SOPHOS

Managed Detection and Response (MDR) vs. In-house Security Operations Center (SOC)

What you get with Sophos MDR services

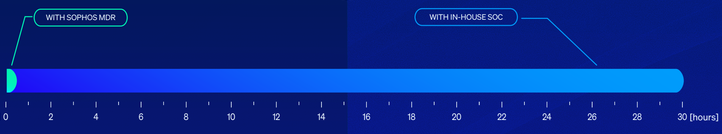
Supplementing an in-house SOC

Time to detect with current staff

38 minutes
Average time to detect and fully remediate a threat.

vs.

Up to 30 hours
Identifying and mitigating a threat could take days.



Cybersecurity skills

WITH SOPHOS MDR

Robust expert team
You're protected by a team of cybersecurity experts including analysts, incident responders, threat hunters, researchers, data engineers, and data scientists.

vs.

WITH IN-HOUSE SOC

In-house skills gap
Your in-house SOC is only as strong as your current team's skills, and expanding those capabilities demands significant time and investment in hiring, training, and retaining top talent.

Sorting through a mountain of alerts

WITH SOPHOS MDR

Proactive remediation
Sophos MDR goes beyond alerts and notifications, stopping active threats on your behalf around the clock.



WITH IN-HOUSE SOC

Alert fatigue
You're totally dependent on building and acquiring the right combination of technology and people to identify legitimate threats and act upon them.

Lower cyber insurance claim values

WITH SOPHOS MDR

97.5% less
MDR services users claim 97.5% less on cyber insurance than those that rely on endpoint protection alone.

Source: Sophos Quantifying ROI Report, February 2025



WITH IN-HOUSE SOC

Higher claim values
Higher cybersecurity claim values and slower recovery from attacks.

Integration with current solutions

WITH SOPHOS MDR

Direct integration
Turn-key integrations with your existing IT stack and security solutions.

vs.

WITH IN-HOUSE SOC

Disjointed security solutions
Disjointed security solutions result in complexity, visibility gaps, and data silos.

WITH SOPHOS MDR

Immediate
24/7 coverage.

vs.

WITH IN-HOUSE SOC

Months
of training, hiring, and configuring.

To learn more about Sophos MDR services, speak with an expert:
Sophos.com/stop-threats