



CROWDSTRIKE

Getting Started Guide:
**CrowdStrike: Falcon Endpoint
Protection Enterprise Solution**



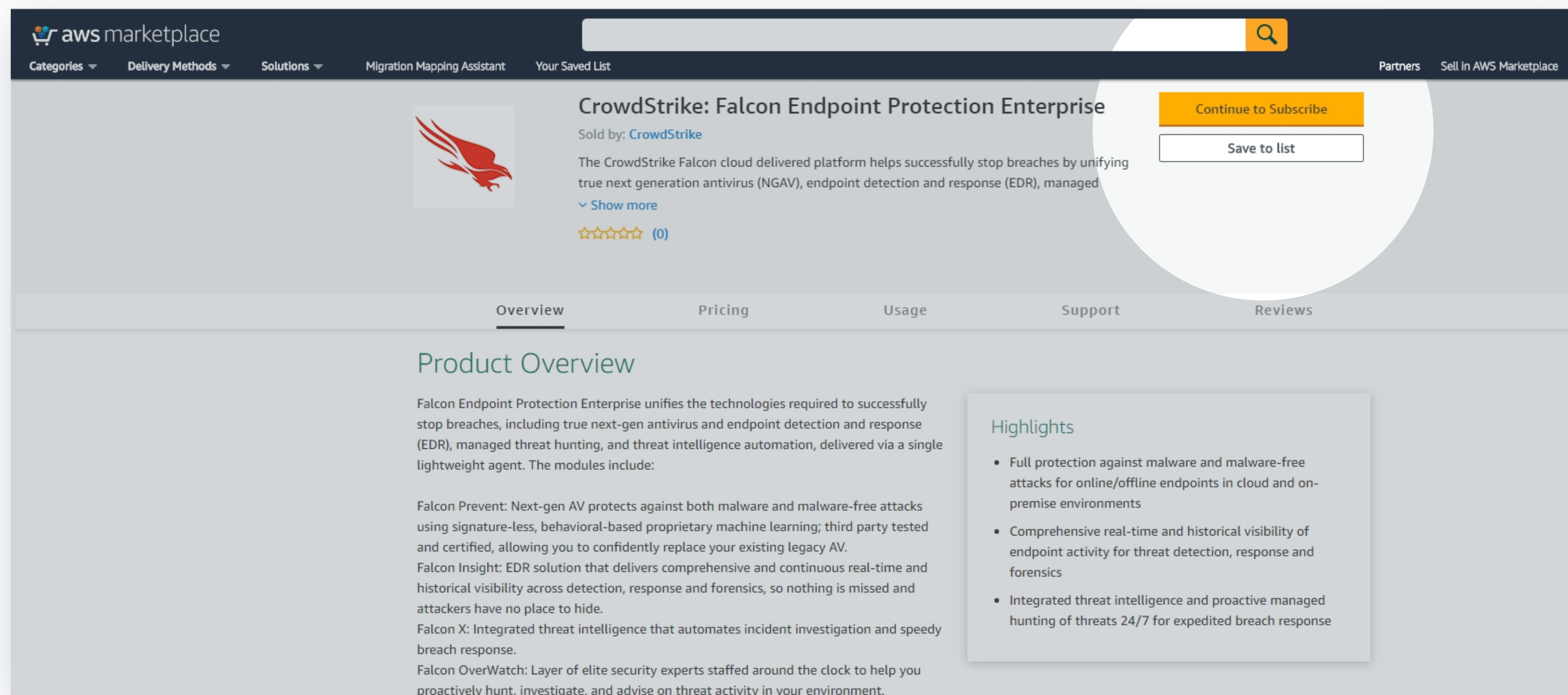
The **CrowdStrike Falcon Endpoint Protection** solution is found in the AWS Marketplace and offers the following key benefits:

- Full protection against malware and malware-free attacks for online and offline endpoints in cloud and on-premise environments.
- Comprehensive real-time and historical visibility of endpoint activity for threat detection, response, and forensics, with integrated threat intelligence and proactive threat hunting.
- Full visibility into all managed endpoints and unmanaged assets across all accounts for improved security and IT hygiene.

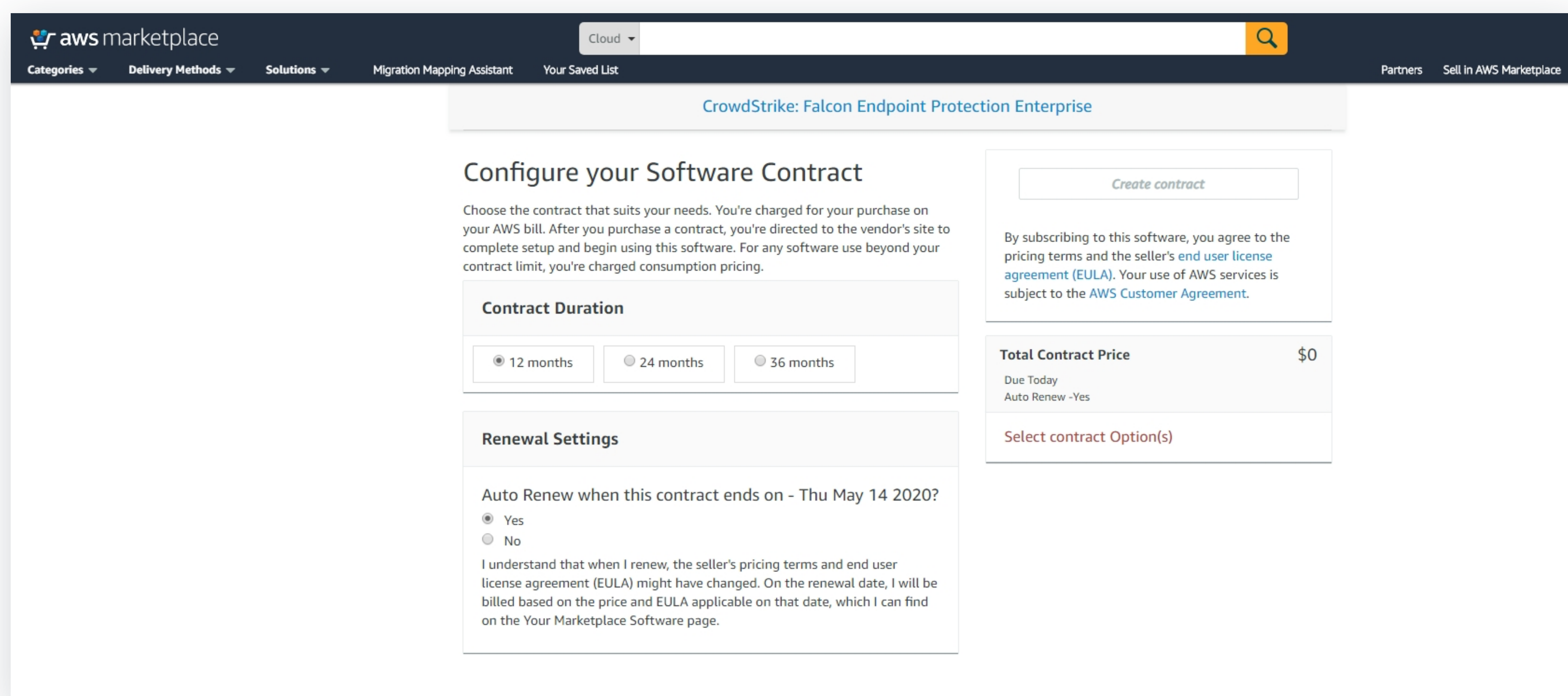


Step 1 Locate **CrowdStrike Falcon Endpoint Protection** solution in the AWS Marketplace.

Step 2 Click the **Continue to Subscribe** button.

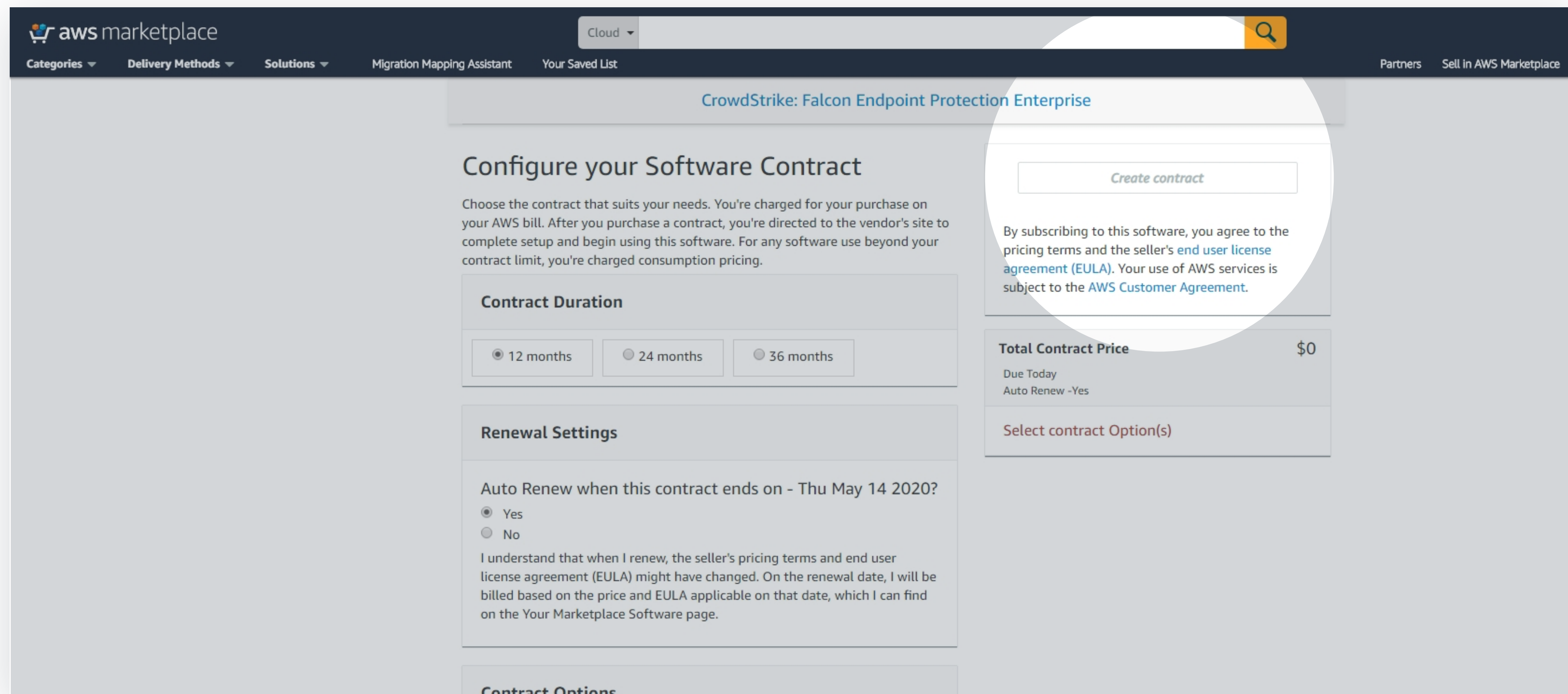


Step 3 Next, select the appropriate contract duration and options for your organization.



Step 4 of 17

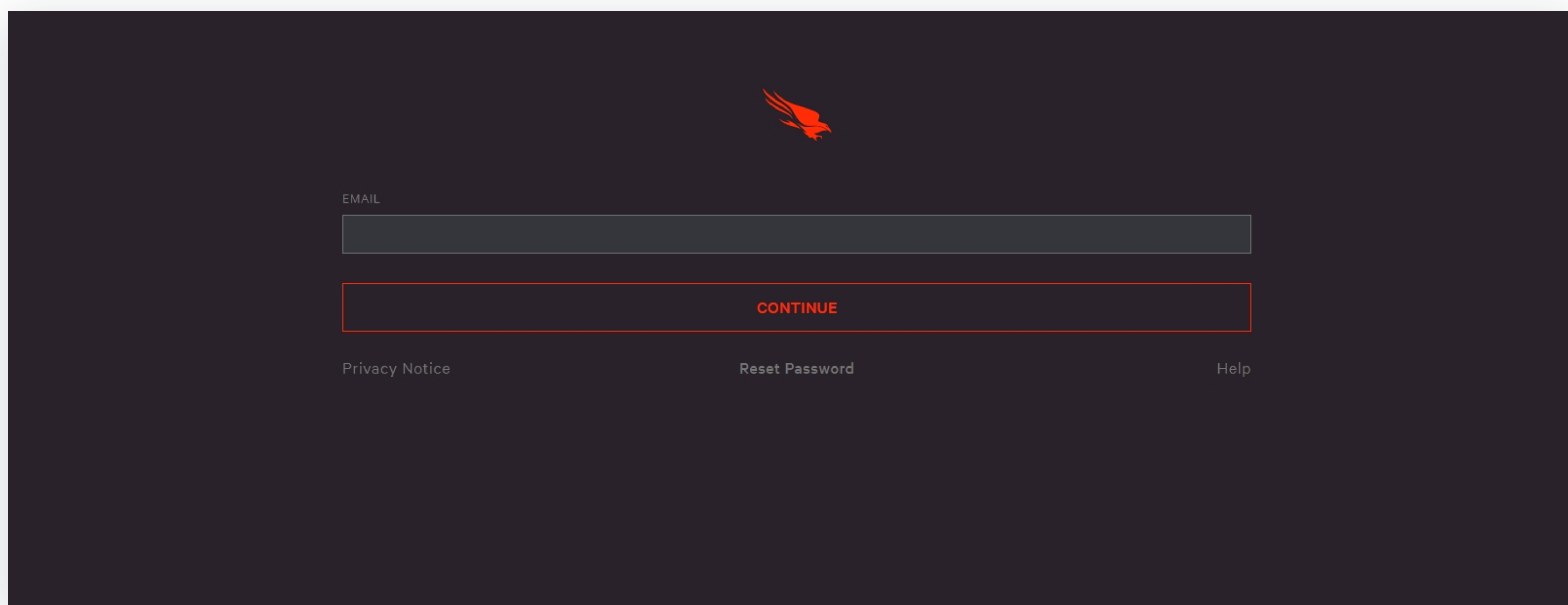
Step 4 Next, select the **Create Contract** button to subscribe to the CrowdStrike Falcon Endpoint Protection solution.



Creating a Policy in the CrowdStrike Falcon Endpoint Protection Solution

Step 5 Once you have subscribed to the CrowdStrike Falcon Endpoint Protection solution and registered, you will be provided with a login URL.

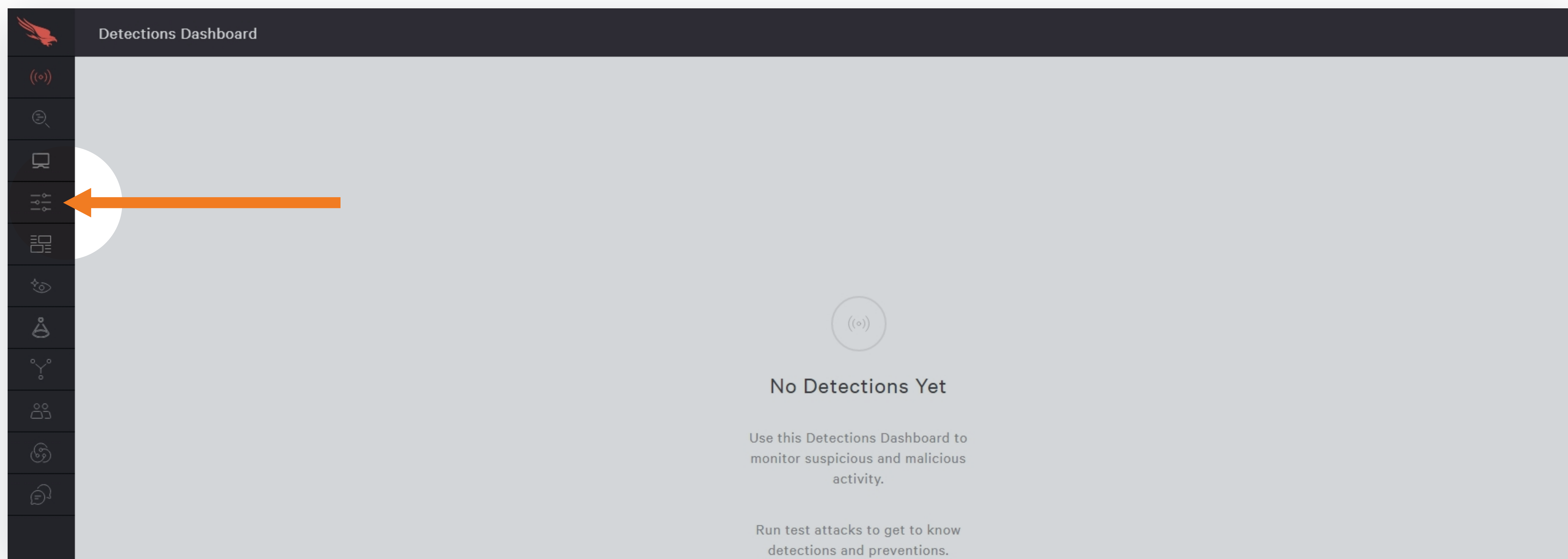
Step 6 At the login page, enter your **email** (the email you used for registration), click **Continue**, and then **enter your password**.



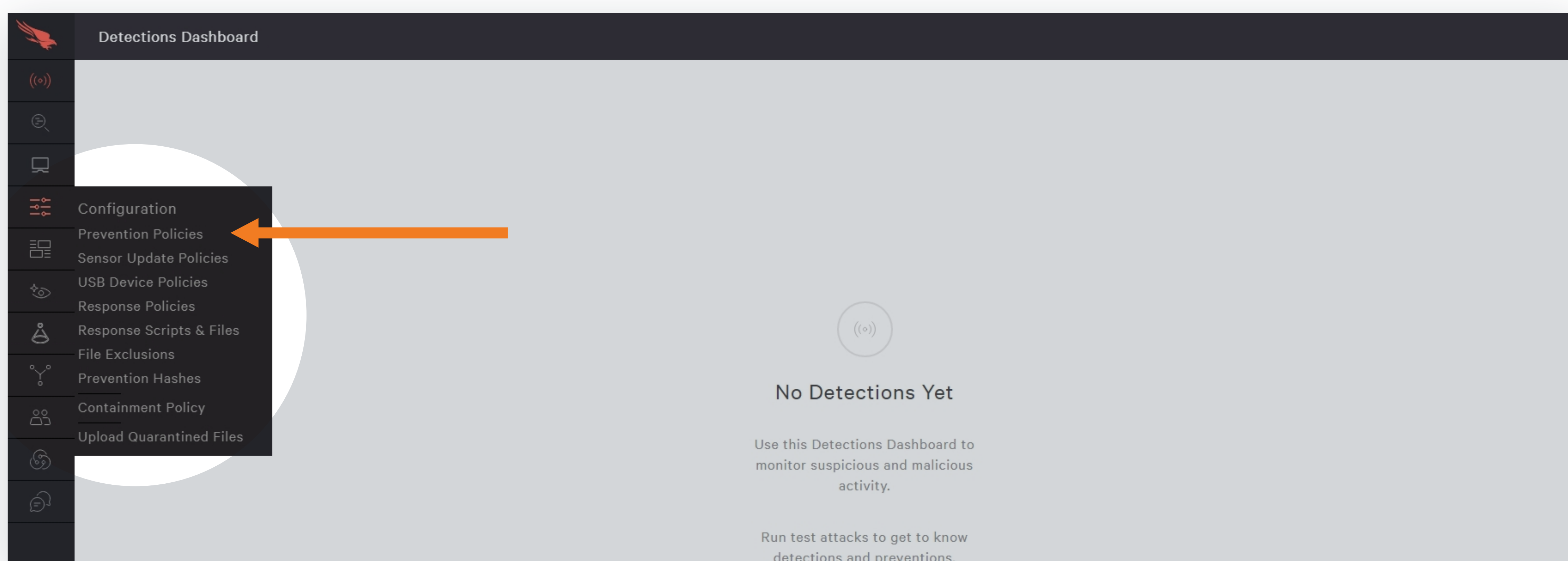
Step 7 Next, you will be taken into the dashboard of the CrowdStrike Falcon Endpoint Protection solution.

Steps 8-10 of 17

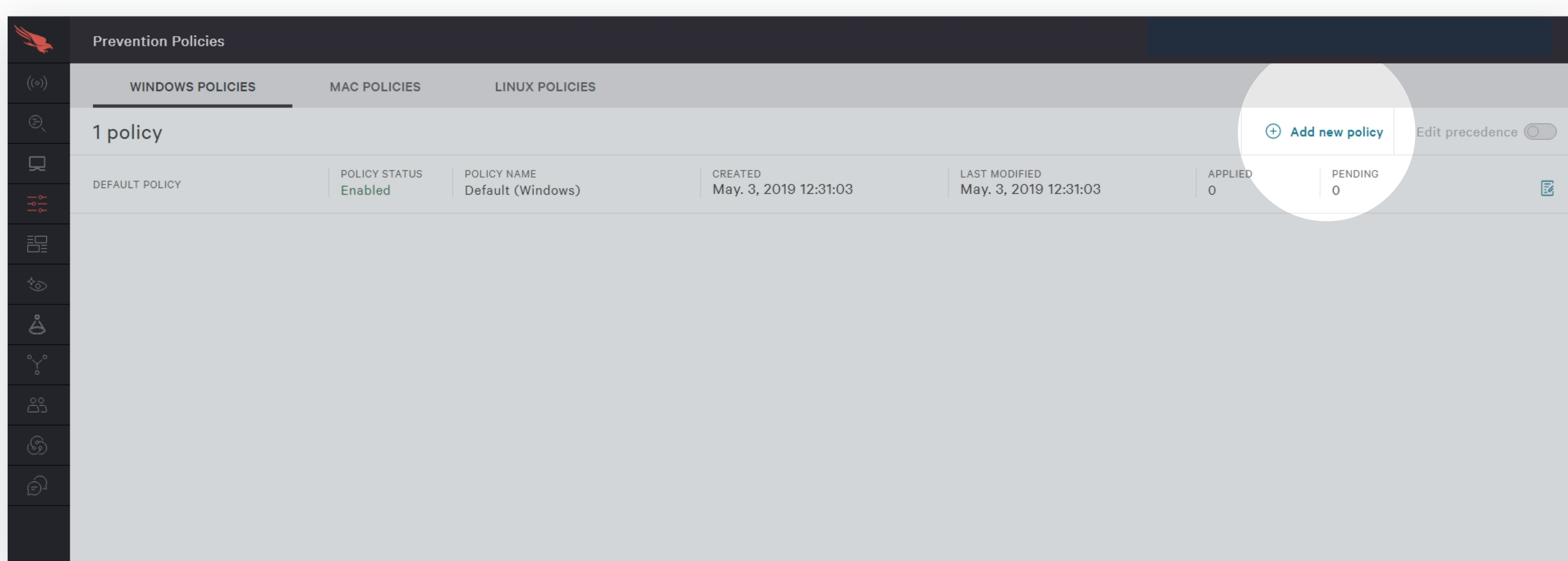
Step 8 On the left-side of the dashboard, select the **menu icon** with three lines.



Step 9 Next, select the **Prevention Policies** option from the menu.

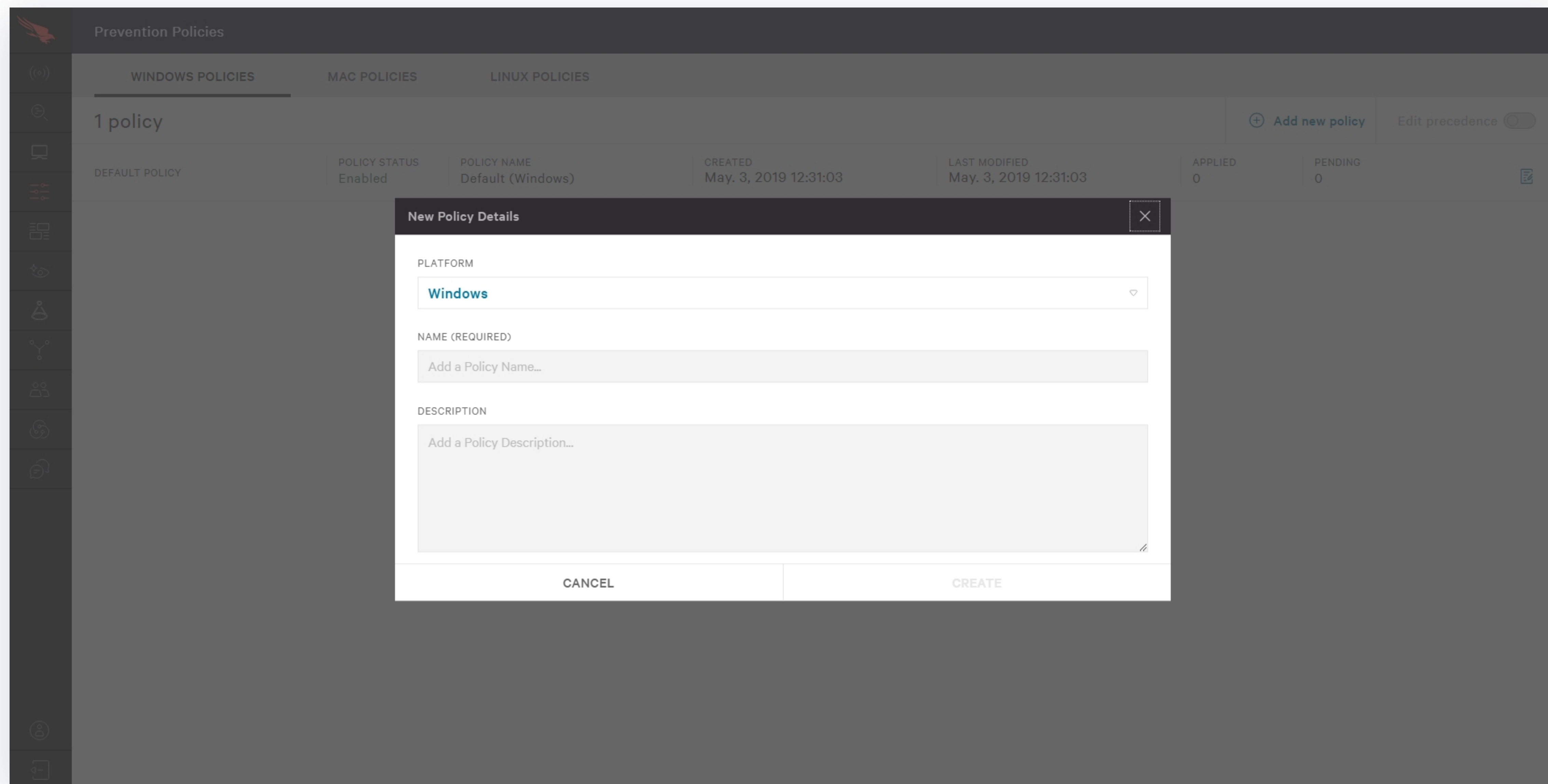


Step 10 Next, you will be taken to the Prevention Policies page and may see some default policies created. Select the **Add new policy** option to create a new policy.

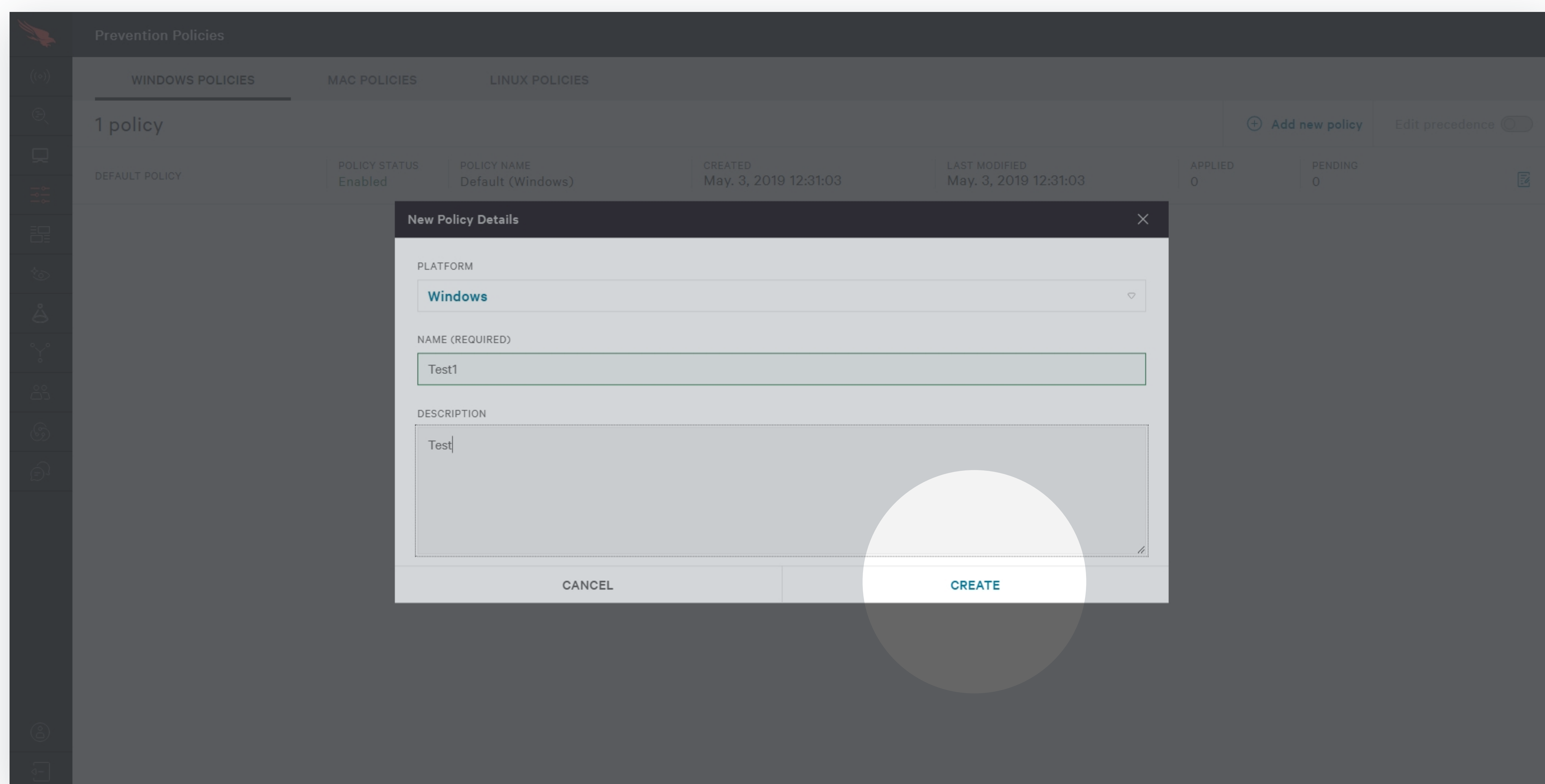


Steps 11-12 of 17

Step 11 Next, you will be able to name your policy and add an optional description of the policy. In this example, let's name the policy Test1 and adding a description of "Test."

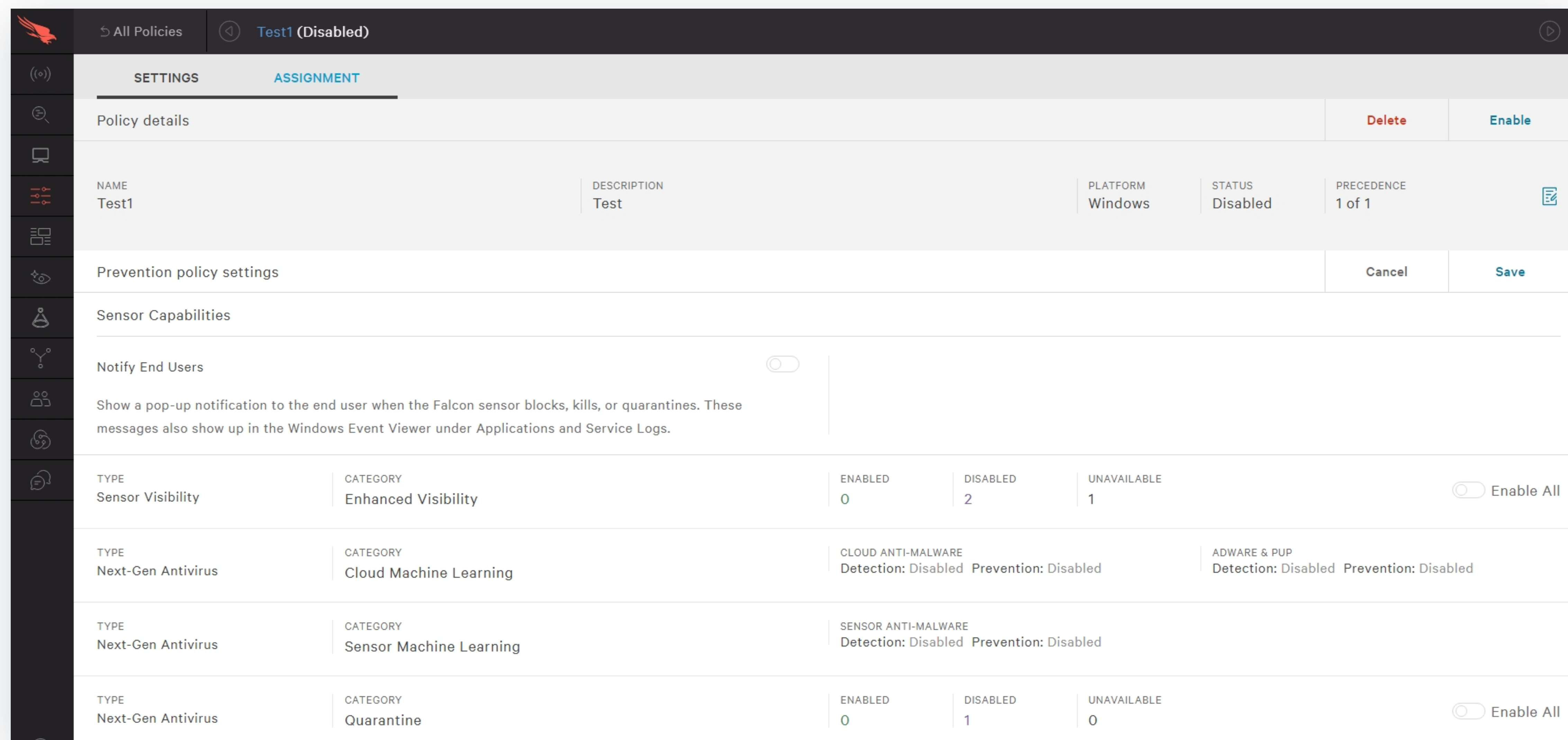


Step 12 After you have named your policy, click the **Create** button.

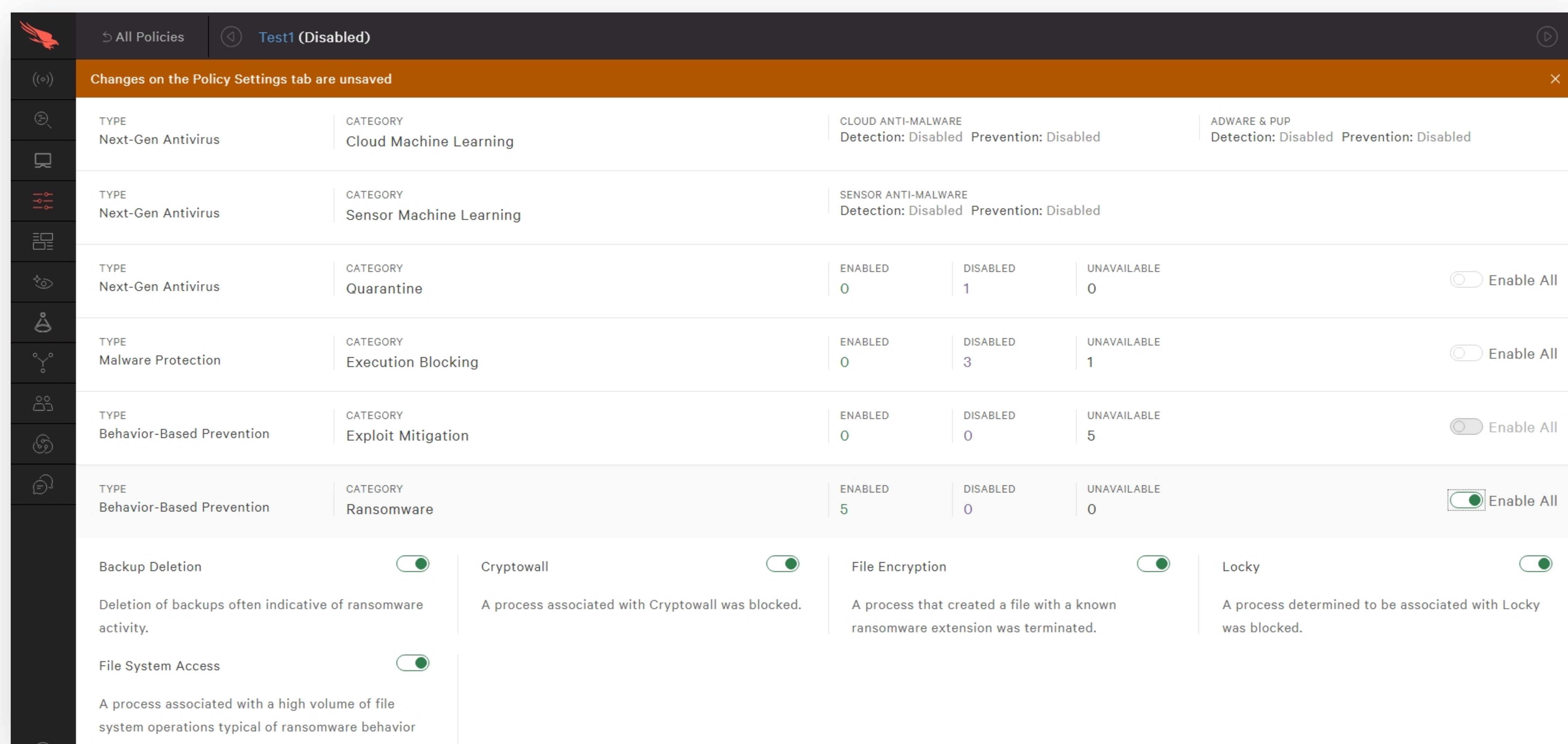


Steps 13-14 of 17

Step 13 Next, you are taken into the policy itself, where you can select the action items to enable.

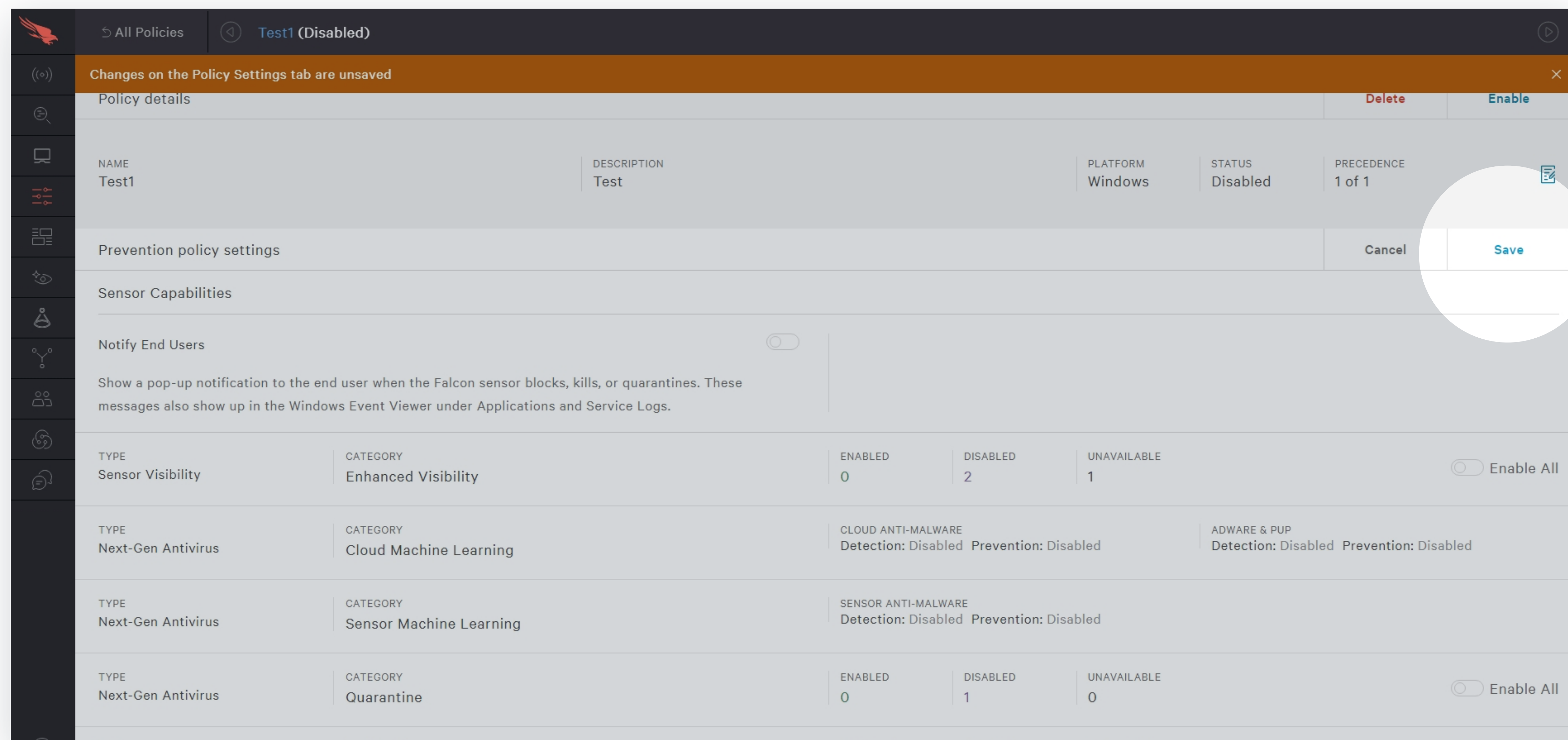


Step 14 In this example, I have selected to enable the ransomware protection.

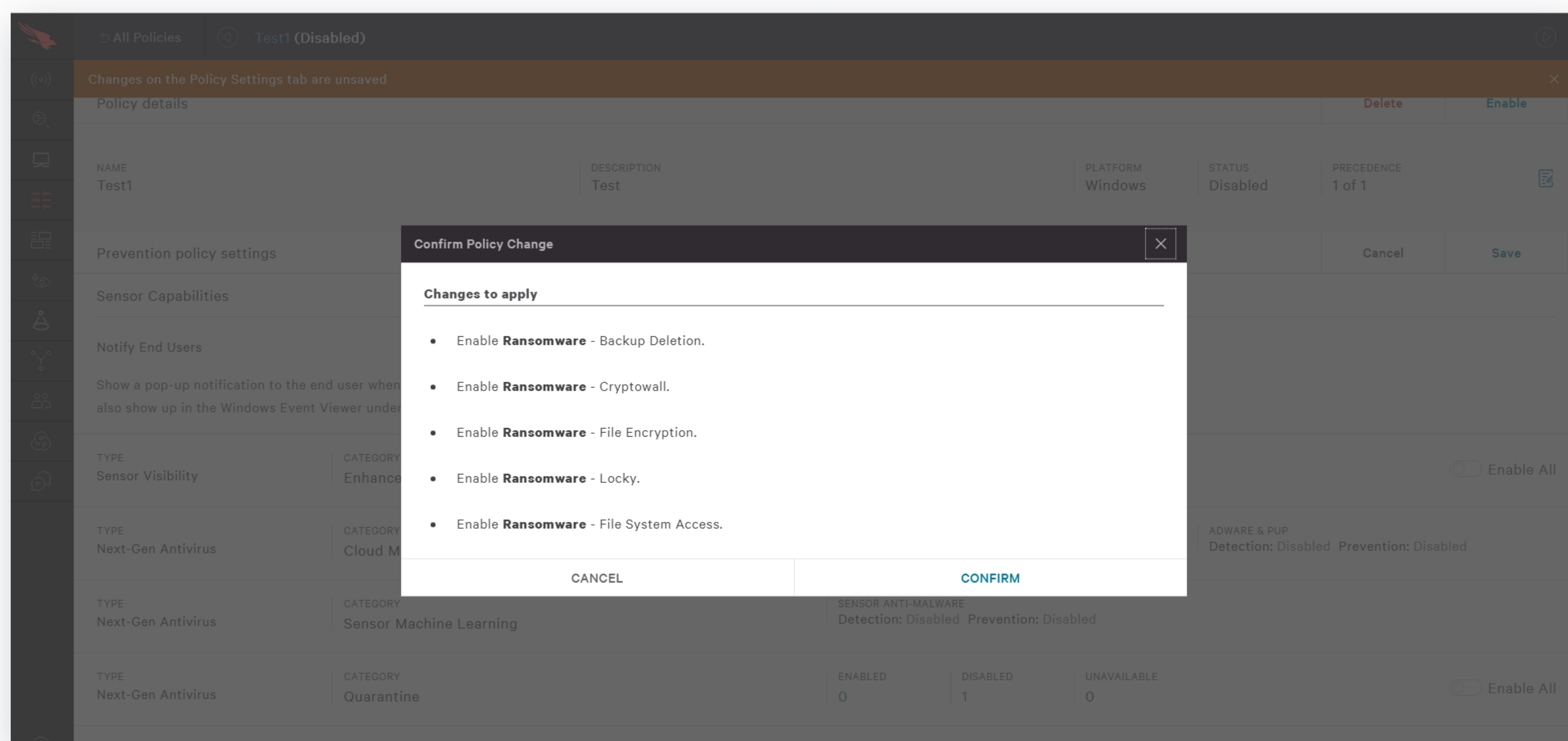


Step 15-16 of 17

Step 15 Next, click the Save button at the top-right to save any changes you have made to the policy.

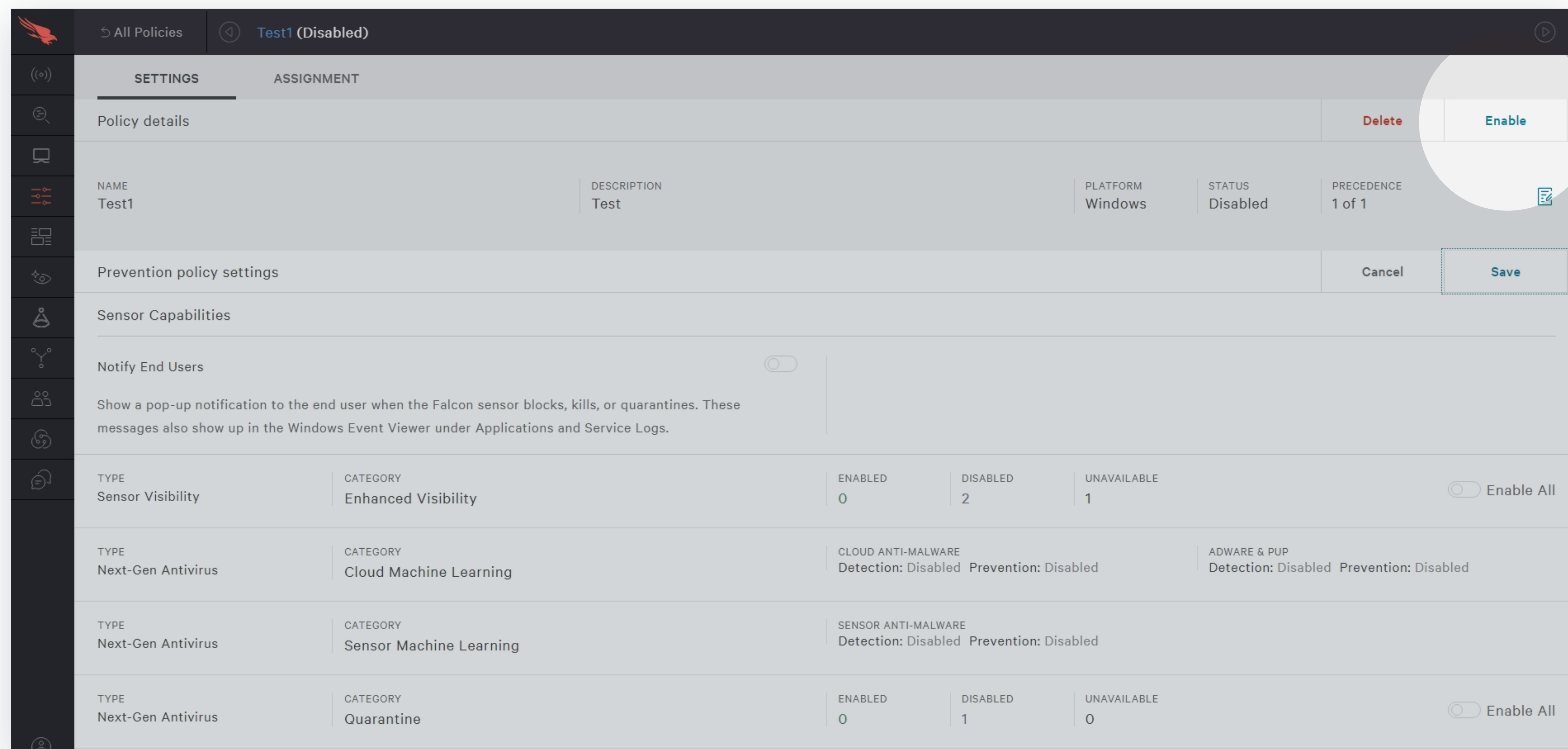


Step 16 You will be asked to review and confirm the changes.



Step 17 of 17

Step 17 Once you have saved the changes, you will then be able to Enable the new policy by selecting the **Enable** option at the top-right of the page.



The screenshot displays the AWS IAM console interface for a policy named 'Test1 (Disabled)'. The page is divided into 'SETTINGS' and 'ASSIGNMENT' tabs. The 'Policy details' section shows the policy name 'Test1', description 'Test', platform 'Windows', status 'Disabled', and precedence '1 of 1'. The 'Prevention policy settings' section includes a 'Notify End Users' toggle and a 'Save' button. The 'Sensor Capabilities' section lists various sensors with their status (Enabled, Disabled, Unavailable) and an 'Enable All' toggle. The 'Test1 (Disabled)' button is highlighted in the top right corner.

NAME	DESCRIPTION	PLATFORM	STATUS	PRECEDENCE
Test1	Test	Windows	Disabled	1 of 1

TYPE	CATEGORY	ENABLED	DISABLED	UNAVAILABLE	Enable All
Sensor Visibility	Enhanced Visibility	0	2	1	<input type="checkbox"/>
Next-Gen Antivirus	Cloud Machine Learning	CLOUD ANTI-MALWARE Detection: Disabled Prevention: Disabled		ADWARE & PUP Detection: Disabled Prevention: Disabled	
Next-Gen Antivirus	Sensor Machine Learning	SENSOR ANTI-MALWARE Detection: Disabled Prevention: Disabled			
Next-Gen Antivirus	Quarantine	0	1	0	<input type="checkbox"/>

Complete

Thank you.

For more information, visit amzn.to/2Fjlf1A

