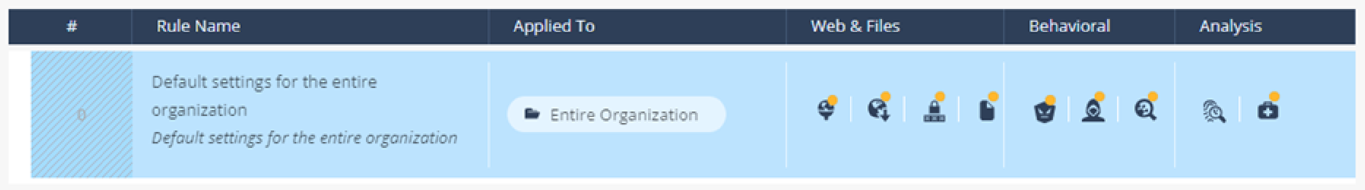
Harmony Endpoint

CHECK POINT
YOU DESERVE THE BEST SECURITY

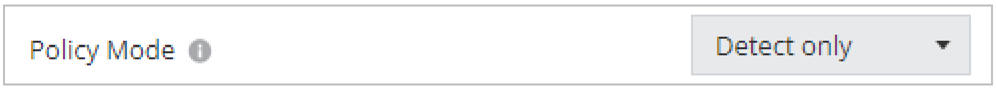
Improved Onboarding Experience

As part of our efforts to create a better user experience during the onboarding process, we are happy to share our new onboarding approach.
The new approach goals are to reduce to minimum unnecessary noise and false positives, allow the system to detect and record incidents and then ask the user to adjust his configuration by setting proper exclusions. Future reminders will notify the user to harden his policy mode.
As part of those efforts, we are happy to share the following updates:

1. **Default Policy:**
   The default policy mode of the 'entire organization' main rule will be set to "**Detect Only**"

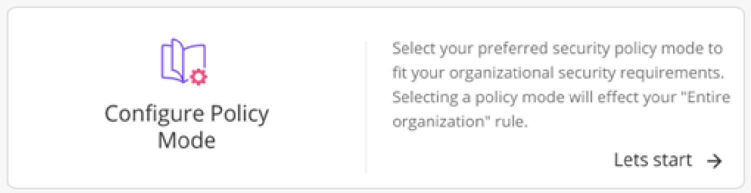


#	Rule Name	Applied To	Web & Files	Behavioral	Analysis
0	Default settings for the entire organization *Default settings for the entire organization*	Entire Organization			



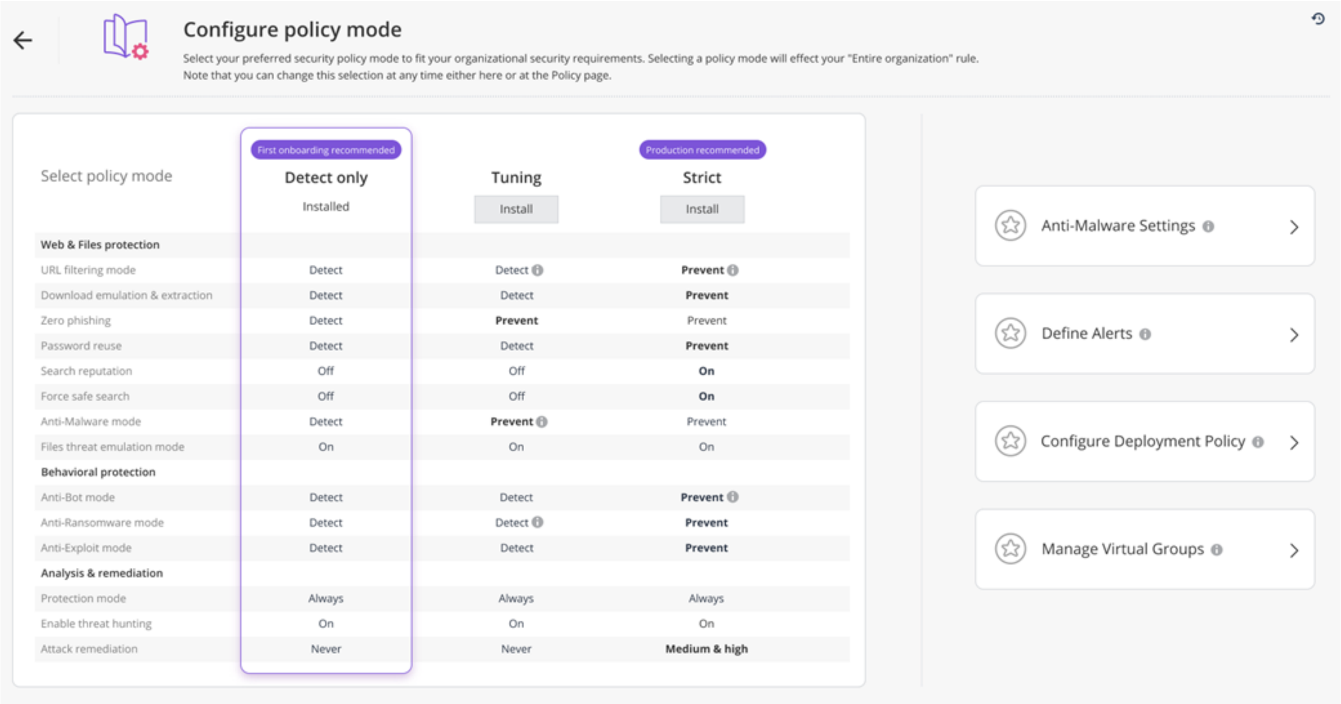
Policy Mode: Detect only

2. **Getting Started:**
   A new Getting Started card will be available to easily configure policy mode.
   This new flow will enable the user to select his preferred security policy mode to fit his organizational security requirements, emphasizing the fact that this flow will impact his 'entire organization' rule.



Configure Policy Mode

Select your preferred security policy mode to fit your organizational security requirements. Selecting a policy mode will effect your "Entire organization" rule.

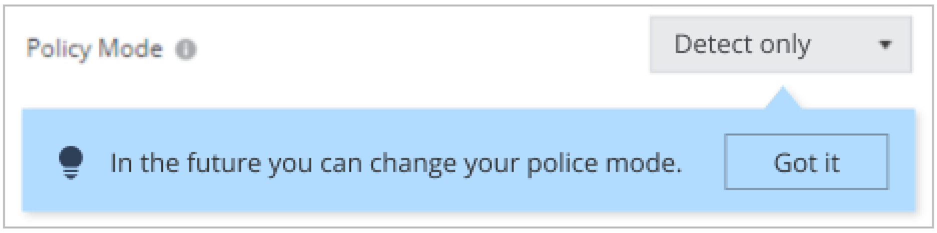


Configure policy mode

Select your preferred security policy mode to fit your organizational security requirements. Selecting a policy mode will effect your "Entire organization" rule.
Note that you can change this selection at any time either here or at the Policy page.

Select policy mode	First onboarding recommended Detect only Installed	Tuning Install	Production recommended Strict Install
Web & Files protection			
URL filtering mode	Detect	Detect	**Prevent**
Download emulation & extraction	Detect	Detect	**Prevent**
Zero phishing	Detect	**Prevent**	Prevent
Password reuse	Detect	Detect	**Prevent**
Search reputation	Off	Off	**On**
Force safe search	Off	Off	**On**
Anti-Malware mode	Detect	**Prevent**	Prevent
Files threat emulation mode	On	On	On
Behavioral protection			
Anti-Bot mode	Detect	Detect	**Prevent**
Anti-Ransomware mode	Detect	Detect	**Prevent**
Anti-Exploit mode	Detect	Detect	**Prevent**
Analysis & remediation			
Protection mode	Always	Always	Always
Enable threat hunting	On	On	On
Attack remediation	Never	Never	**Medium & high**

3. **Recommendations:**
   The first time the admin enters the policy page, we will point and emphasize the policy mode area, to ensure the Admin knows where to find it.



Policy Mode

Detect only

In the future you can change your police mode.

4. **Notifications:**
   48 hours after deployment, we will pop up a top bar reminder to ensure he needs to consider hardening his configuration.