



## **GridApp Webinar**

Five Steps to Simplified Database  
Audit and Compliance

Delivered by:  
Matthew Zito, Chief Scientist

156 5th Avenue  
Penthouse  
New York, NY 10010  
P: 646.452.4100  
[www.gridapp.com](http://www.gridapp.com)

# GridApp Welcomes You

- Thank you for attending
- Our presentation will last approximately 30 minutes
  - Topic: Five Steps to Simplified Database Audit and Compliance
  - Speaker: Matthew Zito, GridApp Chief Scientist
- Stay tuned for the companion white paper
- [response@gridapp.com](mailto:response@gridapp.com)

# About our Speaker

- Matthew Zito
- Chief Scientist
- Expert in large-scale infrastructures
- Previously with EMC and Register.com
- Linux advocate
- Early adopter of technologies such as automation and centralized configuration management

# Today's Agenda

- Auditing the Database
  - Why it's so crucial
  - Why it's so difficult
- Five Steps to Simplified Database Auditing
  - 1) Define What You Need to Audit
  - 2) Set Policies
  - 3) Set Permissions and Access Controls
  - 4) Protect audit data against changes
  - 5) Monitor and Maintain
- Getting Started – Who Can Help?
  - ISVs
  - Automation Specialists
- Q&A

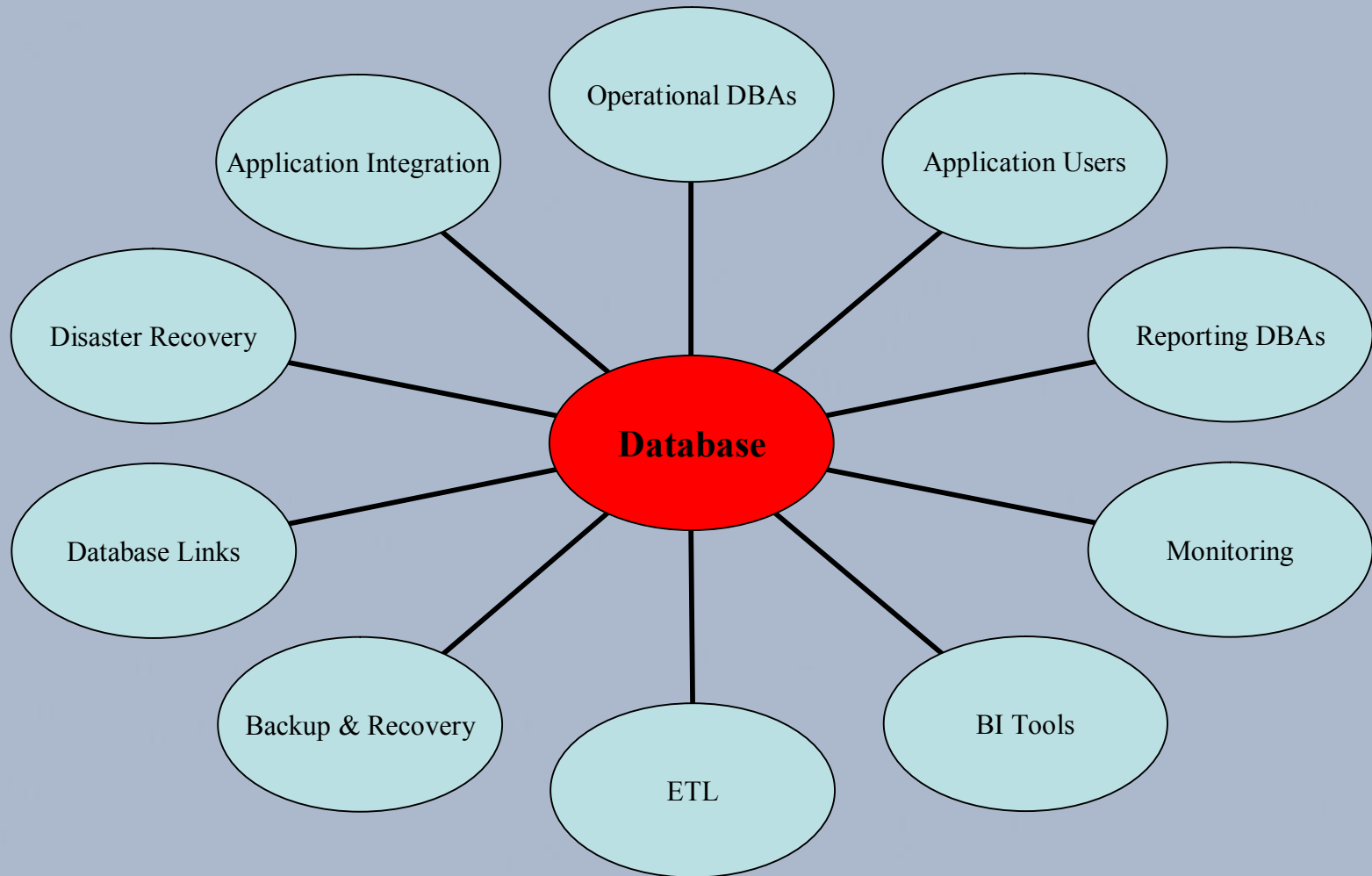
# The Importance of DB Auditing

- In the Past:
  - Auditing Was a Business Accounting Issue
  - “Checkbox” security requirement
- In Today’s Environment:
  - SOX, HIPAA, FDA 21 CFR Part 11
  - No Audit Controls = Jail-time
- Security Breaches are On the Rise
  - Recent Cases: Marriott, Wells Fargo, Bank of America
  - 50 million customers affected in 2005

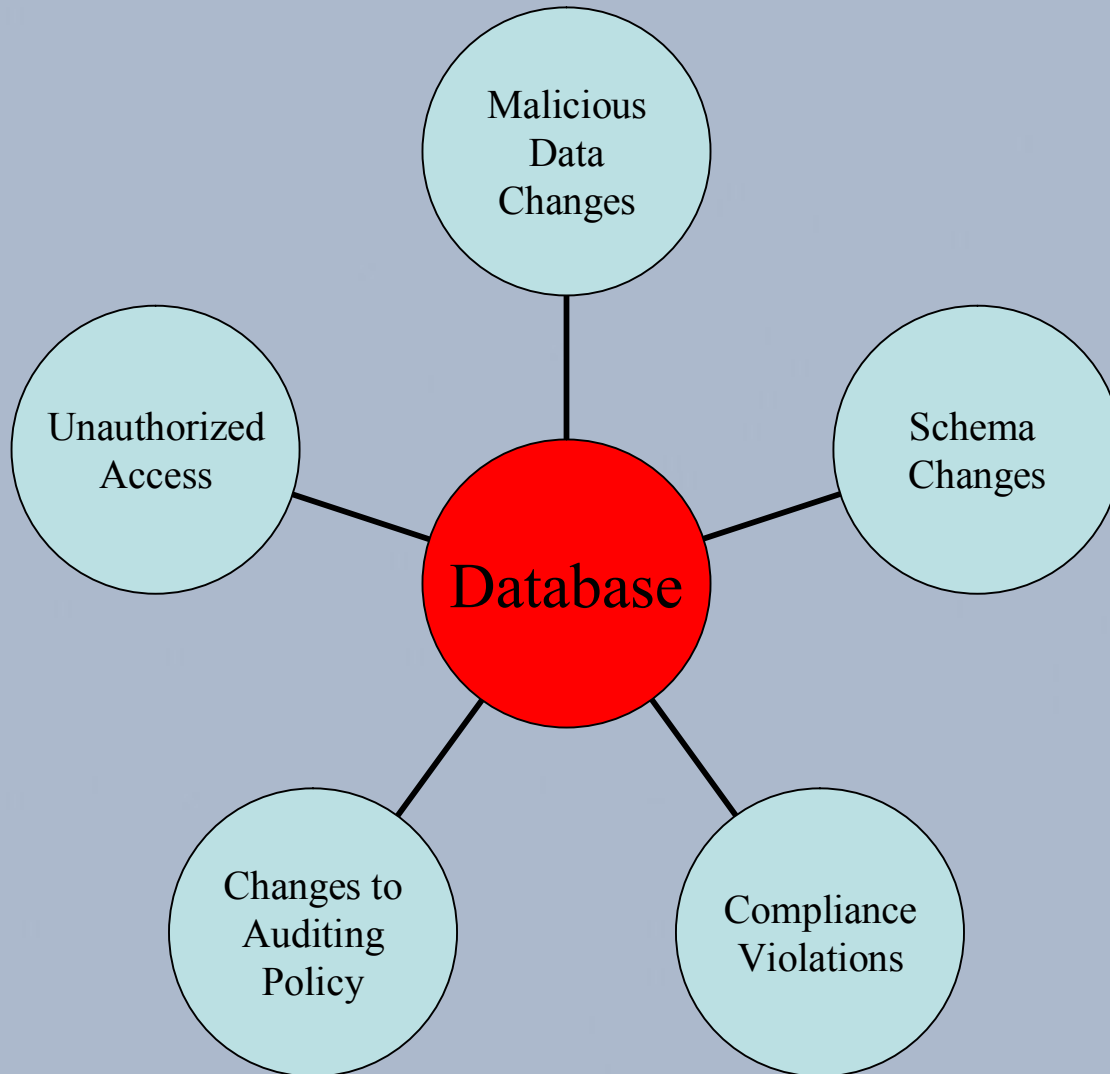
# Challenges to DB Auditing

- Data & Audit trail are stored in individual database “silos”
  - No “cross-infrastructure” view
- Lack of understanding about what needs to be done
  - DBAs Not Trained in Security
  - 60% Don’t Know How to Implement Security Measures - Forrester
- Poorly designed access control procedures
- No clear separation of duty
  - Highly privileged users – “All Powerful DBA”
- Complexity of the environment
  - Lack of resources and time
- Weak database security policies

# Many Touches To Your Database



# What do you need to protect from?



# Five Simple Steps: Step 1

## What Do I Need to Audit?

- Identify Your Infrastructure
  - How many databases?
  - What types – Oracle, SQL Server, etc.?
  - What are the difference between their internal tools?
  - What needs to be done to standardize?
- What information do you need?
  - What regulations do you need to comply with?
  - What is the purpose of those regulations?

# Step 2: Set Policies

- Policies are more about groups and concepts than specific rules
  - “How critical is X group of databases?”
  - “How critical is Y subset of data in those databases?”
  - Create tiers of both database and data criticality
  - Don’t over-engineer
  - Don’t mistake Policies for Permissions

# Step 3: Create Rules

- Permissions must impose control *without* impacting flexibility
- Auditing also must not significantly impact performance for critical systems
- Standard techniques for capturing user activity and changes:
  - Triggers
  - Fine-Grained Auditing
  - Network sniffing and analysis
- Types of changes to track
  - User logins/logouts - failed attempts, etc.
  - Schema changes - identify code changes
  - User access to sensitive data
  - Changes to user permissioning

## Step 4: Centralize and Secure

- Centralize all audit events in near real-time
- Copy to multiple places
- Institute measures to control user access to audit records
- Track proper configuration of auditing rules
- Encrypt the *contents* of auditing records
  - Store keys securely on external HSM devices

# Step 5: Monitor and Maintain

- Ensure Policies are Applied to New Database Environments
  - Retain flexibility to increase or decrease level of auditing for each additional user
  - Institute changes globally
- Scheduled and Ad-Hoc Reporting
  - Generate regular lists of all identified auditing events by user, database, data range, etc.
  - Develop alerts for particular events – ex. Schema changes

Generate weekly and monthly status

reports

[response@gridapp.com](mailto:response@gridapp.com)

# What Can Help?

- Database software
  - Newer database versions have more capability with regards to auditing
- ISVs
  - Variety of different products on the market for assisting with auditing
  - Make sure the products can leverage multiple data sources
  - Make sure the products can secure the audit trail
- Appointing a Database Security Czar
  - Empower someone to take charge
  - Implement a framework to watch the watchers

# Summary

- Database Security is Crucial
- Database Security and Auditing is underdeveloped
- Databases are constantly accessed
  - Auditing and Compliance means reporting on user activity
  - It also means filtering out the noise
- Five Steps to Simplified Audit and Compliance
  - 1) Define What You Need to Audit
  - 2) Set Policies
  - 3) Set Rules
  - 4) Centralize and Secure
  - 5) Monitor and Maintain

# Stay Tuned

- Q&A
- The Companion White Paper
- About GridApp Clarity

# About GridApp Clarity

- Clarity is the only comprehensive database management product in the industry
- Clarity Audit and Compliance:
  - Graphical interface to view all databases and users to be audited
  - Dynamic, secure permissions control
  - Ability to apply policies automatically and globally
  - Simplifies assigning levels of criticality to different policies

# Schedule a Demo

- Email [response@gridapp.com](mailto:response@gridapp.com)
- Subject line = Demo

# The Companion White Paper

- Email [response@gridapp.com](mailto:response@gridapp.com)
- Subject line = White Paper

# Q&A

With Matthew Zito, Chief Scientist



Thank You!