

# 10 things you need to know about shadow IT



You might not be familiar with the term ‘shadow IT,’ but it’s probably happening all over your business. Picture the scene: your team is asked to complete a task - quickly, or to a high standard - but only has access to a limited set of software. A better tool exists but it hasn’t been approved by the IT department yet. Your team signs up anyway and completes the work without telling anyone how they did it. That, in a nutshell, is shadow IT.

Many companies want to eliminate shadow IT altogether. They fear that without their IT department’s oversight, employees will adopt services and habits that create vulnerabilities. Others believe that shadow IT should be allowed to run rampant, as it will make their business more creative and efficient. Unsurprisingly, the correct approach is somewhere in the middle. If you understand the issue and strike the right balance, you can sleep at night knowing your business is secure, even if shadow IT is part of it.

## 1. Everyone is doing it

Shadow IT is notoriously hard to measure. Many employees are using unauthorised software covertly, on a mixture of work and personal devices, which makes it difficult to identify and monitor. But if you had to guess the average number of employees that use shadow IT, what would you say? One in five? A third? Or maybe half? Guess again.

When [we surveyed US workers last year](#), more than 64 percent said they had created at least one shadow IT account in the last 12 months. Of that group, more than half had created between two and five accounts, and roughly 16 percent said they had made more than five accounts. Other research suggests these figures should be even higher. Microsoft, for instance, [believes that 80 percent of staff use unapproved apps](#).

# 64%

*of US workers have created  
at least one shadow IT  
account in the last 12 months*



**The bottom line:** this isn’t a small issue.

## 2. The pandemic has changed everything

The coronavirus pandemic has forced many companies to embrace a work from home model. Away from the office, employees have sought out new tools that make it easier to chat and collaborate on projects. That's led to a 59 percent rise in shadow IT, [according to research by Core](#). Most of it falls into three categories: video calling, instant messaging and file-sharing. And our own research shows that most people think these tools only pose a small security risk.

*The move to remote work has led to a*

**59%**

*rise in shadow IT*



And that can be a worry. Almost half of IT professionals [surveyed by Check Point](#) last year said that shadow IT was one of the biggest challenges when shifting to remote work. Many companies also rushed into major changes at the start of the pandemic. More than half of respondents told Core that they had been pressured to roll out solutions without proper testing. Roughly three quarters said they had introduced “short term fixes” to keep their business moving.

## 3. Your IT department might have a limited perspective

Your IT department might have a warped or incomplete view of what's happening inside your company. In a [survey conducted by Snow Software](#), 83 percent of IT leaders said their business was effectively monitoring software, application and cloud usage. Not bad, you might think. But only 69 percent of general employees agreed with that assessment. Similarly, 82 percent of IT leaders said their company was tracking work devices. But that figure fell to 68 percent when Snow Software quizzed other employees.

Does your IT department have a bad read on the situation? It's possible that your employees are creating accounts outside of their field of view. That means they have an incomplete picture of your company, and shadow IT is potentially putting your organization at risk.

## 4. The people using the most shadow IT might surprise you

Everyone wants to use good software at work. But that doesn't mean everyone adopts the same amount of shadow IT. The volume varies depending on a person's age and position. Our own research has shown that 69 percent of people aged 18 to 39 follow their company's IT policy, compared to 82 percent of workers aged 40 to 55 and 88 percent of employees over the age of 56.

Reading these figures, you might assume that more junior employees use shadow IT more than managers. After all, company directors are typically older than those in entry-level positions. But that's not the case. Research by Snow Software found that management-level employees were almost twice as likely to use unauthorised software than employees with entry-level, associate and specialist roles.

*Research by Snow Software found that Management-level employees are twice as likely to use unauthorized software than employees with entry-level, associate and specialist roles.*

It's important to recognize that shadow IT usage can vary within a company. If you can identify the people that break your policy the most, it'll be easier to figure out their problems and come up with solutions that keep everyone happy and productive.

## 5. Many people don't like talking to their IT department

Keeping your IT department in the loop is difficult if your employees don't want to approach them. In our own research, most people told us their IT department was more of a hindrance than a help. Respondents said they broke the rules primarily to be more productive, but also because it's too hard to get approval from their company's IT specialists.

Other research has exposed the often strained relationship between staff and their IT department. In Snow Software's report, only 35 percent of respondents said they didn't mind asking for permission to use new services and software. Sixteen percent said these conversations were frustrating, while 15 percent commented that it made them feel like they were being watched. Seven percent felt that the entire process was beneath them.

You can avoid a lot of this frustration by nurturing a culture of security inside your organization – if everyone is mindful about security risks, they're more likely to have constructive conversations with the IT team.

## 6. The security implications are real

Okay, so some people in your company signed up for a new project management tool. What's the big deal? Will a hacker really find out and use that information to sneak past your company's defences? Quite possibly. [Oracle and KPMG discovered in 2019](#) that shadow IT, if it's not handled correctly, can create serious vulnerabilities. Half of respondents said unsanctioned software had led to unauthorized access to data.

And it gets worse. Almost half said shadow IT had resulted in a real loss of data or allowed malware to infect their systems. Only 16 percent of respondents said that shadow IT hadn't led to any unauthorized access, data loss or malware. A frightening figure, considering the average cost of a data breach was \$3.86 million last year, [according to research by IBM and the Ponemon Institute](#).

# \$3.86

*million was the average cost  
of a data breach in 2020*



## 7. Shadow IT can cost you money

Breaches aren't the only way that shadow IT can hurt your company's finances. Unapproved software slowly racks up to create a monthly or yearly bill that no-one expected or budgeted for. The [Everest Group](#), for instance, found that large companies spend at least half of their IT budget on unauthorized apps and services.

The problem goes something like this: your company pays for a video-editing app, but it's outdated. The video team is unconvinced that the company will approve something else, so they expense a different app and continue working. Suddenly, the company is paying for two apps that serve a similar purpose. And the finance department might not know that any of this is happening.

This kind of tool duplication is a real problem. Sales people have an incomplete picture of the company, which makes it harder to negotiate new business licenses and "rightsize" existing ones. Shuffling projects between different tools can also make your team less productive. And as the age old saying goes, time is money.

## 8. Some companies don't know how to tackle it

Shadow IT is hardly new, however many businesses still aren't sure if and how to tackle it. Some organizations have tools in place to check what people have installed on their devices and frequently access via the web. But others don't. When we surveyed IT personnel, one in three said they were lax about enforcing their IT policy.

Of these, 38 percent said their organisation's approach to monitoring wasn't robust enough, and 29 percent said it was too difficult and time consuming to track what everyone is using.



*One in three IT departments are lax about enforcing their IT policy.*

## 9. Shadow IT doesn't have to be a problem

Shadow IT sounds bad but rather than asking yourself “How do I stamp out shadow IT?” you should be asking “How do I ensure my team can use the right tools for the job, with the supervision of my IT department?”

It's difficult to keep tabs on every employee all of the time. So the first step should be education. Explain what everyone needs to look out for and consider when choosing a new app or service. You can't expect them to be fully-trained security experts. But if they have a security-first mindset, they can make a good-enough assessment and embrace tools without creating any vulnerabilities.

The second step is to change your company's approval process. Employees often use shadow IT because they know their IT department will spend weeks evaluating a new app. It's important to avoid this kind of relationship, as it prioritizes security over productivity and could be slowing your team down. Instead, encourage your IT specialists to make this process a conversation that weighs up the benefits of a given tool versus potential risks.

## 10. Solve the problem with a password manager

The most important step your company can take to combat Shadow IT? [Adopting a password manager like 1Password.](#)

You might already be using Single Sign-On (SSO) or an identity access management solution to track what your employees have access to. But that doesn't mean your employees haven't found a way to use shadow IT or they're logging into work accounts with passwords that are weak, guessable and easily exploitable. A password manager can help here.

If your team embraces 1Password, it can help to develop a security-first mindset. Password managers like 1Password encourage everyone to protect their work-related accounts with strong, unique passwords. With that mindset in place, and credentials stored securely in 1Password, you'll have a more complete overview of the tools your company is using. That will lower the chances of your team using apps or websites that IT isn't aware of, and creating vulnerabilities in the process.

It's not perfect. Someone could still adopt shadow IT, for example, and choose not to store their login details in your company's password manager. But it's unlikely to happen if you make security a key part of your corporate culture. And it's far better than the alternative - no company password manager, which limits your visibility and encourages people to use weaker passwords.

## **Take action now**

Don't let the words 'shadow IT' keep you up at night. Yes, unauthorized software can create vulnerabilities. But you can keep the problem in check with a password manager like 1Password. It will protect your employees' accounts and help build a new kind of company culture. One where every employee thinks about security and doesn't mind talking about the tools they rely on day-to-day - including those that haven't been approved yet by management.