CUSTOMER CASE STUDY

How INEOS reduced security events by 96% with Sophos

With 96% fewer security events requiring internal intervention, INEOS transformed how its security team operates by combining 24/7 expert monitoring, endpoint visibility, and rapid response.

INEOS

INEOS Group

Industry
Chemicals and petrochemicals

Number of users managed
27,000 users managed

Sophos solutions
Sophos Endpoint
Sophos Managed Detection and Response (MDR) with Next-Gen SIEM

All Sophos solutions are part of Sophos Fusion, the industry's most complete cyber defense system. Powered by agentic AI with human judgment, it sees everything, connects everything, and enables an organization's defenses to respond as one.

SOPHOS

Challenges

- **Protecting a globally distributed organization** across 30 business units in 27 countries.
- **Defending critical national infrastructure** against cybercriminals and state-sponsored actors
- **Managing 3,000+ security events per month**, which force the team to concentrate on reactive firefighting instead of strategic initiatives.
- **Reducing costs** while maintaining strong security controls

Outcomes

- **Enhanced security across the entire environment without building an internal SOC**
- **Continuous protection backed by 24/7 expert monitoring and response**
- **96% reduction in security events requiring internal team involvement**
- **Lower cybersecurity costs and improved visibility through endpoint consolidation**

INEOS is one of the world's largest chemicals companies, operating a complex, globally distributed business that supports critical industries ranging from manufacturing and energy to healthcare and infrastructure.

With approximately 25,000 employees and operations spanning 27 countries, cybersecurity is a business critical priority - one that must scale across diverse environments, business units, and regulatory landscapes.

That responsibility sits with the company's Chief Information Security Officer, Claudio Bolla, and a small internal security team that must balance day-to-day operations with long-term security strategy.

As part of critical national infrastructure, INEOS faces constant attention from cybercriminals, opportunistic attackers, and nation-state actors.

"INEOS is a very large company that spans the world, and we have a lot of third parties coming in. We are a very big attack vector, especially because we are considered a critical national infrastructure," Bolla said. "Everyone has an interest in stopping, controlling, or influencing chemical businesses around the world."

INEOS needed stronger visibility, faster response, and continuous monitoring, without the cost and complexity of building a full internal security operations center.

"[Sophos MDR analysts] are our eyes and ears 24/7,"

Claudio Bolla
CISO at INEOS

How INEOS gained around the-clock security operations support

For INEOS, Sophos MDR has become an extension of the security team, delivering continuous monitoring and expert response capabilities that help the organization stay ahead of threats.

Before adopting Sophos MDR, limited visibility made it difficult to confidently trust alerts or investigate incidents effectively. At the same time, recruiting and retaining specialized security talent presented its own challenges.

"We were not really able to staff our own security operation center," Bolla said. "So it becomes a lot more important for us to have a third party that we can rely on."

Sophos MDR provides INEOS with continuous monitoring, expert-led investigations, and rapid response capabilities. One of the most valuable aspects of Sophos MDR for INEOS is the trust built between teams. Over time, Sophos analysts have become fully integrated into INEOS' day to day operations.

"They are really an integrated part of my team," Bolla said. "We talk to them daily. We have weekly status calls. We are very aligned."

That trust allows Sophos analysts to take decisive action when incidents occur, often outside of normal business hours.

"They have the capacity to block incidents as they see them while we might be sleeping," Bolla said. "I might find out at nine o'clock in the morning that something happened at two o'clock, and they've already blocked accounts, disabled PCs, or isolated servers."

In one instance, a Sophos analyst proactively called Bolla in the middle of the night to request approval to block a device discovered during threat hunting.

"It was two o'clock in the morning, and I was actually quite happy," Bolla said. "She explained what they found and asked if they could block the device. I said, 'Perfect. Go ahead, block it.'"

> "Before, we had around 3,000 events per month, which were too many to handle," Bolla said. "Now, on a bad month, we are talking about 110 or 120 maximum."
>
> **Claudio Bolla**
> CISO at INEOS

Fewer incidents, deeper investigations

Since deploying Sophos MDR, INEOS has seen a dramatic reduction in the number of security events that the in-house team needs to get involved with, allowing them to shift from reactive firefighting to more strategic security work.

That approximately 96% reduction has fundamentally changed how the team operates.

"Before, we just formatted the machine and moved on," he said. "Now we can actually deep dive, understand the threat, and resolve it at the point of origin. The team is doing forensics a lot more than before. It's enabled our team to actually get more skilled."

Instead of spending most of its time responding to alert volume, the team can now investigate threats in greater depth, improve response processes, and focus on strategic initiatives.

Consolidation and visibility at the endpoint

INEOS recently strengthened that approach by migrating approximately 27,000 devices to Sophos Endpoint, completing the rollout in just four months.

According to Bolla, the project was initially driven by the need to reduce costs while maintaining security standards.

"The endpoint migration was driven by cost reduction, to be honest," Bolla said. "The chemical sector is quite hard hit at the moment, so we were looking at a way of saving money while maintaining the same level of security."

Beyond protection, the move has already delivered additional operational benefits. By reducing the number of endpoint agents and improving visibility across the estate, the security team gained clearer insight into software usage and overall device health.

"We've reduced the number of agents making visibility a lot easier. We also have soft benefits, such as knowing what versions of software are being used within the estate" he said. "That's because the tool captures so much data."

By integrating their endpoint protection directly into MDR workflows, INEOS reduced complexity while improving overall visibility across a vast global environment.

> The value of the Sophos partnership cannot be measured in monetary terms — it's infinite," he said. "Without Sophos, we would be lost."
>
> **Claudio Bolla**
> CISO at INEOS

SOPHOS

A partnership built on trust

For Bolla, the value of Sophos goes far beyond technology.

When asked what advice he would give other organizations evaluating MDR services, Bolla pointed to the importance of finding a partner that shares accountability for outcomes and continuously shares new ideas.

“One of the biggest challenges with a lot of service providers is that they are limited by what’s written in the statement of work, while here it’s a real partnership where the analysts, on their own, propose solutions.”

After years of working together, he summed up the relationship simply:

“It’s not only a partnership — it’s a friendship. It’s a long term relationship that we truly cherish.”

To learn more about Sophos MDR, visit our website and speak to an expert today.

To learn more visit Sophos.com

SOPHOS