VMware Carbon Black App Control

Application control and critical infrastructure protection

Use cases

- Lockdown of critical systems
- Fixed function devices, such as point-of-sale terminals, ATMs, industrial control systems, and medical devices
- High-risk endpoints, such as corporate desktops and executive laptops
- Servers, domain controllers, email and web application servers, card data environments, and financial trading platforms
- Legacy systems running unsupported operating systems

Benefits

- Stop malware, ransomware and next-gen attacks
- Eliminate unplanned downtime of critical systems
- Consolidate endpoint agents
- Prevent unwanted change to system configuration
- Inspect file content
- Enable more granular control of security policies
- Meet IT risk and audit controls across major regulatory mandates
- Increase efficiency of IT resources with streamlined IT audit processes
- Protect legacy systems running on unsupported operating systems
- Is a direct control for requirement 5 of PCI DSS

Highly targeted assets demand perfect security but can't afford loss in performance. Critical systems are increasingly targeted because they contain the most valuable information. These systems cannot afford a moment of unscheduled downtime or performance degradation as they are the lifeblood of the organization. They often run on out-of-date or unsupported operating systems, which are costly to secure and support. The most common approach to defending these systems typically relies on layering multiple, ineffective security products, which is costly, creates risk and jeopardizes performance.

VMware Carbon Black® App Control™ is used to lock down servers and critical systems, prevent unwanted changes, and ensure continuous compliance with regulatory mandates. Leveraging cloud reputation services, IT-based trust policies, and multiple sources of threat intelligence from VMware Carbon Black Cloud™, Carbon Black App Control ensures that only trusted and approved software is allowed to execute on an organization's critical systems and endpoints.

Carbon Black App Control combines application control, file integrity monitoring, full-featured device control, and memory/tamper protection into a single agent. Carbon Black App Control watches for behavioral indicators of malicious activity and conducts continuous recording of attack details to provide rich visibility into everything suspicious that attackers attempt to do. With the file delete feature, Carbon Black App Control is a direct control for requirement 5 of PCI DSS, enabling customers to remove traditional antivirus without the need for undergoing the compensating control process. The new content-based inspection feature enables more granular control of security policies.

Security teams can harden their new and legacy systems against all unwanted change, simplify the compliance process, and provide the best possible protection for corporate systems at enterprise scale. Carbon Black App Control is available through managed security service providers (MSSPs) or directly as an on-premises product.

> "It was a standout product for us. The effort required to install and maintain it appeared to be much lower than other products in its class."
>
> Simon Turner, Head of IS Architecture, Kordia

VMware Carbon Black Cloud

VMware Carbon Black Cloud is an endpoint protection platform that leverages unfiltered data and streaming analytics to prevent, investigate, remediate and hunt for threats.

Features

- Application control
- File integrity monitoring and control
- Device control
- Content-based inspection
- Memory protection
- Reputation services
- Open APIs

Platforms

Sensor support:

- Windows XP, Server, Vista, Embedded, POS
- Mac OS X
- RHEL Linux
- CentOS Linux
- Oracle RHCK Linux

For more information or to purchase VMware products

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit vmware.com/products, or search online for an authorized reseller.

To set up a personalized demo, visit vmware.com/resources/security/demo.

Key capabilities

VMware Carbon Black App Control is a powerful positive security solution for data centers and critical systems that allows server admins to control change while consolidating agents. Using a default deny approach, Carbon Black App Control reduces your attack surface and downtime by automating approval of trusted software and eliminating the burden of allowlist management.

Lock down critical systems

Stop malware and non-malware attacks by preventing unwanted changes to your applications and files, providing you with the control over your environment that you need.

Ensure continuous compliance

Accelerate compliance by meeting many of the requirements in regulatory standards and frameworks, such as PCI-DSS, HIPAA/HITECH, SOX, NERC CIP, GDPR and NIST 800-53. Carbon Black App Control is Common Criteria certified.

High-performance and low-touch application control

Be confident that your solution is blocking the bad and allowing the good without interrupting daily operations.

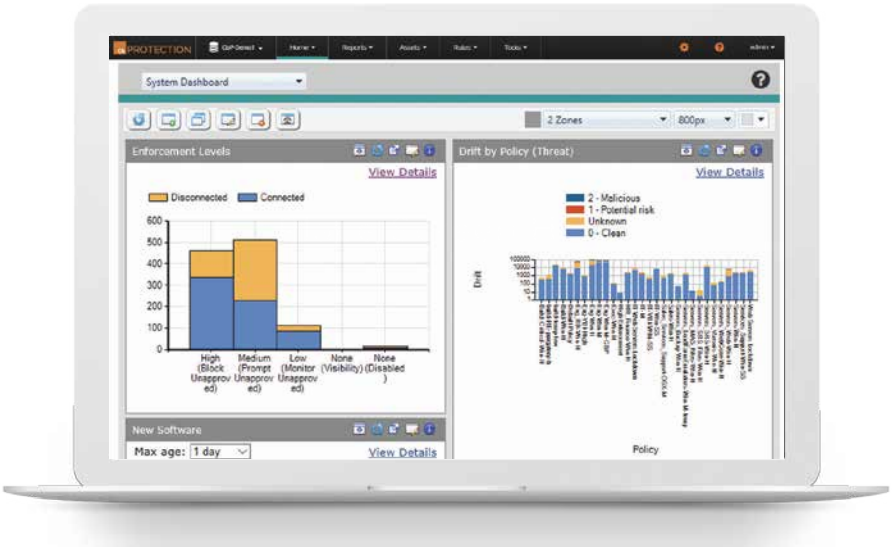

Figure 1: Lock down critical systems from unwanted change.

Item No: 1604262aq-ds-crbn-black-app-ctrl-a4 9/22