



Cyber Resilience with Carbon Black App Control

January 2024 DISA TEM Brief

Carbon Black®



Agenda

- Introduction
- History of Carbon Black
- What is Carbon Black Application Control?
- Where can this deploy?
- Platform Demonstration
- Q&A



The History of Carbon Black

Creating a World Safe from Cyber Attacks



Bit9

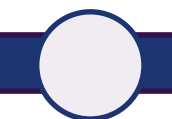
Bit9 + CARBON BLACK

Carbon Black.

Nasdaq
(CBLK)

vmware[®]
Carbon Black.

Carbon Black.



2002

Founded as Bit9, offering a new generation of endpoint and server security based on zero trust positive security.



2014

Bit9 acquired Carbon Black, a leader in endpoint detection and response.



2016

Bit9 rebrands as Carbon Black and is named a leader in endpoint security. Released cloud native NGAV the following year.



2018

Carbon Black (CBLK) goes public, announces managed threat detection and real-time query / response capabilities.



2019

VMware acquires Carbon Black and launches a new security business unit to natively embed security into VMware core products.



2023

With the acquisition of VMware by Broadcom, Carbon Black is a stand-alone business unit with a mature portfolio of security solutions and sole focus of keeping the world safe from cyber attacks.



What is a Positive Security Model?

- Only allows explicitly trusted programs to execute
- Blocks all software “good” or “bad” if not on Agency’s approved list
- Enforces change management policies



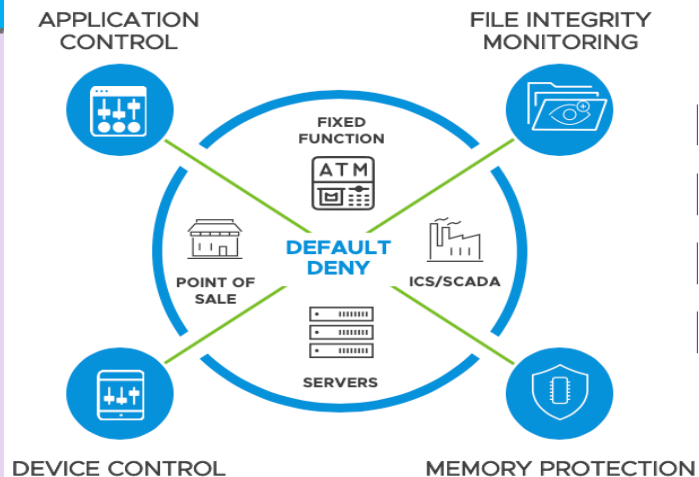
Carbon Black App C Capabilities Today



Carbon Black App Control

Federal Drivers

- ❑ Automate/Simplify trusted publisher
- ❑ Speed toward Remediation (Automation)
- ❑ Consistent Baseline Enforcement
- ❑ Continuous Monitoring for Gaps & Compliance
- ❑ Lack of Visibility
- ❑ Zero Trust Enablement (data/file/app protection)
- ❑ Standardize on Common Platform for Scale
- ❑ Centralized Management



STRONGEST SECURITY POSSIBLE

BLOCKS MALWARE, ADVANCED ATTACKS

PREVENTS ALL UNWANTED CHANGE

CROSS-PLATFORM SUPPORT

Proven Use-Cases

- ❑ Implement “High-Enforcement” Default/Deny - Unapproved
- ❑ Automated Blocking of Malware, Advanced Attacks
- ❑ Software Asset Inventory Management (SWAM): “What SW is on Host?”
- ❑ Continuously Monitor & Prevent unwanted changes on critical servers, desktops and laptops
- ❑ Visibility of all endpoints – Support & Facilitate Risk Mgmt
- ❑ Implement Strict Memory, App, SW & File Change Control
- ❑ Easily Scalable with 150+ Built-In APIs
- ❑ Centralized Management Console / Reduces Silos



Levels of Enforcement






Simple User Interaction

Allow users to be part of the policy tuning

Block unapproved scripts - DEMO



Target: putty-64bit-0.79-installer.msi
Path: c:\users\administrator\downloads\
Process: msixec.exe

Parity blocked an attempt by msixec.exe to run the script putty-64bit-0.79-installer.msi because the file is not approved. If you require access to this file, please contact your system administrator. Scroll down for diagnostic data.

UserName: APPCONTROL\Administrator
ComputerName: APPCONTROL

<https://www.virustotal.com/en/file/%3CTargetSha256%3E/...>

[Submit Approval Request>>](#)

OK

	Process	Target	Path
1	msixec.exe	putty-64bit-0.79-installer....	c:\users\administrator\downloads\

Approval Request

Enter your reason for access (512 characters max).

Your Email:

Priority:

Submit

Carbon Black App Control

Simple User Interactions

Pause or block applications from running

Request input from user on what is changing and why

Allow local approval (by policy)

Flexible Deployment Model

Wherever your endpoints reside (local or remote) your App Control server can be configured to connect to those endpoints whether the server resides in your datacenter, AWS, Azure or Google Cloud.



Data Center



Azure



Amazon Web
Services



Google Cloud
Platform



Private Cloud



Software Asset Management (SWAM) Drivers

Carbon Black App Control

Detect Installed Software		
SWAM-1.1*	The SWAM capability shall uniquely identify each instance of installed software that is detected on endpoint devices on the network.	✓
SWAM-1.2*	When configured by the administrator, the SWAM capability shall scan endpoint devices on the network on an automated basis to detect installed software.	✓
SWAM-1.3	Upon administrator command, the SWAM capability shall scan endpoint devices on the network to detect installed software on an ad-hoc basis.	✓
SWAM-1.4*	The SWAM capability shall authenticate to endpoint devices with privileged access when conducting a scan for installed software.	✓
SWAM-1.5*	When executing a scan, the SWAM capability shall detect between 80% (threshold) and 95% (objective) of installed software on endpoint devices on the agency's network.	✓
SWAM-1.6*	When conducting a scan, the SWAM capability shall detect installed software with a false positive rate no greater than 0.1%.	✓
SWAM-1.7*	When conducting a scan, the SWAM capability shall detect installed software with a false negative rate no greater than 0.1%.	✓
Restrict Changes to Authorized Users		
SWAM-3.1	The SWAM capability shall enforce access control to only allow selected users to perform administrator functions, as defined by agency policy.	✓
Remove Software Upon Request		
SWAM-4.1	When configured by the administrator, the SWAM capability shall remove software installed on endpoint devices on a scheduled time in the future.	✓
SWAM-4.2	Upon administrator command, the SWAM capability shall remove software installed on endpoint devices on an ad-hoc basis.	✓



Software Asset Management (SWAM) Drivers Cont.

Carbon Black App Control

Maintain and Report CDM SWAM Data		
SWAM-5-1*	When conducting a scan, the SWAM capability shall collect all of the following software component information for all installed software detected on endpoint devices: <ul style="list-style-type: none">• Software Product Vendor• Software Product Name• Software Product Version	✓
SWAM-5-2*	When conducting a scan, The SWAM capability shall collect all of the following required actual state information for all installed software detected on endpoint devices: <ul style="list-style-type: none">• Timestamp of when the software was detected on the endpoint device• Endpoint Device Identifier where product was detected• Type/Classification of Software detected	✓
SWAM-5-3*	The SWAM capability shall continuously maintain a timely, updated inventory of installed software that includes every software UID, all software component information, and all actual state software information for each endpoint device on the agency's network.	✓
SWAM-5-4*	The SWAM capability shall report an inventory of installed software that includes every software UID, all software component information, and all actual state software information for each endpoint device on the agency's network.	✓



Application Execution Control Drivers

Carbon Black App Control

Define and Maintain Execution Control List and Policies		
AEC-1-1	When configured by the administrator based on agency policy, the AEC capability shall instantiate the Allow List such that it incorporates between 95% (threshold) and 99% (objective) of the allowed applications on endpoint devices.	✓
AEC-1-2	When configured by the administrator based on agency policy, the AEC capability shall instantiate the Deny List such that it incorporates between 95% (threshold) and 99% (objective) of the denied applications on endpoint devices.	✓
AEC-1-3	If applicable, based on agency policy, the AEC capability shall implement different AEC control policies for each endpoint device type.	✓
AEC-1-4	When configured by the administrator based on agency policy, the AEC capability shall group endpoint devices together for implementation of configured allow and/or deny lists.	✓
AEC-1-5	The AEC capability shall automatically disseminate control policies to attached endpoint devices upon administrator configuration change within 24 hours.	✓
AEC-1-6	The AEC capability shall automatically disseminate control policies to endpoint devices that were not connected to the network during an automatic update, upon connection to the network.	✓
AEC-1-7	When configured by the administrator based on agency policy, the AEC capability shall automatically update the Allow List on the intended execution date/time or on reception date/time of the update, whichever is later.	✓
AEC-1-8	The AEC capability shall automatically distribute application updates to agents on endpoint devices enforcing the Allow List within 24 hours of the intended execution date/time or reception date/time of the update, whichever is later, based on agency policy.	✓
AEC-1-9	For automated updates requiring administrator approval based on agency policy, the AEC capability shall automatically update the Allow List within upon the administrator's approval of the update.	✓
AEC-1-10	For automated updates requiring administrator approval based on agency policy, the AEC capability shall distribute the Allow List to agents on endpoint devices within 24 hours of the administrator's approval of the update.	✓
AEC-1-11	When configured by the administrator based on agency policy, the AEC capability shall automatically update the Deny List on the intended execution date/time or reception data/time of the update, whichever is later.	✓
AEC-1-12	The AEC capability shall automatically distribute application updates to agents on endpoint devices enforcing the Deny List within 24 hours of the intended execution date/time or reception date/time of the update, whichever is later, based on agency policy.	✓
AEC-1-13	For automated updates requiring administrator approval based on agency policy, the AEC capability shall automatically update the Deny List upon the administrator's approval of the update.	✓
AEC-1-14	For automated updates requiring administrator approval based on agency policy, the AEC capability shall distribute the Deny List to agents within 24 hours of the administrator's approval of the update.	✓

Up Next:



Application Control Demonstration

Q&A

Carbon Black®



Carbon Black Primary Points of Contact



Mike Drinkwater: Account Executive, DoD & National Security

- [*mike.drinkwater@broadcom.com*](mailto:mike.drinkwater@broadcom.com)

Joseph Fonti: Sr. Solutions Engineer, Federal

- [*joseph.fonti@broadcom.com*](mailto:joseph.fonti@broadcom.com)

Nathan Bray: Sr. Solutions Engineer, Federal

- [*nathan.bray@broadcom.com*](mailto:nathan.bray@broadcom.com)

Garrett Lee: Director, Federal Operations

- [*garrett.lee@broadcom.com*](mailto:garrett.lee@broadcom.com)

Carbon Black®



Thank You

Carbon Black®

