Ransomware Warranty

September 13, 2021

SENTINELONE RANSOMWARE WARRANTY

This SentinelOne Ransomware Warranty ("**Warranty Agreement**") describes the terms and conditions for the provision of a Ransomware Warranty ("**Warranty**") granted from SentinelOne, Inc. ("**SentinelOne**") to the SentinelOne customer who subscribes to its Control or Complete SKU of SentinelOne's malware protection solutions ("**Company**" and "**Solutions**," respectively) under the SentinelOne Terms of Service ("**Terms**"). This Warranty Agreement governs the Warranty provided that such Warranty is stated in a quote or purchase order among SentinelOne and the Company, or an approved SentinelOne partner and the Company, in each case where approved by SentinelOne (collectively, "**PO**"). This Warranty shall be effective as of the date the PO is executed ("**Effective Date**") and shall remain in effect for the term of the Warranty stated in such PO and so long as the Company subscribes to the Solutions in accordance with the Terms and uses the Solutions in compliance with the terms of this Warranty Agreement (including, without limitation, the Solutions configuration ("**Warranty Term**"). As the Company's authorized representative, you represent that you are authorized by the Company to accept the Warranty under this Warranty Agreement as part of the Company's subscription to the Solutions. Capitalized terms shall have the meaning assigned to such terms where defined in this Warranty Agreement, and capital terms used but not defined in this Warranty Agreement shall have the meaning assigned to such terms in the Terms.

Subject to the terms and conditions described herein and the Terms, the parties to agree as follows:

Specific Ransomware Warranty

1. **Warranty**. During the Warranty Term, so long as the Company also subscribes to the Solutions in compliance with the Terms, the Company's Endpoints will be protected by the Solutions which will screen for any Ransomware. The Warranty granted herein shall apply to all such Endpoints provided that:

- (a) The Solutions are deployed in the Endpoints in accordance with the Documentation and such Endpoints are currently active and properly configured;
- (b) Only Files that are on Endpoints are covered under this Warranty;
- (c) All Endpoints of the Company have the following required configurations:
    - (i) Solutions:
        - Policy mode options are set to Threats: Protect and Suspicious: Protect.
        - All Engines are set to ON (except for Application Control).
        - Cloud Connectivity is not disabled.
        - Anti-Tamper is turned ON
        - Snapshots are turned ON
        - Scan New Agents is turned ON
        - The latest General Availability (GA) version (or GA with a critical security Service Pack (SP), if issued) or the GA (or GA with a critical SP, if issued) version immediately preceding such latest GA version, of the SentinelOne Windows Endpoint Agent (as specified in the SentinelOne Knowledge Base "Latest Information" article) is deployed prior to the time of Ransomware infection.
        - There are no Pending Actions (such as Reboot) listed on any covered Endpoint.
        - A supported version of the Management Console is deployed.
        - Exclusions specified in the SentinelOne Knowledge Base "Not Recommended Exclusions" article, are not deployed in the Management Console or Agent.
        - Binary Vault is enabled (where available)
        - 2 Factor Authentication is enabled=
    - (ii) Operating system:
        - The Warranty applies to Standard (not Legacy) Windows Agents, and on supported versions of Microsoft Windows (as specified in the SentinelOne Knowledge Base "System Requirements" article).
        - Each endpoint is malware-free prior to SentinelOne Windows Agent installation.
        - OS is fully updated and patched for security updates on each covered Endpoint, and all vulnerable applications are updated to latest releases.
        - VSS (Volume Shadow Copy Service) is enabled and functioning on all Windows endpoints. VSS Disk Space Usage allocation must be configured with at least 10% on all disks.
- (d) The Company adheres to the following manual actions post infection (i.e. upon discovery of Ransomware):
    - immediately (no more than an hour upon discovery) adds the specific Ransomware threat to blacklist;
    - in case the Ransomware was not blocked but only detected – takes a remediation and rollback action within 1 hour of infection/discovery of the Ransomware; and
    - notifies SentinelOne of the Ransomware discovery within 24 hours at warranty@sentinelone.com.

    this Section 1(d) shall not apply if the Company is subscribed to the Vigilance Response service during the Warranty Term.

2. **Scope of the Warranty**. Subject to the terms of this Warranty Agreement, including the specific requirements of Section 1 above, in case of a successful ransomware attack on Company Endpoints covered by the Warranty, as shown in SentinelOne's logs and other records, SentinelOne will pay as sole and exclusive remedy to the Company actual damages caused by such attack, capped at $1,000 USD per Endpoint affected by a Breach, and further capped at $1,000,000 USD for every consecutive 12 months in which Company subscribes to the Solutions with respect to the affected Endpoint.

3. **Condition Precedent to Warranty Payment**. SentinelOne shall only provide the remedy for the Breach of the Warranty as described above if (i) the Ransomware attack has occurred, is discovered by the Company and reported to SentinelOne during the Warranty Term and Company's subscription to the Solutions under the Terms; (ii) Company's Endpoints and the Solutions are configured in accordance with the Documentation and Section 1 above; (iii) the Company demands in writing to recover for damages caused by the Breach; (iv) sufficient evidence is provided by the Company supporting the Ransom demand amount for each Ransomware infection covered by this Warranty; (v) sufficient evidence and assurances are provided by the Company that no Warranty payment would be used by the Company to make a payment to any person or entity subject to economic sanctions administered or enforced by the U.S. Treasury Department Office of Foreign Assets Control (OFAC), including any such person or entity listed on OFAC's the Specially Designated Nationals and Blocked Persons (SDN) list or otherwise prohibited under relevant U.S. law.

4. **Exclusions**: The Warranty shall not apply to a breach caused primarily by (i) any deployment, configuration and/or use of the Solutions (or a portion thereof), for any or no reason, in a manner inconsistent with the Documentation or the requirements of Section 1 herein; (ii) Company's negligence or misconduct; or (iii) other products and/or services which directly or indirectly cause the malfunction or non-performance of the Solutions with respect to the subject Ransomware.

5. **Sole and Exclusive Remedy**. The aforementioned remedy for the Breach shall be the Company's sole and exclusive remedy and the entire liability of SentinelOne for any Breach of the Warranty.

6. **Definitions**. The capitalized terms below shall have the following meaning:

- (a) "**Breach**" means the unauthorized access to at least one Company Endpoint in the form of Ransomware which has caused material harm to the Company, whereby "material harm" must include at least one of the following: (i) the unauthorized acquisition of unencrypted digital data that compromises the security, confidentiality, or integrity of personal information or confidential information maintained by the Company; (ii) public disclosure of personal information or confidential information maintained by the Company; or (iii) the compromise of at least one Company Endpoint resulting the blocking of access to such Endpoint.
- (b) "**Ransomware**" means a malware software program that infects Company's systems from external sources (i.e., in the wild), which installs, persists and encrypts a large portion of files at the operating system level, and continuing to demand payment (the "**Ransom**") in order to decrypt the encrypted files. For clarification, Ransomware does not include any malware introduced by the Company or any third party to Company's internal systems, whether intentionally (i.e., malware testing) or through a breach in the system's security.
- (c) "**Endpoints**" shall mean any computing device with a Microsoft Windows operating system, that has the Solutions installed per the Documentation under valid Terms among SentinelOne and the Company.

7. **Other Terms and Conditions**. Any other terms and conditions of the Terms shall be unaffected by this Warranty Agreement, except as expressly stated in the Terms. In case of any conflict between the terms of this Warranty Agreement and the terms and conditions within the Terms relating to the Warranty, the terms and conditions within this Warranty Agreement shall prevail.

8. **Miscellaneous**. This Warranty Agreement represents the complete agreement between the parties concerning the Warranty granted hereunder and supersedes any and all prior agreements or representations between the parties. SentinelOne may revise the terms of this Warranty Agreement from time to time in its reasonable discretion, provided that such revisions shall not reduce or eliminate the monetary remedy described in Section 2 herein. To the extent that SentinelOne pays to the Company under the Warranty, Company agrees that SentinelOne shall acquire a subrogation right to assert a claim against the hacker who delivered the Ransomware to Company and caused damages for which SentinelOne incurred Warranty costs, and Company further agrees to assist SentinelOne should it decide to assert a claim against such hacker. If any provision of this Warranty Agreement is held to be unenforceable for any reason, such provision shall be reformed only to the extent necessary to make it enforceable. This Warranty Agreement is governed by and construed in accordance with the substantive laws of California, irrespective of its choice of law principles, and the competent courts in California shall have sole and exclusive jurisdiction over every dispute arising from, or in connection with this Warranty Agreement.

(Current) 2021-09-13 15:21:30