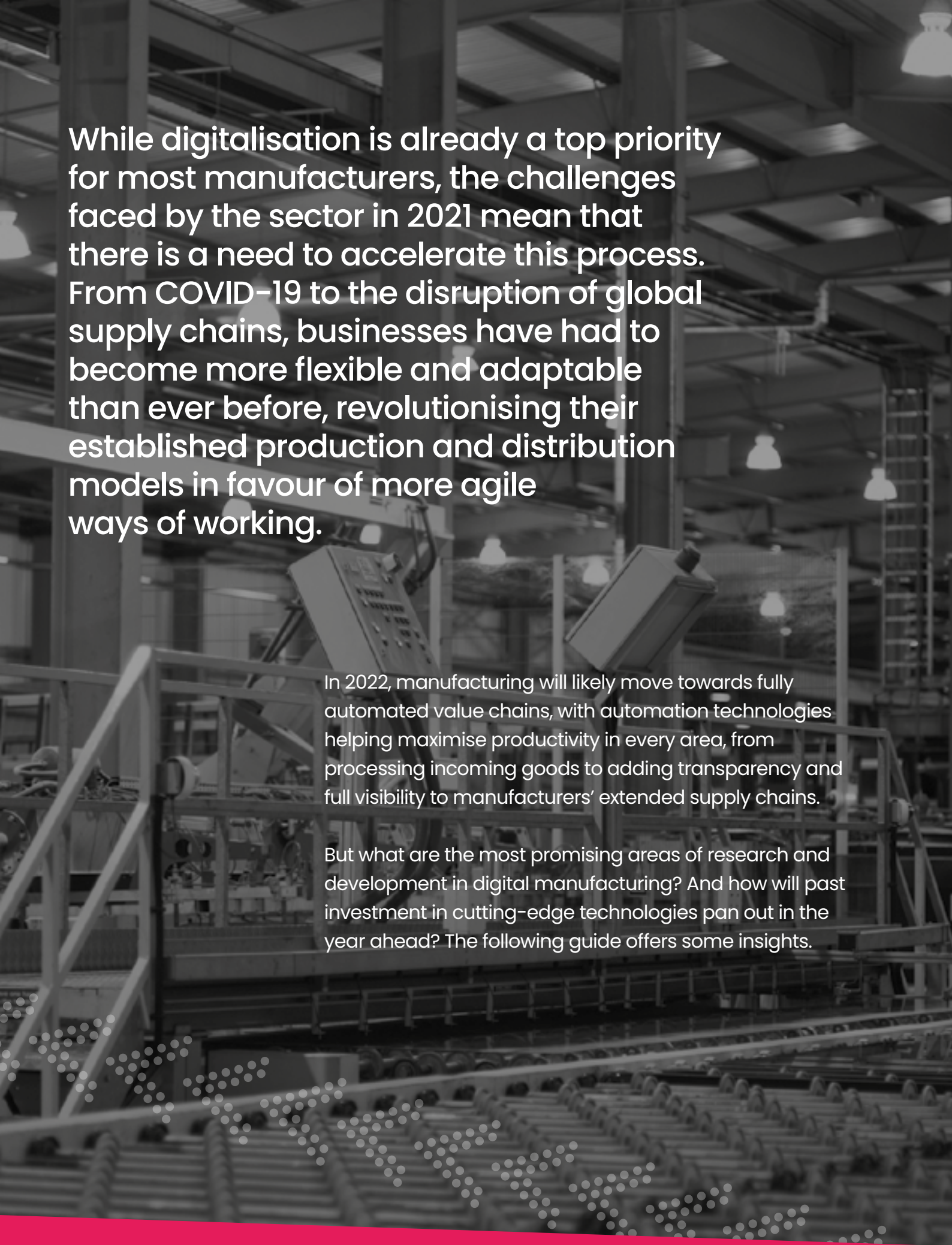
Challenges and opportunities for digital manufacturing in the year ahead

euautomation



While digitalisation is already a top priority for most manufacturers, the challenges faced by the sector in 2021 mean that there is a need to accelerate this process. From COVID-19 to the disruption of global supply chains, businesses have had to become more flexible and adaptable than ever before, revolutionising their established production and distribution models in favour of more agile ways of working.

In 2022, manufacturing will likely move towards fully automated value chains, with automation technologies helping maximise productivity in every area, from processing incoming goods to adding transparency and full visibility to manufacturers' extended supply chains.

But what are the most promising areas of research and development in digital manufacturing? And how will past investment in cutting-edge technologies pan out in the year ahead? The following guide offers some insights.

The good news: Hyperautomation will deliver results

Hyperautomation is a buzzword we're still using from 2020, when Gartner included it in that year's predictions on the most impactful automation trends. Since then, organisations have had to cut their spending and focus on maximising existing resources, while at the same time speeding up their digital transformation journeys.

The result is that manufacturers are focusing on the use of AI and machine learning to automate end-to-end, redesigning inefficient processes and reducing human intervention to the minimum.

Hyperautomation is a business-driven, disciplined approach that organisations use to rapidly identify, vet and automate as many business and IT processes as possible. Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms.

Many organisations have already implemented programmes to reach end-to-end automation, but in 2022 these initiatives will accelerate. While the majority of digital enterprises will start moving towards fully automated value chains, early adopters will start reaping the benefits of their investments and gain a substantial competitive advantage.

Gartner predicts that by 2025, the final customer will be the first human to touch more than 20 per cent of all manufactured products, with all stages of production, packaging and delivery being handled without human intervention. At this pace, those who haven't yet adopted hyperautomation will have just a couple of years to catch up.

The advice:
Explore the potential of virtual experiences

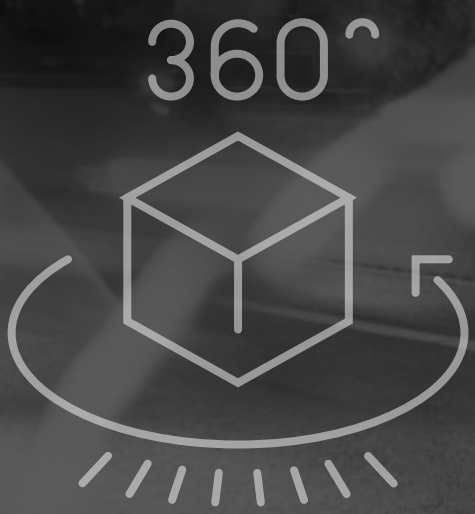
According to Gartner's IT automation predictions for 2022, by 2025 40 per cent of physical experience-based businesses will improve financial results by adding paid virtual experiences.

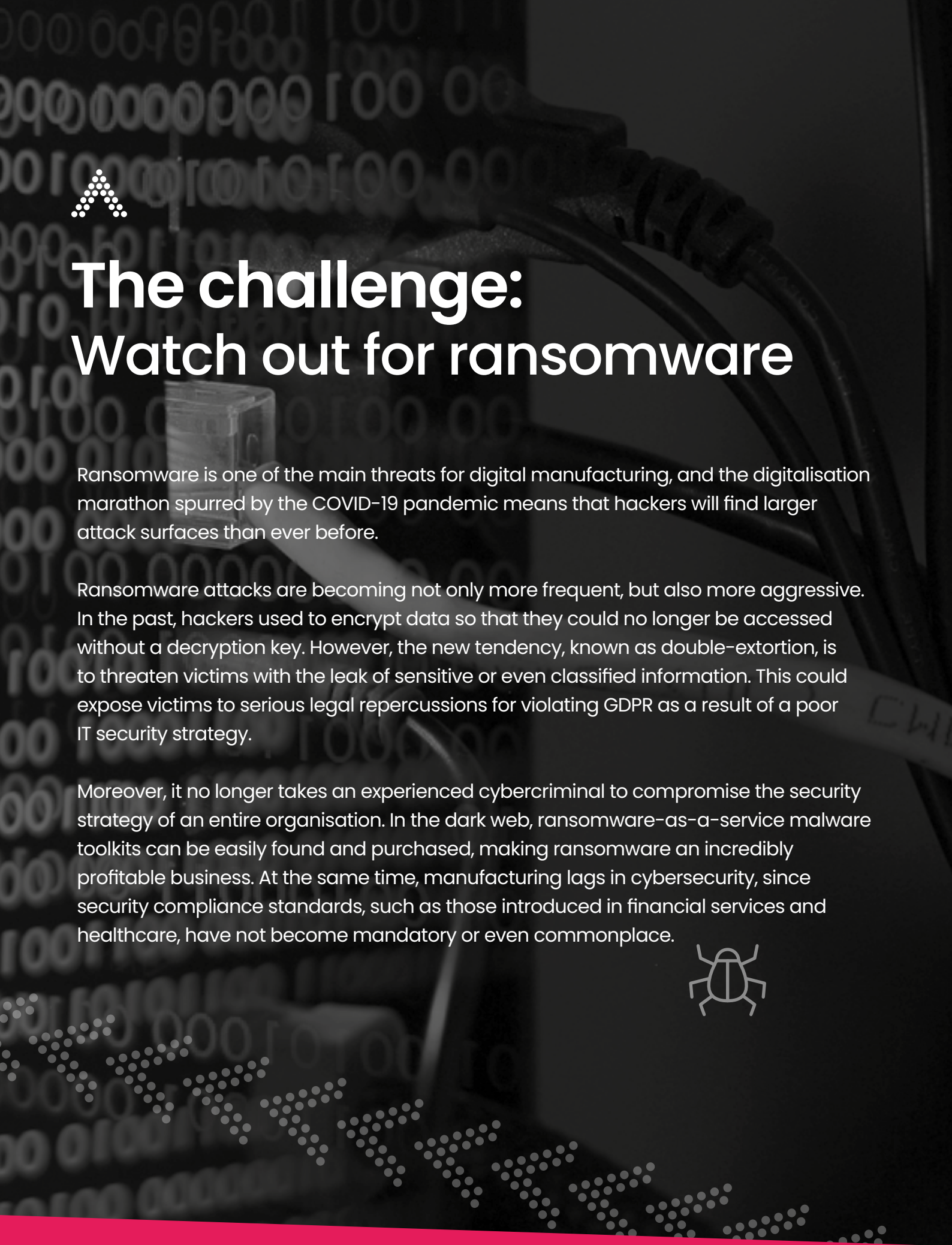
While Gartner mainly refers to the potential of virtual assets for enterprises such as sport venues, theatres and museums, VR experiences can add tremendous value in manufacturing too.

For example, investing in state-of-the-art presentation and simulation technologies to offer demonstrations of new products and services can make a huge difference when travel restrictions prevent face-to-face interactions with potential customers. These technologies can also dramatically expand a business' customer pool, transcending geographical barriers while fostering new partnerships.

In this sense, research is progressing to make virtual experiences as close as possible to in-person ones. For example, haptic technology could realistically replicate the sense of touch. These technologies use pressure and vibrations to replicate the signals human nerves process when we touch something, allowing people to experience the textures of materials remotely.

Virtual experiences will also become increasingly popular for training. VR-based learning can in fact lower costs while increasing information retention, all the while facilitating social distancing. For example, any employee equipped with AR glasses can be guided remotely by a more experienced colleague, who can simply simulate the actions to be performed. This eliminates the need to fly specialists across the globe, lowering costs while retaining the possibility to be trained by the best specialists in a given field.





The challenge:
Watch out for ransomware

Ransomware is one of the main threats for digital manufacturing, and the digitalisation marathon spurred by the COVID-19 pandemic means that hackers will find larger attack surfaces than ever before.

Ransomware attacks are becoming not only more frequent, but also more aggressive. In the past, hackers used to encrypt data so that they could no longer be accessed without a decryption key. However, the new tendency, known as double-extortion, is to threaten victims with the leak of sensitive or even classified information. This could expose victims to serious legal repercussions for violating GDPR as a result of a poor IT security strategy.

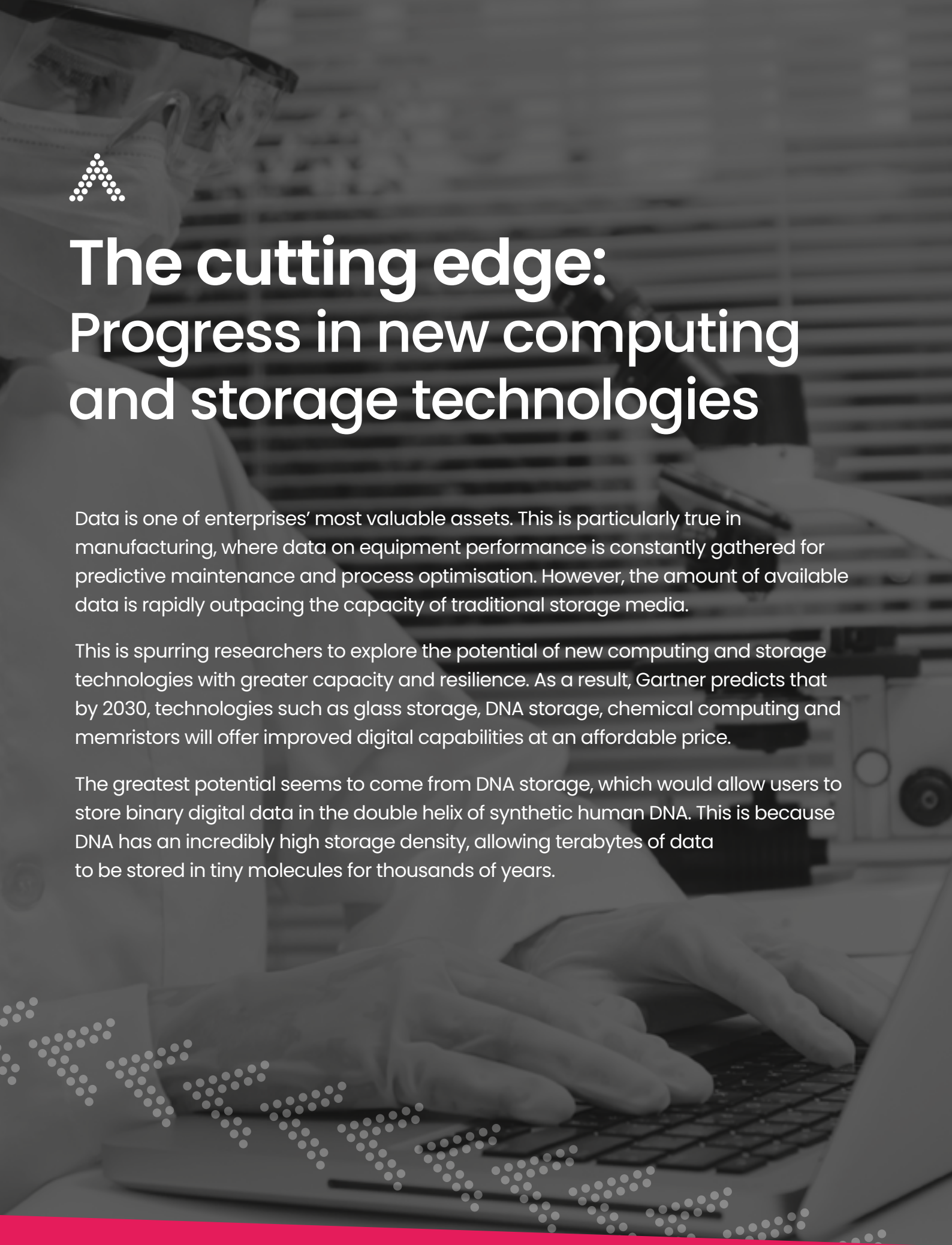
Moreover, it no longer takes an experienced cybercriminal to compromise the security strategy of an entire organisation. In the dark web, ransomware-as-a-service malware toolkits can be easily found and purchased, making ransomware an incredibly profitable business. At the same time, manufacturing lags in cybersecurity, since security compliance standards, such as those introduced in financial services and healthcare, have not become mandatory or even commonplace.

In the past, the most recommended defence strategy was to use multiple backup solutions, ensuring that at least one of those would be offline at all times. However, double-extortion means that this is no longer enough.

Content scanning and email filters can add an extra layer of protection and detect malicious links, but it's also important to develop a standardised security protocol throughout the company and to train employees to recognise suspicious emails and links.

Finally, it's important to come up with a recovery plan for a potential attack, including strategies to mitigate legal and reputational consequences and a PR plan to explain the situation to customers, investors and the press.

According to Cybersecurity Ventures, by 2031 there will be a ransomware attack every two seconds, with damage exceeding USD 265 billion. This is based on figures predicting a 30 per cent yearly growth in damage costs over the next ten years.

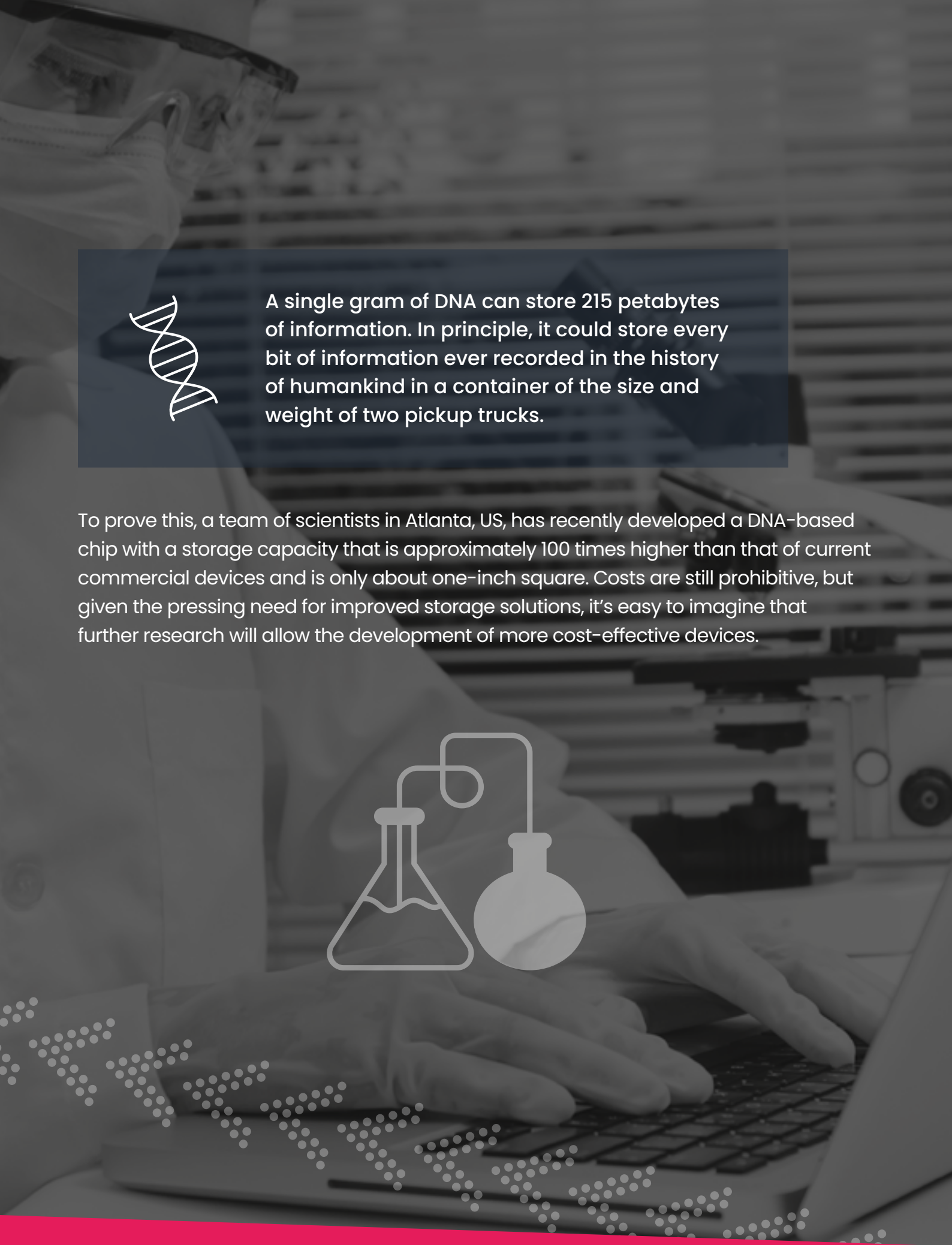


The cutting edge: Progress in new computing and storage technologies

Data is one of enterprises' most valuable assets. This is particularly true in manufacturing, where data on equipment performance is constantly gathered for predictive maintenance and process optimisation. However, the amount of available data is rapidly outpacing the capacity of traditional storage media.

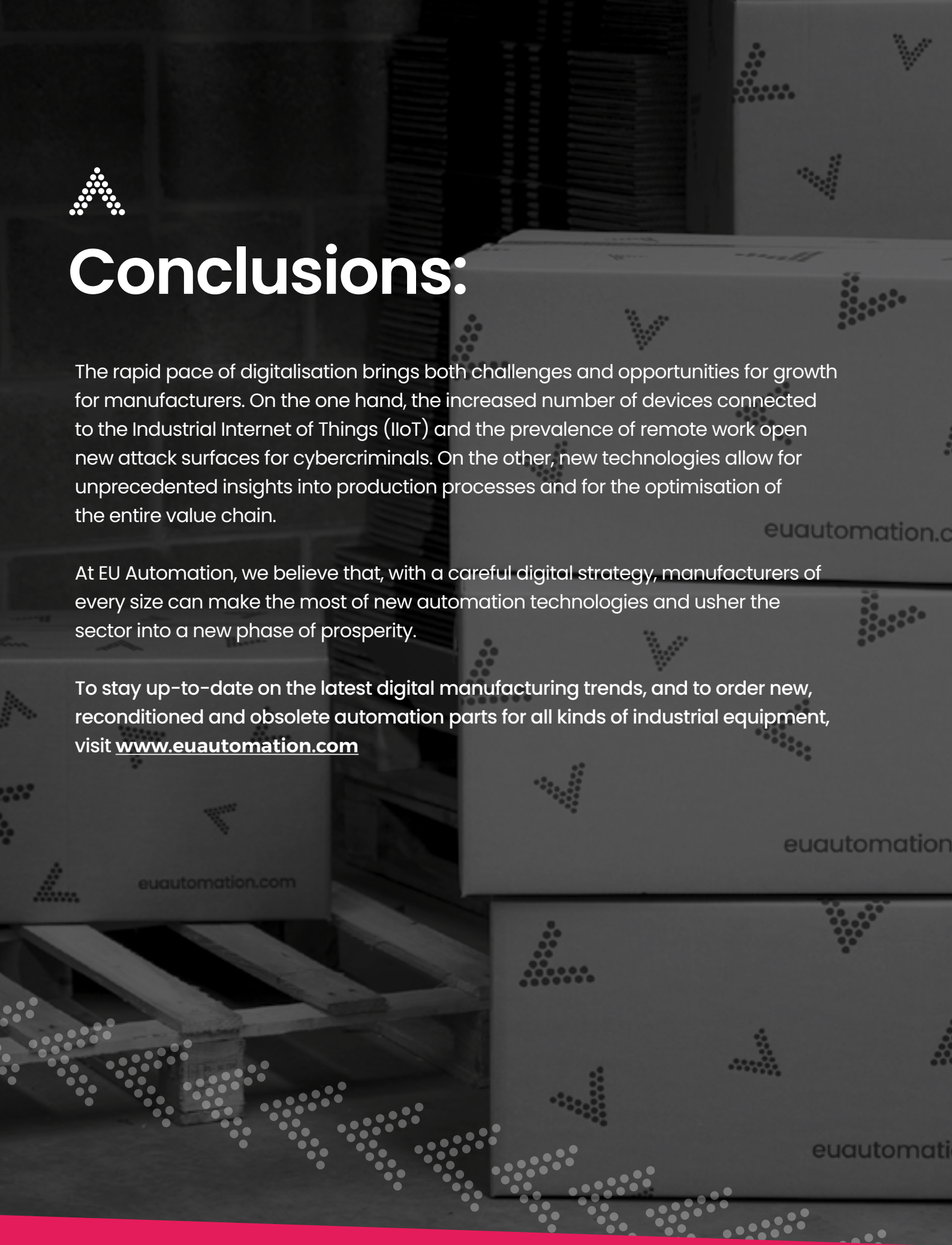
This is spurring researchers to explore the potential of new computing and storage technologies with greater capacity and resilience. As a result, Gartner predicts that by 2030, technologies such as glass storage, DNA storage, chemical computing and memristors will offer improved digital capabilities at an affordable price.

The greatest potential seems to come from DNA storage, which would allow users to store binary digital data in the double helix of synthetic human DNA. This is because DNA has an incredibly high storage density, allowing terabytes of data to be stored in tiny molecules for thousands of years.



A single gram of DNA can store 215 petabytes of information. In principle, it could store every bit of information ever recorded in the history of humankind in a container of the size and weight of two pickup trucks.

To prove this, a team of scientists in Atlanta, US, has recently developed a DNA-based chip with a storage capacity that is approximately 100 times higher than that of current commercial devices and is only about one-inch square. Costs are still prohibitive, but given the pressing need for improved storage solutions, it's easy to imagine that further research will allow the development of more cost-effective devices.



Conclusions:

The rapid pace of digitalisation brings both challenges and opportunities for growth for manufacturers. On the one hand, the increased number of devices connected to the Industrial Internet of Things (IIoT) and the prevalence of remote work open new attack surfaces for cybercriminals. On the other, new technologies allow for unprecedented insights into production processes and for the optimisation of the entire value chain.

At EU Automation, we believe that, with a careful digital strategy, manufacturers of every size can make the most of new automation technologies and usher the sector into a new phase of prosperity.

To stay up-to-date on the latest digital manufacturing trends, and to order new, reconditioned and obsolete automation parts for all kinds of industrial equipment, visit **www.euautomation.com**