

# O ambiente de riscos da proteção de dados

---



**Em meio à transformação digital e aos eventos mundiais recentes, nunca foi tão importante ter uma sólida estratégia de proteção de dados. As organizações de todos os setores compartilham a preocupação de que suas estratégias de proteção de dados talvez não consigam lidar com a ampla variedade de desafios que elas enfrentam, à medida que avançam para a década dos dados.**

**A nova economia do trabalho remoto, a proliferação de ameaças cibernéticas, a adoção contínua de novas tecnologias e a onnipresença da infraestrutura híbrida e com várias nuvens exigem uma abordagem holística de proteção de dados – para simplificar a TI e garantir a proteção confiável e a rápida capacidade de recuperação de ativos de dados essenciais.**

Este eBook apresenta as descobertas do estudo Global Data Protection de 2021 da Vanson Bourne, uma pesquisa feita com mil responsáveis pelas decisões de TI (ITDMs) do mundo todo

**4** O ambiente de riscos

**5** A crescente ameaça de ataques cibernéticos

**6** Acompanhando o ritmo das tecnologias novas e emergentes

**7** Vulnerabilidades da proteção de dados em ambientes de nuvem

**9** O crescimento do "as a service"

**10** Simplificação da proteção de dados

**11** Resumo

# O ambiente de riscos

Sessenta e quatro por cento das organizações temem sofrer um evento disruptivo nos próximos 12 meses.

Além disso, 65% dos tomadores de decisões não estão confiantes de que sua organização conseguirá recuperar todos os sistemas/dados para atender aos SLOs após um incidente de perda de dados.

Além desse motivo de preocupação, os problemas de perda de dados e de tempo de inatividade dos sistemas continuam causando um impacto financeiro significativo sobre as organizações.

**US\$ 959.493,00**

Custo médio da perda de dados nos últimos 12 meses

**US\$ 513.067,00**

Custo médio do tempo de inatividade não planejado dos sistemas nos últimos 12 meses

Conteúdo

4

5

6

7

9

10

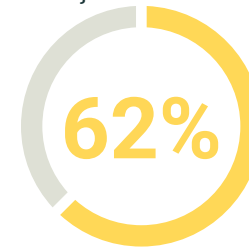
11

# As crescentes ameaças de ataques cibernéticos

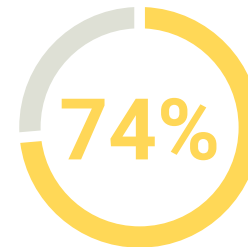
Para um número cada vez maior de organizações, a probabilidade de ataques cibernéticos subiu para o topo da lista como o maior risco que ameaça os negócios. As preocupações são alimentadas, em parte, por um rápido aumento das práticas de trabalho remoto, uma vez que o trabalho em casa ampliou significativamente o vetor de superfície para possíveis ataques.

A ameaça atual de ataques cibernéticos e a importância de manter a confidencialidade, a disponibilidade e a integridade dos dados requerem soluções e estratégias modernas para proteger dados e sistemas vitais.

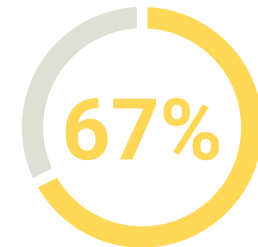
Mas muitos não confiam que a proteção de dados de sua organização possa oferecer capacidade de proteção suficiente e recuperação de ameaças cibernéticas.



temem que as medidas existentes de proteção de dados talvez não sejam suficientes para lidar com ameaças de malware e ransomware



concordam que há mais exposição à perda de dados causada por ameaças cibernéticas, devido ao maior número de funcionários trabalhando em casa



não estão muito confiantes de que seja possível recuperar todos os dados essenciais em caso de um ataque cibernético destrutivo

Garantir a possibilidade de rápida recuperação de seus dados e sistemas mais essenciais após um ataque cibernético ou outro evento disruptivo é uma etapa fundamental na retomada das operações normais de negócios.

As soluções e os serviços Dell EMC PowerProtect Cyber Recovery oferecem os mais altos níveis de proteção, integridade e confidencialidade para seus dados mais valiosos e seus sistemas de negócios essenciais.

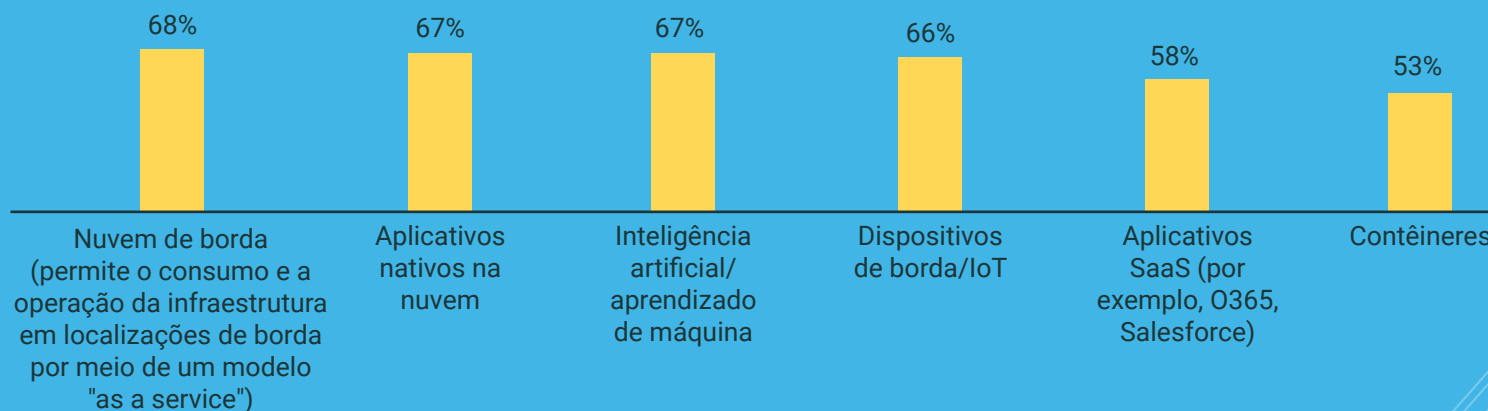
[Faça a avaliação de resiliência cibernética da Dell Technologies.](#)

# Acompanhando o ritmo das tecnologias novas e emergentes

O surgimento de novas cargas de trabalho e tecnologias emergentes pode resultar em maior complexidade da TI e em menos confiança geral, caso a proteção de dados não acompanhe o ritmo de tudo isso.

As organizações estão investindo em muitas tecnologias novas, o que pode complicar seus desafios de proteção de dados, e muitas delas têm dificuldades para proteger essas tecnologias.

**"Para quais tecnologias mais novas/emergentes, em particular, sua organização tem dificuldades para encontrar soluções de proteção de dados?"**



No momento, as preocupações com os riscos apresentados pelas novas tecnologias provavelmente estejam contribuindo para o temor dos tomadores de decisões de que sua organização sofra um evento disruptivo nos próximos 12 meses. Ao mesmo tempo, 82% dos participantes da pesquisa acreditam que suas tecnologias atuais de proteção de dados não conseguirão enfrentar todos os futuros desafios da empresa.

As organizações precisam de soluções inovadoras de proteção de dados para proteger as cargas de trabalho tradicionais (como Oracle, SQL, SAP, Exchange e serviços de arquivos de NAS) e modernas, como contêineres do Kubernetes, os aplicativos nativos na nuvem (como Mongo DB) e os aplicativos de SaaS, como Microsoft Office 365, Salesforce e Google Workspace.

**Saiba mais sobre as soluções modernas e comprovadas de proteção de dados em nuvem da Dell Technologies.**

# Vulnerabilidades da proteção de dados em ambientes de nuvem

Conteúdo

4

5

6

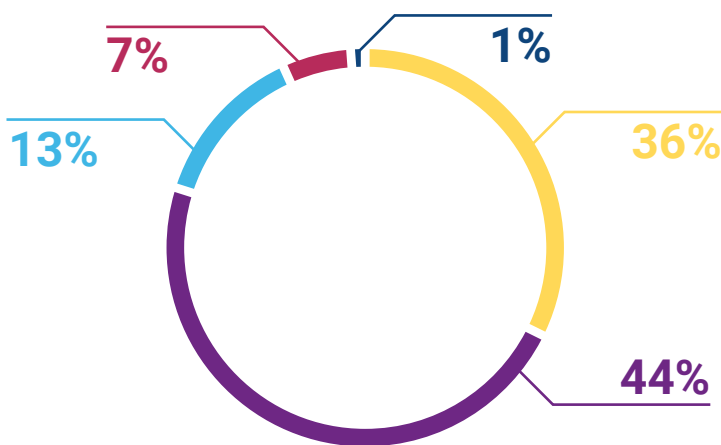
7

9

10

11

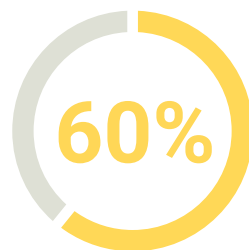
Muitas organizações utilizam a infraestrutura híbrida e com várias nuvens para implementar cargas de trabalho de aplicativos; no entanto, apenas 36% declararam estar muito confiantes em seus recursos de proteção de dados em nuvem. Por outro lado, um quinto dos entrevistados indicou ter algumas dúvidas ou afirmou não estar muito confiante ou não estar nem um pouco confiante em sua capacidade de proteger os dados na nuvem pública.



- Muito confiantes – protegemos todos os nossos dados na nuvem pública
- Moderadamente confiantes – protegemos todos os nossos dados essenciais na nuvem pública, mas não o total de nossos dados
- Algumas dúvidas – protegemos a maior parte de nossos dados essenciais na nuvem pública
- Não muito confiantes – protegemos alguns de nossos dados essenciais na nuvem pública
- Nem um pouco confiantes – não protegemos dados na nuvem pública



usam a nuvem pública para recuperação de desastres atualmente



usam a nuvem pública para retenção em longo prazo atualmente

E, como a maioria das organizações usa a nuvem pública para importantes iniciativas de negócios, como recuperação de desastres (DR) e arquivamento de longo prazo, essa falta de confiança na proteção de dados pode indicar um ponto de vulnerabilidade na prontidão para DR e na viabilidade dos repositórios de dados de longo prazo dessas organizações.

Conteúdo

- 4
- 5
- 6
- 7
- 9
- 10
- 11

Muitas organizações executam cargas de trabalho em vários ambientes de nuvem ou executam cargas de trabalho virtualizadas usando o VMware na nuvem.

Cerca de uma em cada quatro acredita que os provedores de serviços em nuvem são responsáveis por proteger essas cargas de trabalho — mas será que isso é verdade? Sem saber, ao fazer essa suposição, muitas organizações podem estar se expondo a riscos.

De aplicativos físicos e virtualizados a contêineres, aplicativos nativos na nuvem e SaaS, as soluções de proteção de dados da Dell Technologies proporcionam às organizações a flexibilidade para proteger as cargas de trabalho essenciais onde quer que elas estejam, seja em ambientes híbridos, de borda ou com várias nuvens. Ao mesmo tempo, elas facilitam para as organizações a movimentação e a migração de dados a fim de aprimorar a prontidão para DR, garantir a conformidade, aumentar a segurança e reduzir os custos.



**Cada provedor de serviços em nuvem é responsável por proteger nossas cargas de trabalho em vários ambientes de nuvem**



**Nosso provedor de serviços em nuvem é responsável por proteger nossas cargas de trabalho virtualizadas**



# O crescimento do "as a service"

As ofertas "as a service" continuam atraindo o interesse de muitas organizações e apresentam uma nova oportunidade de simplificar ainda mais a implementação e o consumo da proteção de dados.

Os serviços de Armazenamento as a Service, Backup as a Service e Recuperação de desastres as a Service estão entre as ofertas de soluções "as a service" mais priorizadas.

Armazenamento "as a service" 47%

Backup "as a service" 43%

Recuperação de desastres "as a service" 41%

Sistema de rede "as a service" 37%

Cyber Recovery "as a service" 35%

Computação "as a service" 32%

IA "as a service" 29%

Borda "as a service" 23%

Nenhuma oferta "as a service" é uma alta prioridade para minha organização 4%

# 82%

das organizações são mais propensas a contratar um fornecedor que tenha várias ofertas "as a service"

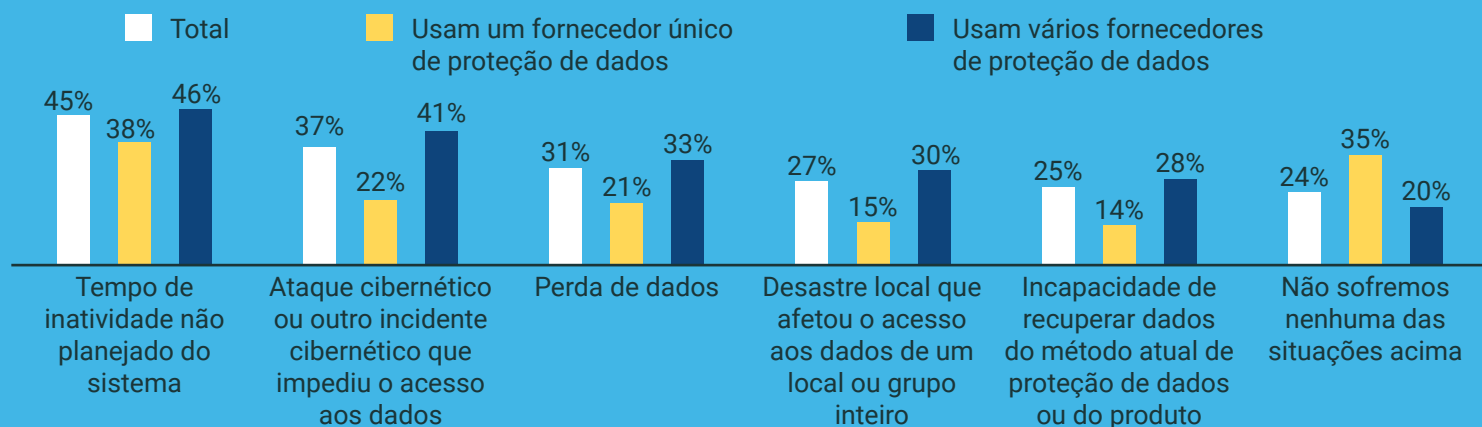
A grande maioria prefere trabalhar com um fornecedor que tenha várias ofertas "as a service", o que sugere um desejo de consolidar as cargas de trabalho com menos fornecedores a fim de simplificar as operações.

**APEX** combina a facilidade e a agilidade dos modelos operacionais "as a service" com o poder e o controle da infraestrutura líder da Dell Technologies, permitindo que as organizações entreguem recursos "as a service" onde eles forem necessários, do data center às localizações de borda ou uma instalação de colocação.

O APEX oferece soluções completas de infraestrutura de TI para atender a vários requisitos de dados e carga de trabalho, permitindo que as organizações acelerem a inovação, adaptem-se aos requisitos em evolução e permaneçam no controle das operações de TI.

# Simplificação da proteção de dados

Simplificar a proteção de dados reduzindo o número de fornecedores que oferecem soluções pode resultar em menos incidentes com menos impactos sobre os negócios. Essa abordagem única também pode simplificar a proteção de dados em ambientes híbridos, de borda e com várias nuvens, oferecendo mais flexibilidade e opções para garantir a solução certa para atender os requisitos exclusivos de uma organização.



Ao utilizar o portfólio de soluções modernas e comprovadas de proteção de dados em nuvem da Dell Technologies, as organizações podem simplificar a TI, reduzir riscos, diminuir os custos e aprimorar a proteção e a segurança de seus ativos de dados e cargas de trabalho essenciais. Essas soluções oferecem suporte a cargas de trabalho físicas e virtualizadas, além de contêineres do Kubernetes, aplicativos nativos na nuvem e SaaS, para proporcionar às organizações resiliência cibernética e proteção completa de dados nos ambientes híbridos, de borda e com várias nuvens – tudo isso proveniente de um só provedor de soluções de proteção de dados.

# Resumo

Na atual economia sob demanda, nada acontece sem dados. Remova o acesso a eles, e as ondas de progresso cessarão. No entanto, a maioria das organizações admite abertamente não estar confiante em sua proteção de dados e na prontidão de sua capacidade de recuperação. Os departamentos de TI precisam de soluções abrangentes de proteção de dados que atendam a um amplo conjunto de requisitos, que variam de resiliência cibernética e proteção de cargas de trabalho modernas a opções flexíveis para proteger aplicativos e dados em localizações híbridas, de borda e com várias nuvens. Também é importante que essas soluções sejam simples, confiáveis, eficientes, escaláveis e mais automatizadas, permitindo que os departamentos de TI gastem menos tempo em operações de proteção de dados e mais tempo se concentrando em iniciativas estratégicas.

**O amplo portfólio da Dell Technologies de soluções modernas e comprovadas de proteção de dados e resiliência cibernética entrega proteção e recuperação simplificadas, eficientes e confiáveis de aplicativos e dados, onde quer que elas sejam implementadas.**

Como líder em software de proteção de dados e equipamentos integrados de proteção de dados, a Dell Technologies tem o compromisso de entregar soluções completas e inovadoras de proteção de dados que ajudem as organizações a ter confiança na segurança ininterrupta de seus dados essenciais. Assim, elas poderão se concentrar menos no gerenciamento da infraestrutura de proteção de dados e mais na administração dos negócios.

# Reduzir o risco e ficar um passo à frente

Conteúdo

4

5

6

7

9

10

11



**Realizar análises regulares de prontidão da proteção de dados**



**Tornar a resiliência cibernética uma prioridade**



**Consolidar iniciativas de proteção de dados com a Dell**

Para saber mais, acesse: [DellTechnologies.com/pt-br/data-protection/index.htm](https://DellTechnologies.com/pt-br/data-protection/index.htm)





A Dell Technologies ajuda organizações e indivíduos a construir o próprio futuro digital, além de transformar a maneira como trabalham, vivem e se divertem. A empresa oferece aos clientes o mais amplo e inovador portfólio de tecnologias e serviços do setor para a era dos dados.



A Vanson Bourne é uma empresa independente especializada em pesquisa de mercado para o setor de tecnologia. Sua reputação em análises sólidas e confiáveis com base em pesquisas é fundada sobre rigorosos princípios de pesquisa e a capacidade de pedir opiniões de importantes tomadores de decisões de funções técnicas e de negócios, em todos os setores de negócios e em todos os principais mercados. Para obter mais informações, visite [www.vansonbourne.com](http://www.vansonbourne.com).

