Replace Symantec with VMware Carbon Black Cloud

BENEFITS OF REPLACING SYMANTEC WITH VMWARE CARBON BLACK CLOUD

- **Performance improvements on physical and virtual infrastructure:** When tested, VMware Carbon Black Cloud showed a max utilization of 3-5 percent. This is a significant difference when compared to other legacy AV vendors, which operate at or above 15 percent.
- **Infrastructure reduction:** VMware Carbon Black Cloud is entirely cloud hosted, ensuring that your distributed workforce remains up to date and eliminates the on-premises *infrastructure requirements* of Symantec Endpoint Protection.
- VMware Carbon Black provides better protection than many legacy AV provides; see the 2020 AV Comparatives *results*.

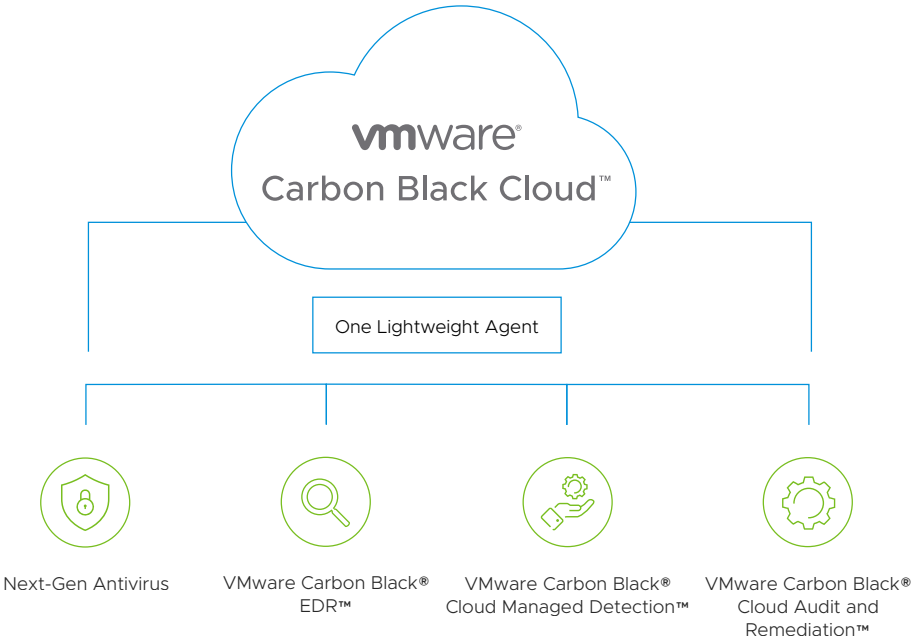
MIGRATION PHASES

- **Phase 1: Preparation** – Prepare to co-install VMware Carbon Black Cloud with Symantec AV. Configure policy requirements and implement communication exclusions.
- **Phase 2: Co-installation and baselining** – Deploy VMware Carbon Black Cloud alongside Symantec AV. Allow VMware Carbon Black Cloud to complete the compromise assessment of your fleet.
- **Phase 3: Uninstallation of Symantec AV** – Successfully remove Symantec AV after deploying VMware Carbon Black Cloud and validating the protection state.

VMware Carbon Black Cloud™ is a cloud native endpoint protection platform (EPP) that combines the intelligent system hardening and behavioral prevention needed to keep emerging threats at bay, using a single lightweight agent and an easy-to-use console.

By analyzing more than 1 trillion security events per day, VMware Carbon Black Cloud proactively uncovers attackers' behavior patterns and empowers defenders to detect and stop emerging attacks. As a key means to realizing intrinsic security, VMware Carbon Black Cloud simplifies and strengthens your approach to security across any app, any cloud and any device.

Consolidate multiple endpoint security capabilities, and operate faster and more effectively with a single, cloud native platform.



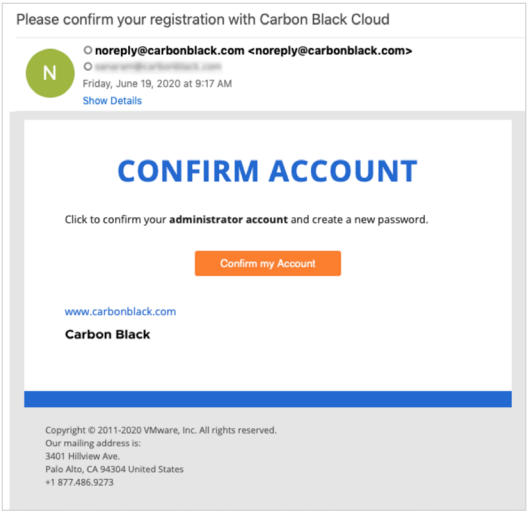
Phase 1: Preparation for deployment and co-install with SEP

To begin the roll out of VMware Carbon Black Cloud, you will need to prepare for co-installation and ensure connectivity to our cloud back-end. Installation of two security products can cause performance issues if not properly excluded. Adhere to the following instructions to prepare your environment for the installation of VMware Carbon Black Cloud.

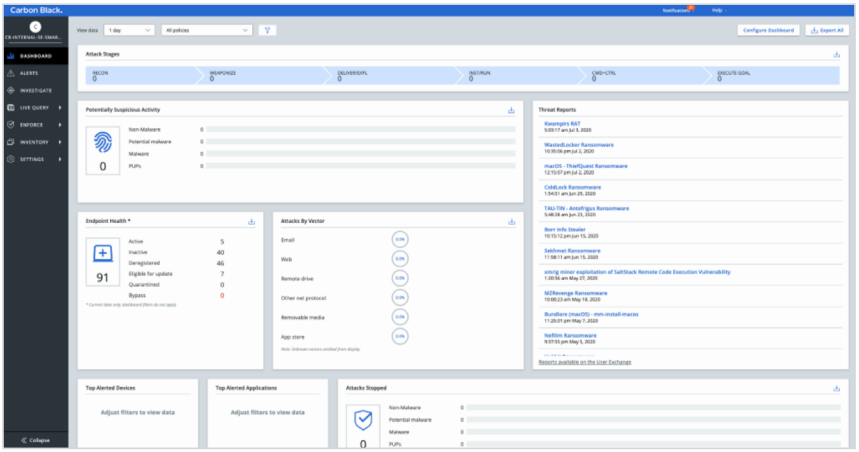
1. Access the VMware Carbon Black Cloud portal.
2. Create a replace AV policy.
3. Configure proxy and internet settings.

Access the VMware Carbon Black Cloud portal:

Administration Account: Check for an email from *noreply@carbonblack.com* to confirm your administrator account.



Once you confirm your account, you will be logged into the VMware Carbon Black Cloud dashboard.

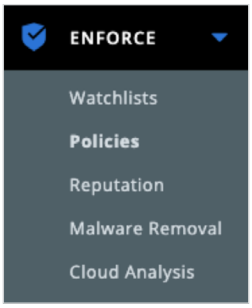


Refer to the "Getting Started" widget on the dashboard for best practices.

Create a replace AV policy

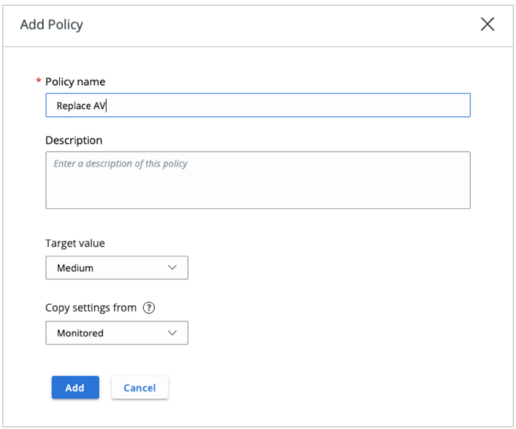
Define a Replace AV Policy: Functionality will include the ability to block known malware as well as anything on the company ban list.

1. Navigate to ENFORCE > Policies on the left panel.



2. Duplicate the monitoring policy in the top right.

3. Define the desired policy name and set the target value to "Medium."



4. Click ‘Add’

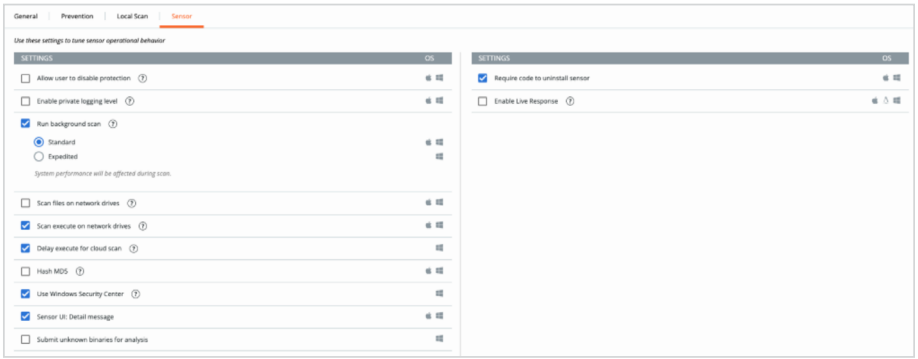
• Configure policy and implement exclusions

Summary of policy configurations:

GENERAL	PREVENTION	GENERAL	PREVENTION
Policy name: Replace AV **Target value:** Medium	**Permissions rules:** Application Path (add path for Symantec AV) – Performs any operation – Bypass **Blocking and isolation rules:** Known malware – Runs or is running – Terminate Application on company banned list – Runs or is running – Terminate	**Scanner Config:** On-Access File Scan Mode: Normal **Signature Updates:** Allow Signature Updates: Enabled	**Run background scan:** Enabled – Standard **Delay execute for cloud scan:** Enabled **Require code to uninstall sensor:** Enabled

Policy settings:

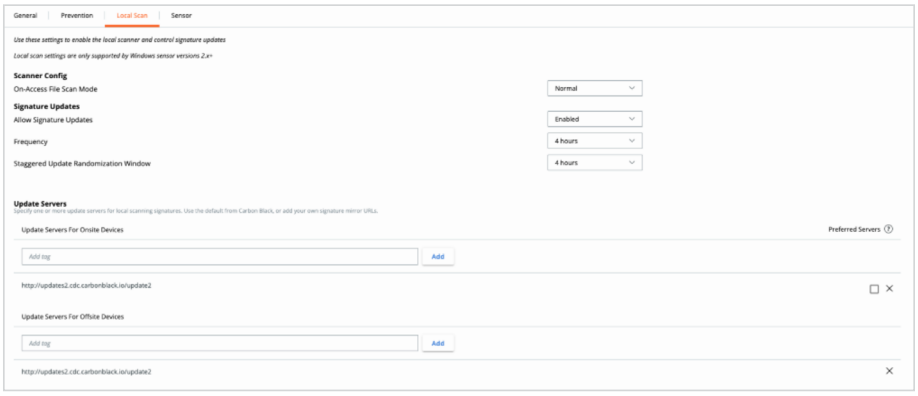
1. Select the newly created AV replacement policy.
2. Select Sensor tab:
   – Enable “Run background scan” and set to “Standard.”
   – Enable “Delay execute for cloud scan.”
   – “Require code to uninstall sensor” for tamper protection.



3. Select Local Scan tab:

– Enable “On-Access File Scan Mode” and set to “Normal.”

– Enable “Allow Signature Updates.”



Prevention:

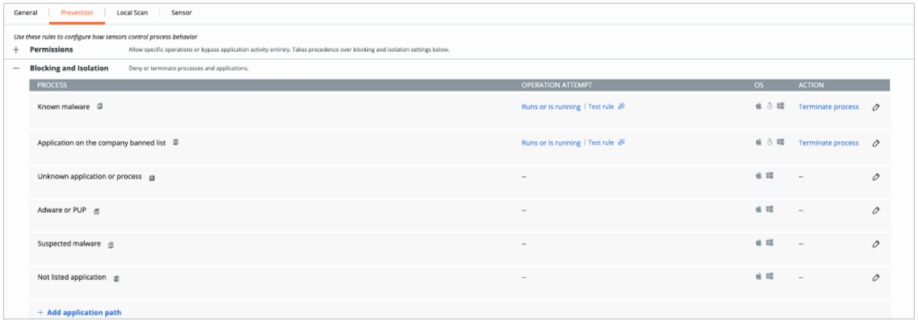
1. Select the newly created AV replacement policy.
2. Select the Prevention tab to define rules to ensure parity with Symantec AV protection. Select the edit button in the far right and add the following rules:

– Known malware – Runs or is running – Terminate

– Application on the company banned list – Runs or is running – Terminate

Note: These rules allow you to block malicious hash values and anything your company has explicitly banned. This ensures comparable protection to what is offered in SEP.

– Click the Save button to confirm



Exclusions/permissions

1. Under the Prevention tab, expand the top Permissions section.
2. Implement AV exclusions into VMware Carbon Black Cloud: To ensure no disruption to the systems co-installed with SEP, we will require permission rules to permit the application to run as usual.

– Click into the "Application(s) at path" field.

3. Enter the AV's recommended file/folder exclusions from the security vendor.

– Set the Operation Attempt to "Performs any operation" and the Action to "Bypass."

– Click Confirm, then Save.

For detailed information, visit: *community.carbonblack.com/t5/Knowledge-Base/CB-Defense-How-to-Set-up-Exclusions-in-the-PSC-Web-Console-for/ta-p/42334*

4. To add the VMware Carbon Black Cloud Endpoint™ Standard sensor as an exclusion to your other security products, use:

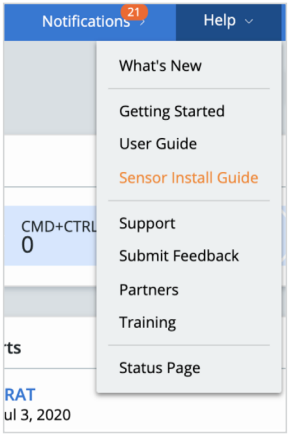
– VMware Carbon Black Cloud Endpoint Standard on Windows: C:\Program Files\Confer\

– VMware Carbon Black Cloud Endpoint Standard on Mac/Linux: /Applications/Confer.app/

– *community.carbonblack.com/t5/Knowledge-Base/Carbon-Black-Endpoint-Standard-How-Can-The-Endpoint-Standard/ta-p/47533*

Internet and connectivity requirements

Please refer to the Sensor installation guide under Help > Sensor Install Guide for communication information, or Help > User Guide > Search Communication and open "Configure Carbon Black Cloud Communications."



Once internet exclusions are set, verify connectivity by running KIRK.

Phase 2: Co-install and baseline with SEP

Now that the replace AV policy has been defined and internet connectivity has been verified, you are ready to begin deploying the VMware Carbon Black Cloud sensor. Once installed, VMware Carbon Black Cloud will perform a compromise assessment to determine if there is any pre-existing malware or suspicious applications within your enterprise.

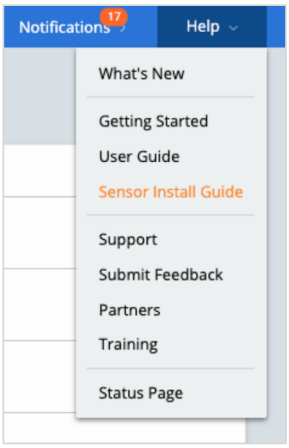
1. Sensor installation

2. Compromise assessment

Installation considerations

Now you are prepared to install the sensor onto your Windows, Mac and Linux systems. Please follow the recommendations outlined in the Sensor Installation Guide. You can also view additional *deployment videos and considerations*.

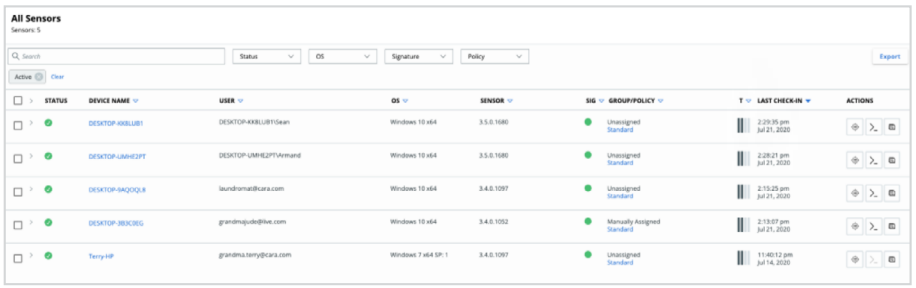
Complete Installation Guide is available under Help > Sensor Installation Guide



We recommend the following parameters for Windows installations.

PARAMETER REQUIREMENTS	VALUE
Group_Name	Replace AV Note: If you created a different name for your policy, please substitute with the correct name.
CLI_Users	S-1-5-18 Note: This is the SID for the local systems. Feel free to substitute with a different security administrator SID.
Company_Code	Available under ENDPOINTS > Sensor Options > Company Codes

2. To verify that endpoints are reporting into the back end navigate to the Endpoints page under the left side Inventory drop-down.



Compromise assessment

No action required. Once deployed, VMware Carbon Black Cloud will initiate the background scan. This will baseline the environment and identify any pre-existing malware on your systems. All identified malware will be surfaced within the VMware Carbon Black Cloud console for review.

Phase 3: Onboard and uninstall SEP

With the VMware Carbon Black Cloud sensors now deployed and the compromise assessment complete, you are ready to begin removing Symantec AV agents. Note: Ensure you are in either the replace AV policy or an equivalent policy to ensure known malware will continue to be blocked on transition.

Uninstall Symantec

1. *Disable Tamper Protection* in Symantec.
2. Delete the uninstall password for Symantec:
   - On your Windows devices, open Registry Editor as an administrator.
   - Go to HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SMC.
   - Look for an entry named **SmcInstData**. Right-click the item, and then choose **Delete**.
3. Remove Symantec from your devices. If you need help with this, see the following Broadcom resources:
   - *Uninstall Symantec Endpoint Protection*
   - Windows devices: *Manually uninstall Endpoint Protection 14 clients on Windows*
   - macOS computers: *Remove Symantec software for Mac using RemoveSymantecMacFiles*
   - Linux devices: *Frequently Asked Questions for Endpoint Protection for Linux*

You have successfully deployed and configured Carbon Black to replace your Symantec AV.