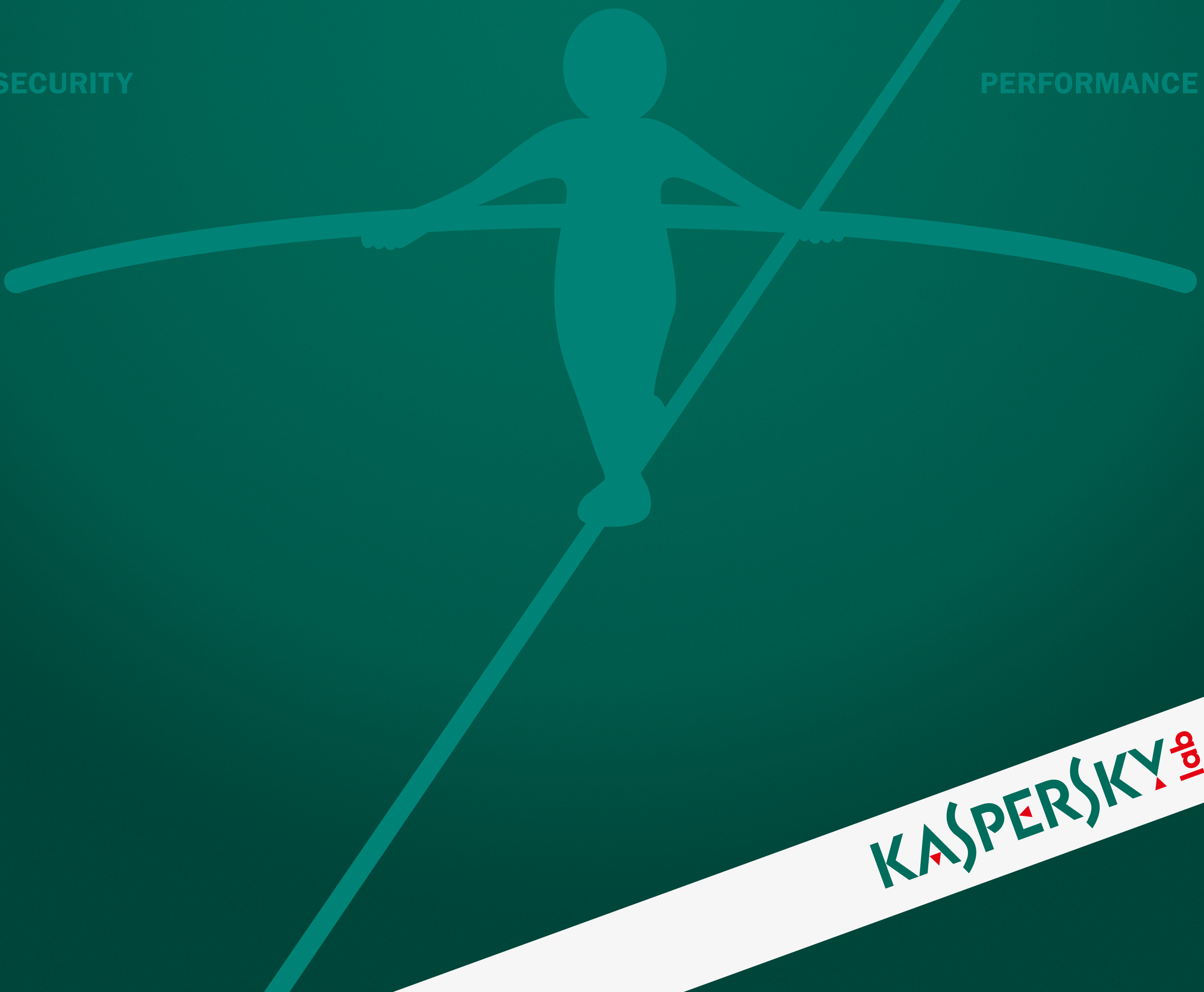
KASPERSKY SECURITY FOR VIRTUALIZATION 1.1 AND TREND MICRO DEEP SECURITY 8.0 – VIRTUAL ENVIRONMENT DETECTION RATE AND PERFORMANCE TESTING BY AV-TEST



Kaspersky Security for Virtualization 1.1 and Trend Micro Deep Security 8.0 – virtual environment detection rate and performance testing by AV-Test

Kaspersky Security for Virtualization, Kaspersky Lab's corporate security solution for virtualized IT environments, has undergone its first detection rate test at the highly reputable independent IT security institute AV-TEST.org. The test of specialized agentless security solutions for virtualized environments was conducted in March-April of 2012, during which Kaspersky Security for Virtualization 1.1 was evaluated along with Trend Micro Deep Security 8.0.

Kaspersky Security for Virtualization is delivered as a virtual security appliance that integrates with VMware vShield™ Endpoint to provide agentless, anti-malware security based upon Kaspersky Lab's advanced AV engine. Using the same engine as Kaspersky Lab's award-winning line of endpoint security products, Kaspersky Security for Virtualization avoids the needless complexity and resource-drain associated with security programs that typically "bolt-on" acquired technology for virtual environments.

The AV-Test.org regime evaluated the efficiency of specialized agentless solutions for virtualized environments in various situations, including a real-world test of malicious URLs, a dynamic detection test and a static detection test. Product performance (based on how much it slowed down the everyday use of the computer) and false detections or warnings concerning legitimate programs were also taken into consideration. The tests were performed in VMware ESXi environments and both security solutions used VMware vShield to protect the virtual machines. The virtual machines for the tests ran Windows XP with the latest Service Packs and updates.

Kaspersky Security for Virtualization turned in an excellent performance, significantly outscoring its competitor on detection rates in the 'Real World' attacks test and, in similar conditions, on static malware detection rates.

In the **static malware collection** the Kaspersky Lab solution detected 98.6% of 141,290 malware samples, including Trojans, backdoors, bots, viruses, worms, Droppers and other malware. In similar product settings, without cloud-based file reputation enabled, Kaspersky Security for Virtualization outperformed Trend Micro Deep Security by 24.38%. That translates to more than 34,000 samples detected by Kaspersky Lab's solution and missed by its rival.

When the file reputation service was enabled, Trend Micro Deep Security was almost on a par with Kaspersky Security for Virtualization, detecting 98.84% of static malware. But this reputation technology requires an Internet connection, which cannot be guaranteed in all cases because of corporate security policies and network configuration.

However, Trend Micro's reputation technologies do not help a lot in **'Real World' attack test scenarios**, where Trend Micro's solution missed 25% of attacks. In other words, every fourth attack by real-world malware on a virtual machine protected by Trend Micro Deep Security resulted in an infection during this test. Kaspersky Security for Virtualization achieved a result of 86.11% in this case, demonstrating a much higher level of protection against zero-day malware web threats.

Kaspersky Security for Virtualization 1.1 and Trend Micro Deep Security 8.0 – virtual environment detection rate and performance testing by AV-Test

DETECTION RATE TEST RESULTS

	Kaspersky Security for Virtualization 1.1	Trend Micro Deep Security 8.0
Blocking of "Real World" attacks	86.11%	75.00%
Completely blocked malware attacks	83.33%	75.00%
Partially blocked malware attacks	2.78%	0.00%
Attacks not blocked (system infected)	13.89%	25.00%

	Kaspersky Security for Virtualization 1.1	Trend Micro Deep Security 8.0
Detection of static malware - Standard Settings	98.6%	74.22% (with activated file reputation – 98.84%)

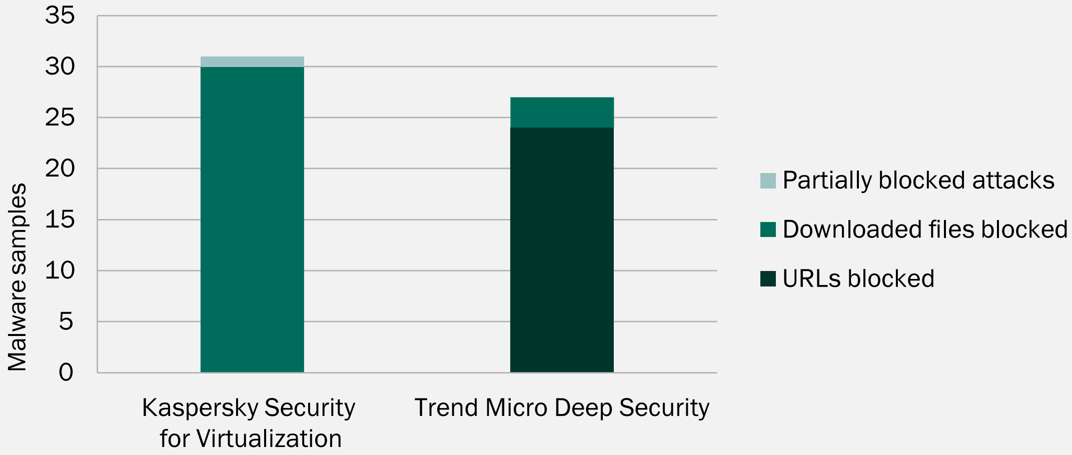
FALSE POSITIVE DETECTIONS OF NON-CRITICAL FILES

As for false positives, Kaspersky Security for Virtualization 1.1 generated zero false alarms while Trend Micro Deep Security produced two.

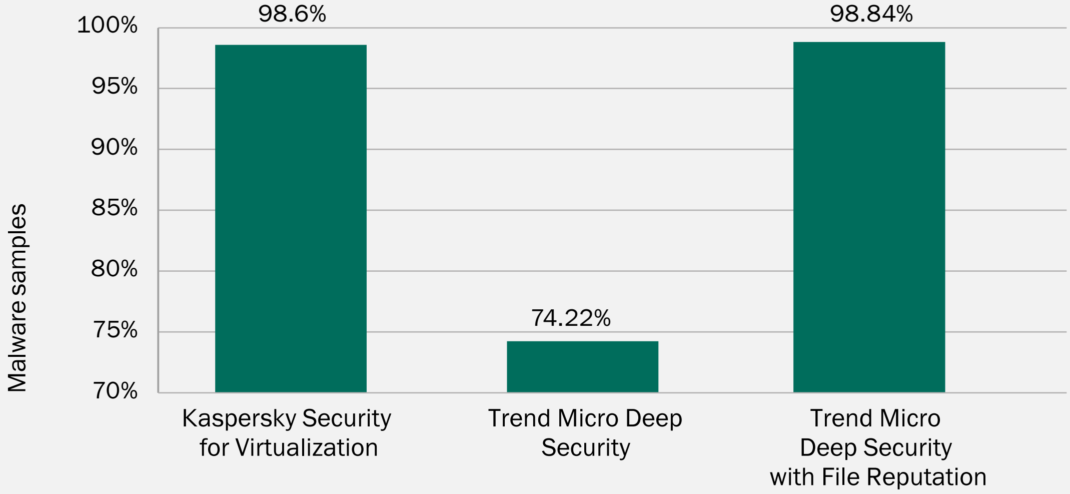
	Kaspersky Security for Virtualization 1.1	Trend Micro Deep Security 8.0
False positives (static set of files)	0	2

Kaspersky Security for Virtualization 1.1 and Trend Micro Deep Security 8.0 – virtual environment detection rate and performance testing by AV-Test

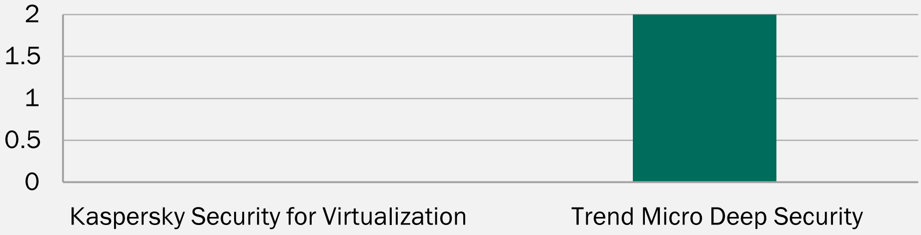
REAL WORLD DETECTION RESULTS



DETECTION OF STATIC MALWARE



FALSE POSITIVE DETECTIONS OF NON-CRITICAL FILES



PERFORMANCE TEST RESULTS

Other tests by AV-Test.org assessed the effectiveness of typical tasks performed by users on virtual desktops. These operations include downloading files, loading websites, installing applications, running applications to open specific documents and copying files. In all those scenarios Kaspersky Security for Virtualization outperformed Trend Micro Deep Security. The difference was significant in the following operations: loading websites (15%), installing applications (93%) and running applications to open specific documents (>25%).

These results reflect the fact that Kaspersky Security for Virtualization offers better performance and more efficient scanning.

	Kaspersky Security for Virtualization 1.1	Trend Micro Deep Security 8.0	% difference
Real-world performance tests *			
Download files (total average time)	325.39	349.02	**7.26%**
Load websites (total average time)	372.58	428.54	**15.02%**
Install applications (total average time)	323.13	625.14	**93.46%**
Run applications to open specific documents (total average time)	20.64	26.04	**26.16%**
Copy files (total average time)	764.00	812.48	**6.35%**

* values in seconds, lower = better

CONCLUSION:

Specialized agentless security solutions for virtual environments provide a more efficient way to protect virtualized infrastructure – with greater performance and less impact on virtualization density.

When it comes to comparing Kaspersky Security for Virtualization with another similar solution, the difference is immediately apparent. Kaspersky Lab's industry-leading anti-malware engine provides superior detection rates and heuristic analysis to detect and block even the most sophisticated polymorphic malware. It also has less impact on the performance of typical daily operations on virtual desktops.

Moreover, by having Kaspersky Security for Virtualization deployed on a virtualized host appliance, all virtual machines are protected by the same centralized malware database which is constantly updated as new threats emerge. This model ensures all virtual machines receive the same level of protection, regardless of when the machines were created, or whether they have been offline for extended periods of time. There are no "Instant-On" gaps for virtual machines that haven't been used for extended periods of time and no "AV Storms" that hog network resources while updating virtual machines.

Also, the Kaspersky Security Center administrative solution brings unified management to all virtual and physical endpoints across a wide variety of platforms. With Kaspersky, IT security professionals get a "single-pane" view of all protected machines whether they are virtual, physical or mobile.

Detailed information on the test results for Kaspersky Security for Virtualization 1.1 can be found here: http://www.kaspersky.com/security-virtualization.