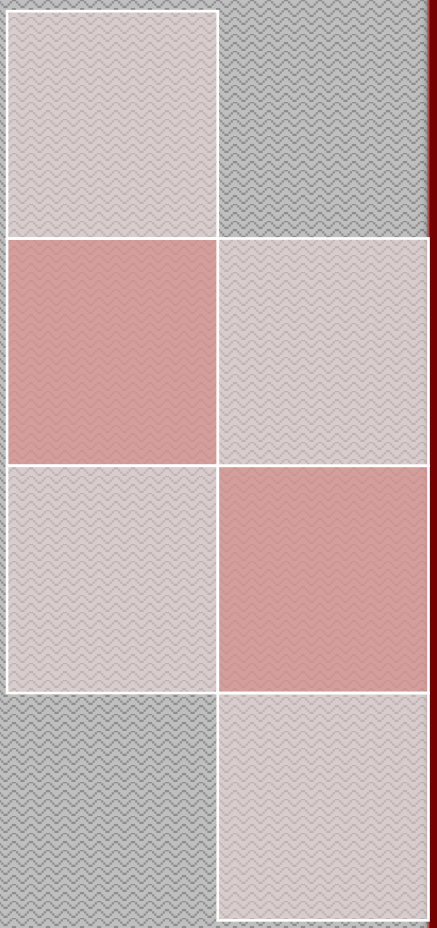


McAfee™
Together is power.

Summary Document:
Adaptive Threat Prevention (ATP) operational recommendations

Version:
007 draft

Customer:
Generic

Prepared by:
Steen Pedersen

Cover Page

Notices

Copyright

For information, please contact:

McAfee
Steen Pedersen, Principal Architect, steen_pedersen@McAfee.com

Trademarks

Disclaimer

The information contained in this document is subject to change without notice.
McAfee MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. McAfee shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

McAfee reserves the right to add, subtract or modify features or functionality, or modify the product, at its sole discretion, without notice.

McAfee makes no commitment, implied or otherwise, to support any functionality or technology discussed or referenced in this document.

Table of Contents:

1 ADAPTIVE THREAT PREVENTION (ATP) OPERATIONAL RECOMMENDATIONS 1

1.1 INTRODUCTION 1
1.2 INFORMATION ABOUT ATP/JTI RULES 2
1.3 COMMON ISSUES - CONNECTION, PROTECTION AND VISIBILITY OF ATP 2
1.3.1 Lack of visibility of ATP events - ENS Common Option Policy 2
1.3.2 ATP cloud connection is missing 4
1.3.3 Overcautious policies – causing reduced security and visibility 5

2 THREAT EVENTS RELATED TO ATP 7

2.1 ATP/JTI RULE DETECTIONS 7
2.2 REAL PROTECT DETECTIONS 8
2.3 DYNAMIC APPLICATION CONTAINMENT (DAC) 9
2.4 PROCESS RUNTIME REPUTATION 11
2.5 MANY "ADAPTIVE THREAT PROTECTION WOULD CONTAIN" – EVENT ID 35111 11

3 INCREASE VISIBILITY WITH ATP RULES 12

4 RECOMMENDED PROCEDURES FOR HANDLING FILE REPUTATION 13

4.1 SERVICE DESK – SET ADAPTIVE THREAT PROTECTION TO OBSERVE MODE 13

5 SOFTWARE DEVELOPERS 15

5.1 FOR POLICY MANAGEMENT OF THE DEVELOPER WORKSTATIONS 15
5.2 HOST FIREWALL CONFLICT WITH DEVELOPER 16

APPENDIX A : ACRONYMS AND TERMS 17

APPENDIX B : ATP EXECUTION FLOW 19

Change History Log:

Version No	Release Date	Updated by	Summary of Changes	Accepted by
001	20201104	Steen Pedersen	Draft version	
003	20210324	Steen Pedersen	Updated with section 3 Developer information	
005	20210505	Steen Pedersen	Updated with ENS Common policy	
006	20210519	Steen Pedersen	Updated structure	
007	20210519	Steen Pedersen	Cleaned the document	

1 Adaptive Threat Prevention (ATP) operational recommendations

1.1 Introduction

Adaptive Threat Prevention (ATP) module introduces several features and additional capabilities to improve security and provide visibility and prevention. In general, the ATP features are activated "on execute" and also how Office document and PDF interact with executables and scripts.
ATP and Threat Prevention also provide technologies that protect against fileless attack methods in which no persistent malware file exists. Fileless attacks include network streaming of payloads and commands, abuse of dual-use applications, and living-off-the-land techniques.

This document covers some of the common situation with ATP rules, events and different options for handling these. Some events are based on file reputation and other are based on behaviours which changes the reputation of the process at runtime. Known trusted file can get a different reputation on execution and while running, which will have an effect on how ATP can contain, block or kill the process. This document cannot cover all the different situations which can occur.

List of the different ATP capabilities:

- ATP rules
  - Provide on-execute runtime reputation to files and processes based on ATP rules which also utilize GTI/TIE file and certificate reputation
  - The ATP rules can be viewed and default state changed in the ePO console –> Server Settings –> Adaptive Threat Prevention (State can be Enabled, Observe or Disabled)
- ATP Option Policy
  - ATP Rule group assignment – Productivity, Balanced and Security
  - Action enforcement based on the runtime calculated reputation:
    - Contain
    - Block
    - Clean with options for
      - Enhanced remediation
      - Monitor and remediate deleted and changed files
  - Real Protect
    - Client based scanning
    - Cloud based scanning
    - Enhanced script scanning using AMSI
    - Credential Theft Protection
  - Dynamic Application Containment
  - Story Graph
- Dynamic Application Containment Policy
  - Containment Rules and reaction on contained processes

Many of the ATP rules are mapped against the MITRE ATT&CK matrix with a Txxxx number. The T is for Tactic or Technique which has been assigned by MITRE. An overview is available here:
https://attack.mitre.org/
The Txxx number will often be included the ATP rule description. There can be multiple ATP rules for the same Txxxx and not all Txxx has an ATP rule.

Appendix B : contains more information about the ATP execution flow.

1.2 Information about ATP/JTI rules

The ATP rules (currently 120+) and there are currently updates to the ATP rules about every second week automatically. The ATP rules are included in the AMCore (DAT) updated. The rules are design to handle file and processes reputation and some of the rules are monitoring the behaviours of application and how usage of these applications are initiated. This can provide visibility and identify malicious activity. Based on this ATP can set a processes reputation which can lead to a process is being blocked. The detection can also be listed as JTI (Joint Threat Intelligence).

With ATP you can see Block or Would Block of well-known and trusted application based the rules.
Examples:

1. The method on how PowerShell is being executed
2. How and what applications are executed by Word
3. And many more

The ATP rules can be viewed and the current state viewed and modified in the ePO console – Server Settings –> Adaptive Threat Prevention

The ATP rules has 3 states. Enabled/On, Observe/Evaluate and Disable/OFF

The ATP rules are included in the AMcore updates and automatically included by ePO.
The current and previous Release Notes for the ATP rules can be found here:
https://www.mcafee.com/enterprise/en-us/release-notes/threat-intelligence-exchange.html

Identify what rule corresponds to an Adaptive Threat Protection and Threat Intelligence Exchange event
https://kc.mcafee.com/corporate/index?page=content&id=KB82925

1.3 Common issues - Connection, Protection and Visibility of ATP

There are some common situations and configures mistakes done. This section is covering some of the common configuration mistakes and how they can be addressed.

1.3.1 Lack of visibility of ATP events - ENS Common Option Policy

Common issues - There are events and no visibility to all the ATP rules in “Observe” state.

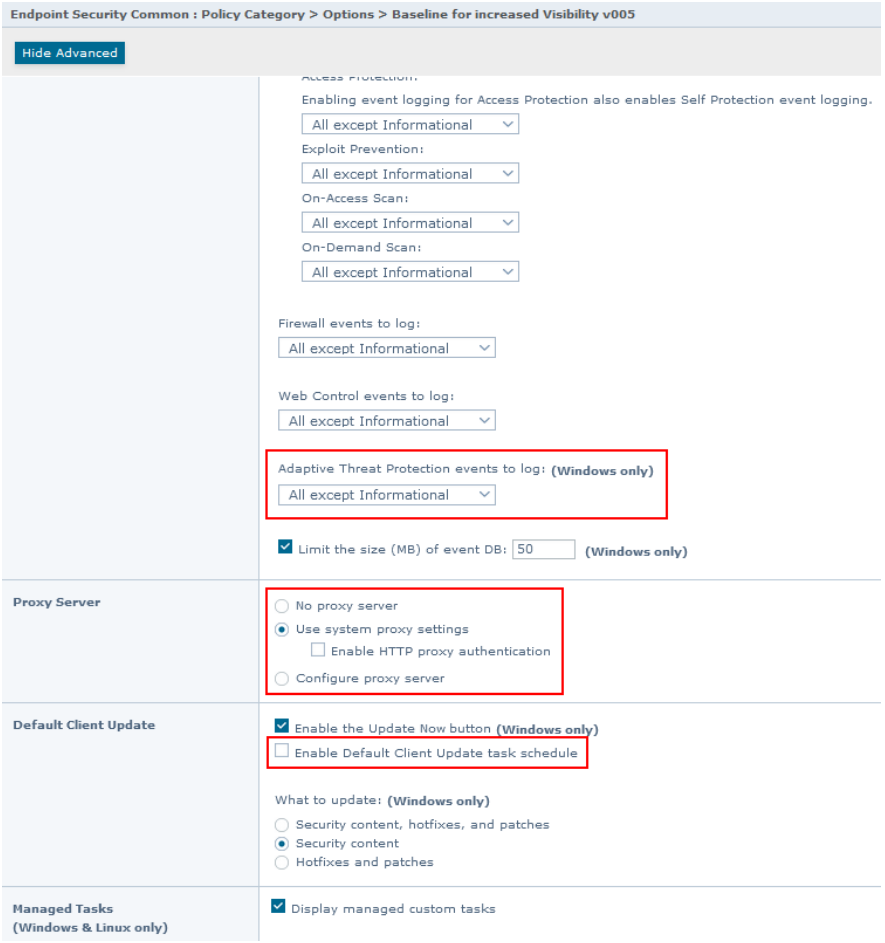
Check the state of the ATP rules in ePO -> Server Settings -> Adaptive Threat Protection. The state includes a star * if it changes from the default state provided by McAfee.

IMPORTANT

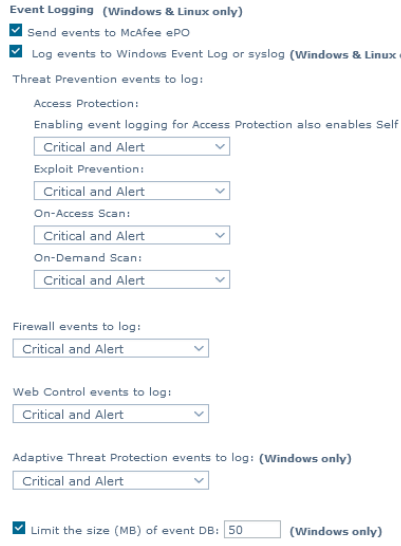
The default configuration of ENS Common Option policy do not provide visibility into any ATP rules in Observe state. It is highly recommended to change the ENS common Policy. Change the log level for ATP from default setting: “Critical and Alert” to “**All except Informational”** or “All” – as this will provide visibility to all the ATP rules which are in Observe state. Without this setting there are no events local on the endpoint and no events are send to ePO for these ATP rules in Observe state.

Note: About every 2-3 weeks there are updates to the ATP rules. These updates can include current rules being updated, new rules added, and default state of rules can change. It is recommended to review the ATP content release notes. There can be new ATP rules which can help you improve the prevention and visibility of different attacks.

Here is the ENS Common Options policy where the ATP log level is set to “All except Informational” which is the recommended setting for visibility for all ATP rules in Observe state. These rules will generate Would Block and Would Clean events with the Threat Severity “Notice”. The other high lighted settings are cover below in this section.



ENS Common Option policy Default setting does not provide enough visibility



1.3.2 ATP cloud connection is missing

Common mistake: ATP lack cloud connection.

ATP utilize several cloud services like GTI and Real Protect Cloud. Access to some of the cloud services are still required even with an internal TIE infrastructure. There is a common expectation that all cloud connectivity will be handled by TIE Server. That is not correct - TIE will handle the GTI file and certificate reputation lookup for ATP, there is still a need for cloud access for Real Protect.
ATP will try to access the Cloud servers directly from the endpoint. This will fail if there are a requirement that all endpoints utilize a proxy to access the Internet.

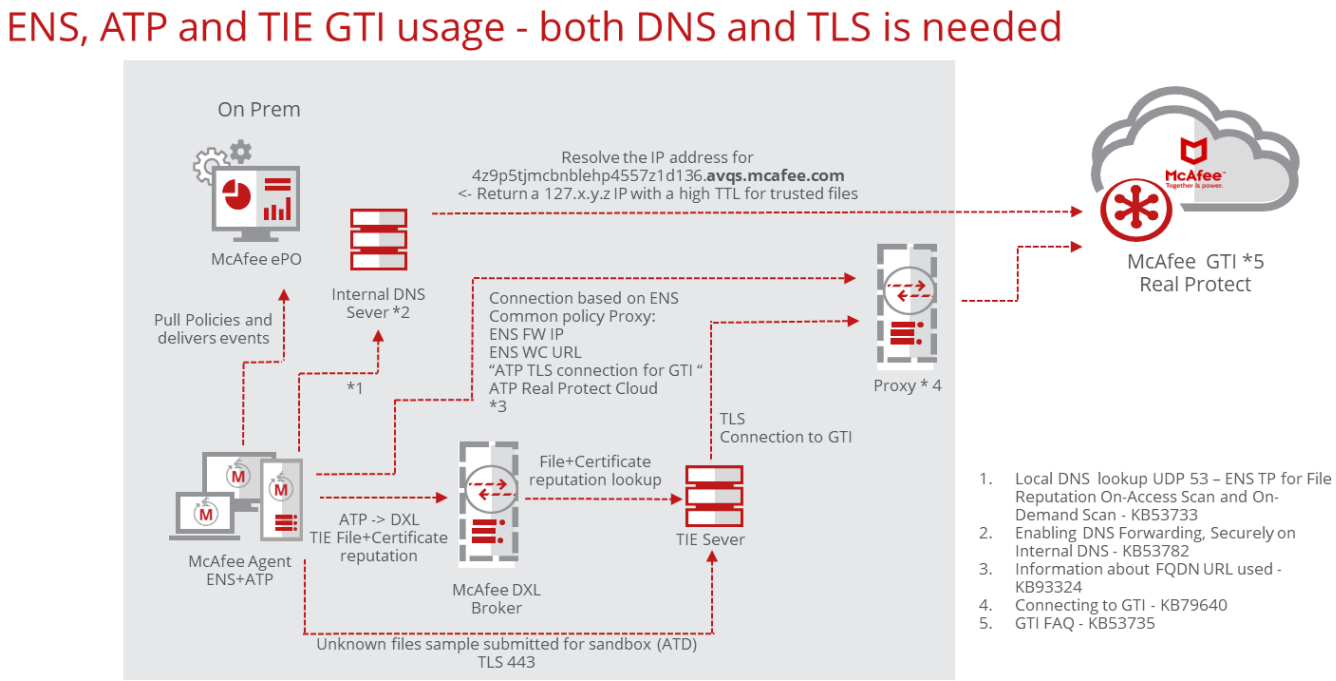
The ENS Common Option policy include the setting for the proxy access if required and the ATP module with utilize this. Make sure this is proxy setting is correctly configured for your environment and test this with the Real Protect Cloud test files. See below link.

Test files to test Real Protect scanning and Credential Theft Protection
https://kc.mcafee.com/corporate/index?page=content&id=KB88828

Endpoint Security off-box communication URLs
https://kc.mcafee.com/corporate/index?page=content&id=KB93324

1.3.2.1 Overview of cloud connections for ENS and ATP

High level overview of how ENS and ATP utilize cloud connections and how TIE can handle some of the GTI cloud connectivity.



1. Verify that GTI File Reputation is installed, and endpoints can communicate with the GTI server - https://kc.mcafee.com/corporate/index?page=content&id=KB53733
2. Global Threat Intelligence and split Domain Name System (DNS) - https://kc.mcafee.com/corporate/index?page=content&id=KB53782
3. Endpoint Security off-box communication URLs - https://kc.mcafee.com/corporate/index?page=content&id=KB93324

4. Connecting to Global Threat Intelligence - https://kc.mcafee.com/corporate/index?page=content&id=KB79640
5. FAQs for Global Threat Intelligence File Reputation - https://kc.mcafee.com/corporate/index?page=content&id=KB53735

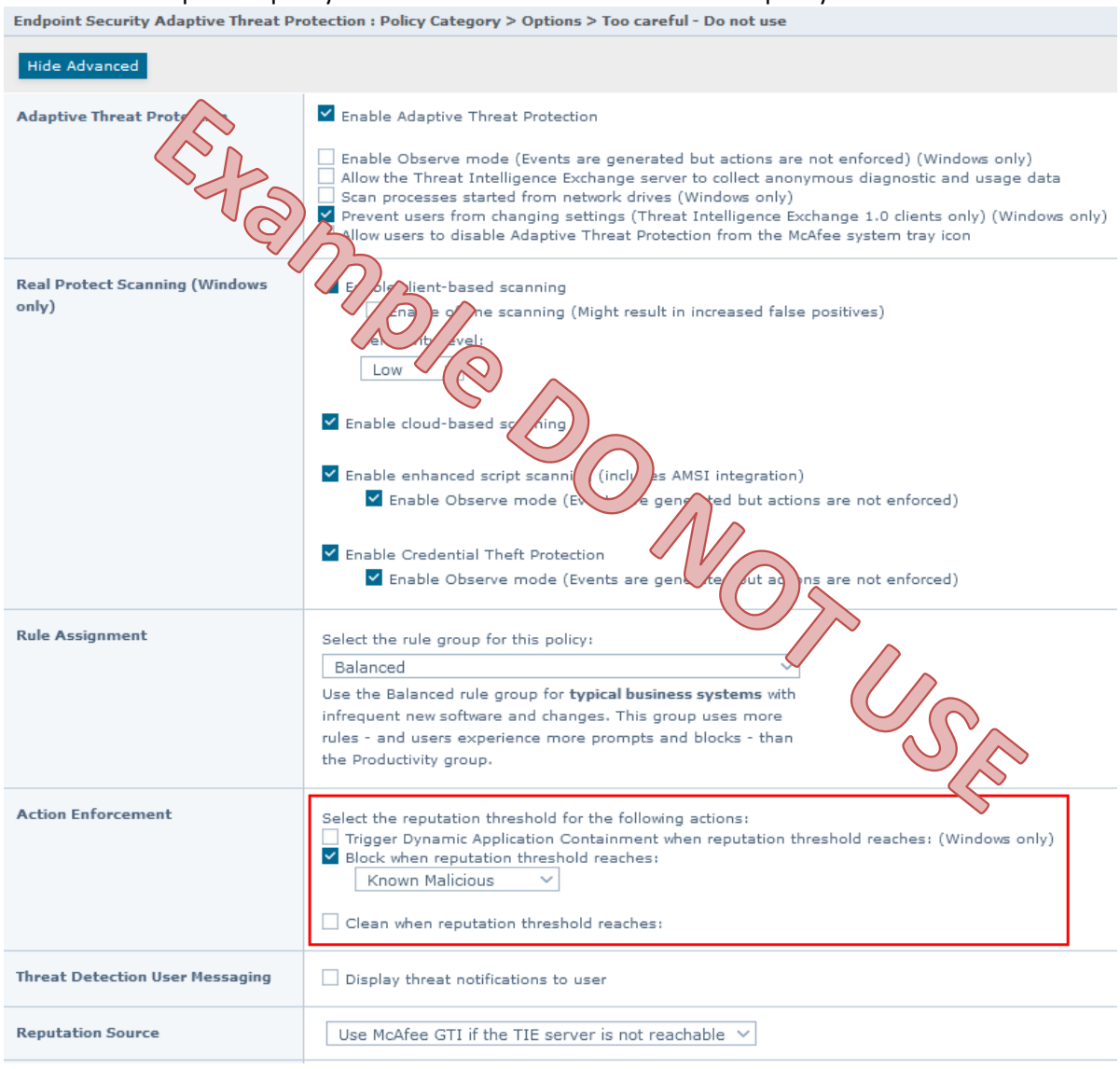
The plan is to move the GTI DNS lookup to utilize a TLS connection instead. There is a KB with the information. https://kc.mcafee.com/corporate/index?page=content&id=KB94339

Information about the Security Bulletin:
https://kc.mcafee.com/corporate/index?page=content&id=SB10354

1.3.3 Overcautious policies – causing reduced security and visibility

Some customers have ATP policies which has been configured to be too cautious. The configurations are done with good intention to reduce risk of impact with ATP false positives. Problem is that the settings are severely reducing the detection capabilities and visibility of the ATP events.

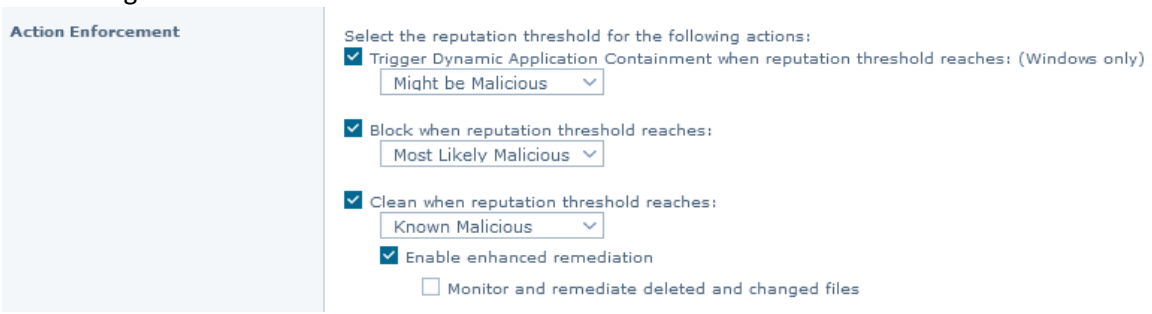
Here is an example of a policy which is "Too careful" Do not use this policy.



Some of the issues with this policy:

1. All the ATP rules which are setting the reputation to “Most Likely Malicious” or “Might be Malicious” are not in effect. No local logs, Threat Events or visibility to any of these ATP rules.
2. Real Protect Cloud is not working as it requires ATP options set to: Clean – Known Malicious enabled, as the Real Protect Cloud first will convict a file after it has been running for some time

The Setting should be:



2 Threat Events related to ATP

The ATP can have different reactions depending on which module and rule are triggered. Some rules can be in "Observe" state and the Threat Event can report Action Taken like:

- "Adaptive Threat Protection Would Block" Event ID 35102
- "Adaptive Threat Protection Would Clean" Event ID 35106
- "Adaptive Threat Protection Would Contain" Event ID 35111

The "Would" means that this was reported only and no Action taking on the file and not blocking of the behaviour.

Threat Event can also report prevention in Action Taken:

- "Adaptive Threat Protection Blocked" Event ID 35104
- "Adaptive Threat Protection Cleaned" Event ID 35107
- "Adaptive Threat Protection Contained" Event ID 35112
- "Contained" Event ID 37275
- "Blocked" Event ID 37279
  - Contain the DAC rules which has been violated and blocked. The DAC rule is written in the Threat Name. Like "*Deleting files commonly targeted by ransomware-class malware*"
- "Would Block" Event ID 37280
  - Contain the DAC rules which has been violated and reported only. The DAC rule is written in the Threat Name. Like "*Reading from another process' memory*"

Here are 3 different kind of ATP detections and how to address these if there are many events. issue which identify the ATP module is not getting the correct policy assigned.

2.1 ATP/JTI rule detections

ATP can provide a "runtime" process reputation based on ATP rules This can be different levels of Trusted or Malicious. The reputation can lead into that process execution being reported and possibly blocked depending on the ATP Option policy (Observe or Enable) or the ATP rule state (Observe or Enable). The processes block can be known trusted processes and they are blocked based on the way they are executed or how they access other files, processes or DLL.

Example of ATP event where PowerShell has been executed with an obfuscated command line (include selected important fields from Threat Event):

Threat Target Process Name:	powershell.exe
Event Category:	Reputation
Event ID:	35104
Threat name:	JTI/Suspect.524543
Action Taken:	Adaptive Threat Protection Blocked
Analyzer Detection Method:	On-Execute Scan
Rule Name:	Detect potentially obfuscated command line parameters
Rule Description:	Mitre-T1027: Trigger on command line arguments that are highly obfuscated
Rule Detailed Description:	Tactic: Defense Evasion - Technique: T1027. This rule is designed to analyze command line parameters passed to programs to alert on potentially obfuscated strings that could indicate malicious behavior

There are different methods for handling ATP rule events depending on what have been detected and the impact (Blocked or Would Block):

A) The activity looks to be malicious and is correctly identified
B) The activity looks to be an acceptable and not malicious in nature

Reaction for option A (looks to be malicious activity):

1. Do an investigation of the endpoint as is might be compromised or an attempt to compromise the endpoint has been prevented.
    a. Inspect all the Threat Events from this endpoint
    b. Verify if there are other endpoints with the same ATP events
    c. If the event is reported as "Would Block" the actions has not been blocked and the endpoints needs to be investigated.
        i. Consider if the ATP rule should be changed to Enabled state – verify if there are Threat Events generated with that ATP rule which should be accepted
    d. This should not be seen as a complete list of all activities needed to be done as there can be many different activities required depending on the environment and company incident response procedures

Reaction for option B (acceptable behavior) – different options:

1. Let it be - If the event is the just a "report only" - "Would Block" and there are few of these events
    a. Or of the event is "Blocked" but do not have an impact on the user
2. Disable the specific ATP rule (which are in Observe or Enable state) in ATP "Balanced" tab in Adaptive Threat Prevention
    a. This will disable the rule for all endpoints running with "Balanced"
3. Disable the specific ATP rule in ATP "Productivity" mode and switch the ATP Option policy for the affected endpoints to use an ATP policy which is configured for "Productivity" assignments
    a. Every endpoint will maintain the ATP rule active except the endpoints switch to the "Productivity" policy
4. Stop getting all Observe events from the ATP rules in Observe state
    a. Change the ENS common log level for ATP to "Critical and Alert" for a group of endpoints - so the ATP rules in Observe state will not generate any events from these endpoints
        i. This does lose visibility to all the ATP rules in "Observe" state
5. Get a Service Request created at McAfee to request the ATP rule to be tuned/updated to reduce the amount of events/noise generated

Access to all the ATP rules for adjusting the state of the rules: ePO Console – Sever Setting – Adaptive Threat Prevention

2.2 Real Protect detections

Real Protect will only inspect Unknown files when they are executed. Real Protect can trigger a detection on the unknown files which is being identified as malicious by the Real Protect engine. When this happen a Threat Event will include the Threat Name which starts with "Real Protect". Real Protect Client will scan the file before it is finally executed and Real Protect Cloud will monitor and collect information about how the files is behaving and report this to McAfee Real Protect Cloud (requires Internet connection). With Real Protect Cloud the

There are different methods for handling a file detected as infected by Real Protect depending on what have been detected:

A) The file looks to be malicious and is correctly convicted

B) The file looks to be an unknown good file which should not be convicted (false positive)

Reaction for option A (new malware detected):

1. New unknown malware has been detected! Start procedure for handling new unknown malware detection to track down the source of infection.
2. If TIE is implemented get the file hash set to Enterprise reputation to "Known Malicious" which will block execution and remove it from other endpoints.
3. Know that the malware might have been running for minutes if file was convicted by Real Protect Cloud – See "Analyzer Detection Method" in the Threat Event

Reaction for option B (false positive):

1. A file has been convicted by Real Protect and it needs to be trusted and allowed to execute. (If the file is not needed nothing is required to be done)
    a. The deleted file can be recovered from ENS quarantine folder on the endpoint
2. If TIE is implemented get the file hash set to Enterprise reputation "Known Trusted" or "Most likely Trusted" which will allow execution of the file
3. If TIE is not available, the files needs to be excluded from ATP:
    a. The exclusion is done in the ENS OAS Policy Standard section
        i. The exclusion should be as specific as possible like: C:\APP\BIN\PROGRAM.EXE
    b. The file can also be submitted to McAfee Support and requested to be trusted by GTI, which will allow the file to be executed without Real Protect conviction

ATP use the exclusions configured in the ENS On-Access Scan Policy. ATP exclusions are based on ENS OAS exclusion for standard processes.

2.3 Dynamic Application Containment (DAC)

Dynamic Application Containment (DAC) is initiated based on the process reputation at runtime. The threshold for containment is configured in the ATP Option Policy. Common configuration is performing containment for reputation level "Might be malicious" files. Containment can be configured for "Unknown" files which can have many benefits. It does require a good management and ongoing procedures to reduce the "Unknown" applications and DLL used in the organization as there can be good but unknown files contained and generate a lot of event in ePO and potential also block different actions based on the containment rules.

Reduce the "Unknown" application include procedures for getting the unknown good applications trusted by GTI or TIE or excluded in DAC policy.

If ATP is configured to run for Observe mode there is only one event generated and there are no future details about what the process was doing:

- "Adaptive Threat Protection Would Contain" Event ID 35111

If ATP is not running in Observe mode there can be

- "Adaptive Threat Protection Contained" Event ID 35112
- "Contained" Event ID 37275
- "Blocked" Event ID 37279
    - Contain the DAC rules which has been violated and blocked. The DAC rule is written in the Threat Name. Like "*Deleting files commonly targeted by ransomware-class malware*"
- "Would Block" Event ID 37280

- Contain the DAC rules which has been violated and reported only. The DAC rule is written in the Threat Name. Like "*Reading from another process' memory*"

There are different methods for handling containment:

A) The file or process looks to be malicious and is correctly contained
B) The file or process looks to be an unknown good file which should not be contained

Reaction for option A (malicious process has been contained)

1. Do an investigation of the endpoint as is might be compromised or an attempt to compromise the endpoint has been prevented.
2. Same procedure as the ATP/JTI rule detections

Reaction for option B (acceptable unknown trusted file) – different options:

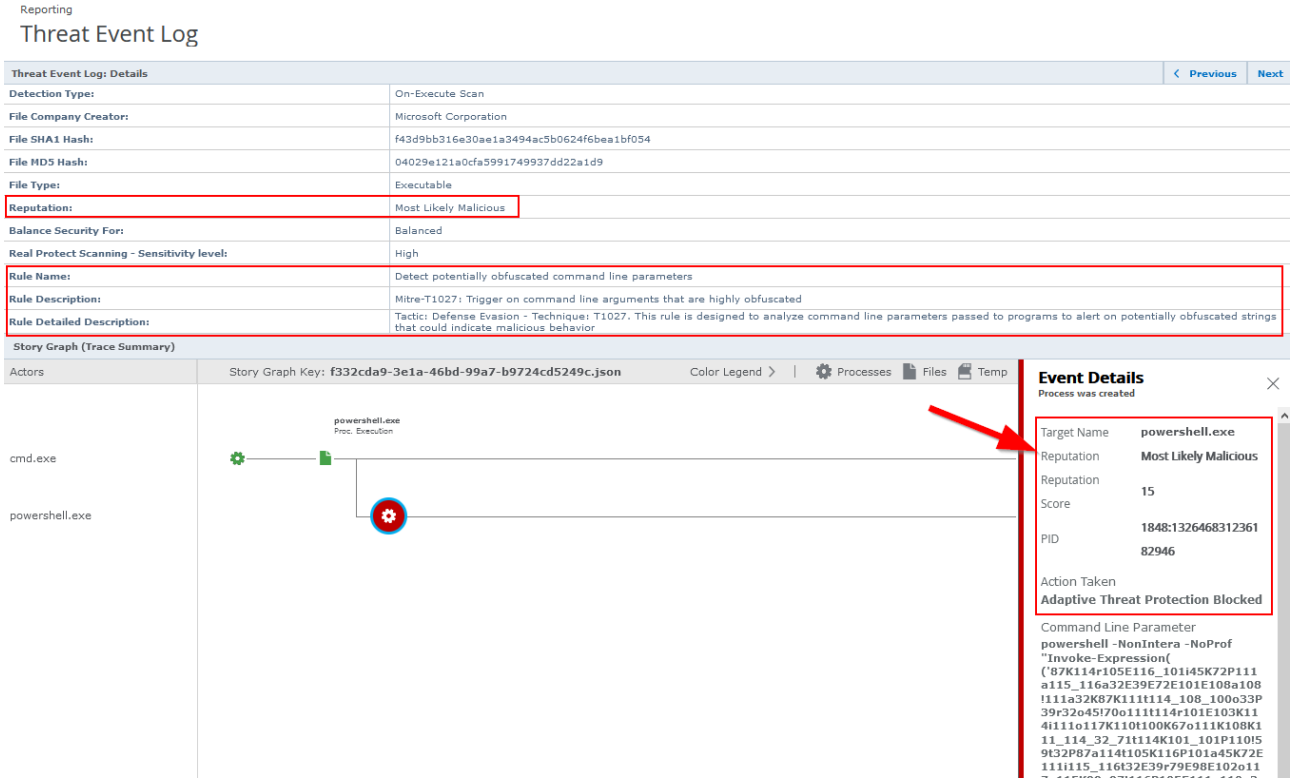
1. Let it be - If the DAC policy rules and events are report only - "Would Block" events are generated and if there are few of these events it is not super important to adjust
2. To avoid the file being contained it must be trusted or excluded
    a. Trusted
        i. If TIE is implemented get the file hash set to Enterprise reputation "Known Trusted" or "Most likely Trusted" which will allow execution of the file
        ii. Or get the file trusted by GTI using GetClean tool.
    b. Excluded
        i. If TIE is not available, the files needs to be excluded from ATP:
            1. The exclusion is done in the ENS OAS Policy Standard section
            2. The exclusion should be as specific as possible like: C:\APP\BIN\PROGRAM.EXE
        ii. Or the file information of the contained file can be added in the exclusions section in the DAC Policy

2.4 Process runtime reputation

Be aware: an application can be trusted by GTI/TIE and signed and still get a different runtime reputation. This can occur if the process loads unknown DLL or get unknown DLL injected.
So when reducing the amount of unknown application it is also important to look at the other unknown applications and unknown DLL located on the endpoint.

The run reputation can also be affected by ATP rules based on the behaviour of the process, how it is loaded, utilized or what command line options are being used etc.

Here is an example where PowerShell.exe which is “Known Trusted” is getting a “Most Likely Malicious” reputation at runtime when attempted to be started with “potentially obfuscated command line parameters“ (ATP rule 255). The “story” is visible in the Story Graph section



2.5 Many “Adaptive Threat Protection Would Contain” – Event ID 35111

There can occur and issue on old version of ATP modules where the Agent cannot correctly apply the ATP policy provided by ePO and the ATP will then use a “built-in” default policy which is in Observe mode and performing DAC on “Unknown” files.
This issue can be identified by many Event ID 35111 “Adaptive Threat Protection Would Contain” and the reputation of the processes are “Unknown”.

Solution:
Upgrade the all the ENS modules including ATP to the latest currently approved version. Make sure that all the modules are upgraded.
If the ENS modules cannot get upgrade there is an ENS Removal tool which can remove all the ENS modules and the latest release can be installed.

3 Increase visibility with ATP rules

The ATP rule set contains many rules. Some are enabled and some are with observed or disabled state. The Observe state can provide visibility and no protection, and the disabled rules provide no information at all.

An ATP rule can be in a Disabled state for different reasons:

- The rule is new and can be tested by customers
- The rule can possibly generate noise in some environments
- The rule can generate additional events and if these are not utilized then it will take additional storage on the ePO server

Example for May 2021

Rule	Description	State
500	Block lateral movement from other windows machines in the network	Disabled
502	Detect new service creation	Disabled
503	Detect binaries signed with Suspicious Certs	Disabled
504	Prevent use of sdbinst.exe to install application shims	Disabled
505	Detect obfuscated cmd.exe command line parameters	Disabled
506	Detect commands for user discovery	Disabled
507	Detect commands used to discover more information about a system	Disabled
508	Detect commands used to discover permission information related to users and groups	Disabled
509	Detect commands used to discover network related configurations	Disabled
510	Detect data encryption attempts for suspicious activities	Disabled
511	Detect attempts to dump sensitive information via registry or lsass	Disabled
512	Detect commands that allow for indirect execution outside of cmd and powershell	Disabled
513	Detect commands used for copying files from a remote system	Disabled
514	Detect DLL loads that have potentially been hijacked	Disabled
515	Protect against office apps launching unknown processes from non-standard locations.	Disabled
516	Identify and block processes executing with non-standard command lines	Disabled
517	Prevent actor process with unknown reputations from launching processes in common system folders	Disabled

4 Recommended procedures for handling file reputation

To mitigate this risk of false positives and impact - three new procedures are recommended to be implemented:

1. **Preapprove of the applications**
    a. Have a procedure so new software is analysed and submitted to McAfee Global Threat Intelligence before deployment – Using GetClean (Separate Operational GetClean document has been provided) *1
    b. Get the software deployed to a pre-production/test environment and monitor Threat Events. This is part of the Software Deployment team procedures.
    c. Continue to push/request software/service providers to sign the code and then approve the code signing certificate in TIE. This is a long-term process.
2. **Monitor the Reputation Events**
    a. Monitor events for executable being blocked or clean based on reputation. The Enterprise Reputation should be corrected either to Trust the file or Block the file.
    b. Monitor the ATD convictions of “Known Malicious” and “Most Likely Malicious” and set Enterprise Reputation to the right level.
3. **Service Desk can temporarily disable the Adaptive Threat Protection**
    a. Service Desk can have a very simple procedure for switching the ATP from Enable to Observe on selected endpoints. This can be done by a tag in ePO or in User-Info systems or anywhere where the ePO API can be enabled.
    b. Service Desk can also as a final resolution uninstall ATP if there are performance issues which needs to be addressed urgent

If the procedure 1. is being follow the other 2 procedures will not be needed for good unknown software.

*1 GetClean note:
The procedure for submitting a file using GetClean will only collect executable files. EXE, DLL, SYS etc. no data files are collected. Files submitted via GetClean are not distributed outside McAfee or shared with competitors and third-party vendors. Files submitted with GetClean will help you and other customers with a good McAfee GTI reputation.
Other procedures are possible if, for some reason, a vendor/service provided do include sensitive information in the executable files and therefor do not want to McAfee to obtain a copy. There are multiple optional procedures:

A) All the files can be uploaded to a server and these files can automatically be scanned, hashed and injected in to TIE as Enterprise Trusted (procedure has not been implemented)
B) Place the ATP on the target server in Observe mode and then install the software on the server. Monitor the ATP Observation events for this server and monitor the TIE for reputation request for unknown files on the target server. Set the TIE reputation for the unknown files as Enterprise Trusted.

4.1 Service Desk – Set Adaptive Threat Protection to Observe mode

Service Desk can adjust the ATP configuration if there is an urgent issue where an unknown application is being blocked because the Adaptive Threat Protections is reacting on a wrong file reputation level.

1. In ePO Console -> System Tree -> Apply Tag “ATP Observe” on the endpoint
2. Wake-up endpoint from ePO or ask user at the endpoint to perform a “Collect and Send Props” from the McAfee Agent Icon or command line.

a. `C:\Program Files\McAfee\Agent>cmdagent.exe -p`

If the communication is not initiated manually it can take up to 120 minutes before the ATP has gone into Observe mode.

3. Make a Support incident and have the McAfee Administrators review the events collected from the endpoint to address the issue and switch the endpoint back into ATP Enable mode.

Information

It is still possible to see what is happening in ATP Observe mode. The Observe mode do generates Adaptive Threat Protection events - Would Block, Would Clean, or Would Contain - and sends them to the server, the actions are not enforced.

5 Software developers

The software developers will often be generating multiple new executables and they will all be new and unknown in file reputation based on file hash.
There are several suggested solutions to address these issue:

A. Adjust the setting for the On-Access scanner - Exclude development folders
    - Specific folder exclusions - Exclude selected developer directories to avoid all the software builds to be inspected by the antimalware and file reputation systems
        - Example could be:
            - C:\Internal\Development\ and subdirectories
            - D:\Internal\Development\ and subdirectories
            - C:\USERS*\DOCUMENTS\VISUAL STUDIO 2017\PROJECTS\ and subdirectories
        - **Important: These directories must to be agreed with the developers so they will be using the correct folders and is aware of the security implications**

B. Code signing certificate - All executables which are ready to be released are signed by a trusted code signing certificate and this certificate is configured to be trusted throughout the organization.
    - The code signing certificate needs to be marked as trusted by the internal TIE server and all executable signed by this certificate will be fully trusted.

C. Update the McAfee GTI – so the unknown executables become known and trusted by GTI
    - When the developer is ready to release the application, the unknown files can be submitted to McAfee using GetClean
    - Developer execute the GetClean against the directories with the new software
    - McAfee will send email to confirm the files has been received and will notify when the executables has been added to McAfee GTI (normal turnaround is less than 2 hours maximum 48 hours)

D. Disable the enhanced security setting based on file reputation on the developer systems
    - Not recommended

Option A is the recommended approach and the common solution used by organizations. It does require communication between the software developer teams and the ePO management teams to be able to agree on the software developments folders to exclude.
Option B is recommended as this will marked the executables as known good in McAfee GTI global file reputation

More details about GetClean can be found in separate document: “Operational GetClean”

5.1 For Policy management of the Developer workstations

If the exclusions are accepted to be included in the company baseline policy then there is no need to specially identify the developer’s workstations.

There are multiple options if there is a need to identify the developer workstations in the ePO management system for assigning specific Developer policies to these workstations.

Options for ePO to identify of developer workstations:

A) Systems can have a registry key set (CustomProps) so ePO can assign special policies to the developer workstations
   a. Example run command: `maconfig -custom -prop3 "Developer"`
   b. Then ePO will be set to tag the system as Developer if the custom Props 3 contains "Developer" and then have a policy assignment rules for the Developer policies
B) Systems can be moved to Developer OU in AD and synchronized with ePO's system tree and all systems in this systems tree group will get Developer policies assigned
C) Maintain a list (text file) located on ePO server with all the host names of the developer workstations. ePO will then schedule like every 1 hour read all hostnames from this list and tag them as Developer workstation.
   a. Then ePO will be set to tag the system as Developer if the custom Props 3 contains "Developer" and then have a policy assignment rules for the Developer policies
D) McAfee System Information Reporter (SIR) – (Windows only and on-prem ePO) can also be used to identify the development software installed and then automatically have ePO Tag the developer systems based on this. (SIR information: https://kc.mcafee.com/corporate/index?page=content&id=KB67830)
   a. It does require that it is known what developer software to look for.

Option A, B or D is recommended. Where D is the most flexible and dynamic solution as long as it is known what software "identify" a Developer system.

5.2 Host Firewall conflict with developer

ePO will not get events for all the network traffic (blocked or allowed) unless it is specifically defined as an Intrusion by an ENS Firewall Rule (only recommend for very specific traffic). Therefore, it might be needed to inspect the local ENS Firewall log file.

Depending on the ENS firewall rules applied in the organization there might be a need to apply specific Host firewall rules to the software developers' workstations.
This is only needed if software developers are creating applications which are opening and listening on network IP ports. The ENS firewall rules must then be adjusted to accommodate these behaviours on the developer's workstations.
Block traffic can be monitored in the ENS log file **FirewallEventMonitor.log** located in:
%PROGRAMDATA%\McAfee\Endpoint Security\Logs\
Or
%DEFLOGDIR%

It is possible to provide the developers options to disable the ENS firewall and provide a justification. This information will be send back to ePO.

MacOS
In order to troubleshoot ENSFW for Mac issues, you must first enable debug logging for the firewall in your Endpoint Security Common Options policy. Then, the debug firewall information will get logged into /var/log/system.log with line flags of MFE_FW.

Appendix A : Acronyms and Terms

Acronym	Description
Admin:	ePO administrator or network administrator (previously Global Admin)
Agent:	McAfee software used to manage point products on endpoint machines
AH	Agent Handler: Component of ePO used to communicate with agents installed on endpoints
AR	Active Response – also seen as MAR – McAfee Active Response
ASCI:	Agent-server communication interval
ASSC:	Agent-to-server secure communication
ATD	Active Threat Defence
ATP	Adaptive Threat Protection
CEE	Complete Protection Enterprise Suite
DAC	Dynamic Application Containment
DLPE	Data Loss Prevention for Endpoints (previously known as HDLP)
DR	Disaster Recovery
DXL	Data Exchange Layer (used by TIE and AR)
EDR	Endpoint Detection and Remediation
EEFF	McAfee Endpoint Encryption for Files and Folders (now named FRP)
EEPC	Endpoint Encryption for PC (now named MDE)
EERM	Endpoint Encryption for Removable Media (now named FRP)
ENS	Endpoint Security
EP	Exploit Prevention
ePO	ePolicy Orchestrator
ESM	Enterprise Security Management (SIEM)
FIM	File Integrity Monitor (Solidcore)
FRP	McAfee File and Removable Media Protection (previously known as EEFF)
FW	Firewall
GUID:	Globally Unique Identifier; random 64-bit value used specifically by ePO
HA	High Availability
HDLP	Host Data Loss Prevention (now named DLPE)
HIPS	Host Intrusion Prevention
MA	McAfee Agent
MAC	McAfee Application Control (Solidcore)
MAR	McAfee Active Response
MCC	McAfee Change Control (Solidcore)
MDE	McAfee Device Encryption (previously known as EEPC)
MOVE	Management for Optimized Virtual Environments
MVM	McAfee Vulnerability Manager
NDLP	Network Data Loss Prevention
NSP	Network Security Platform
NTBA	Network Threat Behaviour Analyses
OAS	On-Access Scan
ODS	On-Demand Scan

PA	Policy Auditor
Policy:	Settings and configurations applied to point-products on endpoint machines
RA	Risk Advisor
Repository:	Collection of the software used to deploy and update point-products on endpoint machines
RP	Real Protect
RSD/Sensor:	Rogue System Detection Sensor
SA	McAfee SuperAgent
SAE	Site Advisor Enterprise
SIEM	Security Information and Event Management (Nitro)
TIE	Threat Intelligence Exchange
TP	Threat Prevention
VSE	McAfee VirusScan Enterprise
WC	Web Control

Appendix B : ATP Execution flow