Global Data Protection Index 2021

Principais conclusões – Julho de 2021

VansonBourne

DELL Technologies

Foco das principais conclusões

1

O ambiente de risco de proteção de dados

2

A ameaça representada por ataques cibernéticos

3

Acompanhar o ritmo das tecnologias novas e emergentes

4

Vulnerabilidades da proteção de dados em ambientes de nuvem

5

O crescimento do "as a service"

6

Simplificação da proteção de dados

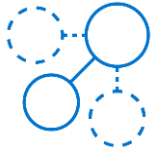
Cinco principais conclusões

A ampla adoção do trabalho em casa aumentou os **riscos cibernéticos e de proteção de dados**

Muitos não têm confiança na capacidade da proteção de dados de sua organização para se defender e se recuperar suficientemente de ameaças cibernéticas

Investimentos contínuos em tecnologias emergentes e nuvem **podem aumentar os desafios da proteção de dados**

Muitos **estão interessados em aproveitar o "as a service"** para aumentar a simplicidade e a flexibilidade da proteção de dados



Há evidências de que trabalhar com **menos fornecedores de proteção de dados** contribui para **melhores resultados na proteção de dados**

Quem entrevistamos?

1.000 responsáveis pelas decisões de TI foram entrevistados em fevereiro, março e abril de 2021

Organizações de uma ampla variedade de setores públicos e privados

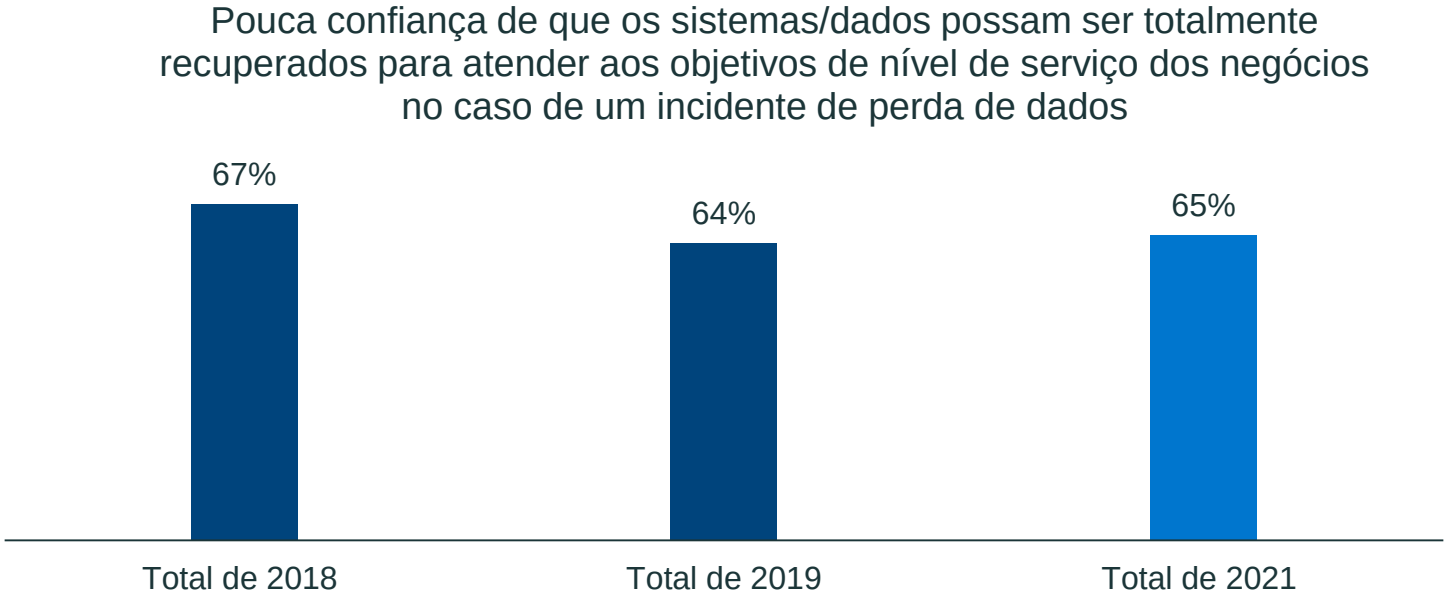
Organizações com mais de 250 funcionários

4 regiões:

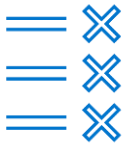
Américas (200)
EMEA (450)
APJ (250)
China (100)

1. O ambiente de risco de proteção de dados

Os responsáveis pelas decisões de TI não têm confiança na capacidade de suas próprias organizações de atender aos SLOs de recuperação



Além disso, a confiança de que os recursos de proteção de dados correspondam aos padrões internos e externos é baixa — isso se torna mais preocupante pelo fato de dois terços acreditarem que terão um evento disruptivo no próximo ano



58%

não estão muito confiantes de que a organização **esteja cumprindo seus objetivos de nível de serviço de backup e recuperação**

63%

não estão muito confiantes de que a infraestrutura e os processos de proteção de dados atuais da organização estejam em **conformidade com as normas regionais de governança de dados**

64%

estão **preocupados com a possibilidade de enfrentarem um evento disruptivo** nos próximos doze meses

Além desse motivo de preocupação, os problemas de perda de dados e de tempo de inatividade dos sistemas continuam a ter um impacto financeiro significativo nas organizações

US$
959.493

é o custo médio da perda de dados nos últimos 12 meses (em dólares americanos)

US$
513.067,00

é o custo médio do tempo de inatividade não planejado dos sistemas nos últimos 12 meses (em dólares americanos)

2. A ameaça representada por ataques cibernéticos

As organizações não têm a confiança de que suas medidas de proteção de dados possam reduzir os efeitos dos ataques cibernéticos. Além disso, a maioria acredita que há uma maior exposição com os funcionários trabalhando em casa

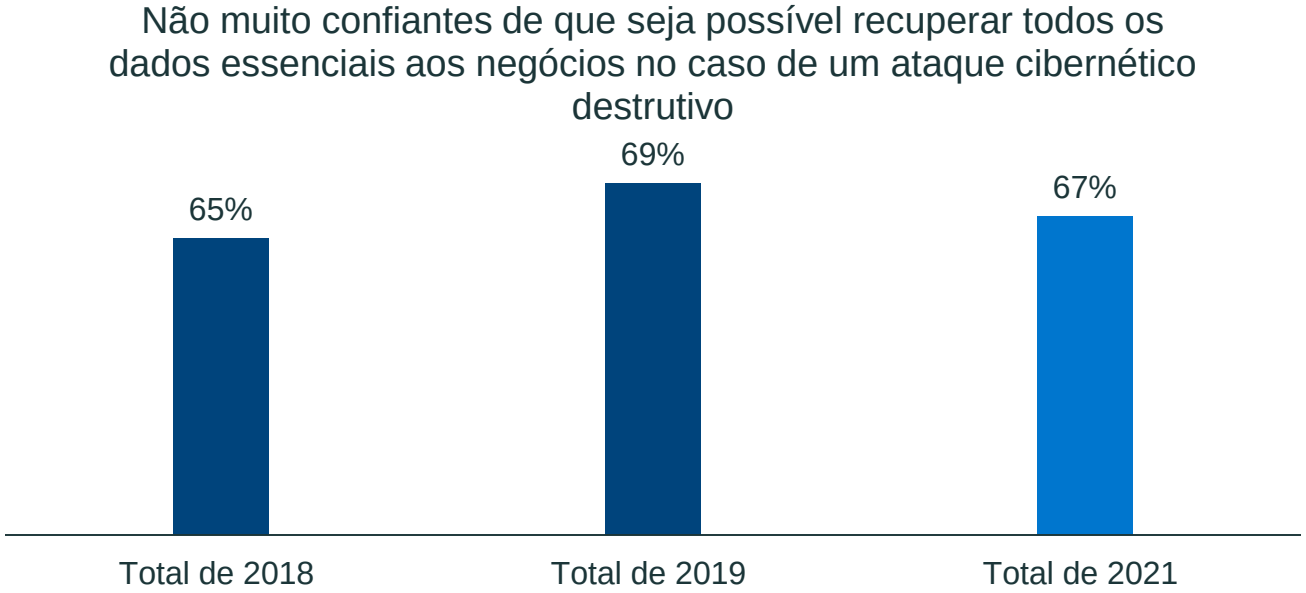
62%

dos entrevistados estão preocupados com as medidas de proteção de dados existentes na organização, **pois talvez não sejam suficientes para lidar com ameaças de malware e ransomware**

74%

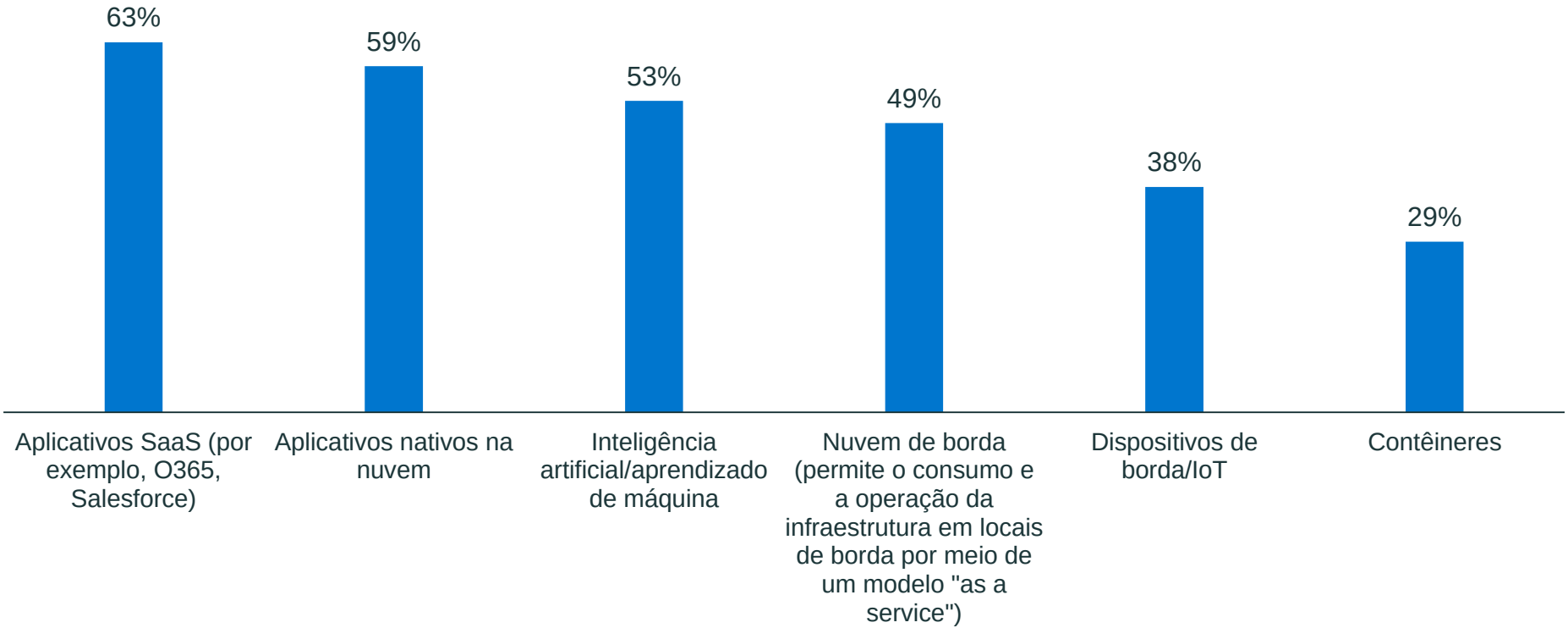
concordam que há **mais exposição à perda de dados** proveniente de ameaças cibernéticas devido ao aumento de **funcionários trabalhando em casa**

Preocupando-se com a capacidade das organizações de lidar com ameaças de malware e ransomware, muitos não têm a confiança de que poderiam recuperar todos os dados essenciais aos negócios em caso de um ataque cibernético destrutivo



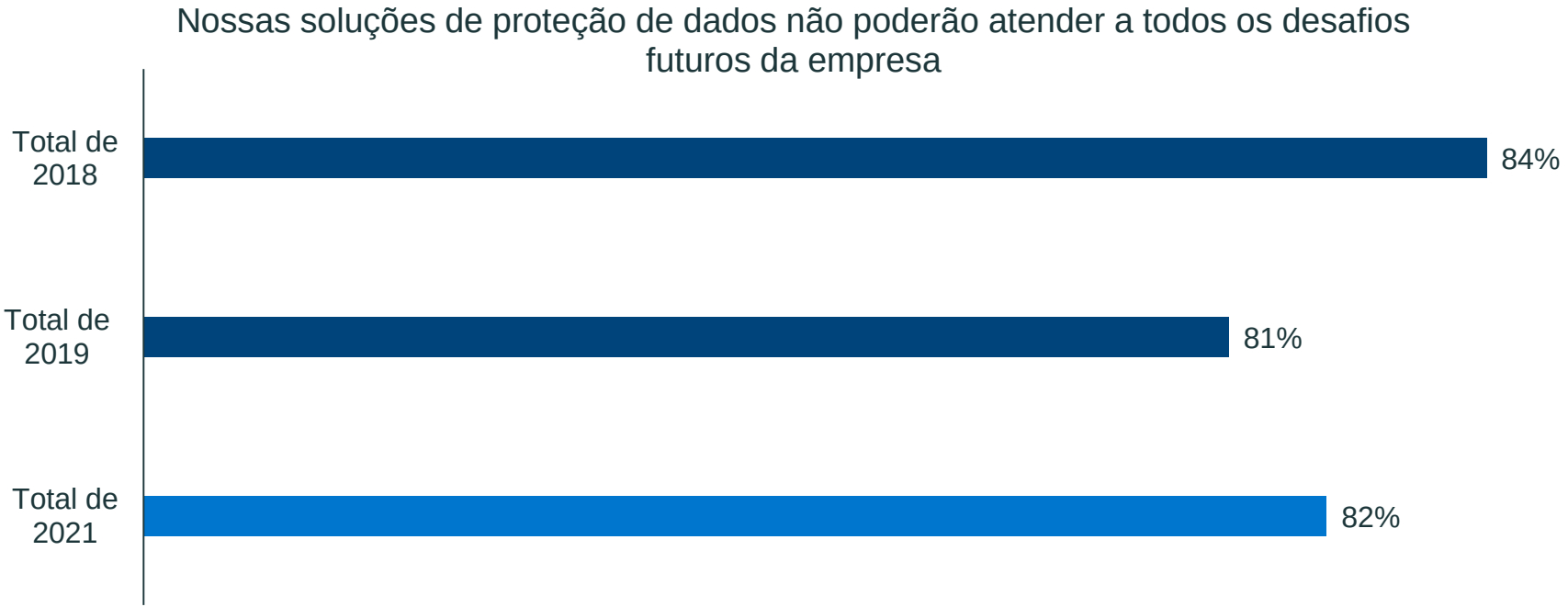
3. Acompanhar o ritmo das tecnologias novas e emergentes

As organizações estão investindo em muitas novas tecnologias, o que pode estar complicando seus desafios de proteção de dados



E ocorre que muitas organizações estão lutando para proteger essas tecnologias

A dificuldade de proteger tecnologias novas e emergentes provavelmente contribui para a baixa confiança de que as soluções de proteção de dados estejam prontas para o futuro



Muitos veem as tecnologias emergentes como um risco de proteção de dados, e a preocupação com eventos disruptivos futuros é alta, especialmente entre aqueles que usam vários fornecedores de proteção de dados

As tecnologias emergentes (como IA, IoT, Borda) representam um risco à proteção de dados

Usam um fornecedor único de proteção de dados

57%

Usam vários fornecedores de proteção de dados

64%

Estou preocupado que enfrentemos um evento disruptivo (por exemplo, perda de dados, tempo de inatividade dos sistemas etc.) nos próximos 12 meses

Usam um fornecedor único de proteção de dados

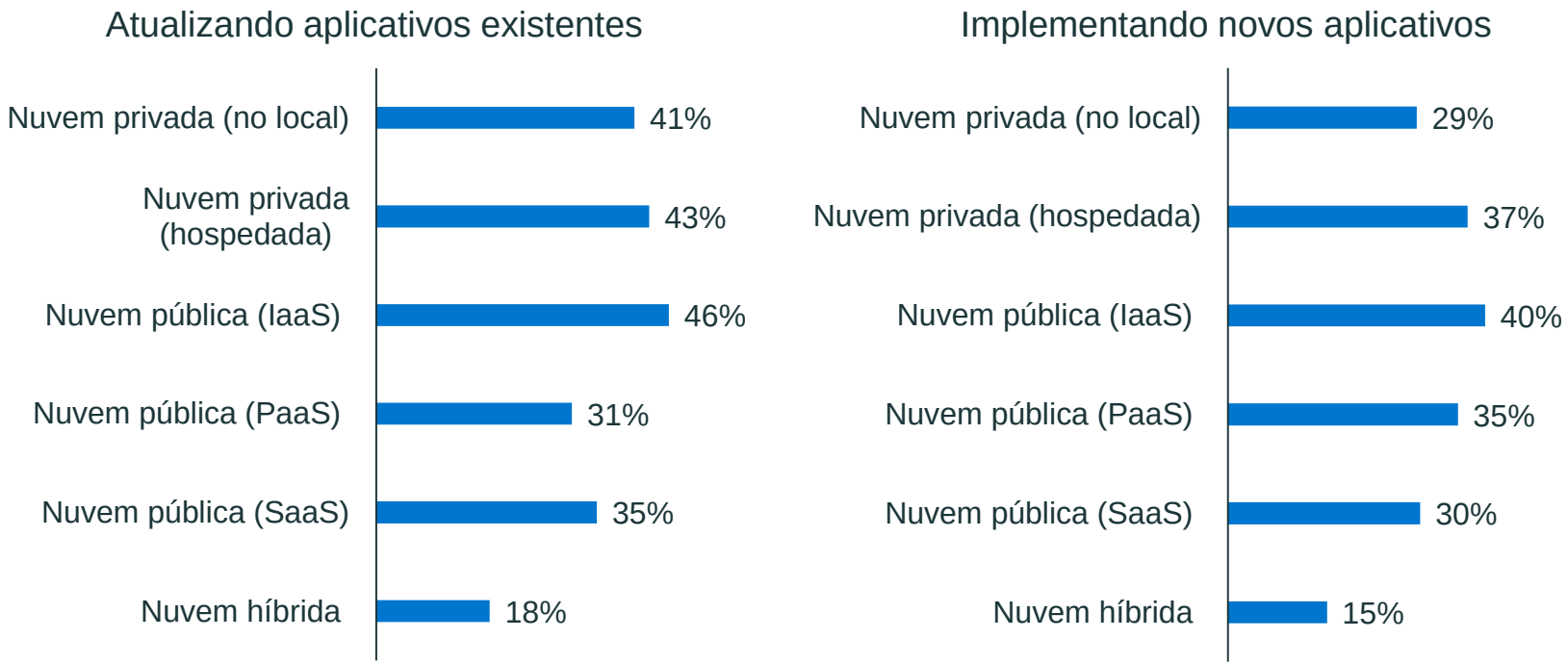
54%

Usam vários fornecedores de proteção de dados

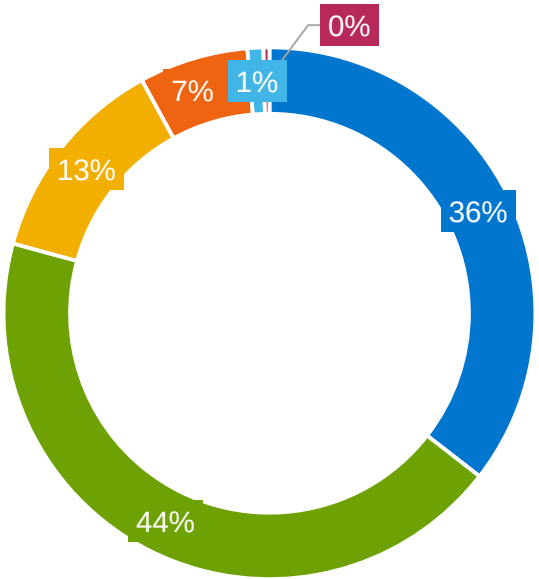
68%

4. Vulnerabilidades da proteção de dados em ambientes de nuvem

Os aplicativos estão sendo atualizados e implementados em uma variedade de ambientes nas infraestruturas de TI das organizações



No entanto, muitos não têm confiança quanto à forma como podem proteger seus dados em ambientes de nuvem pública



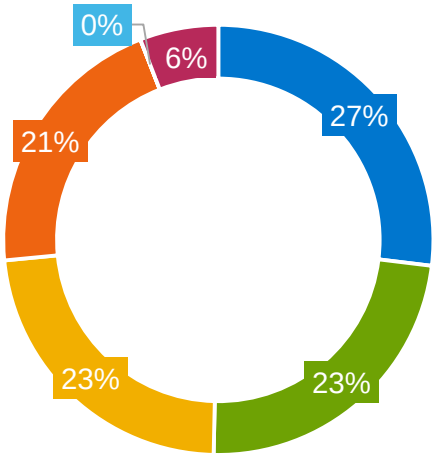
- Muito confiante: protegemos todos os nossos dados na nuvem pública
- Moderadamente confiante: protegemos todos os nossos dados essenciais na nuvem pública, mas não todos os nossos dados totais
- Algumas dúvidas: protegemos a maior parte dos nossos dados essenciais na nuvem pública
- Não muito confiante: protegemos alguns de nossos dados essenciais na nuvem pública
- Nem um pouco confiante: não protegemos nossos dados na nuvem pública
- Não sabem

A nuvem pública tem um papel cada vez maior a desempenhar nas estratégias de recuperação de desastres e retenção em longo prazo das organizações

Inúmeras organizações que usam vários ambientes de nuvem não estão usando soluções específicas para protegê-las

21%

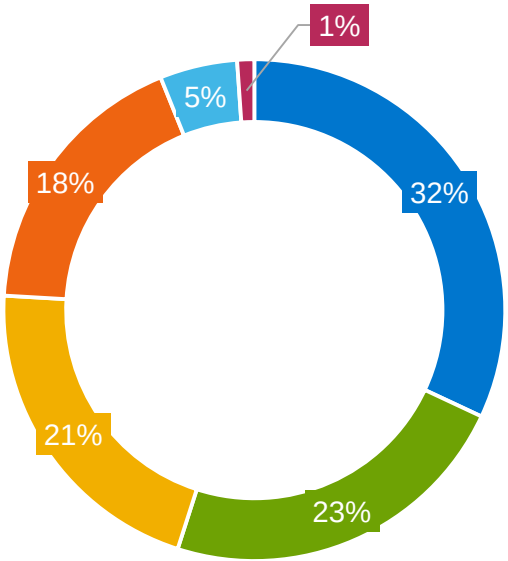
acreditam que, ao usar vários ambientes de nuvem, **cada provedor de serviços em nuvem** é responsável por **proteger suas cargas de trabalho**



- Planejamos atualizar nossa solução de proteção de dados para ativar o backup de cargas de trabalho em várias nuvens
- Nossa solução de backup atual nos permite proteger as cargas de trabalho executadas em várias nuvens
- Usamos várias ferramentas de backup para proteger as cargas de trabalho executadas em várias nuvens
- Cada provedor de serviços em nuvem é responsável por proteger nossas cargas de trabalho
- Outros
- Não estamos executando cargas de trabalho em vários ambientes de nuvem

E o mesmo é verdade quando se considera a proteção de cargas de trabalho virtualizadas usando VMware na nuvem

- Planejamos atualizar nossa solução de proteção de dados para ativar o backup de nuvem híbrida das cargas de trabalho da Vmware
- Nosso provedor de serviços em nuvem é responsável por proteger nossas cargas de trabalho
- Com ferramentas de backup que usamos atualmente e executamos no local
- Com ferramentas de backup disponíveis no mercado de provedores de serviços em nuvem
- Não executamos nem planejamos executar cargas de trabalho na nuvem usando o VMware
- Não sabem

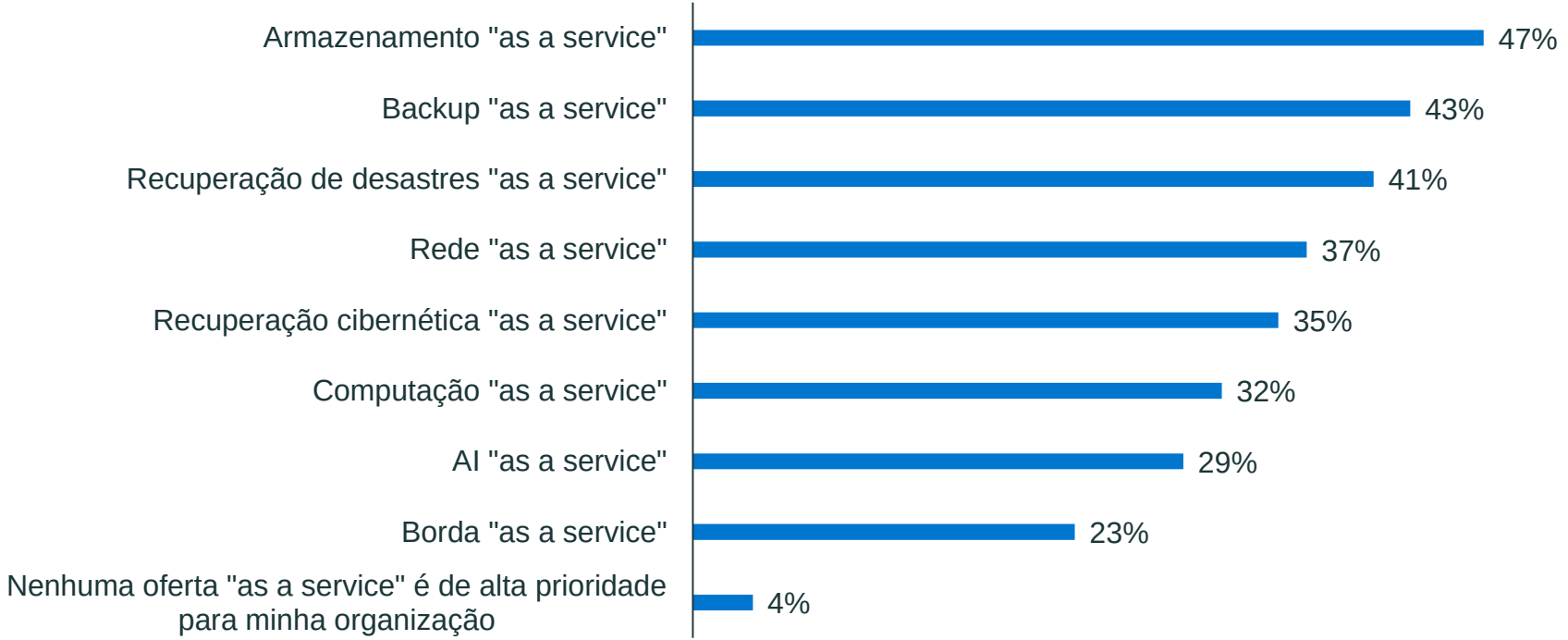


23%

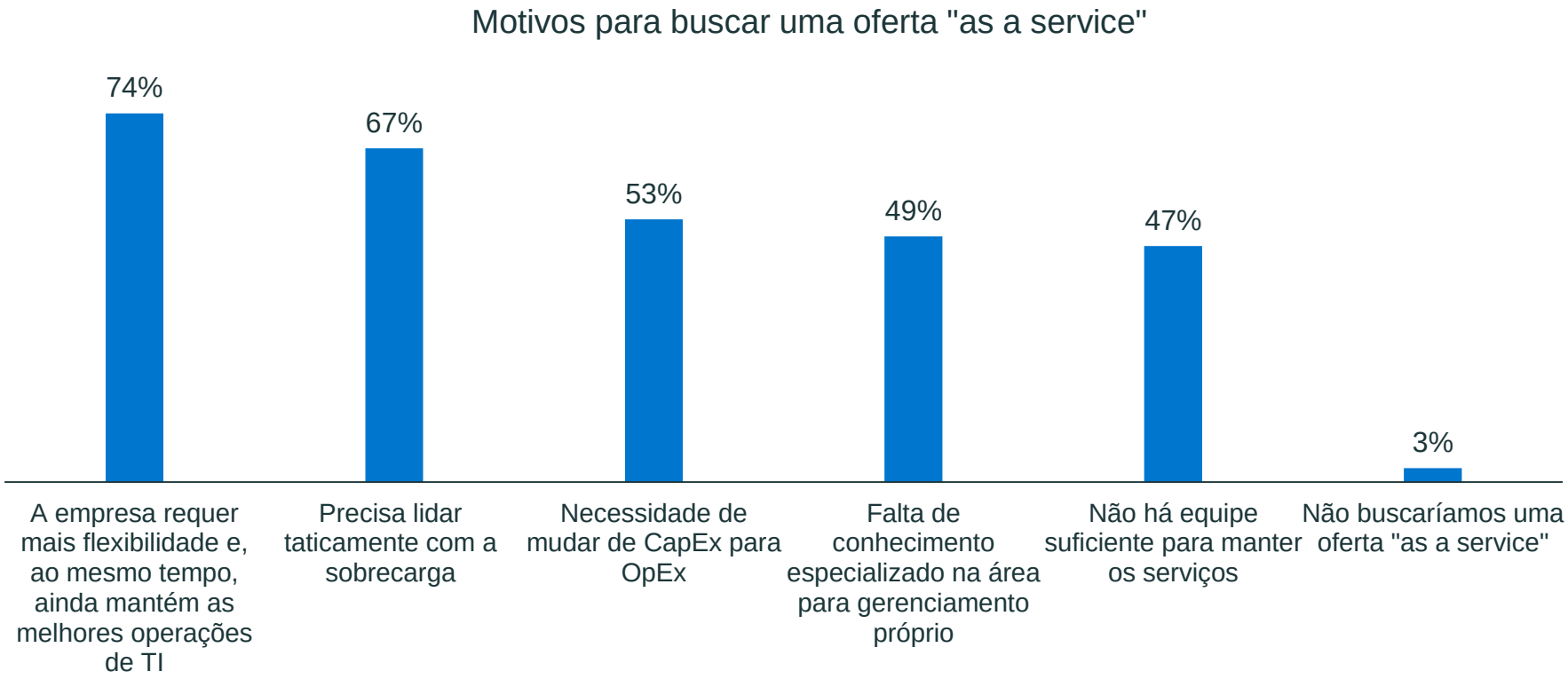
acreditam que o **provedor de serviços em nuvem** é responsável por **proteger as cargas de trabalho virtualizadas**

5.O crescimento do "as a service"

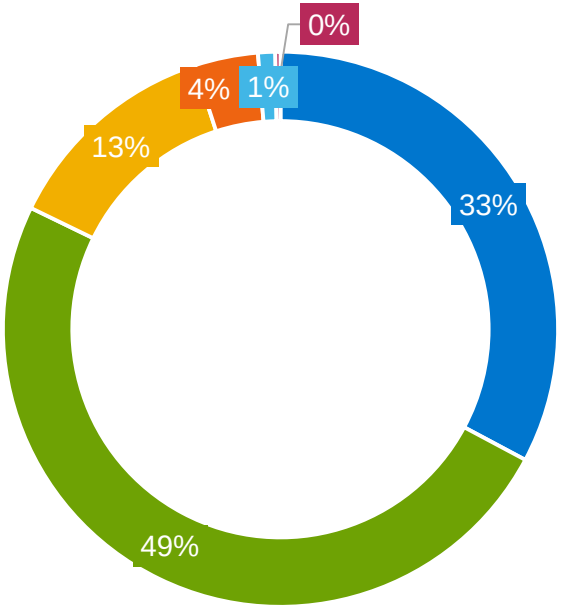
As ofertas de "as a service" estão sendo priorizadas pela maioria das organizações, com Backup "as a service" e Recuperação de desastres "as a service" entre as mais comumente priorizadas



A popularidade das ofertas "as a service" muitas vezes resulta de sua flexibilidade



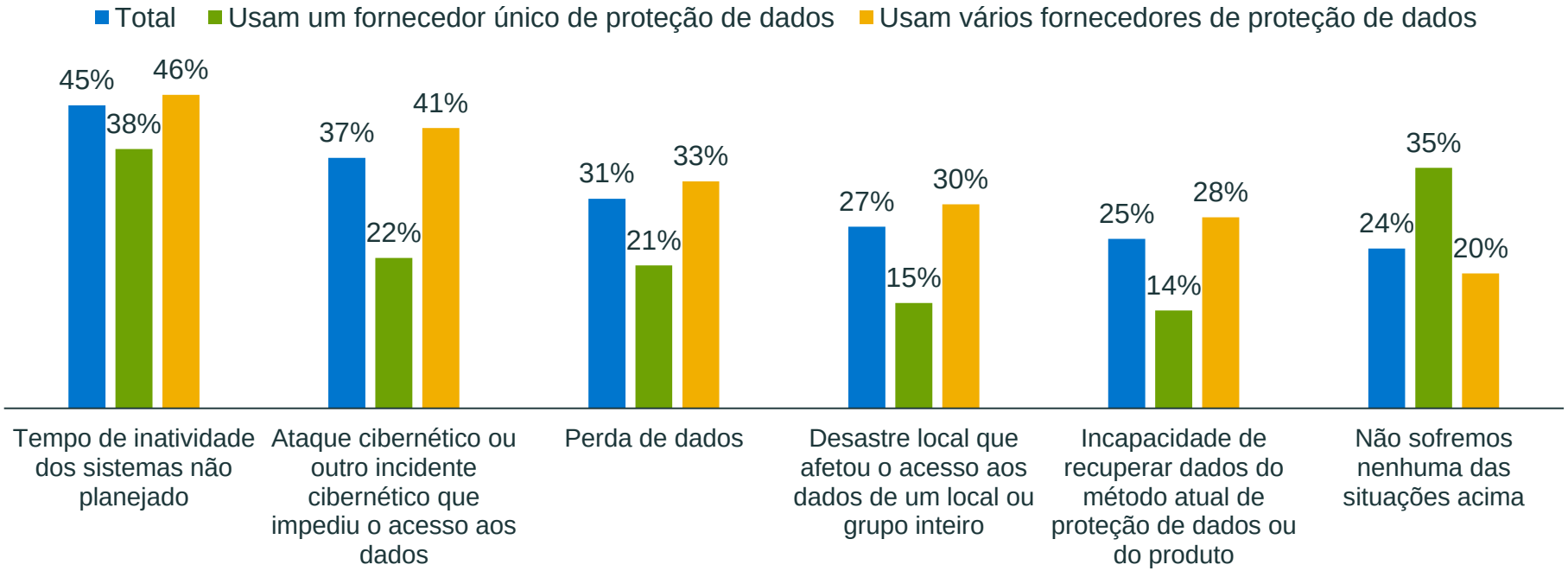
A grande maioria prefere trabalhar com um fornecedor que tem várias ofertas "as a service", sugerindo um desejo de consolidar suas cargas de trabalho com menos fornecedores



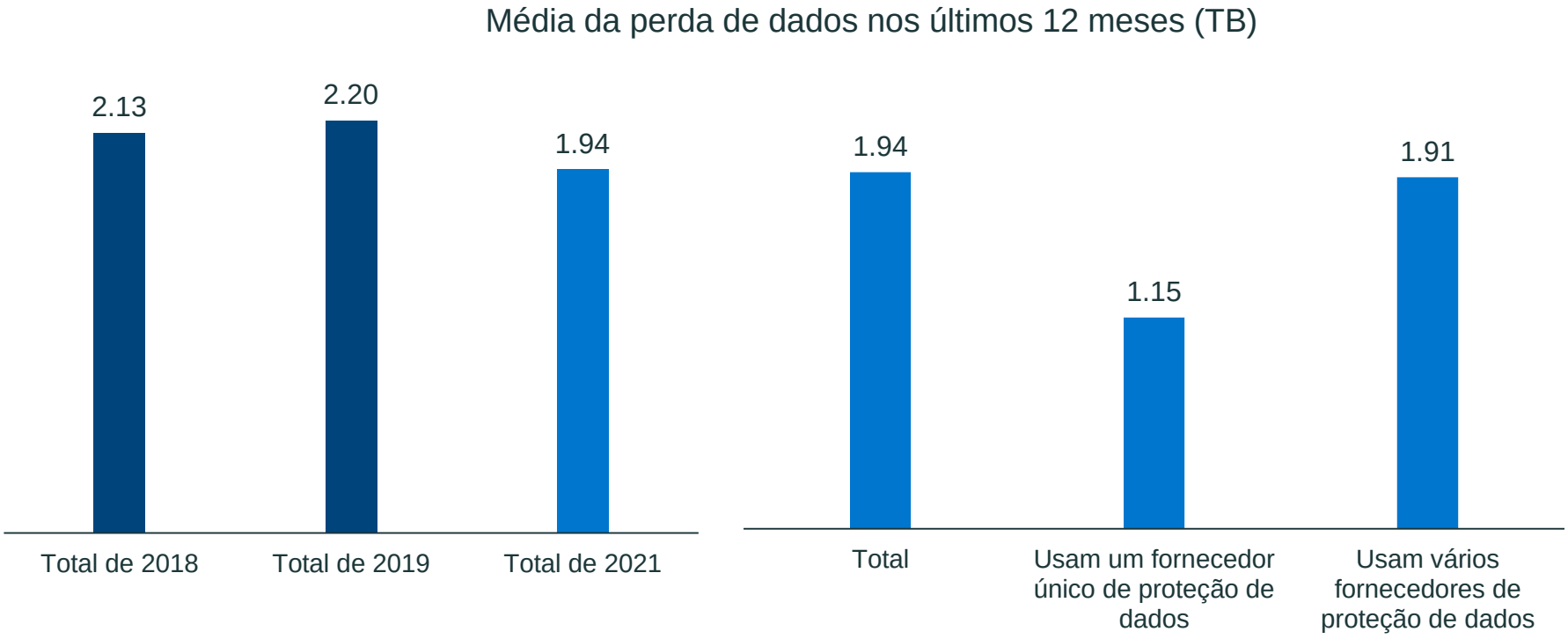
- Estamos muito mais propensos a buscar um fornecedor que tenha várias ofertas "as a service"
- Estamos um pouco mais propensos a buscar um fornecedor que tenha várias ofertas "as a service"
- Somos indiferentes ao fato de um fornecedor ter várias ofertas "as a service"
- Estamos um pouco menos propensos a buscar um fornecedor que tenha várias ofertas "as a service"
- Estamos muito menos propensos a buscar um fornecedor que tenha várias ofertas "as a service"
- Não sabem

6. Simplificação da proteção de dados

As organizações que usam vários fornecedores de proteção de dados têm mais probabilidade de ter sofrido muitos problemas relacionados à perda de dados, ao acesso aos dados ou ao tempo de inatividade dos sistemas no ano passado do que aquelas que usam apenas um único fornecedor



E as organizações que estão usando vários fornecedores de proteção de dados estão perdendo mais dados, em média, do que aquelas que usam um único fornecedor



Principais conclusões — em resumo (1/2)

O ambiente de risco de proteção de dados

- Muitos têm preocupações de que não conseguiriam recuperar todos os sistemas/dados para atender aos SLOs em caso de um incidente de perda de dados
- O medo generalizado é que as organizações sofram um evento disruptivo nos próximos doze meses e os impactos desses eventos disruptivos possam ser financeiramente devastadores
- As organizações devem tomar medidas para garantir que estejam preparadas para responder a esses eventos, caso ocorram

A ameaça representada por ataques cibernéticos

- A preocupação é alta de que as organizações não são capazes de se proteger contra ameaças de malware e ransomware e a maioria concorda que o risco de ataques cibernéticos aumentou com o crescimento do trabalho remoto
- Se as organizações sofrerem ataques, poucas estão confiantes de que conseguiriam recuperar todos os dados essenciais aos negócios

Acompanhar o ritmo das tecnologias novas e emergentes

- As organizações estão investindo em uma variedade de tecnologias novas e emergentes, incluindo aplicativos SaaS, IA/ML e dispositivos de borda/IoT, mas muitas vezes se esforçam para garantir que sua proteção de dados acompanhe o ritmo
- Muitos acreditam que essas tecnologias representam um risco para a proteção de dados e esses riscos provavelmente contribuem para os temores de que as organizações não estejam prontas para o futuro e de que estejam em risco de disrupção nos próximos doze meses
- Os investimentos em tecnologias emergentes são uma coisa boa e devem ser incentivados, mas as organizações devem garantir que sua infraestrutura de proteção de dados ofereça suporte a essas tecnologias

Principais conclusões — em resumo (2/2)

Vulnerabilidades da proteção de dados em ambientes de nuvem

- Os aplicativos estão sendo atualizados e implementados em uma variedade de ambientes de nuvem, mas a confiança geralmente não é suficiente quando se trata de como os dados podem ser protegidos
- A nuvem desempenha um papel importante na recuperação de desastres e nas estratégias de retenção em longo prazo
- As organizações precisam garantir que tenham soluções específicas em vigor para proteger os dados em cargas de trabalho virtualizadas e em várias nuvens, pois algumas organizações ainda acreditam que seus provedores de nuvem são responsáveis por isso

O crescimento do "as a service"

- As soluções "as a service" são de interesse para a maioria das organizações e provavelmente farão parte das soluções de proteção de dados de muitas organizações futuramente — a flexibilidade é muitas vezes um motivo fundamental para esse interesse
- A preferência da maioria seria usar soluções "as a service" de fornecedores com várias ofertas, uma opção que poderia ajudar a simplificar a proteção de dados dessas organizações

Simplificação da proteção de dados

- As organizações que usam um único fornecedor de proteção de dados têm menos probabilidade de ter sofrido perda de dados, problemas de acesso aos dados e incidentes de tempo de inatividade de sistemas não planejados no ano passado do que aquelas que usam vários fornecedores
- Em média, aquelas que usam um único fornecedor também perderam menos dados do que aquelas que usam várias soluções
- Embora as organizações possam se sentir tentadas a expandir seus recursos de proteção de dados investindo em novas soluções, consolidando suas soluções com um único fornecedor, provavelmente estarão mais bem protegidas contra perda de dados e tempo de inatividade

Reduzir o risco e ficar um passo à frente

Ponto de vista da Dell Technologies

Realizar análises regulares de prontidão da proteção de dados

Tornar a resiliência cibernética uma prioridade

Consolidar iniciativas de proteção de dados com a Dell

Acesse DellTechnologies.com/GDPI para saber mais


DELL Technologies