SailPoint

Livro interativo

2024-2025

Horizontes da segurança de identidade

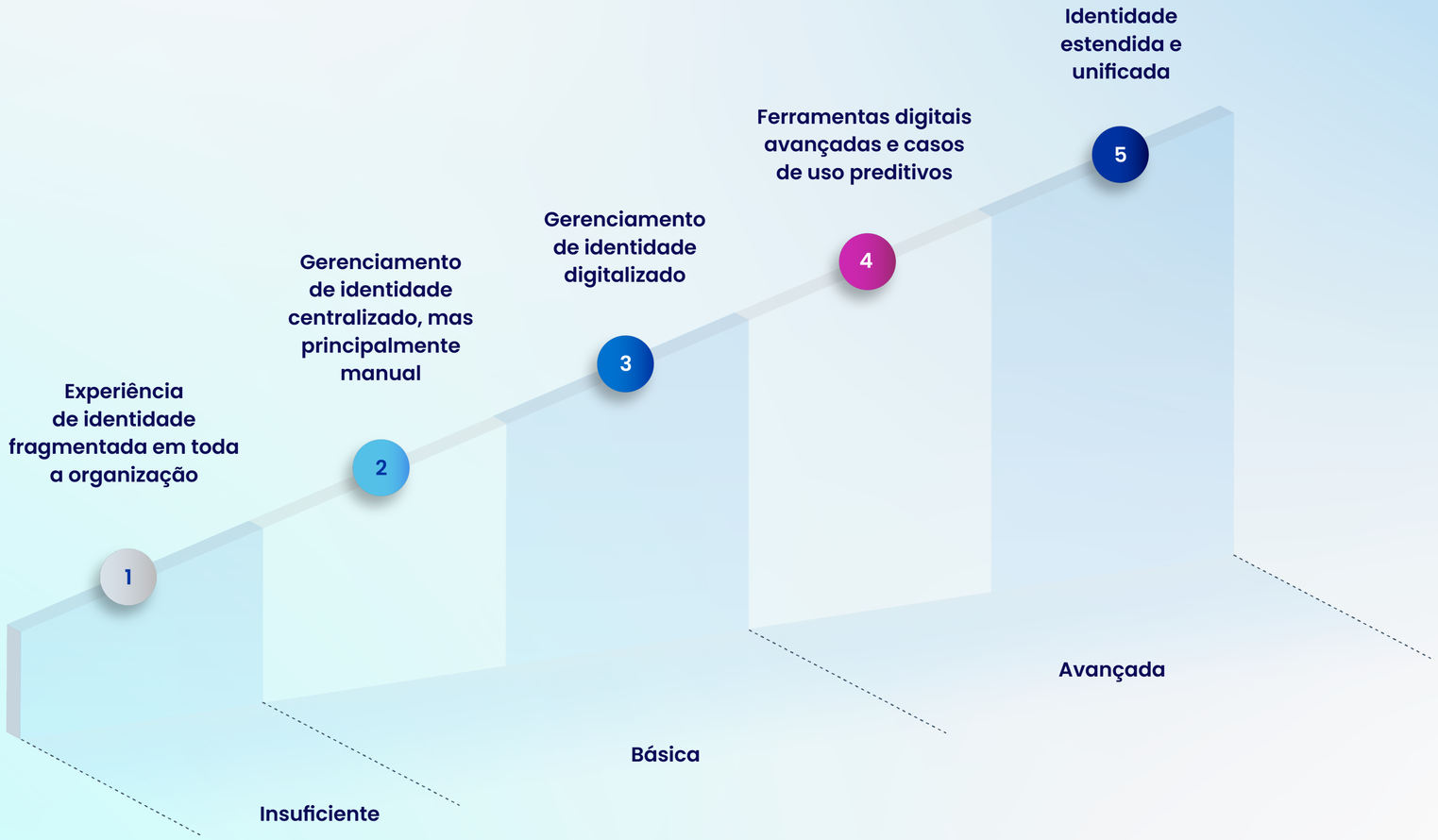
Como usar o poder da segurança de identidade para obter valor da segurança cibernética

Etapas para desenvolver a maturidade em segurança de identidade

Em todo o mundo, organizações de todos os setores enfrentam um duplo desafio: elas precisam combater ameaças cibernéticas cada vez mais complexas e generalizadas, além de lidar com orçamentos restritos e cortes de custos implacáveis.

A pressão é especialmente intensa na área de segurança de identidade, onde as superfícies de ataque aumentam e os orçamentos de TI ficam mais apertados à medida que as organizações crescem. No entanto, as partes interessadas, internas e externas, exigem cada vez mais segurança e experiência digital aprimorada.

Nos últimos três anos, a SailPoint fez uma pesquisa com responsáveis por decisões de gerenciamento de identidade e acesso (IAM, Identity and Access Management) em todo o mundo para avaliar suas capacidades em cinco horizontes de segurança de identidade. Entre os 350 responsáveis por tomar decisões, entrevistados para a pesquisa em julho de 2024, estavam líderes seniores em tecnologia da informação, segurança cibernética e risco; mais da metade trabalhava para organizações com mais de 10.000 funcionários e nos setores de finanças ou tecnologia.más de la mitad trabajan en los sectores financiero o tecnológico.



Fonte: Todos os gráficos deste documento são originários do relatório **The Horizons of Identity Security 2024-2025.**

CAPÍTULO 1

Os avanços da tecnologia moldarão o futuro da segurança de identidade.

O futuro da identidade será definido por quatro elementos-chave

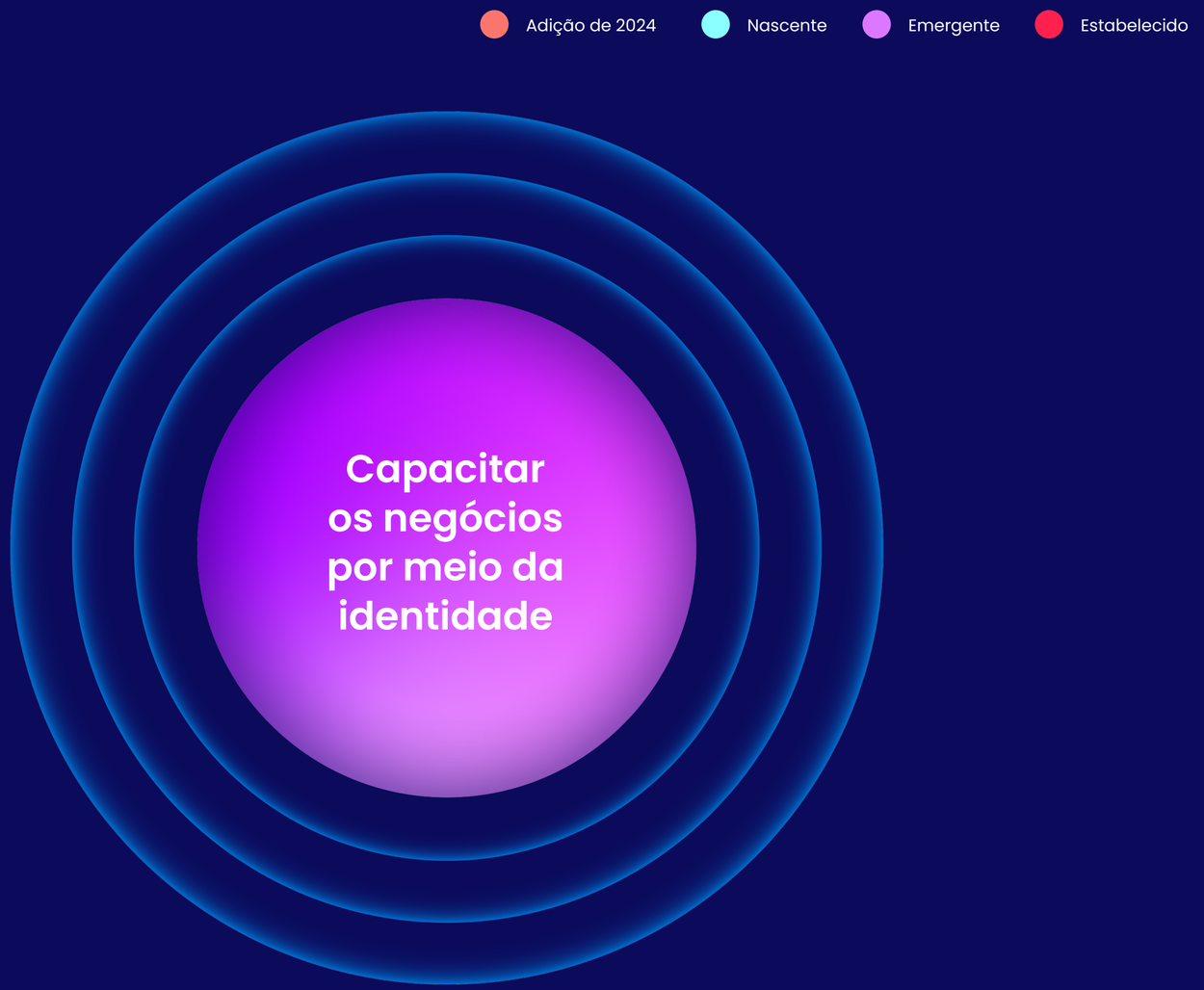
Nos últimos anos, nossa experiência e pesquisa confirmaram que o futuro da segurança de identidade será moldado por programas de identidade integrados.

Os principais elementos são mostrados aqui, acompanhados das tendências que os complementam.

O cenário regulatório e de risco evolui e continua a moldar esses quatro elementos

A estrutura de segurança de identidade se tornará o centro nevrálgico das futuras operações de segurança.

A proliferação de regulamentos e padrões do setor relacionados à segurança de identidade em todo o mundo e em todos os setores levará a um aumento das expectativas relativas à segurança de identidade.



O futuro da identidade será definido por quatro elementos-chave

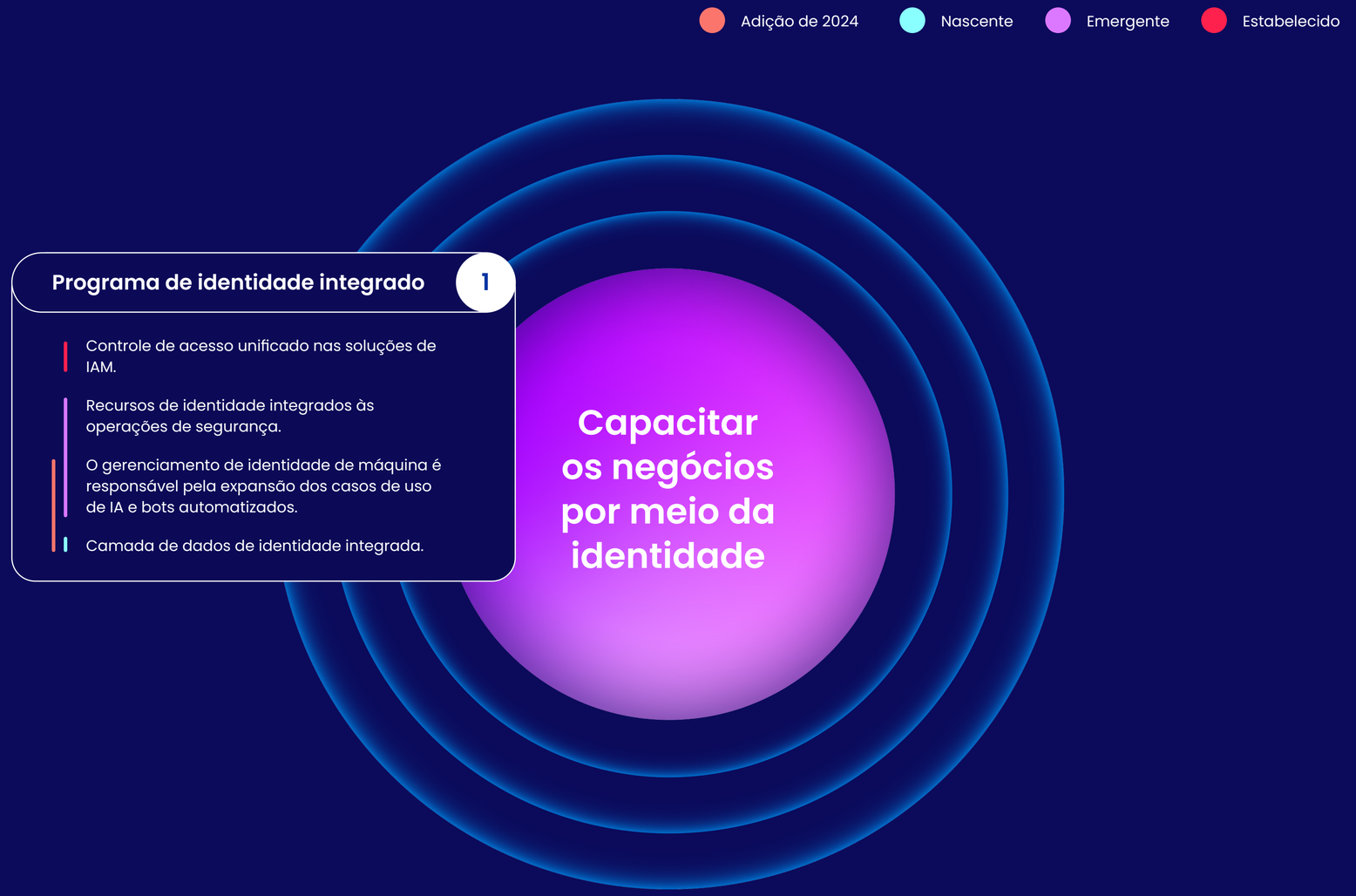
Nos últimos anos, nossa experiência e pesquisa confirmaram que o futuro da segurança de identidade será moldado por programas de identidade integrados.

Os principais elementos são mostrados aqui, acompanhados das tendências que os complementam.

O cenário regulatório e de risco evolui e continua a moldar esses quatro elementos

A estrutura de segurança de identidade se tornará o centro nevrálgico das futuras operações de segurança.

A proliferação de regulamentos e padrões do setor relacionados à segurança de identidade em todo o mundo e em todos os setores levará a um aumento das expectativas relativas à segurança de identidade.



O futuro da identidade será definido por quatro elementos-chave

Nos últimos anos, nossa experiência e pesquisa confirmaram que o futuro da segurança de identidade será moldado por programas de identidade integrados.

Os principais elementos são mostrados aqui, acompanhados das tendências que os complementam.

O cenário regulatório e de risco evolui e continua a moldar esses quatro elementos

A estrutura de segurança de identidade se tornará o centro nevrálgico das futuras operações de segurança.

A proliferação de regulamentos e padrões do setor relacionados à segurança de identidade em todo o mundo e em todos os setores levará a um aumento das expectativas relativas à segurança de identidade.

O futuro da identidade será definido por quatro elementos-chave

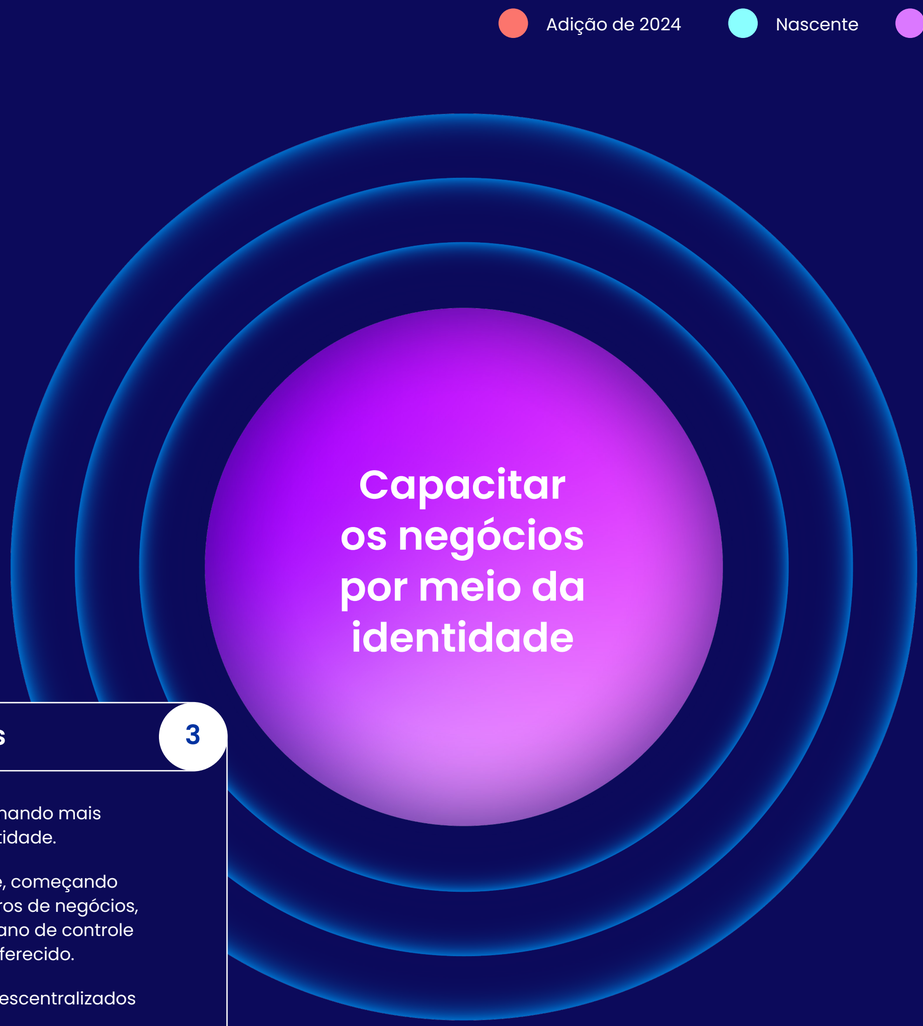
Nos últimos anos, nossa experiência e pesquisa confirmaram que o futuro da segurança de identidade será moldado por programas de identidade integrados.

Os principais elementos são mostrados aqui, acompanhados das tendências que os complementam.

O cenário regulatório e de risco evolui e continua a moldar esses quatro elementos

A estrutura de segurança de identidade se tornará o centro nevrálgico das futuras operações de segurança.

A proliferação de regulamentos e padrões do setor relacionados à segurança de identidade em todo o mundo e em todos os setores levará a um aumento das expectativas relativas à segurança de identidade.



Identidades federadas 3

- O acesso federado está se tornando mais comum entre os tipos de identidade.
- Várias personas de identidade, começando com os colaboradores, parceiros de negócios, máquinas que integram ao plano de controle de segurança de identidade oferecido.
- Os protocolos de identidade descentralizados estão em estágio inicial.

O futuro da identidade será definido por quatro elementos-chave

Nos últimos anos, nossa experiência e pesquisa confirmaram que o futuro da segurança de identidade será moldado por programas de identidade integrados.

Os principais elementos são mostrados aqui, acompanhados das tendências que os complementam.

O cenário regulatório e de risco evolui e continua a moldar esses quatro elementos

A estrutura de segurança de identidade se tornará o centro nevrálgico das futuras operações de segurança.

A proliferação de regulamentos e padrões do setor relacionados à segurança de identidade em todo o mundo e em todos os setores levará a um aumento das expectativas relativas à segurança de identidade.

CAPÍTULO 2

Os investimentos em segurança de identidade podem “dobrar a curva”.

Curva de valor

As organizações com segurança de identidade madura oferecem retornos substancialmente maiores para cada dólar gasto

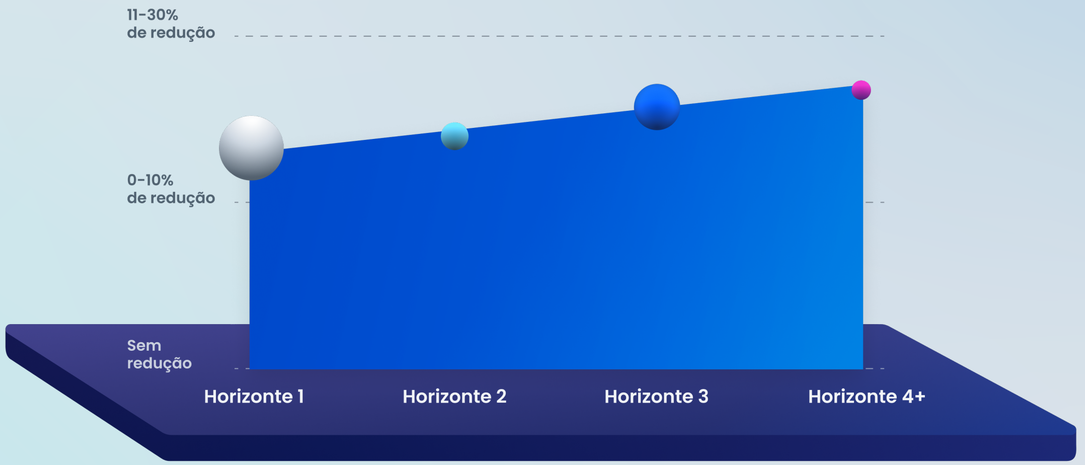
O salto para os Horizontes 3 e 4 tem um impacto comercial expressivo na segurança de identidade, “dobrando a curva” exponencialmente.

O diâmetro indica a distribuição do horizonte

Redução de risco

A movimentação pelos horizontes de segurança de identidade reduz a superfície de ataque contra possíveis violações

83% das organizações relataram menos problemas de segurança relacionados à identidade graças aos seus investimentos em segurança de identidade em 2023.



O diâmetro indica a distribuição do horizonte

Valor de negócios

As organizações com recursos avançados de identidade obtêm um tempo mais rápido de colocação no mercado, além da redução do atrito

Gerar receita bruta: a segurança de identidade avançada acelera a transformação digital, permitindo ciclos de desenvolvimento e velocidade de lançamento no mercado mais rápidos, aumentando a receita.

O diâmetro indica a distribuição do horizonte

Produtividade

As organizações dos Horizontes 3 e 4+ provavelmente terão ganhos significativos de produtividade

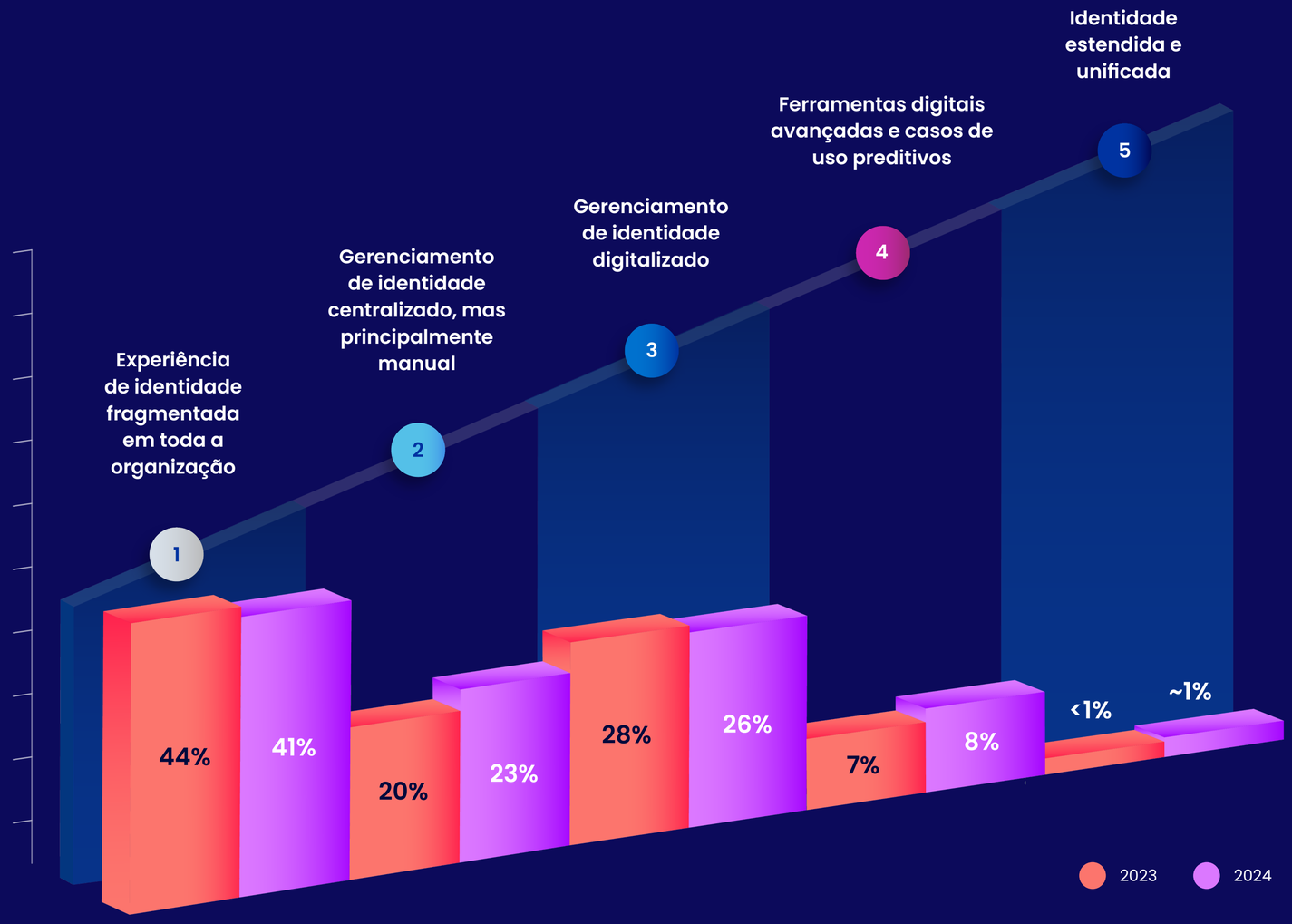
As organizações do Horizonte 4+ veem melhorias significativas de produtividade impulsionadas por uma estratégia integrada de segurança de identidade e adoção de **casos de uso emergentes**, como copilotos para orientação, serviços para usuários finais e concessão automatizada de aprovação de acesso do usuário.

O diâmetro indica a distribuição do horizonte

CAPÍTULO 3

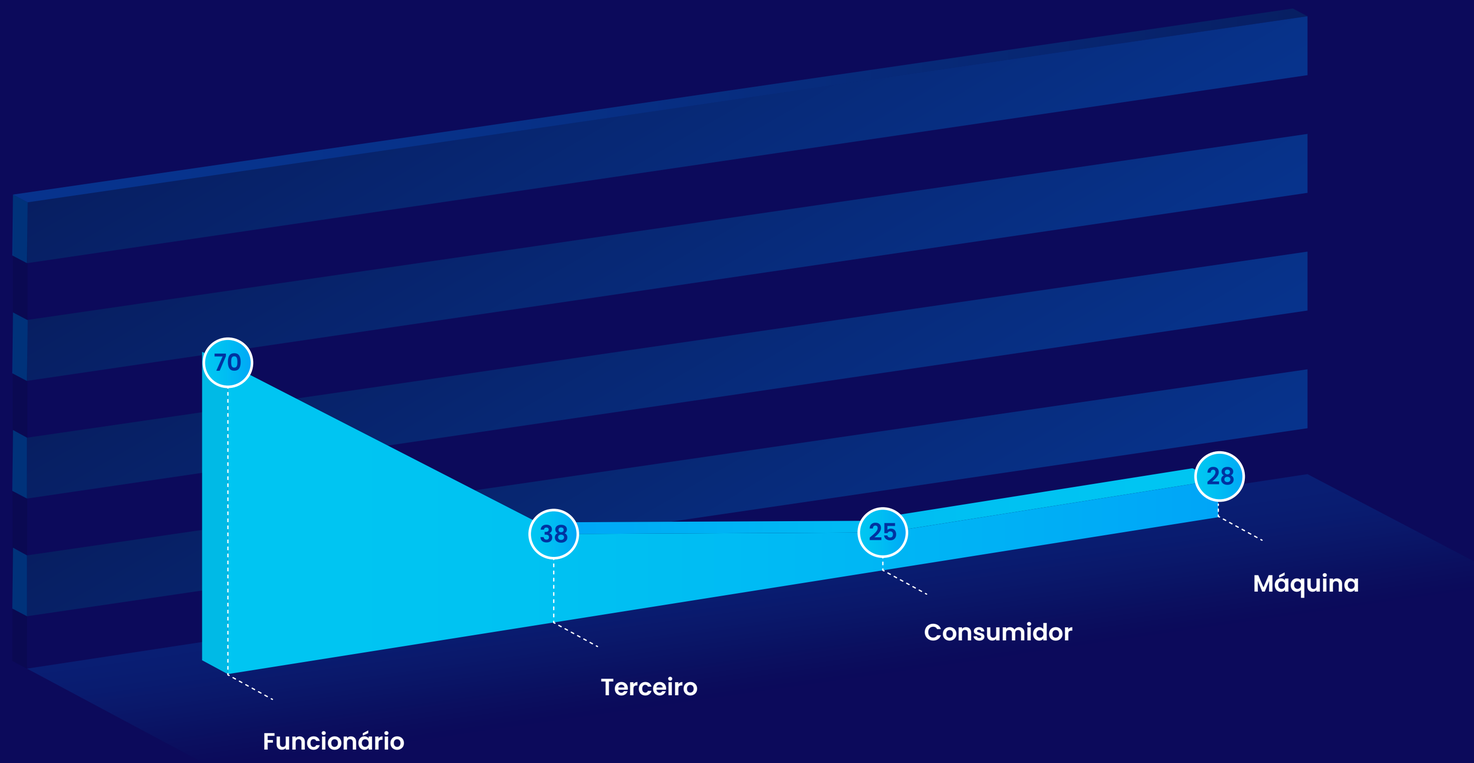
Em que fase as organizações estão em suas jornadas e por que as organizações maduras obtêm retornos mais altos.

Com 41% das organizações ainda no Horizonte 1, há uma grande oportunidade para liberar “todo o potencial” da segurança de identidade



As organizações no Horizonte 4+ reduzem o risco com cobertura de capacidade de 70% em todos os tipos de identidade. O Horizonte 3 está logo atrás.

Horizonte 1-2



As organizações do Horizonte 1 e 2 têm uma **grande falha na cobertura de identidade.**

30% Funcionários

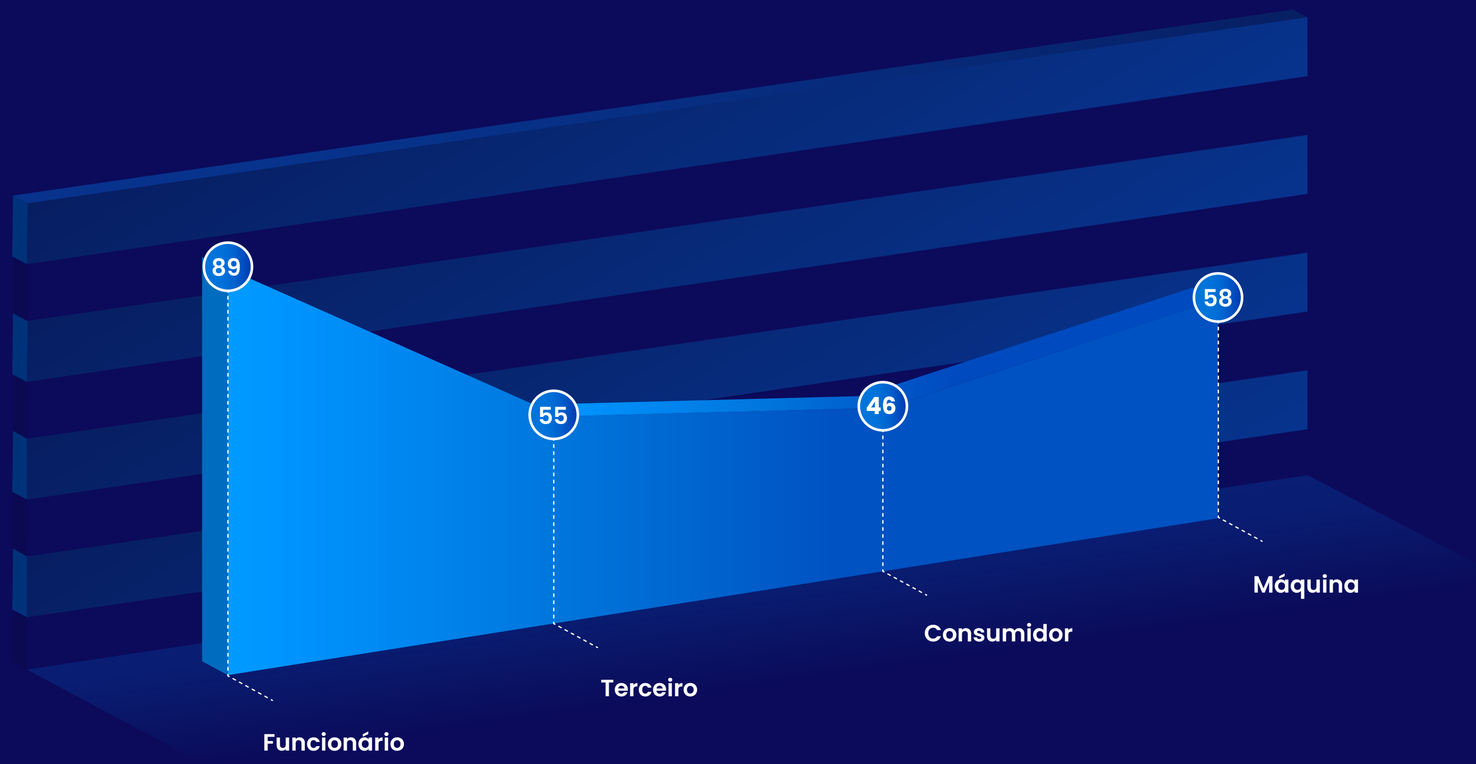
62% Terceiros

72% Identidades de máquina

O último caso é bastante preocupante, uma vez que as identidades de máquina normalmente representam cerca de 40% a 65% do total de identidades em uma organização.

As organizações no Horizonte 4+ reduzem o risco com cobertura de capacidade de 70% em todos os tipos de identidade. O Horizonte 3 está logo atrás.

Horizontes 3



As organizações do Horizonte 1 e 2 têm uma **grande falha na cobertura de identidade.**

30% Funcionários

62% Terceiros

72% Identidades de máquina

O último caso é bastante preocupante, uma vez que as identidades de máquina normalmente representam cerca de 40% a 65% do total de identidades em uma organização.

As organizações no Horizonte 4+ reduzem o risco com cobertura de capacidade de 70% em todos os tipos de identidade. O Horizonte 3 está logo atrás.

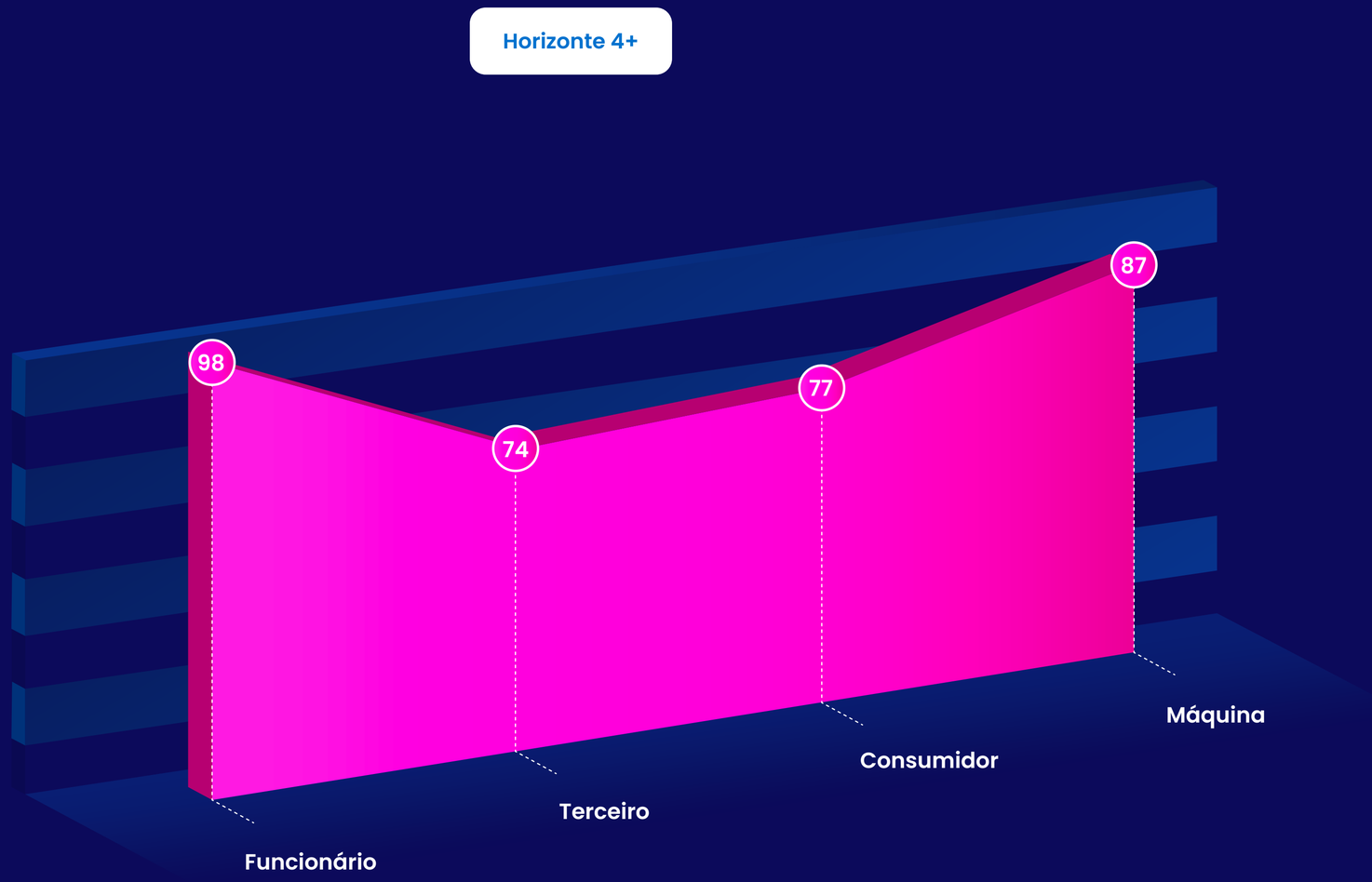
As organizações do Horizonte 1 e 2 têm uma **grande falha na cobertura de identidade.**

30%
Funcionários

62%
Terceiros

72%
Identidades de máquina

O último caso é bastante preocupante, uma vez que as identidades de máquina normalmente representam cerca de 40% a 65% do total de identidades em uma organização.



As organizações no Horizonte 4+ reduzem o risco com cobertura de capacidade de 70% em todos os tipos de identidade. O Horizonte 3 está logo atrás.

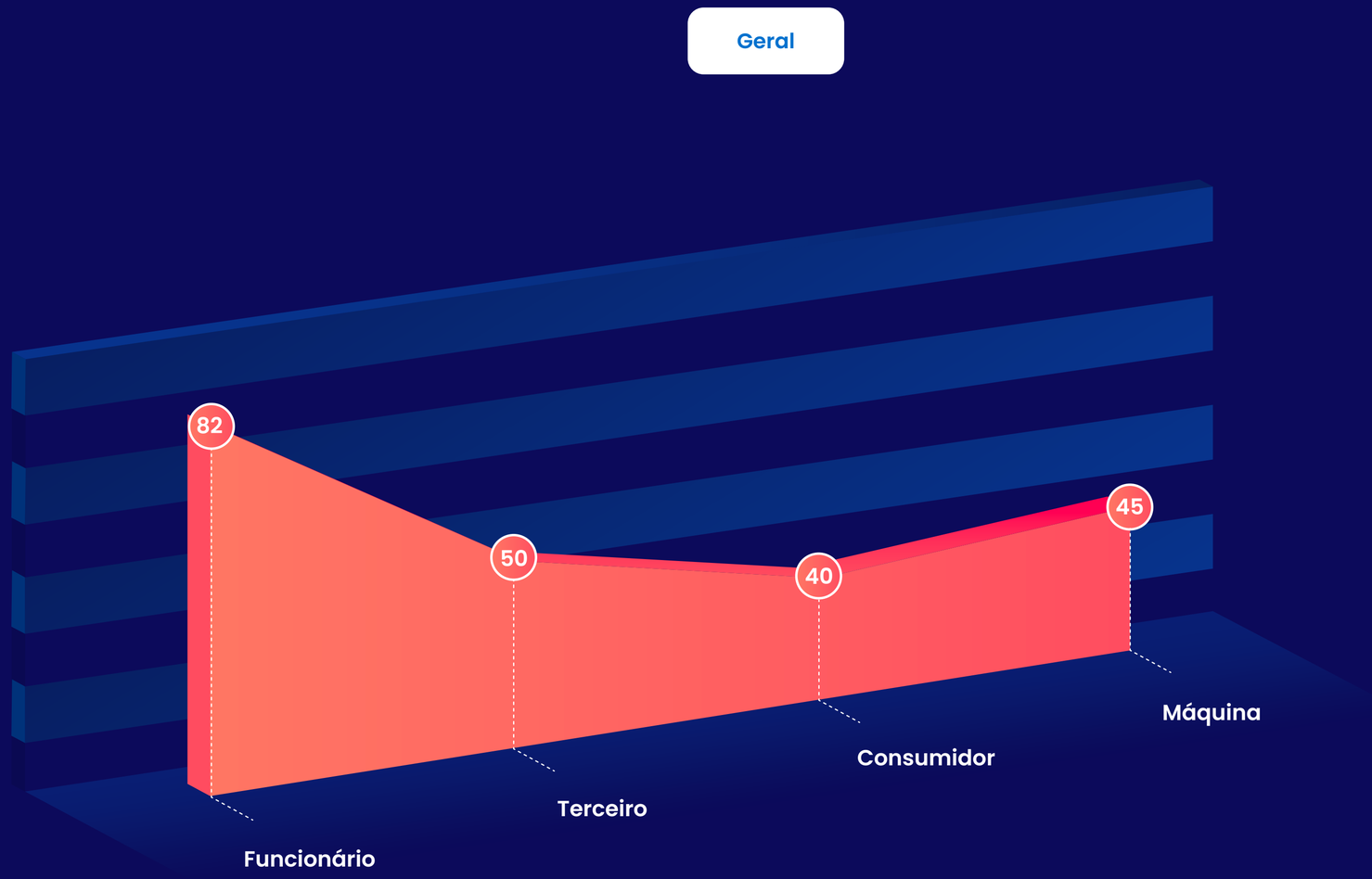
As organizações do Horizonte 1 e 2 têm uma **grande falha na cobertura de identidade.**

30%
Funcionários

62%
Terceiros

72%
Identidades de máquina

O último caso é bastante preocupante, uma vez que as identidades de máquina normalmente representam cerca de 40% a 65% do total de identidades em uma organização.



As organizações no Horizonte 4+ reduzem o risco com cobertura de capacidade de 70% em todos os tipos de identidade. O Horizonte 3 está logo atrás.

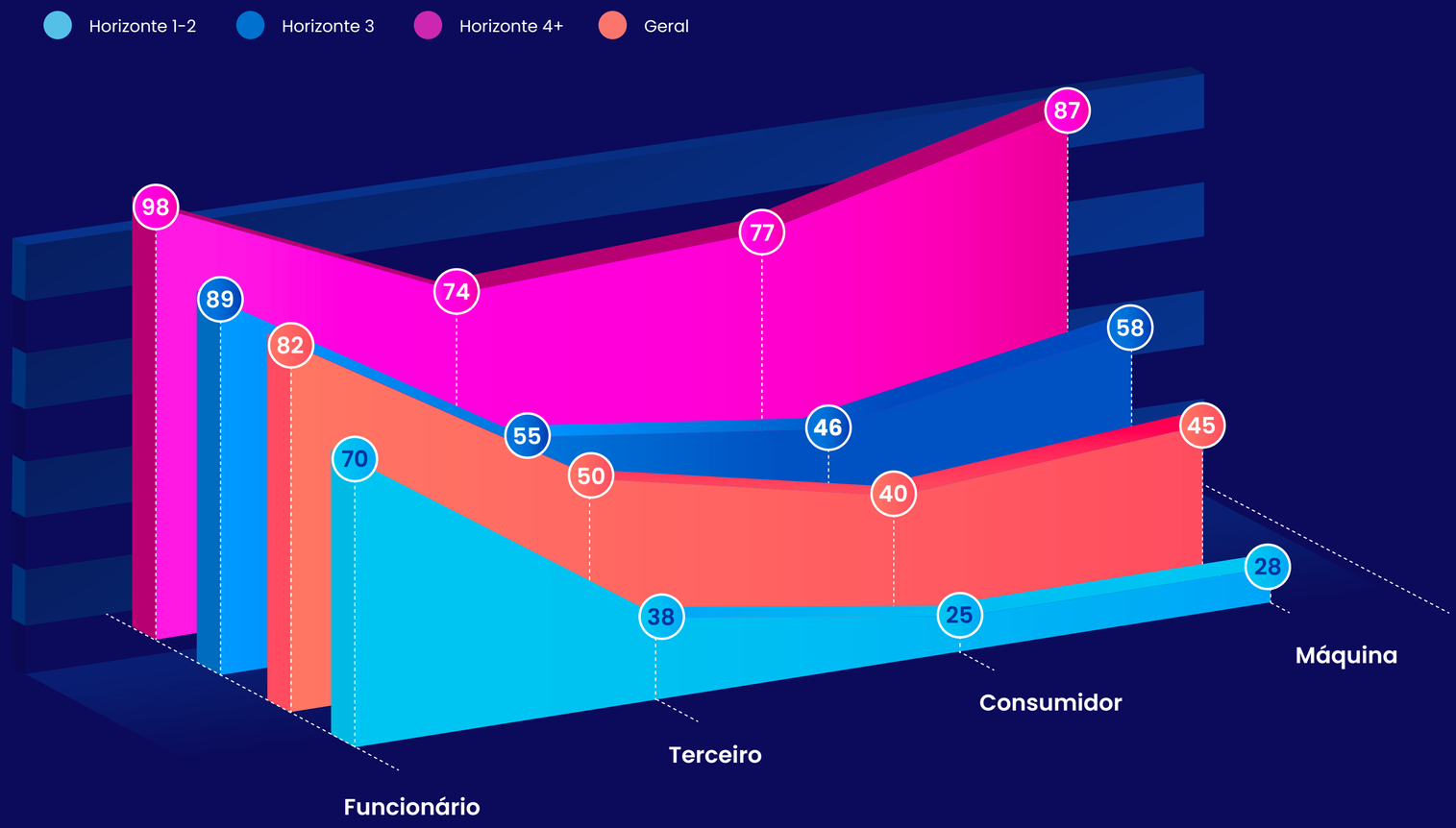
As organizações do Horizonte 1 e 2 têm uma **grande falha na cobertura de identidade.**

30%
Funcionários

62%
Terceiros

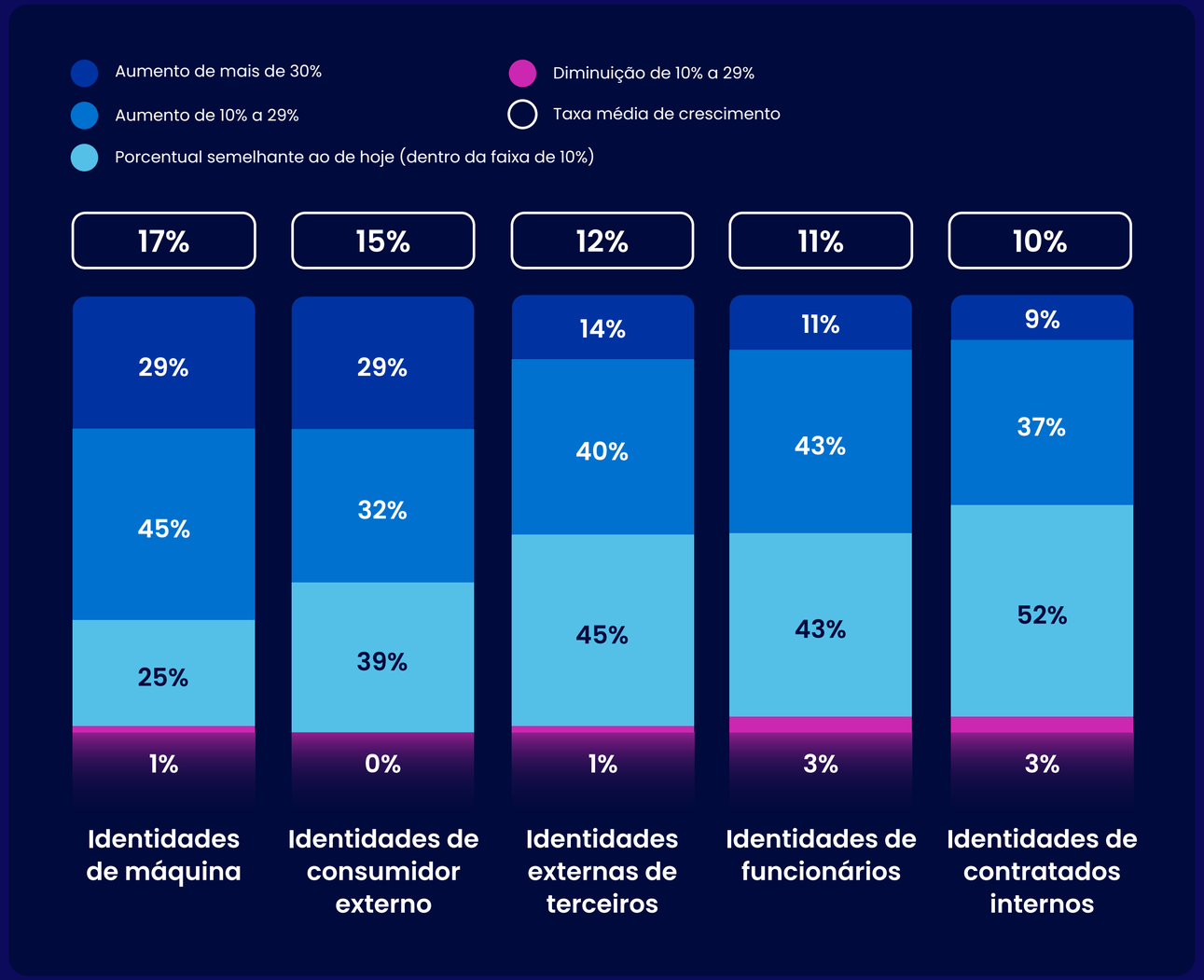
72%
Identidades de máquina

O último caso é bastante preocupante, uma vez que as identidades de máquina normalmente representam cerca de 40% a 65% do total de identidades em uma organização.

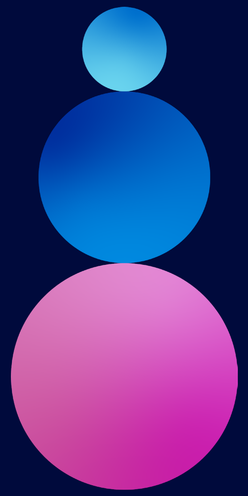


Supostamente todas as identidades devem crescer cerca de 14% nos próximos 3 a 5 anos e as identidades de máquinas deverão crescer mais rapidamente.

O crescimento do número de identidades de máquinas pode superar o crescimento das identidades humanas.



As organizações do Horizonte 4+ têm o dobro de chances de usar dados de identidade para inteligência acionável e novos casos de uso



<20%

das organizações do Horizonte 1 e 2 aproveitam os dados de inteligência de identidade em escala.

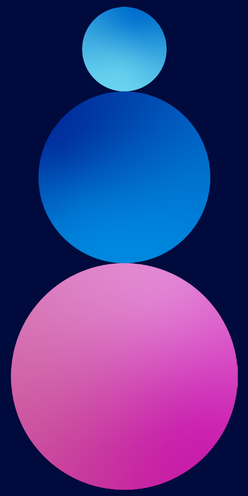
<40%

das organizações do Horizonte 3 aproveitam dados de inteligência de identidade em escala.

~50%

das organizações do Horizonte 4+ usam orientação inteligente a partir de dados estruturados e não estruturados para acesso do usuário, políticas de segurança e análises de acesso.

As organizações do Horizonte 4+ têm o dobro de chances de usar dados de identidade para inteligência acionável e novos casos de uso



<20%

das organizações do Horizonte 1 e 2 aproveitam os dados de inteligência de identidade em escala.

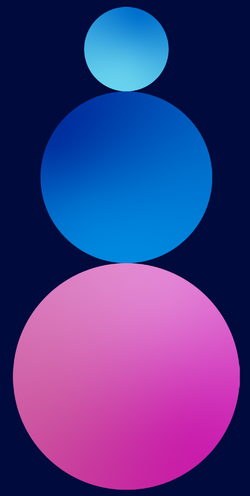
<40%

das organizações do Horizonte 3 aproveitam dados de inteligência de identidade em escala.

~50%

das organizações do Horizonte 4+ usam orientação inteligente a partir de dados estruturados e não estruturados para acesso do usuário, políticas de segurança e análises de acesso.

As organizações do Horizonte 4+ têm o dobro de chances de usar dados de identidade para inteligência acionável e novos casos de uso



<20%

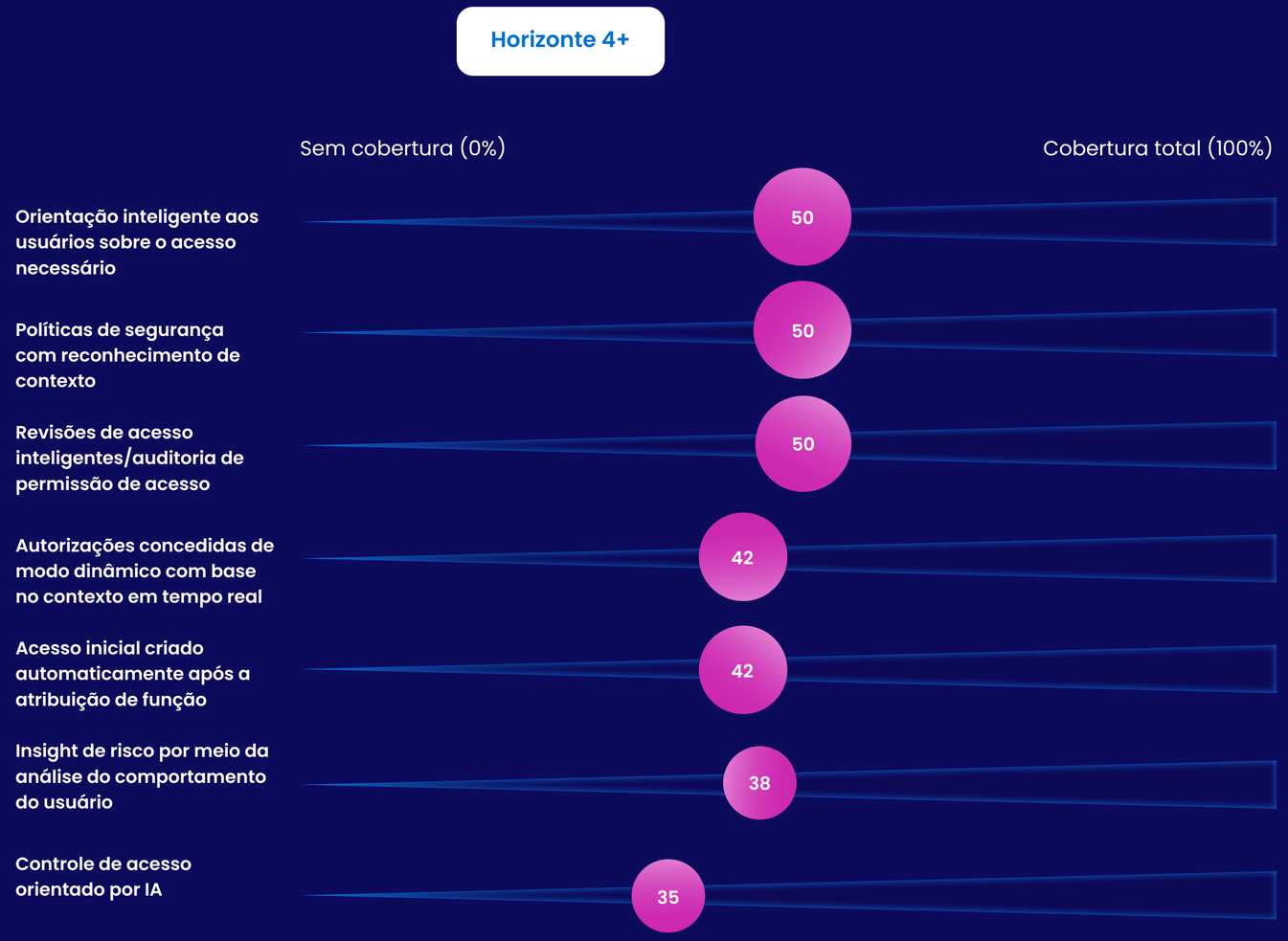
das organizações do Horizonte 1 e 2 aproveitam os dados de inteligência de identidade em escala.

<40%

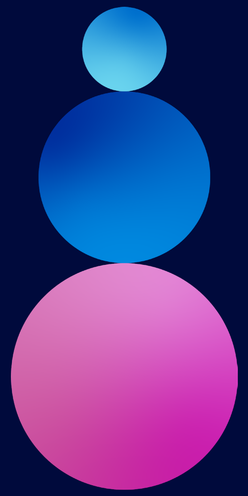
das organizações do Horizonte 3 aproveitam dados de inteligência de identidade em escala.

~50%

das organizações do Horizonte 4+ usam orientação inteligente a partir de dados estruturados e não estruturados para acesso do usuário, políticas de segurança e análises de acesso.



As organizações do Horizonte 4+ têm o dobro de chances de usar dados de identidade para inteligência acionável e novos casos de uso



<20%

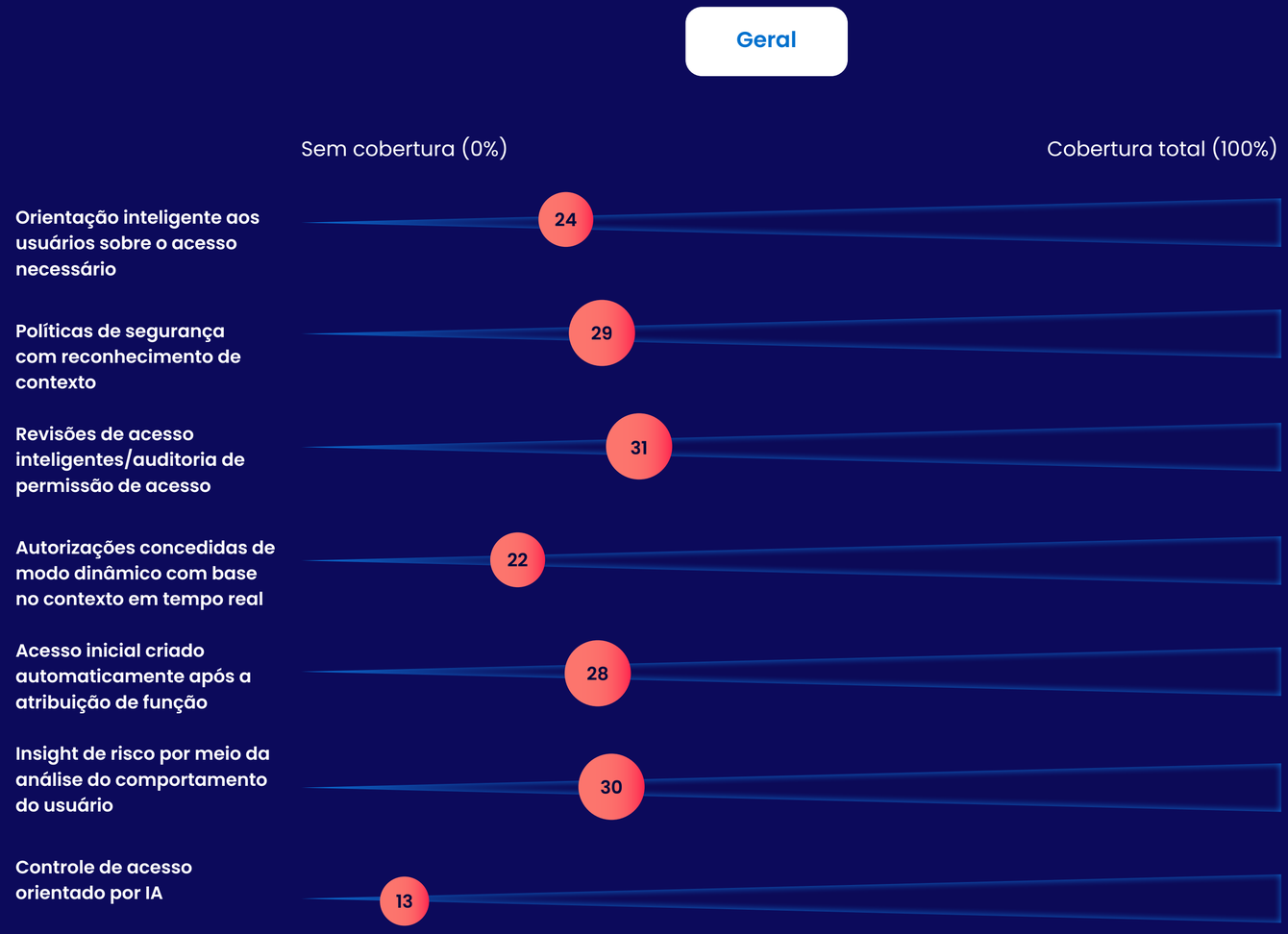
das organizações do Horizonte 1 e 2 aproveitam os dados de inteligência de identidade em escala.

<40%

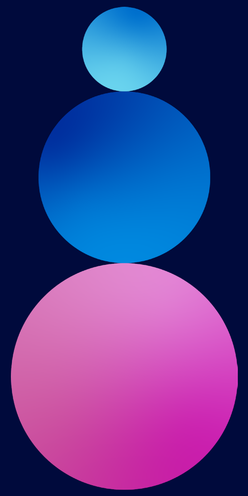
das organizações do Horizonte 3 aproveitam dados de inteligência de identidade em escala.

~50%

das organizações do Horizonte 4+ usam orientação inteligente a partir de dados estruturados e não estruturados para acesso do usuário, políticas de segurança e análises de acesso.



As organizações do Horizonte 4+ têm o dobro de chances de usar dados de identidade para inteligência acionável e novos casos de uso



<20%

das organizações do Horizonte 1 e 2 aproveitam os dados de inteligência de identidade em escala.

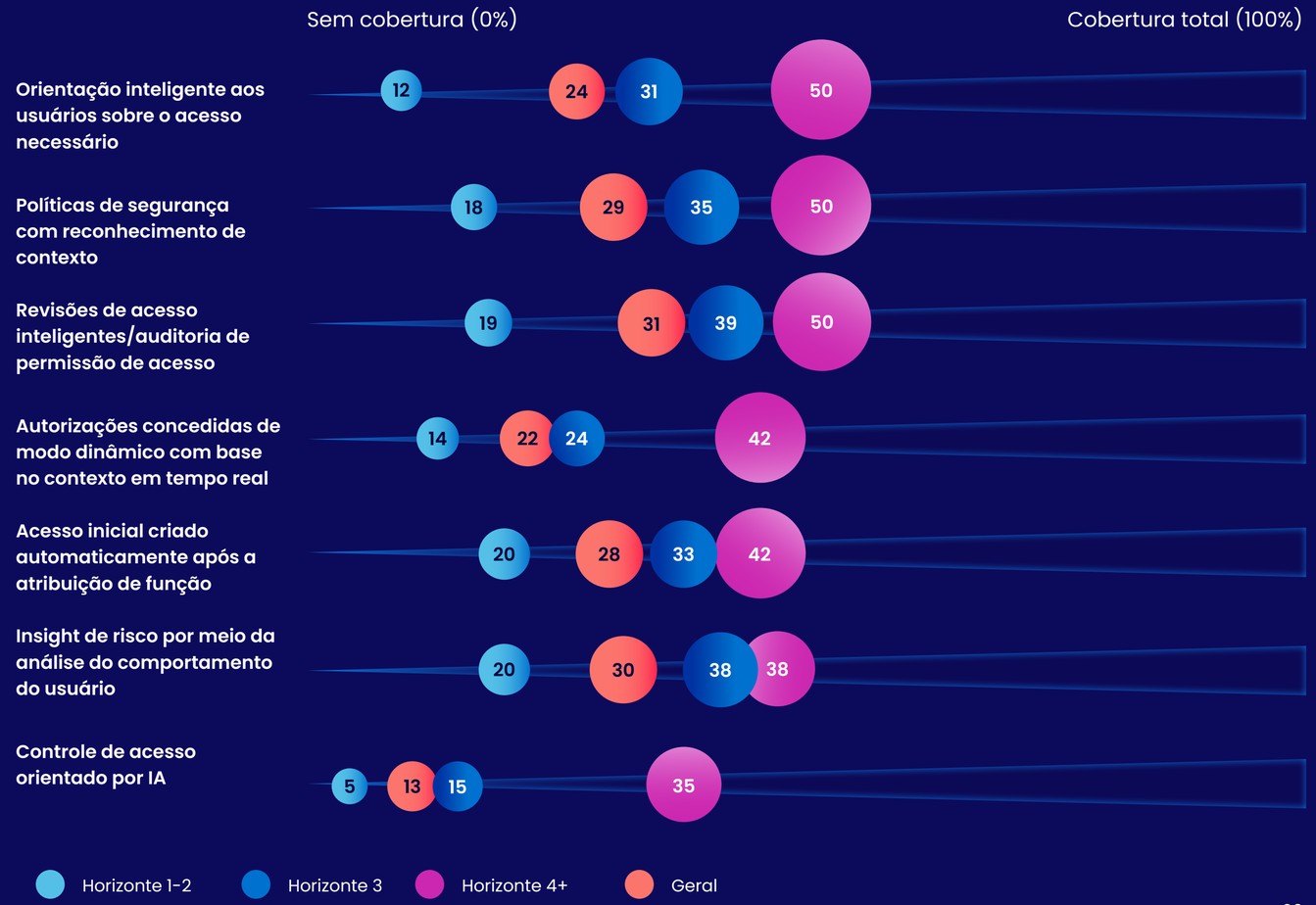
<40%

das organizações do Horizonte 3 aproveitam dados de inteligência de identidade em escala.

~50%

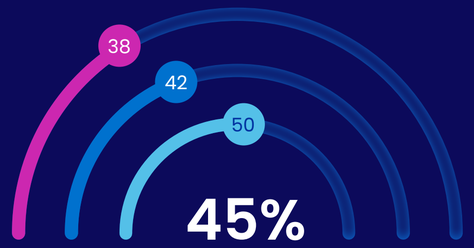
das organizações do Horizonte 4+ usam orientação inteligente a partir de dados estruturados e não estruturados para acesso do usuário, políticas de segurança e análises de acesso.

Todos os dados

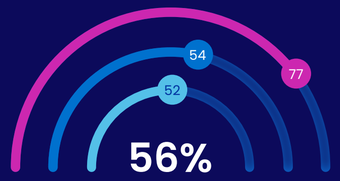


As organizações com segurança de identidade madura têm os pré-requisitos para investir em casos de uso dimensionáveis com base em GenAI

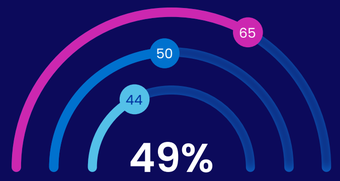
As organizações do Horizonte 3+ têm a atenção voltada para a engenharia de soluções em escala para aumentar e dimensionar sua segurança de identidade. As organizações do Horizonte 1-2, por sua vez, se concentram na automação de atividades repetitivas do tipo helpdesk.



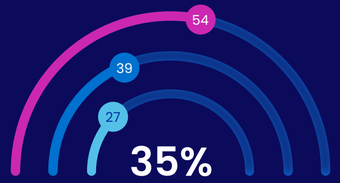
Chatbots de IA para suporte instantâneo ao IAM e tratamento de riscos



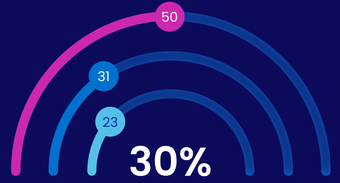
Criação de fluxo de trabalho baseado em IA (incluindo provisionamento de usuários, revisões de acesso e gerenciamento de funções)



Direito de usuário gerado por IA e descrições de funções (incluindo direitos, privilégios e níveis de acesso)



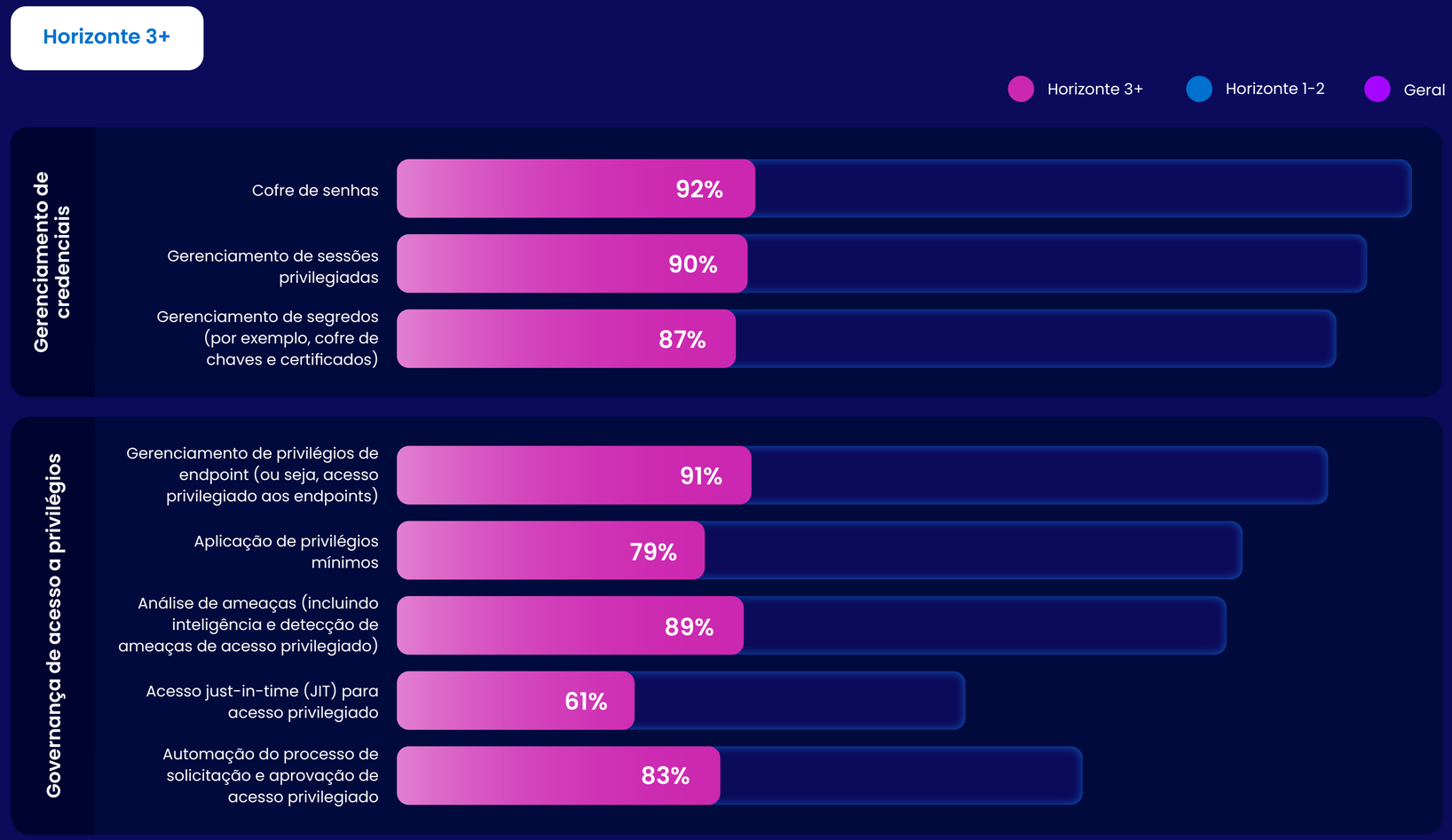
Pesquisa em linguagem natural para obter dados de IAM com facilidade



Copilotos para desenvolvimento de conectores automatizados

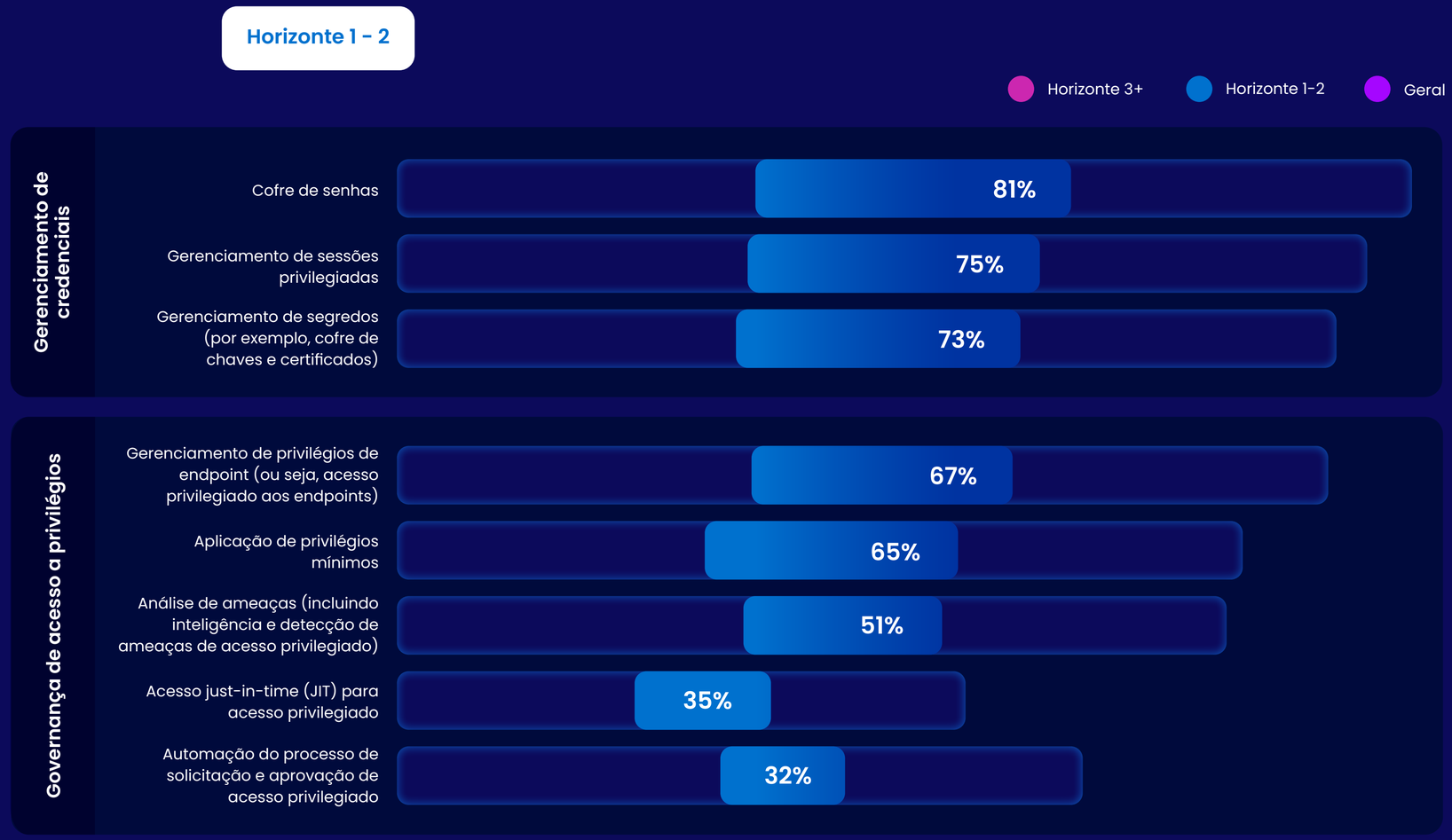
As organizações do Horizonte 3+ têm adoção até 50% maior dos recursos de governança de acesso a privilégios em comparação aos Horizontes 1–2

Com investimento em soluções além do cofre de credenciais e do gerenciamento de sessões, as organizações podem simplificar a aprovação e as solicitações de acesso e melhorar a análise de ameaças para contas privilegiadas.



As organizações do Horizonte 3+ têm adoção até 50% maior dos recursos de governança de acesso a privilégios em comparação aos Horizontes 1-2

Com investimento em soluções além do cofre de credenciais e do gerenciamento de sessões, as organizações podem simplificar a aprovação e as solicitações de acesso e melhorar a análise de ameaças para contas privilegiadas.

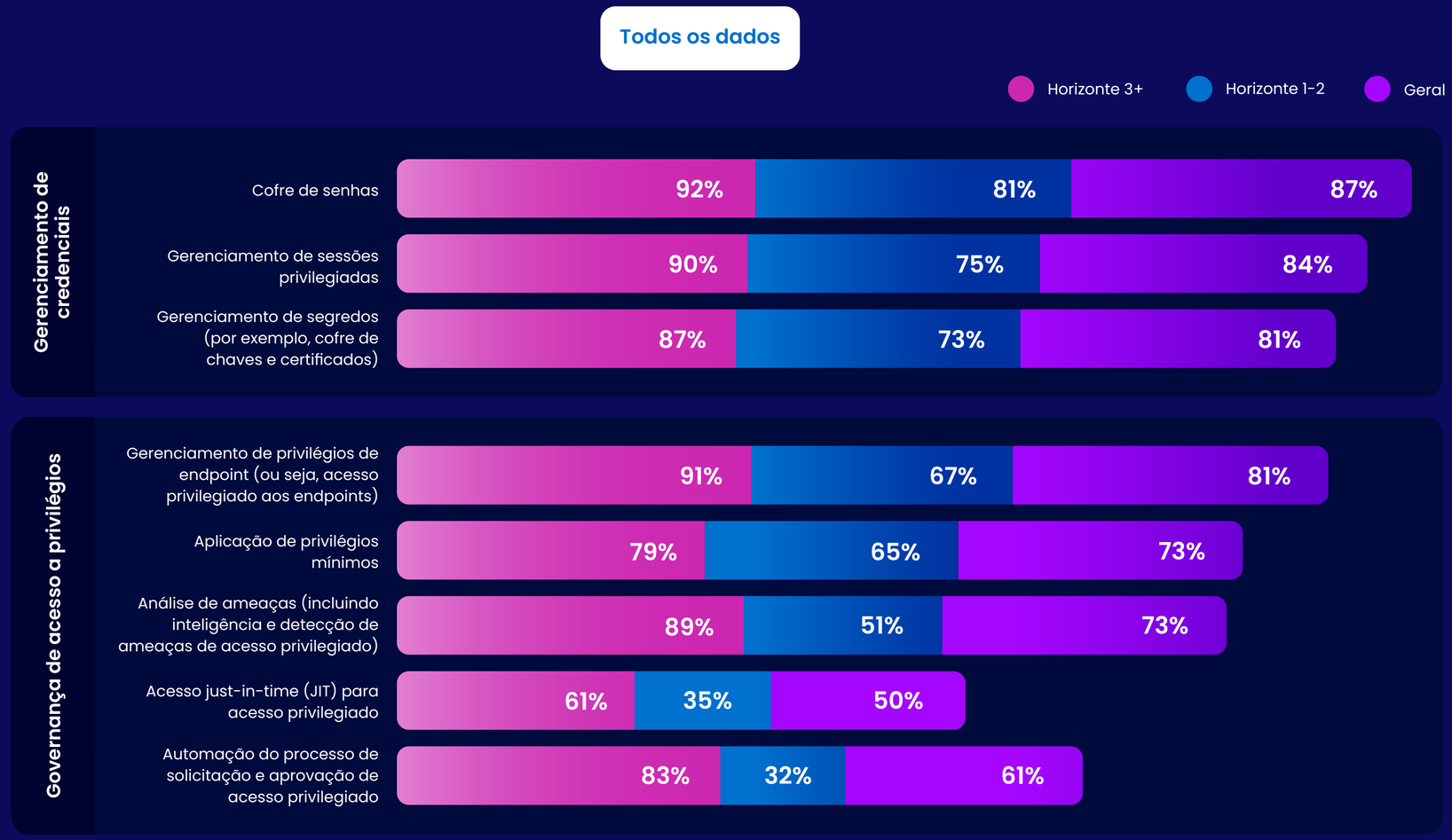


As organizações do Horizonte 3+ têm adoção até 50% maior dos recursos de governança de acesso a privilégios em comparação aos Horizontes 1-2

Com investimento em soluções além do cofre de credenciais e do gerenciamento de sessões, as organizações podem simplificar a aprovação e as solicitações de acesso e melhorar a análise de ameaças para contas privilegiadas.

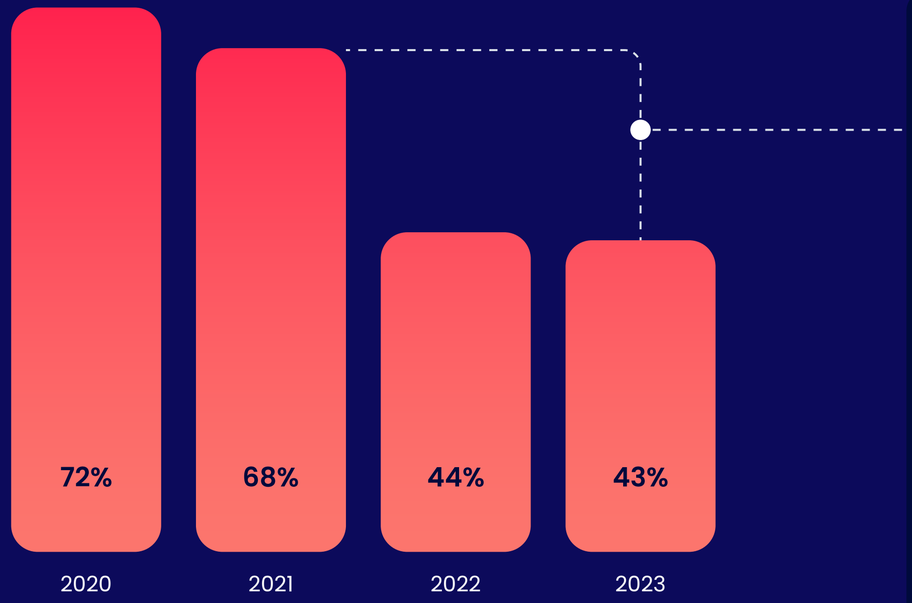
As organizações do Horizonte 3+ têm adoção até 50% maior dos recursos de governança de acesso a privilégios em comparação aos Horizontes 1-2

Com investimento em soluções além do cofre de credenciais e do gerenciamento de sessões, as organizações podem simplificar a aprovação e as solicitações de acesso e melhorar a análise de ameaças para contas privilegiadas.



À medida que as seguardoras especializadas desenvolvem métodos mais maduros de avaliar o gerenciamento de riscos cibernéticos, os prêmios de seguro cibernético aumentam

As seguradoras cibernéticas reduziram os índices de perda, amadureceram a avaliação e o gerenciamento de riscos. . .

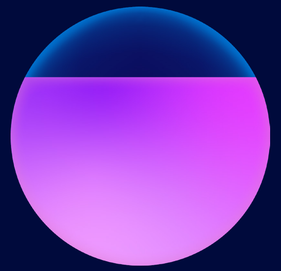


Índices de perda de cobertura cibernética independente, parcela de prêmios pagos como sinistros.

40%

A redução das perdas entre as seguradoras cibernéticas indica uma melhor gestão do risco cibernético

. . .e aumentaram os prêmios para corresponder ao perfil de risco elevado.



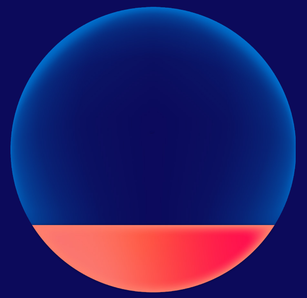
77%

Das organizações relataram aumento nos prêmios nos últimos três anos

As seguradoras estão agora analisando mais a fundo para saber que controles de segurança uma empresa tem... elas podem incentivar com descontos para a implementação de novos controles de segurança.

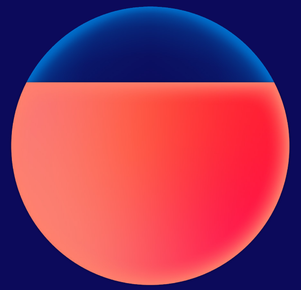
Profissional de seguros cibernéticos de uma grande corretora

Os clientes de seguros cibernéticos relatam que os recursos de segurança de identidade têm o maior impacto nas avaliações de seguros



25%

25% dos entrevistados consideram o IAM o elemento mais crítico nas avaliações de seguro cibernético, a maior parcela.



73%

dos clientes de seguros cibernéticos consideram os recursos de IAM entre as três principais funções que influenciam as avaliações de seguros.

Principais recursos de segurança cibernética que influenciam as avaliações de seguro cibernético. % dos entrevistados que selecionaram o recurso como o que tem maior influência.

[1] Inclui segurança web e MSSP/terceirização

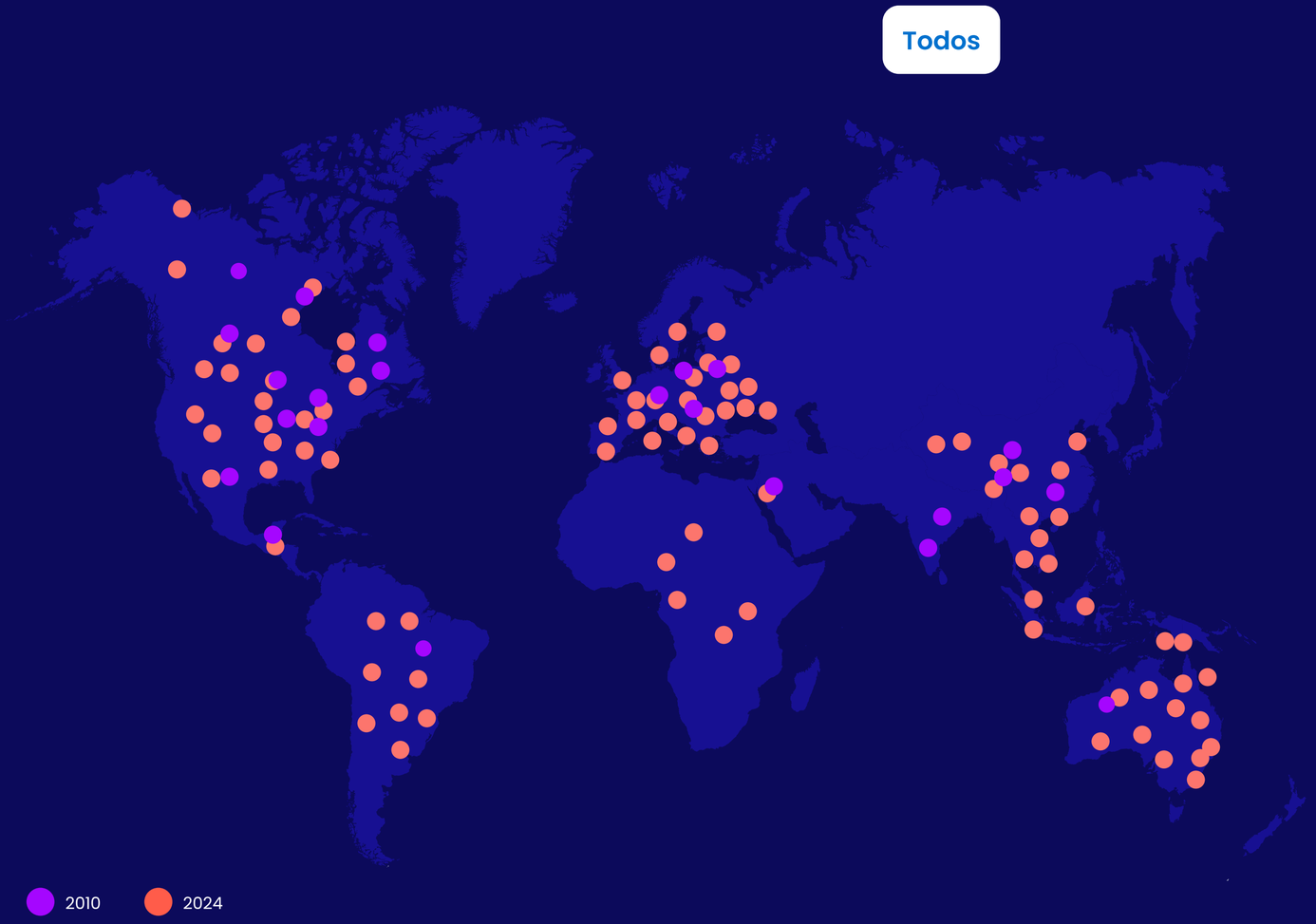
Regulamentações relativas à identidade cresceram sete vezes desde 2010 em todas as regiões e setores

Aumento de mais de 5x

em regulamentações de setores fora de finanças e saúde.

Aumento de mais de 13x

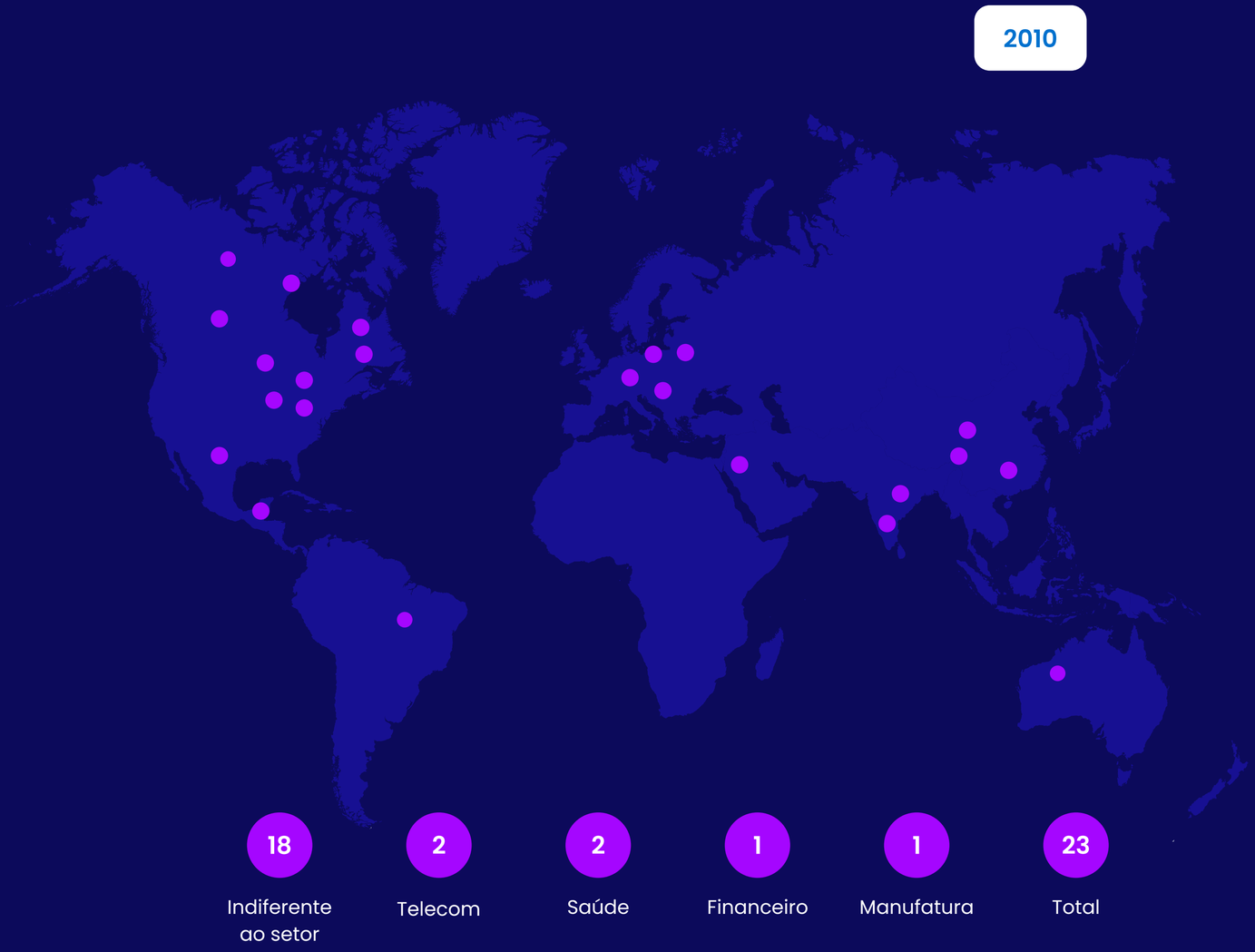
em regulamentações fora da América do Norte, APAC e Europa.



Regulamentações relativas à identidade cresceram sete vezes desde 2010 em todas as regiões e setores

~25

egulamentações e estruturas totais estavam concentradas em regiões maduras e setores selecionados em 2012.

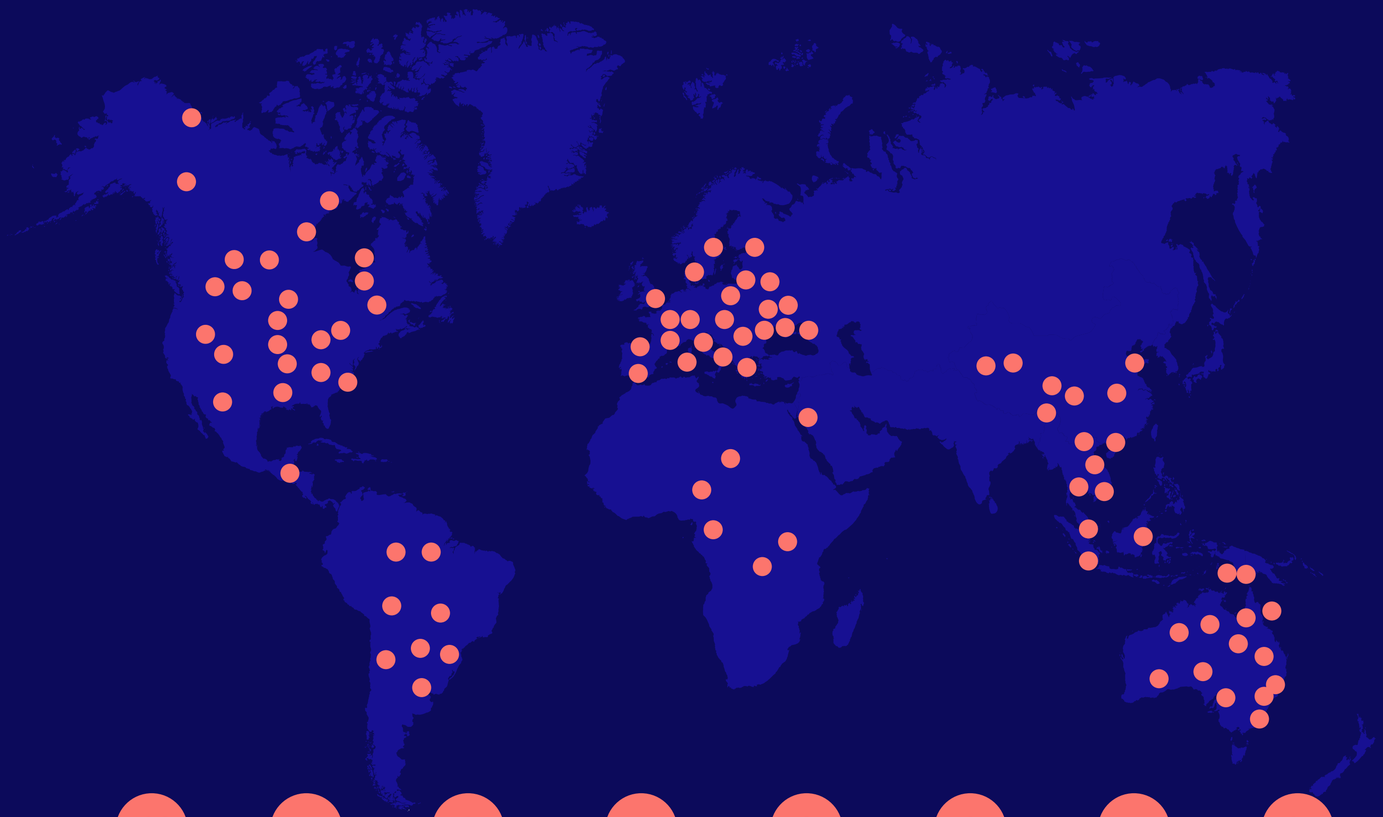


Regulamentações relativas à identidade cresceram sete vezes desde 2010 em todas as regiões e setores

~135

regulamentações e estruturas com crescimento substancial em todas as regiões e setores em 2024.

2024



Indiferente ao de setor	Telecom	Financeiro	Saúde	Manufatura	Outro	Governo	Total
103 ~6x	11 ~5x	9 9x	5 ~3x	3 3x	2	1	134

CAPÍTULO 4

Como as organizações líderes estão otimizando a curva de valor.

Estudos de caso de organizações

Em todo o mundo e em todos os setores, as principais organizações estão investindo em segurança de identidade para otimizar a curva de valor da segurança cibernética, oferecendo retornos desproporcionais em conformidade, eficiência operacional, produtividade e segurança do usuário.

BNP PARIBAS

Meta:

Reduzir o risco cibernético e melhorar a produtividade

O BNP Paribas Bank Polska aumentou a produtividade com uma grande automação de tarefas manuais de IAM.

Após uma série de fusões, o banco estava gerenciando 10.000 usuários e cerca de 1.000 aplicativos por meio de programas de IAM desconexos. Sem automação, a equipe de TI não conseguia lidar com o volume de solicitações de usuários ou tarefas de IAM. Com a automação, todas as campanhas de certificação agora são gerenciadas por apenas dois funcionários e cada um dedica apenas cerca de 15% do tempo de trabalho.

40 mil

tarefas de identidade automatizadas executadas mensalmente

90%

das solicitações de acesso executadas de forma automática

4 mil

redefinições e alterações de senha automatizadas por mês

Meta:

Produtividade

Uma grande empresa farmacêutica com 72.000 funcionários aumentou a produtividade e a eficiência automatizando as tarefas de IAM.

A empresa buscava um sistema escalável e baseado na nuvem para substituir sua solução de identidade, local e antiquada, que exigia uma manutenção manual significativa. Ao integrar um novo sistema baseado na nuvem, a empresa simplificou a conformidade regulatória e alcançou reduções notáveis no tempo gasto em revisões de acesso e espera por acesso.

40%

de redução no tempo gasto em revisões de acesso

20%

de redução no tempo gasto na espera pelo acesso

30%

de redução de tarefas manuais realizadas pela equipe de TI

Meta:

Maior valor de negócios

O banco Absa, uma instituição financeira panafricana com mais de 35.000 funcionários, simplificou a integração e a gestão de identidade de terceiros, reduzindo os custos.

Para garantir a conformidade com as regulamentações GDPR e POPIA, o banco implantou uma ferramenta de gerenciamento de risco baseada em IA com provisionamento just-in-time e certificação padronizada para identidades de terceiros. Esse modelo de acesso baseado em risco reduziu a sobrecarga operacional e simplificou a governança de identidade para colaboradores contratados e não funcionários.

US$300

redução de custo por identidade integrada

15

dias: redução do tempo de integração de identidades de terceiros

12 mil

não funcionários com identidades seguras

Meta:

Redução de risco cibernético

A Currys, uma empresa varejista de tecnologia sediada no Reino Unido com mais de 800 lojas, reduziu o próprio perfil de risco aprimorando a governança da identidade e automatizando a segurança de identidade.

A Currys, uma empresa varejista de tecnologia sediada no Reino Unido com mais de 800 lojas, reduziu o próprio perfil de risco aprimorando a governança da identidade e automatizando a segurança de identidade. Sua metodologia anterior, com processos manuais baseados em Excel com um grupo de funcionários que mudava constantemente, levou a riscos de provisionamento excessivo e de conformidade. Agora, a automação fornece uma trilha de auditoria completa, minimizando os desafios de conformidade e as permissões não executadas, ao mesmo tempo em que fortalece a postura geral de segurança.

3x

redução de risco definindo privilégios apropriados para cerca de 6.000 contas

210

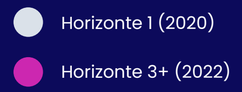
horas de tarefas manuais economizadas por ano

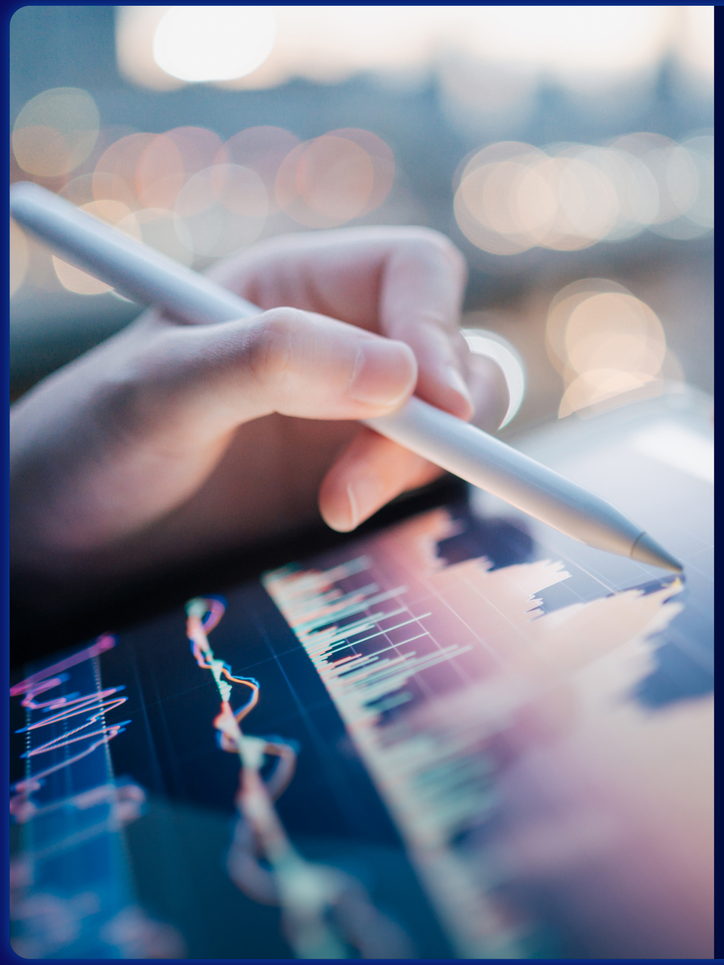
24MIL

identidades gerenciadas

Aboitiz, um grupo global de tecnologia, saltou do Horizonte 1 para o Horizonte 3+ em 24 meses com uma iniciativa de “Grande Transformação”

Passe o mouse sobre cada seção para ver qual ação foi tomada





“

Começamos do zero e isso nos deu a oportunidade de progredir usando a tecnologia...Decidimos investir tempo e recursos no ativo mais valioso da organização: a identidade.

CISO, Aboitiz Equity Ventures

aboitiz

CAPÍTULO 5

Seu caminho para o próximo horizonte.

Seu caminho para o próximo horizonte

1. Defina uma visão para seguir
2. Invista nas soluções certas, especialmente naquelas com IA para saltar horizontes e obter maiores retornos
3. Proteja todos os tipos de identidades
4. Integre IAM às operações de segurança mais amplas para monitoramento contínuo e controle de prêmios de seguro
5. Utilize dados de identidade para obter insights acionáveis e políticas de segurança adaptáveis
6. Antecipe-se aos novos regulamentos e padrões emergentes para manter a conformidade

Entenda melhor a maturidade da segurança de identidade e o horizonte da sua organização.

IB2569-2501