KASPERSKY lab

VIRTUALIZATION SECURITY

KNOW YOUR OPTIONS

kaspersky.com/business

1.0 ONE SIZE DOES NOT FIT ALL

For virtualization security, there is no one-size-fits-all solution. You have numerous options to take into consideration, and trying to fit your organization's specific needs into the wrong security products can be a costly mistake. Do you know how to pick the right option for your organization?

This whitepaper describes the different virtualization security solution options—conventional agent-based; agentless; and Light Agent—as well as possible scenarios for aligning the right security approach to your organization's virtual environment.

2.0 THE VIRTUALIZATION MARKETPLACE

Virtualization is widely deployed today. Organizations are embracing the business benefits of virtualization, including:

- Energy and IT cost savings
- Improved server provisioning
- Simplified application deployment
- Improved disaster recovery
- Decreased hardware costs
- Minimized space requirements
- Increased reliability
- Centralized management and monitoring tools
- Rapid launch of new services
- An easily-scalable, dynamic IT infrastructure

Unfortunately, as the prevalence of virtualization grows, cybercriminals are increasingly looking at virtual environments as a ripe frontier for launching attacks. While today's organizations recognize the importance of securing their virtual environment, many IT professionals don't know that specialized security solutions have been designed to deliver both security and efficiency for virtual environments. In fact, only a third of IT decision makers possess strong knowledge of their options when it comes to virtualization security. Yet, 53% of businesses are concerned about securing their virtualized environment.[1] Why the disconnect? For one thing, virtualization security is a complex topic. Let's take a look at the options available.

1. Global IT Security Risks Survey 2015

3.0 SECURITY IN VIRTUAL ENVIRONMENTS

The myth that virtual machines are more secure takes its origin from the fact that virtualization-aware malware would avoid performing any malicious operations when it would detect it was launched within a virtual machine. The authors of the malware used to do this to avoid the possibility that their programs would be analyzed. This is no longer the case.

While virtual machines may be less prone to threats such as spyware and ransomware, they are just as vulnerable to malware in the form of malicious email attachments, drive-by-downloads, botnet Trojans and even targeted "spearphishing" attacks.

Another misconception is that malware doesn't specifically target virtual machines. This couldn't be further from the truth. Malware authors always seek the easiest and most expedient route to targets. If an attacker has access to VM storage, he is able to introduce changes to VMs so next time they are booted up, they are already infected! Therefore not giving virtual environments proper security consideration is highly unadvisable.

Virtualization is often an important element in the IT department's efforts to do more and spend less. Whether you're running applications on physical or virtual machines, you still need to guard against the constant increase in sophisticated cyber threats that could jeopardize your day-to-day operations. Some of these threats include disrupting your business processes, stealing and exposing your confidential business information, compromising the security of your data and destroying the competitive advantage that your business gains from its intellectual property.

While virtualization is ultimately beneficial for companies — and is often seen as the best way to expand networks, improve efficiency and optimize data security — IT managers are now facing a whole new set of challenges. While the business benefits are clear, the risks are less well-documented and understood, which makes selecting the right virtual-aware anti-malware solution even more important.

Performance, protection and resource issues arise from traditional agent-based anti-malware solutions operating in virtual environments. Virtualization is all about maximizing your investment through optimizing your IT infrastructure. If your anti-malware solution requires that database dedicated security agent be installed on each of your virtual machines, the object of the exercise is partly defeated —protection is compromising productivity.

4.0 VIRTUALIZATION SECURITY SOLUTION OPTIONS

A great first step to securing a virtualized environment is as easy as taking your already established security and operational policies for your physical servers and desktops, and replicating them across your virtual environment. However, it is important to keep in mind that while replicating these security policies is an easy first step; this does not mean that you should use the same security technologies. In fact, doing so may result in security gaps, increase IT costs and introduce system inefficiencies.

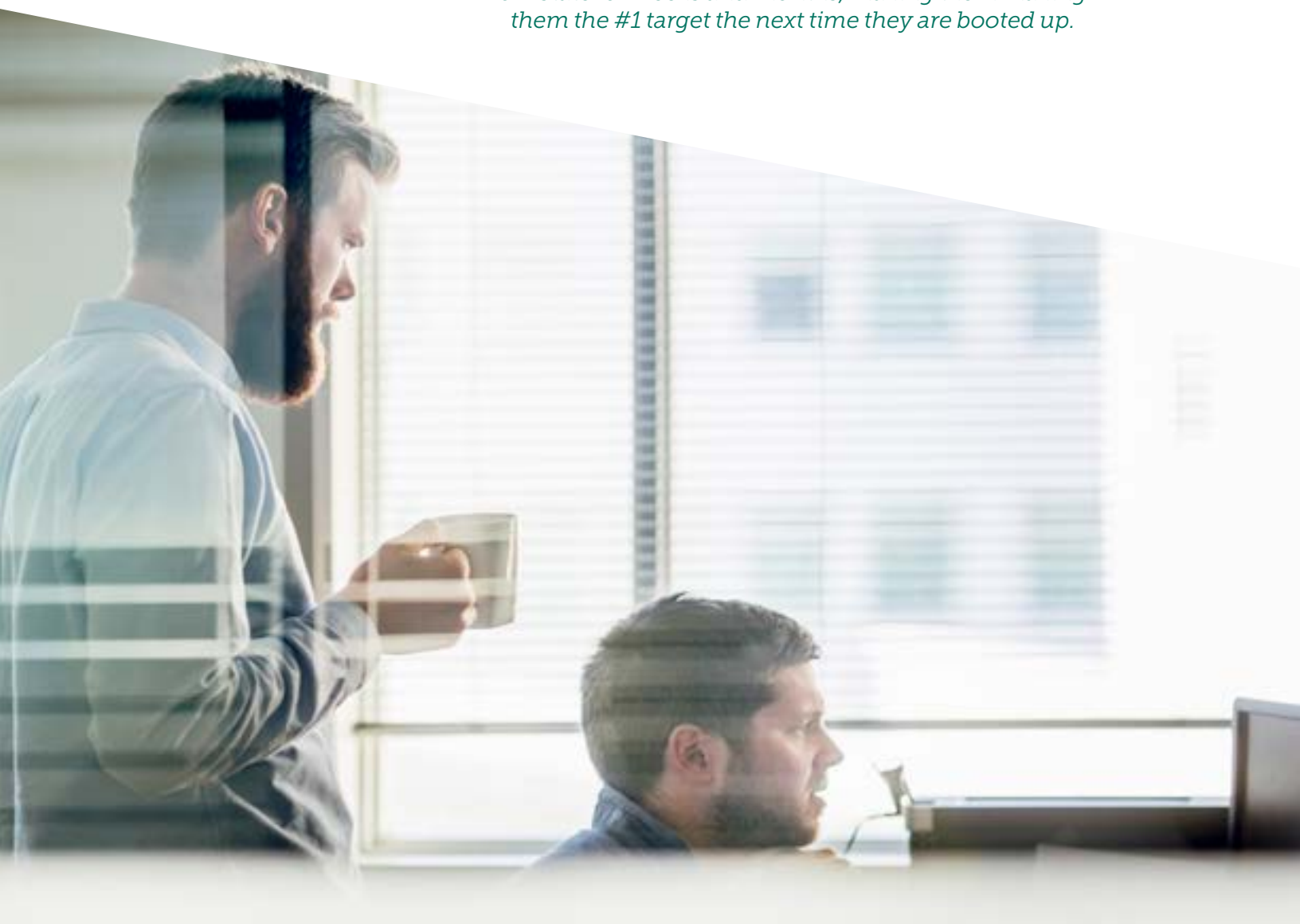
There are three options that exist for delivering security for virtual server and desktop environments.

Agent-Based Security

While many conventional agent-based security solutions are virtual-aware and provide excellent protection, they consume significant resources and very quickly become counter-productive when scaling virtual environments. Additionally, traditional agent-based security solutions may overwhelm resources when updating or scanning as well as create gaps in security when overdue updates need to be applied.

While this architecture offers advanced security options it creates inefficiencies that you should be aware of. An agent is deployed on each and every virtual machine (VM) in this host environment. Relying on this agent-based approach introduces inefficiencies related to agents deployed per VM creating excessive resource consumption. There is also the concept of scanning and update storms which occur when multiple VMs in a host environment simultaneously update the agent or scan files. Additionally, instant on gaps may occur when a non-persistent VM has been offline for some time. It won't have received updates while dormant and until an update can be applied to this machine it is more vulnerable. These things do not allow tight packing of VMs on a virtualization host and seriously lower the highest possible consolidation ratio.

Instant-on gap is the time between VM boot up and when an AV solution updates its database. Given VM procurement simplicity and as a result VM sprawl, some VMs may sit in off-state for weeks and months, making them making them the #1 target the next time they are booted up.



Agentless Security

Agentless security leverages a Virtual Security Appliance (VSA) that is deployed per host environment offloading the burden from the individual VMs.

There are two key functions available in agentless security. The first is file scanning which is delivered via vShield technology, authored by VMware®. In this architecture all files used by all VMs within the host are relayed to the VSA for scanning by means of vShield to ensure security. Also, importantly, this architecture ensures that a VM is instantly protected upon creation, vMotion or, in the case of a non-persistent VM, once it is re-activated.

The second function available with agentless security is a network attack blocker. It leverages a Network Security Appliance (NSA), which is similar to VSA but the NSA is deployed per cluster environment and relays all the network traffic between all the VMs sitting on this host. This feature requires an additional VMware license—vCloud®: Networking and Security. Through interaction among the NSA, the virtual filter and virtual distribution switch, network attack blocking functionality is efficiently delivered.

With agentless virtualization security, consolidation ratios are kept high. Also, this solution is extremely simple and fast to deploy and manage. The drawbacks are simple. It is for VMware environments only and, having been authored by a virtualization vendor, it lacks some of the advanced security functionality.

Light Agent Security

Light agent is a new approach for securing virtual environments. Through a combination of deploying a dedicated security virtual appliance, similar to that deployed in agentless security environments, together with a small software agents (Light Agent) advanced capabilities are available for each VM. Similar to the agentless architecture, a VSA is tasked with file scanning and keeping the security profile continuously updated. Similar to agentless security the VM is instantly protected upon creation or activation though interaction with the VSA. The light agent provides the more advanced security functionality including application controls, web and device controls, advanced proactive protection, firewall, HIPS, memory scanning and vulnerability monitoring.

These advanced security capabilities are not available in agentless security and represent an excellent security choice for environments with frequent internet interaction or those that are far removed from an organization's security perimeter. For example a VDI environment would be well served by a light agent security solution.

This architecture allows Kaspersky to deliver efficient virtualization-security solutions to the market for Citrix®, Hyper-V® as well as VMware hypervisor installations while maintaining the performance advantages of a virtualization-optimized solution. Light Agent's impact on the host performance is minimal and the consolidation ratios are comparable with an agentless solution.

What's Your Best Option?

The optimum approach for your organization – and the unique architecture of your IT infrastructure – will depend on a number of factors, including the level of risk you're likely to encounter, the value of the data that your systems store and process, the consolidation ratios that you're aiming to achieve, your organization's virtual environment (both your servers and desktops) and your virtualization hypervisor vendor.

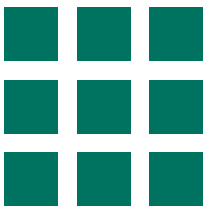
When considering security for virtualization, it's important to evaluate agentless solutions as well as light agent security solutions. For example, if you operate a VMware-based virtual environment, agentless security, which is today only available in VMware environments, can help you to achieve high consolidation ratios and significant ROI due to its ease of deployment and simple administration. In a tightly controlled data center environment – where servers are performing work that doesn't require them to be constantly connected to the Internet – an agentless security solution may provide adequate protection.

Citrix-based, Microsoft®-based or some VMware implementations may benefit from light agent products to provide efficient and comprehensive security that keeps consolidation ratios high. For some businesses, a mixture of both agentless and light agent security products may be appropriate. If you are using a non-Windows® guest operating system or you're running a less common hypervisor, a virtualization-aware full agent solution may be your best option.

In general, it's important to perform some due diligence and understand the options that exist. In most cases, security that's optimized for virtual environments is most desirable as it will offer the most attractive performance, consolidation and operating cost benefits.

At the end of the day, businesses need to remember the most important guide to virtualization security – make sure security is considered at the very outset of any virtualization project and that you understand the options that exist for securing these business-critical environments.

ALIGNING THE SECURITY APPROACH TO THE ENVIRONMENT

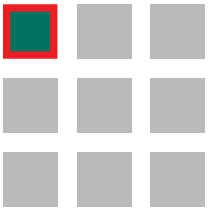


Traditional Agent-Based

> Works on any hypervisor

> Where VM density is not critical

> Windows, Linux® or Mac® guest VMs



Agentless Security

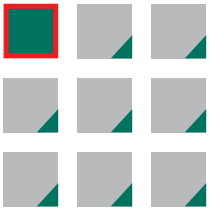
> VMware only

> Allows high VM density

> Windows guest VMs only

> Minimal IT resources for installation and management

> Typical installation would be server virtualization with controlled internet connectivity (no browsing)



Traditional Agent-Based

> VMware, Citrix, or Hyper-V

> Allows high VM density

> Windows guest VMs

> Advanced security requirements:

- > IM, Web and Mail AV
- > Automatic Exploit Prevention
- > Application, Web and Device controls

> Typical usage would be VDI and servers with critical roles

JOIN THE CONVERSATION

Watch us on YouTube


Like us on Facebook


Review our blog


Follow us on Twitter


Join us on LinkedIn


Visit Knowledge Center

ABOUT KASPERSKY LAB

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com, to learn more about Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.

KASPERSKY lab
THE POWER OF PROTECTION