Global Data Protection Index – Sonderedition 2024

Wichtigste Erkenntnisse – Oktober 2023

VansonBourne

DELL Technologies

Schwerpunkt der wichtigsten Erkenntnisse

1
Die Data-Protection-Risikolandschaft

2
Die zunehmende Bedrohung durch Cyberangriffe

3
Die Nutzung von Multi-Cloud

4
Sicherung einer Multi-Cloud-Umgebung

Copyright © Dell Inc. All Rights Reserved.

5 wichtige Erkenntnisse

Die Zahl der Cyberangriffe nimmt weiter zu.

Die Kosten von Cyberangriffen steigen.

Versicherungspolicen decken die Kosten von Angriffen nicht ausreichend ab.

Eine verstärkte Nutzung von generativer KI könnte zu hochwertigeren Daten führen.

Dies führt zu größeren Risiken und mehr finanziellen Auswirkungen von Cyberangriffen.

Copyright © Dell Inc. All Rights Reserved.

Wen haben wir befragt?

1.500 IT-EntscheidungsträgerInnen und IT-Sicherheitsentscheidungs-trägerInnen im September und Oktober 2023

Unternehmen aus einer Vielzahl von öffentlichen und privaten Branchen

Unternehmen mit mehr als 250 MitarbeiterInnen

4 Regionen:

Nord-, Süd- und Mittelamerika (300)
EMEA (675)
APJ (375)
China (150)

Copyright © Dell Inc. All Rights Reserved.

1. Die Data-Protection-Risikolandschaft

Copyright © Dell Inc. All Rights Reserved.

Die Bedenken hinsichtlich der Data-Protection-Maßnahmen sind weit verbreitet und da das Vertrauen fehlt, befinden sich die Unternehmen in einer verwundbaren Position

60 %

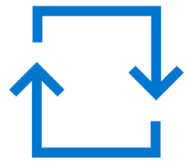
sind **nicht sehr zuversichtlich**, dass ihr Unternehmen **seine Servicelevelziele für Backup und Recovery (SLOs) erfüllt**.

79 %

der Unternehmen **befürchten eine Unterbrechung Ihrer Geschäftstätigkeit durch ein Ereignis** innerhalb der nächsten zwölf Monate.

75 %

befürchten, dass die vorhandenen Data-Protection-Maßnahmen des Unternehmens **nicht ausreichen, um mit Malware- und Ransomwarebedrohungen umzugehen**.



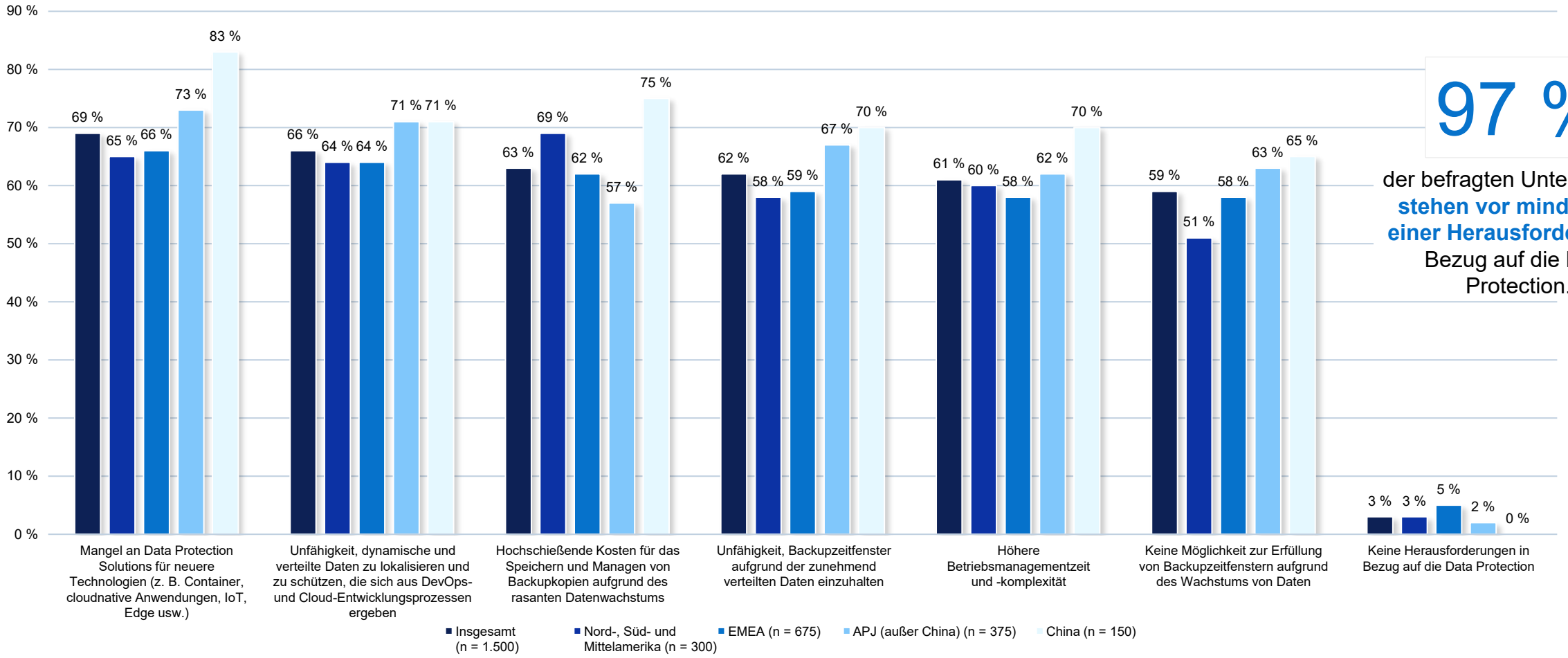
65 %

sind **nicht sehr zuversichtlich**, dass ihr Unternehmen im Falle eines Datenverlusts **die Systeme/Daten aller Plattformen vollständig wiederherstellen kann**.

Copyright © Dell Inc. All Rights Reserved.

Neben den Bedenken hinsichtlich der Data Protection stehen viele Unternehmen vor weiteren Herausforderungen

Top-5-Rangliste: Herausforderungen in Bezug auf Data Protection, aufgeschlüsselt nach Regionen

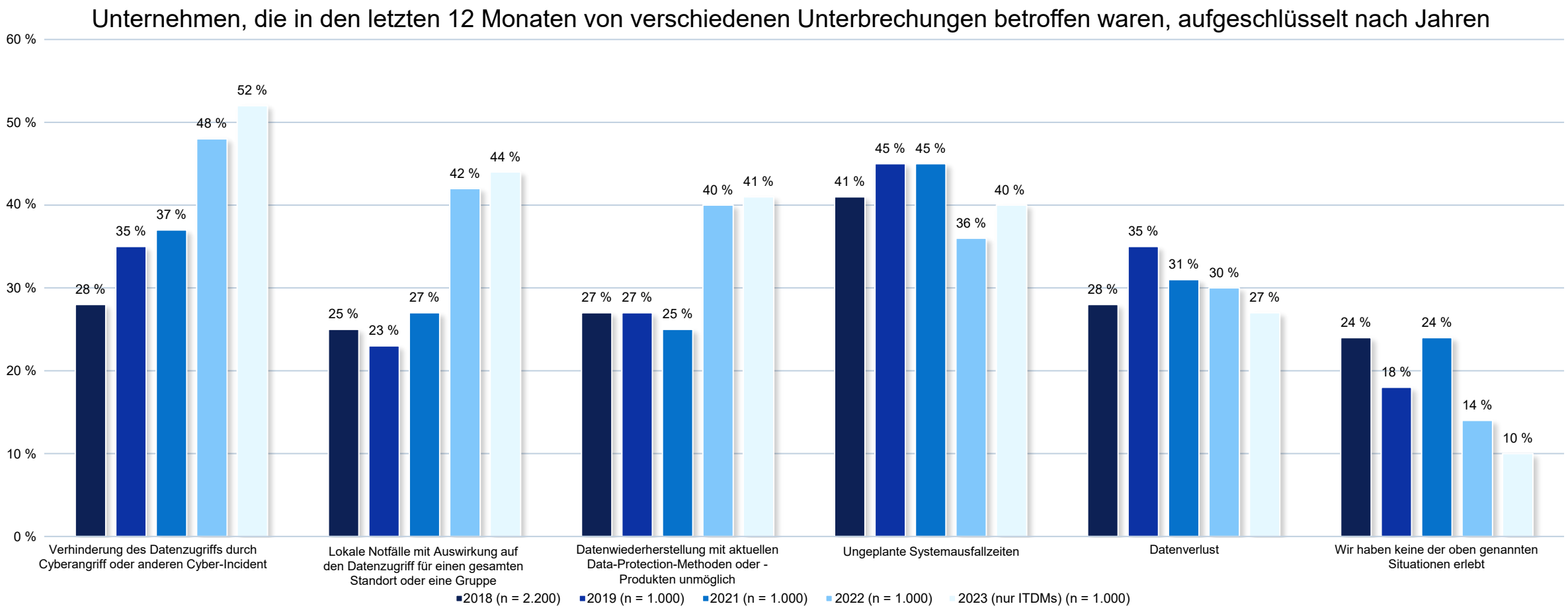


97 %

der befragten Unternehmen **stehen vor mindestens einer Herausforderung** in Bezug auf die Data Protection.

Copyright © Dell Inc. All Rights Reserved.

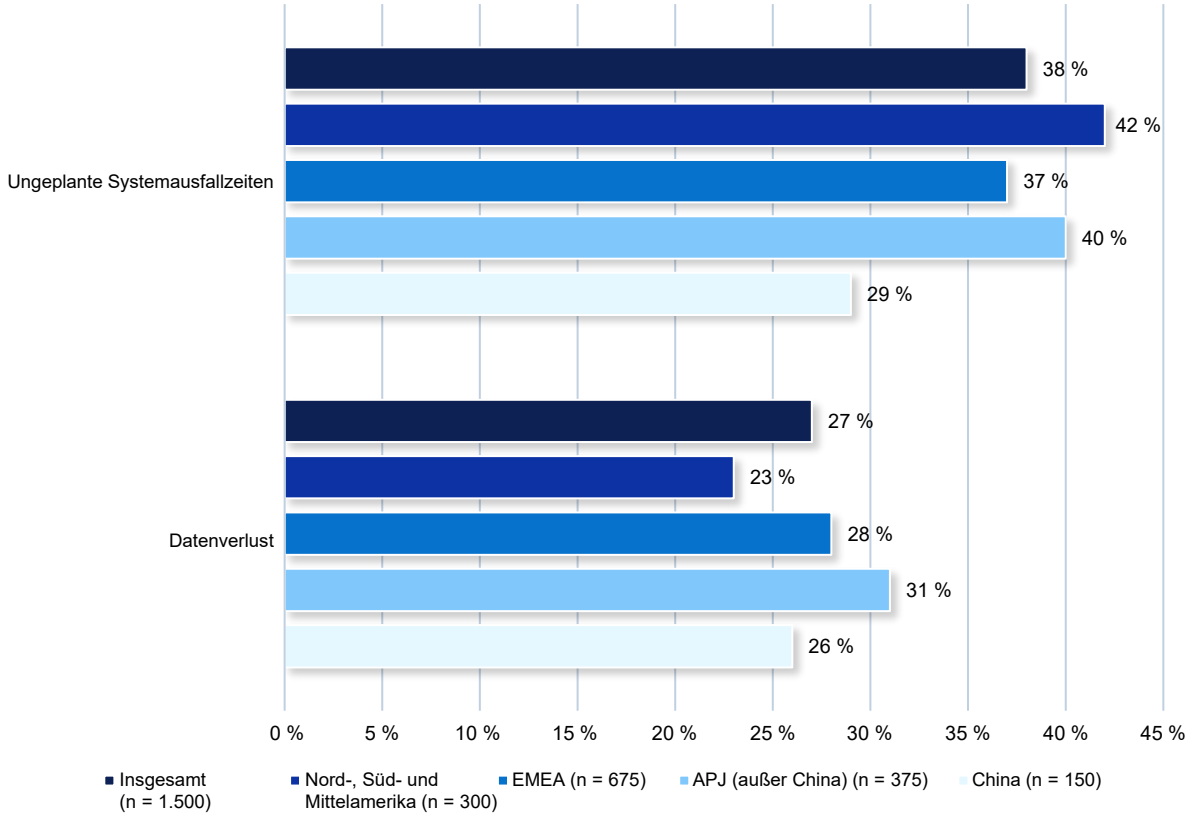
In den letzten 12 Monaten waren Unternehmen mit erheblichen Unterbrechungen konfrontiert, wobei Cyberangriffe eine allgegenwärtige und ständig wachsende Bedrohung darstellen



Copyright © Dell Inc. All Rights Reserved.

Datenverluste haben nicht nur zu Unterbrechungen beigetragen, sondern auch Auswirkungen auf den Nettogewinn

Prozentualer Anteil der Unternehmen, die in den letzten 12 Monaten ungeplante Systemausfälle oder Datenverluste erlitten haben, aufgeschlüsselt nach Regionen



In den letzten 12 Monaten:

26 Stunden

ungeplante Systemausfallzeiten, die im Durchschnitt auftreten

2,45 TB

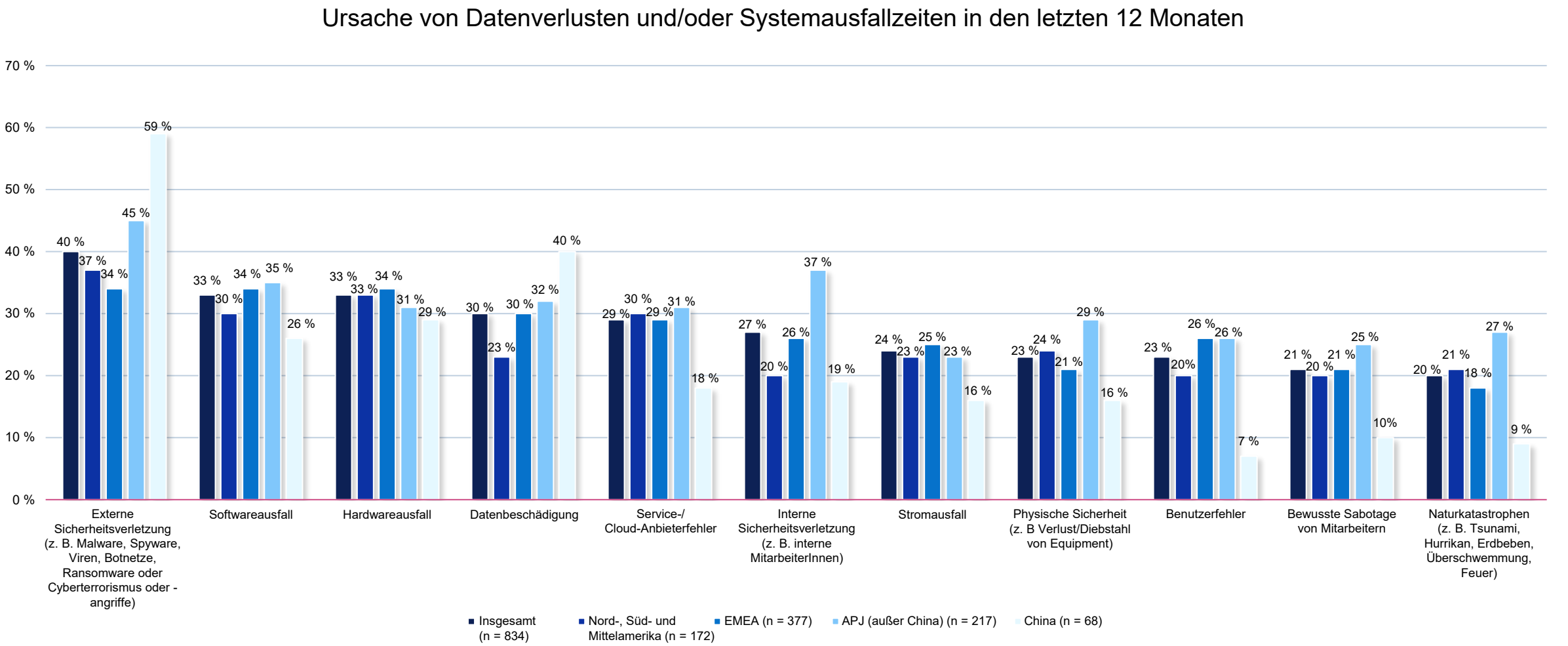
an Daten verloren gegangen, im Durchschnitt

2,61 Mio. USD

durchschnittliche **Kosten durch Datenverlust**

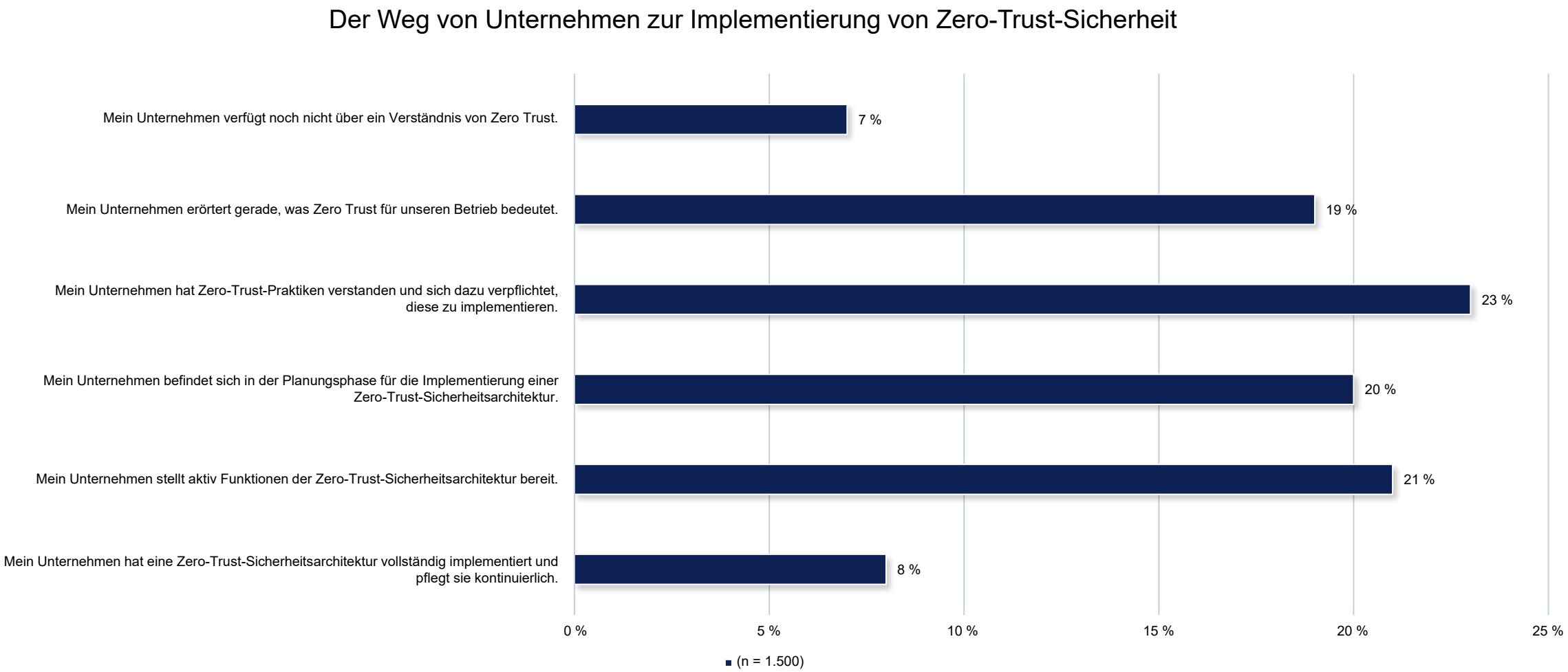
Copyright © Dell Inc. All Rights Reserved.

Externe Sicherheitsbedrohungen sind die häufigsten Ursachen für Datenverluste und/oder ungeplante Systemausfälle in den letzten 12 Monaten



Copyright © Dell Inc. All Rights Reserved.

Trotz der Herausforderungen und Bedenken in Bezug auf die Data Protection haben nur wenige Unternehmen Zero-Trust-Sicherheit vollständig umgesetzt



Filter: Datenteilung: Region = Gesamt

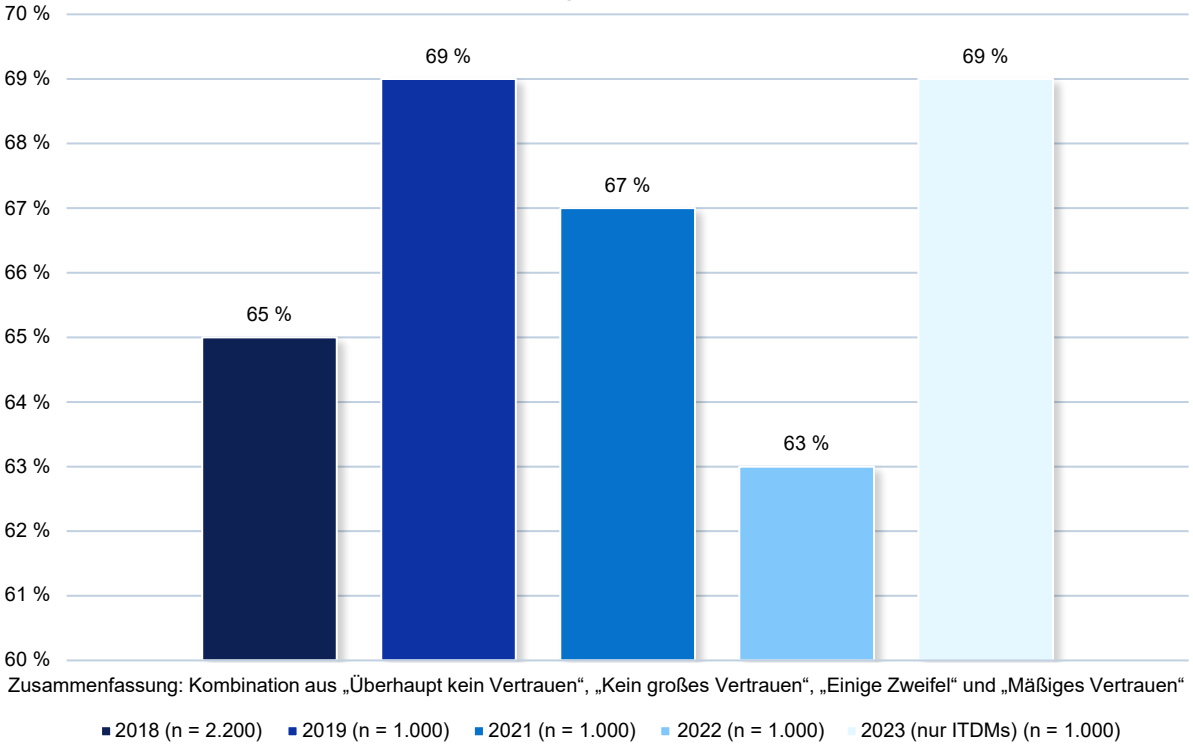
Copyright © Dell Inc. All Rights Reserved.

2. Die zunehmende Bedrohung durch Cyberangriffe

Copyright © Dell Inc. All Rights Reserved.

Die Bedenken hinsichtlich der Data-Protection-Maßnahmen sind weit verbreitet und da das Vertrauen fehlt, befinden sich die Unternehmen in einer verwundbaren Position

Kein großes Vertrauen, dass alle geschäftskritischen Daten im Falle eines zerstörerischen Cyberangriffs zuverlässig wiederhergestellt werden können, aufgeschlüsselt nach Jahren



81 %

stimmen zu, dass Ihr Unternehmen mit der wachsenden Zahl an Homeoffice-MitarbeiterInnen **einem höheren Risiko von Datenverlust durch Cyberbedrohungen** unterliegt.

74 %

sind **besorgt**, dass ihre Backupdaten **durch Ransomwareangriffe infiziert oder beschädigt werden könnten**.

Copyright © Dell Inc. All Rights Reserved.

Das Risiko wird noch dadurch erhöht, dass ein falsches Vertrauen in die Folgen eines Ransomwareangriffs herrscht

72 %

sind der Meinung, dass ihre Arbeit und die MitarbeiterInnen in ihrem Unternehmen **nicht von einem Ransomwareangriff betroffen sein werden**.

74 %

stimmen zu, dass sie im Falle eines Ransomwareangriffs auf ihr Unternehmen **alle Daten zurückerhalten**, um den Betrieb wieder aufzunehmen, **wenn sie das Lösegeld zahlen**.

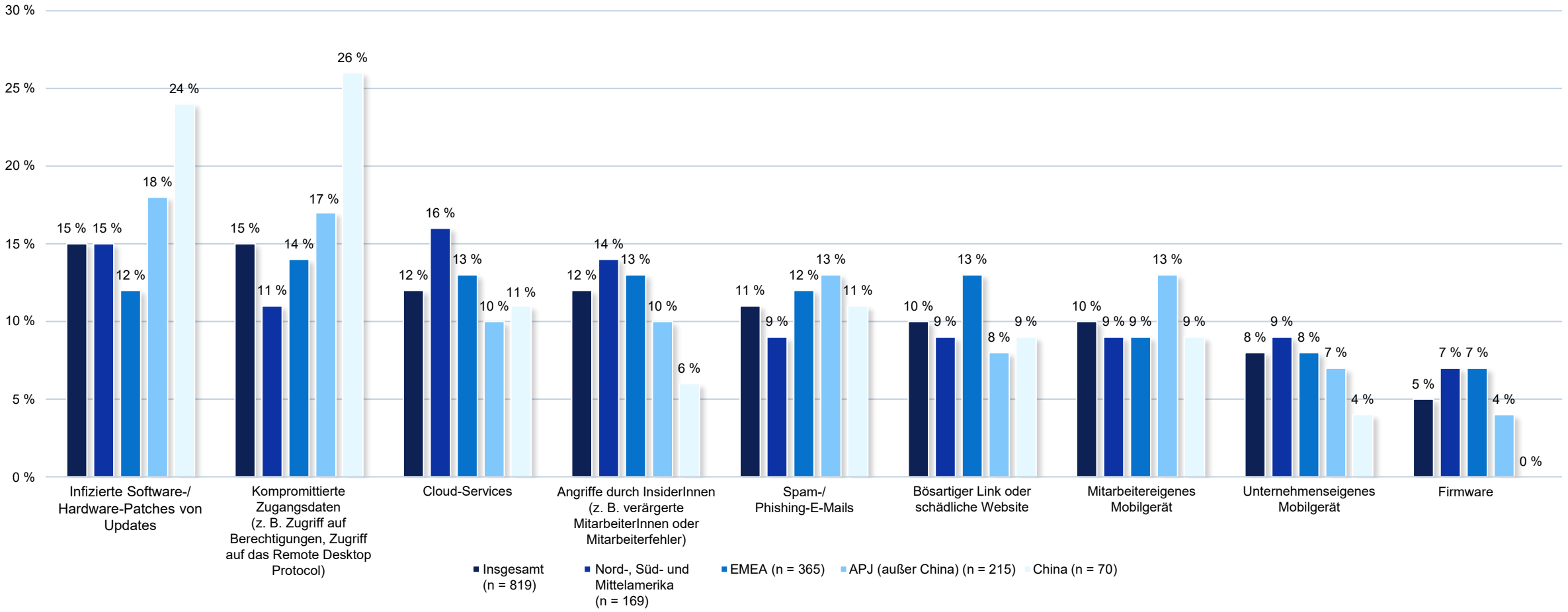
66 %

glauben, dass ihr Unternehmen im Falle eines Ransomwareangriffs nach der Zahlung des Lösegelds **nicht erneut angegriffen wird**.

Copyright © Dell Inc. All Rights Reserved.

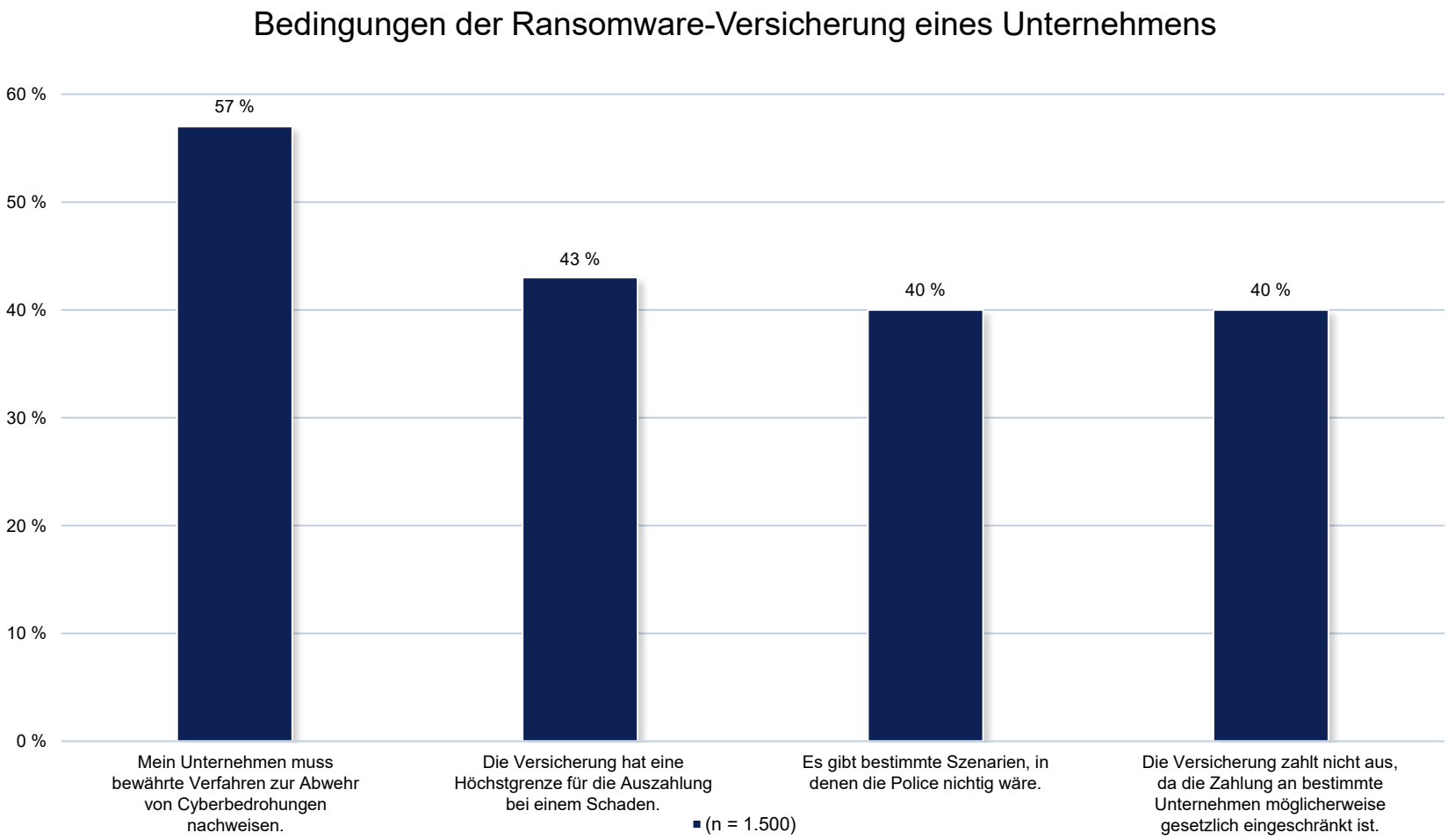
Cyberkriminelle haben es auf verschiedene Einstiegspunkte abgesehen, aber die Angriffe kommen eher von externen Quellen

Einstiegspunkt für den jüngsten Cyberangriff auf ein Unternehmen, aufgeschlüsselt nach Regionen



Copyright © Dell Inc. All Rights Reserved.

Ransomware-Versicherungen sind in Unternehmen üblich, werden jedoch unter strengen Auflagen abgeschlossen

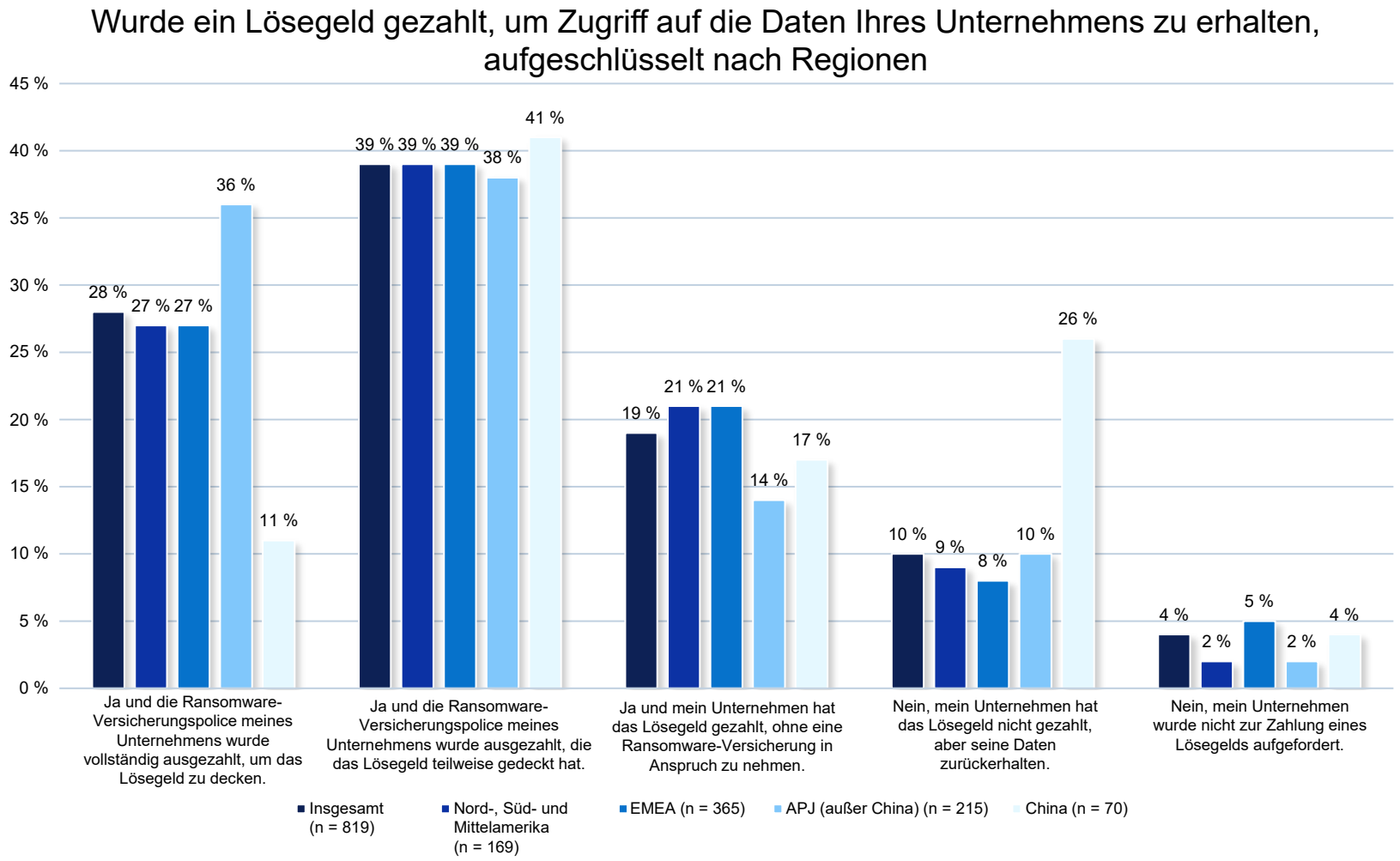


93 %

der Unternehmen **verfügen über eine Ransomware-Police**.

Copyright © Dell Inc. All Rights Reserved.

Obwohl viele Unternehmen über Ransomware-Policen verfügen, sind sie immer noch finanziell gefährdet



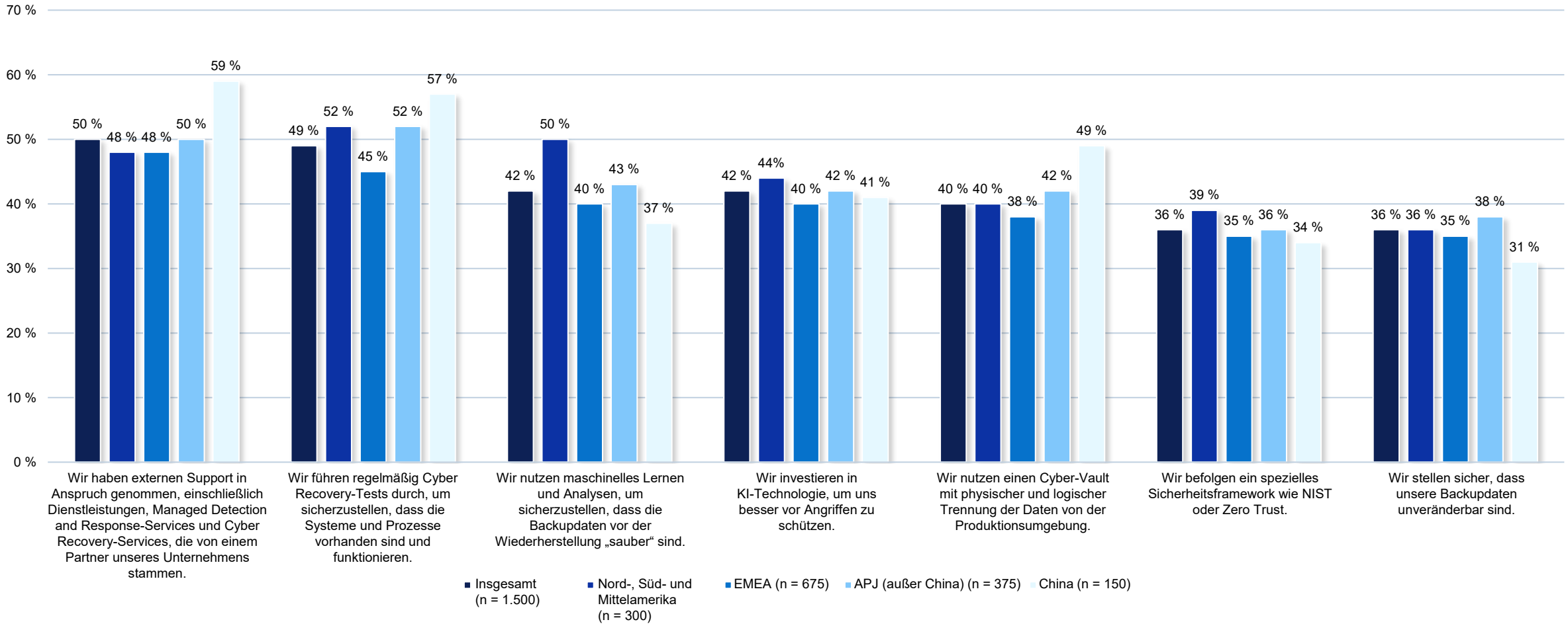
1,92 Mio. USD

Die durchschnittlichen Kosten, die Unternehmen in den letzten 12 Monaten durch **Cyberangriffe und andere Cyber-Incidents** entstanden sind

Copyright © Dell Inc. All Rights Reserved.

Erfreulicherweise ergreifen Unternehmen Schritte, um ihre Ausfallsicherheit bei Cyberangriffen zu verbessern

Schritte, die Unternehmen ergreifen, um ihre Ausfallsicherheit bei Cyberangriffen zu verbessern, aufgeschlüsselt nach Regionen



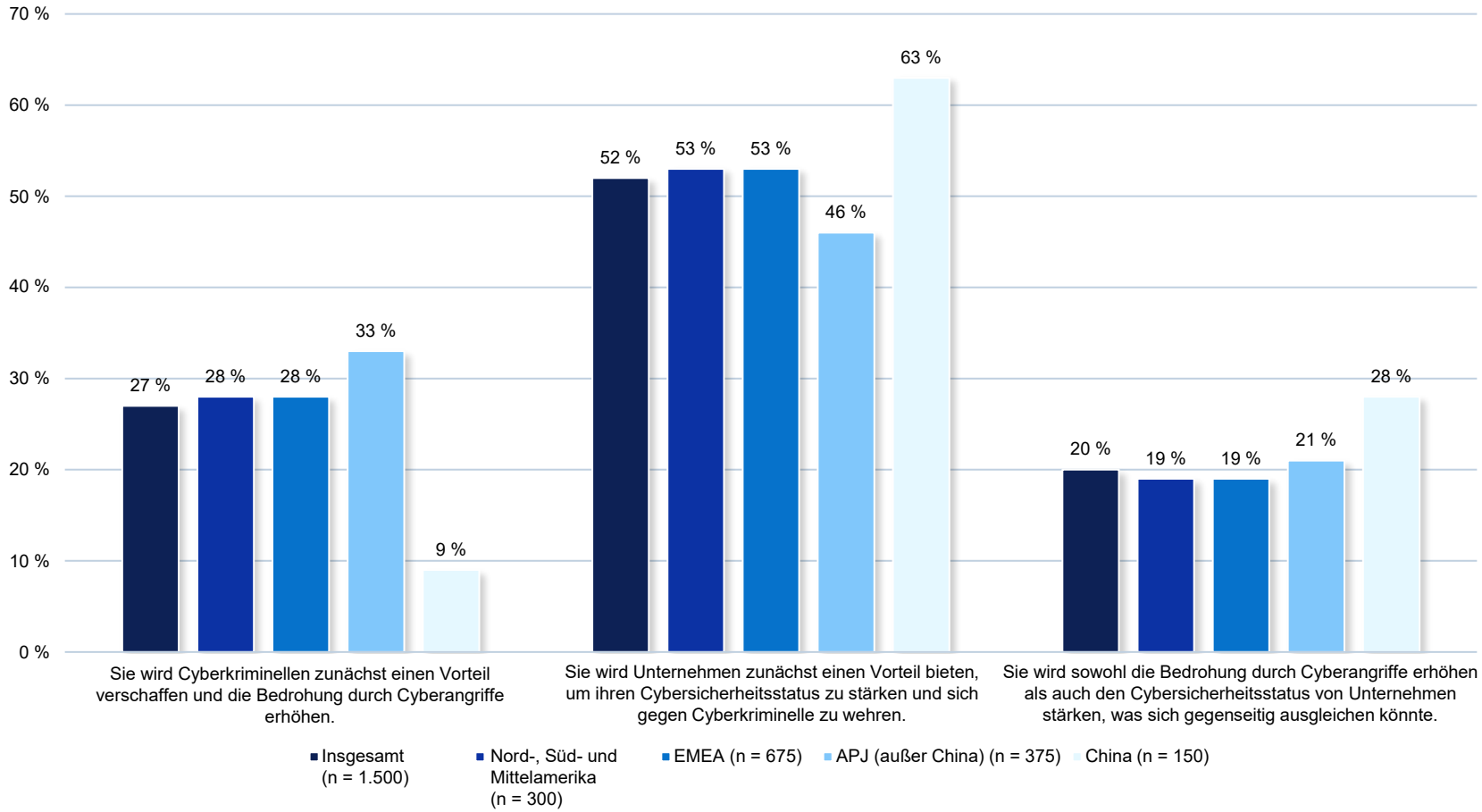
Copyright © Dell Inc. All Rights Reserved.

Allerdings glauben nicht alle Befragten, dass die generative KI ihre Ausfallsicherheit bei Cyberangriffen verbessern wird

81 %

stimmen zu, dass neue Technologien (wie KI, IoT, Edge) **ein Risiko für die Data Protection darstellen**.

Auswirkungen generativer KI auf Cyberbedrohungen und Datensicherheit, aufgeschlüsselt nach Regionen



Copyright © Dell Inc. All Rights Reserved.

Da sich Unternehmen bereits um die Data Protection sorgen, glauben viele, dass generative KI neue Herausforderungen mit sich bringen wird

88 %

stimmen zu, dass generative KI große Mengen neuer Daten erzeugen wird, die **geschützt und gesichert werden müssen**.

88 %

sind der Meinung, dass generative KI den Wert bestimmter Datentypen erhöhen wird, was **höhere Data-Protection-Servicelevel erfordert**.

85 %

stimmen zu, dass eine **Beschädigung** von Datenvolumen, die für generative KI verwendet werden, **Auswirkungen auf die Ergebnisse der generativen KI haben wird**.

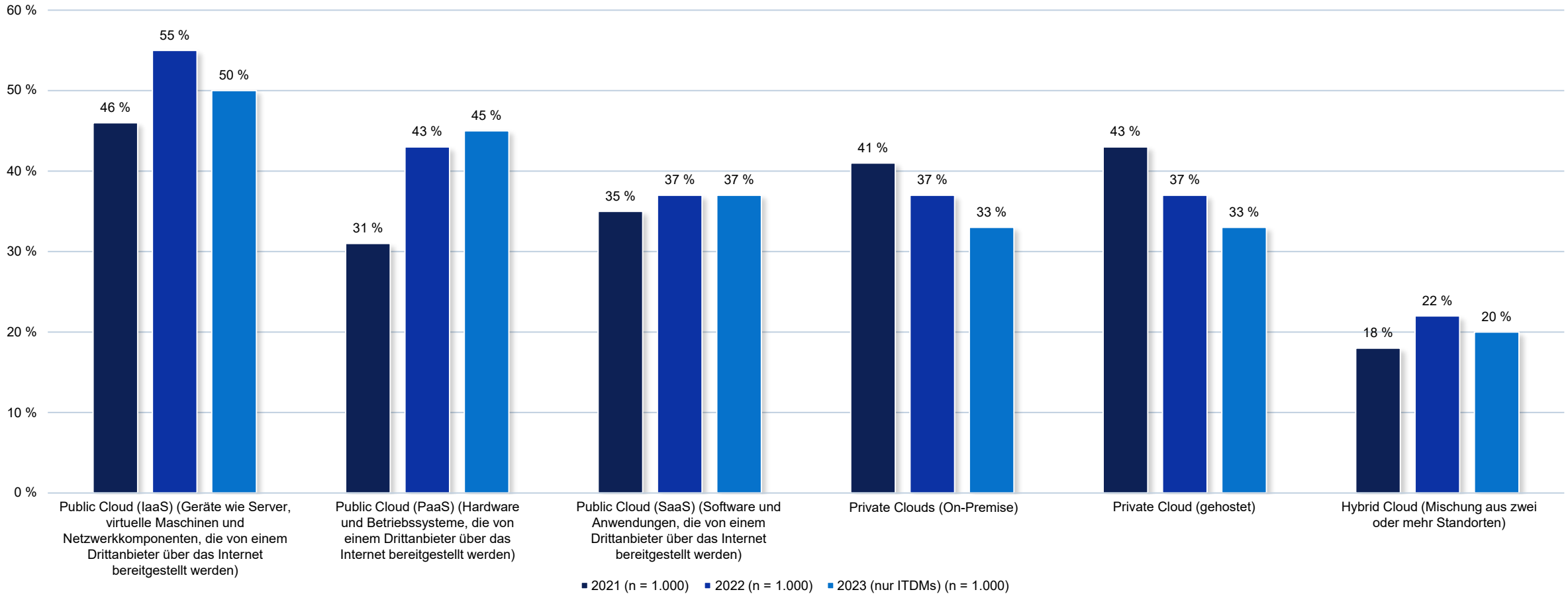
Copyright © Dell Inc. All Rights Reserved.

3. Die Nutzung von Multi-Cloud

Copyright © Dell Inc. All Rights Reserved.

Die Public Cloud ist nach wie vor eine beliebte Wahl bei der Aktualisierung bestehender Anwendungen, während die Präferenz für die Private Cloud abnimmt

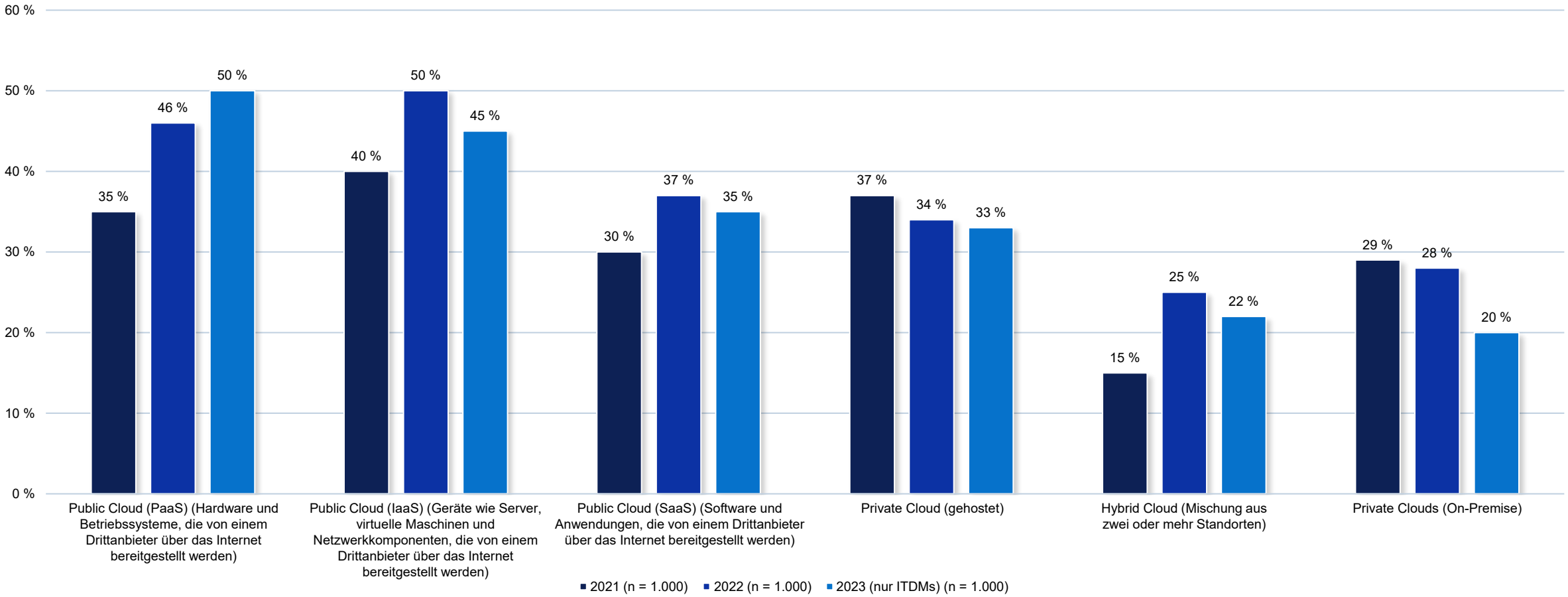
Richtungen, die bei der Aktualisierung bestehender Anwendungen eingeschlagen werden, aufgeschlüsselt nach Jahr



Copyright © Dell Inc. All Rights Reserved.

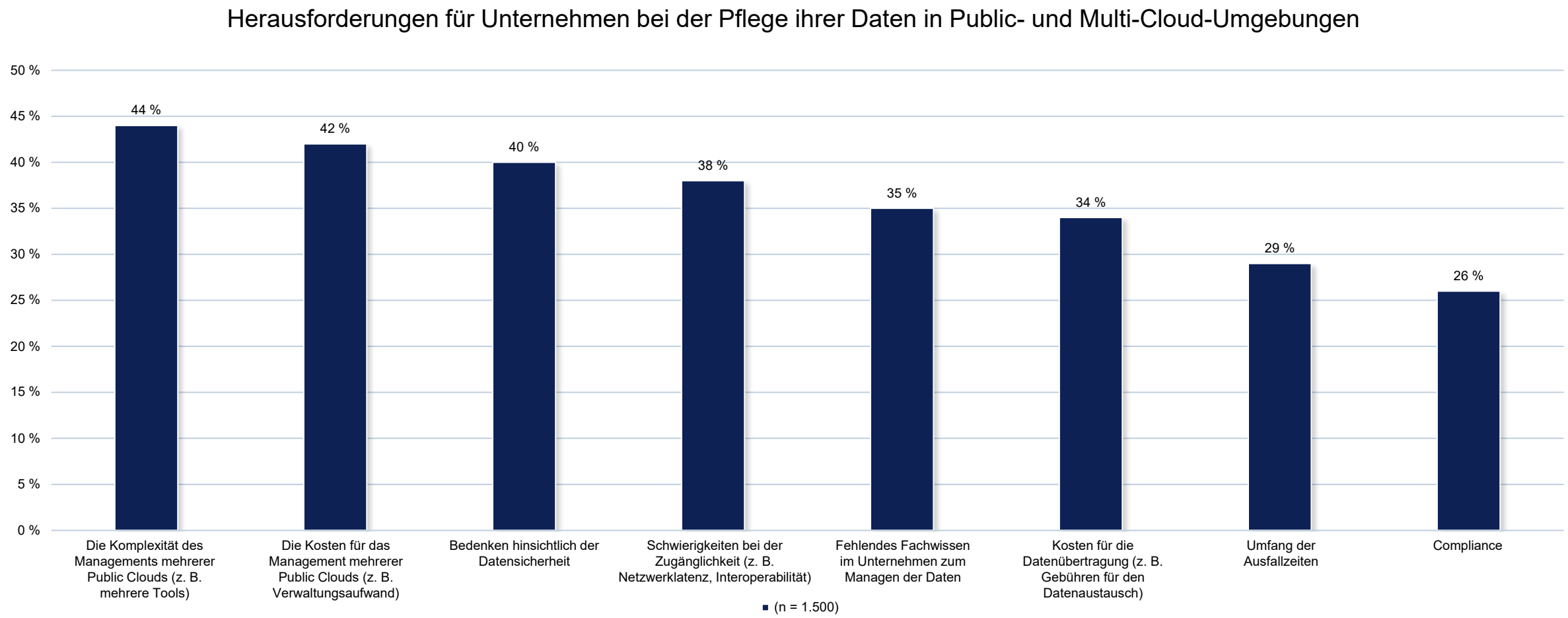
Auch die Public Cloud ist nach wie vor eine beliebte Wahl für die Bereitstellung neuer Anwendungen, aber der Support könnte abnehmen

Richtungen, die bei der Bereitstellung neuer Anwendungen eingeschlagen werden, aufgeschlüsselt nach Jahr



Copyright © Dell Inc. All Rights Reserved.

Trotz der Beliebtheit von Public Clouds stehen viele Unternehmen bei der Pflege ihrer Daten vor Herausforderungen

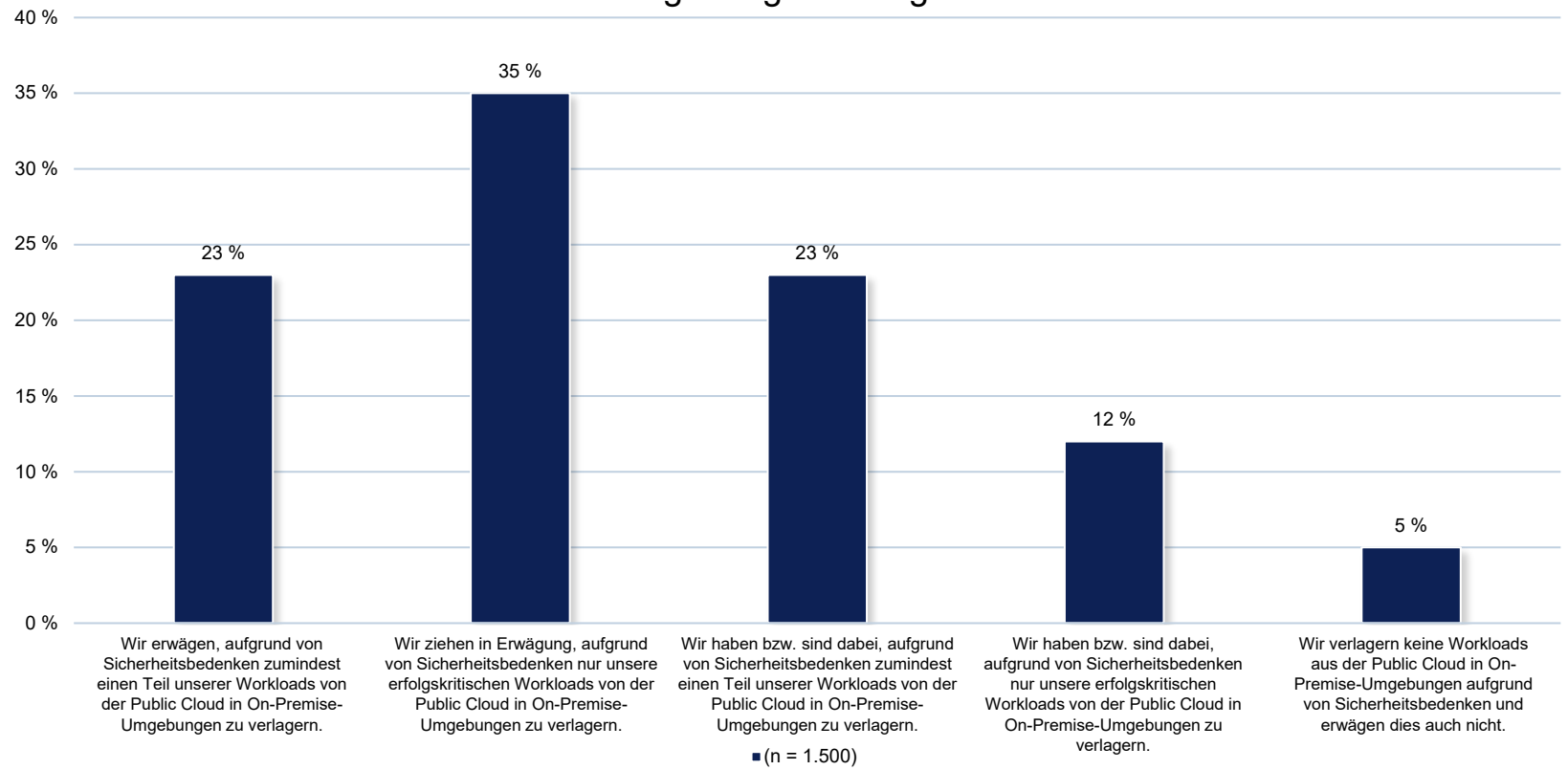


Filter: Datenteilung: Region = Gesamt

Copyright © Dell Inc. All Rights Reserved.

Aufgrund von Sicherheitsbedenken verlagern viele Unternehmen einen Teil ihrer Workloads von Public Clouds in On-Premise-Umgebungen oder ziehen dies in Betracht

Das Ausmaß, in dem Unternehmen Workloads aus der Public Cloud in On-Premise-Umgebungen verlagern



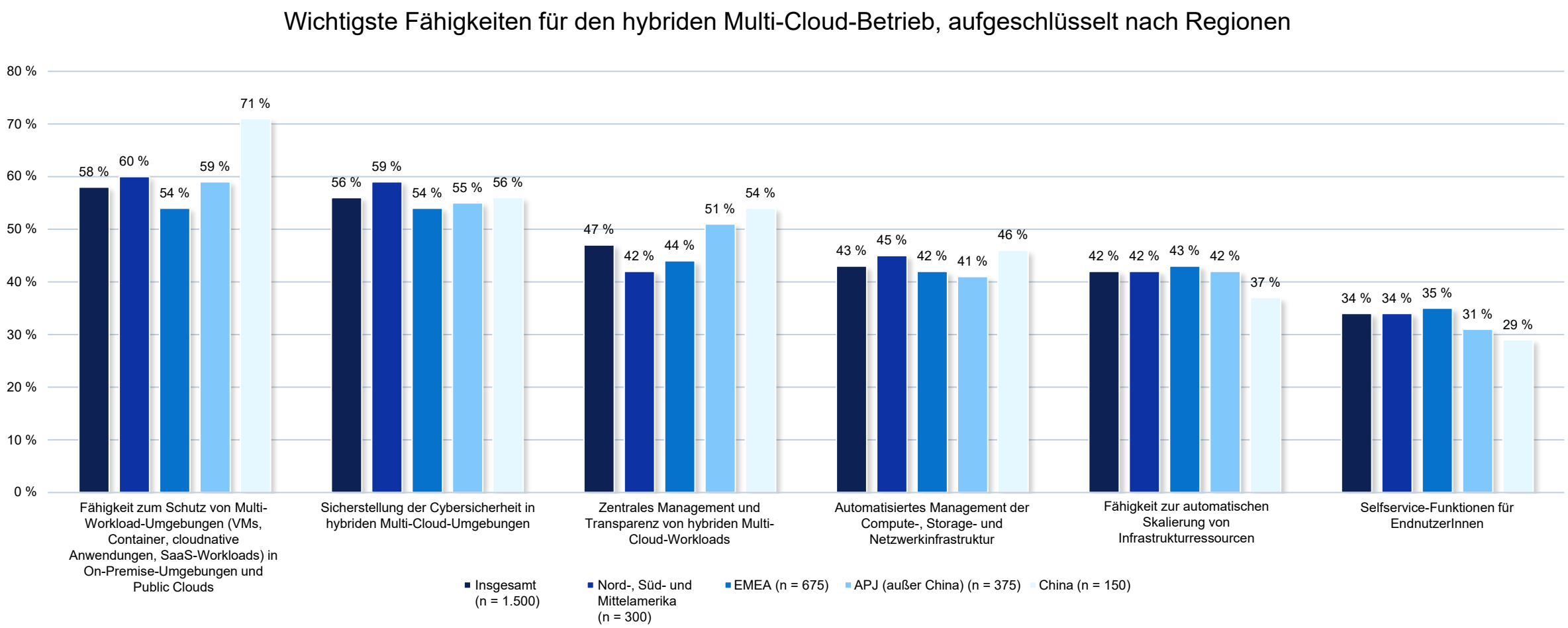
Filter: Datenteilung: Region = Gesamt

79 %

sind **nicht sehr zuversichtlich**, dass ihr **Unternehmen alle seine Daten** in Public-Cloud-Umgebungen schützen kann.

Copyright © Dell Inc. All Rights Reserved.

Angesichts der zunehmenden Zahl von Cyber-Incidents und des geringen Vertrauens in Data-Protection-Strategien sehen viele Unternehmen die Sicherheit als die wichtigste Voraussetzung für den hybriden Multi-Cloud-Betrieb an

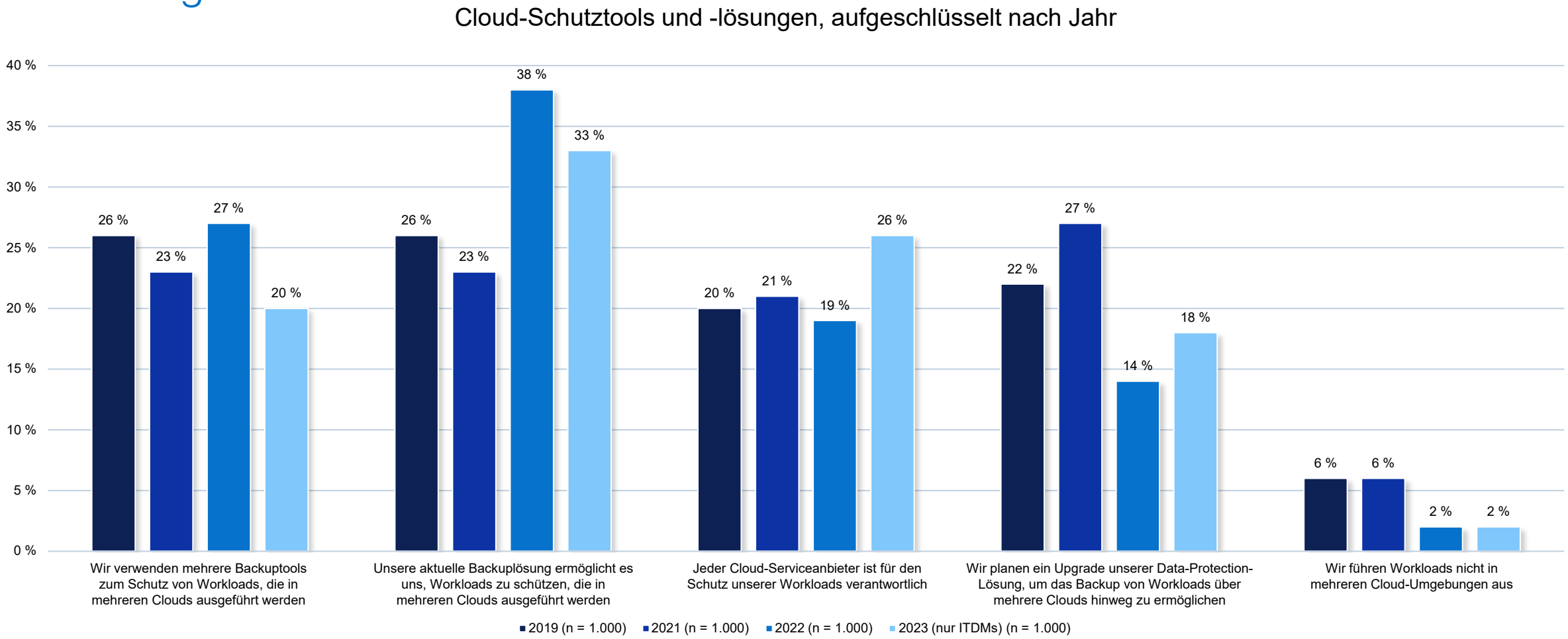


Copyright © Dell Inc. All Rights Reserved.

4. Sicherung einer Multi-Cloud-Umgebung

Copyright © Dell Inc. All Rights Reserved.

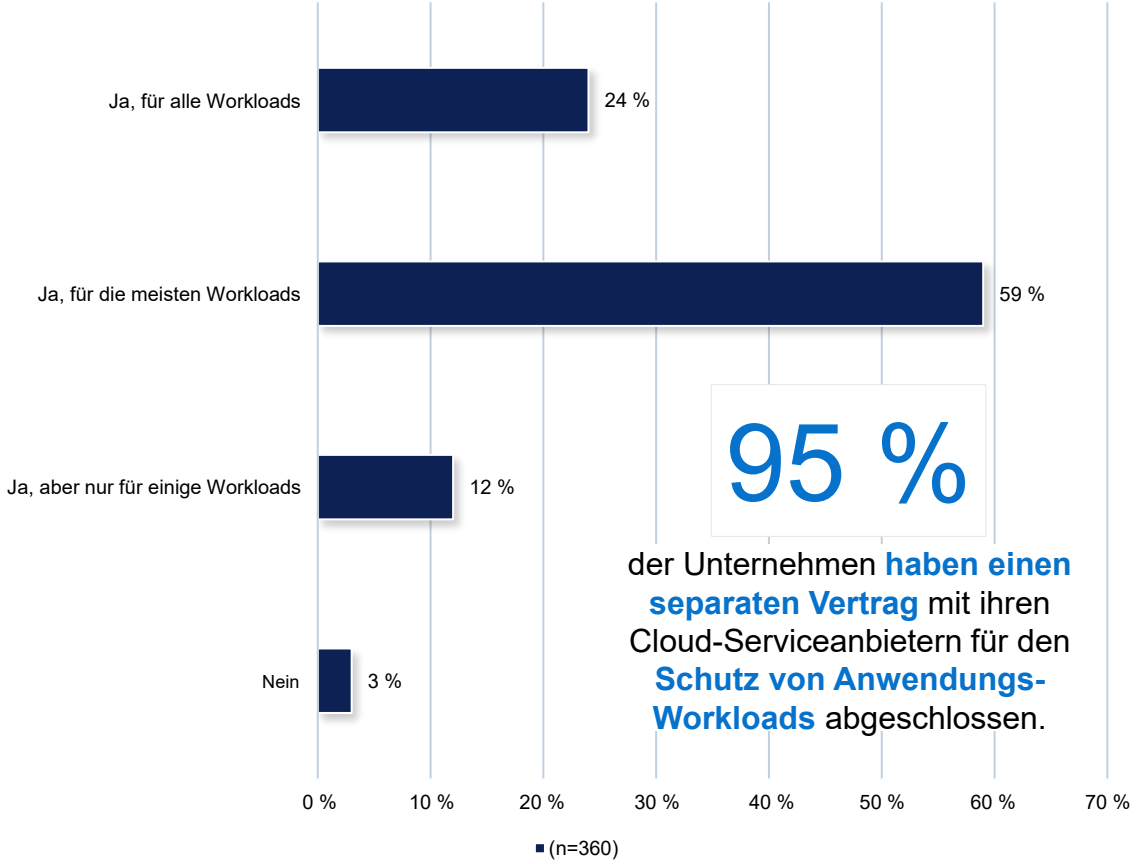
Unternehmen verwenden derzeit verschiedene Backup-Tools und -Lösungen, um ihre Workloads zu schützen, aber die Notwendigkeit von Upgrades wird zur Kenntnis genommen



Copyright © Dell Inc. All Rights Reserved.

Unternehmen verlassen sich zunehmend auf Cloud-Serviceanbieter, um ihre Workloads in Cloud-Umgebungen zu schützen

Separater Vertrag mit CSP für den Schutz von Anwendungs-Workloads

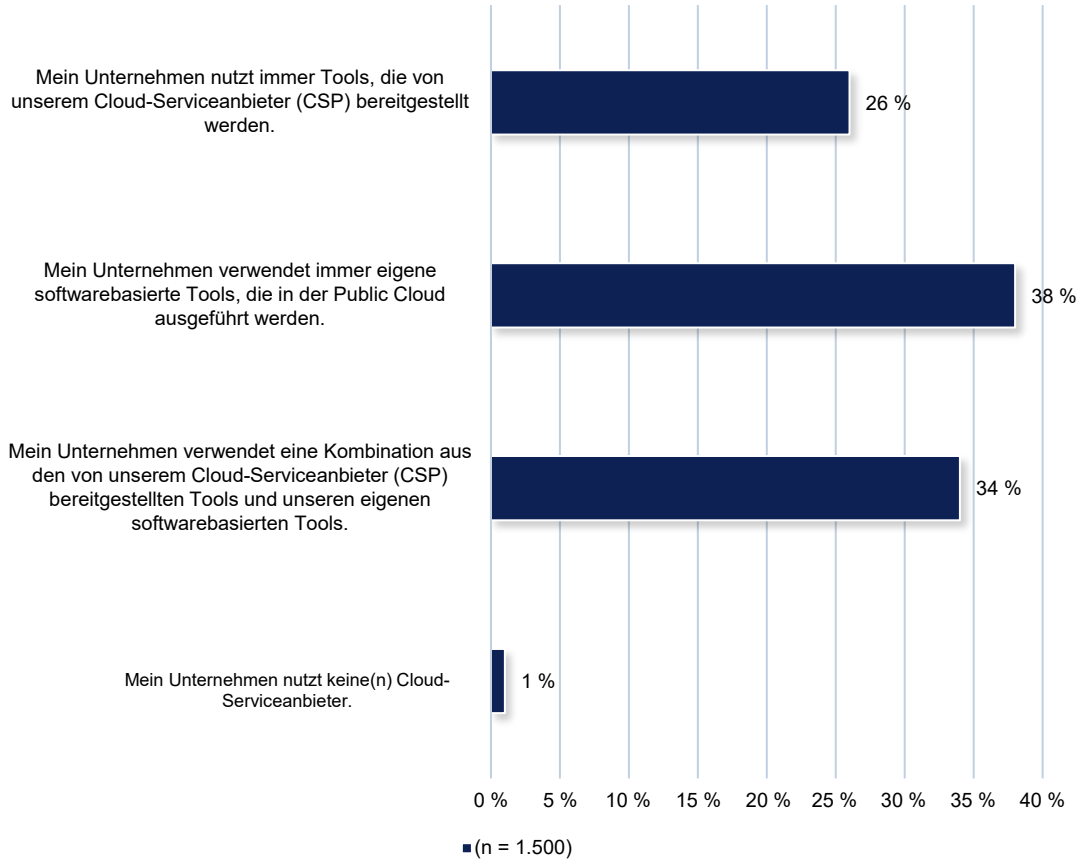


95 %

der Unternehmen **haben einen separaten Vertrag** mit ihren Cloud-Serviceanbietern für den **Schutz von Anwendungs-Workloads** abgeschlossen.

Filter: Datenteilung: Region = Gesamt

Vom Cloud-Serviceanbieter bereitgestellte Backup- und Recovery-Tools



Filter: Datenteilung: Region = Gesamt

Copyright © Dell Inc. All Rights Reserved.

Wichtigste Erkenntnisse – Zusammen-fassung

Die Data-Protection-Risikolandschaft

- Die Bedenken hinsichtlich der Data-Protection-Maßnahmen sind weit verbreitet und da das Vertrauen fehlt, befinden sich die Unternehmen in einer verwundbaren Position.
- Nahezu alle Unternehmen stehen vor Herausforderungen in Bezug auf ihre Data Protection, wobei viele Unternehmen in den letzten 12 Monaten erhebliche Unterbrechungen aufgrund von Datenverlusten und/oder ungeplanten Systemausfallzeiten erlitten haben.
- Externe Sicherheitsbedrohungen waren die häufigsten Ursachen für Datenverluste und/oder ungeplante Systemausfälle in den letzten 12 Monaten.
- Trotz der Herausforderungen und Bedenken in Bezug auf die Data Protection haben nur wenige Unternehmen Zero-Trust-Sicherheit vollständig umgesetzt.

Die zunehmende Bedrohung durch Cyberangriffe

- Die Zahl der Unternehmen, die in den letzten 12 Monaten von einem Cyberangriff oder -Incident betroffen waren, hat zugenommen und kostete die Unternehmen im Durchschnitt 1,92 Millionen USD.
- Viele Unternehmen sind besorgt, dass ihre Backupdaten durch Ransomwareangriffe infiziert oder beschädigt werden könnten.
- Das Risiko wird noch dadurch erhöht, dass ein falsches Vertrauen in die Folgen eines Ransomwareangriffs herrscht.
- Obwohl Ransomware-Versicherungspolicen weit verbreitet sind, werden sie nur unter strengen Auflagen abgeschlossen. Unternehmen sind dadurch finanziell gefährdet.

Die Nutzung von Multi-Cloud

- Die Public Cloud ist nach wie vor eine beliebte Wahl für die Aktualisierung bestehender und die Bereitstellung neuer Anwendungen, aber es gibt Bedenken hinsichtlich der Datensicherheit
- Aufgrund von Sicherheitsbedenken verlagern viele Unternehmen einen Teil ihrer Workloads von Public Clouds in On-Premise-Umgebungen oder ziehen dies in Betracht.
- Angesichts der zunehmenden Zahl von Cyber-Incidents und des geringen Vertrauens in Data-Protection-Strategien sehen viele Unternehmen die Sicherheit als die wichtigste Voraussetzung für den hybriden Multi-Cloud-Betrieb an.

Sicherung einer Multi-Cloud-Umgebung

- Unternehmen nutzen derzeit verschiedene Backuptools und -lösungen zum Schutz ihrer Workloads, räumen aber ein, dass Upgrades erforderlich sind.
- Unternehmen verlassen sich zunehmend auf Cloud-Serviceanbieter, um ihre Workloads in Cloud-Umgebungen zu schützen.

Copyright © Dell Inc. All Rights Reserved.