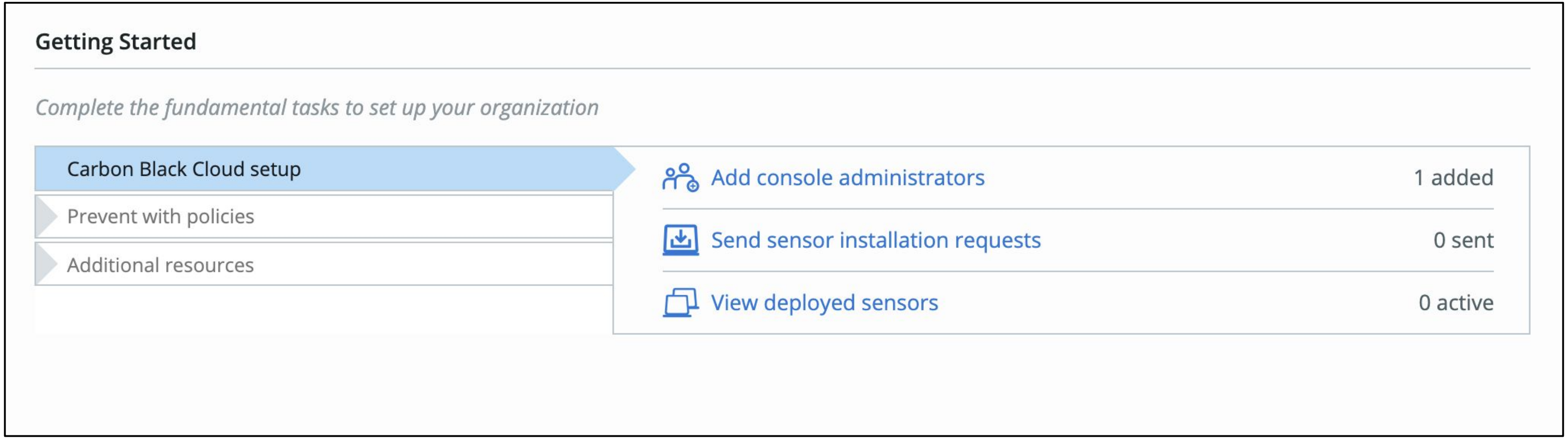
Getting Started with Endpoint Standard

Endpoint Standard uses advanced predictive models to analyze endpoint data and stop attacks before they compromise your system.

Complete the Carbon Black Cloud setup tasks

Before getting started with Endpoint Standard, add console administrators and deploy sensors

Sign in to the Carbon Black Cloud console and follow the **Getting Started** widget to complete these tasks.



Getting Started

Complete the fundamental tasks to set up your organization

Carbon Black Cloud setup

Prevent with policies

Additional resources

Add console administrators	1 added
Send sensor installation requests	0 sent
View deployed sensors	0 active

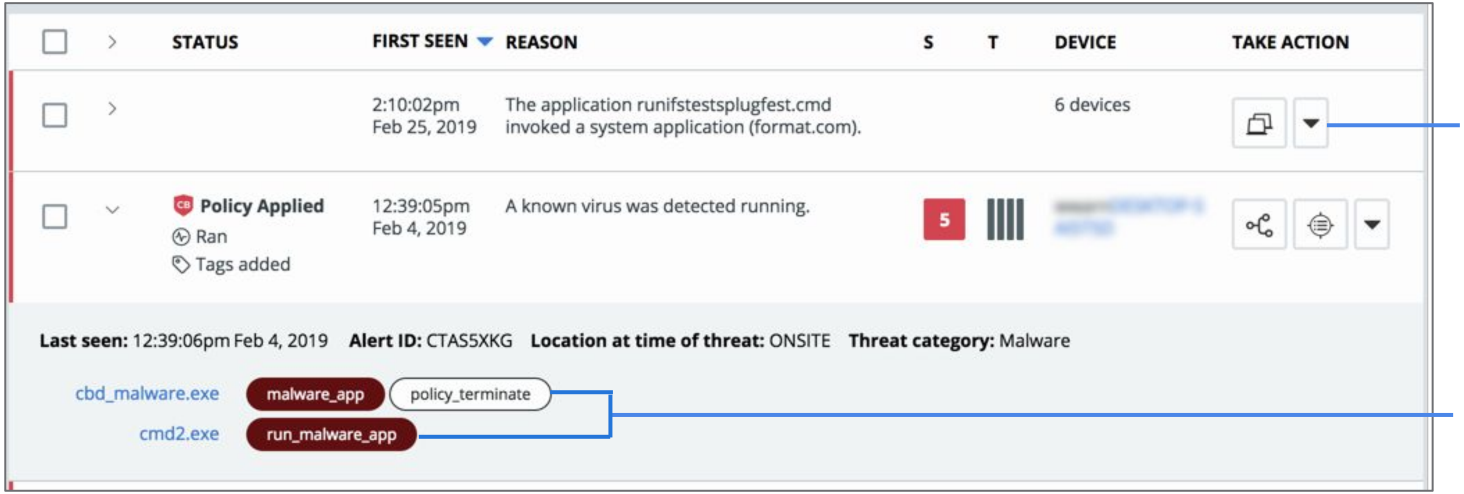
If you don't see the **Getting Started** widget on your dashboard, click **Configure Dashboard** to add it.

1 View alerts

View alerts raised by Endpoint Standard on the Alerts page

Endpoint Standard raises alerts based on suspicious behavior and known threats. Regularly review alerts to distinguish between normal activity and an attack. Use the left panel to filter alerts by severity, policies, devices, and more.

Click the **Alert Triage** icon (⋲) to see the flow of an event.



□	›	STATUS	FIRST SEEN ▾	REASON	S	T	DEVICE	TAKE ACTION
□	›		2:10:02pm Feb 25, 2019	The application runifstestsplugfest.cmd invoked a system application (format.com).			6 devices	⧉ ▾
□	⌄	Policy Applied Ran Tags added	12:39:05pm Feb 4, 2019	A known virus was detected running.	5	▮▮▮▮	[redacted]	⋲ ⊕ ▾

Last seen: 12:39:06pm Feb 4, 2019 **Alert ID:** CTAS5XKG **Location at time of threat:** ONSITE **Threat category:** Malware

cbd_malware.exe malware_app policy_terminate

cmd2.exe run_malware_app

Dismiss an alert or view notification history

Tactics, Techniques, and Procedures (TTPs) are descriptors used to provide context on attack and suspicious behavior methods. For additional information, click **Help > User Guide.**

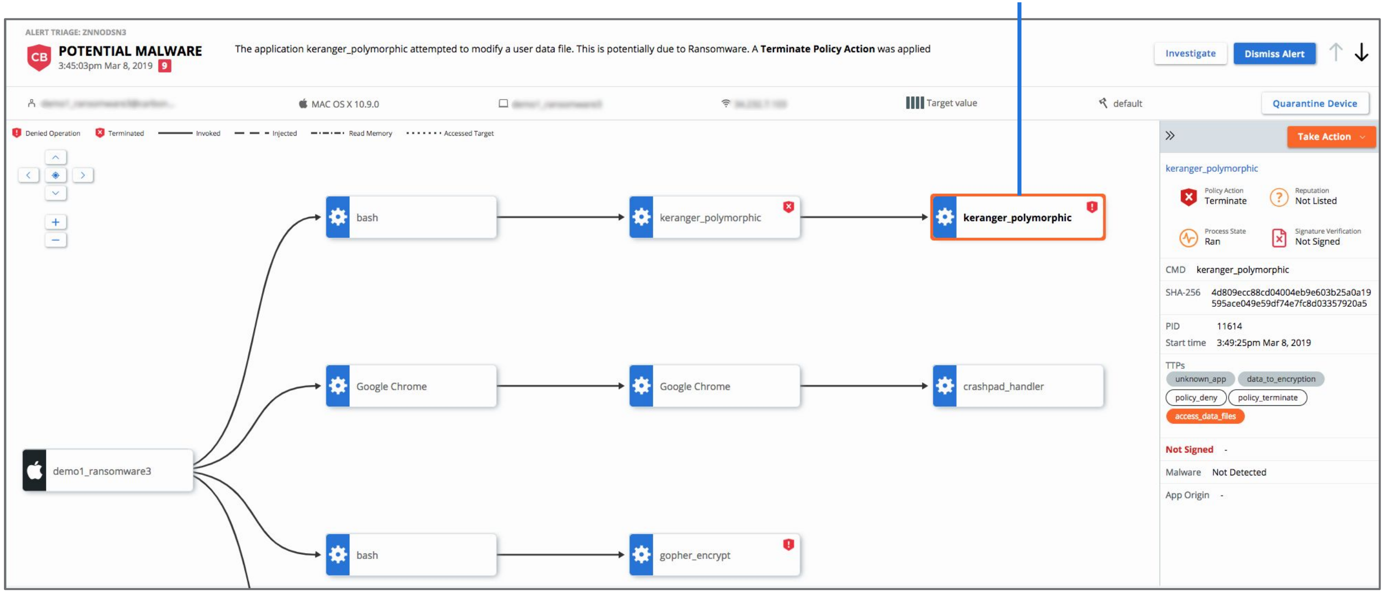
2 Triage alerts

On the Triage Alert page, view the process tree and select events, or nodes, to see more information

The right panel provides a summary of attributes of the selected node, including Policy Action, Reputation, and Process State. If you also have CB ThreatHunter, you'll see some alternate information.

To investigate an alert further, click **Investigate**.

A **Terminate Policy Action** was applied here because an application without an Allow List reputation attempted to modify a user data file



ALERT TRIAGE: ZNNODSN3

POTENTIAL MALWARE
3:45:03pm Mar 8, 2019 9

The application keranger_polymorphic attempted to modify a user data file. This is potentially due to Ransomware. A **Terminate Policy Action** was applied

[redacted] MAC OS X 10.9.0 [redacted] [redacted] Target value default

keranger_polymorphic

Policy Action: Terminate
Reputation: Not Listed
Process State: Ran
Signature Verification: Not Signed

CMD keranger_polymorphic

SHA-256 4d809ecc88cd04004eb9e603b25a0a19595ace049e59df74e7fc8d03357920a5

PID 11614

Start time 3:49:25pm Mar 8, 2019

TTPs: unknown_app, data_to_encryption, policy_deny, policy_terminate, access_data_files

Not Signed -

Malware Not Detected

App Origin -

🟥 = Deny

☒ = Terminate

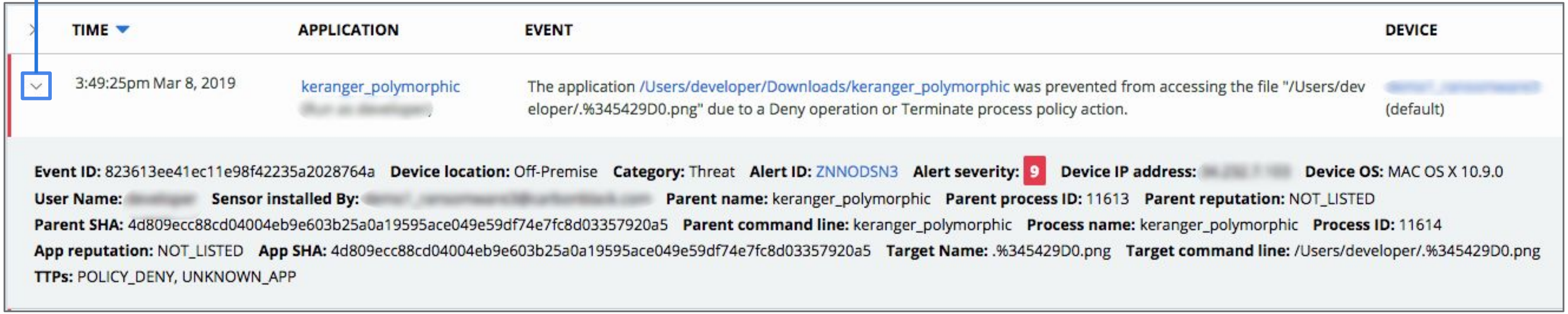
3 Investigate alerts

On the Investigate page, view more details about an event

Use the left panel to filter the events by devices, connection locations, applications, and alerts.

You can view additional details about an event such as the file or application hash, parent and child processes, network connections, command line arguments, TTPs, and file reputation, which is based on cloud threat intelligence.
Click **Help > User Guide** to learn more about file reputation.

Click to expand the information window



TIME	APPLICATION	EVENT	DEVICE
3:49:25pm Mar 8, 2019	keranger_polymorphic [redacted]	The application /Users/developer/Downloads/keranger_polymorphic was prevented from accessing the file "/Users/developer/.%345429D0.png" due to a Deny operation or Terminate process policy action.	[redacted] (default)

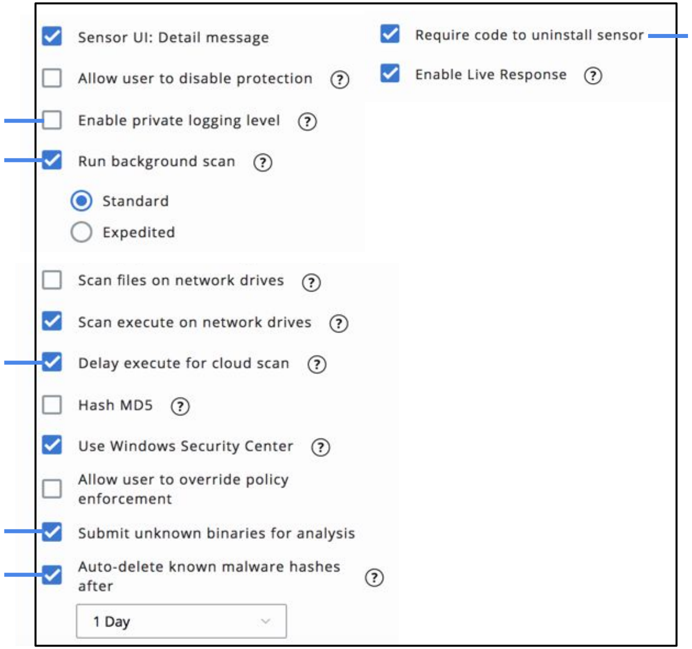
Event ID: 823613ee41ec11e98f42235a2028764a **Device location:** Off-Premise **Category:** Threat **Alert ID:** ZNNODSN3 **Alert severity:** 9 **Device IP address:** [redacted] **Device OS:** MAC OS X 10.9.0
User Name: [redacted] **Sensor installed By:** [redacted] **Parent name:** keranger_polymorphic **Parent process ID:** 11613 **Parent reputation:** NOT_LISTED
Parent SHA: 4d809ecc88cd04004eb9e603b25a0a19595ace049e59df74e7fc8d03357920a5 **Parent command line:** keranger_polymorphic **Process name:** keranger_polymorphic **Process ID:** 11614
App reputation: NOT_LISTED **App SHA:** 4d809ecc88cd04004eb9e603b25a0a19595ace049e59df74e7fc8d03357920a5 **Target Name:** .%345429D0.png **Target command line:** /Users/developer/.%345429D0.png
TTPs: POLICY_DENY, UNKNOWN_APP

4 Set policies as recommended

Fine-tune your policies to meet your organization's security needs

Policies define rules for how applications behave on endpoints. Use predefined policies or create custom ones by clicking **Enforce**, then **Policies**. In the **Prevention** tab, ensure that all policies block all types of malware from executing known, suspect, and potentially unwanted programs (PUPs). Adjust your policies based on our recommended settings below.

Sensor tab



- ☑ Sensor UI: Detail message
- □ Allow user to disable protection ?
- □ Enable private logging level ?
- ☑ Run background scan ?
  - ● Standard
  - ○ Expedited
- □ Scan files on network drives ?
- ☑ Scan execute on network drives ?
- ☑ Delay execute for cloud scan ?
- □ Hash MD5 ?
- ☑ Use Windows Security Center ?
- □ Allow user to override policy enforcement
- ☑ Submit unknown binaries for analysis
- ☑ Auto-delete known malware hashes after ?
  - 1 Day
- ☑ Require code to uninstall sensor
- ☑ Enable Live Response ?

Unless required, do not enable

Perform an initial, one-time inventory scan to identify pre-existing malware

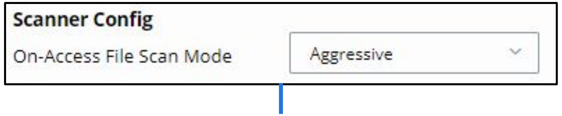
Request updated reputation data from the cloud; effective against emerging threats

Enable cloud analysis

Enable auto-delete of known malware

To prevent unwanted uninstalls and malware from tampering with sensor connectivity, enable this setting for each policy

Local Scan tab



Scanner Config

On-Access File Scan Mode: Aggressive

Test this setting on a subset of policies first to ensure machine performance isn't greatly impacted

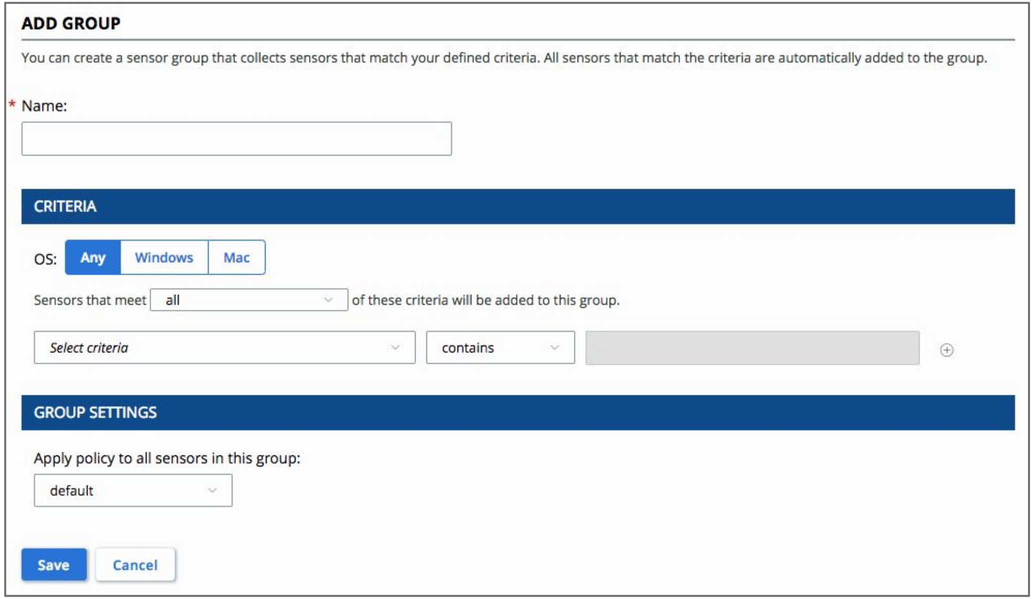
5 Create sensor groups

Before you roll out Endpoint Standard to your whole organization, you can create sensor groups to manage sensors and policies across different teams within your organization, such as Sales, Finance, IT, and Engineering. For example, you might define a sensor group as the Active Directory Finance Organizational Unit.

To create a sensor group, click **Endpoints**, then **+ Add Group**.

Customize policies based on how your teams work and what level of security is required. Then, associate a policy with a sensor group.

New endpoints in a sensor group are automatically protected by the policy that is associated with the sensor group.



ADD GROUP

You can create a sensor group that collects sensors that match your defined criteria. All sensors that match the criteria are automatically added to the group.

* Name:

CRITERIA

OS: Any | Windows | Mac

Sensors that meet all of these criteria will be added to this group.

Select criteria | contains

GROUP SETTINGS

Apply policy to all sensors in this group:

default

Carbon Black.

Next Steps

Learn more about Endpoint Standard and the Carbon Black Cloud

Connect with the Carbon Black User Exchange for additional resources, including product documentation, release notes, knowledge base articles, support, discussions, product news, updates, and more.

Learn more about Endpoint Standard by taking a Carbon Black training course.