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.

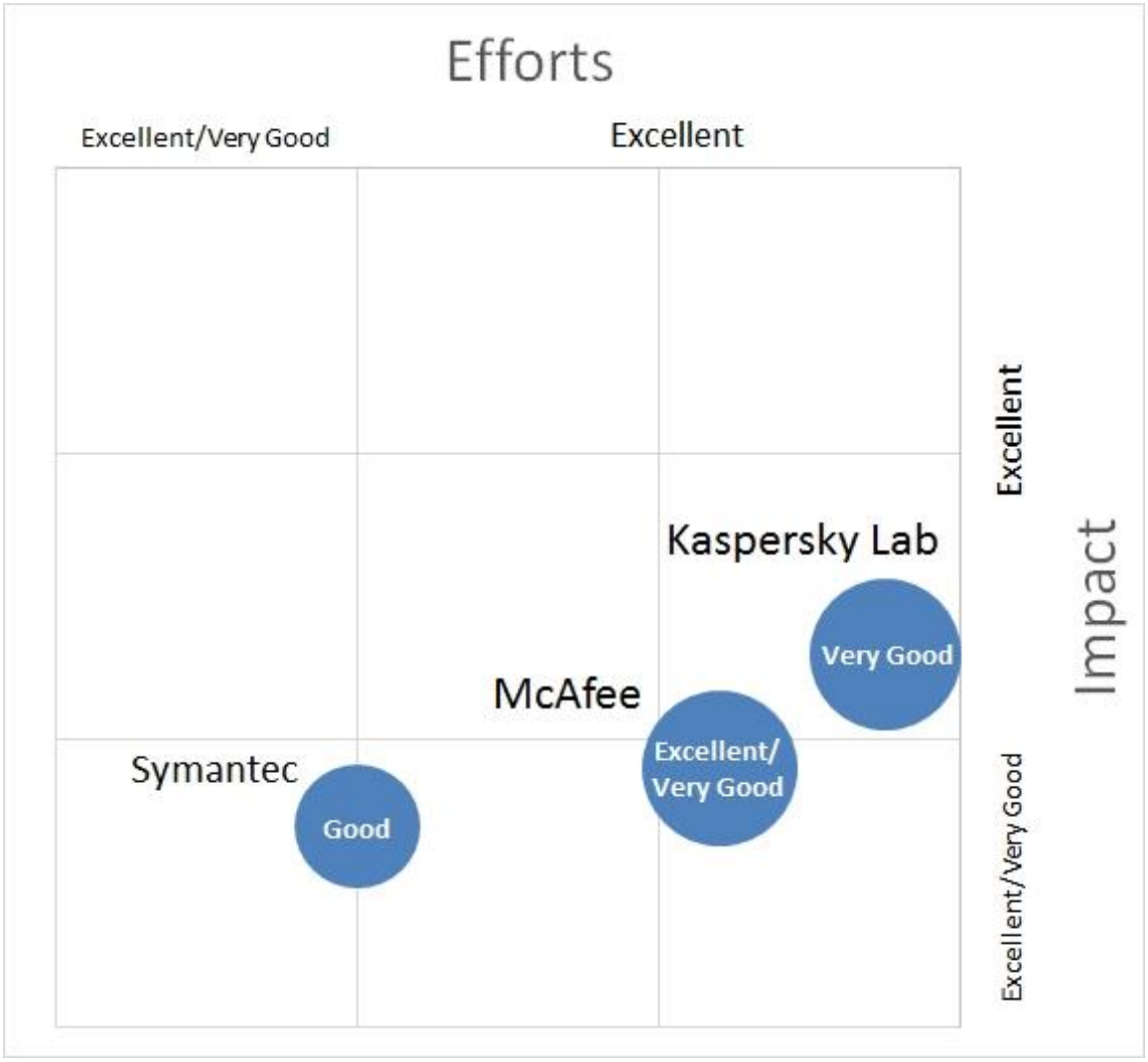
Impact: Most efficient resource usage, greatest transparency

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.



* The bubble size and its label represent the product's scores in category Value

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.

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

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