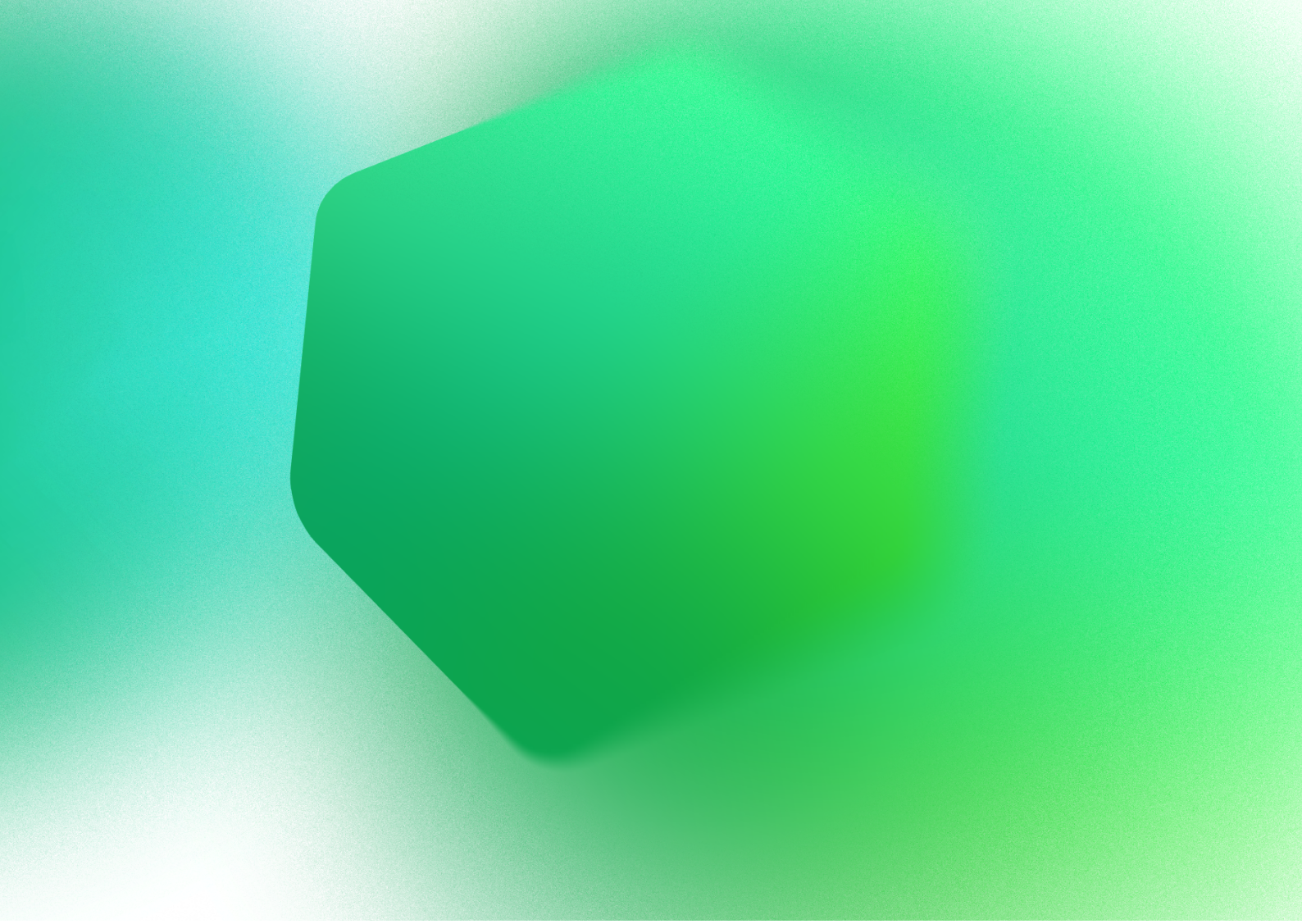


Protection where you need it: securing your move to the cloud

kaspersky

Learn more on kaspersky.com

Digital transformation – changing the face of corporate it

As enterprises embrace digital transformation and build their infrastructures out into the cloud, there are some very real fights to be had. Can you retain control over your corporate assets – or will it be wrested from you? How will you close integration gaps and eliminate boundaries, so you can harvest the benefits of the move? And how can you minimize performance impact during these changes, while being sure you're maximizing the return on your substantial investment?

Digital transformation takes many forms. Building new IT functions in the cloud from scratch. Migrating existing servers or applications. Facilitating the de-commissioning of old hardware by moving over to the cloud. Enabling service auto-scaling, enabling fast-changing work-styles - and so on and so forth.

Moving into the cloud: more relevant than ever right now

The reality is that we've only just begun to tap into what cloud adoption may mean for us all.

During the 2020 Coronavirus outbreak, and the resultant mass-movement into remote working, public cloud providers have been able to meet the surge in demand without apparent effort, spinning up nodes at breakneck speed. Working from home has also demonstrated (as if we didn't already know it) just how reliant all aspects of corporate life are on uninterrupted online access and communications, and just how easily (or not) we can manage our infrastructures with no physical access to the hardware layer. Businesses who had already achieved cloud adoption have really felt the benefits during this latest crisis, with cloud providers being hailed as 'unsung heroes'[1]

Another technology that has shown an instant increase in traction during the pandemic is VDI. Many businesses have found themselves unable to procure the laptops and computers needed to provide all employees with the necessary equipment for remote working, and have had to ask their workforces to work from their own devices. Those who had pivoted and rolled out VDI have been able to operate in a secure and controlled way, while allowing their employees to work from a variety of devices. VDI also provides a multitude of backup options should a device stop working – you can resume work nearly instantly from any other available device.

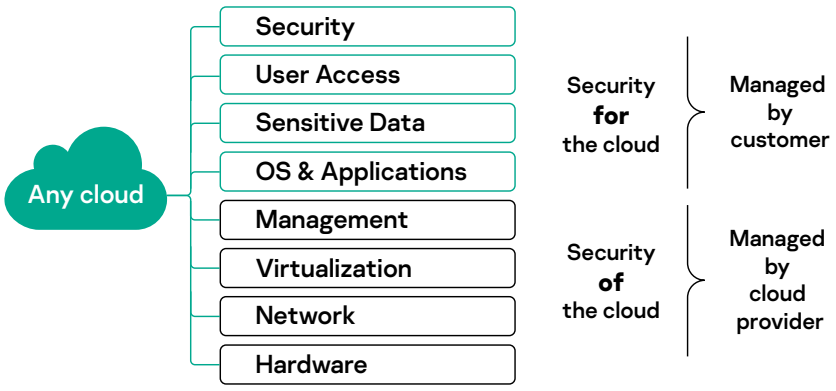
With cloud-based working having demonstrated clear benefits it terms of business continuity and resilience during challenging times, it's almost inevitable that the vast majority of businesses will transition at some future point. And the process of evolving with and into the cloud will very probably result in an intermediate stage, where we're working with a complex heterogeneous hybrid infrastructure spanning physical, virtual and cloud platforms - which must be managed, fine-tuned and supported, all at the same time.

When your infrastructure is suddenly not on your network

There was a time when we, as our own network builders and owners, could run a discovery tool that would create an inventory of our workstations, servers, services and applications. And that was relatively easy, because we had control over our own network. We could trace a cable. We could dig into hypervisor settings to figure out the extent of our software-defined network.

In the world of IaaS, we don't have that luxury more - and this is a good thing. We can relax - the hardware layer is no longer our responsibility. It's up to the IaaS provider now.

Shared Security Responsibility Model



1 https://www.crn.com/news/cloud/in-coronavirus-crisis-public-cloud-is-an-unsung-hero-

With all that responsibility gone, control and, alas, visibility are gone also. The old way of doing things is still possible – you can VPN-stitch different parts of infrastructures together and treat your cloud IT-assets in almost the same way as you treat your virtualized workloads. But the thing is – more often than not you don't really want that, because each time you choose the old way over the new, you also decline the benefits of the new approach.

New tools for new realities

And here's a dilemma. Old tools don't work well with hybrid infrastructures. And the new tools focus on migration aspects, too often treating workload security as a post-migration issue. The only option for most of us is just to use different security tools for the different parts of the infrastructure. The result – the sprawl of domains of responsibility, visibility gaps, control failures and eventually those security gaps that cybercriminals love so much.

To enable digital evolution, the tools you use need to change and adapt to the new realities and function usefully across numerous platforms, wherever these may be – on premises, physical or virtualized, or 'in the cloud' – a term we've got so used to, but which for most people still means 'on someone else's computer'.

Consistent visibility across all workloads

Here at Kaspersky, we think about security gaps almost as much as about the threats that utilize them. Arguably, the inability to control, enforce policy and ensure configuration uniformity across all of your infrastructure is a bigger danger than a vulnerability in your operating system or line of business application. Vulnerabilities in software can be fixed by the software vendor or your security vendor. But who's going to spot a difference in settings on multiple security management consoles, that's created a convenient entry-point for an interested attacker?

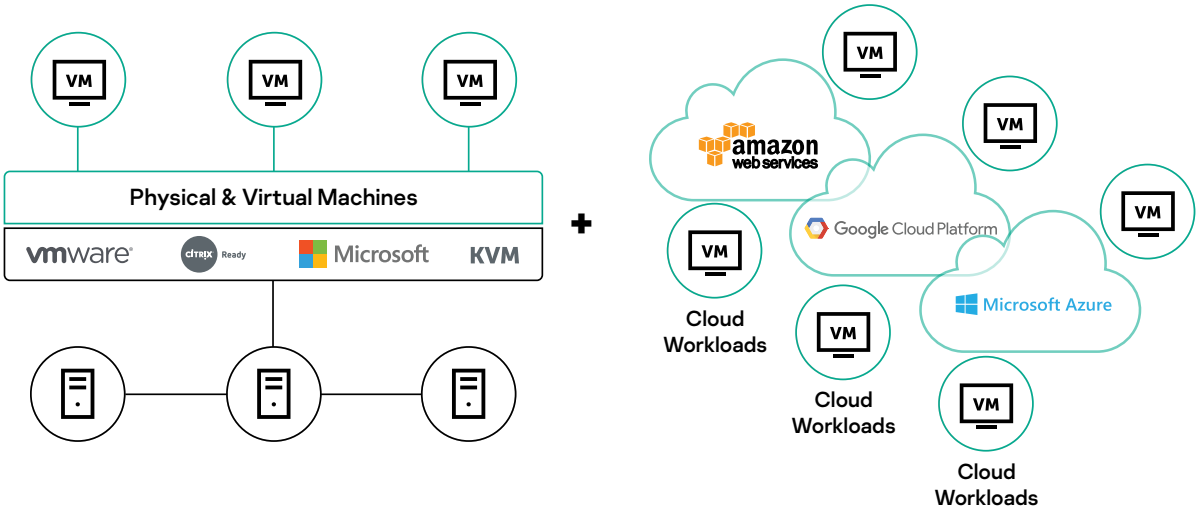
We believe that a 'single pane of glass' management console best addresses this problem. When you can seamlessly control security for all physical, virtualized, mobile and cloud elements of your environment, the chances of human error leading to a security gap are so much lower.

Across-the-board security for complex hybrid enterprises

Kaspersky Hybrid Cloud Security protects hybrid IT infrastructures, delivering consistent 'single-pane of glass' visibility and centralize control across cloud based workloads, virtualized infrastructure and physical machines and every stage of your transition journey and beyond. You remain fully compliant at all times, and systems performance remains unaffected A single management console with unified policies cuts management time and complexity, and helps close those all-important security gaps.
Public clouds – visibility and convenience

Kaspersky Hybrid Cloud Security simplifies orchestration for public cloud deployments, through things like:

- A single pane of glass management console that can be deployed in any number of sub-infrastructures and organized in a management server hierarchy to cover even the most complex deployments, with no gaps.
- Native API integration with AWS, Microsoft Azure and Google Cloud platforms
- Protection for Windows and Linux workloads
- Very straightforward cloud infrastructure inventory, and automated security provisioning of security agents regardless of their location.
- A flexible consumption model:
  - Pay-Per-Use (PPU), enabling security procurement and billing directly through the cloud provider's marketplace
  - Yearly contracts with SaaS fulfilment available on selected platforms
  - A Bring Your Own License (BYOL) - the solution can be activated using a license obtained from a Kaspersky partner



Auto-discovery and rollout

Integration with cloud APIs provides automation and administrative flexibility. The management console must be able to see all the instances running under the specified accounts, and use that information to deploy security agents, as well as applying security policies to them. When a new instance is created, an IAM role or a script deployment mechanism can be used to ensure the instance is fully protected the moment it's created.

Auto-scaling groups support

The elastic configurability of Kaspersky Hybrid Cloud Security means the solution is able to respond automatically to the increasing load as new instances are created and run by the cloud. API and auto-scaling policies ensure that every new instance in each auto-scaling group has security deployed to it, and conforms to the policy set by the organization.

Container security

One of the important use cases for public cloud is the enablement of DevOps. But the adoption and wide (often loosely controlled) use of container technologies, such as Docker, creates a persistent challenge for security managers. Kaspersky Hybrid Cloud Security secures Docker and Windows Containers to prevent an attacker from using a vulnerable or malicious container component as a stepping stone into the organization's internals. Containerization host memory protection, tasks for container and image scanning and scriptable interfaces all enable 'security as code' approach , with the ability to integrate security tasks into CI/CD pipelines.

Virtualization – balancing security and efficiency in the datacenter

While public clouds maybe be changing the face of IT, on-premises virtualization and private clouds remain here to stay. Managing corporate risk means securing every Virtual Machine (VM) and virtualization storage, but while the goals for public and private clouds security are the same (reduce and manage cyber-risk), the challenges on the way are different.

Virtualization is all about getting more from your on-premises hardware resources than can be achieved with physical machines. So the performance benefits of investment in virtualization must be conserved through applying appropriate security designed specifically to protect virtual environments. Effective virtualization security must find ways to centralize security tasks, reuse available information and eliminate redundancy, balance the load between VMs, and utilize the possibilities provided by virtualization platforms to maximize protection with the lowest possible performance impact.

Protection for virtualized servers and for VDI

Designed and built specifically for use in virtualized environments, eliminating all superfluous operations and data, Kaspersky Hybrid Security saves up to 30% of virtualization hardware resources compared to using a traditional endpoint security solution. After learning the environment, the solution can often instantly produce a verdict, without spending a single extra cycle. Rich and flexible systems hardening functionality drastically reduces the attack surface, preventing arbitrary code execution on servers and blocking exploits – all with no noticeable increase in resource consumption.

For virtual desktops, login time is drastically cut compared to traditional endpoint security solutions, eliminating hiccups and choke points when scaling and pushing the limits of the virtualization host. Deploying same extensive security feature-set as our solutions for physical endpoints, Kaspersky Hybrid Cloud Security creates a secure and responsive user environment, allowing users to focus on their job without the risk of falling victim to fileless malware, ransomware, exploits and the like. Kaspersky Hybrid Cloud Security has several deployment options to better address a customer's needs — in terms of deployment complexity, platform integration and support, resource use optimization, feature sets and ultimately the level of security.

Agentless Security

VMware features an API that enables 'agentless' file-level security for its vSphere virtualization platform and allows Kaspersky Hybrid Cloud Security to natively integrate with the VMware ecosystem, including vShield Endpoint and NSX Guest Introspection, while seamlessly and instantly enveloping all virtualized assets. Only one Security Virtual Machine (SVM) – a specialized VM carrying an anti-malware scanning engine and signature databases – is needed per host, removing this burden from individual VMs and so greatly reducing resource consumption.

Light Agent Security

Another approach, adopted by the 'light agent' application also included in Kaspersky Hybrid Cloud Security is a platform-independent solution which utilizes a lightweight agent optimized to operate inside the OS of each VM being protected. With the file scanning engine and databases still held centrally on the SVM, 'light agent' technology delivers a dramatically smaller resource footprint than a traditional full agent solution. The solution sits between 'agentless' and traditional full agent solutions in terms of resource consumption, but is not tied to or limited by VMware technologies and can also be used on popular platforms, including Microsoft Hyper-V, Citrix Hypervisor and KVM, to provide significantly higher level of security.

These approaches allow efficient deployment of secure virtualization, and solve the issues of:

- Excessive resource consumption. By centralizing most security tasks and using a single instance of a database as well as caching verdicts, we can avoid replicating signature databases and active anti-malware engines on each protected VM.
- 'Storms'. With smart queueing, balancing and caching of verdicts on the SVM, we can eliminate storms caused by simultaneous database updates and/or anti-malware scanning processes on each VM, and see and end the risk of 'vulnerability windows' caused by scanning delays.
- 'Instant-on gaps'. Databases and modules can't be updated on inactive VMs. So from the moment a VM starts up until the update process completes, the VM's vulnerable to attack. This is resolved by using an always-on always-updated SVM.

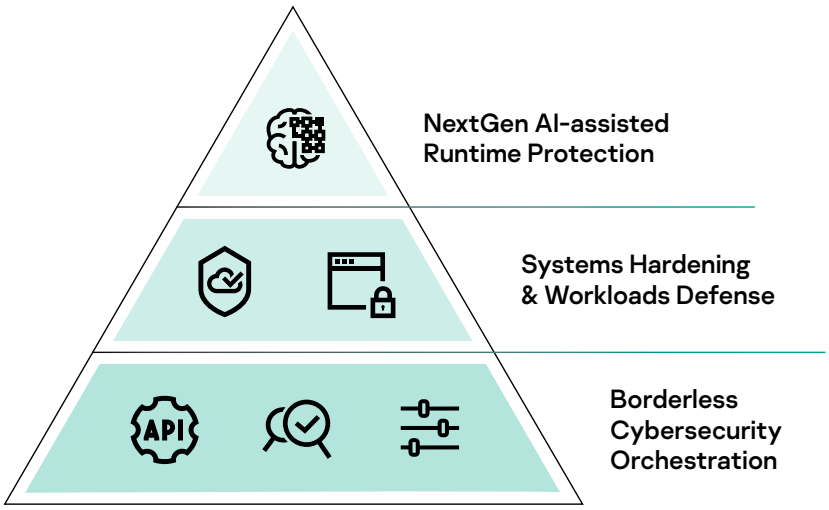
Physical machines and mobile devices

Physical servers and most importantly – physical workstations and mobile devices also need security – this is the role of yet another kaspersky solution - kaspersky endpoint security for business. Multiple layers of protection and control combine with security process automation tools means that the security status of every workstation, laptop, tablet or mobile phone is fully visible and under your control as part of your wider hybrid infrastructure, and all are subject to kaspersky's award-winning, best-of-bred protection.

Best-of-breed protection

The same rule applies whether your security is running on a mobile phone, a physical server, a virtual machine or in the cloud – it needs to be up to the job.

Best of breed protection is at the heart of all Kaspersky products and services. Based on unparalleled sources of real-time threat intelligence and machine learning, our technologies continually evolve to protect your endpoints from the latest exploits, keeping your data, and shared folders safe and secure from advanced threats and ransomware.



Hybrid Cloud Security draws upon the same unequalled feature-set whether protecting physical or virtual endpoints and servers or workloads in public clouds. These include:

- **Our Award-winning anti-malware engine** providing automatic, real-time file level protection for every computer, VM and workload – on-access and on-demand.
- **Cloud-based Intelligence** rapidly identifying new threats and providing automatic updates
- **Behavior Detection,** monitoring applications and processes, protecting against advanced threats and even bodiless malware and rolling back any malicious changes if needed.
- **Exploit Prevention,** controlling systems operation processes and applications behavior, helping block advanced threats including ransomware.
- **Anti-Ransomware,** protecting cloud workloads, virtual and physical endpoints and their shared networks against attacks, rolling back any affected files to their pre-encrypted state.
- **HIPS / HIDS,** detecting and preventing network-based intrusions into physical and cloud-based assets.
- **Application Controls,** enabling you to lock down all your hybrid cloud workloads in Default Deny mode for optimum systems hardening, as well as dictating what applications can run where, and what they can access.
- **Web Control** protecting against internet-based cyber-threats, including those that prey on employee ignorance or error, as well as promoting productivity through reducing time wasted on social media communications and irrelevant browsing.
- **Network Segmentation,** providing visibility and automated protection for hybrid cloud infrastructure networks.
- **Mail Security** including Anti-Spam, protecting email traffic in cloud workloads
- **Web Security** including Anti-Phishing, protecting against threats from potentially dangerous websites and scripts.

Compliance

Compliance is an important requirement for every organization. Kaspersky products enable compliance through multiple controls and features, such as:

- **Management server hierarchy** – providing the flexibility to support infrastructure complexity
- **Different deployment options** – on-premises or in the cloud
- Comprehensive and highly configurable **reporting and log inspection** to simplify audits
- **Role-Based Access Control (RBAC)** to ensure the segregation of control rights between different groups of administrators according to the organizational structure and IT policies.
- **Agent password protection and self-defense,** to prevent security systems tampering
- **Secure communications** between all solution components
- **Vulnerability Assessment and Automated Patch Management,** preventing advanced malware and zero-day threats from exploiting unpatched vulnerabilities
- **User-transparent FIPS 140-2 certified encryption** fully securing confidential data on portable devices and on-site. Integrated technology means encryption can be centrally re-enforced
- **System hardening** – executable lock-down with Default Deny and the prevention of substitution attacks though File Integrity Monitoring (FIM)
- **Device Control** for the granular control of attached storage, camera, microphone and other hardware in use
- **Configurable anti-malware protection and personal firewalls** for enhanced server and workstation security

There are also features and mechanisms to ensure full visibility, sufficient granularity and high levels of control, as well as continuous improvement and adaptation to the risk landscape.

Enabling secure digital transformation

Digital transformation produces a whole spectrum of new opportunities - for you, and for the cybercriminals targeting you. Make the very most of your own business opportunities, while firmly removing all those of your attackers, with Kaspersky's integrated best-of-breed security solutions for hybrid environments.

Kaspersky Hybrid Cloud Security: www.kaspersky.com/hybrid
Security for AWS: www.kaspersky.com/aws
Security for Microsoft Azure: www.kaspersky.com/azure
Security for Google Cloud: www.kaspersky.com/gcp

www.kaspersky.com

kaspersky **BRING ON THE FUTURE**