Five Data Privacy Challenges in the Cloud

If you're worried about data privacy in the cloud, you're not alone. Here are the top five challenges facing organizations right now:

2. Data being stored without the correct level of encryption.
3. Shadow IT from other departments within the organization.
4. The cloud environment doesn't meet the regulatory standards of the industry.
5. A lack of understanding of the security protocols being used by cloud providers.

Data Sharing is a Necessary Risk

As this digital transformation continues, controlling unauthorized access to data should become a priority because sharing data externally is a necessary part of your business operations.

What’s your sharing habit?

82% say sharing data externally is a daily occurrence.
44% share data in a continuous basis.
83% share data daily.
13% share data every hour.

Do you know with whom you’re sharing?

68% say they are most likely to share data with trusted partners.
61% are also sharing with industry leaders and third-party regulators.
57% share with suppliers.
57% say they share data with customers.

Or how all of this data is being shared?

50% of organizations share data externally via email.
61% use cloud file storage systems like Google Drive, Dropbox, and iCloud.
51% use file transfer solutions like IBM Aspera and Salesforce Connect.
52% use transfer solutions like Dell Secure and Sendbox Secure.

Data Protection Checklist

It's okay to share data—but you need to maintain constant control over who has access and when. Look for a vendor that provides:

- Consistent policy enforcement across disparate environments.
- Persistent data control as data is shared.
- Zero-Trust architecture.
- An easy user experience.

Are you ready to gain control over your data across multi-cloud environments, applications, and devices? Fast in touch with Virtru to learn more.

Learn More