Stalking the Hackers: Effective Tips for Auditing and Monitoring Oracle Database

November 21, 2019

Ashok Swaminathan

Sr. Director, Database Security Product Management,
Oracle Database Security

Ram Subramanian

Director, IT, ERP & Database Services,

Symantec Corporation

Safe Harbor

The preceding 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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at http://www.oracle.com/investor. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.

Data Breaches Exploding World-Wide(2018-2019)

It's no longer about **WHETHER** you'll get breached; it's about **WHEN** !

1M Google Plus 2018

150M Under Armour 2018

11M **Quest Diagnostics** 2019

1M **Orbitz** 2018

540M Facebook 2019

106M Capital One 2019

5M Bulgaria National Revenue Agency 2019

0.5M British Airways 2018

500M **Marriott** 2018

885M First American Corporation 2019

2M **T-Mobile** 2018

3M Dominion National 2019

300M Truecaller 2019

92M MyHeritage 2018

9.4M **Cathay Pacific** 2018

3M **Toyota** 2019

60M US Postal Service 2018

100M Quora 2018

28M HauteLook 2018

100M JustDial 2019

1M Health Sciences Authority (Singapore) 2019

1M Westpac 2019

2.9M Desjardins 2019

2M Earl Enterprises 2019

6.8M StockX 2019

7.7M LabCorp 2019

1.5M SingHealth 2018

19 years of Data Australian National University 2019

140M Canva 2019

British Airways - £183M
Marriott - $123M
Google - $57M

Security Zones of Control for Oracle Databases

Assess

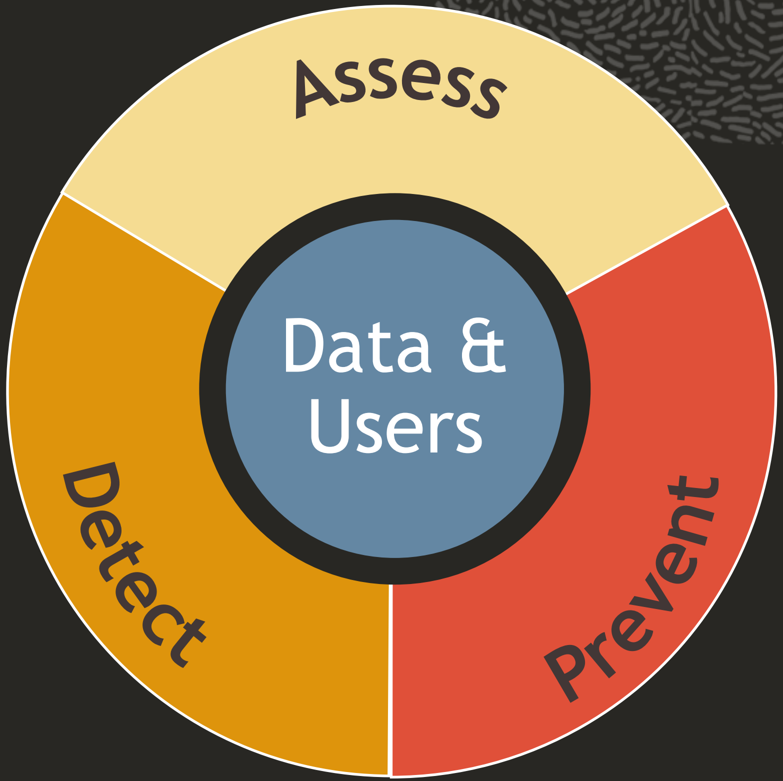
Security-Assessment (DBSAT)
Data Discovery
Privilege Analysis*

Detect

Activity Auditing/Monitoring
Audit Vault
Database Firewall*

Prevent

Encryption & Key Vault
Data Masking, Data Redaction
Database Vault*



Data

Crypto Toolkit
Virtual Private Database
Label Security
Real Application Security*

Users

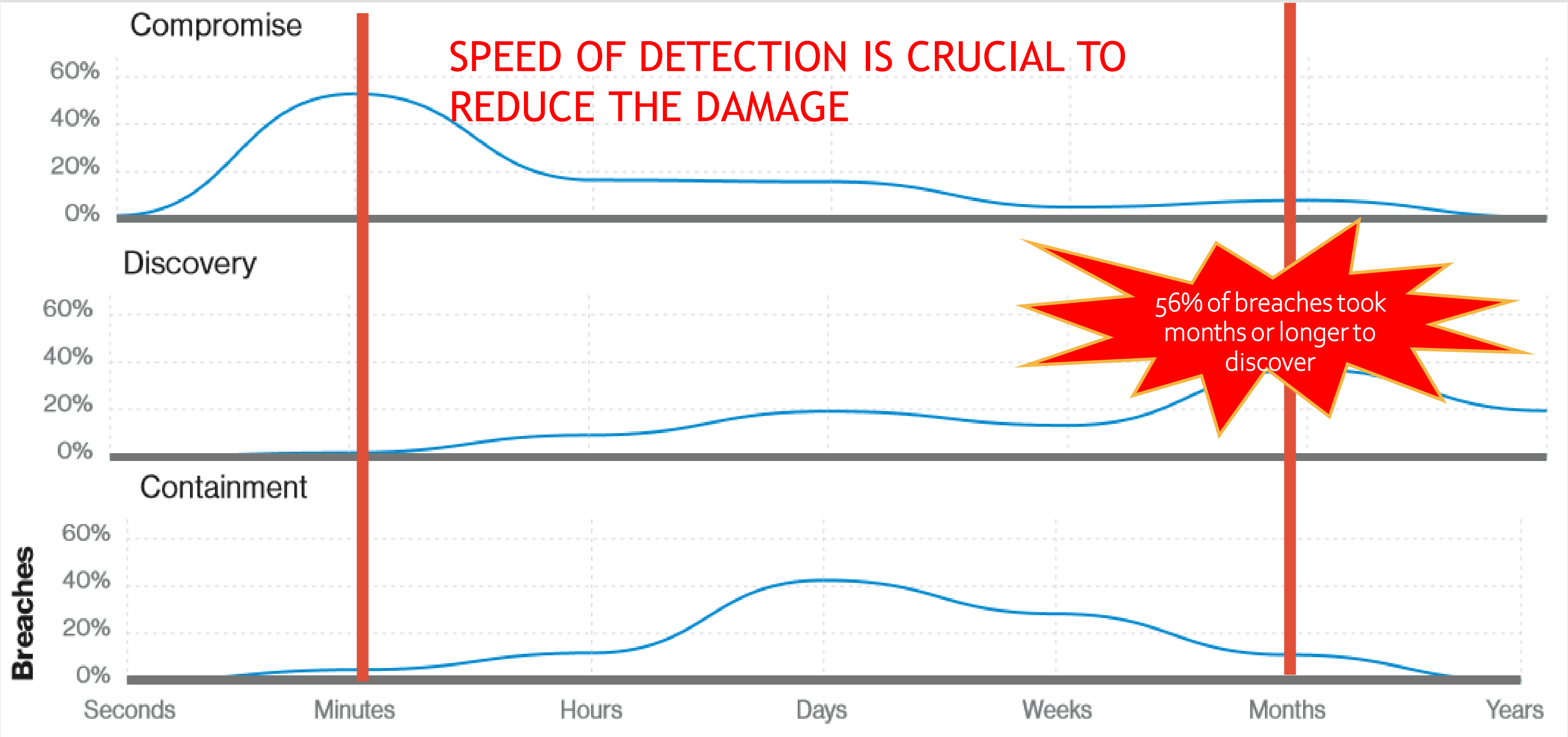
Password, PKI, Kerberos, Radius
Proxy Users, Password Profiles
Oracle & Active Directory

*** unique to Oracle**

Minimizing Time To Discovery

Data Breaches typically take minutes for compromise, but months to discover

Database Activity Monitoring (DAM) is key to identifying breaches and responding quickly



SPEED OF DETECTION IS CRUCIAL TO REDUCE THE DAMAGE

56% of breaches took months or longer to discover

Verizon’s 2019 Data Breach Investigations Report

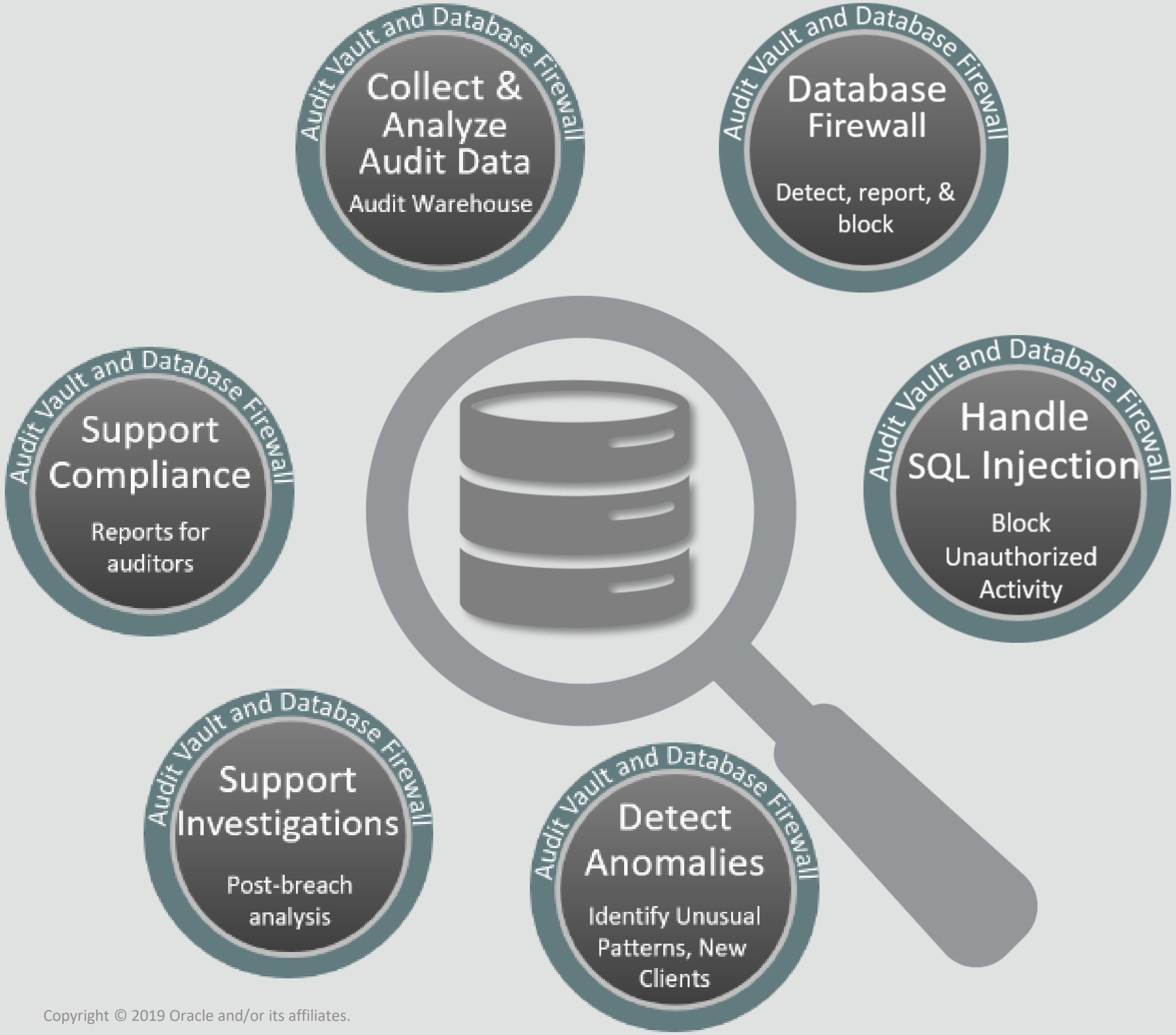
What is Database Activity Monitoring(DAM) ?

- Observing database actions and reporting policy issues in real time
- Complementary methodologies:

	Database Auditing	Network Monitoring
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	Identify SQL-Injections and other unauthorized activity, enforce corporate data security policy

Oracle Audit Vault and Database Firewall: DAM solution for Oracle and non-Oracle databases

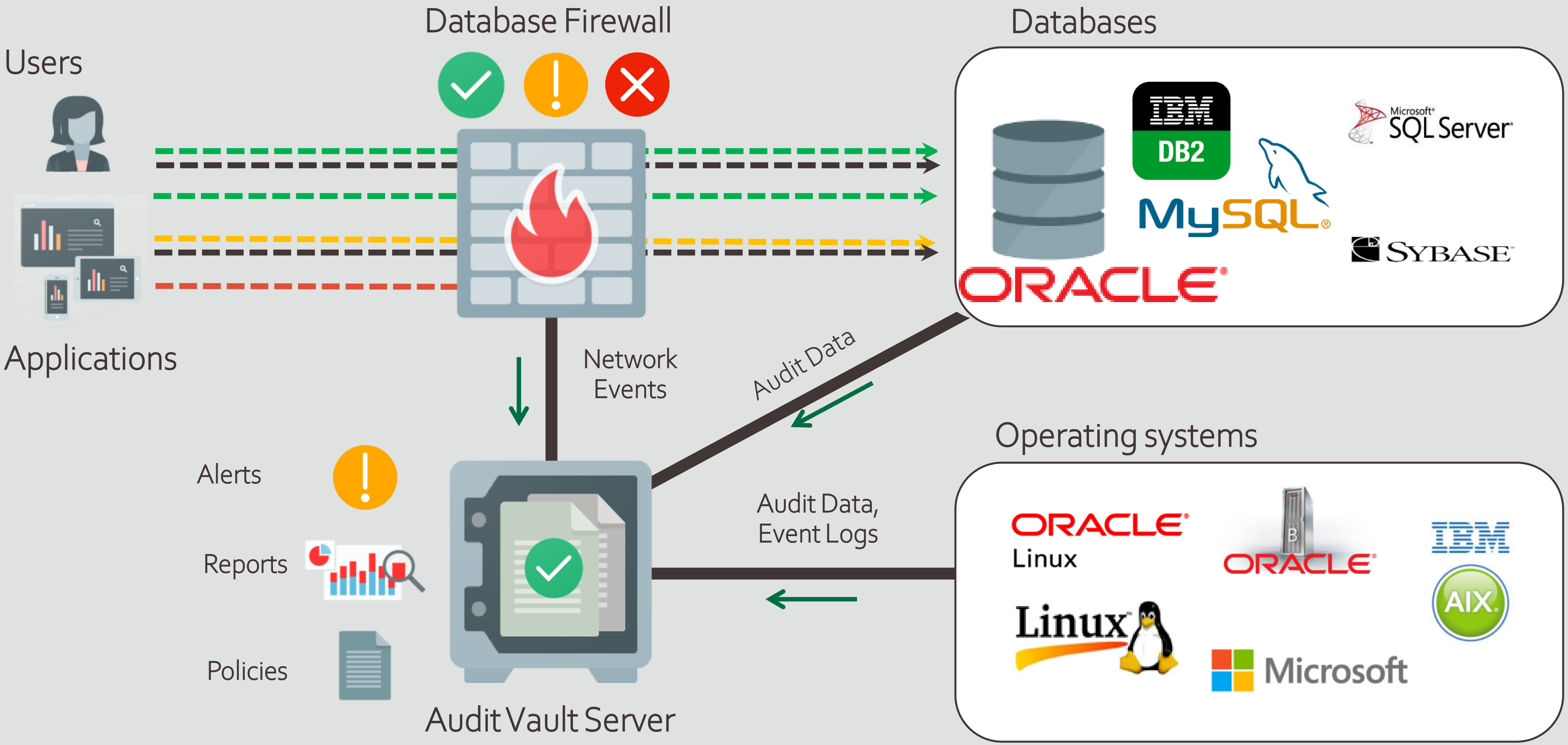
Oracle Audit Vault and Database Firewall


Audit Vault and Database Firewall
Collect & Analyze Audit Data
Audit Warehouse
Audit Vault and Database Firewall
Database Firewall
Detect, report, & block
Audit Vault and Database Firewall
Support Compliance
Reports for auditors
Audit Vault and Database Firewall
Handle SQL Injection
Block Unauthorized Activity
Audit Vault and Database Firewall
Support Investigations
Post-breach analysis
Audit Vault and Database Firewall
Detect Anomalies
Identify Unusual Patterns, New Clients

Key capabilities

- Security hardened software appliance
- Consolidates audit data from databases, operating systems, and directories
- Supports Oracle and non-Oracle Databases
- Database Anomaly Detection
- Detect and block SQL Injection
- Custom and pre-defined regulatory reports
- Custom generated alerts

Oracle Audit Vault and Database Firewall



Configuring Oracle Audit Vault and Database Firewall

Database Audit Collection

Network Monitoring

Database Audit Collection with AVDF

CONFIGURE TARGETS AND TRAILS

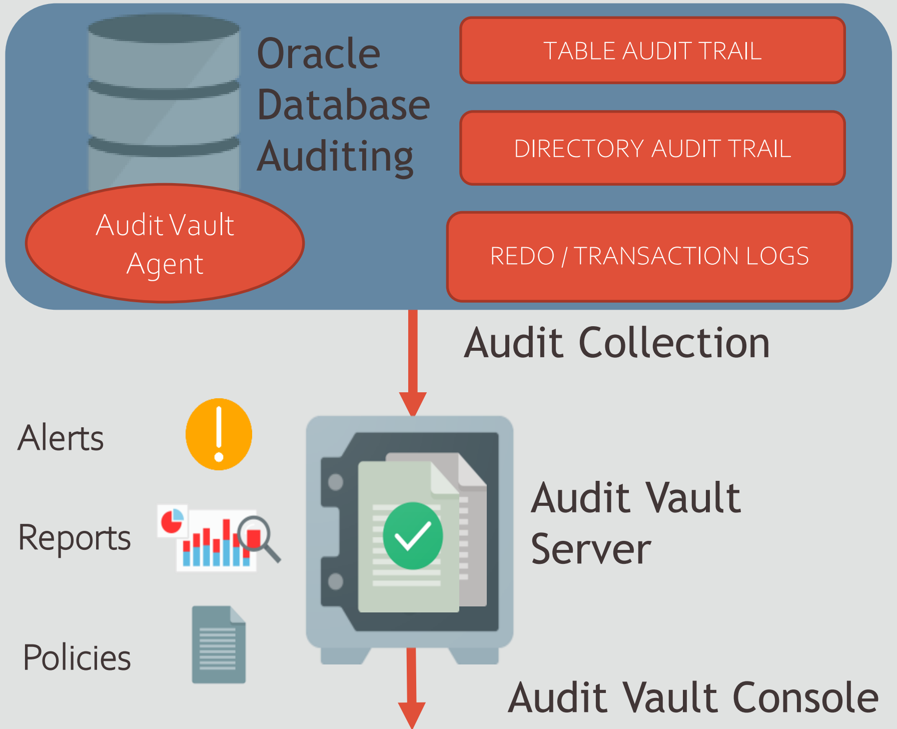
- Targets
- Audit Vault Agents
- Audit data collection
- Data retention policy

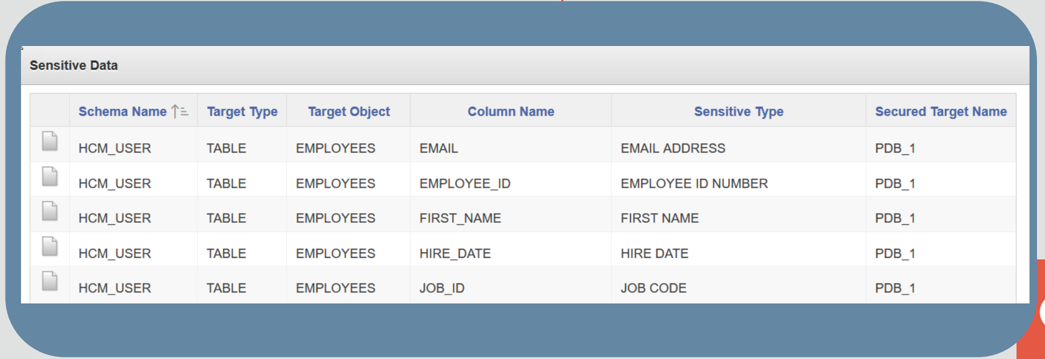
CONFIGURE AUDIT POLICIES

- Who
- What
- When
- Where

CREATE REPORTS AND ALERTS

- Define alert baselines
- Create and schedule reports





Sensitive Data

	Schema Name	Target Type	Target Object	Column Name	Sensitive Type	Secured Target Name
	HCM_USER	TABLE	EMPLOYEES	EMAIL	EMAIL ADDRESS	PDB_1
	HCM_USER	TABLE	EMPLOYEES	EMPLOYEE_ID	EMPLOYEE ID NUMBER	PDB_1
	HCM_USER	TABLE	EMPLOYEES	FIRST_NAME	FIRST NAME	PDB_1
	HCM_USER	TABLE	EMPLOYEES	HIRE_DATE	HIRE DATE	PDB_1
	HCM_USER	TABLE	EMPLOYEES	JOB_ID	JOB CODE	PDB_1

Tips for Effective Oracle Database Auditing

TIPS & TRICKS

ALWAYS-ON Audit

ALWAYS audited with Mandatory Auditing

1. Top level Statements by administrative users SYS, SYSDBA, SYSOPER, and SYSDG until database opens
2. Data/metadata modification attempt of unified audit tables

TIPS & TRICKS

PREDEFINED Unified Audit Policies

Pre-designed commonly used policies

1. Logon Failures
2. Secure Configurations
3. CIS Recommended Audit

Tips for Effective Oracle Database Auditing

TIPS & TRICKS

SELECTIVE and FOCUSED Unified Audit Policies

→ Audit all administrative user Top-Level actions

→ Audit based on conditions to reduce noise

→ Use Exception-based auditing

→ Extend the audit trail to include default or application contexts

AUDIT CONTEXT NAMESPACE ebusiness_context ATTRIBUTES form, action, active_responsibility;

Custom Application Contexts are supported!

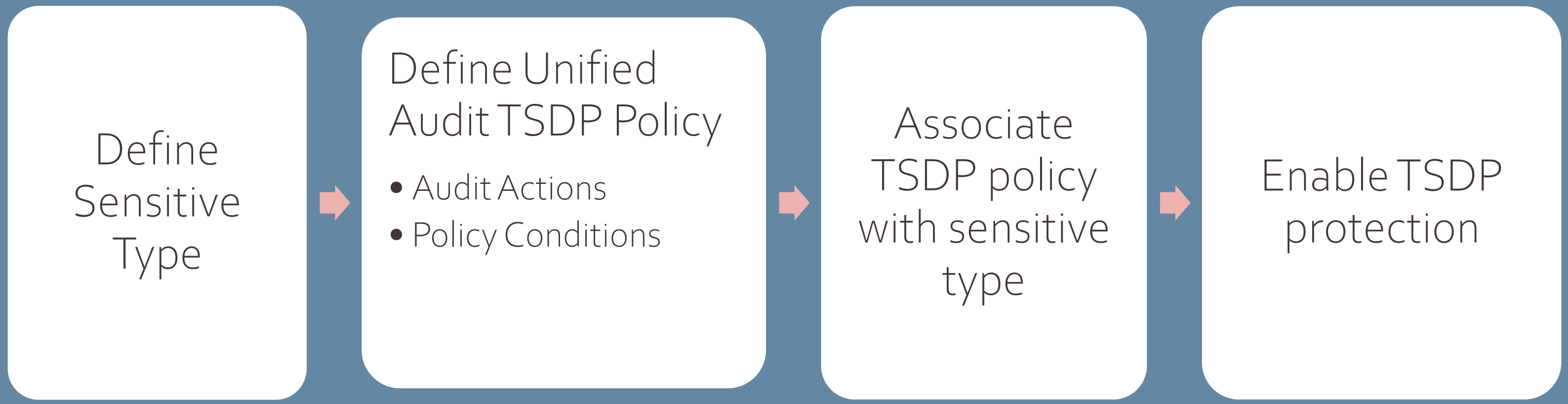
Tips for Effective Oracle Database Auditing

TIPS & TRICKS

Audit Sensitive Data Access

- Identify sensitive data (DBSAT / Enterprise Manager's ADM)
- Audit access to sensitive data
- Monitor using AVDF Data Privacy Reports

Use Transparent Sensitive Data Protection (TSDP) policies with Unified Auditing



Define Sensitive Type

Define Unified Audit TSDP Policy
- Audit Actions
- Policy Conditions

Associate TSDP policy with sensitive type

Enable TSDP protection

employee_id between 100 and 110 PHONE_NUMBER, SALARY

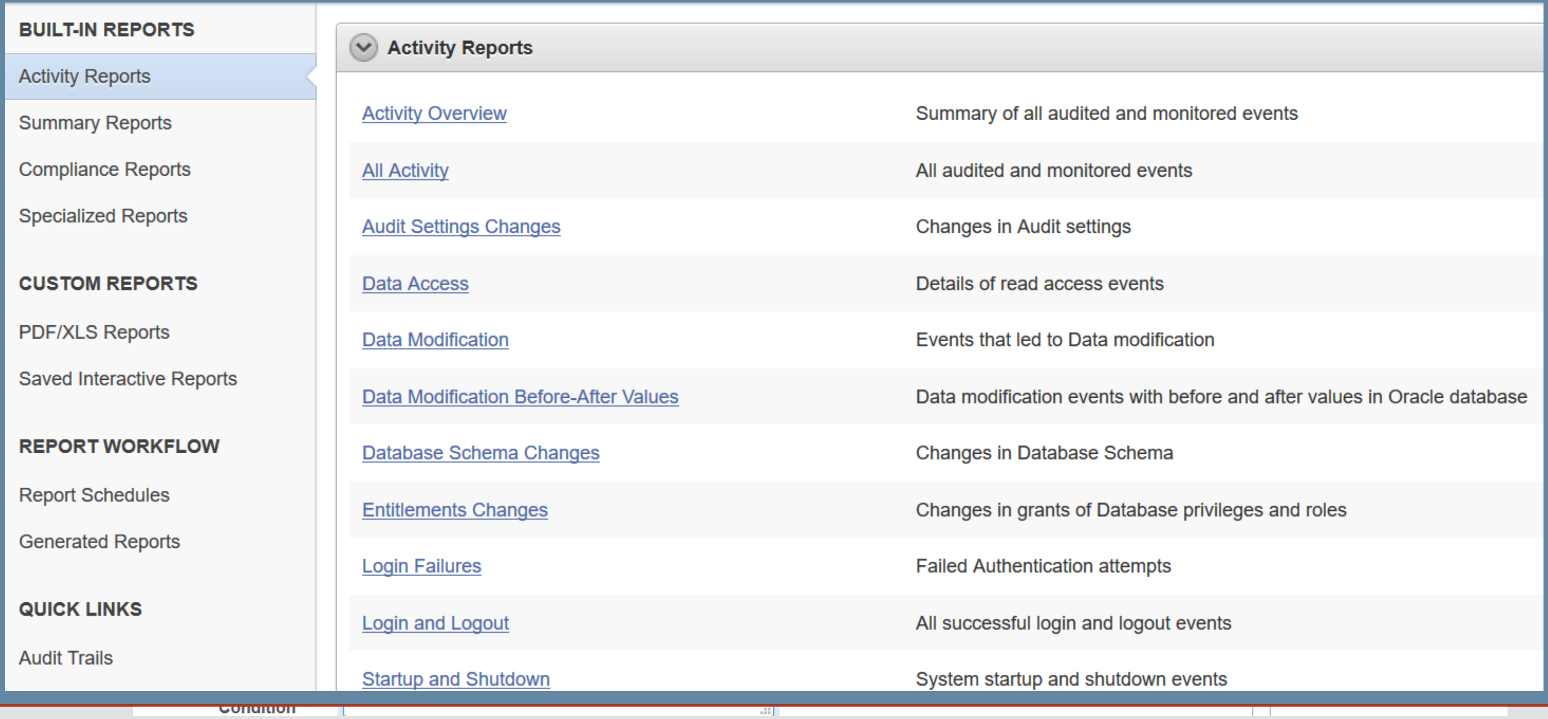
Oracle Database Auditing: Alerting Tips

TIPS & TRICKS

Baseline Alerts

- → Plan and Configure Alerts That Work for You!
- → Define alerts that are actionable and granular
- → Monitor alerts from console dashboard / alert reports

Define meaningful alerts for events that concerns you!



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

Activity Reports

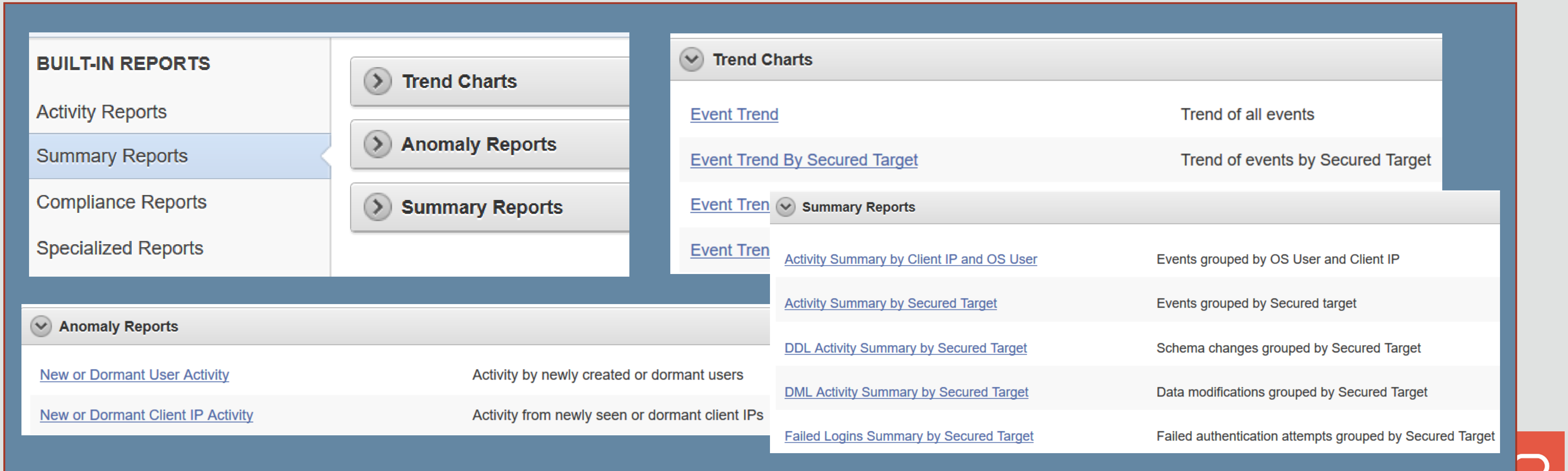
Activity Overview	Summary of all audited and monitored events
All Activity	All audited and monitored events
Audit Settings Changes	Changes in Audit settings
Data Access	Details of read access events
Data Modification	Events that led to Data modification
Data Modification Before-After Values	Data modification events with before and after values in Oracle database
Database Schema Changes	Changes in Database Schema
Entitlements Changes	Changes in grants of Database privileges and roles
Login Failures	Failed Authentication attempts
Login and Logout	All successful login and logout events
Startup and Shutdown	System startup and shutdown events

Oracle Database Auditing: Reporting Tips

TIPS & TRICKS

Examine audit data in a consolidated manner with AVDF Reports

- Activity Reports tracks general database access activities
- Summary Reports shows user activity on specific targets or across the enterprise
- Compliance Reports to help meet regulations



BUILT-IN REPORTS

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

Trend Charts

Event Trend	Trend of all events
Event Trend By Secured Target	Trend of events by Secured Target
Event Tren	
Event Tren	

Summary Reports

Activity Summary by Client IP and OS User	Events grouped by OS User and Client IP
Activity Summary by Secured Target	Events grouped by Secured target
DDL Activity Summary by Secured Target	Schema changes grouped by Secured Target
DML Activity Summary by Secured Target	Data modifications grouped by Secured Target
Failed Logins Summary by Secured Target	Failed authentication attempts grouped by Secured Target

Anomaly Reports

New or Dormant User Activity	Activity by newly created or dormant users
New or Dormant Client IP Activity	Activity from newly seen or dormant client IPs

Configuring Oracle Audit Vault and Database Firewall

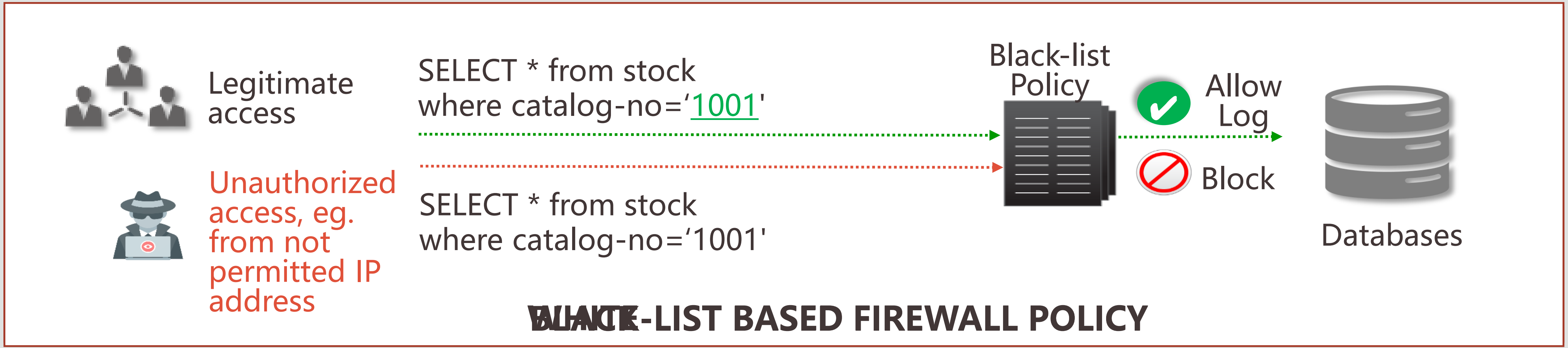
Database Audit Collection

Network Monitoring

Network Monitoring with AVDF

Monitoring SQL with Database Firewall

- Detection and blocking based on capturing normal application SQL patterns
- Does not use easy-to-defeat regular expressions
- Detect or block never-before-seen SQL from ever reaching the database
- Anomaly detection and threat blocking with white-list /black-list based policy



Legitimate access

SELECT * from stock
where catalog-no=‘1001'

Unauthorized access, eg. from not permitted IP address

SELECT * from stock
where catalog-no=‘1001'

Black-list Policy

Allow
Log

Block

Databases

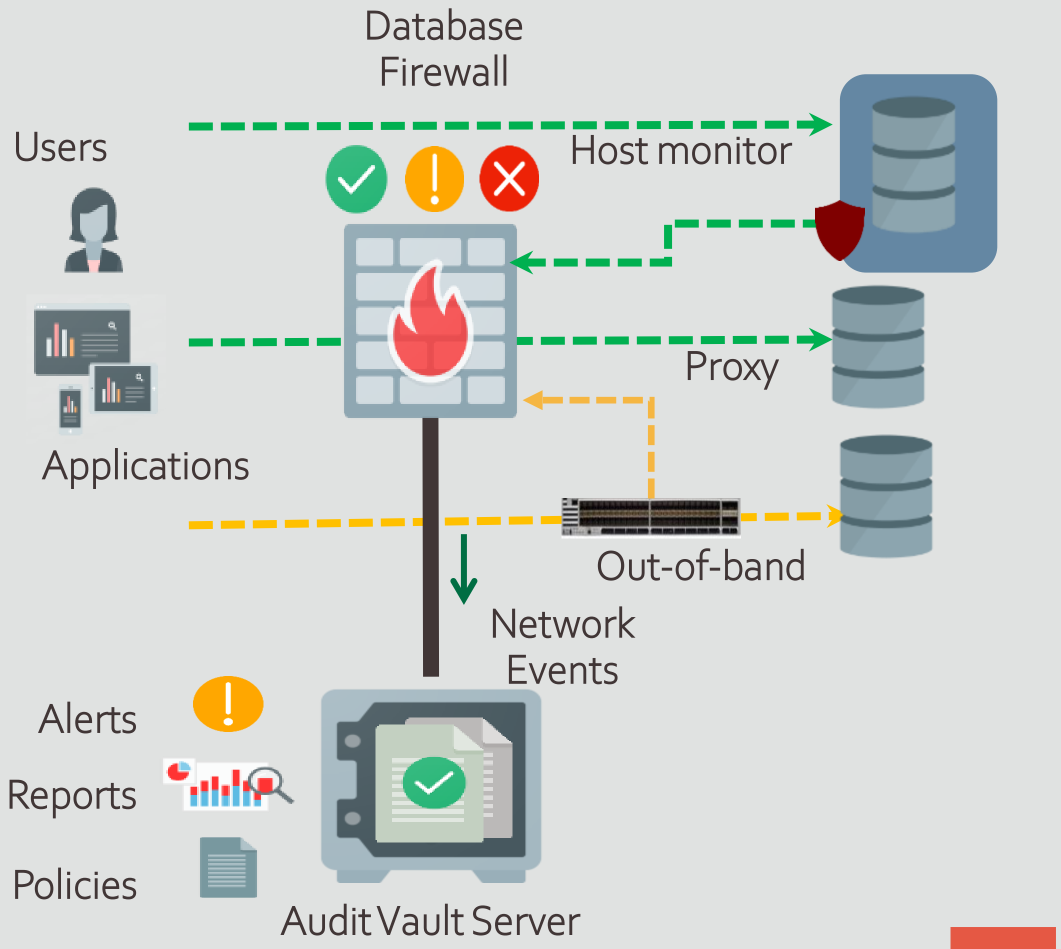
WHITE BLACK-LIST BASED FIREWALL POLICY

Network Monitoring: Deployment Tips

TIPS & TRICKS

Choose from 3 flexible deployment options

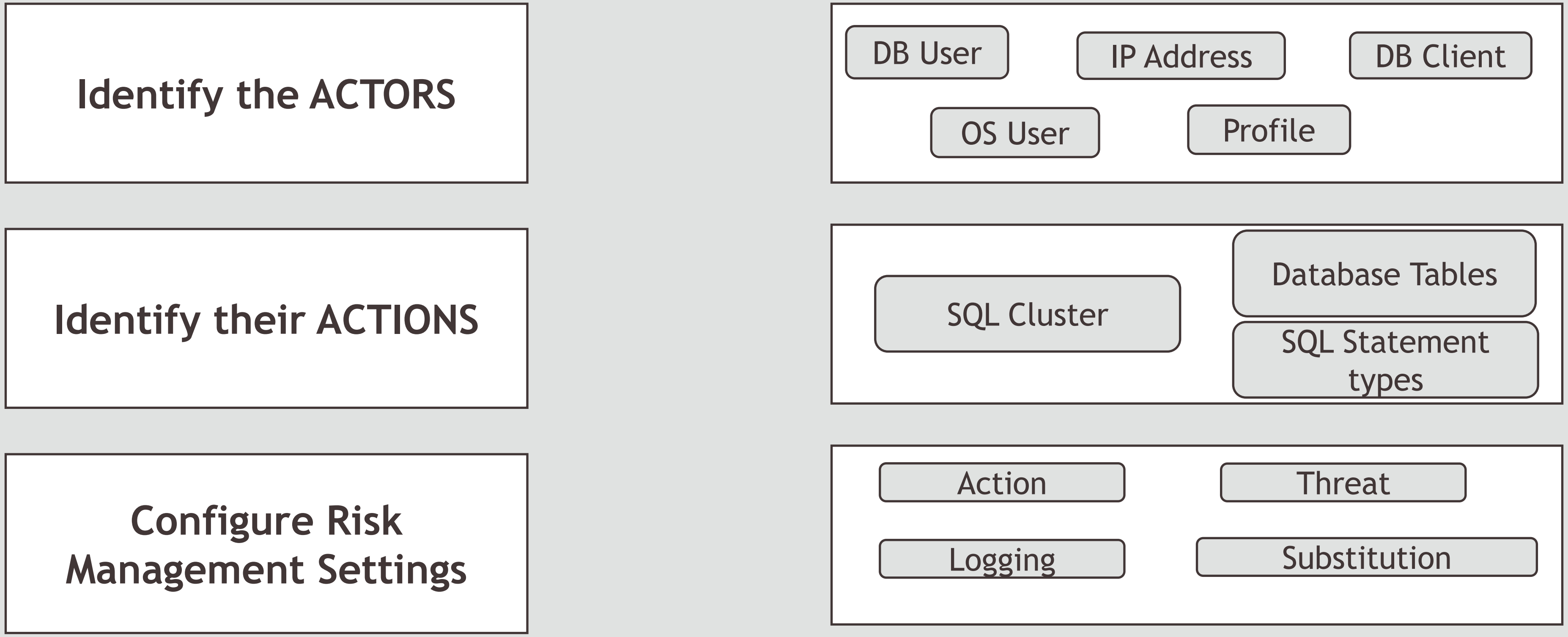
Proxy	Detect and prevent unauthorized access over access over the network to the database database
Host Monitor Monitor	Actively monitor database network traffic traffic
Out-of-band	Actively monitor database traffic over network agent-free



Network Monitoring :Tips for Configuring Database Firewall Policy

TIPS & TRICKS

- → Identify the Actors
- → Identify their Actions
- → Configure Risk Management Settings



Identify the ACTORS

DB User

IP Address

DB Client

OS User

Profile

Identify their ACTIONS

SQL Cluster

Database Tables

SQL Statement types

Configure Risk Management Settings

Action

Threat

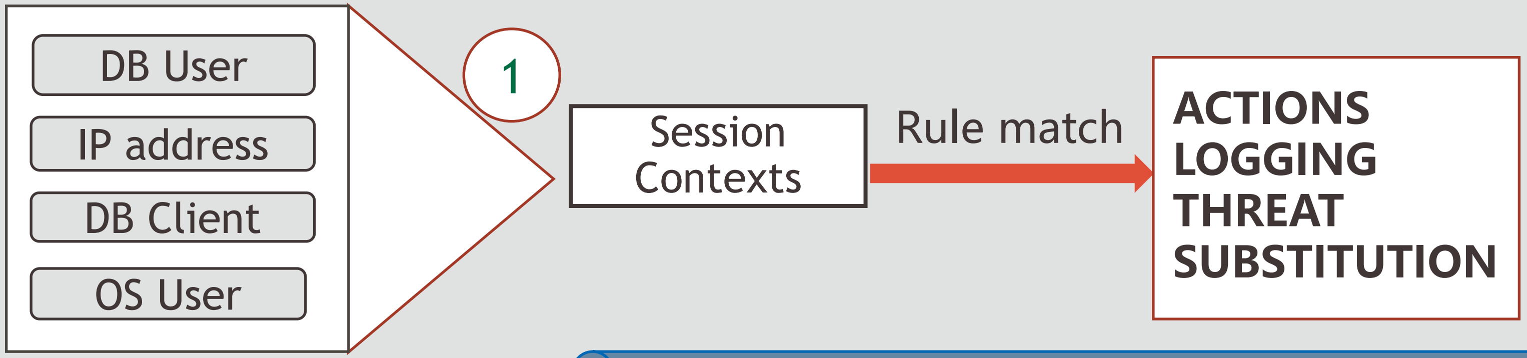
Logging

Substitution

Network Monitoring : Tips for configuring Firewall Policy Rules

TIPS & TRICKS

Configure Session Context rules based on Actors and Risk Management Settings

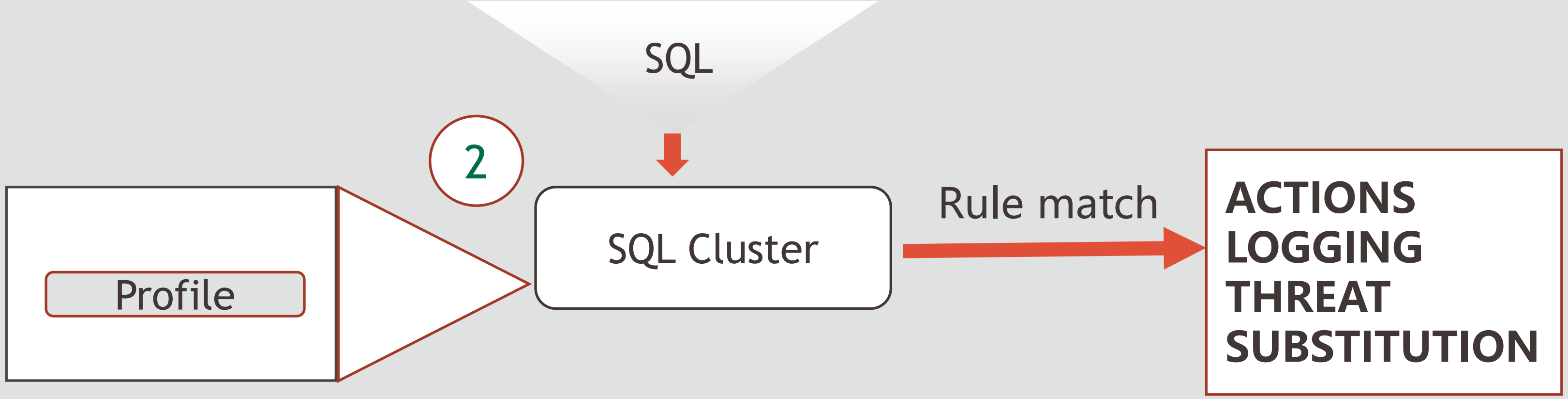


- Trusted Application paths based on session attributes
- Create KNOWN “profiles” for groups of actors

Network Monitoring : Tips for configuring Firewall Policy Rules

TIPS & TRICKS

Configure SQL Cluster rules based on Actors, Actions and Risk Management Settings

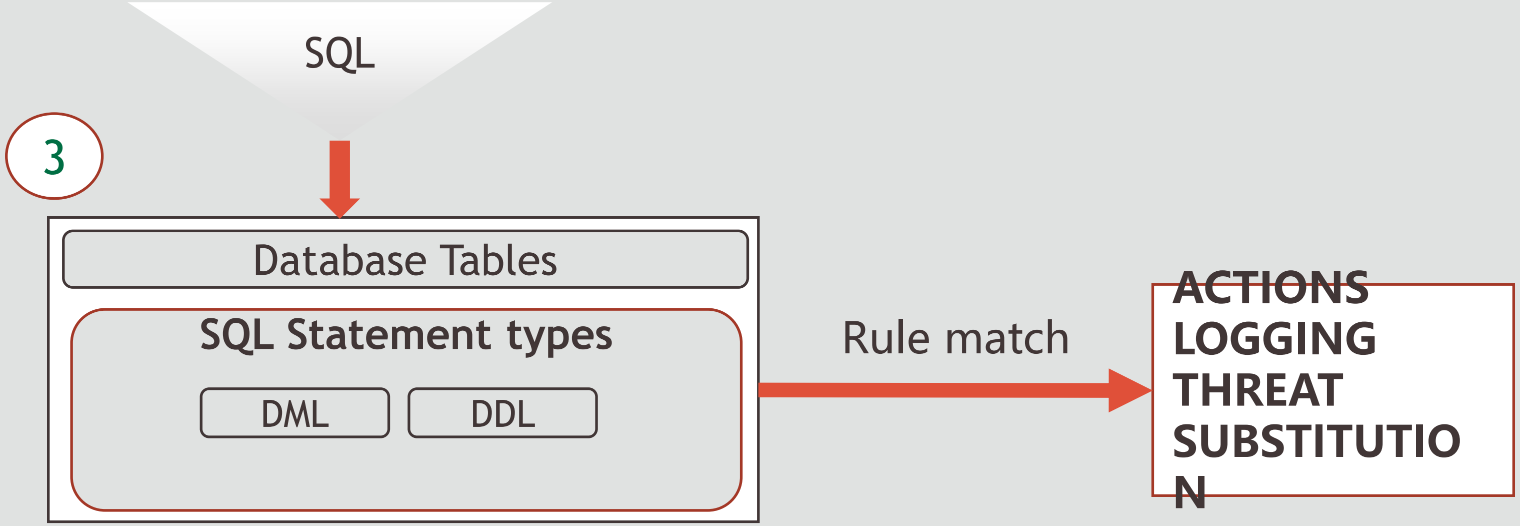


- Policy rules based on session attributes and SQL Statements.
- Control privileged user activity

Network Monitoring : Tips for configuring Firewall Policy Rules

TIPS & TRICKS

Configure database table specific rules based on Actions and Risk Management Settings



- Identify unauthorized access to Sensitive Data

Please Welcome
Symantec Corporation

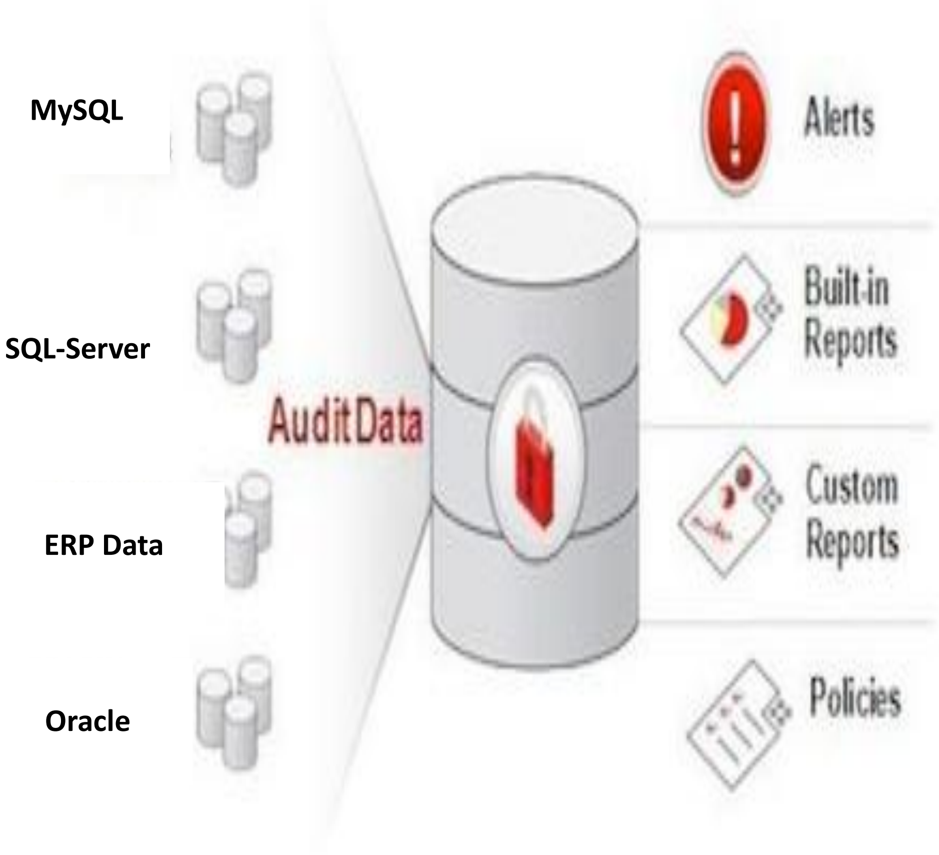
Effective Tips for Auditing and Monitoring Oracle Database using Oracle Audit Vault and Database Firewall (AVDF)

Agenda

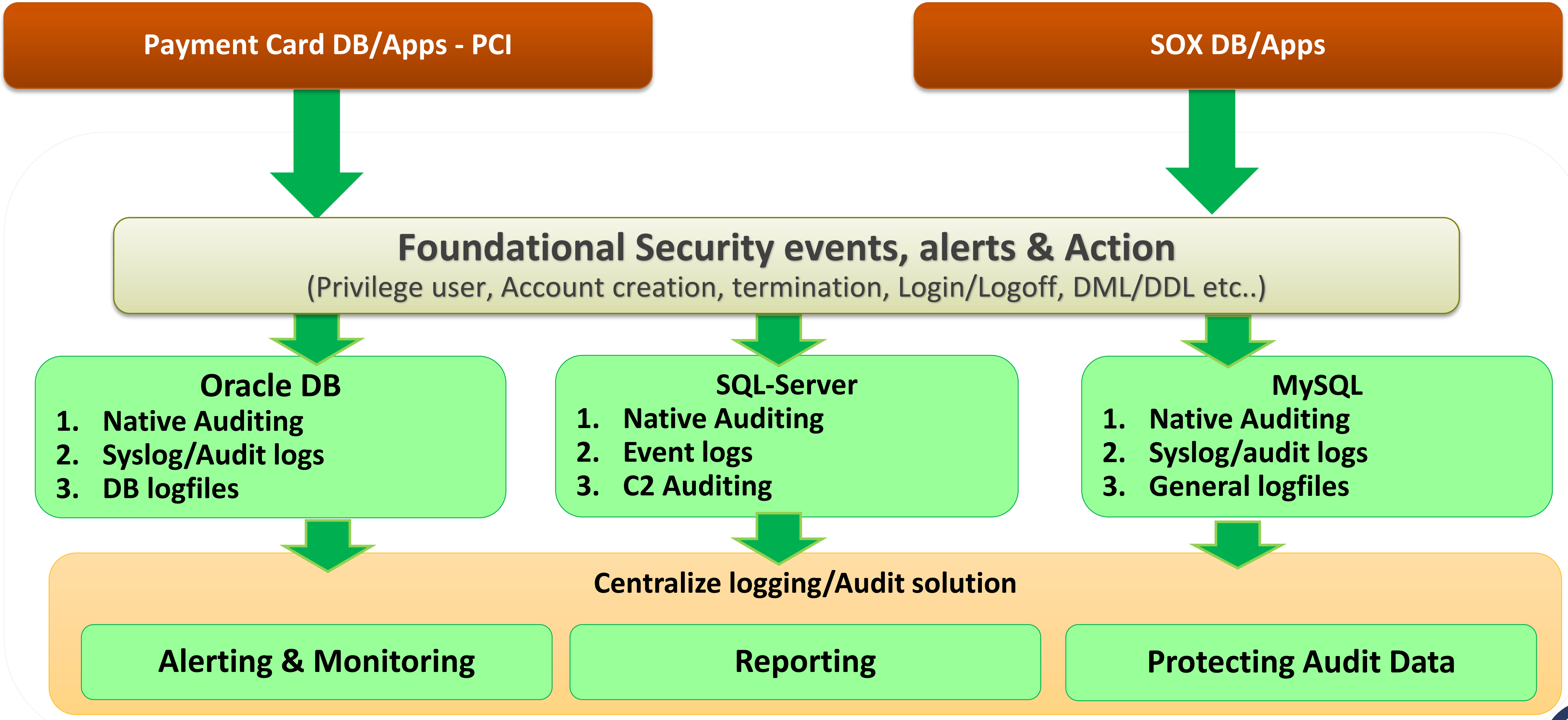
1. Overview of Symantec
2. Symantec’s Current Auditing requirement
3. Audit Vault and Database Firewall Architecture
4. Symantec’s Auditing & Logging Framework
5. Implementation and Future Directions

Auditing Challenges & Top AVDF Features Symantec Leveraged

Challenges	AVDF Feature
Distributed & Unsecured Audit Data	Centralized & Encrypted Audit Data. Support for Heterogeneous DB platforms
Lack of Intelligent Alerting	Powerful and Customizable alert policies to Detect & Report security threats for Hosts/Databases
Audit Trailing with compliance	Ensure regularity compliance and guaranteed Audit Trail to enable strong controls over who, when, and where application can be accessed
Manual Report Generation	SOX - QAR reporting is now out-of-box with click of a button
Tedious Manual Review for Historical Analysis (Scan-Through)	AVDF designed to be a secure data warehouse of Information Log and Audit Log. Easy Navigation & Reporting
Manual Audit Log Purging	Real Time Data Collection by AV Agents, including option to Purge old Audit Data from Secured Target



Symantec’s Auditing & Logging Framework



Payment Card DB/Apps - PCI

SOX DB/Apps

Foundational Security events, alerts & Action

(Privilege user, Account creation, termination, Login/Logoff, DML/DDL etc..)

Oracle DB

1. Native Auditing
2. Syslog/Audit logs
3. DB logfiles

SQL-Server

1. Native Auditing
2. Event logs
3. C2 Auditing

MySQL

1. Native Auditing
2. Syslog/audit logs
3. General logfiles

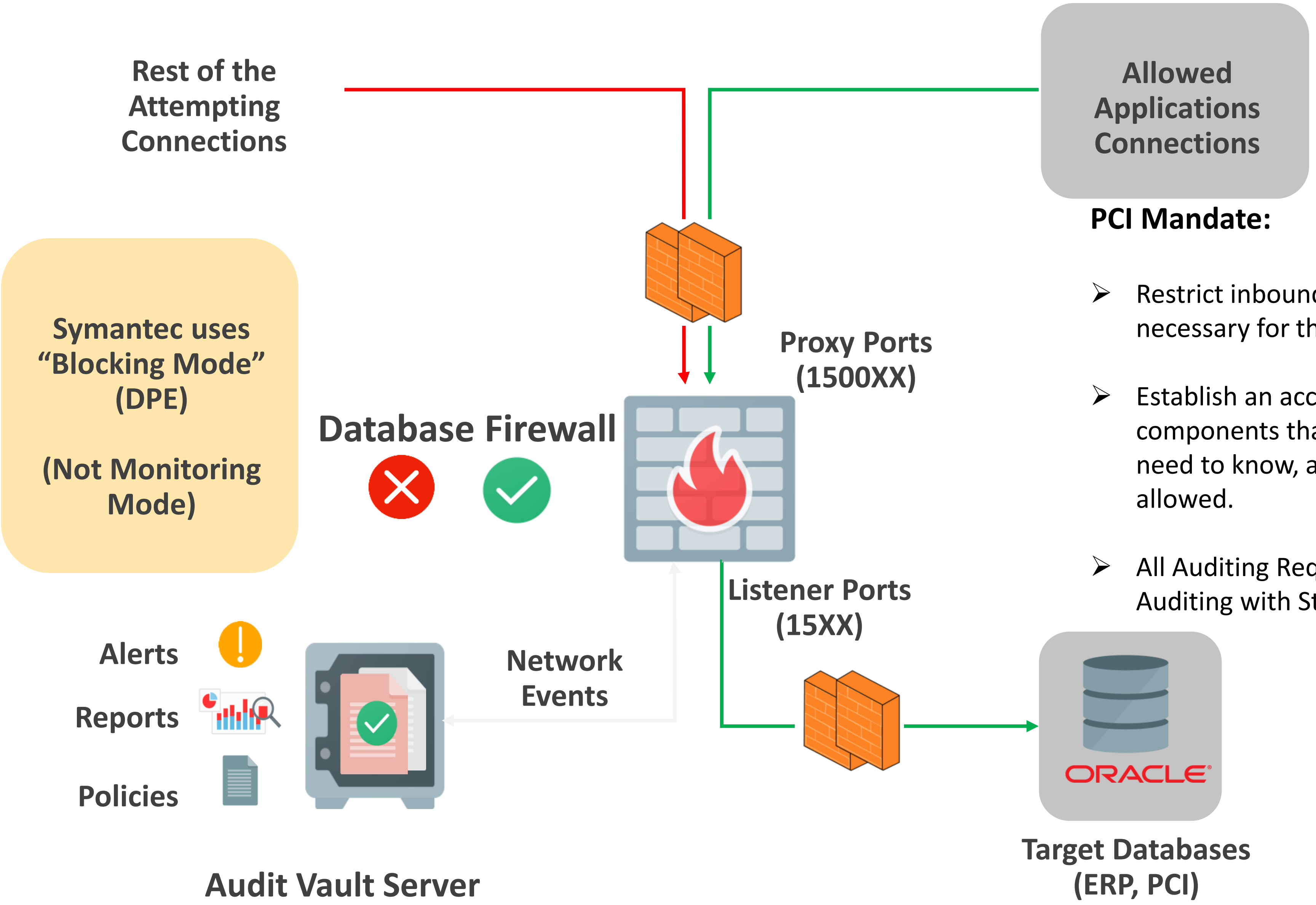
Centralize logging/Audit solution

Alerting & Monitoring

Reporting

Protecting Audit Data

Symantec's AVDF Setup



Rest of the Attempting Connections

Allowed Applications Connections

Symantec uses "Blocking Mode" (DPE)

(Not Monitoring Mode)

Database Firewall

Proxy Ports (1500XX)

Listener Ports (15XX)

Network Events

Alerts

Reports

Policies

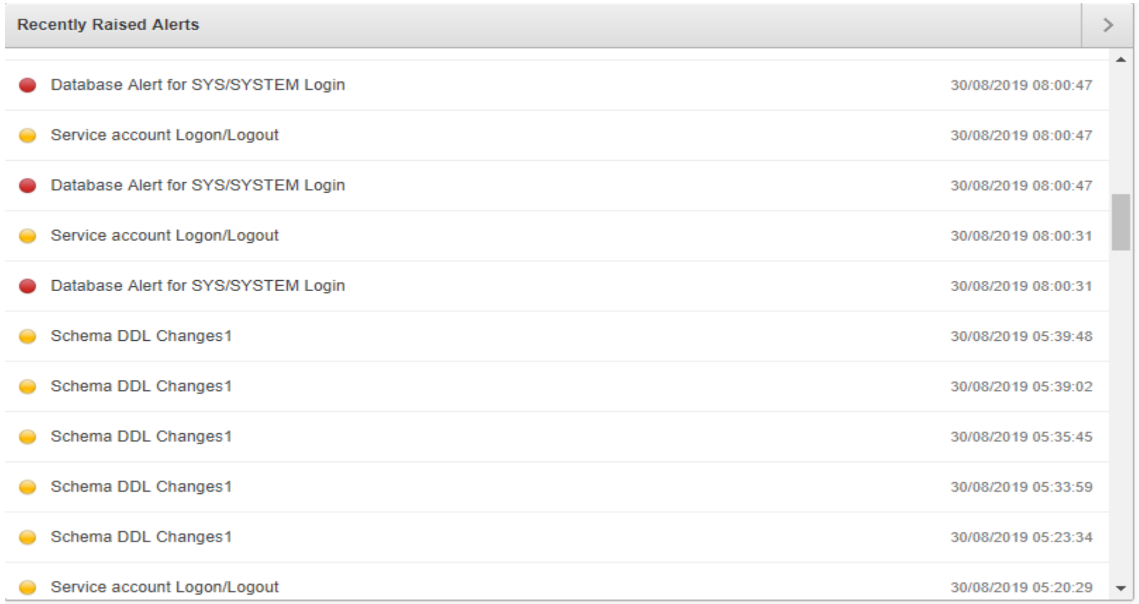
Audit Vault Server

Target Databases (ERP, PCI)

PCI Mandate:

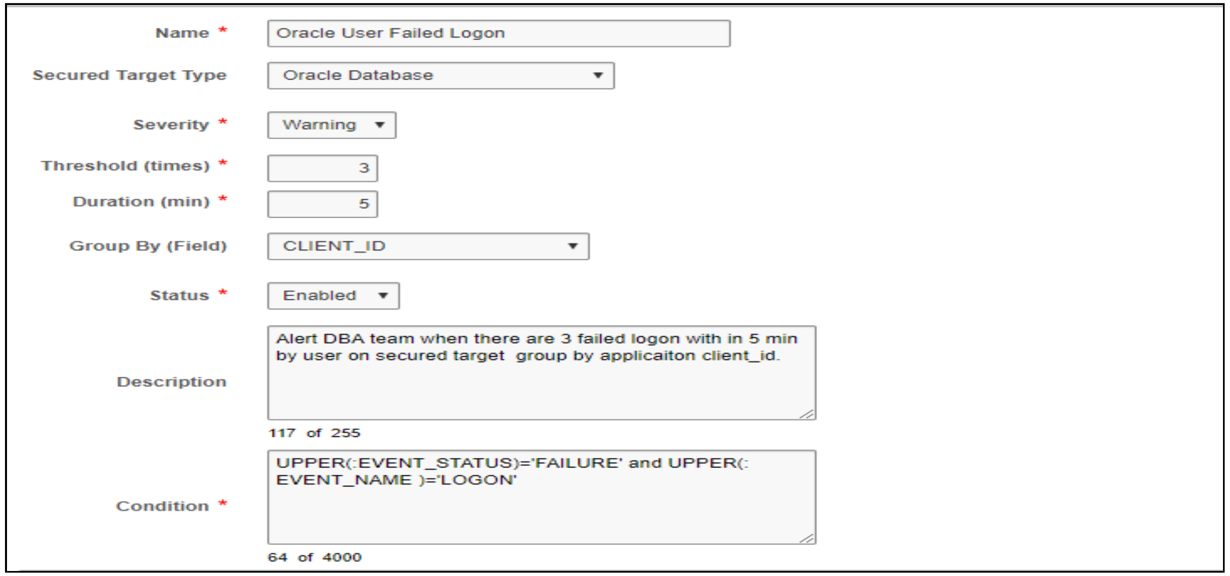
- Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
- Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
- All Auditing Requirements like SYS, Object, Login etc. Auditing with Status.

Powerful Alerting & Dashboard For Holistic View



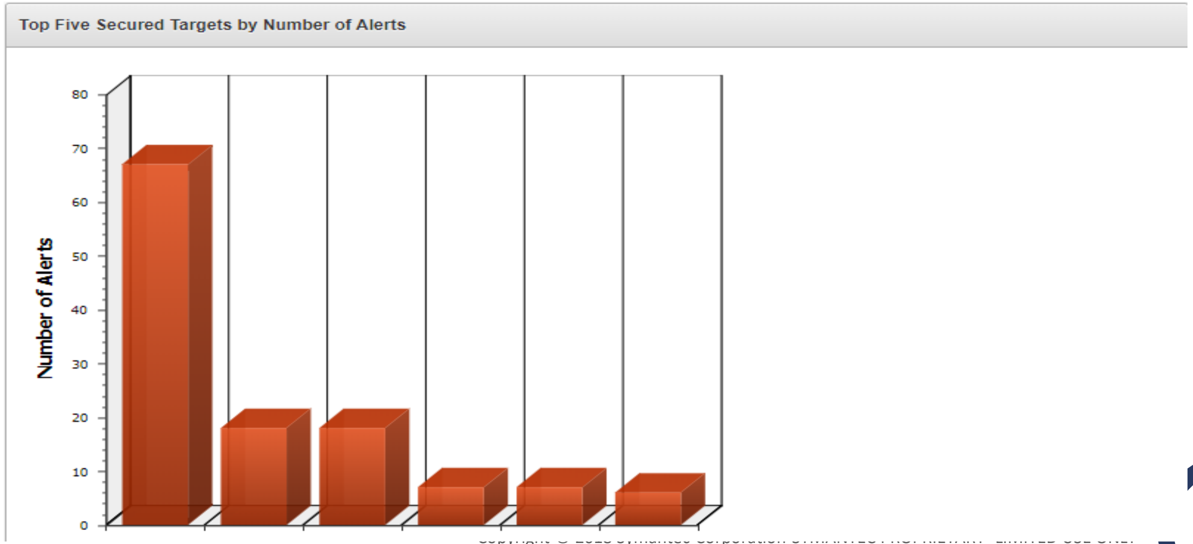
Recently Raised Alerts

●	Database Alert for SYS/SYSTEM Login	30/08/2019 08:00:47
●	Service account Logon/Logout	30/08/2019 08:00:47
●	Database Alert for SYS/SYSTEM Login	30/08/2019 08:00:47
●	Service account Logon/Logout	30/08/2019 08:00:31
●	Database Alert for SYS/SYSTEM Login	30/08/2019 08:00:31
●	Schema DDL Changes1	30/08/2019 05:39:48
●	Schema DDL Changes1	30/08/2019 05:39:02
●	Schema DDL Changes1	30/08/2019 05:35:45
●	Schema DDL Changes1	30/08/2019 05:33:59
●	Schema DDL Changes1	30/08/2019 05:23:34
●	Service account Logon/Logout	30/08/2019 05:20:29



Name *	Oracle User Failed Logon
Secured Target Type	Oracle Database
Severity *	Warning
Threshold (times) *	3
Duration (min) *	5
Group By (Field)	CLIENT_ID
Status *	Enabled
Description	Alert DBA team when there are 3 failed logon with in 5 min by user on secured target group by applicaiton client_id. 117 of 255
Condition *	UPPER(:EVENT_STATUS)='FAILURE' and UPPER(:EVENT_NAME)='LOGON' 64 of 4000

- Powerful Alerting Engine
- Flexible Conditional Alerting
- Alerting Via Email
- Real-Time Monitoring & Alerting
- Multi-Event alerts with threshold and time duration.
- Holistic view using Dashboard & Drill-down

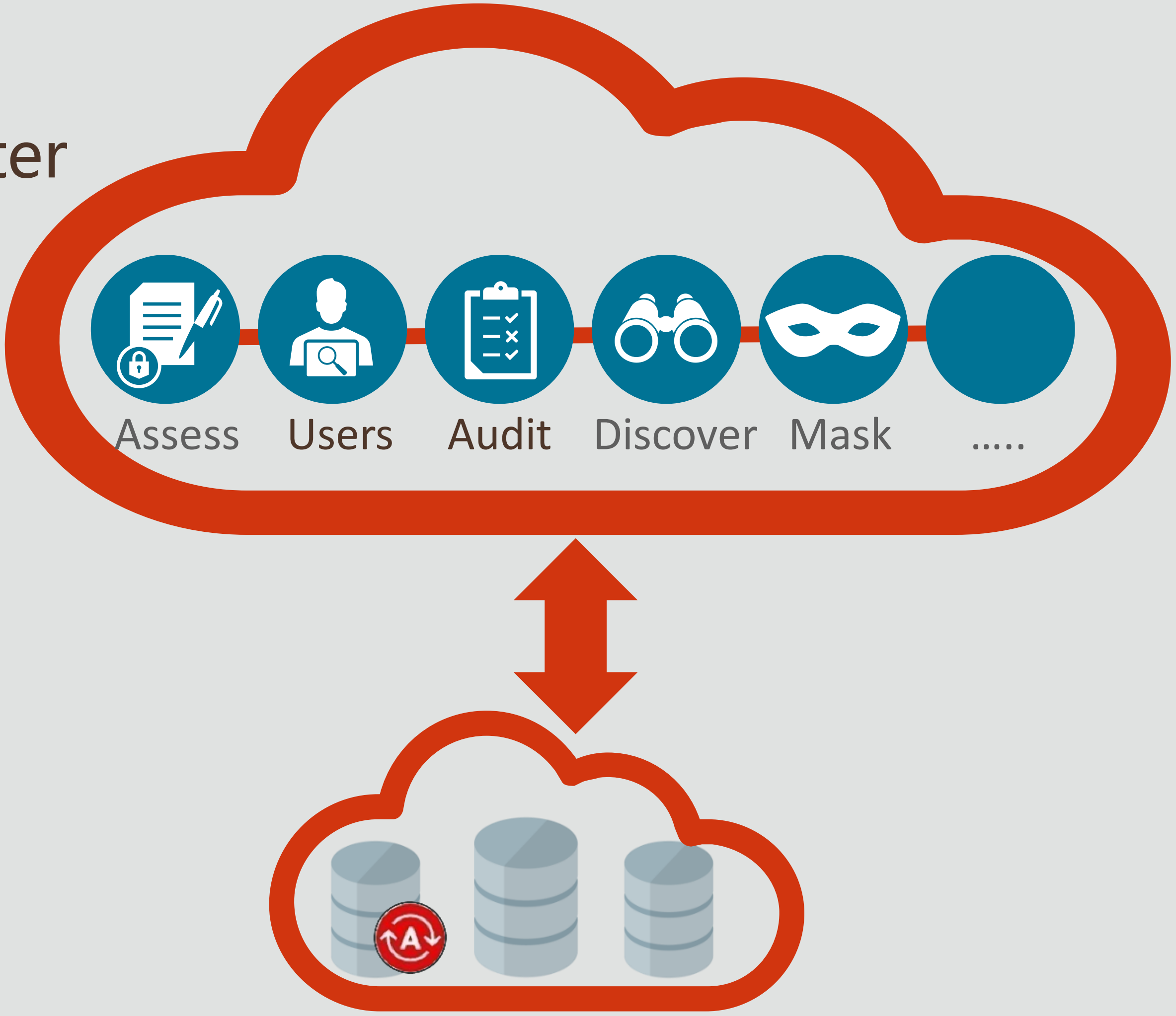


Top Five Secured Targets by Number of Alerts

Oracle Data Safe

Security for Cloud Databases

- Unified Database Security Control Center
  - Security Assessment
  - User Assessment
  - User Activity Auditing
  - Sensitive Data Discovery
  - Sensitive Data Masking
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed

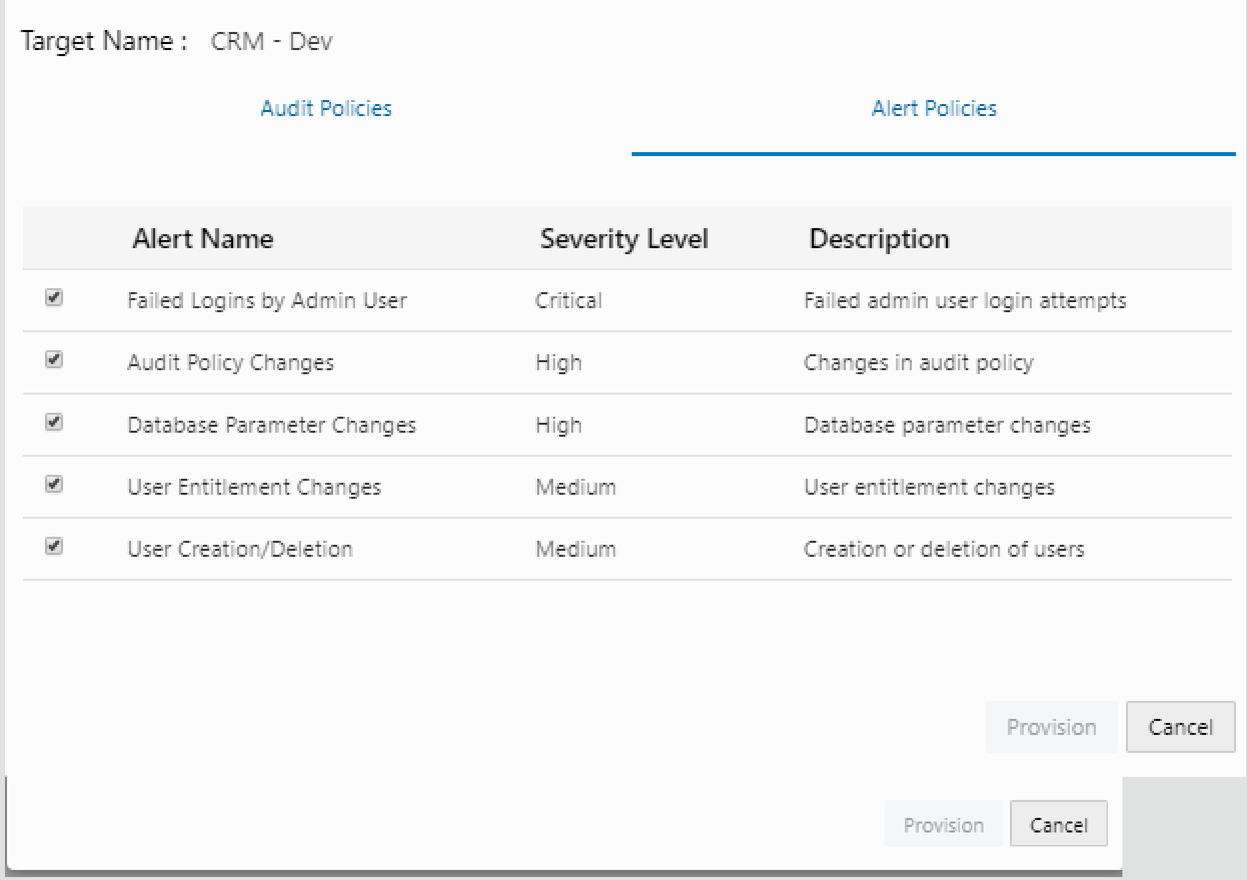


Databases in Oracle Cloud

User Activity Auditing

Track user actions and streamline auditing with robust reporting

- Provision audit, compliance, and alert policies
- Collect audit data from databases, and track sensitive operations
- Audit Reports
  - Interactive reports for forensics
  - Summary and detailed reports
  - PDF reports for compliance



Target Name : CRM - Dev

	Alert Name	Severity Level	Description
☑	Failed Logins by Admin User	Critical	Failed admin user login attempts
☑	Audit Policy Changes	High	Changes in audit policy
☑	Database Parameter Changes	High	Database parameter changes
☑	User Entitlement Changes	Medium	User entitlement changes
☑	User Creation/Deletion	Medium	Creation or deletion of users

Summary

- Database Activity Monitoring is key to identifying breaches and responding quickly
- Both database auditing and network monitoring are important components of Database Activity Monitoring
- Database Activity Monitoring solutions:
  - Oracle Audit Vault and Database Firewall (AVDF)
  - Oracle Data Safe

Securing the Oracle Database

Third Edition

Oracle Database Security Team

URL:
https://oracle.com/securingthedatabase

Database Security Office Hours

Direct line into Database Security PM

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

Ask Tom
Database Security

Thank You

Ashok Swaminathan
Oracle Corporation
Ashok.Swaminathan@oracle.com

Ram Subramanian
Symantec Corporation
Ram_Subramanian1@symantec.com