



# Securing Business Critical Workloads

Threats, Implications and Outcomes

---

**Marella Folgori**

**Oracle Senior Sales Manager Security and Manageability – Italy Russia & CIS**

**Paola Marino**

**Oracle Principal Sales Consultant - Italy**

## Safe Harbor

---

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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at <http://www.oracle.com/investor>. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.



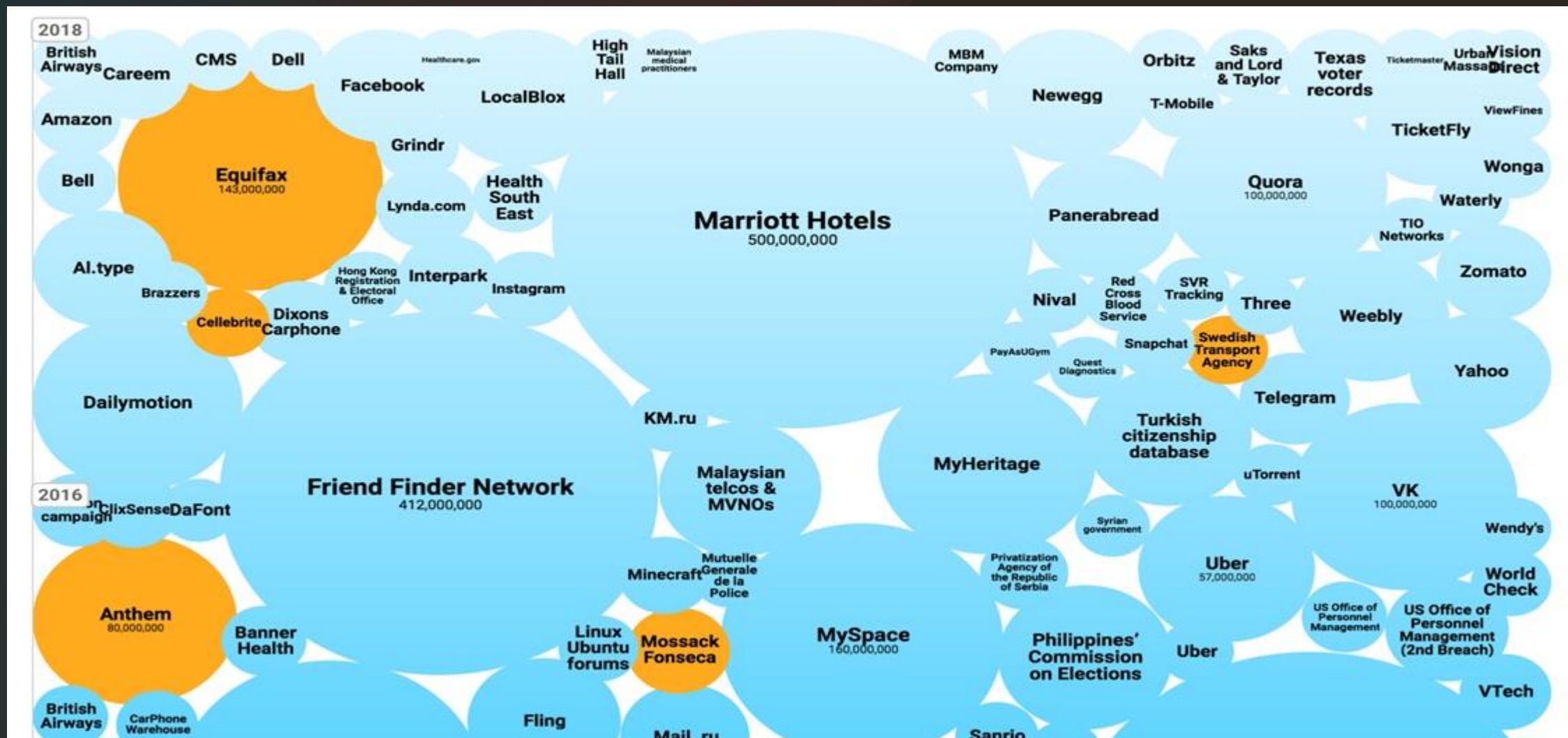


Threats are real





# Major 2018 Breaches



# Cloud Data breaches



## Accenture

**137GB of data and 40,000 passwords**

- Secret API data
- Authentication credentials
- Certificates
- Decryption keys
- Customer information



## Aus. Broadcasting

**1,800 daily MySQL database backups**

- Emails, logins, hashed passwords for ABC Commercial users
- Requests for licensed content by TV and media producers to use ABC's content and pay royalties.
- Secret access key and login details for repository, with advance video content



## FedEx

**119,000 scanned documents**

- Photo ID from Mexico, Canada, EU, Saudi Arabia, Kuwait, Japan, Malaysia, China, Australia
- Names, home addresses, and phone numbers



## Dow Jones

**1.6 million entries** Dow Jones Risk and Compliance, a subscription-only corporate intelligence program

- Names, addresses, account information, email addresses, and last 4 digits of credit card of millions of subscribers



## Adidas

**"Few million customers" affected**

- Contact details
- Usernames
- Encrypted passwords



## GoDaddy

**31,000 GoDaddy systems details exposed**

- Server config information
- CSP billing information
- Server workload info


# World wilde Data breaches (August 2019)

**CNN BUSINESS**

## A hacker gained access to 100 million Capital One credit card applications and accounts

By Rob McLean, [CNN Business](#)


Updated 2117 GMT (0517 HKT) July 30, 2019




**Capital One Data Breach**

"The largest category of information accessed was information on consumers and small businesses as of the time they applied for one of our credit card products from 2005 through early 2019."

**HACKER ARRESTED IN MASSIVE CAPITAL ONE DATA BREACH**



**ERRATiC**  
882 Tweets




**ERRATiC**  
@0xA3A97B6C

gpg --RECV-KEYS 0xA3A97B6C

📍 Seattle, WA 📅 Joined June 2019

200 Following 47 Followers





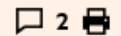
# Italian Data breaches (August 2019)



## “UniCredit and Ford launch probes after Capital One hack”



Hannah Murphy in San Francisco, Kadhim Shubber in Washington and Rachel Sanderson in Milan  
JULY 31 2019



Italian bank UniCredit and US carmaker Ford have launched investigations into whether their data has been caught up in the [Capital One data security breach](#), as experts and lawmakers race to assess whether the hack had other targets.

A UniCredit spokesperson said on Wednesday that the bank had “contacted the relevant authorities” and launched a probe after a cyber security expert discovered a post by the accused Capital One hacker that suggested she had also stolen data from the company.

# Italian Data breaches (Dec 2018)

## Saipem servers suffer cyber attack in Middle East.



MILAN (Reuters) - Italian oil services company Saipem (SPMI.MI) said it had identified a cyber attack out of India on Monday that had primarily affected its servers in the Middle East.

**Hackers** attacked to 400 servers, mainly in Saudi Arabia.  
"We are collecting all the elements useful for assessing the impact on our infrastructures and the actions to be taken to restore normal activities" the firm said in a statement



A Saipem logo is seen on the bridge of the Saipem 10000 deepwater drillship in Genoa's harbour, Italy,



A blurred background image of an office interior. Several people are visible, some standing and some sitting, in front of a large whiteboard. The scene is brightly lit, possibly by natural light from a window. The overall tone is professional and collaborative.

Risks are real



\$3.9M

Average total cost of  
data breach

\$148 per  
record

Average financial impact  
of data breach





Organizations must be right  
100%...

An attacker only has to be  
right once!



100%



A man with short brown hair and a light beard is looking intently at a computer monitor. He is wearing a grey cardigan over a white t-shirt. His hands are on a keyboard. In the background, a woman is also working at a computer, her face partially obscured by her hand. The office is dimly lit, with warm light from the monitors and ambient light from the room. A semi-transparent red banner is overlaid across the middle of the image.

# Oracle Security as an Enabler



# Defense in Depth

*Cloud and On-premises*





# Security as an Enabler



## Infrastructure

Secure isolation/integrity



## Data

Automatic protection/access



## Applications

Identity/access/protection



## Users

Adaptive authentication/access



# Oracle Security Solutions

- Uses ML /AI to automate and simplify security
- Protects sensitive data throughout lifecycle
- Detects anomalous behavior, improves attack resilience
- Reduces identity risk with adaptive authentication
- Enables a layered security strategy



**Database  
Security**



**Hybrid Identity  
Management**



**CASB Cloud  
Service**



**Web Application  
Firewall**



**OCI  
Security**

# Oracle Security Solutions



## **DataBase Security**

Protect sensitive data  
against threats



## **Hybrid Identity Management**

Control access to apps  
and infrastructure



## **CASB Cloud Service**

Gain visibility, enforce  
policy, identify high risk



## **Web Application Firewall**

Defend web apps against  
external threats



## **OCI Security**

Securely deploy apps  
with layered defenses





# Security Zones of Control

## Assess

---

Assess the current state of the database

## Detect

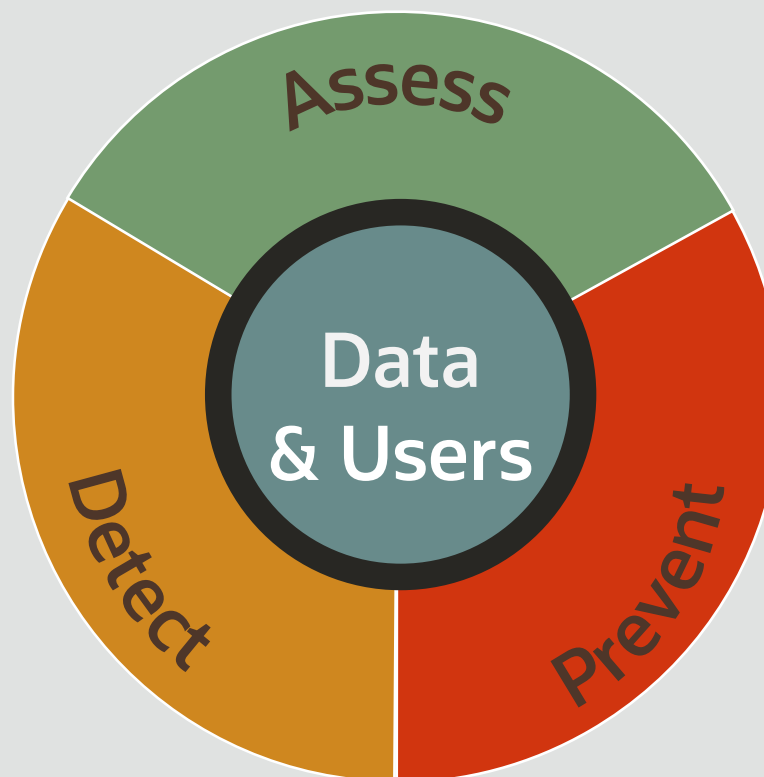
---

Detect attempts to access data, especially attempts that violate policy

## Prevent

---

Prevent inappropriate or out of policy access to data



## Data

---

Your organizations most valuable asset, but also a source of significant risk. In this case, data is stored in a database

## Users

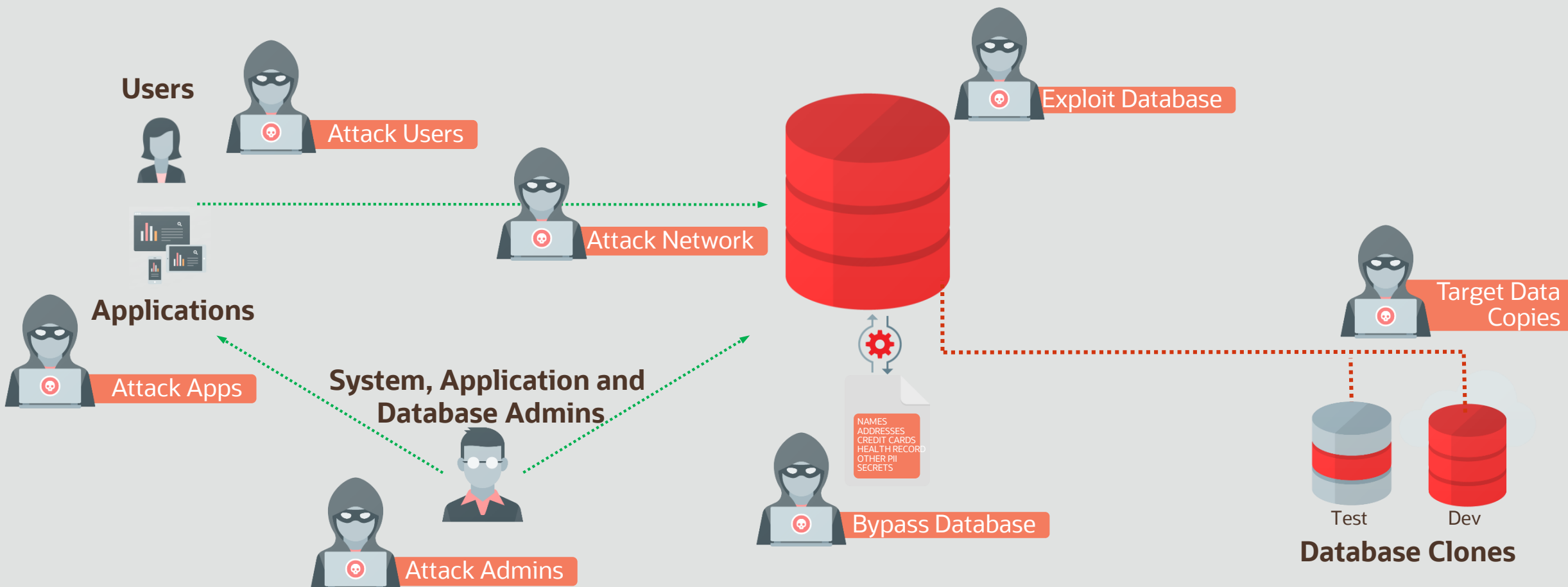
---

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



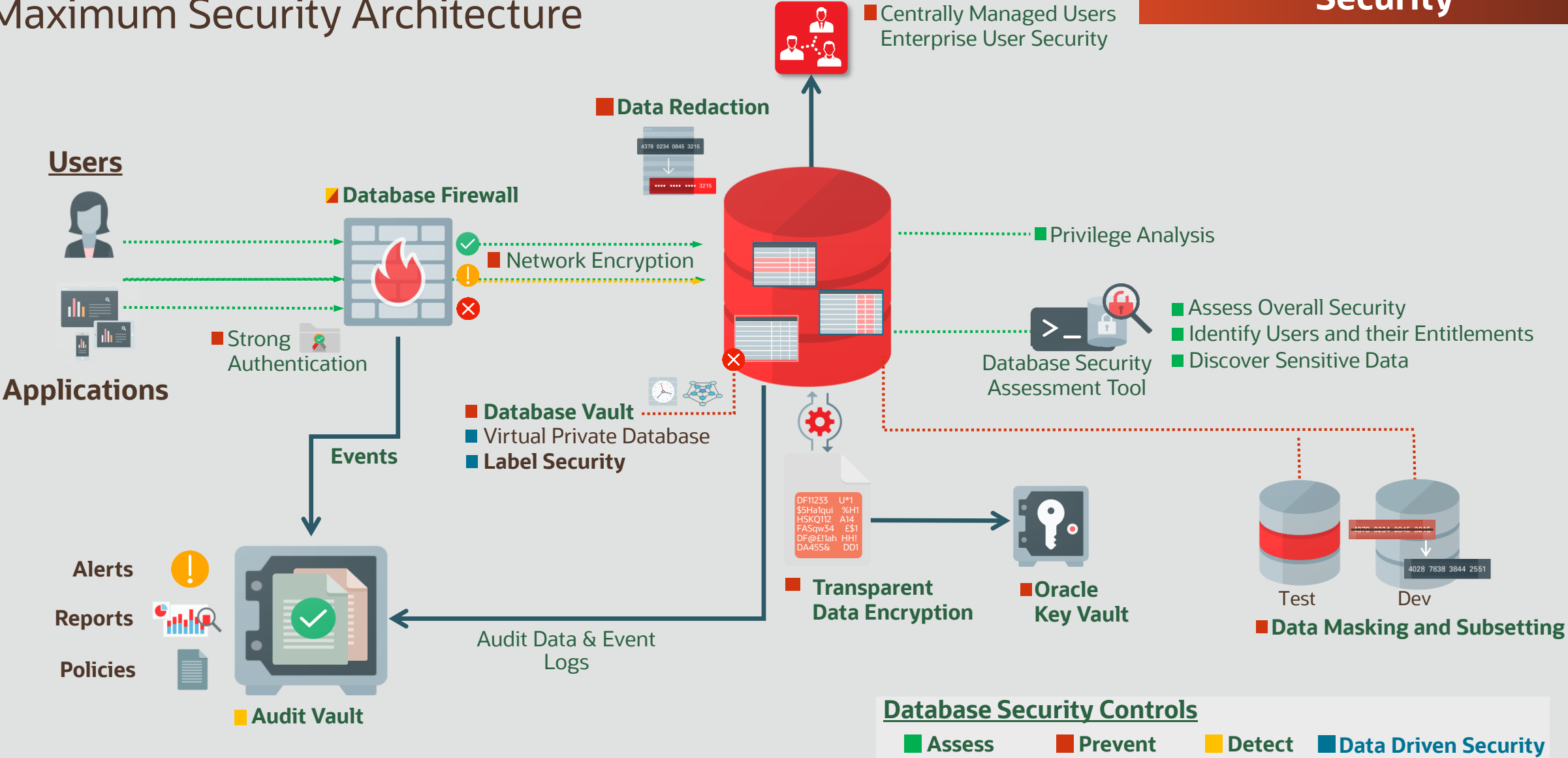


## How Do Hackers Attack the Database?





# Maximum Security Architecture





# Security Zones of Control for Oracle Databases

## Assess

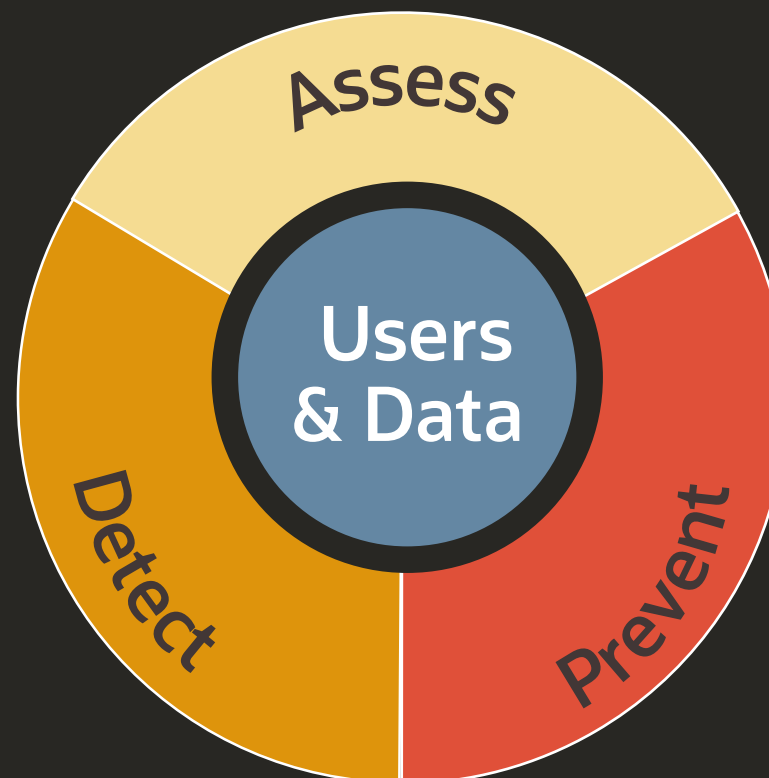
Security-Assessment (DBSAT)  
Data Discovery  
Privilege Analysis

## Detect

Activity Auditing  
Audit Vault  
Database Firewall

## Prevent

Transparent Data Encryption & Key Vault  
Data Masking, Data Redaction  
Database Vault



## Data

Label Security  
Virtual Private DB

## Users

Password, PKI, Kerberos, Radius  
Proxy Users, Password Profiles  
Oracle & Active Directory



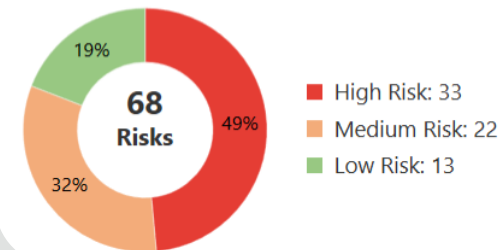




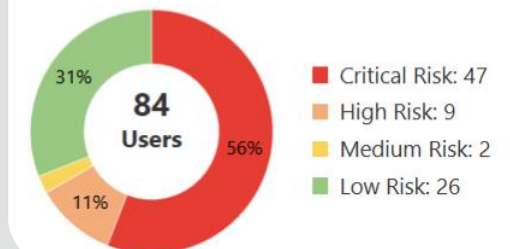
## Data Safe – Database Security Control Center

- Unified Database Security Control Center
  - Security Assessment
  - User Assessment
  - User Auditing
  - Data Discovery
  - Data Masking
- Saves time and mitigates security risks
- Defense in Depth for all customers
- No special security expertise needed

### Security Assessment

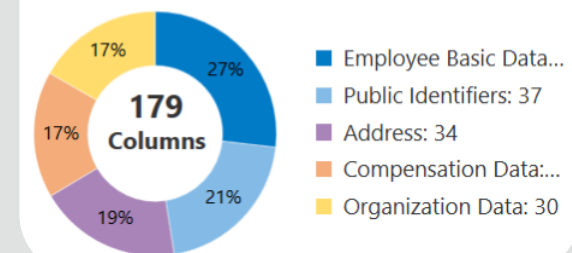


### User Assessment



### Data Discovery

Top 5 categories



# Enterprise IAM Platform



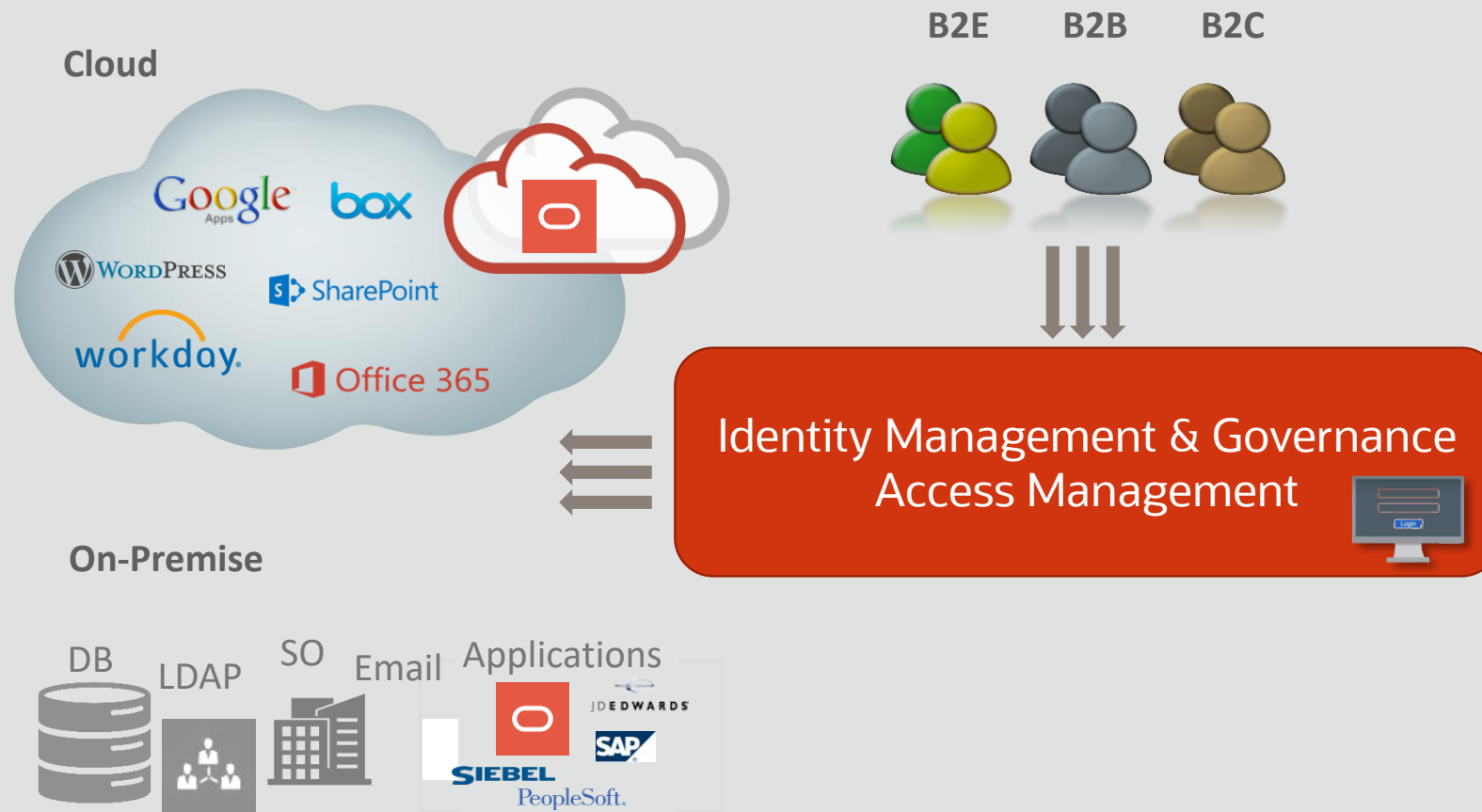
## Hybrid Identity Management

### Identity Mngmt & Governance

- OOTB Connectors to Automate Provisioning To On-premise & Cloud Apps
- Persona-focused User Experience
- Intelligent Access Catalog
- Flexible Workflows for Approvals In Series, Parallel, Community & Group
- Risk-based Certification
- Preventive and Detective SoD
- Roles Lifecycle Mngmt and Analytics
- Advanced Reporting

### Access Management

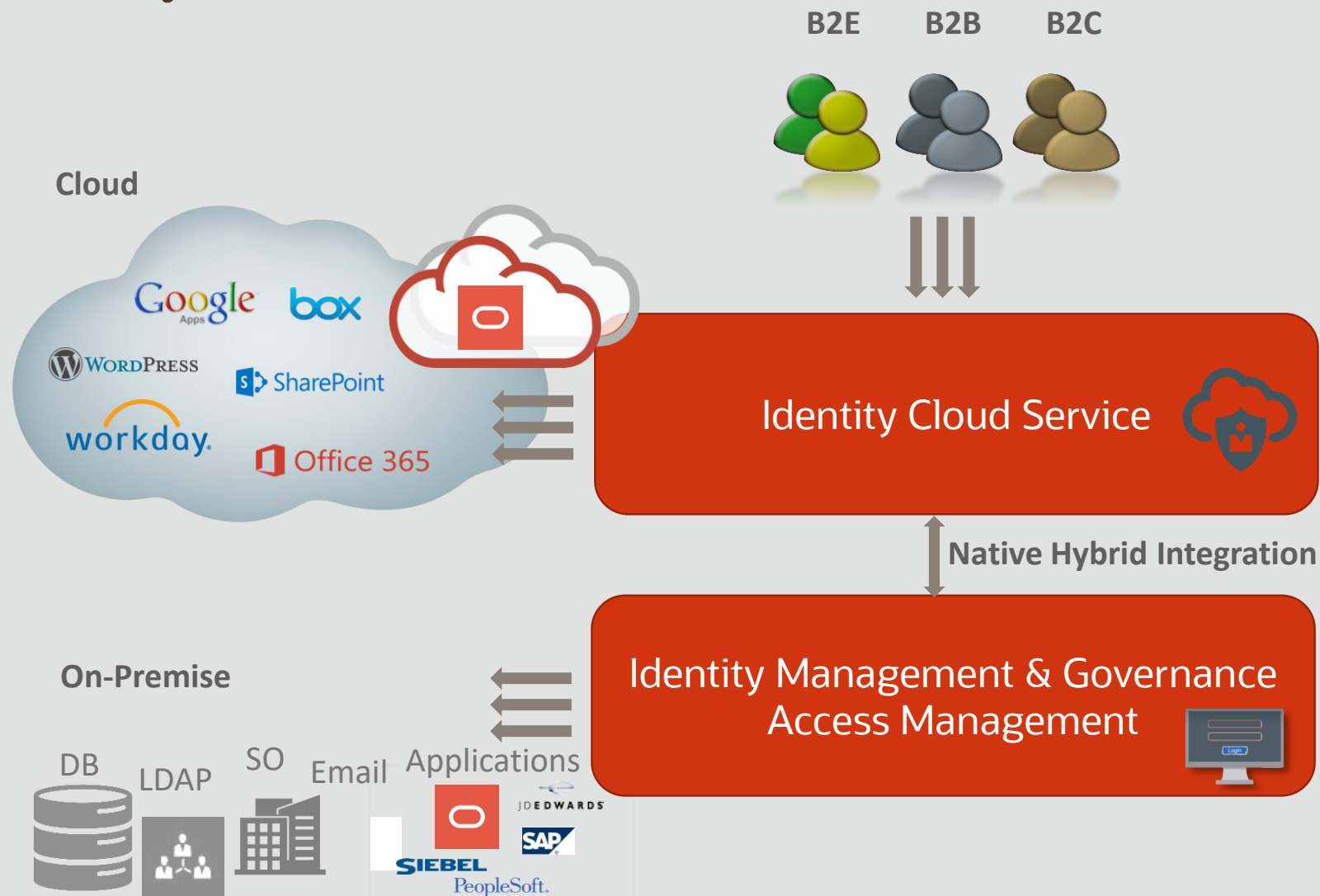
- Dynamic Context-Aware Adaptive AuthN
- Fine-grained, attribute-based Authorization
- Session Management
- Extended Federated Access Security
- Mobile Access Management







## Hybrid IAM Platform



### Identity Cloud Service

- Centralized authentication, authorization, user management and self-service
- Hybrid Identity: Manage identities for cloud and on premises applications with enterprise-grade hybrid deployments
- Open & Standard-based: Rapidly integrate with applications using a 100% open and standards-based solution
- Secure Defense-in-Depth: Reduce risk using behavioral authentication for application access control
- Sync identities, SSO, Federation



# Oracle CASB



CASB Cloud  
Service



Provisioning,  
Automation and  
Orchestration



Governance  
and Policy



Monitoring  
and Metering



Security  
and Identity



Continuous  
Configuration  
Automation



Capacity And  
Resource  
Optimization

## KEY BENEFITS

- 100's of hours of effort saved
- Consistent security posture
- Heterogeneous cloud services

Out of The Box  
(OOTB)  
SmartPolicies

**Oracle CASB  
Cloud Service**

Machine Learning +  
Threat Intel + Threat  
Feeds

Sales &  
Marketing

G Suite



AWS

salesforce

Global IT



AWS

Office 365

GitHub

Human  
Resources

ORACLE<sup>®</sup>  
Oracle ERP  
Cloud

ORACLE<sup>®</sup>  
HUMAN CAPITAL  
MANAGEMENT

ORACLE<sup>®</sup>  
Cloud Infrastructure

Research &  
Development



# slack

AWS

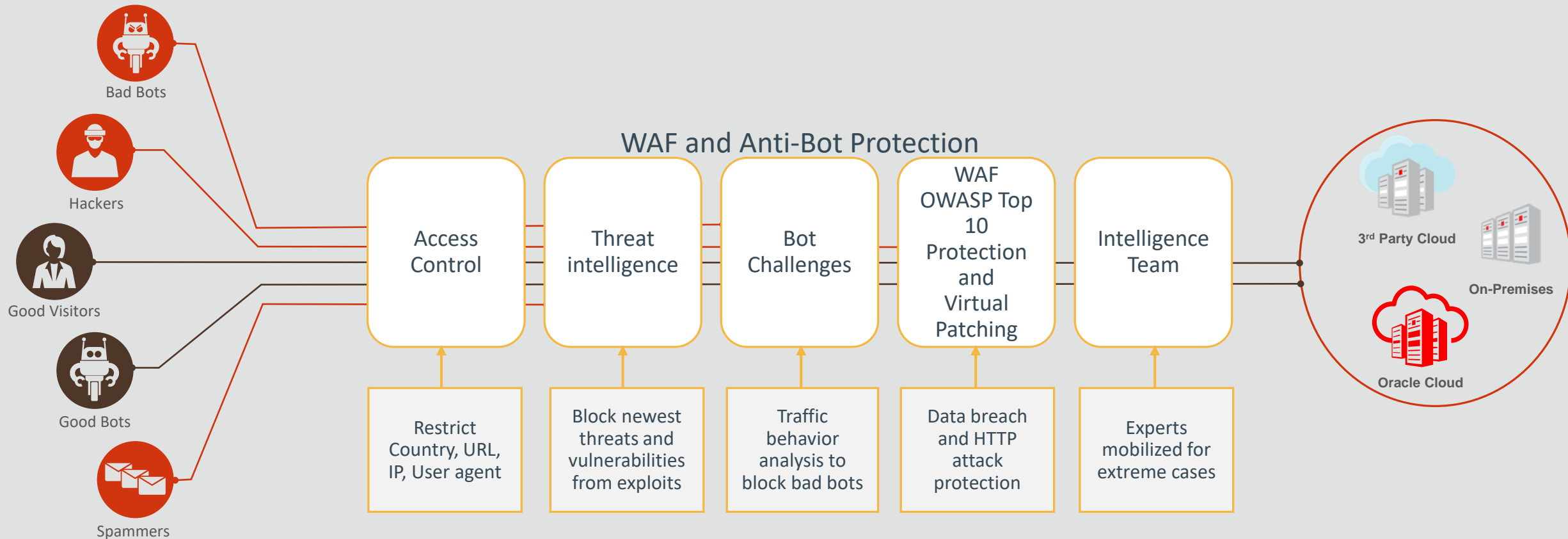






## Web Application Firewall

# Oracle WAF

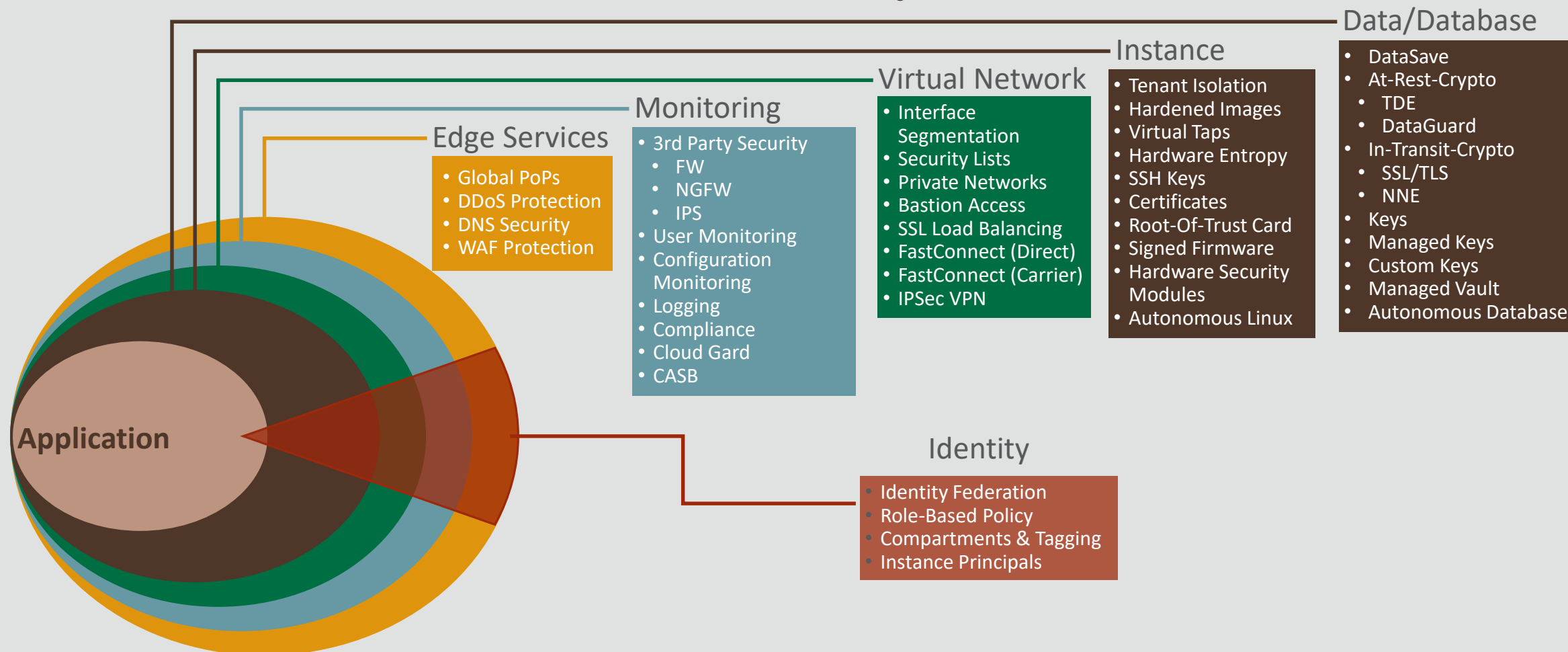


Setup and activation can be done within the minutes.  
No hardware or software implementation





## Oracle Cloud Infrastructure Security



Stronger Isolation and Advanced Controls from Core to Edge







Voices from the World

# Intesa Sanpaolo (Tier 1 Bank)

Italy and Eastern Europe

Full Data Protection Architecture and Cloud Security paradigm definition



## Business Challenge

Intesa Sanpaolo is facing multiple corporate challenges, including: Digitalization, Innovation, Operations trans, Cost reduction, Law compliance (GDPR, PCI).

Intesa Sanpaolo is also consolidating a centralized security strategy to support Cloud adoption.

## Solution

Customer adopted multiple **Oracle DB Security functions and tools**, to protect its data on a very large installation of **Oracle Exadata Stack**.

Customer is testing **Oracle Security Cloud Services** to protect heterogeneous Cloud environment.

## Benefits

Complete data protection and auditing for better compliance.

Customer leverages on Oracle Cloud Security to consolidate strategy and guidelines that go beyond existing tactical separated solutions.



# Intesa Sanpaolo (Tier 1 Bank)

Italy and Eastern Europe

Full Data Protection Architecture and Cloud Security paradigm definition

A large red key graphic is positioned on the left side of the slide. The key's shaft is a vertical line with five white circular nodes. Each node is connected to a horizontal red bar containing text. The key's head is a large red circle with a white outline of a keyhole.

**TDE** – Transparent Data Encryption for Database protection

**EUS** – IAM Integration, centralized management of database authorizations

**DB Vault** – Privileged user control

**DB Auditing** – enables selective and effective auditing using policies and conditions

**CASB** - protects your entire cloud footprint with automated security monitoring.

## From traditional On-Premise Identity Management to Hybrid Identity Architecture

### Business Challenge

With more than 137.000 employees they offer integrated products including postal service, postal saving, logistics, mobile and financial service.

Customer's CyberSecurity Office has the goal to ensure a consistent security posture aligned to the new strategy for supporting the business and for protecting information assets.

### Solution

Many Oracle DB Security Features including [Oracle Advanced Security](#), [Oracle DB Vault](#), [Oracle Audit Vault & Database Firewall](#).

Customer evolved from an existing on-premise IAM solution based on [Oracle Identity Governance](#) to a hybrid scenario with [Oracle IDCS](#).

Customer has chosen [Oracle CASB on Oracle HCM and Office 365 application](#) for mitigating cloud security risks, gaining visibility across the cloud, responding to the [shared responsibility model](#).

### Benefits

Visibility into risky users, user behaviour and anomalous activities for improved security and better compliance.

Customer ready for new initiatives by protecting users and assets.



# Healty regional public organizations

Italy

## Personal Sensitive Data Protection

### Business Challenge

Digit PA – Process of Digital transformation for Local Public Administration.

Compliant to several Italian and International regulations.

### Solution

Many Oracle DB Security Features including Oracle Advanced Security, Oracle DB Vault, Oracle Audit Vault & Database Firewall, Oracle Data Masking and Subsetting Pack.

### Benefits

Increase efficiency and reduce operational costs.

Reduce operational risks and human errors; prevent unauthorized data exposure.

Meet Compliance obligations.

# Healty regional public organizations

Italy

## Personal Sensitive Data Protection



**TDE** – Transparent Data Encryption for Database protection

**Data Masking** – Data Masking in Test & Dev env

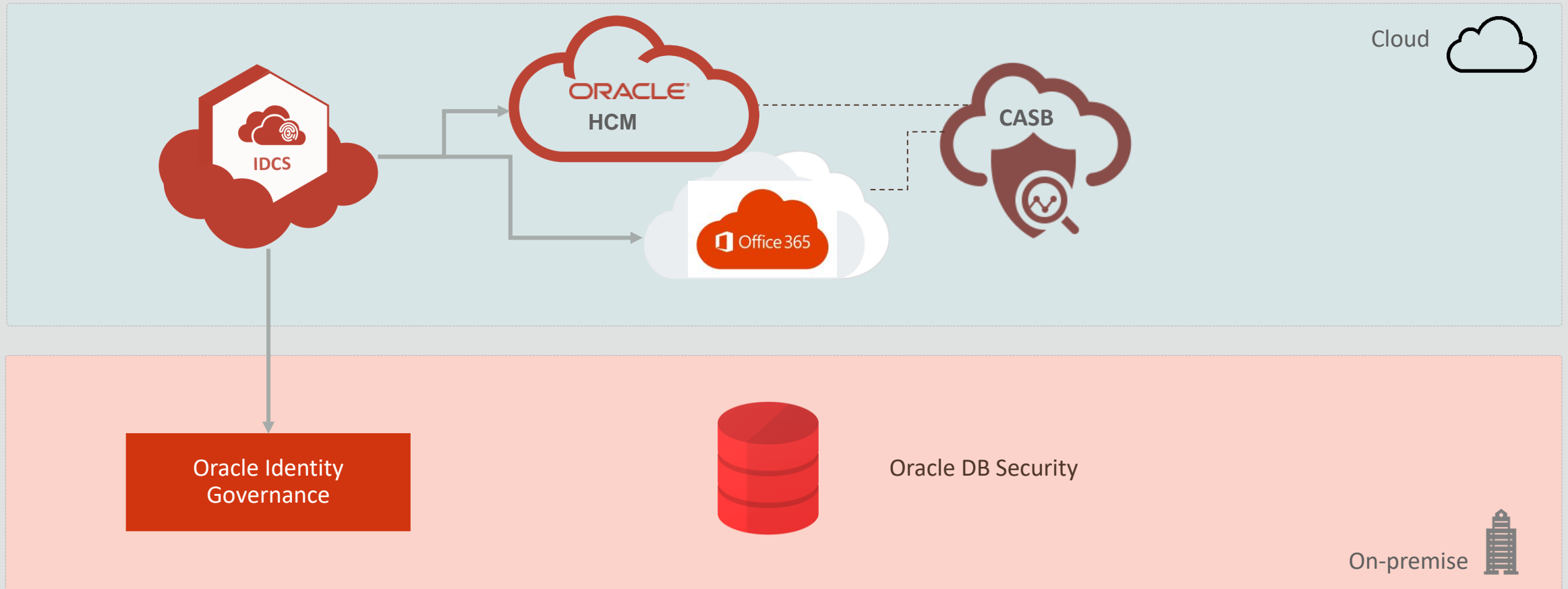
**DB Vault** – Privileged user control

**DB Auditing** – enables selective and effective auditing using policies and conditions

# Postal Service

Italy

From traditional On-Premise Identity Management to Hybrid Identity Architecture





# Siram, Veolia Group

Italy, France



Journey to the Cloud enabling with robust Identity and Edge security services

## Business Challenge

Move Energy Management Enterprise workloads from On-premise to Cloud.

Use native cloud technologies (SaaS, PaaS, IaaS) to increment performance, accessibility and optimization.

Access in SSO to services (Oracle SaaS, Custom and Legacy Applications) with Gmail credentials with one credentials.

Reduce number of Help-Desk tickets about reset password, issues to login to applications and manage user credentials

## Solution

Oracle IDCS to access Cloud and on-premise applications, federated with external Identity Provider.

Oracle WAF to protect edge security for mitigating vulnerability and attacks.

## Benefits

Simplified User-Experience to access to services

Reduced Integration and Operational Costs

Faster and Efficient on-boarding applications and cloud services, release new business services

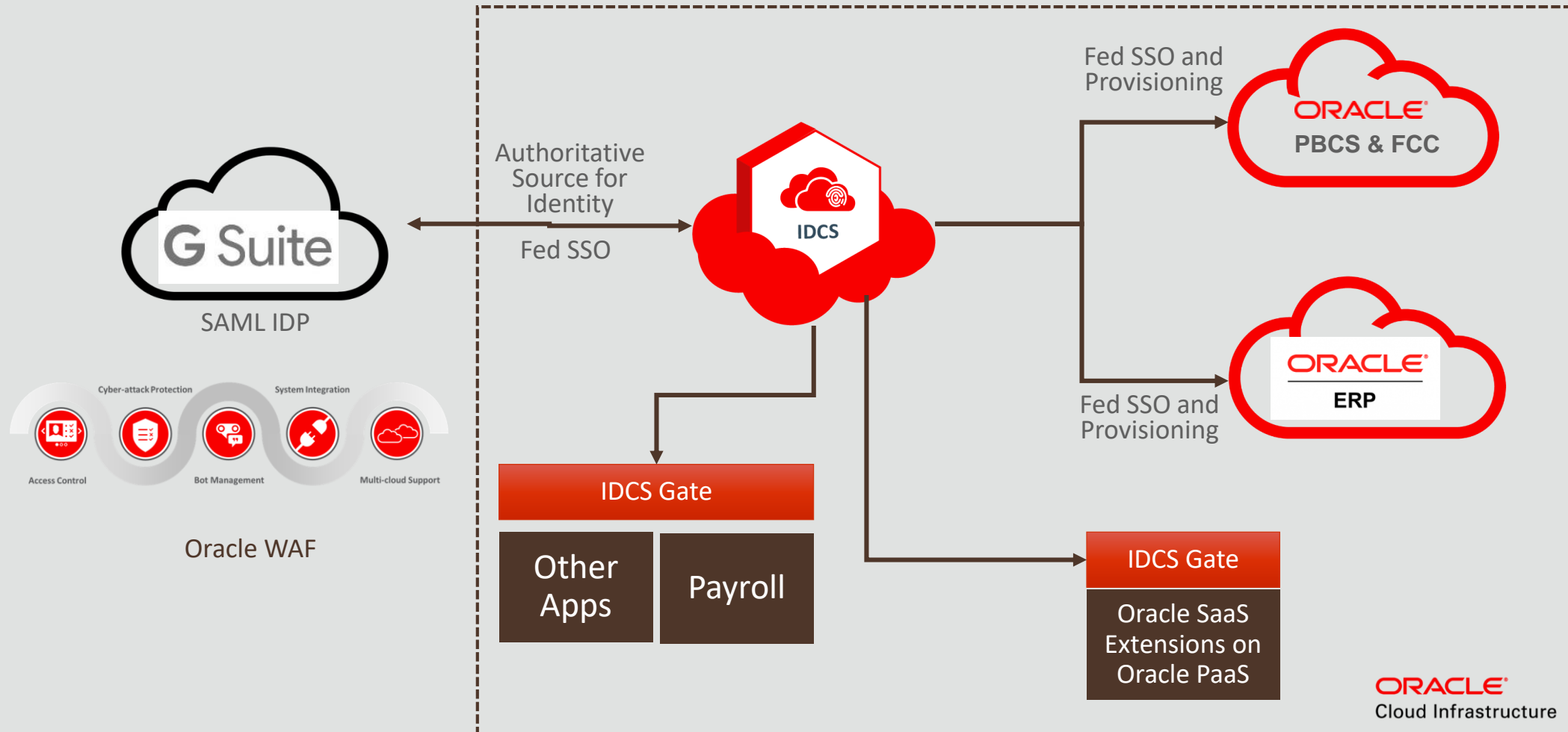
Facilitated a smooth migration to the cloud

Improvement in compliance for regulations such as the EU's GDPR

# Siram, Veolia Group

Italy, France

Journey to the Cloud enabling with robust Identity and Edge security services





# Oracle is a Security Company

- Decades of experience safeguarding sensitive data
- Extensive security investments
- Defense-in-depth security offering
- Solutions to achieve compliance with fewer resources
- Secure by design cloud for sensitive data and applications





ORACLE®

## Safe Harbor

---

The preceding 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.

Statements in this presentation relating to Oracle's future plans, expectations, beliefs, intentions and prospects are "forward-looking statements" and are subject to material risks and uncertainties. A detailed discussion of these factors and other risks that affect our business is contained in Oracle's Securities and Exchange Commission (SEC) filings, including our most recent reports on Form 10-K and Form 10-Q under the heading "Risk Factors." These filings are available on the SEC's website or on Oracle's website at <http://www.oracle.com/investor>. All information in this presentation is current as of September 2019 and Oracle undertakes no duty to update any statement in light of new information or future events.