Carbon Black Cloud Endpoint Standard - FAQ

© VMware LLC.

Table of contents

vmware by Broadcom © VMware LLC.

Carbon Black Cloud Endpoint Standard - FAQ

Overview

The VMware Carbon Black Cloud Endpoint Standard Frequently Asked Questions (FAQs) document provides answers to some of the most popular Endpoint Standard questions. We will continue to grow this list of FAQs so check back regularly for updates.

Endpoint Standard offers Next-Generation Antivirus and Behavioral EDR. Protect your organization and customer data with an easy-to-manage, cloud-native endpoint protection platform (EPP) that combines prevention and automated detection to defend your organization from today's advanced cyber-attacks. Endpoint Standard helps you stop most attacks. Most breaches do not use malware. Streaming prevention goes beyond machine learning AV to stop all types of attacks before they compromise your system. It also helps you see every threat.
If you are new to Endpoint Standard or if you want an overview of the features, components, see What Is Carbon Black Cloud Endpoint Standard?

Want to learn more about Endpoint Standard? see our Endpoint Standard Activity Path!

Audience

This Endpoint Standard FAQ document is intended for existing or prospective Security administrators.

© VMware LLC.

Operations

What is a Supported Endpoint?

Endpoint Standard is supported on endpoints (desktops, laptops, servers, VMs) with a supported OS and a full OS.

What Operating Systems are Supported?

Endpoint Standard is supported on Windows, MacOS, and Linux operating systems. Full Breakdown of OS version support can be found
here: https://community.carbonblack.com/t5/Documentation-Downloads/Carbon-Black-Cloud-Sensor-Support/ta-p/66274

What are the Utilization Metrics for the Sensor?

Endpoint Standard minimizes environmental impact. The solution is not full system scan-based; Carbon Black analyzes events as they occur in real-time. Because of this methodology, the average agent utilization is under 1% CPU.

Does Carbon Black Integrate with SIEM tools?

Yes. Carbon Black Endpoint Standard can forward alert data to SIEMs that accept standard Syslog data.

What are the supported Two-Factor Authentication apps for Carbon Black Cloud?

The Carbon Black Cloud Platform does support Multi-Factor Authentication via:

- Google Authenticator
- Duo Security.

SAML configuration is also supported.

Ability to handle False Positives

With VMware Carbon Black we provide customers with the context and transparency needed to quickly resolve true positives, while aiding with recommendations and flexible options to resolve false positives even prior to a block occurring. All of these factors instill our customers with the operational confidence needed to migrate to Carbon Black Cloud.

© VMware LLC.

Prevention

Is the Sensor able to be Protected from Uninstallation?

Within sensor policies, an optional setting is 'code required for uninstall'. The uninstall code is only visible to administrators within the Carbon Black console. This prevents even users with administrative credentials from disabling the Carbon Black sensor.

How does Endpoint Standard Prevent Attacks?

Carbon Black Endpoint Standard provides multiple layers of prevention to prevent/detect a variety of attacks such as known malware, non-malware, and fileless.

The first prevention layer, signature-based prevention, detects and prevents known bad signatures. Machine learning (ML) is layered on top of this to prevent and detect signature variations seen in malware variants/polymorphic attacks. The final layer of prevention leverages behavioral analytics; Endpoint Standard applies prevention by looking at the behaviors that applications exhibit. Behavioral-based rules can be specified to apply prevention to even trusted tools if they are being used maliciously.

How does Endpoint Standard Prevent Against Ransomware?

Endpoint Standard has robust ransomware prevention capabilities. Using behavioral analytics, we can detect and prevent behaviors associated with ransomware. Those behaviors include detecting/preventing access of the main boot record, modification of volume shadow copies, and the encryption of data. Additionally, alongside the Carbon Black agent we deploy canary/decoy files to track and stop processes attempting to encrypt, modify or delete our files.

Does Endpoint Standard Support Device Control?

Yes. Carbon Black Endpoint Standard supports the ability to block read, write, and execution of unapproved USB devices.

Can Carbon Black identify malware pre-existing on the system?

Pre-existing malware threats can be detected on systems – even before they are run.

Endpoint Standard supports proactive background scan to identify, and quarantine malicious pre-existing files to ensure you are operating in a clean environment. Many NGAV solutions on the market today wait until the malicious file executes before being able to classify the file, this can lead to unnecessary risk on the organization.

Does Endpoint Standard Require Full Scans?

No. Carbon Black Endpoint Standard performs a low-resource consumption one-time scan on installation to take inventory and detect pre-existing malicious items. After this one-time scan Endpoint Standard looks at events as they occur in real-time.

Does Endpoint Standard offer the ability to identify false positives prior to enforcement?

Yes. Carbon Black gives capabilities to understand how changes to your policies will affect your environment. Rules can be back tested to see events related to the rule within the past 30 days – allowing for confidence in determining the effect of a new rule or change.

Does Endpoint Standard make use of signature-based protection?

Endpoint Standard can utilize traditional, signature-based prevention to block known malware, suspect malware, and potentially unwanted programs. Traditional signature prevention is useful for stopping commodity malware pre-execution, allowing Endpoint Standard to focus resources on new, advanced threats that are unknown.

© VMware LLC.

Detection

How Can Alerts be Investigated?

Alerts can be viewed in a process tree visualization. Alert triage shows events that occurred during an attack in an easy-to-understand format. Click into individual events for additional process information and take action all from a single page.

Does Carbon Black give Information on Non-Alert Events?

Yes. Benign events can be searched across in a console with intuitive fuzzy search and filtering capabilities. Benign events are stored for 30 days on the Carbon Black backend.

© VMware LLC.

Remediation

Does Carbon Black Endpoint Standard Provide Remote CLI?

Yes. Live Response can be used to remotely shell w/a command-line interface to any endpoint with a sensor deployed. Live Response is proprietary to Carbon Black and provides a variety of pre-built commands for remediation along with the ability to use commands to execute background processes such as PowerShell commands or scripts, Mac terminal commands, etc. Remote command line activity is tracked within the audit log

Is Remote Quarantined Supported?

Yes. Endpoint(s) can be quarantined from the rest of the network. A tunnel is kept open only to the Carbon Black Cloud backend so that administrators can retain visibility and take additional response actions within the console.

Ability to Detect and Rollback Ransonmware

Yes. Ransomware is pervasive, and as defenders, it is VMware's responsibility to adapt and provide security that is future-ready. So in the case of rollback providing not only the ability to restore to a particular shadow copy, it is also providing disaster recovery tools to ensure business operations can resume as quickly as possible.

© VMware LLC.

General

Does Endpoint Standard support PCI DSS Compliance Malware Requirement 5?

VMware Carbon Black Cloud Endpoint Standard is certified to replace antivirus in meeting PCI DSS requirement 5 for Windows, Mac and Linux systems.

Does Carbon Black support USB Device Control?

Carbon Black offers device control for USB storage devices connected to Windows & Mac endpoints. Device control is available to Endpoint Standard customers free of additional charge.

Has Carbon Black participated in any recent 3rd party testing?

In recent AV-Test results, the VMware Carbon Black Cloud (Endpoint Standard) scored a perfect 6/6 in preventing attacks, and in AV-Comparatives testing, we scored a Prevention rating of 99.8%, with only 1 false positive (compared to CrowdStrike's 97% rating and 8 false positives). You can find more information on AV-Test here and AV-Comparatives here.

In the latest MITRE Engenuity ATT&CK, VMware Carbon Black Cloud delivered robust telemetry coverage with correlated, high-fidelity alerts at each and every step of the detection test, ensuring complete visibility into any similar real-world threat. This year, VMware Carbon Black also pioneered the use of network detection and response (NDR) via NSX Advanced Threat Prevention, together with VMware Carbon Black Cloud, to correlate detected threats across endpoint and network telemetry.

Does Carbon Black Offer a Managed Service?

Yes. Carbon Black offers a light managed service. This service provides managed alert monitoring and triage solution. We have a team dedicated to watching your environment. They act as additional eyes to validate high-level alerts, analyze them, and provide recommendations to you and your team. When a high-level alert occurs in your environment the Managed Detection team analyzes, confirms it is not a false positive and provides insight. For fully managed services Carbon Black partners with leading managed service providers.

© VMware LLC.

Summary and Additional Resources

Conclusion

This document provided answers to the most popular Endpoint Standard FAQs.

Additional Resources

For more information about Endpoint Standard, explore the Endpoint Standard Activity Path. The activity path provides step-by-step guidance to help you increase your understanding of the Carbon Black Endpoint Standard, including articles, videos, and labs.

You can also see the VMware Carbon Black Cloud Endpoint Standard Overview which provides a basic overview, architecture along with a demo.

© VMware LLC.

© VMware LLC.

Copyright © 2005-2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.