CUSTOMER CASE STUDY

# How ESCO Technologies connects inherited tools into one defense with Sophos

As acquisitions introduce new tools, teams, and security signals into the business, ESCO Technologies uses Sophos to connect them into a coordinated defense that reduces IT burden and improves visibility across 9 primary business units.

SOPHOS

**ESCO Technologies**

**Industry**
Energy & Utilities

**Sophos solutions**
Sophos Managed Detection and Response (MDR)

Sophos Extended Detection and Response (XDR)

Sophos Endpoint

*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.*

# Overview

- 3,400+ employees globally
- Operations across utilities, aerospace & defense, and testing environments
- 9 major business units, several with additional subsidiary companies
- Distributed IT model, with each business running its own IT organization
- Frequent acquisitions that bring new tools, processes, and security requirements into the environment

# Challenges

- Keeping cybersecurity consistent across 9 independently operated business units.
- Gaining visibility across acquired businesses with different tools, processes, and security maturity.
- Identifying and closing coverage gaps across a distributed environment.
- Reducing alert fatigue and response burden on lean IT teams.
- Giving leadership a clearer view of risk, readiness, and progress of the security program.

# Outcomes

- **Shared visibility across subsidiaries and acquired businesses**, helping ESCO understand risk across independently operated IT teams.
- **24/7 monitoring, investigation, and response through Sophos MDR**, extending ESCO's security team without adding headcount.
- **Faster onboarding of acquisitions**, with Sophos helping to connect existing tools into ESCO's broader security strategy.
- **Reduced operational burden**, with Sophos narrowing 3.6 million identified security events to 186 cases requiring ESCO involvement in 2025.
- **Less manual triage for lean IT teams**, so corporate and local teams can focus on the decisions that matter most.
- **Clearer evidence of coverage, gaps, and risk reduction** for executive and board-level conversations.

"We run a very distributed IT organization. Every business has their own IT organization. With that, we need a strong partner like Sophos that's going to allow us to protect all of our assets from a security perspective."

**Amy Sawvell**
**Senior IT Director**
**ESCO Technologies**


*Sophos narrowed 3.6 million identified security events to just 186 cases requiring ESCO involvement in 2025.*

# Turning acquired tools into connected defense

For Amy Sawvell, Senior IT Director at ESCO Technologies, cybersecurity is about protecting a collection of highly engineered businesses that operate in industries where resilience matters, such as utilities, aerospace and defense, and advanced testing environments.

ESCO Technologies has approximately 3,400 employees globally and 9 major subsidiaries, several of which own additional subsidiary companies. Each business runs its own IT organization, giving local teams the flexibility to support their own operations.

But that very distributed model creates a more complex challenge for corporate cybersecurity leadership: how can ESCO Technologies protect what they can't always see?

"We run a very distributed IT organization," says Sawvell. "Every business has their own IT organization. With that, we need a strong partner like Sophos that's going to allow us to protect all of our assets from a security perspective."

That challenge becomes even more complex with every new acquisition. New businesses often join ESCO with their own tools, processes, and security requirements already in place. ESCO needed a way to bring those businesses into a shared cybersecurity strategy without disrupting what was already working or forcing teams to replace investments that were still delivering value.

The goal was not to make every business operate the same way. It was to connect them into a unified defense, giving corporate security leaders and local IT teams a clearer view of risk across the organization while preserving the flexibility that makes ESCO's operating model work.

# Built to connect, not replace

Instead of asking the newly acquired businesses to replace their existing investments, Sophos Fusion connects all control points – Sophos and non-Sophos – from those environments into a single, unified defense system. Security signals become visible across the organization, and protection extends faster with less disruption.

For Sawvell, that flexibility is non-negotiable and central to the way she chooses cybersecurity providers.

"I don't look for a vendor, I look for a partner," she says.

> "The nice benefit with Sophos is we've got that functionality and flexibility," says Sawvell. "They can pull in their existing security stack, connect it to Sophos, and we've got protection right away."
>
> **Amy Sawvell**
> **Senior IT Director**
> **ESCO Technologies**

That means working with a provider willing to understand how ESCO operates, support the tools and teams already in place, and help build a security strategy around the business—not the other way around.

This is where Sophos Fusion's architecture makes a difference. By connecting disparate tools and security signals into a coordinated defense system, ESCO can scale cybersecurity across a decentralized, growing organization. Corporate leadership gains a clearer view of risk, local IT teams stay connected to the broader strategy, and acquired businesses become visible, protected, and integrated into ESCO's broader defense faster.

## 24/7 protection without 24/7 pressure on IT

With Sophos MDR, ESCO can connect security visibility, investigation, and response across its distributed environment. Corporate security leadership can see activity across all business units, while local IT teams continue to own day-to-day operations. The result is a shared security model that works across independent businesses without adding more complexity for already busy teams.

More importantly, it creates a dramatic reduction in noise. In 2025, Sophos solutions identified approximately 3.6 million security events and investigated roughly 360,000 cases. Only 186 cases required involvement from ESCO's internal IT teams.

"The real benefit  was [that] only 186 cases ever were touched by our internal IT department in 2025," says Sawvell.

That is the difference between seeing everything and having to handle everything. Sophos MDR investigates activity around the clock, giving ESCO's teams the context they need and escalating only when their involvement matters.

The value is especially clear after hours.

"We've had situations where a user comes over and says, 'I think I clicked on something I shouldn't have,' and we already knew about it," says Sawvell.

By turning connected security signals into action, Sophos helps ESCO's local lean IT teams focus on the work that moves the business forward instead of continually triaging alerts.

"We've had situations where a user comes over and says, 'I think I clicked on something I shouldn't have,' and we already knew about it."

**Amy Sawvell**
**Senior IT Director**
**ESCO Technologies**

# A connected defense for what comes next

Growth will continue to bring new complexity for ESCO. Every acquisition introduces different tools, processes, and security requirements, while existing businesses continue to operate with the independence they need.

Sophos helps ESCO bring those environments into a more connected defense, giving corporate security leadership clearer visibility while helping local IT teams stay focused on their businesses. For Sawvell, that connected approach matters because it is backed by a partner ESCO trusts.

"Having a partner like Sophos that has our back 24/7, whether it's a holiday weekend or 2:00 in the morning, allows you as an IT leader to sleep," she says. "You've got a trusted partner that's going to be there, watching your systems."

That trust gives ESCO a stronger foundation for the future. With Sophos, the company can continue integrating acquired businesses, connecting security signals, and strengthening protection across its portfolio without forcing every team to operate the same way.

For a business supporting critical infrastructure industries, that flexibility – backed by a defense system that sees everything and responds as one – helps ESCO grow with greater confidence.

"Having a partner like Sophos that has our back 24/7, whether it's a holiday weekend or 2:00 in the morning, allows you as an IT leader to sleep. You've got a trusted partner that's going to be there, watching your systems."

**Amy Sawvell**
**Senior IT Director**
**ESCO Technologies**

To learn more visit Sophos.com



SOPHOS