Defense-in-Depth for Cloud Databases

Unifying Cloud and On-Premises Database Security

ORACLE WHITE PAPER | MARCH 2017

AUTHOR: DINESH RAJASEKHARAN | PRINCIPAL PRODUCT MANAGER | DATABASE SECURITY

Table of Contents

Executive Summary 2

Databases Continue to be the Treasure Hunt for Attackers 2

Databases for the Cloud 3

The Hybrid Cloud Model - Today’s Reality 4

Cloud Raises New Data Security Concerns 4

Strategy for Uniformly Protecting Data On-Premises and in the Cloud 5

- Always-on Encryption to Minimize Breaches due to Data Loss or Theft 6
- Make the Data Unusable with a Click using Oracle Key Vault 6
- Compare Configuration and Compliance of Cloud Databases 7
- Restrict Cloud Administrators Accessing your Sensitive Information 8
- Mask and Subset to Limit Exposure of Sensitive Production Data 8
- Detect Threats and Mitigate Audit Tampering through Off-Site Consolidation 9
- Centralized and Unified Security Policy Management 10
- Defense-in-Depth with Transparency, Accuracy, Performance, and Scale 11

Conclusion 12

Bonus Content 13

- Comparing Database Security of different Cloud Providers 13

Executive Summary

Cloud computing is revolutionizing information technology through its cost and operational flexibility. Organizations are rapidly adopting cloud computing, but the transition is still in progress with many organizations keeping their mission-critical applications on-premises. Even though migrating to the cloud can be a cost-effective option, some organizations are concerned about the availability of their applications, network latency, and network throughput. For some organizations, lift and shift of their on-premises applications is not trivial due to several platform and application components. But there is one common concern cutting across all organizations and that is “security.” Shared infrastructure and lack of direct control fueled by increasing data breaches are the top concerns for organizations considering cloud adoption.

Whether on-premises or in the cloud, databases are the repositories of sensitive data and therefore present attractive targets for attackers. Furthermore, regulations such as the European Union’s General Data Protection Regulation (GDPR) spell out companies’ responsibilities to secure personal information and notify individuals of data breaches with adverse impact. This paper describes a methodology to protect sensitive information in cloud databases and yet retain control on-premises.

Databases Continue to be the Treasure Hunt for Attackers

Data breaches have become daily news, so much so that security researchers are now afraid that breaches will slowly go from being headlines to the back page. Attackers are now targeting Intellectual Property (IP), Personally Identifiable Information (PII), and Personal Health Information (PHI) in addition to Payment Card and Financial Information. Some of these breaches have directly targeted databases, including recent attacks exposing 21.5 million records from US Office of Personnel Management, 191 million records from US Voter Databases, and $81 million from Bangladesh National Bank.

Databases continue to be the most attractive targets for attackers because they are the information store with all the sensitive data. Organizations fortify access to databases with layers of security such as firewalls and intrusion detection systems. However, recent attacks have leveraged channels that have legitimate access to the database such as users, administrators, developers, testers, partners, and outsourced services. The rapidly evolving IT landscape and adoption of agile development methodologies are increasing the number and frequency of the channels directly accessing databases. It is becoming critical to directly secure databases, shrink the attack surface, and reduce the number of ways attackers can reach databases. Directly securing databases requires placing security controls closer to a database or, where possible, embedding them into the database itself.

The following picture illustrates how attackers try to target databases containing IP, PII, PCI, and PHI through a variety of threat actors such as database users, administrators (DBAs), testers, developers, application users, and support users.

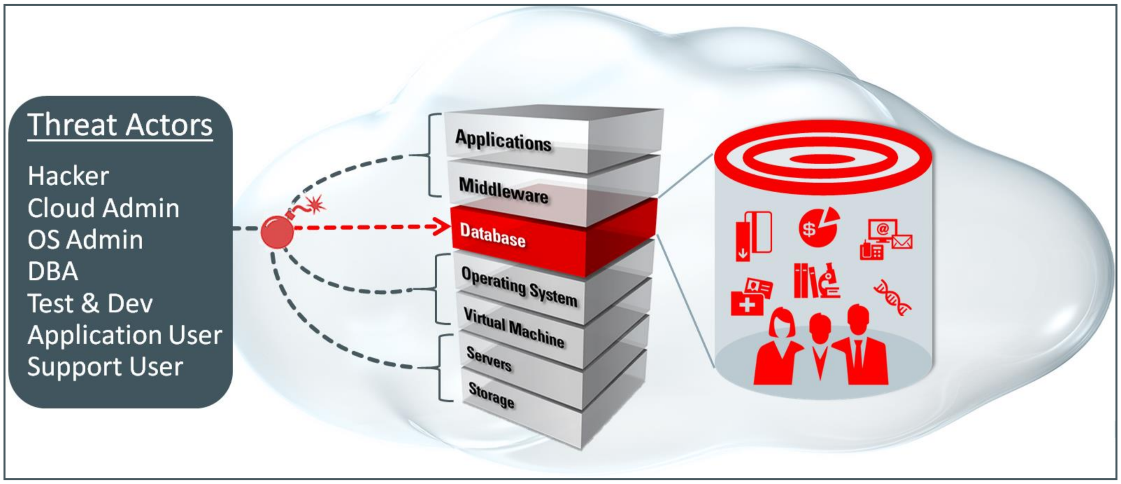

Figure 1: Databases continue to be attractive targets for attackers.

Databases for the Cloud

Public clouds are generally categorized into three areas:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Just as with an on-premises IT stack, databases (being part of PaaS) became the heart of the cloud stack by storing mission critical business data. Databases are the foundation for applications (SaaS) and must integrate with underlying infrastructures (IaaS).

Oracle Database Cloud Services caters to the needs of different organizations by offering a variety of database configurations. A developer may only need a low cost schema to quickly start coding an application module. A tester may need a database schema or a database that provisions data quickly. A small business such as a bookstore may need a low cost single instance database. Enterprises may require full-fledged databases to host their mission critical applications. The following table summarizes some of the Oracle Database Cloud Services available:

Database Cloud Service	Use case
Live SQL	Zero cost service for introduction to the cloud
Exadata Express Cloud Service	Fully managed service for application development targeting small to medium sized data
Database Cloud Service	Complete Oracle Database with all the premium features
Database Cloud Service – Bare Metal	Database Cloud Service with the performance of dedicated hardware and local NVMe storage
Exadata Cloud Service	World’s fastest database machine for heavy applications

Whether running a low cost or an enterprise class database, organizations should not compromise on data security in this era of mega breaches. Moreover, organizations must have a consistent and robust data security methodology across all databases, whether on-premises or in the cloud. Oracle Data Security methodology explained in this paper applies to the Oracle Databases on-premise as well as to the most popular Oracle Database Cloud Services.

The Hybrid Cloud Model - Today’s Reality

» **Public Cloud**

When application, platform, and infrastructure components are hosted in any cloud provider’s data centers, the underlying resources are shared among multiple tenants or subscribers. Cloud vendors such as Oracle provide a dedicated platform in addition to the shared platform model.

» **Private Cloud**

Applications, platform, and infrastructure components are hosted in the subscriber’s or customer’s data centers with all the facilities of the cloud such as multi-tenancy, scaling on-demand, and subscription based pricing. Cloud vendors such as Oracle also provide professional services and technical expertise through fully managed services while Oracle provides an added ability to move between private and public cloud infrastructures using Oracle Cloud Machines.

» **Hybrid Cloud**

Today several enterprises are exploring public clouds for their development and testing needs while their mission-critical production applications are still on-premises. Cloud adoption or migration will continue to be a work-in-progress item for these enterprises due to the complexity and the criticality of their on-premises applications involving multiple components such as storage, databases, application servers, web servers, and more.

Even if these enterprises fully adopt cloud, most likely they may use a private cloud for their mission critical production applications. Until then, they will continue to operate in a hybrid cloud model with a mix of on-premise and cloud applications. Having a common unified framework providing a transparent bridge between on-premise and cloud platforms will simplify the cloud adoption, minimize the learning curve, and expedite the transition.

Cloud Raises New Data Security Concerns

Data privacy and security are the top concerns for some organizations considering moving to the cloud. Some of their key data security concerns can be broadly summarized into the following topics:

Cloud provider’s ability to protect against data loss or thefts

Public clouds are black boxes to many organizations involving multiple administrators and processes around data management, governance, and compliance. As data is frequently backed up, exported, replicated, and integrated, organizations are concerned about the cloud provider’s ability to protect data against data loss or thefts.

Enterprises are concerned about the lack of control on the data in the cloud due to on-going data breaches, lawsuits, government/regulatory agencies involvement, the volume of the data being generated by hundreds of applications and the related components.

Sharing underlying compute and network with other customers

Public clouds generally use a common server to host applications of multiple tenants or customers through virtual machines. Organizations are highly concerned about sharing a server with others as some attacks such as DoS (Denial-of-Service) can have a ripple effect on all the applications hosted in a shared server model.

The who’s, when’s, and how’s of data access

Enterprises are not clear about the who’s, when’s, and how’s of data access in the cloud such as:

- Who is accessing the data? End users, cloud administrators, third-party cloud providers? (For example, some cloud providers host their SaaS in another cloud provider’s IaaS and outsource operations to a managed services provider.)
- When is the data accessed and through which channels?
- How to make sure that the native cloud and third-party administrators are not seeing the sensitive information such as personal, financial, and intellectual property (IP)?
- How to audit the different aspects of data access? What if an attacker tampers with audit records?

Strategy for Uniformly Protecting Data On-Premises and in the Cloud

Oracle’s Cloud Data Security is built on the following principles addressing the key concerns about protecting data in the cloud:

- **Security should be always-on**

In Oracle Cloud, foundational data security features such as encryption and auditing are always-on.

- **Security should be pushed down the stack**

To shrink the attack surface, and reduce the number of ways in which attackers can access the databases, it is important to enforce security as close to the data as possible. Also, embedding security with the data minimizes disruptions and performance penalty to the applications and the databases.

- **Establish customer’s control on the data**

As organizations continue to upload large amounts of data to the cloud, Oracle provides hybrid cloud technologies such as Key Vault, Audit Vault and Database Firewall to monitor, detect, and deny access to data upon malicious activity from on-premises.

- **Restrict Database Administrator’s (DBA) access to the sensitive data**

Oracle Cloud provides unique technologies such as Database Vault to mitigate insider attacks by restricting cloud subscriber’s as well as provider’s DBAs accessing the sensitive information and yet perform their day-to-day operations such as tuning, taking backups and applying patches.

- **De-identify data on-premises or in the cloud**

As many organizations have started using cloud for development and test use cases, Oracle Cloud provides Data Masking and Subsetting to anonymize sensitive information on-premise or in the cloud. This approach serves to mitigate intentional or accidental disclosure of sensitive information and minimize the compliance boundary.

- **Transparently migrate security policies between on-premise and the Cloud environments**

To support enterprises operating in the hybrid cloud model, Oracle Enterprise Manager provides a unified user interface for migrating and managing security policies between on-premises and cloud environments.

The rest of this paper expands upon Oracle Cloud Data Security principles and technologies. In addition, the following white paper describes Oracle Cloud Network and Infrastructure Security.

Whitepaper: Oracle Infrastructure and Platform Cloud Services Security

Always-on Encryption to Minimize Breaches due to Data Loss or Theft

In the modern IT landscape, data often gets proliferated to multiple data sources, making it hard for the organizations to keep track of the sensitive information.

Consider the following scenarios:

- How many times is the data being backed up in the cloud?
- What are the backup, storage, and archive locations?
- What are the different channels (export dumps, backup tapes, clones, mailing, etc.) through which organizations are sending data to the cloud?
- Are the stale backups, tapes or dumps being properly shredded?
- What is happening to the data archives?
- What happens if a tape, a disk, a dump or an archive gets lost or stolen by an attacker?
- What happens if an attacker taps into the network to sniff data packets?

Improperly managed database files, backups, data dumps, archives, storage, tapes, and networks packets can lead to data loss or theft.

Encrypting data at-rest and in-transit helps to minimize breaches due to data loss or theft. Data Protection laws and standards such as PCI-DSS and EU General Data Protection Regulation (GDPR) mandates encryption as one of the security controls. Oracle Cloud encrypts data at-rest and in-transit by default with negligible performance impact.

Data in-transit to Oracle Cloud Databases is encrypted by default using database native network encryption. In addition to native network encryption, industry standard SSL/TLS network encryption can be configured. SSL/TLS network encryption adds the ability to enforce mutual authentication using client certificates. All network encryption options support strong ciphers such as Advanced Encryption Standard (AES) and 3DES. Integrity checking supports modern hashing algorithms including SHA-256.

Data at-rest in the Oracle Database Cloud Service is encrypted by default using Transparent Data Encryption (TDE). TDE encrypts data in any user-created tablespace with the CREATE TABLESPACE command in SQL or any tool using the AES-128 algorithm. You can optionally increase the key size to 192 or 256 bits. You can also encrypt RMAN backups and Data Pump exports. Optimizations in the database will pass through already encrypted tablespace data or encrypt the whole data stream where necessary. Backups and exports can be encrypted with the same key used by tablespace encryption, with a password, or both.

Master encryption keys used for encrypting data are created automatically and stored in a per-database wallet (a PKCS-12 and PKCS-5 compliant key storage file). Historical master keys are retained in the wallet for encrypted backups that may need to be restored in the future. Oracle recommends Key Vault - a centralized key management solution, for customers with many on-premises and cloud databases with several encryption keys, wallets, and Java keystores. The next section provides more details about Oracle Key Vault.

Make the Data Unusable by Attackers with a Click using Oracle Key Vault

Encryption is only as strong as the ability to manage the encryption keys securely and efficiently. What good is an encryption solution if attackers can get hold of the encryption keys? On the other hand, inefficient key management can lead to huge operational overhead and data loss. For many organizations, rotating and managing encryption keys, wallets, Java keystores, and credentials among several IT assets such as databases, application servers, storage, operating systems, applications is not a trivial task. Oracle Key Vault addresses these challenges by centrally managing encryption keys, wallets, Java keystores, and credential files.

One of the unique differentiators of the Oracle Cloud is that it helps organizations establish control over the data on-premises. Oracle Key Vault (OKV) plays a major role in establishing customer's control on the data by providing a facility to manage the encryption keys on-premises and suspend access to the corresponding cloud databases with the click of a button upon any suspicious activity.

Oracle Key Vault is a full-stack, security-hardened software appliance using Oracle Linux and Oracle Database technology for security, availability, and scalability. It supports the OASIS KMIP (Key Management Interoperability Protocol) industry standard and Hardware Security Module (HSM) as a "root-of-trust" for the key hierarchy that protects encrypted data stored in Key Vault. A browser-based management console simplifies administration. The platform also provides RESTful APIs for automating several administrative and key management tasks.

Oracle Key Vault 12.2 or higher deployed on-premises manages Transparent Data Encryption (TDE) keys of the Oracle Database Cloud Service. Figure 3 represents the Key Vault Hybrid Cloud management architecture.

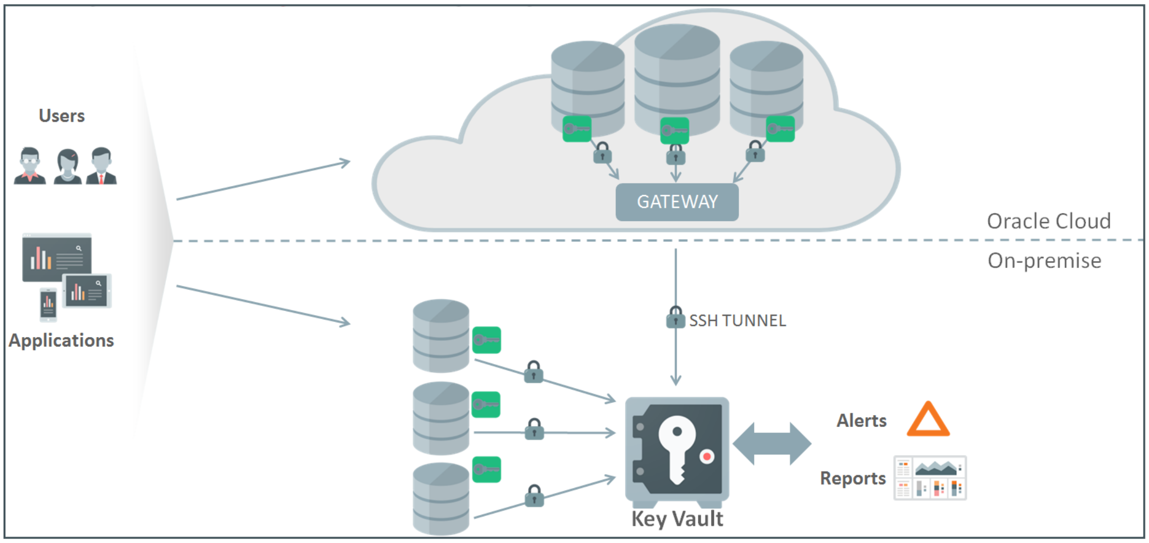

Figure 2: Oracle Key Vault provides key management in hybrid cloud deployments.

Compare Configuration and Compliance of Cloud Databases

With databases distributed across on-premises and cloud and each database containing many tunable configuration parameters, monitoring, synchronizing, and securing the configuration of databases is a challenge for several organizations. Oracle Clouds address this challenge by providing a Configuration and Compliance Management functionality.

The Configuration and Compliance Management functionality is part of Oracle Enterprise Manager Database Lifecycle Management Pack and requires on-premises Oracle Enterprise Manager. It helps to compare the configuration of on-premises and cloud databases to ensure that configuration is still secure, has not drifted over time, and enforce the current set of best practices. It can be used to run more than 100 out-of-the-box policy checks against Oracle Databases, identify trends, and monitor drift from the golden configuration. Also, custom configuration checks can be defined to supplement checks provided by Oracle. Database Lifecycle Management is included in the select editions of Oracle Database Cloud Service.

Not just your DBAs - Also Restrict Cloud Administrators Accessing your Sensitive Information

Data breaches due to accidental or intentional compromise of privileged user accounts is one of most common attack types. Organizations typically have multiple database administrators (DBAs) managing multiple applications. In the case of Software as a Service (SaaS) and Managed Cloud Services, day-to-day database administrative tasks such as cloning, patching, and maintenance are handled by the cloud vendor's database administrators (DBAs).

Increasing privileged user attacks and limited control on the cloud DBA's activates are putting organizations in a dilemma about cloud uptake. Enterprises such as financial and healthcare institutions with strict separation of duties (SODs) and compliance with data privacy laws and standards are even more concerned with the lack of control on cloud DBA activities. "Database Administrators" and "locked down sensitive data" are two terms that never got along - until Oracle invented Database Vault. Oracle Database Vault is a unique Oracle security control embedded into the Oracle Database kernel for restricting privileged database accounts (including cloud DBAs) from accessing sensitive information and yet allow them to perform day-to-day activities such as backup and patching.

Oracle Database Vault establishes customer's control on data by enforcing three distinct separation of duty controls for security administration, account management, and day-to-day database administration activities. It creates data realms around application schemas, sensitive tables, and stored procedures providing controls to prevent privileged accounts from being exploited by hackers and insiders to access sensitive application data. Oracle Database Vault SQL Command Controls allow customers to control operations inside the database, including commands such as create a table, truncate table, and create a user. Various built-in factors such as IP address, authentication method, and program name help implement multi-factor authorization to deter attacks leveraging stolen passwords. These controls prevent accidental configuration changes and also prevent hackers and malicious insiders from tampering with applications.

Oracle Database Vault is included in select editions of Oracle Database Cloud Service and is available as a fully managed subscription service for select modules of Oracle Fusion SaaS.

Mask and Subset to Limit Exposure of Sensitive Production Data

Many organizations understand the cost and operational benefits of the cloud. They have passed the stages of 'what is cloud?' and 'why the cloud?' Now the discussion is about use cases. The immediate requirement is for non-production use cases such as development and testing, but these organizations are concerned about using the sensitive production data for test and development purposes. Moreover, copying the entire production data to test and development environments can increase the costs, expand the security perimeter, and delay the production to test provisioning time. On the other hand, small and medium businesses (SMBs) may leverage the public cloud for both production and non-production use cases. Most likely, they will first evaluate the cloud infrastructure with test data instead of using real data for data privacy and compliance reasons.

Whether an enterprise or an SMB, development, and test environments are paving the path for the cloud adoption. However, development and test environments are one of the potential targets for an attack as they contain copies of production data. Data Privacy laws and standards such EU General Data Protection Regulation and PCI-DSS recommend anonymizing sensitive production information for test and development purposes.

Oracle Cloud helps organizations to accelerate cloud adoption, achieve data privacy and compliance by masking and subsetting sensitive data. Data Masking and Subsetting is an Oracle Cloud differentiator which helps to extract entire copies or subsets of application data from the databases, anonymize, and minimize personal data so that the data can be safely shared with the developers, testers, partners, and other third parties. The integrity of the database is preserved ensuring the continuity of the applications.

One of the challenges with anonymization is that if it is not done properly, the de-identified or scrambled data may not be usable for testers and developers. Moreover, it could break the data integrity of the applications and databases. Oracle Data Masking and Subsetting addresses these challenges by capturing sensitive columns and parent-child relationships in reusable Application Data Models. It provides a comprehensive and extensible library of anonymization and masking formats, functions or transformations, and application templates. Sensitive Personal Data such as credit card numbers, national identifiers, and other personally identifiable information (PII) can be easily masked using built-in library of masking and anonymization formats.

Data Masking and Subsetting is integrated with Oracle Enterprise Manager's data cloning workflow. You can mask before or after moving data into the Oracle Cloud while cloning the databases between on-premises and cloud environments. Data Masking and Subsetting is included in the select editions of Oracle Database Cloud Service and is available as a fully managed subscription service for select modules of Oracle Fusion SaaS.

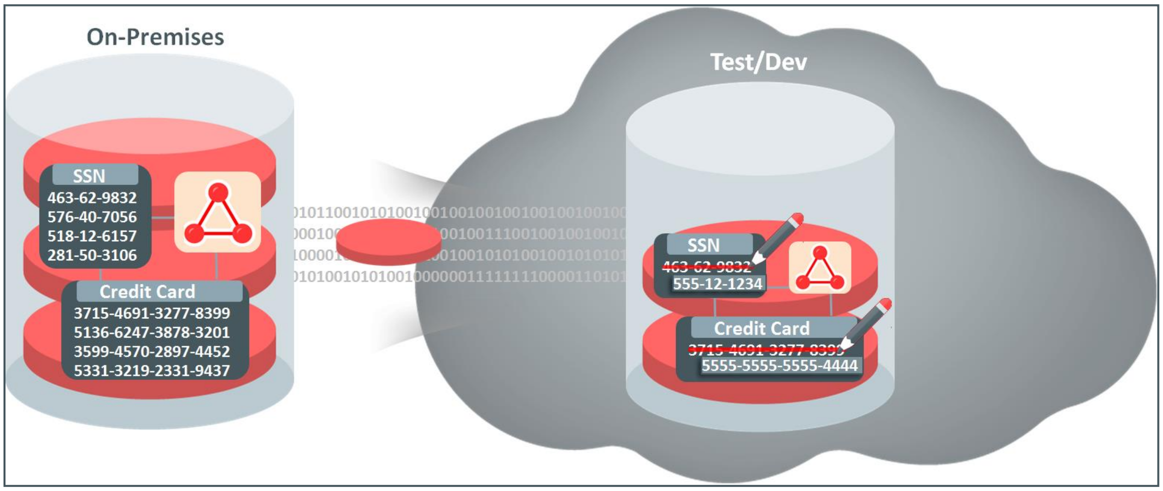

Figure 3: Oracle Data Masking and Subsetting protects data on-premises or in the cloud.

Detect Threats and Mitigate Audit Tampering through Off-Site Consolidation

Attacks have grown increasingly sophisticated bypassing perimeter security, taking advantage of trusted middle tiers, and even masquerading as privileged insiders. Also, attackers typically try to tamper the audit records to cover their tracks. Surveys of numerous security incidents have shown that timely examination of audit data could have helped detect unauthorized activity early and reduce the resulting financial impact. Just like encryption, auditing has become a fundamental data security requirement mandated by data privacy laws and standards.

Oracle Cloud offers comprehensive, fine-grained, and unified auditing functionality as part of its Database Cloud Service. Just like encryption, auditing is also enabled-by-default. In addition, it also establishes customers control on their audit data by providing an option to store and manage audit records on-premise Audit Vault and Database Firewall.

Oracle Audit Vault and Database Firewall (AVDF) is a software appliance which consolidates database activity monitoring events and audit data from databases, operating systems, and directories. AVDF 12.2 can also consolidate audit data from cloud databases to a central location. AVDF facilitates a unified enterprise-wide audit infrastructure for on-premises and cloud databases including consistent policies, unified reporting, and common alert management.

AVDF provides pre-fabricated reports for several data privacy standards such as PCI-DSS, SOX, and HIPAA. These reports aggregate audit data from monitored systems. For a detailed analysis of trends, event data from the cloud and on-premises targets can be combined, filtered and presented interactively or in static PDF and Excel format. Administrators can define threshold-based alerts on activities that may indicate attempts to gain unauthorized access and abuse system privileges on any of their databases.

Like Oracle Key Vault, AVDF is also a full stack security-hardened software appliance with a web-based management console. All network connections are encrypted and authenticated, and management duties are separated among distinct administrative roles. The following picture represents the AVDF Hybrid Cloud management architecture.

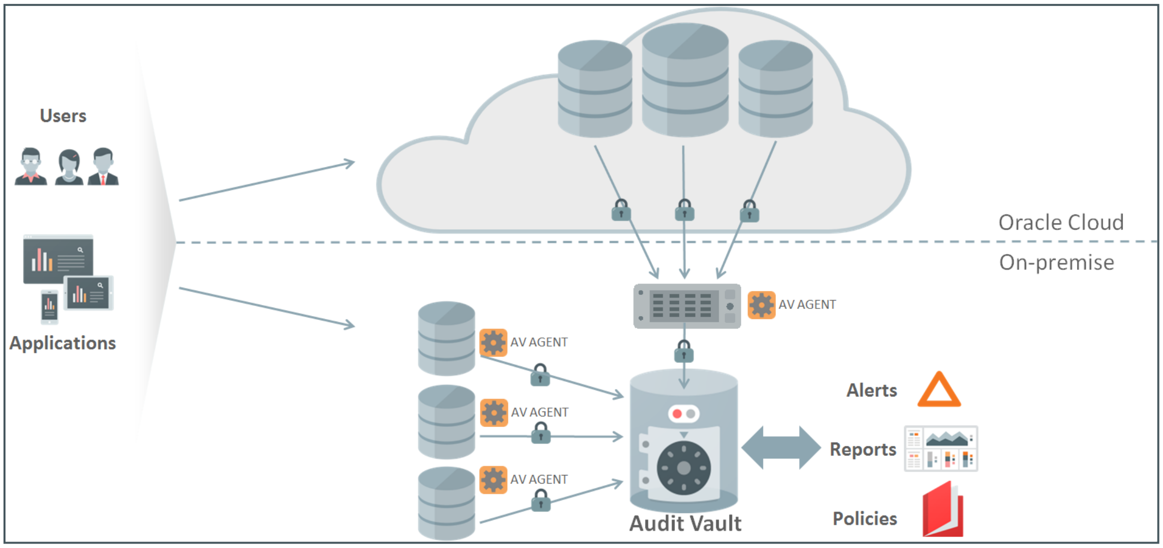

Figure 4: Oracle Audit Vault and Database Firewall monitor databases on-premises and in the cloud.

Centralized and Unified Security Policy Management

Whether an enterprise operating in Hybrid Cloud model or an SMB trying to lift-and-shift their on-premise applications to the cloud, having a centralized and unified policy management with a common user interface reduces overall complexity and decreases the likelihood of security incidents. Oracle Key Vault and Audit Vault provide centralized web-based user interfaces for managing Encryption Keys and Audit Records. In addition, ‘Oracle Enterprise Manager Cloud Control’ provides a common interface for managing data security policies in the Oracle Database on-premise and the Oracle Cloud.

Oracle Enterprise Manager Cloud Control 12.1.0.5 or above helps organizations to transparently migrate databases and the associated security policies between on-premise and the cloud environments using various data provisioning methods such as RMAN, Data Pump, Pluggable Database (PDB), and Snap Clone. Transparent migration of security settings and policies such as encryption settings, audit policies, access controls, and row level security controls from on-premise to the cloud and vice versa with zero application and database greatly simplifies the cloud migration efforts for organizations.

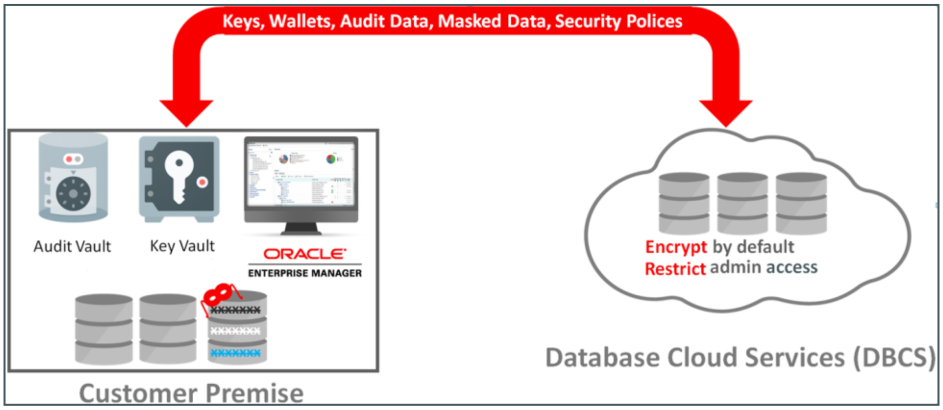
Keys, Wallets, Audit Data, Masked Data, Security Polices
Audit Vault
Key Vault
ORACLE ENTERPRISE MANAGER
Customer Premise
Encrypt by default
Restrict admin access
Database Cloud Services (DBCS)

Figure 5: A unified user interface provides visibility across the hybrid data center.

Defense-in-Depth with Transparency, Accuracy, Performance, and Scale

Modern applications contain multiple underlying components such as web gateways, web proxies, web servers, application servers, and database servers. Defining and implementing all the security controls in a multi-layered environment is a challenging task. Oracle Data Security technologies address this challenge by pushing controls closer to the data and enforcing security within the databases. Most of the data protection controls offered by Oracle are built into the Oracle Database. Securing data at the source not only simplifies the design and deployment but also improves the accuracy of protection, and minimizes the attack surface.

Oracle Key Vault and Oracle Audit Vault and Database Firewall complement the data protection at the source by centralizing the control and administration. Whether it is thousands of encryption keys, millions of audit records, or different types of security policies, these components can be managed centrally, greatly simplifying the administration related tasks. All Oracle Database Security controls are well integrated with each other to protect sensitive data.

Oracle has been the undisputed leader in data security for decades and has been developing security products for several years to help organizations address attacks from different threat vectors. Oracle Database whether on-premises or in the cloud offers many sophisticated assessment, preventive, and detective security controls. Some of the fundamental security controls such as Row Level Security and auditing has been there for more than a decade. Next generation data-centric security controls such as Data Redaction and Real Application Security help developers embed data security within the applications with zero or minimal changes. The following whitepaper discusses Oracle Database security controls for defense-in-depth security.

Whitepaper: Oracle Database Security and Compliance

The following table summarizes how different Oracle Data Security technologies mitigate different threat vectors.

Risk	Mitigation
Sensitive data exposure on test/dev/partner	Mask and subset before moving to cloud
Loss of clear-text data	Data is encrypted by default
Unauthorized access to encryption keys	Control keys with on-premise Key Vault

Unauthorized access by the cloud DBAs	Restrict DBA access with Database Vault
Unable to quickly detect breaches	Audit and monitor with on-premise Audit Vault and Database Firewall

Conclusion

Oracle's vision for data security in the cloud is based on the following principles:

- Security should be always-on
- Security should be pushed down the stack
- Customer should have control over the data
- Security policies should be same for on-premise and the Cloud

To implement the above principles, Oracle Database Cloud Service offers unique and differentiated set of the technologies to:

- Physically consolidate, manage, and control encryption keys and audit records
- Restrict the privileged users accessing sensitive data using Database Vault
- Mask and Subset sensitive information on-premise or in the Cloud
- Manage and migrate security policies using unified browser-based user interface

In addition, Oracle Database whether on-premise or in the cloud offers comprehensive assessment, preventive, and detective controls for maximum security.

Enterprises and SMBs (small and medium) businesses adopting or migrating to the cloud can accelerate their cloud journey by leveraging the data security technologies offered by Oracle Cloud for mitigating data privacy and security concerns.

References

- Oracle Cloud
- Oracle Database Cloud Service
- Oracle Data Security
- Whitepaper: Oracle Database Security and Compliance
- Whitepaper: Oracle Infrastructure and Platform Cloud Services Security

Bonus Content

Comparing Data Security in Oracle Database Cloud Service with Other Cloud Providers

The following table compares Data Security in Oracle Database Cloud Service with the database offerings of Amazon Web Services (AWS) and Microsoft Azure as of publication time.

	AWS AURORA	AZURE SQL DB	ORACLE CLOUD DB
Encrypt Data	✓	✓	✓
Control Encryption Keys On-Premises			✓
Restrict DBA Access to Sensitive Data			✓
Mask Sensitive Data for Test/Dev			✓
Collect Audit Records On-Premises			✓
Migrate Security Policies between Cloud and On-Premises			✓

- **Comparing Key Management**
  - Oracle Key Vault can be deployed on-premises to centrally collect and manage database encryption keys of on-premise and Oracle Cloud Databases. Also, users can suspend the encryption keys with the click of a button, making the application data not usable without shutting down the databases.
  - In comparison, Amazon Key Management and Azure Key Vault services are limited to their respective clouds. Customers cannot deploy these key management solutions on-premises to control encryption keys. Lack of direct ownership is a major issue for enterprises.
- **Comparing Privileged User Access Control**
  - Oracle Database Cloud Service provides Database Vault for restricting DBAs accessing sensitive information including Oracle Cloud administrators.
  - In comparison, AWS and Azure do not have Database Vault equivalent technology.
- **Comparing Data Masking and Subsetting**
  - Oracle Database Cloud Service provides Data Masking and Subsetting to discover, mask, and subset sensitive production information on-premises or in the Oracle Cloud.
  - In comparison, AWS and Azure does not provide Data Masking and Subsetting equivalent technology.
- **Comparing Cloud Database Audit and Monitoring**
  - Oracle Audit Vault can be deployed on-premise to centrally collect and manage auditing information of Oracle Databases on-premises and in the Oracle Cloud. Managing database auditing information off-site will minimize the chances of a potential attacker tampering the audit records.
  - In comparison, Amazon Cloud Watch (monitoring service), Amazon Cloud Trail (API auditing service), and Azure Security Center cannot be deployed on-premise to maintain database audit records off-site.

- **Comparing User Interfaces for Security Policy Management**
  - Oracle Enterprise Manager, Key Vault, and Audit Vault provide a unified user interface for managing data security components and policies such as encryption keys, wallets, audit records, audit policies, masking rules, database vault policies, row-level security policies, and more for Oracle Databases on-premise and in the Oracle Cloud. Customers can clone/migrate/transfer data security components and policies between their on-premise and Oracle Cloud environments.
  - In comparison, AWS and Azure do not provide a unified user interface to clone/migrate/transfer data security components policies between on-premises and the cloud databases.

ORACLE®

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services