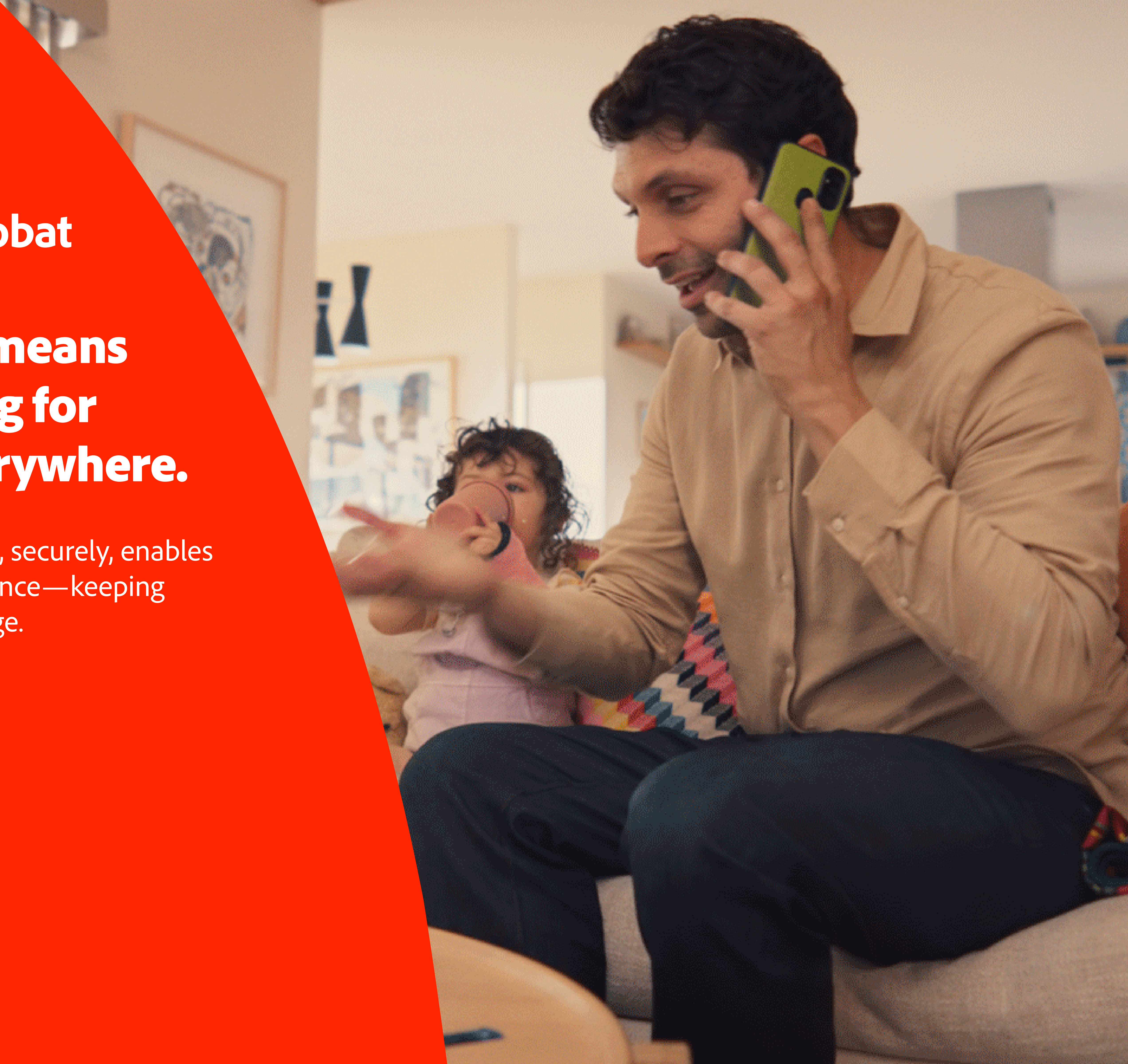
Adobe Acrobat

Working well means secure working for everyone, everywhere.

Using the right technology, securely, enables collaboration with confidence—keeping everyone on the same page.

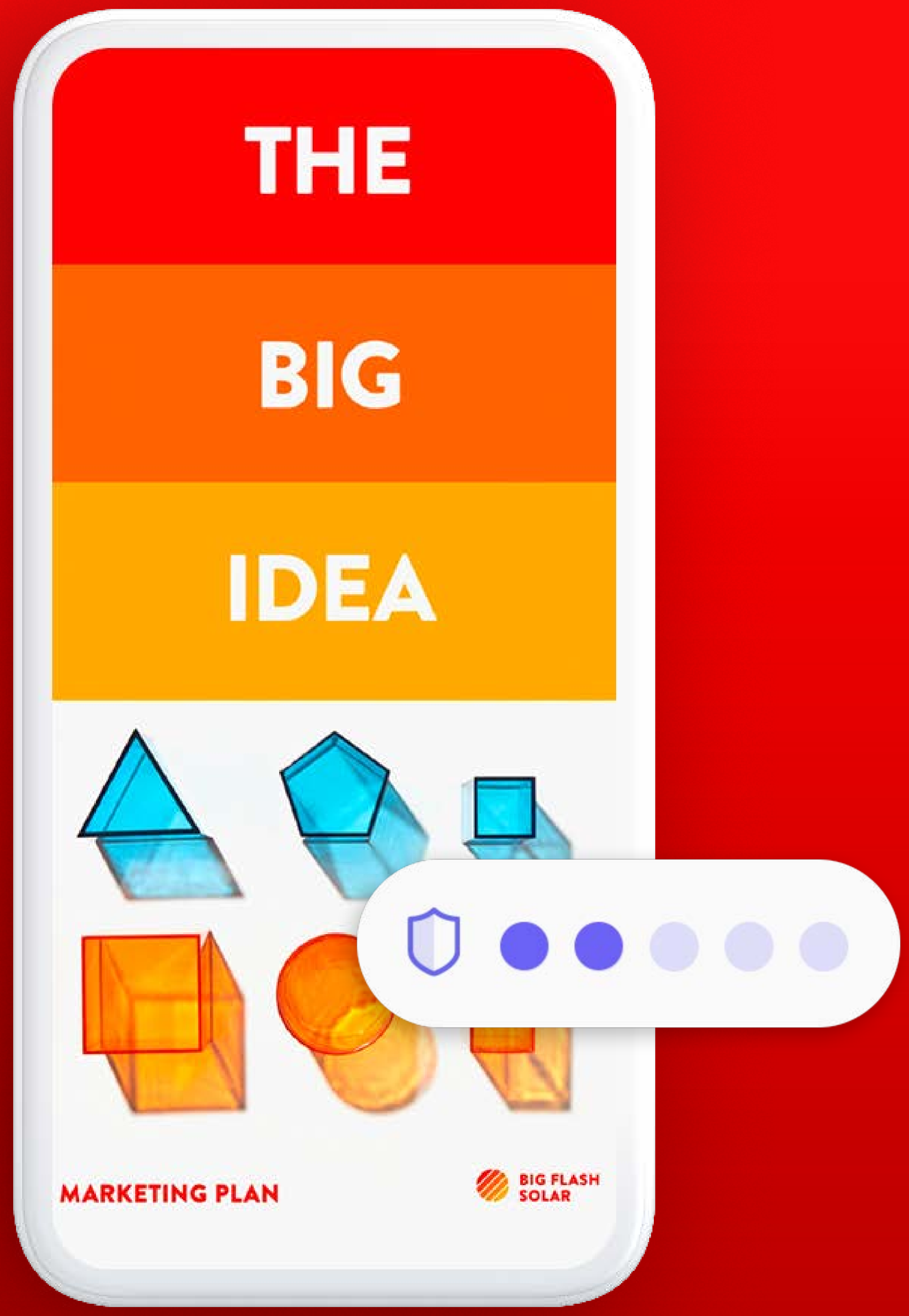


For better or worse, hybrid and remote working is now a fact of life for businesses great and small. It all comes down to flexibility. Many teams have the choice to work where they like or when they like—or both. And the benefits are undeniable not only in terms of employee satisfaction but also in business measures like improved performance. According to Gartner, 43% of employees globally said that flexible work options improve their productivity and efficiency.[1]

None of this would be possible without the right tech—not only video meetings but also the less talked-about capabilities like enhanced security, browser-based applications, and collaboration tools—and the infrastructure that ties it all together. This puts IT teams at the heart of any push toward flexible working. Although when IT does its job well, other parts of the business rarely see the effort and resources needed to keep everyone working together securely.

In a 2022 study, 57% of 1,200 security professionals said over half of their company's workforce works remotely at least 2 days a week.[2] There's a lot involved in enabling teams across the business to do their best work. You might be helping them use different devices and apps together, move from work to home and back again, and use personal devices on office networks (or vice versa). Or just helping them get to grips with device management policies. Trying to keep everyone and everything secure, on top of that, can be quite a handful.

But it's important to keep one eye on the future while dealing with today's issues. IT professionals have more influence over what the future of work will look like than most. This gives us an extra responsibility to help keep everyone working well—today, tomorrow, and for the foreseeable future.



Working well means secure working for everyone, everywhere.

Using the right technology, securely, enables collaboration with confidence—keeping everyone on the same page.

1 So, what do we mean by “working well”?

Working well is all about thriving at work, not just surviving—giving people the chance to enjoy what they do. Practically, that means offering individual employees the flexibility to work in the ways that suit them best—whether that’s location, working hours, or both. This means that working well looks different for everyone.

Some employees work best late into the night by themselves, when they know nobody will disturb them. Others are energized by the hum of a busy office and feel lost without it. And many like the autonomy of going for a long walk to clear their heads or doing laundry between different work tasks so they can spend quality time with their families later.

What’s needed is a human-centric approach, where flexibility is applied creatively to balance these individual needs with those of your business. Ideally, you’ll consider your employees, customers, and community. IBM has created a guide to building a human-centered organization that discusses the challenges of making potentially deep structural changes to allow this all to happen.[3] For tech teams, this will involve finding ways for people to work securely without getting slowed down—or, even better, finding solutions that can speed up their workflow.

Supporting everyone, everywhere.

When businesses strive to let employees work in the way that’s best for them, they often end up with a hybrid working situation. This means that the support and infrastructure supplied by IT has to be adaptable. Selecting the right solutions can make all the difference.

UK-based legal services firm Slater & Gordon exemplifies the tech needs of a hybrid workplace. The geographically dispersed team communicates with each other and with customers around the country.

Slater & Gordon connects retail clients who need legal support for a major life event—like buying or selling a home, writing a will, or dealing with a personal injury claim—with local legal experts all over the UK. These specialists need to engage with clients conveniently and securely from anywhere, anytime—via mobile and email as well as web chat, online requests, and online case and claim platforms.

To manage this unusual business model, the firm developed a creative technology strategy: Work Anywhere, Automate Everything & Innovate. It allows the firm to discard the traditional paperwork of legal firms for secure, digital transactions using Adobe products in a Microsoft environment.

Using Adobe Acrobat and Acrobat Sign, the team can turn any type of document into a sharable, highly secure digital file and streamline workflows with electronic signatures, audit trails, and intuitive tracking. Full integration with Microsoft Managed Desktop and Teams means it can support document work from desktops, laptops, and mobiles—all through a familiar interface. This lets Slater & Gordon process an incredible 13,000 documents each month, allowing the team to expand its client base.[4]

2 Why is it important to support working well?

When employees can work in the ways that suit them best, not only are they happier, but they may find more motivation and energy to work. For instance, we've already seen that many employees say a choice about where, when, and how much they work makes them more productive.

And IBM research[5] has found that companies that prioritize employee experience reap the rewards: Those scoring in the top 25% **for employee experience reported twice the return on sales (ROS)**[6] of those in the bottom quarter.

If that isn't enough, there are downsides to ignoring the need to work well. It's likely that you'd find it harder to attract talented people and create and maintain a diverse workforce. You might even lose some of the workers you have now. In a recent Adobe study, for example, 54% **of enterprise workers said they'd switch jobs for the option to work remotely**—rising to 63% for Gen Z and 66% for Millennial employees.[7]

Given estimates in the US that a replacement can cost around 150% **of an employee's annual salary**[8] **for hiring, recruiting, training, upskiling, and conducting orientations** —as well as reduced productivity in the meantime—it's not worth ignoring the chance to support working well.

3 Working well means working securely.

For the IT department, the challenge is to give everyone, everywhere, what they want while keeping them—and the business—secure. With people working inside and outside your firewalls and VPNs—and maybe using personal devices on company networks and company devices on home networks—it's not surprising that many businesses face security breaches.

$4.24M was the average cost of a data breach incident, according to a 2021 global study of over 500 businesses.[9] As you might expect, the most common cause of breaches was found to be stolen user credentials, while customer personal data was the most common type of information exposed.

80% of data breaches still involve human error.[10] Given this, IT's role in securing flexible work options must not be underestimated. The latest tech solutions must go hand in hand with appropriate cybersecurity training and procedures for a multi-layered approach. Storing documents and data in a central, secure cloud-based location means less risk of employees using multiple data servers to get tasks done. Your valuable business data stays where you can keep an eye on it—and back it up safely too.

4 It’s hard to keep everyone on the same page safely.

The overall challenge is to help underpin flexible working in a way that empowers employees and protects the business at the same time. Given that overarching consideration, there are a few key factors that are essential:

Devices, devices everywhere.

There’s a lot of risk involved when employees are forced to use a range of devices. Remote workers may be left juggling laptops, personal and work mobiles, and even home printers and tablets. Nearly half (47.8%) of those polled in a 2021 UK and US survey use 2 devices, 19.2% use 3, and almost 1 in 10 (8.5%) use more than that.[11] It’s hardly surprising that an overwhelming 83% of IT teams that took part in a global survey find it impossible to set and enforce corporate policies around cybersecurity now that personal and professional lives are so blurred.[12]

Another dangerous area is letting unvetted personal devices onto your networks—whether from the office or remotely. A 2022 global security report[13] found that 70% of businesses allow personal laptops and mobile devices on their networks, while only 17% limit remote access to workers using corporate laptops.

But if home workers use work devices on their own networks, that’s risky for you as well. 70% of those working from home connect corporate laptops to their home networks, while over half (52%) have IoT devices connected to their networks too. Internet-enabled gadgets are notoriously insecure, especially lesser-known brands, with everything from unchanged factory-set passwords to unpatched firmware weaknesses.[14]

Users are only human.

Dispersed working relies on individuals being aware of cybersecurity and understanding how their simplest actions might affect the safety of the business. But lack of training and simple human error make employees one of the weakest links in the security chain.

In fact, in a 2019 study,[15] only 36% of global office workers surveyed had been given training on how to protect their home network, and 54% of those aged 18–24 were more worried about deadlines than exposing the business to a data breach.

A 2021 global security research report[16] found that 79% of employees working remotely took shortcuts with security even though they knew they shouldn’t. A third (33%) saved passwords to their browsers, 32% used public wi-fi, and nearly a quarter (23%) recycled passwords across multiple sites or shared credentials with colleagues. And, in a 2021 IBM survey, an astounding 82% admitted that they use the same passwords across multiple accounts.[17]

Improve your tech without increasing your stack.

Hybrid working, dispersed teams, and flexible working hours mean that the need for collaboration tools and other remote software solutions has grown in recent years.

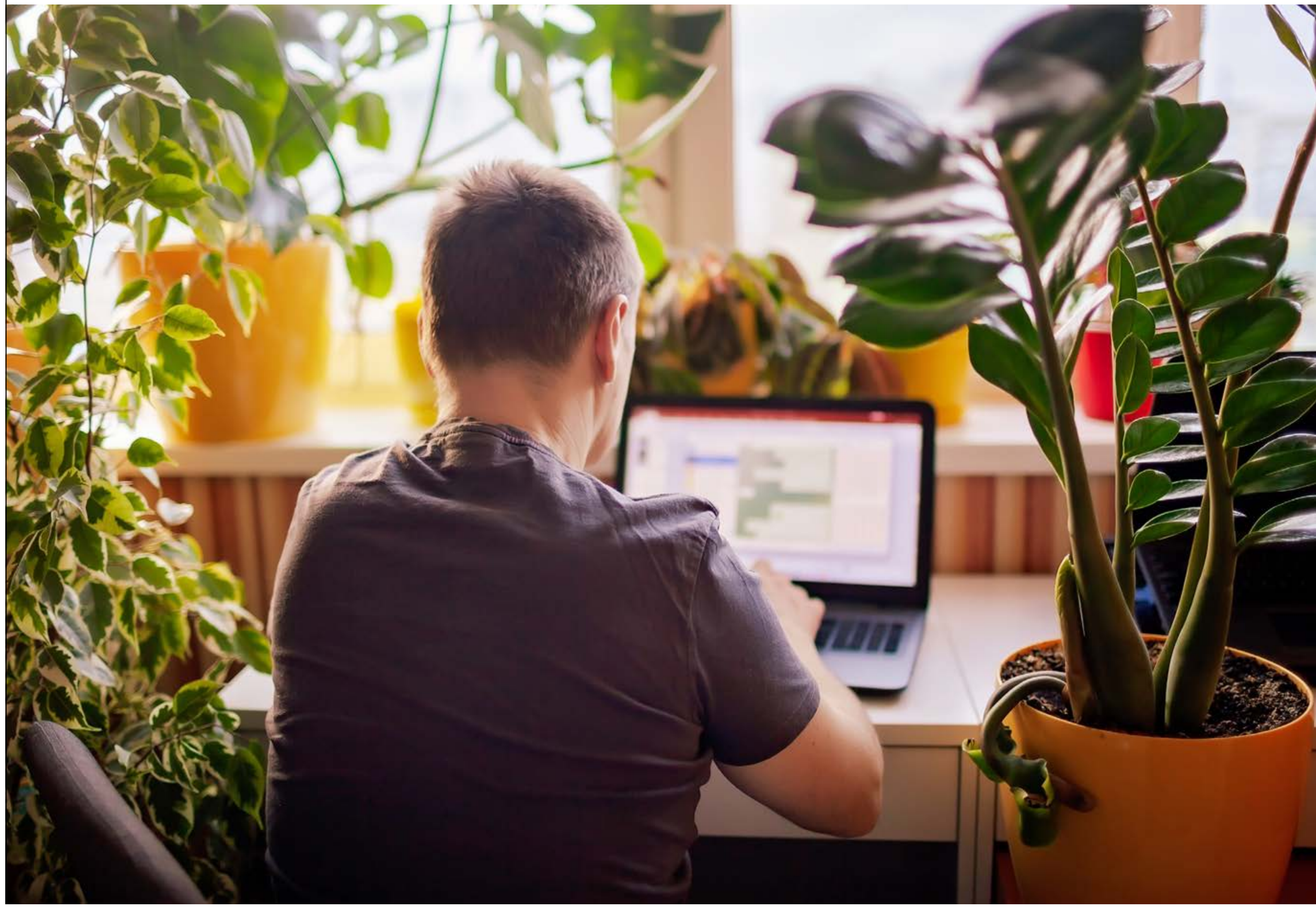
Some estimates say the average enterprise-level business has more than 1,000 cloud services,[18] while Gartner estimates worldwide spending on public cloud services will total $494.7 billion by the end of 2022. In 2020, businesses were using an average of 137 unique SaaS apps each,[19] with smaller companies spending an average of $202,000 and medium-sized companies $2.47 million.

After a couple of years of rapid growth in spending on cloud tech, the trend now is for optimization. Gartner has predicted that by 2026, 50% of organizations using multiple SaaS applications will centralize management and usage metrics of these apps using a SaaS Management Platform.[20]

Setting the costs aside, using multiple standalone apps can cause inefficiencies in your business processes. It leaves data siloed in separate systems, denying decision-makers visibility across all the relevant information and leading to fragmented or even broken customer experience. Plus switching between different interfaces and diverse user interfaces can slow users down to a crawl, as can learning and getting familiar with new software.

Sticking to a smaller number of integrated apps and platforms also makes it more likely that you can take advantage of automation to streamline repetitive tasks. When a third of the working week can be lost to "unimportant" tasks, this could make a huge difference.[21]

And finally, integrated software solutions make security super simple—everything stays safely within the same ecosystem.



5 IT leaders are at the heart of working well.

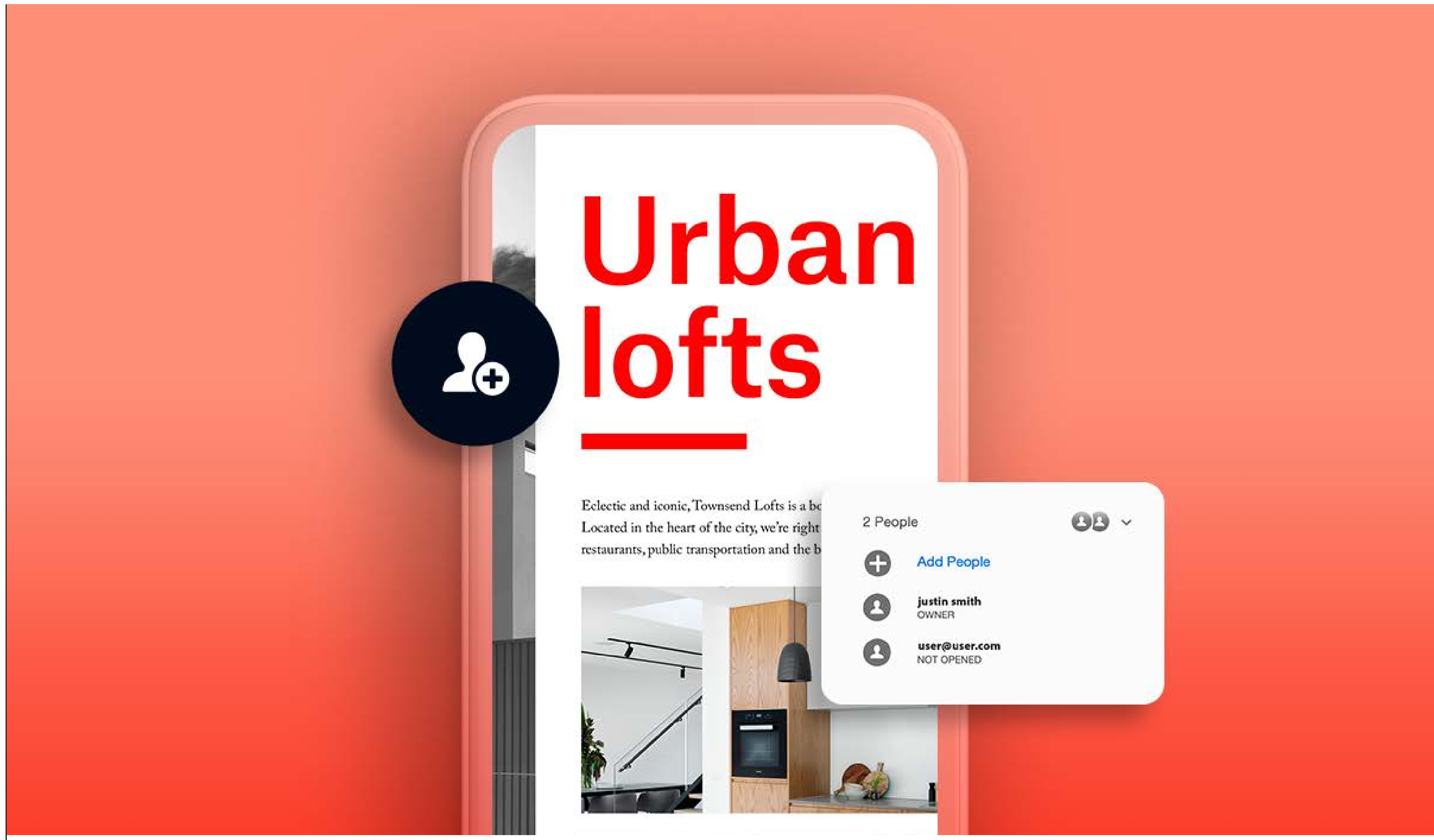
The skills and knowledge based in the IT department make it well placed to lead the transformation to working well.

This is an opportunity to re-evaluate your long-term digital capability. You should build in the ability to stay agile and refine your hybrid working solutions, keep collecting data from users to make the most of their experience, identify insights for improvement, and establish a center of excellence for best practices across key digital tools.

There are some key tricks to let you support working well without spiraling costs or compromising productivity.

Getting serious about security.

If your business will be relying on workers coming in and out of your secure networks, it might be time to take a Zero Trust security approach. This model proposes that the safest way to operate is by assuming that the network, or certain user identities, may already be compromised. Rather than introducing security protocols and tools one piece at a time, organizations rely on AI and analytics to continuously validate interactions between users, data, and resources. IBM Security found that businesses with a long-established Zero Trust strategy saved $1.76 million on data breach costs in 2021 compared to those who didn't employ this strategy at all.[22]


Urban lofts
Eclectic and iconic, Townsend Lofts is a be
Located in the heart of the city, we're right
restaurants, public transportation and the b
2 People
Add People
justin smith
OWNER
user@user.com
NOT OPENED

Choosing digital tools that streamline workflows.

With the right tools, you can empower employees while avoiding wasted effort and unnecessary security risks. All-in-one solutions that are simple to use and easy to integrate are ideal, as well as online browser-based apps that work on any device. Taking a unified approach to using remote collaboration tools can improve the flow of work within remote teams. Similarly, when separate teams use different sets of tools, it can disrupt their workflow.[23] According to a global study on the hybrid workplace, 70% of Gen Z enterprise workers say they'd actually switch jobs if they could use tools that make them more efficient.[24]

One key area where automation and integration can speed up workflow and increase productivity is document flow. **72% of enterprise workers name "searching for, sharing, and accessing files" as a task that gets in the way of doing their job effectively.[25]**

Creating, collaborating on, and approving documentation is still a key requirement for most businesses. And for companies that need to circulate documents to customers, the processes are even more vital.

A cost savings and business benefits analysis conducted by Forrester Consulting[26] shows that using an all-in-one solution that integrates with other productivity tools can create significant gains in workflow speed and efficiency. This can lead to reduced costs, improved customer experience, and the capacity to take on additional business.

Adobe Acrobat is an integrated, all-in-one PDF and e-signature solution that works securely on any device. It lets everyone create, collaborate on, and sign PDFs—everywhere. You can use it from within your preferred Microsoft app such as Microsoft 365 (with Acrobat Sign also being Microsoft's preferred e-signature solution). It speeds up sending, signing, tracking, and managing documents while helping to maintain security and compliance.

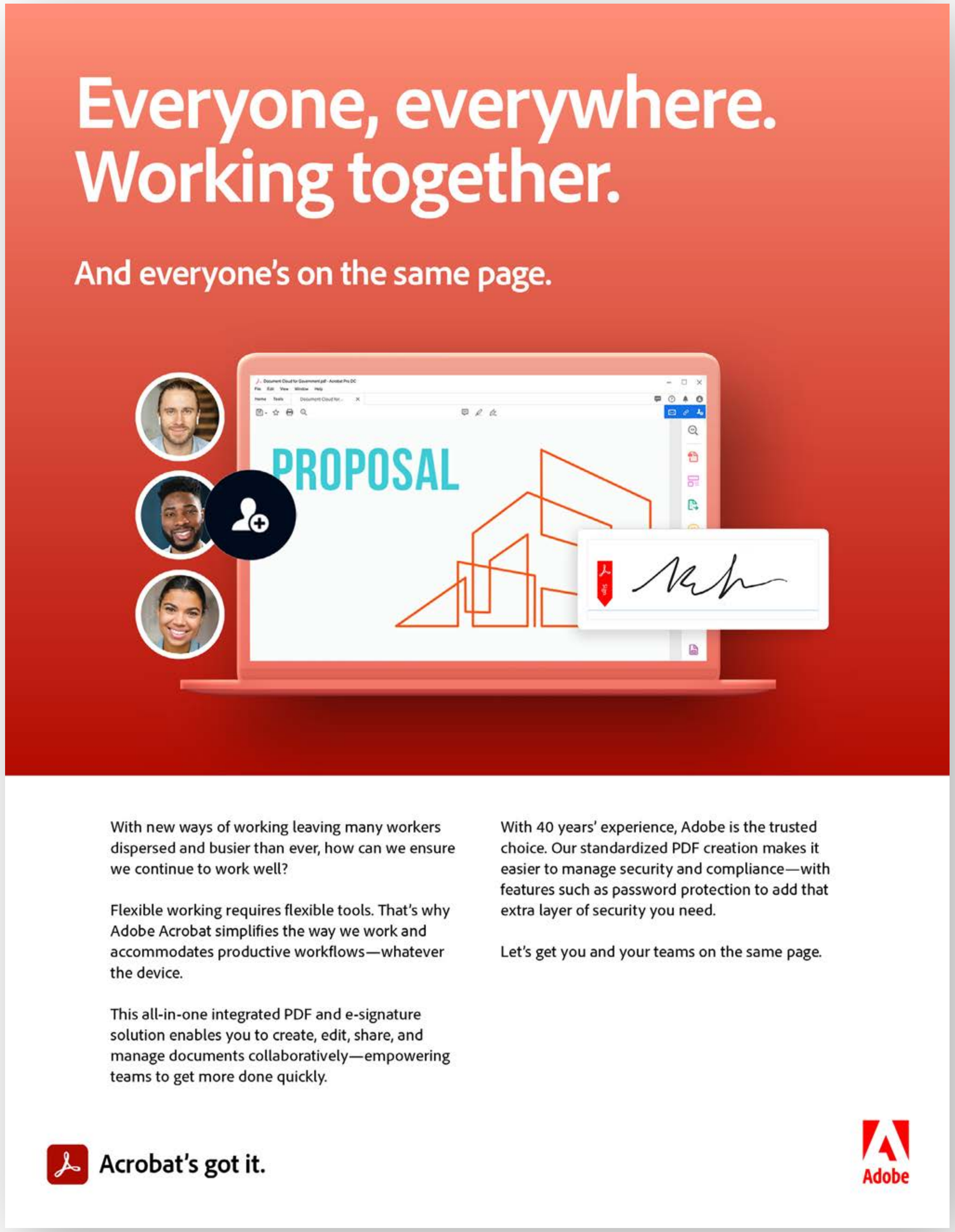
Forrester's study shows that Adobe Acrobat Sign offers businesses an average return on investment of 519%, with a 25% reduction in e-signature solution costs. When used with Microsoft applications, it offers average back-office efficiency gains of 47%, with savings in transaction times worth $9.2 million. Acrobat Sign also supports more accuracy, with 85% of businesses reporting a reduction in document errors with the solution, improving the customer experience—and 58% experiencing a reduction in employee churn.[27]

6 Secure today, secure tomorrow...

Moving to working well will require flexibility and creativity from IT leadership to make sure it's always seamless and secure—now and in the future. The challenges may expand and evolve as time goes on, but the principles will remain the same.

To give everyone as much freedom as possible to work in the way that's right for them, we need to consider the individual while safeguarding the interests of the business. Looking for integrated solutions that can save money, reduce your tech stack, and minimize workflow friction will help you support everyone, everywhere.

Acrobat brings teams together. We get everyone on the same page, even when they're apart. This all-in-one solution enables secure, smart collaboration and empowers individuals to work from anywhere and everywhere.



Everyone, everywhere. Working together.

And everyone's on the same page.

With new ways of working leaving many workers dispersed and busier than ever, how can we ensure we continue to work well?

Flexible working requires flexible tools. That's why Adobe Acrobat simplifies the way we work and accommodates productive workflows—whatever the device.

This all-in-one integrated PDF and e-signature solution enables you to create, edit, share, and manage documents collaboratively—empowering teams to get more done quickly.

With 40 years' experience, Adobe is the trusted choice. Our standardized PDF creation makes it easier to manage security and compliance—with features such as password protection to add that extra layer of security you need.

Let's get you and your teams on the same page.

Acrobat's got it.

Adobe

Why Adobe?

Business still runs on documents, and today's teams expect to work seamlessly on them from anywhere using trusted, well-integrated software. Made by the inventor of PDFs, Adobe Acrobat is the single PDF and e-signature tool made for today's hybrid organizations. With an all-in-one solution from a trusted brand like Adobe Acrobat, your organization can operate with confidence in the flow of work.

Learn more ›

Contact us ›

Adobe

Sources

[1] Laurence Goasduff, "Digital Workers Say Flexibility Is Key to Their Productivity," Gartner, June 9, 2021.

[2] Danielle Guetta, "The 2022 Workforce Security Report," Check Point Software Technologies, February 2, 2022.

[3] "Building a Human-Centered Organization," IBM.

[4] "World-Class Legal Services for Everyone," Adobe customer success story for Slater & Gordon.

[5] *The Financial Impact of a Positive Employee Experience*, IBM and Globoforce, 2018.

[6] Ibid.

[7] *The Future of Time*, a global study by Adobe Document Cloud, August 2021.

[8] Brandon Rigoni and Bailey Nelson, "Many Millennials Are Job-Hoppers—But Not All," Gallup, August 9, 2016.

[9] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM Newsroom, July 28, 2021.

[10] *2022 Data Breach Investigations Report*, Verizon, 2022.

[11] *Netmotion Software Experience Monitoring Report 2021,* Netmotion, 2021.

[12] *Rebellions & Rejections Report*, HP Wolf Security, 2021.

[13] Danielle Guetta, "The 2022 Workforce Security Report," Check Point Software Technologies, February 2, 2022.

[14] *Head in the Clouds: How Remote Working Behaviours Are Exposing Organisations to Cyber Risks*, Trend Micro.

[15] *Rebellions & Rejections Report*, HP Wolf Security, 2021.

[16] *Cybersecurity Team's Guide: Balancing Risk, Security and Productivity*, Delinea, 2021.

[17] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM Newsroom, July 28, 2021.

[18] Ray Canzanese, "Cloud and Threat Report: Shadow IT in the Cloud," Netskope, February 24, 2021.

[19] Ariel Diaz, "71+ SaaS Statistics &Trends," Vendr, August 17, 2020.

[20] Chris Silva, Manjunath Bhat, Dan Wilson, and Ryan Stefani, *Gartner Market Guide for SaaS Management Platforms*, Gartner and BetterCloud, February 10, 2021.

[21] *The Future of Time*, a global study by Adobe Document Cloud, August 2021.

[22] "IBM Report: Cost of a Data Breach Hits Record High During Pandemic," IBM Newsroom, July 28, 2021.

[23] Jaime Teevan, Nancy Baym, Jenna Butler, Brent Hecht, Sonia Jaffe, Kate Nowak, Abigail Sellen, and Longqi Yang (Eds.), *Microsoft New Future of Work Report 2022*, Microsoft, 2022.

[24] *The Future of Time*, a global study by Adobe Document Cloud, August 2021.

[25] Ibid.

[26] *The Total Economic Impact™ of Adobe Acrobat Sign*, January 2022.

[27] Ibid.