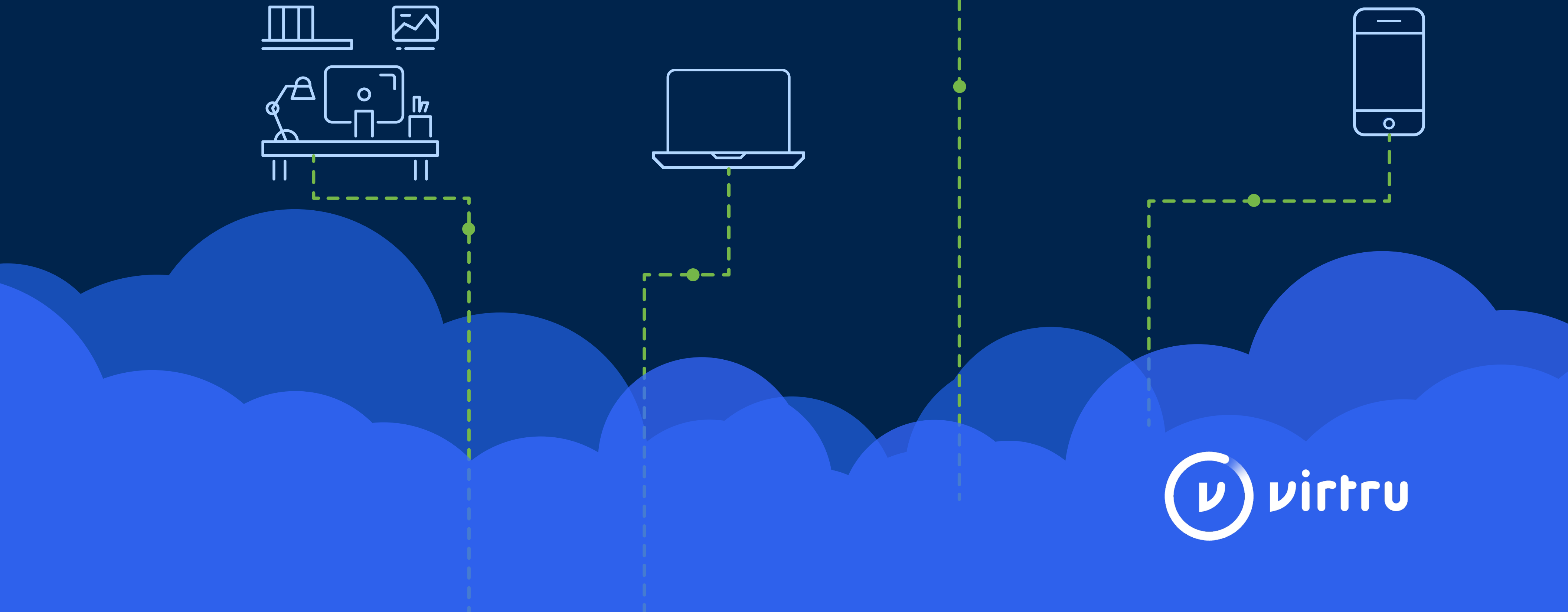
Improve Your Relationship with Data

How to Embrace Collaboration and Build Trust in the Cloud

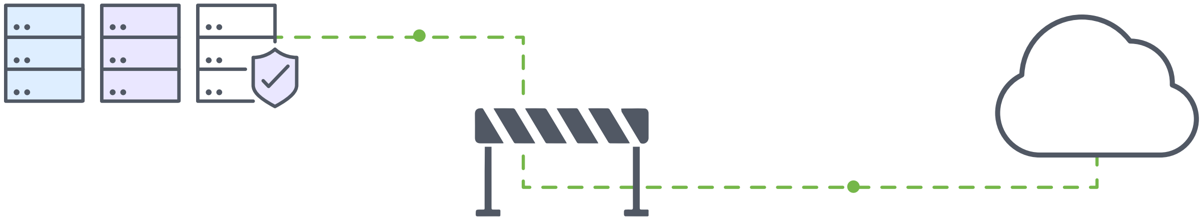


virtru

Table of Contents

Chapter 1

Cloud Data Blockers



You have a love-hate relationship with data—and you're not alone. 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. Data is alive inside and outside of your environment, flowing through seemingly limitless places, from devices and email systems to third-party networks and beyond.

Four Common Cloud Blockers

Many enterprise organizations are grappling with the constraints of legacy, on-premises infrastructures, massive volumes of 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**
Enterprises have to sort through mountains of data (sometimes billions of files) to determine what types are in their environment, where it's located and whether 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.

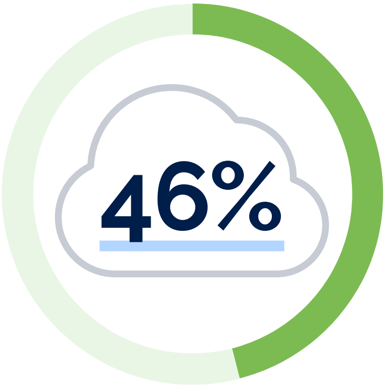
More Enterprises are Moving Their Data to the Cloud

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 effect 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.

Strengthening Data Controls

Data can be your most valuable asset or your biggest liability. Do you know who, inside your organization, has access to it? According to cross-industry research, more than 60% of employees have access to data they should not.

This increases the likelihood of a breach, leads to rogue data sets propagating in silos and results in IT security leaders that are unaware of the potential points of exposure.

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

Many enterprises will develop in-house applications to address their data-sharing challenges and associated customer service and workforce productivity needs.

- More than 90% of enterprises have at least some internal development resources and close to 45% of them develop exclusively in-house.
- Organizations with fewer than 1,000 employees run an average of 22 custom apps, while large Enterprises with more than 50,000 employees run approximately 788.

DATA PROTECTION CHECKLIST:

If your in-house development team doesn't have the cryptographic expertise to build data protection capabilities, that's okay. You can work with a proven third-party vendor that you trust. Look for:

- ✓ Consistent policy enforcement across disparate environments
- ✓ Persistent control as data is shared
- ✓ Automatic key and policy management
- ✓ An easy user experience
- ✓ Software Development Kit

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.

Breaking Through Legacy Barriers

If your data is being stored in either a hybrid environment or on-premises, you're missing out on important cloud benefits like scalability and increased innovation and effectiveness—all while reducing cost, increasing collaboration and giving employees the ability to share and be more productive.

Plus, keeping all of your data on-prem is risky and complex.

Like many risk-averse organizations, you're likely seeking the savings and digital transformation benefits that the cloud can offer while also focusing on the need to eliminate the risk of blind government subpoenas and lost IP.

What you really need is trust. Trust that a cloud provider truly has the features, infrastructure and expertise required to keep your data private and secure. But how do you cross the threshold of placing enough trust in the right cloud provider and remain in control of your data?

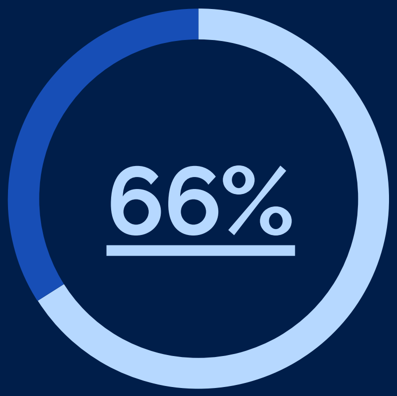
Ask yourself this:
"Do these features meet my specific data privacy needs?"

If you’re faced with extensive governance mandates or certain regulatory needs that require more control and visibility features than mainstream cloud providers can offer, you can work with a third-party cloud security vendor to complete your data protection solution.

The right vendor will have capabilities such as extending internal privacy and security assurances to data that leaves its premises, ensuring that enterprise data remains protected throughout its lifecycle.

You have options. So, what’s holding you back from a full-scale cloud adoption?

DID YOU KNOW?



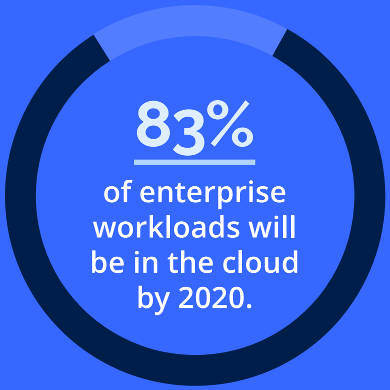
of IT professionals

say security is their most significant concern in adopting an enterprise cloud strategy.

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:



83% 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.

22% are predicted to be running on hybrid cloud platforms.

20% are predicted to be private-cloud-based.

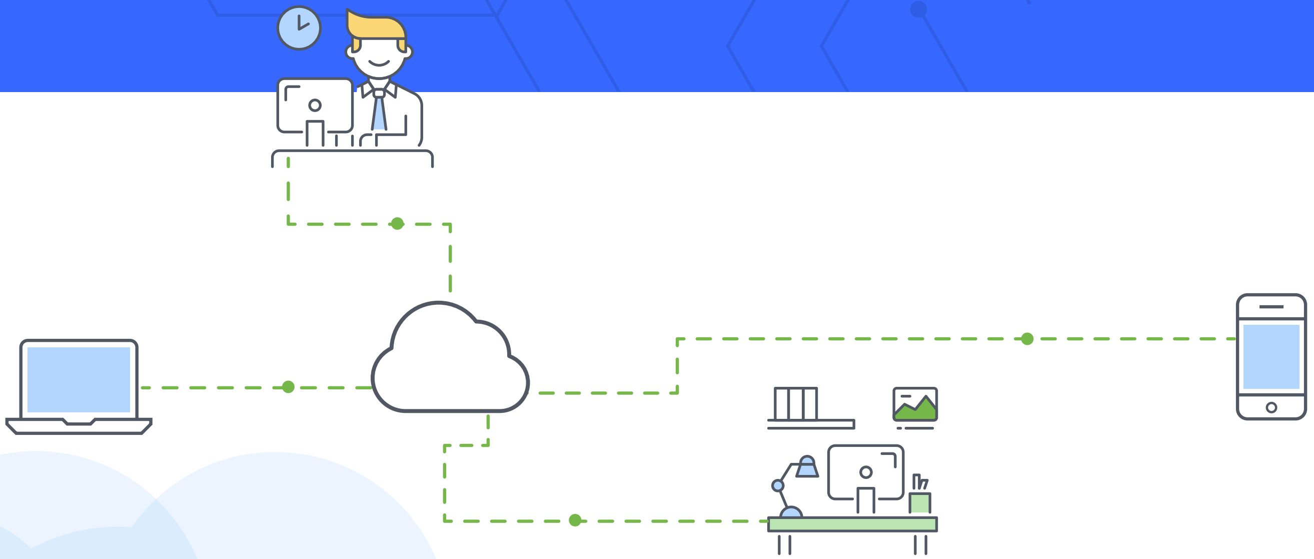
On-premises workloads are expected to shrink from 37% today to 27% of all workloads by 2020. And Gartner says to prepare for on-premises email services to “diminish rapidly,” stating that: by 2021, 70% of public and private companies are expected to be using one or more cloud email service.

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

Getting Personal With Your Data



A digital transformation sounds great, right? First, you have to get to know your data better: where is it located; what can be migrated to the cloud and what is required to stay on-prem; who has access; and what are normal data patterns?

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, like 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. Things like 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 of it.

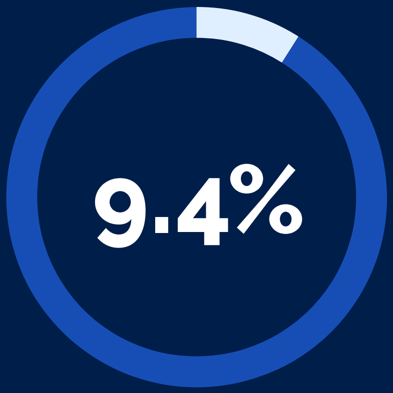
Three Encryption Features You Need Now

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

2 **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.

3 **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.

Work with a cloud provider that gives you complete control over your data and how it's protected.

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.

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 **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.

3 **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.

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

Be Prepared for Data Privacy Laws

As the cybersecurity landscape continues to intensify, and as threat actors become more sophisticated, the need to keep data private and secure is paramount. This is why data privacy policies, mandates and regulations apply to organizations across the globe, regardless of industry or size.

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.

These mounting data privacy regulations underscore the importance of knowing where your data is located, what your data classifications are and how to track the data.

CALIFORNIA CONSUMER PRIVACY ACT

One of the most influential upcoming data protection laws is the California Consumer Privacy Act (CCPA), which will take effect in 2020. Similar to the European Union General Data Protection Regulation (GDPR), which took effect in 2018, the CCPA will require any company doing business in California (with more than $25 million in revenue), or handling the data of 50,000 or more California residents, to have consumers' personal data readily available upon request, with rights to opt-out should a breach occur.

How to Build a Compliance Readiness Plan

1 **KNOW YOUR DATA INVENTORY**
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.

Four Data Privacy Rules to Live by

When it comes to your data in the cloud, stop worrying about blind subpoenas, government surveillance, unauthorized access and even loss of visibility and control. Just remember these four data privacy rules to live by and you'll be on your way to a successful cloud journey:

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.

Schedule a demo.

About Virtru

At Virtru, we understand that data is an organization’s most valuable asset and sharing it is critical for business success. But sharing data creates significant risk. We believe no one should have to choose between protecting data and sharing it. We help more than 5,000 organizations, large and small, across almost every industry, protect data wherever it’s created or shared so they can collaborate with confidence. Virtru provides the power to get the job done. For more information, visit www.virtru.com or follow us on Twitter at @virtruprivacy.

virtru