# Kaspersky® Hybrid Cloud Security

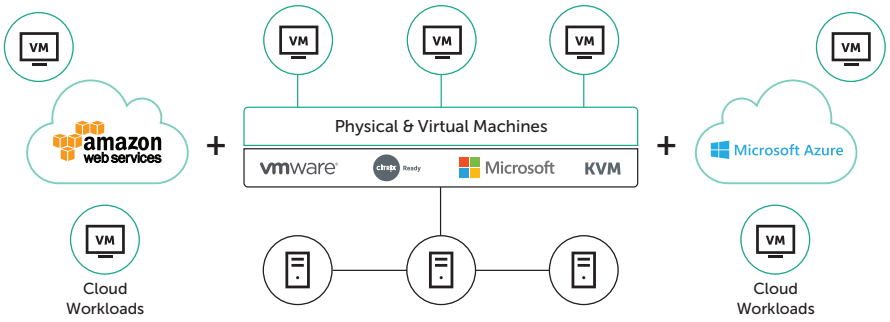
# Best in class protection and borderless orchestration for your hybrid cloud

**Top challenges of cloud adopters:**

- Growing Infrastructure complexity can mean decreased transparency
- True reliable security comes only through multi-layered integration
- Traditional heavyweight security eats into precious systems resources
- Disparate controls and tools present administrative challenges
- Inefficiently designed security leads to inefficient systems processes
- Malware and ransomware both attack virtual as well as physical endpoints
- Poor cybersecurity leads to non-compliances
- Reactive protection is no substitute for proactive, adaptive security

Combining public and hosted cloud resources with on-premise capabilities results in a highly cost-efficient IT environment, but also introduces new security considerations. The same rigorous security standards must apply throughout your multi-cloud environment. Fail in this, and your organization's most valuable assets – its data and people – are at risk.

Kaspersky Hybrid Cloud Security enables a seamlessly orchestrated and adaptive cybersecurity ecosystem. Wherever you process and store critical business data – in a private or public cloud, or both – we deliver a perfectly balanced combination of agile, continuous security and superior efficiency, protecting your workloads against the most advanced current and future threats without compromising on systems performance.




**Why Kaspersky Hybrid Cloud Security?**

1. Engineered for physical, virtual & cloud workloads
2. Multi-layered integrated security for any private data center
3. Seamless, automated and agile security for AWS and Azure public clouds
4. Helps to meet shared responsibility with a full set of security tools
5. Enterprise-level security orchestration across your entire hybrid cloud

## Next Generation security for physical, virtual and cloud environments

- Patented technologies and our award-winning cybersecurity engine secure all your workloads, wherever they're sitting.
- Multi-layered real-time protection supported by machine learning secures your data, processes and applications against emerging threats.
- A holistic approach to data security helps maintain full GDPR compliance.

## Resource-efficient hybrid cloud security

- Agentless and light agent based virtual machine technologies secure software-defined data centers without impacting performance.
- Integration with native public and managed cloud security helps secure your applications, OSs, data flows and users, with the smallest possible resource footprint.
- Unified management of physical and virtual resources increases administrative efficiency.

## Unified management and orchestration

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

### Seamless orchestration

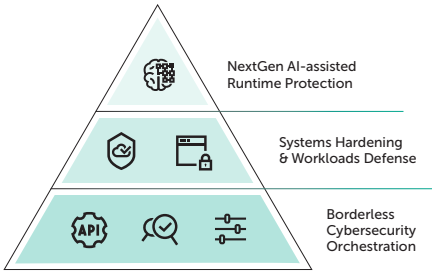
Unified management for all your software assets, on-premise and in the cloud, through a single console, providing full visibility and transparency and enabling smooth and efficient orchestration and administration.

### Unified cybersecurity

Edge-to-edge 'best of breed' security for every workload and device, physical as well as virtual, throughout your software-enabled data center and your managed and public cloud presence.

### Next Generation protection

Real-time multilayered protection for cloud workloads, based on machine learning assisted anti-malware combined with a raft of protection and prevention technologies, and cloud-assisted threat intelligence.




### Unified Security for Any Cloud:

Public Clouds
- Amazon Web Services (AWS)
- Microsoft Azure

Private Data Centers
- VMware NSX
- Microsoft Hyper-V
- Citrix XenServer
- KVM

VDI environments
- VMware Horizon
- Citrix XenDesktop

Physical Servers
- Windows
- Linux

CITRIX Ready · Microsoft Azure · vmware · amazon web services

# Technological Excellence That Matters

## Borderless Visibility

- **Unified Security Orchestration** allows cybersecurity management of all your enterprise devices, including endpoints and servers – in the office, in your data center, and in the cloud - from a single console.
- **Cloud API Seamless** integration with public AWS and Azure environments allows for 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, permissions-based account management and role-based access control, providing flexibility while retaining the benefits of unified orchestration from a single server.

## Cloud Workloads Defense

- **Application Controls** enable 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.
- **Device Control** specifies which virtualized devices can access individual cloud workloads, while Web Control protects against internet-based cyberthreats.
- **Network Segmentation** provides visibility and automated protection of hybrid cloud infrastructure networks, including scanning specific networks or ports, integrating with software-defined network platforms like VMware NSX.
- **Vulnerability Shielding** prevents advanced malware and zero-day threats from exploiting unpatched vulnerabilities

## AI-assisted Runtime Protection

- **Award-winning Anti-malware Engine** provides automatic, real-time file level protection for every cloud workload – on-access and on-demand.
- **Cloud-based Intelligence** rapidly identifies new threats and provides automatic updates.
- **Mail Security** including **Anti-Spam** protects email traffic in cloud workloads.
- **Web Security** including **Anti-Phishing** protects against threats from potentially dangerous websites and scripts.
- **File Integrity Monitoring** protects critical and system files while Log Inspection scans internal log files to ensure operational hygiene.
- **Behavior Analytics Engine** monitors applications and processes, protecting against advanced threats and even bodiless malware and rolls back any malicious changes made inside cloud workloads if needed.
- **Exploit Prevention** controls systems operation, processes and applications behavior, helping block advanced threats including ransomware.
- **Anti-Ransomware** protects cloud workloads and their shared networks against attacks, rolling back any affected files to their pre-encrypted state.
- **HIPS / HIDS** detects and prevents network-based intrusions into cloud-based assets.

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

**Learn more about cybersecurity:** www.securelist.com

**www.usa.kaspersky.com**
**#truecybersecurity**

Kaspersky Lab, Inc.
500 Unicorn Park Dr, 3rd Floor, Woburn, MA 01801 USA
Tel: 866-563-3099 | Email: corporatesales@kaspersky.com