Enterprise Strategy Group | Getting to the bigger truth.™

O que as equipes de segurança querem dos provedores de MDR

Dave Gruber, analista diretor

SETEMBRO DE 2022

Objetivos da pesquisa

Usar serviços de detecção e resposta gerenciadas (MDR) se tornou uma estratégia mainstream dos programas modernos de segurança. Porém, as organizações de TI não devem se enganar pelo nome: os provedores de MDR estão oferecendo muito mais do que detecção e resposta básicas, o que ajuda os líderes de TI e segurança a acelerar o desenvolvimento do programa e melhorar a postura de segurança. Sem um fim previsto para a escassez de habilidades de segurança cibernética, os serviços de MDR podem disponibilizar on-line recursos especializados e imediatos, juntamente com ferramentas e processos comprovados e avançados, que podem ajudar as quipes de segurança a assumir o controle e se preparar para o sucesso futuro do programa de segurança.

Para entender essas tendências, bem como avaliar o estado geral das ofertas de serviço de detecção e resposta gerenciadas, o ESG entrevistou 373 profissionais de segurança cibernética pessoalmente envolvidos com tecnologias de segurança cibernética, inclusive produtos, serviços e processos.

ESTE ESTUDO BUSCOU:

Determinar como, onde e por que os serviços de MDR são usados para dar suporte aos programas de segurança.

Identificar casos de uso específicos de MDR e os perfis organizacionais daqueles que os utilizam.

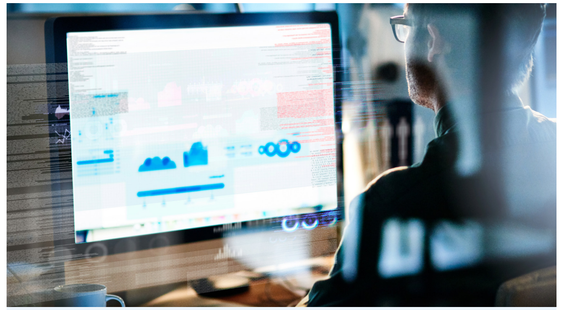
Obter percepções sobre o que é mais importante para as operações de TI, os executivos da LoB (Linha de negócios) e os usuários finais.

Estabelecer quais megatendências do setor estão afetando a escolha de provedores de MDR.

VOLTAR AO ÍNDICE

PRINCIPAIS **CONSTA-TAÇÕES**

CLIQUE PARA SEGUIR



Três fatores principais motivam o engajamento de MDR inicial

As organizações são motivadas por avaliações proativas, lacunas operacionais e engajamentos de IR.

Vários casos de uso são apoiados por MDR

Especialistas, inteligência contra ameaças, treinamento de habilidades, cobertura, desenvolvimento do programa e muito mais estão impulsionando o engajamento contínuo.

A MDR está trazendo resultados de segurança positivos

As organizações desenvolvem a maturidade, detêm ataques, melhoram as habilidades cibernéticas e aumentam a confiança dos executivos.

Espera-se uma pilha de tecnologia aberta, mas a MDR deve trazer todos os mecanismos

Espera-se que os provedores tenham uma pilha de tecnologia completa, se necessário, mas eles devem se integrar à infraestrutura existente para conquistar o cliente.

Os modelos de engajamento com o cliente de MDR são importantes

Embora os modelos variem, a confiança é estabelecida por meio de comunicações regulares focadas nas pessoas.

As megatendências do setor estão afetando a escolha de MDR

O movimento XDR, o suporte a MITRE ATT&CK e a modernização do SOC são importantes.

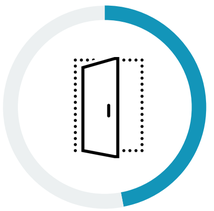
Três fatores principais motivam o engajamento de MDR inicial

As avaliações proativas têm mais chances de iniciar o engajamento de MDR

O que faz com que as equipes de TI e segurança busquem um provedor de serviços de detecção e resposta gerenciadas? Considerar a MDR segundo sua interpretação mais literal, ou seja, lacunas nas habilidades operacionais, na cobertura ou nos processos de segurança, seria uma resposta óbvia. No entanto, mais da metade (57%) das organizações citou as avaliações proativas de segurança como um fator que levou ao engajamento de MDR inicial. Na verdade, a interação com os provedores de MDR geralmente começa com avaliações de segurança, inclusive avaliações de vulnerabilidades, pois elas podem servir para expor os pontos fracos na postura de segurança em termos de programas, ferramentas, cobertura e habilidades. O terceiro grande fator é a resposta a crises ou incidentes, que revela as ineficiências do programa de segurança. As necessidades operacionais, como a resposta a incidentes, também são motivadores comuns dos engajamentos de MDR.

Fatores que geraram engajamentos iniciais com provedores de MDR.

57%
Avaliações de segurança

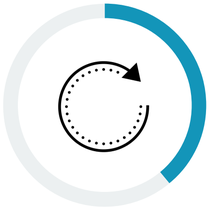


47%
Avaliação e gerenciamento de vulnerabilidades

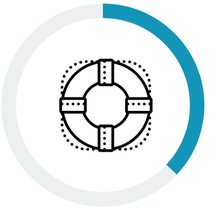
46%
Serviços de inteligência contra ameaças

39%
Redução/resposta a incidentes

39%
Detecção de incidentes



39%
Correção/recuperação de incidentes



37%
Engajamento de resposta a incidentes graves ou violações

36%
Resposta a incidentes de crise/violação que revelaram ineficiências em nosso programa

34%
Investigação de incidentes

33%
Triagem e priorização diárias de alertas

30%
Busca de ameaças

25%
Avaliação proativa com simulação de ataque e violação

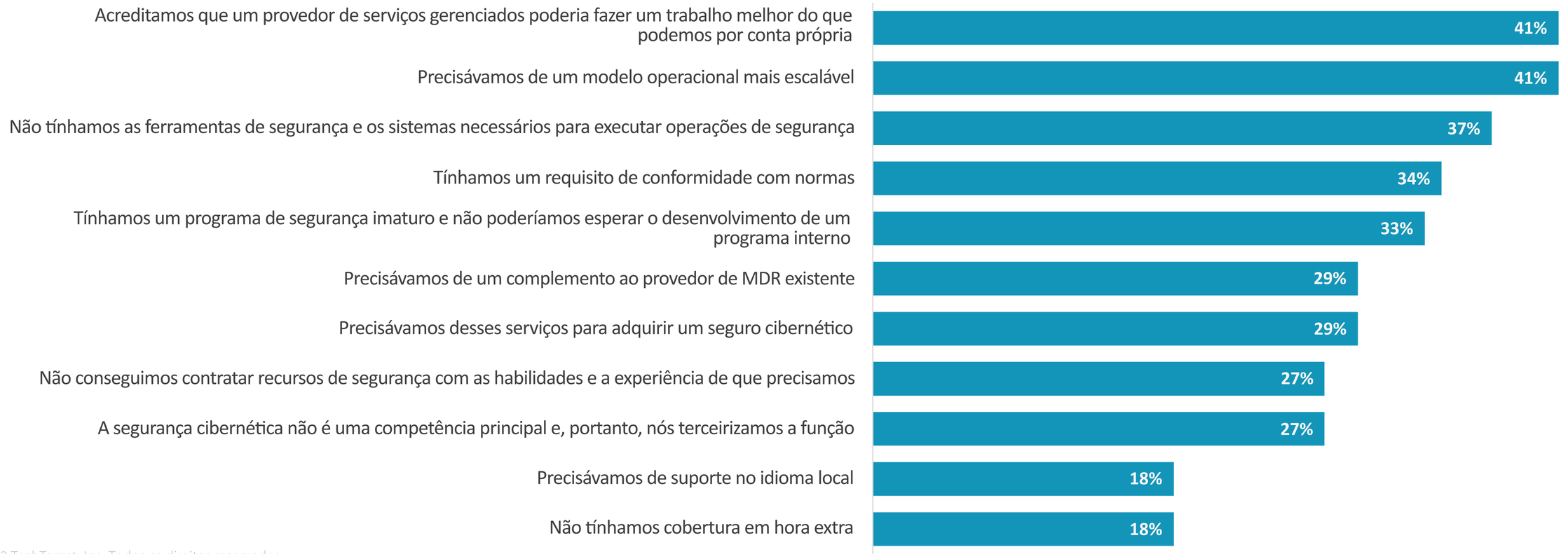
VOLTAR AO ÍNDICE

Fatores motivadores do atual engajamento de serviços de MDR

À medida que as equipes de segurança se esforçam para ampliar os programas de segurança a fim de atender ao crescimento e à complexidade do ambiente de ameaças e da superfície de ataque, muitas estão recorrendo a provedores de MDR para acelerar e dimensionar seus modelos operacionais. As organizações veem a MDR como um caminho para acelerar o desenvolvimento do programa e superar as ineficiências. Mais de quatro em dez acham que os provedores de serviços de MDR podem simplesmente fazer um trabalho melhor do que os recursos internos. Um terço relata programas de segurança imaturos, sem as ferramentas e os sistemas necessários. Além disso, outros fatores importantes incluem uma lista escalonada de controles e processos de segurança necessários para adquirir um seguro de segurança cibernética, assim como requisitos de conformidade com normas.

Em relação às deficiências de habilidades e cobertura, algumas relatam ineficiências, embora elas ocupem uma posição baixa na lista em comparação com os objetivos gerais de crescimento e desenvolvimento do programa.

Fatores determinantes para que as organizações interajam com seus atuais provedores de MDR.



VOLTAR AO ÍNDICE

Vários casos de uso **são apoiados pela MDR**

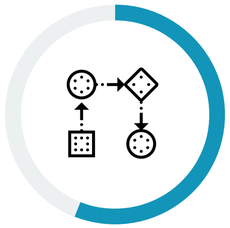
> Quase metade utiliza um provedor de MDR para **terceirizar totalmente as operações de segurança.”**

Casos de uso de MDR nos programas de segurança das organizações.

Casos de uso principais: acesso a recursos especializados e desenvolvimento do programa de segurança

Os provedores de MDR oferecem uma variedade de serviços que são usados para atender a vários casos de uso. Embora acelerar o desenvolvimento do programa de segurança e ter acesso a recursos de segurança especializados liderem a lista, quase metade utiliza um provedor de MDR para terceirizar totalmente as operações de segurança. A outra metade usa a MDR para complementar o programa interno, resolvendo as ineficiências de cobertura, obtendo acesso à inteligência adicional contra ameaças e adicionando recursos de busca de ameaças. Vale a pena também observar que quase metade das organizações terceirizam totalmente suas operações de segurança ou desejam fazer isso.

56%
Acesso a recursos de segurança especializados

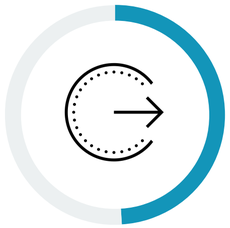


56%
Desenvolvimento do programa de segurança

54%
Complemento do programa interno de operações de segurança

50%
Cobertura

50%
Inteligência contra ameaças



49%
Terceirização completa das operações de segurança

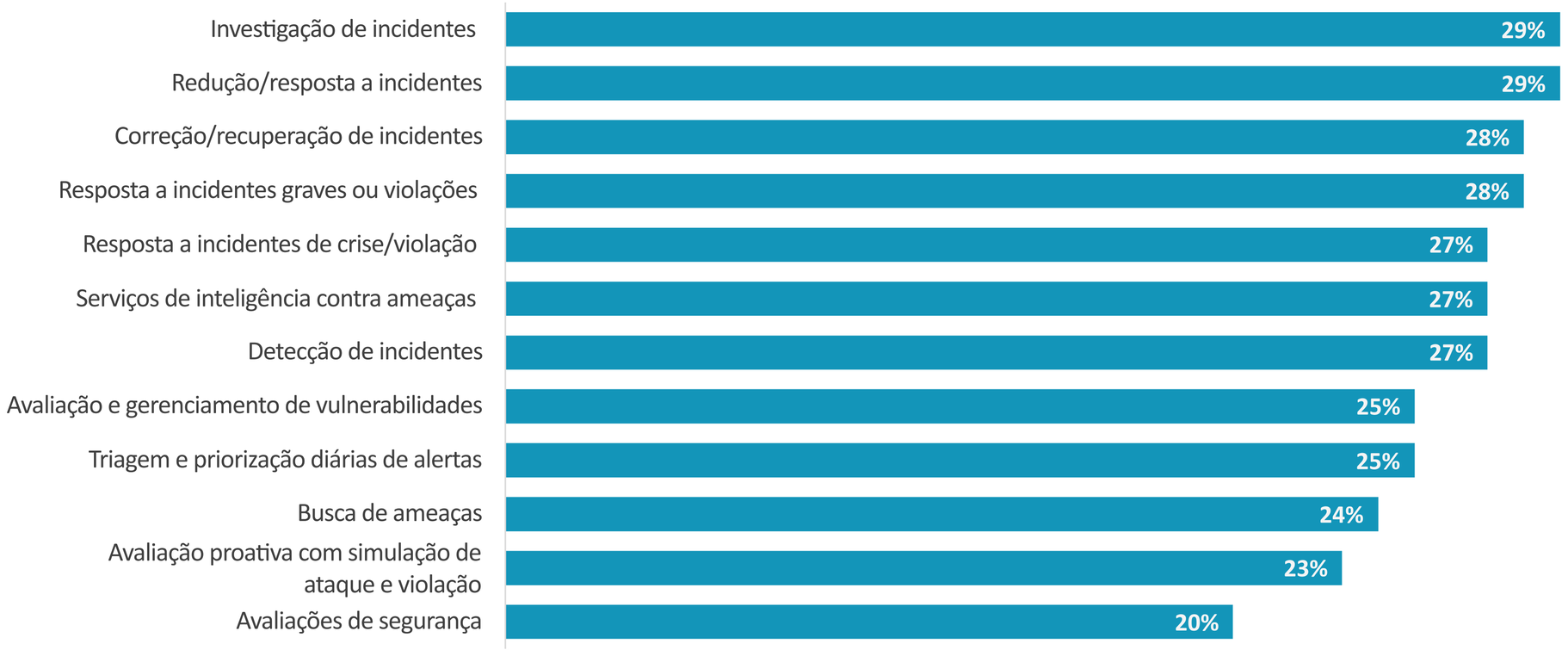
49%
Busca proativa de ameaças

VOLTAR AO ÍNDICE

Os engajamentos de MDR normalmente crescem ao longo do tempo

Os engajamentos de MDR geralmente crescem ao longo do tempo, adicionando novos serviços para fortalecer a investigação, a redução e a resposta a incidentes, desde um grande evento de crise/violação até as atividades diárias de resposta. Os provedores de MDR modernos ampliam os recursos além das tradicionais funções reativas de SecOps, oferecendo serviços proativos que dão suporte a inteligência contra ameaças, busca de ameaças, simulações de ataque, avaliações de segurança e gerenciamento de vulnerabilidades. Analisando esse amplo conjunto de serviços, os provedores de MDR estão oferecendo muito mais do que detecção e resposta básicas. Em vez disso, eles estão se tornando parceiros do programa de segurança em escala completa, pois ajudam organizações de todos os portes a ampliar os respectivos programas de segurança.

Atividades de segurança adicionadas desde a interação inicial com os provedores de MDR.



> “Os provedores de MDR estão oferecendo **muito mais do que detecção e resposta básicas.”**

VOLTAR AO ÍNDICE

Mais do que detecção e resposta: os provedores de MDR são parceiros operacionais estratégicos de longo prazo

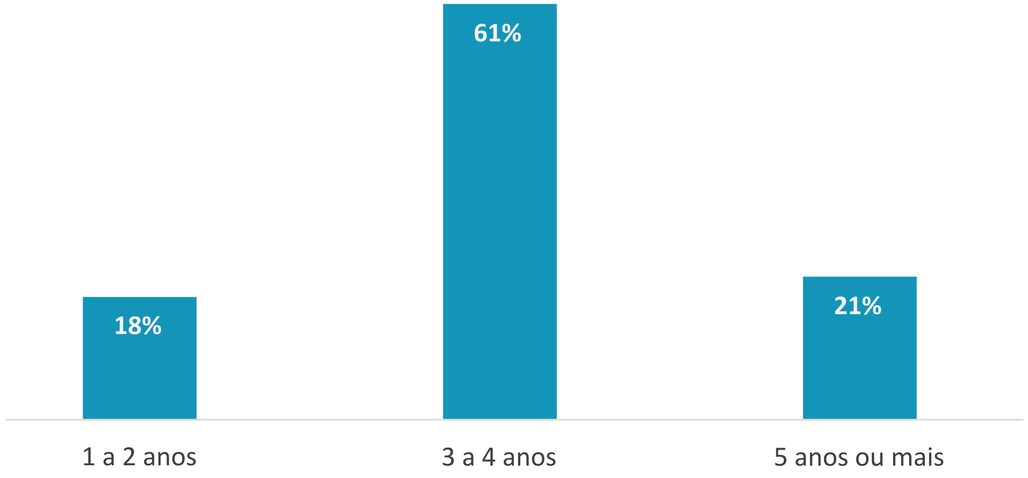
À medida que os engajamentos de MDR persistirem e as relações se solidificarem, os provedores de MDR assumirão uma função mais estratégica. Isso é claramente demonstrado pelo fato de que mais de três quartos (77%) das organizações descreve seu provedor de MDR como um parceiro operacional estratégico em termos de alinhamento com o respectivo programa de segurança. Essas relações persistem, sendo que 82% das organizações relatam que estão envolvidas com um provedor de MDR há pelo menos três anos. Além disso, a maioria está usando mais de um provedor de MDR, sendo que 34% fazem parcerias com três ou mais provedores de serviços de MDR para dar suporte aos casos de uso e ativos que compõem a respectiva superfície de ataque.

Como as organizações veem os atuais provedores de MDR.

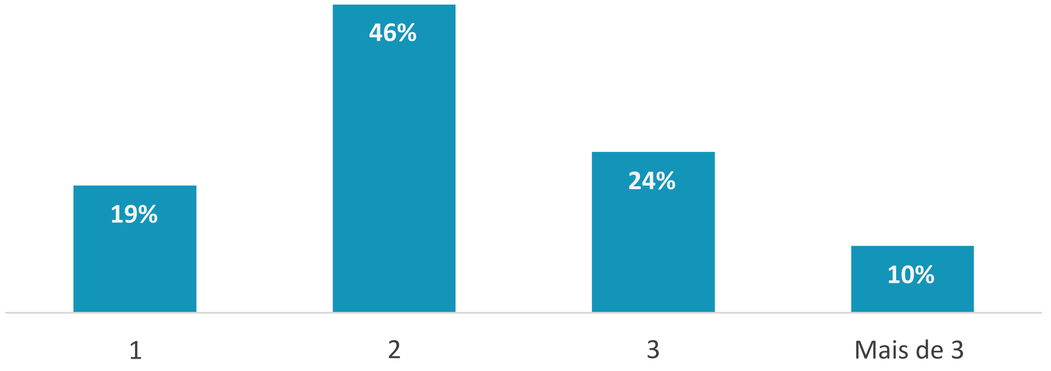
77%

Um parceiro operacional estratégico **que aprimorou nosso programa geral de segurança**

Tempo em que as organizações trabalham com um provedor de MDR.



Número de provedores de serviços de MDR com quem as organizações trabalham.



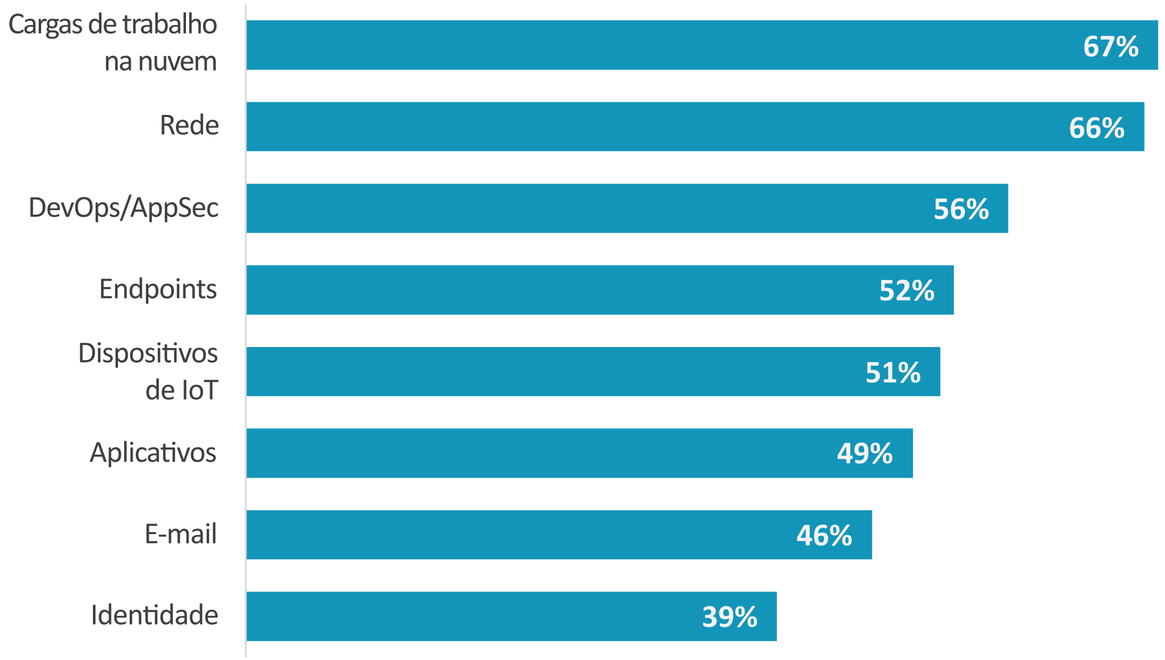
VOLTAR AO ÍNDICE

> “Poucas recorrem aos provedores de MDR **para cobrir toda a superfície de ataque.”**

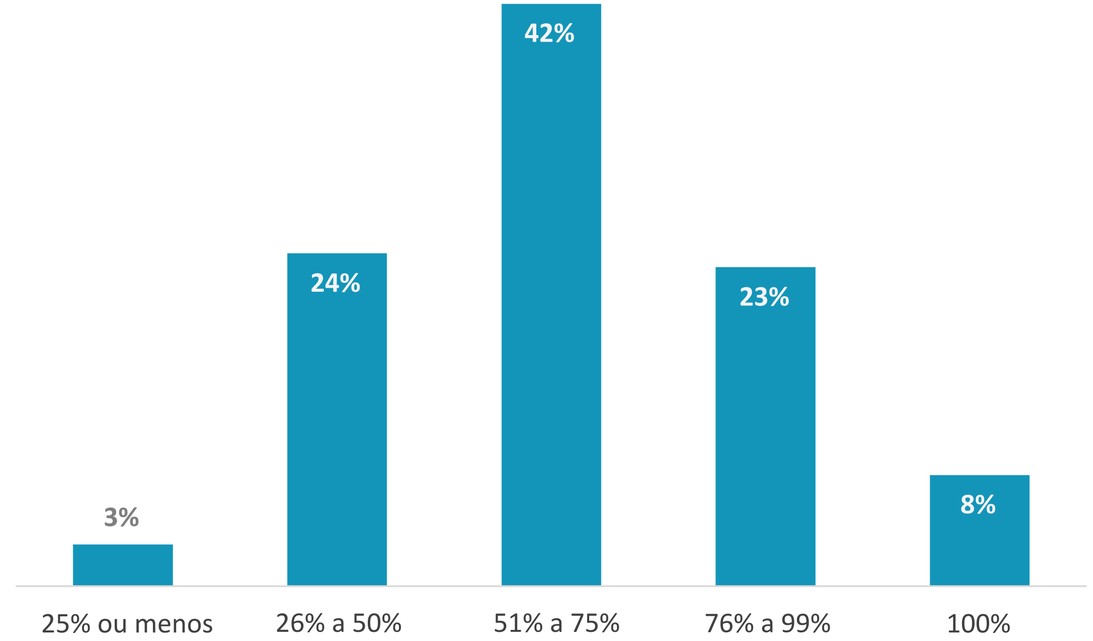
Espera-se que os provedores de MDR monitorem todos os tipos de ativo, mas raramente o acervo todo

Em relação à cobertura da superfície de ataque, a maioria espera que os provedores de MDR deem suporte às operações de segurança para todos os tipos de ativo de TI. No entanto, poucos recorrem aos provedores de MDR para cobrir toda a superfície de ataque. Especificamente, mais de dois terços relata que o provedor de MDR é responsável por cobrir no máximo 75% do acervo, enquanto apenas 8% indicam que o provedor de MDR cobre 100%.

Escopo de cobertura dos atuais provedores de MDR das organizações.



Porcentagem da superfície de ataque que os provedores de MDR são responsáveis por cobrir.



VOLTAR AO ÍNDICE

A MDR está trazendo **resultados de segurança positivos**

Os provedores de MDR estão ajudando a aprimorar os recursos no local e a maturidade do programa de segurança

Quanto aos resultados reais alcançados, os provedores de MDR estão ajudando as organizações a diminuir os ataques bem-sucedidos, acelerar o desenvolvimento geral do programa de segurança e abrir oportunidades de investimento em iniciativas de segurança mais estratégicas. Especificamente, metade afirma que o respectivo provedor de MDR está ajudando a melhorar as habilidades de segurança dos recursos internos, e 45% conseguiram investir em iniciativas de segurança mais estratégicas. Mais de quatro em cada dez relata que observa significativamente menos ataques bem-sucedidos e/ou uma melhoria geral no programa de segurança. Sob a perspectiva da linha de negócios, 42% afirmam que a confiança dos executivos e/ou da diretoria aumentou, enquanto 38% relatam que conseguem cumprir os objetivos de conformidade ou os requisitos do seguro cibernético. Corroborando esses resultados positivos para os negócios, houve um aumento significativo no número de organizações que categorizam a maturidade dos respectivos programas de segurança como muito alta depois de recorrer a um provedor de MDR.

Resultados obtidos com a utilização de um provedor de MDR

50%
Habilidades aprimoradas na equipe de segurança obtidas com o provedor de MDR

45%
Investimento em iniciativas de segurança mais estratégicas

42%
Significativamente menos ataques bem-sucedidos

42%
Melhoria significativa no programa de segurança

42%
Aumento da confiança dos executivos e/ou da diretoria

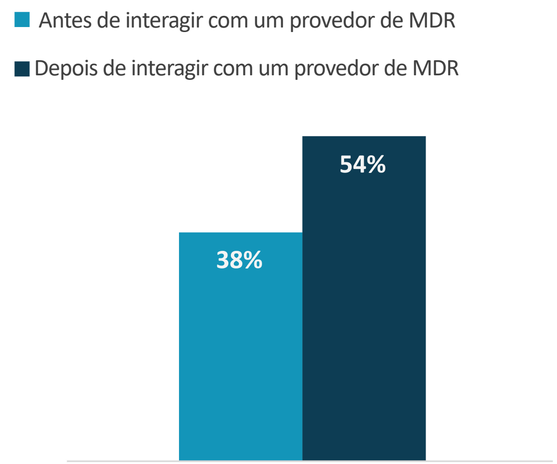
38%
Requisitos de conformidade/seguro cibernético atendidos

38%
Redução dos custos de operação de segurança

35%
Menos estresse na equipe interna de segurança

32%
Redução nas tarifas de seguro cibernético

Maturidade do programa de MDR.



Muito maduro (ou seja, processos formais e operacionalizados, especialistas na equipe, cobertura e visibilidade completas da superfície de ataque, perfis de risco, programa de IR formal e treinado, colaboração da TI, ferramentas e lógica analítica de segurança altamente eficazes etc.)

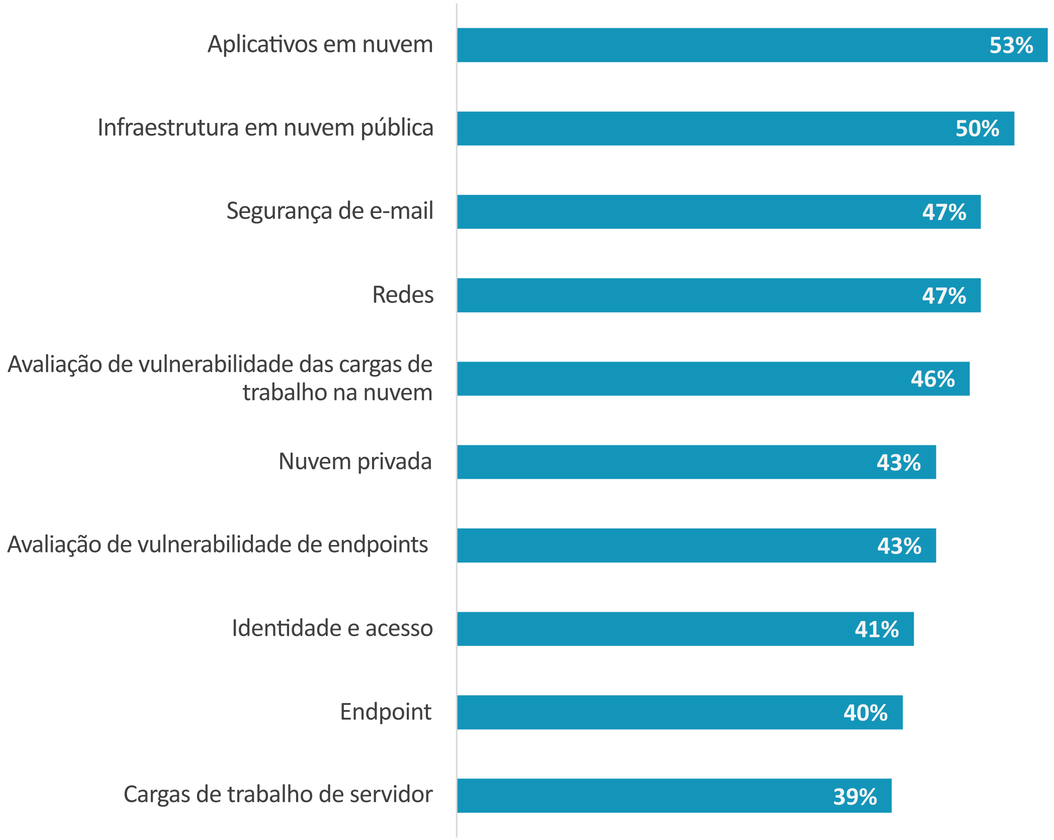
VOLTAR AO ÍNDICE

Espera-se uma pilha de tecnologia aberta, mas **a MDR deve trazer todos os mecanismos**

As operações de nuvem e segurança são os principais critérios tecnológicos para a escolha de MDR

Os clientes de MDR esperam que o provedor apresente cobertura abrangente da segurança em todos os vetores de ataque. Além disso, os usuários de MDR esperam que o provedor trabalhe em conjunto com os mecanismos de segurança já estabelecidos, desde um conjunto completo de controles de segurança, inclusive endpoint, rede, nuvem e e-mail, até uma pilha completa de ferramentas de operações de segurança, inclusive SIEM, SOAR, EDR, NDR, XDR, gerenciamento de superfície de ataque, detecção de ativos e gerenciamento de vulnerabilidades.

Tecnologias de detecção/agente que as organizações esperam de um provedor de MDR.



Tecnologias de operações de segurança que as organizações esperam de um provedor de MDR.

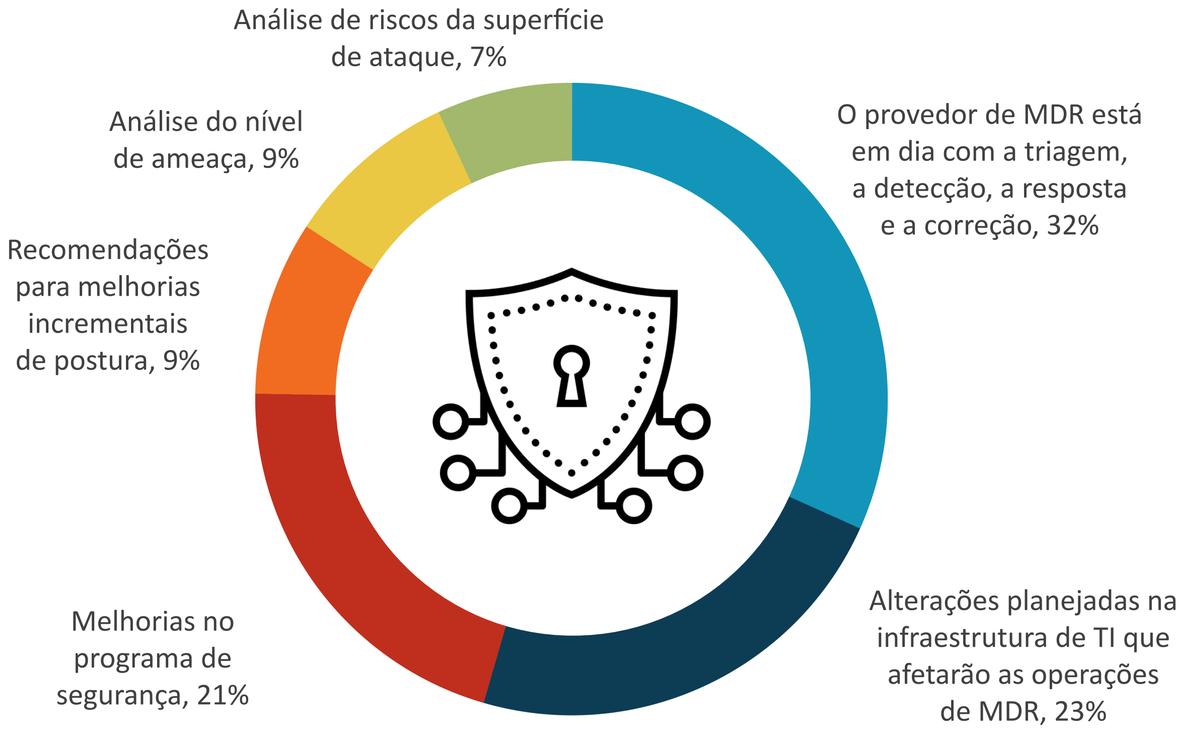
VOLTAR AO ÍNDICE

Os modelos de engajamento com o cliente de MDR **são importantes**

Análises operacionais de MDR: o que é mais importante

Os líderes de segurança enfatizam que os modelos de engajamento de MDR são muito importantes, solicitando que os provedores de MDR não apenas fiquem em dia com a triagem, a detecção, a resposta e a correção, mas também acompanhem as alterações planejadas na infraestrutura de TI, as melhorias contínuas do programa de segurança, a análise de riscos da superfície de ataque e as análises no nível da ameaça — tudo isso enquanto recomendam ações para melhorar cada vez mais a postura de segurança. Essas expectativas são altas, mas demonstram por que a maioria das organizações considera o provedor de MDR um parceiro estratégico.

Mais importante aspecto das análises operacionais do provedor de MDR.



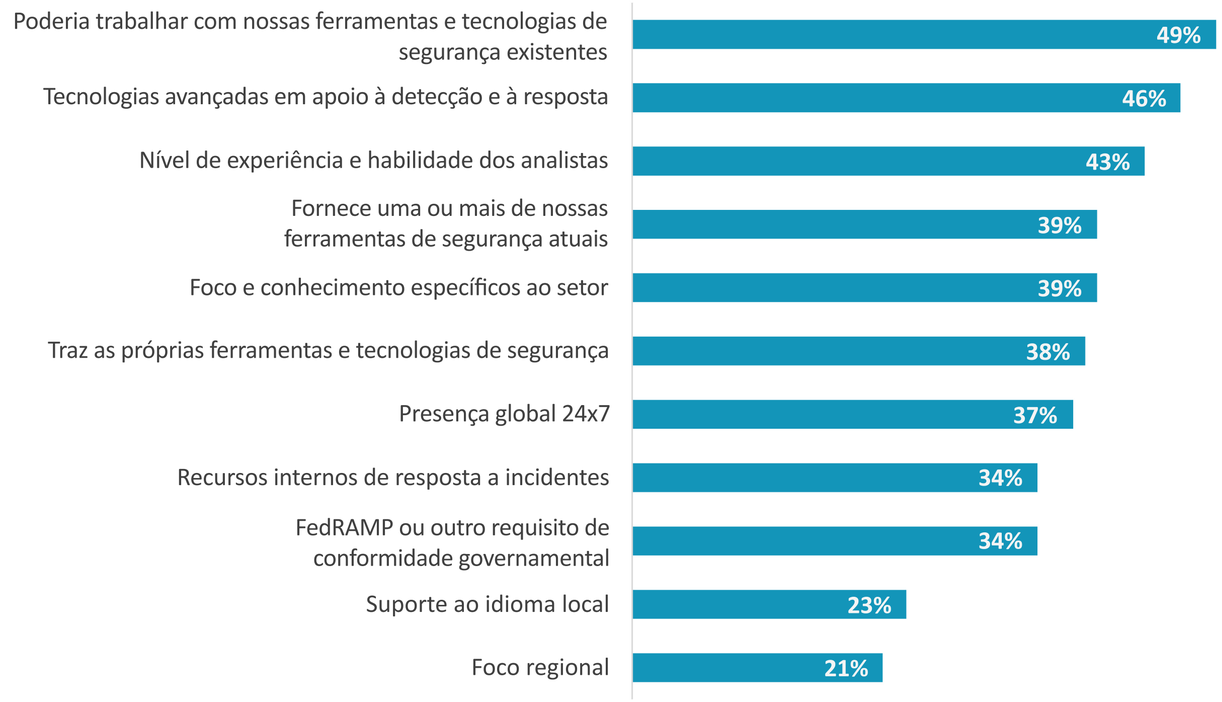
> Os líderes de segurança enfatizam que **os modelos de engajamento de MDR são muito importantes.”**

VOLTAR AO ÍNDICE

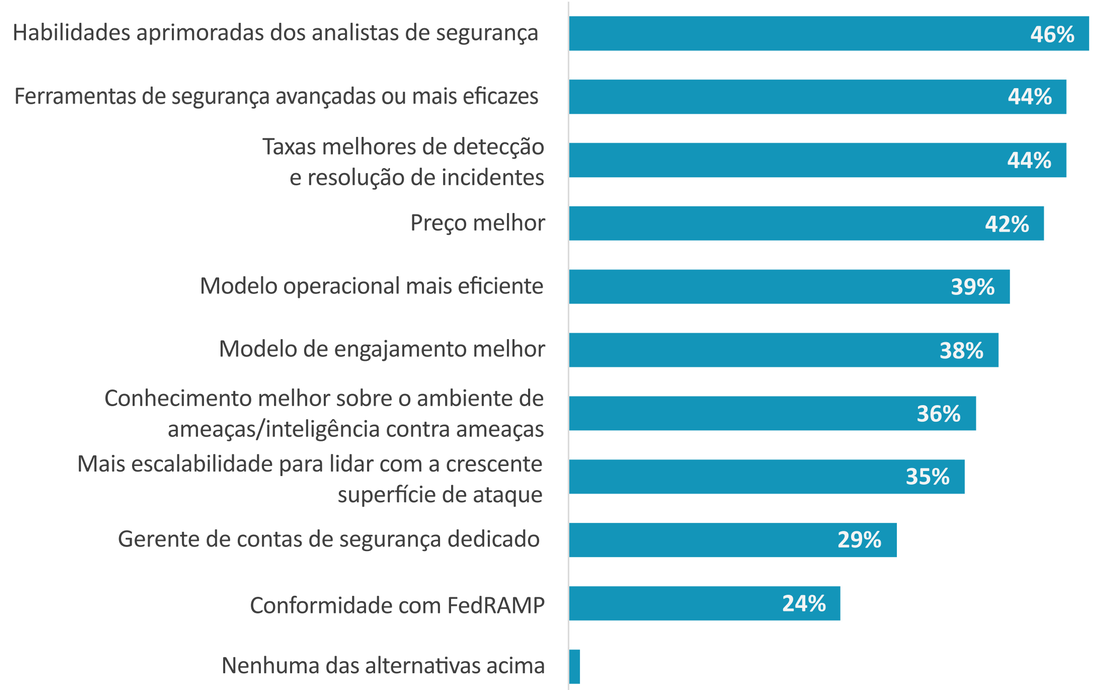
Habilidades e ferramentas avançadas podem incentivar a mudança de provedor de MDR

Quais considerações são importantes para as organizações quando elas avaliam e escolhem um provedor de MDR? Quase metade (49%) disse que eles devem trabalhar com a ferramenta de segurança e o ecossistema de tecnologia existentes, enquanto 46% querem ter recursos avançados de detecção e resposta. Outras 43% querem que o provedor de MDR tenha recursos de segurança especializados, que também é o fator mais comumente citado como um motivo para as organizações trocarem de provedor. Outros motivos incluem ferramentas de segurança mais avançadas e taxas aprimoradas de detecção e resolução, embora o preço e os modelos operacionais também sejam importantes.

Critérios importantes de seleção de provedores de MDR.



Fatores que motivariam as organizações a mudarem os provedores de MDR.



VOLTAR AO ÍNDICE

As megatendências do setor **estão afetando a escolha de MDR**

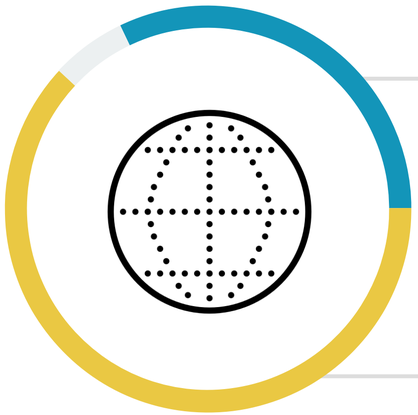
Mais de nove em dez

organizações identificam o suporte a MITRE ATT&CK como essencial ou muito importante.

O suporte a MITRE e XDR são fundamentais para a maioria na escolha de provedores de MDR

A escolha de um provedor de MDR geralmente envolve mais do que uma checklist de recursos e a cobertura. Amplas agendas do setor estão afetando ainda mais a escolha de provedores de MDR, sendo que mais de nove a cada dez organizações identificam o suporte a MITRE ATT&CK como essencial (32%) ou muito importante (62%). Além disso, quase três quartos (73%) relata que a tecnologia de segurança de detecção e resposta estendidas (XDR) foi considerada no processo de escolha de serviços de MDR. A borda de serviço de acesso seguro (SASE) e o gerenciamento de superfície de ataque (ASM) também foram considerados importantes por dois terços.

Importância de o provedor de MDR dar suporte à estrutura MITRE ATT&CK.



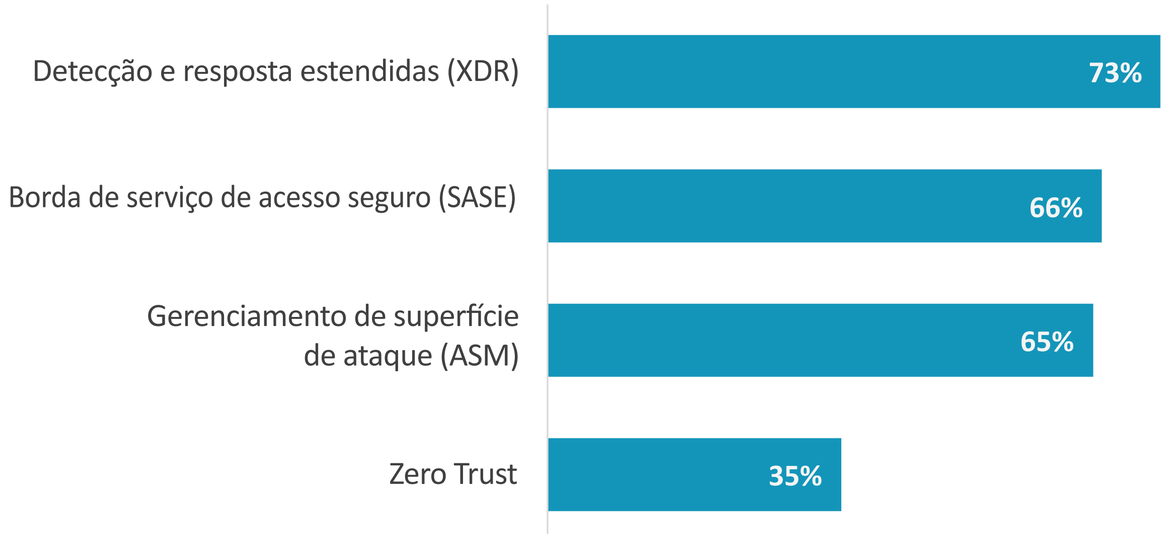
32%

Essencial — não consideraríamos um provedor de MDR que não desse suporte à estrutura MITRE ATT&CK

62%

Muito importante — preferimos trabalhar com um provedor de MDR que dê suporte à estrutura MITRE ATT&CK, mas consideraremos outros

Megatendências de segurança consideradas no processo de escolha de serviços de MDR.



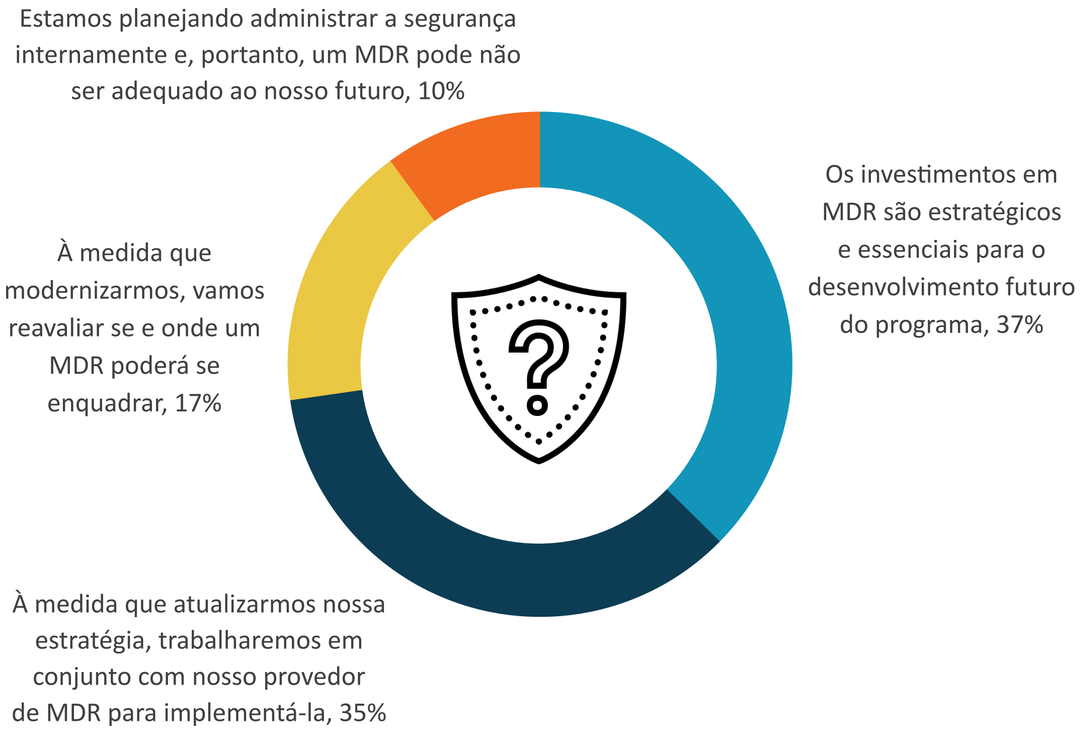
VOLTAR AO ÍNDICE

A MDR está se tornando uma estratégia de segurança mainstream

O uso de serviços de MDR tornou-se um componente principal da estratégia do programa de segurança, elevando os provedores de MDR a parceiros estratégicos. Elas ajudam as equipes de segurança e TI a acelerar o desenvolvimento do programa, melhorar a postura de segurança e colher benefícios menos visíveis, como o suporte aos objetivos de conformidade, a aquisição de seguros cibernéticos e a melhoria de habilidades e processos internos de segurança. Dessa forma, a maioria vê a MDR como parte contínua do investimento no programa de segurança, sendo que 37% relatam a MDR como estratégica e essencial, e outras 35% planejam trabalhar com o provedor de MDR à medida que atualizarem e implementarem estratégias futuras de segurança.

O ESG considera a MDR uma estratégia de segurança importante e mainstream e recomenda que as organizações explorem ainda mais os casos de uso adicionais que podem acelerar o desenvolvimento e a postura do programa de segurança.

Onde a MDR se enquadra no contexto mais amplo da modernização do SOC.



> A maioria vê a MDR como uma **parte contínua do investimento no programa de segurança.”**

VOLTAR AO ÍNDICE

DELL Technologies

A Dell Technologies (NYSE: DELL) ajuda organizações e indivíduos a construir o respectivo futuro digital e transformar a forma como trabalham, vivem e se divertem. A empresa fornece aos clientes o mais amplo e inovador portfólio de tecnologia e serviços do setor para a era dos dados.

SAIBA MAIS

SOBRE O ESG

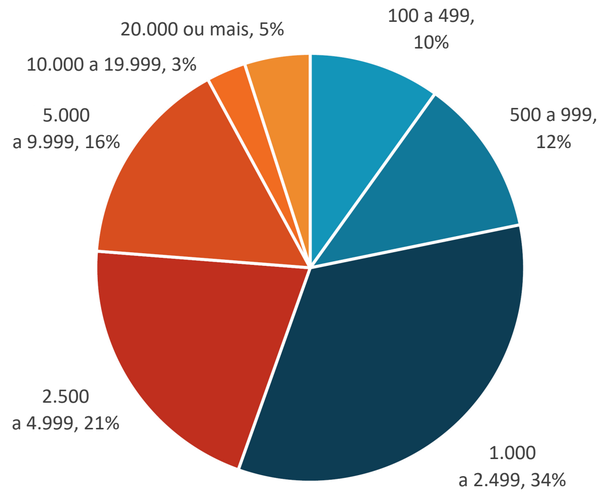
O Enterprise Strategy Group é uma empresa integrada de análise, pesquisa e estratégia de tecnologia, que fornece inteligência de mercado, percepções acionáveis e serviços de conteúdo de comercialização para a comunidade global de tecnologia.

Metodologia de pesquisa e dados demográficos

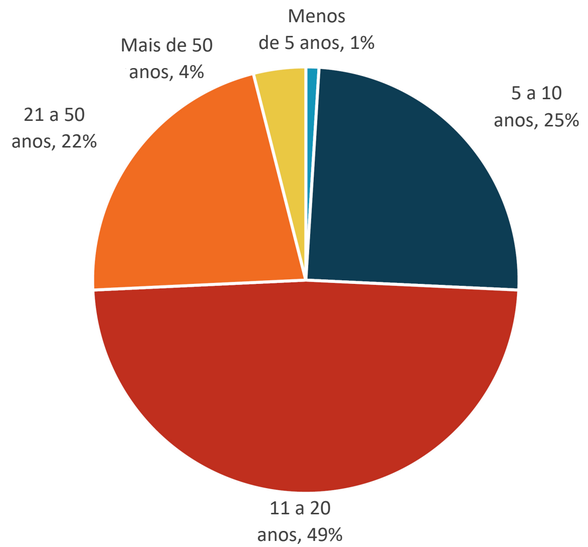
Para coletar dados para este relatório, o ESG conduziu uma abrangente pesquisa on-line com profissionais de segurança cibernética de organizações dos setores público e privado na América do Norte (Estados Unidos e Canadá) entre 3 de agosto e 14 de agosto de 2022. Para se qualificar a esta pesquisa, os entrevistados precisaram ser profissionais de segurança cibernética pessoalmente envolvidos com uma tecnologia de segurança cibernética, inclusive produtos, serviços e processos. Para concluir a pesquisa, todos os entrevistados receberam um incentivo no formato de prêmios em dinheiro e/ou equivalentes em dinheiro.

Depois de filtrar os entrevistados não qualificados, remover as respostas duplicadas e fazer uma triagem das respostas restantes (de acordo com diversos critérios) para garantir a integridade dos dados, restou uma amostra final de 373 profissionais de segurança cibernética.

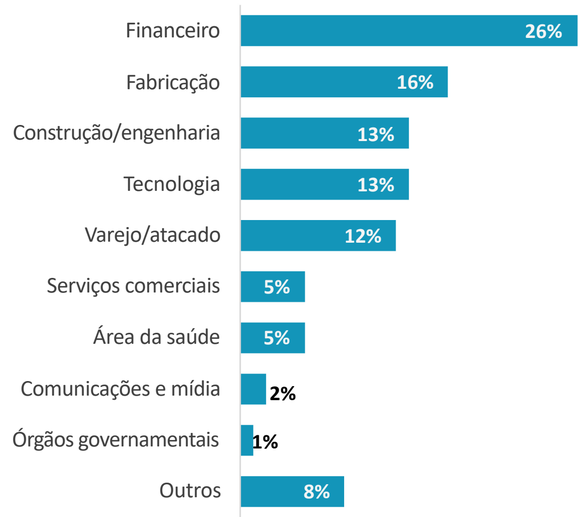
ENTREVISTADOS POR NÚMERO DE FUNCIONÁRIOS



ENTREVISTADOS POR IDADE DA EMPRESA



ENTREVISTADOS POR SETOR



VOLTAR AO ÍNDICE

O Enterprise Strategy Group é uma empresa integrada de análise, pesquisa e estratégia de tecnologia, que fornece inteligência de mercado, percepções acionáveis e serviços de conteúdo de comercialização para a comunidade global de tecnologia.