

# Detecting and Blocking Attacks with Oracle Audit Vault and Database Firewall

ORACLE  
OPEN  
WORLD

Ram Subramanian - Director, IT, ERP & Database Services, Symantec

Rohit Muttepawar - IT Architect, ERP & Database Services, Symantec

Rajesh Tammana – Senior Director, AVDF Development

Russ Lowenthal - Director, Oracle 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, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.



# Symantec | At a Glance



**175M**

endpoints under protection



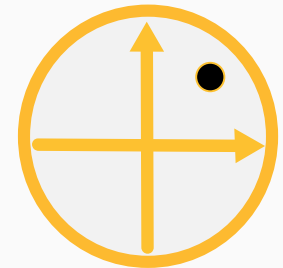
**\$5B**

FY18 revenue



**2100+**

patents



**Leader in 5 Gartner MQs**

EPP, SWG, DLP, MSS, and CASB



**350,000+**

customers worldwide



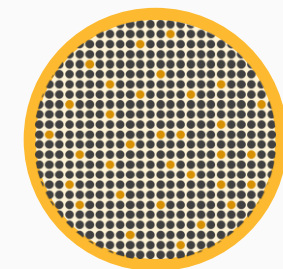
**~3,500+**

company wide R&D



**9 SOC**

threat response centers



**9 Trillion**

telemetry points



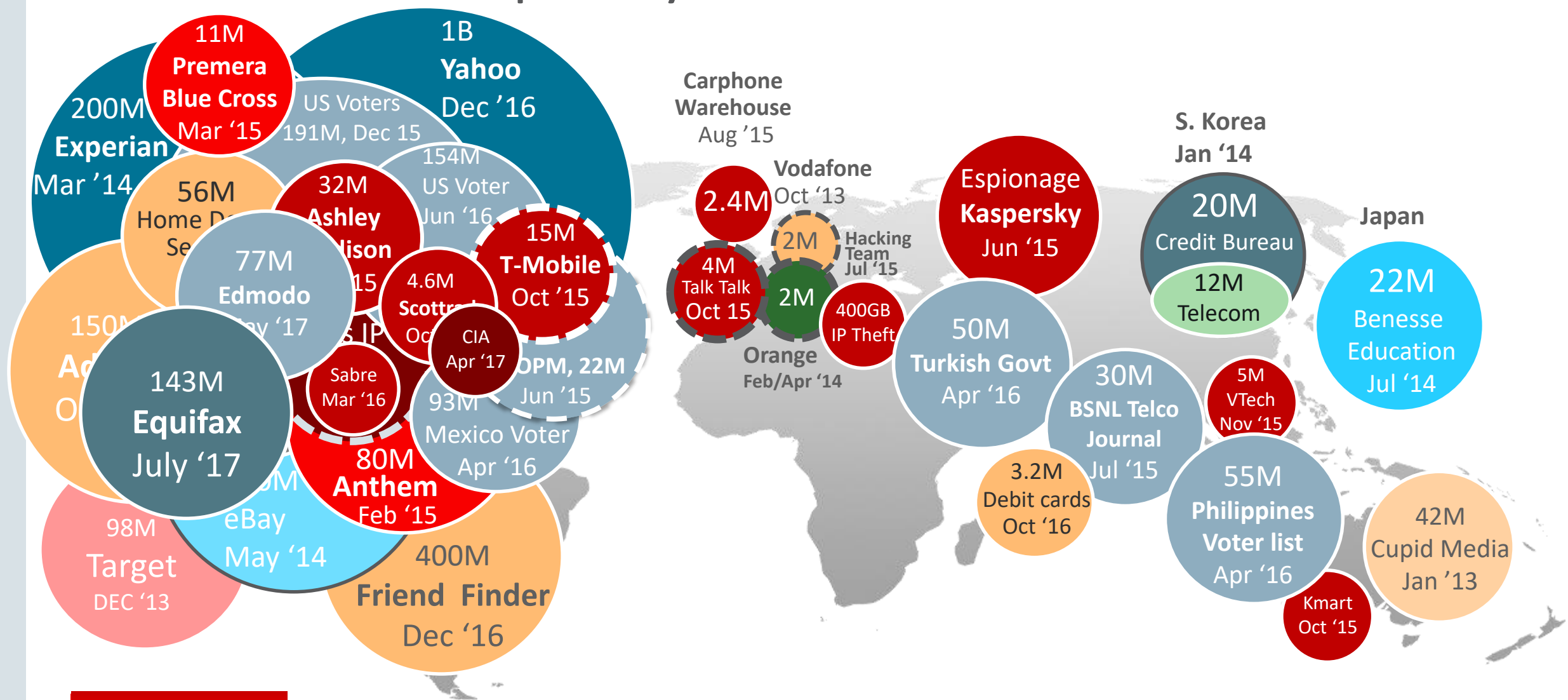
# About Oracle Database Security

- Database customers in 175 countries
  - in-cloud and on-premises
  - Very small to extremely large customers in every industry
- Much of the worlds' relational data resides in an Oracle Database
- Providing database-security products for more than 20 years
- First to market with Database Security Innovation
  - Transparent Data Encryption
  - Database Vault
  - Virtual Private Database
  - Data Redaction
  - Label Security
  - Database Firewall
  - Real Application Security





# Data Thieves Frequently Succeed...

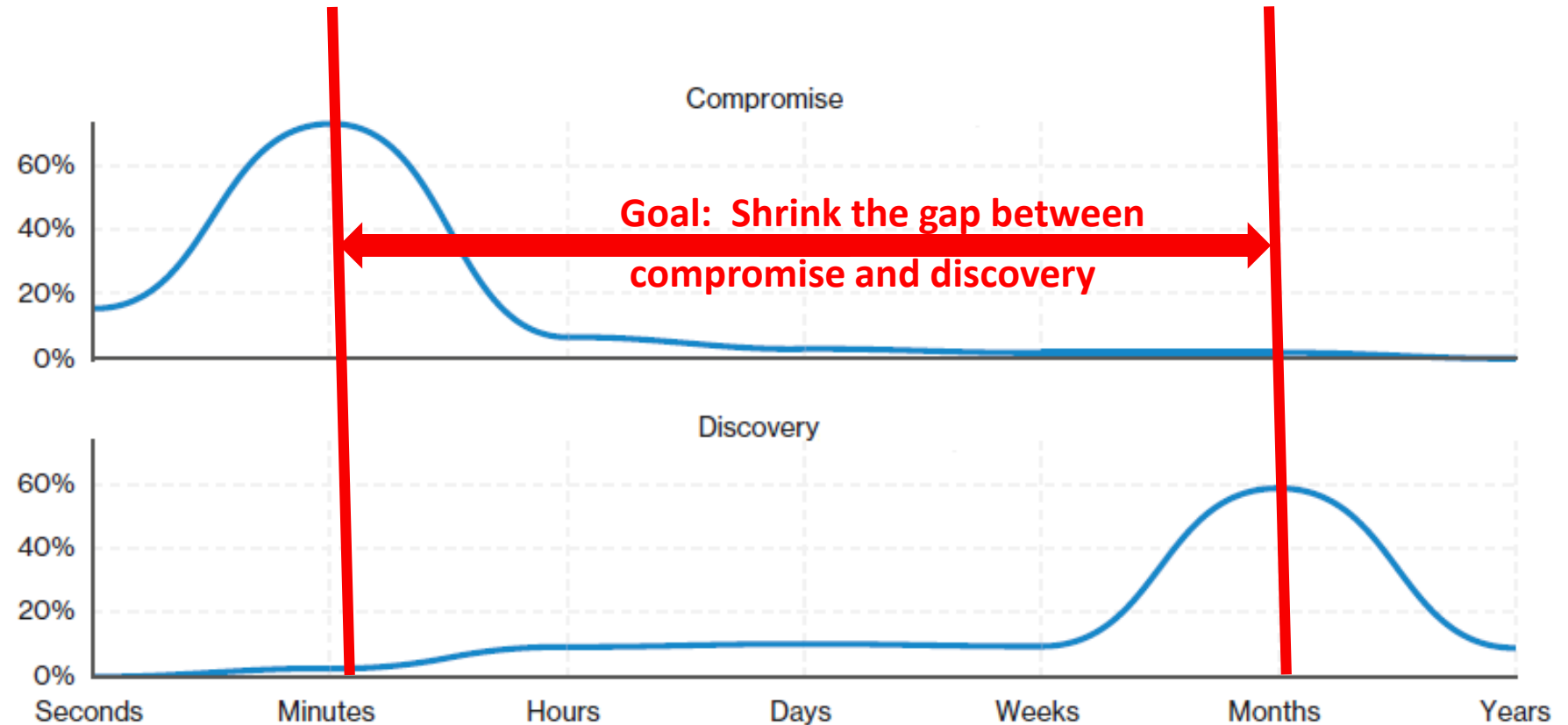




# Database Activity Monitoring is Important

“Improvements in ... time to discovery can result in the prevention of a high-impact confirmed data breach.”

— *Verizon Data Breach Investigation Report, 2018*



Breaches continue to succeed in minutes,  
but not be discovered for months!



# About Oracle Audit Vault and Database Firewall



## Monitor Access to Data

### Database Activity Monitoring

- Centralized management of audit data for Oracle and non-Oracle Databases
- Database Anomaly Detection – if it's new, it should be investigated
- Support forensic investigation
- Detect and block SQL Injection



# Collect, Analyze, and Report on Database Activity



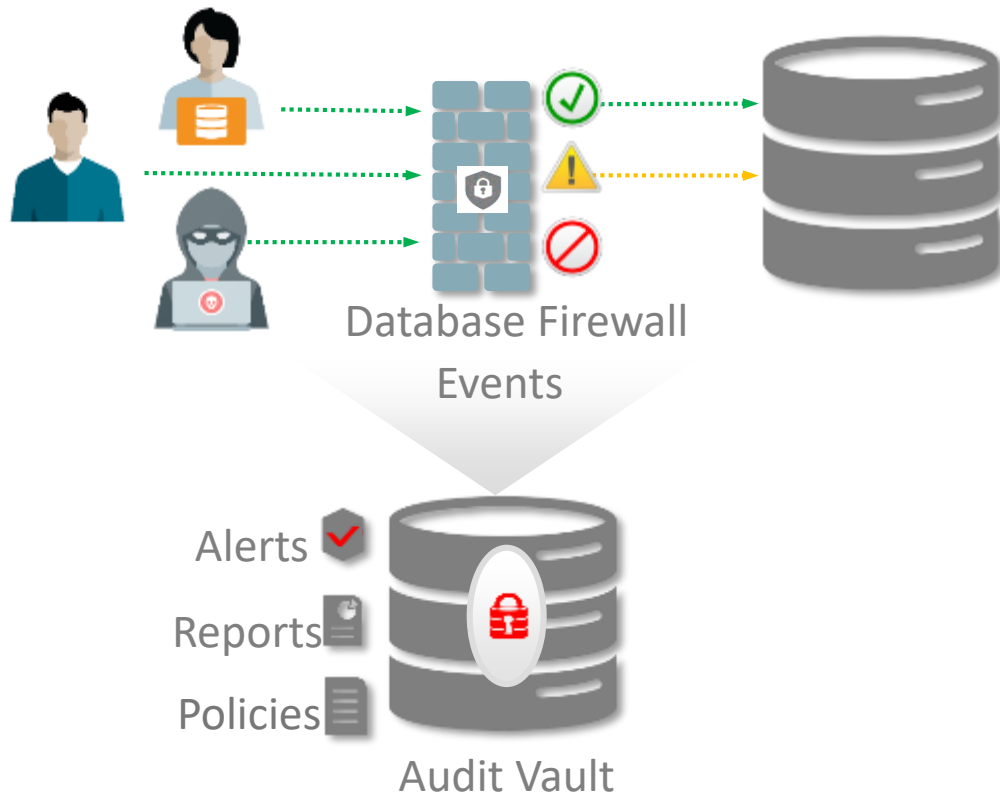
## Audit Vault and Database Firewall

### Database Auditing

- Dynamic query and filter-by-example makes investigations easy to conduct
- Collect and securely store native audit records from databases, operating systems, and directories with out-of-box collectors
  - Easy-to-use custom collectors for any audit source using XML or relational database
  - Flexible Java SDK for collectors from virtually ANY audit source
- Flexible, easily customizable reporting based on Oracle BI Publisher
  - Open, documented schema



# Detect and Prevent Unusual Database Activity



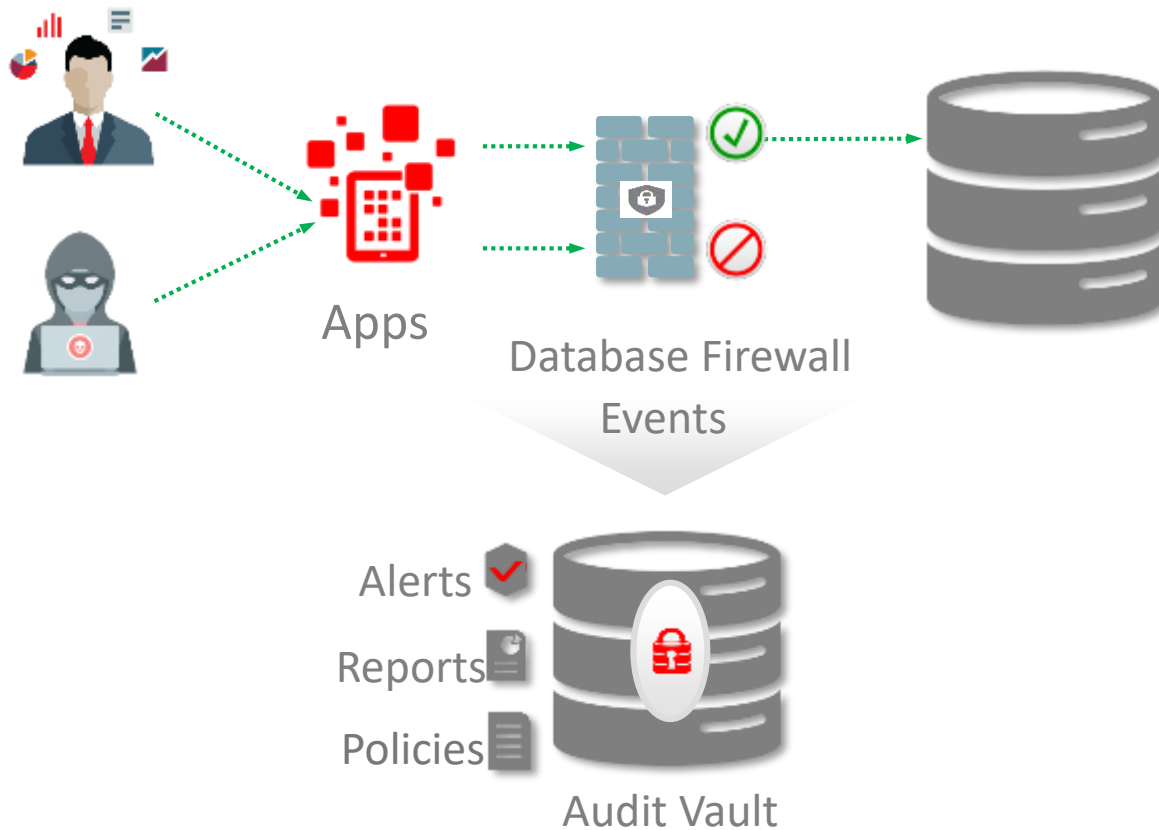
## Audit Vault and Database Firewall

### Anomaly Detection

- Monitor ALL database activity with network-based monitoring
  - Zero performance impact on the database
  - Support Oracle Native Network Encryption
- Profile typical database activity and quickly identify changes in access patterns
  - New tools being used
  - Unusual IP addresses
  - New laptops/workstations connecting to the database
- Stop anomalous activity from ever reaching the database



# Identify and Block SQL Injection Attempts



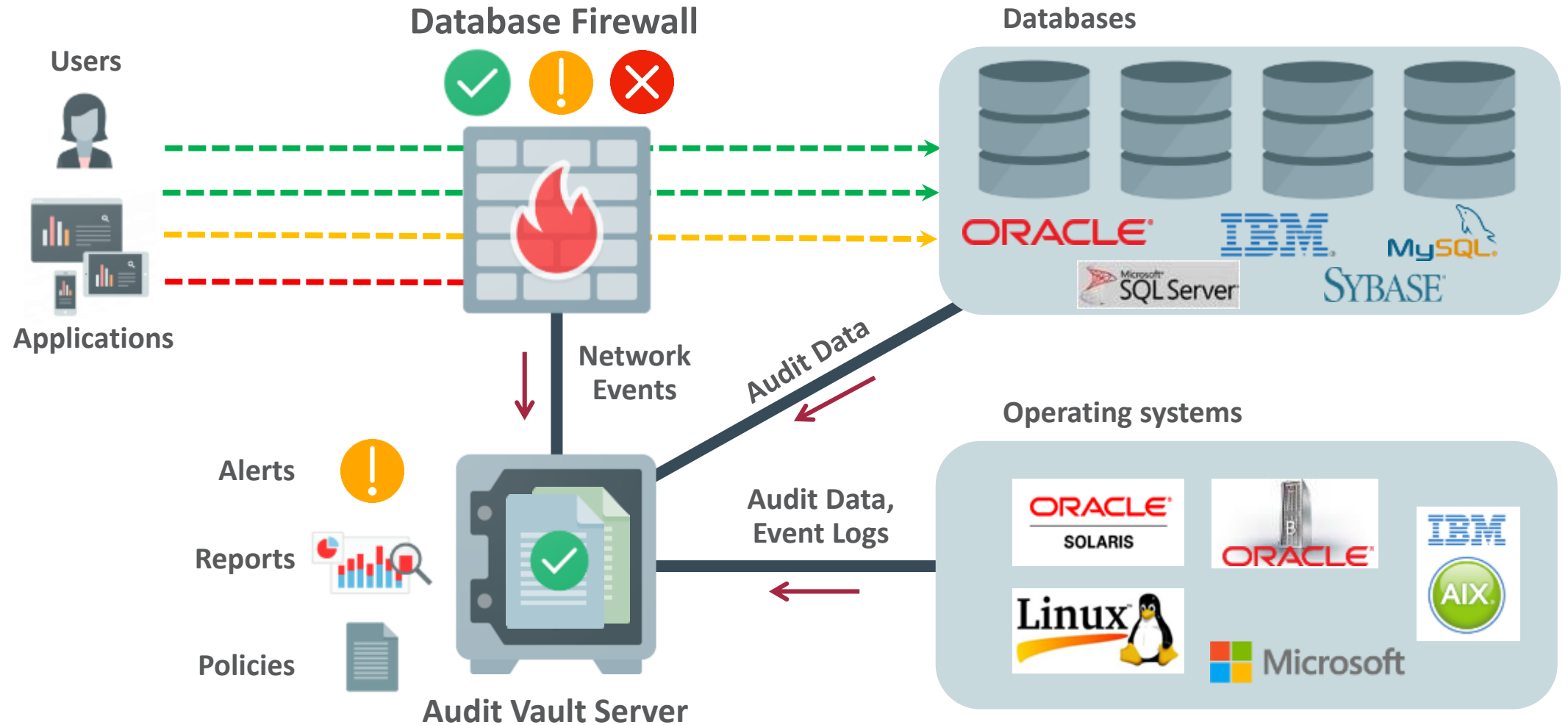
## Audit Vault and Database Firewall

### SQL Injection Prevention and Detection

- Detection and blocking based on learning normal application SQL patterns. Does not use easy-to-defeat signature files or regular expressions
- Zero False Positives
- Detect or block never-before-seen SQL from ever reaching the database
- Available blocking actions include:
  - Substitute another statement
  - Terminate the connection



# Oracle Audit Vault and Database Firewall (AVDF)



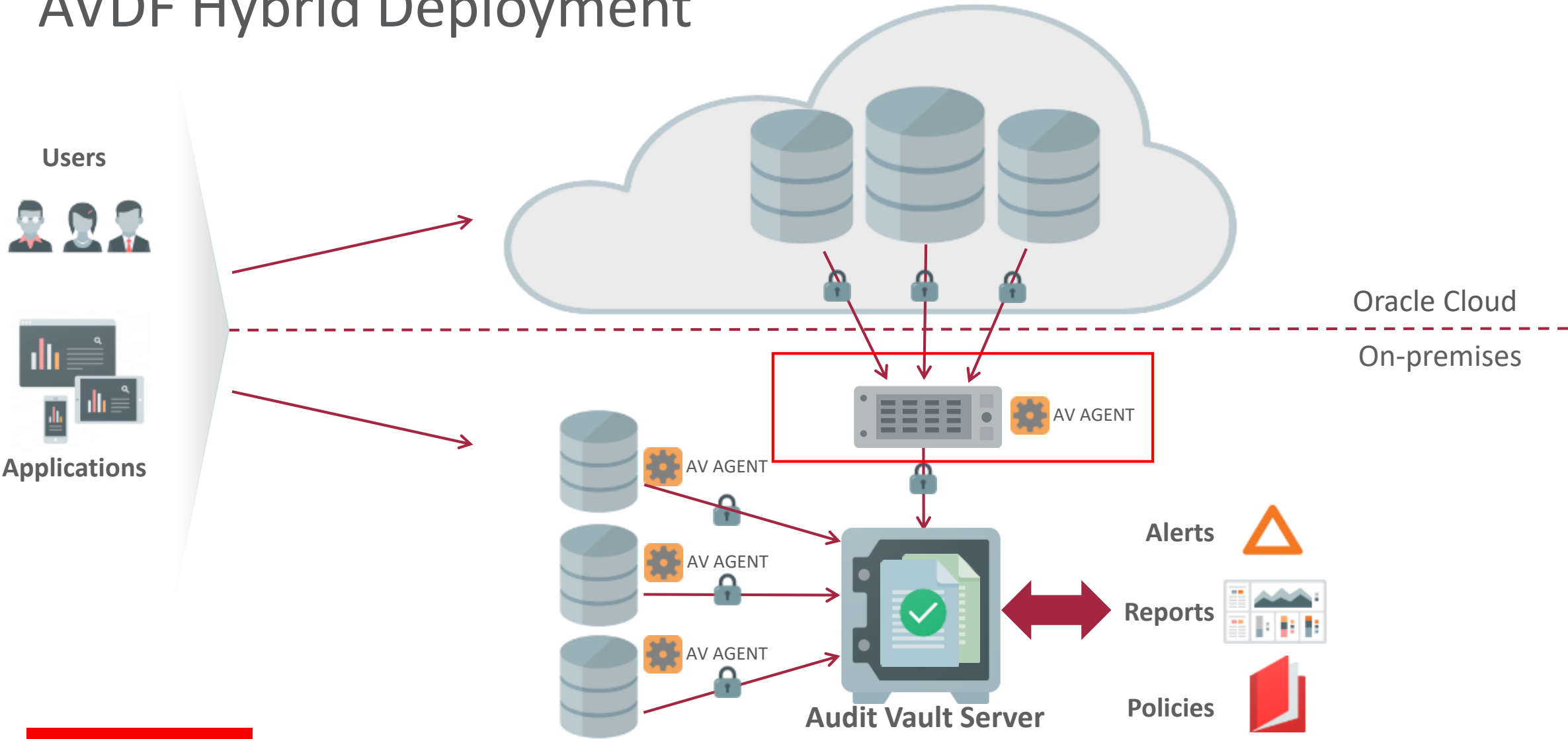


# Database Activity Auditing and Monitoring

	<b>Auditing (Audit Vault Agents)</b>	<b>Monitoring (Database Firewalls)</b>
Information	Who, what, where, when Before/After values Full execution and application context	Who, what, where, when
Pathways	All: stored procedures, direct connections, scheduled jobs, operational activities	Network
Impact on database	Requires native database auditing, minimal performance impact	Completely independent, negligible performance impact
Purpose	Ensure regulatory compliance, provide guaranteed audit trail to enable control	Prevent SQL-injections and other unauthorized activity, enforce corporate data security policy

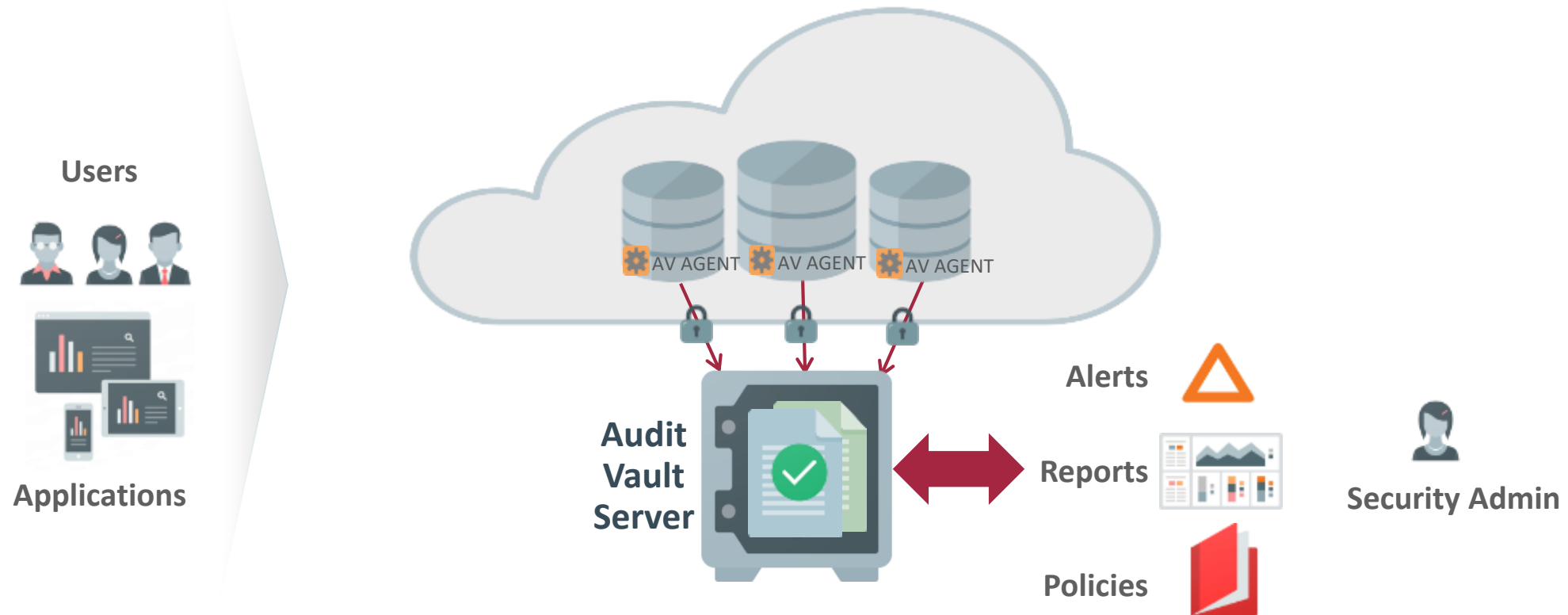


# AVDF Hybrid Deployment



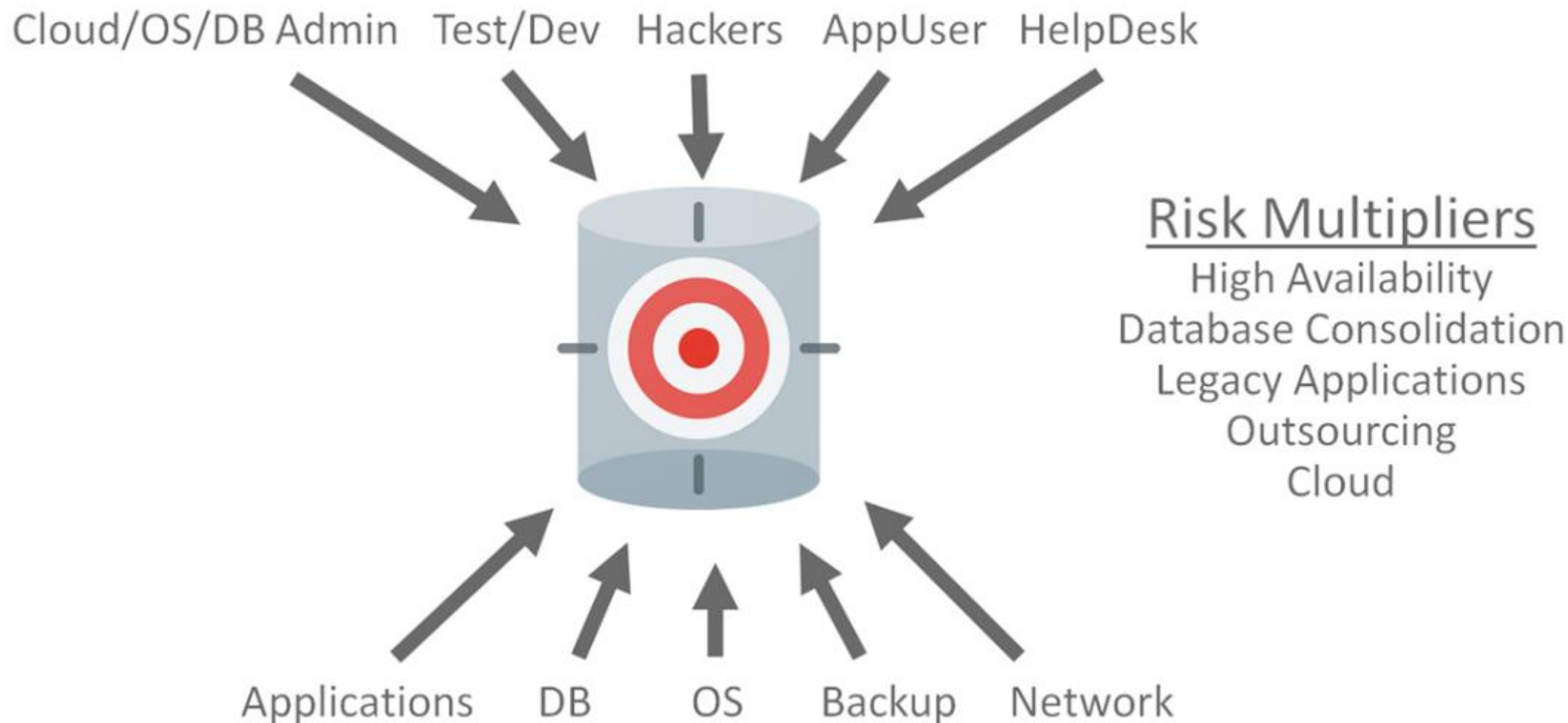


# AVDF on Oracle Cloud Infrastructure



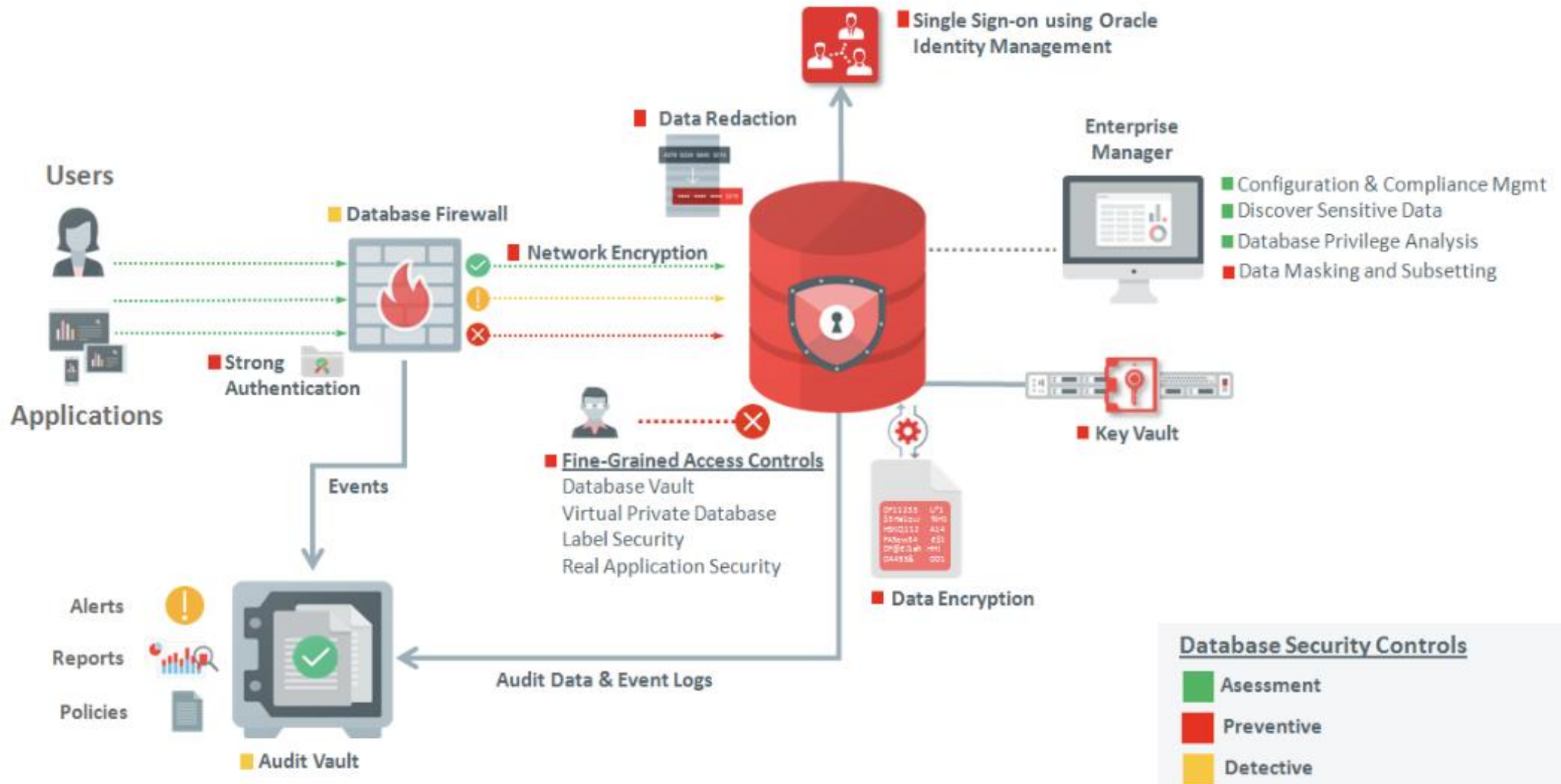


# Threats for Databases



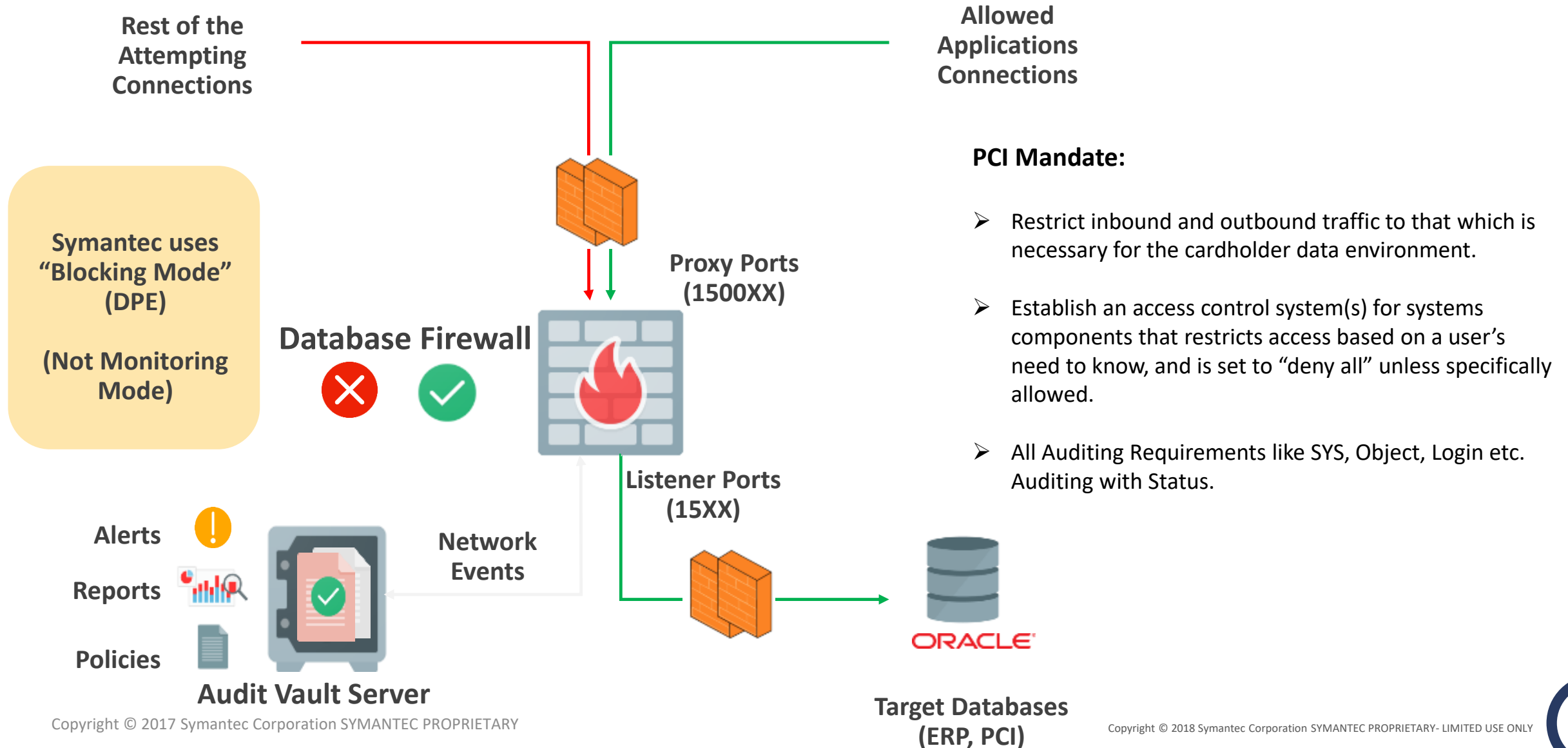


# Oracle's Maximum Security Architecture





# Recap of AVDF Session 2017 – Database Firewall





# Audit Vault & Database Firewall – Who owns What?

## ❑ Industry Dilemmas

- AVDF is an Appliance provided by Oracle which is helpful for the Enterprise Organizations
- Database Auditing is DBAs responsibility – Common Norms goes with DBAs to own this
- Appliance is System Admins Ownership – Can SAs own it?
- Firewall is Network Admins Ownership – Can Network Admins own it?
- Enterprise Auditing is Security Teams Ownership – Can Security Ops Own it?
- AVDF is an application – Can application Admins own it?

## ❑ How Audience is solving this Dilemma today?

## ❑ How Symantec Addressed Ownership Roles & Responsibilities?

- ✓ DBAs owns the Administration, Configuration & Install work of AVDF Application and Database.
- ✓ System Admin owns the VM Administration
- ✓ Security Team owns the Audit Reporting and Scheduling
- ✓ Firewall team, App team are the Governance Body. No Active involvement as such





# Auditing Challenges Solved (using Audit Vault)



- ☐ Manual/Distributed availability of Audit Data – Not at a consolidated place
- ☐ Less controls to protect the audit data – Vulnerable for threats
- ☐ Manual Reviews of Audit Log files
- ☐ Lack of intelligence for immediate actions/alerting when suspicious access is observed (Database Activity Monitoring)
- ☐ Historical trends are very difficult to capture
- ☐ Integration of Audit Data with Other Enterprise Tool Sets like Splunk, Syslog etc
- ☐ SOX, PCI Reporting – QAR Reports





# Audit Vault – SOX & PCI Reporting (QAR Reports)



- ☐ Automated QAR (Quarterly Access Report)
  - Users, Privileges assigned, Last\_Password\_Change etc etc
- ☐ Schedule report weekly/monthly/quarterly/yearly OR run ad-hoc as needed
- ☐ Historical reports are preserved
- ☐ Two reports can be compared easily to find the changes
- ☐ Auditor have authority to schedule as well as review the QAR reports directly

Authentication	Success and Failure
Sensitive Table Access*	Success and Failure
Sensitive Command**	Failure
Account Management	Success or Failure
Database Auditing	Enabled

• For auditing Access related to Sensitive Tables, Use the following AUDIT SQL statement settings:

o AUDIT SELECT, INSERT, DELETE, UPDATE ON <<Table\_Name>> BY ACCESS

• Database schema or structure changes. Use the following AUDIT SQL statement settings:

o AUDIT ALTER ANY PROCEDURE BY ACCESS;  
o AUDIT ALTER ANY TABLE BY ACCESS;  
o AUDIT ALTER DATABASE BY ACCESS;  
o AUDIT ALTER SYSTEM BY ACCESS;  
o AUDIT CREATE ANY JOB BY ACCESS;  
o AUDIT CREATE ANY LIBRARY BY ACCESS;  
o AUDIT CREATE ANY PROCEDURE BY ACCESS;  
o AUDIT CREATE ANY TABLE BY ACCESS;  
o AUDIT CREATE EXTERNAL JOB BY ACCESS;  
o AUDIT DROP ANY PROCEDURE BY ACCESS;  
o AUDIT DROP ANY TABLE BY ACCESS;

• Database access and privileges. Use the following AUDIT SQL statements:

– AUDIT ALTER PROFILE BY ACCESS;  
– AUDIT ALTER USER BY ACCESS;  
– AUDIT AUDIT SYSTEM BY ACCESS;  
– AUDIT CREATE PUBLIC DATABASE LINK BY ACCESS;  
– AUDIT CREATE SESSION BY ACCESS;  
– AUDIT CREATE USER BY ACCESS;  
– AUDIT DROP PROFILE BY ACCESS;  
– AUDIT DROP USER BY ACCESS;  
– AUDIT EXEMPT ACCESS POLICY BY ACCESS;  
– AUDIT GRANT ANY OBJECT PRIVILEGE BY ACCESS;  
– AUDIT GRANT ANY PRIVILEGE BY ACCESS;  
– AUDIT GRANT ANY ROLE BY ACCESS;  
– AUDIT ROLE BY ACCESS;

• Ensuring That Auditing Is Enabled in the Target Database:

```
SQL> SHOW PARAMETER AUDIT_TRAIL
NAME      TYPE      VALUE
-----
audit_trail string    DB
```

## PDF/XLS Reports

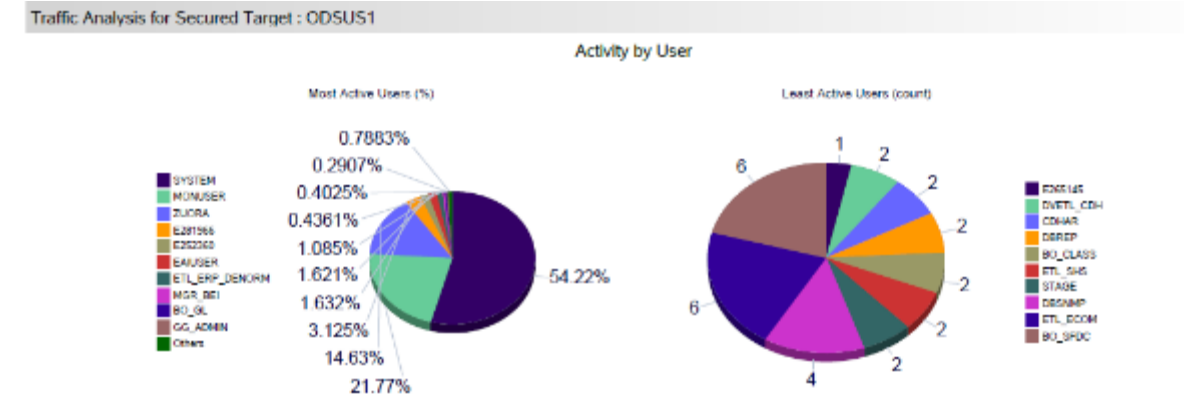
<input type="checkbox"/>	Report Name	Report Description	Category	Schedule Report	Download Report Template	Download Report Definition	Uploaded By
<input type="checkbox"/>	Activity Overview_Sox	Test	Uploaded Reports				AVAUDITOR
<input type="checkbox"/>	SOX QAR ODSUS1	TEST odsus1 QAR report	Uploaded Reports				AVAUDITOR



# Audit Vault Reporting – GDPR reporting needs



- ☐ User Access to sensitive objects Report
  - Monitoring the Sensitive data Usage (ultimate resolution will be using Database Vault)
- ☐ User Privileges Report
  - Track access to Users and its privilege changes
- ☐ User log-in, log-out, log-in failures Report
  - To understand User usage pattern.
  - Failure tracking can lead to track suspicious activity
- ☐ Database Config/Schema Change Report
- ☐ Stored Procedure Modification History
- ☐ Startup and Shutdown Report



Payment Card Industry (PCI) Reports	
To associate Secured Target(s) with this Compliance Category, click on the Go button	
	Go
<a href="#">Activity Overview</a>	Summary of all audited and monitored events
<a href="#">All Activity</a>	All audited and monitored events
<a href="#">Alert Settings Changes</a>	Changes in alert settings
<a href="#">Stored Procedure History</a>	Creation history of stored procedures
<a href="#">Data Access</a>	Details of read/write events
<a href="#">Data Modification</a>	Events related to data modification
<a href="#">Database Schema Changes</a>	Changes in Database Schema
<a href="#">Deleted Stored Procedures</a>	Deletion history of stored procedures
<a href="#">Privileges Changes</a>	Changes in grants of Database privileges and roles
<a href="#">Login Failures</a>	Failed Authentication attempts
<a href="#">Lockdown/Logout</a>	All successful login and logout events
<a href="#">New Stored Procedures</a>	Recently created stored procedures
<a href="#">Startup and Shutdown</a>	System startup and shutdown events
<a href="#">Stored Procedure Activity Overview</a>	Summary of stored procedure activity
<a href="#">Stored Procedure Modification History</a>	Modifications of stored procedures



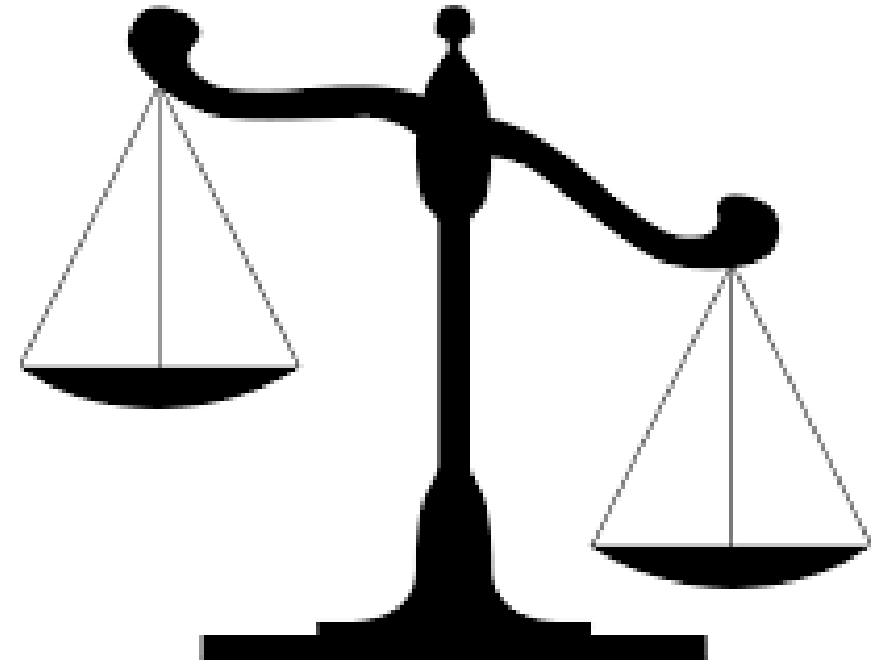
# AVDF – Strengths & Requests

## ☐ Strengths of AVDF

- ✓ The only available solution in its space
- ✓ Easy install and configure
- ✓ Easy to Maintain
- ✓ Monitoring is through OEM

## ☐ Enhancements We'd like to See

- Automated Backups
- Easier troubleshooting
- Schedulable, Automated Archiving



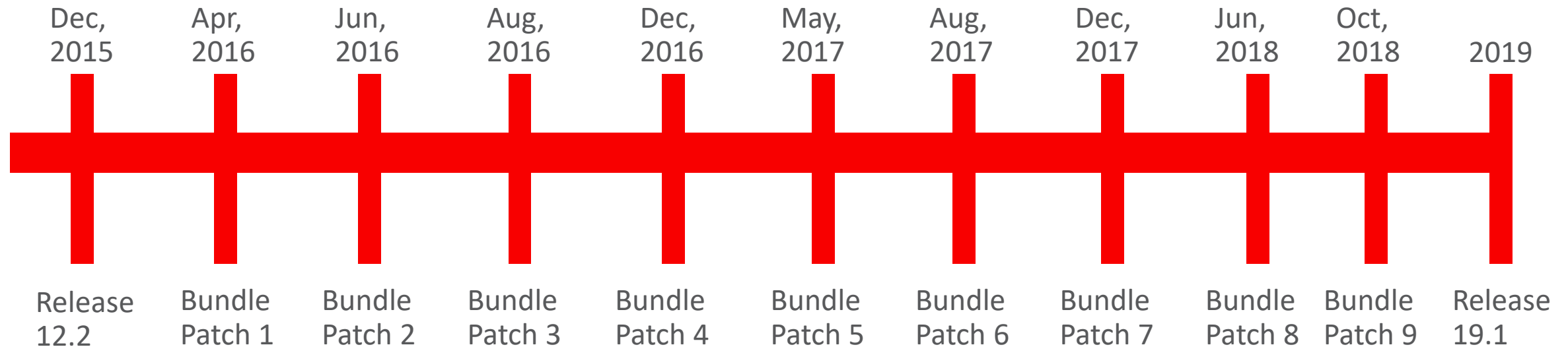


# Audit Vault and Database Firewall version 12.2

- Released December, 2015
- Support for Hybrid Cloud deployments
- Oracle Database In-Memory for AVDF reporting
- Automated fault detection and restart for audit trails
- New reports
  - Database Vault
  - IRS Compliance
  - Summary Reports
  - SUDO correlation for local user activity
- Usability enhancements including non-interactive AVCLI, new backup and restore utility, ability to use your own certificates for the web UIs, registration of hosts using hostname or domain name,



# Audit Vault and Database Firewall – History of Innovation



Each Bundle Patch includes the relevant security patches for the entire AVDF appliance (Database, OS, etc)



# Recent Enhancements to AVDF

- December 2017 (Bundle Patch 7)
  - Target audit collection support for:
    - Red Hat Enterprise Linux 6.7-6.9, 7.1-7.3
    - Microsoft Windows 2016 64-bit
    - Oracle Database 18c
    - AIX 7.2
    - MySQL 5.5.34-5.5.57, 5.6.13-5.6.37, and 5.7.0-5.7.19
    - Active Directory 2016
    - Host Monitor for SUSE Linux 12
  - AVCLI command structure for user and password management



# Recent Enhancements to AVDF

- June 2018 (Bundle Patch 8)
  - New Data Privacy reports to support GDPR and other privacy regulations
  - Support for Autonomous Data Warehouse Cloud Service and MySQL 5.7.21
- October 2018 (Bundle Patch 9)
  - Strict TLS 1.2 for internal communications



# AVDF New Data Privacy Reports – GDPR and Beyond

The screenshot shows the Oracle Audit Vault Server interface. The top navigation bar includes Home, Secured Targets, Reports, Policy, and Settings. The left sidebar lists various report categories: BUILT-IN REPORTS (Activity Reports, Summary Reports, Compliance Reports, Specialized Reports), CUSTOM REPORTS (PDF/XLS Reports, Saved Interactive Reports), REPORT WORKFLOW (Report Schedules, Generated Reports), and QUICK LINKS (Audit Trails, Enforcement Points, Jobs). The main content area is titled 'Data Privacy Reports' and contains a section for associating Secured Target(s) with a Compliance Category. Below this, there are links for Sensitive Data, Access Rights to Sensitive Data, Activity on Sensitive Data, and Activity on Sensitive Data by Privileged Users. At the bottom, there are buttons for various regulatory reports: Payment Card Industry (PCI) Reports, Gramm-Leach-Bliley Act (GLBA) Reports, Health Insurance Portability and Accountability Act (HIPAA) Reports, Sarbanes-Oxley Act (SOX) Reports, Data Protection Act (DPA) Reports, and Reports based on IRS Publication 1975.

ORACLE Audit Vault Server

version: 12.2.0.8.0 | avauditor | Help | Logout

Home | Secured Targets | Reports | Policy | Settings

Home > Reports > Compliance Reports

**BUILT-IN REPORTS**

- Activity Reports
- Summary Reports
- Compliance Reports
- Specialized Reports

**CUSTOM REPORTS**

- PDF/XLS Reports
- Saved Interactive Reports

**REPORT WORKFLOW**

- Report Schedules
- Generated Reports

**QUICK LINKS**

- Audit Trails
- Enforcement Points
- Jobs

**Data Privacy Reports**

To associate Secured Target(s) with this Compliance Category, click on the Go button

[Sensitive Data](#) Details of sensitive data

[Access Rights to Sensitive Data](#) User's access rights to sensitive data

[Activity on Sensitive Data](#) Activity on sensitive data by all users

[Activity on Sensitive Data by Privileged Users](#) Activity on sensitive data by privileged users

Payment Card Industry (PCI) Reports

Gramm-Leach-Bliley Act (GLBA) Reports

Health Insurance Portability and Accountability Act (HIPAA) Reports

Sarbanes-Oxley Act (SOX) Reports

Data Protection Act (DPA) Reports

Reports based on IRS Publication 1975

All times are UTC-04:00  
Copyright (c) 1998, 2018 Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

The screenshot shows the 'Sensitive Data' report interface. It includes a search bar with a 'Go' button and an 'Actions' dropdown. Below the search bar, there is a section for 'Secured Target Name' with a checkbox and a red 'X' icon. The main content is a table titled 'Secured Target Name : target2' with columns: Sensitive Schema Name, Target Type, Target Object, Column Name, and Sensitive Type. The table lists 12 rows of sensitive data. The bottom right corner shows '1 - 12'.

Sensitive Data

Q Go Actions

Secured Target Name ☒ ☒

Secured Target Name : target2

Sensitive Schema Name ▲	Target Type	Target Object	Column Name	Sensitive Type
SCOTT	TABLE	CCDATA	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CREDITCARD	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	TEST	CREDIT_CARD_NUMBER	CREDIT_CARD_NUMBER
SCOTT	TABLE	CCDATA	EMAIL_ID	EMAIL_ID
SCOTT	TABLE	CCDATA	IP_ADDRESS	IP_ADDRESS
SCOTT	TABLE	CCDATA	ISBN_10	ISBN_10
SCOTT	TABLE	CCDATA	ISBN_13	ISBN_10
SCOTT	TABLE	CCDATA	NATIONAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_INSURANCE_NUMBER	NATIONAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	PHONE_NUMBER	PHONE_NUMBER
SCOTT	TABLE	CCDATA	SOCIAL_SECURITY_NUMBER	SOCIAL_INSURANCE_NUMBER
SCOTT	TABLE	CCDATA	UNIVERSAL_PRODUCT_CODE	UNIVERSAL_PRODUCT_CODE

1 - 12



# How does AVDF Know What Is Sensitive

- Import Sensitive Data Discovery results from
  - Enterprise Manager
  - Database Security Assessment Tool (DBSAT)
- Review the Reports chapter of the AVDF Auditor's guide for details

The screenshot displays the 'Oracle Audit Vault and Database Firewall Auditor's Guide' table of contents on the left. The 'Reports' chapter is expanded, and the 'Data Privacy Reports' sub-chapter is highlighted with a red box. A red arrow points from this box to the 'Importing Sensitive Data Into AVDF Repository' section on the right. The right side shows the content of this section, including a 'Note' about supported Oracle Enterprise Manager versions and a 'See Also' list of related guides. Below the 'See Also' list, a numbered list of steps is provided for importing sensitive data.

## Importing Sensitive Data Into AVDF Repository

Information about sensitive data is imported and stored in the AVDF repository. You can import a data file in .csv and .xml format. These data files are sourced from *Oracle Enterprise Manager* and *Oracle Database Security Assessment Tool* by running data discovery job to search for sensitive data in specific Oracle Database secured targets.

Oracle Database Security Assessment Tool generates the file in .csv format and Oracle Enterprise Manager generates the file in .xml format. The data file extracted contains a list of sensitive columns that is imported into the AVDF repository. It is viewed in the Audit Vault Server GUI using **Data Privacy Reports**.

**Note:**  
Oracle Audit Vault and Database Firewall supports 13.1 and 13.2 versions of Oracle Enterprise Manager Cloud Control.

**See Also:**


- *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* to run data discovery job and search for sensitive data for specific targets using *Oracle Enterprise Manager*.
- *Oracle Database Security Assessment Tool User Guide* to run a discovery job using *Oracle Database Security Assessment Tool*.
- *Oracle Data Masking and Subsetting Guide* for more information on Application Data Modeling that stores the list of applications, tables, and relationships between table columns and maintains sensitive data types.

1. Ensure you have the sensitive data report in .csv or .xml format by running data discovery job through Oracle Database Security Assessment Tool or Oracle Enterprise Manager respectively.
2. Save the file in your local drive.
3. Log in to the Audit Vault Server GUI as root user.
4. Switch to oracle user, by executing  
`su - oracle`



# What's Next for AVDF?

- We're working on
  - New target types
    - MongoDB
    - Cloudera Hadoop
  - Expanded Custom Target Framework
    - JSON
    - REST
  - Infrastructure improvements
    - AVDF console integration with LDAP
    - Before/After Values
    - Automated, Schedulable Archiving



Potential product  
direction. Please  
refer  
to safe harbor  
slide 2



# Parting Thoughts

- No security solution is complete without auditing/activity monitoring
- Database activity monitoring is particularly important because of the threat to the data and the risk involved if a breach occurs
- Oracle Audit Vault and Database Firewall not only works with Oracle Databases, but also with most common RDBMS platforms

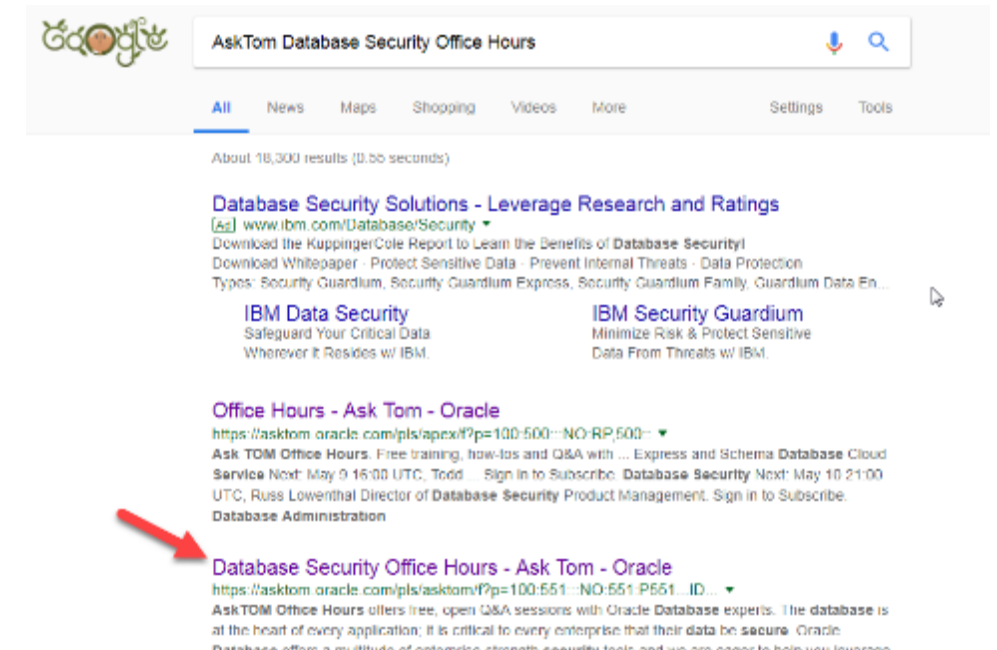


# AskTOM Database Security Office Hours



- Direct line into Database Security product development
- Second Thursday of every month, 09:00 and 20:00 UTC (identical sessions)
- URL: <http://bit.ly/asktomdbsec>
- Or, just search

AskTom Database Security Office Hours







Don't Let Your Data Assets  
Become a Liability

Secure Your Data, Secure Your  
Business

Oracle Security Solutions

