

Sales and Technical FAQ

General overview

What is Sophos DFIR?

Sophos Digital Forensics and Incident Response (DFIR) is there for you when a cyber emergency strikes, working quickly to assess, contain, understand, and provide remediation recommendations. Our team of cross-functional experts apply their years of experience and learnings to rapidly triage, contain, and neutralize active threats, and eject adversaries to prevent additional damage.

Sophos DFIR also helps you determine if your organization was impacted by an incident, and understanding the scope of that incident. The service provides a variety of investigative activities to help identify the root cause of incidents, perform compromise assessments to determine if observed behavior is malicious, conduct threat hunting activities and threat intelligence, and assist with ransom negotiations.

Who is Sophos DFIR for?

Any organization experiencing an active security incident, a recent attack that requires further investigation, or suspicious activity that needs investigating to understand if it poses a threat.

Do I need to be a Sophos customer to purchase Sophos DFIR?

No. Sophos DFIR 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 Sophos DFIR experts:

- **Australia:** +61 272084454
- **Austria:** +43 73265575520
- **Canada:** +1 7785897255
- **France:** +33 186539880
- **Germany:** +49 61171186766
- **Italy:** +39 02 94752 897
- **Switzerland:** +41 445152286
- **United Kingdom:** +44 1235635329
- **USA:** +1 4087461064

Contact us via email at DFIR@sophos.com.

Is Sophos DFIR remote or onsite?

Both remote and onsite options are available.

How fast is the Sophos DFIR service?

Most customers are onboarded in two hours and triaged in 48 hours. Since the service can be conducted completely remote, response can begin in a matter of hours after you first contact Sophos.

How quickly can you begin onboarding?

The Sophos DFIR team can begin the onboarding process and start the investigation as soon as they receive your approval.

What is the Sophos DFIR methodology?

After you accept the service agreement, we hold the engagement kickoff call. This can be done via email if you prefer. The investigation begins once we understand your objectives for the engagement.

Sophos DFIR includes different categories of work that we can offer. During the initial scoping call, we work with you to identify the required categories and an estimated number of hours.

Categories of focus include Engagement Management, DFIR, Compromise Assessment, Threat Hunting, Threat Intelligence and Research, Ransom Negotiation, Engagement Report, Onsite Support (if applicable), Business Email Compromise, and Software Deployment.

What language(s) is Sophos DFIR offered in?

Currently the service is offered in English and Japanese. You must speak English or Japanese with technical proficiency.

Do I have to install Sophos technology on my endpoints?

No, Sophos DFIR can be delivered using Sophos XDR, or we can deploy the Sophos XDR sensor alongside your incumbent solution. Either option allows us to quickly investigate the incident.

The Sophos DFIR team does not need to wait for deployment to be complete before 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?

Sophos will estimate the number of hours needed to respond to the incident based on scoping questions. You pay for only the actual hours used.

Are there additional costs?

If onsite work is requested, travel costs are billed to you.

Can we deploy Sophos DFIR on a segment of our environment, or does our entire environment have to be part of the scope?

In select situations, Sophos DFIR can be applied to a segment of your environment. An Sophos DFIR specialist can provide further details as part of project scoping.

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

Yes. Working with an intermediary is possible.

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

The Sophos DFIR 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 my behalf?

No. This is not part of the Sophos DFIR service.

Will Sophos help me negotiate or facilitate a ransom payment?

Sophos DFIR includes expert ransom negotiation with threat actors. However, Sophos does not facilitate ransom payment, but can recommend and work with third parties for this if needed.