TEST REPORT

Tolly.

#211132
October 2011
Commissioned by
Kaspersky Lab

Kaspersky Endpoint Security 8 for Windows

Comparative Functionality Evaluation vs. ESET, McAfee, Sophos, Symantec and Trend Micro

Executive Summary

Today's network administrators are always searching for tools to assist them in providing comprehensive security for their network, while adapting to an increasingly mobile, cloud-centric and geographically-distributed workforce. Functionality and reporting with Web, application and device controls can no longer be secondary to protection when administrators are faced with managing an increasing number of endpoints.

By combining multiple technologies into a single, centrally-managed solution, Kaspersky Endpoint Security 8 for Windows offers an extensive set of tools to ensure security and control over an array of applications, devices and Web content. Kaspersky's features range from ready-to-use templates to granular policy controls, to help administrators customize Kaspersky's solution to their organizations' unique needs, thus simplifying the user experience while providing extensive security and management.

The Bottom Line

Kaspersky Endpoint Security 8 for Windows:

1. Offers superior Web, device and application control compared to competitors
2. Provides easy-to-use flexible policy creation tools to ensure comprehensive endpoint control
3. Leverages application control and whitelisting to strengthen security posture against targeted attacks through system-wide or employee-specific policies together with Application Privilege Control to control access to system operations
4. Utilizes the Application Vulnerability Monitor, to provide complete reports on outdated software

Kaspersky Endpoint Security 8 Application Control Features

Application Control and Whitelisting Capabilities	Kaspersky	ESET	McAfee	Sophos	Symantec	Trend Micro
'Default Deny' support with built-in exclusion of necessary system processes and trusted updaters	✔		✔			
Allow/block applications by:						
Selecting from an applications registry list	✔[2]			✔[3]		
Selecting executable files from an inventory list	✔[4]					
Inputing metadata of executable files *(e.g. file name, version, application name, application version, manufacturer)*	✔		Partial[5]			
Inputing checksum of executable files (MD5, SHA1)	✔		✔		✔	
Inputing executable files' path *(either a local path or UNC path)*	✔		✔		✔	✔
Selecting built-in application categories *(e.g. browsers, security tools, games)*	✔			✔		
Allow/block applications for specific Active Directory users or user groups	✔		✔			
Monitor and restrict application privileges *(read/write permissions to networks, registries, system files and certain system settings)*	✔		✔[8]		✔	✔
Monitor and prioritize application vulnerabilities (Microsoft and third-party)	✔	Partial[6]	✔[7]			

Notes: 1. Empty cells denote feature is not present. 2. Kaspersky pulls existing applications (e.g. Adobe Reader 9, iTunes)on all managed clients to an applications registry list in the Security Center console for administrators to create policies. 3. Sophos provides built-in common use application templates using metadata and checksum of executable files at the back end. Administrators cannot customize application templates. 4. Kaspersky pulls existing executable files (e.g. Skype.exe, chrome.exe) on all managed clients to an executable files inventory list in the Security Center console for administrators to create policies. 5. McAfee supports file name. 6. ESET can show available Microsoft updates on clients but not in the ESET Remote Administrator Console. ESET does not support third party vulnerability monitoring functionality. 7. Requires McAfee Risk Advisor and McAfee Vulnerability Manager or Policy Auditor. 8. Using McAfee Host Intrusion Prevention and McAfee VirusScan Enterprise.

Source: Tolly, October 2011

Table 1

Exec Summary (Con't...)

Tolly engineers evaluated Kaspersky Lab's Endpoint Security 8 for Windows and compared it to endpoint security suites from leading vendors like ESET, McAfee, Sophos, Symantec and Trend Micro. See Table 5 for information on the products tested.

The evaluation focused on the functionality offered by each product in the areas of Web control, device control, application control and manageability/reporting. Engineers also observed the ease-of-use associated with each product in terms of the number of steps and time required to install/configure the solution and perform tasks.

Tolly engineers found that Kaspersky offers extensive application control, Web control and device control capabilities with a single product and an intuitive management console. Unlike other vendors' offerings, all policies in Kaspersky can be computer specific, user specific and with scheduling. This allows administrators to create very flexible policies and have greater control over endpoints with less time spent.

For application control policy creation, Kaspersky allows administrators to either choose from an inventory list or manual enter metadata of applications while other vendors only support one way. Only Kaspersky and McAfee support Microsoft and third-party vulnerability monitoring, though McAfee requires the purchase of additional products to do so.

For Web control, Kaspersky is the only vendor to provide specific Web control policies with built-in content categories (e.g. social networks) and data type (e.g. executable file) while other vendors have to use a firewall or purchase add-on products or modules to achieve a similar level of functionality.

Kaspersky and McAfee offer three tiers of device control (bus, device type and serial number) while other vendors offer two at the most.

Kaspersky Lab

Endpoint Security 8 for Windows

Comparative Endpoint Security Feature Evaluation

Tolly. Certified

Tested October 2011

Application Control

In all size businesses, enterprise and SMB, environments, managing applications on

Kaspersky Endpoint Security 8 Web Control Features
vs. ESET, McAfee, Sophos, Symantec and Trend Micro

Web Control Capabilities	Kaspersky	ESET	McAfee	Sophos	Symantec	Trend Micro
Allow/Block/Warn Web resources by:						
URL	✔	✔[2]	✔[2]		✔[2]	
Selecting built-in content categories *(e.g. chat and forums, web-mail, casual game sites, social networks, etc...)*	✔		Partial[3]			
Selecting built-in data type categories *(e.g. video, executable file, archives, etc.)*	✔					
Integration with Active Directory *(AD user group/user specific policies)*	✔		✔[4]			
Allow/block Web resources based on date/time periods	✔		Partial[4]		✔[2]	
Report detailed PC usage for Web browsing activities	✔		✔[5]			

Notes:1. Empty cells denote feature is not present. 2. No Web control policy support. Can configure the firewall to block remote domain. McAfee SiteAdvisor Enterprise Plus 3.0 supports blocking URL. But it does not support Chrome and latest version Firefox 6 and 7. 3. Using McAfee Web Filtering for Endpoint Module which is an add-on for McAfee SiteAdvisor. McAfee SiteAdvisor Enterprise Plus 3.0 does not support Chrome and latest version Firefox 6 and 7. See KnowledgeBase: https://kc.mcafee.com/corporate/index?page=content&id=KB51244 4. McAfee HIPS Firewall rules support scheduling but McAfee SiteAdvisor does not support scheduling. 5. Using McAfee Web Reporter which requires a dedicated server.

Source: Tolly, October 2011

Table 2

Kaspersky Endpoint Security 8 Device Control Features/ Capabilities
vs. ESET, McAfee, Sophos, Symantec and Trend Micro

Device Control/ Capabilities	Kaspersky	ESET	McAfee	Sophos	Symantec	Trend Micro
Policy-based control of devices:						
By port type/bus *(e.g. USB, FireWire, serial, etc.)*	✔	Partial[2]	✔		✔	✔[3]
By connecting device type *(e.g. removable media, printer, CD/DVD, etc.)*	✔	✔	✔	✔	✔	✔
By Active Directory user group level	✔		✔			
Whitelist creation based on serial numbers of devices	✔		✔	✔		
Read/write permission granularity of device access with scheduling	✔		✔	Partial *(no scheduling)*	Partial[4] *(no scheduling)*	Partial *(no scheduling)*
Temporary access permission management	✔		✔			
Priority based 'default deny' policies *(e.g. serial number over device type and device type over bus level)*	✔	✔[2]	✔	✔		

Note: 1. Empty cells denote feature is not present. 2. ESET supports blocking removable media. On the client, administrator can add a specific port as exception. ESET does not support other bus-level blocking. 3. USB only. 4. Using application control rules

Source: Tolly, October 2011 Table 3

endpoints and the threats that come with them can become a full-time job.

"Default Deny" and "Default Allow" Scenarios

Default deny means that when the endpoint security product is installed, applications are automatically "denied" access until they are explicitly "approved" by the administrator.

Kaspersky offers a predefined set of categories from the cloud and local rules to manage "default deny" by creating customized administrative whitelisting and "default allow" by defining categories of applications that should be blocked.

Tolly engineer evaluated a solutions' ability to provide a convenient way to exclude necessary system processes and trusted updaters. Kaspersky provides built-in "golden image"[1] and "trusted updaters" categories, which must be allowed in the "default deny" scenario.

Among the competitors, only McAfee implements "default deny" by pre-scanning the client and whitelisting all current applications. ESET, Sophos, Symantec and Trend Micro do not offer this feature.

While each approach requires some up-front attention from administrators, surely it requires less effort in the long run to utilize "default deny" approach. The increased security of the hardened and locked endpoint requires little further attention from administrators since no unauthorized code or malware can be run on the system.

Policy-Based Control of Applications

Kaspersky allows network administrators to have a high level of control over endpoints and their applications by providing tools to make their own menu of categories to block/ allow using registry and inventory tools to create custom categories from a list of all available applications. (See Table 1.)

Categories from Registry/ Inventory List

Kaspersky allows administrators to pull all existing applications and associated executable files (MD5 hash) on clients in 'real-time' to the management console, and then create custom policies. In addition to custom category-building from a registry, only Kaspersky provides approximately 100 predefined categories that are updated from the cloud database (i.e. browsers, security tools, games, etc.).

Sophos provides template categories to create policies, but these are built-in, not available in real-time. As a result, some templates may not work with the latest versions, as was the case with this test (i.e. FileZilla Client version 3.5.1).

ESET, Sophos, Symantec and Trend Micro administrators must manually input the name and file path or the hash of the executable files to add them to application policies.

[1] "Golden Image" and "trusted updater" are used by Kaspersky to describe application category which includes necessary system processes.

Kaspersky Endpoint Security 8 for Windows Manageability and Reporting Features
vs. ESET, McAfee, Sophos, Symantec and Trend Micro

Manageability and Reporting Capabilities	Kaspersky	ESET	McAfee	Sophos	Symantec	Trend Micro
Customize report generation with filters	✔	✔	✔	✔	✔	✔
Utilizes useful and relevant built-in report templates *(e.g. Summary and management-level report, policy violations and activities report)*	✔	✔	✔	✔	✔	✔
Customize notifications to users *(e.g. Why an application was blocked, what policy spawned the block and who to contact within their organization)*	✔		Partial[2]	✔	✔	✔

Note: 1. Empty cells denote feature is not present. 2. Available for Web control but not application control

Source: Tolly, October 2011 Table 4

Metadata, Checksum and File Path Filtering

Engineers also evaluated a product's ability to detect specific applications allowed or blocked by using a number of different filters such as metadata (i.e. file name, version, application name), file path (i.e. local or UNC path [2]) and checksum to manage and create their own policies. Kaspersky supports all of the above.

McAfee partially supports metadata, by file name only, but does support inputing checksum and file path.

Symantec supports only inputing checksum and file path, while Trend Micro only supports file path.

Monitor/Restrict Application Privileges

In addition to allowing network administrators to control which applications are run, and by whom, administrators are also able to direct how applications are run by monitoring and restricting privileges.

This allows an application to run within certain parameters, but as soon as the application attempts to alter the system, by attempting to access registries, system files and/or certain system settings, that application is restricted from doing so. (See Table 1.)

Integration with Active Directory

This test evaluated a products' ability to integrate with Microsoft Active Directory and use existing user groups to set application allowances using those groups.

Kaspersky and McAfee are able to integrate with Active Directory, whereas the other solutions under test, ESET, Sophos, Symantec and Trend Micro are unable to use existing Active Directory user groups.

Vulnerability Monitoring

Engineers tested each products' ability to scan and analyze applications, both Microsoft and third-party, and list vulnerabilities and their associated severity. Kaspersky provides monitoring for both Microsoft and third-party applications, utilizing their Security Center console.

ESET can only show available Microsoft updates on clients, but not on the ESET remote administrator console. ESET does not support third-party vulnerability monitoring functionality.

McAfee can monitor vulnerabilities from Microsoft and third-party applications, but requires the addition of McAfee Risk Advisor and McAfee Vulnerability Manager or Policy Auditor.

Sophos, Symantec and Trend Micro do not have any vulnerability monitoring capability.

Web Control

Although the core of endpoint coverage is focused on applications, as most malware is spread through the Web, having integrated Web controls is an integral part of endpoint security.

Web Control by Category Resource/ Data Type

To evaluate Web control features, Tolly engineers tested block/allow/warn features by URL (Tolly engineers used www.google.com), built-in content category type (i.e. chat rooms/ forums, web-mail, game sites, social networking, etc.) and data type, which tested if a solution can block certain data types like video, executable files, archives, etc.

Engineers found that Kaspersky Endpoint Security 8 is the only endpoint protection product out of those tested that provides across-the-board Web management and protection in a single product. McAfee

[2] Universal Naming Convention (UNC) Path describes a location of a volume, directory or file by server name, a share name and an optional file path.

requires additional products to achieve similar levels of functionality. (See Table 2.)

Kaspersky also supports "warn" control policies, so if a user goes to a monitored or prohibited site (i.e. Facebook), the user will get a warning that if they choose to proceed their usage can be audited by the administrator.

The ESET and Symantec solutions are only able to block/allow by URL, and the solutions under test from Sophos, and Trend Micro lack any Web control feature and require the purchase of additional solution(s) to achieve similar levels of Web control. (See Table 2.)

Active Directory Integration

Engineers also tested products' ability to integrate with Microsoft Active Directory (AD) to use previously defined user groups and user-specific policies. Being able to leverage this existing organizational data within the administrator portal saves a significant amount of time when setting up and assigning organizational Web policies.

Allow/Block Based on Time/Date

Another level of control is found in being able to tailor Web policies, not only to user type, but also to the time of day; allowing/blocking Web resources based on time/date. For example, administrators can block social networking sites such as Facebook and Twitter from 9 A.M to 5 P.M., but allow it outside of work hours.

Kaspersky offers these features, while McAfee and Symantec Firewall rules support scheduling, but McAfee SiteAdvisor does not (See Table 5). ESET, Sophos, and Trend Micro do not support scheduling.

Web Usage Reporting

Additionally, the Kaspersky administrator console provides a report of detailed PC usage for Web browsing activities, so administrators can track browsing history by workstation.

Device Control

Removable media devices such as USB, DVD/CDs and printers can also be potential entry points for threats.

Policy- Based Control of Devices

Tolly engineers evaluated each solutions' capability to control the use of devices that are compatible with company PCs. Engineers tested each product's ability to define the port(s) or bus (USB, Fire Wire, serial, PCMCIA, etc.) which can be utilized by types of devices at any given time by any given user.

Kaspersky, McAfee and Symantec all are able to control device access by port type and connecting device type. ESET is able only to support blocking removable media. ESET is able to add a specific port as an exception, but they do not support other bus blocking levels.

Sophos offers allow/block based on connecting device type, but not by port. Trend Micro only supports control by the USB port type and three device types.

Active Directory Integration

Permissions can also be set by the network administrator. Engineers tested each solutions' ability to pull from existing Microsoft Active Directory data to grant permission to existing user groups.

Out of the products tested, only Kaspersky and McAfee have this feature, which allows easy creation of user/user group-specific policies.

ESET, Sophos, Symantec and Trend Micro are not able to set specific user policies using Active Directory.

Whitelist Creation by Serial Number

For this feature, Tolly engineers evaluated each products' ability to pull device access events with device serial numbers from clients and allow administrators to create policy exceptions.

Kaspersky, McAfee and Sophos offer administrators a way to automatically authorize trusted devices based on device serial number rather than just device type.

ESET, Symantec and Trend Micro do not provide this feature.

Read/Write Permission Granularity

Tolly engineers evaluated whether or not the products under test could manage users' ability to read and/or write files on a device. This test also evaluated if a product could determine permissions based on date/time scheduling.

Kaspersky and McAfee offer scheduled read/write restrictions whereas Sophos, Symantec and Trend Micro only offer the restrictions, with no scheduling capability. ESET offers no portion of this functionality in the products tested.

Temporary Access Permission Management

Tolly engineers tested if a solution allows users to request temporary access when a device is blocked and administrators are able to grand the access.

Users of Kaspersky and McAfee are able to request this temporary permission while Trend Micro, Sophos, ESET and Symantec, are not.

"Default Deny" Policy

For this scenario, Tolly engineers evaluated if a solution supports device control rules with priorities. Such priorities include serial number of over device type, or device type over port type (bus level).

All solutions except Symantec and Trend Micro can be set to use these policies .

Ease of Use

Tolly engineers engaged in numerous test scenarios that relate to everyday responsibilities for administrators.

Features such as built-in categories, Active Directory integration and policy scheduling

Solutions Under Test

Vendor	Product	Version
Kaspersky Lab	Kaspersky Security Center	9.0.2756
	Kaspersky Endpoint Security 8 for Windows	8.1.0.629
ESET Software	ESET Remote Administrator Console 4.0.138 + ESET Smart Security Business Edition	4.2.71.2
McAfee, Inc.	McAfee ePO	4.6.0 (Build: 1029)
	McAfee Agent	4.6.0.1694
	McAfee Application Control	5.1.2.8122
	McAfee Host Intrusion Prevention	8.0.0.1741
	McAfee SiteAdvisor Enterprise Plus	3.0.0.476
	McAfee Virus Scan Enterprise	8.8.777
	McAfee Risk Advisor	2.6.0.160
	McAfee Data Loss Prevention (McAfee Device Control License)	9.1.100.7
	McAfee Web Filtering for Endpoint	3.0.0.165
	McAfee Vulnerability Manager	
	McAfee Web Reporter	
Sophos, Ltd.	Sophos Enterprise Console	4.7.0.13
	Sophos Endpoint Security and Control	9.7.6
Symantec Corp.	Symantec Endpoint Protection Manager	12.1.671.4971
	Symantec Endpoint Protection	12.1.71.4971
Trend Micro, Inc.	Trend Micro OfficeScan	10.5 (Build: 1083)

Source: Tolly, October 2011 Table 5

exist with the administrator in mind, geared towards leveraging existing information and creating policies that can be set up and managed with minimal effort.

Tolly engineers observed that Kaspersky is the only solution tested that provides these features across the board, along with application, Web and device control policies in a single product.

Engineers found that while McAfee supports most features, it requires almost 10 components/products/modules to do so. Some of these are extensions or packages, but some require designated servers. See Table 5.

Other solutions do not have Web control policies at all, and administrators can only use firewalls to block certain URLs.

Test Methodology and Test Bed Setup

Test Methodology

Tolly engineers used one Windows Server 2008 R2 virtual machine and one Windows 7 Enterprise 32-bit virtual machine for each solution. One USB drive was used for device control tests.

Firefox, Chrome, Skype, AIM, Adobe Reader, FileZilla FTP client, uTorrent, iTunes, Microsoft Internet Explorer and Microsoft Office 2007 were used for application control and whitelisting tests. Adobe Reader 9.0 was used to test the application vulnerability monitoring feature.

Application Control

Engineers evaluated several areas of application control functionality: "default deny", application registry, application inventory, control policies using metadata,

control policies using checksum, control policies using file path, pre-existing categories, Active Directory integration, application vulnerability monitoring and restriction of application privileges.

Tolly engineers enabled the "default deny" scenario with exclusion of necessary system processes and trusted updaters. Whether the Windows system runs without any problems and can be updated, the solution is considered to support "default deny" scenario.

For the application registry, whether a solution provides an application list with all the applications listed above (either pulled from clients or pre-configured), and administrators can create application control policies using items in the list, the solution is considered to support allow/block certain applications by an application registry.

For application inventory, whether a solution provides an executable file inventory list with existing executable files (e.g. skype.exe, chrome.exe, aim.exe, etc.) on all clients, and administrators can create application control policies using items in the list, the solution is considered to support allow/block certain applications by the executable file inventory list.

Whether a solution supports application control policies creation using metadata of executable files like file name, version, application name, application version and manufacturer, the solution is considered to support allow/block certain applications by metadata of the executable file.

Tolly engineers evaluated whether a solution supports application control policies creation using checksum (e.g. MD5 or SHA1) of executable files, the solution is considered to support allow/block certain applications by checksum of executable files.

To determine whether a solution supports application control policy creation using a local path (e.g. C:\Program Files\AIM) or a UNC path (e.g. \\sampleserver\share \applications), to allow/block all executable files in the path to launch, the solution is considered to support allow/block certain applications by executable files location path.

To test whether a solution supports application control policies creation with pre-configured application categories (e.g. browsers, security tools, games, etc.) to block/allow all applications in the categories, the solution is considered to support allow/block certain applications by categorization to application functionality. Tolly engineers tested browsers category using Chrome, Firefox and IE.

If a solution supports the option to specify an existing Active Directory user/user group in the application control policy, the solution is considered to support allowance or block for a specific user or user group.

For the monitor and restrict application privileges test, Tolly engineers tested whether a solution supports prohibiting a program, AIM, for example, to modify Windows startup settings. If so, the solution exhibits this feature.

If a solution's management console provides a list of all Microsoft and third-party application vulnerabilities existing on clients with severity flags, it is considered to support monitor and prioritize application vulnerabilities.

Web Control

Tolly engineers evaluated the devices under test to determine if they could exhibit allow/block/warn capabilities when programmed by: URL, content category and data type.

Content category is defined as if a solution provides built-in categories to select from, such as game sites, social network sites, web mail and chat/forums, etc.

Data type is defined as if a solution can block a certain data type such as video, executable files and archives, etc. Functionality was evaluated on whether or not this was an option in the administrator portal.

Device Control

Tolly engineers evaluated whether a solution could control block/allow by using "Default Deny" by port (bus), by device type, by user group (pulled from Active Directory), by serial number, whitelist creation by serial number, by read/write permission with scheduling and temporary access management.

For "default deny", Tolly engineers evaluated whether a solution could be controlled by rules with priorities (i.e. serial number over device type and device type over bus level).

For "on bus" Tolly engineers tested whether a solution could block a device by port like USB, FireWire, Serial, PCMCIA, etc.

To test block/allow "on type" Tolly engineers evaluated whether a solution could block removable devices such as printers, storage, CD/DVD, Wi-Fi, etc.

Engineers tested whether they could sync a given solution with Microsoft Active Directory users/user groups, and use those to create a custom block/allow policy.

For whitelist creation based on serial numbers, Tolly engineers evaluated whether a solution can pull device access events with device serial numbers from clients and allow administrators to create policy exception (trusted device).

Tolly engineers defined the temporary access permission management feature as a solution that allows users to request temporary access when a device is blocked and administrators are able to grant the access. Whether users are able to request this access from the administrator determines if the feature is present in the product under test.

Read/write permission granularity and scheduling is defined by Tolly engineers as a solution allowing the user to read the files on the device, or read and write on the device. Scheduling is defined as being able to set policies based on date/time.

About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 20 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at *sales@tolly.com*, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at:
http://www.tolly.com

Interaction with Competitors

In accordance with Tolly's Fair Testing Charter, prior to the start of the testing, Tolly personnel invited representatives from ESET, McAfee, Sophos, Symantec and Trend Micro to participate in the project and provided details on the proposed tests and methodology. ESET, McAfee and Sophos representatives chose to participate in this review. Upon the completion of testing, ESET, McAfee and Sophos confirmed their results. Symantec and Trend Micro representatives chose not to participate in this review.

For more information on the Tolly Fair Testing Charter, visit:
http://www.tolly.com/FTC.aspx.

Terms of Usage

lgohgpxe-mts-02Nov2011-Ver0