KASPERSKY lab

CAPTAINING DATACENTER SECURITY: PUTTING YOU AT THE HELM

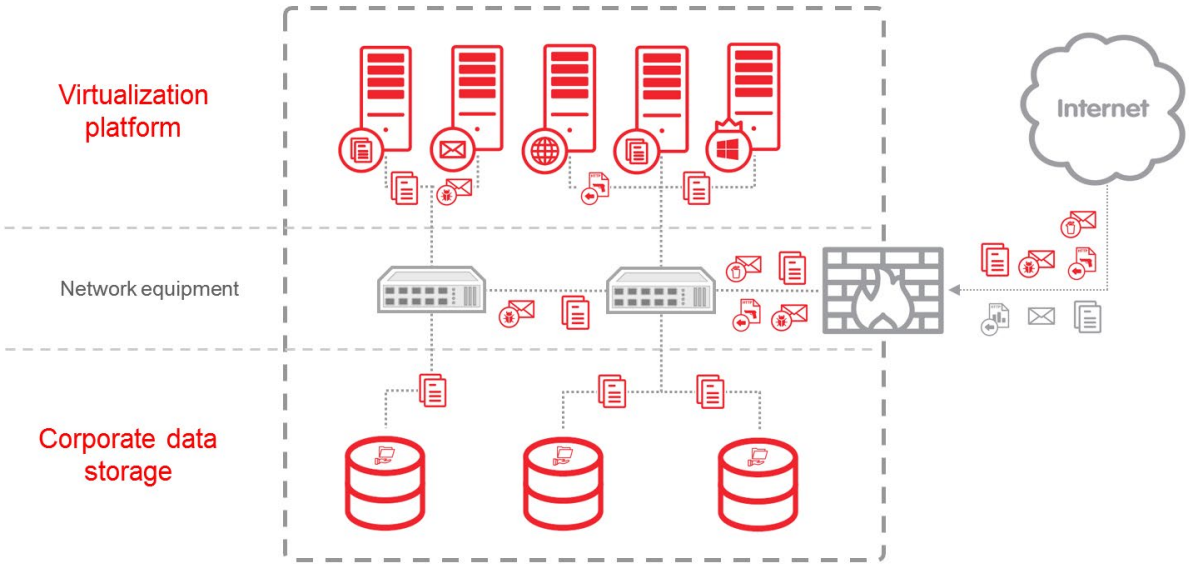
INTRODUCTION

Running a datacenter involves a plethora of complex tasks, of which security is just one. But the security of virtual environments and data storage in particular is critical to the modern datacenter. Securing these two areas is inherently challenging, and failure to address these challenges fully can result in unpleasant consequences, both for your clients and for the datacenter itself. Unfortunately, some issues are not that obvious, or just get ignored until it's too late. Let's take a detailed look at these issues, and what can be done to prevent problems from arising.

VIRTUALIZATION SECURITY: MISTAKES AND THEIR CONSEQUENCES

Virtualizing different corporate assets is a rapidly growing trend, delivering optimal resource consumption, greater flexibility and scalability. And many scenarios involving virtual infrastructure lend themselves to being handed off to the care of a datacenter. However, with datacenters undertaking wide-ranging activities, the security of hosted assets is too often out of scope.

There can be a number of reasons for this. Clients may feel more comfortable with their own traditional way of running their security, or may be reluctant to hand security management over to a third party. Or providers may themselves prefer not to take on responsibility for the security of hosted assets.



A datacenter provides its clients with different type of resources – which all have to be secured.

The consequences of such attitudes can be dire. "Running things as we used to" may result in a cacophonous 'zoo' of virtualization-agnostic security solutions owned by different clients, all running on the same host – or, even worse, the absence of any security solution at all. This absence may be justified by surprisingly persistent myths about 'virtual environments being inherently safe' and 'malware not running on virtual machines'.

The truth, of course, is quite the opposite: virtual machines (VMs) are subject to most regular forms of attack, and even offer additional vulnerabilities for exploitation. VDIs (Virtual Desktop Infrastructures), usually used in the just same way as their physical counterparts (including access to the Web and all its dangers), are especially susceptible to infection. In no time at all, unprotected vulnerabilities can lead to a malware outbreak, which can affect not just the client initially attacked, but others whose assets are held on the same host. A sudden increase in resource usage triggered by an outbreak can result in lags, and can even crash of the whole host – particularly annoying for uninfected clients involved.

One specific virtualized infrastructure in the datacenter may even be used as a jump-off point for further attacks, causing whole IP address ranges to become banned, attracting the attention of the authorities and thoroughly disrupting the smooth functioning of the datacenter.

Installing virtualization-agnostic security solutions onto virtualized endpoints, however, can create its own problems.

These include:

- Excessive resource consumption, with each protected machine carrying complete sets of replicated components: a scanning engine, a local signature database, a Host-based Intrusion Prevention System etc. And if cloud-based threat data feeds are used, each will also require its own bandwidth share.

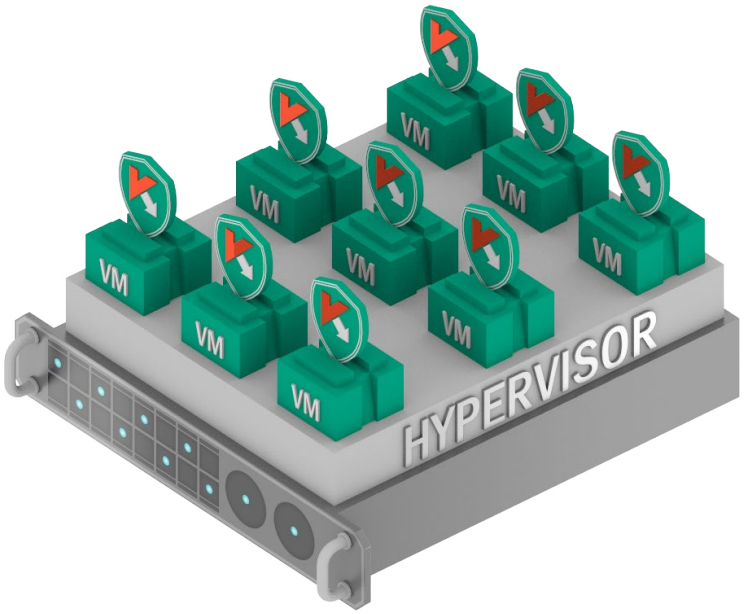
- Unpredictable surges in resource consumption known as 'storms' - induced by the simultaneous execution of similar tasks, such as updating or file system scanning, on a number of VMs. This can result in serious lags, or even denial of service for the whole host machine.

- Panic attacks: malware outbreaks often induce a switch to "paranoid' mode, triggering out-of-schedule scans, increased scanning depths etc. The resulting decrease in performance can affect all the VMs hosted on the same server.

- 'Instant-on security gaps': some VMs can stay dormant until their services are required. In this state, they cannot be updated (which includes vulnerabilities patching and security solution updates). So immediately after boot-up, the machine remains vulnerable until it is fully updated – easily time enough to contract an infection.

- Incompatibility. While VMs are similar in many aspects to their physical counterparts, they differ in some ways. Virtualization-agnostic security solutions are not designed to work with, for example, dynamically assigned virtual storages or VM migration - which can lead to glitches or to more serious faults.

It is crucial to recognize that the service provider would ultimately be held responsible for the consequences outlined here – the fact that you have no control over hosted resources is not a defense. The more so because there ARE ways of taking things under your efficient control in a virtualized environment.



1. Causes "Update storms"
2. Causes "Scan storms"
3. "Instant-On gaps"
4. Excessive resource usage
5. Lowers VM density
6. No security for network resources

Using virtualization-agnostic protection creates multiple problems – starting from inefficient use of resources.

The answer is to use specialized security solutions, specifically designed with virtualization in mind.

USE PROTECTION DESIGNED FOR YOUR NEEDS

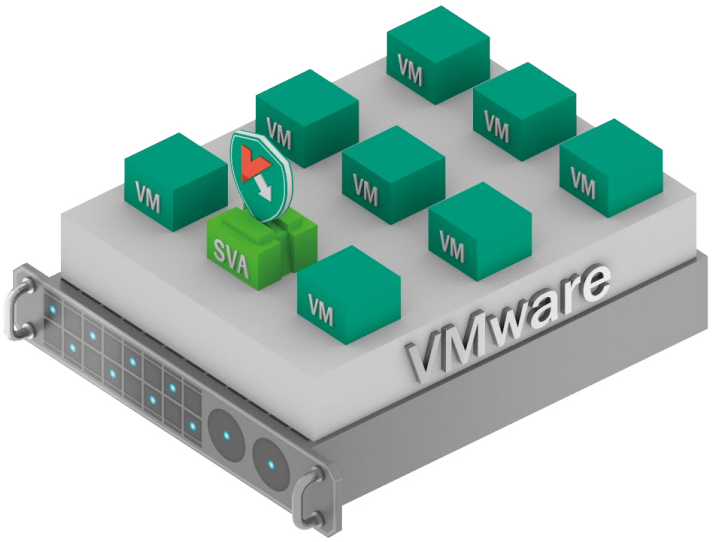
Kaspersky Security for Virtualization was designed with a full understanding of virtual infrastructure specifics and built by us to naturally fit into such environments, avoiding issues generated by inadequate, inefficient or inappropriate solutions.

First, redundancy resulting from having identical components on every single VM is eliminated. A dedicated VM called a **Security Virtual Appliance (SVA)** carries both the scanning engine and security database centrally, protecting every VM running under the same hypervisor. This updates continuously and uses smart scheduling techniques to manage scanning, so avoiding storms.

Of course, the SVA does have to reach into every protected VM. Kaspersky Security for Virtualization provides two different ways of doing this:

Agentless

This option works only in VMware-based environments. As the name implies, it doesn't require the installation of any software agent into the VM, but instead uses native vShield technology. With this Agentless option, **every VM receives protection automatically**, from the moment it spins up, while an additional SVA provides network **Intrusion Prevention System (IPS)** functionality.



Agentless solution allows instant protection without the need to install anything to VM

This agentless approach makes the perfect choice when protecting clients who are sensitive about letting alien software inside their machines, or who run only a strictly defined set of apps. And in situations where clients are unwilling to use ANY security solution, this may be the only way to avoid gaping security holes.

However, there are some considerations to be addressed. Agentless technology does not allow the security solution to survey processes running inside the VM's memory: vShield technology only allows access to machines' file systems, limiting the effectiveness of protection against sophisticated malware (e.g. bodiless variations).

It is also not possible to implement additional proactive security layers such as Application, Device or Web Controls. So for some scenarios, such as the increasingly popular Virtual Desktop Infrastructures (VDI) now replacing physical workstations, we recommend using another option offered by Kaspersky Security for Virtualization: protection with Light Agents.

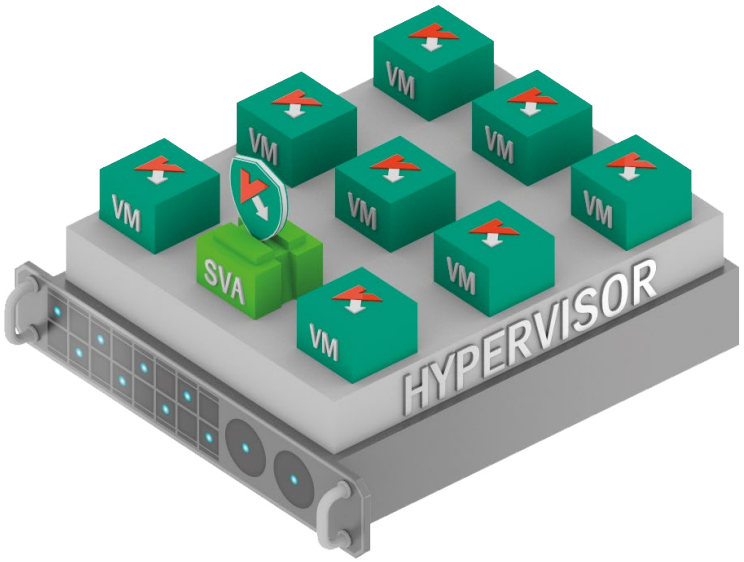
Light Agent

Unlike Agentless security, this option doesn't rely on a **platform-dependent intermediate layer** – so can work with a broader range of hypervisors, adding Microsoft Hyper-V and Citrix to the supported list. This is possible through using a **lightweight software agent** deployed into the protected VM. The presence of these agents not only allows the SVA anti-malware engine to reach into protected machines, but also provides for a much broader range of protective technologies, raising the level of security to the **equivalent of a full-scale endpoint protection solution**, such as Kaspersky Endpoint Security for Business.

Among other options, Kaspersky Security for Virtualization | Light Agent provides:

- Control over processes in the VM's memory, using advanced behavioral mechanisms
- Exploit mitigation through Automatic Exploit Prevention technology
- Web antivirus with cloud-supported anti-phishing
- A full set of security controls, which help explicitly define the set of applications, web resources or even external devices allowed on individual VMs.
- Network protection enhanced with network attach blocking mechanisms and advanced firewalls and monitors allows ensuring help level security for each virtual machine operation within virtualized networks.

For all this power, the agent remains very light- the SVA still handles updates and scan management, eliminating redundancies and keeping agent-based activity at the VM to a secure minimum.

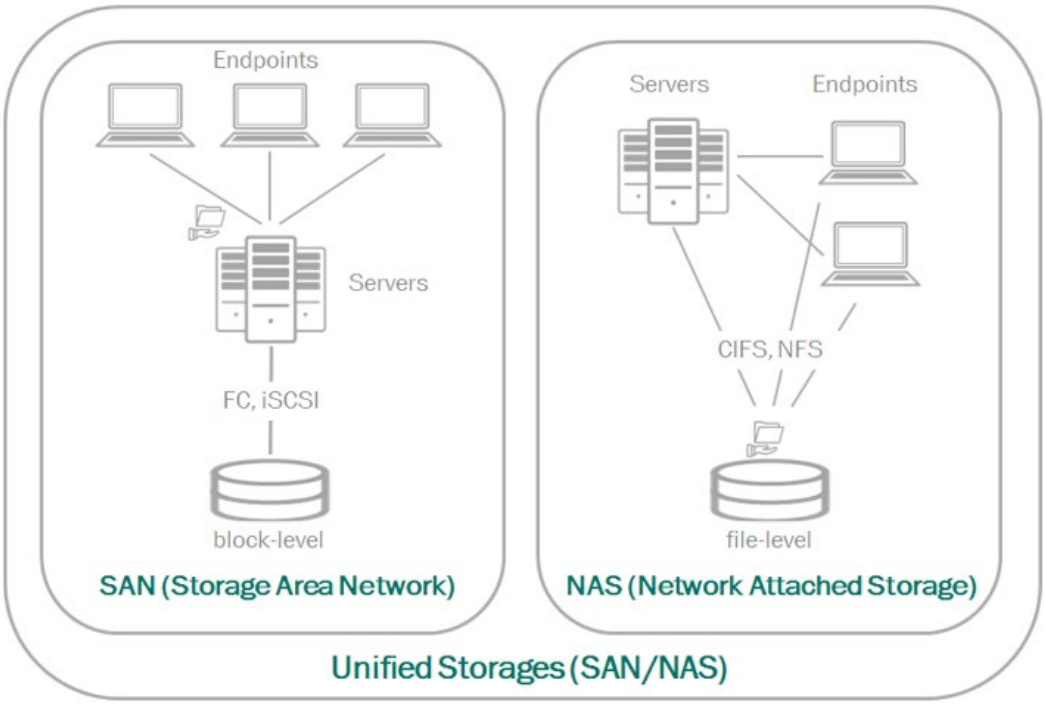


A solution with Light Agents provides advanced protection using lightweight apps to see into VMs. These apps can be pre-installed to VM images.

For scenarios involving higher risk and broader potential attack surfaces (e.g. virtualized desktops with full Internet capability), such multi-layered protection is a must – and not only because of the greater chances of an attack. As virtualized networks are so much more efficient, infection can spread lightning-fast, giving attackers control over a whole poorly protected infrastructure in no time at all. On the other hand, a well-defended virtual infrastructure makes a less attractive target, even for targeted attack operators in search of easy gains.

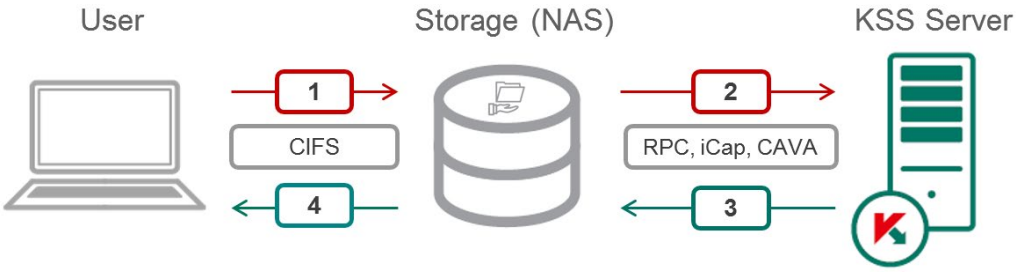
SECURING DATA STORAGE – VIRTUALIZED OR NOT

When considering datacenter security, data storage must not be overlooked. Vast volumes of data are stored, updated and shared – a potential source of danger to hundreds of users should just one user be careless or even ill-intentioned. it's also worth bearing in mind that users may be located outside the protected perimeter - the datacenter has absolutely no power over, or even information about, their security stance. So special measures should be taken to secure different types of data storage, especially if not all are virtualized and protected by a virtualization-specific security solution.



Different types of storage equally require protection

While **Storage Area Networks (SAN)** are fairly straightforward to protect (as they are only accessible via servers), securing **Network-Attached Storages (NAS)**, directly accessed by network users, is more complex.



Protecting NAS is more complicated than SAN

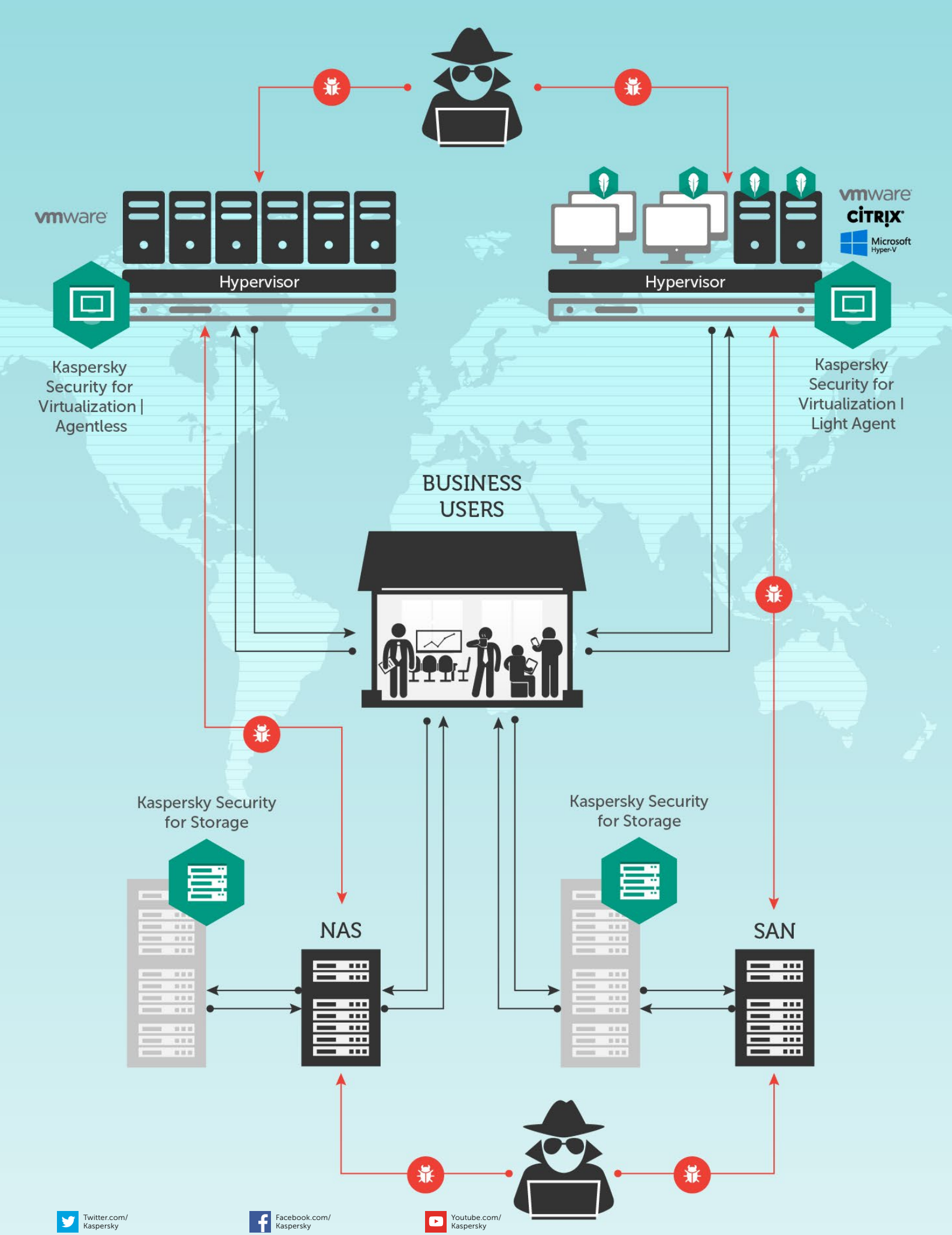
Fortunately, there are specialized security solutions that can provide protection for both; a good example is Kaspersky Security for Storage. SAN resources are secured just as with regular file systems, but, every object sent to – or requested from – NAS based data storage is first checked by the Kaspersky Lab solution. On the basis of the solution's verdict, the NAS can grant or deny permission to complete the requested action. To cope with more intensive data streams, several instances of the solution can be deployed, with the load balancing managed by the NAS itself.

ONE CONSOLE TO RULE THEM ALL

With the growing number and sophistication of modern cyber-attacks, it's important for the datacenter security helmsman to have a comprehensive view of the entire infrastructure, ensuring timely awareness and effective threat counteraction. And here, Kaspersky Lab solutions deliver a further advantage: all security is monitored and managed through one flexible, single-pane-of-glass console - Kaspersky Security Center. And optional role-based access means you can offer your clients the opportunity to manage their own security status if required, without compromising on overall datacenter security.

CONCLUSION

Whether you're dealing with virtualized or physical assets, Kaspersky Lab's Security Solution for Data Centers (part of our Enterprise Security Platform) offers a convenient way to transform IT security into an attractive – and profitable – option as part of your portfolio of datacenter services. But one thing is absolutely clear: taking the helm of your datacenter's security into your own hands is key to surviving any upcoming storms.



Twitter.com/ Kaspersky

Facebook.com/ Kaspersky

Youtube.com/ Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab