



Microsoft Security Portfolio

Improve the security posture of
Windows Azure AD



Innovative technology consulting for business.

Agenda



1

Introduction

- Business → Trust → Security
- Devoteam Security Portfolio

2

IAM = Security Foundation

- IAM Fabric Definition
- Microsoft IAM = Azure AD

3

Azure AD

- 3 common scenarios to start with Azure AD
- Azure AD Maturity Level
- The 6 domains of Azure AD

4

Security Posture Improvement

- Agile Methodology based on continuous improvement
- How to start the initiative?

5

Questions?

How to create the Trust ?

What are your 3 major expectations to create the Trust, Business Catalyser ?



Experience

Consumers, customers, business partners, and employees all expect great user experiences.

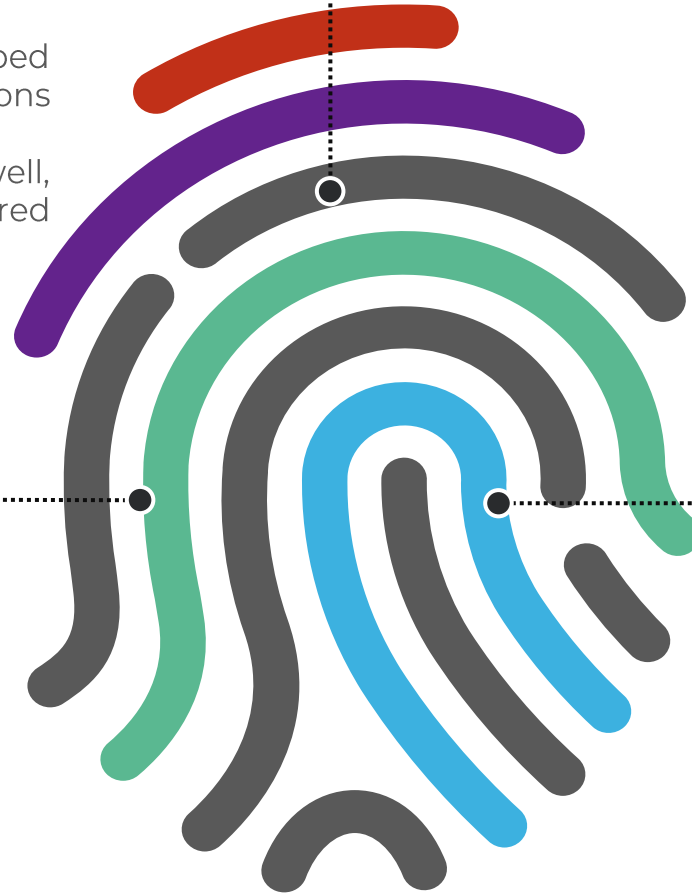
Their loyalty and commitment are shaped by friction less experience of interactions when using new digital services.

Failure to manage digital identities well, threatens the quality of the delivered services.



Consent

Consumers want that the sharing of their personal information is possible if and only if they give the consent. This consent can be easily given and removed thanks to a frictionless application. They also want a complete transparency and tracability about the consents they have.

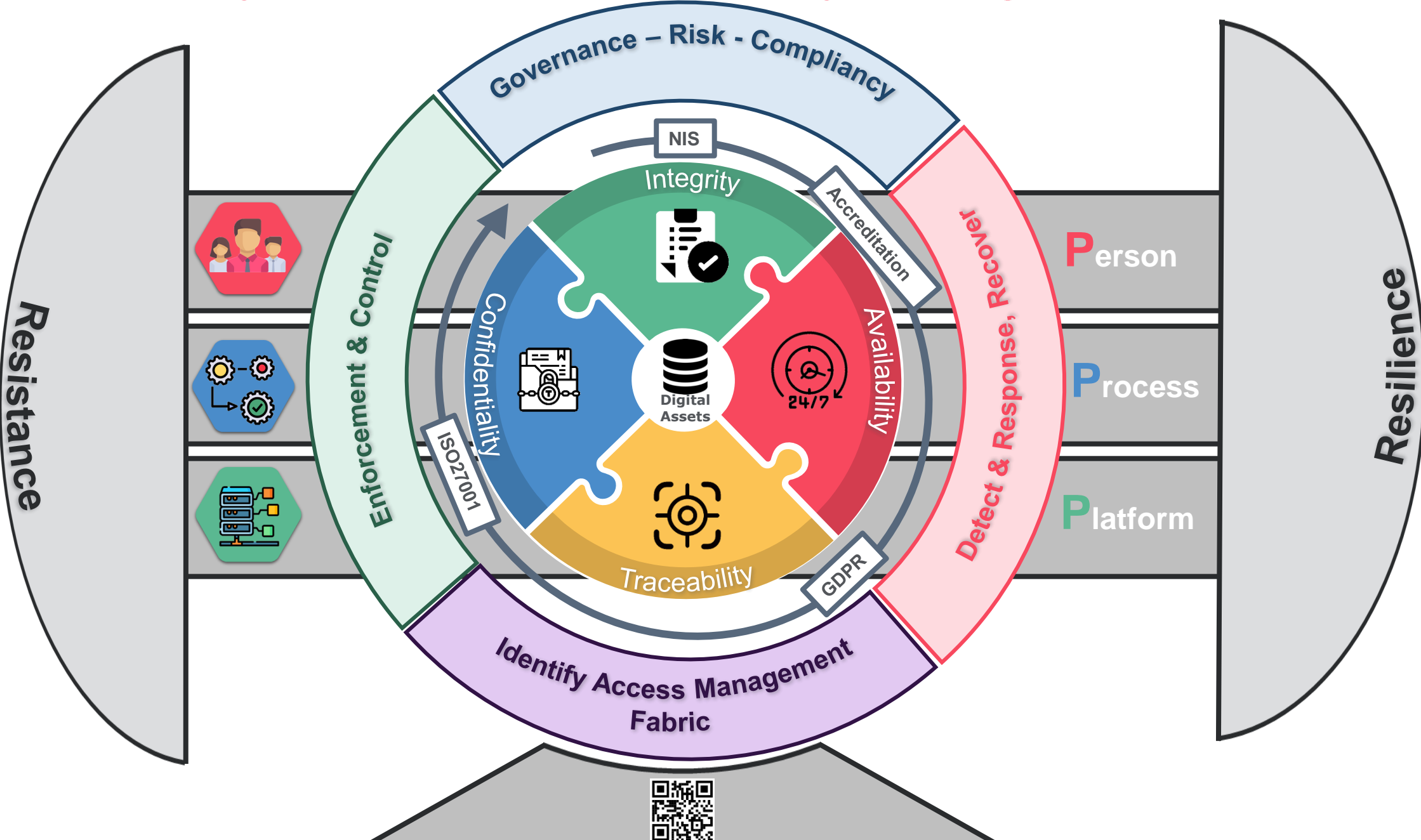


Accountability

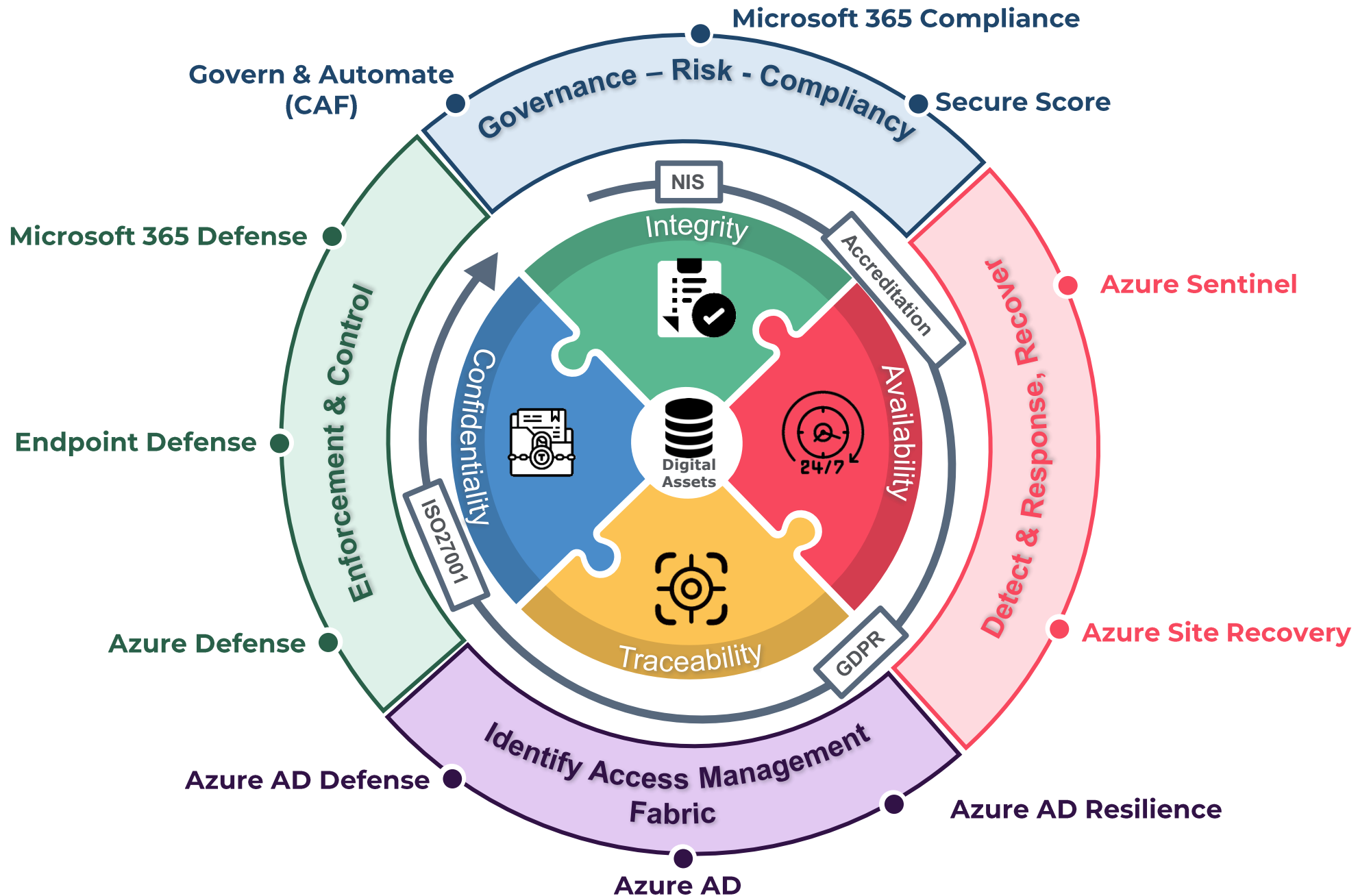


The majority of the consumers is not aware of the amount of information they shared about themselves online. Their knowledge of their rights regarding the use and the protection of their personal data is really limited

Cyber Security Portfolio calibrated for your Digital Transformation



The Microsoft Roadmap for a best-in-class security posture



What is the reason to start Azure AD initiative ?

The three common scenarios

M365 Driver

Due to the Office licensing model change and/or the Covid19 crisis, the company needed to urgently move to Office 365 required the activation of Azure AD.



Azure AD is quickly installed (AD connect) and configured to be functional for the activation of Microsoft 365 without considering a security posture defined by the CISO

Azure Driver

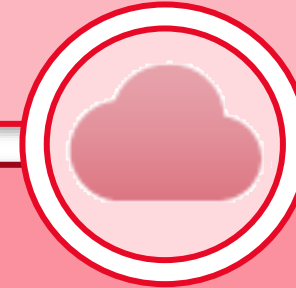
Onprem data center extension to the cloud for a partial or complete move to the Azure driven by Business or technical motivations



Azure AD is quickly installed (AD connect) and configured to be functional for the activation of a specific Azure service without considering a security posture expected by the CISO

CAF Driver

This is the best scenario to propose a security posture expected by CISO because the initiative is driven by the cloud adoption framework



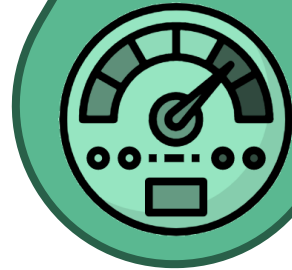
Except if the security is not considered at the start of that initiative and decisions are taken without considering the security (Security needs to shift left in the decision process)

What's your Azure AD maturity level ?

Two approaches

Identity Maturity Audit

Assessment providing an overview of the secure posture of the Azure AD according to the 3P (**P**eople – **P**rocess – **P**latform)



Identity Secure Score

The identity secure score is a number that functions as an indicator for how aligned you are with Microsoft's best practice recommendations for security.

What's your Azure AD level of maturity ?

Driven by an assessment covering six dimensions

Identity Foundation

- Did you connect (bidirectional) your Active Directory with your Azure AD? AD connect cloud sync?
- Are you able to guarantee the resiliency of your Identity Fabric ?
- Did you federate Azure AD with other IdPs?
- Did you enable the collaboration outside your organization (B2B) ?

Identity Management

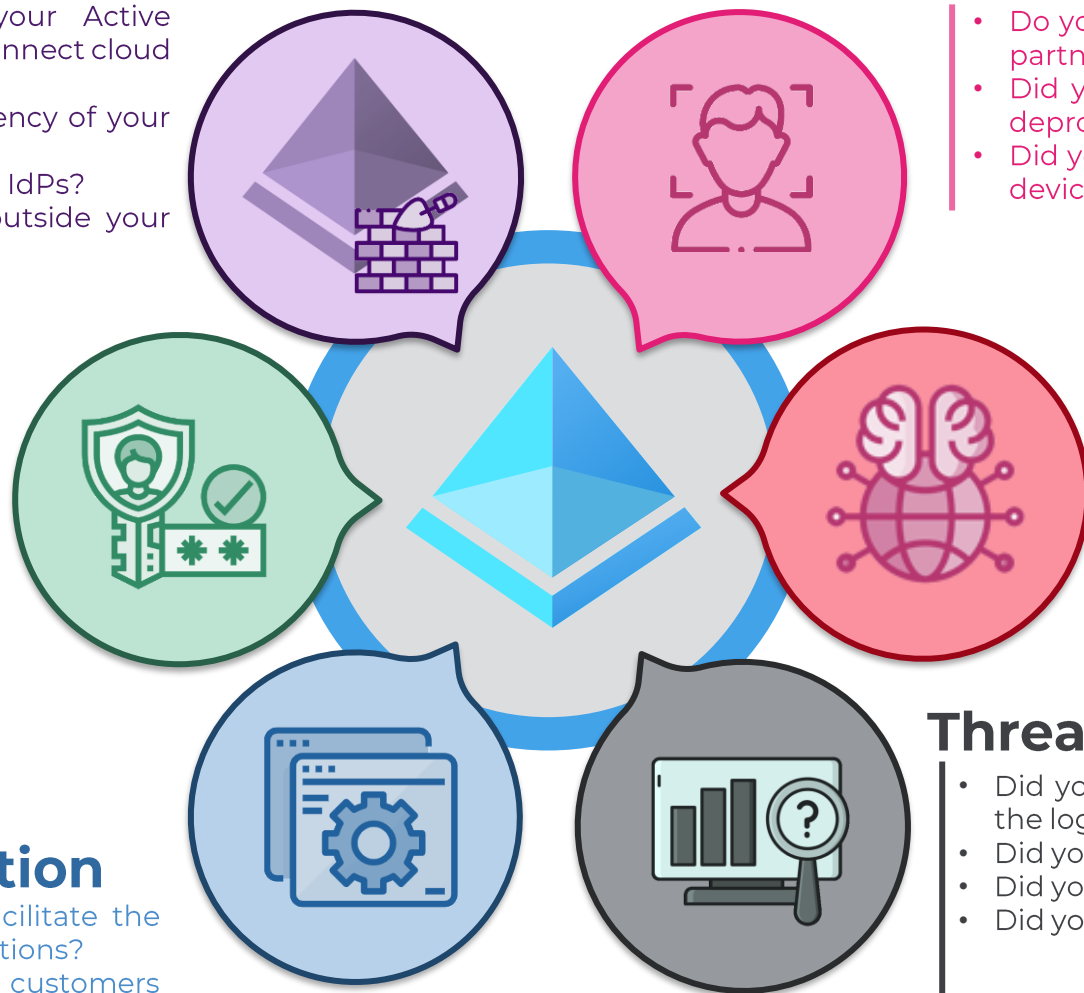
- Do you manage hybrid identities (employees – partners – clients - ...) on the same Azure AD?
- Did you automate the user provisioning and deprovisioning ?
- Did you define an onboarding strategy for your devices (Registered - Join - Hybrid Join) ?

Authentication

- Is your authentication only password-based ?
- Did you deactivate your legacy auth?
- Did you create a password policy include reset password? Is it included in a process?
- Is the password synchronized between the cloud and onprem ?
- Are your employees informed about the importance of a good password? (Awareness)
- Did you already use MFA for specific accounts (Administrators?)
- Did you envisage passwordless approach ?

Applications Integration

- Do you use application proxy to facilitate the integration of the onpremise applications?
- Do you scale your apps to your customers (B2C)?
- Do you introduce the cloud SaaS apps in your Azure AD?



Authorization

- What's the authorization model that you use (RBAC – ABAC – ReBAC?)
- Is your RBAC aligned with your organization's role definition ?
- Do you use a PAM for the privileged accounts ?
- Did you already introduce conditional access in your strategy?

Threat Analytics

- Did you implement a process seccops for the analysis of the logs generated by Azure AD?
- Did you analyse the Risky Users or the Risky sign-in?
- Did you enable the Identity protection
- Did you use Identity protection for the

How to improve your Security Posture ?

Activities proposed per domain

Identity Foundation

Hybrid Identity (AD)

Federation

External identities (B2B & B2C)

Identity Resilience

Authentication

SSPA & Password Reset



Passwords Policies



Multi factors of Authentication



Password-Less

Applications

 Cloud Apps

 App Proxy

 App Registration



Identity Management



Identity Lifecycle Management



Person



Device

Authorization



Roles (RBAC,...)



PIM



Conditional Access

Threat Analytics



Logs Management



Identity Protection



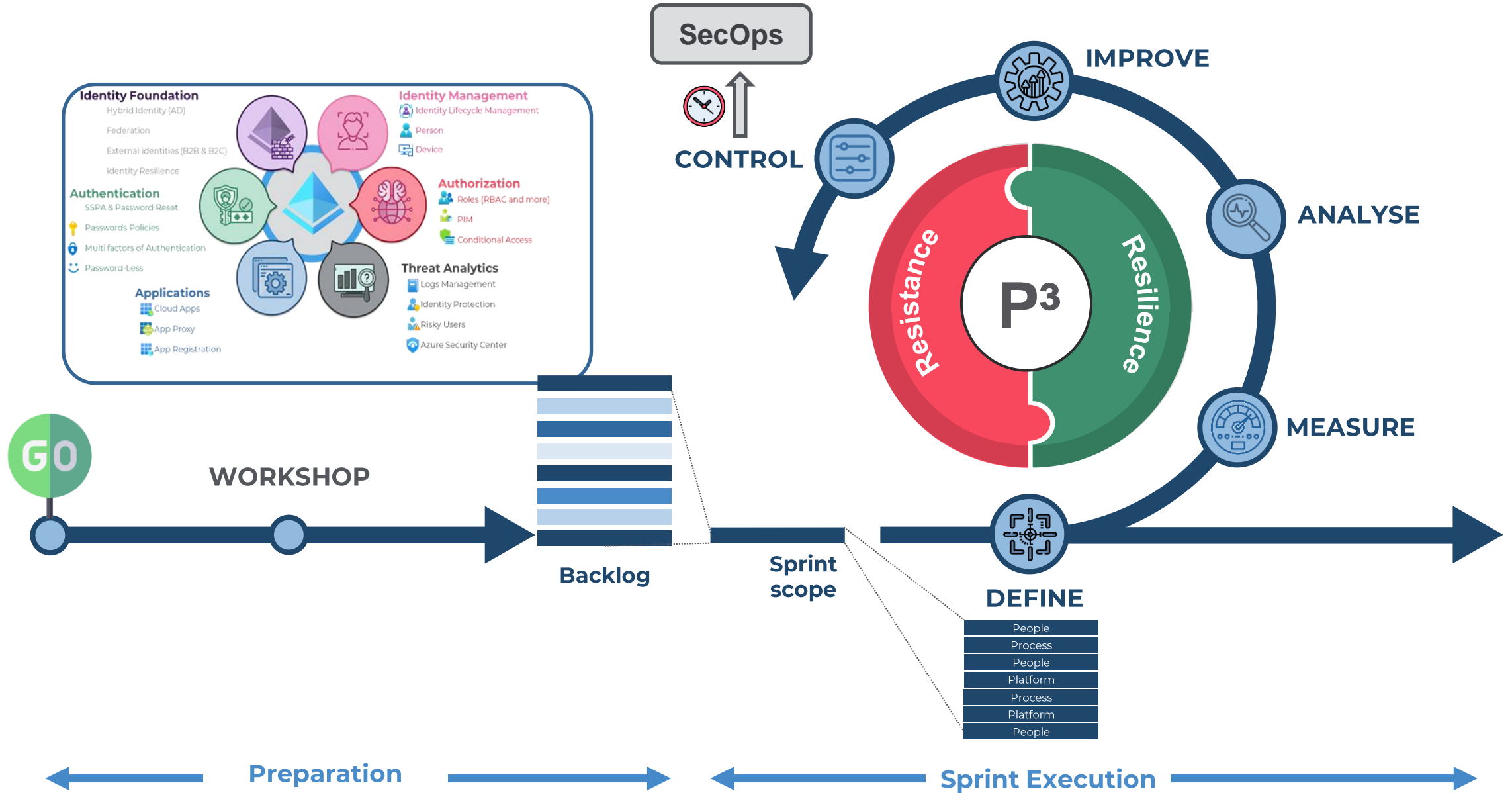
Risky Users



Azure Security Center

How to improve your Security Posture ?

An Agile Methodology focused on Continuous Improvement



How to improve your Security Posture ?

The Workshop

Engagement Setup

- Kick-Off Meeting
- Secure Score Overview & Security Posture
- Application Discovery Presentation & Setup

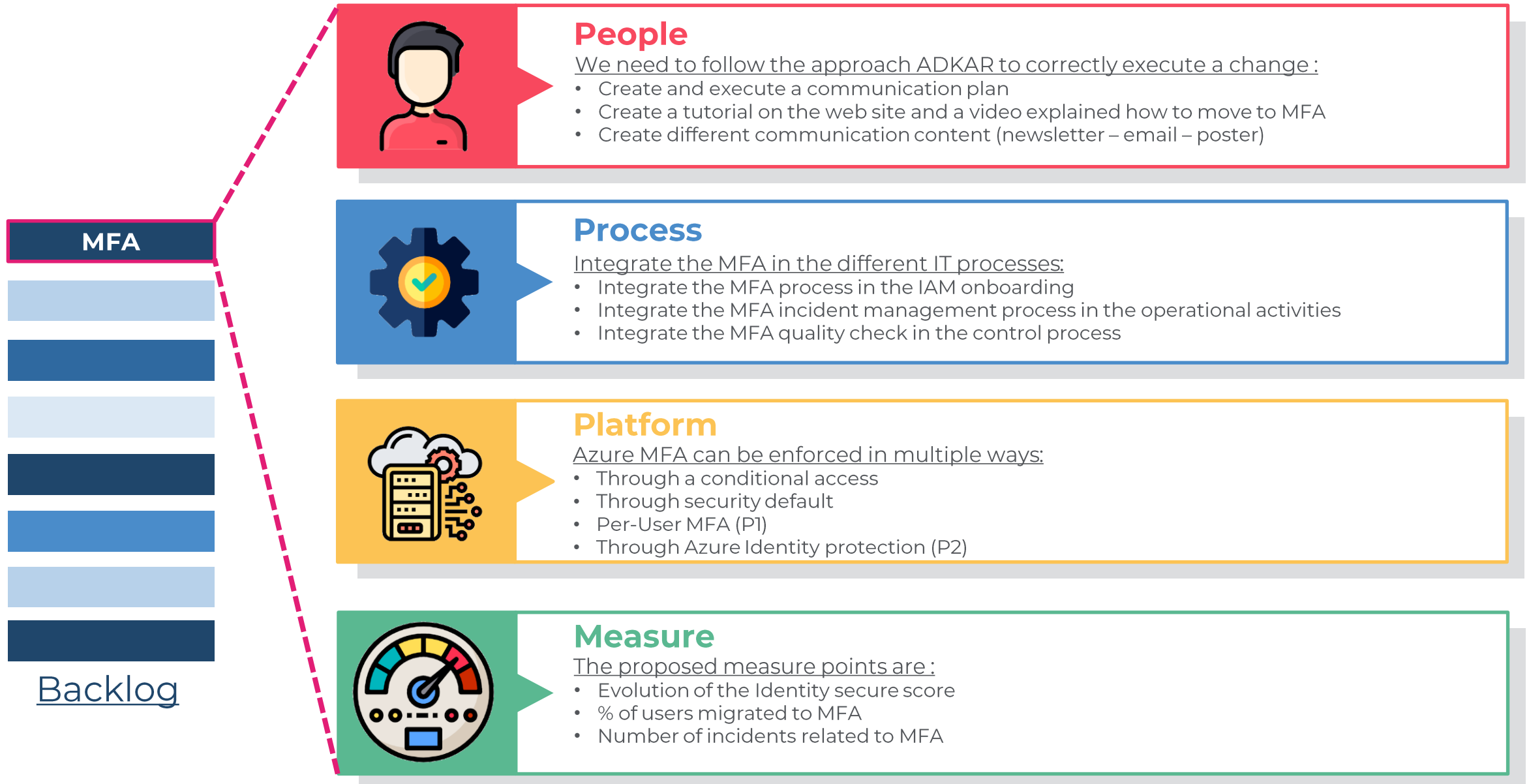
Design & Planning

- Identity Fundamentals
- SSPA
- MFA
- Conditional Access
- Applications Management




How to improve your Security Posture ?

Iteration loop for the Multi Factor Authentication activity



How can we start ?

Check if you are eligible for the identity workshop...


 **Security, Compliance and Identity Workshops**

Security


Compliance

Identity


Endpoint Management

 **Partner criteria**

- FastTrack Ready or Co-Sell Ready
- And SSPA Compliant


 **Customer criteria**

- Must have 1000+ AADP Paid Available Units (PAU) with < 40% usage.


 **Payout structure**

- Identity Workshop: \$3,500

Workshop Execution Requirements

 **Workshop requirements**

- In this workshop the expectation is that you have covered the following topics:
 - Identity Fundamentals (Azure AD Integration and Hybrid Authentication)
 - Self-Service Password reset
 - Multifactor Authentication
 - Conditional Access
 - Azure AD Application Management
 - Identity security posture assessment using Microsoft Secure Score
- The following activities must be completed:
 - Application Discovery
 - Design and Planning Sessions
 - Key results, recommendations and next steps

 **Proof of Execution requirements**

- Complete Customer satisfaction survey
- Complete Partner Findings Survey
- Upload completed POE Report Template found in the workshop kit
- Partner Invoice (see template)

#TechforPeople.