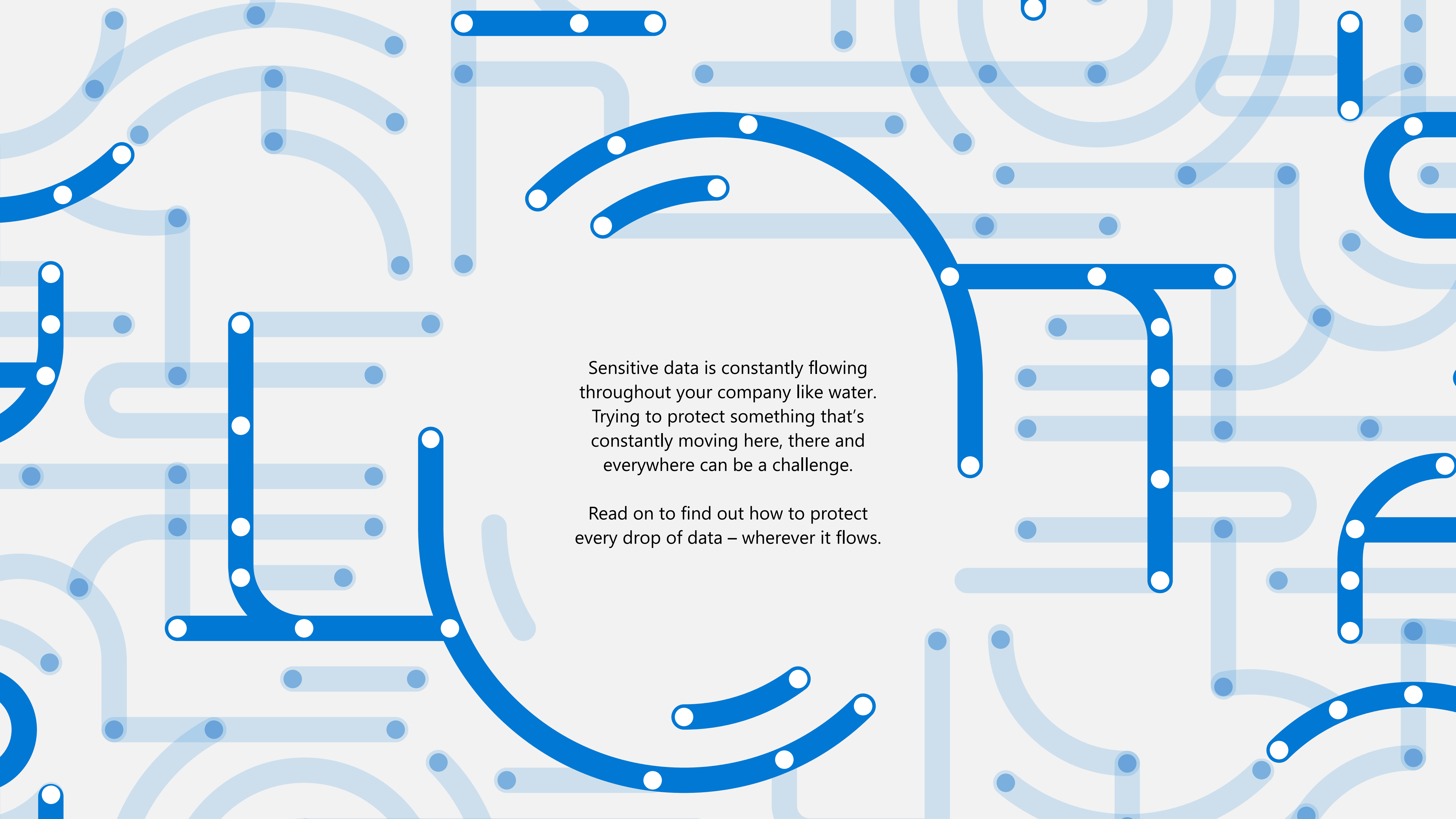


# Protecting Data Together

A team playbook for securely handling your company's data



The background is a light gray color with a complex pattern of blue and light blue lines. These lines are of varying thicknesses and are mostly curved, creating a sense of movement and flow. Some lines are straight, while others form loops or zig-zags. Small white dots are placed at various points along the lines, particularly at bends or endpoints, resembling data points or nodes in a network.

Sensitive data is constantly flowing  
throughout your company like water.  
Trying to protect something that's  
constantly moving here, there and  
everywhere can be a challenge.

Read on to find out how to protect  
every drop of data – wherever it flows.

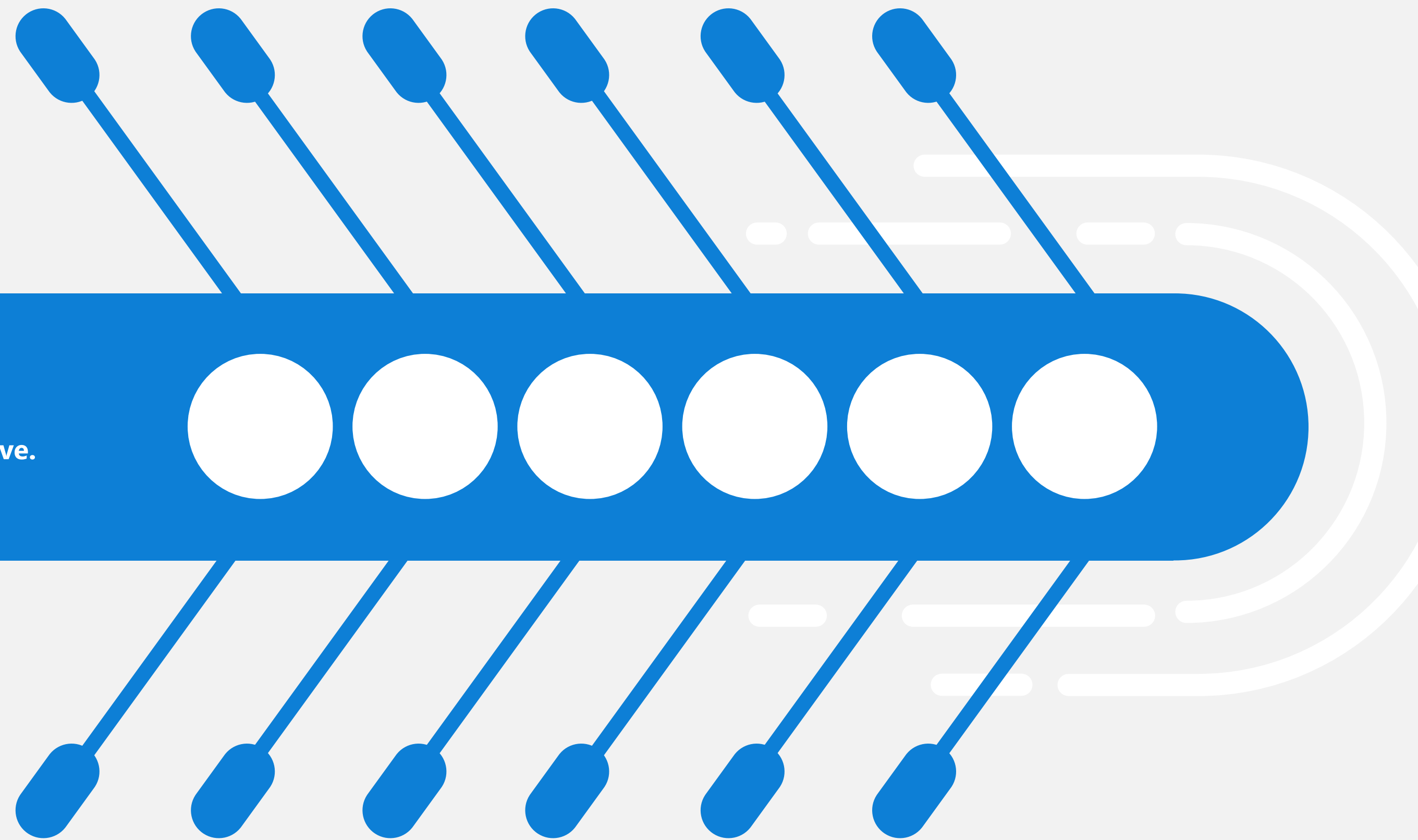
# All hands on deck

It's easy to think that data protection is someone else's job. But safeguarding critical data is a team effort requiring everyone in your company to row in the same direction.

**74%** of employees said they would be willing to bypass cybersecurity guidance if it helped them or their team achieve a business objective.

– “[Gartner](#) Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025”, February 23, 2023

Some of the biggest data breaches in history were the result of an employee, a team or a supplier just trying to “get the job done.” But getting things done should never come at the expense of your organisation's security. Working *the right way* means understanding where your data is, how to handle it and how to protect it – at all times. **We'll show you how to get started.**



A stylized illustration of a grey faucet on the left side of the image. Water, represented by blue vertical bars and circles of varying shades, is dripping from the spout. The background is a solid light grey, and the bottom of the image features a solid blue horizontal bar.

# Data, data everywhere

It's 10:15 a.m. on a Monday. You've already responded to 15 emails, finished a report with a coworker, performed five web searches and been in three different online meetings. Just then you hear a *Ding!* and look over at your phone. Nancy, a vendor, asks you to send over a spreadsheet that your manager shared with you. Should you send it? Why or why not? And if you do, what's the safest way to do so?

Your company's security team thinks a lot about these kinds of questions. And it's a big task. They're responsible for managing and protecting a never-ending flood of spreadsheets, emails, photos, documents and more – a deluge of data that gets bigger by the day.

**But they can't do it alone.** Why? Because protecting data is a team effort – the responsibility of every single person in your company. How you handle certain types of data in the moment could have no impact or it could yield disastrous consequences. And knowing the difference will make all the difference.

# Protect your data, wherever it flows

We've all heard we're supposed to protect data, but what exactly does that mean? What's included in "data" and how do you protect this thing that is often out of sight and out of mind?



**Data is information created by people and machines that's converted into a form that can be processed, shared, stored, interpreted and turned into value for your company and your customers.**

Your data is constantly on the move. It's created, deleted, stored, shared and used on computers, phones, USB drives, security cameras, printers, cloud storage, email and apps. Data takes countless forms including text, numbers, video, voice, images, emails, spreadsheets, strategy documents, employee records, customer names and credit card information.





# Stop the **ripple** before it starts

You don't have to be an expert in security, but you should embrace a mindset of constant care and watchfulness. Most of the people you'll share data with have good intentions. But controlling where your data travels will go a long way towards protecting your company from unintentional mishaps, violations of government and industry policies and potential attacks by bad actors. Government and industry data security standards can be strict with significant consequences if you fail to follow them. If you do business across international borders, the stakes can be even higher. We recommend talking to your legal and security teams to find out what measures you need to take to meet these standards.

Here are some common scenarios that illustrate how ordinary decisions can turn into a small leak or a big breach. These are all honest mistakes that could have been stopped before they started.

**A manager is working from a coffee shop and signs in to public Wi-Fi without following company security policies, such as using a VPN.**



**An attacker, using the same public Wi-Fi, manipulates network activity and tricks the manager into disclosing their email credentials. The attacker then downloads all of their emails.**



**An executive on a flight reviews a presentation deck for a highly confidential product launch without protecting their screen.**



**The people around the executive see the presentation, and the launch is leaked to the press and to competitors.**



**An employee connects a third-party software application to their corporate Microsoft 365 account. They quickly skip over the setup screens, granting the software near limitless permissions.**



**The application records the "file names" of all files opened by the employee and stores them in an improperly managed cloud storage medium that is easily accessed by hackers on the open internet.**



# Don't drop your guard

You and your colleagues are like front doors to your company's data, so it's important to be vigilant. Sometimes people make mistakes that lead to a leak. Other times, cybercriminals will actively come after your company and try to get their hands on your most sensitive data.

Some of the biggest data breaches in history started when people were just taking care of business as usual and making small decisions in the moment. But those decisions resulted in extraordinary damage to their companies.



**A top US-based retailer became the victim of one of the largest data breaches ever, with hackers accessing the credit and debit card information of around 40 million customers. This breach was traced back to a heating, ventilation and air conditioning contractor that was working in some of the retailer's stores and had access to the corporate network. The hacker stole the contractor's credentials and used them to access the retailer's systems. The rest is history.**

## Vendors and suppliers are on the team, too

Do you work with vendors and suppliers? As we saw with the retailer breach, hackers love to go after third parties who have access to their clients' networks and use them as a back door to steal company data. This is why it's critical that you hold them accountable to your company's standards for data handling. Reach out to your legal and security teams to find out how you can do this through your contracts and processes.





# Don't take the bait

Your company's sensitive data is a lucrative target that outside bad actors would love to get a hold of. Phishing is one tactic that is often used by cybercriminals who disguise themselves as people or organisations you can trust.



Phishing attacks are designed to steal or damage sensitive data by deceiving people into revealing sensitive data. Attackers use email, social media, texts and other methods to try and get you to take actions that could open the door to your company data.

## **Attackers generally use one or more of the following tactics...**

- Convincing you to open an attachment containing malware that they could use to grab your data
- Enticing you to click on a malicious link that enables them to break in and steal sensitive data
- Tricking you into signing into a service – for example a fake, but highly realistic, Microsoft sign-in page – that gives them direct or indirect access to company data

## **Signs someone might be phishing for secrets...**

- Emails from people you don't recognise, especially from someone outside your organisation (look closely at email addresses to be sure)
- Threats or urgent calls to download an attachment or click on a link
- Generic greetings, such as "Dear sir or madam"
- Suspicious links or unexpected attachments

**If you suspect you're being targeted by one of these attacks, reach out to your security team.**



Every single time you handle data,  
it should be second nature to **see**  
it, **label** it and protect it





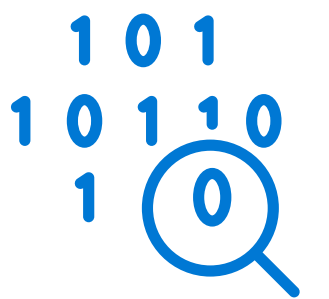
# See your data

A lot of your data is hidden away in dusty digital folders in email, in the cloud or on your phone. In fact, **42% of organisations said at least half of their data is "dark,"** meaning it's collected but unused. Leaving this data unattended can be incredibly risky. But it's hard to protect what you can't see, especially when data is constantly moving, growing, being shared or being deleted.

— July 2022, [Enterprise Strategy Group](#), 2022 State of Data Governance and Empowerment Report

## Making it practical

Here are three critical questions you can answer to get a clear picture of your data:



### Where does all your data live?

Is it in your inbox, deleted items, browser downloads, in the cloud, on a thumb drive in your rucksack or somewhere else?



### Who is the appropriate audience?

Is it for your entire company, for a restricted internal audience, for customers only or for the public?



### How is this data being used or shared?

Are people collaborating on it, sharing it over email, presenting it or forgetting about it and leaving it untouched for years?

# Label your data

Now that you have a clear picture of the data you're dealing with, it's time to label it. Your company likely has a policy you can follow to label your data appropriately so you can protect it from loss, misuse or access by someone who is unauthorised. Does it contain details, plans and discussion of products or services that haven't been released yet? That likely means it should be labelled Confidential when you share it. Or is it the final version of a product support document? Then perhaps this data is something you can label Public.

## Making it practical

You're just about to send off an email to your leadership team and to vendors with a presentation attached.

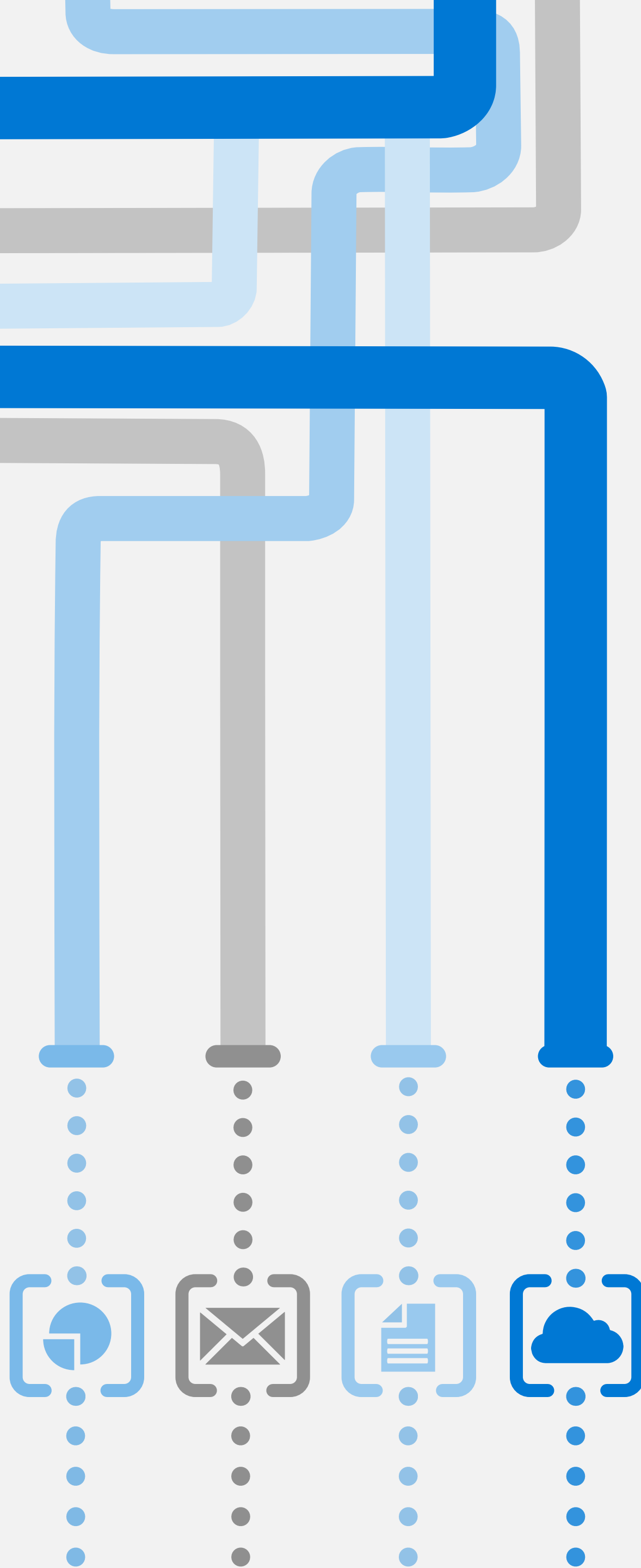


### You pause for a moment to consider how to label it:

*Public, General, Confidential or Highly Confidential.* You recall the company training that says this should be Confidential, so you label the presentation that way.

You press "send," and now this Confidential label will travel with the email and presentation wherever it goes.

If everyone else on your team does their part, this classification will help every person who handles it to immediately understand how to manage it with the appropriate level of care.

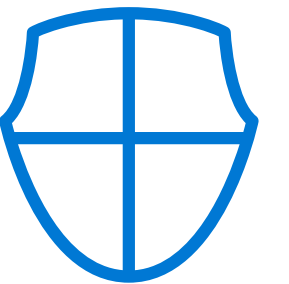


# Protect your data

You've identified your data and have classified it – now it's time to protect it. Whenever you handle data, take a few extra seconds to think through how to handle it and then take the appropriate steps to safeguard it. **The best way to get started is to learn and always apply your company's data protection policies, including:**

- What data you need to protect and who is allowed to see it
- Where data should be stored and how it can be shared
- Who can modify data or destroy it
- What to do when things get out of hand

## Making it practical



### Are you working on a flight or from a coffee shop?

Protect your screen from nearby gawkers and follow company policies to securely connect to your corporate network, especially if you're using public Wi-Fi.



### Need to use software that isn't on the approved list?

Reach out to your manager or to IT for permission; you don't know where that software provider might publish or store your data.



### Are you creating a new password?

Use your company's password manager to keep all your usernames and passwords under lock and key instead of under your keyboard.

# Ride the **wave**

Now that you know the basics, it's time to put these principles into practice. Remember that staying on top of data protection is a team effort.

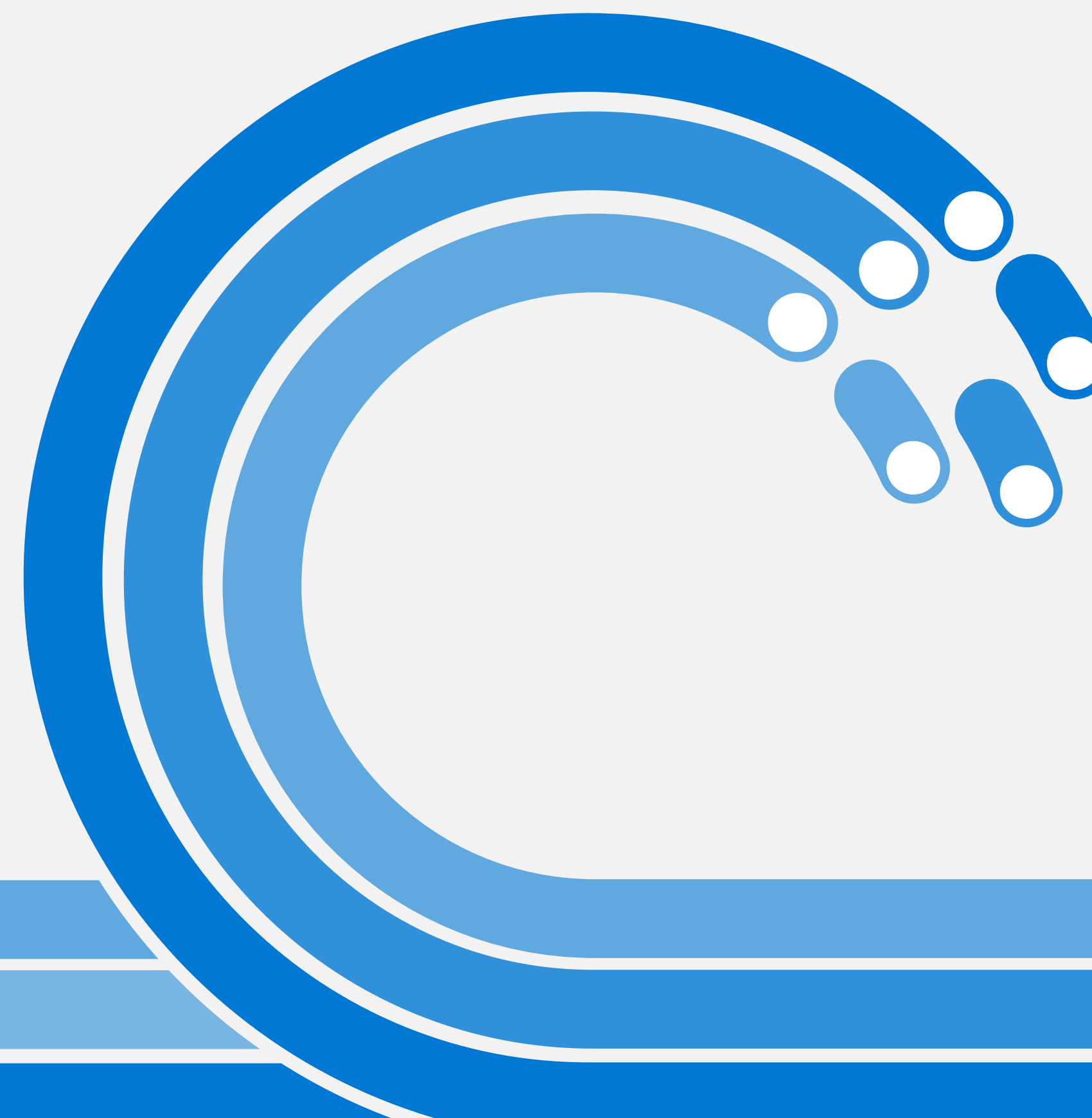
## Here are some simple ways to build momentum and protect data wherever it flows:

- Share this playbook with a coworker and help keep each other accountable.
- If you see anything suspicious or make a mistake in sharing your data, don't ignore it. Report any concerns to your security team right away. Sweeping a potential issue under the rug is never a safe approach.
- Every time you're about to create, share, save or delete data, get in the habit of pausing for five seconds to consider how to apply your company's security policies.

**69%** of employees have bypassed their organisation's cybersecurity guidance in the past 12 months.

— [Gartner](#) Predicts Nearly Half of Cybersecurity Leaders Will Change Jobs by 2025", February 23, 2023

**40%** of respondents in a McKinsey survey ceased doing business with a company when they found out the company did not protect customer data.

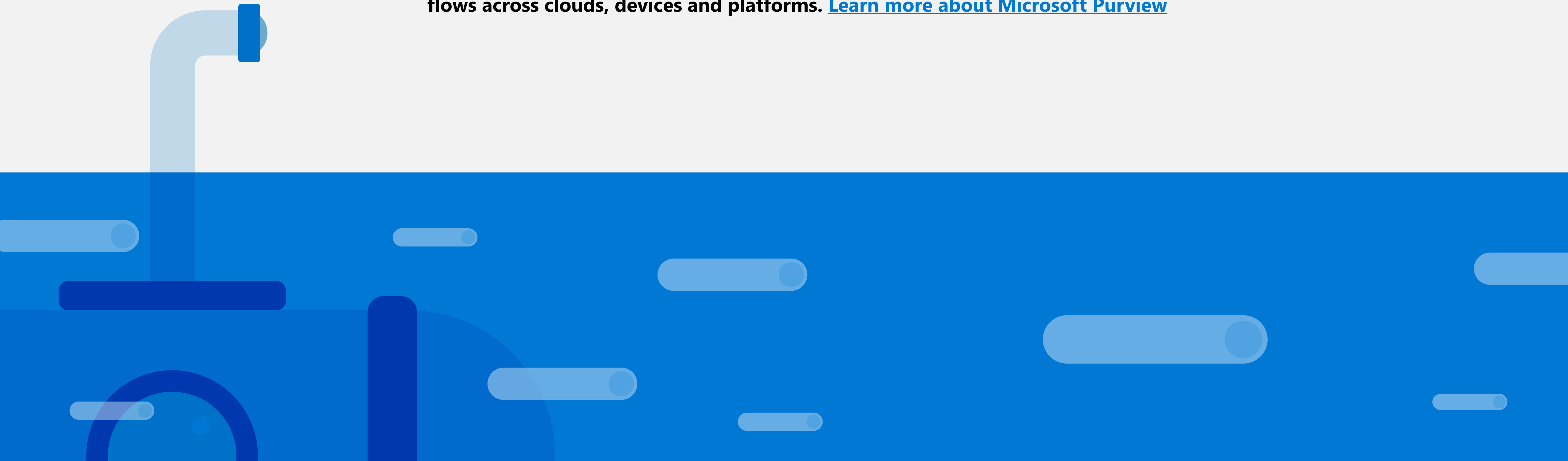




# Keeping a watchful eye

If you're a security leader, we recognise that your job is likely harder than ever with the shift to hybrid work, an explosion of endpoints and a deluge of data. If you'd like to increase visibility into your data, govern and safeguard it more effectively and improve your risk and compliance posture, we'd like to help.

**Microsoft Purview can give you greater peace of mind by helping you secure and govern your data as it flows across clouds, devices and platforms. [Learn more about Microsoft Purview](#)**





GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

©2023 Microsoft Corporation. All rights reserved. This document is provided "as-is". Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.