Advanced PAM

Better visibility, greater control

Igal Dahan

Senior Cybersecurity Engineer

MultiPoint Ltd

Delinea

MULTIPOINT GROUP

delinea.com

Delinea at-a-glance

We are a PAM leader

Delinea

Leader(s)

IN GARTNER, FORRESTER &
KUPPINGER COLE ANALYST REPORTS

4.8 / 5

COMBINED CSAT RANKING

50%+

OF FORTUNE 100 CUSTOMERS

1,000+

COMBINED NEW CUSTOMERS
ADDED IN 2022

700+

5-STAR GARTNER PEER REVIEWS

150+

COMBINED INTEGRATIONS

The PAM Maturity Model

December 2022

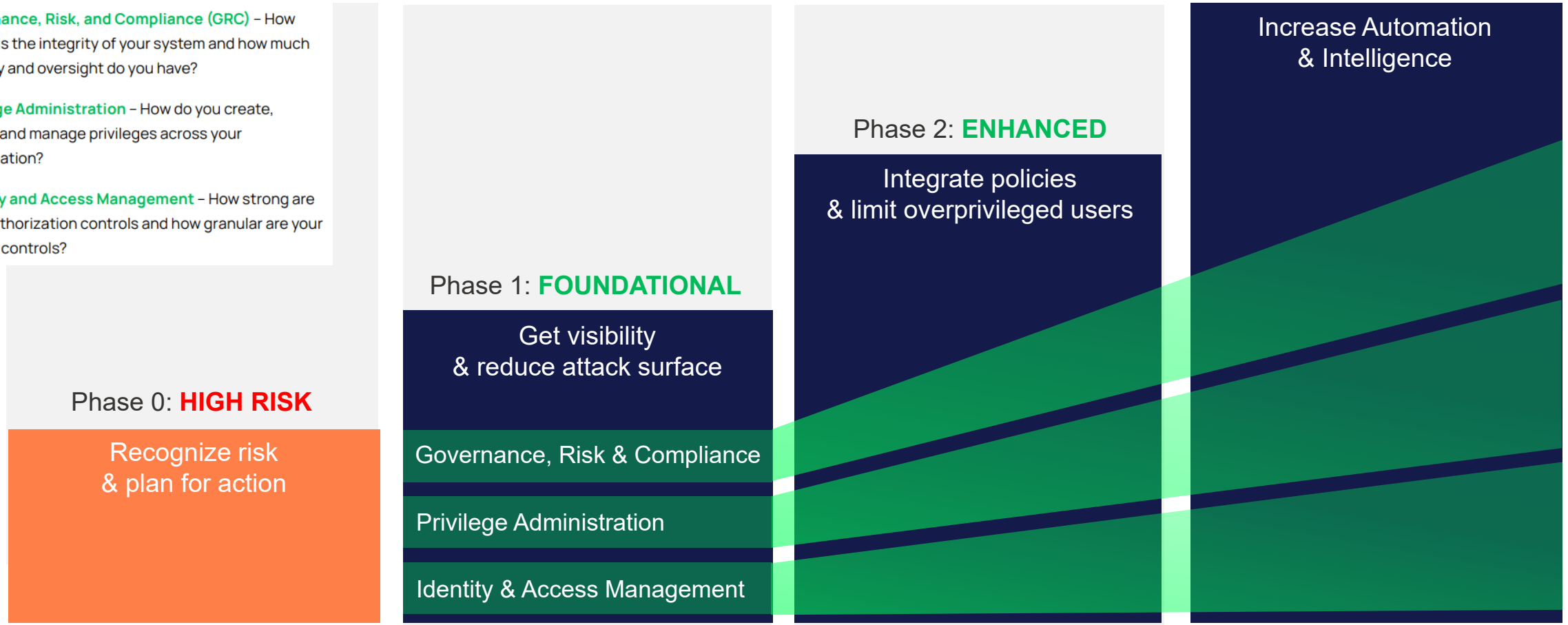
Delinea

delinea.com

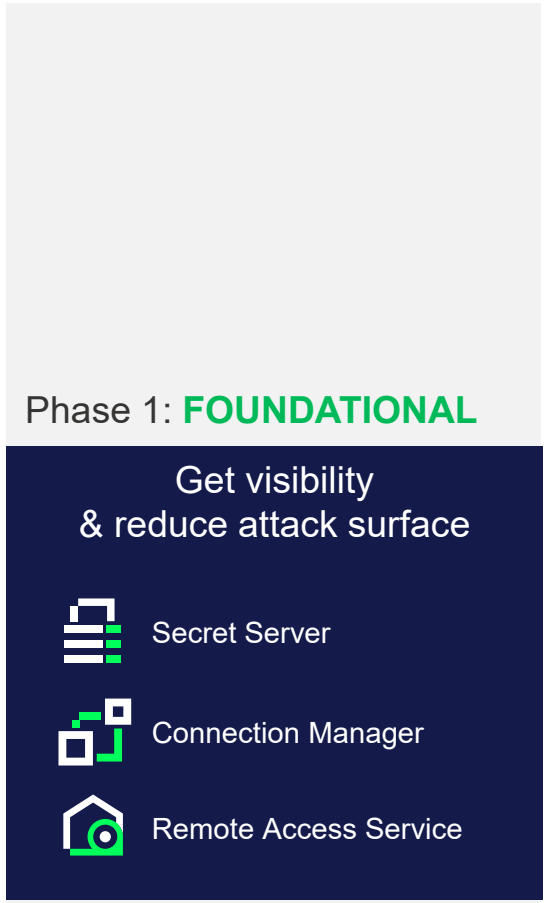
The PAM Maturity Model

Three Dimensions

- **Governance, Risk, and Compliance (GRC)** – How strong is the integrity of your system and how much visibility and oversight do you have?
- **Privilege Administration** – How do you create, define, and manage privileges across your organization?
- **Identity and Access Management** – How strong are your authorization controls and how granular are your access controls?



The PAM Maturity Model – Phase 1



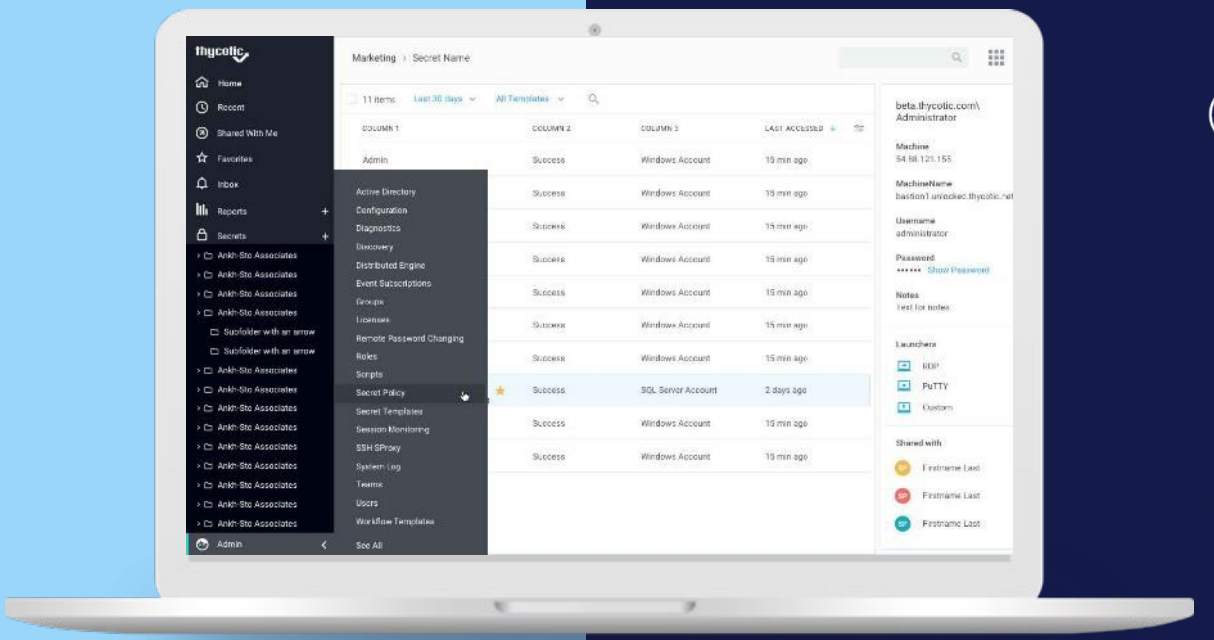
FOUNDATIONAL

Phase 1: **Investments**

- ✓ Visibility into accounts, access, and privilege
- ✓ Vaulting to manage, protect and rotate passwords
- ✓ MFA for identity assurance
- ✓ Privileged access workflows for JIT access and privilege
- ✓ “Clean Source” to protect internal systems from infected client workstations
- ✓ Alternate Admin accounts instead of public accounts

Secret Server

Fully-featured PAM solution available both on-premises and in the cloud. Centralized management, control and auditing of all Privileged accounts, credentials and activity. Userbase is any human user who uses elevated privileges such as IT admins, engineers, DevOps, etc. and licensing is based on human Privileged users. Available in cloud, subscription on-premise and perpetual on premise.



Establish Vault

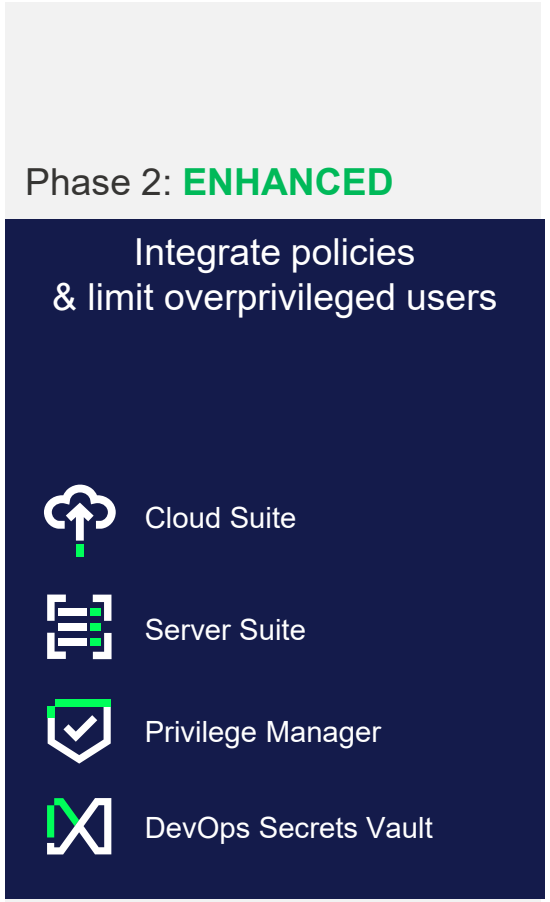
Discover Unknown Accounts

Delegate Access

Manage Secrets

Control Sessions

The PAM Maturity Model – Phase 2



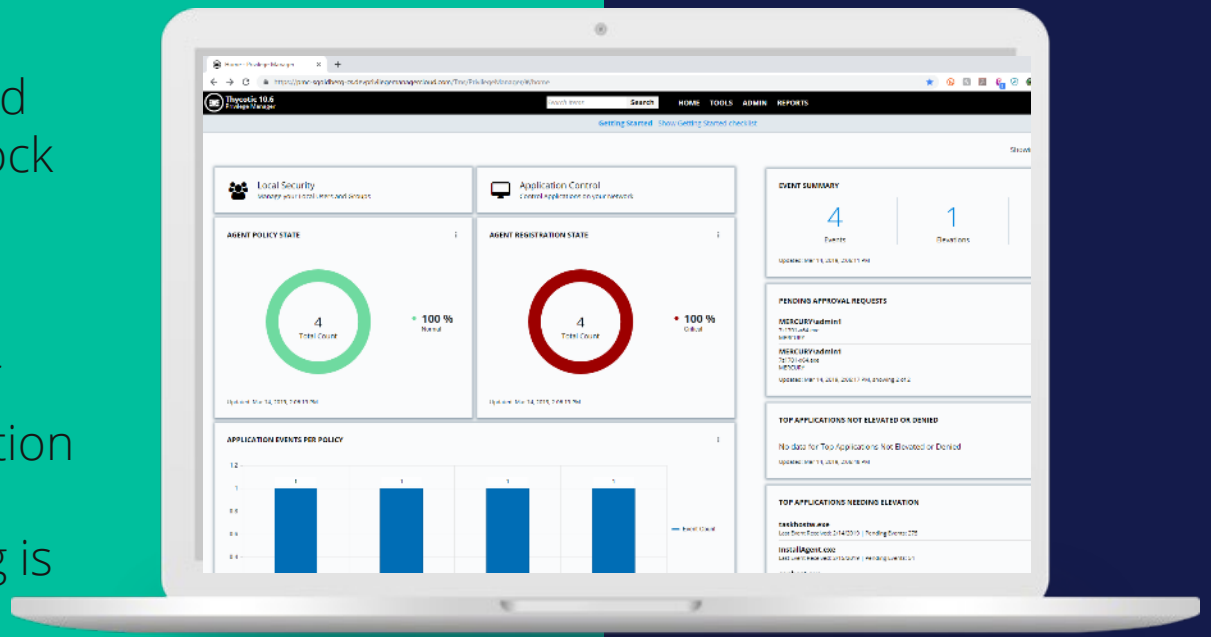
ENHANCED

Phase 2: **Investments**

- ✓ Alternate Admin Accounts + Privilege elevation
- ✓ Discover/manage local endpoints accounts & groups
- ✓ Secure VPN-less remote access to servers for 3rd-parties
- ✓ Just-in-time access requests from ITSM workflows
- ✓ Host-level privileged audit & session recording
- ✓ Eliminate local admin accounts
- ✓ Automate privilege security for DevOps
- ✓ MFA everywhere

Privilege Manager

Allows the implementation and enforcement of least privilege policies for Windows, Unix/Linux and Mac. Elevate Privileges for applications and processes and not users. Block ransomware through application white/black/greylisting. Userbase can be any user of any role since every workstation and server can operate with elevated privileges. Licensing is based on workstations or servers which need to have these controls implemented. Available in cloud, subscription on-premise and perpetual on premise.



Deploy Agents

Manage Accounts

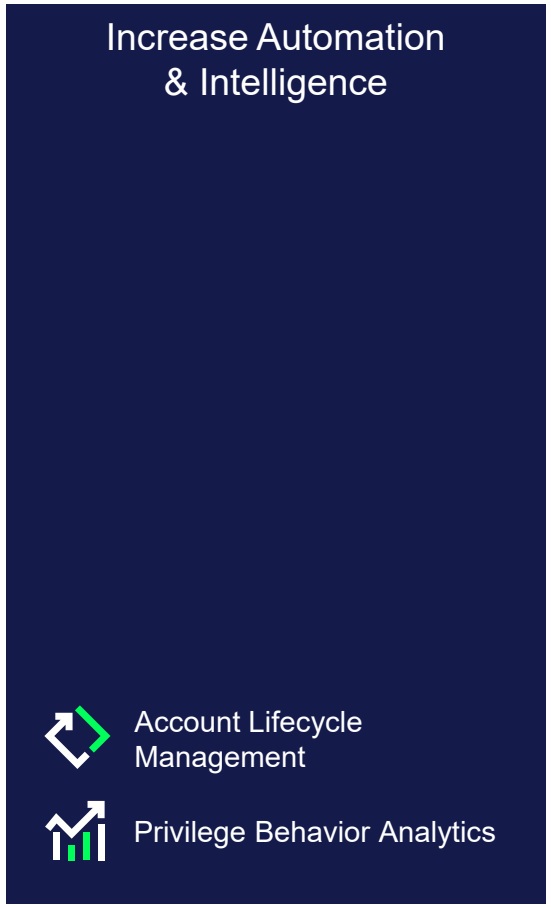
Define Policies

Elevate Applications

Improve Productivity

The PAM Maturity Model – Phase 3

Phase 3: **ADAPTIVE**



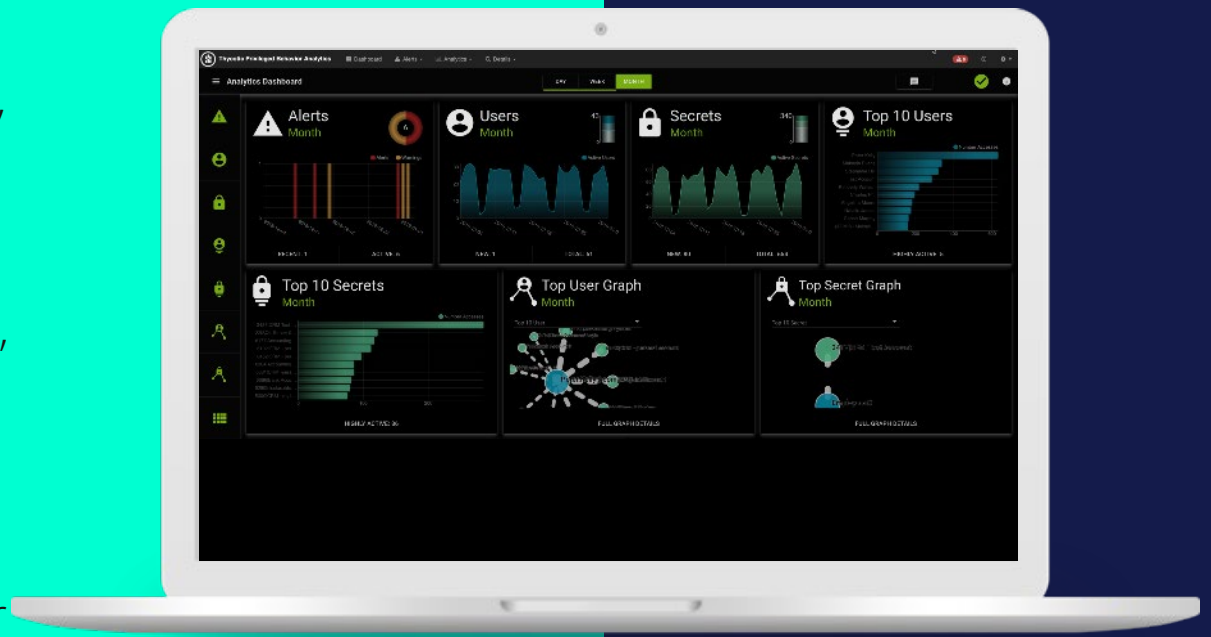
ADAPTIVE

Phase 3: **Investments**

- ✓ Leverage audit data, analytics, & automation
- ✓ Establish granular privilege elevation
- ✓ Continuous discovery and new asset onboarding
- ✓ Establish cryptographic trust
- ✓ Integration with IGA for attestation
- ✓ Service account discovery & governance
- ✓ MFA at the highest NIST assurance levels

Privileged Behavior Analytics

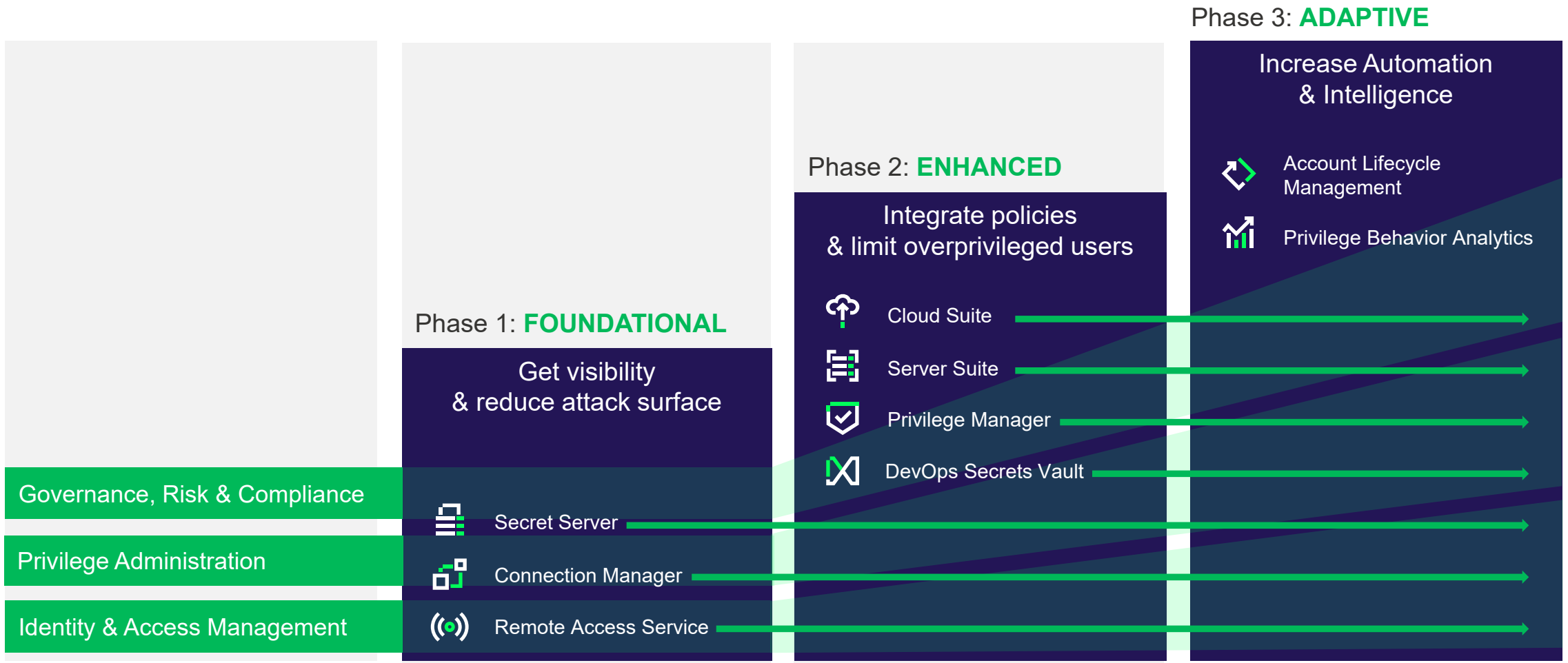
Included in Secret Server, this component provides threat enhanced reporting, detection, and incident response for all activity managed by Thycotic Secret Server. Any account, credential or user managed by Thycotic Secret Server can be monitored and reported on with Privileged Behavior Analytics. Licensing is included with Secret Server.



- **Secure Accounts**
- **Establish Baselines**
- **Monitor & Identify**
- **Identify & Alert**
- **Take Action**

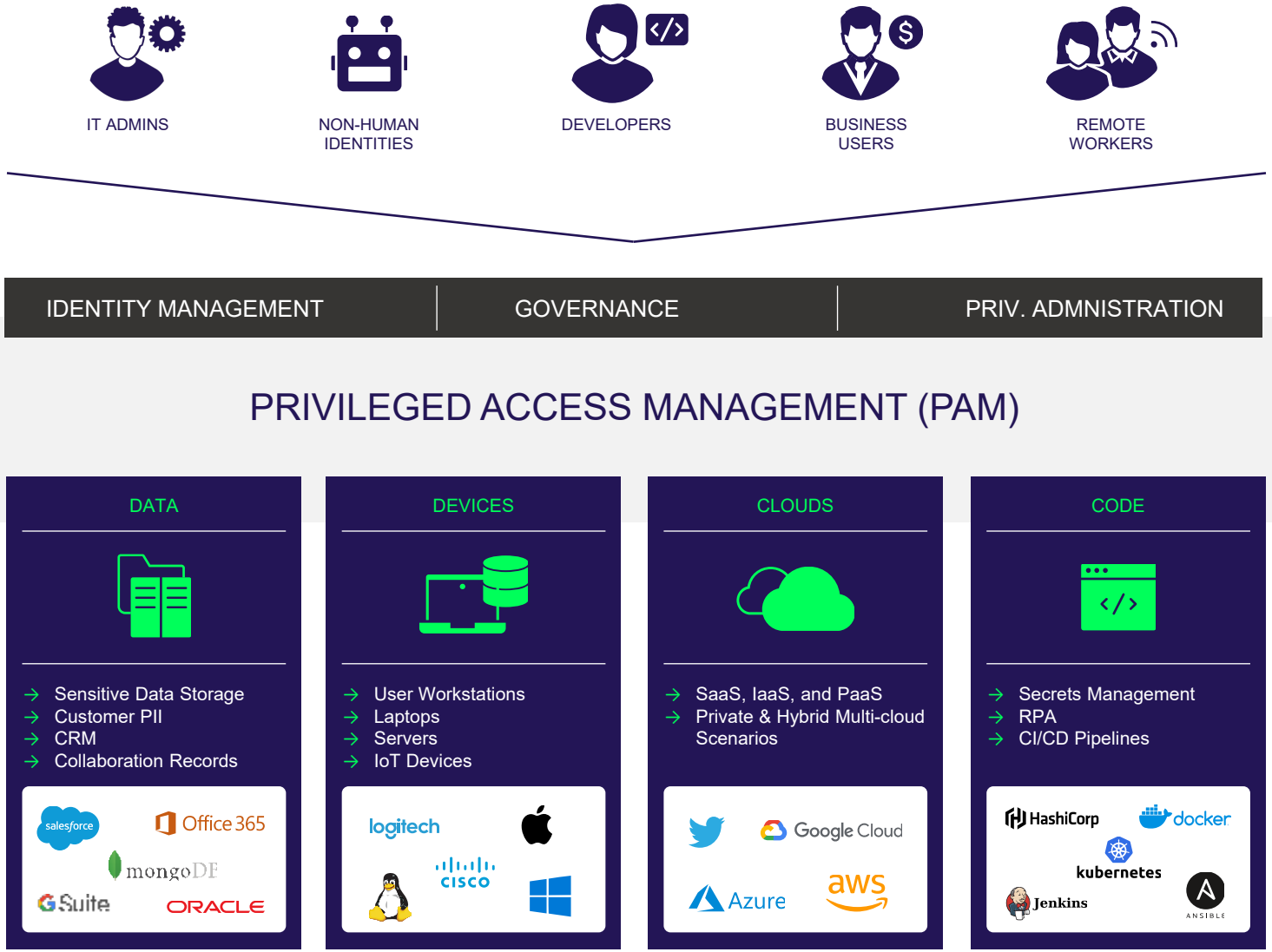
The PAM Maturity Model

Delinea's portfolio addresses XPM and supports the PAM journey



Modern PAM challenge:

Access control for anyone, anytime, anywhere



Journey to “Advanced” - Building beyond a Vault

Vault-centric access control is essential but can be further supplemented by **identity centric controls rooted in zero trust framework**

- ✓ Establish **Identity Assurance**, Least Access and Privilege
- ✓ Prevent lateral movement with host-enforced **MFA** and workflow-based **just-in-time** (JIT) access and **just-enough-privilege** (JEP) policies
- ✓ **Secure remote access** and privileged sessions ensure a secure, clean-source admin environment
- ✓ Log, monitor and record all privileged access

A vault solution alone is not enough

There are several Audit and Security challenges with Vault alone

- Audit logs on servers indicate the shared account
- Logs from vault and servers must be correlated to determine who was responsible for access and activity
- Log correlation doesn't help if multiple admins access a server during the same time period
- Shared account grants its full privileges to the user
- Server cannot determine if appropriate human access or not

- Audit logs on servers clearly identify the user for full accountability
- Specific privileges granted to the user based on role
- Server enforces MFA to ensure appropriate access

Least Privilege and Just-in-Time Access

How Delinea Server PAM enables Just-in-Time (JIT) and Zero Standing Privilege

Workflows based on three elements of privileged access.

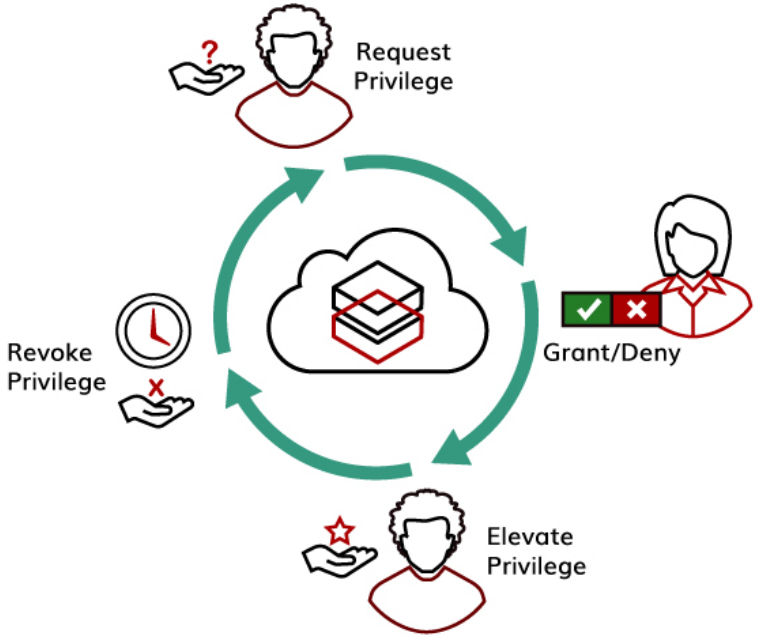
- Location: Where users exercise privileges
- Actions: What users do with those privileges
- Time: When privileges can be used

Pre-Defined Authorization

- Defined scope (location, actions, time) as policy
- No request/approval process needed

Built-in & 3rd Party Approval-Required Workflows

- On-demand request for access (location, actions, time)
- Approval needed to proceed with access
- **Service Now and Sailpoint**



Thank You.

Delinea

Defining the boundaries of access