Guardium®
SAFEGUARDING DATABASES™

Enterprise Database Security & Monitoring: *Guardium Overview*

Phone: 781.487.9400

Email: info@guardium.com

Guardium: *Market-Proven Leadership*

Vision

Enterprise platform for securing critical data across your database & application infrastructure.

Customer Proven

Most widely-used solution for database activity monitoring, security & auditing.

Safeguarding 100,000+ databases in the most demanding datacenter environments worldwide

Technology

100% visibility & intelligence -- with no impact on performance or IT infrastructure.

11 patents pending in database security, monitoring, logging, access control, analytics and storage

Heterogeneous Support

DBMS
- Oracle
- Microsoft
- IBM DB2
- IBM Informix
- Sybase ASE, IQ
- Others

Applications
- Oracle EBS
- PeopleSoft, JDE
- Siebel
- SAP
- Custom & other packaged apps

OS
- Solaris
- HP-UX
- AIX
- z/OS
- Linux
- Windows

DB Protocols
- TCP
- IPC
- SHM
- Named Pipes
- Oracle BEQ
- TLI

Authentication
- LDAP
- Kerberos
- RSA SecurID

Technology partners
- BMC
- IBM
- EMC
- NEON (mainframe)
- NetApp (encryption)

Independent Validation

FORRESTER®

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

SC MAGAZINE

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

INFORMATION SECURITY MAGAZINE

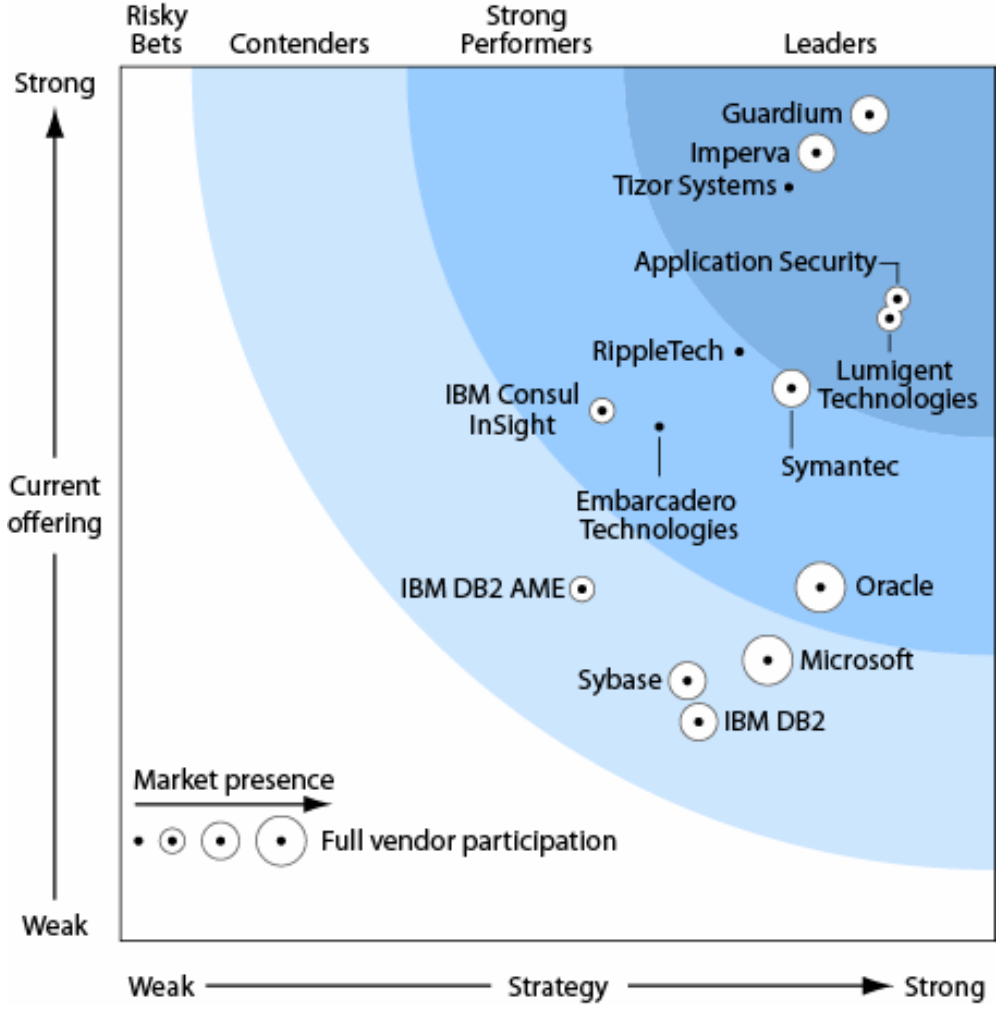
"**Enterprise-class** data security product that should be on every organization's radar."

CISCO

Strategic Investor

Highest Overall Score for Current Offering, Corporate & Product Strategy

- "Dominance in this space."
- "A Leader across the board."
- #1 score for Architecture
- "Leadership in supporting large heterogeneous environments,… high performance and scalability, simplifying administration …and real-time database protection."
- "Strong road map ahead with more innovation and features."



Source: "The Forrester Wave™: Enterprise Database Auditing and Real-Time Protection, Q4 2007" (October 2007)

Guardium®

Top Data Protection Challenges

Where is my sensitive data located & who is using it?

How can I enforce access & change control policies for critical databases?

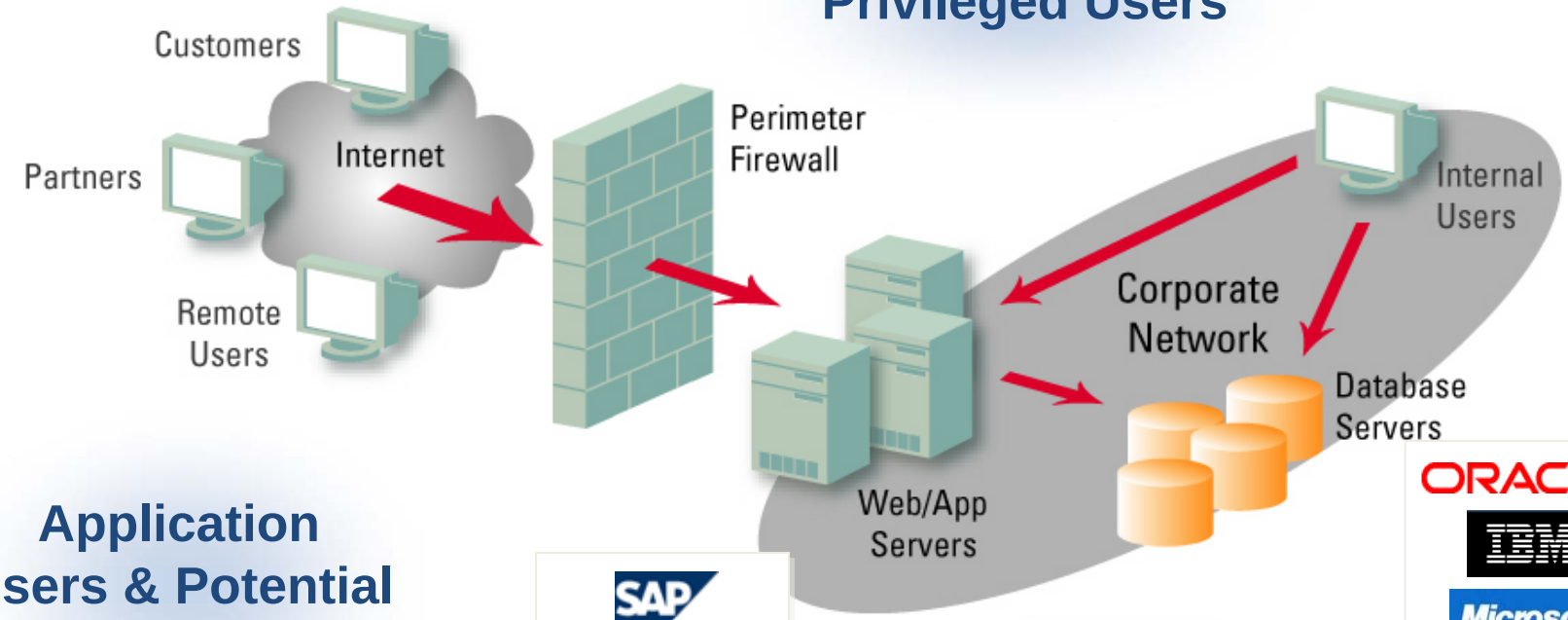
How do I simplify & automate compliance?

Top Regulations Impacting DB Security

Audit Requirements	CobiT (SOX)	PCI DSS	National Data Privacy Laws	CMS ARS	GLBA & HIPAA	ISO 17799 (Basel II)	NERC	NIST 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*

The Data Security Challenge: Limited Controls => Undue Risk



Address Security, Risk Management & Compliance

Monitor Privileged User Activity

- Changes to DBs (schemas, data, configurations)
- Access to sensitive data
- Permissions & elevation of privileges

Secure Web & Application Server Requests

- Pooled connections (Oracle Financials, SAP, etc.)
- End-user fraud
- Potential hackers (e.g., SQL Injection)

Simplify Complex Environments

- Silos of database logs
- Multiple OS & DBMS platforms (distributed & MF)
- Diverse connection mechanisms (local & network)
- Separate compliance initiatives & retention needs

Guardium Solution: Addressing Key Stakeholders

SECURITY OPERATIONS

- ✓ Real-time policies
- ✓ Secure audit trail
- ✓ Data mining & forensics

COMPLIANCE AUDIT

- ✓ Separation of duties
- ✓ Best practices reports
- ✓ Automated controls

APPLICATION & DATABASE

- ✓ Minimal impact
- ✓ Change management
- ✓ Performance optimization

Guardium: 100% Visibility & Unified View

Guardium®

100% Visibility & Intelligence

Suite of security, compliance & data management applications

Real-time SQL event data	Audit log data repository

Network collectors and/or host-based probes

Corporate network

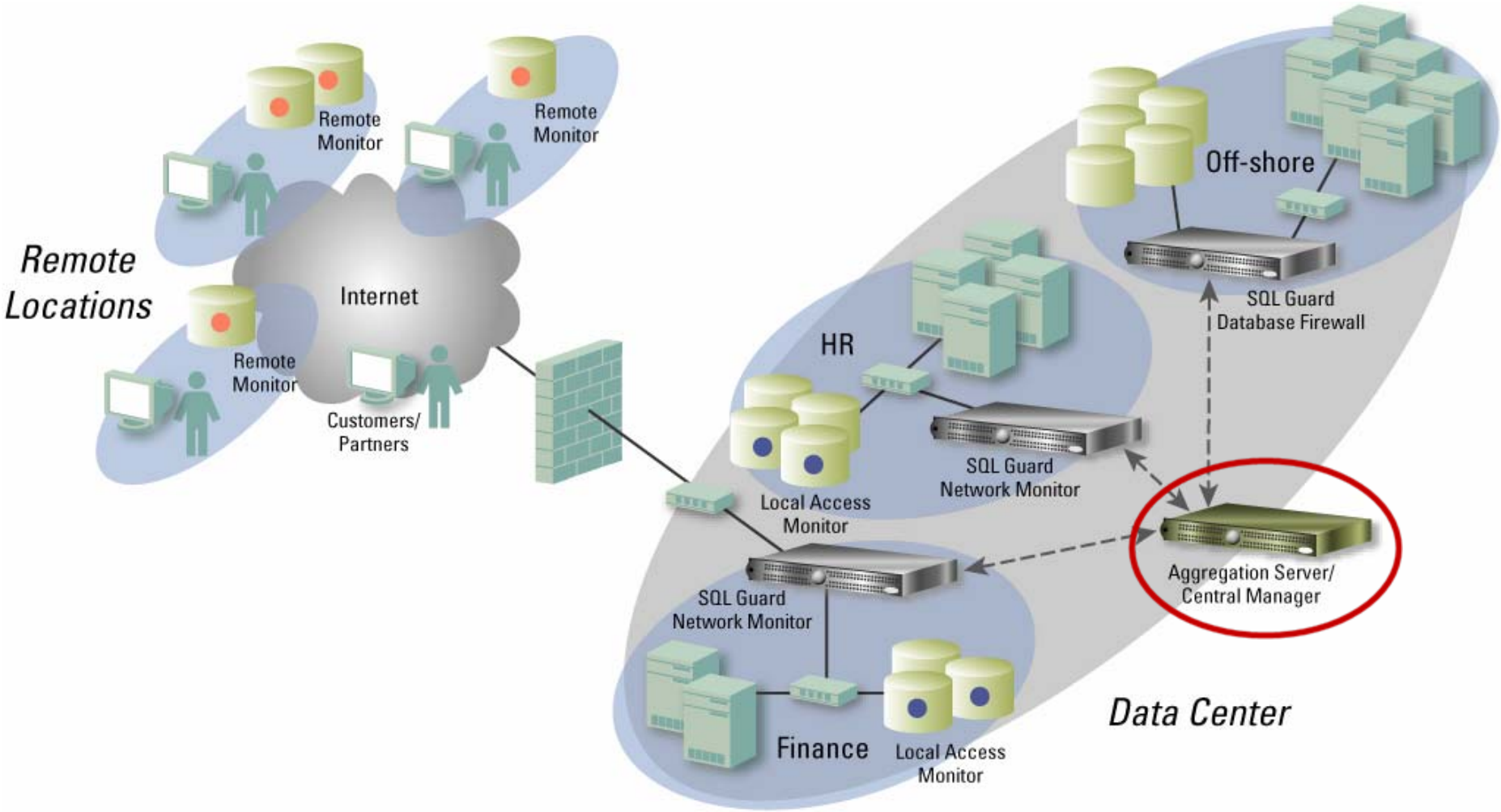
Database servers

S-TAPs

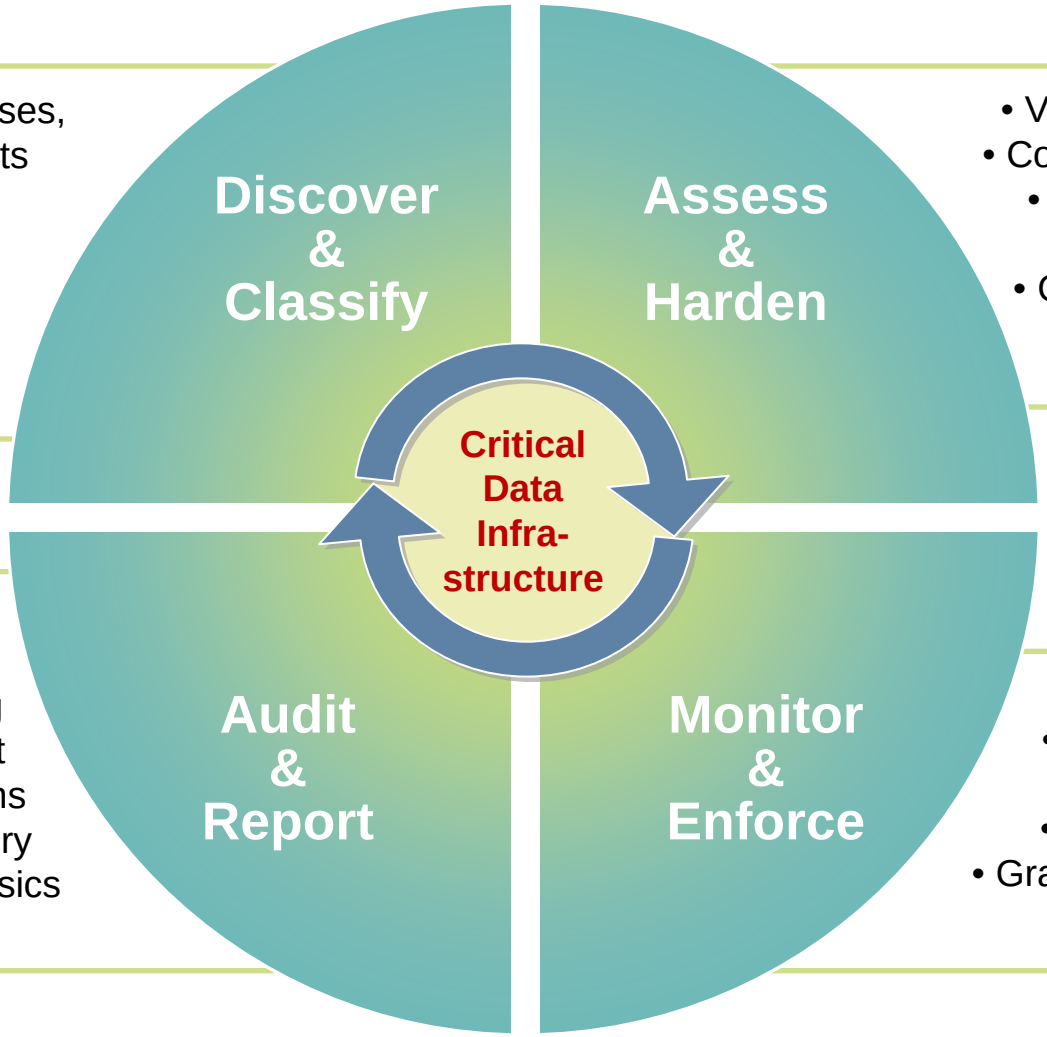
Web/app servers

- *Non-invasive*
- *Cross-platform*
- *Centralized*
- *Automated*

Scalable Multi-tier Architecture



Database Security, Risk Management & Governance Lifecycle



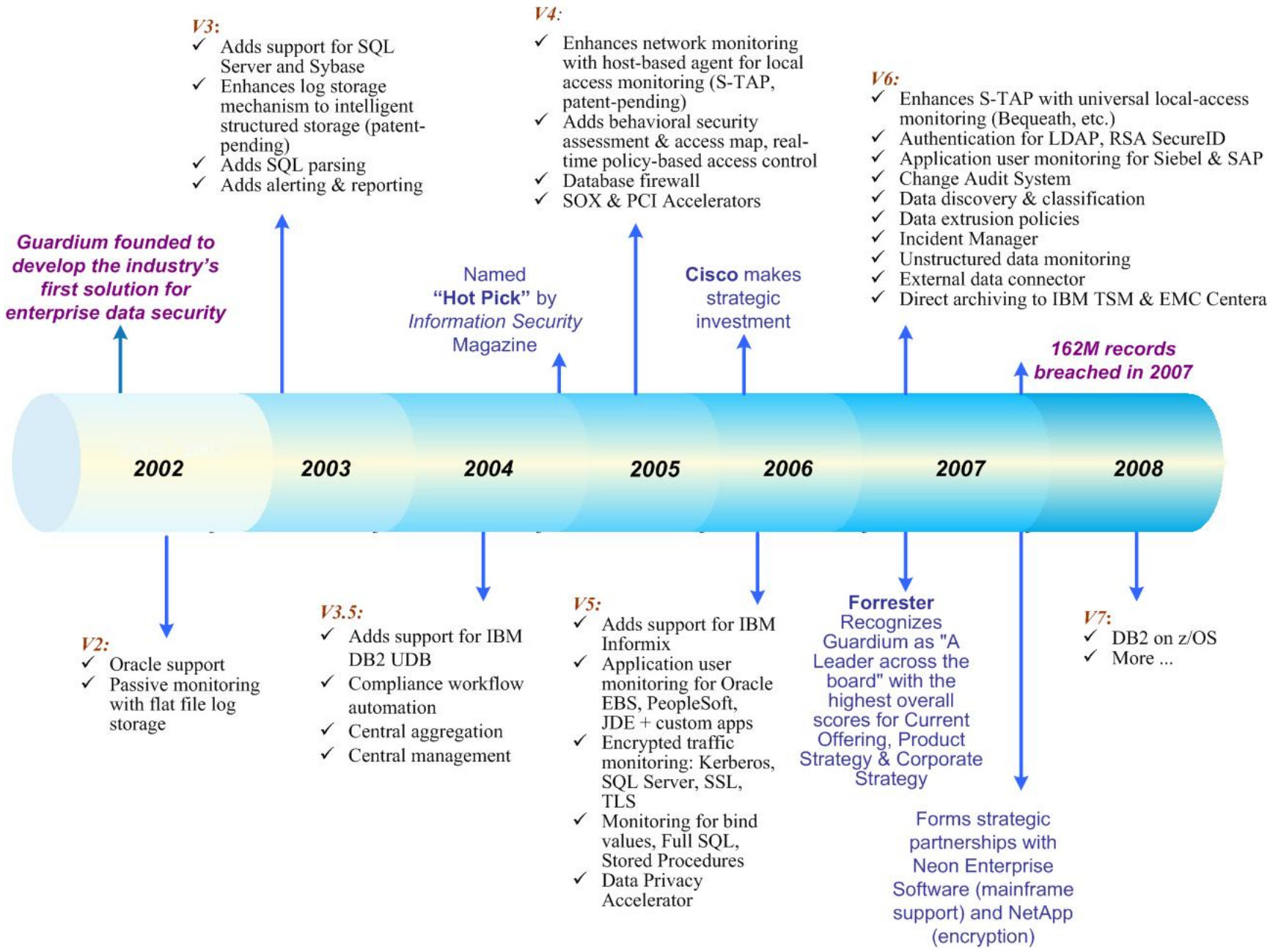
- Discover all databases, applications & clients
- Discover & classify sensitive data

- Vulnerability assessment
- Configuration assessment
- Behavioral assessment
- Baselining
- Configuration lock-down & change tracking
- Encryption

- Centralized governance
- Compliance reporting
- Sign-off management
- Automated escalations
- Secure audit repository
- Data mining for forensics
- Long-term retention

- 100% visibility
- Policy-based actions
- Anomaly detection
- Real-time prevention
- Granular access controls

Proven Vision



Case Study: Global Manufacturer with 239% ROI

- **Who:** **F500 consumer food manufacturer ($15B revenue)**
- **Need:** **Secure SAP & Siebel data for SOX**
  - 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** *(see Forrester Consulting case study)*
  - **Proactive security**: Real-time alert when changes made to critical tables
  - **Simplified compliance**: Passed 4 SOX-related 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."*

Financial Services Firm with 1M+ Sessions/Day

- **Who:** **Global NYSE-traded company with 75M customers**
- **Need:** **Improve database security for 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, DDLs, etc.)
  - Caught DBAs accessing databases with Excel & shared credentials
  - Producing daily automated reports for SOX; sign-off by DB & InfoSec teams
  - Automated change control reconciliation using ticket IDs
  - Passed 2 external audits

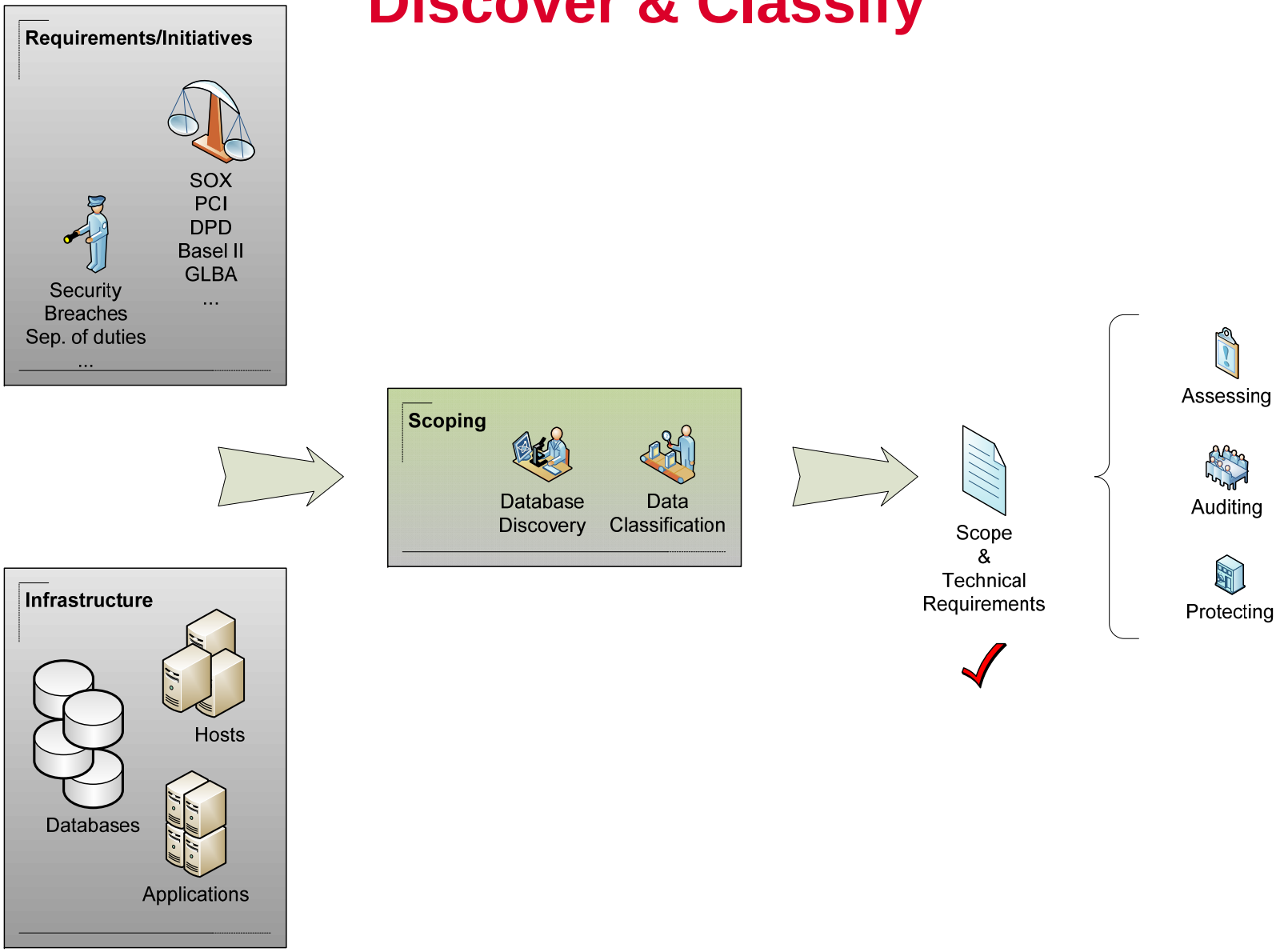
Major Retailer with Multiple PCI Requirements

- **Who: National retailer with 6,000 stores**
- **Need: Address PCI-DSS & protect cardholder data**
  - **without impacting performance or creating more work for DBAs**
- **Environment:** Multiple data centers with Oracle, SQL Server, Sybase, Informix
- **Alternatives considered**
  - Native auditing
  - DB monitoring appliance from major security vendor
- **Results**
  - Compensating control for PCI-DSS Requirement 3.4 (V1.1 Appendix B)
    - Restrict access to cardholder data based on IP address, application, …
    - Restrict logical access to the database independent of LDAP
    - Prevent/detect common application or DB attacks (e.g., SQL injection)
  - Requirement 6: Maintain secure systems
    - Enforce change controls
  - Automated solution for PCI-DSS Requirement 10
    - Track & monitor all access to cardholder data

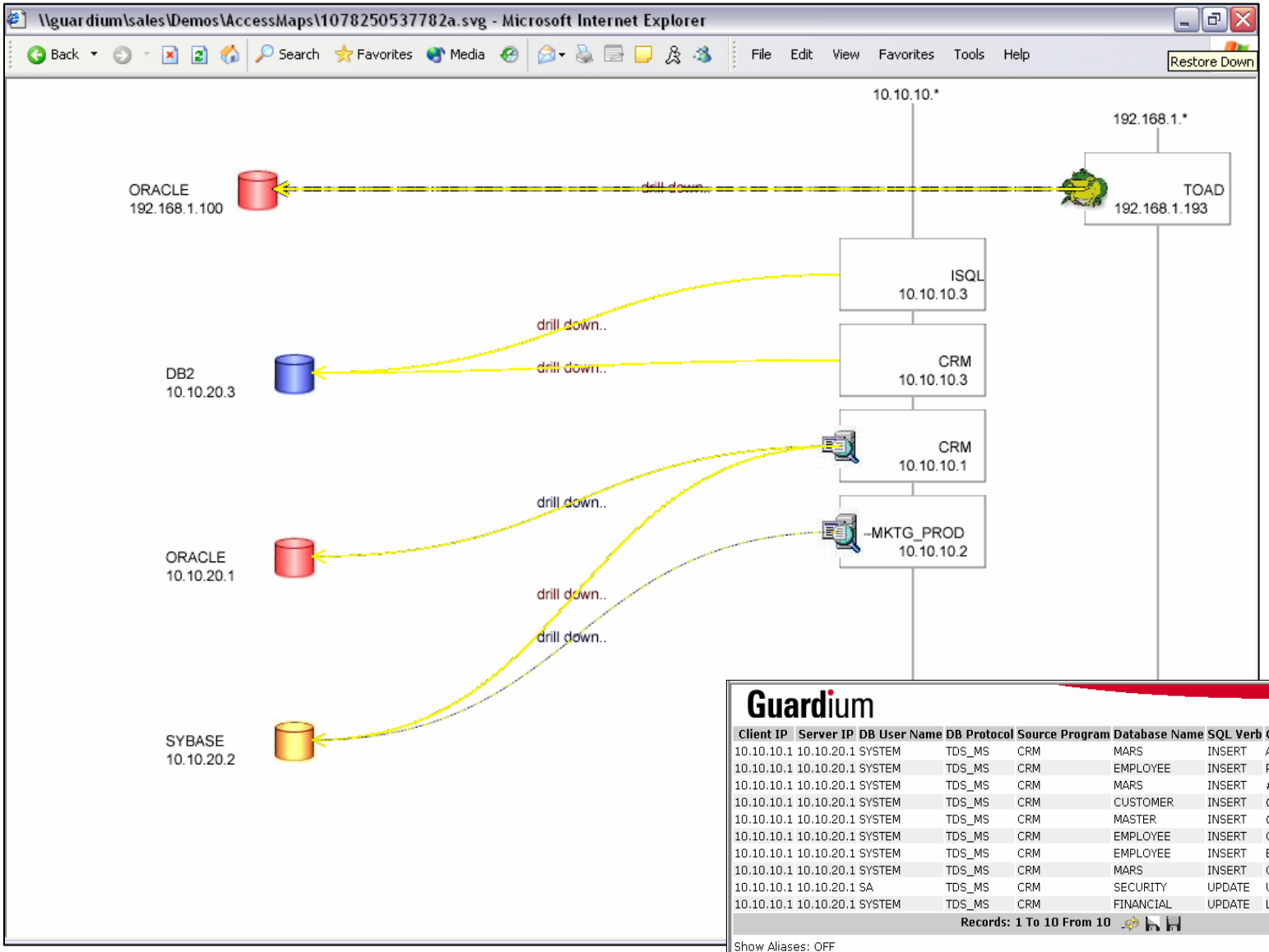
Why Enterprises Choose Guardium

- **Most widely-deployed solution**
  - *Continuously enhanced since 2002, based on real-world enterprise feedback*
- **Most scalable enterprise architecture**
  - *Federated multi-tier system, intelligent data management, efficient storage*
  - *Virtually anything can be automated …*
- **Most flexible**
  - *Multiple collection options, configurable policies, drag-and-drop reports, …*
- **Broadest support for heterogeneous environments**
  - *Database & OS platforms, enterprise applications, LDAP, authentication, …*
  - *Both network & local access (privileged users)*
- **Richest set of applications**
  - *Security & forensics, auditing & compliance reporting, change control, automated workflow & oversight, sensitive data discovery, data mining, correlation…*

Discover & Classify



Database auto-discovery



Drill-down

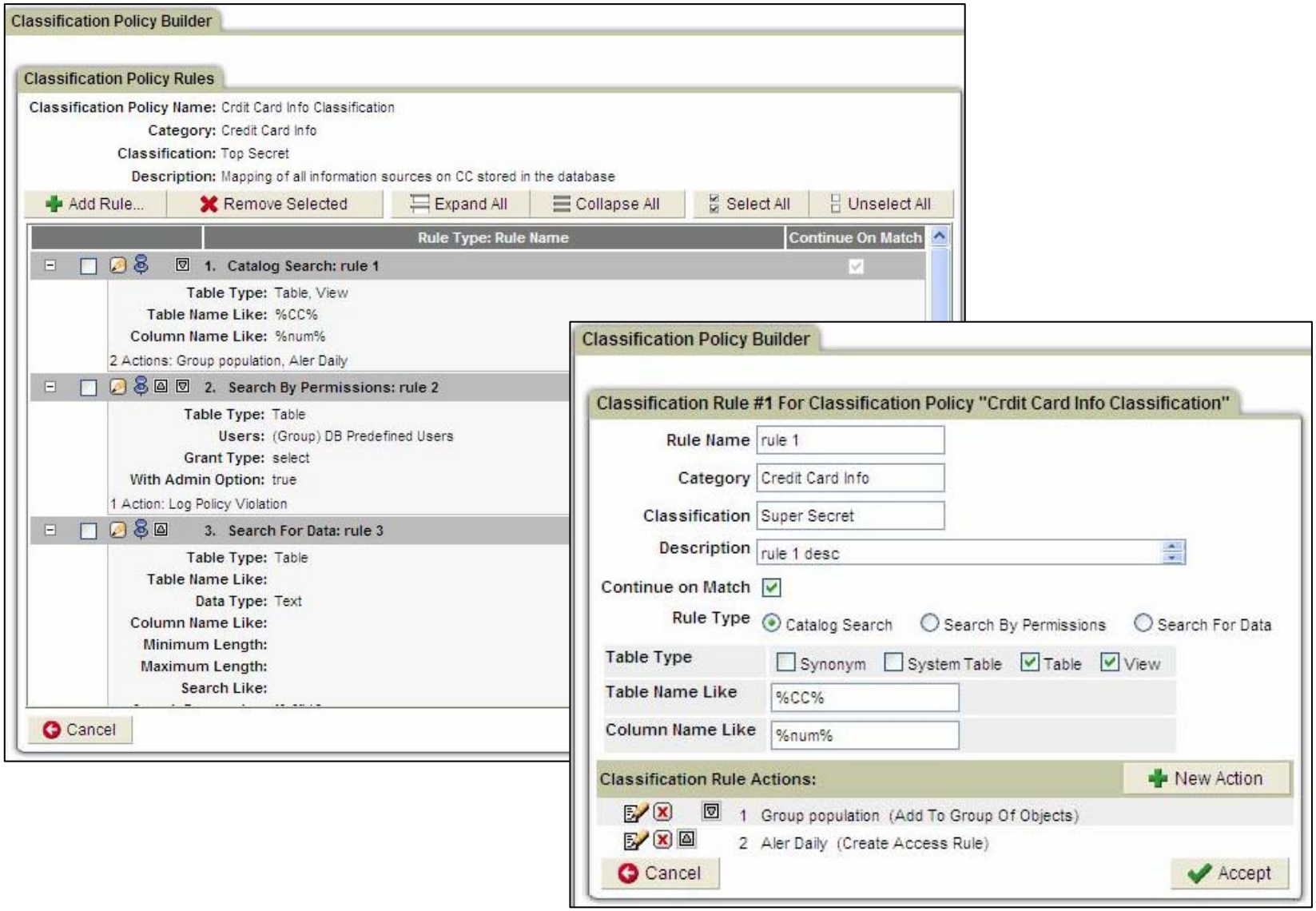
Guardium

Client IP	Server IP	DB User Name	DB Protocol	Source Program	Database Name	SQL Verb	Object Name	Total access
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	MARS	INSERT	ADDRESS	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	EMPLOYEE	INSERT	PHONE	4
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	MARS	INSERT	#EW_CUST	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	CUSTOMER	INSERT	@Counter	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	MASTER	INSERT	@Reports	4
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	EMPLOYEE	INSERT	CHAR	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	EMPLOYEE	INSERT	EMP	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	MARS	INSERT	CUSTOMERS	4
10.10.10.1	10.10.20.1	SA	TDS_MS	CRM	SECURITY	UPDATE	USER_RIGHTS	2
10.10.10.1	10.10.20.1	SYSTEM	TDS_MS	CRM	FINANCIAL	UPDATE	LEDGER	8

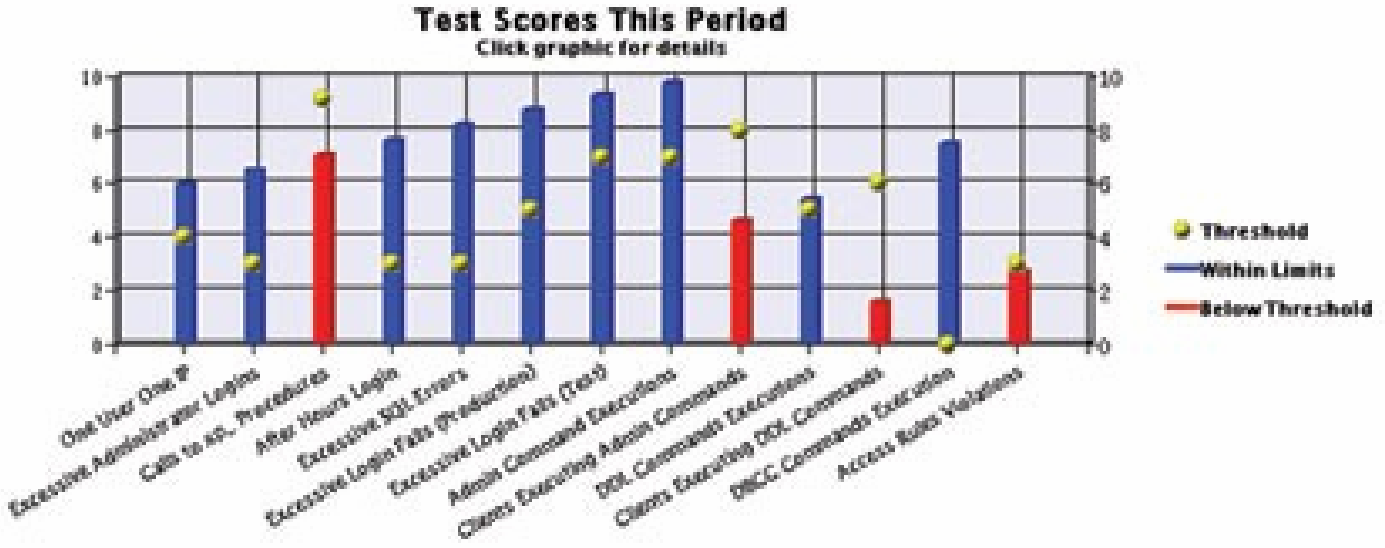
Records: 1 To 10 From 10

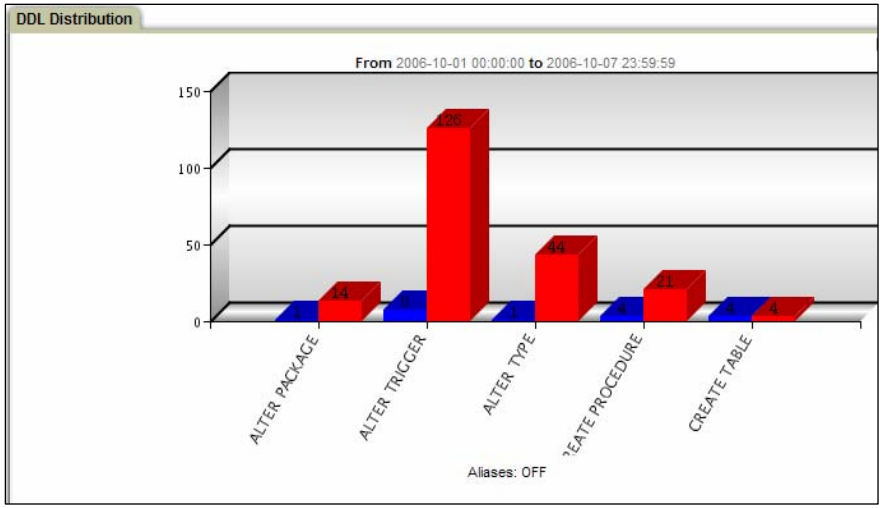
Show Aliases: OFF

Data discovery & classification



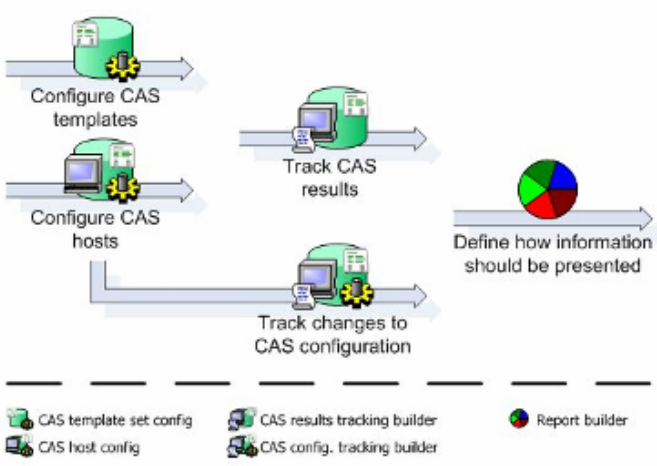
Vulnerability assessment





Track database configuration changes

$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	Environment Variable	12h	✓	⊘
ORACLE_SID	Environment Variable	12h	✓	⊘
TNS_ADMIN	Environment Variable	12h	✓	⊘
select * from dba_db_links	SQL Script	12h	✓	⊘



200+ pre-configured knowledge templates for all major OS/DBMS configurations

Configuration Change History

Start Date: 2007-04-30 14:26:18 **End Date:** 2007-08-08 14:26:18

S-Tap Host	DB Server Type	DB Port From	DB Port To	DB Client IP	DB Client Mask	Timestamp
192.168.200.108	ORACLE	1521	1521	192.168.200.108	255.255.255.255	2007-08-02 14:54:48
192.168.200.108	SYBASE	4200	4200	127.0.0.1	255.255.255.255	2007-08-02 14:54:48

Records: 7 To 8 From 8

Baselining to identify anomalous behavior

- Automatically suggests rules based on profiling
- Prevents unusual activities & attacks such as SQL injection
- Merge new policies as environment changes

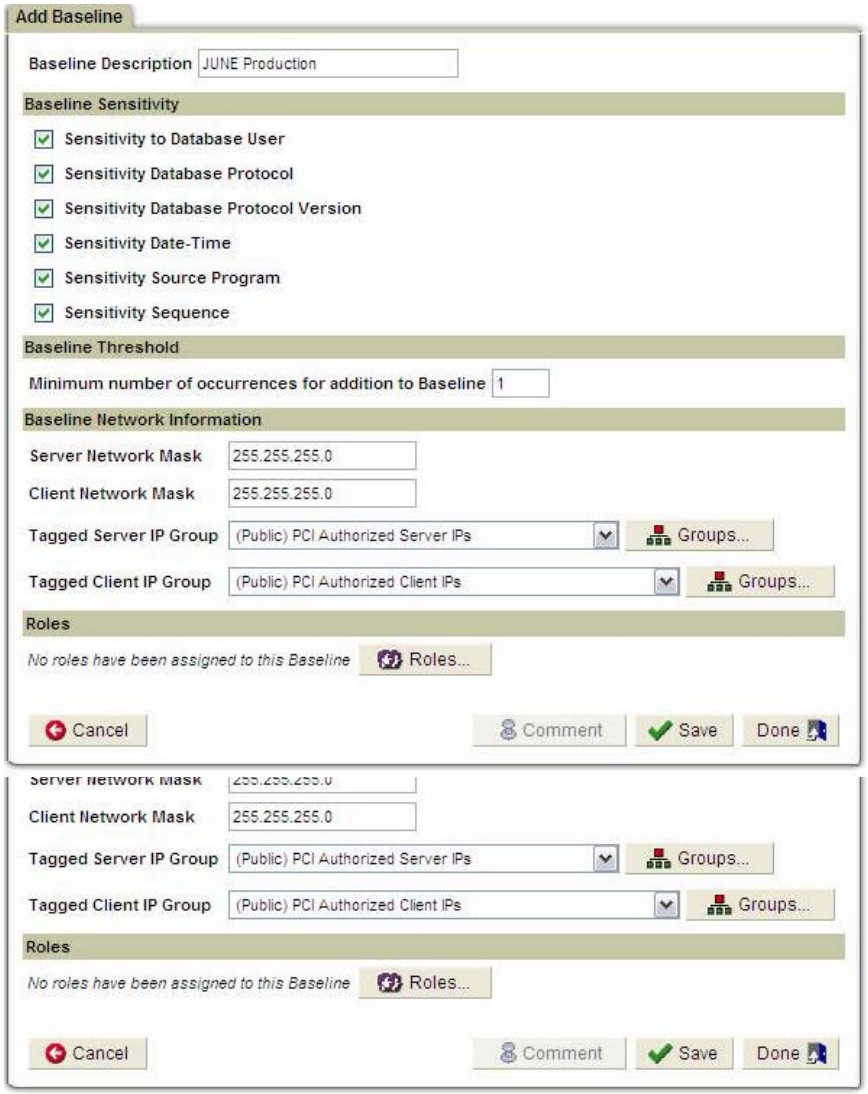
1 Access Rule: Suggested Rule1_2007-06-18 18:19:05 (24235 occurrences)

Cat.	Classif.	Sev.	Client IP	Server IP	Src App.	DB Name	DB User	App. User
ANY	ANY	i	192.168.200.0 / 255.255.255.0	192.168.200.0 / 255.255.255.0	DB2HMON	ANY	DB2INST1	ANY

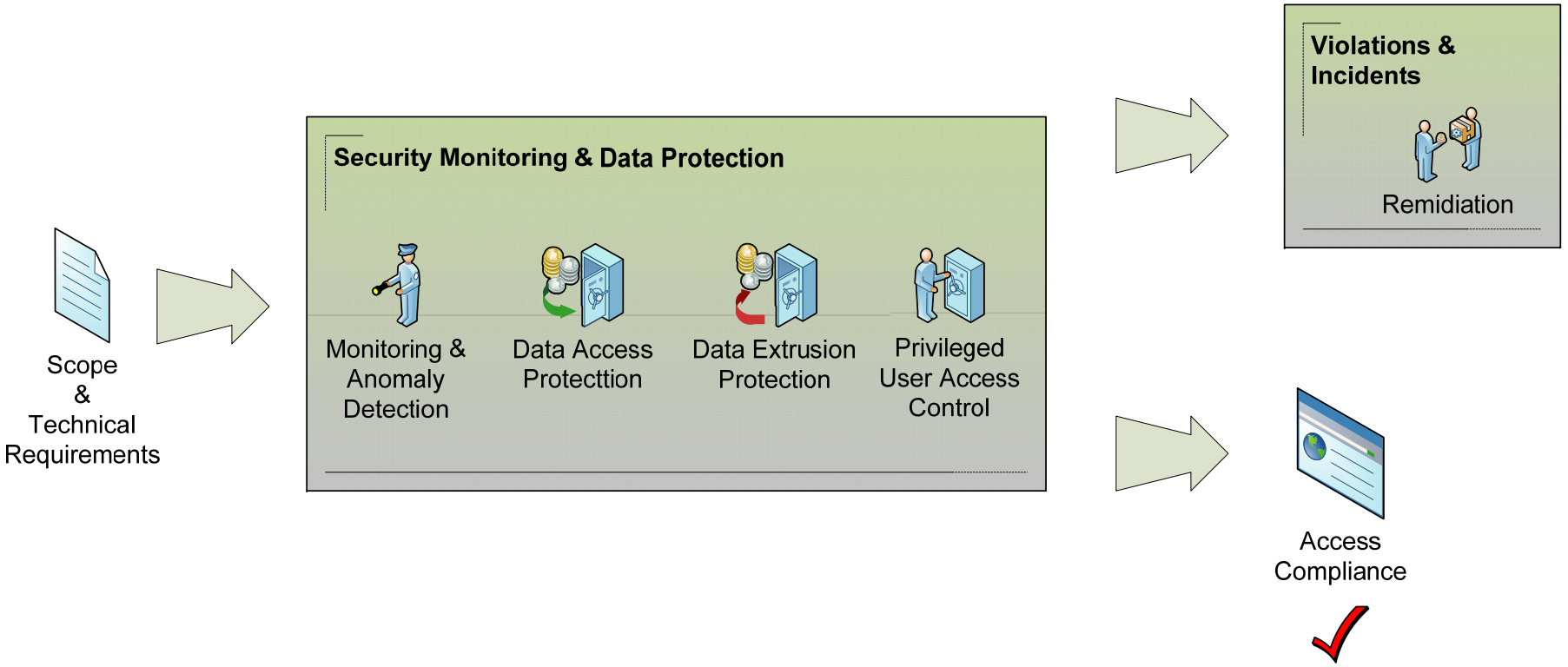
OS User	Service Name	Net. Protocol	Field Name	Pattern	DB Type	Client MAC
ANY	ANY	ANY	ANY	ANY	ANY	ANY

Object	Command	Object/Command Group	Object/Field Group	Period	Min. Ct.	Reset Int.	Action	Rec. Vals.	Cont.
DB2_SYS_OBJ	EXECUTE Commands	ANY	ANY	REGULAR WORK DAY	0	0	☑	☐	☐

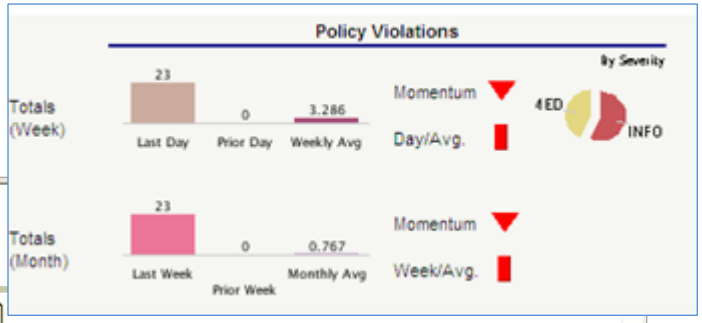
App Event Exists	Event Type	App Event Str. Val.	App Event Num. VaL.	App Event Date	Event User Name
☐	ANY	ANY	ANY	ANY	ANY



Monitor & Enforce



Monitor and …



Guardium You have 1 item on your Audit To-Do list

PCI Accelerator | Data Classification | ROCs

Overview | REG 3 Protect | REG 6 Maintain | REG 7 Restrict | REG 8 Assign | REG 10 Track / Monitor | REG 11 Test | PCI Policy Monitoring

Overview
10.2 and 10.3 Automation
10.2.1 Data Access
10.2.2 Admin Activity
10.2.3 Audit Trail Access
10.2.4 Invalid Access
10.2.6 Initialization Log
10.5 Secure audit trails
10.6 Access Auditing

PCI - Invalid Logical Access Attempts

Start Date: 2004-07-28 18:07:13 End Date: 2007-04-24 18:07:13

DB User Name	Client IP	Server IP	Server Type	Count of Exceptions
39BMBC1\MGamache	192.168.20.107	192.168.200.110	MS SQL SERVER	1
abcd	192.168.20.222	192.168.200.108	ORACLE	1
admin	192.168.20.178	192.168.200.108	INFORMIX	1
bfederman	192.168.20.178	192.168.200.108	DB2	1
bfedermann	192.168.20.107	192.168.200.108	DB2	19
bfedermann	192.168.20.107	192.168.200.108	SYBASE	3
bfedermann	192.168.20.178	192.168.200.108	DB2	10
CustomApp_PooledUser	192.168.200.110	192.168.200.108	ORACLE	5
DBPOOLEDUSER	192.168.200.110	192.168.200.108	ORACLE	3
dsmith	192.168.20.222	192.168.200.108	ORACLE	4
DSMITH	192.168.200.101	192.168.200.108	ORACLE	1
dvalovcin	192.168.20.107	192.168.200.108	DB2	1
dvalovcin	192.168.20.178	192.168.200.108	DB2	8
gdemodb2\bfedermann	192.168.20.107	192.168.200.109	MS SQL SERVER	1
gdemodb2\lmetaxotos	192.168.20.119	192.168.200.109	MS SQL SERVER	3
gdemodb2\nshapira	192.168.20.107	192.168.200.109	MS SQL SERVER	5
gdemodb2\nshapira	192.168.20.107	192.168.200.110	MS SQL SERVER	1
gdemodb\nshapira	192.168.20.107	192.168.200.110	MS SQL SERVER	4
guardadmin	192.168.20.222	192.168.200.108	ORACLE	2
GUARDUSER	192.168.20.222	192.168.200.108	ORACLE	1

Records: 1 To 20 From 54

Aliases: ON

PCI - Unathorized Application Access

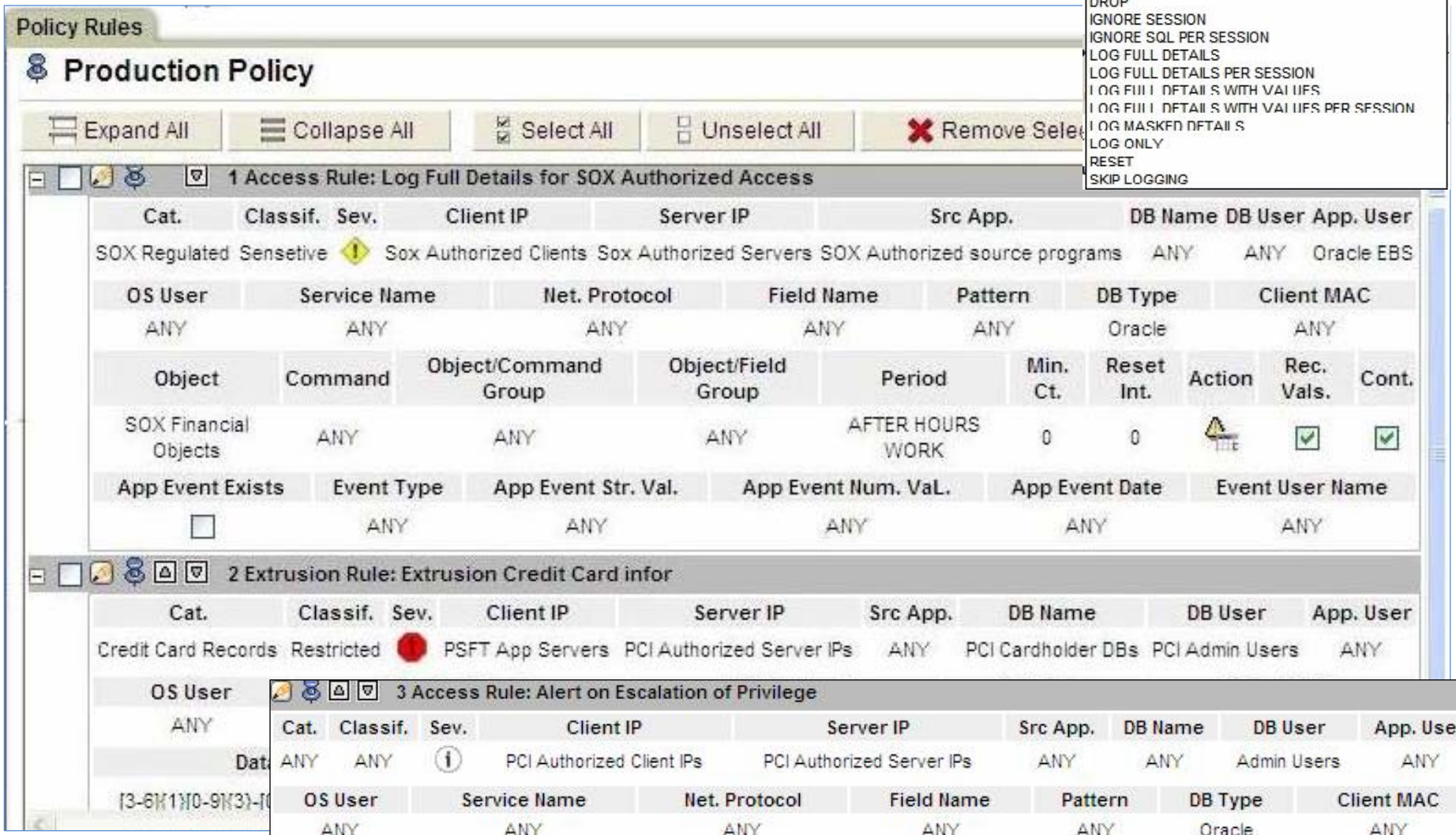
Start Date: 2004-07-28 18:07:13 End Date: 2007-04-24 18:07:13

Source Program	Client IP	Server IP	Server Type	Count of Sessions
TXN_PROC	192.168.1.120	192.168.2.51	ORACLE	6
CUSTOMER_SERVICE_APP	192.168.1.120	192.168.2.51	ORACLE	92
AQUA_DATA_STUDIO	192.168.20.107	192.168.200.108	SYBASE	124
AQUA_DATA_STUDIO	192.168.20.107	192.168.200.109	MS SQL SERVER	26
AQUA_DATA_STUDIO	192.168.20.107	192.168.200.110	MS SQL SERVER	11
AQUA_DATA_STUDIO	192.168.20.119	192.168.200.108	SYBASE	21
AQUA_DATA_STUDIO	192.168.20.119	192.168.200.109	MS SQL SERVER	25
AQUA_DATA_STUDIO	192.168.20.119	192.168.200.110	MS SQL SERVER	12
AQUA_DATA_STUDIO	192.168.20.178	192.168.200.108	SYBASE	34
AQUA_DATA_STUDIO	192.168.20.178	192.168.200.109	MS SQL SERVER	4
AQUA_DATA_STUDIO	192.168.20.178	192.168.200.110	MS SQL SERVER	19
AQUA_DATA_STUDIO	192.168.20.222	192.168.200.108	SYBASE	6
C:\ORACLEXE\APP\ORACLE\PRODUCT\10.2.0\SERVER\BIN\SQLPLUS-JOE	192.168.1.207	192.168.200.108	ORACLE	1
C:\ORACLEXE\APP\ORACLE\PRODUCT\10.2.0\SERVER\BIN\SQLPLUS-JOE	192.168.20.222	192.168.200.108	ORACLE	2
SQLPlus	192.168.1.207	192.168.200.108	ORACLE	5
SQLPlus	192.168.20.107	192.168.200.108	ORACLE	7
SQLPlus	192.168.20.110	192.168.200.108	ORACLE	2
SQLPlus	192.168.20.119	192.168.200.108	ORACLE	5
SQLPlus	192.168.20.178	192.168.200.108	ORACLE	6
SQLPlus	192.168.20.222	192.168.200.108	ORACLE	54

Records: 1 To 20 From 67

Aliases: ON

Enforce with real-time policies



Guardium

Granular access controls

- **Restrict access to sensitive objects by**
  - Client IP, MAC address
  - Domain ID
  - Source application
  - Time-of-day, etc.

PCI - Unathorized Application Access

Start Date: 2004-07-28 18:07:13 **End Date:** 2007-04-24 18:07:13

Source Program	Client IP	Server IP	Server Type	Count of Sessions
TXN_PROC	192.168.1.120	192.168.2.51	ORACLE	6
CUSTOMER_SERVICE_APP	192.168.1.120	192.168.2.51	ORACLE	92
AQUA_DATA_STUDIO	192.168.20.107	192.168.200.108	SYBASE	124
AQUA_DATA_STUDIO	192.168.20.107	192.168.200.109	MS SQL SERVER	26

- **Groups & LDAP for simplified management**
- **Flexible proactive actions**
  - Alerts (SNMP, SMTP, Syslog), log full details, reset
  - Blocking mode when installed in-line
  - Custom Java actions e.g., account lock-out
  - Integration with SIEM systems

Application user monitoring

SAP Application Access

Start Date: 2005-03-11 16:45:06 **End Date:** 2006-11-11 16:45:06

Application Type	Application Code	Item Name	User	Operation Type	Transaction Code	System Id	Change Date	Record Detail 1	Record Detail 2	Record Detail 3
SAP	SAPE	CALLCENTER	DDIC	?		800	2006-11-09 13:49:21	0000000001		CLB1
SAP	SAPE	DEBI	DDIC	I	VD01	800	2006-11-09 14:06:01	0000010002		
SAP	SAPE	QMEL	RBENNATAN	?		800	2006-11-09 15:41:06	000500000010	IQS2SAPLIQS0	LTXT
SAP	SAPE	STAT_PR	RBENNATAN	U	HRCMP0050	800	2006-11-09 15:18:35	5E8B9A2E9392D411858200902761A739		

Records: 1 To 4 From 4

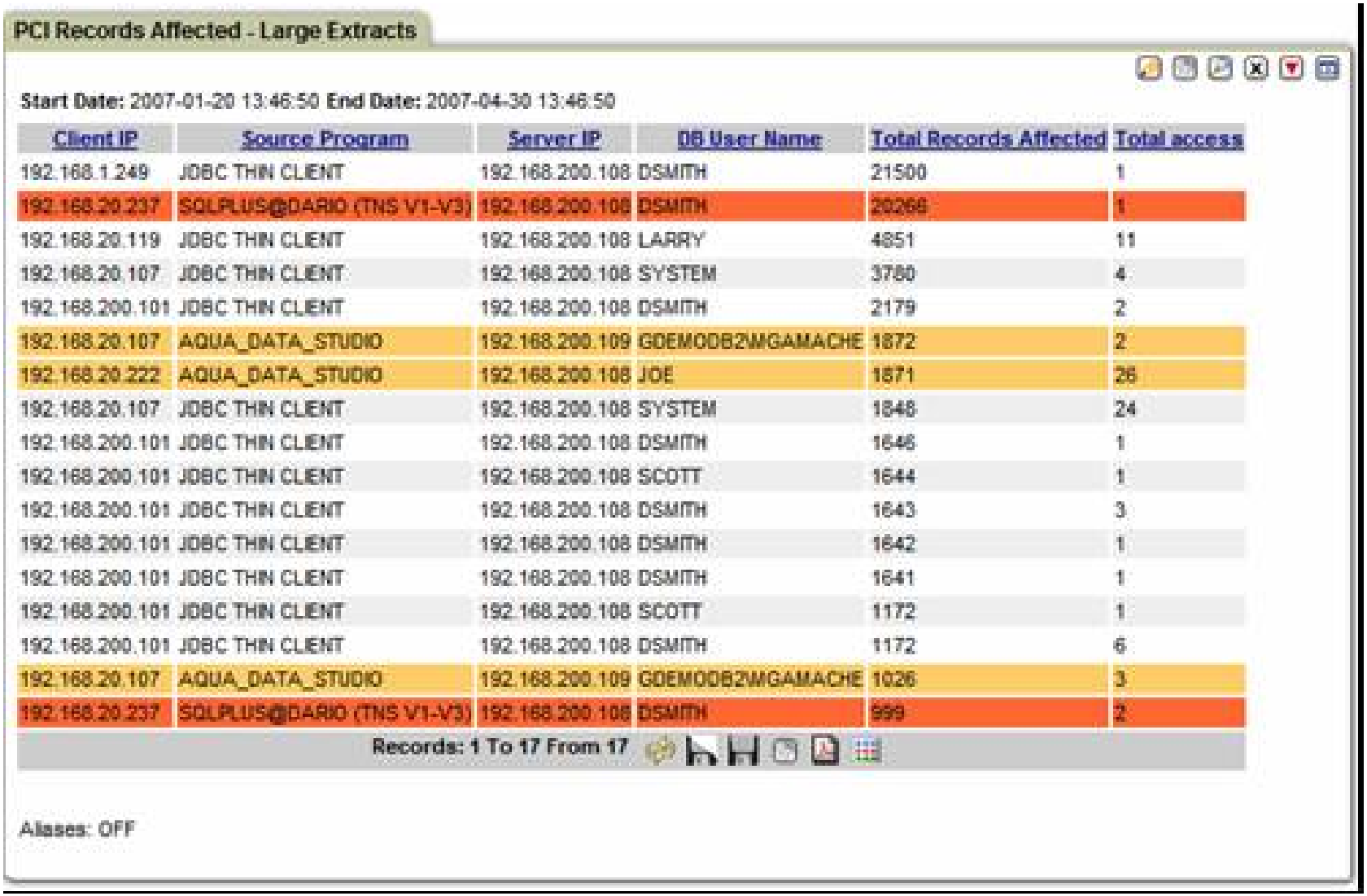
PSFT Application Access

Start Date: 2006-10-28 12:15:57 **End Date:** 2006-11-28 12:15:57

Period Start	Client IP	DB User Name	Application User	SQL Verb
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	catadmin,,davidr.guardium.com,epsys,psappsrv.exe,	INSERT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	catadmin,,davidr.guardium.com,epsys,psappsrv.exe,	SELECT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	cindy,,artm.guardium.com,epsys,psappsrv.exe,	INSERT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	cindy,,artm.guardium.com,epsys,psappsrv.exe,	SELECT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	exa1,,davidr.guardium.com,epsys,psappsrv.exe,	INSERT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	exa1,,davidr.guardium.com,epsys,psappsrv.exe,	SELECT
2006-11-20 13:00:00	psftoracle.guardium.com	SYSADM	exa1,,davidr.guardium.com,epsys,psappsrv.exe,	UPDATE

Records: 1 To 7 From 7

Extrusion policies: identify “outbound” sensitive data



PCI Records Affected - Large Extracts

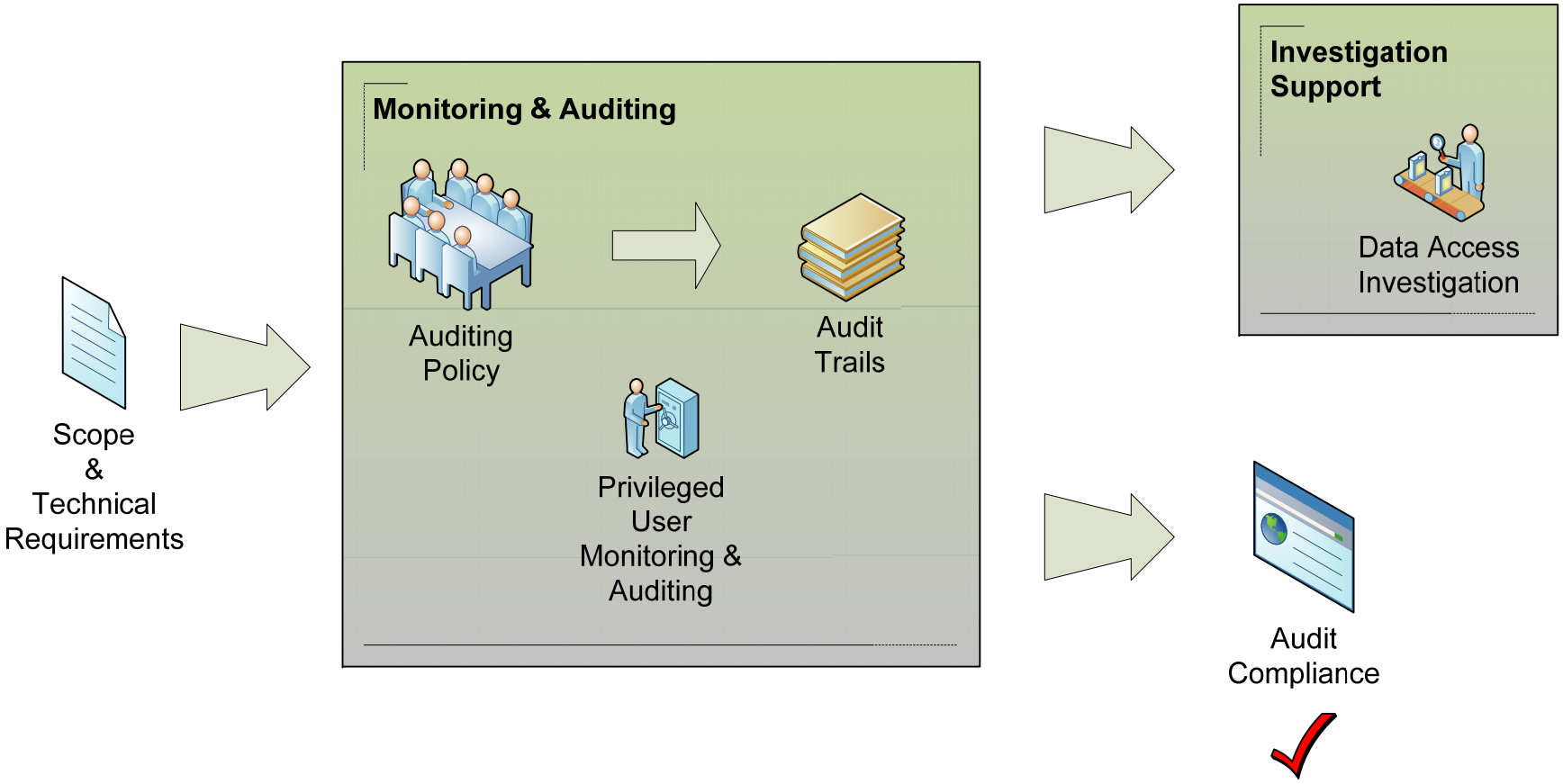
Start Date: 2007-01-20 13:46:50 End Date: 2007-04-30 13:46:50

Client IP	Source Program	Server IP	DB User Name	Total Records Affected	Total access
192.168.1.249	JDBC THIN CLIENT	192.168.200.108	DSMITH	21500	1
192.168.20.237	SQLPLUS@DARIO (TNS V1-V3)	192.168.200.108	DSMITH	20266	1
192.168.20.119	JDBC THIN CLIENT	192.168.200.108	LARRY	4851	11
192.168.20.107	JDBC THIN CLIENT	192.168.200.108	SYSTEM	3780	4
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	2179	2
192.168.20.107	AQUA_DATA_STUDIO	192.168.200.109	GDEMODB2MGAMACHE	1872	2
192.168.20.222	AQUA_DATA_STUDIO	192.168.200.108	JOE	1871	26
192.168.20.107	JDBC THIN CLIENT	192.168.200.108	SYSTEM	1848	24
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	1646	1
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	SCOTT	1644	1
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	1643	3
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	1642	1
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	1641	1
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	SCOTT	1172	1
192.168.200.101	JDBC THIN CLIENT	192.168.200.108	DSMITH	1172	6
192.168.20.107	AQUA_DATA_STUDIO	192.168.200.109	GDEMODB2MGAMACHE	1026	3
192.168.20.237	SQLPLUS@DARIO (TNS V1-V3)	192.168.200.108	DSMITH	999	2

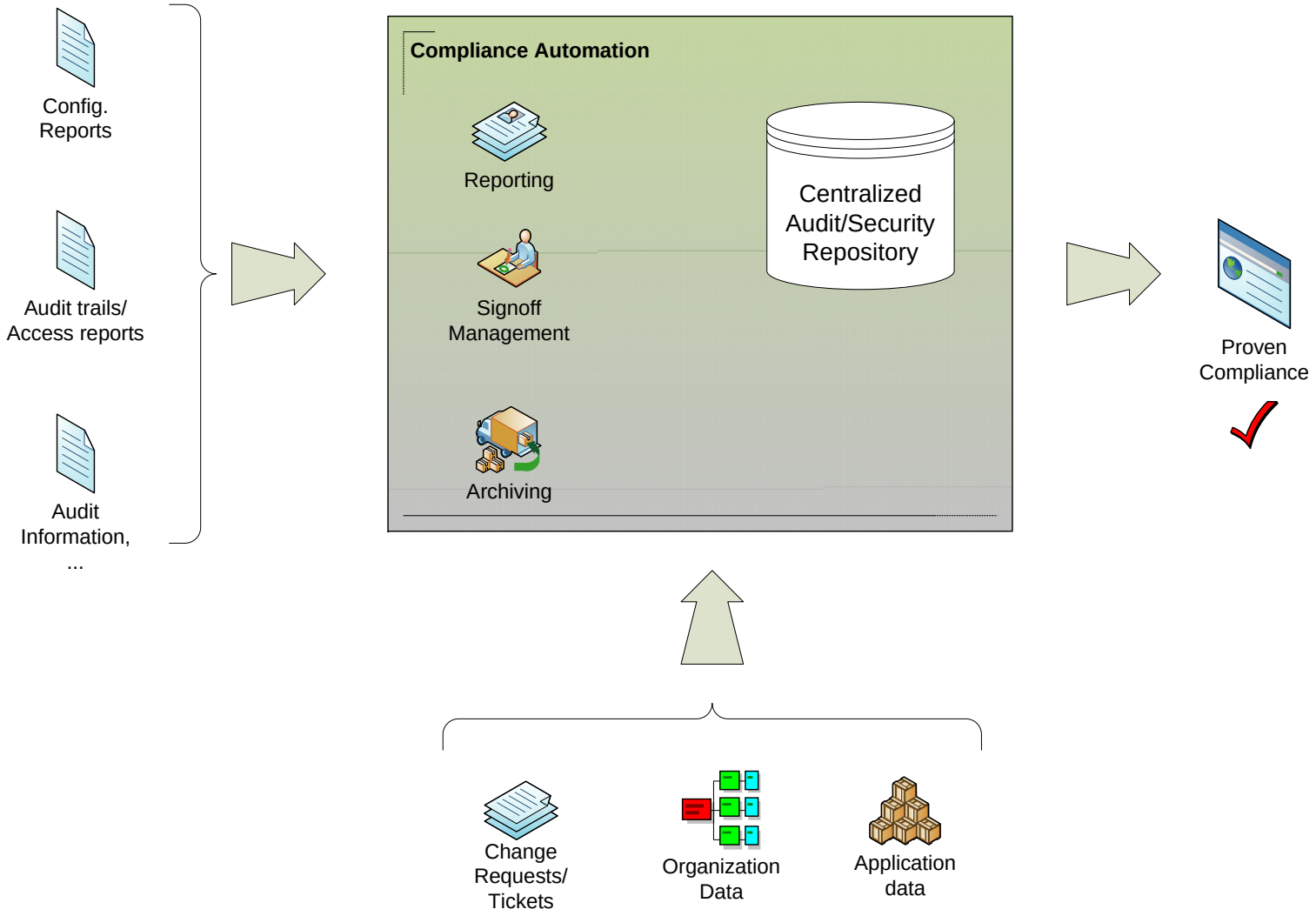
Records: 1 To 17 From 17

Aliases: OFF

Audit & Report

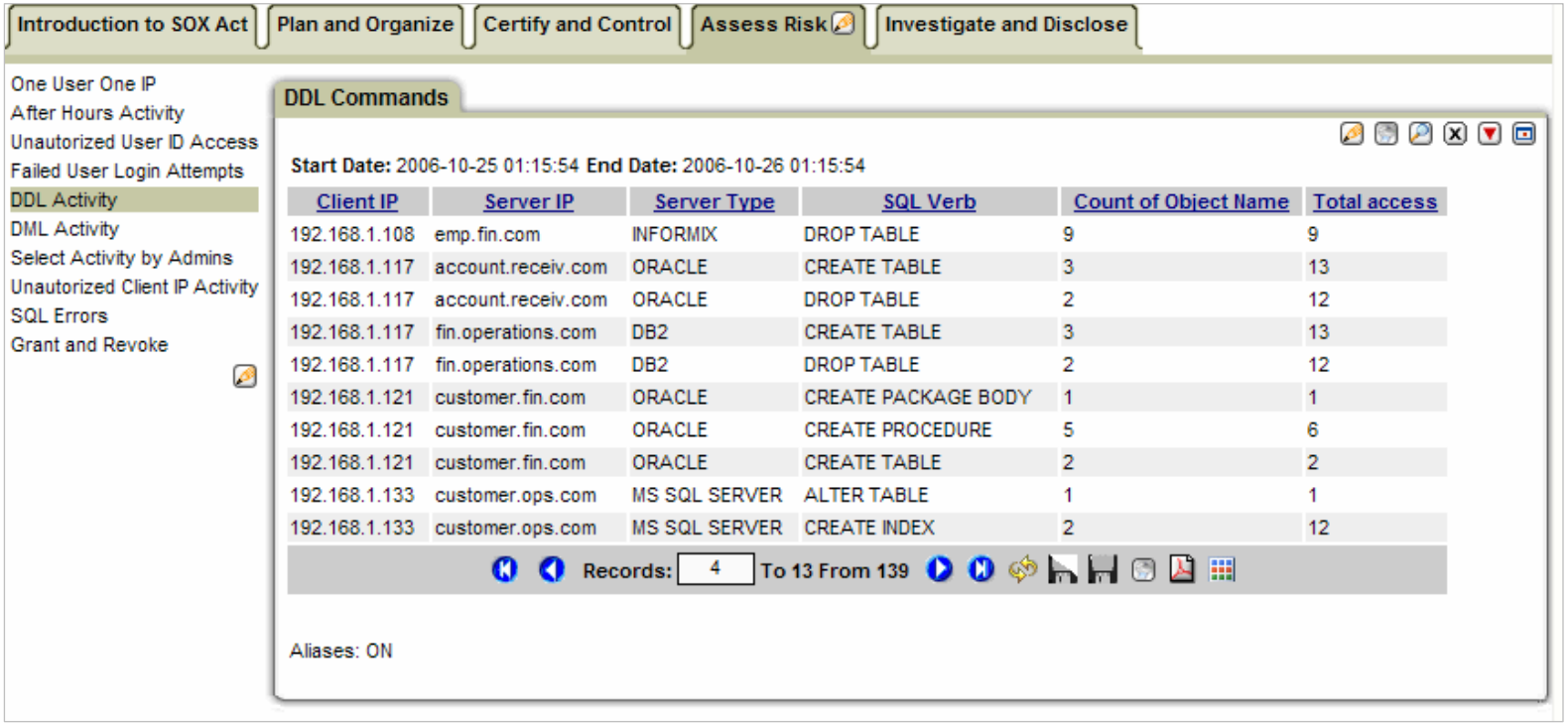


Prove Compliance



Library of “best practices” compliance reports

- **100+ pre-configured reports for data privacy, SOX & PCI**
  - Based on industry best practices
  - Drag-and-drop customization
  - Thresholds to identify anomalous activities
- **Can be managed by security teams without DBA expertise**



Change control reconciliation

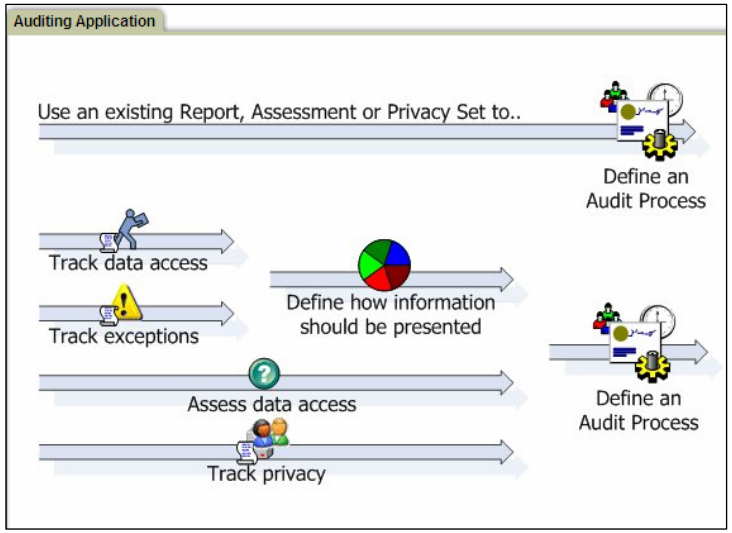
- **Automatically tag all changes with ticket numbers (e.g., Remedy)**
- **Compare changes to authorized work orders**
- **Detect & report on all unauthorized changes**
  - No ticket #'s, outside authorized periods, unauthorized IDs, …

Start Date: 2007-01-12 21:20:06 **End Date:** 2007-01-26 21:20:06

Timestamp	TICKET	Full Sql	BUS_UNIT	APPROVER_ID	DESCRIPTION
2007-01-22 20:03:29	CHANGE REQUEST 23	create table t3(i int)	HR	4612	Change security attributes per terminated employee cycle
2007-01-22 20:03:29	CHANGE REQUEST 23	drop table t3	HR	4612	Change security attributes per terminated employee cycle
2007-01-22 16:47:51	CHANGE REQUEST 22	drop table t2	FINANCE	7984	Add table for RIMS application
2007-01-22 16:47:47	CHANGE REQUEST 22	create table t2(i int)	FINANCE	7984	Add table for RIMS application

Workflow automation

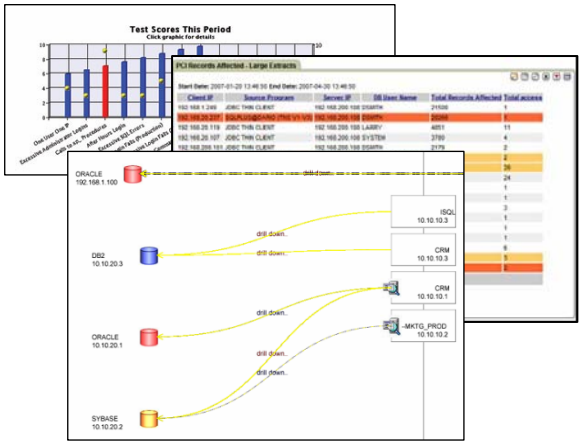
- **Scheduled & automated tasks**
- **Example 1: Find sensitive data as it "migrates" due to ongoing changes**
  - Find by pattern, table name, etc. – and then:
  - Assign classification, alert, add to group, etc. (policy-based)
  - Run on regular basis to keep security policies updated
- **Example 2: Compliance reporting**
  - Automatically generate reports
  - Distribute to oversight team
  - Track electronic sign-offs
  - Escalate when required
  - Store process trail in secure repository
  - *Demonstrates oversight process for auditors*



The Threat Profile Has Shifted

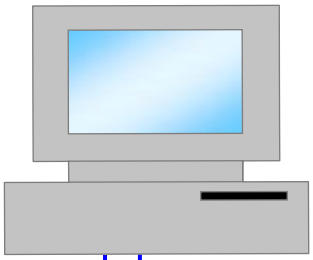
- **75% of threats come from insiders (Forrester)**
  - 65% of internal threats are undetected
  - 60% of enterprises are behind in database security patches
  - DBAs spend less than 7% of their time on database security
- **Enterprise application & database environments are:**
  - Complex & heterogeneous
  - Critical to business continuity
  - Performance-sensitive
  - Difficult to change
- **Traditional AAA model is insufficient**
  - Data access activities are invisible to traditional network security systems

Mainframe solution: Tightly-integrated



Guardium Security Suite

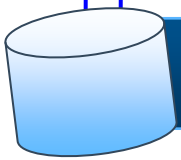
Z2000 Appliance



z/OS

Mainframe apps (CICS, etc.)

Z-TAP Service



DB2 for Z/OS

Developed by Guardium

Developed by NEON Enterprise Software

Single set of security policies & compliance views for both mainframe & distributed environments