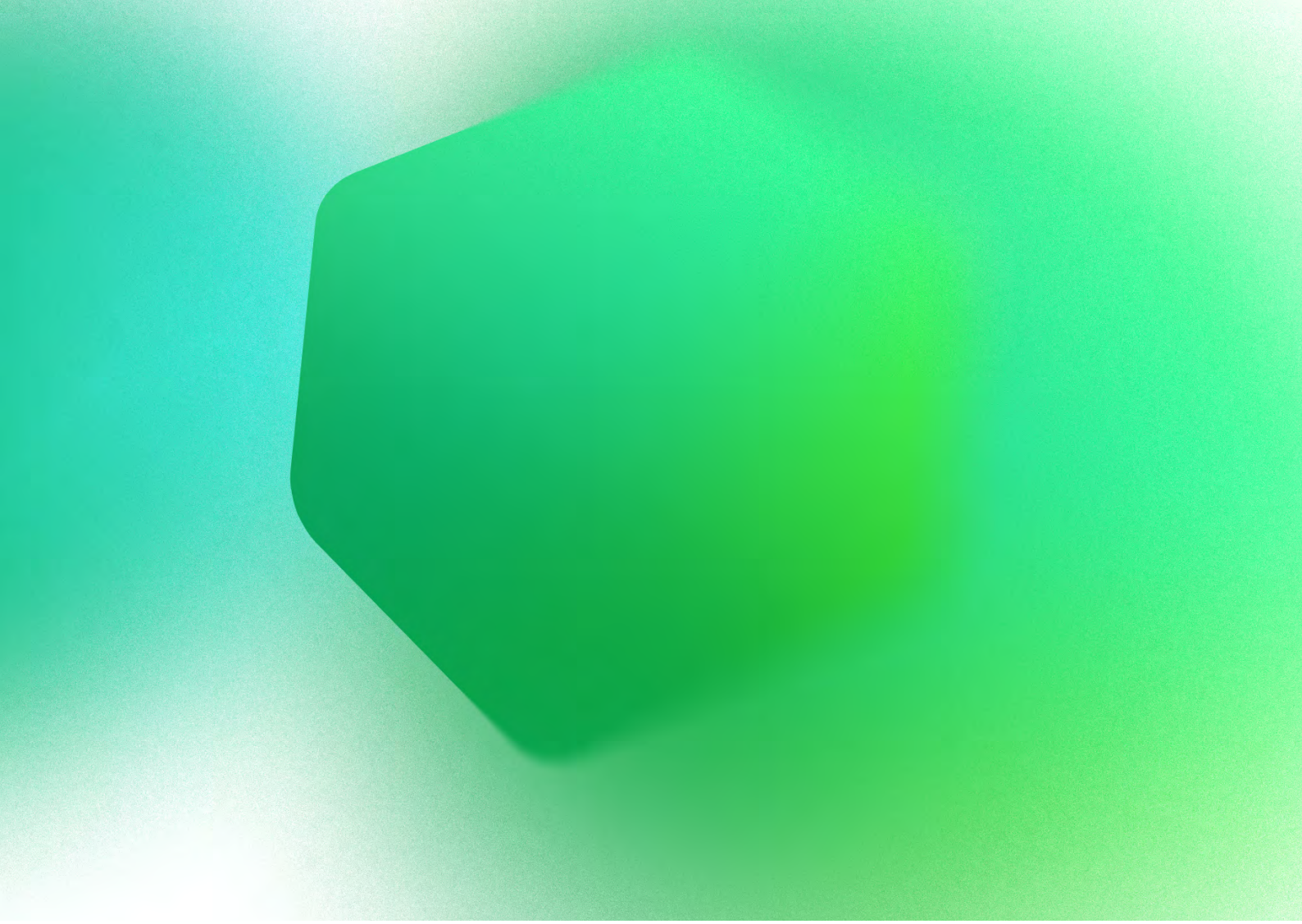


2020

Proven protection and borderless orchestration for your hybrid cloud

kaspersky

Learn more on kaspersky.com
#truecybersecurity

Kaspersky Hybrid Cloud Security

Virtualization has become a mainstay approach for every business trying to be flexible and efficient. Cloud computing is the next natural step. It brings relief from the constraints of complex infrastructure support and offers previously unattainable level of efficiency. But the cloud journey has its perils and complications, some of them new and some retained from the physical world.

Kaspersky Hybrid Cloud Security offers unified security for any stage or scenario of your cloud journey. Suitable for both cloud migration and native cloud scenarios, it secures your physical and virtualized workloads whether running on-premise, in a datacenter or in a public cloud. Because its applications were created with the specifics of both virtualization and server functioning in mind, it delivers perfectly balanced protection against the most advanced current and future threats without compromising on system performance.

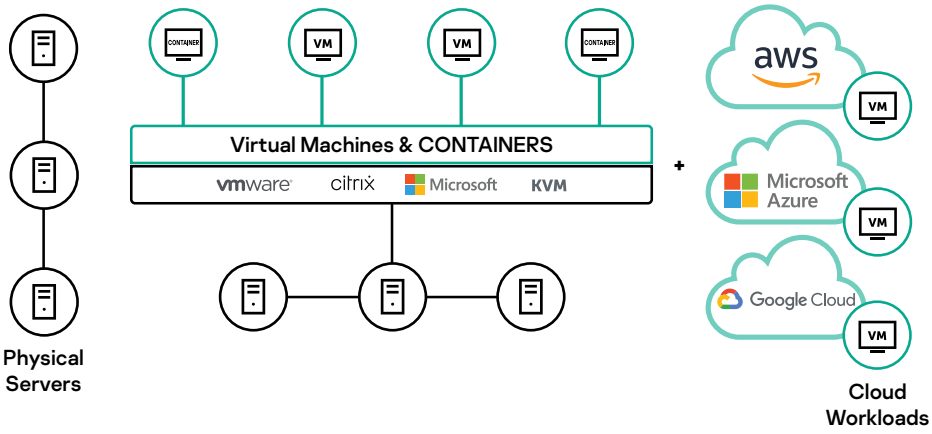
Top challenges of cloud adopters:

- Growing infrastructure complexity can result in reduced transparency
- A multi-layered approach, key to reliable protection, is rarely found in a single product
- Traditional heavyweight security eats into valuable systems resources
- A silo approach and disparate controls bring extra administrative and security challenges
- Malware and ransomware attack virtual as well as physical endpoints
- Failure to implement adequate cybersecurity measures for personal data protection may result in legal issues.

Why Kaspersky Hybrid Cloud Security?

- Engineered for physical, virtual and cloud workloads
- Integrated multi-layered security for all types of workloads
- Consistent, automated and agile security for AWS Azure and Google public clouds
- Helps meet shared responsibility with a full set of security tools
- Seamless security orchestration across your entire hybrid cloud
- Most tested, most secure protection, according to numerous awards and independent tests[1]

Key benefits



Enables a secure cloud journey – without compromising on protection levels

- Patented technologies and our award-winning cybersecurity engine secure all your workloads – physical, virtualized or cloud-based.
- Multi-layered real-time protection, powered by machine learning, secures your data, processes and applications against emerging threats.
- A holistic approach to data security helps reduce legal and reputational risks relating to data protection regulations.

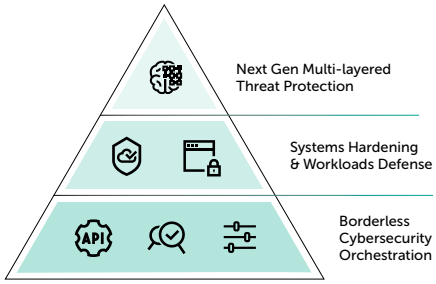
Ensures that you get the most from your resources and investments

- Agentless and light agent-based protection secure virtualized assets in regular and software-defined networks without impacting performance.
- Integration with native public and managed cloud security helps secure your applications, operating systems, data flows and user workspaces with the smallest possible resource footprint.
- Single-point-of-view management of physical and virtual resources saves man-hours during adoption and maintenance.

1 The tests referred to cover a range of Kaspersky products based on the same threat protection technologies as utilized in Kaspersky Hybrid Cloud Security. Learn more at kaspersky.com/top3

Features

Features	Description
Multi-layered threat protection Kaspersky's next-generation malware protection incorporates multiple proactive security layers capable of blocking the broadest range of cyberattacks that threaten your business-critical workloads.	
Global threat intelligence	Provides real-time data on the state of the threat landscape, even as it shifts, ensuring your protection at all times.
Machine Learning	The big data of global threat intelligence is processed by the combined power of machine learning algorithms and human expertise, for proven high detection levels with minimal false positives.
Web and mail threat protection	Enables the safe functioning of virtual and remote desktops, protecting them from email- and web-based threats.
Log Inspection	Scans internal log files for optimum operational hygiene.
Behavior Analysis	Monitors applications and processes, protecting against advanced threats including bodiless or script-based malware.
Remediation engine	Rolls back any malicious changes made inside cloud workloads, if needed.
Exploit Prevention	Provides effective protection against attack spearheads while ensuring perfect compatibility with protected applications, all with minimal impact on performance.
Anti-ransomware functionality	Protects virtualized workloads against any attempts to hold business-critical data to ransom, rolling back affected files to their pre-encrypted state and blocking remotely initiated encryption.
Network Threat Protection	Detects and prevents network-based intrusions into cloud-based assets.
Container protection	Ensures that infections can't be transported into your hybrid IT infrastructure via compromised Docker or Windows containers.
System hardening boosts resilience	
Application Control	Lets you lock down all your hybrid cloud workloads in Default Deny mode for optimum system hardening, allowing you to limit your range of running applications to legitimate and trusted only.
Device Control	Specifies which virtualized devices can access individual cloud workloads.
Web Control	Regulates the use of web resources by virtual and remote desktops to lower risks and boost productivity.
Host-based Intrusion Prevention System (HIPS)	Assigns trust categories to launched applications, restricting their access to critical resources and limiting their capabilities.
File Integrity Monitoring	Helps ensure the integrity of critical system components and other important files.
Vulnerability Assessment and Patch Management	Centralizes and automates essential security, system configuration and management tasks, such as vulnerability assessment, patch and update distribution, inventory management and application rollouts.
Borderless visibility	
Unified Security Management	From Kaspersky Security Center facilitates singlepoint-of-view security administration across the whole infrastructure, endpoints and servers – in the office, in your data center and in the cloud.
Cloud API	Seamless integration with public AWS and Azure environments enables infrastructure discovery, automated security agent deployment and policy-based management, as well as easier inventory and security provisioning.
Flexible management options	Feature multi-tenancy capabilities, permission-based account management and role-based access control, providing flexibility while retaining the benefits of unified orchestration from a single server.
SIEM integration	In infrastructures with more mature IT, Security Information and Management Systems can be used as a unified window for different aspects of a company's cybersecurity – across the entire hybrid IT network.



Unified security for any cloud:

Public clouds
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

Private data centers
- Vmware NSX
- Microsoft Hyper-V
- Citrix Hypervisor
- KVM
- Proxmox

VDI environments
- Vmware Horizon
- Citrix Virtual Apps and Desktops

Physical servers
- Windows
- Linux

Physical desktops:
- Windows
- Linux

aws

Microsoft Azure

vmware

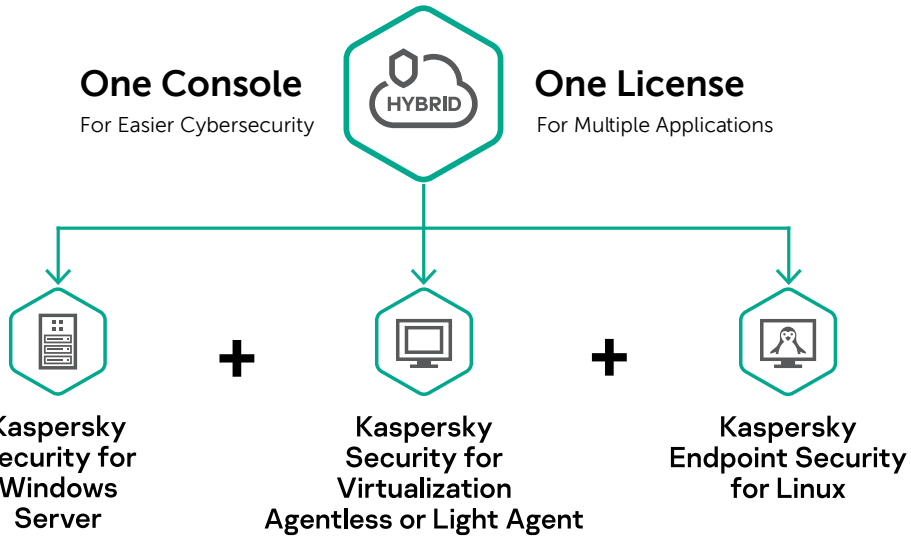
citrix

Google Cloud

KVM

Offers consistent visibility and control regardless of your hybrid infrastructure configuration

- Easier security services provisioning and policy-based operations are enabled right across your hybrid cloud.
- Manageability and security orchestration operate seamlessly across multiple clouds.
- Full visibility, control and holistic protection against the most advanced threats for every workload, in every location.



Kaspersky Hybrid Cloud Security delivers multiple award-winning, industry-recognized security technologies to support and simplify your the transformation of your IT environment. It secures your migration from physical to virtual, and to the cloud, while visibility and transparency guarantee flawless security orchestration.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

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 tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.