



Entre a intenção e a consequência

O que os dados de 2026 revelam sobre a distância entre avaliar fornecedores e reduzir risco de terceiros

Uma leitura cruzada do Verizon DBIR 2026, do SecurityScorecard Supply Chain Cybersecurity Trends 2026 e do ProcessUnity/Ponemon State of Third-Party Risk Assessments 2026.

Cinco achados

O que a leitura cruzada dos três estudos permite afirmar.

01 O denominador mudou de patamar em duas edições.

Terceiros passaram de 15% para 30% e agora 48% das brechas confirmadas. Não é tendência gradual: é mudança de categoria.

02 A confiança dos gestores não se apoia em avaliação — apoia-se em inventário incompleto.

90% confiam que operariam normalmente durante um incidente em fornecedor; 78% admitem cobrir menos de metade do próprio ecossistema.

03 Quando se mede de dentro do fornecedor, o controle declarado e o controle existente divergem.

37% das organizações tinham conta administrativa sem MFA em IaaS. A pergunta “você exigem MFA?” tem resposta afirmativa em quase todo questionário.

04 O programa existe, o resultado não é medido.

A maioria das organizações não aplica nenhuma métrica para verificar se o programa de terceiros de fato reduz risco — e ainda assim reporta 12 incidentes de terceiros por ano.

05 A conversa para na brecha; o negócio para na interrupção.

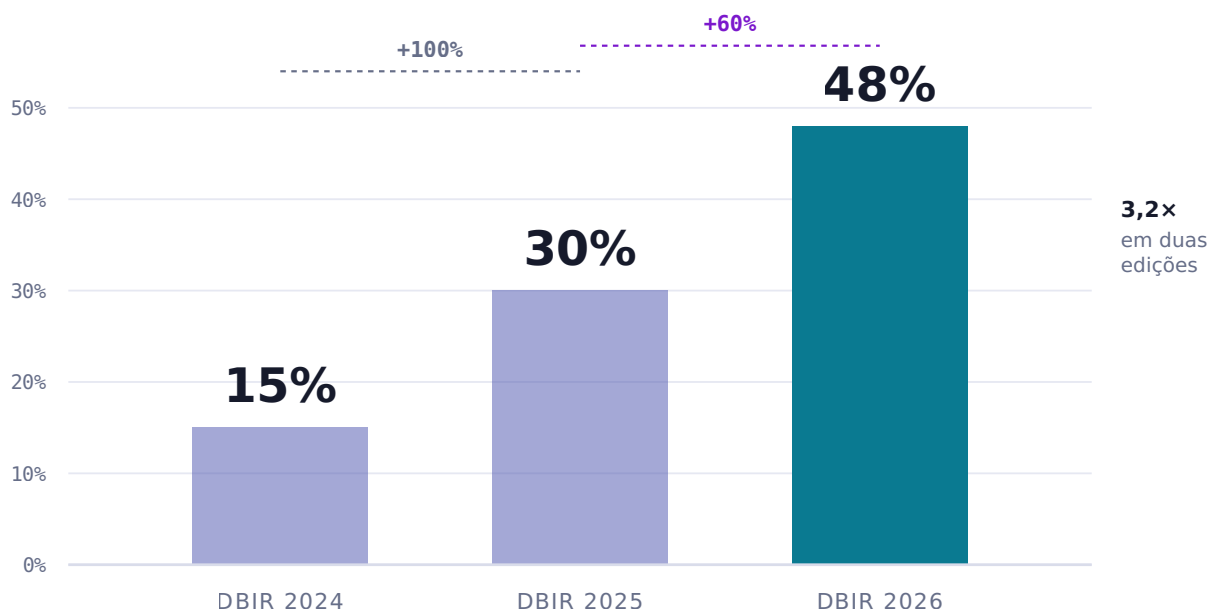
Nenhum dos três estudos avança da violação de dados para a indisponibilidade de produto ou serviço. É exatamente aí que o inventário incompleto cobra o preço mais alto.

SEÇÃO 01

O denominador mudou

Terceiros deixaram de ser uma categoria de risco para virar o meio de acesso predominante.

Três edições consecutivas do Verizon Data Breach Investigations Report descrevem a mesma curva: 15%, 30%, 48%. O envolvimento de terceiros em brechas confirmadas triplicou em duas edições, com alta de 60% apenas no último ano. A base de 2026 é a maior já publicada pela série — mais de 22 mil brechas confirmadas em 145 países.



Percentual das brechas confirmadas com envolvimento de terceiros.

Fonte: Verizon DBIR, edições 2024, 2025 e 2026 (2026: 22.000+ brechas confirmadas, 145 países).

O número merece uma leitura cuidadosa antes de virar manchete. O relatório não atribui o salto a uma causa única, e parte do movimento pode refletir melhoria de método: nesta edição a Verizon passou a contar com dados coletados de dentro dos ambientes cloud dos próprios terceiros, e não apenas com observação externa. Reconhecer isso não enfraquece o argumento — fortalece. O que sustenta este relatório não é a magnitude do salto, e sim o fato de a causa raiz ser, em cada caso, um controle nomeável.

Em brechas de pequenas e médias empresas, terceiros estiveram envolvidos em 55% dos casos. O problema é mais agudo justamente onde não existe equipe dedicada a gerir risco de terceiros.

Um caso brasileiro

Em 1º de julho de 2025, a C&M Software — provedora de serviços de tecnologia da informação que conecta ao Sistema de Pagamentos Brasileiro instituições sem ligação direta com o Banco Central — teve sua infraestrutura comprometida. Em uma janela de poucas horas, contas reserva de seis instituições foram esvaziadas. As estimativas divulgadas variaram entre R\$ 400 milhões e R\$ 1 bilhão, com R\$ 800 milhões como número mais citado. Entre as instituições atingidas estavam BMP, Banco Paulista, Credsystem e Banco Carrefour.

A causa raiz não foi uma vulnerabilidade sofisticada. Foram credenciais legítimas de um funcionário da provedora, vendidas por R\$ 15 mil. Do ponto de vista das instituições clientes, não havia controle interno a acionar: o acesso partiu de dentro do fornecedor, com credencial válida, pelo canal previsto para aquele tráfego.

O desdobramento é o que interessa a este relatório. O Banco Central impôs suspensão cautelar à C&M, e a interrupção alcançou instituições que sequer haviam sido alvo do desvio — todas as que dependiam daquela conexão para operar. A brecha aconteceu em um fornecedor; a indisponibilidade aconteceu no ecossistema. É a distância entre a seção 03 e a seção 06 deste relatório, percorrida em um único evento de poucas horas.

Nenhum questionário respondido pela C&M teria mudado o desfecho. Uma pergunta sobre concentração — quantas das nossas conexões críticas passam por este único provedor, e qual é a alternativa — teria.

SEÇÃO 02

O paradoxo da confiança

Noventa por cento de confiança sobre menos de cinquenta por cento de visibilidade.

O levantamento do SecurityScorecard registra duas afirmações que, colocadas lado a lado, não fecham. Noventa por cento dos líderes se declaram confiantes de que o negócio seguiria operando normalmente caso um fornecedor sofresse um incidente de segurança. Setenta e oito por cento admitem que seus programas internos cobrem menos de metade do ecossistema de fornecedores, incluindo terceiras, quartas e quintas partes.

Confiam que o negócio seguiria operando durante um incidente em fornecedor



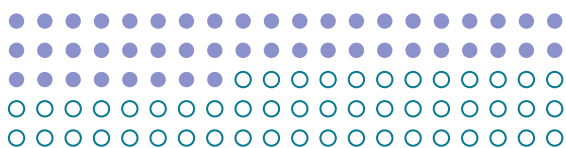
Declaram preocupação profunda com risco de cadeia de suprimentos



Admitem cobrir menos de 50% do ecossistema (3ª, 4ª e 5ª partes)



O DENOMINADOR REAL — 100 FORNECEDORES, MENOS DE 50 SOB ALGUM OLHAR



Fonte: SecurityScorecard, 2026 Supply Chain Cybersecurity Trends Report.
Ilustração do denominador; o corte declarado no estudo é “menos de 50%”.

A leitura mais defensável não é que os gestores estejam sendo otimistas. É que a confiança e a preocupação estão medindo objetos diferentes. A preocupação — declarada por 86% da mesma amostra — olha para o noticiário e para o setor. A confiança olha para uma lista. E a lista está incompleta.

Some-se a isso a natureza do que é usado para formar essa confiança: 67% recorrem a auditorias de segurança e 46% a monitoramento periódico mensal ou trimestral, mesmo reconhecen-

do ameaças conduzidas por inteligência artificial como o principal risco de cadeia. Instrumento de fotografia sendo usado para acompanhar um filme.

Uma ressalva antes de seguir

O relatório do SecurityScorecard descreve a amostra como “centenas” de profissionais, sem divulgar o número exato nem a distribuição por região, porte ou setor. Isso limita o que se pode afirmar a partir dele: os percentuais indicam a direção e a ordem de grandeza do fenômeno, não sua magnitude precisa em um mercado específico. O contraste com o estudo conduzido pelo Ponemon Institute, com 1.465 respondentes identificados por função e região, é deliberado — as duas fontes são usadas aqui para triangular, nunca para somar.

SEÇÃO 03

O que se vê de dentro

A diferença entre o controle declarado e o controle existente, quantificada.

A mudança metodológica mais relevante do DBIR 2026 não está no total, e sim na origem do dado. Ao olhar de dentro dos ambientes cloud dos terceiros, o relatório deixa de registrar o que o fornecedor diz sobre si mesmo e passa a registrar o que existe.

MEDIDO DE DENTRO DOS AMBIENTES CLOUD DOS PRÓPRIOS TERCEIROS — NÃO POR QUESTIONÁRIO



“Autenticação insegura — ausência de MFA, rotação inadequada de credenciais — ou falta de aplicação de menor privilégio para usuários ou contas de serviço.” — causa raiz, DBIR 2026

Fonte: Verizon DBIR 2026, seção de terceiros.

Esses achados são, nas palavras da própria análise, inteiramente visíveis para quem olha e quase inteiramente invisíveis para quem depende de questionário autodeclarado. É uma distinção operacional, não retórica: nenhum dos três números acima poderia ter sido produzido por um formulário respondido pelo fornecedor.

Por que o certificado não fecha a lacuna

Um fornecedor com relatório de auditoria limpo pode manter acesso a dados pessoais de clientes, a registros financeiros ou a propriedade intelectual por meio de uma conexão que ninguém revisa há dois anos. O certificado atesta um escopo, em um período, sob critérios definidos por quem contratou a auditoria. Ele não atesta a configuração de hoje da conta que tem acesso ao seu ambiente.

O que uma verificação causal exige

O requisito não é substituir o questionário por uma varredura. É reconhecer que cada um dos três degraus abaixo responde a uma pergunta que o anterior deixa aberta, e que parar no primeiro é o que produz a distância medida acima.

Primeiro, evidência produzida em conjunto, não enviada e cobrada. O modelo de remeter o questionário e aguardar cria um incentivo perverso: a resposta é otimizada para encerrar a pendência, não para descrever a realidade. Quando a avaliação é construída junto ao fornecedor, com escopo negociado e prazo acordado, o que chega é evidência — e o fornecedor tem interesse em que ela esteja correta, porque foi ele quem definiu o que seria demonstrado.

Segundo, análise do que a evidência efetivamente demonstra. Receber um relatório de auditoria não é o mesmo que lê-lo. É preciso verificar qual escopo foi auditado, em que período, sob quais critérios, e quais exceções foram registradas. Um relatório limpo com escopo estreito diz muito pouco sobre o ambiente que efetivamente se conecta ao seu.

Terceiro, verificação técnica não intrusiva do controle no ambiente. É o degrau que fecha o ciclo, porque é o único que transforma controle declarado em controle observado. Não exige acesso privilegiado nem agente instalado: exige uma leitura de configuração acordada com o fornecedor, no escopo que diz respeito à relação — as contas que acessam seus dados, as permissões que essas contas carregam, os fatores de autenticação que as protegem.

Os três degraus são cumulativos. O primeiro sem o segundo produz evidência que ninguém lê. Os dois primeiros sem o terceiro produzem exatamente o programa que os três estudos descrevem: maduro em processo, cego em resultado.

SEÇÃO 04

A física da resposta

Prazo de resposta não é má vontade do fornecedor. É fricção de processo e informação descentralizada.

O estudo conduzido pelo Ponemon Institute com 1.465 líderes e praticantes de risco de terceiros descreve um processo que não fecha no tempo em que o risco se move. Sessenta por cento relatam prazos de resposta de fornecedores entre quatro e mais de doze meses. Vinte e sete por cento dos fornecedores simplesmente não respondem.

ONDE O TEMPO É PERDIDO — DO ENVIO DA AVALIAÇÃO À REMEDIAÇÃO EM CRISE

27% dos fornecedores não respondem à avaliação
PONEMON 2026

60% levam de 4 a mais de 12 meses para responder
PONEMON 2026

55% usam telefone, reunião ou e-mail para falar com o fornecedor durante uma brecha
SECURITYSCORECARD 2026

60% levam 8 dias ou mais para remediar achado de alta severidade
SECURITYSCORECARD 2026

Se o canal já é o e-mail no dia normal, ele continua sendo o e-mail no pior dia.

A leitura corrente atribui esses números a descaso. A leitura mais útil é econômica: o mesmo fornecedor responde a dezenas de questionários por ano, sobre os mesmos controles, em formatos incompatíveis, para interlocutores diferentes de organizações diferentes, sem qualquer remuneração por esse esforço. Os 27% de não-resposta são triagem racional de um custo que ninguém paga.

A descentralização agrava o efeito. A informação sobre um mesmo fornecedor costuma estar repartida entre suprimentos, jurídico, segurança e a área de negócio que efetivamente o utiliza — e nenhuma dessas quatro tem a figura completa. Quando o incidente acontece, a organização descobre que não sabe quem é o ponto de contato técnico do fornecedor, qual o compromisso contratual de recuperação e quais dados estão sob a custódia dele.

Os oito dias para remediar um achado de alta severidade não são medidos em situação normal. São medidos durante uma brecha. Se o canal já é o e-mail no dia comum, ele continua sendo o e-mail no pior dia.

A consequência direta é que qualquer solução que não reduza o custo do lado do fornecedor está tratando sintoma. Reuso de evidência, centro de confiança e canal único de interlocução não são conveniências: são a resposta desenhada para o dado.

SEÇÃO 05

O ponto cego de classificação

Provedor de nuvem é fornecedor. Em muitos programas, não é assim que ele está classificado.

Há uma explicação simples e verificável para o paradoxo da seção 2: parte relevante das dependências críticas nunca entrou na lista de fornecedores. Provedores de nuvem, provedores de identidade, plataformas de e-mail, gateways de pagamento e ferramentas de colaboração entram pela porta do contrato de infraestrutura, não pelo processo de homologação de fornecedores — e por isso não passam por avaliação de terceiros.

O DBIR ajuda a nomear o ponto cego ao separar três arquétipos de terceiro: o fornecedor na cadeia de software, o fornecedor que hospeda os dados e o fornecedor com conexão ativa para dentro do ambiente. Os três cresceram, e os três levam às mesmas causas raiz. O segundo arquétipo é, na maioria das organizações, o provedor de nuvem — o mesmo que quase nunca aparece no inventário de TPRM.

Concentração é risco, não eficiência

Padronizar em uma única plataforma simplifica a operação e concentra a exposição. Quando aplicações críticas, autenticação de usuários e serviços de produtividade dependem do mesmo provedor, uma única indisponibilidade atinge simultaneamente processos que a organização considerava independentes. O critério de escrutínio deveria ser a criticidade da dependência, a substituíbilidade e a concentração geográfica e tecnológica — não o valor econômico do contrato.

É erro de inventário, não erro de julgamento. Inventário de dependência se constrói a partir da pergunta “o que para se isto cair?”, não a partir da lista de contratos do jurídico.

Dez perguntas para testar o próprio inventário

Não há pontuação, e não é um diagnóstico de maturidade. Cada “não” abaixo é um item que falta ao inventário — informação a levantar, não falha a corrigir.

- 01 Sua lista de fornecedores foi construída a partir dos processos de negócio ou da carteira de contratos do jurídico?
- 02 O provedor de nuvem principal está no inventário de terceiros, com avaliação e ciclo de revisão definidos?
- 03 E o provedor de identidade, a plataforma de e-mail e o gateway de pagamento?
- 04 Você consegue nomear as quartas partes dos seus cinco fornecedores mais críticos?
- 05 Cada fornecedor crítico tem um responsável interno nomeado — uma pessoa, não uma área?
- 06 Você sabe quais fornecedores mantêm hoje conexão ativa para dentro do seu ambiente, e com qual nível de privilégio?
- 07 Se o fornecedor mais crítico ficar indisponível por 72 horas, qual processo de negócio para primeiro?
- 08 Existe alternativa contratada ou testada para esse fornecedor, ou apenas identificada no papel?
- 09 O tempo de recuperação declarado por ele já foi confrontado com o tempo que o seu processo efetivamente suporta?
- 10 Existe um canal de contato técnico com esse fornecedor que não seja o e-mail do executivo de conta?

Na prática, a pergunta 4 é a primeira a travar e a pergunta 9 é a mais cara. A 4 revela que o inventário para na primeira camada; a 9 revela que o plano de continuidade nunca foi confrontado com a realidade do fornecedor que ele pressupõe.

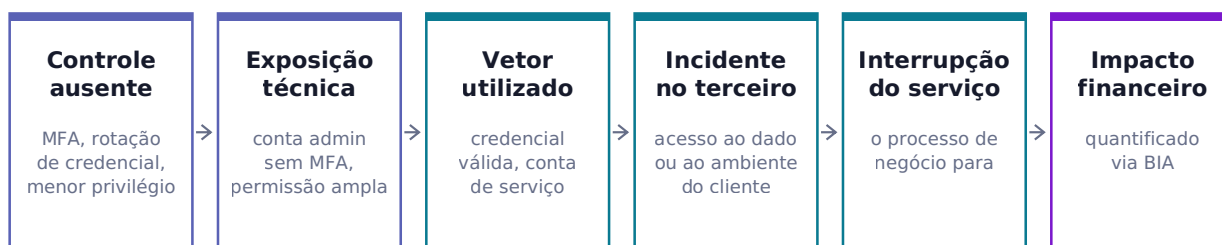
SEÇÃO 06

O elo que falta: da brecha à interrupção

Os três estudos param na violação de dados. O negócio para na indisponibilidade.

Este é o ponto em que a evidência disponível se esgota e a consequência começa. Nenhum dos três levantamentos avança da brecha para a interrupção de produto ou serviço — e é nesse trecho não medido que o inventário incompleto cobra seu preço mais alto.

A CADEIA QUE A NOTA NÃO DESCREVE



O que o questionário pergunta

O que a organização de fato sofre

A avaliação pontual registra a intenção declarada no primeiro quadro. O risco vive nos quatro últimos.

Causas raiz conforme Verizon DBIR 2026; encadeamento até impacto financeiro conforme metodologia Aranis.

A cadeia é direta. Se o inventário de fornecedores está incompleto, a análise de impacto no negócio está errada. Se a análise de impacto está errada, os tempos objetivos de recuperação declarados são ficção. E um plano de continuidade construído sobre tempo de recuperação fictício não falha no papel: falha no dia.

Há ainda uma dependência não declarada em quase todo plano de continuidade. O plano pressupõe a disponibilidade de recursos que a organização não controla — o suporte do fornecedor, o canal de comunicação com ele, a capacidade dele de restaurar dentro do prazo que o processo de negócio exige. Com 55% das organizações dependendo de telefone, reunião e e-mail para falar com o fornecedor durante uma brecha, essa dependência é frágil já no primeiro passo do plano.

Avaliar a segurança do fornecedor sem avaliar a continuidade dele é medir metade da exposição. A maioria dos programas verifica se o fornecedor tem firewall; poucos verificam se ele tem plano de recuperação testado, tempo de

recuperação declarado compatível com o do cliente e comunicação de crise definida.

Pesquisa global recente indica que 42% dos líderes afirmam que a organização não dispõe da infraestrutura e das competências necessárias para gerir esse tipo de disrupção — e que, como as indisponibilidades globais recentes demonstraram, muitas organizações só descobrem a própria exposição durante a crise.

SEÇÃO 07

O que medir

Nove métricas causais. Nenhuma delas é uma nota.

O achado mais incômodo do estudo Ponemon não é o volume de incidentes. É a constatação de que a maioria das organizações pesquisadas não aplica métrica alguma para avaliar se o programa de terceiros reduz risco. Isso não é uma lacuna de reporte: é uma lacuna de decisão.

Sem métrica, três perguntas de conselho ficam sem resposta. Qual é a exposição financeira agregada via terceiros hoje? Se um fornecedor crítico for comprometido amanhã, em quanto tempo conseguimos conter? O que mudou desde o último ciclo — melhoramos, ou apenas reavaliamos?

A tabela a seguir propõe um conjunto mínimo. O critério de seleção foi um só: cada métrica precisa descrever uma causa ou uma capacidade, nunca uma opinião consolidada em pontuação. Os limiares marcados com referência derivam dos estudos citados; os demais são pontos de partida a calibrar por setor e apetite de risco.

#	MÉTRICA	O QUE REVELA	ONDE O DADO NASCE	LIMIAR DE ATENÇÃO
1	Cobertura efetiva do ecossistema	O denominador real da exposição, incluindo quarta e quinta partes	Inventário construído a partir dos processos de negócio	Abaixo de 50% · ref. SecurityScorecard
2	Razão entre controle verificado e controle declarado	A distância entre a intenção registrada e o controle existente	Evidência analisada + verificação técnica no ambiente	Abaixo de 30% · a calibrar
3	Tempo médio de remediação de achado crítico em fornecedor	Capacidade real de remediação, não a declarada em contrato	Ciclo de plano de ação, por severidade	Acima de 8 dias · ref. SecurityScorecard
4	Idade média da evidência em carteira	Validade do que a organização acredita saber sobre o fornecedor	Data de emissão da evidência aceita	Acima de 180 dias · a calibrar
5	Taxa de não-resposta a avaliações	Confiabilidade do inventário e fricção percebida pelo fornecedor	Ciclo de avaliação	Acima de 27% · ref. Ponemon
6	Tempo de ciclo da avaliação, do envio à conclusão	Fricção do processo e descentralização da informação	Registro de início e conclusão por avaliação	Acima de 120 dias · ref. Ponemon
7	Exposição financeira agregada por processo de negócio	Tradução do risco de terceiros para linguagem de conselho	Análise de impacto no negócio ligada à cadeia causal	Acima do apetite declarado

#	MÉTRICA	O QUE REVELA	ONDE O DADO NASCE	
8	Fornecedores críticos sem alternativa viável	Concentração e ausência de estratégia de saída	Mapa de dependência por processo	Qualquer um sem plano de saída
9	Fornecedores críticos cujo tempo de recuperação excede o do processo que sustentam	Continuidade fictícia — o plano não fecha no tempo do negócio	Confronto entre a análise de impacto e o compromisso do fornecedor	Qualquer ocorrência

Nenhuma dessas nove métricas exige tecnologia proprietária para ser adotada. Todas exigem, porém, que o inventário de fornecedores tenha sido construído a partir dos processos de negócio, e não da carteira de contratos.

Nota metodológica e limitações

O que este relatório afirma, o que ele apenas sugere e o que ele não sustenta.

Este relatório é uma leitura cruzada de fontes públicas de terceiros. Não foi conduzida pesquisa primária. As três bases têm naturezas distintas e não são diretamente comparáveis entre si: o DBIR analisa incidentes e brechas confirmadas; os outros dois são levantamentos de percepção e prática declarada, sujeitos a viés de autorrelato.

As bases

O Verizon Data Breach Investigations Report 2026 analisa mais de 31 mil incidentes e mais de 22 mil brechas confirmadas em 145 países, com dados agregados de dezenas de organizações contribuintes. O State of Third-Party Risk Assessments, conduzido pelo Ponemon Institute e publicado pela ProcessUnity, ouviu 1.465 líderes e praticantes de risco de terceiros. O Supply Chain Cybersecurity Trends Report, do SecurityScorecard, descreve a amostra apenas como “centenas” de profissionais, sem divulgar o número exato nem sua distribuição — limitação já registrada na seção 02 e que vale reafirmar aqui.

A ressalva sobre a série histórica

O salto de 30% para 48% não deve ser lido como medida limpa de variação anual. A edição de 2026 do DBIR passou a incorporar dados coletados de dentro dos ambientes cloud dos próprios terceiros, ampliando o que é possível observar. Parte do aumento pode, portanto, refletir melhoria de instrumento e não apenas piora do fenômeno. O relatório não atribui o movimento a uma causa única, e este documento tampouco o faz.

Declaração de interesse

As três fontes primárias são publicadas por organizações com interesse comercial no tema que medem. O mesmo vale para este relatório: a Aranis desenvolve uma plataforma de gestão de risco de terceiros e se beneficia de que o problema aqui descrito seja reconhecido. Os dados citados são públicos e verificáveis nas fontes listadas; a leitura que os conecta é nossa, e deve ser avaliada como argumento, não como achado de pesquisa primária.

Uso de inteligência artificial

Ferramentas de IA foram usadas na pesquisa de fontes, na organização do material e na revisão de texto. Não foram usadas para gerar dados, estimativas ou citações: todo número presente neste relatório foi conferido contra a publicação original. As conclusões, o enquadramento e as nove métricas propostas são de autoria humana e de responsabilidade da Aranis.

Nenhum dos três estudos apresenta correlação entre pontuação de fornecedor e incidência de brecha. A ausência desse dado é, por si só, o achado mais eloquente da série.

FONTES

Referências

Todas as fontes são públicas e verificáveis na data de publicação.

Verizon Business. 2026 Data Breach Investigations Report. Maio de 2026. verizon.com/business/resources/reports/dbir/

SecurityScorecard. 2026 Supply Chain Cybersecurity Trends Report. Março de 2026. securityscorecard.com/resources/research/

ProcessUnity / Ponemon Institute. State of Third-Party Risk Assessments 2026. Janeiro de 2026. processunity.com/resources/

BDO. Managing third-party and cloud dependency risks. 2026. bdo.com.au/insights/cyber-security/

Cobertura de imprensa — caso C&M Software. Exame, Valor Econômico, O Tempo e Mobile Time. Julho de 2025. [reportagens de 2 e 3 de julho de 2025](#)



A avaliação pontual registra intenção. A Aranis mede consequência.

A Aranis é uma plataforma de gestão de risco de terceiros e risco cibernético construída sobre uma cadeia causal: cada controle ausente é ligado à exposição técnica que ele abre, ao processo de negócio que ela ameaça e ao impacto financeiro correspondente. O fornecedor não é penalizado por não ter o controle — é avaliado pela consequência da ausência dele.

- Avaliação conduzida em conjunto com o fornecedor, com evidência analisada criteriosamente
- Verificação técnica não intrusiva no ambiente do fornecedor
- Cobertura de segurança, privacidade, continuidade de negócios e risco de IA no mesmo ciclo
- Caminho de risco e caminho de ataque navegáveis na interface, não apenas na metodologia
- Autoatendimento: você cria a conta e avalia o primeiro fornecedor no mesmo dia

[aranis.ai](#) · crie sua conta e avalie o primeiro fornecedor