Adaptive Anomaly Control: Stop Attacks before They Start

An effective pre-execution protection methodology that combines the simplicity of blocking rules and the smartness of automatic tuning based on behavior analysis.

kaspersky

www.kaspersky.com/fraudprevention
#truecybersecurity

Adaptive Anomaly Control: Stop Attacks before They Start

Why Hardening Is Hard

To fight modern cyber-threats, EPP developers are constantly looking for new ways to detect malware, unsafe links and other indicators of attacks. However, despite the use of complex and resource-intensive technologies (Big Data, Machine Learning), intruders still manage to bypass these protection systems, causing significant damage to enterprises.

On the other hand, many of these threats, including APTs, can be successfully fenced off by simple non-signature methods of prevention that focus, not on attackers' tools, but on the 'hygiene' of the system under attack. If you know your system's vulnerabilities, you can proactively block actions that could lead to their exploitation. In recent years, there has been an increased focus on methods of attack surface reduction, or 'hardening', because:

Old vulnerabilities are at the root of the vast majority of recent attacks. Many well-documented flaws stay unpatched for months or even years, as fixing them involves additional technical work, together with the interruption of important business processes. The most effective way to 'cover' these unpatched vulnerabilities is to harden your security policies.

An example: the mass outbreak of attacks by the WannaCry and ExPetr cryptolockers in May-June 2017 was based on the exploitation of the EternalBlue vulnerability in the SMB protocol. The security patch for this vulnerability had become available two months earlier, but many systems hadn't yet been updated. However, some system admins prevented the infection of their vulnerable systems by implementing simple restrictions: they disabled vulnerable SMB1 transport and blocked particular TCP-ports which were likely to be attacked by the malware.

An excess of functionality built into many of todays' computer systems also helps intruders. Software vendors promote products as both 'feature-rich' and 'easy access'. When these products are run 'out of the box' as advertised, their full, excessive functionality is generally activated by default, with security settings at 'off'. So you can see why today's attackers often use legitimate applications instead of bothering with specially crafted malware, or apply social engineering to force legitimate users to do malicious actions themselves.

Take the case of MS Word documents. In early 1990, these files were considered safe, as they weren't executable. But when macros appeared, it became possible, for example, to run PowerShell straight from the document. This 'useful' functionality has lead to many malware epidemics, including attacks by cryptolockers (PowerWare), spyware (August Stealer) and APTs targeting financial institutions (Odinaff, Turla). To prevent these attacks, you don't actually have to wait until every new Trojan is detected - just disable macros in MS Office docs. It's that simple.

So, attack surface reduction can be a highly effective and inexpensive prevention technique. But - there can be drawbacks in everyday use.

General restrictions ignore specific scenarios, which can penalize legitimate users. Imagine hardening your system by applying general blocking rules like DefaultDeny throughout, only to find that the financial department has to use MS Word docs with macros, while the marketing department needs to check banner ads on websites – and your general blocking of macros and Adobe Flash has suddenly made all their lives a nightmare. If a blocking rule can't be adjusted to different scenarios, it may be impossible to apply in practice.

Manual tuning takes a lot of expert labor. Some vendors already offer hardening solutions that allow more subtle configuration of blocking rules. However, even experienced administrators are unlikely to apply these tools in full, as the manual adjustment of every rule for a whole lot of different groups and applications would take a prohibitive amount of time. On top of this, new threats and infrastructure changes require that these security policies are regularly revised, making hardening even more labor-intensive.

What is Adaptive Anomaly Control?

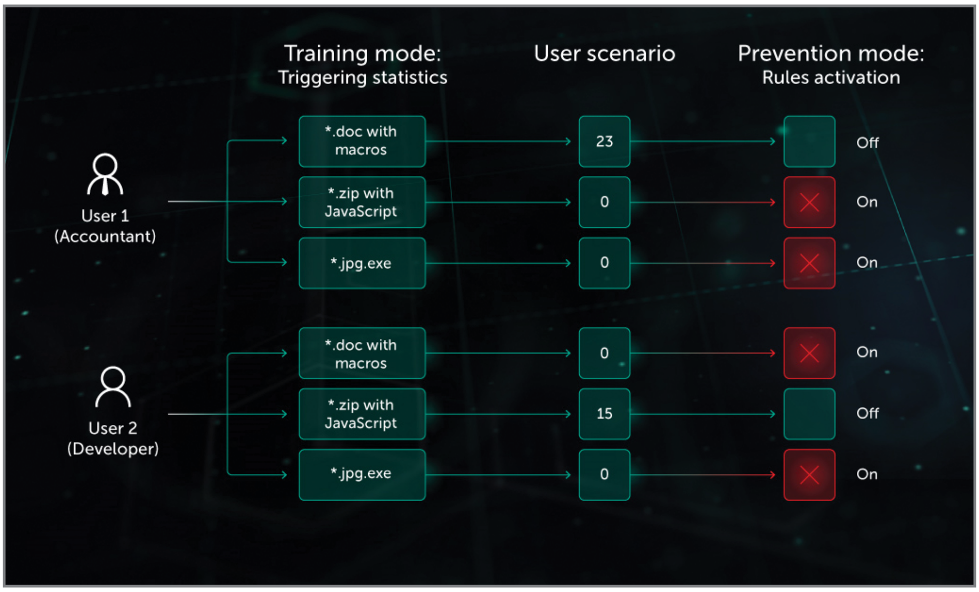
Adaptive Anomaly Control (AAC) is a smart tool for automated attack surface reduction, preventing the exploitation of the vulnerabilities or excessive functionality in a system protected by Kaspersky Endpoint Security for Business solution (KES). Key features include:

(1) A comprehensive set of effective control rules created by KL experts and based on data retrieved by Machine Learning techniques. Behavior analysis algorithms allow us to find new potential heuristics of suspicious actions in the system, but these actions could be legitimate in some specific instances – so general blocking can't be used. However, the defining and 'pinpointing' of such exceptions by experts can turn these potential heuristics into fully-functioning hardening rules.

A common example of suspicious behavior is when an application is started by some system process: Windows Session Manager, for example, or Local Security Authority Process, or Windows Start-Up Application. There are cases where this could be a legitimate action – for instance, when Windows OS boots up. The experts' task is to identify these conditions, then create a control rule that would block the execution of applications by the system process– but with appropriate exceptions allowing for the proper operation of OS.

(2) Automated adaptation (Smart Mode) based on user activity analysis. This significantly reduces the need for manual configuration of control rules. First, the AAC module starts to work in Learning Mode, collecting statistical data about control rules triggered over a specific time period - to create a normal activity model for a user or group (legitimate scenario). Then, in Prevention Mode, the system activates only those rules that block the actions anomalous to this group or user's scenario. If a pattern of normal activity should change for any reason, the AAC module can be switched back to Learning Mode, so it can create a new scenario.

For example, one indicator of a dangerous email attachment is the presence of JavaScript in the archive: Finance Department employees would never need to legitimately exchange such archives. On the other hand, this situation is common among developers. So when Adaptive Anomaly Control discovers these different scenarios it will block the attachments with active content for one group of users (Finance Department) but it will not block it for another group (developers).



	Training mode: Triggering statistics	User scenario	Prevention mode: Rules activation
User 1 (Accountant)	*.doc with macros	23	Off
	*.zip with JavaScript	0	On
	*.jpg.exe	0	On
User 2 (Developer)	*.doc with macros	0	On
	*.zip with JavaScript	15	Off
	*.jpg.exe	0	On

(3) Fine tuning. Alongside automatic mode, the system admin can control the activation of blocking rules and create individual exceptions, when the behavior to be blocked could be a part of legitimate activity of particular users, applications or devices.

For example, blocking the execution of double extension files (like img18.jpg.exe) would be the correct control rule in 99% of all cases. However, in some systems, double extension files may be used legitimately (update.txt.cmd). In this case, the admin can easily add an exception to allow for this.

(4) Multi-tool synergy. The Adaptive Anomaly Control module not only reduces the attack surface and exposure to threats, including zero-days: it also improves the collaborative performance of Kaspersky Endpoint Security for Business as a part of a Multi-Layered Security platform. The triggering of a particular AAC rule can act as a signal for closer examination of a suspicious object by other protection modules, or by experts.

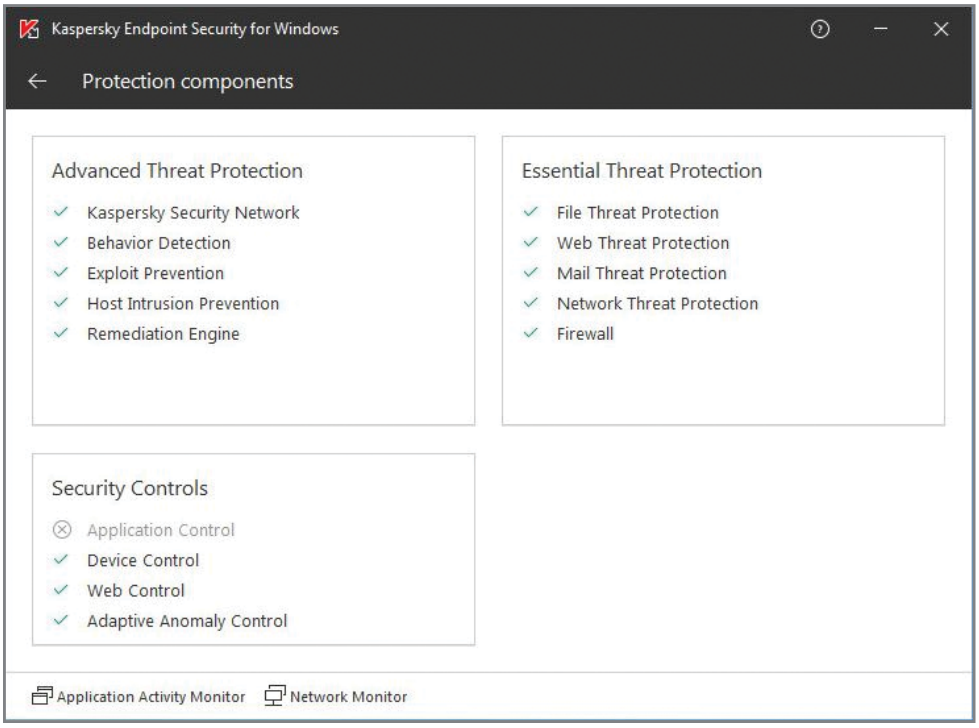
In Detail: Adaptive Control Rules

Adaptive Anomaly Control's blocking rules are created by Kaspersky Lab experts with the help of behavior analysis algorithms. New rules are added to the AAC database regularly via Kaspersky Endpoint Security for Business database updates. Rules in the database are collected into groups, such as "Abnormal program activity", "Use of WMI", "Activity of script engines and frameworks". The table below gives some basic control rules from a latest version of KES:

Rule name	Action to be blocked
RTF document anomaly	The Microsoft Word application has opened an RTF document containing anomalies typical of the RTF format
Document with SWF attachment	Office application opens a document with an SWF attachment containing code
Start of Microsoft Register Server from office application	Office application starts Microsoft Register Server
Start of Microsoft HTML Application Host from office application	Office application starts Microsoft HTML Application Host
Start of Microsoft Console Based Script Host from office application	Office application starts Microsoft Console Based Script Host
Start of Microsoft Windows Based Script Host from office application	Office application starts Microsoft Windows Based Script Host
Start of Microsoft Windows Command Processor from office application	Office application starts Microsoft Windows Command Processor
Start of Microsoft PowerShell from office application	Office application starts Windows PowerShell
Start of embedded file from Office application	Running an executable file embedded in an Office document
Start of Microsoft HTML Application Host from WMI	Running Windows Powershell through Windows Management Instrumentation (WMI)
Start of Microsoft Powershell From WMI	Running Windows Powershell through Windows Management Instrumentation (WMI)
PowerShell executes external code	PowerShell script executes external (downloaded) code
PowerShell script executes unknown dynamic code	PowerShell script executes unknown dynamic code (generated on execution)
PowerShell executes obfuscated code	PowerShell script executes obfuscated code
PowerShell calls Native API	PowerShell script calls the Native API application programming interface
Non-standard file for the folder	The program and/or script is run from a standard or system directory that does not contain such executable files in the default configuration
System file in a non-system folder	The program with the name of the system process (for example, explorer.exe) is run from a non-system directory
Untrusted application with a system-like name	Running an untrusted program with a name similar to the name of the system process (for example, explorer.exe)

Adaptive Anomaly Control in the Kaspersky Endpoint Security for Business Interface

The AAC module settings can be found in the Security Controls menu:



Advanced Threat Protection

- ✓ Kaspersky Security Network
- ✓ Behavior Detection
- ✓ Exploit Prevention
- ✓ Host Intrusion Prevention
- ✓ Remediation Engine

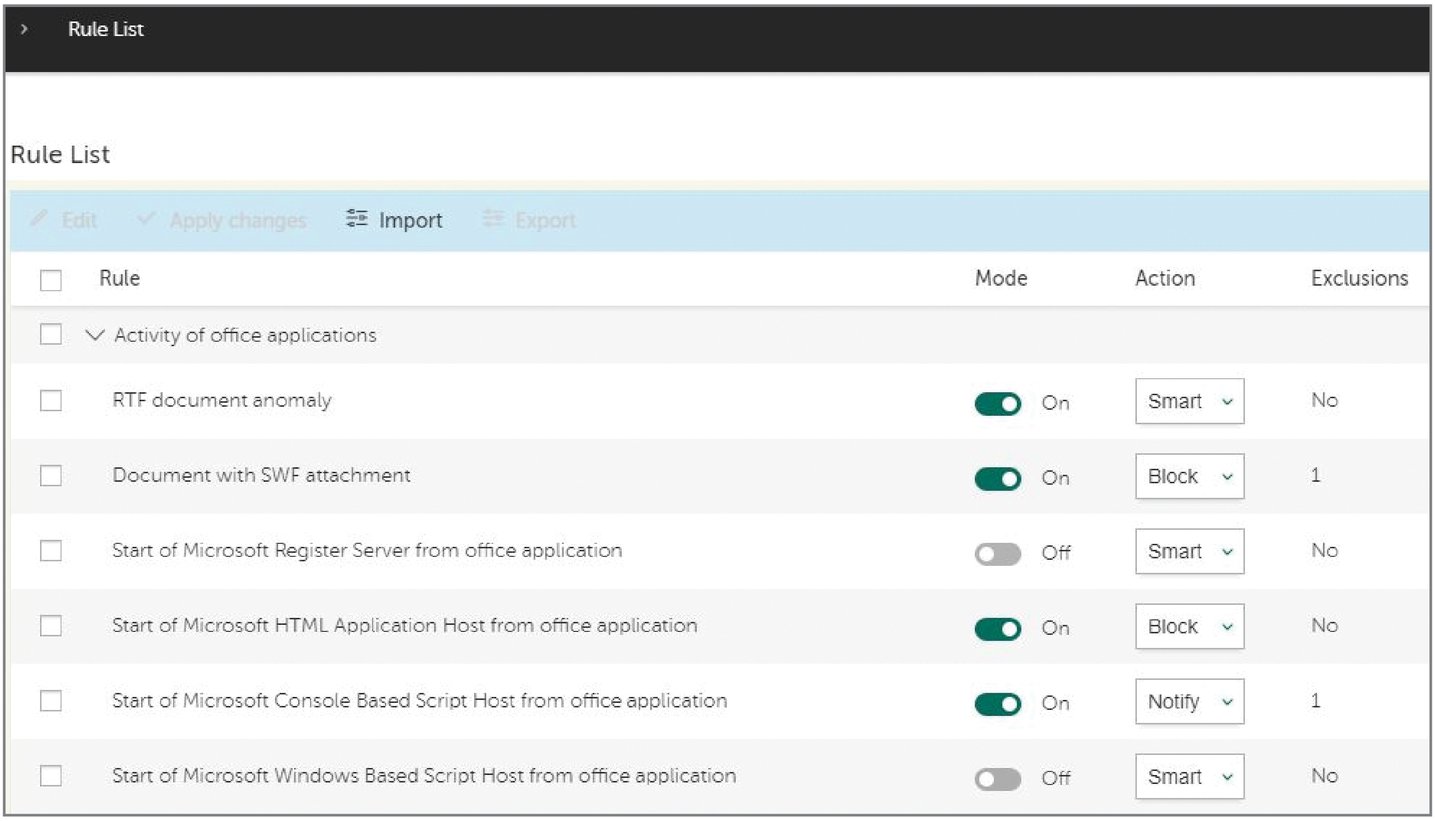
Essential Threat Protection

- ✓ File Threat Protection
- ✓ Web Threat Protection
- ✓ Mail Threat Protection
- ✓ Network Threat Protection
- ✓ Firewall

Security Controls

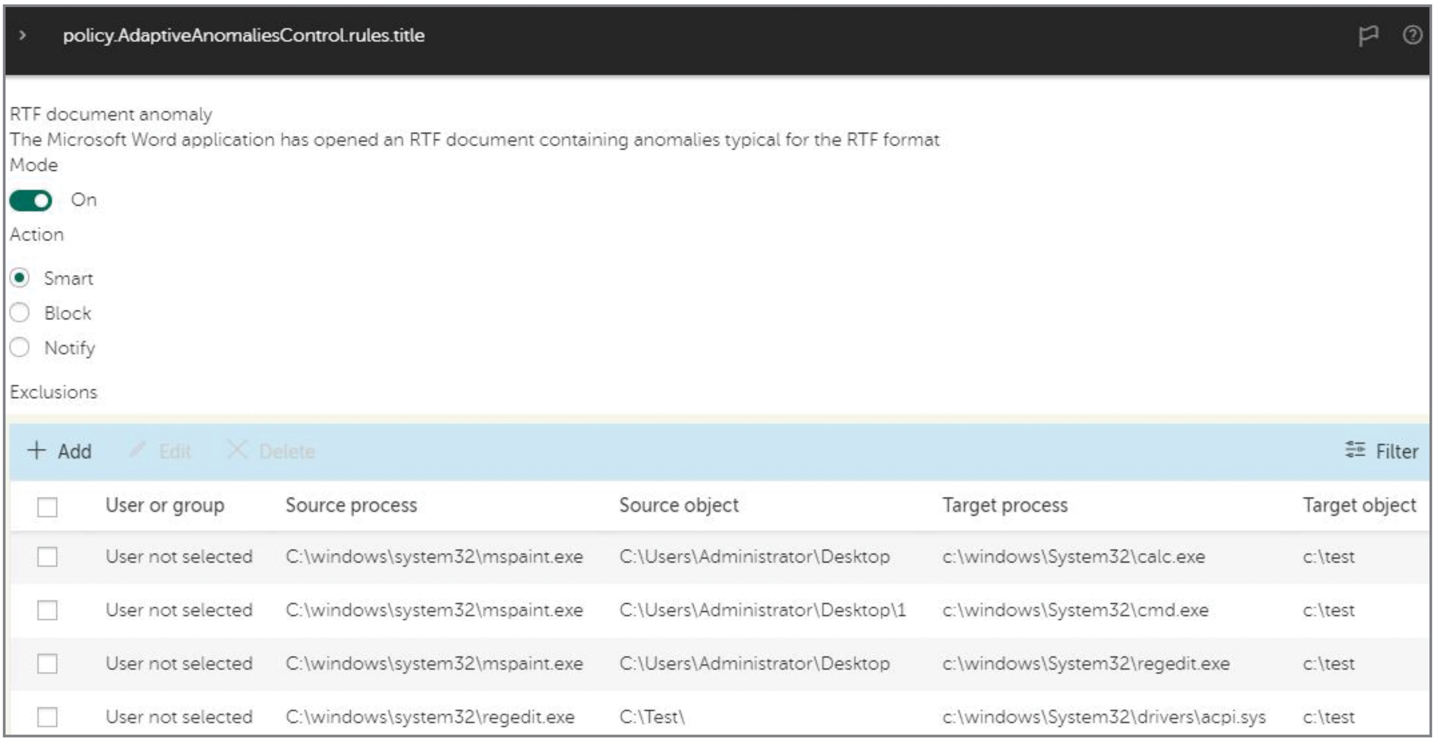
- ⊗ Application Control
- ✓ Device Control
- ✓ Web Control
- ✓ Adaptive Anomaly Control

Below, you can see a list of AAC rules being applied - with their Mode, Action and Exclusions parameters:



□ Rule	Mode	Action	Exclusions
□ Activity of office applications			
□ RTF document anomaly	On	Smart	No
□ Document with SWF attachment	On	Block	1
□ Start of Microsoft Register Server from office application	Off	Smart	No
□ Start of Microsoft HTML Application Host from office application	On	Block	No
□ Start of Microsoft Console Based Script Host from office application	On	Notify	1
□ Start of Microsoft Windows Based Script Host from office application	Off	Smart	No

Tuning a particular AAC rule - you can select Action and set a list of Exclusions here:



RTF document anomaly
The Microsoft Word application has opened an RTF document containing anomalies typical for the RTF format
Mode

On

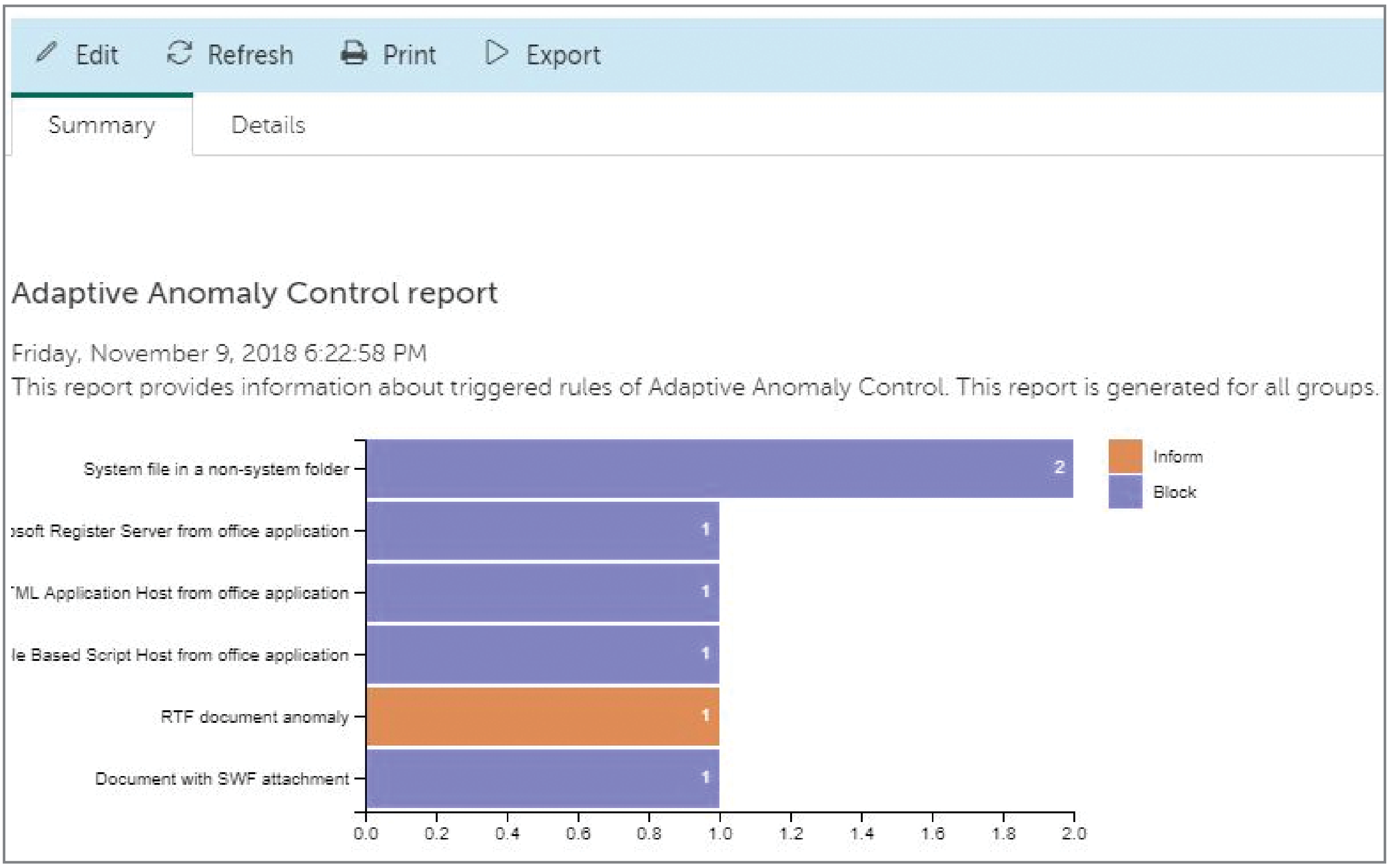
Action

● Smart
○ Block
○ Notify

Exclusions

☐	User or group	Source process	Source object	Target process	Target object
☐	User not selected	C:\windows\system32\mspaint.exe	C:\Users\Administrator\Desktop	c:\windows\System32\calc.exe	c:\test
☐	User not selected	C:\windows\system32\mspaint.exe	C:\Users\Administrator\Desktop\1	c:\windows\System32\cmd.exe	c:\test
☐	User not selected	C:\windows\system32\mspaint.exe	C:\Users\Administrator\Desktop	c:\windows\System32\regedit.exe	c:\test
☐	User not selected	C:\windows\system32\regedit.exe	C:\Test\	c:\windows\System32\drivers\acpi.sys	c:\test

Here you can view the most triggered AAC rules for all user groups:

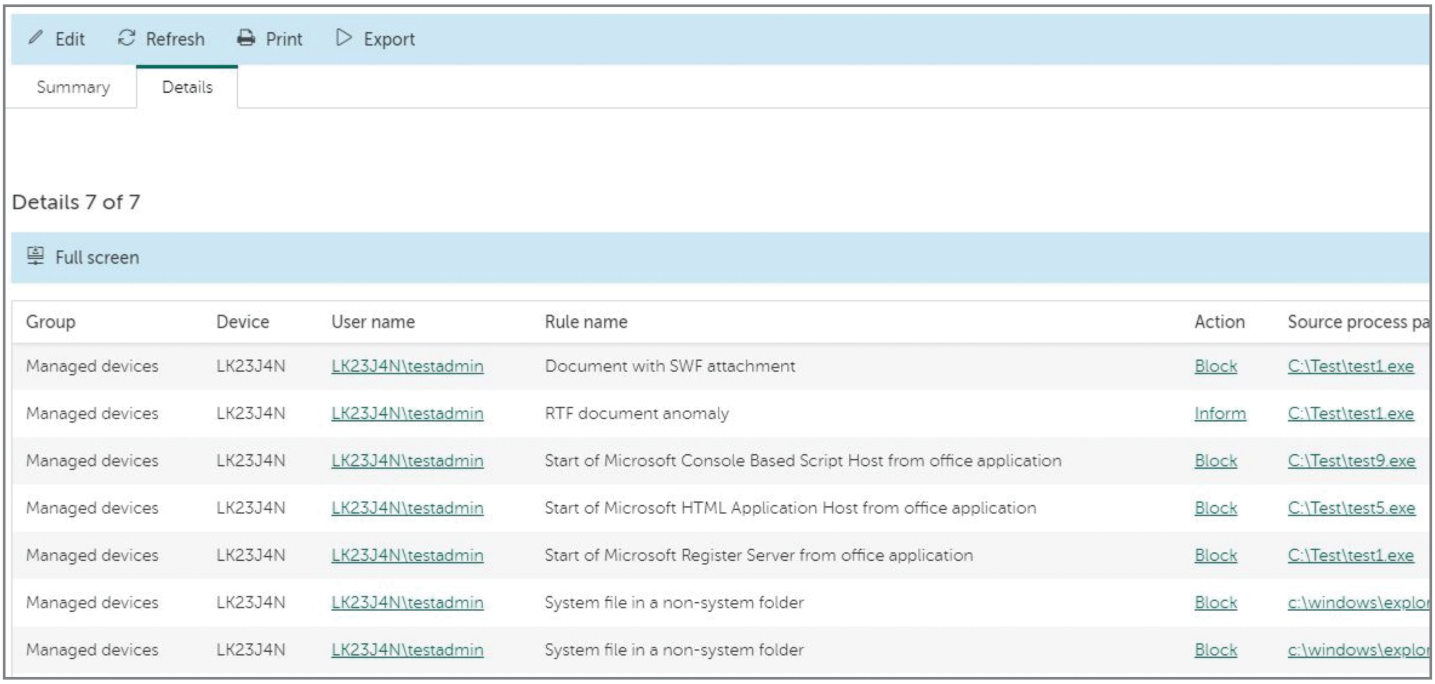

Edit
Refresh
Print
Export
Summary
Details

Adaptive Anomaly Control report

Friday, November 9, 2018 6:22:58 PM
This report provides information about triggered rules of Adaptive Anomaly Control. This report is generated for all groups.

System file in a non-system folder
2
ɔsoft Register Server from office application
1
'ML Application Host from office application
1
le Based Script Host from office application
1
RTF document anomaly
1
Document with SWF attachment
1
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
1.8
2.0
Inform
Block

The detailed log of Adaptive Anomaly Control rules applied to different user groups:



Details 7 of 7

Group	Device	User name	Rule name	Action	Source process pa
Managed devices	LK23J4N	LK23J4N\testadmin	Document with SWF attachment	Block	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	RTF document anomaly	Inform	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft Console Based Script Host from office application	Block	C:\Test\test9.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft HTML Application Host from office application	Block	C:\Test\test5.exe
Managed devices	LK23J4N	LK23J4N\testadmin	Start of Microsoft Register Server from office application	Block	C:\Test\test1.exe
Managed devices	LK23J4N	LK23J4N\testadmin	System file in a non-system folder	Block	c:\windows\explor
Managed devices	LK23J4N	LK23J4N\testadmin	System file in a non-system folder	Block	c:\windows\explor

Summary

Attack surface reduction is a highly effective and comparatively inexpensive method of defending your systems against a wide range of threats, both known and completely new ones. However, general hardening can also be a bit of a blunt instrument. Adaptive Anomaly Control is our way to fine-tune that instrument, applying Machine Learning techniques to minimize the manual labor required from system administrators and security experts to ensure that every user is protected, but no user is inconvenienced. This technology enables you to customize systems hardening right down to the level of the individual, or to apply tailored access rules to each of the different areas of your workplace, reflecting their various unique requirements. This smart automated tuning of the blocking rules adds another layer of protection to the Kaspersky Endpoint Security's for Business technology stack that provides you with powerful defenses in a dangerous and unpredictable cyber-world.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

www.kaspersky.com

BRING ON
THE FUTURE