SOPHOS

Guia da Sophos para seguro de proteção digital

Como controles cibernéticos robustos podem melhorar a elegibilidade às ofertas de seguro e reduzir o prêmio.

O mercado de seguro de proteção digital continua mudando, e suas exigências mantêm-se acirradas em resposta ao aumento no número e no custo de sinistros nos últimos anos. Embora a maioria das organizações já tenha algum tipo de seguro de proteção digital, muitas começam a notar que o nível da segurança cibernética necessária para se qualificarem para cobertura está mais alto, as apólices estão mais complexas e os prêmios continuam a subir.

Ainda que a cobertura de seguro de proteção digital esteja disponível, os provedores estão mais seletivos sobre para quem querem dar cobertura, evitando sistematicamente as empresas que representam riscos mais altos. Ao investir em defesas cibernéticas robustas, as organizações podem reduzir seus riscos cibernéticos, o que, por sua vez, melhora sua classe de bônus no mercado de seguros. Do acesso facilitado à cobertura até prêmios mais baixos e limites mais altos, defesas cibernéticas robustas oferecem várias vantagens ao segurado.

Este guia oferece uma visão geral do estado do mercado de seguro de proteção digital e explica as diferentes formas em que a segurança cibernética pode afetar o seu seguro de proteção digital de modo positivo. Também detalha as tecnologias e os serviços da Sophos que podem ajudar a diminuir seus riscos cibernéticos e otimizar sua classe de bônus no mercado de seguros.

Documento técnico Sophos. Dezembro, 2023

O básico

Por que ter seguro de proteção digital

O seguro de proteção digital, também chamado de seguro para riscos digitais e seguro de responsabilidade cibernética, protege você do impacto causado pelo crime cibernético (mas não do crime em si). De modo geral, há quatro benefícios básicos em se ter um seguro de proteção digital:

1. **Financeiro.** O seguro cobre os custos no caso de um incidente cibernético
2. **Comercial.** A cobertura do seguro de proteção digital é um requisito cada vez mais presente ao se fazer negócios com muitas organizações
3. **Operacional.** A equipe de seguro oferece acesso imediato a especialistas no caso de um incidente, incluindo peritos forenses de TI, advogados especialistas em privacidade e profissionais de relações públicas
4. **Tranquilidade.** Ter um seguro de proteção digital dá a seus clientes, parceiros, fornecedores e funcionários a tranquilidade e a segurança de que você está pronto e coberto no caso de acontecer um incidente cibernético

Causas de sinistros de seguro de proteção digital

Os sinistros de seguro de proteção digital podem ser acionados por uma ampla gama de incidentes, mas as causas mais frequentes dos sinistros, de acordo com o estudo NetDiligence's Cyber Claims divulgado no Relatório de 2023, são:

1. Ransomware
2. Comprometimento de e-mail corporativo
3. Hackers
4. Roubo de dinheiro
5. Erros cometidos por funcionários[1]

1 Relatório do NetDiligence Cyber Claims Study 2023

O que é coberto pelo seguro de proteção digital

O seguro de proteção digital cobre os custos que incorrem como resultado de um ataque cibernético. Ainda que as apólices individuais variem, em geral, elas cobrem:

- Custos de interrupção do negócio
- Análise forense para identificar a origem do ataque
- Pedidos de resgate e especialistas para negociar o resgate
- Custos para reaver o acesso ou restaurar os dados de backups ou outras fontes
- Custos legais
- Serviços de relações públicas
- Notificação de clientes e/ou órgãos reguladores
- Serviços de monitoramento de crédito para as pessoas afetadas

Ao reunir apólices e comparar custos, vale lembrar que os custos da interrupção dos negócios, como perda de receita ou custos adicionais de trabalho devido ao ataque cibernético, estão incluídos em algumas apólices, mas não em outras.

Na eventualidade de um ataque cibernético, o fornecedor de seguro entrará em ação e fornecerá especialistas para ajudar a lidar com a situação. Para um ataque de ransomware, eles geralmente:

- Apontam um consultor para instruir como tratar da demanda e negociar o resgate
- Identificam o custo mais baixo para restaurar os dados (pagamento de resgate, backups etc.)
- Trazem peritos necessários para lidar com o problema

Cobertura de primeiro beneficiário x terceiros

Muitas apólices incluem a cobertura de primeiro beneficiário e terceiros. Cobertura de primeiro beneficiário engloba os custos diretos associados com a resposta ao ataque, por exemplo, taxas jurídicas, taxas forenses, taxas de notificação ao cliente, taxas de RP e assim por diante. Cobertura de terceiros engloba os custos primários associados com processos judiciais.

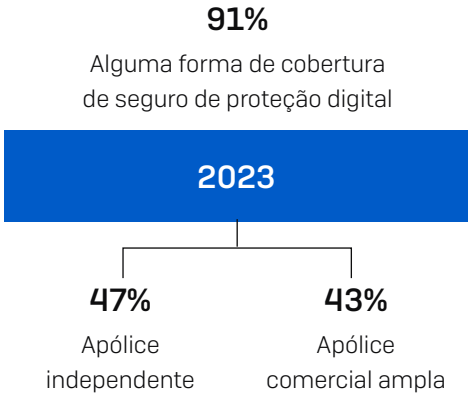
Em uma apólice, podem haver sublimites específicos para a cobertura de primeiro beneficiário, e também para itens específicos da cobertura do primeiro beneficiário. Por exemplo, a cobertura do primeiro beneficiário pode estar limitada a US$ 500.000, o que inclui um limite de US$ 50.000 para custos de RP.

A realidade do seguro de proteção digital

A prevalência do seguro de proteção digital

Ter um seguro de proteção digital hoje é a norma: 91%[2] das organizações tinham alguma forma de seguro de proteção digital em 2023, de acordo com uma pesquisa independente encomendada pela Sophos – um aumento notável em comparação aos 84% registrados em 2020[3], mas alinhado aos 92% das organizações que disseram ter cobertura em 2022. Das organizações que disseram ter cobertura em 2023, algumas tinham apólices de proteção digital independentes (47%) enquanto outras incluíram a cobertura de proteção digital em apólices de seguro comercial mais amplas.

Contudo, esses números não contam toda a história. As apólices variam e nem todas cobrem ransomware, que é a maior causa dos sinistros de seguro de proteção digital. Quase uma em cada dez organizações que tinham cobertura de proteção digital em 2022 não estava assegurada contra ransomware, ficando totalmente suscetível aos altos custos e grandes desafios de recuperar-se desses tipos de ataque.



2 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.
3 O Estado do Ransomware 2021, Sophos

Adoção de seguro de proteção digital por setor

Quando categorizada por setores, a pesquisa revelou que o setor da educação (fundamental e superior) registrou o mais alto nível de cobertura de seguro de proteção digital (96%), embora essas organizações sejam mais propensas a ter a proteção digital como parte de uma apólice de seguro comercial mais ampla do que ter uma apólice independente.

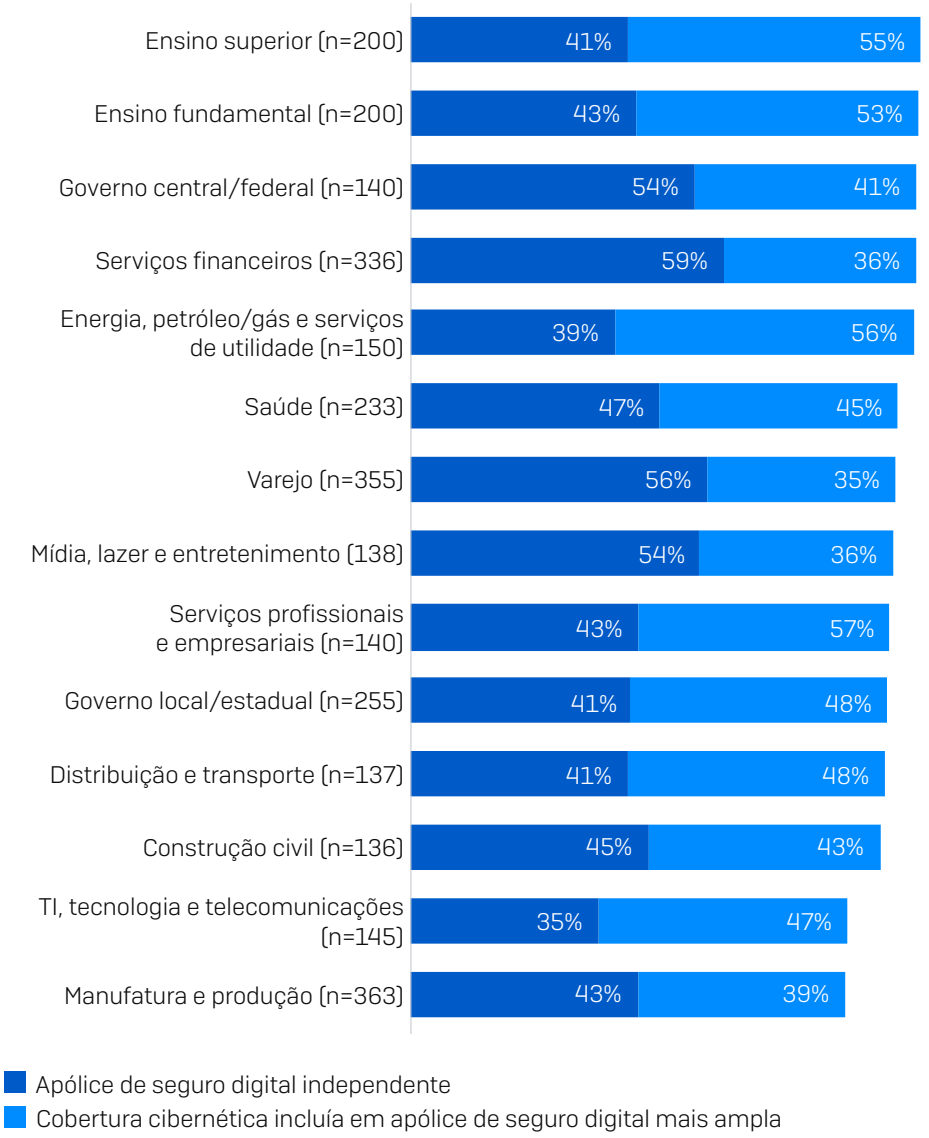
Esse alto nível de cobertura fica claro quando observamos que esse setor relatou o mais alto índice de ataques de ransomware em nosso estudo Estado do Ransomware 2023, em que 80% dos provedores do ensino superior e 79% do ensino fundamental disseram ter sido atingidos por ransomware no ano anterior. Os serviços financeiros registraram a mais alta propensão a ter apólices de seguro de proteção digital independentes (59%), seguidos de perto pelo varejo (56%).

Adoção de seguro de proteção digital por receita

Como seria de se esperar, a adoção de seguro de proteção digital aumenta com a receita. 96% das organizações com receita anual superior a US$ 5 bilhões têm algum tipo de cobertura de proteção digital em comparação aos 79% daquelas que relataram rendimentos inferiores a US$ 50 milhões.

Organizações com receitas maiores têm maior propensão a adquirir uma apólice de proteção digital independente do que aquelas com receitas menores: 58% das organizações com receita anual superior a US$ 5 bilhões têm uma apólice independente em comparação aos 34% daquelas que relataram rendimentos anuais inferiores a US$ 10 milhões. No geral, nossa pesquisa revela um aumento uniforme na adoção de apólices independentes com a receita[4].

Adoção de seguro de proteção digital por setor, 2023



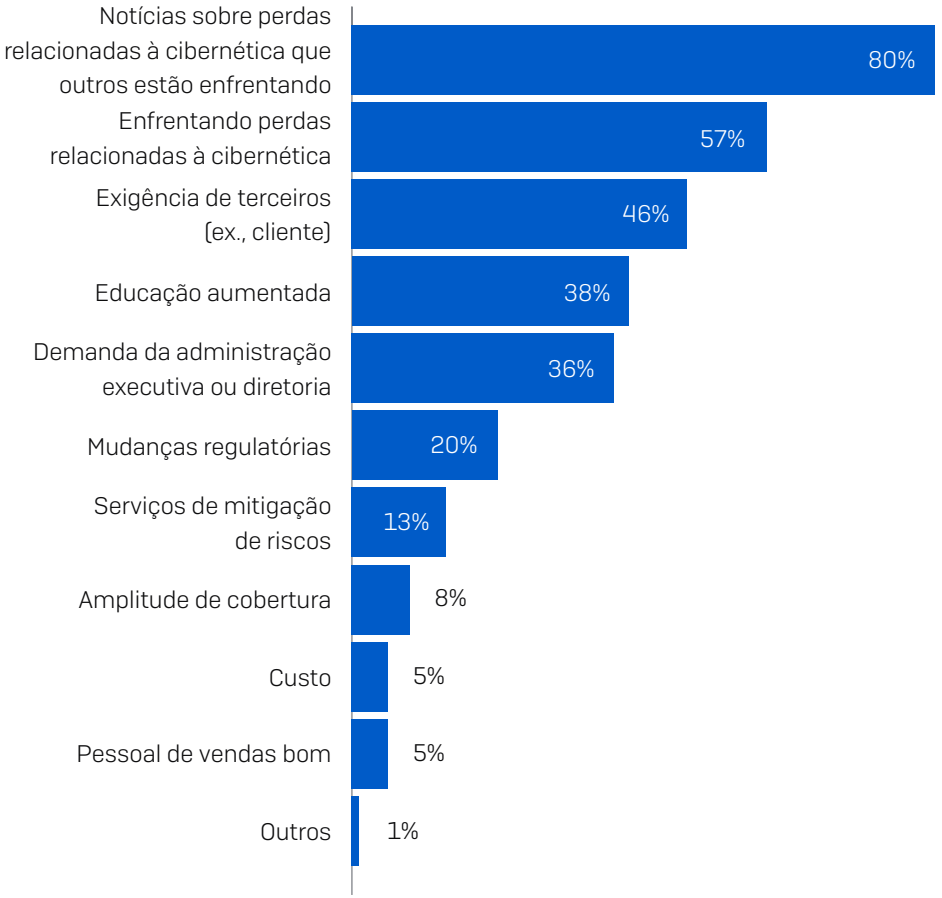
A sua organização tem seguro de proteção digital? Sim, temos uma apólice de seguro de proteção digital independente, Sim, temos seguro de proteção digital como parte de uma apólice de seguro comercial mais ampla (por exemplo, uma apólice de responsabilidade geral). Números de base no gráfico

4 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.

Ataques cibernéticos estão estimulando o seguro de proteção digital

Uma pesquisa com corretoras de seguro de proteção digital e companhias de seguro de proteção digital em todo o mundo realizada pela Advisen e PartnerRe oferece insights sobre os principais impulsionadores das vendas novas/aumentadas de seguro de proteção digital. Não é de surpreender que os dois principais fatores por trás do incremento em seguro de proteção digital sejam as notícias sobre perdas relacionadas à cibernética que outros enfrentaram e as perdas que enfrentam relacionadas à cibernética. Contudo, em terceiro lugar aparece "a exigência de terceiros". Com o aumento de ataques à cadeia de suprimentos, as organizações estão cada vez mais se vendo obrigadas a apresentar um seguro de proteção digital como pré-requisito para se aventurarem nos negócios, de modo a cobrir seus clientes caso enfrentem um acidente cibernético como resultado de uma parceria.

Mais de uma em cada três (36%[5]) mencionaram a demanda da administração executiva ou diretoria como um dos maiores incitadores da aquisição do seguro de proteção digital. Esse alto grau de exigência pelas equipes de liderança reflete o nível da devastação que um incidente cibernético de peso pode causar nas organizações. Defender-se contra as implicações de um ataque cibernético é agora uma questão comercial consolidada, não apenas um problema de TI.



Seguro de proteção digital: The Market's View – Advisen, PartnerRe

5 Cyber Insurance: The Market's View, PartnerRe e Advisen

O custo do seguro de proteção digital

Como acontece com todas as outras formas de seguro, os custos dependem de diferentes fatores, incluindo:

- **Dados demográficos:** tamanho, indústria, setor, localização, receita etc.
- **Exposição potencial:** tipo e volume de dados confidenciais armazenados/coletados/processados
- **Nível da segurança cibernética:** as defesas de segurança que uma organização usa
- **Histórico:** sinistros anteriores invariavelmente resultam em maiores prêmios
- **Condições da apólice:** cobertura/limite de reponsabilidade etc.

É importante saber a diferença entre as apólices de dedução e de retenção. Em uma apólice de dedução, a dedução (conhecida também como 'franquia') está incluída no limite da apólice total. Reciprocamente, em uma apólice de retenção, o valor de retenção é adicionado ao limite da apólice.

DEDUÇÃO	RETENÇÃO
Limite da apólice $100 mil, dedução de $10 mil (franquia)	Limite da apólice $100 mil, retenção de $10 mil
Você paga os primeiros $10 mil do sinistro, a seguradora paga $90 mil	Você paga os primeiros $10 mil do sinistro, a seguradora paga $100 mil
Cobertura total $100 mil	**Cobertura total $100 mil**

Domínios de seguro

No mercado das pequenas e médias empresas, não é raro haver apenas uma entidade provedora do seguro de proteção digital. Contudo, já para o mercado das grandes empresas, o domínio de defesa por diferentes companhias de seguro de proteção digital é lugar-comum, já que uma única seguradora não pode absorver toda a transferência de risco necessária. As corretoras de seguros desenvolvem domínios de defesa para os clientes individualmente, agregando dois, três ou mais provedores. O primeiro fornecedor cobre a transferência de risco primária, enquanto os outros cobrem a transferência de risco franqueada.

Quadro de seguros

As corretoras de seguro de proteção digital têm geralmente um quadro de seguradoras, que chamam de "panel", com quem trabalham na eventualidade de um acidente. Se a empresa passando por um incidente não tiver relações pré-existentes com as seguradoras, a corretora do seguro de proteção digital incentivará, chegando a exigir, que ela trabalhe com uma das organizações participantes desse quadro, consideradas "on-panel".

Ainda assim, muitas corretoras também estão abertas a trabalhar com seguradoras bem-conceituadas, especialmente se uma relação pré-existente e/ou termos contratuais já estiverem estabelecidos. A isso chamamos de aprovação "off-panel". Naturalmente, existem várias vantagens financeiras e operacionais em se trabalhar com seguradoras que já conheçam a organização que está passando por um ataque e estar familiarizado com sua estrutura de negócios e de TI.

Se a sua seguradora preferida não estiver "on-panel", ou seja, no quadro da sua corretora, você pode solicitar que ela seja acionada. Uma boa comunicação prévia com a sua corretora é essencial para que a equipe de seguro de proteção digital da sua seguradora preferida possa estabelecer uma relação apropriada com a corretora para que as aprovações pertinentes sejam definidas.

Necessidades de cobertura

Ao selecionar uma apólice de seguro digital, é importante escolher o nível apropriado de cobertura para a sua organização. Você precisa poder se recuperar com sucesso e manter seus negócios circulando, caso passe por um ataque cibernético, e ao mesmo tempo manter seus prêmios em um nível aceitável.

Os custos para se restabelecer de um ataque cibernético são consideráveis e crescentes. O custo médio para uma organização retificar o impacto do ataque de um ransomware em 2023 foi de US$ 1,82 milhão[6] – um bom aumento comparado a US$ 0,76 milhão em 2020. Vale ressaltar que, ainda que pequena, essa foi uma queda bem-vinda, do US$ 1,85 milhão em 2021, o que reflete que, como os ransomwares se tornaram mais prevalentes, o dano reputacional de um ataque diminuiu. Paralelamente, as seguradoras estão mais aptas a orientar as vítimas com rapidez e eficácia no processo de resposta a incidentes, reduzindo o custo do reparo.

6 O Estado do Ransomware 2023, Sophos

O mercado do seguro de proteção digital

Condições para seguro de proteção digital enrijeceram

O seguro de proteção digital foi, por muitos anos, um mercado "brando", caracterizado por alta capacidade e baixos prêmios. Porém, o mercado enrijeceu em 2021 pela primeira vez em seus mais de 15 anos de história como uma apólice independente, conforme as seguradoras observaram o rápido aumento no pagamento de indenizações em contrapartida à receita gerada pelos prêmios: a taxa de perda do setor subiu de modo regular desde 2018, chegando a 72,8% em 2020[7]. (A taxa de perda é o produto do custo do seguro dividido pelo prêmio total recebido. Por exemplo, se uma empresa paga US$ 80 em indenização para cada US$ 160 em prêmio coletado, a taxa de perda seria 50 %.)

Vários fatores estavam por trás da rigidez do mercado:

- Os ataques cibernéticos aumentaram em volume e complexidade –
  - 57% dos gerentes de TI disseram que sentiram um aumento no volume dos ataques cibernéticos[8]
  - 59% disseram que sentiram um aumento na complexidade dos ataques[9]
- Os custos para recuperação de um ataque cibernético aumentaram – como mencionado, a média dos custos de remediação de um ataque de ransomware em 2023 chegou ao valor assustador de US$ 1,82 milhão.

Com o enrijecimento do mercado, ficou mais difícil contratar uma apólice de seguro de proteção digital. Essa situação foi confirmada em nossos estudos com 5.600 profissionais de TI realizados no início de 2022, que revelaram que 94% daqueles com seguro de proteção digital disseram que o processo para garantir a cobertura mudou bastante no decorrer do último ano:

- 54% disseram que o nível de segurança cibernética de que precisam para se qualificarem era mais alto
- 47% disseram que as apólices eram mais complexas
- 40% disseram que menos empresas ofereciam seguro de proteção digital
- 37% disseram que o processo demorava mais
- 34% disseram que era mais caro[10]

7 S&P Global, 1º de junho de 2021
8 O Estado do Ransomware 2022, Sophos
9 O Estado do Ransomware 2023, Sophos
10 Seguro de proteção digital 2022: a realidade pela InfoSec Frontline, Sophos

"Nosso seguro de proteção digital está subindo e estamos passando por situações cada vez mais difíceis."
Empresa de viagens corporativas

Esse enrijecimento do mercado criou uma situação particularmente desafiadora para as entidades públicas, frequentemente vistas como alvo fácil pelos criminosos cibernéticos devido às suas defesas fracas. Consequentemente, as organizações públicas que buscam obter ou renovar a cobertura encontraram menos fornecedores e condições mais rígidas, com preços que chegam a dobrar anualmente.

"[Seguradoras] Costumavam oferecer limite de US$ 10 milhões, e agora foi para US$ 5 milhões."
Jack Kudale, CEO, Cowbell Cyber Inc.

A segunda metade de 2023 presenciou um relaxamento seletivo no mercado de seguro de proteção digital. A capacidade aumentou com as novas ofertas lançadas no mercado. Porém, esses novos provedores são altamente seletivos quanto a quem querem dar cobertura: organizações de baixo risco estão encontrando melhores ofertas de seguro enquanto empresas de mais alto risco continuam a enfrentar obstáculos para conseguir cobertura.

O seguro de proteção digital vale a pena

Uma boa notícia para quem tem um seguro de proteção digital é que as apólices invariavelmente pagam o que devem no caso de o pior acontecer e você ser vítima de um ataque cibernético. Na pesquisa Estado do Ransomware 2022 da Sophos, 98% dos entrevistados segurados que foram atingidos por ransomware disseram que o fornecedor do seguro cobriu os custos resultantes do ataque. Em quase três quartos (73%) dos incidentes, o fornecedor do seguro cobriu os custos com limpeza para colocar a empresa de volta nos trilhos. Em 36 % dos incidentes, o seguro pagou o resgate, e, em 33 %, pagou também outros custos extras incorridos, como por tempo de inatividade e perda de oportunidades.

O seguro de proteção digital está levando a melhorias nas defesas

Dado o enrijecimento do mercado, praticamente todas as organizações (97%) com seguro de proteção digital fizeram mudanças em suas defesas cibernéticas para melhorar sua classe de bônus no mercado de seguros.

- 64% implementaram novas tecnologias e serviços
- 56% aumentaram o índice de treinamento dos funcionários e atividades educativas
- 52% mudaram seus processos e comportamentos[11]

Mas quais as mudanças que você deve implementar?
O que ajudará a melhorar sua classe de bônus do seguro de proteção digital?

11 Seguro de proteção digital 2022: a realidade pela InfoSec Frontline, Sophos

Uma segurança cibernética robusta ajuda a otimizar sua classe de bônus do seguro de proteção digital

Existe uma relação direta entre a segurança cibernética e o seguro de proteção digital – em verdade, 95% das organizações que contrataram um seguro em 2023 disseram que a qualidade de suas defesas afetou diretamente sua classe de bônus no mercado de seguros[12]. Investir em defesas robustas proporciona vários benefícios ao segurado:

1. Facilidade de acesso à cobertura

60% das organizações com seguro de proteção digital disseram que a qualidade de suas defesas impactou sua habilidade de obter cobertura[13]. Os provedores estão focados cada vez mais em gerenciar – e reduzir – o risco. Uma segurança cibernética robusta permite reduzir o seu risco cibernético, o que, por sua vez, transforma você em um produto mais atraente para um contrato de seguro de proteção digital. Ainda que os requisitos específicos de cada seguradora possam variar, diversos controles cibernéticos se mantêm comuns ao mercado:

Autenticação multifator

A autenticação multifator é um requisito essencial para a cobertura de seguro, com as seguradoras buscando fechar uma lacuna muito comum à segurança antes de absorverem os riscos.

"Nosso seguro de proteção digital será renovado se introduzirmos a autenticação MFA para o acesso remoto."

Provedor de serviços e suporte de TI, EUA

"Disseram que se não integrarmos a autenticação MFA em um ano, nosso seguro de proteção digital será cancelado."

Provedor na área de saúde, EUA

12 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.
13 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.

Endpoint Detection and Response (EDR) ou Extended Detection and Response (XDR)

Proteção de endpoint de alta qualidade que bloqueia automaticamente as ameaças é uma camada fundamental que assegura a base de uma defesa cibernética forte. Contudo, os adversários continuam a evoluir seus ataques explorando ferramentas de TI legítimas, credenciais comprometidas e vulnerabilidades, e a proteção de endpoint apenas não é mais suficiente. Para bloquear ransomwares avançados e violações (e os sinistros resultantes), é essencial também monitorar, investigar e responder a atividades suspeitas proativamente antes que os agentes de ameaças possam lançar seus ataques.

EDR e XDR são ferramentas que permitem que especialistas em segurança detectem e investiguem possíveis comprometimentos e neutralizem um ataque cibernético avançado antes que o estrago seja feito. Como o próprio nome sugere, o EDR trabalha exclusivamente com pontos de dados provenientes da tecnologia de proteção de endpoint, enquanto o XDR reúne as fontes de dados das soluções de endpoint e de toda a pilha de segurança, incluindo soluções de firewall, e-mail, nuvem e segurança móvel, para oferecer maior visibilidade e acelerar a detecção e a resposta. O sistema EDR, em particular, é geralmente um pré-requisito para a cobertura oferecida pela maioria das seguradoras, e as organizações sem esse recurso normalmente têm dificuldade para conseguir uma apólice.

Managed Detection and Response (MDR)

O MDR é um serviço totalmente gerenciado – 24 horas por dia, sete dias por semana – entregue por peritos especializados em detectar e responder a ataques cibernéticos que as soluções tecnológicas por si só não conseguem evitar. Ele oferece o mais alto nível de proteção contra ameaças cibernéticas, minimizando o risco e a probabilidade de um sinistro. Ainda que a sua falta não tenha o peso de coibir uma venda no que se refere à cobertura, as organizações que usam serviços MDR são, geralmente, consideradas clientes de "Nível 1" pelas seguradoras, pois representam o nível de risco mais baixo.

"O departamento jurídico quer fazer seguro contra ransomware e [o MDR] é o passo certo nessa direção."

Provedor de tecnologias e soluções de TI, global

Plano de resposta a incidentes

A melhor forma de parar um ataque virtual antes que se torne uma violação total é se preparar com antecedência. Frequentemente, depois que uma organização passa por uma violação, ela se dá conta que poderia ter evitado boa parte do custo, estresse e interrupção se tivesse um plano de resposta a incidentes em vigor. Ter um plano detalhado que o capacite a minimizar o impacto de um incidente reduzirá o seu risco cibernético, transformando você em um produto mais atraente para as seguradoras.

2. Reduzir o prêmio

62% das organizações com seguro de proteção digital disseram que a qualidade de suas defesas impactou o custo de suas coberturas[14]. Da mesma forma que um cadeado e um alarme na janela diminuem o prêmio do seguro da casa, ter defesas cibernéticas avançadas ajuda a reduzir os custos do seu seguro de proteção digital. Os algoritmos que as seguradoras usam no cálculo do prêmio exato são um segredo guardado a sete chaves, mas os clientes dizem consistentemente que a qualidade da proteção tem efeito no prêmio que pagam.

"Como não tínhamos o EDR 100% instalado em nossos dispositivos e equipamentos o [custo do] seguro dobrou."

Empresa de hosts de armazenamento na Web, EUA

"Com a Measured, os clientes que implementaram os produtos Sophos MDR ou Sophos Endpoint podem reduzir o prêmio de seus seguros de proteção digital em até 25%."

Measured Insurance, EUA

3. Diminuir a probabilidade de um sinistro

Como acontece com outras formas de seguro, ao dar entrada a um aviso de sinistro, você pode ter dificuldades para renovar a sua apólice. Organizações que deram entrada a sinistros também sentiram uma aumento significativo nos prêmios dos anos seguintes. Ao minimizar o risco do impacto de um ataque cibernético com defesas cibernéticas robustas, você reduz a probabilidade de precisar usar a sua apólice e ajuda a manter o prêmio baixo.

4. Reduzir o risco de não pagamento

A higiene insatisfatória da segurança de TI pode impedir que você receba ajuda financeira no caso de um incidente. Se a seguradora acreditar que você 'deixou a porta aberta' devido a práticas inadequadas, eles talvez tenham fundamento para justificar o não pagamento. Ao eliminar essas lacunas, você pode ajudar a garantir que, se o pior acontecer, a companhia seguradora irá interceder.

"Não pagamos por sinistros, perdas, violações, investigações de privacidade ou ameaças devidos ao uso de softwares ou sistemas desatualizados ou sem suporte."

Texto da política da Hiscox Cyberclear™, Reino Unido, junho de 2021

5. Minimizar o impacto e os custos se ocorrer um incidente

A resposta rápida e eficiente a um ataque cibernético pode reduzir significativamente o impacto e o custo do incidente. Ter um plano de resposta a incidente de malware em vigor e poder contar com uma equipe experiente de resposta a incidentes ajudará a minimizar os resquícios do ataque.

14 The Critical Role of Frontline Cyber Defenses in Cyber Insurance Adoption – Sophos.

Como a Sophos pode ajudar

Otimizar as suas defesas cibernéticas

A Sophos capacita as organizações a atenderam a muitos dos controles cibernéticos que são cada vez mais necessários para se qualificar para a cobertura do seguro e ter acesso aos melhores preços e condições da apólice – tudo com o respaldo dos especialistas em inteligência de ameaças e segurança cibernética do Sophos X-Ops.

Sophos Endpoint Detection and Response (EDR)

O Sophos EDR combina a abordagem da prevenção em primeiro lugar do Sophos Endpoint com poderosas funcionalidades de detecção e resposta, permitindo que analistas de segurança e administradores de TI localizem, investiguem e respondam a atividades suspeitas em todos os seus endpoints e servidores. As detecções são priorizadas pela análise conduzida por IA, o que ajuda você a identificar para onde é melhor direcionar seu tempo e energia. Os operadores podem acessar dispositivos remotamente para investigar problemas, instalar e desinstalar softwares, encerrar processos ativos, executar scripts ou programas, editar arquivos de configuração e muito mais.

Sophos Extended Detection and Response (XDR)

Quanto mais você vê, mais rápido pode agir. O Sophos XDR aproveita os dados de telemetria de seus investimentos em segurança com produtos da Sophos e de terceiros para você detectar, investigar e responder a atividades suspeitas em todo o seu ambiente de segurança.

- **Detectar:** Detecções alimentadas por IA oferecem visibilidade instantânea de atividades suspeitas nas suas principais superfícies de ataque, e nossa pesquisa simples, sem SQL, permite sair no encalço de ameaças em alta velocidade
- **Investigar:** Casos criados e detecções priorizadas automaticamente facilitam o enfoque no que realmente importa, enquanto nossa UX projetada por analistas lhe dá as informações e ferramentas que você precisa para realizar suas investigações com facilidade
- **Responder:** Ferramentas extensivas de gerenciamento de casos e ações de resposta permitem colaborar com os membros da equipe e neutralizar ataques rapidamente

Sophos Managed Detection and Response (MDR)

O Sophos MDR é o serviço MDR mais confiável do mundo, protegendo mais organizações do que os outros provedores. Oferecendo detecção, investigação e resposta a ameaças, 24 horas por dia, sete dias por semana, ditadas por um time de especialistas como um serviço totalmente gerenciado, o Sophos MDR proporciona o máximo em proteção. Com um tempo médio de fechamento de incidente de apenas 38 minutos, o Sophos MDR minimiza imensamente o risco de um incidente cibernético de maiores proporções e otimiza sua classe de bônus de seguro.

Diminuir a probabilidade de sinistro

A Sophos proporciona proteção líder de mercado contra ransomware, hackers mal-intencionados e outras ameaças avançadas. Nossas soluções ajudam você a minimizar o risco de passar por um incidente cibernético de peso, reduzindo a probabilidade de sinistro e mantendo os prêmios baixos no futuro.

"Não conseguimos bloquear tudo o que chega, por isso confiamos essa tarefa à Sophos."
Vancouver Canucks, Canadá

Validado por analistas e clientes da Sophos

As soluções Sophos são amplamente reconhecidas por clientes, analistas da comunidade e testes independentes, incluindo:

Sophos Managed Detection and Response (MDR)

- Condecorada com o 2023 Gartner® Customers' Choice™ em Managed Detection and Response (MDR) com pontuação 4,8/5 na Gartner Peer Insights
- Condecorada como líder geral em Managed Detection and Response (MDR) nos relatórios G2 Grid® Fall 2023
- Top performer em Serviços Gerenciados na Avaliação 2022 MITRE Engenuity ATT&CK

Sophos Extended Detection and Response (XDR)

- Condecorada como líder geral em XDR nos relatórios G2 Grid® Fall 2023
- Top performer nas Avaliações 2023 (Turla) MITRE Engenuity ATT&CK
- Reconhecidamente a Nº 1 na liderança geral da Omdia Universe em Comprehensive Extended Detection and Response (XDR)

Sophos Endpoint Detection and Response (EDR)

- Líder na 2022 Gartner® Magic Quadrant™ em Plataformas de Proteção de Endpoint por 13 vezes consecutivas
- Condecorada com o 2023 Gartner® Customers' Choice™ em Plataformas de Proteção de Endpoint pelo segundo ano consecutivo com pontuação 4,8/5 na Gartner Peer Insights
- Condecorada como líder geral em Endpoint Protection Suites e EDR nos relatórios G2 Grid® Fall 2023Top performer nas Avaliações 2023 (Turla) MITRE Engenuity ATT&CK
- Classificações AAA e pontuações 100% em Total Protection no relatório Q3 2023 SE Labs em Segurança de Endpoint nas categorias Enterprise e SMB.

Para obter mais informações sobre soluções da Sophos, clique aqui

A Sophos oferece soluções de segurança cibernética líder do setor para empresas de todos os tamanhos, protegendo-as em tempo real de ameaças avançadas como malware, ransomware e phishing. Com recursos comprovados de última geração, seus dados comerciais ficam protegidos de modo eficiente por produtos que incorporam inteligência artificial e machine learning.

2024-01-12 (WP-PC)

SOPHOS