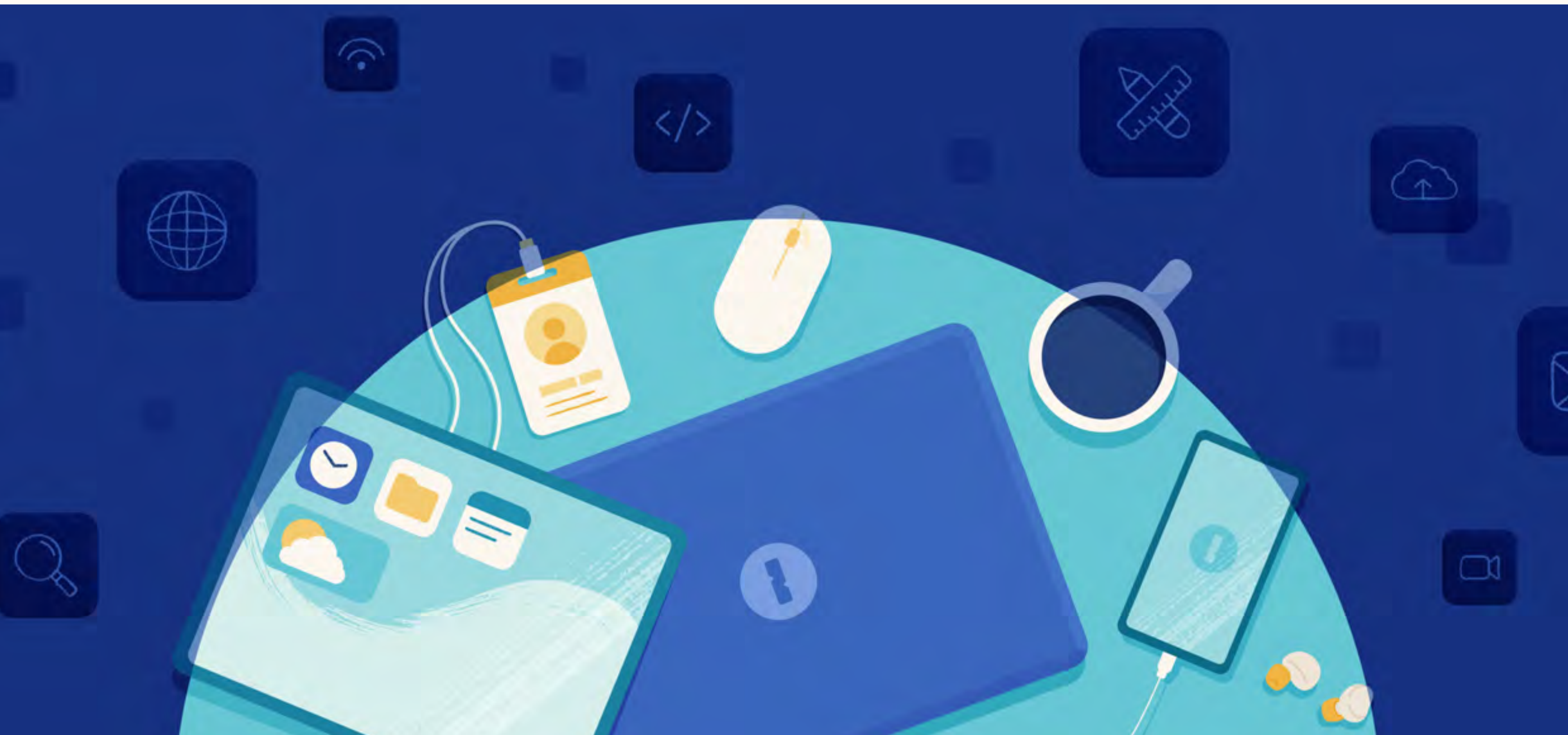
1Password

GUIDE

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 (or both). The team finds a new tool that will help them complete the task, but it hasn't been approved by the IT department yet. Your team signs up anyway to complete the work – and IT has no idea a new tool has been added to the company tech stack. That, in a nutshell, is shadow IT.

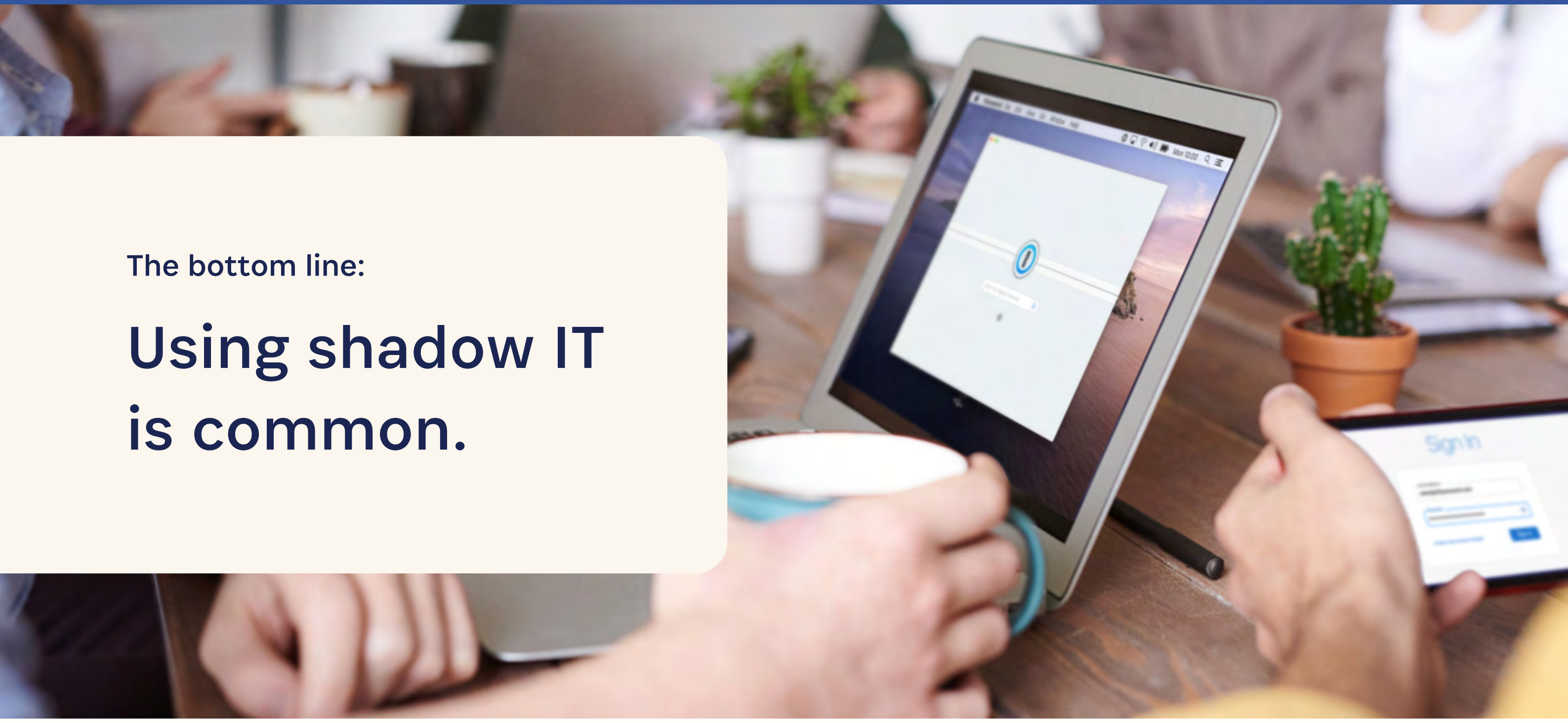
Many companies want to eliminate shadow IT altogether. They fear that without their IT department's oversight, employees will adopt services and habits that create vulnerabilities. Others believe that shadow IT should be allowed to run free, as long as it makes their business more productive and efficient. Unsurprisingly, the correct approach is somewhere in the middle. If you understand the issue, you can help your team complete their work securely, no matter what apps they use.

1 Everyone is doing it

Shadow IT is notoriously hard to measure. Many employees are using unauthorized software 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?

When we surveyed US workers, 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:

Using shadow IT is common.

2 The new normal is here to stay

The pandemic forced many companies to embrace a work-from-home model. Away from the office, employees 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. And our own research shows that most people think these tools only pose a small security risk.

And that can be a worry. Almost half of IT professionals surveyed by Check Point 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. While the pandemic may have been the inciting incident, shadow IT existed before, and it's here to stay.

Changes in how we work have led to a

59%

rise in shadow IT

3 Your IT department might have a limited perspective

Your IT department may have an 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.

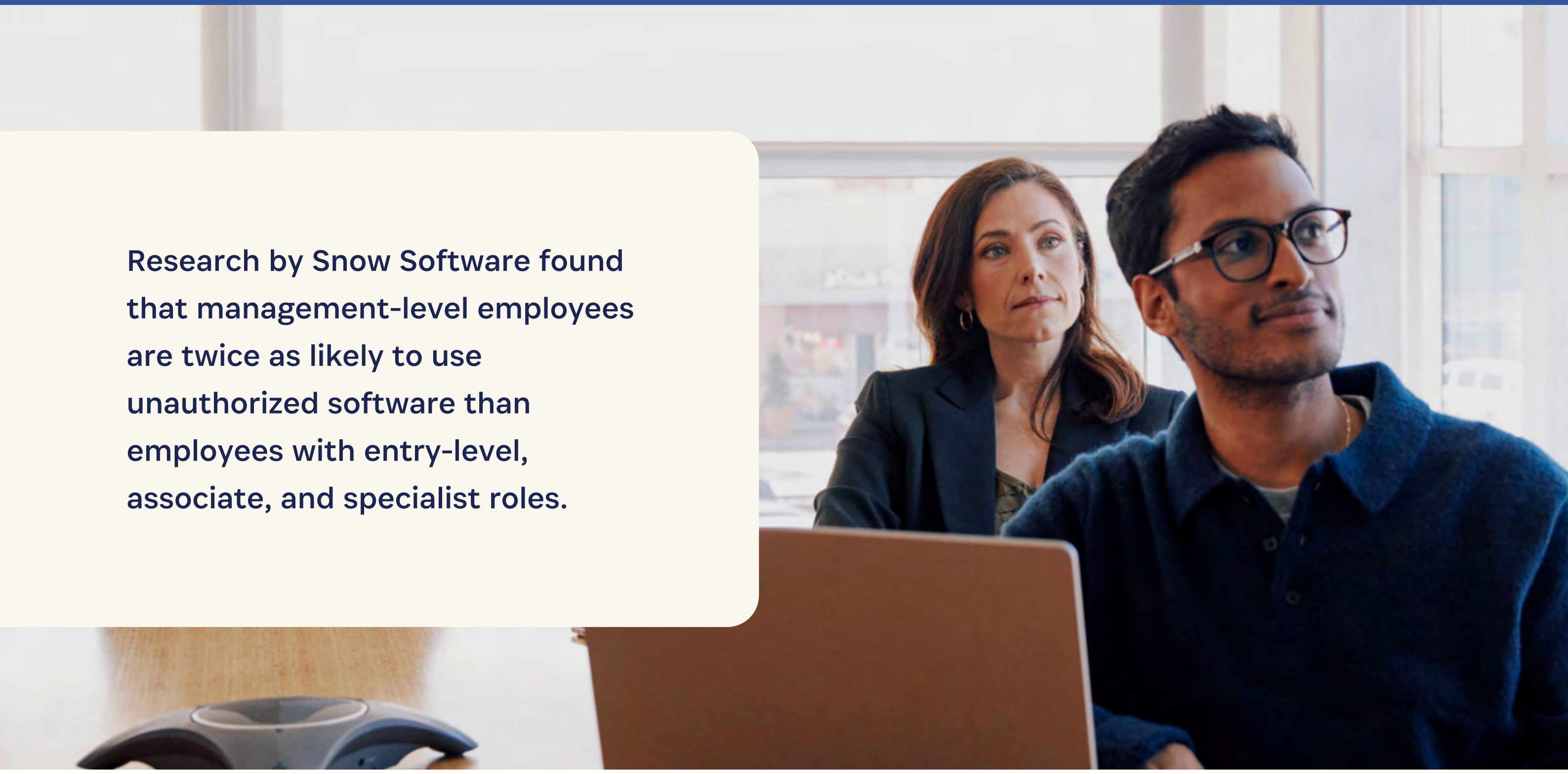
Does your IT department have a bad read on the situation? It's possible that employees are creating accounts outside of their field of view. That means they have an incomplete picture of your company, and shadow IT is potentially putting your organization at risk.

4 It's about getting things done

Everyone wants to use good software at work. We found that the use of shadow IT varies depending on a person's age and position. Our 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 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 unauthorized software than employees with entry-level, associate, and specialist roles. Turns out executives are just as interested in getting things done efficiently and with the best tools available as anyone else.

Shadow IT usage can vary within a company. Finding workers who are looking for software workarounds will help you identify their problems and, together, come up with solutions to keep everyone happy and productive.



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.

5 Do you have an “IT department” or a “Department of No”

Keeping your IT team in the loop is difficult if your employees don’t want to approach them. In our research, most people told us their IT department was more of a hindrance than a help. Respondents said they used unauthorized apps 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 teams 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 helping your IT team become a productivity ally. Find ways to make requesting new software or hardware accessible to all employees. And if a specific request is rejected, educate employees on the security risks posed by the software, so they’re more likely to stick with approved apps. You can also nurture 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 You may be underestimating the security implications

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 defenses? Quite possibly. Oracle and KPMG discovered 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.

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. Keep in mind that the average cost of a data breach is $4.45 million, according to research by IBM and the Ponemon Institute.

$4.45M

was the average cost of a data breach in 2023

7 Ignoring the problem isn't the answer

Breaches aren't the only way that shadow IT can hurt your company's bottom line. 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.

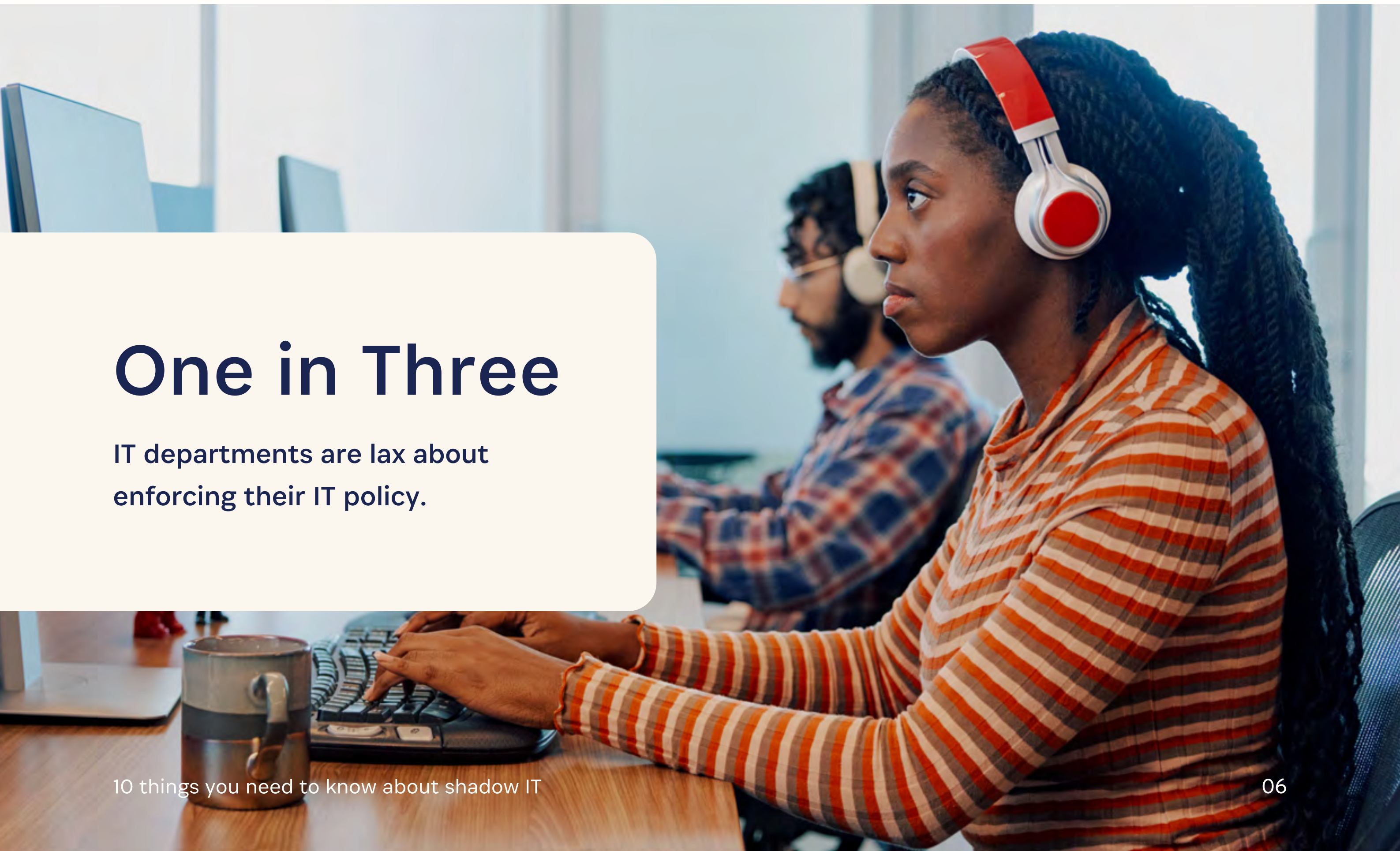
The problem goes something like this: your company pays for a video-editing app, but it's outdated. The video team is unconvinced that the company will approve something else, so they expense a different app and continue working. Suddenly, the company is paying for two apps that serve a similar purpose.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

This kind of tool duplication is a real problem. Vendors may 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.

8 Companies are struggling to adapt

Shadow IT is hardly new, but many businesses still aren't sure how to tackle it. The pandemic and rapid shift to hybrid work caught many companies off-guard. Some organizations had, or have since implemented, tools 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 organization'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. While the shift to hybrid work highlighted the shadow IT challenge, many businesses just don't know how to effectively and securely manage shadow IT.



One in Three

IT departments are lax about enforcing their IT policy.

9 The path forward: Start small, and think big

Instead of asking “How do I stamp out shadow IT?”, the savvy leader asks, “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 review your company’s approval process. Employees often use shadow IT because they know their IT department will spend weeks evaluating a new app. Just as employees need to learn about security, it’s important for the IT team to recognize the reason employees are looking for app alternatives. Prioritizing security over productivity could be slowing your team down. Instead, encourage IT to make this process a conversation that weighs the benefits of a given tool versus potential risks.

10 Enterprise password managers were built for this

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 aren’t using shadow IT outside of managed apps, or that they’re logging into those accounts with secure, strong passwords. That’s where a password manager shines.

1Password helps your team develop a security-first mindset. Password managers like 1Password encourage everyone to protect all of their work-related accounts (approved or not) with strong, unique passwords (in fact, 1Password generates passwords for them, so they don’t have to).

With that mindset in place, and credentials stored securely in 1Password, you get a more complete overview of the tools your company is using. With 1Password Insights, your IT team can identify company email addresses that have been caught up in a data breach, even if it's shadow IT that's being used. That gives your IT team the information they need to notify people about potential vulnerabilities.

Someone could still adopt shadow IT and choose not to store their login details in your company's password manager. But it's less likely 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 results in people using weaker passwords.

Take action now

Shadow IT is here to stay. It gives workers more flexibility and more freedom to do work their way. Work now happens in the cloud, which means work can and will be done on any device with internet access.

The challenge for IT and security teams is to align security and productivity. Doing so requires understanding the business's objectives, and what workers are trying to accomplish – to secure employees' daily workflows without slowing them down.

That starts with giving them the right tools for the job. Paired with proper education and nurturing a culture of security, 1Password makes it easy to get things done, securely.