IBM SolutionsConnect 2013

Turning Opportunity into Outcomes.

Database Auditing & Security

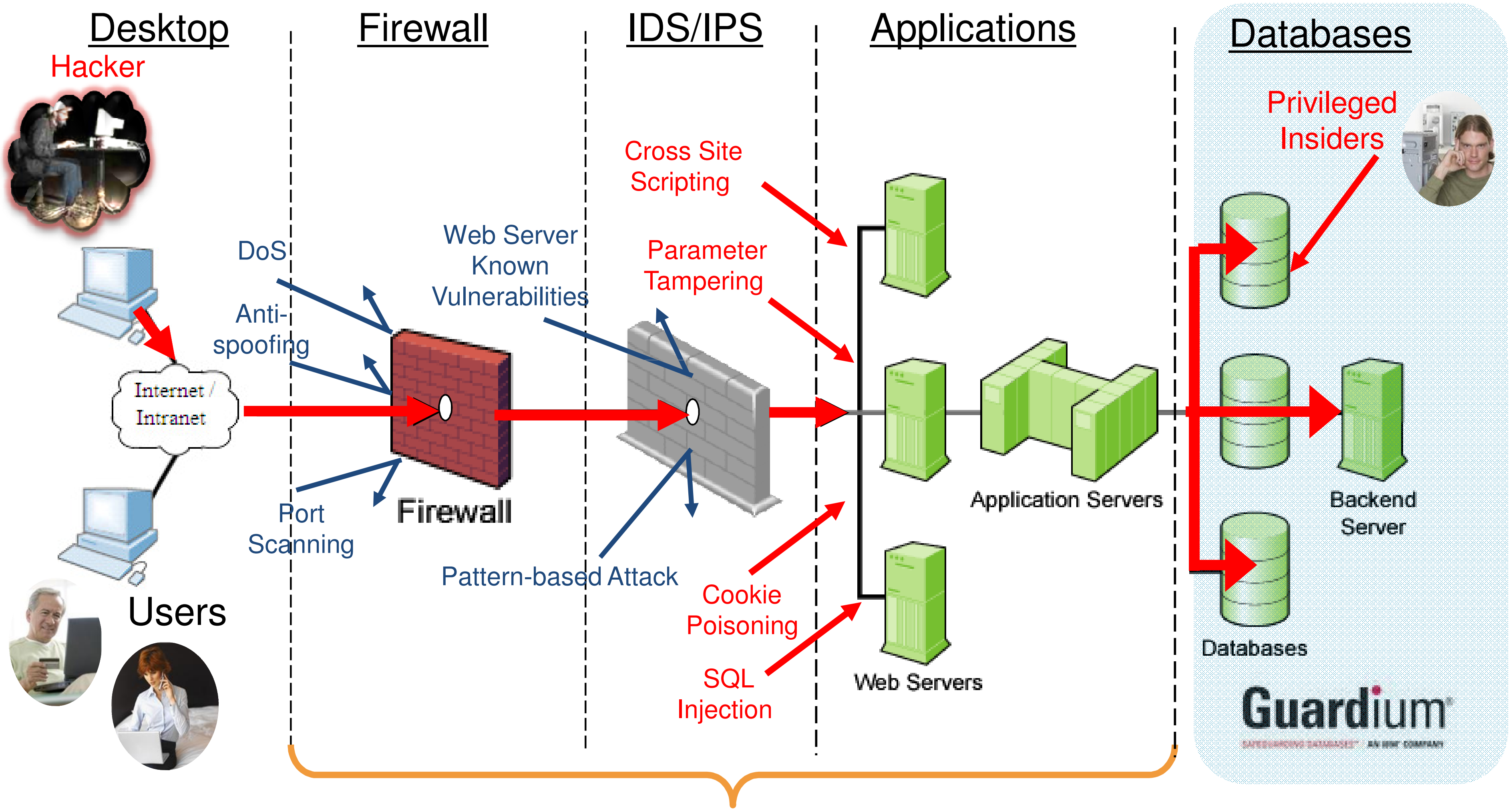
Brian Flasck

Agenda

- Introduction
- Drivers for Better DB Security
- InfoSphere Guardium Solution
- Summary
- Netherlands Case Study

The need for additional security for databases

Protecting the “Crown Jewels” and why it’s necessary



Modern-day data breaches demonstrate that traditional security solutions are not always effective – therefore a last line of defense is vital

5 Common Database Auditing & Security Challenges

1. How can we monitor access to sensitive data and detect anomalies or policy violations in an automated way?

2. How can we track the activities of privileged users, such as DBAs or sysadmins, who have direct access to databases?

3. Can we have segregation of duties and store DB audit logs in a secure repository operated by IT Security and audit specialists?

4. Is it possible to have one central audit repository for all database types including Oracle, MS SQL Server, DB2 and more?

5. How can we achieve all of this without impacting the performance or stability of our database and application servers?

Why is database auditing still so challenging in 2013 ?

Native DB logging is now considered inadequate

× **Lack visibility and granularity**

- Privileged users difficult to monitor
- Anomalies and violations not promptly detected

× **Inefficient and costly**

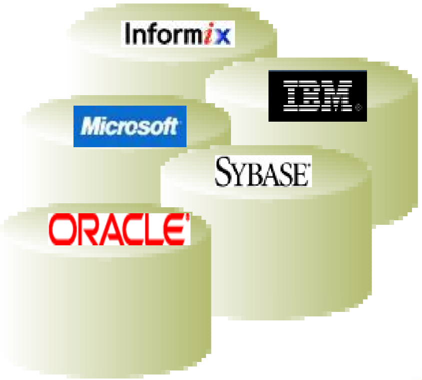
- Database performance is impacted
- Manual processes consume valuable resources

× **Provide little value to the business**

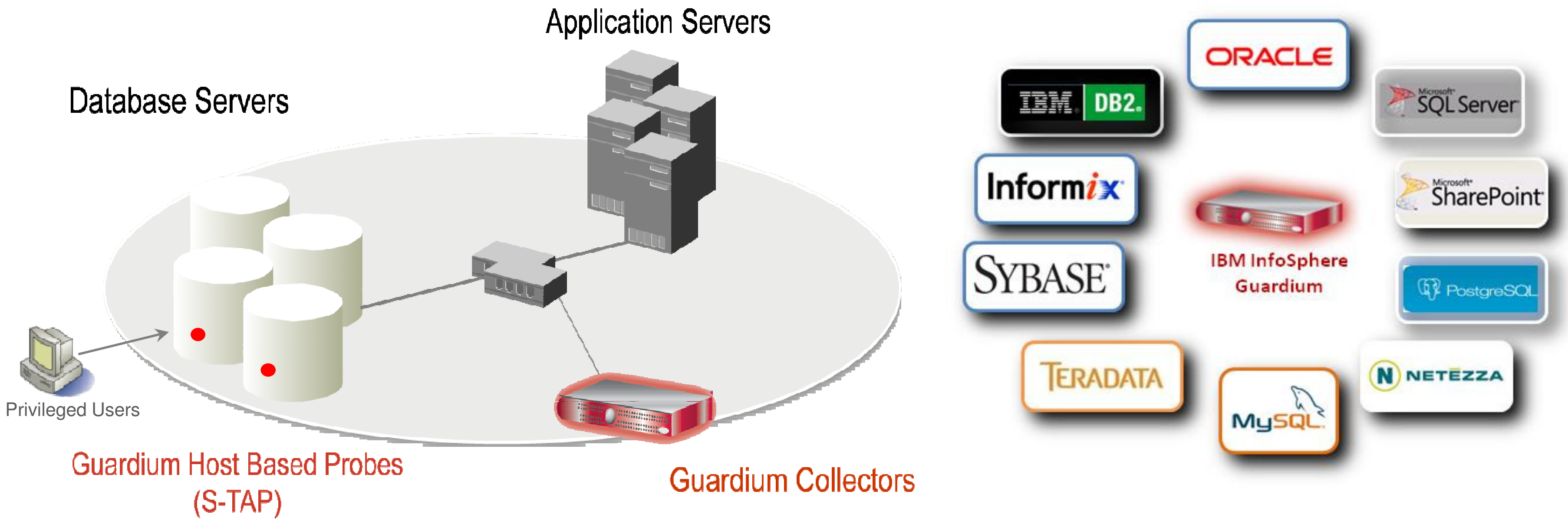
- Logs are complex and rarely reviewed
- Vulnerabilities are not resolved

× **No segregation of duties**

- Audit trail can be tampered with
- Privileged users can bypass the system

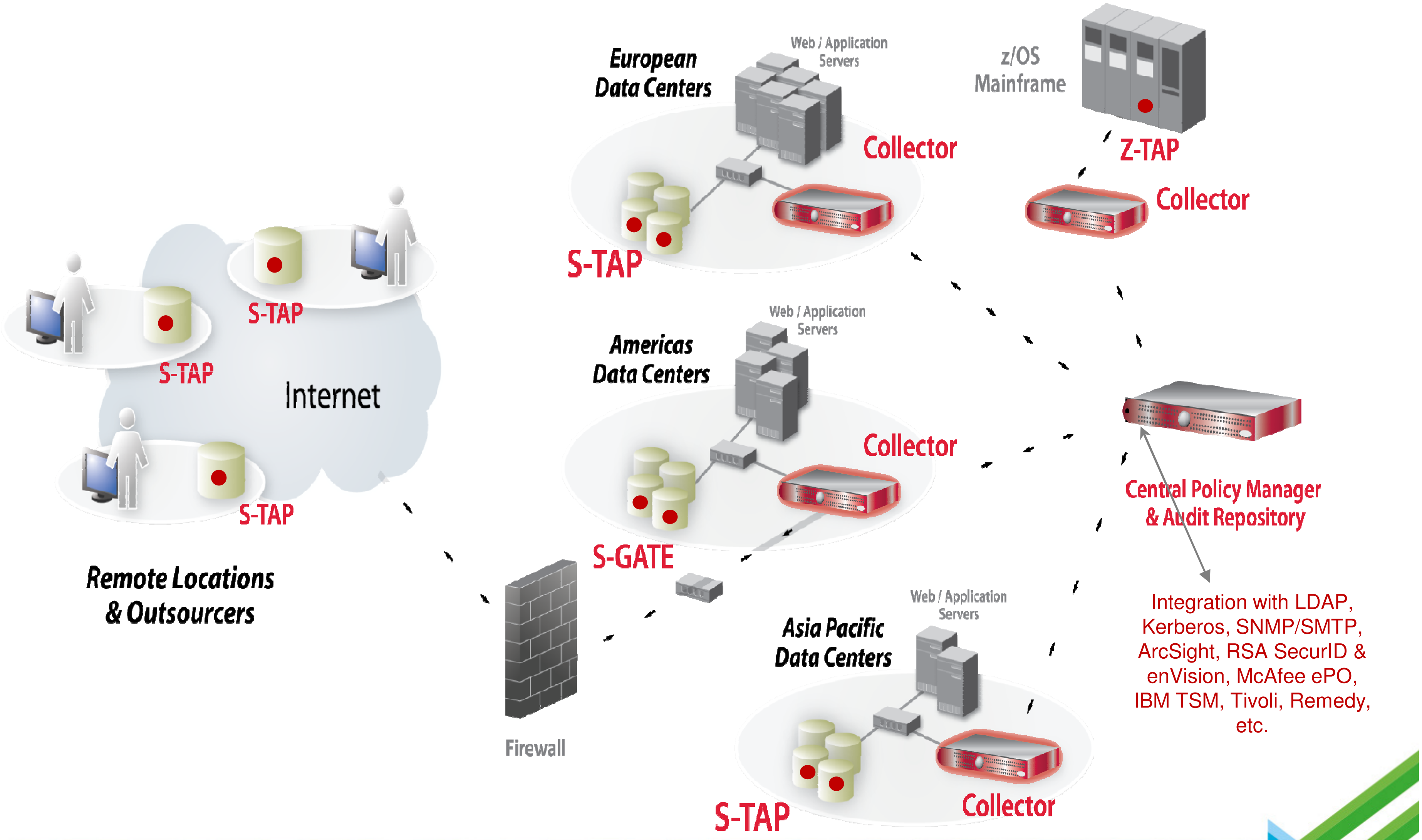


Real-Time Database Security & Monitoring



- 100% visibility including local DBA access
- No DBMS or application changes
- Minimal impact on DB performance
- Enforces separation of duties with tamper-proof audit repository
- Granular policies, monitoring & auditing providing the Who, What, When & How
- Real-time, policy-based alerting
- Can stores between 3-6 months worth of audit data on the appliance itself and integrates with archiving systems

Scalable Multi-Tier Architecture



Integration with LDAP, Kerberos, SNMP/SMTP, ArcSight, RSA SecurID & enVision, McAfee ePO, IBM TSM, Tivoli, Remedy, etc.

Summary

- Risks related to data privacy breaches have never been greater and most confidential data is on a database.

- Fine-grained monitoring of database access is the best way to protect from information being compromised

- A unified and consistent approach across the database infrastructure will save time, money, and increase security

- Guardium continues to be the market leader because of comprehensive functionality and ease of implementation

Netherlands Case Study

IBM SolutionsConnect 2013
Turning Opportunity into Outcomes.

Netherlands Case Study

Louis Joosse – BPSolutions

Principal Consultant Information Management

Case description

- A typical case
- Implementation scenario
- Results

AkzoNobel
Tomorrow's Answers Today

Why wait for a data breach?

A typical case

- **Outsourced infrastructure**
  - Several ‘trusted’ parties and ( ) owner have potential access to data
- **SAP enterprise application landscape**
  - High-value confidential data
  - Some critical tables

Who is accessing data, what is going on and can I accept/reject immediately?

Risk mitigation:

Governance issue or Information Management ?

- **Governance**
  - Provide oversight, assess compliance, manage risks
- **Information Management**
  - How can the desired level of security be supported
  - How can compliance be enforced

How to secure data, intercept inappropriate actions, and trust reports about activity history?

Implementation scenario

- Monitor and protect a selected set of tables
  - Continuously track actions
  - Detect or block unapproved activity
    - Not relying on native logs and triggers
- Simplified audit and validation processes
- Report the results for data governance and audit-compliance

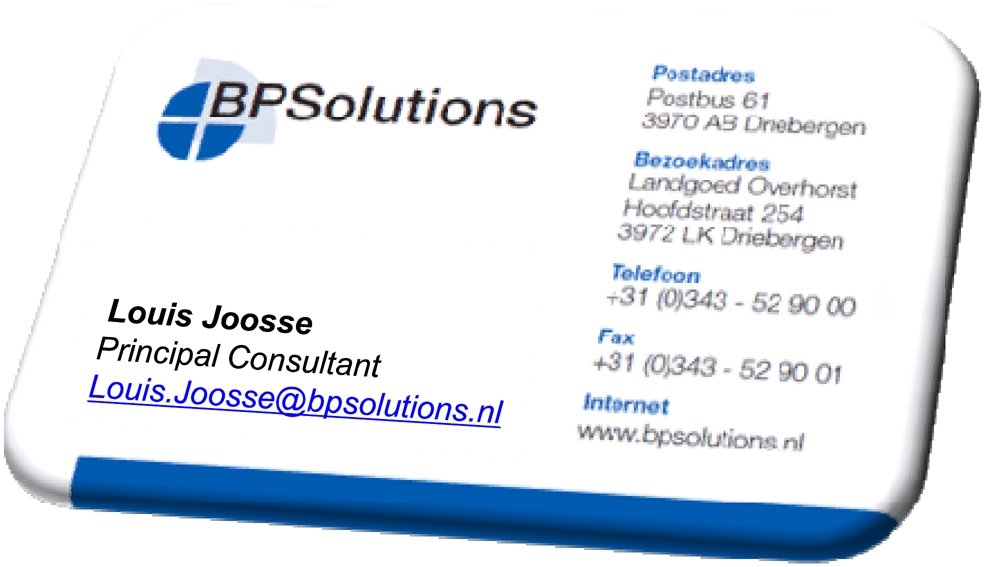
Support the rules of governance!

Benefits

- Maintain security on a key ERP outsourcing
  - Automate and simplify audit process
  - Without impact the performance of secured systems
- Show the results of data security compliance
  - Internally
  - Auditors

Your case?

- Protect high-value / business critical data?
- Simplify auditing and reporting process?
- Support information governance rules?
- Enforce compliance?
- Enable ‘security thinking’?



BPSolutions

Louis Joosse
Principal Consultant
Louis.Joosse@bpsolutions.nl

Postadres
Postbus 61
3970 AB Driebergen

Bezoekadres
Landgoed Overhorst
Hoofdstraat 254
3972 LK Driebergen

Telefoon
+31 (0)343 - 52 90 00

Fax
+31 (0)343 - 52 90 01

Internet
www.bpsolutions.nl