

Detection, response, and the depth to match any incident

Fully managed 24/7 detection and response, with experienced human responders ready to take control when an incident escalates.

Serious multi-stage attacks often involve high-stakes decisions, where context and business impact require human judgment. What separates a contained incident from a business-stopping breach is whether that expertise takes control fast enough, and whether it was in place before the phone rang. Sophos offers four choices, from 24/7 detection and response to specialist forensics.

Sophos Managed Detection and Response (MDR) service

Sophos MDR is the world's largest Agentic SOC, where AI investigates and responds in seconds, and human analysts own the outcomes.

Sophos MDR

Sophos MDR is the core service tier: 24/7 fully managed threat detection, investigation, proactive threat hunting, and response, delivered by the world's largest Agentic SOC. The goal is to stop live attacks and remove endpoint threats, with remediation guidance to close gaps and prevent reoccurrence. It works with Sophos Endpoint or your existing third-party endpoint protection and integrates with 500+ security and IT tools.

Sophos MDR Plus

Sophos MDR Plus includes everything in Sophos MDR, plus critical incident response and a breach protection warranty. A dedicated Incident Advisor owns communication and coordination, delivering an incident timeline, written summary, remediation guidance, and a post-incident account health check. Requires Sophos Endpoint deployed across your estate.

For details on the response actions included in Sophos MDR and Sophos MDR Plus, please refer to the [Supported Response Actions documentation](#).

Sophos Digital Forensics and Incident Response (DFIR) and the Sophos Security Services Retainer

Sophos DFIR is available to any organization, including both Sophos and non-Sophos customers, for when fast assistance is needed to identify and stop active threats against your organization. It also includes additional incident response services and capabilities not included with Sophos MDR and Sophos MDR Plus.

Sophos DFIR

When a cyber emergency strikes, Sophos DFIR provides cross-functional experts who rapidly triage and stop the active threat, then identify how the attacker got in and recommend actions to prevent recurrence.

Sophos Security Services Retainer

The Sophos Security Services Retainer combines proactive preparedness that lowers risk and strengthens resilience with guaranteed DFIR access when a threat actor strikes.

Not every alert is an incident

Sophos MDR investigates suspicious activity and validates what the evidence shows. Incident Response is initiated when that evidence confirms a compromise or unauthorized access that threatens your systems or data and requires coordinated action to remove the threat.

EXAMPLES INCLUDE:

- An active attacker in your environment
- Misuse of privileged access
- Unauthorized access to sensitive data
- Encryption, destruction, or disruption of critical systems

A single alert, exposed credential, or phishing email may prompt an investigation, but does not by itself qualify as an Incident.

Capabilities

DETECTION AND THREAT RESPONSE

	Sophos MDR	Sophos MDR Plus	Sophos DFIR
24/7 monitoring, triage and investigation	✓	✓	
Proactive threat hunting	✓	✓	
Active threat response	✓	✓	
Remediation guidance	✓	✓	
Endpoint threat removal	✓	✓	✓

INCIDENT RESPONSE

	Sophos MDR	Sophos MDR Plus	Sophos DFIR
Formal incident-response engagement		✓	✓
Incident timeline and written summary		✓	✓
Post-incident health assessment		✓	
Breach protection warranty		✓	

DEEP FORENSICS AND SPECIALIST WORK

	Sophos MDR	Sophos MDR Plus	Sophos DFIR
Onsite assistance	Remote	Remote	✓
Disk-level forensics and evidence analysis			✓
Legal/regulatory-grade investigation			✓
Ransomware negotiation and decryption support			✓
Coverage for unprotected assets and 3rd-party data			✓

Who leads the incident

Incident Advisor

A named Incident Advisor keeps communication and context clear between your organization and the Sophos MDR team as they detect, contain, and stop threats across your environment.

Incident Lead

The default for a formal DFIR engagement, an Incident Lead directs the response and owns the incident end-to-end across specialists, evidence, decisions, and communication.

	Sophos MDR	Sophos MDR Plus	Sophos DFIR
Incident Advisor		✓	
Incident Lead			✓

In particularly complex incidents, Sophos may recommend engaging additional specialized roles, such as an Incident Commander, to provide enhanced coordination, governance, and oversight throughout the response effort. When appropriate, these optional services will be discussed with you during the Sophos DFIR intake and assessment process.

The Sophos Security Services Retainer

The Sophos Security Services Retainer brings proactive services, professional services, and DFIR coverage into one subscription, using a flexible service-unit model that lets organizations prioritize the testing, assessments, and readiness work that uncovers weaknesses and strengthens defenses. If an incident occurs, the retainer guarantees rapid access to experienced DFIR experts, defined response SLAs, and pre-negotiated discounted emergency hourly rates, so there is no delay or uncertainty when it matters most.

- Flexibility via prepaid Service Units
- Broad access to proactive and professional services
- Complete coverage across the security lifecycle
- Included DFIR retainer with guaranteed SLAs
- Access to worldclass security expertise

Speak with an expert

sophos.com/MDR →

Request a custom service proposal for Sophos MDR.