CASE STUDY

Ping Access Management, Federation, MFA Powered By Simeio

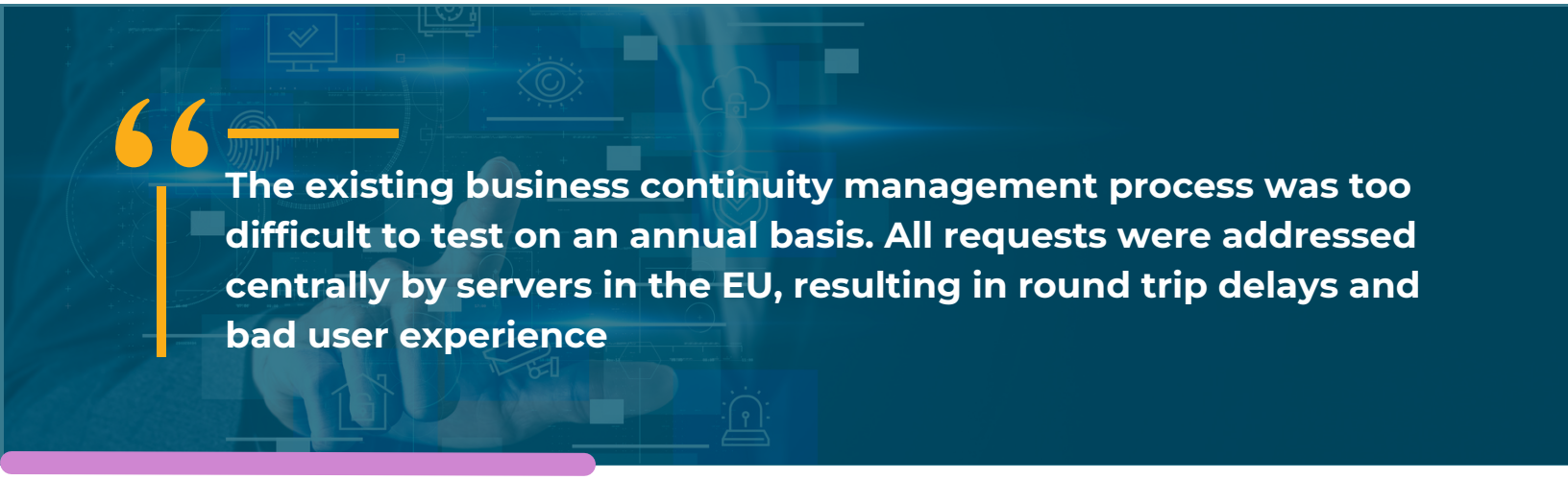
Background

The customer is the United States-based subsidiary of a multinational oil company ("supermajor") of Anglo Dutch origins. The multinational figures amongst the six largest oil companies in the world and ranked as one of the largest companies in the world by revenue. Although approximately 22,000 employees are based in the U.S, the solution described below addresses use cases that support 150,000 employees worldwide, including 15000 external users. The U.S. head office is located in Texas. The client is vertically integrated, with many joint ventures and a high rate of acquisition. Including its consolidated companies and its share in equity companies, the client operates across exploration and production, refining, transport, distribution and marketing, petrochemicals, power generation and trading.

The upstream and downstream businesses that comprise the client's value chain require access from and provide access to data and information according to policy and processes defined by the client. This complex set of interactions up and down the chain is governed according to various levels of confidentiality, and degrees of business impact. Availability, performance, reliability and integrity of accesses and data are critical as associated issues impact employee productivity, operational risks, and regulatory compliance.

The Challenge

Employees, contractors and vendors were unable to access corporate applications – in particular, Office 365, where most of the tickets had been created. Missing attributes, and duplicate users created during synchronization caused user downtime; and word of such problems spread among application owners.



> **The existing business continuity management process was too difficult to test on an annual basis. All requests were addressed centrally by servers in the EU, resulting in round trip delays and bad user experience**

This resulted in:

- Significant employee and contractor productivity issues
- Vendor access problems, impacting revenue and productivity
- Application owners rejecting onboarding of their applications into the enterprise Access Management system - preferring instead to take on operational risk
- High risk exposure
- Audit findings associated with non-compliant SOX-scoped systems

The client had been using a dated and poorly architected implementation of CA SiteMinder, “FAAS”, hosted internally within two datacenters in Europe. The deployment was performing so inadequately that application owners preferred to manage access directly rather than subject users to the flawed corporate access management system.
This was reflected in a low and slow backlog of applications to be onboarded. Issues associated with the 7-year old design including:

- Service outages which impacted business critical applications
- Bad user experience
- Not scalable
- Low application adoption rate
- On-premise solution

Simeio found the following main causes of the outages:

Identity Synchronization Issues	Data Integrity Issues
Excessive Attribution / Wrong Attribution for Federation	No Disaster Recovery In Place
All requests were addressed centrally by servers in the EU, resulting in round trip delays and bad user experience	The existing business continuity management process was too difficult to test on an annual basis

The Solution

The client partnered with Simeio to build and deploy a pure IDaaS solution exclusively for the client (single rather than multi-tenant), powered by PING. This Access Management (AM), Federation and Multi-Factor Authentication (MFA) project involved setting up IAM service to support 150,000 B2E users, 50,000 B2B users, and over 90 applications, worldwide.

Simeio manages the client's **PING Identity Suite environment**, including *PingFederate – High Availability Cluster, PingAccess – High Availability Cluster, and PingOne/PingID MFA Tenant.*

- **Simeio cloud with two regions: US and Europe**
- **70+ Servers, 3 Environments**
- Supports **116 federations**
- **150,000 users** across multiple domains
- **Simeio Expert Managed Services**

1. Access Management
2. Federation
3. Multi-Factor Authentication

- **24/7/365 Support -** Hybrid on/off shore model
- **Outage Support and Ticket Management**
- **Deployment, rollout and on-going** app/privileged account on-boarding services
- **Environment upgrades and stabilization,** including infrastructure support such as patching, and server and OS upgrades
- **Trusted IAM advisor**
- **Vendor evaluations and technology and industry best practice recommendations.**

The client selected Simeio to be the IAM service provider and PING IAM Suite to address the challenges and other needs and requirements. Simeio Managed Services proved to be a true solution, beating competitive demonstrations from other vendors and service providers.

150,000 B2E Users

50,000 B2B Users

90+ Applications

simeio
Identity, intelligently managed.

PingIdentity

The Impact

Simeio addressed end user experience issues that were inhibiting adoption by application owners.

Simeio implemented geo-based clustering, auto-scaling, and addressed multiple levels of redundancy with automatic failover.

- To handle peak and increasing load (traffic or number of requests) globally, without placing excess load on any one region
- To ensure business critical applications can be serviced, addressing adoption challenges from application teams.
- To reduce Recovery Time Objective (RTO) timelines

Ensured access from a given regional domain was authenticated from AWs servers within the same region.

Aligned with the client's strategic goal to transition to SaaS platforms. They required a true SaaS IAM platform that could provide SSO to SaaS applications.

Provided a robust monitoring and alerting system to notify teams if there is an issue with a server on an application authentication.

***PING MFA* worked seamlessly across all mobile platforms and improved user experience. The offline *PING ID MFA* capability was a significant advantage.**

Within 8 Months, Simeio was able to significantly improve productivity and vastly reduced help desk tickets. The environment was run as a security program, with security and compliance reporting supplied by Simeio and the access management environment was vertically and horizontally scalable.

Applications Migrated in 40 Days

Uptime for the AM* environment governed by SLA

Increase in Adoption by Application Owners

*Access Management