Focus of key findings

1. The data protection risk landscape
2. The increasing threat posed by cyberattacks
3. Protecting new and emerging tech
4. Securing a cloud environment
5. Looking to the future: the growth of as-a-Service
6. Simplifying data protection
Five key takeaways

The last 12 months have brought higher levels of disruption for organizations than in previous years.

Experience of cyberattacks or incidents are more prevalent this year and are contributing to increased disruption.

Almost all are facing challenges in relation to data protection.

There has been a shift towards public cloud use, which may create further data protection issues for organizations.

Working with fewer data protection vendors is linked to better data protection outcomes.
Who did we interview?

1,000 IT decision makers were interviewed in August, September and October 2022.

Organizations from a wide range of public and private sector industries.

Organizations with 250+ employees.

4 regions:
- Americas (200)
- EMEA (450)
- APJ (250)
- China (100)
1. The data protection risk landscape
Concerns and a lack of confidence surrounding the capabilities of their existing data protection measures are prevalent, exposing organizations to risk.

- **55%** are not very confident that their organization is meeting its backup and recovery service level objectives (SLOs).
- **69%** are concerned that they will experience a disruptive event in the next twelve months.
- **67%** are concerned their organization’s existing data protection measures may not be sufficient 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.
Alongside commonplace data protection challenges organizations are faced with:

**Ranked top 5: Challenges faced in relation to data protection**

- **76%**: Lack of data protection solutions for newer technologies (e.g., containers, cloud-native applications, IoT, edge, etc.)
- **72%**: Inability to locate and protect dynamic and distributed data resulting from DevOps and cloud development processes
- **69%**: Inability to meet backup windows because of increasingly distributed nature of data
- **68%**: Ballooning costs of storing and managing backup copies because of rapid data growth
- **65%**: Increased operational management time and complexity
- **64%**: Inability to meet backup windows because of growth in size of data
- **3%**: We are not facing any challenges in relation to data protection
Although many organizations have an understanding and are planning or deploying Zero Trust security, few have fully implemented the architecture.

Organizations’ journey to implementing Zero Trust security, split by region

- **My organization does not yet have an understanding of Zero Trust**: 9% (Total), 6% (Americas), 9% (EMEA), 3% (APJ), 3% (China)
- **My organization is just now discussing what Zero Trust means to our operations**: 19% (Total), 20% (Americas), 23% (EMEA), 16% (APJ), 15% (China)
- **My organization understands and is committed to implementing Zero Trust practices**: 16% (Total), 10% (Americas), 16% (EMEA), 15% (APJ), 8% (China)
- **My organization is in the planning phase of implementing a Zero Trust security architecture**: 21% (Total), 19% (Americas), 24% (EMEA), 38% (APJ), 3% (China)
- **My organization is actively deploying Zero Trust security architecture capabilities**: 23% (Total), 27% (Americas), 20% (EMEA), 22% (APJ), 10% (China)
- **My organization has fully implemented a Zero Trust security architecture and its ongoing maintenance**: 12% (Total), 18% (Americas), 10% (EMEA), 13% (APJ), 8% (China)

**Legend:**
- **Total [1,000]**
- **Americas [200]**
- **EMEA [450]**
- **APJ [250]**
- **China [100]**
The majority of organizations still have a way to go to ensure Zero Trust is executed to best-practice standards and are potentially vulnerable to risk in the meantime.

| Identify all data sources & computing services resources | 2% | 14% | 23% | 30% | 31% |
| All communication is secured regardless of network location | 3% | 14% | 19% | 33% | 30% |
| Access to individual enterprise resources is granted on a per-session basis | 3% | 16% | 20% | 31% | 31% |
| Access to resources is determined by dynamic policy | 3% | 16% | 24% | 34% | 23% |
| Monitor and measure the integrity and security posture of all owned and associated assets | 2% | 14% | 22% | 35% | 27% |
| Resource authentication and authorization are dynamic and strictly enforced before access is allowed | 3% | 14% | 23% | 30% | 31% |
| Collect as much information as possible about the current state of assets, network infrastructure & communications & uses it to improve its security posture | 2% | 16% | 23% | 33% | 27% |

Unsure how to implement  ■ Planning implementation  ■ Beginning implementation  ■ Implementation is underway  ■ Fully implemented
In addition, levels of disruption which are more likely being driven by cyber incidents, local disasters and problems recovering from current data protection methods have increased...

Organizations suffering various disruptions in the last 12 months, split by year

- Cyberattack or other cyber incident that prevented access to data: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]
- Local disaster which affected access to data for an entire site or group: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]
- Inability to recover data from the current data protection method or product: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]
- Unplanned systems downtime: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]
- Data loss: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]
- We have not experienced any of the above: 2018 [2,200], 2019 [1,000], 2021 [1,000], 2022 [1,000]

86% of 2022 respondents' organizations have experienced at least one disruption in the last 12 months.
...with data loss increasingly impacting bottom lines

Average estimated cost of data loss in the last 12 months, split by year

<table>
<thead>
<tr>
<th>Year</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>$995,613</td>
</tr>
<tr>
<td>2019</td>
<td>$1,013,075</td>
</tr>
<tr>
<td>2021</td>
<td>$959,493</td>
</tr>
<tr>
<td>2022</td>
<td>$1,057,895</td>
</tr>
</tbody>
</table>
2. The increasing threat posed by cyberattacks
Confidence that organizations’ data protection measures can mitigate the effects of cyberattacks is lacking. Moreover, most are aware there are increased vulnerabilities with 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.
- **70%** agree their organization has increased exposure to data loss from cyberthreats with the growth of employees working from home.
This lack of confidence is echoed in their organization’s ability to recover business-critical data in the event of cyberattack.

Not “very confident” that all business-critical data can be reliably recovered in the event of a destructive cyberattack, split by year:

- 2018 [2,200]: 65%
- 2019 [1,000]: 69%
- 2021 [1,000]: 67%
- 2022 [1,000]: 63%
Compounding this, there is a misguided over-confidence surrounding the consequences of a ransomware attack, another factor that could expose organizations to further risk.

- 64% agree that their job and the employees within their organization will not be affected by a ransomware attack.
- 61% agree that if their organization suffers a ransomware attack, they'll get all data back to resume business if they pay the ransom.
- 54% agree that if their organization suffers a ransomware attack, once they pay the ransom they won’t be attacked again.
Which is concerning as there has been a considerable increase in IT decision makers reporting that their organizations’ have suffered a cyberattack or other cyber incident in the last 12 months.

<table>
<thead>
<tr>
<th>Year</th>
<th>Incident Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018</td>
<td>2,200</td>
<td>28%</td>
</tr>
<tr>
<td>2019</td>
<td>1,000</td>
<td>35%</td>
</tr>
<tr>
<td>2021</td>
<td>1,000</td>
<td>37%</td>
</tr>
<tr>
<td>2022</td>
<td>1,000</td>
<td>48%</td>
</tr>
</tbody>
</table>
Even those who suffered data loss and/or systems downtime are more likely to cite security breaches as their cause, considerably increasing since 2021.

Causes of data loss and/or systems downtime, split by year:

- **External security breach (e.g. malware, spyware, viruses, botnets, ransomware or cyber-terrorism or attack)**: 42% (2021), 41% (2022)
- **Software failure**: 31% (2021), 38% (2022)
- **Service/cloud provider error**: 27% (2021), 25% (2022)
- **Data corruption**: 35% (2021), 35% (2022)
- **Internal security breach (e.g. internal employee)**: 18% (2021), 14% (2022)
- **Hardware failure** (e.g. loss/theft of equipment): 46% (2021), 31% (2022)
- **Physical security** (e.g. Deliberate employee sabotage): 28% (2021), 21% (2022)
- **User error**: 26% (2021), 24% (2022)
- **Loss of power**: 32% (2021), 24% (2022)
- **Natural disaster** (e.g. tsunami, hurricane, earthquake, flood, fire): 20% (2021), 9% (2022)
When they do attack, cyberattackers reportedly use various points of entry, with external attacks more likely compared to internal ones.

<table>
<thead>
<tr>
<th></th>
<th>Attacker’s first point of entry of most recent cyberattack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromised credentials</td>
<td>15% (e.g. privilege access, Remote Desktop Protocol access)</td>
</tr>
<tr>
<td>Cloud services</td>
<td>15%</td>
</tr>
<tr>
<td>Malicious link or website</td>
<td>15%</td>
</tr>
<tr>
<td>Spam/phishing email</td>
<td>15%</td>
</tr>
<tr>
<td>Infected software/hardware patch of updates</td>
<td>12%</td>
</tr>
<tr>
<td>Insider attack (e.g. disgruntled employee or employee mistake)</td>
<td>9%</td>
</tr>
<tr>
<td>Employee-owned mobile device</td>
<td>8%</td>
</tr>
<tr>
<td>Firmware</td>
<td>5%</td>
</tr>
<tr>
<td>Corporate-owned mobile device</td>
<td>5%</td>
</tr>
</tbody>
</table>
There is some variation in what organizations consider important for cyber resiliency.

Items and processes considered important for cyber resiliency:

- Vulnerability management for storage and backup: 62%
- Non-corrupt data backups for recovery: 58%
- Air-gapping critical data from the production environment: 58%
- Storage snapshot replication: 49%
- Immutable storage and vault: 44%
3. Protecting new and emerging tech
Adopting newer technology can help drive modernization, but many report a lack of data protection solutions for them as a challenge and barrier.

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

76% rank a lack of data protection solutions for newer technologies (e.g. containers, cloud-native applications, IoT, edge, etc.) within the top 5 challenges their organization faces in relation to data protection.
Many see emerging technologies posing a risk to data protection and, potentially as a result, are increasing security in edge computing locations.

67% agree that emerging technologies (such as AI, IOT, edge) pose a risk to data protection.

Current protection of data in edge computing locations, split by year:

- **Backed-up to private cloud**:
- **Backed-up to public cloud**:
  - 2022: 56%, 2021: 49%, 2019: 42%.
- **Backed-up locally (at edge locations)**:
  - 2022: 59%, 2021: 37%, 2019: 30%.
- **We do not have a formalized method for data protection in edge locations**:
  - 2022: 1%, 2021: 2%, 2019: 2%.

We do not have a formalized method for data protection in edge locations.
4. Securing a cloud environment
Organizations appear to be shifting towards using public cloud for updating existing and deploying new applications

### Updating existing applications

<table>
<thead>
<tr>
<th>Service Type</th>
<th>2022 [1,000]</th>
<th>2021 [1,000]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public cloud (IaaS)</td>
<td>46%</td>
<td>55%</td>
</tr>
<tr>
<td>Public cloud (PaaS)</td>
<td>31%</td>
<td>43%</td>
</tr>
<tr>
<td>Private cloud (on-premises)</td>
<td>37%</td>
<td>41%</td>
</tr>
<tr>
<td>Private cloud (hosted)</td>
<td>37%</td>
<td>43%</td>
</tr>
<tr>
<td>Public cloud (SaaS)</td>
<td>37%</td>
<td>35%</td>
</tr>
<tr>
<td>Hybrid cloud (mix of two or more locations)</td>
<td>22%</td>
<td>18%</td>
</tr>
</tbody>
</table>

### Deploying new applications

<table>
<thead>
<tr>
<th>Service Type</th>
<th>2022 [1,000]</th>
<th>2021 [1,000]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public cloud (IaaS)</td>
<td>40%</td>
<td>50%</td>
</tr>
<tr>
<td>Public cloud (PaaS)</td>
<td>35%</td>
<td>46%</td>
</tr>
<tr>
<td>Public cloud (SaaS)</td>
<td>30%</td>
<td>37%</td>
</tr>
<tr>
<td>Private cloud (hosted)</td>
<td>34%</td>
<td>37%</td>
</tr>
<tr>
<td>Private cloud (on-premises)</td>
<td>28%</td>
<td>29%</td>
</tr>
<tr>
<td>Hybrid cloud (mix of two or more locations)</td>
<td>15%</td>
<td>25%</td>
</tr>
</tbody>
</table>
However, this shift towards public cloud may create data protection challenges for many organizations

Confidence to protect all data across public cloud environments

- 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
Moreover, the move from organizations planning to use public cloud for Disaster Recovery in the future is increasingly becoming a reality.

**Use of public cloud for Disaster Recovery**

- Yes, we use the public cloud for this currently: 80%
  - 2022 [1,000]
  - 2021 [1,000]

- No, but we plan to use the public cloud for this in the future: 16%
  - 2022 [1,000]
  - 2021 [1,000]

- No, and we do not plan to use the public cloud for this: 4%
  - 2022 [1,000]
  - 2021 [1,000]
There has been a shift in how organizations plan to protect their workloads in multiple cloud environments, although a number aren’t using specific solutions to protect them.

<table>
<thead>
<tr>
<th>Year</th>
<th>Protection of Workloads, %</th>
</tr>
</thead>
<tbody>
<tr>
<td>2022</td>
<td>38% Our current backup solution allows us to protect workloads running in multiple clouds</td>
</tr>
<tr>
<td>2021</td>
<td>23% Our current backup solution allows us to protect workloads running in multiple clouds</td>
</tr>
<tr>
<td>2019</td>
<td>26% Our current backup solution allows us to protect workloads running in multiple clouds</td>
</tr>
</tbody>
</table>

19% believe when using multiple cloud environments, each cloud service provider is responsible for protecting their workloads.
Protecting multi-workload environments and ensuring cybersecurity are most important capabilities for enabling hybrid, multicloud operations

<table>
<thead>
<tr>
<th>Capability</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to protect multi-workload (VMs, containers, cloud-native apps, SaaS workloads) environments across on-premises and public clouds</td>
<td>64%</td>
</tr>
<tr>
<td>Ability to ensure cybersecurity across hybrid, multicloud environments</td>
<td>61%</td>
</tr>
<tr>
<td>Automated management of compute, storage and networking infrastructure</td>
<td>54%</td>
</tr>
<tr>
<td>Centralized management and visibility of hybrid, multicloud workloads</td>
<td>53%</td>
</tr>
<tr>
<td>Ability to auto-scale infrastructure resources</td>
<td>45%</td>
</tr>
<tr>
<td>End-user self-service capabilities</td>
<td>36%</td>
</tr>
</tbody>
</table>
5. Looking to the future: the growth of as-a-Service
As-a-Service offerings are more likely to be a priority this year, with a greater need for tactically moving applications to public cloud.

Ranked within top 3: Highest priority as-a-Service offerings, split by year:

<table>
<thead>
<tr>
<th>Service-as-a-Service</th>
<th>2022 1,000</th>
<th>2021 1,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage-as-a-Service</td>
<td>44%</td>
<td>47%</td>
</tr>
<tr>
<td>Cyber-Recovery-as-a-Service</td>
<td>41%</td>
<td>35%</td>
</tr>
<tr>
<td>Backup-as-a-Service</td>
<td>40%</td>
<td>43%</td>
</tr>
<tr>
<td>Disaster Recovery-as-a-Service</td>
<td>38%</td>
<td>41%</td>
</tr>
<tr>
<td>Networking-as-a-Service</td>
<td>36%</td>
<td>37%</td>
</tr>
<tr>
<td>AI-as-a-Service</td>
<td>34%</td>
<td>29%</td>
</tr>
<tr>
<td>Compute-as-a-Service</td>
<td>34%</td>
<td>32%</td>
</tr>
<tr>
<td>Edge-as-a-Service</td>
<td>31%</td>
<td>23%</td>
</tr>
</tbody>
</table>

No as-a-Service offerings are high priority for my organization: 1% in 2022, 4% in 2021.

Ranked within top 3: Main reasons for pursuing as-a-Service offerings:

<table>
<thead>
<tr>
<th>Reason</th>
<th>2022 1,000</th>
<th>2021 1,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need to tactically address bursting (movement of an application from private data centers or private cloud to a public cloud when demand for computing capacity spikes)</td>
<td>67%</td>
<td>80%</td>
</tr>
<tr>
<td>The business requires more flexibility while still maintaining optimal IT operations</td>
<td>70%</td>
<td>74%</td>
</tr>
<tr>
<td>Need to shift from CapEx to OpEx</td>
<td>54%</td>
<td>53%</td>
</tr>
<tr>
<td>Lack of expertise in area to manage ourselves</td>
<td>53%</td>
<td>49%</td>
</tr>
<tr>
<td>Not enough staff to maintain services ourselves</td>
<td>42%</td>
<td>47%</td>
</tr>
<tr>
<td>We wouldn't pursue an as-a-Service offering</td>
<td>1%</td>
<td>3%</td>
</tr>
</tbody>
</table>
There are a range of attributes considered important for as-a-Service backup solutions.

Most important attributes of as-a-Service backup solution

- Disaster recovery and long-term retention for hybrid workloads, (e.g. VMs, databases, file servers and NAS) - 55%
- Cloud to cloud backup and restore - 51%
- Protection of SaaS apps (e.g. M365, Salesforce, Google Workspace) - 50%
- Protection for endpoints (e.g. desktop, laptop, mobile devices) - 45%
- Ransomware protection and recovery - 43%
- Centralized monitoring and management - 40%
- Ease of deployment - 37%
- Data reuse - 34%
- No ongoing infrastructure management - 31%
6. Simplifying data protection
Organizations using multiple data protection vendors are more likely to have suffered disruption, suggesting this approach exacerbates these challenges – particularly for cyber incidents.

Organizations suffering various disruptions in the last 12 months, split by number of data protection vendors in use.
And cyber security incidents are estimated to cost organizations who use multiple data protection vendors more than those who use a single vendor.
The vast majority of those using multiple data protection vendors believe they would benefit from reducing the number of vendors they use – which has grown YoY

Benefit in reducing the number of vendors worked with for data protection needs

- **2022 [827]**
  - Yes, we would see a large benefit: 56%
  - Yes, we would see a small benefit: 29%
  - No, we would not see a benefit: 12%
  - I’m not sure: 3%

- **2021 [777]**
  - Yes, we would see a large benefit: 38%
  - Yes, we would see a small benefit: 40%
  - No, we would not see a benefit: 19%
  - I’m not sure: 3%
Key findings – in summary (1/2)

The data protection risk landscape

• Most are not very confident that they would be able to recover all systems and data to meet SLOs in the event of a data loss incident
• Many have an understanding of Zero Trust standards, yet few have fully implemented the architecture or their associated 7 tenets
• Fear that organizations will experience a disruptive event in the next 12 months is extensive, with the potential impacts financially damaging
• Such fear is likely justified with increasing levels of disruption seen YoY and encountering data protection challenges are commonplace

The increasing threat posed by cyberattacks

• Most are concerned that their organization’s data protection may not be able to cope with a malware or ransomware threat, and that they have become increasingly vulnerable with more employees working from home
• Organizational confidence in recovering lost data from a cyberattack is low
• Further, many are misguided and over-confident about the likelihood and consequences of ransomware attacks
• There has been an increase in organizations suffering a cyberattack or incident in the last 12 months and security breaches have been more likely to be the cause of data loss and/or systems downtime

Protecting new and emerging tech

• Many believe that emerging technologies pose a risk to data protection, and these risks are likely contributing to fears that organizations aren’t future-ready, and that they are at risk of disruption in the next twelve months
• The adoption of containers and cloud-native apps can help drive modernization, but most IT decision makers cite the lack of data protection solutions for these newer technologies as a challenge
• Investment in emerging technologies is a positive move for organizations, which must be accompanied by supporting and robust data protection infrastructure
• It is, therefore, encouraging to see that security in edge computing locations is on the rise
Key findings – in summary (2/2)

Securing a cloud environment

- Organizations have moved towards the use of public cloud for updating existing and deploying new applications, and disaster recovery
- However, few are very confident that their data will be protected across their organization’s public cloud environment, and this could create data protection challenges for many
- Organizations need to ensure they have specific solutions in place to protect data across multicloud workloads, as some still believe their cloud providers are responsible for this
- Considering the landscape, it is encouraging that organizations consider protecting multi-workload environments and ensuring cybersecurity as the most important capabilities for enabling hybrid, multicloud operations

Looking to the future: the growth of as-a-Service

- As-a-Service solutions are more likely to be a priority this year, and probable in forming part of many organizations’ data protection solutions in the future
- Storage, cyber-recovery and backup are organizations’ top three priorities for as-a-Service offerings

Simplifying data protection

- Organizations using a single data protection vendor are less likely to have suffered disruption in the past year compared to those using multiple vendors, particularly those related to cyberattacks or other cyber incidents
- These cyber incidents are also estimated to be more costly to those using multiple protection vendors, on average
- Most organizations using multiple data protection vendors believe they would see benefit in reducing the number of vendors – and this sentiment has increased this year
Mitigate risk and get ahead of the curve

Dell Technologies point of view

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

Learn more at dell.com/GDPI