kaspersky BRING ON THE FUTURE

Kaspersky Hybrid Cloud Security

Balanced security for server virtualization and VDI

A traditional agent-based approach to security in a virtualized environment creates competing conditions for VMs vying for hypervisor resources. The resulting degradation of service has a direct and an indirect impact on the bottom line - requiring more hardware/compute, slowing down operations, hurting revenues, and negatively affecting the company's image. When agents compete for resources to protect virtual desktops, it's the users who feel the pain... Kaspersky Hybrid Cloud Security delivers measurable performance benefits while providing the latest security technologies and multi-layered protection for virtual servers and/or VDI in hybrid environments. This is achieved by designating a dedicated Security Virtual Machine (SVM) to maintain the malware databases and issue file threat level verdicts to all the VMs on the host.

The solution supports a wide range of **server virtualization and VDI platforms**:

- VMWare vSphere, NSX, Horizon
- Microsoft HyperV
- Citrix Hypervisor, Virtual Apps and Desktops
- KVM
- and others

Light Agent security for VMware, Hyper-V, Citrix, KVM and more

Native API integration with leading virtualization platforms and patented architecture simplifies deployment, ensures consistent visibility and control and closes security gaps.

Up to 30% reduction in virtualization resources use

Light Agent significantly reduces the 'security tax' and through a number of smart optimizations, such as shared caching and the elimination of redundant information, is able to cut the amount of data and number of operations needed. This dramatically reduces IOPS, CPU cycles, memory and disk footprints, which helps to achieve high consolidation ratios and protect investments in virtualization projects.

Efficient protection for VDI

Kaspersky Security for Virtualization Light Agent was designed with VDI in mind. It leverages patented architecture to ensure linear scalability as the load on virtualization hardware increases. Simplified procurement and native support for Golden Image allows to dynamically spawn virtual desktops as needed. Flexible licensing allows for gradual migration from physical machines with roll-backs as needed making Kaspersky Hybrid Cloud Security ideal companion for VDI roll-out project and beyond.

System hardening and multi-layered security

Rich and flexible system hardening drastically reduces the attack surface, eliminates arbitrary code execution on servers and blocks exploits. Memory and data control algorithms defuse ransomware attacks, both host and network-borne. Kaspersky Hybrid Cloud Security ensures a secure and responsive VDI environment, allowing users to focus on their work without risk of becoming a victim of cyberattack.

Single pane of glass management console

Kaspersky Security Center is the single pane of glass management console that takes the complexity out of security administration and IT systems management. Fully scalable, the console supports digital transformation and facilitates comprehensive security management, with easy separation of administrator responsibilities. The rich reporting tool enables a continuous audit of physical, virtual and public cloud infrastructures.

Native integration with leading Virtualization Platforms

Native API integration simplifies deployment, streamlines daily administration routines and ensures consistent visibility and control. The single pane of glass management console provides the means for efficient orchestration of physical, virtual and public cloud workload security.

Features

Protection for Linux and Windows Servers

Kaspersky Hybrid Cloud Security is the ideal solution for hybrid data centers, delivering advanced security capabilities to virtualized Windows and Linux server workloads.

Supports the rapid provisioning of VDI machines

Kaspersky Hybrid Cloud Security fully supports linked and full cloning. Thanks to the pre-installed lightweight agent, provisioning a new VM involves simply cloning a template. Once cloning is complete, the new machine is automatically protected by the SVM. This simplifies VDI management, eliminating the need to update security products on the VDI image.

Shared Cache – eliminating redundant operations

Virtual environments – especially VDIs – often include many similar VMs, each containing identical files. Full agent-based solutions waste time and resources running multiple scans of the same file on different VMs. Kaspersky's Shared Cache feature shares the results of file scans, which minimizes the overall load on the IT infrastructure.

Exploit Prevention

To deal with the risks from exploitation of unpatched vulnerabilities, Kaspersky Hybrid Cloud Security incudes a range of Exploit Prevention technologies. The Exploit Prevention mechanism monitors the most frequently targeted applications – including Office applications, Web-browsers, Java, Adobe Flash and many more – delivering an extra layer of security monitoring and protection against unknown threats.

System, vulnerability and patch management

Streamlining and centralizing admin tasks with:

- Advanced in-depth scanning for vulnerabilities, and automated patch distribution
- Hardware and software inventory reports - helping control software license obligations.

Application Control

Configurable Application Control allows you to specify which applications are allowed to run on which VMs. This reduces exposure to risk and wasted resources due to running unnecessary software. This is also the single computationally cheapest and most effective security measure that, combined with Exploit Prevention, presents the biggest challenge to an attacker.

SVM failover protection

The solution is designed so that Light Agents can use a SVM on another host if the local SVM in unavailable or overloaded. This eliminates single points-of-failure in infrastructures of any size. If there's significant stress on the virtualized infrastructure, the Light Agents can locate and reconnect to the optimal SVM almost immediately. This ensures uninterrupted real-time protection for the entire virtualized environment.

Silent Mode for maximum performance gains

The user interface can be completely disabled (by unloading it) on any or all VMs for additional performance optimization..

Host-based Intrusion Prevention System (HIPS) and personal firewall

HIPS – working together with Kaspersky's two-way firewall – controls inbound and outbound network traffic. Flexible tools enable granular control over security according to a policy containing a wide range of parameters, including settings for particular ports, individual IP addresses or specific applications' network activity.

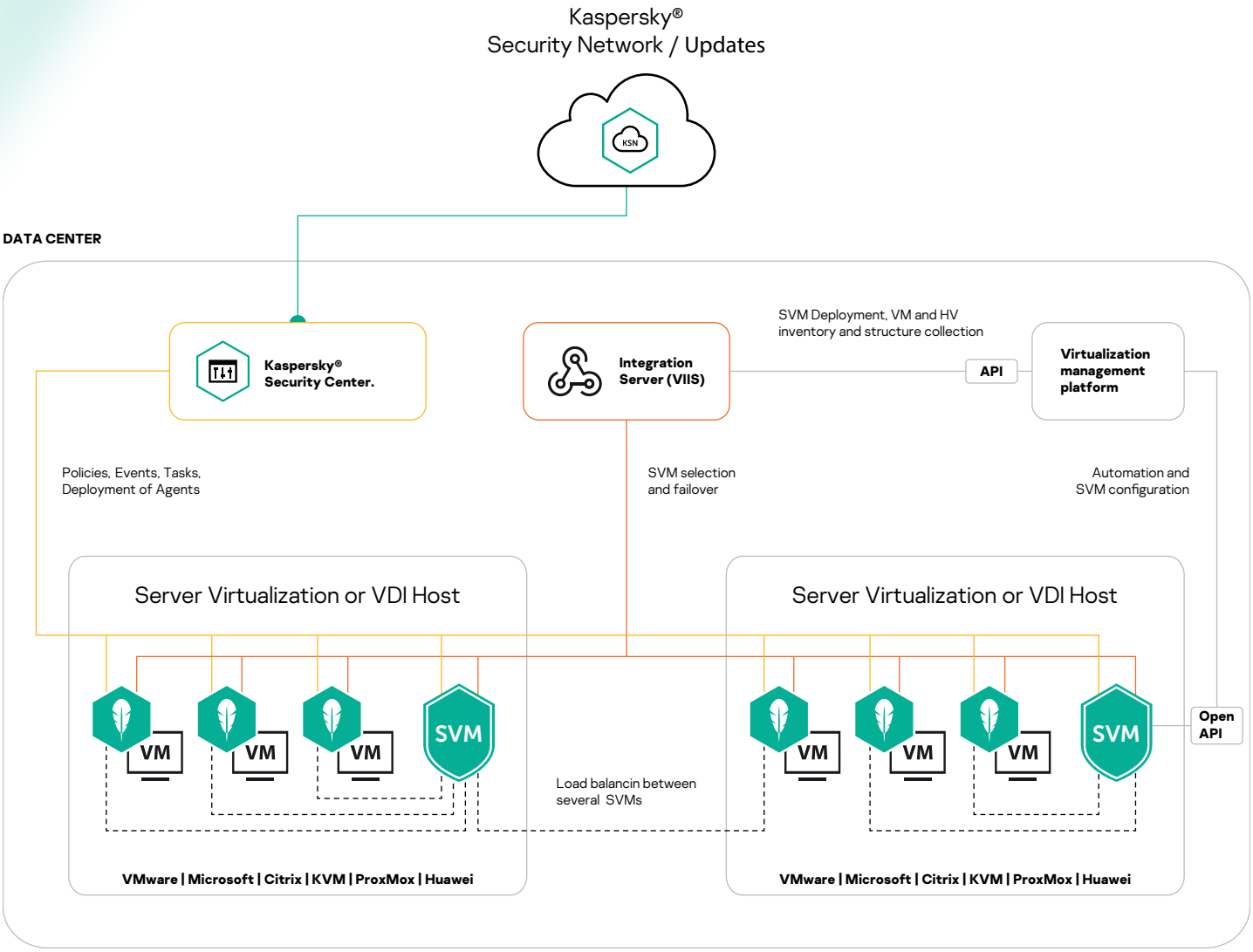
File Integrity Monitoring

The Integrity Monitoring component helps track changes in files and registry as well as on hard drives, optical drives, USB devices and external network adapters. Integrity Monitoring can operate in real time, by schedule or on demand.

Large scale and complex network architecture support

Kaspersky Hybrid Cloud Security deploys and operates seamlessly in complex enterprise infrastructures that run multiple logical networks on different hypervisor hosts and platforms. The Protection Server can be deployed and configured via the virtualization platform's own API.

After the protection server is deployed, security administrators can automate the rollout of security agents and optimize infrastructure protection. SVM discovery and selection are optimized for largescale environments.



Kaspersky Hybrid Cloud Security is just one in a range of products and solutions from Kaspersky, originated in-house, drawing on 20+ years of expertise, built from the same code base and designed to work together seamlessly to provide a comprehensive and reliable security platform.

If you are already using any of Kaspersky's security solutions, such as Kaspersky Endpoint Security for Business, choosing Kaspersky Hybrid Cloud Security protects investments devoted to building administration and security expertise and leverages existing management servers and policies to ensure that there are no security gaps in your entire hybrid infrastructure.

Kaspersky Hybrid Cloud Security works best when it is deployed as part of a multi-layered all-encompassing organization security safeguards, that includes:

Kaspersky Endpoint Security for Business — combines multi-layered security with extended control tools to deliver an agile solution for businesses of every size. The unified security and systems management console for Hybrid cloud environments and endpoints drives efficiency, while extra layers of defense help eliminate vulnerabilities and further safeguard sensitive data.

Kaspersky Endpoint Detection and Response — advanced endpoint protection that provides comprehensive visibility across all endpoints on the corporate network, enabling the automation of routine tasks in order to discover, investigate and respond to advanced threats and targeted attacks. The result is a significant increase in the speed and effectiveness of complex incident processing, at no extra cost.

Kaspersky Maintenance Service Agreement — when a security incident occurs, rapidly detecting and solving an issue can save businesses hundreds of thousands of dollars. You need round-the-clock access to security experts, appropriate and informed issue prioritization with guaranteed response times and private patches – and that's precisely what Kaspersky Maintenance Service Agreement provides.

How to buy

Kaspersky Hybrid Cloud Security is sold as a stand-alone solution and can be purchased through a Kaspersky partner.

Applications inside

The capabilities described in this datasheet are delivered by Kaspersky Security for Virtualization Light Agent application, which is a part of Kaspersky Hybrid Cloud Security solution designed to protect physical and virtual servers and desktops, public cloud instances and provide security and integration interfaces for DevOps.

Licensing

Kaspersky Security for Virtualization Light Agent is a part of Kaspersky Hybrid Cloud Security that is licensed either per Virtual Machine (server or desktop) or per CPU. The latter option offers greater flexibility for dynamic datacenters.

Try Before Buying

Kaspersky Hybrid Cloud Security now with our free 30-day trial.

Request a Call

Still feel you need more information? Request a call to clarify everything you require!

Buy Via a Trusted Partner

Feel like you are ready to buy? Find a reseller in your geography to help you with your purchase!

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for Enterprise: kaspersky.com/enterprise
Kaspersky Hybrid Cloud Security: www.kaspersky.com/hybrid

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.