Software

Shadow IT: **The hidden apps putting your organisation at risk**

www.breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms
Empowering You Through Secure Technology

You could probably name the main technology your organisation relies on without giving it much thought.

Your email, accounting software, CRM, Microsoft 365 and perhaps a few systems specific to your business or school.

But what about the other apps and online services being used across your organisation that you might not even know about?

An employee might use a free file-sharing service because sending large files by email is awkward.

Someone might find an AI tool that helps them with a repetitive task.

A team could start using an online app to organise work because the system they already have feels slow or cumbersome.

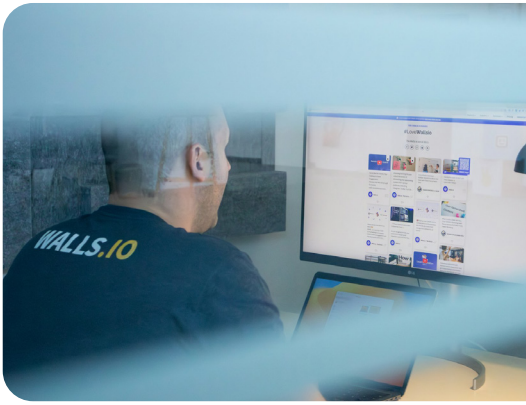
This is known as **"shadow IT"** – technology being used for work that isn't formally approved or managed by the organisation.

IIn most cases, they're simply trying to solve a problem. They've found something that makes a frustrating task easier or saves them time.

The concern is that the wider organisation may have no idea the app exists, what information people are sharing through it, or who has access.

Something that saves one person a few minutes could create a much bigger issue elsewhere. And when different people start making these decisions independently, it becomes harder to keep track of the technology your organisation relies on.

How shadow IT gets into an organisation



It used to be much harder to introduce new technology into an organisation.

Software had to be purchased, installed and configured. Usually, someone responsible for IT would be involved somewhere along the way.

Now, an employee can find an app online and start using it within minutes.

They might create an account using their work email address, add a browser extension or sign up for an AI service. If the free version does what they need, there may not even be a purchase for the organisation to approve.

This makes it easy for people to find their own solutions to everyday frustrations.

Perhaps someone is struggling to share a large file, so they upload it to their personal cloud storage and send a link.

A team might start using a free project management tool because their existing system makes it difficult to keep track of work.

Someone who used a particular messaging app in a previous job might introduce it to colleagues because they already know how it works.

And AI has made this even easier.

If an employee discovers a service that can summarise a document or help with a repetitive task, it's understandable that they might want to use it. They probably won't see it as introducing new technology into the organisation.

But shadow IT can also tell you something useful about the technology you've already provided.

When people repeatedly look elsewhere for better ways to do their work, there may be an underlying frustration that hasn't been addressed.

Perhaps an existing system is too cumbersome, two pieces of software don't work well together, or employees simply don't realise that a tool like Microsoft 365 already includes the feature they need.

Finding unapproved apps is vital, but understanding why somebody felt they need them can be even more useful.



One app can quickly become **a much bigger problem for your organisation.**

The difficulty with an unapproved app starts with what gets put into it.

A tool that starts as a convenient way to organise a task can end up holding customer details, internal documents or notes about ongoing work.

An AI service might be given information from a report because someone wants help summarising it.

A file-sharing service could gradually become the place where an employee stores documents they need to access from different locations.

Before long, your organisation has information stored in places you may not even know about.

There can also be connections to other systems.

Many apps let people sign in using a Microsoft or Google account, or ask for permission to access files, emails, contacts or calendars.

Clicking 'Allow' is easy, but it can give an external provider access to parts of your organisation's systems and information.

And that access can remain in place long after the employee has stopped using the app.

Ownership can become muddled too.

If an account was created by one employee, using credentials only they know, important information can become tied to that person.

This can cause problems if they leave the organisation and nobody realises that a process or collection of files depends on an account they set up.

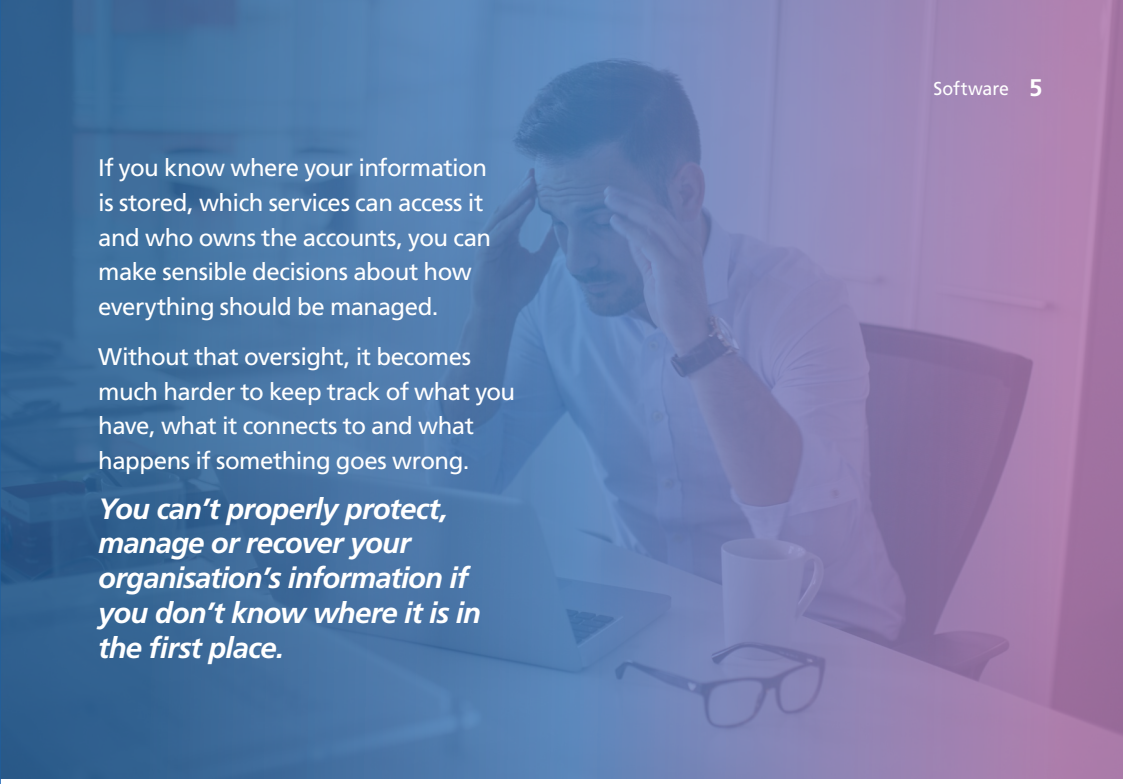
Then there's the money being spent.

One department may be paying for a project management tool while another has subscribed to something similar.

Employees might also put relatively inexpensive subscriptions through company cards without realising that the organisation already pays for software that can do the same job.

None of these issues means the app itself is necessarily bad or unsafe. Many of the tools employees discover are perfectly legitimate services.

The concern is how much visibility and control your organisation has over them.



If you know where your information is stored, which services can access it and who owns the accounts, you can make sensible decisions about how everything should be managed.

Without that oversight, it becomes much harder to keep track of what you have, what it connects to and what happens if something goes wrong.

You can't properly protect, manage or recover your organisation's information if you don't know where it is in the first place.

The **productivity problem**

A new app usually gets introduced because someone thinks it will make a task easier.

And it might.

The trouble starts when you look at how that app fits with everything else your organisation uses.

If two systems don't share information, someone has to bridge the gap.

They might copy customer details from one place to another, download a file and upload it somewhere else, or update the same information twice.

Each task takes only a few minutes, so it's easy to accept as part of the working day.

Finding information can become harder too.

A document might be in Microsoft 365, someone's personal cloud storage or attached to a conversation in a messaging app.

Employees can end up spending time working out where the latest version lives before they can get on with the task at hand.

These small delays are where a lot of productivity can be lost.

A major system failure gets everyone's attention because work stops. But losing a few minutes to another login, searching for a file or copying information between systems barely registers.

When these interruptions happen throughout the day and across several employees, they soon add up.

There can be a financial cost too.

Small monthly subscriptions are easy to overlook, particularly when different people sign up for tools independently.

You could end up paying for several services with overlapping features, while already paying for software that provides much of the same functionality.

Looking at shadow IT can help you understand where employees have created workarounds because the technology around them isn't making their jobs as easy as it could.

By addressing those everyday frustrations, you can reduce unnecessary work and give people more time to focus on what you employ them to do.

What happens **when somebody leaves?**

When an employee leaves, you can discover just how dependent your organisation has become on technology you didn't know they were using.

They may have found a useful app a couple of years ago and gradually made it part of their daily routine.

Perhaps they use it to manage information, store documents or handle a particular task. Their colleagues might even use it too, without anyone ever formally deciding that it had become part of the organisation's technology.

This can make handing their work over to someone else more complicated.

You need to know who owns the account and whether anyone else has access to it.

If it was set up using a personal email address, the organisation may have little control over what happens to it.

Even if a work email address was used, the password or other access details might only be known by the person who's leaving.

But the bigger concern is the information held inside that app.

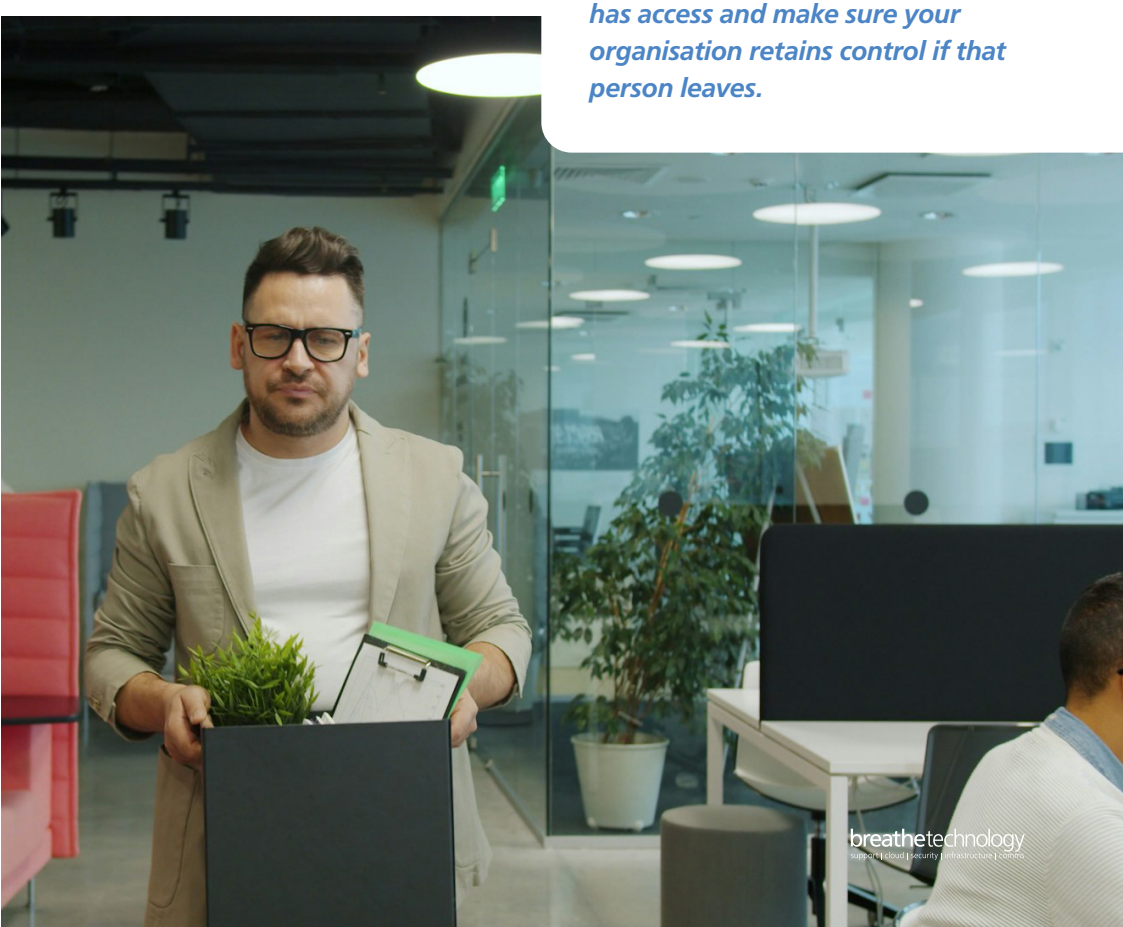
There could be documents, customer details or records of work that the organisation needs to keep.

If nobody knew the app was being used, it could easily be missed when reviewing accounts and access as part of the employee's departure.

This is why ownership matters.

If an app becomes important to the way your organisation works, the organisation needs to own and control it. The same applies to the information stored within it.

Employees will naturally find their own ways to work more efficiently, and some of those ideas can be useful. But when an app starts holding important business or school information, or becomes part of an important process, you need to know it exists, who has access and make sure your organisation retains control if that person leaves.



Don't ban **everything**

When you discover that employees are using apps you didn't know about, the temptation may be to tighten things up and insist that nobody uses anything for work unless it's been approved first.

And yes, there should be clear guidelines around the technology used across your business or school. But rules alone won't solve the everyday frustrations that led people to look for their own solutions in the first place.



If someone started using a different file-sharing service because sending large files was difficult, removing it simply leaves them with the original problem.

If a team adopted another system because entering the same information twice was wasting time, they'll still have that extra work to do once the system disappears.

It's more useful to understand why people went looking for an alternative in the first place.

Your business or school may already have a suitable tool that employees don't know about or haven't been shown how to use.

Microsoft 365, for example, includes plenty of features that can easily be overlooked.

In other cases, an existing system may simply be making a job harder than it needs to be.

Giving employees a straightforward way to request new apps can help.

They can explain what they're trying to achieve, and someone can check whether there's already an approved way to do it.

If there isn't, the new tool can be properly assessed before any business or school information is stored in it.

Ideally, the approved option should also be the easiest one to use. If the official process creates extra work, people will naturally look for a quicker alternative.

Listening to why they're doing that can help you fix the underlying problem rather than continually chasing the apps that appear as a result.



How to get **shadow IT under control**

When you're getting to grips with shadow IT, a sensible starting point is to build an accurate picture of the technology already being used across your organisation.

Your official software list will only tell you part of the story. Look at subscriptions being paid for across the business or school, browser extensions, AI services and apps connected to your work accounts.

It's also worth speaking to employees about the tools they use to get their work done.

These conversations can be useful if you focus on the job rather than the technology.

Find out where people have created their own shortcuts and which parts of their work feel unnecessarily complicated.

You may discover tools that nobody knew about, along with perfectly reasonable explanations for why they started using them.

Once you know what's being used, you can decide what makes sense to keep.

From there, make it easy for employees to check before introducing something new.

There doesn't need to be a lengthy approval process. Just a straightforward way to establish whether a tool is suitable, whether your business or school information will be safe and whether you already have something that does the same job.

Your IT support partner can help with this too.

A good IT partner should understand which technology is being used across your organisation and help identify unnecessary overlap, security concerns or potential problems.

They can also help assess new tools when employees find them, so useful technology can be adopted sensibly without creating another unmanaged system in the background.


The more visibility you have, the easier it becomes to keep your technology useful, manageable and working well together.
breathetechnology

Gain visibility, **retain control**

New technology will keep finding its way into businesses and schools.

AI has accelerated this, giving employees access to useful tools they can start using in minutes.

You need to understand where your organisation's information is stored, which systems employees rely on and who has access to them.

You also need to know that if someone leaves, an app changes or something goes wrong, your organisation still has control of the information it needs.

That starts with having a clear picture of what's being used and how it all fits together.

If you're not sure how complete that picture is, it might be time to take a closer look.

We can review the applications and services being used across your organisation and look for opportunities to make the technology you already have work better.

Get in touch.

www.breathetechnology.com
(live chat available)

London 020 3519 0124
Cambridge 01223 209920
Sheffield 01143 498054
Suffolk 01440 592163

lucy@breathetechnology.com

breathetechnology
support | cloud | security | infrastructure | comms

Empowering You Through Secure Technology