PAM

credenziali e privilegi dei server in cassaforte e semplificazione nella gestione dei PC

Nicola D'Ottavio –Delinea Partner Alliance Manager – Italy & Med

Bologna 12 ottobre 2023 – Bottega Portici Due Torri

Delinea

delinea.com

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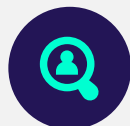
Seamlessly customize to your environment, and integrate with your other security services

Faster time to value

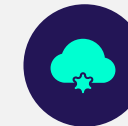Provision in days, not months and deploy quickly

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

Building a cloud-first platform to address extended PAM challenges

Leader
IN GARTNER, FORRESTER & KUPPINGER COLE ANALYST REPORTS

1,300+
NEW CUSTOMERS ADDED IN 2022

4.8 / 5
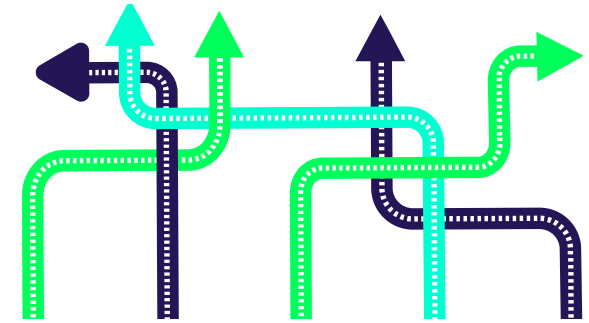CSAT RANKING

750+
5-STAR GARTNER PEER REVIEWS

150+
INTEGRATIONS

Why security risks are increasing

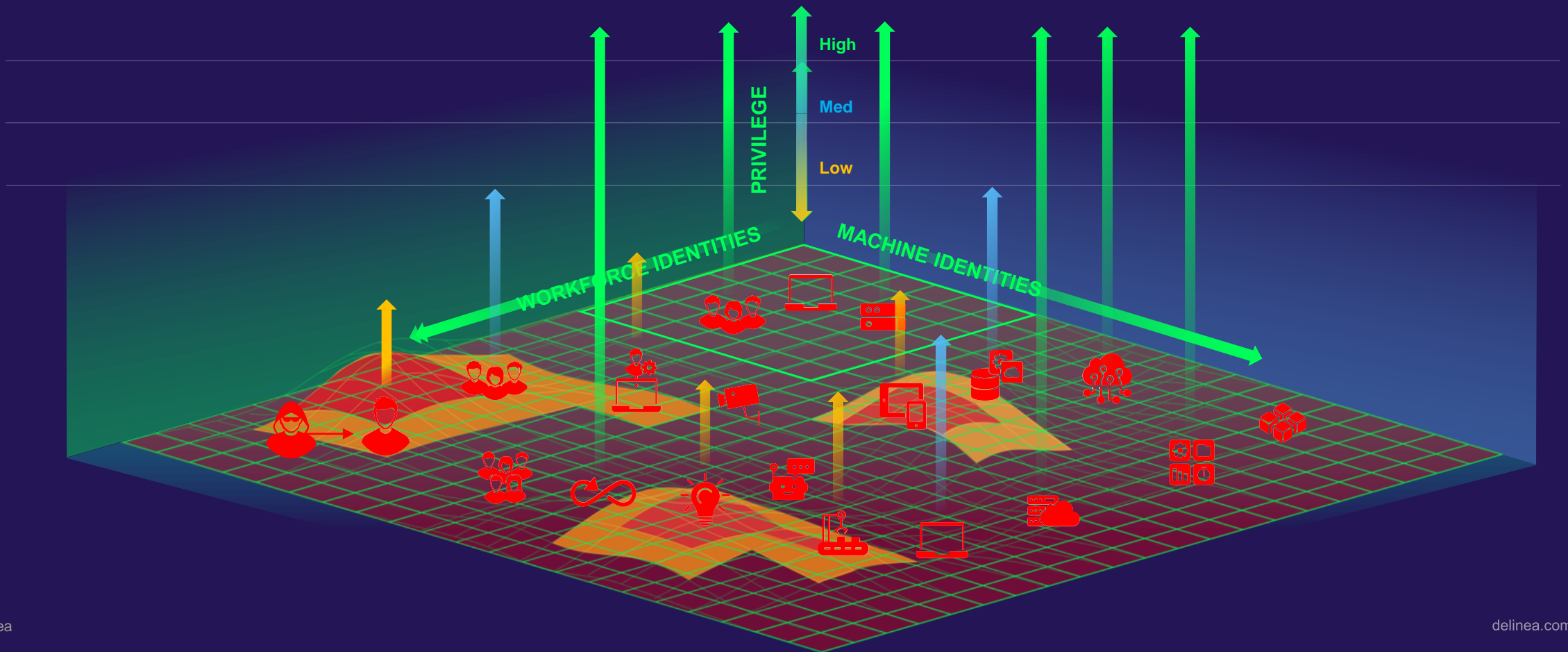Accelerating IT Complexity

**Accelerating
IT Complexity**

**Expanding
Threat Landscape**

**Security Vendors
Proliferating**

Everything has an identity
# Human & machine identities are multiplying
Identities must be secured

PAM only covers *some* of your systems & privileged accounts
Extended PAM (XPM) reduces the attack surface for the entire enterprise

All assets across on-premises and cloud, all human and non-human identities

On-premises servers

PRIVILEGE

Admins

WORKFORCE IDENTITIES

Traditional PAM

MACHINE IDENTITIES
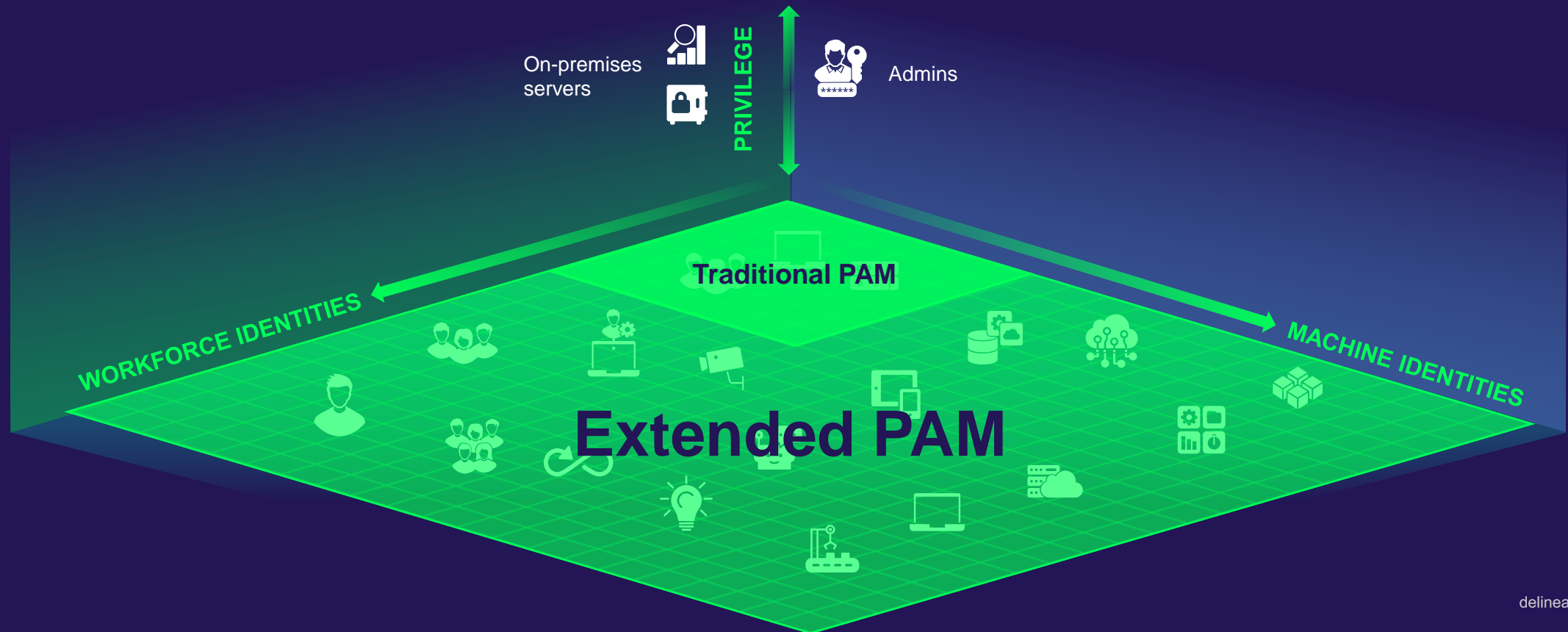
Extended PAM

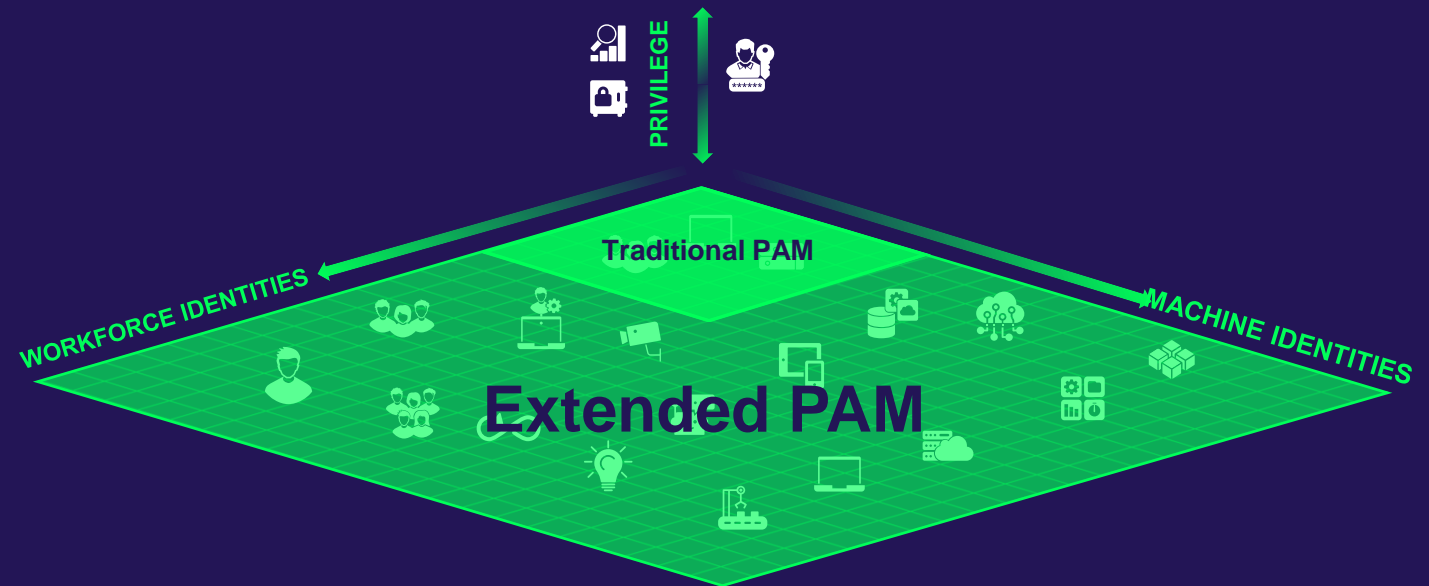# The Delinea Vision for Extended PAM

Prevent identity/credential theft by increasing visibility and discovery across all identities
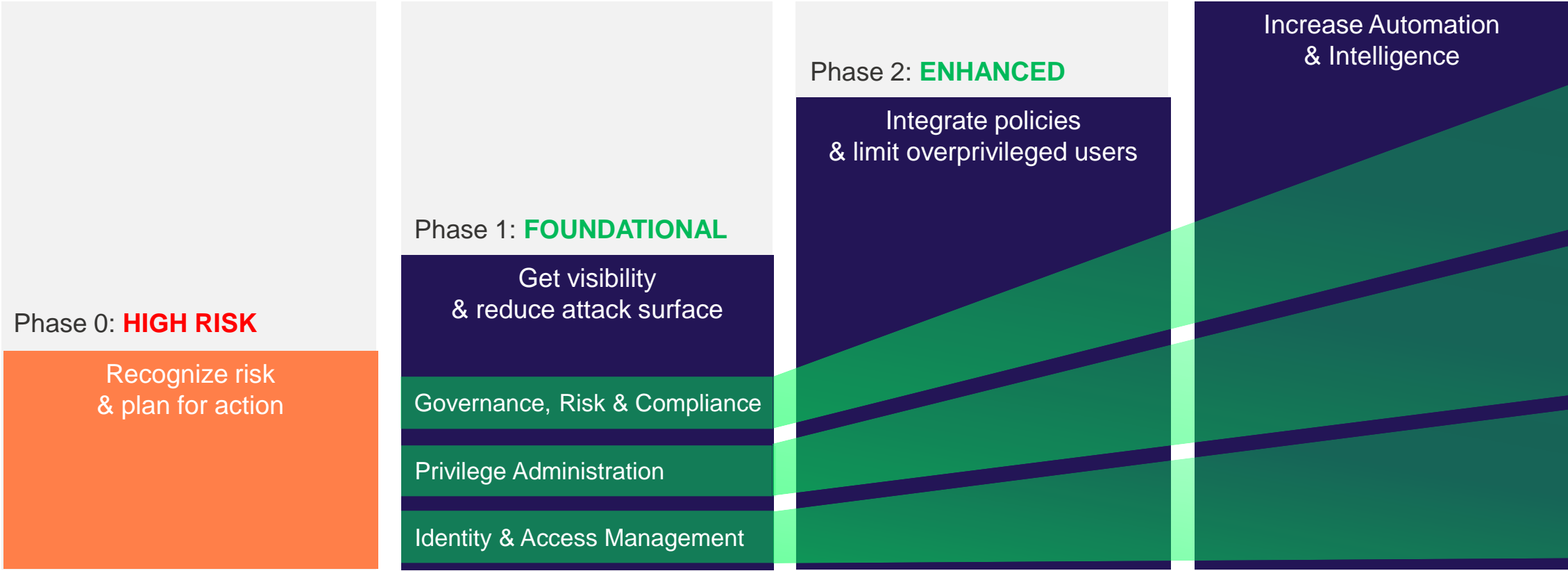
Establish controls over all privileged access to restrict unnecessary lateral movement

Limit privilege escalation by adapting access when and where needed with analytics-informed policies

PRIVILEGE

WORKFORCE IDENTITIES

MACHINE IDENTITIES

Traditional PAM

Extended PAM

The PAM Maturity Model

Phase 3: **ADAPTIVE**

Phase 2: **ENHANCED**

Phase 1: **FOUNDATIONAL**

Phase 0: **HIGH RISK**

Increase Automation & Intelligence

Integrate policies & limit overprivileged users

Get visibility & reduce attack surface

Recognize risk & plan for action

Governance, Risk & Compliance

Privilege Administration

Identity & Access Management

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

Ⅺ DevOps Secrets Vault

Phase 1: FOUNDATIONAL

Get visibility & reduce attack surface

Governance, Risk & Compliance

Privilege Administration

Identity & Access Management

🗄 Secret Server

🖥 Connection Manager

((•)) Remote Access Service

Delinea Platform

Secret Server

Fully-featured
PAM solution available
both on-premises and
in the cloud on the
Delinea Platform
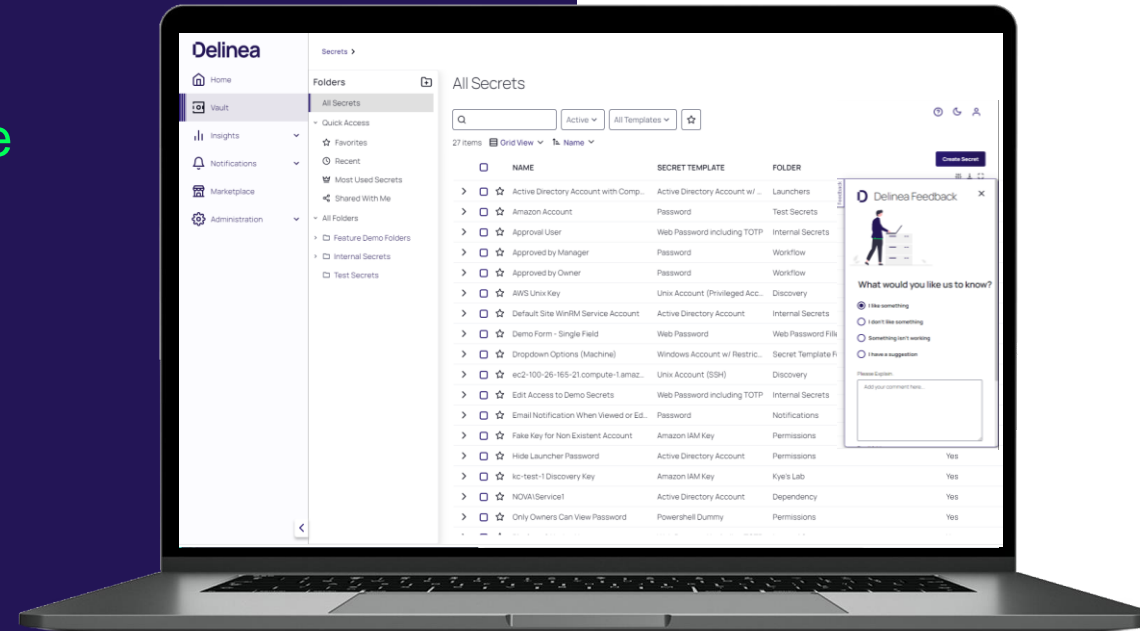
Protect privileged access with an enterprise Vault

Discover and Identify All Accounts

Delegate access with Role-Based Access

Manage secrets with visibility and automation

Control, monitor and record sessions
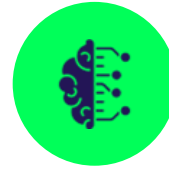
Improve resiliency and business continuity

Full connectivity on the Delinea Platform

Protecting privileged account credentials are business critical and required for cyber insurance

Secure credentials with an enterprise grade vault

Mitigate risk with real-time session monitoring and recording

Reduce human error with the automation of complex tasks

Ensure business continuity with HA and disaster recovery

Identify all privileged accounts across your entire infrastructure

Simplify proof of compliance and passing audits

Poll Question

How do you manage privileged accounts and access now?

over 40%

Just over 40% of organizations had an existing Privileged Access Management solution in place that satisfied cyber insurance requirements.

40%

40% needed to purchase additional solutions to meet the cyber insurance demands.

Cyber insurance checklist:

Cyber insurance providers will ask questions that help them determine your risk across your IT infrastructure and organization

Identify: Do you know your risk

Protect: Are you protecting every asset

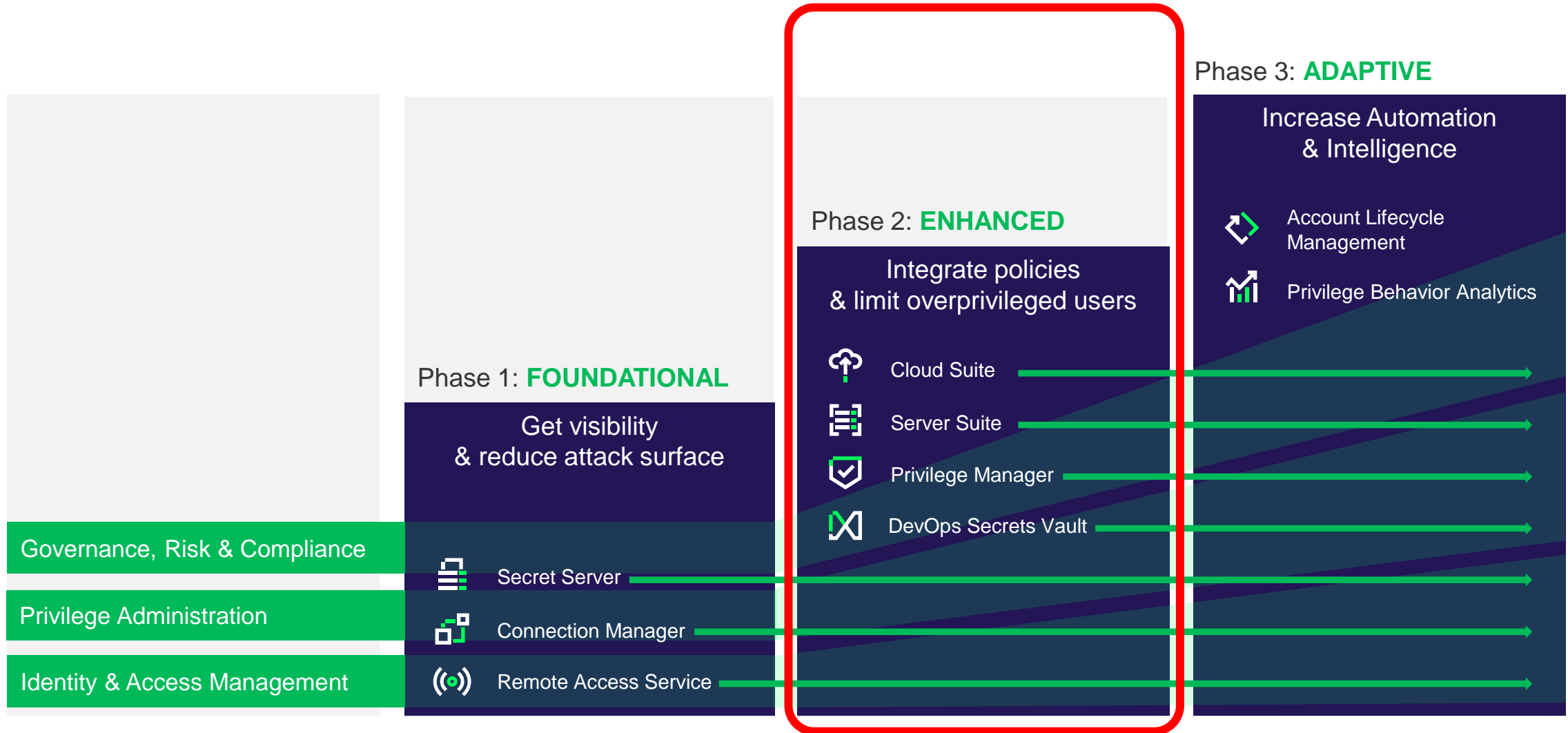**Detect:** What and how are you monitoring to determine anomalies?

Respond: Are you prepared to respond?

Recover: Do you have a plan to recover and repair quickly?

PAM Maturity Model: Phase 2 of the Journey

Governance, Risk & Compliance

Privilege Administration

Identity & Access Management

Phase 1: **FOUNDATIONAL**

Get visibility & reduce attack surface

- Secret Server
- Connection Manager
- Remote Access Service

Phase 2: **ENHANCED**

Integrate policies & limit overprivileged users

- Cloud Suite
- Server Suite
- Privilege Manager
- DevOps Secrets Vault

Phase 3: **ADAPTIVE**

Increase Automation & Intelligence

- Account Lifecycle Management
- Privilege Behavior Analytics

85%

of cyberattacks start with a compromised endpoint

Source: SANS Institute

Privilege Manager

Top Use Cases

Rise of Ransomware and Malware	Cyber Insurance and Compliance	Operational Efficiency and Productivity	Changes in Workforce
by 435% YoY	rose 96% in 2021	75% security failure - by inadequate identities privilege management	95% cyber breaches caused by human

Source: Help Net Security 2022

Source: Marsh 2022

Sources: Gartner 2022

Sources: World Economic Forum 2022

Endpoint Challenges?

Managing local admin & application privileges

Different users w/different permissions & security policies

Regulatory mandates to implement least privilege approach

Benefits of Delinea Privilege Manager

Control Applications

Ensure users can only install and execute approved applications

Implement Least Privilege

Create an environment where users can perform their job role without admin rights

Improve Productivity

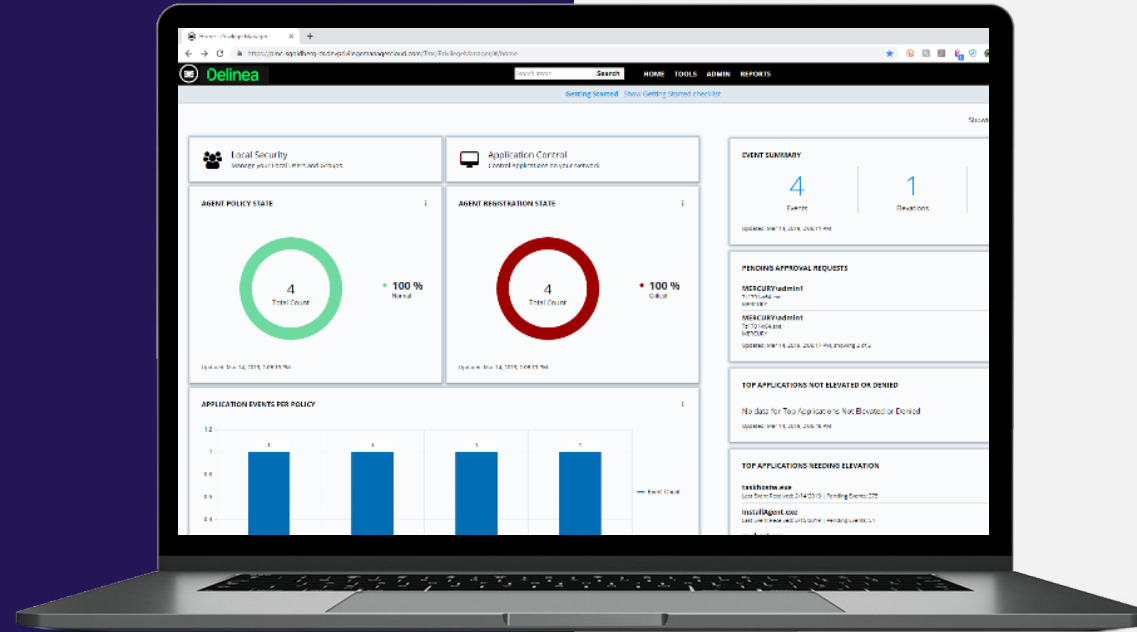Ensure users and support staff are productive and efficient

Prove Compliance

Deliver reporting including event logging and user activity auditing

Privilege Manager

Implement and enforce least privilege policies for Windows and Mac

Deploy agents

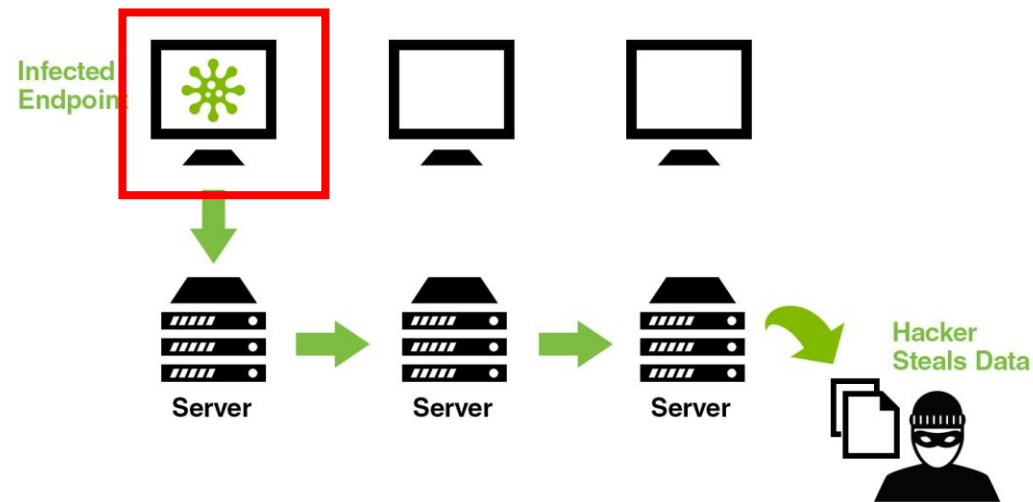**Manage accounts**

Define policies

Elevate applications

Improve productivity

Elevating Privileges via Local Administrators

Threat agents can leverage credentials to move laterally throughout your network to reach sensitive data.

Infected Endpoint

Server   Server   Server   Hacker Steals Data

Local Admin Can:
- Bypass security settings
- Install Software
- Clear logs
- Add Remote Printers
- Run exploit code
- Change Wifi Settings

Most Attacks don't start on a server

The Delinea Platform

OBSERVE

End-to-End Visibility
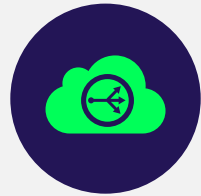
CONTROL

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.

Grazie !

Delinea
Defining the boundaries of access

Nicola D'Ottavio
Partner Alliance Manager – Italy & Med
+39 345 2158928
nicola.dottavio@delinea.com