RELATÓRIO

O Estado da Segurança de Identidade 2026

Perspectivas de 5.000 líderes de TI e segurança cibernética em 17 países

SOPHOS

Introdução

A identidade constitui o perímetro da segurança cibernética, e esse perímetro está se ampliando com a expansão contínua do acesso dos sistemas de IA aos dados empresariais por meio de e-mails, arquivos, aplicativos SaaS e identidades humanas e não humanas. O resultado é o aumento da exposição, com informações confidenciais agora mais acessíveis e mais fáceis de serem transferidas.

À medida que as organizações continuam a acelerar a adoção da nuvem, o trabalho remoto e a proliferação de aplicativos e serviços que dependem de conexões entre máquinas, o número de identidades digitais, humanas e não humanas, disparou. Cada credencial de usuário, chave de API, conta de serviço e token OAuth representa um ponto de entrada potencial para adversários. Isso torna a segurança de identidade uma das áreas mais críticas e desafiadoras da defesa cibernética moderna.

Os invasores já perceberam essa mudança. Credenciais roubadas, contas de serviço comprometidas e ataques de engenharia social direcionados a funcionários estão agora entre os vetores de acesso inicial mais comuns nas violações de segurança em todo o mundo. Os adversários estão utilizando IA e automação para agir com maior rapidez e abranger mais sistemas. As consequências vão desde o roubo de dados e extorsão até incidentes de ransomware em grande escala, capazes de paralisar as operações comerciais por dias ou semanas.

Para compreender a verdadeira dimensão e o impacto das ameaças relacionadas à identidade, a Sophos encomendou uma pesquisa independente com 5.000 líderes de TI e segurança cibernética em 17 países sobre as experiências e os impactos das ameaças à identidade em 2025. Este relatório apresenta as conclusões, analisando a frequência dos ataques à identidade, a capacidade das organizações de detectar e impedir os ataques, as consequências decorrentes, as causas primárias das violações bem-sucedidas, o impacto financeiro e o estado da higiene da segurança de identidade.

Os resultados revelam um quadro preocupante: as ameaças à identidade são generalizadas, têm consequências graves e estão profundamente interligadas a ransomwares. As organizações que deixam de investir na segurança de identidade colocam em risco as suas operações, finanças e reputação.

5.000

Líderes de TI e segurança de 17 países participaram de uma pesquisa global independente de fornecedores

Pontos-chave

- **71% das organizações sofreram pelo menos uma violação** de segurança relacionada à identidade nos últimos 12 meses, com uma média de três ataques por organização afetada.
- **14% das organizações que sofreram violações não conseguiram detectar e impedir** o ataque de identidade mais significativo antes que fossem causados danos.
- **O custo médio para corrigir uma violação de identidade foi de US$ 1,64 milhão**, com a mediana situando-se em US$ 750.000.
- **O roubo de dados (49%) e o ransomware (48%) foram as consequências** mais comuns dos ataques de identidade bem-sucedidos.
- **Dois terços das vítimas de ransomware (67%) relataram que o incidente de ransomware foi também o ataque à identidade mais** significativo que sofreram, estabelecendo uma clara ligação entre ataques à identidade e ransomware.
- **O gerenciamento deficiente de identidades não humanas (NHI) foi citado em 41% dos casos de violação de identidade**, tornando-se a segunda causa individual mais comum, depois do erro humano (43%).
- **As organizações com um gerenciamento deficiente de identidades não humanas têm 22% mais probabilidade de sofrer roubo financeiro, 24% mais probabilidade de sofrer extorsão** e relatam custos totais de recuperação que chegam a quase US$ 150.000 acima da média.
- **Apenas 1 em cada 3 organizações (34%) realiza regularmente a rotação ou a auditoria de contas de serviço e identidades não humanas**, e apenas 11% as fazem de forma contínua, abrindo brechas de segurança que os invasores exploram.
- **Apenas 24% das organizações monitoram continuamente tentativas de login** suspeitas, e mais da metade faz essa verificação a cada três meses ou com menor frequência.
- **Os fornecedores dos setores de energia, petróleo/gás e serviços públicos (80%) e do governo central/federal (78%) registraram as taxas mais elevadas de** violação de identidade, enquanto os setores de TI, tecnologia e telecomunicações (63%) e saúde (63%) apresentaram as taxas mais baixas.
- **As organizações de menor porte (100 a 250 funcionários) apresentaram 72% de probabilidade de não detectar um ataque** de identidade em comparação com as organizações com 1.001 a 3.000 funcionários (19% x 11%).

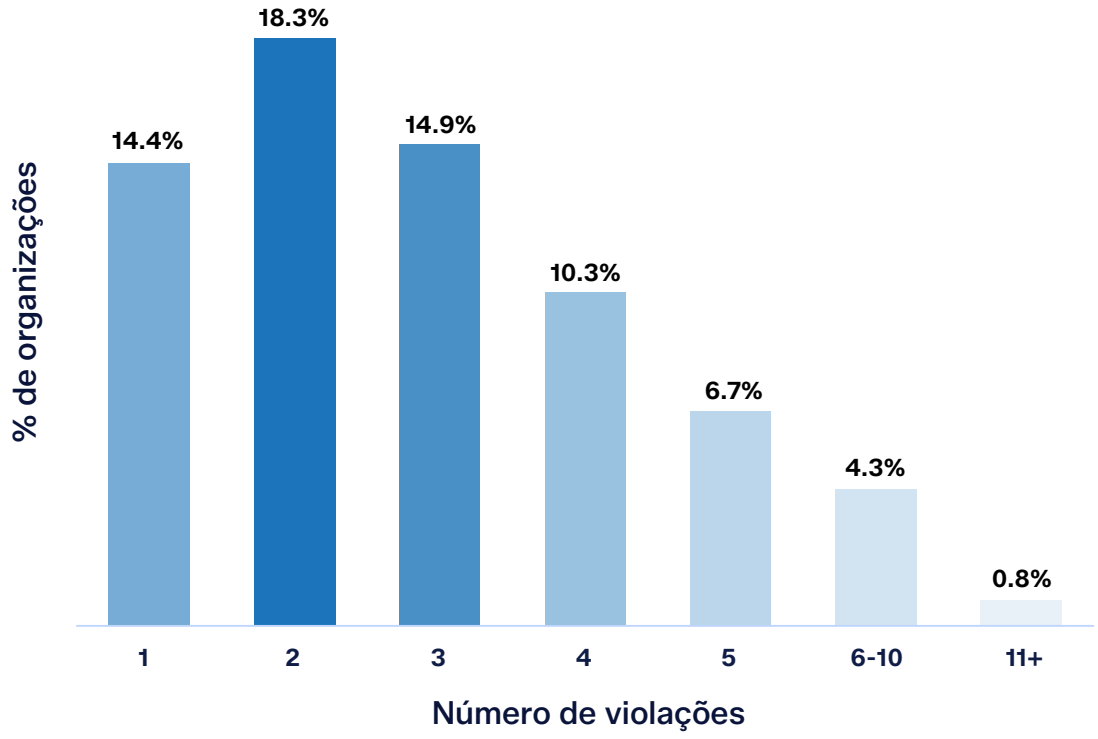
Descobertas detalhadas

Frequência dos ataques de identidade

A pesquisa revela que as violações relacionadas à identidade não são casos isolados; elas são a regra. Mais de sete em cada 10 organizações (70,9%) sofreram pelo menos uma violação de segurança relacionada à identidade nos últimos 12 meses. Apenas 22,6% afirmaram categoricamente que não haviam sofrido nenhuma violação, enquanto 6,4% reconheceram que podem ter ocorrido violações sem o conhecimento deles.

Entre as vítimas, a média de incidentes foi de 3,1, o que indica que os ataques de identidade raramente são eventos isolados. 5% dos entrevistados relataram seis ou mais violações no último ano.

Distribuição de frequência de violações



A sua organização sofreu alguma violação de segurança relacionada à identidade nos últimos 12 meses? Se for o caso, quantas? n=5.000

67%

de todos os incidentes investigados pelo Sophos Incident Response e Sophos MDR em 2025 tiveram origem em ataques relacionados à identidade.

Sophos X-Ops Insight

Sobre os países

Existe uma grande variação geográfica nas taxas de violação. A Suíça (88,7%) registrou a taxa mais elevada, 18 pontos percentuais acima da média global, seguida pelo México (83,3%) e pela Itália (80%). A Alemanha (62,6%), a Colômbia (62,7%) e o Japão (64,7%) foram os países menos afetados, embora mesmo as taxas mais baixas ultrapassem os 60%.

País	Taxa de violação	x Global (70.9%)
Suíça	88.7%	+17,8 pp
México	83.3%	+12,4 pp
Itália	80.0%	+9,1 pp
Austrália	79.7%	+8,8 pp
Índia	76.8%	+5,9 pp
África do Sul	75.0%	+4,1 pp
Brasil	74.0%	+3,1 pp
Emirados Árabes Unidos	73.3%	+2,4 pp
Cingapura	72.0%	+1,1 pp
Espanha	70.0%	-0,9 pp
Chile	66.7%	-4,2 pp
EUA	66.1%	-4,8 pp
França	66.0%	-4,9 pp
Reino Unido	65.3%	-5,6 pp
Japão	64.7%	-6,2 pp
Colômbia	62.7%	-8,2 pp
Alemanha	62.6%	-8,3 pp

A sua organização sofreu alguma violação de segurança relacionada à identidade nos últimos 12 meses? Se for o caso, quantas? n=5.000.

Sobre os setores

Ao analisar os dados sob a ótica setorial, os setores de energia, petróleo/gás e serviços públicos (80,3%) e do governo central/federal (78,4%) registraram as taxas mais elevadas de violação de dados. Os setores de TI, tecnologia e telecomunicações (63,1%) e da saúde (63,4%) foram os menos afetados, o que talvez reflita uma maior maturidade no investimento em segurança nesses setores.

Setor	Taxa de violação
Energia, petróleo/gás e serviços de utilidade	**80.3%**
Governo central/federal	78.4%
Construção civil	76.1%
Manufatura e produção	73.6%
Varejo	72.0%
Ensino básico	71.1%
Serviços financeiros	71.0%
Mídia, lazer e entretenimento	70.9%
Governo local/estadual	69.6%
Distribuição e transporte	67.6%
Ensino superior	65.9%
Serviços profissionais e empresariais	64.5%
Saúde	63.4%
TI, tecnologia e telecomunicações	63.1%

A sua organização sofreu alguma violação de segurança relacionada à identidade nos últimos 12 meses? Se for o caso, quantas? n=5.000.

A conformidade como indicador

As organizações que descreveram o cumprimento dos requisitos de conformidade como "muito desafiador" apresentaram uma taxa de violação de 82,4%, ou seja, 14 pontos percentuais a mais do que aquelas que consideraram a conformidade um desafio moderado ou que não a consideraram um desafio (68,3%). Isso sugere que as dificuldades de conformidade são um indicador antecipado de falhas de segurança mais amplas.

Noções básicas sobre segurança de identidade

Quatro tipos de organizações de identidade para gerenciar

Todas as organizações concedem acesso a diferentes tipos de identidades. Cada uma delas acarreta seus próprios riscos.

Categoria 1 – Identidades da força de trabalho

Pessoas dentro da organização que precisam de acesso a sistemas e dados para desempenhar suas funções.

- Funcionários
- Empresas contratadas
- Administradores de TI e de segurança da informação (pessoas cujas funções exigem acesso privilegiado ao sistema)
- Executivos (pessoas cuja função as torna particularmente valiosas para um adversário)

Categoria 2 – Identidades externas

Pessoas externas à organização às quais é concedido acesso, temporariamente ou de forma contínua, para desempenhar uma função ou interação específica e definida.

- Parceiros
- Fornecedores
- Clientes

Categoria 3 – Identidades não humanas (NHI)

Softwares, sistemas e processos automatizados aos quais é concedido acesso para realizar tarefas sem a intervenção humana.

- Contas de serviço (por exemplo, backups agendados)
- Chaves de API (por exemplo, integrações de aplicativos)
- Agentes de IA (por exemplo, tarefas autônomas)
- Dispositivos IoT (por exemplo, sensores, câmeras)

Categoria 4 – Identidades privilegiadas (risco máximo)

Qualquer identidade, humana ou não humana, com permissões elevadas que concedam acesso privilegiado a sistemas e dados confidenciais.

- Super admins (ou seja, pessoas com controle total do sistema)
- Contas root (por exemplo, acesso de administrador na nuvem)
- Contas compartilhadas (por exemplo, logins de equipe)
- Acesso de emergência (por exemplo, contas de emergência)

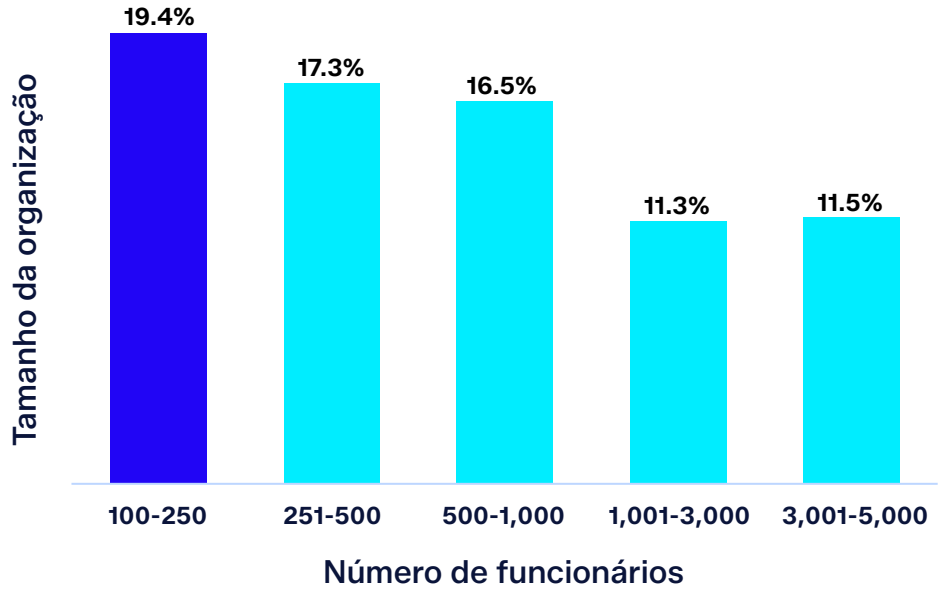
Cada identidade é um ponto de entrada em potencial. Gerenciar quem e o que tem acesso aos seus sistemas e garantir que esse acesso seja adequado e monitorado é uma das medidas mais importantes que uma organização pode tomar para se manter segura.

Capacidade de detectar e impedir ataques de identidade

Dos 3.545 participantes da pesquisa que sofreram uma violação relacionada à identidade em 2025, 85,4% conseguiram detectar e impedir o ataque mais significativo antes que fossem causados danos. Embora isso demonstre que a maioria possui alguma capacidade de detecção, os 14,4% que não conseguiram impedir o ataque representam um risco de cauda substancial e, como revelam as conclusões subsequentes, as consequências para essas organizações são graves.

Falhas na detecção por tamanho da organização

As organizações de menor porte foram significativamente menos propensas a detectar ataques. Entre as empresas de menor porte pesquisadas (100 a 250 funcionários), 19,4% não conseguiram impedir o ataque, o que representa quase o dobro da taxa observada nas organizações com 1.001 a 3.000 funcionários (11,3%). Essa lacuna ressalta os desafios que as pequenas empresas enfrentam em termos de recursos e capacidade.



Pensando no ataque à identidade mais significativo que sua organização sofreu nos últimos 12 meses, vocês conseguiram detectar e impedir o ataque antes que fossem causados danos? Base: a organização sofreu uma violação de segurança relacionada à identidade. n=3.545.

Falhas na detecção por país

O Brasil (21,6%) e a Suíça (21,1%) apresentaram as taxas mais elevadas de falha na detecção, enquanto o Reino Unido (7,1%) e o México (9,6%) tiveram um melhor resultado. É importante destacar que a elevada taxa de violações na Suíça, aliada à baixa taxa de detecção, torna o país um mercado particularmente vulnerável.

País	Falha na detecção
Brasil	**21.6%**
Suíça	21.1%
Japão	19.6%
Espanha	18.1%
Chile	18.0%
Cingapura	17.6%
Alemanha	17.4%
França	14.6%
Itália	14.6%
Austrália	13.8%
Colômbia	13.8%
EUA	12.8%
Emirados Árabes Unidos	11.8%
Índia	11.2%
África do Sul	10.7%
México	9.8%
Reino Unido	7.1%

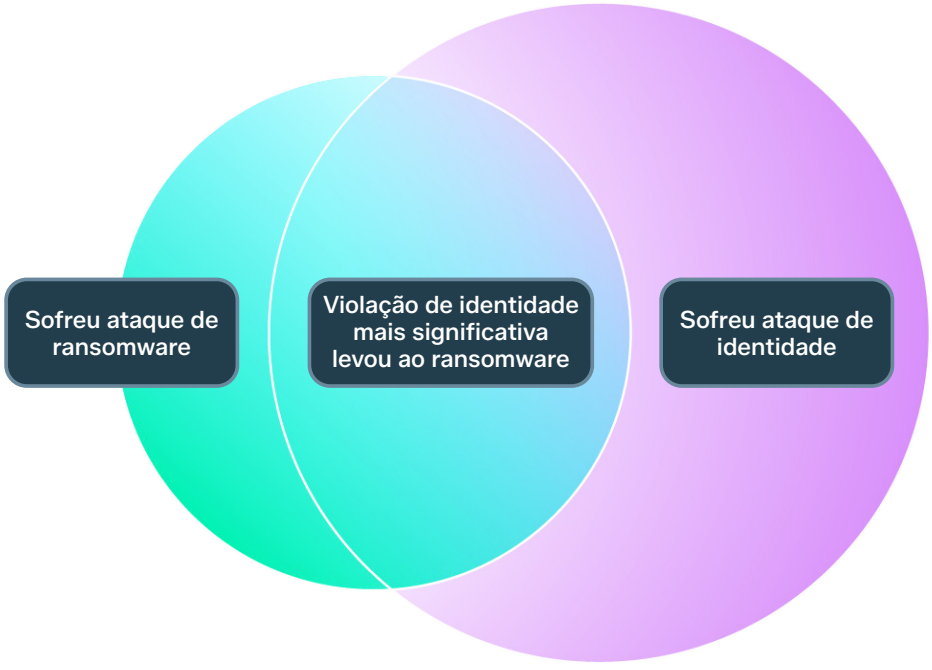
Pensando no ataque à identidade mais significativo que sua organização sofreu nos últimos 12 meses, vocês conseguiram detectar e impedir o ataque antes que fossem causados danos? Base: a organização sofreu uma violação de segurança relacionada à identidade. n=3.545

Falhas na detecção por setor

O setor de mídia, lazer e entretenimento (22,4%) apresentou a maior taxa de falhas em detecção, seguido pelo setor de manufatura (18,4%) e pelos serviços financeiros (17,9%). O setor de saúde (8,1%) apresentou o melhor desempenho em termos de detecção, um possível reflexo da pressão regulatória para investir no monitoramento de ameaças.

A relação entre identidade e ransomware

Uma das conclusões mais marcantes da pesquisa é a relação direta entre os ataques de identidade e o ransomware. Entre as organizações que foram atingidas por ransomware em 2025, dois terços (66,5%) confirmaram que o incidente de ransomware e o ataque de identidade mais significativo foram o mesmo evento. Embora nem todos os ataques tenham resultado na criptografia de dados, isso confirma o roubo de identidade como o principal mecanismo de disseminação de ransomware.



No último ano, a sua organização foi atingida por ransomware? n=5.000). A sua organização sofreu alguma violação de segurança relacionada à identidade nos últimos 12 meses? Se for o caso, quantas? (n=5.000) [Se sim para as duas perguntas] Esse incidente de ransomware e o ataque de identidade mais significativo foram o mesmo evento?

Relação entre ransomware e identidade por tamanho da organização

A relação entre identidade e ransomware foi mais forte em organizações com 1.001 a 3.000 funcionários (71,6%) e mais fraca nas organizações com 100 a 250 funcionários (62,4%). Essa variação pode refletir as diferenças na complexidade da infraestrutura organizacional, nos níveis de visibilidade ou na capacidade de correlacionar o vetor de ataque com o resultado do ataque nos diversos segmentos.

Tamanho da organização	Ransomware = Ataque à identidade
100-250 funcionários	62.4%
251-500 funcionários	68.2%
501-1,000 funcionários	62.5%
1.001-3.000 funcionários	**71.6%**
3.001-5.000 funcionários	64.6%

No último ano, a sua organização foi atingida por ransomware? n=5.000). A sua organização sofreu alguma violação de segurança relacionada à identidade nos últimos 12 meses? Se for o caso, quantas? (n=5.000) [Se sim para as duas perguntas] Esse incidente de ransomware e o ataque de identidade mais significativo foram o mesmo evento?

Sobre os setores

O ensino superior (76,8%) e a distribuição/transporte (75,0%) apresentaram a maior correlação entre ransomware e identidade, enquanto os serviços financeiros (57,6%) e o setor de TI, tecnologia e telecomunicações (61,1%) apresentaram índices mais baixos (embora ainda bem acima do limiar da maioria).

Consequências de violações de identidade não detectadas

Para as 510 organizações que não conseguiram impedir seu ataque de identidade mais significativo, os impactos foram graves e multifacetados, com as vítimas relatando, em média, duas consequências decorrentes do incidente.

Consequência	% de organizações vítimas de violação
Roubo de dados – invasores roubaram dados sensíveis	**48.8%**
Ransomware – credenciais roubadas utilizadas para ajudar na execução do ataque de ransomware	48.4%
Extorsão – invasores exigiram dinheiro com ameaças	43.9%
Sabotagem – invasores utilizaram credenciais para causar danos à organização	30.0%
Roubo financeiro – desvios de pagamentos	28.0%
Roubo financeiro – desvio de dinheiro de contas	25.5%
Resumo: Roubo financeiro (em qualquer forma)	**46.7%**

Quais foram as consequências dessa violação de identidade para a sua organização? Base: a organização não conseguiu impedir a violação de segurança. n=510.

Quase metade das organizações vítimas de violação sofreu roubo de dados (48,8%), e uma proporção quase idêntica foi alvo de ransomware (48,4%). Quase metade (46,7%) sofreu algum tipo de roubo financeiro direto (desvio de pagamentos, desvio de fundos ou ambos). Quando considerados em conjunto com a extorsão (43,9%), esses resultados demonstram que os ataques à identidade não detectados quase sempre resultam em consequências de grande impacto.

Por que as organizações foram vítimas

Compreender por que os ataques são bem-sucedidos é essencial para a prevenção. A pesquisa revelou o conjunto de falhas humanas, processuais e técnicas que levou as organizações a serem vítimas de ataques baseados em identidade. O estudo também revela que raramente a razão é apenas uma, com os entrevistados citando, em média, duas causas primárias que contribuíram para o incidente.

Causa raiz	% de organizações vítimas de violação
Erro humano — funcionário foi induzido a fornecer suas credenciais	**42.7%**
Gerenciamento deficiente de identidades não humanas (por exemplo, chaves de API armazenadas no código, credenciais estáticas, contas de serviço abandonadas que anteriormente conectavam aplicativos aos sistemas, etc.)	40.6%
Gerenciamento deficiente de identidades humanas, usadas por funcionários	38.6%
Falta de visibilidade do acesso e das permissões concedidas a aplicativos externos	35.7%
Gerenciamento deficiente de identidades humanas, usadas por empresas contratadas e fornecedores	31.4%
Falta de controle do acesso e das permissões concedidas a aplicativos externos	30.8%
Atividade interna maliciosa – funcionário que facilitou o ataque deliberadamente	26.7%
Resumo: Gerenciamento deficiente de identidades humanas (em qualquer forma)	**60.2%**
Resumo: Problemas com o acesso e as permissões concedidas a aplicativos externos (em qualquer forma)	**56.1%**

Por que sua organização foi vítima de um ataque relacionado à identidade? Selecione todas as opções que se aplicam. Base: a organização não conseguiu impedir a violação de segurança. n=510.

O erro humano foi o principal fator individual responsável pelas violações de identidade, citado por 42,7% das vítimas. Em segundo lugar, o gerenciamento deficiente de identidades não humanas (40,6%), o que é particularmente preocupante, pois abrange chaves de API armazenadas no código, credenciais estáticas e contas de serviço abandonadas, que são mais difíceis de auditar e monitorar.

Atividades internas maliciosas por parte de funcionários, que facilitaram deliberadamente o ataque, foram citadas em mais de um quarto (26,7%) dos ataques, o que ressalta a importância de manter controles internos rigorosos e de permanecer vigilante.

No geral, o gerenciamento deficiente de identidades humanas (60,2%) é a razão mais comum pela qual as organizações foram vítimas de ataques de identidade, enquanto os problemas com o acesso e as permissões concedidas a aplicativos externos foram um fator presente em 56,1% dos incidentes.

59.5%

A MFA, uma tecnologia que já existe há décadas, não estava disponível no sistema visado em 59,5% dos casos de MDR analisados no Relatório Sophos de Adversários Ativos 2025.

Sophos X-Ops Insight

Sobre o tamanho das organizações

As organizações de maior porte enfrentam mais dificuldades do que as empresas menores em várias áreas da exposição de identidade, um provável reflexo da dimensão e complexidade dos ambientes que precisam monitorar e proteger.

Mais da metade (55,6%) das empresas com 1.001 a 3.000 funcionários apontaram o erro humano como causa primária, comparado a apenas 29,0% das empresas com 251 a 500 funcionários. Da mesma forma, 68,6% das organizações com 3.001 a 5.000 funcionários afirmaram que o gerenciamento deficiente de identidades humanas contribuiu para que fossem vítimas de ataques, comparado a 58,5% das empresas com 100 a 250 funcionários.

Explicação sobre identidades não humanas

Uma identidade não humana (NHI) é uma credencial digital atribuída a um software, sistema ou processo automatizado para que possa acessar recursos sem intervenção humana. Em vez de senhas, NHIs utilizam credenciais não humanas para comprovar sua identidade, incluindo:

- Chaves de API para conectar aplicativos
- Contas de serviço que executam backups
- Tokens OAuth para integrações SaaS
- Agentes de IA que acessam bancos de dados

As credenciais NHI podem ser roubadas e utilizadas indevidamente da mesma forma que os dados de login das pessoas [humanas]. Isso se torna ainda mais problemático quando as organizações não realizam auditorias regulares das permissões NHI, que, com frequência, são amplas e significativas.

NHIs superam significativamente o número de identidades humanas, com algumas organizações registrando proporções superiores a 100:1. A IA agêntica tem sido um dos principais fatores por trás desse aumento em proporções nos últimos anos.

96%

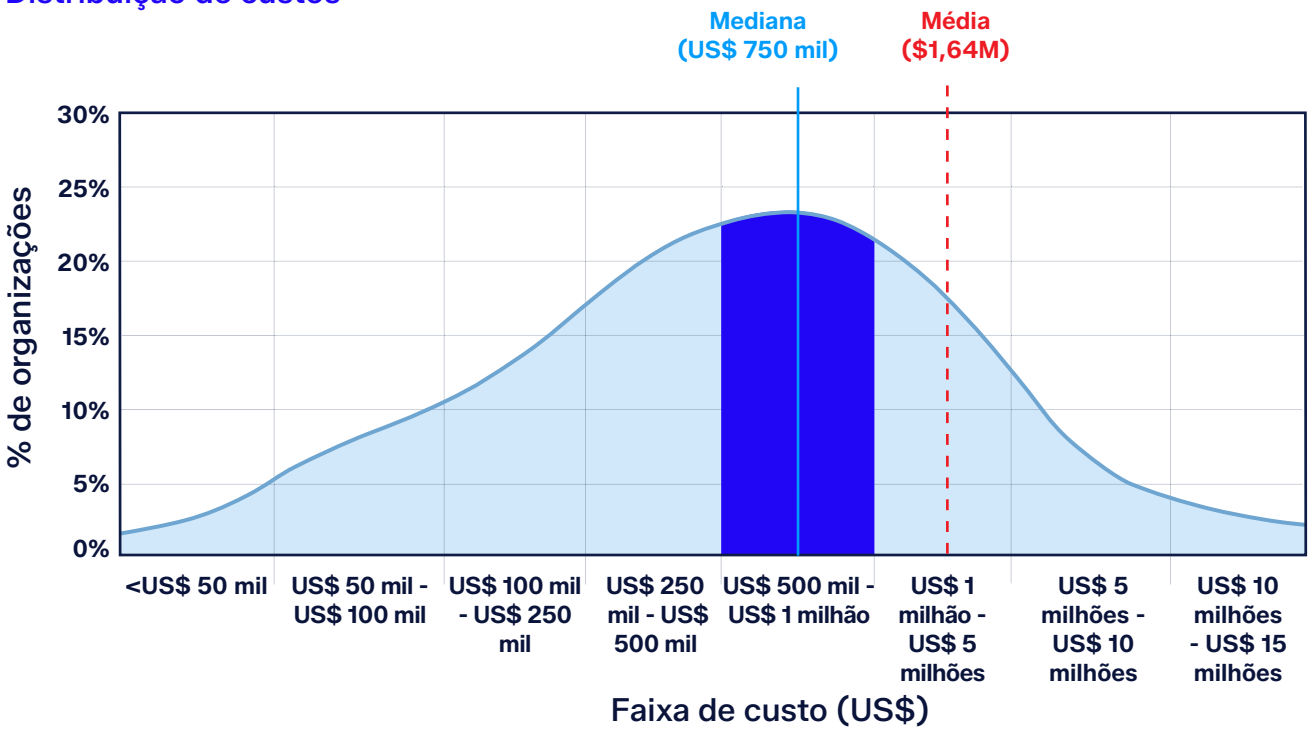
dos ambientes dos clientes do Sophos ITDR têm aplicativos multilocatário presentes. Auditar ou simplesmente listar as identidades NHI envolvidas nessas relações pode ser difícil.

Sophos X-Ops Insight

O impacto financeiro das violações de identidade

As organizações que sofreram uma violação de identidade bem-sucedida incorreram em custos significativos de remediação. O custo médio global de recuperação foi de US$ 1.637.363, e a mediana foi de US$ 750.000. Das organizações afetadas, 73% estimaram custos de US$ 250.000 ou mais, e quase um quarto (23,7%) situou-se na faixa de US$ 500.000 a US$ 1 milhão.

Distribuição de custos



Qual é a sua estimativa do custo total para a sua organização para corrigir a violação de identidade? Base: a organização não conseguiu impedir a violação de segurança. n=510.

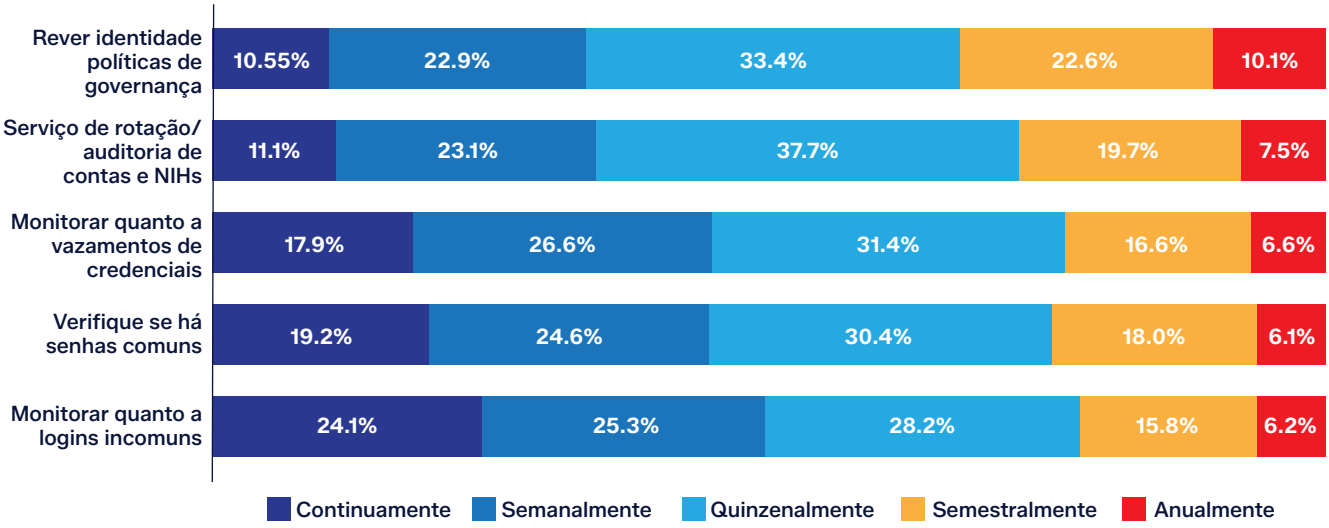
Custo por tamanho da organização

Tamanho da organização	Média de custo	Mediana de custo
100-250 funcionários	US$ 1.125.562	US$ 375.000
251-500 funcionários	US$ 1.978.043	US$ 750.000
501-1,000 funcionários	US$ 1.009.205	US$ 375.000
1.001-3.000 funcionários	US$ 1.907.594	US$ 750.000
3.001-5.000 funcionários	US$ 2.452.929	US$ 750.000

Qual é a sua estimativa do custo total para a sua organização para corrigir a violação de identidade? Base: a organização não conseguiu impedir a violação de segurança. n=510.

Higiene da segurança de identidade

A pesquisa analisou cinco atividades básicas de gerenciamento de identidades e a frequência com que as organizações as realizam. Os resultados revelam lacunas significativas entre as melhores práticas e a realidade — lacunas que aumentam a exposição a ataques de identidade.



Com que frequência a sua organização realiza as seguintes atividades de gerenciamento de identidades? n=5.000

O monitoramento de tentativas de login suspeitas é a atividade mais comum realizada em tempo real (24,1% de forma contínua); no entanto, mesmo assim, mais da metade das organizações (50,6%) não realiza mais de uma verificação a cada três meses. No que diz respeito à rotação ou à auditoria de identidades não humanas — uma atividade fundamental, uma vez que esta é a segunda causa primária individual de violações de segurança —, apenas 34,3% realizam rotação e auditoria de identidades semanalmente ou com maior frequência.

A revisão das políticas de governança de identidade é a atividade realizada com menor frequência de forma contínua (10,5%), sendo que um terço das organizações (33,3%) revê essas políticas no máximo trimestralmente e 22,6% apenas a cada seis meses. Dado que as ameaças à identidade estão evoluindo rapidamente, as revisões anuais, semestrais e mesmo trimestrais deixam lacunas perigosas.

IA agêntica: acelerando o problema com NHI

A IA Agêntica tornou o desafio do gerenciamento de NHI exponencialmente mais difícil: mais identidades, criadas mais rapidamente, com acesso mais amplo e com muito menos supervisão humana. Principais desafios com NHI:

- **Os agentes de IA multiplicam NHIs automaticamente**
  Todo agente de IA precisa de sua própria identidade e credenciais. Fundamentalmente, os agentes têm total autonomia para criar novos agentes para realizar subtarefas, cada um deles gerando mais credenciais sem nenhuma intervenção ou supervisão humana.
- **Os agentes de IA exigem acesso amplo e persistente**
  Para desempenhar suas funções, os agentes de IA precisam interagir com diversos sistemas: calendários, bancos de dados, CRMs, repositórios de arquivos e APIs. Ao contrário das contas de usuários, esses direitos de acesso raramente expiram e raramente são auditados.
- **Os agentes de IA são mais difíceis de monitorar do que NHIs tradicionais**
  Uma conta de serviço de backup executa a mesma tarefa à mesma hora todas as noites, o que é fácil de monitorar. Os agentes de IA, por outro lado, tomam decisões autônomas, agem de forma imprevisível e operam 24 horas, o que torna muito difícil perceber quando algo está errado.
- **Os agentes de IA de terceiros acarretam riscos desconhecidos**
  A pesquisa mostra que quando as organizações utilizam recursos de agentes de IA de terceiros, elas herdam todas as credenciais e permissões de acesso a esses agentes, embora com visibilidade limitada sobre o nível de segurança com que foram desenvolvidos ou sobre o que podem acessar.
- **As regras de segurança não foram criadas para agentes de IA**
  A maioria das estruturas de segurança de identidade foi criada para usuários humanos e contas de máquinas simples. Elas não levam em consideração os agentes capazes de criar, delegar e revogar autonomamente suas próprias credenciais no meio do fluxo de trabalho, o que deixa uma lacuna significativa na governança.

A IA agêntica é um dos principais motivos pelos quais a segurança de NHI passou a ocupar o topo da agenda do CISO.

Consequências de um gerenciamento deficiente de identidades não humanas

Conforme já foi mencionado, o gerenciamento deficiente de identidades não humanas (NHI) foi a causa primária em 40,6% dos ataques bem-sucedidos. Ao analisar mais a fundo, os dados revelam que o comprometimento de NHIs agrava drasticamente as consequências financeiras das violações.

Mais notavelmente, as organizações com um gerenciamento deficiente de NHI são consideravelmente mais suscetíveis a roubos financeiros (nos quais os adversários desviaram pagamentos de contas), +27,9% acima da média, e a extorsões (nas quais os atacantes exigem dinheiro mediante ameaças), +24,4% acima da média. As únicas categorias em que as organizações com gerenciamento deficiente de NHI tiveram um desempenho ligeiramente melhor do que a média foram o roubo de dados e ransomware, embora as diferenças sejam mínimas.

Consequência	% do total de organizações vítimas de violação	% de organizações vítimas de violação com gerenciamento de não humanos deficiente	% de variação com gerenciamento de identidade não humana deficiente
Roubo de dados – invasores roubaram dados sensíveis	48.8%	47.8%	-2.1%
Ransomware – credenciais roubadas utilizadas para ajudar na execução do ataque de ransomware	48.4%	46.4%	-4.1%
Extorsão – invasores exigiram dinheiro com ameaças	43.9%	**54.6%**	**+24.4%**
Sabotagem – invasores utilizaram credenciais para causar danos à organização	30.0%	33.8%	+12.7%
Roubo financeiro – desvios de pagamentos	28.0%	**35.8%**	**+27.9%**
Roubo financeiro – desvio de dinheiro de contas	25.5%	29.9%	+15.7
Resumo: Roubo financeiro (em qualquer forma)	**46.7%**	**57.0%**	**+22%**

Quais foram as consequências dessa violação de identidade para a sua organização? Base: a organização não conseguiu impedir a violação de segurança. n=510 (todas as violações), n=207 (violações envolvendo NHI)

Dado o crescente impacto financeiro de identidades NHI fracas, não é de se surpreender que as organizações com um gerenciamento deficiente de NHI relatem custos globais de recuperação significativamente mais elevados decorrentes de violações de identidade, ficando quase US$ 150.000 acima da média.

Custo médio para se recuperar de violações de identidade

Existe uma correlação clara entre a higiene deficitária de NHI e a propensão a sofrer uma violação relacionada a NHI. Embora um terço (34%) de todas as organizações faça rotação ou auditoria das contas de serviço e NHI de forma contínua ou semanal, esse número cai para um quarto (24%) entre aquelas cuja violação foi causada por NHIs comprometimentos.

Conclusão

Os resultados desta pesquisa não deixam margem para complacência. As violações relacionadas à identidade afetaram mais de 7 em cada 10 organizações no último ano, com uma média de mais de três incidentes por empresa afetada. Esse não é um risco teórico nem um problema restrito a setores ou regiões específicas. Trata-se de uma ameaça universal e generalizada que afeta organizações de todos os tamanhos, setores e regiões. Os dados mostram que os ataques à identidade são a porta de entrada pela qual o ransomware, o roubo de dados e a extorsão se infiltram nas organizações: 67% das vítimas de ransomware atribuíram o incidente diretamente ao comprometimento de identidade.

Quando os ataques à identidade são bem-sucedidos, o impacto é grave e com múltiplas vertentes. Quase metade das organizações vítimas de violação sofreu roubo de dados ou ataque de ransomware, e o custo médio de remediação, de US$ 1,64 milhão, torna cada incidente um evento financeiro substancial.

As causas primárias apontam para deficiências sistêmicas: erros humanos (42,7%), gerenciamento deficiente de identidades não humanas (40,6%) e visibilidade insuficiente das permissões de aplicativos de terceiros (35,7%) são problemas que podem ser resolvidos, mas apenas com investimento e atenção contínuos. O fato de as organizações de menor porte terem quase o dobro de chances de não detectar de ataques em comparação com as de maior porte destaca uma disparidade em matéria de segurança cibernética que exige a atenção da comunidade de segurança.

Talvez o mais preocupante seja o estado das práticas de higiene e manutenção da segurança de identidade. Apenas cerca de um quarto das organizações monitora continuamente atividades incomuns de login, e menos de uma em cada três altera regularmente as credenciais não humanas — exatamente os pontos fracos que os invasores exploram.

As organizações precisam reconhecer que a segurança de identidade não é um projeto com começo e fim, mas, sim, uma disciplina operacional contínua. Aqueles que a encararem dessa forma estarão em uma posição muito mais favorável para se defender contra as ameaças que marcaram o ano de 2025 e que continuarão a se intensificar em 2026.

Recomendações

Conforme demonstrado pela pesquisa, uma segurança de identidade robusta é um elemento essencial de uma estratégia eficaz de mitigação de riscos cibernéticos. Para reduzir a exposição a ataques relacionados à identidade, as organizações devem procurar implementar uma defesa multicamada, tanto para identidades humanas quanto para identidades não humanas. Comece pelas Etapas essenciais e avance até as Etapas recomendadas seguindo um programa de melhoria contínua.

Etapas essenciais

Identidades humanas

- Exija a autenticação multifator (MFA) para todas as contas de usuário.
- Use credenciais diferentes para operações com e sem privilégios.
- Implemente o bloqueio de conta e a proteção contra ataques de força bruta.
- Centralize o gerenciamento de identidades com logon único (SSO).
- Certifique-se de que o treinamento de conscientização de seus usuários reflita as técnicas mais recentes de phishing e roubo de credenciais.

Identidades não humanas

- Faça um inventário e classifique todas as identidades não humanas periodicamente.
- Use credenciais de curta duração em lugar de segredos de longa duração.

Identidades humanas e não humanas

- Aplique o princípio do privilégio mínimo.
- Proteja e gerencie as credenciais da maneira correta.
- Desative ou remova identidades inativas o mais rápido possível.
- Imponha um processo formal de desligamento que verifique e cancele o acesso de ex-funcionários aos recursos da empresa.
- Registre e monitore todas as atividades de autenticação e mantenha os logs por pelo menos 30 dias.

Etapas recomendadas

Identidades humanas

- Implemente o Acesso condicional e políticas baseadas no risco.
- Implemente chaves de acesso (por hardware ou software) como seu principal método de autenticação.
- Agrupe as identidades usando protocolos de identidade amplamente aceitos, como o Security Assertion Markup Language (SAML) ou o novo OpenID Connect (OIDC).

Identidades não humanas

- Use a federação de identidades de carga de trabalho em vez de segredos estáticos.
- Adote uma plataforma de gerenciamento de segredos para NHI em grande escala.
- Ative a varredura de segredos nas plataformas compatíveis (GitHub, GitLab).

Identidades humanas e não humanas

- Implante uma solução de Gerenciamento de acesso privilegiado (PAM).
- Adote um modelo de segurança Zero Trust.
- Realize revisões periódicas de acesso e a recertificação de permissões.
- Implemente recursos de Detecção e resposta a ameaças de identidade (ITDR).
- Segmente o acesso à rede por identidade e função.
- Defina e teste um ou mais playbooks de resposta a incidentes de identidade que abordem incidentes relacionados à identidade, como os descritos neste relatório.

Saiba mais

Leia o nosso Guia de Melhores Práticas de Segurança de Identidade

Metodologia

Esta pesquisa foi realizada pela Vanson Bourne em nome da Sophos no primeiro trimestre de 2026. Foram entrevistados 5.000 tomadores de decisão nas áreas de TI e segurança cibernética em 17 países: EUA, Brasil, Chile, Colômbia, México, Reino Unido, França, Alemanha, Itália, Espanha, Suíça, Austrália, Índia, Japão, Cingapura, África do Sul e Emirados Árabes Unidos. Os participantes pertenciam a organizações com 100 a 5.000 funcionários, distribuídas em 15 setores de atividade.

SOPHOS

Para tratar das suas necessidades de segurança de identidade e saber como a Sophos pode ajudar, visite nosso site ou fale com um consultor.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

2026-05-08 PTBR (TA) CRE-5312