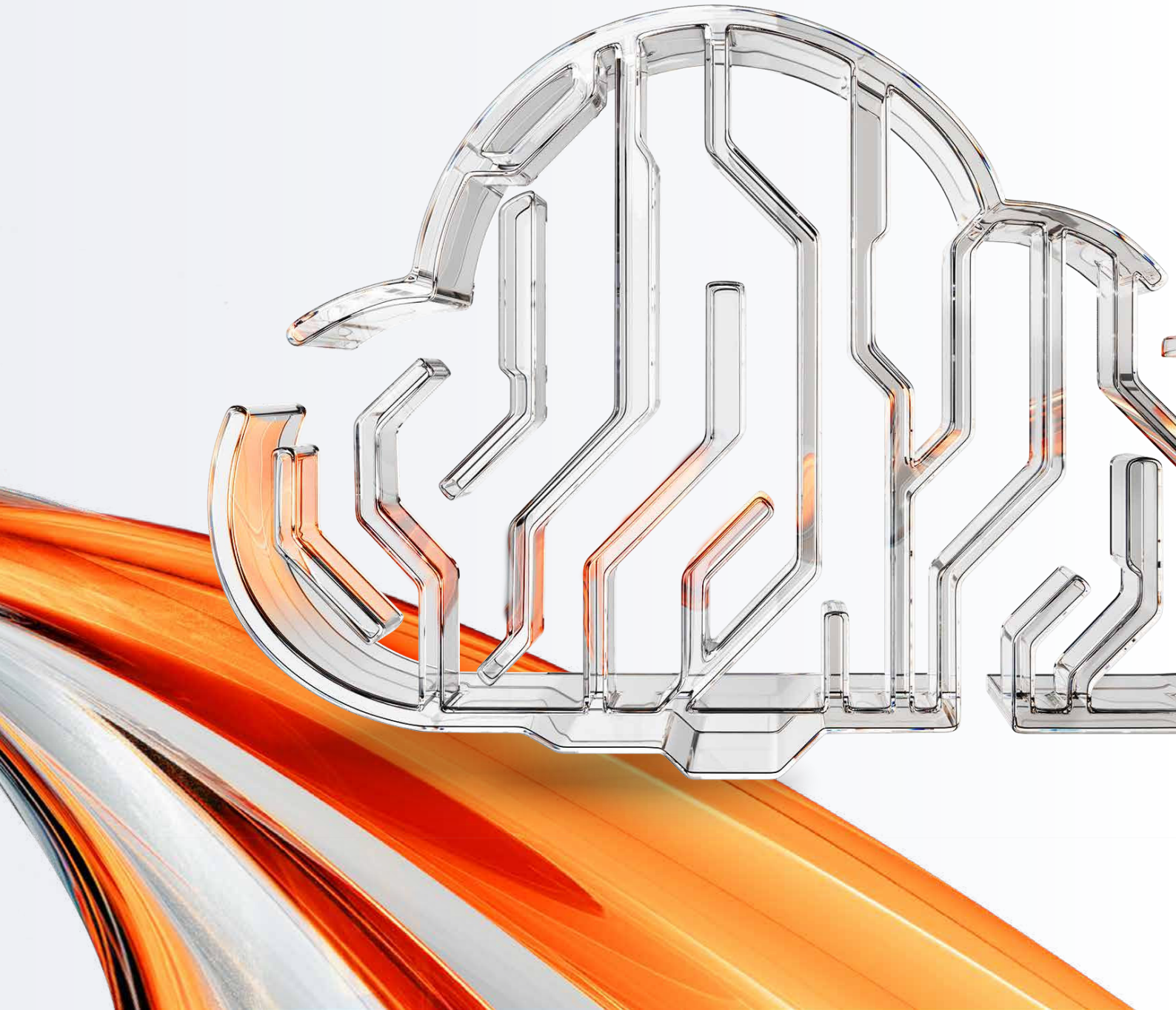
tenable | Relatório da pesquisa

O estado da segurança de IA e nuvem 2025



Agradecimentos

Autora principal

Hillary Baron

Colaboradores

Marina Bregkou
Josh Buker
Ryan Gifford
Alex Kaluza
John Yeoh

Design gráfico

Claire Lehnert
Stephen Lumpe

Sobre o patrocinador

A Tenable® é a empresa de Exposure Management, que oferece soluções de gerenciamento de exposição ao risco cibernético para descobrir e eliminar as lacunas de segurança cibernética que desgastam o valor, a reputação e a confiança de nossos clientes. A plataforma empresarial de gerenciamento de exposição com tecnologia de IA da Tenable unifica totalmente a visibilidade da segurança, as informações e a tomada de decisões para a superfície de ataque. Dessa forma, as organizações modernas podem se proteger contra qualquer tipo de ataque cibernético a diferentes ambientes, como a nuvem, a infraestrutura crítica ou a TI, entre outros. Ao proteger as empresas contra exposição da segurança, a Tenable reduz o risco de negócio para mais de 44 mil clientes em todo o mundo. Saiba mais em pt-br.tenable.com.

pt-br.tenable.com

Índice

Resumo executivo

As arquiteturas híbridas e multinuvem tornaram-se o padrão para a maioria das organizações; 82% operam ambientes híbridos e 63% usam vários provedores de nuvem. Ao mesmo tempo, a adoção da IA está acelerando; mais da metade das organizações implementam a IA para atender às necessidades de negócios, e 34% das organizações com workloads de IA já sofreram violações. No entanto, as estratégias de segurança não acompanham o ritmo, deixando as equipes reativas e fragmentadas.

Esta pesquisa mostra seis insights críticos:

1. Ambientes híbridos e multinuvem dominam:
A infraestrutura flexível exige visibilidade de segurança unificada e aplicação de políticas, o que ainda não existe para a maioria.

2. Riscos de identidade lideram, mas permanecem mal gerenciados:
A identidade é agora a principal causa de riscos e violações, mas muitas organizações dependem de métricas e controles básicos, deixando passar lacunas mais profundas na governança.

3. A lacuna de conhecimento impede o progresso:
Conhecimentos limitados sobre segurança da nuvem prejudicam o alinhamento da equipe de liderança, a estratégia e o investimento.

4. Medição de violações, sem prevenção:
Os KPIs permanecem reativos, com foco em incidentes em vez de redução de riscos e resiliência.

5. A adoção da IA supera a prontidão da segurança:
As organizações priorizam a conformidade e os novos riscos de IA aos controles comprovados de nuvem e identidade.

6. A liderança deve redefinir a estratégia:
Suposições desatualizadas e baixos investimentos deixam as equipes de segurança sem o suporte estrutural para amadurecer.

Para abordar essas lacunas, as organizações devem:

- Criar visibilidade e controles integrados em infraestruturas híbridas e multinuvem;
- Amadurecer a governança de identidade para identidades humanas e não humanas;
- Concentrar os KPIs na prevenção e na resiliência;
- Melhorar o entendimento da liderança sobre as verdadeiras necessidades operacionais;
- Tratar a conformidade, e não o endpoint, como uma linha de base para a segurança de IA.

A maturidade da segurança depende do alinhamento estratégico e do planejamento orientado por riscos. As organizações que vão além de soluções e produtos individuais e operações reativas estarão mais bem equipadas para proteger ambientes de nuvem e IA em evolução.

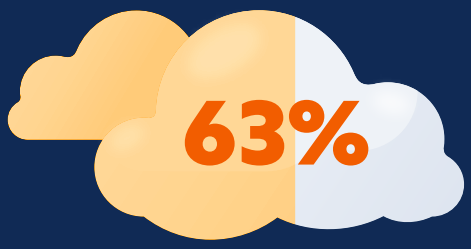
Principais descobertas

A nuvem e a IA não são mais tendências emergentes; estão incorporadas à maneira como as organizações atuam, com arquiteturas híbridas e multinuvem que proporcionam flexibilidade e com a IA passando rapidamente de projetos-piloto para workloads críticas ao negócio. No entanto, embora a adoção tenha aumentado, as estratégias de segurança têm dificuldades para acompanhar o ritmo. As descobertas mostram uma clara lacuna entre conscientização e execução: embora a maioria das organizações reconheça onde estão seus riscos, muitas permanecem reativas, fragmentadas e desalinhadas.

Principal descoberta 1:
Ambientes híbridos e multinuvem dominam

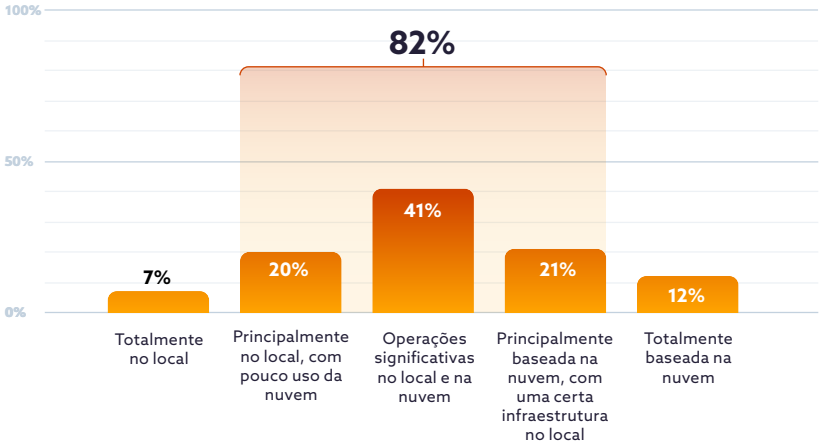
As arquiteturas híbridas e multinuvem não são tendências emergentes; já são a norma para a maioria das organizações e vieram para ficar. Em vez de migrar tudo para um único provedor ou abandonar totalmente implementações locais, as organizações estão optando deliberadamente por uma combinação de ambientes para atender às suas necessidades operacionais, financeiras e regulatórias. Esses modelos oferecem a flexibilidade de executar workloads onde fizerem mais sentido, seja na nuvem, em vários provedores ou ainda no local.

Sessenta e três por cento das organizações declaram usar mais de um provedor de nuvem; usuários multinuvem operam uma média de dois a três ambientes de nuvem



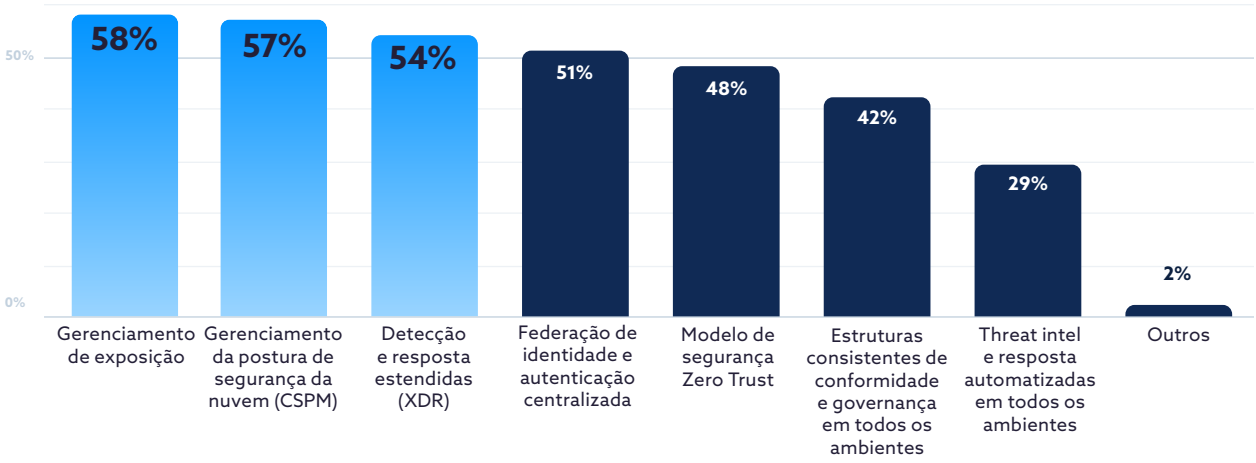
Sessenta e três por cento das organizações declaram usar mais de um provedor de nuvem; usuários multinuvem operam uma média de dois a três (2,7) ambientes de nuvem. Ao mesmo tempo, **82% das organizações mantêm algum tipo de infraestrutura híbrida**, dividida igualmente entre implementações locais e em nuvem ou contando mais com um dos dois tipos de ambiente.

O que melhor descreve a infraestrutura de TI/nuvem de sua organização?



Para proteger essa infraestrutura fragmentada, as organizações contam com ferramentas projetadas para abranger a nuvem e o local. **O monitoramento de segurança unificado e a priorização de riscos (58%)**, **o gerenciamento da postura de segurança na nuvem (CSPM) (57%)** e **detecção e resposta estendidas (XDR) (54%)** são os controles mais usados em ambientes híbridos. Isso sinaliza uma mudança de ferramentas isoladas ou nativas do provedor para mecanismos mais amplos de visibilidade e controle que podem acompanhar a complexidade da infraestrutura híbrida.

Que medidas de segurança sua organização está tomando para entender e agir sobre a exposição e os riscos relacionados nos seus ambientes híbridos?



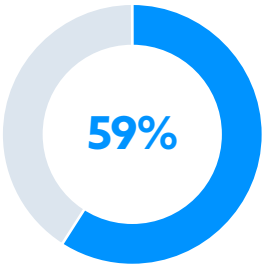
A mudança para nuvem híbrida e multinuvem provavelmente é impulsionada por uma combinação de otimização de custos, demandas regulatórias e requisitos de desempenho. Em alguns casos, as organizações estão até mesmo transferindo as workloads de volta para o local para gerenciar melhor as despesas ou obter um controle mais direto, conforme observado em um antigo relatório de pesquisa da Cloud Security Alliance (CSA). Independentemente da motivação, esse modelo exige estratégias de segurança capazes de fornecer uma aplicação consistente de políticas, gerenciamento de identidades e monitoramento de riscos em um cenário que não é nada uniforme.

Principal descoberta 2:

A identidade tornou-se o elo mais fraco da nuvem (e o mais observado pelas organizações)

Os problemas relacionados à identidade agora estão no topo da lista de preocupações com a segurança da nuvem, superando riscos tradicionais, como configurações incorretas, ameaças internas e vulnerabilidades de workload no que se refere a percepção, impacto de violação e foco estratégico. Embora isso sinalize um progresso significativo na conscientização, há uma lacuna crítica entre a compreensão da identidade como uma ameaça importante e as medidas tomadas para protegê-la efetivamente. A governança, a medição e a coordenação operacional estão aquém da intenção relatada.

Principal risco de segurança à infraestrutura da nuvem da organização

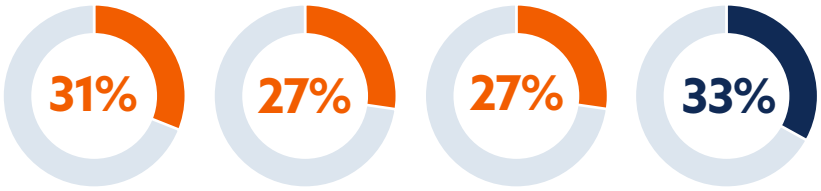


Identidades desprotegidas e permissões perigosas

Cinquenta e nove por cento das organizações identificaram identidades desprotegidas e permissões perigosas como o principal risco de segurança à infraestrutura da nuvem. Essa preocupação também é confirmada pelos dados de violação. Entre as empresas que sofreram uma violação relacionada à nuvem, três das quatro principais causas estavam relacionadas à identidade: **excesso de permissões (31%)**, **controles de acesso inconsistentes (27%)** e **má higiene de identidade (27%)**.

Quais dos seguintes fatores você acha que mais contribuíram para uma violação relacionada à nuvem que ocorreu sua organização?

Relacionados à identidade



Excesso de permissões (ex.: contas ou funções com excesso de privilégios)

Controles de acesso inconsistentes nos ambientes de nuvem

Má higiene de identidade (ex.: ausência de MFA, chaves de acesso inativas)

Infraestrutura ou serviços de nuvem mal configurados

Essas questões estão interconectadas, mas são distintas. Excesso de permissões, como acesso permanente de administrador ou atribuições amplas de funções, podem transformar até mesmo pequenos comprometimentos em grandes violações. Controles de acesso inconsistentes entre ambientes criam proteções desiguais e pontos cegos que podem ser explorados pelos invasores. Uma má higiene de identidade, definida como processos deficientes para identificar e corrigir comportamentos de risco, como chaves sem rodízio, credenciais não utilizadas ou contas órfãs, gera vulnerabilidades de longa duração que geralmente não são detectadas até a ocorrência de um incidente.

Juntos, esses padrões apontam para um problema sistêmico e em camadas: não se trata apenas de algumas contas mal configuradas, mas de um colapso fundamental na forma como a identidade é governada entre equipes e sistemas. Não se trata apenas de lapsos técnicos, mas de desafios operacionais enraizados na falta de propriedade, supervisão e responsabilidade compartilhadas entre as funções de nuvem e de gerenciamento de acesso a identidades (IAM).

Mesmo quando as organizações afirmam que reconhecem esses riscos e priorizam o Zero Trust, a maturidade da segurança ainda fica para trás. Quando indagados sobre os principais desafios, **28% dos entrevistados citaram o desalinhamento entre as equipes de nuvem e IAM** e **21% relataram dificuldade em aplicar privilégios mínimos**. Isso indica que muitas organizações sabem onde está o problema, mas ainda não têm a estrutura ou os fluxos de trabalho para resolvê-lo em escala.

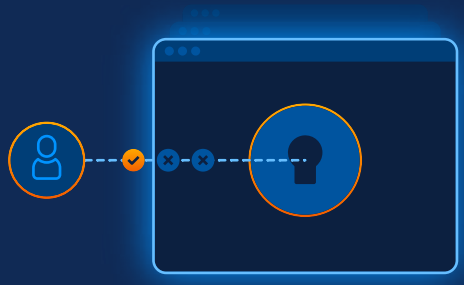
Principais desafios à segurança da infraestrutura da nuvem da organização

28% Falta de alinhamento entre a segurança da nuvem e as equipes de IAM

21% Dificuldade em aplicar privilégios mínimos

Para fechar a lacuna, as organizações estão priorizando arquiteturas Zero Trust e **implementando privilégios mínimos para identidades, que foi a prioridade de segurança da nuvem mais selecionada para os próximos 12 meses (44%)**. No entanto, as práticas de medição continuam em estágio inicial. **Quarenta e dois por cento das organizações monitoram as taxas de adoção de autenticação multifator (MFA) ou logon único (SSO)**, o KPI de IAM mais comum, mas isso só mostra se os controles estão em vigor, não se eles são eficazes. Poucas organizações monitoram indicadores mais profundos de risco de identidade, como uso indevido de privilégios, anomalias de acesso ou abuso de identidade não humana.

44%
das organizações consideram a implementação de privilégios mínimos para identidades uma prioridade máxima



42%
das organizações monitoram as taxas de adoção de autenticação multifator (MFA) ou de logon único (SSO)

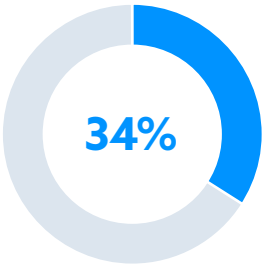
Os dados mostram uma imagem da identidade como uma ameaça bem reconhecida e uma disciplina ainda em amadurecimento no gerenciamento seguro. As organizações estão caminhando na direção certa, mas um progresso significativo exigirá mais do que declarações de políticas. Elas precisarão reestruturar os programas de IAM e os sistemas de suporte, como provedores de identidade, melhorar a coordenação com as equipes de nuvem e passar de métricas de adoção binárias para indicadores de risco de identidade e resiliência mais dinâmicos.

Principal descoberta 3:

A lacuna de conhecimento cria um desafio para o alinhamento da liderança

A falta de conhecimento especializado em segurança da nuvem não é apenas um problema de equipe ou de implementação prática, é um obstáculo estratégico que molda a forma como as organizações planejam, orçam e priorizam a segurança em todos os níveis. À medida que as equipes de segurança batalham para operacionalizar as proteções de nuvem com conhecimento limitado, essa lacuna começa a moldar as decisões que afetam o alinhamento das equipes de liderança, a alocação de recursos e a postura de risco organizacional.

Principais desafios à segurança da infraestrutura da nuvem da organização



Falta de conhecimento especializado

Trinta e quatro por cento dos entrevistados identificaram a falta de conhecimento como o principal desafio para proteger a infraestrutura da nuvem — mais do que qualquer outro problema. Mas o impacto dessa lacuna não se limita ao nível prático. Isso cria um efeito cascata que prejudica o planejamento e a execução. Quando indagados sobre as barreiras para a implementação de novos recursos de segurança da nuvem, os entrevistados apontaram **estratégia pouco clara (39%)**, **orçamento insuficiente (35%)** e **desvios de recursos para outras prioridades (31%)** — todos sintomas de que a liderança está enfrentando dificuldades para definir a direção, avaliar as compensações ou compreender totalmente os riscos que estão em jogo.

Quais são as três principais barreiras para a implementação de novos recursos de segurança da nuvem na sua organização?

39% Estratégia ou plano pouco claro para a segurança da nuvem

35% Verba insuficiente

31% Recursos desviados para outras prioridades

30% Falta de conhecimento especializado

29% Integração com sistemas legados

26% Falta de processos ou documentação

23% Falta de apoio da gestão sênior

20% Restrições de tempo

17% Ficar preso a um só fornecedor ou fidelidade interna aos fornecedores

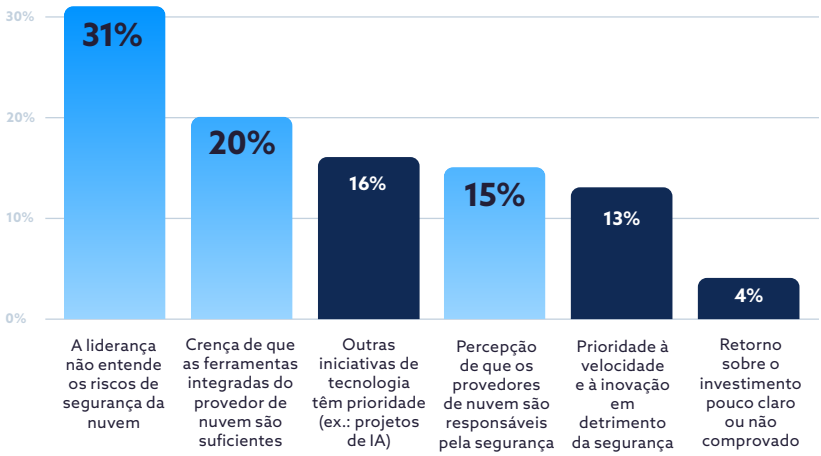
16% As ferramentas e as soluções disponíveis não atendem às necessidades da organização

11% Atrito com a equipe de DevOps

1% Outros

Essa desconexão é ainda mais ressaltada pela forma como a liderança vê a segurança da nuvem. Quase **um terço dos entrevistados (31%) disse que sua liderança executiva não tem conhecimentos suficientes dos riscos de segurança da nuvem**. Outros observaram que os líderes acreditam que as **ferramentas integradas do provedor de nuvem são "boas o suficiente" (20%)** ou presumem que o **provedor de nuvem é o principal responsável pela proteção do ambiente (15%)**, um claro mal-entendido sobre o modelo de responsabilidade compartilhada. Essas percepções sugerem que muitas equipes executivas ainda atuam com base em suposições de segurança antigas, o que dificulta para as equipes de segurança obterem suporte para as ferramentas, o pessoal ou o tempo necessário para proteger os complexos ambientes híbridos e multinuvem atuais.

Se a sua organização não conta com o apoio da gestão sênior, qual é o principal motivo do apoio limitado às novas iniciativas de segurança da nuvem?



Em vez de tratar a especialização apenas como uma questão de contratação ou treinamento, as organizações podem reformular o problema como um desafio operacional mais amplo, que pode ser resolvido por meio de uma combinação de capacitação interna, parcerias externas e opções de plataforma que reduzam a carga cognitiva. Há também uma clara oportunidade de usar essas plataformas e ferramentas não só para melhorar a postura de segurança, como também ajudar a educar a liderança ao longo do caminho. Ao alinhar o entendimento dos executivos com as realidades de segurança, as organizações podem passar de um raciocínio reativo e de soluções pontuais para programas de segurança mais estratégicos e integrados.

Principal descoberta 4:

Combater incêndios em vez de preveni-los — medir violações, não a prevenção

A segurança da nuvem continua presa em um ciclo reativo. Embora as violações continuem sendo um desafio persistente e significativo, as organizações estão medindo o desempenho com base no que já deu errado, em vez de medir a eficácia com que o risco está sendo reduzido ou evitado. O resultado é uma cultura de métricas que reforça a resposta à crise em detrimento da resiliência de longo prazo.

O KPI de segurança da nuvem mais comumente monitorado é a **frequência e a severidade dos incidentes de segurança (43%)**, uma métrica que só se torna relevante após a ocorrência de um incidente. No IAM, a principal métrica é a **taxa de adoção de MFA/SSO (42%)**, que monitora se os controles básicos estão em vigor, não se são eficazes ou se estão sendo mal utilizados. Juntos, esses números sugerem que as organizações continuam concentradas em indicadores de nível superficial, em vez de medidas de desempenho mais estratégicas e voltadas para o futuro.

Essa mentalidade de olhar para o passado também se reflete nos dados de violação. As organizações relataram uma média de 2,17 violações relacionadas à nuvem nos últimos 18 meses, mas **apenas 8% delas foram classificadas como "graves"**. Embora alguns incidentes possam ser realmente de baixo impacto, a discrepância sugere que muitos estão sendo percebidos como menos graves, talvez porque não acionaram os limites obrigatórios de relatórios, uma cobertura significativa da mídia ou um impacto operacional óbvio.

Em média, classifique o nível de severidade das violações relacionadas à nuvem que sua organização sofreu.

Quais dos seguintes fatores você acha que mais contribuíram para a relacionada à nuvem que sua organização sofreu?

Os dados revelam uma desconexão entre a frequência das violações e a forma como os incidentes são avaliados internamente, o que complica as iniciativas para medir e comunicar o verdadeiro desempenho da segurança. Essa desconexão torna-se ainda mais preocupante quando considerada paralelamente às causas básicas dessas violações, muitas das quais podem ser evitadas. **Trinta e três por cento citaram serviços de nuvem mal configurados**, enquanto **31% apontaram excesso de permissões**, **20% ameaças internas** e **15% comprometimento de credenciais** — problemas que poderiam ser mitigados por meio de gerenciamento de configurações, governança de acesso e detecção proativa mais fortes.

Tudo isso aponta para um perigoso ponto cego de medição. As taxas de violação permanecem altas, mas poucos incidentes são classificados como graves, e os KPIs que a maioria das organizações monitora permanecem enraizados na reação, não na prevenção. A medição continua vinculada à resposta pós-incidente, e não à redução de riscos com visão de futuro.

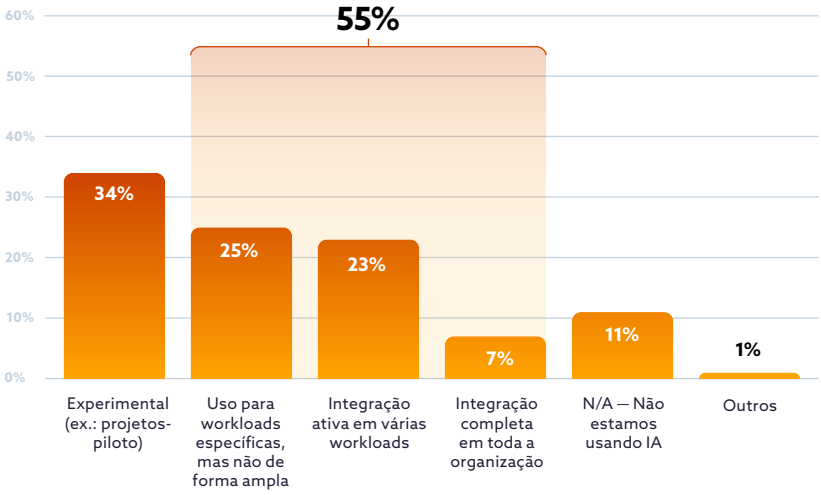
Essa abordagem falha de duas maneiras críticas: não demonstra o valor do investimento proativo para a liderança e obscurece o escopo total do risco ao presumir que os incidentes são sempre visíveis, reportáveis e classificados corretamente. Em ambientes com recursos de detecção limitados, ou quando o desempenho é avaliado pela ausência de incidentes "graves", eventos críticos podem passar despercebidos ou ser subestimados. Romper esse ciclo requer mais do que novas medições ou ferramentas; requer uma redefinição de sucesso centrada na redução de riscos, não no controle de danos.

Principal descoberta 5:

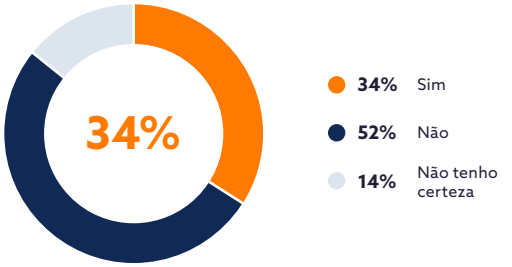
A adoção da IA acelera enquanto a segurança tem como alvo os riscos errados

A adoção da IA está ultrapassando a prontidão de muitas equipes de segurança. Embora 34% das organizações descrevam seu uso de IA como "experimental", uma quantidade ainda maior já ultrapassou essa fase. **Um total de 55% está usando IA para necessidades ativas do negócio** — 25% para workloads específicas, 23% integrando ativamente vários sistemas e 7% totalmente integrada em toda a organização. Não são pilotos teóricos; representam implementações operacionais com impacto real ao negócio. No entanto, à medida que a IA entra em produção, as iniciativas de segurança nem sempre acompanham o ritmo. Resultado: **mais de um terço das organizações com workloads de IA (34%) já sofreram uma violação relacionada à IA**, levantando questões urgentes sobre a prontidão da segurança da IA e a gestão de riscos.

Qual é o nível de desenvolvimento de aplicações de IA na nuvem na sua organização?



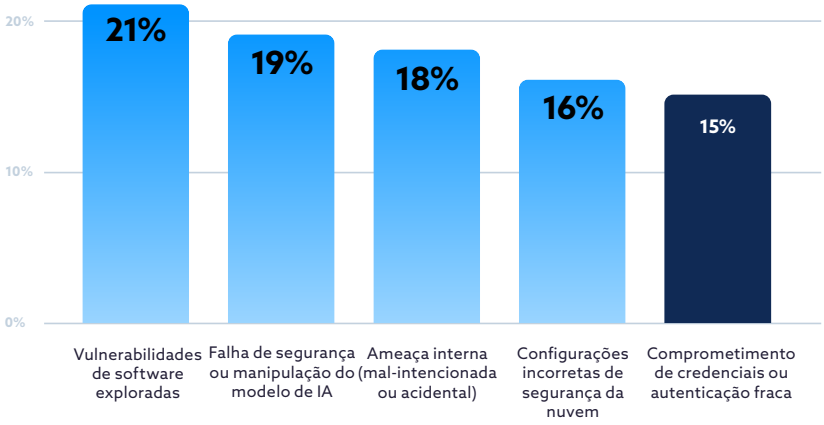
Alguma violação de dados na nuvem sofrida pela sua organização envolve uma workload de IA?



A ocorrência de violações relacionadas à IA aponta para um problema mais profundo: embora a IA esteja sendo operacionalizada, as práticas de segurança ainda não acompanharam totalmente.

As organizações estão agindo rapidamente para implementar a IA, mas sua compreensão dos riscos e de como mitigá-los ainda parece imatura. Essa desconexão fica ainda mais evidente ao comparar o que realmente está causando as violações com o que mais preocupa as equipes de segurança. As causas mais comuns de violações relacionadas à IA incluem ameaças conhecidas: **vulnerabilidades de software exploradas (21%)**, **falhas no modelo da IA (19%)**, **ameaças internas (18%)** e **configurações incorretas da nuvem (16%)**. No entanto, quando indagadas sobre os tipos de violação que mais as preocupam, as organizações gravitaram em torno de riscos desconhecidos ou "nativos da IA", como a **manipulação de modelos (18%)** e o **uso de modelos de IA não autorizados (15%)**, enquanto **as preocupações com ameaças internas (9%)** e comprometimento de credenciais (7%) ficaram muito abaixo. Esse desalinhamento sugere que muitos programas de segurança ainda tratam a IA como algo fundamentalmente novo, em vez de aplicar princípios comprovados de segurança da nuvem e identidade a esses novos sistemas.

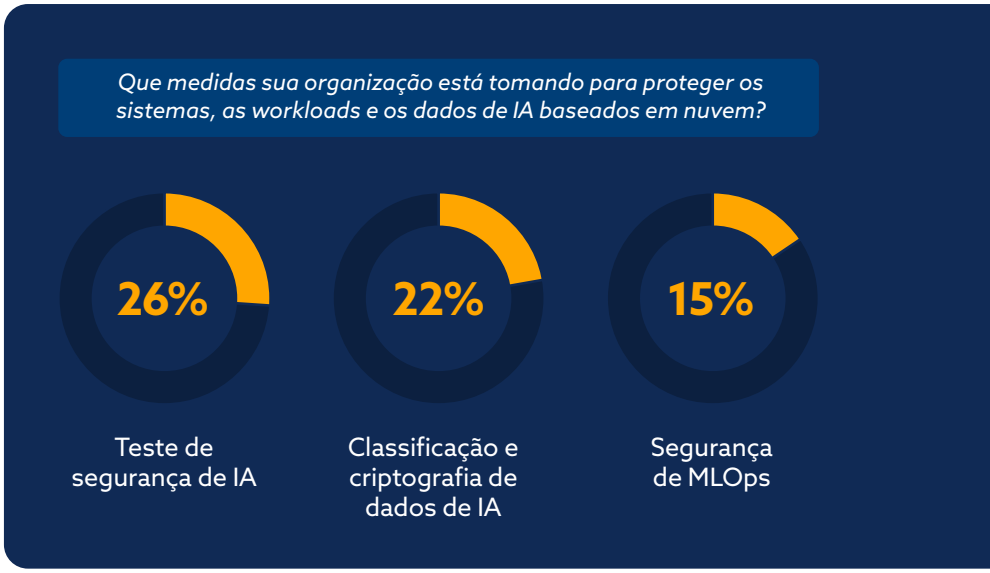
Qual foi a principal causa da violação de dados que envolveu uma workload de IA?



Com qual tipo de violação de dados na nuvem envolvendo workloads de IA sua organização mais está preocupada?

18%	Falha de segurança ou manipulação do modelo de IA	**10%**	Causa incerta ou desconhecida	**5%**	Vulnerabilidades de software exploradas
15%	Uso de modelos de IA não autorizados em desenvolvimento	**9%**	Ameaça interna (mal-intencionada ou acidental)	**2%**	Descomissionamento ineficaz de ativos de IA na pré-produção
13%	Configurações incorretas de segurança da nuvem	**8%**	Ataque a cadeia de suprimentos ou fornecedores terceirizados		
11%	Prefere não informar	**7%**	Comprometimento de credenciais ou autenticação fraca		

Os controles de segurança ilustram ainda mais esse desequilíbrio. Mais da **metade das organizações (51%) contam com estruturas de conformidade**, como NIST AI RMF ou EU AI Act, para guiar suas iniciativas de segurança de IA. O alinhamento regulatório é essencial e oferece uma base necessária, mas as estruturas, por si só, não foram criadas para acompanhar a velocidade e a complexidade da adoção da IA.



Um programa de segurança sólido deve abordar proativamente o perfil de risco específico da organização. No entanto, a baixa adoção das principais proteções técnicas sugere que muitas organizações param na conformidade. Apenas **26% realizam testes de segurança específicos para IA**, como a formação de red teams", apenas **22% classificam e criptografam dados de IA** e apenas **15% implementam práticas de segurança de MLOps**. Essa postura de conformidade pesada, mas tecnicamente superficial, pode deixar as workloads de IA expostas.

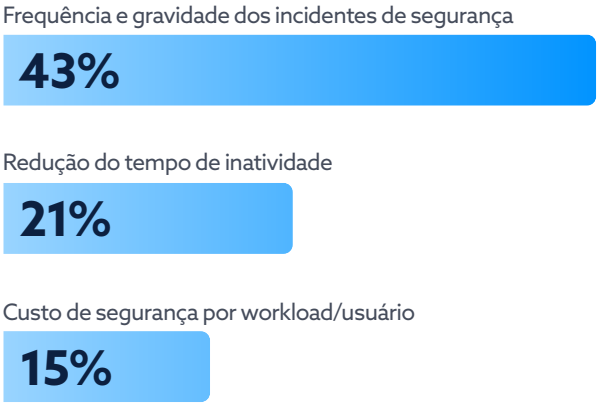
Sem um investimento técnico mais profundo e estratégias embasadas em riscos, as organizações correm o risco de ignorar práticas fundamentais de segurança que já existem em outros domínios, como governança de identidade, fortalecimento da workload e proteção de dados. E isso se refere apenas ao uso sancionado; com o aumento da shadow AI, a parte não monitorada do cenário da IA pode representar um risco ainda maior.

Principal descoberta 6:

É hora de redefinir a estratégia de segurança

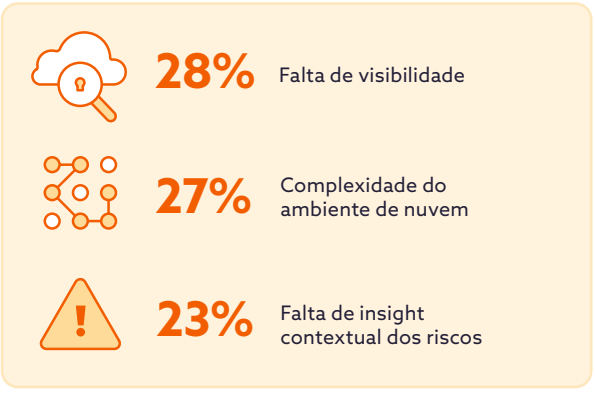
Muitas equipes de segurança sabem o que precisa ser feito, mas a liderança ainda atua com suposições ultrapassadas. À medida que as implementações de nuvem e IA se expandem em ambientes híbridos e multinuvem, a complexidade da segurança aumenta. Porém, em nível executivo, concepções incorretas sobre responsabilidade e risco estão atrasando o progresso e impedindo que as organizações ampliem suas estratégias de segurança de forma eficaz.

Como você demonstra os KPIs dos seus investimentos em tecnologia de segurança da nuvem?



Como observado anteriormente, muitos executivos ainda superestimam a cobertura de segurança fornecida pelos provedores de nuvem ou pelas ferramentas integradas, e esse mal-entendido molda a forma como o sucesso é medido.Embora os provedores de nuvem continuem a aprimorar suas ofertas de segurança nativa, eles costumam se limitar às suas próprias plataformas e não se estendem a cenários híbridos ou multinuvem, deixando lacunas de visibilidade e controle. A maioria das organizações ainda depende de KPIs reativos, como **frequência e severidade de incidentes (43%)**, enquanto poucas monitoram métricas mais proativas, como **redução do tempo de inatividade (21%)** ou **custo da segurança por workload (15%)**. Para agravar esse desafio, ainda há relativamente poucas soluções que unificam a visibilidade e a avaliação de riscos em ambientes híbridos, o que dificulta ainda mais para as equipes medirem e gerenciarem os riscos de forma holística. O resultado é um ponto cego estratégico persistente. Sem um entendimento claro ou indicadores de desempenho significativos, as equipes de segurança não têm a direção e os recursos necessários para priorizar a maturidade a longo prazo.

Principais desafios à segurança da infraestrutura da nuvem da organização



As implicações são significativas. As organizações têm ambientes complexos — 82% operam ambientes híbridos e 63% têm um ambiente multinuvem — e têm dificuldades com eles. Alguns dos principais desafios, além dos já discutidos, incluem a **falta de visibilidade (28%)**, a **complexidade do ambiente de nuvem (27%)** e a **falta de perspectivas contextuais sobre os riscos (23%)**, todos necessários para entender e priorizar os riscos. Mas, em vez de investir em iniciativas básicas, como visibilidade unificada ou simplificação do panorama de ferramentas, apenas 20% priorizam a avaliação unificada de riscos e somente 13% estão focadas na consolidação de ferramentas.

Isso faz com que as equipes de segurança gerenciem soluções fragmentadas sem o suporte estrutural para reduzir o risco de forma holística ou escalar suas iniciativas de forma eficaz.

Para quebrar esse ciclo, as organizações precisam de mais do que correções técnicas; precisam de uma redefinição estratégica. A liderança deve ir além das suposições de que a segurança está "embutida" e investir em plataformas e processos que ofereçam visibilidade integrada, reduzam a complexidade e permitam uma gestão de riscos voltada para o futuro. Essa mudança é particularmente urgente conforme a adoção da IA se acelera, introduzindo novos riscos que exigem maturidade da segurança básica e agilidade para responder às ameaças emergentes. Até que essa redefinição ocorra, até mesmo as equipes de segurança mais capacitadas permanecerão estagnadas em operações reativas, sem o alinhamento estratégico necessário para escalar, adaptar e amadurecer.

Conclusão

A maioria das organizações já opera em ambientes híbridos e multinuvem, e mais da metade usa IA para workloads críticas ao negócio. Embora a infraestrutura e a inovação tenham evoluído rapidamente, a estratégia de segurança não acompanhou esse ritmo. Em todos os setores, as organizações enfrentam dificuldades com ferramentas de segurança fragmentadas, governança de identidade imatura e práticas de medição que permanecem reativas, em vez de proativas. Para fortalecer os programas de segurança da nuvem e IA, as organizações precisam passar de respostas reativas a estratégias proativas e embasadas em riscos. Isso significa:

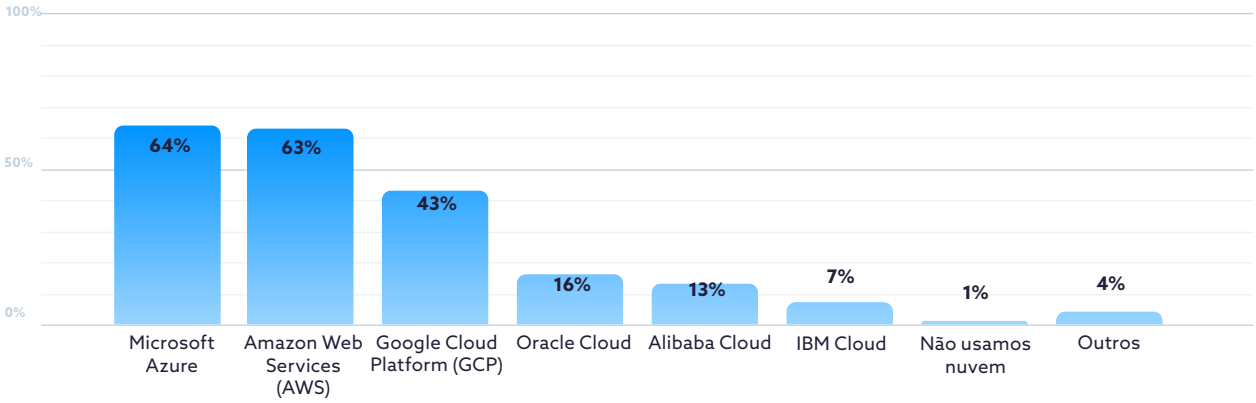
- Priorizar a visibilidade unificada e a aplicação consistente de políticas em ambientes híbridos e multinuvem;
- Investir em governança de identidade, incluindo controles para privilégios mínimos e identidades não humanas;
- Expansão dos KPIs para refletir a prevenção e a resiliência, não apenas a resposta a incidentes;
- Alinhar o entendimento da liderança com as realidades operacionais para apoiar o planejamento e a alocação de recursos mais inteligentes;
- Ir além da conformidade como o teto da segurança de IA, usando-a como ponto de partida para proteções técnicas mais profundas.

A maturidade da segurança não vem apenas das ferramentas; faz-se necessário um esforço coordenado entre as equipes, a liderança e a estratégia. As organizações bem-sucedidas serão aquelas que criarem as estruturas para entender, priorizar e reduzir os riscos antes que os incidentes ocorram.

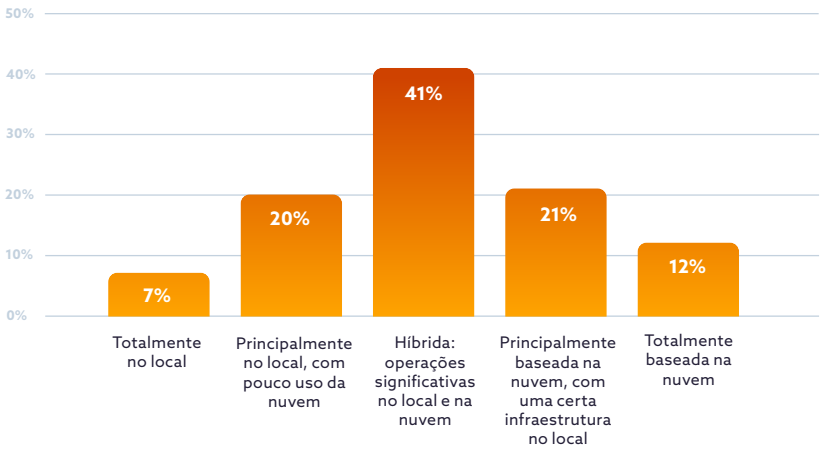
Resultados completos da pesquisa

Infraestrutura da nuvem

Qual dos seguintes provedores de nuvem sua organização usa?

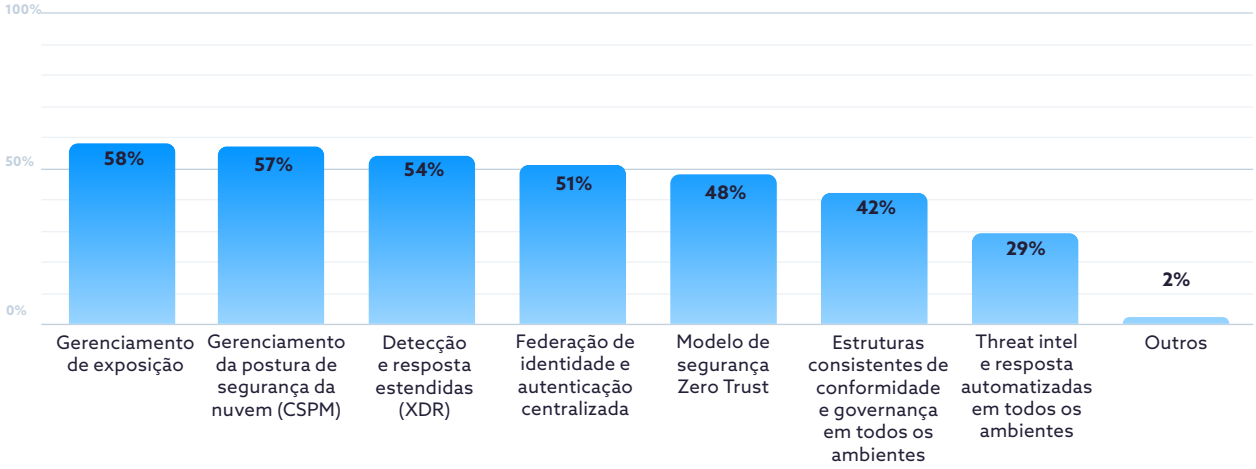


O que melhor descreve a infraestrutura de TI/nuvem da sua organização?



Segurança da nuvem

Que medidas de segurança sua organização está tomando para entender e agir sobre a exposição e os riscos relacionados nos seus ambientes híbridos?



Quais medidas de segurança sua organização está usando para entender e agir sobre a exposição e os riscos relacionados no seu ambiente de nuvem?

63% Segurança de API

59% Estruturas de conformidade e governança para ambientes de nuvem

58% Gerenciamento da postura de segurança na nuvem (CSPM)

57% Modelo de segurança Zero Trust

53% Federação de identidade e autenticação centralizada

42% Detecção e resposta estendidas (XDR)

41% Verificação de segurança da infraestrutura como código (IaC)

34% Threat intel e resposta automatizadas

27% Priorização e monitoramento unificado de riscos na nuvem

19% Gerenciamento de direitos da infraestrutura de nuvem (CIEM)

6% Outros

Riscos, desafios e barreiras

Na sua opinião, quais são os três maiores riscos de segurança à infraestrutura da nuvem na sua organização?

59%	Identidades humanas/de serviço desprotegidas e permissões perigosas	**22%**	Recursos da nuvem expostos publicamente	**15%**	Configuração incorreta da rede
47%	Configurações incorretas da nuvem	**21%**	Vulnerabilidades da workload ou ameaças no tempo de execução	**11%**	Não conformidade com as normas
31%	Riscos de terceiros/ataques à cadeia de suprimentos	**20%**	APIs ou outras interfaces perigosas	**11%**	Documentação ou processos deficientes
31%	Erro humano	**19%**	Ataques de ransomware	**1%**	Outros

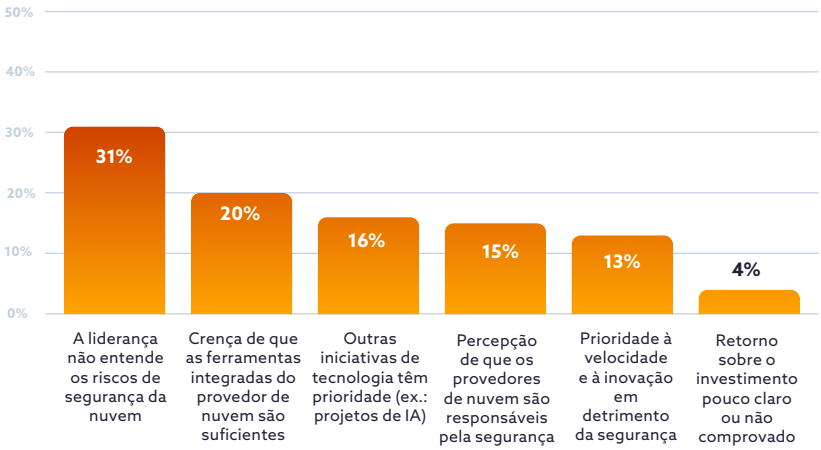
Quais são os três principais desafios à segurança da infraestrutura da nuvem da sua organização

34%	Falta de conhecimento especializado	**23%**	Restrições de tempo	**16%**	Atrito com DevOps
28%	Falta de alinhamento entre a segurança da nuvem e as equipes de IAM	**22%**	Falta de processos ou documentação	**12%**	Falta de controles granulares
28%	Falta de visibilidade	**21%**	Dificuldade em aplicar privilégios mínimos	**7%**	Falta de controles de acesso temporário (Just-in-Time)
27%	Complexidade do ambiente de nuvem	**19%**	Falta de automação ou ferramentas adequadas	**2%**	Outros
23%	Falta de insight contextual dos riscos	**17%**	Dificuldade com o gerenciamento do ciclo de vida de identidades		

Quais são as três principais barreiras para a implementação de novos recursos de segurança da nuvem na sua organização

39%	Estratégia ou plano pouco claro para a segurança da nuvem	**29%**	Integração com sistemas legados	**17%**	Ficar preso a um só fornecedor ou fidelidade interna aos fornecedores
35%	Verba insuficiente	**26%**	Falta de processos ou documentação	**16%**	As ferramentas e as soluções disponíveis não atendem às necessidades da organização
31%	Recursos desviados para outras prioridades	**23%**	Falta de apoio da gestão sênior	**11%**	Atrito com a equipe de DevOps
30%	Falta de conhecimento especializado	**20%**	Restrições de tempo	**1%**	Outros

Se a sua organização não conta com o apoio da gestão sênior, qual é o principal motivo do apoio limitado às novas iniciativas de segurança da nuvem?



Prioridades e KPIs

Quais são as três principais prioridades de segurança para a infraestrutura da nuvem nos próximos 12 meses

44% Implementar Zero Trust e privilégios mínimos para identidades

36% Detectar e corrigir configurações incorretas na nuvem

26% Manter a conformidade (ex.: NIST, SOC2, ISO, PCI-DSS, CIS)

24% Implementar acesso elevado temporário (JIT) para DevOps e outras equipes (ex.: remover privilégios permanentes)

21% Avaliar e reduzir a superfície de ataque da infraestrutura da nuvem

20% Unificar a avaliação de riscos para 20% dos ambientes híbridos (ex.: na nuvem, no local, OT)

20% Implementar detecção e resposta na nuvem (CDR)

17% Otimização do orçamento

17% Gerenciar vulnerabilidades da workload

15% Melhorar a resiliência e a recuperação de desastres

15% Integração de segurança de IA e análise de dados

15% Implementar a verificação da infraestrutura como código (IaC)

13% Consolidação de ferramentas

2% Preparar-se para ameaças quânticas

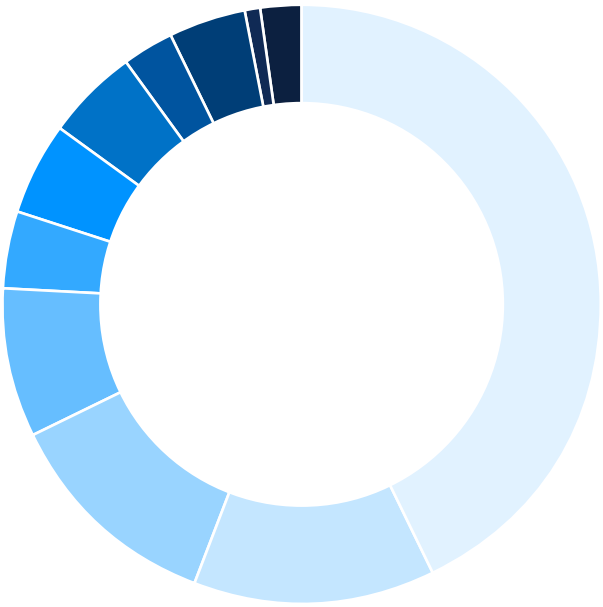
Como você demonstra os KPIs dos seus investimentos em tecnologia de segurança da nuvem?

43%	Frequência e gravidade dos incidentes de segurança	**21%**	Redução do tempo de inatividade	**14%**	Tempo para obtenção de valor (TTV)
36%	Tempo médio para corrigir (MTTR)	**18%**	Taxa de falsos positivos	**14%**	Relatórios observacionais sobre o desempenho da tecnologia
33%	Pontuação de conformidade e auditorias	**17%**	Tempo médio para conter (MTTC)	**6%**	Não medimos o desempenho dos nossos investimentos em tecnologia
32%	Tempo médio para detectar (MTTD)	**17%**	Tempo médio para restaurar a normalidade (MTTRN)	**1%**	Outros
25%	Tempo médio para identificar (MTTI)	**15%**	Custo de segurança por workload/usuário		

Como você demonstra os KPIs dos seus investimentos em tecnologia de segurança de IAM?

42%	Taxas de adoção de autenticação multifator (MFA) ou de logon único (SSO)	**21%**	Tempo médio para corrigir (MTTR)	**13%**	Tempo médio para conter (MTTC)
28%	Frequência e gravidade dos incidentes de segurança	**21%**	Frequência de anomalias de acesso	**13%**	Tempo para obtenção de valor (TTV)
24%	Pontuação de conformidade e auditorias	**16%**	Frequência de abuso de acesso a privilégios	**12%**	Tempo médio para restaurar a normalidade (MTTRN)
22%	Tempo médio para detectar (MTTD)	**16%**	Custo de segurança por workload/usuário	**9%**	Relatórios observacionais sobre o desempenho da tecnologia
22%	Tempo médio para identificar (MTTI)	**14%**	Taxa de falsos positivos	**9%**	Não medimos o desempenho dos nossos investimentos em tecnologia

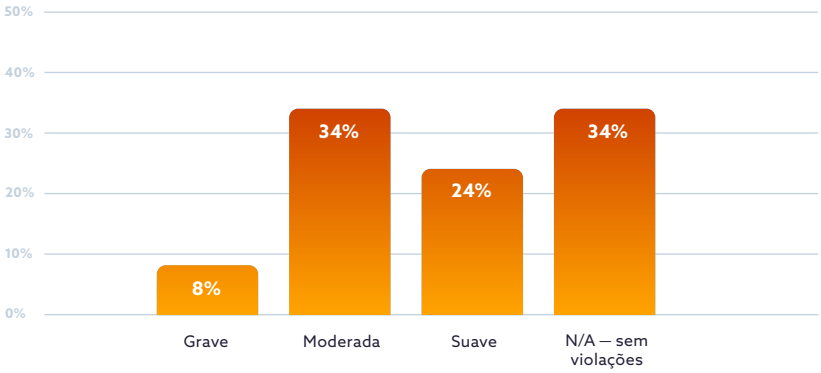
Violações na nuvem



Quantas violações relacionadas à nuvem sua organização sofreu nos últimos 18 meses?

42%	0	**5%**	6
13%	1	**3%**	7
12%	2	**4%**	8
8%	3	**1%**	9
4%	4	**2%**	10
5%	5		

Em média, classifique o nível de severidade das violações relacionadas à nuvem que sua organização sofreu.

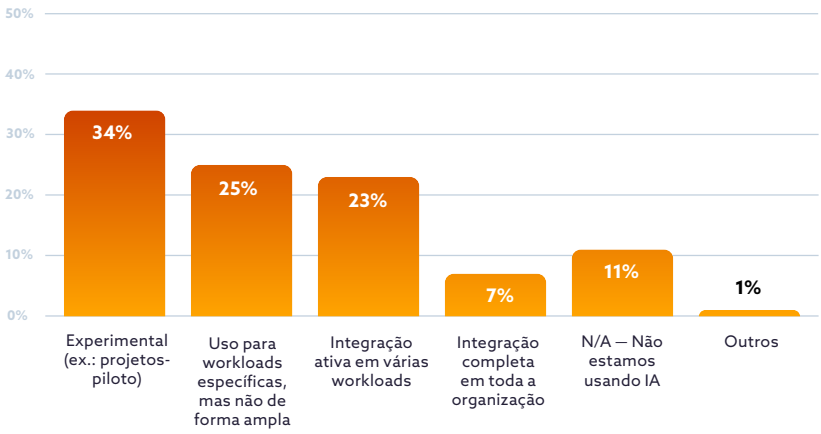


Quais dos seguintes fatores você acha que mais contribuíram para a violação da sua organização?

33%	Infraestrutura ou serviços de nuvem mal configurados	**20%**	Ameaça interna (intencional ou acidental)	**15%**	Comprometimento de credenciais (ex.: phishing, vazamento de segredos)
31%	Excesso de permissões (ex.: contas ou funções com excesso de privilégios)	**20%**	APIs ou outras interfaces perigosas	**15%**	Experiência insuficiente ou falta de mão de obra
27%	Controles de acesso inconsistentes nos ambientes de nuvem	**18%**	Comprometimento de terceiros/ fornecedores	**9%**	Vulnerabilidades exploradas
27%	Má higiene de identidade (ex.: ausência de MFA, chaves de acesso inativas)	**17%**	Exposição pública não intencional (por exemplo, buckets S3 abertos, bancos de dados mal configurados)	**25%**	N/A — sem violações

Segurança de IA

Qual é o nível de desenvolvimento de aplicações de IA na nuvem na sua organização?

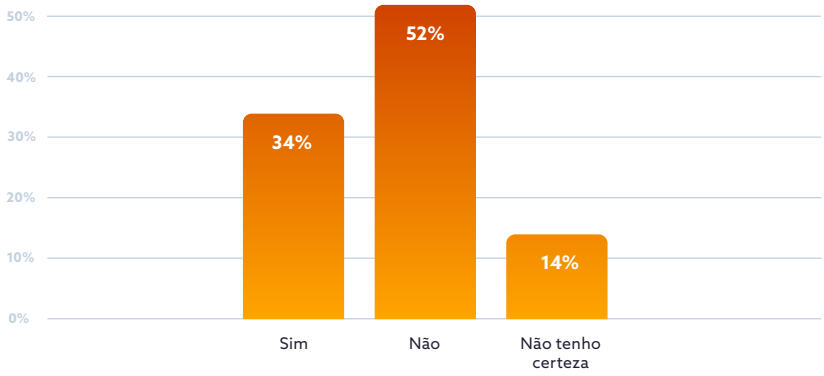


Que medidas sua organização está tomando para proteger os sistemas, as workloads e os dados de IA baseados em nuvem?

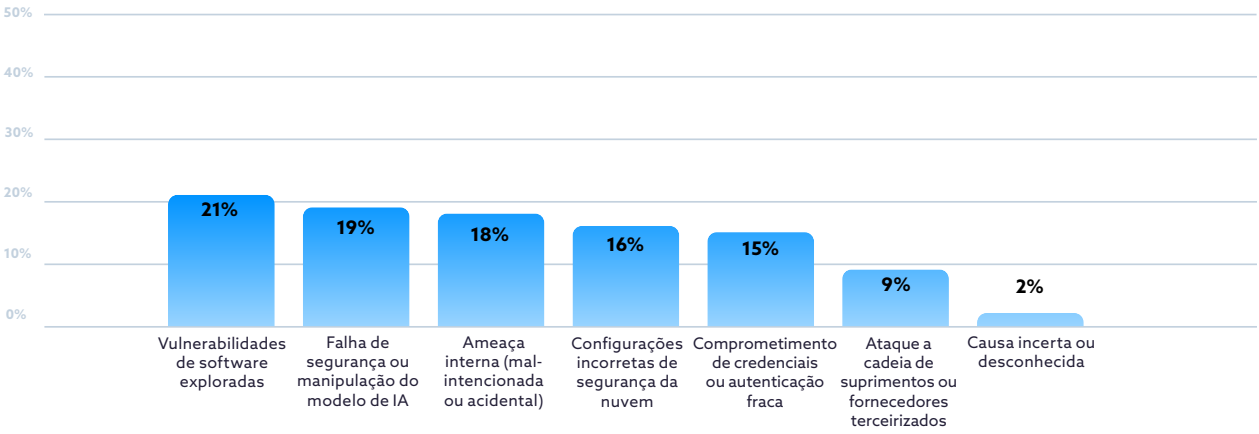
51%	Aplicar conformidade com as estruturas de segurança da IA/nuvem	**30%**	Zero Trust e segmentação de rede das workloads de IA	**22%**	Classificação e criptografia de dados de IA
46%	Adoção das práticas recomendadas do setor	**30%**	Detecção de ameaças e resposta a incidentes para atividades relacionadas à IA	**15%**	Segurança de MLOps
35%	Auditorias regulares de segurança das proteções de integração de modelos de IA	**26%**	Teste de segurança de IA	**5%**	Nenhuma dessas opções se aplica
34%	Controles de identidade e acesso específicos da IA	**23%**	Segurança da cadeia de suprimentos de IA	**1%**	Outros

Violações de IA

Alguma violação de dados na nuvem sofrida pela sua organização envolve uma workload de IA?



Qual foi a principal causa da violação de dados que envolveu uma workload de IA?



Com qual tipo de violação de dados na nuvem envolvendo workloads de IA sua organização mais está preocupada?

18% Falha de segurança ou manipulação do modelo de IA

15% Uso de modelos de IA não autorizados em desenvolvimento

13% Configurações incorretas de segurança da nuvem

11% Prefere não informar

10% Causa incerta ou desconhecida

9% Ameaça interna (mal-intencionada ou acidental)

8% Ataque a cadeia de suprimentos ou fornecedores terceirizados

7% Comprometimento de credenciais ou autenticação fraca

5% Vulnerabilidades de software exploradas

2% Descomissionamento ineficaz de ativos de IA na pré-produção

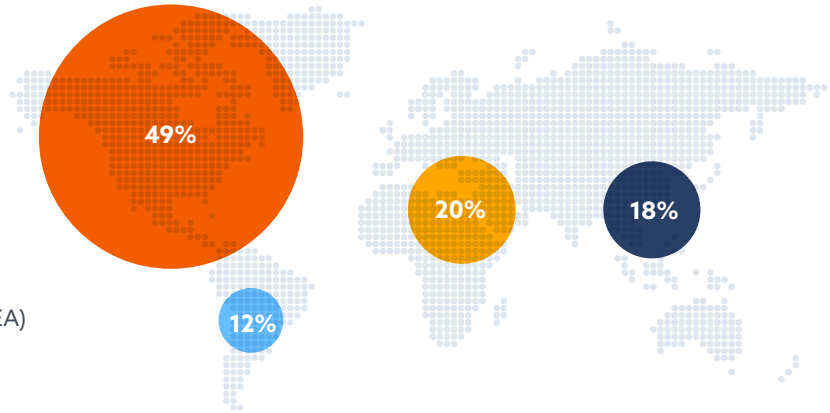
3% Outros

Dados demográficos

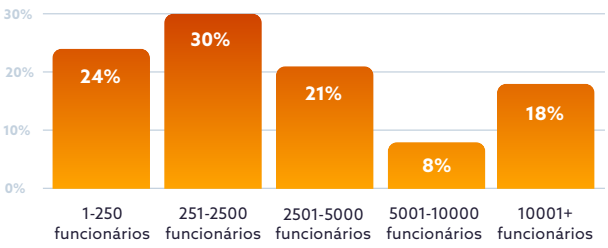
Esta pesquisa global reuniu perspectivas de 1.025 profissionais de TI e segurança de diversas organizações, setores, portes e regiões geográficas. O detalhamento demográfico fornece um contexto importante para a compreensão dos resultados, destacando as diferentes experiências e desafios enfrentados pelas organizações em diversos setores e escalas operacionais.

Em que região do mundo você está?

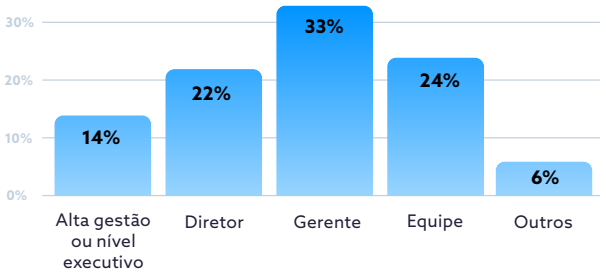
- América do Norte
- América Latina/América do Sul
- Europa, Oriente Médio, África (EMEA)
- Ásia-Pacífico (APAC)



Porte da organização



O que melhor descreve seu nível de cargo?



Qual das opções a seguir melhor descreve o principal setor da sua organização?

23%	Telecomunicações, tecnologia, Internet e eletrônicos	**3%**	Seguros	**2%**	Varejo e bens de consumo duráveis
17%	Finanças e serviços financeiros	**3%**	Indústria automobilística;	**2%**	Transportes e entregas
7%	Educação	**2%**	Linhas aéreas e aeroespacial (incluindo defesa)	**1%**	Agricultura
6%	Governo	**2%**	Serviços públicos, energia e extração	**1%**	Saúde e condicionamento físico
5%	Suporte comercial e logística	**2%**	Propaganda e marketing	**1%**	Mercado imobiliário
5%	Manufatura	**2%**	Entretenimento e lazer	**4%**	Prefere não responder
4%	Saúde e área farmacêutica	**2%**	Alimentos e bebidas		
3%	Construção, maquinário e residências	**2%**	Organizações sem fins lucrativos		

Metodologia de pesquisa e criação

A Cloud Security Alliance (CSA) é uma organização sem fins lucrativos que tem a missão de promover amplamente as práticas recomendadas e garantir a segurança cibernética na computação em nuvem e nas tecnologias de TI. A CSA também educa várias partes interessadas desses setores sobre as preocupações com a segurança em todas as outras formas de computação. Os membros da CSA são uma ampla coalizão de profissionais, corporações e associações do setor. Um dos principais objetivos da CSA é conduzir pesquisas que avaliem as tendências de segurança da informação. Essas pesquisas fornecem informações sobre a maturidade, as opiniões, os interesses e as intenções atuais das organizações no que se referem a segurança e tecnologia da informação.

A Tenable contratou a CSA para desenvolver uma pesquisa e um relatório a fim de entender melhor o conhecimento, as atitudes e as opiniões do setor em relação às tendências de segurança de nuvem e IA. A Tenable financiou o projeto e desenvolveu o questionário em conjunto com os analistas de pesquisa da CSA. A pesquisa foi realizada on-line pela CSA em maio de 2025 e recebeu 1.025 respostas de profissionais de TI e segurança de organizações de vários portes e locais. Os analistas de pesquisa da CSA conduziram a análise e a interpretação dos dados para este relatório.

Objetivos do estudo

Esta pesquisa foi projetada para entender melhor como as equipes de segurança estão passando por essa complexidade; ela aborda de tudo, como proteção de identidade e infraestrutura, alinhamento da liderança e a função emergente da IA em workloads na nuvem. O objetivo é descobrir como as organizações estão adaptando suas estratégias, priorizando os riscos e medindo o progresso em um cenário de ameaças que muda rapidamente.

Principais objetivos:

- Entender como as organizações estão respondendo à evolução dos desafios de segurança em ambientes de nuvem, multinuvem e híbridos;
- Explorar como a infraestrutura, as workloads, as identidades e os dados estão sendo protegidos em configurações híbridas e nativas da nuvem;
- Identificar os principais riscos, barreiras e prioridades que moldam as estratégias modernas de segurança da nuvem;
- Examinar como as organizações monitoram e comunicam os KPIs de segurança relacionados à nuvem para a liderança do negócio;
- Avaliar o estado da adoção da IA na nuvem e como os sistemas de IA, as workloads e os dados estão sendo protegidos.