Application Control Comparison

NOVEMBER 2012

Dennis Technology Labs
www.DennisTechnologyLabs.com

This comparative test looks closely at the features and abilities of security software that seeks to control which applications run on the network.

The products selected are, in the main, best known for their role in anti-malware defense. The test aims to explore how effective application control can be for locking down a network effectively while allowing users enough freedom to achieve the tasks necessary for the business.

The testing criteria used is based on Dennis Technology Labs' vision of the ideal application control system. The tested products are measured against the ideal criteria rather than directly against each other.

EXECUTIVE SUMMARY

- **Products tested**
  - Kaspersky Endpoint Security for Windows
  - McAfee Application Control
  - Sophos Endpoint Protection - Advanced
  - Symantec Endpoint Protection

- **Regular application control**
  Kaspersky Endpoint Security for Windows was the most fully-featured and functional solution for managing application control on a network. It was relatively easy to use and provided a high level of detail for administrators.

- **Auditing software and managing users**
  Not one product was outstanding when identifying all of the software on the network. Symantec Endpoint Protection was the strongest solution for managing users and their systems.

- **Advanced persistent threats**
  While no one product came close to providing an ideal level of protection, Kaspersky Endpoint Security for Windows was the most effective.

- **Is there one ideal approach to application control?**
  It is clear that the default deny (whitelist) policy approach is the strongest taken by the products tested, and that significant steps have been made by some vendors to mitigate the associated disadvantages to this potentially disruptive and highly restrictive method of managing systems.

Simon Edwards, Dennis Technology Labs, 30th November 2012

Contents

INTRODUCTION TO APPLICATION CONTROL

■ Why use application control?

Businesses face a number of threats to their operations, ranging from users wasting time to attackers stealing money, intellectual property and business opportunities.

Users may waste time using sub-optimal software, or applications that are more suited to leisure time than working productively.

If all users are allowed to run all software then, even with the best will in the world, they may install applications for which the business does not have a license. Clearly it is undesirable to allow pirated software to run on the network, but also some free utilities are not permitted for commercial use.

Perhaps more seriously, users who run vulnerable applications pose a security risk to the business. Doing so increases the chance of malware running on the network, which in turn may reduce the network's integrity and stability.

At the most sinister end of the threat scale, competitors and their agents may attempt industrial espionage by penetrating business networks and using malware to steal information or disrupt operations.

■ Why not use application control?

The greatest criticism leveled against application control is that it hampers users from achieving their business goals.

Problems may include irritating users by restricting their choice of software, which is disempowering. Aside from moral issues, restricting the available software may even prevent them from completing their work.

For example, if a user is working outside of regular work hours and needs to generate a PDF file urgently, but there is no appropriate software available, they may attempt to download and use a free PDF creation tool. If the application control system blocks its use, the user is unable to complete the work.

■ Types of application control

At the highest level, application control systems manage the relationship between users and the software that they may and may not run.

To achieve this the system needs to be able to identify the users, or groups of users, and has to be able to determine what software these users are trying to run.

There are two main approaches that application control systems take. These are generally known as blacklisting (default allow) and whitelisting (default deny).

Default allow (blacklisting)

Also known as blacklisting, a default allow policy takes an open approach. All software may run by default, except those applications that are entered into the blacklist.

One great benefit of a default allow policy is that users are unlikely to be blocked from using legitimate applications accidentally. This is because the administrator must actively block programs that should not run on the network.

Default deny (whitelisting)

Also known as whitelisting, a default deny policy takes a restrictive approach. No software may run by default, except those applications that are entered into the whitelist.

A default deny policy is far more likely to block legitimate applications than is a default allow policy. However, the trade-off is far more control over what can and cannot run on the network.

■ Targeted attacks

A targeted attack is an attempt by a business' competitor or other adversary to gain some level of unauthorized access to the network, usually with the aim of stealing information.

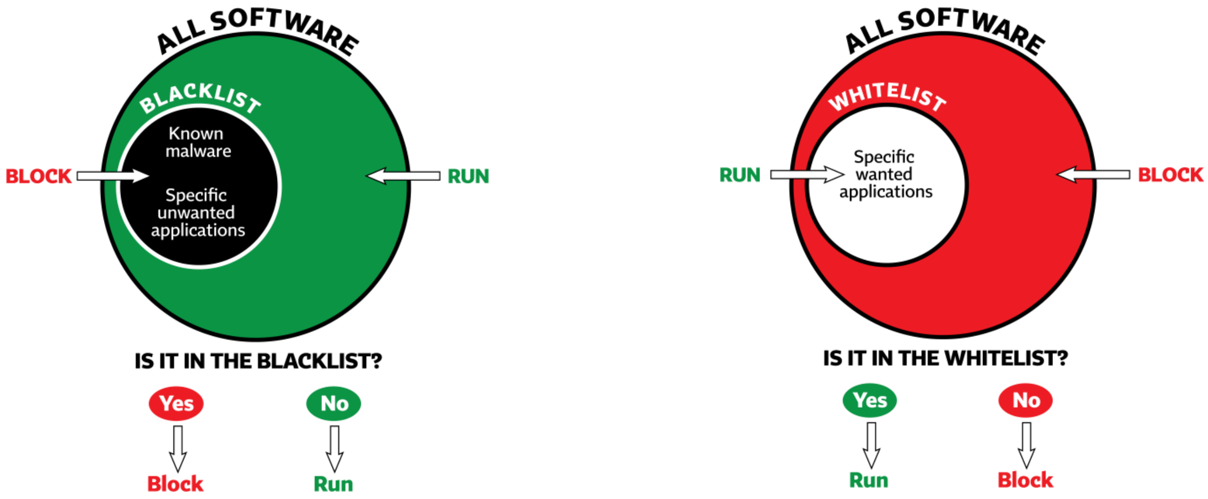
Such attacks are often called Advanced Persistent Threats (APTs)[1] or Targeted Persistent Attacks (TPAs)[2].

This type of threat is a particular challenge to security software vendors because it implies a

[1] Gartner http://blogs.gartner.com/john_pescatore/2010/11/11/defining-the-advanced-persistent-threat

[2] NSS Labs https://www.nsslabs.com/reports/analysis-brief-targeted-persistent-attack-tpa-misunderstood-security-threat-every-enterprise

THE DIFFERENCE BETWEEN BLACKLISTING AND WHITELISTING SOLUTIONS



A default allow policy permits everything to run, except software listed in a blacklist

A default deny policy prevents everything from running, except software listed in a whitelist

never-ending series of attacks against a small number of targets, such as employees in a single, specific business.

The challenge for anti-virus

Should such an attack use largely unpublicized exploits to gain and maintain unauthorized access to a network, traditional anti-virus protection faces a much harder challenge than it does when dealing with malware that spreads across the internet, touching large numbers of systems relatively indiscriminately.

Application control systems that block everything from running, save for known and trusted applications, are in a much stronger position to prevent a targeted attack from succeeding.

That is not to say that 'default deny'-based solutions are completely immune from APTs.

When this report refers to targeted attacks it means technically advanced attacks that are aimed at a particular business and that are capable of penetrating standard security layers and then remaining operational, but hidden, on the target.

WHAT PRODUCTS WERE (AND WERE NOT) TESTED?

The following products were tested:

Vendor	Product
Kaspersky Lab	Endpoint Security for Windows 8.1
McAfee	Application Control (Agent for Solidcore 4.6)
Sophos	Endpoint Protection – Advanced (Endpoint Security and Control 10.0)
Symantec	Endpoint Protection 12.1

Additionally we invited a number of other vendors to participate in the test. The following declined for various stated or unstated reasons.

Vendor	Product	Reason stated
Bit9	Parity Suite	Bit9 claimed that unspecified timing issues were a barrier to involvement in this test. Bit9 failed to respond to queries asking for more detail.
CoreTrace	CoreTrace Bouncer	CoreTrace refused to participate and declined to answer queries requesting a reason for the refusal.
Lumension	Endpoint Management and Security Suite	Lumension completely failed to respond to our request for its participation in the test.
Signacert	Enterprise Trust Server	Signacert declined to provide access to its software and services because, it claimed, it had been unavailable to the market for some time and faced significant changes before a re-launch. Additionally the company noted that the product requires a service engineer to install it. No employee was available because of the first claim above. We requested access in May 2012, a month after Signacert released version of 5.7 of its Enterprise Trust Server software suite on 10th April 2012.

Overall test results

A word on weighting

The following overall results are presented as percentages of the maximum possible score. The scores are weighted so that some parts of the test are more significant than others. For example, we considered that it most more important for products to be able to create groups of applications than to allow the administrator to delegate a user to handle blocked applications.

Businesses will have different priorities, so it is possible to adjust the weightings to generate scores that are more suited to your organization.

For those who want to dig down into the details, and even adjust the scores according to their own priorities, please see *Main Test Goals* on page 7.

Overall test results

	Deny all non-work-related, non-authorized and non-legitimate software	**Defend** against Advanced Persistent Threats (APTs)	**Total**
Kaspersky Endpoint Security for Windows	75%	67%	71%
Symantec Endpoint Protection	48%	32%	40%
McAfee Application Control	39%	28%	34%
Sophos Endpoint Protection	35%	25%	30%

Testing Application Control Solutions

It is important, when evaluating and comparing application control systems, to provide a clear, accurate and fair assessment.

How not to test

One flawed approach is to take a product, usually the one sold by the company that has paid for the test, and generate a table of its features against which the other products are compared.

This creates a biased set of results. The sponsor's product will almost inevitably beat or, at least, equal the competition. It is nearly impossible for a competing product to win such a test.

Comparing with the ideal solution

In this test we took a different approach. Instead of listing each feature from one or more of the products, we set out a list of challenges that the ideal solution should handle.

These challenges represent high-level requirements such as, "Do not affect adversely business processes and users' workflows" and "Provide in-depth logs and reporting".

As a result, all application control products can be assessed fairly, regardless of their approach.

The test may highlight general advantages and disadvantages to particular approaches, perhaps answering questions such as, "is default deny better than default allow?"

Business goals

This test is split into two main areas. We assessed each product according to its abilities in both of the following business goals, each of which is in turn split into separate groups of distinct tests:

1. Deny all non-work-related, non-authorized and non-legitimate software.

1.1 Identify all software in the network

1.2 Classify software as appropriate and inappropriate

1.3 Do not affect adversely business processes and users' workflows

1.4 Manage users (and machines) in distinct groups, applying different policies according to their requirements

1.5 Provide in-depth logs and reporting

2. Defend against advanced persistent threats.

2.1 Allow only legitimate software

2.2 Remove risks posed by using legitimate but vulnerable software

2.3 Do not affect adversely business processes and users' workflows

2.4 Block all pre-installed unknown or unwanted software

Main Test Goals

1. Identify software
2. Classify software
3. Allow business as usual
4. Manage users
5. Log and report

Each of the tests listed (left and above) comprise a number of detailed steps.

The details and scores for each of these are available in a separate document, *Dennis Technology Labs Application Control Comparison Test, Results*.

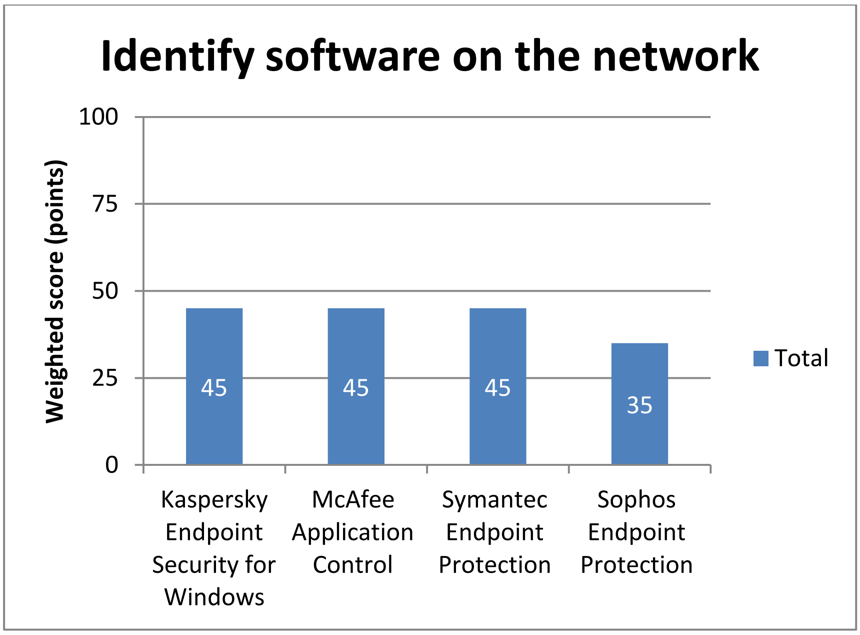
http://dennistechnologylabs.com/reports/s/app-control/kaspersky/DTL_2012_KL-AppCtl_scores.xlsx

TEST RESULTS

The test consist of a series of challenges, each containing detailed test cases. The graphs summarize the products' performance in each high-level challenge. Data is shown as point scores, not percentages. Maximum possible scores are reflected by the maximum y-axis value.

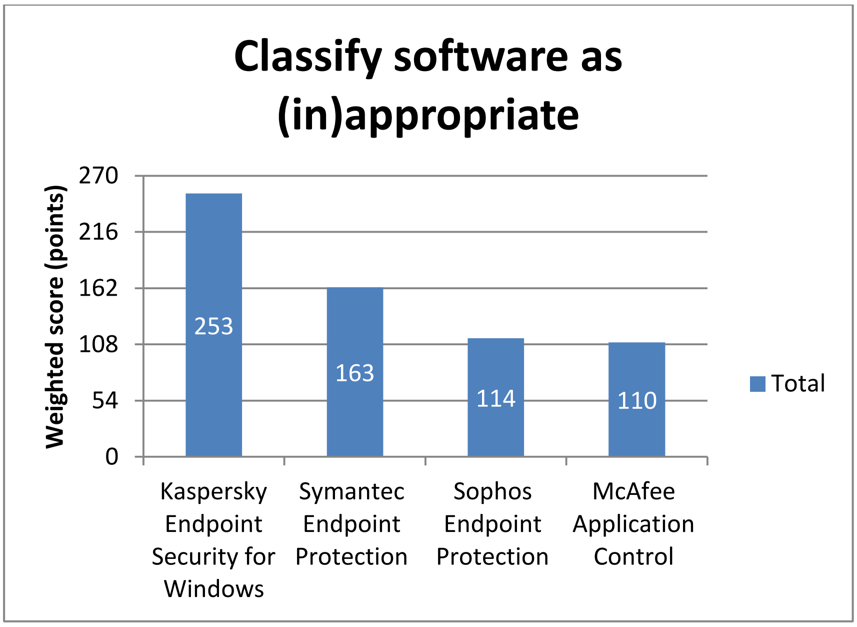
- **Test 1: Deny all non-work-related, non-authorized and non-legitimate software**

1.1 Identify all software in the network



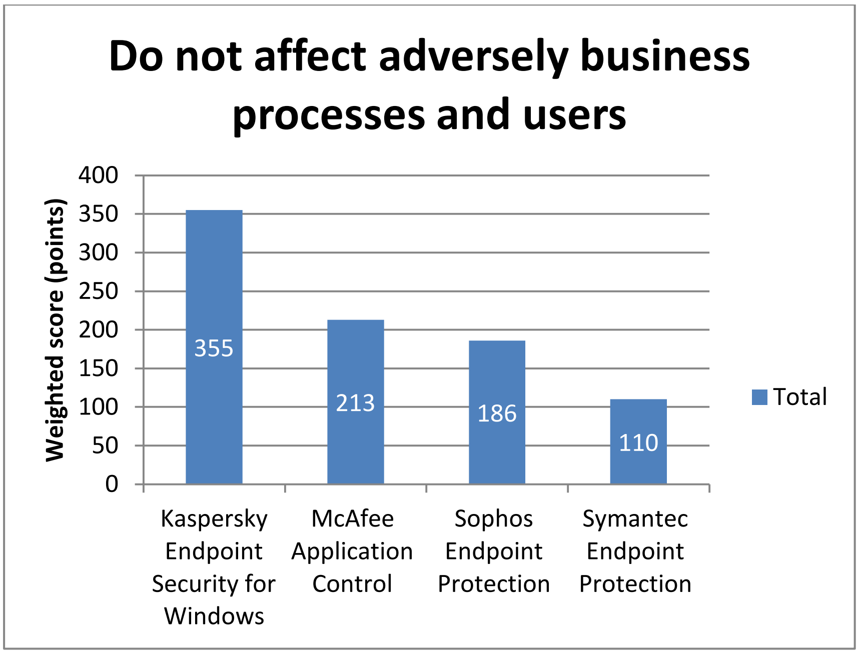
Products that performed best in this test were capable of building an inventory of software running on the network, and were then able to inform the administrators when new software ran.

1.2 Classify software as appropriate and inappropriate



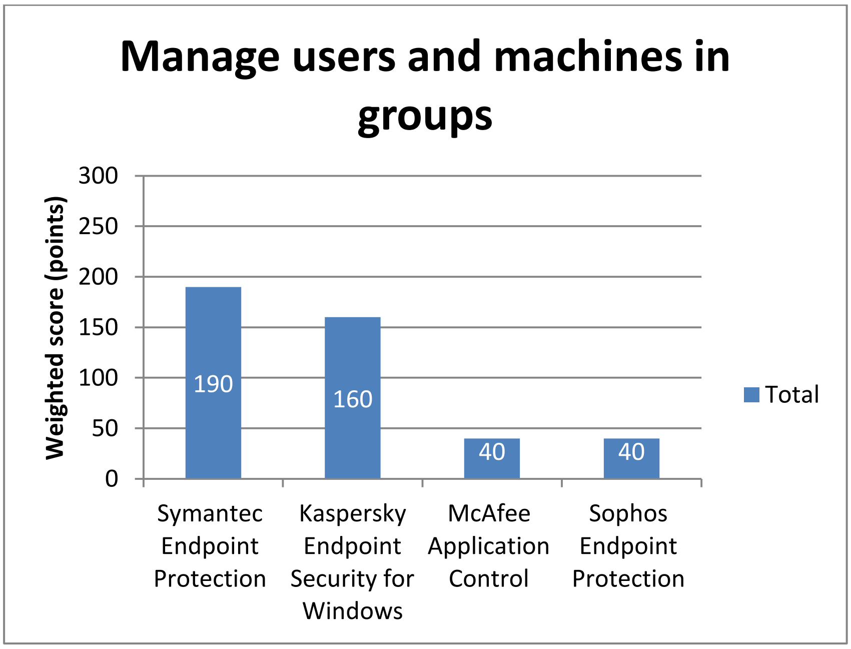
Products performed well when they provided lots of information about applications, the ability to create groups of applications and pre-defined application groups.

1.3 Do not affect adversely business processes and users' workflows



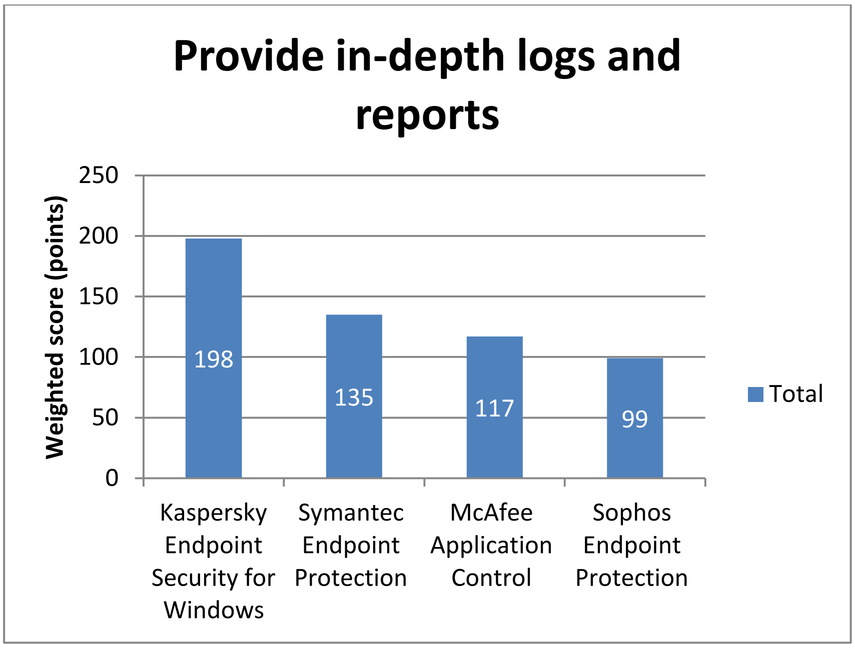
This test investigated the existence and implementation of a test (or observation) mode, as well as the chain of trust that exists between applications and their updaters. The ability for users to provide feedback was also important.

1.4 Manage users (and machines) in distinct groups, applying different policies according to their requirements



Products that provided powerful and flexible policy management, alongside the ability to group users and their machines, performed well in these test cases.

1.5 Provide in-depth logs and reporting

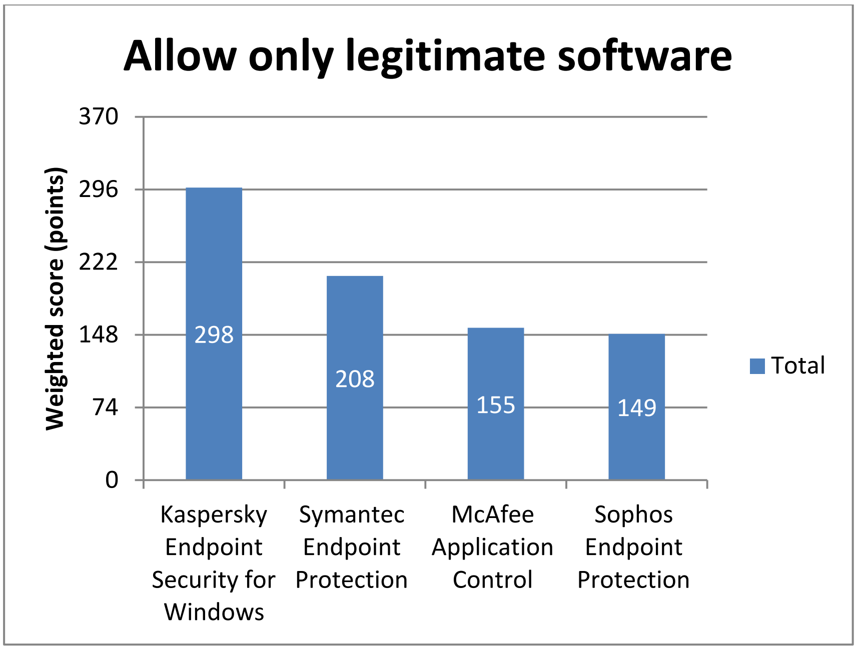


This test examined not only the logs that the products generated when users accessed applications but also logs relating to changes in the products' own configurations.

Test 2: Defend against Advanced Persistent Threats (APTs)

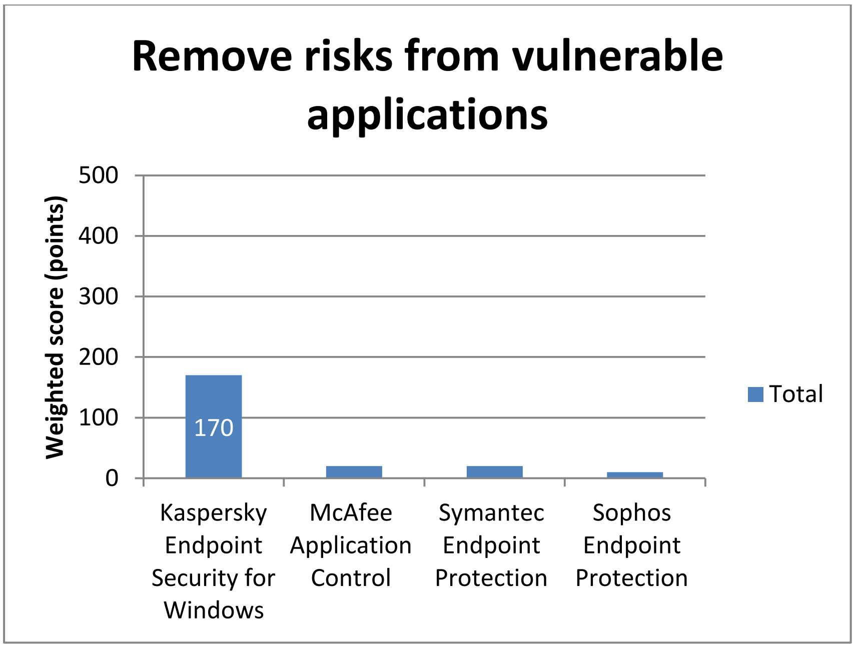
This set of tests includes some data from the previous set. In addition to this duplicate data we tested two areas that specifically address the issue of targeted attacks.

2.1 Allow only legitimate software



These results are a combination of tests 1.1 and 1.2.

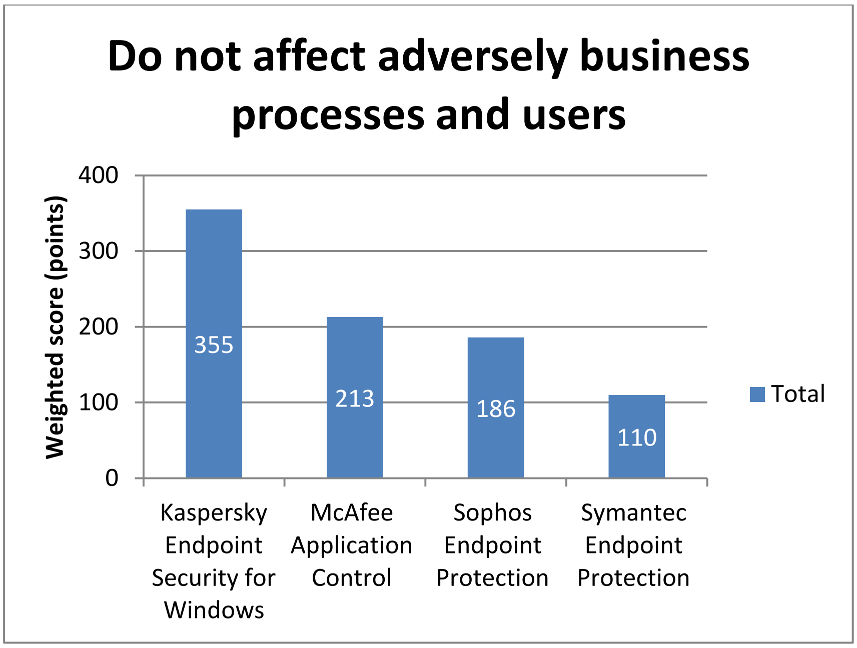
2.2 Remove risks posed by using legitimate but vulnerable software



This test examined the products' abilities to identify, manage and protection vulnerable applications. Most were unable to identify vulnerable applications, which severely hampered their attempts to further manage or protect them.

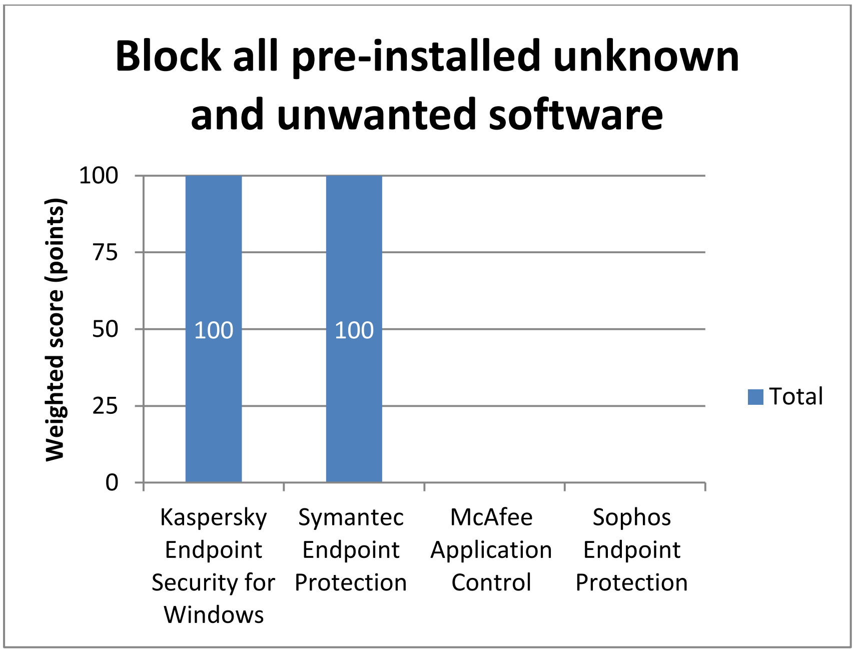
No product was able to identify or block the exploitation of the vulnerable applications. At best they prevented the result of the successful exploitation, which is helpful but not as ideal as blocking the exploitation itself.

2.3 Do not affect adversely business processes and users' workflows



These results reflect the outcomes in test 1.3.

2.4 Block all pre-installed unknown or unwanted software



The above results show that only Kaspersky and Symantec products were able to recognize and block an unauthorized application that was pre-installed on a system before the security software was installed.

Reviews

Kaspersky Endpoint Security for Windows

Product	Kaspersky Endpoint Security for Windows
Developer	Kaspersky Lab
Website	www.kaspersky.com
Endpoint	Kaspersky Endpoint Security for Windows 8.1.0.831
Management console	Kaspersky Security Center 9.2.69
Scores	
Control users' software	75%
APT defense	67%
Total	71%

1. Deny all non-work-related, non-authorized and non-legitimate software.

The product was able to produce an inventory of applications and it generated a report listing most, but not all, of them.

When monitoring the inventory, the administrator must list the executable files and order this list by the column called "Discovered", which shows the dates when new files were added to the inventory. This workaround is not ideal.

Once a file has been identified, the solution provides a vast amount of detail, including checksums and its location on the system.

Applications can be added into groups easily and there are well-populated pre-defined groups.

The solution has a test mode that allows administrators to see clearly which applications would be blocked should the system be switched to providing full protection. Additional tools to help analyse the logs would be welcome.

The products were expected to handle applications that update other applications. This involved testing with a combination of trusted, and mistrusted updaters, as well as permitted, blocked and unapproved (not formally blocked, but not allowed) applications. This is a subtle and potentially confusing test, which Kaspersky managed to pass with full points.

Application control software is suspected of causing users some inconvenience but Kaspersky's method of allowing feedback from users was exemplary.

However, it was less effective at providing users with useful information when they discover that their chosen software is blocked. If the customisable messages were more flexible users could be led to a specific and tailored solution rather than left with an error.

The software was good at allowing the creation of policies for individuals and groups of users. It also allowed the creation of groups of applications.

Unfortunately, administrators were unable to delegate the task of handling user requests for accessing software.

The Kaspersky product really stood above the crowd where logging was concerned. It was capable of providing in-depth logs and reports, although it failed to log unapproved applications. The detail provided was excellent, however.

As with all other products tested, work is required by the administrator who wants to roll back policy changes.

2. Defend against advanced persistent threats.

The APT test was challenging but Kaspersky did the best out of the products tested. The key to this result was its ability to recognise vulnerable applications.

Although, like the competition, it was not able to identify or prevent the actual act of exploitation, it was able to block known vulnerable applications until they were updated to a safe state.

The software also managed to remediate the pre-infected network, a performance that only Symantec was able to match.

McAfee Application Control

Product	McAfee Application Control
Developer	McAfee
Website	www.mcafee.com
Endpoint	McAfee Agent for Windows 4.6.0 – minor version 1694 McAfee Agent for Solidcore 4.6.0 – minor version 2918
Management console	McAfee ePolicy Orchestrator 4.6.0 – minor version 1444
Scores	
Control users' software	39%
APT defense	28%
Total	34%

1. Deny all non-work-related, non-authorized and non-legitimate software.

McAfee Application Control did a great job of compiling an inventory of software running on the network, although exporting that list is either impossible or requires very obscure knowledge of the necessary technique.

The list's accuracy was unsurpassed, although the system failed to provide useful "what if" information when in observation mode. This means that administrators would not be able to see the possible fallout from their policies before imposing them fully.

The information provided about installed applications was very detailed, including file locations, checksums and details of certificates.

Creating groups of applications is not possible, although administrators can create groups of rules, which leads to a fairly complex workaround to achieve this goal.

There were no pre-defined groups of applications so administrators face some work when trying to handle bundles of programs.

The system was more than capable of handling trusted updaters, which puts it above most of the competition. However, it failed to prevent security issues posed by compromised updaters.

Administrators can use the system to provide users with customised feedback when their attempts to run blocked applications fail.

Users are able to send requests to unblock software to administrators, although these alerts are only sent as email messages and do not appear in the management console.

While policies may be applied to computers and groups of computers, they cannot be set up for individuals and groups of users. This is a significant limitation, as is the lack of functionality for delegating the task of unblocking applications to specific non-administrators.

It is not possible to create policies defining groups of applications that can then be applied to groups of users.

The logging facilities are average, recording blocked events but ignoring access to permitted applications. There is a lack of detail in logging the system's own configuration changes and it is not possible to roll back policies, other than backing up and restoring policies manually.

2. Defend against advanced persistent threats.

The software does not recognise vulnerable applications and has a very limited ability when it comes to updating vulnerable applications, which stems from the fact that it can't recognise them in the first place.

As with all of the products tested here, McAfee's solution was unable to identify or prevent the exploitation of vulnerable software.

Unfortunately the solution also failed to remediate the pre-infected network. Installing the endpoint agent is possible but it allows the pre-existing software to launch when the system starts.

Sophos Endpoint Protection - Advanced

Product	Sophos Endpoint Protection – Advanced
Developer	Sophos
Website	www.sophos.com
Endpoint	Sophos Endpoint Security and Control 10.0
Management console	Sophos Enterprise Console 5.1.0.1839
Scores	
Control users' software	35%
APT defense	25%
Total	30%

1. Deny all non-work-related, non-authorized and non-legitimate software.

Sophos' solution takes a default allow approach, which means that it is less capable, by design, of building and maintaining an inventory. This is possible to achieve with some work in test mode, but the results are limited. If an application does not exist in the lists that are pre-defined by the vendor then it is not listed in the inventory.

Monitoring the inventory is an onerous, manual process that includes only software known to Sophos' database.

This database is well-populated, though, and scores top marks for being so. Sadly it is not possible to create custom groups of applications and only minimal information is provided for those applications that are included. For example, there are no details on checksums or certificates.

The test mode is excellent and allows administrators to see exactly which applications are running, and which would be blocked by an impending policy. Additional analysis tools would be useful.

The system can handle trusted updaters but only those in its database of known applications. One problem is that, with a few exceptions (namely Adobe Reader) it does not distinguish between versions of updater.

It is possible to compromise an application through its updater because it appears that the chain of trust that should run through the updater and into the updated application is not monitored.

There is no integrated way for users to provide feedback when they are blocked from using software, although this is less significant with this solution than with some others as it uses a default allow policy. For this reason we have allocated it some points even though it lacks this feature.

When software is blocked users may be alerted with a customisable message, although there is no feedback option, as mentioned above.

Possibly because the software was designed with the philosophy that the vendor should do most of the work, it is not possible for administrators to delegate the role of unblocking software to non-administrator users.

Neither is it possible to create groups of policies that can be applied to groups of users, although administrators may apply policies to groups of computers. No user-based policies are permitted, though.

Logging of application events is at an acceptable level, with a good range of alert types, although the system does not log the use of allowed applications.

There do not appear to be any logs created for changes to the system itself and reversing policy changes is, as with all the products tested, a case of restoring a backup policy manually.

2. Defend against advanced persistent threats.

The solution performed very poorly in this part of the test. In fact it takes almost all of its scores from the first section of tests (see above).

It failed to identify vulnerable applications, to identify attempts to exploit them and to prevent the exploitation.

The system was unable to limit the functionality of known vulnerable applications and it did not remediate the pre-infected network.

At the very least it allowed the updating of vulnerable applications and the launch of patched software.

■ Symantec Endpoint Protection

Product	Symantec Endpoint Protection
Developer	Symantec
Website	www.symantec.com
Endpoint	Symantec Endpoint Protection 12.1
Management console	Symantec Endpoint Protection Manager 12.1
Scores	
Control users' software	48%
APT defense	32%
Total	40%

1. Deny all non-work-related, non-authorized and non-legitimate software.

The product was unable to create a full inventory of the test network, generating instead a list of applications that had been executed on the endpoints. It also quarantined software that posed a potential threat.

The report on executed applications was functional but with few options to export the data in such a way that it could be used by another system for further analysis.

Symantec's inventory monitoring system surpassed those of the competition and generated email alerts when new applications were launched.

Although the solution provided no pre-defined groups of applications, it was the easiest to use for allowing administrators to create their own groups.

Additionally, the amount of data it provided for each application was exceptionally detailed, including checksums. It did not provide information on each file's digital signatures, though.

The product scored quite poorly in the test labelled "Do not affect adversely business processes and users" because it failed to manage trusted updaters at all, and was unable to defend against corruption introduced via a compromised updater.

Furthermore, there was no integrated way for users to request that an blocked application be released.

To its credit the system did provide a mechanism to display a customised message when an application is blocked.

When disgruntled users call the help desk to request a new application administrators may shift some of the workload by delegating a non-administrator to handle the query.

Such delegates may even change firewall rules. There is no clear way to give the delegate power to allow only a sub-set of applications.

It is possible to group applications into bundles, which may then be provided to groups of users. The user management system for this is awkward to use but is functional.

The logging system recorded events in which applications were blocked, but when the system was not in test mode no logs were produced for applications included in rules-based policies. Nevertheless, the product performed strongly in this area.

It performed less well when logging its own changes, providing little detail. It records that a change occurred, but not what the change was.

Reverting to old policies was, as with the other products, a case of restoring a backup policy manually.

2. Defend against advanced persistent threats.

The system was unable to identify vulnerable applications and, as a result, could not manage the update of vulnerable software beyond a very basic and manual scope.

There is no ability to identify or block the act of exploiting vulnerable software and such software cannot be restricted in functionality to improve security.

On the plus side, when the solution was installed on a pre-infected endpoint it successfully recognized and deactivated the unauthorized application.

Conclusions

Monitoring the network

All applications were capable of auditing the software on the network to some degree, but none was close to reaching ideal levels of control and integrity.

Classifying software

Kaspersky Endpoint Security for Windows was the strongest product when it came to identifying and grouping software.

Not only did it provide lots of pre-defined information on applications but it also allowed the administrator to create application groups as well as providing high levels of detail about the files involved.

The competition tended to provide lots of detail or allow the creation of groups, but not both.

Business as usual

It is essential that users are not hampered in their work, and the Kaspersky product was deemed least likely to do so.

Its effective test mode and apparently unique approach to managing updaters puts it on the top of the pile.

Should a problem occur, Kaspersky's user feedback system is rivaled only by that provided by McAfee.

User and machine groups

Symantec's software scored most highly, closely followed by Kaspersky's system, leaving the other two products trailing far behind.

This is largely because they were able to apply policies to users and user groups, which was something the competition could not do.

Logging

Kaspersky's logging facilities lead the field, followed at a distance by all three competitors.

In most cases its advantage lay in the level of detail provided, which outstrips the log systems of both McAfee and Symantec. Sophos' system did not seemingly log its own events at all.

Advanced Persistent Threats

While Kaspersky's product scored the highest in the APT test, it still only achieved 67 per cent of the possible maximum score.

It succeeded where others failed by recognizing and then handling the update of vulnerable applications. The other products were much less functional in this regard.

It also succeeded in remediating a pre-infected network. Symantec's product was the only other software to achieve this.

All products would do well to identify and block the exploitation of vulnerable applications. This is an action distinct from detecting a past exploit and remediating the attack by removing malicious files that were created as a result.

Overall conclusion

The products that performed the best overall tended to use, or make available at least, a default deny policy. Their success in a production environment will rely on how well administrators handle user complaints.

Products from Kaspersky and, to a lesser degree, McAfee are the strongest contenders in this area.

For user management roles, Symantec Endpoint Protection comes out best.

Sophos' solution is, in terms of application control, a lightweight option providing administrators with a near hands-off experience. For more granular control a more fully-featured system is required.

Appendix A: Terms Used

Advanced Persistent Threat (APT)	A targeted attack that must by definition be sufficiently advanced to penetrate defenses such as anti-malware systems; that must remain undetected over time; and that causes damage to the organization (e.g. via data stealing or data loss).
Blacklist	A list of applications that are banned from running on the network.
Default allow	A policy that allows all software to run, except applications listed on a blacklist.
Default deny	A policy that prevents all software from running, except applications listed on a whitelist.
Exploit	A means of causing a vulnerable application to perform unintended tasks or to behave in an otherwise unexpected fashion. In the context of this report an exploit is used to gain unauthorized access to the target system.
Observation mode	See 'Test mode'.
Test mode	An operational setting that causes an application control system to monitor the effects of its policies without enforcing them.
Vulnerability	A mistake in the coding of an application that makes it possible to exploit it.
Whitelist	A list of applications that are allowed to run on the network.

Appendix B: FAQs

- This test was sponsored by Kaspersky.
- The tests were conducted between 27th July 2012 and 30th November 2012 using the most up to date versions of the software available on any given day.
- All products were able to communicate with their back-end systems over the internet.
- The products selected for this test were chosen by Dennis Technology Labs.
- All vendors invited to participate were made aware of the above details in advance.
- All vendors were invited to provide suitable system settings and technical support to the testers as if they were genuine customers needing to solve the challenges outlined in the testing methodology.

WHILE EVERY EFFORT IS MADE TO ENSURE THE ACCURACY OF THE INFORMATION PUBLISHED IN THIS DOCUMENT, NO GUARANTEE IS EXPRESSED OR IMPLIED AND DENNIS PUBLISHING LTD DOES NOT ACCEPT LIABILITY FOR ANY LOSS OR DAMAGE THAT MAY ARISE FROM ANY ERRORS OR OMISSIONS.