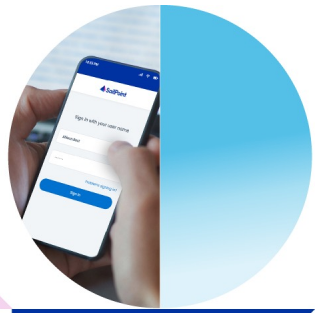
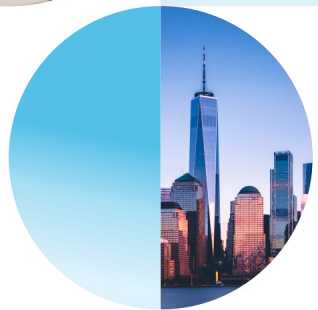
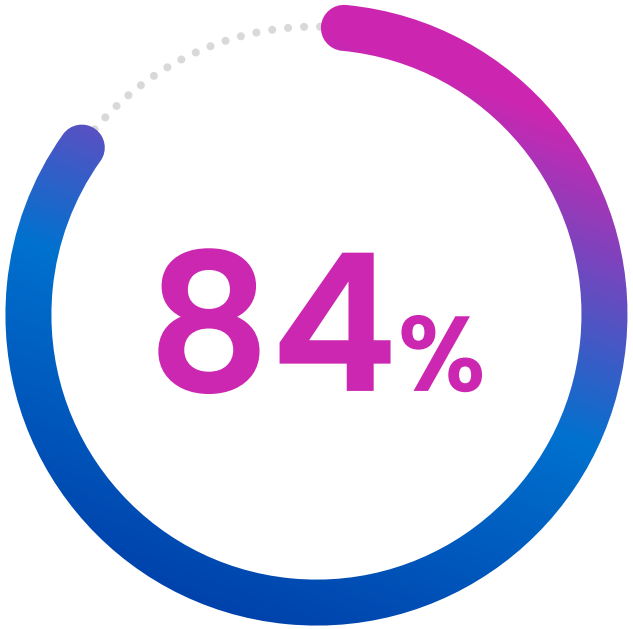
SailPoint

Identity Day

Horizons of identity security workshop







# of organizations experienced an identity-related breach.

Source: “2022 Trends in Securing Digital Identities”, Identity Defined Security Alliance.

$3-4B

Cost of the Epsilon breach which could have been avoided with a strong identity program

~50%

IT helpdesk calls are password related and can be eliminated through modern IAM solutions such as passwordless

Identity creates business value

Top 10% of the most secure companies realize significant benefits, including increased resilience, by investing in identity security

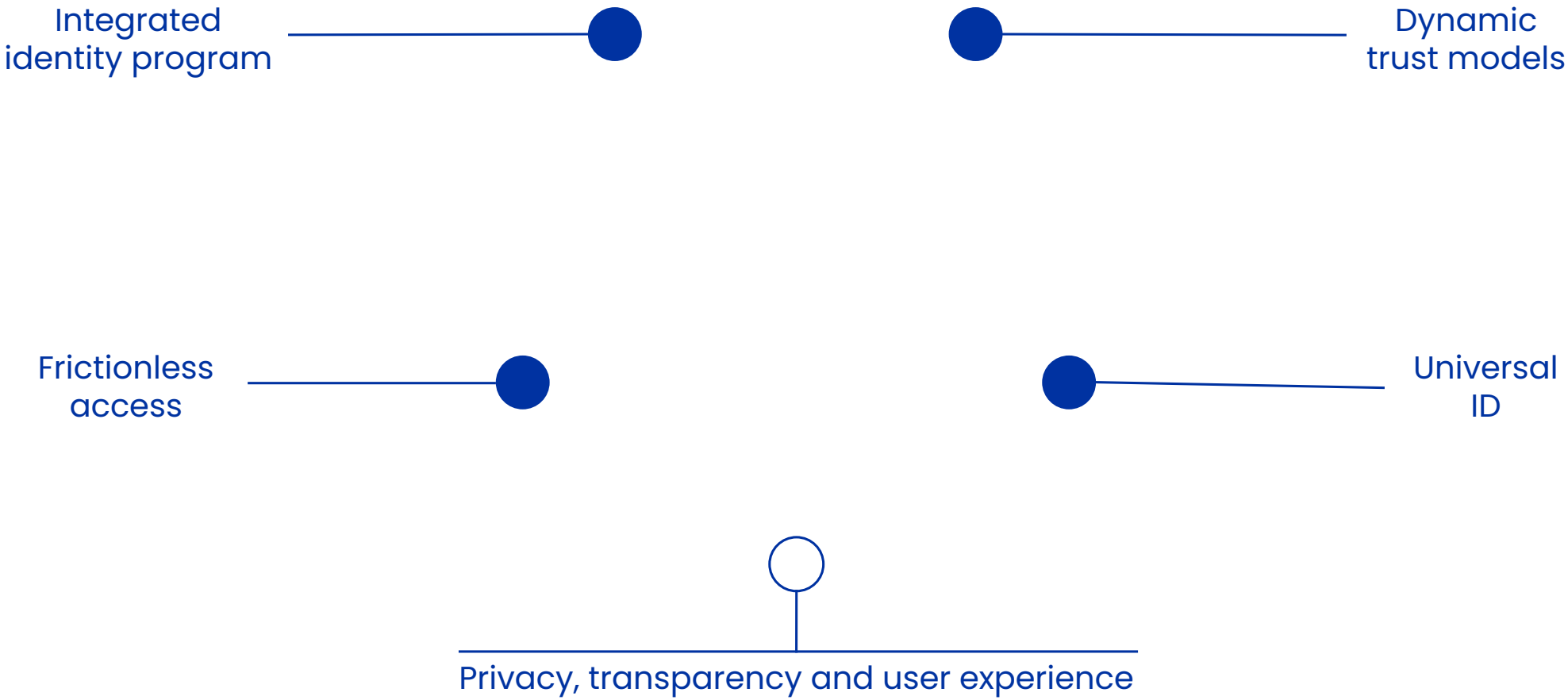
– McKinsey benchmarking report, August 2021

Identity security is business essential

Discover the 5 horizons of identity security

We surveyed over 350 Identity and Access Management (IAM) decision makers globally and identified 5 horizons of identity security with key insights and takeaways. One key insight is that 74% of companies still have immature, fragmented or manual identity programs.

Shaping the future of identity



Shaping the future of identity

- **First, Security is becoming Identity-Centric**.
  - **That common link**, that stiches everything together across multiple technology environments.
  - **integrated identity model** that is resilient and where the identities themselves are linked to cover the cloud, SaaS, Apps, devices, and data.

- **Secondly**, Identity programs will move to **dynamic trust models** which means adopting AI and machine learning to help identify anomalous behaviors and patterns.
  - AI and Machine Learning will be utilised to analyse interactions across identities and environment and adjust access rights autonomously and in real time.
  - Think about how you engage and work with applications,

- **The third** element is super cool, **universal identities will be able to merge** with federated access across domains and geographies.
  - And identities will be verified through decentralised protocols such as blockchain.
  - (Think about moving from one company to the next, and bringing your own identity) – B.Y.O.I.

- **Finally**, the fourth element shows that **frictionless access will be possible** when authorisation becomes dynamic, automated, and code-driven.
  - Seamless or password-less authentication will become the norm.
  - Imagine, being able to have in the moment access throttling, or just in time provisioning based off how you work, without the need to remember your password or to request access

Most companies will adopt these technologies and make this vision a reality over the next five to ten years and organisations need a path, a framework to get there

Maturity across vectors

1

Strategy

2

Technology
& Tools

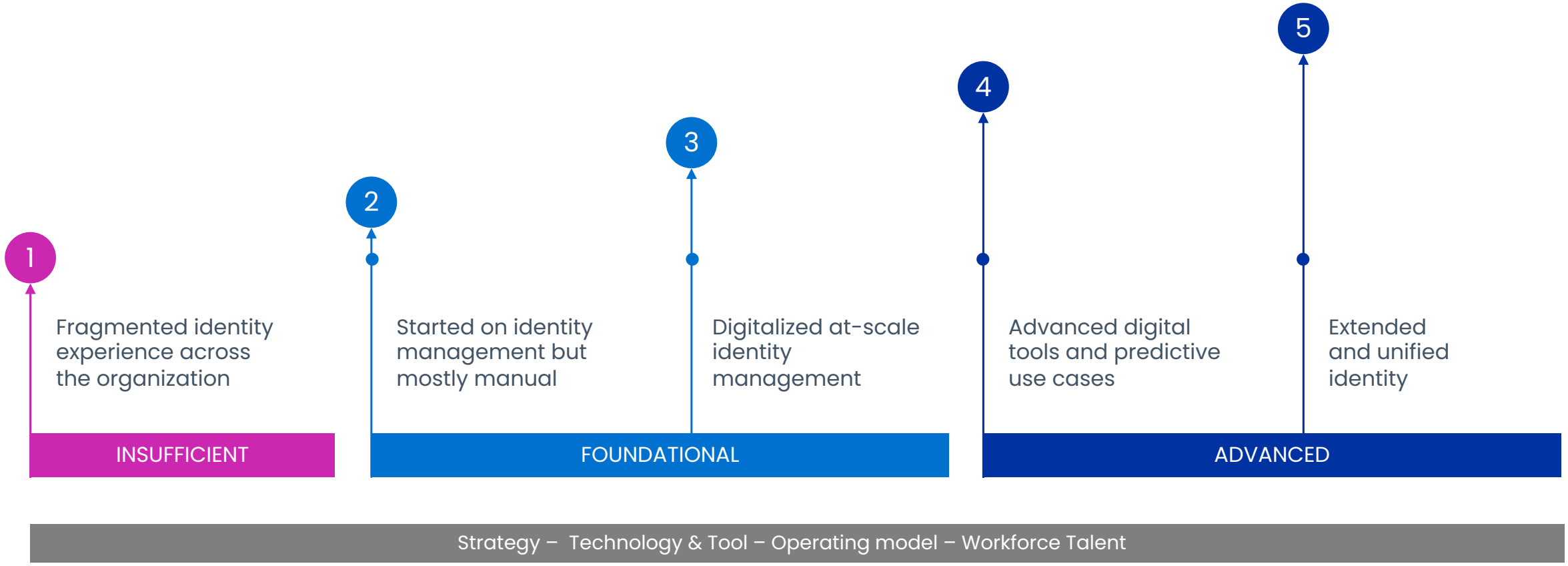
3

Operating Model

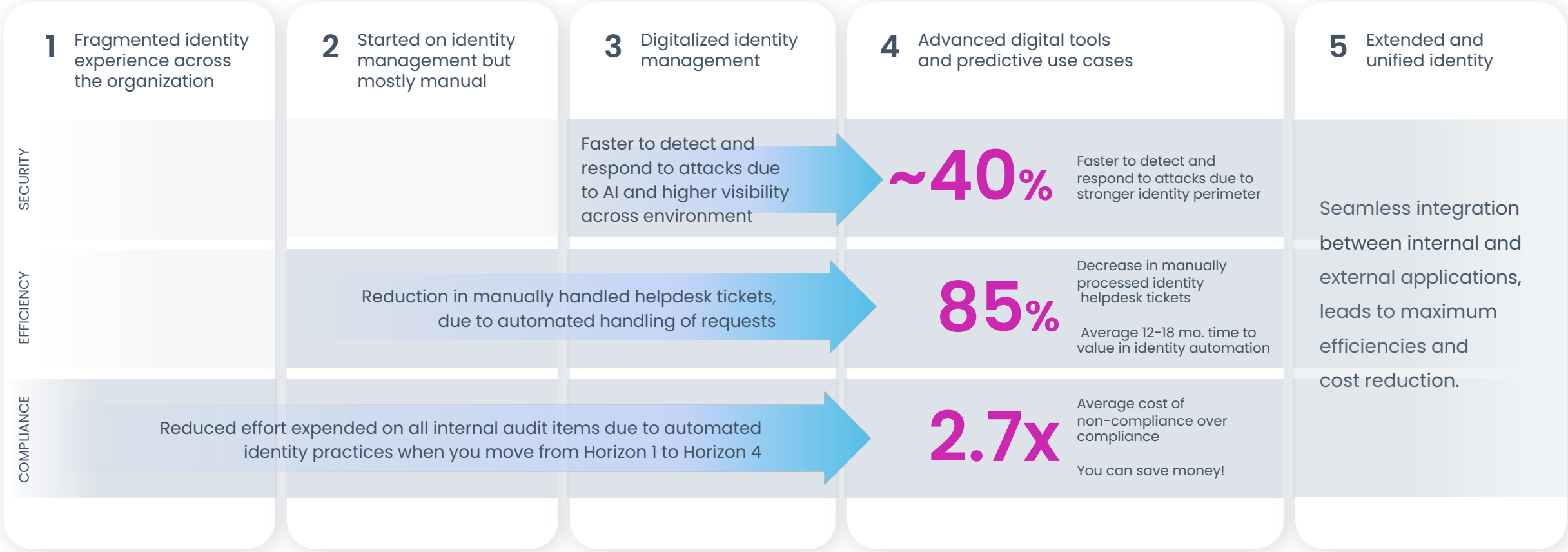
4

Talent

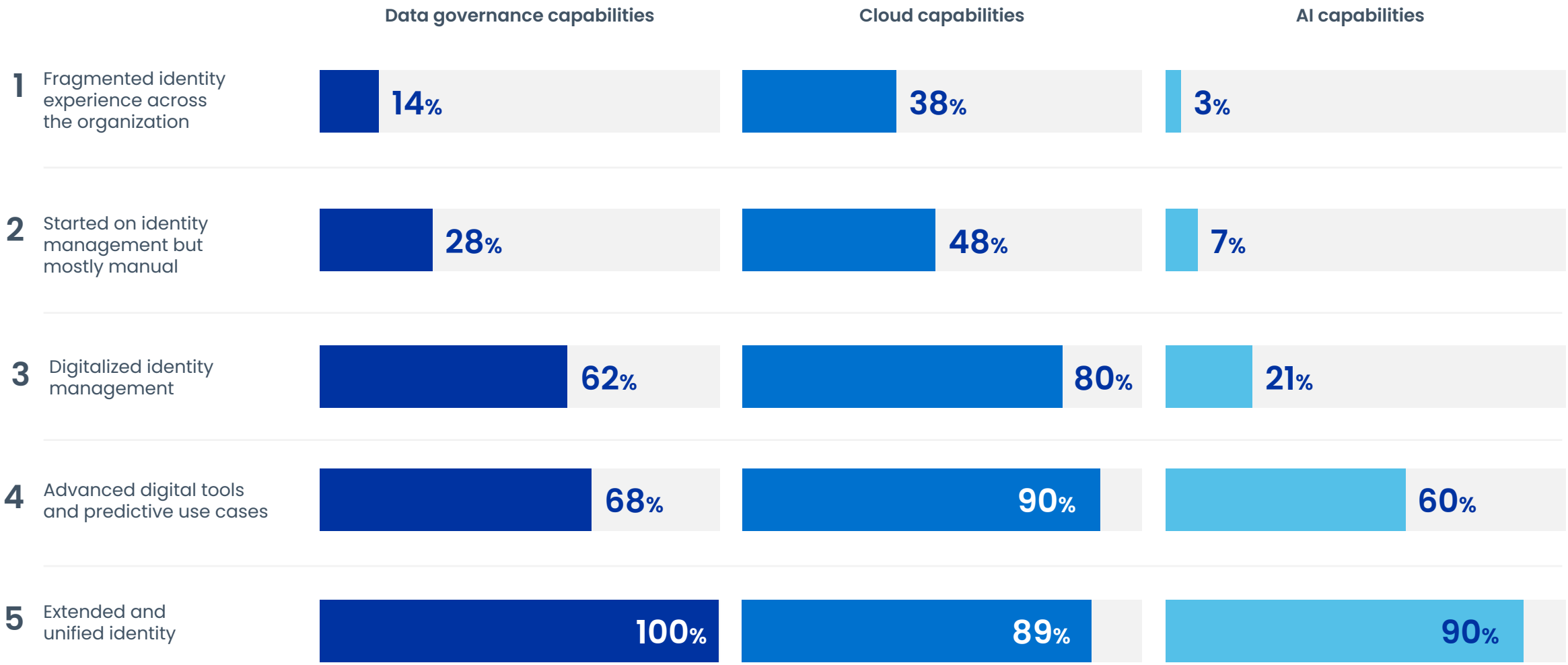
On a journey to the future of identity security



Improvement in security posture & resilience



Adoption of key capabilities



Where are you in your journey?

Question 1

Does your identity security program align to your overall business strategy, so that it is understood and utilized across your organization?

Rate the focus of identity security within your organization's strategy

Not a focus

We do not have an organization wide identity strategy.

Somewhat of a focus

There is a very low adoption rate and focus is usually a tactical response to external stresses (e.g., compliance, security breach or business transformation).

Identity is a focus

Our identity program is digitized and scaled with wide adoption across the organization.

A strong focus

Our identity program is a strong enabler for business transformation, innovation and security resilience.

A very strong focus

Our IAM strategy is a pillar of our broader organization's innovation strategy.

Question 2

Which one of the following options is the closest representation of your Identity and Access Management (IAM) team's operating model i.e., the way identity services are managed across your organization?

Rate the operating model of your Identity and Access Management (IAM) team

Not managed at all

Most forms of identities (e.g., employee, third parties, machines) are managed ad-hoc in silo-groups or not managed at all.

Somewhat managed

Identity management is mostly reactive and focused on fulfillment of service tickets, such as creating accounts.

Managed

Centralized IAM, organized based on specific tools (e.g., a team for directory services system or another team for identity governance tool).

Strongly managed

Centralized IAM, organized on a product operating model with agile teams, there is a continuous drive for automation and AI.

Very strongly managed

Our operating model enables collaboration with external entities, it is a key control point to engage with our workforce and customers.

Question 3

Which one of the following options is the closest representation of your organization's Identity and Access Management (IAM) teams' talent distribution?

Identify who manages the identity of your workforce

Helpdesk focused

Mostly helpdesk staff manages provisioning and deprovisioning access.

Helpdesk and IT focused

Composed of mostly helpdesk staff along with a general IT team who maintains some basic identity tools.

Identity tool centric team

Tool or product focused teams doing development on specific identity tools and supported by helpdesk and IT support staff.

Innovation focused identity team

Data scientist or automation engineers along with identity product engineers. Very lean helpdesk and IT support.

Distributed identity talent

Spans beyond the enterprise boundaries; there is collaboration with an ecosystem of other companies and other industry forums to enable distributed identity capabilities.

Question 4

How would you rate your organization's technical capabilities when adopting new identity tools?

Rate the capability of your organization to adopt new identity tools

Very limited capabilities

Either no tools or some legacy directory and access management tools.

Some capabilities

Some identity tools implemented but low adoption across the organization (e.g., some capabilities in pilot mode such as lifecycle management., access reviews, and Privilege Access Management but cover <50% of the organization).

Generally capable

Identity tools have been adopted across a majority of your organization.

Strong capabilities

Capabilities adopted at scale and integrated with SecOps – detection and response correlated with identity.

Very strong capabilities

In addition to having IAM capabilities adopted at scale and integrated with SecOps, your organization supports the future of identity. Can accept Universal IDs provided by institutions or decentralized IPs, dynamic trust models, identity integrated with security and data governance, frictionless access.

Question 5

Which most closely aligns to your IAM automation capabilities (e.g., account creation, access provisioning, access reviews)?

Rate the automation capabilities of your organization

Highly manual

Most if not all capabilities are manual (manual fulfillment of access, access reviews).

Some automation

Some capabilities are automated but the majority are performed manually.

Mostly automated

Automated IAM capabilities with 80%+ transactions automated (e.g., lifecycle mgmt., provisioning and deprovisioning of access). Additional capabilities such as Segregation of Duties and Privileged Access Management adopted at scale.

Highly automated

Highly automated capabilities with AI driving decisions based on risk estimation.

Question 6

How would you rate your organization's technical capabilities towards coverage of additional identities?

Rate the capability of your organization to cover additional identities

No coverage

No IAM program coverage of machine identities and environments such as cloud and SaaS applications.

Limited coverage

Limited coverage of additional identities such as machine identities. Environments such as cloud and SaaS apps are mostly manually managed.

Good coverage

Additional identities such as machine identities and environments such as cloud and SaaS applications are managed at scale and automated.

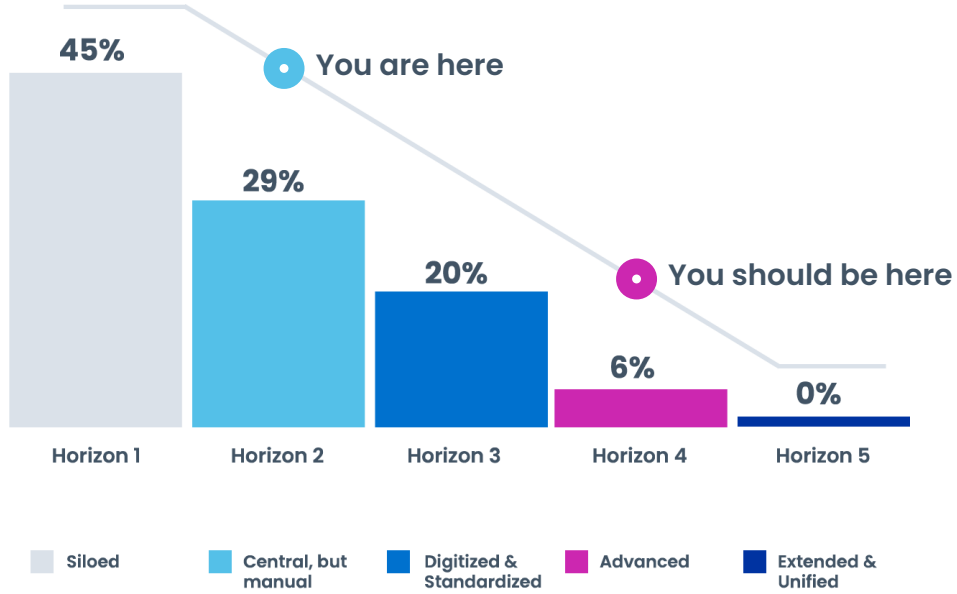
Very good coverage

Identity coverage spans most identities and environments are linked to data governance (structured and unstructured) and cloud workload level access.

Overall Assessment

Your identity program is Central, but Manual
Currently, the identity program gets some attention, but there is low adoption of technical capabilities and resources for the identity program are mostly based on tactical response to some external stress (i.e. regulatory)

You should be Advanced
The target state uses the identity program as a strategic enabler for business transformation, innovation, and security resilience. The identity program becomes widely adopted across the organization and many identity processes are automated.



% are total number of organizations in the study

Strategy

Currently, your identity strategy is formalized and owned by a central function. Metrics to measure IAM program impact are mostly ad-hoc or manual.

Recommendation

The target state requires that IAM strategy is formalized, owned by a central function, measured through automated tools and also that strategy feeds into innovation and other predictive capabilities.

Operational Model

Currently, your identity operations are centralized. The operating model is organized around specific tools, each tool for different functions and with different product teams.

Recommendation

The target state requires centralized identity operations to be organized on product operating model, with agile scrum teams. There will be a continuous push to automate and use analytics for IAM delivery.

Talent

Currently, your identity team is composed of tool/product security teams doing development on specific identity tools (e.g., tool specific developer team).

Recommendation

The target state requires an innovation focused identity team (e.g., data scientists, automation engineers) along with product engineers. There will be a very lean helpdesk and IT Support team.

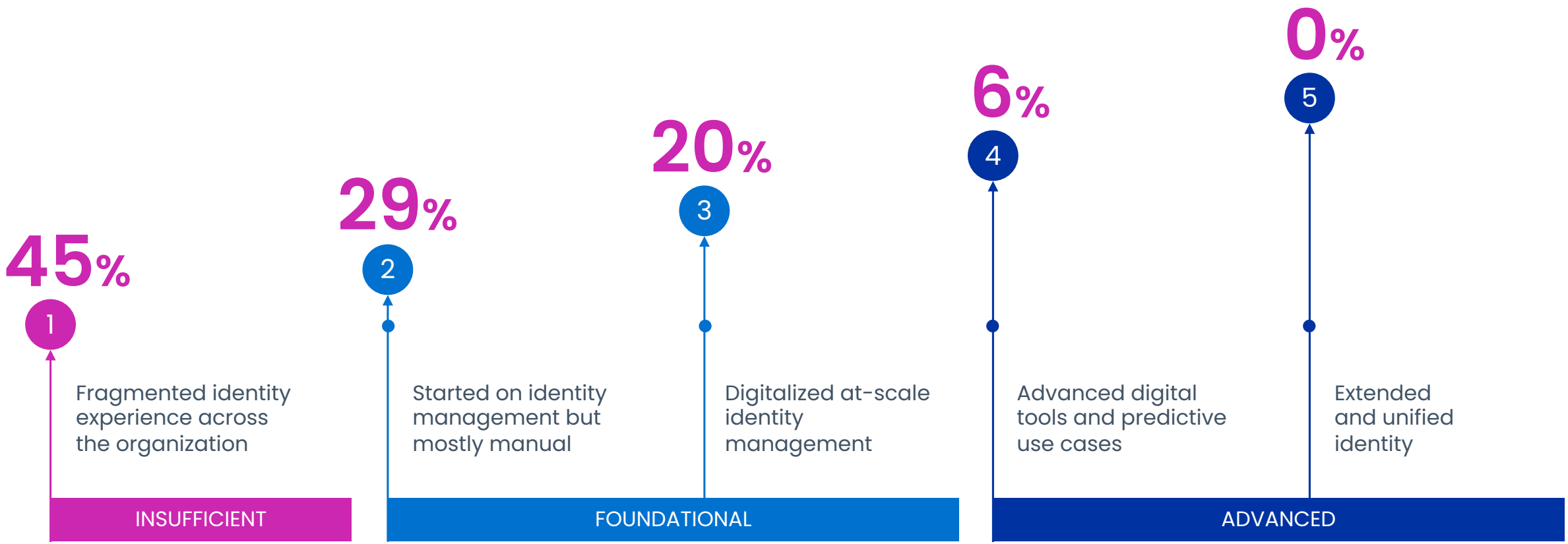
Tech Capabilities

Currently, you have identity tools adopted across the majority of your organization. These tools highly automated IAM needs with 80%+ transactions automated (e.g., lifecycle management, provisioning and deprovisioning of access). Machine identities are managed at scale.

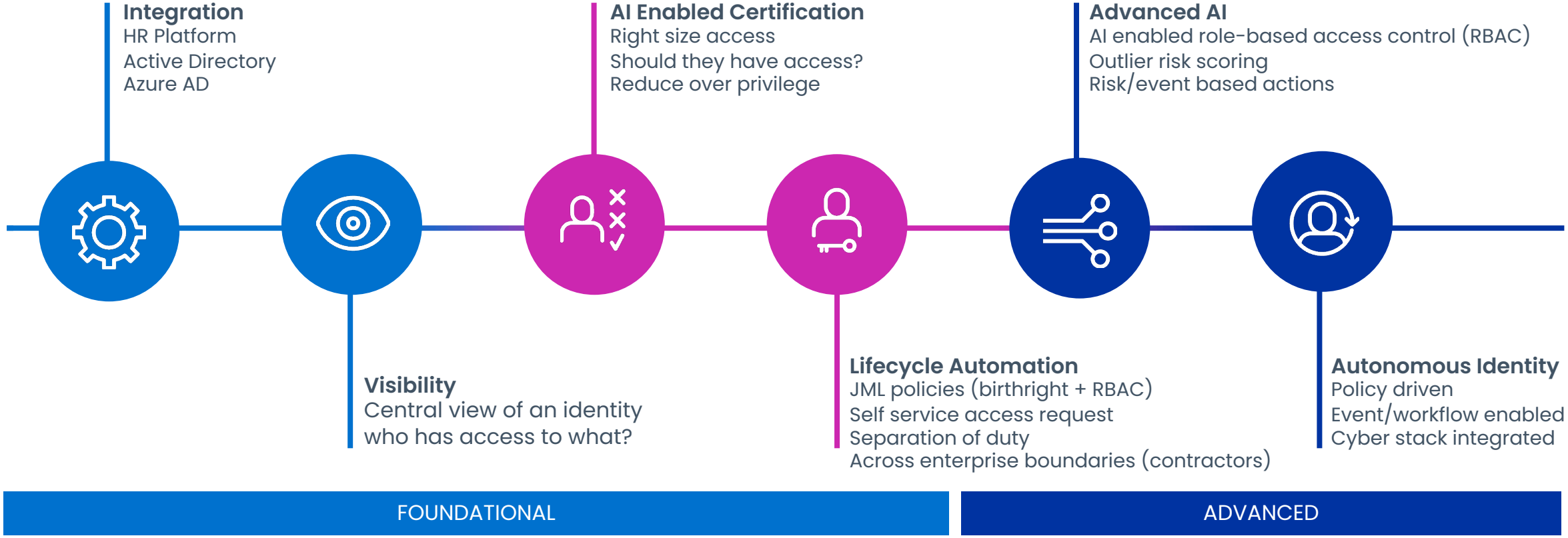
Recommendation

The target state requires you to adopt highly automated capabilities with AI driven risk models, integrate identity with SecOps and expand identity coverage to cover most identities and environments, and is linked to data governance and cloud workload level access.

On a journey to the future of identity security



Your path to Horizon 5 maturity



Path to the next horizon

1

Identify the outcomes worthy of investment

2

Bring the whole organization along the journey

3

Choose a transformation path

Call to Action

Complete the Maturity Assessment

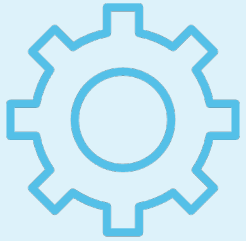
Organise an Exploratory Call

Set up a Maturity Assessment Workshop

Business Value Assessment

Multiple benefits beyond cost justification

Assess current state and benchmark KPI's against peers



Elevate executive and business stakeholder engagement

Prioritize pain points and use cases for implementation

Identity security is critical to business strategy

	Business Strategy	Identity Security Program
Application Access Risk	Improve general IT controls (GITCs) to prevent inappropriate access to IT applications as the organization grows	Manage identities across expanding ecosystem of applications and ensure seamless integration of controls during M&A
Regulatory Compliance	Adhere to new operational resilience requirements for UK financial services firms	Manage and enforce SoD policies while ensuring audit readiness to comply with operational impact tolerances
Bottom Line Improvement	Deliver cost efficiency and profitability to meet 2019 growth strategy goal of £100M in net cost savings	Automate arduous workflows and enable seamless access using artificial intelligence to drive employee productivity
Physical Footprint Reduction	Reducing physical footprint by closing 153 branches in 2021 and 70 in 2022 to drive higher digital adoption	Minimize security risk and improve operational efficiency associated with role changes and terminations

Thank You!