



Getting Started with VMware Carbon Black App Control

Table of contents

| | |
|--|----|
| Getting Started with VMware Carbon Black App Control | 3 |
| Introduction | 3 |
| System Configuration | 4 |
| Global Password | 4 |
| Licensing | 5 |
| Email Notifications | 7 |
| Alerts | 7 |
| Detecting Advanced Attacks | 8 |
| Policies | 9 |
| Deploying an Agent | 10 |
| Device Status | 10 |
| Events | 12 |
| Conclusion | 13 |

Getting Started with VMware Carbon Black App Control

Introduction

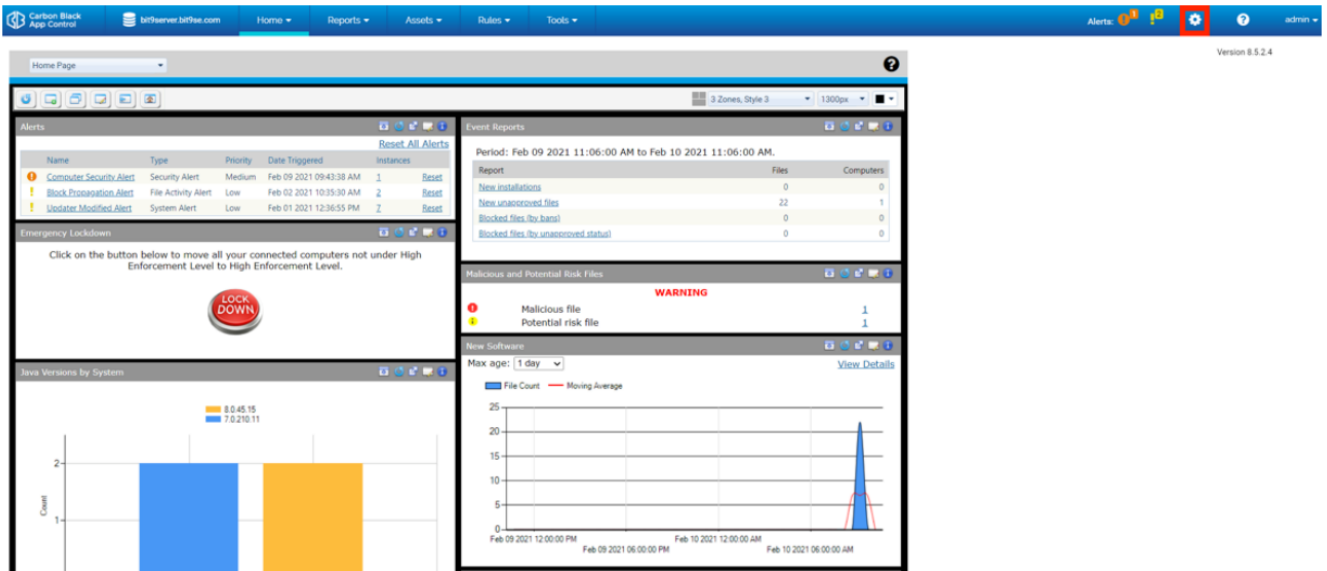
The purpose of this guide is to get you up and running with VMware Carbon Black App Control in less than an hour. It assumes your App Control server is ready to go, and you have access to the console and can deploy agents onto the operating systems you want to cover. As you're going to discover, App Control is very rich in capabilities and robust in its power to prevent unwanted execution and change, yet low touch and easy to manage. It makes application control something possible to do across an entire enterprise, without as much work as it would take using other solutions.

Successfully implementing application control in your environment is perhaps the most powerful step you can take to prevent attacks on endpoints, because it enforces the positive security model, which is only allowing trusted files to run, and trusted to change to occur.

System Configuration

Global Password

The first thing we want to do in App Control ensures it is optimally configured. This will be quick and easy. Let's get started by configuring the global password for your App Control agents. This is needed in case you ever need to uninstall an agent, and it enables an emergency tamper protection override. The default password is "control," but the best practice is to replace that right away. To do this, we need to navigate to **Cog Wheel (red box) > System Configuration > General > Edit**.



The Edit button will be at the bottom of the General tab page (**green box**), and what we want to edit is the Global Password in the Agent Management section (**orange box**). Please note the Active Directory/LDAP integration section (**red box**). This is where you would be able to swiftly configure AD/LDAP mapping in your production environment. Additionally, you can enforce your organization's password policy for your App Control administrators (**blue box**).

System Configuration

General | Events | Security | Advanced Options | Mail | Licensing | External Analytics | Connectors | Unified Management | SAML Login

General Settings

Server Status

Carbon Black App Control Version: 8.5.2.4
Server Address: bit9server.bit9se.com
Server Port: 41002
Server Timezone: -Automatic-
Database Schema Version: 8.5.2.4
Database Address: local
Database Auth. Type: NT
Database Size: 1826.25 MB
Free Local Disk Space: 22.4 GB / 95.0 GB
CL Version: 2920428

Active Directory / LDAP integration

AD-Based Logins: Enabled
AD Security Domain: bit9se.com
AD-Based Policy: Enabled
Windows 2000 DCs:
Test AD Connectivity:

Agent Management

Windows User/Group To Manage Agents: None User or group Pre-defined group
Mac User/Group To Manage Agents: None User Group
Linux User/Group To Manage Agents: None User Group
Enable Global Password:

User Passwords

Minimum Length: 8
Minimum Special Character Count: 0
Expiration: 0 Days
Expiration Warning Period: 14 Days
Expiration Grace Period: 0 Days

Licensing

Next, it is important to ensure licensing is taken care of. Navigate to **Cog Wheel > System Configuration > Licensing**. Let's

input your SRS (software reputation services) key. This will drastically enrich the data within the console, as it leverages an aggregation of over one billion unique binaries we have seen over time and assigned trust score ratings to. This will allow you to verify the “good” software that currently exists in your environment, as well as identify files that VMware knows are malicious in your environment. You should have received your SRS key in an automated email sent out by your VMware Carbon Black Solution Engineer. Paste your SRS key into the Carbon Black File Reputation section (**blue box**), and accept the prompts.

The screenshot displays the 'System Configuration' interface. At the top, a navigation bar includes tabs for 'General', 'Events', 'Security', 'Advanced Options', 'Mail', 'Licensing', 'External Analytics', 'Connectors', 'Unified Management', and 'SAML Login'. The 'Licensing' tab is selected and highlighted in pink. Below the navigation bar, the 'Licensing' section is visible, containing a 'Summary' and a 'Licenses' section. The 'Licenses' section has two radio buttons: 'Paste license key' (selected) and 'Specify license file' (highlighted with a red box). Below these is a text input field and an 'Add License' button (highlighted with a purple box). The 'Carbon Black File Reputation Activation' section shows that the subscription is activated, with a 'Carbon Black File Reputation Key' (blacked out) and 'Synchronization Of Files' at 100%. It includes 'Deactivate' and 'Options' buttons. The 'Carbon Black File Reputation Proxy Settings' section at the bottom has an 'Enabled' checkbox (unchecked), a 'URL' field with '(none)' and a 'Test' button (highlighted with a green box). An example URL is provided: 'http://hostname_or_ip[port]'.

Now, we are going to input your license file, which was also attached to the automated email coming from your VMware Carbon Black Solution Engineer. You can paste the contents of the “.lic” file into the Licenses section (**orange box in screenshot above**), or put the “.lic” file on your App Control server, select “Specify license file” (**red box in screenshot above**) and select your license file. Regardless of your preferred method, once this is complete, click “Add License” (purple box in screenshot above). This is also where you would input proxy server information for connectivity to VMware Carbon Black reputation services, if it is needed in your organization (**green box in screenshot above**). Next up, we will configure email notifications, so mosey on over to the “Mail” tab just to the left of the licensing tab (pink box in the screenshot above).

Email Notifications

The Mail tab is very straightforward. Select “Edit” (**purple box**), enter your mail server, port, and the “from” address you wish to use (**red box**), and save your changes. Finally, enter your email to test email notifications (**green box**).

System Configuration

General
Events
Security
Advanced Options
Mail
Licensing
External Analytics
Connectors
Unified Management
SAML Login

Mail Notification Configuration

Alert Settings

Mail Notification Enabled:

Global Subscriber Enabled:

Approval Request Settings

Mail Notification Enabled:

Server Settings

Mail Server: mail.bit9se.com

Mail Server Port: 25

Mail "From" Address: bit9server@mail.bit9se.com

Secure Mail (TLS):

Validate Server

Test Address:

▶ Send Mail

Edit
 Update
 Cancel

Alerts

As with any security solution, it’s necessary to ensure optimal prioritization of alerts. So, let’s do that for App Control. Navigate to **[Tools (red box) > Alerts]**. Within the blue box you can see two icons – one that looks like a notepad (left icon), and the other with paper and a pen (right icon). The notepad allows you to see prior detections for a given alert type, and the paper and pen button allows you to edit an alert. Alerts are highly customizable. You will notice that essentially everything in App Control is quite granularly customizable, which is the result of the product being very mature, having been on the market since 2002, and having incorporated literally thousands of customer requests into the product over time. You can determine how and to whom an alert would be received, and much more. For a POC, it is recommended to enable “malicious file detected” and set it to high. It is also recommended to move Indicator Set Alerts to high, as Indicator Sets are strong indicators of malicious activity.

Getting Started with VMware Carbon Black App Control

1 alert modified.

Alerts

Group By: Priority Ascending

Show Filters | Show Columns | Export to CSV | Refresh Page

Action | 1 2 | Add Alert

| | Name | Type | Enabled | Priority | Date Triggered | Instances | Date Created | Created By |
|-------------------------------------|--|------------------------|---------|----------|-------------------------|-----------|-------------------------|------------|
| Priority: High | | | | | | | | |
| <input checked="" type="checkbox"/> | Carbon Black File Reputation Unavailable Alert | System Alert | Yes | High | Feb 09 2021 09:41:38 AM | | Aug 15 2012 07:56:10 AM | System |
| <input checked="" type="checkbox"/> | Malicious File Detected | File Security Alert | Yes | High | Jun 26 2017 10:17:11 AM | | Aug 15 2012 07:56:10 AM | System |
| <input checked="" type="checkbox"/> | System Health GER Alert | System Health Alert | Yes | High | May 18 2015 09:26:17 AM | | May 18 2015 09:26:17 AM | System |
| <input checked="" type="checkbox"/> | System Health Infrastructure Configuration Alert | System Health Alert | Yes | High | May 18 2015 09:26:17 AM | | May 18 2015 09:26:17 AM | System |
| <input checked="" type="checkbox"/> | System Health Product Configuration Alert | System Health Alert | Yes | High | May 30 2017 11:07:26 AM | | May 30 2017 11:07:26 AM | System |
| <input checked="" type="checkbox"/> | System Health Rules Alert | System Health Alert | Yes | High | May 30 2017 11:07:26 AM | | May 30 2017 11:07:26 AM | System |
| <input checked="" type="checkbox"/> | System Health Backlog Alert | System Health Alert | Yes | High | May 30 2017 11:07:26 AM | | May 30 2017 11:07:26 AM | System |
| <input checked="" type="checkbox"/> | System Health Environment Alert | System Health Alert | Yes | High | May 30 2017 11:07:26 AM | | May 30 2017 11:07:26 AM | System |
| <input checked="" type="checkbox"/> | Agent Install Package Generation Disabled | System Alert | No | High | Sep 30 2019 10:54:52 AM | | Sep 30 2019 10:54:52 AM | System |
| <input checked="" type="checkbox"/> | Host Package Not Found (Windows) | System Alert | Yes | High | Sep 30 2019 10:54:52 AM | | Sep 30 2019 10:54:52 AM | System |
| <input checked="" type="checkbox"/> | Host Package Not Found (Mac) | System Alert | Yes | High | Sep 30 2019 10:54:52 AM | | Sep 30 2019 10:54:52 AM | System |
| <input checked="" type="checkbox"/> | Host Package Not Found (Linux) | System Alert | Yes | High | Sep 30 2019 10:54:52 AM | | Sep 30 2019 10:54:52 AM | System |
| <input checked="" type="checkbox"/> | Default Rules Not Found | System Alert | Yes | High | Sep 30 2019 10:54:52 AM | | Sep 30 2019 10:54:52 AM | System |
| <input checked="" type="checkbox"/> | Indicator Set Alert | Event Alert | No | High | May 30 2014 07:50:27 AM | | May 30 2014 07:50:27 AM | System |
| <input checked="" type="checkbox"/> | Database Limit Alert | System Alert | Yes | High | Aug 15 2012 07:56:10 AM | | Aug 15 2012 07:56:10 AM | System |
| <input checked="" type="checkbox"/> | Backup Missed Alert | System Alert | No | High | Aug 15 2012 07:56:10 AM | | Aug 15 2012 07:56:10 AM | System |
| <input checked="" type="checkbox"/> | Database Verification Failed | System Alert | Yes | High | Aug 15 2012 07:56:10 AM | | Aug 15 2012 07:56:10 AM | System |
| Priority: Low | | | | | | | | |
| <input checked="" type="checkbox"/> | Block Propagation Alert | File Activity Alert | Yes | Low | Feb 02 2021 10:35:30 AM | 2 | Aug 15 2012 07:56:10 AM | System |
| <input checked="" type="checkbox"/> | Updater Modified Alert | System Alert | Yes | Low | Feb 01 2021 12:36:55 PM | 7 | Aug 15 2012 07:56:10 AM | System |
| <input type="checkbox"/> | Justification Alert | Approval Request Alert | No | Low | Aug 19 2013 11:44:11 AM | | Aug 19 2013 11:44:11 AM | System |
| <input type="checkbox"/> | New Certificate Alert | Certificate Alert | No | Low | Aug 19 2013 11:44:11 AM | | Aug 19 2013 11:44:11 AM | System |

Detecting Advanced Attacks

Let's take a look at those aforementioned indicator sets. To get there, navigate to [Rules > Indicator Sets]. Indicator Sets are pre-built by our experienced in-house staff and are aimed at detecting advanced attacks, such as process injection attacks, strange application behavior, process hollowing, and various other methods, which you can see in the screenshot below. Enable all indicator sets by checking off the top box (red box), selecting the Action button (green box), and clicking on "Enable Indicator Set."

Indicator Sets

Group By: (none) Ascending

Show Filters | Show Columns | Export to CSV | Refresh Page

Action

| <input type="checkbox"/> | Indicator Set Name | Version | Enabled | Platform |
|--------------------------|--|---------|---------|----------|
| <input type="checkbox"/> | Linux Possible Backdoor | 1405 | Yes | Linux |
| <input type="checkbox"/> | Linux Startup Configuration | 1405 | Yes | Linux |
| <input type="checkbox"/> | Mac Application Behavior | 1407 | Yes | Mac |
| <input type="checkbox"/> | Mac Shell Activity | 1407 | Yes | Mac |
| <input type="checkbox"/> | Mac Suspicious Based on Path | 1405 | Yes | Mac |
| <input type="checkbox"/> | Mac Suspicious Based on Path and File Name | 1407 | Yes | Mac |
| <input type="checkbox"/> | Mac System Configuration | 1409 | Yes | Mac |
| <input type="checkbox"/> | Windows Admin Tool Tracking | 1408 | Yes | Windows |
| <input type="checkbox"/> | Windows Application Behavior | 1408 | Yes | Windows |
| <input type="checkbox"/> | Windows POS Indicators | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows Process Injection | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows Ransomware Indicators | 1407 | Yes | Windows |
| <input type="checkbox"/> | Windows Startup Configuration | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows Suspicious Based on File Name | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows Suspicious Based on Parent | 1407 | Yes | Windows |
| <input type="checkbox"/> | Windows Suspicious Based on Path | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows Suspicious Based on Path and File Name | 1405 | Yes | Windows |
| <input type="checkbox"/> | Windows System Configuration | 1408 | Yes | Windows |

Policies

Policies are where we can define different user groups, which allows you to apply different rules to various policy groupings. Different application requirements dictate the need for different policies. You can have as many policy groups as you need, and they can be mapped to Active Directory/LDAP groups and accounts as well. Navigate to [Rules > Policies > +Add Policy]. What we're going to do now is create four initial policies, to get us started. They are:

- Deployment (Disabled)
- Learning Mode (Low Enforcement)
- Block and Prompt (Medium Enforcement)
- Default-Deny (High Enforcement – VMware Carbon Black App Control is an approved, PCI-compliant antivirus solution in this policy) To make the Deployment policy, simply type "Deployment" into Policy Name (**blue box**), select "Disabled" under Mode (**green box**) and click "Save & Exit" (**purple box**).

To make the Learning Mode policy, type "Learning Mode" into Policy Name (**blue box**), select "Control" under Mode (**orange box**), select "Low Enforcement" for both connected and disconnected machines under "Enforcement Level" (**red box**), select "Allow Upgrades" (pink box) and Save & Exit (**purple box**).

To make the Block and Prompt policy, follow the same steps as creating the Learning Mode Policy, except select "Medium" under "Enforcement Level" (**red box**).

To make the Default-Deny policy, follow the same steps as creating the Learning Mode Policy, except select "High" under "Enforcement Level" (**red box**).

Add Policy

Policy Name:

Description:

Mode: Visibility Control Disabled

Enforcement Level: Connected: High (Block Unapproved) ▼ Disconnected: High (Block Unapproved) ▼

Initial Settings: Template Policy ▼

Automatic Policy Assignment For New Computers:

Reputation Enabled: Check to enable reputation approvals in this policy

Options: Allow Upgrades Track File Changes
 Load Agent in Safe Mode Suppress Logo In Notifier

Total Computers: 0

Connected Computers: 0

It is best practice to ensure you only push out agents in Disabled mode, as it's a precaution that makes it easier to uninstall an agent, if need be, before tamper prevention kicks in. You can install an App Control agent manually by executing the installer and clicking through the prompts, or you can install it silently via a deployment tool, a script, the command prompt/terminal, and more. App Control installs require no system reboots unless you're using GPO (this is a limitation of Microsoft GPO which requires reboots for most software installations, not VMware Carbon Black) or installing on a Windows XP or Windows Server 2003 system. The next step is to do a quick agent installation on the App Control server itself.

Deploying an Agent

To download an agent package, navigate to [Rules > Policies] and select your installer download link (red box). Remember to download the installer for the “Disabled” policy.



Home » Policies

Users can download Carbon Black App Control Agent software from <https://bit9server.bit9se.com/hostpkg>

Click here to view available Carbon Black App Control Agent/Rules versions.

Policies

Policies Mappings

Group By:

(none) Ascending

Show Filters Show Columns Export to CSV Refresh Page

Action Add Policy

Once you have downloaded and installed the App Control agent on your App Control server, you should see it under [Assets > Computers]. Select your App Control server by checking off the box next to it (green box). Then select “Action” (orange box) and move your App Control server from Disabled mode into “Learning Mode.”

Computers

Computers connected: 1 Total computers: 7 Current CL version: 2920428 CL version for upgrade: 2920289

Saved Views: (none) Group By: (none) Days Disconnected: (none)

Show Filters Show Columns Export to CSV Refresh Page

Action Search: Go Clear

| Computer Name | Connected | Policy Status | Upgrade Status | Connected Enforcement | Disconnected Enforcement | IP Address | Policy |
|-----------------------|-----------|---|-------------------|--------------------------|--------------------------|-------------------------|---------------------|
| BIT9SEAD\BIT9SERVER | ● | Up to date | Up to date | High (Block Unapproved) | High (Block Unapproved) | fe80:e4af45b0:6314:8078 | Application Servers |
| BIT9SEAD\W7-HIGH | ● | Approvals out of date, Yara rules out of date | Upgrades disabled | Low (Monitor Unapproved) | Low (Monitor Unapproved) | 192.168.230.4 | Executive Desktops |
| BIT9SEAD\W7-LOW-Y | ● | Approvals out of date, Yara rules out of date | Upgrades disabled | Low (Monitor Unapproved) | Low (Monitor Unapproved) | 192.168.230.5 | Executive Desktops |
| CENTOS65 | ● | Approvals out of date | Up to date | Low (Monitor Unapproved) | Low (Monitor Unapproved) | 192.168.230.9 | Linux Servers |
| localhost.localdomain | ● | Approvals out of date | Up to date | High (Block Unapproved) | High (Block Unapproved) | 192.168.230.184 | Linux Servers |
| OSX1010.local | ● | Approvals out of date | Up to date | Low (Monitor Unapproved) | Low (Monitor Unapproved) | 10.37.5.206 | -Default Policy- |
| OSX1010.local | ● | Approvals out of date | Up to date | Low (Monitor Unapproved) | Low (Monitor Unapproved) | 192.168.230.8 | Mac laptops |

At this point, two things will happen. Firstly, App Control will start its initialization crawl and inventory all files, applications, certificates and removable devices with storage capacity on or attached to your App Control server. Secondly, tamper prevention will kick in immediately. Finally, App Control can apply custom rules, such as ransomware prevention, if it’s enabled under Rapid Configs, which is beyond the scope of this workshop, but worth noting. You can see the progress of your initialization crawl. Let’s add some additional fields to our Computers view so we can do so across the board going forward.

Device Status

To modify what information you are viewing on the Computers page, select “Show Columns” (red box). We want to ensure we can see % Initialized, % Synchronized, and Policy Status, which are under the “Available” items (blue box). Move over the items we need into the “Selected” items list by using the rightward arrow (orange box). Once you’re all set, click “Apply” (green box). If you like your new view, save it permanently by giving it a name and clicking “Add” (purple box).

Computers

Computers connected: 1 Total computers: 7 Current CL version: 2920428 CL version for upgrade: 2920289

Saved Views: (none) [Add]
 Group By: (none) [Ascending]
 Days Disconnected: (none)

Show Filters | **Hide Columns** | Export to CSV | Refresh Page

Column Settings

Available: % Synchronized, Active, Agent Debug Level, Agent Version, CL Version, Clone Inventory
 Selected: Upgrade Status, Connected Enforcement, Disconnected Enforcement, IP Address, Policy, % Initialized

[Apply] [Cancel] [Reset]

Action Search: [Go] [Clear]

| <input type="checkbox"/> | Computer Name ▲ | Connected | Policy Status | Upgrade Status |
|--------------------------|-----------------------|-----------|---|-------------------|
| <input type="checkbox"/> | BIT9SEAD\BIT9SERVER | ● | Up to date | Up to date |
| <input type="checkbox"/> | BIT9SEAD\W7-HIGH | ● | Approvals out of date, Yara rules out of date | Upgrades disabled |
| <input type="checkbox"/> | BIT9SEAD\W7-LOW-Y | ● | Approvals out of date, Yara rules out of date | Upgrades disabled |
| <input type="checkbox"/> | CENTOS65 | ● | Approvals out of date | Up to date |
| <input type="checkbox"/> | localhost.localdomain | ● | Approvals out of date | Up to date |
| <input type="checkbox"/> | OSX1010.local | ● | Approvals out of date | Up to date |
| <input type="checkbox"/> | OSX1010.local | ● | Approvals out of date | Up to date |

% Initialized shows what percentage of files have been inventoried from a given endpoint and sent to your App Control server. % Synchronized lets you know what percentage of files from a given endpoint have been checked against VMware Carbon Black threat intelligence using software reputation services. Our reputation services are optional, many organizations use App Control in completely air-gapped environments, but if your environment is not air-gapped you might as well make use of the services. It can identify known malware leveraging dozens of antivirus engines even beyond VMware Carbon Black's own ban list, let you know how trustworthy certain files are, and you can auto-approve files based on reputation if desired. Finally, Policy Status shows us if an endpoint has the most up to date rules for the policy group it is a part of.

Events

App Control provides significant visibility into what is occurring on your machines. To see what App Control is recording, navigate to **[Reports > Events]**. The list is in reverse-chronological order. This useful data can be quickly sorted through by leveraging different columns and filters and saved for future reference, allowing you to quickly sort through different logs for pertinent information. Get started by taking a look at new unapproved files on your current devices by selecting them from your current, default saved views in the drop-down menu (**blue box**).

| Events | | | | | | | | | |
|---|-------------------------|----------------------------|-----------|---|---|-----------------------------|---------------------------|--|----------------|
| Saved Views: <i>(The Current View Has Unsaved Changes - Discard)</i> New Files (Unapproved) <input type="button" value="Cache"/> <input type="button" value="Add"/> | | Group By: (none) | | Subgroup By: (none) Descending by count | | Max Age: 3 months | | Show Filters Show Columns Export to CSV Access Event Archives Refresh Table | |
| Action Search: <input type="text"/> <input type="checkbox"/> Automatically apply Showing 100 out of 273 item(s) | | | | | | | | | |
| Select | Timestamp | Severity | Type | Subtype | Description | Source | IP Address | User | File Name |
| <input type="checkbox"/> | Feb 10 2021 09:41:21 AM | Notice | Discovery | New unapproved file to computer | Computer BIT9SEAD\BIT9SERVER discovered new file 'c:\program files (x86)\bit9\parity server\hostpkg\baseline.msi' [6BA3C...AD569]. DiscoveredBy[Kernel:Rename] FileCreated[7/31/2019 3:39:15 PM] Discovered[2/10/2021 4:41:19 PM (Hash: 2/10/2021 4:41:19 PM)] YaraClassifyVersionId[3650] Rules[MSI,VirtualProtect] | BIT9SEAD\BIT9SERVER | fe80::e4af:45b0:6314:8078 | BIT9SEAD\admin | baseline.msi |
| <input type="checkbox"/> | Feb 10 2021 09:41:16 AM | Notice | Discovery | New unapproved file to computer | Computer BIT9SEAD\BIT9SERVER discovered new file 'c:\program files (x86)\bit9\parity server\hostpkg\deployment.msi' [B1FBC...96421]. DiscoveredBy[Kernel:Rename] FileCreated[7/18/2019 3:49:09 PM] Discovered[2/10/2021 4:41:14 PM (Hash: 2/10/2021 4:41:14 PM)] YaraClassifyVersionId[3650] Rules[MSI,VirtualProtect] | BIT9SEAD\BIT9SERVER | fe80::e4af:45b0:6314:8078 | BIT9SEAD\admin | deployment.msi |

Conclusion

Successfully applying application control is very likely the most powerful thing you can do as far as endpoint security goes. Properly-configured application control is the closest you can get to perfect prevention, although no prevention tool can be 100% perfect 100% of the time. Applying application control successfully with VMware Carbon Black App Control is all about defining commonality, and defining vectors of trusted change. For example, software deployed by your deployment solutions should be auto-approved, and App Control can do that. You should also be able to approve software based on publisher, certificate and more. App Control is a robust tool with a ton of capabilities, because we understand what other capabilities are a necessity for application control to be successful, having been doing this since 2002. Application control needs device control, file integrity control and monitoring, behavioral prevention abilities, in-memory rules, and more, to scale to an enterprise level. App Control ensures that everything needed for success is in one product, spanning Windows, Linux and macOS operating systems, including many embedded and IoT editions.

