



CUSTOMER CASE STUDY

How moveero gained immediate visibility into previously unseen activity

Sophos MDR helped moveero rapidly detect suspicious activity, strengthen incident readiness, and extend the capabilities of its small security team.



moveero

Industry
Manufacturing

Sophos Solutions
Sophos Managed Detection
and Response (MDR)

About moveero

Moveero is a global manufacturer of wheels for off-highway equipment in agriculture, construction, material handling, forestry, and mining, that also specializes in structural assemblies for the automotive market.

Headquartered in the U.S., moveero is a global company with manufacturing facilities in the U.S., UK and Denmark, and research and development centers in the U.S. and Italy.

The challenges

- Small security team with limited security resources.
- Lacked visibility and capabilities to detect and respond to threats.
- Struggled to manage vulnerabilities posing the biggest risk to their business.

Charged with keeping the growing business safe from cyber threats, Global IT Director Faisal Jaffri found himself with a small team and a security strategy reliant on third-party support for threat detection and vulnerability management. His team was focused on the basics, such as patching and making sure antivirus software was up to date. Building out an internal team to monitor moveero's environment for threats and respond when something is detected wasn't a viable option.

"We didn't have any threat detection capabilities, and we certainly didn't have any playbooks or a model for how to respond to an attack if one occurred," Jaffri said. "What kept me up at night was how do I know if we've been breached, and what would we do in the event of a breach. It would give me sleepless nights."

When it came to managing vulnerabilities, moveero's previous solution was difficult to configure and only allowed a point in time vulnerability assessment. The solution did not have a mechanism to continuously scan for vulnerabilities, or the ability to prioritize those vulnerabilities based on the level of risk posed.

The solution

- Provide holistic visibility and threat detection across IT environment.
- Perform powerful proactive threat hunting and incident response exercises.
- Continuously run vulnerability management, with risk-based prioritization and easy configuration.

Even if moveero possessed a security platform, Jaffri said his team could not scale to manage their security on their own. That led him to look for a solution combining technology — driven by advanced analytics and machine learning — with human

"What kept me up at night was how do I know if we've been breached, and what would we do in the event of a breach. It would give me sleepless nights."

Faisal Jaffri

Global IT Director, moveero

intelligence from a team of security experts.

As part of Sophos Fusion, Sophos MDR connects telemetry from control points across moveero's environment, including endpoint, network, cloud, identity, and business systems. Around-the-clock monitoring and access to Sophos security experts help moveero's small team detect suspicious activity quickly and respond with confidence.

Jaffri studied research from third-party analysts and conducted an extensive RFP process to assess options.

"In the grand scheme of things, in terms of looking at overall value, I felt the value we would gain from Sophos would be greater than from anybody else," he said.

The onboarding process for both solutions was easy, Jaffri recalled.

"We did a small proof of concept just to make sure our team understood the solutions, then deployment across our entire environment occurred relatively quickly, in a matter of weeks and not months," He said.

Results and impact

- Rapid notification of detected threats.
- Impactful context from quarterly security posture reviews.
- Vulnerability assessment reporting to drive remediation activities.

Sophos MDR delivered immediate value by detecting activity that moveero would not otherwise have seen. Sophos and the moveero team quickly investigated and confirmed the activity was an authorized action by a system administrator.

"We would not have seen that activity," Jaffri said. "We would not have known there was any behavior of that type occurring. The fact that it turned out benign is great, but the real impact is Sophos MDR detected and identified that activity quickly, in the first few days we went live with the Sophos solution. It just solidified the fact that we made the right decision."

Beyond this early result, Sophos MDR gives moveero access to proactive capabilities that would be difficult to maintain in-house. Monthly threat hunts draw on the expertise and global threat knowledge of Sophos specialists to uncover potential threats that automated detection alone may not identify.

"It's something that we would never, ever have been able to do," Jaffri said. "If we wanted any proactive threat hunting, we would have to find somebody who would take that on for us, and we would have to pay specifically for that threat hunt each time we want it. The way I look at it, we get at least 12 proactive threat hunts a year as part of Sophos MDR."

"We would not have known there was any behavior of that type occurring. The fact that it turned out benign is great, but the real impact is Sophos MDR detected and identified that activity quickly, in the first few days we went live with the Sophos solution. It just solidified the fact that we made the right decision."

Faisal Jaffri

Global IT Director, moveero

Looking ahead

Sophos MDR also provides customers with a quarterly security posture review. Delivered by a Sophos Threat Engagement Manager, these reviews include discussions on observed activity in moveero's environment, and steps Jaffri and his team can take to elevate the organization's security posture. moveero appreciates being assigned a Threat Engagement Manager, a designated resource who partners with a customer to help maximize value received from Sophos solutions.

"It gives us a more detailed view of the threat landscape," Jaffri said. "The Threat Engagement Manager gives us a summary of all the relevant information from the previous quarter, from the activity the Sophos team observed in our environment, the investigations performed, and they direct us to the important stuff. We like to say we are trained up, in that we are able to have a proper, more in-depth discussion with our leadership about what we as an organization should be doing."

"The knowledge of the Sophos incident response team, the information they provided, the support in creating the plan and running tabletop exercises with our executives. We now have our full executive team that's bought into the incident response plan and their responsibilities in the plan."

- Faisal Jaffri, Global IT Director, moveero

"Taking a more risk-based contextualized approach has specifically allowed us to use our resources more effectively. You're not chasing a seemingly critical vulnerability that actually doesn't have any impact on your business."

Faisal Jaffri

Global IT Director, moveero

To learn more visit [Sophos.com](https://www.sophos.com)

© Copyright 2025. Sophos Ltd. All rights reserved.
Registered in England and Wales No. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, UK
Sophos is the registered trademark of Sophos Ltd. All other product and company names mentioned are trademarks or registered trademarks of their respective owners. (11-2025)

