ESET MDR frees up more resource for in-house IT teams

Mid-size manufacturing business

(Approx. 100 endpoints)

ESET® Digital Security
Progress. Protected.

Customer

Company M is a UK-based mid-size manufacturing business with only one person working in the IT department and around 100 endpoints.

Why did they come to ESET

The IT personnel carried out a risk assessment, which highlighted that the business would only last two days if it was taken offline.After that, it would lose revenue and not be able to recover. The company also experienced a breach when an employee was on a hotel WiFi where VPN was not allowed. This resulted in a ransomware attack and solidified the need for a stronger cybersecurity posture.

The customer used cyber insurance requirements as a guiding template to improve the organisation's cyber resilience and reduce the risk of business disruption.

The ESET Solution

ESET took the customer through the product portfolio and showed how the technology corresponded to the requirements set in the cyber insurance guidelines. This included XDR, vulnerability and patch management, and multi-factor authentication.

The customer had already expressed an interest in multi-factor authentication following the breach and also wanted to know the difference between the tech support provided in the different ESET Essential and Advanced solutions. The customer acknowledged that there wouldn't be enough resource in-house to manage the ESET XDR 24/7 with only one person in the IT department.

ESET therefore offered the ESET PROTECT MDR solution. This would take the task of monitoring and managing the organisation's cybersecurity away from the organisation, and safelyin the hands of the ESET experts. This enables the company's solo IT personnel to spend more time on other critical business operations.

Company M now has a dedicated ESET Account Manager available to support and assist with remediation, and 24/7 surveillance and monitoring of their network from ESET experts. Their cybersecurity posture has improved dramatically with a reduced risk of attack and therefore less risk of business disruption.