vmware ®

Carbon Black
App Control

Count
Weighted Drift

Supported Integrations

Product Version: 8.5.0

Document Date: September, 2020

Contents

Overview

This document describes the supported integrations for the VMware Carbon Black App Control. For hardware and operating requirements, please refer to *VMware Carbon Black App Control Operating Environment Requirements* document.

SIEM

Security Information and Event Management (SIEM) [1]			
Publisher	**Product**	**Supported Versions**	**Additional Notes**
HP	ArcSight	6.2x, 6.3x	
IBM	QRadar	V7.3.3 R-1, V7.4.0 R	

Note[1]: App Control can output in syslog format. Therefore, applications that can ingest syslog format should work.

Enterprise Security Appliances

Enterprise Security Appliances			
Publisher	**Product**	**Supported Versions**	**Additional Notes**
Palo Alto Networks	PA, VM All Series, WildFire Cloud, WF-500	PAN OS 8.0, 8.1, 9.0, 9.1	
Check Point	Thread Emulator Cloud Threat Emulator Blade	Threat Prevention API 1.0	

Big Data Analysis

Big Data Analysis			
Publisher	**Product**	**Supported Version**	**Additional Notes**
Splunk	Splunk Enterprise	5.0, 6.0, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 7.0, 7.1, 7.2, 7.3	See Note[1].

Note[1]: The Splunk App for App Control is published under the Creative Commons license (https://creativecommons.org/licenses/by/4.0/)
There are no restrictions on modifying Carbon Black Splunk App code, as long as:
1. Attribution is given to VMware Carbon Black, and…
2. For any code that is published based on the VMware Carbon Black Splunk App code, no additional restrictions are added.