SOPHOS

Perspectivas para MSP 2024

Insights de 350 provedores MSP sobre ferramentas de segurança cibernética, riscos, desafios e oportunidades de negócios.

Documento técnico Sophos. Maio de 2024

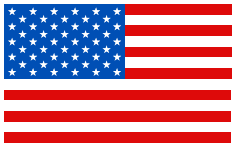
Apresentação

O relatório Perspectivas para **MSP 2024** oferece insights sobre cinco áreas principais de negócios para provedores:

- Ferramentas RMM e PSA
- Gerenciamento de segurança cibernética
- Serviços MDR
- Desafios e riscos que MSPs e seus clientes enfrentam
- Impacto do seguro de proteção digital

Os resultados se baseiam nas revelações obtidas de uma pesquisa independente com 350 MSPs dos EUA (200), Reino Unido (50), Alemanha (50) e Austrália (50). A pesquisa foi encomendada pela Sophos e realizada em março de 2024 pela empresa de pesquisas de opinião Vanson Bourne.

350 MSPs
em quatro países



EUA
200 entrevistados

Reino Unido
50 entrevistados

Alemanha
50 entrevistados

Austrália
50 entrevistados

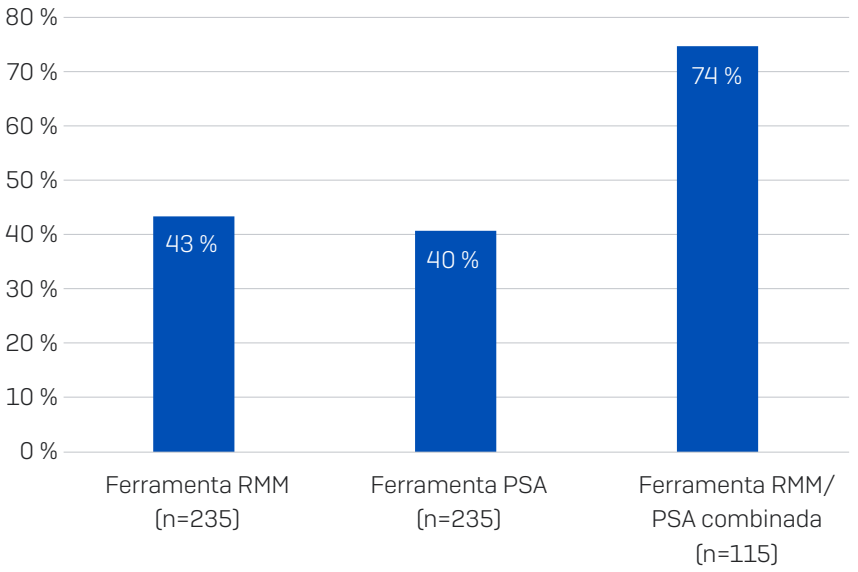
Ferramentas RMM e PSA

As ferramentas RMM (Remote Monitoring and Management) e PSA (Professional Services Automation) incrementam a eficiência e eficácia dos serviços realizados pelos MSP e consolidam suas despesas operacionais. A pesquisa destacou dois insights em particular em relação a essas tecnologias fundamentais para um MSP.

As ferramentas RMM e PSA combinadas proporcionam níveis de satisfação bem mais altos do que separadamente

Quase três quartos (74%) dos MSPs que usam uma ferramenta RMM/PSA combinada estão "muito satisfeitos" com a solução em comparação a apenas 43% dos MSPs que usam ferramentas RMM independentes e 40% dos que usam ferramentas PSA independentes.

Entrevistados que estão "muito satisfeitos" com suas ferramentas RMM e PSA existentes

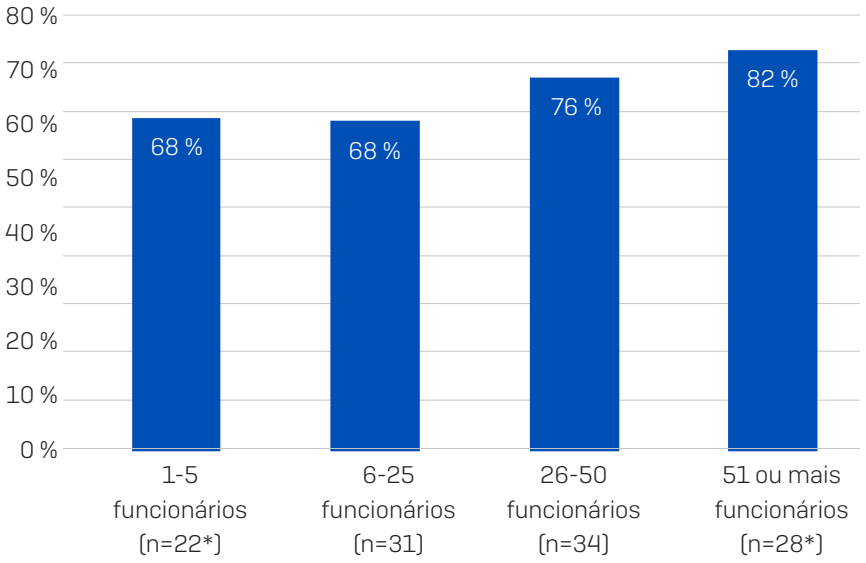


Qual o nível de satisfação da sua organização com suas ferramentas RMM e PSA existentes? Números de base no gráfico

Satisfação com ferramentas RMM/PSA combinadas aumenta com o tamanho do MSP

Mais de dois terços (68%) dos MSPs com até 25 funcionários estão muito satisfeitos com suas ferramentas RMM/PSA combinadas, subindo para 76% entre os provedores com 26 a 50 funcionários e para 82% entre os MSPs com 51 funcionários ou mais. Como é de se esperar, grandes MSPs trabalham com um maior número de clientes, e nossos resultados sugerem que quanto maior o número de clientes, maior o benefício obtido das ferramentas RMM/PSA combinadas.

Entrevistados que estão "muito felizes" com suas ferramentas RMM/PSA combinadas



Qual o nível de satisfação da sua organização com suas ferramentas RMM e PSA existentes? Números de base no gráfico.
* Devido ao baixo número de entrevistados nesse segmento, os resultados devem ser considerados um mero indicativo, sem grande relevância estatística.

Recomendação: os MSPs que usam ferramentas RMM/PSA separadas devem ponderar e considerar o uso de uma solução RMM/PSA combinada para aumentar a conveniência e a satisfação geral, especialmente se planejam expandir suas bases de clientes.

Gerenciamento de segurança cibernética

Parcerias com fornecedores de segurança cibernética

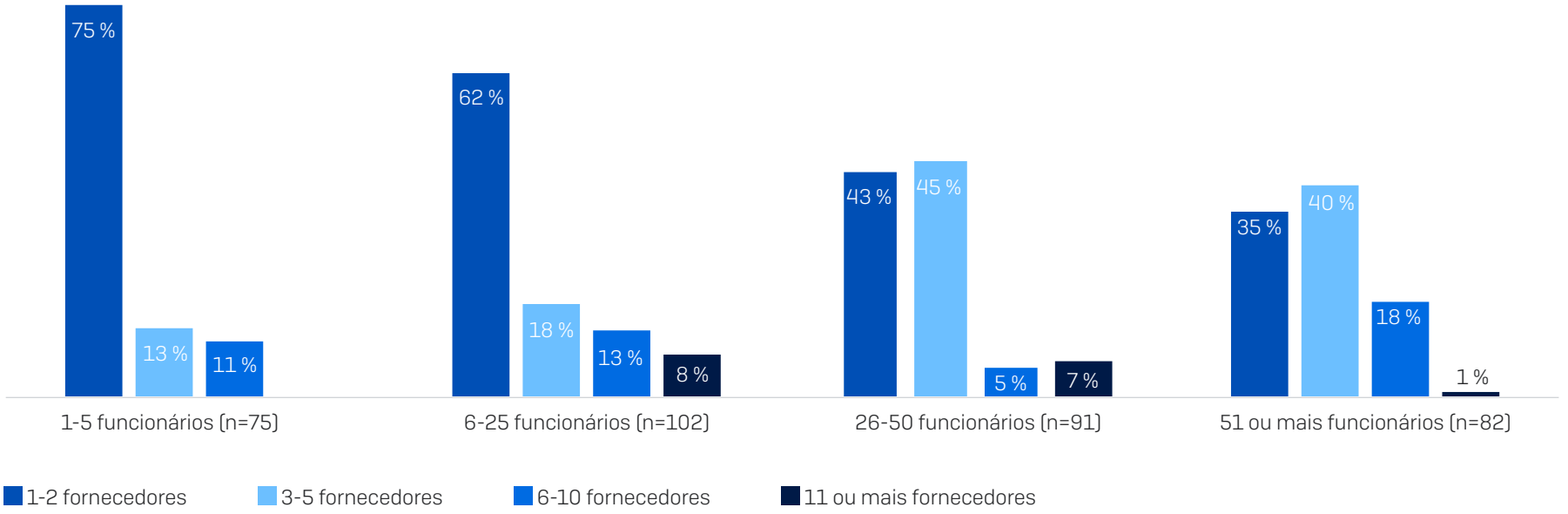
A segurança cibernética é uma oferta fundamental para a maioria dos MSPs. O estudo revelou que MSPs normalmente trabalham com um pequeno número de fornecedores de segurança cibernética para proteger seus clientes:

- 53% trabalham com um ou dois fornecedores de segurança cibernética
- 83% trabalham com um e cinco fornecedores de segurança cibernética
- 4% trabalham com 11 ou mais fornecedores de segurança cibernética

Os dados também mostram que o número de fornecedores de segurança cibernética usados geralmente aumenta com o tamanho da organização MSP. 75% dos pequenos MSPs (1 a 5 funcionários) trabalham com um ou dois fornecedores de segurança cibernética, em comparação a apenas 35% dos MSPs com 51 funcionários ou mais.

Em contrapartida, os MSPs maiores são quase duas vezes mais propensos a trabalhar com seis ou mais provedores de segurança cibernética do que os menores (20% arredondados x 11%). Ainda que trabalhar com mais provedores de segurança cibernética possa aumentar a variedade de serviços oferecidos, muito provavelmente também aumentará as despesas gerais com o gerenciamento de fornecedores e os desafios da integração de tecnologias díspares.

Número de fornecedores de segurança cibernética usados para proteger clientes



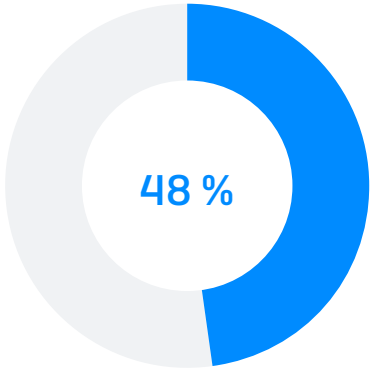
Quantos fornecedores de segurança cibernética a sua organização usa no momento para proteger seus clientes? n=350. Número de base no gráfico. Exclui respostas "Não sei".

Consolidação da plataforma de segurança cibernética

A pesquisa revela que existe um grande potencial para os MSPs aumentarem a eficiência e reduzirem as despesas gerais com a consolidação da plataforma de segurança cibernética.

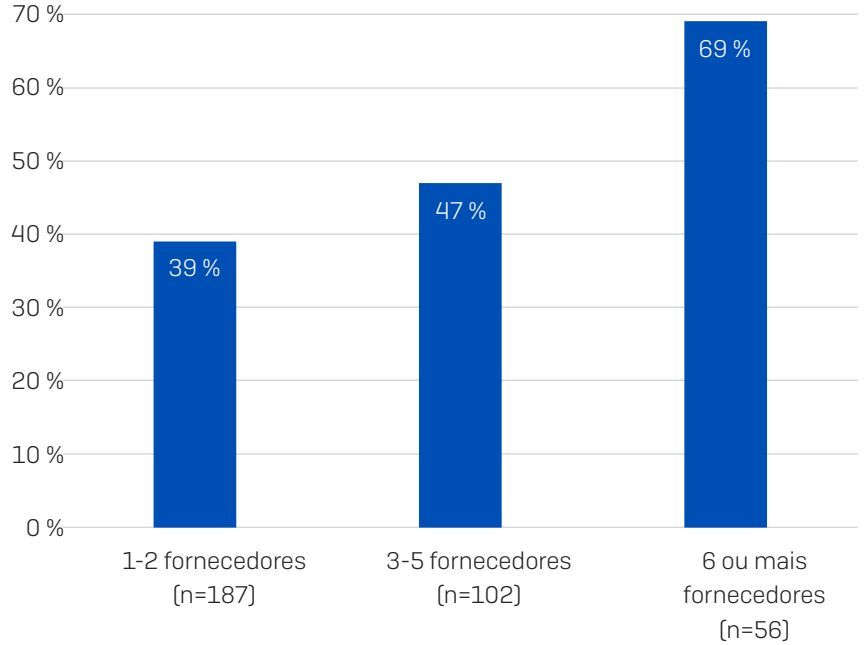
Os MSPs que, no momento, usam várias plataformas estimam que, em média, poderiam economizar 48% de seu tempo de gerenciamento diário se pudessem gerenciar todas as suas ferramentas de segurança cibernética a partir de uma única plataforma.

Economia estimada de tempo de gerenciamento diário com a consolidação em uma única plataforma



O potencial de economia de tempo de gerenciamento aumenta com o número de fornecedores de segurança cibernética atualmente em uso. Os MSPs que trabalham com seis ou mais fornecedores de segurança cibernética estimam que poderiam reduzir seu tempo de gerenciamento diário em mais de dois terços (69%) se pudessem gerenciar todas as suas ferramentas de segurança cibernética a partir de uma única plataforma. Reduções de despesas de gerenciamento dessa magnitude fariam uma diferença substancial na rentabilidade, além de liberar membros das equipes para atividades geradoras de receita.

Economia média estimada de tempo de gerenciamento diário com a consolidação em uma única plataforma – dividida por número de fornecedores usados



Qual a estimativa de tempo de gerenciamento que a sua organização poderia economizar diariamente se pudesse gerenciar todas as suas ferramentas de segurança cibernética em uma única plataforma? Números de base no gráfico.

Recomendação: Os MSPs que usam várias plataformas de segurança cibernética deveriam explorar as opções de consolidação e a economia que poderiam obter em custo total de propriedade (TCO) com o gerenciamento de todas as suas ferramentas de segurança cibernética através de uma única plataforma.

Serviços MDR

Adoção de serviços MDR

A demanda por serviços MDR de resposta e detecção gerenciadas está aumentando com rapidez, levada pela maior complexidade das ameaças cibernéticas e das ferramentas e tecnologias que as bloqueiam. Dados recentes da Gartner indicam um valor total de mercado de US$ 7,5 bilhões e uma taxa de crescimento anual composta (CAGR) de 25,8%.

Com esse nível de demanda e crescimento, não surpreende que a maioria (81%) dos MSPs já ofereça um certo nível de serviços MDR, e que a maioria do restante planeje adicionar o MDR às suas ofertas a curto ou médio prazo. Contudo, a pesquisa revelou uma variação considerável no nível de maturidade da adoção do serviço MDR nos quatro países entrevistados.

Os MSPs nos EUA estão na liderança, com praticamente todos (94%) já incluindo a oferta de serviço MDR, em comparação a 70% na Alemanha, 62% no Reino Unido e 58% na Austrália. Em termos globais, entre os MSPs que ainda não oferecem MDR, quase todos planejam adicioná-lo a seus portfólios nos próximos anos, e quase um terço (32%) dos MSPs no Reino Unido planejam adicionar o MDR em 2024.

				
Oferta atual de serviços MDR	**94 %**	**62 %**	**70 %**	**58 %**
Planeja adicionar MDR em 2024	5 %	32 %	20 %	18 %
Planeja adicionar MDR em 2025 ou depois	2 %	6 %	10 %	22 %

A sua organização fornece atualmente um serviço de detecção e resposta gerenciadas (MDR) para seus clientes? n=350 (EUA 200, Reino Unido 50, Alemanha 50, Austrália 50), exclui algumas opções de resposta.

Entrega dos serviços MDR

Existem três modelos primários de um MSP fornecer os serviços MDR: através do centro de operações de segurança (SOC) do próprio MSP, através de um fornecedor terceirizado e através da combinação do SOC do MSP com um fornecedor terceirizado.

A pesquisa revela que 66% usam um fornecedor terceirizado para o serviço MDR, 20% usam seus próprios SOCs e 15% usam um fornecedor terceirizado combinado a seus próprios SOCs. No geral, 80% (arredondados) dos MSPs trabalham com um fornecedor terceirizado de alguma forma para fornecer seus serviços MDR.

34% (arredondados) dos MSPs têm um SOC interno que faz os serviços MDR, seja de modo independente ou em parceria com um fornecedor terceirizado. O provisionamento interno é notadamente consistente entre organizações de todos os tamanhos, com uma diferença de apenas quatro pontos porcentuais separando a mais alta propensão de ter um SOC interno (37%, 26 a 50 funcionários) e a mais baixa (33%, todas as outras faixas).

Método de entrega dos serviços MDR

SOC próprio do MSP	Fornecedor de MDR terceirizado	SOC do MSP e fornecedor de MDR terceirizado
20 %	66 %	15 %

A sua organização fornece atualmente um serviço de detecção e resposta gerenciadas (MDR) para seus clientes? n=282 que fornecem um serviço MDR. Exclui algumas opções de resposta.

Habilidades necessárias de provedores de MDR

Como vimos anteriormente, quatro em cada cinco MSPs usam fornecedores terceirizados para seus serviços MDR. Dada a significância e crescente demanda pelos serviços MDR, passa a ser vital que os MSPs escolham o provedor certo para suas próprias organizações e para seus clientes.

Os provedores de MDR atuam como uma extensão do MSP, portanto, sua capacidade e competência refletem diretamente no MSP. Além disso, as competências do fornecedor de MDR afetam a amplitude dos serviços que o MSP pode oferecer a seus clientes e o nível do trabalho e do retorno que o MSP precisa entregar.

Serviço de resposta a incidentes 24/7 está no topo da lista de funcionalidades imprescindíveis, com 36% dizendo ser "essencial", e esse valor sobe para 49% nos MSPs com 1 a 5 funcionários. 91% dos ataques de ransomware começam fora do horário comercial regular[1], portanto, ter uma cobertura 24 horas por dia, sete dias por semana, é vital para a eficácia da defesa de uma organização. Trabalhar com um provedor de MDR que ofereça cobertura 24/7 dá aos MSPs a tranquilidade de saber que seus clientes estão sempre protegidos, sem o encargo de ter de sustentar esse nível de perícia internamente.

Em segundo lugar está a *Capacidade de detectar ameaças de tomada de controle de contas no Microsoft 365 e/ou Google Workspace*, com um terço (33%) dos MSPs dizendo ser um requisito "essencial" e 43% classificando-o como "muito importante".

A *capacidade de obter ferramentas adicionais de segurança — particularmente segurança de rede/firewalls e proteção de endpoint — do provedor de MDR* também é altamente requisitada, com três quartos dos entrevistados classificando-a como "essencial ou muito importante". Ter a opção de trabalhar com um único provedor das ferramentas de segurança cibernética e serviços MDR diminui os gastos operacionais administrativos ao mesmo tempo que agiliza as operações.

O estudo também deixa claro que os MSPs exigem flexibilidade e não querem ter limites impostos às ferramentas que podem usar nem serem obrigados a comprar ferramentas de segurança cibernética de seus provedores de MDR. 71% dizem que é "essencial ou muito importante" que o fornecedor possa *usar a telemetria de suas ferramentas de segurança existentes para a detecção e resposta a ameaças.*

Serviço de resposta a incidentes 24/7 é o requisito nº 1 em um provedor de MDR

RECURSO	"ESSENCIAL"	"ESSENCIAL" OU "MUITO IMPORTANTE"
Serviço de resposta a incidentes 24/7	36 %	74 %
Capacidade de detectar ameaças de tomada de controle de contas no **Microsoft 365 e/ou Google Workspace**	33 %	77 %
Capacidade de obter **segurança de rede/firewall** do provedor de MDR	31 %	74 %
Capacidade de obter **proteção de endpoint** do provedor de MDR	28 %	75 %
Painel único para MDR e outras soluções de segurança	28 %	74 %
Provisionamento **de garantia** contra violações	26 %	70 %
Capacidade de usar telemetria de **ferramentas de segurança existentes** para a detecção e resposta a ameaças	25 %	71 %

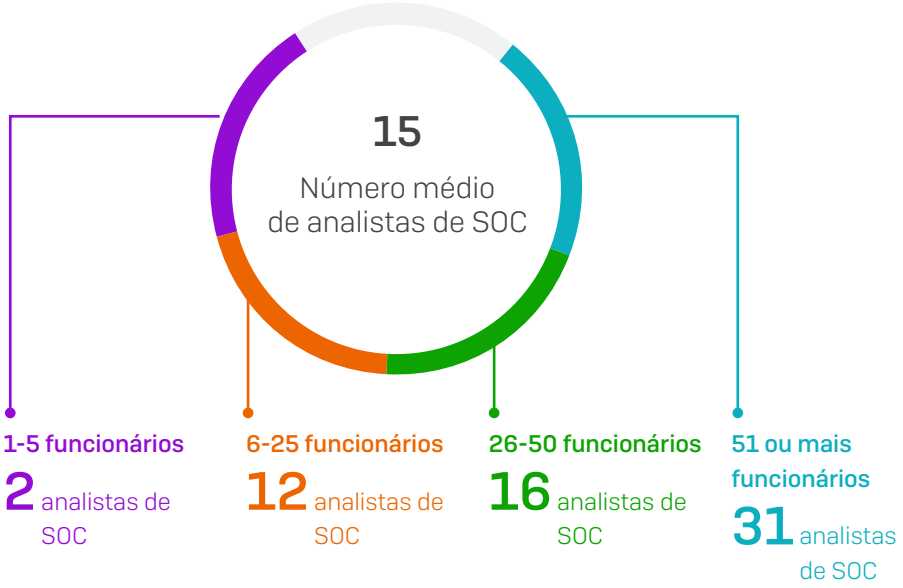
Se a sua organização precisa selecionar um provedor de MDR, qual a importância do provedor de MDR oferecer os seguintes recursos? n=350 (EUA 200, Reino Unido 50, Alemanha 50, Austrália 50), exclui algumas opções de resposta.

Analistas de SOC interno

34% dos MSPs que oferecem um serviço MDR têm um SOC interno, que requer analistas internos especializados. A pesquisa revela que um SOC de MSP típico tem, em média, 15 analistas. Contudo, esse número mascara uma variação considerável por tamanho de organização.

MSPs com 1 a 5 funcionários têm, em média, dois analistas monitorando o ambiente de seus clientes e detectando e respondendo a ameaças. O número de analistas sobe progressivamente com o tamanho da organização, e os grandes MSPs registram uma média de 31 analistas de SOC. Observe que o número de entrevistados em cada segmento, individualmente, é bastante baixo, portanto, esses resultados devem ser considerados um mero indicativo, sem grande relevância estatística.

Como os adversários aplicam seus golpes deliberadamente à noite e nos fins de semana e feriados, a cobertura 24 horas é essencial para um serviço MDR eficiente. Para os pequenos MSPs com poucos analistas de SOC, o fornecimento apenas interno provavelmente coloca grande pressão em seus recursos limitados.



Pensando no SOC da sua organização, quantos analistas a sua organização tem monitorando e respondendo a eventos suspeitos no ambiente de seus clientes?

Recomendação: MSPs que atualmente não oferecem serviços MDR devem considerar adicioná-los a seus portfólios o mais rápido possível para evitar ficar para trás. Ao selecionar um fornecedor de MDR terceirizado, esteja certo de determinar as funcionalidades que lhe são importantes e avaliar as condições do provedor em atendê-las.

Desafios e riscos cibernéticos

Principais desafios para MSPs hoje

O universo MSP não para. As ameaças continuam evoluindo, levando a mudanças e avanços dos controles de segurança cibernética e das necessidades dos clientes.

A pesquisa revela que ***manter-se em dia com as mais recentes tecnologias e soluções em segurança cibernética*** é o maior desafio que os MSPs enfrentam atualmente: o maior e um dos três principais desafios.

Dada a velocidade de inovação nessa área, não surpreende que muitos MSPs tenham dificuldades para acompanhar as mudanças. Conforme as ameaças evoluem, evoluem também os controles cibernéticos que as bloqueiam. As tecnologias existentes adquirem novas funções e novos produtos são lançados regularmente no mercado. Acompanhar todos esses desenvolvimentos é difícil e toma tempo.

No âmago do segundo maior desafio enfrentado pelos MSPs hoje está a dificuldade de reter o número suficiente de analistas em segurança cibernética:

- ***Oferecer cobertura fora do expediente (incluindo noites e fins de semana)*** é o segundo maior desafio dos MSPs
- ***Adicionar novos analistas de segurança cibernética para acompanhar o crescimento*** é o segundo principal desafio da lista

Analistas especializados em segurança cibernética são poucos e exigem salários altos, e para aumentar o desafio, a cobertura 24/7 requer, no mínimo, 5 a 6 analistas, o que é uma exigência difícil de se cumprir para muitos MSPs.

O maior dos desafios

Nº 1	Manter-se em dia com as mais recentes tecnologias e soluções em segurança cibernética
Nº 2	Oferecer cobertura fora do expediente (incl. noites, fins de semana e feriados)
Nº 3	Conquistar novos clientes

Três principais desafios

Nº 1	Manter-se em dia com as mais recentes tecnologias e soluções em segurança cibernética
Nº 2	Adicionar novos analistas de segurança cibernética para acompanhar o crescimento do cliente
Nº 3	Manter-se em dia com as mais recentes ameaças cibernéticas

Pensando na sua organização, quais são os principais desafios que a sua organização enfrenta no dia a dia? Classifique os três principais. n=350

Riscos cibernéticos

A pesquisa explorou o que os MSPs veem como os maiores riscos cibernéticos para suas organizações e para seus clientes. Os resultados revelam as áreas comuns e diferenciais.

Dois fatores despontaram na lista tanto para os MSPs quanto para seus clientes:

- Credenciais e dados de acesso roubados
- Escassez de especialistas em segurança cibernética nas equipes internas

Os adversários não se infiltram, eles acessam. Usando credencias e dados de acesso roubados, geralmente obtidos na dark web por meio de um intermediador de acesso inicial (IAB), eles assumem o papel de funcionários legítimos para entrar na rede de suas vítimas. Como destacado no relatório Estado do Ransomware 2024 da Sophos, 29% dos ataques de ransomware do último ano começaram com credenciais comprometidas, o que mostra o tamanho do desafio.

MSPs

O maior dos riscos		Três principais riscos	
Nº 1	Escassez de especialistas em segurança cibernética nas equipes internas	Nº 1	Credenciais e dados de acesso roubados
Nº 1	Rede sem fio desprotegida	Nº 2	Ferramenta de segurança com erro de configuração
Nº 3	Falta de ferramentas de segurança cibernética	Nº 3	Rede sem fio desprotegida

Clientes MSP

O maior dos riscos		Três principais riscos	
Nº 1	Escassez de especialistas em segurança cibernética nas equipes internas	Nº 1	Credenciais e dados de acesso roubados
Nº 2	Vulnerabilidades sem patches	Nº 2	Falta de ferramentas de segurança cibernética
Nº 3	Ferramentas de acesso remoto	Nº 3	Vulnerabilidades sem patches

Quem ou quais você considera como sendo os três maiores riscos à segurança cibernética para a sua organização ou para os clientes da sua organização? n=350

Apesar dos avanços contínuos da inteligência artificial e tecnologia de segurança cibernética, os seres humanos mantêm sua posição central na efetivação da segurança cibernética. Profissionais capacitados precisam configurar, implantar, gerenciar, atender e atualizar as soluções tecnológicas, e a tecnologia por si só não consegue evitar todas as ameaças cibernéticas automaticamente. A escassez de profissionais capacitados é de conhecimento geral, e as organizações estão cada vez mais se voltando para os MSPs para preencher essa lacuna, exacerbando o desafio.

Ainda que o principal risco seja comum aos MSPs e seus clientes, é quando descemos na lista classificatória que as diferenças começam a surgir.

Rede sem fio desprotegida é o risco cibernético mais observado pelos MSPs (o primeiro também na classificação "o maior dos riscos", e o terceiro dos "três principais riscos"). Usar redes desprotegidas pode levar a vários perigos, incluindo a interceptação de dados que são posteriormente usados para extrair dados de login e senha que habilitam o acesso a contas pessoais e corporativas pelos adversários.

A *configuração incorreta das ferramentas de segurança* também está no topo da lista de riscos para os MSPs. Firewalls, proteção de endpoint e outras ferramentas só funcionam se estiverem configuradas corretamente.

Vulnerabilidades sem patches são um dos principais riscos para os clientes MSP (segundo na classificação "o maior dos riscos" e terceiro dos "três principais riscos"). Com 32% dos ataques de ransomware no último ano começando com a exploração de uma vulnerabilidade sem patches, os MSPs estão certos em classificá-la como um dos maiores perigos para os seus clientes.

Recomendação: para minimizar as despesas gerais com gerenciamento diário e fornecedores frente a esse amplo cenário de riscos e desafios, os MSPs devem buscar parceiros de segurança cibernética que ofereçam uma linha completa de serviços e ferramentas. Soluções de implantação que combinam proteção robusta e adaptável contra o avanço das ameaças sem a necessidade de implantações e configurações complexas vai ajudá-los a se manterem em dia. Além disso, os MSPs devem aproveitar os provedores de MDR para aumentar e expandir as habilidades e perícia de suas equipes internas, focando em parceiros que deem suporte a seus modelos de negócios e possam se adaptar às suas necessidades conforme evoluem.

Impacto do seguro de proteção digital

O uso de seguro de proteção digital para repassar o risco cibernético cresceu com regularidade, com 90% das organizações de médio porte tendo, agora, alguma forma de cobertura, de acordo com as pesquisas da Sophos. 50% têm uma apólice de seguro de proteção digital independente, enquanto 40% têm cobertura de proteção digital como parte de uma apólice de seguro comercial mais ampla, como uma apólice de responsabilidade geral.

A ampla adoção do seguro de proteção digital está levando a altos níveis de engajamento de canais, com 99% dos MSPs relatando um aumento na demanda para que o suporte e as soluções atendam aos requisitos do seguro de proteção digital.

Globalmente, a solicitação mais comum (47%) vem de clientes que querem implementar um serviço MDR para melhorar sua elegibilidade ao seguro, seguida de perto por clientes que precisam de ajuda para cumprir com as propostas de seguro de proteção digital (45%). Esses dois requisitos oferecem grandes oportunidades de gerar receita para os MSPs, baseado na oferta de MDR e faturamento de serviços profissionais.

NECESSIDADE DO CLIENTE	GLOBAL				
Obter MDR para melhorar a elegibilidade ao seguro	**47 %**	49 %	38 %	56 %	36 %
Ajuda para preencher a **proposta** de seguro	**45 %**	49 %	46 %	30 %	42 %
Obter **EDR** para melhorar a elegibilidade ao seguro	**34 %**	31 %	32 %	28 %	52 %
Obter tecnologias e serviços **não EDR/ MDR** para melhorar sua elegibilidade ao seguro	**33 %**	31 %	22 %	48 %	40 %

Sua organização observou um aumento na necessidade de suporte e soluções para atender aos requisitos de segurança cibernética de seus clientes? n=350 (EUA 200, Reino Unido 50, Alemanha 50, Austrália 50).

Um terço (34%) dos MSPs relatam clientes buscando adicionar detecção e resposta de endpoint (EDR) a seus arsenais de segurança para melhorar a elegibilidade ao seguro. É interessante notar que, fora da Austrália, a demanda por MDR levada pelo seguro é consideravelmente maior do que a demanda por EDR, refletindo a grande redução de risco que um especialista em serviços MDR 24/7 pode oferecer para compensar as equipes internas exauridas.

Um terço (33%) dos entrevistados relatou que notou um aumento na demanda por tecnologias e serviços não EDR/MDR de clientes que querem melhorar sua elegibilidade ao seguro. Ainda que o estudo não tenha explorado o assunto mais a fundo, os requisitos provavelmente incluem ferramentas de autenticação multifator (MFA), e-mail e segurança de rede — exigências ou sugestões comuns feitas pelos provedores de seguro.

Recomendação: o provisionamento de serviços e tecnologias para melhorar a elegibilidade ao seguro é uma excelente oportunidade para os MSPs, e as organizações deveriam focar em otimizar o suporte que oferecem nessa área para maximizar seu potencial de receita.

Conclusão

Em face à inevitabilidade dos ataques cibernéticos, os MSPs têm muitas oportunidades de aumentar seus negócios e melhorar sua rentabilidade. Da redução das despesas gerais do dia a dia através da consolidação da plataforma de gerenciamento à otimização do engajamento com fornecedores de MDR terceirizados para expandir suas ofertas de serviços e alinhar suas atividades às necessidades do seguro de proteção digital, os MSPs podem incrementar seus negócios elevando a proteção de seus clientes contra ransomwares e violações.

O mercado de MSPs pode ser um ambiente bastante competitivo, mas alavancando esses insights para se antecipar e crescer, os MSPs poderão aproveitar ao máximo as oportunidades futuras.

Programa Sophos MSP

A Sophos ajuda os MSPs a expandir seus negócios e aumentar sua rentabilidade. Defesas inovadoras e adaptáveis e um sistema completo de segurança cibernética de MSP são evidências cibernéticas que levam ao sucesso.

- Atenda às necessidades presentes e futuras de seu clientes com um portfólio completo de serviços e produtos de segurança cibernética em mãos
- Minimize as despesas diárias do gerenciamento e libere seu tempo com a plataforma de segurança Sophos Central que permite gerenciar a segurança de todos os seus clientes em um único painel
- Desfrute de margens lucrativas, incentivos atraentes e faturamento agregado com o Programa Sophos MSP

1 Active Adversary Report for Business Leaders, Sophos, 2023

Para saber mais sobre o programa Sophos MSP, acesse sophos.com/MSP, e para explorar o Sophos MDR, acesse sophos.com/MDR

Sophos MDR: resposta a incidentes 24/7 como o padrão

O Sophos MDR é o serviço gerenciado de detecção e resposta mais confiável do mundo, utilizado por mais organizações do que qualquer outro provedor. Com detecção 24 horas e resposta prática incluídas como o padrão, os MSPs e seus clientes desfrutam a tranquilidade de saber que os peritos da Sophos estão prontos para bloquear ataques a qualquer hora do dia ou da noite. Alguns destaques:

- Remediação prática via teclado 24/7
- Resposta abrangente a incidentes
- Chamada direta para assistência 24/7
- Liderança dedicada à resposta a incidentes
- Escolha dos modos de resposta
- Provisionamento de garantia contra violações
- Caça a ameaças proativa
- Funciona com a proteção de endpoint da Sophos e de outros fornecedores
- Detecta a tomada de controle de contas no Microsoft 365 e Google Workspace
- E muito mais.

Seja um serviço totalmente terceirizado ou uma extensão flexível ao seu SOC interno, o Sophos MDR pode ajudar você a expandir o seu negócio.

"O Sophos MDR salvou vários clientes de catástrofes iminentes a seus negócios. Nossas margens cresceram 100%, enquanto a receita aumentou 300%."

James Wagner, Presidente, The ITeam

2024-05-21 (WP-NP)

SOPHOS