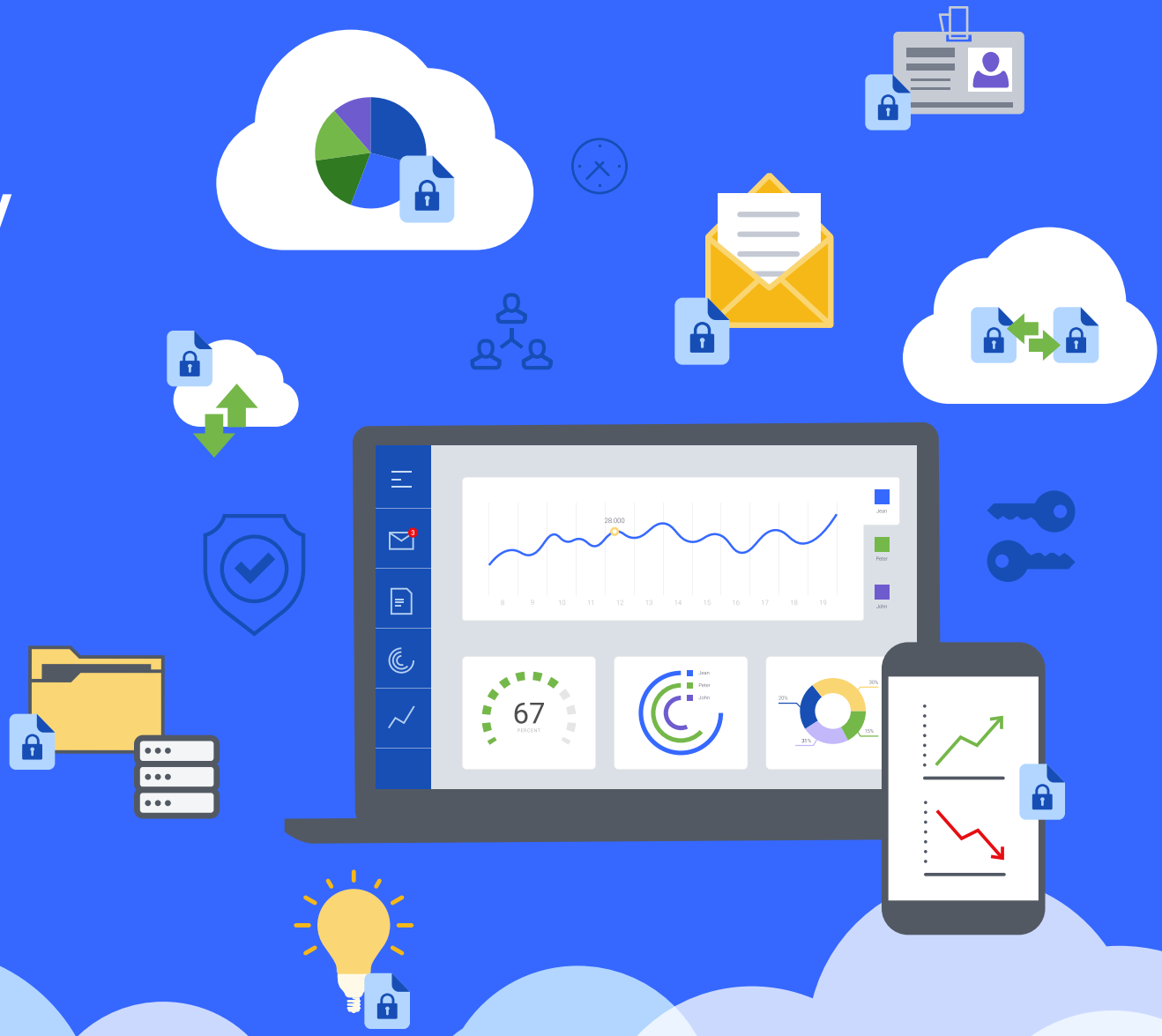
Data Security and Privacy in the Digital Workplace



virtru

Table of Contents

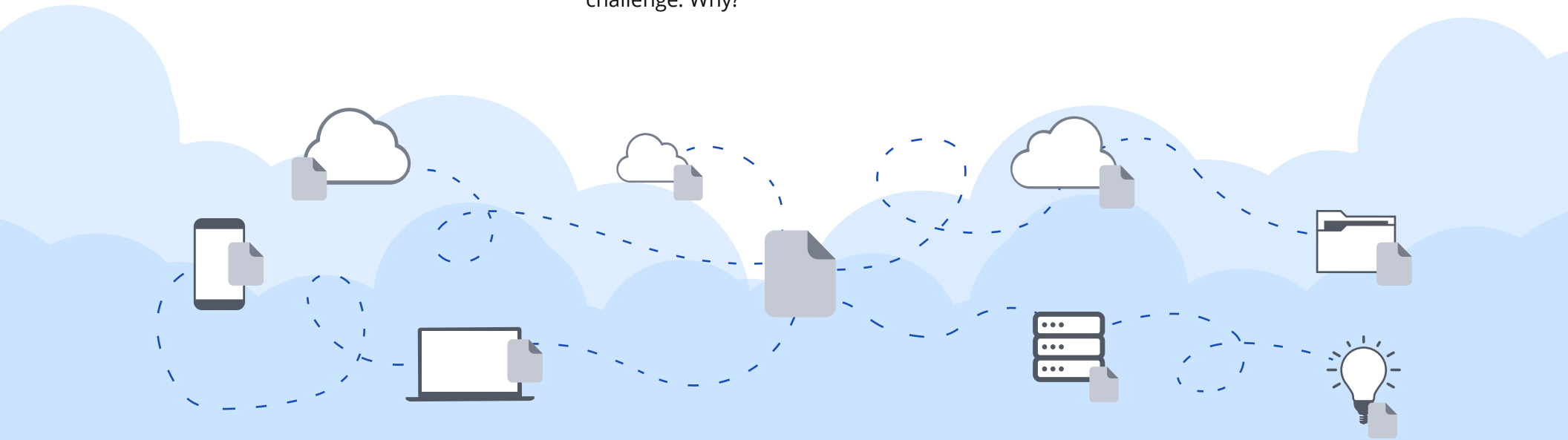
Chapter 1

Data is personal, confidential, and often times mission-critical information that keeps your business operations running, ensures timely and consistent communication with customers and partners, and empowers employees to always be productive and collaborative. In today's digital workplace, data flows seemingly everywhere, from devices and email systems to multiple cloud environments and applications.

Organizations are producing data at record speed:
It's estimated that by 2025, worldwide data will grow to 175 zettabytes.

Maintaining the right level of visibility and control over this data should be a top priority for all organizations across the globe. But doing so is often a major challenge. Why?

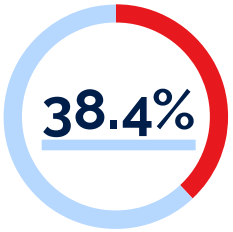
Widespread cloud usage and fast-growing data volumes, combined with hundreds of scratch-built applications and the use of various consumer devices, leave IT and security decision-makers without a clear or accurate view of who inside their organization has access to their data. This is a major problem when it comes to ensuring the security and privacy of your data.



of organizations store data in the cloud.

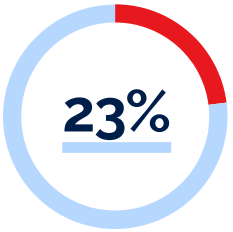
According to new research from Vanson Bourne, commissioned by Virtru, more than **90%** of organizations store data in the cloud. And **84%** have multi-cloud environments, using four or more cloud providers at once. Organizations are managing tens to hundreds of custom applications at once while supporting multiple devices. In fact, many are using an average of **78 different cloud-based applications** every week.

The stark reality is, IT and security teams often don't have a full view of the data moving in and out of their organization, which means they also lack the information needed to protect it against threats—both internal and external. According to cross-industry research, more than 70% of employees have access to data they shouldn't.



Further, IT security professionals are only aware of 38.4% of the applications known to IT administrators.

And unauthorized data access extends to external third-parties—including some cloud providers.



On average, about 23% of the data stored in the cloud is accessible to third-party cloud providers.

This means that nearly one-quarter of your organization's data could be accessible to cloud providers that don't have the sufficient security technology, best-practices or expertise in place to ensure it remains private.

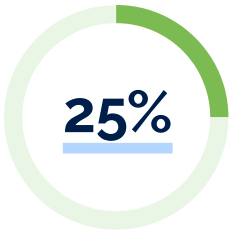
What's Your Sharing Habit?

For **82%** of organizations, sharing data externally is a fundamental part of doing business, with **44%** sharing on a continuous basis and **26%** sharing data daily. Another **13%** share data every hour.

But do you know with whom you're sharing?

say they are most likely to share data with trusted partners.

However, nearly **60%** are also sharing with industry bodies and third-party regulators, another **57%** share with suppliers and finally, **55%** say they share data with customers.



of organizations believe that sharing data with each of these groups is equally essential to their business operations.

So *how* is all of this data being shared?

While **51%** of organizations share data externally via email, **60%** are also using cloud file storage systems like Google Drive, Dropbox, and iCloud. And **52%** say they use file transfer solutions like IBM Aspera and Salesforce Connect. Though these consumer file sharing solutions make it easy to transfer data externally, they don't keep data private and secure throughout its lifecycle.

51%

of organizations share data externally via email.

60%

are also using cloud file storage systems like Google Drive, Dropbox, and iCloud.

52%

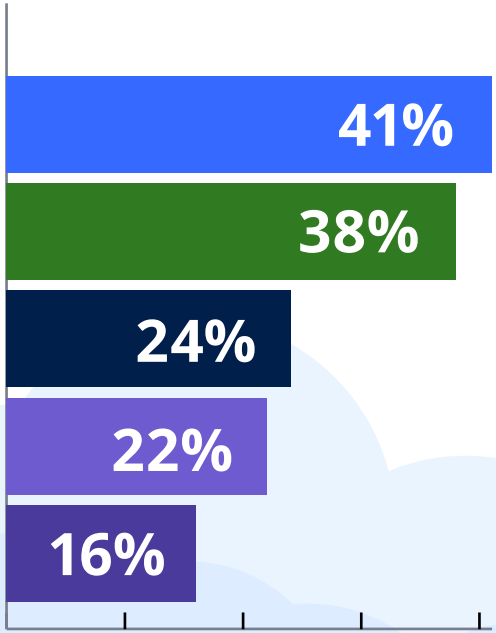
say they use file transfer solutions like IBM Aspera and Salesforce Connect.

Five Data Privacy Challenges in the Cloud

According to research from Vanson Bourne, there are two major concerns when it comes to maintaining data privacy and security in the cloud: Managing data across multi-cloud environments and storing data without the correct level of encryption. Both leave organizations at risk of suffering a data breach or incurring costly penalties for non-compliance.

If you're worried about keeping your data private in the cloud, you're not alone.

Here are the top five challenges facing organizations right now:



Managing data across a multi-cloud environment.

Data being stored without the correct level of encryption

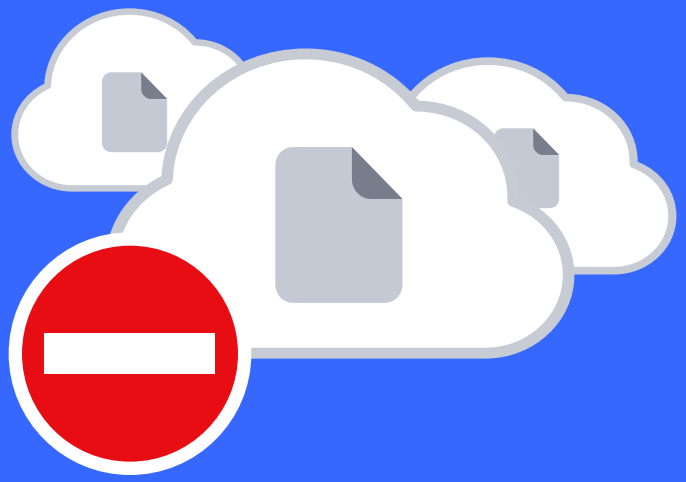
Shadow IT from other departments within the organization

The cloud environment doesn't meet the regulatory standards of the industry.

A lack of understanding of the security protocols being used by cloud providers.

Four Common Cloud Blockers

Many organizations are grappling with the constraints of legacy, on-premises infrastructures, massive volumes of (uncategorized) data, lack of resources, and mounting data privacy regulations. Not to mention, the fact that data needs to be kept private and secure.



Here are four common roadblocks to full-scale cloud adoption:

1. INDUSTRY
If you're in a regulated environment or hold a large amount of intellectual property, you likely can't move all of your data to the cloud due to compliance policies.

2. LACK OF RESOURCES
Many organizations are dealing with shrinking operating margins, limited resources, and a security skills-gap.

3. LEGACY BUILD-UP
Organizations have to sort through mountains of data (sometimes billions of files) to determine what types are in their environment, where it's located, and how it's classified before developing a strategy around where this data can go.

4. FALSE SENSE OF SECURITY
Keeping data on-premises exposes it to pitfalls like human error and outages, not to mention the additional layer of risk associated with a single point of failure.

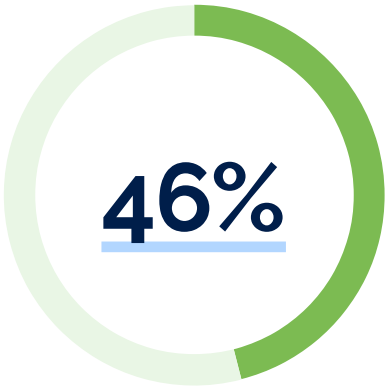
More Organizations are Moving Their Data to the Cloud

You might be wondering how to balance IT security priorities, move data and workloads into the cloud, and keep business operations running.

All while maintaining consistent data privacy and security.

After all, without the right technology in place, there's the risk of being breached; and the consequences can impact the health of your organization. Aside from the potential financial loss, you could suffer from brand erosion, reputational damage, downtime, and the exposure of confidential company information. This could affect not only your bottom line, but also valuable relationships with customers and partners.

This isn't stopping enterprises from cloud adoption.



of organizations are increasingly putting more business data into the cloud.

The top reasons are:

46%

say they need to protect their business data from cybercriminals but also from insider theft, abuse, and misuse.

40%

say that they are concerned about the reputational damage from a data breach or exposure.

38%

view data protection as a corporate social responsibility.

Data Protection Checklist

It's okay to share data—but you need to maintain persistent control over who has access and when.

Look for a vendor that provides:

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

The Impact of Data Sharing

Despite evolving privacy regulations, high-profile data breach incidents, and public sentiment toward data privacy,

54%

are sharing data either slightly or more frequently than they did last year.

But are they doing so safely or leaving themselves open to risk?

When it comes to rising data regulations, the need to train employees on security best practices and making an investment in the right technology infrastructure are top-of-mind for most organizations.

Here's a look at what's impacting organizations that are sharing data on the regular:

QUICK FACT

Sharing data in files, like in the form of email attachments, is commonplace. And this data should be shared. But if files aren't protected with the right level of encryption, they can pose a significant risk to the privacy of your mission-critical data.

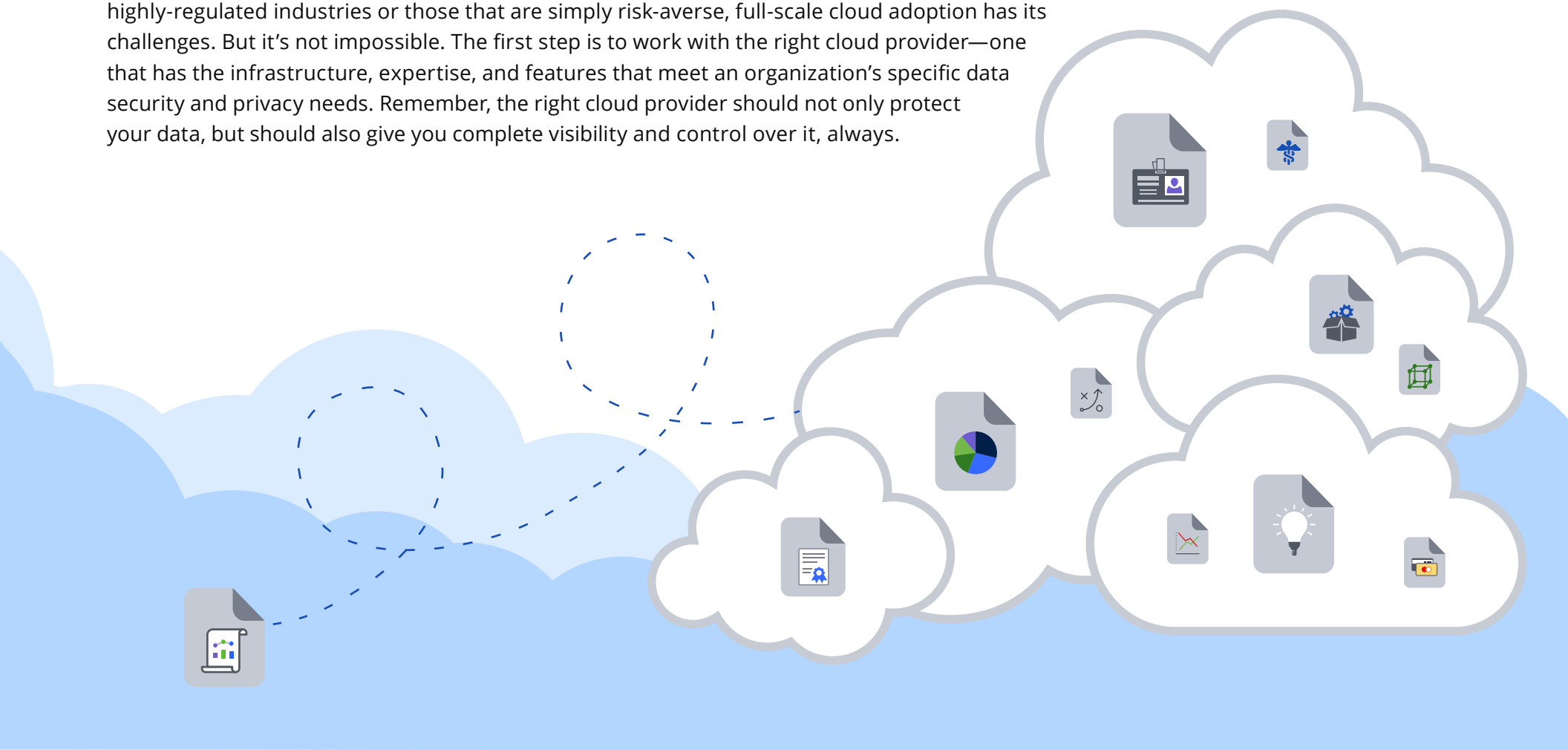
The fact is, 21% of all files in the cloud contain sensitive data, and this has grown nearly 20% year-over-year.

Not to mention, there has been a 53% increase in the volume of sensitive data shared in the cloud.

Make Cloud Adoption a Reality

More small- and mid-sized organizations are taking a cloud-first approach to their business operations, leveraging productivity tools like Google G Suite, Amazon Web Services, and Microsoft Office 365. After all, the cloud comes with benefits such as scalability and increased innovation and effectiveness. Plus, it can help organizations reduce cost, increase collaboration speed, and give employees the ability to share and be more productive anywhere they work.

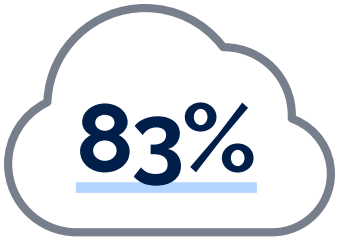
But for many organizations, especially those bound by the constraints of legacy infrastructure, those in highly-regulated industries or those that are simply risk-averse, full-scale cloud adoption has its challenges. But it's not impossible. The first step is to work with the right cloud provider—one that has the infrastructure, expertise, and features that meet an organization's specific data security and privacy needs. Remember, the right cloud provider should not only protect your data, but should also give you complete visibility and control over it, always.



Don't Get Left Behind

Moving your data to the cloud—while keeping it private and secure—can be a reality for your organization.

It's predicted that:



of enterprise workloads will be in the cloud by 2020.

41% of these workloads are predicted to run on public cloud platforms like Amazon Web Services (AWS), Google Cloud Platform, and Microsoft Azure.

20% are predicted to be running on hybrid cloud platforms.

22% are predicted to be private-cloud-based.

On-premises workloads are expected to shrink from **37% today to 27%** of all workloads by 2020. And **Gartner says** to prepare for on-premises email services to "diminish rapidly," stating that: by 2021, **70%** of public and private companies are expected to be using one or more cloud email service.

So where does this leave organizations that can't shake their legacy-first approach?

Remaining entirely on-premises means enabling a single point of failure, which puts your data at risk of being breached, leaked, lost, or corrupted. But it also means you miss out on things like innovation, the ability to scale and grow your business, and easy collaboration and data sharing among your workforce.

Chapter 2

Data Privacy and Encryption in the Age of the Breach

Without a data-centric approach to security—encryption that stays with the data wherever it's created or shared—you're putting the privacy of your corporate information at risk. When it comes to mitigating data breaches, privacy and security need to be synonymous. But what's keeping organizations up at night when it comes to securing their data in the wake of a breach?

Although the list of concerns about the impact of a data breach continues to grow, preparedness to react is lacking. Only **one-third** of organizations believe that they are "completely prepared" to react to a data breach, should one occur. This means **64%** are ill-prepared to react to a breach, perhaps due to the lack of response protocols, appropriate security technology, or expertise to sufficiently react.

Getting Personal With Your Data

Here are **five best practices** that will give you control over your data—and ensure it stays private and secure—at every stage of your cloud journey:

1. CLASSIFY YOUR DATA

Data discovery is an important first step because one, it helps you identify all the places your data is located in your environment, and two, it helps you determine what's too sensitive to migrate based on classification rules. Breaking down your data into four categories of sensitivity—Classified Data, Restricted Data, Private Data and Public Data—will make your cloud migration easier to execute.

2. ASSIGN DATA POLICIES

Once your data is classified, determine what kind of control and protection each tier should receive. For example, consider policies like access control, watermarking, and expiration dates, based on the set level of sensitivity. And only share these controls with authorized users.

3. ESTABLISH ATTRIBUTE-BASED AUTHENTICATION

This will give you the ability to track everything that happens to your data in the cloud and immediately mitigate risk. Security-focused tools like auditability and automatic notifications will allow you to identify anomalies in your environment so you can take action fast—identifying outliers and cutting off access.

4. CONDUCT THIRD-PARTY AUDITS

All it takes is one weak link in your supply chain to expose your data. Some industries, like healthcare, which accounts for **one-third** of all potentially compromised records, are particularly susceptible to value-chain attacks. You can reduce this risk by regularly conducting penetration testing and SOC audits. And don't forget to review and audit your vendors' access and control policies.

5. PICK THE RIGHT CLOUD PLATFORM

Working with the right cloud partner is a critical part of your digital transformation. The key is to find a partner that makes it easy to get started, and more importantly, one that is transparent about their data policies. You should have a clear understanding of what they do with their data, who they share it with and who has access. Avoid "black box" vendors at all costs.

Your Key to Data-Centric Protection

Being skeptical of managing your data in the cloud is okay. Locking yourself into working with a single vendor or, worse, blindly trusting one, will put your data at risk. And when it comes to really protecting your data, securing the communication layer in your environment isn't enough. You have to protect the data itself to ensure persistent and perpetual control.

Three Encryption Features You Need Now

DATA-CENTRIC ENCRYPTION

Data-centric encryption protects the data itself, wherever it is created and shared. This also gives you the power to add or remove access to your encryption keys (versus the data itself).

GRANULAR AUDIT

Granular audit gives you visibility into everything that is happening with your data in the cloud—who is accessing it, how often, and from where. It also allows you to monitor and adapt access controls and privileges as environments change.

ACCESS CONTROLS

Access controls give you the ability to perform advanced actions like scheduled email revocation, watermarking, and the prevention of email forwarding. In addition, you can do things like revoke email attachments but not the email content.

QUICK FACT

Only 9.4% of cloud providers encrypt data once it's stored at-rest in the cloud, leaving it vulnerable to unauthorized data breaches.

It's All About Key Management

The purpose of encryption is to ensure that only authorized users can access your data. This is the only way to truly keep your organization's information private. However, unless you trust how your keys are managed, encryption is virtually useless. Cloud providers, themselves, don't give you complete control over your data and how it's protected. Find a complementary technology solution that gives you this control by owning your encryption keys. By hosting the keys yourself, you eliminate the fear associated with third-party access to your data, as well as the potential for government surveillance and blind subpoenas.

But know that not all key management is created equal.

Encryption At-A-Glance

When it comes to key management, it's important to first understand how encryption in the cloud works. There are two common forms of encryption used today: symmetric and asymmetric.

SYMMETRIC KEY ENCRYPTION ***uses the same key to encrypt and decrypt your data.***

This can be as simple as a user-facing, password-protected PDF or as complex as a software developer platform that allows developers to encrypt their own data and return that same key to other users that want access.

ASYMMETRIC KEY ENCRYPTION ***uses two keys: one to encrypt data and one to decrypt it.***

Anyone can send out an email or file encrypted with the recipient's public key, but only the recipient can read it, since only they have the private decryption key.

While key management is tied to all types of encryption, it plays the biggest role in the asymmetric type, since the creation of multiple keys results in added complexity.

Four Pillars of Key Management

It's no surprise that you have concerns about the privacy and security of your data in the cloud. In 2018, there was **more data stolen** than ever before, with a total of **4.5 billion records** compromised in the first half of the year alone. And intellectual property theft costs U.S. companies as much as **$600 billion each year.**

While encryption is a critical part of data security, it's only as effective as the methods that protect and distribute the keys being used.

Here are four pillars to a comprehensive data security plan:

1. **KEY STORAGE**
Common email and file-sharing providers usually store all keys and content on their servers, which means they can access and read your unencrypted data whenever they want. Asymmetric encryption technologies prevent unwanted third-party access to unencrypted data by keeping encryption and decryption keys solely in your hands.

2. **POLICY MANAGEMENT**
While the primary role of encryption keys is to protect data, they can also add control capabilities to a given piece of content. Policy management allows you to add and adjust these capabilities. You can revoke, expire, or prevent the sharing of the keys, and as a result, the unencrypted data.

3. **AUTHENTICATION**
Since keys enable users to unlock your encrypted data, it's important to verify recipients' identities before granting them access. Authentication verifies who can access encryption keys.

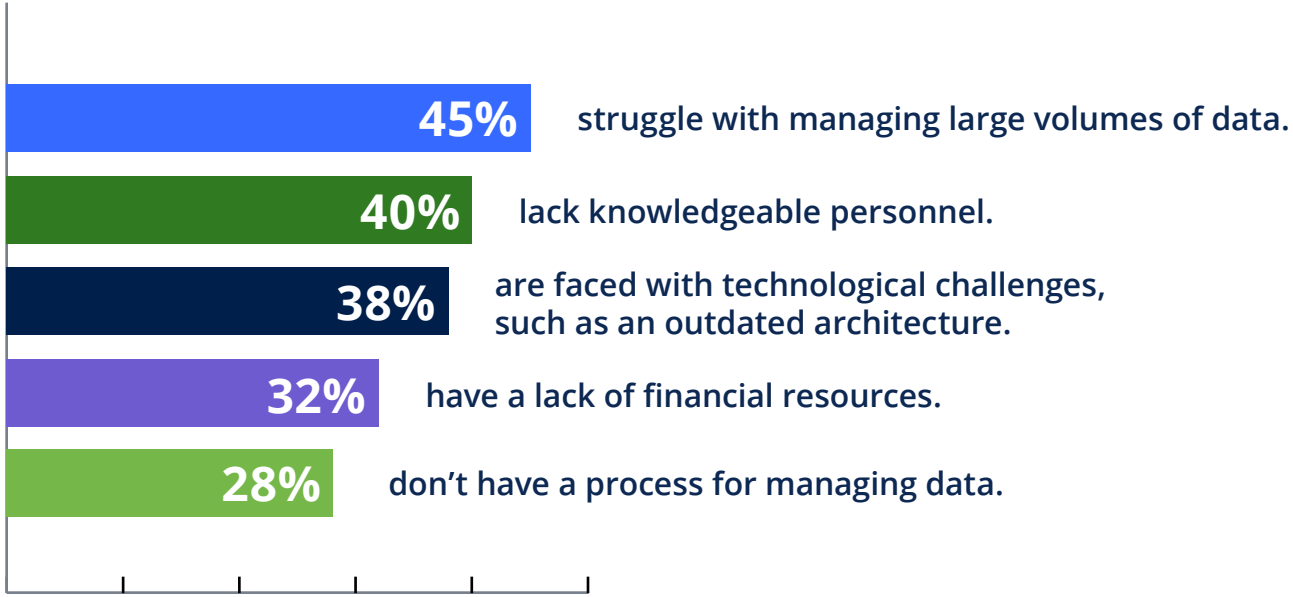
4. **AUTHORIZATION**
This feature verifies the actions that users can take on encrypted data once they've been authenticated. Authorization enforces encryption key policies and ensures that you always maintain control over the data that's being shared.

Chapter 3

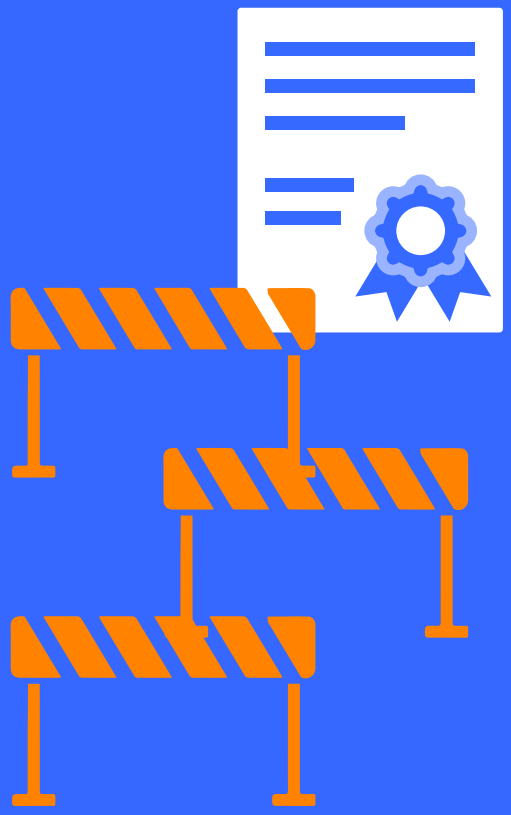
Keeping up with Data Privacy Regulations

Global data regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have changed the way **88%** of organizations approach their data protection strategy. In fact, **72%** say compliance, governance and data regulations are a higher priority now than they were 12 months ago. And for nearly **50%** of organizations, governance, and compliance regulations are among the top-three motivators when structuring their data management strategy.

But keeping up with new and emerging rules and regulations isn't easy. In fact, 90% of organizations say they encounter challenges when it comes to managing compliance, governance, and data regulations:



Six Ways to Overcome Regulatory Hurdles



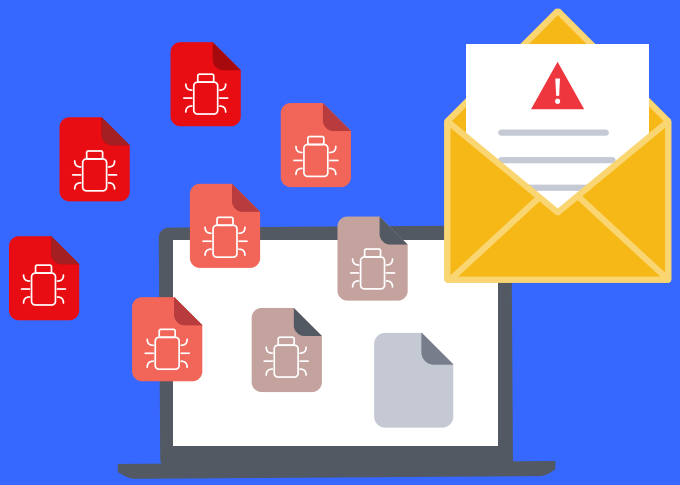
The only way to ensure compliance with the latest data privacy regulations is to join the **99%** of organizations that are already taking action and the **82%** who plan to increase their investment in regulation management.

Here are the top six ways to manage compliance, governance, and data regulations:

1. Consistent staff training.
2. Investment in upgrading security protocols.
3. Hiring experienced data controllers and/or processors.
4. Implementing a data governance tool.
5. Using a centralized strategy for handling data.
6. Hiring a Chief Data Protection Officer or someone to oversee privacy.

Strengthening Your Data Security Posture

Right now, there are more than **50 data breach notification laws across the U.S. alone**, all with different timelines and requirements. Lack of compliance with these laws and regulations could result in fines costing thousands of dollars per violation—or more.



For example, the penalty for not complying with GDPR could cost upwards of $22 million or four percent of an offending organization's yearly worldwide revenue, whichever is higher.

While the fines for these violations may vary, focusing on making them impactful enough to alter behavior toward a stronger security posture will usher in the change needed to keep data private and secure. As the industry shifts toward a universally stronger security posture, the Federal Government has instituted **10 Data Principles** that serve as motivational guidelines in the areas of Ethical Governance, Conscious Design, and a Learning Culture. These principles aim to strengthen the protection of personal information, as well as how information is managed.

It's important to find a data protection solution that both fits into your existing workflow and provides the right technology features, such as encryption, key management, and access controls, to help you safely manage data in the cloud.

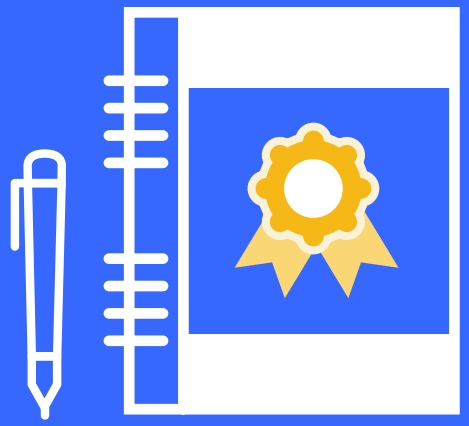
QUICK FACT

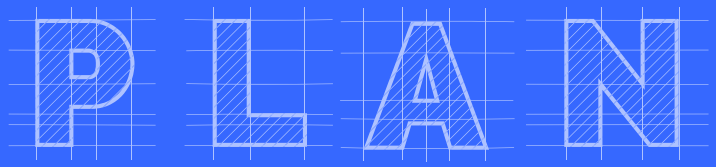
Data, in its many forms and places, is simply hard to manage. And without the right privacy and security technologies in place, it can be a major vulnerability.

In a recent study, Ponemon Institute found that the average total cost of a data breach, the average cost for lost or stolen records, and the average size of a data breach have all increased beyond 2017 averages.

Not only could a breach cost you an estimated $3.86 million, but there is a nearly 30% likelihood that you'll experience not one, but two, data breaches over the next 24 months.

How to Build a Compliance Readiness Plan





1. INVENTORY YOUR DATA

Identify what data you have in your environment, where it's located, and where it goes.

2. IMPLEMENT AUDIT AND CONTROL CAPABILITIES

Make sure your systems are equipped with these features so you can perform discreet access and enable better security of the data as it moves inside and outside your organization.

3. DEVELOP AN INCIDENT RESPONSE PLAN—AND TEST IT

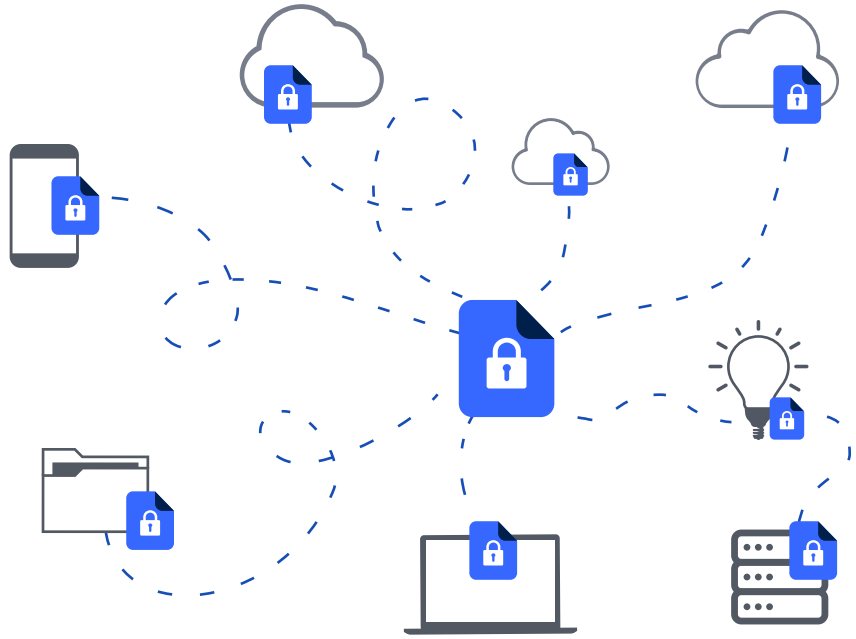
Breach notification requirements can be hours or a few days, so having a working response plan in place is essential to determine what data has been compromised.

4. PRACTICE DATA MINIMIZATION

Only maintain data as long as necessary and only keep what you need. By keeping only what you need, the impact of a breach could be less severe.

The Bottom Line

No matter where you are in your cloud journey, there's still time to improve your relationship with your data. Sure, there will be challenges along the way. But this shouldn't be to the detriment of your business operations. Becoming familiar with your data and knowing all the places it resides, along with implementing the right security technology—and a compliance readiness plan—will give you the agility needed to respond to adverse cyber events while maintaining data privacy and integrity.



Here are four rules to live by to keep your data private and secure in the digital workplace:

1. Implement **data-centric protection** to ensure cloud vendors and other unauthorized parties will not be able to access proprietary data.
2. Only work with a cloud provider that offers **customer-hosted key management** to maintain direct control of the data you have stored in the cloud and block unwanted access.
3. Establish attribute-based **access controls** to ensure proprietary data is only accessed by authorized collaborators and remains private, wherever it's shared.
4. Look for the ability to perform **granular audit** for visibility into who has accessed your data, and when.

Learn more about how Virtru secures the digital workplace: virtru.com/contact-us

At Virtru, we protect data throughout its lifecycle, helping to prevent unauthorized access while enabling secure sharing across environments, applications, and devices. Our Data Protection Platform, built on the Trusted Data Format, enables organizations to integrate data protection into their products and applications. IT and security teams can leverage the Platform through our Email Encryption, Enterprise App Protection and Google Drive Protection solutions. And, via the Virtru Developer Hub, developers can embed platform-agnostic data protection into custom applications or connected devices. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.