THIRD-PARTY SECURITY TERMS

These Third-Party Security Terms are part of, and subject to the terms of, any Vendor ordering document and/or licensing agreement that that references these terms (the "Agreement"). Capitalized terms used but not defined in these terms will have the meaning assigned to them in the Agreement.

1.   Third-Party Security Tools are limited to the following third-party end point detection, response and vulnerability scanning tools. Vendor will not connect the Vendor open virtual appliance ("OVA") with third-party tools not listed below.

Third-Party Provider	Tool	Component approved for installation on OVA
CrowdStrike Inc.	CrowdStrike Falcon Insight XDR	CrowdStrike Falcon Sensor
Qualys, Inc.	Qualys	Qualys cloud agent daemon
Splunk Inc.	Splunk Enterprise	Splunk Universal Forwarder
Rapid7 LLC	Rapid7 InsightIDR; InsightVM; InsightOps	Rapid7 Insight Agent
Tenable, Inc.	Tenable Vulnerability Management	Tenable Nessus Agent

2.   If Customer identifies any incident through a Third-Party Security Tool related to the OVA which Customer believes requires further action, Customer will immediately notify Vendor by submitting a support ticket prior to taking any such action.

3.   Customer agrees that (a) Third-Party Security Tools are not managed by Vendor and Vendor shall have no liability for connectivity if any Third-Party Security Tool is changed or discontinued by the respective third party; and (b) Vendor does not support, license, control, endorse or otherwise make any representations or warranties regarding any Third-Party Security Tool.

4.   Customer agrees that it is solely responsible and liable for all protection and use of Customer's access for the OVA (as such may be updated by Vendor in its sole discretion) and will not use its access to the OVA for any purpose other than end point detection, response and vulnerability scanning in accordance with Customer's established industry-standard security practices. Customer acknowledges and agrees that Third-Party Security Tools are non-standard configurations for the OVA, constitute "Customer Systems" for purposes of the Agreement, and that accordingly Customer shall be solely responsible and liable for (a) security monitoring of the OVA; and (b) any issue, incident, interruption, performance degradation, or other problem (including unavailability of Vendor's software or services) arising out of or in connection with the deployment thereof.

Last Updated: November 12, 2025