reports
 - www.darkreading.com/database_security/
- ***Next Webcast: “Beyond Monitoring: Guardium 8 Overview”, Thursday, September 30 at 11am ET***



SECURITY
darkREADING
Protect The Business  Enable Access

Thank
You

Appendix

Blue Cross Blue Shield Case Study



- **Who:** BCBS organization with 475,000 members
- **Need:** Secure financial data for SOX; secure patient data for HIPAA; adhere to NIST
 - Monitor all access to critical databases, including access by privileged users
 - Create a centralized audit trail for all database systems
 - Produce detailed compliance reports for auditors
 - Implement proactive security via real-time alerts
- **Environment:**
 - Oracle, SQL Server 2003/2005, IBM DB2, Sybase
 - AIX & Windows
 - LDAP & Microsoft MOM
- **Alternatives considered**
 - Native logging: Rejected due to performance overhead & need for centralized management
 - Application Security Inc (AppSec): Preferred Guardium's appliance model
- **Results:**
 - Monitoring 130 database instances on 100 servers (3 week implementation)
 - Guardium helped client to interpret regulations and implement policies
 - Integrated with Tivoli Storage Manager (TSM) for archiving of audit data

Similar Monitoring Requirements

Audit Requirements	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)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)

DML = Data Manipulation Language (data value changes)

DCL = Data Control Language

Vulnerability Assessment Example

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](#)

Assessment Result History

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 Showing 92 of 92 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Other	Excessive Login Failures (Production)	[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.	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

Overall Score

Historical Progress or Regression

Detailed Scoring Matrix

Filter control for easy use

Show only: [Reset Filtering](#)

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

Sort by:

First	Second	Third
Severity	Score	Datasource

Apply

Another Insider's Tale

“While it took years for his employer to develop its sophisticated computer code, it allegedly only took Samarth Agrawal days to steal it.” U.S. Attorney Preet Bharara



From
LinkedIn

- Trader for Wall Street firm
- Had access to codes for proprietary trading algorithms (IP)
- Stole data shortly before resigning to join another firm
- Theft only noticed after employee resigned
- What IT security missed
 - Unauthorized access to sensitive data
 - Policy in place but no ability to enforce
 - After-hours access – did not review logs
 - Credentials not sufficient – need continuous real-time monitoring

Forrester: Seven steps to a successful database security plan

Step 1. Establishing a team

Step 2. Understanding data security policies and compliances

Step 3. Understanding your database environment

Step 4. Establishing security policies

Step 5. Training and accountability

Step 6. Baseline and risk assessment

Step 7. Refining security plan

Gartner: 10 Database Activities Enterprises Need to Monitor

		Gartner	DAM
Privileged Users	Access or changes to data		●
	Access via inappropriate or unapproved channels		●
	Schema modifications		●
	Addition or modification of accounts		●
End Users	Access to excessive or unneeded data		●
	Data access outside standard hours		●
	Access via inappropriate or nonapproved channels		◐
Developers Sys. Admins Analysts	Access to live production systems		◐
IT Ops	Nonapproved changes to databases or applications		◐
	Out-of-cycle patching of production systems		◐