IBM Software Universe

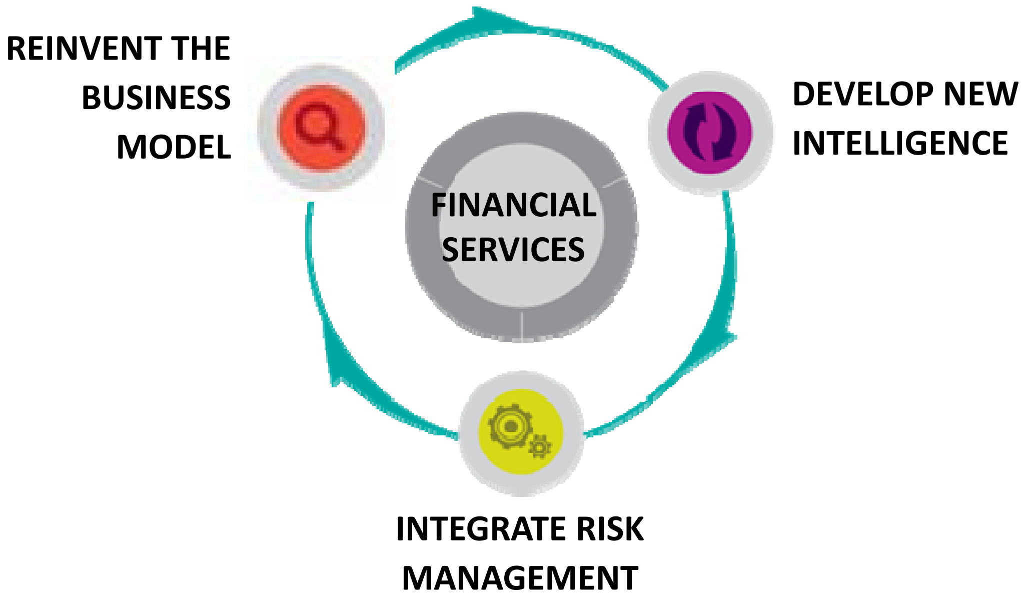
Smarter Businesses, Smarter Industries.

8th March 2011, Pan Pacific, Dhaka.

Safeguarding Enterprise Data with Real-Time Database Security & Continuous Monitoring

Ms. Najiah Abide
Technical Sales,
Information Management Software
IBM India/SA

A Smarter BFSI focuss on ***three*** key imperatives….



- IBM BSFI Industry Solutions - Enabling speed, flexibility & choice in solution deployment
- Banking Performance Management
- Managing Security, Risk & Compliance in BFSI
- **Securing Enterprise Data for Banks**
- Managing Quality & Security of Banking Applications
- Unified Business Process Management for Collaborative Process Improvement
- Payment Systems: Evolution and Framework
- Better Customer Service Through Exceptional Web Experiences

Oracle Survey: Most Organizations Have Very Weak Database Controls

- 3 of 4 organizations can't prevent privileged users from reading or tampering with data in their databases
- 2 of 3 can't detect or prove that privileged DB users aren't abusing their privileges
- Only 1 of 4 use automated tools to monitor databases for security issues on a regular basis
- Close to half said an end-user with common desktop or *ad hoc* tools either could gain unauthorized direct access to sensitive information (or they weren't sure about it)
- Majority don't apply Critical Patch Updates in timely manner

IOUG

independent oracle users group

For the Complete Technology & Database Professional

2010 IOUG DATA SECURITY SURVEY

By Joseph McKendrick, Research Analyst
Produced by Unisphere Research, a division of Information Today, Inc.
September 2010

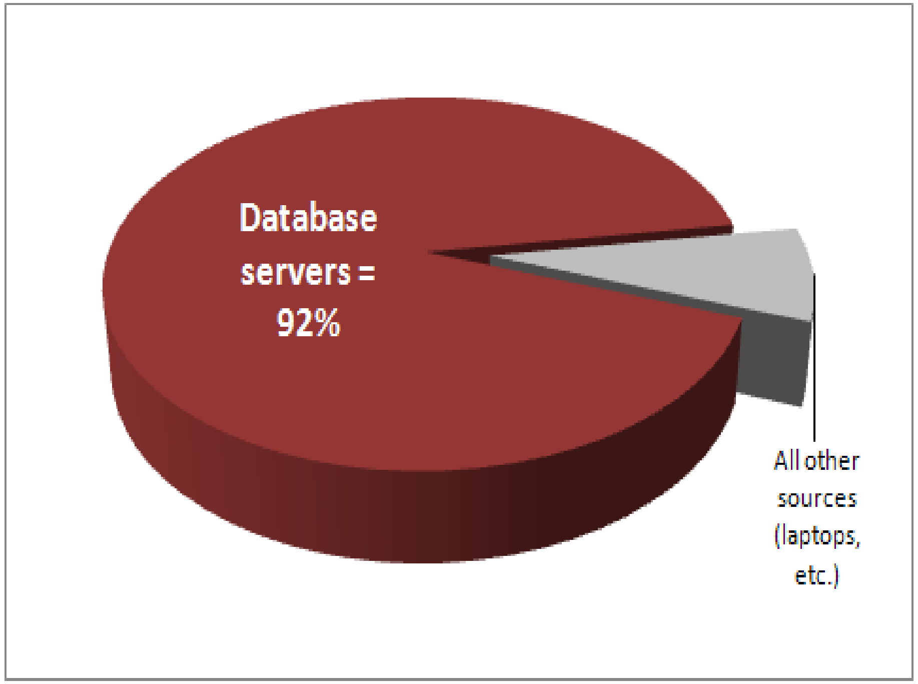
Sponsored by ORACLE

Produced by UNISPHERE RESEARCH

Source: 2010 Independent Oracle User Group (IOUG) Data Security Survey, based on survey of 430 members.
http://www.oracle.com/dm/offers/fy11/50651_2010_report_ioug_data_security_survey.pdf

Database Servers Are The Primary Source of Breached Data

Source of Breached Records



2010 Data Breach Report from Verizon Business RISK Team

… up from 75% in 2009 Report

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

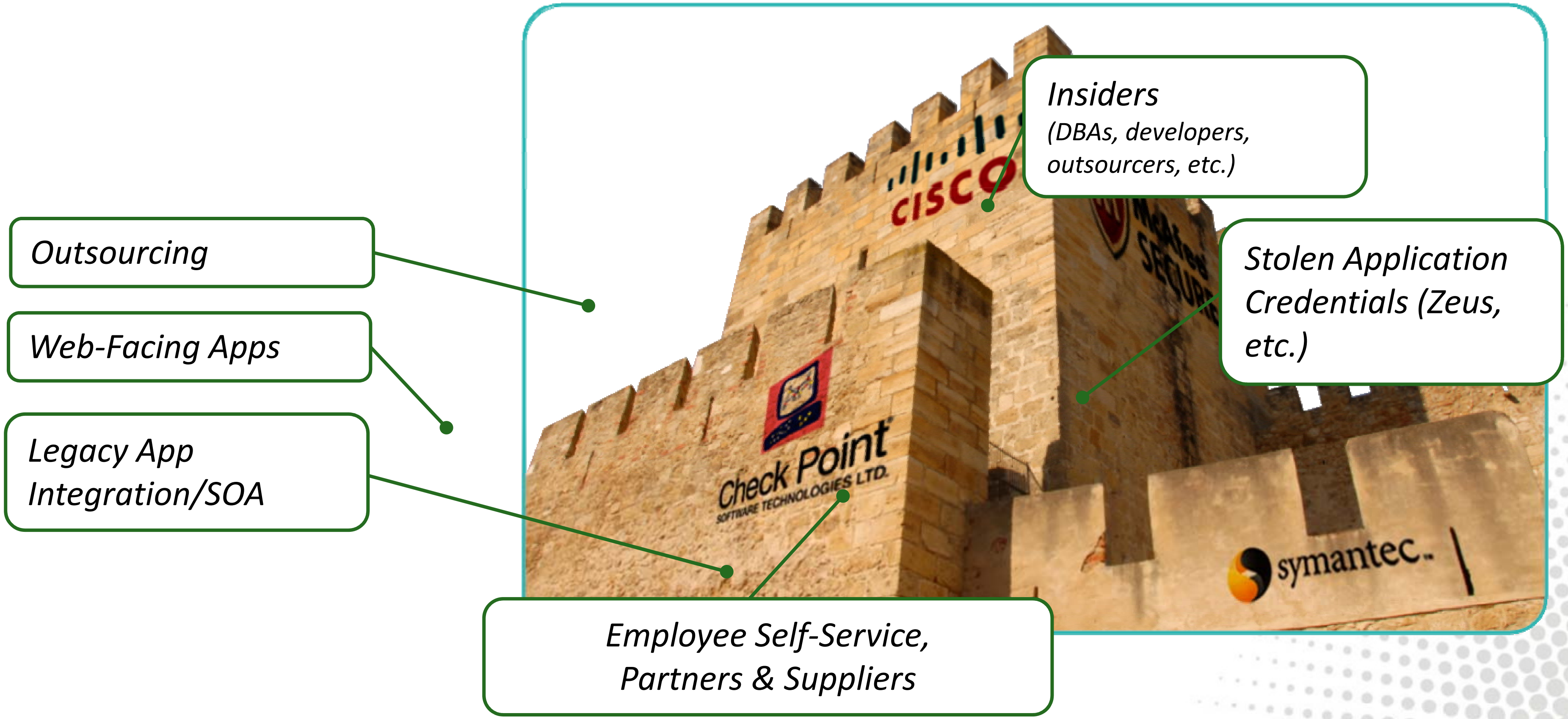
SQL injection played a role in 79% of records compromised during 2009 breaches

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

Perimeter Defenses No Longer Sufficient

“A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls.”

- William J. Lynn III, U.S. Deputy Defense Secretary



Outsourcing

Web-Facing Apps

Legacy App Integration/SOA

Insiders
(DBAs, developers, outsourcers, etc.)

Stolen Application Credentials (Zeus, etc.)

Employee Self-Service, Partners & Suppliers

PCI Compliance Still a Major Challenge

- Organizations struggle <u>most</u> with:
  - Req. 10: Track & monitor all access to cardholder data
    - Typically have no problem with audit logging for network devices & OS's
    - But massive amount of audit data at DB layer => how to identify "needle in haystack"?
  - Req. 3: Protect stored cardholder data
    - Encryption is a challenge due to performance, key management & application changes
- ¾ of organizations don't realize they aren't compliant
  - Most appear overconfident when assessing security practices
  - Organizations are better at "planning and doing" than monitoring ongoing compliance
- It's difficult & cost prohibitive to assess all "need to know" entitlements
  - Need automated approaches
- SQL injection and backdoors and are top 2 threat actions in actual payment card breaches
- ***Most organizations treat compliance as an event, rather than a continuous process***

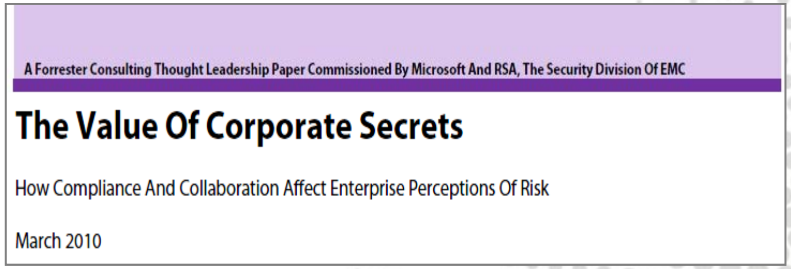
VERIZON 2010 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

A study conducted by the Verizon PCI and RISK Intelligence teams.

Source: Verizon 2010 Payment Card Industry Compliance Report, based on roughly 200 assessments.
http://www.verizonbusiness.com/resources/reports/rp_2010-payment-card-industry-compliance-report_en_xg.pdf

Cost of a Data Breach

- Forrester survey of 305 IT decision makers
- Secrets (e.g., strategic plans) are twice as valuable as custodial data (personal information, credit card data, etc.)
    - 2/3 of value in corporate information portfolio from non-regulated data (secrets)
- Companies focus mainly on preventing accidents (email, etc.)
    - But deliberate theft of information by employees is much more costly
    - Damage caused by rogue IT administrator = $482K (average)
    - Average cost of accidental leakage = $12K
- Most CISOs don't really know if their controls really work
- Note: Survey does not address other costs such as fines
    - Australian bank was fined $500K by VISA
    - Heartland breach cost = $140M



A Forrester Consulting Thought Leadership Paper Commissioned By Microsoft And RSA, The Security Division Of EMC

The Value Of Corporate Secrets

How Compliance And Collaboration Affect Enterprise Perceptions Of Risk

March 2010

Key Compliance Drivers for Financial Services

- **SOX, MAR (NAIC), COBIT/Best Practices** …
  - Prevent unauthorized changes to financial, CRM, ERP & HR data
  - Includes changes to both data (DML) and schemas (DDL)
- **Consumer privacy laws, GLBA, FTC "Red Flag Rule"** …
  - Prevent unauthorized access to personal information (PII), especially by privileged users such as DBAs, developers & outsourced personnel
- **PCI**
  - Track and monitor all access to cardholder data (Req.10)
  - Protect stored cardholder data (Req. 3)
  - Identify unpatched systems & enforce change controls (Req. 6)
  - Compensating control for column-level encryption (Req. 3)
  - Compensating control for network segmentation (Req. 7)
  - Regularly test systems (Req. 11)

- **Reduce compliance costs & effort**
  - Streamline compliance with automated & centralized controls
  - Rapid ROI with < 6 months payback (typical)

How can Guardium help Financial Services Organizations

1. **Prevent data breaches & fraud**
   - Mitigate external & internal threats
   - Secure customer & credit card data, ACH data, strategic plans & IP
2. **Assure data governance**
   - Prevent unauthorized changes to financial & ERP data
3. **Reduce cost of compliance**
   - Automate & centralize controls
   - Simplify processes

… *Without performance impact or changes to databases & applications*

Chosen by Leading Financial Services Organizations Worldwide

- 5 of the top 5 global banks
- 4 of the top 6 global insurers
- A leading global cardholder brand
- Major investment & brokerage firms
- Leading payment processing firms
- Government financial organizations
- Major healthcare payers
- 25 of the world’s leading telcos
- World’s favorite beverage brands
- A top 3 auto maker
- A top 3 aerospace company
- Leading energy suppliers

Financial Services Firm with 1M+ Sessions/Day

Who

Global NYSE-traded company with 75M customers

Need

Enhance SOX compliance, data governance & data privacy

- *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 from change ticketing system
- Passed multiple external audits

Top 5 Global Bank with Multiple Business Units via M&A

Who

Major global bank with multiple business units via mergers & acquisitions viz. Retail & corporate banking, Investment banking, Mortgage banking

Need

Ensure privacy & integrity of all critical enterprise data

- Financial & HR data; ERP data; credit card data; PII; strategic & intellectual property
- Address PCI (Reqts. 3, 6 & 10); SOX; international data privacy laws; internal standards

Environment

- Oracle, SQL Server, Sybase, DB2 UDB; DB2 on z & iSeries; Informix; MySQL; Teradata
- Solaris, HP-UX, AIX, Windows, Linux
- <u>Now monitoring ~2,000 database instances</u>

Alternatives considered

- Native logging/auditing from Oracle
- Symantec/ESM plus products from smaller vendors

Results

- Saving $1.5M per year in storage costs for native audit trails
- Saved $20M+ by using Guardium for DB encryption (PCI)
- Guardium now a standard part of bank infrastructure
- Culture change – awareness of data security
- New processes to investigate insider threats

Regional Bank for SOX, PCI, GLB, FINRA, …

Who

Regional bank with 800 branches

Need

Ensure privileged users are not inappropriately accessing or jeopardizing the integrity of enterprise data such as:

- Financial and transactional data
- Credit card – PAN data (magnetic stripe)
- ACH transaction data
- HR data

Environment

- Oracle (initial focus), SQL Server, DB2 on mainframe, MySQL
- Solaris, AIX, Windows, Linux

Alternatives considered

- Lumigent (incumbent solution that relies on native logs)
- Native logging/auditing from Oracle

Results

- Monitoring for unauthorized or suspicious activities
- Passing audits faster
- Planning to expand to data leak prevention (data-level blocking)

Securing SAP & Siebel: 239% ROI and <6 Months Payback

Who

F500 organization ($15B revenue)

Need

Secure SAP & Siebel data for SOX

- Enforce change controls & implement consistent auditing across platforms

Environment

- SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems (KFS)
- Oracle & IBM DB2 on AIX; SQL Server on Windows

Forrester Consulting

FORRESTER

Prepared for Guardium, Inc.
January 2008

The Total Economic Impact™ Of Guardium Database Monitoring, Security and Auditing

For A Global Consumer Products Company

Project Director: [illegible], Principal Consultant

Commissioned Forrester Consulting Case Study

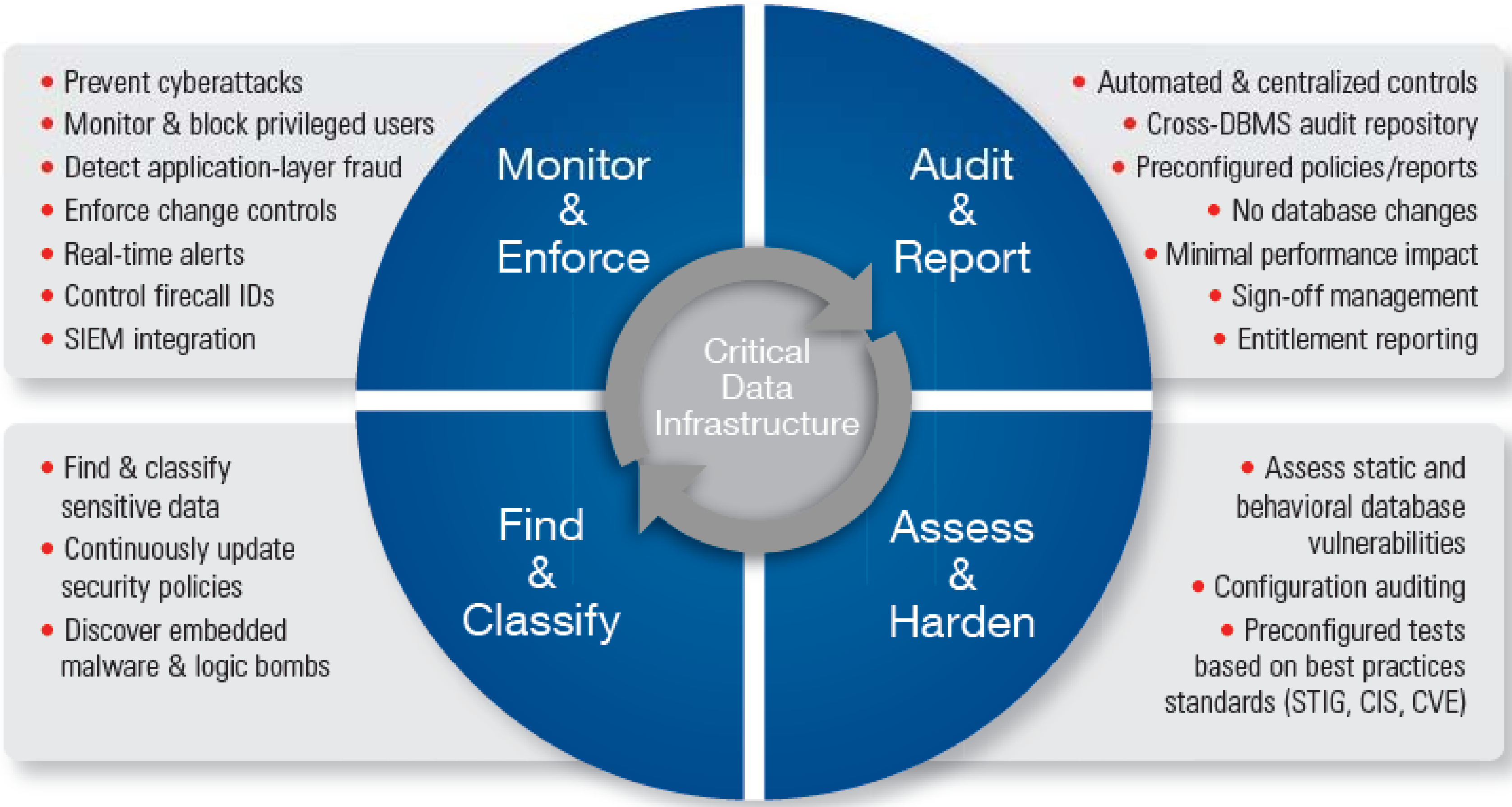
Results

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 … 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.”

Addressing the Full Lifecycle of Database Security & Compliance

Real-time Database Security & Monitoring



Monitor & Enforce

- Prevent cyberattacks
- Monitor & block privileged users
- Detect application-layer fraud
- Enforce change controls
- Real-time alerts
- Control firecall IDs
- SIEM integration

Audit & Report

- Automated & centralized controls
- Cross-DBMS audit repository
- Preconfigured policies/reports
- No database changes
- Minimal performance impact
- Sign-off management
- Entitlement reporting

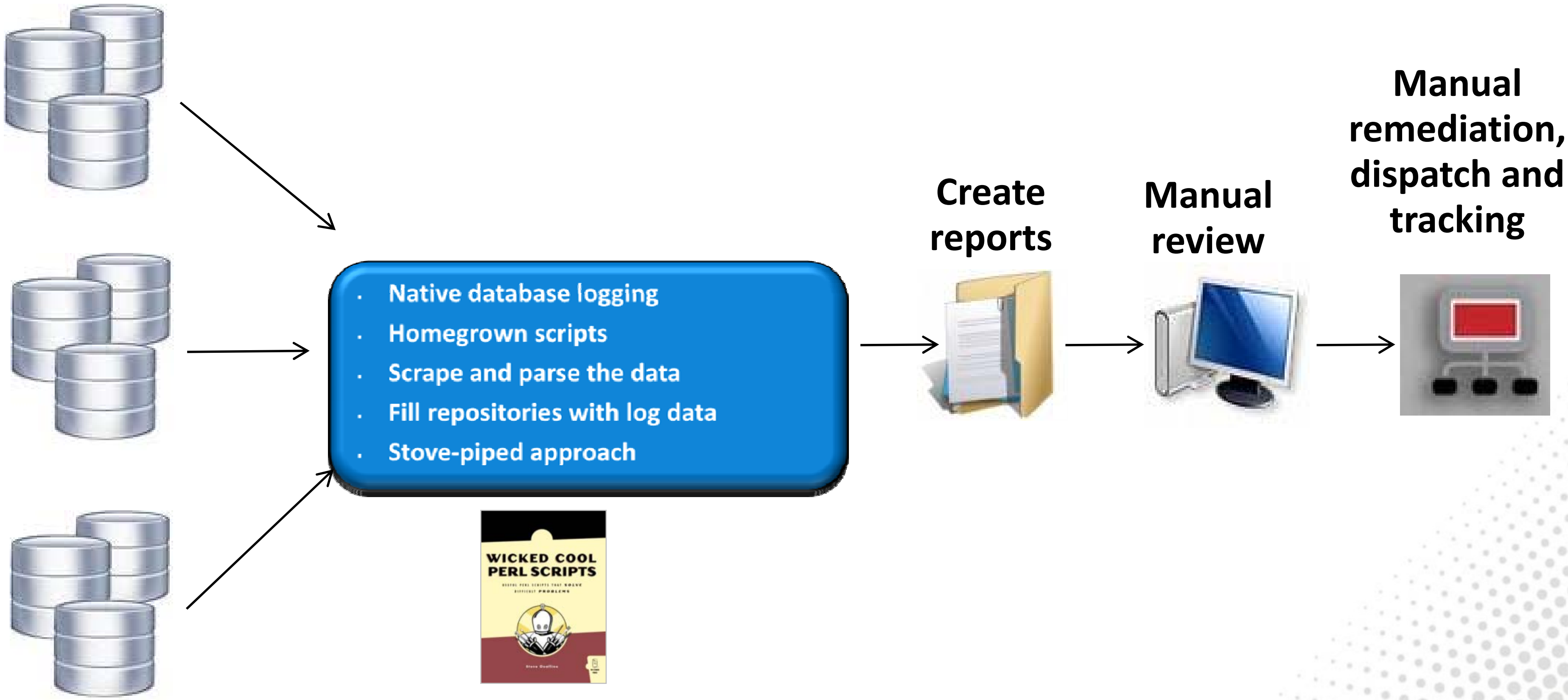
Find & Classify

- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

Assess & Harden

- Assess static and behavioral database vulnerabilities
- Configuration auditing
- Preconfigured tests based on best practices standards (STIG, CIS, CVE)

Which Database Audit Tools are Enterprises Using Today?



- Native database logging
- Homegrown scripts
- Scrape and parse the data
- Fill repositories with log data
- Stove-piped approach

Create reports

Manual review

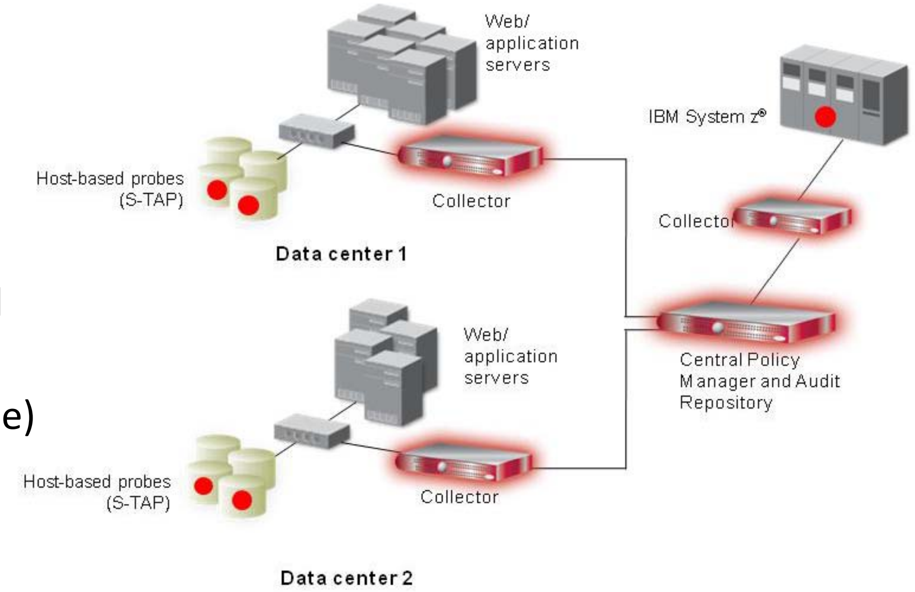
Manual remediation, dispatch and tracking

What Are the Challenges with Current Approaches?

- No separation of duties -- DBAs & hackers can easily tamper with logs to cover their tracks
- Performance impact of native logging on the DBMS
- Limited scope & granularity of log data
- Not real-time
- No preventive controls
- Another data store to secure and manage ($$$)
- Inconsistent policies across apps, DBMS platforms, compliance initiatives
- Can’t identify end-user fraud for connection-pooled applications that use generic service accounts (SAP, PeopleSoft, etc.)
- Lack of DBMS & application expertise on security teams
- Last-minute audit scrambles -- significant labor cost to clean & review data, create reports, maintain oversight processes

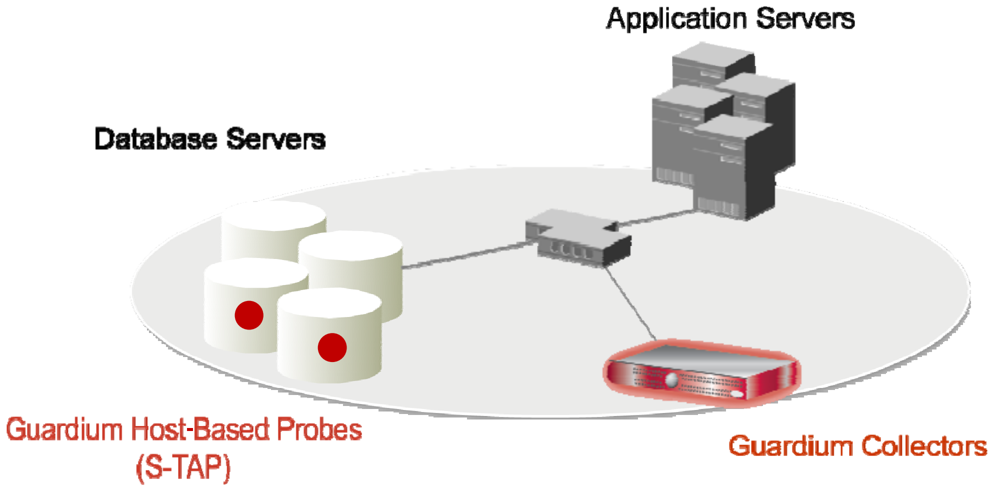
What Sets Guardium Apart

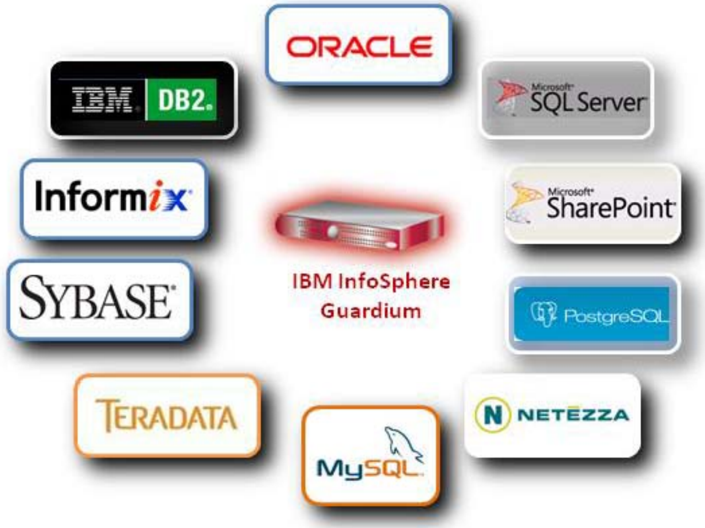
- Most widely-deployed solution, with continuous enhancements based on feedback from the most demanding data center environments worldwide
- Rated by Forrester as “a Leader across the board” with #1 scores for Architecture, Product Offering (Functionality) & Product Strategy
- Available as physical or virtual (software-only) appliance
- Key architectural advantages: enterprise solution
  - Scalable multi-tier architecture
  - Broad heterogeneous support
  - Full visibility into all database activities
  - Advanced analytics/forensics based on centralized audit data warehouse
  - Deep automation to reduce TCO & workload
  - Comprehensive, integrated lifecycle solution (common back-end, workflow & Web console)



Source: “The Forrester Wave™: Enterprise Database Auditing and Real-Time Protection, Q4 2007”

Non-Invasive, Real-Time Database Security & Monitoring





- Continuously monitors all database activities (including local access by superusers)
- Heterogeneous, cross-DBMS solution
- Does not rely on native DBMS audit logs
- Minimal performance impact (2-3%)
- No DBMS or application changes

- Supports Separation of Duties
- Activity logs can't be erased by attackers or DBAs
- Automated compliance reporting, sign-offs & escalations (SOX, PCI, NIST, etc.)
- Granular, real-time policies & auditing
  - *Who, what, when, where, how*

IBM/Guardium vs. Oracle Database Security

	Oracle Database Vault, Oracle Audit Vault	IBM/Guardium
Heterogeneous support	😨	✓
Minimal performance impact or changes	😖	✓
Enforces Separation of Duties (SoD)	😖	✓
Real-time monitoring & alerting	😖	✓
Extrusion (data leakage/breach) monitoring	😖	✓
Application monitoring (EBS, PeopleSoft, SAP, etc.)	😖	✓
Reduces DBA workload	😖	✓

Next Steps

Smarter Businesses, Smarter Industries.