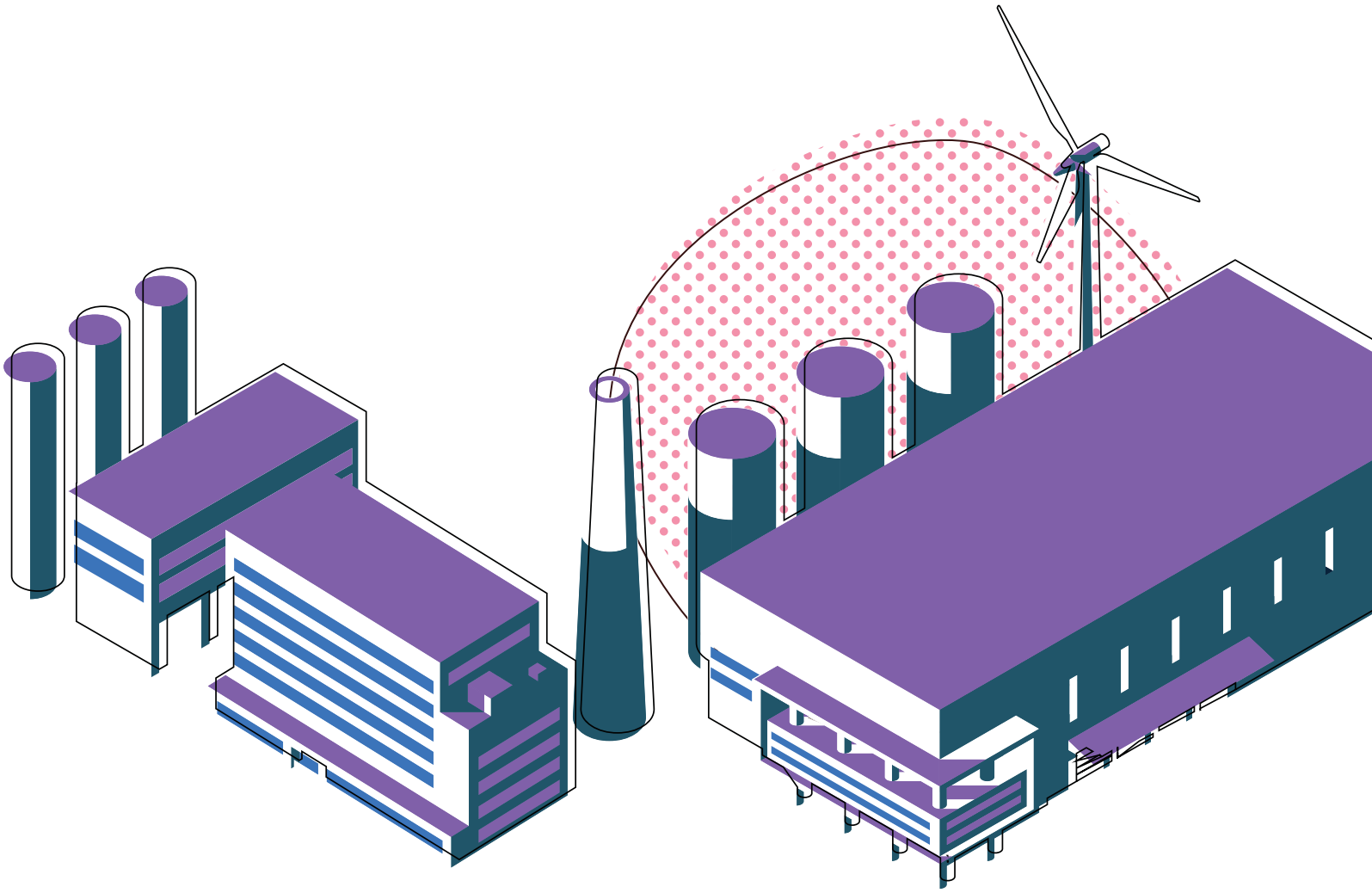
Debunking 6 Industrial IoT Myths

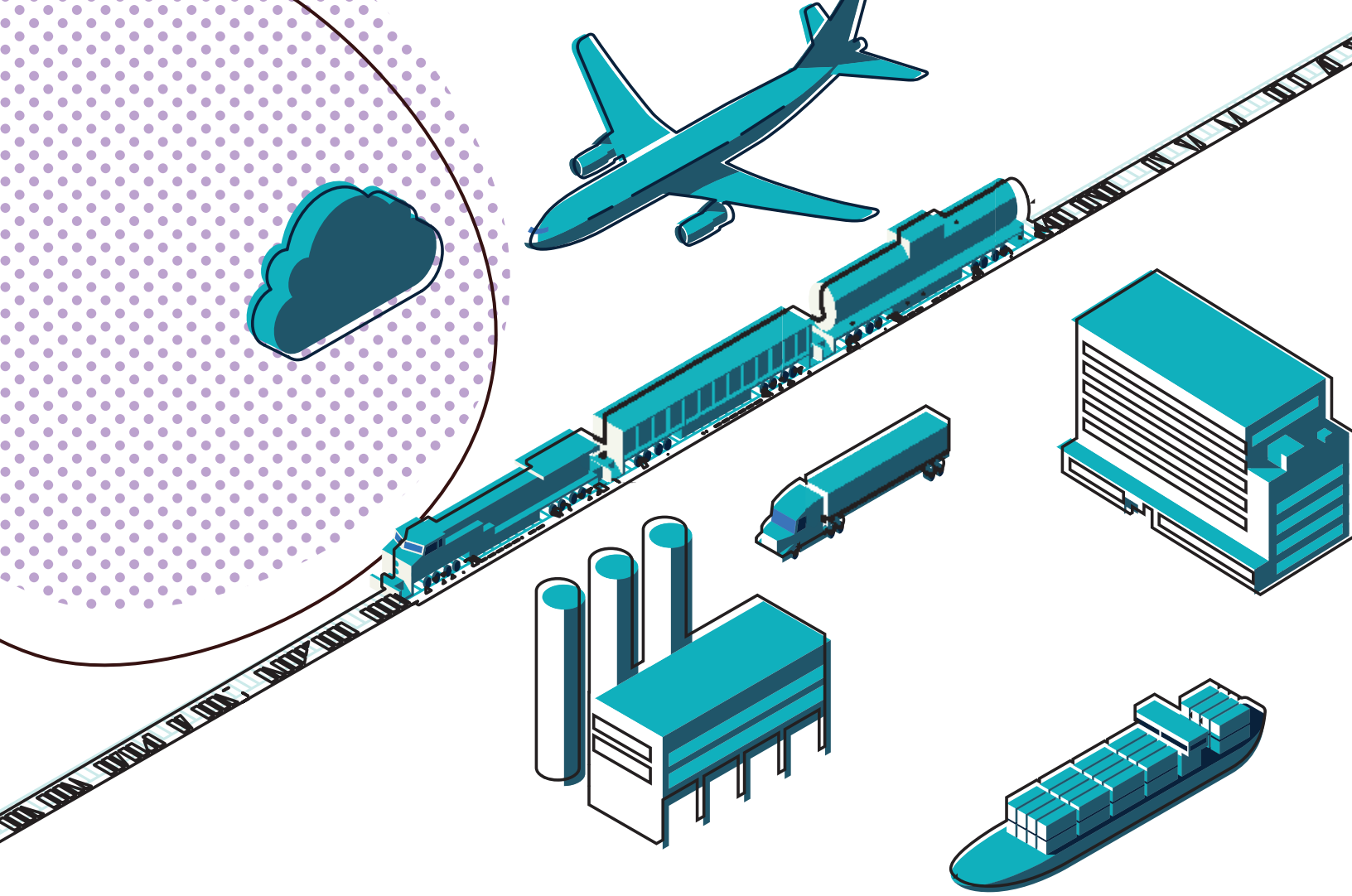
Debunking Common Myths about Digital Transformations for Manufacturers



It’s no secret that manufacturing is changing.

Business models are changing too. Product ownership is evolving toward service consumption models—Everything as a Service—wherein customers pay only for what they use. To reflect these shifts in technology, attitude and business process, products are getting smarter. So are the factories that make them, the products those factories build and even the cities we live in. The Internet of Things (IoT) is the key enabler for this new, connected world, and the first step for anyone in a manufacturing or industrial role is to understand service asset conditions.

To support this growing demand, manufacturers must diversify their revenue streams from equipment sales to digital services and software. Building smart solutions results in more-resilient and repeatable revenue streams that don’t require direct equipment sales.



Is your company ready?

And if it's not, what about your competitors? Are they ready? Gartner thinks so. "By 2025, 50% of industrial enterprises will use industrial Internet of Things (IIoT) platforms to improve factory operations, up from 10% in 2020," the company predicted.[1] In addition, by 2024, 50% of industrial enterprises will manage IIoT platform deployments from up to six vendors, up from less than 10% of industrial enterprises today.[2]

What does that mean? It means that IIoT will be a $500 billion (USD) market by 2025, according to McKinsey.[3]

Manufacturing, transportation and utilities are three industries that particularly stand to gain from this technology. In fact, Gartner predicts that IIoT will eventually replace legacy control systems.

Equipment manufacturers that haven't adopted IoT (or IIoT) now compete against companies that do. Those competitors have significantly different cost and revenue structures, which lets them offer their customers a more flexible range of purchase options and service programs that operate more efficiently.

IIoT has so much potential to disrupt manufacturing that some people are calling it the Fourth Industrial Revolution, or 4IR.[4]

So what's stopping you? Chances are you think that implementing IIoT is too hard. Too expensive. Or you don't have the expertise. But the transition is easier than you think.

To set the record straight, in this eBook we look at a few IIoT myths you may have heard—wrong assumptions that may stand in the way of your company's success.

MYTH 1

You need to buy new equipment to adapt to IIoT.

You don't want to replace equipment that still works.

And you shouldn't have to. In fact, the average age for a piece of production equipment is 22.5 years[5]—and typically these pieces of equipment do not run on uniform or open protocols.

But that doesn't get in the way of using IIoT. You can still use your reliable legacy hardware. That is, as long as you use an IIoT platform that lets you take advantage of all your brownfield assets, introduce greenfield assets as you need them and keep your network costs down.

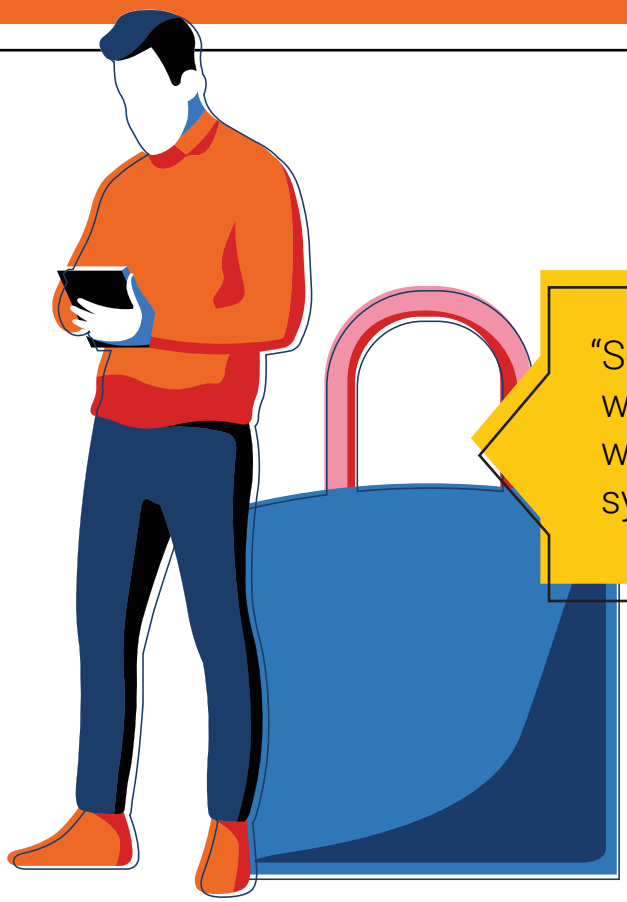
How? A modern IIoT platform can tell you how, when and where your equipment is used. You'll know when you need to add enhancements. You'll also learn which existing features aren't being used, so you can deprecate the right equipment and focus on optimizing the features people actually rely on. In fact, according to McKinsey, most of IIoT's value comes from improving brownfield sites.[6]

So, how do you do this? One strategy is to connect an inexpensive add-on device to your manufacturing equipment—a low-power, wireless hardware unit that adds IIoT connectivity to legacy hardware. Some of these units support more than 100 kinds of devices and more than 300 protocols—including low-power WAN. Organizations using these units found they reduced average time to repair and cut their service costs by 5 to 7%.

Manufacturers can also certify their equipment to run with these units, so you know it'll work out of the box—without needing a programmer to write custom code.

MYTH 2

IIoT expands the attack surface and makes industrial equipment more vulnerable to attack.



> "Security is a vital concern within our company. We don't want to add anything to our system that can put it at risk."

There's no question that detecting and repairing vulnerabilities is more important than ever because of the rise in hacker attacks, such as the Colonial Pipeline ransomware attack.[7] Gartner predicts that by 2025, cyberattackers will learn how to weaponize operational technology environments to successfully harm or kill humans,and that the financial impact of these attacks will reach more than $50 billion by 2023[8]—for which CEOs could be held personally liable.[9] Attacks like this have already been detected.[10]

The thing is, older hardware is already more vulnerable because it was designed before this type of concern came along. But these add-on units can address device vulnerabilities through centrally controlled and audited firmware update rollouts, and can isolate compromised devices.

That gives manufacturers a secure software development and governance process that supports vulnerability management and reporting, which can close newly detected vulnerabilities with security-tested hotfixes.

The add-on units also add encryption. Throughout your system, data needs to be encrypted during transmission, without using broker technology for device connections. That means broker-based attacks are not possible, and it ensures that compromised or malicious device endpoints have no access to data originating from other devices.

MYTH 3

You need a team of developers and coders to build IIoT solutions.

"Okay, but I don't have the budget for that. Have you seen the salary for IIoT specialist programmers lately?!"

You don't have to hire an entirely new team of programmers.

Good thing. Just calculating the time and costs for a brand-new IIoT project, constructed from scratch, is more work than you have time for.

But some of these devices have out-of-the-box rules for business users. Power users can build analytics for manufacturing hardware using drag-and-drop tools—without coding. These rules let you monitor events and act on them.

Often, this is through the use of an electronic or digital "twin," with which you can view and interact. It keeps track of the device's current and historical state. The electronic twin view works virtually; you don't have to be there in person. Organizations that already implemented IIoT technology such as electronic twins found out how useful it was during the COVID-19 pandemic, when they could manage equipment remotely without having to go on-site.[11]

These systems are designed for people of all skill levels—not just IT professionals or software developers. On the other hand, if you want to engage IT in the process, some of them support that functionality as well—they just don't require it.

MYTH 4

You need a team of data scientists to make sense of all that data.

Collected data doesn't do any good if people don't look at it. In fact, some studies have found that 73% of manufacturers' collected data goes unused.[12]

But the same no-code/low-code setup that enables you to collect the manufacturing data helps you analyze it too. Some platforms include streaming analytics engines to analyze data in real time using machine learning and predictive analytics models.

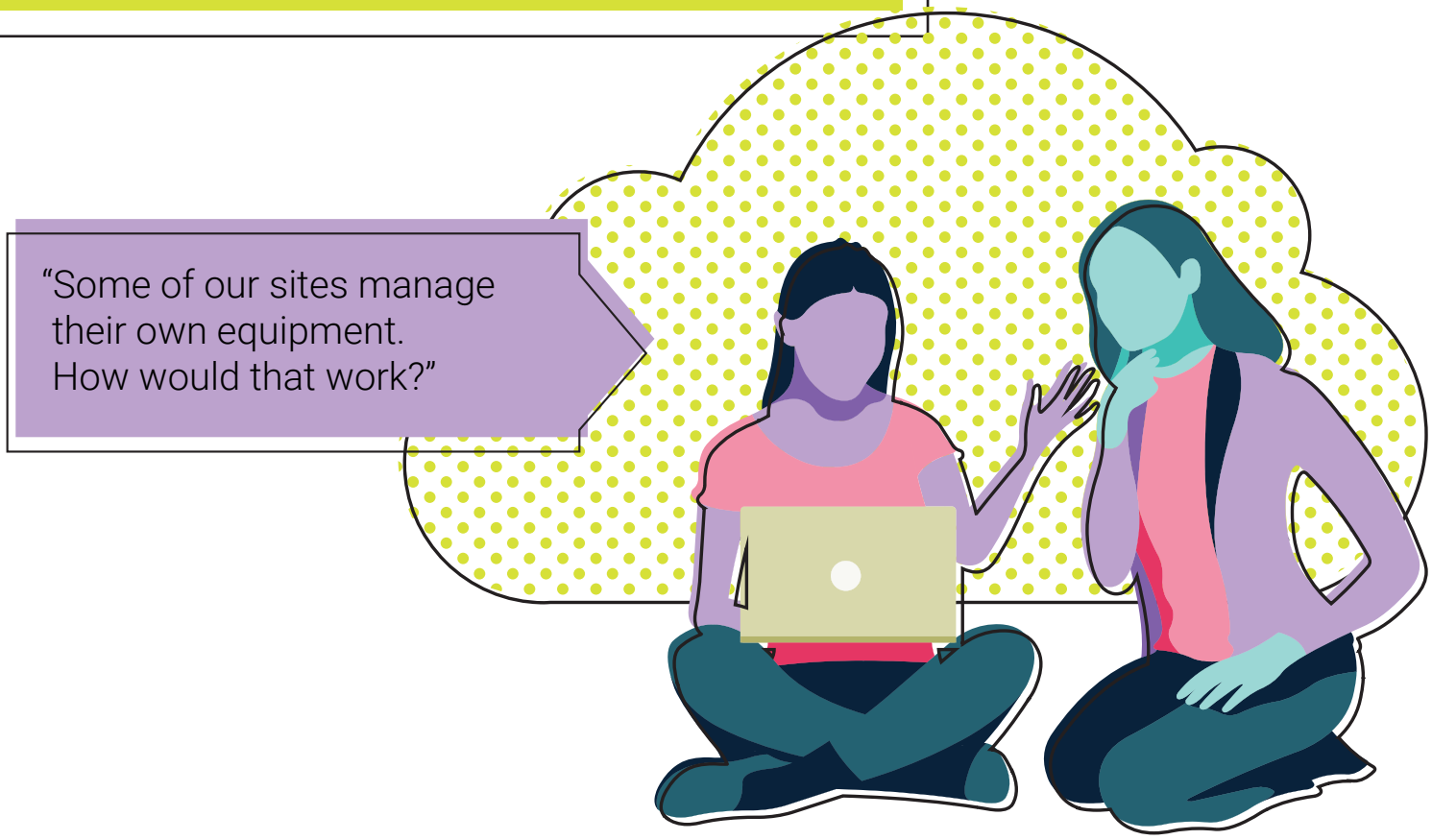
Technicians, engineers and operations professionals can set up analytics that help them make better decisions. The system also saves historical data, giving you a permanent record for trendspotting.

For example, you could create a dashboard to pull together data in a single view that shows the status of every device in the manufacturing facility. Then you could create a preventive maintenance program or use predictive models to figure out the remaining useful life of each device. You can set up the system to control who sees the dashdboard and manage how much they are authorized to view.

And if your company is already using third-party applications or enterprise systems to track and analyze data, some systems can integrate with them too—often without programming.

MYTH 5

You have to be 100% cloud-based or 100% on-premises.



It doesn't matter. You can use one, the other or a mix. Sites on the edge can collect and analyze data locally, then aggregate data on-site to reduce latency and to manage the amount of data that is sent back to headquarters. That keeps the volume of data from overwhelming the transmission—which matters even more if it's in a location with slow or no connectivity. The organization still can monitor industrial processes in real time. You don't need a permanent data connection.

The result: Local sites can manage their own data and events, acting more quickly and making decisions locally—at the plant, on the factory floor or in the field. IIoT sensors can even be deployed in places that are too inhospitable for humans.[13]

In fact, according to Gartner, "The IIoT platform must be able to be deployed on the edge with adequate computing capabilities to manage the data, integrate with replacement assets or new software capabilities on-site and process data and events for transmission to extraction." Edge processing can also be more environmentally friendly.[14]

IIoT processing on the edge safeguards sensitive data by ensuring that nothing is transmitted, stored or visible outside its location. IIoT data is a valuable asset that must be fully protected to the highest recognized standards. In some cases, this is a matter of regulatory requirement as well as best practices.

MYTH 6

It can take months or years to get a solution up and running

This project doesn't take long. You can put together a minimum viable product in less than a month, start collecting and analyzing data and use a stepping-stone approach to add value over time. The result can be an initial ROI of 90 days or less.

Some platforms provide access to professional services or prepackaged offerings to help you set up and get it running. That way, even if you don't have the in-house resources, you can still get the solutions you need to build a business case and to maintain your competitive advantage.

Case in point: Gardner Denver, an industrial equipment provider, launched and commercialized an IIoT-enabled condition monitoring solution that dramatically reduced the downtime for the equipment of one of its customers—in just six weeks.

"Sounds like it's worth looking at! Where do I go now?"

So why Software AG?

We have the expertise, the experience and the industry know-how. Software AG has been solving these problems for some of the world's biggest companies for decades. Consider:

- **70% of the Fortune 1000 chooses Software AG**
  We have earned industry-leading analyst ratings across all our solutions
- **You can work with Software AG — a company that offers a comprehensive solution in an emerging technology (not just haphazard, disparate pieces of it)**

Cumulocity IoT® is Software AG's number one self-service, low-code IoT platform, available for less than $200 per device. It's the only platform that includes the leading streaming analytics engine, Apama®, built in. If you need more, companies with built-in machine-learning models can plug those models directly into Cumulocity IoT for immediate results without the risk of coding errors.

As you can see, it can be fast and easy to begin collecting actionable data—and then insights from that data—to improve manufacturing processes and business decision-making. You can enhance your customers' experience with faster time to market and responsiveness—improving retention, growth and acquisition.

Want to learn more?

Find out how Software AG can help.

1. Gartner, "Magic Quadrant for Industrial IoT Platforms," Oct. 2020, https://www.gartner.com/doc/reprints?id=1-2452KT61&ct=200911&st=sb.
2. Gartner, "Critical Capabilities for Industrial IoT Platforms," Oct. 2020, https://www.gartner.com/doc/reprints?id=1-24M0HOQP&ct=201117&st=sb.
3. McKinsey & Company, "Leveraging Industrial IoT and advanced technologies for digital transformation," Feb. 2021, https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/a%20manufacturers%20guide%20to%20generating%20value%20at%20scale%20with%20iiot/leveraging-industrial-iot-and-advanced-technologies-for-digital-transformation.pdf
4. McKinsey & Company, "Industry 4.0," July 2019, https://www.mckinsey.com/~/media/mckinsey/industries/advanced%20electronics/our%20insights/capturing%20value%20at%20scale%20in%20discrete%20manufacturing%20with%20industry%204%200/industry-4-0-capturing-value-at-scale-in-discrete-manufacturing-vf.pdf
5. Software AG, "How to leverage IIoT for smart factories," Feb. 2021, https://blog.softwareag.com/iiot-smart-factories
6. McKinsey & Company, "Industrial IoT generates real value—if business overcome six myths," June 2020, https://www.mckinsey.com/business-functions/operations/our-insights/industrial-iot-generates-real-value-if-businesses-overcome-six-myths
7. Bloomberg, "Hackers Breached Colonial Pipeline Using Compromised Password" June 2021, https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
8. Gartner, "Gartner Predicts by 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans," June 2021, https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we
9. Gartner, "Gartner Predicts 75% of CEOs Will Be Personally Liable for Cyber-Physical Security Incidents by 2024," Sept. 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl
10. The New York Times, "'Dangerous Stuff,' Hackers Tried to Poison Water Supply of Florida Town," Feb. 2021, https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html
11. McKinsey & Company, "Coronavirus: Industrial IoT in challenging times," April 2020, https://www.mckinsey.com/industries/advanced-electronics/our-insights/coronavirus-industrial-iot-in-challenging-times
12. Software AG, "How to leverage IIoT for smart factories," Feb. 2021, https://blog.softwareag.com/iiot-smart-factories
13. The Engineer, "IIOT sensors need protection in harsh environments," Feb 2020, https://www.theengineer.co.uk/iiot-sensors-coatings
14. TechNative, "Reducing Emissions, Carbon Footprint with Edge Computing," June 2020, https://technative.io/reducing-emissions-carbon-footprint-with-edge-computing

software AG