ORACLE

Oracle Energy and Water
Customer Edge
Conference

Securing Your Data in Oracle Cloud

Keep utilities IT systems secure

Hafid Elabdellaoui
VP Cybersecurity

Natalie Leykin
Senior Director, Product Development

Oracle Energy and Water Business Unit

March 13, 2023

Speakers

Hafid Elabdellaoui
VP Cybersecurity

Natalie Leykin
Senior Director, Product Development

Safe harbor statement

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

Securing Customer Data and Infrastructure & Integration Security

Agenda:

- Current threat landscape
- Integrating security in the EWGBU development lifecycle
- Data encryption by default
- Customer data protection
- Integration security challenges
- Different security protocols
- E&W integrations:
  - OIC Utilities Adapter security
- Use cases :
  - How to connect to the 3rd party system
  - Multiple security zones

Treat escalation in critical infrastructure

Oracle's focus on securing customer data and infrastructure

Threat landscape

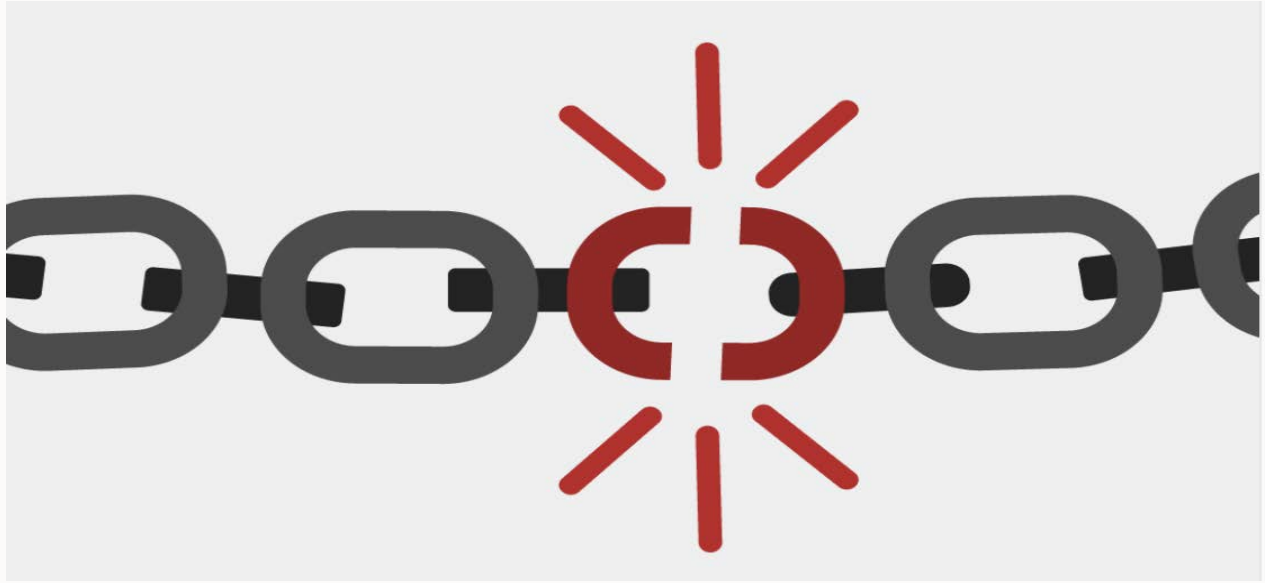
- Nation States & geopolitical conflicts

Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion

Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion
- Supply chain compromise is top of mind for every organization

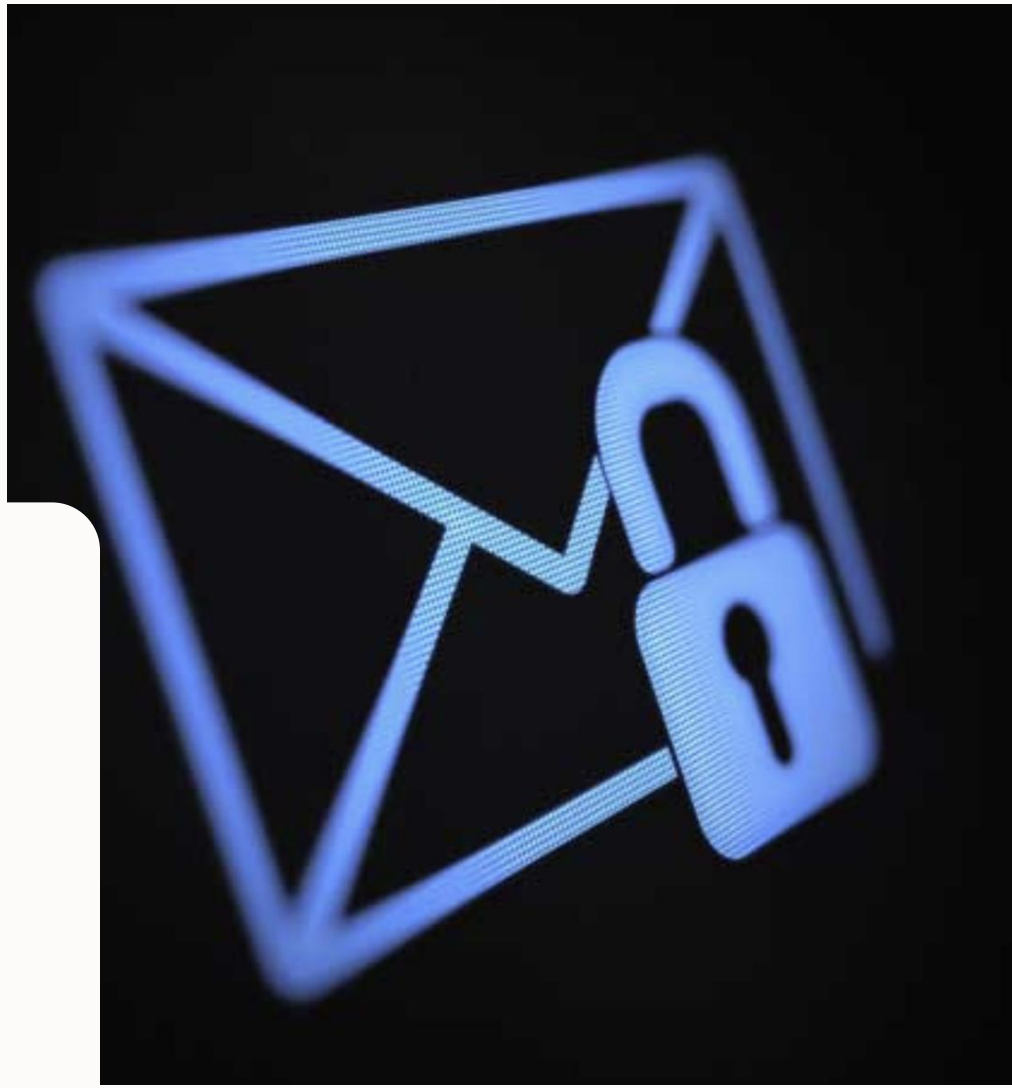


Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion
- Supply chain compromise is top of mind for every organization
- Common misconfigurations lead to compromise

Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion
- Supply chain compromise is top of mind for every organization
- Common misconfigurations lead to compromise
- Identity attacks continue to be prominent
- Phishing led compromises slowing but becoming more targeted



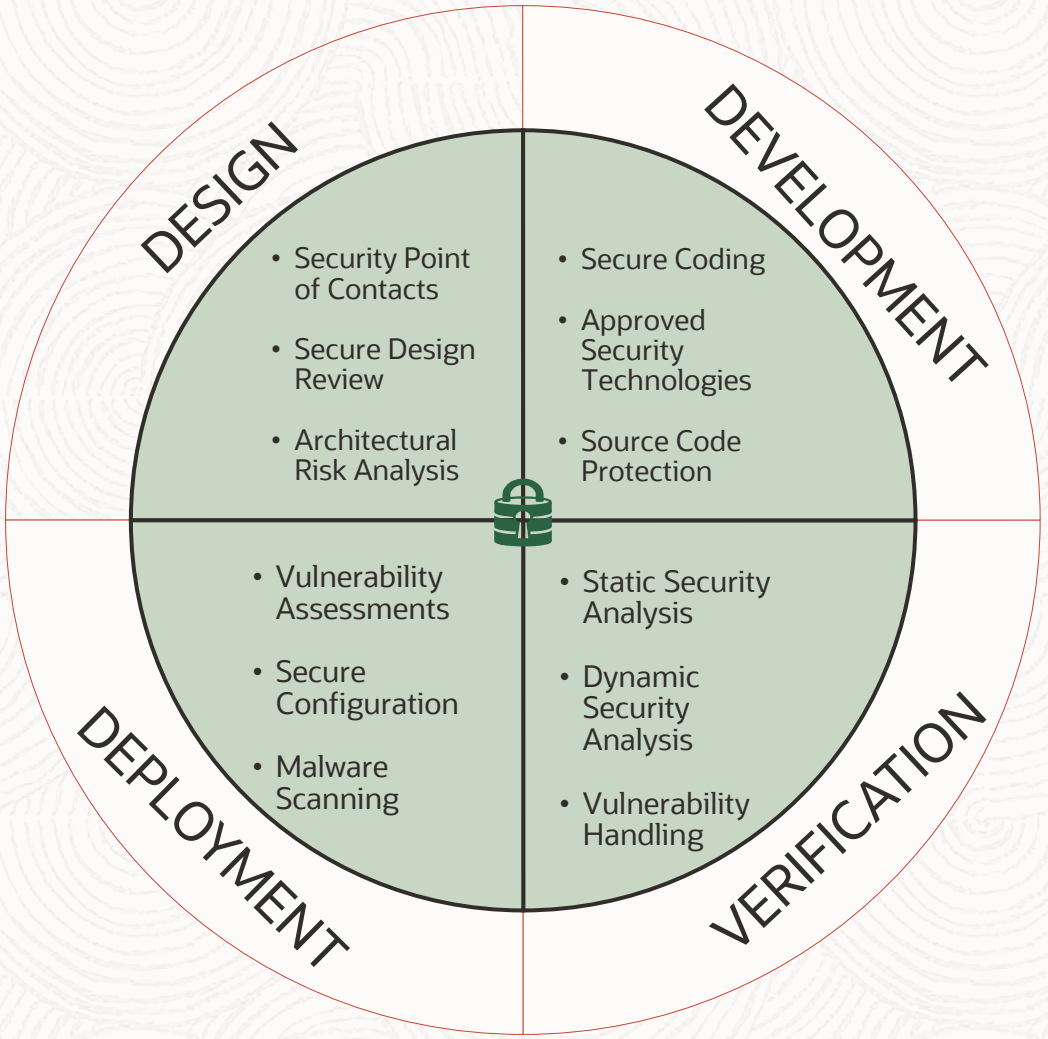
Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion
- Supply chain compromise is top of mind for every organization
- Common misconfigurations lead to compromise
- Identity attacks continue to be prominent
- Phishing led compromises slowing but becoming more targeted
- Intrusions and data exfiltration continually using encrypted channels to avoid detection

Threat landscape

- Nation States & geopolitical conflicts
- Ransomware – multifaceted extortion
- Supply chain compromise is top of mind for every organization
- Common misconfigurations lead to compromise
- Identity attacks continue to be prominent
- Phishing led compromises slowing but becoming more targeted
- Intrusions and data exfiltration continually using encrypted channels to avoid detection
- Over 2800 threat groups globally being tracked by Mandiant
  - 1,100 threat groups were new in 2021

Robust development practices built into every phase of the lifecycle



Security & Privacy across the Product Lifecycle

Oracle's Software Security Assurance (OSSA) model incorporates resiliency into the design, build, test & maintenance of products.

- Reduces occurrences of security weaknesses in Oracle products
- Deploying and maintaining Cloud Services in a fully secure configuration
- Identification of weaknesses and security risks through pro-active analysis and testing
- Expedited remediation of weaknesses with transparent disclosure and documentation policies

Data Encryption

Data Encryption in transit

TLS is implemented or configurable for all web-based TLS-certified applications deployed at Oracle: SaaS, Cloud Portal, APIs

If access is through a TLS enabled connection

- that connection is negotiated for at least 128 bit encryption using either RSA or Elliptic Curve Cryptography (ECC).
- The private key used to generate the cipher key is at least 2048 bits

Data encryption at rest

Transparent Data Encryption (TDE) protects all data at rest by default

- Data in the database files is protected (DBF files are encrypted)
- Each tablespace within the DB has its own encryption key
- Tablespace keys are stored and encrypted (AES-256) within the Oracle Wallet by the master encryption key, unique to each tenant
- Backups are also encrypted with tenant specific keys
- Break Glass & BYOK allows for customer managed keys

Break Glass & Bring Your Own Key (BYOK)

Break Glass (Workflow)

- Restricts Oracle access to customer data
- Oracle personnel require customer approval before accessing customer data
- Based on Principle of Least Privilege
- Time boxed
- Audit reports of all Oracle activity provided

Bring Your Own Key (ROADMAP)

- Customers provide and manage the Transparent Data Encryption (TDE) encryption keys used to encrypt the cloud service data
- Customers manage key rotation, access and revocation
- Requires subscription to OCI Vault

Benefits:

- Additional security controls to safeguard customer data
- Supports compliance with local regulations around data control and ownership

Integration security challenges

E&W integrations use cases

Integration security concerns

Some of the main concerns around integration security include:

- Data security
- System security
- Network security
- Application security
- User access control

Overall, integration security is important to protect against data breaches, unauthorized access, and other security threats

Integration security challenges

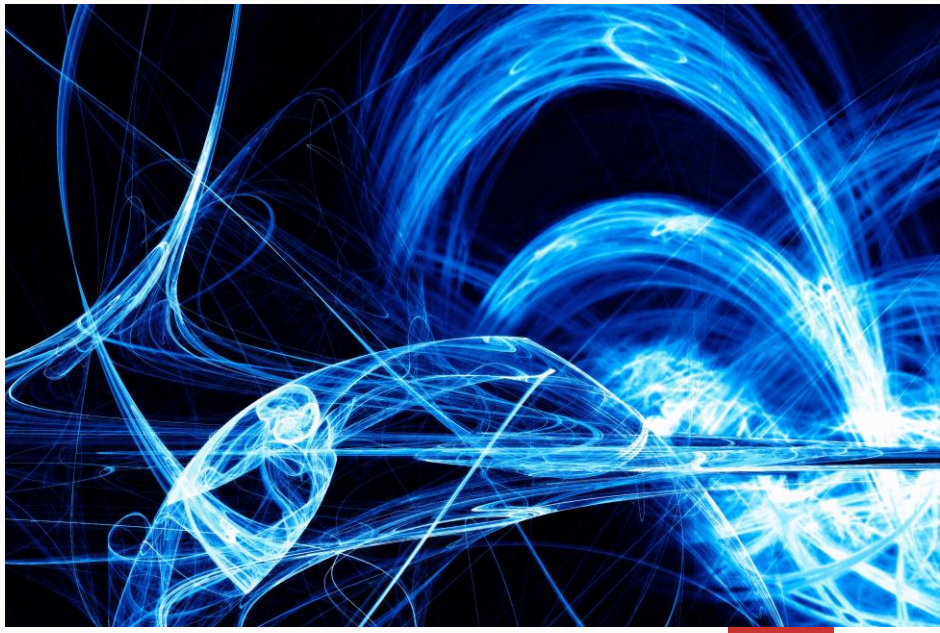
- Different landscape (premise/cloud, oracle and non-oracle)
- Different security protocols and requirements
- Security segmentation
- Password rotation

Security protocols

Basic Authentication vs. OAuth: Key Differences

Oracle is moving away from the password-based Basic Authentication

- What is Basic Authentication?
  - Basic authentication only requires user ID and password to access their account.
  - The user's credentials are sent from the application for every request
- What is Modern Authentication?
  - Uses tokens provided by an identity provider instead of the actual password of the user's account
  - These specify additional rules for accessing the account, such as
    - An expiration date
    - Which application can use the token



Security protocols

Why OAuth 2.0 is better than basic auth?

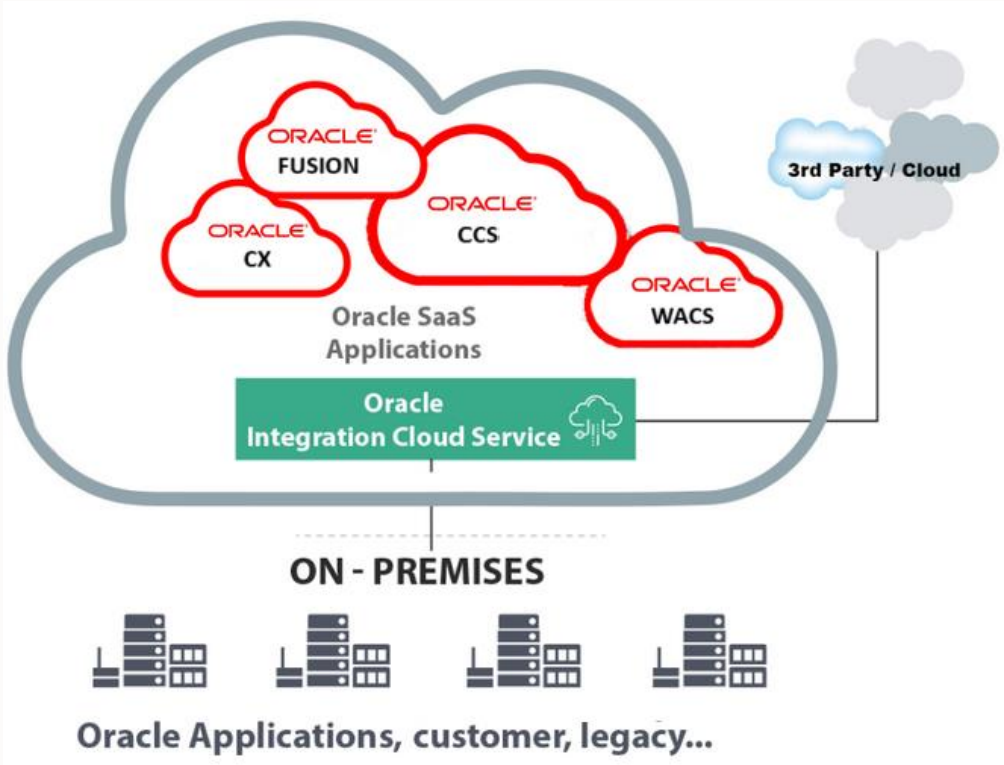
Unlike Basic Auth, OAuth doesn't give away your password. This keeps your credentials safe.

- Benefits of Using OAuth
  - The user does not need to share login credentials with the client.
  - The client is only permitted to access specific parts of a user’s resource.
  - Tokens can easily be revoked if the user unauthorizes a client without modifying any login credentials.
  - OAuth ensures that access tokens are shared via a secure channel.
  - A user does not need to create multiple accounts on different third-party applications.

OAuth is the way to go!

Oracle Integration Cloud (OIC)

- Simplified integration
  - Simplified design time and runtime console
  - Web based point and click integration experience
- Increased business agility
  - Connectivity agents and pre-built adapters
  - Faster deployment and Monitoring capabilities
  - Customization and extension using Oracle Cloud SDK
- Security and Redundancy
  - Managed Oracle backups, patches and upgrades
  - Secure and highly available with clustering
- Faster time-to-market
  - Configuration approach
  - Prebuilt integrations and commonly used adapters



Demo OIC Connection setup

OIC Utility Adapter

What type of security is supported?

23A

- OAuth support - no username/psw for REST inbound into OUAF
- OAuth support - no username/psw for REST inbound into NMS

23B

- OAuth support - no username/psw for REST outbound from OUAF
- OAuth support - no username/psw for REST outbound from NMS
- OAuth support - no username/psw for SOAP inbound into OUAF
- OAuth support - no username/psw for SOAP outbound from OUAF

Use cases

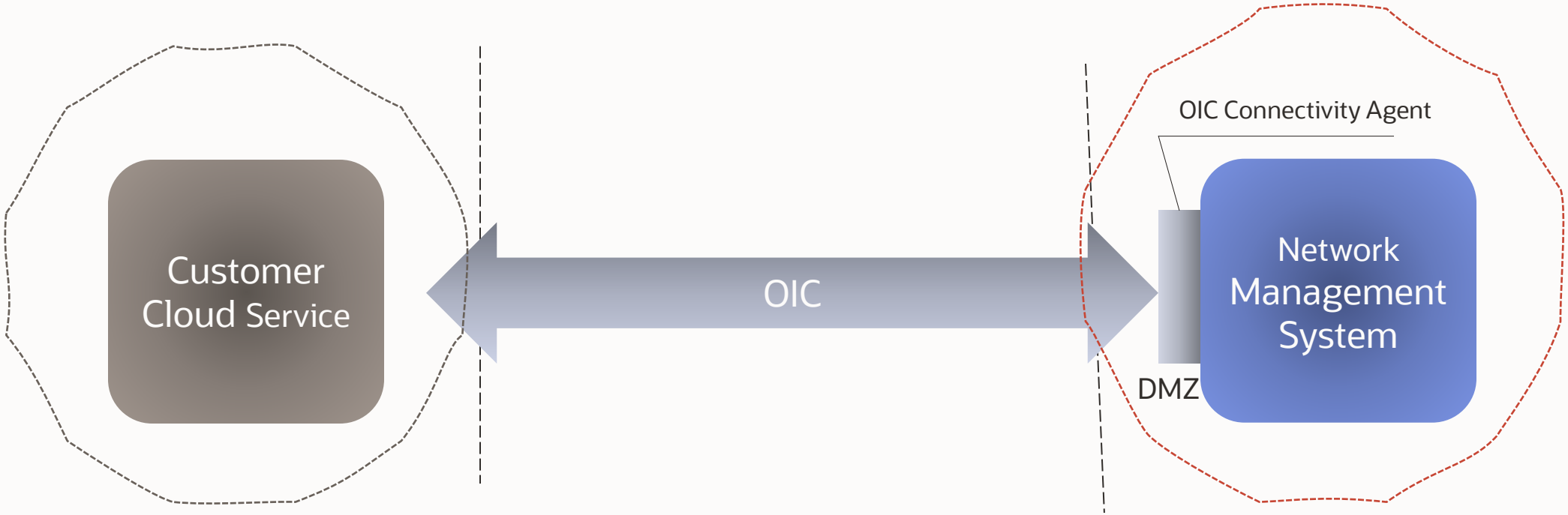
How to connect to the 3rd party systems

Legacy systems may not have advance security protocols, even if no web services. How to integrate?

- One of the solutions – use file extracts
- Place a file in sftp location or Object Storage
- Modify the file and transfer it using OIC
- OUAF applications can upload the file, or it can be parsed by OIC and submitted record-by record

Use cases

Multiple security tiers



Low security tier

Oracle Utilities Customer Cloud Service

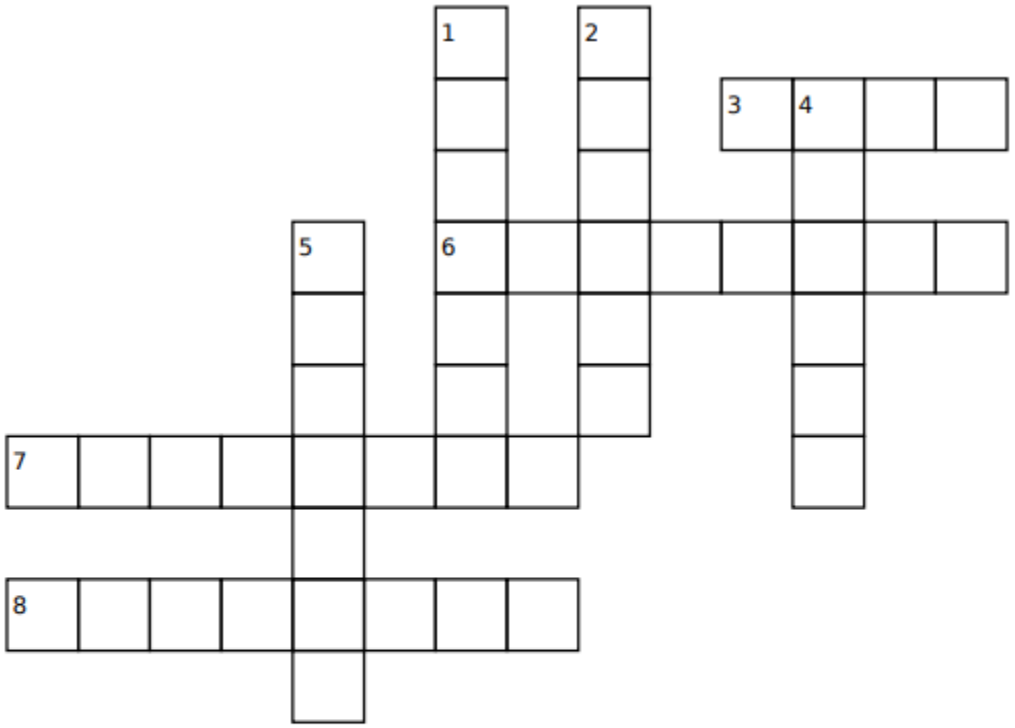
Medium security tier

Oracle Integration Cloud

High security tier

Oracle Utilities Network Management System

Crossword puzzle



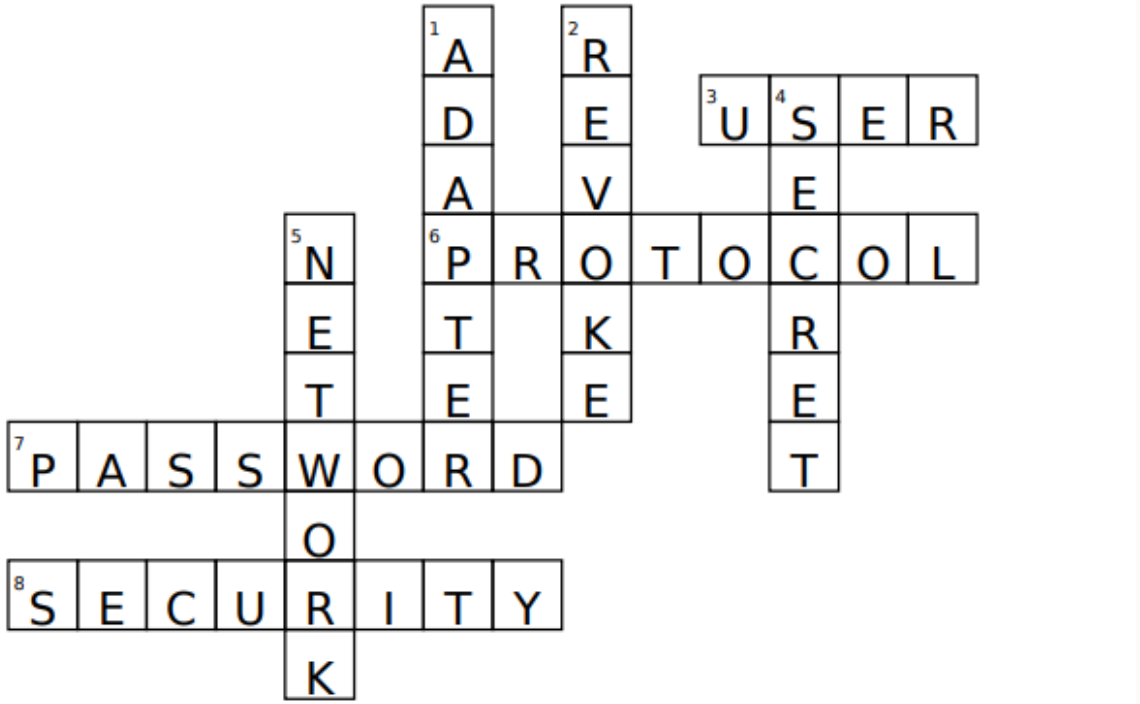
Down:

1. the interface for computers and other devices to connect to a network
2. put an end to the validity or operation
4. not meant to be known or seen by others
5. two or more computers

Across:

3. a person who uses or operates something
6. an agreed sequence of actions performed by two or more communicating entities
7. a secret word or phrase
8. the state of being free from danger or threat

Crossword puzzle (with answers)



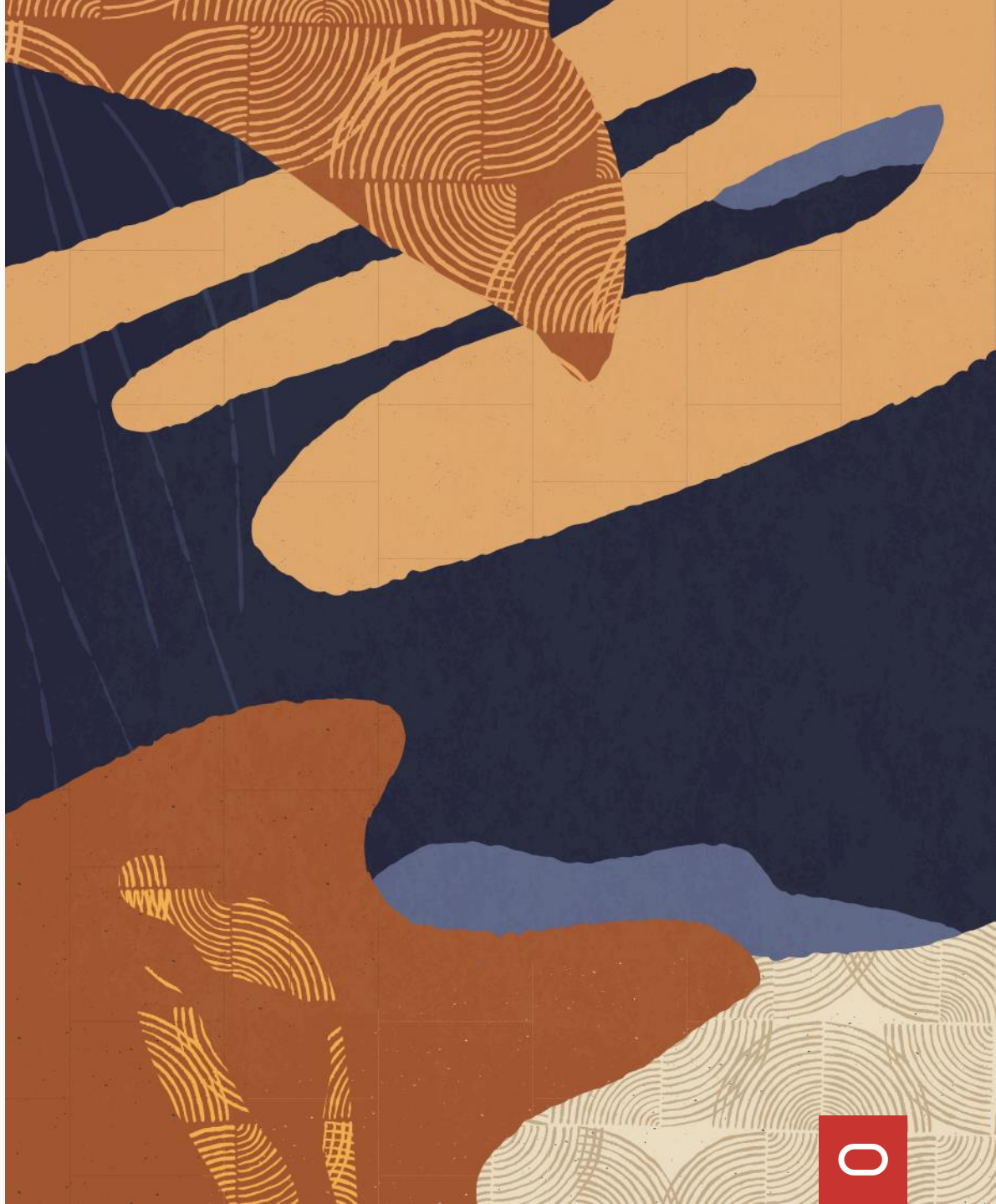
Down:

1. the interface for computers and other devices to connect to a network
2. put an end to the validity or operation
4. not meant to be known or seen by others
5. two or more computers

Across:

3. a person who uses or operates something
6. an agreed sequence of actions performed by two or more communicating entities
7. a secret word or phrase
8. the state of being free from danger or threat

Thank you




ORACLE