The Complete Guide to BUSINESS PRIVACY

Your Organization's Greatest Responsibility – and Opportunity

The Complete Guide to BUSINESS PRIVACY

Your Organization's Greatest Responsibility—and Opportunity

In this guide:

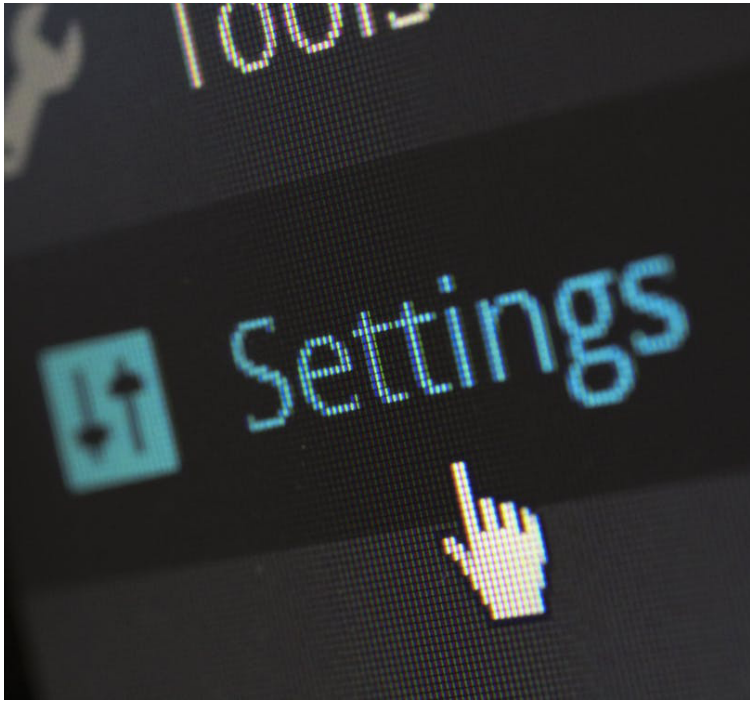
There Is Not a Single, Perfect Security Solution.

If you've read cybersecurity white papers before, you know what to expect: frightening stats, an explanation of why things are so bad, and then, the "perfect" solution: that company's cybersecurity tools.

But that's not really how things work. The right set of tools can make breaches less likely, less damaging, and less costly—but no single technology solution is a substitute for a strong, layered security strategy.

Your technology stack exists to support business leaders and their cybersecurity strategy. Regardless of your tech stack, you will still need to train and retrain your staff about good security practices. You still need to stay vigilant against new risks and work with compliance monitors to mitigate those risks as much as possible.

And you'll probably experience a data breach at some point. Nearly every company does. That's why it's important to be realistic and prepared.



Privacy Is Your Responsibility—And Your Advantage.

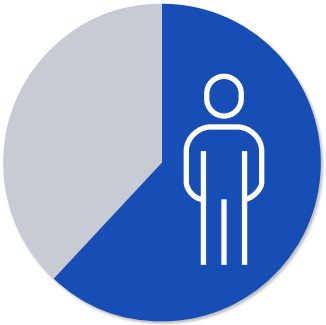
Your ecosystem of partners, clients, and other stakeholders recognize that their data becomes vulnerable when it leaves their hands. In a recent Pew Research survey, 62% of respondents said they believe it's not possible to go through daily life without companies collecting data on them—and 81% believe they have very little or no control over the data companies collect.

The same survey found that 70% of respondents feel their data is less secure than it was 5 years ago, and roughly 30% report having experienced some kind of data breach in the past 12 months.

It's clear that the public doesn't have a lot of trust in the way companies collect and use their data. So your organization can set itself apart by giving your customers and partners the assurance that their data is kept private and secure when it's entrusted to you—and this can be a huge competitive advantage.

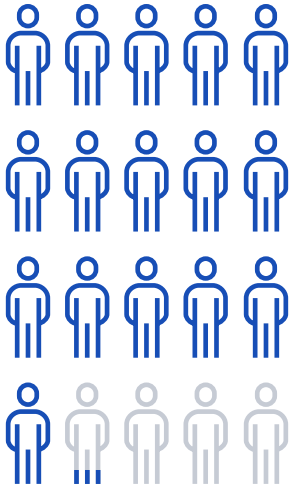
62%

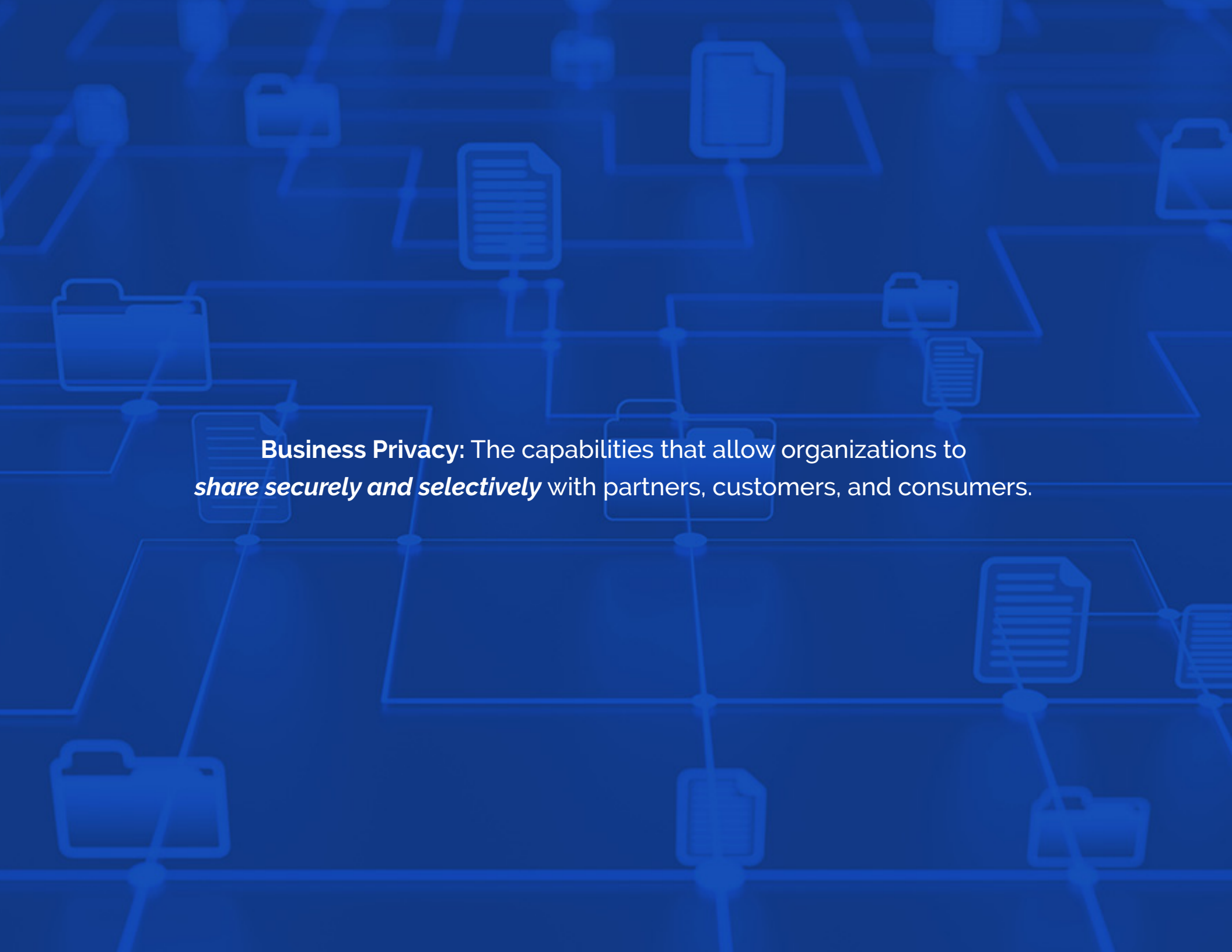
believe it's not possible to go through daily life without companies collecting data on them



81%

believe they have very little or no control over the data companies collect





Business Privacy: The capabilities that allow organizations to ***share securely and selectively*** with partners, customers, and consumers.

By trusting you, your clients and partners make their privacy your responsibility.

So what's going on? If customers question the way companies collect and use their data, why don't they take matters into their own hands? Because they feel that it's not manageable to maintain full control over their data.

It's certainly daunting for an individual to take back control of their data when so many companies have collected it. A 2020 NordPass survey found that the average internet user has 100 account passwords across websites. Presumably, if consumers have taken the time to create these accounts, they also store personally identifiable information such as address, phone number, or payment card data.

Consumers generally feel powerless against potential cyber attacks and breaches, but at the same time, they know that they have to use online businesses and social media to participate in the modern world. So, they wall off their fear and trust that companies will do the right thing to keep their data safe.

By trusting you, your clients and partners make their privacy your responsibility. And if your company has a serious privacy breach, they're going to see it as your fault, even if it's not.

But there's an upside to all of this. If you can proactively protect your customer and partner data rather than simply reacting when breaches occur, they will stick by you. If you rise to the occasion while others do the bare minimum to meet compliance regulations, you'll be a champion of your department, a champion of your industry, and a champion of consumer rights.

Business Privacy: The Challenge of the Cloud Era

The data you hold is valuable because it's not just *your* data. It belongs to your clients, your shareholders, and your partners, too. Each information source and group that requires certain data access presents new security and ethical challenges. You need to serve customers without breaching their financial or personal data, maintain HR records without compromising employee privacy, and work with partners while keeping their trade secrets confidential. Each use case presents an opportunity to honor a stakeholder's trust or betray it.

Internal data is every bit as important and just as tricky to safeguard. Your corporate strategy or a piece of intellectual property might be shuffled among dozens of lawyers, consultants, executives, office workers, contractors, and other stakeholders. Unless you have a system that gives access to all of these parties while always keeping out unauthorized outsiders, your data remains vulnerable.

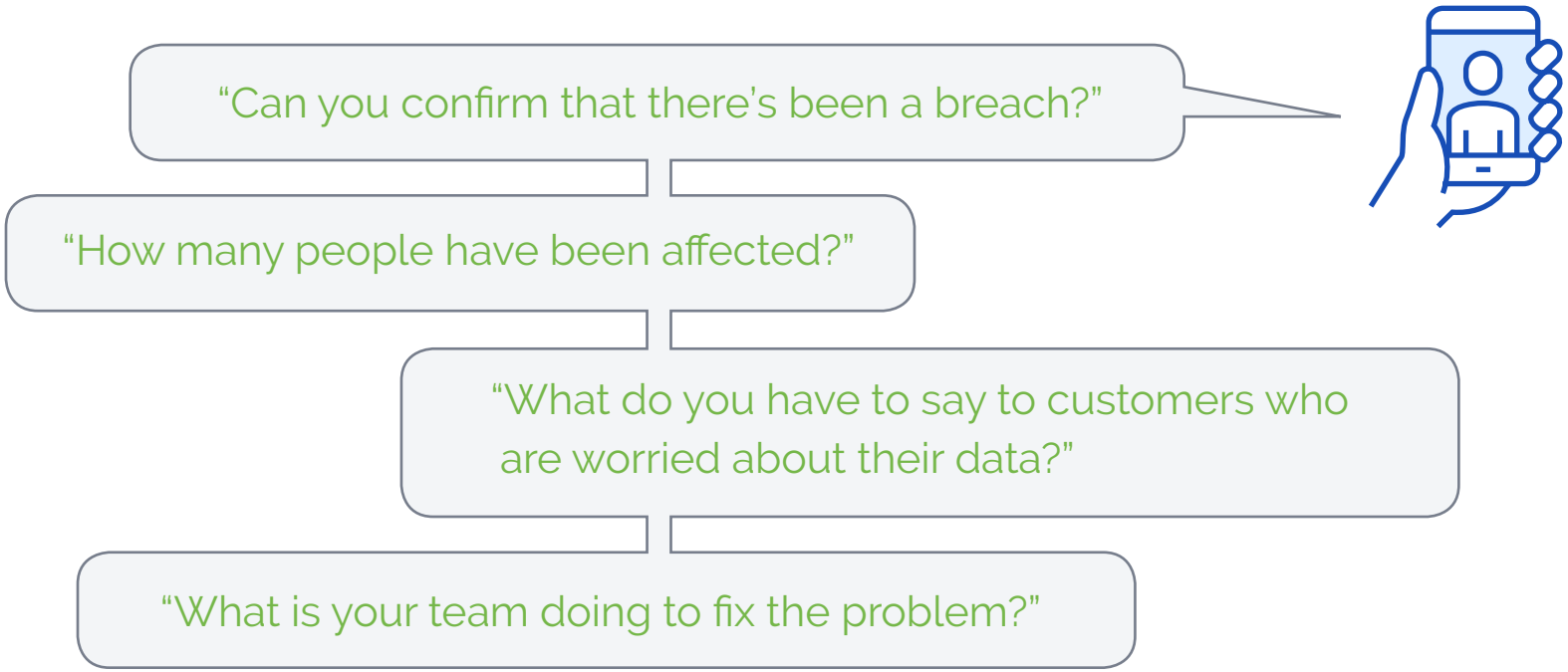
Many business challenges ultimately boil down to business privacy—for example, your organization's ability to collect sensitive information, consume it, and share it quickly without exposing it to hackers or third party providers.

Business privacy encompasses your duty to enable protection of, control over, and easy access to sensitive data. Organizations that embrace business privacy—those that secure their data without compromising existing workflows—will lead the way. The rest of this guide will show you how to get there.

Each use case presents an opportunity to honor a stakeholder's trust or betray it.

Part 1:
Real-World Threats to Business Privacy

Imagine you're at home getting ready for bed, when you get a call from a reporter. What looks like a cache of sensitive customer data has been leaked and exposed.



You get off the phone as quickly as possible, then call your security team to find out what's going on. Apparently, this is the first they've heard of it, too.

What Could Have Happened? Your team runs through some possibilities:

- An employee could have accidentally leaked the data.
- A malicious insider could have intentionally leaked the data.
- A hacker could have gained access to employee email accounts.
- A hacker could have intercepted an email sent between two employees, or hacked the connection while an employee was accessing your database.
- A cybercriminal could have exploited a security vulnerability caused by a third party with access to your data. This could be the company hosting your files, your internet service provider, a partner, a client, or even the maker of an unapproved app installed on one of your employee's computers.

That's not a complete list—not even close. And many cyber attacks don't have one clear entry point.

Regardless, the consequences of breaches will catch even the most prepared companies off guard. According to IBM, the global average cost of a breach is $3.86 million. Costs such as damage to brand reputation, future heightened regulatory scrutiny, and legal fees are hard to predict. Regulatory bodies and courts have long memories, and the presence (or absence) of past breaches could determine whether a future incident is treated as an act of negligence.

With the average employee sending more than 10,000 emails every year, data flows in and out of organizations at high velocity. It's not unlikely that a breach could have been caused by a careless email or inadvertently shared file. To calculate just how much data your organization shares via email, use Virtru's Data Sharing Calculator.

The global average cost of a breach:

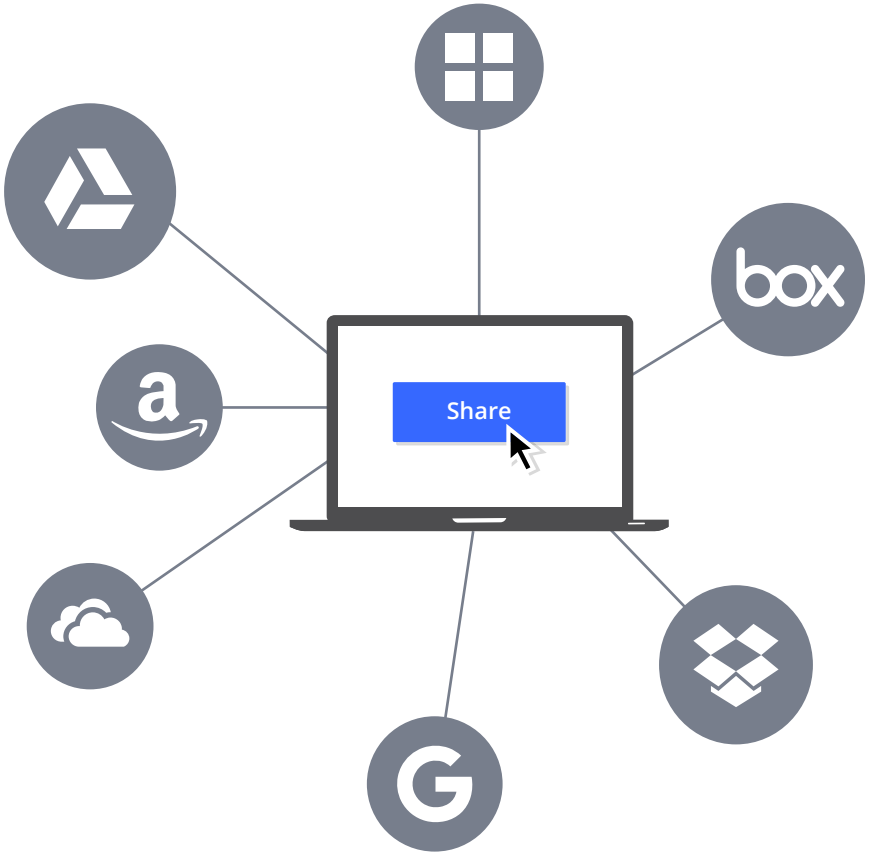
Can Organizations Trust Cloud Providers?

Everyone who can access your data can potentially breach your data, and that includes your cloud service provider. Encryption protects against this danger by scrambling your data into an unreadable form. So long as a party doesn't have access to both the data and the keys protecting it, your information is more likely to be safe.

However, providers that encrypt your content usually control both the data and the key for unlocking that data. This isn't done for any nefarious purpose, but rather for convenience. It allows your provider to protect your data from outside attacks, while automatically unlocking it for you when you need it.

But this also means that your cloud provider can read your data in plaintext (unencrypted) form and have full access to it. This access creates an unnecessary business privacy risk for your company, partners, and clients. It also inhibits your ability to comply with certain compliance regulations, such as Criminal Justice Information Services (CJIS), International Traffic in Arms Regulations (ITAR), and data sovereignty requirements.

For more information about protecting data in the cloud, read Virtru's data sheet, Meet Data Sovereignty and Maintain True Privacy for Data Stored in the Cloud.



A Breach of Data Privacy is a Breach of Rights

“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”

-Universal Declaration of Human Rights

Privacy isn’t just an economic necessity — it’s a fundamental right. When customers purchase your products, they’re trusting that you can protect their financial data and identities. When partners collaborate with you on sensitive projects, they’re working under the belief that you can keep that project safe from competitors, the press, and the public. When new employees submit their passport, health data, and bank account information to HR, they’re depending on your internal controls to keep their most private data confidential.

If you fail to safeguard that data, you’re not just creating risks for your clients or extra costs for your company. You’re betraying the trust that encourages people to do business with you.

Most businesses try their best to protect cybersecurity internally, but your customers and partners don’t care how much work and money you put into cybersecurity. They judge your brand by the success or failure of your programs.

And the old programs are broken.

Part 2:
Why Business Privacy Matters More Than Ever

Business privacy is critical in a changing digital landscape, particularly as workforces have become more widely distributed. While organizations continue to evolve the ways in which they communicate and share information, their data security approaches often fail to keep pace, and the world has taken notice.

As a result, there are several ways that data can be left vulnerable. Among them are:

1. **Attacks against your internal organization and infrastructure.** Hackers can target your employees directly on the tools they use to access the internet—and their methods have become increasingly sophisticated and believable. That puts your own internal data, strategy documents, and communications at risk.

2. **Attacks against infrastructure that you use but don't own.** For example, if you outsource billing and your financial partner has their email hacked, it can compromise your data. Similarly, if your email travels across a misconfigured server on the way to your partner, a hacker can intercept the data on the way. In a world where so much information travels via email and thousands of cloud-based SaaS apps, this presents a lot of opportunity for data to be put in the wrong hands.

3. **Attacks against other organizations that have ties to your employees or customers.** If someone in your organization is affiliated with another company, hackers may target them through their email account, a device owned by that group, or some other vector, gaining access to your proprietary data in the process.

   Executives, board members, investors, and other high-ranking figures involved in your organization can be especially vulnerable to this collateral damage, since they're more likely to be connected to targeted organizations. Additionally, they may themselves be targets of a hacker with an axe to grind, such as a hacktivist or disgruntled associate.

4. **Attacks against common human error.** We've all accidentally sent an email to Mike S. instead of Mike P., or perhaps forwarded an email thread without checking all the previous messages for sensitive data. The easier it is to share information, the more damage you can do by accidentally sharing it with the wrong person. Open your mouth at the wrong time, and you might give away a valuable secret to one person. But email a confidential spreadsheet or report to the wrong group or individual, and you've potentially compromised thousands of records — and given the recipients the power to share those records with the public.

Lessons in Business Privacy: Data is Not Just Shared via Email - Protecting Video Data

Surveillance camera footage represents some of the most sensitive data available. In addition to enabling businesses to capture video footage of their properties, security companies also provide video cameras to families, some of which capture the interior of their homes.

In early 2021, two major breaches targeted security camera footage: One impacting Verkada, a U.S. enterprise building security company, and another incident in China where hackers gained access to thousands of videos from private security cameras, including footage of families in their homes, and travelers in hotel rooms.

Sensitive data is everywhere, whether it's contained in a database, an email correspondence, a file, or full-motion video. What types of sensitive data are entrusted to your company?

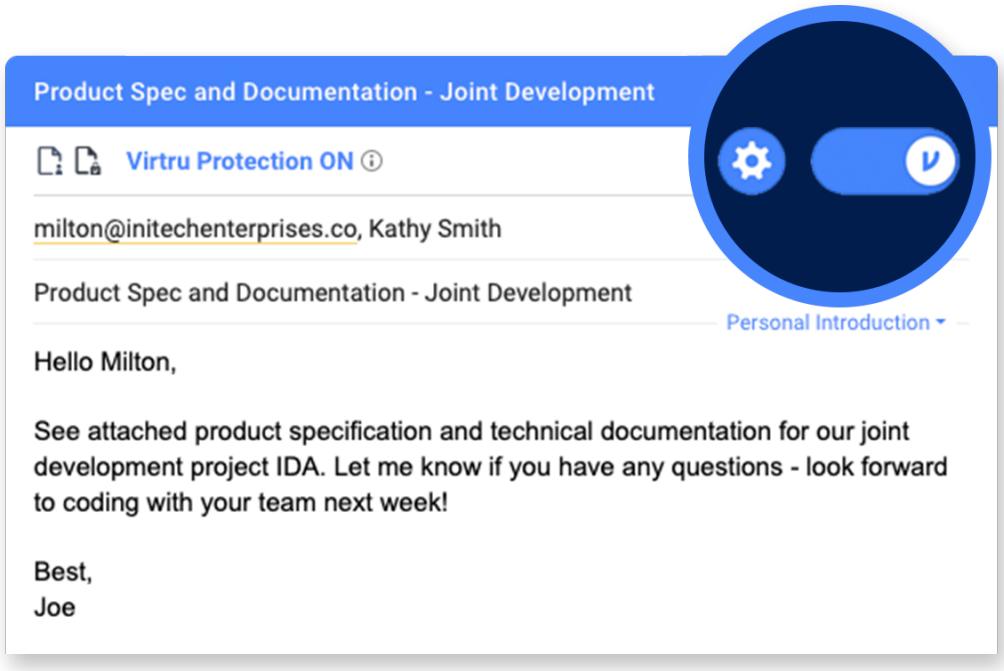
Part 3:

How Virtru Empowers the Sharing of Data

Virtru is a cloud-based, data-centric security platform that empowers organizations and governments to protect and share data as they wish without losing control of that data—anywhere and everywhere.

The company provides an overlay of originator-controlled data encryption, access control and key management to protect highly sensitive data in any environment—auditable and revocable at all times.

Virtru's pioneering technology, the Trusted Data Format (TDF), is an open data tagging and encryption standard used by over 6,000 Virtru customers globally.



How Virtru Data Encryption is Different

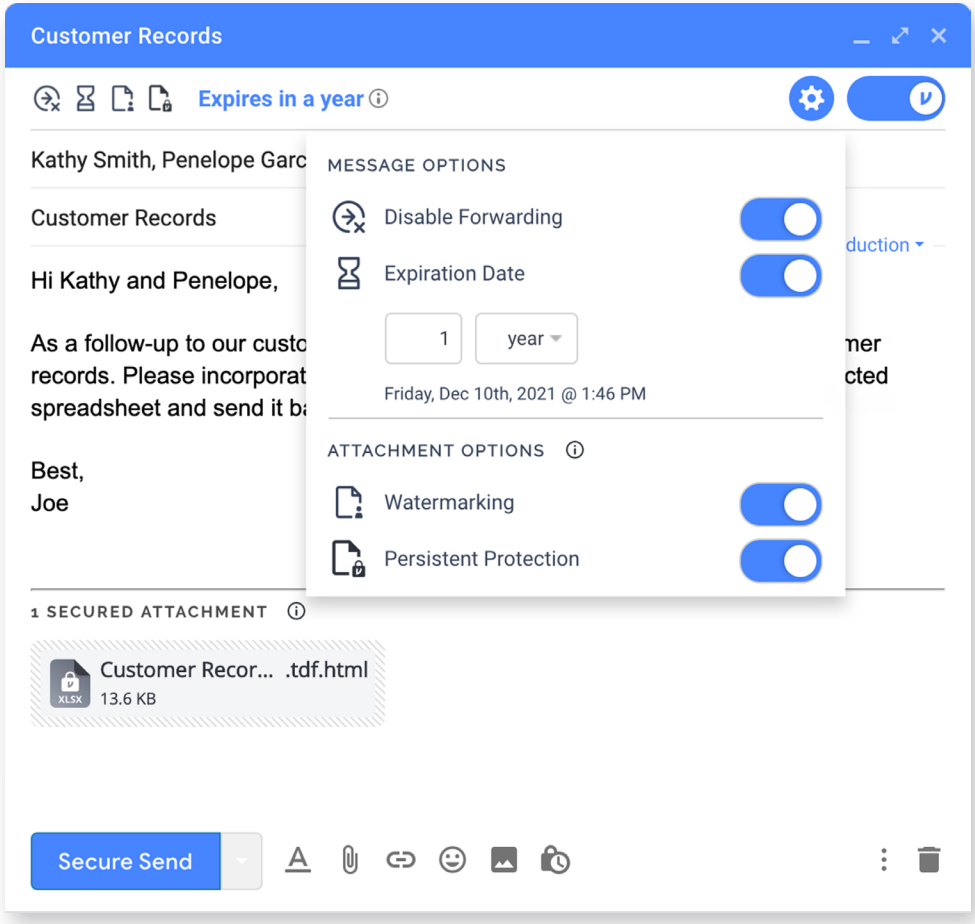
1. **Protect your data at the object level, everywhere it travels — not just the perimeter:** Virtru uses data-centric encryption to protect your files and emails across their entire digital journey. Each piece of data is encrypted before it leaves your network, and only decrypted when the intended recipient opens it.

   Content is stored and transmitted separately from the encryption keys that protect it. This means that even if hackers intercept your emails and files, they can't access them because they won't have the encryption keys.
   This split-knowledge architecture is critical for organizations looking to comply with Health Insurance Portability and Accountability Act (HIPAA), CJIS, or EAR requirements that restrict third party access to sensitive data.

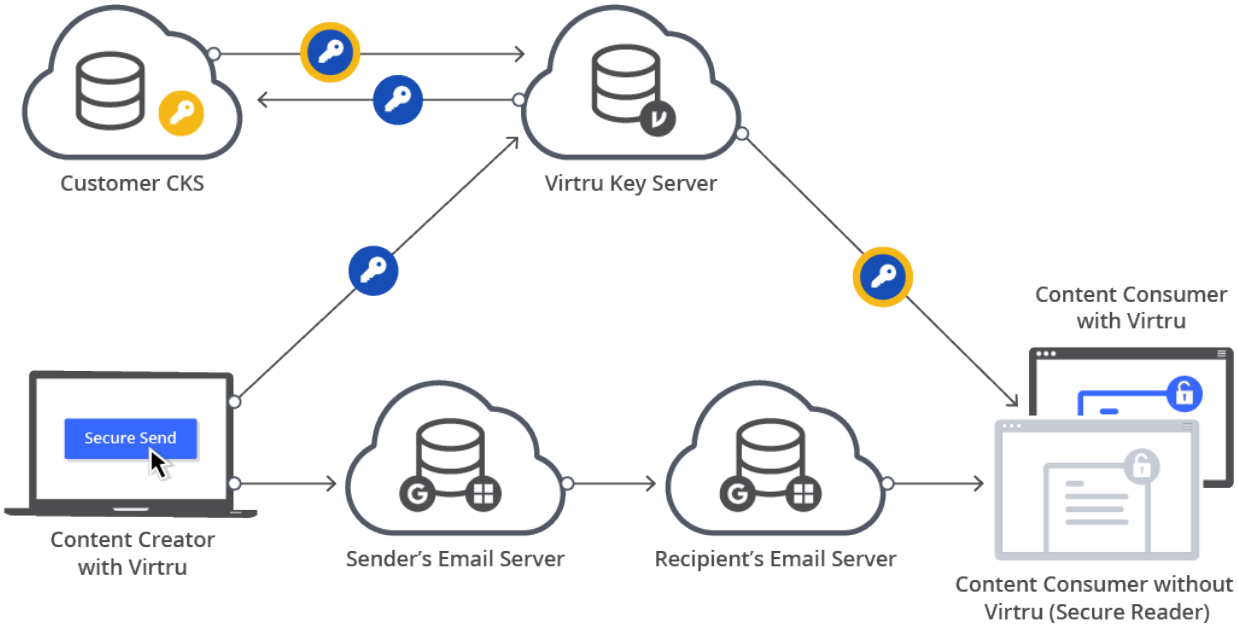
   Most importantly, this means there's no single point of failure. It doesn't matter that you can't protect the whole perimeter, because the data itself remains safe across its whole journey.

2. **Share data without undermining your ability to protect it:** It's common that you lose control over your data when you give it to someone else. Whether you're handing someone a file or sending an email, once this data leaves your hands, you have to trust external parties to protect it.

   With Virtru, that's no longer the case. You always control who can access your keys, which means you always control who can access your data. If you send an email or attachment to the wrong person, you can revoke access to prevent them from reading it in the future – even if they've already read it. You can also set time limits, after which your recipient will lose access, or disable forwarding to prevent them from passing on sensitive content to other recipients.



3. **Use the cloud solutions of your choice while maintaining full control over your data:** By separating the storage location of encryption keys and content, Virtru's encryption enables you to leverage cloud-based platforms while ensuring your data remains protected. For the highest level of protection, you can manage your own keys on premise or in a private cloud. Even though cloud providers have access to customer content, this content is encrypted and providers do not have access to the encryption keys. The only people (besides you and your organization's administrators) who can unlock your data are the recipients you've selected.



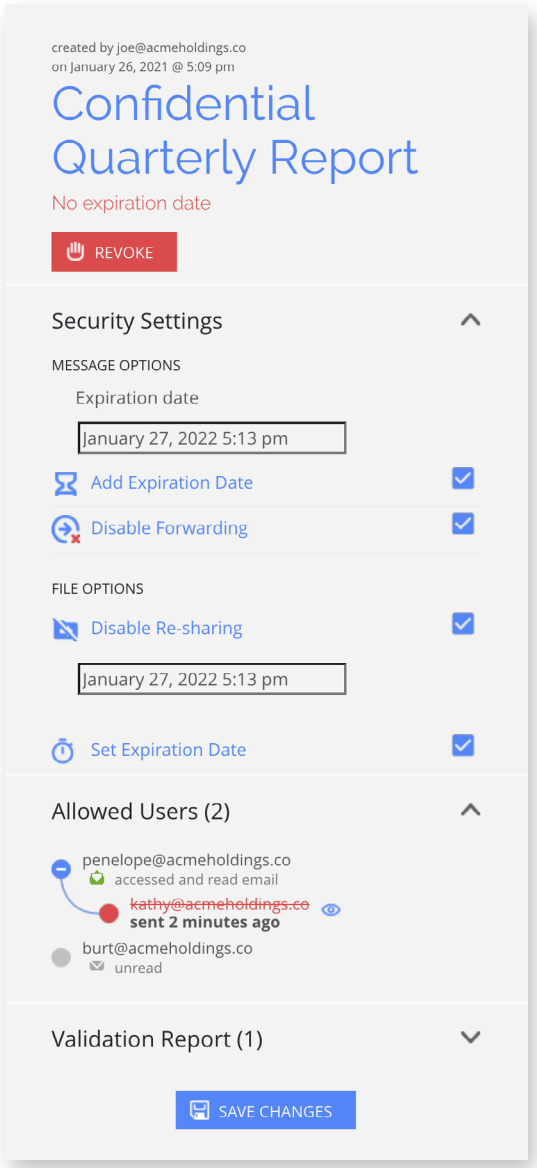
In the case of a breach—when so many questions are up in the air—it's invaluable to know exactly who has viewed and shared the data in question.

4. **Eliminate the struggle to get your customers to comply:** Instead of forcing new programs and technologies on customers, Virtru lets you work with the tools you already use, such as Gmail, Google Drive, Microsoft Outlook, iOS, and Android. Virtru allows customers to receive, read, and reply to encrypted Virtru emails without installing new software or creating new credentials.

   Recipients can reply using their existing email accounts, and even send secure responses with attachments with a few clicks. This greatly increases adoption rates over secure portals and traditional email encryption tools. It also means you can send secure messages to prospective clients, new partners, and others who may not have a secure communication tool available.

5. **Improve visibility and control:** Virtru allows employees to monitor and control access inside and outside of the organization. When a recipient accesses encrypted data, Virtru lets the sender know. Even if a message has been forwarded or sent to multiple recipients, the sender can see exactly who has opened the message.

   Combined with tools like message revocation and forward disabling, this visibility provides a powerful tool to address potential breaches. If senders revoke a message before it is opened, Virtru provides proof, averting breach notification. If unintended recipients have already accessed your data, Virtru becomes a powerful tool for breach mitigation. You can prevent recipients from opening or sharing content in the future and isolate your mitigation specifically toward those recipients who have already gained access. In the case of a breach—when so many questions are up in the air—it's invaluable to know exactly who has viewed and shared the data in question.



The Future of Business Privacy

The future of business privacy is data-centric. Organizations no longer have to choose between securing their data and sharing their data. With Virtru, they can achieve both, with confidence.

By protecting business privacy, you can harness the full power of the cloud while protecting customer trust. Those businesses that can lead the way will be rewarded.

To learn more, contact us today to start the conversation.

virtru

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 6,000 customers trust Virtru for data security and privacy protection. For more information, visit virtru.com or follow us on Twitter at @virtruprivacy.