Oracle
Cloud Security Day

ORACLE

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, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Oracle Cloud Security Day

• **Introductions - *Oracle***	9:00 - 9:15 am
• **Threats, Vulnerabilities and Fraud Events in the Cloud - *KPMG***	9:15 -10:15 am
• **Break**	10:15 -10:30 am
• **Oracle Security For the Cloud - *Oracle***	10:30 am - 12:00 pm
• **Lunch - Cloud Threat Report An inside look & discussion**	12:00 - 1:00 pm
• **Oracle Cloud Security Test Drive**	Test Drive Setup (1:00 - 1:30 pm) IDCS Test Drive (1:30 - 2:30 pm) CASB Test Drive (2:30 - 3:30 pm) SMA Test Drive (3:30 - 4:30 pm)
• **Next Steps** (4:30 - 4:45 pm)	4:30 - 4:45 pm

ORACLE

Threats, Vulnerabilities and Fraud Events in the Cloud

Brian Jensen
KPMG

ORACLE

KPMG | Oracle

Recognized Cyber Practice

The Forrester Wave™: Information Security Consulting Services, Q3 2017

The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change

"KPMG has the clearest, most direct vision. KPMG asserts its desire to help CISOs and boards of directors come together on information security as a business issue, not an IT issue. The company's go-to-market approach leads with vertical expertise, while it is also applying investments across global member firms in areas like data analytics to cybersecurity engagements."

"Organizations should look to KPMG when they need help with technical, advisory, or compliance engagements."

Key Oracle Partner

Platinum

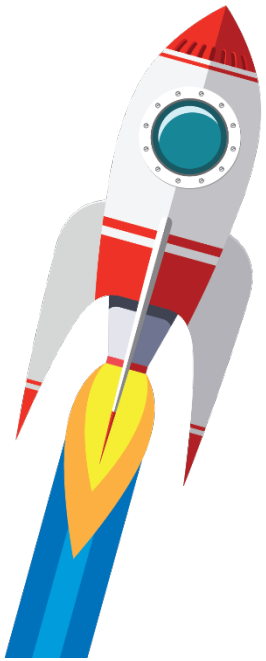
Partner

Global Cloud Elite

Expanding Cyber Capabilities

KPMG LLP completed its acquisition of the Identity and Access Management (IAM) business of Cyberinc, one of the world's largest independent IAM technology providers.

The acquisition enhances KPMG's existing capabilities as a leader in information security consulting services* and expands the firm's ability to provide clients with emerging and more agile IAM solutions.



What's Driving the Market? | Cloud Applications & Platforms

Percentage of fraud resulting in loss of $1 million or more

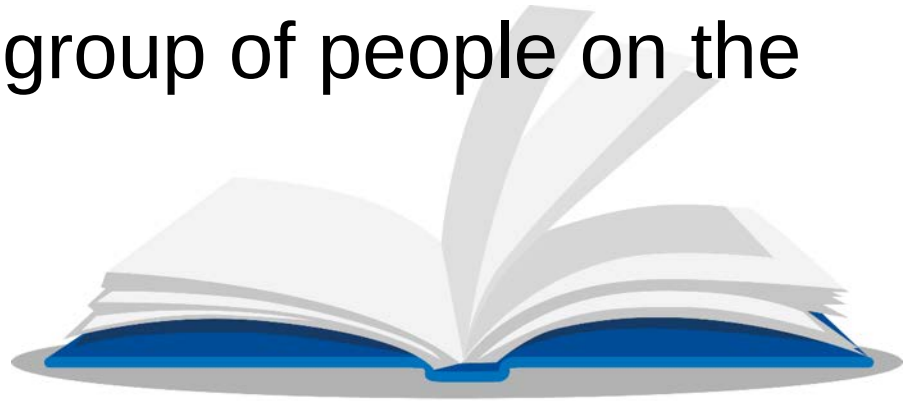
42%*

of fraud events were perpetrated by purely **internal** fraudsters

*Source: Global profiles of the fraudster, KPMG, 2016.

KPMG Global Profiles of the Fraudster

"Companies have to design anti-fraud mechanisms that look **both ways, inside and outside**. And they need to be aware of the possibility that a lone, inside fraudster may be working with a sizeable group of people on the outside."



What's Driving the Market? | Cloud Applications & Platforms

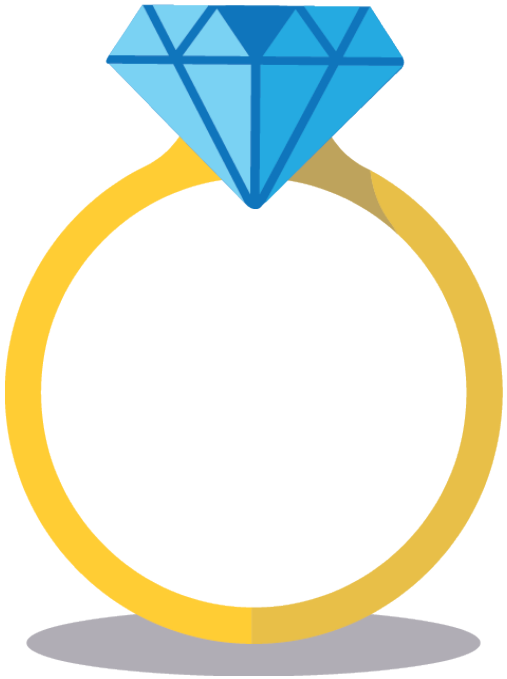
Top 5 Security Threats Impacting Enterprise Cloud

1	**Fraud**
2	**Cloud Scams**
3	**Data Theft**
4	**Data Exposure**
5	**Cloud Ransom**
Beyond	**Cloud Trojan Horse**

Top 5 Cloud Threats | 2018

1 Fraud

Multinational insurance and finance company…..suffered a $30 million net loss from the massive fraud



THE multinational insurance and finance company … suffered a $30 million net loss from the massive fraud committed by its senior accountant, court documents reveal.

While most of the incredible haul of luxury goods and property purchased with the money - including $16 million worth of jewelry and eight waterfront apartments - has been recovered and resold by the company, it has taken a substantial hit.

It is understood the fraudster did not have any formal accounting qualifications, but had worked her way up from the position of assistant accountant. As a senior accountant she made 200 illegal transfers into her personal accounts or directly to shops and real estate agents.

She then used the computer log-ins of former staff to delete the records or alter them so the transactions appeared legitimate.

Top 5 Cloud Threats | 2018

2 Cloud Scams

Protect Your People: Newest Cloud HCM -Focused Scam Reroutes Employee Direct Deposit Funds

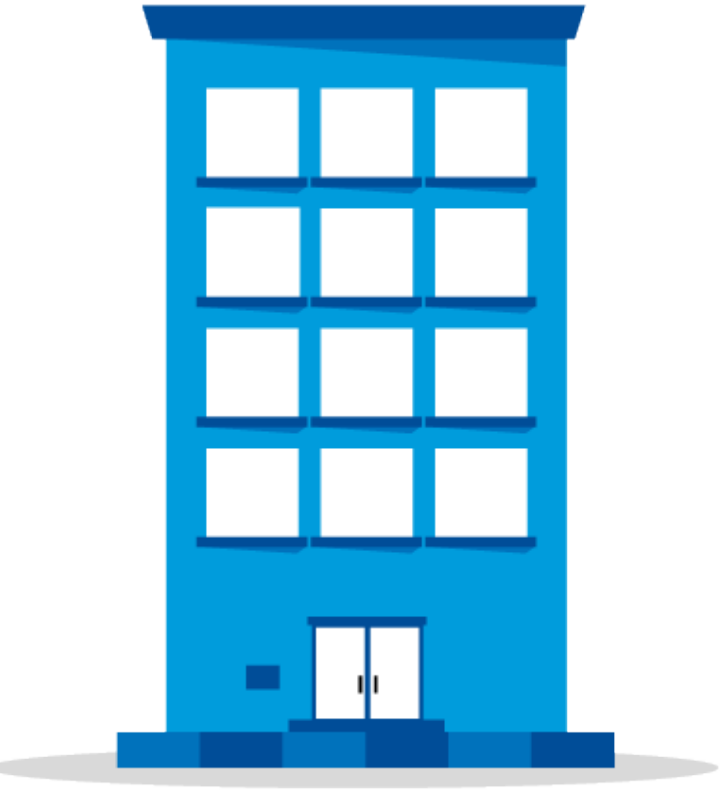
“Another week, another well-concocted phishing scam. The most recent fraudulent activity targeted businesses that use Workday, though this is not a breach or vulnerability in Cloud HCM itself. Specifically, the attack involves a well-crafted spam email that is sent to employees purporting to be from the CFO, CEO, or Head of HR or similar.

Sometimes the emails include the name, title, and other personal information of the “sender” that we believe might be harvested from LinkedIn or other business databases. The email asks employees to use a link in the phishing email or attached PDF to log into a fake Workday website that looks legitimate. **The threat actors who run the fake Cloud HCM website then use the user name and password to log into the Workday account as the employee and change their direct deposit bank/ACH information to another bank, relatable Green Dot, or similar credit card.**

The fraud is typically only discovered when the employees contact HR inquiring as to why they did not receive their direct deposit funds. Unfortunately it appears that spam filters and other controls are failing to prevent this email from infiltrating the organization’s network.”

Top 5 Cloud Threats | 2018

3 Data Theft



…a 3rd party provider for a Large US Government Agency, was hacked

Hackers infiltrated a third-party software packaged(Cloud & On-Premise) in 20XX with the goal of collecting personal records on federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider.

That software package was an SAP enterprise resource planning application.

Assailants infiltrated the agency by piggybacking on an "exploit," that was "present in a widely used and highly-regarded enterprise resource planning ('ERP') software package," to carve out sensitive data while allowing the interface program to appear to execute as expected.

Top 5 Cloud Threats | 2018

4 Data Exposure

…Customer Records for Millions of Large Wireless Company's Subscribers Exposed

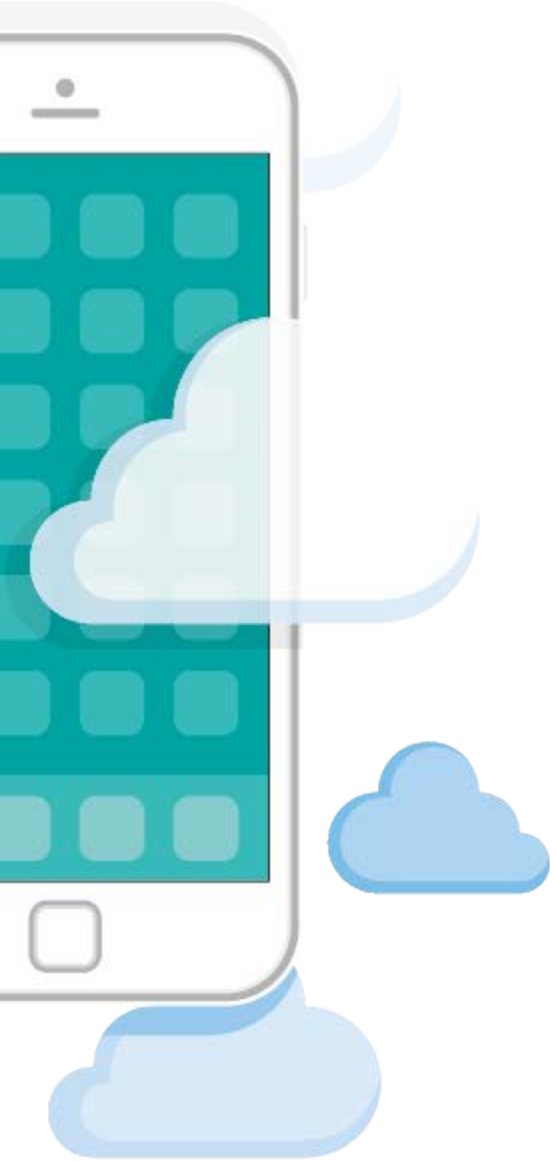
Cloud security research firm found a **misconfigured cloud-based file repository containing the names, addresses, account details, and account personal identification numbers of millions of large wireless company customers**.

The firm came to this number after analyzing the average number of accounts exposed per day in the sample that was downloaded.

The data dump—on a publicly accessible AWS S3 bucket owned and operated by a third-party software and data company called NICE systems—appears to have been created to track customer call data for "unknown purposes,"…

Top 5 Cloud Threats | 2018

5 Cloud Ransom



Large State Voter Database Exposed Online (Again), Held for Ransom (Again)

For the second time in two months, the voter registration information of over 19 million people was leaked online via an unsecured MongoDB database, which was later held for ransom by hackers.
This second incident originates with a newspaper, which acknowledged the breach in an article published on its site.

Newspaper says the ransomed database contained voter registration data from the Secretary of State and contact information for 53,000 current and former newspaper subscribers who registered accounts prior to 2017.

Instead of paying the ransom, the newspaper said it deleted the database for good and will notify affected subscribers of the breach.

Top 5 Cloud Threats | 2018

Beyond Cloud Trojan Horse

KPMG Forensic Lab Forward looking position: Organizations should look to quickly move to protect themselves from a cloud Trojan horse breach scenarios.

Cloud Trojans Horse Breach Profile

1) Nefarious agent is hired in low level role with elevated access
2) Agent works quietly for months gaining trust and stealing credentials
3) Agent leverages stolen credentials to corrupt key vendor master records (fraudulent interface)
4) While organization is distracted with “cleans-up” efforts, agent works with offsite fraudsters to create fake vendors
5) The fraudsters processes several fraudulent vendor payments for millions of dollars
6) When the company realizes the fraud event, it’s too late

Call to Action | Cloud Security

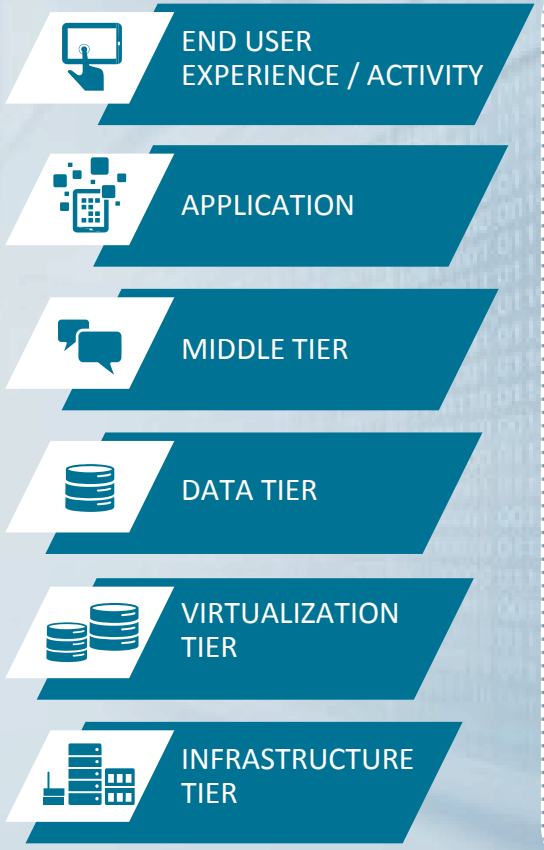
When you get back to your office….

1. Help leadership appreciate the risk realities of the Cloud
   - ➢ Cloud Threat Report
2. Review your current Cloud applications and platform portfolio
3. Enhance your current cyber program and capabilities to support the requirements of the cloud platforms (SAAS, PAAS, IAAS)
   - Cloud Discovery & Usage Monitoring
   - Configuration Monitoring
   - Cloud Event Monitoring
   - Cloud Data
   - User Behavior
4. Extend your IAM platforms to support the requirements of the Cloud Platforms

The Next-Generation Security Cloud Services

ORACLE

Drowning in Data, Lacking in Insight



Global threat feeds
Cloud access
Identity

Real users
Synthetic users

App metrics
Transactions

Server metrics
Diagnostics logs

Host metrics
VM metrics
Container metrics

Configuration
Compliance
Tickets & Alerts

Security & Network events

Too many separate tools

Too much human effort

Not enough context

Oracle Transforms IT Security and Management with New Machine Learning Capabilities

"**Existing approaches to security and management are no longer sufficient**, which is why the headlines are now full of security breaches and performance outages…"

"Our vision for security and management is very simple. **We need all of the data in one place**. **We need purpose-built machine learning that can be used by security and operations professionals, not data scientists. We need automated remediation that does not require human effort.**"

– Larry Ellison
Chief Technology Officer, Oracle

Watch the Highlights of Larry Ellison's Keynote
Read the press release

ML Is Ideally-Suited for Security & Management

- **Massive Data Volume**

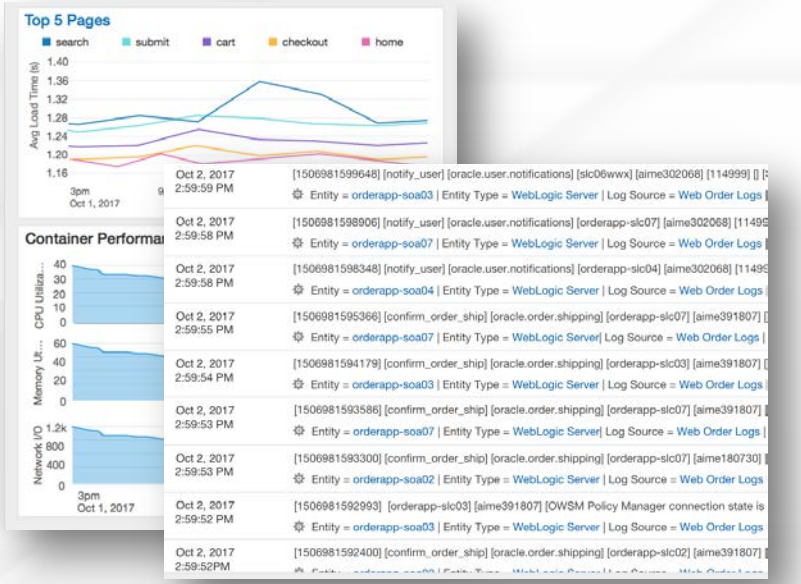
  Terabytes of telemetry generated every day overwhelm humans

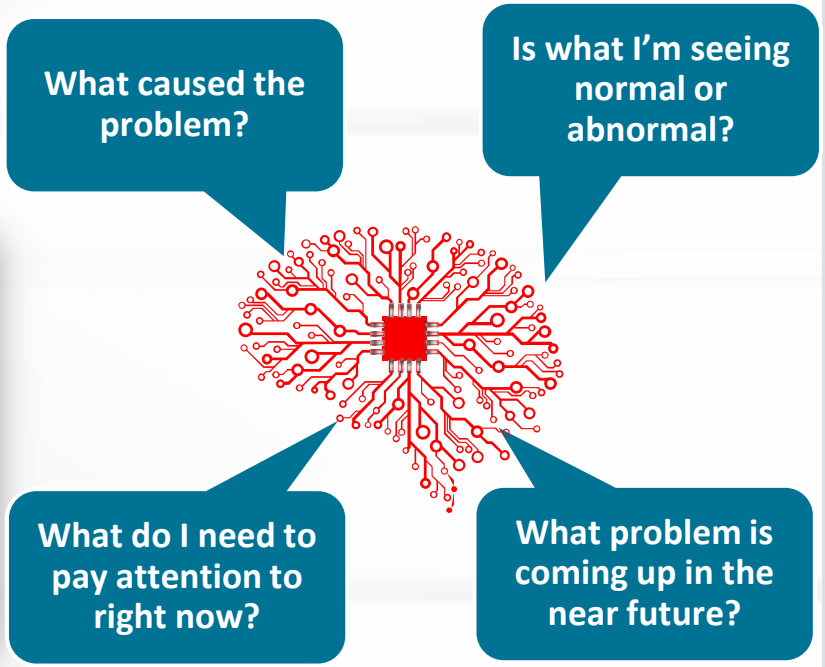
- **Data Is Highly-Patterned**

  Unified metric and log data can be understood by purpose-built ML

- **Need Insights, Not Data**

  We know the kinds of questions we want to ask





Oracle Expands **IdentitySOC with New AI and Automation Services**

IdentitySOC Security Network for 3rd Party Technology Integrations

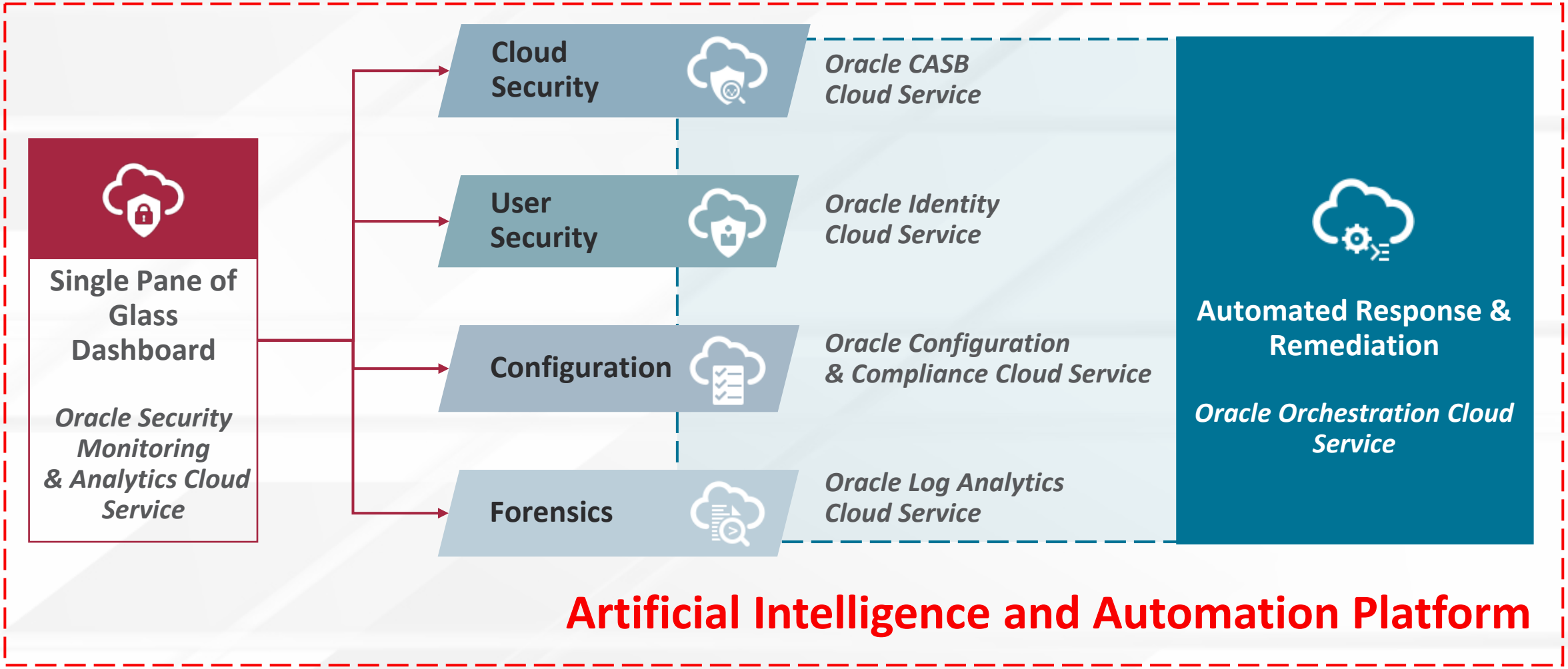
Intelligent Cloud-native Identity Governance as a Service

Dynamic Risk-based Cloud Access Controls with CASB

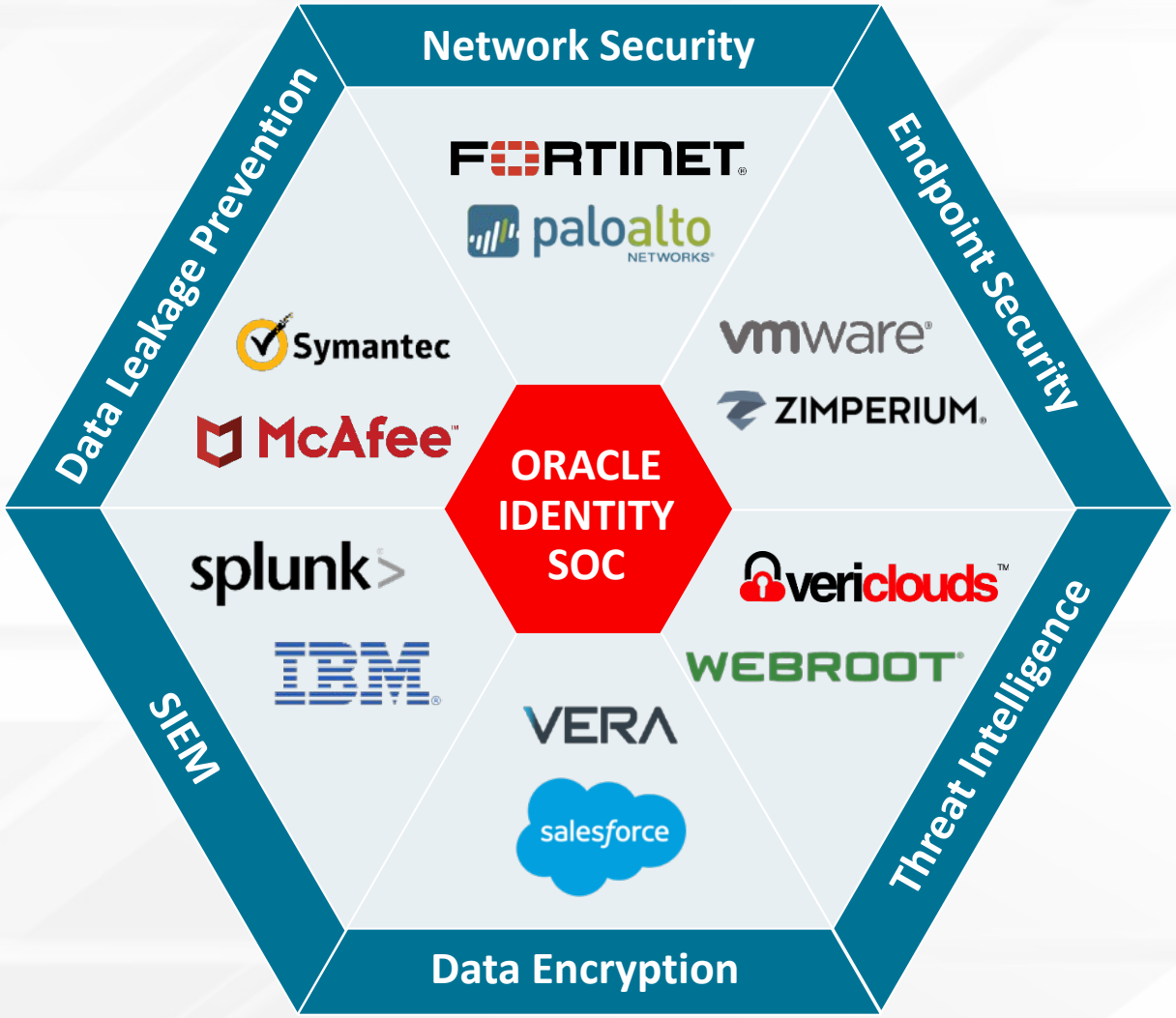
Consumer IAM with Native Integrations to Oracle OnRamp and Customer Experience Applications

ORACLE

Oracle Identity SOC Functional Overview



Identity SOC Security Network



Identity Cloud Service (IDCS)

Announcing
New Intelligent Cloud-Native Identity Governance as a Service

Oracle Identity Cloud Service (IDCS)

Open Standards

Leverage the power of open standards to deliver highly flexible integrations with other applications

Identity Management

Manage user credentials across cloud, mobile and on-premises applications– quickly, easily and from only one place

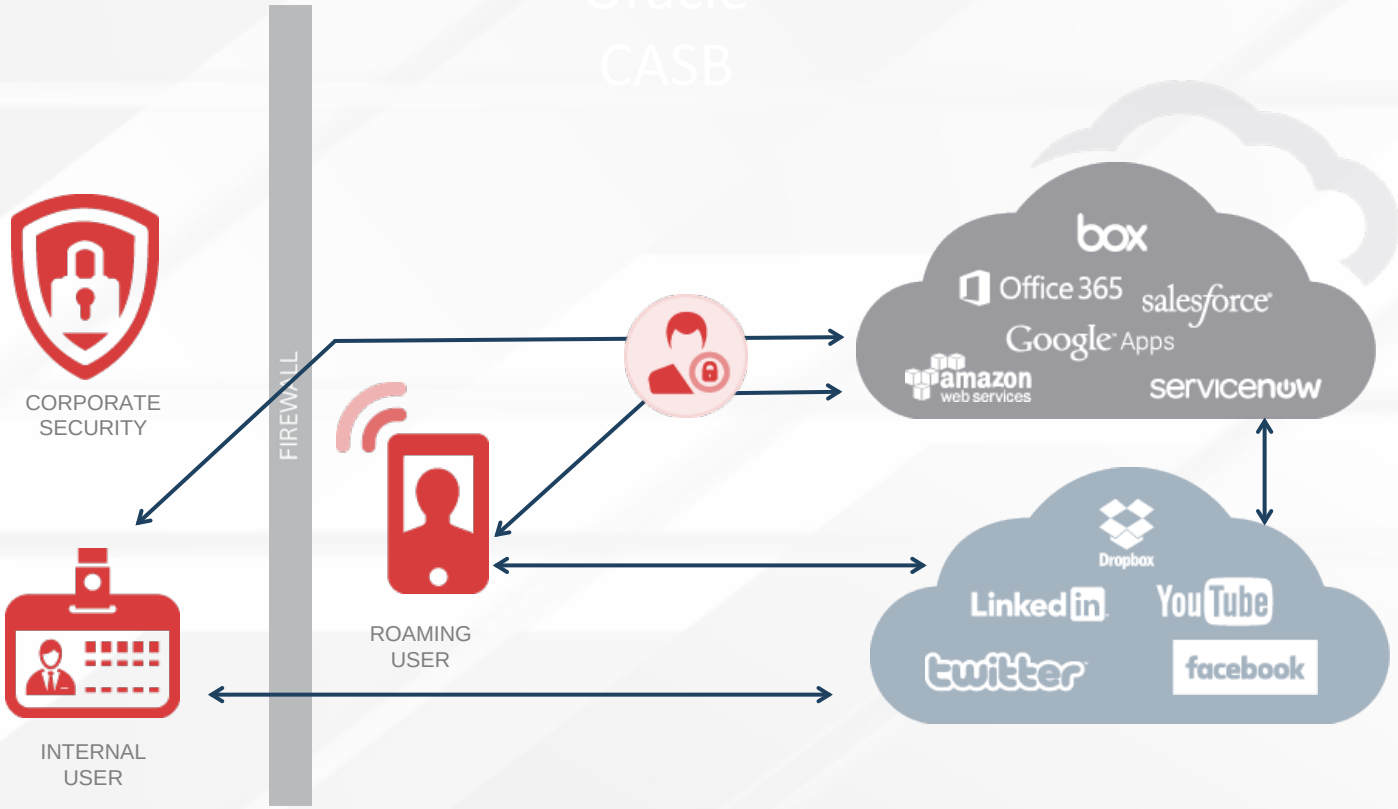
SSO & Authorization

Use SSO and authorization to access applications on-premises and in the cloud from any device, everywhere

Hybrid Identity Management

Synchronize your users and SSO between Microsoft Active Directory or your Oracle Identity Management Suite and the cloud

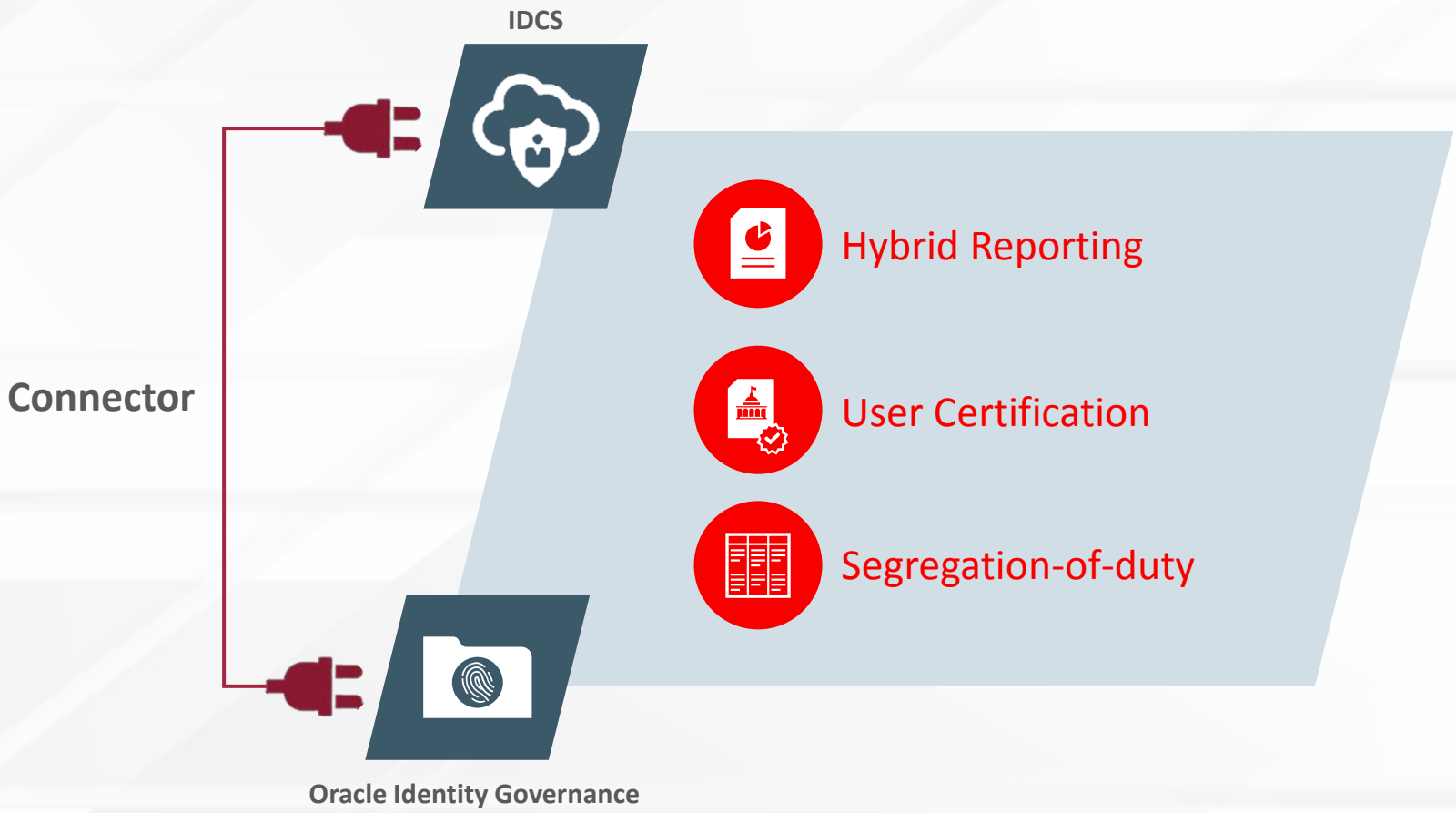
Oracle Identity Cloud Service (IDCS)



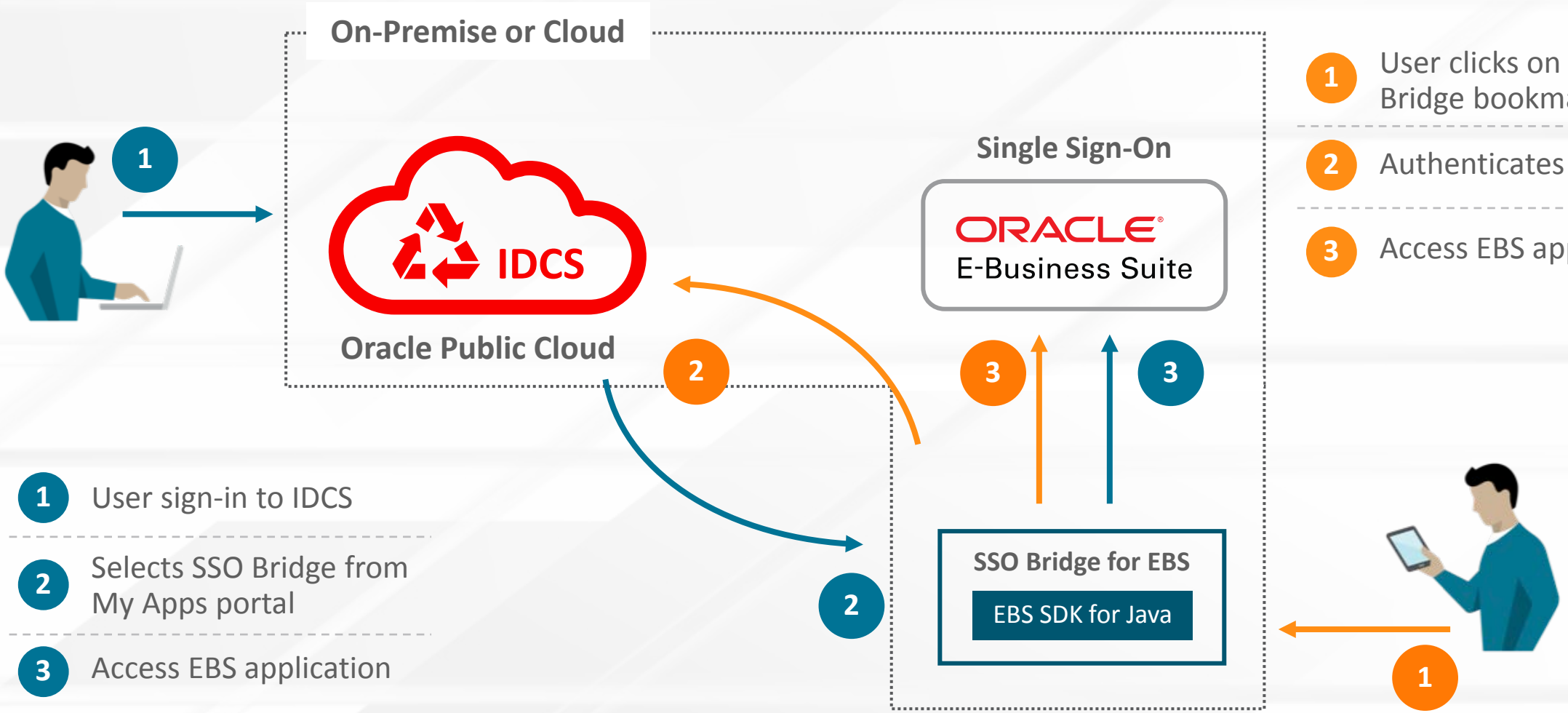
Hybrid Identity Management

- Synchronize or Federate Identities from On-premises to the Cloud without the need of extensive re-factoring or re-writing
- Only IDaaS that can automatically provision and de-provision users to Oracle Public CLoud
- Identity Management for on-premises applications (EBS, PeopleSoft, etc)
- Pre-Integrated with on-prem Oracle IAM enabling a single pane of glass

Oracle Identity Cloud Service: Integration with Oracle Identity Manager

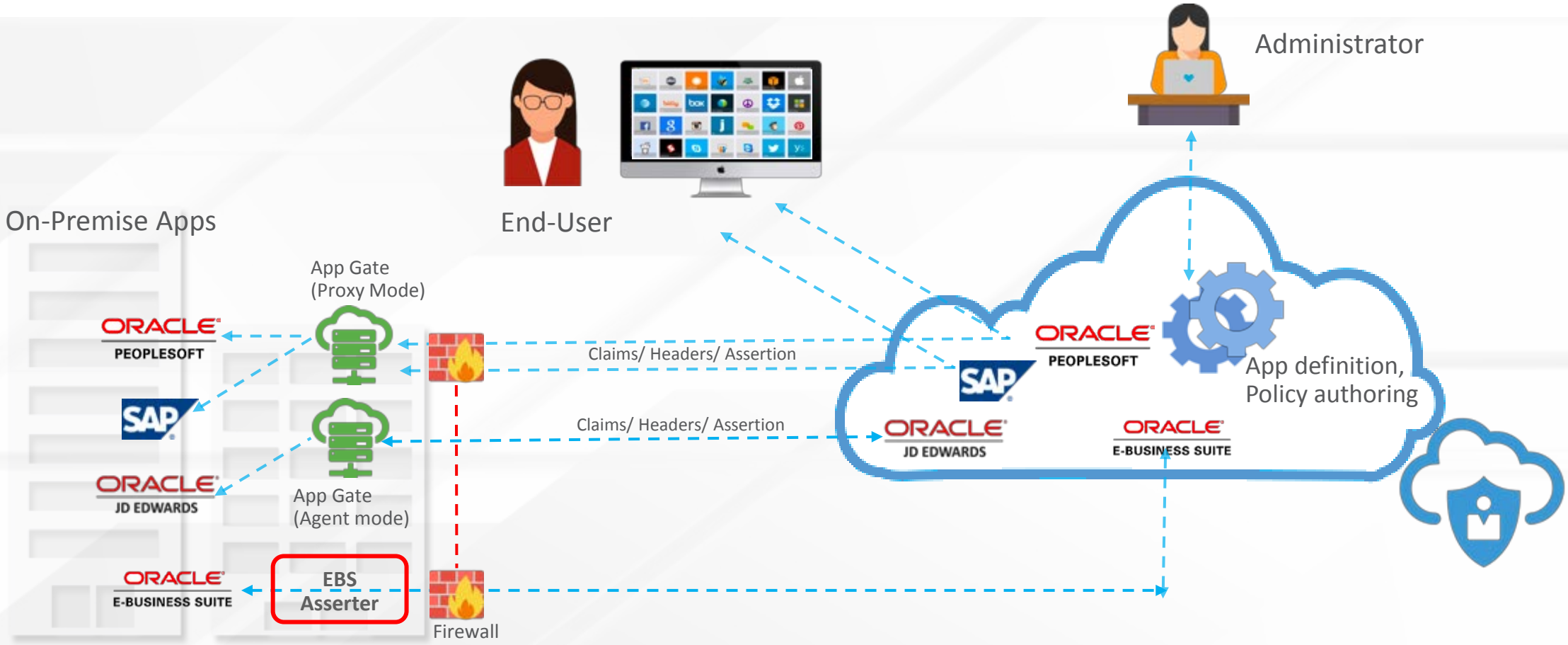


IDCS Integration with Oracle E-Business Suite

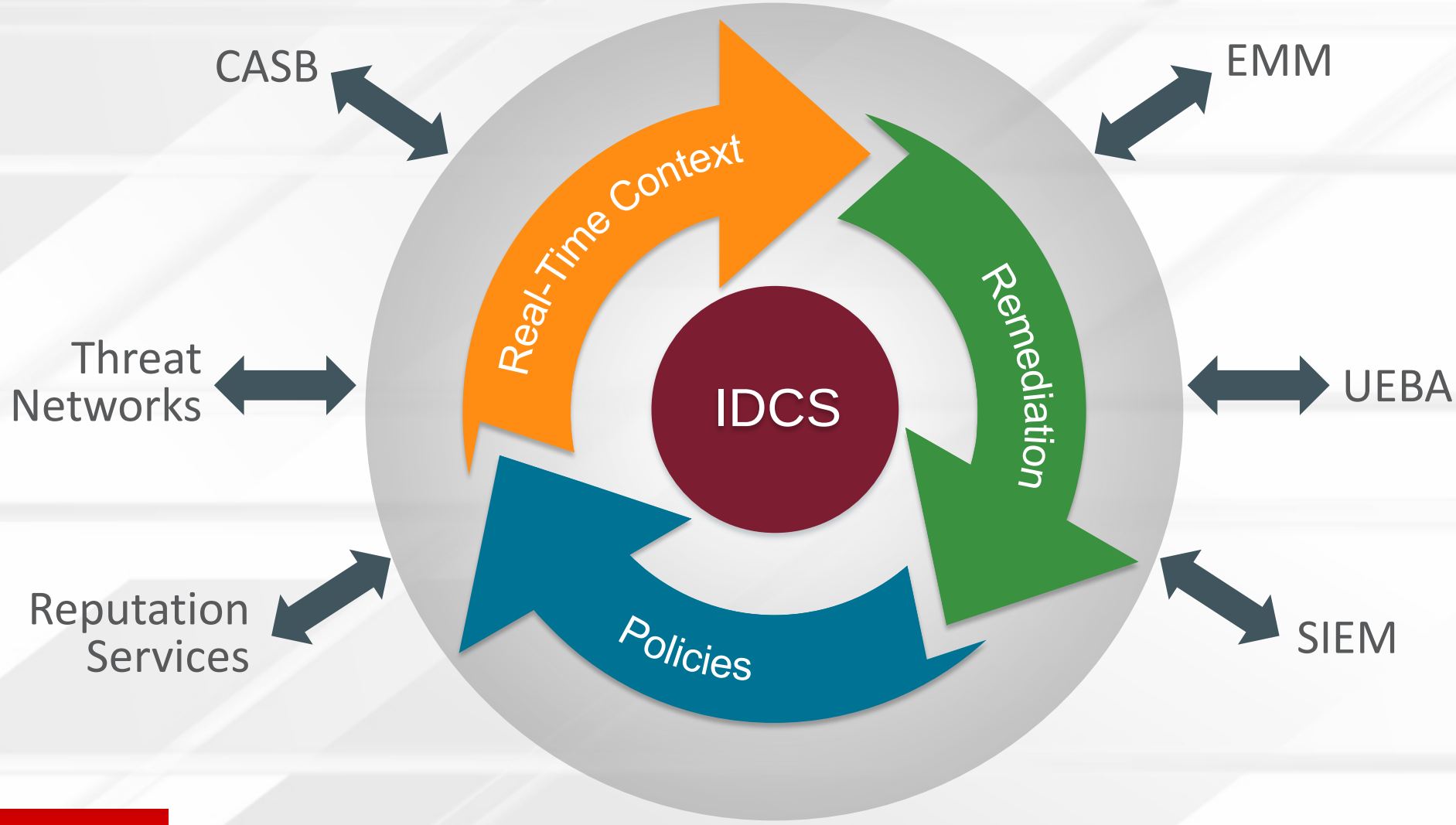


Oracle Identity Cloud Service

Integration with on-premises applications

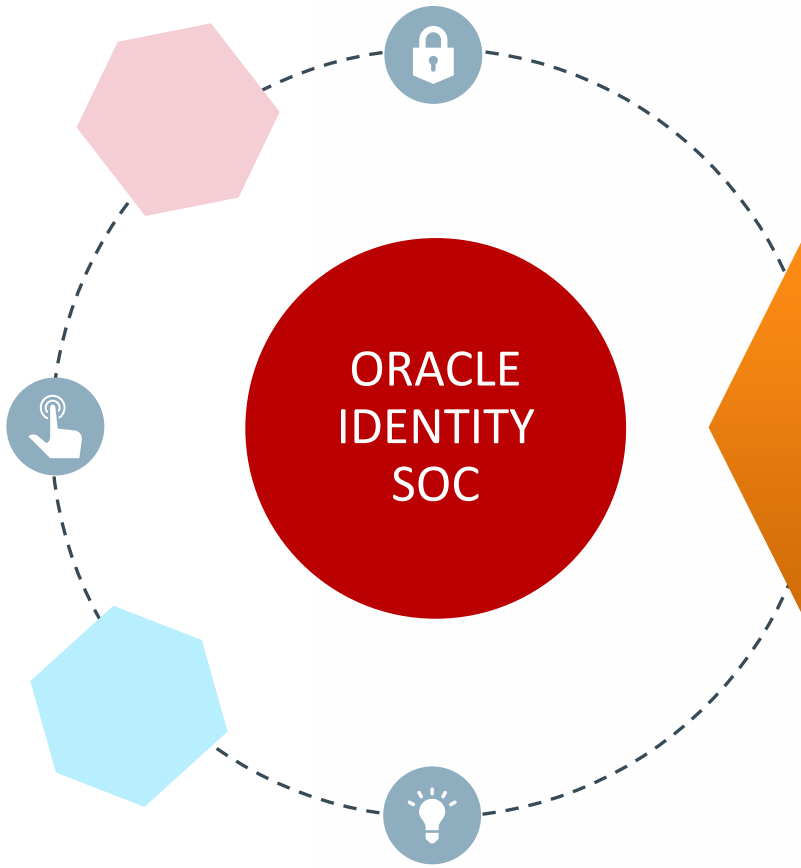


Identity as a Security Service



Cloud Access Security Broker Cloud Service (CASB)

Dynamic Risk-based Cloud Access Control with Oracle CASB



Dynamic Risk-Based Cloud Access Control

- Control User Access to Cloud Apps based on Real-time Session Context
- Prevent Privileged Account Misuse And Exfiltration with Risk-based Controls
- Remediate Risk In-Session with Step-up Auth or Dynamic Access Revocations

Protecting Cloud Apps with Adaptive Security

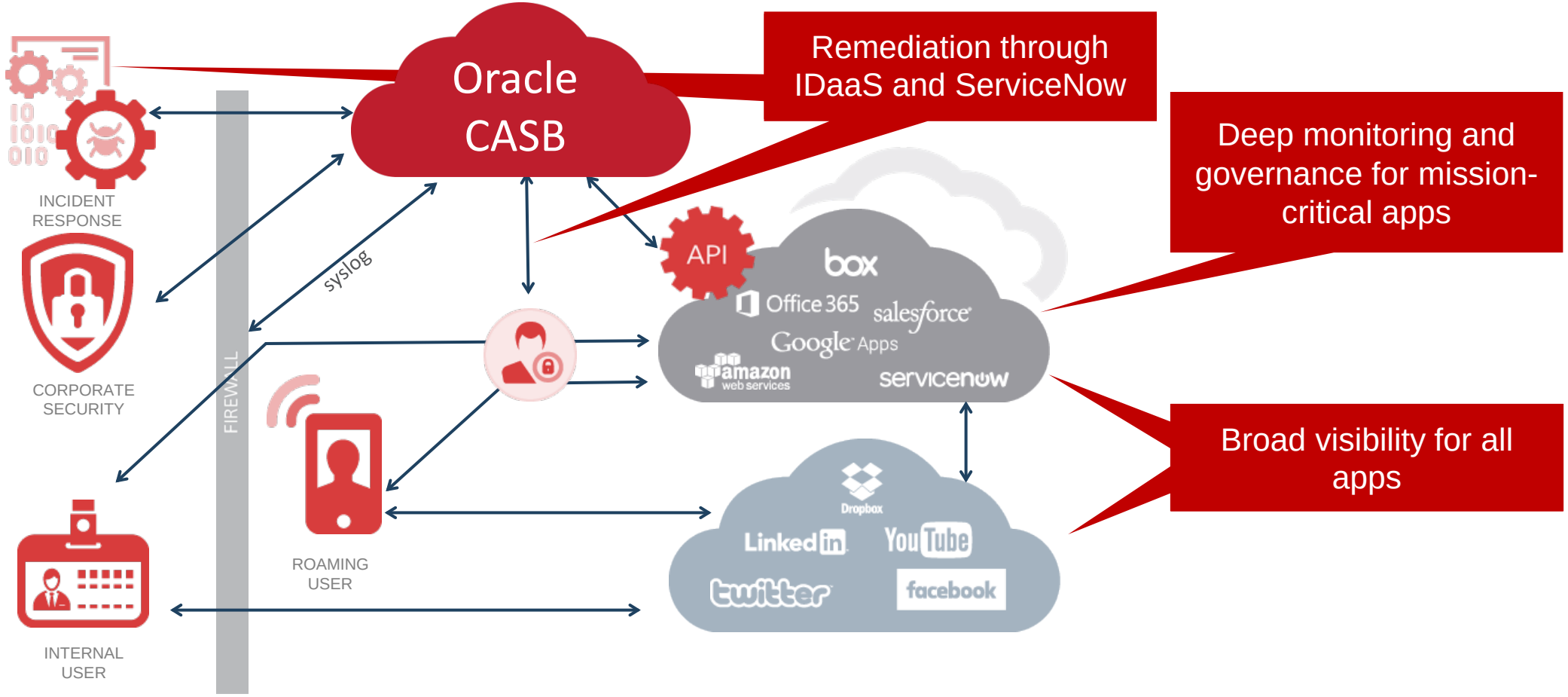
- Data Leakage Prevention (DLP) for additional contextual controls on sensitive content
- Advanced role monitoring of users, privileged administrators and PII information
- Machine Learning-driven Behavioral Analytics based on Device, Geo-location and real-time session attributes
- Enterprise Integrations with IDM, SIEM and ITSM for real-time remediation and alerting

Oracle CASB Cloud Service

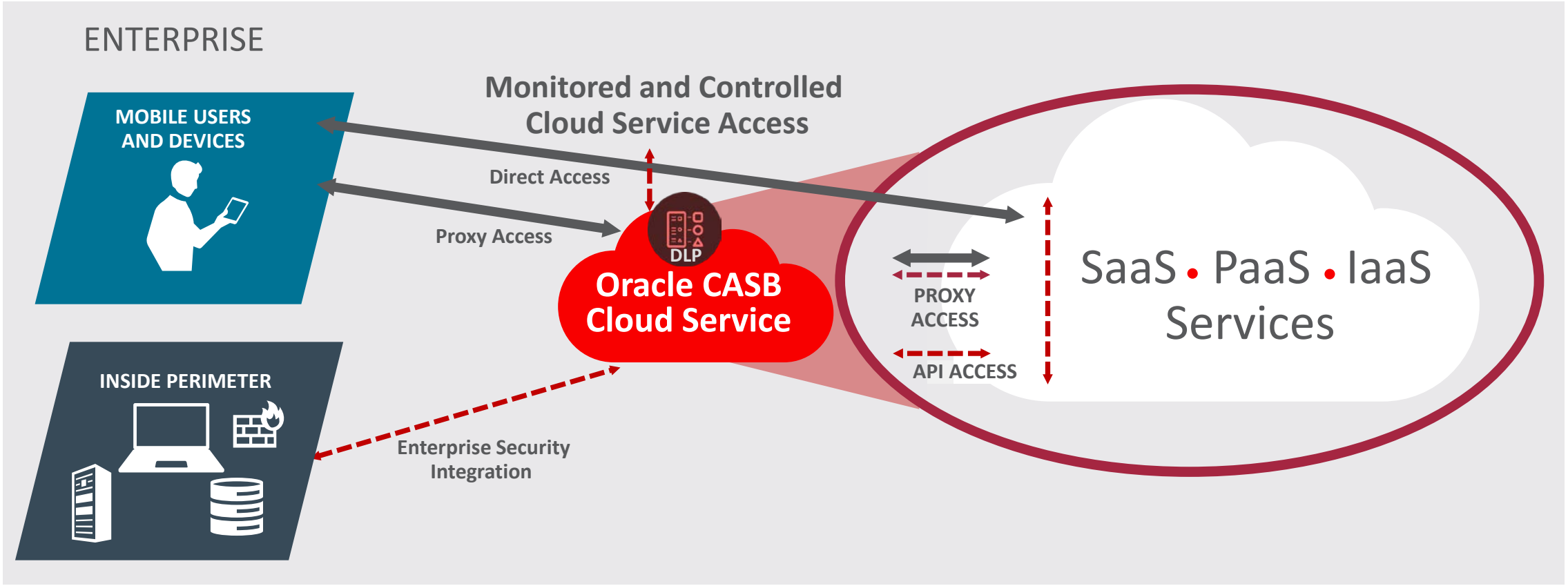
CASB – FOUR PILLARS OF FUNCTIONALITY

Visibility **Compliance** **Data Security** **Threat Protection**

Oracle CASB



Oracle's CASB: The only CASB to be deployed in <5 minutes



Oracle CASB – Top Use Cases

Visibility into All the Sanctioned Cloud Applications Used in the Enterprise

Discovery of Non-Sanctioned Cloud Applications Used in the Enterprise

Data Threat Detection for Cloud Applications

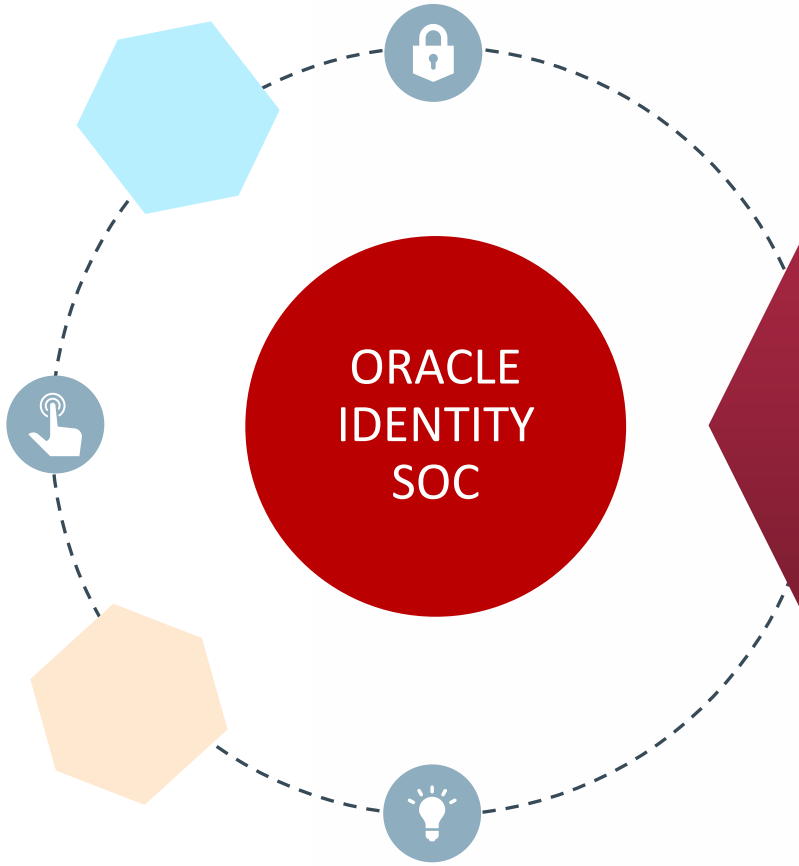
Comprehensive Data Security with DLP and Anti-Malware

Active Protection for Cloud Data and Cloud Applications

Oracle CASB Cloud Service

Oracle Management Cloud (OMC)

Autonomous-Driven Security with Oracle Management Cloud



ORACLE IDENTITY SOC

Automated Security Analysis and Response

- Unified and Heterogeneous Platform
- Maximize threat analysis and detections with integrated Machine Learning to spot suspicious patterns
- Leverage automated orchestration to respond / remediate risks

Oracle Management Cloud

- END USER EXPERIENCE / ACTIVITY
- APPLICATION
- MIDDLE TIER
- DATA TIER
- VIRTUALIZATION TIER
- INFRASTRUCTURE TIER

Global threat feeds
Cloud access
Identity

Real users
Synthetic users

App metrics
Transactions

Server metrics
Diagnostics logs

Host metrics
VM metrics
Container metrics

Configuration
Compliance
Tickets & Alerts

Security & Network events

- INTELLIGENT, UNIFIED PLATFORM
- POWERED BY MACHINE LEARNING
- INFORMED BY A COMPLETE DATA SET
- HETEROGENEOUS AND OPEN

ORACLE

OMC Key Capabilities

Unified Monitoring

- Application & Infrastructure Monitoring
- Complete Transaction Visibility
- Real, Mobile & Synthetic Users

Log Management

- Monitor, aggregate, and analyze
- Topology-Aware log exploration
- Deep support for Oracle

Analytics

- Out-of-the-box ML
- IT Analytics
- Pre-built dashboards
- Data Explorer

Remediation

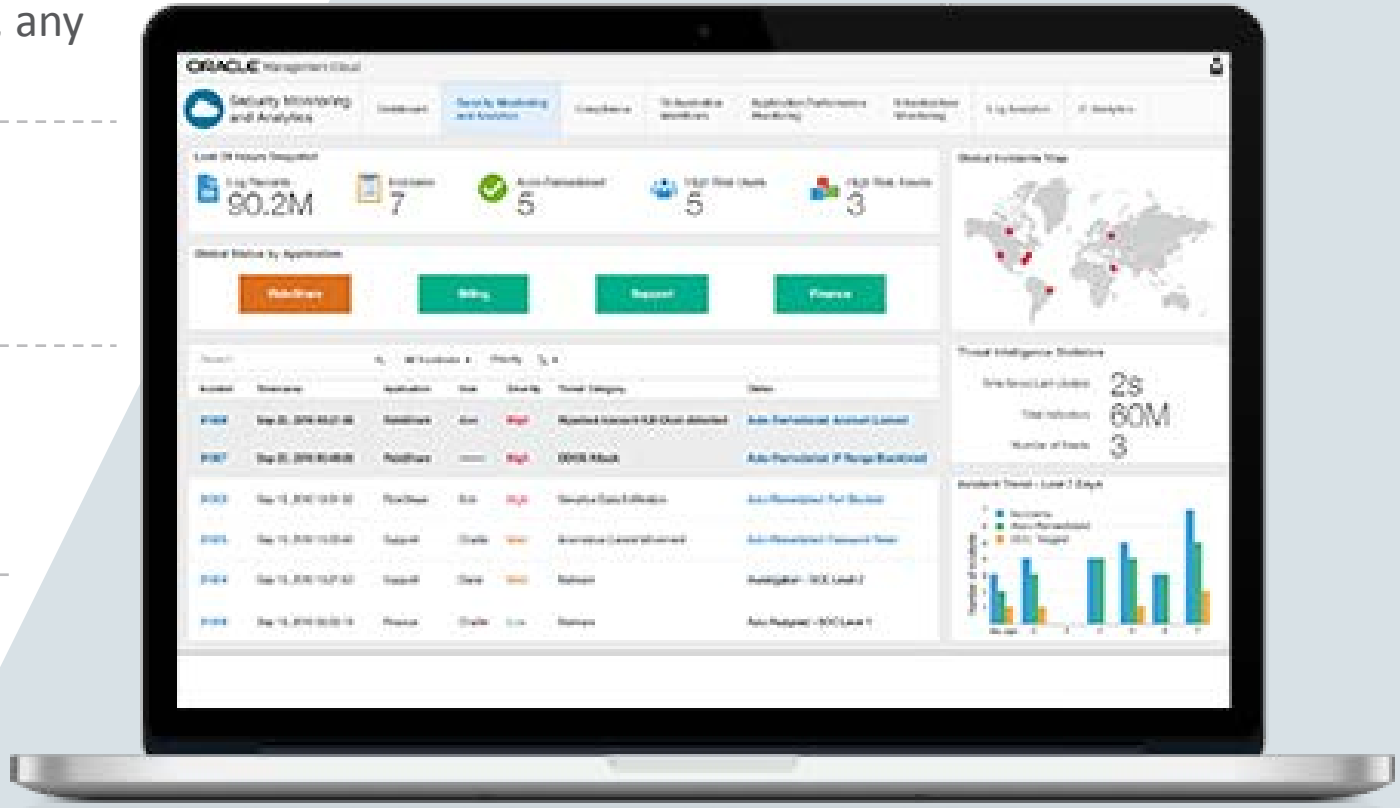
- Automated actions and runbook
- Simple & complex workflows
- Integrations with 3p systems

Security

- Security Monitoring
- User Behavior
- Incident Response
- Config. & Compliance

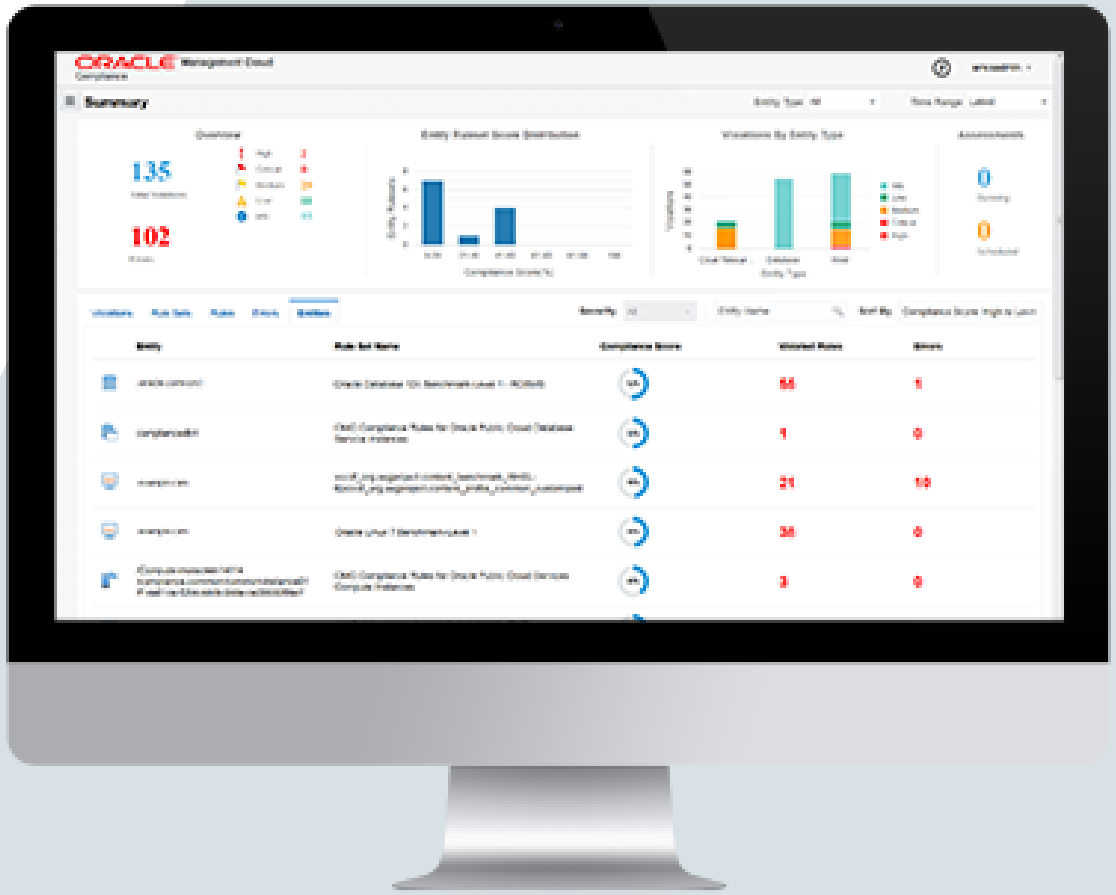
Security Monitoring and Analytics Cloud Service

- **Comprehensive Detection**
  - Any log, any intelligence feed, any metric, any location (on-premises or cloud)
- **Rapid Investigation**
  - Intuitive visualization of threats and early warning signs
- **Intelligent Remediation**
  - Powerful auto-remediation framework for any IT stack
- **Faster Time to Value**
  - Next-gen cloud service with SOC ready content



Configuration and Compliance Cloud Service

- **Efficient & Actionable**
  - Quickly determine your enterprise compliance posture and remediate violations
- **Extensible**
  - Execute custom scripts and enforce your organization's standards
- **Application & Cloud Aware**
  - Assess compliance against infrastructure and applications stacks, on-premises or in the cloud
- **Standards Based**
  - Execute industry standard compliance benchmarks at cloud scale

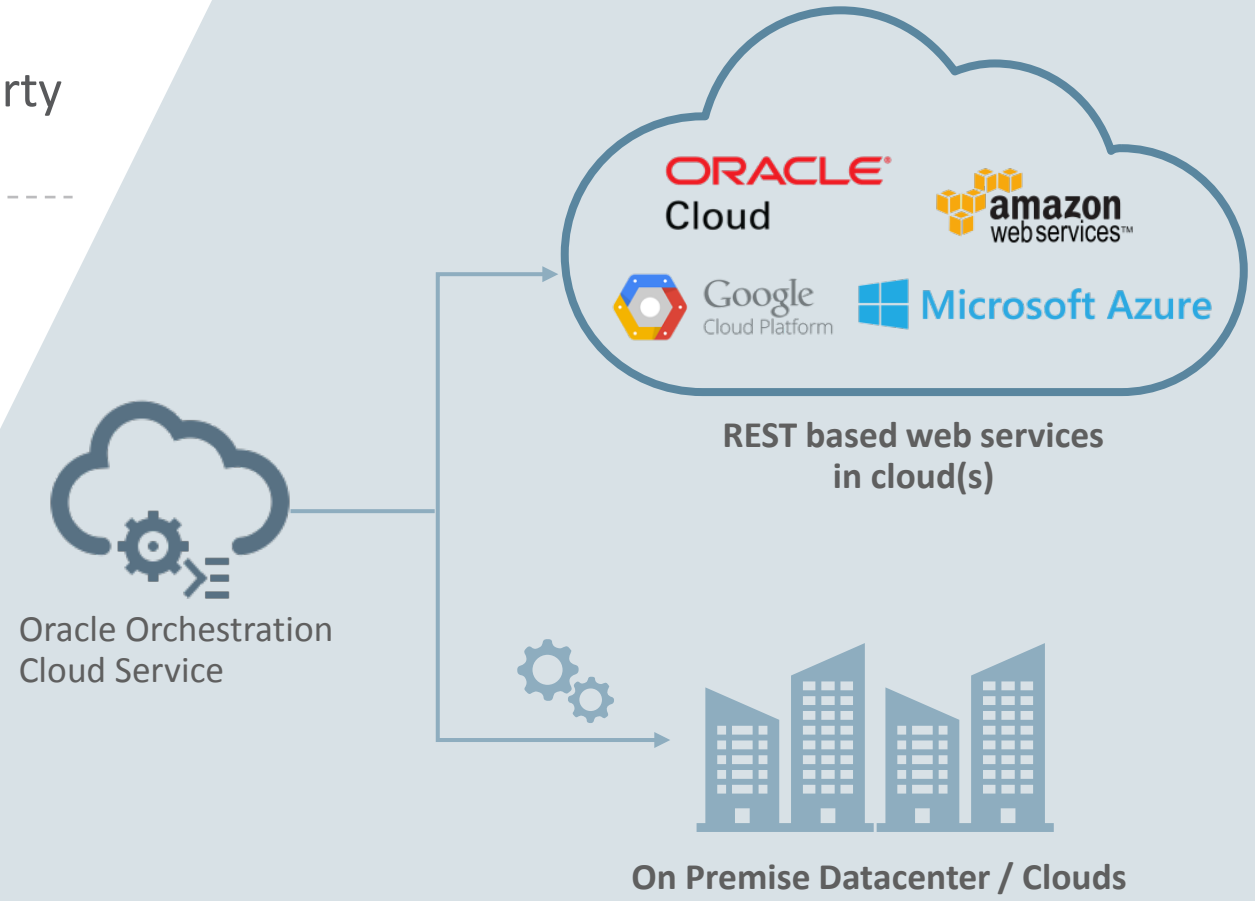


OMC Orchestration Cloud Service

For Automated Remediation

- **Invoke** scripts, web service endpoints or 3rd party automation frameworks

- **Use Cases**
  - See infected device, move to quarantine VLAN, run AV update and scan
  - Enforce password reset or two-factor authentication (Identity Management)
  - Block the associated domain or IPs on the internet gateway (firewall, web filtering)
  - Open incidents in Service Now or Jira

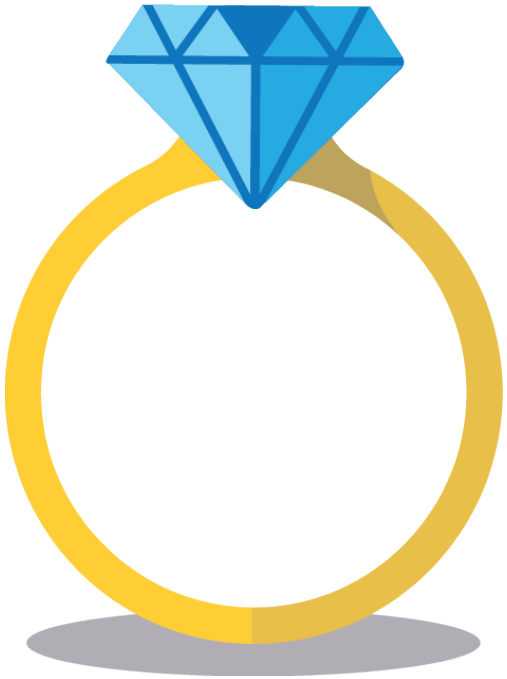


Use Cases

Top 5 Cloud Threats | 2018

1 Fraud

Multinational insurance and finance company…..suffered a $30 million net loss from the massive fraud



THE multinational insurance and finance company … suffered a $30 million net loss from the massive fraud committed by its senior accountant, court documents reveal.

While most of the incredible haul of luxury goods and property purchased with the money - including $16 million worth of jewelry and eight waterfront apartments - has been recovered and resold by the company, it has taken a substantial hit.

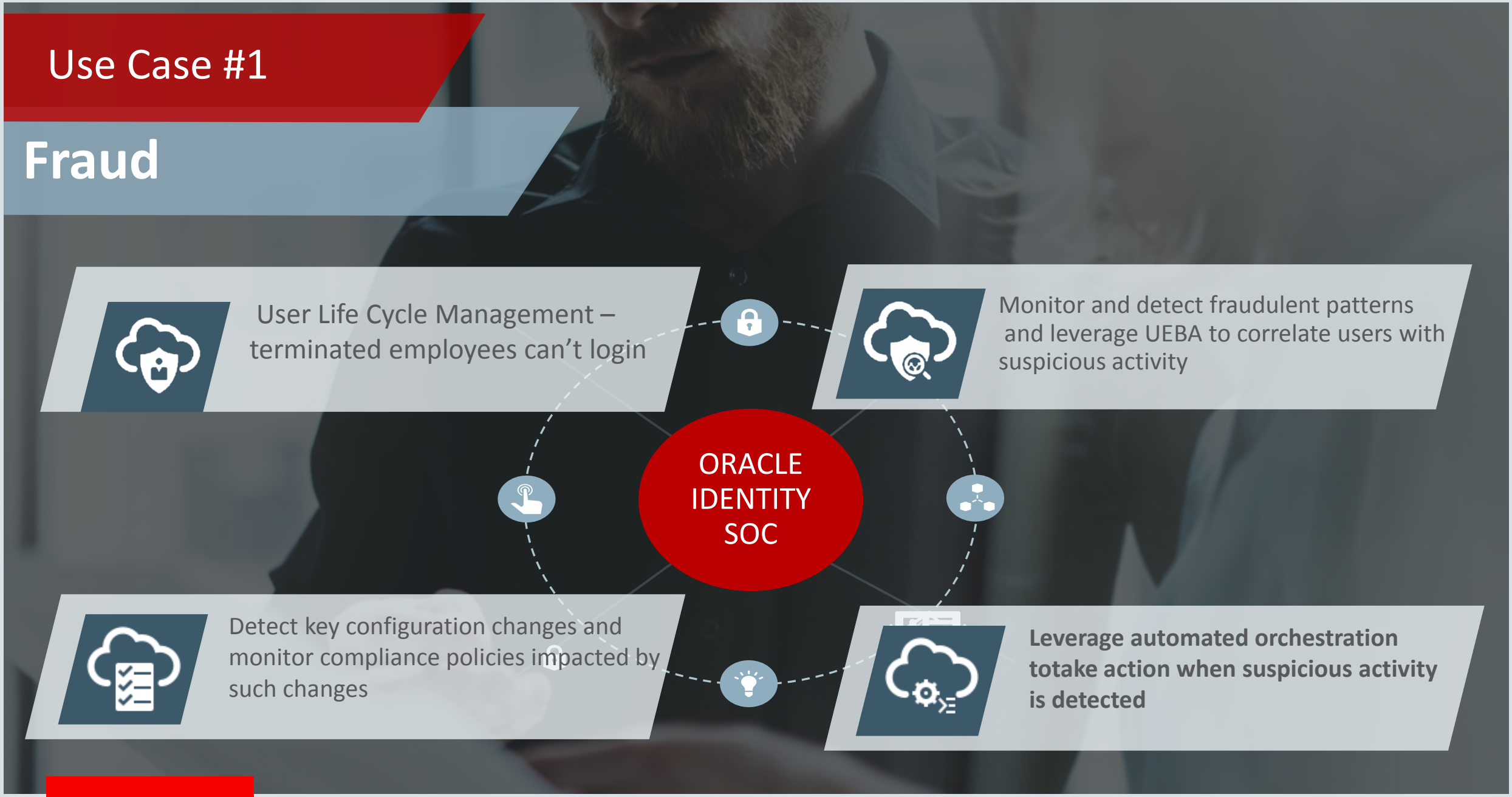
It is understood the fraudster did not have any formal accounting qualifications, but had worked her way up from the position of assistant accountant. As a senior accountant she made 200 illegal transfers into her personal accounts or directly to shops and real estate agents.

She then used the computer log-ins of former staff to delete the records or alter them so the transactions appeared legitimate.

ORACLE

Use Case #1

Fraud



Top 5 Cloud Threats | 2018

2 Cloud Scams

Protect Your People: Newest Cloud HCM -Focused Scam Reroutes Employee Direct Deposit Funds

“Another week, another well-concocted phishing scam. The most recent fraudulent activity targeted businesses that use Workday, though this is not a breach or vulnerability in Cloud HCM itself. Specifically, the attack involves a well-crafted spam email that is sent to employees purporting to be from the CFO, CEO, or Head of HR or similar.

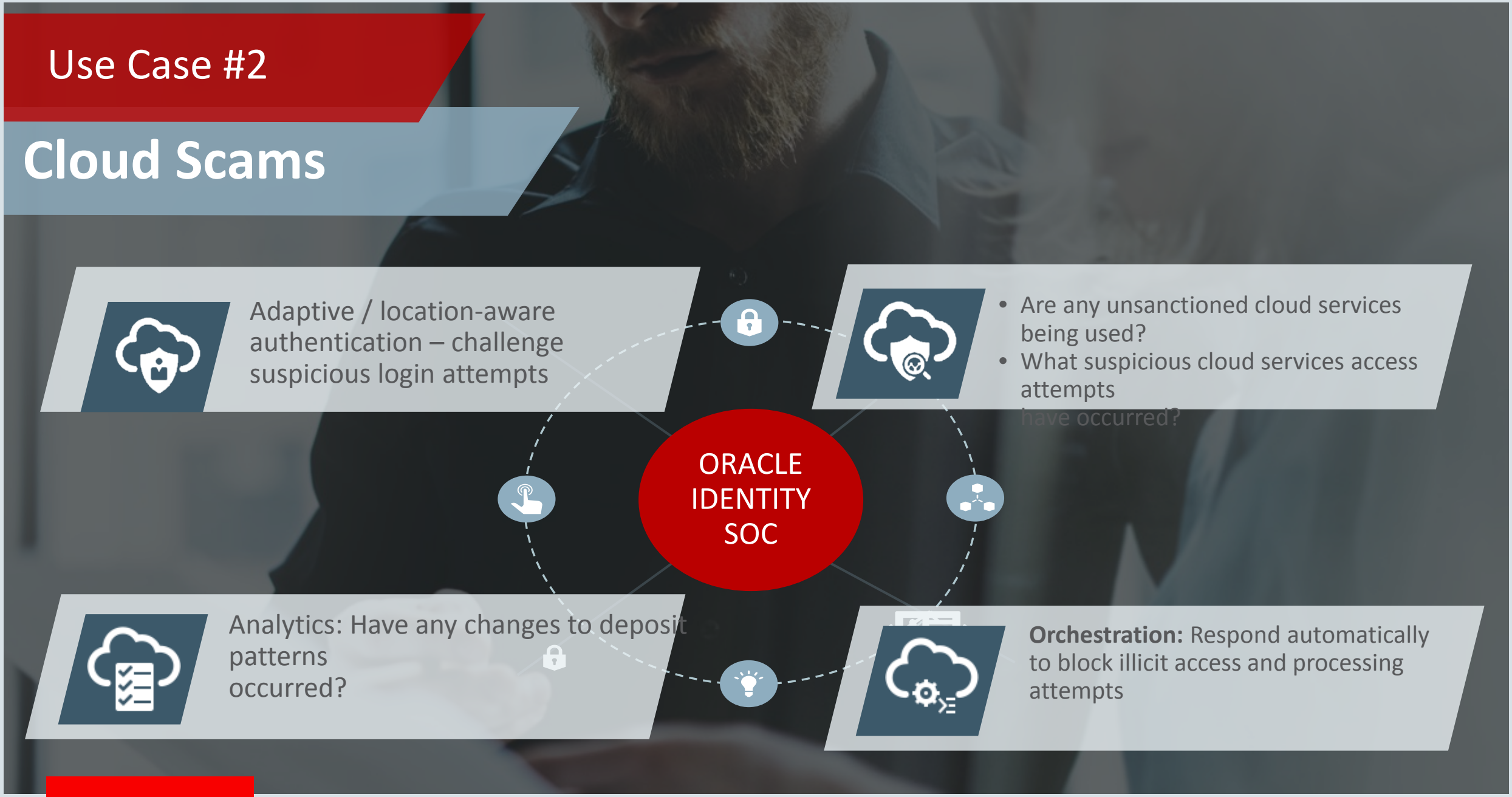
Sometimes the emails include the name, title, and other personal information of the “sender” that we believe might be harvested from LinkedIn or other business databases. The email asks employees to use a link in the phishing email or attached PDF to log into a fake Workday website that looks legitimate. **The threat actors who run the fake Cloud HCM website then use the user name and password to log into the Workday account as the employee and change their direct deposit bank/ACH information to another bank, relatable Green Dot, or similar credit card.**

The fraud is typically only discovered when the employees contact HR inquiring as to why they did not receive their direct deposit funds. Unfortunately it appears that spam filters and other controls are failing to prevent this email from infiltrating the organization’s network.”

ORACLE

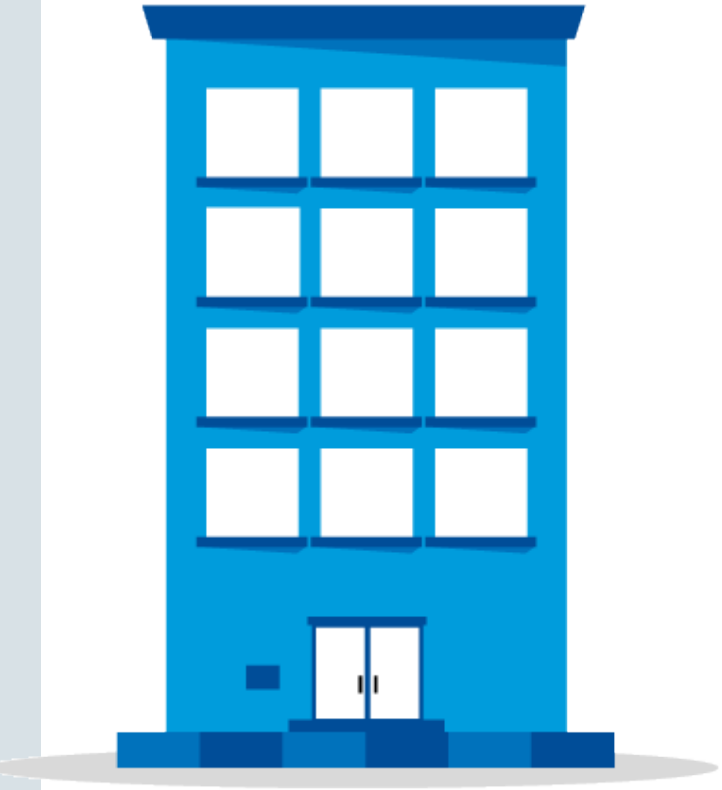
Use Case #2

Cloud Scams



Top 5 Cloud Threats | 2018

3 Data Theft



…a 3rd party provider for a Large US Government Agency, was hacked

Hackers infiltrated a third-party software packaged(Cloud & On-Premise) in 20XX with the goal of collecting personal records on federal employees and contractors with access to classified intelligence, according to the government's largest private employee investigation provider.

That software package was an SAP enterprise resource planning application.

Assailants infiltrated the agency by piggybacking on an "exploit," that was "present in a widely used and highly-regarded enterprise resource planning ('ERP') software package," to carve out sensitive data while allowing the interface program to appear to execute as expected.

ORACLE

Use Case #3

Data Theft

Identity: What access controls are in place? Are all access attempts in harmony with audit standards?

Cloud Access Security Broker : Are cloud services being secured as per audit standards? Was email to outsiders coming from appropriate sources?

Security Monitoring and Analytics: What illicit access attempts were detected?

Configuration and Compliance: What changes have occurred? What change controls are in place?

Top 5 Cloud Threats | 2018

4 Data Exposure

…Customer Records for Millions of Large Wireless Company's Subscribers Exposed

Cloud security research firm found a **misconfigured cloud-based file repository containing the names, addresses, account details, and account personal identification numbers of millions of large wireless company customers**.

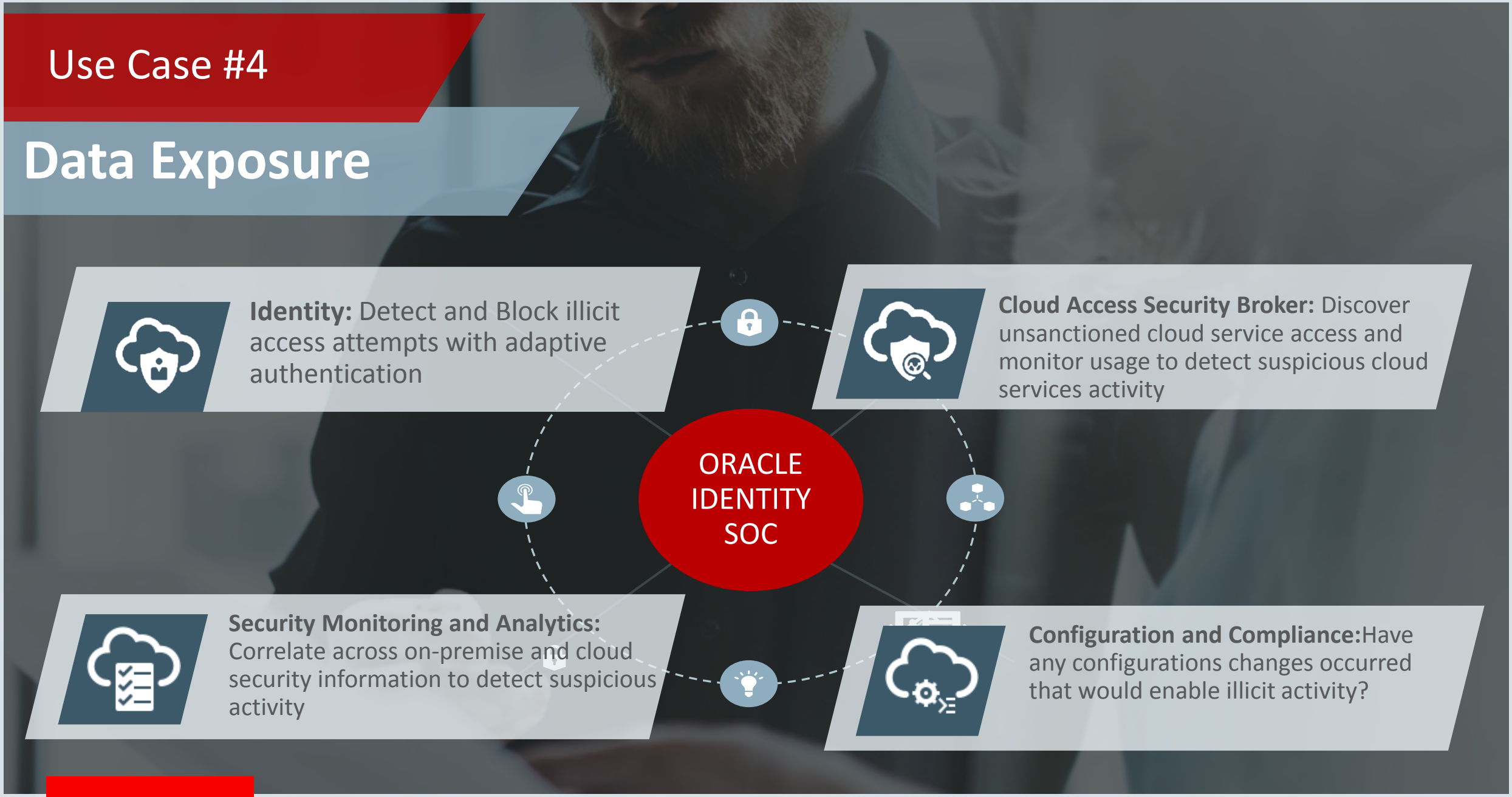
The firm came to this number after analyzing the average number of accounts exposed per day in the sample that was downloaded.

The data dump—on a publicly accessible AWS S3 bucket owned and operated by a third-party software and data company called NICE systems—appears to have been created to track customer call data for "unknown purposes,"…

ORACLE

Use Case #4

Data Exposure



Identity: Detect and Block illicit access attempts with adaptive authentication

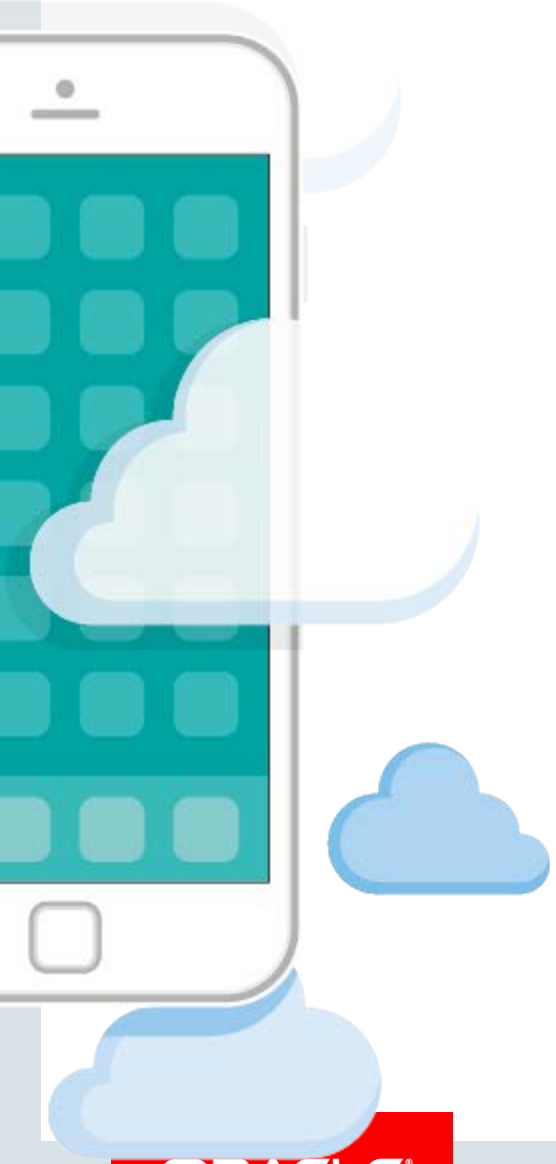
Cloud Access Security Broker: Discover unsanctioned cloud service access and monitor usage to detect suspicious cloud services activity

Security Monitoring and Analytics: Correlate across on-premise and cloud security information to detect suspicious activity

Configuration and Compliance: Have any configurations changes occurred that would enable illicit activity?

Top 5 Cloud Threats | 2018

5 Cloud Ransom



Large State Voter Database Exposed Online (Again), Held for Ransom (Again)

For the second time in two months, the voter registration information of over 19 million people was leaked online via an unsecured MongoDB database, which was later held for ransom by hackers.
This second incident originates with a newspaper, which acknowledged the breach in an article published on its site.

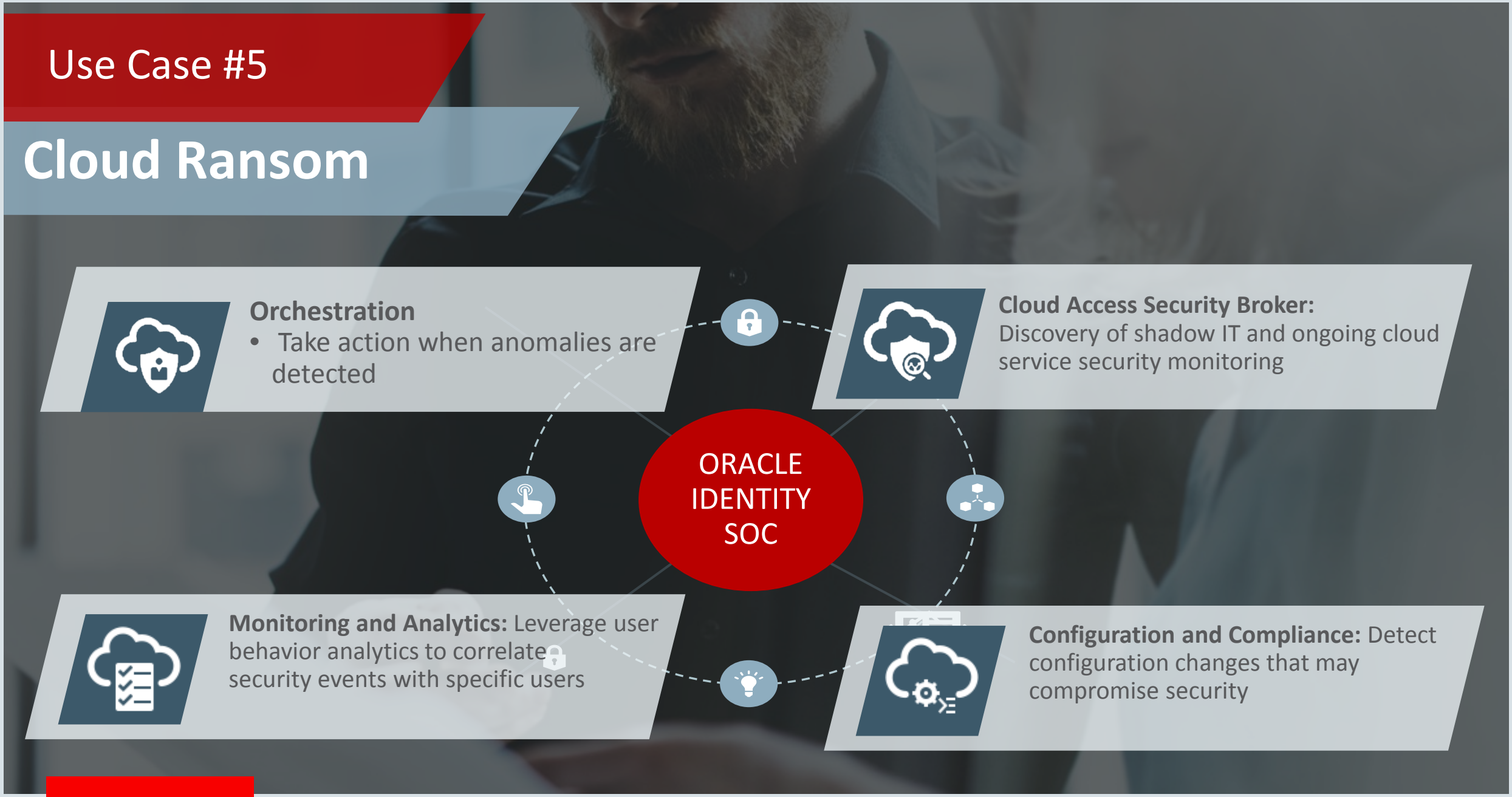
Newspaper says the ransomed database contained voter registration data from the Secretary of State and contact information for 53,000 current and former newspaper subscribers who registered accounts prior to 2017.

Instead of paying the ransom, the newspaper said it deleted the database for good and will notify affected subscribers of the breach.

ORACLE

Use Case #5

Cloud Ransom



Orchestration
- Take action when anomalies are detected

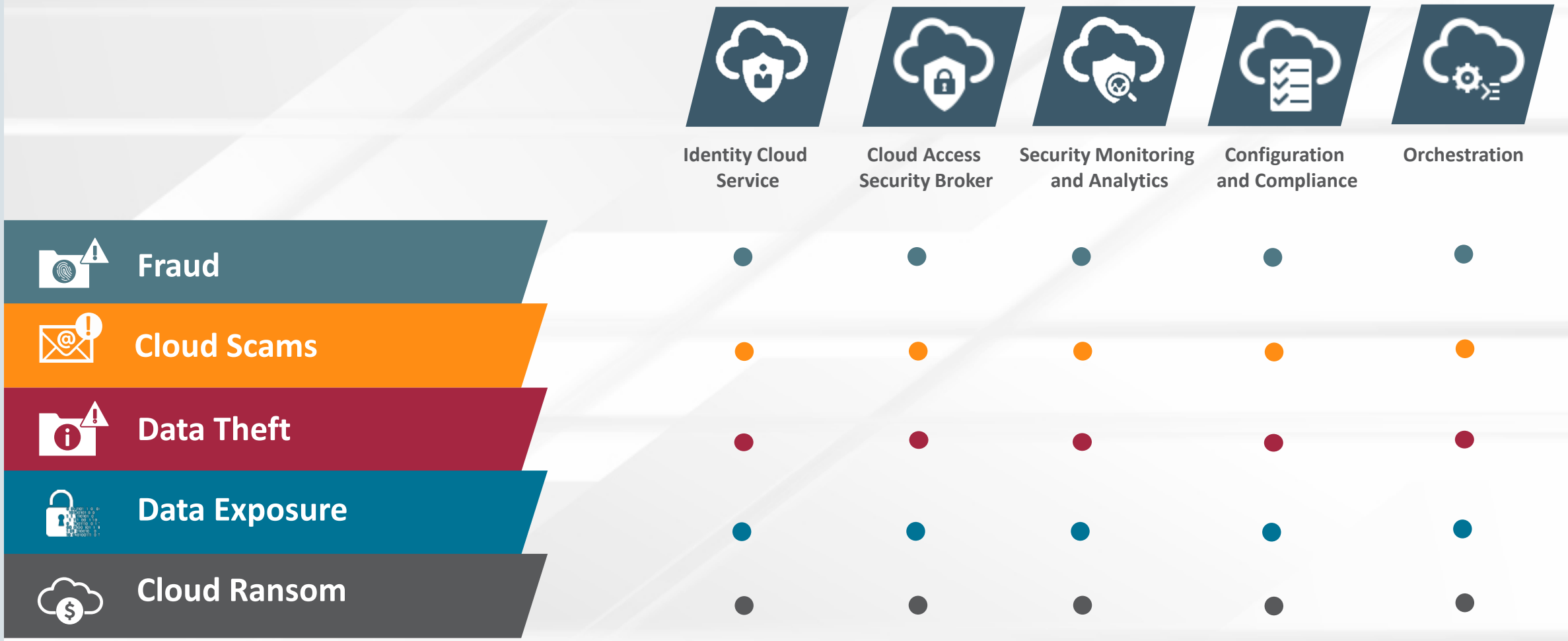
Cloud Access Security Broker: Discovery of shadow IT and ongoing cloud service security monitoring

Monitoring and Analytics: Leverage user behavior analytics to correlate security events with specific users

Configuration and Compliance: Detect configuration changes that may compromise security

ORACLE

Oracle Cloud Security: Addressing the Use Cases



Call To Action

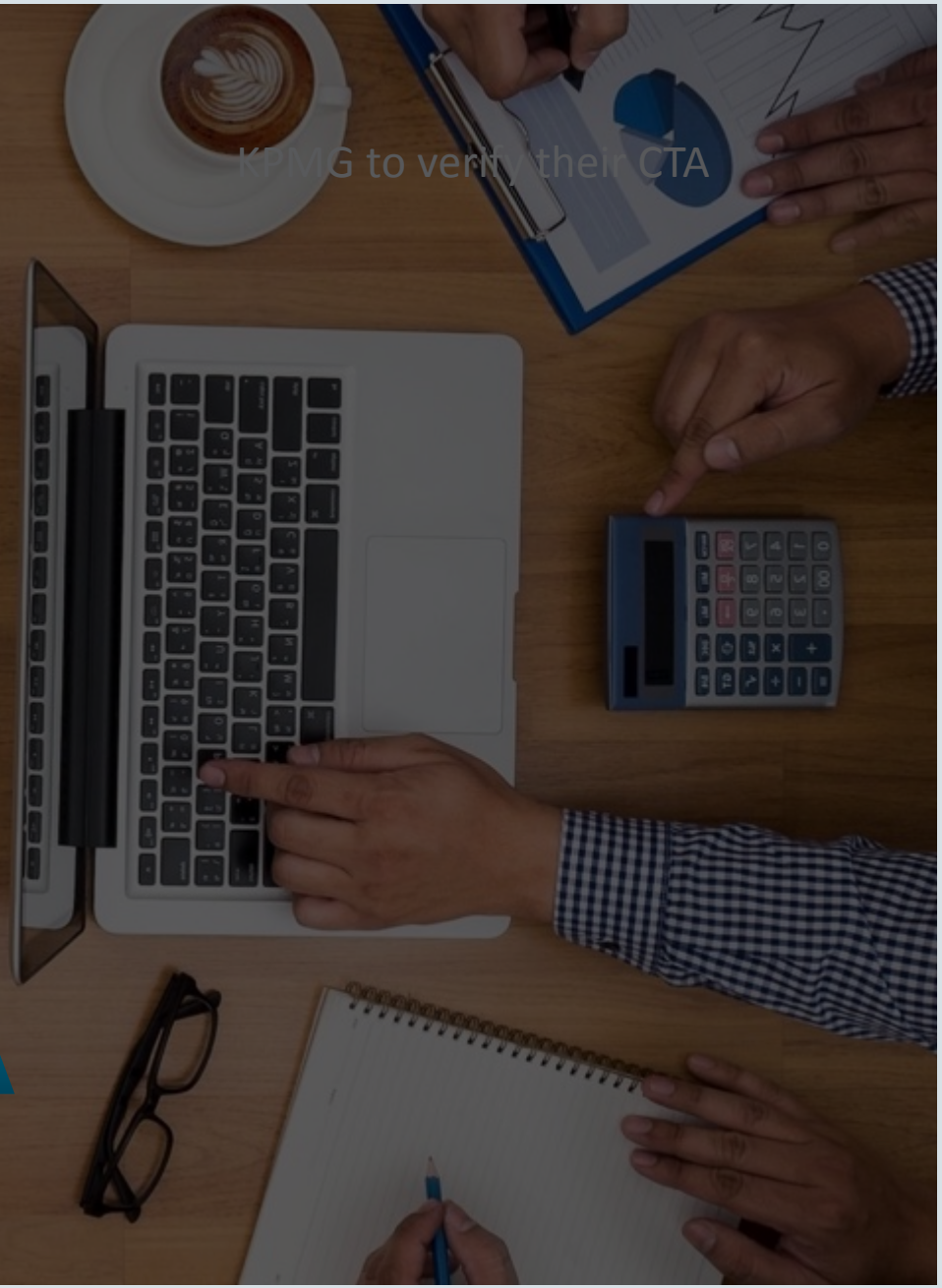
KPMG to verify their CTA

Pre-register: The Oracle and KPMG Cloud Threat Report

Request KPMG Security Assessment

Request Oracle Cloud Security Assessment

Free Cloud Trial



LUNCH

The Oracle and KPMG Cloud Threat Report

An Inside Look and Discussion

- Akshay Bhargava (Oracle)
- Brian Jensen (KPMG)

What is the Oracle KPMG Cloud Threat Report?

- Global survey-based report, 450 participants from 5 countries (UK, Cn, US, Aus, Sin)
- Focus on the key security issues impacting customers along their journey to the cloud
- Cloud security architects, application owners, DBsec, C-level, DevSecOps, risk & compliance owners
- Key analysis from both Oracle and KPMG on the drivers behind the statistics and metrics

Source: Ponemon Privacy & Security of Healthcare Data, 2016

Is Your Ability to Secure Keeping Pace With Your Need to Scale?

90%
CATEGORIZE HALF, OR MORE, OF THEIR CLOUD-RESIDENT DATA AS **SENSITIVE**

51%
CANNOT **ANALYZE** THE MAJORITY OF THEIR **EVENT DATA**

MALWARE
IS STILL THE TOP CONCERN TOPPING OUT **4** OUT OF **TOP 5 THREAT TYPES**

2018 Oracle KPMG Cloud Threat Report : Keeping Pace At Scale

CLOUD ADOPTION

- **61%** report NOC and SOC teams **collaborate**
- **87%** of organizations have a **cloud-first orientation**
- **36%** have cloud-related **security event mgmt challenges**

THREATS & CHALLENGES

- **66% have experienced a cyber-attack that has disrupted business**
- While **97% have a cloud app policy**, only **28% are "very concerned"** about violations.

APPROACHES

- **#1** cybersecurity challenge is detecting and reacting to security incidents in the cloud
- **66%** are interested in **adaptive MFA**
- **91%** use **NPM/APM** as an identifier for threats

*2018 Oracle KPMG Cloud Threat Report **www.cloudthreatreport.com** Available April 16, 2018

Oracle Cloud Security Test Drive

- IDCS
- CASB
- OMC


ORACLE®

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia