Application Control Comparison Test

A test commissioned by Kaspersky and performed by AV-TEST GmbH

Date of the initial report: December and November 2013

Executive Summary

Application Control and Whitelisting technologies help protect systems from both known and unknown threats by giving administrators complete control over the kinds of applications and programs that are allowed to execute and run on their endpoints, regardless of end user behavior.

In addition to being able to block or allow specific, chosen applications, some solutions allow administrators to control how applications behave – for example, what resources they can use, what kind of user data they can access or modify, whether they can write to registries etc. This means administrators can prevent any application from executing actions that could endanger both the endpoint and the network to which it is connected.

At the end of 2013, Kaspersky Lab worked with AV-TEST to develop and agree on a universal test outline for Application Control and Default Deny functionality using Whitelisting. AV-TEST compared the Application Control solutions of leading enterprise security vendors; Kaspersky, McAfee and Symantec agreed to participate in this test, while Bit9 and Sophos declined.

By preventing the execution of unsolicited, unnecessary and potentially dangerous programs, Application Control and Whitelisting makes the corporate network environment controllable, predictable and safe. The main business benefits of using Application Whitelisting solutions are:

- Enhanced awareness of what is running on your IT network
- Continuously updated Dynamic Whitelists ensure you will always know whether an application can be trusted.
- Ability to block executable malware agents – even unknown ones
- Choice of Default Allow scenario for 'safer freedom' or Default Deny scenario for maximum security
- Granular controls and categorization let you decide which programs are allowed to run – reducing the risk of Data Leaks, License Violation or unneeded Resource Consumption
- Lowers ownership costs by reducing need for maintenance

Application Control provides an additional layer of protection to a broader IT security strategy. As such, this test should not be regarded as a standalone security test for protection but complementary to existing security features for host protection in an enterprise environment.

While most solutions support dynamic systems and evolving user environments, ease of implementation and operation can vary significantly, including:

- **Effort**: Ease with which administrators can deploy and maintain application control.
- **Value:** Genuine usefulness of features and functionality to system administrators.
- **Impact**: Potential negative impact of Application Controls on user experience and network performance.

These three parameters, which may influence the adoption of Application Control within the enterprise, formed the basis of this test report. Each solution was analyzed and scored for effort, value and impact in the following categories: Deployment, Configuration, Monitoring, Response and Support.

Effort: Easiest to deploy and maintain

Kaspersky's Application Control solution was the easiest to deploy and maintain, receiving the highest grade 'Excellent' in the 'Effort' test category. A feature of Kaspersky's Endpoint Security solution, Application Control is managed centrally through the Kaspersky Security Center. It convinced with its combination of quick and easy to use functions and available features. A complete, out-of-box product, it requires little training and offers a full administrator feature set. Many unique capabilities are available for specific use cases.

Value: Feature range, capabilities and options

McAfee's Application Control - a module of its ePolicy Orchestrator(ePO) - came first in the 'Value' category, receiving the 'Excellent to Very Good' grade. It provides a wide range of features: from extensive filters to GUI customization capabilities. This solution offers almost all the features you would expect in an Application Control solution.

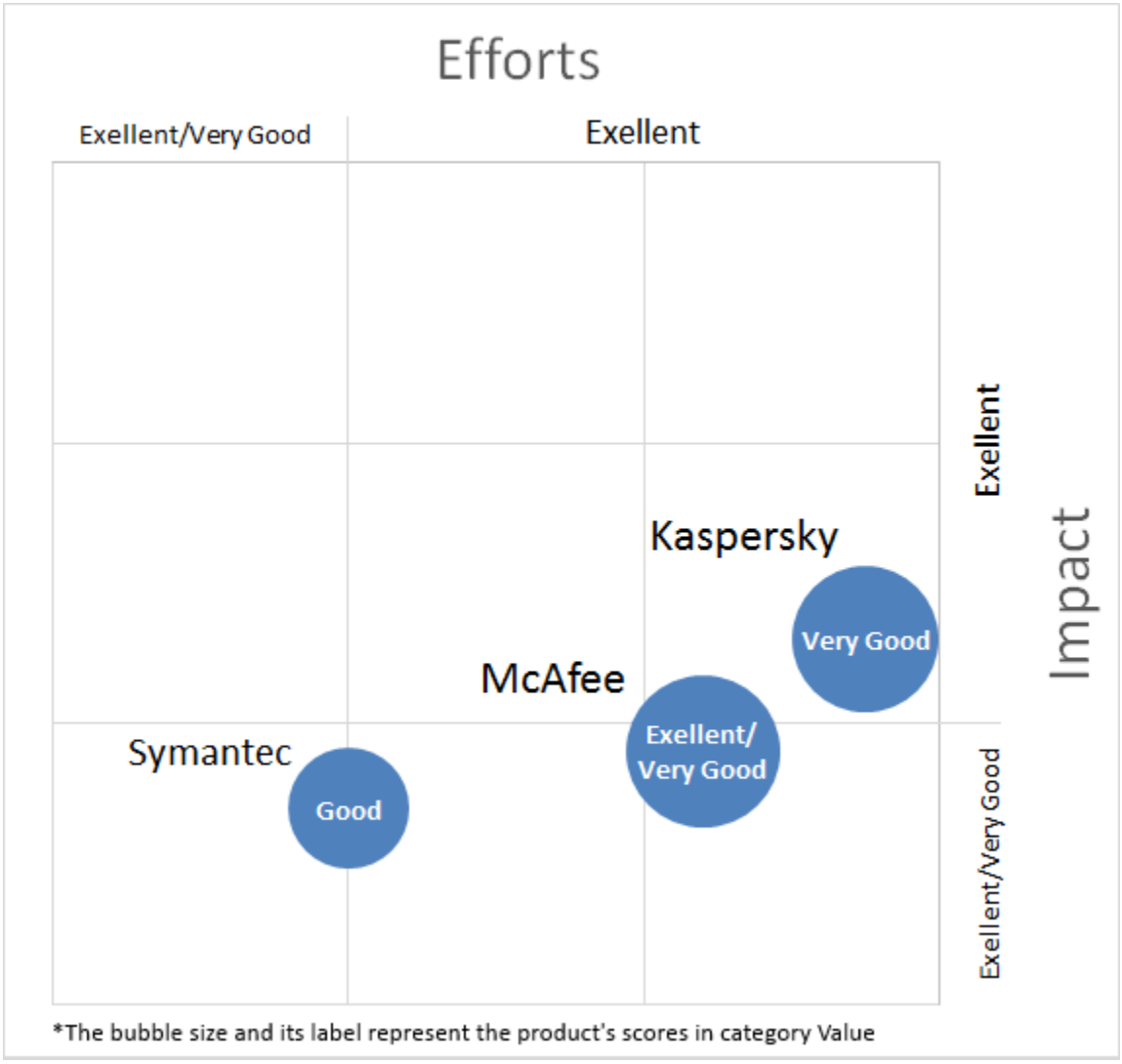
Impact: Most efficient resource usage, greatest transparency

Kaspersky's Application Control solution offered the greatest transparency with the most efficient system resource usage, earning it the 'Excellent' grade in the 'Impact' category. Administrator actions take place in the background; inventory creation is automatic and takes place imperceptibly, ensuring that there are no breaks in normal productivity and significantly reducing the potential for user complaints. Following deployment, no reboot is required and no client interaction is needed at either set up or running stages, meaning performance issues are almost non-existent.

Overall, Kaspersky outperformed all test participants, achieving the best results. McAfee came second, while Symantec Endpoint Protection came third in this test.

Application Control in Symantec's Endpoint Protection software comes as a static Whitelisting module that offers only standard Whitelisting functionality. Its 'Lockdown' function provided the basic security levels required by any Whitelisting program and tasks were easy to perform in just a few steps. The user interface and design make using most of the features a quick and easy process; Symantec scored 'Very Good to Excellent' in the Effort and Impact categories.

The below chart illustrates the overall results for each product tested, where X is used for scores in the 'Impact' category and Y represents scores for 'Effort'; bubble size and labels indicate scores for the 'Value' category.



Products Tested

The following products were tested:

Vendor	Product	Version
Kaspersky	Security Center	10.1.249
	Endpoint Security	10.2.1.23
McAfee	ePolicy Orchestrator	5.0.1 (Build: 228)
	Solidcore	6.1
Symantec	Endpoint Protection	12.1.4013.4013

In addition to the tested vendors, Bit9 and Sophos had been contacted by AV-TEST in order to include their solutions in the test as well. The test methodology has been shared with those companies, however they declined having their product tested. Bit9 claimed that their product does not fit into the test; also, Bit9 stated they generally do not participate in tests that are initiated or sponsored by other vendors. Sophos made similar claims, stating that their product works differently and that the testing methodology would be biased to certain products/features.

AV-TEST is of course respecting the decisions of those two vendors but still believes that their products would have perfectly fit into the test. Bit9 clearly states that they support features that are reviewed in this test, proof can be found on their website[1]. Sophos defines application control as a blacklist based approach instead of a whitelist based one. However, the test was designed to cover both approaches equally well and if problems would have occurred here, the testing methodology could have been revised.

[1] https://www.bit9.com/solutions/application-control/

Overview

Modern security products in private and corporate environments provide security protection in depth using a number of features. One of these is the classic approach of blacklisting malicious files. The ever increasing volume of malware samples, along with a significant increase in highly targeted attacks make it hard for traditional security techniques to protect systems completely. Whitelisting of known good files, along with the default prevention of any unauthorized applications from executing can help increase protection significantly.

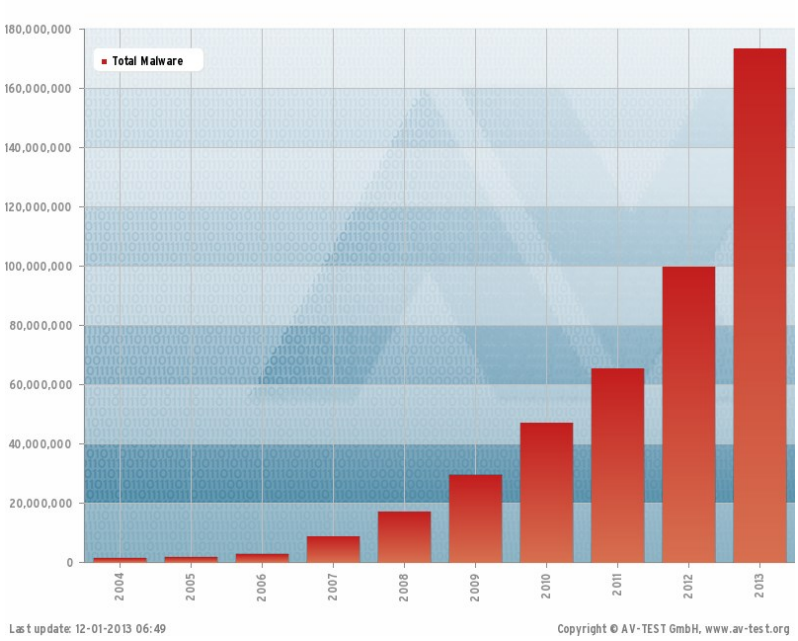


Figure 1: development of new malware sample found per year over the last 10 years[2]

Application Control technology was developed by security vendors around 2005; recent years have seen wider enterprise recognition of its value as a "must have" feature in Endpoint Protection solutions. Building on developments in Application Control, including Default Deny (or lockdown mode), Whitelisting has become a key element in protecting corporate networks, making 100% detection rates possible. This represents a shift away from the traditional 'pursuit paradigm' of older Antivirus technologies; the 'blacklisting' approach can lead to inferior detection rates, enabling highly sophisticated malware to side-step Antivirus.

It is now clear to many security experts that Default Deny is a mandatory countermeasure to protect critical infrastructure and organizations from Advanced Persistent Threats (APTs). In addition, European and US governments have begun developing regulations that will oblige organizations to implement Default Deny in their networks.

[2] http://www.av-test.org/en/statistics/malware/

Notes on tested products

Kaspersky

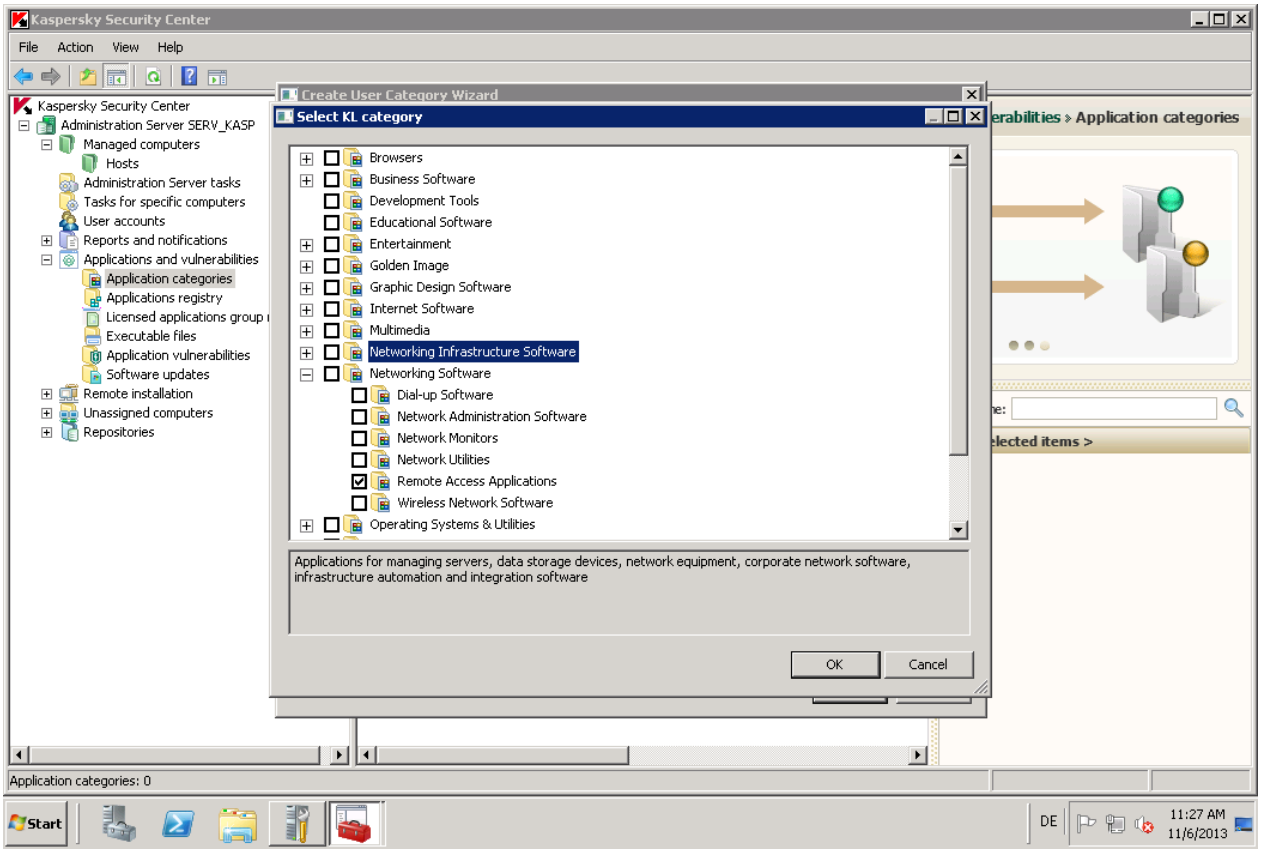


Figure 2: The "Application Startup Control" module in Kaspersky Security Center shows predefined categories of software

Kaspersky's Application Startup Control is part of a standalone Kaspersky Endpoint Security product which, like other Kaspersky products, can be managed from the Kaspersky Security Center. It is an ideal extension for existing Kaspersky installations. The good integration in Kaspersky Security Center (KSC) is a significant advantage, especially for enterprises already using Kaspersky. The usability is similar to other modules such as Endpoint Security. Enforced policies include conditions and exceptions, which can be assigned using multiple options. Newly executed files are added automatically to the inventory, where they can be assigned to custom categories. Kaspersky's cloud-based KSN feature assigns the Trust Level of a file, which can be viewed in the inventory.

McAfee

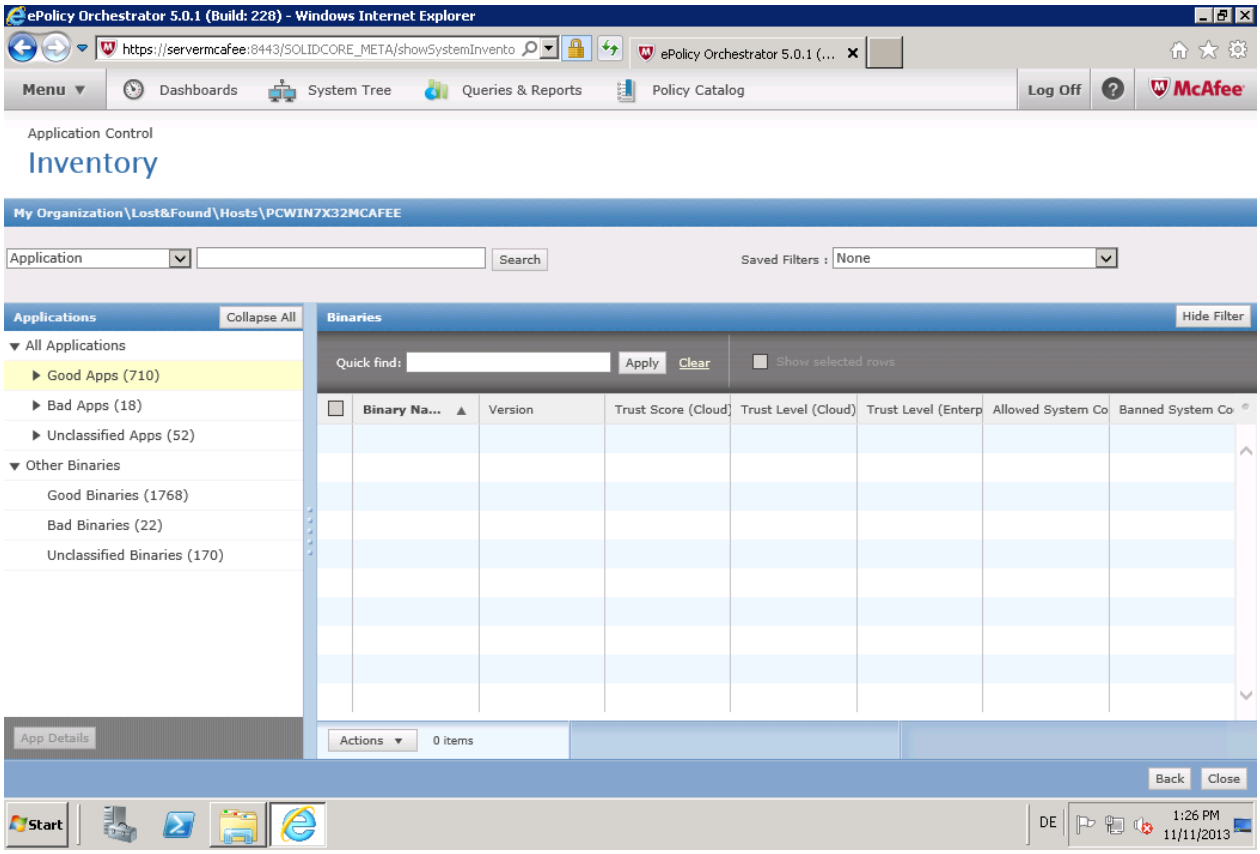


Figure 3: The "Application Control" module in the ePolicy Orchestrator shows all applications listed on the controlled hosts

McAfee Application Control (former Solidcore) is one of many additional software modules available for McAfee corporate management framework. As with Kaspersky, it is a great extension for existing McAfee installations. The usability is similar to the rest of the ePolicy modules. McAfee uses its GTI file reputation service to classify files found and executed on the systems. The original solidified[3] files from the hosts are allowed by default whatever the classification and it is up to the administrator to ban them from execution. Helpful for this task are the filter option made available. Newly added files are automatically added to the Inventory and can be added to the rules, which are then added to the applied policies.

[3] A solidified file, is a file added to the inventory by McAfee and allowed to execute.

Symantec

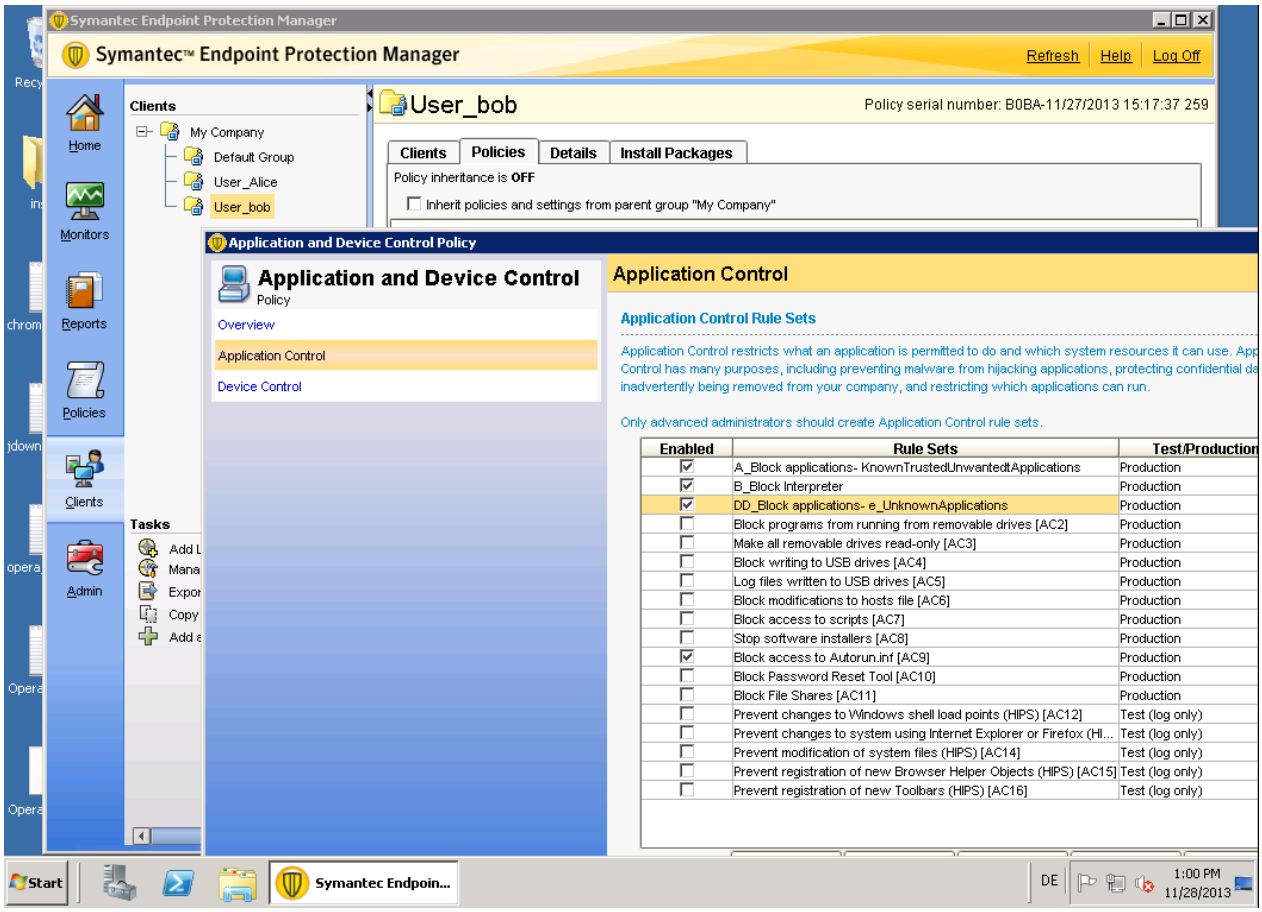


Figure 4: The Application Control in Symantec is the "lockdown" mode allowing specific rules applied for the separate users or host machines

Symantec's application control feature is readily available in the Endpoint Protection (SEP). An inventory has to be created which adds all DLL and EXE files found on the client system. After, the activation lockdown feature can be enabled. All files added to the inventory will be allowed to execute. The users or computers are added to groups which are assigned policies in which either the rules are inherited or they can be manually changed. Symantec offers two options for delivering policies to the clients, the administrator can choose between the push and the pull options.

Test Setup and Methodology

This test is focused on the business case for protecting the corporate environment from Advanced Persistent Threats by using Application Control technology operating in Default Deny mode. This test measures the efficiency of an Application Control solution as either a standalone product or a feature integrated into an Endpoint Protection suite. The efficiency of tested solutions was measured in terms of Effort, Value and Impact through a generic lifecycle of a security solution, consisting of five stages: Deployment of product's agent to endpoints, configuration of product's settings & policies, monitoring for events, response to threats and support of end users. Due to the different whitelisting approaches adopted by the vendors, a direct feature comparison between the products is not productive. The products were evaluated against the assumed "ideal" solution under the given conditions. (Details on ideal solution in Appendix).

Application Control is part of security applications used to centrally manage corporate environments. To emulate this, a HyperV2012© based network of systems was set up, including a Domain Controller and Server for the products, both in the form of a Windows 2008 R2. Also included in the network was a Windows XP SP3 32bit and a Windows 7 SP1 32bit machine to function as client system.

The Domain Controller is used to provide control over users in the emulated corporate network. It also provides an Active Directory for the protection server to choose hosts from.

The two host systems Windows XP and Windows 7 are not fully updated. This enables Vulnerability Detection by the Administration Console. The updates have been disabled in order to measure how well exploitable systems can be handled. The to-be tested applications are installed on these systems before the deployment of host agents (Appendix).

The pre-assembled systems are cloned for the three tested products and added to the Domain Controller. They are equal in setup, except for network configurations. After preparing the emulated corporate environment the Administration Consoles are installed using best practice methods or, if not available, default settings.

All products will be fully-functional licensed software unless the vendor of a specific product confirms that a trial version is fully equivalent to a licensed version and is willing to have it tested as such.

A live internet connection will be provided to all systems.

The third-party software used to demonstrate a product's application control abilities will be comprised of a range of products, including professional productivity applications (and different versions thereof); internet and other communication tools; software designed for leisure (e.g. games); and other applications that users are likely to want or need to install in a business environment.

This concludes the preparation of the test environment.

Test Results

Overview

Kaspersky

	Effort	Value	Impact
Deployment	Excellent/Very Good	Very Good	Excellent/Very Good
Configuration	Excellent	Excellent/Very Good	Excellent
Monitoring	Excellent	Very Good	Excellent
Response	Excellent	Very Good	Excellent
Support	Excellent/Very Good	Very Good	Excellent
Total	Excellent	Very Good	Excellent

McAfee

	Effort	Value	Impact
Deployment	Very Good/Good	Excellent	Very Good
Configuration	Excellent/Very Good	Very Good	Excellent
Monitoring	Excellent	Excellent	Excellent
Response	Excellent	Very Good	Excellent
Support	Excellent/Very Good	Excellent	Excellent
Total	Excellent/Very Good	Excellent/Very Good	Excellent

Symantec

	Effort	Value	Impact
Deployment	Excellent	Good	Very Good
Configuration	Excellent/Very Good	Good	Excellent
Monitoring	Excellent	Very Good	Excellent
Response	Excellent	Very Good/Good	Excellent
Support	Very Good/Good	Poor	Very Good
Total	Excellent/Very Good	Good	Excellent/Very Good

Deployment

General

All products have the hosts added to the Administrator Consoles followed by the configuration of deployment and deployment of the agents. The option to deploy the agent to the hosts can be scheduled by all products. The domain and administrator credentials need to be entered for the deployment to the hosts. After confirmation of deployment the Administrator Consoles will show the status of the deployment.

Kaspersky

Adding the host is quick and straightforward. The list of host machines to be added is taken from the Active Directory. Subsequently, the deployment of the agent is not dependent on the active state of the machine but can be scheduled to run at a later time at which the machines are active. This is quite an advantage, it reduces the step of deployment for non-active machines which would otherwise need to be added first to the list of hosts. If the machines already have the product installed, the option to skip these hosts is made available. The Agent installs successfully and starts without requesting an additional reboot of the host; there are some minor performance issues during the installation of the agent.

The task for the deployment of agents offers some useful options to the administrator, such as deletion of previously installed security products, an adaptable reboot warning or the option to force/skip the reboot of the system after deployment, which may be required by other security features available in KSC or if other security products have been removed.

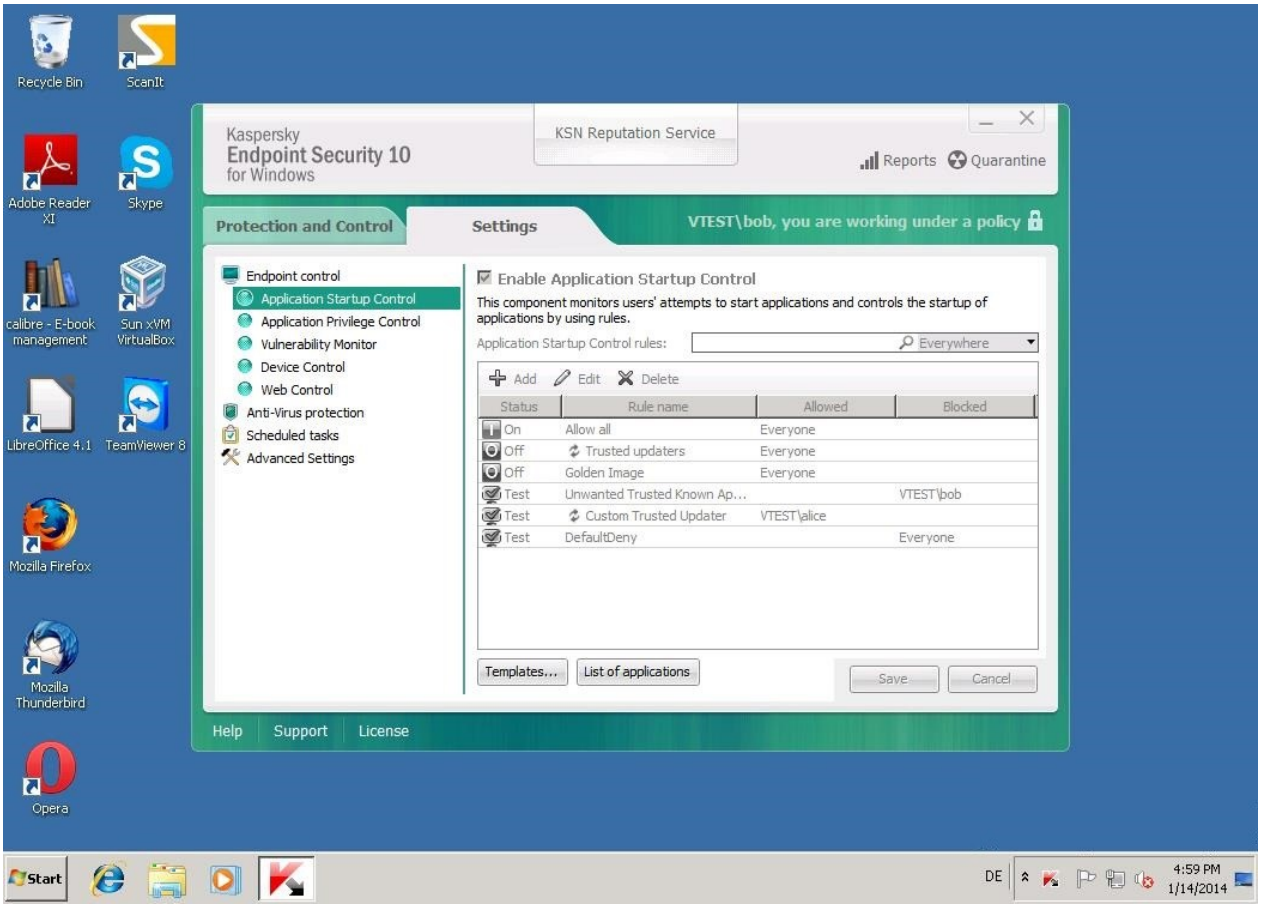


Figure 5: Kaspersky Endpoint Security Agent deployed on Windows 7 with active policies

McAfee

The Application Control in McAfee requires more steps to deploy than the other products tested. When adding the host to the administrator console, the option to deploy the ePolicy Orchestrator agent, which is required for the management, is offered. This can be done quickly and would usually not be necessary if the product was already in use in the corporate environment. Most actions in McAfee ePolicy Orchestrator require a particular task to be created and assigned. The same applies for the deployment of the Application Control. This takes few steps and must only be done once and can be reused for future deployments. After the deployment of the Application Control to the hosts, the system will reboot with a timer of five minutes. The user cannot abort or postpone the reboot by default. The administrator has the options in the deployment task to change the reboot time, activate the postpone option and to create a customized message accordingly.

The deployment agent offers some useful options to the administrator, such as choosing the type of operating system to deploy to, install or removal of the product deployed and deployment only to hosts with certain tags.

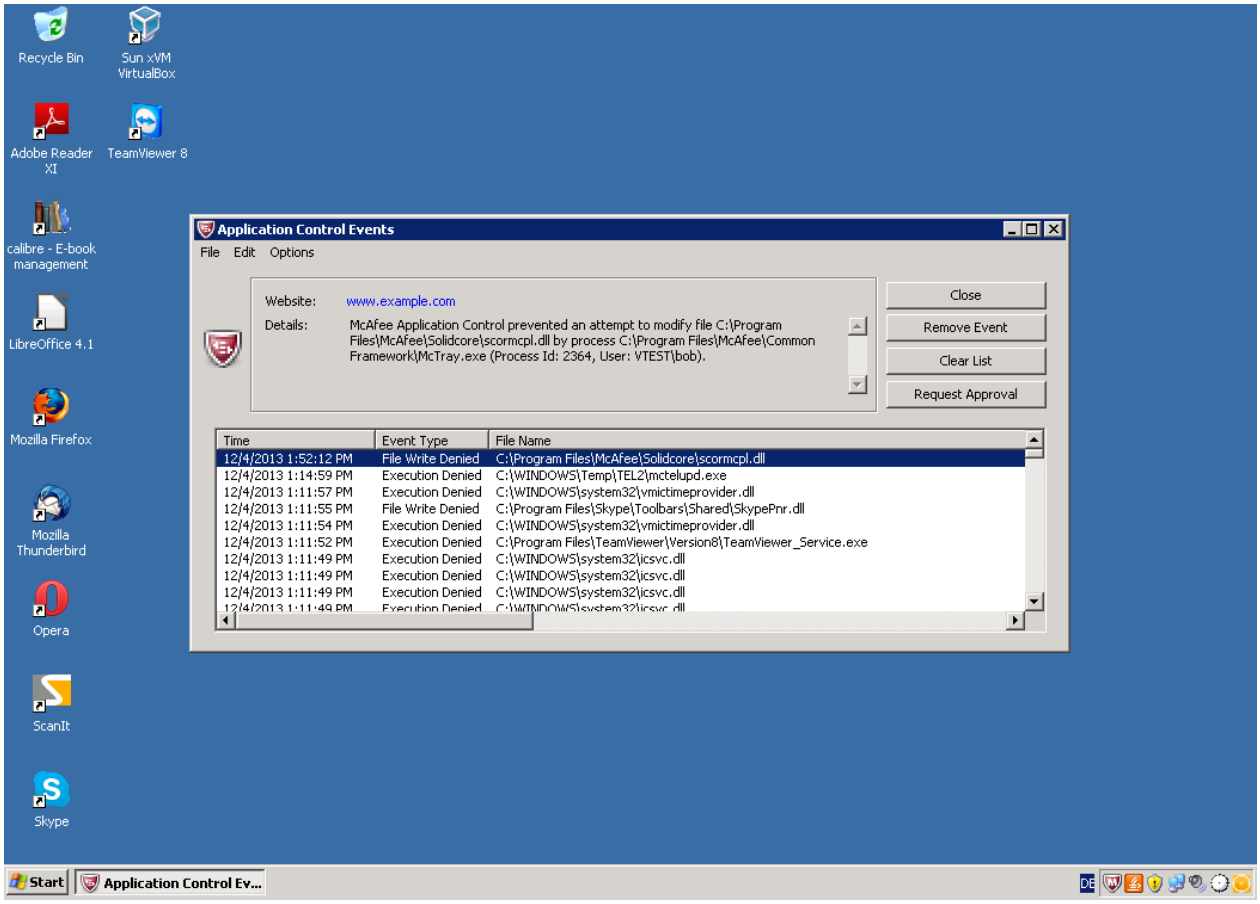


Figure 6: McAfee's Application Control as part of the Agent displays blocked files

Symantec

Symantec offers client deployment straight from the welcome window following the start of the Endpoint Protection Manager. When adding the hosts for deployment, only active systems are displayed. Systems which are offline, disconnected or simply not displayed can be added using the import option which allows adding hosts from a list, holding either the computer name or IP addresses. If a host is for some reason not available in the list but active, there is also the option to search by IP or IP range. The default deployment does not include scheduling but the task can be added easily at a later stage. The host system asks for a reboot after deployment, which can be postponed by the user. The lockdown enablement needs to be started manually in the SEP.

The deployment agent offers some useful options to the administrator, such as selecting the features and package to be deployed and the option of default mode used after deployment, which is either computer mode or user mode (more on this later).

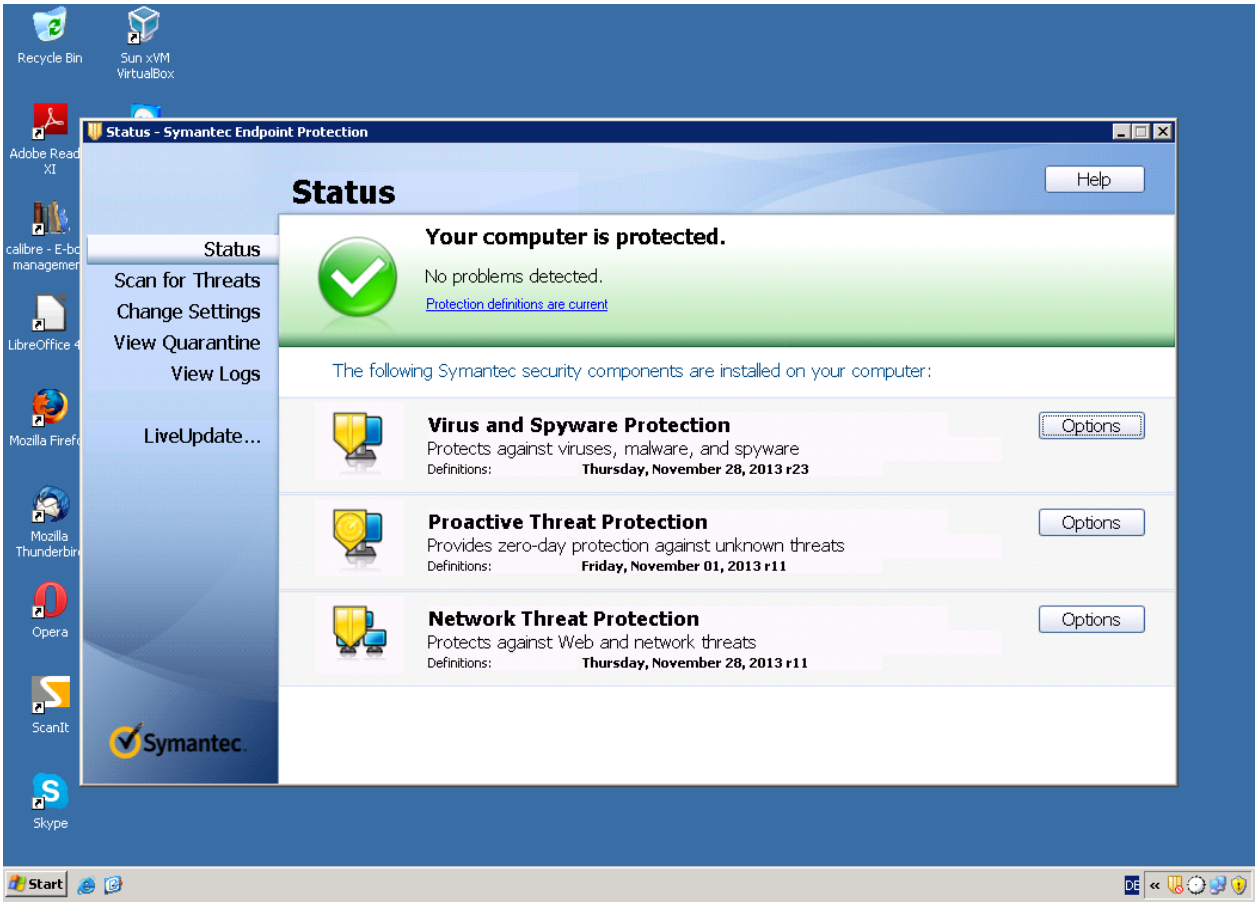


Figure 7: Symantec Endpoint protection has the "Lockdown" integrated as an additional security feature

Conclusion

Kaspersky takes only a few more steps for complete roll-out than Symantec but considerably less than McAfee. Ease of use is similar to Symantec but the GUI is the best organized of all the products. Adding inactive hosts and being able to schedule agent deployment for those is a great advantage.

Most tasks in McAfee take more effort due to the module setup of the Administrator Console. On the other hand, McAfee convinces with its options for deployment configuration. Once the tasks are created, the usage and further deployment is a lot easier and quicker. Like Kaspersky, systems can be added from the Active Directory or even by listening for ARP noise to detect non-managed systems in the network. This requires the Rogue System Detection module to be added to the ePo.

Symantec takes significantly fewer steps for adding hosts and agent deployment. It is also very simple, intuitive and can be used out of the box. Having said that, the scheduling option is not included in the default deployment of the agent and following deployment, rebooting and adding inactive hosts through IP tables is a inconvenience.

Configuration: Policy creation and Information gathering

General

In order to manage the clients with any of the Application Controls, an inventory needs to be created. The inventory lists the files which are allowed or forbidden to execute. The file types listed vary with the product. Symantec and Kaspersky list only PE files such as DLL and EXE whereas McAfee also includes script files. All products can block files by path and filename or by their hash. Kaspersky and McAfee also offer the option to schedule the creation or update of the inventory tasks. When creating the inventory basic system information is also gathered, such as details on the operating system, available memory and hard drive space. One way to block or allow interpreter scripts in all products is by simply including extensions in an assigned rule.

All products provide some form of "Test" mode. It allows normal execution of an application but instead of blocking the application, the execution is allowed and the usual action such as block is only logged. This allows testing of applied policies and how they would interfere with the day to day work.

Kaspersky

When creating the inventory task the user can choose to scan certain paths or entire drives. The administrator can also choose to scan archives, MSI packages or exclude scanning large compound files above a certain size. The process of creating an inventory also gathers an exhaustive range of information from the host. This includes a list of all applications found in the registry, detailed hardware information and available Windows updates. The file details in the inventory include among others a trust level assigned from the Kaspersky HIPS.

Kaspersky allows the creation of whitelists for the systems, which can be added to a policy as a category. In addition to this classic approach, Kaspersky provides a classification of many files into predefined categories, including 16 main- and numerous sub- categories. These categories can be used to create a baseline to ensure running of the system without allowing non-required applications. This ensures that only approved applications installed on the system upon deployment of the security product can be executed by default, which is a great security advantage. The created categories are added to a policy and applied to a user or user groups found in the Active Directory. An action is assigned to a rule being either Allow or Block. The policy will be applied to a host or group of host machines.

Different methods for filling the custom categories can be used such as: file hash or file information; using details from installer packages; by device type; using manufacturer name which can be extracted from the registry, files and installer; and from extracted information from files in specified folder.

The test mode in Kaspersky makes it possible to deploy a rule in a policy and let it log potential policy violations without having to actually enforce them. This allows the administrator to validate a new rule before implementing is across the entire corporate environment.

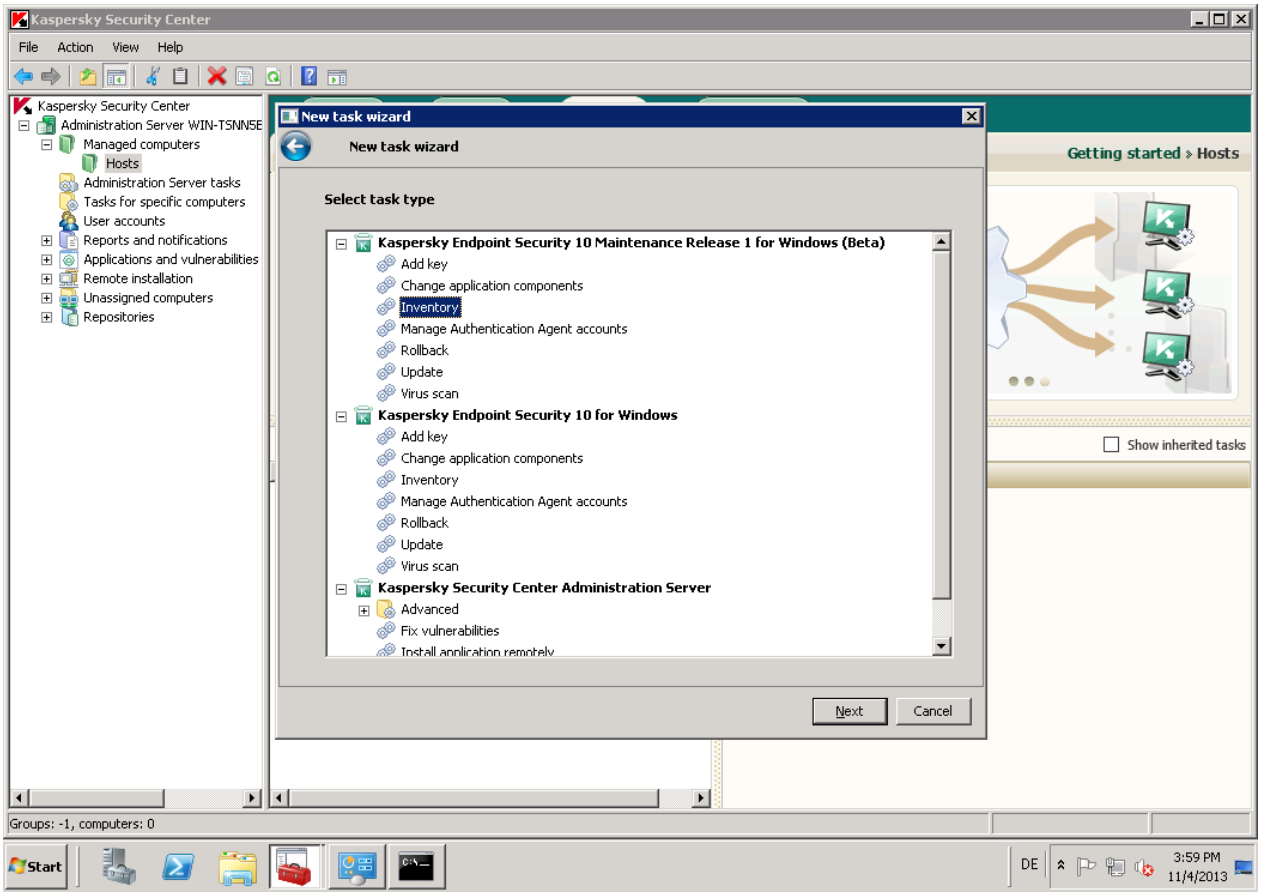


Figure 8: Creating a new inventory task in Kaspersky only takes a few steps

McAfee

For McAfee's ePolicy Orchestrator the task to create the inventory has to be generated and then run on the hosts. Bit by bit the information are uploaded to the inventory and can there be reviewed. The information are separated into Applications and Other Binaries and include the sub-groups Good, Bad and Unclassified. This classification is made through McAfee's own GTI technology. The user can also decide to pull the inventory manually from the hosts or even create it when rolling out the Application Control. When creating the inventory from the client systems the performance is slightly affected. All added files from the original inventory are allowed by default, there is no distinction even for those files McAfee places at a low trust level.

To change the execution behavior of an application the binaries need to be added to a rule. For many application McAfee provides a predefined list which includes over 100 rules. A problem arises with files not found in a predefined rules. McAfee can spread the binaries from one over several applications. When the user wants to treat all files from an applications, all binaries from these individual applications need to be separately added to the rules. One way to avoid this and allow applications is by using trusted publisher, which can be extracted from installer files, if they are including the publisher. By running a command line through a created task, interpreter like Python or Perl can be added to the control. This is

well documented in the manual and after adding the new rule, the according scripts can be added to the inventory.

McAfee ePolicy Test Mode is called Observe Mode. All applications which are not blocked by a policy are allowed to execute. When switching back to Enabled Mode newly created files can be whitelisted. This mode can be used on a designated administrator machine for testing of new blocking policies. Observations made during this mode can be reviewed and McAfee provides a suggestion on how to handle these newly added executables.

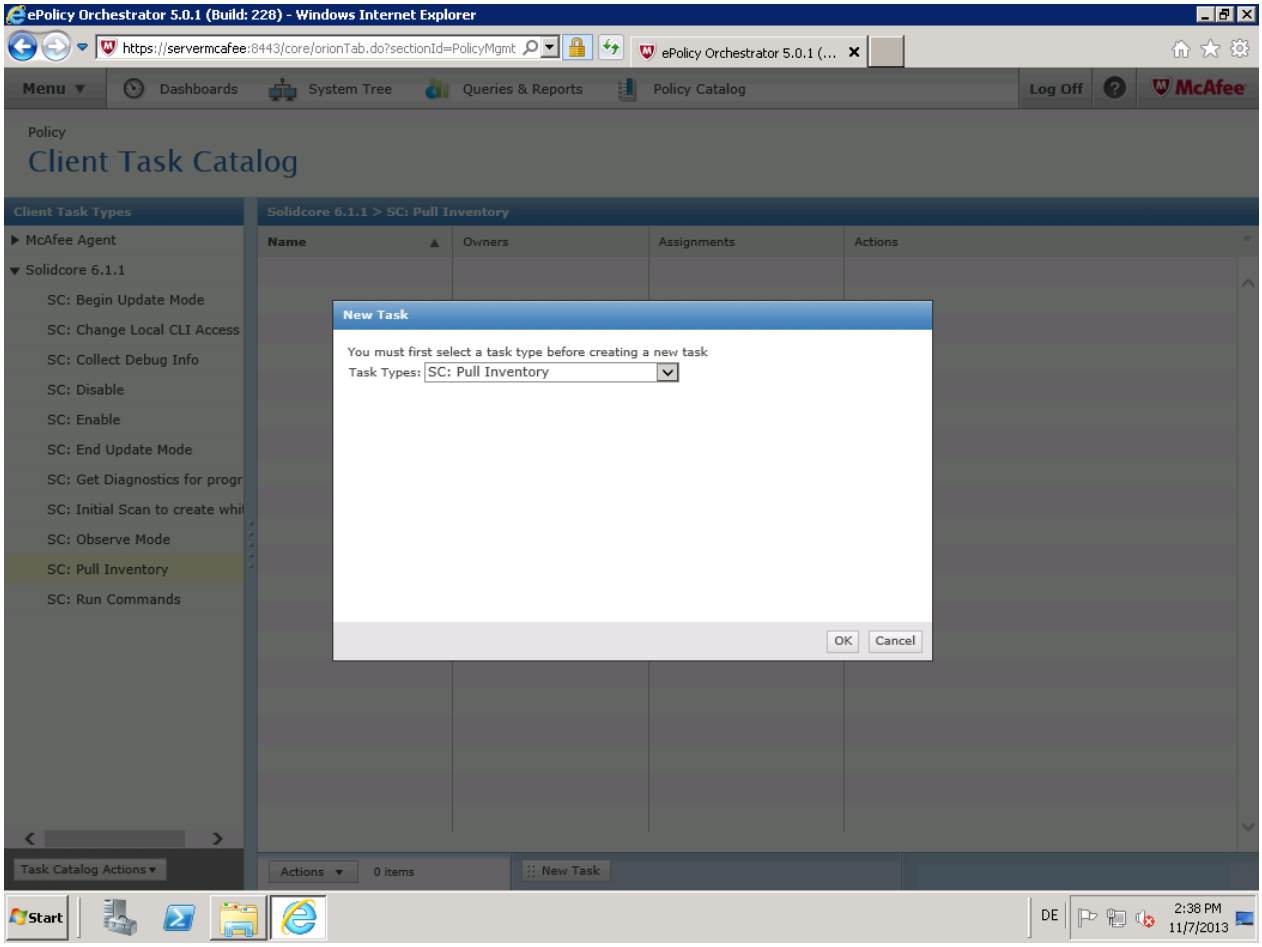


Figure 9: Pulling the inventory from the McAfee agents can be done through a task or with the deployment of the Application Control module

Symantec

Symantec's Endpoint Protection inventory has to be created using a command line instruction on the hosts. Even though the path to fingerprint can be chosen, by default it is likely to be the main drive at first execution. The hash value and path of the files are saved into a specified text file. The inventory files are manually added to the fingerprinting list on the server. Only files included in the fingerprinting list will be allowed to execute after activation of the "System Lockdown". The lists can be managed

separately or merged to be used universally as one. There are no additional options available. The default policies in SEP include 16 predefined example rules, which can be copied and changed according to the requirements. After specifying the files or paths in a rule, the action is set to either Allow or Block and the level at which to log the events is defined. When the rules are set, the policy is assigned to a group. The group can either contain client machines or users from the Domain Control. The policies for a group can be inherited to sub groups or switched off and individually assigned.

Script files can be managed like any binary file by adding the extensions to a rule and setting the action for the rule.

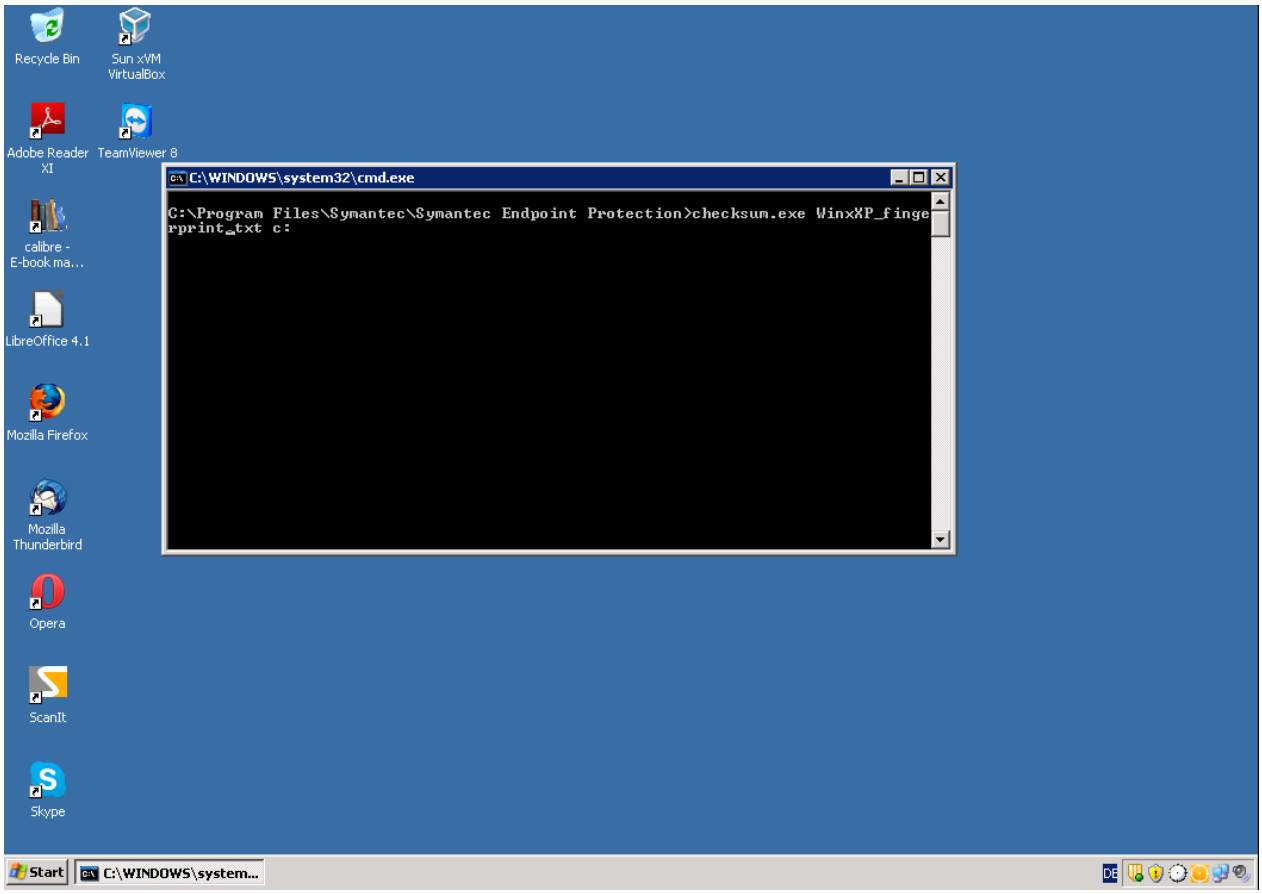


Figure 10: The fingerprinting file on the hosts need to be created manually through command line

Conclusion

Kaspersky creates an inventory, populates the categories and assigns them to policies with ease. Creating a complete policy set from start to finish is the easiest and the most straightforward of all tested products. It is possible to assign policies for users, specific to every machine. Also, the amount of information gathered on the systems hardware can be extremely useful to the administrator.

McAfee's created inventory is very impressive, not solely including executable files but scripts and additional files and providing the classification in Good, Bad and Unclassified; Cloud Trust Score and Enterprise Trust Level provided for most files. Viewing the inventory for all or just a single machine, adding new files automatically to the inventory or searching by different criteria is implemented very well. The way the rules are filled with binaries, updater, installer, trusted user and publisher is way ahead of the competition. The only issue remains the creation of tasks and the selection from the application list which is intricate.

Symantec allows easy adding and editing of rules. It is the only product that allows control of users and host machines and their assigning of rules equally. Compared to the competition, fewer options are implemented but Symantec is quicker and easier when it comes to setting up and configuration of rules and policies. The main issue is the need to perform additional manual work outside the general usage of the Administrator Console, such as: manually running a command on every machine of which a whitelist is required instead of having the client perform this task; and manually adding of created fingerprinting lists to the Administrator Console.

Monitoring

General

Administrator Consoles provide monitoring options through graphical interfaces, generating reports and critical event overviews for administrators themselves and general management. All of the tested products log events such as policy violations and provide a way of processing these events.

Kaspersky

Kaspersky enables the addition of a monitor for blocked applications to an existing or newly created dashboard. Newly added files can be viewed by sorting the inventory by Discovery date. The monitor displays all blocked applications on the chosen hosts; the time period of events can be selected in the configuration. When selecting a blocked application, more details are available such as according clients, run time and last access.

Groups of events can be created and filtered according to computer name, administration group, DNS domain, Windows domain or IP range. Any event on the selected computers will be displayed and allows, for example, the addition of applications directly to a category. Export of all or selected events into a CSV file is also possible.

A scheduled server task can be set up to run on report templates. Some templates are provided but they can also be created - for example for blocked applications or the applications registry history. Three formats can be used for the report: XML, HTML or PDF, which can be saved to a specific location and/or emailed. Upon successful completion, administrators can choose to send an email, SMS or run an application.

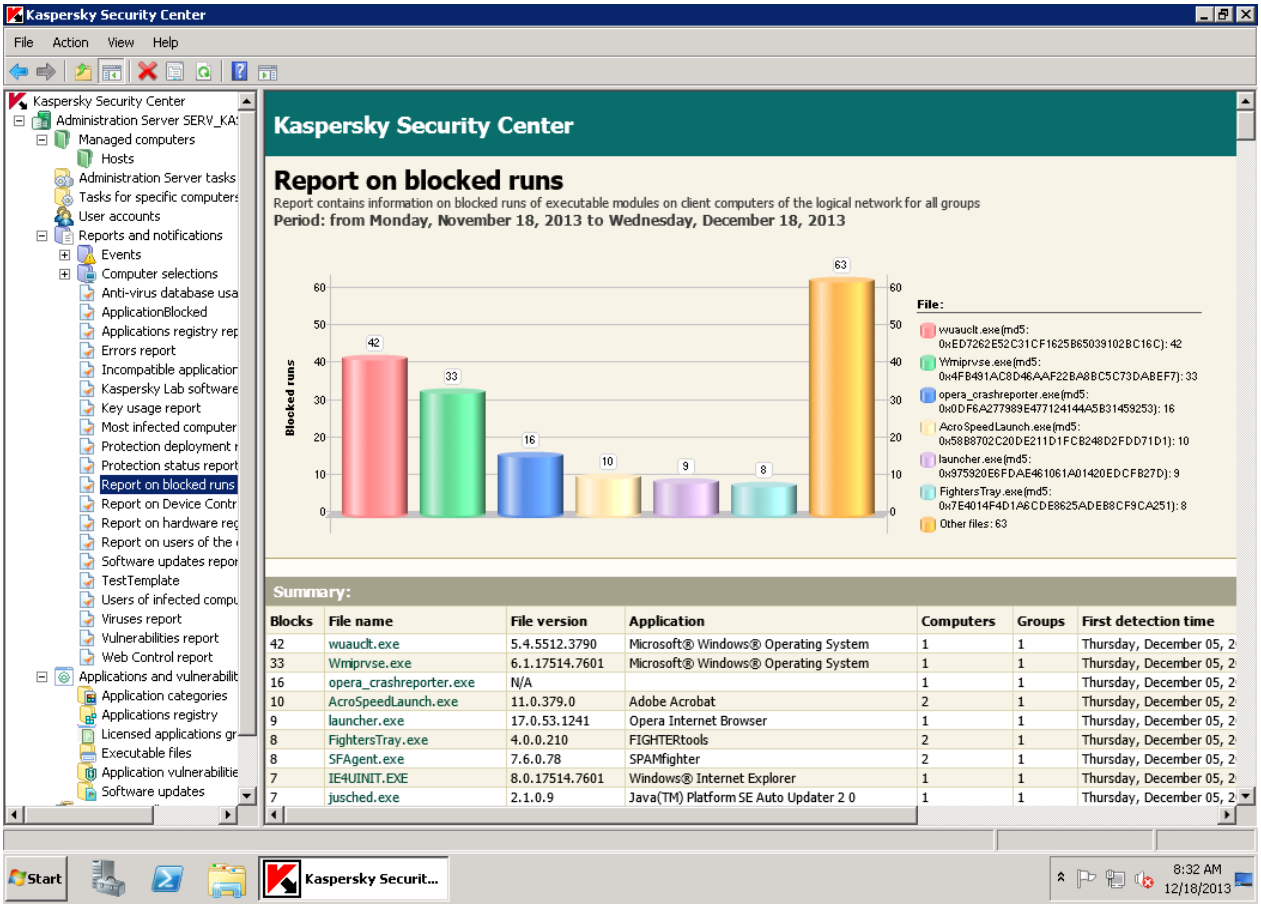


Figure 11: Kaspersky allows creation of templates to be used in scheduled reports

McAfee

McAfee provides seven different default dashboards specifically for the application control but more can be created and added. They provide information such as applications in the inventory based on enterprise trust level, predominant observations, top five bad applications or 10 main observations in the last 24 hours. The dashboards can be set to be public, private or shared in the network with a certain permission set. Selecting any entry on a graph will open the related menu such as the filtered inventory or the observation window.

Events such as the attempt to open an unknown application are logged as observations or in more detail in the event logs. Files automatically added to the inventory due to granted permissions are also displayed in the event view. A pending classification for approval or blockage of an application can be changed just like adding a file to a category directly from the log. A combination of different filters can be applied to the observations to view specified results. Those results can be exported in four different file formats and packed or emailed to a recipient. Events can be browsed and filters applied, for this task 43 different filters are available allowing for a high level of customization. The option to send notification by email in case of certain events can be achieved using a created task.

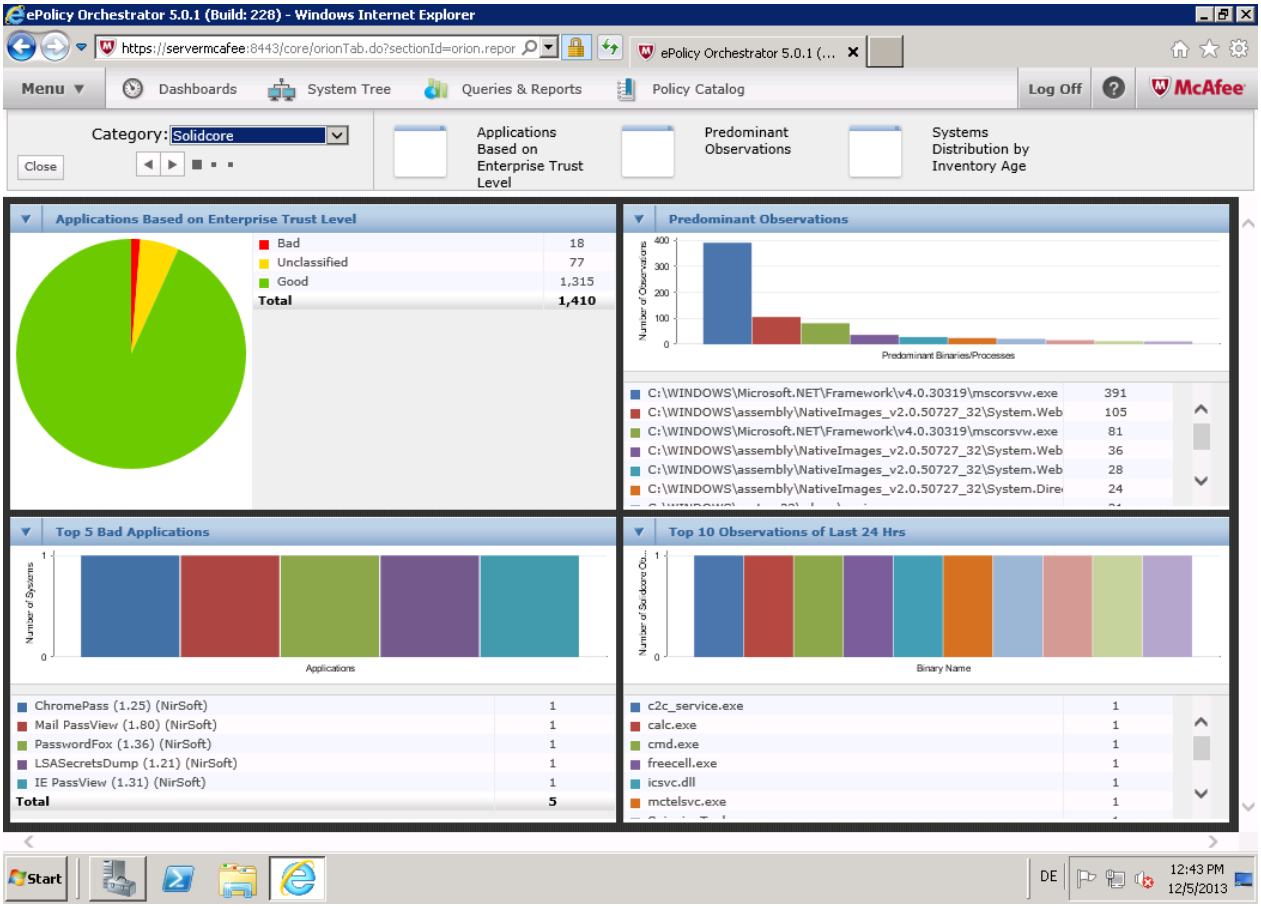


Figure 12: McAfee provides a variety of great graphical overviews which can be shared in the network

Symantec

For the application control, Symantec offers the option to use filters to create reports similar to dashboards. The administrator can either use the simple filters to get a quick overview or the advanced filters which range from severity of the event to caller process, providing an overall of 18 options. The created report can also be printed or pulled as a MHT file from the client and saved on the server. The option to schedule the creation of the report is also available. The scheduled report can be saved or even emailed to one or several recipients.

To view the events on the host a monitor is provided with the same filter options as provided for the reports. The displayed events can be exported as a CSV file, pulled directly from the host computer. In the created log, the details to an event can be reviewed in more detail.

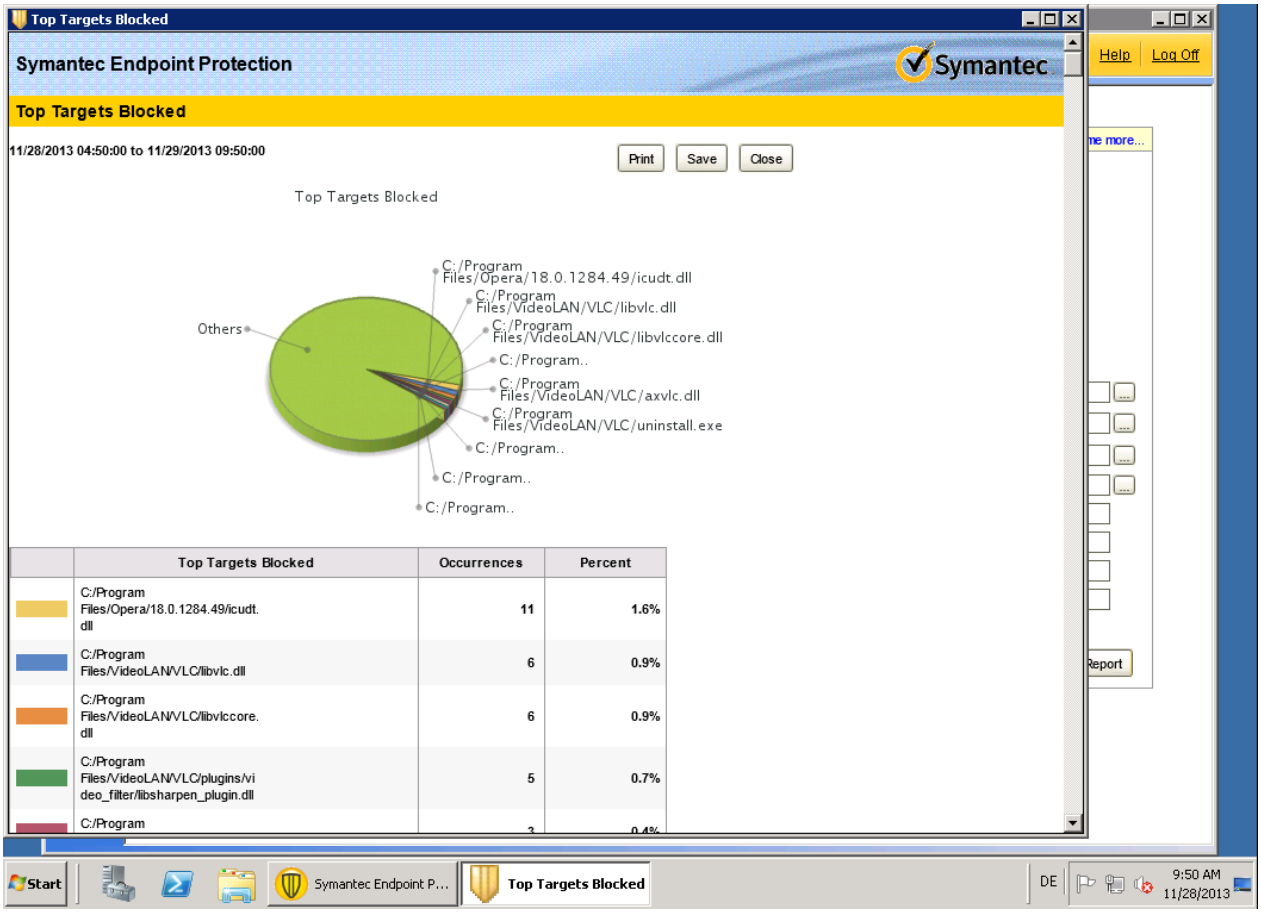


Figure 13: Creating a new inventory task in Kaspersky only takes few steps

Conclusion

All products provide the option to display the actions on the systems using graphs. They show the status of the current system in relation to the application control. Monitoring of events and filtering of such allows the administrator to detect events which require intervention. The options provided by McAfee leaves hardly anything to be desired, is highly advanced and provides options for notifications. Symantec's emailed schedule report can make life easier for regular reports to be provided to the management. And Kasperskys' option to create a specified event view for defined machines allows quick and individual support when end user issues arise.

Response: Application of policies and rules

When it comes to policy enforcement, all products hold up their end. In our test none of the products hindered the operating systems from working properly or influenced performance significantly. Only policy-designated applications were blocked, such as: any new unknown application; any known but unwanted application; any application running through an exploit (e.g. from a browser); and specified types of scripts. Symantec and McAfee by default block any file not included in its original inventory.

Kaspersky allows new applications if they are in a predefined Kaspersky category and added to an allowed policy. This has the advantage of eliminating the need to add all additional applications to the system manually, but also means they have to be classified by Kaspersky.

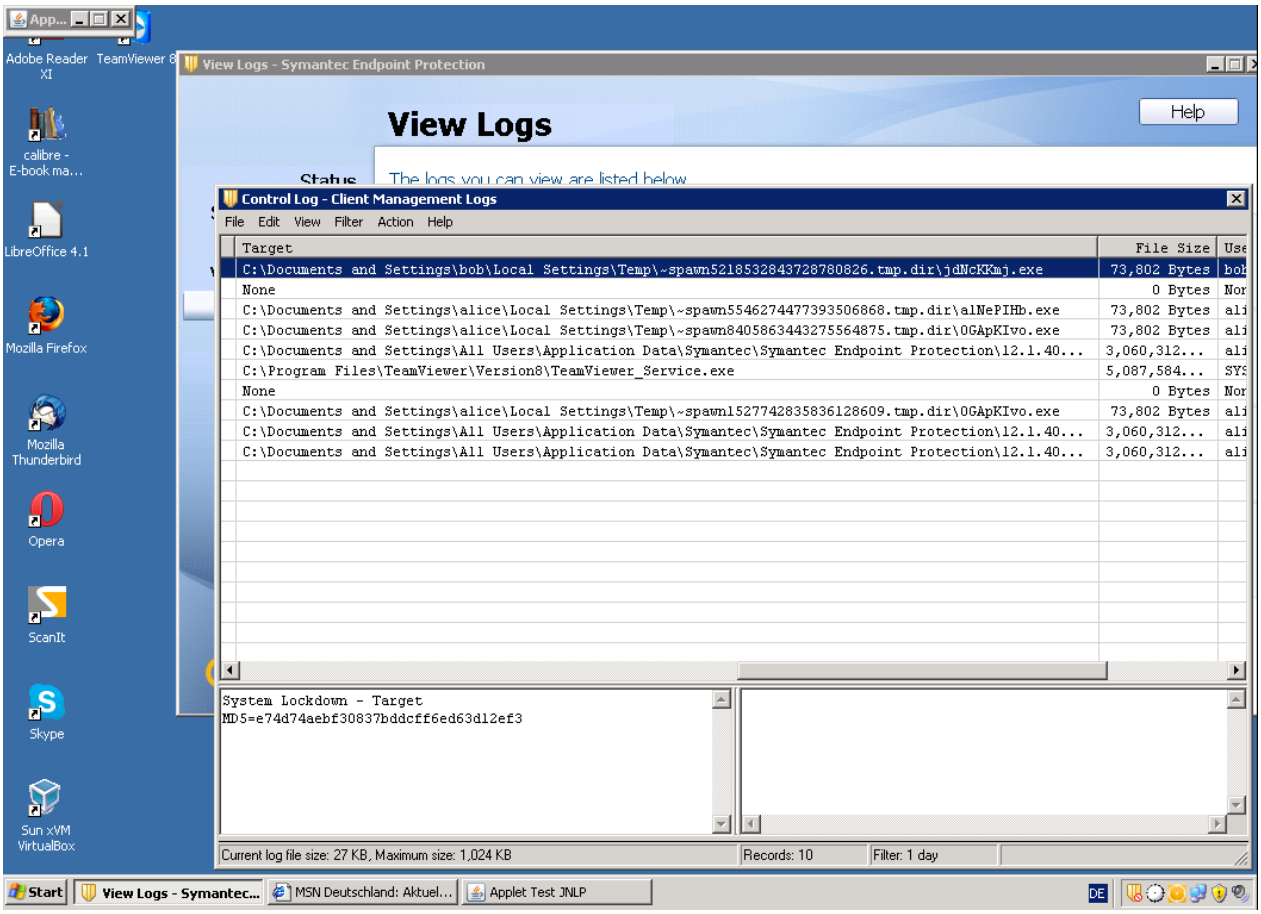


Figure 14: Symantec shows blocked application created and executed by an exploit

Blocked applications are communicated to the Administrator Consoles and logged. Kaspersky does this very quickly; McAfee's default communication period is 60 minutes, but this can be lowered by the administrator. McAfee and Kaspersky allow the addition of blocked applications straight from the logs to a rule giving them install, update or plain execute privileges. McAfee also offers the Cloud Trust Score and Enterprise Trust Level in the logs providing support for the decision making process.

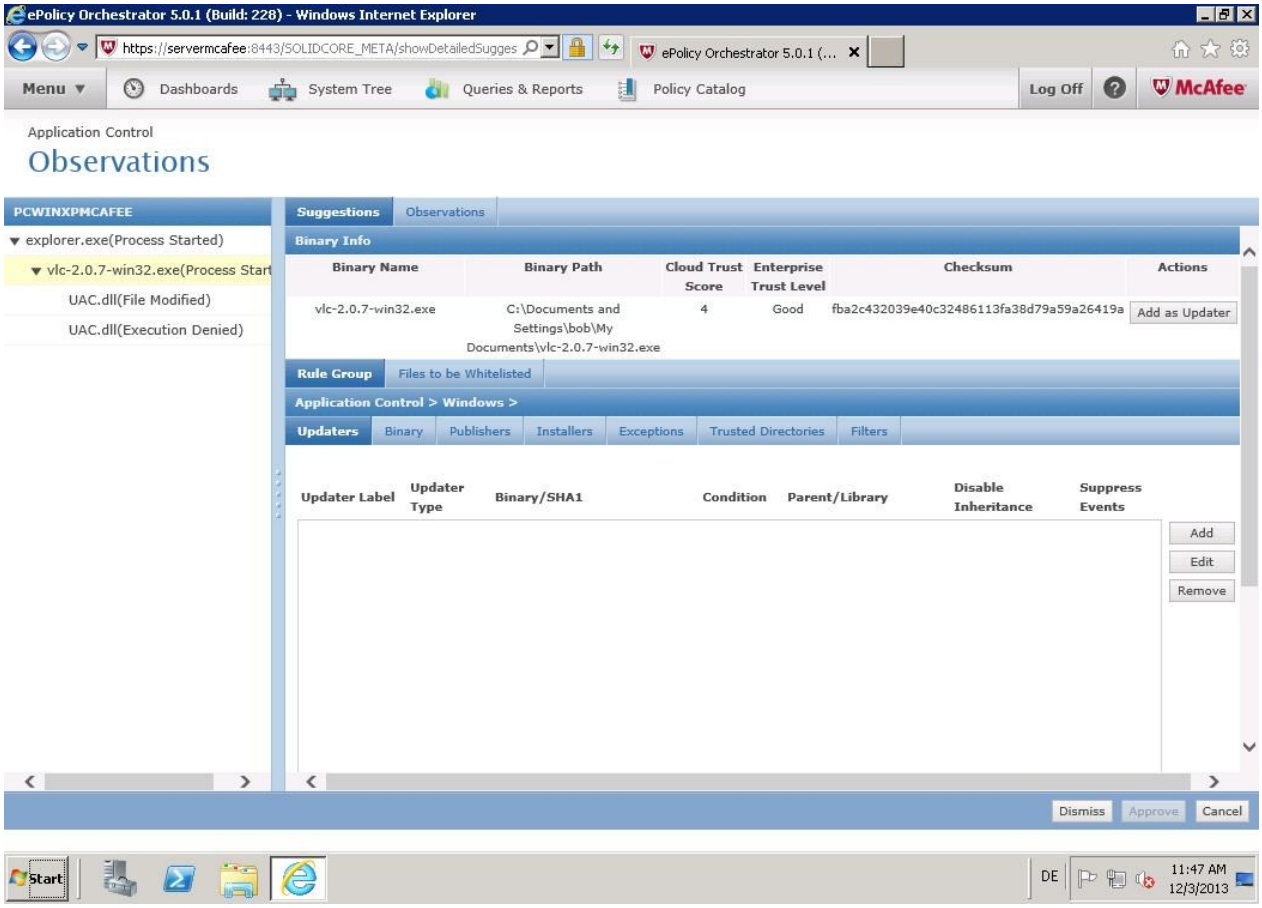


Figure 15: McAfee offers the option to allow a previously blocked application in the administrator console

Worth mentioning here is the Application Privilege Control included by default in KSC. This highly customizable HIPS, can be used by the administrator to, for example, block creation of new processes from interpreter, providing the option to manually improve the security.

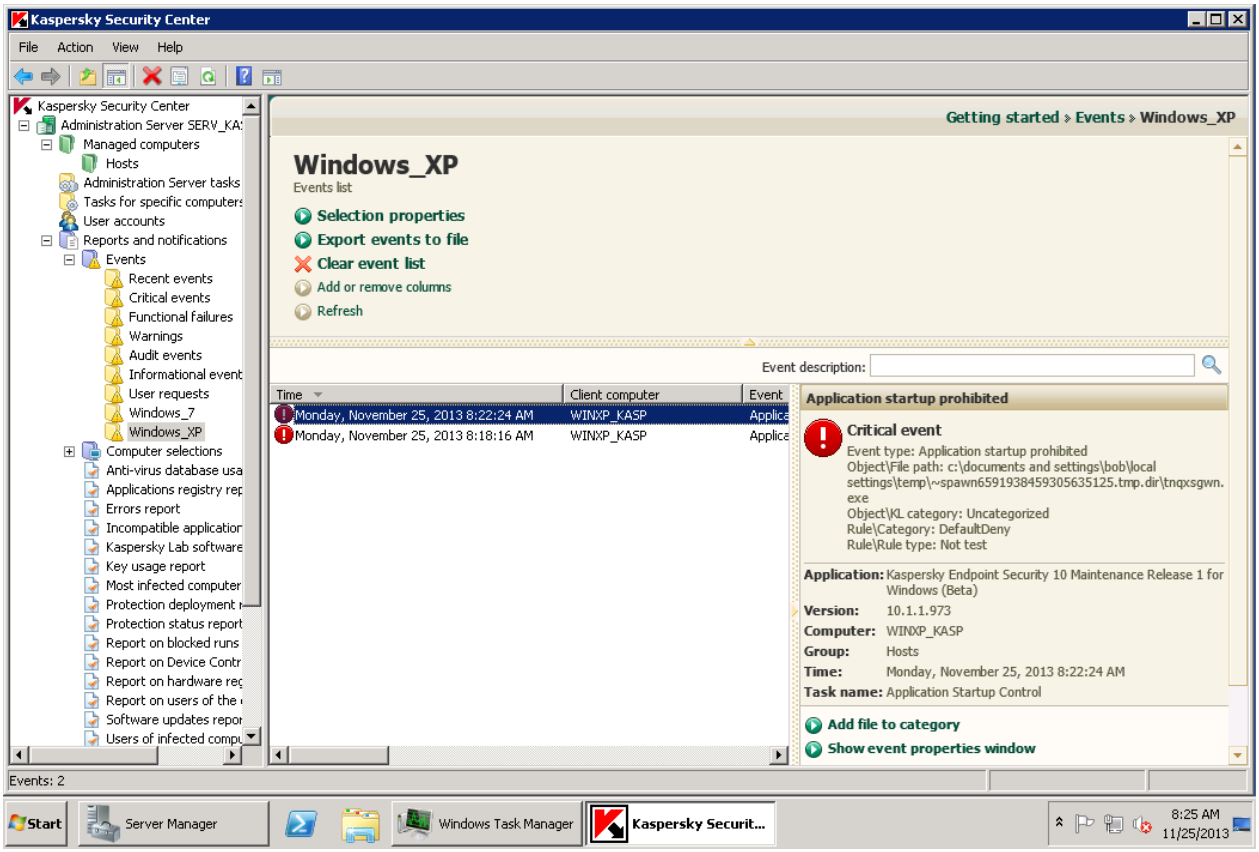


Figure 16: Kaspersky displays the blocked files and offers options for the application such as adding it to a category

Support: Installation and Updates

General

Effective application control solutions support the option of allowing updates and new software installations. Generally, only installations and updates approved by administrators are allowed, but most products provide functionality that, when enabled, allows end users to decide for themselves. This capability is handled very differently across the products tested.

Kaspersky

Any application included in Kaspersky's pre-defined 'Trusted Updater' category can be added to policies, enabling client updates to take place seamlessly and without intervention.

Under a classic Default Deny approach, where a complete list of 'trust by default' files is in place, the installation and update of new applications is possible; a new inventory list is created and extended to reflect the changes every time a new application is launched.

In cases where end users require legitimate access to an unknown or deliberately blocked application, Kaspersky's solution has user feedback and support functionality; new software requests can be granted or blocked at the click of an administrator button. Even in Default Deny mode, flexibility is ensured through an easy complaints/request management feature that allows users to contact administrators directly. These messages can be predefined by the administrator and files added directly from the event log in the administrator console.

A further option for updates and installation is available in Kaspersky: dynamic categories. This enables administrators to specify a folder for installer or update files - these are processed by Kaspersky, unpacked and added to the desired category. This feature allows new installations or updates that were not previously included in internal Kaspersky categories.

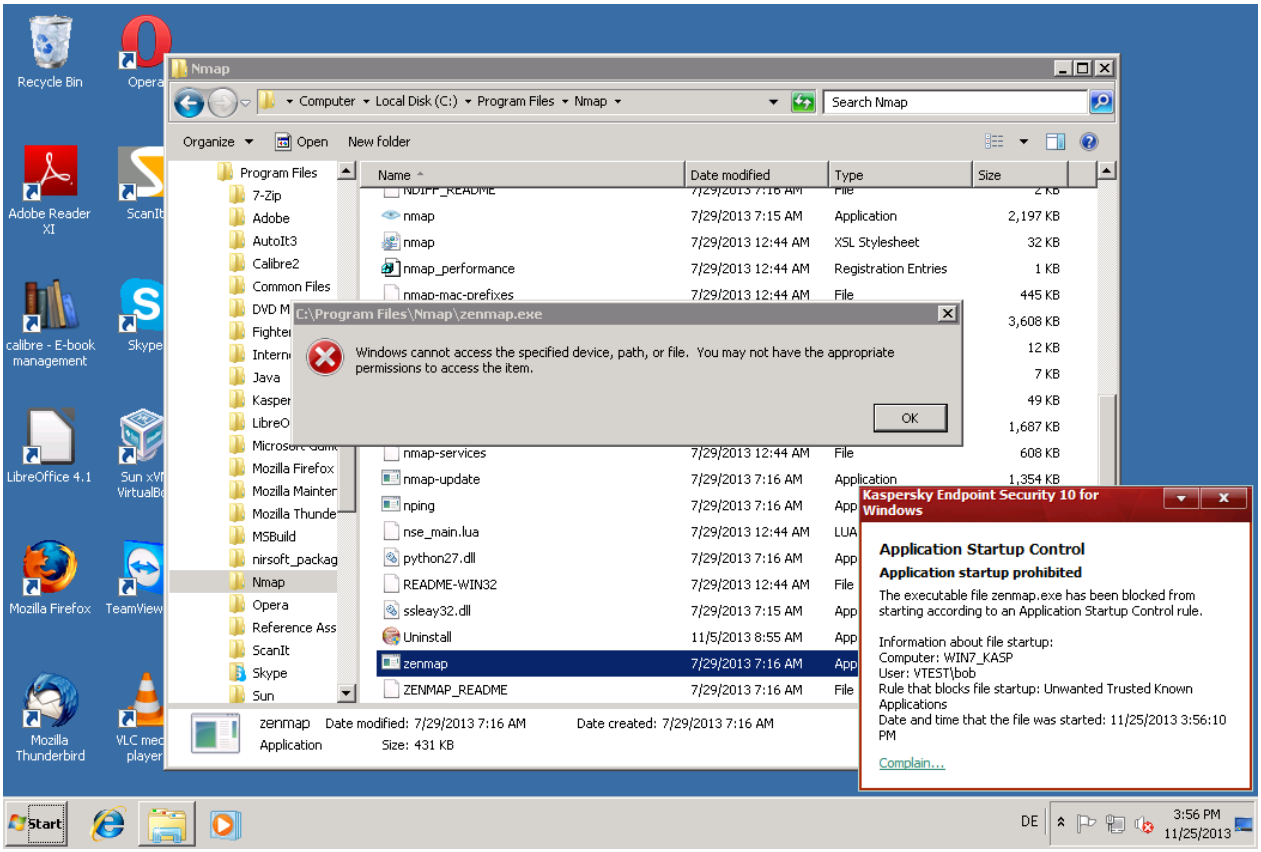


Figure 17: Kaspersky blocks an application which might be unwanted in a corporate environment and offers the option to "Complain…"

McAfee

McAfee provides a variety of options to update or install new applications, such as different usage modes, self-approval, trusted user, and trusted publisher or trusted applications, regardless of the trust level of an application. The administrator can decide on a method and then preconfigure the options so the applications can be installed on the machines. If the installation or update has not been previously allowed by the administrator, the Administrator Console will show the event of a blocked application and offer to add the publisher or binary to a rule which can be allowed.

McAfee offers the option to "Request approval" if an application was denied execution. Using an email the user can specify further reasons for the request. The agent needs to be available in the tray icon list, in order to be able to use this option. The administrator can view the requests by checking the emails or in the Observations menu. The event provides all details required to make an intelligent security related decision on approval or denial of the request such as the Cloud Trust Score, Enterprise Trust Level and Certificate details.

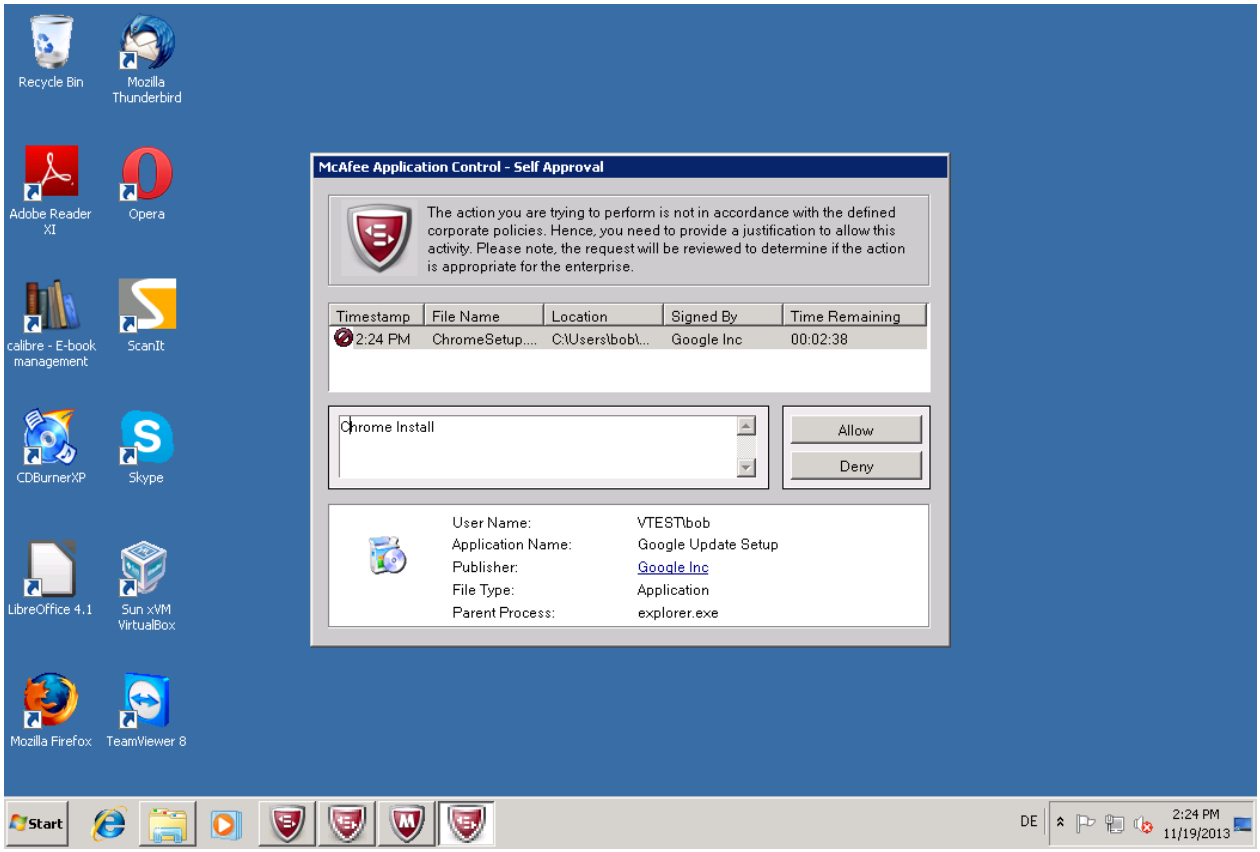


Figure 18: McAfee's self-approval option will allow the user to decide for himself and send the event to the administrator

Symantec

Symantec requires the user to change to "Test" mode, install the application followed by the creation of a new fingerprinting file and adding it to the rules on the server in the Administrator Console. This will guarantee an execution of the newly installed files, but all files required during installation need to remain on the system when the fingerprinting is done, otherwise the installation during the active protection will fail on other systems in the network.

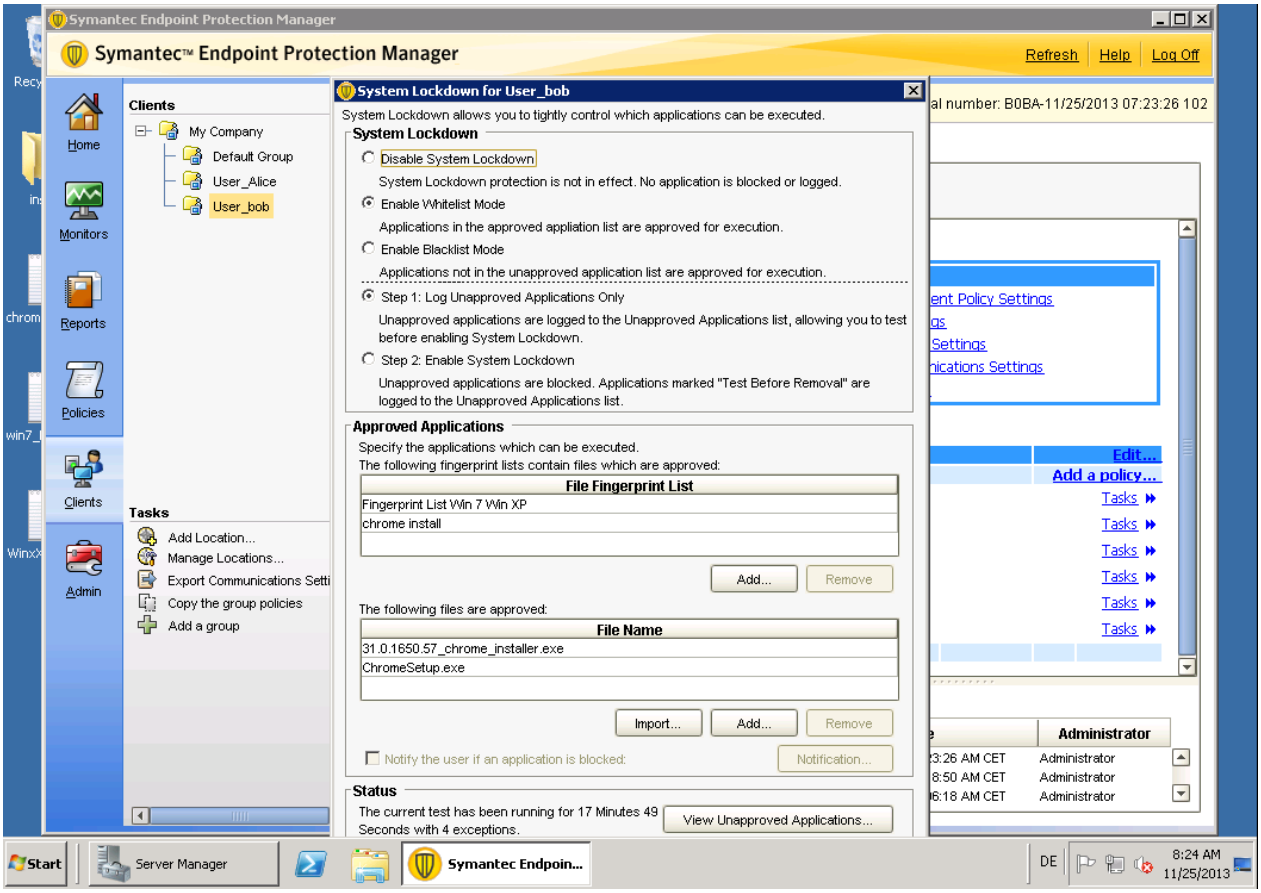


Figure 19: Symantec Endpoint Protection allows change to the test mode which allows installation and update so a new fingerprinting file can be created

Conclusion

McAfee and Kaspersky both offer options for updating and installing new applications. Kaspersky's individual comments on approval' request are a great way for the user to explain their requests for permissions. Users can also employ the predefined categories from Kaspersky if available to use as a suggestion for allowing or denying execution of an application. McAfee is extremely flexible providing the most options for the administrator to handle installation, updates and incoming requests but it didn't provide the option to justify the request directly to the administrator in the event log. The GTI and process information provided, help greatly for decision making on the possible approval. Symantec doesn't include an option to notify the administrator, also in order to install or update applications, one has to go through the entire process of creating the fingerprinting files again.

None of the products allowed exploitation of execution privileges through inheritance.

Appendix

Appendix A

The ideal solution will:

1. **Deployment**

1.1 Deploy Application Control functionality to endpoints

- Automatically identifies all unprotected endpoints on the network (online or offline, deployment to IP range or list of computer)
- Allows to schedule (periodical) deployment task of agent
- Chose modules to be included in deployment
- Offer of different deployment options (push, mail, link, package)
- Deploys full-functional agent and modules that provide control over endpoints, once installed neither disturbs users activities nor reduces endpoint performance nor reboot
- Advanced options – Deployment Wizard, force install (even if already exist), select install path, create/pull inventory on setup, deployment only under certain conditions (such as OS version), deployed modules enabled/disabled, notification up on (scheduled) deployment, Network options (such as time shift deployment or proxies), handling of conflicts (such as previous installed security products), handling required reboot (prompts, postpone etc.)
- Finishing with a status overview of progress for deployment and inventory creation for all systems and all missing systems

2. Configuration

2.1 Gather information on corporate environment

- Automatically identifies all installed applications, files and their properties (path, filename, hashes, file version information, vendor, signatures, etc.)
- Provides comprehensive information about endpoint systems
- Provides additional vendor's expert knowledge (files and registry entries according to products, categories, trust level, globe statistics, advises, etc.)
- Neither disturbs users' activities nor reduces endpoint performance, option for task priority.
- Advanced options – Select path to add to inventory, scan skip options (file size, max scan time), scan installation packages, Schedule scanning, add more than binaries such as scripts and selectable extensions.

2.2 Setup Application Control policies

- Apply gathered information (installer, publisher, trust level, path, filename, hashes, file version information, signatures, etc.)
- Apply vendor's expert knowledge (categories, trust level, globe statistics, advises, etc.)
- Provide predefined policies/rules (out-of-the-box)
- Allows exceptions

- Allows to customize policies for single user, groups of users and machines
- Allow updater/installer categories which add updated/installed files to category/whitelist
- Provide a well arranged overview of the inventory allowing the administrator a good perspective (e.g. grouping by different properties)
- Ease for group selection of files to be added to rules (such as advanced filter, adding all files from path, etc.)
- Advanced options – Logging level for events, notification options, copy existing policies, fill categories/rules from list or imports

2.3 Verify correctness of created policies

- Predict implication of policies statically by using gathered information
- Test created policies against possible collisions or false alarms
- Handling conflicts efficiently and include options for auto handling

3. Monitoring

3.1 Monitor and report on policies violations and threats

- Perform monitoring near real-time for critical events
- Monitor for policy violations, attempts to exploit vulnerabilities, suspicions application's behavior
- Allows for different notification options (dashboard, email, SMS, etc.)
- Sort events by critically level, originate from customer's or vendor's knowledge
- Allows for different exports options (excel, pdf, word, SQL, etc.)
- Allows to flexible analyze by filtering or grouping events by its' properties
- Collect extensive event information
- Neither disturb users activities nor reduce endpoint performance
- Advanced options – sharing monitor/report/dashboard with person in charge, further details/configuration options from the monitor, different display options

3.2 Monitor and report on changes in corporate environment

- Perform monitoring near real-time
- Monitor for new application installation, configurations changes, etc. relative to machine and/or user
- Allows for different notification options (dashboard, email, SMS, etc.) and scheduling of those.
- Allows for different exports options (excel, pdf, word, SQL, etc.)
- Collect extensive event information
- Allows to flexible analyze by filtering or grouping events by its' properties
- Monitor inventory composition by different attributes (Hips, categories, trust level, etc.) Neither disturb users activities nor reduce endpoint performance
- Advanced options – sharing monitor/report/dashboard with other users, further details/configuration options from the monitor, different display options, selection of data for different time periods, create and safe filter

4. Response

4.1 Remediate on infected network

- Blocks all hidden threat in a single click by applying out-of-the-box policies/rules
- Blocks all hidden threats near real time after policy was assigned
- Provide vendor's expert knowledge on prevented threats (trust level, categories, globe statistics, advises, etc.)
- Allows to investigate by downloading files and collecting additional information from infected endpoints
- Allows direct decision on category of file and advanced options such as updater or installer or delete from all systems in case of malware infection.
- Doesn't block end users' OS from operate normally

4.2 Prevent execution of unknown threats, attempts to exploit vulnerability, potentially harmful actions

- Prevents execution of unknown executable, libraries, scripts, memory injection, etc.
- Restricts harmful actions for known vulnerable application
- Provides vendor's expert knowledge on threats (trust level, globe statistics, advises, etc.) and what has to be done to resolve incident (what-to-do help)
- Allows to investigate by downloading files and collecting additional information from infected endpoint
- Allows to execute custom action on endpoint (e.g. launch tool or task) while investigation
- Not disrupt legal end users' activity

5. **Support**

5.1 Provide help to end user when blocks unknown application

- Allows to customize blocking response
- Provides advises and valuable information to user when blocks (e.g. alternative software etc.)
- Allows users to complaint
- Add complained files to rules with different privileges such as installer or updater not just as executable.
- Provides case-related information to administrator for further investigation
- Allows administrator to delegate complain handling to other user (e.g. manager)
- Allows to use case-related information by administrator to fix incorrect policy/rule
- Switch complain on and off

5.2 Allow software to be updated through self-updates

- Provide predefined policies for sources of trusted updates (repositories, trusted installers, trusted users, etc.)
- Customizable setup of trusted updates' source (local share, trusted user, appropriate updater, etc.)
- Allows system and legal applications to self-update or to be updated from trusted source
- Restricts capabilities for users to install legal but not allowed applications (e.g. using source of trusted updates)

- Prevents compromise of trusted updates' source or installation of unknown/malware software through compromised trusted updates' source
- Provide alternative methods for updating and installation depending on user/machine (self-approval, allow binary, allow vendor, system update mode)
- Not breaks end users' software from operate normally

Appendix B

List of installed applications

Application	Version
7-Zip	9.20
Active Perl	5.18.1.1800
Active Python	3.3.2.0
Adobe Air	3.9.0.1030
Adobe Reader	11.0.03
AutoIT Debugger	0.47.0
Calibre	1.8.0
CD BurnerXP	4.5.2.4291
Chrome	27.0.1453.93
Firefox	24.0
FreeCAD	0.13.1828
Java RE	1.7.0.10
Libre Office	4.1.2.3
Nirsoft Package	1.18.30
Nmap	6.40
Opera	16.0.1196.80
ScanIT	1.0.0.14
Skype	6.9.0.106
Spamfighter	7.6.78
SysInternalsSuits	30.10.2013
TeamViewer	8.0.22298
Thunderbird	24.1.0
VirtualBox	3.0.0-49315

Unknown trusted applications, copied to system

Application	Version
calc	WinXP (changed)
cmd	WinXP (changed)
freecell	WinXP (changed)
Hello world	autoit
Hello world	cmd

Hello world	perl
Hello world	python
Notepad	WinXP (changed)
SnippingTool	Win7 (changed)

Unknown untrusted applications (malware), copied to system

Application (SHA256)
0383872f300e48f6cda287f1bff146d666fc1e6fc8b4a063c1adbd42e1c7a59f
24fdcf83705bbb75ee39d1bef063ee3d8eadd5347c589f9a9ffc634cd94f2a8c
251bf0c4afba35f32a9037f07b712cc4e8f7ff2e34ba2dada7c2a960649ce58f
39d7ff03421a00bfe11a0e023dea0405e4862dc1be87da8d0769ac1694dd79de
56aa822495aad35b589082f3353eeef4ef220d077b0d0110d01e312c0fb193cb
5db70fbea2da6a744a5ac01de9b345059470cc930c71e9c21c0afaf33c4acb56
92bcb5a40e129cf0470f27bfef088006720ad8630c43a36ae66f774dc4357e58
a9a999e28bf030f405864c69b22fd2cbe6ed8b0768bb916f7eef0fd212dfa6ae
caa0b7b7bbcc7dc9bc757006375de9df35563bd707e953386846a73c1782449a
e8ccae872725d042127dc14e3831aa1f70e7b2242e2cbd19b6c18e56100b6988

Unknown untrusted applications with revoked signatures (malware), copied to system

Application (SHA256)
0a76bccb0729bfb5c12d857c714160b4c8d71625161d406e44ed01559123101d
3d439e8b34a28bee87c280e6b82002d7eec5471ec4fbbab61ccf7913933cdc82
4f4c5da5b80c7319087cb983d7edda94e87eccaad73da8a00392a5321761dd3b
57b295283bfb2192670005a7190f4b20ea1abd44d9a0c578bb3af831fadf764c
730b5b51997ba2f37227e08dfb6b6eb3f746a85c25f857afac1e01567ad8aebe
765008b5ddd88abb16791e5f328d5325cc9ca92ce91fd1ff317ace48d24fe9ea
8e9a753e1a5deb3a4cb1b0bad8b074d103739090baabe408018b623fd80b9473
9fc3754fe6e5cf7ba1b0b64272f0a45a13a34a281bbed9f27a5ade531d006ddc
a100cd3c7080db828766deba728c774a6f5a28f2ff50d9bb0091e940d125f705
a737ad257128c99023b10c63f4872e288ee875abe7f5ae9c89c8e790d7a048e7
bc0b9843a2f6569f4662a11b4239ffc16f15b1193adf16f71634f22434bdf4b6
bf353cb77c6075410bc3d8270a6aa1c448b0cfdcb07daaeb736beae90f3c8240
c9ca820ed5bbb481c679cae8bc60ca41654e44831e109f8b3bba0d4570e183b2
f3bca02fdf06e62e2800d6d82597ebf28b7f5dae9efe71eebc97b5f5c4d90527

Appendix C

Scoring

	Kaspersky				McAfee				Symantec			
	Effort	Value	Impact	E*	Effort	Value	Impact	E*	Effort	Value	Impact	E*
1 Deployment												
1.1 Deploy Application Control functionality to endpoints	2,5	7,5	2,5	0,38	4,5	9,0	4,0	0,28	2,0	6,0	4,0	0,16
2. Configuration												
2.1 Gather information on corporate environment	2,0	8,0	0,0	0,64	2,5	7,5	4,0	0,26	4,5	4,0	3,5	0,03
2.2 Setup configuration control policies	2,5	9,0	0,0	0,68	2,5	8,0	0,0	0,60	1,5	5,5	0,0	0,47
2.3 Verify correctness of created policies	1,0	7,5	0,0	0,68	2,5	7,5	0,0	0,56	1,0	7,0	0,0	0,63
3. Monitoring												
3.1 Monitor and report on policies violations and threats	1,5	7,5	0,0	0,64	2,0	9,5	0,0	0,76	1,0	7,5	1,0	0,59
3.2 Monitor and report on changes in corporate environment	1,5	7,0	0,0	0,60	1,0	8,5	0,0	0,77	1,0	6,0	1,0	0,45
4. Response												
4.1 Remidate on infected network	1,0	8,0	0,0	0,72	1,0	8,0	0,0	0,72	3,0	6,5	3,5	0,21
4.2 Prevent execution of unknown threats, attempts to exploit vulnerabilities, potentially harmful actions	0,0	8,0	0,0	0,80	0,0	8,0	0,0	0,80	0,0	6,5	0,0	0,65
5. Support												
5.1 Provide help to end user blocking unknown application	1,0	7,5	0,0	0,68	2,5	8,5	0,0	0,64	4,5	2,0	3,5	0,00
5.2 Allow software to be updated through self-updates	4,0	7,0	0,0	0,42	2,5	9,0	0,0	0,68	4,5	2,0	3,5	0,00
Overall Score				6,21				6,06				3,18

Where E is represent scores for 'Efficiency' of security product that was calculated by using the following formula:*

$$Efficiency = \begin{cases} \frac{(Value - Impact) * (10 - Effort)}{100}, & Value - Impact > 0 \\ 0, & Value - Impact \leq 0 \end{cases}, \quad Efforts > 0$$

Overall Score

The following overall scores represent how close a products' implementation is to the 'Ideal Solution':

- Kaspersky: 62,1%
- McAfee: 60,6%
- Symantec: 31,8%

Scoring Scale

Scores	Efforts	Value	Impact
9-10	**Manual operations labor**	**Excellent capabilities & implementation**	**Loss of data, Out-of-Protection, Incompatible**
8-7	* Most operations in administration interface has to be remembered according to technical manual	* Advanced Features	* Breaks business' processes flow * Compatibility issues
5-6	* Hard to intergrade into environment	* Satisfy most requirements * Few bugs	* Disturbs users activities * Under secured or Over secured
3-4	* The product is not as flexible/scalable as expected	* Too much Bugs & Issues	* Modest performance slowdown * Noisy Pop-ups and notification
2-1	* The product provides out-of-the-box solution	* The product has significant deficiencies in implementation	*Almost invisible from users' perspective *Few notifications
0	**No Efforts**	**No Capabilities**	**No Impact**

Value Table

Effort/Impact	Value	Evaluation
0-2	9-10	Excellent
2,5	8.5	Excellent/Very Good
3-4	7-8	Very Good
3.5	6.5	Very Good/Good
5-6	5-6	Good
6.5	3.5	Good/Fair
7-8	3-4	Fair
8.5	2,5	Fair/Poor
9-10	0-2	Poor

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org