
ORACLE®

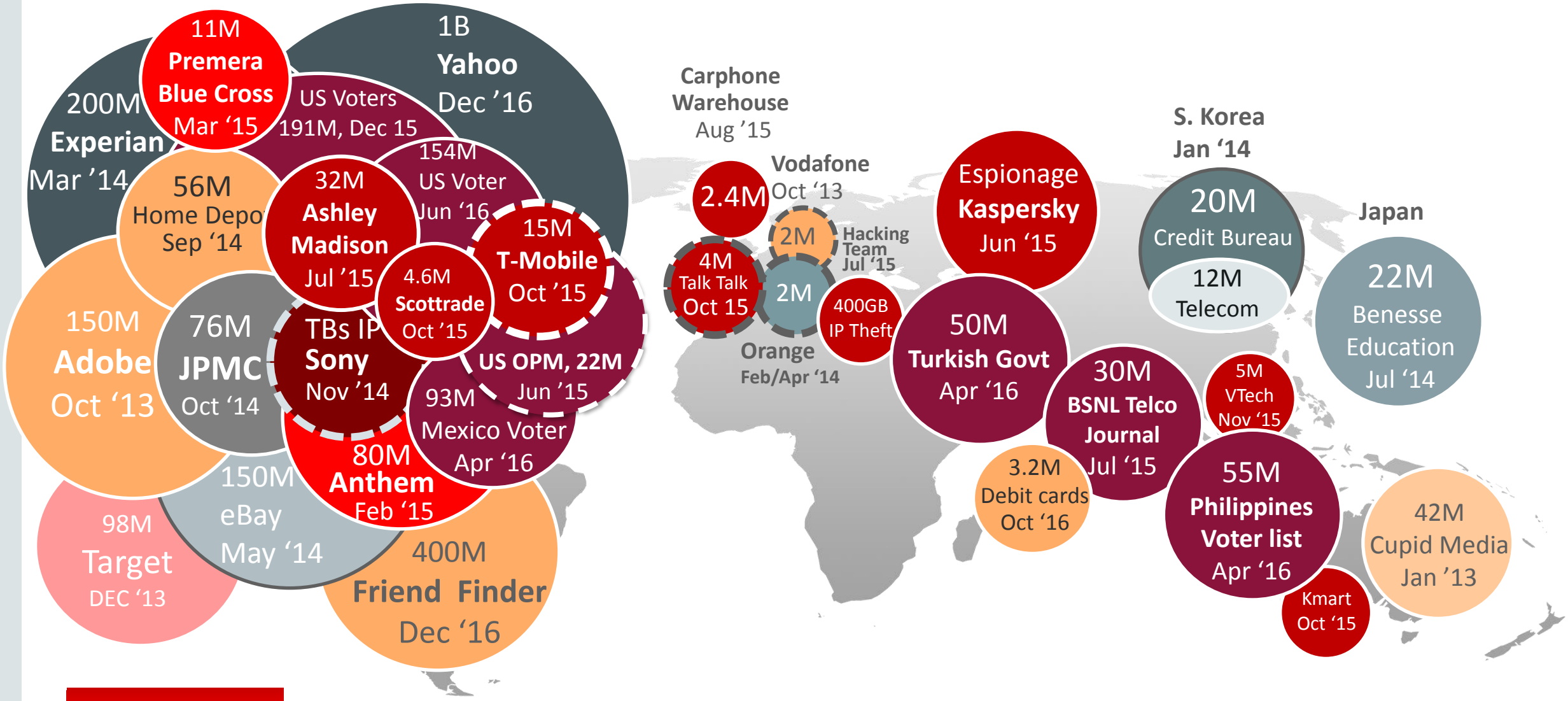
BẢO MẬT CƠ SỞ DỮ LIỆU
Database Security

ORACLE

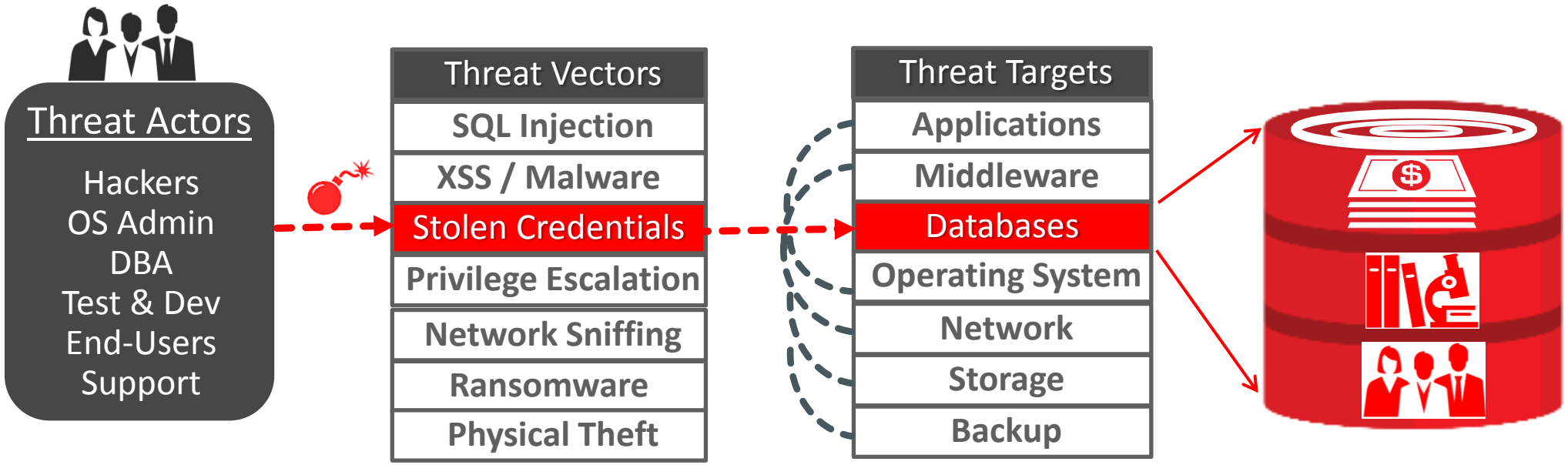
Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Thất thoát dữ liệu đang diễn ra khắp thế giới



Thay đổi cách thức tấn công
Databases vẫn là mục tiêu chính

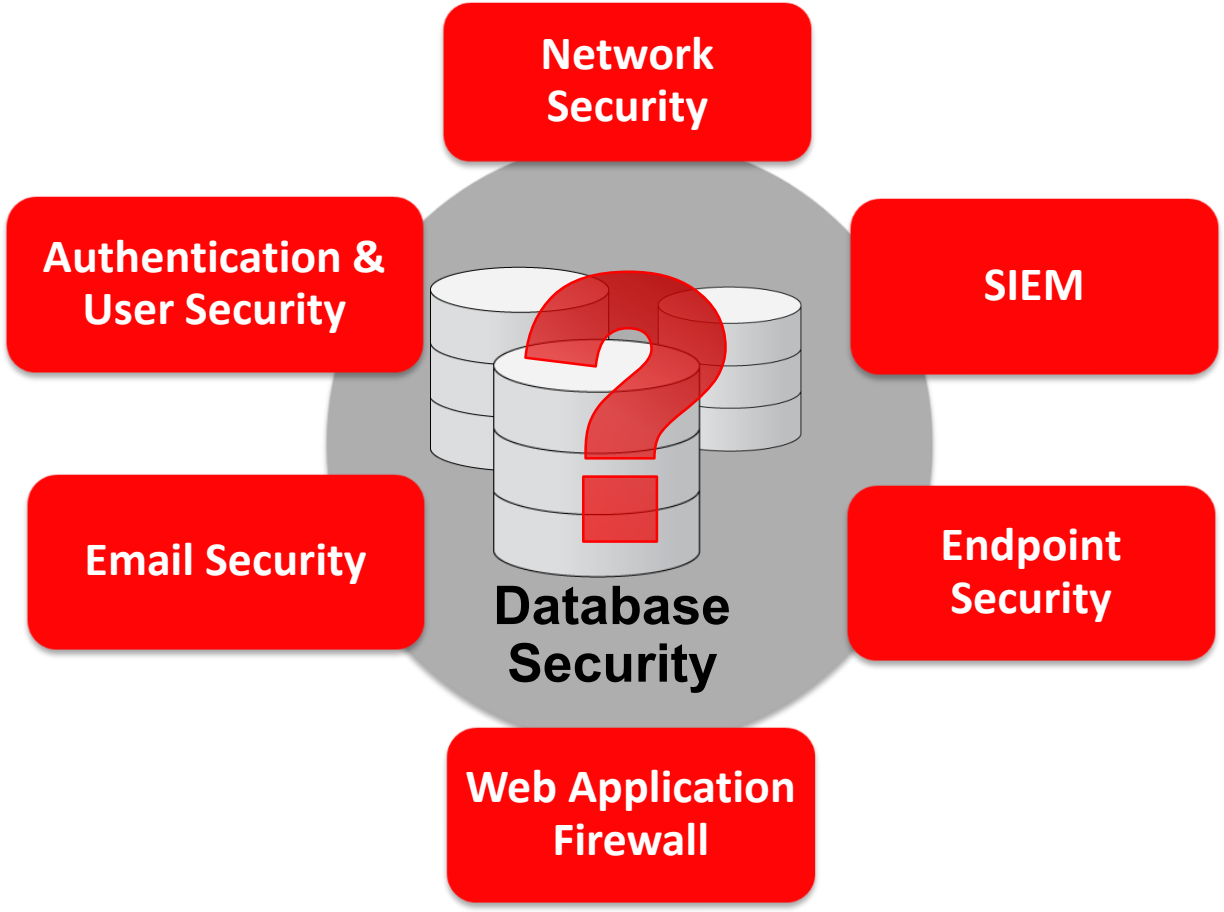


Tại sao CSDL lại dễ bị tấn công như vậy?

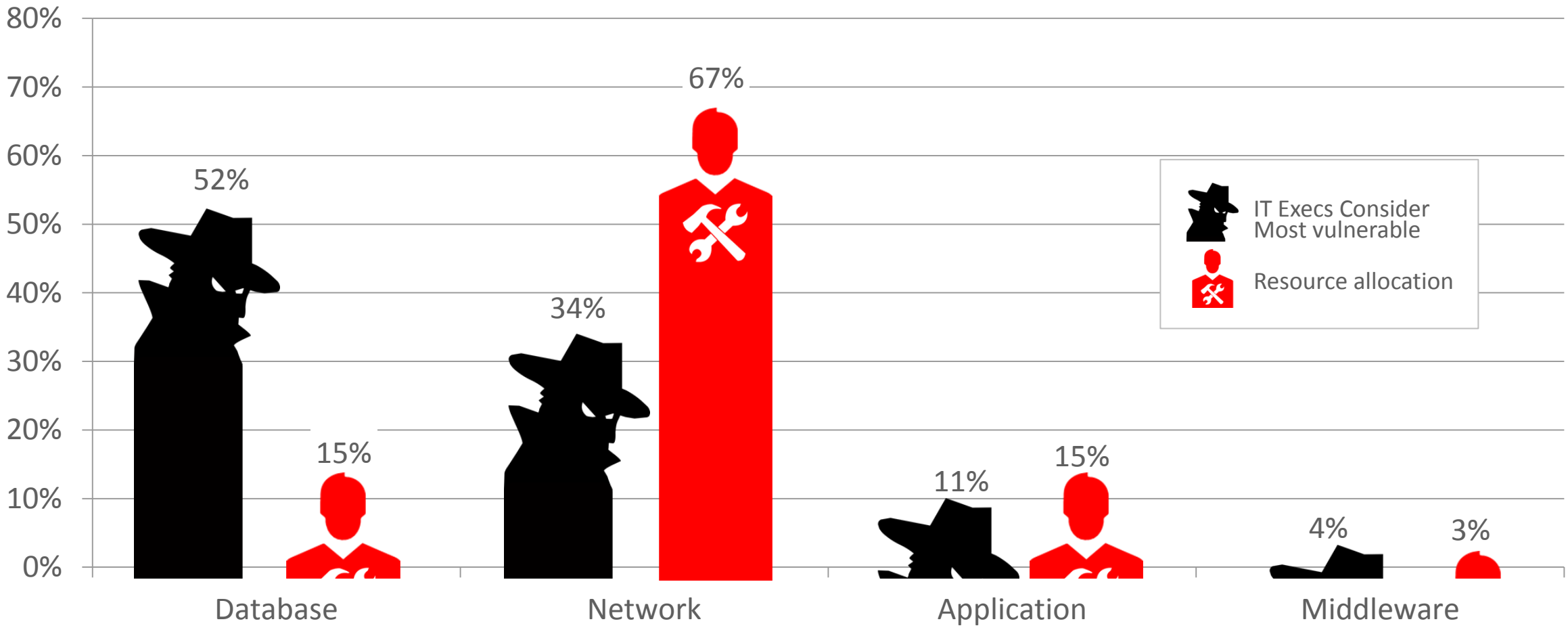
80% các chương trình bảo mật chưa bảo vệ đầy đủ CSDL

Forrester Research

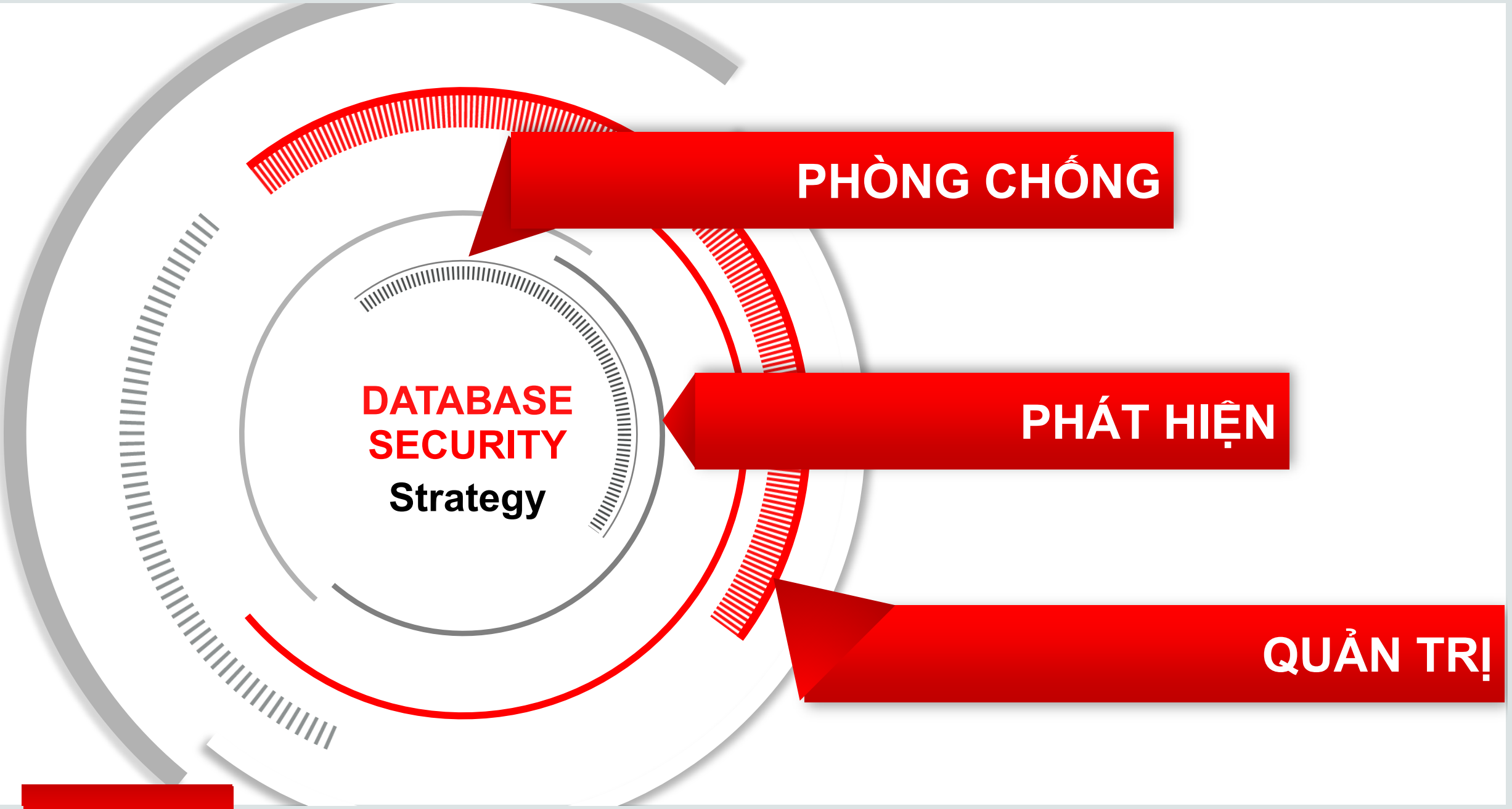
*"**Enterprises are taking on risks that they may not even be aware of.** Especially as more and more attacks against databases exploit legitimate access."*



Mục tiêu tấn công vs Đầu tư an ninh bảo mật



Source: CSO Online



Các giải pháp bảo mật CSDL

PHÒNG CHỐNG PREVENTIVE	GIÁM SÁT DETECTIVE	QUẢN TRỊ ADMINISTRATIVE
Mã hóa & Ẩn Encryption & Redaction	Giám sát hoạt động Activity Monitoring	Quản lý bộ chìa Key & Wallet Management
Che dấu& Thay đổi Masking & Subsetting	Tường lửa CSDL Database Firewall	Khám phá dữ liệu và đặc quyền Privilege & Data Discovery
Quản lý người dùng đặc quyền Privileged User Controls	Kiểm tra & Báo cáo Auditing & Reporting	Quản lý cấu hình Configuration Management

ORACLE

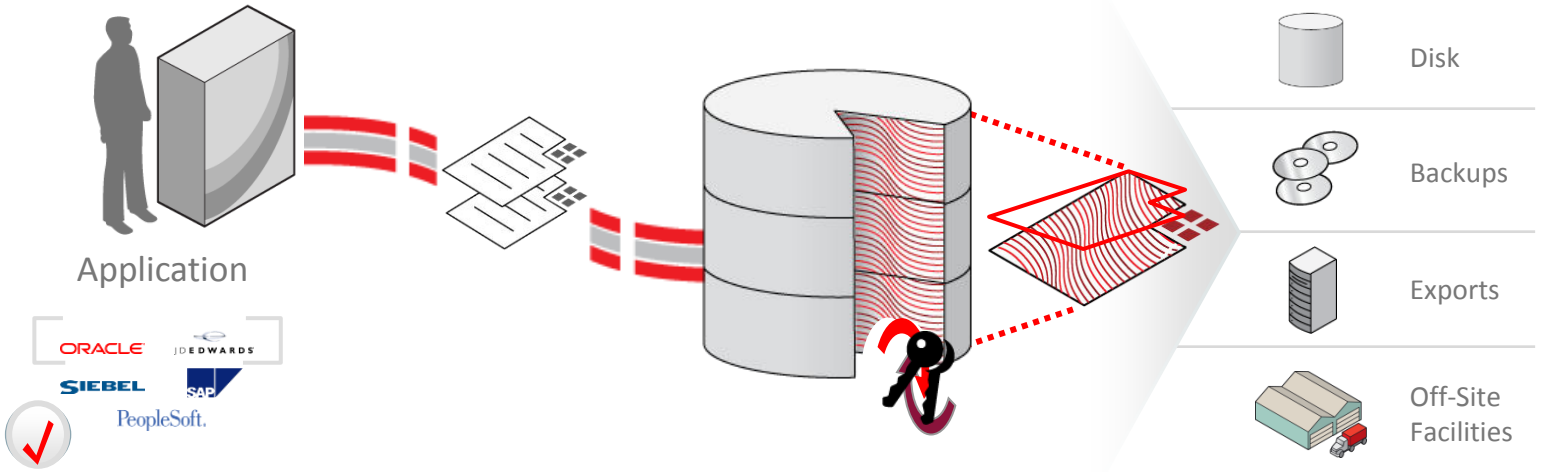
ORACLE

ORACLE

ORACLE

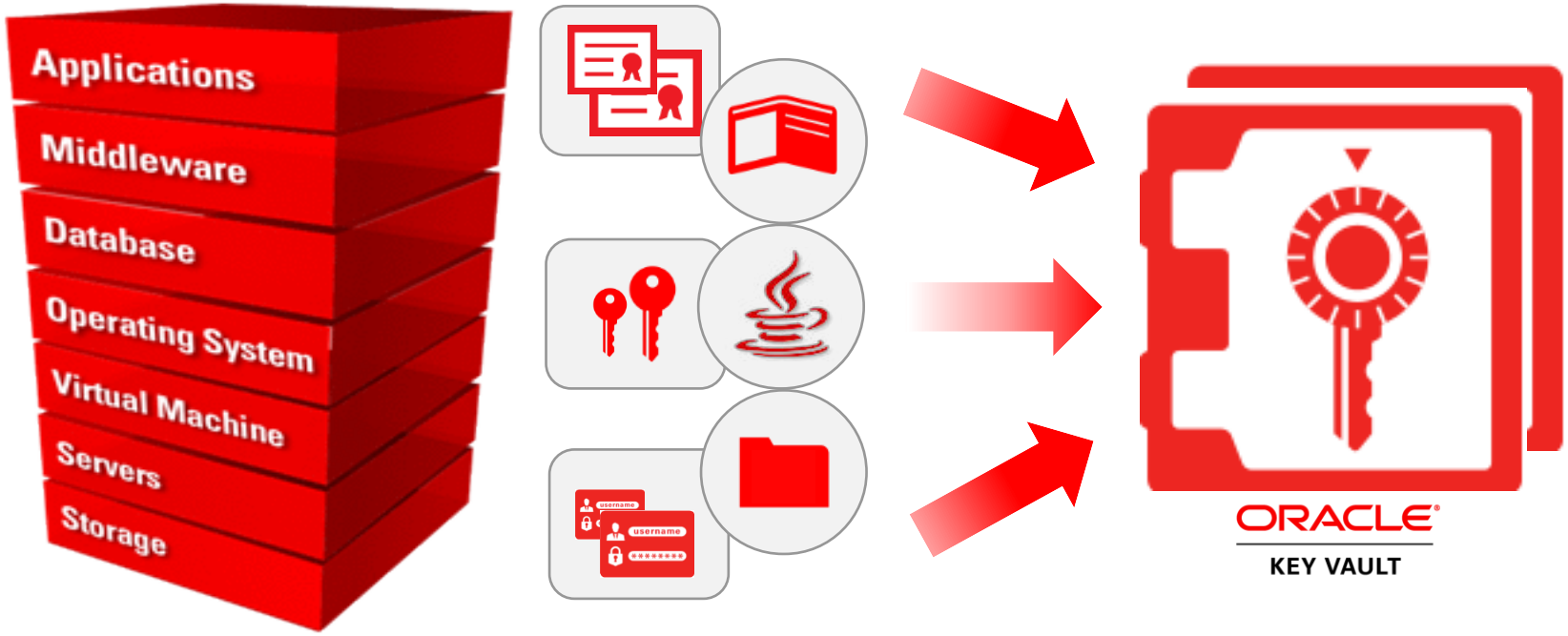
Oracle Advanced Security

Bảo vệ dữ liệu khỏi người sử dụng trái phép



- Mã hóa toàn bộ dữ liệu ứng dụng, ngăn chặn việc truy nhập trực tiếp dữ liệu được lưu trữ trong các tập tin CSDL (datafiles), và các thiết bị khác (disk, backups, exports…)
- Giải pháp mã hóa dữ liệu trong suốt ở phần CSDL, không cần thay đổi ứng dụng.
- Ẩn bớt các thông tin hiển thị tùy biến theo yêu cầu
- Mã hóa được quản lý ở 2 cấp độ đảm bảo tính độc lập cao. Tích hợp với các công nghệ quản lý mã hóa tập trung sử dụng HSM.
- Mã hóa truyền tin trên lớp mạng (TTL, SSL)
- Xác thực mạnh cho người dùng CSDL (PKI, Kerberos)

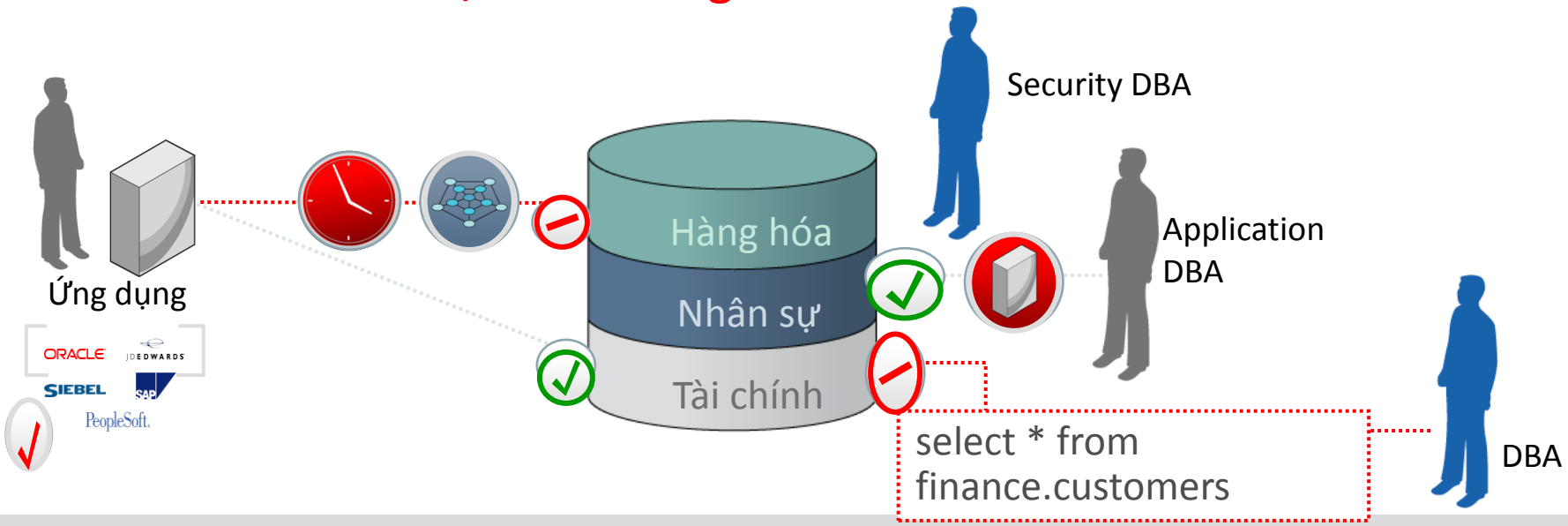
Oracle Key Vault
Quản lý key mã hóa



- Quản lý, chia sẽ key tập trung cho các sản phẩm Oracle và bên thứ 3
- Tối ưu cho các sản phẩm của Oracle bao gồm Database, Middleware, Systems và Advanced Security TDE
- Tự động, an toàn bảo mật và tuân theo các chuẩn về quản lý key (OASIS KMIP)

Oracle Database Vault

Thực thi các chính sách bảo mật bên trong CSDL



- Cung cấp các chính sách tự động và tùy biến bảo vệ các quyền hạn và tác vụ của những người quản trị CSDL (DBA).
- Xác định các quy tắc và yếu tố bảo mật sẽ được áp dụng cho ai, khi nào, ở đâu và bằng phương thức nào.
  - Hạn chế các quyền hạn đặc quyền
  - Ngăn chặn việc truy nhập trái phép và sử dụng dữ liệu không thông qua ứng dụng
- Cũng cố tính an toàn dữ liệu của ứng dụng.

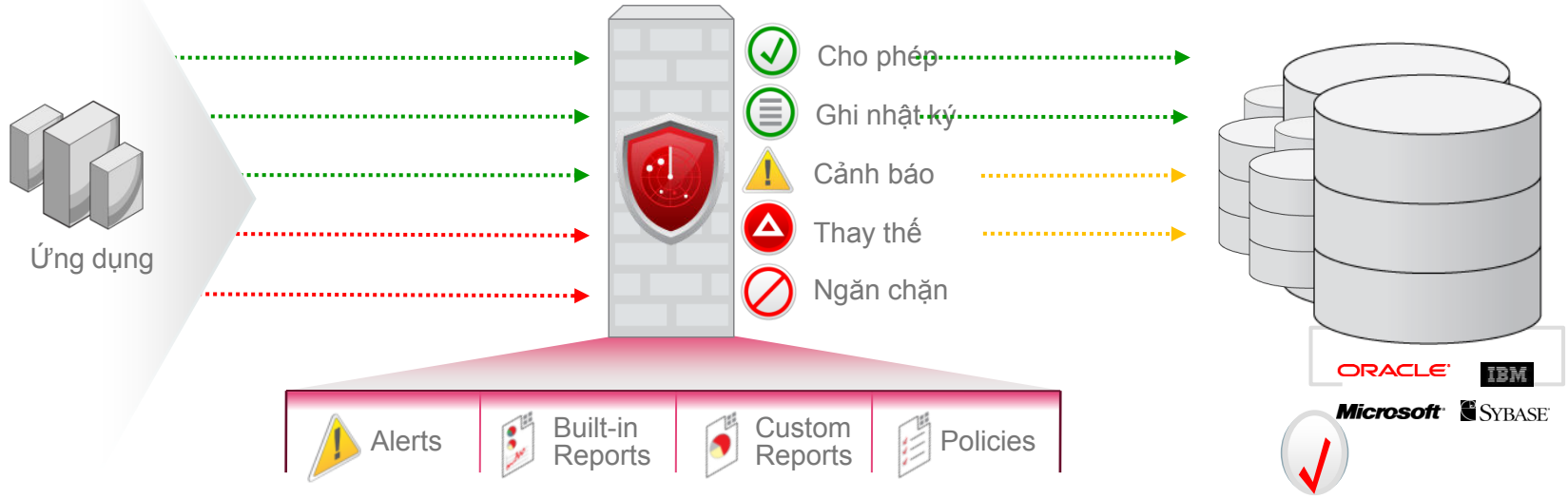
Oracle Data Masking & Subsetting

Che dấu dữ liệu nhạy cảm

- Đảm bảo an toàn , che dấu thông tin nhạy cảm của dữ liệu trong các môi trường Kiểm thử, phát triển v..v
- Ngăn chặn bên phát triển ứng dụng, đối tác xem dữ liệu thực mà vẫn đảm bảo tính đúng đắn của dữ liệu.
- Cung cấp thư viện mẫu và các chính sách đảm bảo việc tự động hóa che dấu dữ liệu nhạy cảm.
- Toàn vẹn tham chiếu tự động để ứng dụng tiếp tục làm việc.

Oracle Database Firewall

Tường lửa CSDL

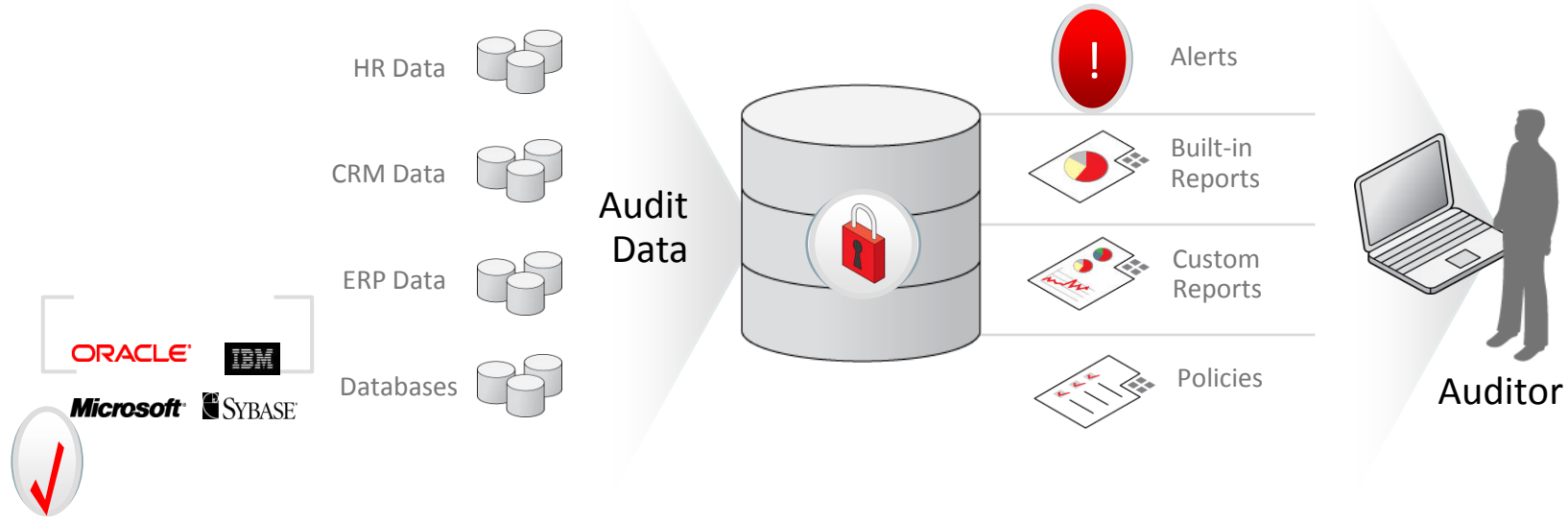


- Giám sát các hoạt động của CSDL để ngăn ngừa việc truy nhập bất hợp pháp, tấn công SQL injection, thay đổi quyền và vai trò, truy cập bất hợp pháp vào các dữ liệu nhạy cảm.
- Tính chính xác cao của cú pháp SQL không chỉ dựa dựa trên việc phân tích ngữ pháp.
- Tính linh hoạt về thực thi của các câu lệnh SQL dựa trên các danh sách (trắng, đen).
- Kiến trúc mở rộng đảm bảo hiệu năng cao với nhiều phương án triển khai.
- Tính tích hợp sẵn và tùy chỉnh của các báo cáo phù hợp với SOX, PCI và các quy định khác.

ORACLE

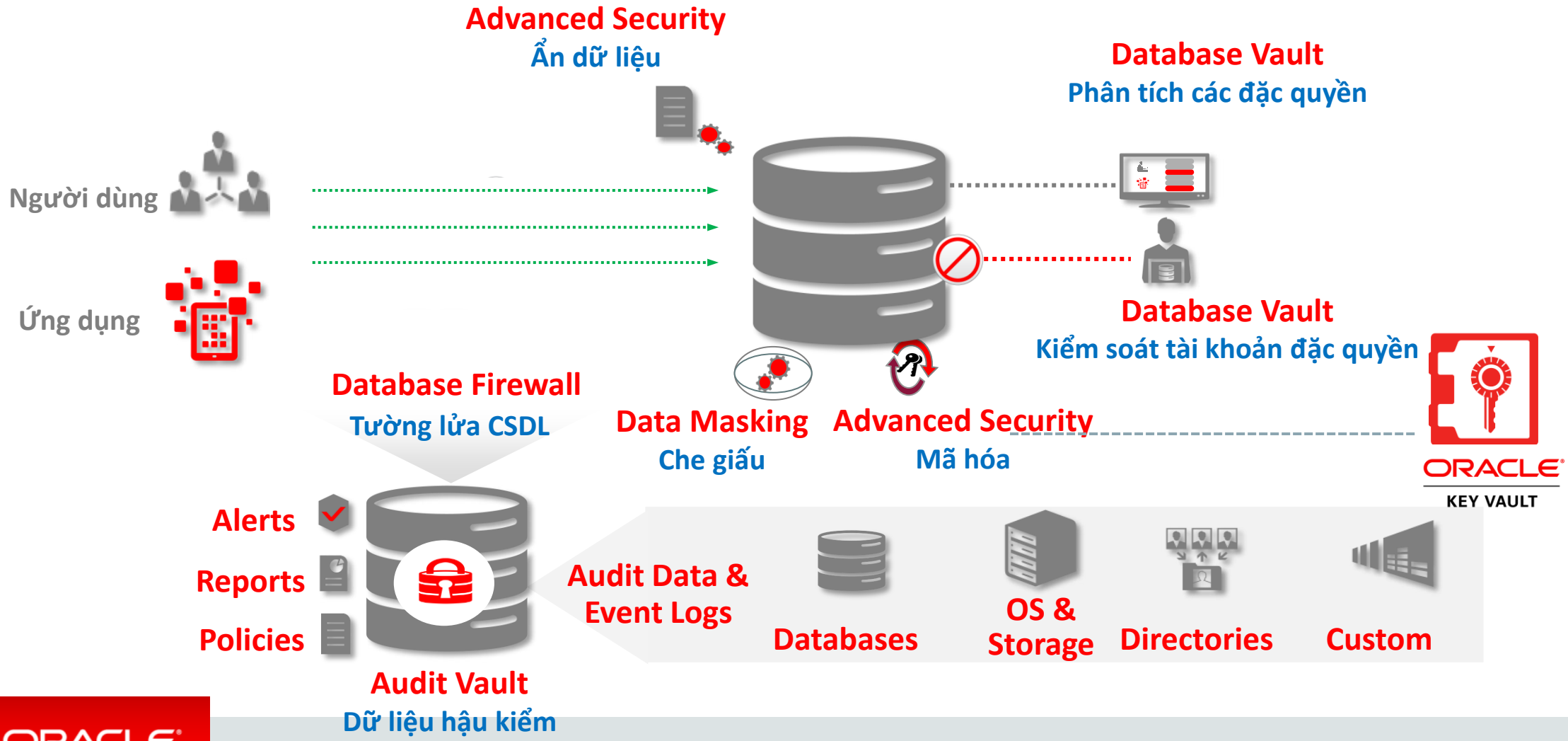
Oracle Audit Vault

Kho lưu trữ thông tin giám sát



- Tập trung kiểm soát các hoạt động CSDL
- Kho lưu trữ dữ liệu tập trung , an toàn.
- Phát hiện và cảnh bảo các hoạt động đáng ngờ, bao gồm cả người sử dụng đặc quyền.
- Các báo cáo tuân thủ sẵn có : PCI, DSS, các báo cáo do người dùng định nghĩa.
  - Vd : ., kiểm toán người sử dụng đặc quyền, quyền lợi, đăng nhập không thành…
- Quy trình khép kín với việc phát hiện, cảnh bảo, đưa ra báo cáo và các chính sách.

Oracle Database Maximum Security Architecture




ORACLE®