



Securing IT Admin Identities: Balancing Access, Security, and Productivity in a Hybrid World

Scott Shields

Enterprise Solutions Engineer – Northern Europe, Delinea



The Evolving Security Landscape

The traditional **network perimeter** is **fading** — identity is now the frontline of defense.



The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

- **Cloud** adoption & hybrid work models



The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

- **Cloud** adoption & hybrid work models
- Rise in identity-based **cyber threats**



The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

- **Cloud** adoption & hybrid work models
- Rise in identity-based **cyber threats**
- Stricter **compliance** & regulatory mandates



The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

- **Cloud** adoption & hybrid work models
- Rise in identity-based **cyber threats**
- Stricter **compliance** & regulatory mandates
- **Zero Trust** frameworks reshaping security strategies



The Evolving Security Landscape

The traditional **network perimeter** is fading — identity is now the frontline of defense.

What is driving the shift?

- **Cloud** adoption & hybrid work models
- Rise in identity-based **cyber threats**
- Stricter **compliance** & regulatory mandates
- **Zero Trust** frameworks reshaping security strategies



Organisations must rethink their approach to secure access in a perimeter-less world.

Organisations face different challenges across identities



IT Admin

Inability to consistently discover privileged IT users and manage their access needs



Workforce

Lack of visibility into employee access, especially across remote and hybrid workers



Non-Human

Overwhelming number of non-human to human identities, dynamically created and deleted all the time



Developer

Velocity required by the business results in workarounds anytime the dev experience is less than frictionless

Organizations face different challenges across identities



IT Admin

Daily work requires privileges

Unchecked privilege sprawl widens the attack surface
...vs evolving cyber threats

Maintain legacy systems while handling digital transformation

Balance productivity with security and usability

Manage access across diverse platforms

Compliance requirements more granular



Organisations face different challenges across identities



Workforce

Lack of visibility to employee access and misconfigurations

Sprawling workforce credentials without centralized visibility

Lack of administrative control over workstations

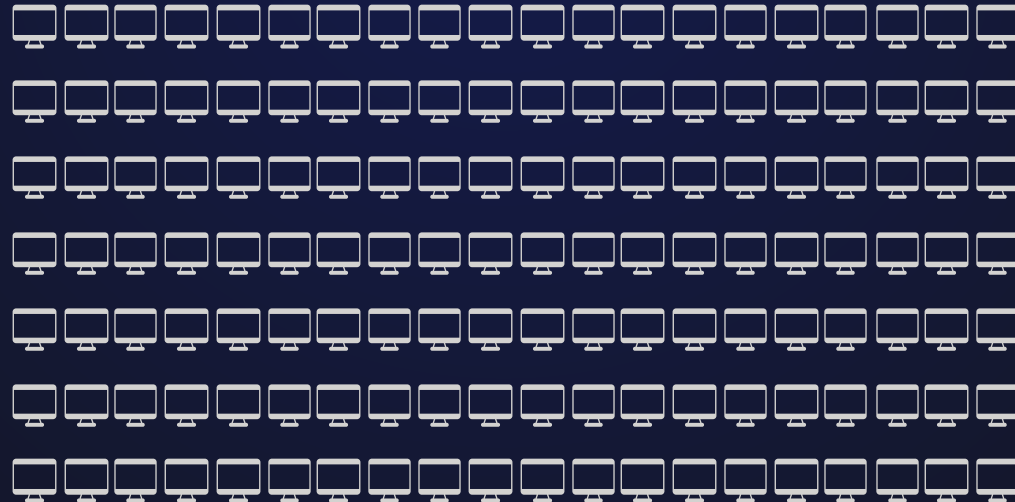
Lack of monitoring into sensitive workforce user sessions

Orphaned accounts and privilege creep among employees

Organisations face different challenges across identities



Non-human: 20x?



Organisations face different challenges across identities



Non-human

Massive quantities of NHI

Widely spread and often overly permissive

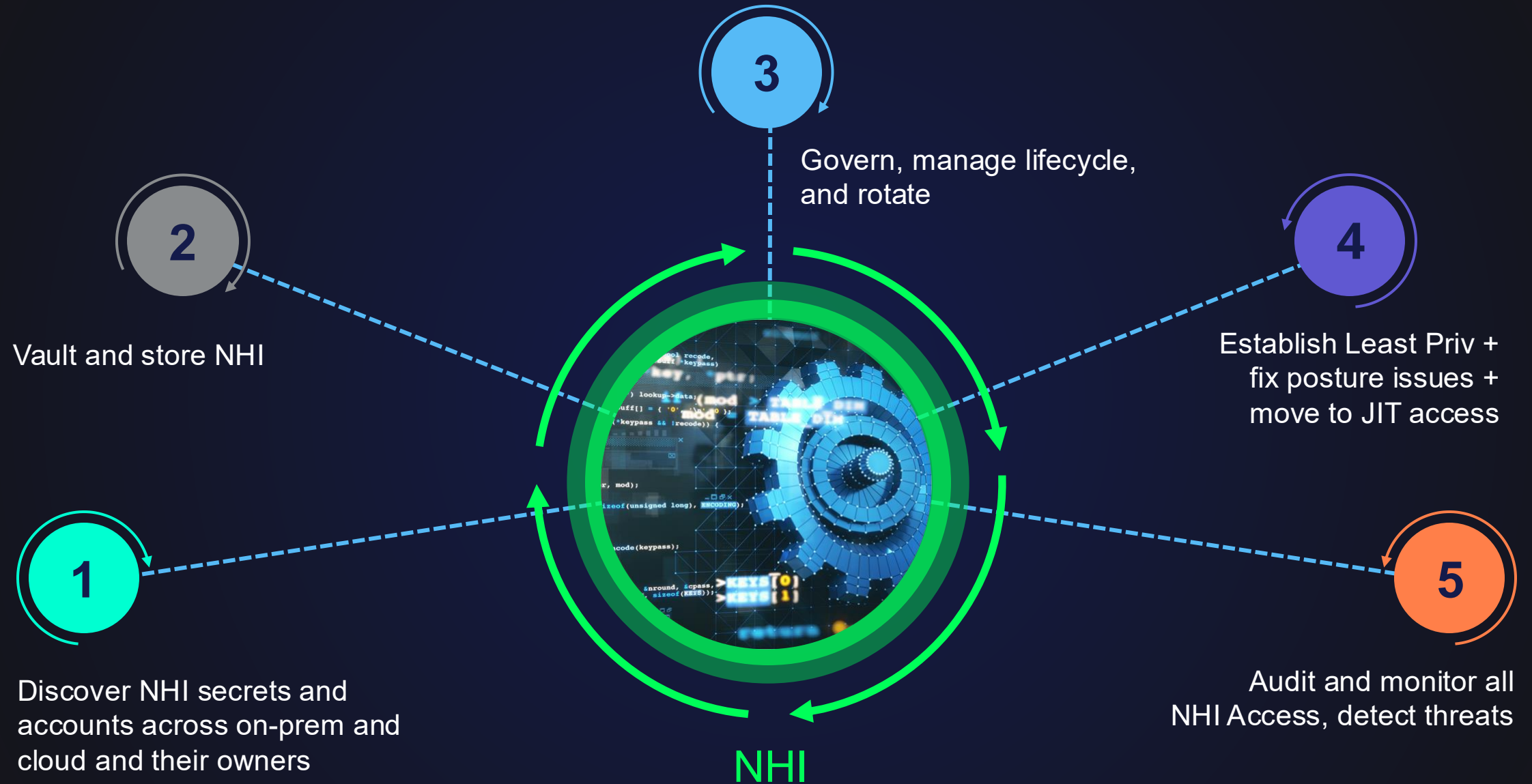
Unknown ownership

Ripe target for attack

Inconsistent governance and compliance

AI introduces even more problems

NHI Customer Use Cases



Beyond Vaulting? The
evolving landscape...

1

Before Delinea Vault

Privilege User Accesses a target system –
this is not protected



Privileged User

Administrator of
environments



Target
System

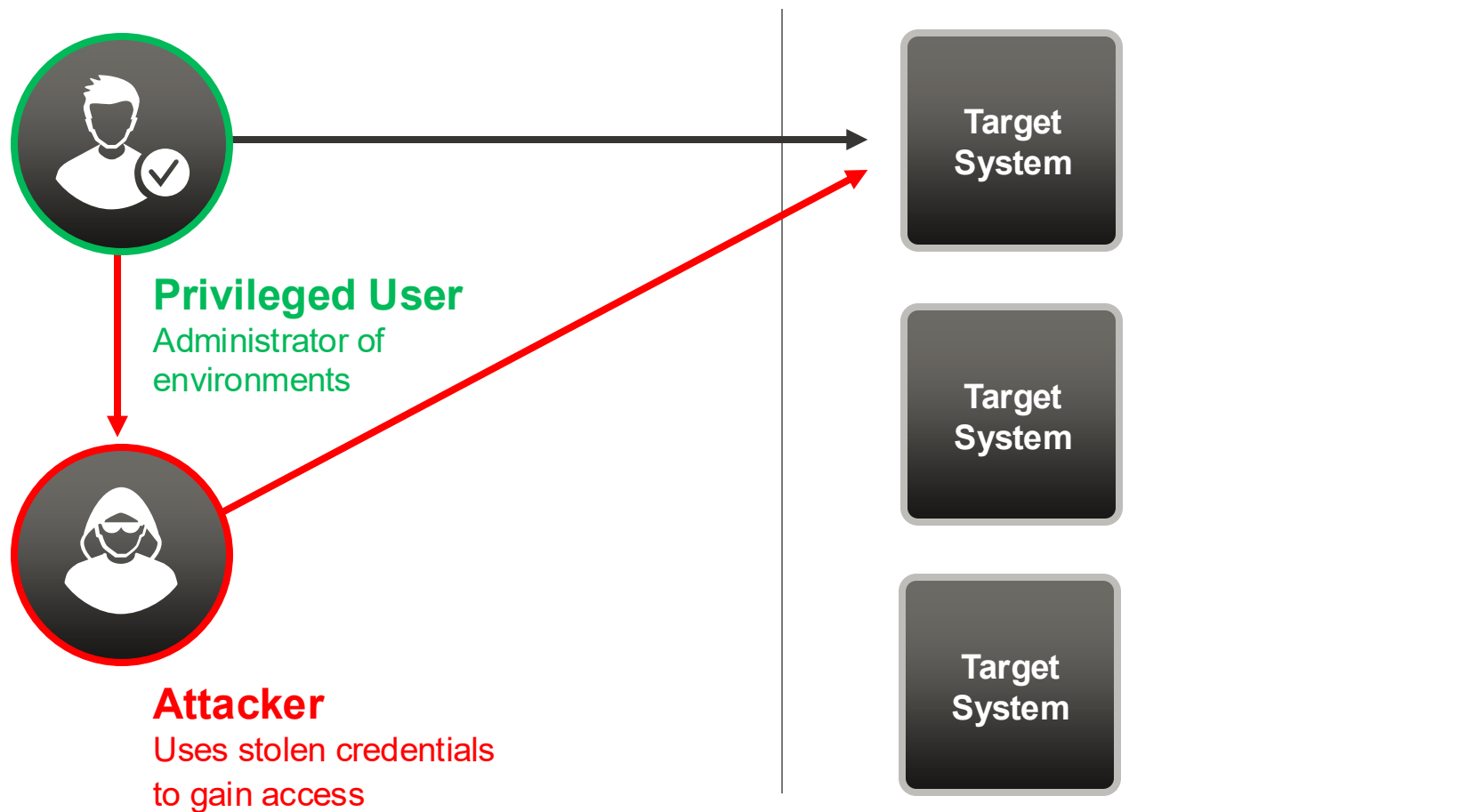
Target
System

Target
System

1

Problem: Attacker steals credentials

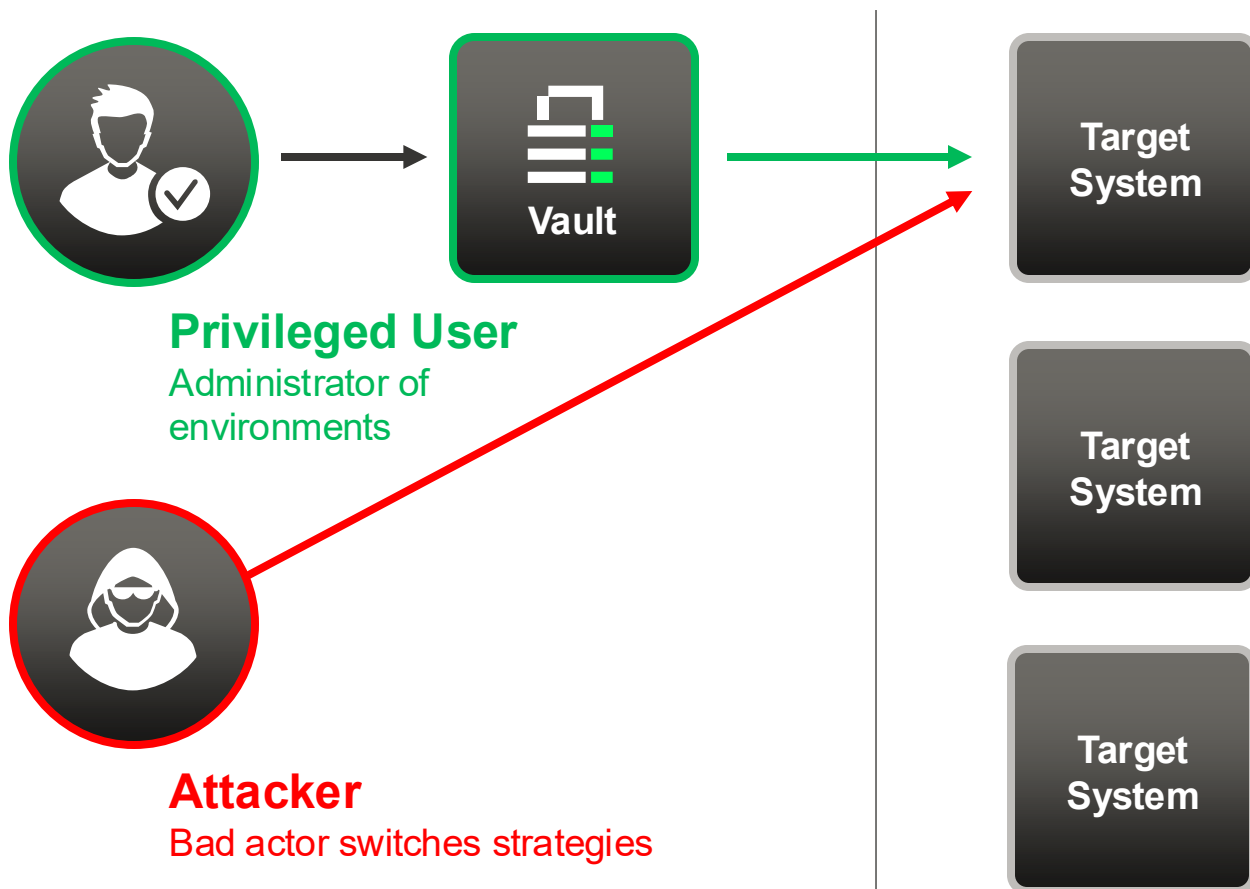
Through fishing or other means, attacker has credentials



1

Vaulted Access

First Step is providing significant advancement



1

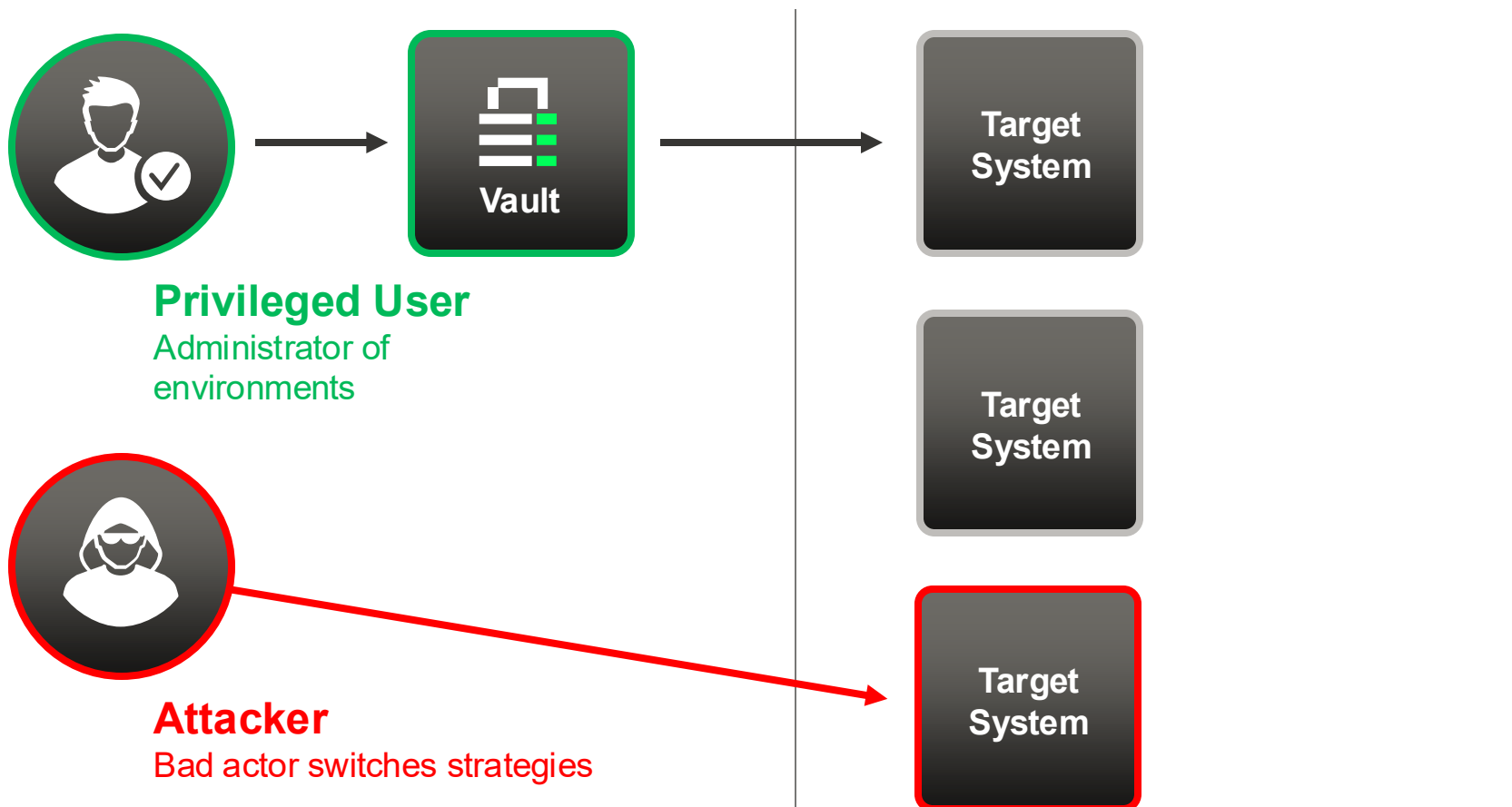
Vaulted Access

First Step is providing significant advancement

2

Problem: Lateral Movement

The target cannot protect itself!



1

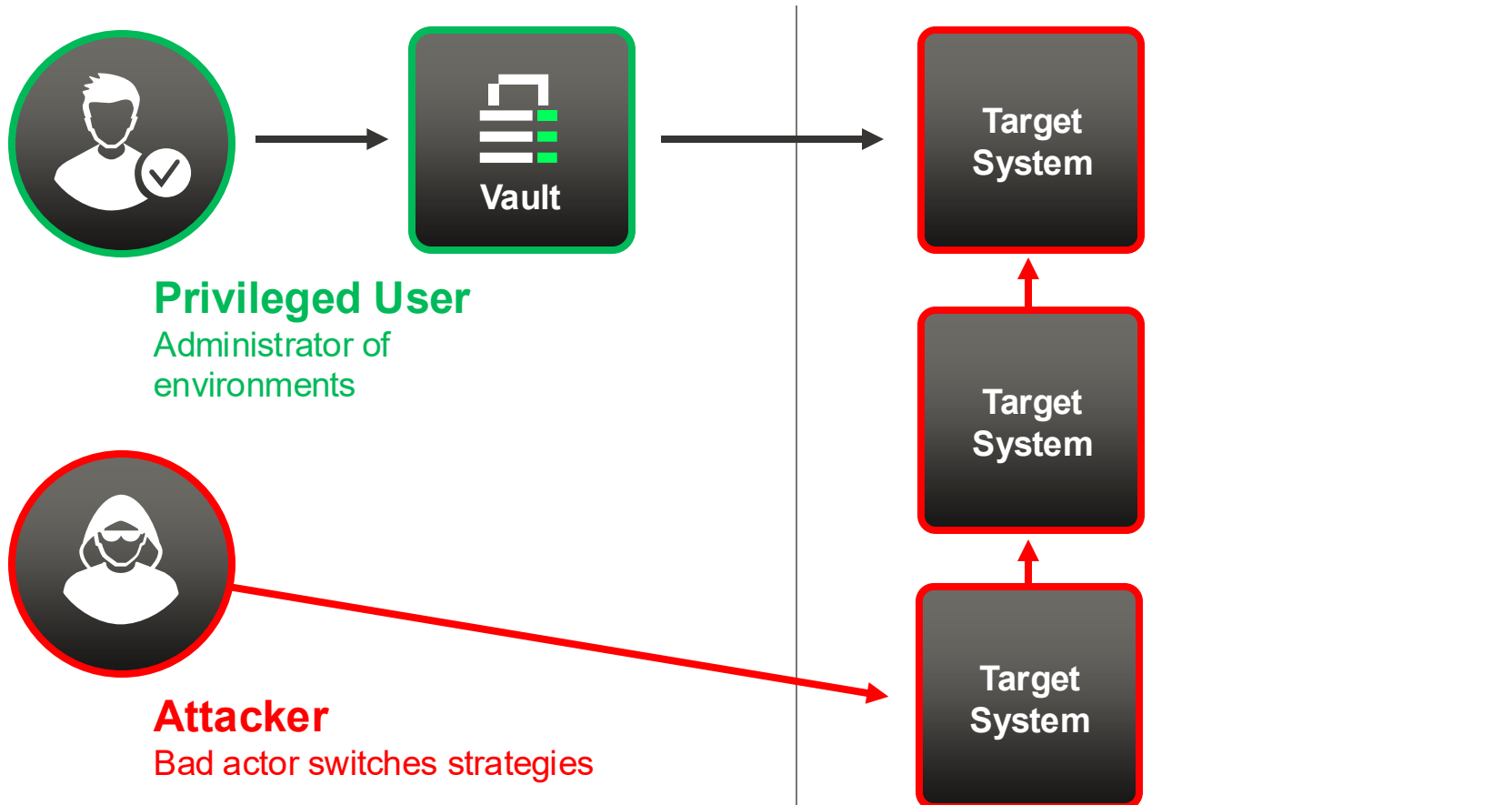
Vaulted Access

First Step is providing significant advancement

2

Problem: Lateral Movement

The target cannot protect itself!



1

Vaulted Access

First Step is providing significant advancement



Privileged User

Administrator of environments



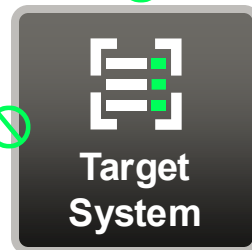
2

Lateral Movement

PCS Installed,
Problem Solved!



PCS 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

2

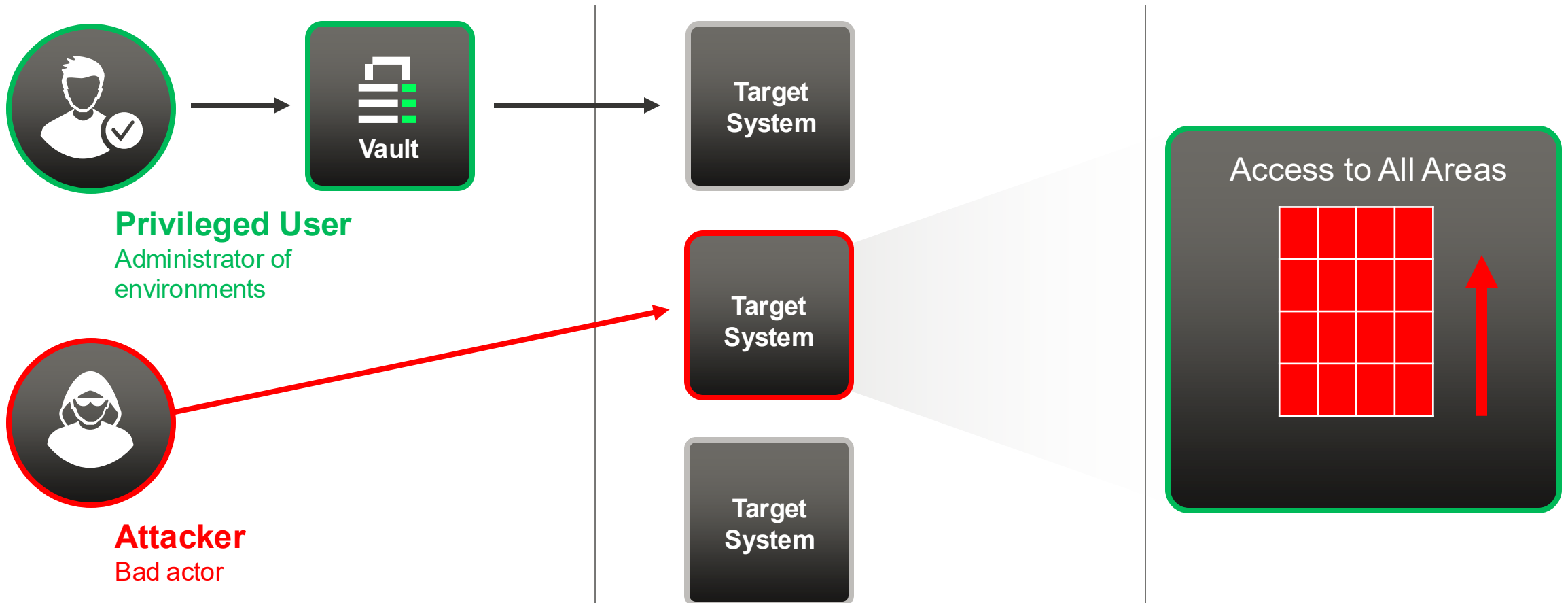
Lateral Movement

Protection for the movement **across** systems

3

Problem: Administrator Access Is Broad

Admins and attackers with admin access can perform any function



1

Vaulted Access

First Step is providing significant advancement



Privileged User

Administrator of environments



Vault

2

Lateral Movement

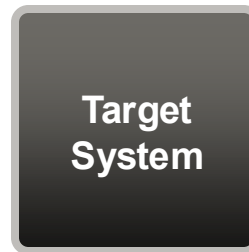
Protection for the movement **across** systems



Target System



Target System



Target System

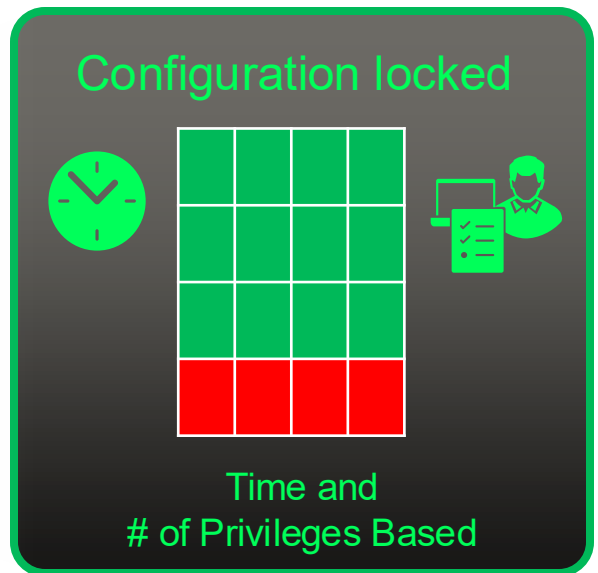
3

Privilege Elevation

Protection **within** systems

Outcome:

Proactive Risk Reduction



Limit Activities and 24x7 AI-driven Audit

Summary Differentiation

1

Cloud Native
Vaulted Access



Privileged User
Administrator of
environments



2

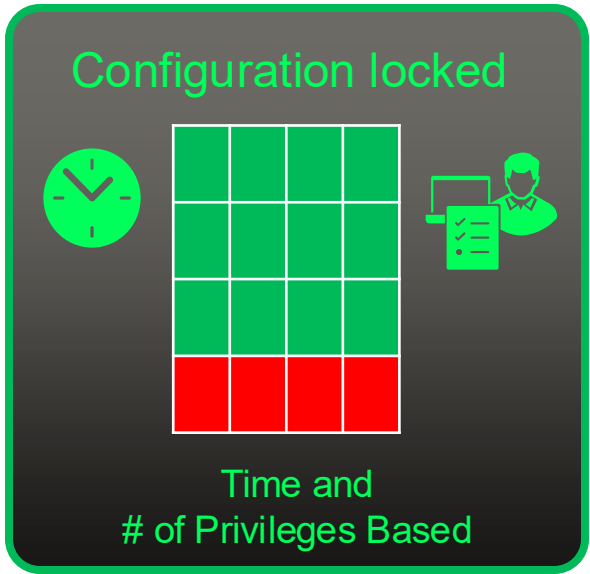
Prevent Lateral
Movement

PCS Agent
Installed



3

Best-in-Class
Privilege Elevation



The Role of Privileged Access Management

Securing the keys to the kingdom

Privileged Accounts: A Prime Target for Attackers

Privileged accounts grant **high-level access to critical systems**, making them a prime target for cyberattacks, credential theft, and insider threats..

The Hidden Danger of Privilege Sprawl

Excessive permissions create risk—privilege sprawl expands the attack surface.

Regulations Demand Stronger Access Controls

Compliance mandates demand control—NIS2, GDPR, and industry frameworks require secure access management.

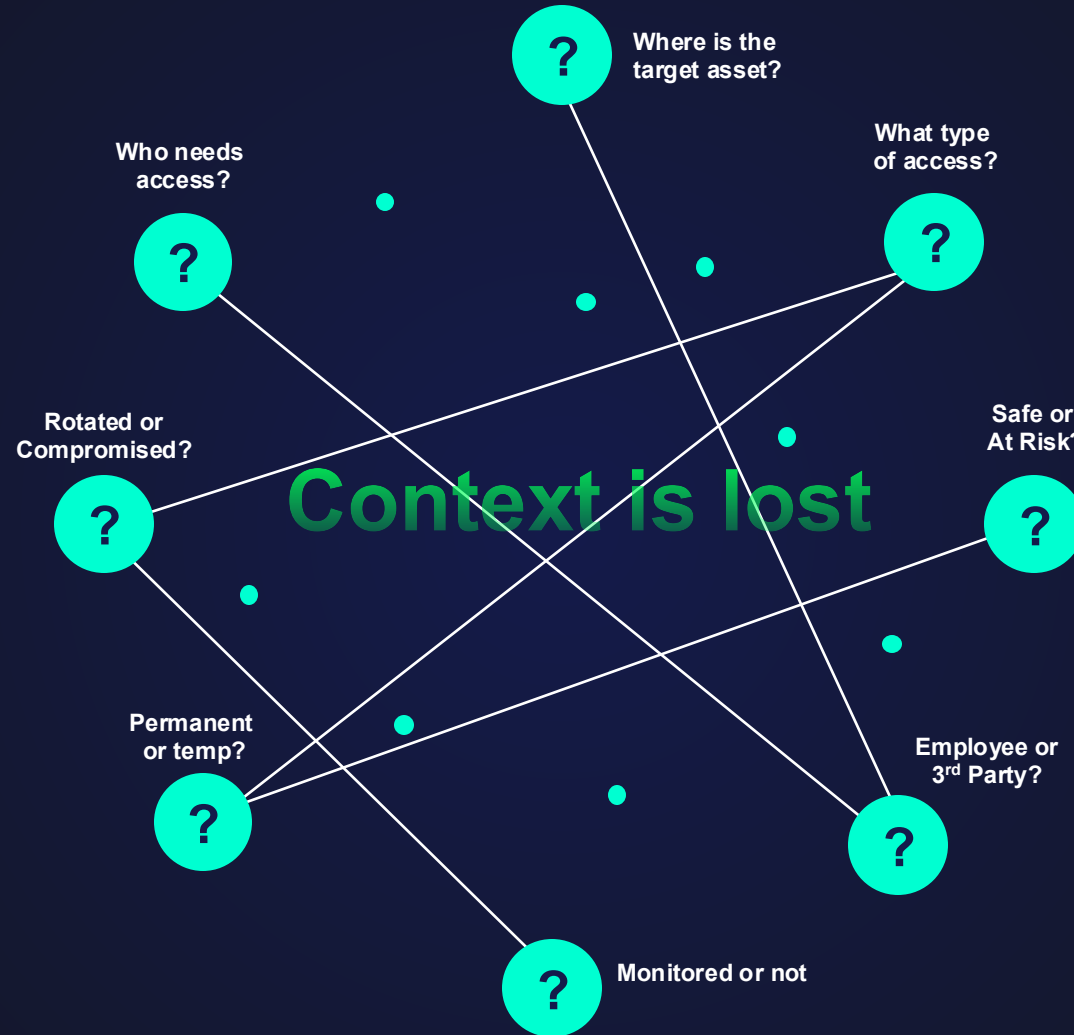
Explosion of identities



Explosion of endpoints



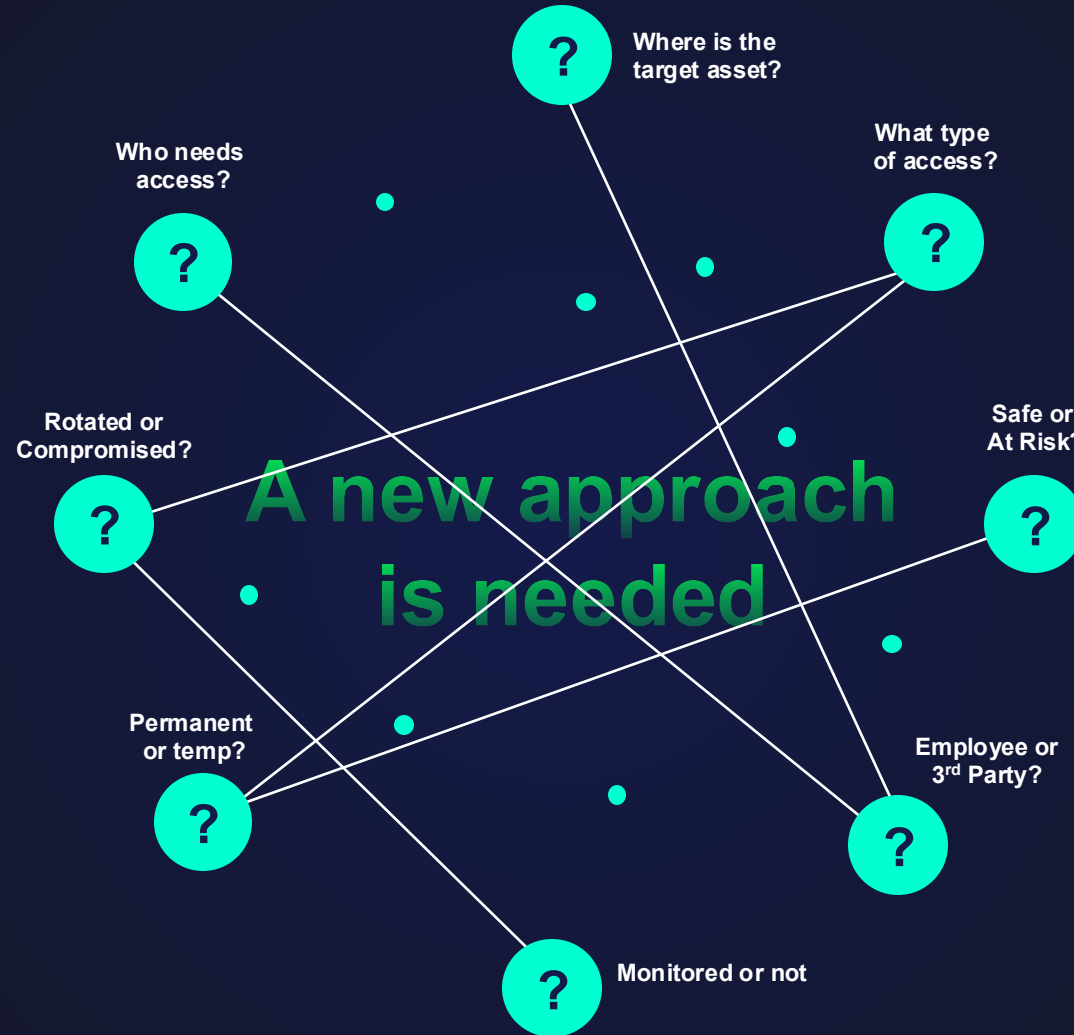
Explosion of identities



Explosion of endpoints



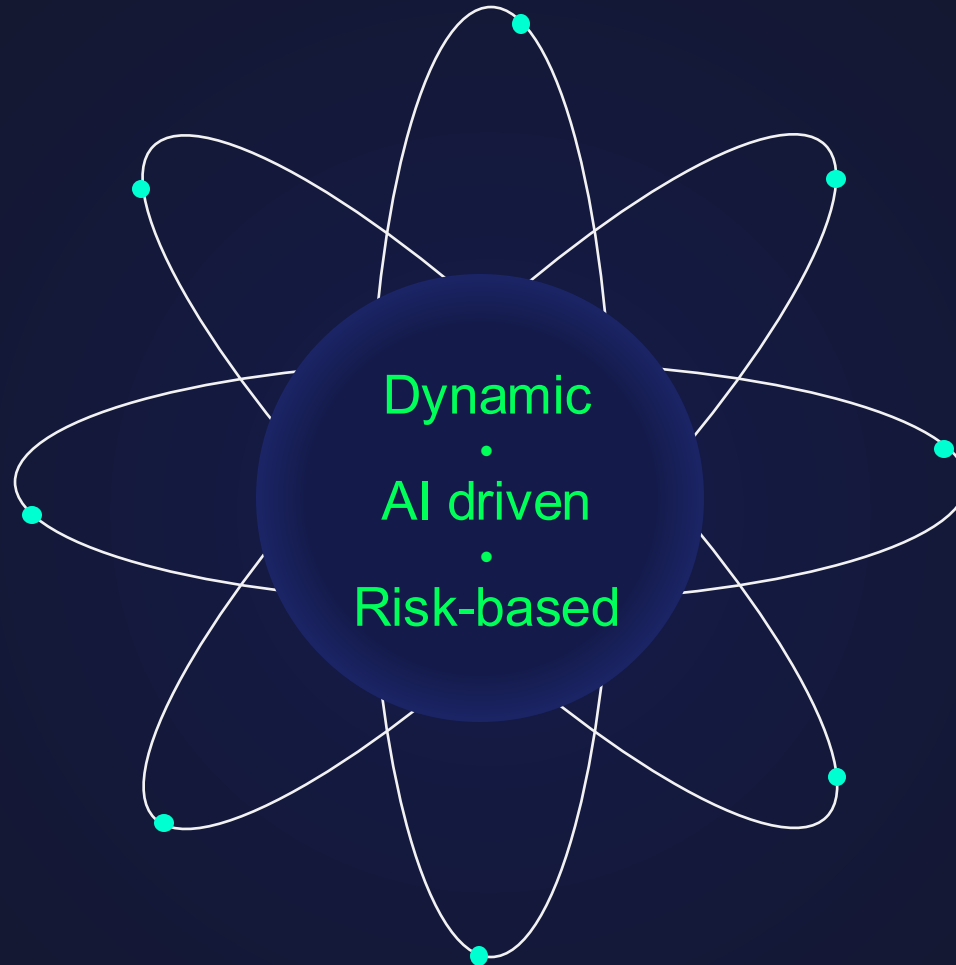
Explosion of identities



Explosion of endpoints



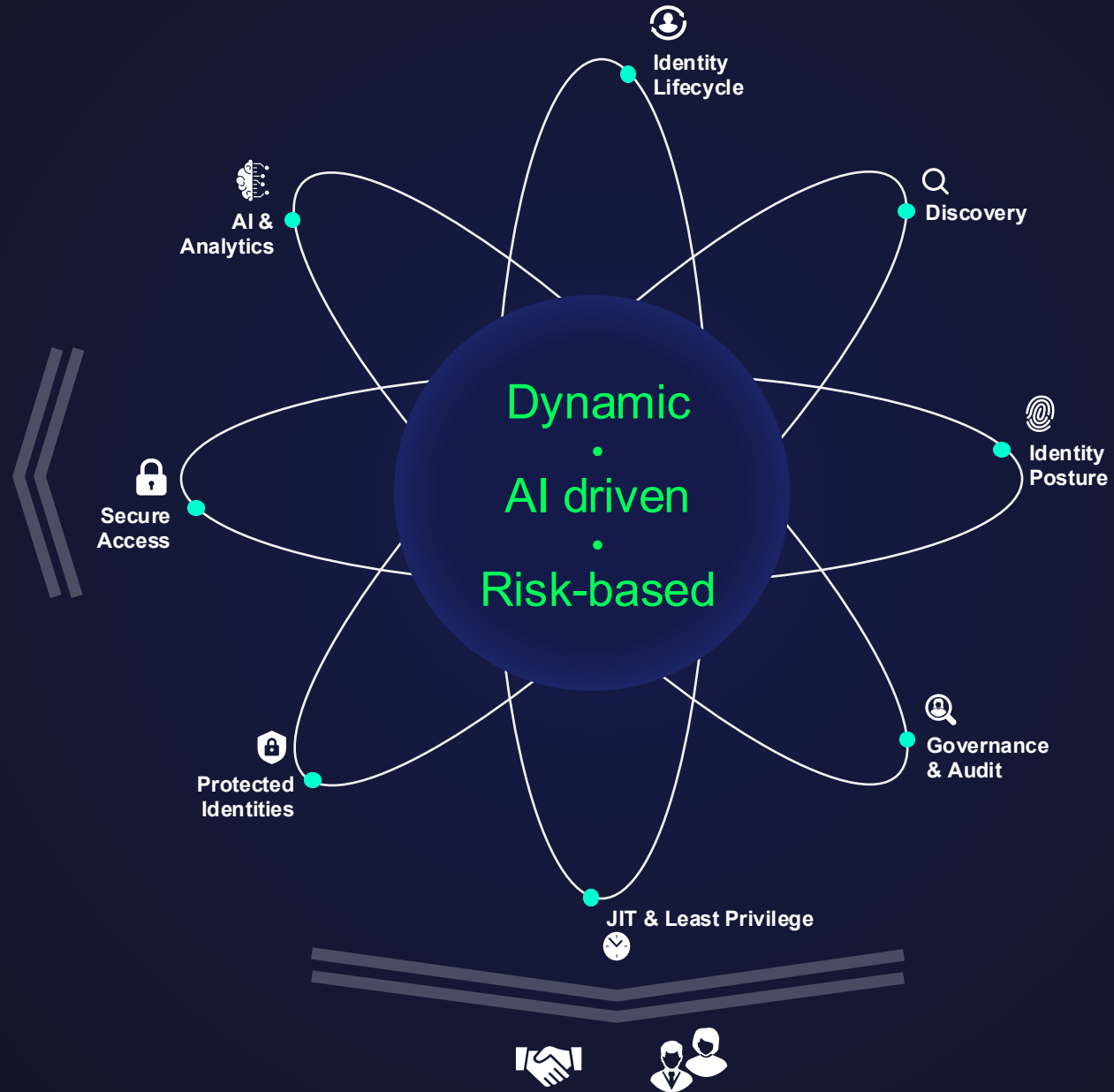
Explosion of identities



Explosion of endpoints



Explosion of identities



Explosion of endpoints

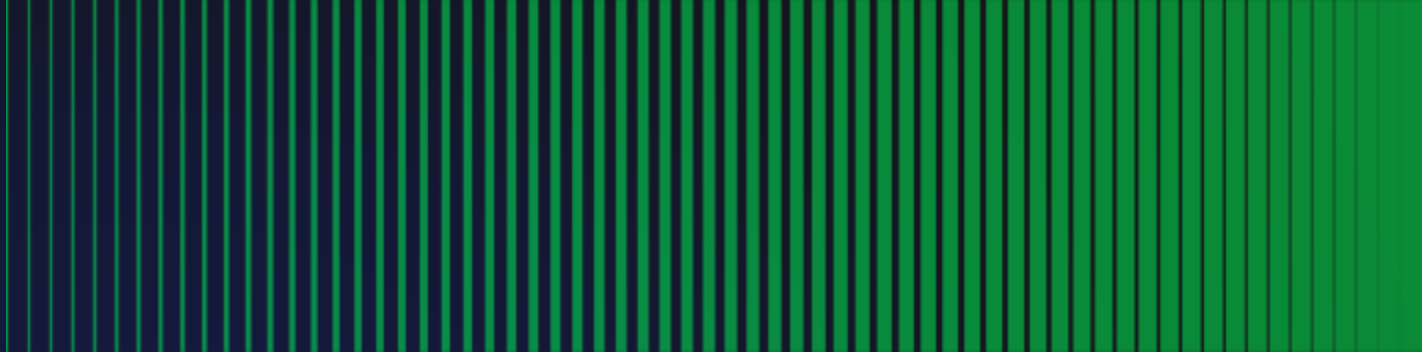


Explosion of identities



Explosion of endpoints



A series of vertical lines in a gradient of green and yellow, located in the top right corner of the slide.

Thank-You.