AV/DF
Advanced Security Option

Paul White
Database Security Specialist

Safe Harbor Statement

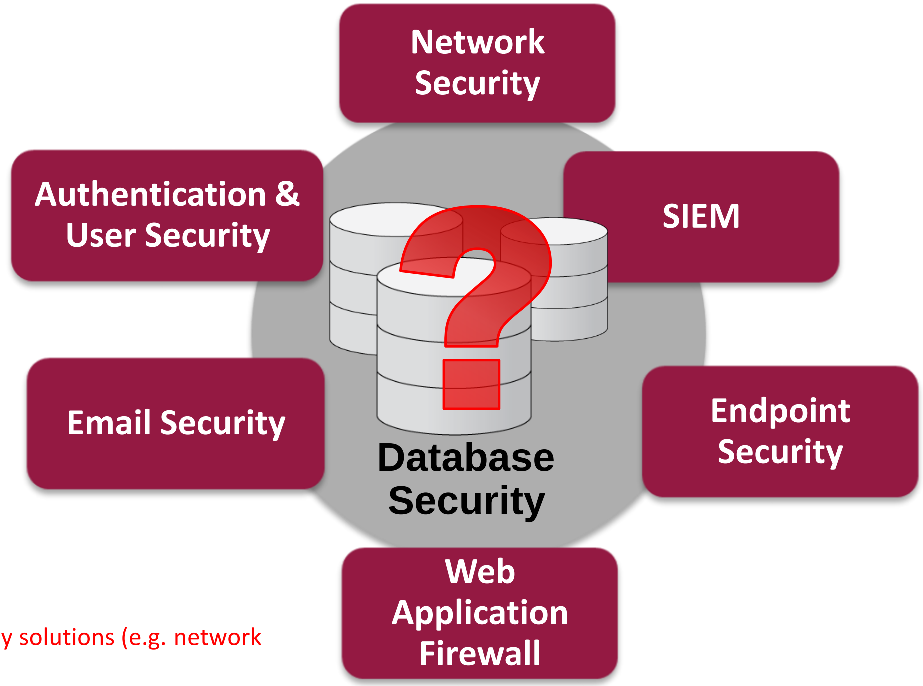
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development,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

Why Are Databases So Vulnerable?

80% of IT Security Programs Don’t Address Database Security

Forrester Research

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

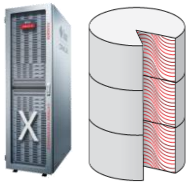


Less than 1% of database breaches are detected or prevented using perimeter security solutions (e.g. network firewalls, IDS, anti-malware)

Oracle Database Security Solutions

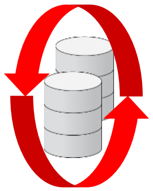
PREVENTION	DETECTION	ADMINISTRATION
Encryption & Redaction	Activity Monitoring	Privilege Analysis
Subsetting and Data Masking	Database Firewall	Sensitive Data Discovery
Privileged User Controls	Auditing and Reporting	Encryption Keys and Certificates

ORACLE



ORACLE

ORACLE



ORACLE®

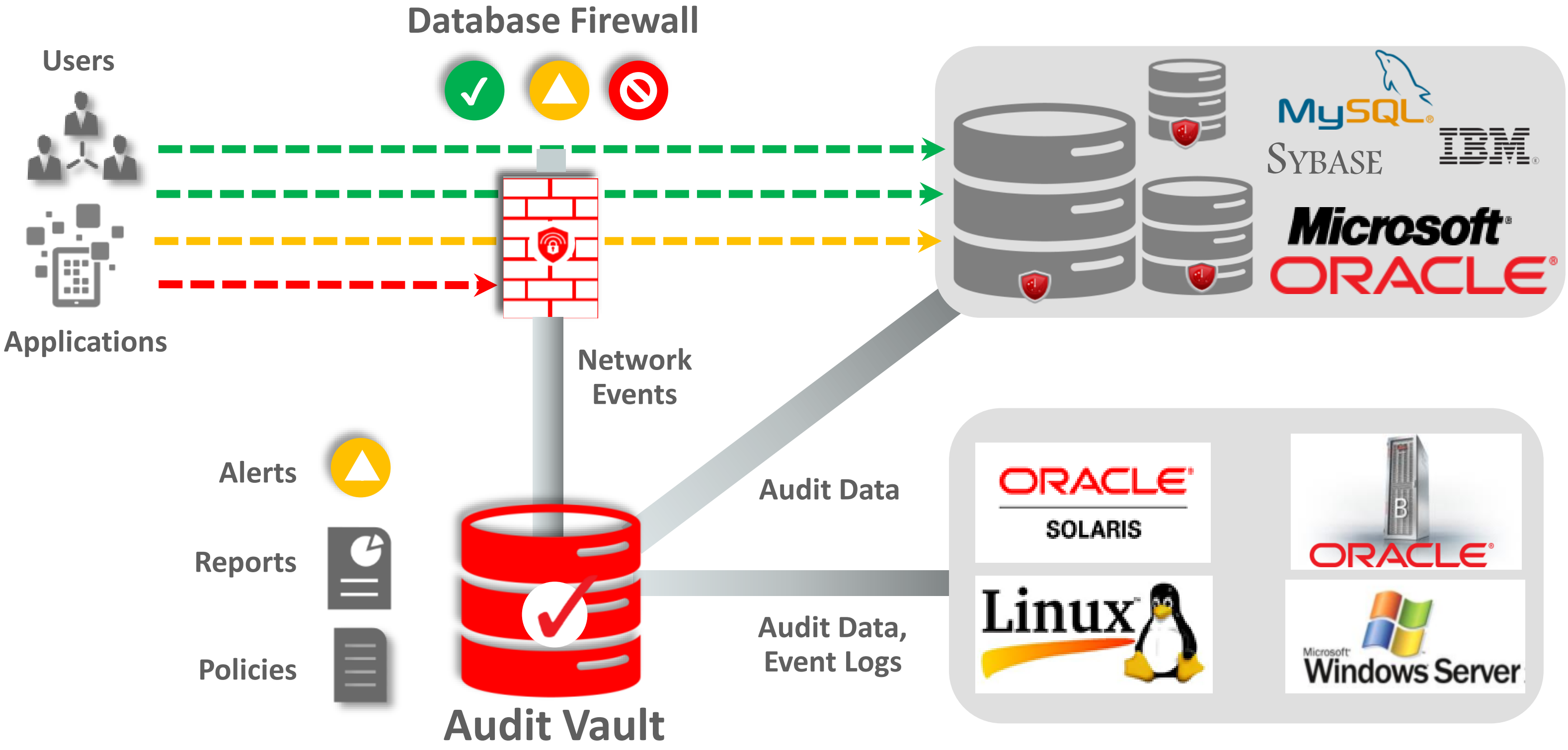
Database Security

Oracle Audit Vault and Database Firewall

Efficient Database Auditing Policy

- Be selective in what you audit – target privileged users, sensitive tables, privileged operations, secure configurations
- Build on default audit policy configurations
- For Oracle audit ‘by access’ to make sure IP addresses are recorded
- Consider using remote agent deployment for table trail types

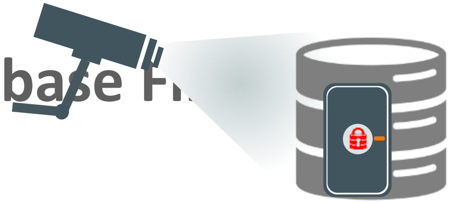
Audit, Monitor, and Detect



PRELIMINARY DRAFT

Database Activity Auditing and Monitoring

Flexible security with Oracle Audit Vault and Database Fi

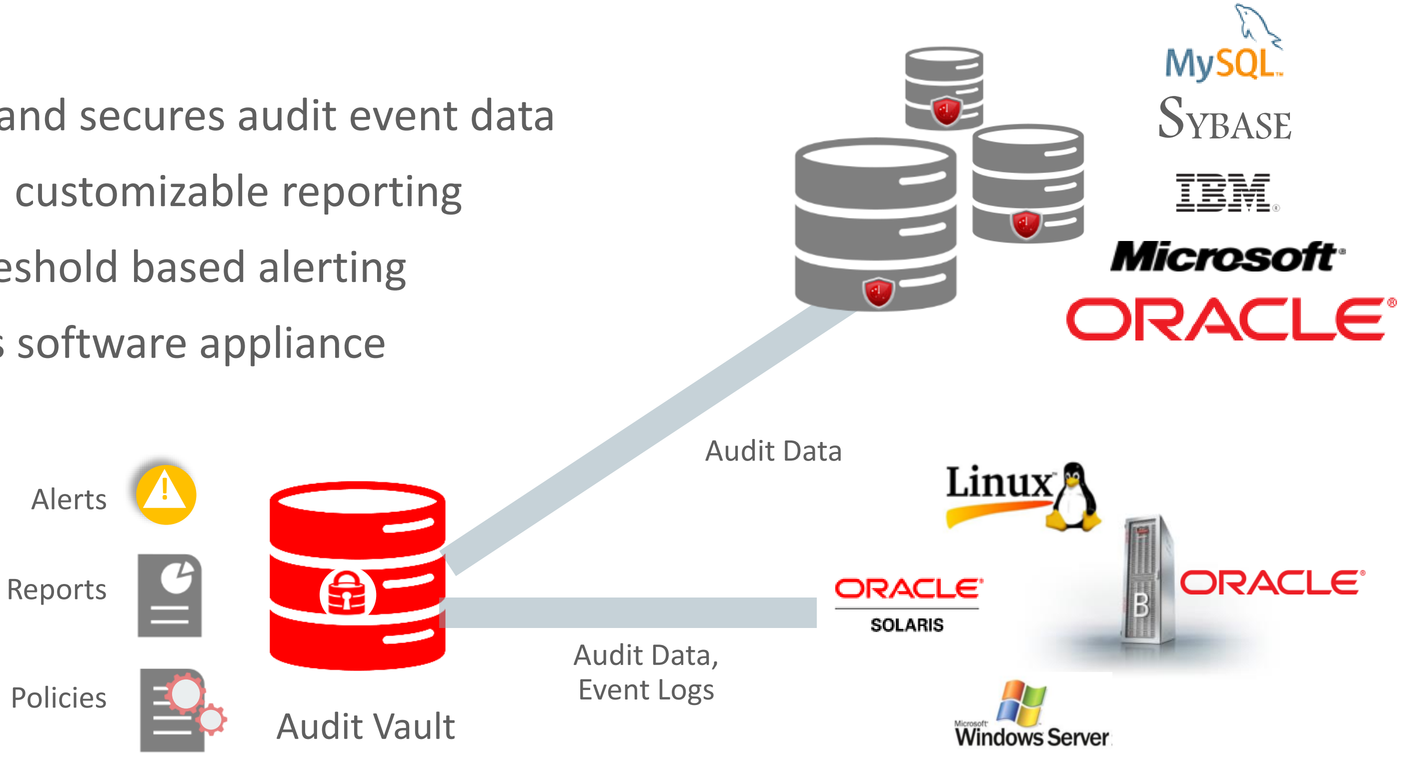


	Monitoring (Database Firewalls)	**Auditing (Audit Vault Agents)**
Information	Who, what, where, when	Who, what, where, when Before/After values Full execution and application context
Pathways	Network	All: stored procedures, direct connections, scheduled jobs, operational activities
Impact on database	Completely independent, negligible performance impact	Requires native database auditing, minimal performance impact (<5%)
Purpose	Prevent SQL-injections and other unauthorized activity, enforce corporate data security policy	Ensure regulatory compliance, provide guaranteed audit trail to enable control

Audit Vault

Audit data consolidation

- Consolidates and secures audit event data
- Extensive and customizable reporting
- Powerful, threshold based alerting
- Distributed as software appliance

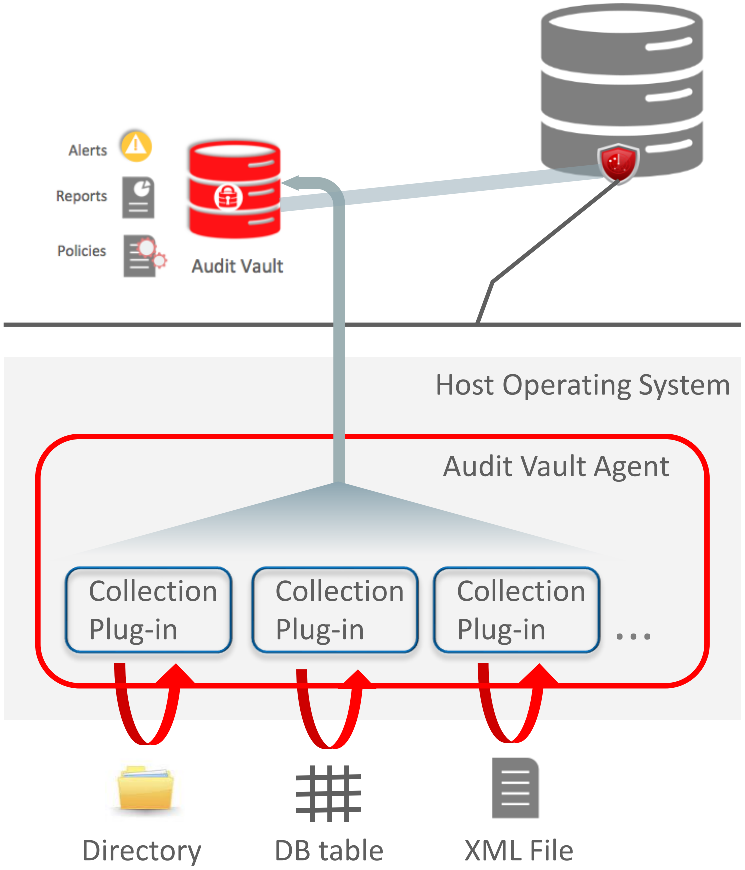


PRELIMINARY DRAFT

Audit Vault Agent

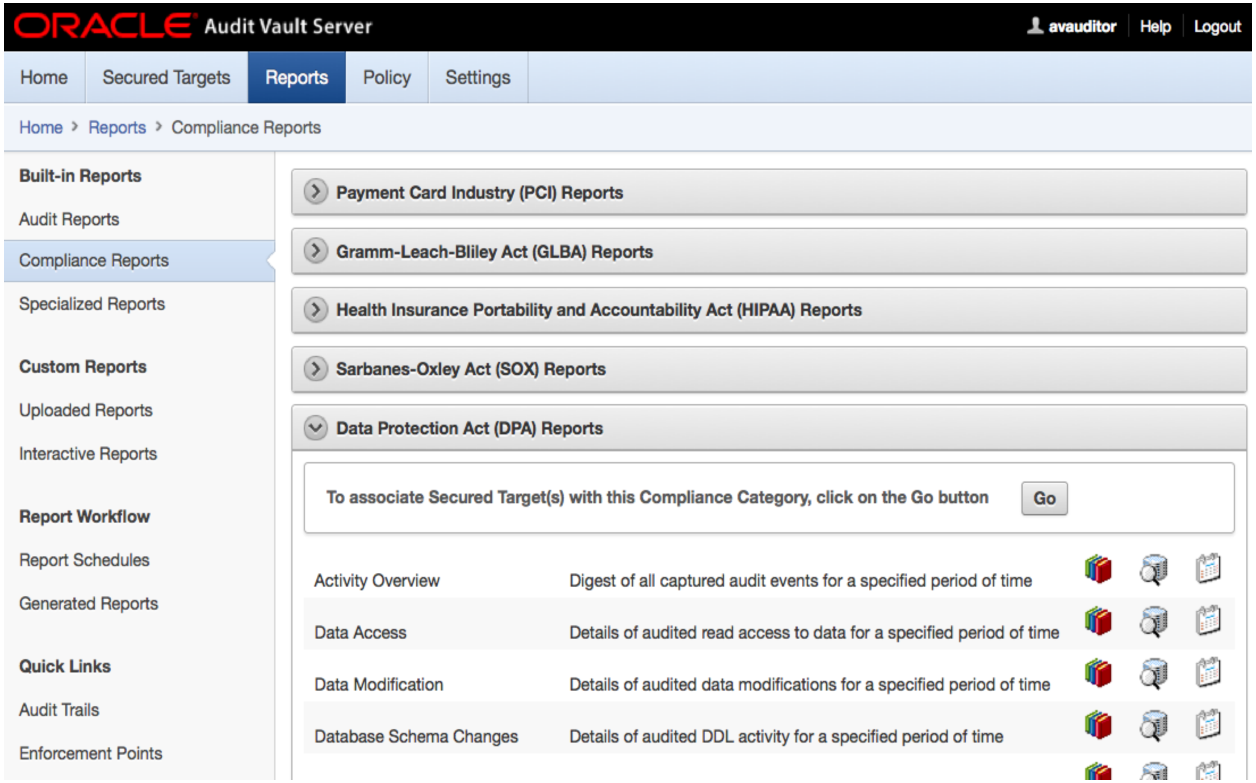
Efficient audit data acquisition

- Retrieves data from multiple native audit trails on the host: database, operating system, directory, custom
- Data immediately sent via encrypted channel to Audit Vault Server repository
- Agent automatically managed and updated by Audit Vault Server
- Easy to create collection plug-ins for custom audit sources



Extensive and Customizable Reporting

- Predefined reports
- Interactive browsing
- Build custom reports
- Report scheduling and notification
- Report attestation



Home › Reports › Compliance Reports

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

Payment Card Industry (PCI) Reports

Gramm-Leach-Bliley Act (GLBA) Reports

Health Insurance Portability and Accountability Act (HIPAA) Reports

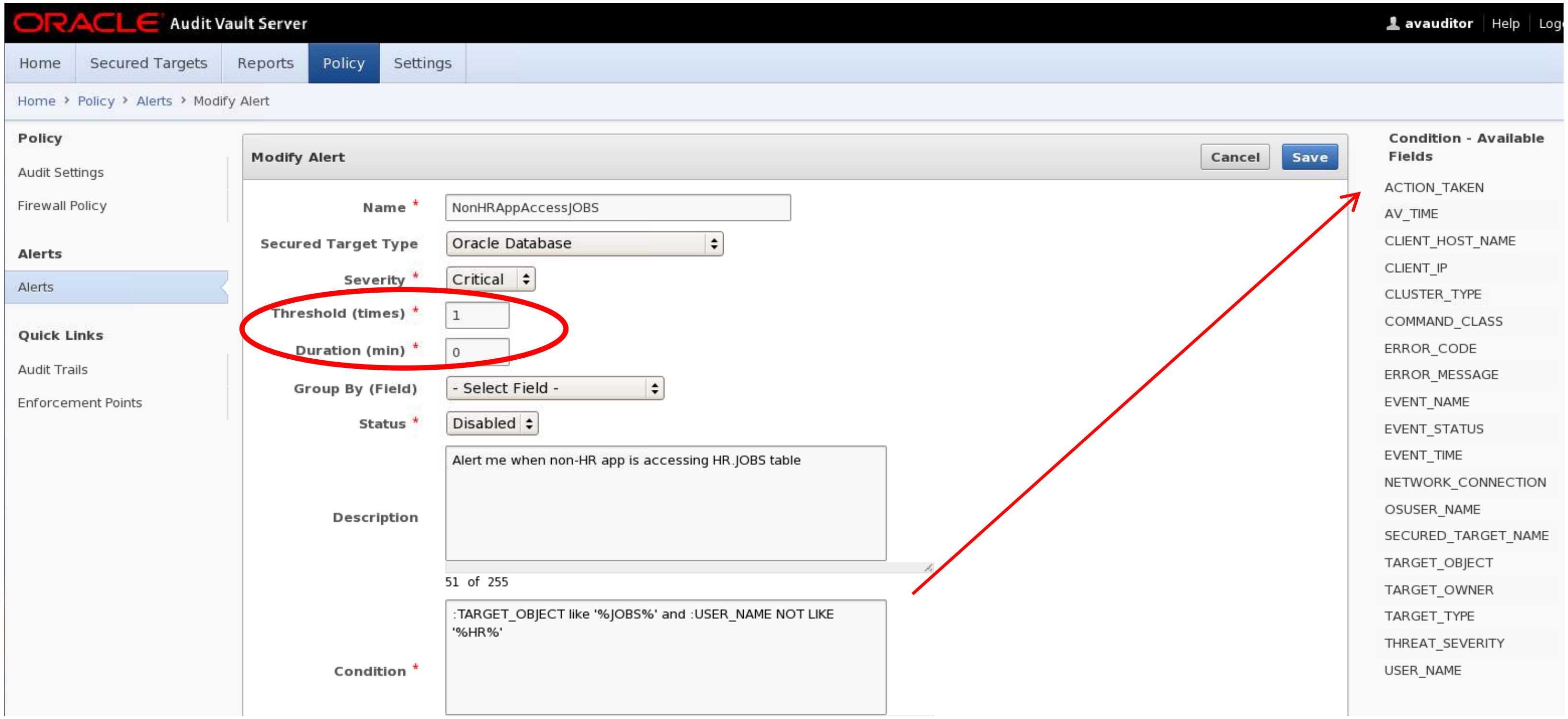
Sarbanes-Oxley Act (SOX) Reports

Data Protection Act (DPA) Reports

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

Activity Overview	Digest of all captured audit events for a specified period of time
Data Access	Details of audited read access to data for a specified period of time
Data Modification	Details of audited data modifications for a specified period of time
Database Schema Changes	Details of audited DDL activity for a specified period of time

Powerful Alerting



Name * NonHRAppAccessJOBS

Secured Target Type Oracle Database

Severity * Critical

Threshold (times) * 1

Duration (min) * 0

Group By (Field) - Select Field -

Status * Disabled

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

51 of 255

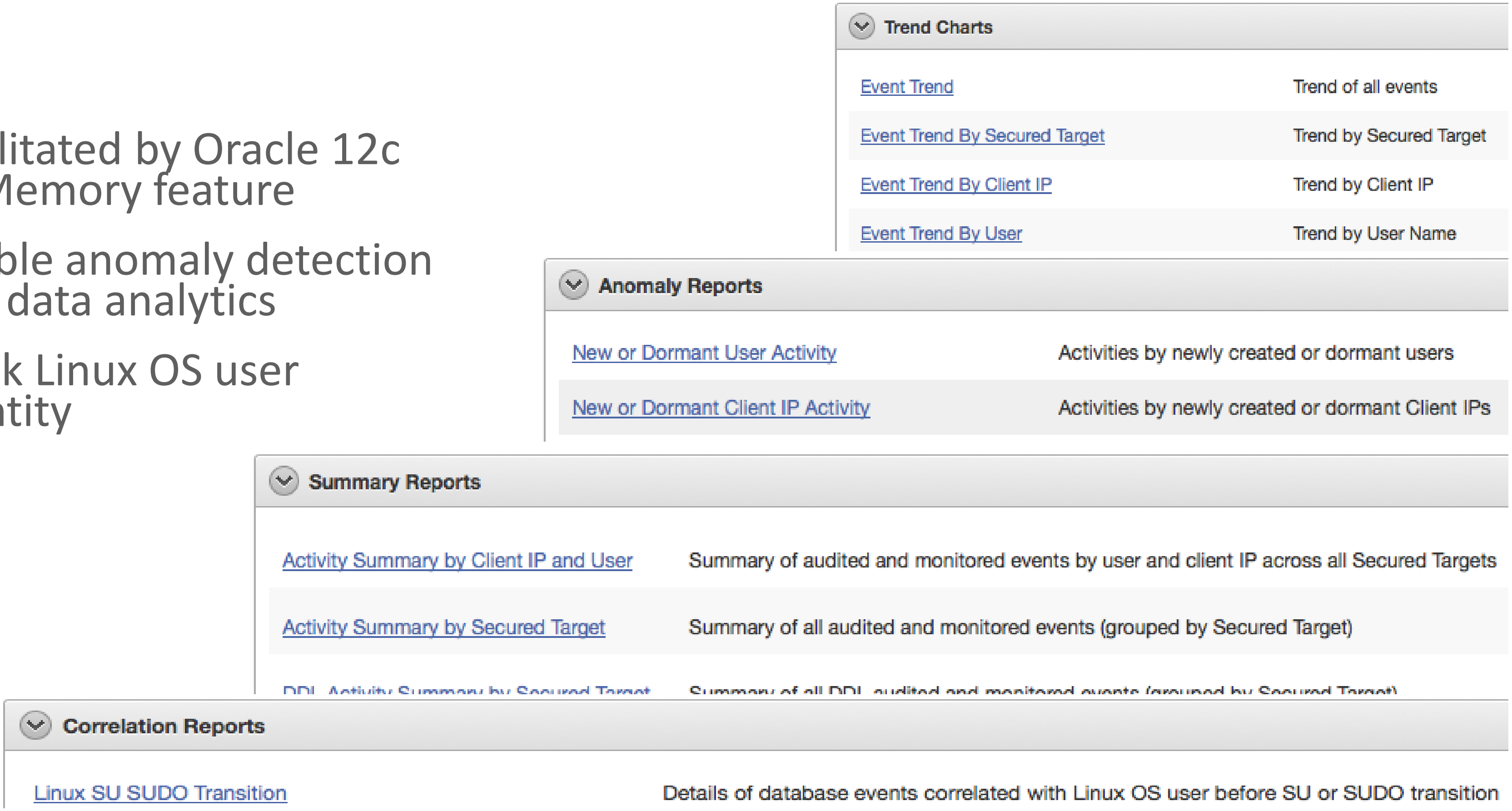
Condition * :TARGET_OBJECT like '%JOBS%' and :USER_NAME NOT LIKE '%HR%'

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

New in AVDF 12.2: Trending and Anomaly Reports

- Facilitated by Oracle 12c In-Memory feature
- Enable anomaly detection and data analytics
- Track Linux OS user identity



Trend Charts

Event Trend	Trend of all events
Event Trend By Secured Target	Trend by Secured Target
Event Trend By Client IP	Trend by Client IP
Event Trend By User	Trend by User Name

Anomaly Reports

New or Dormant User Activity	Activities by newly created or dormant users
New or Dormant Client IP Activity	Activities by newly created or dormant Client IPs

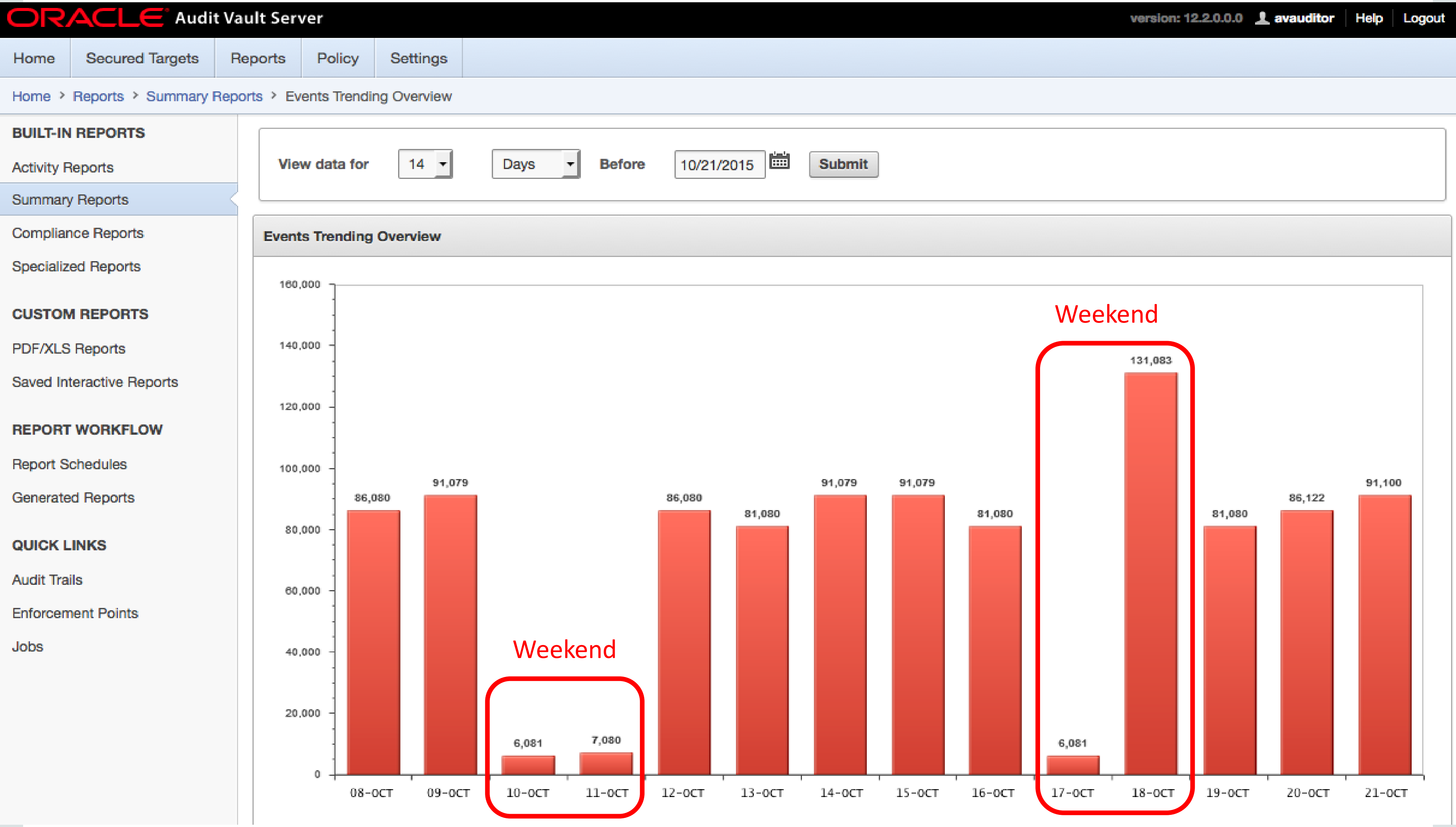
Summary Reports

Activity Summary by Client IP and User	Summary of audited and monitored events by user and client IP across all Secured Targets
Activity Summary by Secured Target	Summary of all audited and monitored events (grouped by Secured Target)
DDL Activity Summary by Secured Target	Summary of all DDL audited and monitored events (grouped by Secured Target)

Correlation Reports

Linux SU SUDO Transition	Details of database events correlated with Linux OS user before SU or SUDO transition

Trending Reports

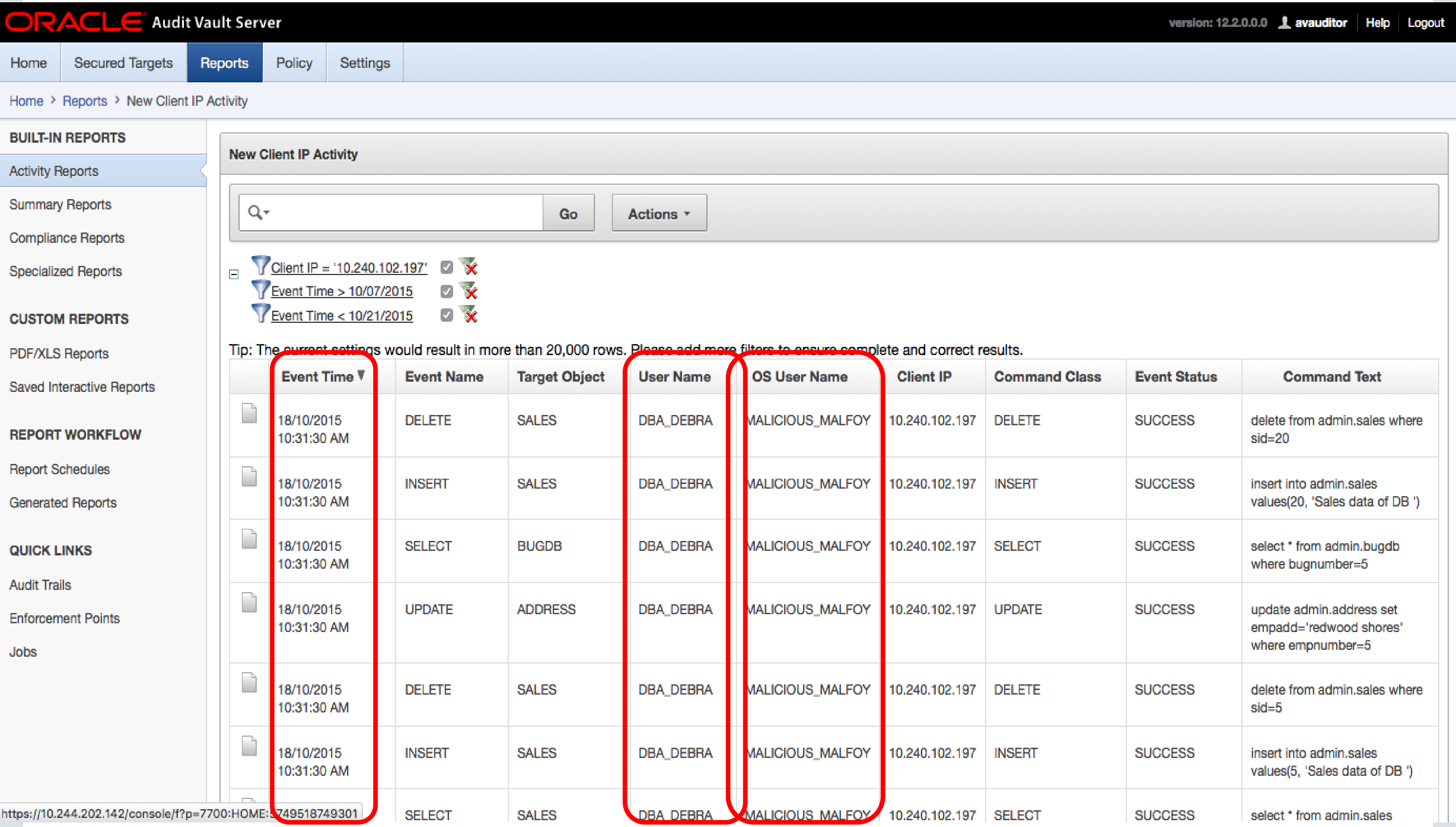


View data for 14 Days Before 10/21/2015

Weekend

Weekend

Anomaly Reports



New Client IP Activity

Client IP = '10.240.102.197' ☑

Event Time > 10/07/2015 ☑

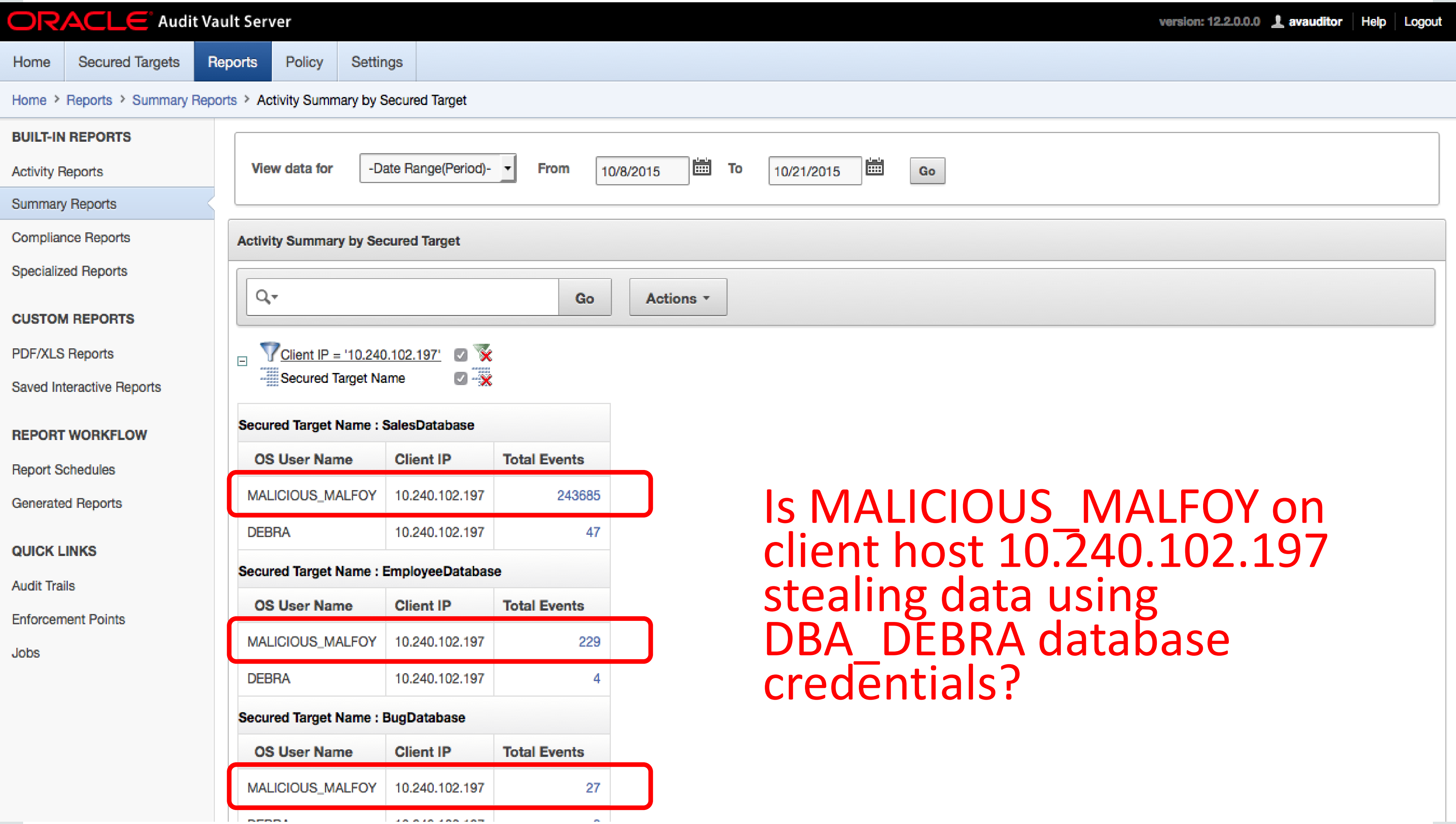
Event Time < 10/21/2015 ☑

Tip: The current settings would result in more than 20,000 rows. Please add more filters to ensure complete and correct results.

	Event Time	Event Name	Target Object	User Name	OS User Name	Client IP	Command Class	Event Status	Command Text
	18/10/2015 10:31:30 AM	DELETE	SALES	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	DELETE	SUCCESS	delete from admin.sales where sid=20
	18/10/2015 10:31:30 AM	INSERT	SALES	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	INSERT	SUCCESS	insert into admin.sales values(20, 'Sales data of DB ')
	18/10/2015 10:31:30 AM	SELECT	BUGDB	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	SELECT	SUCCESS	select * from admin.bugdb where bugnumber=5
	18/10/2015 10:31:30 AM	UPDATE	ADDRESS	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	UPDATE	SUCCESS	update admin.address set empadd='redwood shores' where empnumber=5
	18/10/2015 10:31:30 AM	DELETE	SALES	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	DELETE	SUCCESS	delete from admin.sales where sid=5
	18/10/2015 10:31:30 AM	INSERT	SALES	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	INSERT	SUCCESS	insert into admin.sales values(5, 'Sales data of DB ')
		SELECT	SALES	DBA_DEBRA	MALICIOUS_MALFOY	10.240.102.197	SELECT	SUCCESS	select * from admin.sales

https://10.244.202.142/console/f?p=7700:HOME:5749518749301

Summary Report



Home > Reports > Summary Reports > Activity Summary by Secured Target

View data for: -Date Range(Period)- From: 10/8/2015 To: 10/21/2015

Activity Summary by Secured Target

Client IP = '10.240.102.197' ☑

Secured Target Name ☑

Secured Target Name : SalesDatabase

OS User Name	Client IP	Total Events
MALICIOUS_MALFOY	10.240.102.197	243685
DEBRA	10.240.102.197	47

Secured Target Name : EmployeeDatabase

OS User Name	Client IP	Total Events
MALICIOUS_MALFOY	10.240.102.197	229
DEBRA	10.240.102.197	4

Secured Target Name : BugDatabase

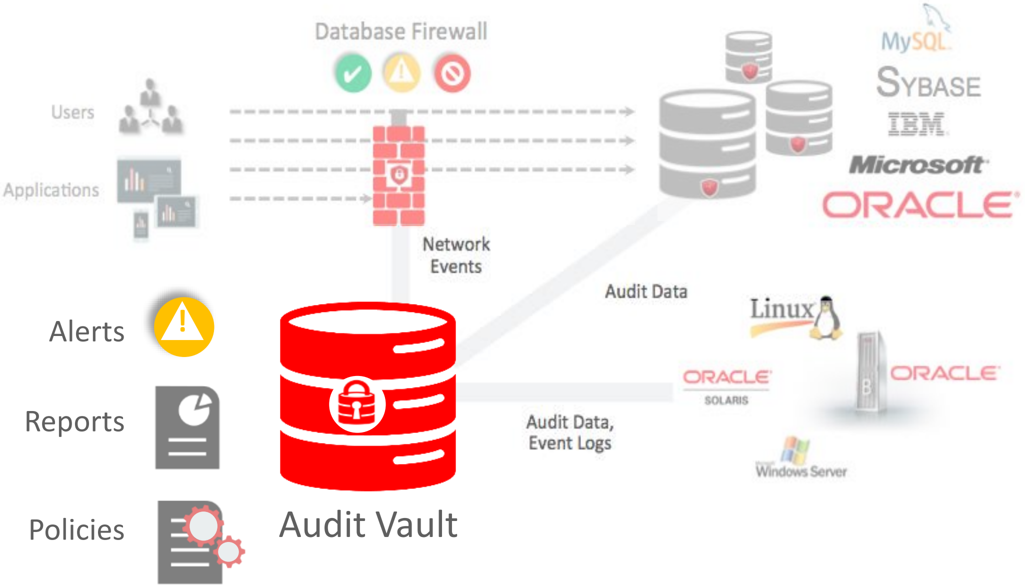
OS User Name	Client IP	Total Events
MALICIOUS_MALFOY	10.240.102.197	27
DEBRA	10.240.102.197	[illegible]

Is MALICIOUS_MALFOY on client host 10.240.102.197 stealing data using DBA_DEBRA database credentials?

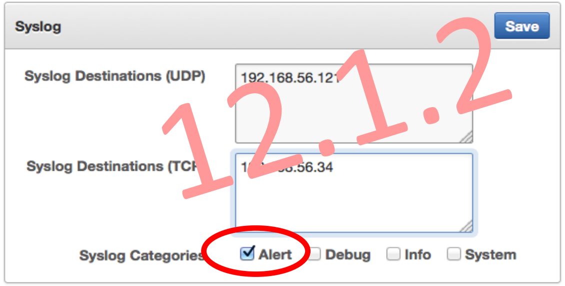
New in AVDF 12.2: Strengthened Data Security

Event data always protected

	12.1.2	12.2
Data encryption in transit	✓	✓
Repository protection with Database Vault	✓	✓
Data encryption (TDE) in Audit Vault Repository		✓
Externally signed UI certificates		✓



New in AVDF 12.2: Custom Syslog Alert Templates



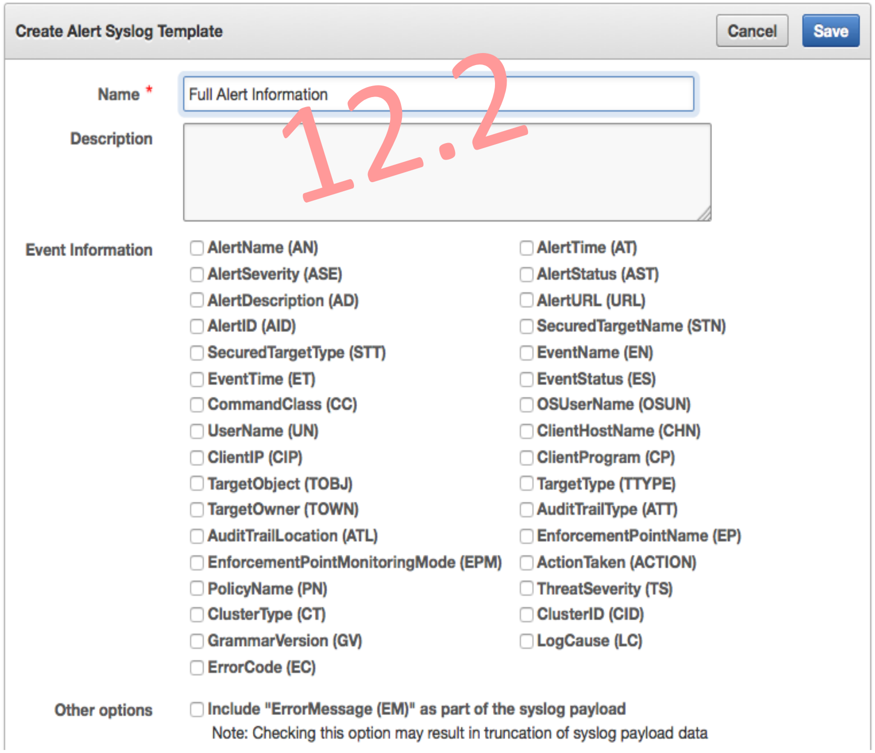
Syslog — Save

Syslog Destinations (UDP): 192.168.56.121

Syslog Destinations (TCP): 1[illegible].56.34

Syslog Categories: ☑ Alert □ Debug □ Info □ System

```
<10>Jan  7 13:59:40 avs00161eb81587 logger:
[AVDFAlert@111 name="Alert_FailLogOn"
severity="Critical"
url="https://10.244.163.91/console/f?p=7700:33:
::NO::P33_ALERT_ID:1" time="2014-01-
07T13:59:40.153746Z" target="avsource"
user="INVALID" desc=" "]
```



Create Alert Syslog Template — Cancel — Save

Name *: Full Alert Information

Description:

Event Information:

□ AlertName (AN)
□ AlertSeverity (ASE)
□ AlertDescription (AD)
□ AlertID (AID)
□ SecuredTargetType (STT)
□ EventTime (ET)
□ CommandClass (CC)
□ UserName (UN)
□ ClientIP (CIP)
□ TargetObject (TOBJ)
□ TargetOwner (TOWN)
□ AuditTrailLocation (ATL)
□ EnforcementPointMonitoringMode (EPM)
□ PolicyName (PN)
□ ClusterType (CT)
□ GrammarVersion (GV)
□ ErrorCode (EC)
□ AlertTime (AT)
□ AlertStatus (AST)
□ AlertURL (URL)
□ SecuredTargetName (STN)
□ EventName (EN)
□ EventStatus (ES)
□ OSUserName (OSUN)
□ ClientHostName (CHN)
□ ClientProgram (CP)
□ TargetType (TTYPE)
□ AuditTrailType (ATT)
□ EnforcementPointName (EP)
□ ActionTaken (ACTION)
□ ThreatSeverity (TS)
□ ClusterID (CID)
□ LogCause (LC)

Other options: □ Include "ErrorMessage (EM)" as part of the syslog payload
Note: Checking this option may result in truncation of syslog payload data

New in AVDF 12.2: Extended Platform Support

New platform	New functionality added in 12.2
SQL Server 2014	Collection Plug-in, Database Firewall support
Windows Server 2012 & 2012 R2	Collection Plug-in, Audit Vault Agent installation
AIX OS 6.1,…,7.1	Collection Plug-in, (Audit Vault Agent installation supported from 12.1.1)
Oracle Linux OS 6.5,…,7	Collection Plug-in, Audit Vault Agent installation
DB2 LUW 10.5	Collection Plug-in, Database Firewall support

See product documentation for full list of supported platforms

SQL Injection

#1 Risks on **SANS TOP 25 Most Dangerous Software Errors**

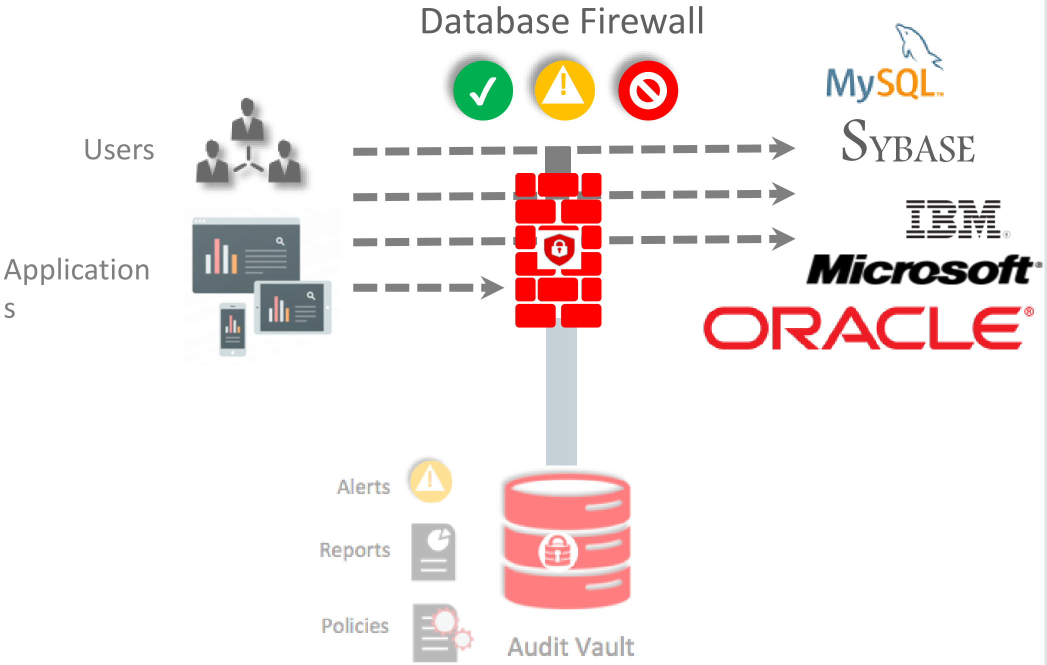
Threat Agent	• Anyone who can sent untrusted data to the database including external users, internal users, and administrators
Attack Vector	• EASY • Attacker sends text based attacks that exploit the uncleansed syntax
Impact	• SEVERE • Injection can result in data loss or corruption, lack of accountability or complete host takeover

ORACLE

Database Firewall

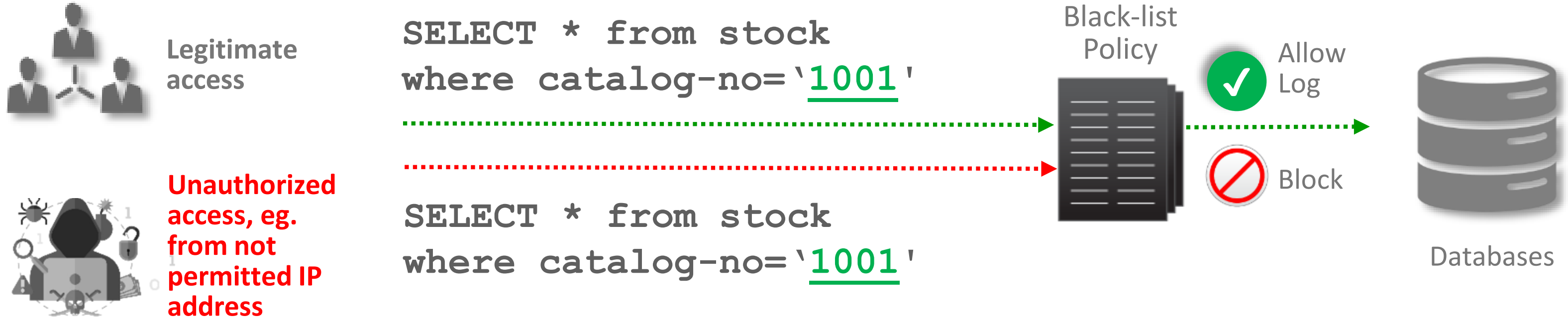
First line of defense

- Application layer firewall monitors SQL activity on network
- Grammar policy engine precisely identifies SQL statements
- Policy-based pass/log/alert/substitute/block
- Support both white-list and black-list security models
- Low latency, high availability and scalability



Enforcing access with black-list based policy

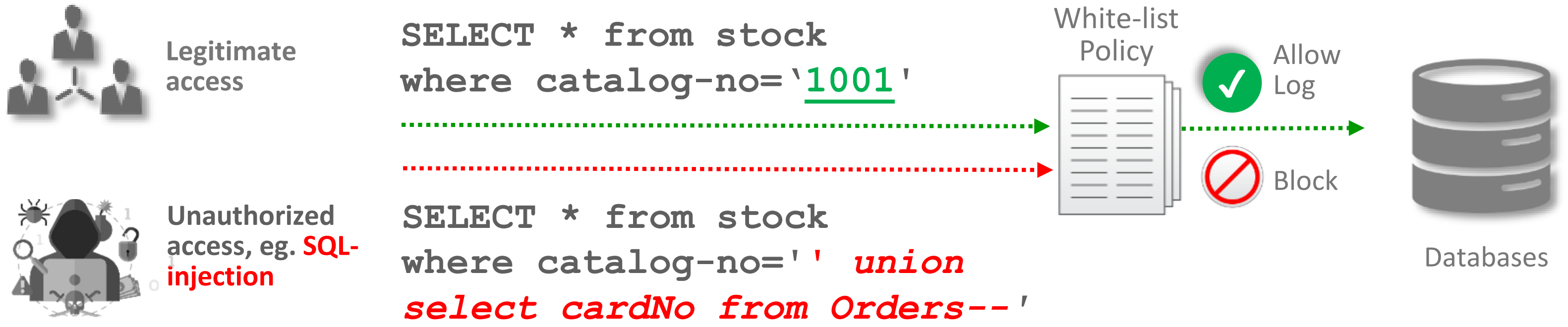
Database Firewall


Legitimate access
Unauthorized access, eg. from not permitted IP address
SELECT * from stock where catalog-no='1001'
SELECT * from stock where catalog-no='1001'
Black-list Policy
Allow
Log
Block
Databases

- Apply negative policy actions on session factors: IP address, application, database and OS user
- Block specific unauthorized SQL statements, users or object access

Anomaly detection and threat blocking with white-list based policy

Database Firewall



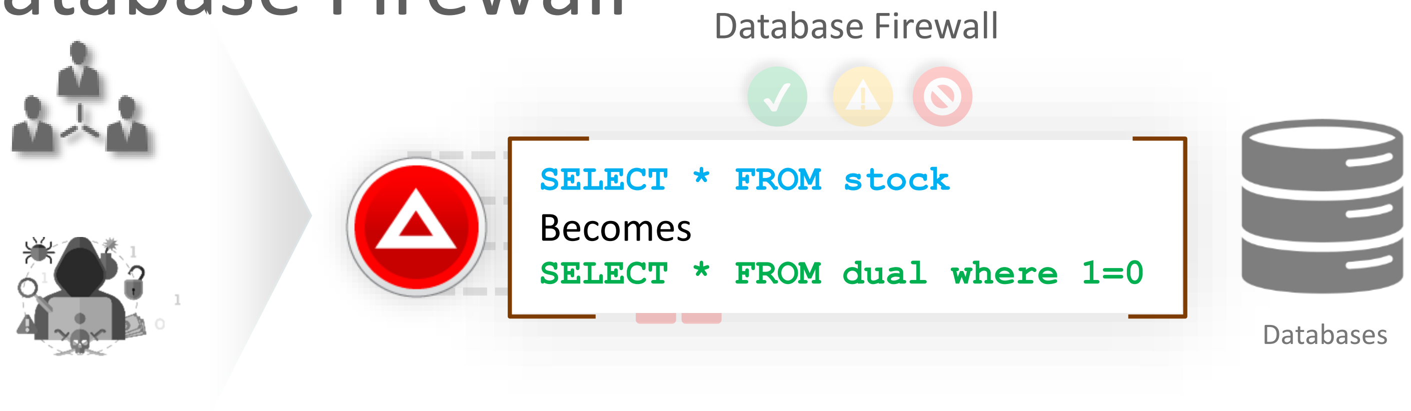
```
SELECT * from stock
where catalog-no=‘1001'
```

```
SELECT * from stock
where catalog-no='' union
select cardNo from Orders--'
```

- Accurately detect and block out-of-policy SQL statements
- Automatically create SQL activity profile of users and/or applications

Transparent blocking with statement substitution

Database Firewall



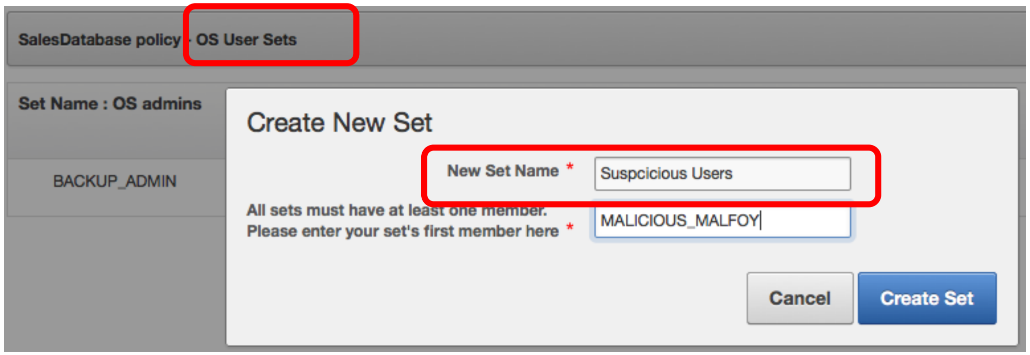
```
SELECT * FROM stock
Becomes
SELECT * FROM dual where 1=0
```

- Block unauthorized SQL statements by substituting with pre-defined innocuous SQL statement
- Preserve application-database connection while blocking

Database Firewall Policy Example

Policy Exception Rule

- OS User Set containing MALICIOUS_MALFOY user name
- IP Address Set containing the IP of MALICIOUS_MALFOY's workstation
- Policy rule with control action (next slide)



SalesDatabase policy - OS User Sets

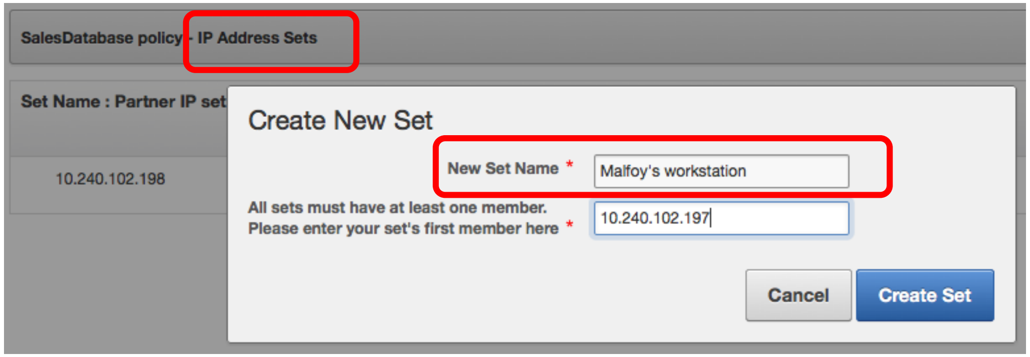
Set Name : OS admins

BACKUP_ADMIN

Create New Set

New Set Name * Suspcicious Users

All sets must have at least one member.
Please enter your set's first member here * MALICIOUS_MALFOY



SalesDatabase policy - IP Address Sets

Set Name : Partner IP set

10.240.102.198

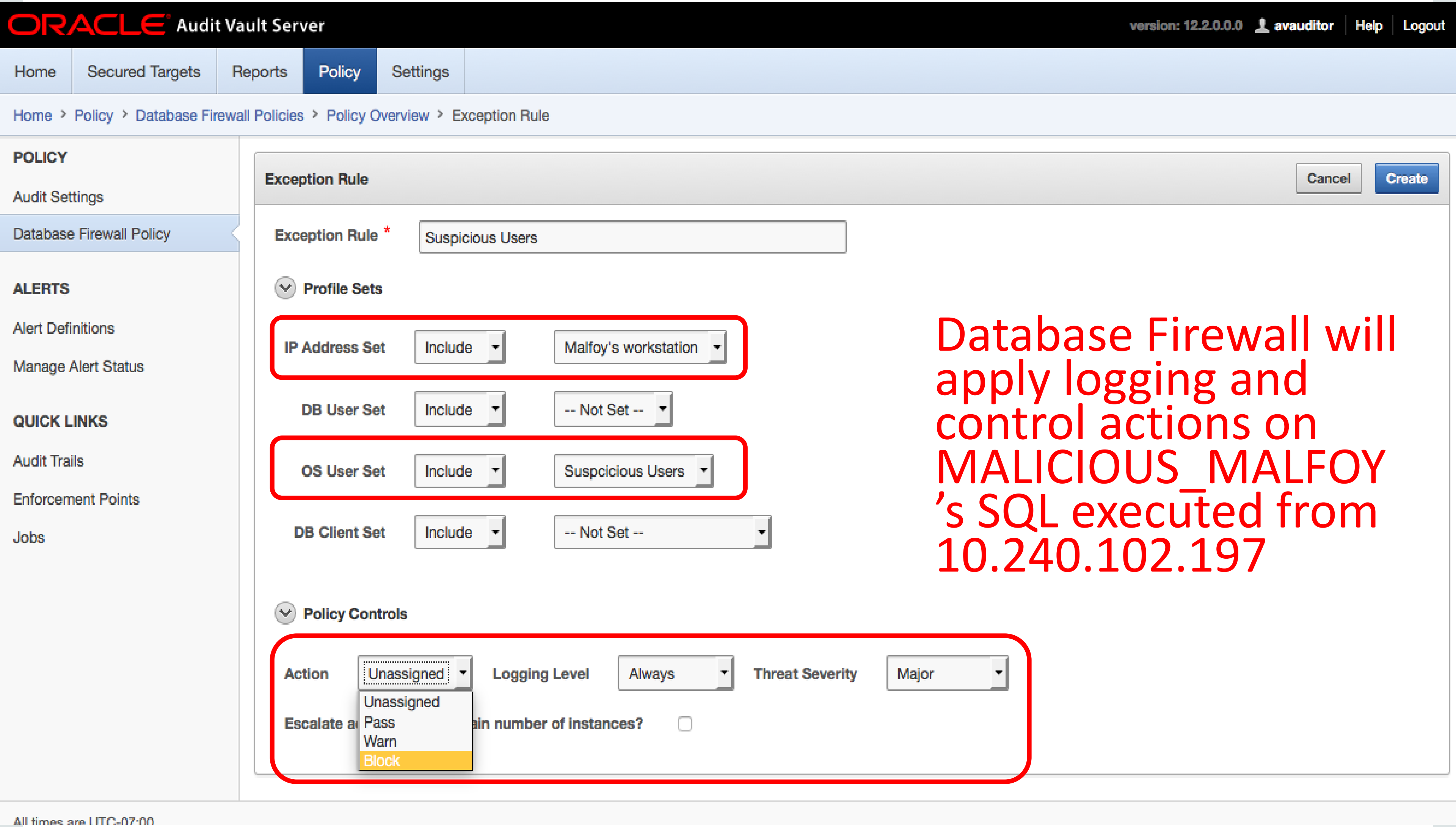
Create New Set

New Set Name * Malfoy's workstation

All sets must have at least one member.
Please enter your set's first member here * 10.240.102.197

Note: This example is meant for illustrative purposes only

Policy Exception Rule



ORACLE Audit Vault Server

version: 12.2.0.0.0 avauditor | Help | Logout

Home | Secured Targets | Reports | Policy | Settings

Home > Policy > Database Firewall Policies > Policy Overview > Exception Rule

POLICY

Audit Settings

Database Firewall Policy

ALERTS

Alert Definitions

Manage Alert Status

QUICK LINKS

Audit Trails

Enforcement Points

Jobs

Exception Rule — Cancel | Create

Exception Rule *: Suspicious Users

Profile Sets

IP Address Set	Include	Malfoy's workstation
DB User Set	Include	-- Not Set --
OS User Set	Include	Suspcicious Users
DB Client Set	Include	-- Not Set --

Policy Controls

Action: Unassigned (Unassigned / Pass / Warn / Block) | Logging Level: Always | Threat Severity: Major

Escalate a…in number of instances? □

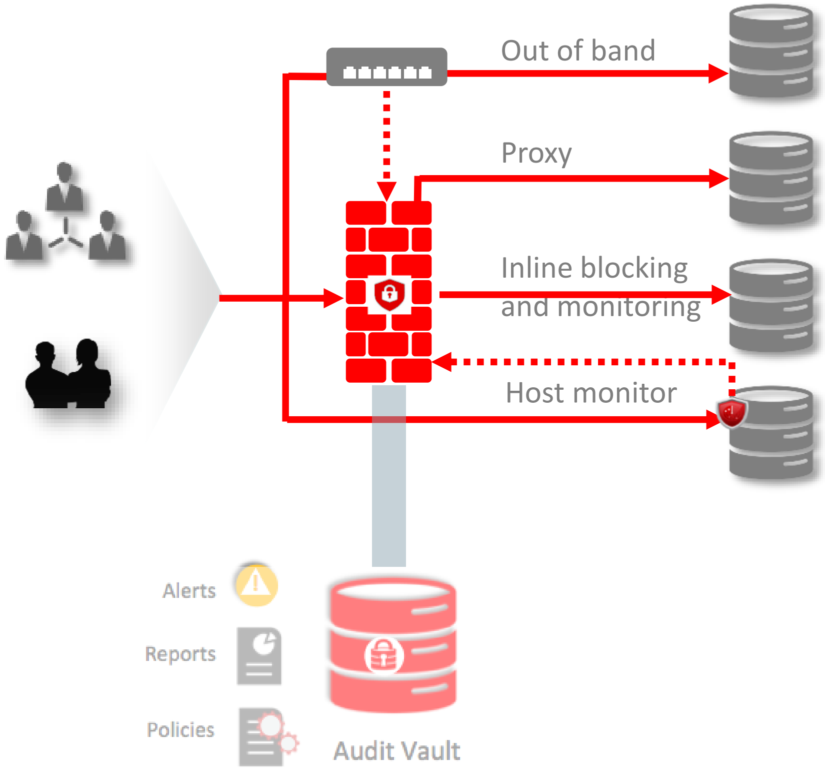
All times are UTC-07:00

Database Firewall will apply logging and control actions on MALICIOUS_MALFOY's SQL executed from 10.240.102.197

Database Firewall

Flexible deployment

- Out of band (off SPAN port)
  - Passive monitoring
- Proxy mode
  - Database clients connect to the IP address of Database Firewall
- In-line
  - Monitoring or blocking
- Host monitor
  - Host agent mirrors traffic back to Database Firewall



Database Security

Oracle Advanced Security Data Encryption

Oracle Advanced Security

Advanced Protection for the Oracle Database

Transparent Data Encryption (TDE)

- Transparently encrypts data-at-rest in Oracle databases and securely manages the encryption keys
- Protects against theft or loss of disks and backups
- Prevents OS users from inspecting the tablespace files

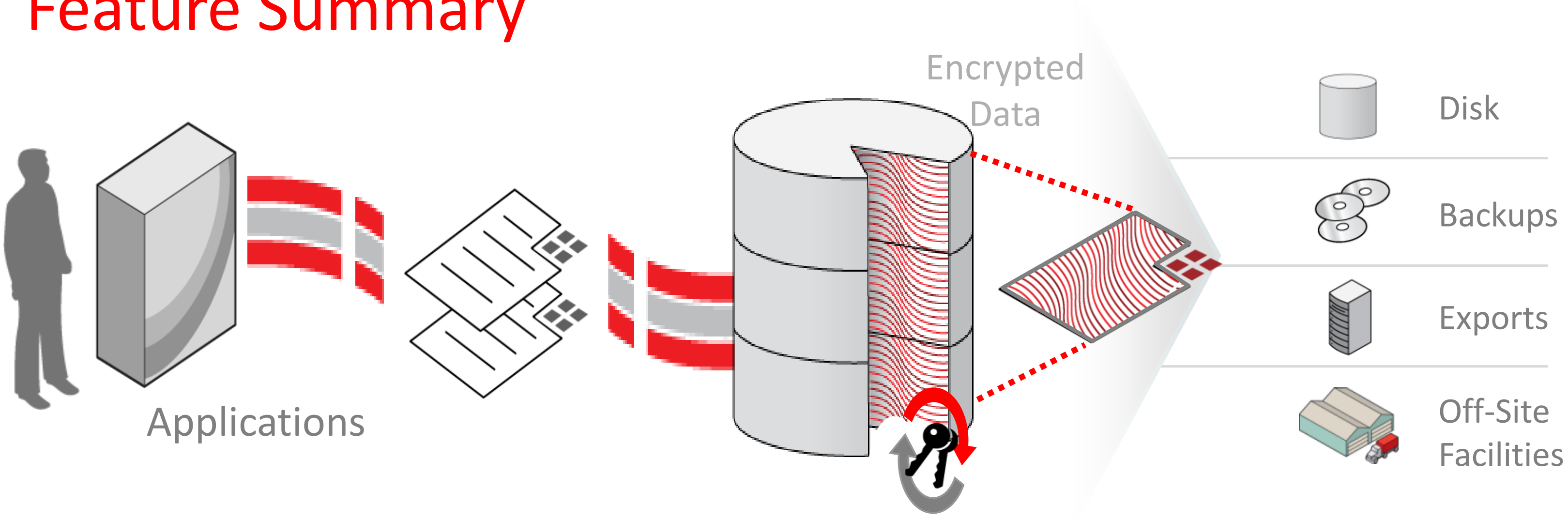
NEW!

Data Redaction

- On-the-fly redaction to limit exposure of sensitive data in applications
- Declarative policies centrally managed in the database
- Business need to know decisions based on application and database contexts
- Multiple redaction transformations to choose from

Transparent Data Encryption

Feature Summary



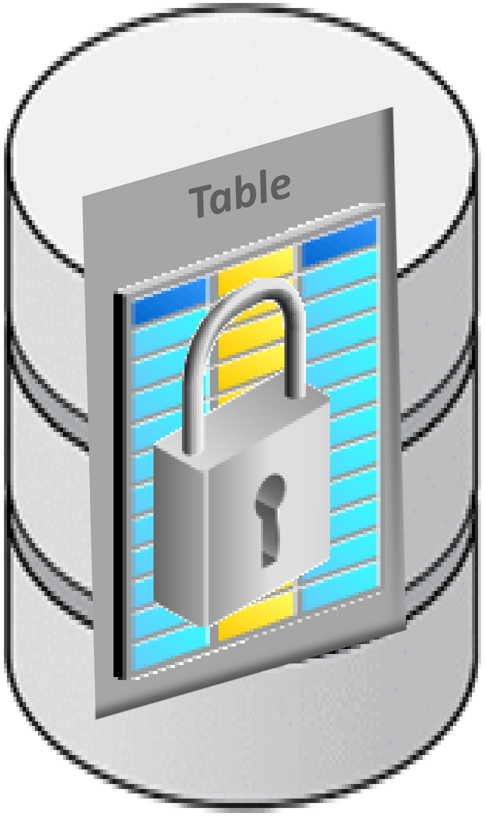
- Encrypts columns or entire tablespaces
- Protects the database files on disk and on backups
- Securely manages the keys, assists with key rotation
- Supports Oracle Exadata engineered systems
- Compatible with applications, no changes required

ORACLE

Types of Encryption Supported

Column Encryption

- Summary
  - Transparently encrypts table columns
  - Provides options for salt and secondary integrity check
- Benefits
  - Useful when the tables are large, a small number of columns must be encrypted, and the columns are at known locations
  - Data remains encrypted in memory (SGA)
  - Oracle Enterprise Manager can automatically discover sensitive columns to be encrypted



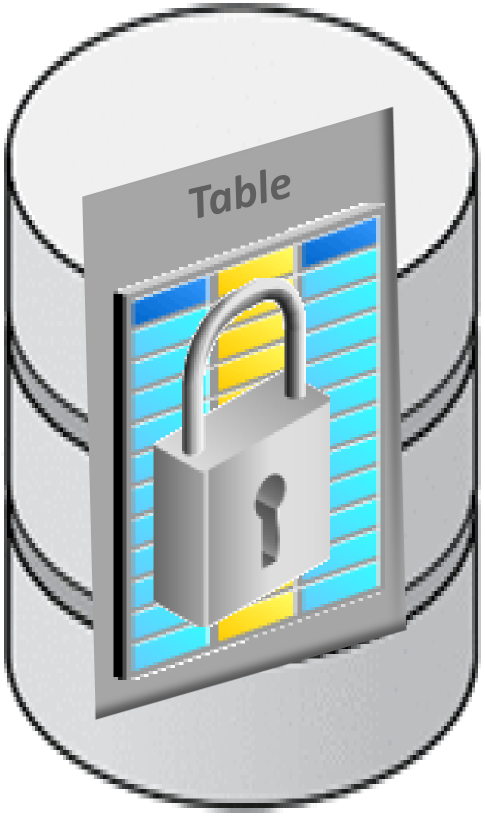
Column Encryption

- TDE enables you to specify a nondefault encryption algorithm

  -3DES168 - AES192 (default)

  -AES128 -AES256

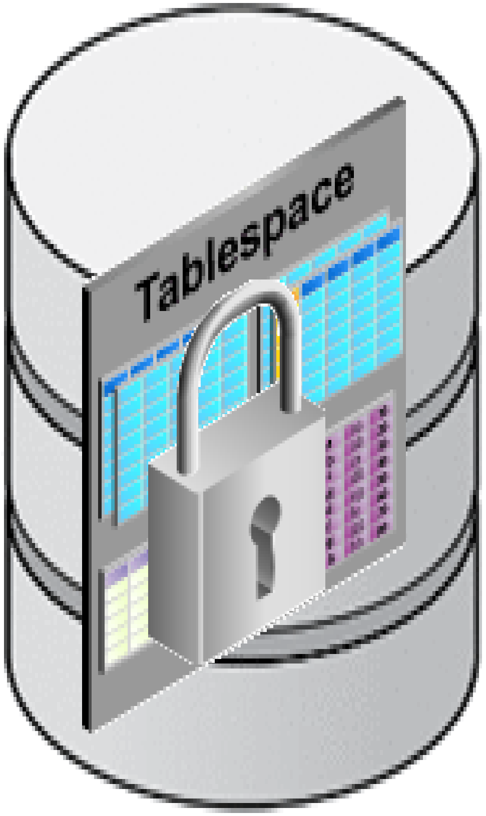
```
CREATE TABLE employee (
   first_name VARCHAR2(128),
   last_name VARCHAR2(128),
   empID NUMBER ENCRYPT NO SALT,
   salary NUMBER(6) ENCRYPT USING '3DES168'
);
CREATE INDEX employee_idx on employee
(empID);
```



Types of Encryption Supported

Tablespace Encryption

- Summary
  - Protects entire tablespaces, encrypting sensitive data at the block level in storage
- Benefits
  - No need to identify columns, and no storage overhead
  - Supports all data types, foreign keys, indexes, etc.
  - Major performance boost from database caching and hardware acceleration
  - Integrated with database compression and backup
  - Uses unique features of Oracle engineered systems



Tablespace Encryption

- The default encryption algorithm (AES128)
  - 3DES168
  - AES192
  - AES256

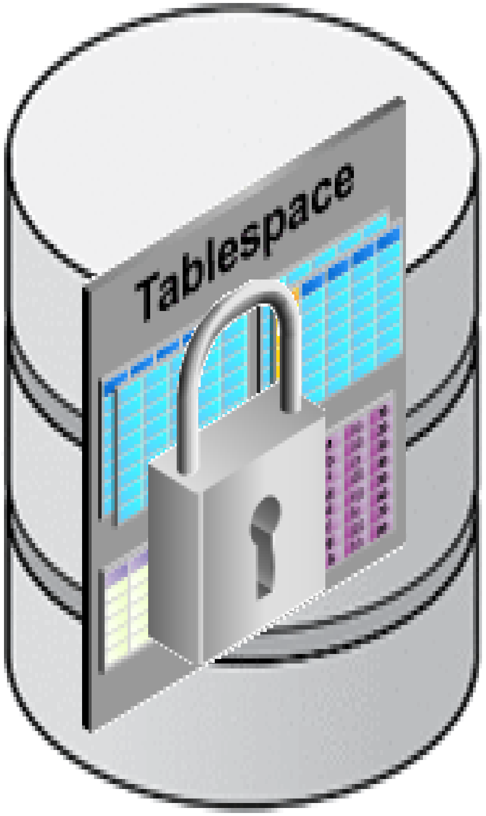
```
CREATE TABLESPACE securespace

DATAFILE
'/home/user/oradata/secure01.dbf'

SIZE 150M

ENCRYPTION USING 'AES256'

DEFAULT STORAGE(ENCRYPT);
```



Deploying TDE on Existing Data Now

- Offline migration during maintenance
  - Oracle DataPump Export / Import
  - Alter table move + alter index rebuild
  - Dbms_metadata.get_ddl + insert as select
  - Create table as select (CTAS)
- Online migration with near-zero downtime
  - Oracle Online Table Redefinition (DBMS_REDEFINITION)
  - *NEW* Combine usage of Data Pump and Data Guard for Oracle Database 11*g*R2 and 12*c*R1

NEW White Papers
Available on OTN

Oracle Maximum
Availability Architecture

Converting to Transparent Data Encryption
Using Data Guard Transient Logical Standby

Oracle Database 11g Release 2

ORACLE WHITE PAPER | MAY 2015

Oracle Maximum
Availability Architecture

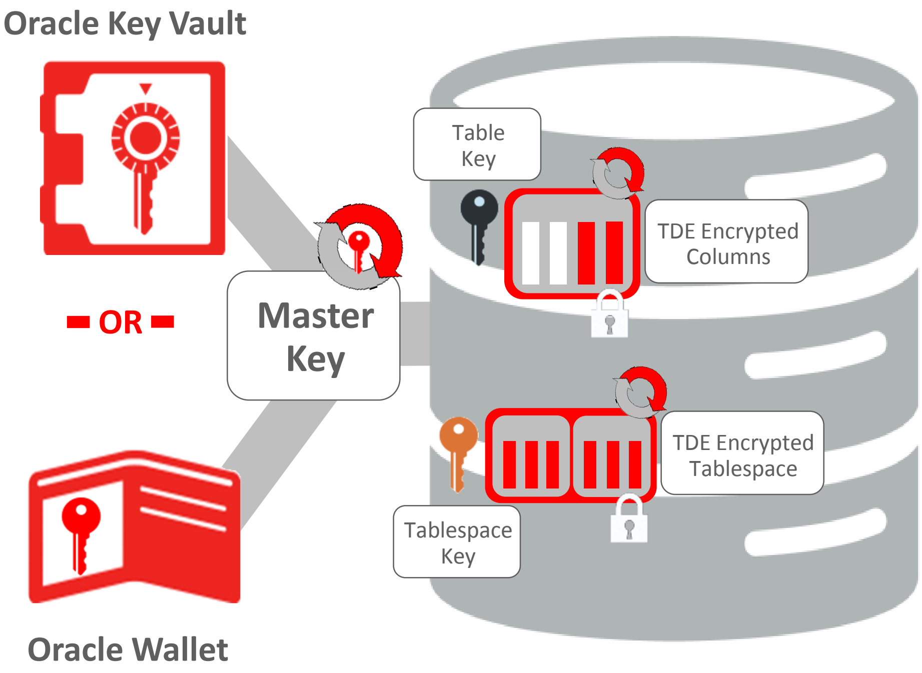
Converting to Transparent Data Encryption
Using Active Data Guard (DBMS_ROLLING)

Oracle Database 12c

ORACLE WHITE PAPER | MAY 2015

TDE Key Architecture

- Data encryption keys are created and managed by TDE automatically
- A master encryption key encrypts the data encryption keys
- The master key typically is stored in Oracle Wallet or Oracle Key Vault



Oracle Wallet Types

- Encryption wallet (`ewallet.p12`)
  - Encrypted with the wallet password (→ PKCS#5)
  - Needs to be opened manually for the database to encrypt and decrypt data
  - **NEVER** delete the encryption wallet
- Auto-open wallet (`cwallet.sso`)
  - Wallet is opened automatically when database accesses encrypted data for the first time
  - **NEVER** backup `cwallet.sso` together with database files!
- Local auto-open wallet (`cwallet.sso`)
  - Auto-opens only on the server is was created on

ORACLE

Managing Master Keys in Oracle Wallet

- ***CRITICAL***: Remember wallet password
- ***CRITICAL***: Do not delete wallet. Retain copy of password-based wallet even if using auto-login
- ***CRITICAL:*** Do not have multiple databases share same wallet
- Set strong wallet password using numbers, capitalization, length >= 12 characters…
- Rotate master encryption key and wallet password approximately every six months
- Backup wallet before and after each rotation operation
- Keep wallet backup separate from encrypted data backup
- Restrict wallet directory and file permissions
- Keep wallet read-only for daily use, set immutable bit where available
- For RAC, consider storing wallet in ACFS (DB 11gR2) or ASM (DB 12*c*R1)
- For DB 12*c*R1, separate duties using SYSKM

Database Security

Oracle Advanced Security Data Redaction

Oracle Advanced Security

Advanced Protection for the Oracle Database

Transparent Data Encryption (TDE)

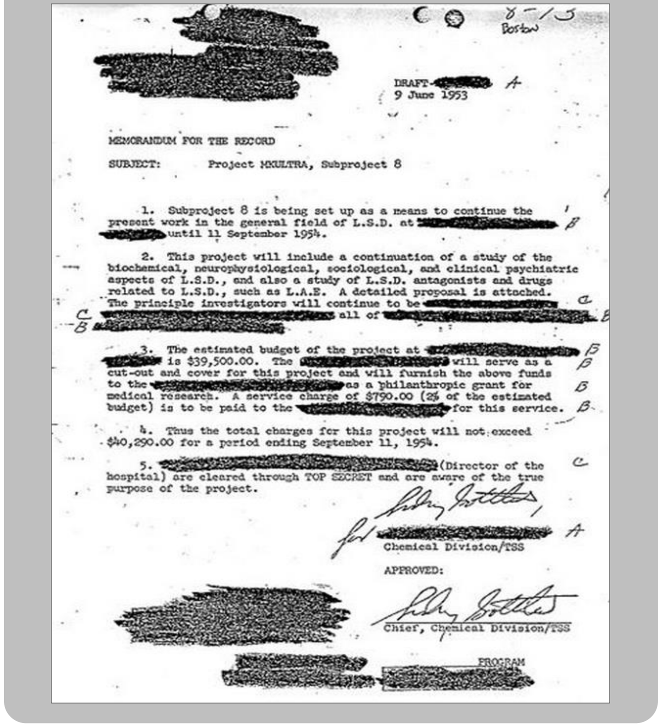
- Transparently encrypts data-at-rest in Oracle databases and securely manages the encryption keys
- Protects against theft or loss of disks and backups
- Prevents OS users from inspecting the tablespace files

NEW!

Data Redaction

- On-the-fly redaction to limit exposure of sensitive data in applications
- Declarative policies centrally managed in the database
- Business need to know decisions based on application and database contexts
- Multiple redaction transformations to choose from

Redacting Sensitive Information to Keep It Private



[redacted]

C 8-13
Boston

DRAFT-[redacted] A
9 June 1953

MEMORANDUM FOR THE RECORD

SUBJECT: Project MKULTRA, Subproject 8

1. Subproject 8 is being set up as a means to continue the present work in the general field of L.S.D. at [redacted] until 11 September 1954. B

2. This project will include a continuation of a study of the biochemical, neurophysiological, sociological, and clinical psychiatric aspects of L.S.D., and also a study of L.S.D. antagonists and drugs related to L.S.D., such as L.A.E. A detailed proposal is attached. The principle investigators will continue to be [redacted] all of [redacted] C B

3. The estimated budget of the project at [redacted] is $39,500.00. The [redacted] will serve as a cut-out and cover for this project and will furnish the above funds to the [redacted] as a philanthropic grant for medical research. A service charge of $790.00 (2% of the estimated budget) is to be paid to the [redacted] for this service. B

4. Thus the total charges for this project will not exceed $40,290.00 for a period ending September 11, 1954.

5. [redacted] (Director of the hospital) are cleared through TOP SECRET and are aware of the true purpose of the project. C

for [redacted] A
Chemical Division/TSS

APPROVED:

[redacted]

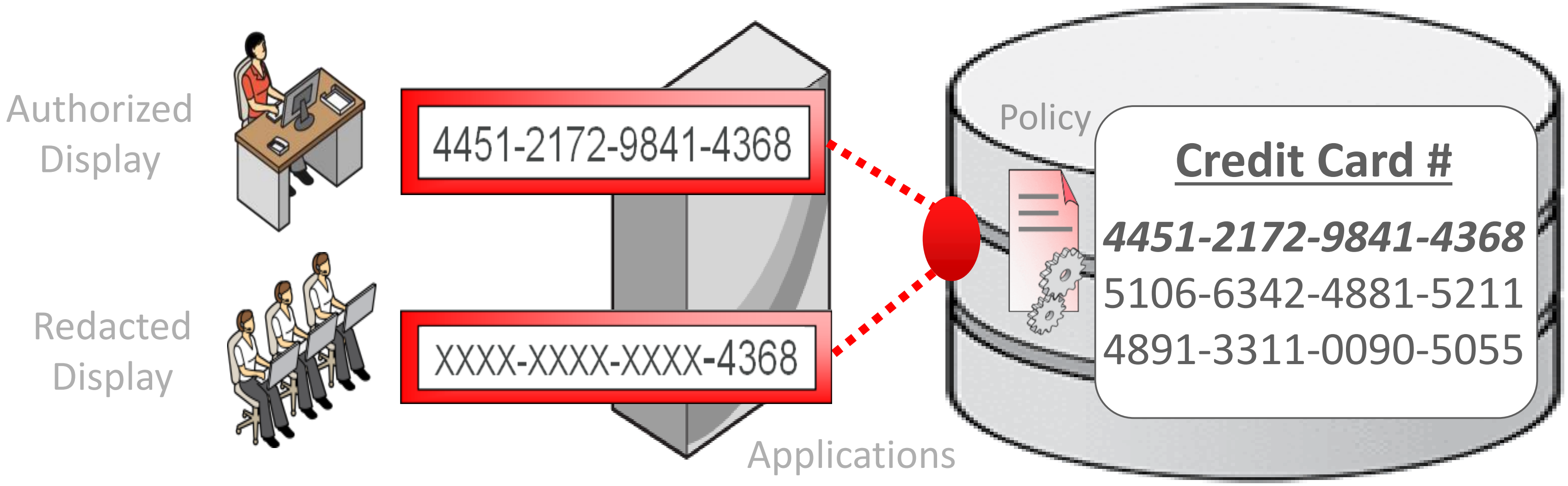
Chief, Chemical Division/TSS

[redacted] PROGRAM [redacted]

- Redacting sensitive information is common for documents.
- Much more sensitive information is consolidated in databases.
- Redacting data displayed from databases improves privacy and security.

Data Redaction in Oracle Database 12*c*

Redacting Sensitive Data for Applications



Authorized Display

4451-2172-9841-4368

Redacted Display

XXXX-XXXX-XXXX-4368

Applications

Policy

Credit Card #

4451-2172-9841-4368

5106-6342-4881-5211

4891-3311-0090-5055

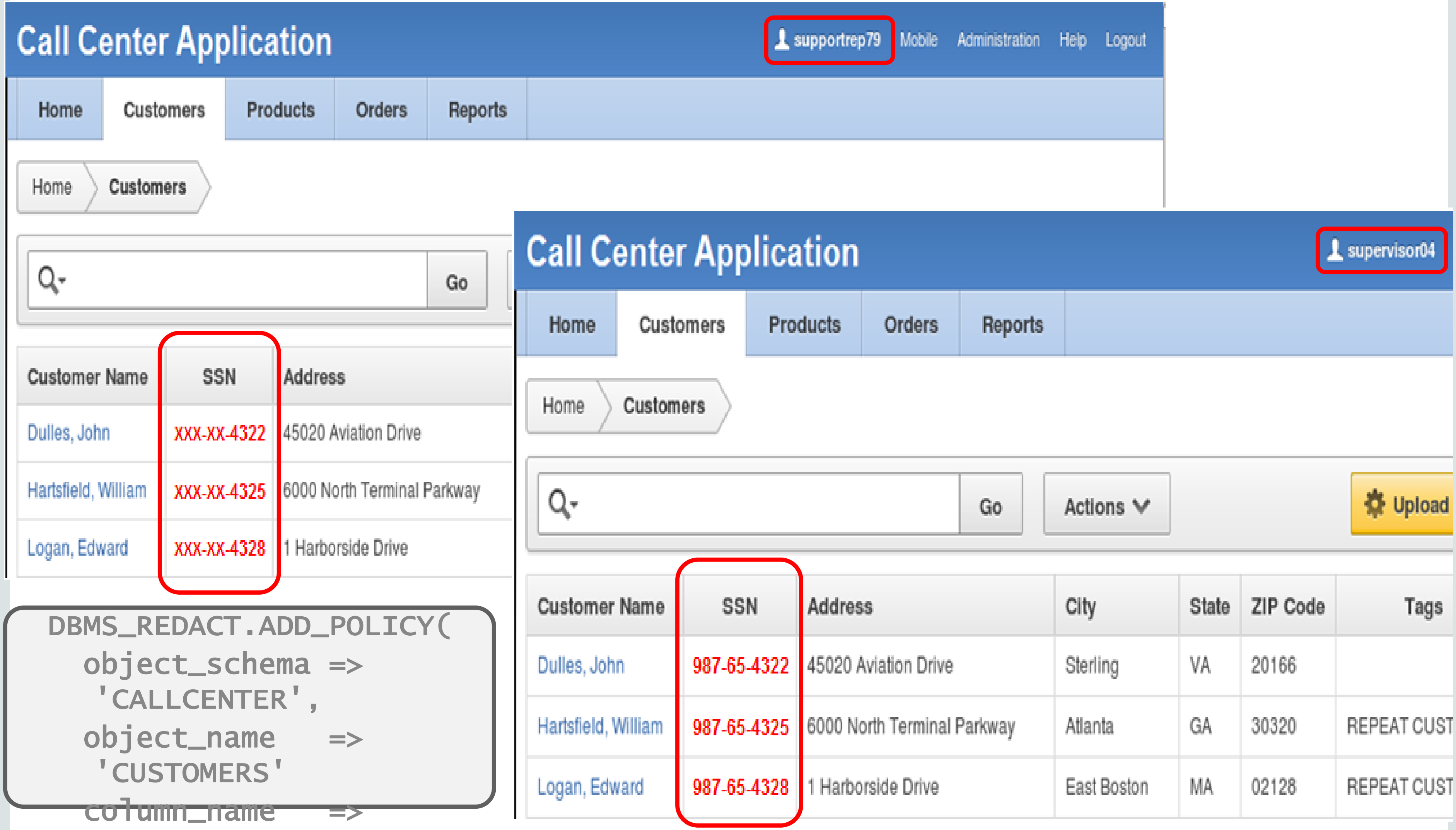
- On-the-fly redaction based on user name, IP address, application context, and other factors
- Transparent in-database enforcement across apps
- Minimal impact on production work loads

Call Centers

Decision Support Systems

Systems with PII, PHI, PCI data

Application Screens After Redacting



Customer Name	SSN	Address
Dulles, John	XXX-XX-4322	45020 Aviation Drive
Hartsfield, William	XXX-XX-4325	6000 North Terminal Parkway
Logan, Edward	XXX-XX-4328	1 Harborside Drive

Customer Name	SSN	Address	City	State	ZIP Code	Tags
Dulles, John	987-65-4322	45020 Aviation Drive	Sterling	VA	20166	
Hartsfield, William	987-65-4325	6000 North Terminal Parkway	Atlanta	GA	30320	REPEAT CUST
Logan, Edward	987-65-4328	1 Harborside Drive	East Boston	MA	02128	REPEAT CUST

```
DBMS_REDACT.ADD_POLICY(
   object_schema =>
    'CALLCENTER',
   object_name   =>
    'CUSTOMERS'
   column_name   =>
    'SSN'...
```

Data Redaction Features

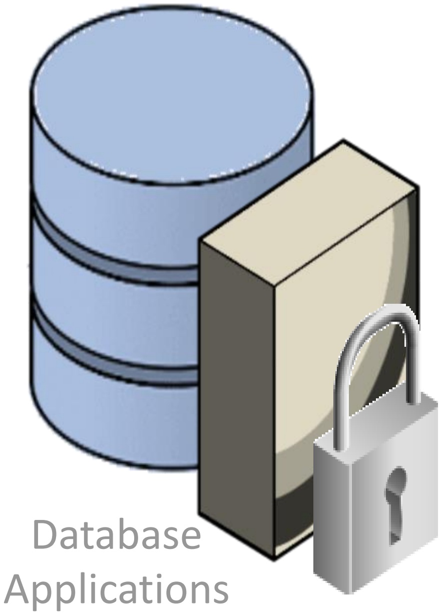
Supported Transformations

	Stored Data	Redacted Display
Full	10/09/1992	01/01/2001
Partial	052-51-2147	XXX-XX-2147
RegExp	tim.lee@acme.com	[redact]@acme.com
Random	4451217298414368	4943634405470110

Redaction PL/SQL API

```
BEGIN
  DBMS_REDACT.add_policy(object_schema       => ’SALES'
                        ,object_name         => ’CUSTOMER'
                        ,policy_name         => 'Protect PII'
                        ,expression          => '(sys_context(''userenv'',''client_ip''), !=
''10.4.111.171'' AND                                      sys_context(''userenv'',
''os_user'') != ”bill.slocumb'')'
                        ,column_name         => 'SSN'
                        ,function_type       => DBMS_REDACT.RANDOM
                        );
END;
/
```

Benefits of Data Redaction



- Can be managed through Oracle Enterprise Manager or a command-line API
- Includes a redaction format library for common PCI and PII data
- Prevents accidental viewing of sensitive data by privileged users who run ad hoc queries
- Avoids sources of leakage where redaction could be undone by copying into unredacted tables

Hardware and Software

ORACLE®

Engineered to Work Together