RELATÓRIO

A realidade da confiança na segurança cibernética em 2026

Insights de uma pesquisa independente de fornecedores realizada com 5.000 líderes de TI e segurança

SOPHOS

Introdução

Quando as organizações escolhem um fornecedor de segurança cibernética, estão colocando sua resiliência operacional crítica — pessoas, dados e receita — nas mãos desse fornecedor.

No entanto, apesar dessa dependência, a maioria das organizações não confia nos fornecedores dos quais depende para garantir sua segurança, de acordo com uma nova pesquisa da Sophos.

Para compreender a realidade da confiança em segurança cibernética, a Sophos encomendou uma pesquisa global independente e imparcial em relação a fornecedores, realizada com 5.000 tomadores de decisão nas áreas de TI e segurança em 17 países. Realizada pela Vanson Bourne, uma empresa especializada em pesquisas, a pesquisa oferece um panorama realista e estatisticamente significativo de como se constrói e se perde a confiança entre compradores e fornecedores de segurança cibernética.

5.000

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

Principais lições aprendidas

Falta confiança. Apenas 5% dos líderes de TI afirmam que tanto eles quanto suas organizações depositam total confiança em seus fornecedores de segurança cibernética.

Evidência verificada é um fator essencial da confiança. As equipes de TI e a alta direção concordam que elementos verificáveis da maturidade em segurança cibernética são o principal indicador de confiabilidade.

Avaliar a confiabilidade dos fornecedores continua sendo um desafio. 79% das organizações consideram difícil avaliar a confiabilidade de novos fornecedores de segurança cibernética, enquanto 62% consideram difícil avaliar seus fornecedores atuais. Os entrevistados citaram vários fatores que reduziram a confiança nos fornecedores, sendo o principal deles o fato de que as informações fornecidas pelos fornecedores não eram objetivas ou detalhadas o suficiente.

Essa falta de confiança tem consequências. 51% dos entrevistados afirmam que a falta de confiança gera ansiedade de que a organização esteja mais propensa a sofrer um incidente cibernético grave.

Os profissionais e a liderança nem sempre estão de acordo. 78% dos entrevistados afirmam que sua equipe de TI e a alta direção ou conselho administrativo têm opiniões divergentes sobre a confiabilidade dos fornecedores de segurança cibernética da organização. Quase um terço das empresas que responderam à pesquisa da Sophos afirma que essa divergência ocorre “com frequência”.

É difícil avaliar a confiabilidade

Apenas 5% dos líderes de TI afirmam que tanto eles quanto suas organizações depositam total confiança em seus fornecedores de segurança cibernética.

Quando você conta com seu fornecedor de segurança cibernética para manter sua rede protegida e suas operações em pleno funcionamento, a confiança é fundamental. Os provedores de segurança cibernética são aqueles que protegem a sua empresa 24 horas por dia, 7 dias por semana, à noite e nos finais de semana, e quando os membros da equipe de TI estão de férias. Para os proprietários de pequenas empresas, que muitas vezes não dispõem de uma equipe de TI dedicada, os produtos ou serviços de segurança cibernética podem atuar como se fossem um funcionário da empresa.

Antes que as organizações possam decidir em quem confiar, elas enfrentam um desafio ainda mais fundamental: simplesmente avaliar a confiabilidade de um fornecedor.

De acordo com a pesquisa, 79% dos entrevistados afirmam que é difícil avaliar a confiabilidade de novos fornecedores ou parceiros de segurança cibernética, o que destaca uma dificuldade generalizada em comparar produtos, validar alegações e compreender se um possível provedor pode realmente proteger a empresa. 62% também têm dificuldade em avaliar a confiabilidade dos fornecedores com os quais já trabalham — um indício de que as lacunas de confiança não desaparecem após a assinatura do contrato (Figura 1).

79%

das empresas entrevistadas afirmaram que é difícil avaliar a confiabilidade de novos fornecedores e parceiros de segurança cibernética

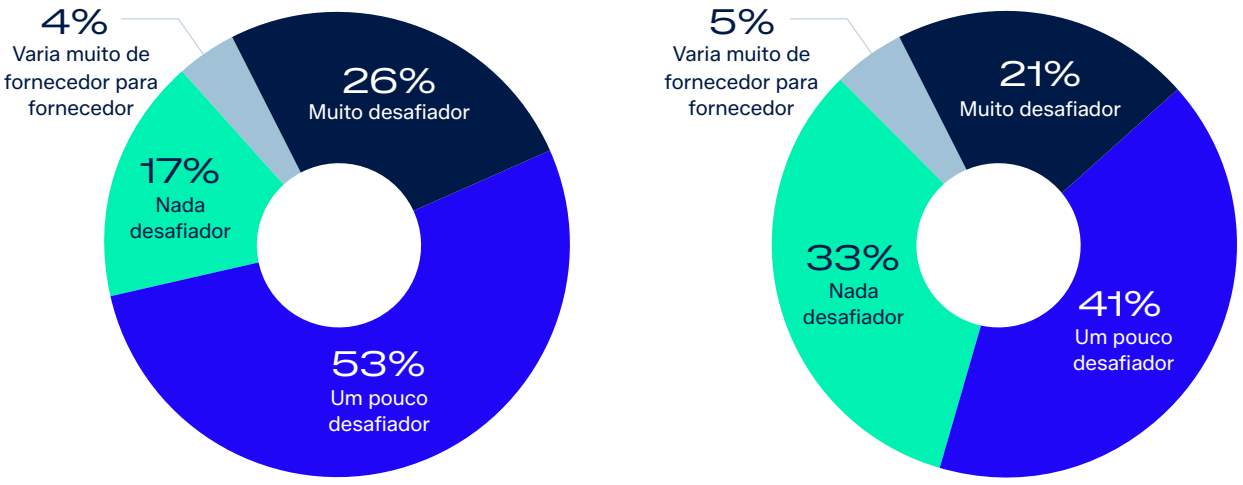

Figura 1: Em geral, até que ponto é difícil para a sua organização avaliar a confiabilidade dos fornecedores e parceiros de segurança cibernética? n=5.000

Obstáculos à avaliação da confiança

Os entrevistados apontaram vários obstáculos à confiança, a maioria deles relacionada à transparência. Muitos têm dificuldade em interpretar as alegações dos fornecedores, avaliar os detalhes técnicos ou encontrar as informações necessárias para tomar decisões com segurança.

Quase metade (47%) afirma que as informações dadas pelos fornecedores não são objetivas ou detalhadas o suficiente, e 45% consideram essas informações difíceis de interpretar ou compreender. Outros 43% admitem não possuir as competências ou os conhecimentos necessários para avaliar os fornecedores de forma eficaz, 41% se deparam com informações contraditórias e 38% têm dificuldade simplesmente em encontrar as informações de que necessitam (Figura 2).

Figura 2: Por que sua organização tem dificuldade em avaliar a confiabilidade dos fornecedores de segurança cibernética? n=4.483

A principal diferença entre as pequenas e médias empresas (com menos de 250 funcionários) e as grandes empresas (com mais de 1.000 funcionários) é que as pequenas e médias empresas tendem muito mais a carecer das competências ou dos conhecimentos necessários para avaliar de forma eficaz a confiabilidade dos fornecedores — as PMEs apontaram essa questão como um problema 8% a mais do que os entrevistados das grandes empresas (Figura 3).

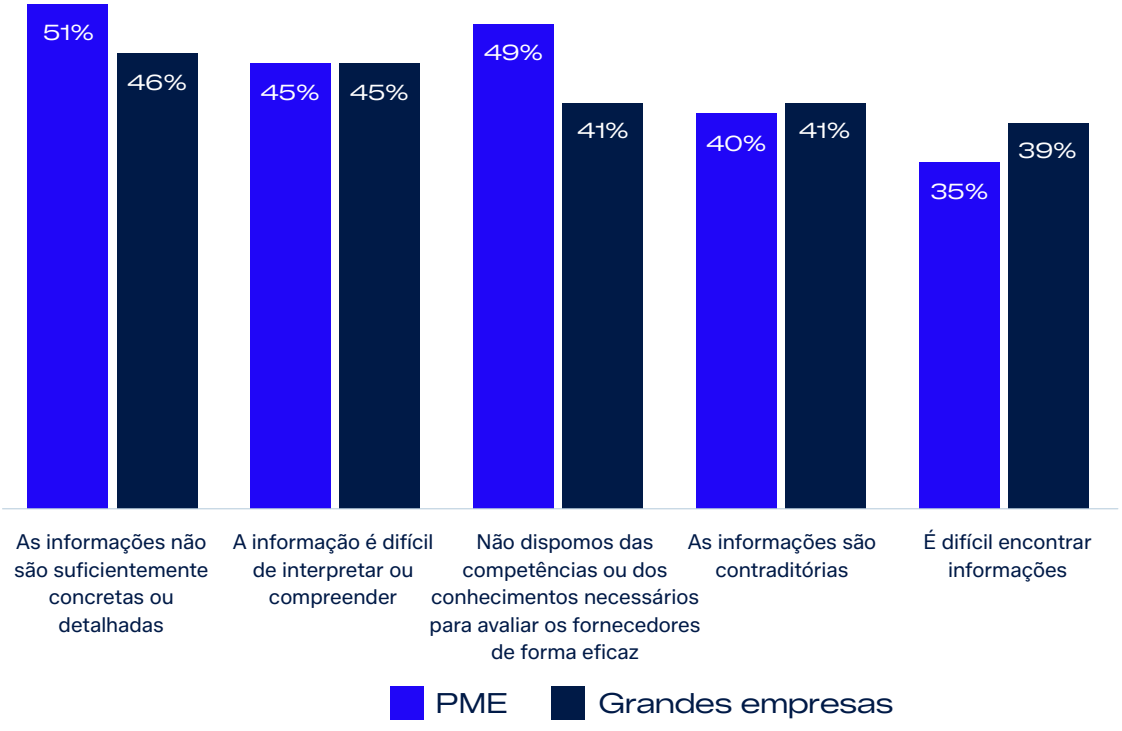

Figura 3: Por que sua organização tem dificuldade em avaliar a confiabilidade dos fornecedores de segurança cibernética? n=504 (PMEs), 2.260 (grandes empresas).

A falta de confiança tem consequências

Esta pesquisa quantifica o impacto da falta de confiança entre um fornecedor de segurança e seus clientes, demonstrando que se trata de uma questão significativa sob vários aspectos. Quando questionados sobre o impacto de não terem total confiança em seus fornecedores de segurança cibernética, os entrevistados destacaram uma combinação de consequências emocionais e operacionais:

- **51%** relatam uma preocupação crescente de que suas organizações possam sofrer um incidente cibernético grave.
- **45%** afirmam que isso os torna mais propensos a mudar de fornecedor — um processo dispendioso e conturbado para a maioria das organizações.
- **42%** observam um aumento nos requisitos de supervisão.
- **41%** relatam menos tranquilidade em relação à postura de segurança cibernética.
- **38%** manifestam preocupação de que eles próprios ou suas organizações possam ter feito uma escolha incorreta de fornecedor.

Esses impactos relatados vêm somar-se às exigências operacionais já impostas às equipes de TI e de segurança cibernética.

Avaliações divergentes entre a equipe de TI e a liderança

Outro desafio crítico é a falta de sintonia entre as pessoas que utilizam as ferramentas de segurança cibernética no dia a dia e aquelas que aprovam os contratos. 78% dos entrevistados afirmam que sua equipe de TI e a alta direção ou o conselho administrativo têm opiniões divergentes sobre a confiabilidade de seus fornecedores de segurança cibernética, e quase um terço afirma que essas divergências ocorrem "frequentemente" (Figura 4).

Os entrevistados indicaram que a alta direção continua fortemente envolvida nas decisões de compra. Apenas 1% das organizações informou que o conselho de administração ou a alta direção não desempenha nenhum papel nas decisões de compra relacionadas à segurança cibernética.

1%

das organizações pesquisadas disse que a alta direção não desempenha nenhum papel nas decisões de compra relacionadas à segurança cibernética.

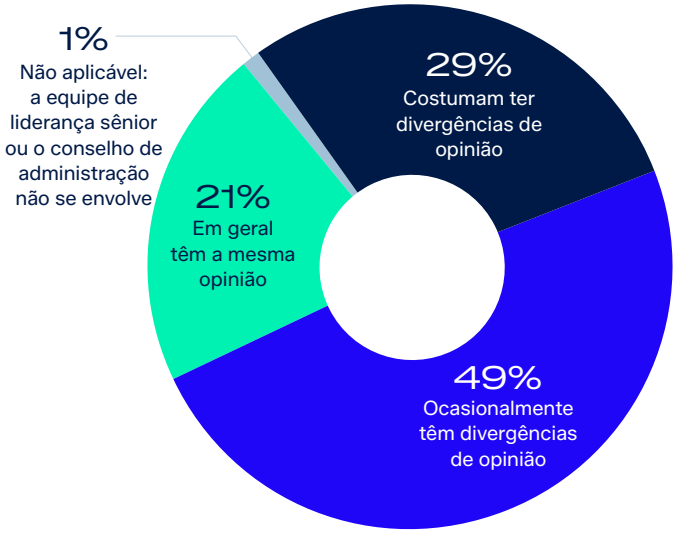

Figura 4: A equipe de TI e a alta direção ou conselho administrativo têm divergências de opinião quanto à confiabilidade dos fornecedores de segurança cibernética da sua organização? n=5.000.

Como construir confiança em segurança cibernética

Os entrevistados indicaram que práticas de segurança transparentes e baseadas em evidências são fundamentais para construir confiança. As organizações buscam fornecedores que inspirem confiança por meio da transparência, da clareza e de práticas de segurança comprovadas.

Tanto entre a alta direção quanto entre as equipes de TI, os "elementos verificáveis que indicam maturidade em segurança cibernética" foram apontados como o principal fator de confiança nos fornecedores de segurança cibernética. Esses tipos de evidências incluem programas de recompensa por bugs, um Centro de Confiança público, alertas detalhando vulnerabilidades em seus produtos (juntamente com a forma como realizaram a correção), avaliações de terceiros e certificações.

"A transparência e a comunicação oportuna durante incidentes e divulgações" também foram consideradas o segundo fator mais importante para os membros da direção e o terceiro entre os membros da equipe de TI.

Fatores de confiança nos fornecedores de segurança cibernética

Drivers	Conselho/ direção	Equipe de TI/ cibernética	Fatores que influenciam
Fatores primários	nº1	nº1	Elementos verificáveis que indicam maturidade em segurança cibernética, por exemplo: programas de recompensa por bugs, Centro de Confiança, consultoria, avaliações de terceiros, certificações
	#2	3º	Transparência e comunicações oportunas durante incidentes e divulgações
	3º	4º	Comentários de especialistas após incidentes cibernéticos de grande repercussão, por exemplo, menções na imprensa ou na televisão
	4º	#2	Entrega consistente de serviços e produtos de segurança cibernética de alta qualidade
	#5	#5	Avaliação em relatórios de analistas, por exemplo, Gartner Magic Quadrant
Fatores secundários	#6	#9	Transparência nos procedimentos de segurança interna
	#7	#7	Desempenho em testes independentes, por exemplo, MITRE, SE Labs
	#8	#6	Suporte ágil e confiável
	#9	#8	Recomendação do seu revendedor/parceiro de segurança cibernética
Fatores terciários	#10	#13	Qualidade das publicações de pesquisas sobre ameaças
	#11	#12	Cobertura na imprensa financeira e comercial
	#12	#11	Experiência de outras pessoas (colegas/clientes)
	#13	#10	Experiência pessoal

Quais são os fatores que mais influenciam ou influenciariam o nível de confiança da alta direção ou do conselho de administração em um fornecedor de segurança cibernética? Respostas classificadas em primeiro
Quais são os fatores que mais influenciam ou influenciariam o nível de confiança da equipe de TI/segurança cibernética em um fornecedor de segurança cibernética? Respostas classificadas em primeiro

O compromisso da Sophos em conquistar a confiança de nossos clientes e parceiros

Na Sophos, sabemos que a confiança se conquista, não se ganha, simplesmente, e trabalhamos para construir essa relação de confiança dia após dia, com transparência, integridade e o firme propósito de proteger sua segurança e privacidade.

No centro de nossos esforços está o Sophos Trust Center, onde publicamos alertas de segurança, documentamos vulnerabilidades e remediações para nossos produtos, descrevemos nossa postura de segurança e compartilhamos como protegemos os dados dos clientes.

Essa transparência também fica evidente na investigação "Pacific Rim" do Sophos X-Ops, que documentou publicamente uma campanha de cinco anos conduzida por agentes de ameaça sediados na China e compartilhou táticas, técnicas e procedimentos (TTPs) detalhados, indicadores de comprometimento (IOCs) e orientações defensivas para ajudar as organizações a fortalecer a resiliência em todo o setor.

Ao revelar atividades sofisticadas de grupos patrocinados por Estados, ao colaborar com governos e outros fornecedores e ao ser franca tanto sobre seus pontos fortes quanto sobre suas fraquezas, a Sophos reforça que a confiança é algo que se conquista diariamente por meio da honestidade, da responsabilidade e do compromisso com a proteção do ecossistema digital.

Saiba mais

Para obter mais informações sobre o nosso compromisso com a promoção da confiança e sobre os recursos que disponibilizamos para ajudar a avaliar a confiança na Sophos, acesse o Trust Center ou entre em contato com o seu parceiro ou representante da Sophos.

SOPHOS

Para obter mais informações, acesse o Trust Center ou entre em contato com seu parceiro ou representante da Sophos.

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

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