Data Protection in a Multicloud World
This eBook presents findings from Dell Technologies’ Global Data Protection Index 2022 Snapshot commissioned through Vanson Bourne, a survey of 1,000 IT decision makers (ITDMs) globally.

<table>
<thead>
<tr>
<th>3</th>
<th>Introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>The data protection risk landscape</td>
</tr>
<tr>
<td>5</td>
<td>The increasing threat posed by cyberattacks</td>
</tr>
<tr>
<td>9</td>
<td>Protecting new and emerging tech</td>
</tr>
<tr>
<td>10</td>
<td>Securing a cloud environment</td>
</tr>
<tr>
<td>13</td>
<td>Looking to the future: the growth of as-a-Service</td>
</tr>
<tr>
<td>14</td>
<td>Simplifying data protection</td>
</tr>
<tr>
<td>15</td>
<td>Conclusion</td>
</tr>
</tbody>
</table>
As data proliferates across edge, core and public cloud, organizations are experiencing increased cyber security disruption and data protection risks. Over the last 12 months, organizations across all regions report a sharp uptick in cyberattacks that prevented access to their data, contributing to rising business disruption and resulting in steep financial losses. And, as more organizations shift to public cloud usage, there are increasing concerns around the protection and security of cloud-based data assets.

To reduce risk and accelerate digital transformation, organizations identify multicloud data protection, cyber resiliency and “as-a-Service” solutions as high priority items for helping them shore up their data protection gaps and enable hybrid, multicloud operations.
The data protection risk landscape

Organizations are encountering increasing levels of disruption, with 86% having experienced at least one disruption in the last 12 months. 69% of organizations are concerned that they will experience a disruptive event in the next 12 months.

Moreover, most organizations lack confidence that they are meeting their backup and recovery service level objectives.

55%

are not very confident that their organization is meeting its backup and recovery service level objectives (SLOs)

Adding to this cause for concern, data loss events continue to have a significant financial impact on organizations.

$1.06m

the average cost of data loss in the last 12 months (in USD)
Organizations cite a considerable increase in cyberattacks or incidents within the last 12 months – reported by nearly one in two respondents – pushing cyberattacks to the top of the list of causes of organizational disruption. Almost half (48%) have suffered a cyberattack or incident that prevented access to data within the last 12 months – up 30% YoY.

Cyberattack or other cyber incident that prevented access to data

- 2019: 35%
- 2021: 37%
- 2022: 48%

60% of attackers’ first point of entry is external - users clicking on spam or phishing emails and malicious links, compromised user credentials and cloud services
This resulted in an estimated cost of: $660k on average

Additionally, organizations suffering data loss or systems downtime are increasingly citing security breaches as the underlying cause.
External breaches are more likely to be the cause of data loss or systems downtime, with the proportion having increased 33% YoY.

There has also been a 73% rise in the percentage of respondents citing internal breaches over the last year. Such stark increases demand that organizations have additional fail-safes for protecting their data from rogue employees.

The sharp rise of employees working from home is partially contributing to levels of concern, alongside a lack of confidence in organizations’ existing data protection capabilities to cope with malware and ransomware threats.

70% agree their organization has increased exposure to data loss from cyberthreats with the growth of employees working from home.

67% are concerned their organization’s existing data protection measures may not be sufficient to cope with malware and ransomware threats.
63% are not very confident that all business-critical data can be reliably recovered in the event of a destructive cyberattack.

64% agree that their job and the employees within their organization will not be affected by a ransomware attack.

Most organizations have an understanding and are planning to implement Zero Trust design principles into their environment, few have fully deployed a Zero Trust architecture. This leaves organizations potentially vulnerable to risks in the meantime.

54% agree if their organization suffers a ransomware attack, once they pay the ransom they won’t be attacked again.

12% of organizations have fully implemented a Zero Trust security architecture and its ongoing maintenance.

Take the Dell Cyber Security Assessment to understand where your organization’s cyber risks and vulnerabilities are now.
As organizations invest in new and emerging technology they need to keep pace with modern data protection infrastructure. This will ensure and maintain security levels, minimize risk and raise confidence levels.

The adoption of containers, SaaS and cloud-native apps is helping organizations to modernize, however, nearly half of the respondents indicate that protecting these workloads is a barrier to digital transformation and application modernization.

**49%** report that protecting newer workloads such as containers, SaaS, and cloud-native apps are a barrier to their organizations’ digital transformation/application modernization initiatives.

**76%** rank a lack of common data protection solutions for newer technologies within the top 5 challenges their organizations face in relation to data protection.

**41%** indicate that getting developers and IT operations to work together is a barrier to their modernization efforts.
Securing a cloud environment

Cloud infrastructure (IaaS/PaaS) usage registered double digit increases in the last year. Organizations are moving towards leveraging public cloud to deploy new and update existing applications, however, this may create data protection challenges for many.

Public cloud can provide agility and flexibility, but the increased distribution of data across multiple public cloud environments can create data protection blind spots.

72% report the inability to locate and protect dynamic and distributed data resulting from DevOps and cloud development processes as one of their organizations’ top five data protection challenges.
Confidence in public cloud data protection capabilities is low, with the majority not very confident they can protect all the data across their public cloud environment.

Additionally, some organizations are running multiple workloads in multiple cloud environments; however, around one in five believe their cloud providers are responsible for protecting their workloads. This assumption may be leaving organizations’ data at risk.

![Confidence to protect all data across public cloud environments](image)

- **Not at all confident** - we do not protect our data across public cloud
- **Not very confident** - we protect some of our critical data across public cloud
- **Some doubt** - we protect most of our critical data across public cloud
- **Moderately confident** - we protect all of our critical data across public cloud, but not all our total data
- **Very confident** - we protect all of our data across public cloud

19% believe when using multiple cloud environments, each cloud service provider is responsible for protecting their workloads.
As newer technologies are deployed, the importance of protecting and securing any workload across any cloud environment is widely recognized, with protecting multi-workload environments and enabling cybersecurity considered the top two most important capabilities.

### Most important capabilities for enabling hybrid, multicloud operations

- **64%** Ability to protect multi-workload (VMs, containers, cloud-native apps, SaaS workloads) environments across on-premises and public clouds
- **61%** Ability to ensure cybersecurity across hybrid, multicloud environments
- **54%** Automated management of compute, storage and networking infrastructure
- **53%** Centralized management and visibility of hybrid, multicloud workloads
- **45%** Ability to auto-scale infrastructure resources
- **36%** End-user self-service capabilities
Looking to the future: the growth of as-a-Service

As-a-Service offerings are a high priority for many organizations and present new opportunities to further simplify the deployment and consumption of data protection.

### Highest priority as-a-Service offerings

<table>
<thead>
<tr>
<th>Service</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage-as-a-Service</td>
<td>44%</td>
</tr>
<tr>
<td>Cyber-Recovery-as-a-Service</td>
<td>41%</td>
</tr>
<tr>
<td>Backup-as-a-Service</td>
<td>40%</td>
</tr>
<tr>
<td>Disaster-Recovery-as-a-Service</td>
<td>38%</td>
</tr>
<tr>
<td>Networking-as-a-Service</td>
<td>36%</td>
</tr>
<tr>
<td>AI-as-a-Service</td>
<td>34%</td>
</tr>
<tr>
<td>Compute-as-a-Service</td>
<td>34%</td>
</tr>
<tr>
<td>Edge-as-a-Service</td>
<td>31%</td>
</tr>
</tbody>
</table>

No as-a-Service offerings are high priority for my organization 1%

### Main reasons for pursuing as-a-Service offerings

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Needing to tactically address bursting (movement of an application from private data centers or private cloud to a public cloud when demand for computing)</td>
<td>80%</td>
</tr>
<tr>
<td>The business requires more flexibility while still maintaining optimal IT operations</td>
<td>70%</td>
</tr>
<tr>
<td>Need to shift from CapEx to OpEx</td>
<td>54%</td>
</tr>
<tr>
<td>Lack of expertise in area to manage ourselves</td>
<td>53%</td>
</tr>
<tr>
<td>Not enough staff to maintain services ourselves</td>
<td>42%</td>
</tr>
<tr>
<td>We wouldn't pursue an as-a-Service offering</td>
<td>1%</td>
</tr>
</tbody>
</table>

Organizations are most likely to pursue as-a-Service solutions as a way to augment on-premises application resources and give their businesses more flexibility. There is also a desire to shift purchasing from CapEx to OpEx and make up for a shortfall in IT expertise and staffing.
Simplifying data protection

Organizations using a single data protection vendor have experienced fewer cyberattacks or other incidents of downtime and data loss compared to those working with multiple vendors. Moreover, cyber incidents are also estimated to be more costly to those using multiple data protection vendors, on average.

In fact, most organizations believe that they would benefit from reducing the number of data protection vendors they work with – and this sentiment has increased this year.

85% of those using multiple data protection vendors believe they would benefit from reducing the number of vendors they use.
Securing and protecting data has become increasingly challenging given the work from home phenomenon, increased public cloud consumption and the continued adoption of newer technologies. To mitigate risk and get ahead of the curve, organizations need to modernize data protection, reduce operational complexity and enhance cyber resiliency.

How can organizations enhance their Data Protection in a World of Digital Transformation?

- Modernize your data protection
- Reduce operational complexity
- Enhance cyber resiliency

Learn more at Dell.com/dataprotection
For complete GDPI results visit Dell.com/gdpi
DELL Technologies

About Dell Technologies
Dell Technologies helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry's broadest and most innovative technology and services portfolio for the data era.

Vanson Bourne

About Vanson Bourne
Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com