ESET Tech Center

How do the Agressive Detections work in ESET Endpoint 7.2 and later (7.x)

Steef | ESET Nederland - 2019-11-12 - Comments (0) - Endpoint Solutions

Changes to the detection engine scanner configuration

Starting in version 7.2, the Detection engine section no longer provides ON/OFF switches as for version 7.1 and below. ON/OFF buttons are replaced with four thresholds - Aggressive, Balanced, Cautious and Off.

INDEX

Real-time & Machine learning protection categories

Real-time & Machine learning protection for all protection modules (for example, Real-time file system protection, Web access protection, ...) allows you to configure reporting and protection levels of the following categories:

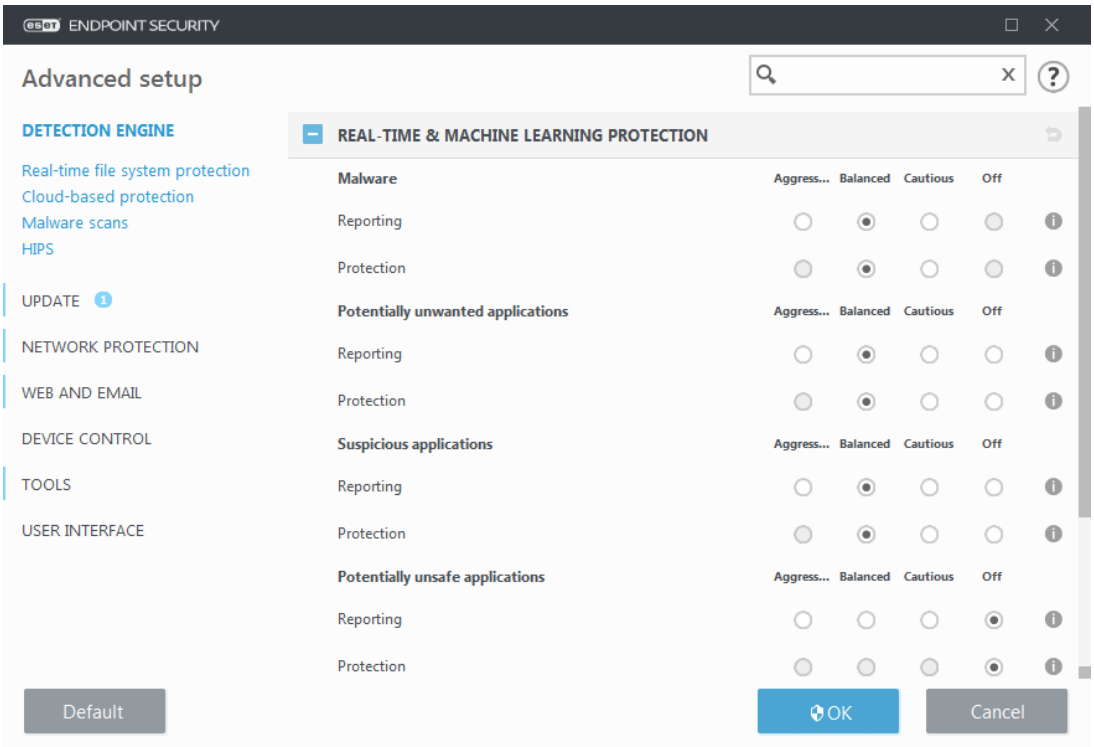
• **Malware** – A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component.
Read more about these types of applications in the Glossary.

• **Potentially unwanted applications** – Grayware or Potentially Unwanted Applications (PUAs) is a broad category of software, whose intent is not as unequivocally malicious as with other types of malware, such as viruses or trojan horses. However, it could install additional unwanted software, change the behavior of the digital device, or perform activities not approved or expected by the user.
Read more about these types of applications in the Glossary.

• **Potentially unsafe applications** – Refers to legitimate commercial software that has the potential to be misused for malicious purposes. Examples of potentially unsafe applications (PUAs) include remote access tools, password-cracking applications, and

keyloggers (programs recording each keystroke typed by a user).
Read more about these types of applications in the Glossary.

• **Suspicious application**s include programs compressed with packers or protectors. These types of protectors are often exploited by malware authors to evade detection.



> Improved protection
>
> Advanced machine learning is now a part of detection engine as an advanced layer of protection which improves detection based on machine learning. Read more about this type of protection in the Glossary.

Reporting setup

When a detection occurs (e.g., a threat is found and classified as malware), information is recorded to the Detections log, and Desktop notifications occur if configured in ESET Endpoint Security.

Reporting threshold is configured for each category (referred to as "CATEGORY"):

1.Malware

2.Potentially unwanted applications

3.Potentially unsafe

4.Suspicious applications

Reporting performed with the detection engine, including the machine learning component. It is possible to set a higher reporting threshold than the current protection threshold. These reporting settings do not influence blocking, cleaning or deleting objects.

Read the following before modifying a threshold (or level) for CATEGORY reporting:

Threshold	Explanation
Aggressive	CATEGORY reporting configured to maximum sensitivity. More detections are reported. The Aggressive setting can falsely identify objects as CATEGORY.
Balanced	CATEGORY reporting configured as balanced. This setting is optimized to balance the performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	CATEGORY reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches CATEGORY behavior.
Off	Reporting for CATEGORY is not active, and detections of this type are not found, reported or cleaned. As a result, this setting disables protection from this detection type. Off is not available for malware reporting and it is default value for potentially unsafe applications.

Availability (enabled or disabled) of a protection module for a selected CATEGORY threshold is as follows:

	Aggressive	Balanced	Cautious	Off*
Advanced machine learning module*	✓ (aggressive mode)	✓ (conservative mode)	X	X
Detection engine module	✓	✓	✓	X
Other protection modules	✓	✓	✓	X

* Available in ESET Endpoint Security version 7.2 and later.

Feature table

ESET Endpoint Antivirus/Security	v7.1	v7.2
Local machine learning module for aggressive detection		✓
Unified exclusions		✓
Exclusion hit history		✓

ESET Endpoint Antivirus/Security	v7.1	v7.2
Interactive alerts configuration	✓	✓
Product upgrade process	✓	✓
Deep behavioral inspection		✓
Improved Anti-Phishing	✓	✓

Best practices

UNMANAGED (Individual client workstation)

Keep the default recommended values as is.

MANAGED ENVIRONMENT

These settings are usually applied to workstations via a policy.

1. Initial phase

This phase might take up to a week.

• Set up all Reporting thresholds to Balanced.
NOTE: If needed, set up to Aggressive.

• Set up or keep Protection for malware as Balanced.

• Set up Protection for other CATEGORIES to Cautious.
NOTE: It is not recommended to set up the Protection threshold to Aggressive in this phase because all found detections would be remediated, including the falsely identified ones.

• Identify falsely identified objects from Detections log and add them to Detection exclusions first.

2. Transition phase

• Implement the "Production phase" to some of the workstations as a test (not for all workstations on the network).

3. Production phase

• Set up all Protection thresholds to Balanced.

• When managed remotely, use an appropriate antivirus pre-defined policy for ESET Endpoint Security.

• Aggressive protection threshold can be set if the highest detection rates are required and falsely identified objects are accepted.

• Check Detection log or ESMC reports for possible missing detections.