Database Monitoring and Security Solutions

Olivier Gillet
ogillet@imperva.com
Achieving Security & Compliance

Assess
• Discover servers and data
• Test configuration
• Evaluate inherent risks
• Assess who uses the data and applications and how

Set Policies/Controls
• Set policies automatically and quickly
• Keep up with changes
• Configurable policies and controls based on situation

Measure
• Built in & custom reports
• Roll-up & drill down of data
• Security event analysis
• Compliance workflow

Monitor and Enforce
• Ensure separation of duties
• Ensure end user accountability
• Capture full details
• Provide security at all layers
• Alert/block in real-time

IMPERVA ADDRESSES THE ENTIRE LIFE CYCLE
Assess

Know your environment
Know the environment
Complete Assessment Should Include:

- **Server and Sensitive Data Discovery**
  - Find rogue servers and the sensitive information they contain

- **Configuration Risks**
  - Discover misconfigurations, bad practices, negligent policies and unauthorized usage

- **Inherent Risks**
  - Find out about OS, database and infrastructure weaknesses that cannot be mitigated by processes or system setup

- **Identify Unique Users and Data Usage Risk**
  - “An ounce of prevention is worth a pound of cure”
  - Manage risk at its source by knowing which users are accessing sensitive data
Know Where Your Sensitive Data Is

- Find & identify “rogue” servers & databases
  - Servers created for testing without authorization
  - Databases replicated onto individual desktops/laptops
  - Unauthorized services (web, SOA)

- Discover/validate location of sensitive data
  - Personal: name, email, SSN
  - Financial: CC numbers
  - System: userid, password
  - Custom formats e.g. MSISDN
- Remediate risks caused by bad configurations
  - Discover mis-configurations, bad practices, negligent policies and unauthorized usage
  - Identify threats & vulnerabilities
  - Risk assessment & response

- Vulnerability Assessments
  - System configuration
  - Presence of inherent SW risks
  - Users, roles, permissions

- Application Defense Center (ADC)
  - Industry recognised security research
  - Always keeps you up to date
Accounted & approved?
Identify and Track Changes

- Track new user accounts and permissions
- Identify inactive & disabled accounts
- Test for and reconcile database configuration changes

- Classify privileged operations
- Attribute operations to the groups responsible (DBAs, developers, user admin etc)
- Report on DDL, TCL, DCL
- Maintain integrity of sensitive data and control access methods
### Test Name: SQL Agent: Password is viewable to public

**Details:** The stored procedure `msdb.dbo.sp_get_sqlagent_properties` can be used by the public group to view SQL Agent's password.

To fix it, drop the "guest" user using `sp_dropuser`, and revoke public's EXECUTE permission on `msdb.dbo.sp_get_sqlagent_properties`.

**Server Name:** 192.168.0.14  
**Assessment Policy:** Terry ONLY Assessment  
**Type:** MsSql  
**Severity:** High  
**Category:** Authentication  
**Result:** Failed

### Test Name: Logins with blank passwords

**Details:** Logins which haven't been assigned a password create a severe security hole.

**Server Name:** 192.168.0.14  
**Assessment Policy:** Terry ONLY Assessment  
**Type:** MsSql  
**Severity:** High  
**Category:** Authentication  
**Result:** Passed
Defining the Rules
Breaking all Records of Complexity

Constant Change

A profiling solution must create and update the policies
without the need for human intervention

Even more information is needed
- User elements
  - Source Apps, work schedules, IP addresses
- Behavior patterns
  - SQL Queries, SQL Tables, Stored Procedures, etc.

Too complex for manual implementation

- Tables/Objects (~ Thousands)
- Users (~ Hundreds to Thousands)
- Applications (~ Tens to Hundreds)
- Databases (~ Tens)
- Regulations (A Few)

Application Profile
Millions of dynamic items

Automatically Built
Automatically Tuned

Dynamic Profiling

A profiling solution must create and update the policies
without the need for human intervention
A profiling solution must create and update the policies without the need for human intervention.
SecureSphere Dynamic Profiling
Automated Data Usage Assessment

- Dynamic Profiling builds the usage model
  - Automatic creation of usage model
  - More robust than a flat static baseline
  - Administrator can view & edit

- User-centric usage model for each DB User and/or DB User Group
  - DB & schemas accessed
  - Objects queried
  - Highlights sensitive & black-listed objects
  - DML operations performed including SP execution

- Profile captures complete end-user behavior
  - Source IP address & hostname
  - Application used
  - Operating System username
Set Controls and Policies

Usage Patterns for every User

- Comprehensive profile for every user
  - All the way down to the individual query level *for each user*
Dynamically Profiles Applications

Automatically learns protected apps
- App structure
- Elements
- Expected user behavior

...by analyzing live Web traffic
Keep up with Changes
SecureSphere Dynamic Profiling

- Cuts deployment time from months to days
- Eliminates ongoing administration burden
  - 5-15 changes per week equals 5-30 man hours of configuration

Understand the application and usage
Adapt to on-going changes to the application
Set Controls and Policies

Define rules of engagement
Setting Controls and Policies:

- **What’s needed**
  - **Detective controls** – understand suspicious activity and take immediate action to remediate undesired effects.
  - **Preventive controls** – prevent undesired usage by defining policies.
  - **Audit** – keep a record of activity for later inspection and use, regardless of the nature of the activity (suspicious, malicious or legitimate)

- **The Challenge**
  - Complexity of problem similar to complexity of usage modeling
  - Useful policies must be
    - Multi-layer & Flexible (to meet different unique requirements)
    - Granular (for accuracy)
    - Easily managed (for large organizations with multiple roles)
# Policy and Controls Model

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Policy Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>- Prohibited services</td>
</tr>
<tr>
<td>Network signatures</td>
<td>- Known OS threats</td>
</tr>
<tr>
<td>Protocol</td>
<td>- Detect audit evasion</td>
</tr>
<tr>
<td>Audit</td>
<td>- Ensure DB integrity</td>
</tr>
<tr>
<td>- Trail of activities</td>
<td></td>
</tr>
<tr>
<td>Application signatures</td>
<td>- Known DB threats</td>
</tr>
<tr>
<td>- Extrusion prevention</td>
<td></td>
</tr>
<tr>
<td>Correlation rules</td>
<td>- Rules-based exceptions</td>
</tr>
<tr>
<td>Dynamic profile</td>
<td>- Data access behaviours</td>
</tr>
</tbody>
</table>
Business relevant application grouping and policy management.
Built in default reactions, which can be modified

*Always up to date* through the ADC
Set Controls and Policies
Profiles can be fine tuned

- Give only “Least Use Privilege” to each user.
- From control operations (which can be sensitive) to individual work schedules (which can be quite flexible)
Custom Policy creation

Tweak controls along a wide variety of metrics and at all layers:
Audit policies -

DB Response Auditing Configuration

- Enable full DB response auditing

Match by the Following Fields

- Match Criteria
- Command Groups
- Available Match Criteria
  - Affected Rows
  - All Privileged Operations On User
  - Application User
  - Columns
  - Command Groups
  - Database User Groups

- Database User Names
  - Match Unknown Value
  - Operations: At least one
  - Selected: Names:
    - System
      - sapid6
      - sapid6viceid6
    - User Defined:

- Database and Schema
- Destination Tables
- Event Type
- OS Host Names
- OS User Names
Tweak controls along a wide variety of metrics and at all layers.
Monitor and Enforce

Implement the defined
Implement the rules
Monitor and Enforce

- Monitoring Challenges:
  - Separation of Duties
  - Knowing the real End User
  - Scalability to capture full detail
  - Temper proof audit log

- Data usage visibility:
  - Continuous auditing
  - Ability to Alert and/or Block in Real-Time
Audit Independence
- SecureSphere management is separate from database and server management

Network-based Gateways
- Monitors activity via database communication protocols (TNS, DRDA, TDS)
- Processes and logs activity from local agent

Host-based Agents
- Lightweight agent intercepts local database activity
- Passes activity to network-based gateway
- If agent is stopped gateway issues alert

Audit Logs are tamperproof
- Role-based management
- Signed and Encrypted archival
SecureSphere Universal User Tracking

Who Is Really Accessing Data?

- No re-writing of application or database code
- Direct User Tracking
  - DB Username + OS Username + Hostname + IP + Application
- Web to DB User Tracking
  
  - End-to-end real user Knowledge

- SQL Connection User Tracking
  
  - Shared & dedicated DB user connections
Implement the rules
What is the full picture?

- Most vendors summarize activity
  - Report only DB action and table
    - e.g. “select customer_table”
  - Do not know if got credit card number and social security number
  - Do not know how many records were fetched
  - Why? – lack of scalability

- SecureSphere collects FULL detail
  - Collects the actual query (also aggregates up)
    - E.g. “Select credit_card_num, SSN from customer_table”
  - Addresses data loss/leakage with full response analysis
    - Tracks/prevents sensitive data loss (Credit card, SSN, Acct info)
    - Monitors/controls amount of data accessed
  - How? – scalable, distributed architecture for activity auditing
Trusted audit data

Integrity of the Audit Control

- Audit data integrity
  - Litigation quality – raw SQL not a normalized interpretation
  - Separation of duty – not dependant upon DBAs, native audit trails, triggers or transaction logs
  - Tamperproof – hardened appliance & signed/encrypted archive

- Track adds, deletes and changes – Internal System Events
  - Audit & monitoring configuration – Rules and Policies
  - Databases/objects that are being audited
  - SecureSphere users & roles

- Detect tampering of DB Agents
  - Disabling DB Agents
  - DB Agent configuration
What auditors want
Achieving Continuous Auditing

- Paper reports & high-light markers make continuous DB auditing impossible
- Audit process too slow to react in dynamic IT environments
- SecureSphere helps automate the continuous audit process
  - Easily identify/classify DML/DDL access/changes to data
  - Flag sensitive data access
  - Ad-hoc grouping of objects
- Real-time Monitoring and Enforcement
  - Identifies deviations from verified baseline
  - Allows immediate response and/or remediation
Measure

Meet Compliance Requirements
What is needed?

- Built in & custom reports
- Roll-up & drill down of data
- Security event analysis
- Compliance workflow
Regulatory Compliance Requirements
History Alone Is Not Enough

Reports Must Answer Two Key Questions

Q: (Easy) What happened & when?  
A: Detailed activity history captured

Q: (Hard) Was it supposed to happen?  
A: SecureSphere Alerting and Reporting interprets the history
Outside the business process?

Data Access & Other Exceptions

- Real-time alert monitoring
- Exceptions outside of expected business process
- Immediate triaging & response
- Easy integration with 3rd-party IT ecosystems
  - SYSLOG, SNMP, Email, Scripts

- ADC Insight & custom templates
- Scheduled or on-demand
- Histograms, charts & tables
- PDF & CSV format
Graphical Reports

- Pre-defined reports
- Custom reports
- Reports created on demand or emailed daily, weekly or monthly
- PDF and CSV (Excel) format
- Integration with 3rd party reporting and SIEM tools
**Compliance Reporting**

**Thorough Analysis Capability**

- Web and Database correlation within reports.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Server Group</th>
<th>Server IP</th>
<th>Source IP</th>
<th>Web Client IP</th>
<th>App User</th>
<th>DB User</th>
<th>DB/Schema</th>
<th>Raw Query</th>
<th>Source URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/02/2007 07:21:41</td>
<td>VEDA-DB</td>
<td>192.168.0.14</td>
<td>152.168.0.13</td>
<td>192.168.0.83</td>
<td>veda_app</td>
<td>(veda_db,N/A)(veda__db,N/A)</td>
<td>SELECT * FROM Orders WHERE Orders.OrderID = 65</td>
<td>/superveda/orderdetailails.asp</td>
<td></td>
</tr>
<tr>
<td>10/03/2007 12:46:33</td>
<td>VEDA-DB</td>
<td>192.168.0.14</td>
<td>152.168.0.13</td>
<td>192.168.0.83</td>
<td>veda_app</td>
<td>(veda_db,N/A)(veda__db,N/A)</td>
<td>SELECT * FROM Orders WHERE Orders.OrderID = 61</td>
<td>/superveda/orderdetailails.asp</td>
<td></td>
</tr>
<tr>
<td>10/03/2007 12:46:29</td>
<td>VEDA-DB</td>
<td>192.168.0.14</td>
<td>152.168.0.13</td>
<td>192.168.0.83</td>
<td>veda_app</td>
<td>(veda_db,N/A)(veda__db,N/A)</td>
<td>SELECT * FROM Orders WHERE Orders.OrderID = 104</td>
<td>/superveda/orderdetailails.asp</td>
<td></td>
</tr>
<tr>
<td>10/03/2007 12:46:31</td>
<td>VEDA-DB</td>
<td>192.168.0.14</td>
<td>152.168.0.13</td>
<td>192.168.0.83</td>
<td>veda_app</td>
<td>(veda_db,N/A)(veda__db,N/A)</td>
<td>SELECT * FROM Orders WHERE Orders.OrderID = 77</td>
<td>/superveda/orderdetailails.asp</td>
<td></td>
</tr>
<tr>
<td>10/03/2007 12:46:27</td>
<td>VEDA-DB</td>
<td>192.168.0.14</td>
<td>152.168.0.13</td>
<td>192.168.0.83</td>
<td>veda_app</td>
<td>(veda_db,N/A)(veda__db,N/A)</td>
<td>SELECT * FROM Orders WHERE Orders.OrderID = 77</td>
<td>/superveda/orderdetailails.asp</td>
<td></td>
</tr>
</tbody>
</table>
Compliance Reporting
Thorough Analysis Capability

• Tracks Logins and Logouts of Database
Closing the continuous audit loop
Audit Oversight Process

- Implement sign-off process
  - Change management reconciliation
  - Regression of DB & OS integrity
  - SQL exceptions and other errors
  - Access by role/duty – within/outside business process
    - Any new access
    - Changes in access patterns

- Task-based workflow
  - Triaging of ‘incidents’
  - Owner, due-date, status
  - Attach report objects to tasks
  - Email notifications on status change
Efficient Deployment and Operations

No Impact to IT, Easily Managed, Low TCO
- Centralised object-based management with RBACs
- Flexible online/offline data retention
- No batched replication
- Distributed data query & storage
- Best-in-class TPS analysis for major commercial DBs
- SPAN, TAP or Bridge for network coverage
- Low impact DB Agents for local or remote DB access
Implement the rules
What are the complete details?

- Exactly what happened, in detail?

- SecureSphere is architected for distributed processing and storage
  - External storage is supported
    - Scales data storage and archiving

- Centralized access to data
  - MX retrieves audit data or aggregation view in real time
  - Scales reporting & data management
Flexible Deployment Options

- **Transparent Inline Bridge**
  - Supports full enforcement
  - High performance, low latency
  - Fail-open interfaces

- **Non-inline Deployment**
  - Primarily for monitoring, zero network latency

- **Inline Bridge Deployment**
Find Help on how to format the other animated text - "

, 1/8/2008
Unified, Scalable Management

- Centralized administration
  - Manages all devices from a single console
  - Integrated alerting and reporting
  - Easy deployment of new appliances
    - Appliances auto-configured by MX server
  - Hierarchical policy management
  - Granular role-based access control
    - LDAP/Active Directory, Certificate Authentication
  - Web browser interface
<table>
<thead>
<tr>
<th>Gateway Models</th>
<th>G4</th>
<th>G8/Crossbeam</th>
<th>G16 FTL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Throughput</td>
<td>500MB/Sec</td>
<td>1GB/Sec</td>
<td>2GB/Sec</td>
</tr>
<tr>
<td>Max Transactions per Second</td>
<td>16,000</td>
<td>24,000</td>
<td>36,000</td>
</tr>
<tr>
<td>Recommended Web Servers</td>
<td>50</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U</td>
<td>1U</td>
<td>2U</td>
</tr>
<tr>
<td>FTL Model:</td>
<td>2U</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment mode</td>
<td>Bridge, Router, Proxy or Monitor</td>
<td>Bridge, Router, Proxy or Monitor</td>
<td>Bridge, Router, Proxy or Monitor</td>
</tr>
<tr>
<td>Max Inline Bridge Segments</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Max Routing Interfaces</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Management Interfaces</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>High Availability</td>
<td>Fail Open, IMPVHA, VRRP</td>
<td>Fail Open, IMPVHA, VRRP</td>
<td>Fail Open, IMPVHA, VRRP</td>
</tr>
<tr>
<td>Fault Tolerance</td>
<td>Available</td>
<td>Available</td>
<td>Yes</td>
</tr>
<tr>
<td>Gateway Models</td>
<td>G4</td>
<td>G8/Crossbeam APM</td>
<td>G16</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------</td>
<td>------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Throughput</td>
<td>500Mbps</td>
<td>1Gbps</td>
<td>2Gbps</td>
</tr>
<tr>
<td>TPS</td>
<td>50,000</td>
<td>100,000</td>
<td>200,000</td>
</tr>
<tr>
<td>Max Recommended DB Servers</td>
<td>25</td>
<td>50</td>
<td>100</td>
</tr>
<tr>
<td>Form Factor</td>
<td>1U (2U for FT Model)</td>
<td>1U (2U for FT Model)</td>
<td>2U</td>
</tr>
<tr>
<td>Deployment mode</td>
<td>Non-inline/Bridge/Router</td>
<td>Non-inline/Bridge/Router</td>
<td>Non-inline/Bridge/Router</td>
</tr>
<tr>
<td>Max Inline Bridge Segments</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Max Routing Interfaces</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Management Interfaces</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>High Availability</td>
<td>Fail Open or STP/VRRP/IMPVHA</td>
<td>Fail Open or STP/VRRP/IMPVHA</td>
<td>Fail Open or STP/VRRP/IMPVHA</td>
</tr>
<tr>
<td>Integrated Management Option</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Easing regulatory compliance through data governance
Meet Business and Technical Needs

Complete Data Governance and Protection
- **Assess** the IT environment
- **Set** Controls and Policies
- **Monitor** Activity and **Enforce** the Rules
- **Measure** against regulatory requirements and security policies

Seamless Deployment, Unrivaled Operational Efficiency
- No Impact on Database Server, Applications or Network
- No On-going Tuning
- Best-in-class audit performance and ease of management
- Hierarchical Object Oriented management of Users, Roles, Applications
Thank You