2022

Cybersecurity INSIDERS

CLOUD SECURITY REPORT

FORTINET®

INTRODUÇÃO

As empresas continuam transferindo cargas de trabalho para a nuvem a um ritmo veloz, para chegar mais rapidamente ao mercado, obter maior capacidade de resposta e reduções de custos. Como a maioria das empresas espera ter mais de metade de suas cargas de trabalho na nuvem nos próximos 12 a 18 meses, não é surpresa que a segurança em nuvem continue a ser uma das principais preocupações.

Este Relatório de Segurança em Nuvem de 2022, baseado num levantamento global abrangente de profissionais de segurança cibernética, revela estes desafios de segurança e oferece novos conhecimentos sobre o estado atual da nuvem e da segurança na nuvem. O estudo analisa as escolhas e respostas das empresas enquanto tentam ganhar mais confiança na segurança de seus ambientes de computação em nuvem.

Os resultados a seguir da pesquisa destacam os insights revelados pelo relatório:

- A maioria das empresas continua a seguir uma estratégia híbrida (39%, acima dos 36% do ano passado) ou multinuvem (33%) para integrar múltiplos serviços, por razões de escalabilidade ou de continuidade dos negócios. Setenta e seis por cento estão utilizando dois ou mais fornecedores de nuvem.
- As empresas continuam transferindo cargas de trabalho para a nuvem a um ritmo veloz. Atualmente, 39% dos participantes têm mais de metade de sua carga de trabalho na nuvem, enquanto que 58% planejam chegar a este patamar nos próximos 12 a 18 meses.
- Os usuários da nuvem confirmam que ela está cumprindo a promessa de capacidade flexível e escalabilidade (53%), aumento da agilidade (50%) e melhoria da disponibilidade e continuidade dos negócios (45%).
- Os profissionais de segurança salientam a falta de visibilidade (49%), o custo elevado (43%), a falta de controle (42%) e a falta de segurança (22%) como os maiores fatores imprevistos que retardam ou suspendem a adoção da nuvem.
- A segurança em nuvem continua a ser uma preocupação significativa para os profissionais de segurança cibernética. Com um aumento de dois pontos percentuais em relação ao ano passado, 95% das empresas estão moderada a extremamente preocupadas com sua postura de segurança num ambiente de nuvem pública.
- Mais de três quartos (78%) dos participantes consideram muito a extremamente útil ter uma única plataforma de segurança em nuvem com um único painel de controle para proteger os dados de forma consistente e abrangente em toda a pegada 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

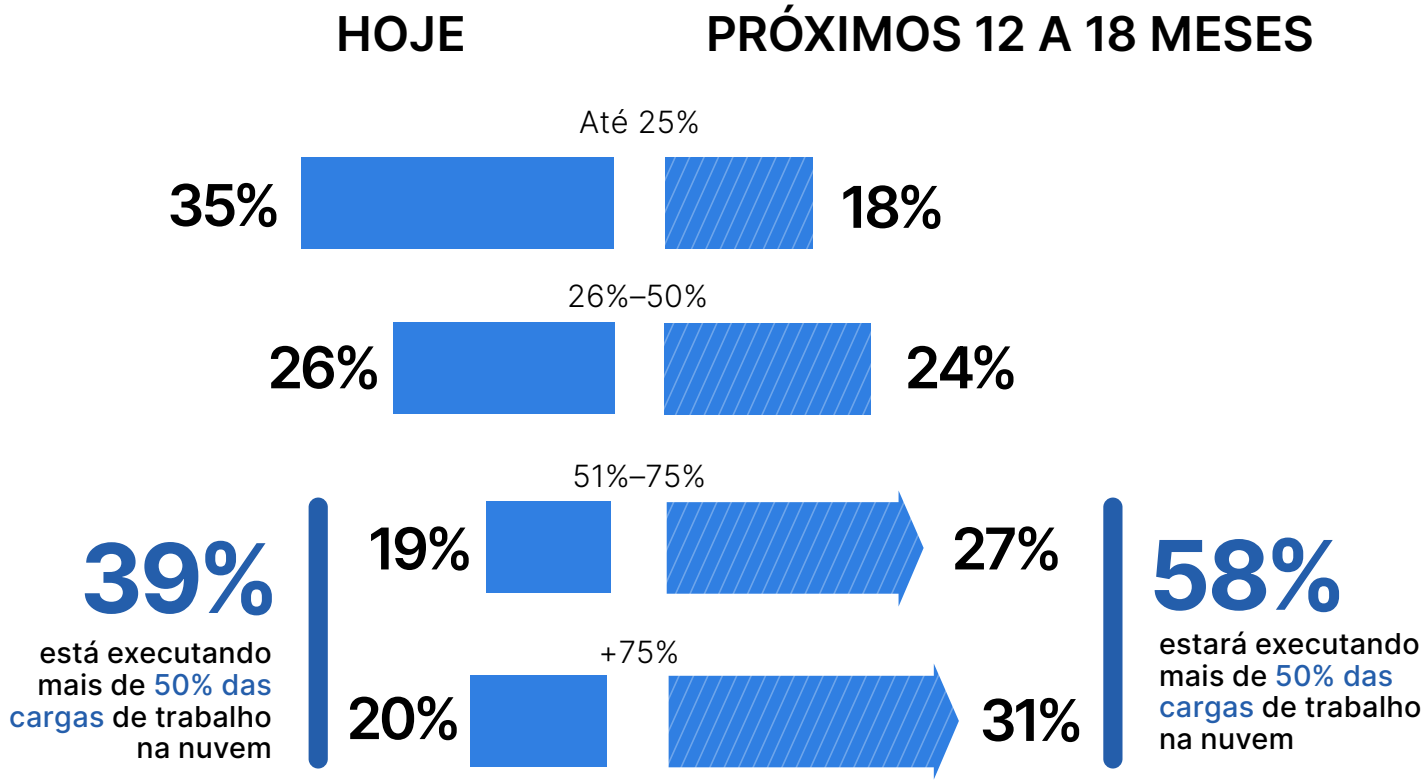
Estado atual da adoção da nuvem

CARGAS DE TRABALHO NA NUVEM

As empresas continuam transferindo cargas de trabalho para a nuvem a um ritmo veloz. Atualmente, 39% dos participantes têm mais de metade de sua carga de trabalho na nuvem, enquanto que 58% planejam chegar a este patamar 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

SERVIÇOS NA NUVEM IMPLANTADOS

Perguntamos aos profissionais de segurança cibernética quais os serviços e cargas de trabalho que suas empresas estão implementando com mais frequência na nuvem. Os serviços de segurança encabeçam a lista (58%), seguidos por computação (56%), armazenamento (55%) e virtualização (53%).

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

58%

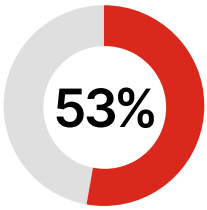
Segurança
(gerenciamento de identidade, controle de acesso, proteção de dados etc.)

56%

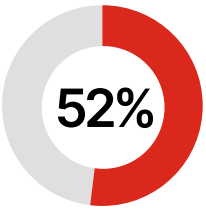
Computação
(servidores, contêineres etc.)

55%

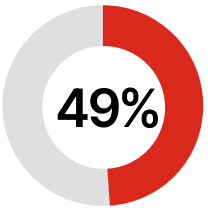
Armazenamento
(armazenamento de objetos, arquivo, backup etc.)



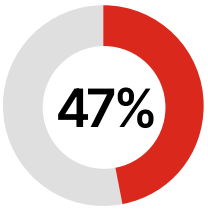
Virtualização



Aplicações comerciais (CRM, automação de marketing, ERP, BI, gerenciamento de projetos etc.)



Banco de dados (relacional, NoSQL, caching etc.)



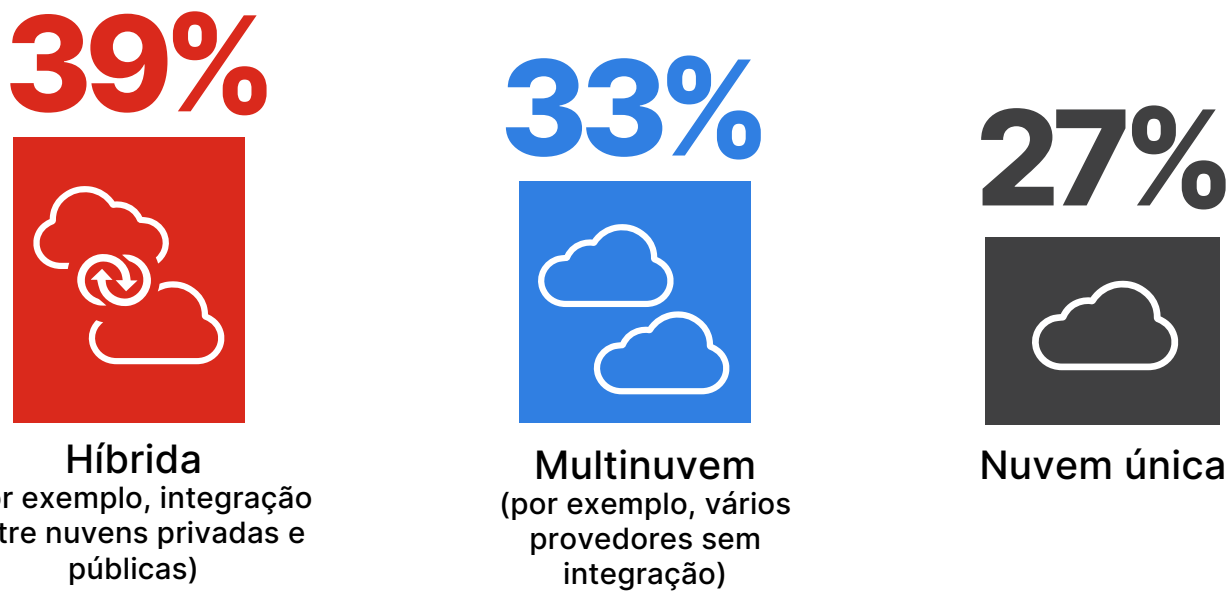
Aplicações de produtividade (e-mail, colaboração, mensagens instantâneas etc.)

Aplicações de desenvolvimento/teste 43% | Aplicações de operações de TI (administração, backup, provisionamento, monitoramento etc.) 42% | Networking e entrega de conteúdos (nuvem privada virtual, DNS etc.) 42% | Sistema operacional 37% | Middleware 27% | Desktop e streaming de aplicações 24% | Tempo de execução 16% | Não sei/outros 6%

ESTRATÉGIAS DE IMPLANTAÇÃO NA NUVEM

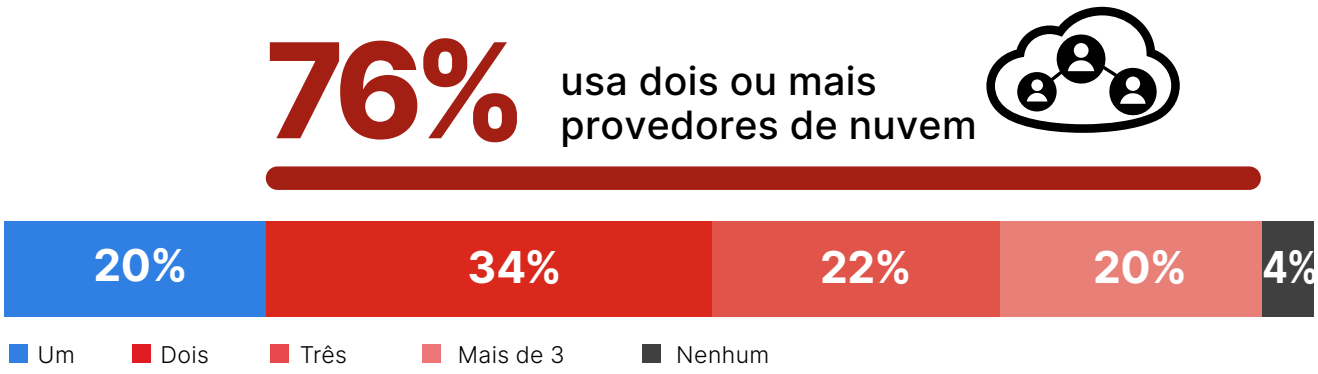
A maioria das empresas continua a seguir uma estratégia híbrida (39%, acima dos 36% do ano passado) ou multinuvem (33%, abaixo dos 35% do ano passado) para integrar múltiplos serviços, por razões de escalabilidade ou de continuidade dos negócios. Setenta e seis por cento estão utilizando dois ou mais fornecedores de nuvem.

Qual é a sua principal estratégia de implantação na nuvem?



Outros 1%

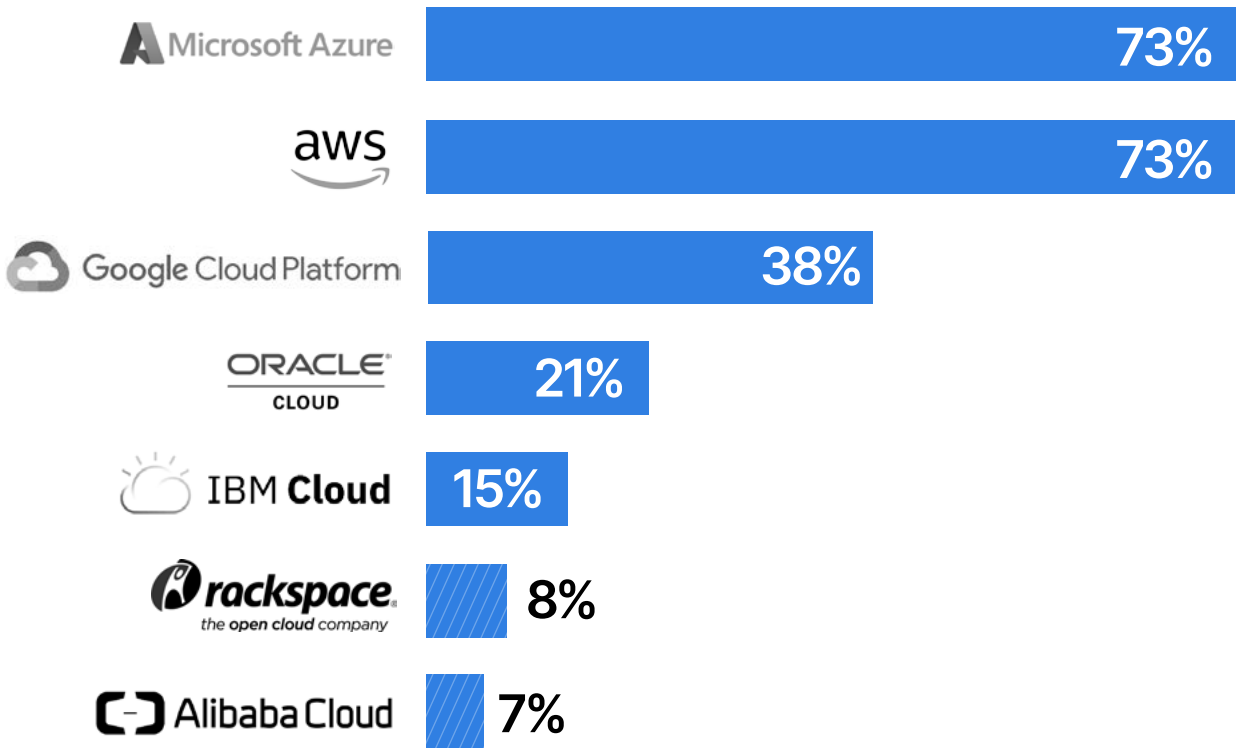
Quantos provedores de nuvem sua organização usa atualmente?



PROVEDORES DE NUVEM POPULARES

Os provedores de nuvem mais populares, Microsoft Azure e Amazon Web Services (AWS), estão empatados (73%), uma vez que a AWS ganhou três pontos percentuais desde a pesquisa do ano passado. Eles são seguidos pela Google Cloud Platform (38%). Ano após ano, o uso da Oracle Cloud foi o que mais cresceu (de 15% para 21%).

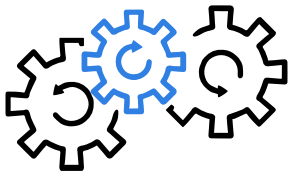
Quais provedores de IaaS em nuvem você usa atualmente?

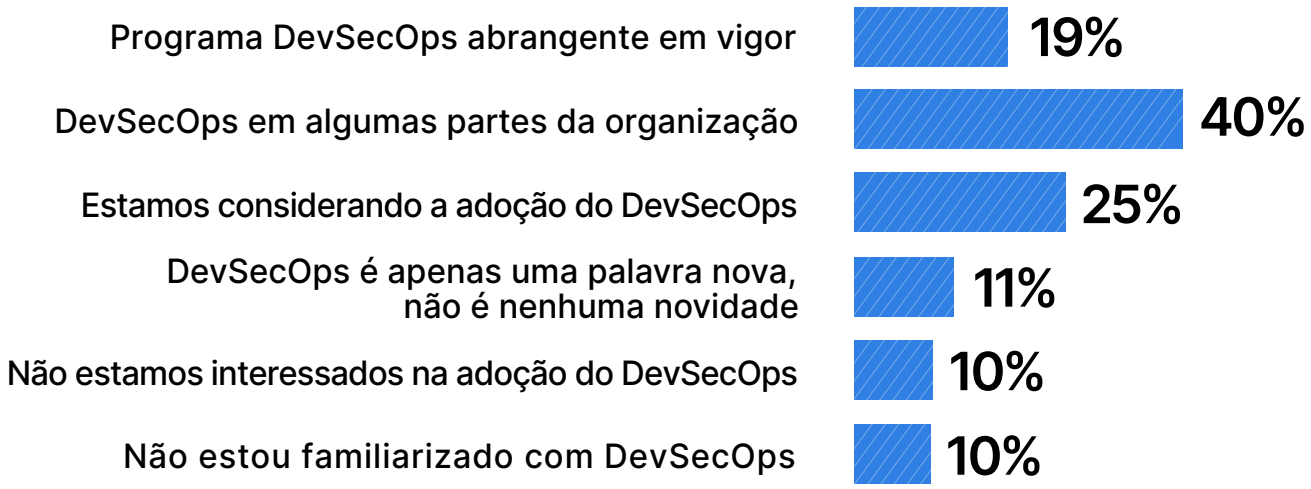


ADOÇÃO DE DEVSECOPS

O DevSecOps ajuda a garantir que a segurança seja abordada como parte das práticas DevOps, integrando segurança e conformidade ao longo de todo o processo de desenvolvimento de software. Embora apenas 19% dos participantes já disponham de DevSecOps completo, 40% incorporam alguns aspectos do DevSecOps à empresa.

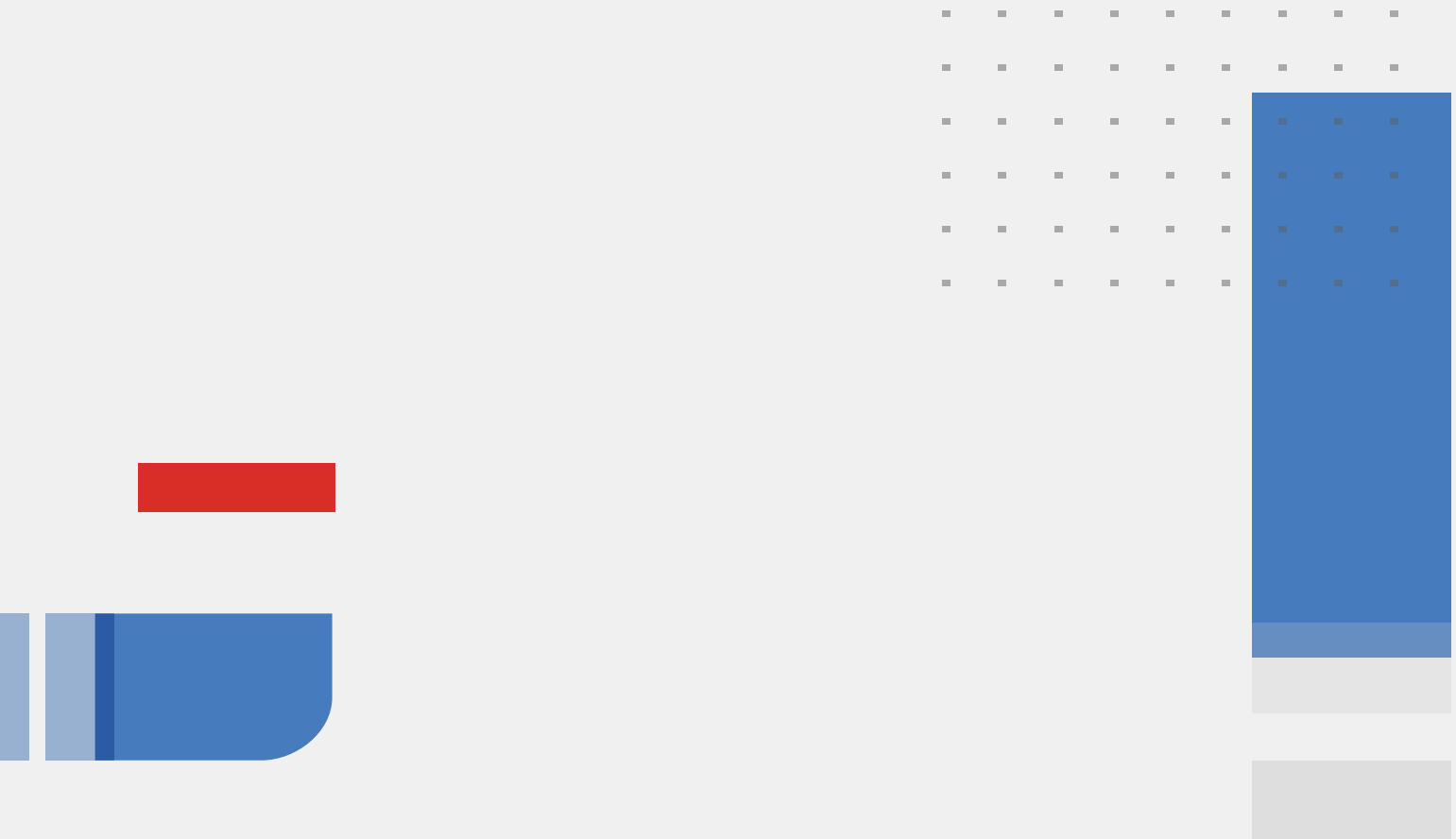
Qual é a posição atual de sua empresa com relação ao DevSecOps?





Outros 3%

Benefícios da nuvem: o melhor dos dois mundos



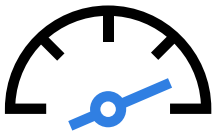
A NUVEM ENTREGA RESULTADOS COMERCIAIS

A pesquisa confirma que as empresas estão recebendo os resultados comerciais prometidos da computação em nuvem: tempo mais rápido de chegada ao mercado (51%), maior capacidade de resposta (50%) e reduções de custos (39%).

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

51%

Tempo acelerado de lançamento no mercado



50%

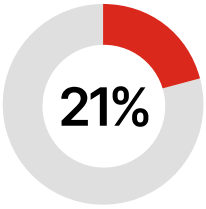
Maior capacidade de resposta às necessidades do cliente

39%

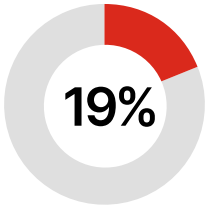
Custo reduzido

37%

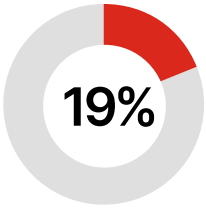
Risco reduzido e segurança aprimorada



Alcance de mercado expandido para novos mercados



Crescimento acelerado da receita nos mercados existentes



Ganho de paridade com os concorrentes

Outros 7%

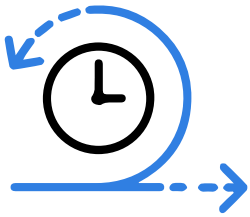
BENEFÍCIOS DA NUVEM

A computação em nuvem proporciona os benefícios esperados? Os usuários da nuvem confirmam que ela está cumprindo a promessa de capacidade flexível e escalabilidade (53%), aumento da agilidade (50%) e melhoria da disponibilidade e continuidade dos negócios (45%).

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

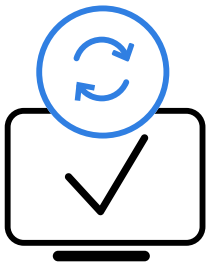
53%

Capacidade/escalabilidade mais flexível



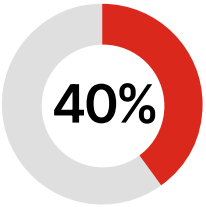
50%

Aumento da agilidade

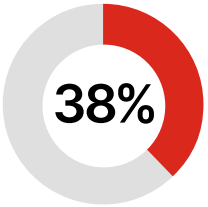


45%

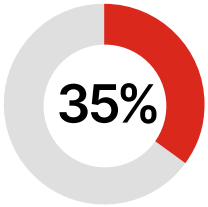
Melhoria da disponibilidade e continuidade dos negócios



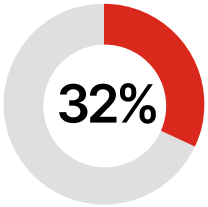
Despesas movimentadas de CAPEX fixo (compra) para OPEX variável (aluguel/assinatura)



Melhoria do desempenho



Custo reduzido



Tempo acelerado de lançamento no mercado

Melhoria da segurança 27% | Aumento do alcance geográfico 27% | Aumento da produtividade dos funcionários 22% | Melhoria da conformidade regulatória 21% | Redução da complexidade 19% | Não tenho certeza/outros 12%

Obstáculos à adoção

BARREIRAS À ADOÇÃO DA NUVEM

As soluções baseadas na nuvem oferecem vantagens significativas, mas ainda existem barreiras à adoção da nuvem. A pesquisa revela que os maiores desafios que as empresas enfrentam não têm a ver principalmente com tecnologia, mas com pessoas e processos. A falta de pessoal qualificado (40%, acima dos 37% do ano passado) é o maior impedimento a uma adoção mais rápida, seguida do cumprimento regulatório e legal (33%) e de questões de segurança de dados (31%).

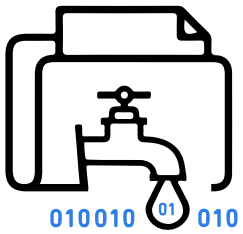
Quais são as maiores barreiras à adoção da nuvem em sua empresa?

40%

Falta de recursos humanos ou experiência

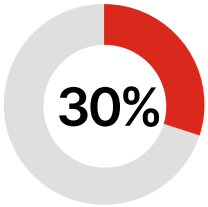
33%

Conformidade regulatória e legal

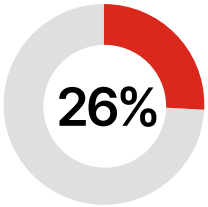


31%

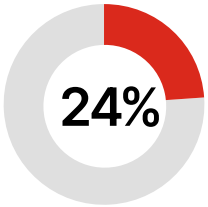
Riscos de segurança, perda e vazamento de dados



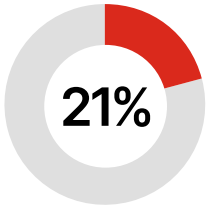
Integração com ambiente de TI existente



Temor de "lock-in" de distribuidor



Riscos gerais de segurança



Perda do controle

Resistência interna e inércia 20% | Custo/falta de ROI 18% | Falta de orçamento 18% | Complexidade na gestão da implantação da nuvem 18% | Falta de transparência e visibilidade 16% | Falta de maturidade dos modelos de serviços na nuvem 15% | Falta de faturamento e acompanhamento 11% | Falta de adesão da gerência 11% | Insatisfação com as ofertas de serviços/desempenho/preços da nuvem 10% | Falta de apoio por parte do fornecedor da nuvem 9% | Desempenho das aplicações na nuvem 9% | Falta de personalização 7% | Disponibilidade 6% | Outros 6%

SURPRESAS DA IMPLANTAÇÃO NA NUVEM

Quando perguntamos que surpresas os profissionais de segurança descobriram que impedem a adoção da nuvem, vimos que a falta de visibilidade (49%), o custo elevado (43%), a falta de controle (42%) e a falta de segurança (22%) são os maiores fatores imprevistos que retardam ou suspendem a adoção da nuvem.

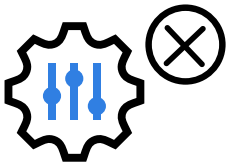
Que surpresas você descobriu que podem atrasar/suspender a adoção da nuvem?

49%

Falta de visibilidade

43%

Custo elevado



42%

Controle insuficiente

22%

Inseguro

Outros 13%

Preocupações de segurança na nuvem

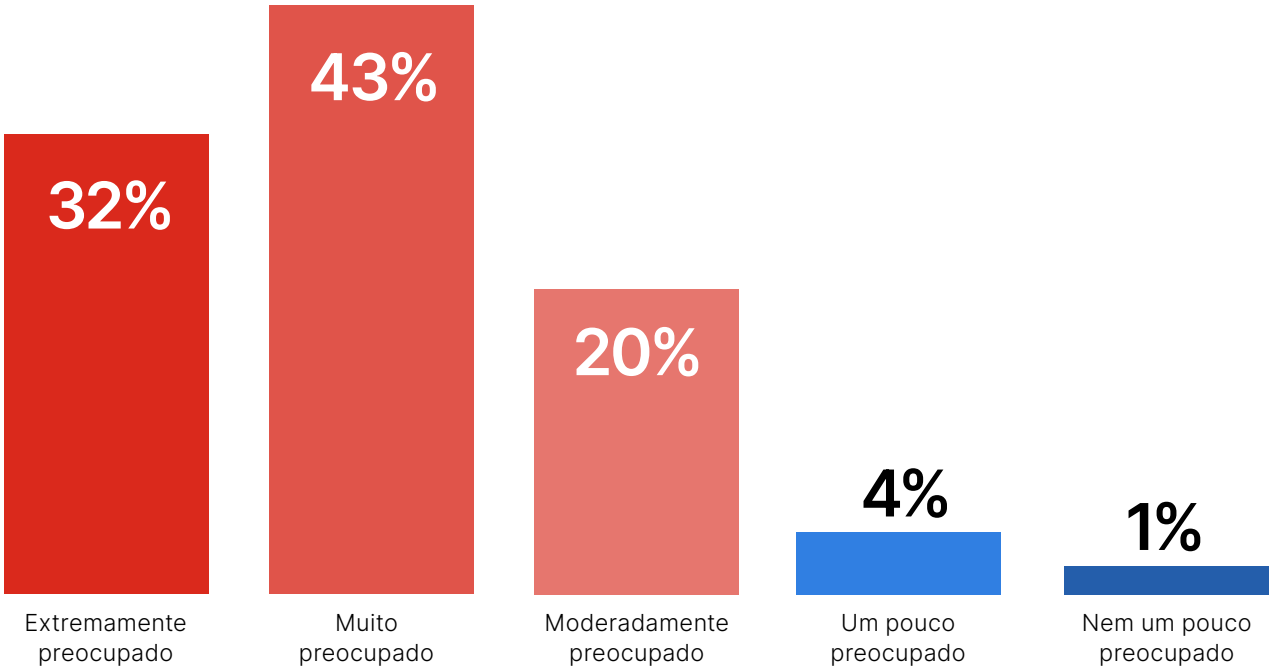
PREOCUPAÇÕES DE SEGURANÇA EM NUVEM PÚBLICA

A segurança em nuvem continua a ser uma preocupação significativa para os profissionais de segurança cibernética. Com um aumento de dois pontos percentuais em relação ao ano passado, 95% das empresas estão moderada a extremamente preocupadas com sua postura de segurança num ambiente de nuvem pública.

O quanto você está preocupado com a segurança das nuvens públicas?

95%

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



MAIORES AMEAÇAS À SEGURANÇA

Perguntamos aos profissionais de segurança cibernética sobre as ameaças de segurança em nuvem que mais os preocupam. A má configuração da plataforma em nuvem continua a ser o maior risco de segurança, segundo 62% dos profissionais de segurança cibernética em nossa pesquisa. Em seguida, interfaces/APIs inseguras (52%, acima dos 49% do ano passado), exfiltração de dados confidenciais (51%) e acesso não autorizado (50%).

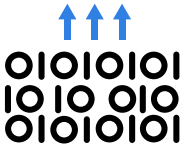
O que você vê como as maiores ameaças à segurança nas nuvens públicas?

62%

Configuração incorreta da plataforma de nuvem/instalação incorreta

52%

Interfaces/APIs inseguras

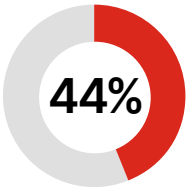


51%

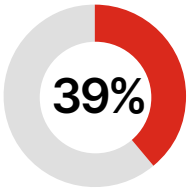
Exfiltração de dados confidenciais

50%

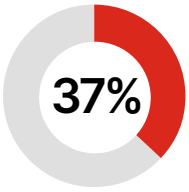
Acesso não autorizado



Roubo de contas, serviços ou tráfego



Compartilhamento externo de dados



Ataques cibernéticos patrocinados por país estrangeiro

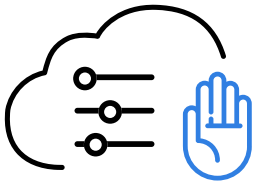
Malware/ransomware 36% | Invasores maliciosos 34% | Ataques de negação de serviço 33% | Cryptojacking em nuvem 20% | Roubo de serviço 18% | Dispositivos móveis perdidos 10% | Não sei/outros 8%

Principais prioridades para a segurança em nuvem

PRIORIDADES
DA SEGURANÇA EM NUVEM

Quando questionadas sobre suas prioridades de segurança para o ano em curso, as empresas destacaram a prevenção de erros de configuração da nuvem (20%), o cumprimento da conformidade regulatória (19%), a segurança das aplicações de nuvem (16%) e a defesa contra malware (15%).

Quais são as prioridades de segurança em nuvem de sua empresa este ano?



20%

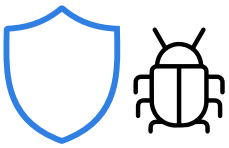
Prevenir configurações incorretas da nuvem

19%

Alcançar a conformidade regulatória

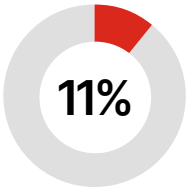
16%

Garantir as principais aplicações de nuvem já em uso

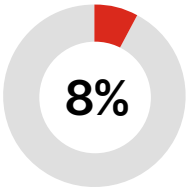


15%

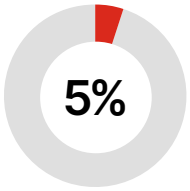
Proteger contra malware



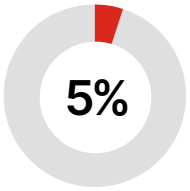
Treinamento em segurança em nuvem



Proteger dispositivos móveis



Descobrir aplicações de nuvem não sancionadas em uso

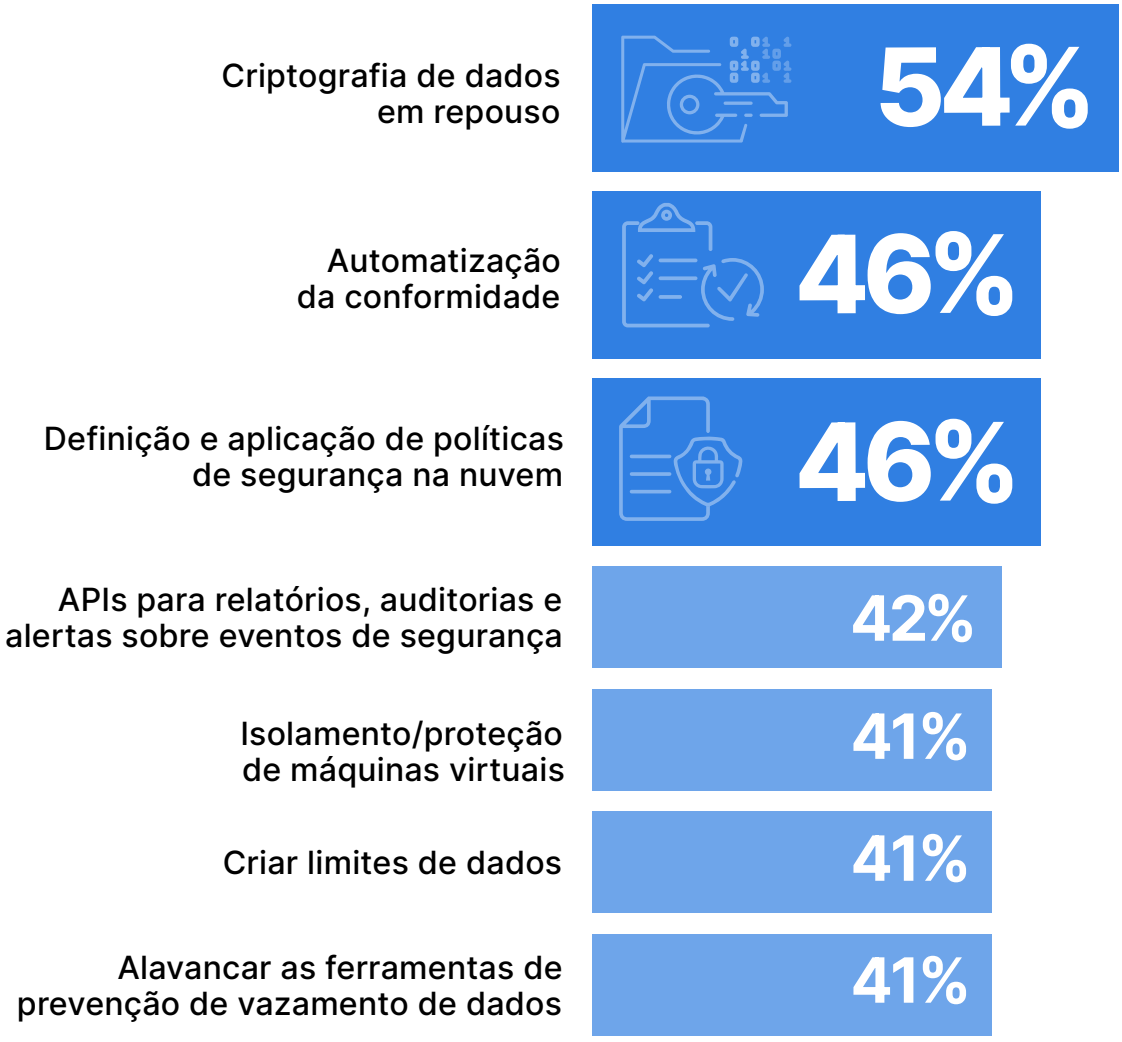


Garantir o BYOD (traga o seu próprio dispositivo)

MELHORAR OS CONTROLES DE SEGURANÇA

Os profissionais de segurança procuram formas de melhorar a segurança das nuvens públicas. Quando questionados sobre quais controles aumentariam sua confiança na adoção de serviços na nuvem, três controles encabeçam a lista: criptografia de dados em repouso (54%), automatização da conformidade (46%) e definição e aplicação de políticas de segurança (46%).

Qual dos seguintes controles de segurança aumentaria mais a sua confiança na adoção de nuvens públicas?



Alavancar as ferramentas de prevenção de ameaças 34% | Limitar o acesso não gerido a dispositivos 32% | Proteger cargas de trabalho 31% | Proxy de tráfego para segurança em tempo real no acesso 23% | Outros 3%

DESAFIOS DA SEGURANÇA MULTINUVEM

Os ambientes multinuvem continuam acrescentando complexidade e desafios de segurança. A falta de competências de segurança torna-se o principal desafio (61%, acima dos 57% do ano passado), seguido da proteção de dados (53%), a compreensão de como as diferentes soluções se encaixam (51%) e a perda de visibilidade e controle (47%).

Quais são os seus maiores desafios para proteger ambientes multinuvem?

61%

Ter as habilidades certas para implantar e gerenciar uma solução completa em todos os ambientes de nuvem

53%

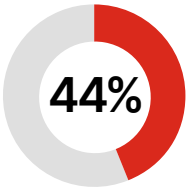
Garantir a proteção dos dados e privacidade para cada ambiente

51%

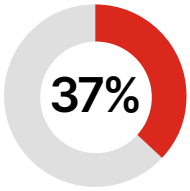
Compreender como diferentes soluções se encaixam

47%

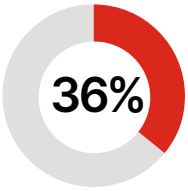
Perda de visibilidade e controle



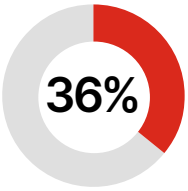
Compreender as opções de integração de serviço



Acompanhar a taxa de mudança



Selecionar o conjunto certo de serviços



Gestão dos custos de diferentes soluções

Proporcionar acesso sem falhas aos usuários com base em suas credenciais 34% | Outros 3%

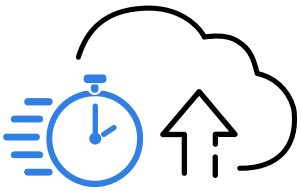
FATORES FUNDAMENTAIS PARA UMA SEGURANÇA BASEADA NA NUVEM

As empresas dão prioridade a vários fatores cruciais ao considerar soluções de segurança baseadas na nuvem, em oposição a plataformas ultrapassadas. Os maiores fomentadores são uma melhor escalabilidade (55%) e tempo de implantação mais rápido (50%), seguidos de economias de custos (43%) e melhor visibilidade da atividade dos usuários e do comportamento do sistema (40%).

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

55%

Melhor escalabilidade

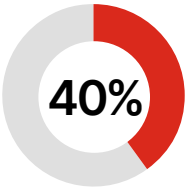


50%

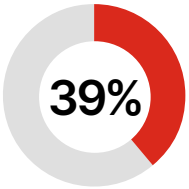
Tempo de implantação mais rápido

43%

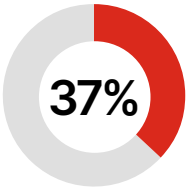
Economia de custo



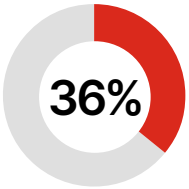
Melhor visibilidade da atividade do usuário e do comportamento do sistema



Esforço reduzido em torno de correções e atualizações de software



Cumprir as expectativas de conformidade da nuvem



Gerenciamento de políticas mais fácil

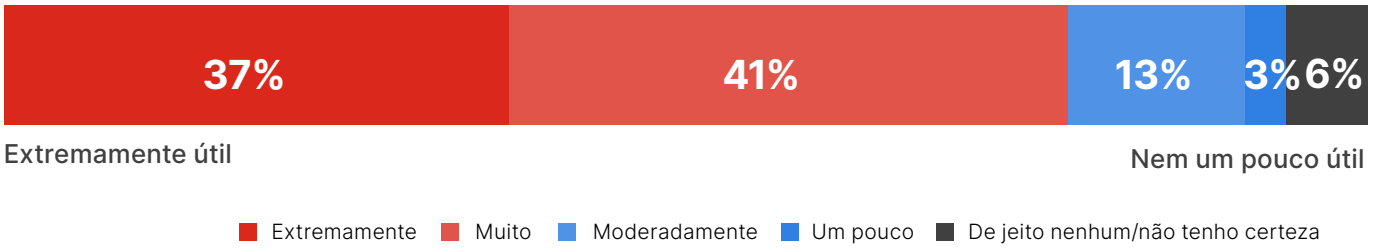
Necessidade de acesso seguro às aplicações a partir de qualquer local 35% | Melhor tempo de funcionamento 34% | Melhor desempenho 32% | Nossos dados/cargas de trabalho residem na nuvem (ou estão sendo transferidos para a nuvem) 31% | Redução da pegada dos aparelhos nas filiais 29% | Outros 3%

PLATAFORMA ÚNICA DE SEGURANÇA EM NUVEM

Não surpreende que mais de três quartos (78%) dos participantes consideram muito a extremamente útil ter uma única plataforma de segurança em nuvem para proteger os dados de forma consistente e abrangente em toda a pegada na nuvem.

O quanto seria útil ter uma plataforma de segurança em 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?

78% de profissionais consideram a utilização de uma única plataforma de segurança em nuvem com um único painel de instrumentos como algo muito a extremamente útil



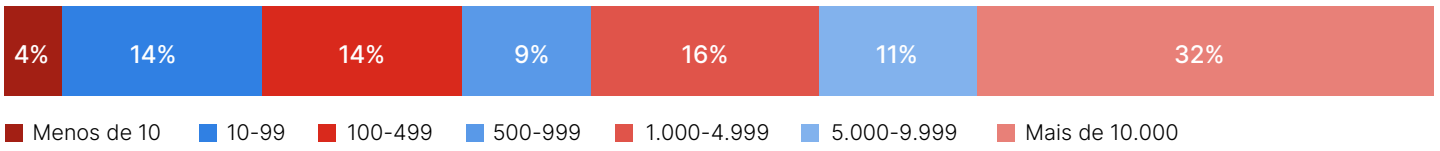
METODOLOGIA
E DADOS DEMOGRÁFICOS

O Relatório de Segurança em Nuvem de 2022 se baseia numa pesquisa global abrangente com 823 profissionais de segurança cibernética, realizada em março de 2022, para descobrir como as empresas de usuários de nuvem estão respondendo às ameaças à segurança em nuvem, e quais treinamentos, certificações e boas práticas os líderes de segurança cibernética das TI estão priorizando em sua mudança para a nuvem. Os participantes vão desde executivos técnicos a profissionais de segurança cibernética, representando uma seção transversal equilibrada de empresas de vários tamanhos e setores.

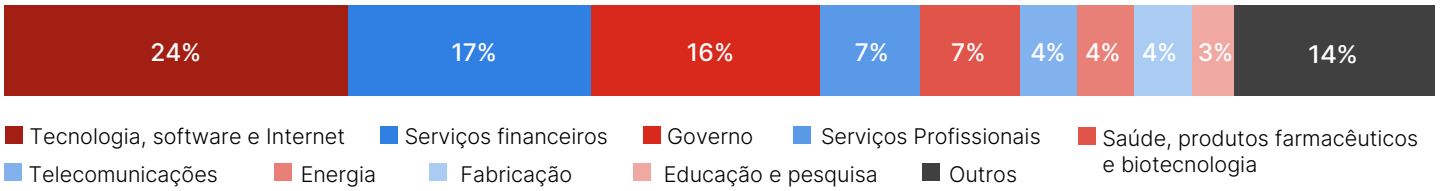
NÍVEL DE CARREIRA

DEPARTAMENTO

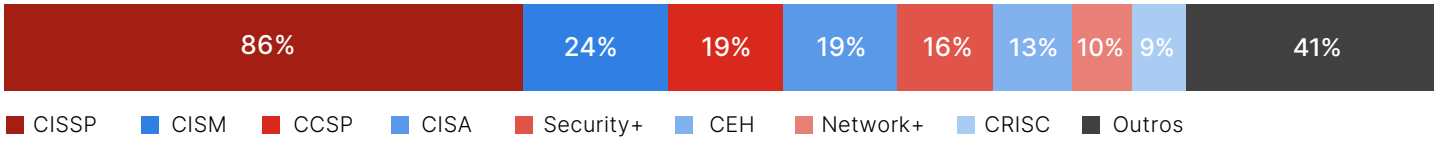
TAMANHO DA EMPRESA



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, multinuvem 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 500.000 clientes confiam na Fortinet para proteger seus negócios.

www.fortinet.com

Cybersecurity
INSIDERS

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 segurança cibernética e à proteção de empresas em todas os setores, tamanhos e funções de segurança.

Fornecemos aos comerciantes de segurança cibernética 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 segurança cibernética.

Para mais informações acesse www.cybersecurity-insiders.com