Cybersecurity
Progress. Protected.

REPORT

ESET for Manufacturing:

Simplified, Scalable, Secure

Progress. Protected.

PROCESSING.....
PROGRAM RUNNING...
64%
Robotic
86%
73%
64%

Introduction

As businesses globally become increasingly reliant on digital infrastructure, the risk from cyber-attacks only grows. The threats, ranging from ransomware to data breaches, disrupt operations, leading to reputational damage and increased regulations. As manufacturing becomes more and more digitised, the exposure to cyber threats grows in parallel. What was once an IT concern now directly affects production, deliveries and revenue, as cyber incidents in manufacturing mostly interrupt physical operations.

For manufacturers across UK the consequences of cyber incidents are immediate and tangible. A major cyber-attack on Jaguar Land Rover in late August/early September 2025 halted production for several weeks, costing an estimated £1.9 billion and affecting over 5,000 businesses. The incident, described as the most economically damaging in UK history, forced a shutdown of IT networks, impacting plants in the UK, Slovakia, India and China.

This goes to show that cyber risk in manufacturing is no longer just about data, it is about business continuity. This report explores the prevalence, impact and management of cybersecurity risk in UK manufacturing, drawing on insights from 500 senior decision-makers across the sector.

Executive Summary

Cybersecurity is no longer just an IT issue in the UK manufacturing sector. A cyber-attack today directly impacts production and supply chains, with incidents capable of stopping physical operations and causing widespread disruption including revenue loss.

This report shows how widespread the problem has become. Nearly 8 in 10 manufacturing organisations (78%) experienced a cyber incident in the past year, making it clear that these events are no longer isolated but part of the day to day. At the same time, threats are becoming more advanced, with AI-enabled attacks now seen as the leading concern for the year ahead.

The impact of these incidents is both financial and operational. Over half of affected organisations reported costs of over £250,000, with nearly one in five facing losses above £1 million. Beyond the direct costs, cyber incidents frequently result in production downtime, missed commitments and supply chain disruption. 95% of organisations reported business impacts, showing that cyber risk is heavily aligned with business risk in manufacturing.

There are positive signs though, organisations are shifting towards a more proactive approach. Many cybersecurity budgets are now allocated to preventative measures, showing a growing understanding that prevention is more cost-effective than response. There is also growing recognition that cybersecurity is a driver of business growth, winning new clients and a competitive advantage.

Key challenges do remain from limited visibility into emerging threats and an over-reliance on IT teams to manage cyber risk, highlighting gaps in organisational readiness. To address these challenges, cybersecurity must be elevated to a board-level priority and rolled out across the organisation. A more strategic, collaborative approach, supported by specialist expertise where needed, will be key.

Ultimately, manufacturers that treat cybersecurity as part of their everyday, not just a technical function, will be in the strongest position to operate securely and stay competitive in an increasingly complex threat landscape.

OVER HALF OF AFFECTED ORGANISATIONS REPORTED COSTS OF OVER £250,000, WITH NEARLY ONE IN FIVE FACING LOSSES ABOVE £1 MILLION.

Prevalence of Cyber Incidents

Cyber incidents are now considered the norm across manufacturing organisations.

78%

of manufacturing organisations experienced a cyber incident in the past year.

With nearly 8 in 10 UK manufacturing organisations experiencing this high level of exposure, it indicates that cyber threats are no longer occasional or unexpected. Without active management these cyber incidents represent a huge and ongoing organisational risk.

This outlook is reinforced by forward-looking expectations. In our Cost of a Cyber Attack report, 43% of respondents believe their organisation is likely to experience a cyber-attack or breach within the next 12 months, rising to 51% among larger businesses, compared with 39% of smaller organisations. This suggests that both current exposure and anticipated risk remain high.

At the same time, the nature of cyber threats is evolving. With the rise of AI-enabled attacks, nearly half of organisations (46%) identify them as a key risk to production in the coming year, overtaking traditional threats such as phishing and ransomware. This indicates that more proactive and sophisticated security must be put in place to avoid heavy production delays and wider business loss.

→ COST OF A CYBER ATTACK REPORT

43% of respondents believe their organisation is likely to experience a cyber-attack or breach within the next 12 months, rising to 51% among larger businesses, compared with 39% of smaller organisations.

> According to our Cost of a Cyber Attack report 43% of respondents believe their organisation is likely to experience a cyber attack within the next year. "Strengthening cyber resilience is essential not just for business continuity but also for safeguarding the UK's economy stability and growth in an increasingly digital world."
>
> **MATT KNELL,**
> **UK COUNTRY MANAGER @ ESET**

Financial Impact of Cyber Incidents

The financial impact of a cyber incident can be severe across any industry. For example, in the retail sector, the recent [Marks & Spencer cyber-attack] **resulted in £324 million in lost sales, while the reputational damage is harder to quantify, our** [ESET for Retail] **research shows many consumers take over five months to return to an affected brand. The financial consequences for manufacturing organisations are no different.**

→ THESE COSTS TYPICALLY INCLUDE...

- Lost revenue during downtime
- Recovery and remediation expenses including reputational damage
- Third-party support and investigation costs

When considered alongside the high prevalence of cyber incidents, the case for robust cybersecurity risk management becomes clear as attacks are not only frequent but financially damaging.

Over

50%

of organisations report costs exceeding £250,000

Nearly

20%

report costs above £1 million

Operational Impact

Unlike many other sectors, cyber-attacks in manufacturing environments can directly interrupt physical operations, bringing production lines to a halt and disrupting the flow of goods.

When operational technology systems are compromised, the impact is immediate and tangible with machinery being forced offline or processes halted. Even short periods of downtime can create a snowball affect putting contractual delivery commitments at risk, particularly in sectors reliant on continuous production or just-in-time supply chains.

> “We’ve got events going on around the world at all times that we needed to be able to ensure constant monitoring was happening and ESET monitor our systems 24/7/365. ESET service and support has been outstanding, we ended up having all our fleet swapped over with no downtime and no lack of protection and that was exactly what we wanted.”

**ALISTAIR TODD,
IT OPERATIONS MANAGER @ M-SPORT**

→ PRODUCTION DOWNTIME

- 75% experienced between one and seven days of downtime
- 56% reported downtime lasting one to three days
- 19% experienced disruption lasting from four to seven days

→ BUSINESS CONSEQUENCES

Suppliers, logistics networks and customers are all affected when production stops, meaning a single incident can quickly escalate into a wider operational and commercial issue. Cyber incidents also lead to wider organisational impacts...

- 53% reported lost revenue
- 44% experienced supply chain disruption
- 39% missed customer or supplier commitments
- More than a third face reputational damage

Notably, only 5% of organisations reported no business impact, reinforcing that cyber incidents almost always result in tangible consequences.

95%

reported tangible consequences

Cybersecurity Investment and Approach

Manufacturing organisations are investing more in cybersecurity, with a clear shift towards preventative measures.

57%

of cybersecurity budgets are allocated to preventative measures

63%

believe preventative measures offer better value

With 57% of budgets allocated to preventative measures and 63% of manufacturing organisations believing these measures offer better value, there is an evident trend between spending decisions and organisational mindset.

→ **THIS SHOWS THAT THERE IS A GROWING RECOGNITION THAT...**

- Preventing cyber incidents is more cost-effective than responding to them
- Cybersecurity is being treated as a long-term investment, not just an operational expense
- Organisations are moving towards a more mature security posture

Looking beyond breach prevention, cybersecurity investment is also delivering measurable business value. According to our Cost of a Cyber Attack report, 53% of businesses report that cybersecurity has a positive impact on turnover, contributing an estimated 0.5% increase in revenue (£27 billion annually across the UK). Key drivers of this growth include winning new clients (70%) and improving IT systems (68%).

This suggests that organisations prioritising cybersecurity are not only protecting themselves from breaches, but also unlocking commercial benefits, including increased client trust and a stronger competitive position.

Risk Visibility and Management

Concerns are shifting towards more advanced threats, suggesting that manufacturers are increasingly aware of more sophisticated, evolving attack methods.

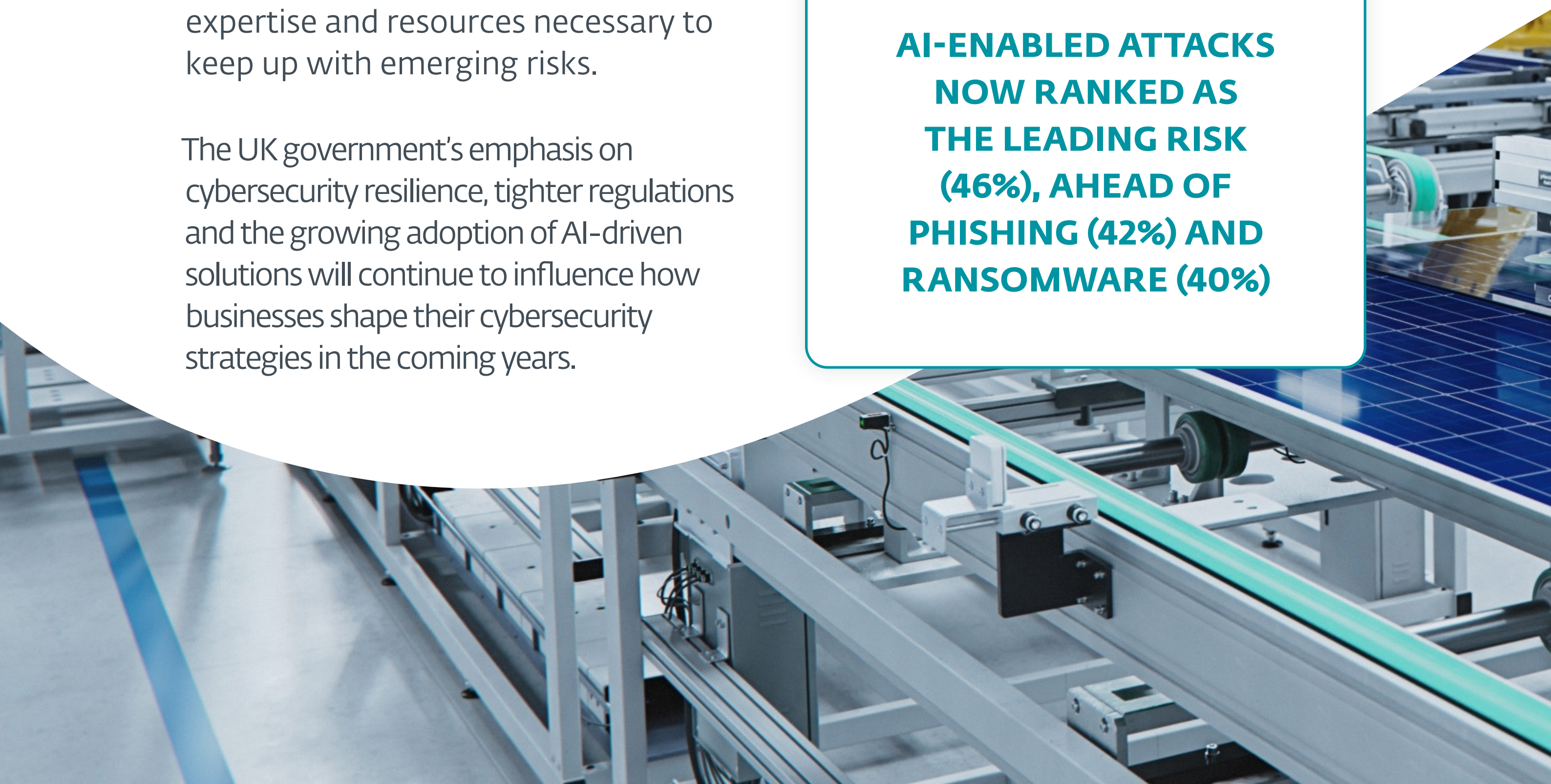
A key challenge identified in the research is limited visibility into these cybersecurity risks. Nearly 1 in 5 organisations report limited or no visibility into these risks.

This lack of visibility can make it difficult for organisations to anticipate and mitigate potential threats, increasing the likelihood of disruption. With the evolving nature of cyber threats and the growing sophistication of attacks, businesses should reconsider their reliance on in-house teams, which may lack the specialised expertise and resources necessary to keep up with emerging risks.

The UK government's emphasis on cybersecurity resilience, tighter regulations and the growing adoption of AI-driven solutions will continue to influence how businesses shape their cybersecurity strategies in the coming years.

The complexity and rapid evolution of cyber threats demand a more specialised approach. Outsourcing cybersecurity to a trusted provider like ESET not only ensures businesses can stay ahead of emerging threats and achieve compliance with evolving regulations but can offer sector specific expertise that enables companies to manage their unique threat landscape to a much more sophisticated level.

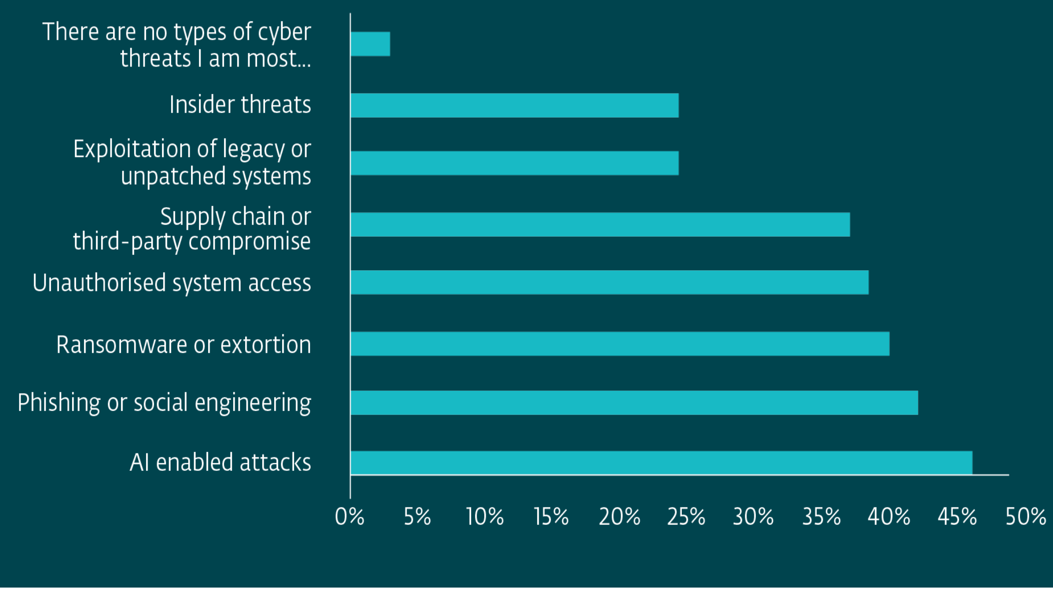
AI-ENABLED ATTACKS NOW RANKED AS THE LEADING RISK (46%), AHEAD OF PHISHING (42%) AND RANSOMWARE (40%)

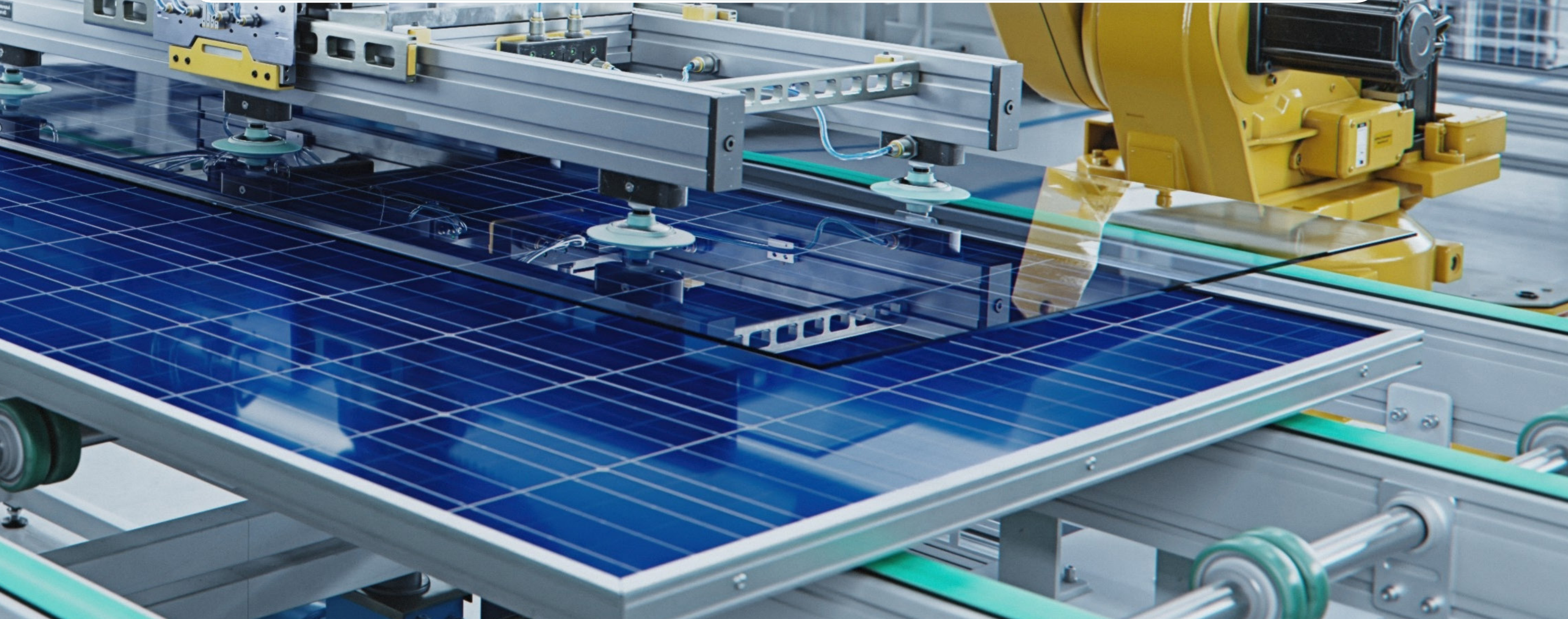


> “For us Managed Detection and Response has shifted from being a “nice to have” to an essential pillar of our security strategy. The value of having real people monitoring, analysing and responding to threats in real time simply cannot be overstated. MDR is now a cornerstone of our cyber defence. Do not wait for an incident to realise the necessity. MDR provides a level of assurance and resilience that automated tools alone cannot offer.”

NEIL MOWFORTH, HEAD OF IT @ BIOSYNTH

WHICH CYBERSECURITY THREATS, ARE YOU MOST CONCERNED COULD DISRUPT YOUR PRODUCTION IN THE NEXT 12 MONTHS?





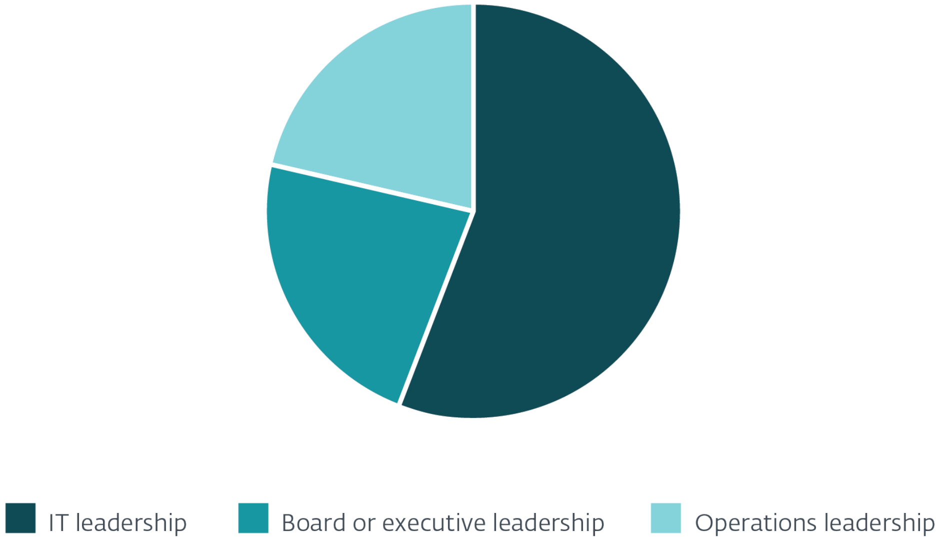
Responsibility for Cyber Risk

With nearly 78% of manufacturing organisations experiencing cyber incidents in the past year and many of these costing over £250,000, cybersecurity can no longer be treated as an operational issue. Responsibility should sit at board level to enable more proactive, strategic investment.

→ RESPONSIBILITY FOR MANAGING CYBERSECURITY RISK IS PRIMARILY ASSIGNED TO IT TEAMS:

- 55% place responsibility with IT leadership
- Only 22% assign responsibility to board or executive leadership
- 21% place it within operations

WHERE, IF ANYWHERE, DOES PRIMARY RESPONSIBILITY FOR MANAGING CYBERSECURITY RISK TO PRODUCTION UPTIME SIT WITHIN YOUR ORGANISATION?



> "If the JLR attack showed us anything, it's how quickly a cyber incident can shut down production at scale and have major consequences for the business and the wider economy. The real challenge is that many organisations still treat cybersecurity as an IT issue rather than a strategic business decision. When it sits outside the boardroom, it's harder to prioritise appropriately.
>
> What's striking is that many organisations still see reactive approaches as more economical, despite the evidence to the contrary. With many major incidents resulting in six-figure losses and widespread operational disruption, the cost of reacting after the fact can be significant. In contrast, investing in advanced endpoint protection and managed detection and response (MDR) services can provide continuous, 24/7 monitoring and access to specialist expertise, helping organisations stay ahead of evolving threats, even when internal teams are stretched, In that context, the idea that prevention is too expensive simply doesn't stand up.
>
> The organisations that get ahead of this will be the ones that treat cybersecurity as a core part of how they run the business, not just something for IT to manage."

MATT KNELL,
UK COUNTRY MANAGER @ ESET

RESPONSIBILITY SHOULD SIT AT BOARD LEVEL TO ENABLE MORE PROACTIVE, STRATEGIC INVESTMENT.

Conclusion

The need for preventative and effective cybersecurity in the UK manufacturing sector is critical. With most organisations experiencing an incident each year and financial losses often reaching six or seven figures, manufacturers must move beyond viewing cybersecurity as a technical concern.

The impact of cyber incidents goes beyond internal systems, with disruption to supply chains, delayed deliveries and missed revenue highlighting the wider business risk. Resilience is now at the forefront of business priorities and cybersecurity should be treated as a business-critical issue requiring collaboration across IT, operations and senior leadership. Organisations that adopt this approach are far more likely to have business continuity in an increasingly complex threat landscape.

→ HOW CAN ESET SUPPORT MANUFACTURING ORGANISATIONS

Manufacturers must also consider how external expertise can support a more proactive and resilient approach, particularly in protecting production systems and supply chains. Providers such as ESET play a key role in delivering this capability.

ESET Security for Air-Gapped Networks

If you're a manufacturing organisation with IT and OT networks that are separated from each other by either a 100% air gap or a hybrid air gap (network segmentation enforced by strict sets of firewall rules), then ESET has some solutions for you.

These same solutions also apply on the IT network, if you have individual computers or groups of them that are segmented or air gapped because they have extremely sensitive information related to personnel, R&D or trade secrets.

For hybrid air-gapped networks: ESET Managed Detection and Response (MDR)

ESET MDR is a 24/7 cybersecurity service that continuously monitors your environment for threats, blocks and contains them before they can execute malicious behaviour and removes and remediates them. If you have networks that contain highly sensitive information that are separated from your main business IT networks by a hybrid air gap that allows specific traffic through the firewall by exception, the ESET MDR service can protect those networks.

For fully air-gapped networks: ESET Inspect managed by in-house security analysts

Some ESET manufacturing customers who can run a fully air-gapped network opt to install ESET Inspect and manage it with an in-house security team. ESET Inspect can be installed in-cloud or on-premises. In-house teams have full use of the ESET threat intelligence that our own security analysts use, including updates on the latest tactics and techniques used by the attacker groups that target manufacturing.

For fully air-gapped or hybrid networks: ESET updating solutions

For devices that aren't allowed to connect to the public internet, ESET has implemented access to updates using a variety of delivery models to best fit organisational security policies.

Via USB drives. A scanner on a USB drive loaded with the current updates makes the process of detecting status and updating devices quick and easy for administrators.

Via a mirrored update server. For devices that are normally behind an air gap but sporadically allowed to connect locally, the ESET PROTECT console maintains a mirrored database of all the current updates. When an otherwise offline device becomes available in the environment, it retrieves the updates from the mirror.

Via an Apache proxy server. For a fully air-gapped network, devices can retrieve updates from an Apache proxy server located behind the air gap.

Two Tiers of MDR Service

→ MDR

The base tier of MDR is designed to be affordable for smaller manufacturers with as few as 25 seats. ESET experts immediately contain the threat, take action by blocking files and processes, and then notify you of the actions taken and any additional steps you need to take.

- Notification of incidents and actions taken
- Optimisation of the ESET Inspect MDR console at the backend level
- Continuous threat hunting
- Feedback to incidents
- Weekly & monthly reports

→ MDR ULTIMATE

Larger manufacturers at the enterprise level tend to have dedicated IT security admins who want to work with our analysts through an incident. ESET MDR Ultimate works as a seamless extension of your IT function. We contain the threat and then interact with your internal security personnel on complete remediation.

- Joint response to incidents with remediation guidance
- Optimised ESET Inspect console for your environment
- Continuous and on-demand threat hunting
- 24/7 availability to analysts
- Periodical reports with human interpretation

Choose the one that's
right for your organisation.

SUCCESS STORY

ESET Keeps M-Sport on Track with 24/7 Cybersecurity Support

M-Sport, a leading motorsport team, was previously using an alternative vendor for cybersecurity. However, they faced significant challenges, including poor support and false positives that disrupted their critical operations, particularly in configuring their rally cars. This led M-Sport to explore alternative solutions.

→ CUSTOMER

We are a dynamic motorsport engineering company based in Dovenby Hall near Cockermouth, Cumbria. Founded in 1979 by Malcolm Wilson, we have a rich history in motorsport, particularly in rallying. Since 1997, we've partnered with Ford to compete in the FIA World Rally Championship, developing iconic vehicles like the Ford Escort WRC and Ford Focus RS WRC. Beyond rallying, we provide engineering expertise, manufacturing services, and operate the Junior WRC championship on behalf of the FIA. Our headquarters at Dovenby Hall also houses a state-of-the-art automotive evaluation facility, supporting our ongoing dedication to excellence in motorsport engineering.

→ CHALLENGE

M-Sport required a cybersecurity solution that wouldn't interfere with their essential car configuration software, used to optimise the performance of their vehicles during races. The alternative vendors support failures during a high-pressure race weekend highlighted the need for a more reliable and efficient solution. With their existing contract coming up for renewal, M-Sport needed a cost-effective and seamless transition to a new security provider.

Understanding the increase in sophistication of cyber attacks over the last few years, M-Sport also wanted to explore a 24x7x365 solution that bolstered their protection and freed up resource for them to concentrate on their core activity – winning races.

→ SOLUTION

We were introduced to ESET through Storm Technologies. They suggested that we compare ESET to our existing setup and after seeing the features and support on offer, we decided to explore it further. We chose ESET MDR for its advanced machine learning, customised protection and proactive threat hunting that minimises false positives while detecting real risks, key for us at M-Sport. Due to the 'anti-social' hours of our operation, 24x7x365 support is critical. ESET do what they do best so that we can do what we do best.

→ OUTCOME

The successful transition to ESET has resulted in improved system performance, better support, and a more reliable security framework. M-Sport now enjoys enhanced protection with reduced false positives and minimal impact on their critical car configuration software. The team is also more confident in ESET's ability to provide timely support during crucial race events.

SUCCESS STORY

BIOSYNTH®

Cybersecurity in Action: How Biosynth Stopped a Sophisticated Attack with ESET MDR

When a sophisticated, socially engineered cyber-attack targeted Biosynth, early detection and expert human response made all the difference. This case study explores how ESET Managed Detection & Response identified suspicious activity, rapidly contained the threat and protected a highly regulated life sciences organisation from serious operational and reputational risk.

→ CUSTOMER

Biosynth is an innovative life sciences company specialising in reagents, custom synthesis and manufacturing services for the pharmaceutical, diagnostic and related industries. We play a vital role in securing supply chains for critical raw materials and provide a broad portfolio of products and services, from custom synthesis and antibody production to large-scale manufacturing. We also supply research materials online, supporting pharmaceutical and biotech organisations in developing new medicines for a wide range of applications, including human health.

→ WHY DID THEY CHOOSE ESET MDR AS A SOLUTION?

I've always been aware that the most damaging cyber-attacks often occur outside normal working hours, typically late on a Friday evening or before a bank holiday. I wanted true 24/7/365 monitoring by real experts, not just automated alerts. After reviewing multiple solutions, including traditional SOC services, ESET MDR stood out for its proactive approach and seamless integration with our existing tools. It enables us to focus on what we do best, while ESET's specialists focus on what they do best.

→ HOW DID ESET WORK WITH YOU TO REMEDIATE THE THREAT FULLY?

Our ESET account manager was instrumental in quickly connecting us with the right technical experts. Working together, we conducted a deeper investigation into the script's behaviour and intent. ESET Support provided clear guidance, helping us validate the threat, confirm containment and ensure complete remediation.

→ WHAT MIGHT HAVE HAPPENED IF ESET MDR HADN'T BEEN IN PLACE?

Without MDR, the attacker could have remained undetected for hours, perhaps longer, given the obfuscated nature of the script. For the affected staff member, the impact could have ranged from credential theft to personal accountability. For the business, the consequences could have been severe: operational disruption, financial loss, reputational damage and erosion of customer trust.

Methodology

The research was conducted by Opinion Matters, among a sample of 500 Senior decision-makers responsible for IT, OT, operations, risk or security (e.g. CIO, CISO, Head of OT, Operations Director), in manufacturing organisations. The data was collected in March 2026. Opinion Matters abides by and employs members of the Market Research Society and follows the MRS code of conduct and ESOMAR principles. Opinion Matters is also a member of the British Polling Council.

Cybersecurity
Progress. Protected.

www.eset.com/uk