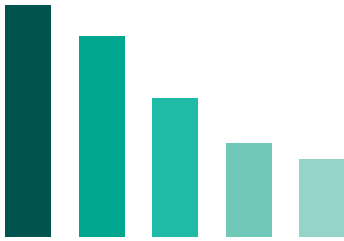




**Proven
cloud-native
protection
and the best
performance
for your hybrid
environment**

Kaspersky Hybrid Cloud Security

kaspersky



- Security 81%
- Managing cloud spend 79%
- Governance and Compliance 75%
- Managing multi-cloud 72%
- Cloud migration 71%

Top cloud challenges for all organizations²

89%

of enterprise use VDI solutions¹

55%

of enterprise workloads are expected to be in a public cloud within twelve months²

Digital transformation – challenges along the road to business efficiency

Today's business focus on digital transformation is triggering rapid cloud adoption. Moving to the cloud allows businesses to become more agile, scale themselves to geographical and market demand, transform their products or services and implement new features, optimize their operations and enhance their customer experience. Transformation initiatives provide many clear advantages for business, but there's a downside - infrastructures become more complex, generating significant concerns in terms of security risk, governance, staff resources, performance optimization, new regulations, and spending.

Different workloads, different concerns

In hybrid infrastructures, workloads can have many faces. They can be physical, virtualized, or based in private, public, and multiple clouds. While challenges associated with security risk, governance, compliance, and infrastructure spending can apply to any organization, working with different types of workload brings in additional concerns.

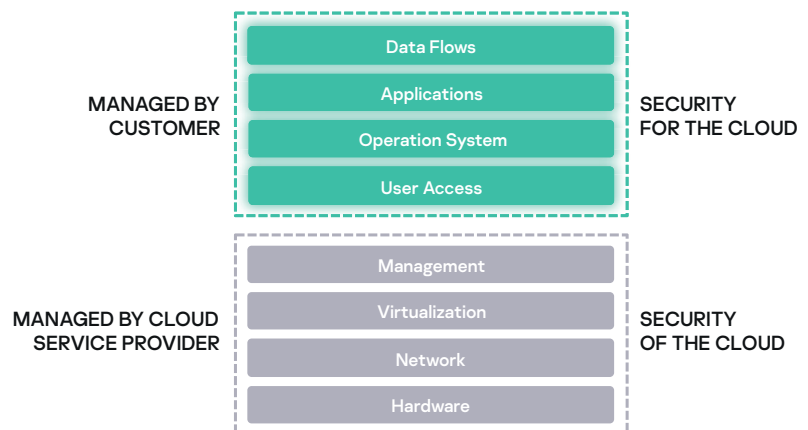
Conserving performance benefits

The adoption of virtualized servers and VDI is widespread across all businesses, regardless of size, sector or geography. Virtualization is 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 potential provided by virtualization platforms to combine maximum protection with the lowest possible performance impact.

Protecting cloud workloads in terms of shared responsibility

Public cloud adoption continues to accelerate, with the average cloud-adopting business using two different cloud services providers. Public clouds offer great scalability and performance, and are used widely by cloud-adopters for compute, data processing and analytics, among other things. Cloud computing means you don't need a support infrastructure, because the hardware layer is no longer your responsibility. Nor are the network, virtualization and management layers – it's all up to your cloud services provider. That's good news, but with loss of responsibility comes loss of control and visibility. And you're still responsible for all the other layers (see below) and need to provide appropriate security for these.

Shared security responsibility



¹ Kaspersky internal research, 2021

² Flexera State of the Cloud Report, 2021

53%

of organizations use Docker³

51%

of organizations use containers as a service offering from AWS³

'This solution helps to protect virtual and cloud environments, without affecting system performance or disrupting user experience.'

Taken from Gartner reviews

Specific requirements of DevOps environments

Developers have switched from annual or semi-annual to daily or even hourly software releases. That's why software development focuses on DevOps tactics – Continuous Integration (CI) and Continuous Delivery (CD). These form an automated pipeline that helps organizations improve business-impacting KPIs. Containers are central to a DevOps approach, because they allow for quicker development and deployment at scale. DevOps enablement is generally based around the use of public clouds – and the focus here on time-to-market, speed and agility all mean that any security solution must integrate seamlessly into development and cloud-native applications.

A cloud-native approach for optimum hybrid infrastructure security performance

Kaspersky Hybrid Cloud Security addresses all these concerns, providing outstanding protection without in any way compromising the full benefits of virtualization and cloud-based operations. The cybersecurity engine protects your entire hybrid infrastructure, whatever the workload – physical, virtualized, or based in private, public, and hybrid clouds – with the lightest possible footprint.

- Light agents optimized for each OS efficiently reduce consumption of virtualization resources by as much as 30%, freeing them up for use in other business operations. A number of optimizations, including shared cache which shares the results of file scans, decrease the amount of data and the number of operations involved. These optimizations minimize the overall load on your IT infrastructure, dramatically reducing IOPS, CPU cycles, memory, and disk footprints – helping you achieve high consolidation ratios and protecting your investment in virtualization projects.
- Our platform-agnostic product protects Windows and Linux workloads and provides native API integration with AWS, Microsoft Azure and Google Cloud platforms. So no more worries about the security responsibilities you share with your cloud service provider. Integration with cloud APIs provides automation and administrative flexibility. You can see all the instances running under the specified accounts through the management console, and use that information to deploy security agents and apply security policies to them. Kaspersky Hybrid Cloud Security also responds 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, conforming to the policy that you as an organization choose to set.
- Kaspersky Hybrid Cloud Security enables a 'security as code' approach, with containerization host memory protection, tasks for containers, image scanning and scriptable interfaces. So you can integrate security tasks into CI/CD pipelines without impacting on the development process – good news for DevOps teams. The product also secures Docker and Windows containers, so an attacker can't use a malicious container component as a stepping stone into the organization's internal workings.

³ Flexera State of the Cloud Report, 2021

64%

of organizations named data loss/leakage as a biggest cloud security concern⁴

'No need to install additional anti-virus software and other agents.'

Taken from Gartner reviews

Rapid growth in security risks

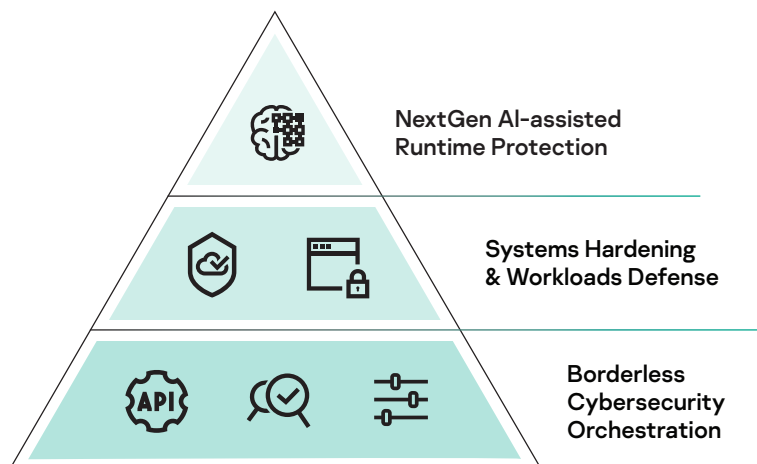
The journey into the cloud is a big opportunity for cybercriminals. Misconfiguration during migration, a lack of visibility, and loss of control over different parts of the infrastructure as a whole can all leave organizations vulnerable to the full spectrum of cyberattacks – from data leakage to ransomware. Rapid cloud adoption means cybercriminals are switching their focus onto the cloud, as is demonstrated by a recent doubling in the number of phishing attacks targeting cloud-based resources⁵. Attackers even arm themselves with tools specifically designed to detect misconfigurations.

Protecting the hybrid infrastructure from these growing threats is vital. But at what cost? Cumbersome intrusion by the security system into the development/deployment process, for example, is not acceptable. Nor is wasting IT and security professionals' time with false positives or low-risk findings. So your security solution must integrate smoothly with your infrastructure, and mustn't burden your team with unnecessary and tedious security tasks.

Best-of-breed protection designed for hybrid environments

Best of breed protection is at the heart of all Kaspersky products and services, so you can be sure that all your data, shared folders and entire hybrid infrastructure are safe.

- Multi-layered threat protection proactively fights the broadest range of cyberattacks including malware, phishing, and more.
- Machine learning algorithms empowered by human expertise deliver the highest detection levels with minimal false positives.
- Real-time threat intelligence data helps defend against the latest exploits.



The product not only detects and prevents network-based intrusions into cloud-based assets, but even allows you to roll back any malicious changes made inside cloud workloads, if needed. Application control means you can lock down all hybrid cloud workloads in Default Deny mode for optimum system hardening, and limit the range of running applications to legitimate and trusted only.

Also, in the age of ransomware, Kaspersky Hybrid Cloud Security protects business-critical data from any attempt to hold it to ransom, including blocking remotely initiated encryption and rolling back any affected files to their pre-encrypted state.

⁴ Statista, 2021

⁵ Kaspersky Security Bulletin, 2021

44%

of businesses have problems with a rapid increase in security costs⁶

'Great way to combine all the security solutions in one license.'

Taken from Amazon reviews

45%

of organizations cite a cloud audit failure⁷

'It has a fully automated security feature.'

Taken from Amazon reviews

The balance between agility, management, and the cost of security

Cloud models offer efficiency benefits in the form of agile development and elastic consumption for the IT infrastructure. But that infrastructure also becomes more complex, requiring additional resources to manage, due largely to the short lifespan of workloads and the lack of visibility. Getting the most from your investment becomes a balance between the overall efficiency benefits delivered by introducing cloud based IT, and the costs of managing and fully securing a more complex hybrid infrastructure.

Cost-efficiency and convenient management for a comfortable cloud journey

We at Kaspersky fully appreciate these practical issues, and Kaspersky Hybrid Cloud Security offers both straightforward management and flexible licensing, optimizing your investment and conserving your resources.

- Our flexible licensing model means you choose only the capabilities you need, getting the most value from your security budget. You can choose one of two tiers and different licensing objects such as desktops, servers, or CPUs. You can also combine different license types. And we offer additional BYOL and pay-per-use licensing options.
- A unified cloud console makes the security management of your whole infrastructure simpler, saving on valuable IT staff resources. All workloads can be managed from the one console.
- Straightforward cloud infrastructure inventory, and automated security provisioning regardless of the agents' location, both contribute further to streamlined management processes and maximum visibility.

Compliance as a cloud routine

Compliance is an important requirement for every organization, from internal standards to compliance with external regulations such as GDPR. Cloud security is a shared responsibility across IT, security teams, DevOps (if present), and the Compliance Analyst, who's responsible for the organization's performance in cloud audits. Your security solution must be able to support compliance with new regulations as they come into effect, making audits a painless routine.

Compliance-ready security for highly regulated industries

Kaspersky Hybrid Cloud Security doesn't just help you adhere to cybersecurity regulations – it reduces the number of routine manual tasks involved in ensuring adherence.

- Adaptive and multi-faceted, this product is designed to enable and continuously support full regulatory compliance, through technologies ranging from system hardening and agent self-defense to vulnerability assessment and automated patch management.
- The wide range of features provides compliance and risk landscape adaptation, keeping your security continuously on top of current legislation.

⁶ Kaspersky internal research, 2021

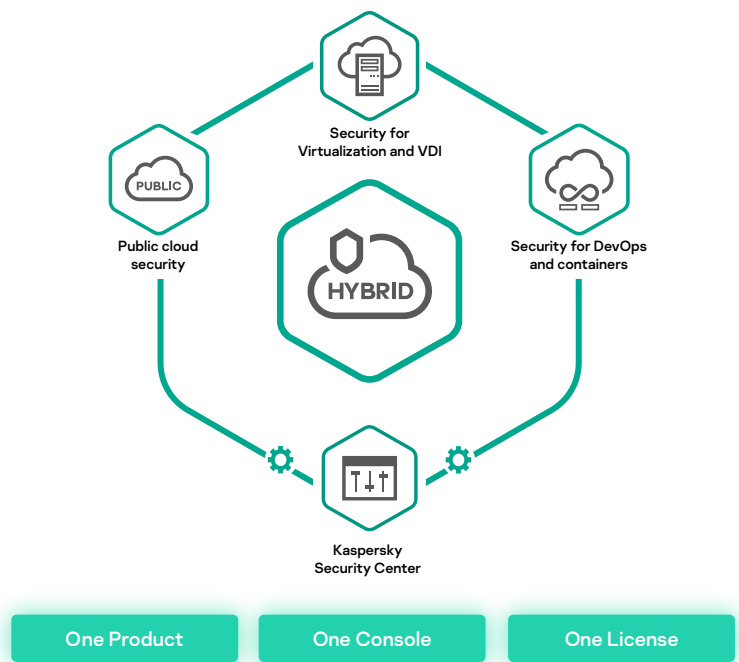
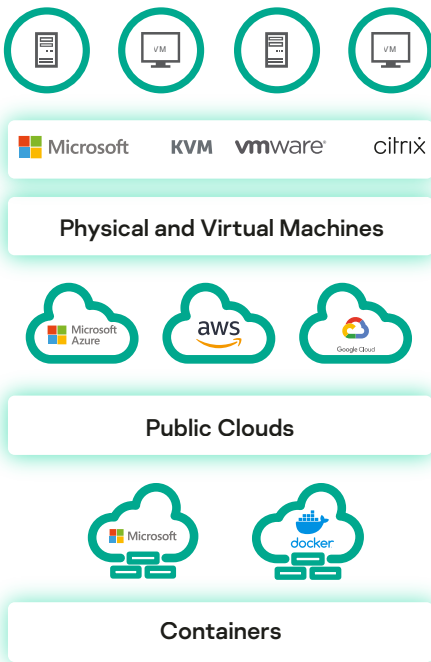
⁷ Fugue The State of Cloud Security Report, 2021

Learn more about
Kaspersky Hybrid Cloud
Security


Learn more

Focus on your digital transformation journey

Digital transformation produces a whole spectrum of new opportunities – for you, and for the cybercriminals targeting you. Kaspersky Hybrid Cloud Security helps you get the best from your digital transformation, because it doesn't just mitigate security risk – it also saves labor hours, infrastructure resources, and money. With one product for all your cloud security needs, one license for all workloads, and one console to manage your whole hybrid infrastructure, security becomes one less thing to worry about – leaving you free to focus on other aspects of your digital transformation journey.



For more about how to ensure the strongest and most efficient protection for your hybrid environment, speak to your Kaspersky reseller or [visit our website](#).



www.kaspersky.com
www.securelist.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks are the
property of their respective owners.