ManageEngine

O cenário da segurança cibernética no Brasil em 2024

manageengine.com/br/

Índice

Introdução 03

Pontos principais 04

Seção 1: Ameaças e impacto 07

Seção 2: Seguro de cibersegurança 09

Seção 3: O papel dos funcionários 11

Seção 4: O papel da IA 13

Seção 5: Aumento do estresse nas equipes de segurança cibernética 14

Seção 6: Conformidade 15

Conclusão 16

Uma pesquisa regional com executivos e profissionais de segurança

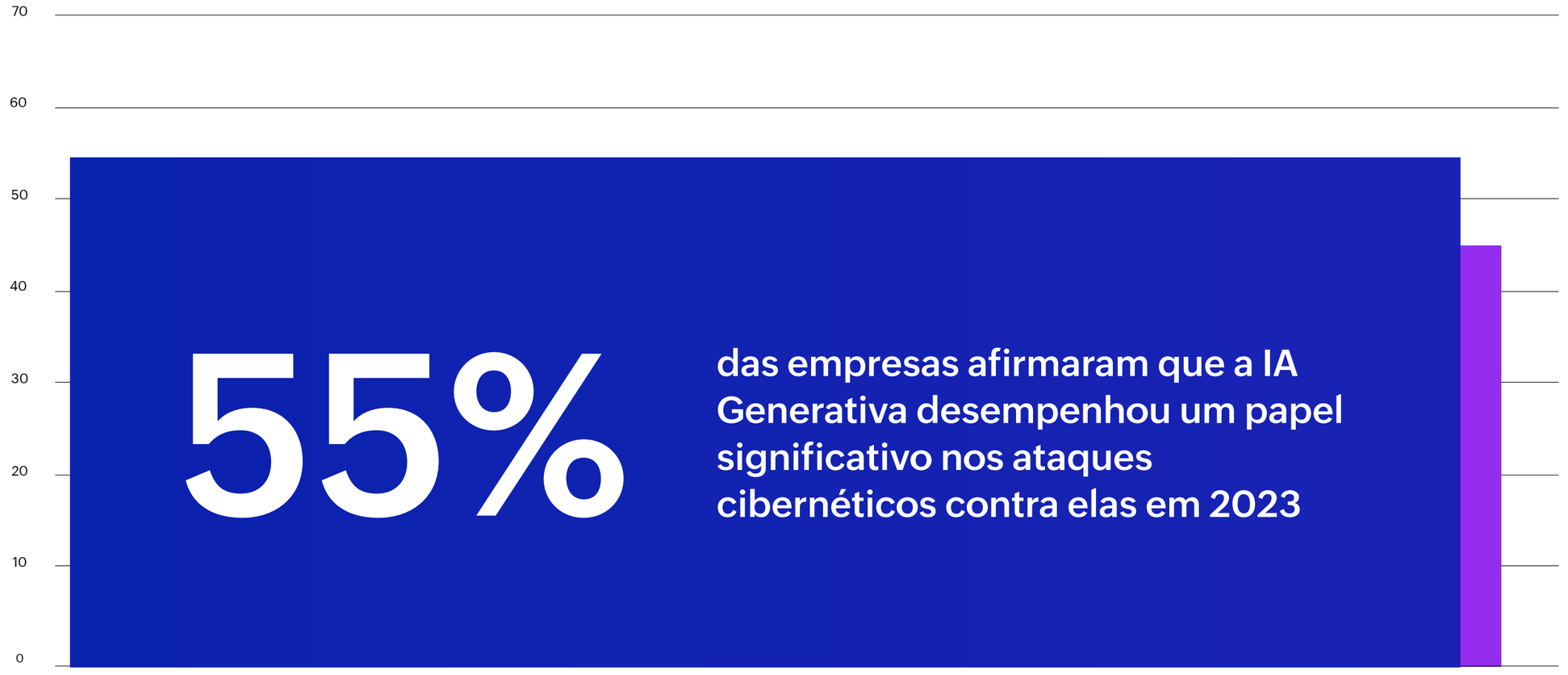
Introdução

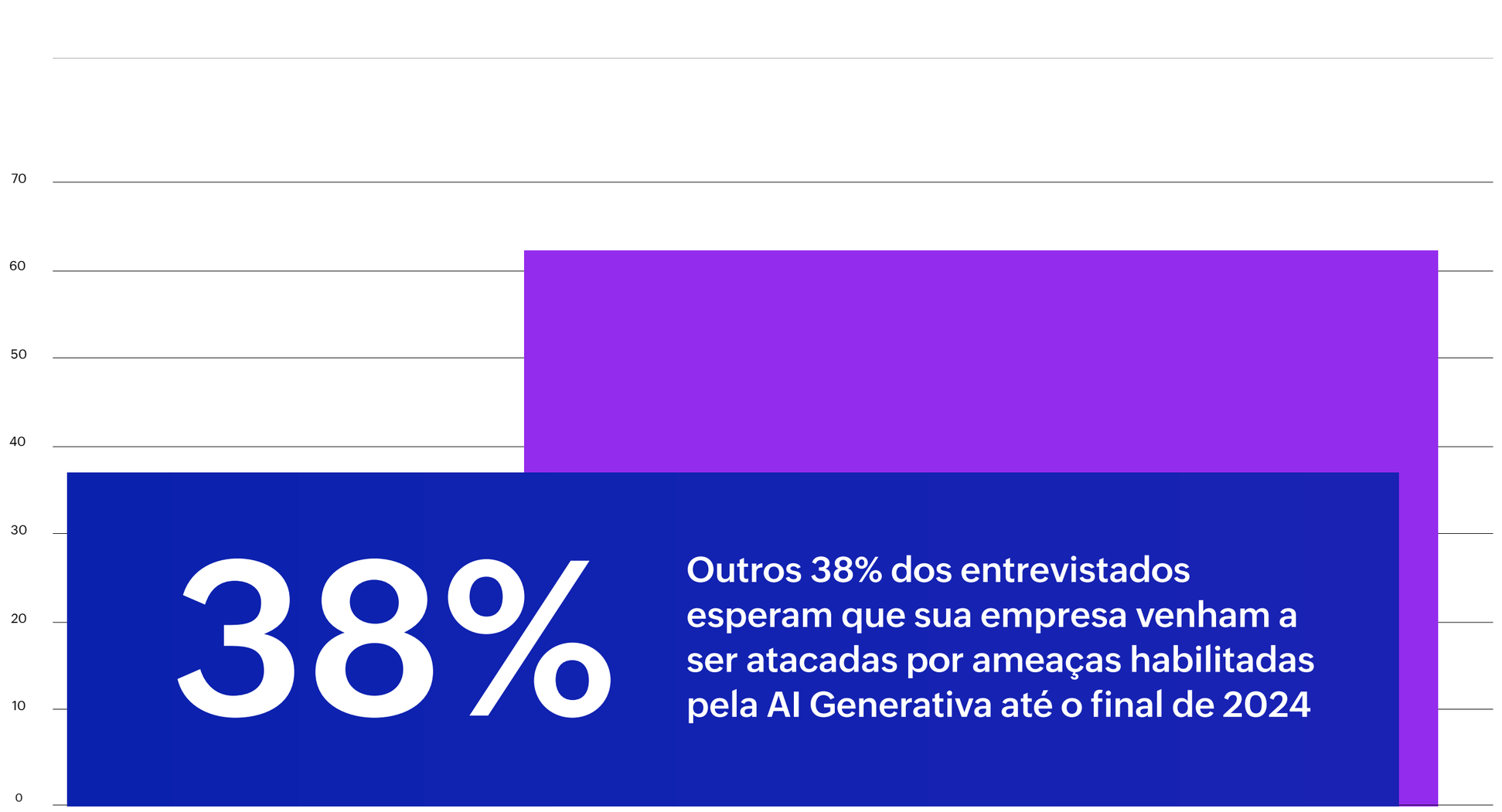
Este relatório fornece uma breve sinopse de uma pesquisa com foco no estado da segurança cibernética no Brasil. A pesquisa lança luz sobre o cenário de segurança de TI do país e o impacto da IA no pessoal de segurança e nas defesas. Além disso, investiga o uso de seguros de segurança cibernética e a capacidade de atender aos requisitos de gestão de dados.

A pesquisa reuniu respostas de 202 participantes que atuam em organizações brasileiras, desde pequenas até grandes empresas, em diversos segmentos da indústria. Os participantes ocupam cargos seniores, de nível gerencial e superior, e são diretamente responsáveis pela defesa e pelas estratégias de segurança de suas organizações.

Pontos principais

Os ataques potencializados pela IA inauguram uma nova era de ameaças à segurança com maior eficácia



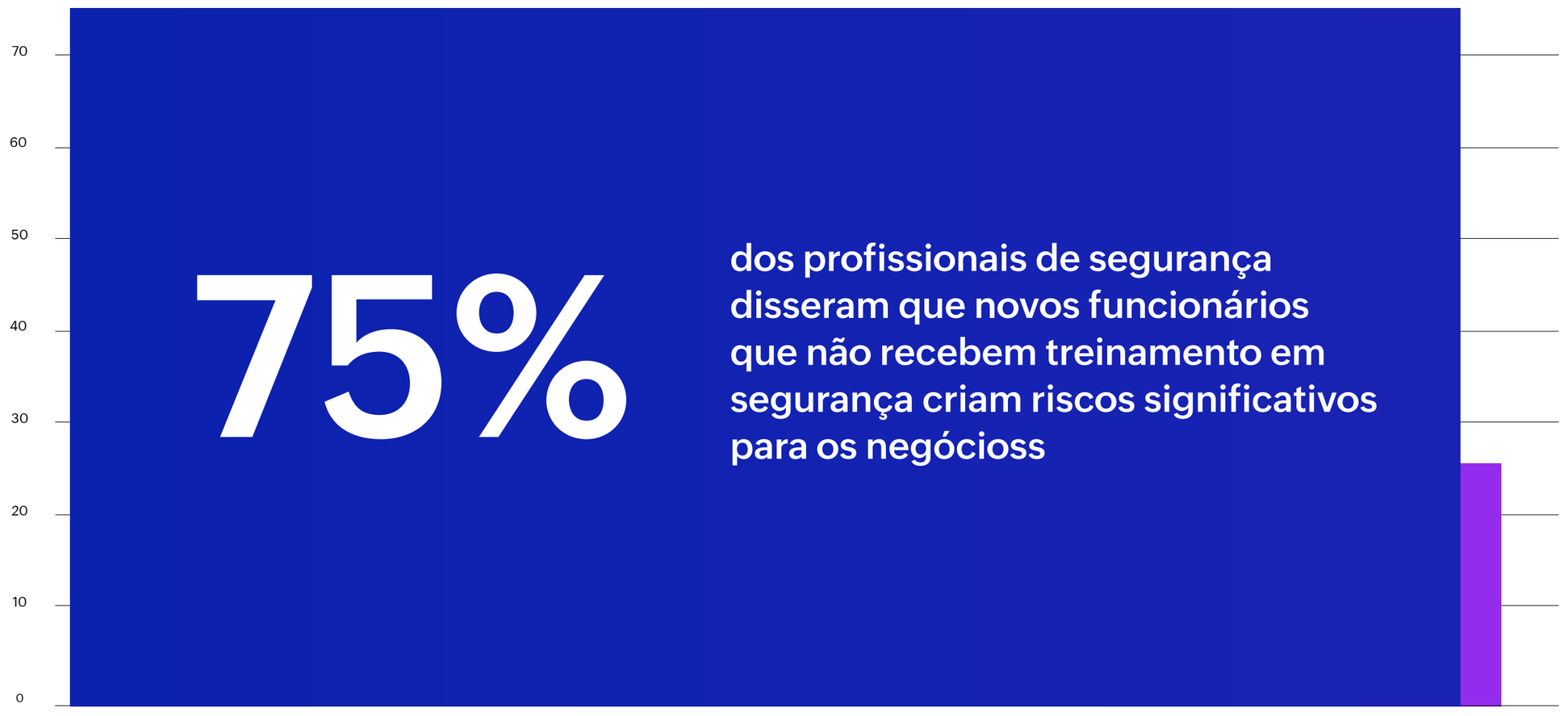


ManageEngine

Pontos principais

Os funcionários continuam sendo um dos elos mais fracos nas defesas de segurança

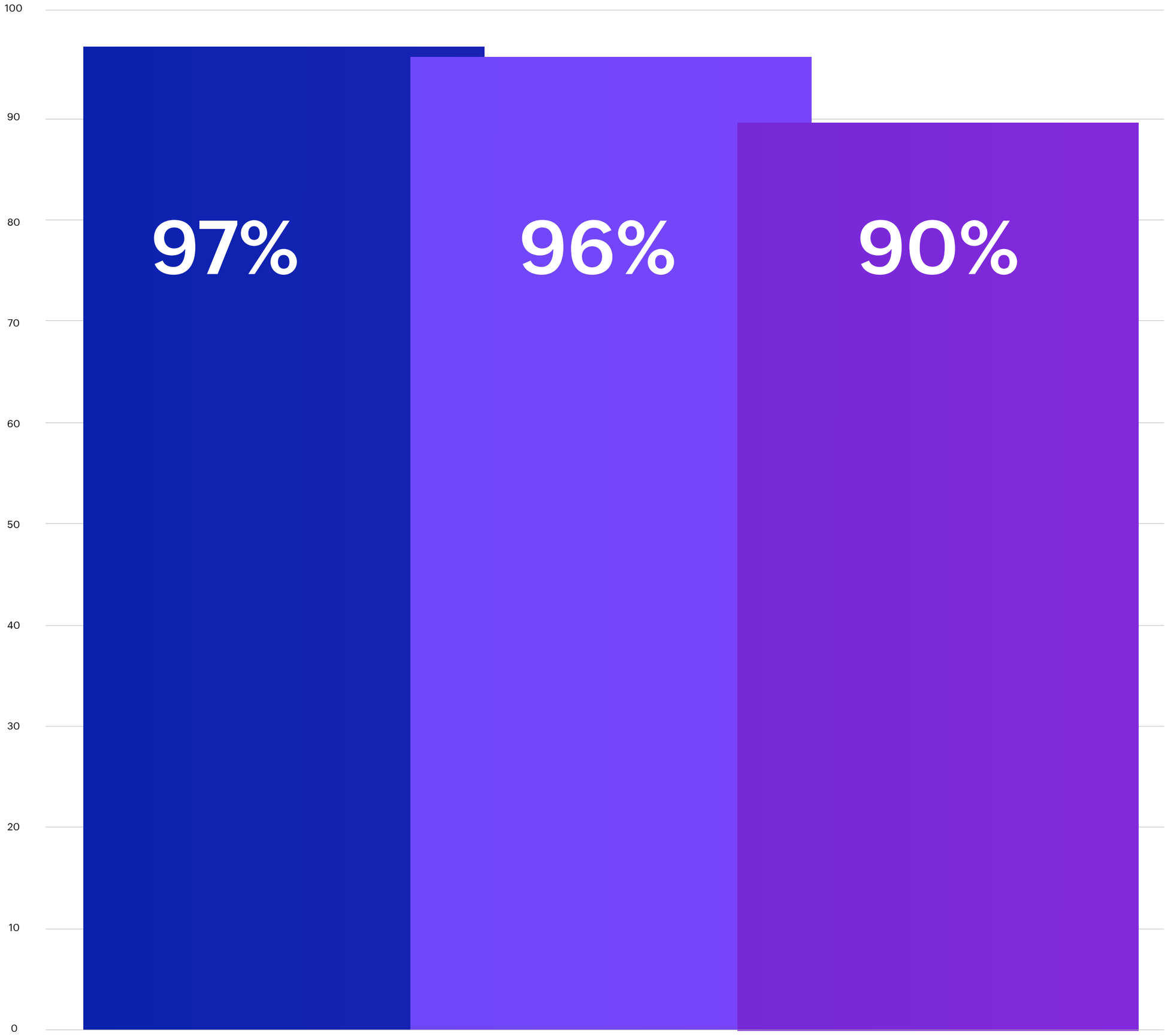
Os funcionários, seja por meio de acidentes ou atos intencionais (sabotagem), representam o segundo e o quarto lugar em vetor de ameaça mais perigosos, depois de entidades externas



ManageEngine

Pontos principais

Soluções de segurança habilitadas para IA são essenciais para defender os negócios em 2024



97% dos entrevistados compartilham que as soluções de segurança habilitadas para IA são essenciais para defender sua empresa

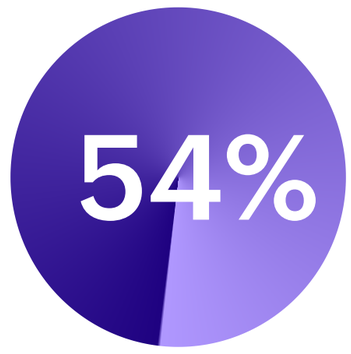
96% indicam que metade ou mais de todas as suas soluções de segurança serão alimentadas por IA até ao final de 2024

90% confiam unilateralmente em ferramentas de segurança habilitadas para IA para fazer mudanças e implementar ações

ManageEngine

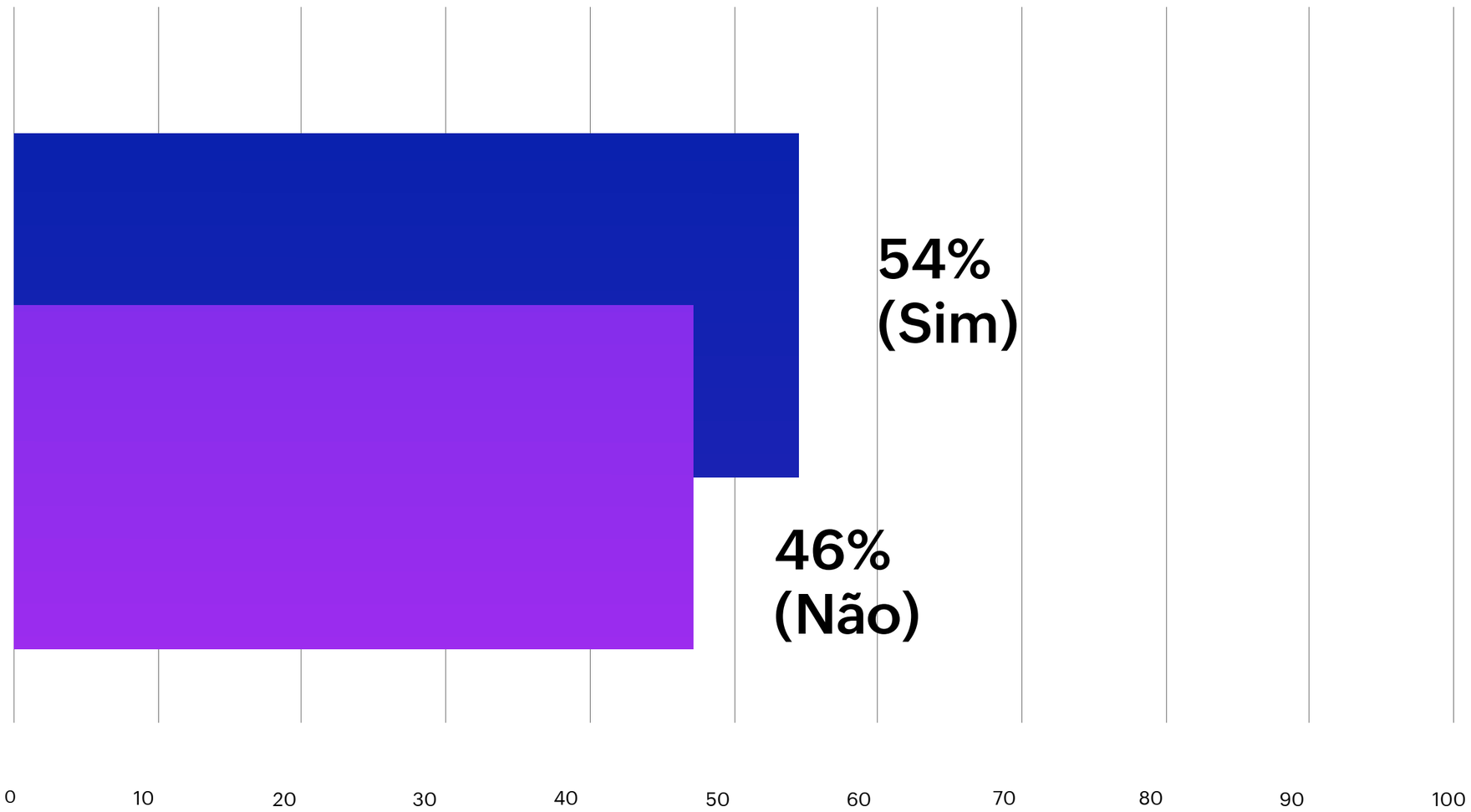
Seção 1: Ameaças e impacto

Em 2023, mais da metade (55%) das empresas brasileiras afirmaram que a IA generativa desempenhou um papel significativo nos ataques cibernéticos contra suas empresas.



54% dos entrevistados reconheceram que as suas empresas encontraram mais violações de segurança cibernética em 2023 em comparação com anos anteriores.

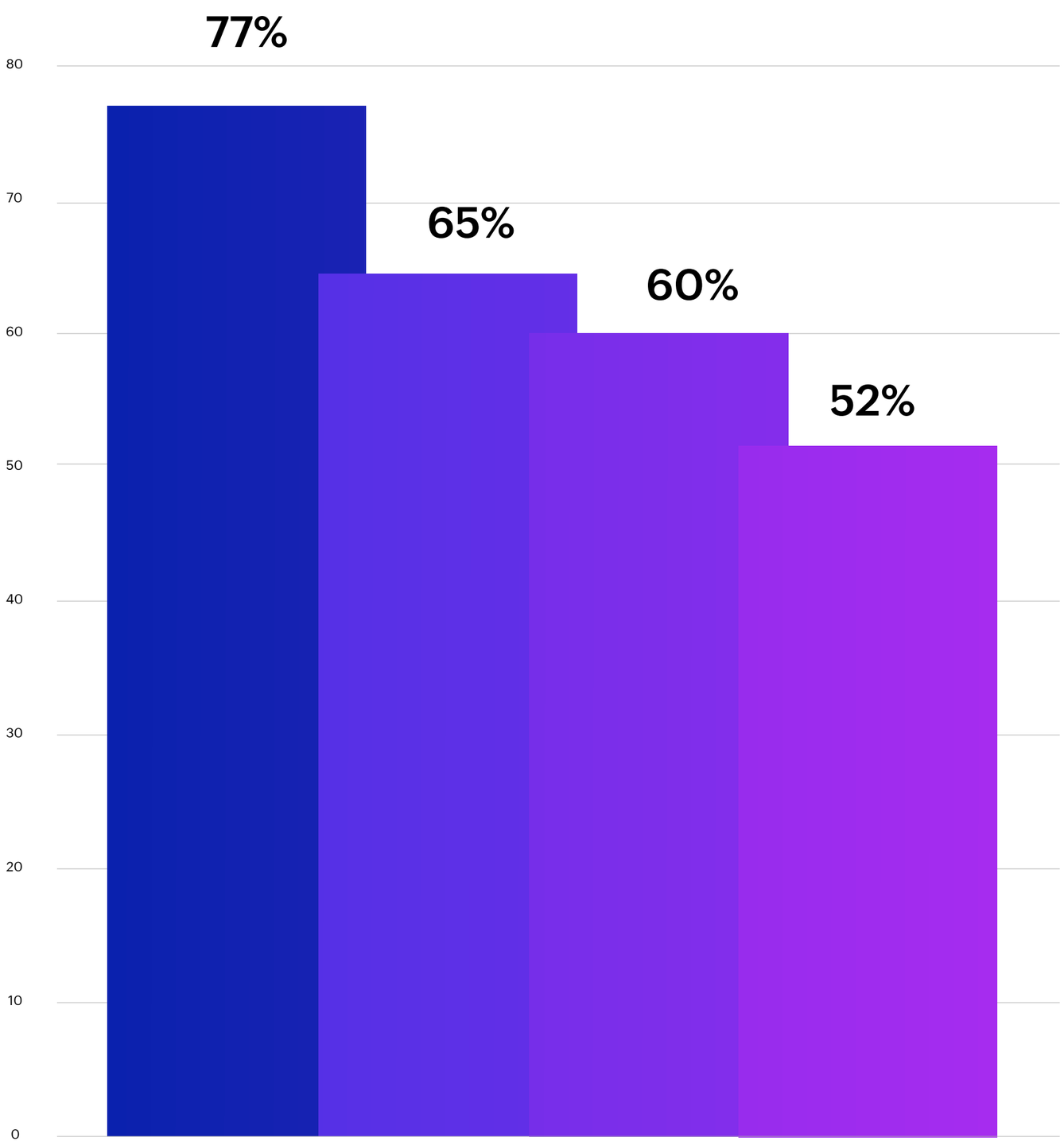
Q	A sua empresa sofreu mais violações de segurança cibernética (ataques bem-sucedidos) em 2023 em comparação com anos anteriores?



ManageEngine

Seção 1: Ameaças e impacto

Q	O que contribuiu para que sua empresa sofresse menos violações em 2023?



Aumento da alocação orçamentária para segurança cibernética: 77%

Soluções de segurança abrangentes implementadas: 65%

Equipe de segurança mais experiente: 60%

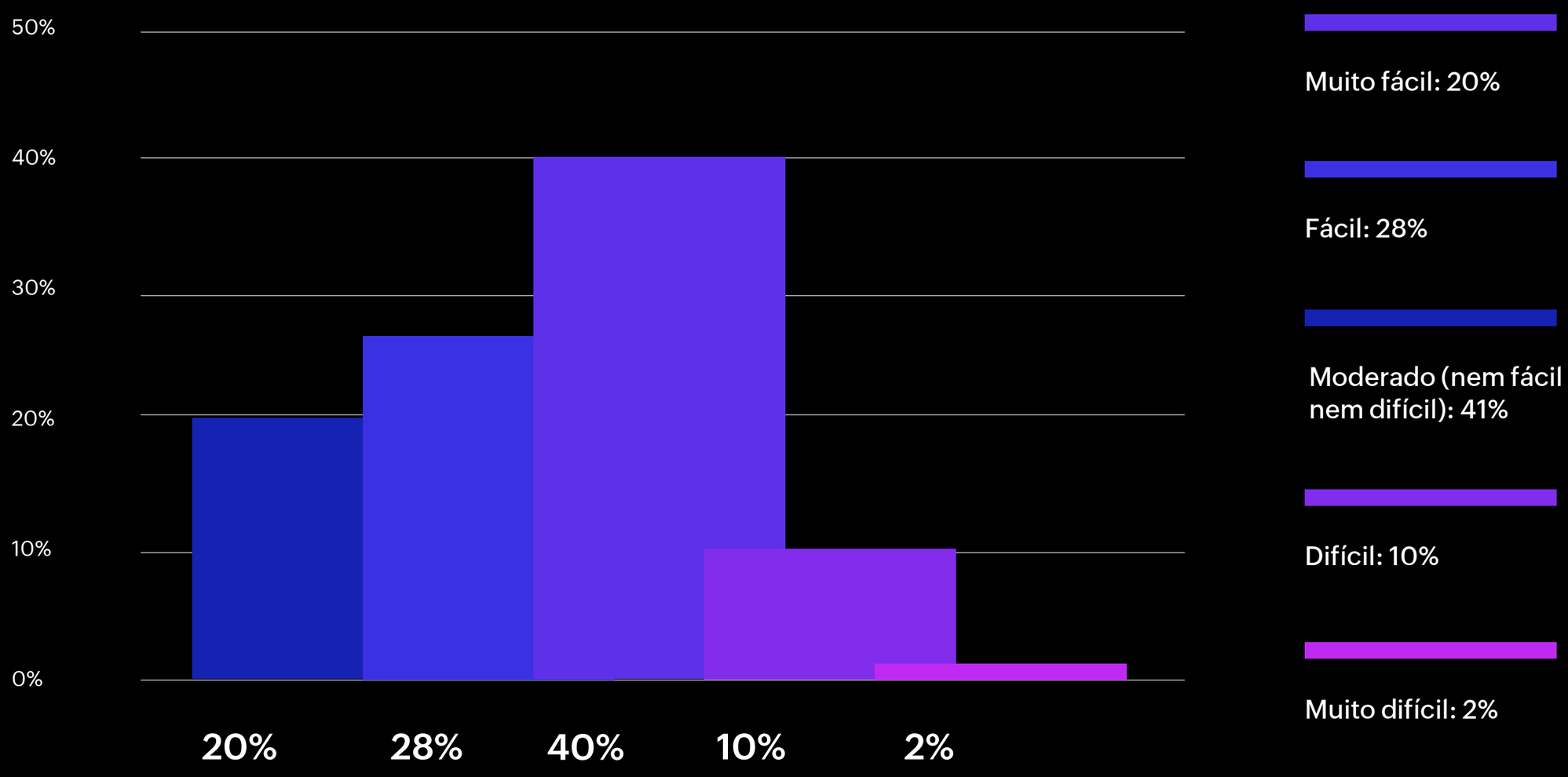
Maior conscientização sobre segurança entre os funcionários: 52%

ManageEngine

Seção 2: Seguro de segurança cibernética

No Brasil, 99% das empresas relataram ter seguro de segurança cibernética, mas apenas 48% acharam fácil ou muito fácil obter esse seguro.

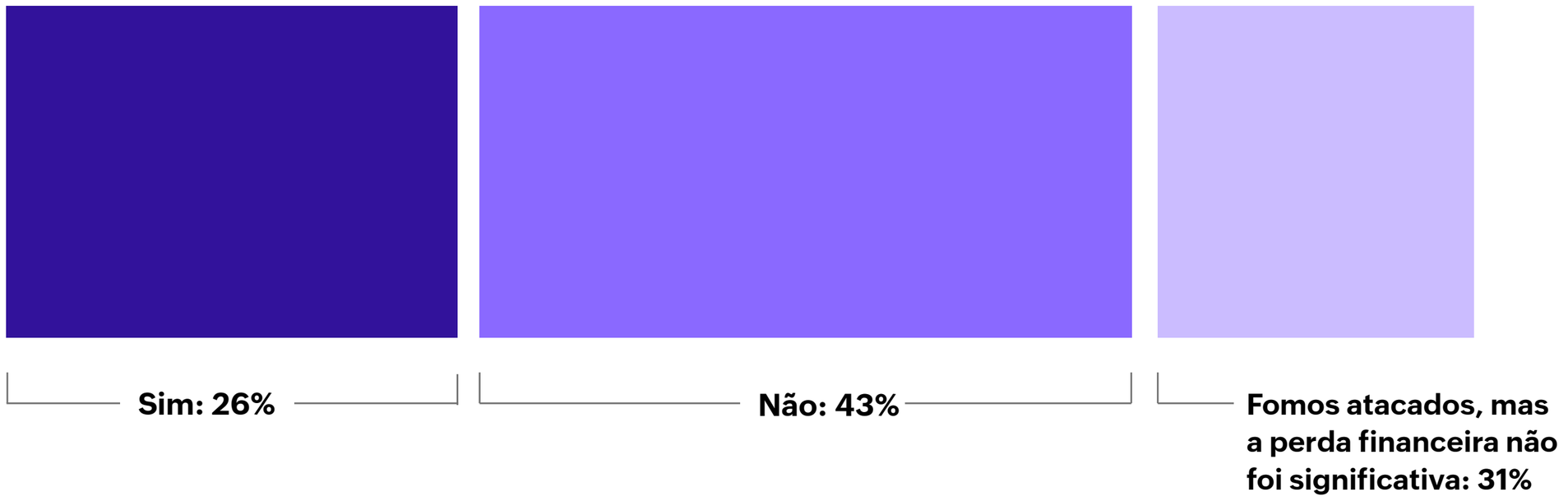
Q	Quão fácil você descreveria o processo de aquisição de seguro de segurança cibernética?



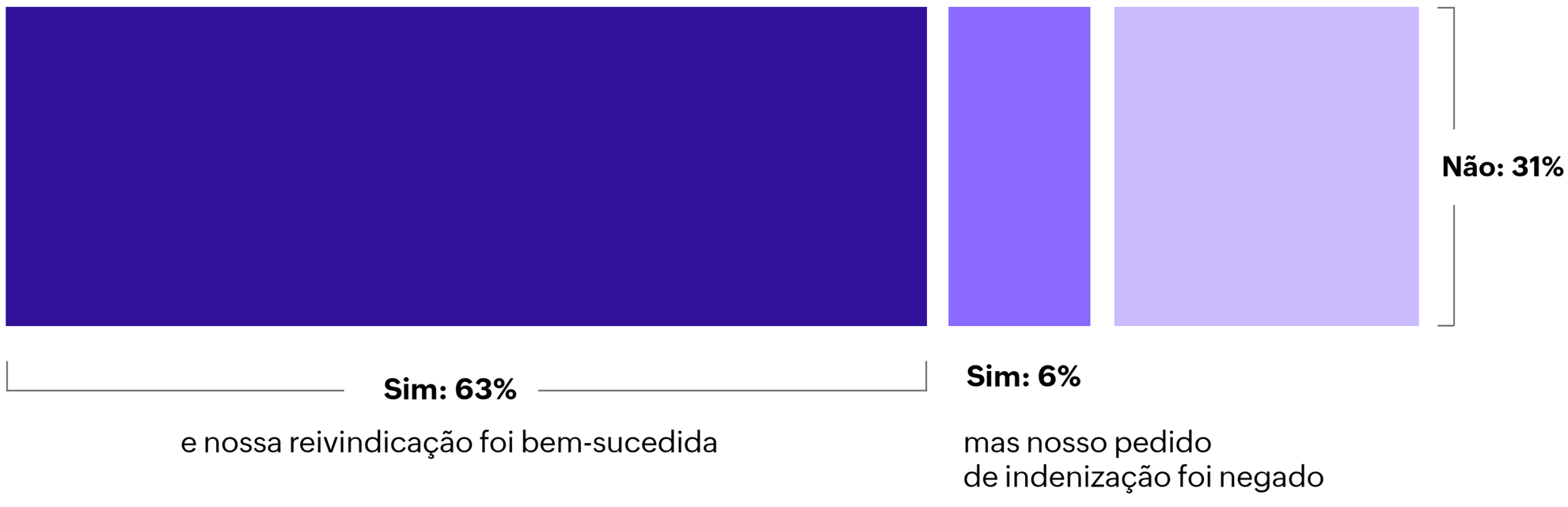
Apenas 26% dos entrevistados relataram que suas organizações sofreram ataques cibernéticos que levaram a uma perda financeira substancial, enquanto 32% reconheceram ter sido alvo de ataques cibernéticos sem sofrer danos financeiros significativos. Dito isso, mais de seis em cada dez entrevistados (63%) revelaram que suas empresas conseguiram obter com sucesso reivindicações de seguro para os ataques cibernéticos que enfrentaram em 2023.

Seção 2: Seguro de segurança cibernética

Q Em 2023, sua empresa sofreu um ataque de segurança cibernética que resultou em perdas financeiras significativas?



Q Sua empresa fez um pedido de indenização de seguro de segurança cibernética por algum dos ataques que sofreu em 2023?



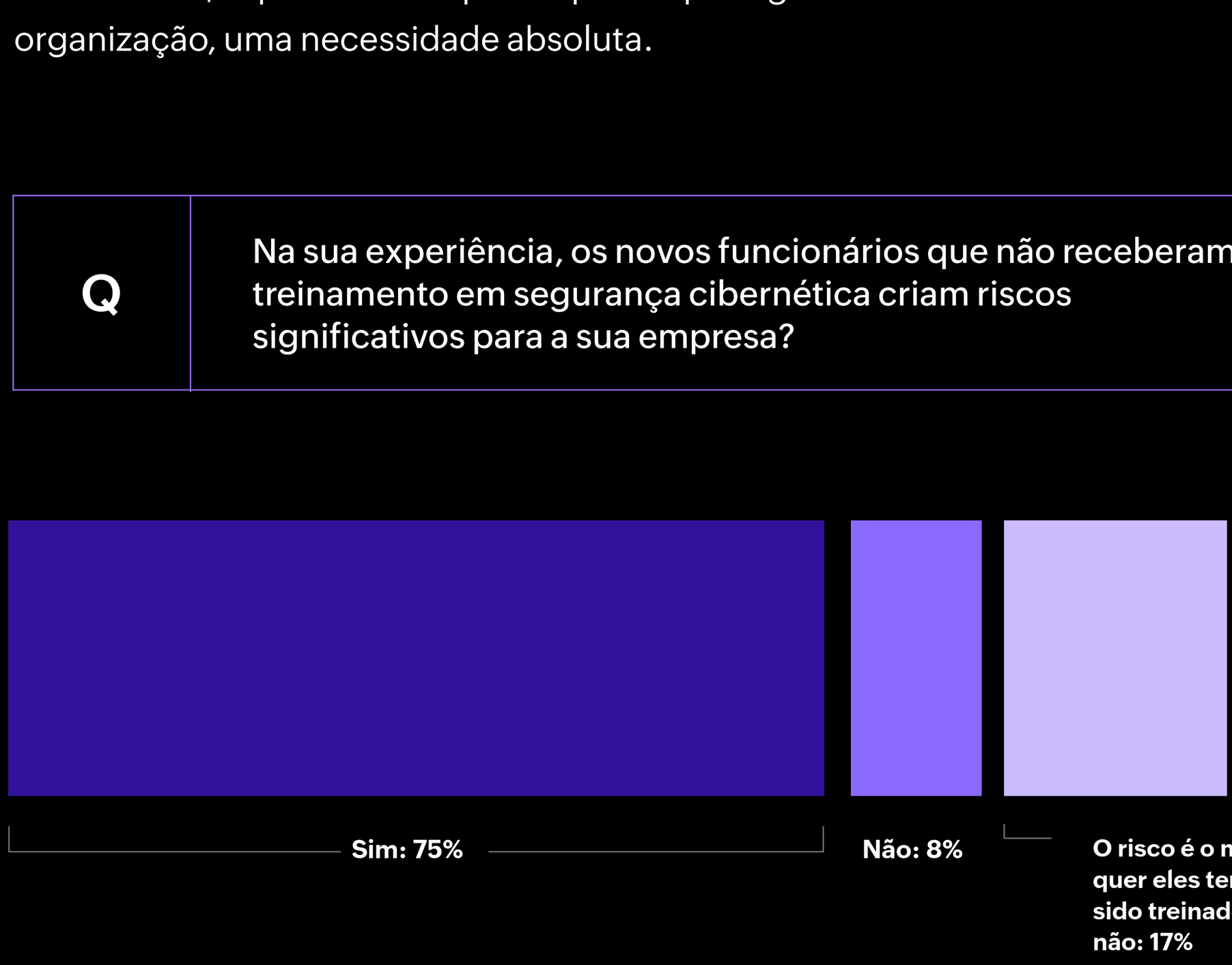
Seção 3: Papel dos funcionários

O forte foco dos seguros no treinamento de segurança dos funcionários é merecido, pois o segundo e o quarto principais vetores de ameaças à segurança em 2023 incluíam funcionários: ações acidentais de funcionários (54%) e ações intencionais de funcionários ou agentes internos mal-intencionados (36%). A análise dos dados revelou que o risco dos funcionários cresce à medida que aumenta o tamanho da empresa.

Além disso, 75% dos profissionais de segurança disseram que os novos funcionários que não recebem treinamento em segurança criam riscos significativos para a empresa. As organizações entendem a ameaça, pois 97% delas informam que os funcionários são treinados em segurança.

No entanto, devido às muitas violações sofridas pelas empresas, há uma preocupação com a qualidade do treinamento dos funcionários. Os dados mostraram novamente que os ataques cibernéticos com IA foram ainda mais eficazes contra os colaboradores, pois podem tornar o phishing, os deepfakes e outras ameaças voltadas para os eles ainda mais sofisticados e convincentes. Isso torna o treinamento, especialmente para aqueles que ingressaram recentemente na organização, uma necessidade absoluta.

Q	Na sua experiência, os novos funcionários que não receberam treinamento em segurança cibernética criam riscos significativos para a sua empresa?



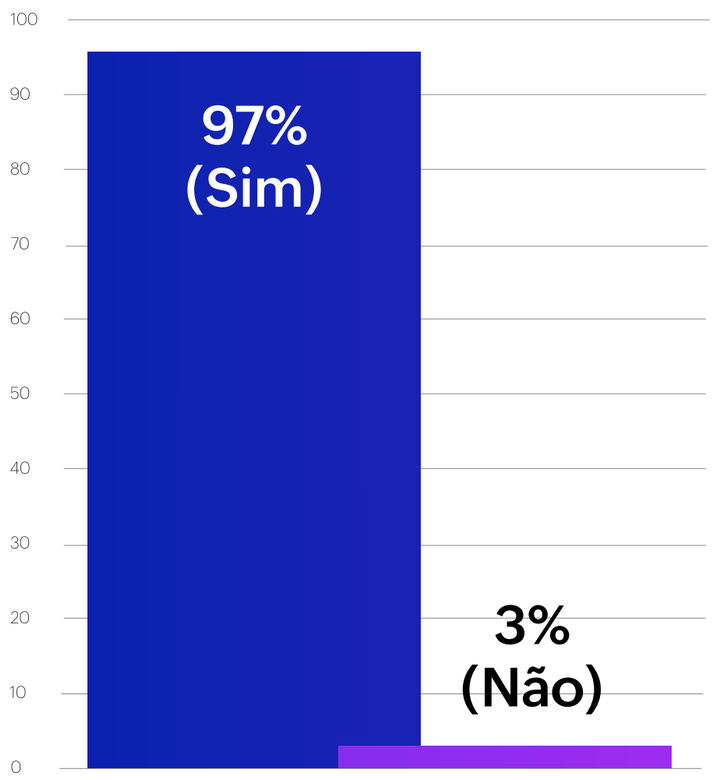
Seção 4: Papel da IA

Os profissionais de segurança afirmam que são necessárias soluções habilitadas para IA, com 97% afirmando que isso é fundamental para defender sua empresa contra ataques cibernéticos em 2024. Isso levou 96% a indicar que metade ou mais de todas as suas soluções de segurança serão habilitadas para IA até o final de 2024.

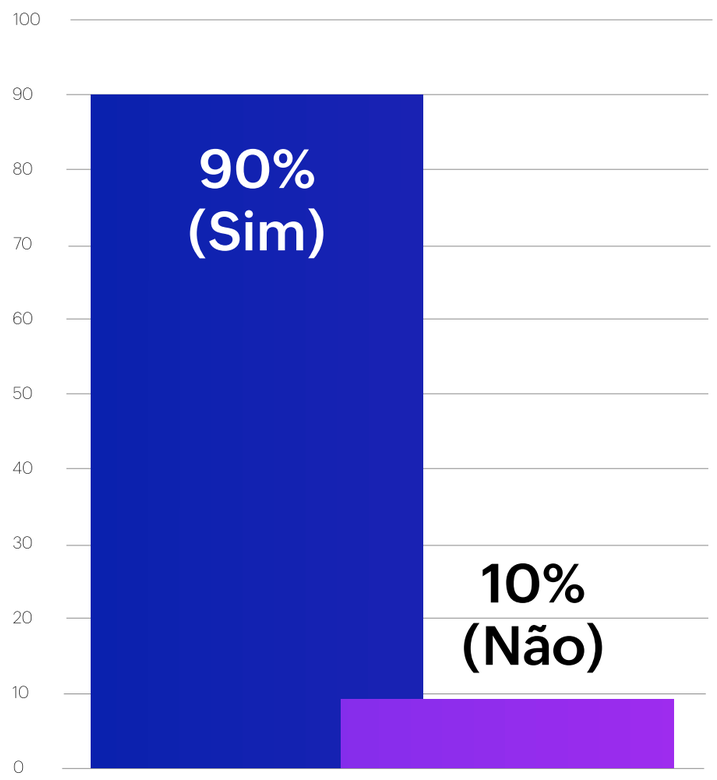
A pesquisa revelou algumas descobertas controversas, pois 90% confiam unilateralmente em ferramentas de segurança habilitadas para IA para fazer alterações e implementar ações sem a necessidade de um ser humano para revisar a ação proposta. No entanto, os profissionais de segurança estão cientes desse risco e 97% afirmaram que é necessária uma organização independente para garantir a confiabilidade das soluções de segurança habilitadas para IA.

As descobertas indicam que os ataques com tecnologia de inteligência artificial são mais eficazes, criam dificuldades financeiras e estressam as equipes de segurança. Em 2024, as empresas precisarão de ferramentas habilitadas para IA e de profissionais experientes para defender os negócios e proteger seus dados contra as crescentes ameaças de IA.

A IA será fundamental para a defesa contra ataques de cibersegurança em 2024?



Sua empresa confia nas soluções de cibersegurança habilitadas para IA para fazer as alterações apropriadas em suas defesas de segurança?



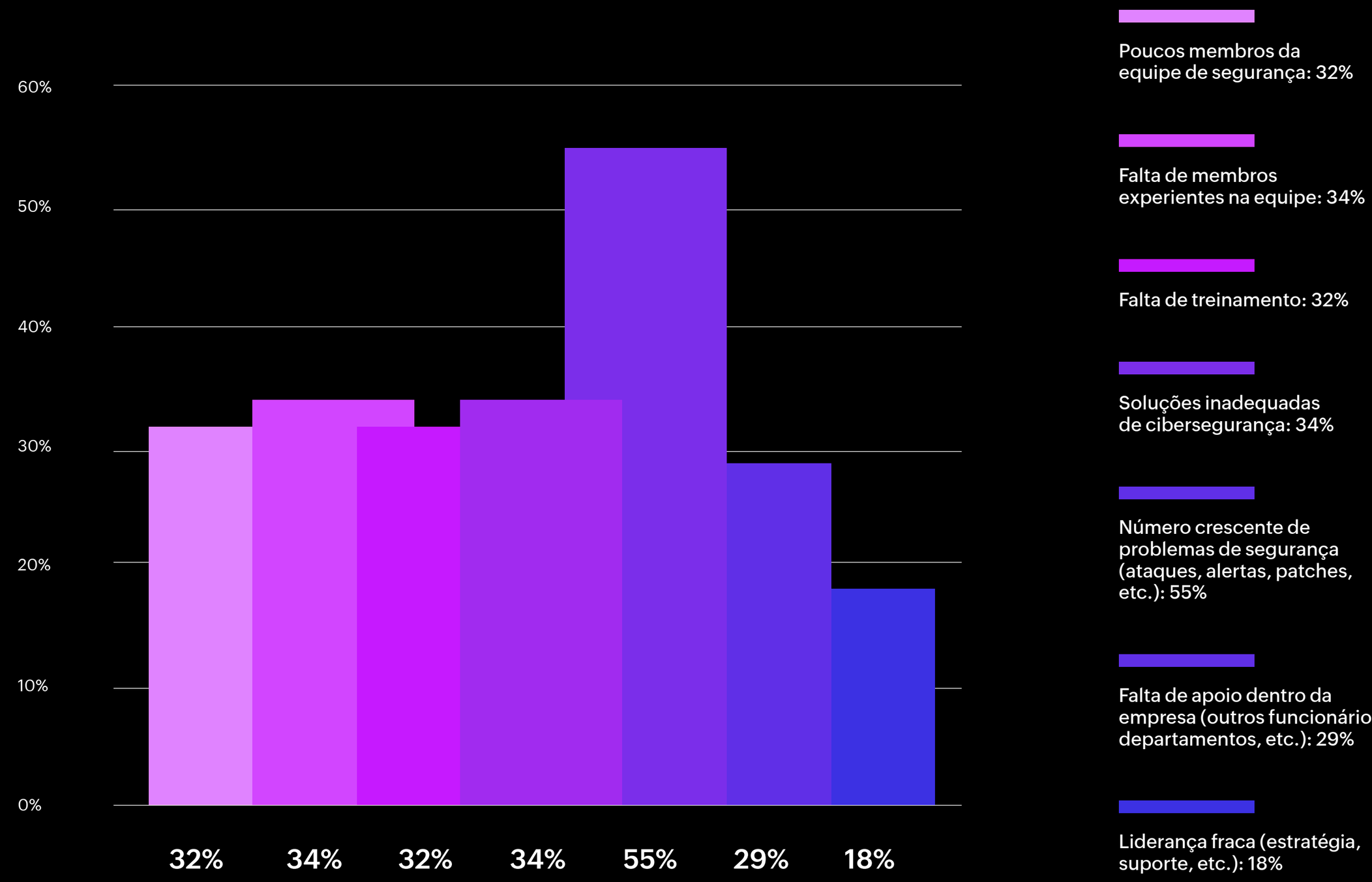
ManageEngine

Seção 5: Aumento de estresse nas equipes de cibersegurança

O desafio da segurança cresce, à medida que profissionais de segurança afirmam que até o final de 2024, 92% das empresas brasileiras teriam enfrentado ataques de segurança alimentados por GenAI. Isso está fazendo com que 66% dos membros da equipe de segurança admitam que seu nível de estresse está aumentando.

O principal item que causa estresse, com 55%, é o número crescente de problemas de segurança (ataques, violações, patches, atualizações, falsos positivos, etc.), seguido pela falta de membros experientes da equipe (34%) e soluções inadequadas de segurança cibernética (também 34%).

Q	O que está causando o aumento do seu nível de estresse? Selecione tudo que se aplica.



ManageEngine

Seção 6: Conformidade

A necessidade de seguro de cibersegurança e o cumprimento dos seus requisitos está gerando um efeito positivo nas empresas, com 81% afirmando que estão atualmente em conformidade com todos os regulamentos de proteção de dados. Outros 18% afirmam que estarão em conformidade até o final de 2024.

Q	Até onde você sabe, sua empresa está em total conformidade com as regulamentações locais e internacionais de proteção de dados?

Sim: 81%

Não, mas estaremos totalmente em conformidade até o final de junho de 2024: 14%

Não, mas estaremos totalmente em conformidade até o final de 2024: 4%

Não, mas estaremos em conformidade após 2024: 1%

Conclusão

As empresas brasileiras enfrentam uma corrente de ataques contínua à segurança que são suficientemente eficazes para que a maioria registre reclamações de seguros. Embora o treinamento tenha aumentado para funcionários e profissionais das equipes de segurança, o fato preocupante é que os ataques potencializados pela IA são ainda mais efetivos, criando mais dificuldades financeiras e aumentando o estresse nas equipes de segurança. Infelizmente, em 2024, as empresas enfrentarão um aumento significativo nos ataques de IA e precisarão de ferramentas e profissionais experientes habilitados para IA para defender o negócio e proteger os seus dados contra essa ameaça crescente. As empresas que desejam aumentar os lucros e os negócios internacionais terão de se antecipar à ameaça da IA, pois ninguém quer fazer negócios com uma empresa que não consegue proteger os seus próprios dados.

manageengine.com/br/

Sobre a ManageEngine

A ManageEngine é uma divisão da Zoho Corporation que oferece soluções abrangentes de gerenciamento de operações de segurança e TI locais e nativas da nuvem para organizações globais e provedores de serviços gerenciados. Empresas estabelecidas e emergentes – incluindo nove em cada 10 organizações da Fortune 100 – contam com as ferramentas de gerenciamento de TI em tempo real da ManageEngine para garantir o desempenho ideal de sua infraestrutura de TI, incluindo redes, servidores, aplicações, endpoints e muito mais. A ManageEngine possui 18 data centers, 20 escritórios e mais de 200 parceiros de canal em todo o mundo para ajudar as organizações a alinharem seus negócios com a TI.

ManageEngine

Para mais informações, visite o site da empresa, siga o blog da empresa e conecte-se no