

2024

Relatório sobre Segurança na Nuvem



FORTINET®

Introdução

As empresas estão adotando cada vez mais uma estratégia centrada na nuvem, desenvolvendo e implantando aplicativos com a nuvem em mente. Com a maioria das organizações adotando uma abordagem híbrida ou de várias nuvens para dar suporte a diversos casos de uso e modelos de trabalho, a superfície de ataque se expandiu significativamente, tornando a proteção dos atuais ambientes de nuvem mais crítica e cada vez mais complexa.

O Relatório sobre Segurança na Nuvem 2024, baseado em uma pesquisa abrangente com 927 profissionais de segurança cibernética em todo o mundo, fornece insights essenciais sobre as tendências atuais que impulsionam a segurança na nuvem. Ele explora os principais desafios na proteção de ambientes complexos de nuvem, quais soluções e estratégias os profissionais de segurança cibernética estão priorizando, como estão alocando seus recursos e as práticas recomendadas que estão adotando para garantir a segurança das cargas de trabalho na nuvem.

As principais observações incluem:

- **Preferência por multinuvem:** A maioria das organizações (78%) opta por estratégias híbridas e de várias nuvens para combinar flexibilidade, controle e os benefícios exclusivos de vários serviços em nuvem.
- **Barreiras à adoção da nuvem:** As preocupações com segurança e conformidade (59%) são obstáculos críticos para a adoção mais rápida de estratégias de várias nuvens. Os desafios técnicos (52%) e as restrições de recursos (49%) apresentam desafios substanciais para a obtenção de visibilidade e controle de políticas em infraestruturas complexas de várias nuvens e enfatizam a necessidade de um sólido conhecimento especializado em segurança na nuvem.
- **Escassez de talentos em segurança cibernética:** As empresas enfrentam uma escassez crítica de conhecimento especializado em segurança cibernética, com 93% dos entrevistados preocupados em encontrar profissionais qualificados para proteger ambientes complexos de várias nuvens. Isso afeta diretamente sua postura de segurança e seus esforços estratégicos. Essa escassez persistente de especialização em segurança na nuvem impede a adoção mais rápida e generalizada de estratégias de várias nuvens.
- **Preferência por uma plataforma unificada de segurança na nuvem:** 95% dos entrevistados defendem uma plataforma única para otimizar a segurança em ambientes de nuvem. O objetivo é simplificar e automatizar o gerenciamento da segurança, atenuar a lacuna de talentos e aprimorar a segurança por meio da aplicação consistente de políticas e da visibilidade, abordando as ineficiências do gerenciamento de vários sistemas de segurança diferentes.

Gostaríamos de agradecer à [Fortinet](#) pelo inestimável apoio a esse importante projeto de pesquisa do setor. Esperamos que este relatório sirva como um guia prático para que os líderes e profissionais de segurança cibernética possam navegar pelas complexidades da segurança na nuvem de forma mais eficaz em seus esforços contínuos para proteger a jornada da nuvem de sua organização contra as ameaças cibernéticas em evolução.

Muito obrigado,

Holger Schulze

Founder, Cybersecurity Insiders

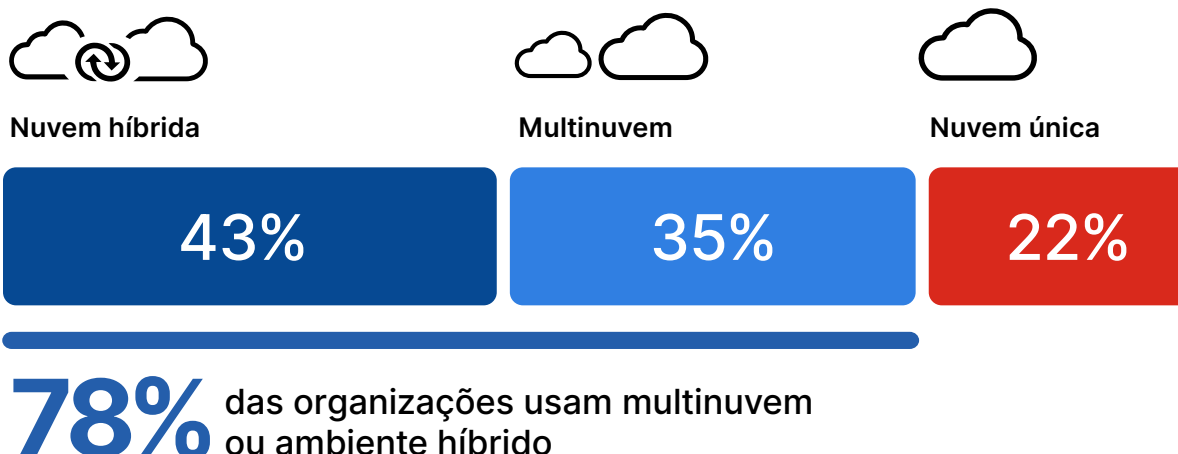
Cybersecurity
INSIDERS

Estratégias de Implantação de Nuvem

A escolha da estratégia correta de implementação da nuvem é fundamental para que as organizações maximizem os benefícios da computação em nuvem e, ao mesmo tempo, minimizem os riscos associados.

A maioria das organizações (78%) prefere uma estratégia híbrida ou de várias nuvens, integrando várias implementações em um único ambiente operacional. Uma grande parte delas (43%) usa uma infraestrutura híbrida de nuvem e local. 35% das organizações têm uma estratégia de várias nuvens, destacando uma preferência por aproveitar os pontos fortes de diferentes provedores de serviços em nuvem para uma variedade de casos de uso. Apenas 22% dependem de um único provedor de nuvem, o que sugere uma abordagem focada que simplifica o gerenciamento, mas pode aumentar a dependência de um único provedor.

► Qual é a principal estratégia da sua organização para a implantação da nuvem?



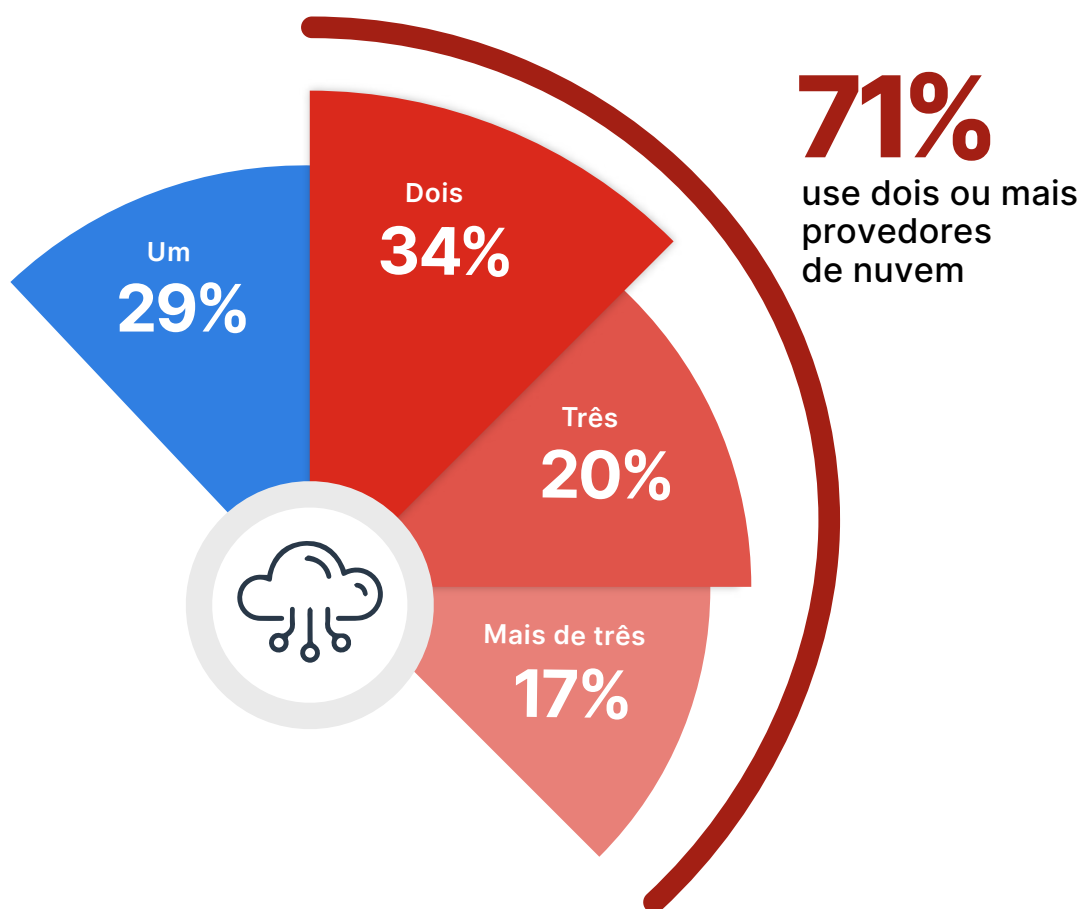
Para navegar melhor pelas complexidades das implementações híbridas e em várias nuvens, as organizações devem priorizar uma estrutura de segurança integrada que garanta uma proteção perfeita em toda a sua pegada digital. Isso é essencial para oferecer a agilidade, a escala e a segurança necessárias para uma defesa robusta contra as ameaças cibernéticas em constante evolução.

Adoção de Multinuvem

O número de provedores de nuvem que uma organização usa é crucial e afeta a flexibilidade operacional, o gerenciamento de riscos e a complexidade das implementações de segurança. A maioria das organizações (71%) usa dois ou mais provedores de nuvem, indicando uma abordagem que busca combinar flexibilidade, controle e os benefícios exclusivos de cada provedor de serviços em nuvem. Um aumento de 2 pontos percentuais em relação à pesquisa do ano passado reflete uma mudança crescente em direção a estratégias de várias nuvens, impulsionada pela necessidade de serviços de nuvem especializados, disponibilidade regional e redundância.

É interessante notar que apenas 29% das organizações dependem de apenas um provedor de nuvem, destacando uma preferência pela simplicidade e talvez uma parceria estratégica com um único provedor de nuvem.

► Quantos provedores de nuvem sua organização usa atualmente?



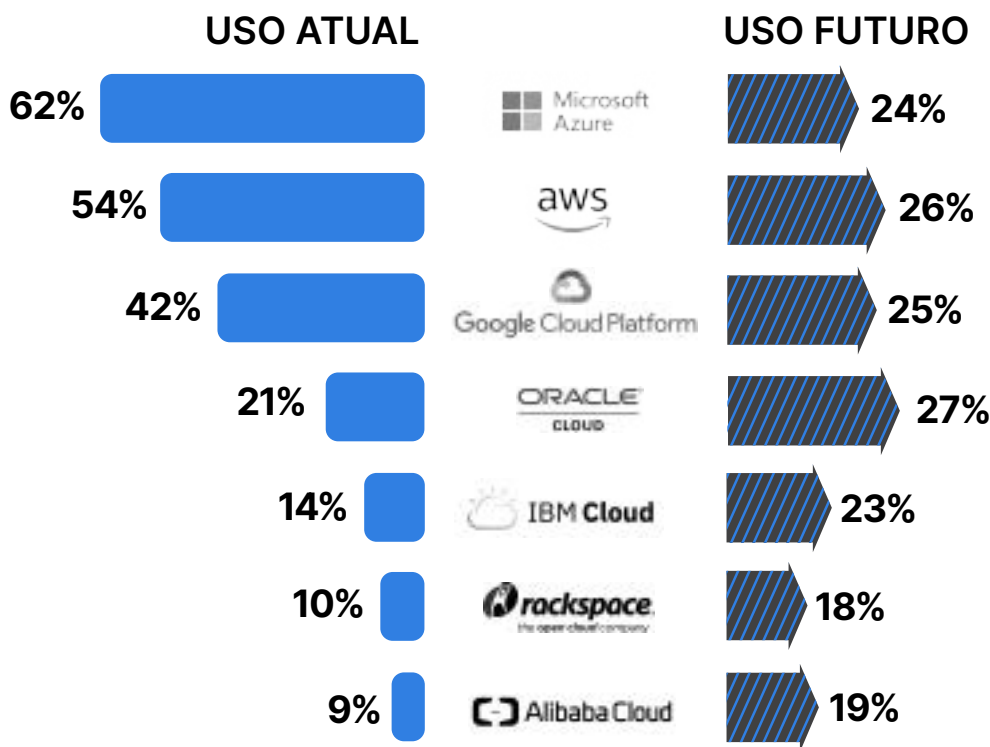
As organizações devem adotar uma abordagem contínua e neutra em relação à nuvem para proteger vários ambientes de nuvem, o que garante políticas de segurança consistentes e visibilidade em toda a sua pegada digital, reduzindo a complexidade e reforçando os mecanismos de defesa contra ameaças cibernéticas cada vez mais sofisticadas.

Provedores de Nuvem Preferidos

A seguir, perguntamos aos profissionais de segurança cibernética sobre o uso atual e futuro de provedores de nuvem, para entender melhor as mudanças na dinâmica do mercado dentro do ecossistema de nuvem. O Microsoft Azure continua a liderar o mercado, com 62% das organizações em nossa pesquisa utilizando atualmente seus serviços, seguido pelo Amazon Web Services (AWS) com 54%. Isso indica uma forte preferência por esses gigantes estabelecidos da nuvem.

Os resultados da pesquisa também destacam um interesse significativo na adoção futura de todos os provedores, especialmente Oracle Cloud e Google Cloud Platform, com 27% e 25% dos entrevistados planejando adotar esses serviços, respectivamente. Isso sugere uma adoção cada vez mais diversificada da nuvem.

► **Quais provedores de IaaS de nuvem você usa atualmente ou planeja usar no futuro? (selecione tudo que se aplica)**



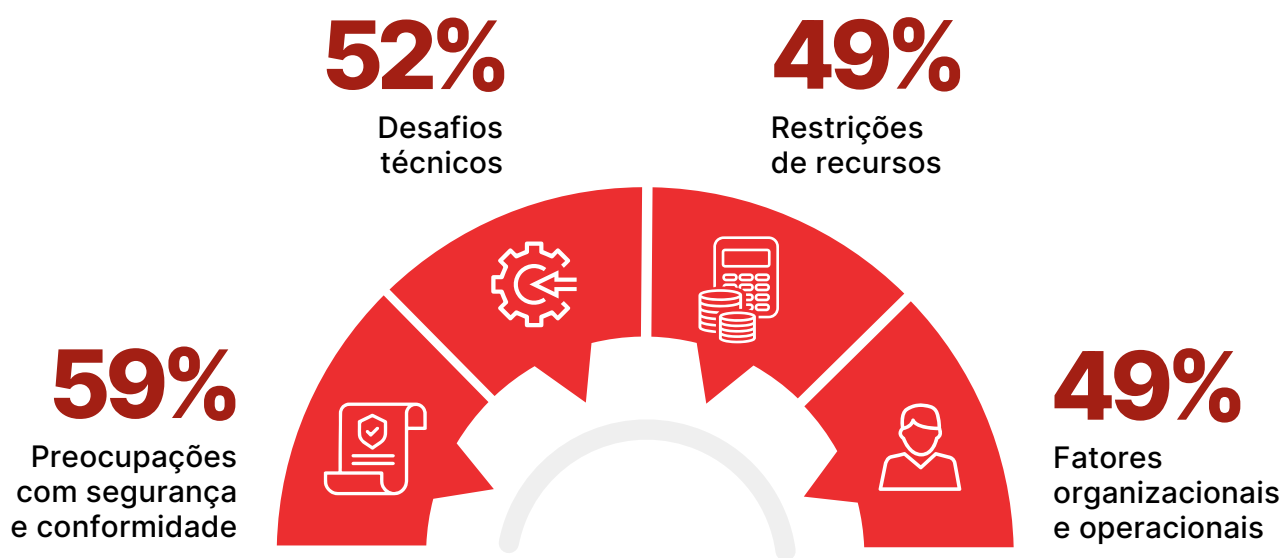
Navegando Pelas Barreiras de Adoção da Nuvem

Identificar e compreender as barreiras para uma adoção mais rápida e generalizada da nuvem é essencial para que as organizações possam navegar melhor pelas complexidades da transição para soluções baseadas na nuvem.

As preocupações com segurança e conformidade estão na vanguarda, com 59% dos entrevistados identificando-as como a principal barreira. Isso destaca a importância de garantir que a segurança e a conformidade sejam um elemento integral da adoção da nuvem. Os desafios técnicos vêm logo em seguida, com 52%, destacando que a facilidade de adoção da nuvem não está isenta de desafios.

49% dos entrevistados citam restrições de recursos, incluindo a falta de experiência da equipe e limitações orçamentárias, ressaltando a necessidade de investimento adequado em recursos humanos e financeiros para apoiar as iniciativas de nuvem. As barreiras organizacionais e operacionais (49%) destacam que a computação em nuvem não é apenas uma nova tecnologia, mas também um novo modelo operacional que oferece métodos de trabalho inovadores e exige a adesão da gerência para lidar com a possível resistência à mudança.

► Quais são as principais barreiras à adoção da nuvem na sua organização? (selecione tudo que se aplica)



Outras respostas incluem:

Preocupações com o serviço de nuvem 28% | Questões e legalidades relacionadas ao provedor 27%

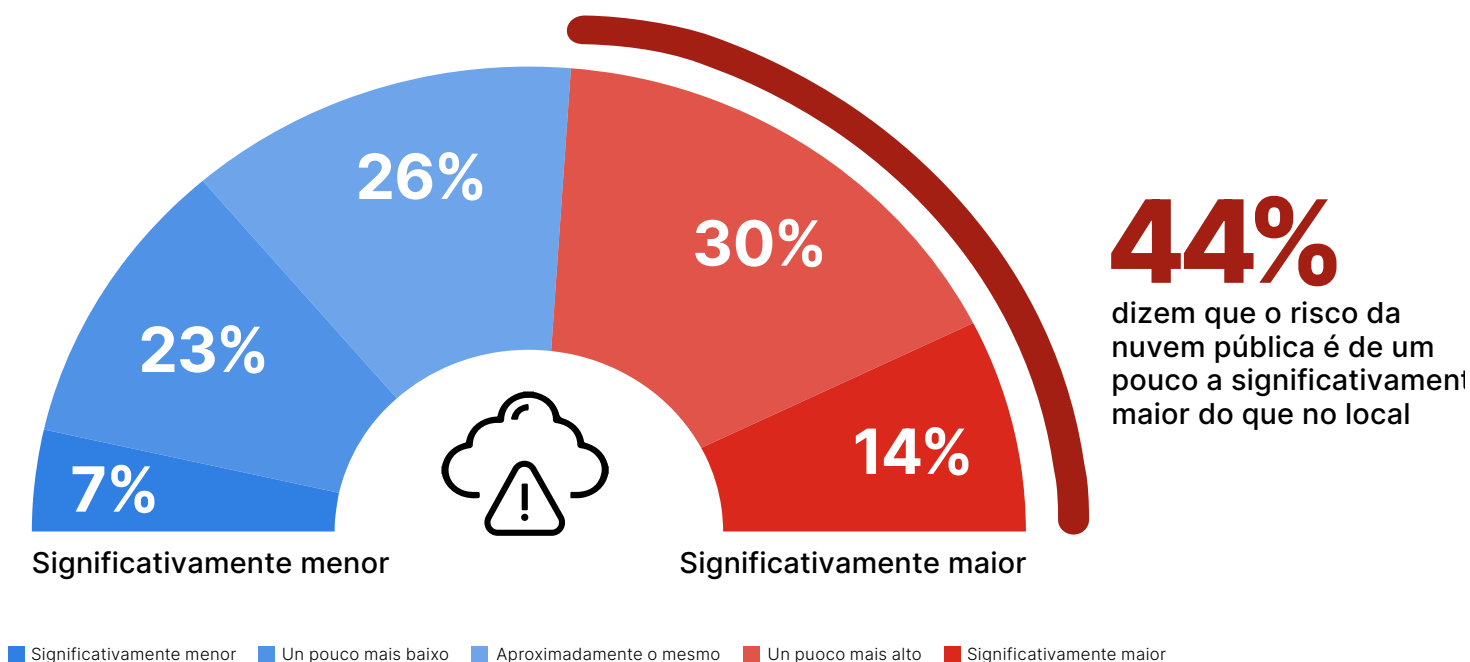
Percepções dos Riscos de Segurança na Nuvem

A avaliação do risco de violações de segurança em ambientes de nuvem pública revela preocupações significativas sobre os riscos e os desafios de segurança exclusivos associados à computação em nuvem, em comparação com os ambientes locais.

Um total de 44% dos entrevistados considera o risco de violações de segurança em ambientes de nuvem pública maior do que em ambientes de TI tradicionais no local, sendo que 30% o consideram um pouco maior e 14% o consideram significativamente maior.

Por outro lado, 30% dos participantes consideram o risco menor em ambientes de nuvem pública, indicando confiança nas medidas e nos avanços de segurança dos provedores de nuvem. Um número notável de 26% dos entrevistados acredita que o risco permanece o mesmo, sugerindo que, embora a nuvem introduza novas dinâmicas, os desafios fundamentais de segurança.

► Em comparação com os ambientes de TI tradicionais e locais, você diria que o risco de violações de segurança em um ambiente de nuvem pública é maior ou menor?



A nuvem pública oferece às organizações a oportunidade de adotar uma abordagem proativa e automatizada à segurança. A adoção de uma mentalidade de segurança desde a concepção oferece às organizações a capacidade de atenuar os riscos de forma eficaz e capitalizar a escalabilidade, a flexibilidade e a inovação que a nuvem oferece.

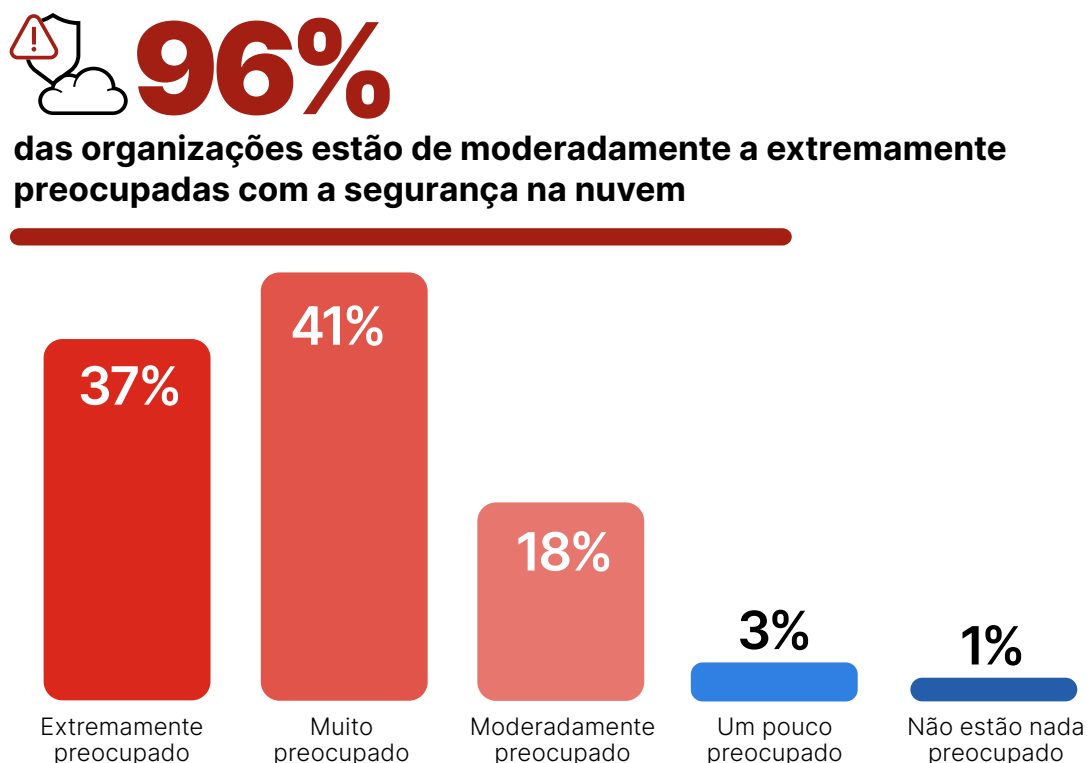
Preocupações com a Segurança da Nuvem

O nível de preocupação em relação à segurança da nuvem pública é um indicador essencial da percepção e da prontidão da comunidade de segurança cibernética para lidar com possíveis riscos e ameaças.

Apesar da crescente adoção da nuvem, as preocupações com a segurança da nuvem não mostram sinais de melhora: uma maioria significativa de 96% expressa altos níveis de preocupação, com 37% extremamente preocupados e 41% muito preocupados com a segurança da nuvem pública. O alto grau de preocupação com a segurança cibernética, que tem se mantido consistente ao longo dos anos, atua como uma barreira significativa para a adoção mais rápida da nuvem, à medida que as organizações enfrentam os riscos percebidos e as complexidades de proteger os ambientes de nuvem. Apenas uma pequena fração (22%) relata preocupação moderada ou nenhuma, indicando um forte consenso sobre a importância de medidas de segurança robustas em implementações de nuvem pública.

Esses dados estão alinhados com a descoberta anterior, em que 44% dos entrevistados perceberam um risco maior de violações de segurança em nuvens públicas em comparação com ambientes tradicionais no local. Isso reforça que, embora a computação em nuvem ofereça inúmeros benefícios e esteja crescendo rapidamente, a segurança continua sendo uma preocupação fundamental.

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



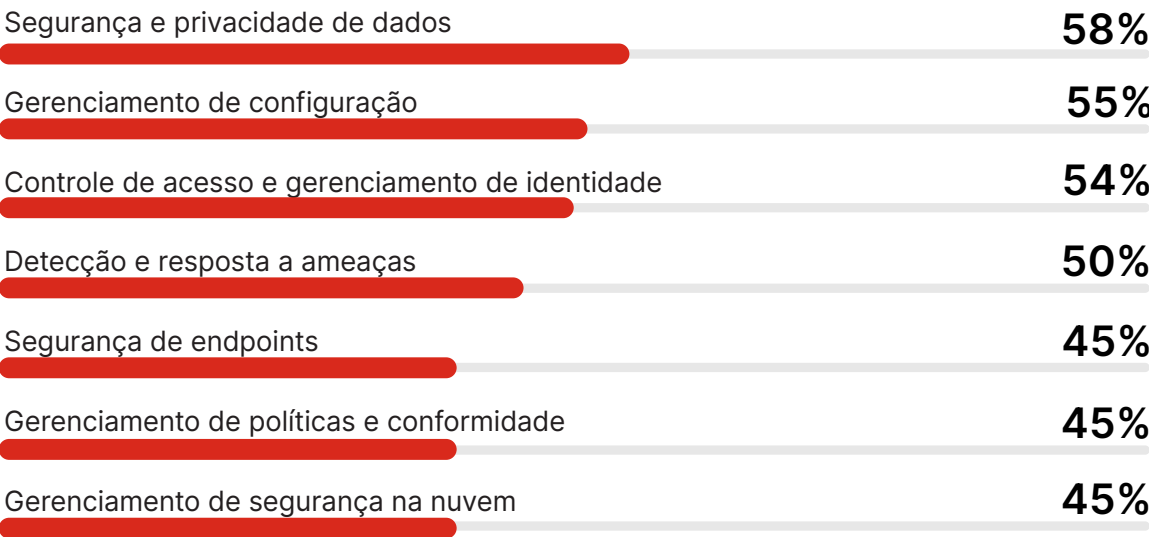
Para lidar com essas preocupações, as organizações devem não apenas manter uma abordagem de segurança desde a concepção, mas também investir em monitoramento contínuo, inteligência contra ameaças e recursos de resposta a incidentes específicos para ambientes de nuvem. A adoção de soluções de segurança de ponta e a promoção de colaborações sólidas com os provedores de nuvem podem ajudar a reduzir o risco percebido e as preocupações associadas à nuvem pública, garantindo uma infraestrutura de nuvem segura e resiliente.

Desafios das Operações de Segurança na Nuvem

O gerenciamento das operações diárias de segurança na nuvem representa um desafio multifacetado para as organizações, exigindo um equilíbrio delicado entre fatores tecnológicos, processuais e humanos. A segurança e a privacidade dos dados surgem como a principal preocupação, com 58% dos entrevistados destacando a importância fundamental de proteger informações confidenciais e evitar vazamentos de dados na nuvem. Isso ressalta a importância de práticas robustas de governança e criptografia de dados. O gerenciamento de configuração está em segundo lugar, com 55%, refletindo a complexidade e os possíveis riscos associados às configurações de nuvem, pois uma única configuração incorreta pode expor as organizações a riscos de segurança significativos.

O controle de acesso e o gerenciamento de identidade é outro grande desafio, citado por 54% dos participantes, enfatizando a necessidade de um controle rigoroso sobre o acesso e os privilégios dos usuários para evitar o acesso não autorizado. A detecção e a resposta a ameaças (50%) e a segurança de endpoints (45%) indicam ainda mais a luta contínua para identificar e atenuar as ameaças à segurança em tempo real e proteger a infinidade de dispositivos que acessam os serviços em nuvem. O gerenciamento de políticas e conformidade (45%) e o gerenciamento de segurança na nuvem (45%) destacam as dificuldades em garantir políticas de segurança consistentes em todos os ambientes e alinhar os recursos de segurança na nuvem com as soluções locais.

► **Quais são seus principais desafios no gerenciamento das operações diárias de segurança na nuvem?**
(selecione todas as opções aplicáveis)



Para enfrentar esses desafios nas operações de segurança na nuvem, as organizações devem priorizar uma estratégia de segurança unificada que aproveite a automação, a análise avançada e as plataformas de segurança integradas para simplificar a segurança dos dados, a aplicação de políticas, o gerenciamento de acesso e a detecção e resposta a ameaças. Enfatizar o desenvolvimento de habilidades de segurança nativas da nuvem nas equipes e promover uma cultura de conscientização sobre a segurança pode aumentar ainda mais a capacidade da organização de gerenciar com eficácia as operações de segurança na nuvem.

Outras respostas incluem:
Shadow IT e uso não autorizado de aplicativos 36% | Integração e automação da nuvem 35% | Agilidade e complexidade operacional 32% | Alocação de recursos 30% | Práticas de DevSecOps 28%

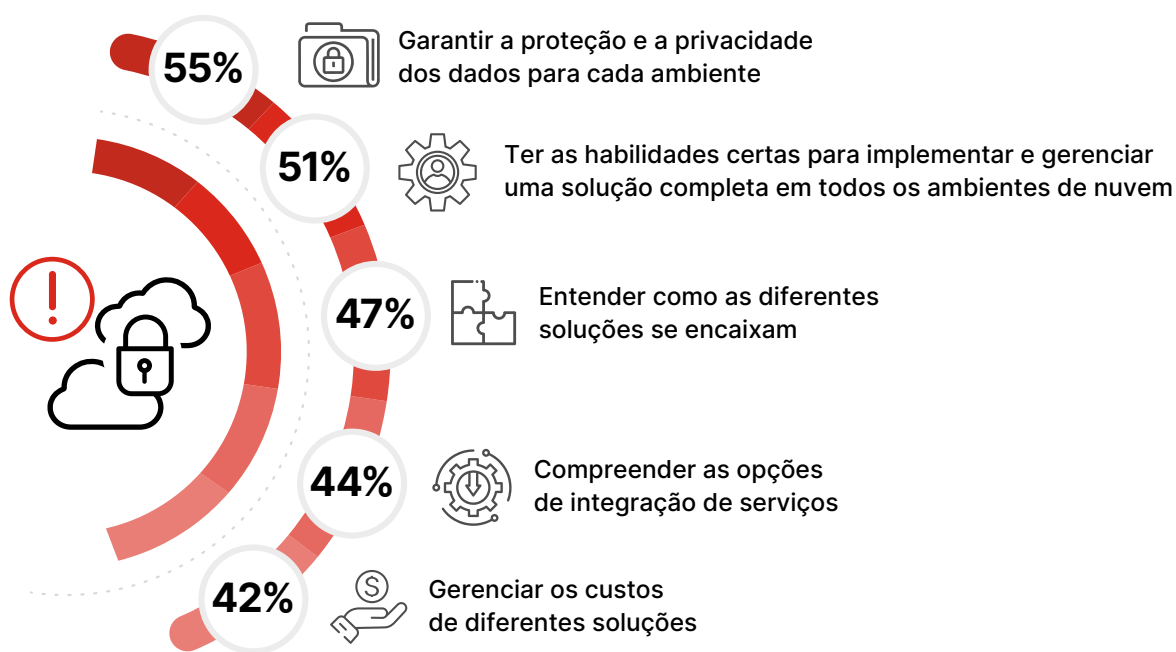
Desafios de Segurança em Multinuvem

Os ambientes de várias nuvens aumentam significativamente a complexidade e os desafios de proteger as cargas de trabalho na nuvem. Garantir a proteção e a privacidade dos dados em cada ambiente é identificado como o desafio de segurança multicloud mais significativo, com 55% dos entrevistados destacando-o como uma preocupação. Isso se alinha com a ênfase anterior na segurança e na privacidade dos dados como questões operacionais críticas, ressaltando a maior complexidade quando os dados estão dispersos em vários ambientes de nuvem.

Ter as habilidades certas para implantar e gerenciar soluções em todos os ambientes de nuvem é um grande desafio para 51% dos participantes, ecoando a necessidade observada anteriormente de especialização em segurança nativa da nuvem para navegar com eficiência no cenário multifacetado de segurança na nuvem. Entender como as diferentes soluções se encaixam e compreender as opções de integração de serviços são desafios críticos para 47% e 44% dos entrevistados, respectivamente.

Essas preocupações destacam as complexidades de se obter integração e interoperabilidade perfeitas entre diversos ambientes de nuvem, um fator crucial para manter a segurança robusta e a eficiência operacional. O desafio de gerenciar os custos de diferentes soluções, citado por 42% dos entrevistados, reflete ainda mais o equilíbrio operacional e financeiro necessário em uma estratégia de várias nuvens.

► Quais são seus maiores desafios para proteger ambientes multinuvem? (selecione tudo que se aplica)



Para enfrentar esses desafios de forma eficaz, as organizações devem utilizar soluções de segurança integradas que ofereçam visibilidade e controle em ambientes multinuvem, apoiando padrões consistentes de proteção de dados e privacidade. Enfatizar as parcerias com fornecedores que oferecem recursos abrangentes de segurança em várias nuvens e promover o desenvolvimento de habilidades pode capacitar as empresas a superar a complexidade da proteção de arquiteturas em várias nuvens. Essa abordagem não apenas atenua os desafios identificados, mas também aproveita todo o potencial dos ambientes multinuvem para aumentar a agilidade, o dimensionamento e a inovação.

Outras respostas incluem:

Fornecer acesso contínuo aos usuários com base em suas credenciais 38% | Perda de visibilidade e controle 37% | Selecionar o conjunto certo de serviços 36% Acompanhar a taxa de mudança 33%

Brecha de Talentos em Segurança Cibernética

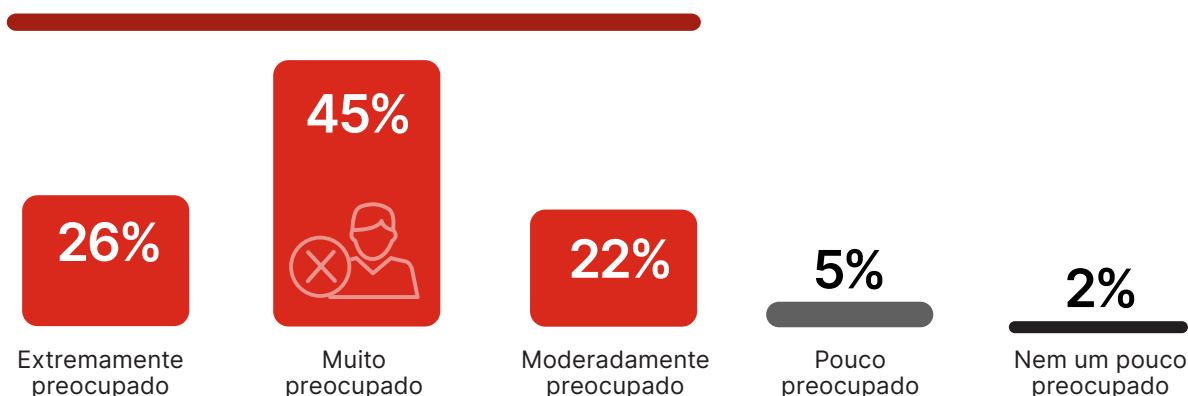
Assim como os desafios destacados na proteção de ambientes com várias nuvens, a escassez contínua de profissionais qualificados capazes de proteger ambientes complexos com várias nuvens se destaca como um problema crítico e contínuo do setor.

Um número impressionante de 93% dos entrevistados expressou preocupação com a escassez de profissionais qualificados em segurança cibernética em todo o setor. Essa apreensão considerável reflete a consciência aguda da lacuna entre a crescente demanda por talentos qualificados em segurança cibernética e a força de trabalho disponível, uma lacuna que exacerba as vulnerabilidades de segurança e os desafios operacionais em um cenário cibernético cada vez mais complexo.

► Qual é o seu grau de preocupação com a escassez de habilidades de profissionais qualificados em segurança cibernética em todo o setor?

93%

das organizações estão de moderadamente a extremamente preocupadas com a escassez de habilidades de profissionais qualificados em segurança cibernética em todo o setor



Um número significativo de 74% dos entrevistados confirma que sua organização está enfrentando atualmente uma escassez de talentos em segurança cibernética. Essa constatação quantifica a extensão em que a escassez de habilidades está afetando as operações diárias de segurança e as iniciativas estratégicas das organizações.

► Sua organização está enfrentando uma escassez de talentos em segurança cibernética?



Para atenuar o impacto da perene escassez de habilidades em segurança cibernética, as organizações devem considerar uma abordagem multifacetada que inclua o fomento de parcerias com instituições acadêmicas para canalizar novos talentos e investir em programas de treinamento e desenvolvimento para cultivar talentos internos e se adaptar às demandas em evolução da segurança na nuvem. As organizações também devem considerar a adoção de soluções de segurança unificadas que substituam as soluções de vários pontos, incorporando inteligência artificial e reduzindo a complexidade operacional para preencher a lacuna de habilidades e, ao mesmo tempo, aprimorar a detecção de ameaças, os recursos de resposta e a postura geral de segurança.

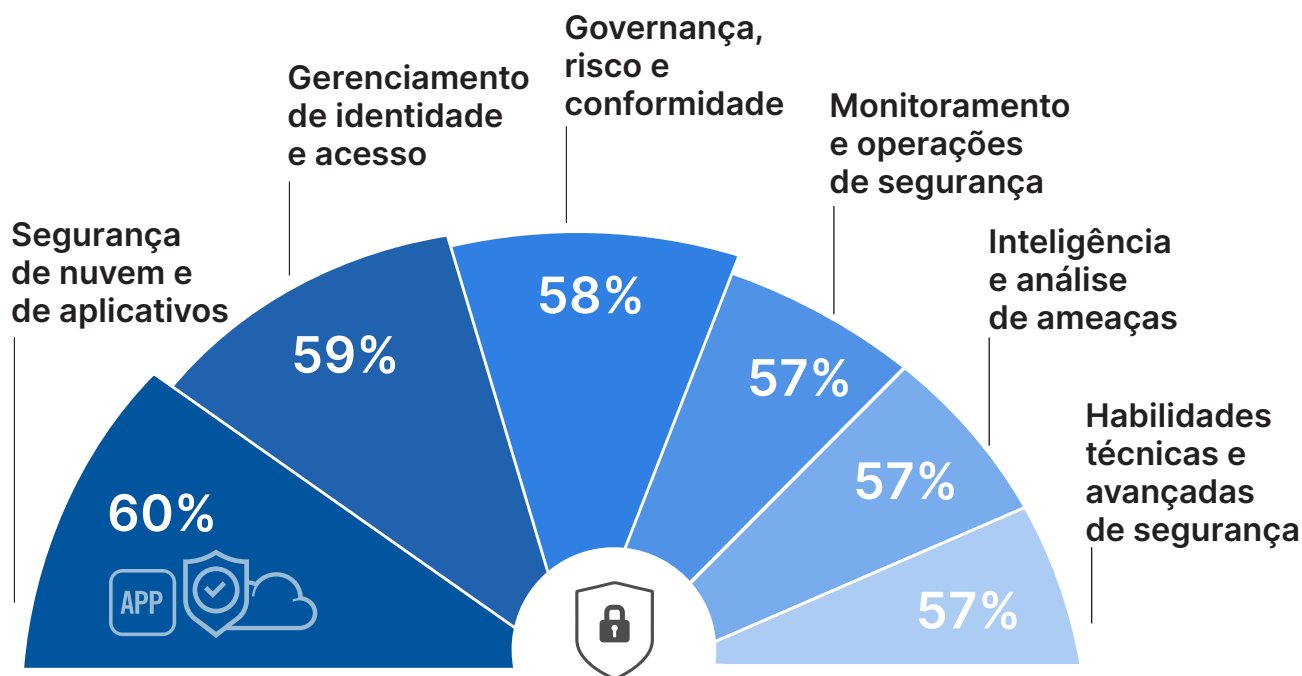
Habilidades Críticas de Segurança Cibernética

No contexto da acentuada escassez de talentos em segurança cibernética enfrentada pelas organizações, perguntamos sobre as habilidades específicas de segurança cibernética consideradas mais importantes para enfrentar os desafios de segurança atuais.

As habilidades de segurança de aplicativos e nuvem ocupam o primeiro lugar, com 60% dos entrevistados destacando sua importância crítica. Isso ressalta a migração acelerada para serviços em nuvem e a necessidade de práticas de segurança robustas no desenvolvimento e na implantação de aplicativos. Em seguida, o gerenciamento de identidade e acesso (IAM) é identificado por 59% das organizações como essencial, refletindo a crescente complexidade de proteger o acesso do usuário em ambientes de TI cada vez mais distribuídos.

A governança, o risco e a conformidade (GRC) são reconhecidos por 58% dos entrevistados como uma habilidade importante, ressaltando a função essencial das estruturas de conformidade regulamentar e de gerenciamento de riscos no atual cenário de ameaças cibernéticas. O monitoramento e as operações de segurança, a inteligência contra ameaças e as habilidades técnicas avançadas de segurança - todos com 57% - demonstram uma ênfase quase igual na detecção proativa de ameaças, na compreensão dos adversários cibernéticos e no aproveitamento de tecnologias avançadas para uma postura de segurança robusta.

► Quais são as habilidades de segurança mais importantes exigidas em sua organização? (selecione todas as que se aplicam)



Outras respostas incluem:

Resposta a incidentes e perícia 55% | Comunicação e estratégia 39% | Treinamento e conscientização 38%

Tendências Orçamentárias da Segurança na Nuvem

A alocação de recursos para a segurança na nuvem é um indicador crítico das prioridades organizacionais e da importância percebida da proteção da infraestrutura de nuvem diante da evolução das ameaças cibernéticas e dos avanços tecnológicos.

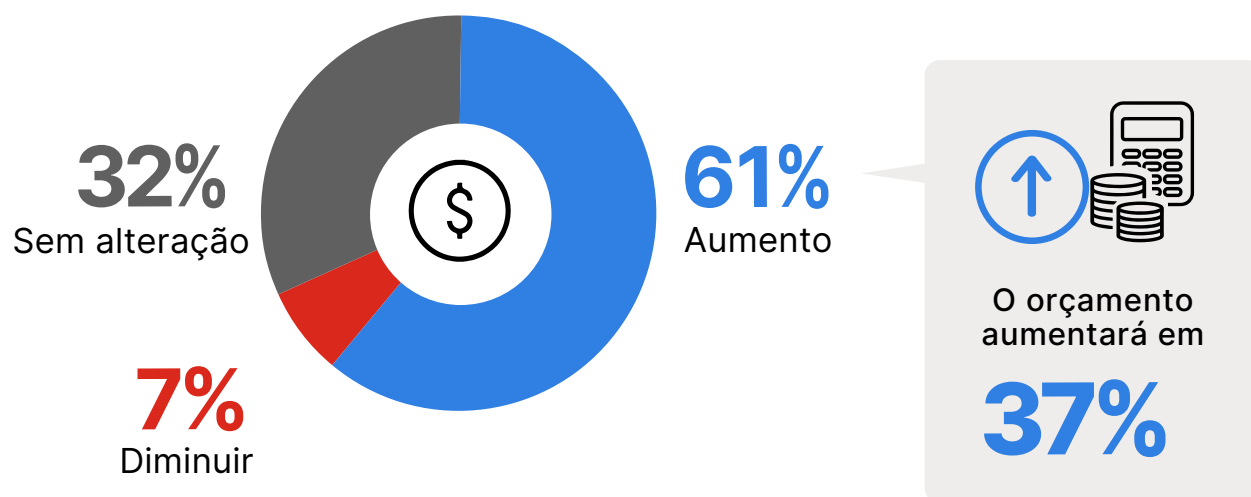
Um número significativo de 61% dos entrevistados prevê um aumento em seu orçamento de segurança na nuvem nos próximos 12 meses.

Essa maioria substancial indica um forte reconhecimento dos crescentes desafios de segurança cibernética e a necessidade de aprimorar as medidas de segurança em ambientes de nuvem, o que levou o orçamento de segurança na nuvem a aumentar em 37%.

A disposição de investir até 37% a mais em segurança na nuvem reflete a percepção de que mecanismos de defesa robustos são essenciais para proteger dados confidenciais e manter a conformidade com os padrões regulatórios em um cenário de negócios cada vez mais centrado na nuvem.

Enquanto isso, um terço das organizações (32%) espera que seu orçamento de segurança na nuvem permaneça inalterado. Apenas uma pequena fração, 7%, projeta uma redução em seu orçamento de segurança na nuvem.

► Como seu orçamento de segurança na nuvem está mudando nos próximos 12 meses?

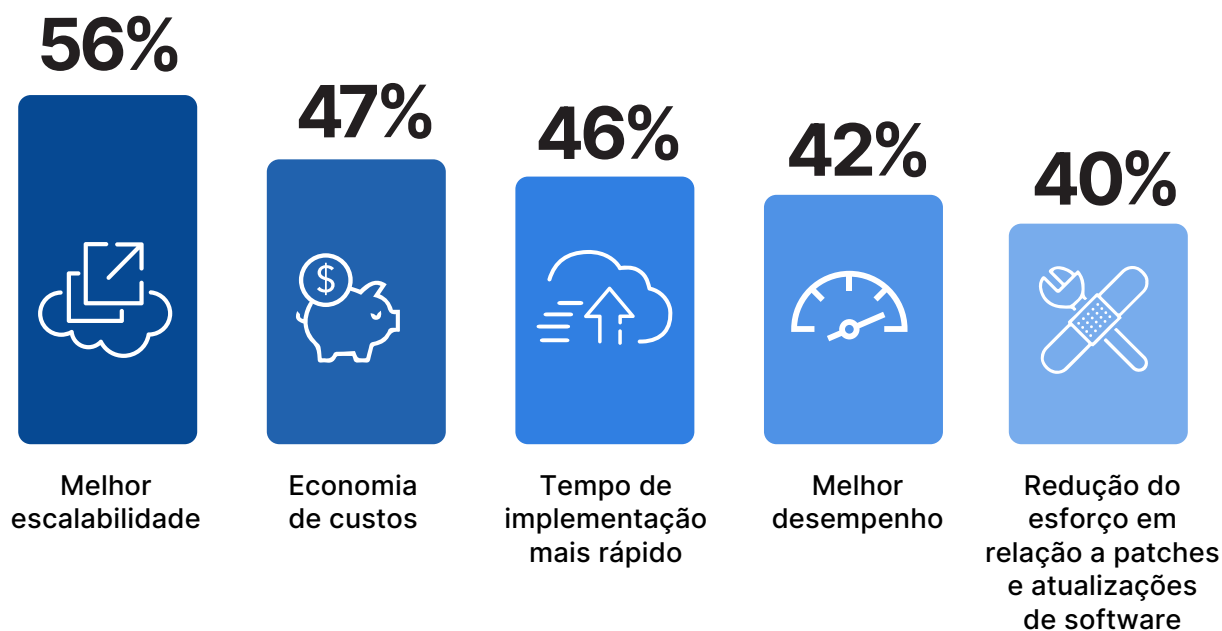


Dada a tendência predominante de aumento do investimento em segurança na nuvem, as organizações devem alocar estrategicamente recursos adicionais para áreas de maior risco e impacto potencial, como detecção avançada de ameaças, gerenciamento de identidade e acesso e automação da segurança. Essa abordagem não apenas prepara as empresas para combater ameaças cibernéticas sofisticadas, mas também aprimora sua postura geral de segurança, aproveitando as mais recentes inovações tecnológicas em segurança na nuvem.

Adotando Soluções de Segurança Baseadas na Nuvem

A decisão de adotar soluções de segurança baseadas na nuvem é motivada por uma série de fatores que se alinham às metas organizacionais de agilidade, eficiência e proteção aprimorada. A necessidade de melhor escalabilidade, reconhecida por 56% dos participantes da pesquisa, destaca a capacidade da nuvem de se ajustar dinamicamente às demandas flutuantes. Logo atrás, a economia de custos e a implementação mais rápida, com 47% e 46%, respectivamente, destacam os benefícios econômicos e operacionais que atraem as organizações para as soluções de segurança em nuvem. O desempenho aprimorado (42%) e a redução dos esforços manuais para aplicação de patches e atualizações de software (40%) catalisam ainda mais a mudança para as soluções de segurança baseadas na nuvem, especialmente à luz da perene escassez de habilidades em segurança cibernética.

► Quais são os principais motivadores para considerar soluções de segurança baseadas em nuvem? (selecione tudo que se aplica)



As organizações que consideram soluções de segurança baseadas na nuvem devem priorizar a escalabilidade, a eficiência de custos e a rápida implementação para capitalizar as vantagens operacionais e econômicas da nuvem. Concentrar-se em soluções que ofereçam gerenciamento simplificado de políticas e conformidade contínua pode melhorar ainda mais as posturas de segurança, garantindo a resiliência diante da evolução das ameaças e dos cenários normativos.

Outras respostas incluem:

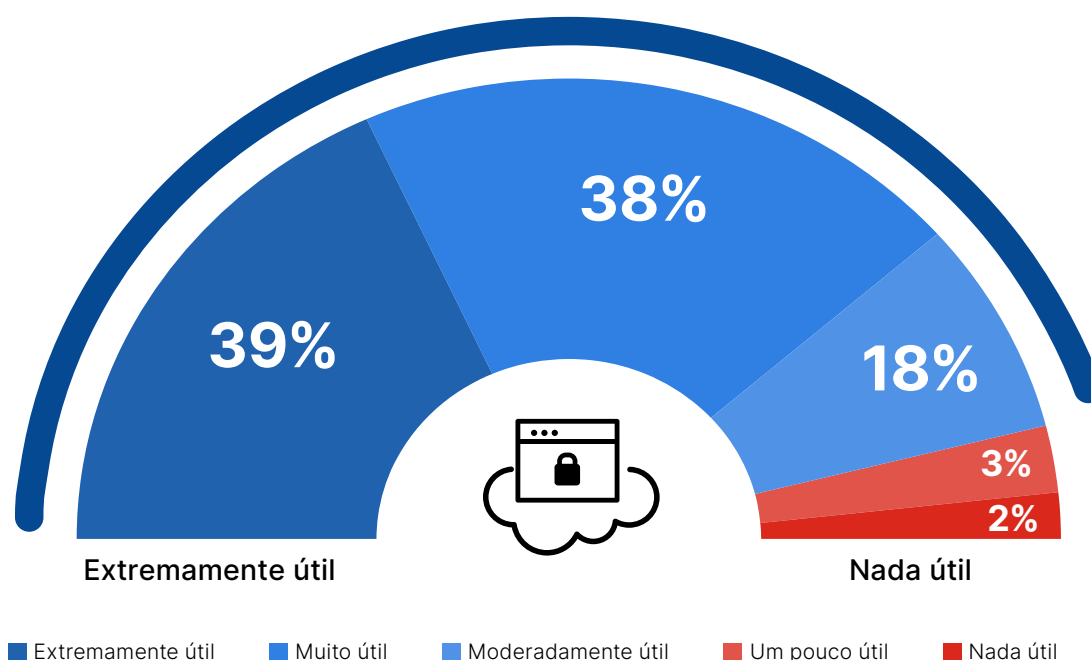
Gerenciamento de políticas mais fácil 39% | Melhor tempo de atividade 38% | Atender às expectativas de conformidade com a nuvem 34% | Melhor visibilidade da atividade do usuário e do comportamento do sistema 33% | Necessidade de acesso seguro ao aplicativo de qualquer local 32% | Nossos dados/cargas de trabalho residem na nuvem 28% | Redução do espaço ocupado pelo dispositivo nas filiais 27%

Plataforma Unificada de Segurança na Nuvem

Considerando a complexidade, as dores de cabeça operacionais e os desafios de habilidades já destacados, não é nenhuma surpresa que as organizações estejam procurando uma plataforma de segurança unificada para simplificar e consolidar o gerenciamento de segurança em diversos ambientes de nuvem. Um número esmagador de 95% dos entrevistados confirma que ter uma plataforma desse tipo seria vantajoso para proteger os dados de forma consistente e abrangente em toda a área de cobertura da nuvem.

- **Quão útil seria ter uma única plataforma de segurança na nuvem 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 da nuvem?**

95% dos profissionais consideram o uso de uma única plataforma de segurança na nuvem com um único painel de controle de moderada a extremamente útil



Essa demanda por uma plataforma de segurança em nuvem única e integrada reflete a mudança do setor para a consolidação da plataforma, impulsionada pela melhoria da eficácia da segurança, integração mais simples e redução da sobrecarga de gerenciamento. Essa é a única abordagem eficaz para lidar com a lacuna de talentos em segurança cibernética e mitigar ataques cada vez mais sofisticados e automatizados. Essa plataforma unificada alivia o ônus operacional de navegar por várias interfaces de segurança e aprimora a postura geral de segurança por meio da aplicação consistente de políticas e da visibilidade abrangente em todos os ambientes de nuvem.

Adotando a Nuvem com Segurança: Estratégias Essenciais de Segurança na Nuvem

No atual cenário de nuvem em rápida evolução, a adoção de uma postura robusta de segurança na nuvem é imperativa para organizações de todos os tamanhos. Este guia descreve as práticas recomendadas essenciais para proteger seus ambientes de nuvem, desde a unificação de plataformas de segurança até o investimento em habilidades especializadas, projetadas para proteger contra as ameaças sofisticadas do futuro.



ADOTE UMA PLATAFORMA DE SEGURANÇA UNIFICADA:

Centralize o controle de segurança e a visibilidade em todos os ambientes de nuvem para agilizar as operações e aumentar a visibilidade, uma estratégia preferida por 95% das organizações.



ENFATIZE A SEGURANÇA AGNÓSTICA DA NUVEM:

Com 78% usando ambientes híbridos ou multinuvem, é crucial desenvolver estratégias que abordem os desafios únicos desses ambientes e garantam políticas e aplicação de segurança consistentes.



AUTOMATIZE A GESTÃO DE POLÍTICAS E CONFORMIDADE:

Implemente sistemas para automatizar e simplificar políticas de segurança em ambientes de nuvem e atender consistentemente aos requisitos regulatórios.



PRIORIZAR A PROTEÇÃO DE DADOS:

Implemente governança e criptografia robustas de dados para proteger informações confidenciais em todos os serviços em nuvem, enfrentando o desafio de segurança mencionado por 58% das organizações.



MELHORE O GERENCIAMENTO DE CONFIGURAÇÃO:

Gerencie ativamente as configurações da nuvem para evitar configurações incorretas e reduzir a exposição a vulnerabilidades de segurança.



FORTALECER O CONTROLE DE ACESSO:

Empregue um gerenciamento rigoroso de identidade e acesso para implementar os princípios de Zero Trust e reduzir o risco de acesso não autorizado.



AUMENTE A DETECÇÃO E RESPOSTA DE AMEAÇAS:

Aproveite análises avançadas e recursos de resposta automatizada para identificar e mitigar ameaças em tempo real.



INVISTA EM HABILIDADES DE SEGURANÇA NATIVAS DA NUVEM:

Com 93% expressando grande preocupação com a escassez de habilidades em segurança cibernética, promova o desenvolvimento de experiência em segurança específica da nuvem dentro de sua equipe para navegar com mais eficiência no complexo cenário de segurança na nuvem.

Metodologia e Dados Demográficos

O Relatório sobre Segurança na Nuvem de 2024 baseia-se em uma pesquisa global abrangente com 927 profissionais de segurança cibernética, realizada em fevereiro de 2024, para descobrir como as organizações usuárias da nuvem estão adotando a nuvem, como elas veem a evolução da segurança na nuvem e quais práticas recomendadas os líderes de segurança cibernética de TI estão priorizando em sua migração para a nuvem. Os entrevistados variam de executivos técnicos a profissionais de segurança de TI, representando uma seção transversal equilibrada de organizações de tamanhos variados em vários setores.

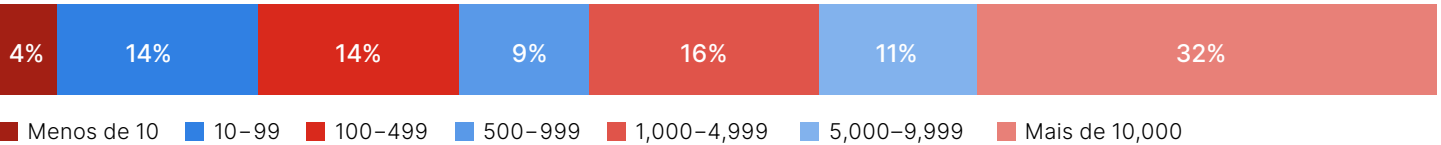
NÍVEL DE CARREIRA



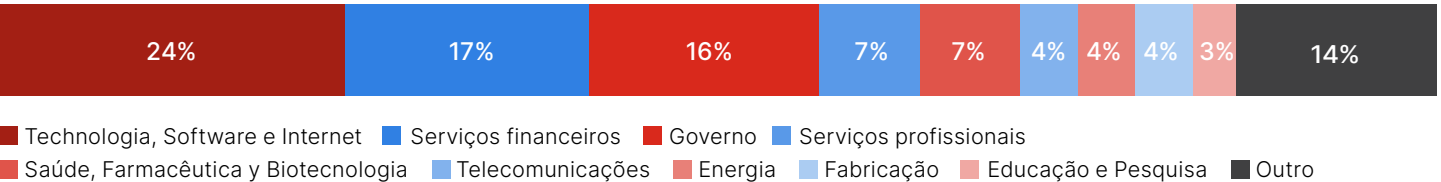
DEPARTAMENTO



TAMANHO DA EMPRESA



INDÚSTRIA



Reutilização de conteúdo

Incentivamos a reutilização de dados, gráficos e textos publicados neste relatório de acordo com os termos desta [Licença Internacional Creative Commons Attribution 4.0](#). Você é livre para compartilhar e fazer uso comercial deste trabalho, desde que atribua o relatório de acordo com os termos da licença. Por exemplo: “2024 Cloud Security Report by Cybersecurity Insiders and Fortinet”.



A Fortinet (NASDAQ: FTNT) protege as maiores empresas, provedores de serviços e organizações governamentais em todo o mundo. A Fortinet oferece aos seus clientes visibilidade e controle completos em todo o mundo. A plataforma Fortinet Security Fabric é capaz de atender aos requisitos de desempenho cada vez maiores, agora e no 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 ambientes de rede, aplicativos, multinuvem ou de borda. A Fortinet está classificada em primeiro lugar como a empresa com maior número de dispositivos de segurança enviados em todo o mundo e mais de 730.000 clientes que confiam na Fortinet para proteger seus negócios.

www.fortinet.com

Cybersecurity

I N S I D E R S

O Cybersecurity Insiders reúne mais de 600.000 profissionais de segurança cibernética e fornecedores de tecnologia de classe mundial para facilitar a solução inteligente de problemas e a colaboração para enfrentar os desafios de segurança cibernética mais críticos da atualidade.

Nosso foco está na criação e seleção de conteúdo exclusivo que educa e informa os profissionais de segurança cibernética sobre as últimas notícias, tendências, soluções e práticas recomendadas de segurança cibernética. Desde estudos de pesquisa aprofundados.

e análises imparciais de produtos a guias eletrônicos práticos, webinars envolventes e artigos educacionais - temos o compromisso de fornecer recursos que ofereçam respostas baseadas em evidências para os complexos desafios atuais de segurança cibernética.

Entre em contato conosco hoje mesmo para saber como a Cybersecurity Insiders pode ajudá-lo a se destacar em um mercado concorrido e impulsionar a demanda, a visibilidade da marca e a presença da liderança de pensamento.

Envie-nos um e-mail para info@cybersecurity-insiders.com
ou acesse cybersecurity-insiders.com