

Cybersecurity

INSIDERS

2023

Relatório de Segurança na Nuvem



FORTINET®

INTRODUÇÃO

Em 2023, a nuvem está produzindo, acima de tudo, os resultados comerciais prometidos, incluindo capacidade e escalabilidade flexíveis, maior agilidade, melhor disponibilidade, e implantação e provisionamento acelerados.

No entanto, as preocupações de segurança continuam a ser uma importante barreira à adoção da nuvem, mostrando poucos sinais de melhoria na percepção dos profissionais de segurança na nuvem. A adoção da nuvem é ainda inibida por uma série de problemas relacionados que impedem a adoção mais rápida e estendida dos serviços na nuvem, incluindo a contínua falta de talento na área de segurança na nuvem, a proliferação de requisitos de conformidade e a significativa falta de visibilidade e controle, especialmente em ambientes híbridos e multinuvem.

O Relatório de Segurança na Nuvem de 2023 entrevistou 752 profissionais de cibersegurança a fim de identificar os principais desafios e prioridades, incluindo:

- A segurança na nuvem continua a ser um importante problema, sendo que 95% das organizações entrevistadas estão preocupadas com a sua postura de segurança em ambientes públicos de nuvem. A má configuração continua a oferecer o maior risco à segurança na nuvem, de acordo com 59% dos profissionais de cibersegurança. Logo em seguida vem a exfiltração de dados confidenciais e interfaces/APIs inseguras (empatados em 51%), e acesso não autorizado (49%).
- Apesar das turbulências econômicas, a maioria das organizações (60%) estão aumentando seus orçamentos de segurança na nuvem em uma média de 33%.
- 44% das organizações estão à procura de formas para obter melhor visibilidade e controle da segurança em redes híbridas e multinuvem, das quais 90% estão à procura de uma única plataforma de segurança na nuvem para proteger os dados de forma consistente e abrangente em toda a sua presença na nuvem.

Gostaríamos de agradecer à [Fortinet](#) por apoiar este importante projeto de pesquisa do setor. Esperamos que o relatório seja informativo e útil à medida que você continua seus esforços para garantir sua jornada rumo à nuvem contra ameaças em rápida evolução.

Obrigado,

Holger Schulze



Holger Schulze

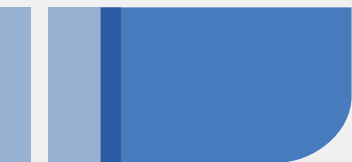
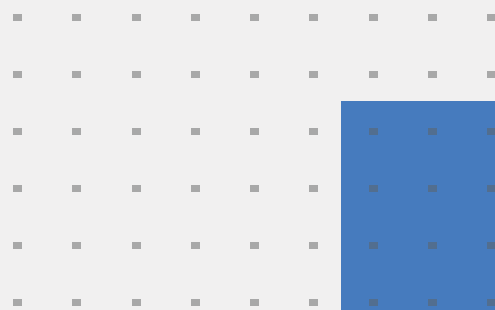
CEO e fundador
Cybersecurity Insiders

Cybersecurity
INSIDERS

ÍNDICE

| | |
|--|----|
| ▶ Estado atual da adoção da nuvem | 4 |
| ▶ Benefícios da nuvem | 10 |
| ▶ Problemas de segurança na nuvem | 13 |
| ▶ Principais prioridades para a segurança na nuvem | 19 |
| ▶ Metodologia e dados demográficos | 24 |

Estado atual da adoção da nuvem

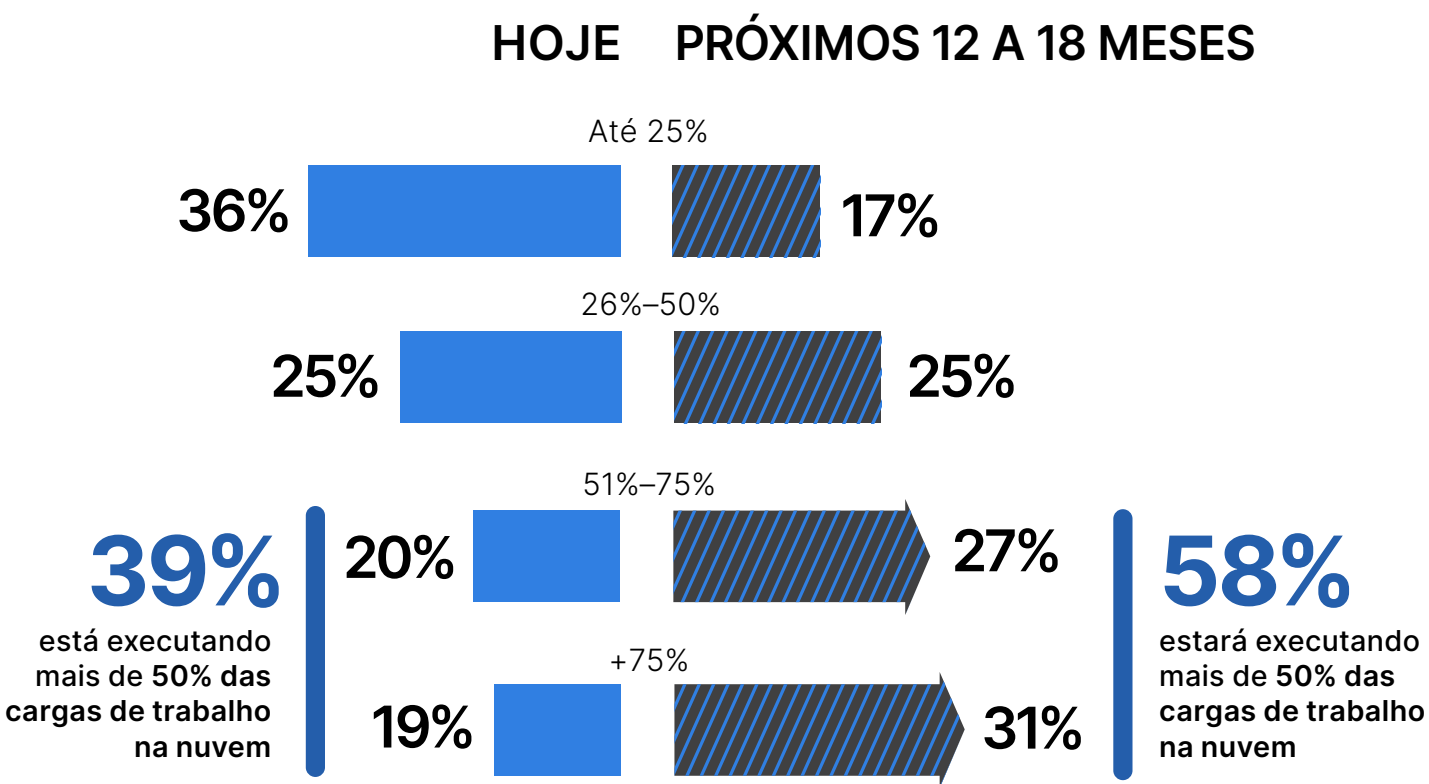


CARGAS DE TRABALHO NA NUVEM

Apesar de haver uma estabilidade na adoção da nuvem ano após ano, o ritmo de transição das cargas de trabalho para a nuvem continua intenso. Atualmente, 39% dos entrevistados têm mais de metade das suas cargas de trabalho na nuvem, enquanto que 58% planejam atingir este nível nos próximos 12 a 18 meses.

▶ Que porcentagem de sua carga de trabalho está hoje na nuvem?

▶ Que porcentagem de sua carga de trabalho estará na nuvem nos próximos 12 a 18 meses?

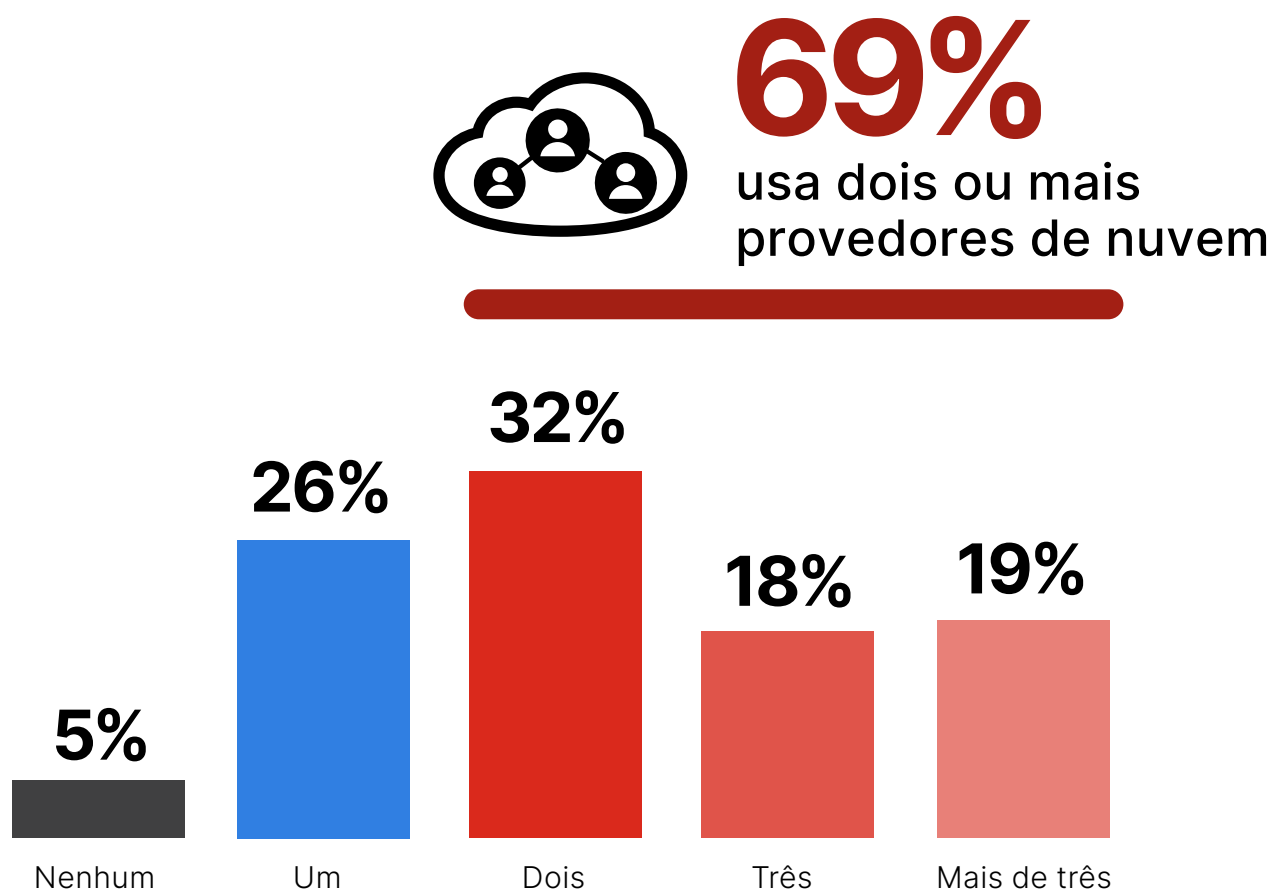


Compartilhamento de cargas de trabalho na nuvem

ADOÇÃO MULTINUVEM

Conforme é feita a transição das cargas de trabalho para a nuvem, as organizações passam a selecionar a plataforma de nuvem que melhor se adapta a cada projeto, o que impulsiona a proliferação multinuvel em quase 7 em cada 10 empresas entrevistadas, as quais usam dois ou mais fornecedores de nuvem (69%).

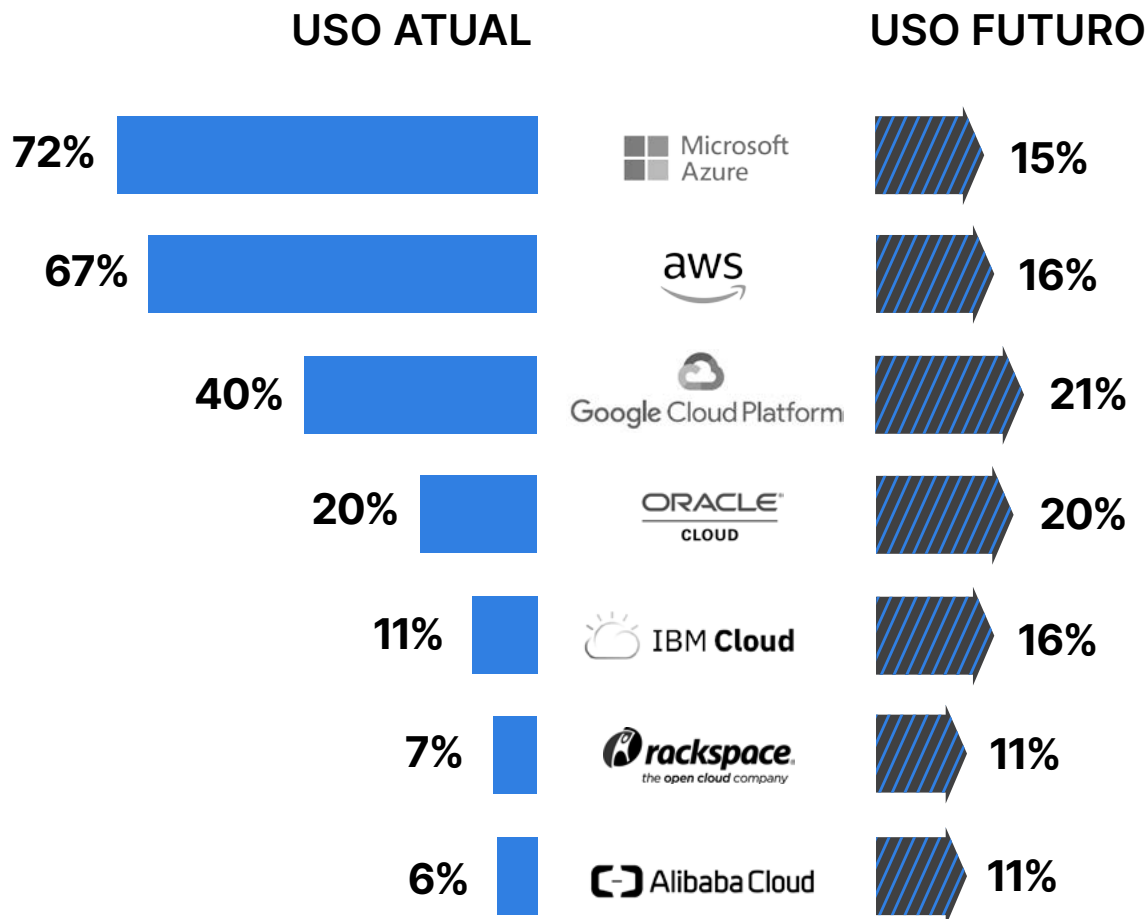
▶ Quantos provedores de nuvem sua organização usa atualmente?



PROVEDORES DE NUVEM PREFERIDOS

A quais provedores de nuvem as organizações dão prioridade? Os grandes provedores, como Microsoft Azure (72%) e Amazon Web Services (67%), continuam a dominar o mercado. Contudo, a futura adoção da nuvem será maior para Google Cloud Platform (+21%) e Oracle Cloud (+20%).

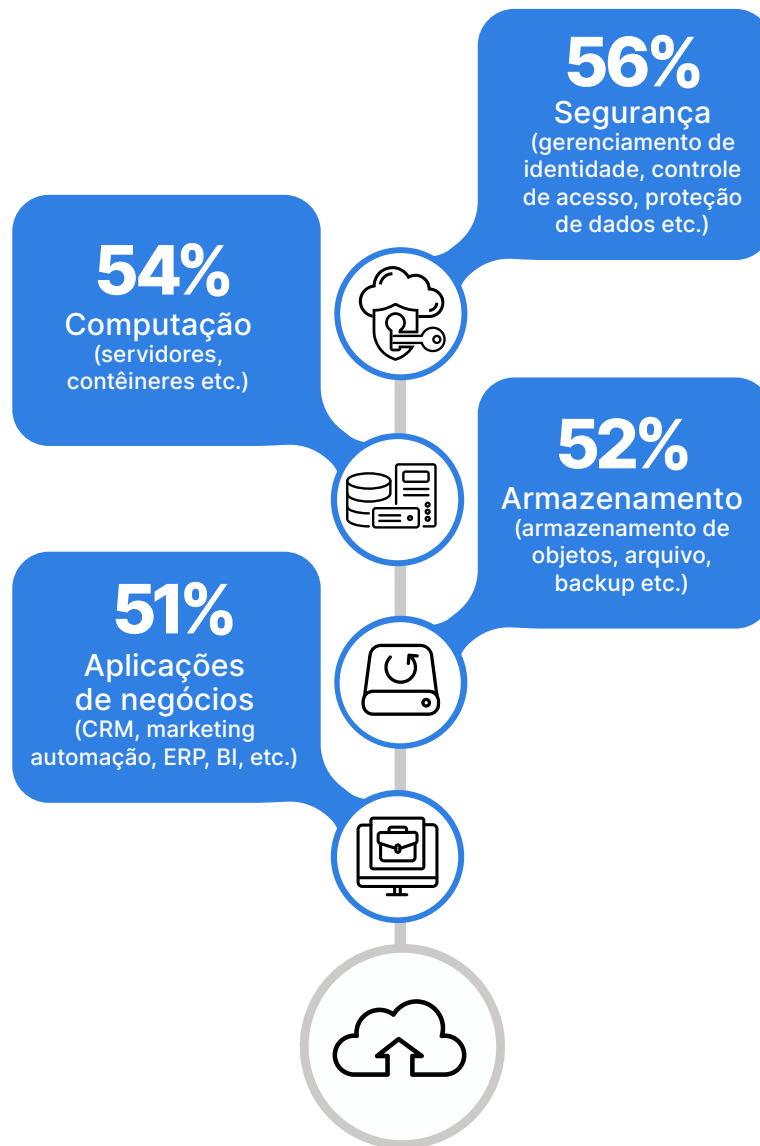
▶ **Quais provedores de IaaS da nuvem você usa atualmente ou planeja usar no futuro?**



PRIORIDADES DE SERVIÇOS NA NUVEM

Aparentemente, a nuvem não se trata apenas de computação e armazenamento. Um fato interessante é que os serviços de segurança representam a principal carga de trabalho implantada na nuvem (56%), ficando à frente da computação (54%), armazenamento (52%) e aplicações (51%).

► Que serviços e cargas de trabalho sua empresa está implantando na nuvem?

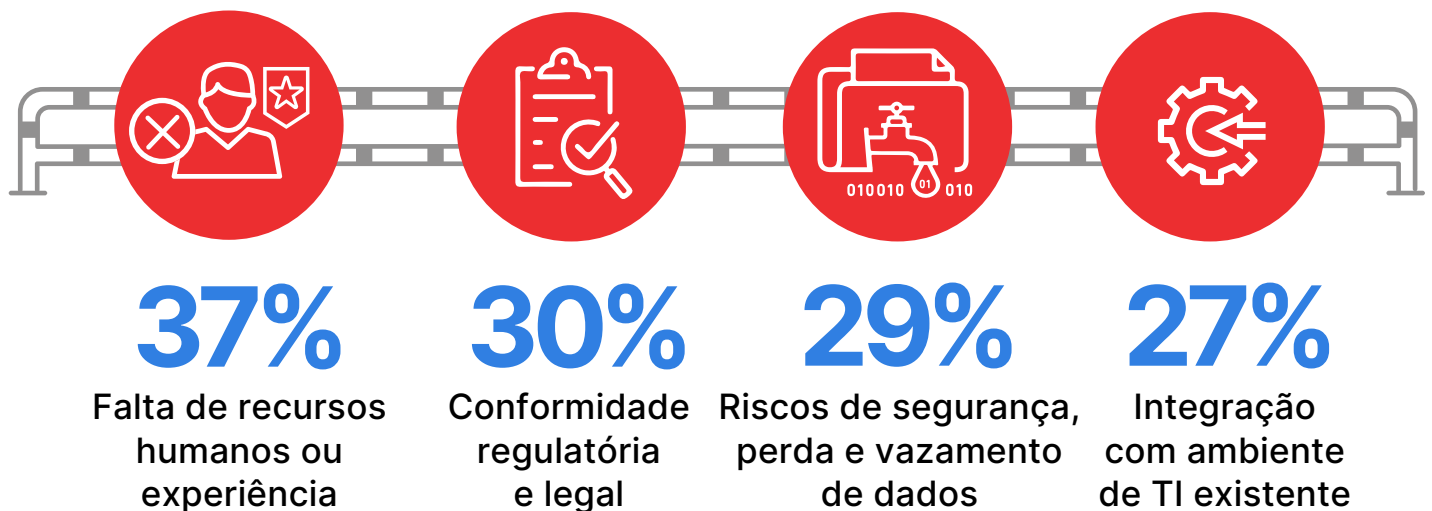


Aplicações de produtividade (e-mail, colaboração, mensagens instantâneas, etc.) 50% | Virtualização 49% | Banco de dados (relacional, NoSQL, caching, etc.) 46% | Aplicações operacionais de TI (administração, back-up, aprovisionamento, monitoramento, etc.) 45% | Aplicações de teste/desenvolvedor 40% | Networking e entrega de conteúdos (nuvem privada virtual, DNS, etc.) 38% | Sistema operacional 34% | Streaming de aplicações e desktop 22% | Middleware 22% | Tempo de execução 14% | Não sei/outro 6%

BARREIRAS À ADOÇÃO DA NUVEM

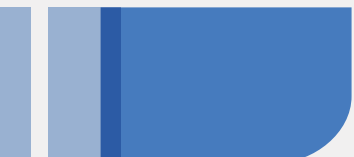
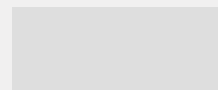
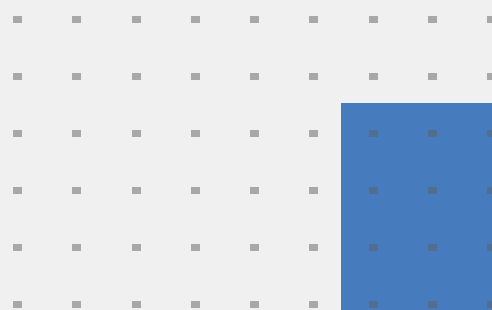
Embora a nuvem ofereça vantagens importantes, ainda existem barreiras significativas à adoção da nuvem. Os maiores desafios que as organizações enfrentam não se tratam, essencialmente, de tecnologia, mas também de pessoas e processos. O mais crucial é a perene falta de pessoal qualificado (37%), que continua a ser o maior impedimento à adoção mais rápida, apesar da pequena queda em relação ao ano passado. Logo em seguida vem a conformidade legal e regulatória (30%), questões de segurança de dados (29%) e integração com os atuais ambientes de TI (27%).

► Quais são as maiores barreiras à adoção da nuvem em sua empresa?



Medo de "lock-in" de distribuidor 24% | Riscos gerais de segurança 23% | Falta de orçamento 22% | Custo/falta de ROI 21% | Estagnação e resistência interna 20% | Perda de controle 19% | Complexidade no gerenciamento da implantação na nuvem 18% | Falta de transparência e visibilidade 15% | Problemas de cobrança e monitoramento 14% | Falta de maturidade dos modelos de serviço na nuvem 13% | Falta de adesão da gerência 13% | Insatisfação com as ofertas de serviços/desempenho/preços da nuvem 12% | Falta de personalização 10% | Falta de apoio por parte do fornecedor da nuvem 8% | Desempenho das aplicações na nuvem 8% | Disponibilidade 8% | Outros 5%

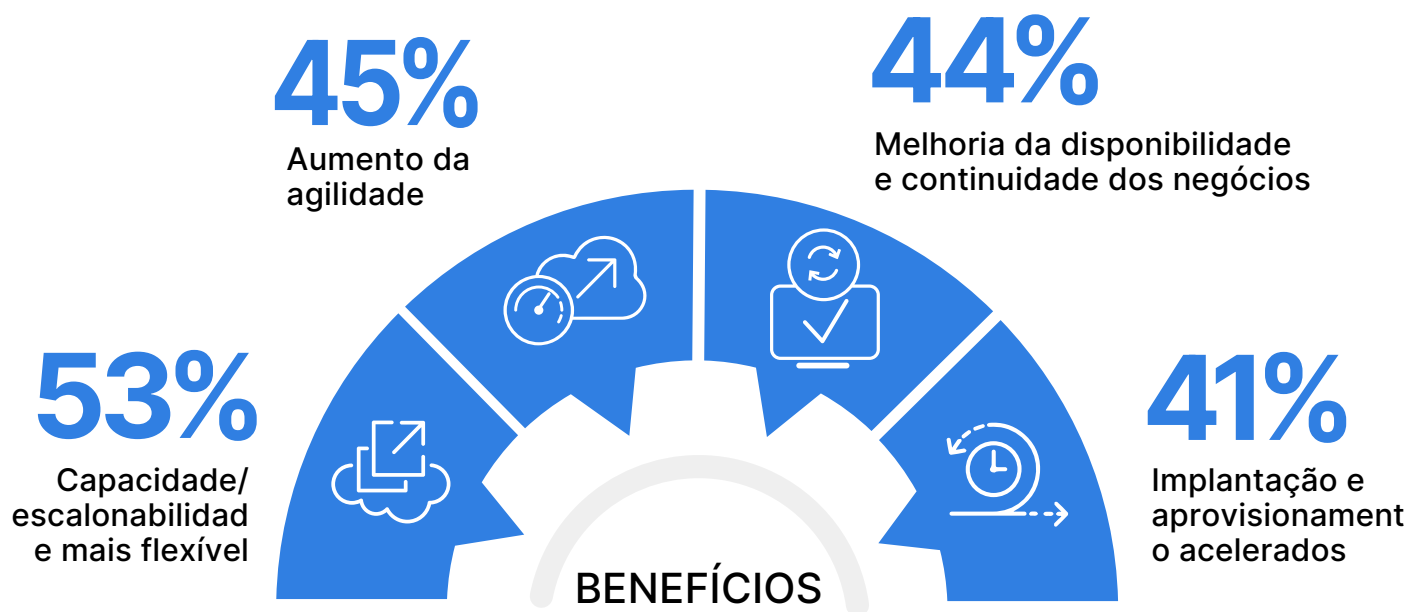
Benefícios da nuvem



PRINCIPAIS BENEFÍCIOS DA NUVEM

Após anos de adoção da nuvem, as organizações acreditam que a computação em nuvem cumpre o prometido? A resposta é sim. Os usuários da nuvem afirmam que ela oferece benefícios comerciais essenciais, como flexibilidade e escalonabilidade (53%), agilidade (45%), continuidade dos negócios (44%) e implantação e provisionamento acelerados (41%). Este é o primeiro ano em que a implantação acelerada está entre os quatro principais benefícios, ultrapassando tanto o desempenho como a transição para a variável OPEX.

► Que benefícios globais você já obteve com sua implantação de nuvem?

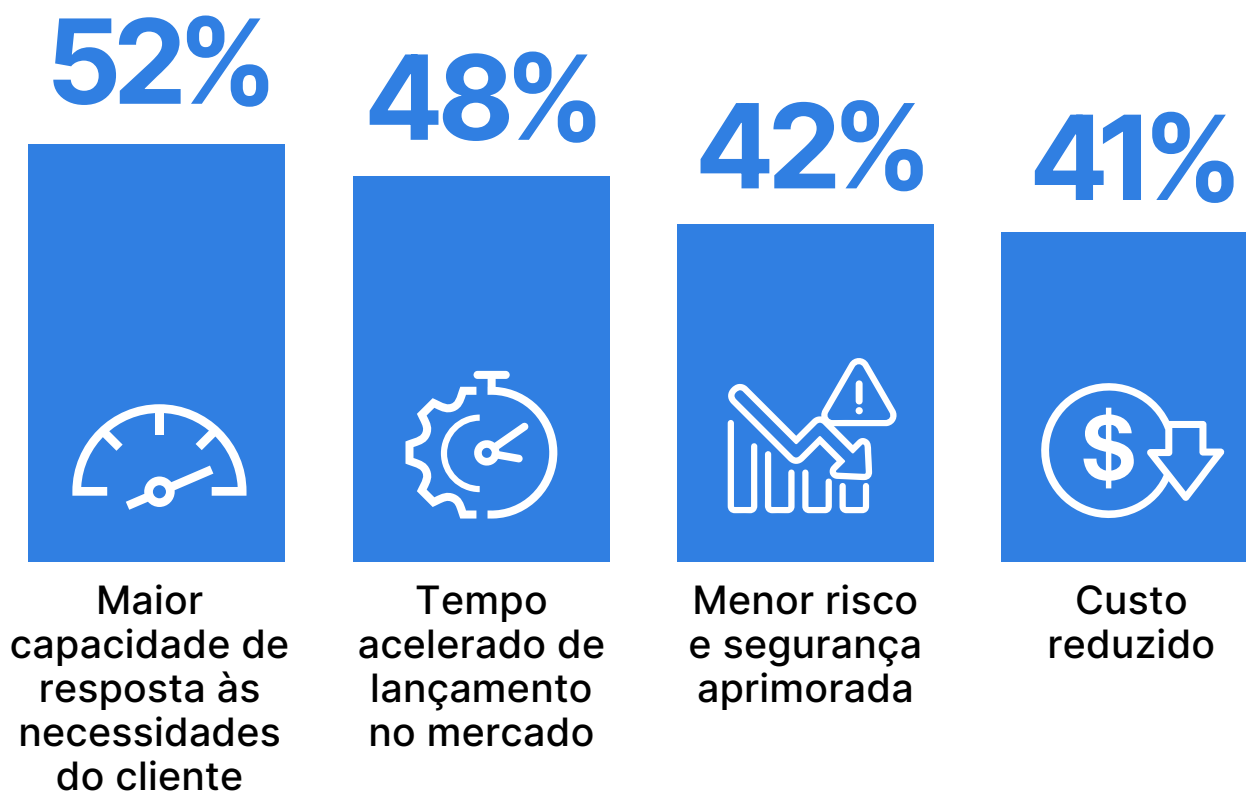


Melhor desempenho 36% | Tempo acelerado de lançamento no mercado 34% | Despesas movimentadas de CAPEX fixo (compra) para OPEX variável (aluguel/assinatura) 34% | Custo reduzido 32% | Maior segurança 32% | Maior alcance geográfico 27% | Maior produtividade dos funcionários 25% | Menor complexidade 23% | Maior conformidade regulatória 22% | Não tenho certeza/outros 12%

RESULTADOS COMERCIAIS DA NUVEM

Os benefícios da nuvem estão impulsionando os principais resultados comerciais, e este ano a capacidade de resposta às necessidades dos clientes (52%) torna-se o principal resultado ao invés do tempo acelerado de lançamento no mercado (48%). Organizações criteriosas quanto à integração da cibersegurança em sua transição para a nuvem também estão percebendo o valor disso para os negócios com menos risco e mais segurança (42%) e custos reduzidos (41%).

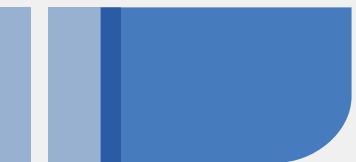
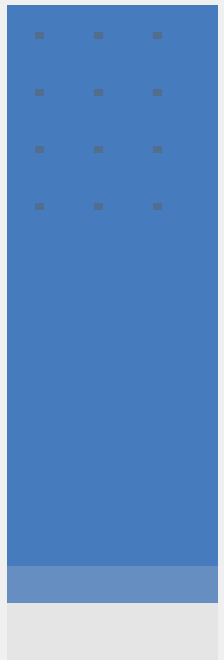
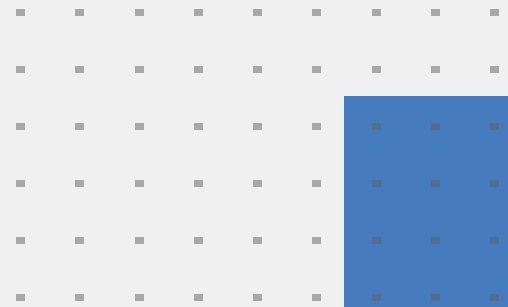
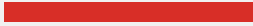
► Quais resultados de negócios você percebeu ao migrar para a nuvem?



Alcance de mercado expandido para novos mercados 23% | Crescimento acelerado da receita nos atuais mercados 22% | Ganho de paridade com os concorrentes 22% | Outros 7%



Problemas de segurança na nuvem



PREOCUPAÇÕES DE SEGURANÇA EM NUVEM PÚBLICA

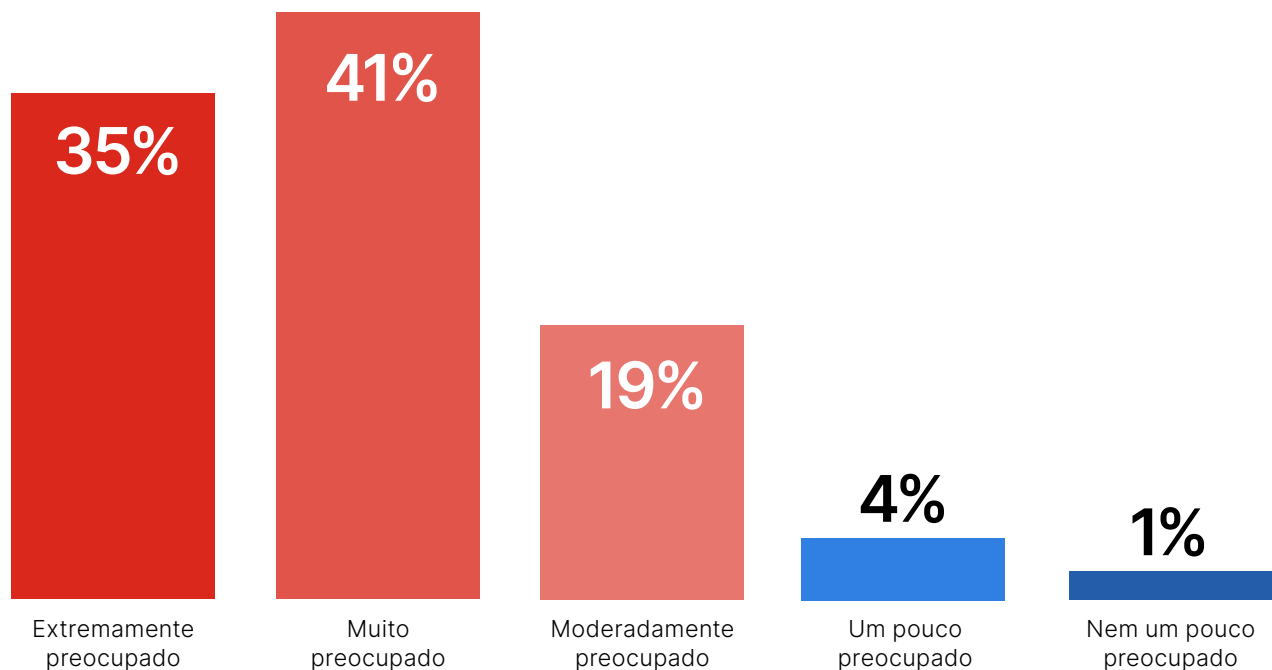
Apesar da crescente adoção da nuvem, as preocupações com a segurança na nuvem não mostram sinais de melhoria. Praticamente todas as organizações entrevistadas estão moderada a extremamente preocupadas com a sua postura de segurança em ambientes de nuvem pública (95%). O número de organizações que estão extremamente preocupadas com a segurança na nuvem pública aumentou este ano, passando de 32% para 35%.

► O quanto você está preocupado com a segurança nas nuvens públicas?



95%

das organizações estão moderada a extremamente preocupadas com a segurança na nuvem



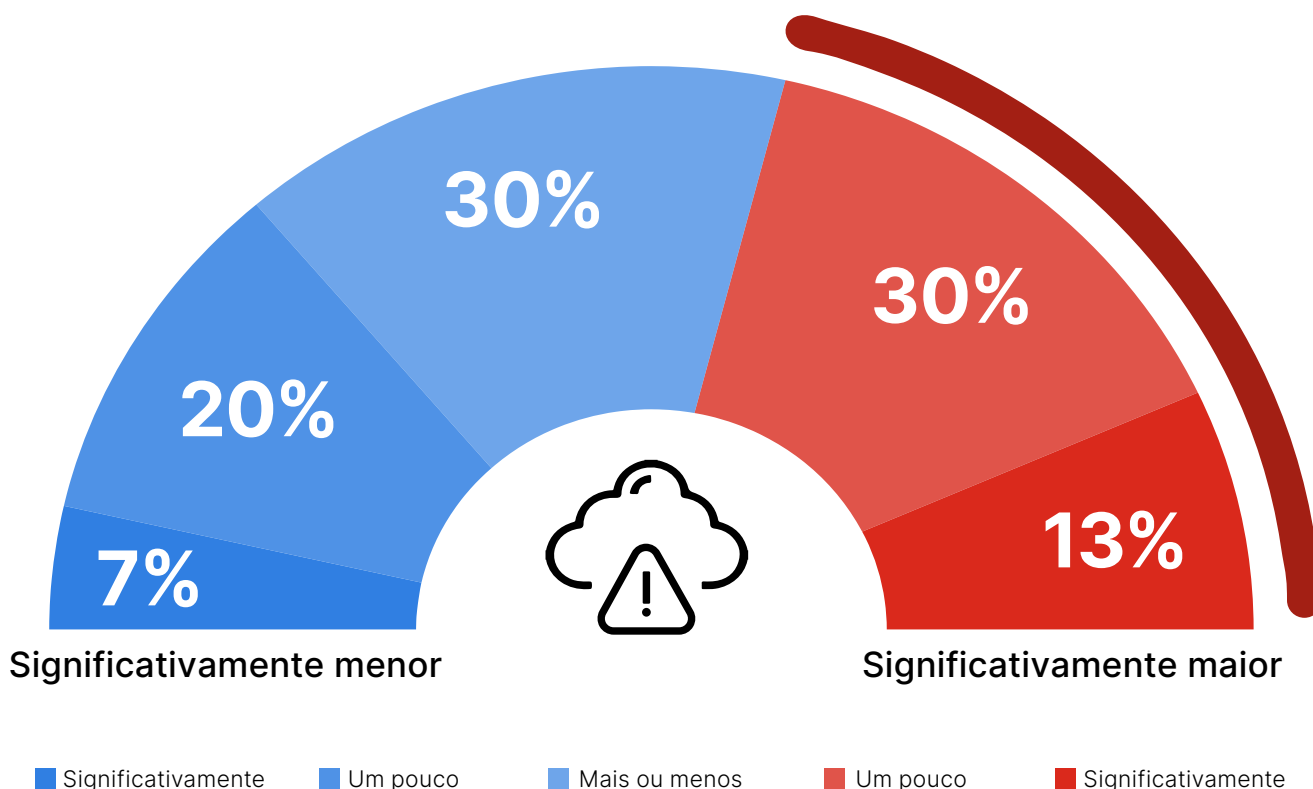
RISCO DE VIOLAÇÃO

As preocupações com a segurança na nuvem pública, combinadas com a falta de recursos e conhecimentos especializados, estão levando à percepção de que o risco de uma falha de segurança na nuvem pública é maior do que nos ambientes locais tradicionais (43%). Apenas 27% dos profissionais de segurança observam que o risco é menor em um ambiente de nuvem pública.

- ▶ **Em comparação com os ambientes de TI locais tradicionais, você afirmaria que o risco de violações de segurança em um ambiente de nuvem pública é maior ou menor?**

43%

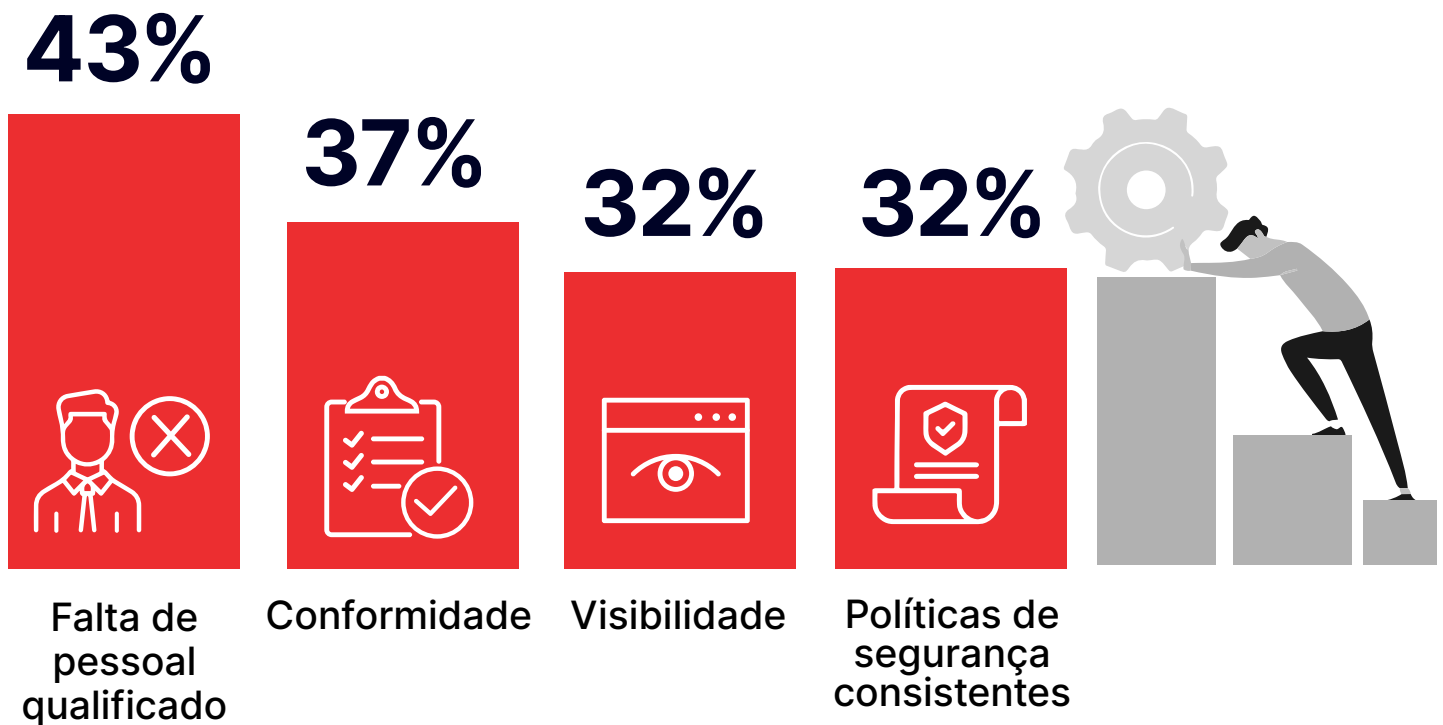
afirmam que o risco de nuvens públicas é de certa forma significativamente mais elevado do que o local



PROBLEMAS NA SEGURANÇA OPERACIONAL

Os profissionais de cibersegurança enfrentam diversos desafios quando se trata de proteger as cargas de trabalho nas nuvens. O fator “pessoas” volta a ocupar o topo da lista, seguido pela falta de pessoal de segurança qualificado (43%) e conformidade (37%). É quase possível afirmar que a proliferação multinuvem é a razão por trás do problema de implementar políticas de segurança consistentes (32%).

► **Quais são os maiores problemas operacionais que você enfrenta no dia a dia ao proteger as cargas de trabalho na nuvem?**

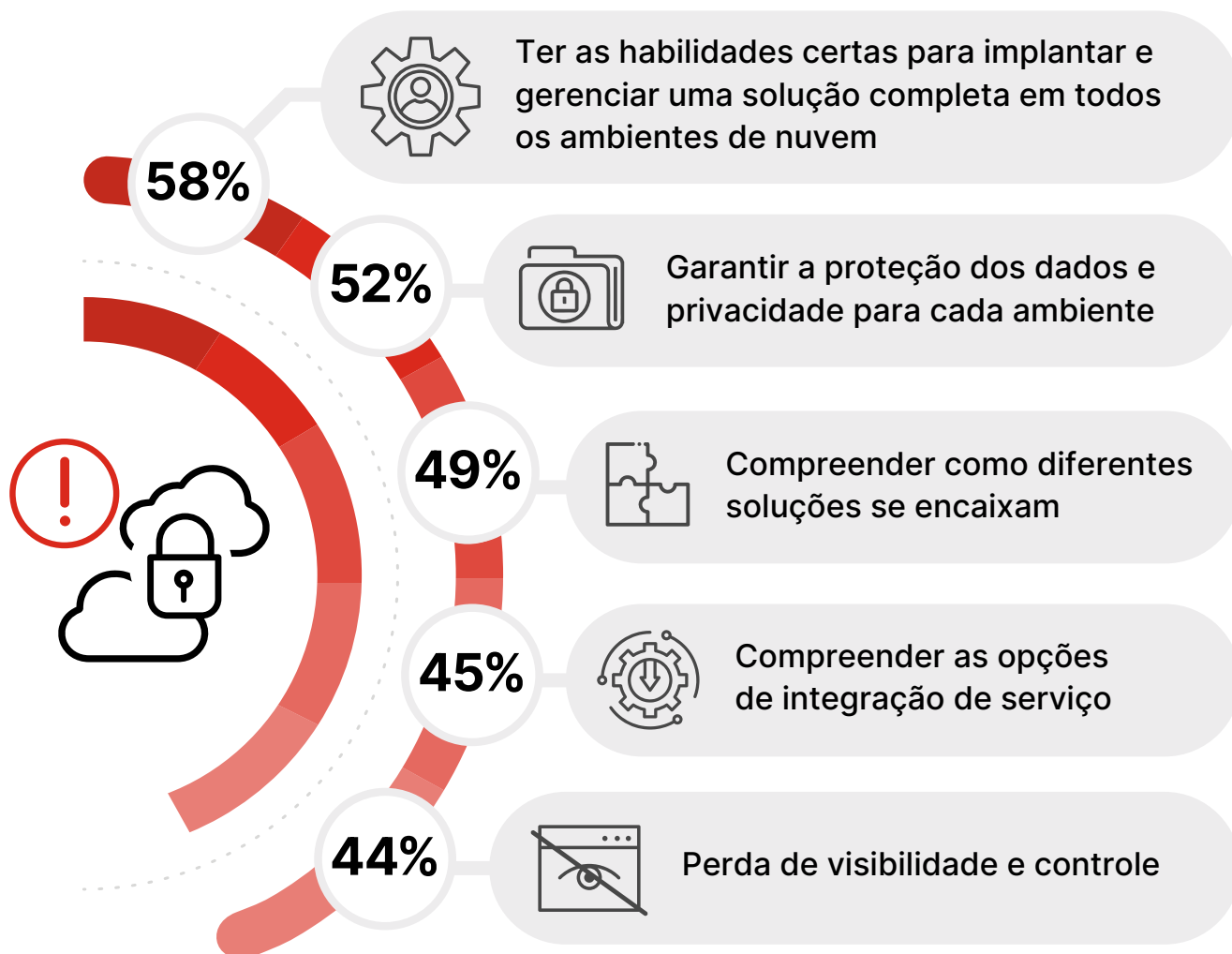


Controles e automação 30% | Não é possível identificar os problemas de configuração com agilidade 29% | Imposição automática de segurança em várias nuvens 29% | Complexidade ao associar normas de nuvem para nuvem/nuvem para local 25% | Proteção dos fluxos de tráfego 25% | Proteção do acesso de dispositivos móveis e pessoais 25% | A segurança não consegue acompanhar o ritmo das mudanças em novas/atuais aplicações 25% | Falta de integração com tecnologias de segurança local 25% | Definir os privilégios de acesso do usuário adequados 24% | Remediar as ameaças 24% | Justificar o aumento nos gastos em segurança 24% | Entender os padrões do tráfego de rede 23% | A identificação/visibilidade/controle da segurança da infraestrutura não é automático 22% | Divulgação de ameaças à segurança 21% | Falta de paridade de recursos com a solução de segurança local 21% | Sem flexibilidade 6% | Não tenho certeza/outros 10%

DESAFIOS DA SEGURANÇA MULTINUVEM

Os ambientes multinuvem aumentam a complexidade e os desafios de proteger cargas de trabalho na nuvem. O fator “pessoas” e o domínio que os ambientes multinuvem exigem é claramente realçado no fato de que três dos quatro principais problemas estarem relacionados com a retenção das competências certas, juntamente com uma compreensão aprofundada de cada plataforma da nuvem.

► Quais são os seus maiores desafios para proteger ambientes multinuvem?



Acompanhar o ritmo da mudança 38% | Gerenciar os custos de diferentes soluções 37% | Fornecer acesso intuitivo aos usuários com base nas suas credenciais 37% | Selecionar o conjunto de serviços ideal 36% | Outros 3%

AMEAÇAS À SEGURANÇA NA NUVEM

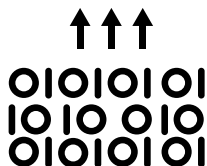
Quais ameaças à segurança na nuvem fazem os profissionais de cibersegurança perderem o sono? As mesmas quatro principais ameaças do ano passado, com a configuração errada ainda ocupando a primeira posição da lista, de acordo com 59% dos profissionais de cibersegurança. Logo em seguida, vem a exfiltração de dados confidenciais e interfaces/APIs inseguras (empatados em 51%) e acesso não autorizado (49%).

► O que você vê como as maiores ameaças à segurança nas nuvens públicas?



59%

Configuração incorreta da plataforma de nuvem/ instalação incorreta



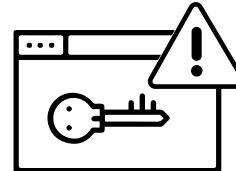
51%

Exfiltração de dados confidenciais



51%

Interfaces/APIs inseguras

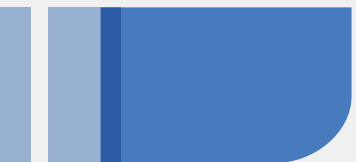
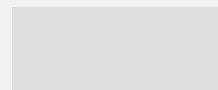
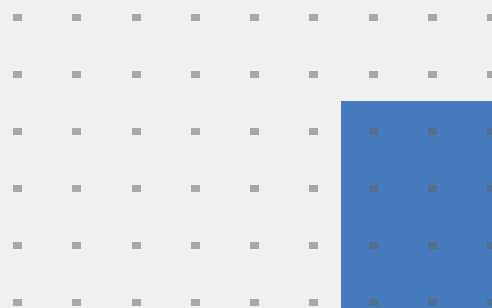


49%

Acesso não autorizado

Sequestro de contas, serviços ou tráfego 45% | Compartilhamento externo de dados 39% | Criminosos cibernéticos externos 38% | Malware/ ransomware 37% | Ataques cibernéticos patrocinados por outros estados 37% | Ataques de negação de serviço 31% | Cryptojacking da nuvem 21% | Roubo de serviço 20% | Dispositivos móveis perdidos 13% | Não sei/outros 7%

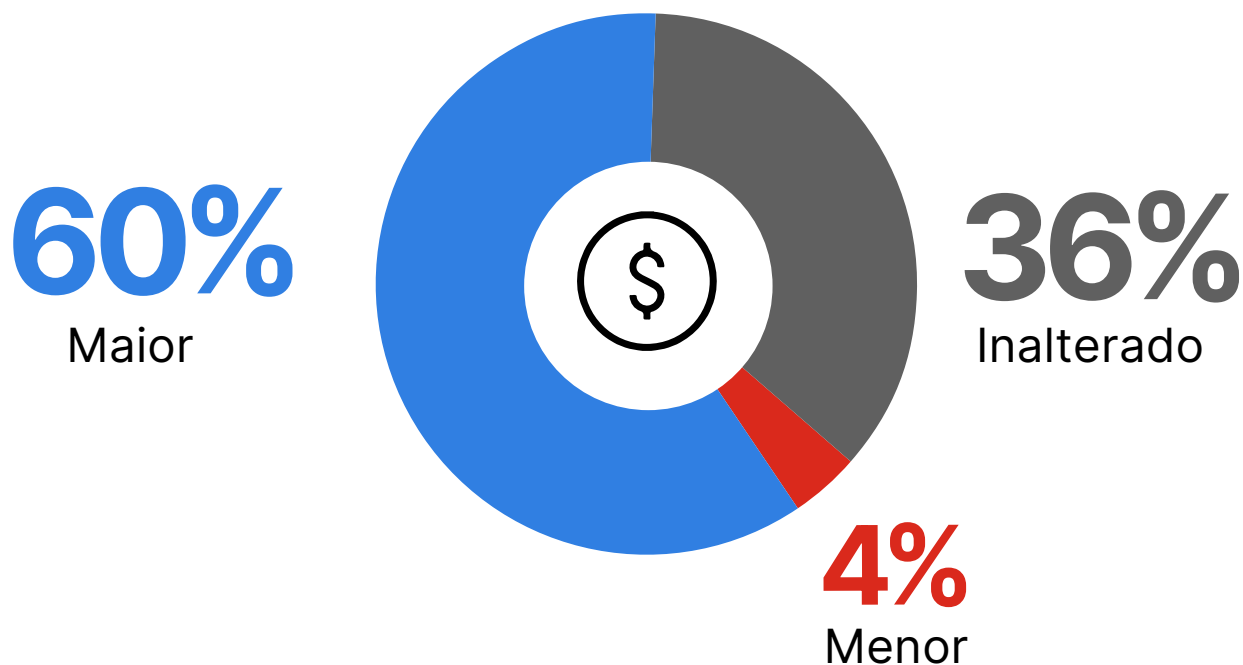
Principais prioridades para a segurança na nuvem



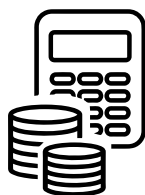
ORÇAMENTO DA NUVEM

Apesar das turbulências macroeconômicas e do abrandamento da carga de trabalho em relação aos anos anteriores, a maioria das organizações (60%) verá este ano um impulso no seu orçamento de segurança na nuvem. Espera-se que esse impulso seja um aumento de 33% no poder de compra em relação ao ano anterior.

▶ Como é que o seu orçamento de segurança na nuvem mudará nos próximos 12 meses?



▶ Seu orçamento do seu programa de segurança aumentará? Se sim, em quantos por cento?



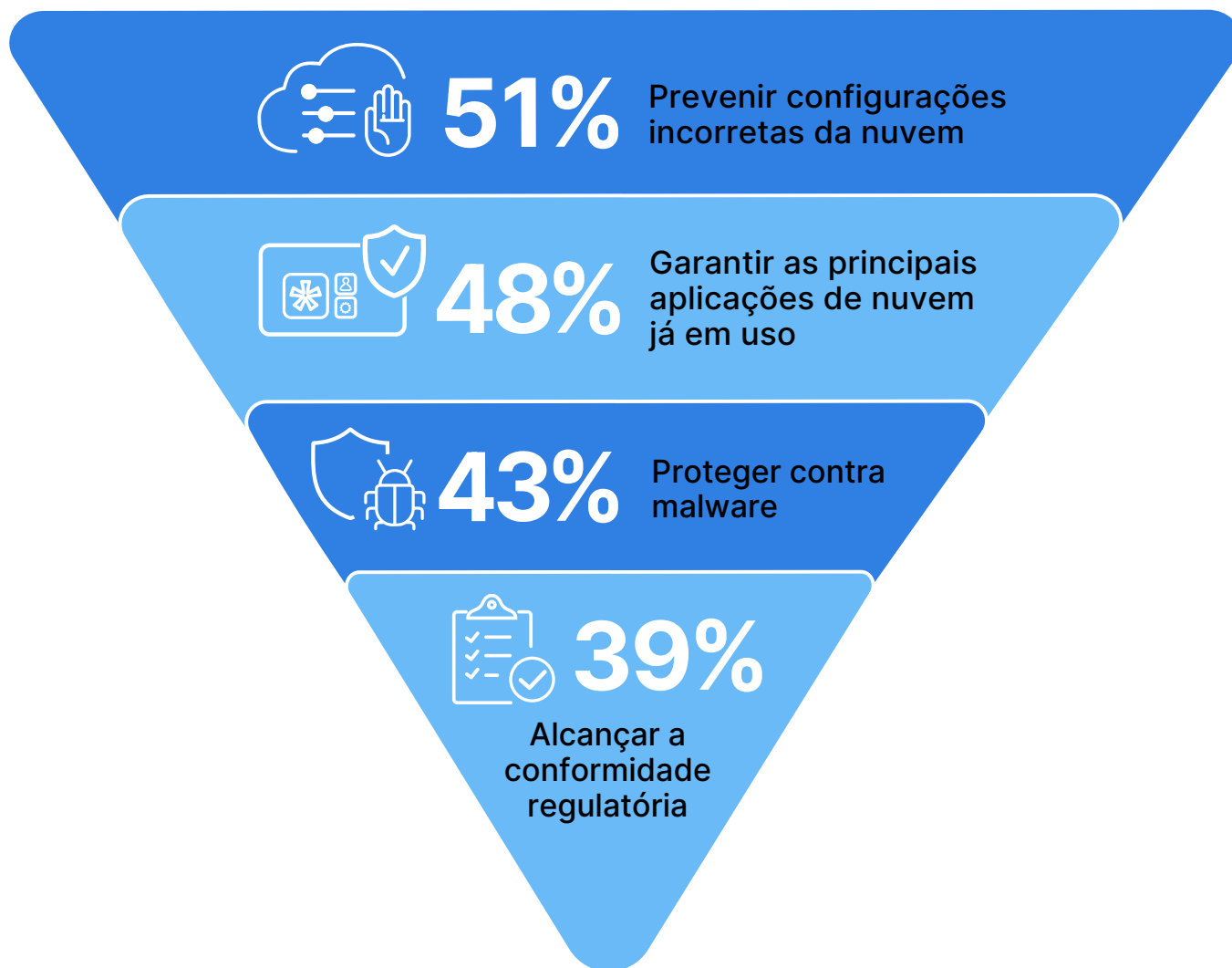
O orçamento irá aumentar em

33%

PRIORIDADES DA SEGURANÇA NA NUVEM

Os profissionais de segurança estão usando seus orçamentos na nuvem de forma criteriosa para enfrentar as ameaças e preocupações que representam o maior risco para o negócio. Não é de se surpreender que a prevenção da má configuração seja a prioridade número um (51%), mas a segurança das aplicações que já transitaram para a nuvem vem logo em seguida (48%).

► **Quais são as prioridades de segurança na nuvem de sua empresa este ano?**

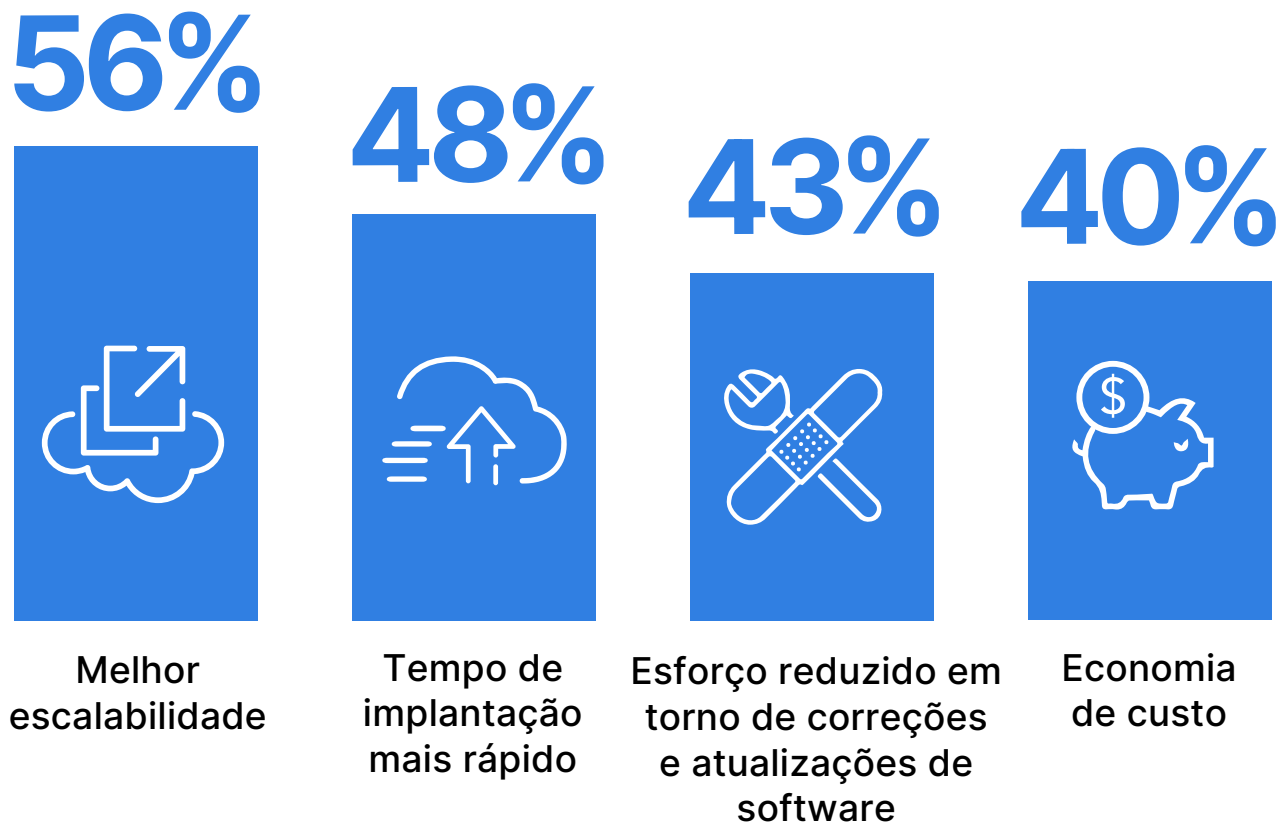


Treinamento em segurança na nuvem 12% | Proteger dispositivos móveis 7% | Descobrir aplicações de nuvem não sancionadas em uso 7% | Proteger BYOD (traga seu próprio dispositivo) 5% | Proteger aplicações de nuvem menos populares já em uso 4%

PRINCIPAIS FATORES DA SEGURANÇA BASEADA NA NUVEM

Com a nuvem, as organizações podem obter para seus serviços de segurança as mesmas vantagens que ela oferece às suas aplicações e cargas de trabalho, o que inclui uma melhor escalabilidade (56%), um tempo de implantação mais rápido (48%), um esforço menor em relação aos patches e atualizações de software (43%), e economia de custo (40%).

► **Quais são os principais fatores para ser possível considerar soluções de segurança baseadas na nuvem?**



Melhor visibilidade da atividade do usuário e do comportamento do sistema 38% | Melhor tempo de atividade 36% | Gerenciamento de políticas mais fácil 35% | Expectativas de conformidade da nuvem atendidas 35% | Melhor desempenho 35% | Necessidade de acesso seguro às aplicações a partir de qualquer local 34% | Nossos dados/cargas de trabalho residem na nuvem (ou estão transitando para a nuvem) 30% | Redução da pegada dos dispositivos nas filiais 29% | Outros 3%

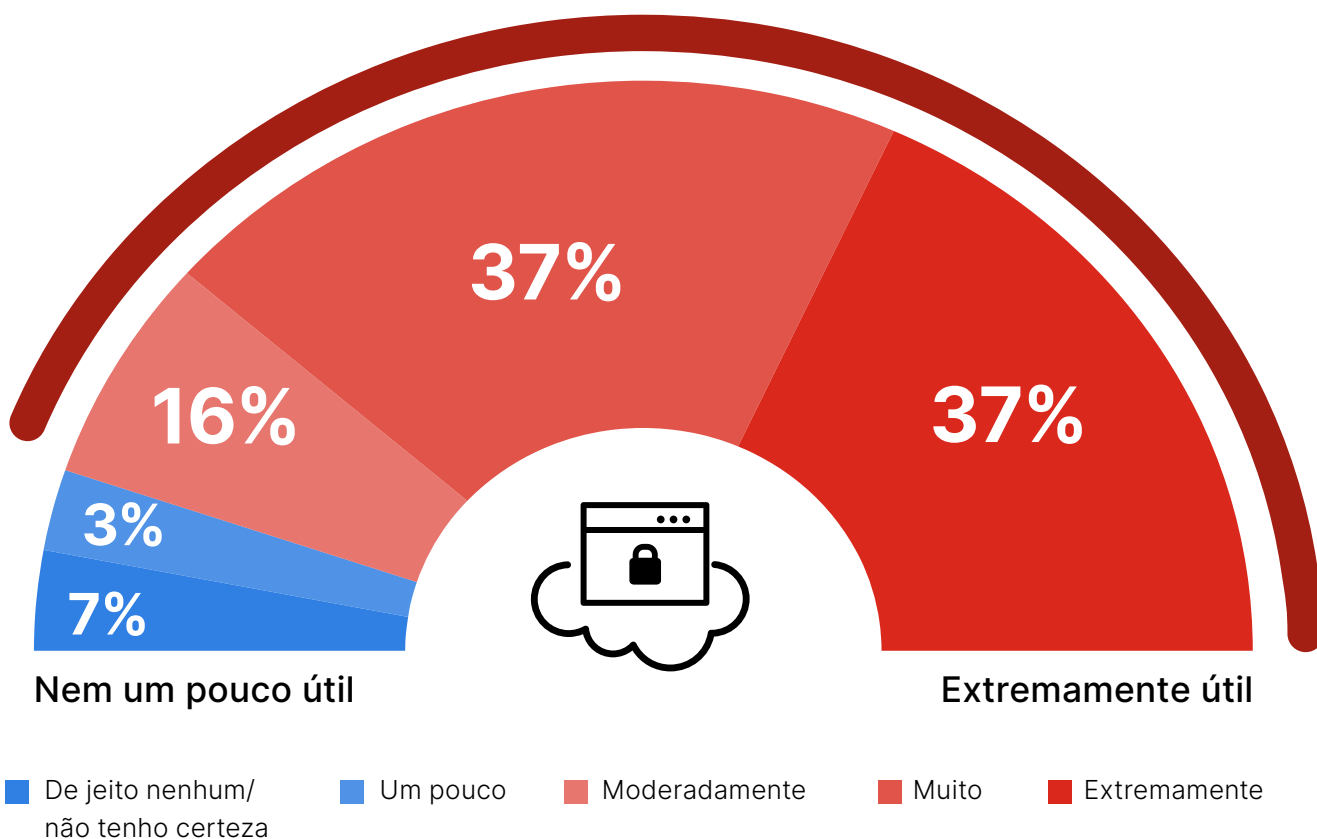
PLATAFORMA ÚNICA DE SEGURANÇA NA NUVEM

Dados os desafios relativos à visibilidade da segurança e à falta de talento cibernético, não é de se surpreender que a grande maioria dos entrevistados (90%) considere moderadamente útil ter uma única plataforma e um só painel de controle de segurança na nuvem para proteger os dados de forma consistente e abrangente em toda a sua presença na nuvem.

- ▶ O quanto seria útil ter uma plataforma de segurança na nuvem única com um único painel onde você pudesse configurar todas as políticas necessárias para proteger os dados de forma consistente e abrangente em toda a sua área de cobertura na nuvem?

90%

dos profissionais consideram a utilização de uma única plataforma de segurança em nuvem com um único painel de instrumentos como algo moderadamente a extremamente útil



METODOLOGIA E DADOS DEMOGRÁFICOS

O Relatório de Segurança na Nuvem de 2023 baseia-se em uma pesquisa global abrangente com 752 profissionais de cibersegurança, realizada em fevereiro de 2023, para descobrir como organizações de usuários na nuvem estão adotando a nuvem, como eles veem a evolução da segurança na nuvem e quais práticas recomendadas estão sendo priorizadas por líderes de cibersegurança de TI em suas transições para a nuvem. Os entrevistados vão desde diretores técnicos a profissionais de segurança de TI, representando uma seção transversal equilibrada de empresas de vários tamanhos e setores.

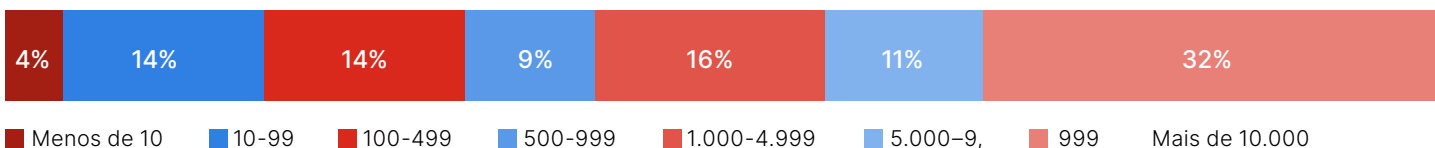
NÍVEL DE CARREIRA



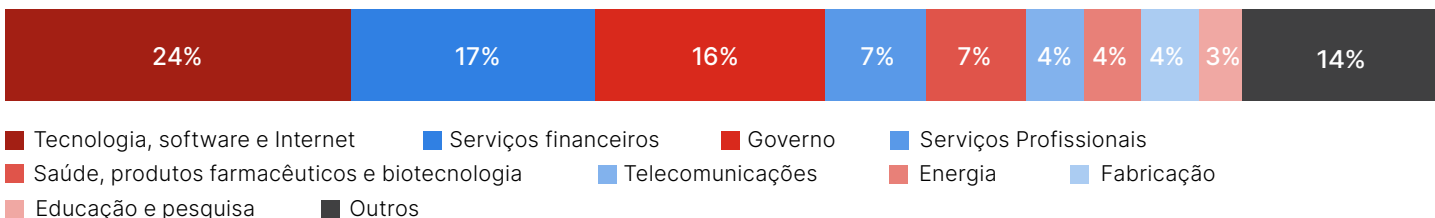
DEPARTAMENTO



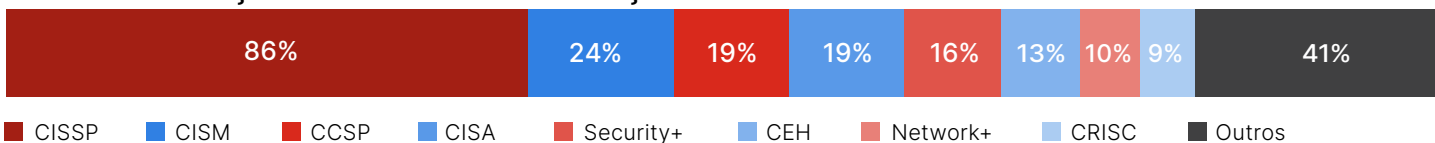
TAMANHO DA EMPRESA



SETOR



CERTIFICAÇÕES DE SEGURANÇA REALIZADAS





A Fortinet (NASDAQ: FTNT) fornece segurança às maiores empresas, provedores de serviços e organizações governamentais em todo o mundo.

A Fortinet capacita nossos clientes com visibilidade e controle completos em toda a superfície de ataque em expansão e tem capacidade de atender aos requisitos de desempenho cada vez maiores hoje e para o futuro.

Somente a plataforma Fortinet Security Fabric pode enfrentar os desafios de segurança mais críticos e proteger os dados em toda a infraestrutura digital, seja em redes, aplicações, mult nuvem ou ambientes de borda.

A Fortinet ocupa o 1º lugar como a empresa com o maior número de appliances de segurança vendidos em todo o mundo e mais de 635.000 clientes confiam na Fortinet para proteger seus negócios.

www.fortinet.com



Cybersecurity

I N S I D E R S

A Cybersecurity Insiders é uma comunidade on-line, com mais de 500.000 membros, para profissionais de segurança da informação, reunindo as melhores mentes dedicadas ao avanço da cibersegurança e à proteção de empresas em todos os setores, tamanhos e funções de segurança.

Fornecemos aos comerciantes de cibersegurança [oportunidades únicas de marketing](#) para alcançar este público qualificado e fornecer conteúdos de liderança inovadora baseada em fatos, programas de geração de demanda e visibilidade da marca no mercado de cibersegurança.

**Para mais informações, acesse
www.cybersecurity-insiders.com**