Carbon Black Enterprise EDR - Technical Overview

Table of contents

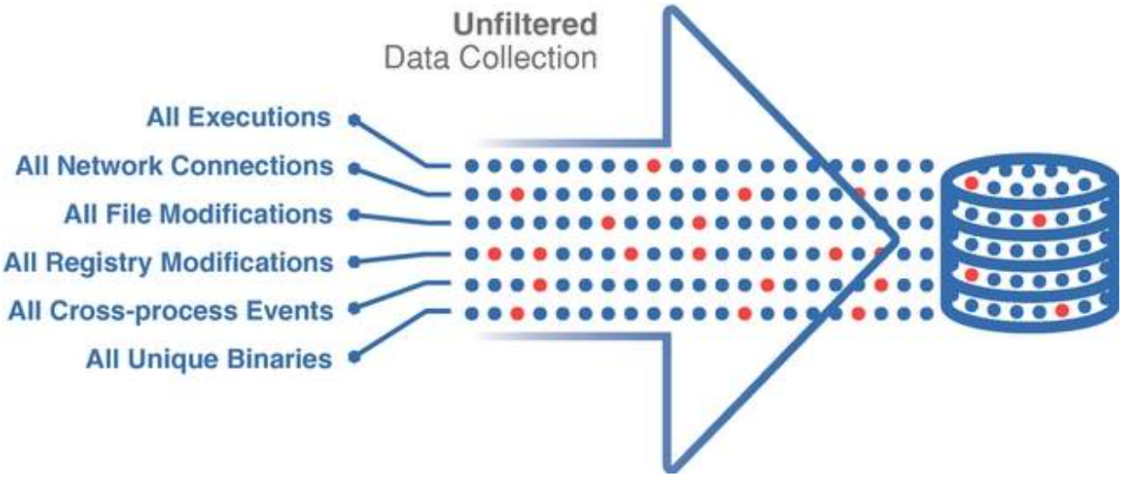
Carbon Black Enterprise EDR - Technical Overview

What is Carbon Black Enterprise EDR?

VMware Carbon Black Enterprise EDR is an advanced threat hunting and incident response solution delivering continuous visibility for top security operations centers (SOCs) and incident response (IR) teams. Enterprise EDR is delivered through the VMware Carbon Black Cloud, a next-generation endpoint protection platform that consolidates security in the cloud using a single sensor, console and dataset.

Enterprise EDR continuously collects comprehensive data giving you all the information you need to proactively hunt threats, uncover suspicious behavior, disrupt attacks in progress, repair damage quickly, manage vulnerability and address gaps in defenses. It allows you to search through raw unfiltered endpoint data by using a powerful query language, even if the endpoint is offline.

You can select third-party threat reports and build your custom watchlists with those, or you can create your own threat reports based on queries you create on the investigate page. Once enabled Enterprise EDR can also collect every unique binary that executes in your environment in the VMware Carbon Black Cloud's unified binary store, from there you can analyze binary metadata or download a binary for reverse engineering and detonation.



How does Enterprise EDR Work?

Threat Hunting and Incident Response

Threat hunting is the proactive technique that’s focused on the pursuit of attacks and the evidence that attackers leave behind

when they're conducting reconnaissance, attacking with malware, or exfiltrating sensitive data. Instead of just hoping that technology flags and alerts you to the suspected activity, you apply human analytical capacity and understanding about environment context to more quickly determine when unauthorized activity occurs. This process allows attacks to be discovered earlier with the goal of stopping them before intruders are able to carry out their attack objectives.

Threat hunting is a very important activity in securing modern networks. While we want it to be as automated as possible, it requires a degree of human analysis by cybersecurity professionals. Fortunately, VMware Carbon Black Cloud simplifies and enriches the data it shows and alerts on so that even individuals with little to no formal training in threat hunting can understand what is occurring on a system when they see it in their VMware Carbon Black Enterprise EDR dashboard.

The key difference between threat hunting and incident response is that threat hunting is proactive, whereas the incident response is reactive. Often times great incident responders make legendary threat hunters because their experience helps them to accurately determine how an attacker will behave and what they might do next. This guide will explore how VMware's Enterprise EDR solution can enable threat hunting and incident response, and, on a basic level, how to leverage Carbon Black Enterprise EDR and Carbon Black Audit & Remediation to do both.

Carbon Black Threat Hunting is an advanced threat hunting and incident response solution delivering holistic visibility for top security operations centers (SOCs) and incident response (IR) teams. Carbon Black Threat Hunter is delivered through the Carbon Predictive Security Cloud (PSC), a next-generation endpoint protection platform that consolidates security in the cloud using a single agent, console and dataset. By leveraging the unfiltered data collected by the PSC, Carbon Black Threat Hunter always provides immediate access to the most complete picture of an attack, reducing lengthy investigations from days to minutes. This empowers teams to proactively hunt for threats, uncover suspicious behavior, disrupt active attacks, and address gaps in defenses before attackers can. Along with unfiltered visibility, Carbon Black Threat Hunter gives you the power to respond and remediate in real-time, stopping active attacks and repairing the damage quickly.

To begin using Enterprise EDR, learn more about watchlists, reports, and IOCs
Watchlists provide custom detection that continuously monitors your environment for potential threats and suspicious activity. Watchlists detect and notify you about a report's IOCs. Enterprise EDR offers pre-built watchlists, curated by Carbon Black and other threat intelligence specialists. This includes the ability to create, tune, and track your own custom-built watchlists, reports, and IOCs.

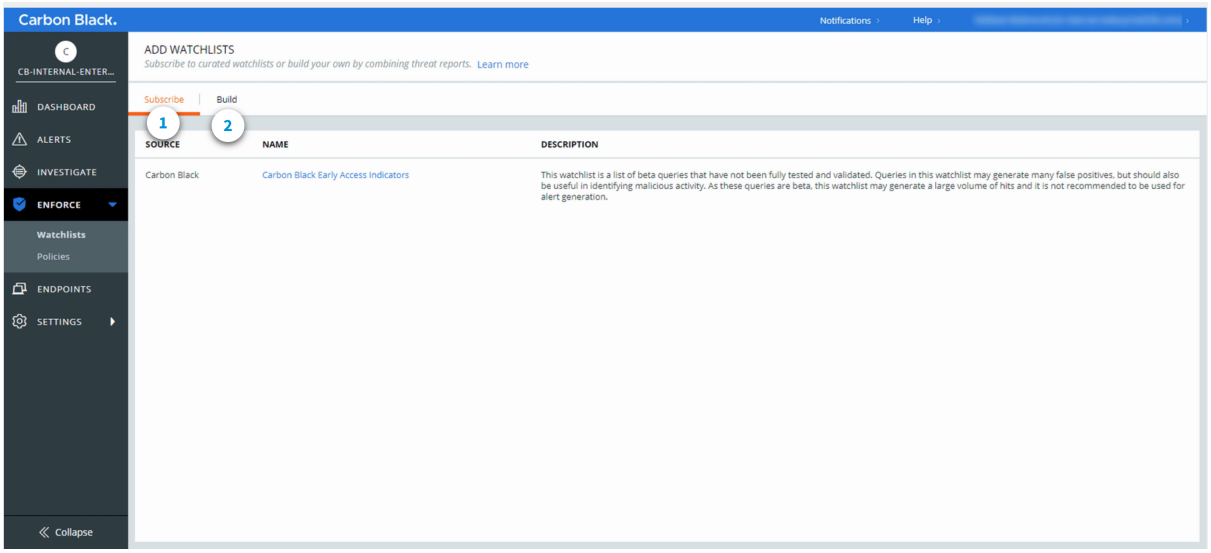
Watchlists

Watchlists provide custom detection that continuously monitors your environment for potential threats and suspicious activity. When an indicator of compromise or IOC is detected in your environment, Enterprise EDR watchlists can mark the process with a hit, can alert and can notify.

Watchlists are comprised of reports and reports are used to organize indicators of compromise like queries, hashes, IPs and domains around a type of event. As your organization's threat landscape or your response to it evolve you can continue to tune and adjust your watchlists.

There are two types of watchlists you can utilize.

1. **Subscribe**: Subscribe to watchlists curated by VMware Carbon Black and other threat intelligence specialists by clicking add watchlists and selecting one or more curated watchlists from the subscribe tab.
2. **Build**: You can build your own watchlist by combining reports and tracking the indicators of compromise that matter most to you.



Understanding Watchlist Types

Learn more about the two types of available watchlists:

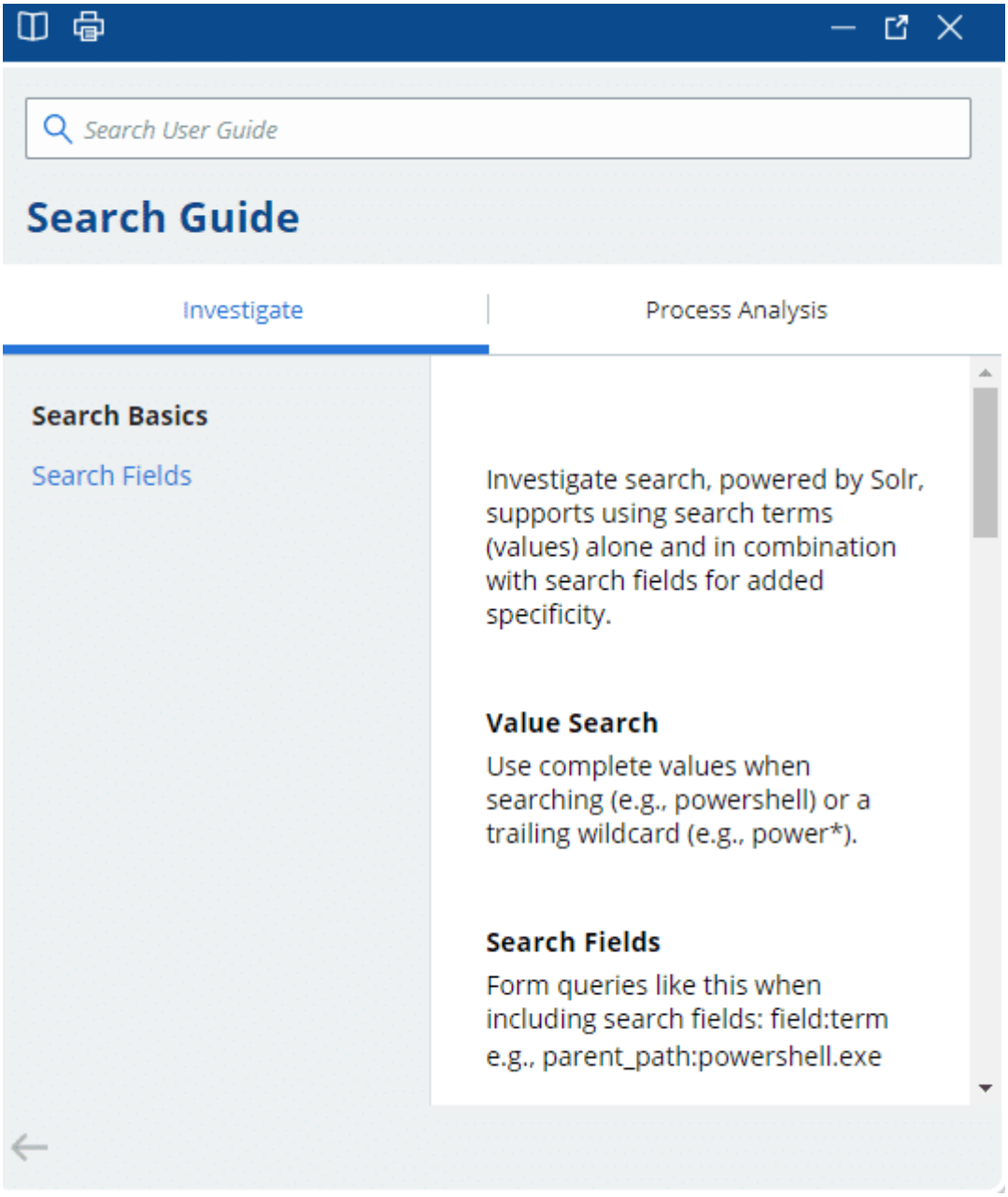
Curated watchlists	Custom watchlists
Subscribe to watchlists that are curated by Carbon Black and other providers.	Build your own watchlists by combining threat reports from multiple sources.
Subscribe to watchlists that are curated by Carbon Black and other providers.	Integrate your own threat intelligence by including queries from the Investigate page.
Disable/Enable reports or IOCs within a watchlist.	Disable/Enable reports or IOCs within a watchlist.

Enterprise EDR Search

With Enterprise EDR you can search through comprehensive data from your endpoints.

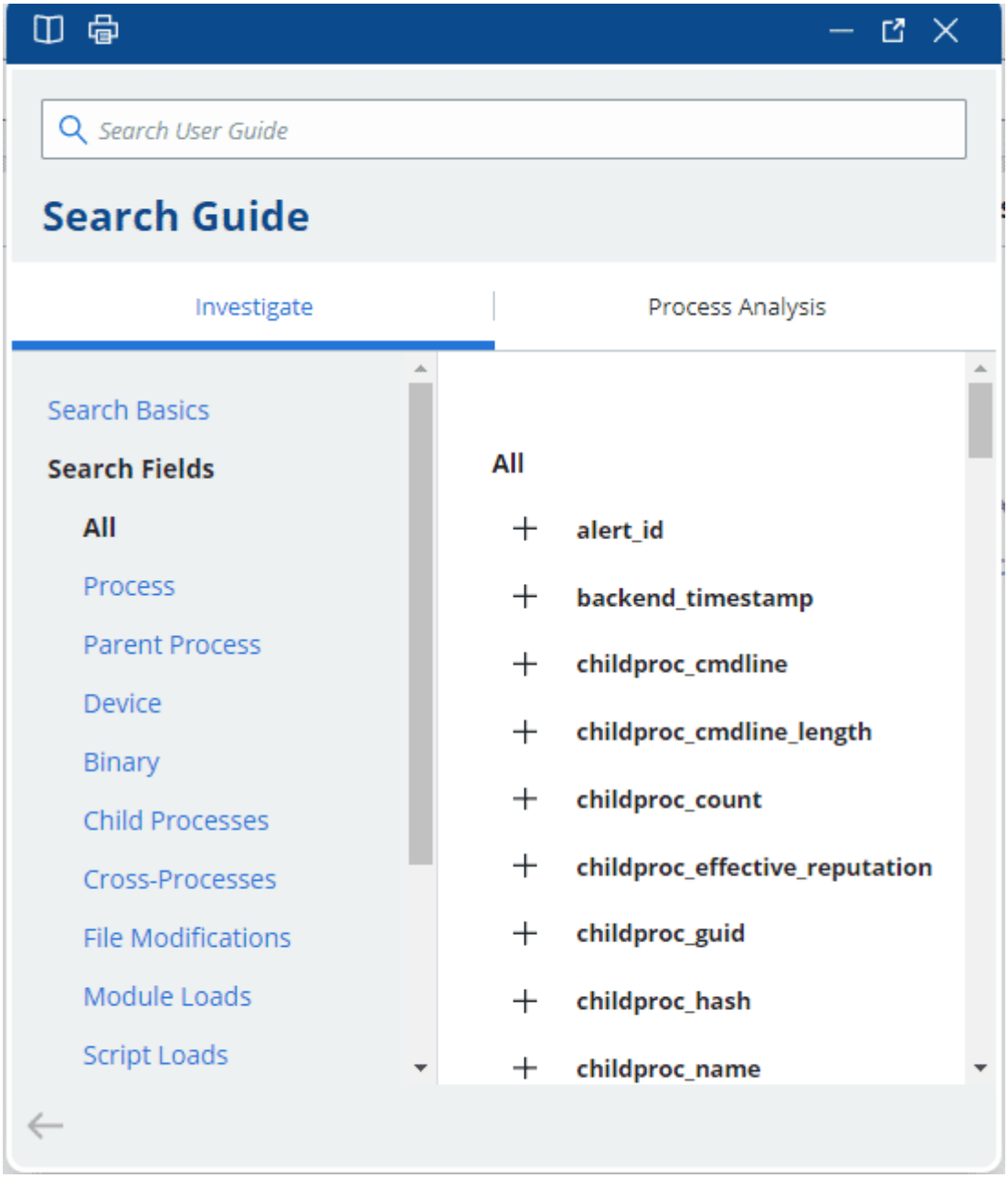
1. You can navigate to the investigate page and enter search terms in the search bar. Enterprise EDR uses the “Solr Query” Language for searching and requires adherence to the “Solr lucene” query parser syntax.
2. Enterprise EDR provides a search guide, filters, and contextual help to jump-start your search inquiries.
3. Use the search guide to access search basics and search fields.

Search basics give you information about searches such as syntax, how wildcards function, and operators.



Search Fields

Search fields provide the list of attributes a process can or will have along with a definition and example of each.



What is the difference between Endpoint Standard and Endpoint Enterprise?

VMware lets you choose the endpoint protection capabilities that are right for your team. With the continuously evolving threat landscape, settling for a checkbox on security is laying out a welcome mat for cyber-attacks. Whether you're looking to replace antiquated malware prevention or want to empower a fully automated security operations process, VMware Carbon Black Cloud meets your needs from the same console and agent.

Endpoint Standard	Endpoint Advanced	Endpoint Enterprise
Replace legacy antivirus and access the context you need to identify fileless attacks before they move laterally to critical assets. •Endpoint Standard - Next-Gen AV + Behavioral EDR •Managed Detection (Optional) - Managed Alert Monitoring and Triage	Assess the state of your endpoints, remediate any vulnerabilities and other risks from the same agent and console preventing attacks. •Endpoint Standard - Next-Gen AV + Behavioral EDR •Vulnerability Management - Risk-prioritized Vulnerability Assessment •Audit and Remediation - Real-Time Device Assessment and Remediation •Managed Detection (Optional) - Managed Alert Monitoring and Triage	Capture all endpoint events, add customized detections and third-party threat intelligence from the same platform preventing and auditing endpoints. •Endpoint Standard - Next-Gen AV + Behavioral EDR •Vulnerability Management - Risk-prioritized Vulnerability Assessment •Audit and Remediation - Real-Time Device Assessment and Remediation •Enterprise EDR - Threat Hunting and Incident Response •Managed Detection (Optional) - Managed Alert Monitoring and Triage

What are the key benefits of Enterprise EDR?

Continuous Visibility

Investigations that typically take days or weeks can be completed in just minutes. VMware Carbon Black Cloud Enterprise EDR collects and visualizes comprehensive information about endpoint events, giving security professionals unparalleled visibility into their environments.

Scale the Hunt

Never hunt the same threat twice. VMware Carbon Black Cloud Enterprise EDR combines custom and cloud-delivered threat intel, automated watchlists and integrations with the rest of your security stack to efficiently scale your hunt across even the largest of enterprises.

Respond Immediately

The days of constantly reimaging are over. An attacker can compromise your environnment in an hour or less. VMware Carbon Black Cloud Enterprise EDR gives you the power to respond and remediate in real time from anywhere in the world. We make it easy to quickly contain threats and repair the damage to keep your business going.

What are the core capabilities of Enterprise EDR?

Complete Endpoint Protection Platform

Built on the VMware Carbon Black Cloud, Enterprise EDR provides advanced threat hunting and incident response functionality from the same agent and console as our NGAV, EDR, and real-time query solutions, allowing your team to consolidate multiple point products with a converged platform.

Continuous & Centralized Recording

Centralized access to continuously collected data means that security professionals have all the information they need to hunt threats in real-time as well as conduct in-depth investigations after a breach has occurred.

Attack Chain Visualization & Search

Enterprise EDR provides intuitive attack chain visualization to make identifying root causes fast and easy. Analysts can quickly jump through each stage of an attack to gain insight into the attacker's behavior, close security gaps, and learn from every new attack technique to avoid falling victim to the same attack twice.

Live Response for Remote Remediation

With Live Response, incident responders can create a secure connection to infected hosts to pull or push files, stop processes, perform memory dumps and quickly remediate from anywhere in the world.

Automation via Integrations & Open APIs

Carbon Black boasts a robust partner ecosystem and open platform that allows security teams to integrate products like Enterprise EDR into their existing security stack.

Top 5 Things you should know about Enterprise EDR

Supported Platforms

•Windows • macOS • Linux

Linux Enterprise EDR

VMware Carbon Black Cloud Enterprise EDR on the latest versions of RHEL/CentOS, SUSE, Open SUSE, Ubuntu, Amazon Linux, Oracle (both RHCK and UEK kernels), Debian, and Generic Linux; brings best-in-class Enterprise EDR to Linux. This new release brings the most sophisticated EDR threat hunting platform to Linux in a single agent.

Importance of Unfiltered Data

Unfiltered data is pivotal to threat hunting. If your tool is making decisions about what it should and should not record regarding an event, it's very likely it will miss vital information regarding an attack. Custom detections and third-party threat intelligence feed need an unfiltered data recording to reliably generate alerts every time a particular action or behavior occurs on an endpoint. Unfiltered data is a prerequisite to effective threat hunting.

Many organizations see the MITRE ATT&CK feed-in CBTH and ask, "if MITRE has a threat feed, how come it's not in other products?" Well, other products cannot assume the risk of having a feed like MITRE ATT&CK, because when the customer invokes a certain behavior they'll notice that sometimes there is no ATT&CK detection because the data never made it to the threat feed because it was not recorded in the first place. You also need an unfiltered data stream to support the integrity of custom detections, which is why VMware's Enterprise EDR is the only tool that supports such flexibility in this area. VMware uses very advanced data-compression and transportation techniques that are ahead of all others in the endpoint security space to make this possible.

Custom IOCs

One of the most powerful things you can do within your cyber environment creates your own custom IOC's. This is because you and your team understand what's normal in your own environment. VMware can help you get a further, more in-depth understanding of what's normal on your network as well, as you analyze its Behavioral and Enterprise EDR recordings over time. Custom IOCs can also be used for things beyond cybersecurity, such as alerting you to when a process in your cloud application was terminated, or when an RDP session to a workstation was established. Many corporate and government organizations use custom watchlists made up of IOCs to track adherence to, and violations of, organizational policy.

Contextual versus Threat Watchlists

There are two primary types of watchlists in Carbon Black ThreatHunter: Contextual watchlists (such as the Carbon Black Suspicious Indicators Feed and the Carbon Black Endpoint Visibility Feed), and Threat Watchlists (such as the Carbon Black Advanced Threats Feed) Contextual watchlists are not meant for generating alerts. They're simply meant to give you context into process behavior on your endpoints and highlight possible abuses. They work in conjunction with watchlists meant for alerting, by offering additional context and explanation into what the processes are doing within an alert.

Summary and Additional Resources

Conclusion

This document provides you with a good understanding and overview of Carbon Black Enterprise EDR and its capabilities. To learn more about the product explore our hands-on-lab and TestDrive experience.

Additional Resources

For more information about Endpoint Standard, explore the Mastering Enterprise EDR. 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.

Additionally, check out the VMware Carbon Black Enterprise EDR FAQ which provides answers to some of our most popular Enterprise EDR questions.

Change Log

The following updates were made to this guide:

Date	Description of Changes
2021/09/16	

Authors and Contributors

With significant contributions from:

- Victor Monga, Senior Tech Marketing Architect, Carbon Black