Sophos Rapid Response

Immediate Response To Active Threats

Sophos Rapid Response provides lightning-fast assistance with identification and neutralization of active threats against your organization, delivered by an expert team of incident responders.

Every Second Counts During an Attack

When responding to an active threat, it is imperative that the time between initial indicator of compromise and full threat mitigation be as small as possible. As an adversary progresses through the kill chain, it is a race against time to ensure they are not able to achieve their objectives.

With Sophos Rapid Response, we get you out of the danger zone fast with our 24/7 team of remote incident responders, threat analysts, and threat hunters who can:

- Quickly take action to triage, contain, and neutralize active threats
- Eject adversaries from your estate to prevent further damage to your assets
- Perform ongoing 24/7 monitoring and response to enhance your protection
- Recommend real-time preventative actions to address the root cause
- Quickly deploy Sophos cloud-based technology stack across your estate
- Analyze supplementary data from third-party technologies
- Provide a detailed post-incident threat summary that describes our investigation

Features of Rapid Response

Rapid Response includes all of the benefits of Sophos Managed Threat Response Advanced as well as a number of additional benefits.

	Sophos Rapid Response
MTR Advanced in "Authorize" threat response mode	✓
24/7 threat monitoring, hunting, and response	✓
Dedicated response lead during active threat and direct call-in access	✓
Analysis of supplemental data from third-party technologies	✓
Expedited quoting and same-day account activation	✓
Formal post-incident threat summary detailing investigation	✓

Highlights

- Rapid identification and neutralization of active threats
- Incident response and 24/7 monitoring for 45 days
- Dedicated point of contact and response lead
- Post-incident threat summary detailing all actions taken
- Predictable pricing with fixed costs and no hidden fees
- Designed to be insurance reimbursable
- Seamlessly transition into a subscription with Sophos Managed Threat Response (MTR) after Rapid Response

SOPHOS

Active Threat Neutralization

The Sophos Rapid Response team are specialists at neutralizing active threats. Whether it is an infection, compromise, or unauthorized access of assets that is attempting to circumvent your security controls, we have seen and stopped it all.

Our expert incident response team is part of Sophos Managed Threat Response (MTR), our 24/7 threat hunting, detection, and response service that proactively hunts for, identifies, investigates, and responds to threats on behalf of our customers as part of a fully-managed service.

Aligned Incentives

Traditional Incident Response (IR) services are priced hourly, leaving you at risk to underestimate the time required to fully mitigate a threat. This leaves you open to needing to purchase additional hours. Worse, it incentivizes the traditional IR service to maximize the number of hours their response takes.

Sophos Rapid Response offers a fixed-fee pricing model with no hidden costs, determined by the number of users and servers in your estate. And it's delivered remotely, so we can initiate response actions on day one. It is in our interest, and yours, to get you out of the danger zone as expeditiously as we can, as time is never a factor in cost.

Rapid Deployment

To ensure the fastest response possible, the Sophos rapid deployment process is laser-focused on immediate distribution of Sophos MTR agents to discoverable endpoints and servers.

After developing a replacement strategy utilizing removal utilities to replace existing products, a remote team of deployment engineers consult with each Rapid Response customer to initiate a custom plan-of-action, leveraging automation tools for mass-deployment across the network.

The team works collaboratively to optimize the Sophos MTR agent health status across the network, ensuring best-practice configurations to quicken investigation.

Rapid Response Methodology

After Rapid Response has been approved and the customer has accepted our service agreement, we jump straight to action. There are four main stages of Rapid Response – onboarding, triage, neutralization, and monitoring.

Onboarding

- Host Kick-off call to establish communication preferences and confirm what (if any) remediation steps have already been taken
- Identify the scale and impact of the attack
- Mutually define a response plan
- Start deploying service software

Triage

- Asses operating environment
- Identify known indicators of compromise or adversarial activity
- Perform data collection and initiate investigative activities
- Collaborate on plan for initiating response activities

Neutralize

- Remove the attackers' access
- Stop any further damage to assets or data
- Prevent any further exfiltration of data
- Recommend real-time preventative actions to address root cause

Monitor

- Transition to the MTR Advanced service
- Perform ongoing monitoring to detect reoccurrence
- Provide a post-incident threat summary

Detailed Threat Summary

Once we have neutralized the active threat against your organization, we will provide you with a formal summary of our investigation, detailing the actions we took, the discoveries we made, as well as recommending long-term guidance on how to mitigate a reoccurrence of similar threats in the future.

Post Incident 24/7 Monitoring and Response

The moment the incident is resolved and the immediate threat to your organization is neutralized, we transition you to our top-tier MTR service, MTR Advanced, providing around-the-clock proactive threat hunting, investigation, detection, and response.

Should the threat return or a new threat emerge, we will be there ready to respond at no additional cost to you. If you are under attack for 45 days, we defend you for 45 days during your subscription term.

Experiencing an Active Breach?

Call your regional number below at any time to speak with one of our Incident Advisors.

USA +1 4087461064

Australia +61 272084454

Canada +1 7785897255

France +33 186539880

Germany +49 61171186766

United Kingdom +44 1235635329

If all the Incident Advisors are busy, please leave a message and someone will get back to you as quickly as possible.

Experiencing an Active Breach?

For more information visit
sophos.com/rapidresponse

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-05-12 DS-EN (DD)

SOPHOS