Sophos Rapid Response

Frequently Asked Questions

Do I need to be an existing Sophos customer to become a Rapid Response service client?

No. The Sophos Rapid Response service is available for both existing Sophos customers as well as non-Sophos customers.

I am experiencing an active breach, what do I do next?

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

Australia: +61 272084454	**Italy**: +39 02 947 52897
Austria: +43 73265575520	**Sweden**: +46 858400610
Canada: +1 7785897255	**Switzerland**: +41 445152286
France: +33 186539880	**United Kingdom**: +44 1235635329
Germany: +49 61171186766	**USA**: +1 4087461064

How fast is the Rapid Response service?

Very fast. The majority of customers are onboarded in a matter of hours and triaged in 48 hours. Since the service is completely remote, response can begin in a matter of hours after Sophos is contacted.

What is the onboarding process?

The Rapid Response team can begin the onboarding process and start their investigation as soon as they receive approval. For organizations that do not have Sophos XDR installed in their environment Sophos offers a Rapid Deployment option. The Rapid Deployment team are experts in quick installs in environments that are currently experiencing an active incident.

Is there an additional cost associated with Rapid Deployment?

No. Rapid Deployment is included as part of the service.

What is the 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

- Assess 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 the issue

SOPHOS

Monitor

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

What languages is Rapid Response offered in?

Currently the service is offered in English only.

Does Sophos work with or replace Data Forensic Incident Response services (DFIR)?

Sophos can work side-by-side with DFIR services and has done so in multiple engagements. Sophos Rapid Response focuses on the incident response aspect of DFIR services and does not provide all the services typically offered of a traditional DFIR engagement.

Does Sophos physically ship equipment? Are incident responders flown to the customer location?

No. All incident response is conducted remotely.

Do customers have to install Sophos onto their endpoints?

Yes. Rapid Response is delivered using the Managed Detection & Response / Sophos XDR to ensure we can provide effective 24/7 monitoring and response. This means they will also need to uninstall or temporary disable their current non-Sophos endpoint protection.

The Rapid Response team does not need to wait for the deployment to be complete before they can start taking remedial actions to contain and neutralize the threat. The team will leverage any data that is available and utilize tools that are suitable to aid the response.

How is pricing generated?

Pricing is based on the total number of users and servers and is priced as a 45-day fixed term.

Are there additional costs?

No. There are no hidden costs to the service.

What happens after the Rapid Response period ends?

At the end of the term customers can either transition to a full Sophos Managed Detection & Response (MDR) customer or the license will expire.

Can we deploy Rapid Response on a segment of the environment, or does the entire environment have to be part of the scope?

In select situations, Rapid Response can only apply to a segment of the customer's environment. A Rapid Response specialist can provide further details as part of the project scoping.

Can Sophos work with an intermediary representing the customer, such as a law firm, on the contract?

Yes. Working with an intermediary is possible.

Can Sophos determine what files have been exfiltrated / stolen in the attack?

The Rapid Response service includes a best effort to determine which (if any) files have been exfiltrated as part of an attack. However, this is not guaranteed as it may depend on the data available as part of the investigation.

Will Sophos decrypt ransomware on behalf of the customer?

No. This is not part of the Rapid Response service.

Will Sophos help the customer negotiate or facilitate a ransom payment?

No. This is not part of the Rapid Response service.

SOPHOS