Global Data Protection Index – Edição especial de 2024

Principais resultados – outubro de 2023

VansonBourne

DELL Technologies

Foco das principais conclusões

1
O ambiente de risco de proteção de dados

2
A crescente ameaça de ataques cibernéticos

3
O uso de multicloud

4
Protegendo um ambiente de nuvem

Copyright © Dell Inc. All Rights Reserved.

Cinco principais conclusões

Os ataques cibernéticos continuam a crescer

O custo dos ataques cibernéticos está aumentando

As políticas de seguro não cobrem o suficiente do custo dos ataques

O aumento do uso da IA generativa pode levar a mais dados de alto valor

Levando a maiores riscos e mais impactos financeiros de ataques cibernéticos

Copyright © Dell Inc. All Rights Reserved.

Quem entrevistamos?

1.500 responsáveis pelas decisões de TI e de segurança de TI foram entrevistados em setembro e outubro de 2023

Organizações de uma ampla variedade de setores públicos e privados

Organizações com mais de 250 funcionários

4 regiões:

Américas (300)
EMEA (675)
APJ (375)
China (150)

Copyright © Dell Inc. All Rights Reserved.

1. O ambiente de risco de proteção de dados

Copyright © Dell Inc. All Rights Reserved.

As preocupações com as medidas de proteção de dados são generalizadas e, com a falta de confiança, as organizações se encontram em uma posição vulnerável

60%

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

79%

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

75%

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**

65%

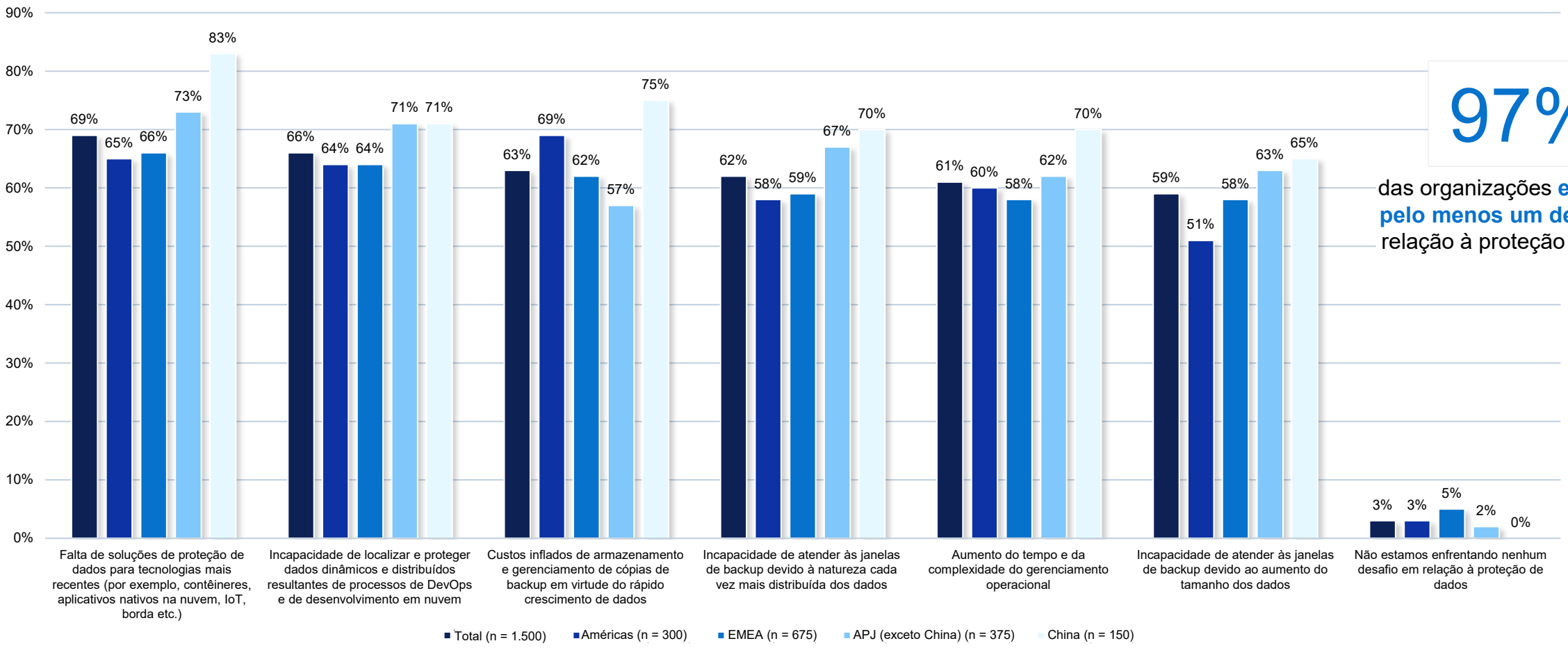
não **estão muito confiantes** de que sua organização pode **recuperar totalmente os sistemas/dados de todas as plataformas** em caso de incidente de perda de dados

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

Além das preocupações com a proteção de dados, muitas organizações enfrentam desafios

As cinco principais classificações: desafios enfrentados em relação à proteção de dados, divididos por região



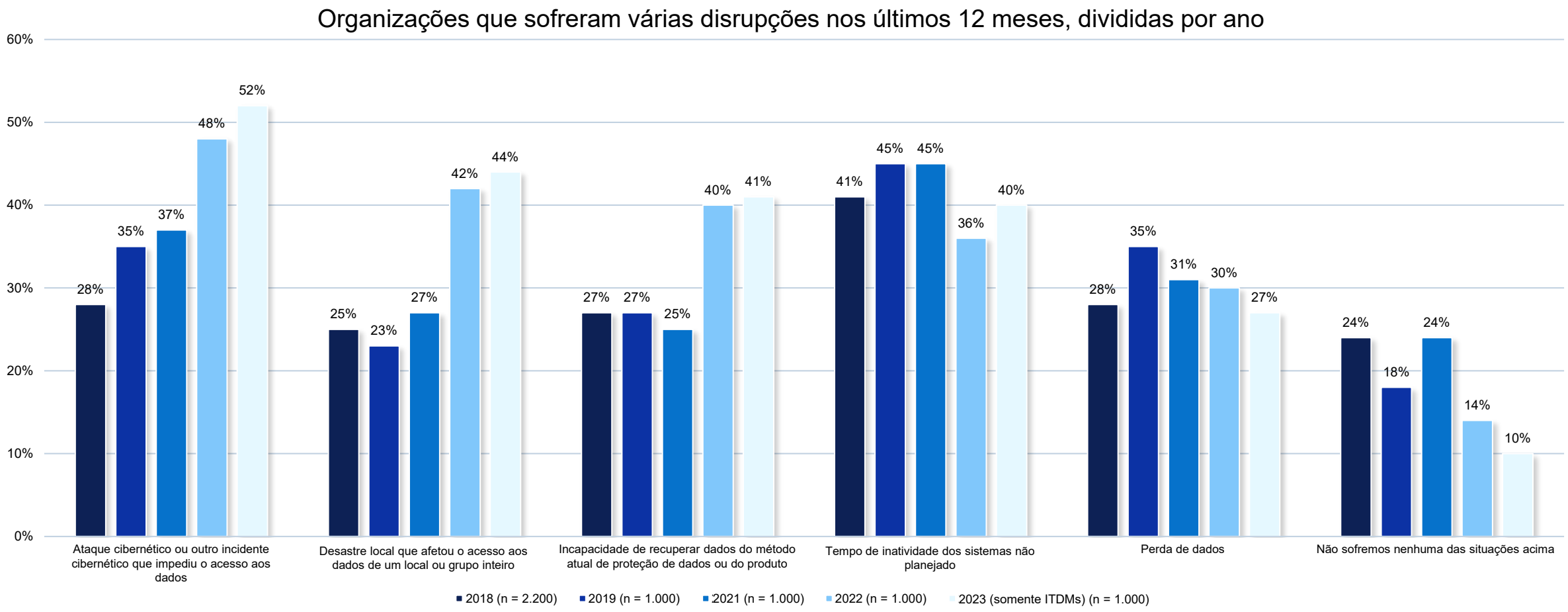
97%

das organizações **enfrentam pelo menos um desafio** em relação à proteção de dados

DELL Technologies

Copyright © Dell Inc. All Rights Reserved.

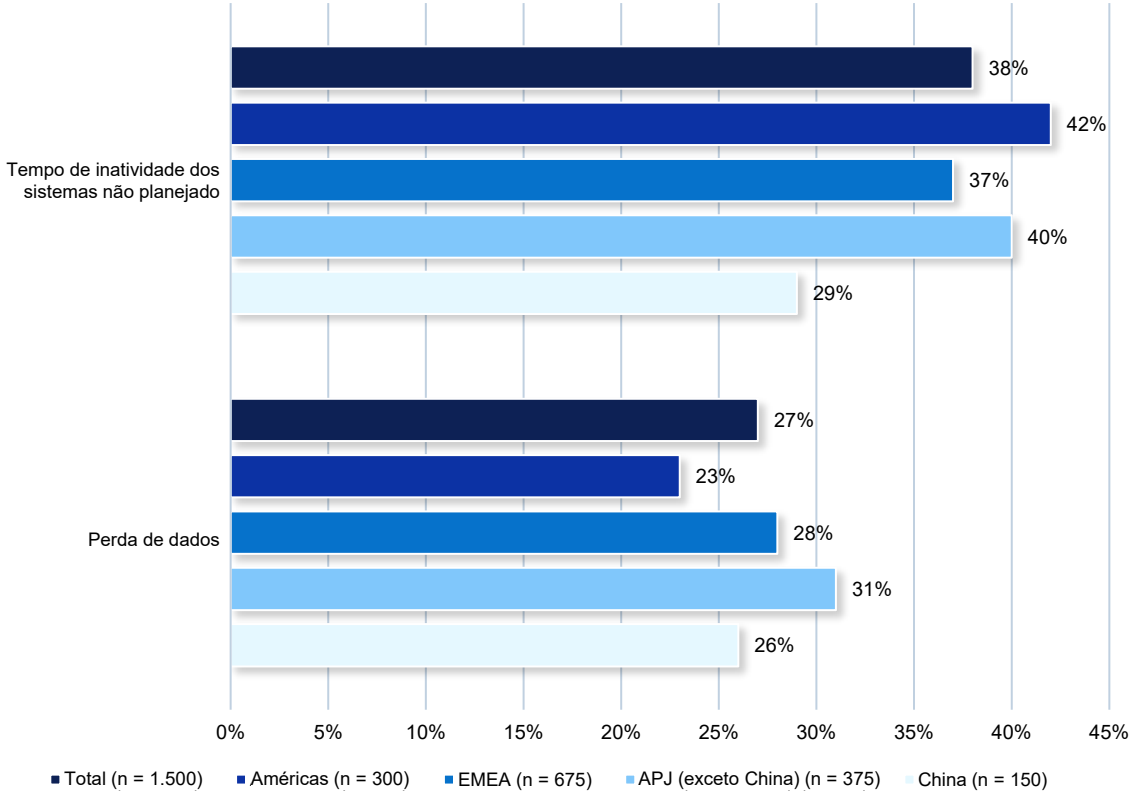
Nos últimos 12 meses, as organizações enfrentaram disrupções significativas, com ataques cibernéticos representando uma ameaça cada vez maior



Copyright © Dell Inc. All Rights Reserved.

A perda de dados não só contribuiu para a disrupção, mas também impactou os resultados

Porcentagem de organizações que enfrentaram tempo de inatividade não planejado dos sistemas ou perda de dados nos últimos 12 meses, divididas por região



Nos últimos 12 meses:

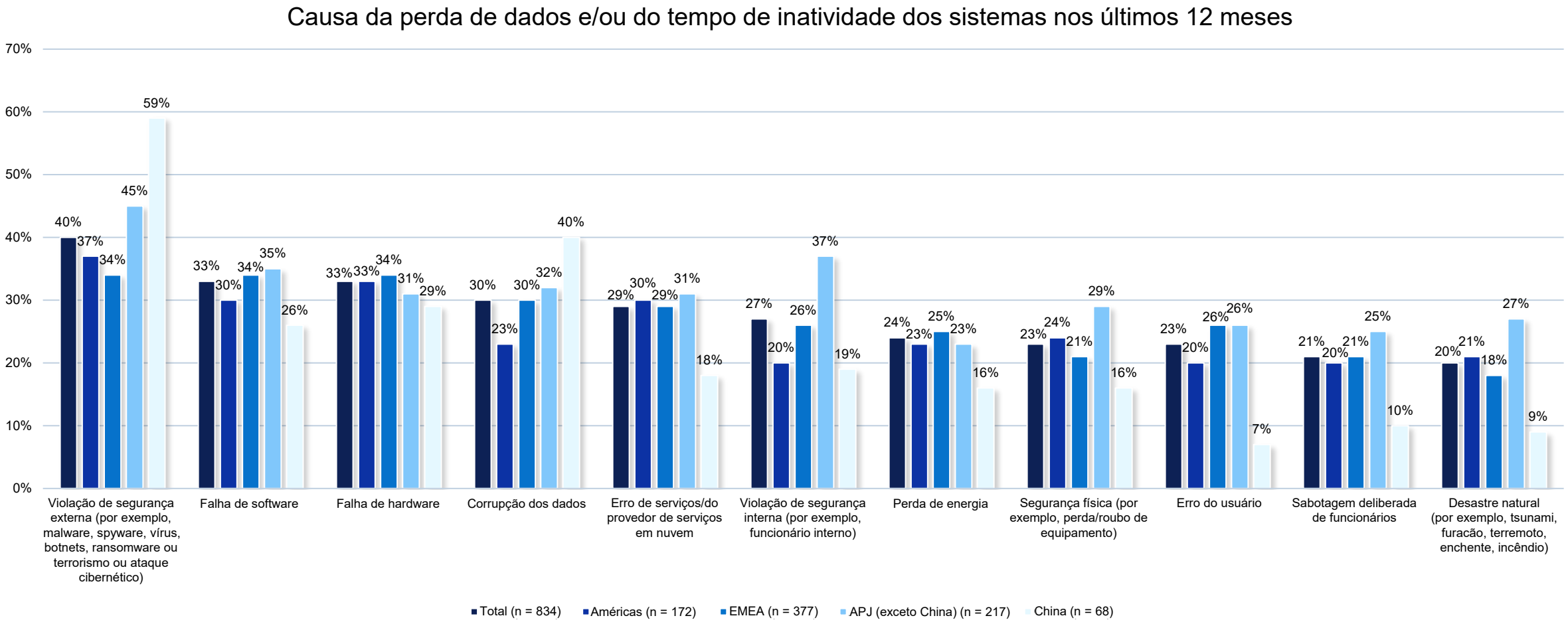
26 horas **de tempo de inatividade não planejado dos sistemas**, vivenciado em média

2,45 TB **valor dos dados** perdidos, em média

US$ 2,61 milhões, a média **do custo da perda de dados**

Copyright © Dell Inc. All Rights Reserved.

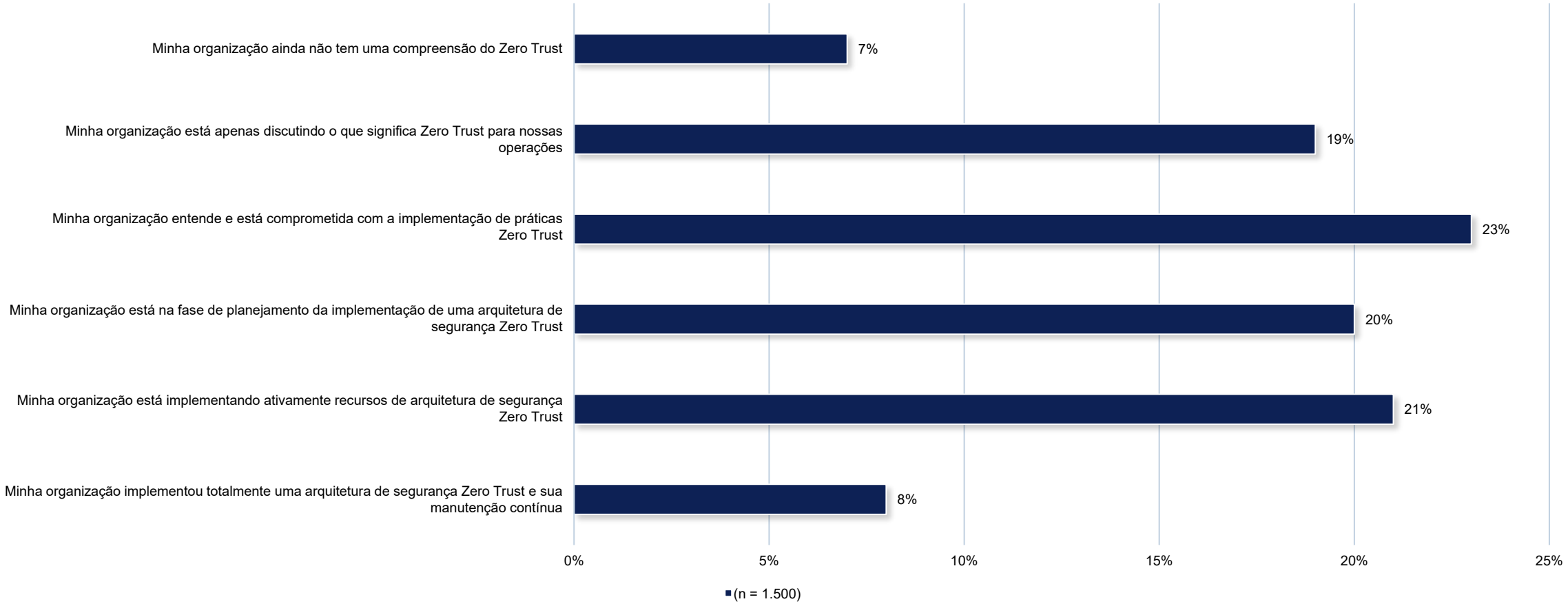
As ameaças de segurança externas são as causas mais comuns de perda de dados e/ou tempo de inatividade não planejado dos sistemas nos últimos 12 meses



Copyright © Dell Inc. All Rights Reserved.

Apesar dos desafios e das preocupações com a proteção de dados, poucos implementaram totalmente a segurança Zero Trust

Jornada das organizações para implementar a segurança Zero Trust



Filtro: divisão de dados: região = total

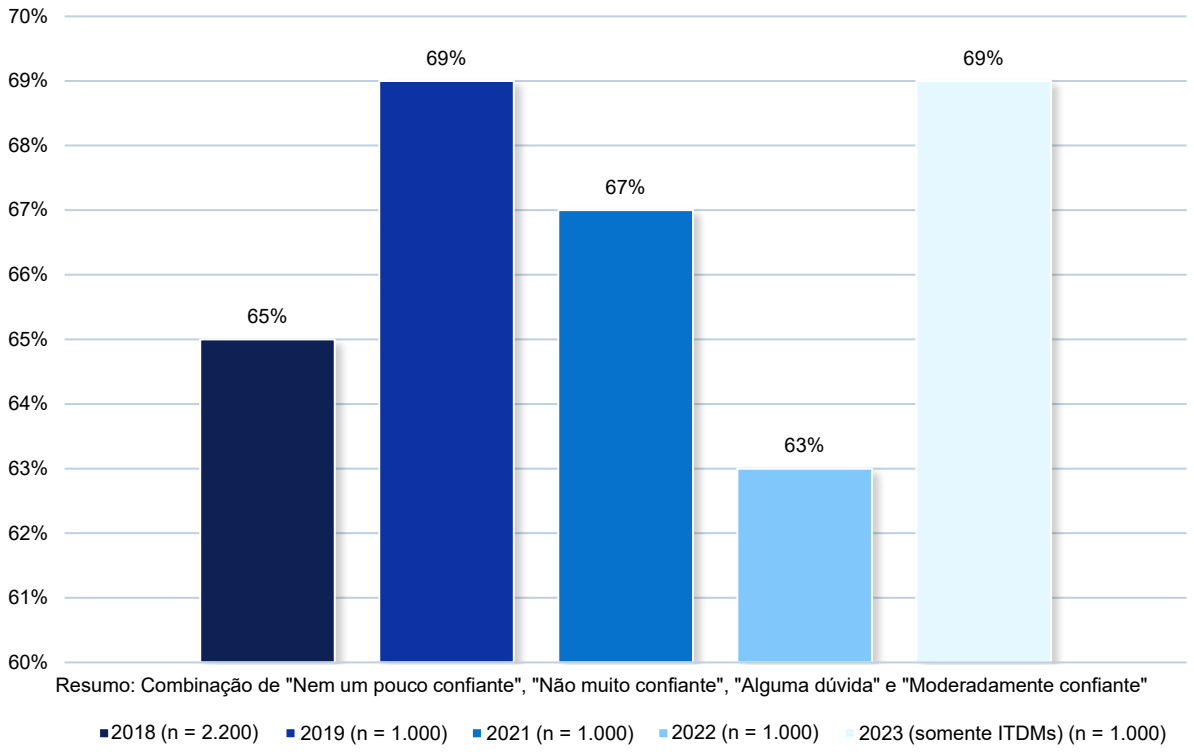
Copyright © Dell Inc. All Rights Reserved.

2. A crescente ameaça de ataques cibernéticos

Copyright © Dell Inc. All Rights Reserved.

As preocupações com as medidas de proteção de dados são generalizadas e, com a falta de confiança, as organizações se encontram em uma posição vulnerável

Não estão “muito confiantes” de que seja possível recuperar todos os dados essenciais de negócios diante de um ataque cibernético destrutivo, divididos por ano



81%

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

74%

estão **preocupados** que seus dados de backup possam ser **infectados ou corrompidos por ataques de ransomware**

Copyright © Dell Inc. All Rights Reserved.

Além do risco, há um excesso de confiança equivocado em relação às consequências de um ataque de ransomware

72%

concordam que seu trabalho e os funcionários dentro de sua organização **não serão afetados por um ataque de ransomware**

74%

concordam que, se a organização sofrer um ataque de ransomware, **receberá todos os dados de volta** para retomar os negócios **se pagar o resgate**

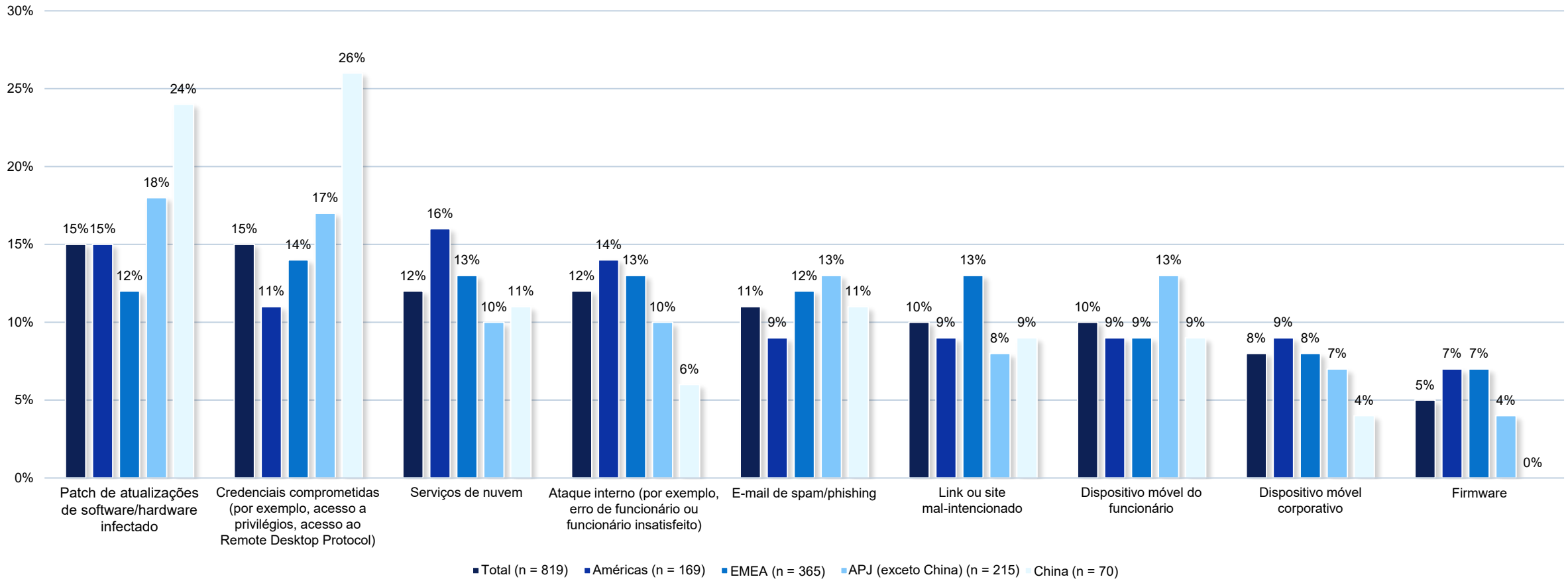
66%

concordam que, se a organização sofrer um ataque de ransomware, depois de pagar o resgate, **não será atacada novamente**

Copyright © Dell Inc. All Rights Reserved.

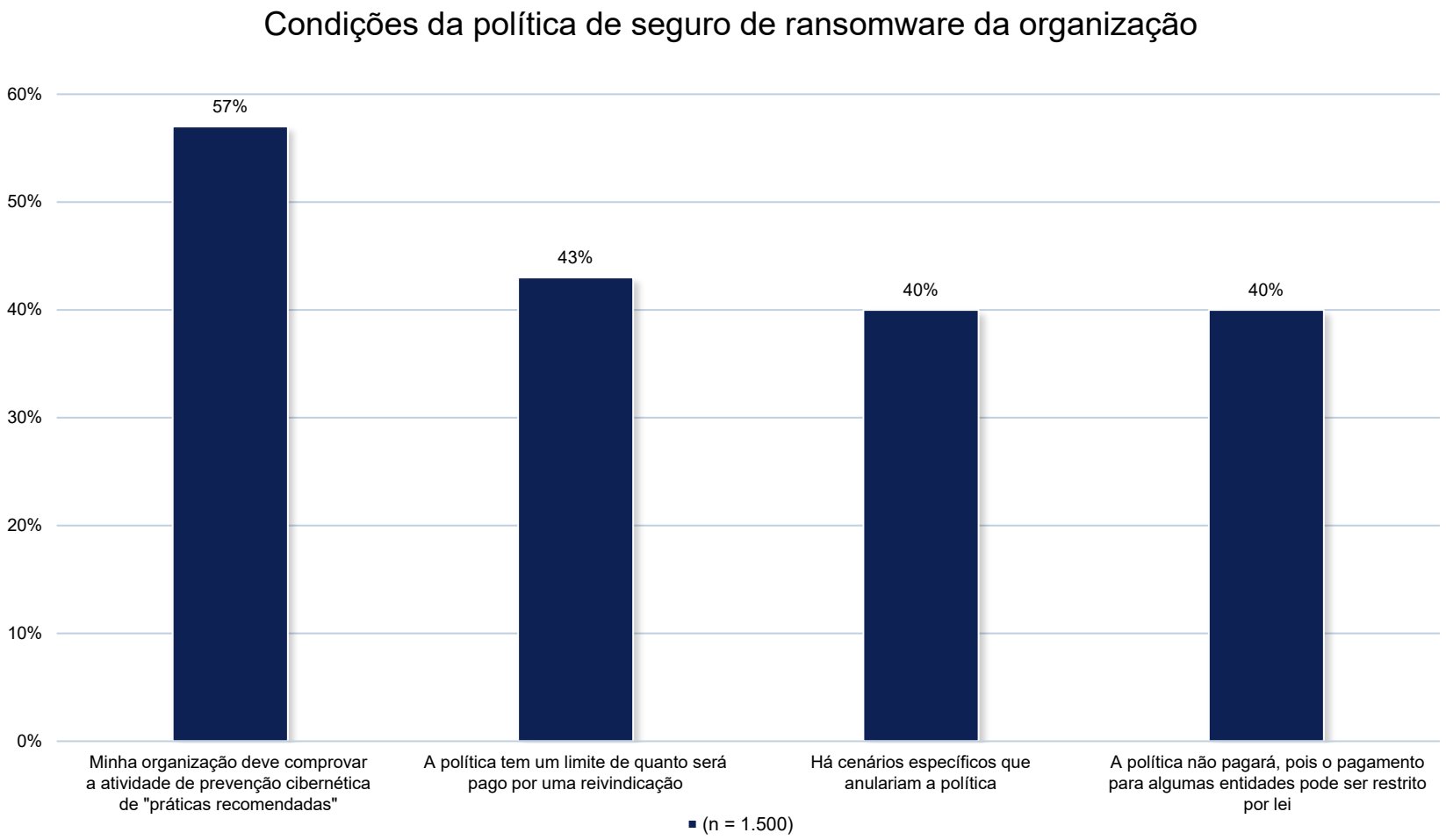
Os criminosos cibernéticos visam vários pontos iniciais, com mais chances de ataques provenientes de fontes externas

Ponto inicial do ataque cibernético mais recente da organização, dividido por região



Copyright © Dell Inc. All Rights Reserved.

As políticas de seguro de ransomware são comuns entre as organizações, mas têm muitas ressalvas



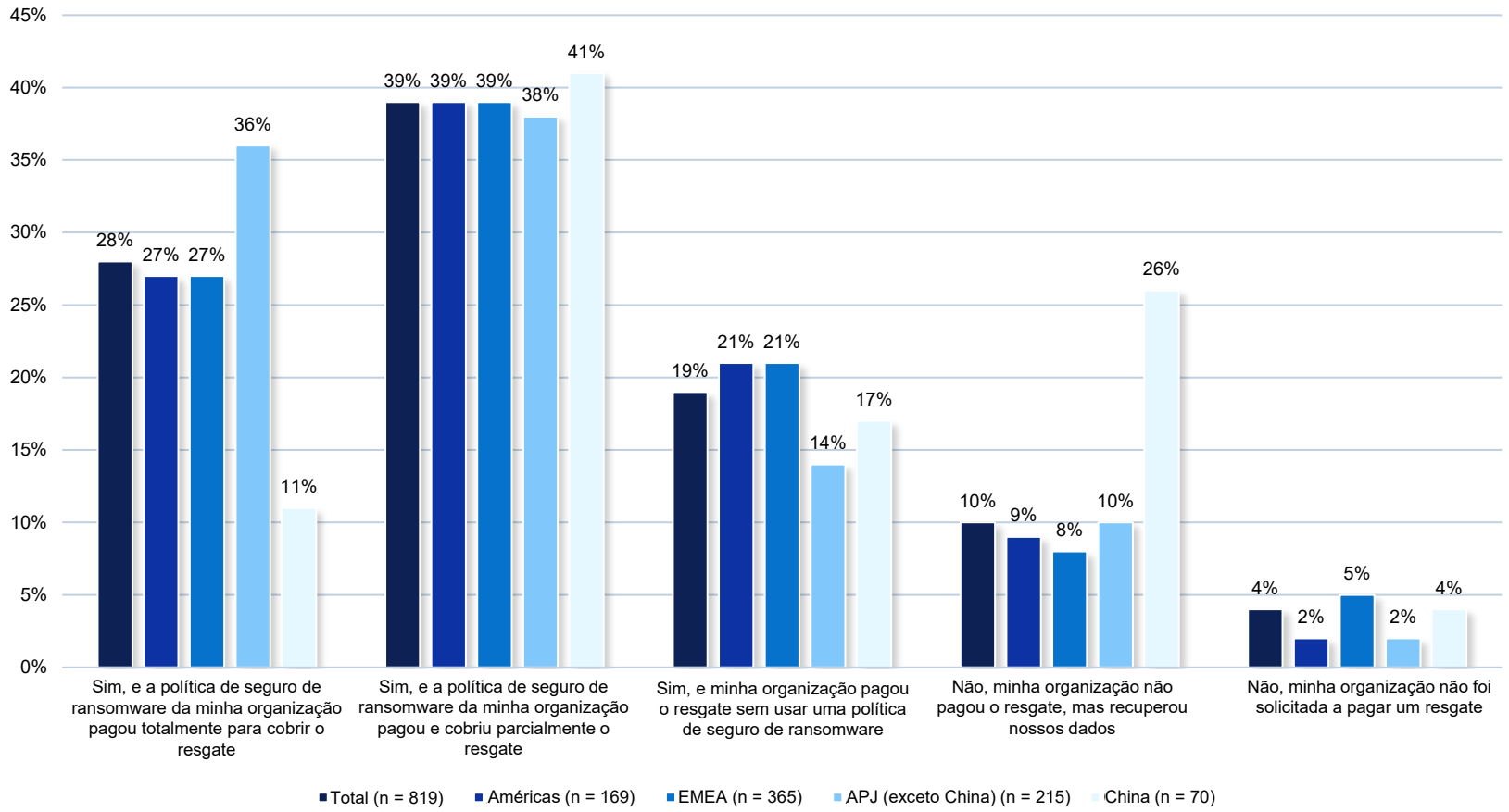
93%

das organizações **têm uma política de ransomware**

Copyright © Dell Inc. All Rights Reserved.

Apesar de muitas terem políticas de ransomware em vigor, as organizações ainda se encontram financeiramente vulneráveis

Um resgate foi pago para ter acesso aos dados da organização, dividido por região



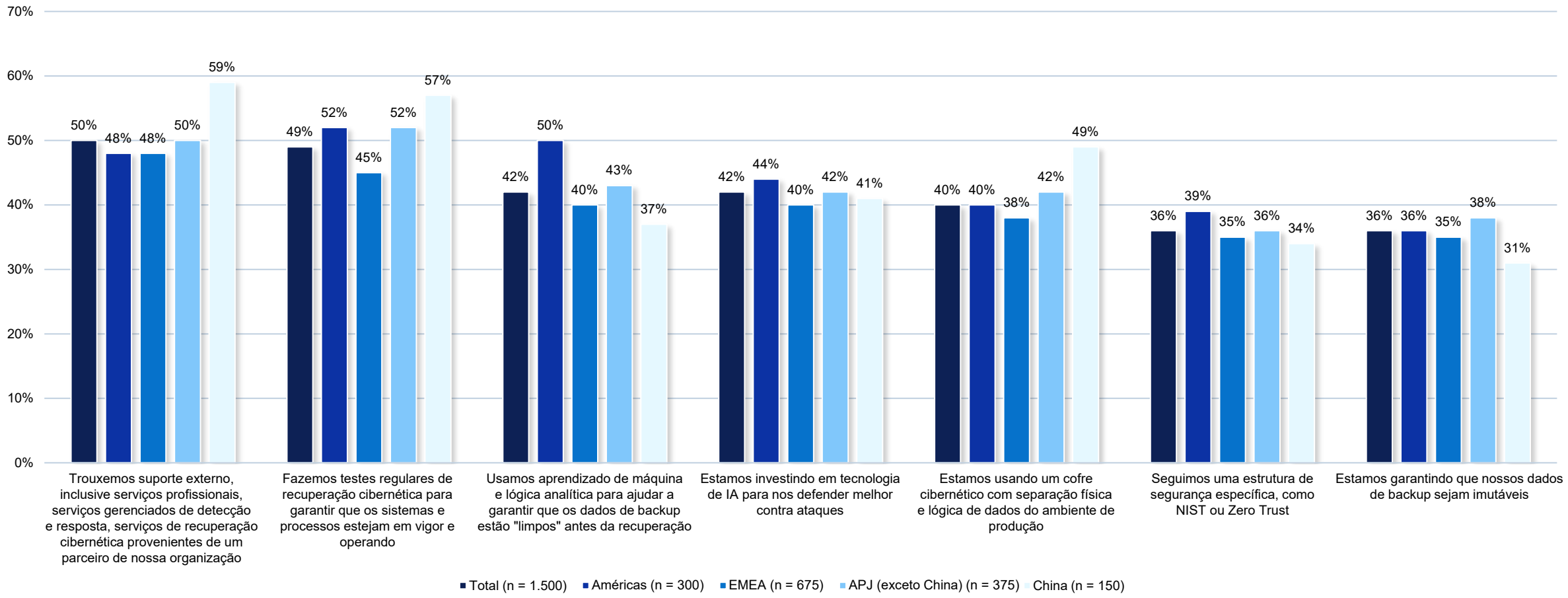
US$ 1,92

milhão — o custo médio para as organizações nos últimos 12 meses, causado por **ataques cibernéticos e outros incidentes** cibernéticos

Copyright © Dell Inc. All Rights Reserved.

Felizmente, as organizações estão tomando medidas para aumentar sua resiliência cibernética

Medidas que as organizações estão tomando para melhorar a resiliência cibernética, divididas por região



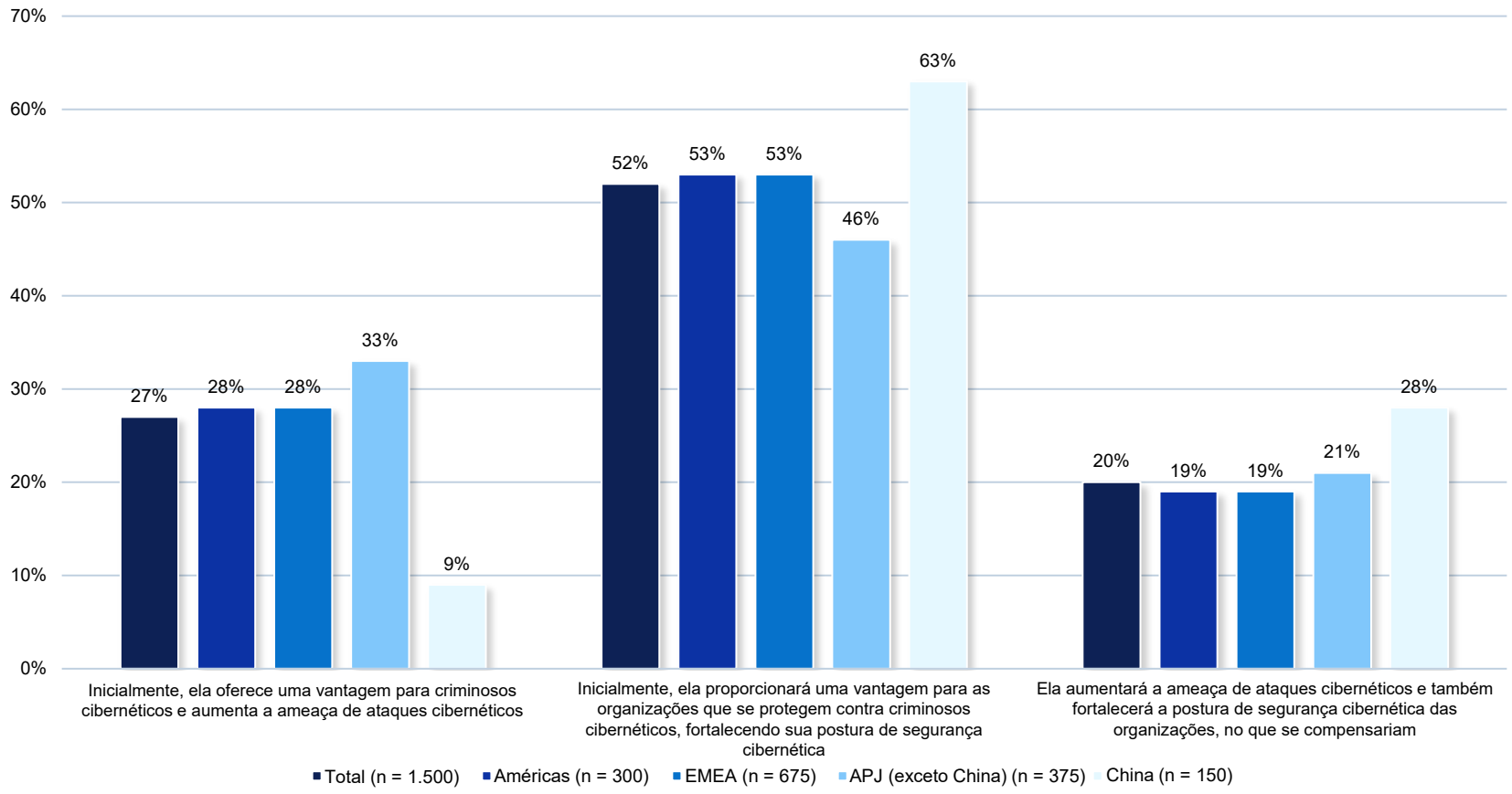
Copyright © Dell Inc. All Rights Reserved.

No entanto, nem todos acreditam que a IA generativa beneficiará sua resiliência cibernética

81%

concordam que as tecnologias emergentes (como IA, IoT, borda) **representam um risco à proteção de dados**

Impacto da IA generativa sobre ameaças cibernéticas e segurança de dados, dividido por região



Copyright © Dell Inc. All Rights Reserved.

Na verdade, com as organizações já preocupadas com a proteção de dados, muitas acreditam que a IA generativa criará novos desafios

88%

concordam que a IA gerativa criará grandes volumes de novos dados que **precisarão ser protegidos e assegurados**

88%

concordam que a IA gerativa aumentará o valor de determinados tipos de dados, o que **exigiria níveis mais altos de serviço de proteção de dados**

85%

concordam que, se os conjuntos de dados usados para IA gerativa estiverem **corrompidos**, isso **afetará o resultado da IA generativa**

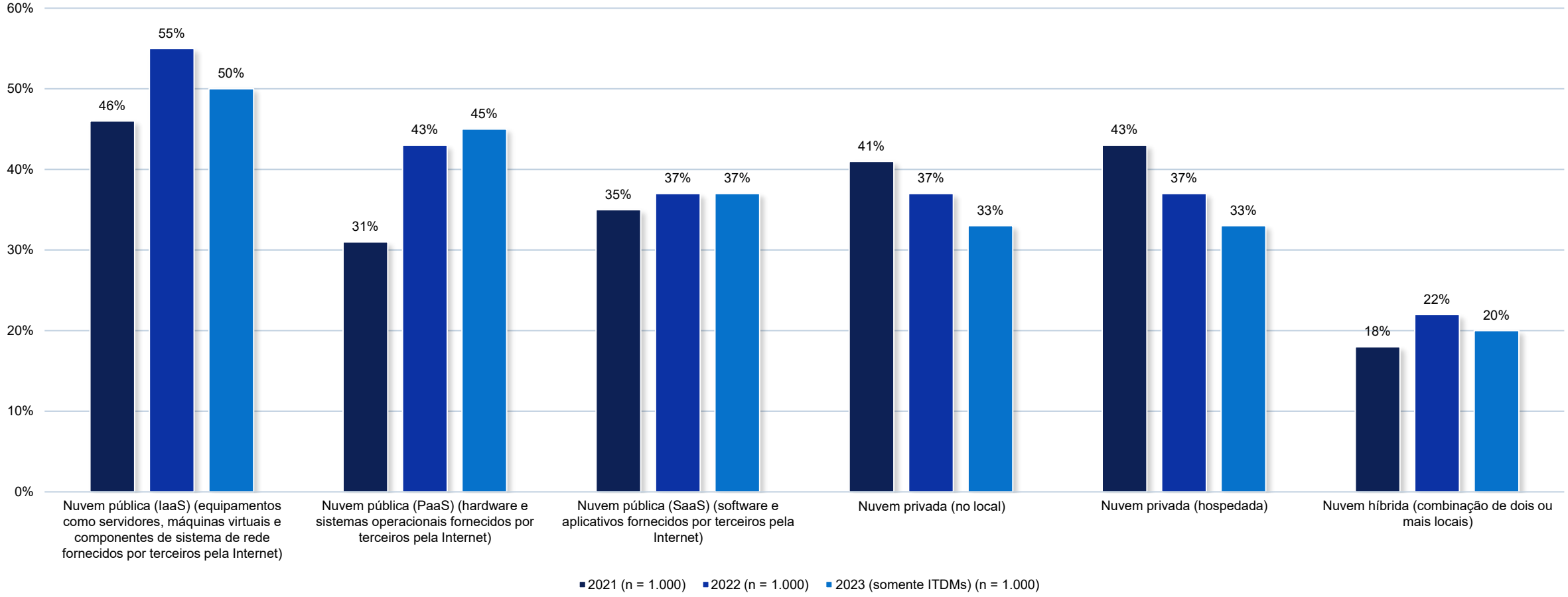
Copyright © Dell Inc. All Rights Reserved.

3. O uso de multicloud

Copyright © Dell Inc. All Rights Reserved.

A nuvem pública continua sendo uma opção popular ao atualizar os aplicativos existentes, enquanto a preferência pela nuvem privada está diminuindo

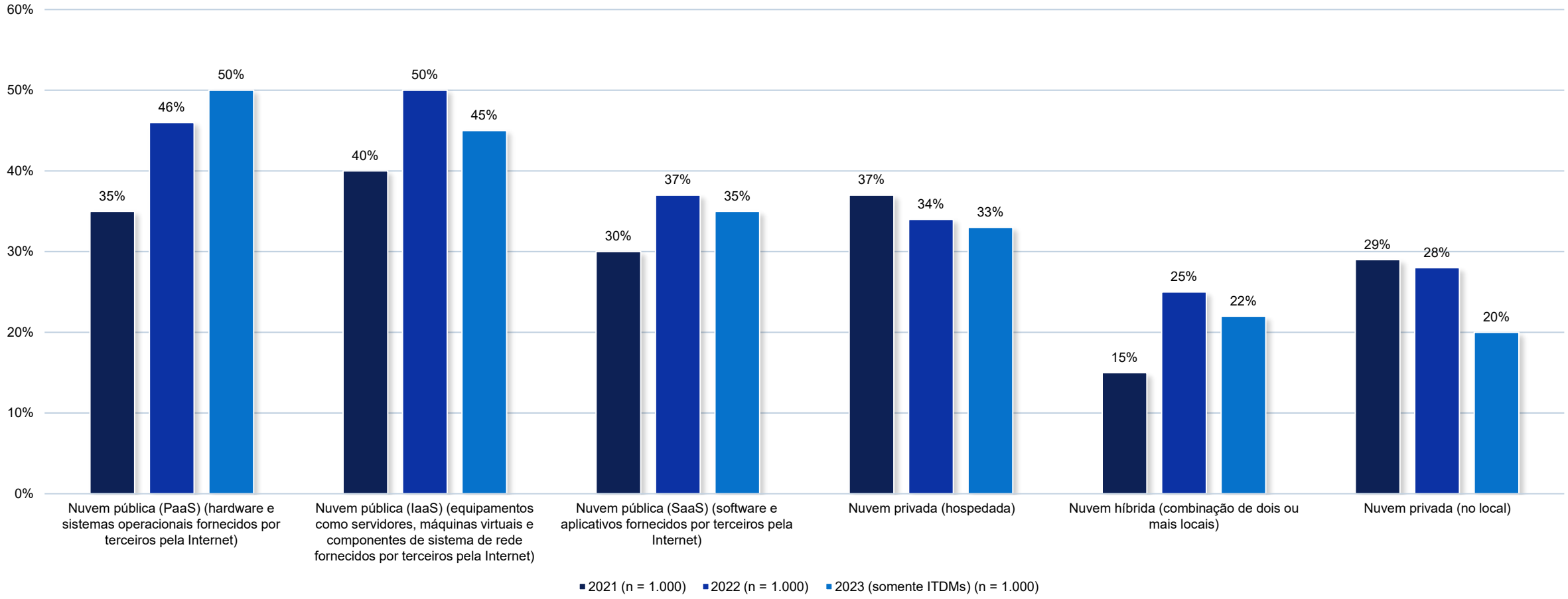
Instruções seguidas ao atualizar os aplicativos existentes, divididas por ano



Copyright © Dell Inc. All Rights Reserved.

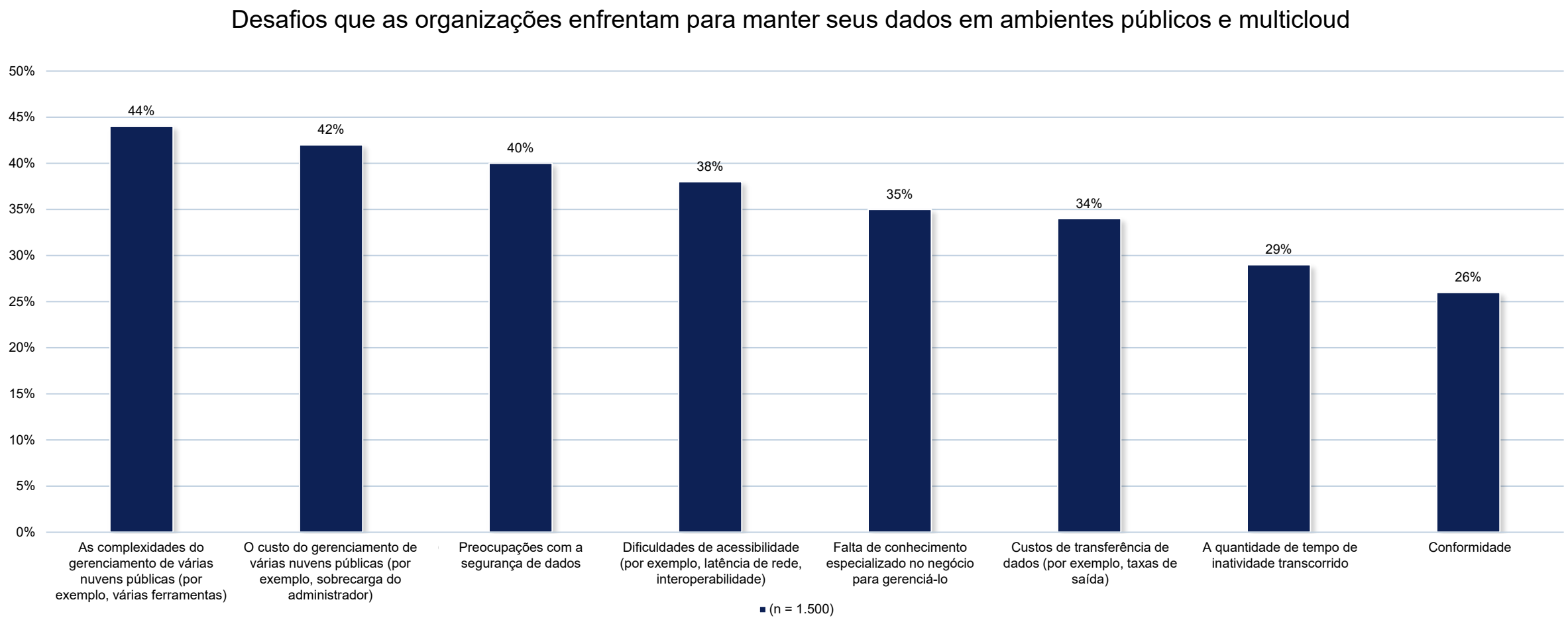
A nuvem pública também continua sendo uma opção popular para implementar novos aplicativos, mas o suporte pode estar em declínio

Instruções seguidas durante a implementação de novos aplicativos, divididas por ano



Copyright © Dell Inc. All Rights Reserved.

Apesar da popularidade da nuvem pública, muitas organizações enfrentam desafios para manter seus dados

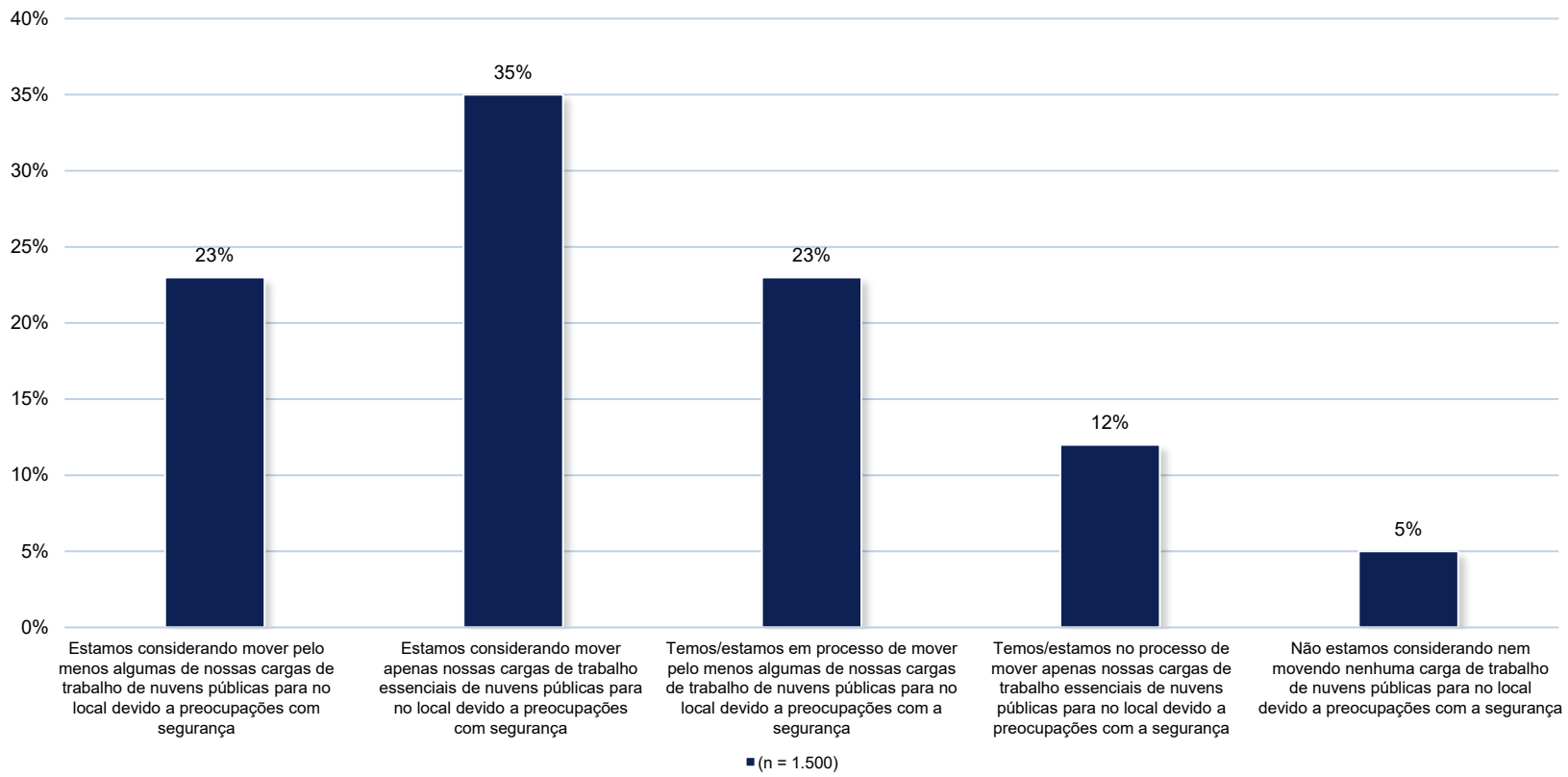


Filtro: divisão de dados: região = total

Copyright © Dell Inc. All Rights Reserved.

Devido às preocupações de segurança, muitas organizações estão migrando ou estão considerando mover uma parte de suas cargas de trabalho de nuvens públicas para no local

A extensão na qual as organizações estão movendo cargas de trabalho de nuvens públicas para no local



Filtro: divisão de dados: região = total

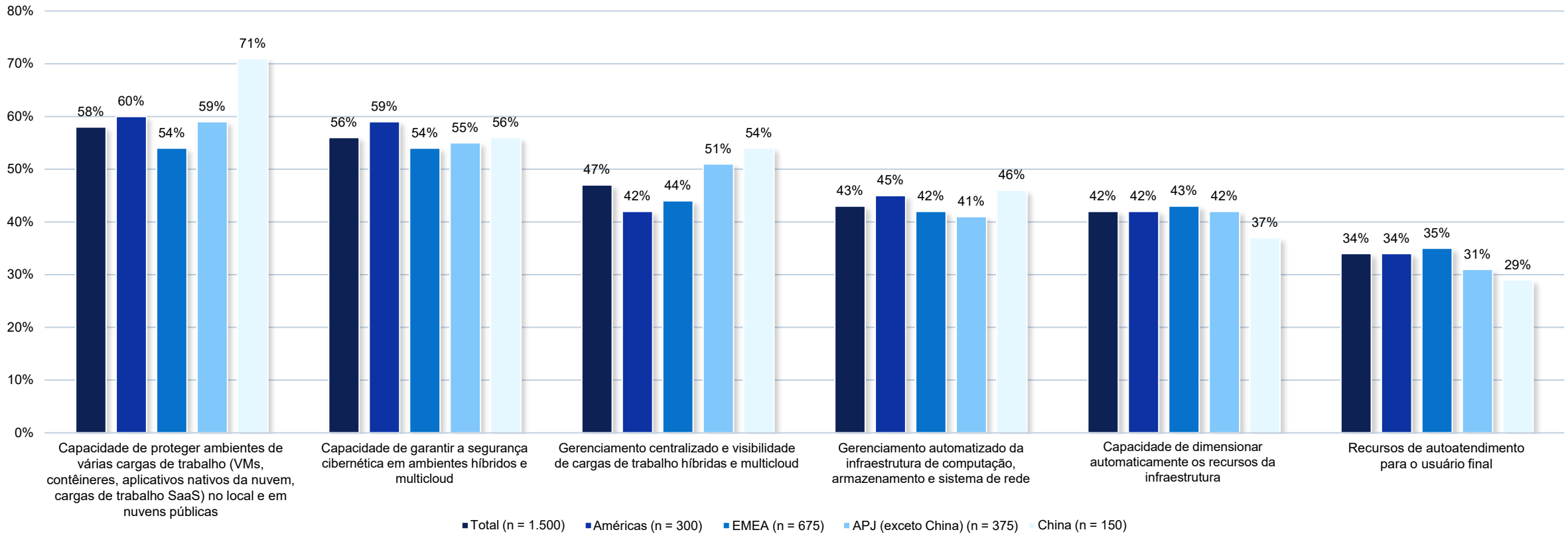
79%

não **estão muito confiantes** de que sua organização pode **proteger todos os seus dados** em ambientes de nuvem pública

Copyright © Dell Inc. All Rights Reserved.

Com incidentes cibernéticos em ascensão e confiança nas estratégias de proteção de dados baixa, muitos veem a segurança como o recurso mais importante ao habilitar operações híbridas e multicloud

Recursos mais importantes ao habilitar operações híbridas e multicloud, divididos por região



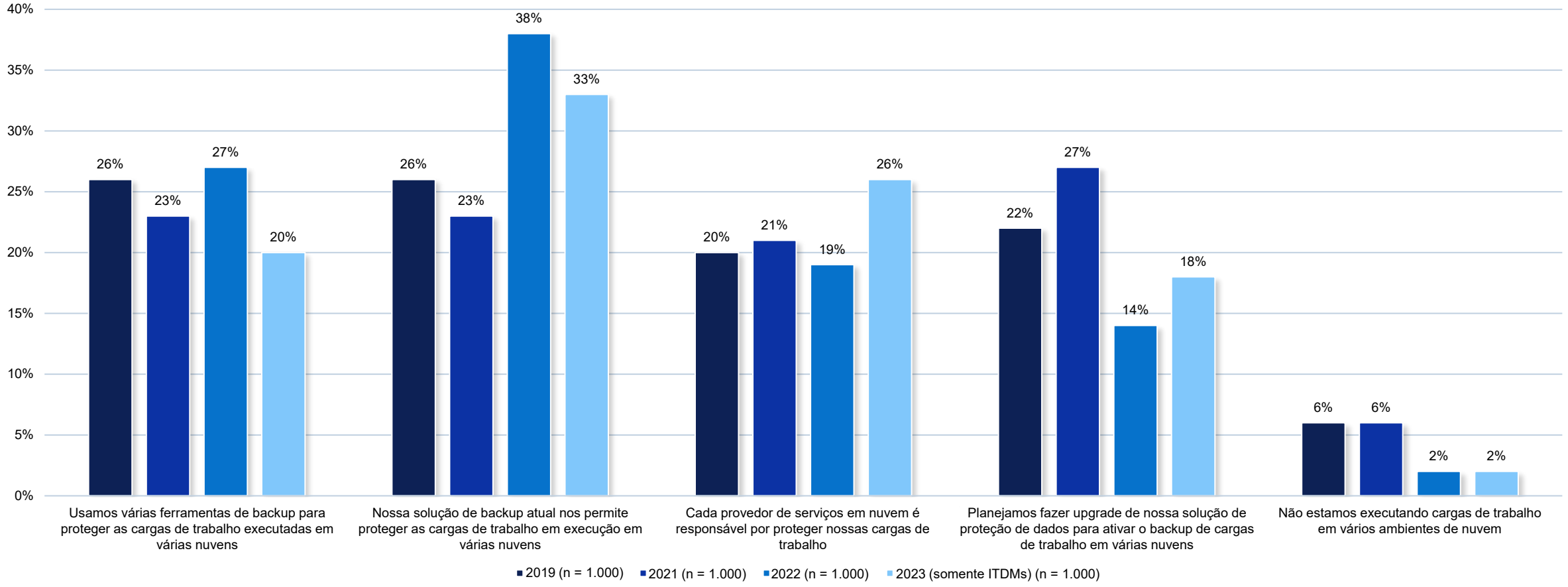
Copyright © Dell Inc. All Rights Reserved.

4. Proteção de um ambiente de nuvem

Copyright © Dell Inc. All Rights Reserved.

Atualmente, as organizações usam várias ferramentas e soluções de backup para proteger suas cargas de trabalho, mas a necessidade de upgrades é mencionada

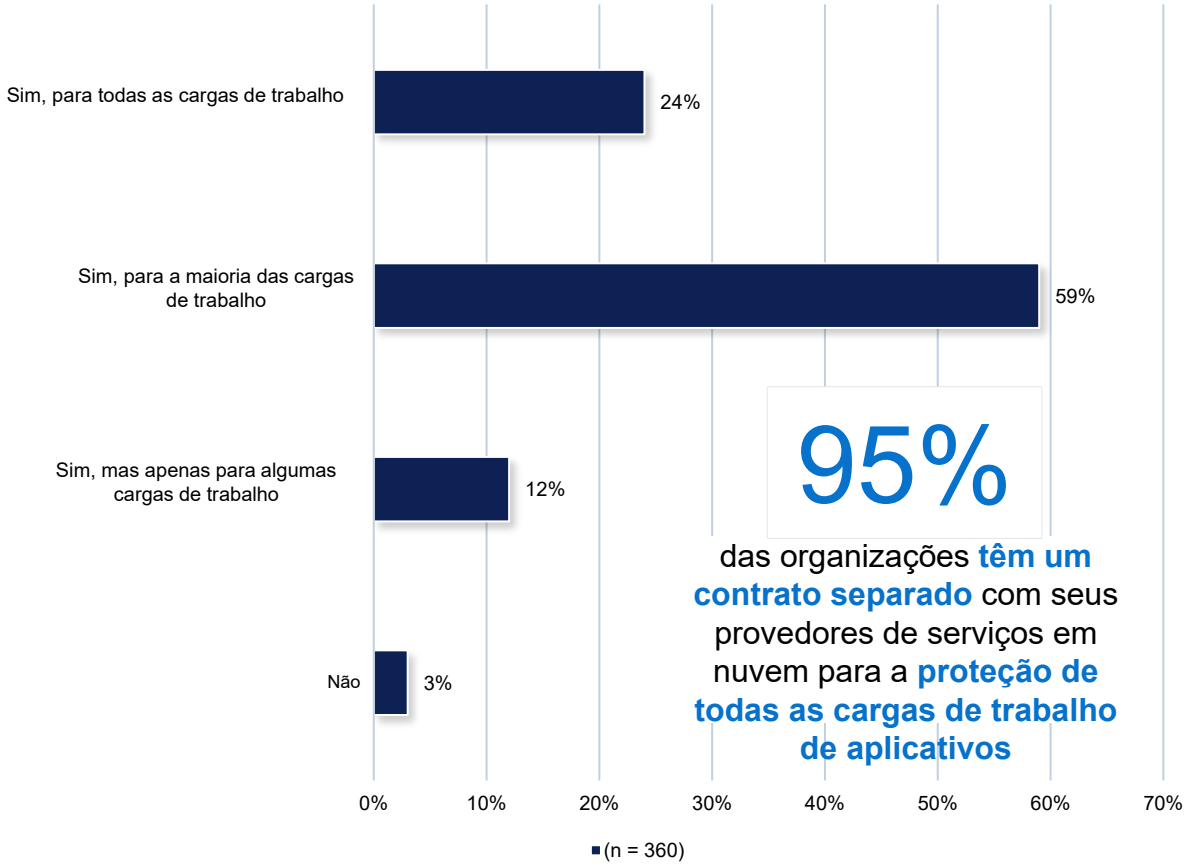
Ferramentas e soluções de proteção em nuvem, divididas por ano



Copyright © Dell Inc. All Rights Reserved.

As organizações estão cada vez mais dependentes de provedores de serviços em nuvem para proteger suas cargas de trabalho em ambientes de nuvem

Contrato separado com o CSP para a proteção de cargas de trabalho de aplicativos

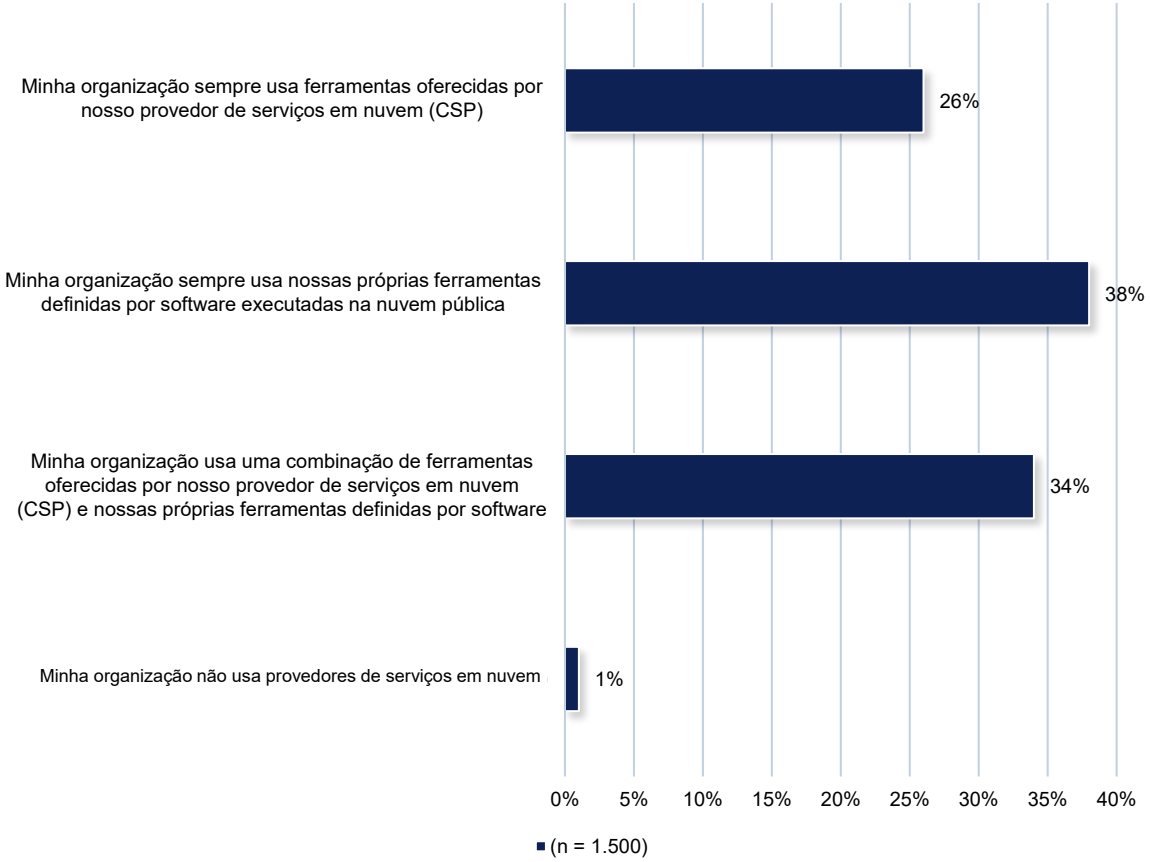


95%

das organizações **têm um contrato separado** com seus provedores de serviços em nuvem para a **proteção de todas as cargas de trabalho de aplicativos**

Filtro: divisão de dados: região = total

Ferramentas de backup e recuperação oferecidas pelo provedor de serviços em nuvem



Filtro: divisão de dados: região = total

Copyright © Dell Inc. All Rights Reserved.

Principais conclusões — em resumo

O ambiente de risco de proteção de dados

- As preocupações com as medidas de proteção de dados são generalizadas e, com a falta de confiança, as organizações se encontram em uma posição vulnerável
- Quase todas as organizações enfrentam desafios em relação à proteção de dados, com muitas também enfrentando interrupções significativas nos últimos 12 meses devido à perda de dados e/ou tempo de inatividade não planejado do sistema
- As ameaças à segurança externa foram as causas mais comuns de perda de dados e/ou tempo de inatividade não planejado dos sistemas nos últimos 12 meses
- Apesar dos desafios e das preocupações com a proteção de dados, poucos implementaram totalmente a segurança Zero Trust

A crescente ameaça de ataques cibernéticos

- Houve um aumento nas organizações que enfrentam um ataque cibernético ou incidente nos últimos 12 meses, custando, em média, US$ 1,92 milhão às empresas
- Muitas organizações estão preocupadas de que os dados de backup possam ser infectados ou corrompidos por ataques de ransomware
- Além do risco, há um excesso de confiança equivocado em relação às consequências de um ataque de ransomware
- Apesar de as políticas de seguro de ransomware serem comuns, elas têm muitas ressalvas, deixando as organizações financeiramente vulneráveis

O uso de multicloud

- A nuvem pública continua sendo uma opção popular ao atualizar e implementar novos aplicativos, mas há preocupações com a segurança de dados
- Devido às preocupações de segurança, muitas organizações estão migrando ou estão considerando mover uma parte de suas cargas de trabalho de nuvens públicas para no local
- Com incidentes cibernéticos em ascensão e confiança nas estratégias de proteção de dados baixa, muitos veem a segurança como o recurso mais importante ao habilitar operações híbridas e multicloud

Protegendo um ambiente de nuvem

- Atualmente, as organizações usam várias ferramentas e soluções de backup para proteger suas cargas de trabalho, mas reconhecem que upgrades são necessários
- As organizações estão cada vez mais dependentes de provedores de serviços em nuvem para proteger suas cargas de trabalho em ambientes de nuvem

Copyright © Dell Inc. All Rights Reserved.

DELL Technologies