Interactive Book

2024-2025

The Horizons of Identity Security

Harnessing the power of identity security to bend the cybersecurity value curve

Get started →

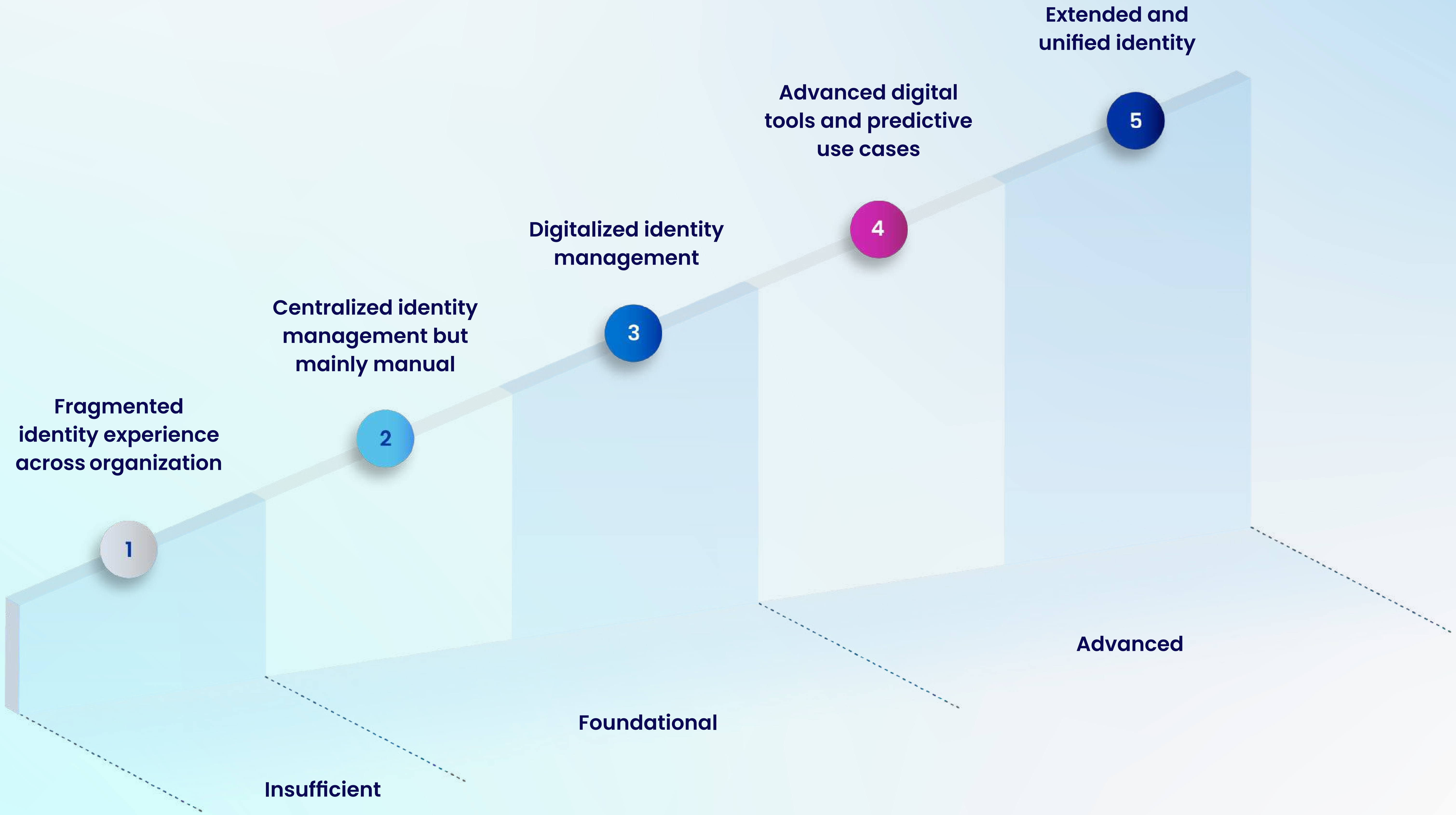
Take the journey to higher identity security maturity

Organizations across sectors around the world face a dual challenge: they must counter increasingly sophisticated and pervasive cyber threats while grappling with constrained budgets and relentless cost-cutting.

The pressures are especially intense in identity security, where attack surfaces grow and IT budgets tighten as organizations scale, yet internal and external stakeholders increasingly demand better security and digital experiences.

Over the last three years, SailPoint has surveyed identity and access management (IAM) decision-makers across the globe to assess their capabilities across 5 identity security horizons. The 350 decision-makers we surveyed in July 2024 included senior leaders in information technology, cybersecurity, and risk; more than half work for organizations with more than 10,000 employees, and more than half work in the finance or technology sectors.

Source: All charts in this document are from **The Horizons of Identity Security 2024-2025 report.**


Extended and unified identity
5
Advanced digital tools and predictive use cases
4
Digitalized identity management
3
Centralized identity management but mainly manual
2
Fragmented identity experience across organization
1
Advanced
Foundational
Insufficient

CHAPTER 1

Advances in technology will shape the future of identity security.

Begin chapter →

The future of identity will be defined by 4 key elements

In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs.

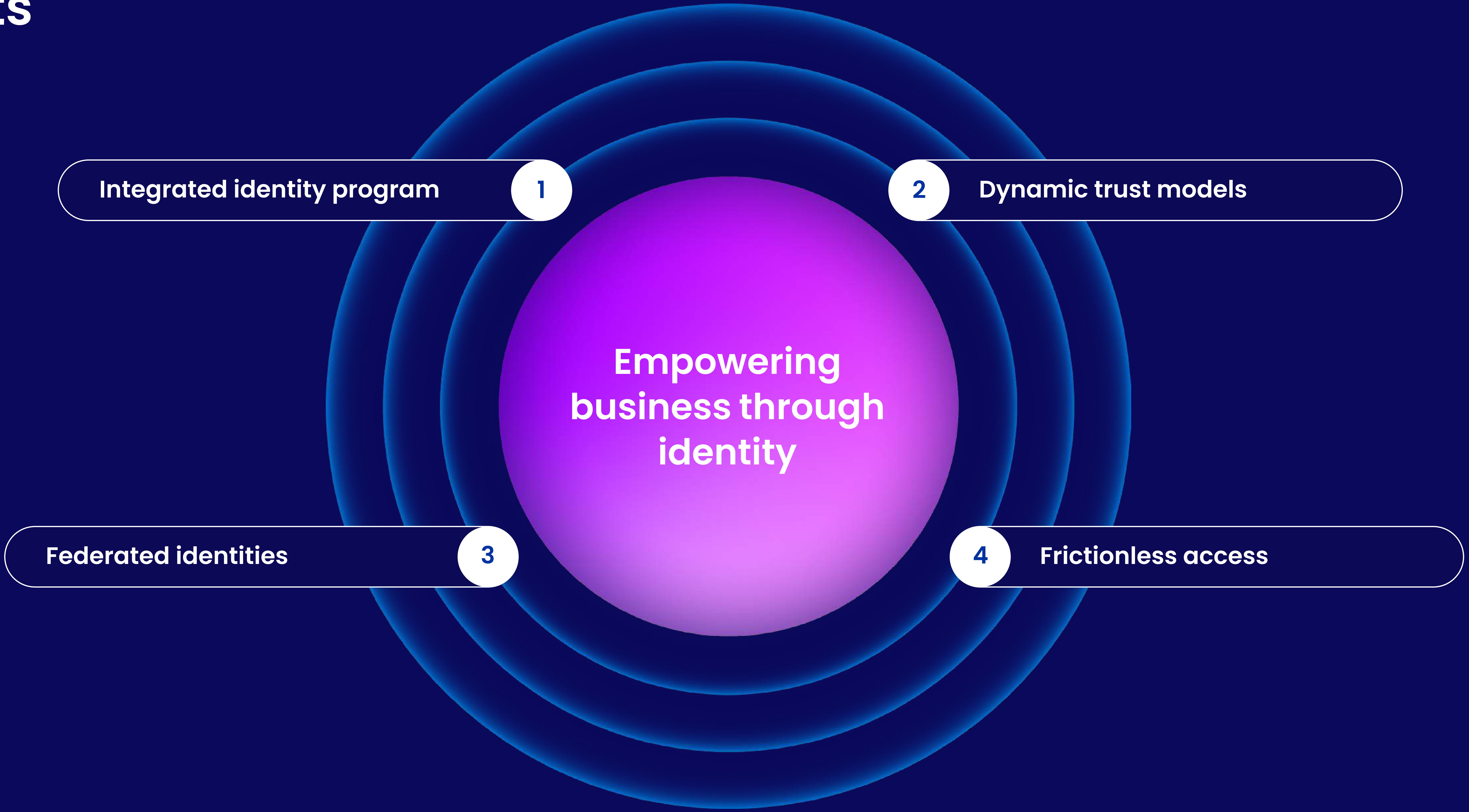
Key elements are shown here along with the trends that complement these elements.

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations.

Proliferation of identity security related regulations and industry standards across the globe and across industries will drive increased expectations on identity security.

● 2024 addition ● Nascent ● Emerging ● Mainstream


Integrated identity program 1
2 Dynamic trust models
Empowering business through identity
Federated identities 3
4 Frictionless access

The future of identity will be defined by 4 key elements

In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs.

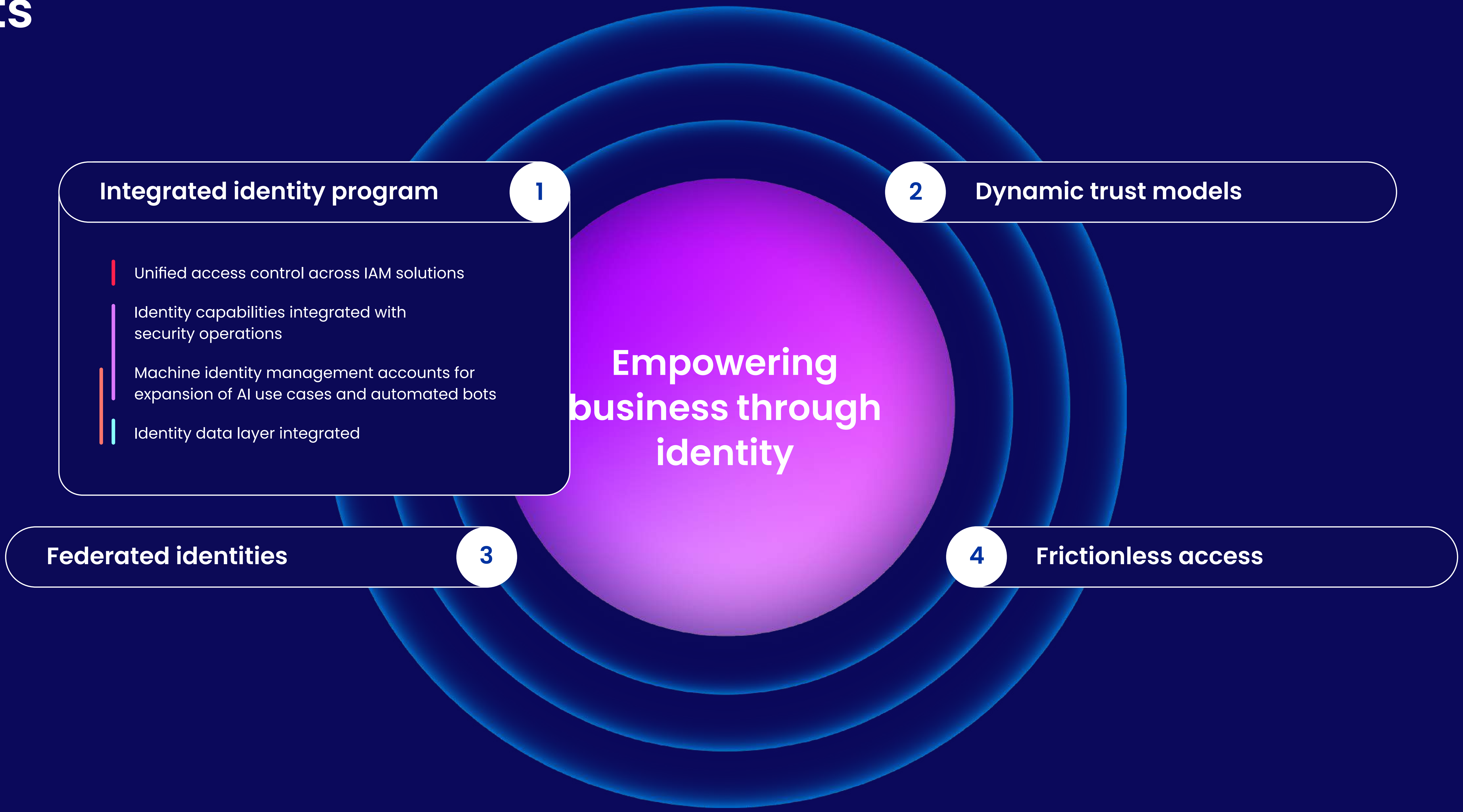
Key elements are shown here along with the trends that complement these elements.

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations.

Proliferation of identity security related regulations and industry standards across the globe and across industries will drive increased expectations on identity security.

● 2024 addition ● Nascent ● Emerging ● Mainstream



Empowering business through identity

1 Integrated identity program

- Unified access control across IAM solutions
- Identity capabilities integrated with security operations
- Machine identity management accounts for expansion of AI use cases and automated bots
- Identity data layer integrated

2 Dynamic trust models

3 Federated identities

4 Frictionless access

The future of identity will be defined by 4 key elements

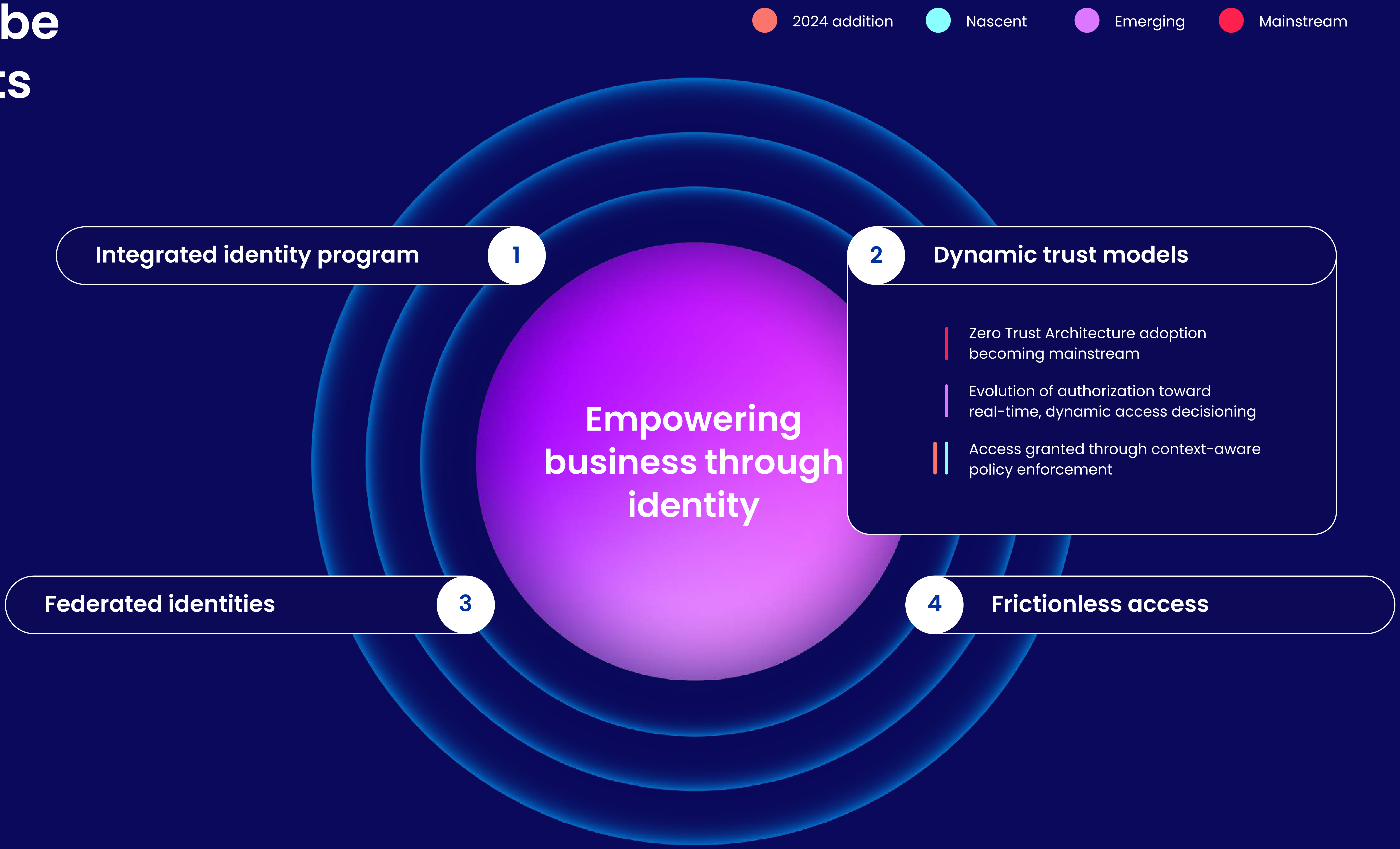
In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs.

Key elements are shown here along with the trends that complement these elements.

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations.

Proliferation of identity security related regulations and industry standards across the globe and across industries will drive increased expectations on identity security.



● 2024 addition ● Nascent ● Emerging ● Mainstream

Empowering business through identity

1 Integrated identity program

2 Dynamic trust models

- Zero Trust Architecture adoption becoming mainstream
- Evolution of authorization toward real-time, dynamic access decisioning
- Access granted through context-aware policy enforcement

3 Federated identities

4 Frictionless access

The future of identity will be defined by 4 key elements

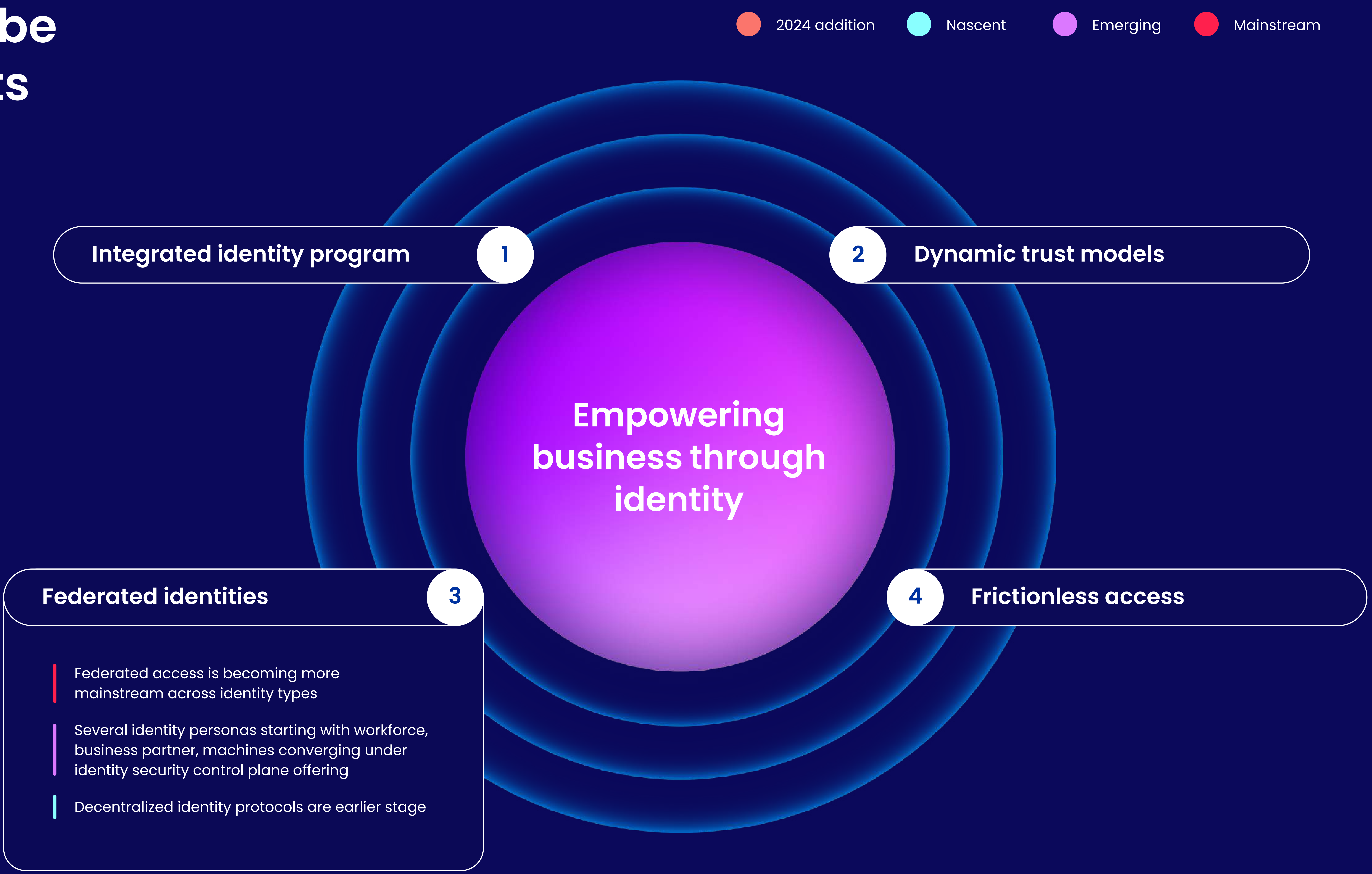
In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs.

Key elements are shown here along with the trends that complement these elements.

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations.

Proliferation of identity security related regulations and industry standards across the globe and across industries will drive increased expectations on identity security.



● 2024 addition ● Nascent ● Emerging ● Mainstream

Empowering business through identity

1 Integrated identity program

2 Dynamic trust models

3 Federated identities

- Federated access is becoming more mainstream across identity types
- Several identity personas starting with workforce, business partner, machines converging under identity security control plane offering
- Decentralized identity protocols are earlier stage

4 Frictionless access

The future of identity will be defined by 4 key elements

In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs.

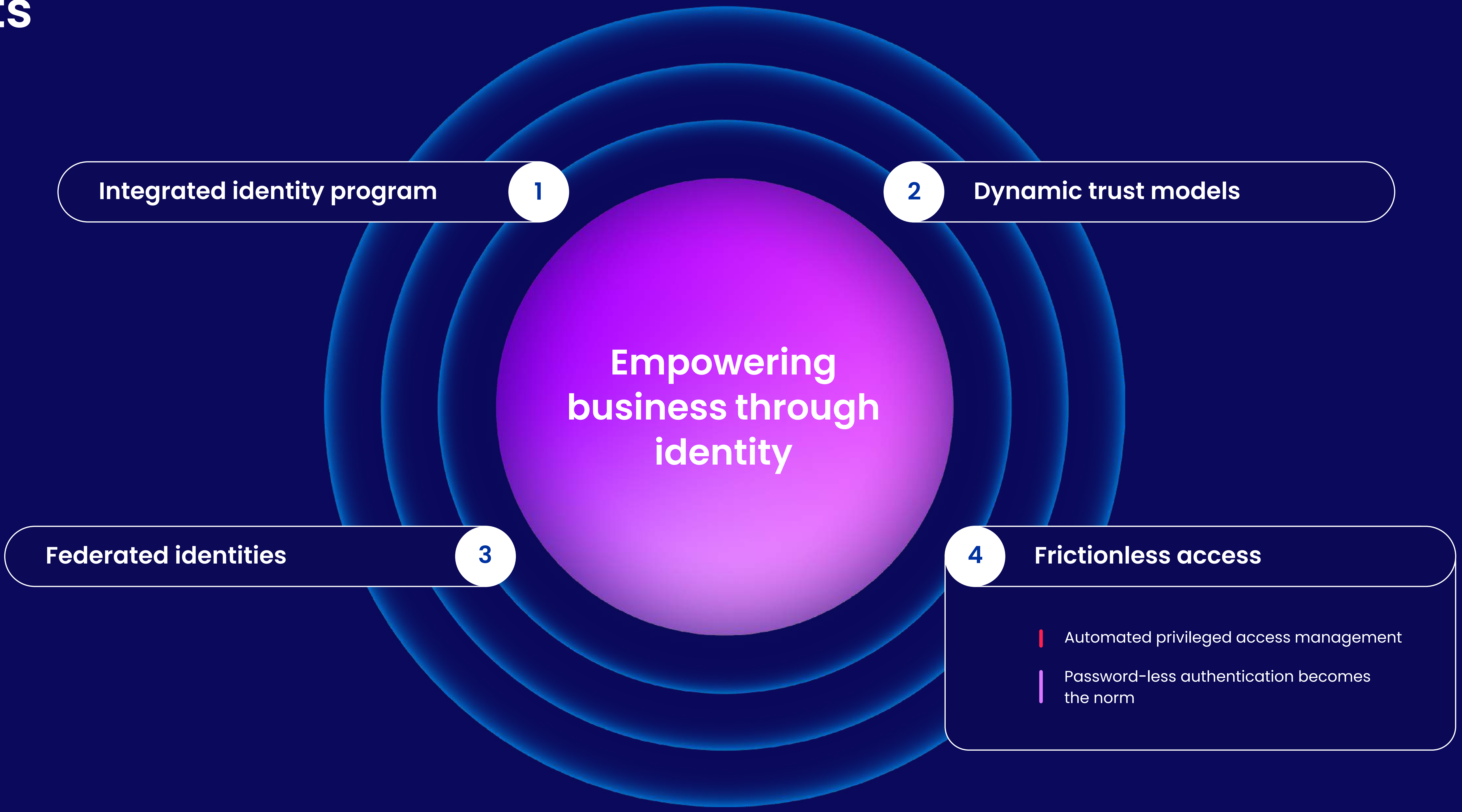
Key elements are shown here along with the trends that complement these elements.

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations.

Proliferation of identity security related regulations and industry standards across the globe and across industries will drive increased expectations on identity security.

● 2024 addition ● Nascent ● Emerging ● Mainstream


Integrated identity program
1
2
Dynamic trust models
Empowering business through identity
Federated identities
3
4
Frictionless access

Automated privileged access management

Password-less authentication becomes the norm

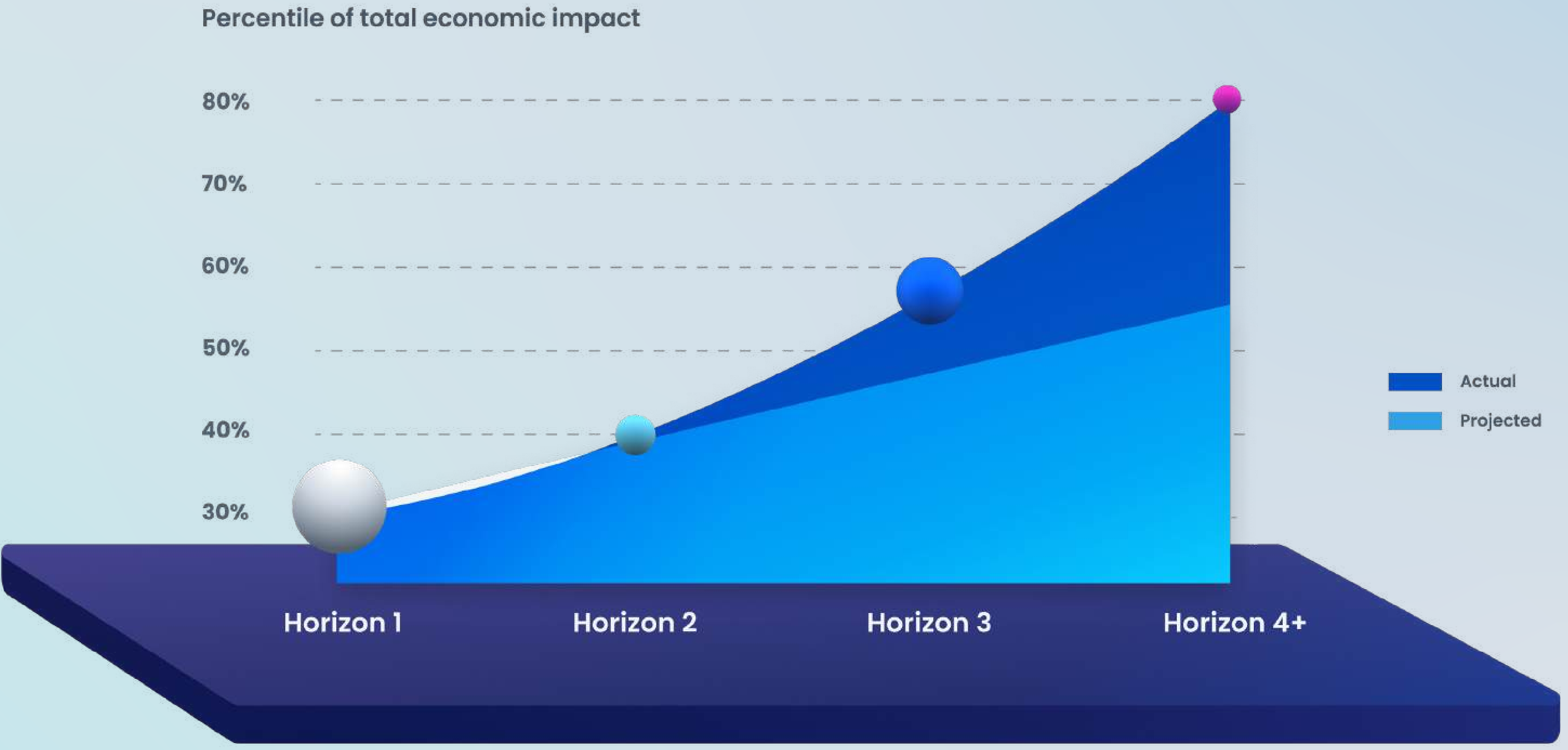
CHAPTER 2

Investments in identity security can "bend the curve."

Begin chapter →

Organizations with mature identity security deliver disproportionately higher returns for every dollar spent

Leapfrogging to Horizons 3 and 4 has an outsized business impact in identity security – “bending the curve” exponentially.



*Sphere diameter indicates horizon distribution

Value curve

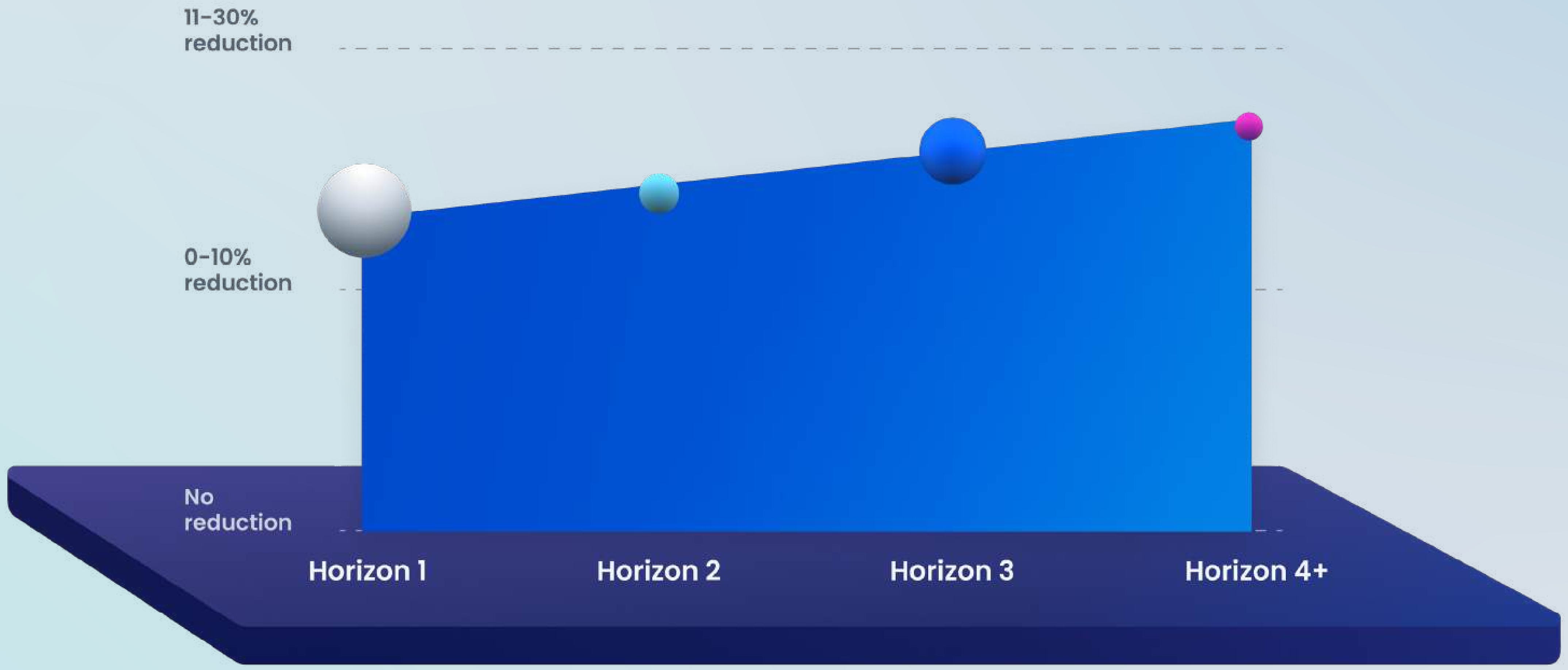
Risk reduction

Business value

Productivity

Moving through identity security horizons reduces the attack surface for potential breaches

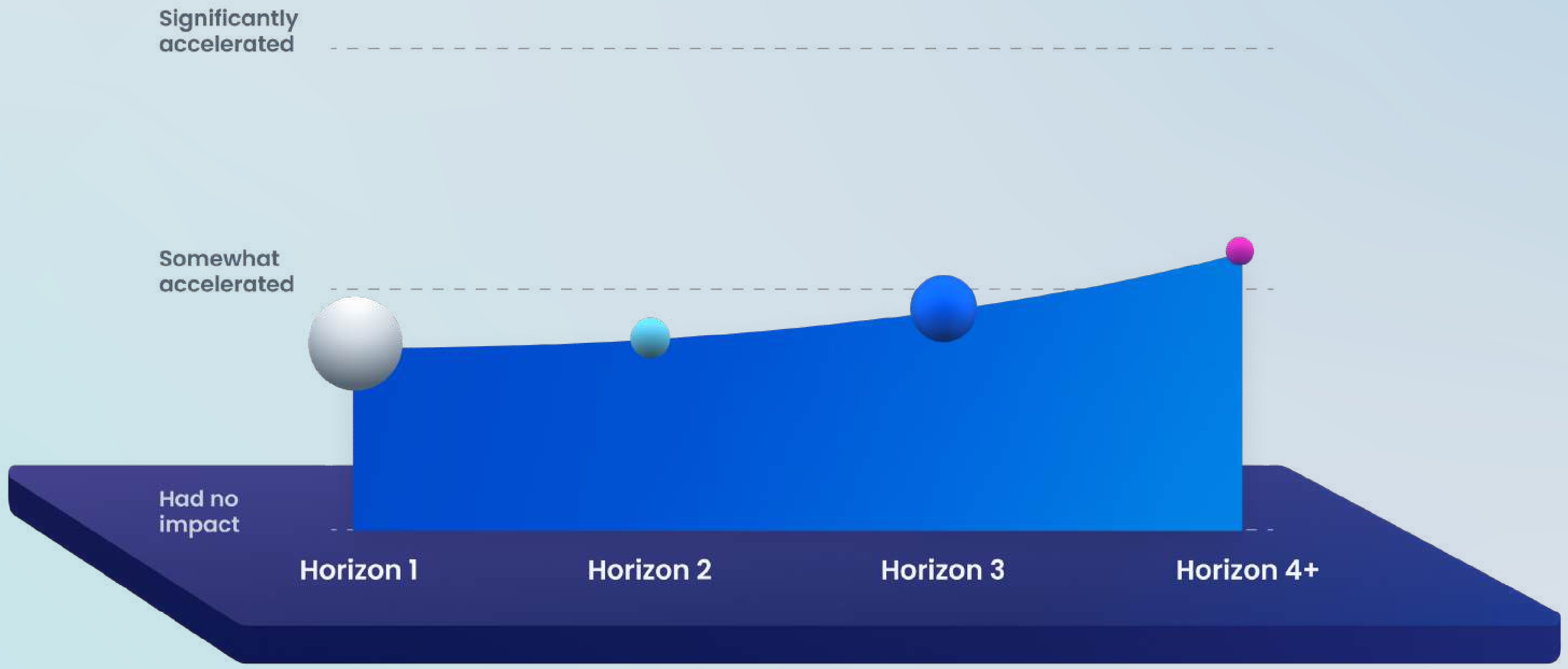
83% of organizations reported fewer identity-related security issues due to their identity security investments in 2023.



*Sphere diameter indicates horizon distribution

Organizations with advanced identity capabilities experience faster time to market and reduced friction

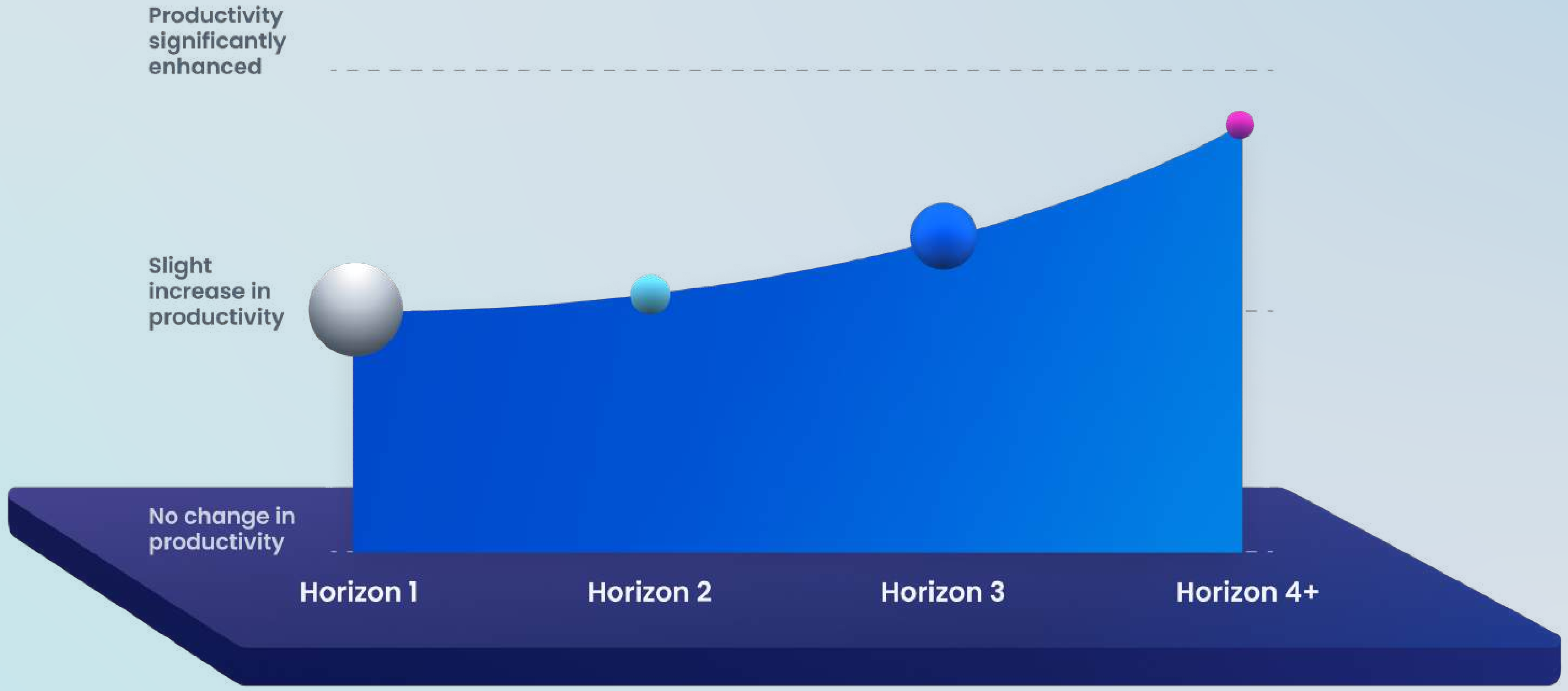
Drive top line revenue: Advanced identity security accelerates digital transformation, enabling faster development cycles and speed to market, increasing revenue.



*Sphere diameter indicates horizon distribution

Horizons 3 & 4+ organizations are likely to see significant productivity gains

Horizon 4+ organizations see significant productivity enhancements driven by an integrated identity security approach, and adoption of **emerging use cases**, such as copilots for guidance, services for end users, and automated user access approval granting.



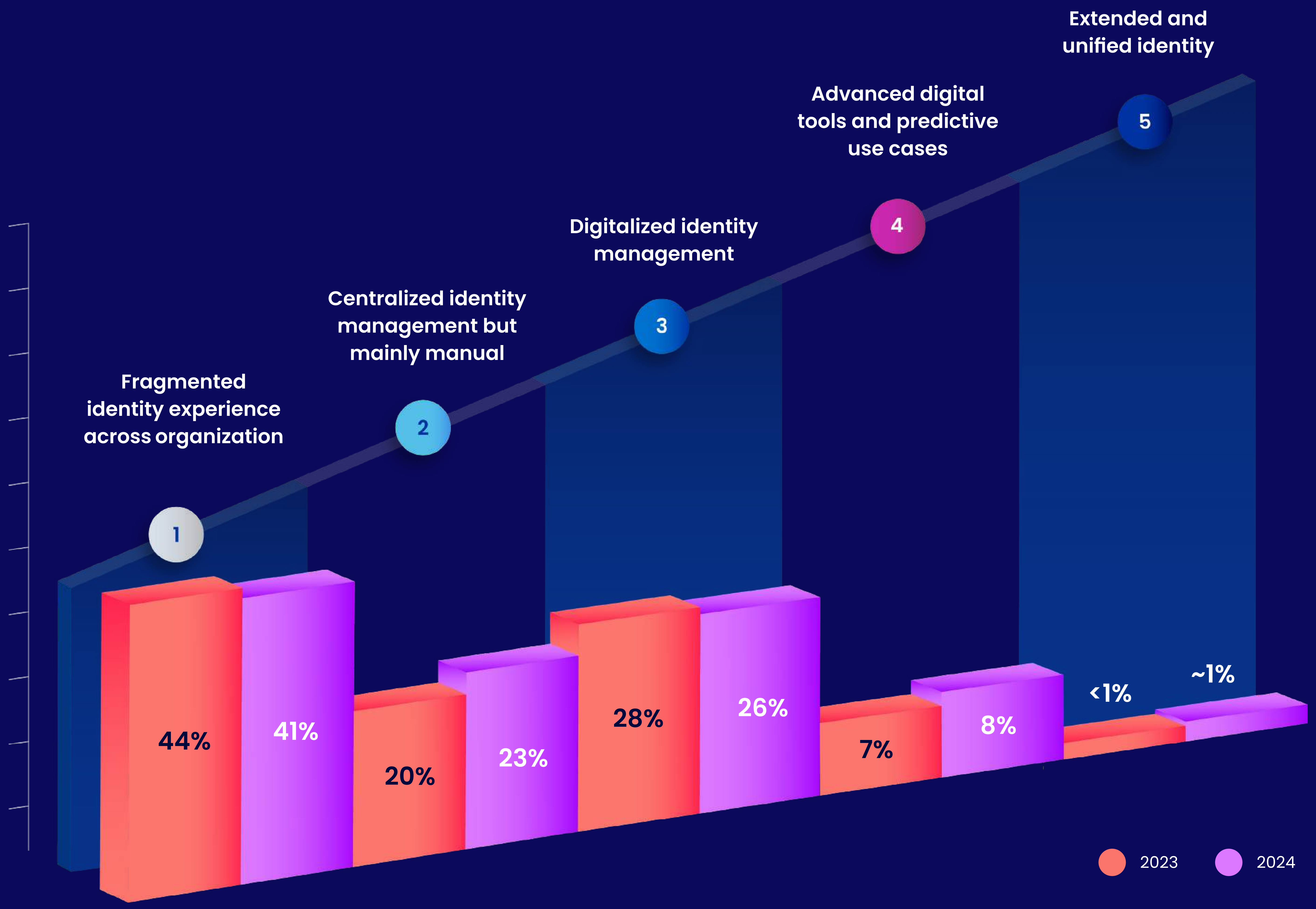
*Sphere diameter indicates horizon distribution

CHAPTER 3

Where organizations are in their journeys and why mature organizations have higher returns.

Begin chapter →

With 41% of organizations still in Horizon 1, significant opportunity exists to unlock the "full potential" of identity security



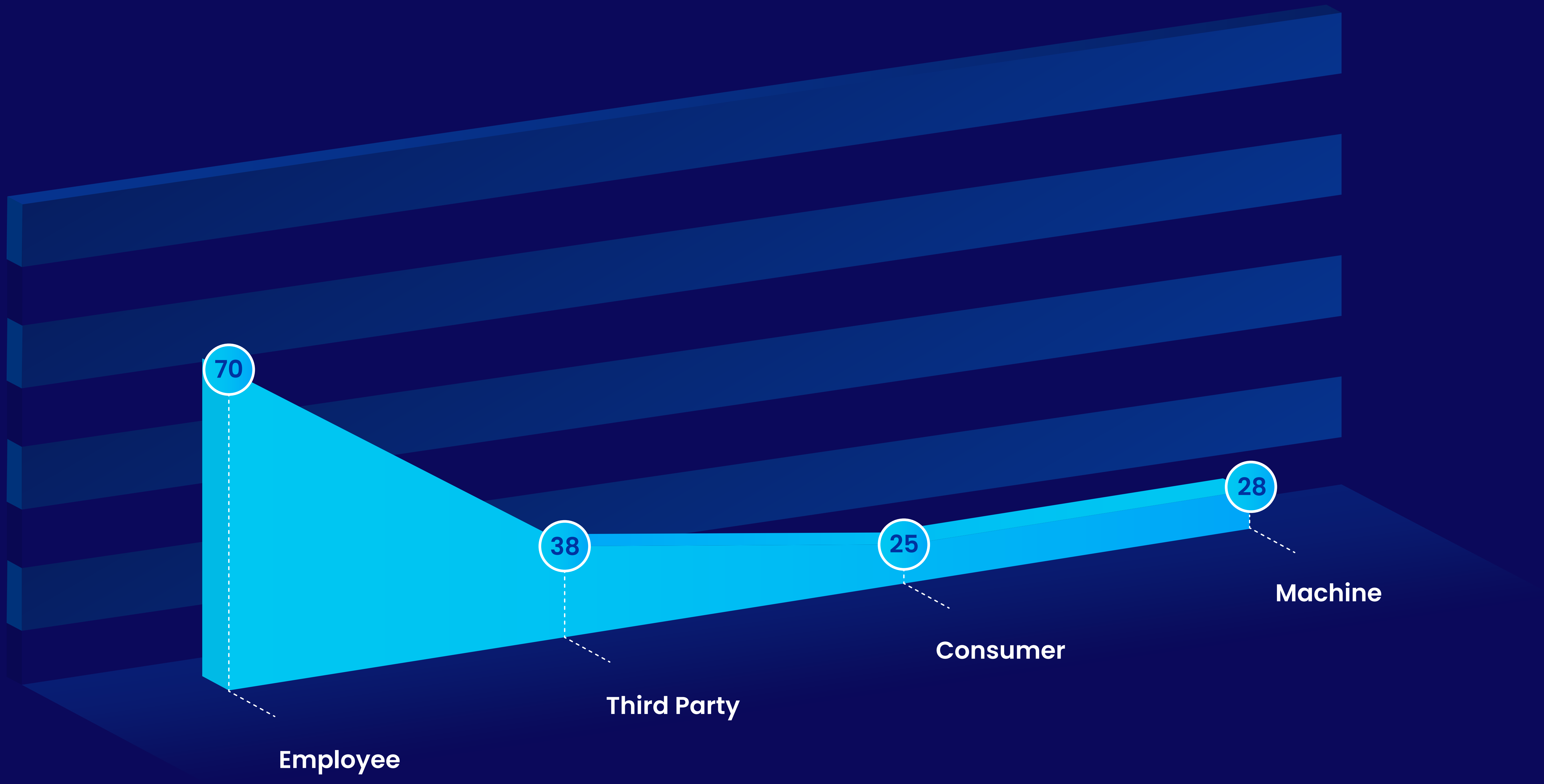
Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

Horizon 1 and 2 organizations, have a **big gap in identity coverage.** The following are currently **not governed.**

30%	62%	72%
Employees	Third parties	Machine identities

The latter being especially concerning given the fact that machine identities typically comprise ~40-65% of total identities across an organization.

Horizon 1-2 Horizon 3 Horizon 4+ Overall All data



Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

Horizon 1 and 2 organizations,
have a **big gap in identity coverage.**
The following are currently **not governed.**

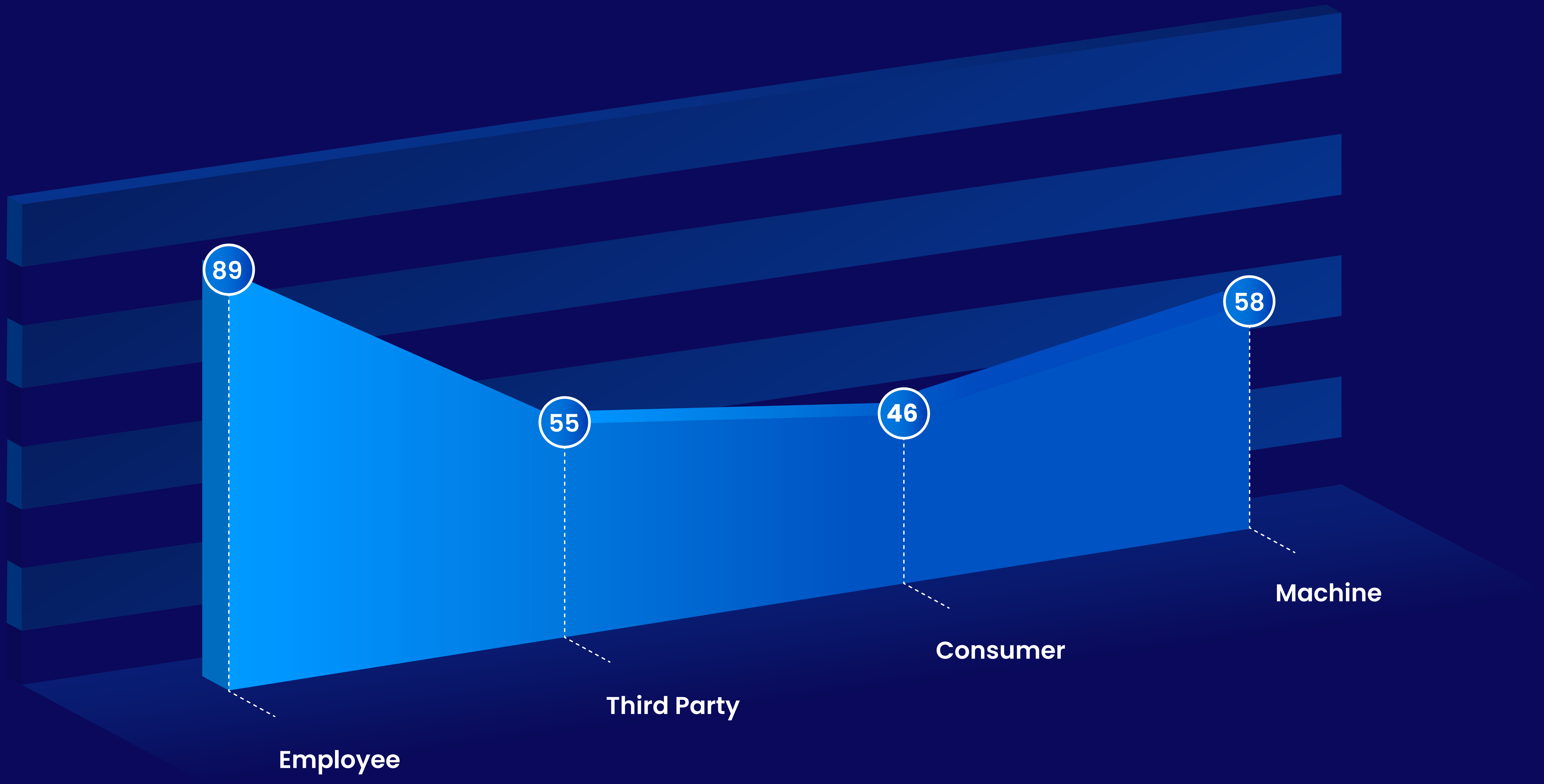
30% Employees

62% Third parties

72% Machine identities

The latter being especially concerning given the fact that machine identities typically comprise ~40-65% of total identities across an organization.

Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | All data



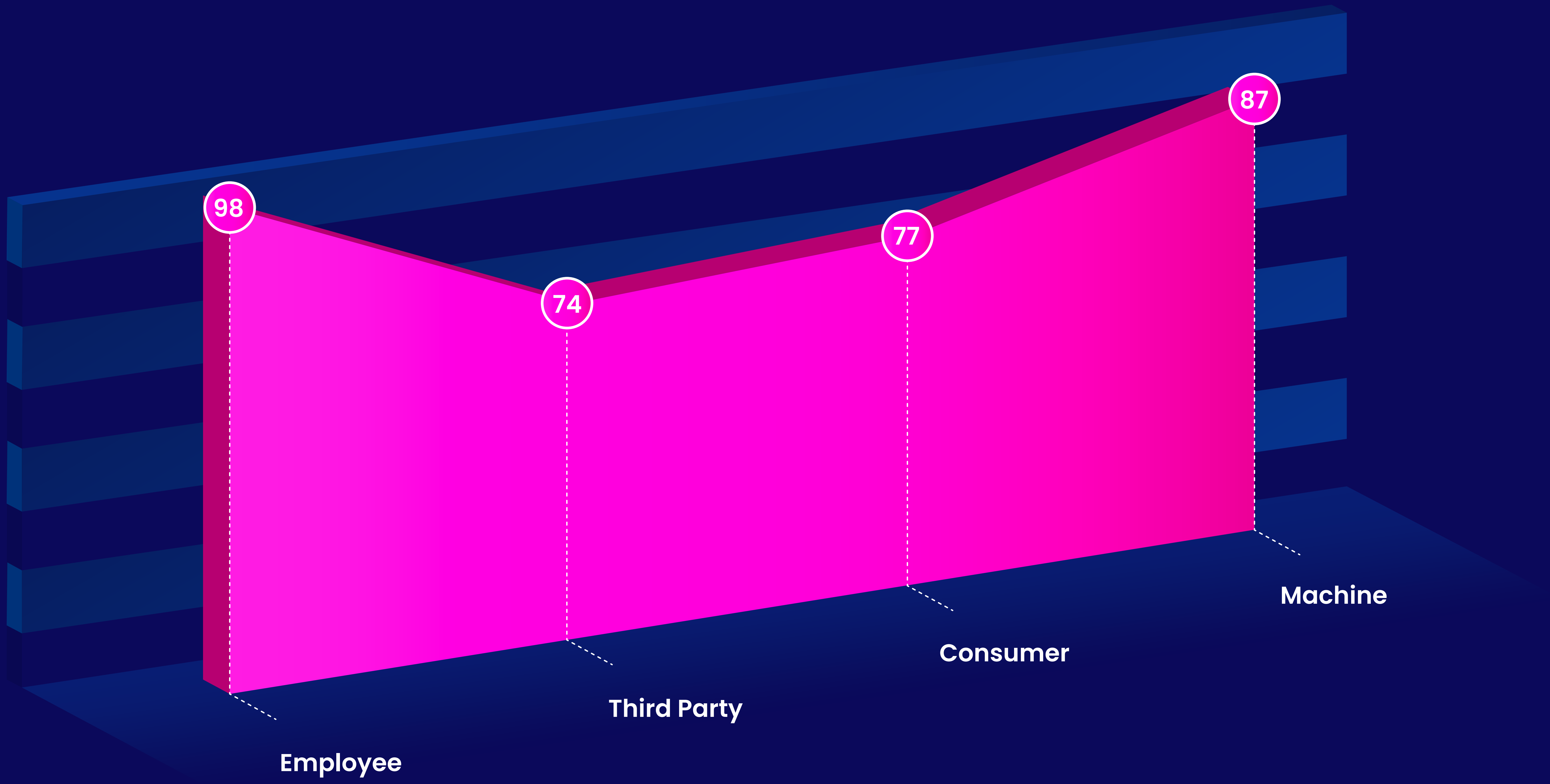
Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

Horizon 1 and 2 organizations,
have a **big gap in identity coverage.**
The following are currently **not governed.**

30%	62%	72%
Employees	Third parties	Machine identities

The latter being especially concerning given the fact that machine identities typically comprise ~40-65% of total identities across an organization.

Horizon 1-2 Horizon 3 Horizon 4+ Overall All data



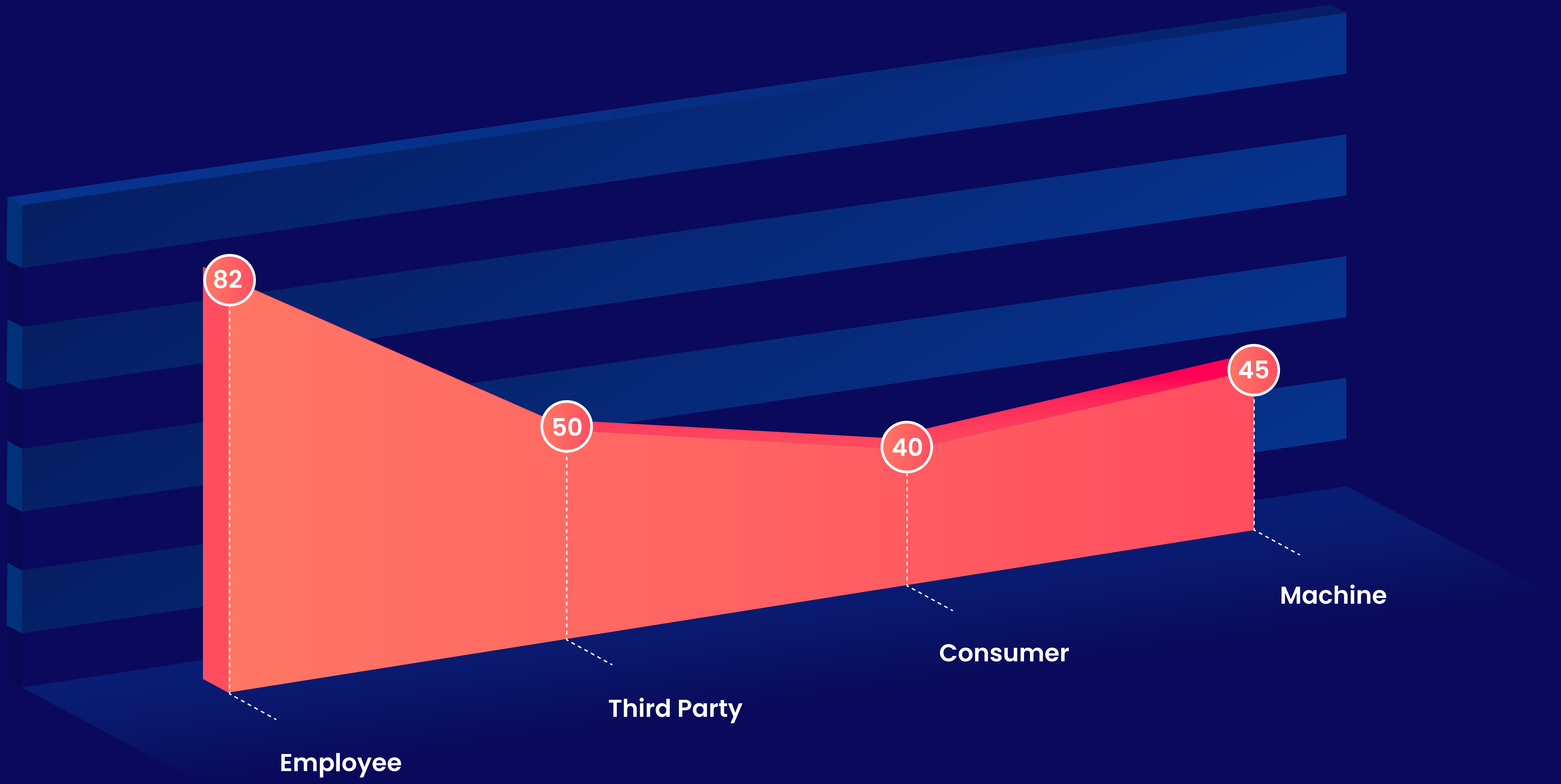
Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

Horizon 1 and 2 organizations, have a **big gap in identity coverage.** The following are currently **not governed.**

30%	62%	72%
Employees	Third parties	Machine identities

The latter being especially concerning given the fact that machine identities typically comprise ~40-65% of total identities across an organization.

Horizon 1-2 Horizon 3 Horizon 4+ Overall All data



Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

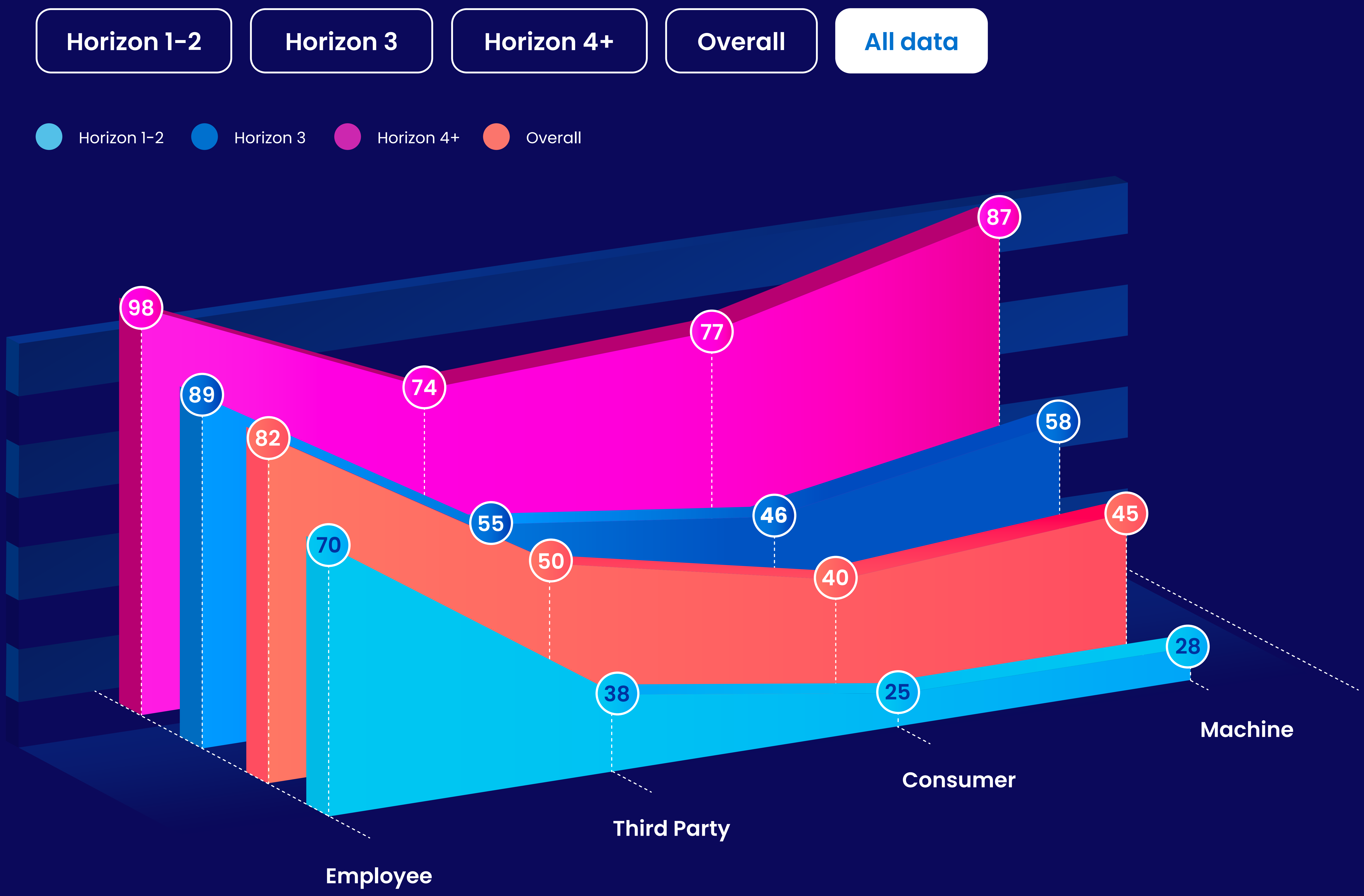
Horizon 1 and 2 organizations, have a **big gap in identity coverage.** The following are currently **not governed.**

30% Employees

62% Third parties

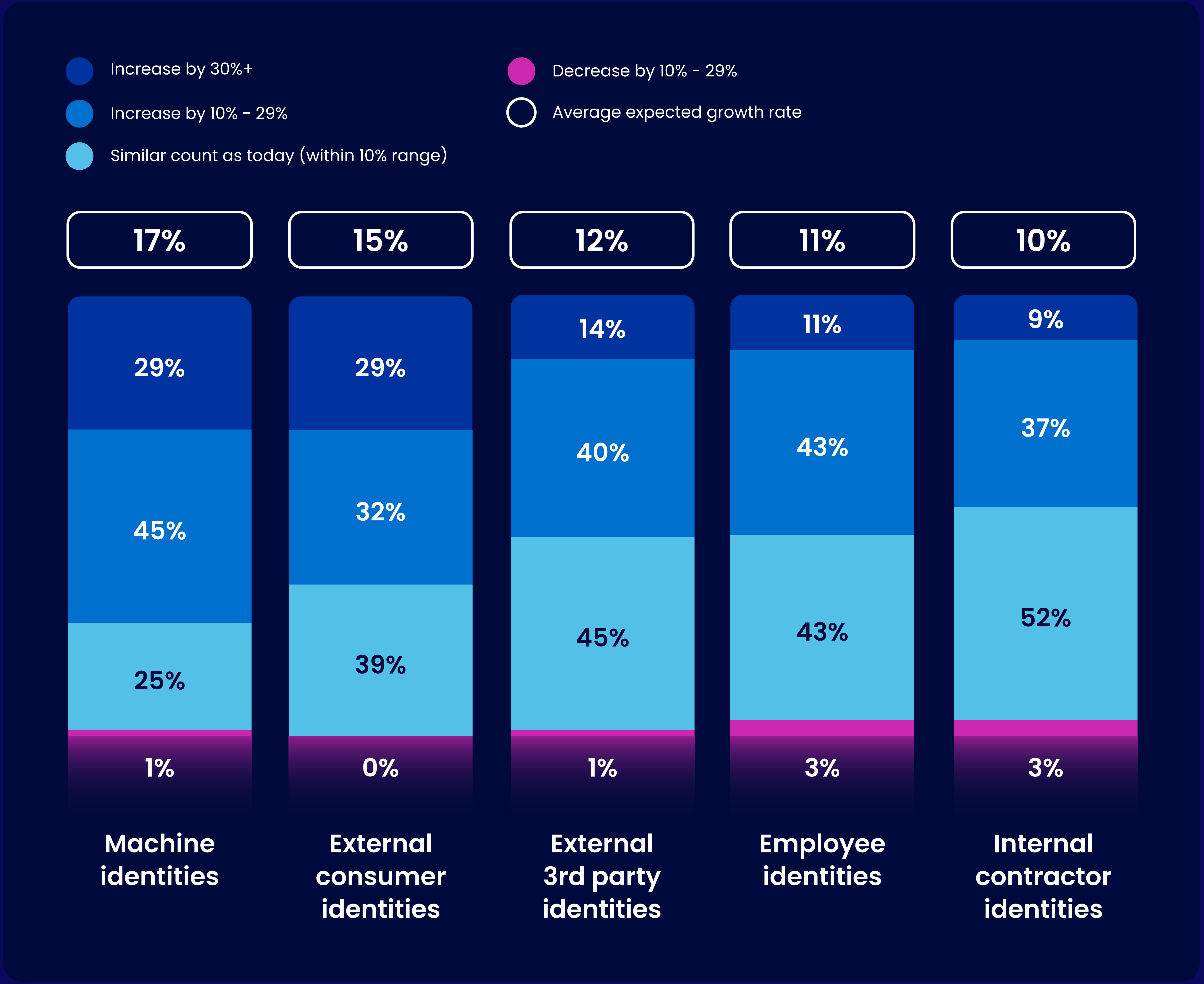
72% Machine identities

The latter being especially concerning given the fact that machine identities typically comprise ~40-65% of total identities across an organization.

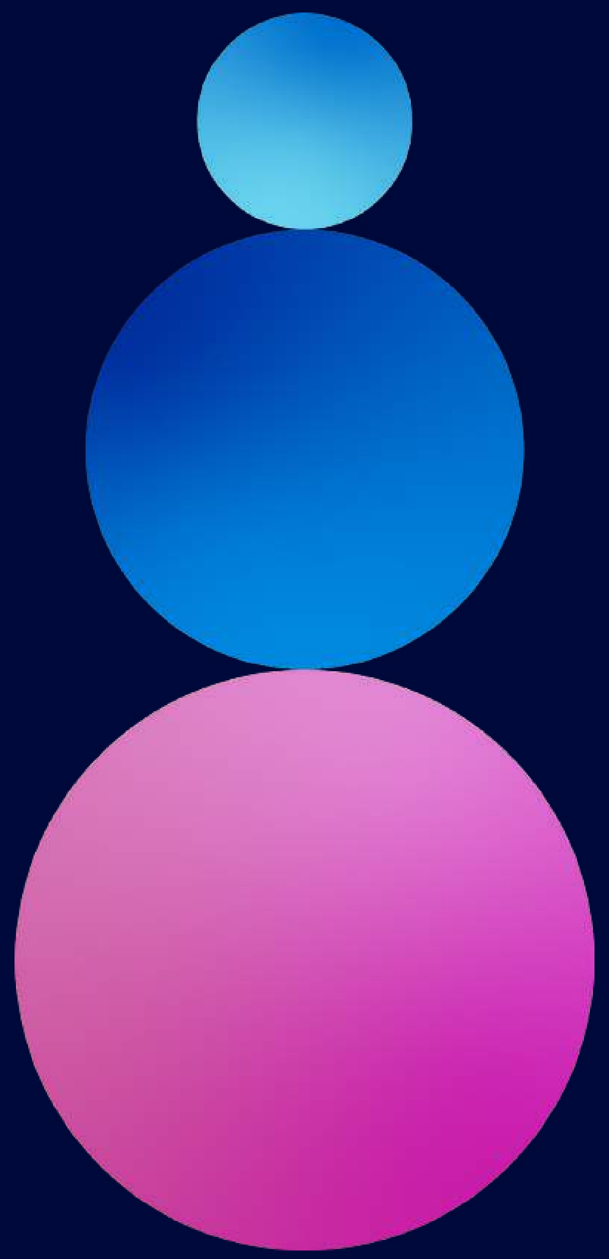


All identities are expected to grow roughly 14% in the next 3-5 years, with machine identities growing the fastest

Growth in **machine identities** may outpace growth in human identities.



Horizon 4+ organizations are twice as likely to use identity data for actionable intelligence and new use cases



<20%

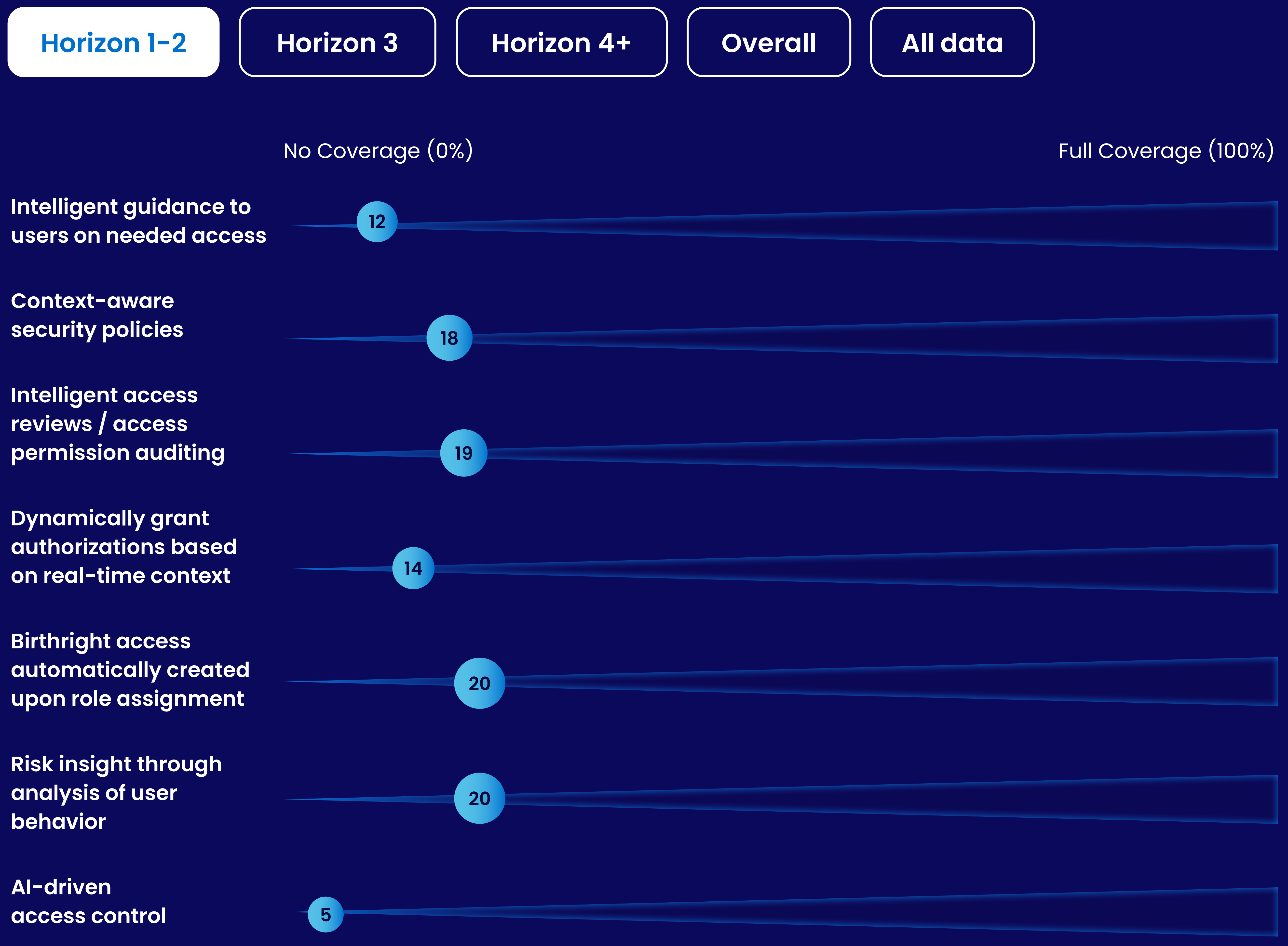
of Horizon 1-2 organizations leverage identity intelligence data at scale

<40%

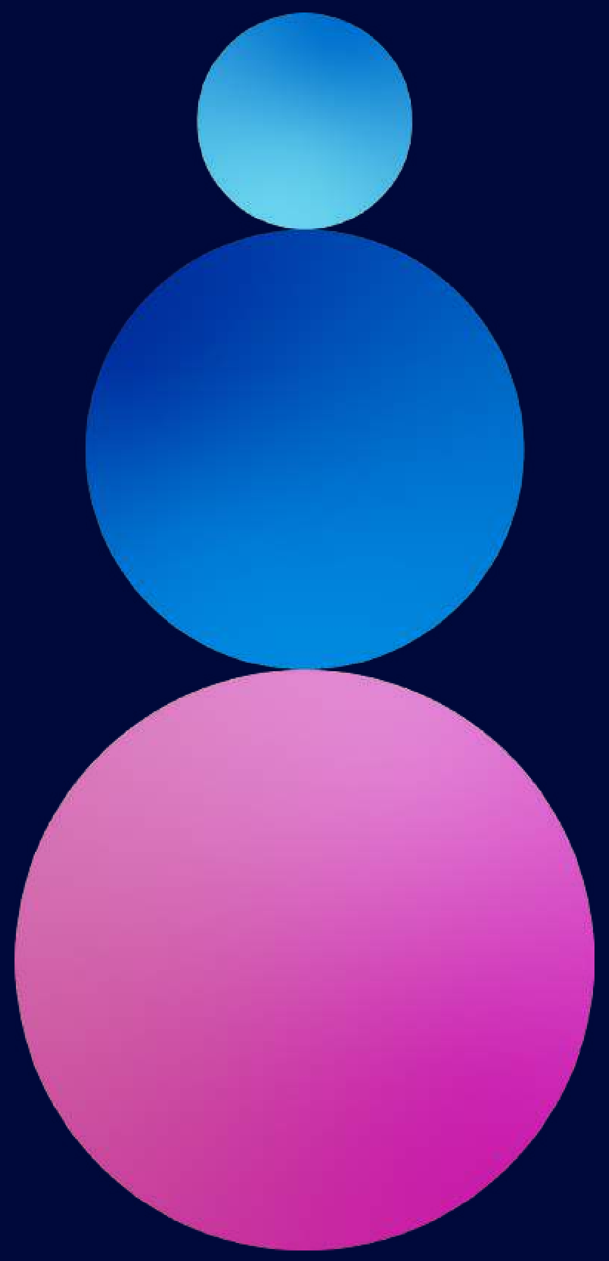
of Horizon 3 organizations leverage identity intelligence data at scale

~50%

Horizon 4+ organizations use intelligent guidance from structured and unstructured data for user access, security policies, and access reviews



Horizon 4+ organizations are twice as likely to use identity data for actionable intelligence and new use cases



<20%

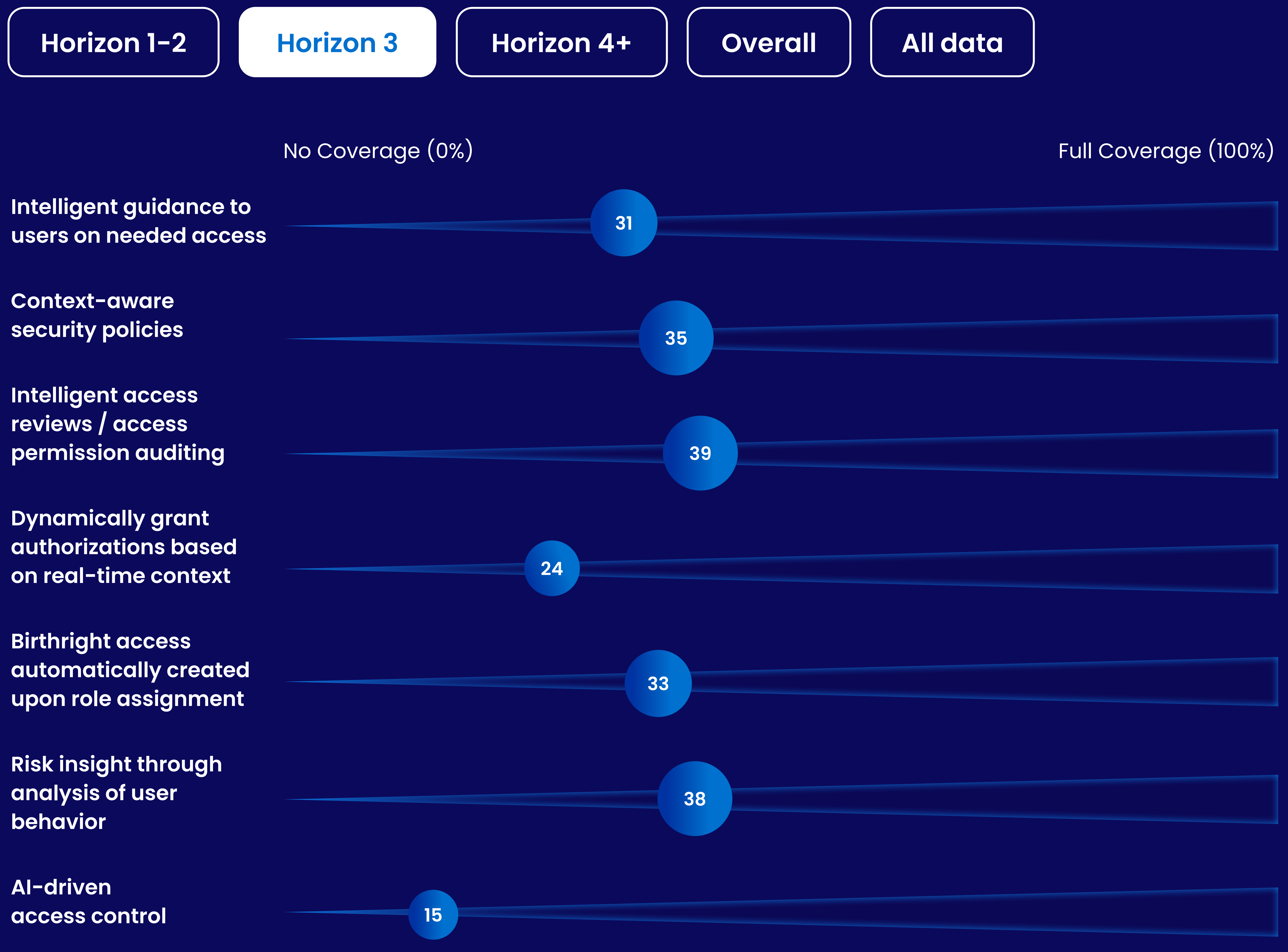
of Horizon 1-2 organizations leverage identity intelligence data at scale

<40%

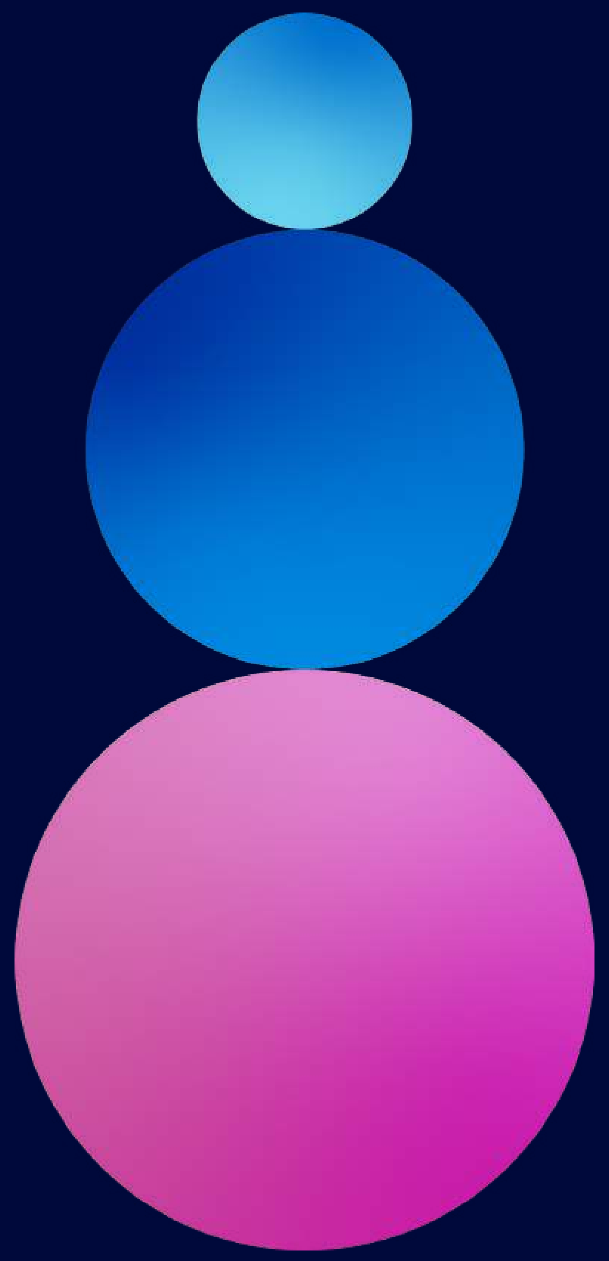
of Horizon 3 organizations leverage identity intelligence data at scale

~50%

Horizon 4+ organizations use intelligent guidance from structured and unstructured data for user access, security policies, and access reviews



Horizon 4+ organizations are twice as likely to use identity data for actionable intelligence and new use cases



<20%

of Horizon 1-2 organizations leverage identity intelligence data at scale

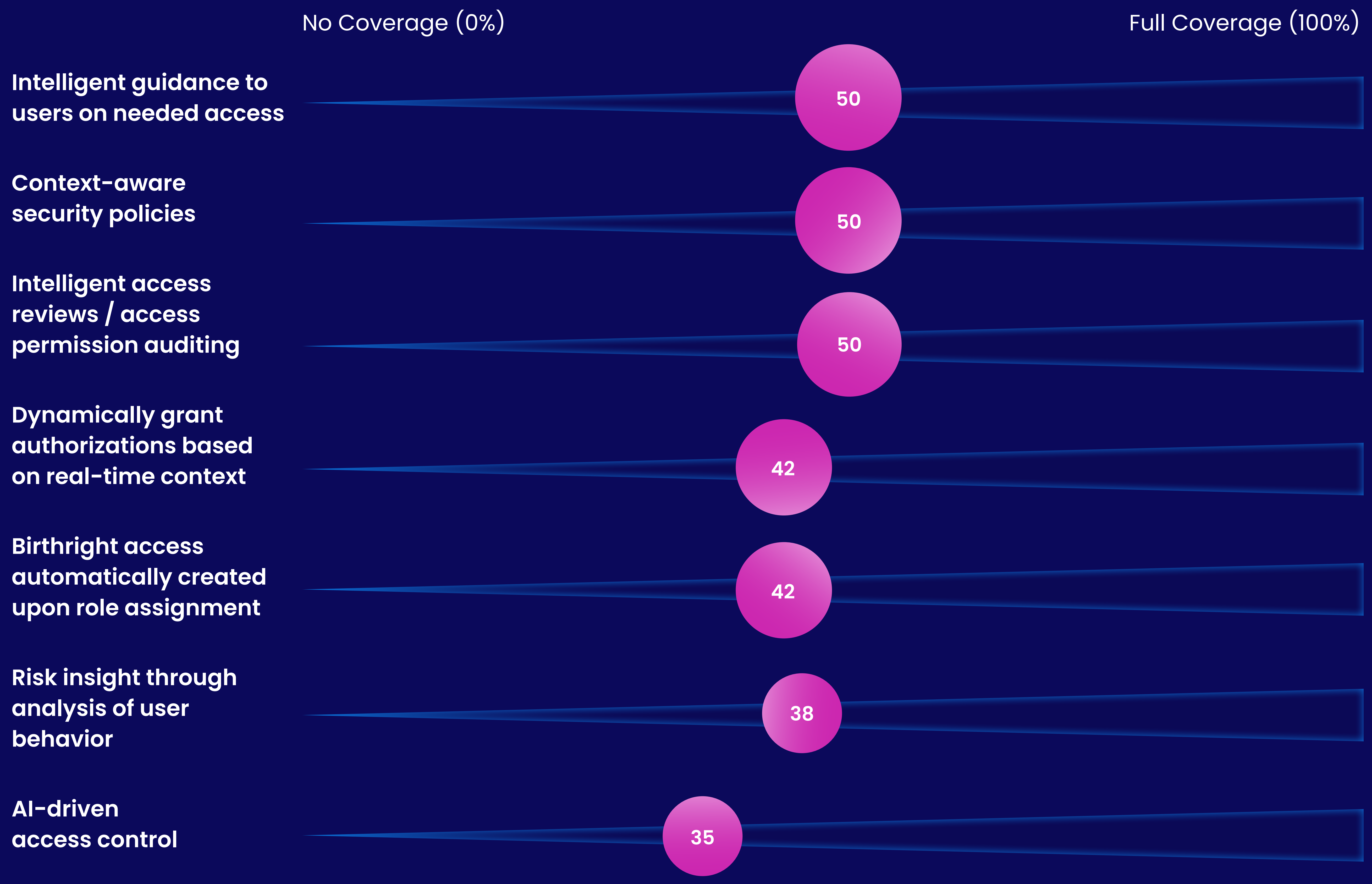
<40%

of Horizon 3 organizations leverage identity intelligence data at scale

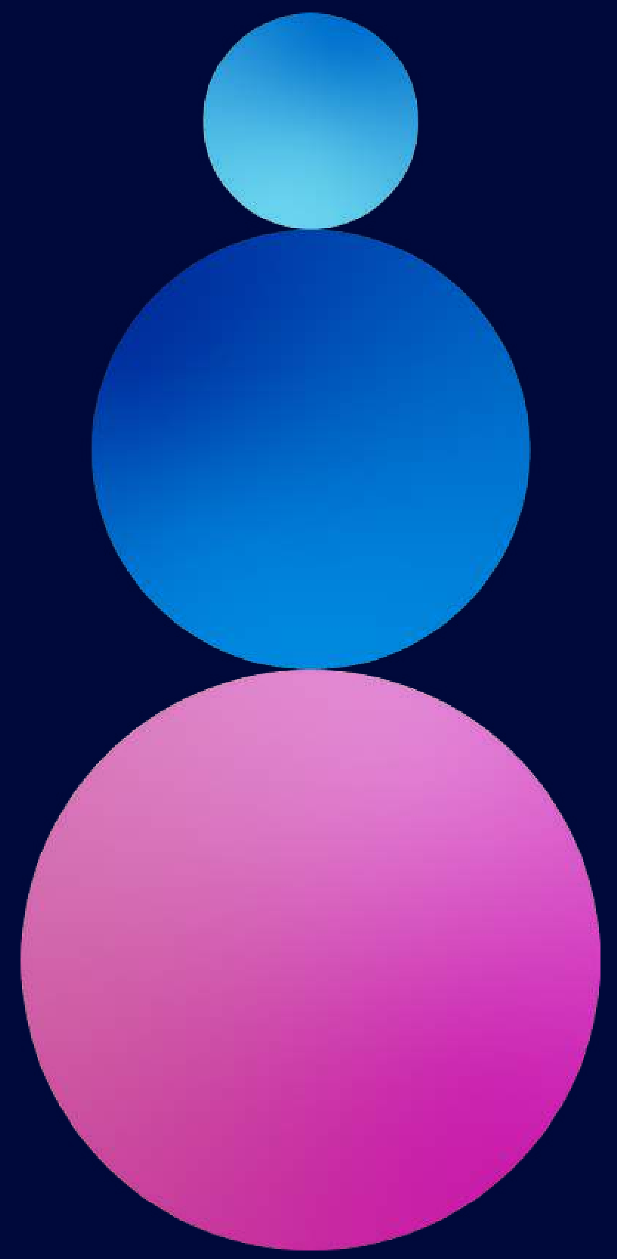
~50%

Horizon 4+ organizations use intelligent guidance from structured and unstructured data for user access, security policies, and access reviews

Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | All data



Horizon 4+ organizations are twice as likely to use identity data for actionable intelligence and new use cases



<20%

of Horizon 1-2 organizations leverage identity intelligence data at scale

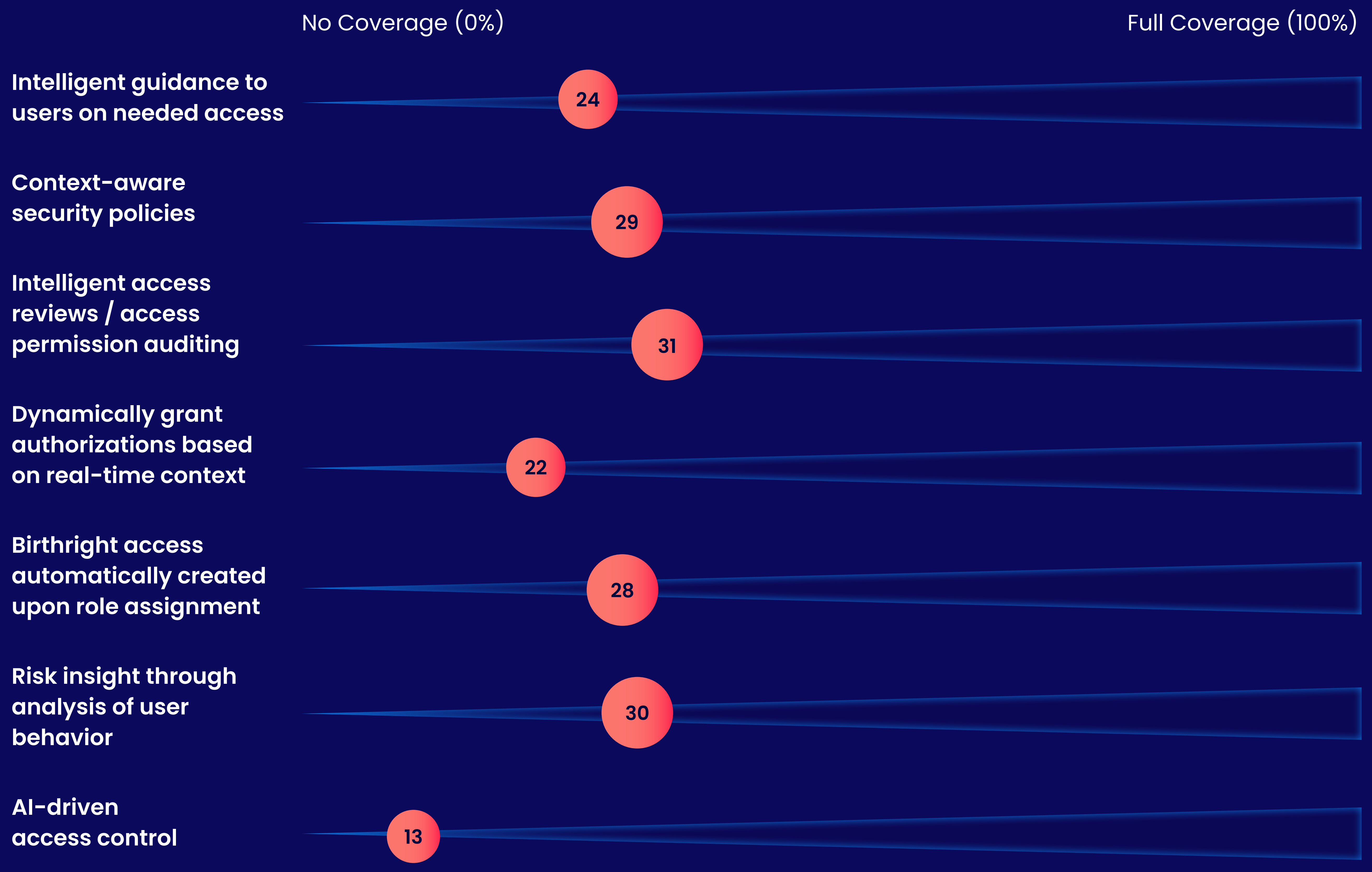
<40%

of Horizon 3 organizations leverage identity intelligence data at scale

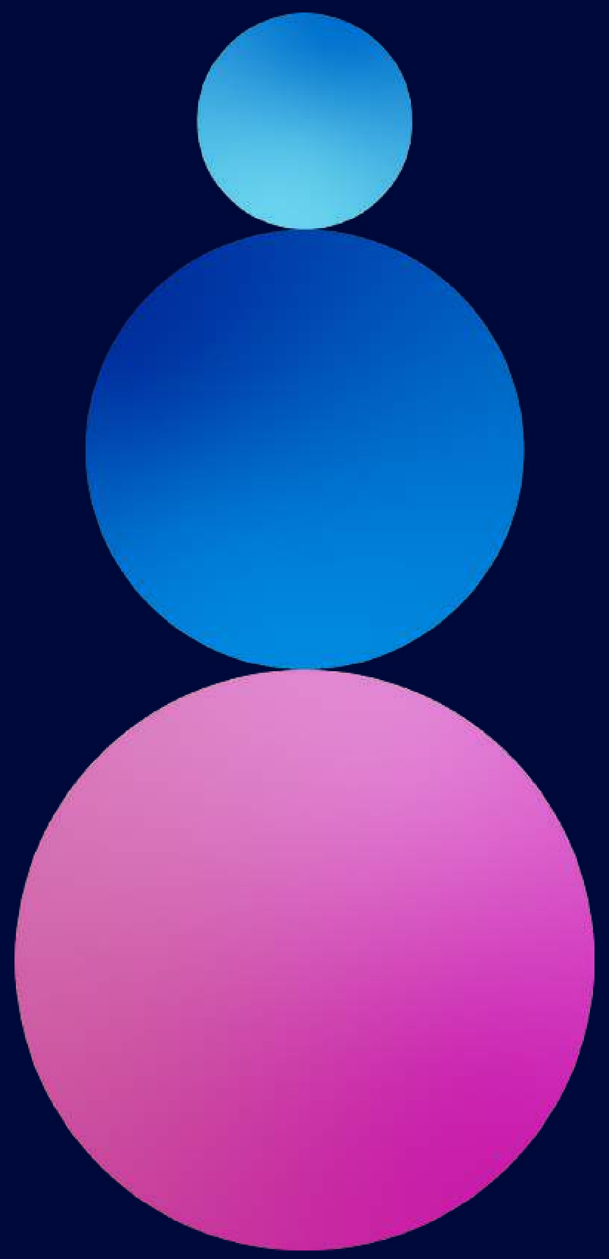
~50%

Horizon 4+ organizations use intelligent guidance from structured and unstructured data for user access, security policies, and access reviews

Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | All data



Horizon 4+ organizations are twice as likely to use identity data for actionable intelligence and new use cases



<20%

of Horizon 1-2 organizations leverage identity intelligence data at scale

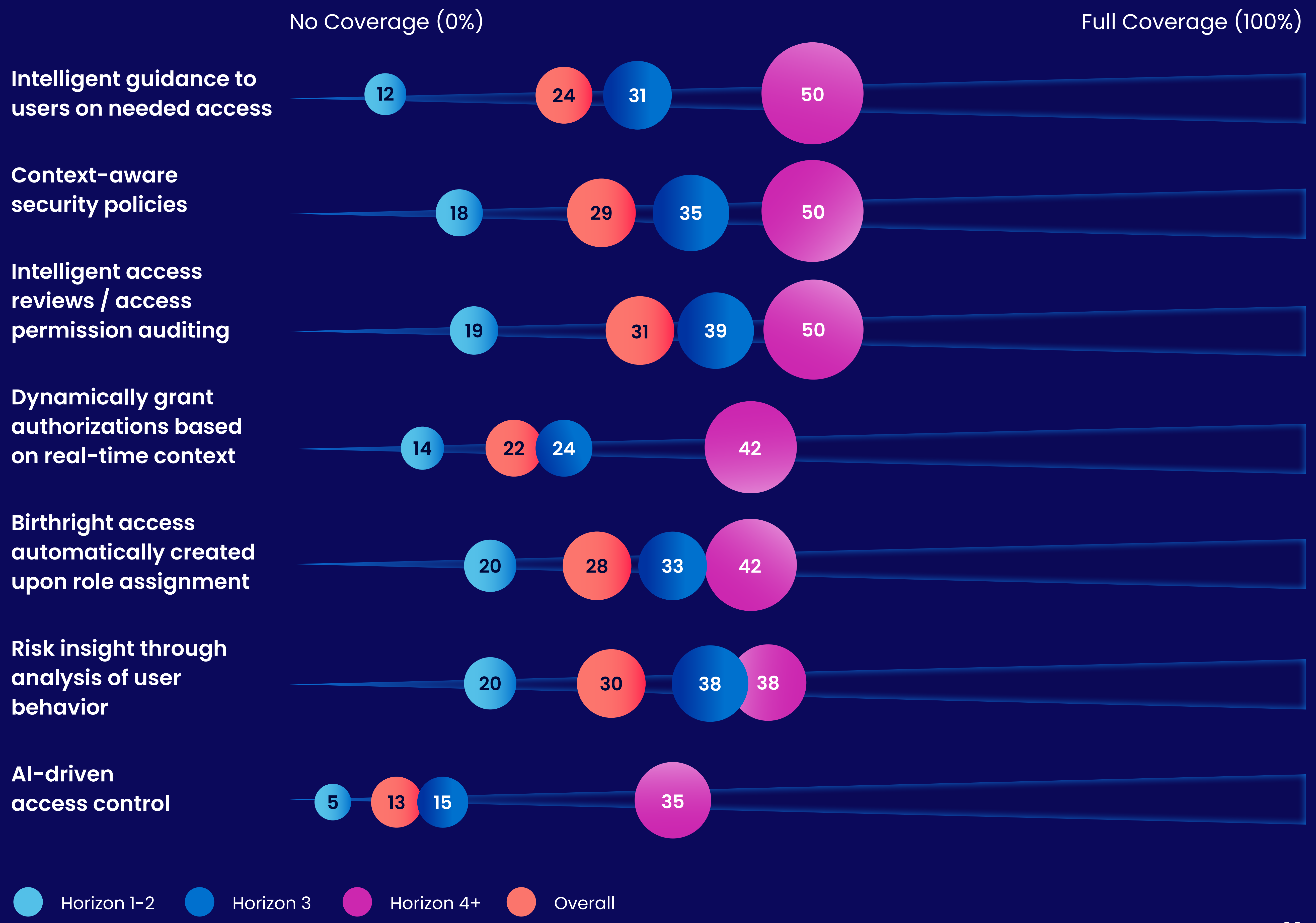
<40%

of Horizon 3 organizations leverage identity intelligence data at scale

~50%

Horizon 4+ organizations use intelligent guidance from structured and unstructured data for user access, security policies, and access reviews

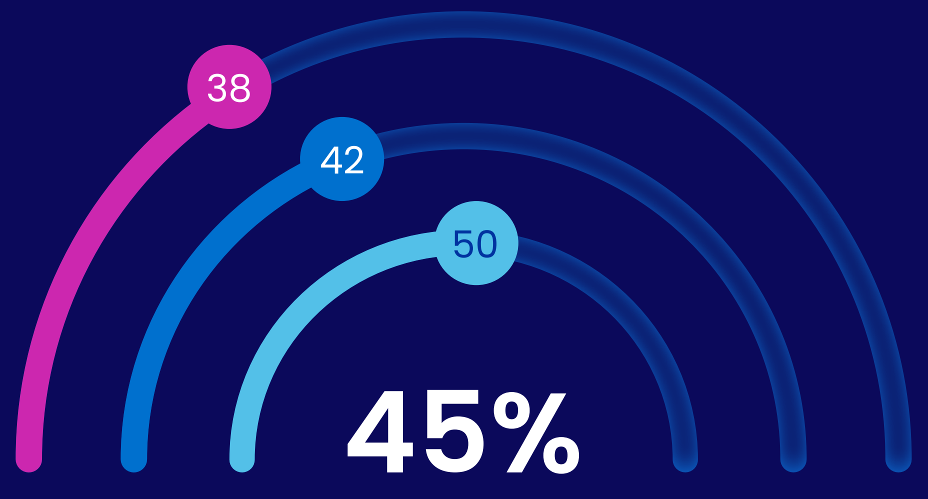
Horizon 1-2 | Horizon 3 | Horizon 4+ | Overall | All data



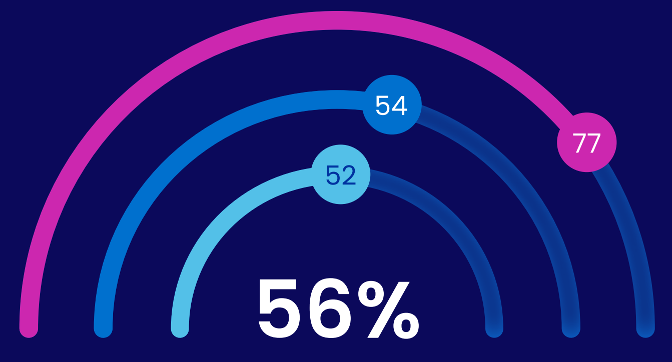
Organizations with mature identity security have the foundations to invest in scalable GenAI-powered use cases

Horizon 3+ organizations are focused on engineering scalable solutions to augment and scale their identity security. Whilst Horizon 1-2 organizations focus on automating helpdesk type repetitive activities.

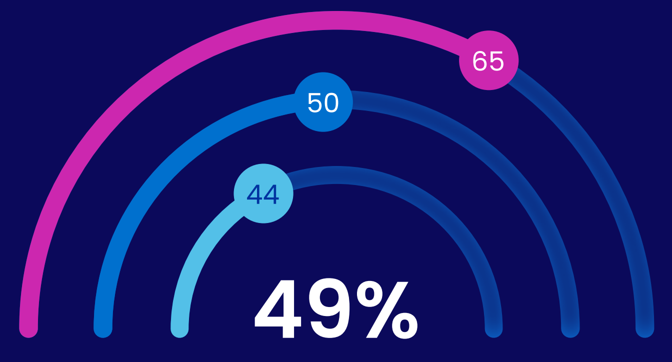
● Horizon 1-2 ● Horizon 3 ● Horizon 4+ ● Overall



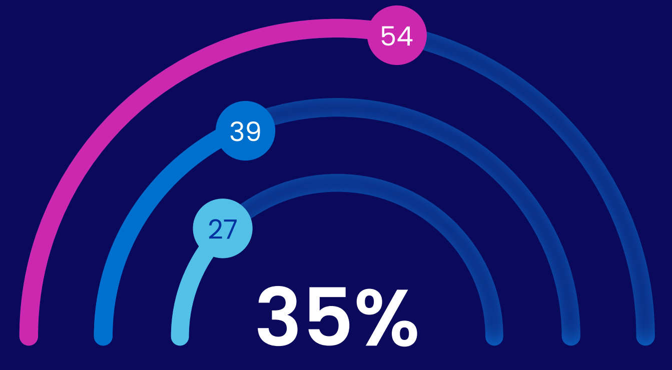
AI chatbots for instant IAM support and task handling



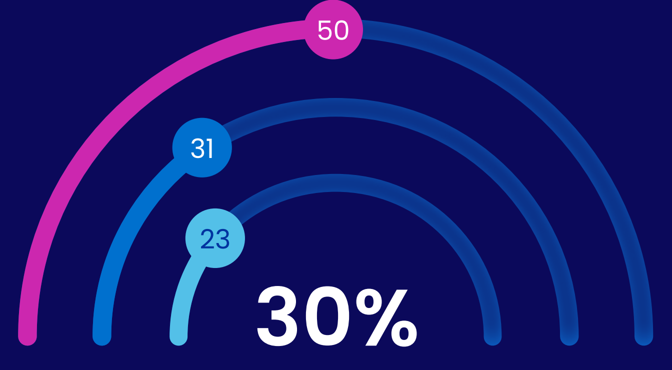
AI-powered workflow creation (incl. user provisioning, access reviews, and role management)



AI-generated user entitlement and role descriptions (incl. rights, privileges, and access levels)

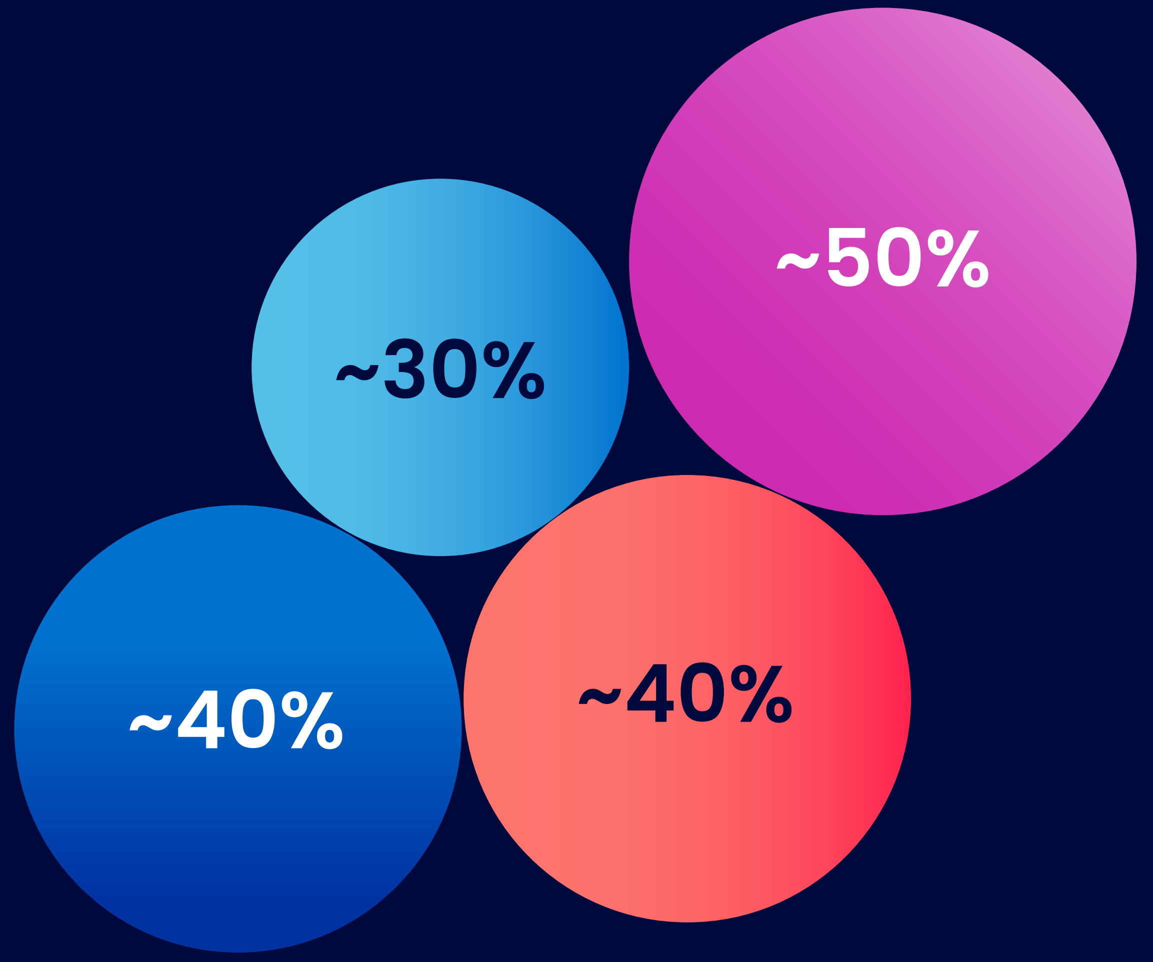


Natural language search to easily retrieve IAM data



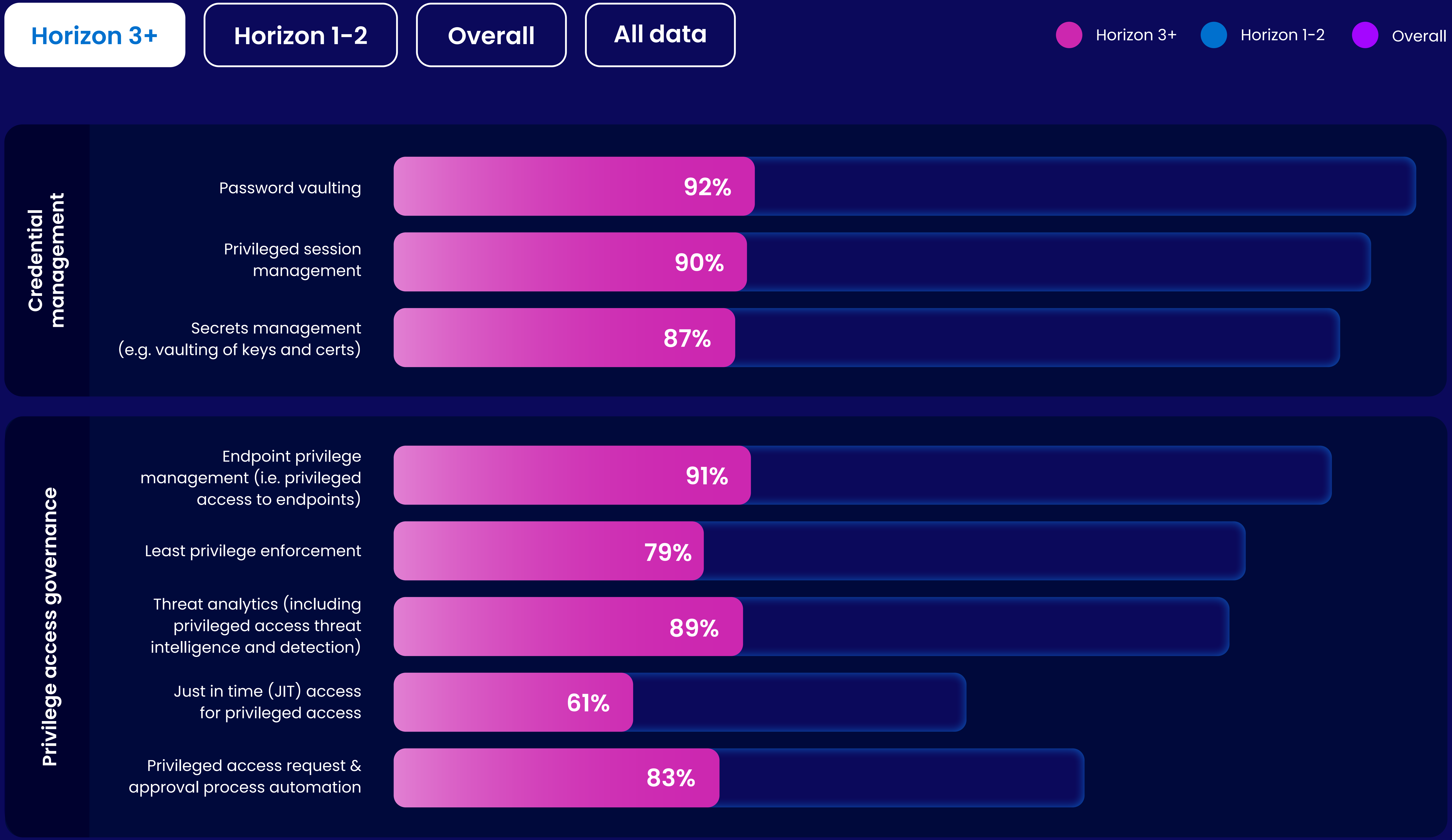
Copilots for automated connector development

(%) Estimated average willingness to invest in GenAI



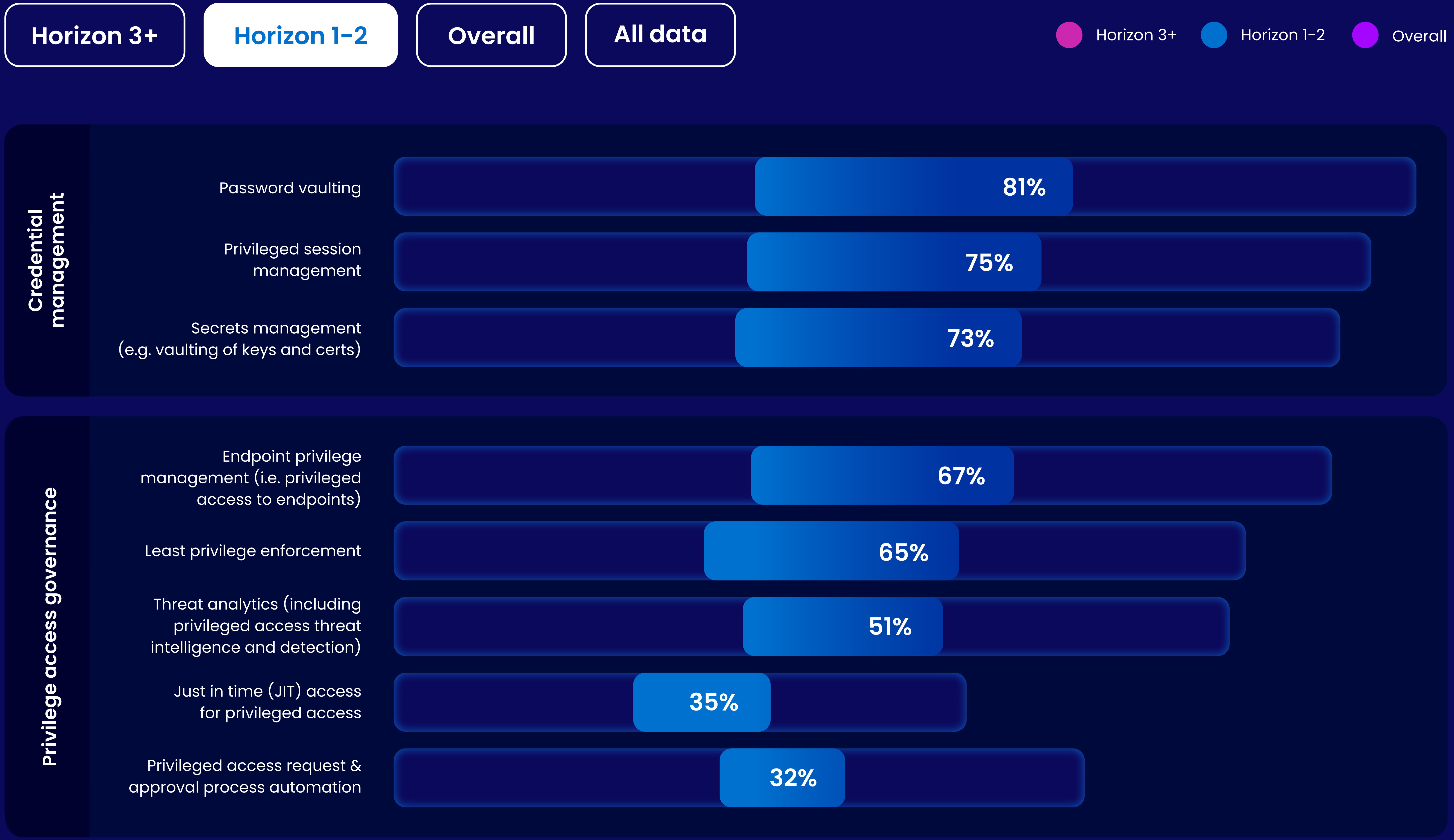
Horizon 3+ organizations have up to ~50% higher adoption of privilege access governance capabilities as compared to Horizons 1-2

By investing in solutions beyond credential vaulting and session management, organizations can simplify access approval and requests while enhancing threat analytics for privileged accounts.



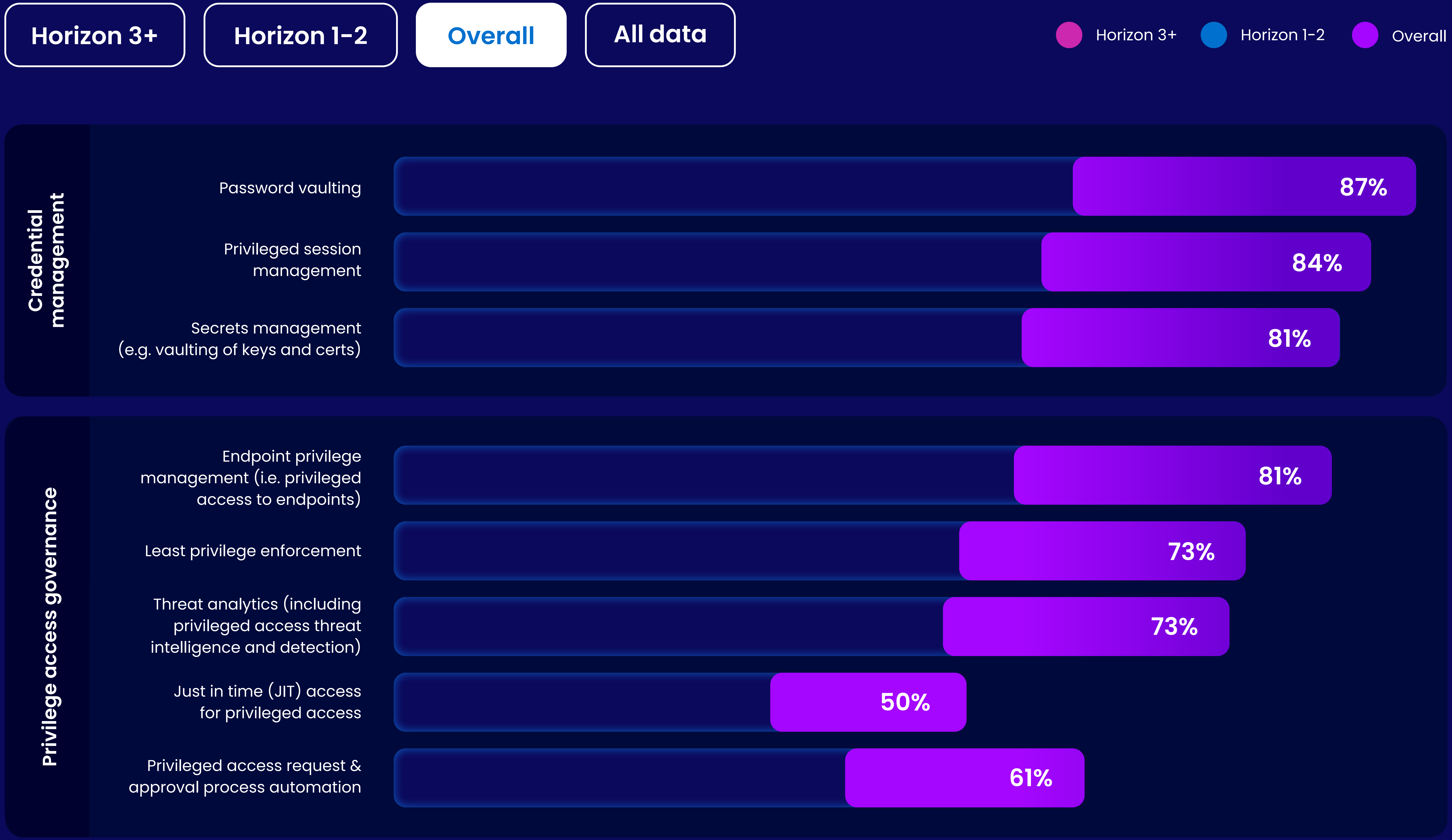
Horizon 3+ organizations have up to ~50% higher adoption of privilege access governance capabilities as compared to Horizons 1–2

By investing in solutions beyond credential vaulting and session management, organizations can simplify access approval and requests while enhancing threat analytics for privileged accounts.



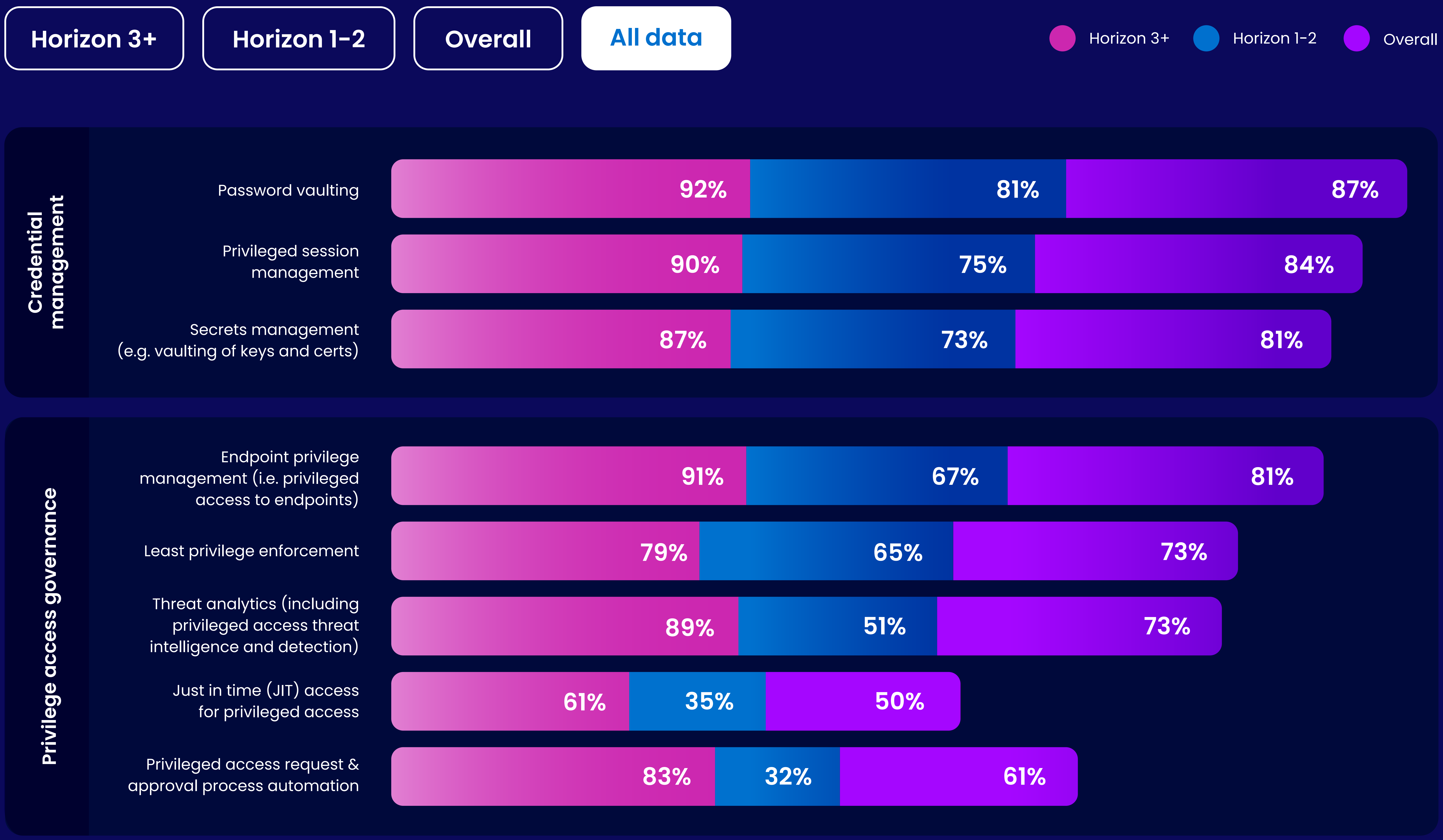
Horizon 3+ organizations have up to ~50% higher adoption of privilege access governance capabilities as compared to Horizons 1-2

By investing in solutions beyond credential vaulting and session management, organizations can simplify access approval and requests while enhancing threat analytics for privileged accounts.



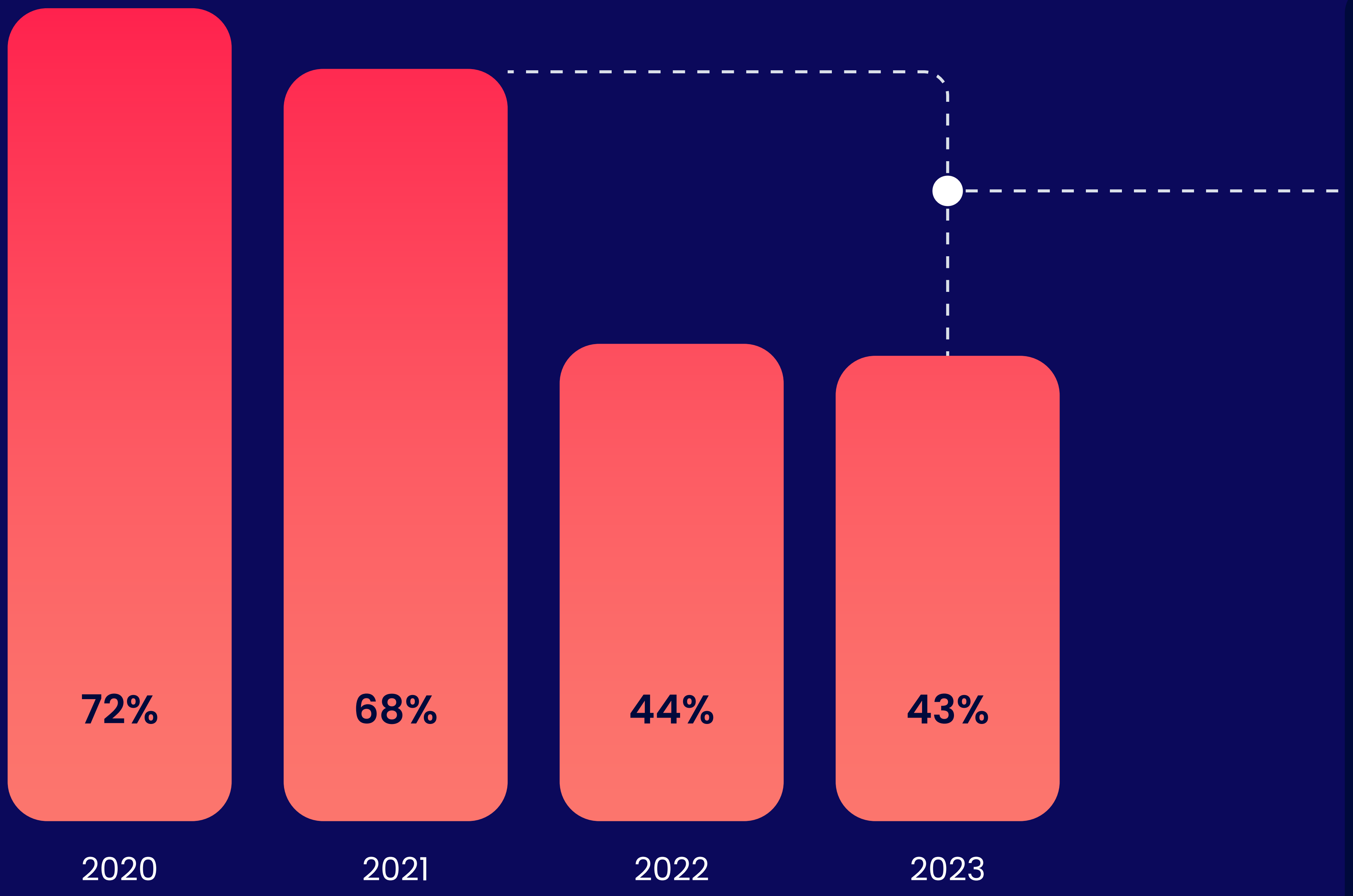
Horizon 3+ organizations have up to ~50% higher adoption of privilege access governance capabilities as compared to Horizons 1-2

By investing in solutions beyond credential vaulting and session management, organizations can simplify access approval and requests while enhancing threat analytics for privileged accounts.



As cyber insurers develop more mature ways to assess cyber risk management, cyber insurance premiums have risen

Cyber insurers have lowered their loss ratios and matured in assessing and managing risk . . .



Standalone cyber coverage loss ratios, share of premiums paid out as claims

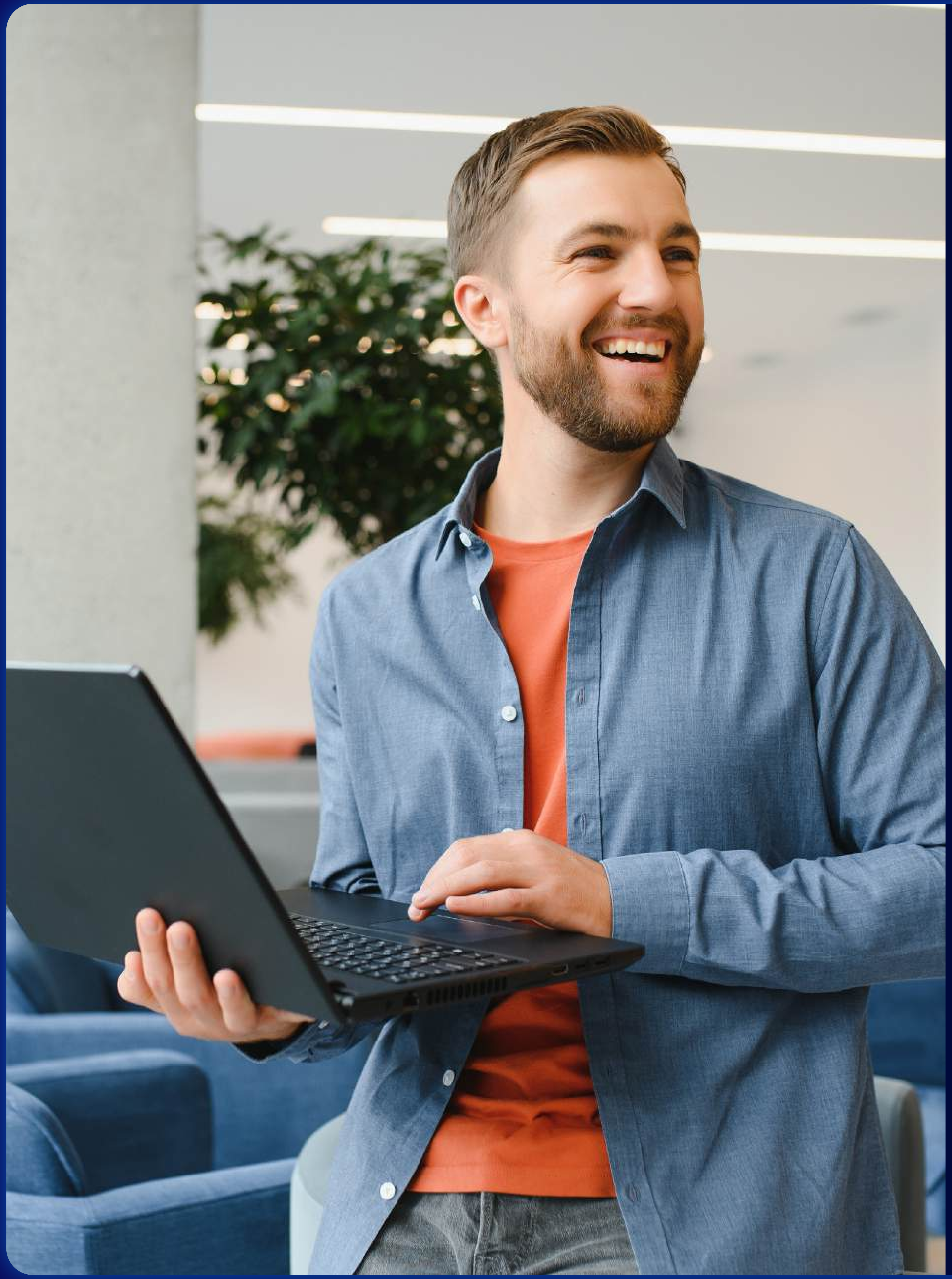
40%

Reduction in losses among cyber insurers indicates improved management of cyber risk

. . . and raised premiums to match heightened risk profile

77%

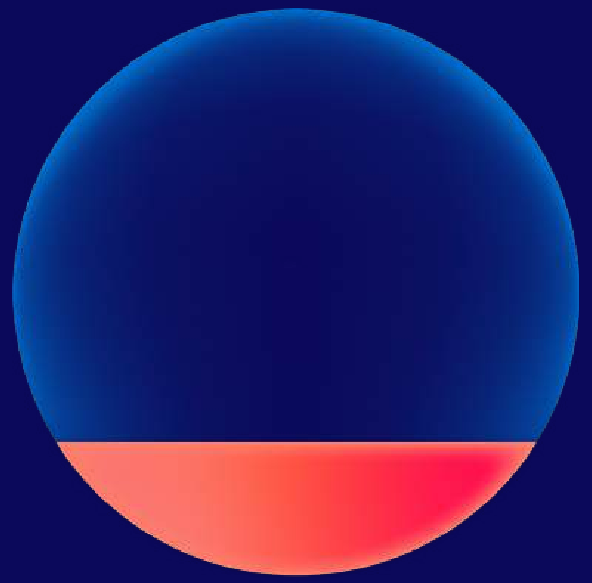
Organizations report premium increases over the last 3 years



> Insurance companies are now drilling down more to see what security controls a company has… they might incentivize you with discounts for implementing new security controls.

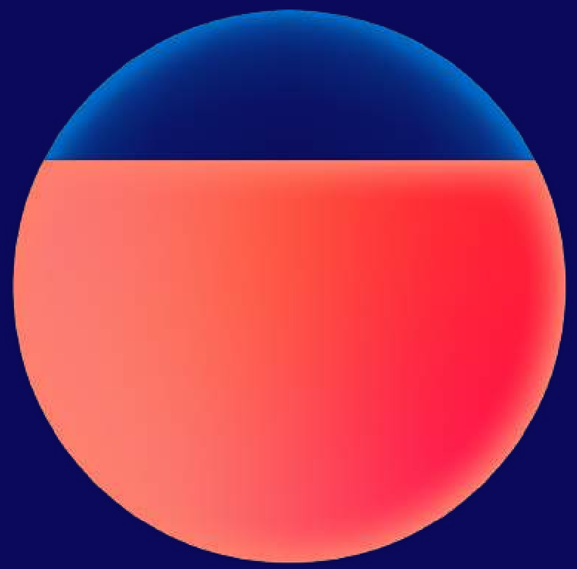
Cyber insurance professional at major brokerage

Cyber insurance customers report that identity security capabilities have the most impact on insurance assessments



25%

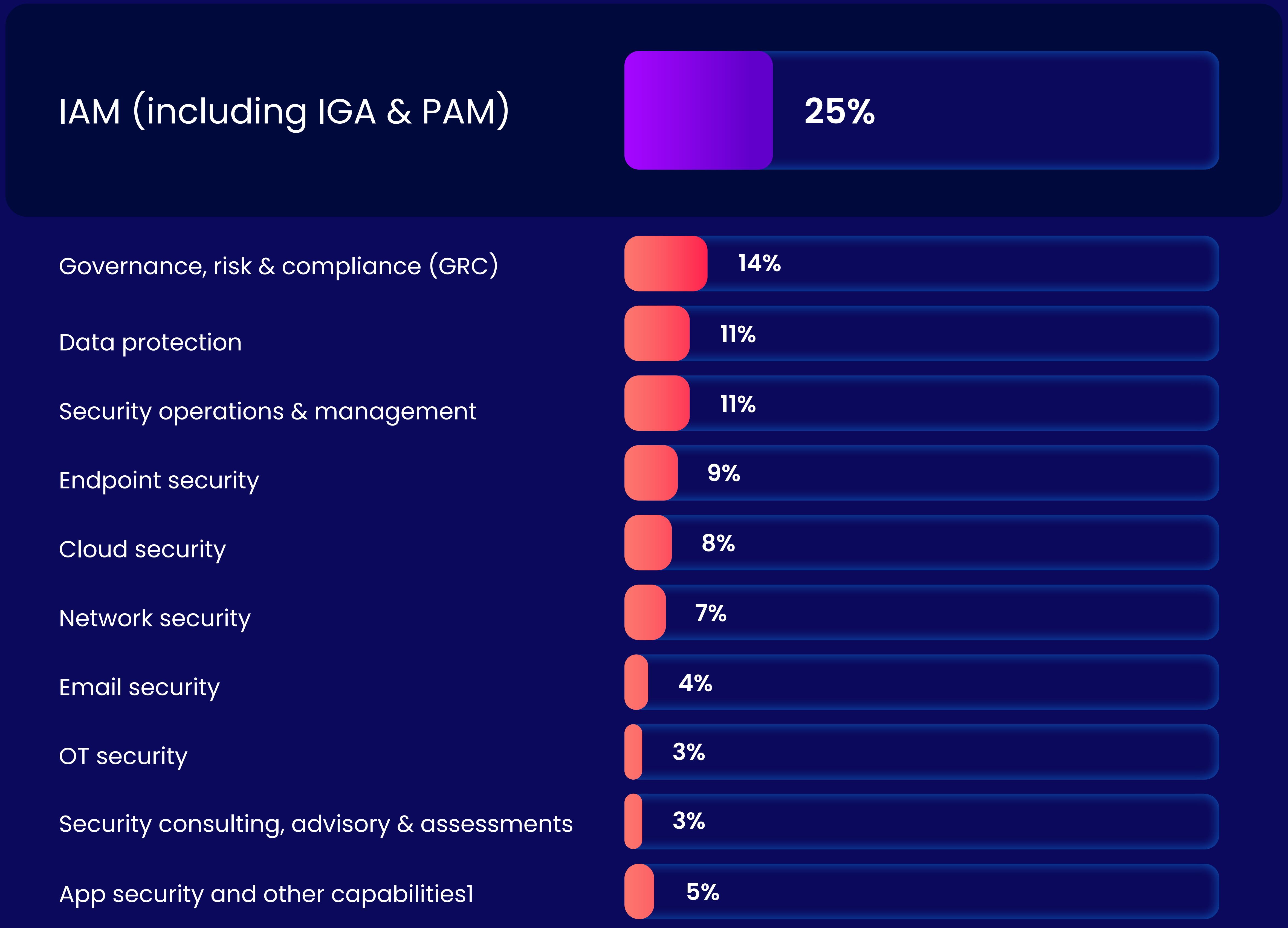
of respondents consider IAM the most critical element in cyber insurance evaluations, the largest proportion



73%

Of cyber insurance customers consider IAM capabilities among the top three capabilities influencing insurance assessments

Top cybersecurity capabilities impacting cyber insurance assessments, % of respondents who selected capability as the most impactful of all



Includes web security and MSSP / outsourcing

Identity-related regulations have grown sevenfold since 2010 across regions and industries

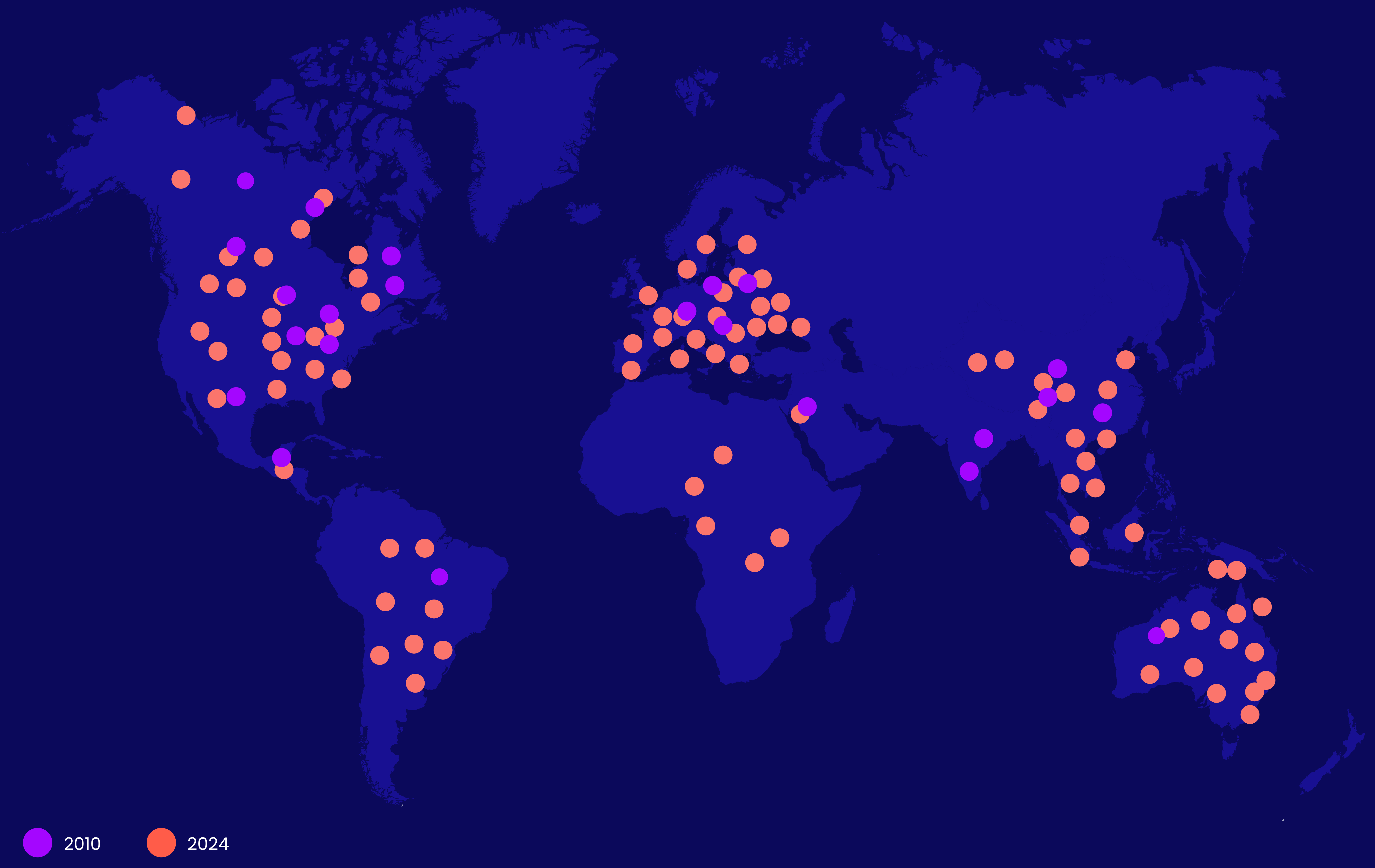
All | 2010 | 2024

5x+ increase

in regulations of industries outside finance and healthcare

13x+ increase

in regulations outside North America, APAC, and Europe

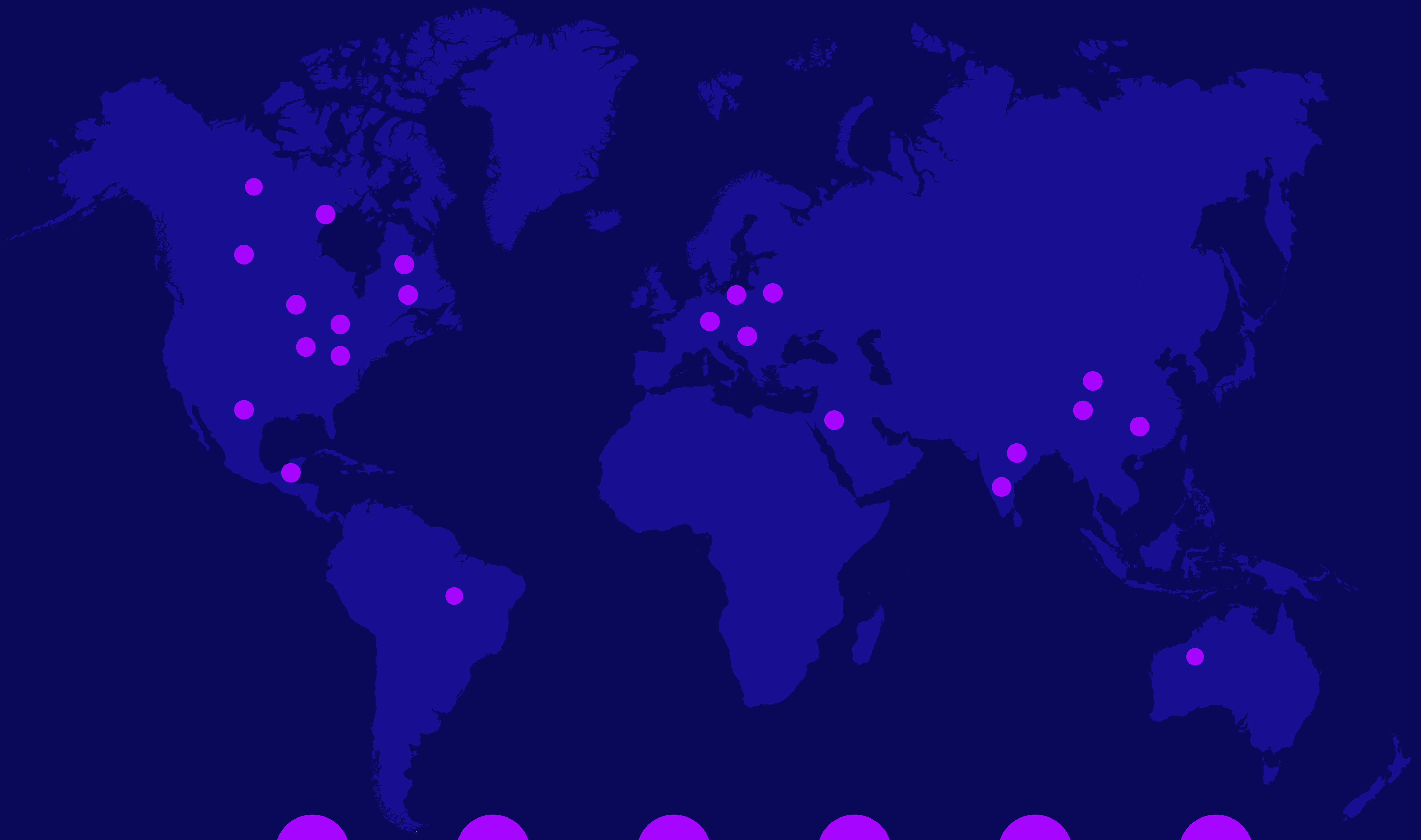


Identity-related regulations have grown sevenfold since 2010 across regions and industries

All | 2010 | 2024

~25

total regulations and frameworks were focused on mature regions and select industries in 2010



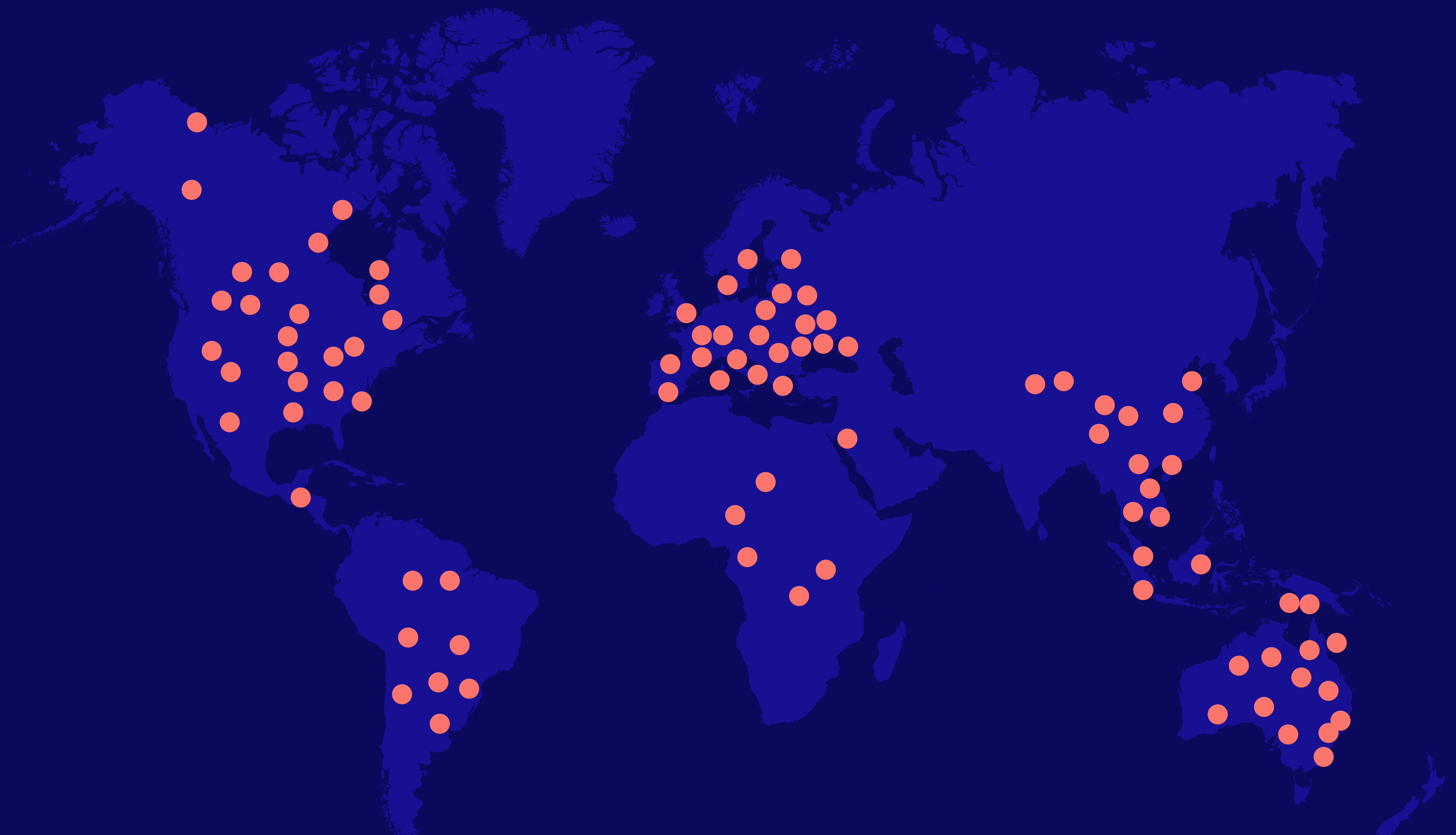
18	2	2	1	1	23
Industry agnostic	Telecom	Healthcare	Finance	Manufacturing	Total

Identity-related regulations have grown sevenfold since 2010 across regions and industries

All 2010 2024

~135

regulations and frameworks with substantial growth across all regions and industries in 2024



Industry agnostic	Telecom	Finance	Healthcare	Manufacturing	Other	Government	Total
103	11	9	5	3	2	1	134
~6x	~5x	9x	~3x	3x			

CHAPTER 4

How leading organizations are bending the curve.

Begin chapter →

Case studies
BNP Paribas
Pharmaceutical company
Absa
Currys

Organization case studies

Around the world and across industries, leading organizations are investing in identity security to bend the cyber security value curve, delivering outsized returns in compliance, operational efficiency, user productivity, and security.

Case studies
BNP Paribas
Pharmaceutical company
Absa
Currys

BNP PARIBAS

Goal:

Reduce cyber risk and improve productivity

BNP Paribas Bank Polska boosted productivity with extensive automation of manual IAM tasks.

Following a series of mergers, the bank was managing 10,000 users and about 1,000 applications through disjointed IAM programs. Without automation, the IT team was unable to cope with the volume of user requests or IAM tasks. With automation, all certification campaigns are now managed by just two employees, each allocating only about 15% of their worktime.

View case study →

40K
automated identity tasks executed monthly

90%
of access requests executed automatically

4K
Automated resets and password changes monthly

Goal:

Productivity

A leading pharmaceutical company with 72,000 employees, enhanced productivity and efficiency by automating IAM tasks.

The company sought a scalable, cloud-based system to replace its dated on-premise identity solution, which required significant manual maintenance. By onboarding a new cloud-based system, they simplified regulatory compliance and achieved notable reductions in time spent on access reviews and waiting for access.

40% reduction in time spent on access reviews

20% reduction in time spent waiting for access

30% reduction of manual tasks performed by IT operations

Case studies
BNP Paribas
Pharmaceutical company
Absa
Currys

absa

Goal:

Higher business value

Absa, a pan-African financial institution with more than 35,000 employees, streamlined onboarding and third-party identity management while lowering costs.

To comply with GDPR and POPIA, the bank deployed an AI-based risk management tool with just-in-time provisioning and standardized certification for third-party identities. This risk-based access model has lowered operational overhead and simplified identity governance for contractors and non-employees.

View case study →

$300 savings per identity onboarded

15 day reduction in onboarding time for 3rd party identities

12K non-employees empowered with secure identities

Case studies
BNP Paribas
Pharmaceutical company
Absa
Currys

currys

Goal:

Reduced cyber risk

Currys, a UK-based tech retailer with over 800 stores, reduced its risk profile by enhancing identity governance and automating identity security.

Currys, a UK-based tech retailer with over 800 stores, reduced its risk profile by enhancing identity governance and automating identity security. Its previous approach, using Excel-based manual processes with a constantly shifting pool of employees, led to over-provisioning and compliance risks. Automation now provides a complete audit trail, minimizing compliance challenges and non-executed permissions while strengthening overall security posture.

View case study →

3x

risk reduction by setting appropriate privileges for about 6,000 accounts

210

hours of manual effort saved annually

24K

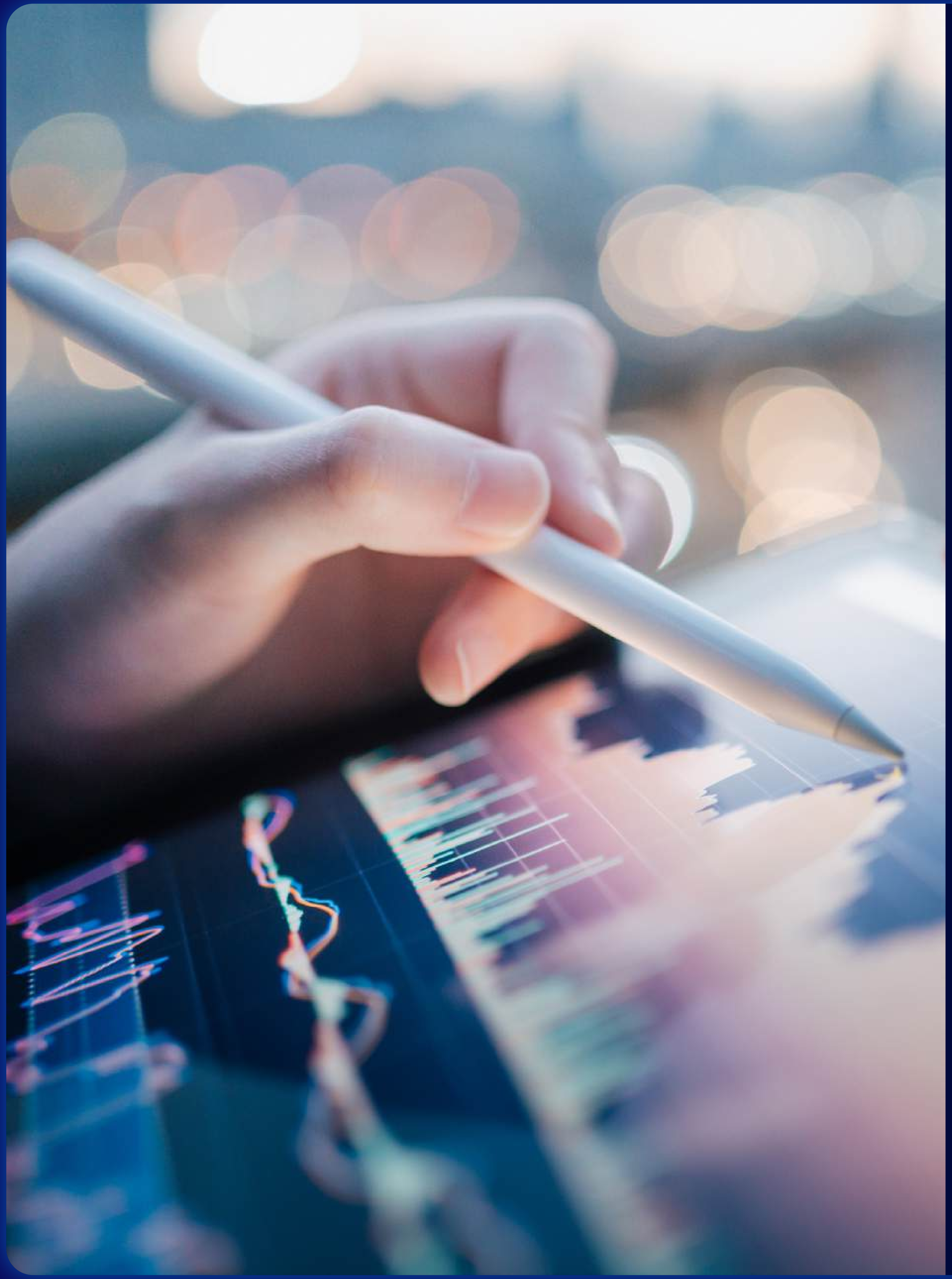
identities managed

Aboitiz, a global technology group, leapfrogged from Horizon 1 to Horizon 3+ over 24 months with a “Great Transformation” initiative

Hover over each section to see what action was taken

○ Horizon 1 (2020)	**0** formal identity and access management processes	**21** days to deactivate and 5 days to activate user accounts	**<5** business units with centralized identity governance	**<1K** accounts managed through automated processes
● Horizon 3+ (2022)	**1** unified identity and access management program governing all staff accounts	**0** wait time with instantaneous provisioning and deprovisioning	**47** business units with centralized governance of about 23,000 application accounts	**144K** automated account modifications and verifications

View case study →



> We were starting from zero. But this gave us the opportunity to leapfrog using technology… We made the call to invest time and effort into the organization's most valuable asset: the identity.

CISO, Aboitiz Equity Ventures

aboitiz

CHAPTER 5

Your path to the next horizon.

Begin chapter →

Your path to the next horizon

1. Set a north star vision
2. Invest in the right solutions, especially AI enabled to leapfrog horizons and for higher returns
3. Secure all types of identities
4. Integrate IAM with broader security operations for continuous monitoring and control premiums
5. Leverage identity data to derive actionable insights and adaptive security policies
6. Stay ahead of emerging regulations and standards to maintain compliance

SailPoint

Understand more about identity security maturity and your organization’s horizon.

Take the assessment

Download the full report