

# ARE YOU PROTECTED?

GET AHEAD OF THE CURVE

DELL EMC – GLOBAL DATA PROTECTION INDEX 2018

# Demographics

**INTERVIEWED  
2,200  
IT DECISION-  
MAKERS  
IN 3 REGIONS:**

INDEPENDENT RESEARCH AND  
ANALYSIS: VANSON BOURNE

**500**  
Americas

**1,100**  
Europe, Middle East,  
and Africa

**600**  
Asia Pacific  
Japan



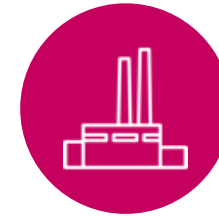
18 COUNTRIES



ORGS OF 250 OR  
MORE EMPLOYEES



BOTH PUBLIC AND  
PRIVATE ORGS

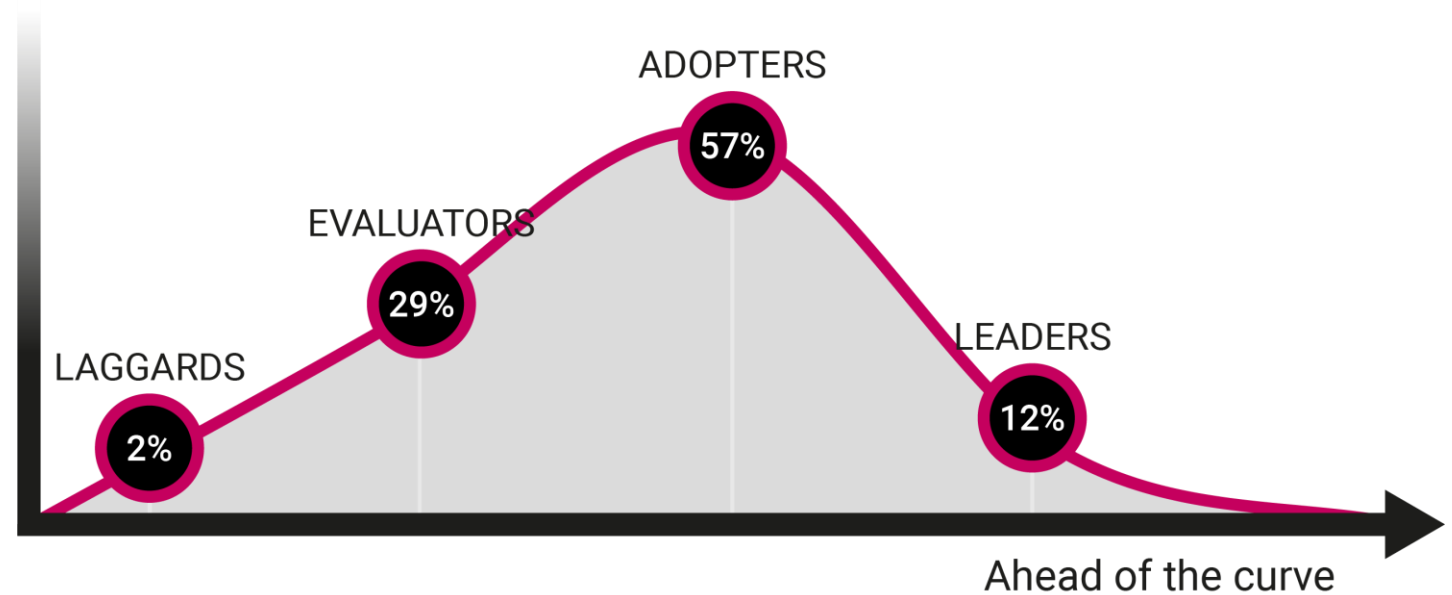


11 INDUSTRIES

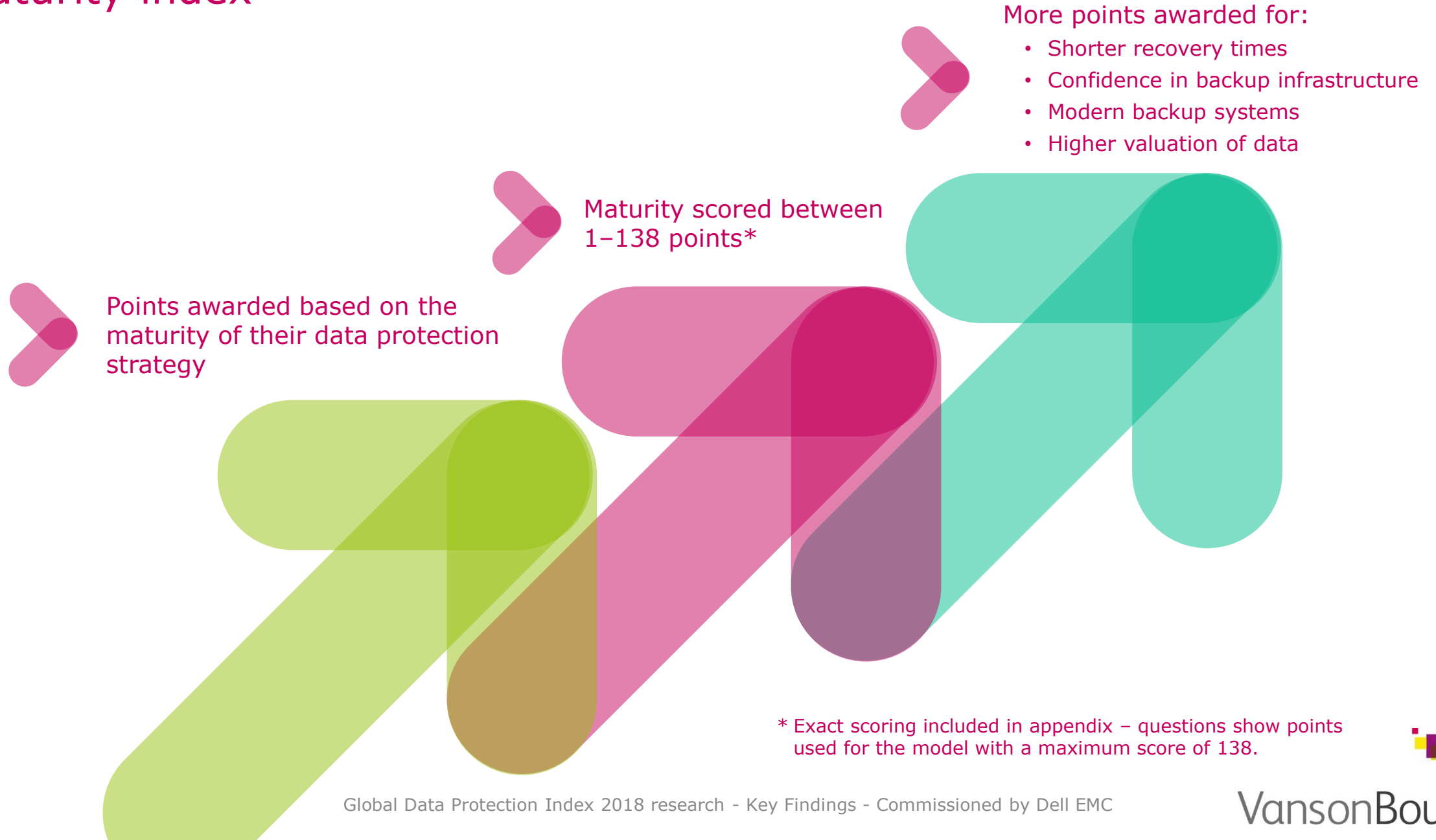
# MATURITY CURVE

# Data protection maturity curve 2018

AROUND  
**ONE IN TEN**  
ORGANIZATIONS ARE  
CONSIDERED TO BE  
DATA PROTECTION  
LEADERS IN 2018  
  
(COMPARED TO 2% IN 2016)



# Maturity index



# Profile characteristics

The profile characteristics for each of the following maturity groups tend to be...

## Laggards



- Place little or no value on data
- Have DP solutions that will not meet future challenges
- No consideration of public cloud for DP
- Recovery times often over 12 hours
- Little or no confidence in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

## Evaluators



- See the potential value of data
- Have DP solutions that will meet a minority of future challenges
- Minimal use of public cloud for DP
- Recovery times 3-9 hours
- Several doubts in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

## Adopters



- Starting to invest in tools to monetize data
- Have DP solutions that will meet most future challenges
- Use of public cloud for DP
- Recovery times 2-6 hours
- Moderate confidence in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

## Leaders



- Place a very high value on data (data = capital)
- Have DP solutions that will meet all or most future challenges
- Advanced use of public cloud for DP
- Recovery times under 2 hours
- Highly confident in terms of DP compliance, meeting SLOs, and recovering data in the event of data loss

## Maturity rank by country

Rank	Country	Percentage of Leaders in 2018	Difference (vs. 2016 ranking)
#1	India	30%	Up 8
#2	Mainland China	27%	Down 1
#3	Brazil	23%	Down 2
#4	Italy	20%	Up 11
#5	Japan	18%	Up 10
#6	US	16%	Up 3
#7	Mexico	15%	Down 1
#8	Netherlands	13%	Up 7
#9	South Africa	12%	(-)

Rank	Country	Percentage of Leaders in 2018	Difference (vs. 2016 ranking)
#10	Switzerland	12%	(-)
#11	Canada	10%	Down 2
#12	UK	9%	Down 6
#13	Singapore	9%	Down 11
#14	UAE	8%	Up 1
#15	Germany	7%	Down 10
#16	Australia	5%	Down 10
#17	France	3%	Down 16
#18	South Korea	1%	Down 9

## FOCUS OF KEY FINDINGS:

- 1: The value of data
- 2: Data protection solutions currently in place
- 3: Challenges surrounding data protection
- 4: Public cloud – changing the data protection landscape
- 5: Disruption experience



# THE VALUE OF DATA

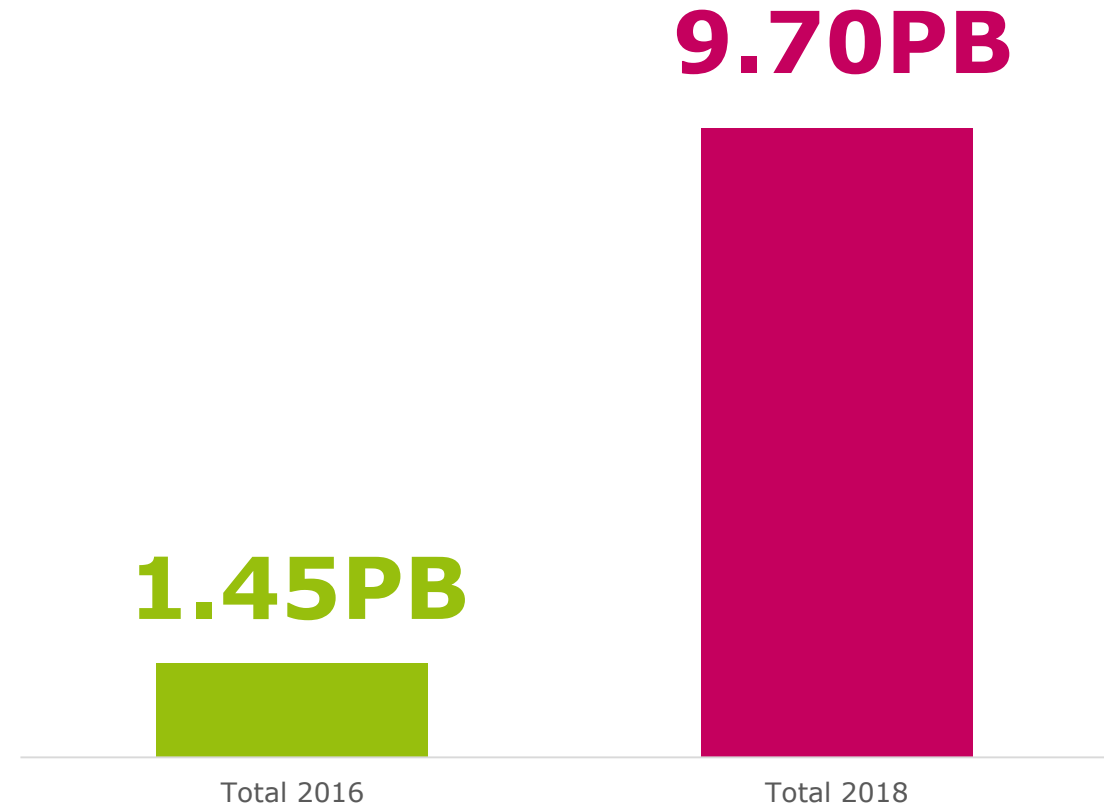
# The ever-increasing volume of data

MANAGE ON AVERAGE

**9.70PB**

OF DATA IN 2018

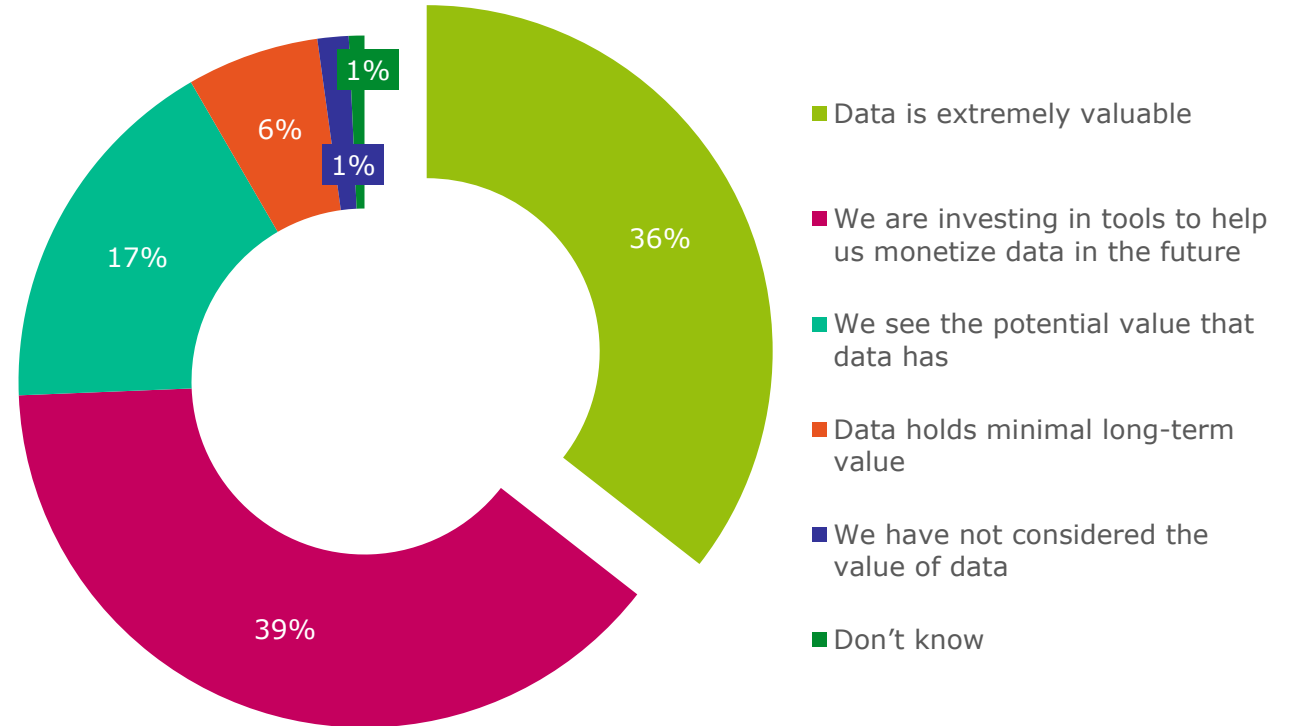
IN 2016 IT WAS 1.45PB  
(A GROWTH OF 569%)



# The value of data

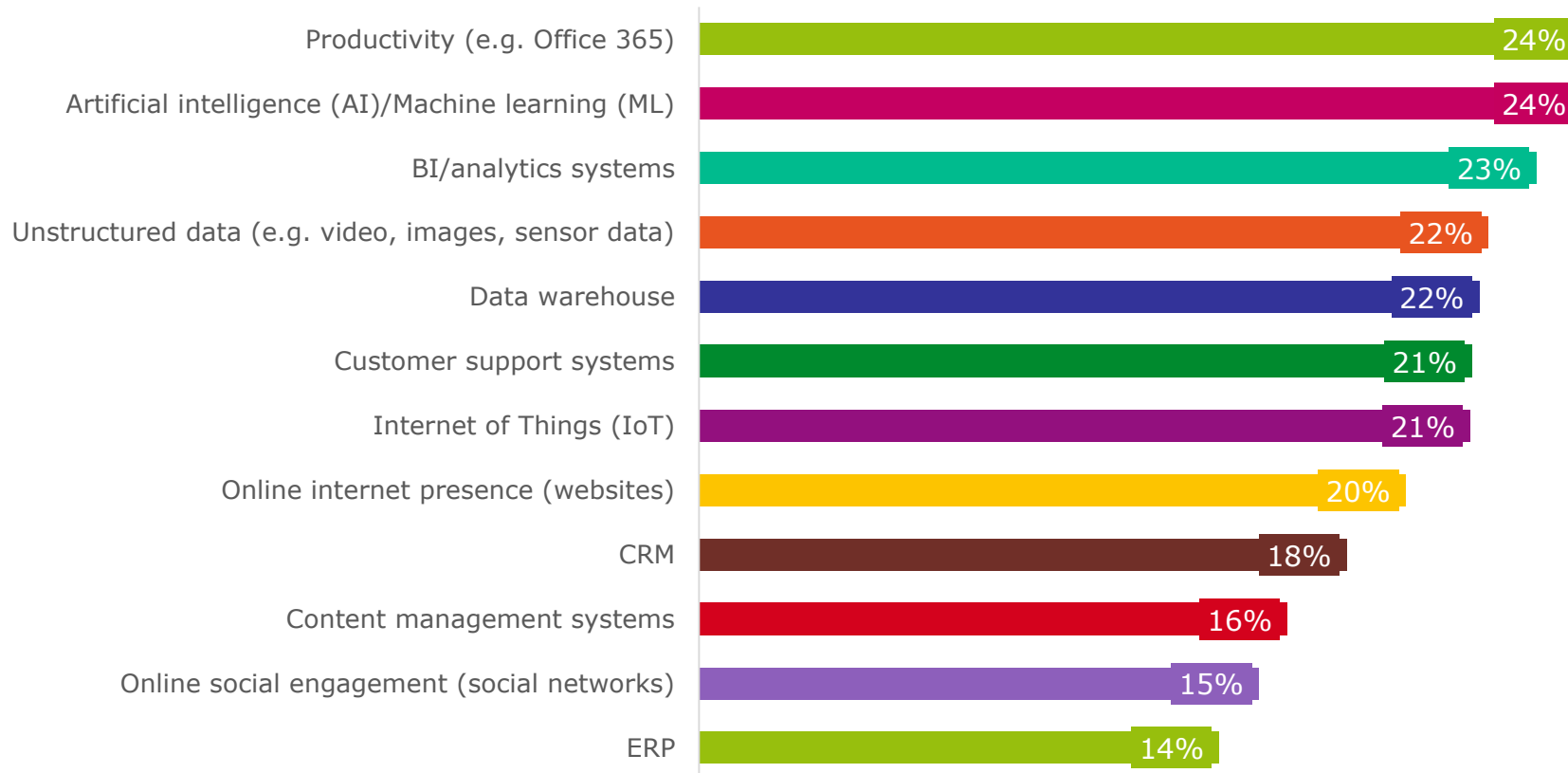
**92%**  
SEE THE POTENTIAL VALUE  
OF DATA

**36%** CONSIDER DATA  
TO BE EXTREMELY VALUABLE



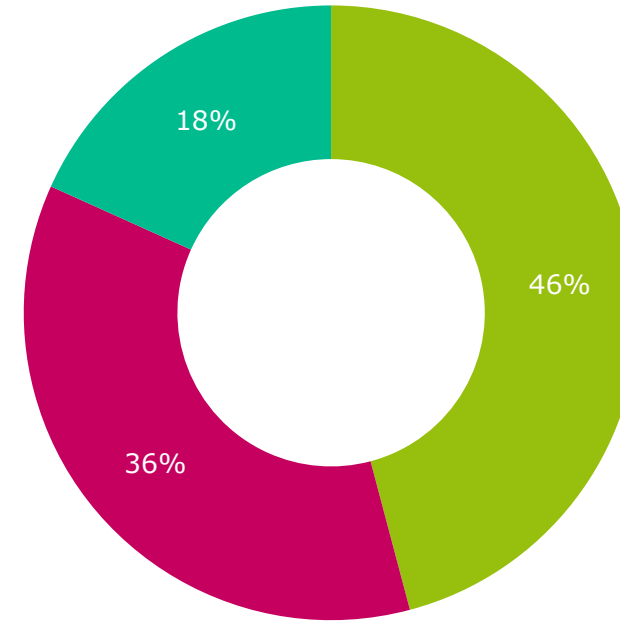
# The most valuable sources of data

## PRODUCTIVITY APPS AND AI/ML CONSIDERED TWO OF THE MOST VALUABLE SOURCES OF DATA



# Treating data protection differently for different data sources

**81%**  
TAKE DATA PROTECTION  
MORE SERIOUSLY FOR  
'MORE VALUABLE' DATA

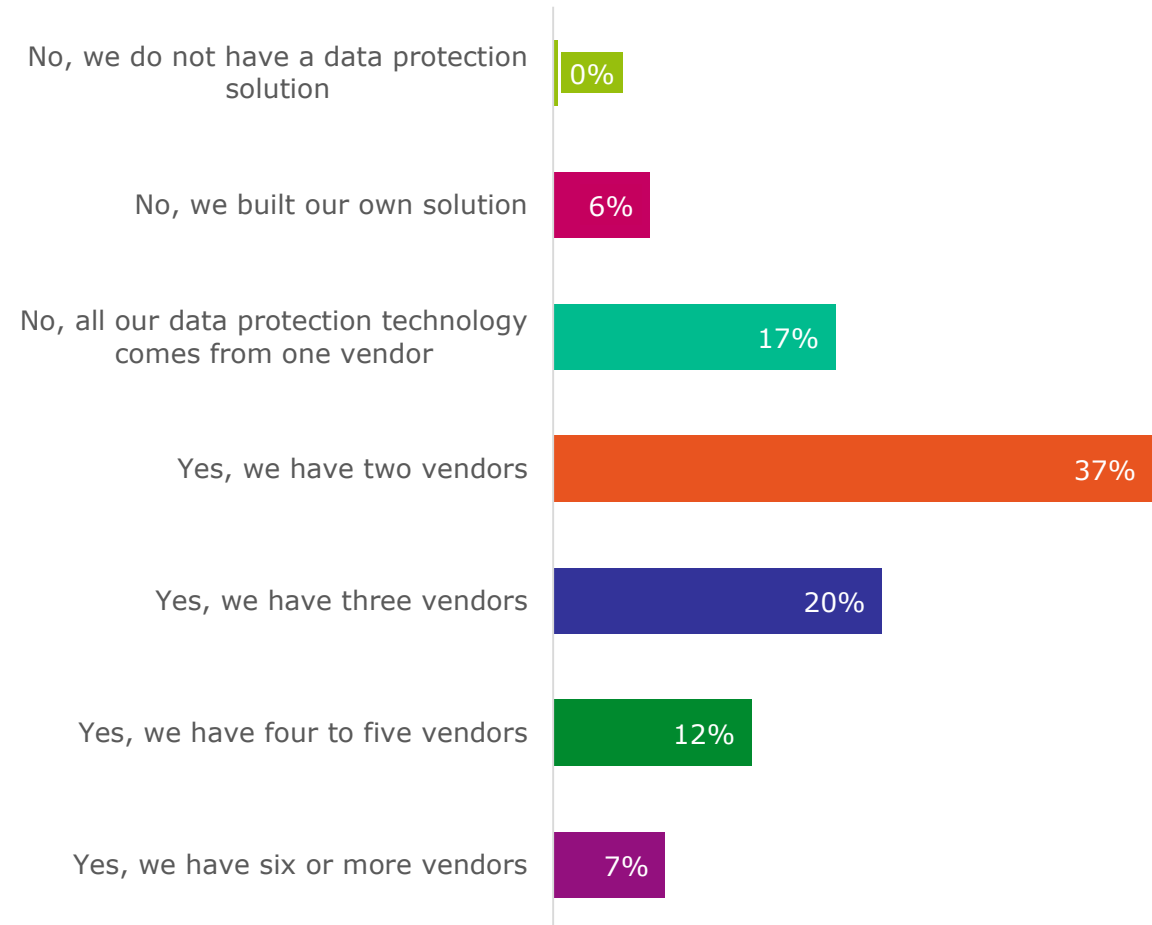


- We take data protection much more seriously for the data that has the greatest monetary value
- We take data protection slightly more seriously for the data that has the greatest monetary value
- We treat all protection of data equally, regardless of the value of the data

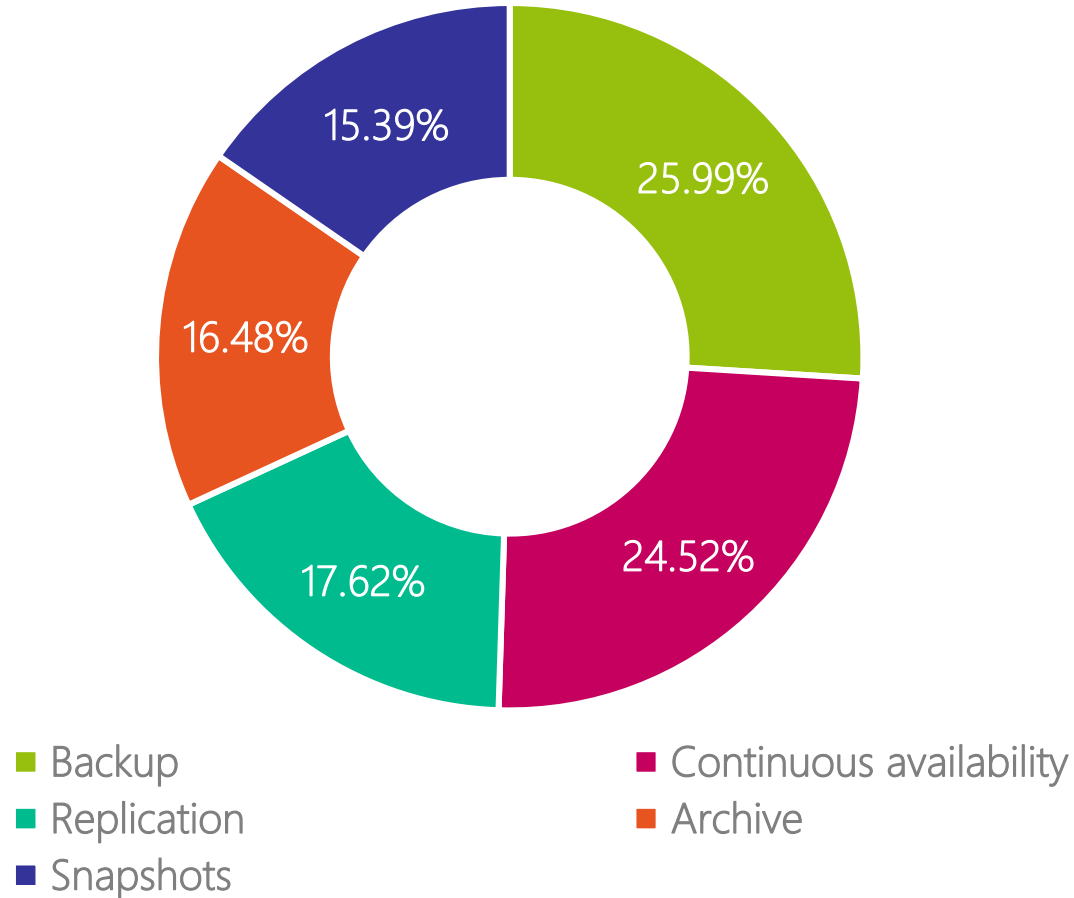
# DATA PROTECTION SOLUTIONS CURRENTLY IN PLACE

# Vendors used for data protection infrastructure

**76%**  
**USE AT LEAST TWO DATA  
PROTECTION VENDORS**



# Data protection solutions used

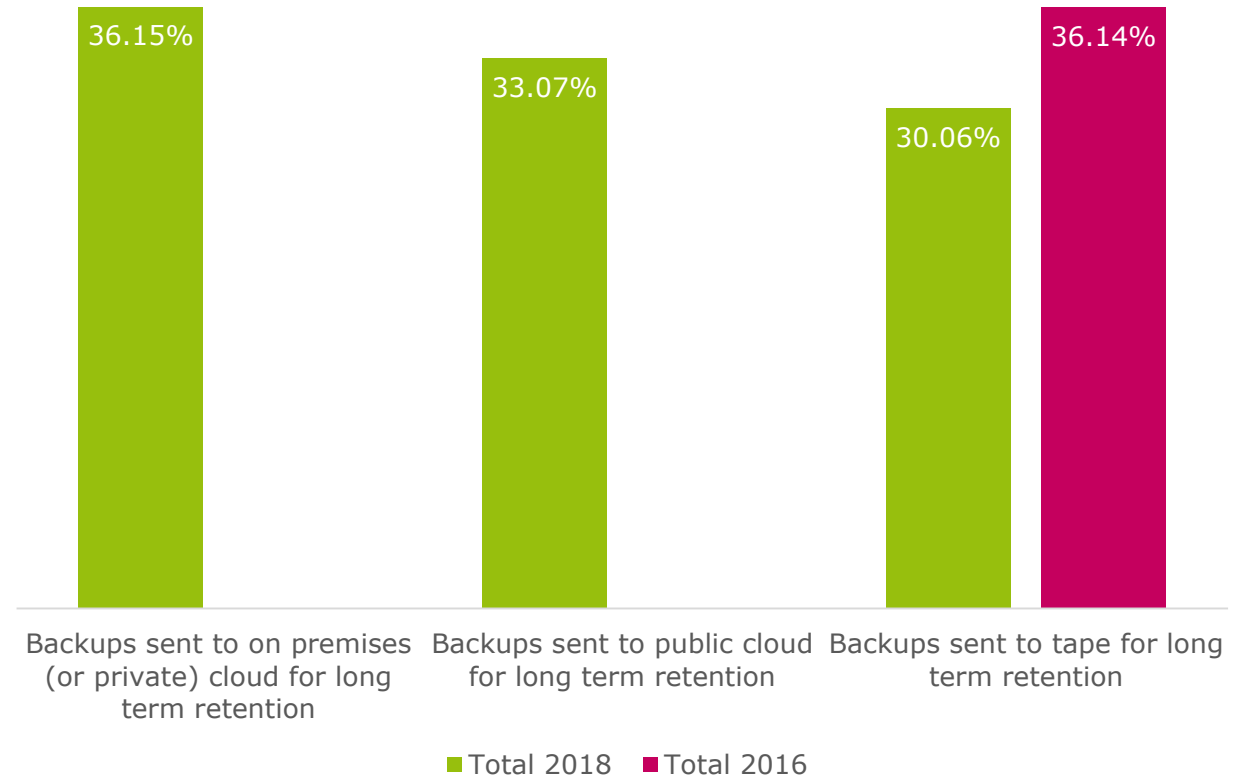


IN MOST CASES, ORGANIZATIONS ARE USING A NUMBER OF DIFFERENT SOLUTIONS – AND LIKELY DIFFERENT VENDORS – SIMULTANEOUSLY



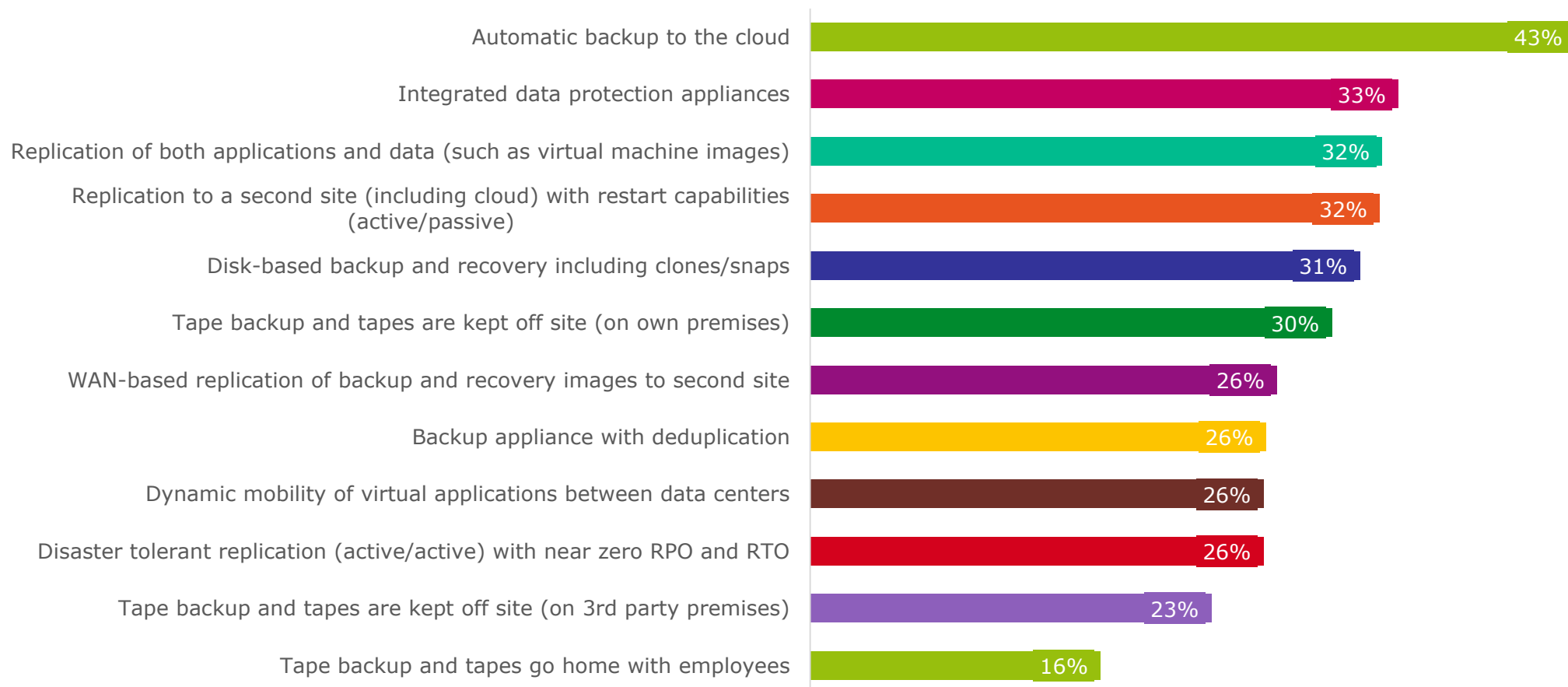
# Backup preferences for long-term retention

PRIVATE CLOUD IS NOW THE MOST POPULAR FOR LONG-TERM RETENTION BUT **30%** ARE STILL USING TAPE



# Technology currently used in availability strategies

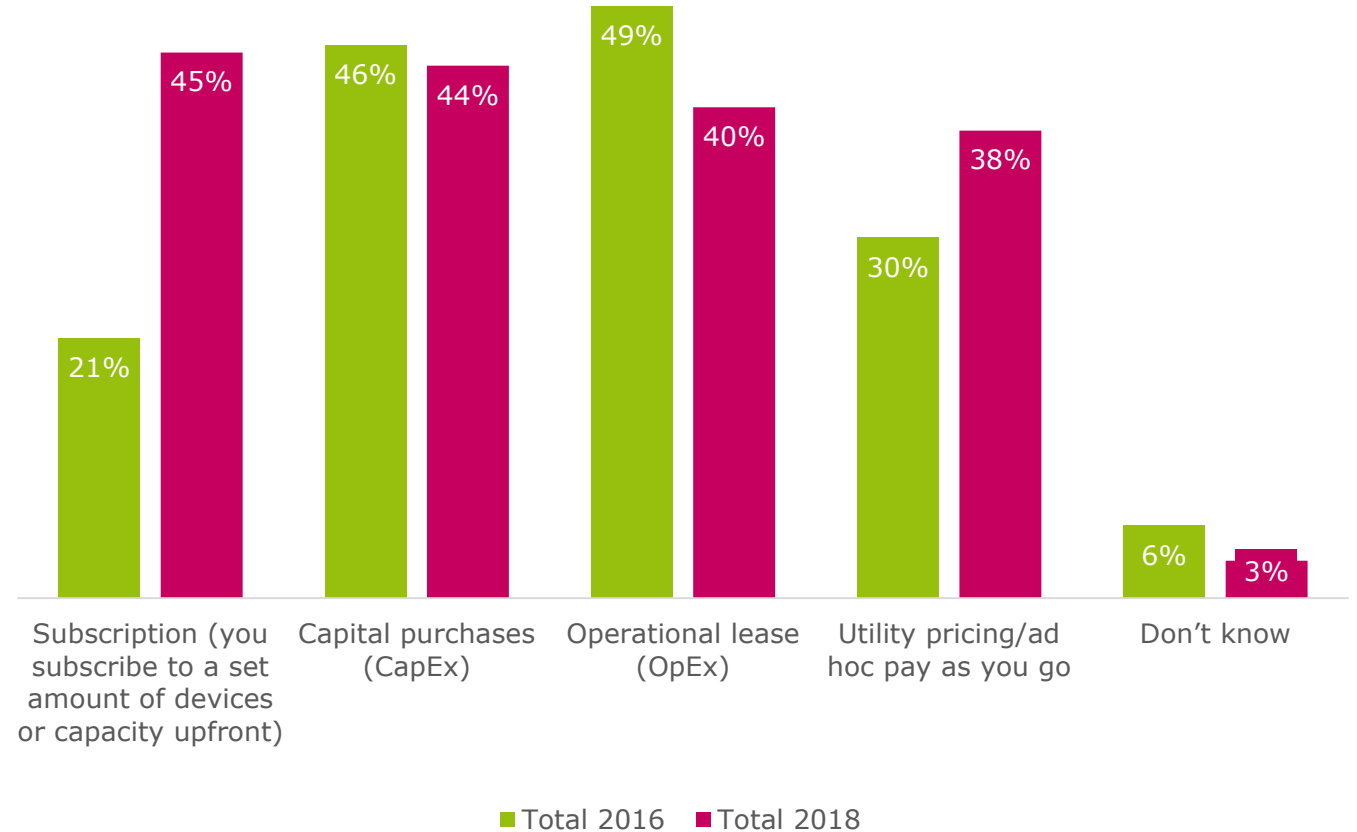
## AUTOMATIC BACKUP TO CLOUD IS THE TECHNOLOGY MOST FREQUENTLY INCLUDED AS PART OF AVAILABILITY STRATEGIES FOR MISSION-CRITICAL WORKLOADS



# Consumption of data protection

CONSUMPTION OF DATA PROTECTION IS CHANGING

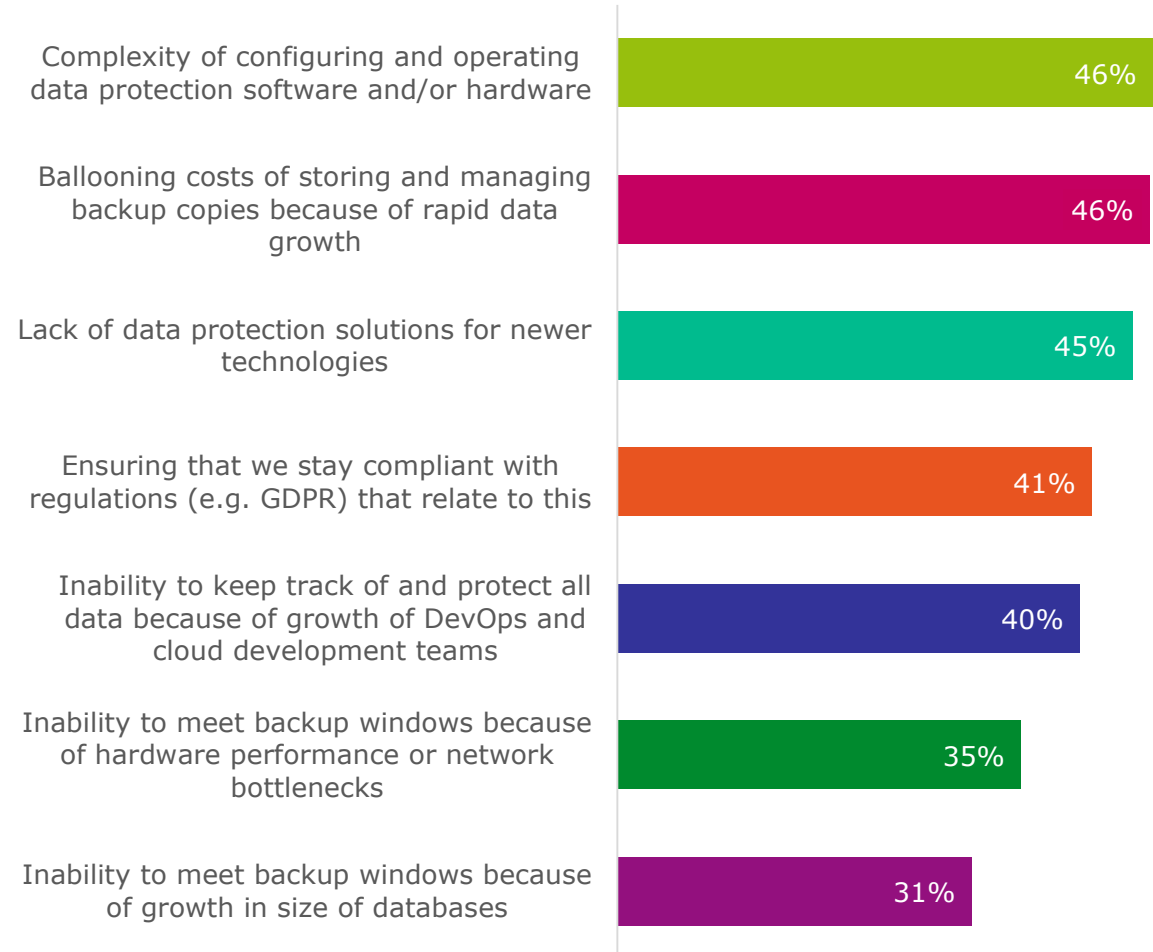
SUBSCRIPTION MODELS ARE NOW THE MOST POPULAR METHOD OF CONSUMPTION - MORE POPULAR THAN CAPEX AND OPEX



# CHALLENGES SURROUNDING DATA PROTECTION

# Data protection challenges

**95%** OF RESPONDENTS' ORGANIZATIONS ARE FACING AT LEAST ONE CHALLENGE IN RELATION TO DATA PROTECTION



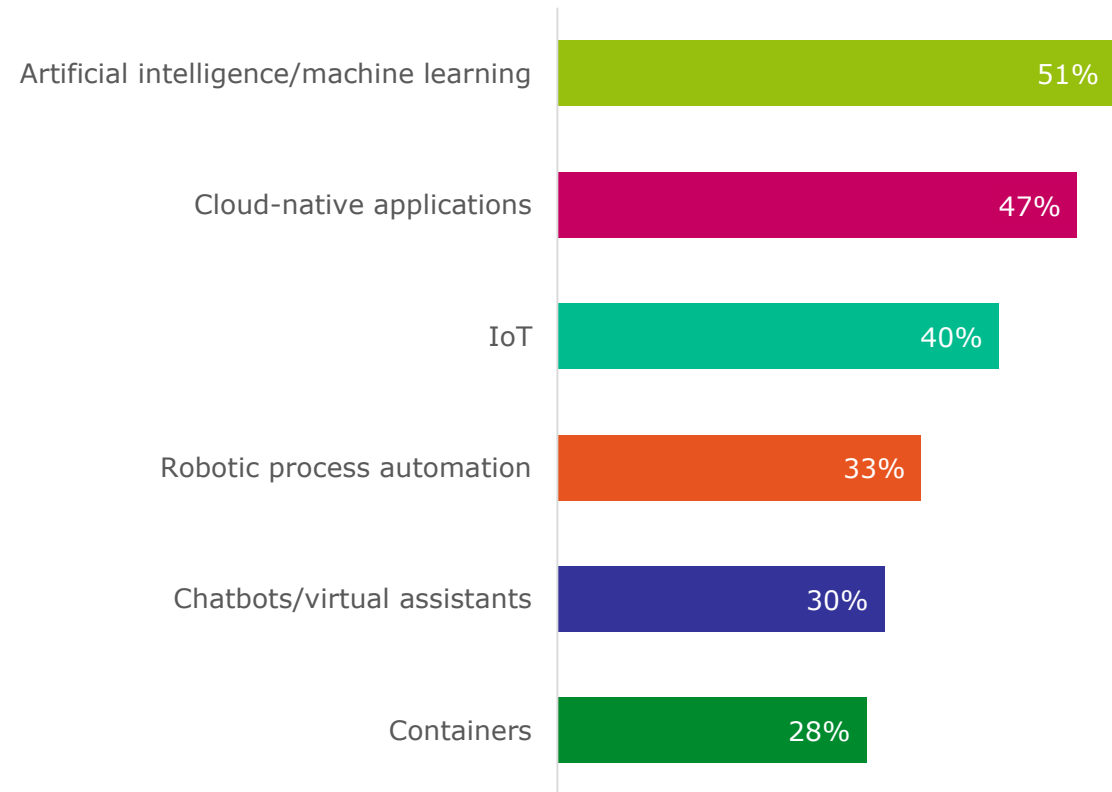
# Lack of data protection solutions for newer technology

FOR THOSE WHO ARE STRUGGLING TO FIND SOLUTIONS FOR NEWER TECHNOLOGIES...

**51%**

CANNOT FIND SUITABLE  
DATA PROTECTION  
SOLUTIONS FOR AI/ML

## WE CAN'T FIND DATA PROTECTION SOLUTIONS FOR...



# Confidence in current data protection solutions

ONLY  
**37%**

ARE VERY CONFIDENT  
THAT THEIR  
ORGANIZATION IS  
**MEETING ITS  
BACKUP AND  
RECOVERY SLOS**



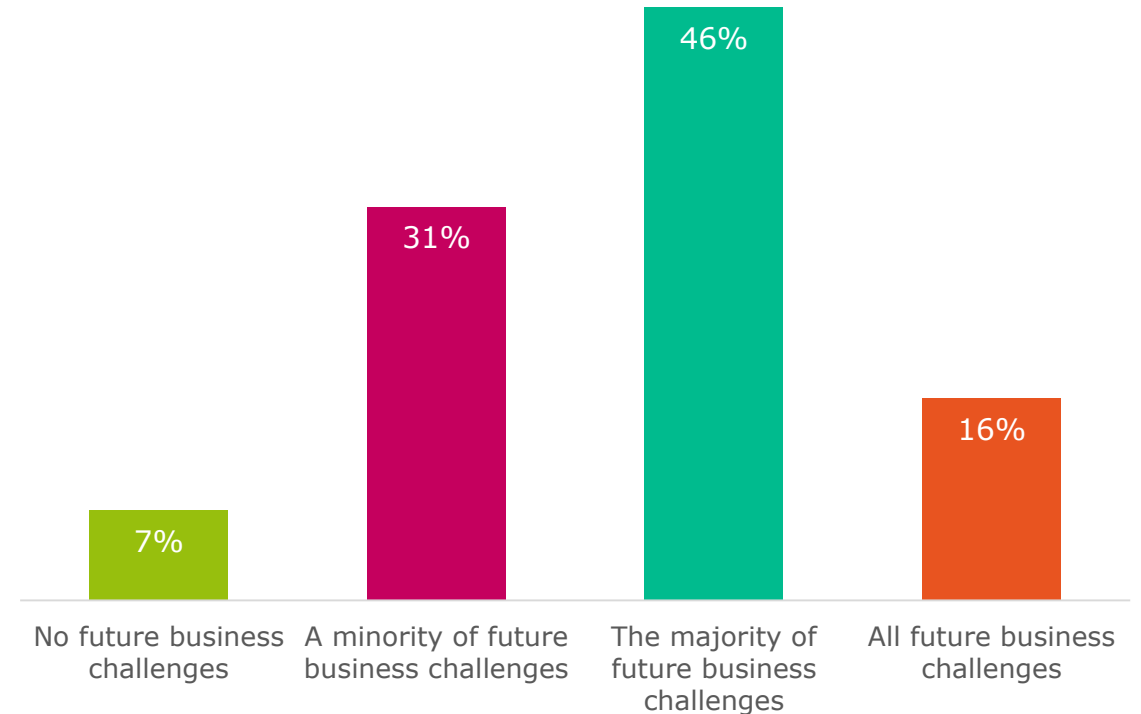
AND ONLY  
**35%**

ARE VERY CONFIDENT  
THAT THEIR DATA  
PROTECTION  
INFRASTRUCTURE IS  
**COMPLIANT WITH  
REGULATIONS**

# Meeting future business challenges

ONLY  
**16%**  
BELIEVE THAT THEIR  
CURRENT DATA PROTECTION  
SOLUTIONS WILL BE ABLE TO  
MEET **ALL** FUTURE BUSINESS  
CHALLENGES

OUR CURRENT DATA  
PROTECTION SOLUTIONS WILL  
BE ABLE TO MEET...



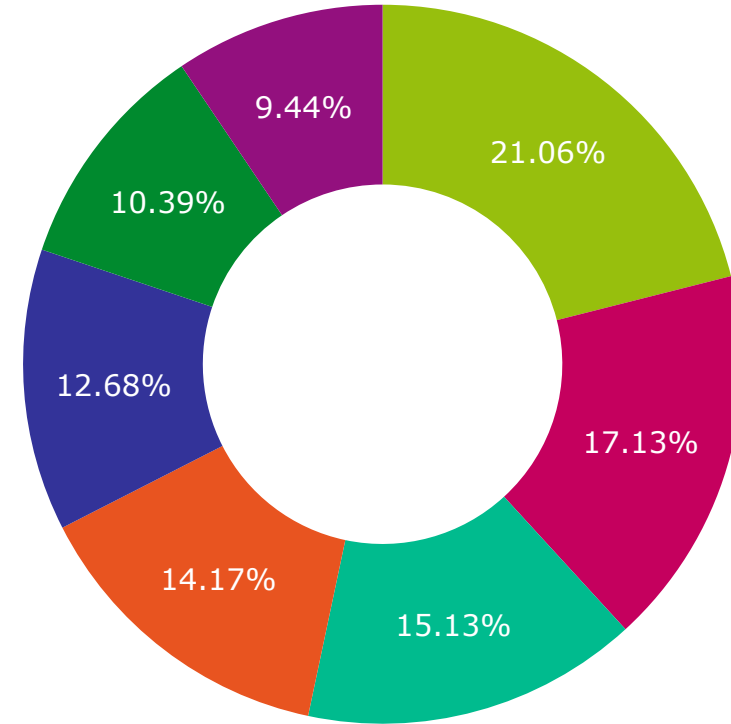


# PUBLIC CLOUD – CHANGING THE DATA PROTECTION LANDSCAPE

# The IT environment in 2018

PUBLIC CLOUD USE HAS INCREASED FROM 28% IN 2016 TO **40%** IN 2018

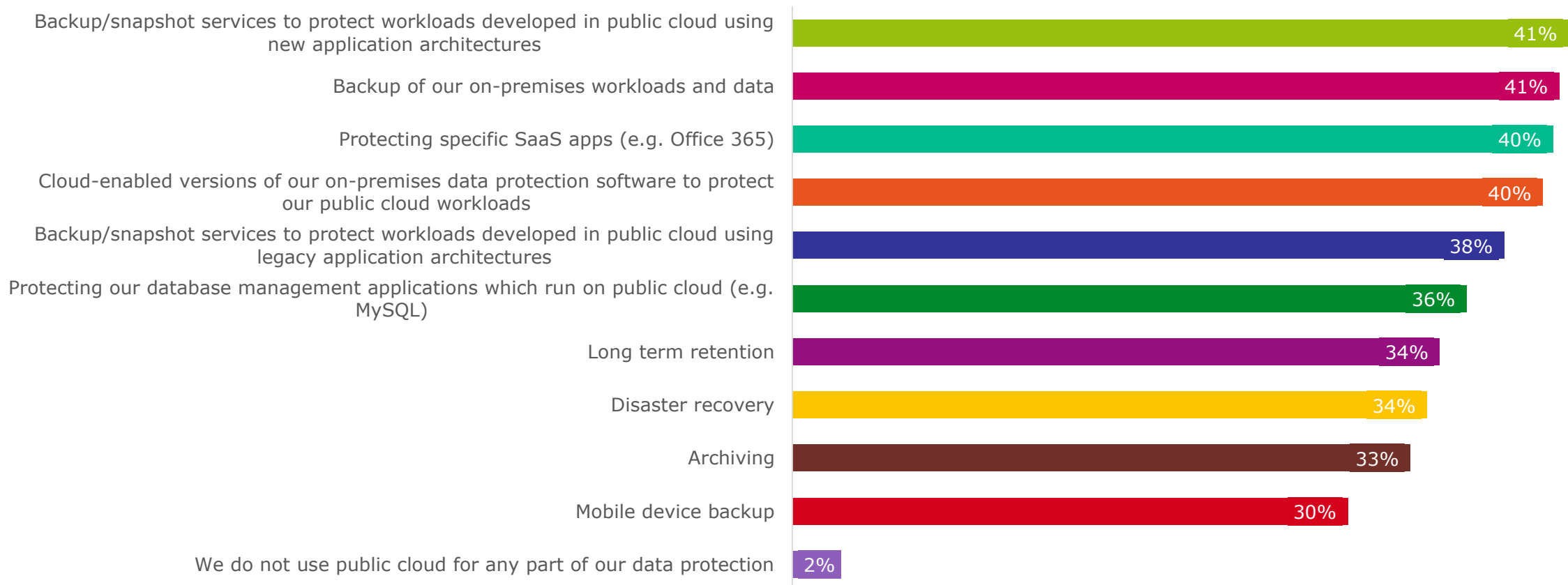
ON-PREMISES SOLUTIONS HAVE SHRUNK FROM 56% IN 2016 TO 38%



- On-premises physical servers
- On-premises virtualized servers
- Public cloud (IaaS) (e.g. Amazon)
- Public cloud (SaaS) (e.g. Salesforce.com, Office 365)
- Private cloud (IT-as-a-Service, e.g. vRealize platform)
- Public cloud (PaaS/containers)
- Managed service provider (MSP)

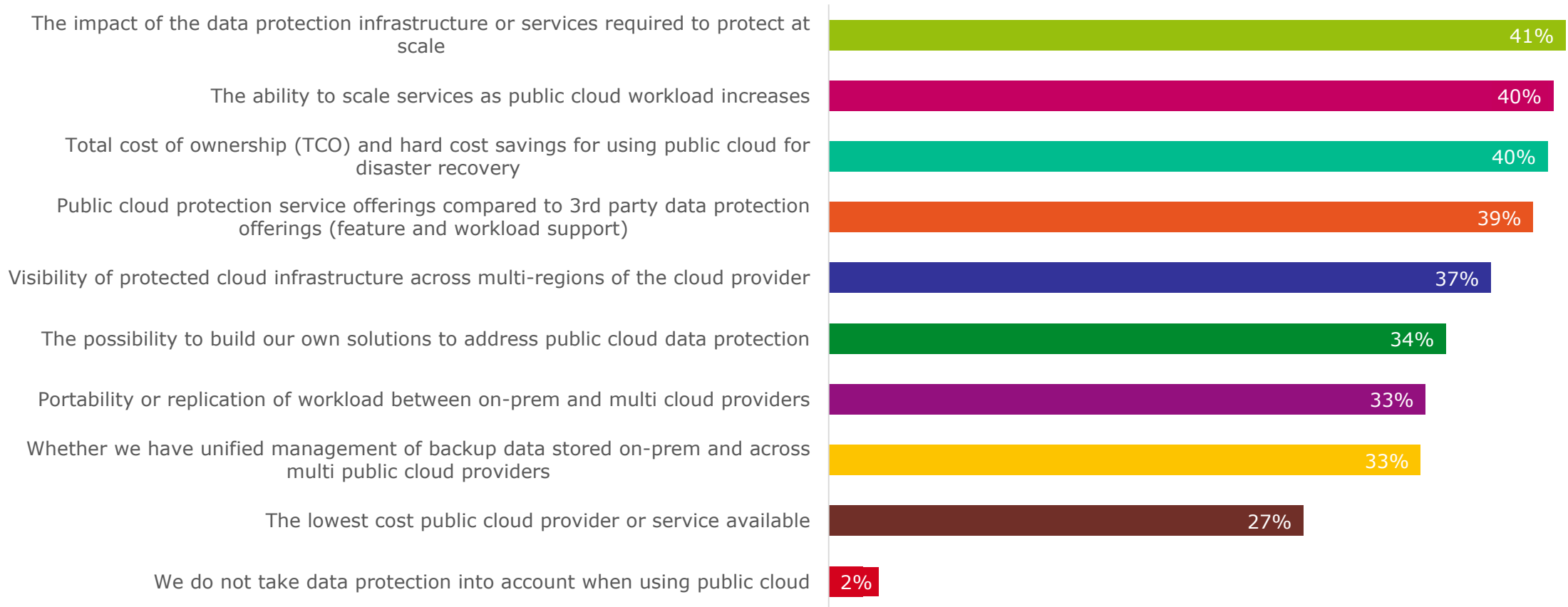
# Using public cloud for data protection

**98%** OF THOSE WHOSE ORGANIZATION USES PUBLIC CLOUD REPORT THAT IT FEATURES AS PART OF THEIR DATA PROTECTION INFRASTRUCTURE



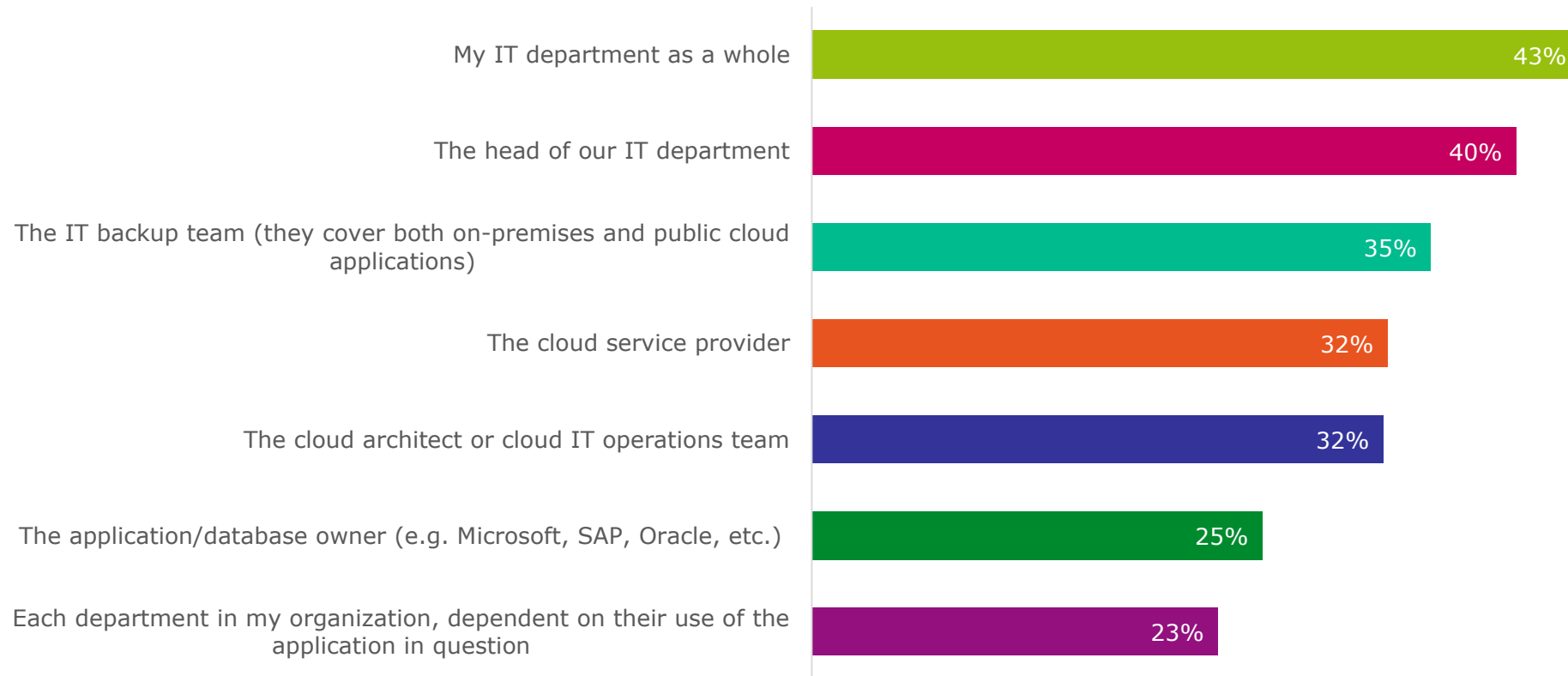
# Data protection considerations in the public cloud

## REQUIREMENTS VARY BY ORGANIZATION WHEN LOOKING AT DATA PROTECTION SOLUTIONS IN A PUBLIC CLOUD ENVIRONMENT



# Responsibility for public cloud-based applications

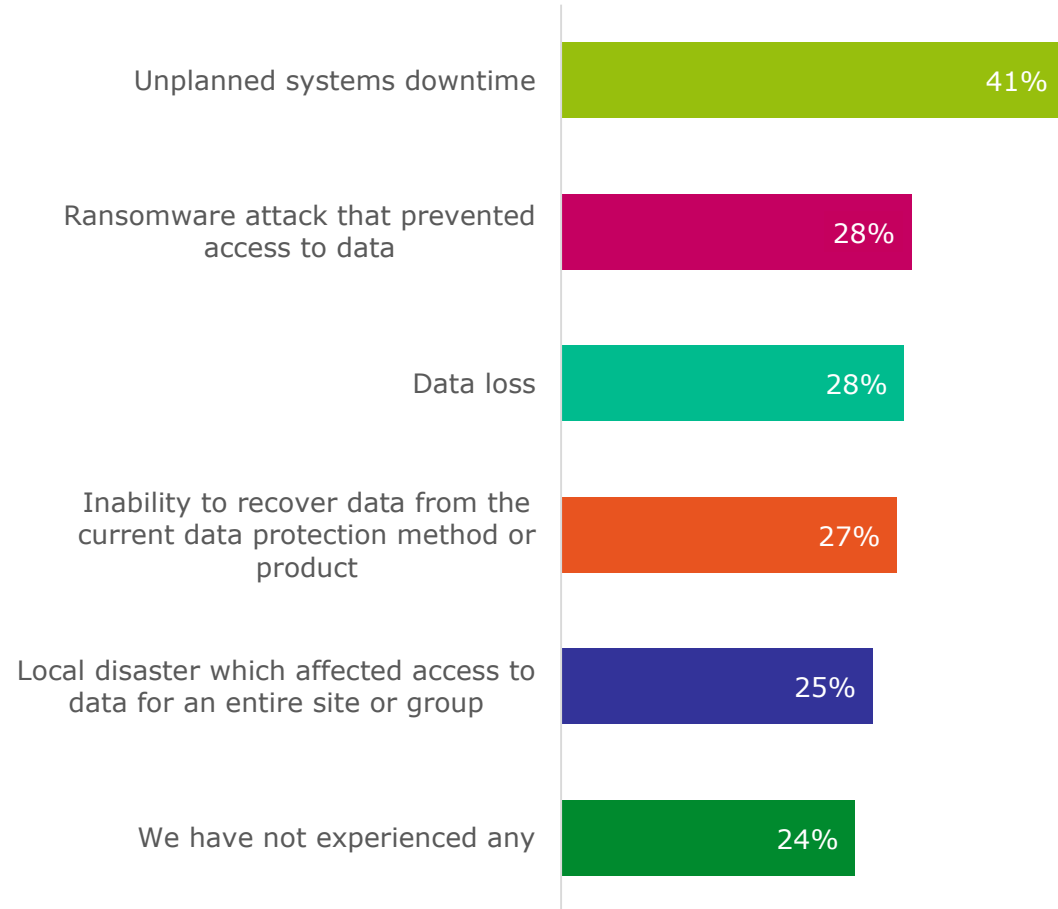
## THE IT DEPARTMENT AS A WHOLE IS MOST LIKELY TO BE RESPONSIBLE FOR DATA PROTECTION OF PUBLIC CLOUD-BASED APPLICATIONS



# DISRUPTION EXPERIENCE

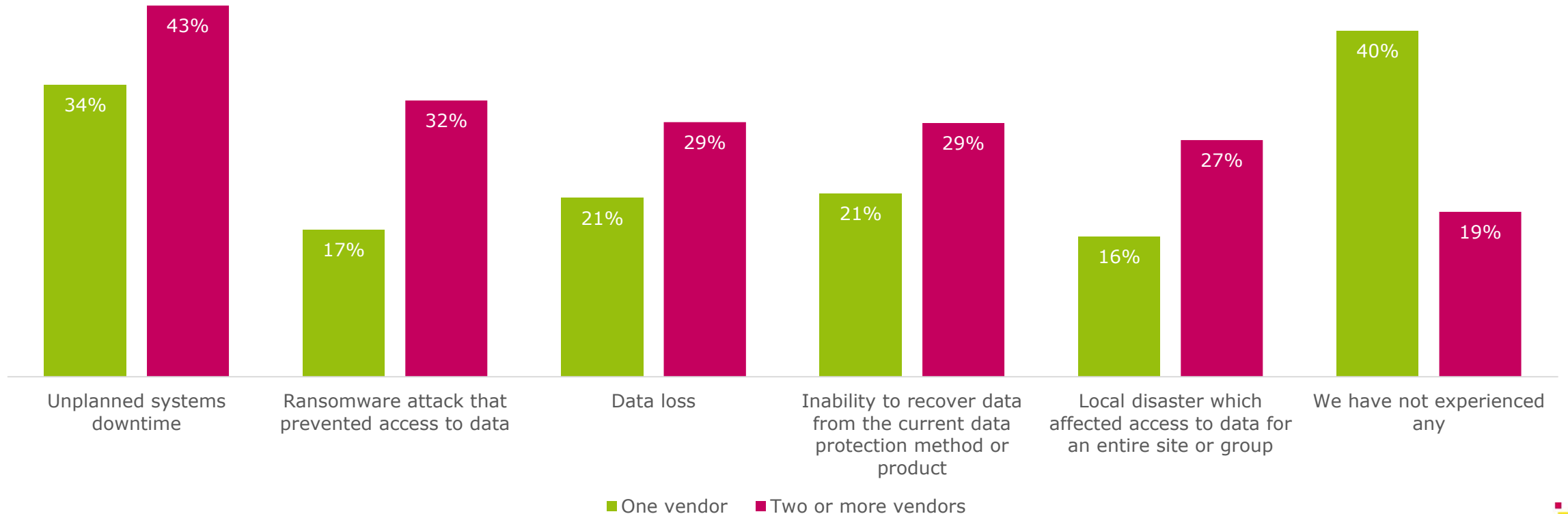
# Disruption experiences in the last 12 months

**76%**  
OF RESPONDENTS'  
ORGANIZATIONS HAVE  
EXPERIENCED DISRUPTION  
OF SOME KIND IN THE LAST  
12 MONTHS



# The impact of multiple vendors on disruption

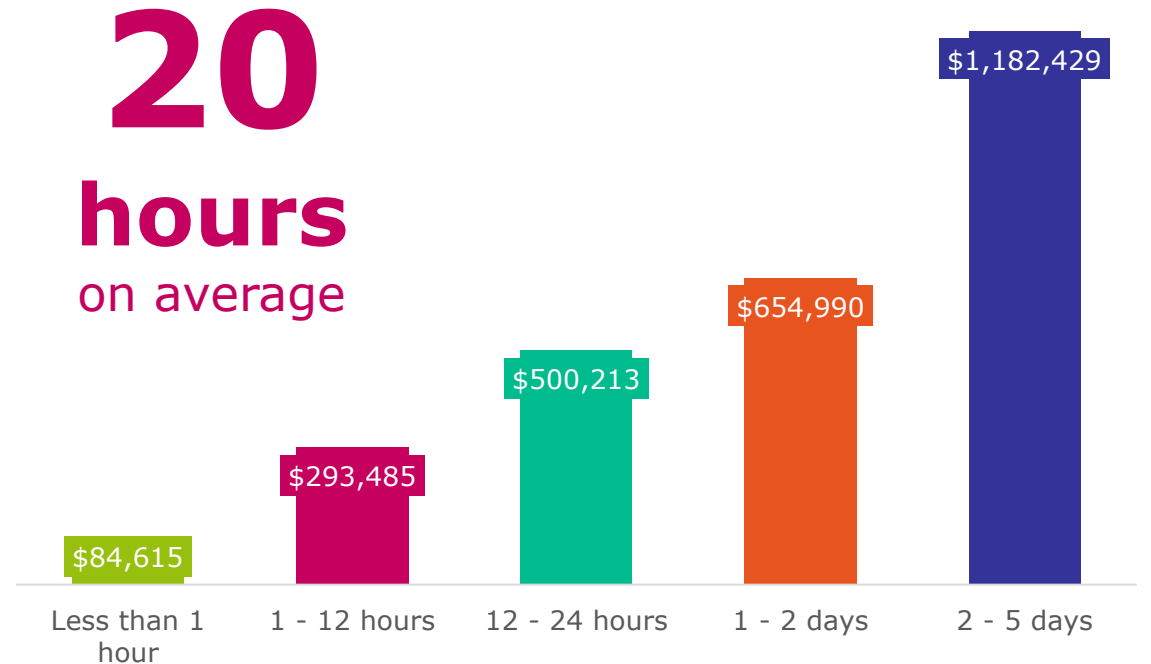
ORGANIZATIONS WITH A SINGLE DATA PROTECTION VENDOR ARE LESS LIKELY TO HAVE EXPERIENCED DISRUPTION IN THE LAST 12 MONTHS





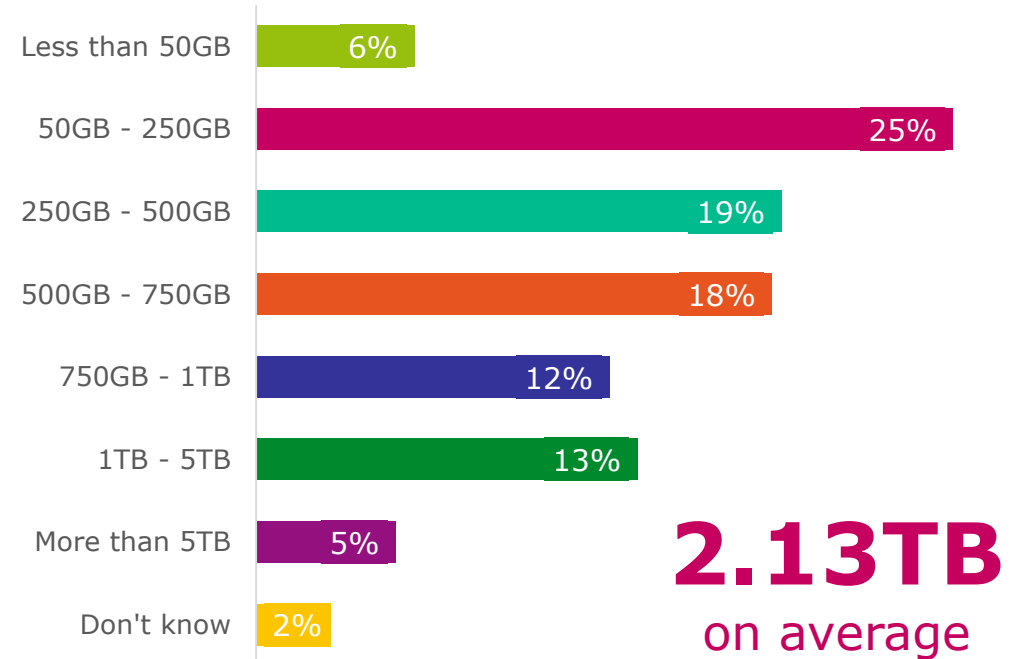
# The cost of unplanned systems downtime

**20 HOURS**  
OF DOWNTIME =  
**\$526,845**  
COST IN THE LAST 12  
MONTHS,  
ON AVERAGE



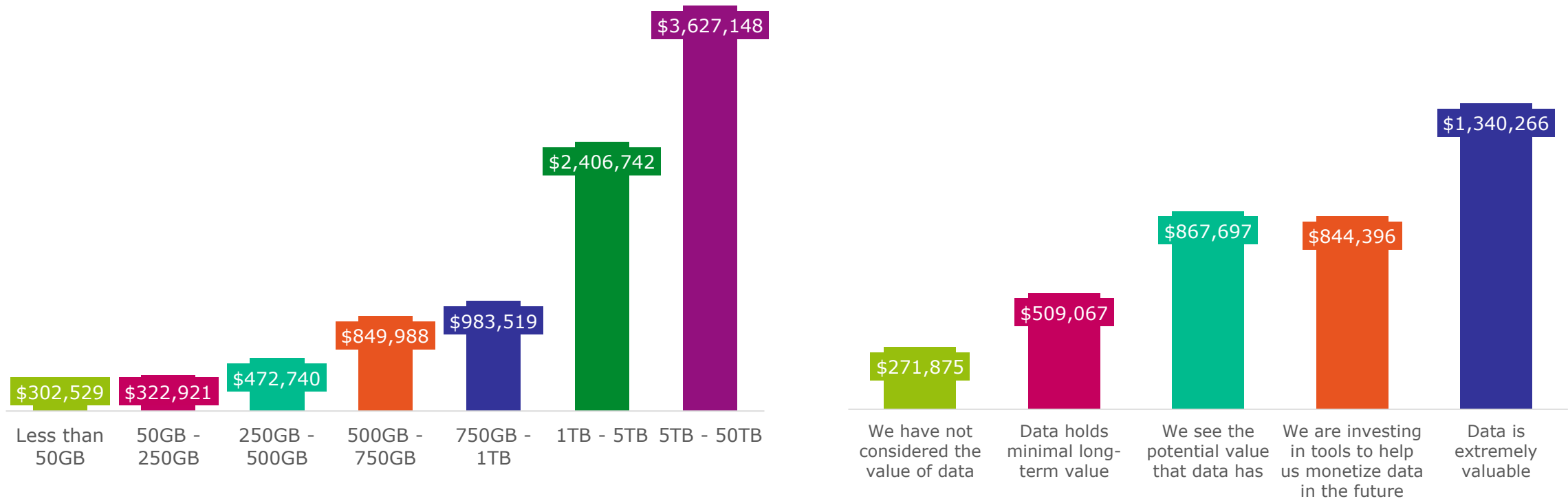
# The cost of data loss

**2.13TB**  
OF DATA LOST =  
**\$995,613**  
COST IN THE LAST 12  
MONTHS,  
ON AVERAGE



# The more you value data, the more it costs to lose it

NOT ONLY DOES THE AMOUNT OF DATA YOU LOSE INCREASE THE COST, SO DOES THE VALUE OF THE DATA ITSELF



# Recovering from unexpected critical application downtime

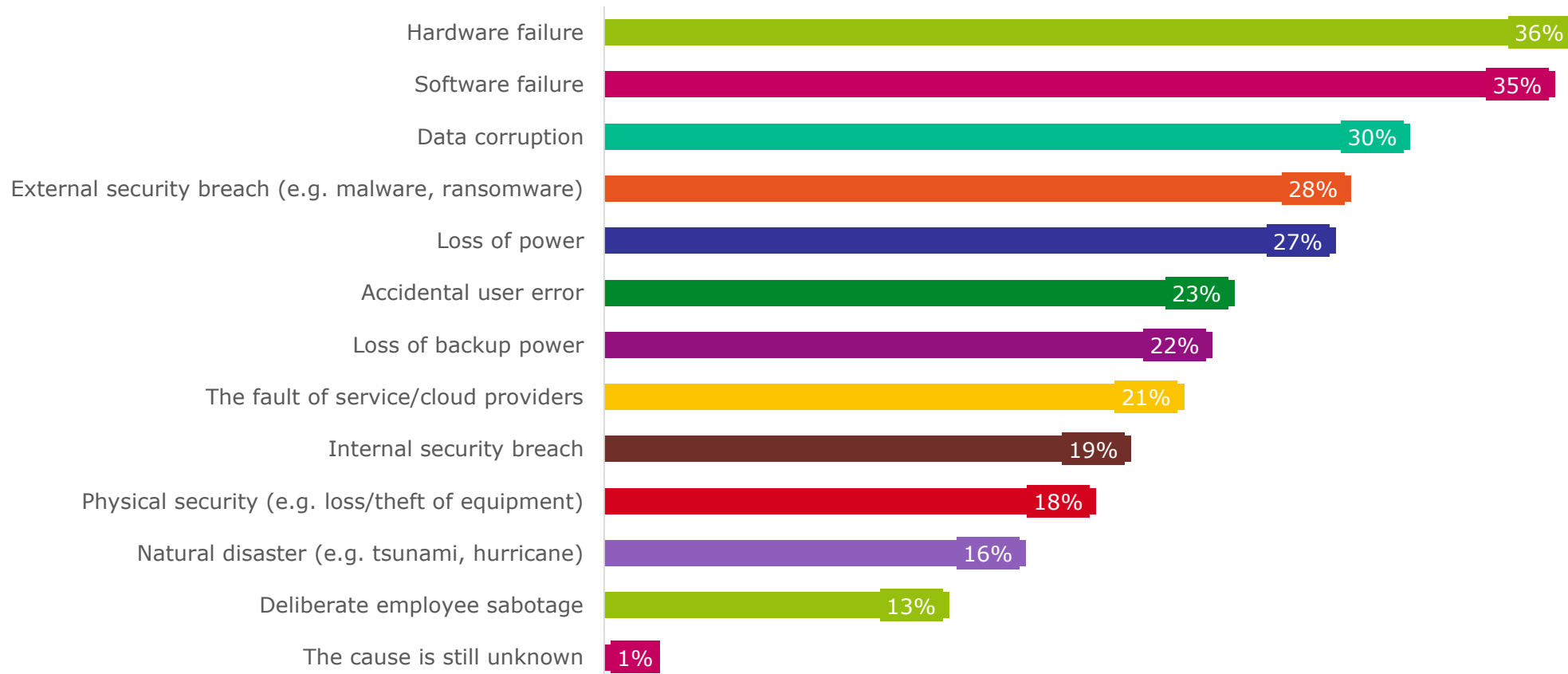
ONLY **8%** OF RESPONDENTS EXPECT THEIR ORGANIZATION'S RECOVERY TIME TO BE LESS THAN AN HOUR

THE AVERAGE IS **7 HOURS**



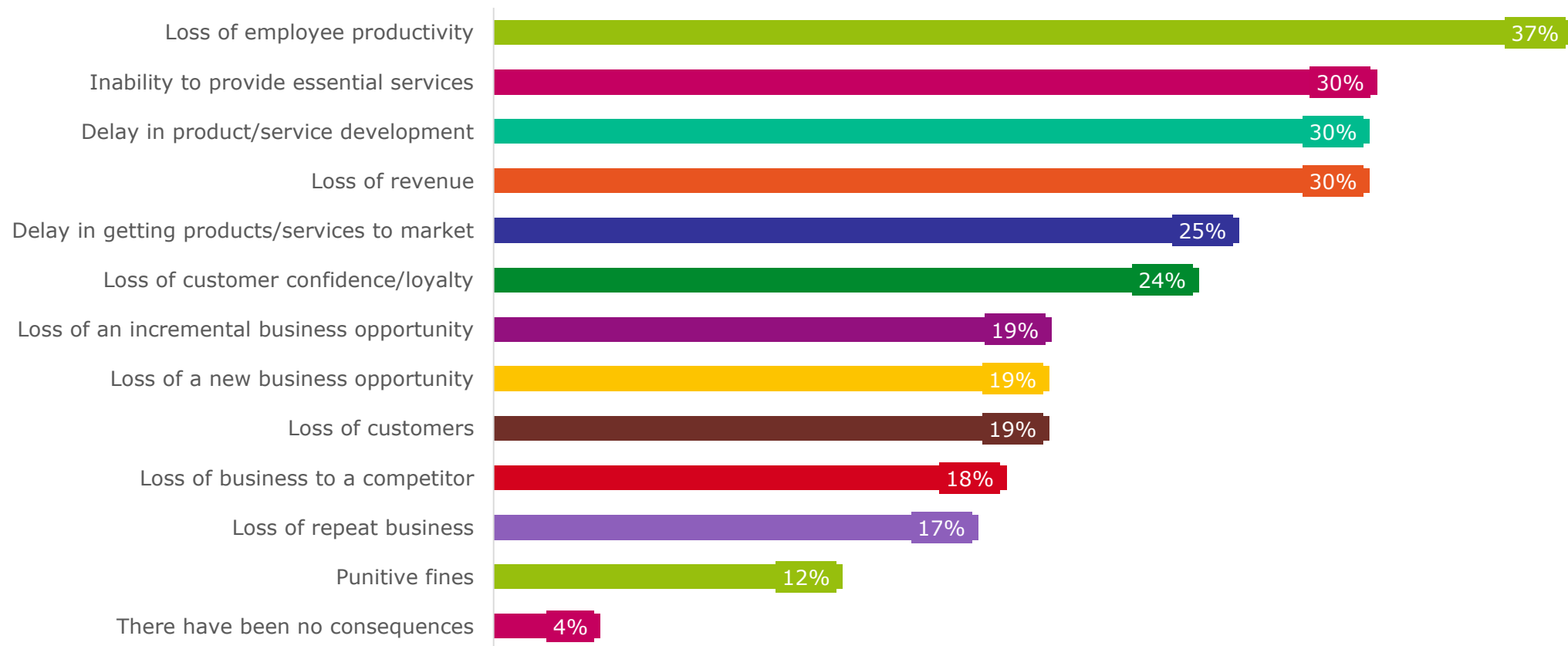
# What are the causes of this disruption?

THERE ARE MANY DIFFERENT CAUSES FOR THIS DISRUPTION, MAKING IT DIFFICULT FOR ORGANIZATIONS TO DEFEND AGAINST



# Consequences of data loss and/or systems downtime

**96%** OF ORGANIZATIONS THAT HAVE SUFFERED DATA LOSS AND/OR UNPLANNED SYSTEMS DOWNTIME HAVE EXPERIENCED CONSEQUENCES



# Confidence in current data protection solutions

IN THE EVENT OF A  
DATA LOSS INCIDENT,  
ONLY

**33%**

ARE VERY CONFIDENT  
THAT THEIR  
ORGANIZATION COULD  
FULLY RECOVER IN  
ORDER TO MEET  
BUSINESS SLOs



IN THE EVENT OF A  
DESTRUCTIVE  
CYBERATTACK, ONLY

**35%**

ARE VERY CONFIDENT  
THAT THEIR  
ORGANIZATION COULD  
RELIABLY RECOVER ALL  
BUSINESS-CRITICAL DATA

## Overall confidence when it comes to data protection

ONLY **8%** ARE VERY CONFIDENT THAT THEIR ORGANIZATION CAN DO ALL OF THESE...



...meet its backup and recovery SLOs



...have data protection infrastructure and processes that are compliant with regional governance regulations



...fully recover all systems/data (both on-premises and off) to meet business SLOs in the event of a data loss incident



...reliably recover all business-critical data and protect the most critical data in the event of a destructive cyberattack

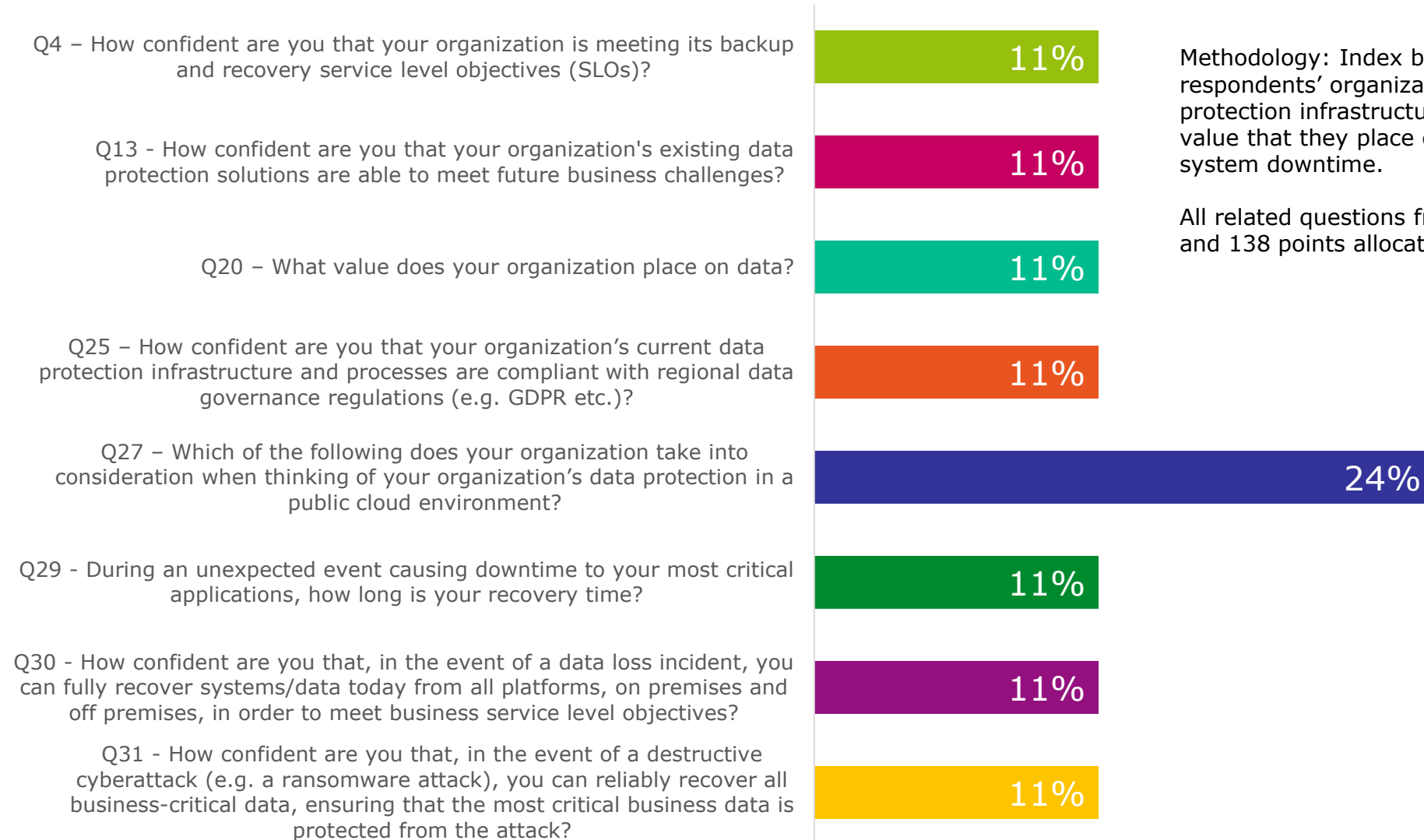


## Conclusions

- Organizations are now managing a greater volume of data than they ever have before and are assigning a greater *value* to that data
- Yet many are still facing disruption, including unplanned systems downtime and data loss – and this is coming at an enormous cost
  - The risk is even greater for Data Protection Leaders as they are the ones assigning the greatest value to data
- In most cases, organizations need to improve their data protection infrastructure – the majority of respondents highlight at least one area that could be improved or that they do not have confidence in
  - This isn't easy though, with multiple vendors often being used and a complex environment being faced
- Organizations need to be investing in *future-ready* data protection. This includes moving data protection to a cloud environment and ensuring that data protection for emerging technologies (e.g. AI/ML) is also accounted for

# APPENDIX – MATURITY MODEL

# Question weighting for DPI maturity model



Methodology: Index based on the performance of respondents' organizations in terms of their data protection infrastructure and their confidence in it, the value that they place on data, and recovery times during system downtime.

All related questions from research were filtered through, and 138 points allocated across the curve.

# Maturity model questions and scores (i)

## Q4 – How confident are you that your organization is meeting its backup and recovery service level objectives (SLOs)?

- Not at all confident **(0 points)**
- Not very confident **(1 point)**
- Some doubt **(5 points)**
- Moderately confident **(10 points)**
- Very confident **(15 points)**

**Maximum score = 15 points**

## Q13 – How confident are you that your organization's existing data protection solutions are able to meet future business challenges?

- Our current data protection solutions will **not** be able to meet **any** future business challenges **(0 points)**
- Our current data protection solutions will be able to meet a minority of future business challenges **(5 points)**
- Our current data protection solutions will be able to meet the majority of future business challenges **(10 points)**
- Our current data protection solutions will be able to meet all future business challenges **(15 points)**

**Maximum score = 15 points**

## Q20 – What value does your organization place on data?

- Data is extremely valuable – we are currently monetizing it (i.e. data = capital) **(15 points)**
- We are investing in data retention and analytics tools that will help us to monetize all relevant data in the future **(10 points)**
- We see the potential value that data has **(5 points)**
- Data is just a by-product of our business process and holds minimal long-term value **(0 points)**
- We have not considered the value that data may bring to our business **(0 points)**
- Don't know **(0 points)**

**Maximum score = 15 points**

# Maturity model questions and scores (ii)

**Q25 – How confident are you that your organization's current data protection infrastructure and processes are compliant with regional data governance regulations (e.g. GDPR etc.)?**

- Not at all confident **(0 points)**
- Not very confident **(1 point)**
- Some doubt **(5 points)**
- Moderately confident **(10 points)**
- Very confident **(15 points)**

**Maximum score = 15 points**

**Q27 – Which of the following does your organization take into consideration when thinking of your organization's data protection in a public cloud environment?**

*Please select all that apply*

- The possibility to build our own solutions to address public cloud data protection **(3 points)**
- The lowest cost public cloud provider or service available **(1 point)**
- Public cloud protection service offerings compared to 3rd party data protection offerings (feature and workload support) **(3 points)**
- The ability to scale services as public cloud workload increases **(5 points)**
- The impact of the data protection infrastructure or services required to protect at scale **(5 points)**
- Whether we have unified management of backup data stored on-prem and across multi public cloud providers **(5 points)**
- Visibility of protected cloud infrastructure across multi-regions of the cloud provider **(3 points)**
- Portability or replication of workload between on-prem and multi cloud providers **(3 points)**
- Total cost of ownership (TCO) and hard cost savings for using public cloud for disaster recovery **(5 points)**
- We do not take data protection into account when using public cloud (exclusive) **(0 points)**

**Maximum score = 33 points**

# Maturity model questions and scores (iii)

**Q29 – During an unexpected event causing downtime to your most critical applications, how long is your recovery time?**

- Our recovery time is more than one working day (please specify in days) **(0 points)**
- Our recovery time is 12 - 24 hours **(2 points)**
- Our recovery time is 6 - 12 hours **(4 points)**
- Our recovery time is 3 - 6 hours **(6 points)**
- Our recovery time is 2 - 3 hours **(8 points)**
- Our recovery time is 1 - 2 hours **(10 points)**
- Our recovery time is less than an hour **(12 points)**
- Our recovery time is zero **(15 points)**
- I do not know **(0 points)**

**Maximum score = 15 points**

**Q30 – How confident are you that, in the event of a data loss incident, you can fully recover systems/data today from all platforms, on premises and off premises, in order to meet business service level objectives?**

- Not at all confident **(0 points)**
- Not very confident **(1 point)**
- Some doubt **(5 points)**
- Moderately confident **(10 points)**
- Very confident **(15 points)**

**Maximum score = 15 points**

**Q31 – How confident are you that, in the event of a destructive cyberattack (e.g. a ransomware attack), you can reliably recover all business-critical data, ensuring that the most critical business data is protected from the attack?**

- Not at all confident **(0 points)**
- Not very confident **(1 point)**
- Some doubt **(5 points)**
- Moderately confident **(10 points)**
- Very confident **(15 points)**

**Maximum score = 15 points**

# ARE YOU PROTECTED?

GET AHEAD OF THE CURVE

DELL EMC – GLOBAL DATA PROTECTION INDEX 2018