Improve your security posture with the PAM Maturity Model

Delinea ACCESS42 Cybersecurity

delinea.com

Who Am I

Patrick van der Veen

- Director, Sales Engineering – Northern Europe
- 3,5 years @ Delinea (Thycotic / Centrify)
- Over 16 years in pre-sales
- Infrastructure, virtualization, disaster recovery, data security, vulnerability management, penetration testing, endpoint detection and response, Privileged Access Management (PAM).

CISSP® Certified Information Systems Security Professional

CCSP℠ Certified Cloud Security Professional

OffSec™ OSCP

CEH™ Certified Ethical Hacker

Poll

In the security world, what does PAM stands for?

- Pulse Amplitude Modulation
- Privileged Account Management ✓
- Prayers And Miracles
- Privileged Access Management ✓ ✓

Today’s Somber Reality

> “
>
> Hackers don’t hack in anymore —
> they log in using weak, default, stolen, or otherwise compromised credentials.

Privilege Management has a big impact on Cyber Incidents

80% of breaches involve Privileged Accounts

Forrester

96% of Critical Vulnerabilities on Windows can be mitigated by removing Local Administrative rights

Microsoft

85% of Cyber Attacks are done through compromised endpoints

SANS

Most attacks target Privileged Access

- Also, non-human accounts
- Local administrator
- Unix ROOT
- Service accounts
- Domain administrator
- CISCO Enable
- Application/SaaS Accounts
- Batch job/scheduled tasks/cron jobs
- Normal User Accounts with access to sensitive data

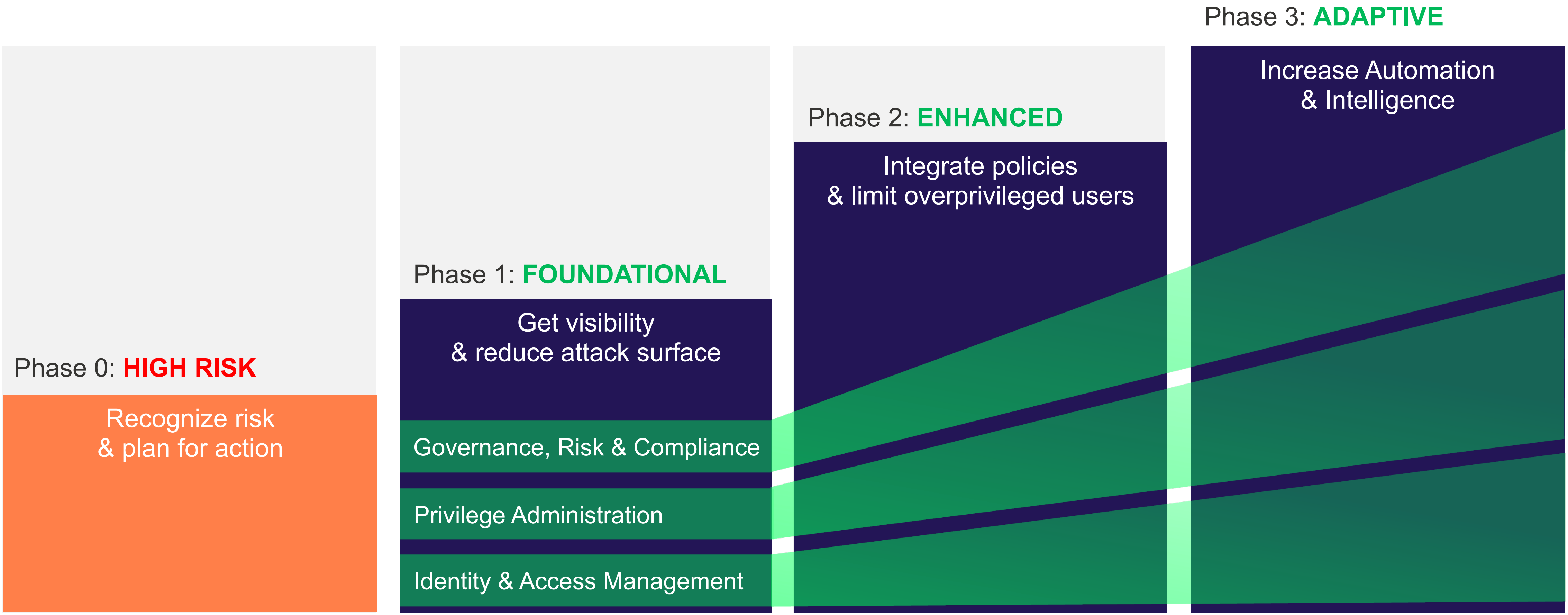
Admin/Security/
Helpdesk/3rd Party

Apps/API/RPA/
Service Accounts

Int./Ext. Business
User or 3rd Party

Almost ALL USERS are PRIVILEGED

The PAM Maturity Model



Phase 0: **HIGH RISK**

Recognize risk
& plan for action

Phase 1: **FOUNDATIONAL**

Get visibility
& reduce attack surface

Governance, Risk & Compliance

Privilege Administration

Identity & Access Management

Phase 2: **ENHANCED**

Integrate policies
& limit overprivileged users

Phase 3: **ADAPTIVE**

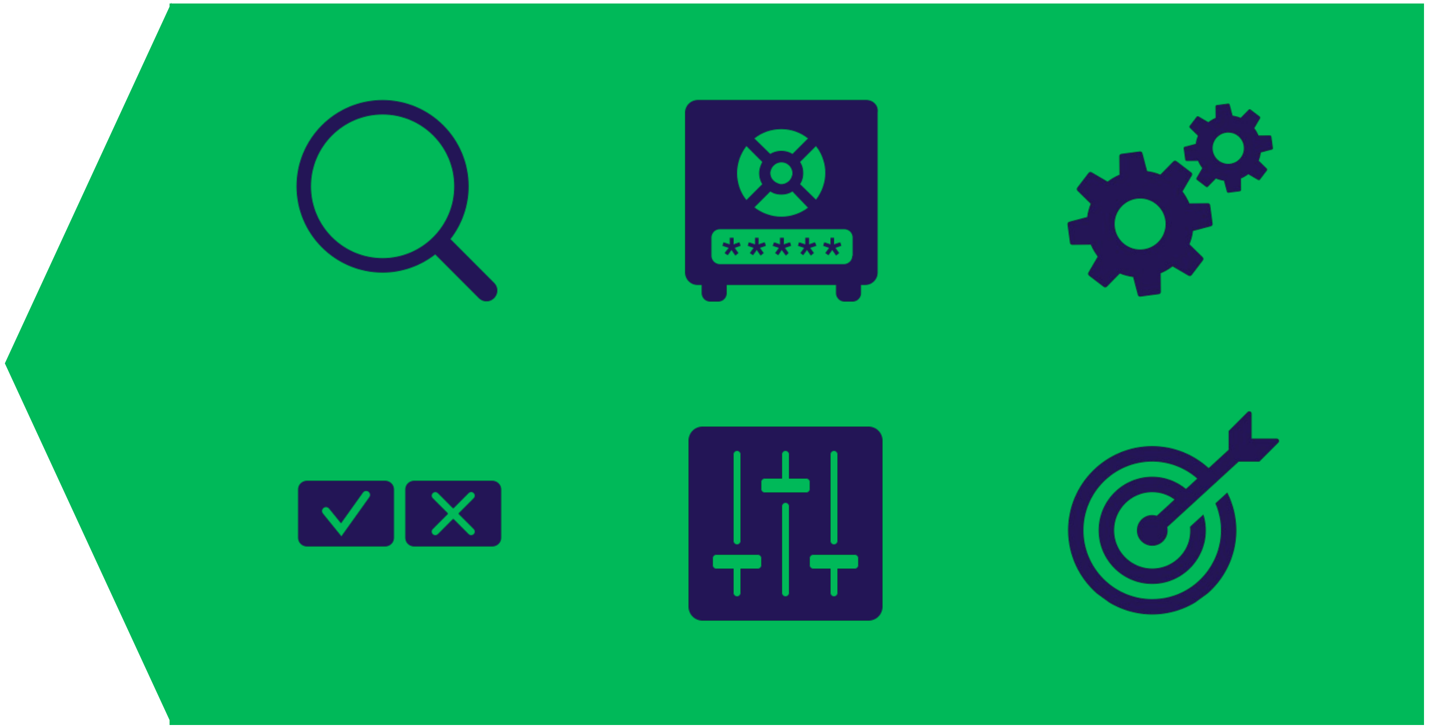
Increase Automation
& Intelligence

The PAM Maturity Model – Phase 1

Phase 1: **FOUNDATIONAL**

Get visibility
& reduce attack surface

- Secret Server
- Connection Manager
- Remote Access Service



The PAM Maturity Model – Phase 1

Phase 1: **FOUNDATIONAL**

Get visibility
& reduce attack surface

- Secret Server
- Connection Manager
- Remote Access Service

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

The PAM Maturity Model – Phase 2

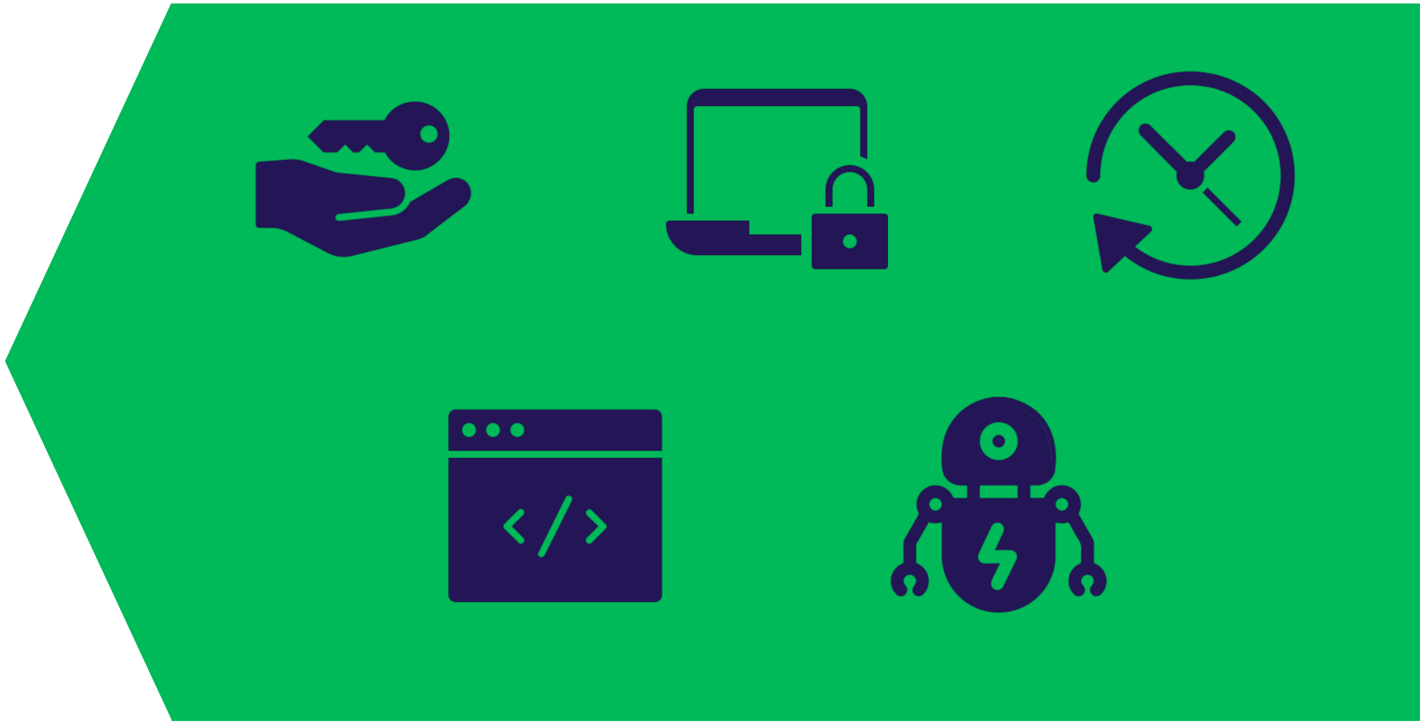
Phase 2: **ENHANCED**

Integrate policies
& limit overprivileged users

Server PAM

Privilege Manager

DevOps Secrets Vault



The PAM Maturity Model – Phase 2

Phase 2: **ENHANCED**

Integrate policies
& limit overprivileged users

Server PAM

Privilege Manager

DevOps Secrets Vault

ENHANCED

Phase 2: **Investments**

- ✓ Basic 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

The PAM Maturity Model – Phase 3

Phase 3: **ADAPTIVE**

Increase Automation & Intelligence

- Account Lifecycle Management
- Privileged Behavior Analytics

The PAM Maturity Model – Phase 3

Phase 3: **ADAPTIVE**

Increase Automation
& Intelligence

Account Lifecycle Management

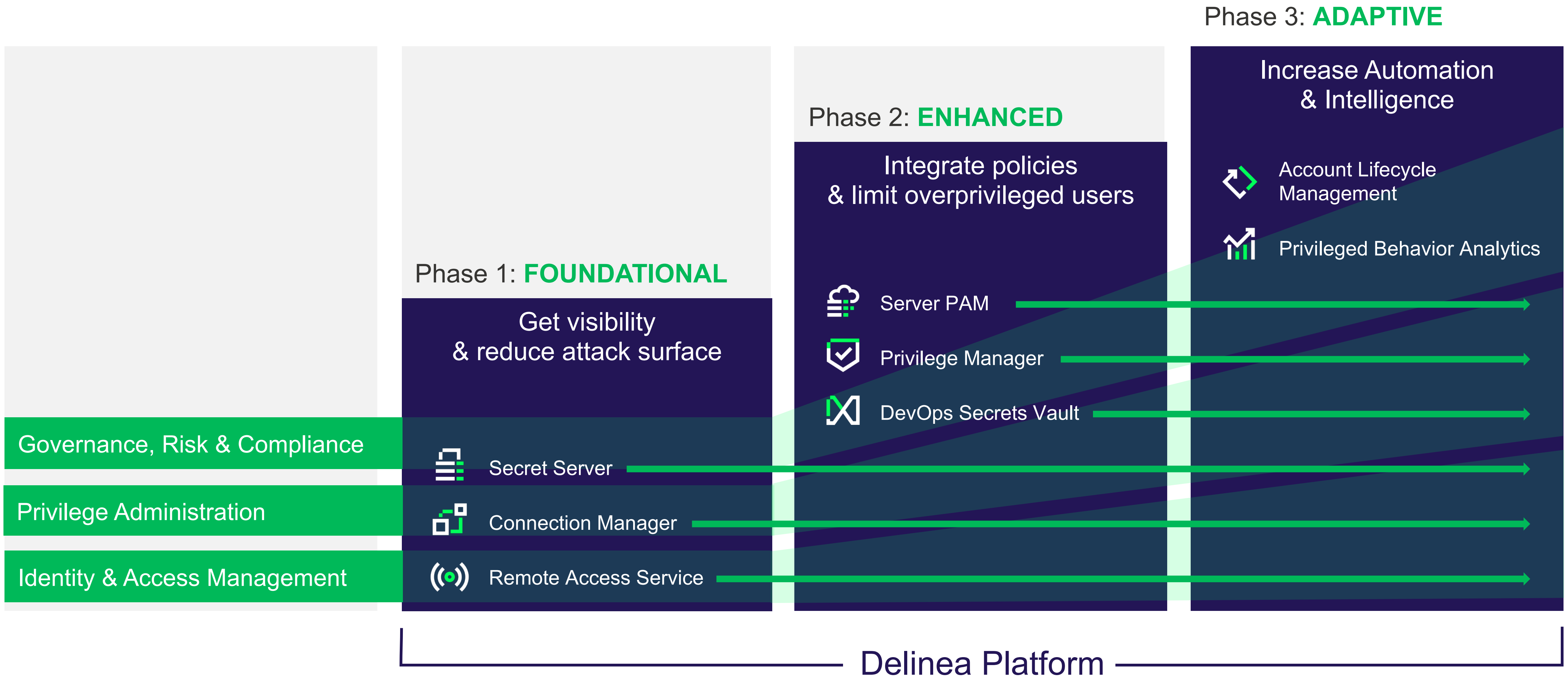
Privileged Behavior Analytics

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

The PAM Maturity Model

The Delinea portfolio addresses Extended PAM and supports the PAM journey



Phase 3: **ADAPTIVE**

Increase Automation & Intelligence

Account Lifecycle Management

Privileged Behavior Analytics

Phase 2: **ENHANCED**

Integrate policies & limit overprivileged users

Server PAM

Privilege Manager

DevOps Secrets Vault

Phase 1: **FOUNDATIONAL**

Get visibility & reduce attack surface

Secret Server

Connection Manager

Remote Access Service

Governance, Risk & Compliance

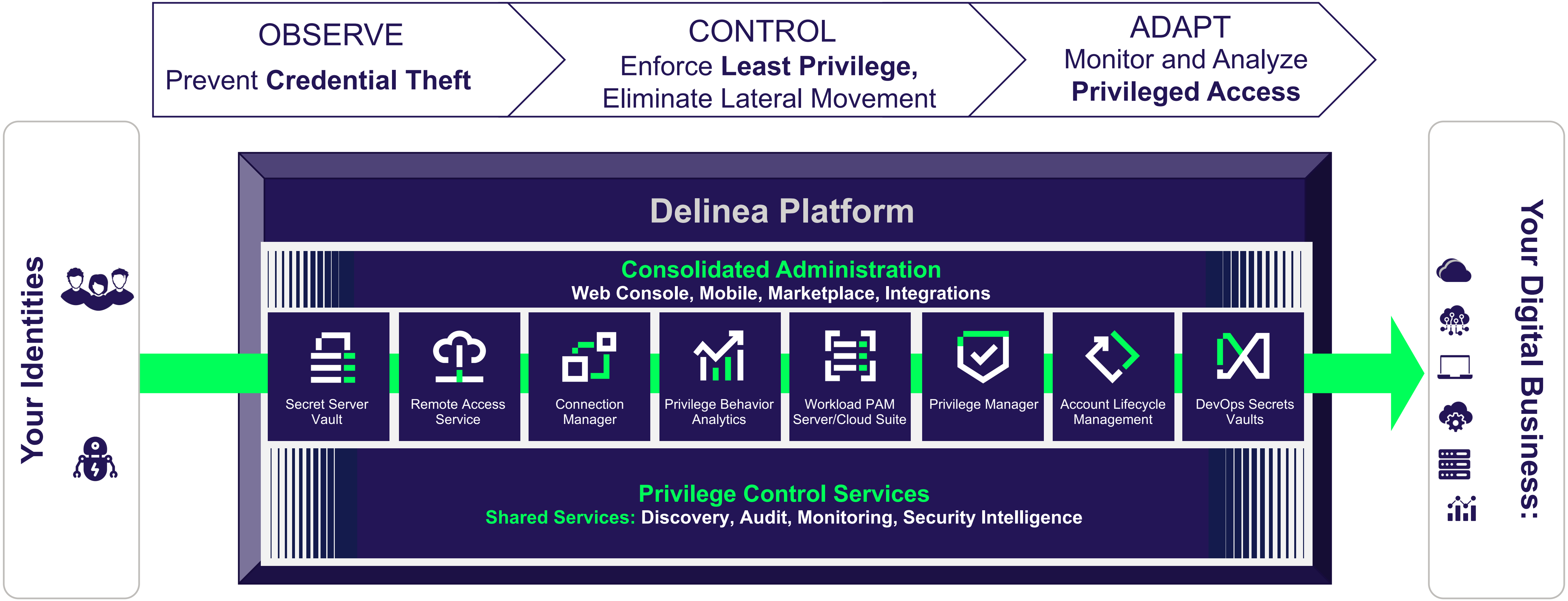
Privilege Administration

Identity & Access Management

Delinea Platform

Delinea Platform

Building Shared Services That Tightly Integrate Delinea PAM Services



OBSERVE

Prevent **Credential Theft**

CONTROL

Enforce **Least Privilege,**
Eliminate Lateral Movement

ADAPT

Monitor and Analyze
Privileged Access

Your Identities

Delinea Platform

Consolidated Administration

Web Console, Mobile, Marketplace, Integrations

Privilege Control Services

Shared Services: Discovery, Audit, Monitoring, Security Intelligence

Your Digital Business:

Thank You.

Delinea
Defining the boundaries of access

Patrick van der Veen
patrick.vanderveen@delinea.com