# Kaspersky Hybrid Cloud Security

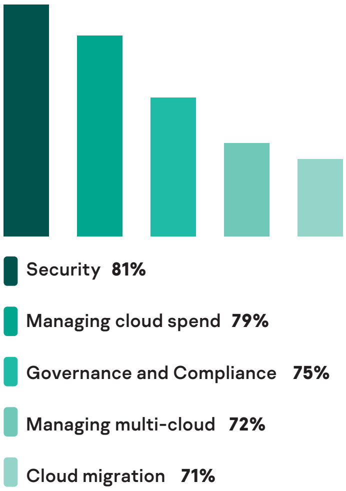
kaspersky BRING ON THE FUTURE

**Today's business focus on digital transformation is triggering rapid cloud adoption. On the one hand, these initiatives provide many advantages for businesses, including greater efficiency. On the other, infrastructures become more complex, generating significant concerns in terms of security risk, governance, staff resources, performance optimization, new regulations, and spending. Kaspersky Hybrid Cloud Security addresses all these challenges.**

# Proven cloud-native protection and the best performance for your hybrid environments

Kaspersky Hybrid Cloud Security makes cloud adoption, digital transformation, and doing business in general safer and more efficient. This single product secures your entire hybrid infrastructure, mitigating risk, reducing virtualization resource consumption, and supporting regulatory compliance. Kaspersky Hybrid Cloud Security delivers increased visibility and simplified management, while saving you and your team valuable time and budgetary resources. Security becomes one less thing to worry about – leaving you free to focus on other aspects your digital transformation journey.

## Top cloud challenges



According to Flexera State of the Cloud Report 2021

### Best-of-breed protection designed to address hybrid environment security risks

- 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.

### A cloud-native approach for the best hybrid infrastructure security performance

- The cybersecurity engine protects the entire hybrid infrastructure, whatever the workload – physical, virtualized, or based in private, public, and hybrid clouds.
- A platform-agnostic approach combined with native integration renders public clouds fully DevOps-enabled.
- 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.

### Cost-efficiency and convenient management for a comfortable cloud journey

- A flexible licensing model means you choose only the capabilities you need, getting the most value from your security investment.
- A unified cloud console makes the security management of your whole infrastructure simpler, saving on valuable IT staff resources.
- Straightforward cloud infrastructure inventory and automated security provisioning regardless of the agents' location both contribute to maximum visibility.

### Compliance-ready security for highly-regulated industries

- 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.

# Features

## Multi-layered threat protection

| | |
|---|---|
| **Global Threat Intelligence** | Collects real-time data on the state of the threat landscape, even as it shifts. |
| **Machine Learning** | Empowers the big data of global threat intelligence with machine learning algorithms and human expertise. |
| **Web and Mail Threat Protection** | Secures virtual and remote desktops, protecting them from email- and web-based threats. |
| **Log Inspection** | Scans log files for optimum operational hygiene. |
| **Behavior Analysis** | Protects against advanced threats, including bodiless or script-based malware, through application and process monitoring. |
| **Remediation Engine** | Rolls back any malicious changes made inside cloud workloads, if needed. |
| **Exploit Prevention** | Provides effective protection against threat penetration in complete compatibility with protected applications, resulting in minimal impact on performance. |
| **Anti-Ransomware Functionality** | Protects business-critical data from any attempt to hold it to ransom, including blocking remotely initiated encryption and rolling back affected files to their pre-encrypted state. |
| **Network Threat Protection** | Detects and prevents network-based intrusions into cloud-based assets. |
| **Container Protection** | Prevents infections from being transported into the hybrid IT infrastructure via compromised containers. |

## System hardening that boosts resilience

| | |
|---|---|
| **Application Control** | Allows the locking down of all hybrid cloud workloads in Default Deny mode for optimum system hardening, and limiting the 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, lowering risk and boosting 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** | Endpoint and server protection for the whole infrastructure can be managed through one console – in the office, in your data center and in the cloud. |
| **Cloud API** | Seamless integration with public environments enables infrastructure discovery, automated security agent deployment and policy-based management, as well as easier inventory and security provisioning. |
| **Flexible Management Options** | Multi-tenancy capabilities, permission-based account management and role-based access control provide flexibility while retaining the benefits of unified orchestration from a single server. |
| **SIEM Integration** | Allows product integration with the Security Information and Management System, bringing different aspects of corporate cybersecurity together in one place – across the entire hybrid IT network. |

# Why Kaspersky Hybrid Cloud Security?

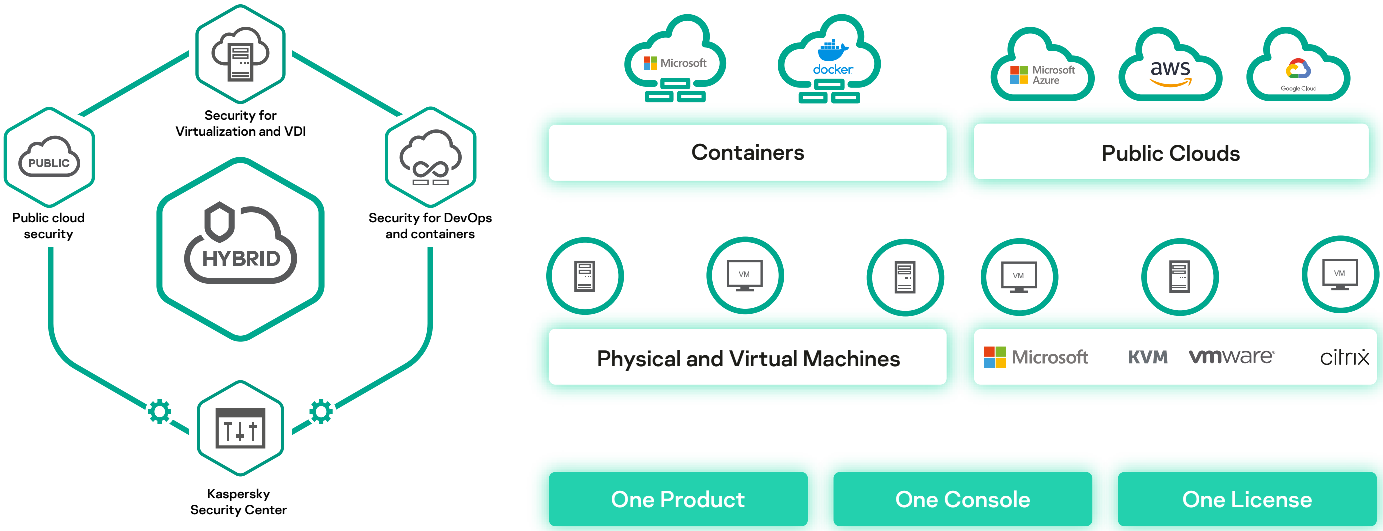
30%

potential savings on virtualization hardware resources compared to using a traditional endpoint security solution.

TOP3

sustained outstanding performance. Last year, Kaspersky products performed once again to exceptional standards across multiple independent tests, achieving 45 first places and 50 top-three finishes (learn more at kaspersky.com/top3).

# One product for all your cloud security needs



# Customer reviews

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

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

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

"Centralized cloud solution for data protection. All in one place."

"Protection applies instantly to all VMs, because you don't need to download new updates at all."

"The optimal solution that does not require long administrator training."

Taken from Amazon and Gartner reviews

Request a demo

**www.kaspersky.com**