Agenda

- Challenges in Cloud Security
- Identity SOC Introduction
- Cloud Identity Service
- Cloud Access Security Brokers
- Security Monitoring and Analytics
- Q&A

The Era Of The Cloud Is Transforming…

Data and applications are moving to the Cloud and users need *anywhere, anytime, anyway* access.

Traditional Approaches Have Not Kept Pace…

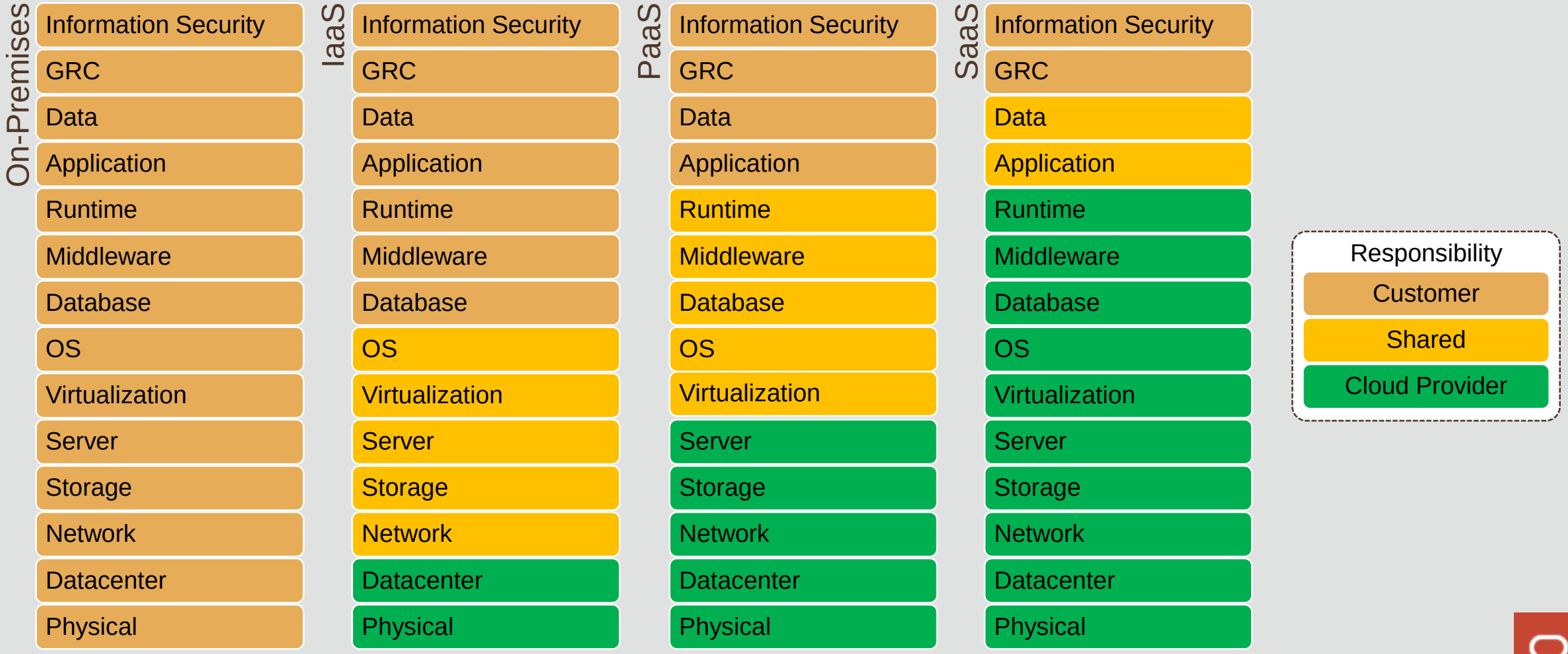
Most enterprises need to secure identities across on-premise and cloud applications, but are forced to use siloed systems that don't integrate well.

The Future Is Clear…

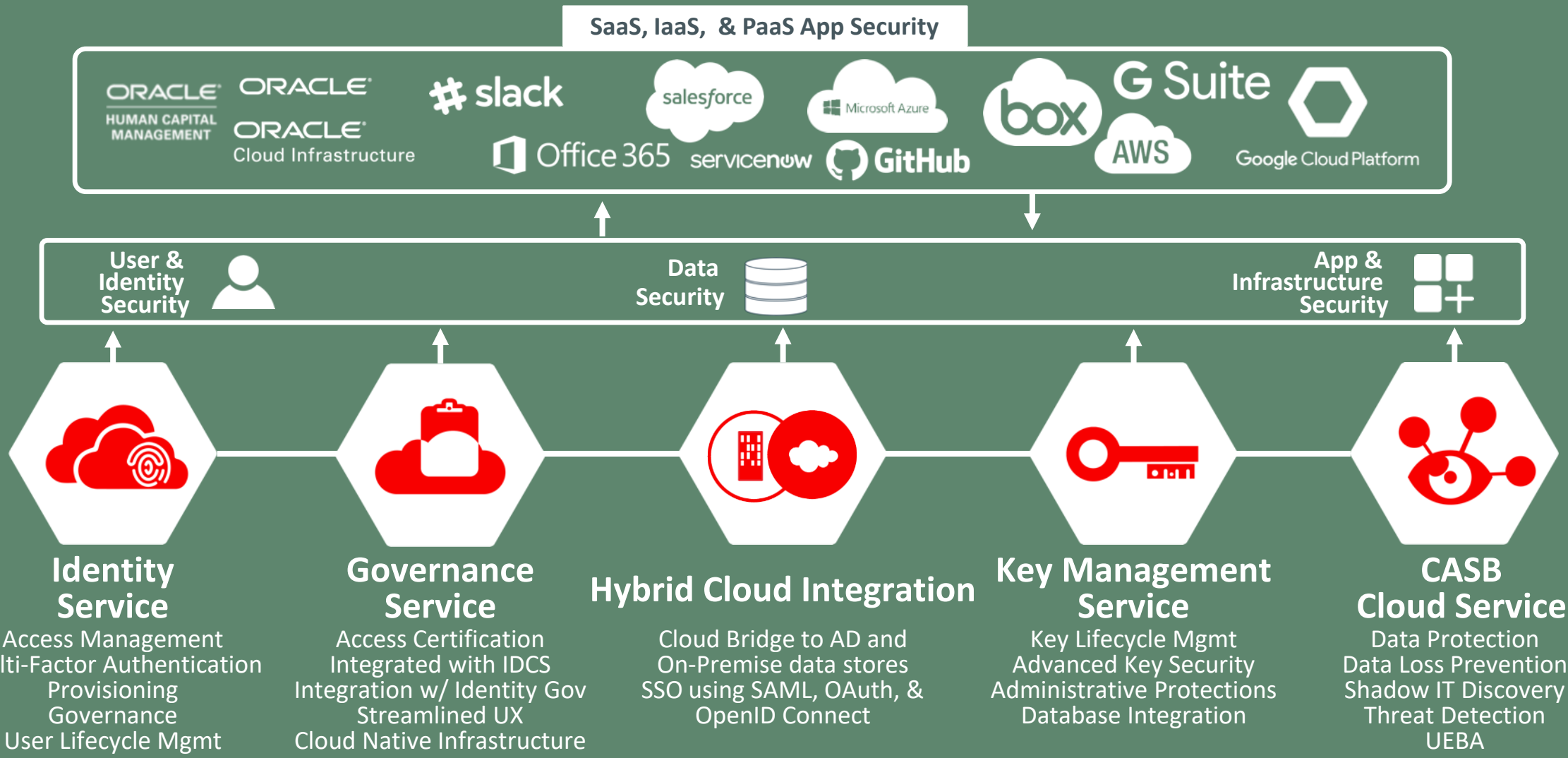
Imagine a hybrid system that's engineered to scale with your business and provides simple, secure, on-demand access to cloud and enterprise apps.

Cloud Platform Security: Shared Responsibilities

"Through 2022, at least 95% of cloud security failures will be the customer's fault." - Gartner



Introducing Identity Based Security Operation Center



Identity SOC Overview

External Threat Scenario

- **THREAT SCENARIO**
  - !DBA compromised by spear-phishing attack
  - !Malware harvests credentials, queries DBs over time
  - !Malware contacts external command & control hosts
- **SMA SOLUTION**
  - ✓ SQL anomaly detection identifies anomalous SQL query for DBA account
  - ✓ Attributes account to specific user & adds user to watch list for closer monitoring
  - ✓ Visually presents sequence of attack chain
- **SECURITY CHALLENGE**
  - 0-day attack evades perimeter/endpoint protection
  - Static, frequency based rules miss low & slow attack
  - No ability to detect anomalous SQL queries by user
- **SMA ENABLING FEATURES**
  - Correlation rules engine
  - SQL query anomaly detection
  - Multi-dimensional behavioral anomaly detection
  - Kill chain visualization

Security Monitoring and Analytics

Protect enterprise wide assets from known and zero-day threats

- Security monitoring visibility across heterogeneous on-premise and cloud assets
- Efficient SOC monitoring with OOTB content for modern threats (rules, anomalies etc.)
- Continuous threat intelligence context (URL/IP classification & reputation)

Detect threats early using machine learning driven analytics and visualization

- Data access (SQL based) anomalies at the user, group, database and application level
- Nuanced anomalies through multi-dimensional baselines (ex: user logins by location, time, host etc.) etc.)
- User session awareness and attack chain visualization (ex: account hijacking)

Harness Monitoring tools and cross-service context for richer security monitoring

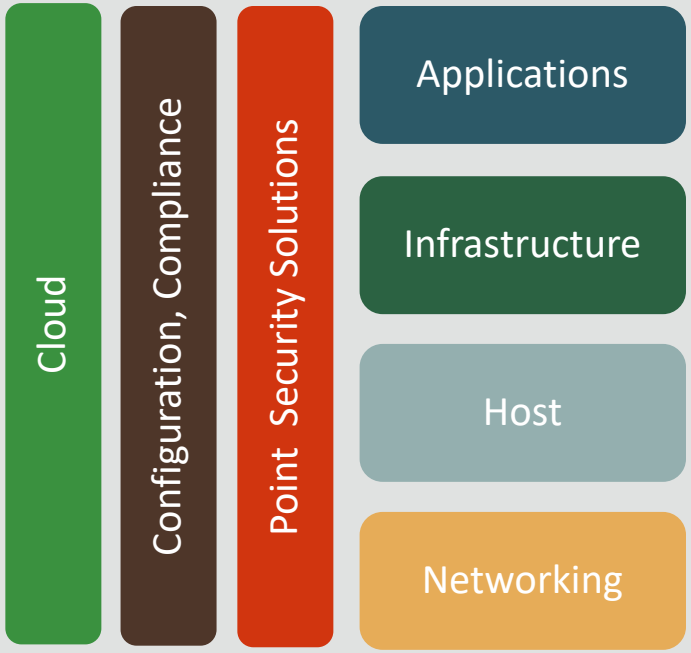
- Continuous configuration drift context in security monitoring
- SOC auto-remediation (account lockouts, port or other configuration change) with Orchestration Orchestration

Data Collection

Heterogeneous activity data sources (formats, stacks, locations)

Extensive data enrichment (identity, asset, threats)

Hybrid configuration assessment results



- IaaS, PaaS, SaaS
- 3rd party applications, Custom applications
- Directory services, Middleware, Database, Hypervisor
- Windows, Linux, Unix
- DHCP, DNS, Load balancer, Flow, Router, Switch
- Firewall, Proxy, VPN, IDS/IPS, AV, DLP, VA scanners, CASB, TIF

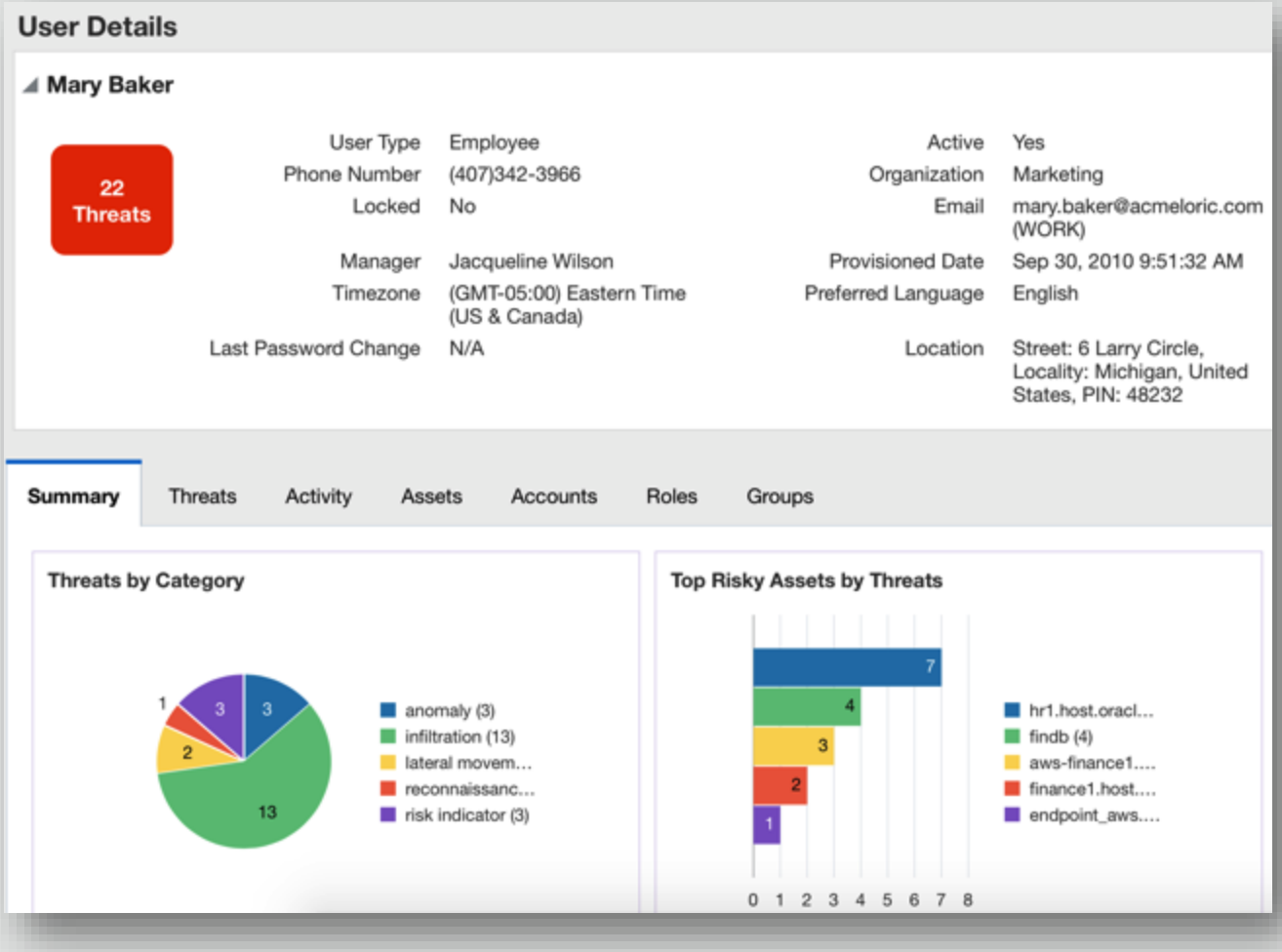
Analysis: Session Awareness - Identity Correlation

Composite identity awareness

- Rich user data model and adapters for identity data sources enable 360 degree user monitoring across all identities
- Security logs are continuously enriched with user context

Activity to identity extrapolation

- Logs with explicit identity context like VPN are used to session and attribute identity to other logs that lack user context



Analysis: Context Awareness, Context Correlation

Users

- Is this a privileged user?
- Is this user on a watch list? (privileged, terminated, suspicious)
- Has this user (across identities) taken other anomalous actions?

Assets

- What is the business role, regulatory classification of a targeted asset?
- Is the asset tied to other recent suspicious or anomalous activity?
- What vulnerabilities is a server exposed to / not patched for?

Threats

- How reputable is a URL being accessed by an end user?
- Is the anomalous communication with a known malicious IP address?
- What category of sites poses the most risk given user browsing behavior?

Analysis: Using Correlation Engine

Insider Threat: Brute force attack

Rule: X failed logins + successful login within 1 min

Context: Asset criticality = High

Compliance: Account misuse (SOX)

Rule: User account created & deleted within 24 hours

Context: Asset role = Production; User Group = Accounting

External Threat: Hijacked account

Rule: Simultaneous user login from multiple locations

Context: Login IP address on *Latest Malicious IP* watchlist

Rules Engine Primitives

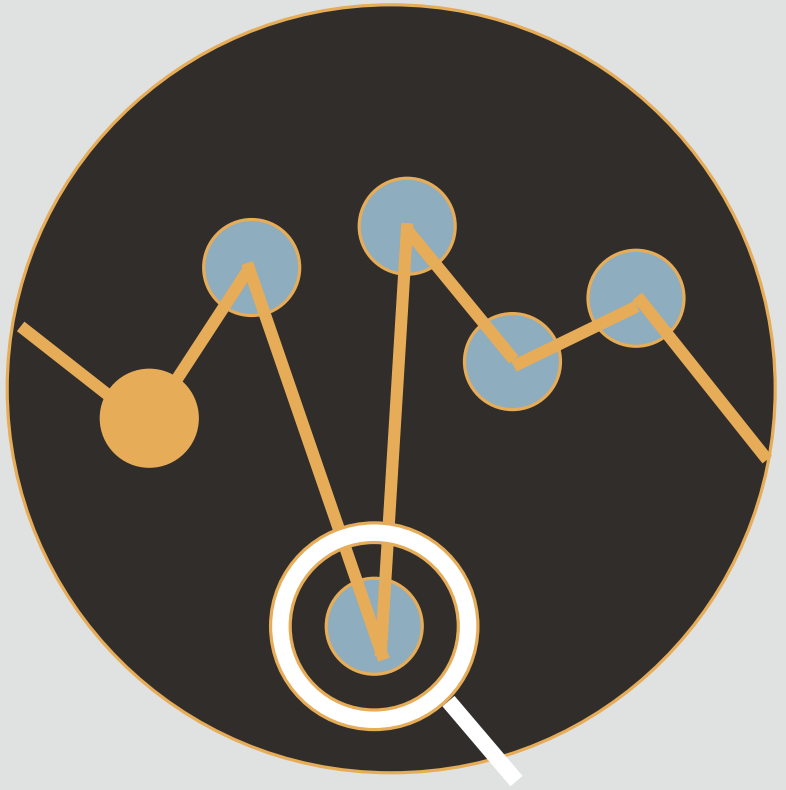
- ✓ Aggregation
- ✓ Windowing
- ✓ Context lookups
- ✓ Escalation (watchlists)
- ✓ Sequence
- ✓ Presence/Absence

…

Analysis: Machine Learning Based Anomaly Detection

Multi-dimensional Anomaly Detection

Baseline behavior for entity members AND peer groups *(network access)*
Across multiple dimensions *(time of access, login location, login host)*
Diane G. is exhibiting anomalous access behavior relative to her peers



Data Access Anomaly Detection

Baseline SQL queries executed
By a user/group, DB/DB group, or host/application
Queries being run against the finance database are anomalous

Dynamic Peer Group Identification

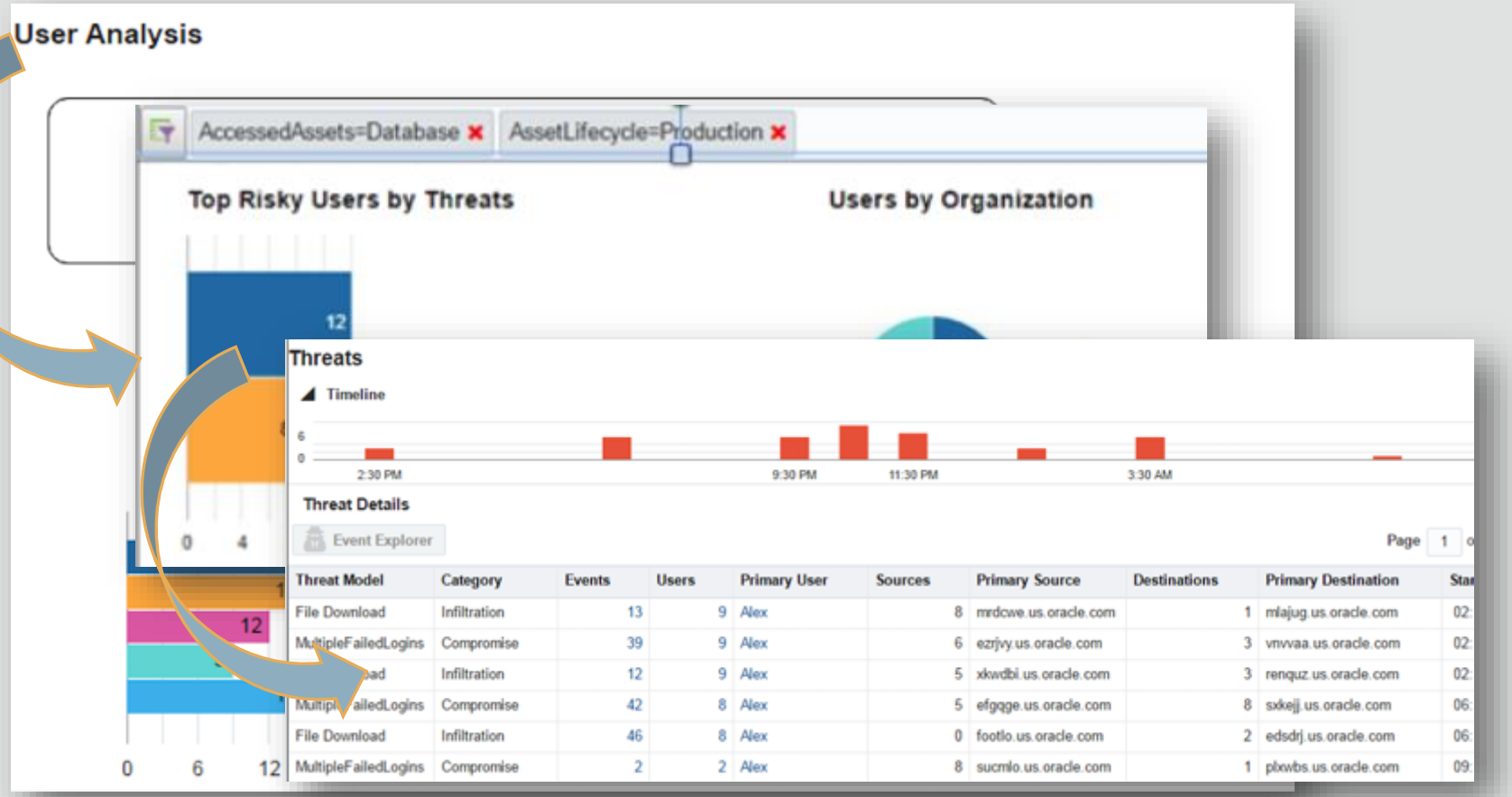
Cluster users based on common behavioral patterns
Identifies peer groups across organizational boundaries
Alice is in Finance, but her behavior matches a peer group that mostly consists of Sysadmins

Investigation: SOC Ready Content

- SOC Level 1
  - Users
  - Assets
  - Threats
- Domain specific analytics
  - Web proxy activity
  - Database activity
  - DNS activity
  - Firewall activity
  - Host activity

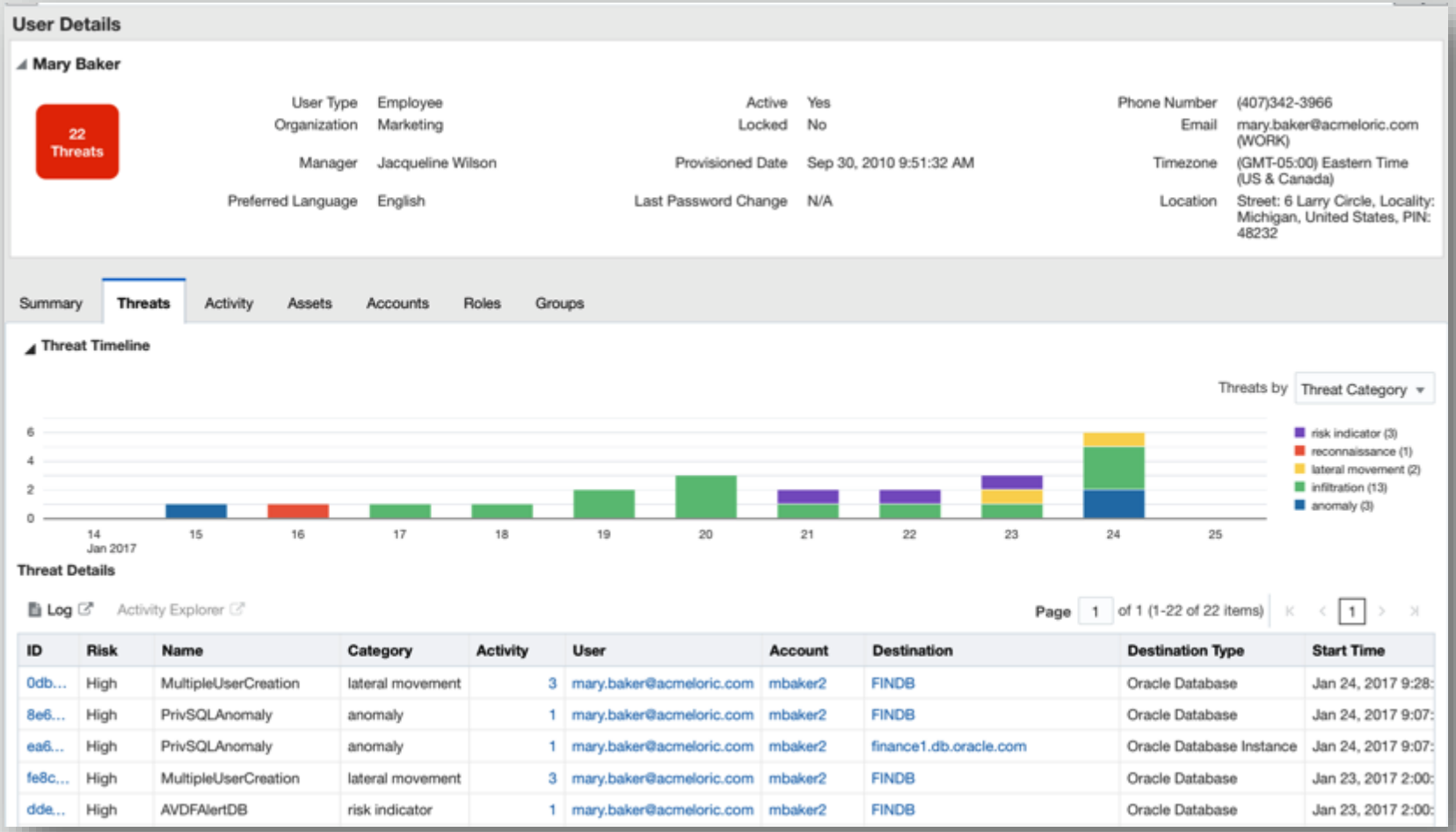
...

Investigation: Role Based Navigation Paths



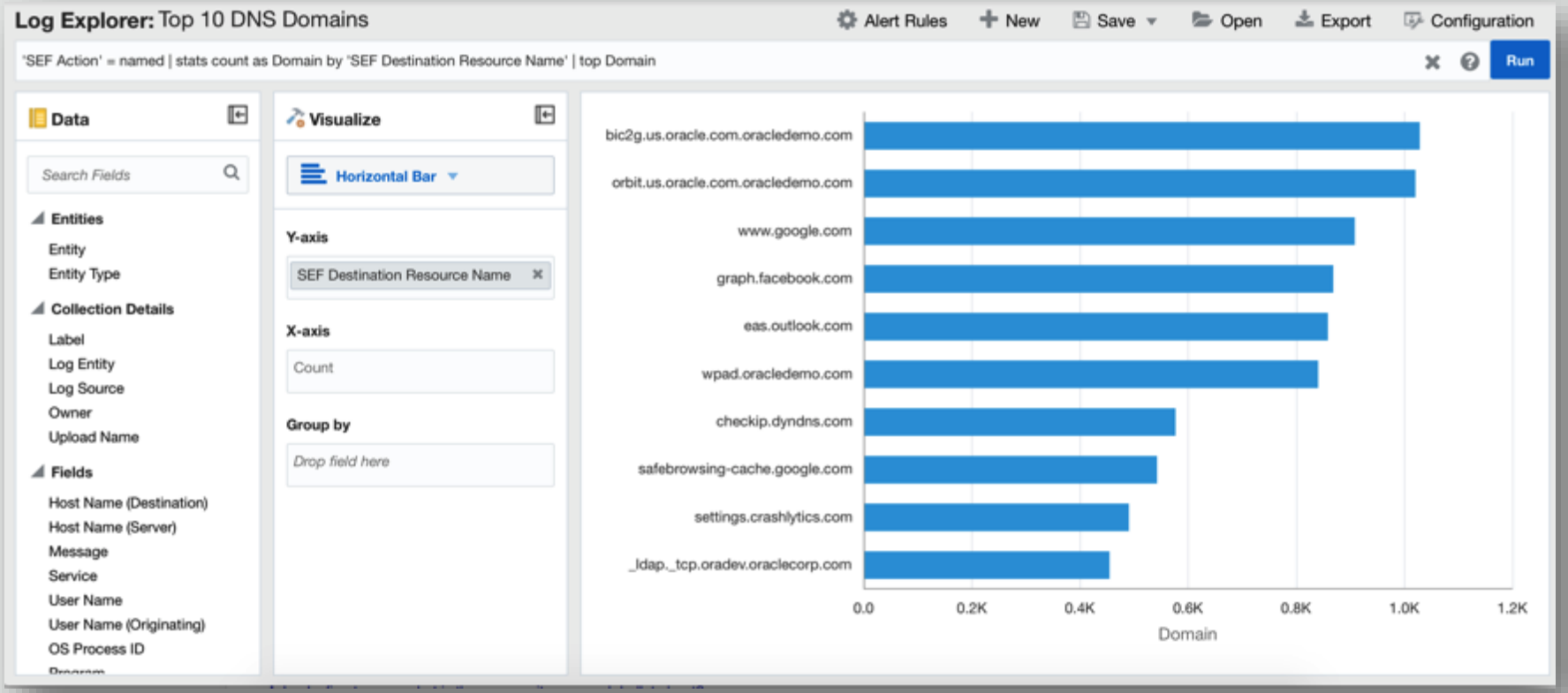
- **Drill down paths to answer next logical question**
  - Pivot to object browsers
  - Overlay “nearby” events
- **Greater SOC efficiency**
  - Faster investigation, remediation
  - Rapid root cause analysis

Investigation: Cyber Kill Chain Visualization



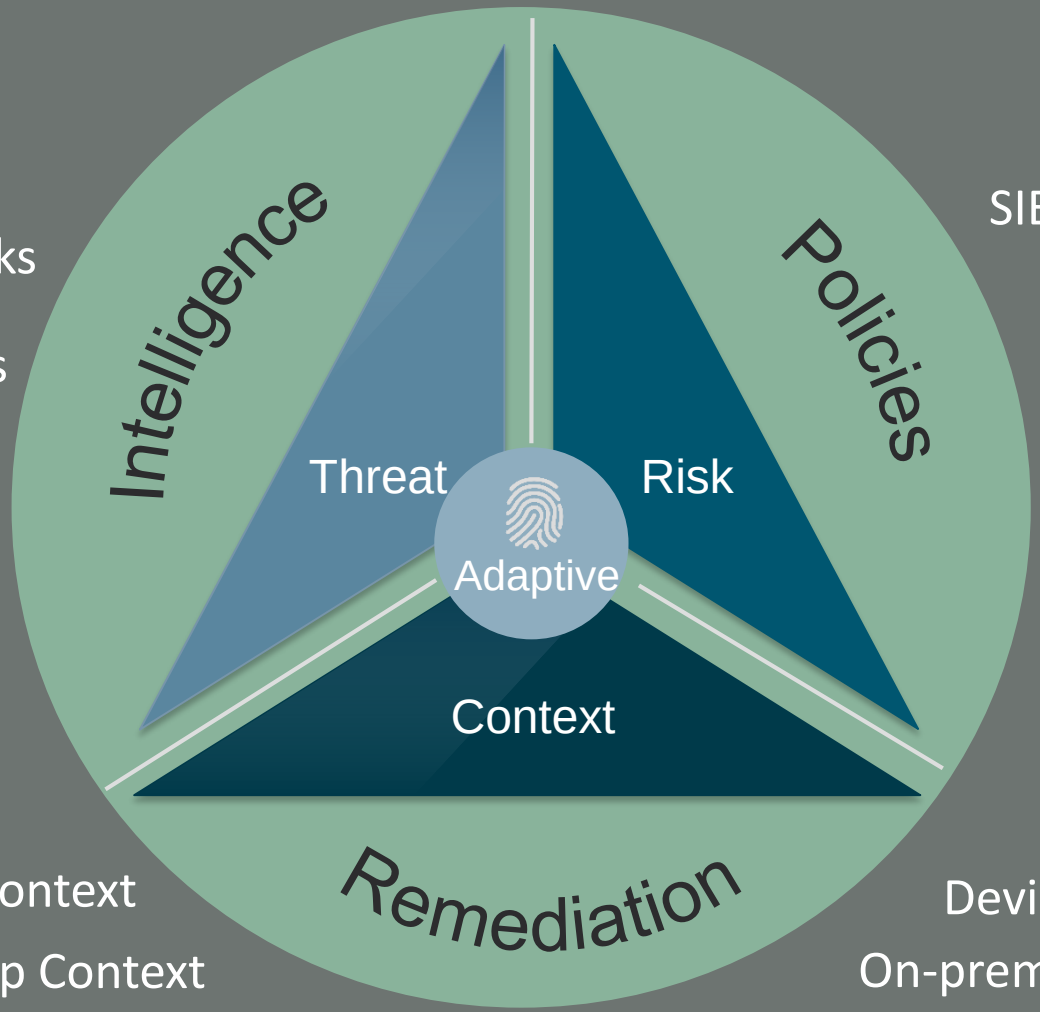
- Timeline visualization of threats and base activity
- Categorized threat events
  - Reconnaissance
  - Infiltration
  - Lateral Movement
  - Compromise
  - [Risk Indicator]

Log Analytics: Powerful Search Driven Forensics



- Filter, explore raw or enriched logs
- Data manipulation
- Statistical analysis
- Saved searches
- Alerting
- ....

Adaptive Security



Threat Networks

Reputation Services

SIEM

CASB

UEBA

User Context

App Context

Access Context

Device Context (EMM)

On-premise IAM Context

Adaptive Security

Reputation Services
(IP/Mobile/Social Identity)

Office 365 · amazon web services · salesforce · Marketo · slack · box · servicenow · GitHub · G Suite · ORACLE CLOUD · NETSUITE · CONCUR · Veeva

CASB

Adaptive Intelligence

ORACLE IDENTITY CLOUD SERVICE

Network · Location · Device · Time of access

External Risk/Threat feeds
(SIEM/UEBA/EMM)

Remediate

User and App Context · Access Context

Enterprise Resources protected by IAM/EMM

Security Ops Center (SIEM/UEBA)

"Block/Challenge access if the user is coming from risky network/geo/untrusted devices"

"Prevent users from accessing sensitive apps & data, based on policies I can define"

"Leverage external feeds and existing security tools to enforce better security"

Adaptive Security

Detect

- Risk/context/threat feeds of users/devices/apps from Oracle Cloud and external risk engines*
- Risk/context Analytics – simple & advanced
- Continuous risk re-evaluation for the user session
- Risk-based transaction controls
- Continuous authentication

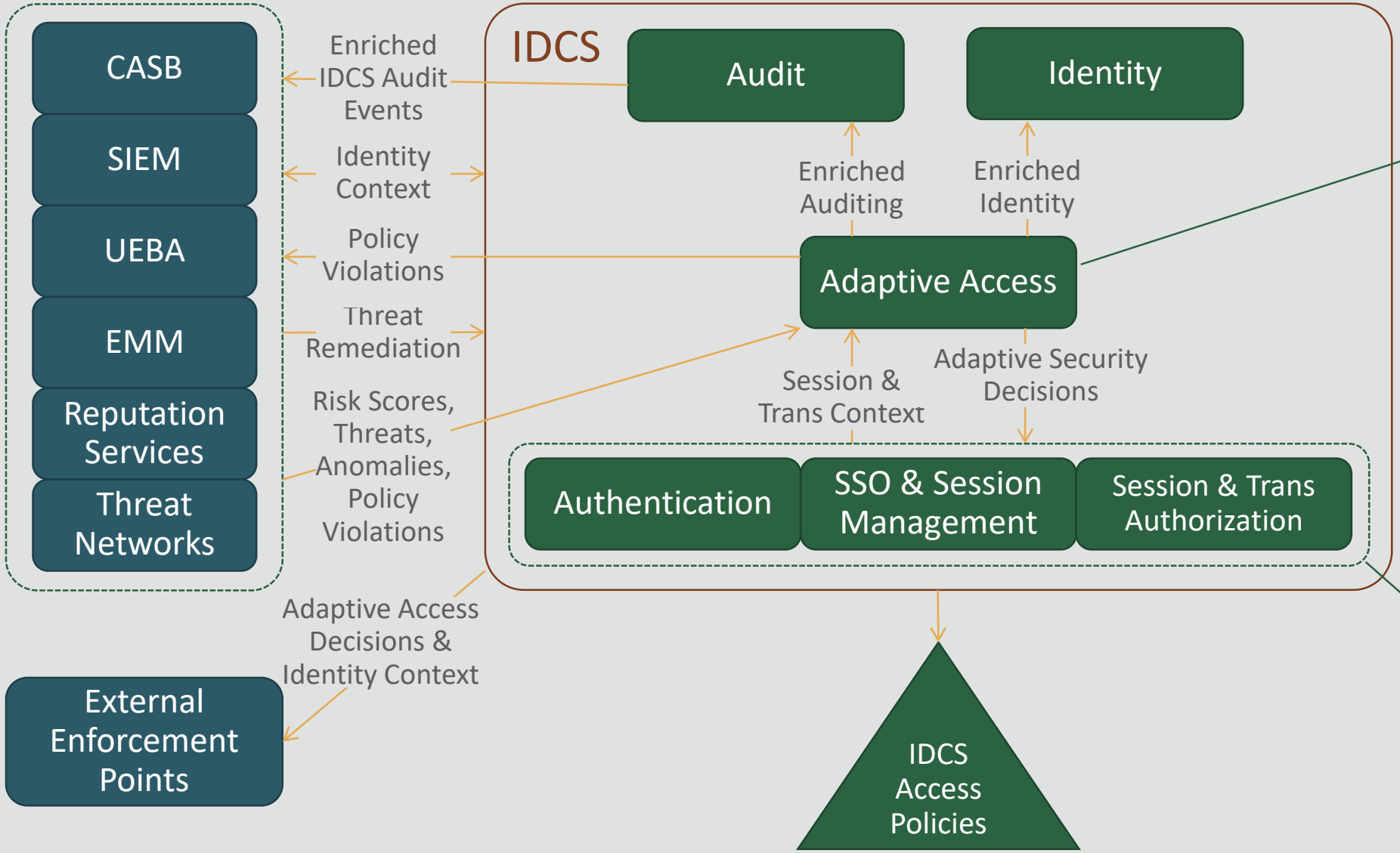
Investigate

- Risk incident notification
- Investigative dashboard with security focused drill downs
- Workflows to track investigations (assign to user, resolve, mark as false positive, ignore)
- Highlight vulnerabilities and provide recommendations

Respond

- Conditional user/app authn policies based on risk & context
- Manual remediation (force password reset, suspend user)
- Automated remediation (block sign-in, require MFA, suspend user, kill session, quarantine user, increase audit, degrade session, trigger on-demand access certification)
- APIs for risk engines to consume Oracle context, update risk score in IDCS and invoke remediation actions

Adaptive Security



Adaptive Access Responsibilities:

-Pluggable framework for integrating with external risk engines
-Normalization and consolidation of risks
-Enriching identity and auditing with risk info
-Risk & context based access/IGA policy decisions

Adaptive Access Enforcement Actions:

-Allow / Deny
-Get more info
-Sign out
-Warning / Alert
-Increase Auditing
-Continuous AuthN
-Step-Up AuthN
-Verify Transactions
-User Suspension
-Federated Sign-Out
-Cascading Sign-Out
-Session Degradation

Adaptive Security

Events Analyzed

- *Device Context*
  - User logins from unknown devices
  - User logins from compromised devices
  - Too many new device registrations
- *Network Context*
  - Logins from anonymous and blacklisted IP addresses
  - Logins outside of network perimeter
  - Windows Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, TOR Proxies, Anonymous Proxies, Spam Sources and Mobile Threats
- *Location Context*
  - Impossible travel (geo-velocity)
  - Logins from unfamiliar locations
  - Geo-fencing
- *Time Context*
  - Unfamiliar time of access
  - Surge of after hour access
- *User Context*
  - Logins by compromised users
  - Too many unsuccessful login, pwd reset attempts
  - Too many password resets
  - Simultaneous login sessions
- *Application Context*
  - Surge of application access
  - Logins to compromised/risky applications
- *And many more*

Adaptive Security

- **Adaptive Risk Score Analytics**
  - Access from unknown devices (**Device Fingerprinting**)
  - Impossible travel between 2 locations (**Geo-velocity**)
  - Logins from anonymous and blacklisted IP addresses. Includes IP address known to have Exploits, Web Attacks, Phishing, Botnets, Denial of Service, Scanners, TOR Proxies, Anonymous Proxies, Spam Sources and Mobile Threats (**IP Reputation**)
  - Logins outside of defined IP Ranges (**IP Fencing**)
  - Too many unsuccessful login attempts
  - Too many unsuccessful MFA attempts
  - Access from unknown and blacklisted locations (**Geo-Location**)
  - Logins outside of defined locations (**Geo-Fencing**)
  - Logins by compromised users
  - Access after business hours (**Time fencing**)

Adaptive Security

Use cases

- **Use case 1: Context based Authentication and SSO**
  - Detect unfamiliar logins, devices, locations, blacklisted IP, geo-velocity violations
  - Enforce corresponding remediation actions at/post authentication and at SSO
- **Use case 2: Risk based Authentication and SSO**
  - Obtain user/app risk scores from existing CASB and/or SIEM and determine risk level of user/app and combine it with context
  - Enforce corresponding remediation actions (like require MFA, deny access, lock user, expire password, trigger on-demand access certification at/post authentication and at SSO
- **Use case 3: Detect and remediate compromised account, insider threat**
  - Identity Analytics to analyze risk events and perform user/device/app risk profiling
  - Detailed dashboard to view risk/threats with drill down to related events and option to take manual remediation
  - Custom recommendations to improve overall security posture by highlighting vulnerabilities (ex. Suggest to always require MFA for an app if the app risk is elevated)
- **Use case 4 : Secure application transactions**
  - For high/medium risk users, if transaction amount > $5000, deny authn to app or require step up authn

Context-awareness

Collecting Context Data for every Access

Device Fingerprinting

Has this device been used before ? By same user ? Is it trusted ?

Geo-Location

Has user logged in from this location before?
Is it a trusted?
Device velocity ?

Network

Is user coming from within corporate network or VPN?
Wired or wireless ?

Time

Is user accessing during his normal allowed business hrs?

Integrate with external risk and threat feeds

Risk-aware, Threat-aware

On-prem Risk Analytics

OAM, SIEM, Log Analytics, UEBA, EMM

Cloud Risk Analytics

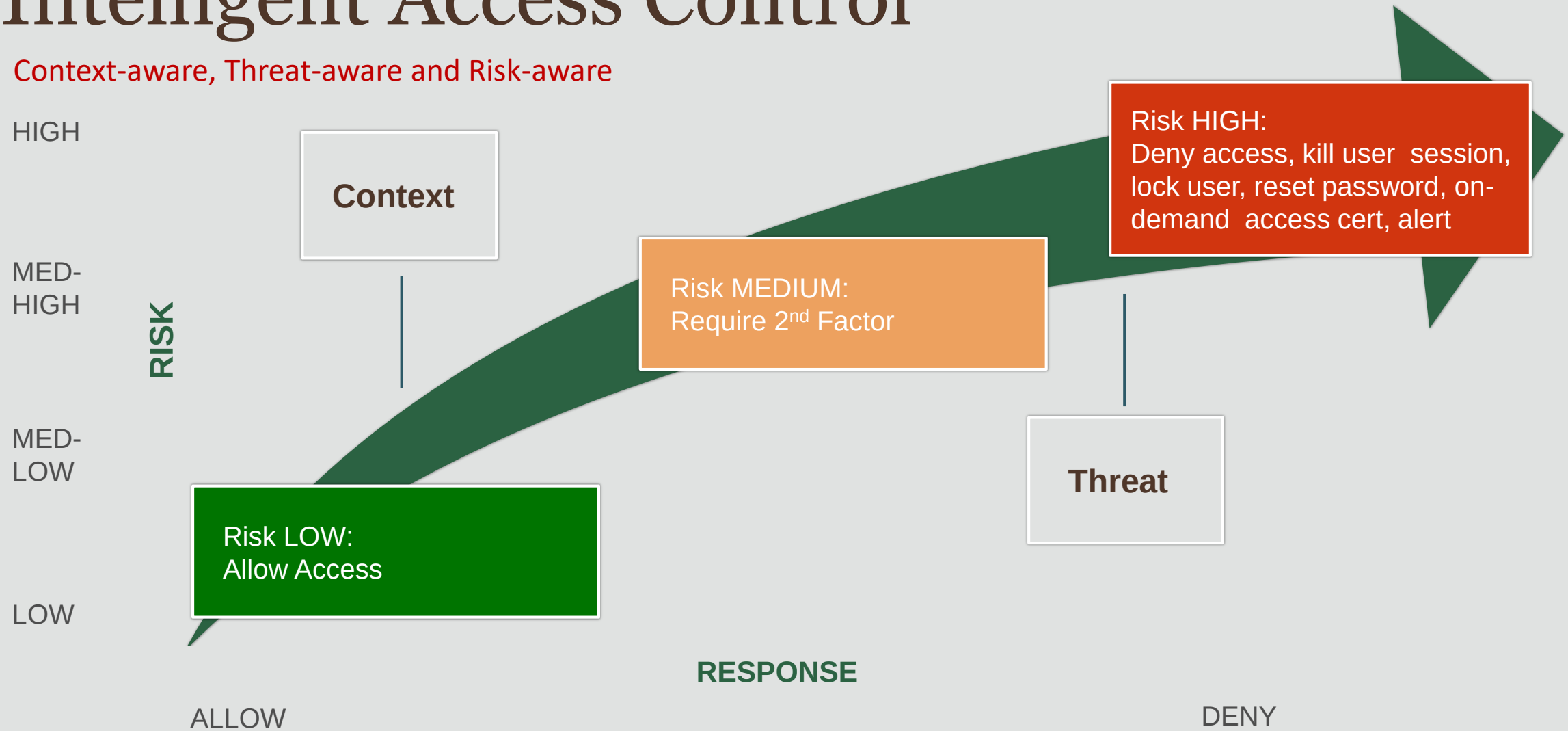
CASB, Threat Networks, Oracle Management Cloud

Reputation Services

Social Behavior, IP/App Reputation

Intelligent Access Control

Context-aware, Threat-aware and Risk-aware



Better user experience, enhanced security, improved compliance

Cloud Access Security Brokers

Cloud Access Security Broker

Securing The Digital Enterprise:
Heterogeneous Cloud Challenges and Opposing Forces

KEY CHALLENGES

- **VERY EXPENSIVE** to build expertise across 100s of cloud services (IaaS, PaaS & SaaS)
- **TIME CONSUMING** to understand each cloud service resources and corresponding actions

Shared Responsibility in Heterogeneous Cloud

Provisioning, Automation and Orchestration

Governance and Policy

Monitoring and Metering

Security and Identity

Continuous Configuration Automation

Capacity And Resource Optimization

Out of The Box (OOTB) SmartPolicies

Cloud Access Security Broker

Machine Learning + Threat Intel + Threat Feeds

KEY BENEFITS

- 100s of hours of effort saved
- Consistent Security Posture
- Heterogeneous Cloud Services

Sales & Marketing

G Suite

box

AWS

salesforce

Global IT

Microsoft Azure

AWS

servicenow

Office 365

Human Resources

ORACLE Oracle ERP Cloud

ORACLE HUMAN CAPITAL MANAGEMENT

ORACLE Cloud Infrastructure

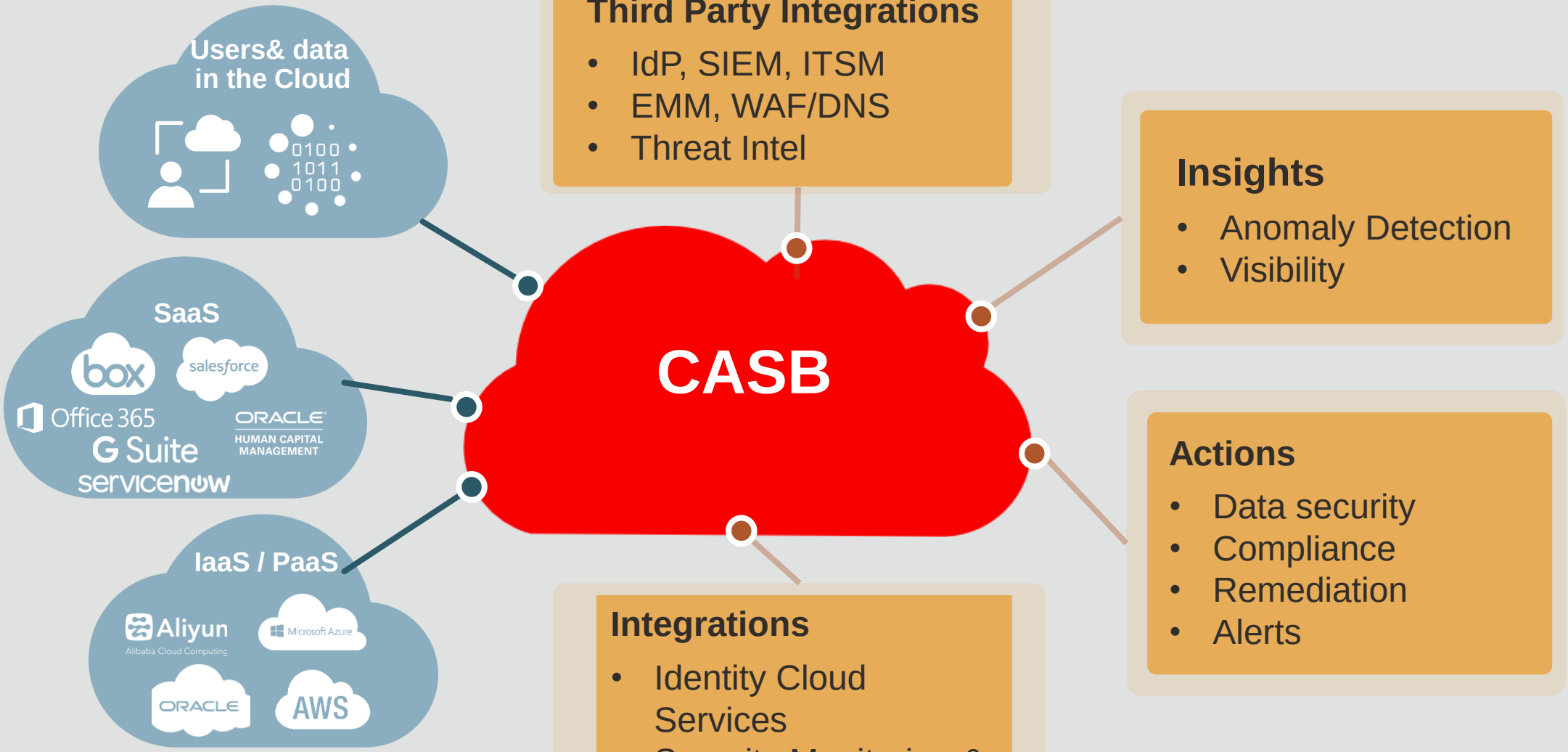
Research & Development

Microsoft Azure

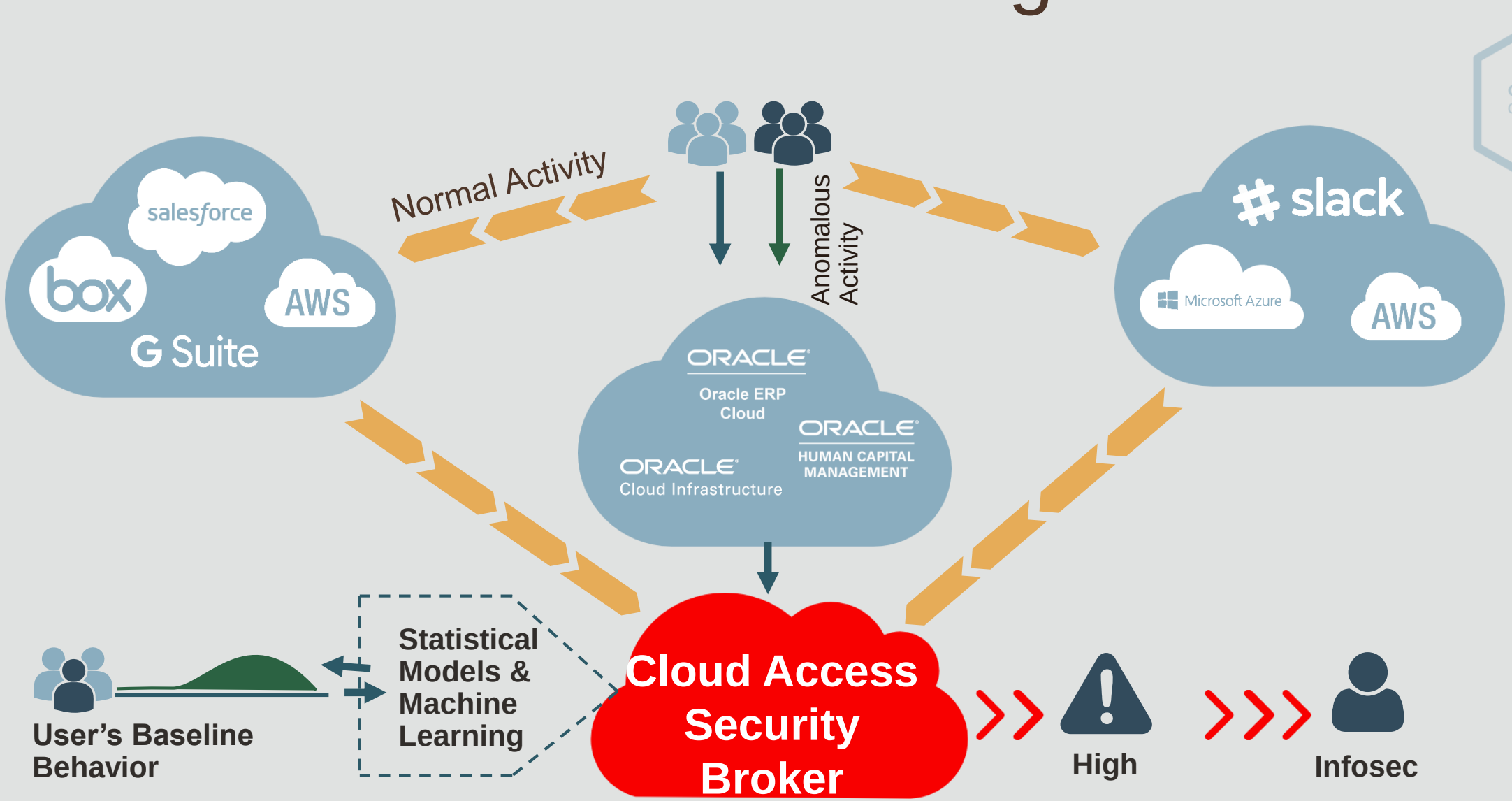
slack

AWS

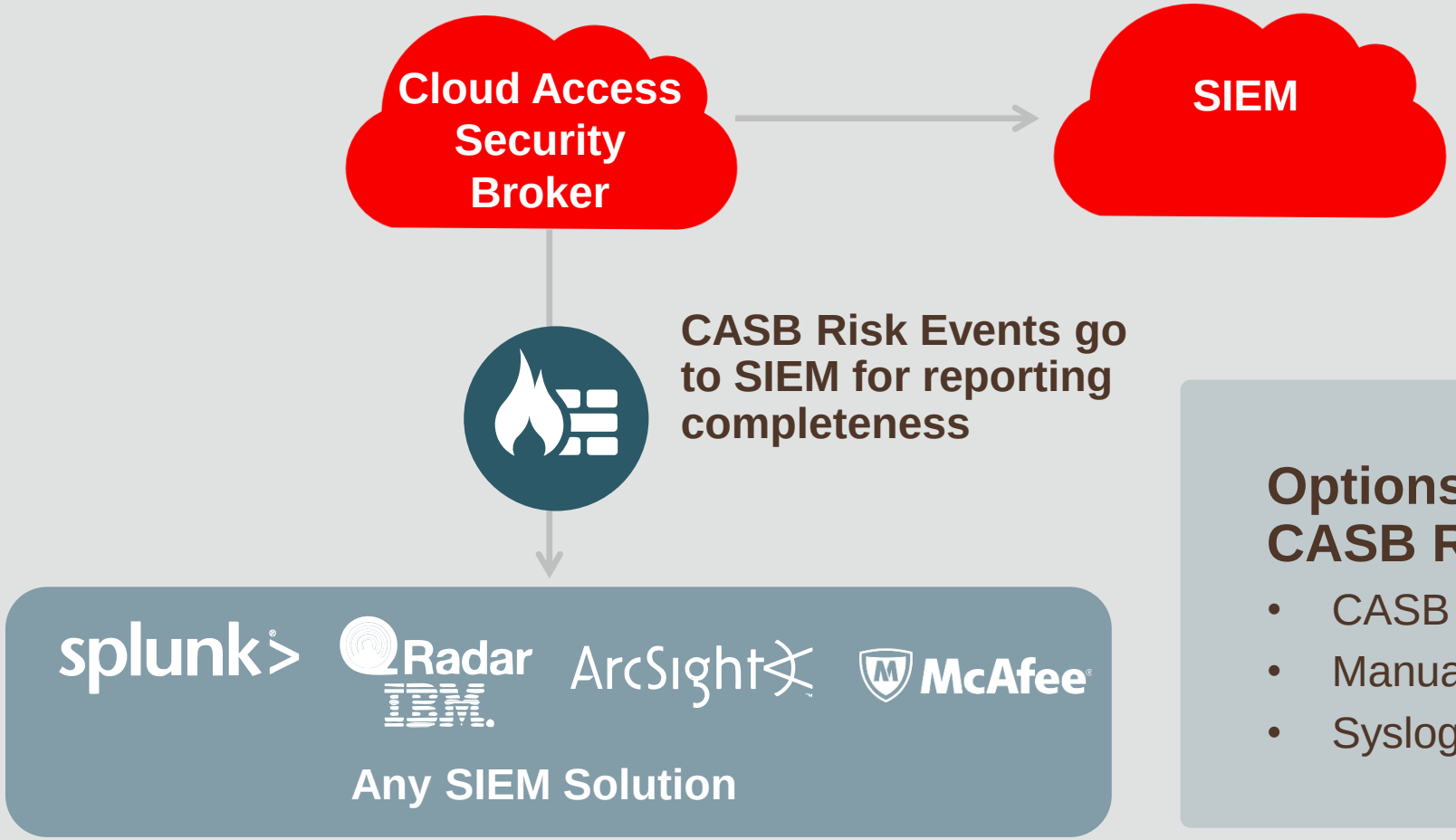
Typical CASB Integrations



Detect Misuse of Admin Privileges with UEBA



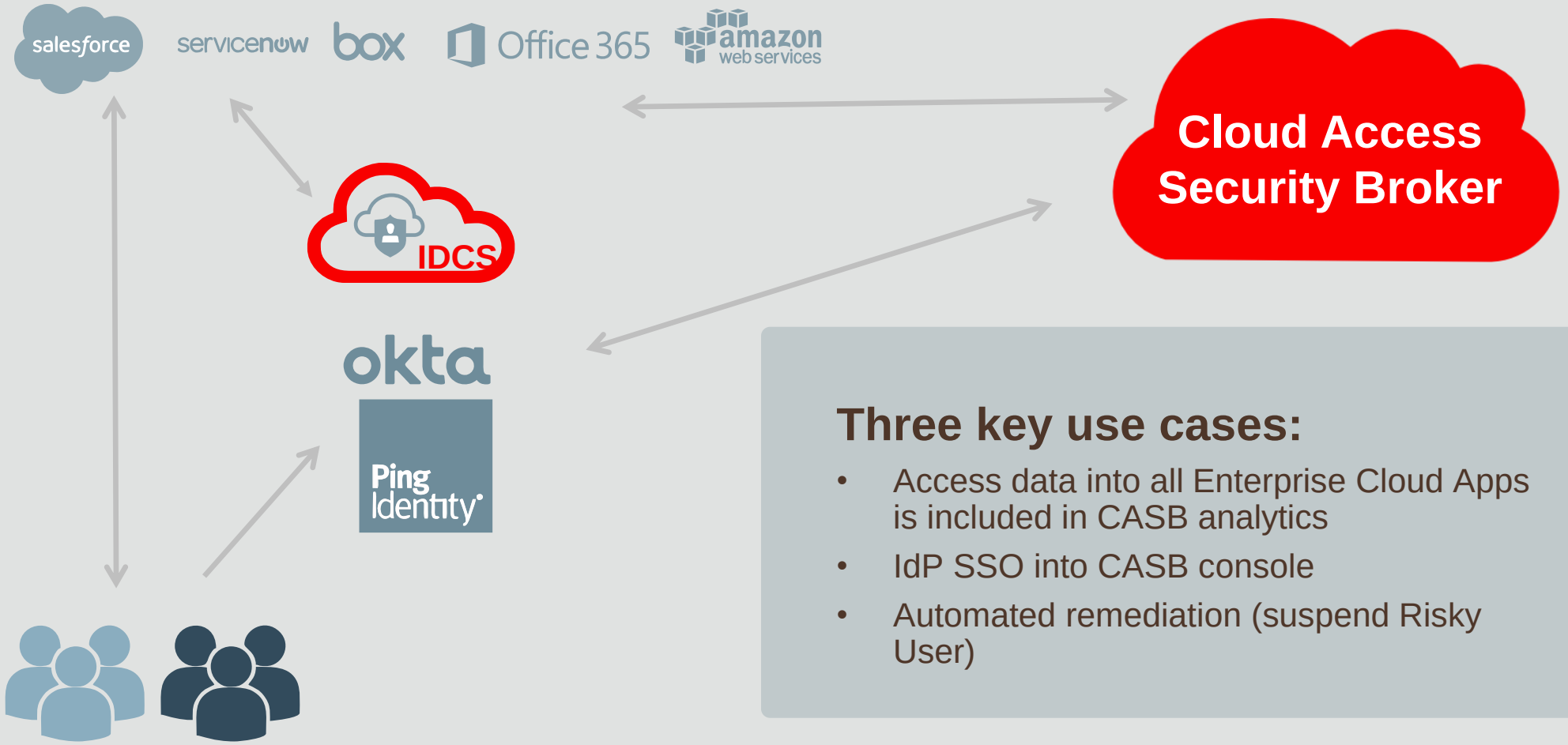
CASB - SIEM Integrations



Options for exposing CASB Risk Events:

- CASB API
- Manual export of Risk Events
- Syslog stream out of CASB

CASB – Identity Provider Integrations



Three key use cases:

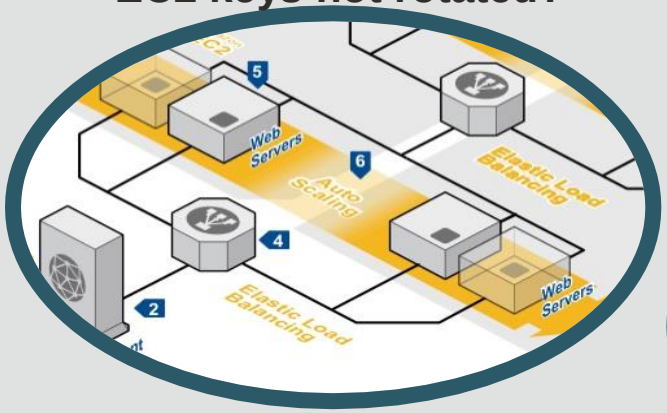
- Access data into all Enterprise Cloud Apps is included in CASB analytics
- IdP SSO into CASB console
- Automated remediation (suspend Risky User)

Challenges in Securing IaaS

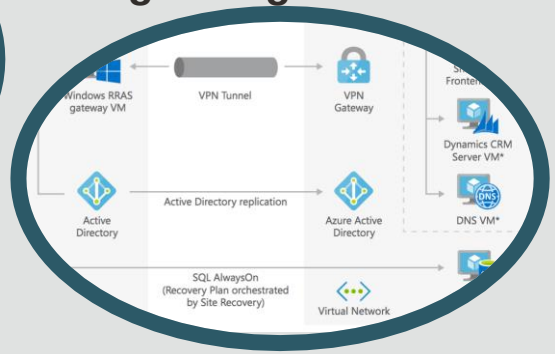
1. Shared responsibility challenges
2. Compliance requirements
3. Data leakage
4. Misuse of admin privileges
5. Control the risk introduced by Shadow IT

1. Shared Responsibility in Heterogenous IaaS

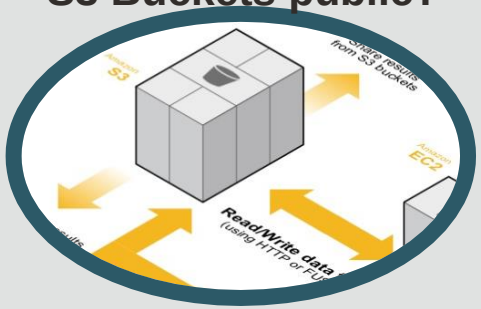
EC2 keys not rotated?



Azure Virtual Network config change?



S3 Buckets public?

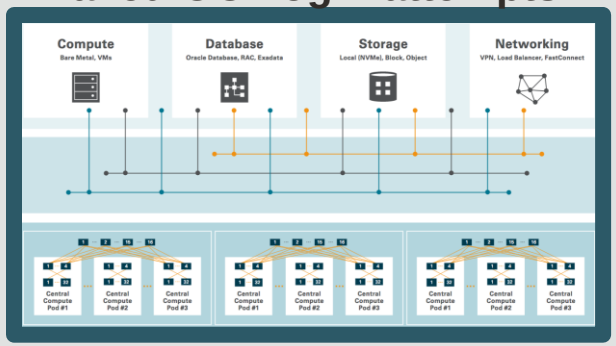


Cloud Access Security Broker

High

Infosec

Failed OCI login attempts?



ACME CORP

Sales & Marketing

G Suite

box

salesforce

AWS

Global IT

servicenow

AWS

Office 365

GitHub

Microsoft Azure

Research & Development

slack

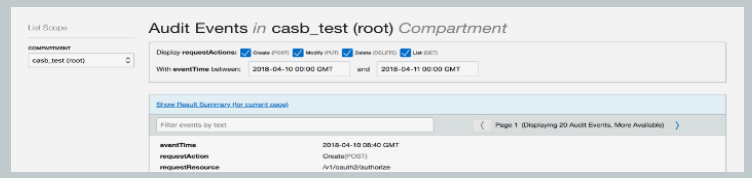
Microsoft Azure

AWS

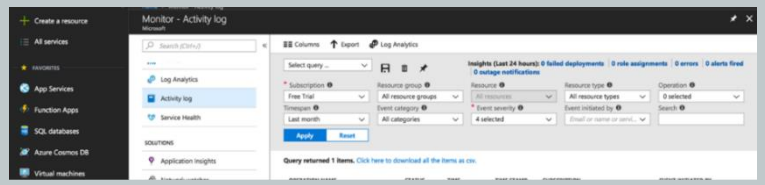
2. Consistent Governance to Meet Compliance

AWS CloudTrail Logs
AWS VPC Flow Logs
AWS CloudWatch Logs

Oracle Cloud Infrastructure Audit



Azure Logging & Auditing



Cloud Access Security Broker

Check policies for:

- Log retention
- MFA
- CIS Framework deviations

Policy Enforcement

InfoSec & IT Department

High

3. Detect Leaky Storage with CASB

Department 1 — Faulty Configurations

Department 2 — Faulty Configurations

Department 3 — Faulty Configurations

Cloud Access Security Broker

No visibility

InfoSec & IT Department

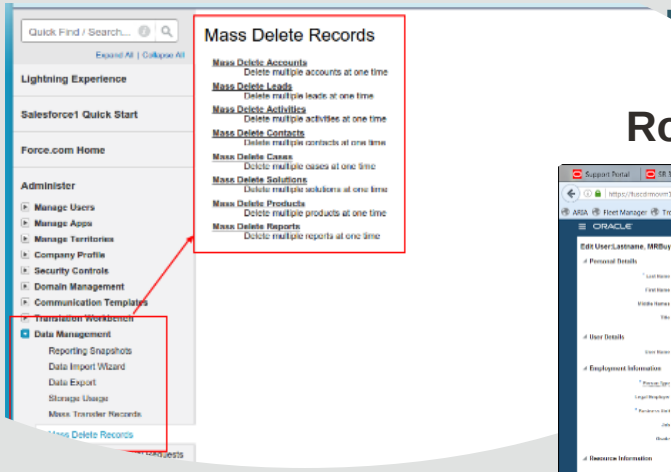
High

Challenges in Securing SaaS

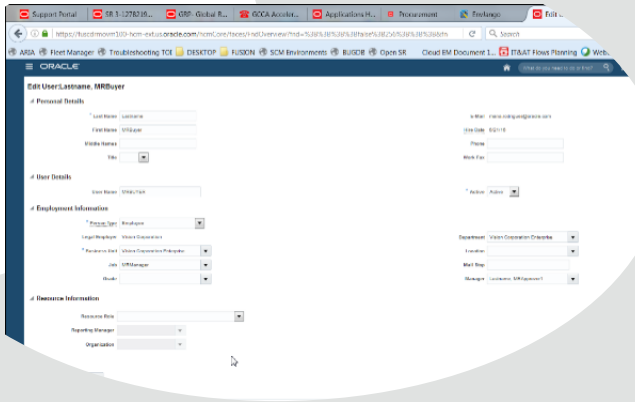
1. Shared responsibility challenges
2. Compliance requirements
3. Data leakage
4. Misuse of admin privileges
5. Control the risk introduced by Shadow IT

1. Shared Responsibility in Heterogenous SaaS

Mass data delete request?



Role change in HCM Cloud?

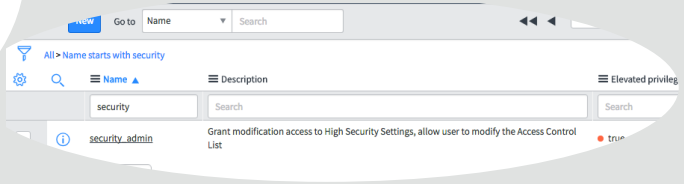


Cloud Access Security Broker

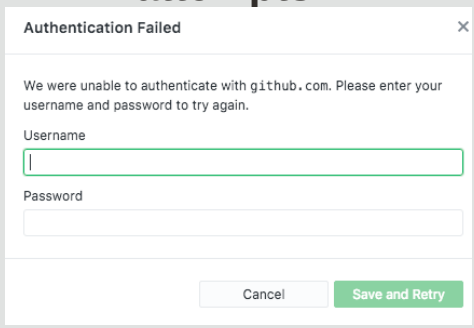
High

Infosec

Privilege escalation in ServiceNow?



Failed GitHub login attempts?



ACME CORP

Sales & Marketing

G Suite

box

ORACLE

salesforce

Global IT

servicenow

Office 365

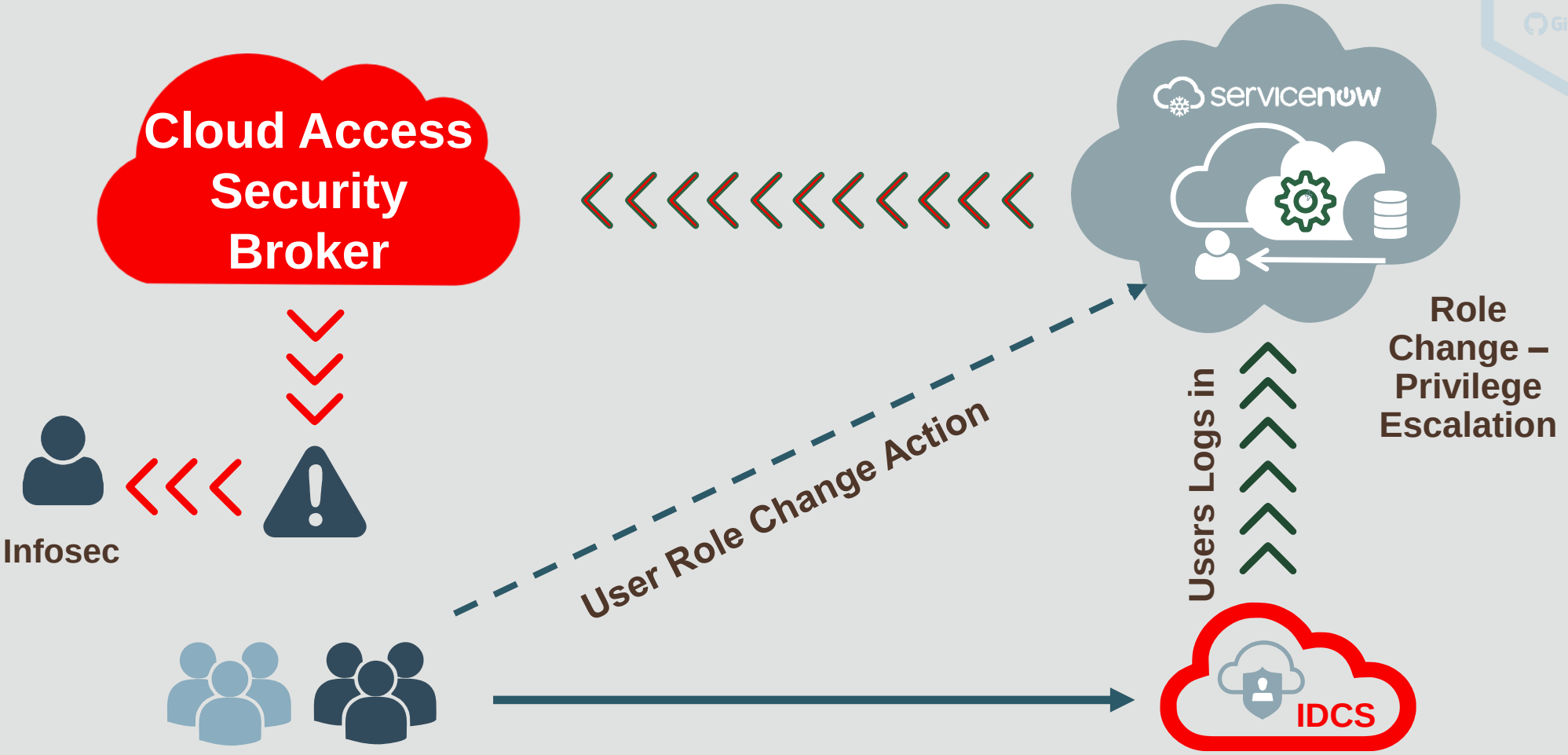
ORACLE HUMAN CAPITAL MANAGEMENT

Research & Development

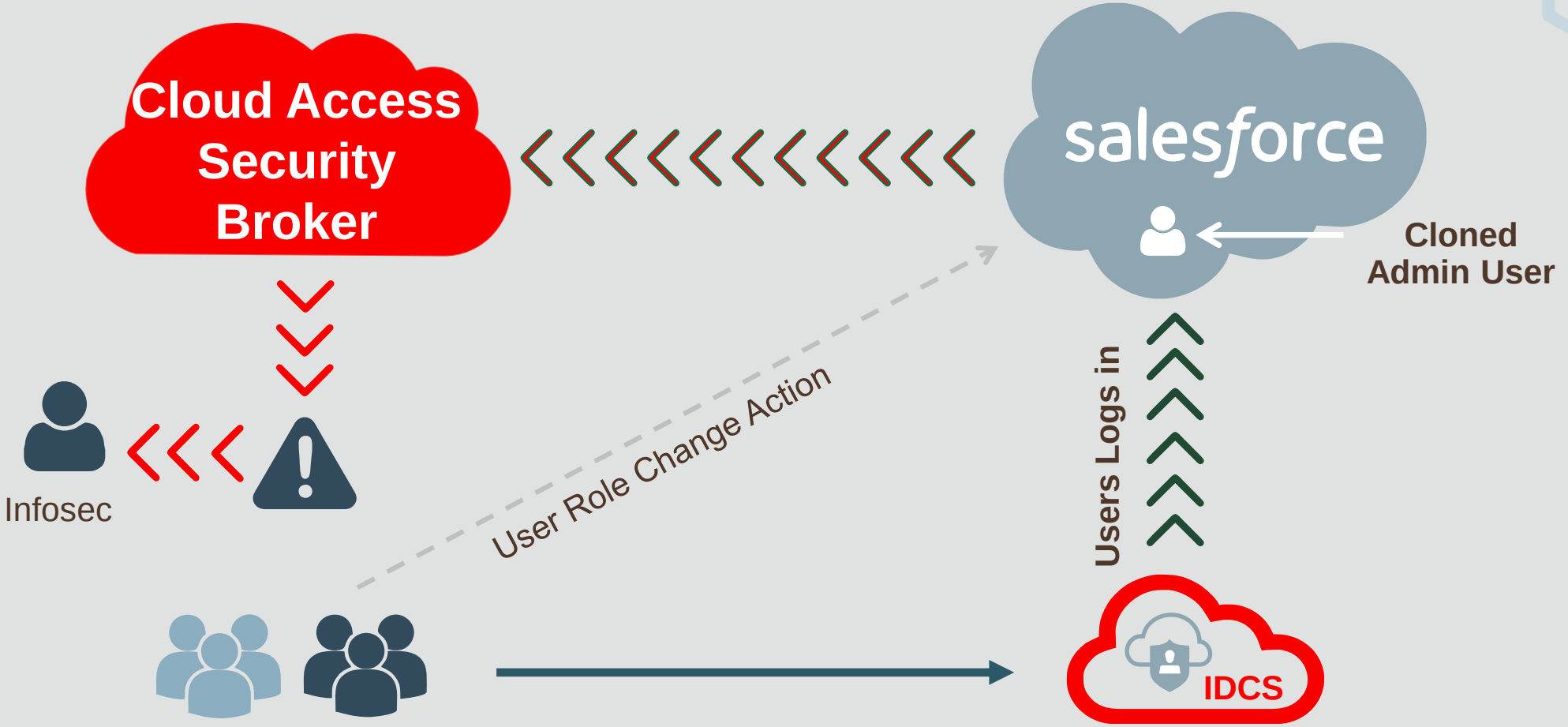
GitHub

slack

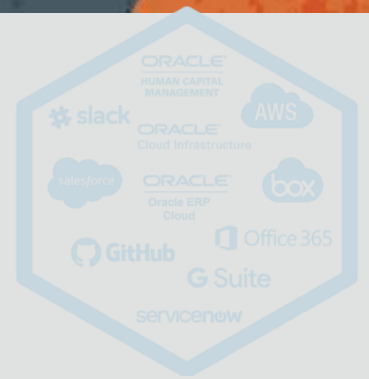
2. Consistent Governance to Meet Compliance

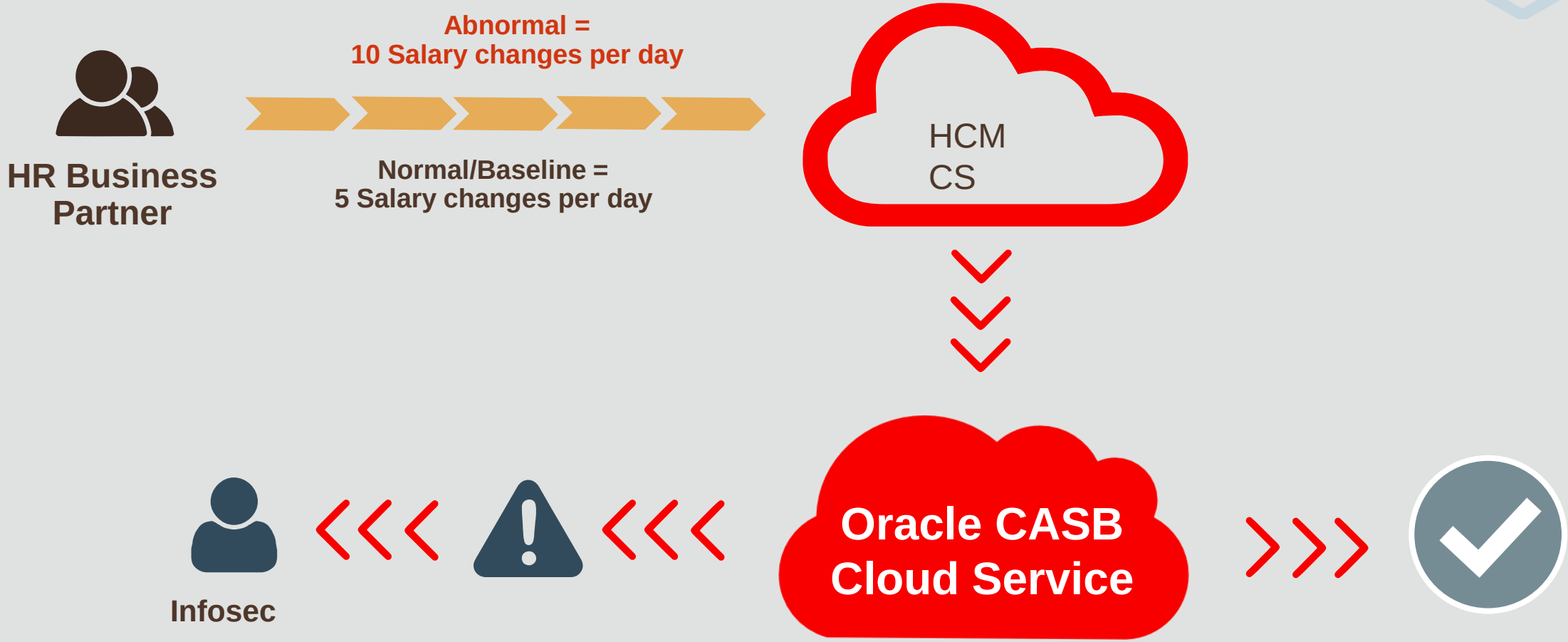


3. Detect Sensitive Data Leakage

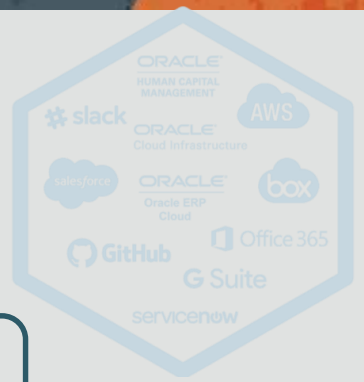


4. Detect Misuse of Admin Privileges with UEBA



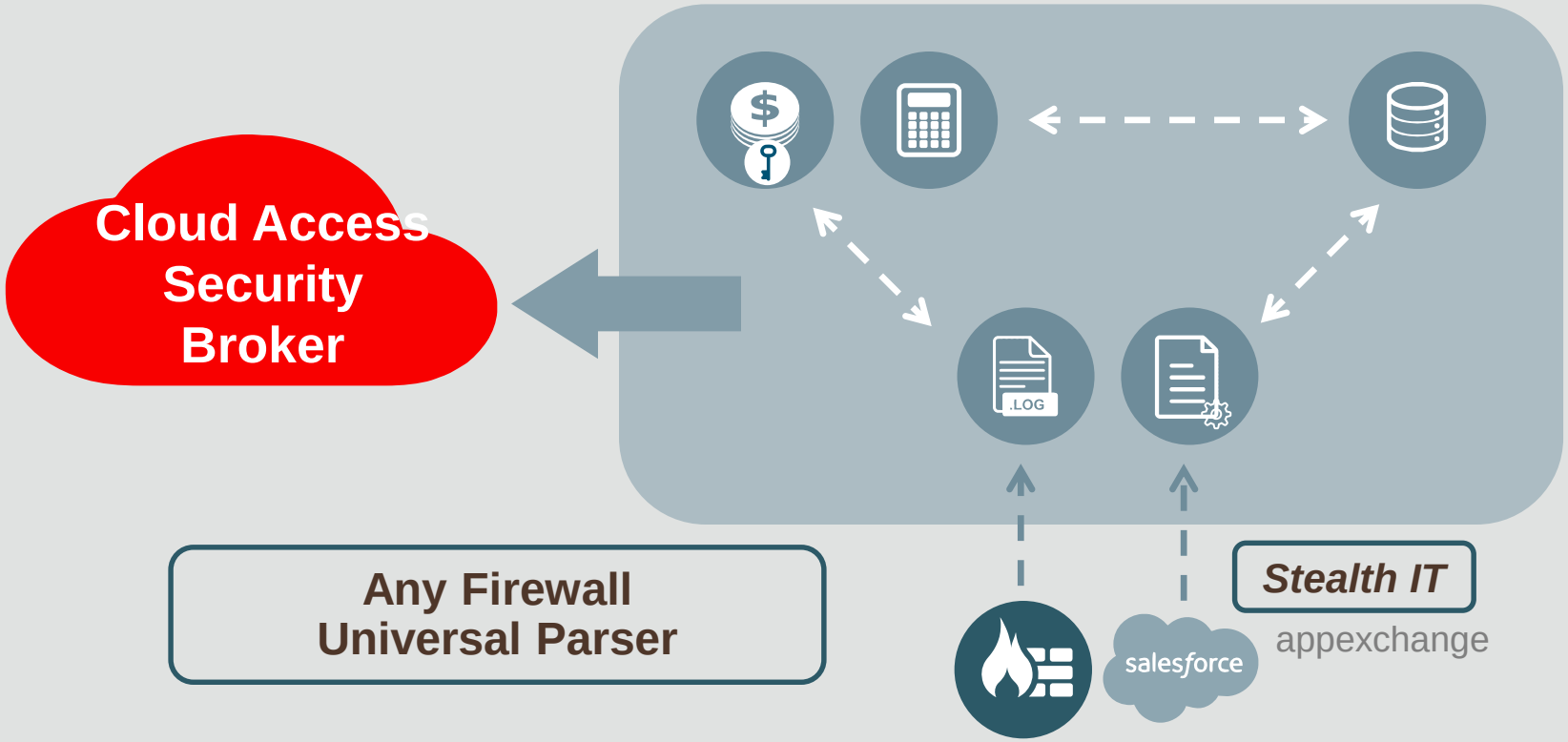


5. Control Shadow and Stealth IT



Machine Learning & App Risk Computation

App Risk Registry

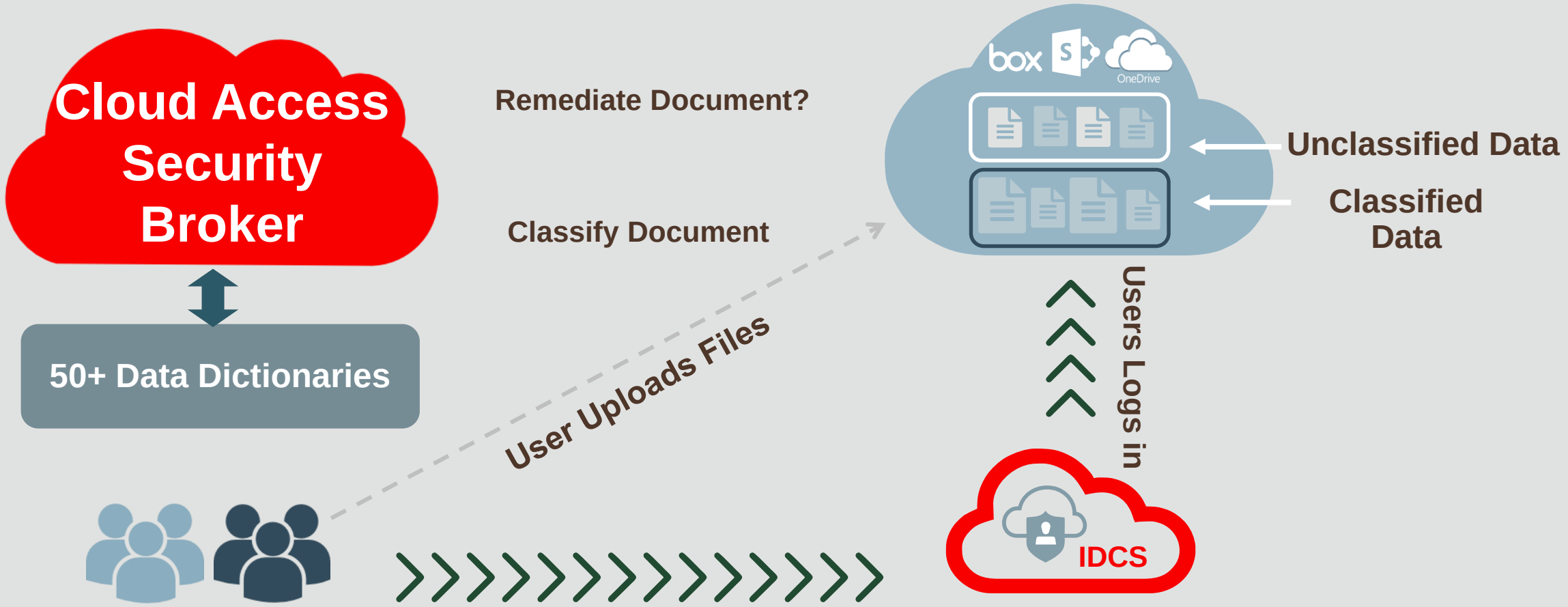


Challenges in Protecting Data

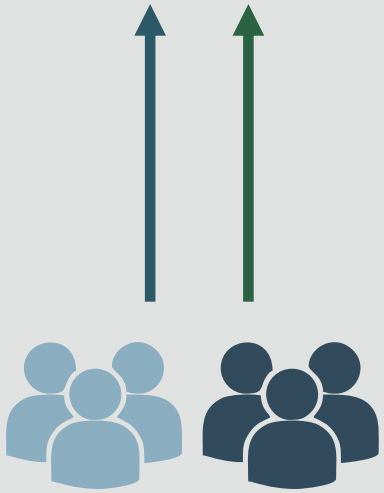
1. Lack of visibility into sensitive data in the Cloud
2. Stopping sensitive content going to unauthorized users
3. Compliance requirements around reporting on Data

1. Visibility Into Cloud Data – Data Classification

Retroactive or On-demand Scan of Documents



2. Stop Sensitive Content Going to Unauthorized Users/Places



Prerequisite: App must be SAML Compliant & Configured for SSO

Prevent otherwise valid actions like:

- Download/Preview/Edit sensitive documents in hostile locations
- Over sharing of sensitive documents