

Industrial networks:

Can AI do the heavy lifting?

Understanding the complex impacts of artificial intelligence on
enterprise networks in the manufacturing and automotive sectors



For many years, robotics and automation have enabled streamlined production lines – increasing precision and boosting productivity.

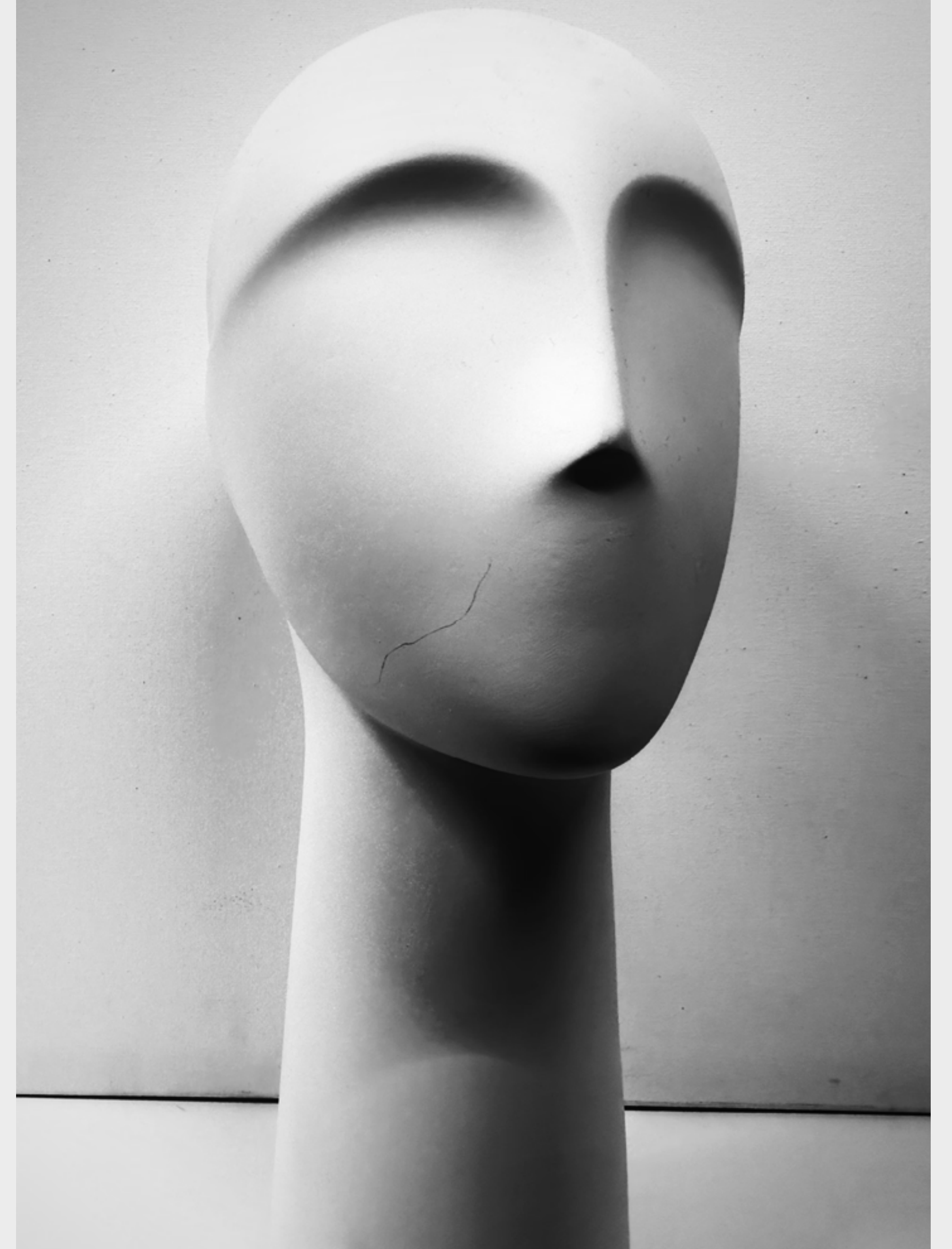
Now, with the advent of AI-powered systems such as machine learning, predictive maintenance has further enhanced production efficiency by reducing downtime.

Emerging technologies have the potential to vastly improve supply chain management; by predicting demand, managing inventory and reducing waste. There is no doubt that AI is transforming the global automotive and manufacturing industries. And connectivity is the very foundation this transition relies on.

Change is happening fast

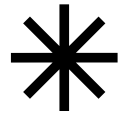
This report offers insights into the critical – and sometimes conflicting – effects of artificial intelligence (AI) on enterprise networks in the manufacturing and automotive sectors.

The report is based on our research survey of 103 senior decision-makers from these industries. They represent a robust sample of 20% of our broader survey of hundreds of senior decision-makers across a wide range of industry verticals in four of the world's biggest markets – the US, the UK, Germany and France, enabling insightful cross-sector and cross-border comparisons. All respondents have a decision-making role in companies with over 2,000 employees, and all are involved in decisions on their company's network development strategy.



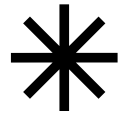
Executive summary





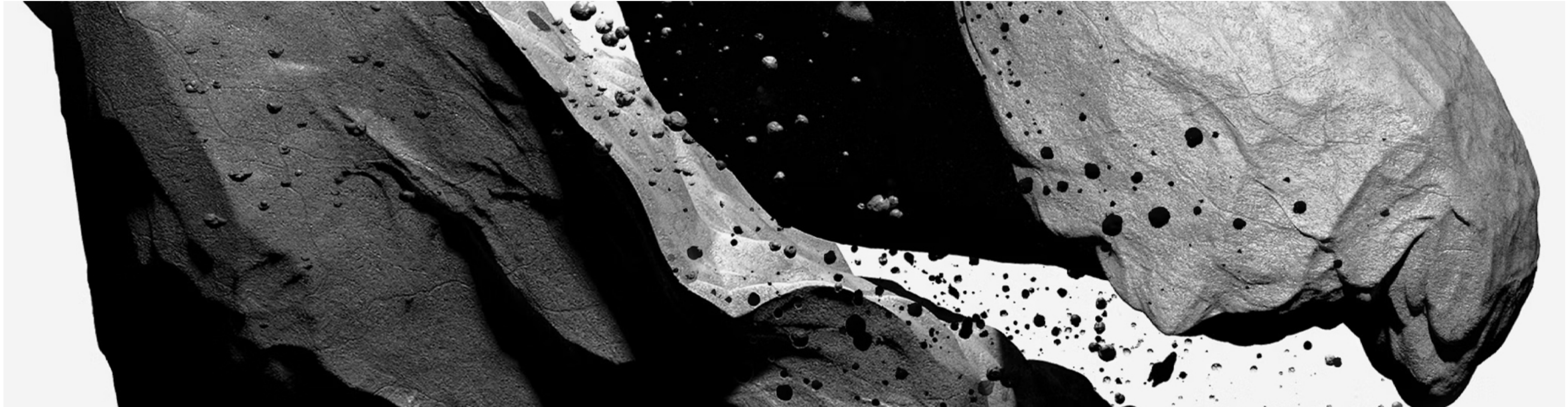
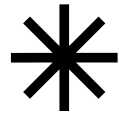
Real benefits already

- A clear majority (57%) of senior network decision-makers in the manufacturing and automotive sectors do not believe AI has been overhyped. They are already seeing real benefits across their businesses.
- More manufacturing leaders (62%) are seeing benefits from AI than their peers in any other sector.
- In Germany – with its strong manufacturing sector – more leaders (70%) are seeing AI benefits than in the US, UK or France. Turning specifically to the impact of AI on enterprise network operations, most manufacturing and automotive sector leaders (69%) are comfortable with AI taking an increasing role in their network operations – perhaps because most (57%) believe it will cut network costs over the next three years.



The number one network challenge

- But our findings are not entirely positive. A significant 18% of manufacturing and automotive sector decision-makers remain skeptical about AI's ability to achieve all the claimed benefits, while many more admit to serious concerns.
- Their biggest fears are that AI is making network operations more complex, increasing infrastructure costs, eroding competency and skills, and causing increased bandwidth consumption.
- Half of manufacturing and automotive decision-makers see cybersecurity as their #1 network challenge, recognizing that AI facilitates a never-ending cycle of cyberattacks and defence.



Security will still rely on humans

- Most leaders expect both DDoS attacks and DDoS attack mitigation to be largely driven by AI within four years. Indeed, it is already happening.
- Manufacturing leaders cite real-time detection and response as the area where AI will have the biggest impact on DDoS attack mitigation.
- But overwhelmingly, decision-makers in both the manufacturing and automotive industries display a chronic lack of faith in current AI-based cybersecurity, with over 90% believing that hackers are more likely to trick AI-based cybersecurity tools than those operated by humans.

Survey findings

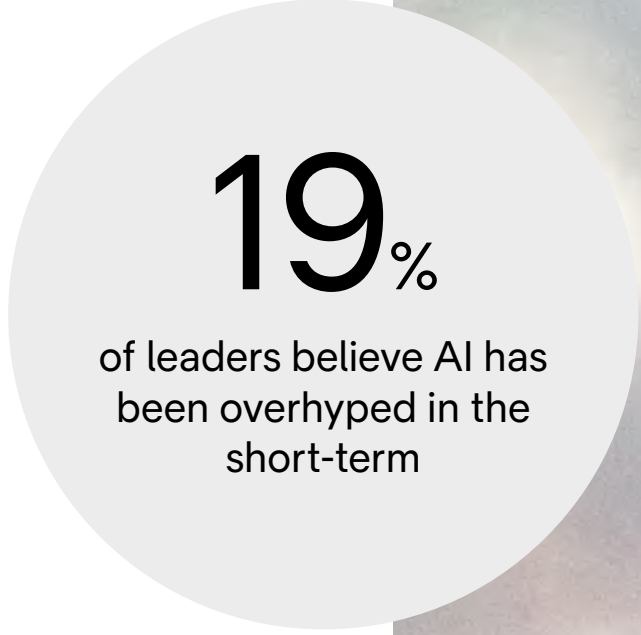


Artificial Intelligence is living up to the hype

In terms of its overall business impact, AI is living up to the hyperbole that often surrounds it.

When measuring the claims for AI against genuine business benefits, a majority of senior network decision-makers in the manufacturing and automotive sectors (57%) do not believe it has been overhyped. They are already seeing real benefits across their businesses.

An additional 19% foresee substantial mid- to long-term benefits from AI, even though they DO think it has been overhyped in the short-term.

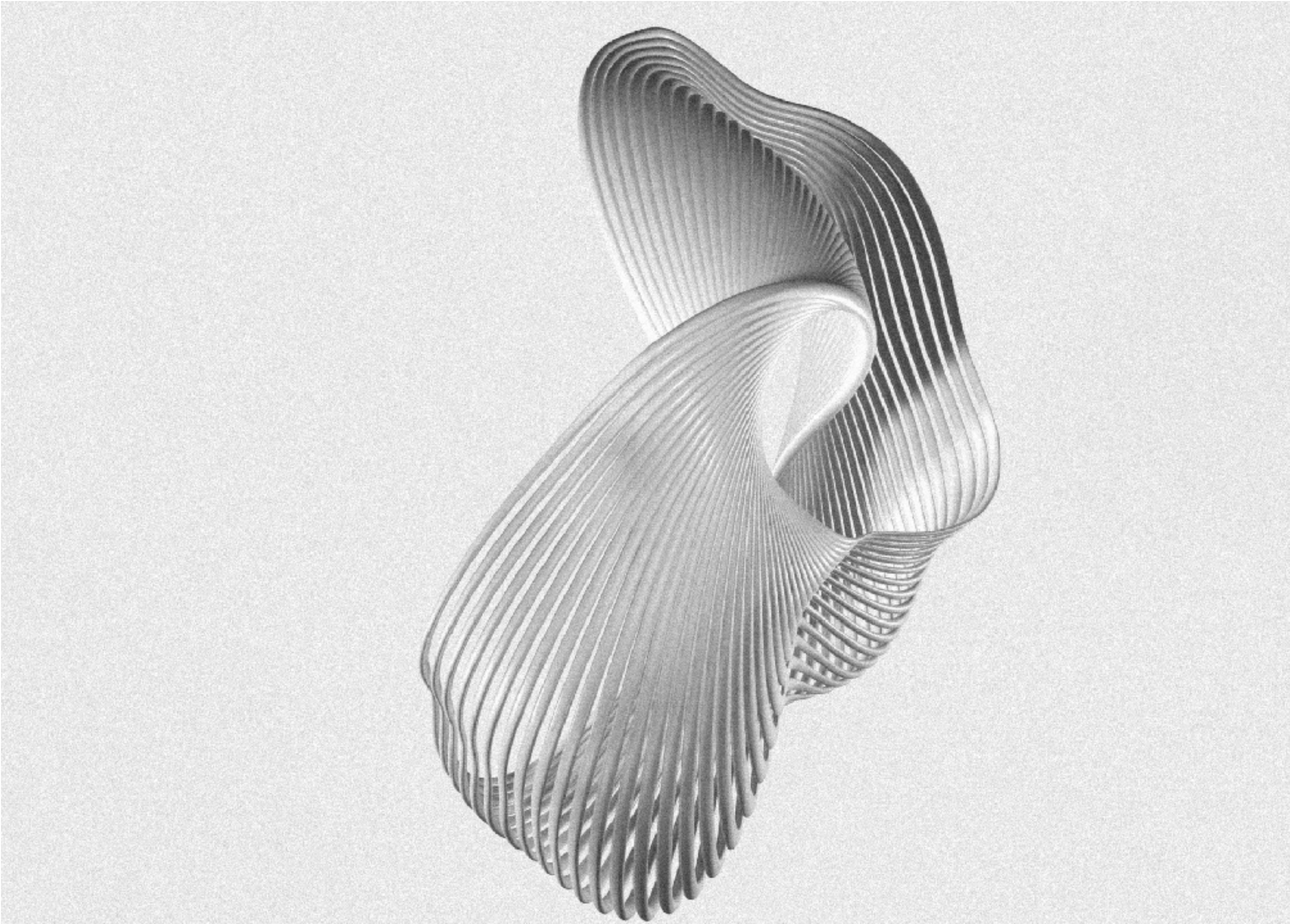




From our broader, cross-sector survey, we can see that manufacturers (62%) are already deriving more benefits than other sectors – perhaps because automated, data-driven production systems lend themselves to the advantages of enhanced connectivity from AI in enterprise networks. This also tallies with our cross-sector finding that more leaders (70%) in Germany – with its strong manufacturing sector – are seeing AI benefits than those in the US, UK or France.

Even so, overall, some 18% of manufacturing and automotive leaders remain wary – particularly 33% of those in the automotive sector – saying they may implement AI but are currently unsure if such technologies will achieve all the claimed benefits. Such caution is more apparent than in our broader cross-sector survey, where the figure was just 12%.

33% of leaders in the automotive sector feel unsure whether AI will achieve all the claimed benefits

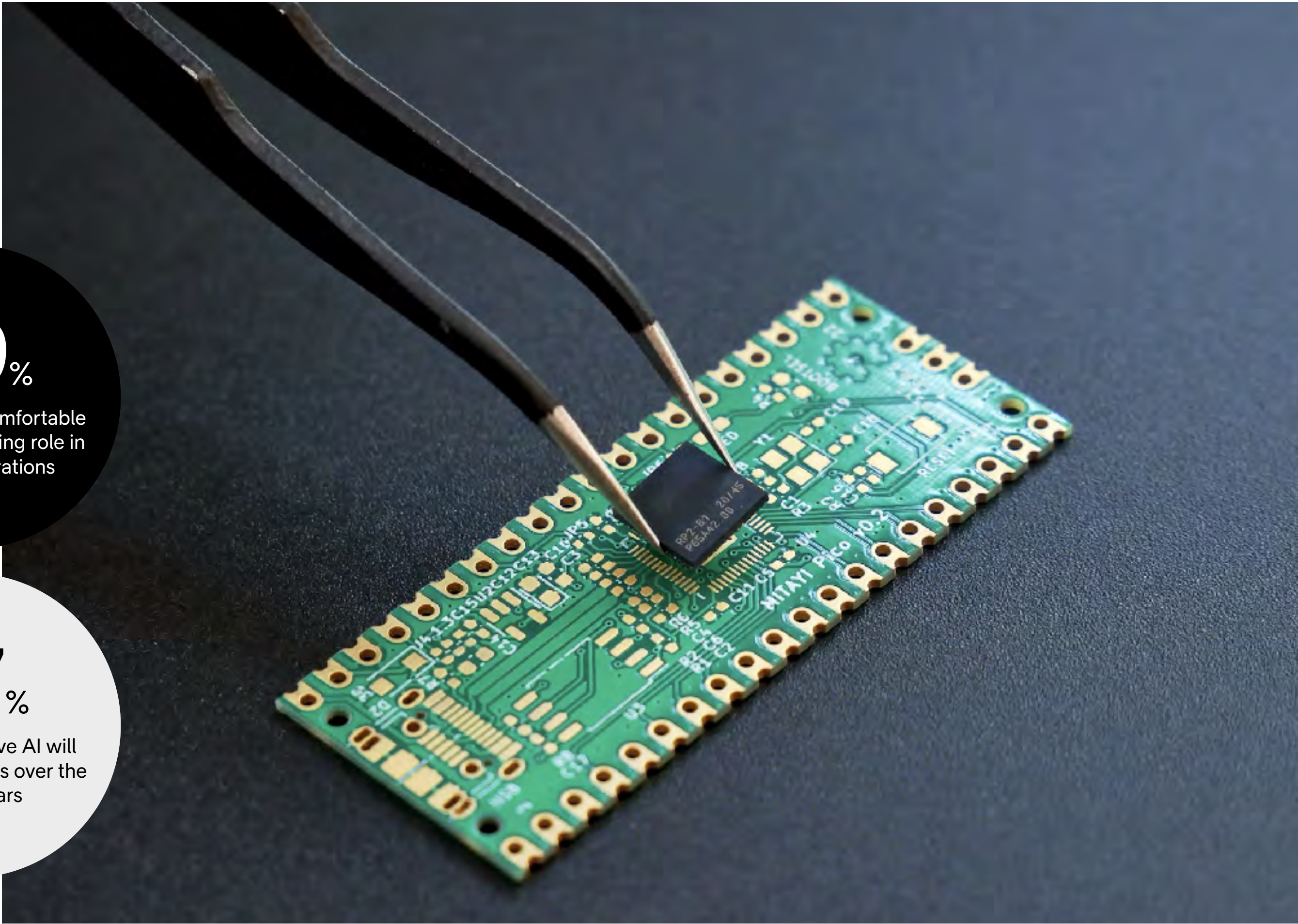
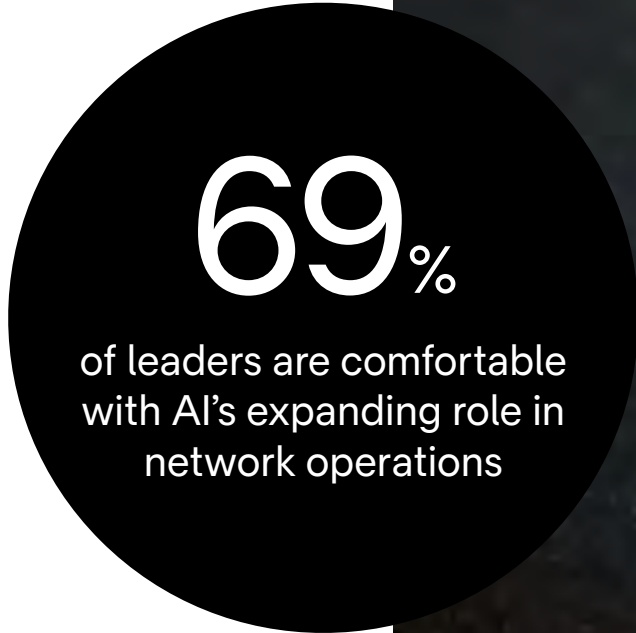




Leaders broadly welcome AI in network operations

Most enterprise network decision-makers in the manufacturing and automotive sectors (69%) are comfortable with AI taking an increasing role in their network operations. That said, a relatively large number of automotive leaders believe "daily network operations will always be carried out by engineers" – perhaps indicating how highly this sector values skilled workers.

Overall, the two sectors' overarching AI comfort level is in line with our broader cross-sector survey. This may be because over half of respondents (57%) believe AI will cut their network costs over the next three years. Even so, a significant minority (37%) foresee AI having the opposite effect, causing costs to rise.





But AI is also raising several major concerns

Among the chief concerns of manufacturing and automotive sector leaders are that AI is:

- **Making network operations more complex** – cited by 71% of respondents, reflecting a similar finding across our broader cross-sector survey
- **Increasing infrastructure costs**
- **Causing a loss of workforce competency and skills**
- **Resulting in increased bandwidth consumption**

Regarding increased bandwidth consumption, 77% of these decision-makers anticipate a 10-50% growth in their core network traffic, 73% predict such growth in traffic between corporate user applications and data centers/cloud resources, and 68% foresee it in traffic to and from the public Internet (where a further 19% expect a 50-100% increase).





Artificial intelligence and the cybersecurity conundrum

Highlighting the complex impact of AI, manufacturing and automotive business leaders recognize that AI facilitates a never-ending cycle of attack and defence on the cybersecurity battlefield. Not only does it pose cybersecurity challenges to their network operations, but it also enables mitigation solutions... and then, in turn, renewed attacks.

Over half of respondents from the two sectors see cybersecurity as their #1 network challenge, a view amplified in every region and industry by our wider survey.

The most likely timescale for DDoS attacks to be largely driven by AI (as opposed to humans) is 2-4 years, cited by 43% of manufacturing and automotive decision-makers, with a further 23% anticipating this in 4-6 years.

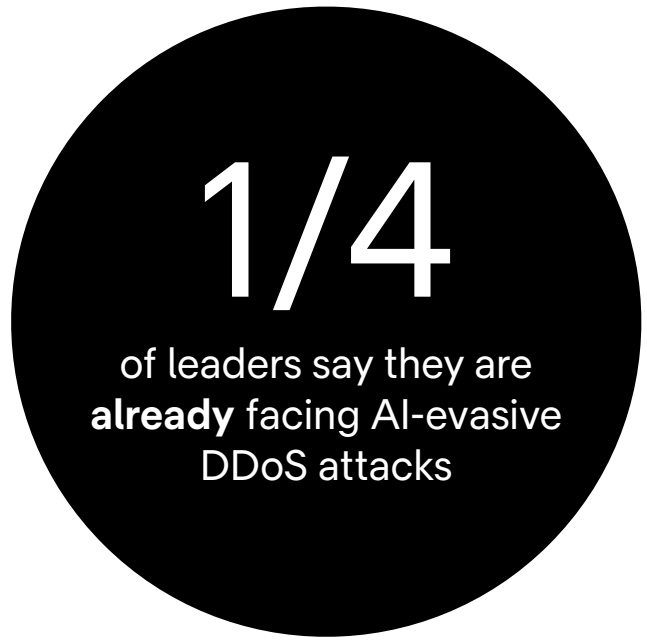
Alarmingly, almost one in four (24%) say they are already facing DDoS attacks specifically engineered to circumvent AI-driven cybersecurity defences.

AI-related cybersecurity threats are considered the #1 network challenge

When asked where they felt AI will have the biggest impact on DDoS attack mitigation, manufacturing leaders primarily go for real-time detection and response (cited by 32%) – again, in line with our broader industry sample.

Automotive leaders suggest that dynamic and adaptive defence mechanisms, and incident response and management, will feature prominently (28% cited for each).

Across both sectors, 70% of respondents expect such mitigation to be largely driven by AI (as opposed to humans) within four years.

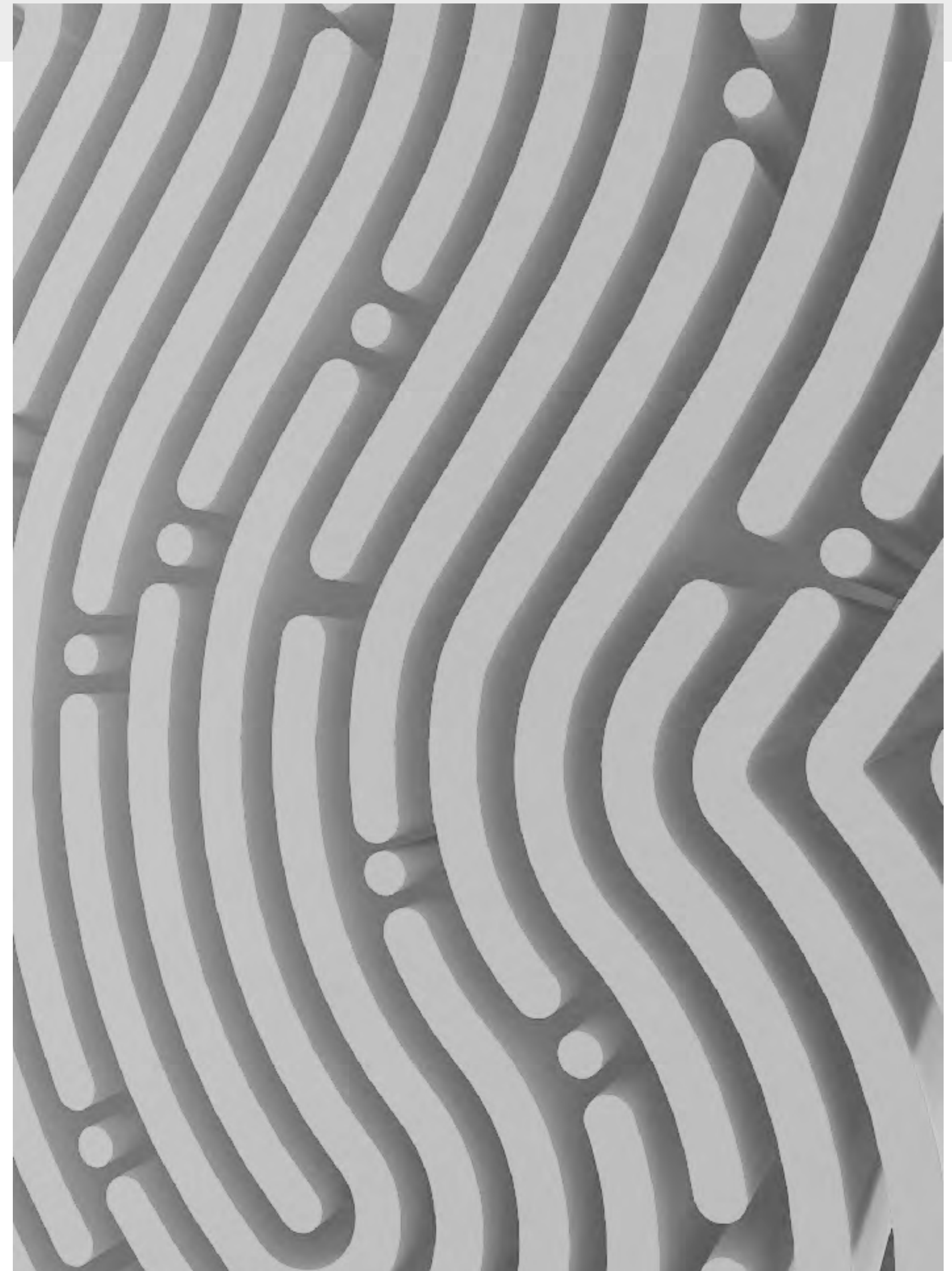




Leaders lack faith in AI-driven cybersecurity solutions

Worryingly, an overwhelming majority of decision-makers in these two sectors show a chronic lack of confidence in current AI-based cybersecurity, **with over 90% stating that they believe hackers are more likely to trick AI-based cybersecurity tools than those operated by humans.**

9 out of 10 leaders believe hackers are more likely to exploit AI cybersecurity tools than those operated by humans



Conclusions

AI is broadly a boon for business

AI is generally regarded positively by manufacturing and automotive businesses, with a majority of leaders – led by those in manufacturing – reporting that they are already experiencing benefits from the technology.

AI is also broadly welcomed specifically in the field of enterprise network operations, notably for its ability or potential to reduce network operating costs.

71%

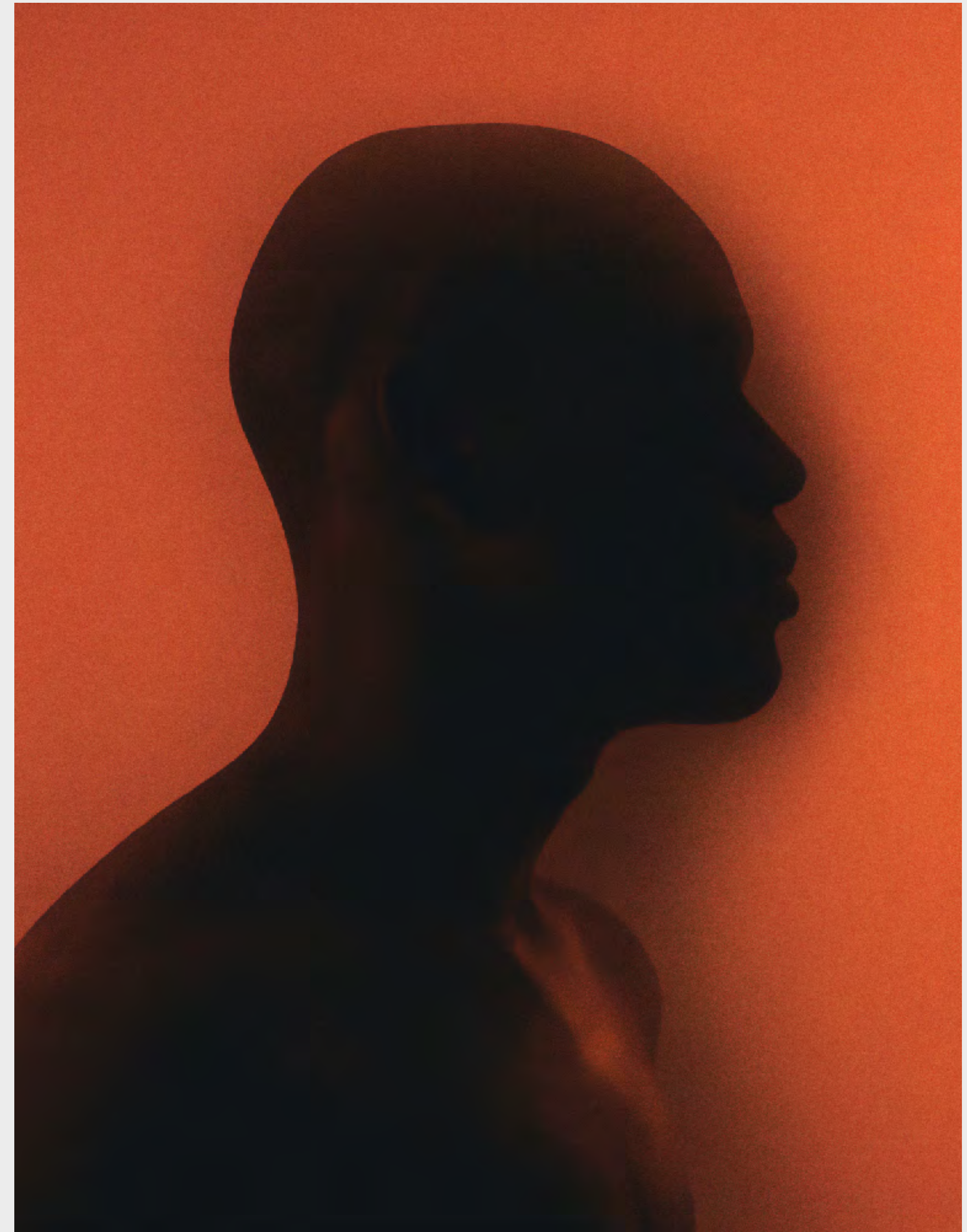
say AI is making network operations more complex



AI brings challenges and solutions

But respondents also see AI bringing potential challenges, including more complex network operations, higher infrastructure costs, erosion of human skills, and increased use of bandwidth. Network operators will need to consider remedial action in all four areas. If complexity is not understood and overcome, hoped-for cost reductions may not be realized, with infrastructure costs actually rising. If workforce skills are not maintained through adequate recruitment and training, lack of human back-up could prove disastrous if AI-driven solutions misfire. And insufficient network capacity will clearly hamper organizational performance at a fundamental level.

Lack of human back-up
could prove disastrous if
AI-driven solutions misfire



The cybersecurity stakes are high

Over half of respondents from the manufacturing and automotive sectors see cybersecurity as their #1 network challenge. Network operators face an ongoing war of attrition with cyber criminals. AI already provides many possibilities for bad actors to target areas of vulnerability in a company's defences. They now have the ability to set a series of protocols to attack relentlessly until they eventually overwhelm cyber defences.

But AI also offers cybersecurity solutions. Intelligent automation is as vital to cyber defence as it is to attackers. AI offers the potential for improved DDoS attack mitigation, for example, through tools such as real-time detection and response. But alongside AI-driven solutions, human skills remain vital.



1/2

See cybersecurity as their
#1 network challenge

Implications for enterprises





The research suggests that, as an enterprise network operator in the manufacturing or automotive sector, you need an enhanced toolkit to tackle key AI-related issues.

When developing your network strategy and choice of network provider, you should consider:

- **Cybersecurity support** – with sufficient scale, experience, expertise, flexibility and speed of response to help you react fast to manage fast-moving cybersecurity threats. It is essential to select a suitably large and capable network provider who can absorb the physical impact of DDoS attacks and, indeed, of any attack.
- **Automation** – is key both at the volumetric level and also at defending your applications from resource exhaustion.
- **DDoS protection capabilities**, including:
 - Large-scale monitoring capacity.
 - An enhanced level of automation with regards to network adaption and filtering bad actors.
 - Commitment to DDoS protection that quickly adapts to the circumstances, and to develop such technology to defend against hackers who now use AI and other automated techniques to try and overwhelm human engineers.
 - Large-scale network capacity. No matter how much intelligence is put behind an attack, the fact remains that DDoS is a resource exhaustion technique, so to remain secure it is vital to stay ahead in terms of raw resources.
- **Independent advice and expertise** – including pan-industry perspectives, resources and clear thinking to unravel increasing complexity in network operations.
- **Support on skills** – helping to nurture in-house workforce talent and offering supplementary external advice and services where necessary.
- **Scalable bandwidth** – offering sufficient network capacity, with flexibility to scale up when required.
- **Geographical spread** – with local knowledge to provide guidance and support in specific markets.
- **A partnership approach** – with a willingness to work collaboratively.



What Arelion is doing to counter AI-generated DDoS threats

Arelion has significantly enhanced the capabilities of its DDoS protection:

- **A doubling of monitoring capacity**
- **An enhanced level of automation** with regards to flowspec filtering and automatic responses in network to attacks.
- **Adaptive DDoS: machine learning** is employed in order to real time adapt to hackers using multiple vectors and changing them rapidly (carpet bombing is a key example). Adaptive DDoS is still being developed and will be directly responding to AI and other automated techniques that attempt to overwhelm human engineers.
- **Also, the level of capacity in the Arelion network is an effective line of defence.** A large and capable network provider can absorb the physical impact of DDoS attacks and other cyber threats before they reach you.

By far, the greatest danger of Artificial Intelligence is that people conclude too early that they understand it.

– Eliezer Yudkowsky, founder of the Machine Intelligence Research Institute



Research methodology

This research was conducted on behalf of Arelion by Savanta, a global leader in digital data collection. An online survey was carried out in the second half of 2024 with 510 industry leaders in the US, UK, Germany, and France.

Respondents come from a range of industries, and this report focuses on 103 (20% of the full sample) from the manufacturing and automotive sectors.

All participants in the research work for enterprises with more than 2,000 employees. All are involved in decision-making regarding their company’s network development strategy (including data center, cloud, and connectivity), with 60% having the last word and final sign-off responsibility for this area.





About us

Arelion is a leading light in global connectivity services. Formerly Telia Carrier, we've been keeping the world connected since 1993 and today our global IP backbone, AS1299, is ranked number one in the world.

Our network spans Europe, North America and Asia, with 77,000km of optical fiber and 1,700 MPLS end points serving customers in 128 countries. Our award-winning customer service team supports our expansive customer base, who rely on us for their business-critical services.

Follow us on [LinkedIn](#) and [X \(formerly Twitter\)](#)

Discover more at www.arelion.com