

### In cooperation with CYBRARY



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



### In cooperation with CYBRARY

# 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.



### In cooperation with CYBRARY

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

С

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

🖅 aws marketolace

?r aws n	narketplace									
tegories 👻	Delivery Methods 👻	Solutions 👻	Migration Mapping Assistant Y	our Saved List					Partners	Sell in AWS Marketplace
				Sold by: CrowdStrike The CrowdStrike Falco	: Falcon Endpoint on cloud delivered platform h antivirus (NGAV), endpoint de	elps successfully stop breac	hes by unifying	Continue to Subscribe Save to list		
			Overv	iew P	Pricing	Usage	Support	Reviews		

#### Product Overview

Falcon Endpoint Protection Enterprise unifies the technologies required to successfully stop breaches, including true next-gen antivirus and endpoint detection and response (EDR), managed threat hunting, and threat intelligence automation, delivered via a single lightweight agent. The modules include:

Falcon Prevent: Next-gen AV protects against both malware and malware-free attacks using signature-less, behavioral-based proprietary machine learning; third party tested and certified, allowing you to confidently replace your existing legacy AV. Falcon Insight: EDR solution that delivers comprehensive and continuous real-time and historical visibility across detection, response and forensics, so nothing is missed and attackers have no place to hide.

Falcon X: Integrated threat intelligence that automates incident investigation and speedy breach response.

Falcon OverWatch: Layer of elite security experts staffed around the clock to help you proactively hunt, investigate, and advise on threat activity in your environment.

#### Highlights

- Full protection against malware and malware-free attacks for online/offline endpoints in cloud and onpremise environments
- Comprehensive real-time and historical visibility of endpoint activity for threat detection, response and forensics
- Integrated threat intelligence and proactive managed hunting of threats 24/7 for expedited breach response

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

🐓 aws marketplace	Cloud 👻		
Categories 👻 Delivery Methods 💌 Solutions 💌	Migration Mapping Assistant Your Saved List		Partners Sell in AWS Marketplace
	CrowdStrike: Falcon Endpoint Prote	ction Enterprise	
	Configure your Software Contract Choose the contract that suits your needs. You're charged for your purchase on your AWS bill. After you purchase a contract, you're directed to the vendor's site to complete setup and begin using this software. For any software use beyond your contract limit, you're charged consumption pricing.	Create contract By subscribing to this software, you agree to the pricing terms and the seller's end user license	
	Contract Duration     12 months     24 months     36 months	agreement (EULA). Your use of AWS services is subject to the AWS Customer Agreement. Total Contract Price \$0	
	Renewal Settings	Due Today Auto Renew -Yes Select contract Option(s)	
	<ul> <li>Auto Renew when this contract ends on - Thu May 14 2020?</li> <li>Yes</li> <li>No</li> <li>I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find</li> </ul>		

#### **Step 4** of 17

### In cooperation with CYBRARY

# Step 4Next, select the Create Contract button to subscribe to the CrowdStrike FalconIndpoint Protection solution.

cor

👯 aws n	narketplace			Cloud -		Q		
Categories 🔻	Delivery Methods 👻	Solutions 👻	Migration Mapping Assistant	Your Saved List			Partners	Sell in AWS Marketplace
				CrowdStrike: Falcon Endpoint Prot	ection Enterprise			
			Config	jure your Software Contract	Create cont	tract		
			your AWS bil	contract that suits your needs. You're charged for your purchase on II. After you purchase a contract, you're directed to the vendor's site to	By subscribing to this softwar	re, you agree to the		

itract limit, you're charged consumption pricing.	pricing terms and the seller's end user license agreement (EULA). Your use of AWS services is
Contract Duration	subject to the AWS Customer Agreement.
I2 months	Total Contract Price\$0Due Today Auto Renew -Yes
Renewal Settings	Select contract Option(s)
Auto Renew when this contract ends on - Thu May 14 2020? • Yes • No	
I understand that when I renew, the seller's pricing terms and end user license agreement (EULA) might have changed. On the renewal date, I will be billed based on the price and EULA applicable on that date, which I can find on the Your Marketplace Software page.	
Contract Options	

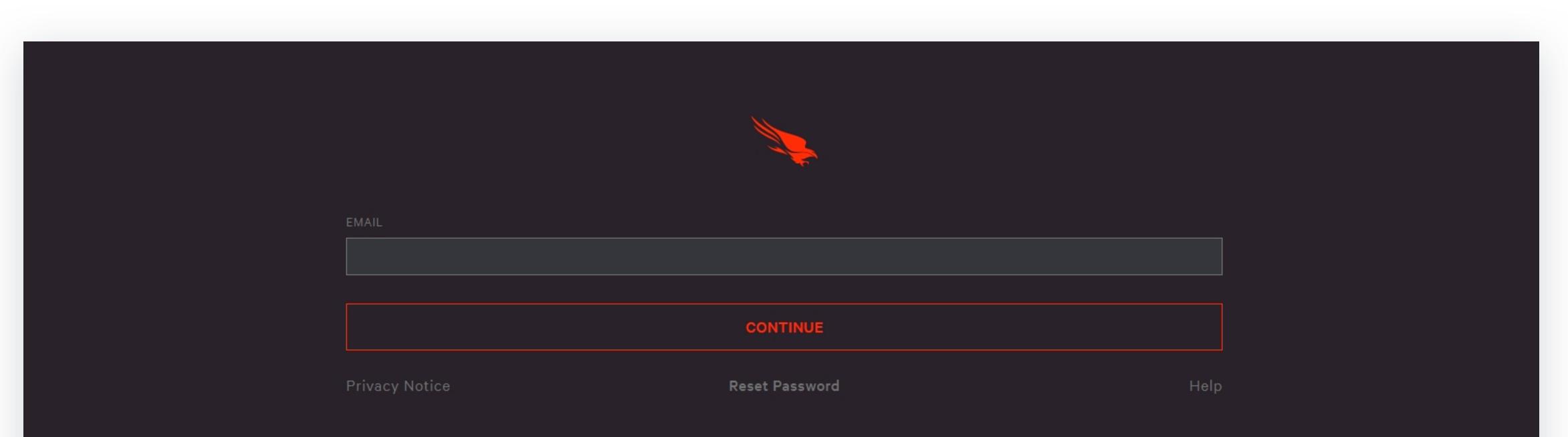
#### **Steps 5-7** of 17

### In cooperation with CYBRARY

### **Creating a Policy** in the CrowdStrike Falcon Endpoint Protection Solution

Step 5Once you have subscribed to the CrowdStrike Falcon Endpoint Protectionsolution 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), clickContinue, and then enter your password.



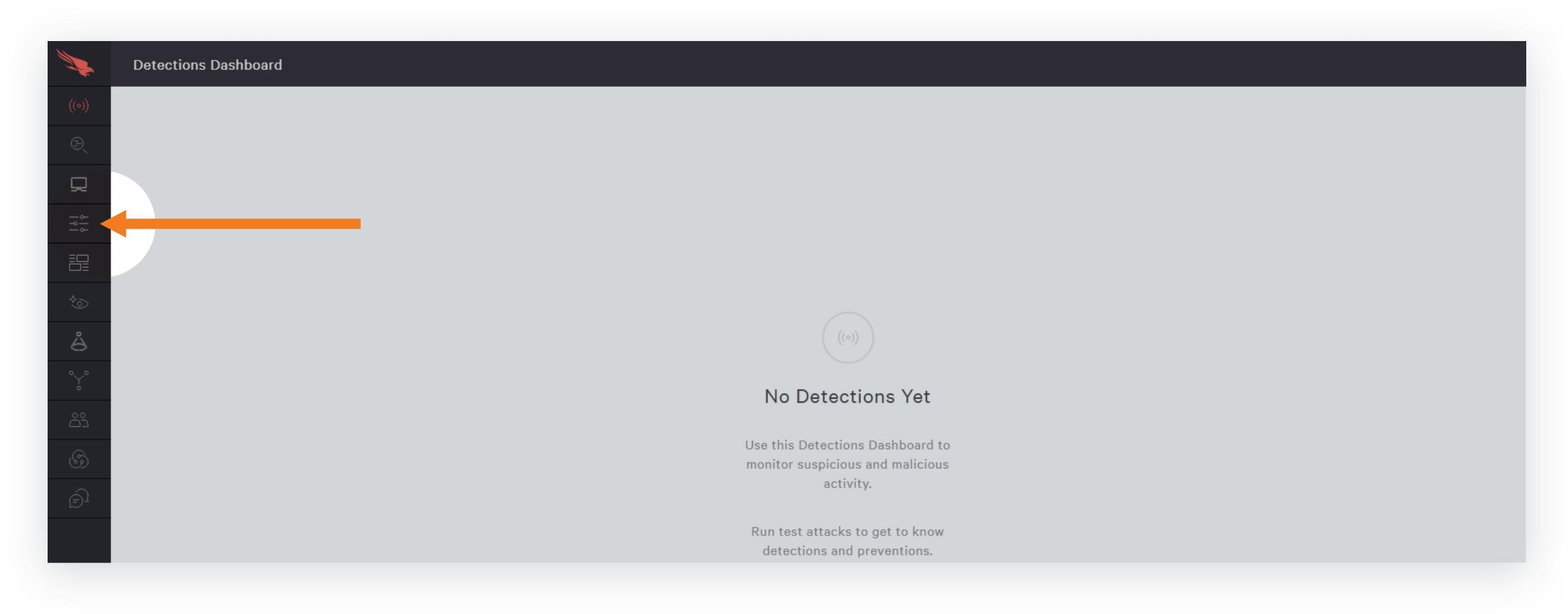
Step 7Next, you will be taken into the dashboard of the CrowdStrike Falcon EndpointProtection solution.

Q

#### **Steps 8-10** of 17

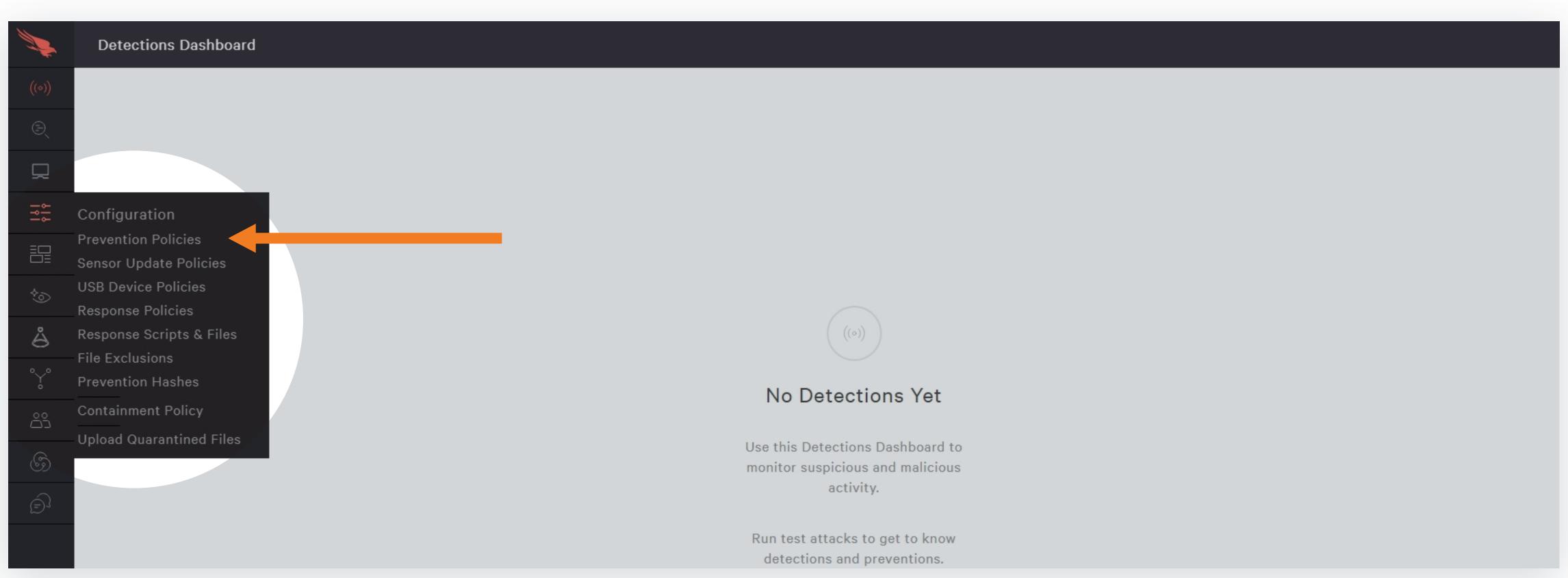
### In cooperation with CYBRARY

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



#### $\bigcirc$

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



#### $\bigcirc$

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.

	Prevention Policies							
((0))	WINDOWS POLICIES	MAC POLICIES	LINUX POLICIES					
Ð	1 policy					🕀 Add new j	policy	Edit precedence O
	DEFAULT POLICY	POLICY STATUS Enabled	POLICY NAME Default (Windows)	CREATED May. 3, 2019 12:31:03	LAST MODIFIED May. 3, 2019 12:31:03	APPLIED PEN O O	NDING	I
¢©								
å								
Ŷ								



#### **Steps 11-12** of 17

### In cooperation with CYBRARY

Step 11Next, 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."

WINDOWS POLICIES	MAC POLICIES							
1 policy						(+) A	dd new policy	
DEFAULT POLICY	POLICY STATUS Enabled	POLICY NAME Default (Windows)	CREATED May. 3, 2019 12:31:03	LAST MODIFIED May. 3, 2019 12:31:0			PENDING O	
	New	Policy Details			×			
		FORM						
		indows						
		e (REQUIRED) Id a Policy Name			_			
	DES	CRIPTION						
	A	d a Policy Description						
					11			
		CANCEL						

0

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

Prevention Policies

1 policy							
		POLICY NAME Default (Windows)	CREATED May. 3, 2019 12:31:03	LAST MODIFIED May. 3, 2019 12:31:03			
	New F	Policy Details			×		
	PLAT	TFORM					
	W	indows					
		E (REQUIRED)					
	Те	est1					
	DESC						
		<i>к</i> эц			1		
		CANCEL		CREATE			

#### Q

#### **Steps 13-14** of 17

### In cooperation with CYBRARY

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

<b>V</b>	S All Policies (	Test1 (Disabled)					
((0))	SETTINGS	ASSIGNMENT					
Ð	Policy details					Delete	Ena
딫							
%     %     %	NAME Test1		DESCRIPTION Test	PLATFORM Windows	STATUS Disabled	PRECEDENCE 1 of 1	

*⊙	Prevention policy settings							Cancel	Save
å	Sensor Capabilities								
Ŷ	Notify End Users		$\bigcirc$						
69 (9)		d user when the Falcon sensor blocks, kills, or quarantines. These ws Event Viewer under Applications and Service Logs.							
Ē	TYPE Sensor Visibility	CATEGORY Enhanced Visibility		ENABLED O	DISABLED 2	UNAVAILABLE 1			O Enable All
	TYPE Next-Gen Antivirus	CATEGORY Cloud Machine Learning		CLOUD ANTI-MALWA	ARE led Prevention: Dis	abled	ADWARE & PUP Detection: Disable	ed Prevention: Disa	bled
	TYPE     CATEGORY       Next-Gen Antivirus     Sensor Machine Learning			SENSOR ANTI-MALW Detection: Disabl	/ARE led Prevention: Dis	abled			
	TYPE Next-Gen Antivirus	CATEGORY Quarantine		enabled O	disabled 1	UNAVAILABLE O			O Enable All
/01									

Q

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



N.	S All Policies  Il Policies  Il Policies	abled)						$(\triangleright)$
((0))	Changes on the Policy Settings tab ar	e unsaved						×
© ,	TYPE Next-Gen Antivirus	CATEGORY Cloud Machine L	earning	CLOUD ANTI-MALV Detection: Disa	VARE bled Prevention: D	isabled	ADWARE & PUP Detection: Disabled Prevention: Disabled	
	TYPE Next-Gen Antivirus	CATEGORY Sensor Machine	Learning	SENSOR ANTI-MAL Detection: Disa	WARE bled Prevention: D	isabled		
*⊙	TYPE Next-Gen Antivirus	CATEGORY Quarantine		ENABLED O	disabled 1	UNAVAILABLE O	0 E	Enable All
<b>Å</b> ℃	TYPE Malware Protection	CATEGORY Execution Block	ng	ENABLED O	DISABLED 3	UNAVAILABLE 1	() E	Enable All
ŝ	TYPE Behavior-Based Prevention	CATEGORY Exploit Mitigatio	n	ENABLED O	DISABLED O	UNAVAILABLE 5		Enable All
Ð	TYPE Behavior-Based Prevention	CATEGORY Ransomware		ENABLED 5	DISABLED O	UNAVAILABLE O	E	Enable All
	Backup Deletion		Cryptowall	File Encryptio	'n		Locky	
	Deletion of backups often indicative activity.	of ransomware	A process associated with Cryptowall was blocked.		t created a file witl extension was term		A process determined to be associated wit was blocked.	h Locky
	File System Access							
$\odot$	A process associated with a high vol system operations typical of ransom							

#### Step 15-16 of 17

0

### In cooperation with CYBRARY

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

	S All Policies				$\bigcirc$
((0))	Changes on the Policy Settings tab are unsaved				×
Đ	Policy details			Delete	Enable
	NAME Test1	DESCRIPTION	PLATFORM STATUS Windows Disabled	PRECEDENCE 1 of 1	
	Prevention policy settings			Cancel	Save

Ś	Sensor Capabilities						
å							
Ŷ	Notify End Users						
ŝ		nd user when the Falcon sensor blocks, kills, or quarantines. These					
	messages also show up in the windo	ows Event Viewer under Applications and Service Logs.					
G	ТҮРЕ	CATEGORY	ENABLED	DISABLED	UNAVAILABLE		
Ð	Sensor Visibility	Enhanced Visibility	0	2	1		Enable All
	TYPE Next-Gen Antivirus	CATEGORY Cloud Machine Learning	CLOUD ANTI-MALW Detection: Disat	VARE bled Prevention: Dis	sabled	ADWARE & PUP Detection: Disabled Prevention: Di	sabled
	TYPE Next-Gen Antivirus	CATEGORY Sensor Machine Learning	SENSOR ANTI-MAL	WARE bled Prevention: Dis	sabled		
	TYPE Next-Gen Antivirus	CATEGORY Quarantine	enabled O	disabled 1	UNAVAILABLE O		Enable All

Q

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

										$\times$
	Policy details								Delete	Enable
	Test1			Test			Windows	Disabled	1 of 1	
	Prevention policy settings	c	onfirm Policy Change				×		Cancel	Save
TO -	Sensor Capabilities		Changes to apply							
å	Notify End Users		• Enable Ransomware	- Backup Deletion.						
Ŷ	Show a pop-up notification to the end	d user when	<ul> <li>Enable Ransomware</li> </ul>	- Cryptowall						
	also show up in the Windows Event V			- Gryptowall.						
		CATEGORY	<ul> <li>Enable Ransomware</li> </ul>	- File Encryption.						
Ô	Sensor Visibility	Enhance	• Enable Ransomware	- Locky.						O Enable All
		CATEGORY	• Enable Ransomware	- File System Access.				ADWARE & PUP		
	Next-Gen Antivirus	Cloud M							ed Prevention: Disa	bled
		CATEGORY	CA	NCEL	SENSOR ANTI-MAL					
	Next-Gen Antivirus		hine Learning			oled Prevention: Dis				
		CATEGORY			ENABLED	DISABLED	UNAVAILABLE			
	Next-Gen Antivirus	Quarantine				1	0			O Enable All
					ENABLED					

#### $\bigcirc$

#### **Step 17** of 17

### In cooperation with CYBRARY

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.

<b></b>	S All Policies (	Test1 (Disabled)					Ø	
((0))	SETTINGS	ASSIGNMENT						
Ð	Policy details					Delete	Enable	
	NAME Test1		DESCRIPTION	PLATFORM Windows	STATUS Disabled	PRECEDENCE 1 of 1	E	
							1	

*>>	Prevention policy settings						Cancel	Save	
å	Sensor Capabilities								
Ŷ	Notify End Users								
<u>6</u>		nd user when the Falcon sensor blocks, kills, or quarantines. These ows Event Viewer under Applications and Service Logs.							
ی آ	TYPE Sensor Visibility	CATEGORY Enhanced Visibility	ENABLED O	DISABLED 2	unavailable 1			Enable All	
	TYPE Next-Gen Antivirus	CATEGORY Cloud Machine Learning	CLOUD ANTI-MALWARE ADWARE & PUP Detection: Disabled Prevention: Disabled Detection: Disabled				bled Prevention: Disabled		
	TYPE Next-Gen Antivirus	CATEGORY Sensor Machine Learning	SENSOR ANTI-MALWARE Detection: Disabled Prevention: Disabled						
٨	TYPE Next-Gen Antivirus	CATEGORY Quarantine	ENABLED O	disabled 1	UNAVAILABLE O			Enable All	

0

#### Complete



### In cooperation with CYBRARY



For more information, visit amzn.to/2FjlF1A

