VMware vDefend Network Detection and Response Specific Program Documentation ("SPD")

The Broadcom software program(s) ("Broadcom Software" or "Software") listed below is provided under the following terms and conditions in addition to any terms and conditions referenced on the Broadcom quote, order form, statement of work, or other mutually agreed ordering document (each a "Transaction Document") under the applicable end user agreement or governing contract (collectively, the "Agreement") entered into by Customer and the Broadcom entity ("Broadcom") through which Customer obtained a license for the Broadcom Software. These terms shall be effective from the effective date of such Transaction Document. Capitalized terms have the meanings ascribed to them herein, or, otherwise, in the Agreement (including the VMware Licensing Glossary).

Program Name: ***VMware vDefend Network Detection and Response***

1. DEFINITIONS.

All terms defined in the VMware Licensing Glossary located at https://www.broadcom.com/company/legal/licensing apply to this SPD unless specified herein.

"NDR Sensor" means the appliance software that is deployed as physical (bare-metal) or virtual form factor, on customer provided hardware. The software is deployed where it can access network data, and implements a full suite of detection technologies.

"Sensor Core" means any Core of a host where a NDR Sensor is deployed that collects data to be processed by this Broadcom Software.

2. USE RIGHTS AND LIMITATIONS.

Customer may use the Broadcom Software to monitor up to the number of Sensor Cores for which Customer has paid the applicable license fees.
Customer license includes a Cloud Service feature for user interface and analysis and storage of network traffic and artifacts for the same duration as Customer's Subscription term.

Threat Intelligence Data Collection. The Software may collect data relating to malicious or potentially malicious code, attacks, and activities on Customer's network ("**Threat Intelligence Data**"). Threat Intelligence Data is collected by VMware for analysis and inclusion in a threat intelligence feed. Prior to inclusion in any threat intelligence feed, Threat Intelligence Data will be: (i) reduced to a unique file hash or to queries or general behavioral descriptions that can be used to identify the same or similar malicious or potentially malicious code in Customer's and other customers' systems; and/or (ii) anonymized and made un-attributable to any particular customer or individual. VMware may distribute Threat Intelligence Data at its discretion as part of its threat intelligence data feed or in published reports or research. By using a Threat Intelligence Data feed, Customer is deemed to have agreed that Threat Intelligence Data is not Customer Data, and VMware may retain, use, copy, modify, distribute, and display the Threat Intelligence Data for its business purposes, including without limitation for developing, enhancing, and supporting products and services, and for use in its threat intelligence feed or in published reports or research. The information provided via any threat intelligence feed is provided on an "AS-IS" and "AS-AVAILABLE" basis only.

The Software is licensed as Subscription Software. Customer may use the Software and Support solely during the Subscription term. Customer must pay for all the Software Customer use .

At the end of the Subscription term, Customer may have the option to renew the Subscription licenses. If Customer does not renew, the Subscription licenses shall expire at the end of the Subscription term. Upon expiration or termination of Customer's licenses to the Software, Customer must cease use of the Software,Documentation and Support and certify cessation of use to VMware. VMware may, at its discretion, retire Software and/or Support from time to time .

3. THIRD PARTY INFORMATION AND TERMS.

Any required third-party software license terms are incorporated by this reference and are set forth in online documentation at techdocs.broadcom.com or legaldocs.broadcom.com.


BROADCOM®