IBM InfoSphere Guardium

Enterprise-wide Database Protection and Compliance

Jānis Bērziņš, DPA
08.11.2012

Data is the key target for security breaches…..

… and Database Servers Are The Primary Source of Breached Data

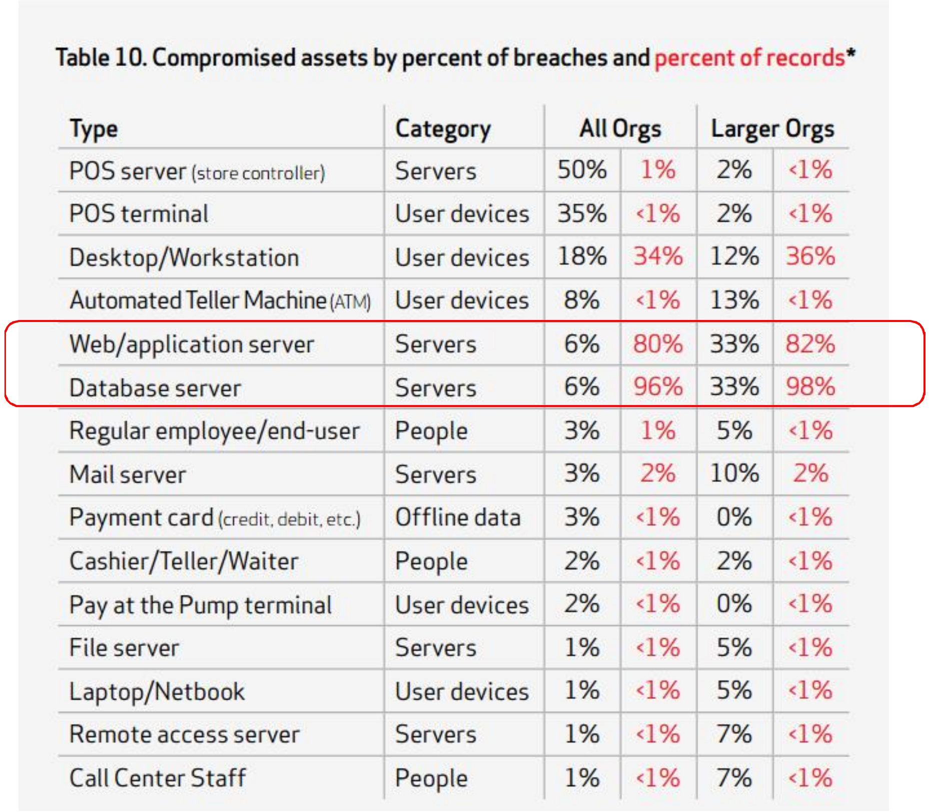


Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
POS terminal	User devices	35%	<1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Regular employee/end-user	People	3%	1%	5%	<1%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

WHY?

2012 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

- Database servers contain your client's most valuable information
  - **Financial records**
  - **Customer information**
  - **Credit card and other account records**
  - **Personally identifiable information**
  - **Patient records**
- High volumes of structured data
- Easy to access

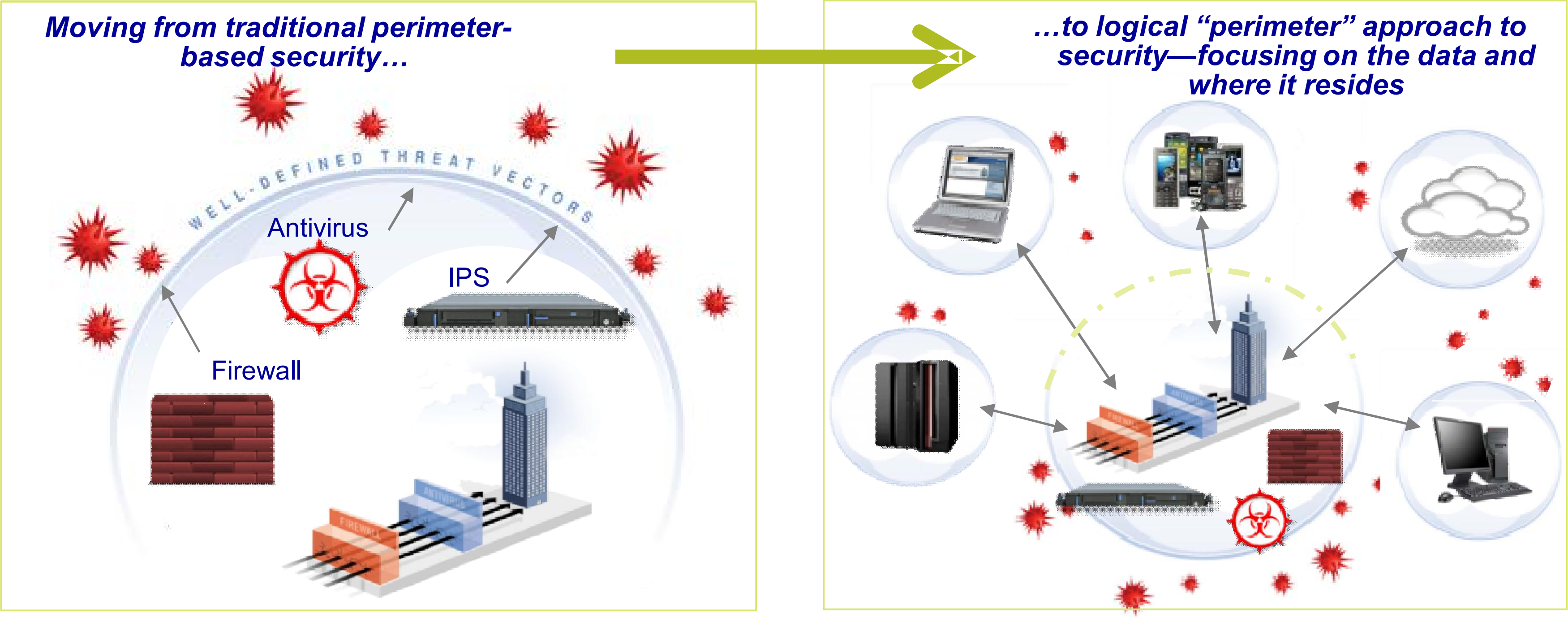
> **"Go where the money is… and go there often."**
>
> **Willie Sutton**

Data Governance and Security are changing rapidly

Data Explosion | Consumerization of IT | Everything is Everywhere | Attack Sophistication

↓ ↓ ↓ ↓

Extending the Perimeter Shifts Protection Focus to Data

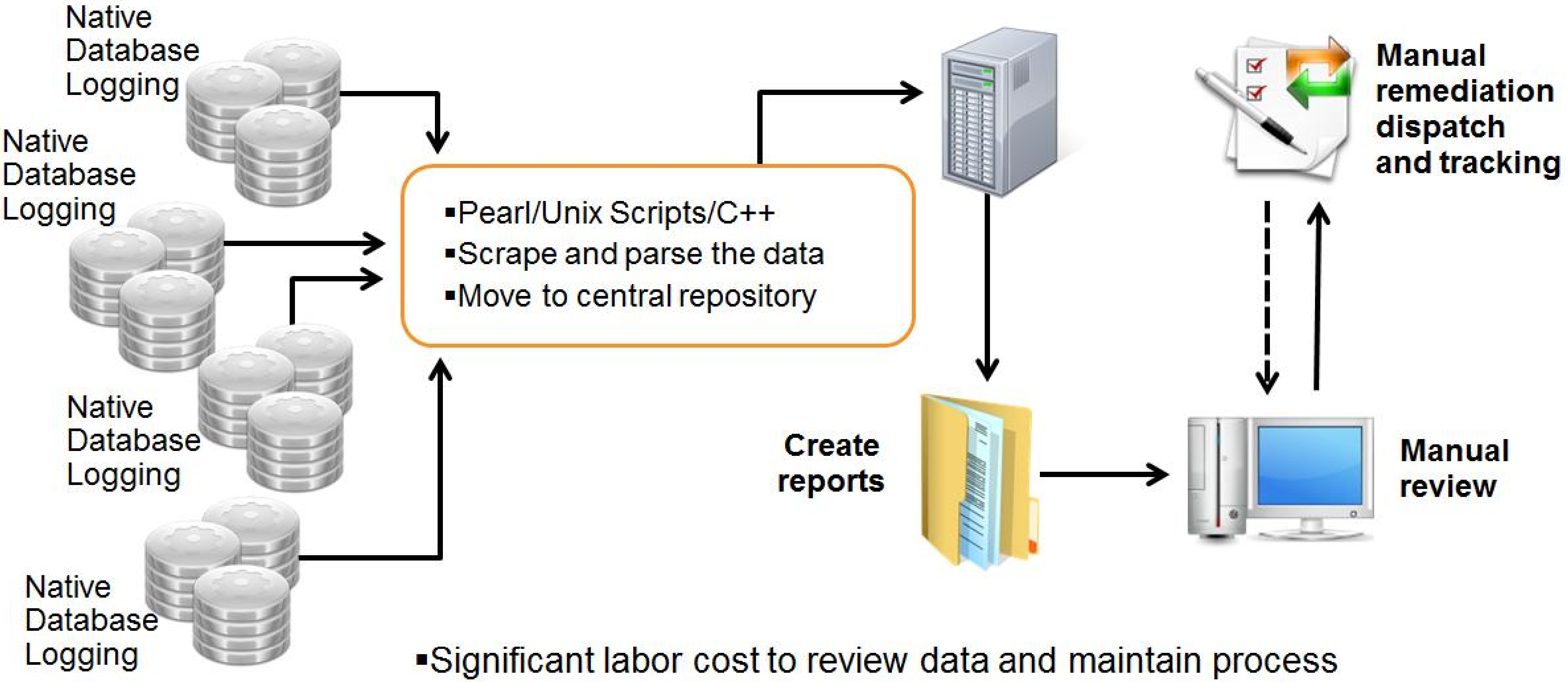


Moving from traditional perimeter-based security…

…to logical "perimeter" approach to security—focusing on the data and where it resides

- Cloud, Mobile and Data momentum is breaking down the traditional perimeter and forcing us to look at security differently
- Focus needs to shift from the perimeter to the data that needs to be protected

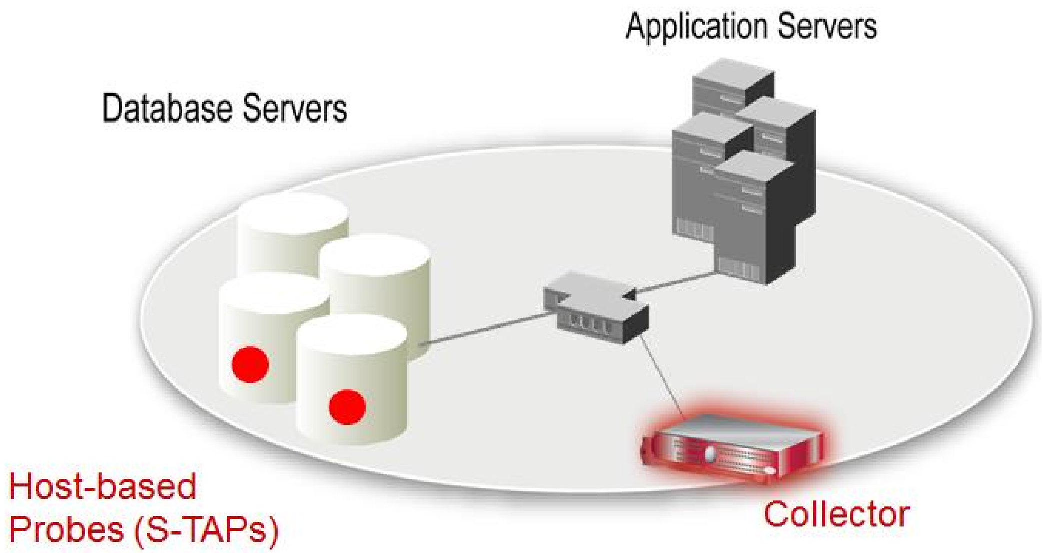
Typical home-grown solutions are costly and ineffective

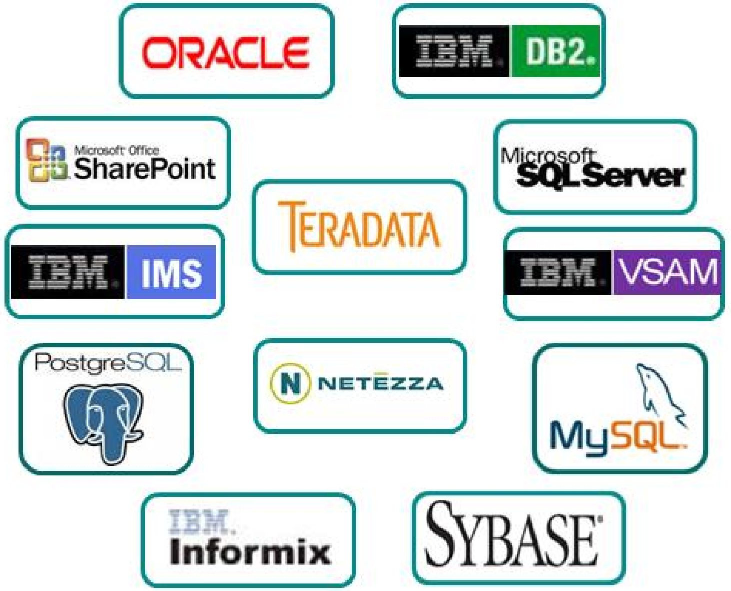


- Pearl/Unix Scripts/C++
- Scrape and parse the data
- Move to central repository

- Significant labor cost to review data and maintain process
- High performance impact on DBMS from native logging
- Not real time
- Does not meet auditor requirements for Separation of Duties
- Audit trail is not secure
- Inconsistent policies enterprise-wide

Real time database monitoring and protection with InfoSphere Guardium





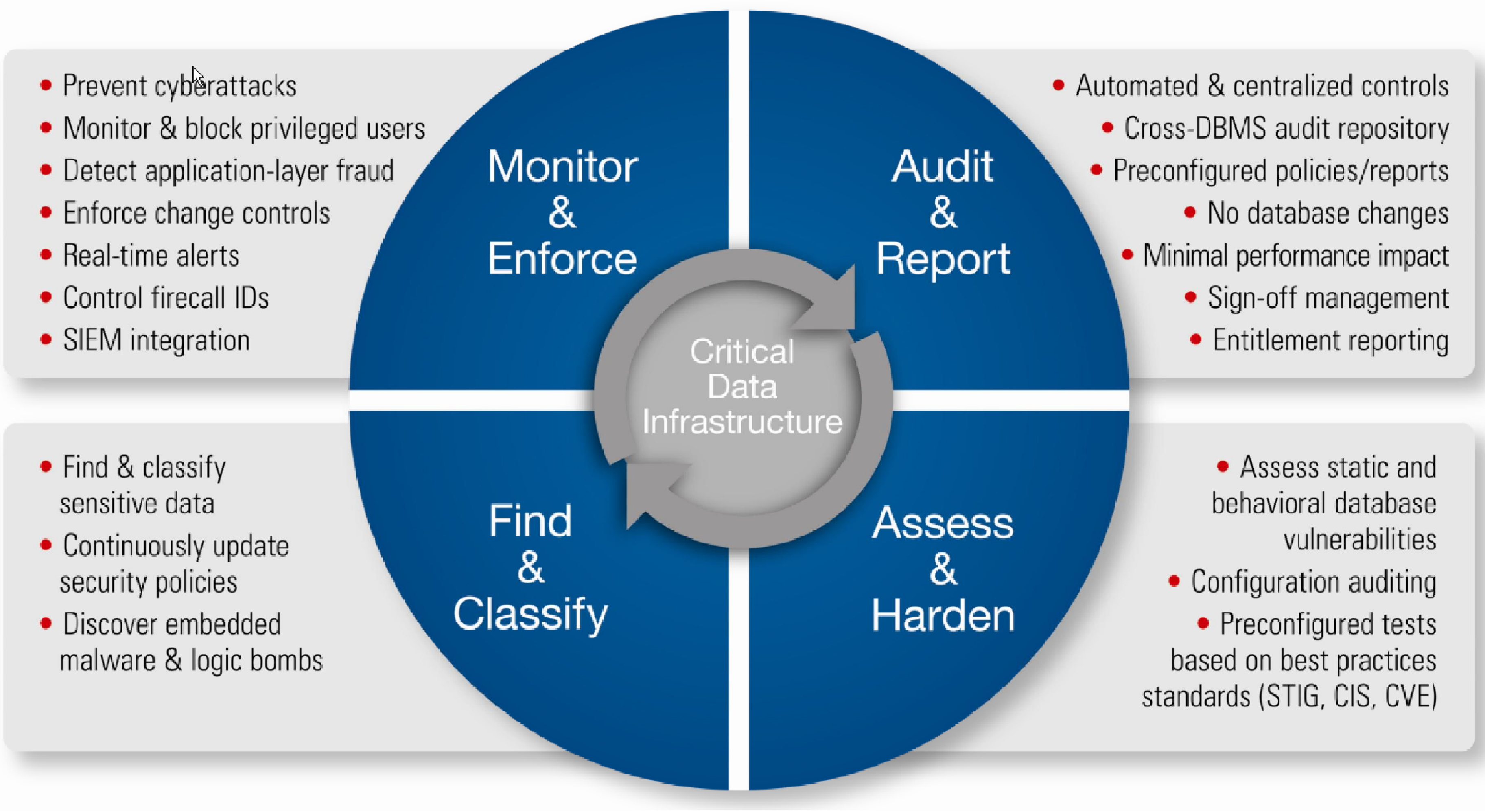
- No DBMS or application changes
- Does not rely on DBMS-resident logs that can easily be erased by attackers, rogue insiders
- 100% visibility including local DBA access
- Minimal performance impact

- Cross-DBMS solution
- Granular, real-time policies & auditing

–*Who, what, when, how*

- Automated compliance reporting, sign-offs and escalations (financial regulations, PCI DSS, data privacy regulations, etc.)

Addressing the full database security lifecycle with IBM InfoSphere Guardium



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

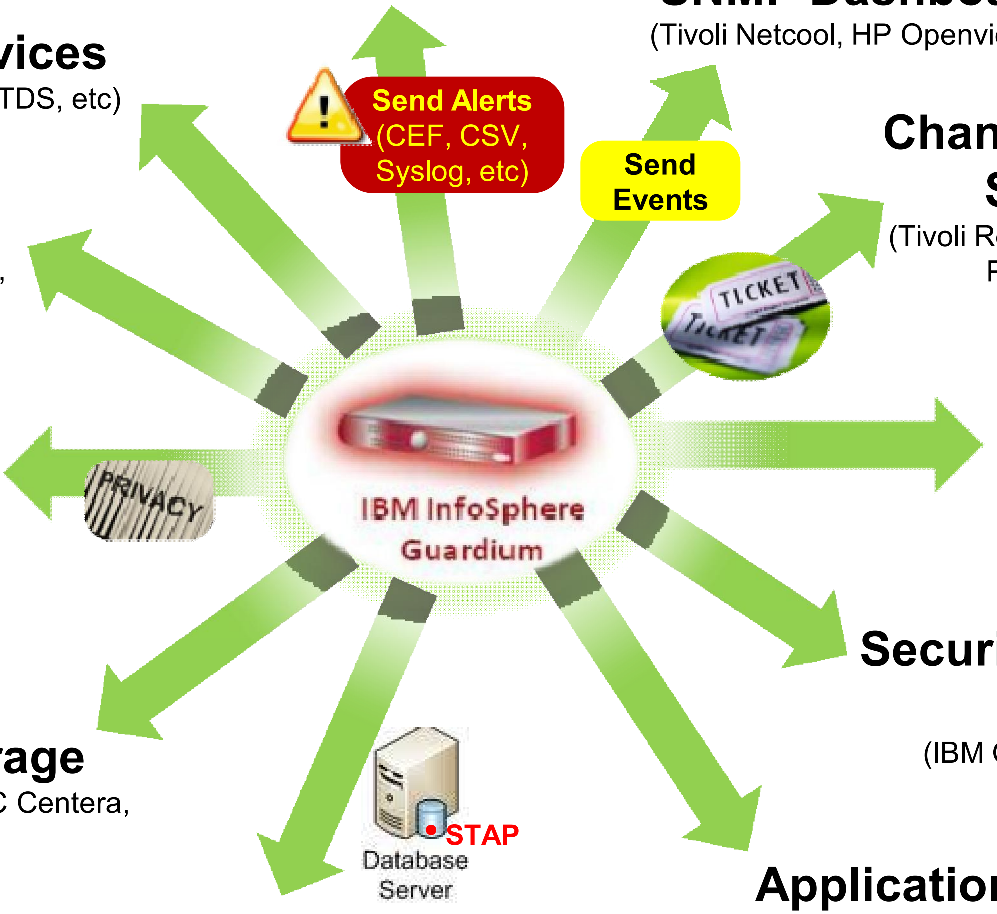
- Find & classify sensitive data
- Continuously update security policies
- Discover embedded malware & logic bombs

Assess & Harden

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

Critical Data Infrastructure

Guardium integrates with IT Infrastructure for seamless operations



SIEM
(IBM QRadar, Arcsight, RSA Envision, etc)

SNMP Dashboards
(Tivoli Netcool, HP Openview, etc)

Change Ticketing Systems
(Tivoli Request Mgr, Remedy, Peregrine, etc)

Vulnerability Standards
(CVE, STIG, CIS Benchmark)

Security Management Platforms
(IBM QRadar, McAfee ePO)

Application Servers
(IBM Websphere, IBM Cognos, Oracle EBS, SAP, Siebel, Peoplesoft, etc)

Software Deployment
(IBM Tivoli Provisioning Manager, RPM, Native Distributions)

Long Term Storage
(IBM TSM, IBM Nettezza, EMC Centera, FTP, SCP, etc)

Data Classification and Leak Protection
(Credit Card, Social Security, phone, custom, etc)

Authentication
(RSA SecurID, Radius, Kerberos, LDAP)

Directory Services
(Active Directory, LDAP, TDS, etc)

Database Activity Monitoring

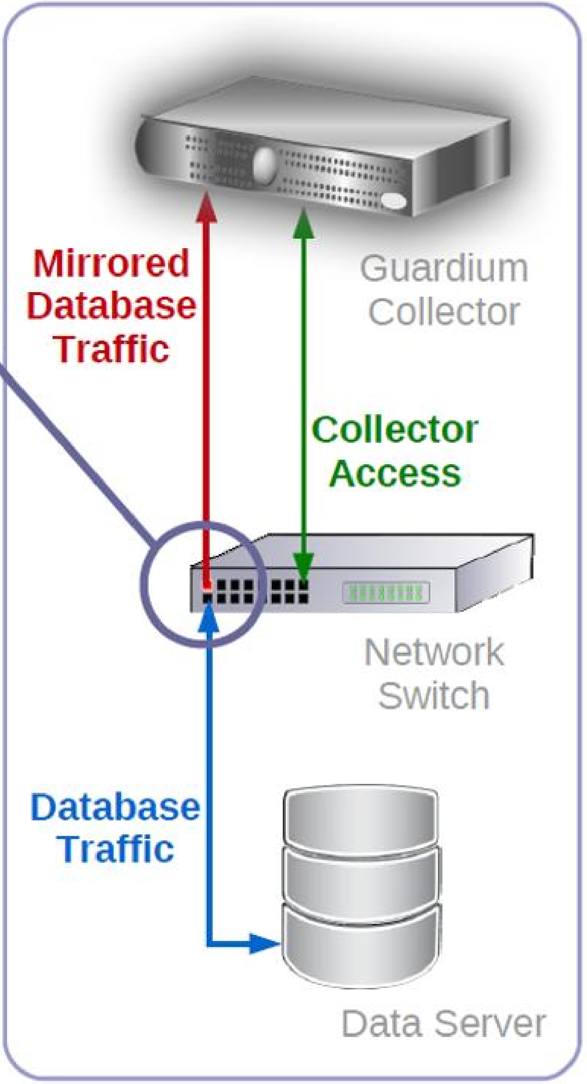
- Database activity needs to be captured to perform parsing, analysis, and auditing
  - Session information
  - Failed log-in attempts
  - SQL commands
  - SQL errors
  - Returned data
- Mechanisms in which the database is accessed
  - Network access
  - Local access
  - Encrypted connection
- Monitoring options
  - Port Mirroring
  - Network Tap
  - Software Tap

Port Mirroring

Copy of network packets observed on the switch port connected to the data server is sent to the Collector

- No impact on data server performance
- Requires network switch with port mirroring:
  - Switched Port Analyzer (SPAN)
  - Roving Analysis Port (RAP)
- Requires direct connection to the Collector
- Existing switch may not be able to accommodate multiple data servers connected to that switch
- Added cost of network switch with port mirroring feature
- Encrypted and local connections will not be monitored

Only recommended if network hardware already exists and data server cannot handle any additional software load

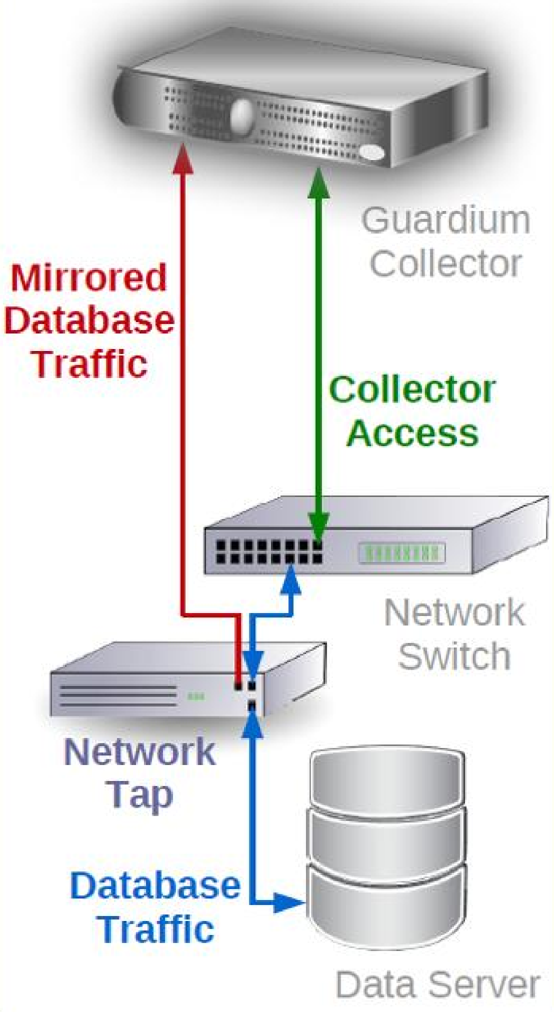


Network Tap

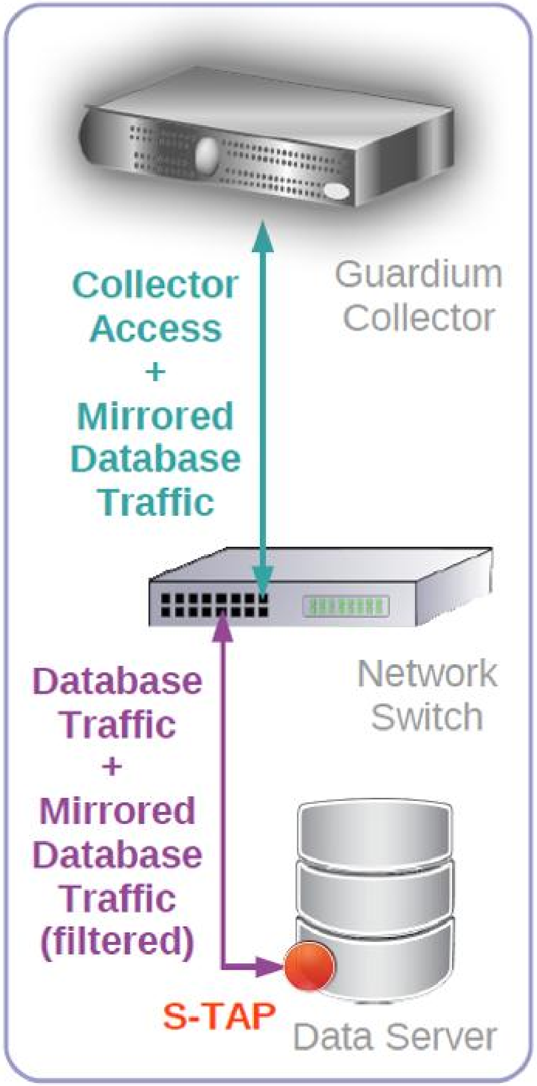
Dedicated network tap hardware sends copy of data server traffic is to Collector (similar to port mirroring)

- No dependency on existing network hardware
- No impact on data server performance
- Added cost of network tap for each data server
- Requires direct connection to the Collector
- Data server has to be taken offline for installation
- Encrypted and local connections will not be monitored

Only recommended if data server has a high load and cannot handle any additional software load



Software TAP (S-TAP)



Host-based DBMS-independent software agent that sends network and local database activities to Collector

- Monitors all database activities at Operating System level:
  - TCP, Shared Memory, Named Pipes, Bequeath
- Handles encrypted traffic:
  - SSH/IPSEC, Oracle ASO, SQL Server SSL
- Does not require any changes to database environment
- Installed only once on every system regardless of how many database instances and types are running on that system
- No additional hardware cost and lower implementation cost
- Specific traffic can be filtered such that not all traffic is sent to the Collector. This reduces network load significantly.
- Less than 5% performance impact on data server

S-TAP is the recommended database activity monitoring option

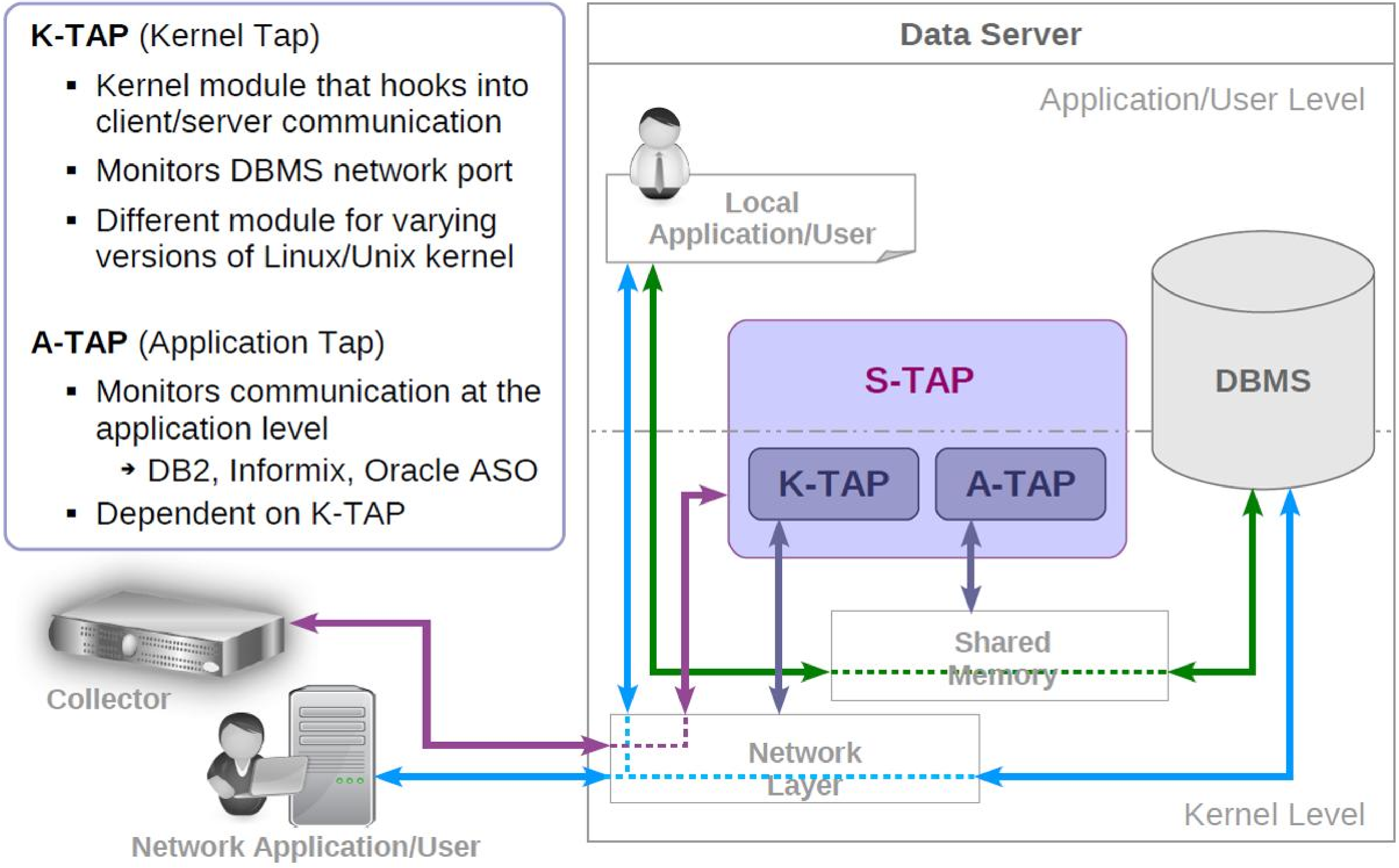
S-TAP Architecture

K-TAP (Kernel Tap)

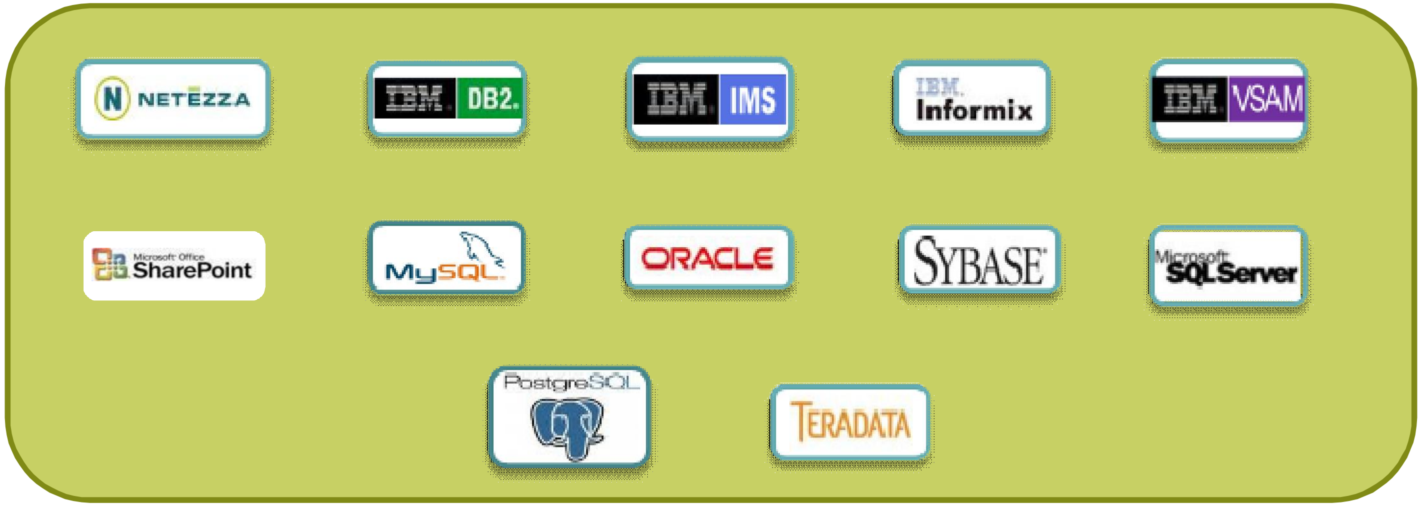
- Kernel module that hooks into client/server communication
- Monitors DBMS network port
- Different module for varying versions of Linux/Unix kernel

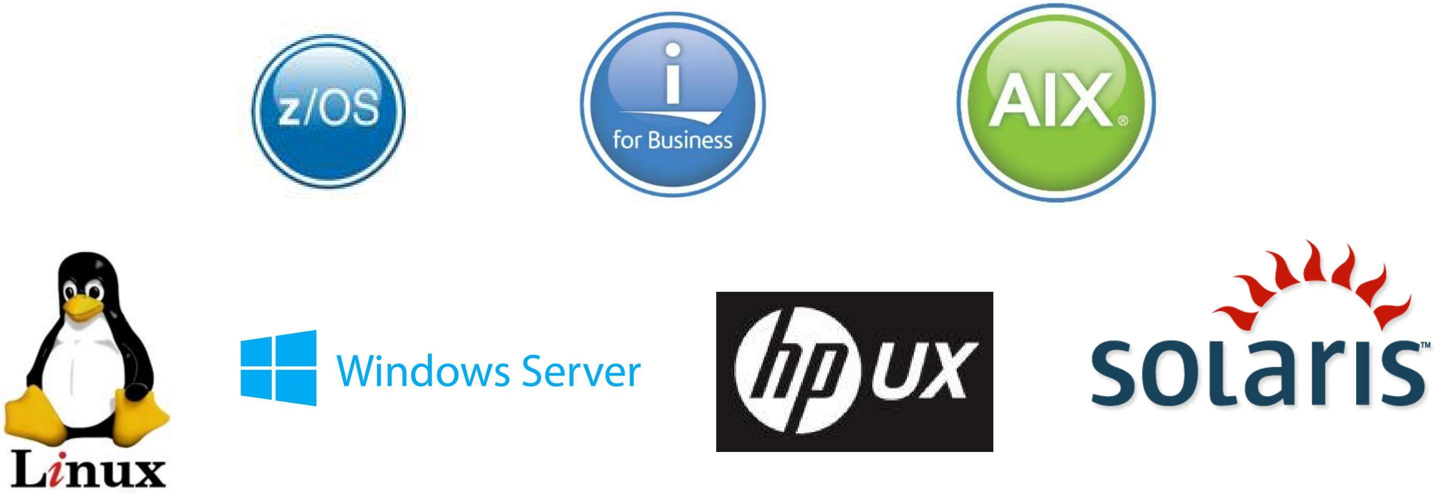
A-TAP (Application Tap)

- Monitors communication at the application level
  - DB2, Informix, Oracle ASO
- Dependent on K-TAP



Supported Operating Systems and DBMS





What Guardium offers?

- Data base auto discovery
- Classifier
- Security policy and reporting
- Real time and correlation alerts
- S-Gate and quarantine
- Redact
- Configuration audit system (CAS)
- Vulnerability assessment
- Entitlement reports

DEMO

Guardium v.9.0 new features

- Expanded scope to all major databases, data warehouses, file systems and big data environments based on Hadoop, such as IBM InfoSphere BigInsights and Cloudera;
- Introducing support for Security Content Automation Protocol (SCAP) reports – allows exporting of reports in SCAP format (OVAL, XCCDF, CPE, CVE, CCE, CVSS)
- Expand system openness and integration with Universal Feed - Universal Feed opens InfoSphere Guardium system, enabling all capabilities to be applied to custom applications and niche data sources
- Extended data security platform coverage – STAP for System i, updated currency for existing support – Solaris-11, SQL Server 2012, DB2 Galileo, Oracle E-Business;
- Better integration with other IT infrastructure products

Paldies par uzmanību!

Supported OS

OS Type	Version	32-Bit & 64-Bit
AIX	5.3	Both (Note: DB2 SHM on 32-bit AIX not supported)
	6.1, 7.1	64-Bit
z/OS	1.11, 1.12	
HP-UX	11.11, 11.23, 11.31	Both
Red Hat Enterprise Linux (includes Oracle Linux)	4, 5, 6	Both
Red Hat Enterprise Linux for System z	5.4	
SuSE Enterprise Linux	9, 10, 11	Both
SuSE Enterprise Linux for System z	9, 10, 11	
Solaris - SPARC	9, 10, 11	Both
Solaris - Intel	10, 11	10-Both, 11-64-Bit only
Windows	2000, 2003, 2008	Both
IBM i	6.1, 7.1	

Supported DBMS

Data source	Supported Versions
Oracle	9i, 10g (r1, r2), 10g RAC,11gR1, 11gR2, 11g RAC
Oracle (ASO, SSL)	9i, 10g (r1, r2), 11gR1, 11gR2
Oracle Exadata	11gR2
Microsoft SQL Server	MS SQL Cluster, 2000, 2005, 2005 x64, 2005 IA64, 2008, 2008 x64, 2008 IA64, 2008 R2 x64/x32/Cluster, 2012
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, UNIX)	9.1, 9.5, 9.7, 10.1
IBM DB2 (Windows)	9.1, 9.5, 9.7, 10.1
IBM DB2 Purescale	9.8, LUW, 10.1
IBM DB2 for z/OS	8.1, 9.1, 10.1
IBM DB2 for i	6.1, 7.1
IMS	9, 10, 11, 12
VSAM	see OS version support, part of z/OS (not separately versioned)
IBM Informix	10, 11, 11.50, 11.70
Sun MySQL and MySQL Cluster	5.0, 5.1, 5.5
Sybase ASE	15, 15.5, 15.7
Sybase IQ	15.0, 15.1, 15.2, 15.3, 15.4
IBM Netezza	NPS 4.5, 4.6, 4.6.8, 5,0, 6.0, 6.02, 7.0
PostgreSQL	8, 9, 9.03, 9.04
Teradata	12, 13, 13.10, 14