




Oracle Audit Vault and Database Firewall

Morana Kobal Butković
Principal Sales Consultant
Oracle Hrvatska

Oracle Security Solutions



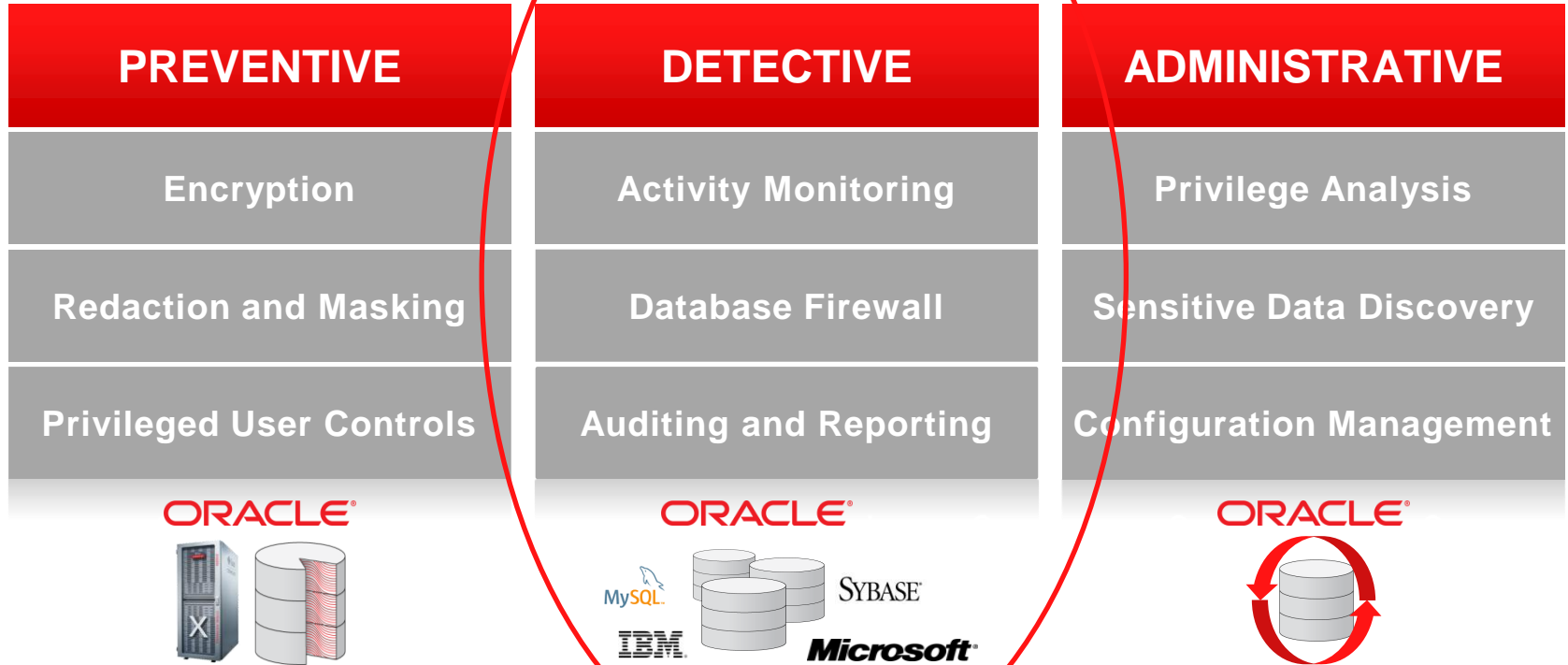


The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract.

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.

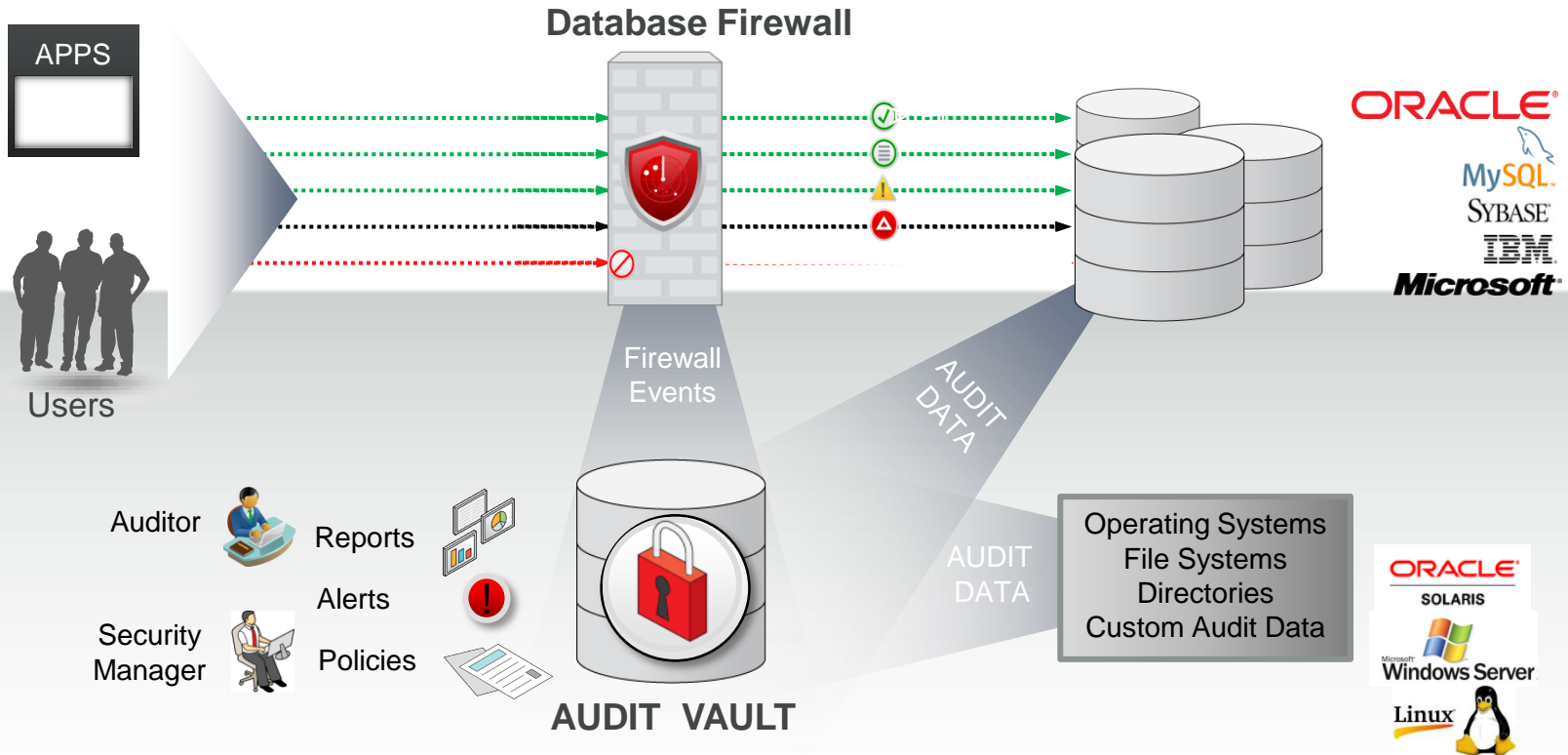
Oracle Database Security Solutions

Defense-in-Depth for Maximum Security

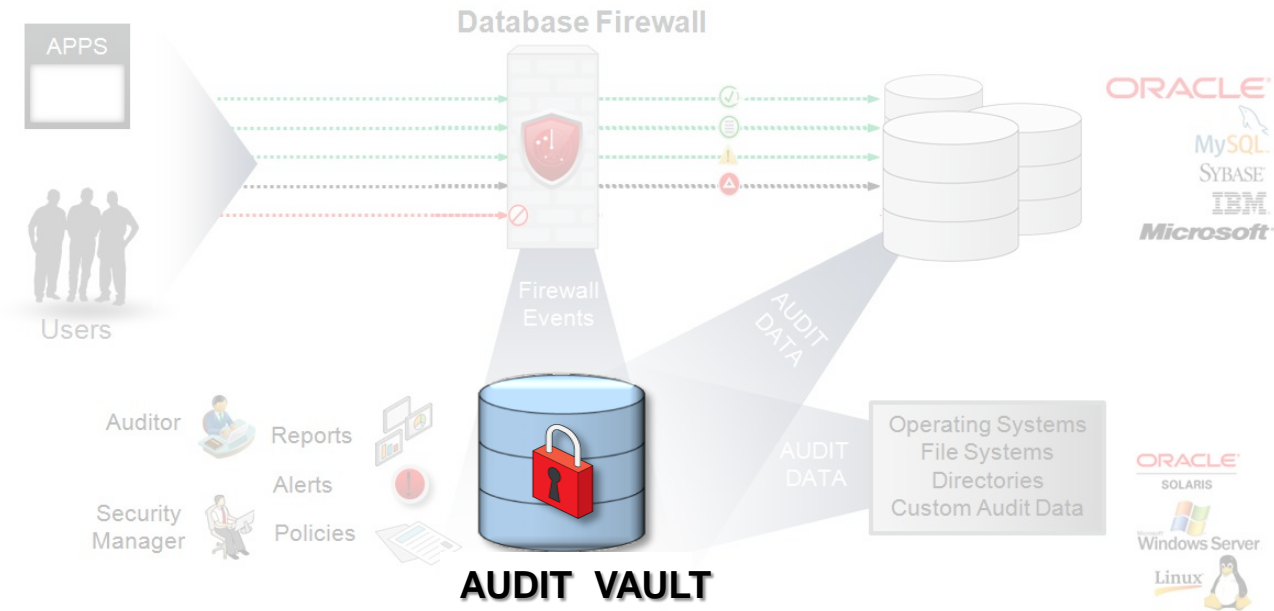


ORACLE®

Oracle Audit Vault and Database Firewall

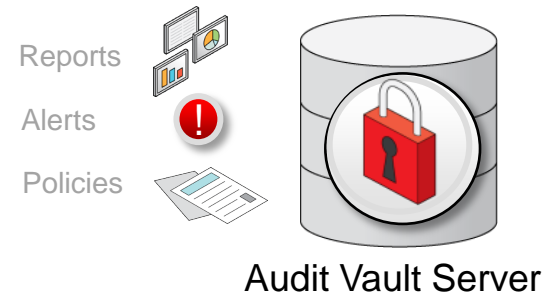


Heterogeneous Enterprise Auditing Collection with Audit Vault Server



Audit Vault Server

Secure Unified Repository for All Activity Data



- Packaged as soft appliance based on OL5.8 x86-64
- Consolidates all audit trails and firewall data into one secure repository
- Contains out-of-the-box reports for SOX, PCI, and other regulations
- Detects and alerts on suspicious activities
- Provides centralized management web-console for administrators and auditors with integrated policy-building UI
- Enables Information Lifecycle Management for event data

Audit Vault Agent

Manages Audit Data Acquisition from Secured Targets

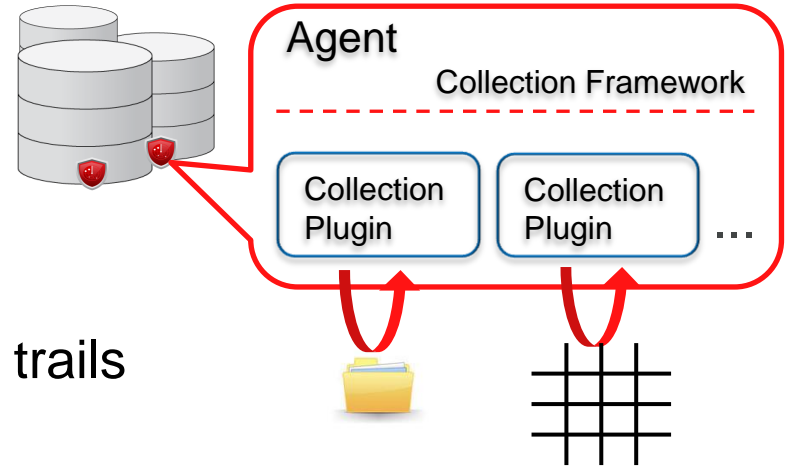


- Securely sends audit event information to Audit Vault Server
- Manages Collection Plugins and Host Monitor
- Installed on target host
- Self-updating (from Audit Vault Server)
- Integrates with native audit trail cleanup tools and procedures
- Supported platforms:
 - Linux, Windows, Solaris (SPARC64, x86-64), AIX Power64, HP-UX

Collection Plugins

Interface to Native Audit Trails

- Work ‘inside’ Audit Vault Agent
- Acquire event data from native audit trails
- Built-in Collection Plugins for:
 - Oracle, DB2 LUW, SQL Server (including 2012R2), Sybase ASE, MySQL
 - Linux (auditd), Solaris, Windows, Active Directory, Oracle ACFS
- ‘No-coding’ templates for custom XML file and DB table audit trails:
 - Configuration XML file maps custom-to-canonical audit elements



Audit Vault Server

Central Repository of Audit Event Data

Secured Targets

Targets

Groups

Access Rights

Monitoring

Audit Trails

Enforcement Points

Register Secured Target

New Secured Target Name *

Linux

Description

OEL 6.0

Secured Target Location *

192.168.56.30

Secured Target Type *

Oracle Database

User Name

Oracle Database
IBM DB2 LUW
Microsoft SQL Server

Password

Sybase ASE
MySQL
Sybase SQL Anywhere
Microsoft Windows
Microsoft Active Directory Server
Oracle Solaris
Oracle ACFS
Linux

Enter Password

Add Secured Target Addresses

Hostname / IP Address

Port Number

Service Name

Audit Vault Server

Central Repository of Audit Event Data

The screenshot shows the Oracle Audit Vault Server web interface. The browser address bar displays the URL: `https://avs/console/f?p=7700:242:839024047332701::NO`. The page title is "ORACLE Audit Vault Server". The navigation menu includes "Home", "Secured Targets", "Firewalls", "Hosts", and "Settings". The "Secured Targets" section is active, showing a search bar and a table of targets. The table has columns for "Name", "Type", and "Description". Four targets are listed, with red and blue boxes highlighting specific rows.

<input type="checkbox"/>	Name ▲	Type	Description
<input type="checkbox"/>	Corporate Human Resource DB	Oracle Database	Oracle DB for Corporate HR @ Tampa
<input type="checkbox"/>	New York Windows 2008 Server	Microsoft Windows	Microsoft Windows Server @ NY
<input type="checkbox"/>	Sales Ordering System DB	Microsoft SQL Server	MSSQL for Sales Ordering @ NY
<input type="checkbox"/>	Tampa Linux System	Linux	Linux System @ Tampa

1 - 4

Audit Vault Server

Central Repository of Audit Event Data

The screenshot shows the Oracle Audit Vault Server web interface. The browser address bar displays the URL: `https://avs/console/f?p=7700:280:839024047332701::NO:::&success_msg=Request to start Audit Trail(s) submitted successfully,%2F86D3AD2837AEE9890590`. The Oracle logo and "Audit Vault Server" are visible in the top left. The user is logged in as "avadmin". The navigation menu includes "Home", "Secured Targets", "Firewalls", "Hosts", and "Settings". The breadcrumb trail is "Home > Secured Targets > Audit Trails".

The "Audit Trails" section contains a table with the following data:

<input type="checkbox"/>	Collection Status	Collection Host	Trail Location	Audit Trail Type	Secured Target Name ▲	Secured Target Type
<input type="checkbox"/>	↓	Tampa.VisionEnterprise.com	SYS.AUD\$	TABLE	Corporate Human Resource DB	Oracle Database
<input type="checkbox"/>	↓	Tampa.VisionEnterprise.com	/u01/app/oracle/admin/db02/adump	DIRECTORY	Corporate Human Resource DB	Oracle Database
<input type="checkbox"/>	↑	NY.VisionEnterprise.com	security	EVENT LOG	New York Windows 2008 Server	Microsoft Windows
<input type="checkbox"/>	↑	NY.VisionEnterprise.com	C:\sqlservertraces*.trc	DIRECTORY	Sales Ordering System DB	Microsoft SQL Server
<input type="checkbox"/>	↓	Tampa.VisionEnterprise.com	/var/log/audit/audit.log	DIRECTORY	Tampa Linux System	Linux

At the bottom right of the table area, the text "1 - 5" is displayed.

Audit Vault Server

Extensive and Customizable Reporting



Dozens of predefined reports



Flexible interactive browsing



Customizable reporting



Scheduling, notification & attestation



Reports Overview

Audit Vault Server

Entitlement Report

ORACLE Audit Vault Server

Home Secured Targets Reports Policy Settings

Home > Reports > User Privileges by Secured Target - Changes

Built-in Reports

Audit Reports

Compliance Reports

Specialized Reports

Custom Reports

Uploaded Reports

Interactive Reports

Report Workflow

Report Schedules

Generated Reports

Quick Links

Audit Trails

Enforcement Points

User Privileges by Secured Target - Changes

Secured Target

Corporate Human Resource DB

Snapshot

9/12/2013 8:19:48 AM

compare

9/12/2013 8:26:04 AM



Go

Actions

Change Category = 'NEW'

Secured Target	Snapshot	Change Category	User/Role ▲	Type	Privilege	Role	Owner	Target
Corporate Human Resource DB	9/12/2013 8:26:04 AM	NEW	DBA_FRANK	USER	UNLIMITED TABLESPACE			
Corporate Human Resource DB	9/12/2013 8:26:04 AM	NEW	DBA_FRANK	USER		DBA		
Corporate Human Resource DB	9/12/2013 8:26:04 AM	NEW	HELEN	USER	UNLIMITED TABLESPACE			
Corporate Human Resource DB	9/12/2013 8:26:04 AM	NEW	HELEN	USER		DBA		

Audit Vault Server

Powerful Alerting

ORACLE Audit Vault Server avauditor | Help | Log

Home | Secured Targets | Reports | **Policy** | Settings

Home > Policy > Alerts > Modify Alert

Policy

Audit Settings

Firewall Policy

Alerts

Alerts

Quick Links

Audit Trails

Enforcement Points

Modify Alert

Name *

Secured Target Type

Severity *

Threshold (times) *

Duration (min) *

Group By (Field)

Status *

Description

Alert me when non-HR app is accessing HR.JOBS table

51 of 255

Condition *

```
:TARGET_OBJECT like '%JOBS%' and :USER_NAME NOT LIKE '%HR%'
```

Condition - Available Fields

- ACTION_TAKEN
- AV_TIME
- CLIENT_HOST_NAME
- CLIENT_IP
- CLUSTER_TYPE
- COMMAND_CLASS
- ERROR_CODE
- ERROR_MESSAGE
- EVENT_NAME
- EVENT_STATUS
- EVENT_TIME
- NETWORK_CONNECTION
- OSUSER_NAME
- SECURED_TARGET_NAME
- TARGET_OBJECT
- TARGET_OWNER
- TARGET_TYPE
- THREAT_SEVERITY
- USER_NAME



Alert Demo

Audit Vault Server

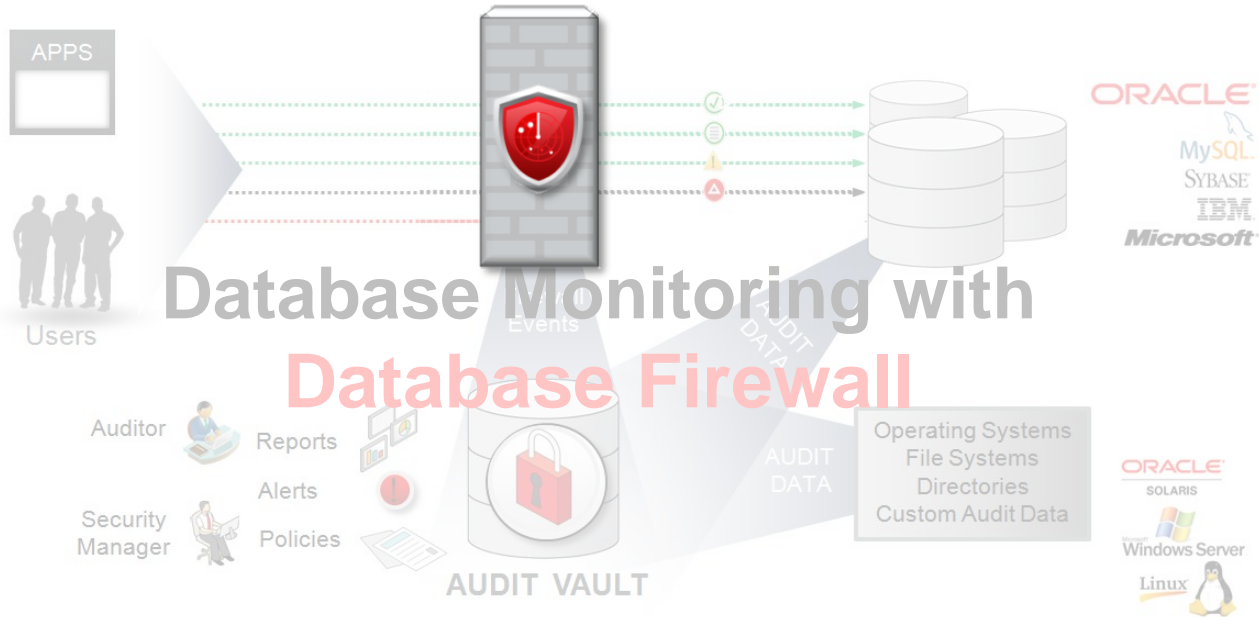
Enterprise Scale Deployment

- Built on Proven Oracle Technology
- Secure
 - Fine-grained security groups
 - Strict separation of Duty
- Life Cycle Management for Audit Event Data
- 3rd Party Integration & Custom Collection plug-in

Audit Vault Server Summary

Heterogeneous Enterprise Audit Collection

- Central Repository of Audit Event Data
- Extensive and Customizable Reporting
- Powerful Alerting
- Enterprise Scale Deployment



SQL Injection

#1 Risks on OWASP Most Critical Application Security Risks - 2013

Threat Agent

- Anyone who can send untrusted data to the database including external users, internal users, and administrators

Attack Vector

- EASY
- Attacker sends text based attacks that exploit the unclesansed syntax

Impact

- SEVERE
- Injection can result in data loss or corruption, lack of accountability or complete host takeover

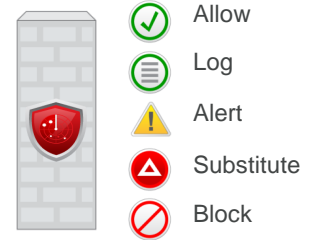
Database Firewall

First Line of Defence

- Real-time Database Activity Monitoring on the Network
- Capture Events for Analysis and Compliance Reporting
- Flexible Deployment Models
- SQL Injections Protection with Positive Policy Model
- Constraining Activities with Negative Policy Model

Database Firewall

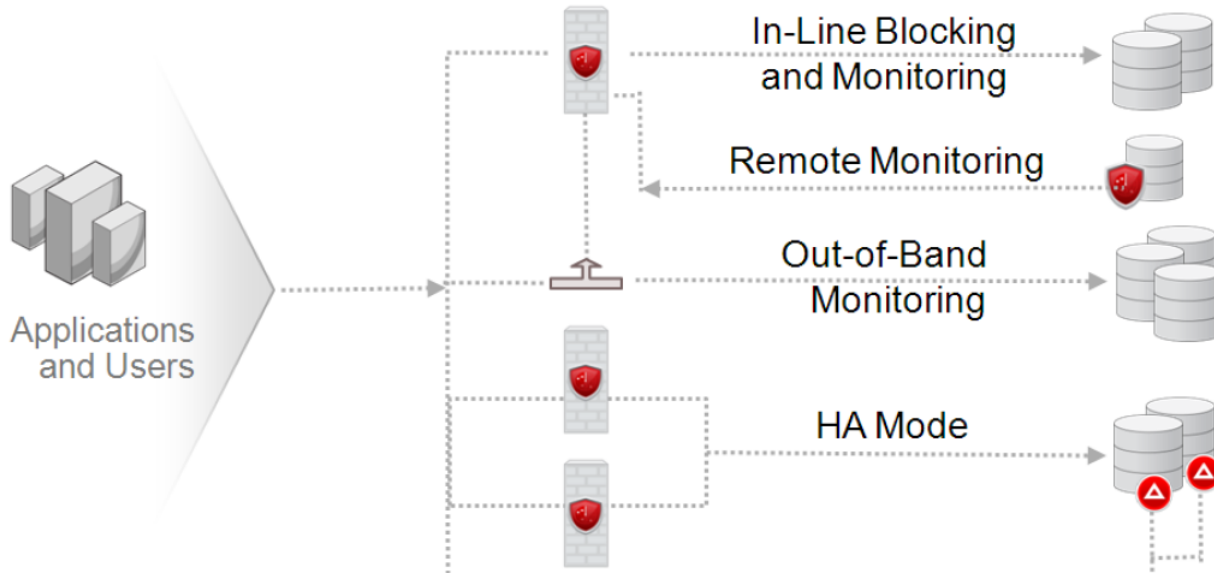
Pro-actively Monitors Database Activity on the Network



- Packaged as soft appliance based on OL5.8 x86-64
- Acquires database activity data from network
- Performs accurate grammatical analysis of database requests
- Supports white-list, black-list and exception-list based policies
- Integrates into customer networking infrastructure
 - Inline, out-of-band, proxy, high availability
- Protects multiple heterogeneous databases simultaneously
- Works with Oracle Database native network encryption

Database Firewall

Flexible Deployment Models



ORACLE®

MySQL®

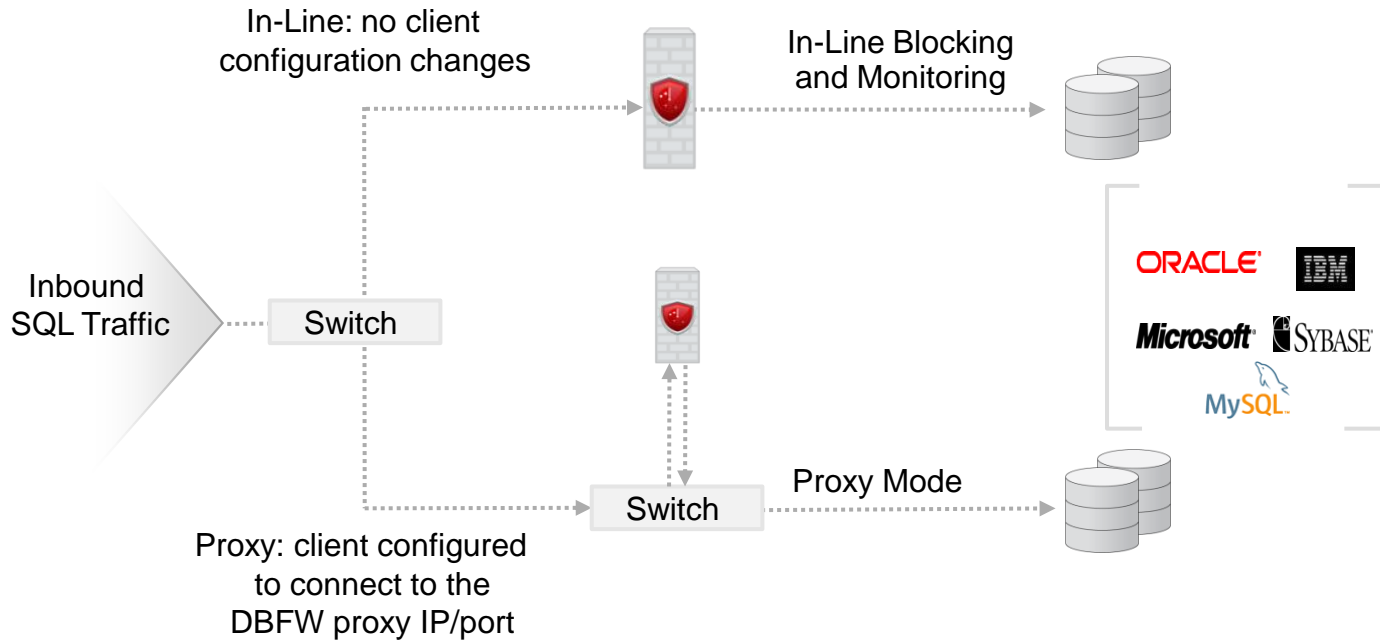
SYBASE

IBM

Microsoft®

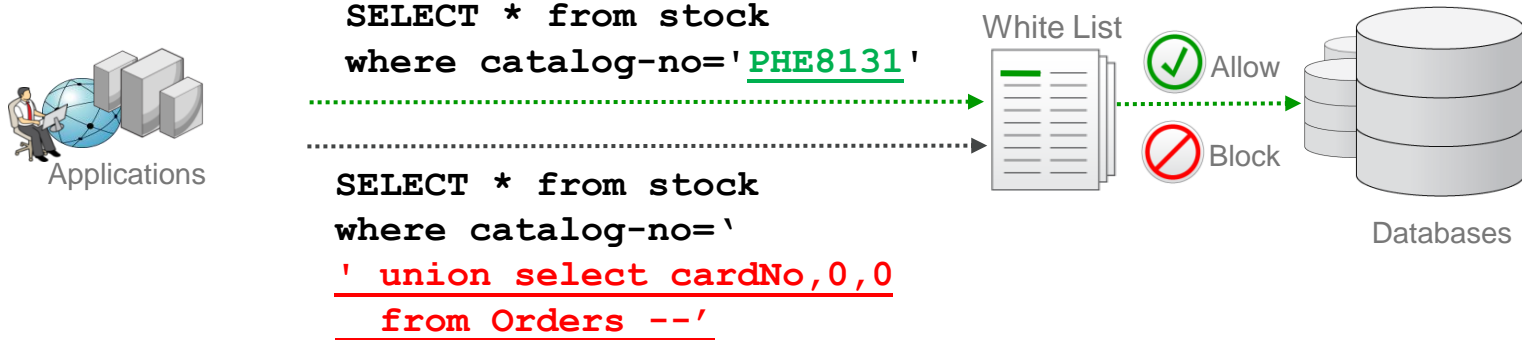
Database Firewall Network Deployment

In Proxy Mode



Database Firewall

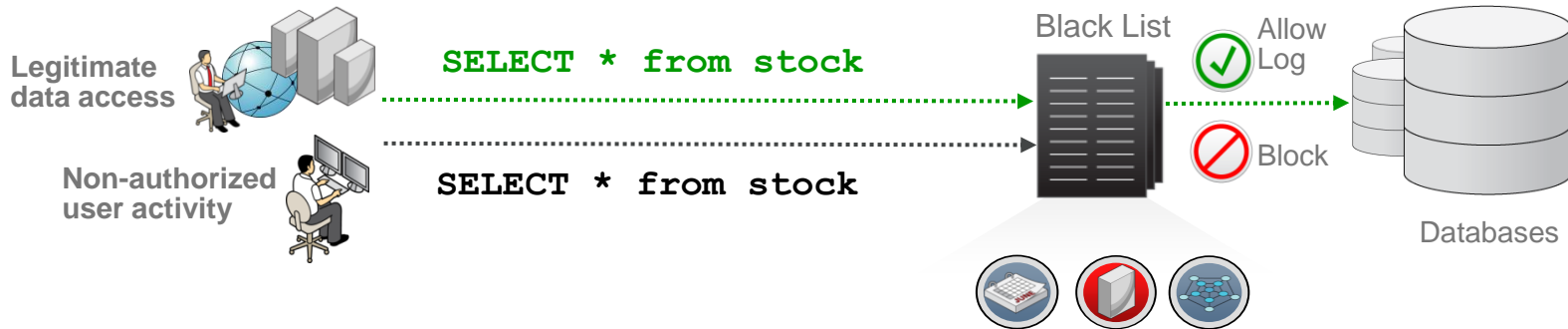
SQL Injection Protection with **Positive** Policing Model



- Define “allowed” behavior for any user or application
- Automated whitelist generation for any application
- Out-of-policy Database network interactions instantly blocked

Database Firewall

Constraining Activity with **Negative** Policing Model



- Stop specific “non-authorized” SQL interactions, user or schema access
- Blacklisting can be done on IP address, application, DB user, OS user
- Provide flexibility to authorized users while still monitoring activity



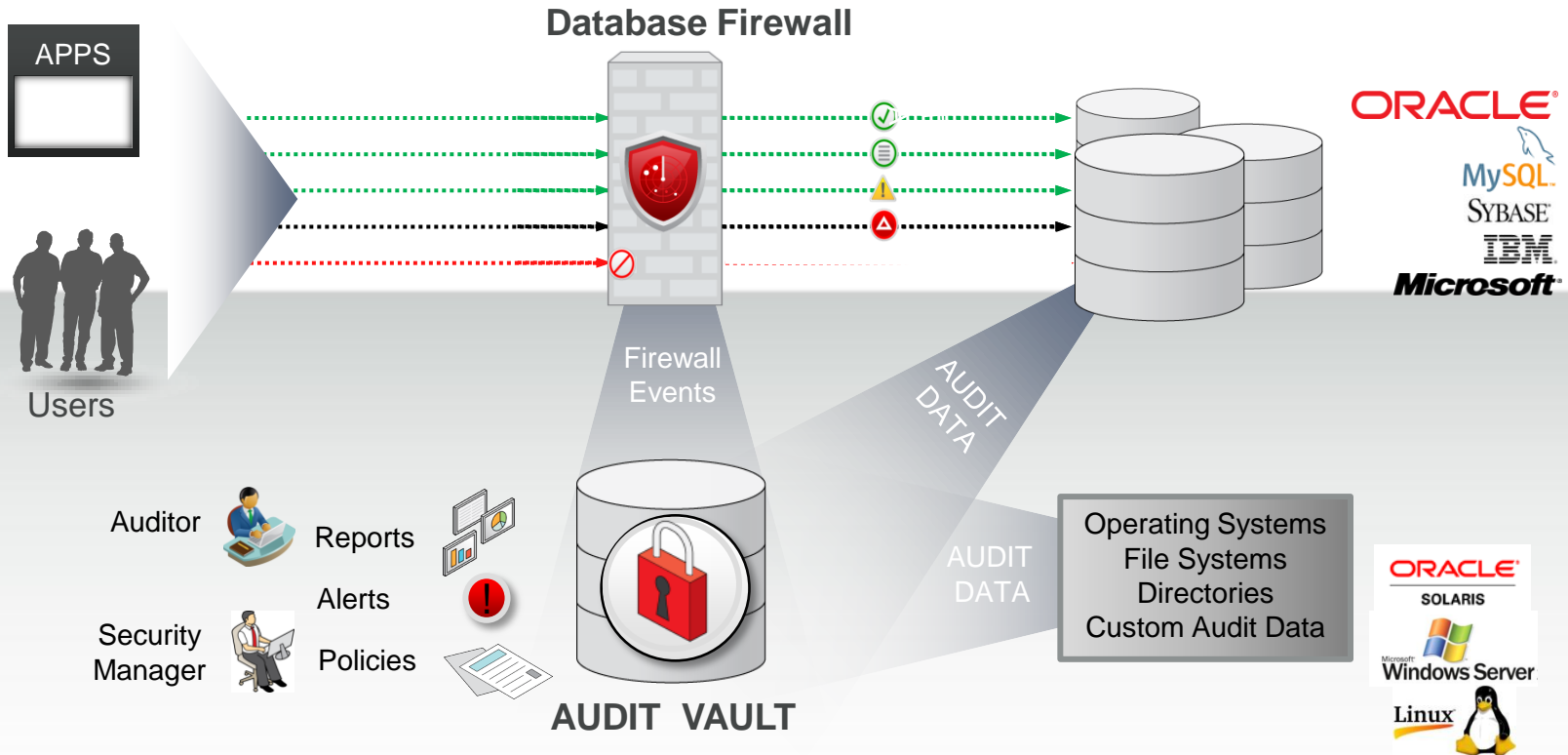
SQL Injection Demo

Other Key AVDF Features

Easy Installation & Administration

- Distributed as Soft Appliance
- One Web UI Management Console for Admin and Auditor
- Fine-Grained Security Groups
- Strict Separation of Duty
- Command Line Client for Automation and Scripting

Oracle Audit Vault and Database Firewall



ORACLE®



Complimentary eBook Register Now

www.mhprofessional.com/dbsec

Use Code: db12c

Securing Oracle Database 12c: A Technical Primer

ORACLE 12c
DATABASE

Michelle Malcher
Paul Needham
Scott Rotondo
James Spooner

Oracle
Press



Hardware and Software

ORACLE®

Engineered to Work Together