5 Steps to Achieving Identity Security in the Cloud

September 2025 – Daniel Comarmond, Pre-Sales Australia + New Zealand

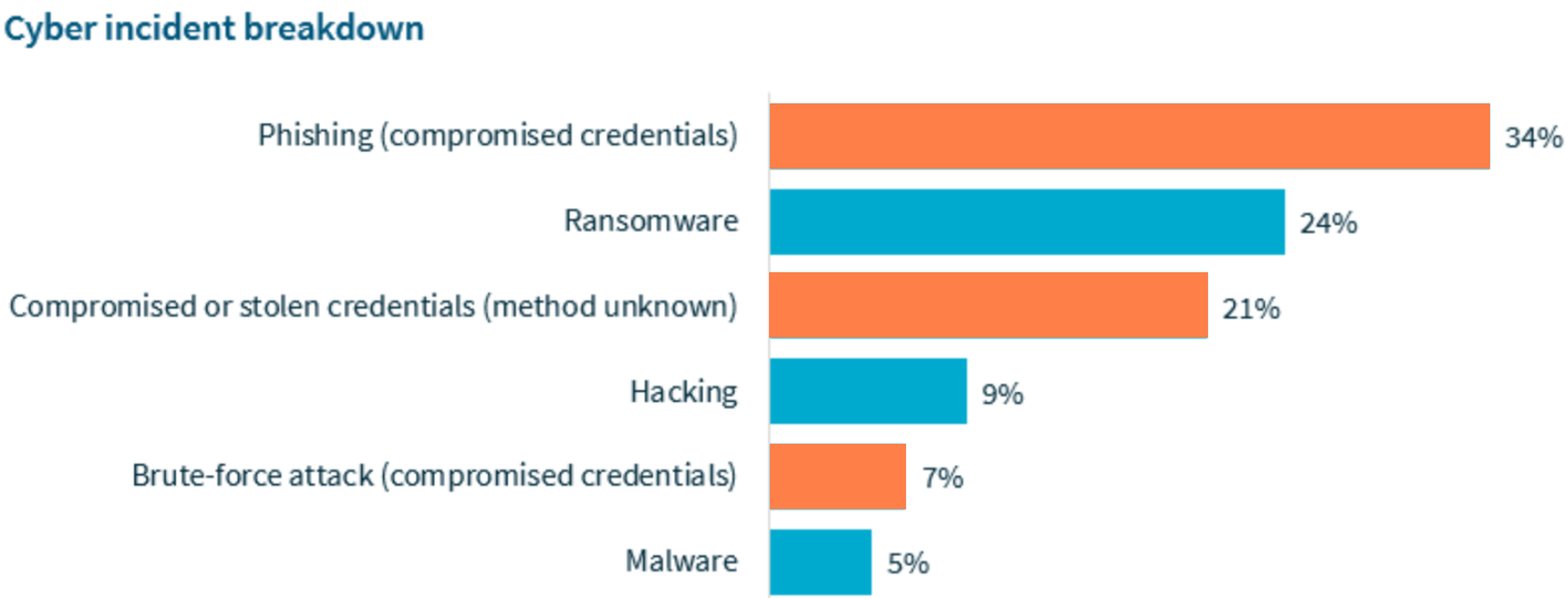
What causes data breaches?

… according to the Office of the Australian Information Commissioner

Compromised credentials – through phishing, a brute-force attack or an unknown method – **comprised 62% of all cyber incidents**.

This reporting period saw a significant increase in data breaches caused by social engineering and **impersonation**, the manipulation of people into carrying out specific actions or divulging information.

- Notifiable Data Breaches Report: July-December 2024
Office of the Australian Information Commissioner
13 May 2025



The Challenge: Identity is the Leading Attack Vector

"Threat actors continue to take advantage of assets with default, simplistic and easily guessable credentials via brute forcing them, buying them or reusing them from previous breaches." – 2024 DBIR page 42

What are we doing about it?

What do we mean by Identity Security?

What have the recent breaches at MGM, Uber, Okta had in common?

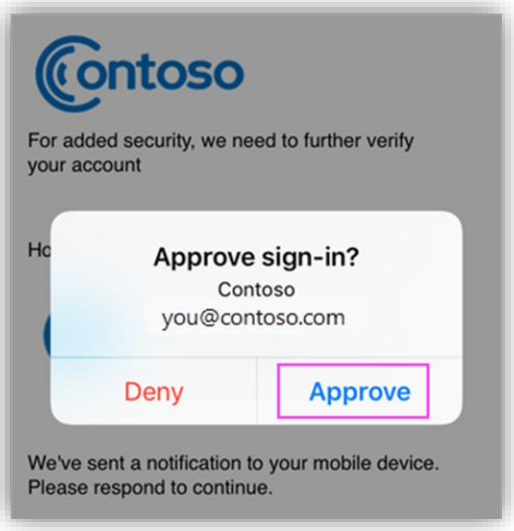
If your employee's credentials were discovered on the dark web right now, how protected are you?

Is your Active Directory / IdP configured properly? How do you know? When did you last check?

Who has administrative rights in your Azure / AWS / GCP production environment?

If an attacker landed in your network today, and stole an admin credentials, how far would they get?

An employee is getting MFA bombed right now. How can you tell? Can you stop it?



Identity and Access Data is Complex and Siloed

80% of modern attacks are identity-driven

CROWDSTRIKE

99% of cloud identities are too permissive

UNIT 42 BY PALO ALTO NETWORKS

75% of security failure will come down to the inadequate management of identity and privileges

Gartner

More than **5 machine identities** for every user identity

paloalto NETWORKS

The Chaos of Complex & Siloed Identity and Privileges Data

- **Lack of visibility**

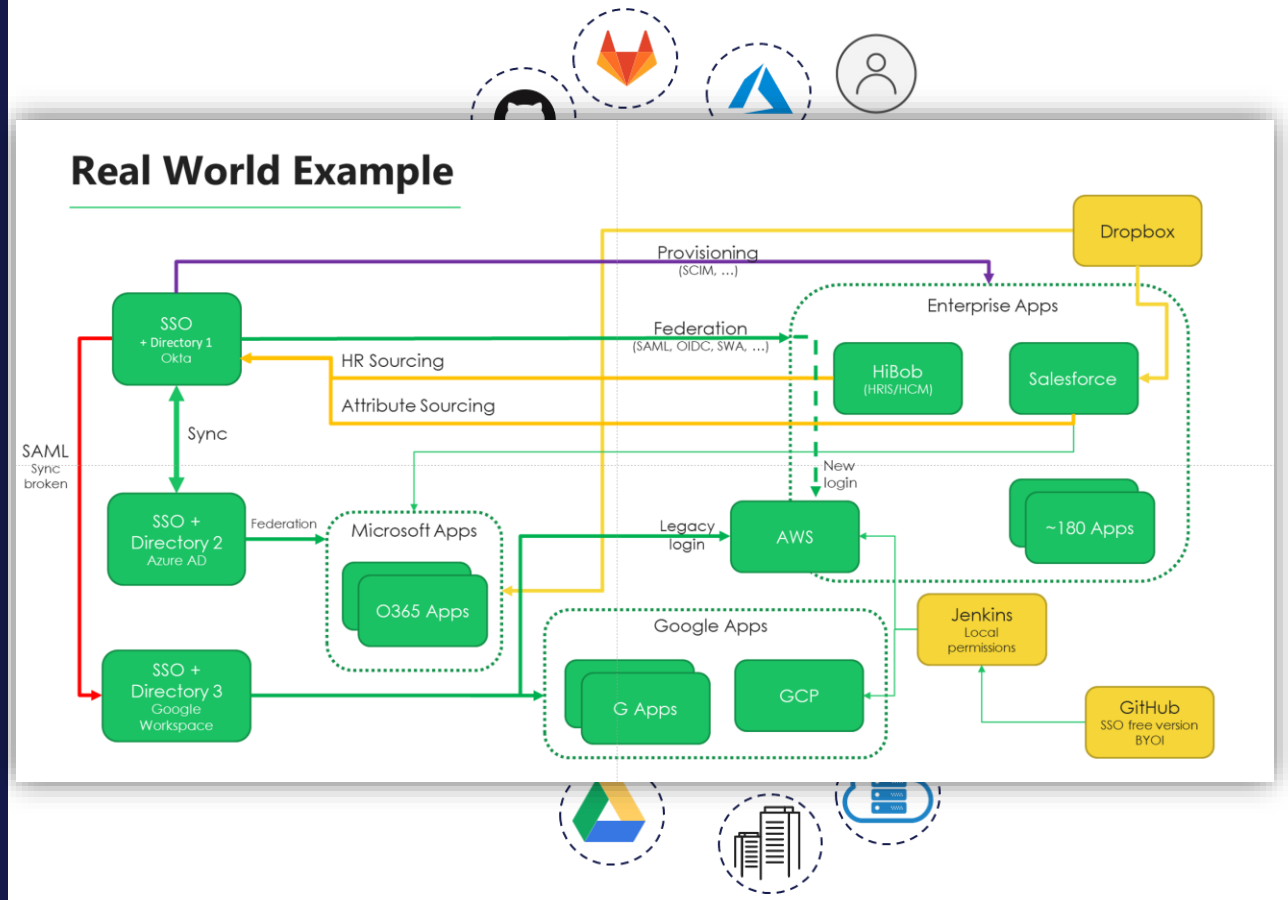
  Who has access to what? Who are my privileged users? Who are my external users? Who are my Non-human users?

- **Unable to stop identity threats**

  - Long investigation time and lacking automated remediation
  - Multiple stakeholders and work practices (IT, Security, App owners, DevOps…)

- **Increased attack surface**

  Stale access/ Overprivileged users/ Partial leavers



Some terms you may hear

CIEM - Cloud Infrastructure Entitlement Management

New category focused on **managing level of entitlement** across identities in **cloud environments**

e.g.

- *Who is overprivileged in my cloud infrastructure?*
- *How many full admins do I have ?*

ITDR - Identity Threat Detection and Response

The cybersecurity discipline focused on **detecting and responding** to threats specifically targeting **identities and credentials**

e.g.

- *prevent an attacker not from breaking in, but from logging in*
- *Where are holes in my Identity posture?*
- *Are there any attacks on my users?*

The 5 Steps to Achieving Identity Security in the Cloud

Delinea

The 5 Steps to Achieving Identity Security in the Cloud

Step 1: Achieve Visibility with Context

Centralise visibility for human and non-human identities, authentication processes, and IAM layer configurations

The 5 Steps to Achieving Identity Security in the Cloud

Step 1: Achieve Visibility with Context

Centralise visibility for human and non-human identities, authentication processes, and IAM layer configurations

Step 2: Refactor Entitlements to Achieve Least Privilege

Identify stale and overprivileged users, and minimise users and roles permission

The 5 Steps to Achieving Identity Security in the Cloud

Step 1: Achieve Visibility with Context

Centralise visibility for human and non-human identities, authentication processes, and IAM layer configurations

Step 2: Refactor Entitlements to Achieve Least Privilege

Identify stale and overprivileged users, and minimise users and roles permission

Step 3: Find and Fix Identity Misconfigurations

Detect identity-based attacks and malicious behaviour across Identity Infrastructure

The 5 Steps to Achieving Identity Security in the Cloud

Step 1: Achieve Visibility with Context

Centralise visibility for human and non-human identities, authentication processes, and IAM layer configurations

Step 2: Refactor Entitlements to Achieve Least Privilege

Identify stale and overprivileged users, and minimise users and roles permission

Step 3: Find and Fix Identity Misconfigurations

Detect identity-based attacks and malicious behaviour across Identity Infrastructure

Step 4: Detect and Remediate Identity-Related Threats

Intrusion Prevention, at the Identity Layer

The 5 Steps to Achieving Identity Security in the Cloud

Step 1: Achieve Visibility with Context

Centralise visibility for human and non-human identities, authentication processes, and IAM layer configurations

Step 2: Refactor Entitlements to Achieve Least Privilege

Identify stale and overprivileged users, and minimise users and roles permission

Step 3: Find and Fix Identity Misconfigurations

Detect identity-based attacks and malicious behaviour across Identity Infrastructure

Step 4: Detect and Remediate Identity-Related Threats

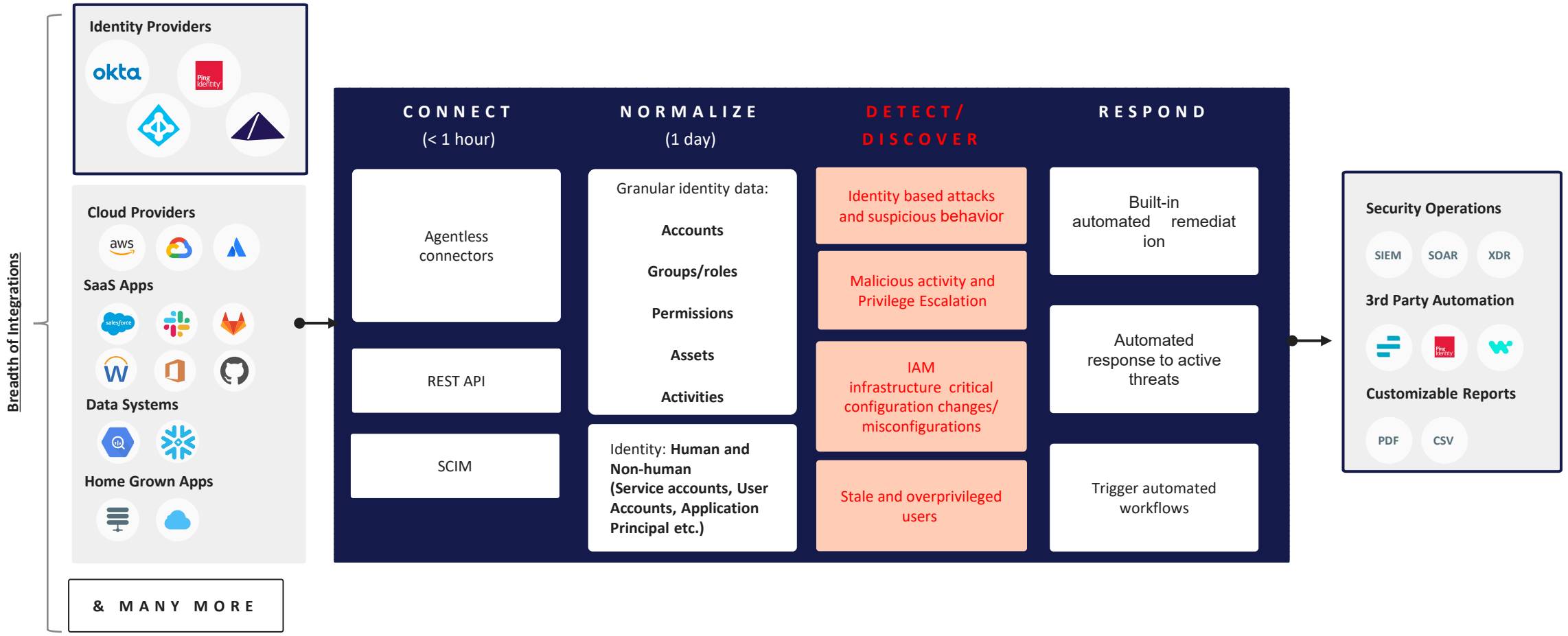
Intrusion Prevention, at the Identity Layer

Step 5: Continuously Monitor and Adjust

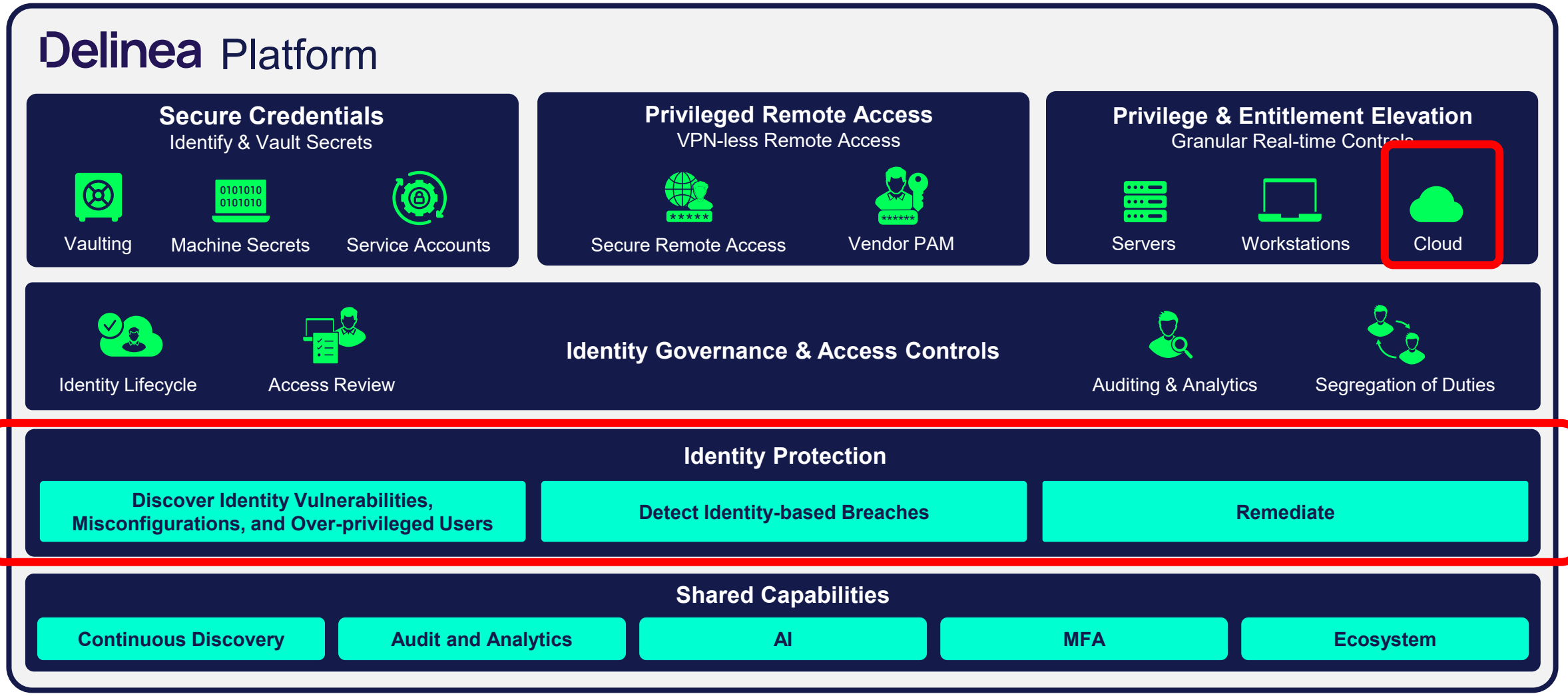
Uncover critical misconfigurations and detect suspicious activities

The Delinea approach

Seamless Integration: Effortless Harmony



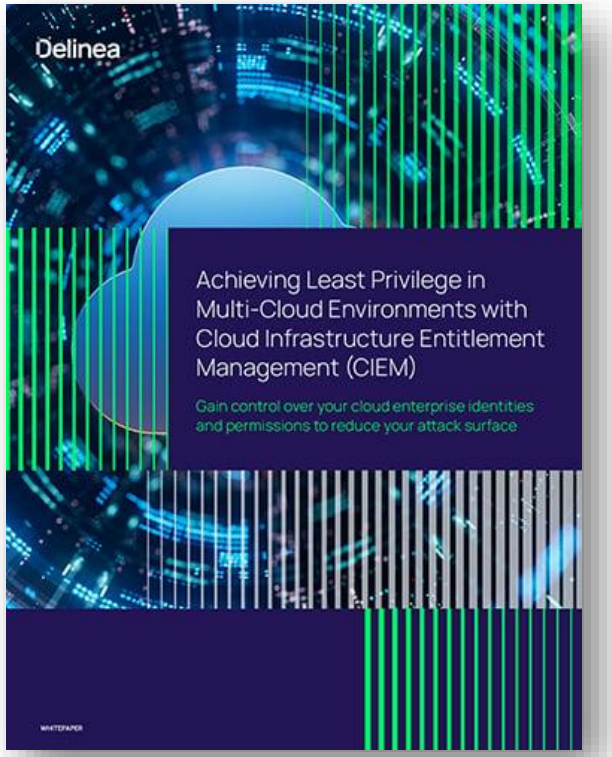
Delinea's expanding portfolio



Download your copy

eBook: 5 Steps to Securing Identity and Access in the Cloud

Whitepaper: Achieving Least Privilege in Multi-Cloud Environments with Cloud Infrastructure Entitlement Management (CIEM)



Any questions please contact:

Daniel Comarmond
Pre-Sales Australia + New Zealand
daniel.comarmond@delinea.com
mobile: +61 433 905 244