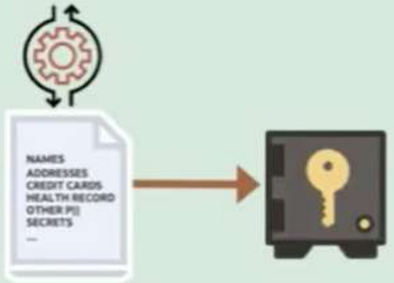
ORACLE
University

Oracle Cloud Infrastructure

Database Maximum Security Architecture

Securing Data at Its Source

How do you protect the database?

Implement a secure configuration and monitor for configuration drift.	Encrypt the data and protect the encryption keys.	Control access to the data.	Monitor access to the data.
			
› Ensure your database configuration follows policy. › Monitor for configuration drift.	› Encrypt data in motion and at rest. › Protect against network sniffing attacks. › Protect against data scraping attacks (for example, ransomware).	› Enforce least privilege. › Control privileged user access to data. › Enforce separation of duties. › Establish and enforce a trusted path to data.	› Use native auditing capabilities to capture high-value activity. › Use network-based monitoring to examine ALL activity.

Securing the Oracle Database

Getting Down to Details

- Database *Strong Authentication*
- Database *Centrally Managed Users*
- Database *IAM integration*
- Database *Password Profiles*

- Advanced Security *Transparent Data Encryption*
- Key Vault
- Database *Native Network Encryption*
- Database *Transport Layer Security (TLS)*

- Database *Roles and Privileges*
- Database *Centrally Managed Users*
- Database *Virtual Private Database*
- Database *Real Application Security*
- Database *Blockchain and Immutable Tables*
- Database Vault
- Label Security
- Advanced Security *Data Redaction*

- Data Safe *User Assessment*
- Database Security Assessment Tool
- Database *Privilege Analysis*
- Data Safe *Masking*
- Data Masking and Subsetting

- Database *Unified Auditing*
- Audit Vault and Database Firewall
- Data Safe *Auditing*

- Database Security Assessment Tool
- Data Safe *Security Assessment*

Legend

Feature · Option · Product · Service

Security Zones of Control

Assess

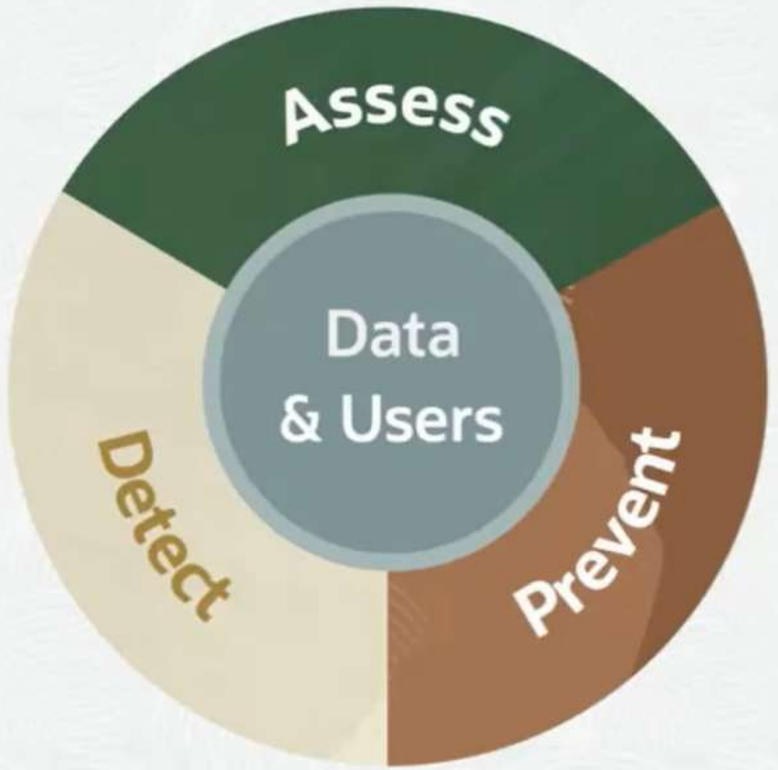
Assess the current state of the database.

Detect

Detect attempts to access data, especially attempts that violate policy.

Prevent

Prevent inappropriate or out-of-policy access to data.



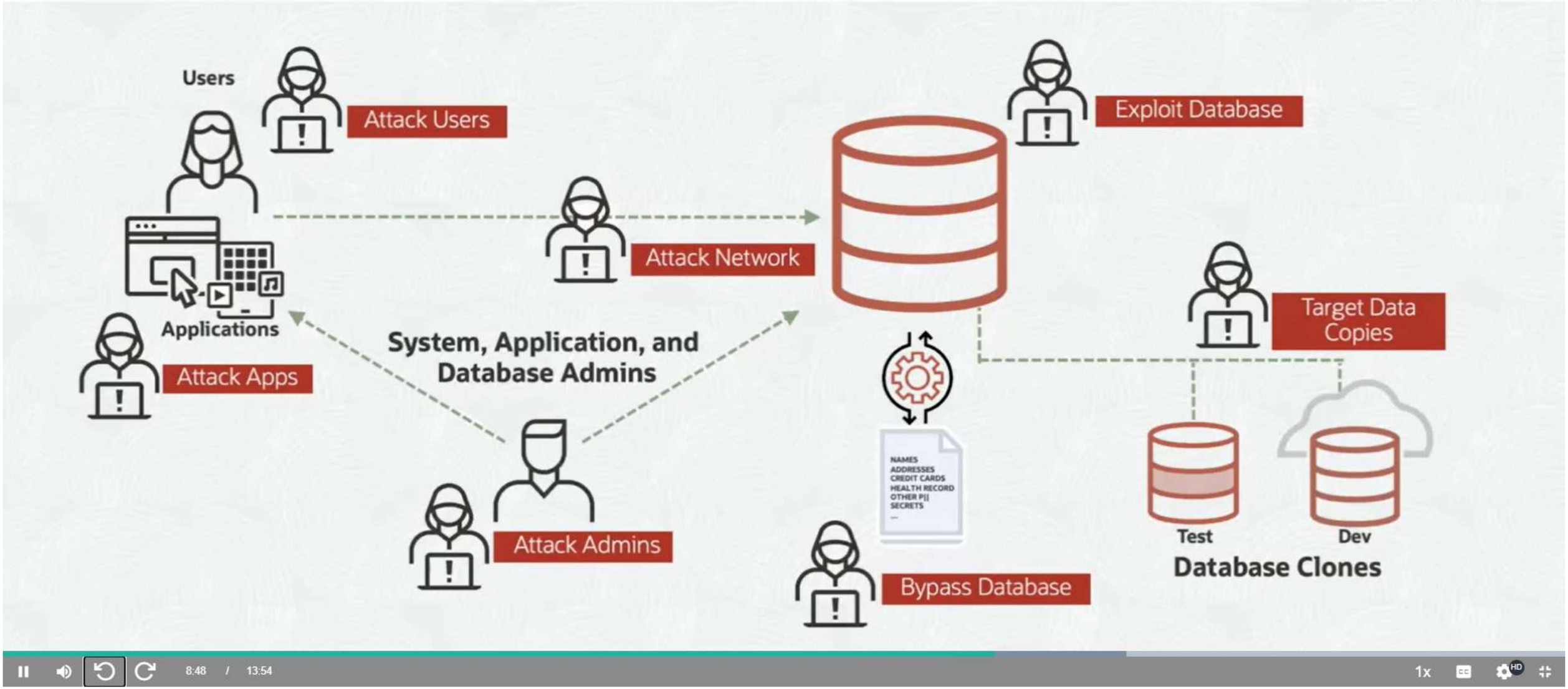
Data

In this case, data is stored in a database – your organization's most valuable asset, but also a source of significant risk.

Users

Users and applications connect to your database to perform authorized business functions.

How do hackers attack the database?



8:48 / 13:54 1x

Baseline Security