IBM SECURITY DAY 2011

Innovare con sicurezza per aprire al futuro

Walter Sartori – IBM SWG
IBM InfoSphere Guardium

Agenda

- Database Security
- Architettura
- Funzionalità
- Referenze

Guardium®
SAFEGUARDING DATABASES™

Protezione dei dati: le sfide

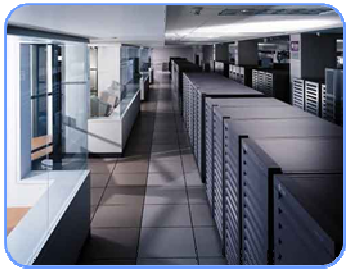
Dove sono i dati sensibili? Chi vi accede?

Come istituire politiche di controllo sugli accessi e le operazioni?

Come individuare *vulnerabilities* (scoperture) nei sistemi?

Come realizzare soluzioni complete, a costi ragionevoli?

Database Monitoring: 3 Business Drivers



1. **Attacchi interni**
   - Individuare modifiche non autorizzate
   - Evitare furti/manomissioni

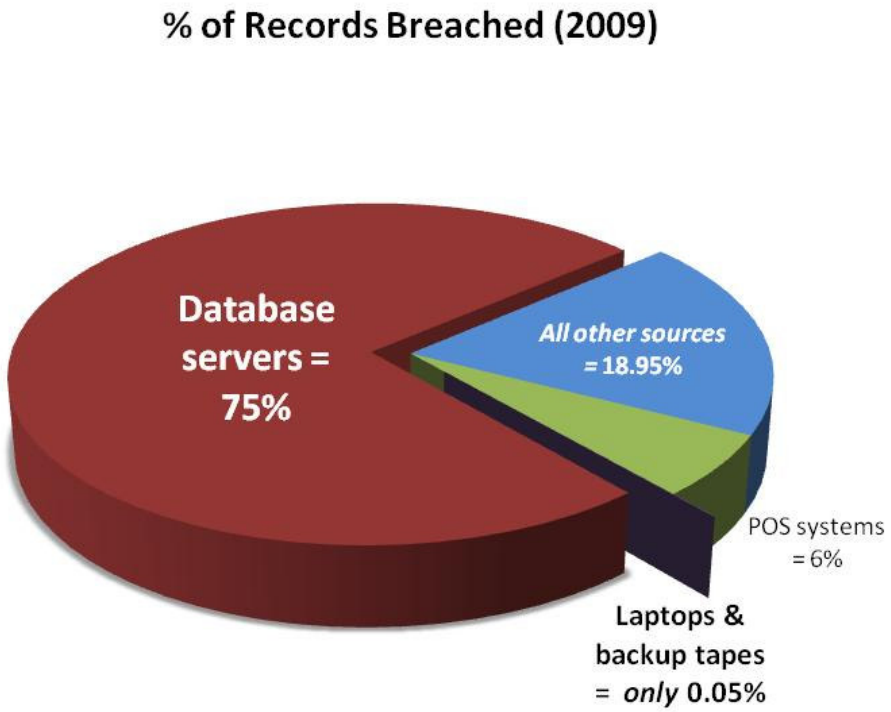
2. **Attacchi esterni**
   - Evitare furti/manomissioni
3. **Compliance**
   - Semplificazione dei processi
   - Riduzione dei costi

Guardium: l'acquisizione

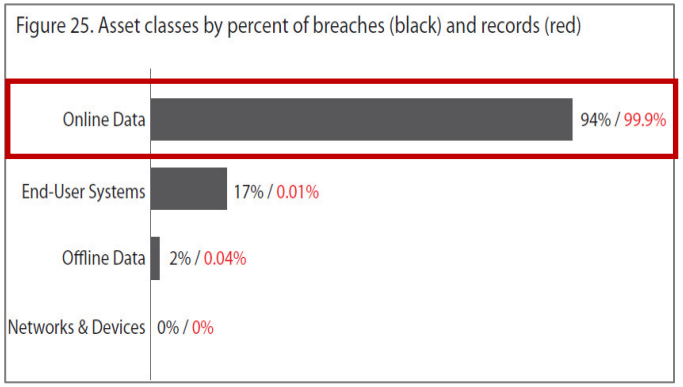
- Acquisizione: 2010
- Totale coerenza w/ strategie IBM
- Irrobustimento delle soluzioni per la protezione dei DBMS
  - Soluzione *cross platform*
  - Allargamento del perimetro:
    - *Proactiveness*
    - *Discovery*
    - *Vulnerability assessment*
  - Integrazione w/ applicazioni (SAP, …)
  - Integration w/ infrastrutture in essere (SIEM, *Change Mgmt*, …)

http://www.ibm.com/developerworks/wikis/display/IBMSecurityBlueprint/IBM+Security+Blueprint+Page

DBMS → principale obiettivo di attacco



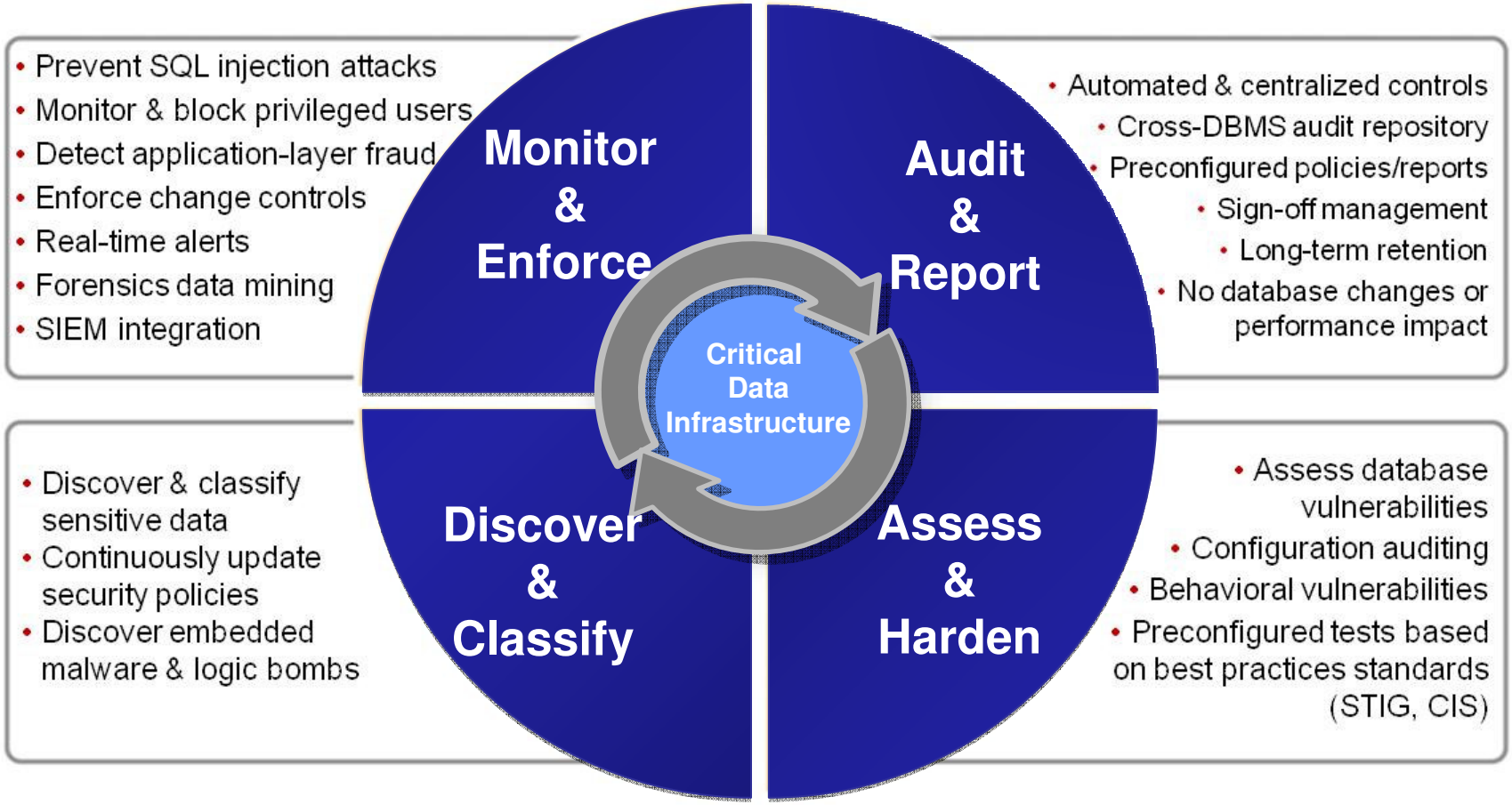
Online data = 99.9% of all compromised records



2009 Data Breach Report -Verizon Business RISK Team
http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

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

Database Security 360°



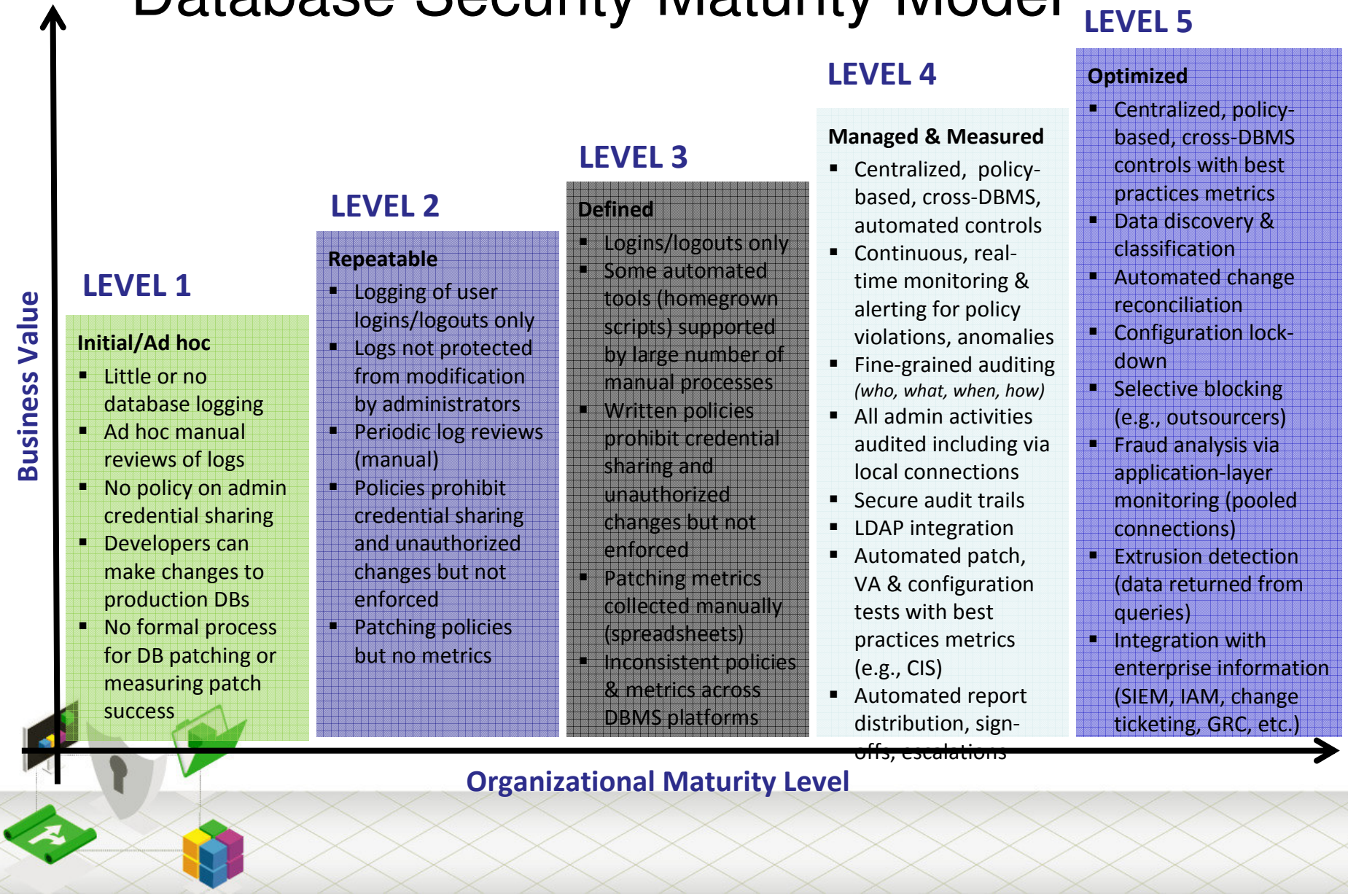
Attacchi dall'interno → *Separation of duties*

- "Organizations overlook the most imminent threat to their databases: authorized users." (Dark Reading)
- "No one group seems to own database security … This is not a recipe for strong database security" … 63% depend primarily on manual processes." (ESG)
- Most organizations (62%) cannot prevent super users from reading or tampering with sensitive information … most are unable to even detect such incidents … only 1 out of 4 believe their data assets are securely configured (Independent Oracle User Group).

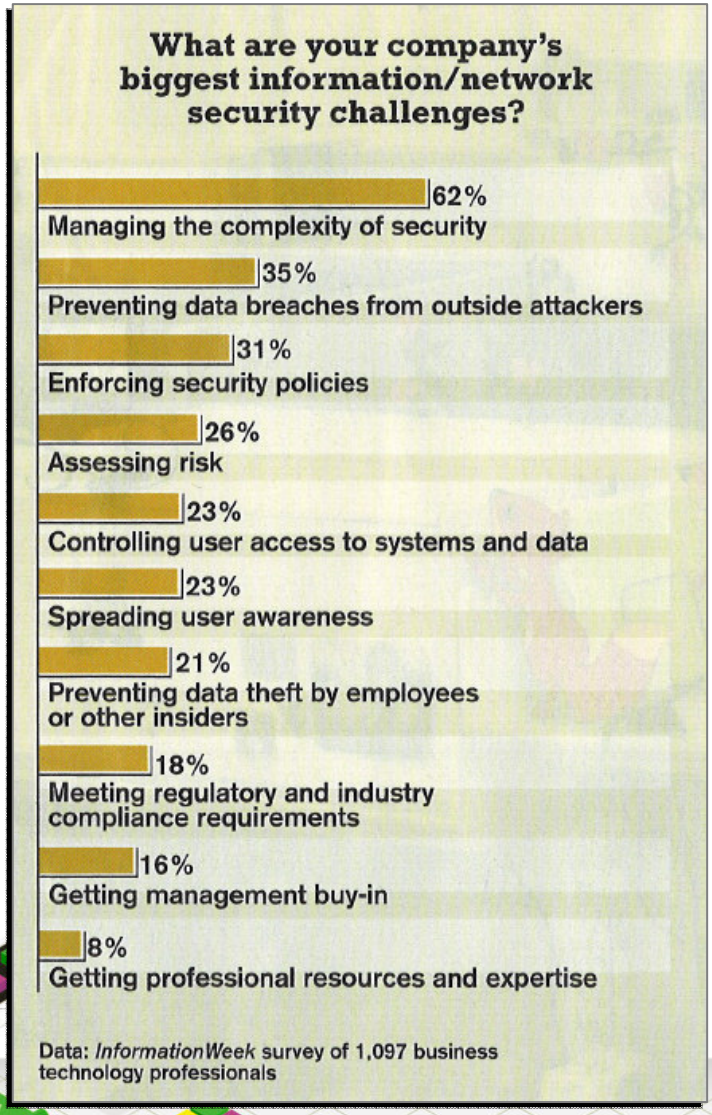
http://www.darkreading.com/database_security/security/app-security/showArticle.jhtml?articleID=220300753

http://www.guardium.com/index.php/landing/866/

Database Security Maturity Model



CIOs: le priorità




ANALYTICS BRIEF | STRATEGIC SECURITY

Secure What Matters

By Mike Fratto

IF YOU HAVE YET TO ADOPT risk management processes when developing security plans, you may as well be shooting blind—and given the cost of the bullets (new infosec technologies like data leakage protection and compliance tools), that's simply not acceptable going into a leaner, meaner 2009. We realize that the process of classifying IT assets, assigning values, evaluating threats, and then using that data to determine where and how to spend security dollars isn't something most of us are comfortable with. But you need to get over it lest you be overwhelmed by the No. 1 challenge cited by the nearly 1,100 respondents to our *InformationWeek* Analytics 2008 Strategic Security Study: complexity.

Risk management requires a holistic view of the threats faced by your organization and a systematic approach to addressing those threats most easily exploited against the highest-value assets. As part of that effort, IT needs to increasingly work with its facilities counterparts to eliminate duplicative efforts and work to manage one master set of threats.

That's far from the only area that begs for simplification. The increased complexity of applications and security products is also a concern. For example, you can harden a Web application by using secure coding methods, performing source-code analysis and repair, adding software to an existing application or application server, or placing a Web application firewall between the server and clients. Which method is best depends on your goal: Do you want to block malicious input, prevent data extrusion, deny access to the underlying operating system or back-end servers, stop privilege escalations, or all of the above? While vendors say they can address all these issues and more, the reality is there's still no silver bullet.

High on our hit list for attention early in 2009 is data leakage protection. A relatively high number of organizations in our survey say they're trying to detect sensitive data loss. They're finding that sometimes it's malicious, such as a disgruntled employee stealing customer lists. But leakage also comes from well-meaning users who send files to their private e-mail accounts so they can work at home, or discussing sensitive topics in e-mail or instant messaging.

Can you protect all data all the time? No, nor should you try. Risk management, after all, is about taking appropriate measures to protect the assets most valuable to your business.

Get the full-length Analytics Report at: *informationweek.com/bi/security_survey*

34 Dec. 1, 2008

InformationWeek
DEFINING THE BUSINESS VALUE OF TECHNOLOGY

December 1, 2008

Normative

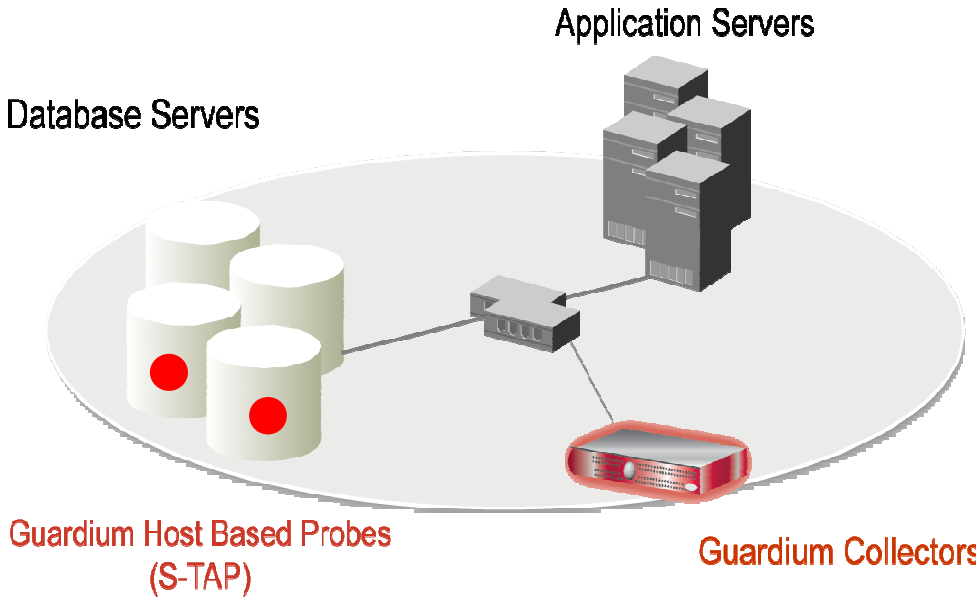
Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

DDL = Data Definition Language (aka schema changes)
DML = Data Manipulation Language (data value changes)
DCL = Data Control Language

Guardium e PCI-DSS

Reqt.	Description	Guardium PCI Capabilities
2	**Do not use vendor defaults for system passwords**	**Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG)**
	• Configure system parameters to prevent misuse	• Checks for default passwords, unpatched systems, misconfigured privileges, etc.
	• Encrypt non-console admin access	• Audits usage and alerts on misuse
		• Locks configurations after vulnerabilities remediated
		• Monitors encrypted traffic (Oracle ASO, SSL, etc.) without need for key storage
3	**Protect stored cardholder data**	**Real-time, database leak prevention**
		• Continuous, real-time, policy-based monitoring with proactive security (alerts, blocking)
		• Compensating control for column-level encryption
		• Auto-discovers & classifies stored data; identifies sensitive data in query result stream
6	**Maintain secure systems**	**Centralized vulnerability and configuration assessment**
	• Establish a process to identify security vulnerabilities	• Ensures current patches applied & vulnerable SPs identified; "virtual patching"
	• Follow change control procedures for all configuration changes	• Alerts on all configuration changes, inside and outside databases
	• Separation of duties (development, test and production)	• Enforces separation of duties with real-time alerting and granular access controls
7	**Restrict access to cardholder data**	**Proactive, real-time access control (independent of native DBMS controls)**
		• Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc.
		• Blocks any unauthorized user, including administrators, from accessing cardholder data
		• Compensating control for unsegmented networks
8	**Assign a unique ID to each person with computer access**	**Complements native DBMS controls with external, cross-DBMS controls**
	• Enforce password policies	• Alerts on credential sharing, failed logins, account creation, privilege escalation
	• Limit repeated access attempts	• Verifies password policies are enforced; can lock accounts or terminate sessions
10	**Track and monitor access to cardholder data**	**Continuous, granular auditing with scalable architecture to handle high transaction volumes**
		• Fine-grained audit trail of all database activities (SELECT, DDL, DML, DCL, logins, logouts, etc.)
		• Does not rely on native trace or audit logs: minimal perf. impact (2-3%), enforces sep. of duties
		• Tracks all network and local connections, including direct access by DBAs (shared memory, etc.)
		• Audit information stored securely in hardened appliance to prevent anti-forensics or tampering
		• Identifies fraud by resolving end-user IDs in connection-pooling apps (SAP, Cognos, PeopleSoft, etc.
		• Integrates with LDAP, IAM, TCIM, TSM, SIEM, change management, CMDBs, etc.
		• Compliance workflow automation (electronic sign-offs, escalations) demonstrates oversight process
		• PCI Accelerator provides pre-configured reports based on best practices
11	**Regularly test security systems and processes**	**Integrated vulnerability scanning, file integrity monitoring & behavioral vulnerability testing**
	• Run internal and external vulnerability scans	• Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations
	• Deploy integrity monitoring to detect modif. of critical sys. files	• Tracks changes to DB configuration files, environ./registry variables, executables and OS files
12	**Maintain an Information Security Policy**	**Robust automated controls for enforcing information security policies**
	• Monitor/analyze alerts and distribute to appropriate personnel	• Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration
	• Monitor and control all access to data	• Automated sign-offs demonstrate formal oversight process
		• 100% visibility & control over all database transactions (with blocking)

Real-Time Database Monitoring

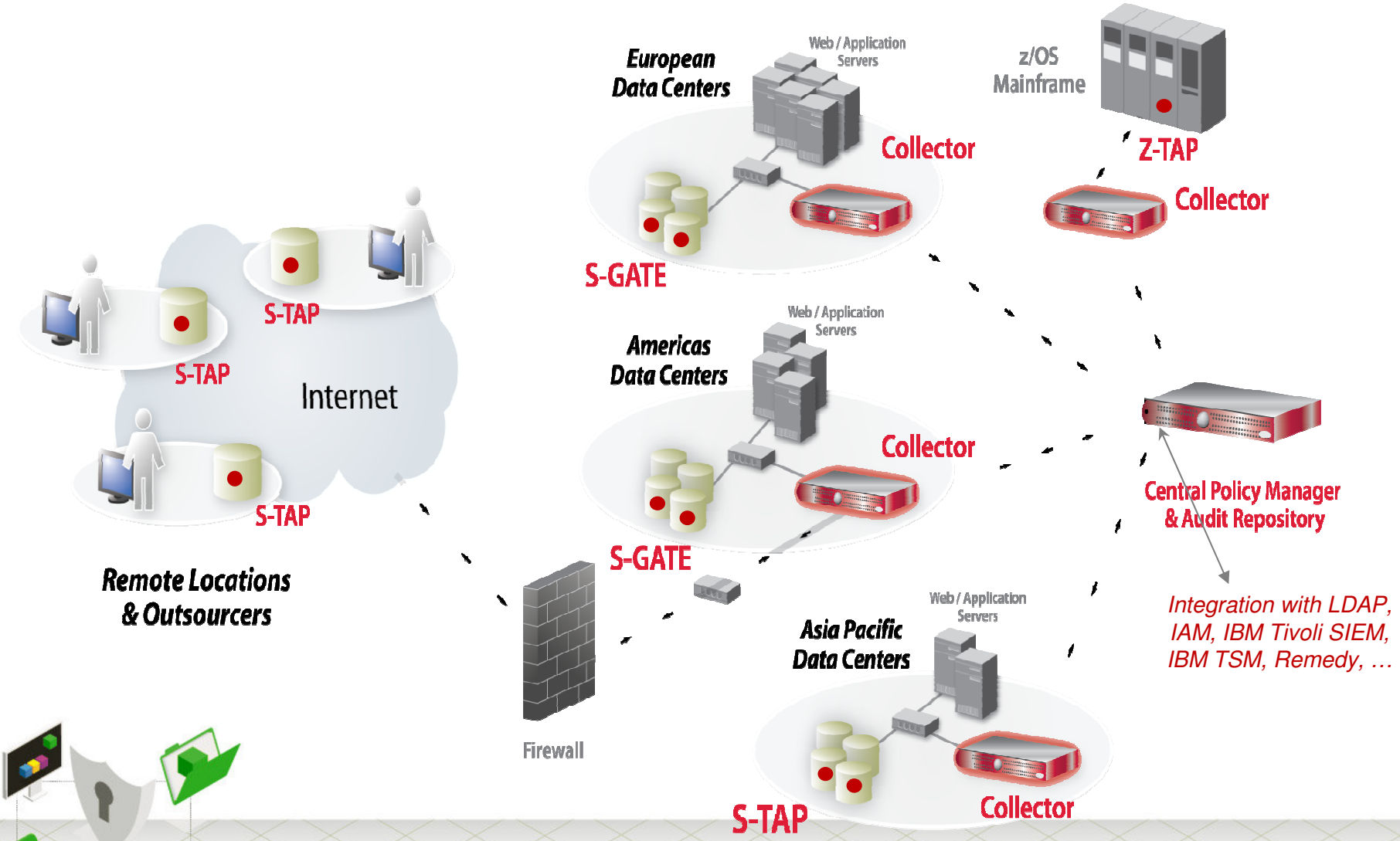


ORACLE
IBM DB2
SQL Server
TERADATA
SYBASE
MySQL
Informix

- Architettura non-invasiva
  - Esterna al database
  - Impatto prestazionale minimo (2-3%)
  - Nessuna modifica DBMS/applicativa
- Soluzione Cross-DBMS

- Separation of duties (“intelligenza” in appliance)
- Nessuna accesso a log DBMS (performance, sicurezza, …)
- Politiche granulari/real-time di *auditing*
  - *Who, what, when, how*
- Compliance reporting, sign-offs, escalations, …

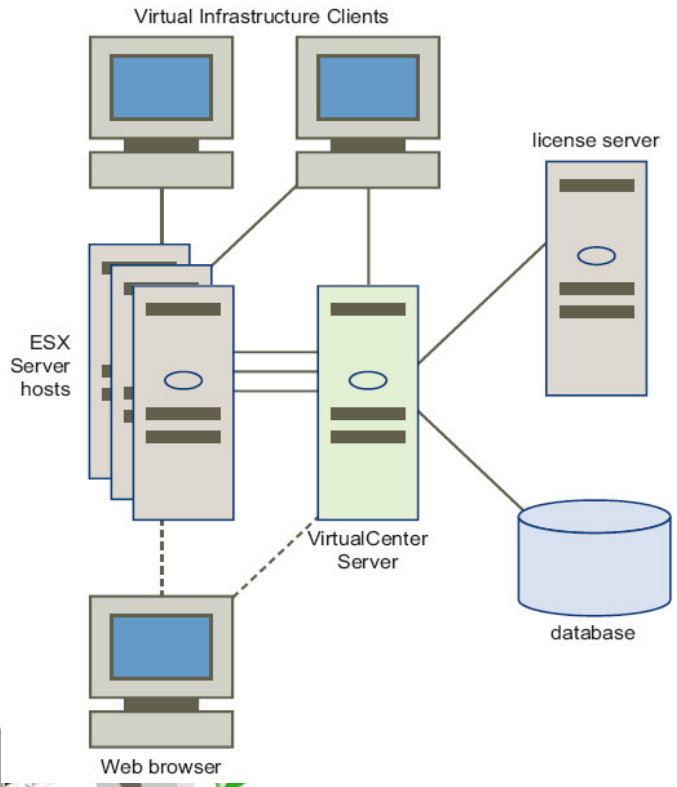
Architettura: scalabilità multi-tier

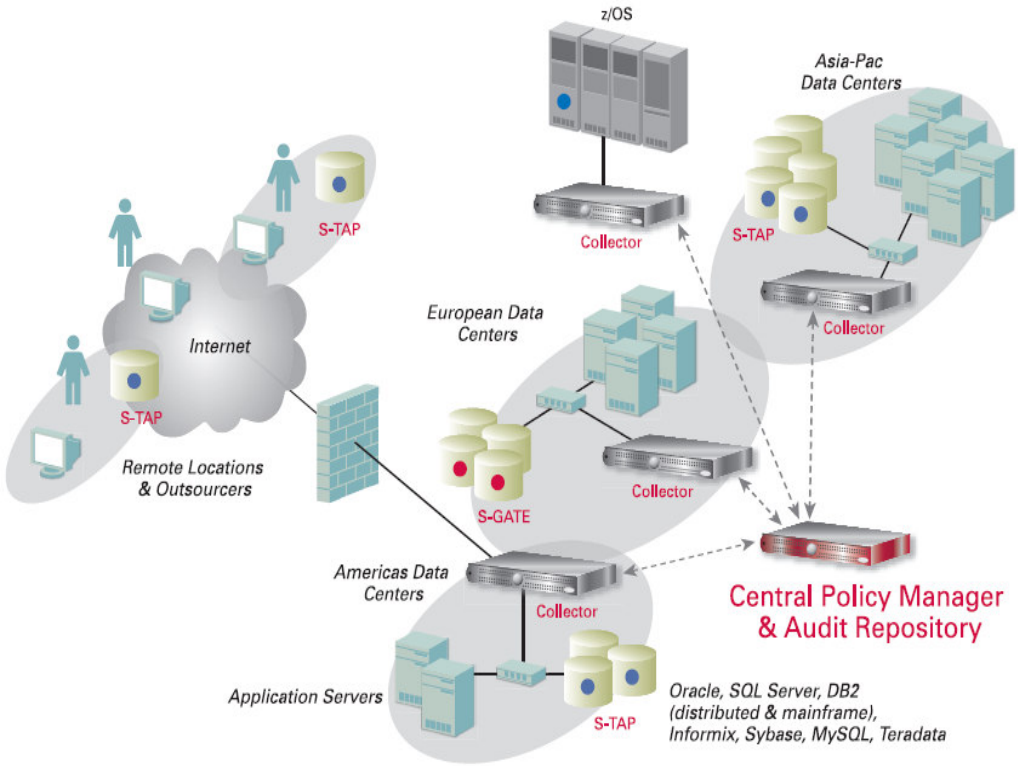


Architettura: virtual vs. physical appliance

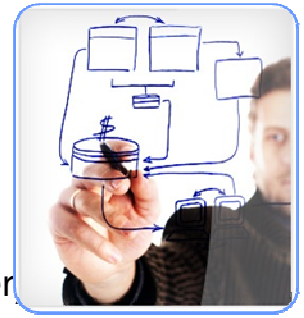
Virtual Appliance

Hardware Appliance





Vulnerability & DBMS



- DBMS contengono la % maggiore di dati critici/sensibili
- DBMS eterogenei: pratica comune
- Sicurezza: dove risiede la responsabilità?
  - "*DBAs spend less than 5% of their time on database security*." (Forrester
  - Proprietari delle applicazioni: maggiore attenzione su disponibilità del servizio, performance, aspetti funzionali
  - Uffici Sicurezza: spesso + orientati a sicurezza di rete
- Database vulnerability assessment:
  - Patch level
  - Utenze/password di default
  - Policies per password e failed logins
  - Controllo ruoli/privileges
  - Configurationi esterne (porte, protocolli, registri, variabili di ambiente, …)
  - "Behavioral vulnerabilities" (failed logins, …)
  - Individuazione dei dati sensibili (data discovery)

Vulnerability Assessment/patch mgmt

"Patch management is one of the most fundamental functions of IT departments, yet in our research we discovered it remains one of the biggest pain points for many organizations." *Rich Mogull, Securosis*

–50% non ha una processo formalizzato per il *patch management*

–68% non ha metriche per misurare l'efficacia della gestione

–> 50% non misura il livello di aderenza a policy/compliance

–> 50% non documenta in modo accurato e consistente le attività

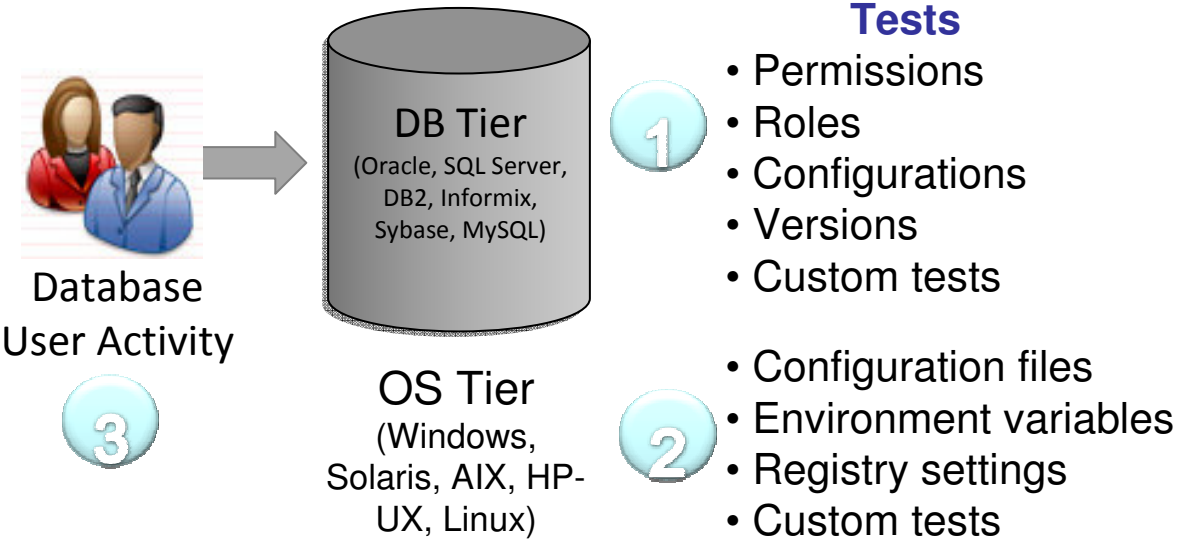
–Solo il 18% misura retroattivamente/periodicamente la situazione

"*The least mature areas of patching seem to correlate almost directly with the fastest-growing areas of attacks, such as … database servers [and] business application servers."*

http://www.darkreading.com/database_security
http://www.securosis.com/projectquant

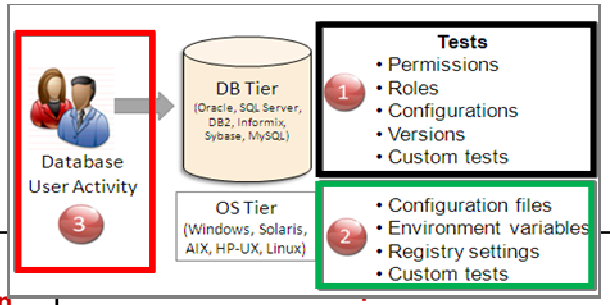
Vulnerability & Configuration Assessment: architettura

- Industry standards (DISA STIG & CIS Benchmark)
- Personalizzabile
  - Custom scripts, SQL queries, …
- Diversi livelli di azione:
  - Database settings
  - Sistema operativo
  - Comportamento



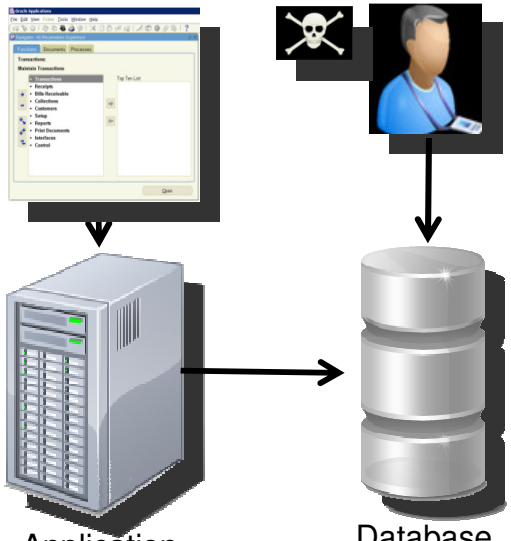
IBM SECURITY DAY 2011

Innovare con sicurezza per aprire al futuro



STIG Section	STIG Requirement	CIS Section		Guardium Monitors
2: DBMS Integrity	Monitor for current versions & patch levels; unauthorized changes; privileges granted to developers on production systems; ad hoc queries.	2,12: Oracle 2: SQL Server	Installation and patch levels; creation of objects for unauthorized changes; monitor developer access to production; avoid ad-hoc queries on production databases; change control process.	✓
3: Access Control	All actions traceable to a user; concept of least privilege (users, roles & applications); no shared accounts; no default accounts; lock accounts after 3 failed logins; minimum password strength; passwords changed every 90 days; restrict access by shared service accounts (connection pooling); all DBA accounts authorized by IAO.	2, 11: Oracle 1, 3, 4, 6, 8: SQL Server	No default accounts, passwords; DB hardening; guest accounts disabled; disable various extended stored procedures; SQL logins have strong passwords; assign permissions to roles rather than users; periodic scan of Role Members.	✓
4: Database Auditing	Audit all DB operations with sufficient granularity to detect intrusive activity; monitor all DBA connections; ensure audit data only readable by authorized personnel; no unauthorized applications or batch jobs; unusual or suspicious patterns of activity; monitor changes to DB objects; review audit data daily; maintain audit data for 1 year.	12: Oracle 4, 5: SQL Server	Review DBA Group membership; review and control which applications access the database; review audit info regularly; audit privileged user activity (object access, ownership, add DB user, etc.).	✓
5: Network Access	Remote admin connections must be encrypted (& monitored); identify DB users when using connection pooling; separate DB accounts for replication; prevent developers from accessing sensitive data.	12: Oracle 1, 2: SQL Server	Encryption; change SQL Server default ports.	✓
6: OS Permissions	Verify file permissions on DB executables, configuration files & data files; ensure only authorized DBAs granted membership to DBMS privileged OS groups.	1: Oracle 1, 3: SQL Server	Windows registry; deny Guest OS Group; OS Benchmark Configuration.	✓

Fine-Grained Policies w/ Real-Time Alerts



Rule #1 Description: non-App Source AppUser Connection
Category: Security | Classification: Breach | Severity: MED
Not Server IP / and/or Group: Production Servers
Not Client IP / and/or Group: Authorized Client IPs
Not Client MAC | Net. Protocol | and/or Group
Not DB Name
Not 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

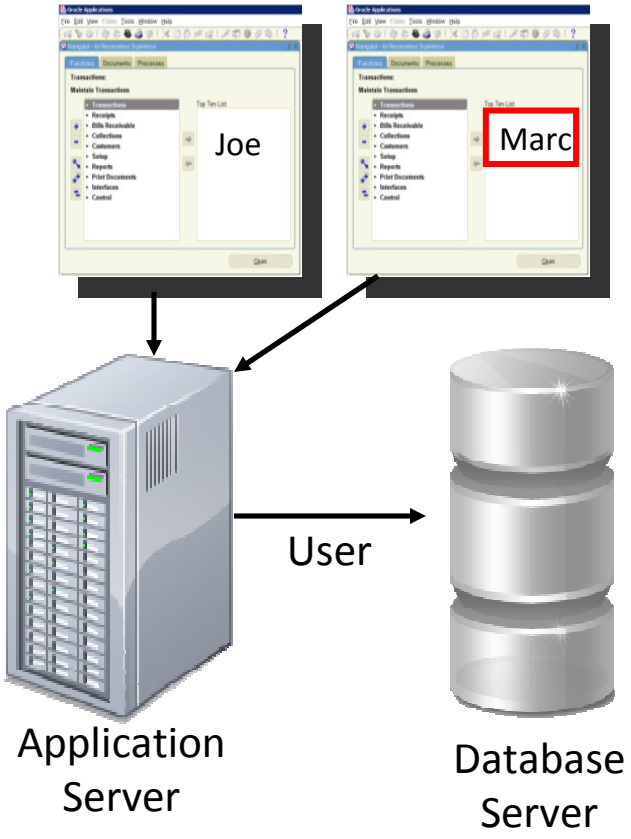
ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

CIFS
DB2
FTP
IBM DB2 Z/OS
IBM ISERIES
IMS
Informix
MS SQL SERVER
MYSQL
Oracle
Sybase
TERADATA

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

Risalire a monte dell'AS



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

- ***Problema***: Application Server usano generici *service account* per affacciarsi sul database
  - Persa l'effettiva identità di chi esegue la transazione (*connection pooling*)
- ***Soluzione***: Guardium riconduce l'azione all'utente effettivo (agente sull'AS)
  - Supporto out-of-the-box support per le applicazioni più diffuse (Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…) e per applicazioni custom (WebSphere….)

Analisi temporale

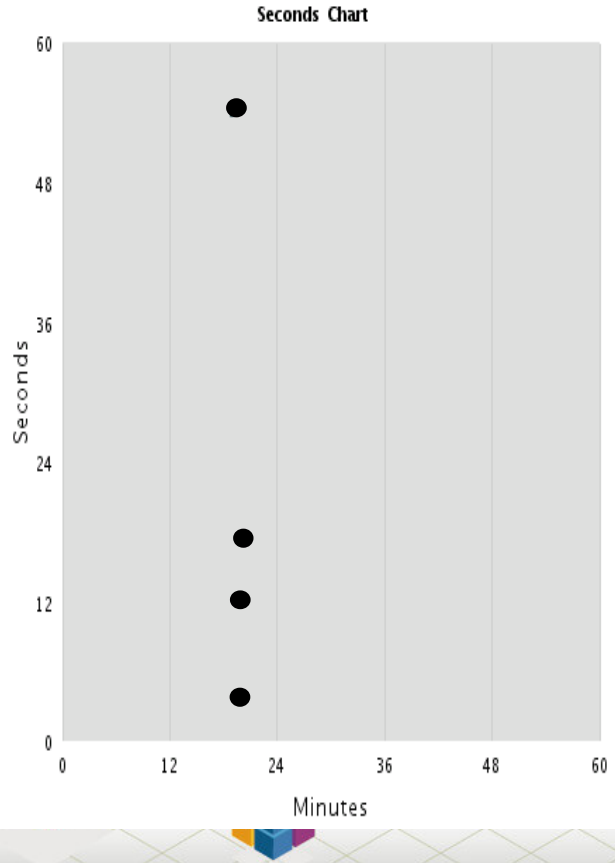
Original SQL: insert into cc (i, cardnumber, name) values(?, ?, ?)
Period Start: 2009-08-11 09:00:00
Period End: 2009-08-11 09:59:59
Client IP: 10.10.9.56
Server IP: 10.10.9.56
DB User: HARRY
Source Program: SQLPLUS@OSPREY
Total Access: 4 Failed: 0 Succeeded: 4

- SQL Timestamp for SQL trace

Start Date: 2009-08-11 08:22:15 End Date: 2009-08-11 09:22:15

Client IP	Server IP	Network Protocol	OS User	DB User Name	Source Program	Show Seconds	Sql	Total access
10.10.9.56	10.10.9.56	BEQUEATH	ROOT	HARRY	SQLPLUS@OSPREY	Seconds Graph	insert into cc (i, cardnumber, name) values(?, ?, ?)	4

Records: 1 to 1 of 1



Details

19 min ,54 sec	20 min ,4 sec	20 min ,12 sec	20 min ,18 sec

Inspection Engine Configuration

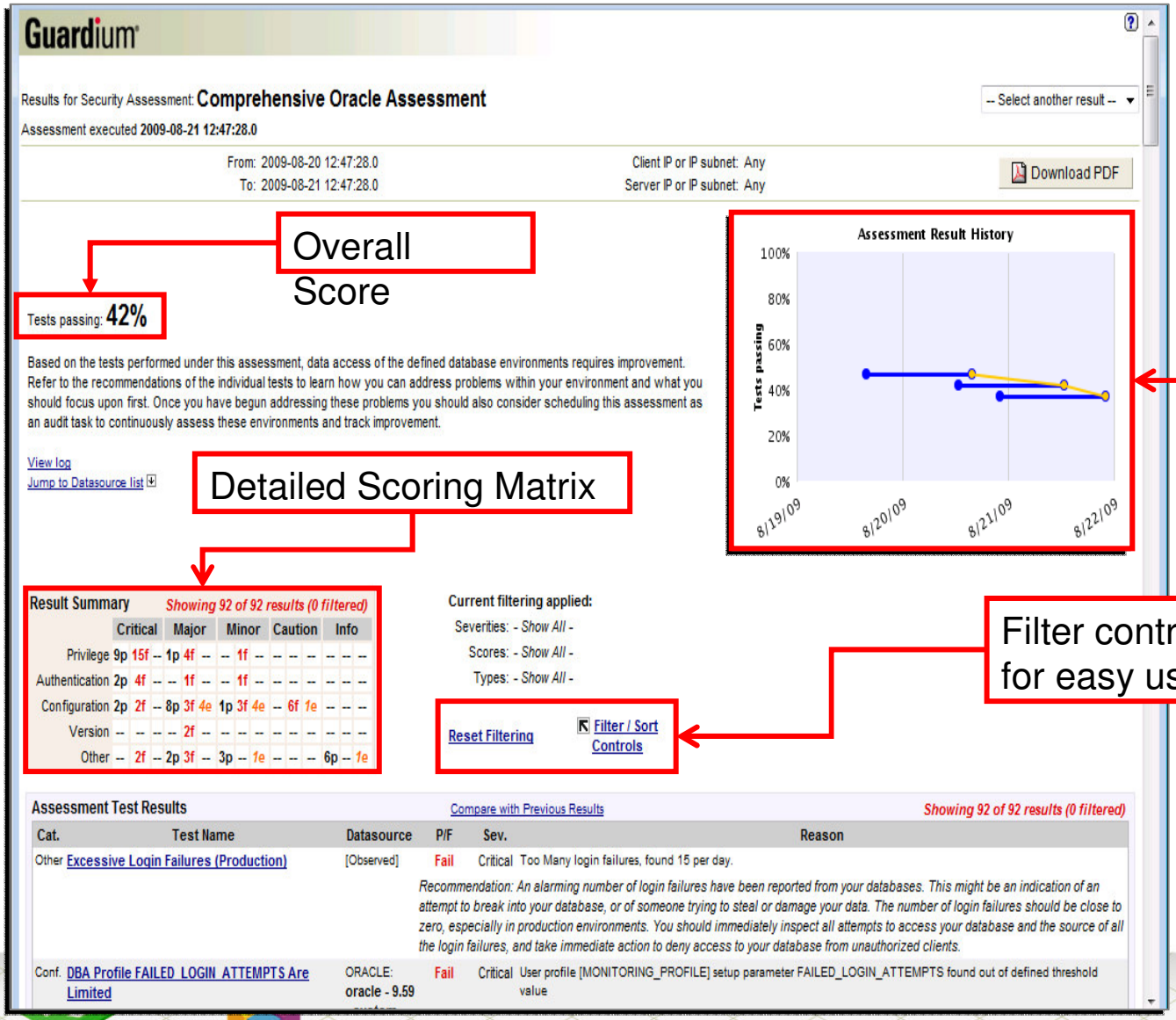
- [x] Log Request Sql String
- [x] Log Exception Sql String
- [x] Log timestamp per second
- [ ] Inspect Returned Data
- [ ] Compute Avg. Response Time
- [ ] Record Empty Sessions
- [ ] Log Sequencing
- [ ] Log Records Affected

Logging Granularity: 60 minutes
Max. Hits per Returned Data 64
Buffer Free: 100 % Ignored Ports List:
Restart Inspection Engines | Comment | Apply
Add Inspection Engine...

root@osprey:~

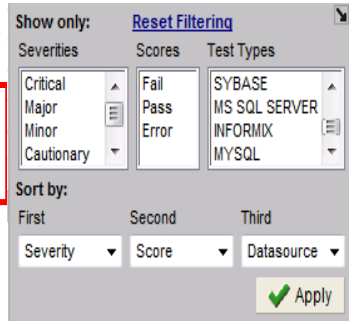
```
Oracle Database 10g Express Edition Release 10.2.0.1

SQL> insert into cc (i, cardnumber, name) values(1, '1234567890123456', 'Joe Smith');
1 row created.

SQL> insert into cc (i, cardnumber, name) values(2, '1234567890123457', 'John Henry');

1 row created.

SQL> insert into cc (i, cardnumber, name) values(3, '1234567890123458', 'James McDowl');

1 row created.

SQL> insert into cc (i, cardnumber, name) values(1, '1234567890123456', 'James Smith');

1 row created.

SQL> commit;

Commit complete.

SQL>
```

Vulnerability Assessment Example

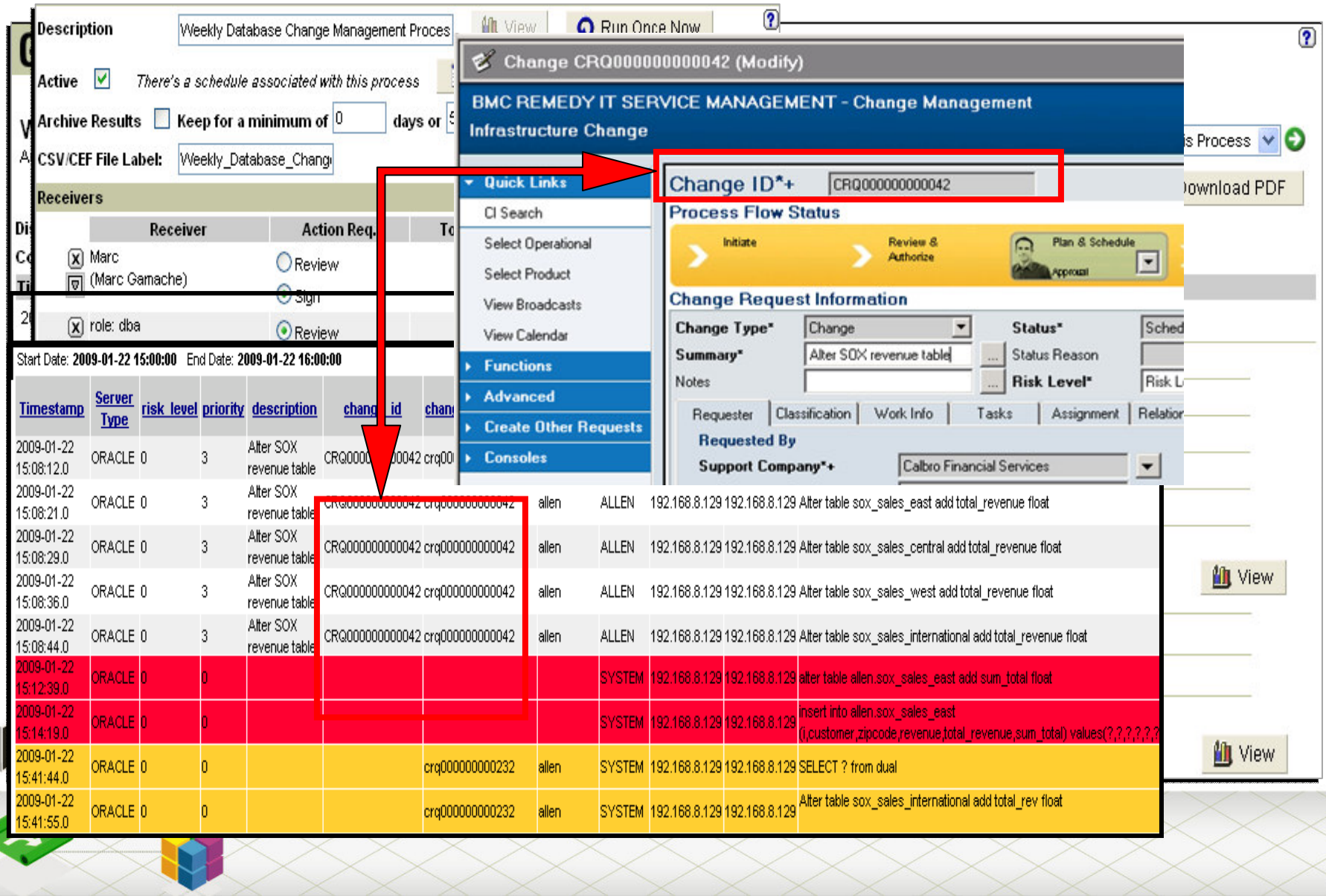


Historical Progress or Regression

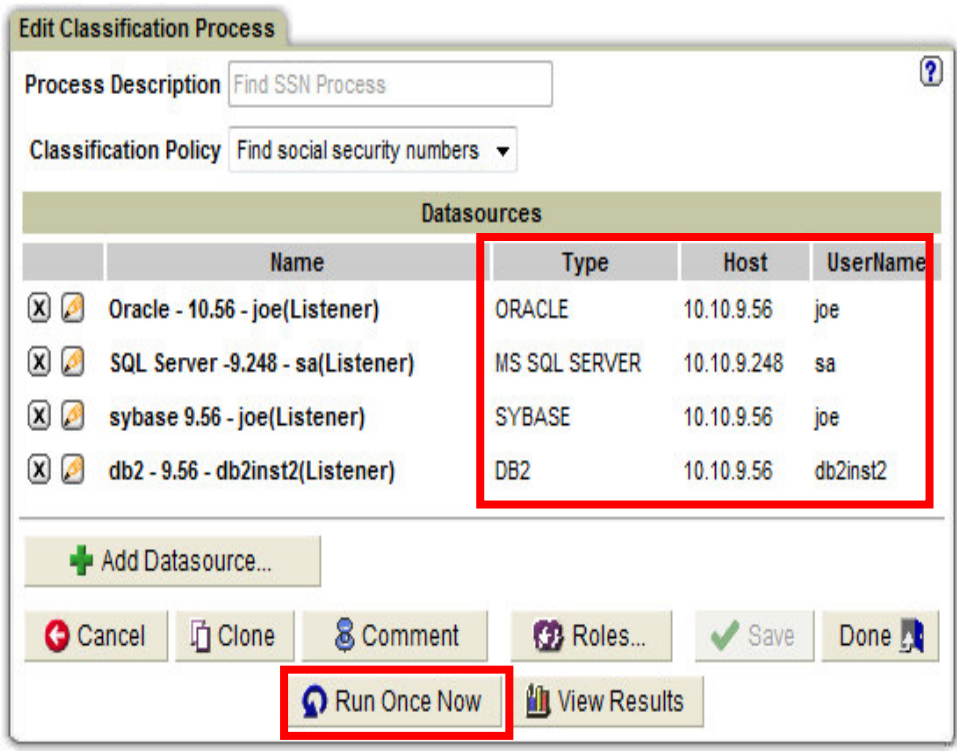
Filter control for easy use



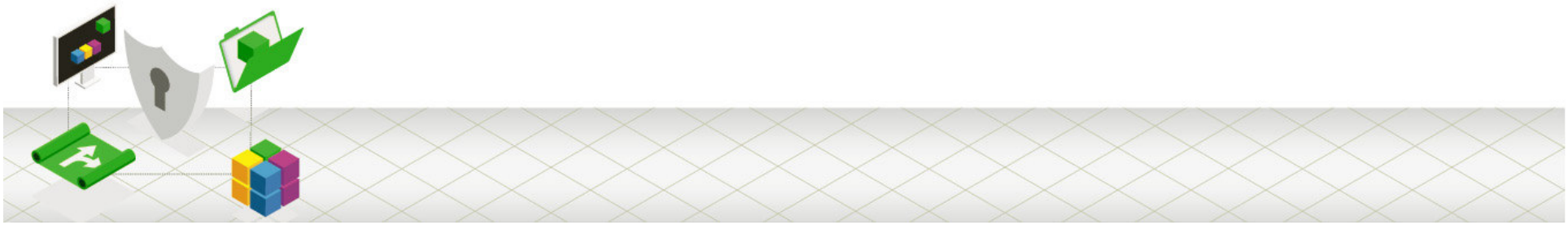
Compliance: Sign-off & Escalation



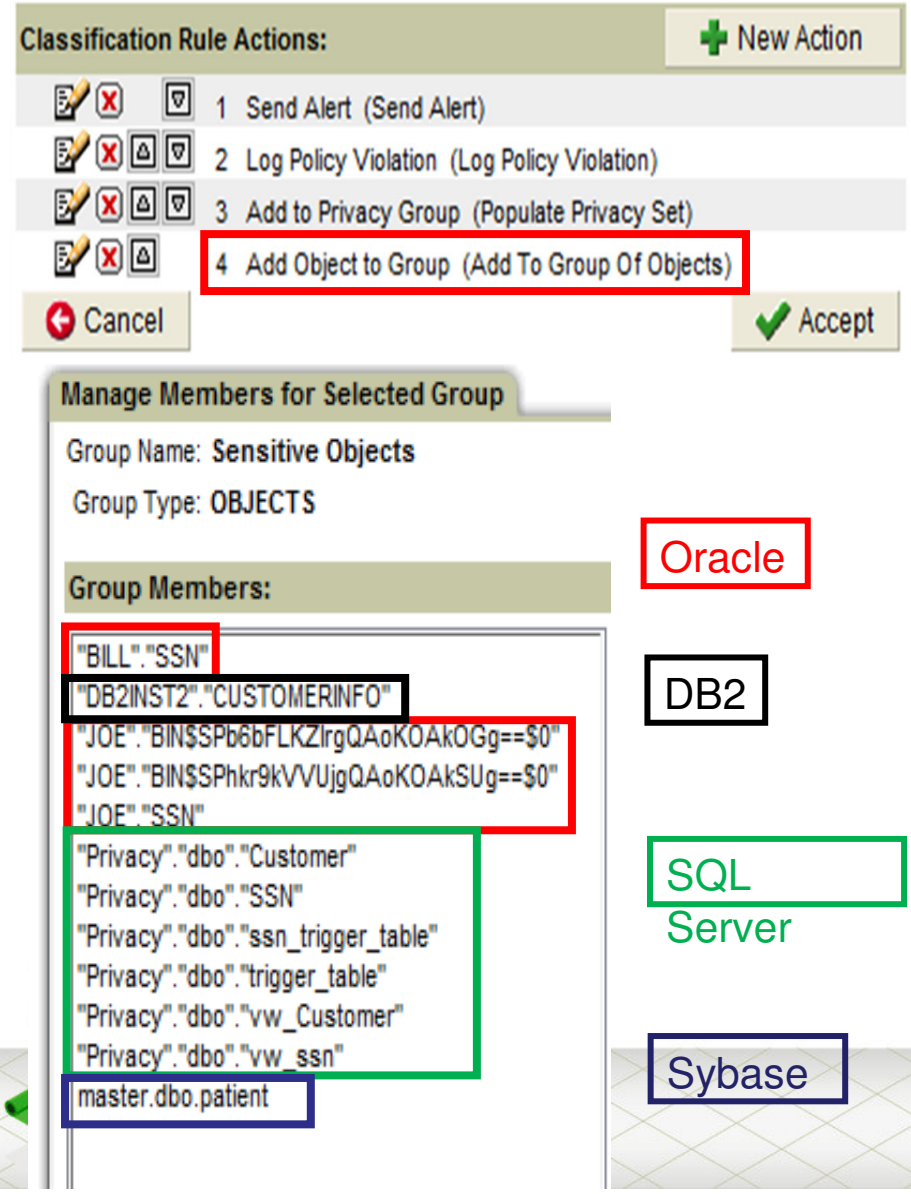
Ricerca dati sensibili - “Find SSN Policy”



- Scan su diversi DBMS (Datasource):
  - DB2
  - SQL Server
  - Sybase
  - Oracle
- Processo singolo/DBMS multipli: risparmio di tempo nel set-up e nella verifica dei risultati.



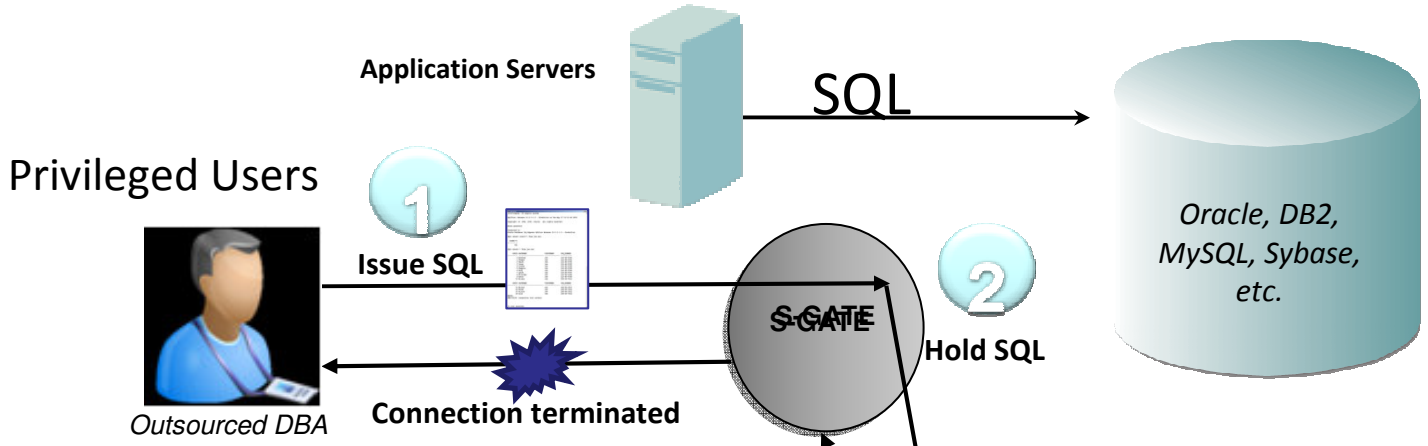
Risultati dello scan



- SSN su 4 tipi di DBMS diversi, individuati tramite unica definizione di policy
  - Oracle
  - DB2
  - SQL Server
  - Sybase
- Oggetti trovati → posti in gruppo
- A seguire, security control impostati a livello dell'intero gruppo.

S-GATE: Blocco preventivo degli acessi

"DBMS software does not protect data from administrators, so DBAs today have the ability to view or steal confidential data stored in a database." Forrester, "Database Security: Market Overview," Feb. 2009

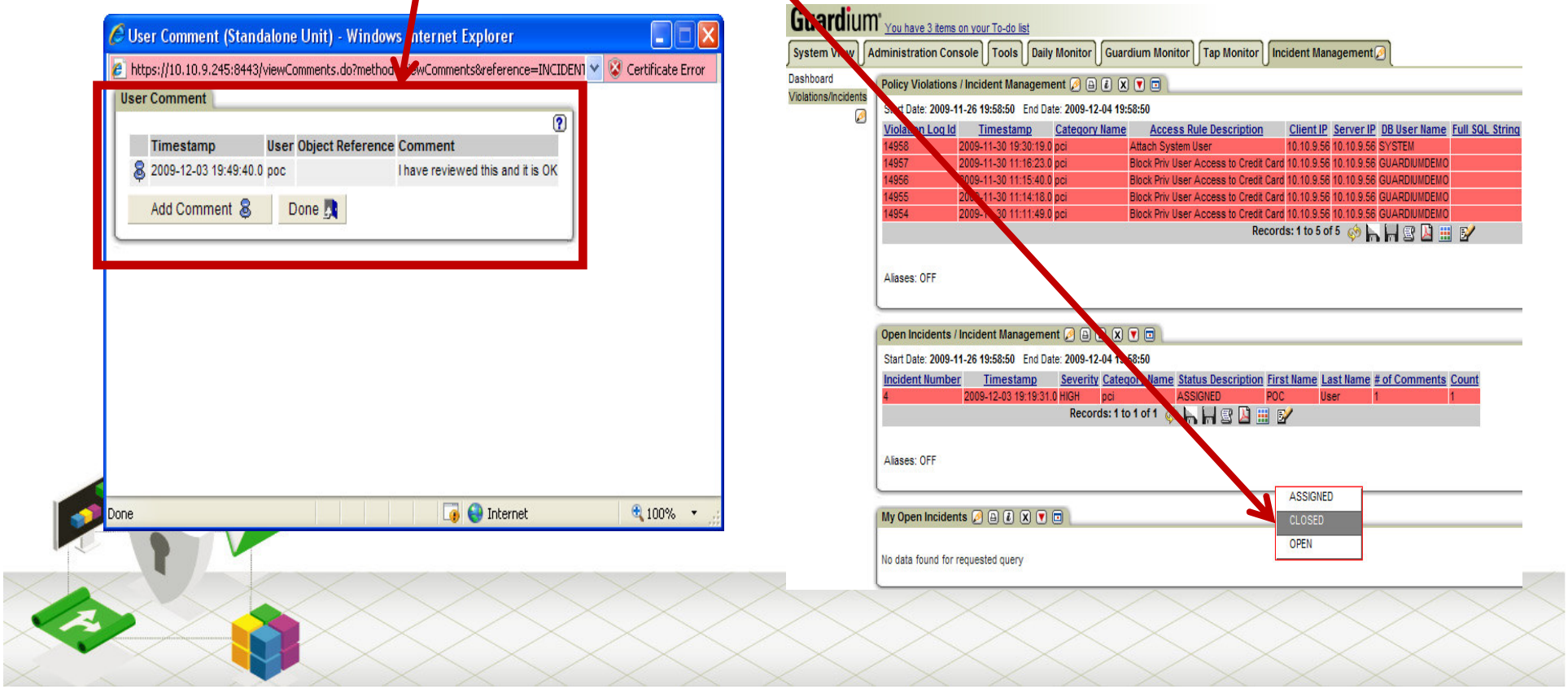



```
root@osprey:~
[root@osprey ~]# sqlplus system

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>
```

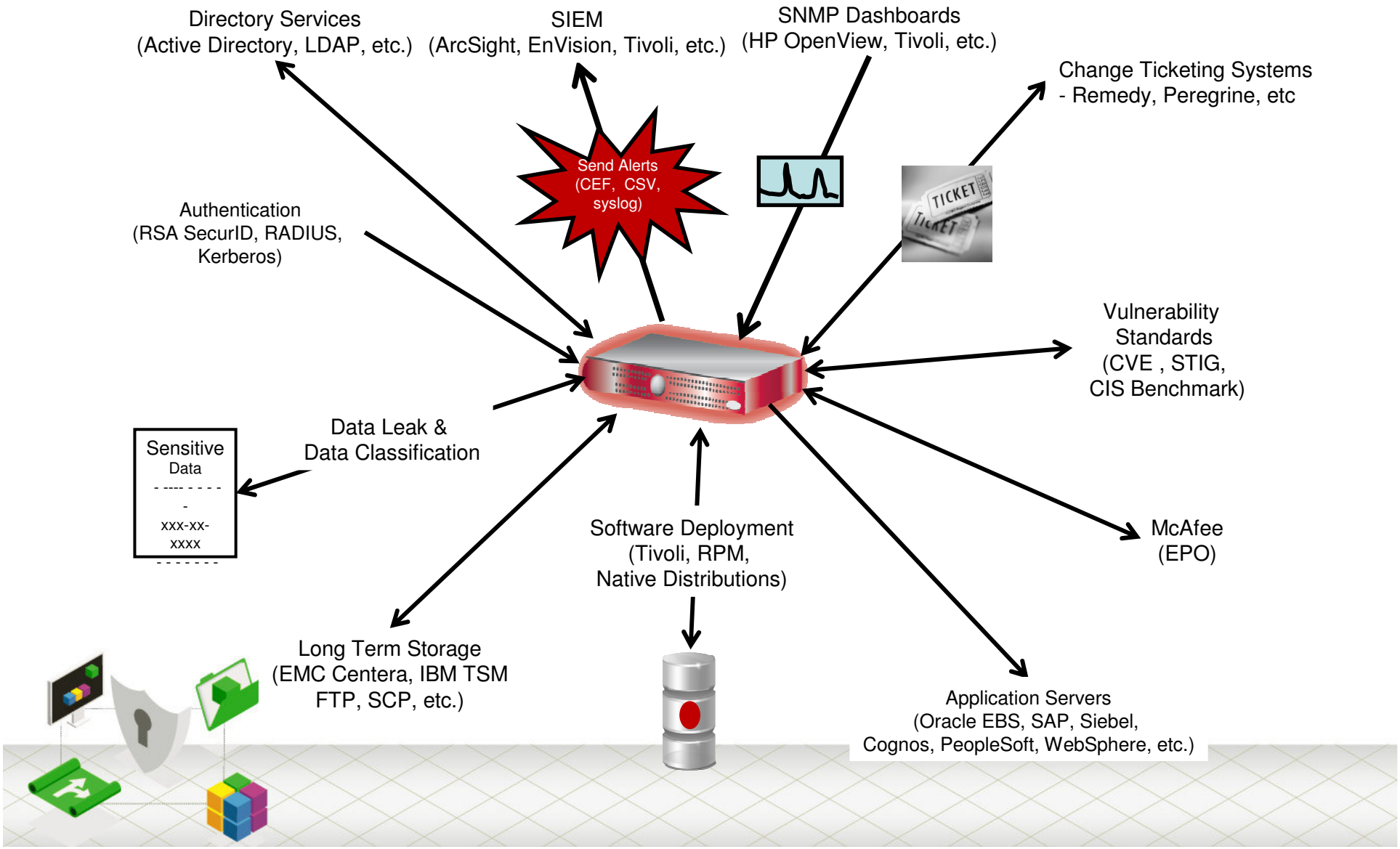
Sessione Terminata

Workflow: apertura di *incident*

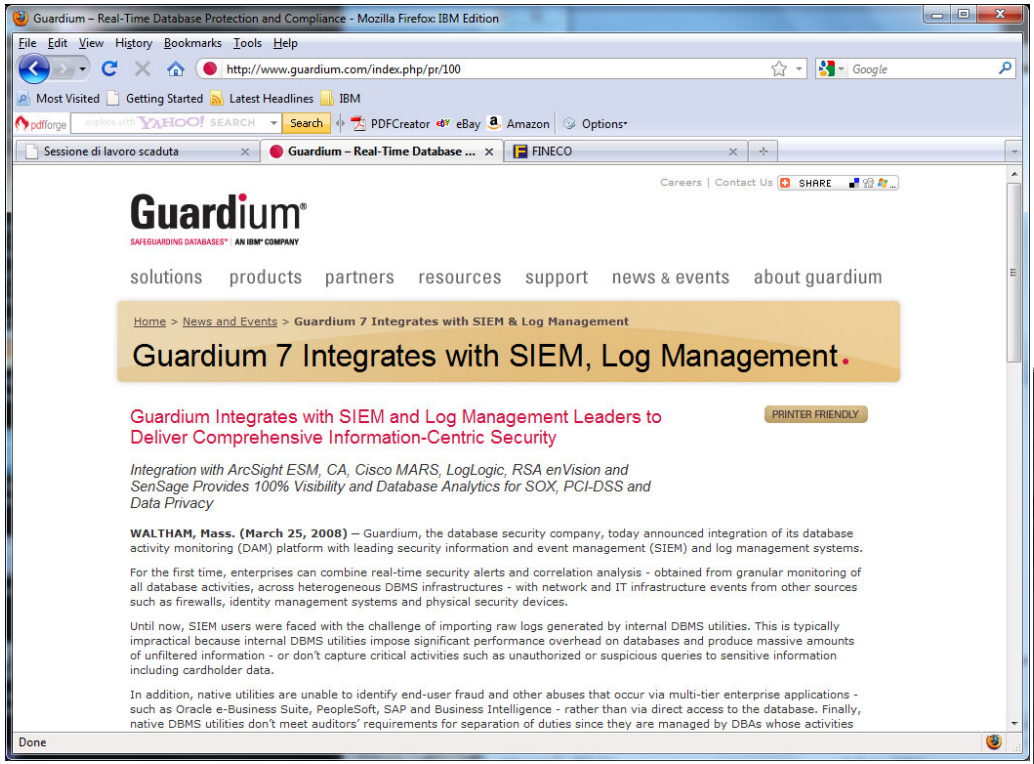
1. Violation associated to an incident
2. Incident reported to attention of responsible(s)

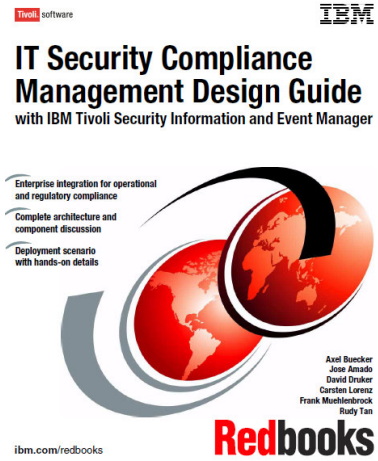


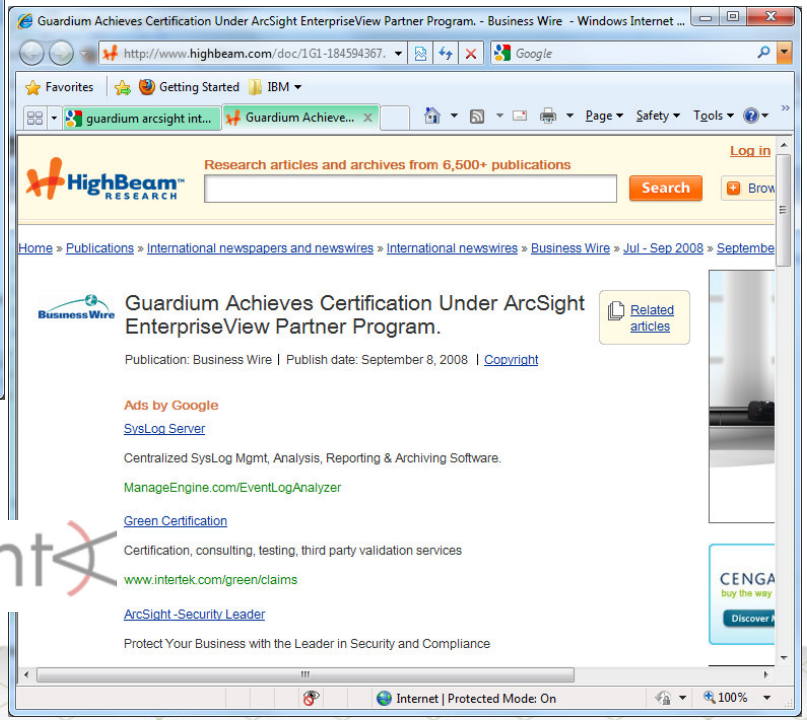
Integrazione nelle infrastructure



Integration w/ SIEM







Certificazioni

Supported Platforms	Supported Versions
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
IBM DB2 UBD (Windows, Unix, z/Linux)	8.0, 8.2, 9.1, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 UBD for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 8, 9, 10,11
MySQL	4.1, 5.0, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02

Referenze

- 5 of the top 5 global banks
- 2 of the top 3 global retailers
- 3 of the top 5 global insurers
- 2 of the world's favorite beverage brands
- The most recognized name in PCs
- 15 of the world's leading telcos
- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

Financial Services Firm with 1M+ Sessions/Day

- **Who:** Global NYSE-traded company with 75M customers
- **Need:** Enhance SOX compliance & data governance
  - *Phase 1*: Monitor all 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 performance 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 for SOX with sign-off by oversight teams
  - Automated change control reconciliation using ticket IDs
  - Passed 2 external audits

Major Retailer with PCI & SOX Controls

- **Who:** National retailer with $50B+ in sales & 6,400 stores
- **Need:** Initially PCI, then extended to SOX, SAS70, data privacy
- **Environment:** 5 major data centers (via M&A)
  - Oracle, SQL Server, DB2, UDB on AIX, Solaris, Windows
  - Dell, IBM midrange, Sun, IBM Z10 on RACF
  - PeopleSoft, SAP plus proprietary claims engines
- **Alternatives considered:**
  - Native auditing; DB encryption; DB appliance from major security vendor
- **Results:**
  - Implemented in ~ 4 weeks
  - PCI certified in stipulated time, saving millions in potential penalties
  - Requirement 3.4: Compensating control for DB encryption
  - Requirement 6: Maintain secure systems (enforce change controls)
  - Requirement 10: Track & monitor all access to cardholder data [automated]
  - Failed DB calls identified for performance optimization
  - Load distribution quantified between servers

Global Manufacturer with 239% ROI

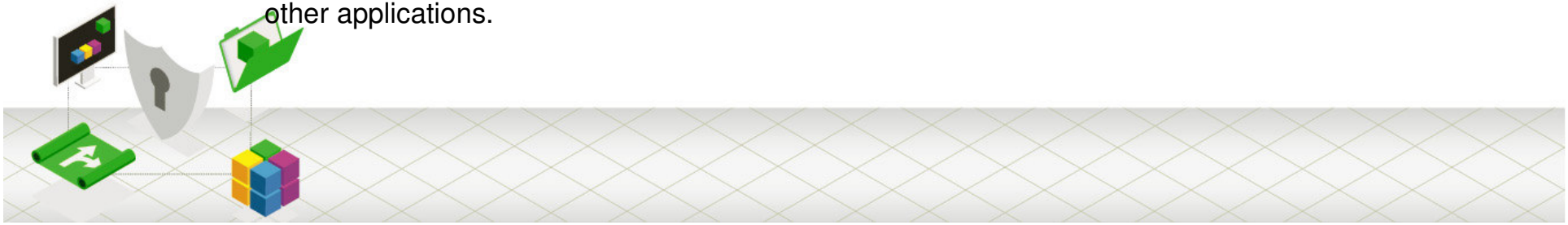
Commissioned Forrester Consulting Case Study

- **Who:** F500 consumer food manufacturer ($15B revenue)
- **Need:** Secure SAP & Siebel data
  - Enforce change controls & implement consistent auditing
- **Environment:**
  - SAP, Siebel, Manugistics, IT2 + 21 other KFS
  - 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. The other products didn't have that capability to automatically put in an associated ticket number with the activity that was going on within the database, which is something the auditors ask about."*

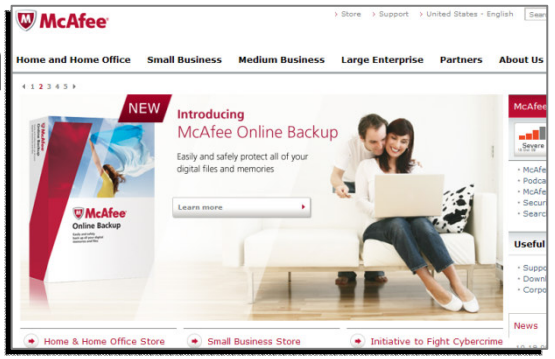
      Lead Security Analyst
  - Strategic focus on data security
    - *"There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers. We now have a clearer focus on security and compliance, promoted in large part by the presence and operation of the Guardium product."*

Major European Telco

- **Who:** Global telco with 70M mobile customers; €30B revenue.
- **Need:** Ensure privacy of call records for compliance with data privacy laws.
  - Phase 1: Safeguard OSS systems
  - Phase 2: Safeguard BSS systems
- **Environment:** 15 heterogeneous, geographically-distributed data centers
  - Oracle, SQL Server, Informix, Sybase
  - HP-UX, HP Tru64, Solaris, Windows, UNIX
  - SAP, Remedy plus in-house applications (billing, Web portal, etc.)
- **Alternatives considered:** Native auditing; Oracle Audit Vault.
  - Not practical because of performance overhead; lack of granularity; non-support for older versions; need for multi-DBMS support.
- **Results:**
  - Deployed to 12 initial data centers in only 2 weeks!
  - Now auditing all traffic in high-traffic environment; centrally managed.
  - Passed several external audits
  - Future plans: Implement application user monitoring; 2-factor authentication; expand scope to other applications.



Guardium Safeguards McAfee.com

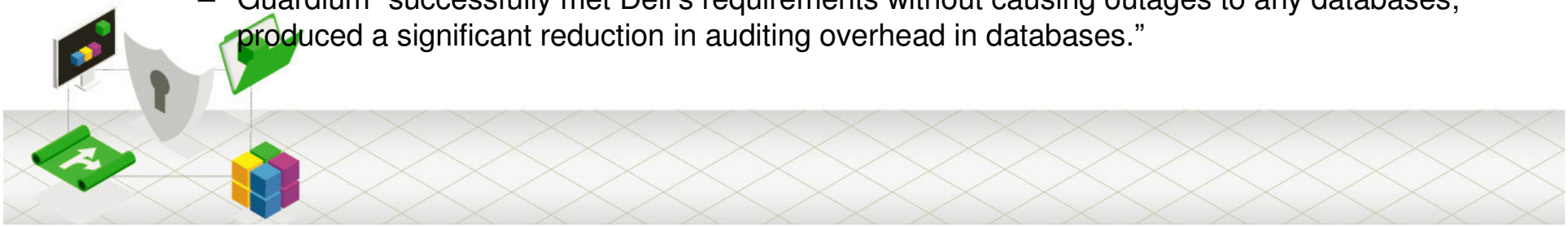


- **Who:** World's Largest Dedicated Security Company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (e.g., Comcast, COX Communications)
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered 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; 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."*
  - *"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 technology also automates our PCI database controls and reduces DBA workload while enforcing separation of duties to protect against both internal and external threats."*
    (Tony Gunn, director of security engineering, McAfee)

Simplifying Enterprise Security for Dell

Published case study in Dell Power Solutions

- **Need:**
  - Improve database security for SOX, PCI & SAS70
  - Simplify & automate compliance controls
- **Guardium Deployment:**
  - Phase 1: Deployed to 300 DB servers in 10 data centers (in 12 weeks)
  - Phase 2: Deployed to additional 725 database servers
- **Environment :**
  - Oracle & SQL Server on Windows, Linux; Oracle RAC, SQL Server clusters
  - Oracle EBS, JDE, Hyperion plus in-house applications
- **Previous Solution:** Native logging (MS) or auditing (Oracle) with in-house scripts
  - Supportability issues; DBA time required; massive data volumes; SOD issues.
- **Results:** Automated compliance reporting; real-time alerting; centralized cross-DBMS policies; closed-loop change control with Remedy integration
  - Guardium “successfully met Dell’s requirements without causing outages to any databases; produced a significant reduction in auditing overhead in databases.”



Washington Metropolitan Area Transit Authority (Metro) Safeguards Customer Information

- **Who:** The Metro operates the 2nd largest U.S. rail transit system and transports more than a third of the federal government to work
- **Need:** Metro needed to safeguard sensitive customer data and simplify compliance with PCI-DSS -- without impacting performance or changing database configurations
  - Protecting customer data
  - Passing audits more quickly and easily
  - Monitoring for potential fraud in PeopleSoft system
  - Leveraging scalable architecture; automated oversight workflows (electronic sign-offs, escalations); library of best practices PCI policies and reports; application-layer monitoring
- **Environment:**
  - More than 9 million transactions per year (Level 1 merchant)
  - Complex, multi-tier heterogeneous environment
- **Alternatives considered:** Native logging and auditing impractical
- **Customer Impact**: "Our customers trust us to transport them safely and safeguard their personal information."
  - "We looked at native DBMS logging and auditing, but it's impractical because of its high overhead, especially when you're capturing every SELECT in a high-volume environment like ours. In addition, native auditing doesn't enforce separation of duties or prevent unauthorized access by privileged insiders."

What Customers Are Saying About Guardium

"The integrity and confidentiality of our ERP, financial and customer data are paramount to our company and enable us to serve our millions of customers safely, reliably and efficiently. We have selected Guardium's real-time database monitoring and compliance automation solution to help us meet our compliance goals for database monitoring."

Cindy Peluso, Director of Information Security, National Grid

"Guardium's technology was key to helping us pass our SOX audit. In the past, we spent hours and hours reviewing logs, but we didn't have real-time controls or the detailed information required by our auditors. We also tried agent-based change control solutions, but they didn't work. The Guardium system gives us both real-time alerting and granular audit reporting while automating the entire process. This helps us meet our auditors' requirements while saving us several hundred hours a year in staff time."

Robert G. Gorrie, Corporate Information Security Manager, USEC
($1B NYSE-traded nuclear energy company)

"Guardium's innovative network-based technology monitors, protects and audits access to key information assets at ING Investment Management."

Charles Kim, Information Security Officer, ING Investment Management

"[Guardium's technology] enabled the customer to improve database security … without impacting the performance of critical business applications."

Forrester Consulting Commissioned Case Study
$10B NYSE-traded energy company

Validated by Industry Experts

FORRESTER®

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

ChannelWeb

"Most Powerful Compliance Regulations Tools ... Ever"

SC MAGAZINE

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based s[illegible]."

the 451 group

"Guardium is ahead of the pack and gaining speed."

"Guardium is ahead of the pack and gaining speed."

InformationWeek

[illegible]

"Practically every feature you'll nee[illegible] sensitive data."

RED HERRING N. AMERICA WINNER 100

SQL SERVER MAGAZINE

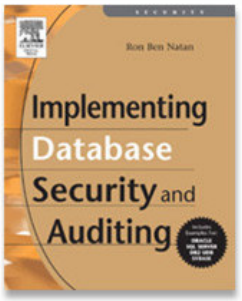
2007 Editor's Choice Award in "Auditing and Compliance"

INFORMATION SECURITY MAGAZINE

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

INFORMATION SECURITY Hotpick

+ info …



- Check out *Implementing Database Security and Auditing*
  - Definitive 413-page text for security, risk management & database professionals
  - Specific tips for DB2, Oracle, SQL Server, MySQL and Sybase
  - Written by database security expert, IBM GOLD Consultant & Guardium CTO, Ron Ben Natan, Ph.D.
  - Free chapter download: www.guardium.com/index.php/landing/520
- See "Resources" section for case studies, ROI examples, white papers & lab reviews
- Check out the *Database Security TechCenter* by Dark Reading
  - Latest news, tips & reports
  - www.darkreading.com/database_security/

Grazie!