Sophos Managed Risk – Service Description | Sophos

Sophos Managed Risk – Service Description

This Service Description describes Sophos Managed Risk (**"Service"**). All capitalized terms in this Service Description have the meaning ascribed to them in the Agreement (defined below) or in the Definitions section below.

This Service Description is part of and incorporated into, as applicable: (i) Customer's or Managed Service Provider's manually or digitally-signed agreement with Sophos covering the purchase of a Service subscription; (ii) Managed Service Provider's manually or digitally-signed agreement(s) with Sophos covering its purchase of Offerings of which the Service is a part; or (iii) if no such signed agreement exists, then this Service Description will be governed by the terms of the Sophos End User Terms of Use posted at https://www.sophos.com/legal (collectively referred to as the **"Agreement"**). To the extent there is a conflict between the terms and conditions of the Agreement and this Service Description, the terms and conditions of this Service Description will take precedence.

Notwithstanding anything to the contrary in the Agreement, Customer/MSP acknowledges and agrees that: (i) Sophos may modify or update the Service from time to time without materially reducing or degrading its overall functionality; and (ii) Sophos may modify or update this Service Description at any time to accurately reflect the Service being provided, and any updated Service Description will become effective upon posting to https://www.sophos.com/legal.

I. DEFINITIONS

Capitalized terms used in this Service Description, and not otherwise defined in the Agreement, have the meaning given below:

"Asset(s)" is any physical or virtual system (e.g., endpoints, servers, firewalls, etc.) that are the targets or subjects of a vulnerability scan.

"Security Services Team" is the Sophos team conducting the vulnerability assessment on Customer/MSP Assets.

II. SCOPE OF SERVICE

The Service consists of identifying internet-accessible Assets and providing vulnerability assessment of Customer/MSP environment by performing automated and recurring vulnerability scans of the Customer/MSP defined Asset(s). All aspects of the Service will be provided remotely.

The Service consists of activities described below:

1. **Onboarding**. During the onboarding process, as a precondition to delivery of the Service, Customer/MSP will (i) identify a primary contact to work directly with the Security Services Team during the Subscription Term; (ii) for **external scanning**,specify root domain(s) for Asset monitoring and configure internet facing IP addresses and set the schedule for weekly external vulnerability scan in Sophos Central that the Customer/MSP wants covered by the Service; (iii) and for **internal scanning**, deploy vulnerability scanning appliance(s) in all networks and configure internal IP ranges that contain the Assets and set the schedule for weekly internal vulnerability scans in Sophos Central that the Customer/MSP wants covered by the Service.
2. **Baseline Review.** Approximately one month post onboarding, Customer/MSP will coordinate with the Security Services Team to: (i) confirm that the specified root domain(s) and Assets are the ones Customer/MSP intended to be covered by the Service; (ii) review initial external and internal scan results; (iii) review prioritized vulnerabilities to be remediated; and (iv) review and discuss Customer's/MSP's environment and relevant context.
3. **External Attack Surface Management.** Sophos will provide weekly reports providing an inventory of Customer's/MSP's discovered external facing assets within the specified root domain(s).
4. **Vulnerability Assessment.**

   a. Vulnerability Scanning. Sophos will perform weekly external and internal vulnerability scanning of Assets on the schedule defined by the Customer/MSP.

   b. Vulnerability Reporting. Sophos will provide a vulnerability assessment report containing the findings after each scan. Each scan report will include the identified vulnerabilities with a description of each vulnerability, level of severity, remediation suggestions, and links to relevant resources on additional information on the identified vulnerabilities. In the event a critical vulnerability is identified during an external scan, or if other vulnerabilities are identified (for both external and internal scans) that the Security Services Team deem to be high risk, the Security Services Team will alert the Customer/MSP.

   c. On-Demand and Ad-Hoc Scans. Upon prior request of Customer/MSP, Sophos will perform on-demand scans. On-demand scans are limited to five (5) per month. Customer/MSP must provide at least one (1) business day of lead time to schedule and run the scan. Additionally, Sophos may initiate ad-hoc scans in the event the Sophos Services Team discovers a new vulnerability with high exposure potential without prior approval of Customer/MSP. The scope and

frequency of Sophos initiated ad-hoc scans will depend on the Sophos Security Team's assessment of the Customer/MSP environment and the nature of the vulnerability.

5. **Quarterly Review.** Sophos will review the external and internal scan findings with the Customer/MSP on a quarterly basis to give visibility into Customer's/MSP's current vulnerability posture and prioritization of the vulnerabilities to be remediated by Customer/MSP based on scan results and key findings observed within Customer/MSP environment, and to discuss Customer's/MSP's overall attack surface security posture and the vulnerability trends.

6. **Scan Reports.** Each scan report will be accessible within Sophos Central for up to two (2) years from the scan completion date. The report is solely for Customer's/MSP's internal use and may not be re-distributed, resold, or otherwise transmitted outside of Customer's/MSP's organization.

7. **Service Scope Change.** If Customer/MSP desires to modify the defined Assets for external scans and/or root domains being monitored, Customer/MSP may open a case requesting the desired changes within Sophos Central. Changes to Asset(s) and root domain(s) are limited to once a month. The Assets targeted for the internal scan can be modified by Customer/MSP.

III. CUSTOMER/MSP RESPONSIBILITIES.

Customer/MSP acknowledges and agrees that, in addition to the actions required of Customer/MSP in Article II above, Customer/MSP must take the following actions to facilitate and enable delivery of the Service, and Sophos shall have no liability for any degraded, incomplete, or failed Service delivery which may result from Customer/MSP's failure to take the required actions. Sophos reserves the right to suspend Service delivery until such time as Customer/MSP performs the required actions. Failure to complete the required actions after written notice from Sophos (including email notice from the Security Services Team to the Customer/MSP designated contacts) shall constitute a material breach by Customer/MSP of the Agreement.

1. **Onboarding.** Customer/MSP will perform all required activities during the onboarding process.

2. **Installation Requirements.** Customer/MSP/Beneficiary must have a valid and active Sophos Central account. If internal vulnerability scanning will be performed, Customer/MSP will need to deploy the vulnerability scanning appliance in networks containing the Assets Customer/MSP wants covered by the Service.

3. **Customer/MSP Personnel.** Customer/MSP must identify an appropriate number of suitably skilled personnel who will work with Sophos during the provisioning of the Service. Customer/MSP's identified personnel must have the necessary technical and business knowledge and authority to make decisions concerning the Service.

4. **Timely Response.** Customer/MSP must promptly acknowledge receipt of Sophos communications in writing (via email or other agreed method) and must timely respond to Sophos's requests.

5. **Authority and Indemnification.** Customer/MSP is responsible for obtaining all necessary permissions and consents to enable the Security Services Team to access and scan the identified Assets, including third-party permissions as required. Customer/MSP represents and warrants that it has the necessary right, title, license, and authority for Customer/MSP to provide and/or facilitate Sophos's access to Asset(s), including any information, data, networks, and systems, in connection with the Service delivery. Customer/MSP agrees to indemnify, defend, and hold Sophos harmless from and against any and all claims, losses, liabilities and damages, including reasonable attorney's fees, arising from (i) any and all third party claims brought against Sophos that arise out of the scanning, testing and/or evaluation of incorrect or unauthorized Asset that are provided by Customer/MSP, or (ii) any breach of a Customer/MSP representation or warranty.

6. **Data Backups.** Customer/MSP acknowledges and agrees that the scanning of IP addresses and/or domain names may expose vulnerabilities and, in some circumstances, could result in the disruption of Service or corruption or loss of data. Customer/MSP agrees that it is Customer's/MSP's responsibility to perform regular backups of all data contained in or available through the devices connected to Customer's/MSP's IP address and/or domain names and that Sophos has no liability for any corruption or loss of data.

7. **Actions Outside the Scope of Service.** All activities that are not expressly provided in this Service Description are outside of the scope of the Service. Customer/MSP is solely responsible and liable for: (i) taking any actions that are outside of the scope of the Service (e.g., Sophos's suggestions regarding patching and vulnerability remediation, and collaboration with law enforcement, etc.); and (ii) for any actions undertaken by Sophos at Customer's/MSP's specific direction that are not provided in this Service Description.

8. **Actions Taken by Partners.** Customer may allow Partners to take certain actions within the scope of the Service on Customer's behalf, in which case Customer is

responsible for all actions or omissions of such Partner. Sophos will not be liable for Partners' actions or omissions.

9. **MSP Additional Responsibilities.** MSP is solely responsible for: ensuring that any Beneficiary for which MSP performs this Service has agreed to accept all risks described in this Service Description or otherwise inherent in the Service. MSP will indemnify and hold Sophos harmless for any claim brought against Sophos by a Beneficiary if such claim results, in whole or in part, from MSP's failure to fully perform its obligations under this Service Description or the Agreement with respect to the Service.

IV. ADDITIONAL TERMS.

1. **Service Exclusion.** Customer/MSP agrees and acknowledges that Sophos will not be liable or be considered in breach of this Service Description or the Agreement: (i) due to any delay or failure to perform its obligations hereunder as a result of industry or infrastructure wide ransomware, cyberwarfare or other cyberattacks that causes the Security Services Team to be unable to provide resources in a timely manner; (ii) due to unforeseen circumstances or to causes beyond Sophos reasonable control including but not limited war, strike, riot, crime, pandemic, acts of God, or shortage of resources; (iii) due to legal prohibition, including but not limited to, passing of a statute, decree, regulation, or order; (iv) during any period of Service suspension by Sophos in accordance with the terms of the Agreement; (v) if Customer/MSP is in breach of the Agreement (including without limitation if Customer has any overdue invoices); or (vi) during any scheduled or emergency maintenance windows.

2. **Service Disclaimer.** Customer/MSP acknowledges and agrees that while Sophos employs industry-standard technologies and methodologies for conducting vulnerability scans, these scans may at times yield false positives or negatives. Furthermore, Customer/MSP acknowledges and agrees that Sophos does not guarantee that vulnerability scans provide a complete and accurate picture of Customer's or a Beneficiary's security flaws, and Customer/MSP agrees not to rely solely on such vulnerability scans.

Revision Date: 12 June 2025