Software

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



SUPERE™

supere.co.uk

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

Your email, accounting software, CRM, Microsoft 365 and perhaps a few systems specific to the work you do.

But there could be other apps and online services being used across your business that you *don't* 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".

That's technology being used for work that isn't formally approved or managed by the business.

In most cases, the person using it is trying to solve a problem. They've found something that makes a frustrating task easier.

The problem is that the rest of the business may have no idea the app exists, what information is being put into it, or who has access.

Something that saves one person a few minutes can create a much bigger issue elsewhere. Once several people start independently making those decisions, it's hard to know which technology your business depends on.

How shadow IT **gets into a business**

It used to be difficult to introduce new technology into a business.

Software had to be bought, installed and configured, and there was a good chance somebody responsible for IT would be involved somewhere along the way.

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

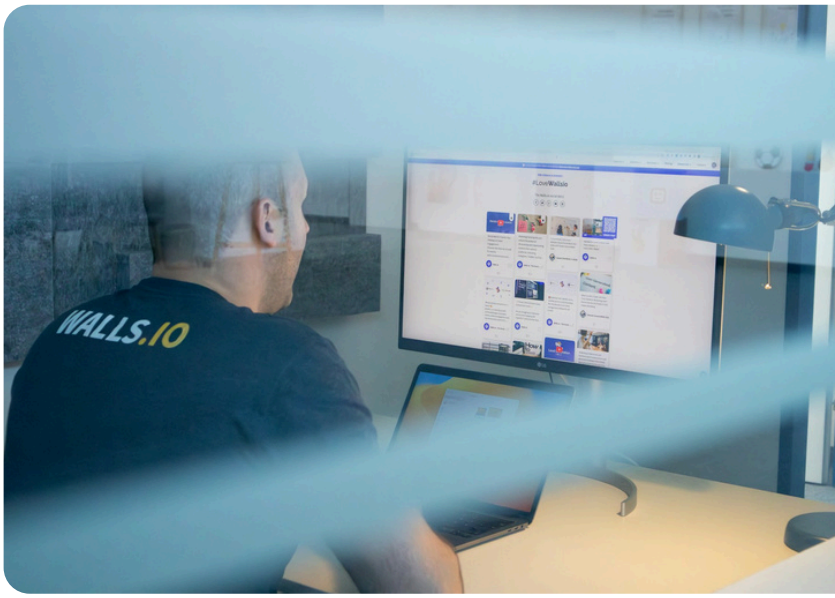
They might create an account using their work email address, add a browser extension or sign into an AI service. If the free version does what they need, there may not even be a purchase for the business to approve.

That makes it easy to solve small frustrations independently.

Maybe someone's 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 may introduce it to a few 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 likely won't think of that decision as introducing new technology into the business.

Shadow IT can tell you something useful about the technology people have been given.

When employees repeatedly look elsewhere for a better way to do their work, there may be a frustration that hasn't been addressed.

Perhaps an existing system is too cumbersome, two pieces of software don't work well together, or employees 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 become **a business problem**

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 contain 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 keeps documents they need to access from different locations.

Before long, you have company information stored in places you don't even know about.

There can also be connections to other systems.

Plenty of apps offer the option to sign in using a Microsoft or Google account, or ask for permission to access files, email, contacts or calendars.

Clicking "Allow" is easy, but it can give another company access to parts of your business systems.

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 effectively become tied to that person.

This becomes more awkward if they leave the business 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 can also put relatively inexpensive subscriptions through on company cards without anyone noticing that the business already pays for software capable of doing the same job.

None of these issues requires an app to be 'bad' or unsafe. Many of the tools employees discover are legitimate services.

The concern is how much control the business has over them.



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

When applications are added without that oversight, decisions are more difficult.

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

The **productivity problem**

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

It may do.

The trouble comes when you look at how that app fits with everything else the business uses.

If two systems don't share information, somebody must 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.

That doesn't take long on its own, so it's easy to accept as part of the working day.

Finding information can become harder too.

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

Employees may spend a few minutes working out which version is current before they can get on with what they wanted to do.

These small delays are where a lot of productivity is lost.

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

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

There can be a financial cost alongside this.

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

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

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

Removing those little points of friction can give people more time to spend on the work you employ them to do.

What happens **when somebody leaves?**

An employee leaving the business can expose how dependent you've 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 the way they work.

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 this was now a business system.

That can make handing their work to somebody else more complicated.

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

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

Even if a company email address was used, the password or other information needed to access the account might only be known by the person who's leaving.

But the bigger concern is the information held *inside* it.

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

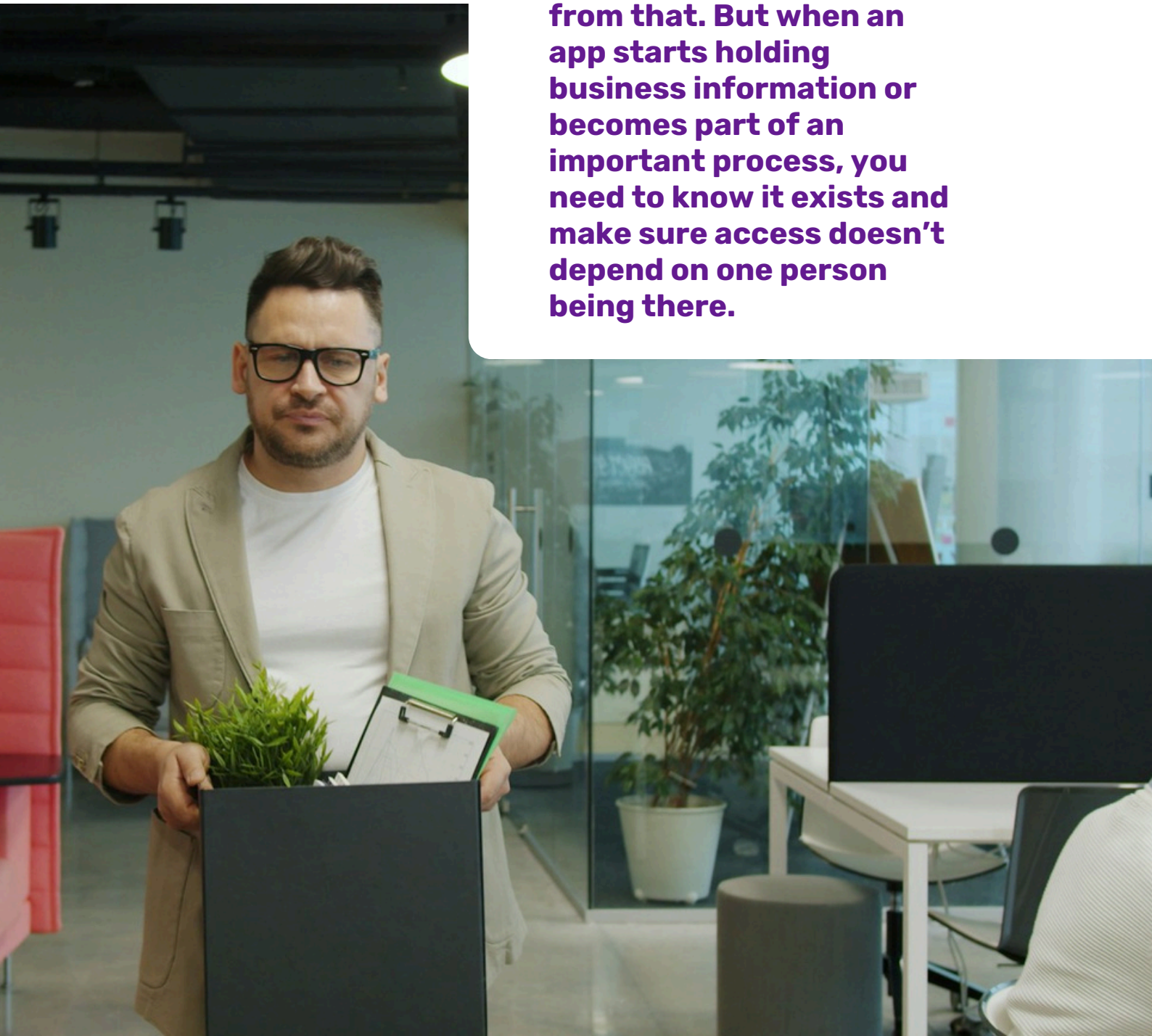
If nobody knew the app was being used, it may be missed completely when accounts and access are reviewed as part of the employee's departure.

This is why ownership is so important.

If an app becomes important to the way your business works, the business needs to own and control it.

And the same applies to the information stored within it.

Employees will develop their own ways of working, and useful ideas can come from that. But when an app starts holding business information or becomes part of an important process, you need to know it exists and make sure access doesn't depend on one person being there.



Don’t ban **everything**

Once you discover that employees are using apps you didn’t know about, the temptation may be to tighten everything up and insist that nobody uses anything unless it’s been approved first.

And yes, there should be some rules around the technology used for work. But rules alone won’t fix the frustrations that led people to find their own solutions.



If somebody started using a different file-sharing service because sending large files was difficult, removing the service leaves them with the original difficulty.

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.

The business 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 a lot of features that can easily be missed.

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

Giving employees a simple way to request a new app helps.

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

If there isn't, the new tool can be looked at properly before company information starts being stored in it.

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

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 a handle on shadow IT, a sensible starting point is to build an accurate picture of what's already there.

Your official software list will only tell you part of the story. Look at subscriptions being paid for across the business, browser extensions, AI services and apps that have been connected to company accounts.

You also need to speak to employees about what they use to get their work done.

Those 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 awkward.

You may discover tools that nobody knew about, along with reasonable explanations for why they appeared.

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 they start using something new.

There doesn't need to be a lengthy approval process, just a quick way to establish whether a tool is suitable, whether company information will be safe in it and whether you already have something that does the same job.

Your IT support partner can help with this.

A good IT partner should understand which technology is being used across your business and help you spot unnecessary overlap or potential problems.

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


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

Gain visibility, **retain control?**

New technology will keep finding its way into businesses.

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

You should understand where your business information is stored, which systems your employees rely on and who has access to them.

You should also know that if somebody leaves, an app changes or something goes wrong, the business still has control of the information it needs.

That starts with having a clear picture of what's being used.

If you're not sure how complete that picture is, it might be time for some help.

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

Get in touch.

CALL: 0333 034 7560
EMAIL: info@supere.co.uk
WEBSITE: supere.co.uk

SUPERE™