ORACLE

混合雲資料安全的最佳實務

David Ueng
翁智泓　0927704816
david.x.ueng@oracle.com
Hybrid Cloud System Solution Engineer
Oracle Taiwan

Agenda

- 資料安全重要性
- 混合雲在資安方面所面臨的挑戰
- 資料備份在資安方面的挑戰
- 總結與Q&A

資料安全重要性

遭勒索攻擊的Colonial Pipeline花了大筆錢，換到不中用的解密工具
https://www.ithome.com.tw/news/144418

1. 彭博社報導指出，Colonial Pipeline付了近500萬美元的贖金來換取解密工具，但是駭客給的解密工具速度太慢，該公司依然得用自己的備份來復原系統，需要一周以上的時間才能讓營運完全恢復正常

2. 美國最大燃油管道系統Colonial Pipeline在（5/7）遭到勒索軟體DarkSide的攻擊，原本有媒體報導Colonial Pipeline無意支付贖金，但彭博社（Bloomberg）引述多名消息來源報導，Colonial Pipeline在意識到被攻擊之後的幾個小時之內，便已支付了接近500萬美元的贖金。

3. Colonial Pipeline肩負美國東岸45%的燃料供應，在遭到攻擊的當下暫停了所有的管道作業，使得美國燃油供應不足，油價更因此而上漲，讓美國於周日（5/9）宣布進入緊急狀態，破例讓燃油業者透過一般道路運送燃油。

4. 駭客通常是透過網釣取得系統的遠端存取帳號，再於受駭系統上注入勒索軟體，也提出完整的建議，包括啟用多因素認證、建立垃圾訊息過濾機制、過濾網路流量、定期更新軟體、限制特定資源的存取，以及部署防毒軟體等。

美國司法部：Equifax案是中國解放軍盜走1.5億名美國民眾個資

https://www.ithome.com.tw/news/135768

1. 美國司法部在本周指控了4名中國軍人，涉嫌在2017年入侵美國第三大消費者信用報告業者Equifax，**盜走了1.5億名美國消費者的個人資料，接近美國總人口數（3.3億）的一半，要求他們為其犯罪行為負責。**

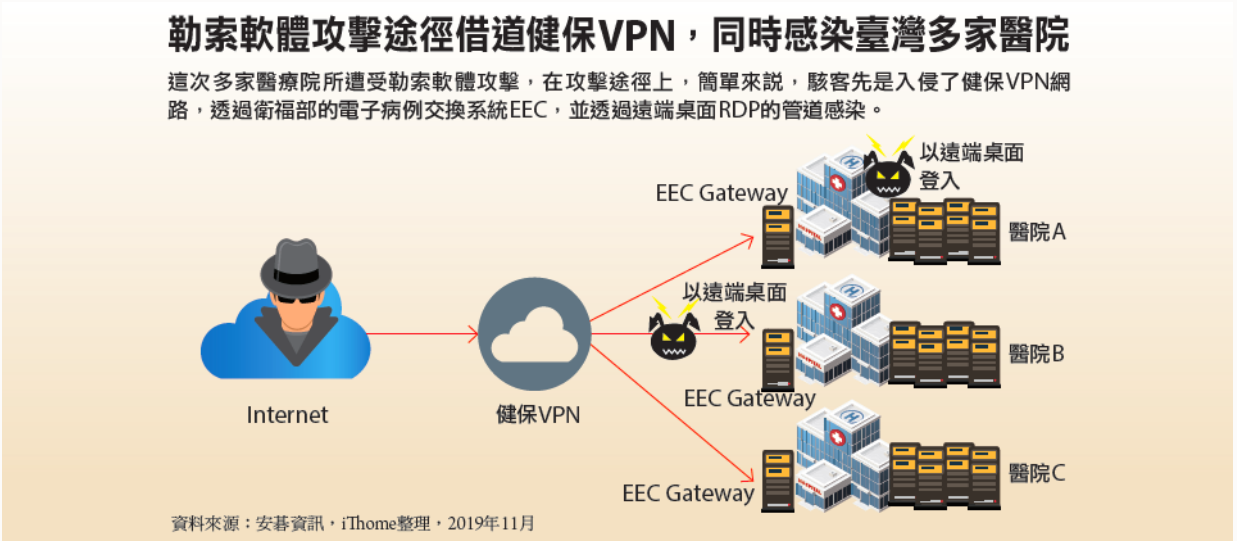
2. 外洩了1.5億名美國消費者的個人資料，包括**姓名、生日、社會安全碼，以及部分消費者的地址、電話號碼、駕照號碼、電子郵件帳號及信用卡資訊**等，在當時排名全球第五大資料外洩事件，僅次於Yahoo在2013年的30億、Yahoo在2014年的5億、MySpace的4.27億與LinkedIn的1.67億

亞太地區國家遭受惡意程式及勒索軟體攻擊遽增

1. 根據調查，駭客平均每天發動**5,000萬次密碼**攻擊，相當於**每秒579次**

2. 疫情爆發至今18個月，亞太地區遭受惡意程式攻擊的比率比疫情前平均提升19%，**遭受勒索軟體攻擊的比率平均提升240%。**

3. 台灣的惡意程式攻擊遭遇率增加了16%，**勒索軟體更增加了407%**，台灣勒索軟體遭遇率位居亞太地區排名**第五**，僅次於紐西蘭（825%）、日本（541%）、中國（463%）及澳洲（453%），顯示防止惡意軟體及勒索軟體攻擊在台灣企業防疫期間更是迫在眉睫。



多家品牌大廠遭收病毒團體勒索高額贖金

1. 蘋果筆電代工廠廣達遭駭客竊取大量資料，要求支付天價贖金。使用勒索軟體REvil的駭客組織宣稱已從**廣達**竊取「大量機密數據」，**駭客要求廣達在 4 月 27 日前支付 5000 萬美元（約新台幣 14 億元）贖金**，否則等到時限倒數結束後要**支付 1 億美元**贖金。廣達今天表示，已與外部技術專家合作，處理此次針對少部分伺服器的網路攻擊，公司日常營運未受影響。

2. 電腦品牌大廠**宏碁近日遭駭客攻擊，REvil 病毒團體勒索要求 5000 萬美元贖金**；宏碁回應表示，已將近期異常事件通報多國執法及資訊保護機關。
3. 筆電大廠「**仁寶電腦」（2324）及工業電腦大廠「研華科技」（2395），兩大廠被勒索的贖金，一共高達新台幣10億元！**

原文網址: 駭客入侵台灣10大企業！研華慘遭勒索10億　仁寶認栽付千萬贖金雲 https://finance.ettoday.net/news/1872347#ixzz78J6c97UL

混合雲在資訊安全方面所面臨的挑戰

混合雲成為趨勢

On-Premises

Cloud

"By 2022, over 90% of enterprises worldwide will be relying on a mix of on-premises/dedicated private clouds, multiple public clouds, and legacy platforms to meet their infrastructure needs."
— International Data Corporation (IDC)

混合雲在安全方面所面臨的挑戰

1

Data Security

2

Visibility
Control

3

Compliance
Governance

混合雲在安全方面所面臨的挑戰

1

Data Security

2

Visibility

Control

3

Compliance

Governance

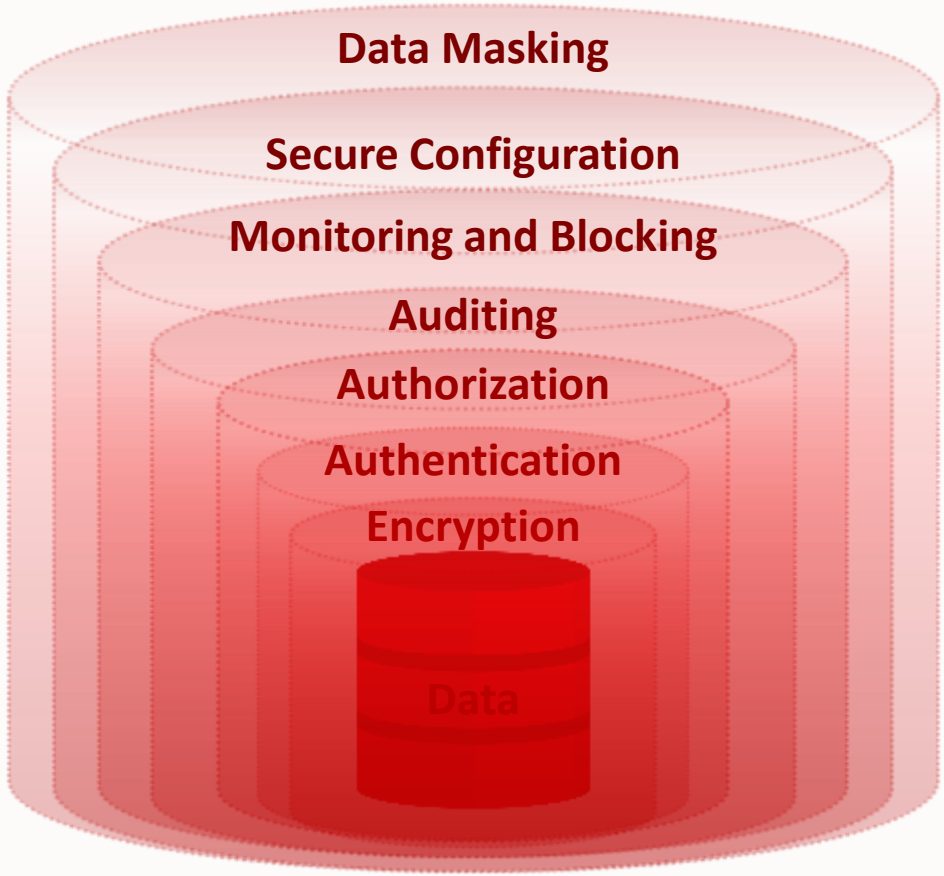
Database層內的深層防護

No single thing makes a database secure.

Securing a database is like securing your house – you need doors, locks on the windows, an alarm system, etc. Just locking the door does no good if the window is open

Securing an Oracle Database requires a combination of several “controls” working together to reduce risk

Only Oracle addresses every single one of these required control areas.



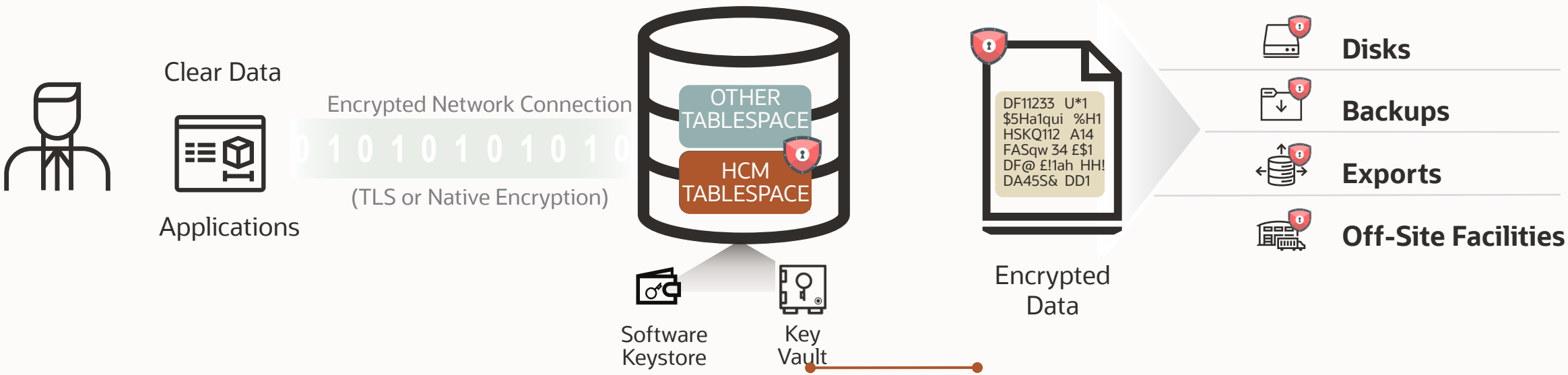
Data Redaction (Part of Advanced Security Option)

- Dynamic masking of application data based upon user name, IP, application context, and other session factors
- Library of redaction policies and point-and-click policy definition
- No impact on operational activities

建議的防護方法 – 加密與外部 Key Vault

Encrypt your Database & protect the keys

- Transparent Data Encryption (part of Advanced Security)
- Oracle Key Vault for key storage and distribution



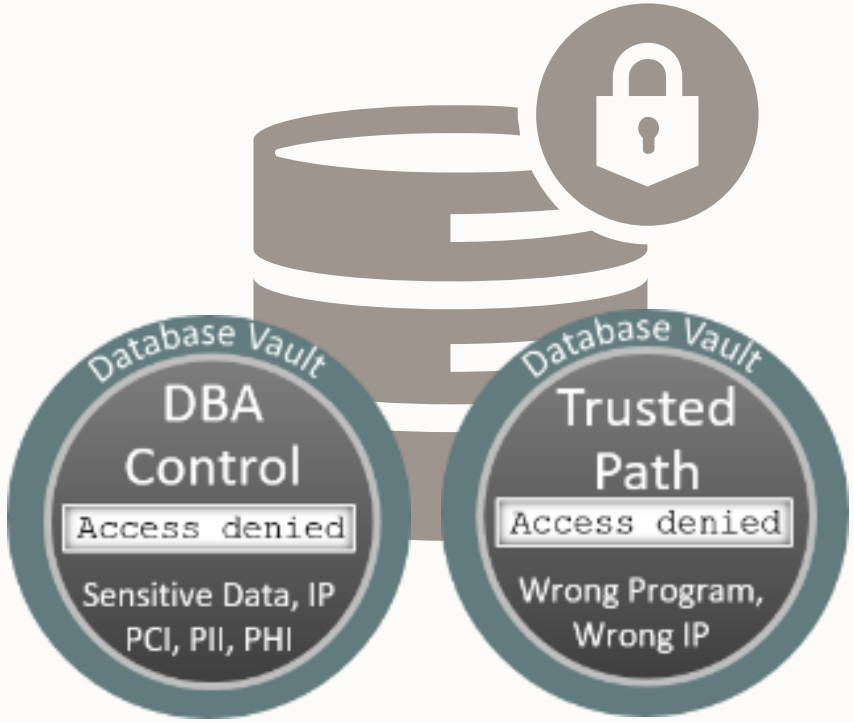
Worthless as a defense against ransomware : Storage level encryption, file system encryption

建議的防護方法 - Database Vault 限制且區分ＤＢＡ權限

Control access to data using Oracle Database Vault

Advanced Access Control

- Separation of duty
  - User administration
  - Database administration
  - Data administration
  - Fine-grained down to command / object level
- Context-aware authorization policies
  - Enforce a Trusted Path to Application Data
  - Rules based on IP address, operating system user, LDAP attributes, program, even time of day



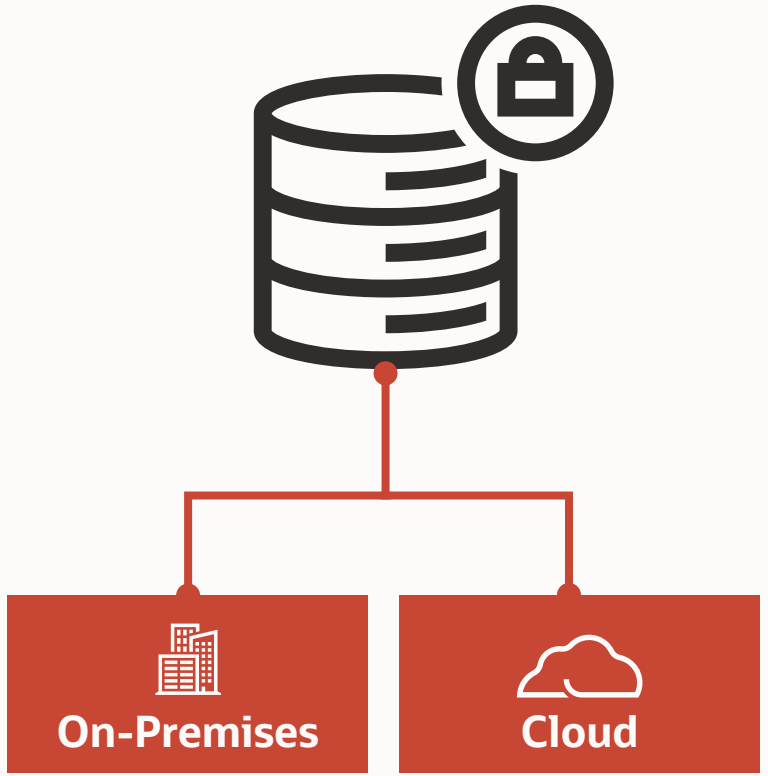
適用在On-Premise & Cloud上的Oracle Database Security

Gartner, Forrester, KuppingerCole, agree that **Oracle Database has the most advanced security controls in the market**

Customers might have databases on-premises, in the cloud, or in both places

Moving to the Cloud can be part of the journey or might happen to support specific use cases

Some customers risk profile/organization might want more control over their deployments or more automation



混合雲在安全方面所面臨的挑戰

1

Data Security

2

Visibility
Control

3

Compliance
Governance

Safeguard Your Data With Data Safe

Unified database security control center

- Risk dashboard: configuration, data, users
- Monitor user activity
- Discover sensitive data and mask it for test/dev
- Extensible: more features to come…

Benefits

- No special expertise needed: click-and-secure
- Saves time and mitigates security risks
- Defense-in-depth security for all customers

On-premises support

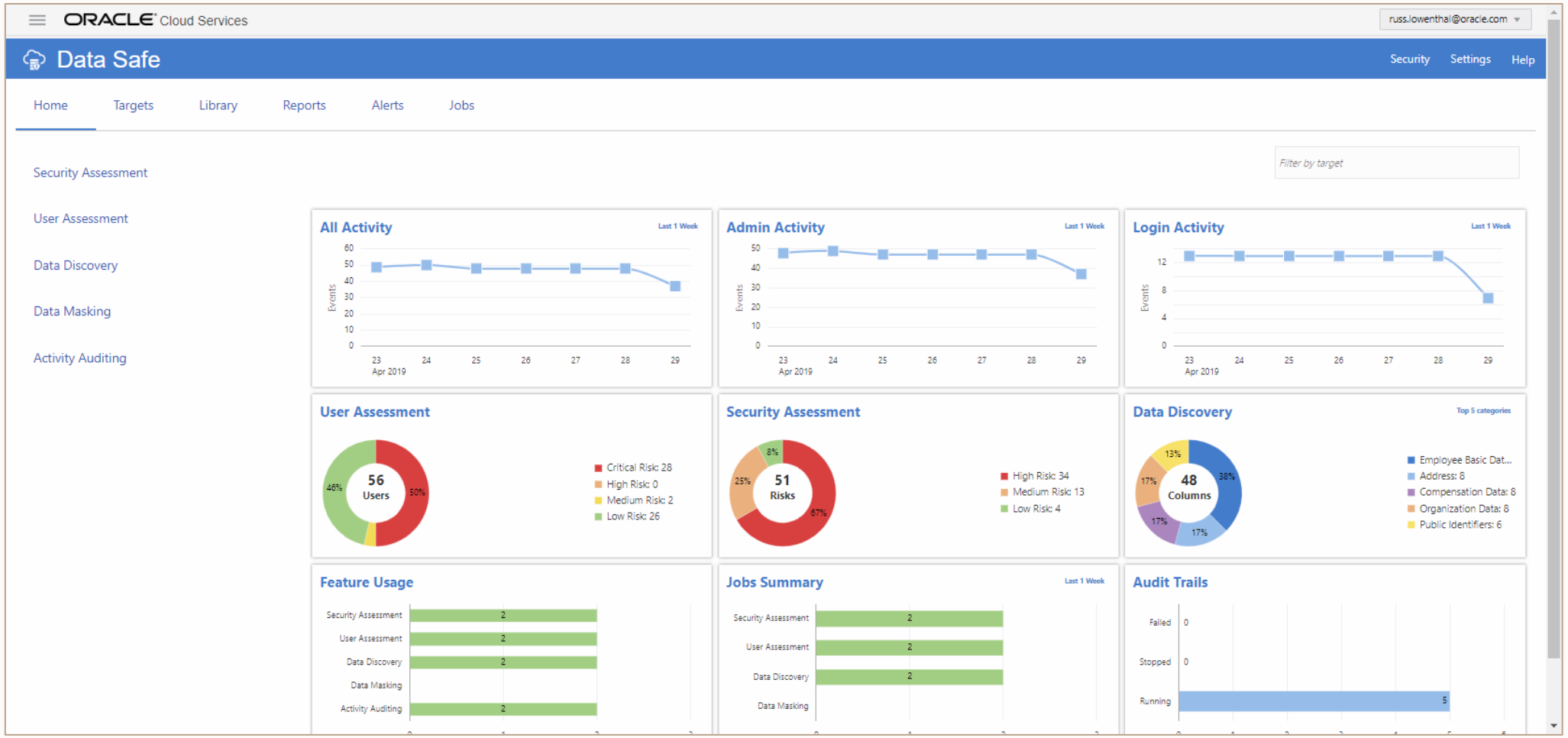
- Oracle database workloads including DB SE

Data Safe Main Components

Data safe comprises five components in a single integrated service and delivers this to any Oracle Database user

Security Assessment	User Assessment	Activity Auditing	Data Discovery	Data Masking

Data Safe : Visibility and Control

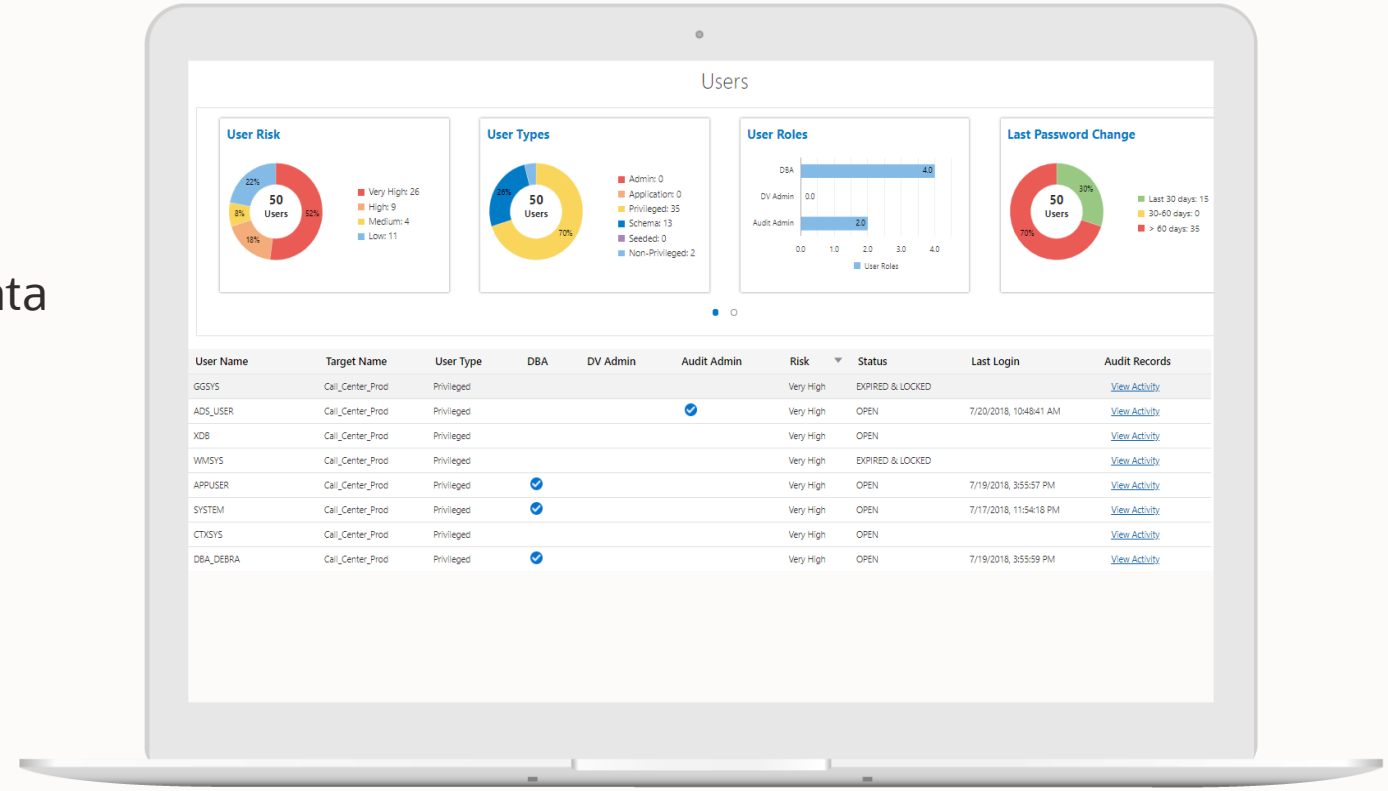


Data Safe : Visibility and Control

User Assessment

Reduce user risk by managing privileges and authentications and identifying risky behavior

- Identify over-privileged risky users
- Static profile: type of user, password policies
- Dynamic profile: last login, audit data



混合雲在安全方面所面臨的挑戰

1

Data Security

2

Visibility
Control

3

Compliance
Governance

Let DBSAT help assess your security profile

Understand how (in)secure is your database

- Database securely configured
- Identify privileged users and risks you carry
- Discover your sensitive data for regulations

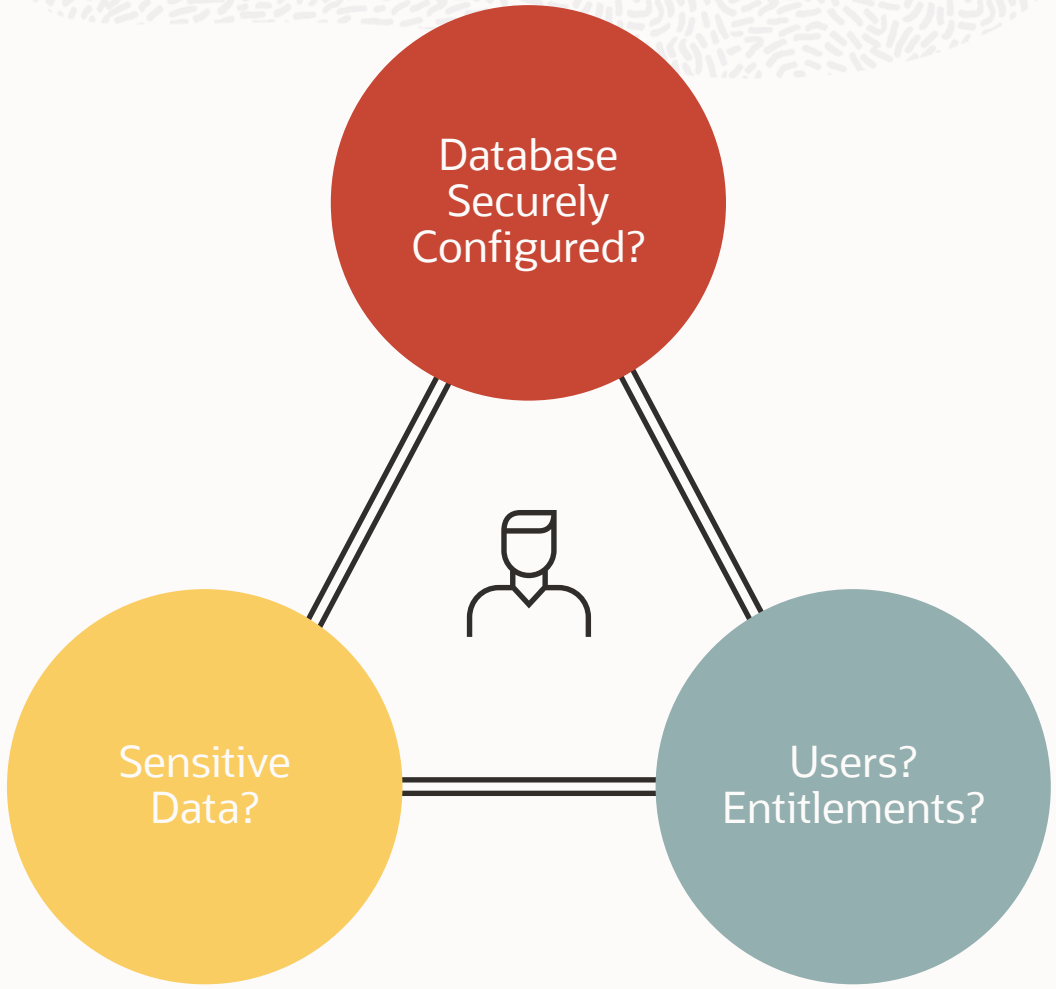
Actionable Reports

- Summary and detailed reports
- Prioritized recommendations
- **CIS, STIG, GDPR findings**

Analyze Oracle Database 11g and later

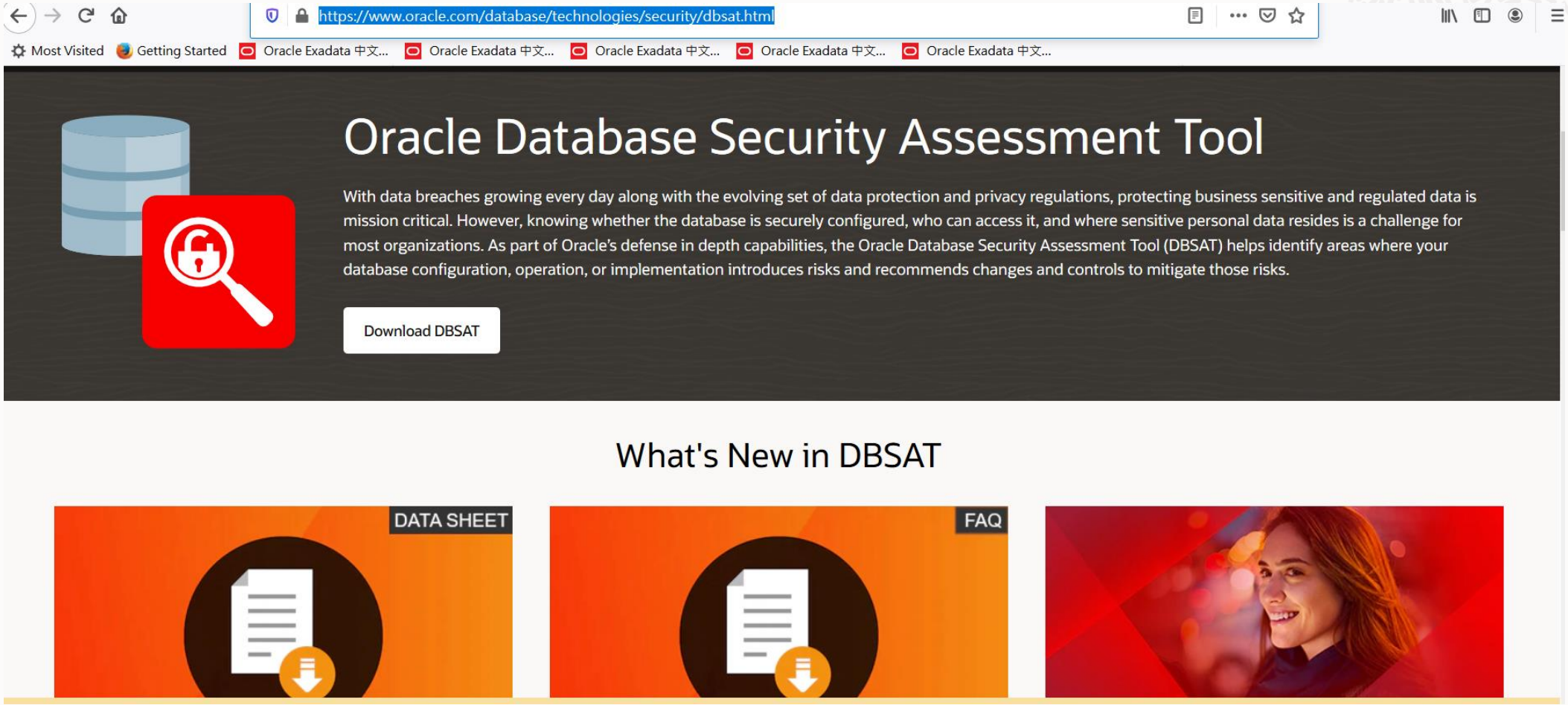
Stand-alone tool: Quick, Easy

FREE to current Oracle customers



Download DBSAT

https://www.oracle.com/database/technologies/security/dbsat.html



Using the Collector and Reporter

$ dbsat collect <database_connect_string> <output_file>

$./dbsat collect system **output_ORCL**

Reports

Summary

Section	Pass	Evaluate	Advisory	Low Risk	Medium Risk	High Risk	Total Findings
Basic Information	0	0	0	0	0	1	1
User Accounts	7	1	2	2	1	0	13
Privileges and Roles	4	17	1	0	0	0	22
Authorization Control	0	0	2	0	0	0	2
Fine-Grained Access Control	0	0	5	0	0	0	5
Auditing	0	7	6	0	0	0	13
Encryption	0	2	1	0	0	0	3
Database Configuration	8	3	0	1	0	1	13
Network Configuration	1	1	2	0	1	0	5
Operating System	1	2	0	1	1	0	5
Total	21	33	19	4	3	2	

Patch Check

INFO.PATCH — CIS STIG

Status	High Risk
Summary	Latest comprehensive patch not found.
Details	Latest comprehensive patch: Jul 06 2020 (451 days ago) Binary Patch Inventory: Patch ID (Comprehensive): 23688465 (created July 2020) SQL Patch History: Action time: Sun Mar 21 2021 18:01:37 Action: APPLY Version: 19.1.0.0.0 Description: OJVM RELEASE UPDATE: 19.8.0.0.200714 (31219897) Action time: Sun Mar 21 2021 18:01:37 Action: APPLY Version: 19.8.0.0.0 Description: Database Release Update : 19.8.0.0.200714 (31281355)

Client Nodes

NET.CLIENTS

Status	Medium Risk
Summary	Valid node check is not enabled, can accept connections from any client. Neith TCP.INVITED_NODES nor TCP.EXCLUDED_NODES is set.
Details	TCP.VALIDNODE_CHECKING is not set (default value = NO). Recommended v is YES. TCP.INVITED_NODES is not set. TCP.EXCLUDED_NODES is not set.
Remarks	TCP.VALIDNODE_CHECKING should be enabled to control which client nodes c database server. Either an allowlist containing client nodes(IP Address/Hostna allowed to connect (TCP.INVITED_NODES) or a blocklist of nodes that are not a (TCP.EXCLUDED_NODES) may be specified. Configuring both lists is an error; c node list will be used in this case.
References	Oracle Database 12c STIG v1 r10: Rule SV-75985r1, SV-76005r2, SV-76305r4

Inactive Users

USER.INACTIVE — STIG

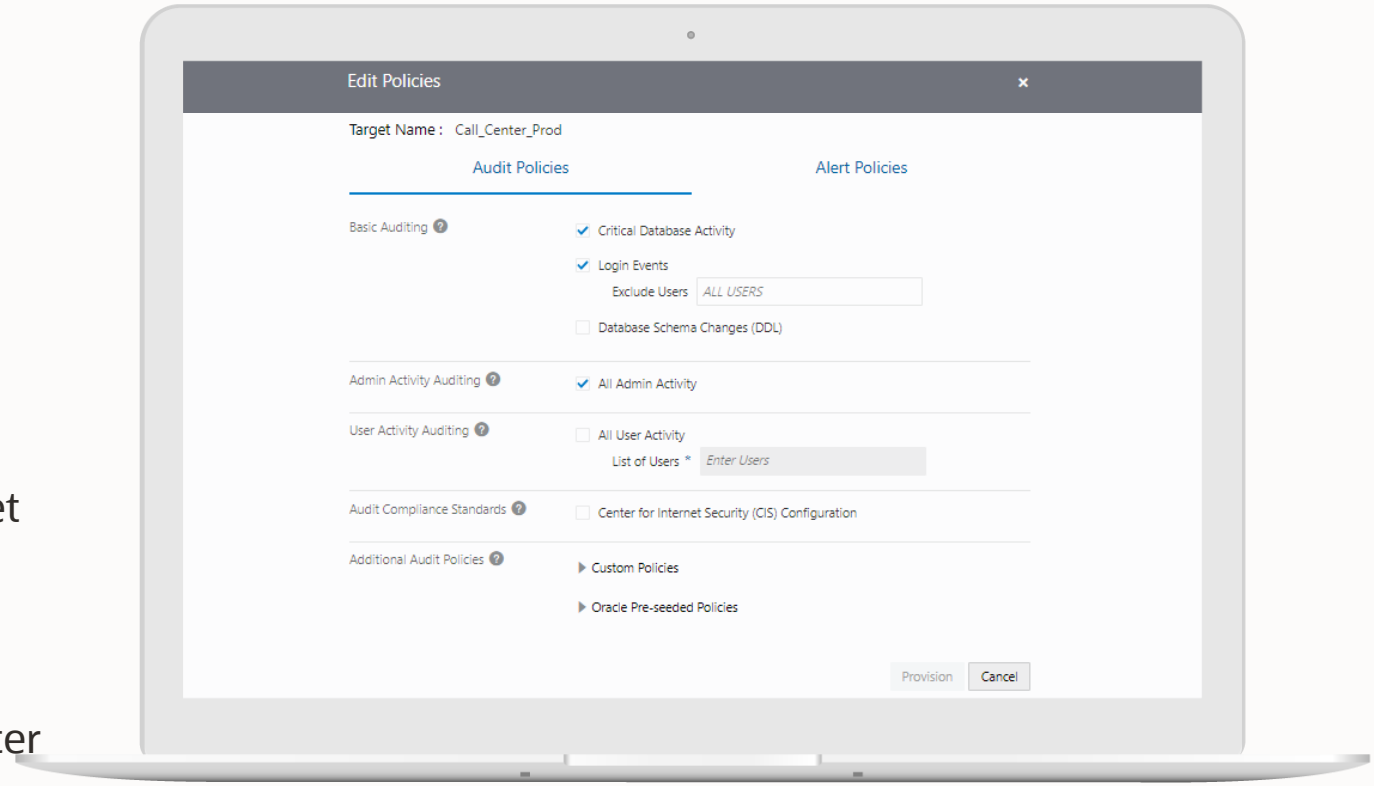
Status	Low Risk
Summary	Found 4 user accounts that would remain open even if inactive. Found 3 unlocked users inactive for more than 30 days.
Details	Users with unlimited INACTIVE_ACCOUNT_TIME: RAY, SYSTEM, T1, TEST1 Inactive users: RAY, T1, TEST1
Remarks	If a user account is no longer in use, it increases the attack surface of the system unnecessarily while providing no corresponding benefit. Furthermore, unauthorized use is less likely to be noticed when no one is regularly using the account. Accounts that have been unused for more than 30 days should be investigated to determine whether they should remain active. A solution is to set INACTIVE_ACCOUNT_TIME in the profiles assigned to users to automatically lock accounts that have not logged in to the database instance in a specified number of days. It is also recommended to audit infrequently used accounts for unauthorized activities.
References	Oracle Database 12c STIG v1 r10: Rule SV-76207r2

Data Safe : Compliance and Governance

Activity Auditing

Track user actions and streamline auditing with robust policy-based reporting

- Collect audit data from databases and track sensitive operations
- Provision audit, compliance, and alert policies
- Generate audit reports
  - Interactive and customizable reports
  - Summary and detailed reports
- Enable/Disable Weekly Auto Purge from target database. Default : Disable
- Audit Data Retention
  - Number of months for online and archive
- Option to continue /stop collect audit data after the free number of audit records is reached.

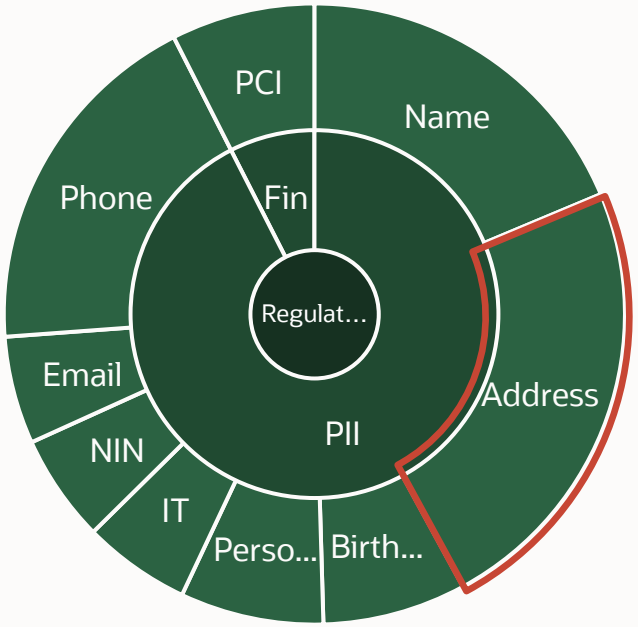


Data Safe : Compliance and Governance

Data Discovery

Prioritize security efforts by revealing the location, type, and amount of sensitive data within the database

- Discovers and classifies 120+ sensitive data types
  - Name, address, SSN, salary, medical health, payment card information and many more
- Supports user-defined sensitive data types
- Supports incremental discovery
- Reports amount and type of sensitive data



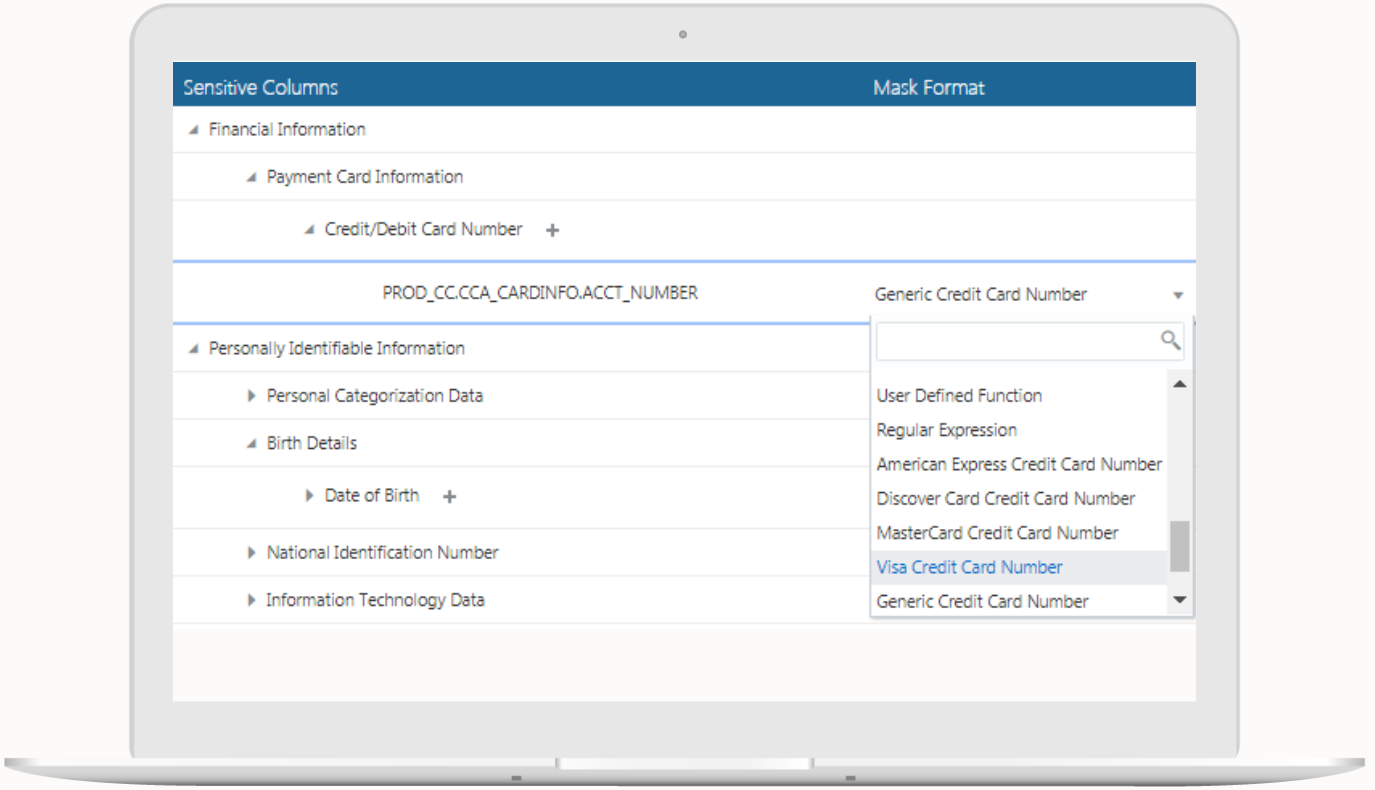
16.6K Sensitive Values	12 Sensitive Types
4 Sensitive Tables	17 Sensitive Columns

Data Safe : Data Security, Compliance and Governance

Data Masking

Minimize risk by replacing sensitive data with realistic yet obscured data for use in development, test, and partner environments

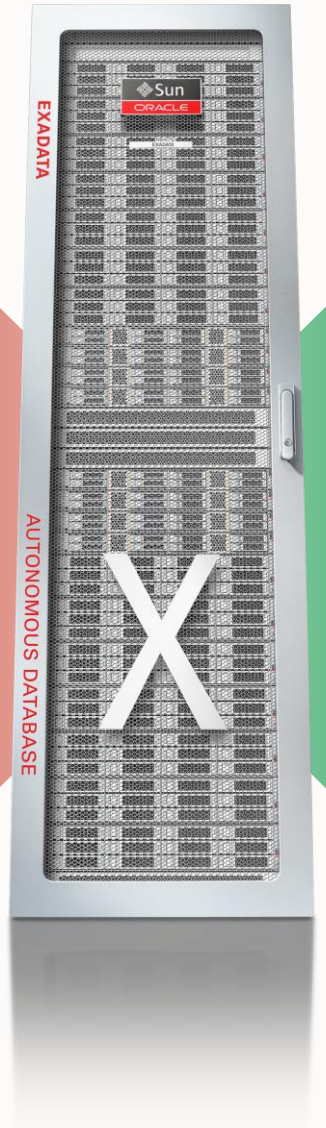
- Mask data identified as sensitive
- 45+ pre-defined masking formats
- Masking transformations
- Masking reports



企業級平台 Industry Hardened Full-Stack Security – Exadata 軟硬體整合

Exadata Database Machine Security

- Industry policing: Banks, Government, Retail, Telcos
- Advanced Intrusion Detection Environment (AIDE)
- Regular security scans
- FIPS 140-2 certification
- PCI-DSS compliance
- Data and network encryption
- Linux minimal distribution
- Secure erase
- System lockdown
- Live kernel patching



Oracle Database Maximum Security Architecture

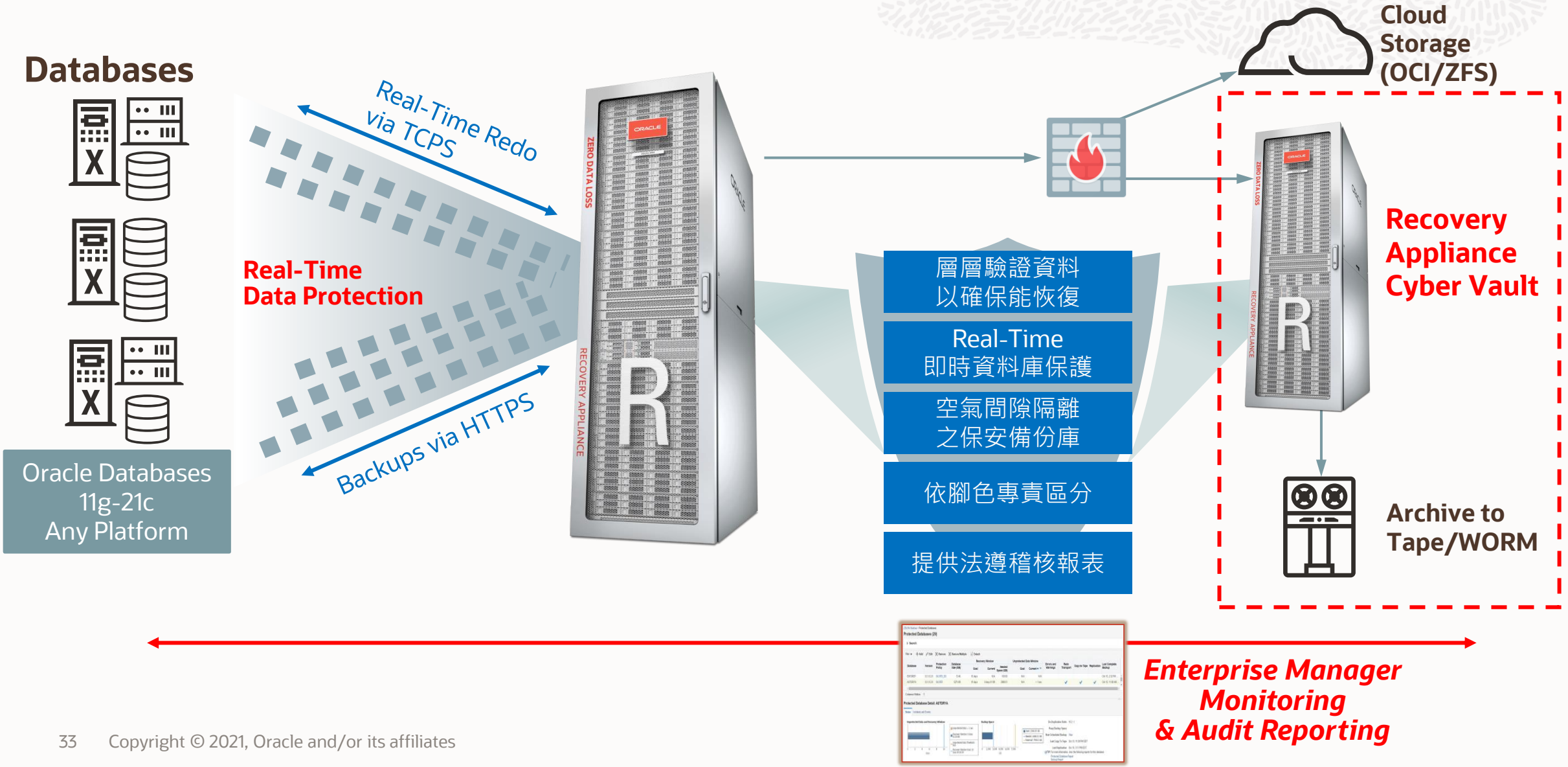
- Identity Management
- Transparent Data Encryption
- Network Encryption
- Database Vault
- Audit Vault
- Key Vault
- Database Firewall
- Virtual Private Database
- Label Security
- Data Redaction
- Data Masking & Subsetting

資料備份在資安方面的挑戰

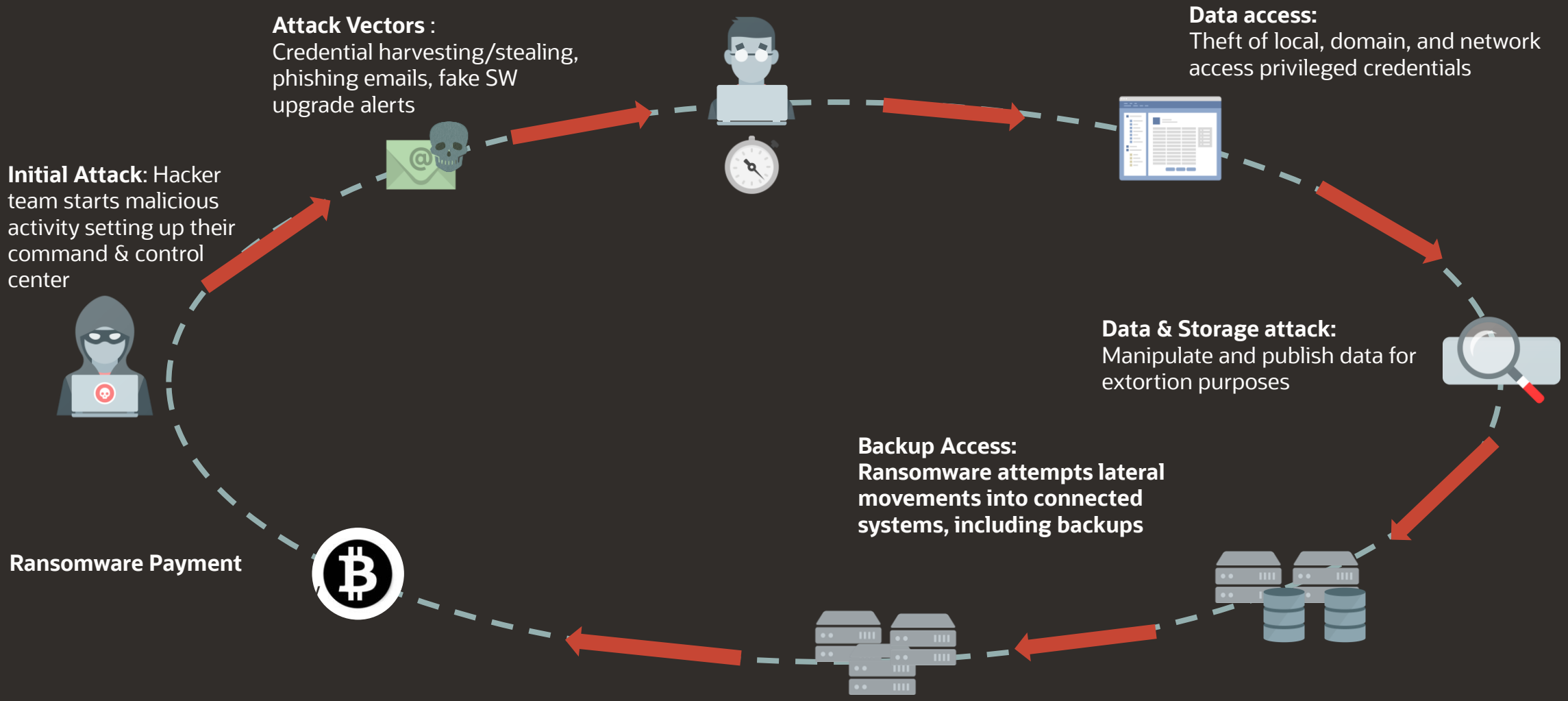
Recovery is Everything, 恢復力是最終手段

Recovery Appliance Cyber Security Architecture

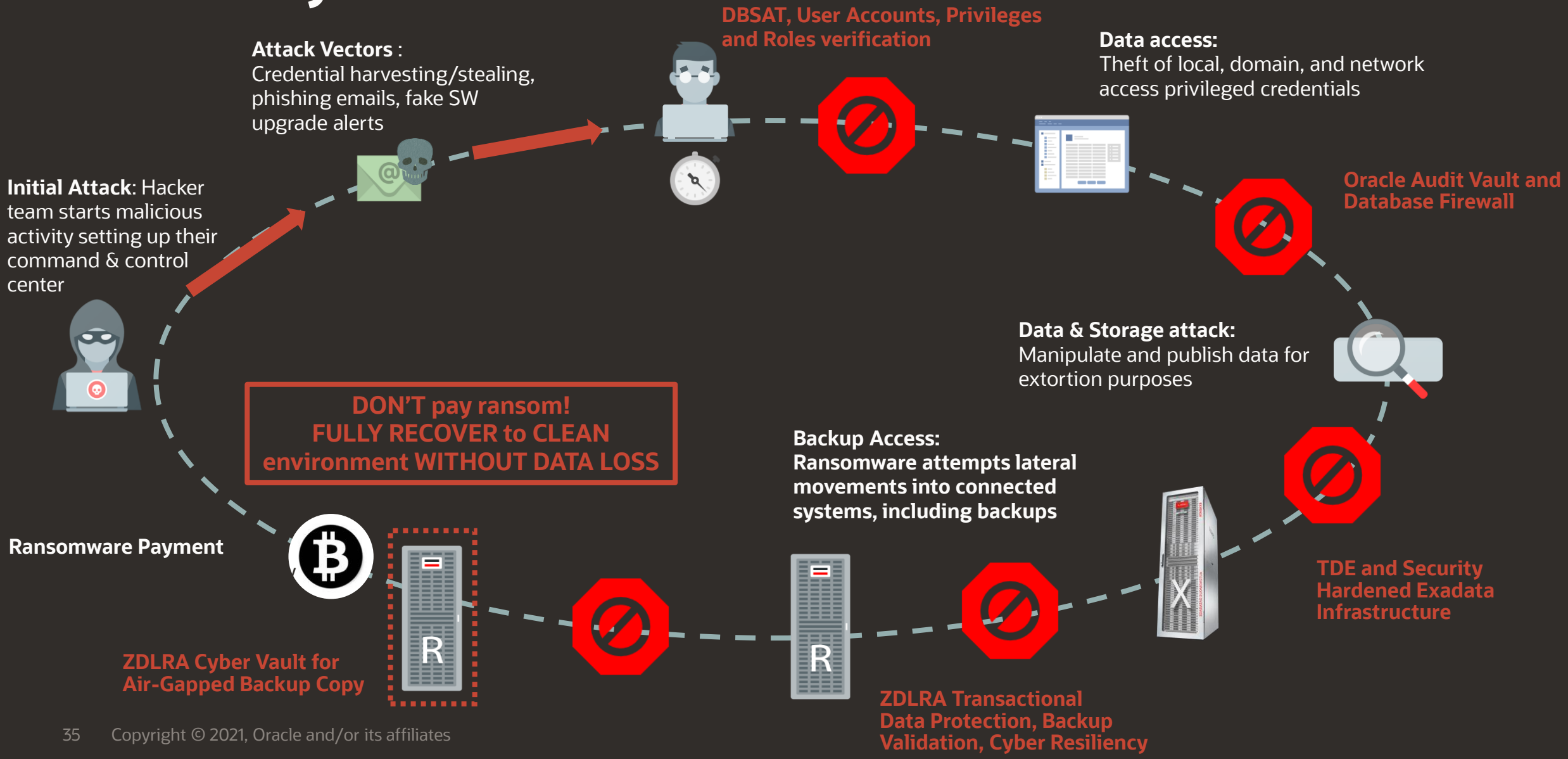
Solution Blueprint for Protecting and Recovering from Ransomware Attacks



Oracle Layered Ransomware Defense & Protection



Oracle Layered Ransomware Defense & Protection



Exadata + Recovery Appliance : 安全滿分

Best in Class Security Database Platform + Data Protection

Most efficient backup/recovery possible

- *Minimal processing impact on PRODUCTION storage, SAN, servers, WAN*
- *Use system resources for transacting business, not running backups*

Provides validated recoverability

- *Never worry again about recoverability of backups (compliance/audit reports)*
- *Real-Time view to recoverability status (mitigate risk, peace of mind)*

Protection from ransomware

- *Cyber vault architecture ensures backups are not impacted by malicious attacks*

Q&A