Security for your private data center: Getting it right

kaspersky

Security for your private data center: Getting it right

The purpose of this document

The paradigm of building corporate data centers has changed significantly and is increasingly software-defined. Concepts related to virtualizing computing resources that have been successfully used over a number of years have also found applications in other industries – one example is the virtualization of the network infrastructure. Virtualization technologies have long since become a corporate standard (according to 2016 statistics, virtualization technology penetration reaches 75% in the corporate segment). The goal of this transition is to bring the management of a corporate data center to a level where it is driven by business processes rather than the infrastructure.

Naturally, all these changes require a review of protection policies for corporate data centers – it is essential to update such policies when upgrading data center technologies. If IT security cannot keep up with infrastructure changes or is unable to adapt to these changes quickly, you should think about replacing your data center's protection with dedicated solutions.

In doing so, remember that data centers originated from the idea of an efficient high-performance platform for achieving business objectives, so security solutions should never affect the performance of systems used in the corporate data center.

Kaspersky offers a dedicated Data Center Security solution engineered specifically to protect corporate data centers against the most advanced cyberthreats, while minimizing any impact on data center systems.

What is a corporate data center and why is protecting it so important?

"Over 75% of companies already work with software-defined data centers, and the virtualization penetration rate continues to grow year over year"

In the modern world, it is very hard to imagine an enterprise that does not need to process, store and transfer information. Today, all of this is done by corporate data centers. A corporate data center can be either private or public. It can be located on or off premises. In most cases, however, a data center is a much more complicated entity, which often combines public, private and geographically distributed infrastructure. A modern data center raises the company's operations to a new level by enabling the infrastructure to follow changes in business more quickly and to provide resources for newly emerging operational tasks in a more efficient manner.

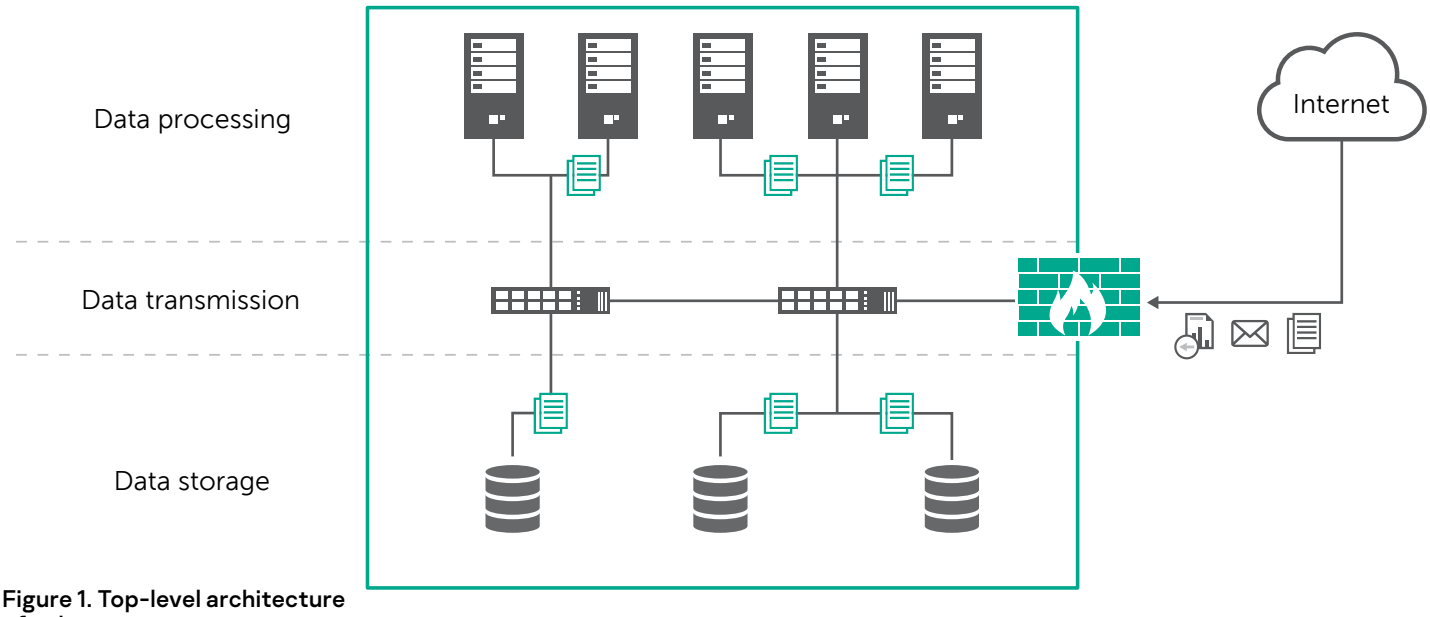


Figure 1. Top-level architecture of a data center

However, even though modern technologies are used to build corporate data centers, the ideology underlying the organization of their infrastructure remains largely traditional:

- **Data processing** — provides computing resources for business applications.
- **Data storage** — responsible for storing the company's data.
- **Data transmission** — helps to organize all the communications and data flows, without any problems.

All these components are essential for the efficient operation of any data center, regardless of whether it is public, private or hybrid.

Today, enterprises regard data centers as a tool with a reliable infrastructure and systems that can be flexibly scaled, with an invariably high level of performance and efficiency. They also have additional requirements for data centers: they need more resources, more control, more reliability, more operational efficiency and more security.

According to the latest studies and surveys, teams operating data centers face the following challenges:

1. The need to minimize risk and optimize security.
2. Avoiding performance issues as server SLA violation and service degradation can have both a direct and an indirect impact on the bottom line
3. Compliance challenges – a comprehensive approach is required to satisfy global and local regulations.
4. Audit-readiness ('show your work') and continuous audit – providing evidence through logging and reporting.

At the same time, as they are moving their business-critical systems to corporate data centers, companies increasingly face the fact that their existing IT security concept has to be revised, because it cannot be used to protect a modern data center.

"The security paradigm of modern data centers needs to be revised to take into account the technologies used by enterprises to build their own data centers."

Essentially, the problem is that the technologies on which modern data centers are built implement new user interaction scenarios and create additional interconnections between infrastructure components.

It should be emphasized that, although security is the main motivating factor for revising the IT security concept of modern data centers, things like maintaining system performance and convenient control of the entire infrastructure remain important issues for senior enterprise managers.

The most important things to protect in your data center

From an infrastructure viewpoint, a modern data center environment is a relatively simple combination of several systems:

- Data processing infrastructure, which is built using a virtualization platform, such as VMware vSphere, Microsoft Hyper-V, Citrix Hypervisor or KVM, with support for virtual servers and workstations.
- Corporate data storage infrastructure, which is most commonly organized as a combination of file servers and data storage systems that are connected directly to the corporate network.
- Network infrastructure, which enables data flows and interaction between data center infrastructure components and includes, among others, virtualized networks, e.g., those built using the VMware NSX technology.

All these components are involved in ensuring the data center's efficient operation. And, of course, the security of each of these components can be placed under threat.

"The tools used to ensure a data center's security should be 'aware' of the technologies they protect."

Kaspersky provides protection for each of the above components, tailored to the specific technologies used by data centers.

A modern data center is no place for heavyweight protection

Sometimes traditional solutions that are commonly used to protect physical servers and workstations are also deployed on virtual machines. However, when a traditional security solution is installed, it begins to consume resources and critical business applications get less computing power, slowing them down. This is inevitably noticed by users, inconveniencing them because they can no longer perform business tasks as quickly and conveniently.

"The idea of using virtualization in data centers is to achieve efficient utilization of resources, and IT security solutions should not be detrimental to this idea."

- As a result, **each virtual machine** performs tasks that are useful in themselves, but redundant at the virtualization host level: it stores antivirus databases locally and updates them, runs anti-malware scans and protects itself from network attacks.
- It would seem that this should provide reliable security for each individual virtual machine. However, this approach to protection results in excessive load on each VM, ultimately adding up to a **significant additional load on the virtualization host**, while reducing efficiency for the entire infrastructure and its users.
- When antivirus databases are simultaneously downloaded by virtual machines or scheduled scans are performed at the same time, this creates a very high load on the data center's infrastructure, resulting in **'update storms'** and **'scanning storms'**.
- Shutting down a virtual machine with a traditional antivirus solution installed on it results in antivirus databases becoming outdated, creating a **'window of vulnerability'** for new malware penetration and posing a significant threat for the security of the entire corporate data center.
- Moreover, the traditional approach is also useless for the protection of network storage systems and file servers, since it will not ensure the **security of all file operations**: protection is limited to scanning files downloaded to user workstations from data storage systems and does not protect network folders from **encrypting malware (including ransomware)**.

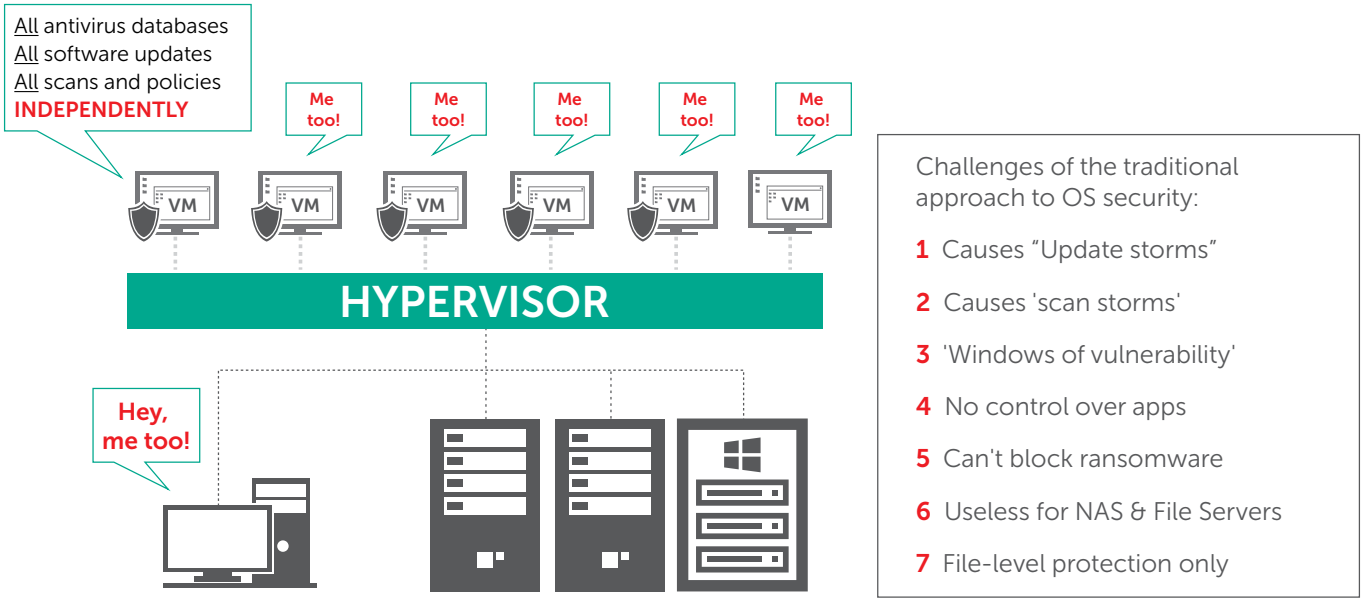


Figure 2. Shortcomings of traditional security solutions

The threat landscape in modern data centers

Traditional solutions, when deployed to protect virtual infrastructures, can damage these infrastructures even without malware, simply by significantly slowing them down and preventing IT systems from functioning normally, as well as making it hard for the company's employees to perform business tasks.

Research by leading IT security companies, including studies by Kaspersky, confirm that many of the existing threats are dangerous even for state-of-the-art data centers if their IT security measures are poorly implemented or non-existent.

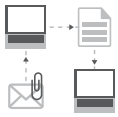
This is not because technologies used in modern data centers are not adequate for resisting threats. On the contrary, new solutions implemented in data centers are based on excellent ideas for ensuring the security of the infrastructure using, to give some examples, zero trust policies on firewalls and micro-segmentation methodologies. Nevertheless, data center protection against cyberattacks and malware should be based on dedicated solutions developed specifically for virtualized environments and data storage systems, capable of providing multi-tier protection for the entire data center.

The entire infrastructure needs new methods of protection

The infrastructures of modern software-defined data centers are increasingly sophisticated, bringing together a large number of systems designed to perform a variety of business tasks. The more varied the tasks, the more connections between systems and their users there are on different levels. Reliable protection of the entire infrastructure must be achieved without affecting performance and the business processes going on in the infrastructure. The most advanced technologies should work in the right place and at the right time, regardless of the complexity and scale of the data center's infrastructure.

Virtual machines sprawl

In very large infrastructures, it is difficult to control the changes in the number of virtual machines. Since virtualization enables virtual machines to be created using templates and cloning, neglecting security is inadmissible. Put more simply, replicating unprotected or infected virtual machines can lead to mass failures and serious losses for the enterprise. In addition, a lack of integration and gaps in protection lead to inadequate security and impair visibility and control.



Network-based attacks

Most network interaction in virtualized infrastructures takes place via virtualized networks, with network traffic and data streams rarely reaching the hardware designed to protect the corporate network infrastructure or its perimeter. As a result, neither expensive routers, nor security devices provide full control of your virtualized data center. A virtual network Intrusion Detection and Prevention System is a must for a modern software-defined data center.

Suspended virtual machines

Each time you suspend or pause a virtual machine, any traditional endpoint security solution installed on it immediately stops updating. After resuming operation, the virtual machine becomes the weak link in the IT security chain of your very own modern data center until it has successfully actualized the threat data. Moreover, you still need to keep an eye on powered-off virtual machines. They may contain malware dormant that waits until a VM is powered back on. You need a reliable solution that is capable of scanning any VM regardless of its current operational status.

Threats for VDI golden images

Desktop virtualization offers many advantages and improves efficiency. One golden image can be used to create hundreds of virtualized desktops in a matter of minutes. However, any damage or infection of the golden image can result in hundreds of vulnerable or compromized virtual machines being created, on which users may work with business-critical data. Also, you're unlikely to make friends with your VDI admins if you ask them to update 'golden images' every day, just because your security systems have been updated. For them this is a major resource-intensive task. Your security solution needs to have the right architecture to eliminate such a wasteful use of resources, while still delivering optimum protection to every VDI machine.

Data storage systems under threat

Most modern network-attached storage (NAS) devices, as well as popular file servers, offer extended data protection capabilities. What is needed is an additional solution designed specifically for critical data; preferably one developed specifically for data storage systems that will not degrade system performance. Moreover, you can never guarantee that traditional solutions will scan all files across your infrastructure. Something might be still hidden from endpoint security solutions on your business-users' PCs. You need a security tool that integrates with the storage device itself and can 'see' everything that travels to or from the storage – every single file operation regardless of its origin.

Excessive consumption of resources

The ideology underlying modern software-defined data centers is based on the principle of improving the efficiency of systems and achieving a high concentration of computing resources. Installing a 'heavyweight' security solution creates an enormous load on each virtual machine, significantly increasing the use of resources on virtualization hosts (hypervisors) as a result. This means that a poorly chosen security solution can easily destroy all the advantages that the business pursued in launching the project to build its own modern software-defined data center.

Protecting your modern data center

Kaspersky offers a dedicated security solution for modern data centers, which provides protection for both virtualized environments (virtualized servers and endpoints) and corporate data storage systems. From the outset, Kaspersky Hybrid Cloud Security and Kaspersky Security for Storage, component parts of the solution, were designed and developed to integrate with technologies used to build corporate data centers and to achieve optimal use of resources.

The solution's unique architecture was developed with the way modern data centers operate in mind, ensuring that it has minimal effect on system performance, helping maintain high consolidation ratios and thereby increasing the business efficiency of the corporate data center building project. An important advantage of the solution is its integration with the technologies used in the data center and centralized management from a single console – this helps system administrators implement security policies more quickly.

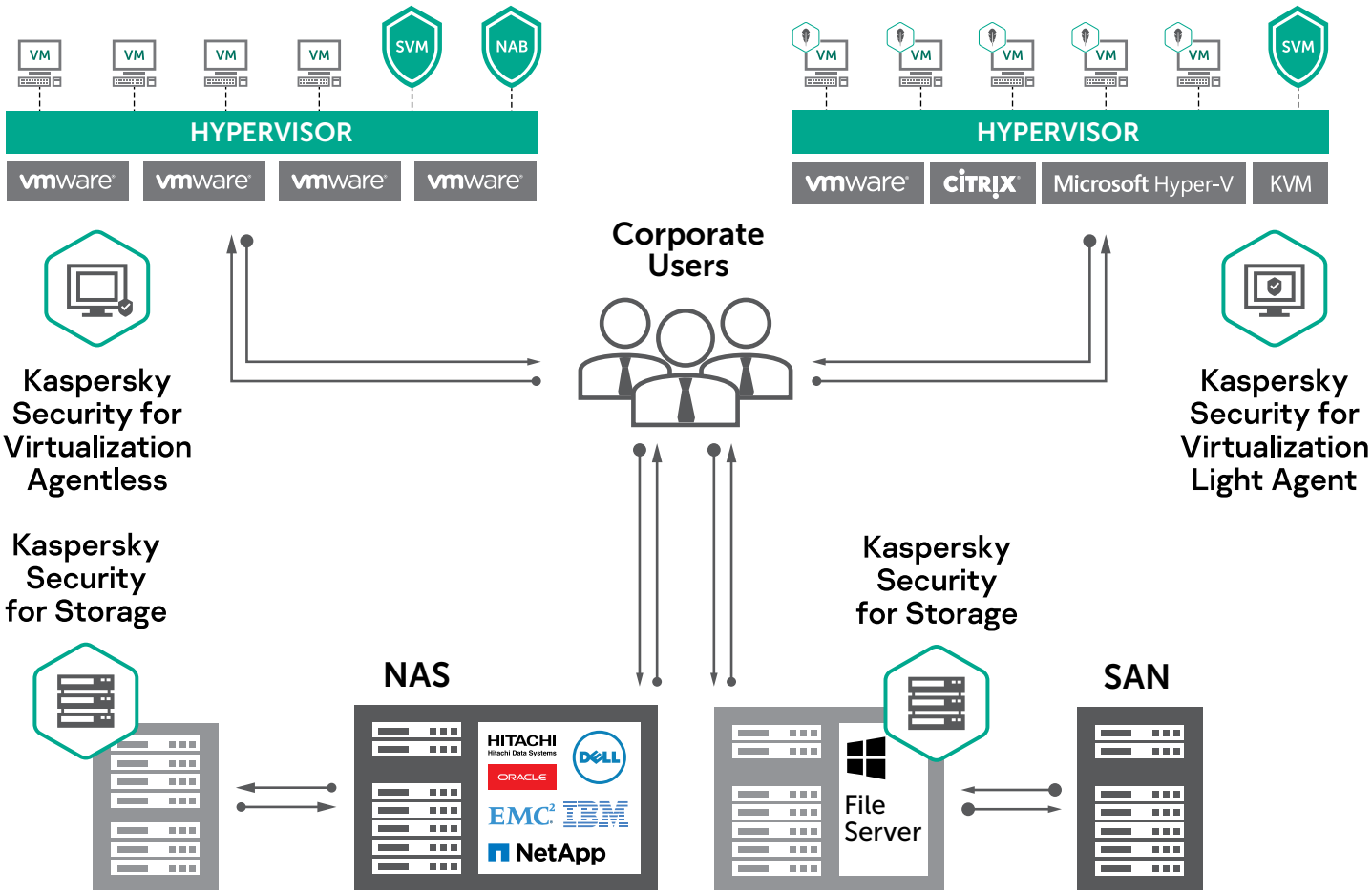


Figure 3. Architecture of the Solution

Security for Virtualization: Harnessing VMware NSX for vSphere

The VMware vSphere platform with NSX technologies reproduces the data center's network using a software-defined model, making it possible to create or reconfigure the network topology in a matter of seconds and quickly implement a data center security strategy based on the "zero trust" model. Kaspersky's solution leveraging VMware's security APIs makes the task of providing integrated protection for a modern data center's infrastructure easy to achieve.

Kaspersky Hybrid Cloud Security Agentless was specifically designed to protect software-defined data centers built on VMware technologies. Since no additional agent needs to be installed on protected VMs and the processes that are 'superfluous' for the virtualized environment are moved to dedicated security devices that provide file and network traffic scanning, the solution's impact on a software-defined data center's systems is minimal and each VM is protected immediately upon startup.

Built-in VMware NSX services	
Distributed Firewall	Virtual networks (VXLAN)
Server Activity Monitoring	VPN (IPSec, SSL L2VPN)
Kaspersky Hybrid Cloud Security	
Anti-malware	Virtual Network IDS/IPS
Security Automation	Policy Based integration
Security Tags integration	Full Infrastructure Scanning even for powered-off VMs

"Compared to traditional solutions, Kaspersky Security for Virtualization Agentless consumes 40% less VM memory and 80% less disk space. The result is efficient and secure operation of business systems."

The solution interacts with the VMware infrastructure via a dedicated API, providing not only protection against malware for each virtual machine and detection and blocking of network threats but also deep integration with the processes taking place within the infrastructure.

- **Automatic deployment** dramatically simplifies the work of IT and IT security staff, enabling full automation of security devices on hypervisors based on security policies defined for each VM.
- **Tight security policy integration** means that each VM now gets the protection functionality specified by the corporate IT security policy.

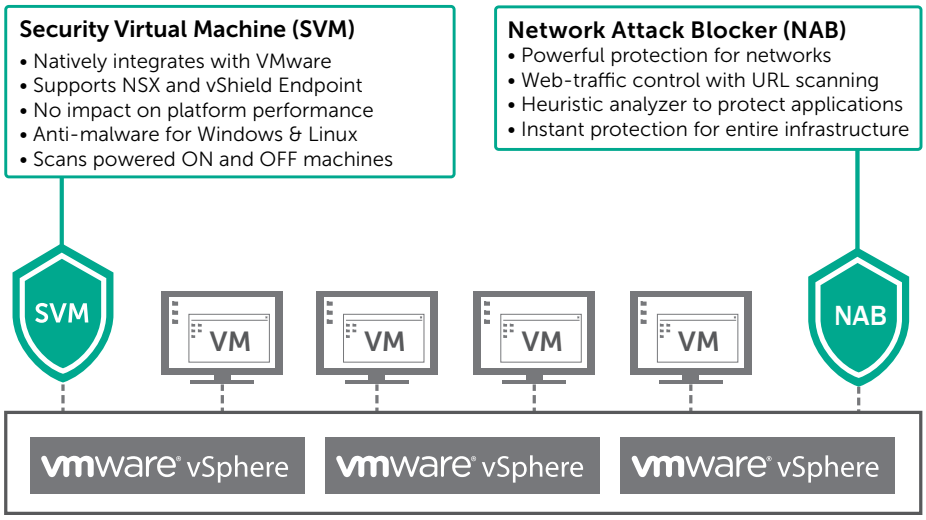


Figure 4. Agentless security solution

- **Integration with NSX Security Tags** extends the boundaries of 'communication' between the infrastructure and the tools that provide its protection, enabling the data center to respond, fully automatically and in real time, to IT security incidents, making management decisions and reconfiguring the network topology of the software-defined data center in seconds.
- **Both running VMs and those that are turned off are scanned** in a completely agentless mode, so the entire corporate data center is protected 24x7.

The solution's architecture was designed from the start to have a near-zero impact on the operation of business-critical servers while providing advanced protection.

Patented light agent technology

Some virtualized environments hosted in corporate data centers lack integration protocols that connect the infrastructure with its security solution, but ensuring the security of such environments is crucial.

Moreover, virtual desktop infrastructures (VDI) require technologies that provide each user with reliable protection regardless of how aware that user is of the relevant threats and prevention methods.

"The Light Agent controls program execution and protects virtual endpoints against encrypting viruses and other threats."

Kaspersky Hybrid Cloud Security Light Agent inherits the agentless solution's principles, while providing additional protection layers. The solution supports the most popular virtualization platforms, including VMware and NSX, Microsoft Hyper-V, Citrix Hypervisor, KVM, Proxmox, Huawei and Skala-R, as well as providing each virtualized endpoint with a balanced combination of completely new protection tools and technologies that preserve the performance of VDI platforms, such as VMware Horizon and Citrix Virtual Apps and Desktops.

- Kaspersky Hybrid Cloud Security Light Agent offers:
- Protection for virtualized Windows and Linux operating systems
- Anti-malware protection and IDS/IPS for virtual servers and VDI
- System Hardening, including Application Startup and Privilege Control
- Powerful yet lightweight security for Virtual Apps and Desktops and Horizon
- Works in harness with your infrastructure, empowering its capabilities.
- Perfectly balanced protection with no impact on performance

The dedicated protection server, called the Security Virtual Machine (SVM), provides centralized scanning of all VMs. At the same time, the Light Agent that is installed on each VM enables that machine's memory and processes to be scanned in addition to files. Deploying the Light Agent on VDI machines enables advanced security features to be activated, including Application Startup and Privilege Control, Device Control, URL Control, as well as heuristic modules that analyze email and Internet traffic. Moreover, the patented protection technologies on which the Light Agent is based provide virtual endpoints with protection against advanced attacks, including encrypting viruses.

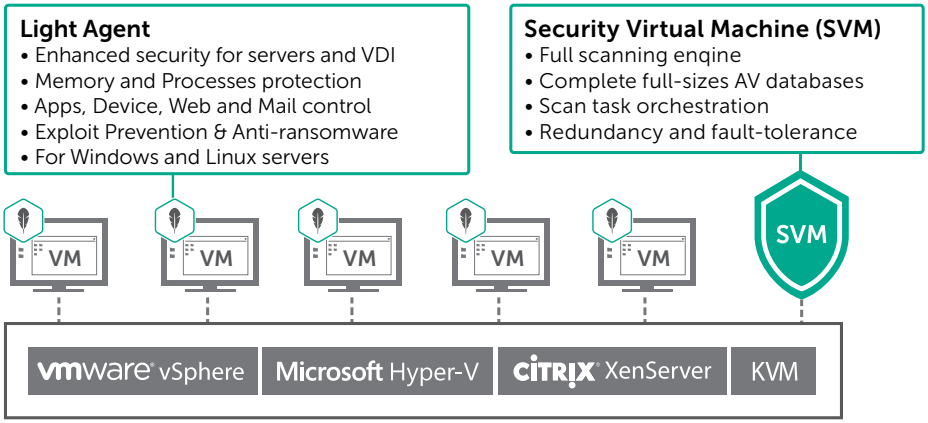


Figure 5. The Light Agent's operating principles

Protecting corporate data storage systems in data centers

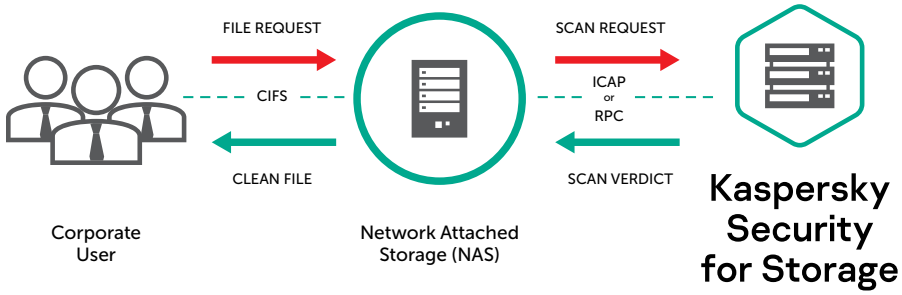
Even with the most advanced protection of endpoints – virtualized servers or workstations – issues related to protecting data, huge volumes of which are stored in modern corporate data centers, should also be addressed using dedicated protection tools.

Kaspersky offers Kaspersky Security for Storage, which is integrated with numerous corporate-level network-attached data storage systems via ICAP and RPC protocols, providing robust, high-performance and scalable protection for each file operation. The solution's architecture, combined with a high-performance engine, reduces to zero any potential risks related to possible malware infection of important corporate files.

"The security solution for storage systems works not only with network-attached storage systems but also protects file servers."

No matter which user performs which file activity – all operations will be processed by the antivirus engine of Kaspersky Security for Storage. The powerful antivirus engine developed by Kaspersky scans each file as it is launched or modified for all forms of malware, including viruses, worms and Trojans. Advanced heuristic analysis identifies even new and unknown threats.

The solution implements flexible scanning controls, with support for so-called "trusted zones" that can be excluded from scanning, together with certain file formats and processes, such as backup copying.



Summary

Kaspersky leverages award-winning anti-malware protection to secure every part of your software-defined data center, while preserving the highest levels of systems efficiency. The solution secures all leading hypervisors, including VMware vSphere with NSX, Microsoft Hyper-V, Citrix Hypervisor and KVM, and integrates with desktop virtualization industry standards – VMware Horizon and Citrix Virtual Apps and Desktops.

Complementing the dedicated security for virtualization platforms, we offer a solution to protect Network Attached Storage (NAS) and corporate file servers, ensuring that every single file activity, regardless of origin, is secured.

Kaspersky Data Center Security solution redefines how your data center's infrastructure and its security work together, combining strengths to create a secure, efficient virtualized environment. Thanks to its integration capabilities, Kaspersky Data Center Security solution brings advanced protection capabilities to your virtualized environment, addressing exactly how and where your data is stored and securing every individual file operation. So your corporate data center remains fully accessible and secure, 24/7.

Kaspersky Hybrid Cloud Security
Hybrid Cloud Security: kaspersky.com/hybrid
Agentless Security: kas.pr/agentless
Light Agent Security: kas.pr/light_agent
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

#virtualization_security
#hybrid

www.kaspersky.com