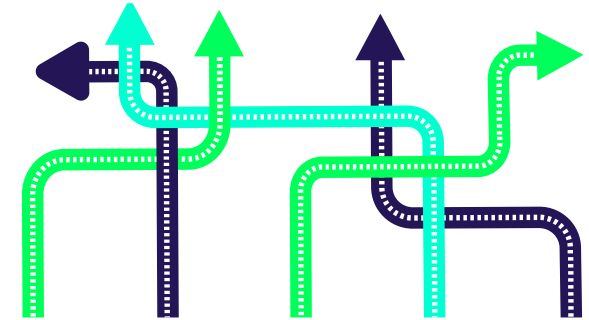# IAM Circle Workshop

How to identify and define Roles and Policies

# Why security risks are increasing

Accelerating IT Complexity

**Accelerating
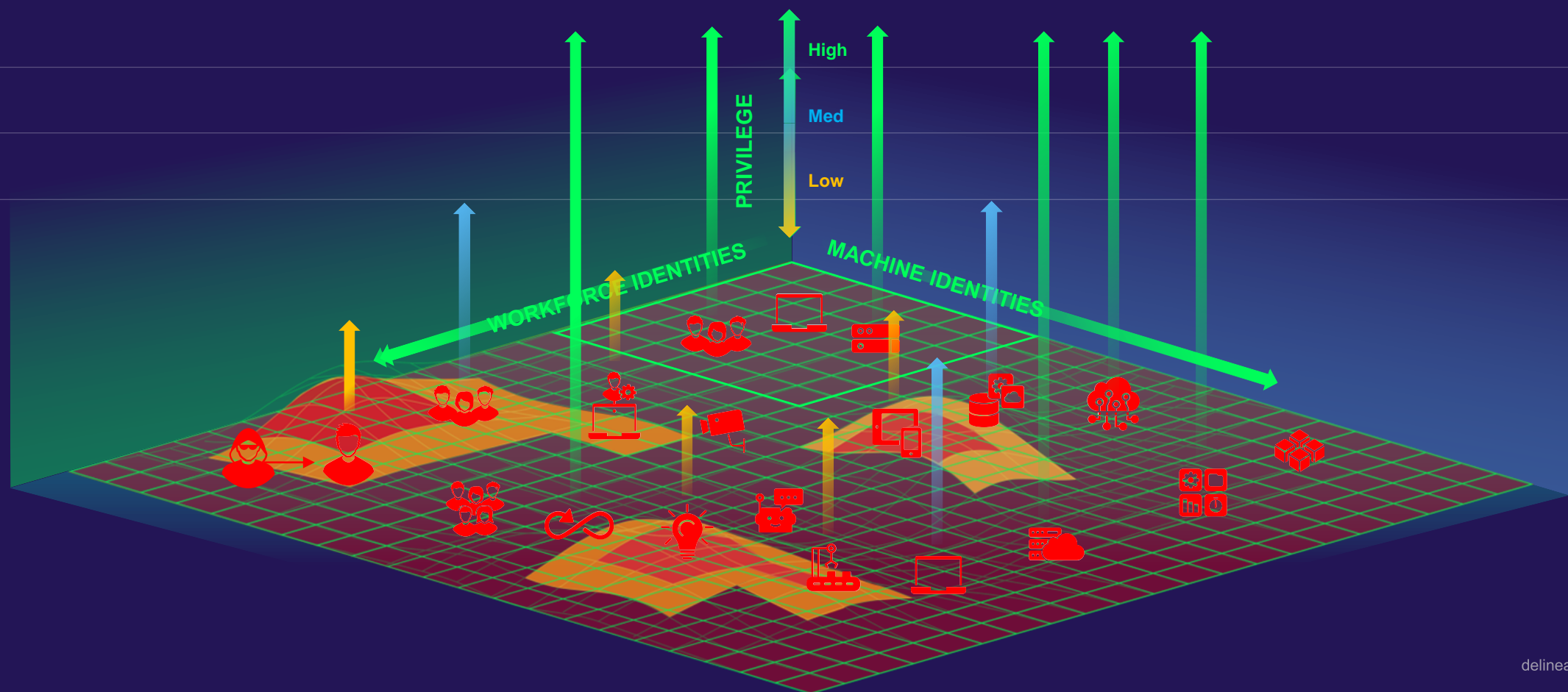IT Complexity**

**Expanding
Threat Landscape**

**Security Vendors
Proliferating**

# Everything has an identity

Human & machine identities are multiplying
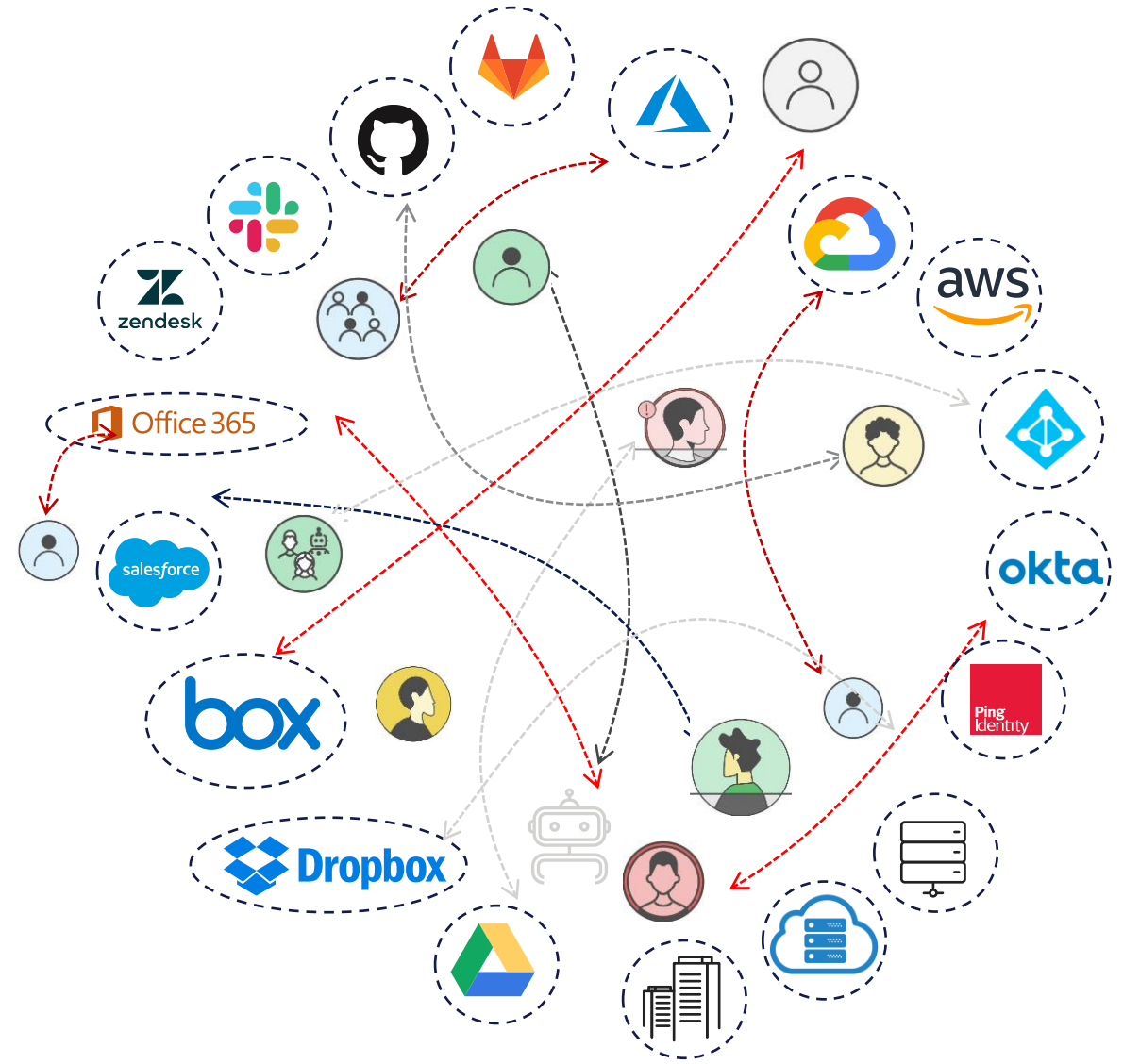
Identities must be secured

Who has access to what and how are they using it?

Are they who they say they are? Should they have access?

# Identity and Access Data is Siloed

- **Lack of visibility**
  - Who are my identities, external identities?
  - Who can access production?

- **Unable to Detect Threats** such as:
  - Identity based attacks (brute force, session hijack)
  - Privilege escalation paths

- **Operational Overhead** due to:
  - Lack of visibility extends time to detect, investigate, and prioritize
  - Long time to respond to identity threats

# The Action Plan

**Phase 3: CONTROL**

**Phase 0: HIGH RISK**

Recognize risk
& plan for action

**Phase 1: DISCOVER**

Get visibility over all Network segments

Governance, Risk & Compliance

Environments

Identities

**Phase 2: REGULATE**

Define Rules and Roles

Implement processes for J/M/L and to automatically detect and remediate violations
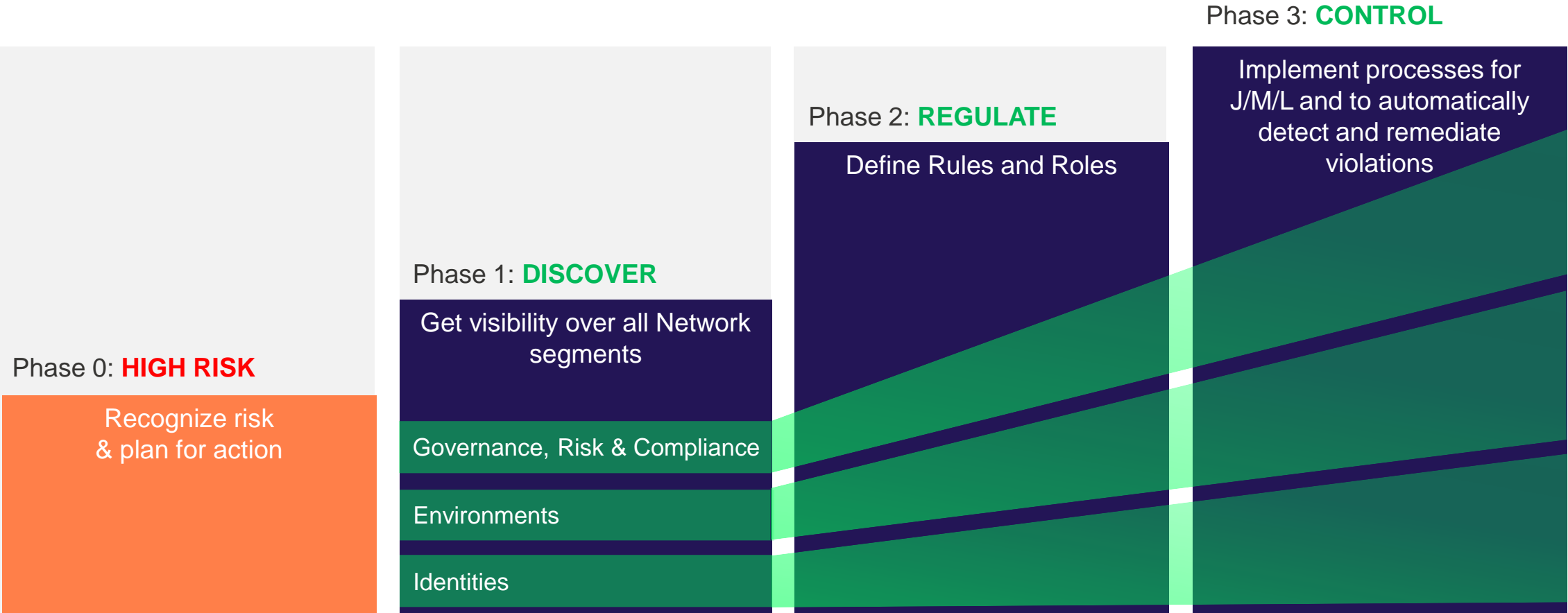
# The Delinea Approach: Classic

## Access Control

Analyze access risk across enterprise applications, report on SoD conflicts and get early sight of potential issues

## Certification

Quickly perform access reviews and certifications, automate reporting and approval workflows, rapidly detect issues and prove to auditors that the right users have access to the right resources

## Change Tracking

Track changes to both transaction and master data, identify the source of the change, the user initiating the change, as well as the before/after values

## Identity

Discover, manage and secure identities across the enterprise to provide a complete view into the identity security of the organization

**Select integrations**

**Protocol-based connectors**

Acumatica · AUDITBOARD · coupa · freshservice · Hitachi ID · JDEdwards Enterprise Software · Jira Software · Microsoft Dynamics

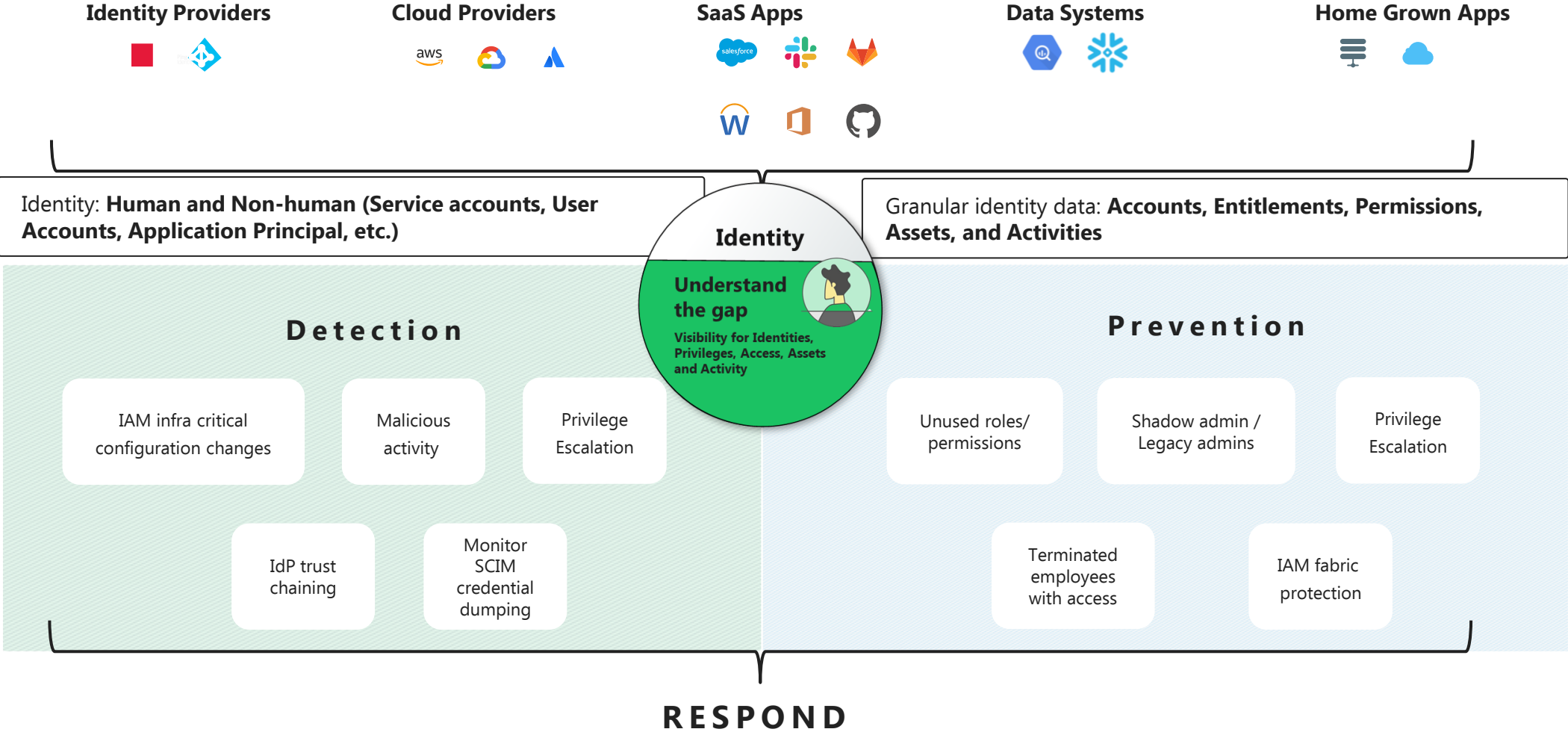ORACLE CLOUD · salesforce · SAP · workday · Workiva · zendesk · zuora

SCIM 2.0 · REST · LDAP · And more...

# The Delinea Approach: Multi-Cloud

Delinea helps organizations combat cyber threats across their entire cloud with identity and access at the center

**Identity Providers**

**Cloud Providers**
aws

**SaaS Apps**

**Data Systems**

**Home Grown Apps**

Identity: **Human and Non-human (Service accounts, User Accounts, Application Principal, etc.)**

Granular identity data: **Accounts, Entitlements, Permissions, Assets, and Activities**

**Identity**

**Understand the gap**

Visibility for Identities, Privileges, Access, Assets and Activity

## Detection

| IAM infra critical configuration changes | Malicious activity | Privilege Escalation |

| IdP trust chaining | Monitor SCIM credential dumping |

## Prevention

| Unused roles/ permissions | Shadow admin / Legacy admins | Privilege Escalation |

| Terminated employees with access | IAM fabric protection |

**RESPOND**

# Who is interested in what?

## Unparallel Visibility to Identity and Access

- Unified normalized view of identities, their access and actual usage
- Visibility to privileged users and their risk

**IAM/IT   Security**

## Elevate Your Identity Posture Security

- Monitor stale and overprivileged users
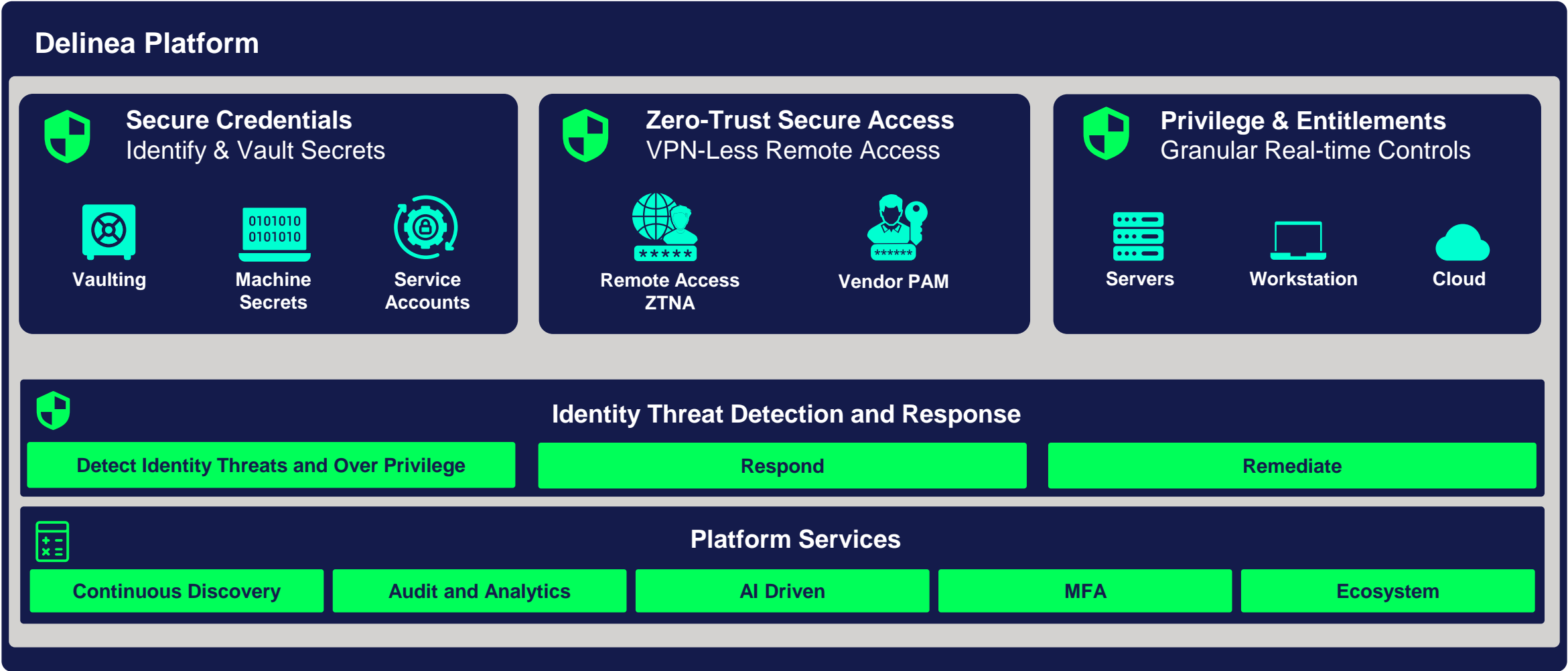- Track Identity and Identity infrastructure misconfigurations

**IAM/IT**

## Detect and remediate Identity and Access Threats (ITDR)

- Detection of identity-based attacks and suspicious behavior
- Built-in automated response

**Security**

# The Delinea Portfolio

## Delinea Platform

### Secure Credentials
**Identify & Vault Secrets**

- Vaulting
- Machine Secrets
- Service Accounts

### Zero-Trust Secure Access
**VPN-Less Remote Access**

- Remote Access ZTNA
- Vendor PAM

### Privilege & Entitlements
**Granular Real-time Controls**

- Servers
- Workstation
- Cloud

### Identity Threat Detection and Response

| Detect Identity Threats and Over Privilege | Respond | Remediate |
| --- | --- | --- |

### Platform Services

| Continuous Discovery | Audit and Analytics | AI Driven | MFA | Ecosystem |
| --- | --- | --- | --- | --- |

# Delinea At-A-Glance

We are a cloud PAM leader

## Easy to use & scale

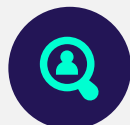Award-winning portfolio makes enterprise-class PAM accessible for all organizations

Seamlessly customize to your environment, and integrate with your other security services

## Faster time to value

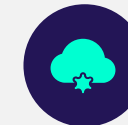Provision in days, not months and deploy quickly

Intelligent discovery & scoring of access vulnerabilities

## Innovating in the cloud

First PAM vendor with solutions built in the cloud and extend PAM across the enterprise

First unified cloud-native PAM platform

## Leader
IN ALL 5 MAJOR ANALYST REPORTS IN 2023

## 8,000+
CUSTOMERS (23% GROWTH)

## 4.8 / 5
CSAT RATING

## 900+
5-STAR GARTNER PEER REVIEWS

## 400+
INTEGRATIONS, TEMPLATES, & TOOLS

# The Delinea Platform

**OBSERVE**

### End-to-End Visibility
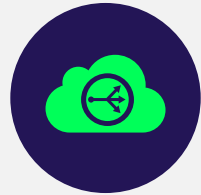
**CONTROL**

### Dynamic Privilege

**ADAPT**

### Adaptive Security

### Cloud Native

Rapid ROI. Lower total costs. Continual uptime. Effortless upgrades.

The Delinea platform seamlessly extends privileged access management across your company's hybrid multi-cloud infrastructure, with adaptive controls that help IT and cybersecurity teams rapidly meet compliance and reduce risk.

# We empower Security Champions
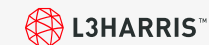
| FINANCIAL SERVICES | TECHNOLOGY | ENERGY | HEALTHCARE | EDUCATION | PUBLIC SECTOR | SERVICES | ENTERTAINMENT |
|---|---|---|---|---|---|---|---|
| BankUnited | IBM | Chevron | KAISER PERMANENTE | JOHNS HOPKINS UNIVERSITY | SEAL OF THE STATE OF INDIANA | ADP | Hard Rock |
| WELLS FARGO | SAAB | (Saudi Arabia emblem) | BlueCross BlueShield | OHIO STATE | UNITED STATES SENATE | CBRE | zynga |
| HSBC | paloalto NETWORKS | bp | Roche | University of San Diego | MINNESOTA | fiserv. | WALT DISNEY |
| TRUIST HH | | ExxonMobil | Pfizer | HARVARD UNIVERSITY | NASA | FIS | CBS |
| Fidelity INVESTMENTS | | DUKE ENERGY. | Johnson&Johnson | Carnegie Mellon University | DEPARTMENT OF DEFENSE | ThermoFisher SCIENTIFIC | AT&T |
| | | Valero | | UCLA Health | NIST | L3HARRIS | |

# Workshop Topics

# Stage 1: Discover

Phase 1: **DISCOVER**

**Get visibility over all Network segments**

Governance, Risk & Compliance

Environments

Identities

- What are the driver for an Identity and Role Mgmt. Implementation
- What Identities are important for this (Kind/Type/User?)
- What environments do you need to include in your Discovery
- What are the first 3 challenges that come to mind with this step?

# Stage 2: Regulate

Phase 2: **REGULATE**

Define Rules and Roles

- What are the typical roles relevant for a company (Min. 4)?
- Why are these roles important?
- How do they fit into regulatory policies
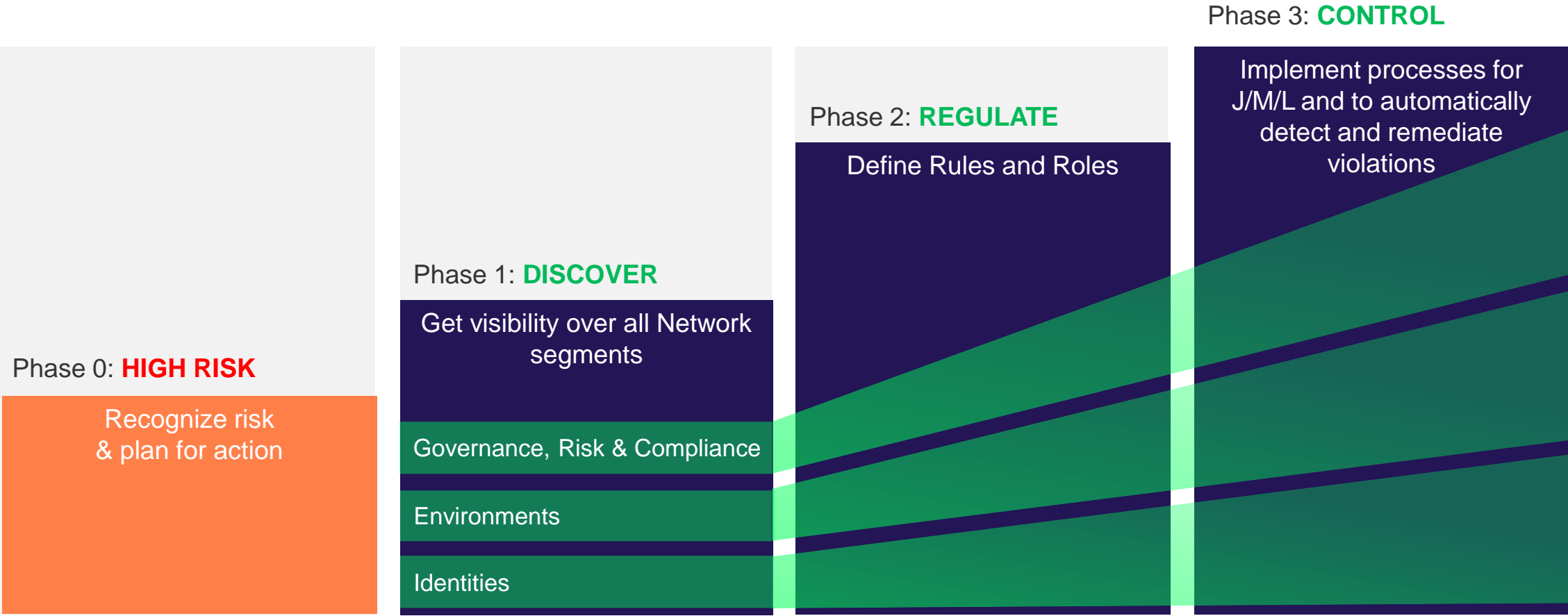
# The Action Plan

Phase 3: **CONTROL**

Implement processes for J/M/L and to automatically detect and remediate violations

- How would you re-certify the Rights of every member in a Role?
- What are important topics to be considered in this process?
- What would be the ideal scenario to get alerted if an case out of policy appears?
- What level of auto remediation would you accept for these cases?

# Where are you and your company now?

Phase 3: **CONTROL**

**Phase 0: HIGH RISK**

Recognize risk
& plan for action

Phase 1: **DISCOVER**

Get visibility over all Network segments

Governance, Risk & Compliance

Environments

Identities

Phase 2: **REGULATE**

Define Rules and Roles

Implement processes for J/M/L and to automatically detect and remediate violations

# Thank You.

**Delinea**

Defining the boundaries of access