Information Management

IBM

Data Management

IBM Guardium

Jan Musil (jan_musil@cz.ibm.com)
Community of Practice for CEEMEA

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Agenda

- The Guardium Solution
- Problems with Native Database Audit
- The Guardium Architecture
- Full Cycle of Securing Critical Data Infrastructure
- Integration with Existing Infrastructure
- DB Security Maturity Model – A Phased Approach
- Summary

Who is Guardium?

- Since 2002, Guardium has been the leader in the Database Activity Monitoring market
- 400+ customers around the globe
- Banking customers include Citibank, Bank of America, HSBC, ING, RBS, and Societe Generale
- Since Dec 2009, part of IBM's Integrated Data Management portfolio

Guardium provides our customers with…

- Real-time monitoring of all database access
- Policy-based controls to rapidly detect unauthorized or suspicious activity
- Automated compliance workflow to efficiently meet regulatory requirements
- Centralized control and policy enforcement for most database and application environments
  - Informix, DB2, Oracle, SQL Server, z/OS, Sybase, etc
  - SAP, Siebel, Oracle EBS, PeopleSoft, WebSphere, etc

Top Regulations Impacting Database Security

Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

Database Activity Monitoring (DAM) Supported Platforms

Supported Platforms	Supported Versions
IBM Informix	7, 8, 9, 10,11
IBM DB2 LUW (Windows, Unix, z/Linux)	8.0, 8.2, 9.1, 9.5
IBM DB2 for z/OS	7, 8, 9, 9.5
IBM DB2 LUW for iSeries (AS/400)	V5R2, V5R3, V5R4, V6R1
Oracle	8i, 9i, 10g (r1, r2), 11g, 11i
Microsoft SQL Server	2000, 2005, 2008
MySQL	4.1, 5.0, 5.1
Sybase ASE	12, 15
Sybase IQ	12.6
Teradata	6.01, 6.02

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

How are most databases audited today?

Reliance on native audit logs within DBMS

× Lacks visibility and granularity

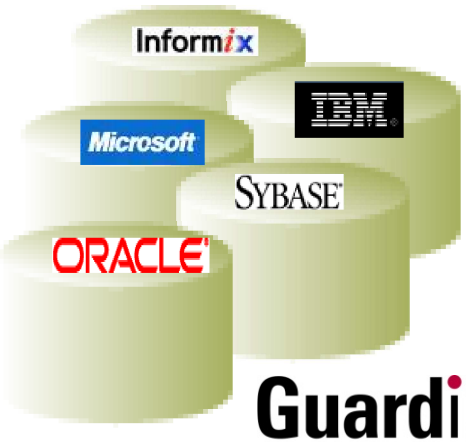
- Privileged users difficult to monitor
- Tracing the “real user” of application is difficult
- Level of audit detail is insufficient

× Inefficient and costly

- Impacts database performance
- Cumbersome reporting, forensics and alerting
- Different methods for each DB type

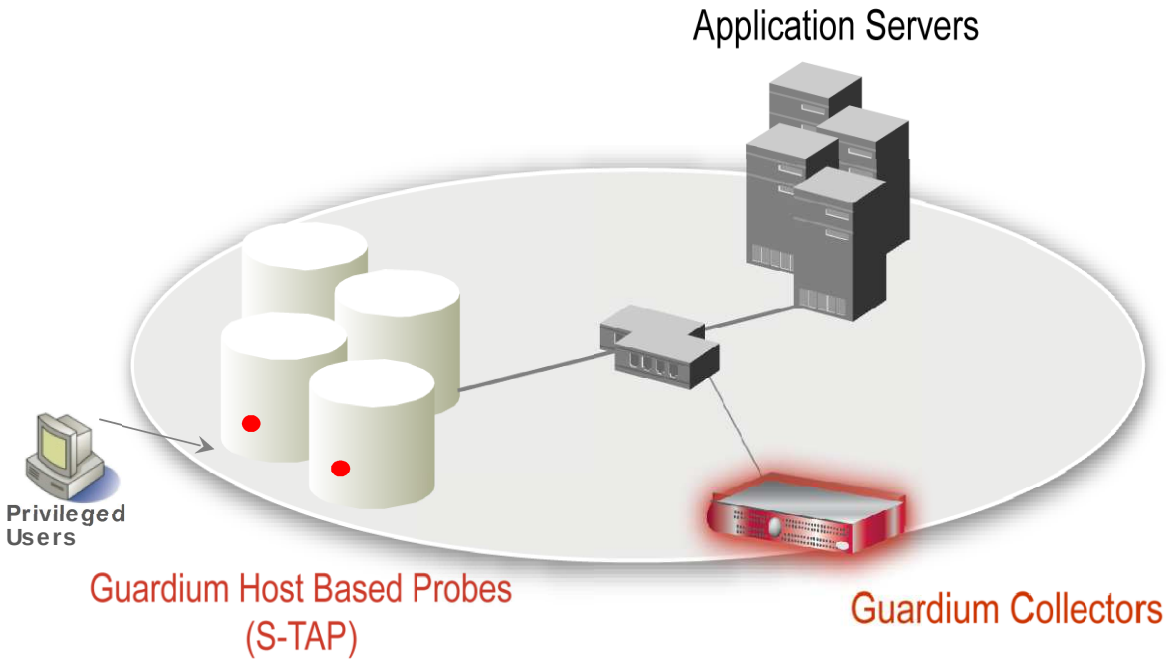
× No segregation of duties

- DBAs manage monitoring system
- Privileged users can bypass the system
- Audit trail is unsecured



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Real-Time Database Security & Monitoring



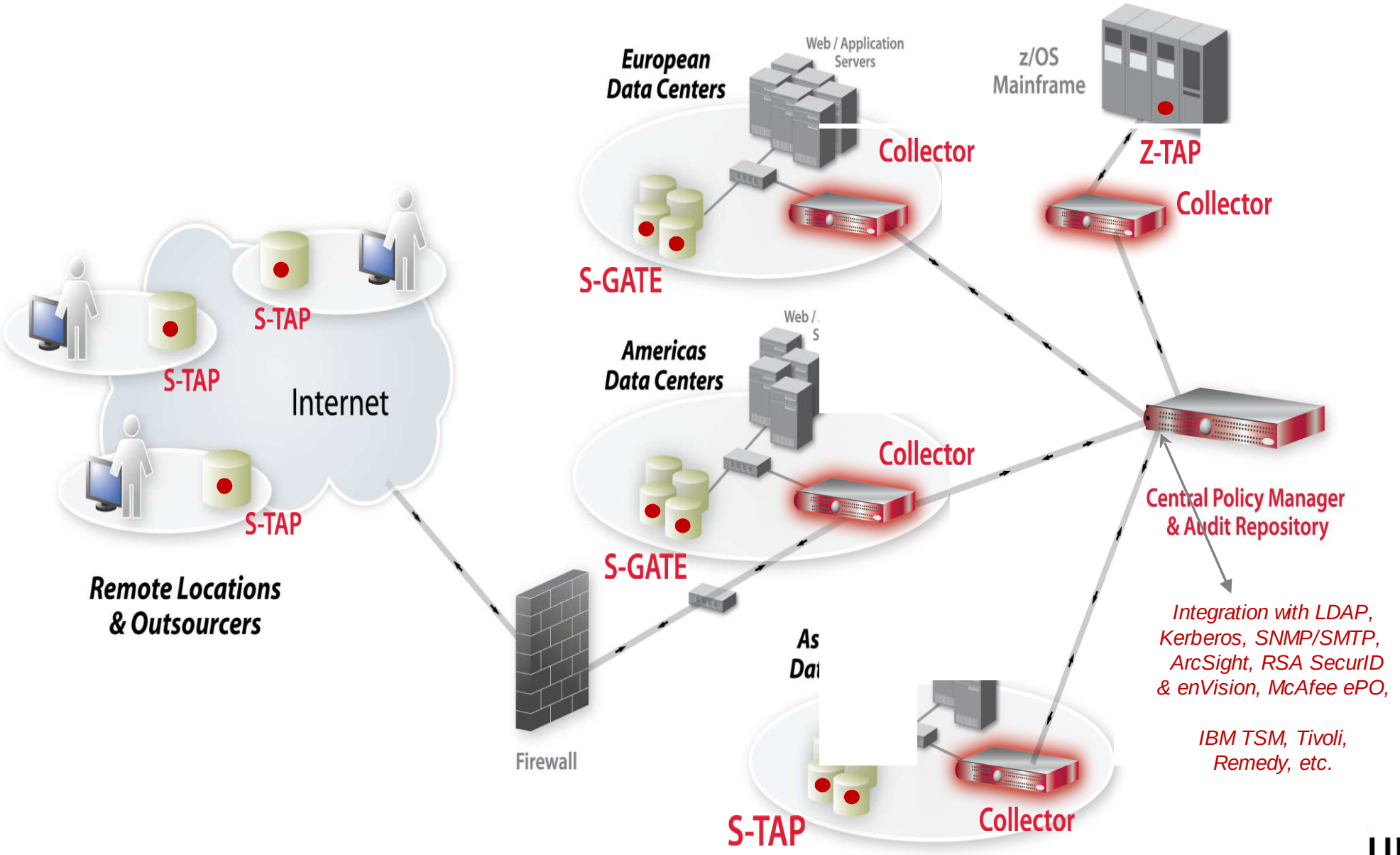
Informix
IBM DB2
Microsoft SQL Server
TERADATA
SYBASE
MySQL
ORACLE

- 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

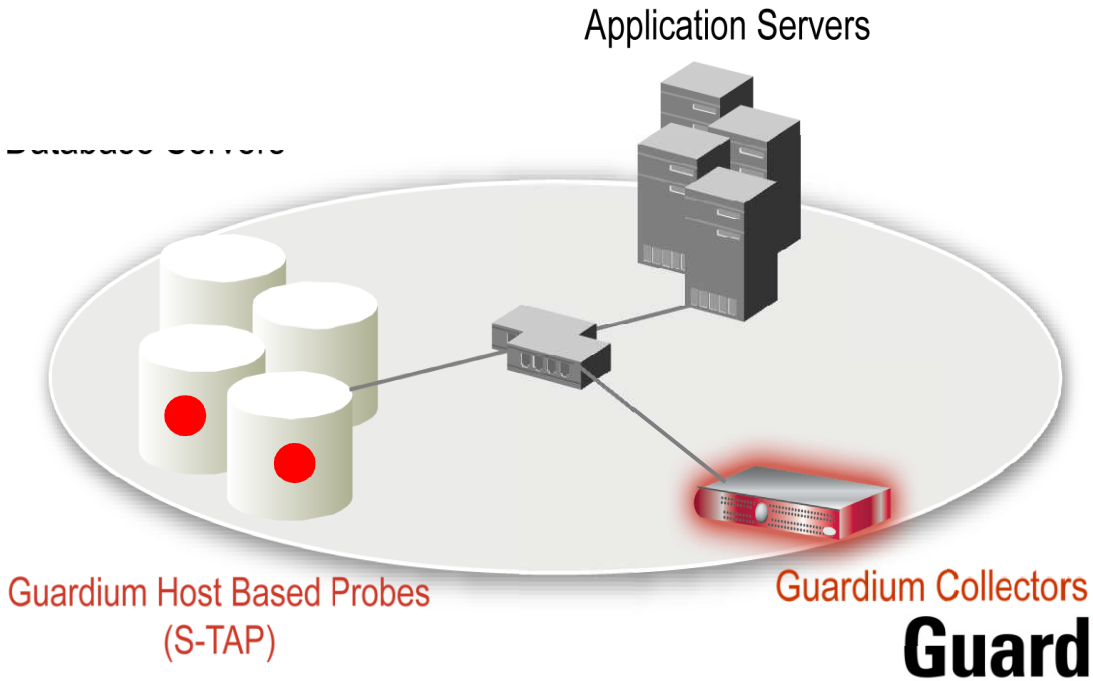
Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Scalable Multi-Tier Architecture



What does Guardium monitor?

- SQL Errors and failed logins
- DDL commands (Create/Drop/Alter Tables)
- SELECT queries
- DML commands (Insert, Update, Delete)
- DCL commands (Grant, Re
- Procedural languages
- XML executed by databa
- Returned results sets



Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Application User Monitoring with Guardium

Identify Users within Connection Pooling applications

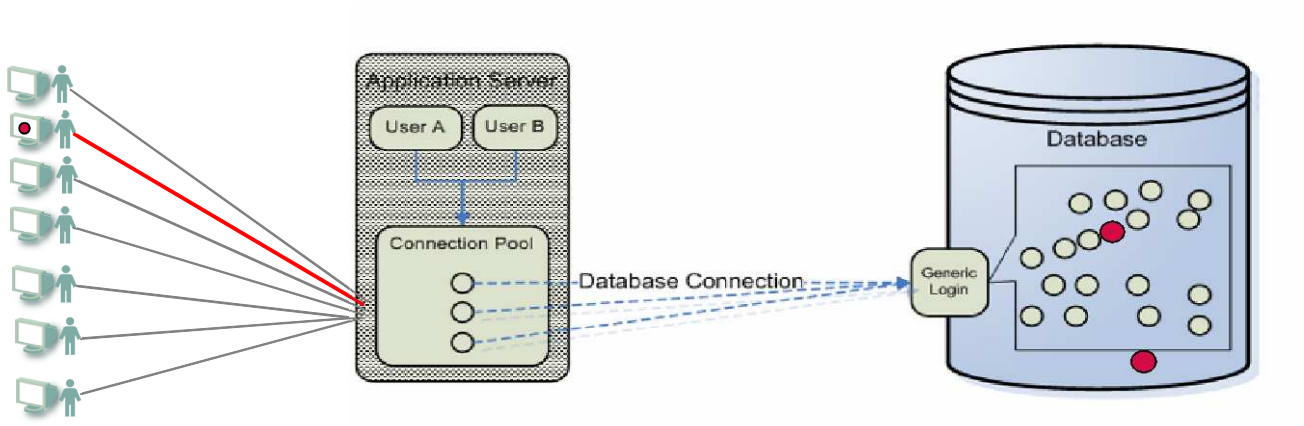
- Uncover potential fraud
- Accurate audits of user access to sensitive tables

Supported Enterprise Applications

- Oracle E-Business Suite, PeopleSoft, Business Objects Web Intelligence, JD Edwards, SAP, Siebel, In-house custom applications

Various Methods Used to Capture Application User ID

- Collect unique ID from the underlying database via table, trigger, etc.
- Monitor calls to a procedures and fetch information from their parameters
- S-TAP probe on application or proxy server grabs the user ID



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Full Cycle of Securing Critical Data Infrastructure

- Discover all databases, applications & clients
- Discover & classify sensitive data

Full Cycle of Securing Critical Data Infrastructure

- Discover all databases, applications & clients
- Discover & classify sensitive data

- Vulnerability assessment
- Configuration assessment
- Behavioral assessment
- Baselining
- Configuration lock-down & change tracking
- Encryption

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Full Cycle of Securing Critical Data Infrastructure

- Discover all databases, applications & clients
- Discover & classify sensitive data

- Vulnerability assessment
- Configuration assessment
- Behavioral assessment
- Baselining
- Configuration lock-down & change tracking
- Encryption

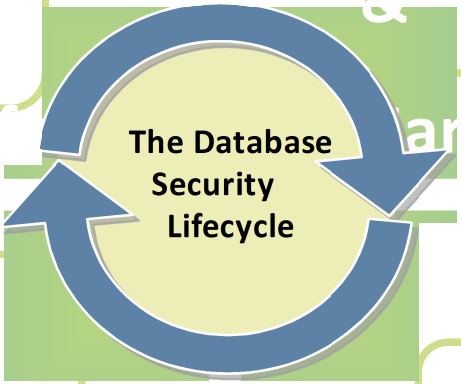
- 100% visibility
- Policy-based actions
- Anomaly detection
- Real-time prevention
- Granular access controls

Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Full Cycle of Securing Critical Data Infrastructure

- Discover all databases, applications & clients
- Discover & classify sensitive data

- Vulnerability assessment
- Configuration assessment
- Behavioral assessment
- Baselining
- Configuration lock-down & change tracking
- Encryption

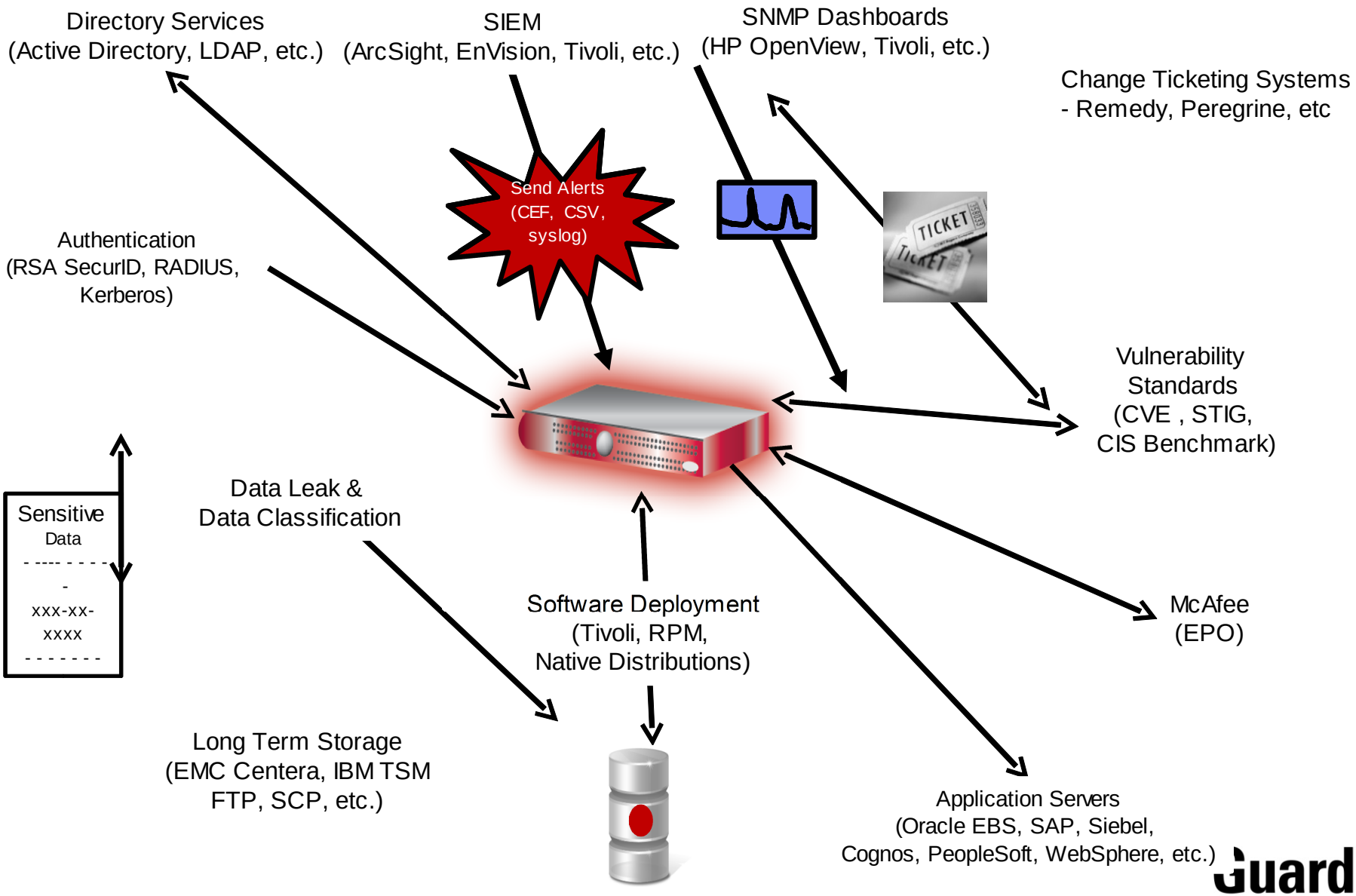


- Centralized governance
- Compliance reporting
- Sign-off management
- Automated escalations
- Secure audit repository
- Data mining for forensics
- Long-term retention

- 100% visibility
- Policy-based actions
- Anomaly detection
- Real-time prevention
- Granular access controls

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Integration with Existing Infrastructure Lowers TCO



Guardium®
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

DB Security Maturity Model – A Phased Approach

Guardium
SAFEGUARDING DATABASES™ | AN IBM® COMPANY

Summary

- Risks related to data privacy breaches have never been greater
- Fine-grained monitoring of database access is the best way to protect from data 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