Last updated: June 2015

KASPERSKY LAB VS. TREND MICRO

(Kaspersky Security for Virtualization vs Trend Micro Deep Security)

Comparison of competitive solutions for securing the virtual infrastructures

This document should help to a sale/presale person to build a dialog with potential customer in a field of virtualization security. There is a set of problems which should be resolved to achieve the best quality of virtualization protection, without suffering the preformance. Any virtualization technologies customer will face these problems.The main aim is to convince the potential customer, that Kaspersky offering is a best way to overcome all the possible problematic situations with protection of virtual infrastructures.

Document structure is a series of the blocks, each block contains four sections:

<*Problem*> - description of an actual information security problem, staying ahead the corporate enterprise. Such problem needs to be resolved quickly and efficiently;

<*How to resolve*> - a possible or recommended way of problem resolution;

<*What Kaspersky Lab offers*> - How Kaspersky Lab software can resolve described problem, what benefits this solution will provide to the customer;

<*How Trend Micro does it*> - what Trend Micro can offer to overcome the problem, how it's approach differs and/or limited comparing with Kaspersky;

<*Problem*>: *There are a lot of different types of threats that are dangerous to any company - viruses, network worms, hacker attacks, phishing, etc. Everyday a lot of new threats and malware samples are discovered. Operational outages, loss of confidential data, or problems with business continuity are very expensive to any company or corporation;*

<*How to relsove*>: Powerful and Efficient information security solution is really needed to provide high-quality defence from all possible threats. These should be a solution from well-known information security vendor, proven by time, and already used by a lot of customers. Deep technical expertise and ability to fight even the most sophisticated malware samples are really needed. High scores in independent tests and comparisons with competitors are also valuable;

<*What Kaspersky Lab offers*>: Kaspersky Lab protects users all over the world for more than 17 years. KL offers a really wide range of security solutions, consumer and corporate - endpoint security software, server safety tools, virualization protection, Web and EMail defence, DDoS prevention, and more. Kaspersky Lab is a worldwide company, which operates in 200 countries and territories and have 34 offices in 31 countries. Authors of KL products is a high-skilled team of security experts, able to analyse and stop any type of harmful content or attack, including the most sophisticated (Flame, Gauss, Carbanak etc.). Kapsersky Labs software took part in many independent tests, high scores in such tests clearly shows the outstanding quality of KL security solutions (see the actual results at the last chapter of the document). TOP3 metric for 2014 year for Kaspersky Lab is **71**%, which means that in a **93** independent tests and reviews KL products received **66** top-three finishes and were achieved First place **51** times (more info available at http://www.kaspersky.com/top3);

<*How Trend Micro does it*>: Trend Micro also a mature security vendor with a good reputation. However on some markets Trend Micro operates very actively, on others it persented less seriously. Trend Micro's business is about 50% Japan, with the other 50% covering the entire rest of the world. Trend Micro results are less impressive in other markets than in home-based Japan. Independent tests and comparisons often demonstrates Trend Micro products, however results are lower, comparing with Kaspersky. TOP3 metric-2014 for Trend Micro is **38**%, which means that in a **76** independent tests and reviews Trend Micro products received **29** top-three finishes and achieves First place **18** times.

<*Problem*>: *Traditional endpoint security solutions demonstrate a serious limitations, being used in virtualized environments. The most important problem is a big negative impact on a performance. The very important metric is a consolidation ratio - the more virtual machines will be hosted on a single physical host, the better.*

<*How to relsove*>: Specifically designed for virtualization security tools should allow to achieve the highest consolidation ratio without affecting performance of user VM's, comparing with traditional endpoint security software. To provide the most possible consolidation ratio, the next problematic scenarios should be fully avoided: 'Instant-on gap' - if virtual machine started after an offline period, it should download the latest security definitions at startup. During this 'security update' period, this VM is vulnerable to recently released malware and attacks. 'Update storm' - if all client VM's will download security updates simultaneously, it will slows down seriously performance of the virtualization host, and may overload the network. 'Scan storm' - if all user VM's start anti-malware scan at the same time, it will lower the performance of both system software and client applications, resulting in slowdown of all virtualized infrastructure.

<What Kaspersky Lab offers>: Kaspersky Lab offers a KSV (Kaspersky Security for Virtualization) product, specifically designed for virtual environments. It uses the same anti-malware engine as endpoint protection solutions from Kaspesky, offering the highest quality of defence against all types of malware and threats. To better address virtualization security issues, KSV offers 'Light Agent' architecture. It means that resource-intensive malware checking tasks are offloaded from any client to the specialized level – Security Virtual Appliance (SVA). SVA is a Linux-based hardended virtual appliance with full-featured anti-malware engine on-board, optimized for high loads. If any protected VM client needs to check some file for malware, it passes this file fully or partially to SVA. SVA checks the file and returns the verdict – clean or infected – to the client which initiates the check. Also, this means the same file has been checked by SVA only once and the results of the scan become available to any other VMs. Such architecture allows to hold antivirus engine with full updateable set of AV-bases only on the SVA, not on every protected client, and it seriously optimizes the protection of virtualization infrastructure. It allows to avoid 'instant-on gap' and 'update storm' – in any case AV-databases should be constantly updated on only one network node, on SVA only. VM clients does not need to update databases at all. 'Scan storm' is also not an issue with SVA and 'Light Agent' – since clients does not check malware itself, performance decrese of subsequent client scans are not really noticeable.

<How Trend Micro does it>: Trend Micro offers a product Deep Security for securing the virtual infrastructures. Agent-based variant of it's protection – Deep Security Agent - performs all antivirus checks on the protected VM. There is no way to offload this check to a specialized system or SVA. And a full set of the antivirus databases is located on every protected endpoint at the C:\Program Files\Trend Micro\AMSP\module catalog. These databases also need to be regularly updated on every protected VM, to ensure the up-to-date status of the virus signatures – so 'Update Storms' are possible. 'Scan storms' also possible, when a lot of Deep Security agents performs a simultaneous malware checking activities. As a result, the agent-based solution from Trend Micro is more resource-intensive than KSV Light Agent. It should be mentioned that Deep Security has a virtual appliance called DSVA (Deep Security Virtual Appliance), but it can be used for agentless protection only, not for Deep Security Agent.

<Problem>: *Malware authors never sleeps. They constantly try to develop newer harmful content, which will be able to penetrate the protection. Creating malware is a serious underground business now, not a rare initiatives of some individuals.*

<How to relsove>: Security tools should offer outstanding protection capabilities, to be 'a step ahead' comparing with the virus creators, hackers and attackers. Multi-layered protection is preferable - even if malware will be able to survive the first protection level, the later security efforts will definitely eliminate the threat.

<What Kaspersky Lab offers>: KSV Light Agent offers a wide range of protection and control modules to provide multi-layered protection from any possible malware threats:

- Mail-Antivirus is one of special security layers, it provides protection for email traffic by scanning the protocols POP3/SMTP/NNTP/IMAP, before malware is received by the client program. Any possible malware will be 'shot on the fly', before it will be able to land into the protected computer;

- IM-Antivirus is another additional layer, which scans instant messenger traffic (ICQ, MSN, AIM, IRC, etc.) for malicious URLs, phishing links, or virus code in the message text;

- KSV Light Agent offers Application Startup Control, which prevents the startup of applications by using specially-configured rules. This can be done based on flexible rules defined by the admin, including creation of dynamically updated black or white-lists, also by using pre-defined application categories. It can also be configured to fully prevent any application starting except those allowed – "default deny" mode. These rules can be also configured for users from Active Directory. Also it should be mention that whitelisting capability of KSV Application Startup Control is very useful feature for VDI (Virtual Desktop Infrastructure), it allows to build pre-defined virtual desktops with limited set of startable applications;

- Device Control also offered by LA, as useful addition to other security modules. The main purpose of this module is to control the connection of removable devices. Lots of different device types are supported for control and monitoring – USB drives, printers, tape devices, smart card readers, removable hard drives, Wi-Fi, Bluetooth devices, external network adapters, etc.

<How Trend Micro does it>: Deep Security Agent also offers a lot of different security capabilities. However many features are combined with each other, which leads to diffculties and inconsistences while configuring and using the protection.

- Trend Micro Deep Security does not offer any special modules to protect email or instant messenger traffic. However, functionality for checking traffic via specified protocols/ports can be achieved by using the Intrusion Prevention feature. But configuring Intrusion Prevention in the Deep Security Agent policy and turning on the necessary IPS rules is a very complicated process. Dedicated 'Mail Antivirus' and 'IM Antivirus' modules from Kaspersky solution provide more convenient, simple administration and better quality of protection for two of the most common vectors of malware attack – email and IM.

- Trend Micro offers Application Control functionality with the Intrusion Prevention feature. The only supported feature is the blocking of traffic associated with specific applications like Skype or file-sharing utilities. Extended functionality such as Application Startup control, application categories, or integration with Active Directory, is not supported.

- Device Control functionality does not presented at all at the Trend Micro Deep Security.

<Problem>: *Health of corporate network should be constantly monitored and controlled for any abnormal circumstances. Situation can change from positive to negative very fast. Administrator should quickly analyse any situation, and rapidly react to all possible variants of its further development.*

<How to relsove>: Corporate information security software is a complex, multi-purpose system. It resolves a lot of tasks - protection deployment, security settings configuration, malware incident reaction, log analysing, management of different security solutions at the same time, etc. Unified convenient administartion tools, that will automate and make more convenient the maximum amount of such operations, is highly anticipated by security administrators.

<What Kaspersky Lab offers>: Kaspersky approach to securing the virtual infrastructures offers a series of advanced features and techniques, that raises the level of corporate network protection, and makes the work of IT-security administrator more efficient and convenient:

- Automated remote deployment. Quick setup and run the protection is an important task. The faster the new client VM receives the protection, the better. KSV LA uses a powerful technique for remote deployment and installation of the Light Agent to any new virtual machine. It's possible to automate the deployment of LA installation package to a new VM, start the installation, and register a fresh LA-client on the administration server. An important moment, the remote deployment can be performed to any amount of new VM's simultaneously, not to only one. Also it should be mentioned that all necessary actions are performed via the Security Center console, no need to direct connections to the client VM via any remote control tool.

- Unified management console. Kaspersky Lab offers a unified corporate administration platform - Kaspersky Security Center (KSC). Almost all KL products, including KSV, are administered through KSC. By using the plug-in architecture, KSC allows you to manage different types of security applications from Kaspersky. As a result, the administrator only needs one console to manage, for example, KES (Kaspersky Endpoint Security) and KSV (Kaspersky Security for Virtualization). It's also possible to build reports with combined data from both products, allowing analysis of security incidents captured by different protection solutions. All these console unification features increase the productivity of administrator work, and raise the quaity of the overall corporate protection.

<How Trend Micro does it>: Deep Security uses a Web-console, allows administrator to perform a lot of virtualization security related tasks. However administration aporach of Trend Micro is weaker, comparing with Kaspersky:

- Deep Security does not offer any built-in tools for remote deployment of Deep Security Agent. One of the possible ways of deploying the agent is to go to the console of the VM that requires protection, and manually perform the installation process. An alternative method is to use third-party software deployment tools (like Microsoft SCCM). A third way is to generate deployment scripts from the Deep Security Manager console, which can be imported and run later by Windows Powershell on the client machine. All these approaches are more complicated and inconvenient that automatic Remote Installation offered by the product from Kaspersky Lab;

- Deep Security uses a proprietary administration console, not compatible with any other product from Trend Micro. As a result, in order to work with Office Scan (traditional endpoint security solution from TM), the administrator needs to switch to another console, compatible with Office Scan only. Work with both products requires the admin to use two consoles simultaneously. It's a non-convenient approach, which will decrease productivity of the administrator;

- Also it should be mentioned that Trend Micro offers some additional unified console with support for different products - Control Manager. Via Control Manager it's possible to work with both software solutions – Deep Security and Office Scan. However not all product features are supported in Control Manager, so administrator often needs to switch from CM console to proprietary product console, and vice versa – it's really inconvenient and lowers the productivity of administering corporate IT-security.

Products versions compared

• Kaspersky Security for Virtualization 3.0.0 Agentless build 92 • Kaspersky Security for Virtualization 3.0.0 Light Agent build 3.1.63.4000 • Kaspersky Security Center 10.1 build 249 MR1	• Deep Security Manager 9.5 build 2456 • Deep Security Virtual Appliance 9.5.2 build 2022 • Deep Security Agent 9.5.2 build 2022 • Deep Security Notifier 9.5.2 build 2022

ANTI-MALWARE AND PERFORMANCE TEST RESULTS

- **Virtual Desktops Security Test Report (May 2014).** Full test results. Independent laboratory AV-TEST performed a comparative review of security solutions for virtual environments to analyze their capabilities to protect against real world malware as well as the performance impact in VDI environments. Kaspersky Security for Virtualization outperforms Trend Micro Deep Security in a number of tests:

  - Real World Detection Results - KSV detects all **48** test samples, Trend Micro failed one test-case and finishes with **47**;

  - Login VSI benchmark suite emulates realistic workloads on every virtual desktop and measures the response time - the lower values, the better. Thereby this test determines the overall system performance. Login VSI value for KSV is **2.751**, for Trend Micro is **4.549**. So the KL solution shows better performance, than Trend Micro;

  - Average Boot Time - another performance-based test, shows the impact of protection software to booting time of VM. Also the lower is better. KSV value is **109**, Deep Security result is **171** - Kaspersky product have less significant impact to boot time, comparing with the competitor.

- **Competitive Anti-virus Performance and Effectiveness in VMware vSphere 5.1 Virtual Environments by Tolly (August 2013).** Full test results. Kaspersky Security for virtualization 2.0 (Agentless) demonstrates:

  - Faster response time while scaling (increase in the number of protected VM's), comparing with agent-based solution from Trend Micro, especially in 140 protected VM test;

  - More efficient HDD usage, as a result higher VM density, comparing with Trend Micro and Symantec solution;

  - Significant reduction in the time of on demand re-scan, compared with other tested solutions that do not require the installation of anti-malware agents;

  - Better malware detection rate than other tested solutions that do not require the installation of anti-malware agents.