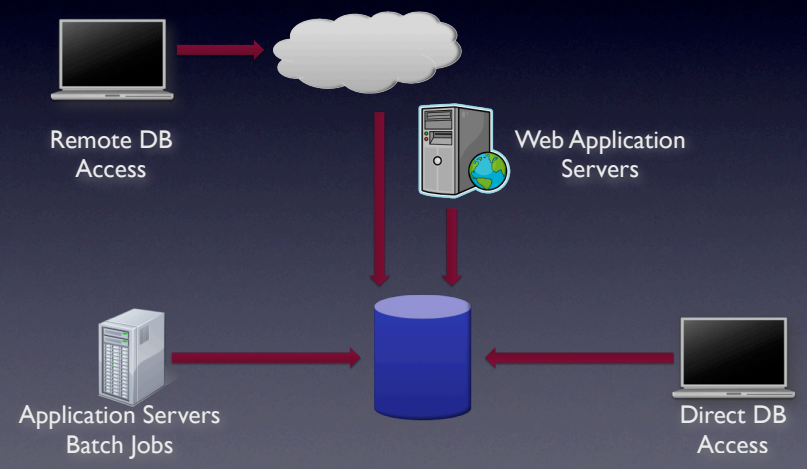
Understanding and Selecting a Database Activity Monitoring Solution

Rich Mogull

Securosis, L.L.C.

http://securosis.com

Do You Really Know What's Happening In Your DB?



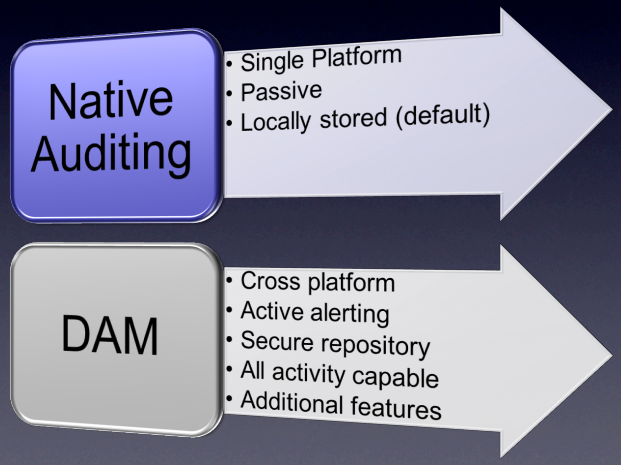
Defining DAM

Database Activity Monitors capture and record, at a minimum, all Structured Query Language (SQL) activity in real time or near real time, including database administrator activity, across multiple database platforms; and can generate alerts on policy violations.

Defining DAM

- Monitor and audit all activity.
- Store data securely.
- Aggregation and correlation across multiple platforms.
- Monitor DBA activity for separation of duties.

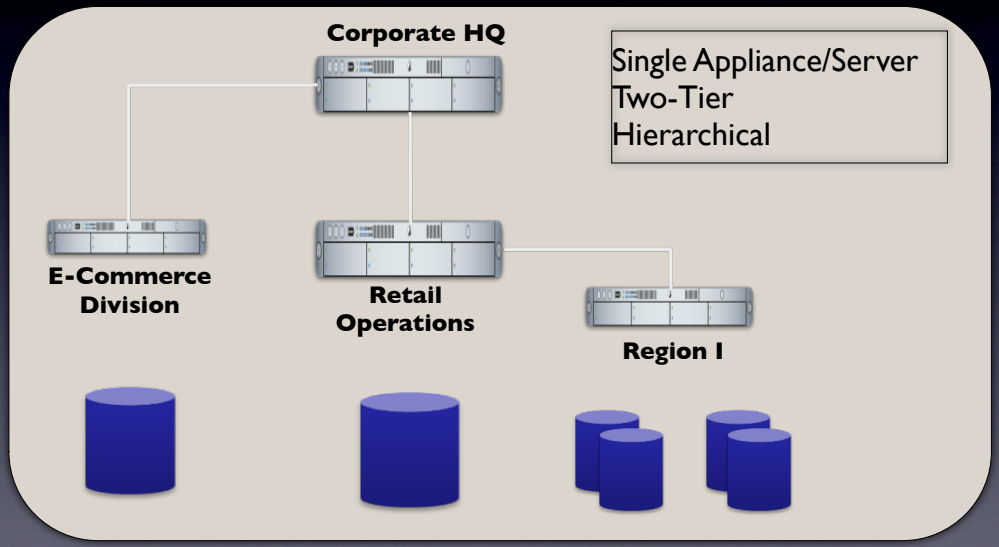
DB Auditing vs. Activity Monitoring



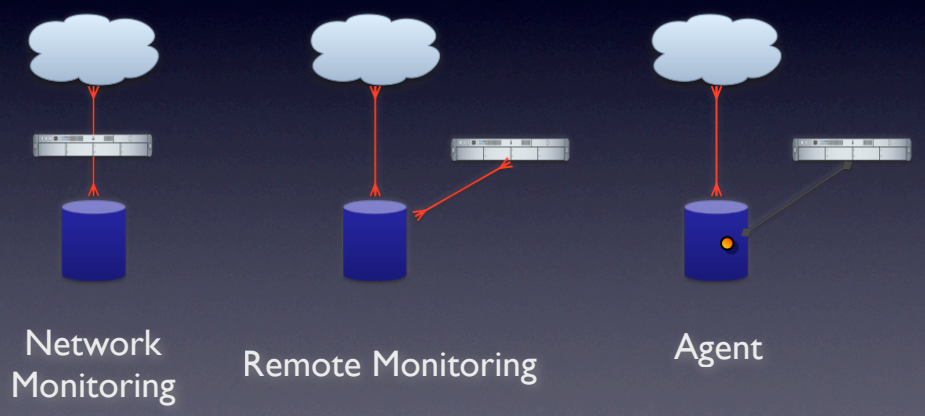
Use Cases

- As a control on DBAs for SOX compliance.
- To detect too many credit card numbers being returned by an application.
- As a compensating control for PCI compliance.
- Change management.
- Audit heterogenous databases when native auditing is unavailable or has performance problems.

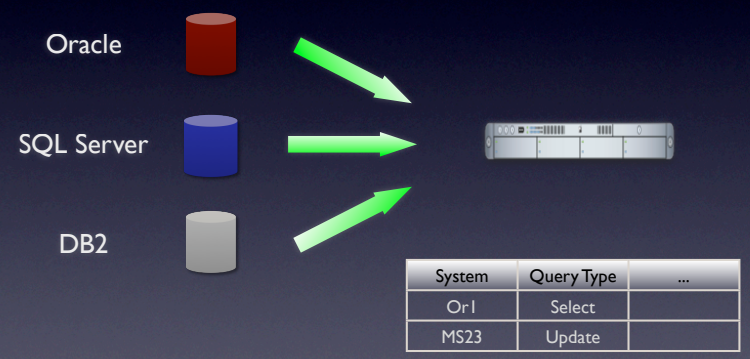
Architecture



Collection Techniques



Aggregation and Correlation



Policy Creation

Database

Object

Action/
Query

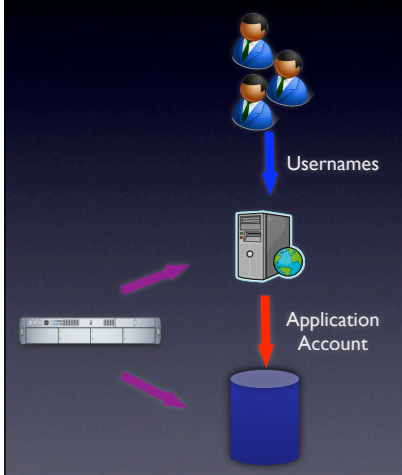
User

Cross-database/Correlation
Compound statements
Criticality
Result sets
Rule Based
Heuristics
Content Based

Alerts and Workflow

ID	Time	Policy	DB	Type	User	Query	Status
1138	1625	SOX/Transaction	ERP_GL	Change	admin	UPDATE tb_ldger...	Open
1139	1632	HIPAA	HR1	View	jsmith	SELECT * from ...	Assigned
1140	1702	PCI/Count	Transact_3	View	192.168.0.213	SELECT CC from ...	Closed
1141	1712	Customer PII	CRM	View	bgates	SELECT * from ...	Closed
1142	1730	Security/SQL Inj	Estore_1	Privilege	192.168.1.94	admin' --	Escalated
1143	12/1/08	Change Mgmt	DB_321	Alter	sjobs	ALTER tab1...	Closed

Advanced Features



Connection Pooled User Identification

Blocking

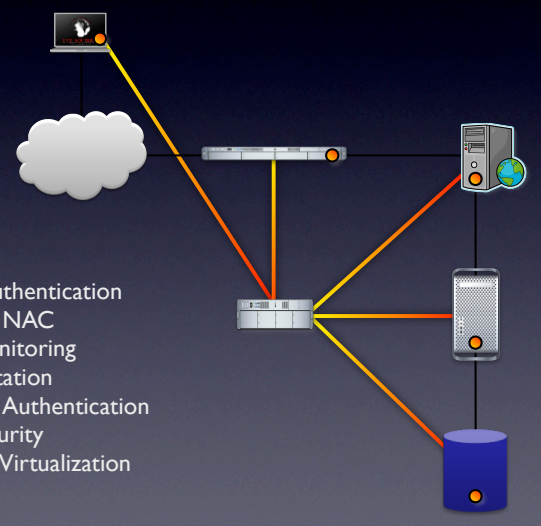
ID	Last	First	SSN
1111	Mogull	Richard	555-12-5555
1112	Smith	John	324-86-3456

Content Discovery

Advanced Features

- Application Activity Monitoring
- Pre-Configured Application Policies
- Pre-Configured Compliance Policies
- Change Management
- Vulnerability Assessment

ADMP



Adaptive Authentication
Application NAC
Activity Monitoring
Anti-Exploitation
Transaction Authentication
Session Security
Application Virtualization

The 3-Step Selection Process

- Define needs
- Formalize requirements
- Evaluate and select

Define Needs

1. Create a selection committee
    1. Include DBAs, security, application administrators, and audit
2. Define systems and platforms to protect
3. Determine protection and compliance requirements

Formalize Requirements

- Issue a formal RFI
- Create a draft RFP
- Confirm requirements with selection committee

Evaluate and Select

1. Issue the RFI
2. Perform paper evaluation
3. Bring in 3 vendors for on-site presentations and risk assessment
4. Finalize RFP and issue to your short list
5. Assess responses and begin deep testing
6. Select, Negotiate, Buy

What To Test

- Platform support
- Performance
- Policy creation and management
- Incident workflow
- Heuristics
- Directory integration

Conclusions

- DAM is more than just auditing.
- Use policies to provide security.
- You can use auditing for separation of duties with DBAs.
- Engage both security and database teams early in the selection process.
- Know your infrastructure and requirements

Rich Mogull

Securosis, L.L.C.

rmogull@securosis.com

http://securosis.com

AIM: securosis