Breach Protection Warranty For Managed Service Providers Of Sophos MDR Complete Subscription

Sophos provides this limited warranty (“MSP Warranty”) for the Sophos MDR Complete software subscription offered by its Authorized Managed Service Providers that: (a) have enabled a subscription for MDR Complete (the “Subscription”) in respect of the MSP’s Beneficiary which suffers a Breach Incident (each as defined below); (b) are not in default with Sophos under the Agreement; and (c) ensure that a currently supported version of the Products (as defined below) are correctly installed and fully operational on the relevant Beneficiary’s Managed Endpoint(s).

This MSP Warranty is part of the Service Description for Sophos Managed Detection and Response offering (“MDR Service Description”) and is subject to the Agreement (as defined in the MDR Service Description). In the case of a conflict between the MDR Service Description or the Agreement in respect of the MSP Warranty, then the terms of this MSP Warranty shall prevail to the extent of such conflict.

MSP hereby acknowledges and agrees to have read, to have understood, and to be bound by this MSP Warranty and the terms and conditions outlined herein with respect to the MSP Warranty offered with the Subscription provided by the MSP.

Capitalized terms not defined in this MSP Warranty shall have the meaning given to them in the MDR Service Description or the Agreement, as applicable, but for the purposes of this MSP Warranty, the following definitions shall apply:

“Authorized Managed Service Provider” or “MSP” means a managed service provider that has (i) either entered into the Agreement with Sophos or agreed to the terms of the Agreement through the online sign-up process and (ii) that has been approved by Sophos as an MSP Flex partner in accordance with the terms of the Agreement.

“Beneficiary” shall have the meaning set forth in the Agreement.

“Beneficiary Agreement” shall have the meaning set forth in the Agreement.

“Breach Incident” means a confirmed ransomware attack from external sources through malware or a virus that denies, by encryption, access by MSP and the Beneficiary to a material portion of Beneficiary’s confidential information, files and/or data located on one or more of Beneficiary’s Managed Endpoints protected by the Products, and demands a ransom payment for its release or return. For clarification, where individual impacts on multiple endpoints are related to the same underlying malware, virus, threat actor, threat campaign, or series of threat campaigns, the multiple

impacts shall be considered one Breach Incident and will be limited to one claim under the MSP Warranty. Provided however, MSP may bring a claim on behalf of each unrelated Beneficiary for a Breach Incident, subject to the terms herein.

“Healthy Environment” means the Beneficiary’s Managed Endpoint environment using a current supported operating system that is free of known malware and/or viruses at the time immediately prior to the Breach Incident, and such environment is designated “green” as indicated by the account health check in Sophos Central. Notwithstanding the foregoing, a Beneficiary’s Managed Endpoint shall not cease to be a Healthy Environment if Sophos has instructed the MSP or the Beneficiary in writing to disable a feature or otherwise change a setting in Sophos Central and such guidance is current (i.e. has not been revoked) at the time of the Breach Incident.

"Product” means, as applicable, (i) Sophos Intercept X Advanced with XDR and MDR, and/or (ii) Sophos Intercept X Advanced for Server with XDR and MDR, and, in each case, with all three components fully installed, configured and enabled to the recommended settings on all of the Beneficiary’s Managed Endpoints in compliance with the MDR Service Description, the relevant Documentation and the terms and conditions of this MSP Warranty.

“Warranty Term” means the period for which a Subscription is enabled for the Beneficiary by the MSP in accordance with the Beneficiary Agreement.

“Year” means the 12 month period beginning on the start date of the Subscription enabled for the Beneficiary.

A: WARRANTY

Sophos warrants that if, during the Warranty Term, a Breach Incident occurs on a Healthy Environment protected by the Products that results in the irretrievable loss of Beneficiary data, Sophos will pay a reimbursement to MSP in an amount up to the limits specified in this MSP Warranty in respect of that Breach Incident. All claims are subject to the terms, conditions, limitations, disclaimers and exclusions of this MSP Warranty.

B: WARRANTY CONDITIONS, DISCLAIMERS & EXCLUSIONS

1. GENERAL

1.1 The MSP Warranty under this program is only available for the MSP in respect of the Beneficiary’s Managed Endpoints, and is non-transferrable and does not confer any rights to any Beneficiary of the MSP.

1.2 The MSP Warranty is only available where the MSP has enabled the Subscription for use on behalf of a Beneficiary in accordance with the Agreement.

1.3 If the MSP: (a) acquired the MDR Complete licenses for a Beneficiary, paying Sophos in advance and on a term basis and/or (b) does not provide the Subscription as a managed service to the Beneficiary pursuant to a Beneficiary Agreement and is rather acting as a reseller of the Subscription under the terms of the Sophos Reseller Agreement as stated at https://www.sophos.com/en-us/legal/partner-application-terms-and-conditions, then the Beneficiary in such case will be treated as the Customer of Sophos (as defined in the Sophos End User Terms of Use) and the applicable terms in relation to the MDR Complete warranty shall be found at the following: https://www.sophos.com/en-us/legal/mdr-complete-warranty ; and this MSP Warranty shall not apply to any such Customer.

1.4 The MSP Warranty is provided AS IS and may be modified at any time at the sole discretion of Sophos, and only the then current version of the MSP Warranty as published at: https://www.sophos.com/en-us/legal/mdr-complete-msp-warranty shall apply.

1.5 For the avoidance of doubt, the MSP cannot file a claim for a Beneficiary for a Breach Incident, if the same Beneficiary has already filed a claim with Sophos for a warranty reimbursement as provided in 1.3 above for the same Breach Incident.

1.6 This MSP Warranty is not intended to and shall not be construed to give any third party any interest or enforceable rights (including, without limitation, any third party beneficiary rights) with respect to or in connection with any agreement or provision contained herein or contemplated hereby. Only the MSP has the right to make a claim under this MSP Warranty.

1.7 THIS MSP WARRANTY MAY BE CANCELLED, SUSPENDED OR REVISED BY SOPHOS BY REASONABLE WRITTEN NOTICE AT ANY TIME AND AT SOPHOS' SOLE DISCRETION. SUCH NOTICE MAY INCLUDE A POSTING TO SOPHOS.COM OR A BANNER ON THE CENTRAL CONSOLE.

1.8 THIS MSP WARRANTY DOES NOT, AND SHALL NOT BE DEEMED TO PROVIDE A CONTRACT OF INSURANCE UNDER ANY LAWS OR REGULATIONS AND SHALL BE NULL AND VOID IN ANY COUNTRY OR JURISDICTION IN WHICH IT IS DEEMED TO BE A CONTRACT OF INSURANCE OR AN OFFERING OF INSURANCE.

2. REQUIREMENTS & CONDITIONS

The benefits of this MSP Warranty will only be available to an MSP that offers the Subscription to the relevant Beneficiary and meets all of the conditions of this Section B.2.

2.1 All Products must be correctly installed, configured and enabled on all the relevant Beneficiary's Managed Endpoints in compliance with the MDR Service Description, relevant Documentation and these terms and conditions.

2.2 MSP shall not be in default of any payments due and payable to Sophos or the distributor (as applicable). The MSP Warranty will take effect in relation to a specific Beneficiary account upon

receipt of payment to Sophos for that account.

2.3 At the time of the Breach Incident the affected Beneficiary's Managed Endpoints must:

a. have been running the currently supported release of the Product, including all updates, patches and bug fixes;

b. have a Healthy Environment;

c. be using a current supported operating system on each of the Beneficiary's Managed Endpoints from either:

(i) Microsoft Windows https://learn.microsoft.com/en-us/windows/release-health/supported-versions-windows-client and https://learn.microsoft.com/en-us/windows/release-health/windows-server-release-info, and the Product continues to support the operating system; or

(ii) Apple, in which case either the current macOS release or a prior release is used for so long as Apple continues to support and provide updates for it, and the Product continues to support the operating system;
An operating system that is under a period of extended support shall not be considered current, and a claim will not be honored under the MSP Warranty.

2.4 The MSP must not be in breach/default of any terms of the Agreement (as defined in the MDR Service Description) or of the MDR Service Description.

2.5 Throughout the Warranty Term,

a. the MSP must:

(i) not turn off or disable any functionality for the Products that permits the Beneficiary's Managed Endpoints to be scanned for malware and viruses;

(ii) allow Sophos to conduct an "on demand" scan of the Beneficiary's Managed Endpoint at Sophos' discretion to determine the health of the Beneficiary's Managed Endpoints;

(iii) provide sufficient training to its employees or agents that access the data of the Beneficiary on basic precautionary steps to be taken to avoid phishing or the inadvertent introduction of malware and viruses; and

(iv) ensure that its remote management of any endpoints and/or servers are securely managed and protected using industry best practices, employing at a minimum: multi-factor authentication (which must be enabled and enforced), and enforcing complex passwords containing alphanumeric and special characters and automatic time-outs.

b. the MSP must ensure that each Beneficiary:

(i) does not turn off or disable any functionality for the Products that permits the Beneficiary's Managed Endpoints to be scanned for malware and viruses;

(ii) routinely backs up its data in accordance with industry best practices;

(iii) provides sufficient training to its employees or agents on basic precautionary steps to be taken to avoid phishing or the inadvertent introduction of malware and viruses; and

(iv) ensures that the remote management of any endpoints and/or servers are securely managed and protected using industry best practices, employing at a minimum: multi-factor authentication (which must be enabled and enforced), and enforcing complex passwords containing alphanumeric and special characters and automatic time-outs.

2.6 MSPs that provide the Subscription services to Beneficiaries in a regulated industry (e.g., banking, energy, healthcare) must comply, to the extent required, with all laws and regulations applicable to such industry, and shall ensure that each Beneficiary comply with all laws and regulations applicable to such industry.

2.7 MSP must reasonably cooperate with Sophos in the investigation of the Breach Incident and any MSP Warranty claim, and shall ensure that each Beneficiary reasonably cooperates with MSP and/or Sophos in the investigation of the Breach Incident and any MSP Warranty claim.

3. DISCLAIMERS/LIMITATIONS

A claim made under this MSP Warranty will be denied by Sophos if any of the following applies:

3.1 A Breach Incident occurs after Sophos reports to, or otherwise notifies MSP in relation to (a) an Incident, Detection, Case or Response Action, or (b) (i) a non-Healthy Environment, (ii) gaps in the MSP's or Beneficiary's system or significant misconfigurations of the Products that could degrade real-time protection, (iii) investigations or the ability of MSP to follow up to take Response Actions, but MSP fails to remediate any identified issues promptly, as reasonably determined by Sophos, and in accordance with good security practice commensurate with the level of security threat.

3.2 MSP fails to notify Sophos of a Breach Incident by opening an MDR case/ticket via email at mdr-ops@sophos.com and/or by calling the relevant number listed at https://docs.sophos.com/support/help/en-us/active-threat/mtr/open/index.html as soon as reasonably practicable, and in any event, within 24 hours of a becoming aware of a potential breach occurring.

3.3 MSP fails to state their intent to claim under this MSP Warranty, within 5 days of a Breach Incident, by providing a written request to Sophos at breachclaims@sophos.com to commence the approval process for the claim in conformance with Section D (Filing a Claim) of this MSP Warranty.

3.4 MSP does not complete the form at www.sophos.com/claim within 15 days from the occurrence of a Breach Incident.

3.5 A review of the Account Health Check in Sophos Central shows that the relevant Beneficiary's Managed Endpoint was not a Healthy Environment at the time of the Breach Incident.

3.6 The Incident Response determined that the Breach Incident occurred because of the following:

a. either MSP or the Beneficiary failed to install bug fixes, patches and/or updates relating to any security vulnerability issued by a vendor/developer from time-to-time for any application and/or operating system running on the Beneficiary's Managed Endpoints within the timeframe for the Common Vulnerability Scoring System (CVSS) outlined below, each such timeframe beginning from the date the fix is made available:

   Critical (score 8.5+) within 7 days;
   High (score 7-8.5) within 30 days; and
   Medium and lower (score < 7.0) within 90 days.

   If a reboot of the system or application was required in connection with any of the above, the application/system will not be considered to have fulfilled this requirement unless and until completion of the applicable reboot.

b. an introduction of an active threat through an unprotected endpoint within the affected Beneficiary's network (i.e., the Breach Incident did not originate from the Beneficiary's Managed Endpoint but was introduced from another end point on the Beneficiary or the MSP network).

c. the Breach Incident occurred before the start of the Warranty Term.

d. the Breach Incident occurred because the MSP failed to identify or remediate issues where the Product was improperly installed on a Beneficiary's Managed Endpoint or was not performing in accordance with the Documentation. (MSP acknowledges that it is the MSP's responsibility to identify and remediate issues arising during installation.)

3.7 The MSP fails to provide reasonably sufficient evidence of compliance (whether by the MSP or Beneficiary) with the obligations and requirements set forth under this MSP Warranty.

3.8 MSP is requesting that a ransomware payment or reimbursement under the MSP Warranty be paid to any person or entity that: (i) would be a violation of the local laws of the country where the Breach Incident occurred; or (ii) resides in or is subject to economic sanctions administered or enforced by the U.S. Treasury Department Office of Foreign Assets Control (OFAC), including (a) any persons or entities listed on OFAC's Specially Designated Nationals and Blocked Persons (SDN) list, (b) persons or entities otherwise prohibited under relevant U.S. law, or (c) persons or entities prohibited by laws of other countries. MSP must provide to Sophos evidence, to Sophos' reasonable satisfaction, that any ransomware payment to be provided by Sophos shall not violate the above.

4. EXCLUSIONS

The following types of claims are expressly excluded from the MSP Warranty and payment reimbursement will not be made:

4.1 Any claims related to a Breach Incident occurring within a virtual desktop infrastructure (e.g. Citrix, VMware, and other virtual desktop infrastructure environments).

4.2 A claim made by an MSP where either (i) the data is *not* irretrievable (i.e., MSP or the Beneficiary can get access to back-up data and is capable of restoring the majority of the deleted or encrypted data with the back-up); or (ii) where the data was not on the Beneficiary's Managed Endpoints affected by the Breach Incident.

4.3 A claim for a Breach Incident caused by a third party product and/or service which directly or indirectly causes the malfunction or nonperformance of the Product or the Subscription.

4.4 A claim resulting from a systemic failure of third party software impacting customers on a significant, large scale basis.

4.5 A claim resulting from a systemic failure affecting the Sophos infrastructure.

4.6 A claim related to any Breach Incident that arises out of or is caused by, directly or indirectly, acts of God, including but not limited to earthquakes, hurricanes, tsunamis, natural disasters, wildfires, solar flares, solar winds, etc., acts of war or terrorism, or reasonably believed to be related to state sponsored cyberattacks, civil or military disturbances, nuclear, and interruptions, loss or malfunctions of utilities, communications, or the systemic failures of the same.

4.7 A claim related to a Breach Incident arising directly or indirectly from the intentional or willful misconduct, collusion, or the negligence of the MSP and/or the Beneficiary, either of their Affiliates, directors, officers, agents, employees, non-employee workers, agents, representatives, contractors or consultants.

4.8 A claim related to a Breach Incident arising as a result of an infection, compromise, malware, virus or other unauthorized access of asset(s) or credentials that attempts to circumvent controls in an effort to compromise an endpoint that was introduced to the MSP or Beneficiary's internal systems (which could be an unprotected endpoint within the MSP's or Beneficiary's network or a Beneficiary's Managed Endpoint) by the MSP or Beneficiary, whether intentionally or unintentionally (e.g. malware or virus testing).

4.9 Claims filed by the MSP are not in good faith or are considered non-meritorious or frivolous, as reasonably determined by Sophos.

C: LIMITS OF REIMBURSEMENT PAYMENT.

1. To initiate a claim under the MSP Warranty, the MSP must have anticipated demonstrable out of pocket expenses of at least $5,000 (US) spent in direct response to a Breach Incident affecting the Beneficiary. A separate claim may be raised by MSP for each separate and unrelated Beneficiary affected by the same Breach Incident subject to the limitations set forth herein. The

MSP may not aggregate or commingle the out of pocket expenses of separate and unrelated Beneficiaries to increase the reimbursable payment; each separate and unrelated Beneficiary must show out of pocket expenses affecting the Managed Endpoints of the specific Beneficiary.

2. Sophos will not be liable to pay more than $1,000 (US) for the lesser of: (i) each fully paid up license enabled by MSP for the Beneficiary, or (ii) each breached Managed Endpoint for the Beneficiary. For the avoidance of doubt, if MSP has purchased 25 licenses for the use by a Beneficiary, the maximum reimbursable claim is limited to $25,000.

3. Subject to the limitations set forth in Sections C.1 and C.2 above, Sophos will reimburse MSP for pre-approved actual, documented out of pocket Expenses, not to exceed $1,000,000 (US) per claim in any Year. The $1,000,000 limit shall apply separately to each separate and unrelated Beneficiary with a Subscription managed by the MSP. A subsequent claim for a Beneficiary cannot be filed by the MSP until at least 12 months have passed from a successful claim that was reimbursed by Sophos for the same Beneficiary. The foregoing restriction shall also apply to valid successful claims made by a Beneficiary treated as a Customer pursuant to Section 1.3 above, where the MSP will be precluded from filing a claim for a period of 12 months from the date of a successful claim made by a Beneficiary/Customer under Section 1.3.

4. For the purposes of C.3 above “Expenses” shall constitute, and be limited to, any of the following costs that are incurred in order to remediate a Breach Incident: (i) reasonable legal fees; (ii) expenses relating to providing notices to affected individuals; (iii) reasonable costs and expenses for public relations; (iv) fines assessed by a regulatory agency; and (v) payment of a ransom to the party causing the Breach Incident to retrieve encrypted data (subject to Section C.5 below and MSP confirming compliance with Section B.2.5 above). Expenses shall not include any value added tax (or similar taxes), any other federal, state, municipal, or other governmental taxes, duties, licenses, fees, excises, or tariffs incurred by MSP that are recoverable, creditable, or in any other way are not a cost to MSP under applicable laws by any reasonable means or endeavours of MSP.

5. A claim for a ransomware payment shall be limited to a maximum payment of $100,000 (US) in any one claim (and remains subject to any further limitation pursuant to the maximum amount payable per affected Beneficiary’s Managed Endpoint as specified in Section C.2 above).

6. If an MSP has multiple Subscriptions for one Beneficiary, the MSP is only entitled to receive reimbursement on 1 claim per separate and unrelated Beneficiary; not 1 claim per Subscription.

7. Sophos shall have no obligation to make any payments that are prohibited by applicable law.

8. The payment reimbursements provided by this MSP Warranty is MSP’s sole and exclusive remedy for any claims arising from a Breach Incident. To the maximum extent permitted by applicable law, Sophos and its Affiliates disclaim all other warranties, whether express, implied or statutory or otherwise, including but not limited to, warranties of merchantability and fitness for a particular purpose and warranties against hidden or latent defects. In no event will Sophos, its Affiliates or their respective suppliers be liable (under any theory of liability, whether in contract, statute, tort or otherwise) for any lost profits, lost business opportunities, business interruption,

lost data, data restoration, or special, incidental, consequential, or punitive damages, even if such party has been advised of the possibility of such damages or losses or such damages or losses were reasonably foreseeable; and in no event shall Sophos' liability under or arising from this MSP Warranty exceed the limits set out above.

9. IN CASE ANY OF THE LIMITS SET FORTH ABOVE ARE DETERMINED TO BE INVALID UNDER APPLICABLE LAW IN ANY COUNTRY OR JURISDICTION, THIS MSP WARRANTY SHALL BE DEEMED NULL AND VOID.

D: FILING A CLAIM

1. A claim under the MSP Warranty must first be approved in writing by Sophos, including the preapproval of qualified vendor(s) selected to remediate a Breach Incident and the costs to be paid for such services. Sophos reserves the right at its sole discretion to exclude the use of a competitor of Sophos.

2. MSP shall reasonably cooperate with Sophos in the investigation of the Breach Incident and MSP Warranty claim, and shall ensure that its Beneficiary does the same.

3. MSP will, within 72 hours of a Breach Incident, state their intent to claim under this MSP Warranty by providing a written request to Sophos at breachclaims@sophos.com to commence the approval process for the claim. MSP acknowledges that a Beneficiary shall have no right to file a claim under this MSP Warranty program, and any claims submitted by a Beneficiary shall be void.

4. Within 15 days from the Breach Incident, MSP must submit full claim details via www.sophos.com/claim. All invoices for costs incurred by MSP must be submitted to Sophos within 2 months of the Breach Incident.

E. GOVERNING LAW & DISPUTES

Only the MSP may raise a good faith dispute under this MSP Warranty, and a Beneficiary is strictly prohibited from raising a dispute under this MSP Warranty. All disputes arising from or in connection with this MSP Warranty shall be governed by the laws of England and Wales.

Any dispute arising out of or in connection with this MSP Warranty, including any question regarding its existence, validity or termination, shall be referred to and finally resolved by arbitration under the London Court of International Arbitration (LCIA) Rules, which Rules are deemed to be incorporated by reference into this clause.

The seat, or legal place, of arbitration shall be London, England. The language to be used in the arbitral proceedings shall be English.