SOPHOS
Cybersecurity delivered.

O Estado do Ransomware na Saúde 2022

Resultados de uma pesquisa independente com 5.600 profissionais de TI em organizações de médio porte, incluindo 381 entrevistados na área de saúde, em 31 países.

Documento técnico Sophos. Maio de 2022

Introdução

Este estudo anual encomendado pela Sophos sobre as experiências reais com ransomwares enfrentadas por profissionais de TI na área de saúde que trabalham na linha de frente revelou um ambiente de ataque muito mais desafiador. Além de demonstrar a carga operacional e financeira que o ransomware coloca em suas vítimas, o relatório também evidencia a relação entre ransomware e seguro de proteção digital, incluindo o papel desempenhado pelas seguradoras no direcionamento das mudanças na defesa cibernética.

Sobre a pesquisa

A Sophos contratou uma agência de pesquisa de opinião, a Vanson Bourne, para realizar um estudo independente com 5.600 profissionais de TI, incluindo 381 entrevistados na área de saúde, em organizações de médio porte (de 100 a 5.000 funcionários) em 31 países. A pesquisa ocorreu durante os meses de janeiro e fevereiro de 2022, e os entrevistados foram solicitados a responder às questões com base na experiência que tiveram no ano anterior.

Os ataques estão crescendo e sua complexidade e impacto estão aumentando

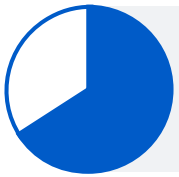
66% das organizações de saúde foram atingidas por ransomwares no ano passado, superior aos 34% em 2020. Trata-se de um aumento de 94% no decorrer de um ano, demonstrando que os adversários estão consideravelmente mais capazes de executar ataques que crescem em significância. Isso muito provavelmente também reflete o sucesso crescente do modelo ransomware como serviço, que amplia significativamente o alcance de um ransomware ao reduzir o nível de aptidão necessário para criar e lançar um ataque. Observação: ser atingido por um ransomware é definido com um ou mais dispositivos impactados por um ataque, mas não necessariamente criptografados.

Se compararmos a predominância dos ataques de ransomware em todos os setores pesquisados, o índice de ataques na saúde se equiparou à média global de 66%.

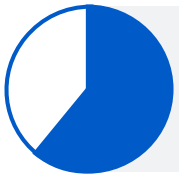
Em termos de índice de criptografia de dados, a saúde, com um índice de criptografia de 61%, apresentou melhor desempenho do que a média global, que foi de 65%, o que indica que a saúde estava mais bem preparada para impedir a criptografia de dados nos ataques de ransomware. Também houve uma queda no índice de criptografia da saúde em relação ao ano anterior (65% em 2020).

O percentual de vítimas que passaram por ataques apenas de extorsão, em que os dados não foram criptografados, mas que a organização ficou sob a ameaça de ter seus dados expostos, caiu de 7% em 2020 para 4% em 2021. Um motivo para essa boa postura pode estar no fato de que mais organizações de saúde estão agora optando pelo seguro de proteção digital, o que demanda grandes melhorias nas defesas de segurança cibernética. Analisaremos essa tendência mais adiante, no fim do relatório.

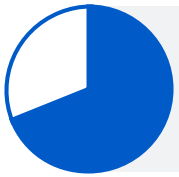
O aumento dos ataques de ransomware de sucesso é parte de um ambiente de ameaças que se torna cada vez mais difícil de tratar e que afetou o setor de saúde mais do que qualquer outro setor. A saúde viu o maior aumento em volume de ataques cibernéticos (69%), bem como em complexidade de ataques cibernéticos (67%), comparado à média entre setores de 57% e 59%, respectivamente. Em termos do impacto desses ataques cibernéticos, a saúde foi o segundo setor mais afetado (59%) comparado à média global de 53%.



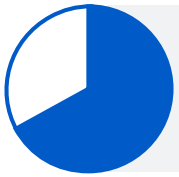
66%
atingidos por ransomwares no ano passado



61%
ataques que resultaram em dados criptografados



69%
aumento no volume de ataques cibernéticos, o mais alto entre todos os setores



67%
aumento na complexidade dos ataques cibernéticos, o mais alto entre todos os setores

59%
aumento no impacto dos ataques cibernéticos, o segundo mais alto entre todos os setores

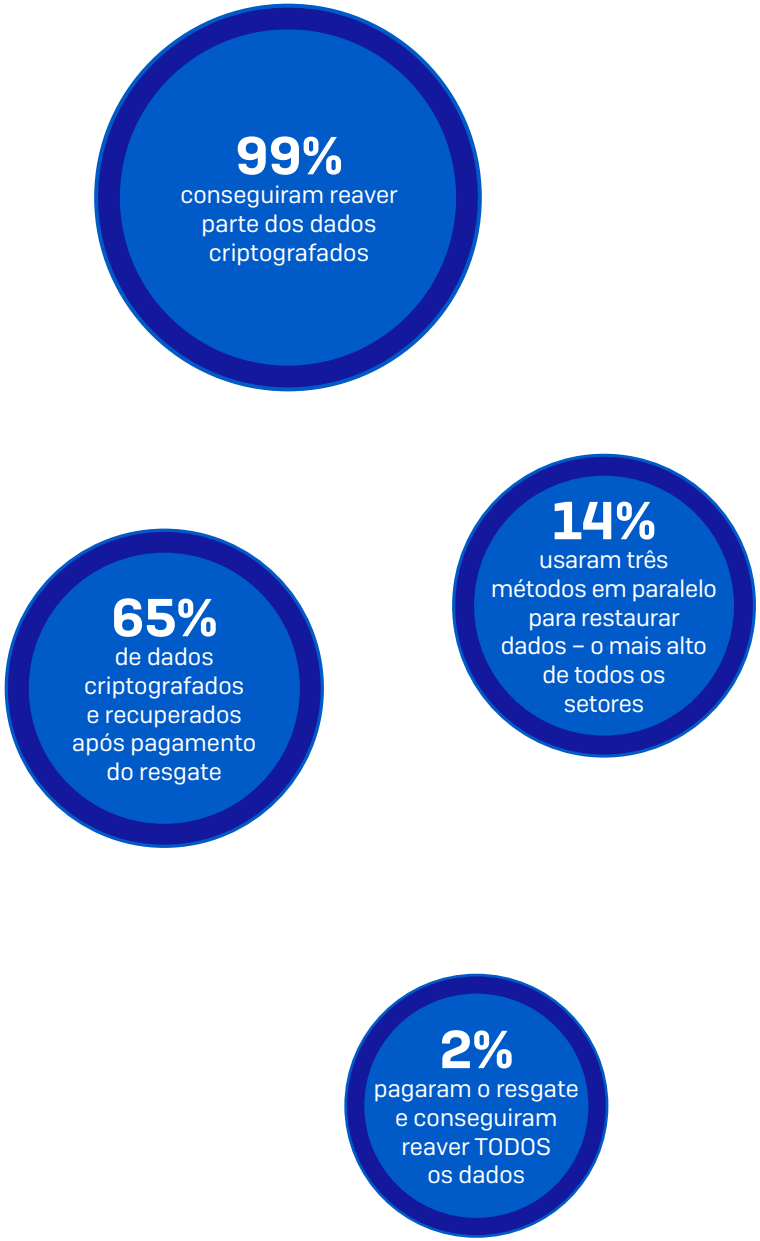
A saúde está melhorando na restauração de dados após um ataque

Com a maior predominância de ransomwares, as organizações melhoraram na forma como tratam as repercussões de um ataque. 99% das organizações de saúde atingidas por ransomwares no ano passado, hoje já conseguem recuperar parte dos dados criptografados, um aumento considerável em relação aos 93% do ano anterior.

Backups são o método mais utilizado para recuperar dados, usados por 72% das organizações de saúde cujos dados foram criptografados. Ao mesmo tempo, 61% disseram ter pago o resgate para restaurar os dados, e 33% disseram ter usado outros meios para restaurar os dados. Esses números refletem o fato de que muitas organizações de saúde usam diferentes abordagens de restauração para maximizar a velocidade e a eficiência com que conseguem voltar ao trabalho. Na verdade, um pouco mais da metade (52%) dos entrevistados de organizações cujos dados foram criptografados usaram vários métodos para restaurar esses dados.

A saúde atingiu o pico do gráfico (14%) por usar todos os três métodos em paralelo para restaurar dados criptografados: backups, pagamento de resgate e outros meios, quando a média global foi de 7%. A saúde é extremamente dependente da disponibilidade de dados para dar continuidade a suas operações comerciais. A falta de acesso imediato a dados pode atrasar o tratamento de um paciente, o que já se mostrou catastrófico. As tentativas da saúde de restaurar dados usando todos os meios disponíveis é compreensível.

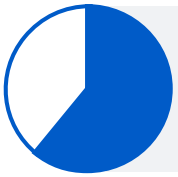
Ainda que pagando o resgate você quase sempre consiga reaver parte dos dados, a porcentagem de dados restaurados após o pagamento diminuiu. Em média, em 2021, as organizações de saúde que realizaram o pagamento recuperaram apenas 65% dos dados, uma queda em comparação aos 69% em 2020. Comparativamente, em 2021, apenas 2% das que pagaram o resgate conseguiram reaver TODOS os dados, inferior aos 8% de 2020.



O setor de saúde está mais propenso a pagar resgate

A saúde é o setor mais propenso a pagar resgate, com 61% dos entrevistados, cujos dados foram criptografados, admitindo que pagaram o resgate, comparado à média entre setores de 46%. Esse número também é quase o dobro dos 34% que pagaram o resgate em 2020. O maior aumento no volume e complexidade de ataques na saúde, quando comparado a outros setores, é um provável motivo por trás da grande propensão a pagar e ultrapassar seus limites, conforme planejado, para lidar com esse tipo de ataque.

Outro motivo, como você verá mais adiante nesse relatório, poderia ser o impacto do ransomware que afeta não apenas os dispositivos e bancos de dados criptografados, mas também as operações e a rentabilidade comercial das organizações de saúde, fazendo com que se apressem para voltar à normalidade. Por fim, os altos custos para reparar um ataque ao setor de saúde – o segundo mais alto entre os setores, US$ 1,85 milhão, como veremos a seguir no relatório – podem levar as organizações de saúde a pagar, em vez de gastar com os custos de remediação.



61%
índice de pagamento de resgate pela saúde

△ Pagamento de resgate △

61%
2021

34%
2020

A saúde pagou o valor de resgate mais baixo

Ainda que a saúde esteja no topo da lista em volume de pagamento, ela está no fim da lista em termos de valor pago. No geral, a saúde apresentou a média mais baixa de pagamento (cerca de US$ 197 mil) de todos os setores citados. Portanto, ainda que seja alta a ocorrência de pagamentos de resgate no setor de saúde, o valor dos resgastes pagos é relativamente baixo. Esses valores baixos são provavelmente fruto dos problemas financeiros pelos quais muitas organizações de saúde vêm passando, especialmente as do setor público. Elas simplesmente não têm mais dinheiro para os invasores sugarem.

É interessante observar que mesmo que o setor de saúde tenha sido o que pagou resgastes mais baixos, o valor total de resgate pago pela saúde em 2021 na verdade subiu 33% comparado a 2020.

Se nos aprofundarmos mais nos detalhes, 60% dos valores de resgate pagos pela saúde foram inferiores a US$ 50 mil. Apenas três entrevistados disseram que suas organizações pagaram US$ 1 milhão ou mais. Isso vai de encontro à tendência vista nos outros setores pesquisados, em que, no ano passado, a proporção de vítimas que pagaram resgates de US$ 1 milhão ou mais quase triplicou, de 4% em 2020 para 11% em 2021. Paralelamente, o percentual que pagou menos de US$ 10.000 caiu de um em cada três (34%), em 2020, para um em cada cinco (21%), em 2021.

US$ 197 mil

pagamento médio de resgate pela saúde, mais baixo entre setores

33%

aumento em pagamento de regaste da saúde no ano anterior

60%

valores de resgate na saúde inferiores a US$ 50.000

Os ransomwares têm um grande impacto comercial e operacional na saúde

Os valores dos resgates são apenas parte da história, e o impacto do ransomware é muito mais amplo do que apenas entre dispositivos e bancos de dados criptografados. 94% das organizações de saúde que foram atingidas por ransomwares no último ano disseram que o ataque mais significativo impactou sua capacidade de operação. Além disso, 90% das organizações de saúde do setor privado disseram que perderam negócios ou receita.

Entre todos os setores, o custo médio para uma organização retificar o impacto do ataque de ransomware mais recente foi US$ 1,4 milhão, em 2021, uma queda em relação a 2020, quando foi US$ 1,85 milhão. Muito provavelmente, essa queda é reflexo da predominância e impacto do seguro de proteção digital, situação em que as seguradoras estão mais aptas a orientar as vítimas com rapidez e eficácia no processo de resposta a incidentes, reduzindo o custo do reparo.

Contudo, no caso da saúde, o custo médio de remediação subiu de US$ 1,27 milhão em 2020 para US$ 1,85 milhão em 2021. Na verdade, a saúde ficou em segundo lugar em termos de custo médio para retificar um ataque de ransomware em comparação à média entre setores (US$ 1,85 milhão x US$ 1,4 milhão). Como vimos no início do relatório, os ataques de ransomware na saúde quase dobraram no ano passado (66% em 2021 contra 34% em 2020). Pode ser esse o motivo de as organizações de saúde ficarem atrás de outros setores em sua capacidade de garantir um seguro de proteção digital – abordaremos isso em mais detalhes mais adiante no relatório. Falta de expertise em segurança cibernética, proliferação de dispositivos IoT médicos, vulnerabilidade dos sistemas legados e sua natureza operacional 24 horas por dia em atividade (o que leva à impossibilidade de reparar rapidamente os sistemas vulneráveis) continuam a afetar o setor de saúde, aumentando os custos gerais de remediação.

44% das organizações de saúde que sofreram um ataque no último ano levaram uma semana para se recuperar do ataque mais significativo, enquanto 25% delas levaram até um mês – um período muito longo para a maioria das organizações. A maior demora na recuperação foi observada no ensino superior e governo central/federal, em que cerca de duas em cada cinco instituições levaram mais de um mês para se restabelecer.

Além disso, algumas organizações continuam a depositar as esperanças em defesas ineficientes. Dos entrevistados da área da saúde cujas organizações não foram atingidas por ransomware no último ano, e que não esperam ser atingidos no futuro, 77% baseiam suas opiniões em abordagens que não impedem que as organizações sejam atacadas: 50% citaram backups e 43% citaram seguro de proteção digital como motivos pelos quais não anteveem um ataque, com alguns selecionando as duas respostas. Enquanto esses elementos ajudam na recuperação de um ataque, eles não impedem que ele aconteça.

94%
o ataque de ransomware impactou a capacidade de operação

90%
o ataque de ransomware causou perda de negócios/receita

US$ 1,85 milhão
custo médio para remediar um ataque na saúde, segundo mais alto entre setores

UMA SEMANA
tempo médio para se recuperar de um ataque

77%
depositam as esperanças em abordagens que não impedem o ataque

Organizações de saúde estão tendo dificuldades para encontrar um seguro de proteção digital

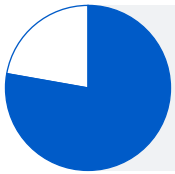
Entre todos os setores, 83% das organizações conseguiram fazer seguro de proteção digital contra ransomware. Em comparação, apenas 78% das organizações de saúde têm cobertura, e 46% delas dizem que há exclusões ou exceções em suas apólices. Dado o alto índice de incidentes de ransomware na saúde, essa brecha na cobertura do seguro deixa muitas organizações suscetíveis aos altos custos de um ataque.

Energia, petróleo/gás e serviços de utilidade são os mais propensos a ter cobertura (89%), seguidos de perto pelo varejo (88%). Manufatura e produção ficou por último com apenas 75% das organizações cobertas pelo seguro.

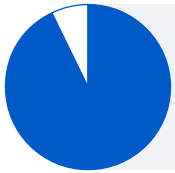
93% daqueles na área da saúde com seguro de proteção digital disseram que o processo para garantir a cobertura mudou bastante no decorrer do último ano, dificultando a obtenção de um seguro de proteção digital. 51% disseram que o nível de segurança cibernética que hoje é necessário para se qualificarem está mais alto, 45% disseram que as apólices estão mais complexas agora, 46% disseram que há menos empresas que oferecem seguro de proteção digital, 48% disseram que o processo está mais demorado e 34% disseram que está mais caro.

Essas mudanças estão estritamente ligadas a ransomwares, o maior propulsor dos sinistros de seguro de proteção digital. Nos últimos anos, os ataques de ransomware aumentaram, e os resgates e custos com pagamentos chegam a valores estratosféricos. Como consequência, algumas seguradoras saíram do mercado, pois, para elas, esse não é mais um negócio vantajoso. Aquelas que permanecem estão tentando diminuir o risco e a exposição. Elas também estão forçando uma alta de preços considerável.

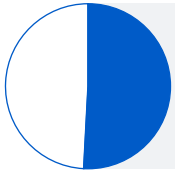
Com menos organizações oferecendo cobertura de proteção digital, o mercado está favorável às seguradoras. Elas ditam as regras e podem ser seletivas sobre quais clientes aceitar. Ter defesas cibernéticas fortes melhorará significativamente a capacidade da organização garantir a cobertura de que precisa.



78%
seguro de proteção digital contra ransomware na saúde



93%
processo para garantir a cobertura mudou no decorrer do último ano

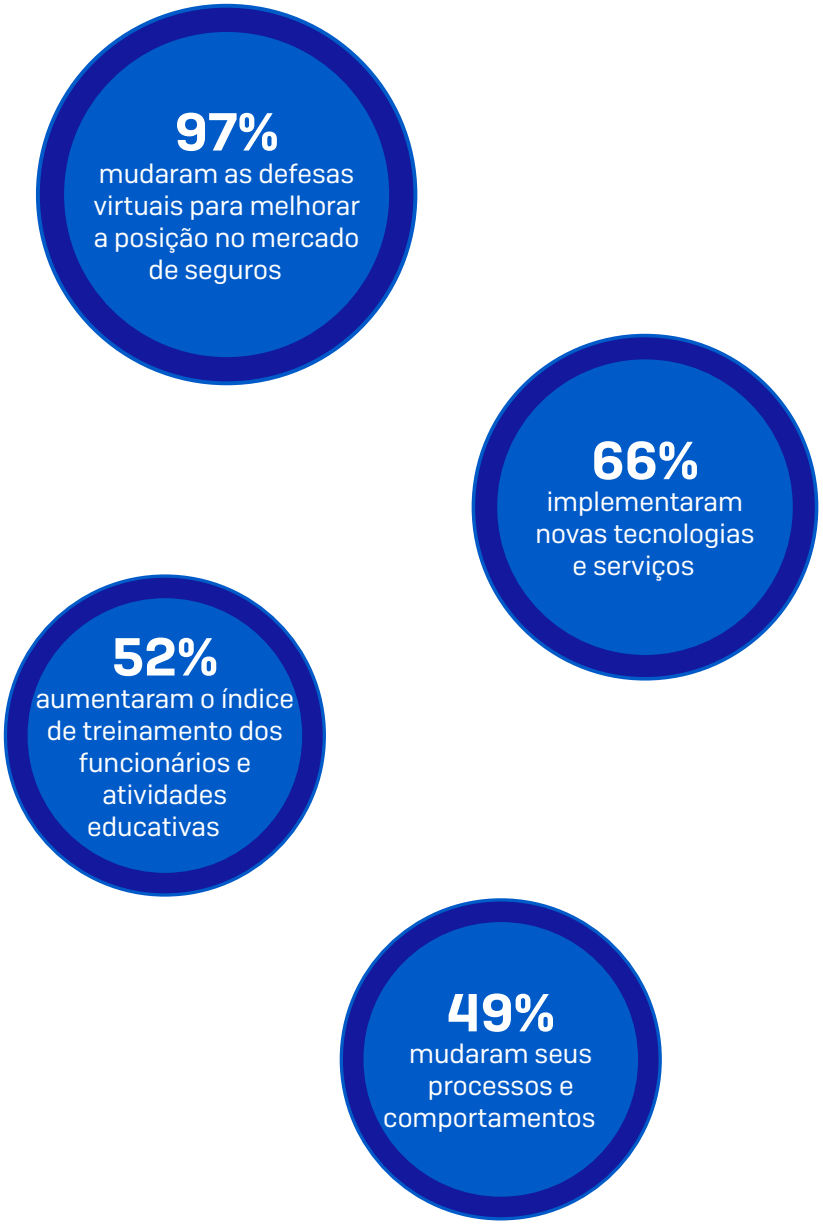


51%
nível necessário de segurança cibernética para qualificar para o seguro de proteção digital está mais alto

O seguro de proteção digital está levando a melhorias nas defesas cibernéticas

Conforme o mercado de seguro de proteção digital fica mais rígido e se torna mais difícil garantir a cobertura, 97% das organizações de saúde que têm seguro de proteção digital fizeram alterações em suas defesas cibernéticas para melhorar suas posições no mercado de seguros de proteção digital. 66% implementaram novas tecnologias e serviços, 52% aumentaram o índice de treinamento dos funcionários e atividades educativas, e 49% mudaram seus processos e comportamentos.

O enrijecimento do mercado de seguro de proteção digital é levado, em grande parte, pelo aumento nos pagamentos de ransomware, tornando-se a força motriz que impulsiona as melhorias nas defesas cibernéticas.

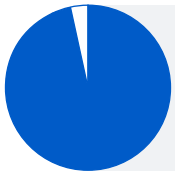


O seguro de proteção digital paga a maioria de todos os sinistros por ransomware

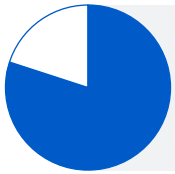
É tranquilizador para as organizações de saúde que têm a cobertura do seguro de proteção digital saber que 97% dos atingidos por ransomware, e que tinham um seguro de proteção digital que cobria ransomwares, disseram que a apólice pagou no ataque mais significativo. 81% dos entrevistados disseram que suas seguradoras pagaram pelos custos de limpeza, ou seja, os custos incorridos para restabelecer as atividades da organização. Comparativamente, 47% disseram que a seguradora pagou o resgate. Analisando o que o seguro de proteção digital pagou entre todos os setores, a pesquisa revela um aumento no pagamento dos custos de limpeza e uma queda nos pagamentos de resgate pelas seguradoras, em comparação aos resultados obtidos na pesquisa de 2020.

Contudo, o índice de pagamentos de resgate realizados varia consideravelmente de um setor para outro. Os mais altos índices, de acordo com a pesquisa, foram 53% no ensino fundamental (educação básica/média), 49% em governo local/estadual e 47% na saúde. Os pagamentos mais baixos foram 30% na manufatura e produção e 32% em serviços financeiros. É interessante observar que os setores com os mais baixos índices de pagamento também são aqueles capazes de se recuperar mais rapidamente de incidentes, enfatizando a importância de se estar preparado para a recuperação de desastres.

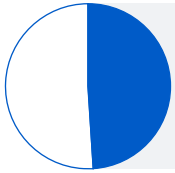
Vale observar que, embora o seguro de proteção digital possa ajudar a organização a voltar ao seu estado original, ele não cobre "melhorias", por exemplo, investimentos em melhores tecnologias e serviços para tratar de um ponto vulnerável que levou ao ataque.



97%
índice de pagamento do seguro de proteção digital na saúde



81%
seguradora pagou os custos de limpeza na saúde



47%
seguradora pagou o resgate

Conclusão

O desafio que as organizações enfrentam com os ransomwares continua a crescer. A proporção de organizações de saúde que são diretamente impactadas por ransomwares quase duplicou em 12 meses: de apenas um pouco mais de um terço em 2020 para dois terços em 2021.

Em face a essa quase normalização, as organizações de saúde ficaram melhores no tratamento que dispensam às consequências de um ataque: praticamente todas agora recebem de volta parte dos dados criptografados, e quase três quartos são capazes de utilizar backups para restaurar dados.

Ao mesmo tempo, a proporção de dados de saúde criptografados e restaurados após o pagamento do resgate caiu, em média, para 65%.

A saúde fez o pagamento médio mais baixo de regaste (US$ 197 mil).

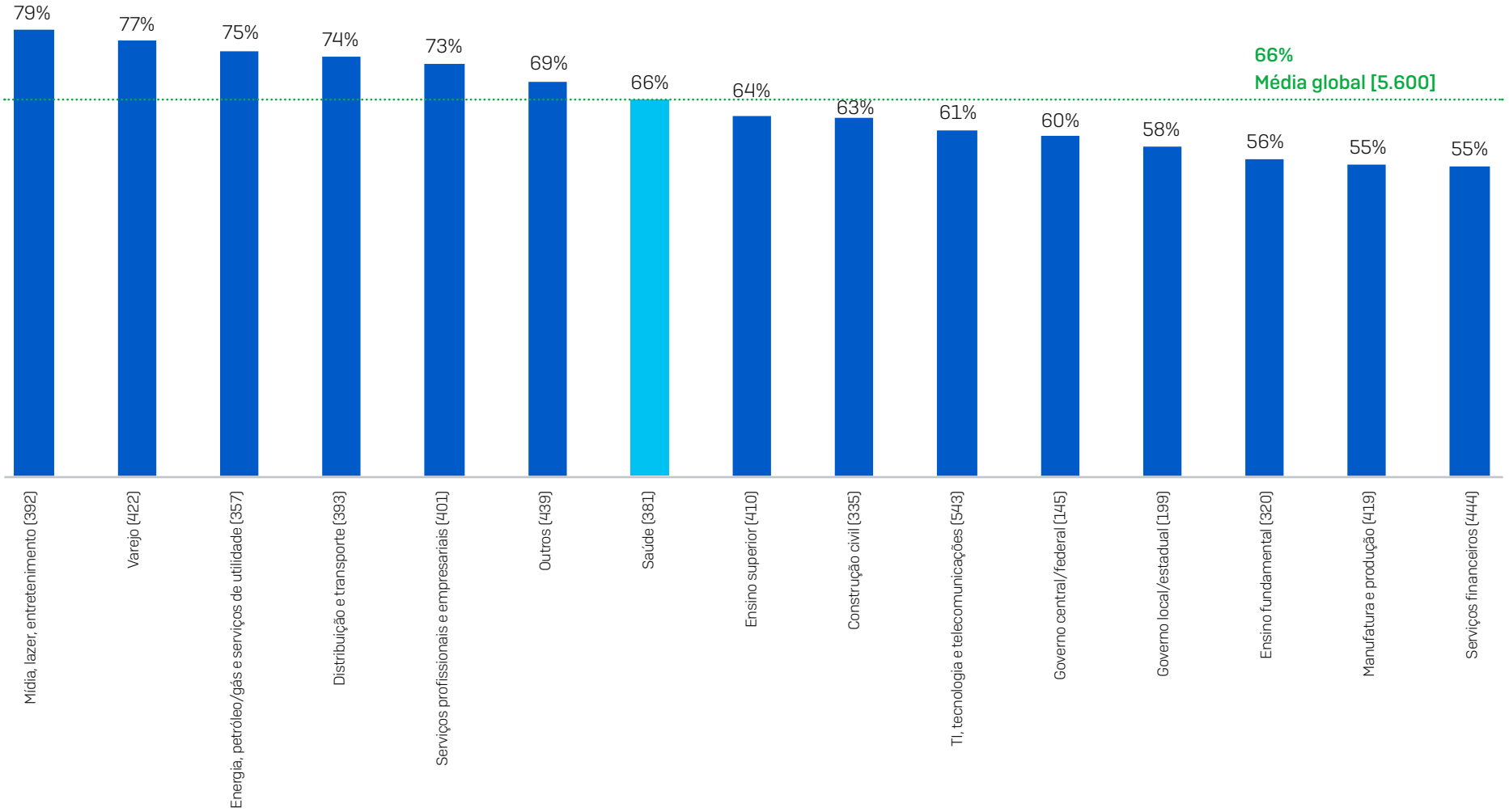
Ransomwares causam impacto nas operações, nos negócios e na receita da saúde. A maioria das organizações da saúde opta por reduzir o risco financeiro associado a tais ataques fazendo um seguro de proteção digital. Para elas, é tranquilizador saber que a seguradora pagará parte dos custos em quase todos os sinistros. Contudo, está ficando mais difícil para as organizações garantir a cobertura. Isso tem levado praticamente todas as organizações a fazer mudanças em suas defesas cibernéticas na intenção de melhorar suas posições no mercado de seguros de proteção digital.

Não importa se você quer ou não garantir a cobertura do seu seguro, otimizar a segurança cibernética é imperativo para todas as organizações. Nossas cinco dicas mais importantes:

- Assegure defesas de alta qualidade em todos os pontos do seu ambiente. Revise seus controles de segurança e confirme que continuam a atender às suas necessidades.
- Busque ameaças de maneira proativa de modo a ser capaz de deter os adversários antes que eles lancem seus ataques – se você não tem tempo nem pessoal interno, trabalhe com um serviço de segurança cibernética MDR especializado.
- Reforce o seu ambiente procurando e eliminando as lacunas na segurança: dispositivos sem patches, máquinas sem proteção, portas RDP abertas etc. A Detecção e Resposta Estendidas (XDR) é ideal para essa finalidade.
- Prepare-se para o pior. Saiba o que fazer na eventualidade de um incidente cibernético e quem você precisa contatar.
- Faça backups e pratique a restauração. Seu objetivo é voltar às atividades rapidamente, com um tempo mínimo de interrupção.

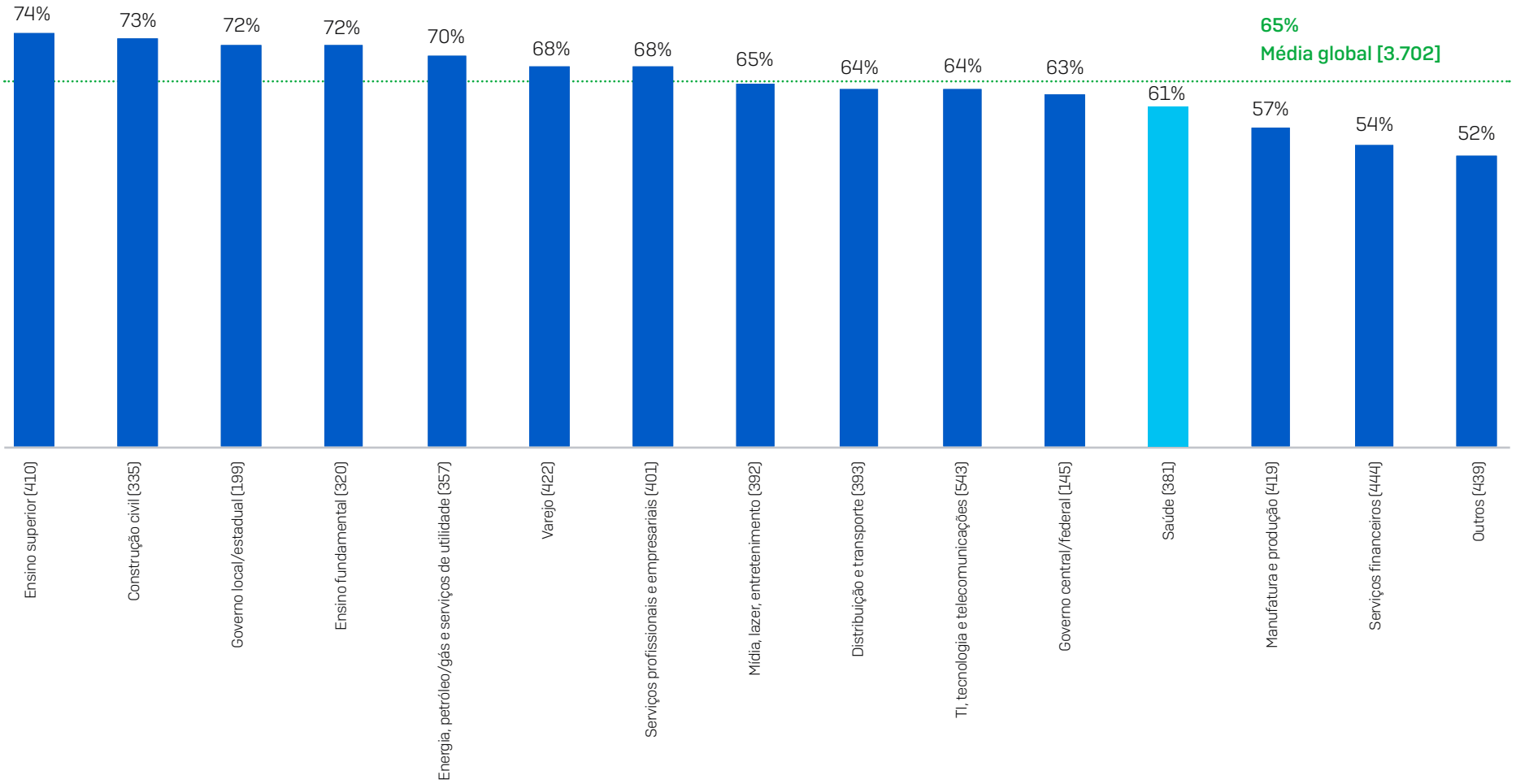
Para obter informações detalhadas sobre grupos individuais de ransomwares, consulte o centro de inteligência da Sophos sobre ameaças de ransomware.

Como a saúde está se saindo: ataques de ransomware por setor



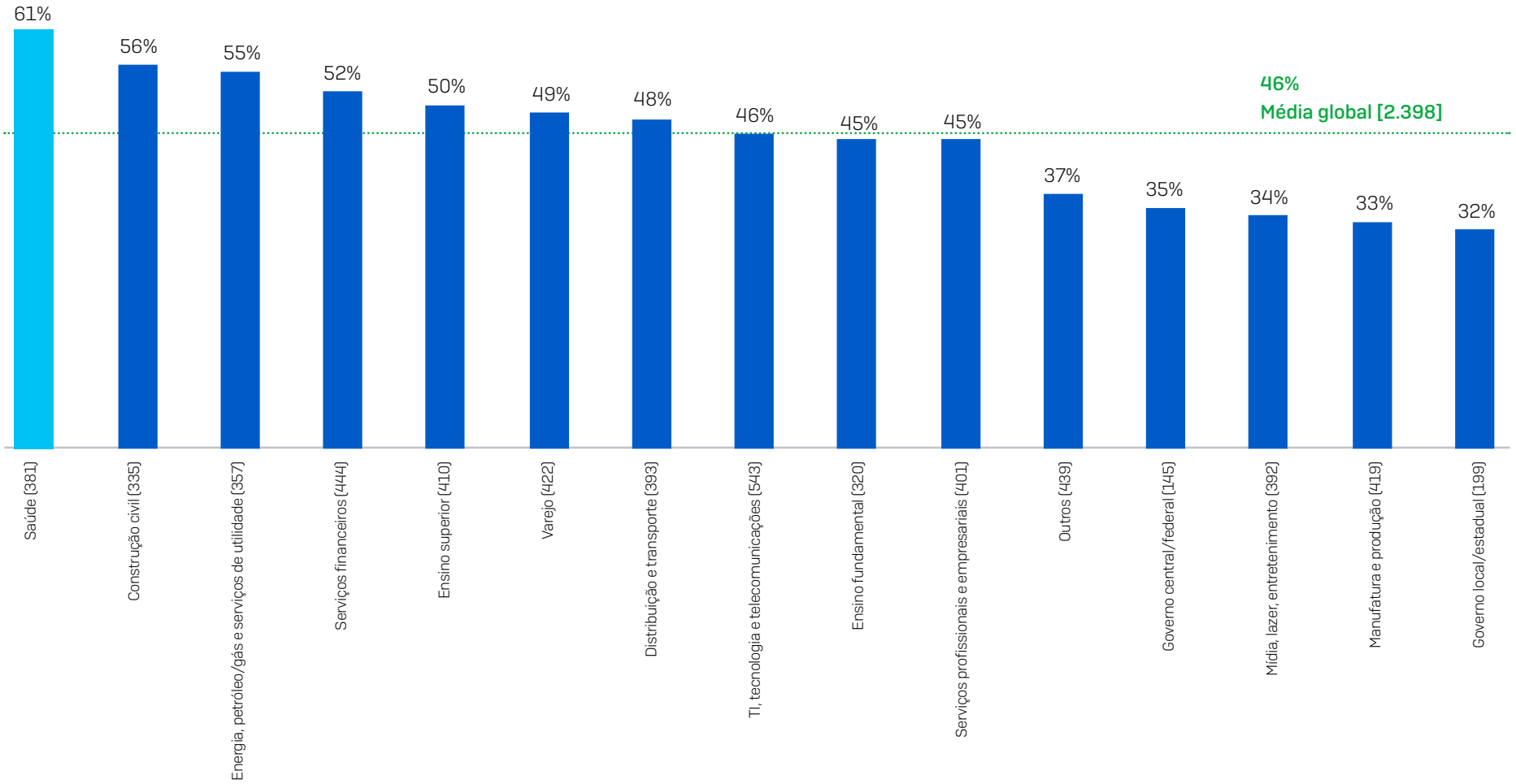
Sua organização foi atingida por ransomware neste último ano? [n=5.600]

Como a saúde está se saindo: índice de dados criptografados por setor



Os criminosos virtuais tiveram sucesso na criptografia de dados da sua organização nos ataques de ransomware mais significativos? (n=3.702 organizações atingidas por ransomwares no ano passado): Sim

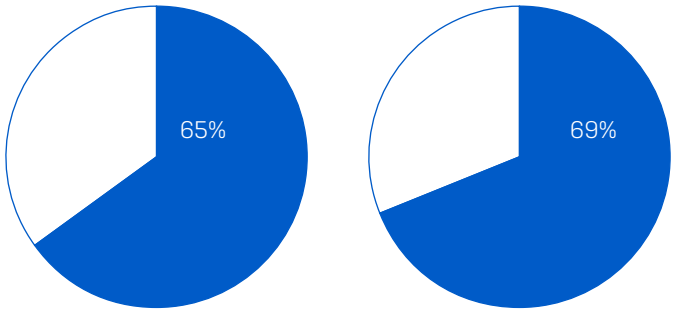
O setor de saúde está mais propenso a pagar resgate



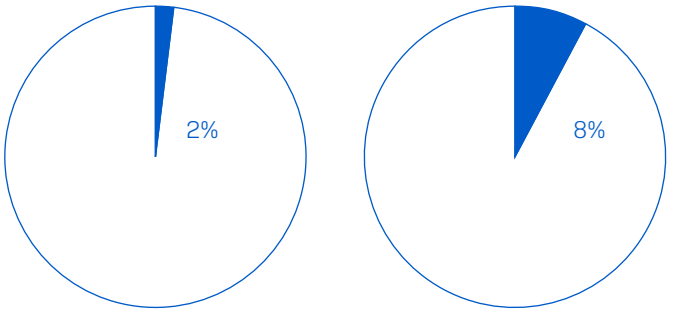
Sua organização conseguiu reaver dados capturados no ataque de ransomware mais significativo?
(n=2.398 organizações tiveram dados criptografados): Sim, pagamos o resgate e conseguimos reaver os dados

Menos dados são recuperados pela saúde do que no ano anterior após pagar o resgate

Porcentagem de dados recuperados após pagar o resgate

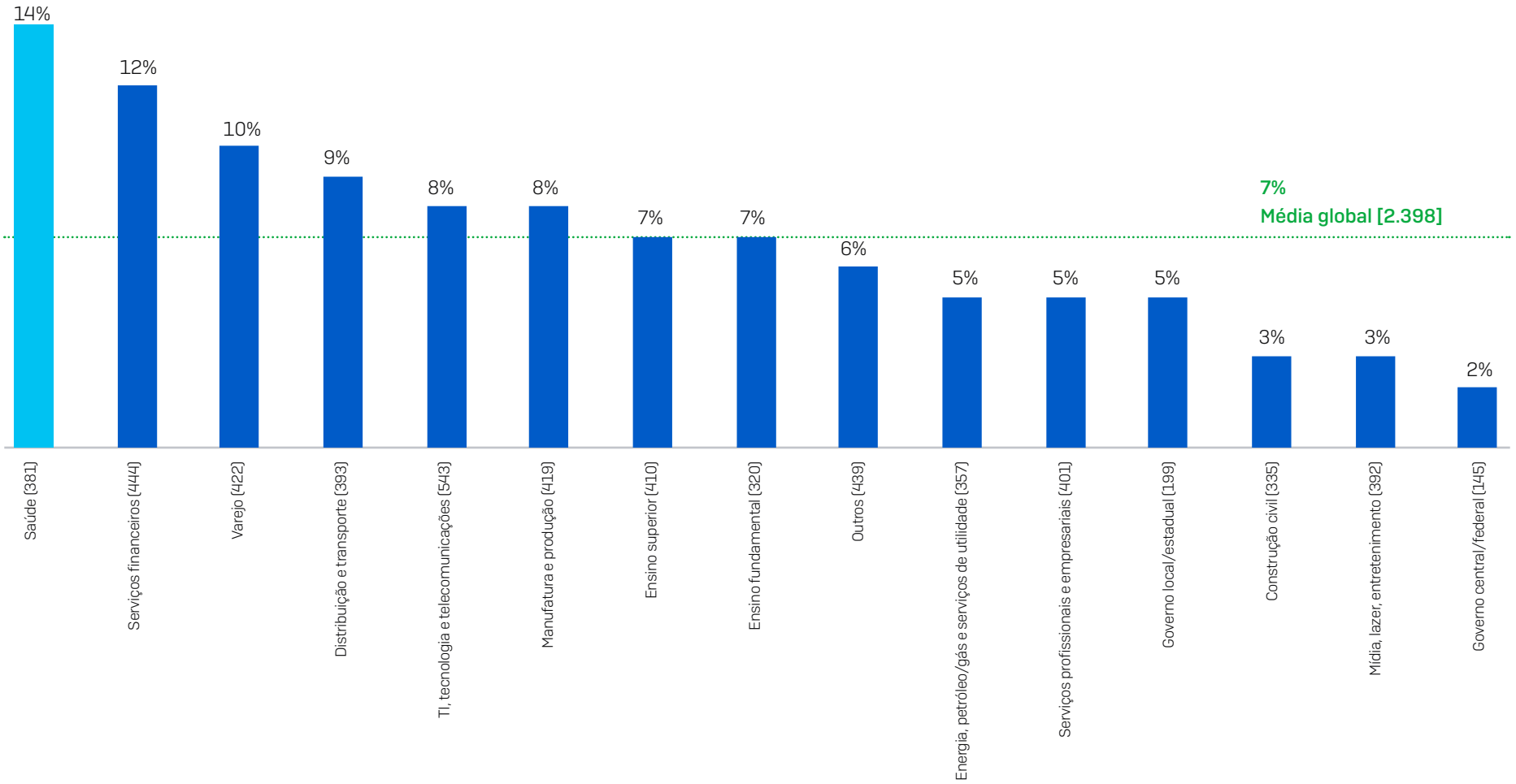


Porcentagem que conseguiu reaver TODOS os dados após pagar o resgate



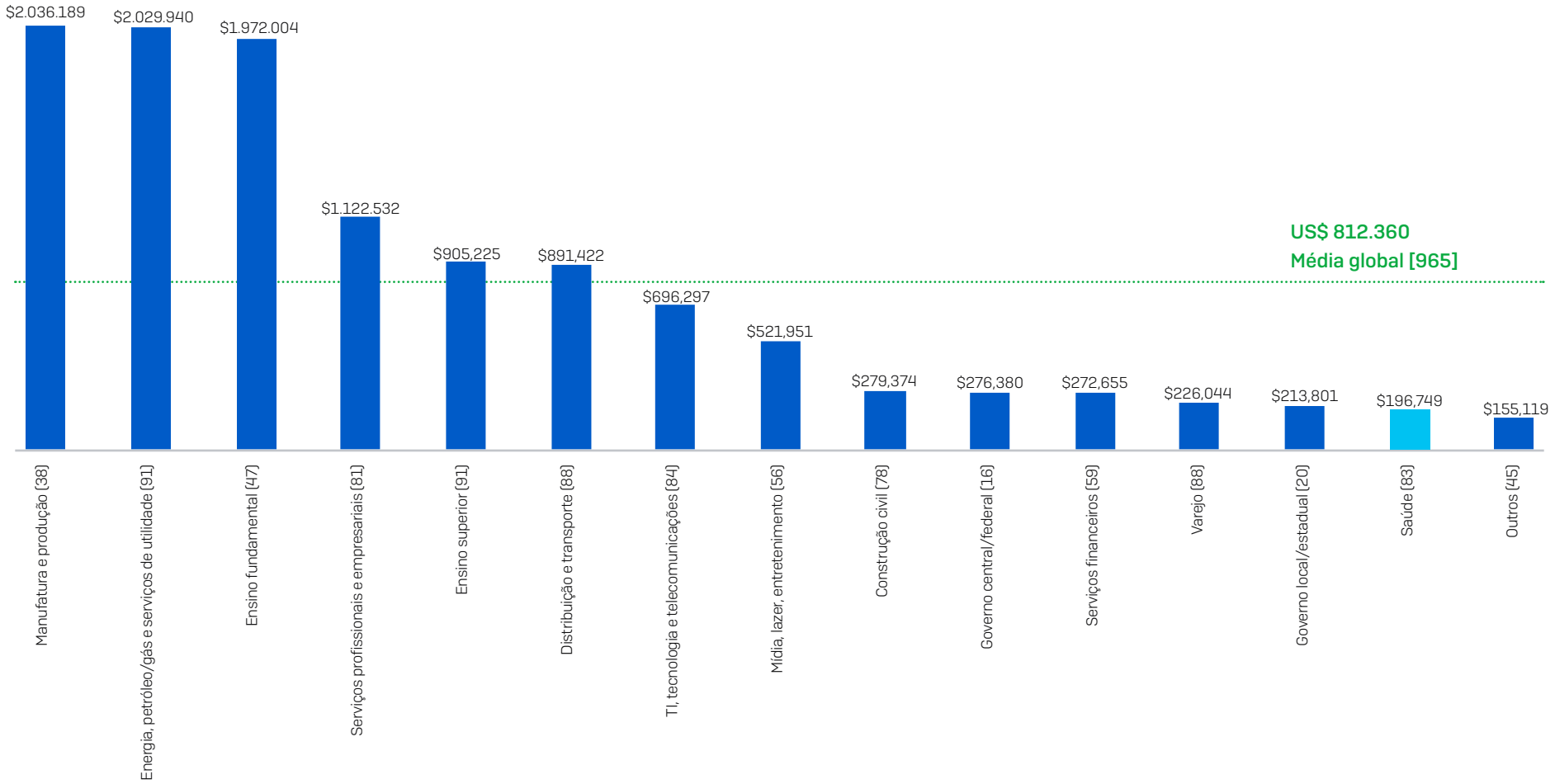
Quantos dos dados da sua organização vocês conseguiram reaver no ataque de ransomware mais significativo?
(94/25 organizações de saúde que pagaram o resgate e conseguiram reaver os dados)

A saúde está mais propensa a usar os três métodos para restaurar dados



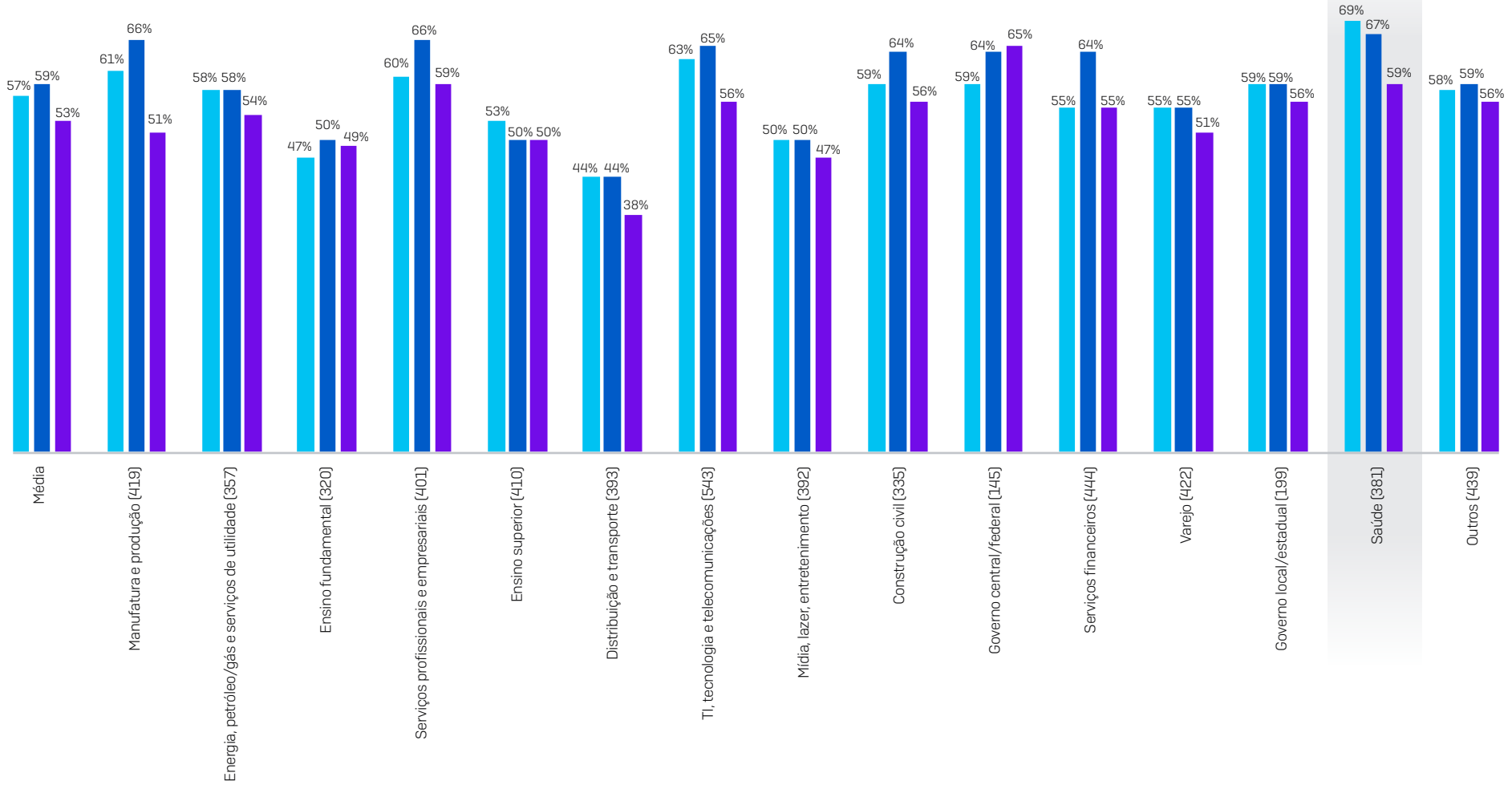
Sua organização conseguiu reaver dados capturados no ataque de ransomware mais significativo?
(2.398 organizações tiveram dados criptografados): Sim, usamos todos os três métodos (backups, pagamento de resgate e outros meios) para reaver os dados

A saúde fez os pagamentos mais baixos de regaste



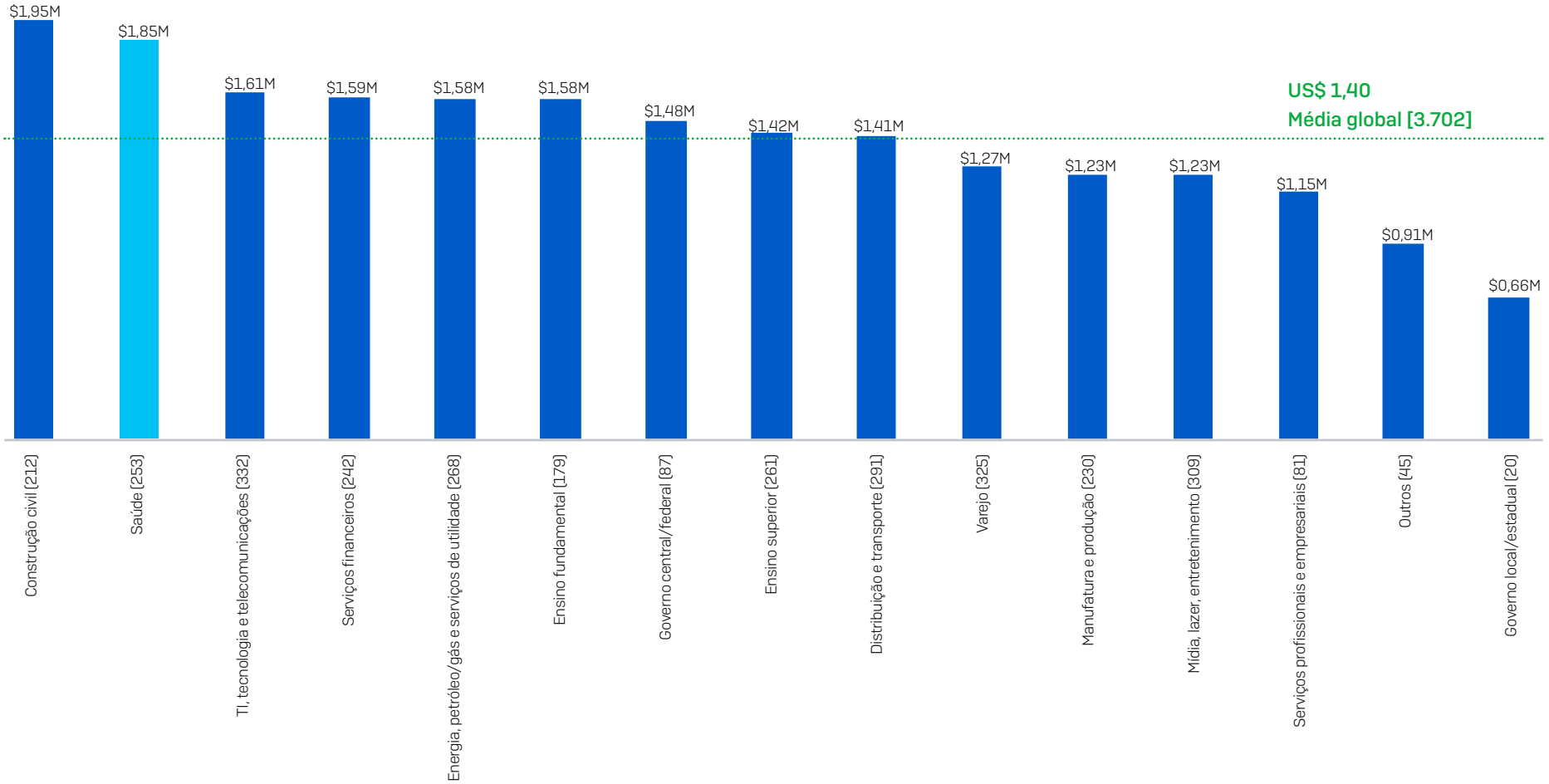
Qual foi o resgate que a sua organização pagou no ataque de ransomware mais significativo? US$. Número de base no gráfico. Excluindo respostas "Não sei".N.B. Para setores com número de base baixo, os resultados devem ser considerados indicativos.

Como a saúde está se saindo: mudança na experiência com ataques cibernéticos durante o último ano



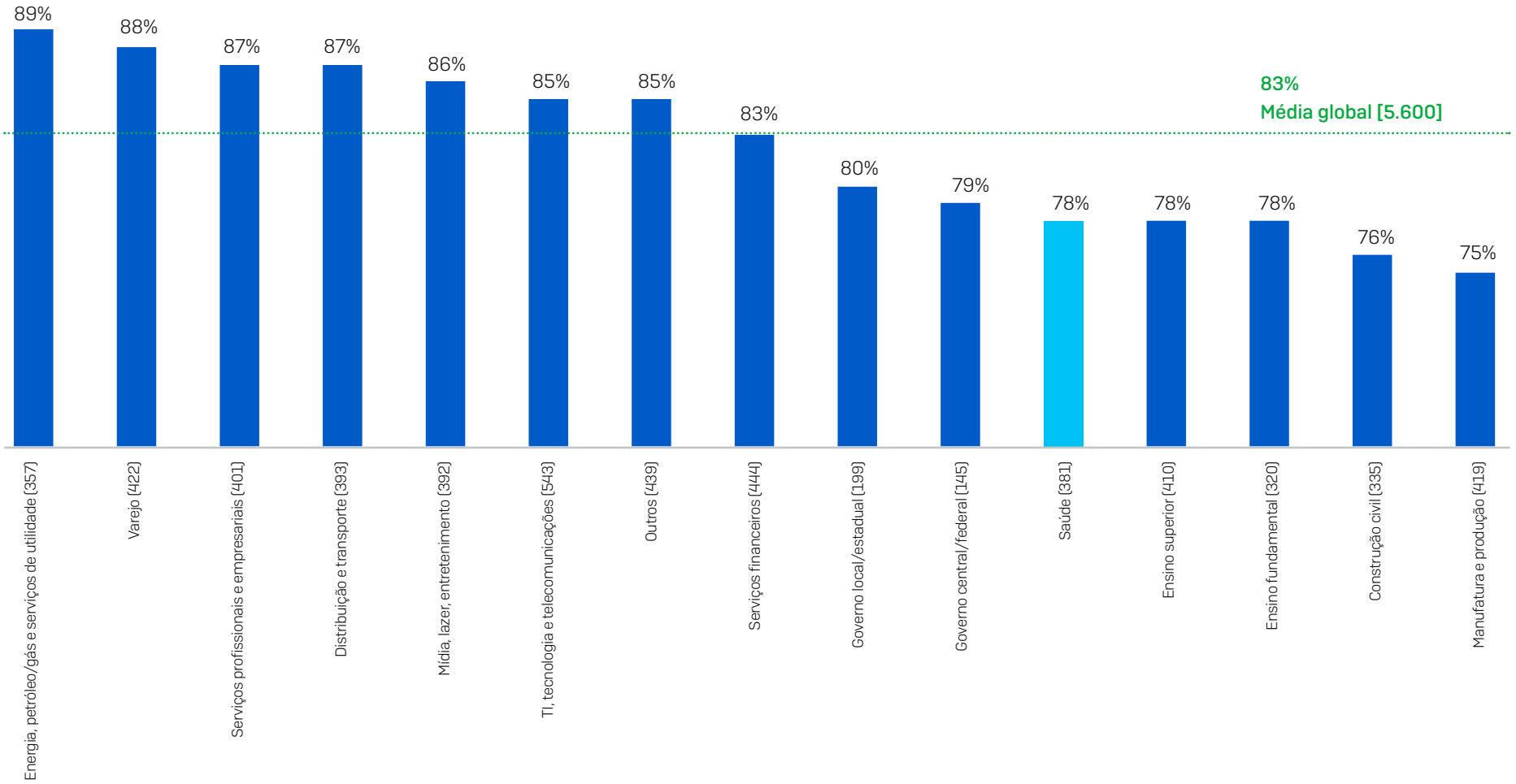
Em relação ao volume, complexidade e impacto, como a experiência da sua organização com ataques cibernéticos mudou no último ano? (n=5.600): Aumentou muito, Aumentou pouco

O custo de remediação de ransomware na saúde está acima da média global



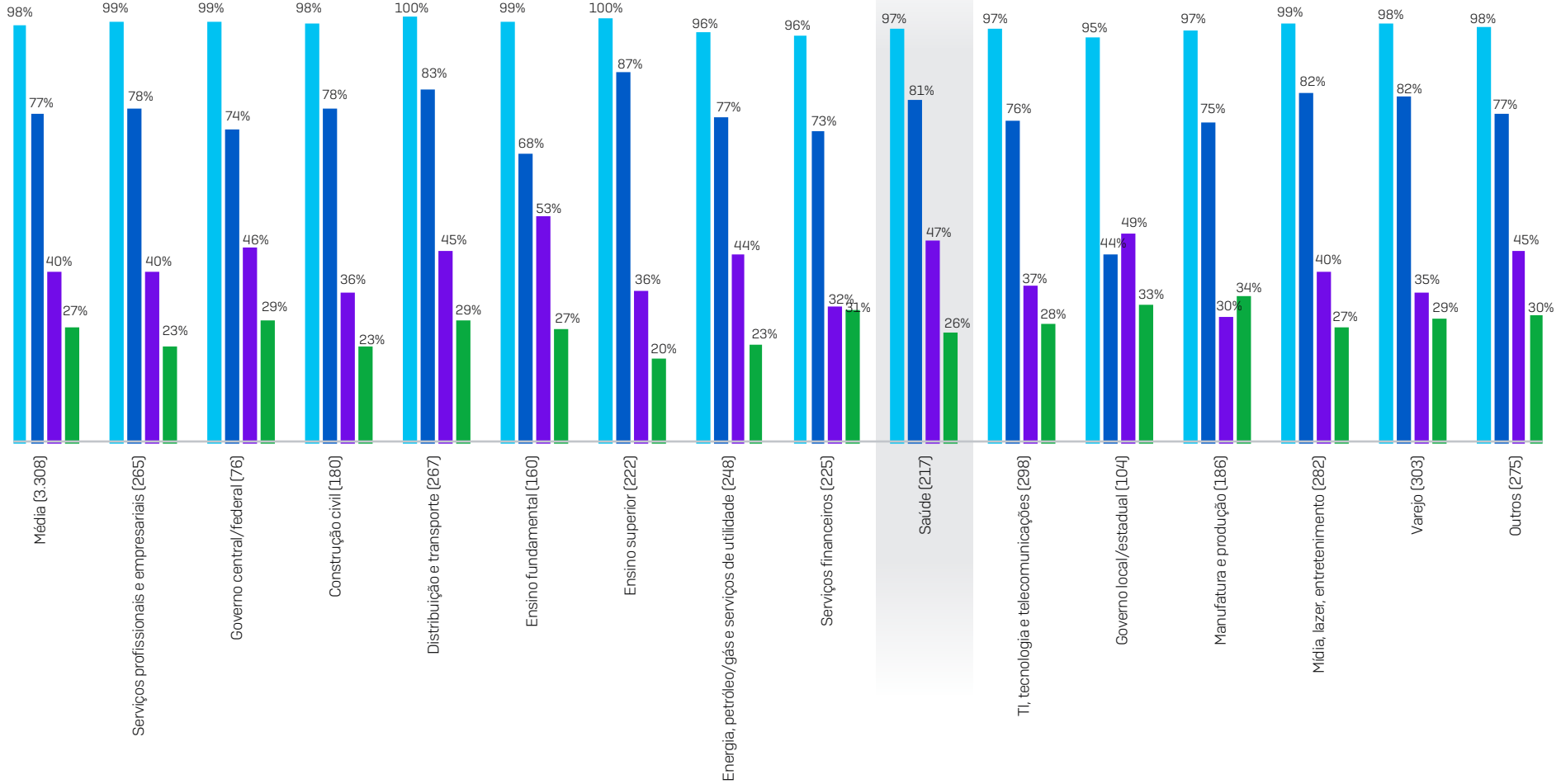
Qual foi o resgate que a sua organização pagou no ataque de ransomware mais significativo? US$. Número de base no gráfico. Excluindo respostas "Não sei".N.B. Para setores com número de base baixo, os resultados devem ser considerados indicativos.

A saúde apresenta índice abaixo da média de cobertura de seguro de proteção digital



Sua organização tem seguro de proteção digital com cobertura contra ataques de ransomware? (números de base no gráfico)
Sim; Sim, mas há exceções/exclusões em nossa apólice

Como a saúde está se saindo: Índice de pagamento de seguro de proteção digital por setor



O seguro de proteção digital pagou de modo a cobrir os custos associados ao ataque de ransomware mais significativo que a sua organização enfrentou? (n=3.308 organizações que foram atingidas por ransomware no ano anterior e que tinham seguro de proteção digital que cobria ransomware.) Sim, pagou pelos custos de limpeza (por exemplo, os custos para recolocar a organização em atividade); Sim, pagou o resgate; Sim, pagou outros custos (por exemplo, custos com inatividade, perda de oportunidades)

Saiba mais sobre ransomware e como a Sophos pode ajudar a defender a sua organização.

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.

© Copyright 2022. Sophos Ltd. Todos os direitos reservados.
Empresa registrada na Inglaterra e País de Gales sob o nº. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, Reino Unido
A Sophos é marca registrada da Sophos Ltd. Todos os outros nomes de produtos e empresas mencionados são marcas comerciais ou marcas registradas de seus respectivos proprietários.

2022-05-23 (WP-NP)

SOPHOS