
ONE IDENTITY™

# Privilegierte Identitäten

Was hat das mit meinem Geschäft zu tun?!

Zoltan Bakos
Externer Berater



ONE IDENTITY™


1 @
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PRS
8 TUV
9 WXY
Anula
Corrige
Entra

# What do these companies have in common?

YAHOO!

500 million Accounts / 2014
3 billion Accounts / Aug 2013

TARGET

110 million Accounts / Nov 2013

ebay

145 million Accounts / May 2014

Aol.

92 million Accounts / 2004

Marriott

500 million Accounts / 2014-2018

JPMORGAN CHASE & CO.

83 million Accounts / July 2014

in

100 million Accounts / June 2012

THE HOME DEPOT

53 million Accounts / April 2014

facebook

+550 million Accounts / 2017-2019

UNDER ARMOUR

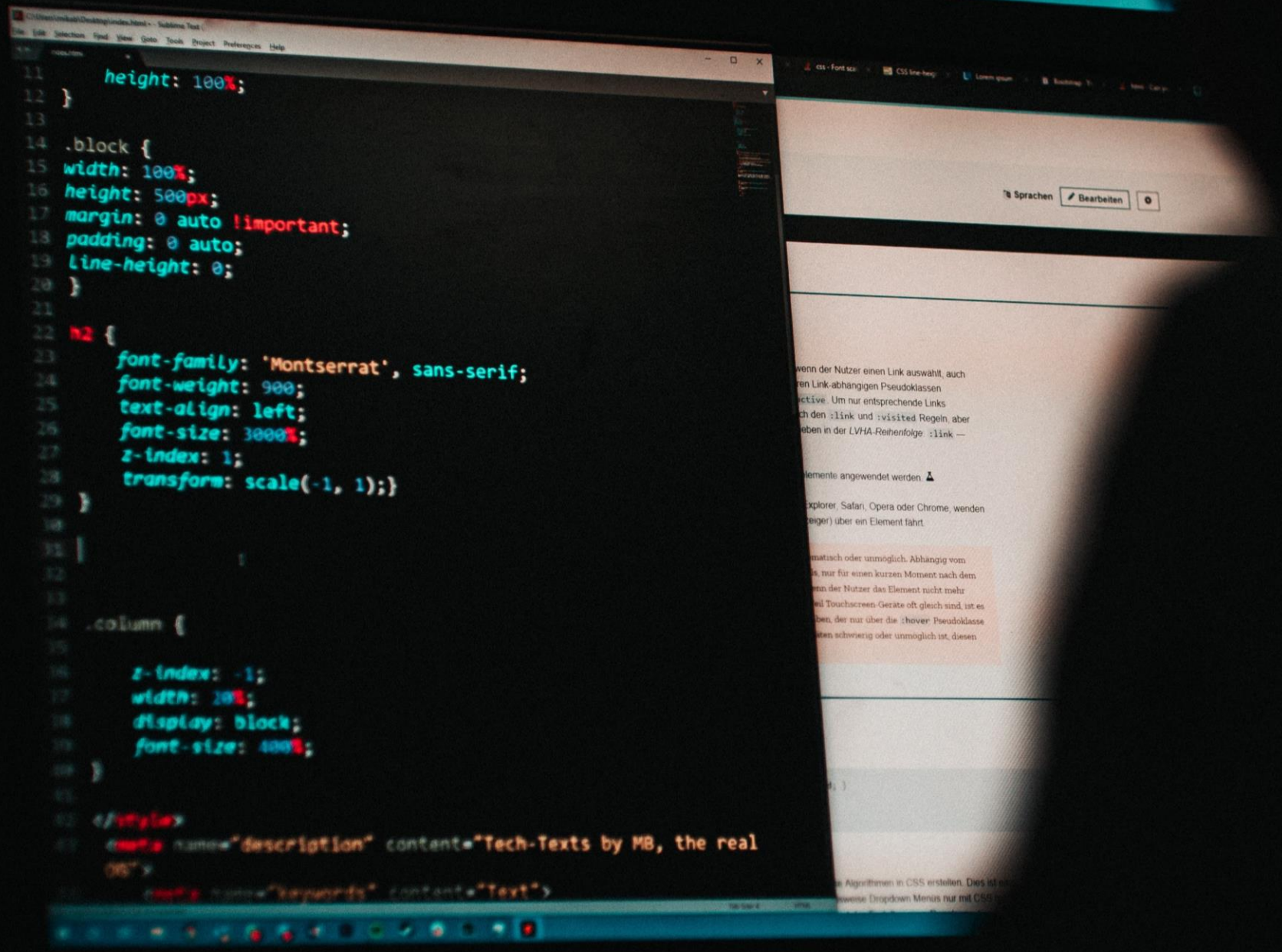
150 million Accounts / Feb 2018

UBER

57 million Accounts / Late 2016

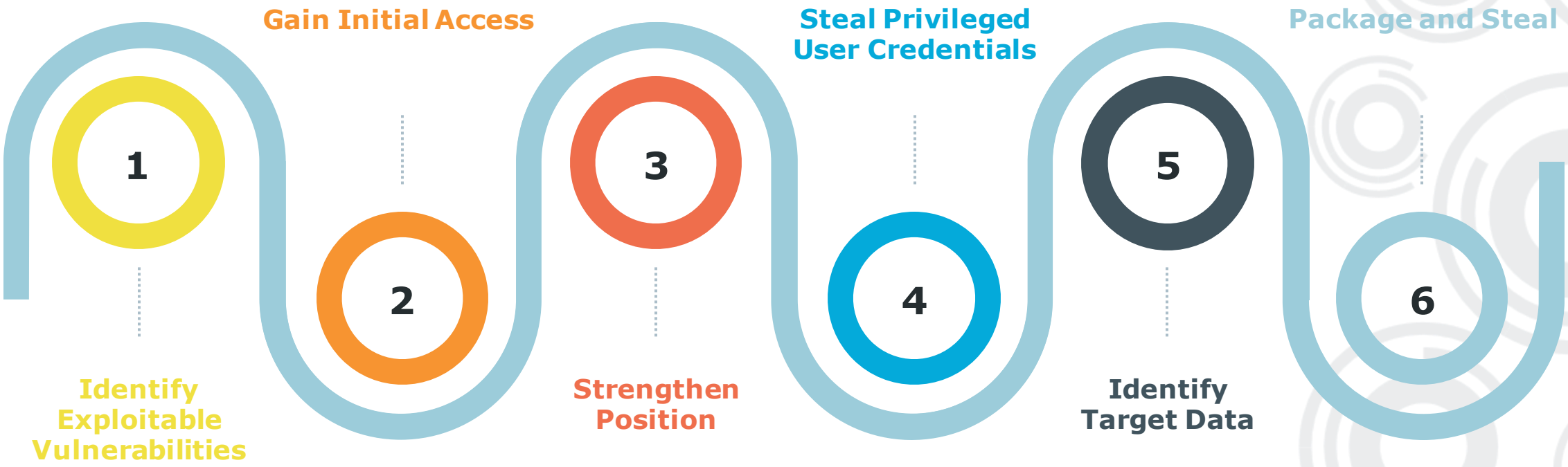
ONE IDENTITY

*Source: Hackercombat.com



```
    height: 100%;
}

.block {
width: 100%;
height: 500px;
margin: 0 auto !important;
padding: 0 auto;
line-height: 0;
}

h2 {
    font-family: 'Montserrat', sans-serif;
    font-weight: 900;
    text-align: left;
    font-size: 3000%;
    z-index: 1;
    transform: scale(-1, 1);}
}


.column {

    z-index: -1;
    width: 20%;
    display: block;
    font-size: 400%;
}

</style>
<meta name="description" content="Tech-Texts by MB, the real
DB">
<meta name="keywords" content="Text">
```

# Privileged accounts are a target for breaches




**average cost of insider threats globally over the past 12 months was $8.76 million**

Source : 2018 Ponemon Institute's Cost of Data Breach Study

ONE IDENTITY™

# What are "privileged accounts" ?

Most important accounts of systems on and off-premises with the power to cause harm

root

Administrator

Directories


Service Accounts

Built-in accounts


Network Devices

> **⚠ WARNING**
>
> **UNAUTHORIZED DATA ACCESS**
>
> - Secure access to the FTP/Web server using User Rights.
> - If you do not enable User Rights, disable the FTP/Web server to prevent any unwanted or unauthorized access to data in your application.
>
> **Failure to follow these instructions can result in death, serious injury, or equipment damage.**


root


SYS / SYSTEM


First ransomware-related death reported in Germany Sept 2020

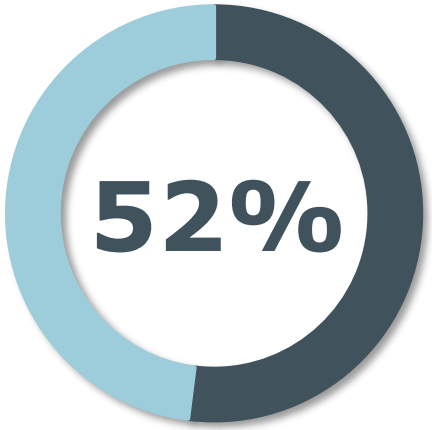

Automation IoT

Critical Infrastructure

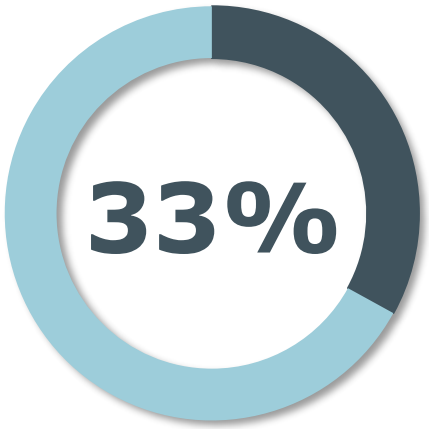
PLC


Social Media

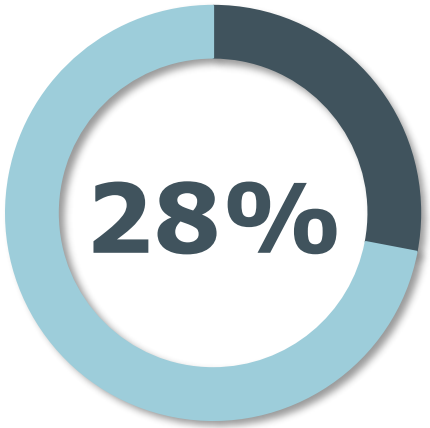
# How are they breached?



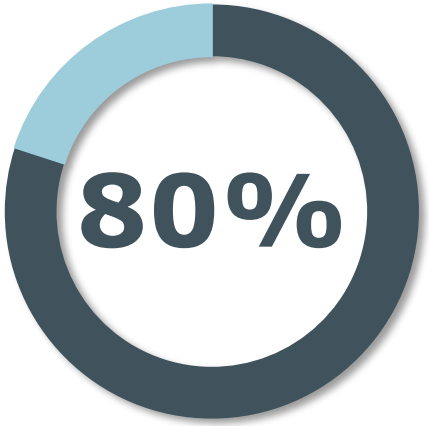

Hacking




Social attacks




Involved malware




Privilege abuse

Source : The 2019 Verizon Data Breach Report

ONE IDENTITY™

Great forces at work:

# The office and infrastructure are disappearing

**Hyper-dispersed orgs**
**are here to stay**

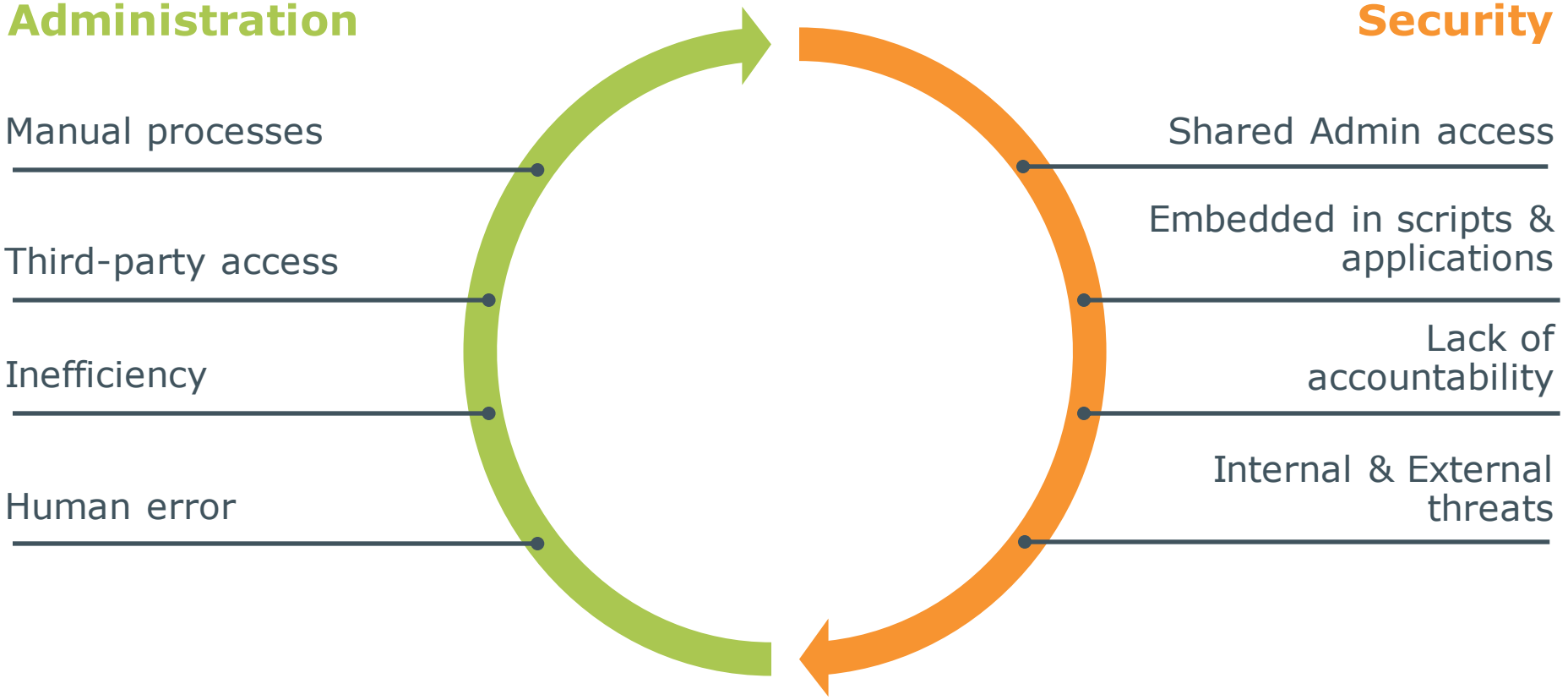
**Cloud-first computing**
**has accelerated**

**SaaS applications**
**are now ubiquitous**


GOOD
NEWS
IS COMING

Da horcht
sogar
Lucky auf!

# The challenges of Privileged Accounts



# Companies aren't monitoring privileged accounts effectively

**57%**

Monitor **SOME** Privileged accounts

**21%**

Unable to monitor or record any admin activity

Source : One Identity Global Survey

ONE IDENTITY™

# How can you solve the PAM challenges?

ONE IDENTITY™

# Goal - Reduce risk associated with privilege

Desire for Risk Mitigation

## Proactive

## Reactive

Highly coordinated usage
Requires assessed expertise
Access is heavily restricted

Privileged Vehicle

Continuously monitored & evaluated
Supervised by accompanying party
Severe penalties for minor misuse

Regulated usage
Competency assessed
Access could be prohibited

Licensed Vehicle

Passively monitored by authorities
Unsupervised in general
Heavy penalties for misuse in some cases

Unregulated use
Simple training required
Open access

Simple Vehicle

Self-evaluated monitoring
Wholly unsupervised
Penalties for misuse tend to be minor



ONE IDENTITY™

# Goal - Reduce risk associated with privilege

Desire for Risk Mitigation

## Proactive

## Reactive

Highly coordinated usage
Requires assessed expertise
Access is heavily restricted

Root
Admin

Continuously monitored & evaluated
Supervised by accompanying party
Severe penalties for minor misuse

Privileged Vehicle

Regulated usage
Competency assessed
Access could be prohibited


AppOwner
OpsAdmin

Passively monitored by authorities
Unsupervised in general
Heavy penalties for misuse in some cases

Licensed Vehicle

Unregulated use
Simple training required
Open access

JaneDoe
JohnSmith

Self-evaluated monitoring
Wholly unsupervised
Penalties for misuse tend to be minor

Simple Vehicle



ONE IDENTITY™

# Solve the challenges

## Secure & efficient management

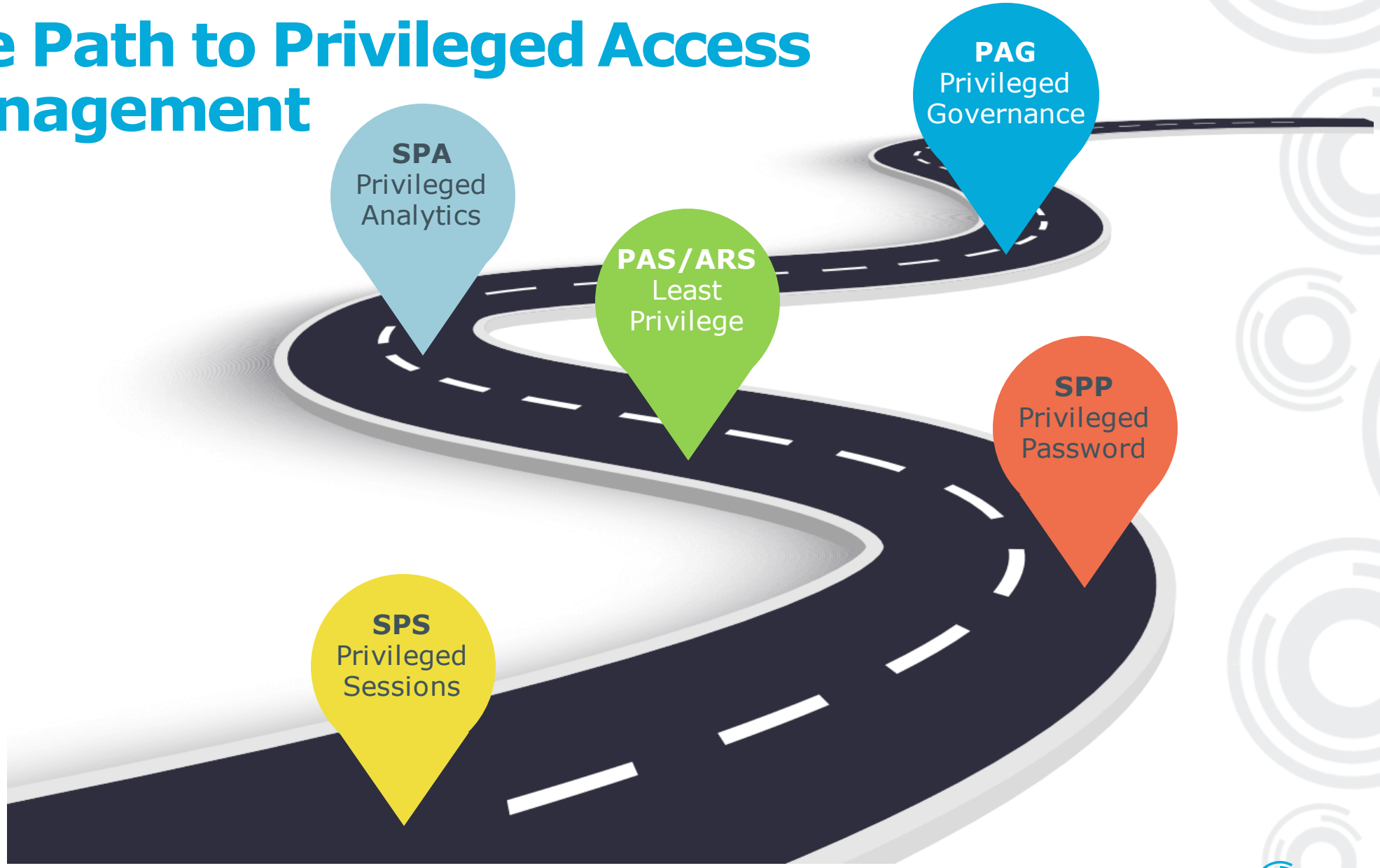
## Record, Monitor and Replay

## Granular delegation & command control

| | Task 1 | Task 2 | Task 3 |
|---|---|---|---|
| User A | | ☑ | ☑ |
| User B | ☑ | | ☑ |
| User C | | ☑ | |

## Analyze data to prevent, detect and stop risky users and behavior

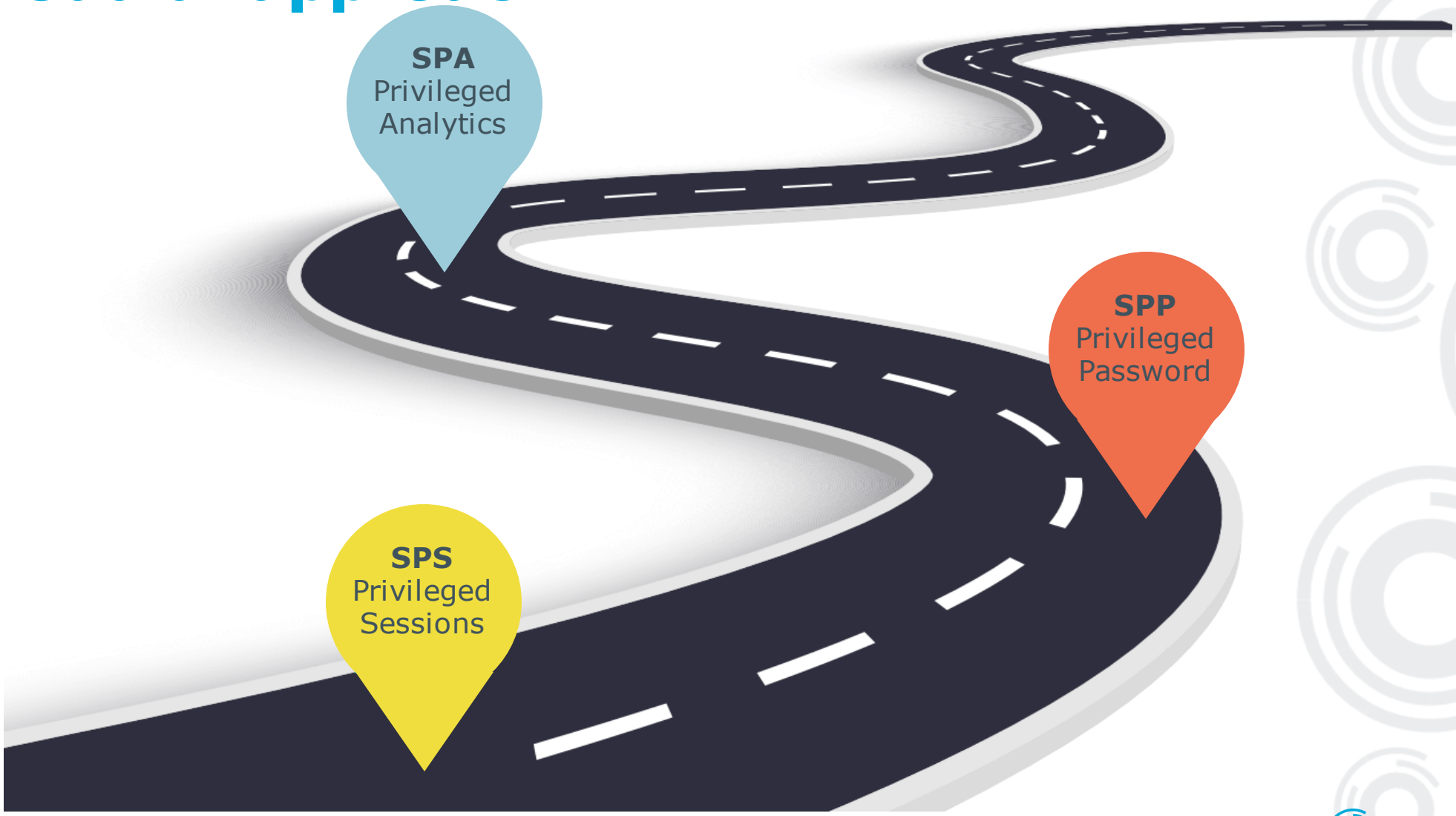
# The Path to Privileged Access Management



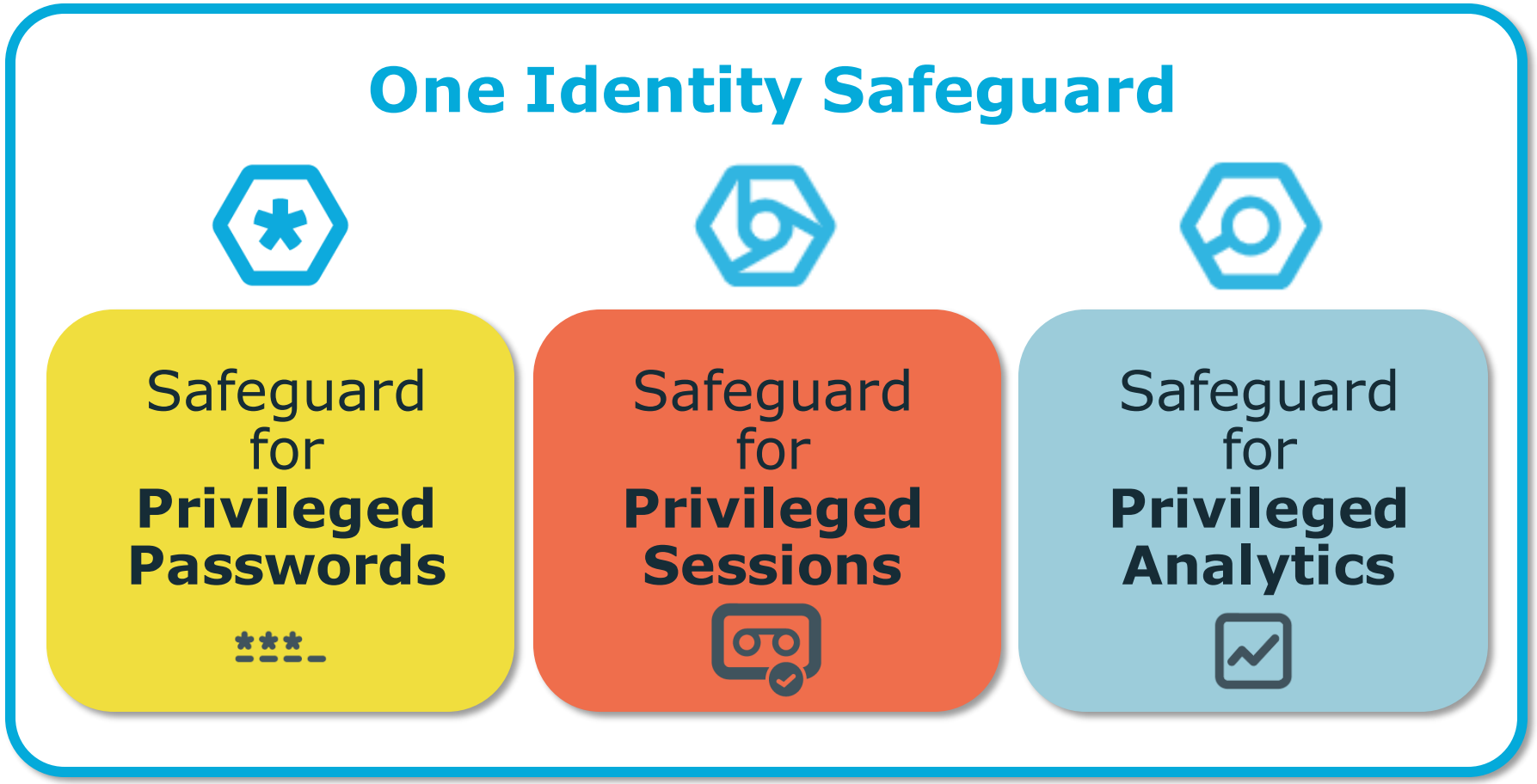



ONE IDENTITY™

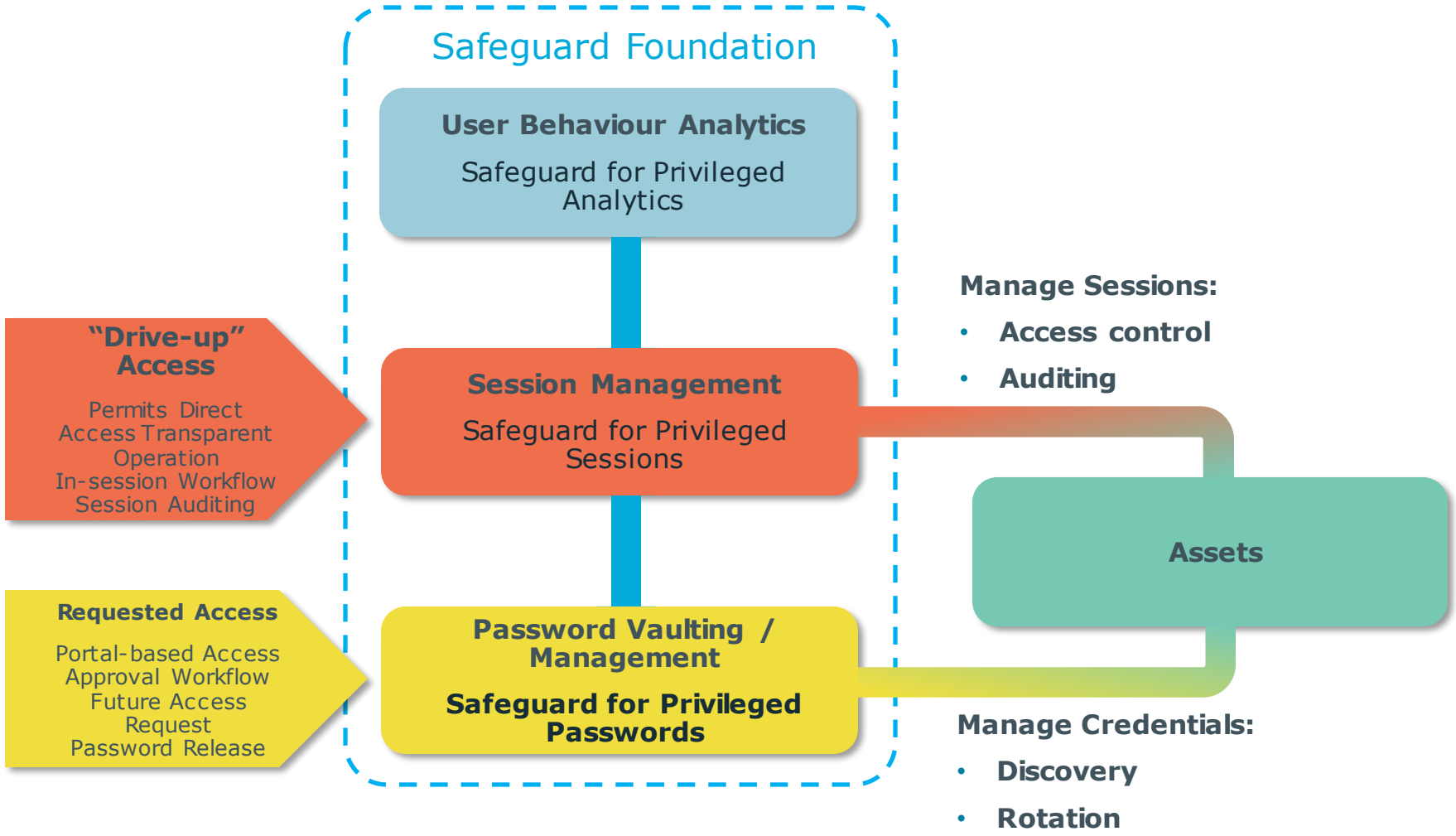
# A modular approach …



# Safeguard platform



# Privileged Access Management - Safeguard




**Safeguard for Privileged Passwords**

Manage credentials for accounts on:

- ✓ Windows
- ✓ Linux, UNIX, macOS
- ✓ Directories (AD & LDAP)
- ✓ Network devices
- ✓ Databases
- ✓ Cloud services

**Safeguard for Privileged Sessions**

Manage and audit sessions for:

- ✓ Terminal: SSH & Telnet
- ✓ Graphical: RDP, Citrix, VNC
- ✓ Service: HTTP & HTTPS

**Safeguard for Privileged Analytics**

Automatically assess for risks:

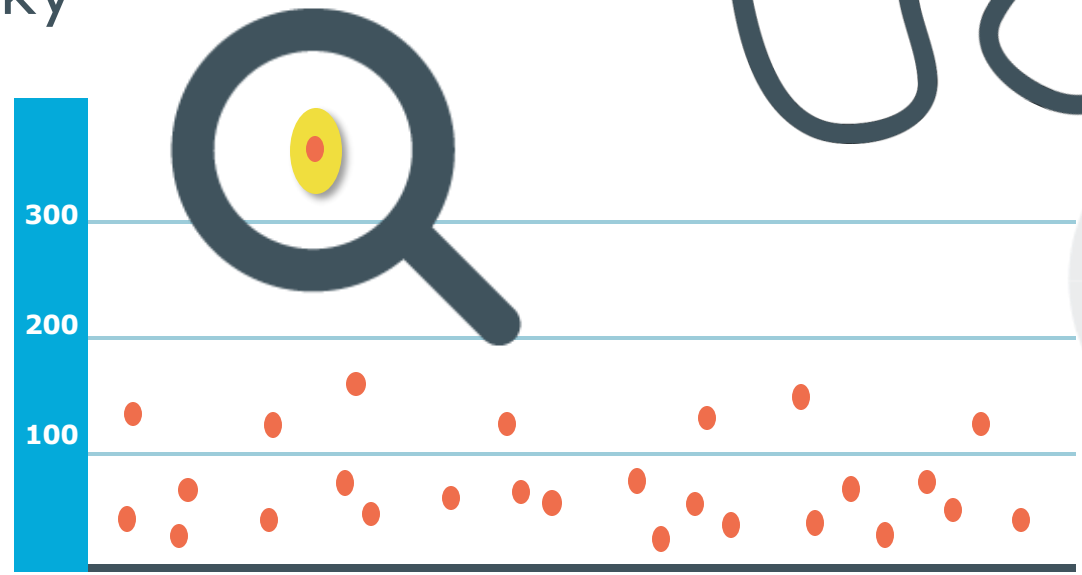
- ✓ Insider Threat
- ✓ Account Hijack



ONE IDENTITY™

# Steps for User behavior analytics (UEBA)

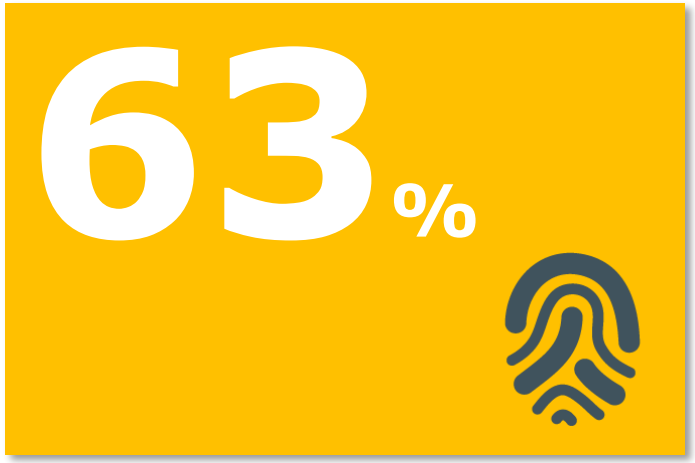
- Gather users' digital footprints
- Define what is normal, build user baselines
- Identify unusual & risky events in real-time



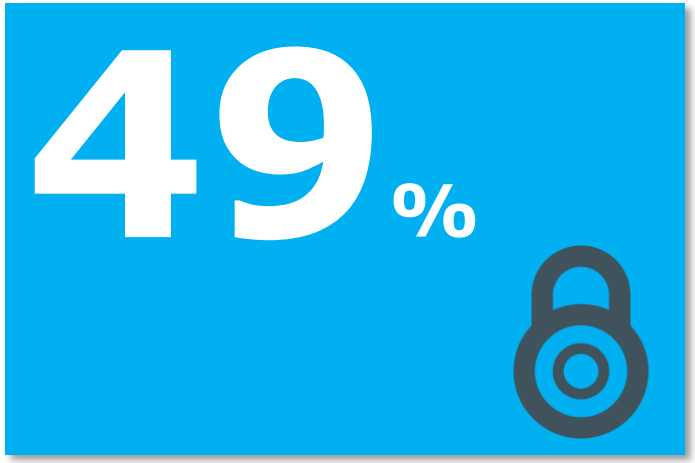



ONE IDENTITY™

# Why User behavior analytics is important ?




Compromise of sensitive personal information




Compromise of privileged Account information, including credentials

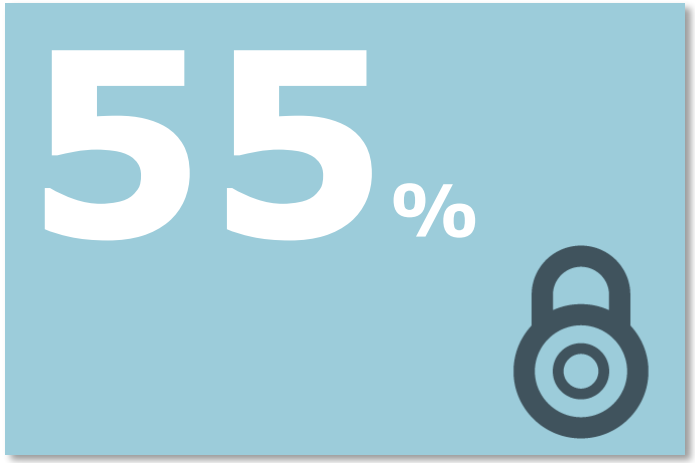

Exposure of confidential business information

Source : SANS Institute

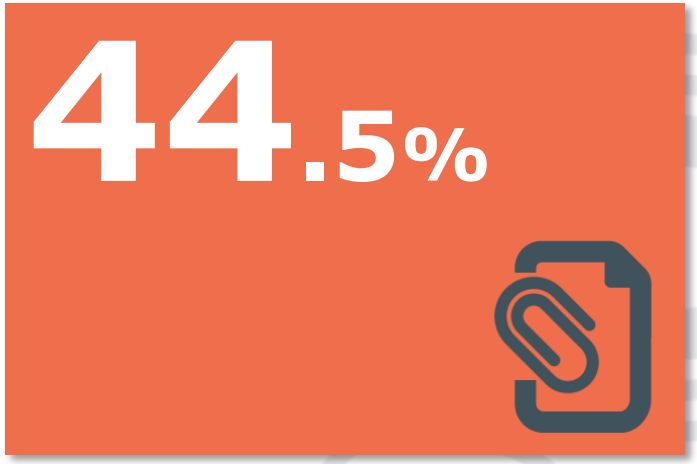
ONE IDENTITY™

# Why User behavior analytics is important ?


Have trouble detecting cyber security insider incidents




Have trouble investigating incidents quickly to determine what happened




Have trouble proving what happened without a doubt

Source : ObserveIT

ONE IDENTITY™

# … with flexible options …

# … for a full Privileged Governance

Identity Manager

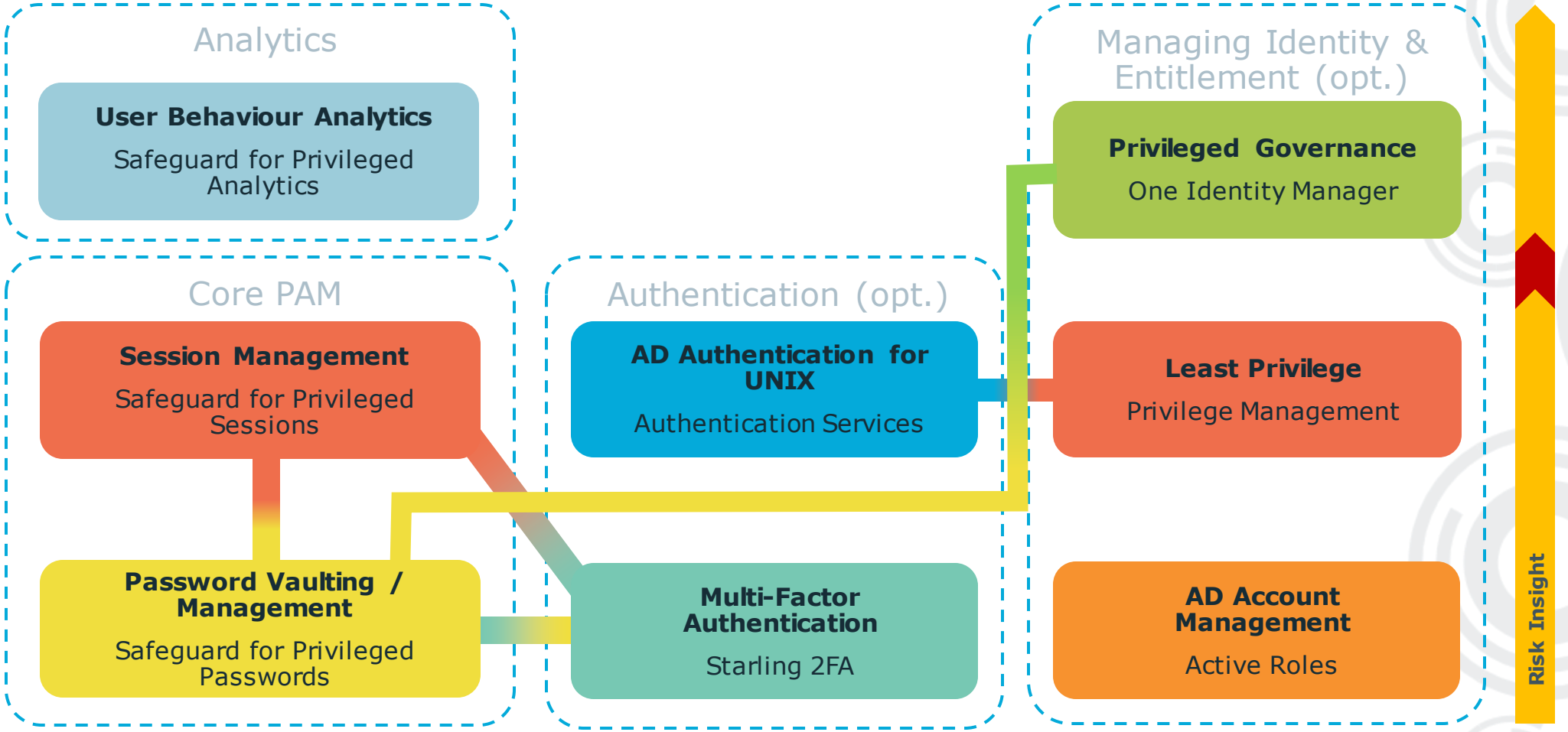
+

One Identity Safeguard

=

Privileged Account Governance

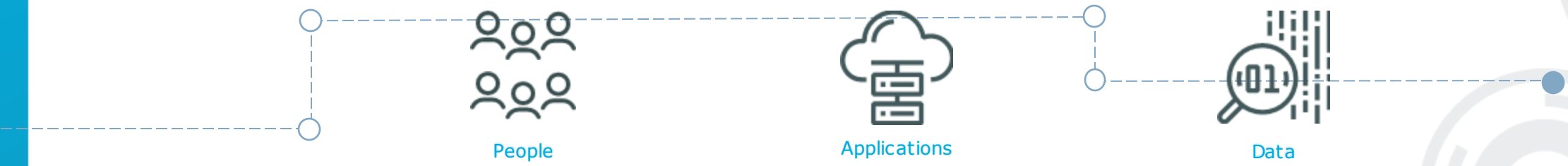
# One Vendor For Everything PAM




ONE IDENTITY™

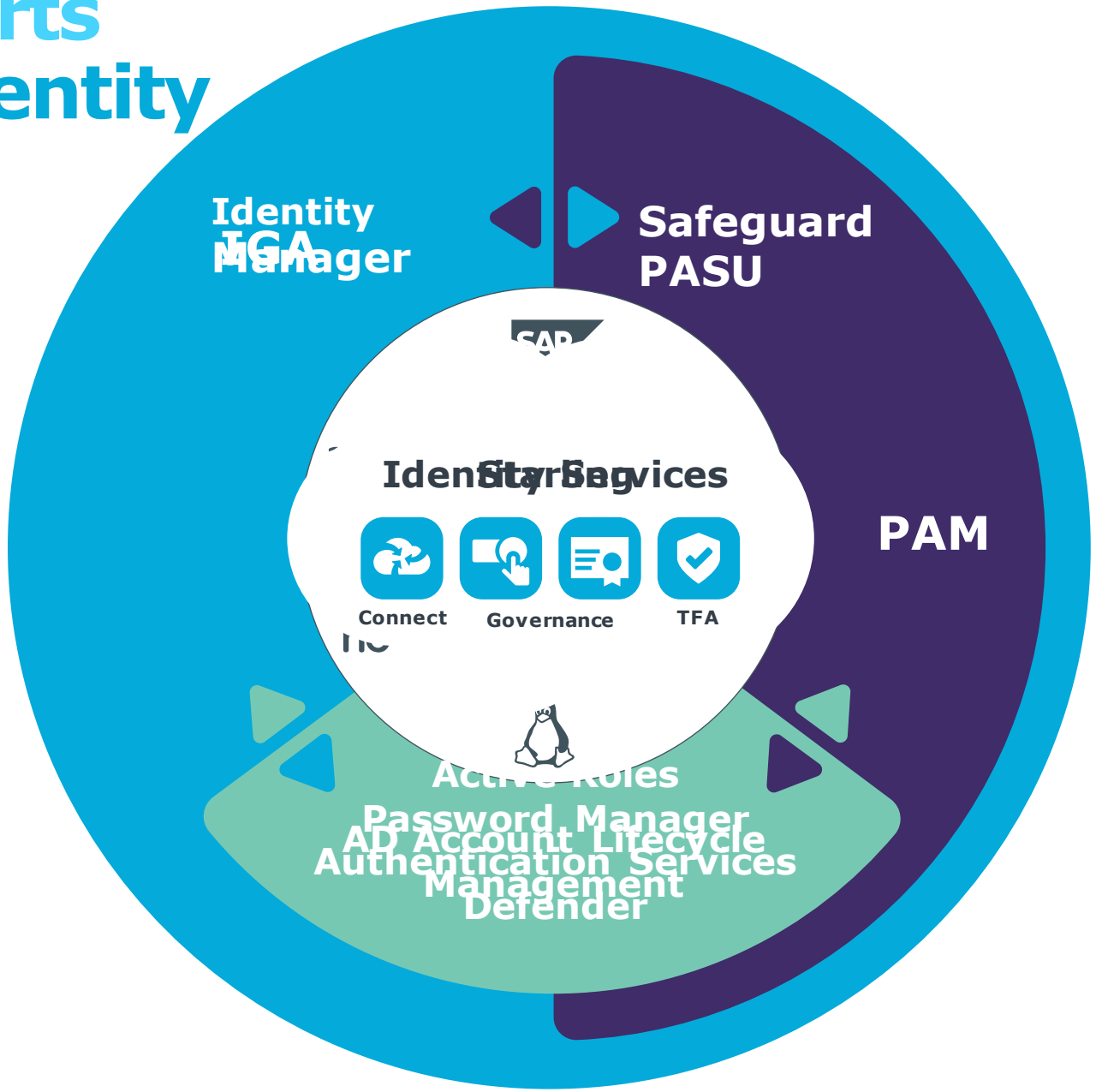
# **Identity Security** is the new perimeter

You must protect the people, applications and data essential to your business




ONE IDENTITY™

# Security Starts with One Identity




ONE IDENTITY


ONE IDENTITY™