



Carbon Black Cloud Endpoint Standard - Technical Overview

Table of contents

Carbon Black Cloud Endpoint Standard - Technical Overview	3
What Is Carbon Black Cloud Endpoint Standard?	3
Endpoint Standard is a Next-Generation Antivirus (NGAV)	3
How Does Endpoint Standard Work?	3
Overview of How Endpoint Standard Works	3
How is Endpoint Standard different from traditional antivirus solutions?	4
What are the key benefits of Endpoint Standard?	6
Top 5 things you should know about Endpoint Standard	7
How Does Endpoint Standard Help?	7
How Does Endpoint Standard Help?	7
How Does Endpoint Standard Help?	8
Summary and Additional Resources	9
Conclusion	9
Additional Resources	9
Change Log	9
The following updates were made to this guide:	9
Authors and Contributors	9

Carbon Black Cloud Endpoint Standard - Technical Overview

What Is Carbon Black Cloud Endpoint Standard?

Endpoint Standard is a Next-Generation Antivirus (NGAV)

VMware Carbon Black Cloud Endpoint Standard is a next-generation antivirus (NGAV) and behavioral endpoint detection and response (EDR) solution that protects against the full spectrum of modern cyber-attacks. Using the VMware Carbon Black Cloud's universal agent and console, the solution applies behavioral analytics to endpoint events to streamline detection, prevention, and response to cyber-attacks. You can extend with [Enterprise EDR](#) and [XDR](#) for your SOC.

How Does Endpoint Standard Work?

Overview of How Endpoint Standard Works

1. Deploy sensors to endpoints
2. Apply security policies to your endpoints
3. Alert and block when threats are observed

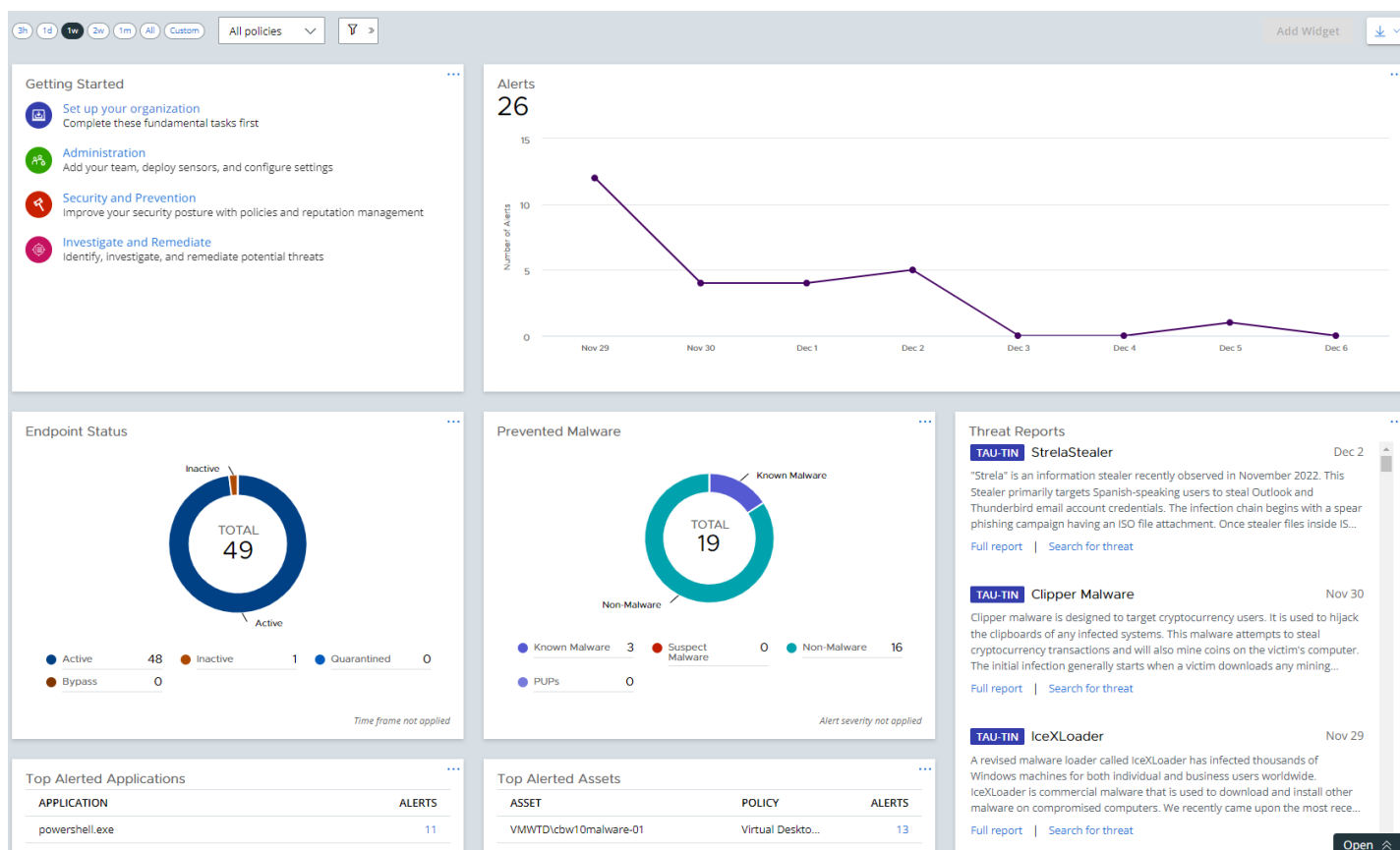
The most essential building block for Endpoint Standard is the **policies**. By default Endpoint Standard is deployed with 3 predefined policies.

Policy	Description
Monitored	Monitors endpoint application activity and logs events to the Dashboard. This policy has no preventive capabilities.
Standard	Blocks known and suspected malware, and prevents risky operations like memory scraping and code injections. Newly deployed sensors are assigned this policy by default. <i>It is the recommended starting point for new deployments.</i>
Advanced	Extends the capabilities of the Standard policy. It blocks operations from system utilizing, and prevents from riskier behaviors that are more likely to be false positives.

While Endpoint Standard comes with some out-of-the-box policies, you can also create, edit, and delete your own custom policies.

Once you have deployed sensors to endpoints and applied policies, you will see information regarding the sensors on the Endpoint Standard dashboard. You could also view your organization's overall security status.





The Endpoint Standard dashboard you can see attacks were stopped, attack vectors, and a summary of overall endpoint health.



In the top right corner, this dashboard can be downloaded for offline reporting, as well as customized to include only the widgets you are interested in reviewing.

How is Endpoint Standard different from traditional antivirus solutions?

Traditional antivirus software has become outdated and rarely successful at detecting smart malware and malwareless attacks. NGAV solutions are rising to the task of stopping these modern threats by using new tactics. Endpoint Standard can prevent and detect a variety of threats – including malware, non-malware, and fileless attacks. The majority of today’s malicious actors leverage fileless or non-malware attacks. Endpoint Standard leverages multiple layers of prevention to take you beyond traditional Anti-Virus protection.

 <p>Cloud Reputation</p> <p>Signature Prevention</p> <p>Delay execute for cloud scan machine learning.</p>	 <p>AMSI Prevention</p> <p>Automatically analyze and block malicious scripts.</p>	 <p>Policy-Level Prevention Rules</p> <p>Customized prevention beyond Known Bad</p> <p>Restrict Unknown/not listed or specific applications from performing undesired behaviors.</p>	 <p>Canary Files</p> <p>Decoy files located on the local file system to prevent encryption.</p> <p>Blocks access to volume shadow copies and master boot record.</p>
--	---	---	--

Be sure to reference our Malware Lab to get hands on and detonate today's latest threats against VMware Carbon Black Cloud Endpoint Standard.

What are the key benefits of Endpoint Standard?

- Stops malware, fileless, ransomware and living-off-the-land attacks
- Out-of-the-box prevention policies and ability to customize to environment
- Visibility into the entire attack chain for easy investigation
- Remote shell into endpoints for immediate action
- Cloud-native platform with single agent & console
- Automation via integrations & open APIs

Top 5 things you should know about Endpoint Standard

Now that you've established a solid foundation of what Endpoint Standard can do for you, learn about the top 5 things you should know about Endpoint Standard. This section helps you understand how Endpoint Standard will work for you.

Endpoint Standard Operating Environment Requirements

- Windows: Windows 7, 8, 10, 11
- macOS: 10.12 and up
- Linux: RHEL 8, CentOS 8, Oracle (UEK 7.6-7.9, 8 and up, RHCK), SUSE, Ubuntu, Amazon Linux, Debian (kernel 4.4 and up)
- Servers: Windows 2008 R2 – Windows 2012 – Windows 2012 R2 – Windows 2016 – Windows 2019 - Windows 2022

Malware and Non-Malware protection

Endpoint Standard helps you gain comprehensive protection of your organization's data and customer information from malware, non-malware, and living off-the-land (LoL) attacks. Simplify deployment and operation with out-of-the-box policies to adapt the protection to your organization. Stay up to date on the latest attacks with in-product updates from our expert VMware Threat Analysis Unit™.

Stopping a non-malware attack requires a different approach than traditional methods that stop malicious files at a single point in time. Since non-malware attacks leverage a series of known, allowed applications and processes, the entire event sequence must be analyzed to uncover the threat.

How Does Endpoint Standard Help?

- **Stops Advanced Attacks:** Innovative streaming prevention technology stops ransomware, malware, and non-malware attacks.
- **Threat Visibility:** Powerful attack visualizations display the entire stop chain, so you can quickly understand the root cause and remediate it.
- **Lightweight & Easy:** Cloud-delivered agents deploy seamlessly, and a dynamic console shows everything you need to know at a glance.

Expedite investigation and response time

Endpoint Standard provides a centralized, cloud-based administrative interface that combines next-generation antivirus (NGAV) and endpoint detection and response (EDR) capabilities into a lightweight solution that is fast to deploy and easy to manage. Endpoint Standard is designed to deliver the best endpoint security with the least amount of administrative effort, combining all the data and tools necessary to perform root cause analysis, real-time investigations, remote remediation, and policy management in a single console.

You can save money and time investigating and responding to incidents. With visibility into the entire attack chain and endpoint activity analysis, there's no need to spend time tracking down which of your systems were affected and when. Respond remotely and minimize downtime to endpoints with a tool that allows you to instantly roll back attacks from the console.

How Does Endpoint Standard Help?

- **Cuts Investigation Time-** Continuously record endpoint activities and store them centrally for rapid access. "Rollback the tape" at any time, often shortening investigation time from days to minutes.
- **Reduces Overhead-** Live Response allows you to remotely investigate and remediate any endpoint, drastically reducing IT overhead and the need for reimaging.
- **Unparalleled Threat Visibility-** Detailed process trees reveal the root cause of every attack, so you can quickly close security gaps and stop future attacks.

Prevent ransomware attacks

Today's ransomware is innovating at a rapid pace. Going beyond simple file encryption, ransomware increasingly leverages unknown variants and file-less techniques. Learn more about these new techniques and how Carbon Black stops them.

How Does Endpoint Standard Help?

- **Streaming Ransomware Prevention** - Advanced prevention stops current and future ransomware variants by monitoring streams of events related to a ransomware outbreak.
- **Protects Against New & Emerging Threats** - Lures all types of ransomware into a trap, even unknown and file-less varieties, to spot it and stop it before it attacks critical files and shares.
- **Ability to Detect and Rollback Ransomware** - In the case of rollback providing not only the ability to restore to a particular shadow copy, but it is also providing disaster recovery tools to ensure business operations can resume as quickly as possible. Like to learn more? Watch the video!

Multi-level protection

Cyberattackers are innovating faster than traditional defenses can withstand. Our NGAV solution employs multiple protection layers, including file reputation and heuristics, machine learning, and behavioral models, to analyze endpoint activity and block malicious behavior to stop all types of attacks before they reach critical systems. With flexible behavioral prevention policies, protection is easily tailored to your organization's distinct needs.

Summary and Additional Resources

Conclusion

This document helped you get a high-level understanding and overview of the Carbon Black Endpoint Standard. To learn more about the product explore our hands-on lab and TestDrive experience.

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.

Additionally, check out the [VMware Carbon Black Cloud Endpoint Standard FAQ](#) which provides answers to some of our most popular Endpoint Standard questions.

Change Log

The following updates were made to this guide:

Date	Description of Changes
2021/09/10	

Authors and Contributors

This document was created by:

- [Sowmya Jayakirithi](#) Content Marketing Manager, Carbon Black, VMware.

