CUSTOMER CASE STUDY

Cyber resilience across industries: Derhem's multisector defense

Derhem Holdings, one of the largest Moroccan private groups, leans on Sophos to balance everything that comes with being in a wide range of industries.

DERHEM HOLDING

Industry
Transportation, logistics, oil and gas, real estate, commercial fishing, quarrying and media

Number of Users
350

Sophos Solutions
Central Managed Detection and Response

Central Mobile Advanced

Central Email Advanced

SOPHOS

Challenges

- As a large holding company, Derhem Holdings is part of a wide range of sectors, which all come with their own set of regulations, risks, and sensitive data that need to be protected.
- The company is constantly growing and expanding into new sectors, which requires a cybersecurity solution that can grow with it.
- Many of the company's interact with Morocco's critical infrastructure, making them a potential high-value target for threat actors.
- Derhem is currently digitizing many of its processes, which is increasing its attack surface and the amount of sensitive data that it holds in network-accessible places.

> "Detecting a threat in minutes rather than hours or days can be the difference between a controlled alert and a major incident."
>
> **Elhichamy Oussama, Infrastructure and security Manager**

Sophos Solutions

- Central Managed Detection and Response
- Central Mobile Advanced
- Central Email Advanced

It can be difficult enough for a logistics company to keep up with the challenges of cybersecurity: an ever-evolving supply chain, expanding attack surface, threat actors looking to disrupt critical systems, and legacy IT systems.

Now, imagine if that logistics company also had to think about the cybersecurity threats of retail, gas stations, restaurants, and even quarrying.

Derhem Holdings, one of the largest Moroccan private groups operating in different lines of business, has to balance everything that comes with being in these different industries, especially when it comes to cybersecurity. The privacy and data needs of a commercial fishery is vastly different from the systems that power a chain of 50 gas stations. And while the company is also helping to conduct research around COVID-19 vaccines, they also have to think about protecting the network at its 66-hectare quarry in South Morocco.

The diversity of Derhem's businesses increases the complexity of the company's cybersecurity needs, because each industry comes with its own regulatory requirements, sensitive data, and specific risks.

Because the company is constantly adapting and evolving, it needed a cybersecurity solution to scale with it. For several years, Sophos has provided a one-size-fits-all solution for Derhem Holding, growing alongside the company as its expanded into new industries.

"Our relationship with Sophos began from a need to modernize our cybersecurity," Oussama Elhichamy, the company's CISO, says. "We were looking for a solution that could offer us global visibility, quick threat response, and proactive protection across various environments."

Expanding into 24/7 coverage

Derhem's relationship with Sophos began with a few areas of coverage: Sophos Email Advanced and Sophos Mobile Advanced.

Because Derhem Holding saw Sophos' solutions as scalable and complementary, they added Sophos Managed Detection and Response (MDR) services. Sophos MDR provides 24/7 coverage of Derhem's companies' endpoints and networks, constantly hunting for threats and alerting their internal IT team of any prominent alerts.

Elhichamy says Sophos MDR relieves his IT team and saves them time because it prioritizes many false-positive or low-priority alerts, leaving them with fewer alerts to manage manually.

The team also enjoys managing all their alerts and activity through Sophos Central's single pane of glass.

Recently, Sophos MDR alerted Derhem to abnormal behavior on a critical server. Sophos MDR's analysts identified the malicious activity, isolated the activity, and neutralized it before it could compromise any of Derhem's operations.

Elhichamy said Sophos and Derhem worked together to quarantine the affected machine so they could perform forensic analysis. Eventually Sophos MDR uncovered several unpatched vulnerabilities that needed to be remediated and provided additional ways to strengthen the monitoring of Derhem's other endpoints.

"Detecting a threat in minutes rather than hours or days can be the difference between a controlled alert and a major incident," Elhichamy says.

> "Our activities are directly linked to the country's critical infrastructure, and any disruption or breach could have serious consequences. This strengthens our duty to protect, build resilience, and anticipate cyber threats."
>
> **Elhichamy Oussama, Infrastructure and security Manager**

‘Time literally means money’

Detecting these types of threats (and avoiding the worst-case scenario) is specially crucial for Derhem because of its adjacency to Moroccan critical infrastructure. Derhem’s operations include shipping and logistics across Morocco, overseeing oil transportation in and out of the Atlantic Ocean and Mediterranean Sea.

Any disruptions to these services could be costly to Derhem and the people and government of Morocco who rely on many of these services and the energy they power.

“In our sector, time literally means money,” Elhichamy says. “Our activities are directly linked to the country’s critical infrastructure, and any disruption or breach could have serious consequences. This strengthens our duty to protect, build resilience, and anticipate cyber threats.”

As in the case Sophos MDR detecting that intrusion, Sophos’ solutions can detect a threat in minutes, not hours or days, which can be the difference between what Elhichamy calls a “controlled alert” that can be quickly remediated and a major incident.

Sophos MDR’s average time to respond and remediate a threat is 38 minutes, 96% faster than the average in-house security operations team (SOC).

Additionally, by avoiding costly incidents like data exfiltration or service interruptions, Sophos helps Derhem protect its profitability and protects the company’s public image.

With Derhem planning to continue to grow, it’s preparing for Sophos to grow with it.

The company is investing in digitizing many of these processes, which also increases the amount of sensitive data it stores and the breadth of its potential attack surface.

“This requires continuous strengthening of our cybersecurity posture. Sophos is a key partner in this proactive approach to securing our digital transformation,” Elhichamy says.

To get started with Sophos solutions today and find a solution that scales to your needs, speak to an expert today.

To get started with Sophos solutions today and find a solution that scales to your needs, speak to an expert today.

2025-10-21 CCS-EN (NP) CRE-1960

SOPHOS