

# Securing Identities at Every Interaction

Jan Maas, Enterprise Account Manager  
Peter Kirst, Principal Systems Engineer

# Delinea's expanding portfolio

## Delinea Platform

### Secure Credentials

Identify & Vault Secrets



Vaulting



Machine Secrets



Service Accounts

### Privileged Remote Access

VPN-less Remote Access



Secure Remote Access



Vendor PAM

### Privilege & Entitlement Elevation

Granular Real-time Controls



Servers



Workstations



Cloud

### Identity Governance & Access Controls



Identity Lifecycle



Access Review



Auditing & Analytics



Segregation of Duties

### Identity Protection

Discover Identity Vulnerabilities, Misconfigurations, and Over-privileged Users

Detect Identity-based Breaches

Remediate

### Shared Capabilities

Continuous Discovery

Audit and Analytics

AI

MFA

Ecosystem



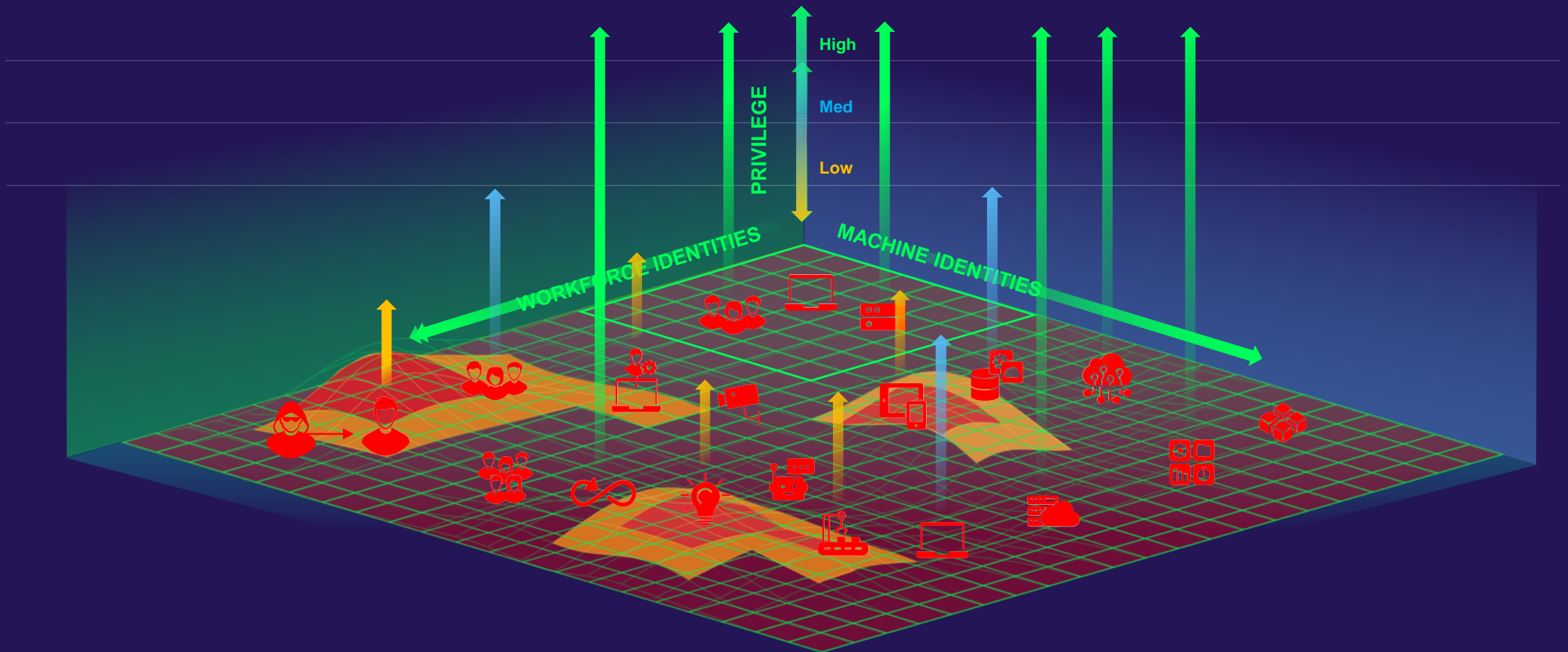
# Paradigm Change

Pure PAM **vs.** JIT / JEP / ZSP

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





# Zero Standing Privilege / JIT / JEP

# Known Challenges

- Too many brokered accounts
- Heavy infrastructure
- Personalized recording and auditing tricky
- Accounts with long lasting high privileges

# Desired Outcome

- Minimized number of long lasting high privilege accounts
- Flexible and lightweight infrastructure in order to adopt quickly on changes and new requirements
- Full reporting of personal usage and easy auditing
- Less Accounts in the system
- NIS2 compliance

# NIS2 requirements in real live

## Cybersecurity/hygiene requirements and further adoption of technology

NIS2 points out the importance of cyber hygiene as the foundation for protecting network and information system infrastructure, hardware, software, application security, and business and personal data. Implementation of cyber hygiene policies by the EU countries will be monitored and analysed by ENISA. Requirements include:

- Password changes
  - Limitation of admin-level access accounts
  - Identity and access management
  - Software and hardware updates
  - Management of new installs
  - Backing-up data
- Zero Trust principles
  - A proactive framework of preparedness and overall safety and security in the event of incidents or cyber threats
  - Companies should also have an active training policy to raise security awareness among the employees

The European Commission advises companies to adopt AI and machine learning systems to further enhance security capabilities. It sees these technologies as tools to enable better detection and prevention of cyberattacks.



# Driving Towards Zero Standing Privilege

For many years the standard approach to securing privileged accounts and access has been through the use of a Vault solution such as Delinea Secret Server.

Vaults will continue to be a requirement to manage break-glass privileged accounts, however Zero Standing Privilege frameworks allow for a continuous, dynamic elevation and de-elevation processes to be added to the target environment. This leads to a reduced privileged attack surface and greatly enhances organizational privilege security.

This document outlines Delinda's recommended approaches to achieving a Zero Standing Privilege Model.

## Core Terminology

The following terms are widely used within this document:

- **Zero Standing Privilege (ZSP):** The model or process aimed at removing static privileges attached to accounts and replacing with automatic elevation and de-elevation of privileges.
- **Just in Time (JIT) Elevation:** The process of attaching elevated privileges to accounts for the specific time period that they are required.
- **Just Enough Privilege (JEP):** A least privilege framework for ensuring that only the privileges specifically required for a user's job role are attached to an account for the JIT window.

# Privilege is Necessary

**Scope**  
Just Enough Access

- What systems or applications can the user access?
- How Much Privilege does the user or application require in order to perform its function?

**Time**  
Just in Time

- When do they need the privilege?
- How long do they need it for?

Why is ZSP / JIT / JEP important?

1

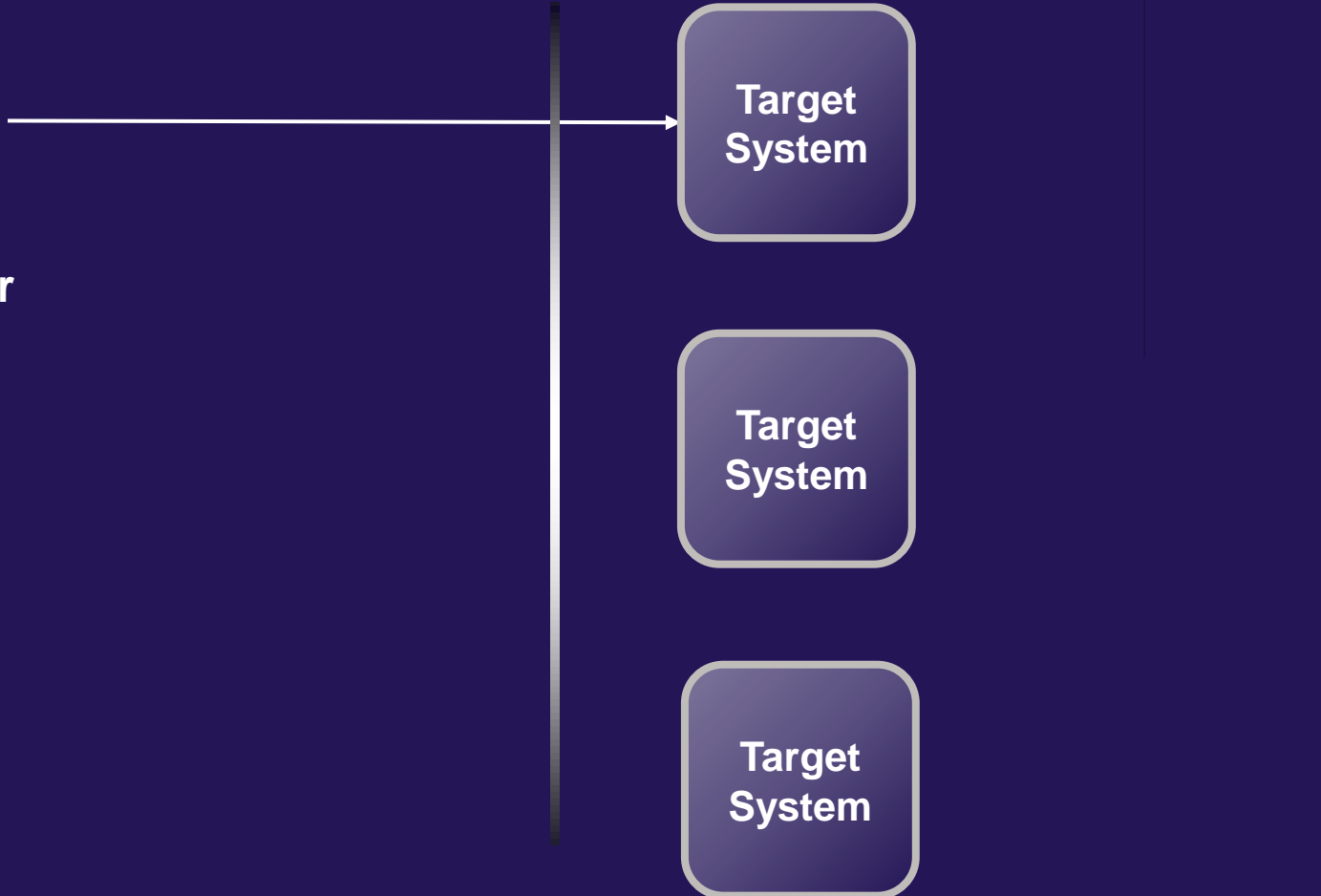
## Before Delinea Vault

Privilege User Accesses a target system – this is not protected



**Privileged User**

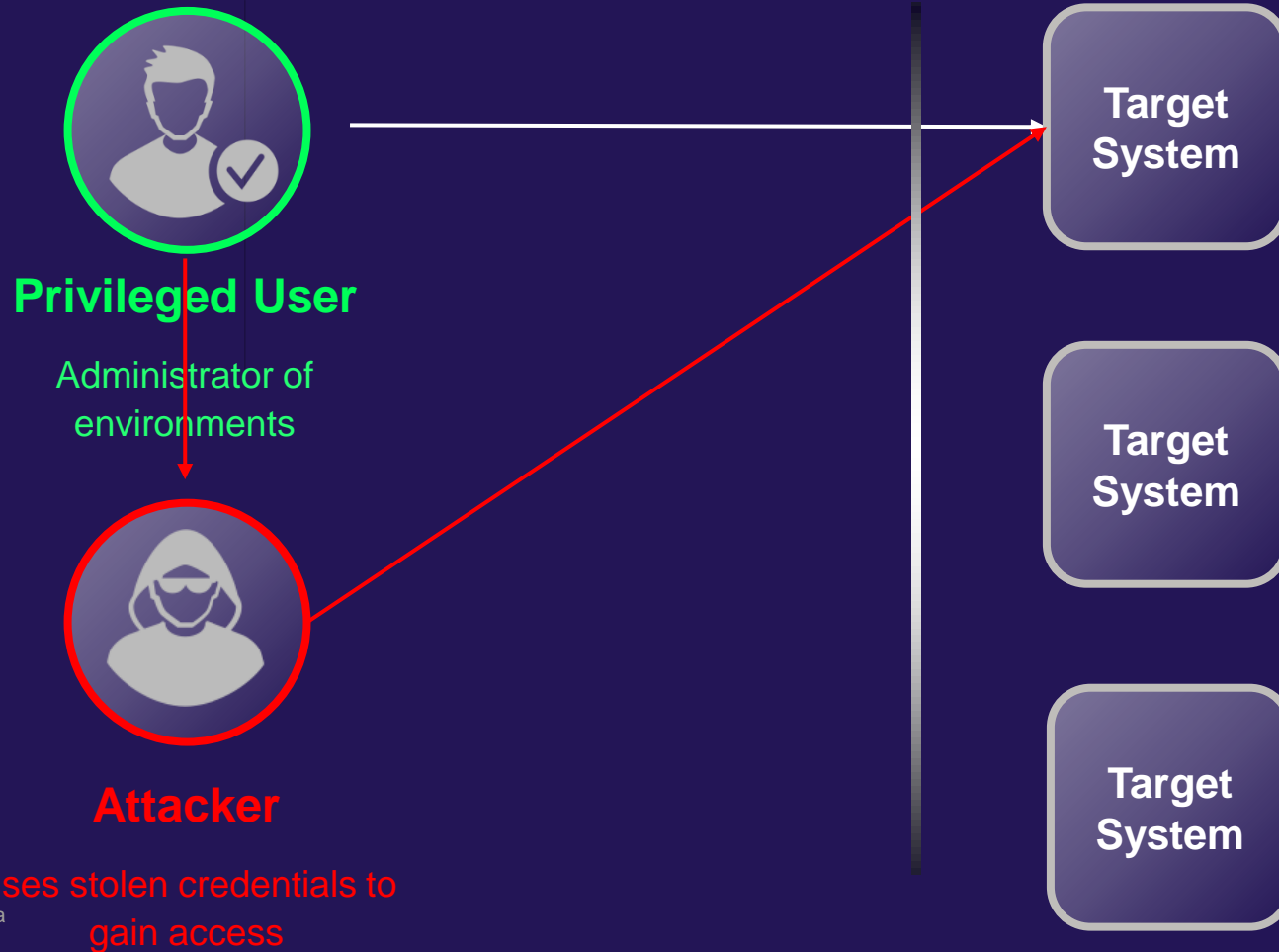
Administrator of environments



1

## Problem: Attacker steals credentials

Through fishing or other means attacker has credentials



1

## Vaulted Access

First Step is providing significant advancement



**Privileged User**

Administrator of environments



**Attacker**

Bad actor switches strategies

1

### Vaulted Access

First Step is providing significant advancement

2

### Problem: Lateral Movement

The target cannot protect itself!



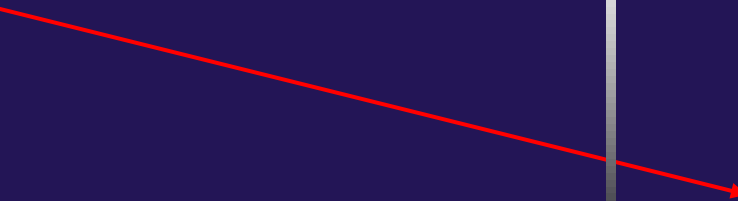
**Privileged User**

Administrator of environments



**Attacker**

Bad actor switches strategies



1

## Vaulted Access

First Step is providing significant advancement



**Privileged User**

Administrator of environments



2

## Problem: Lateral Movement

The target cannot protect itself!



**Attacker**

Bad actor switches strategies

1

### Vaulted Access

First Step is providing significant advancement



**Privileged User**

Administrator of environments



2

### Lateral Movement

Server PAM Installed, Problem Solved!



Server PAM Agent Installed



Outcomes:

- MFA Assurance
- Protects against lateral movement attacks
- Tie activities to users



**Attacker**

Bad actor switches strategies

1

### Vaulted Access

First Step is providing significant advancement



**Privileged User**

Administrator of environments



2

### Lateral Movement

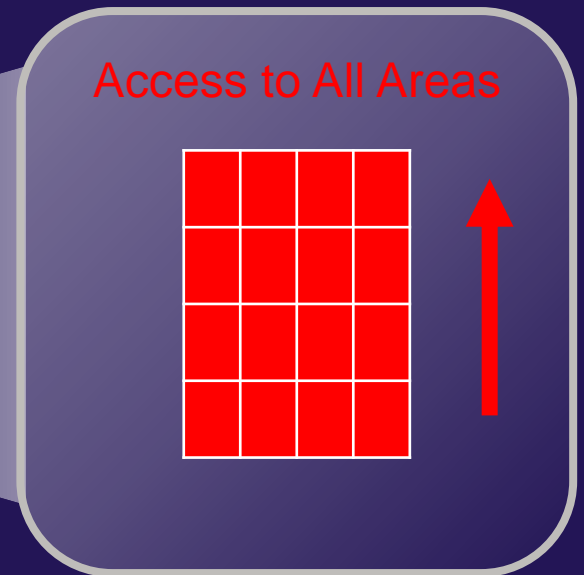
Protection for the movement **across** systems



3

### Problem: Administrator Access Is Broad

Admins and attackers with admin access can perform any function



**Attacker**

Bad actor

1

### Vaulted Access

First Step is providing significant advancement

2

### Lateral Movement

Protection for the movement **across** systems

3

### Privilege Elevation

Protection **within** systems



**Privileged User**

Administrator of environments



**Attacker**

Bad actor



*Outcome: Proactive Risk Reduction*

Configuration locked

Time and # of Privileges Based

*Limit Activities and 24x7 AI-driven Audit*



# Delinea Privilege Control for Servers PCS

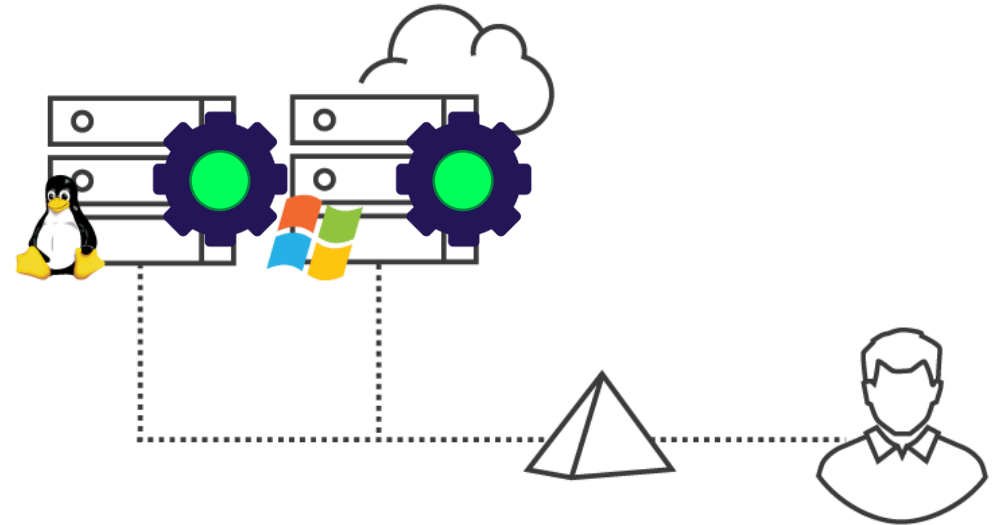
Authentication, Privileged Elevation, Host Auditing Services



# Privilege Elevation Service

# Privilege Elevation

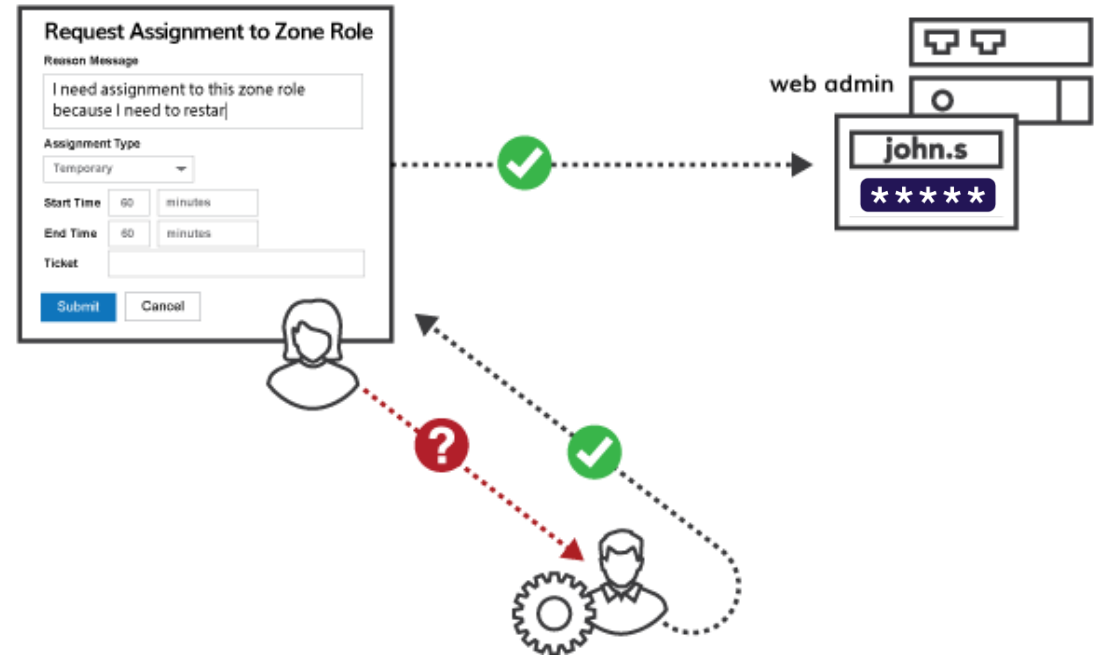
- Manage privilege w/out sharing passwords
- Grant just enough privilege based on role within an organization
- Cross-platform least privilege for Windows and Unix/Linux
- Command-level granularity w/ privileged workspaces
- Hierarchical policy model consistent for both Windows and UNIX/Linux
- Powerful automation tools
  - Sudo import wizard
  - Application rights builder
  - PowerShell cmdlets & Unix CLI



Limit damage inflicted by malicious insiders  
and external attackers

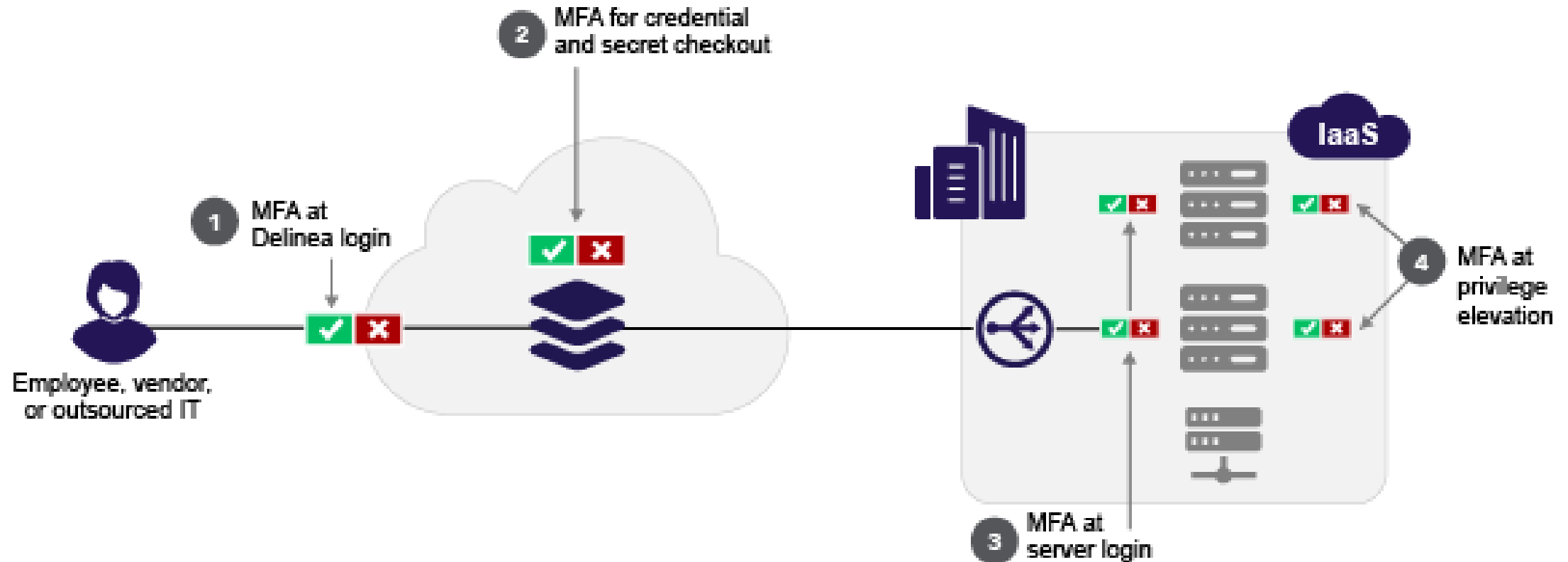
# Time-Based Role Assignment

- Self-Service role requests for Just-In-Time privilege
- Time-Bound privileged access
- Privilege elevation request via 3<sup>rd</sup>-party solutions



Just-in-time access & elevated privilege

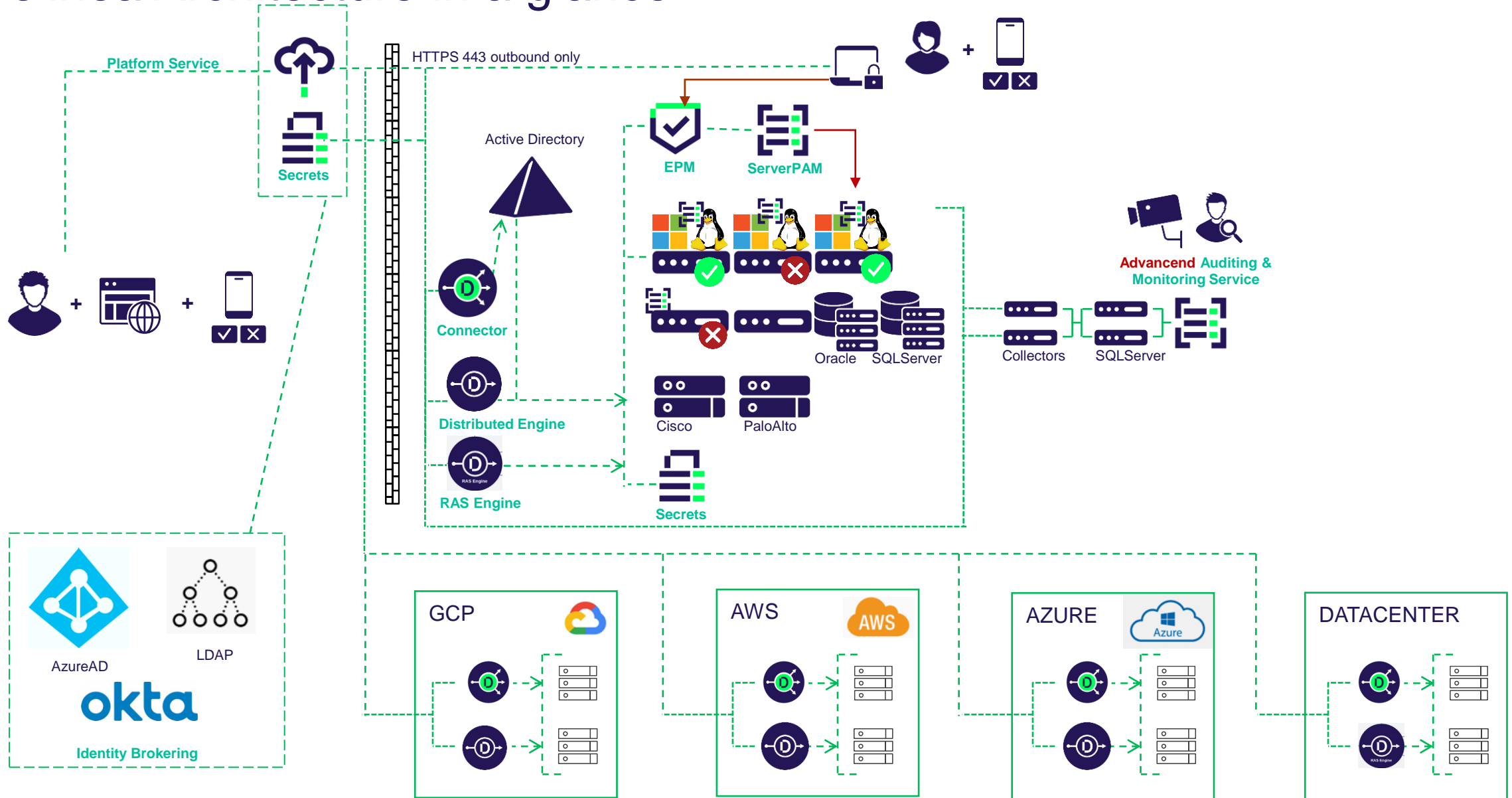
# MFA at Logon and Privilege Elevation





**Delinea Architecture in a glance**

# Delinea Architecture in a glance



Fragen ?



# Thank You.

**Delinea**

Defining the boundaries of access