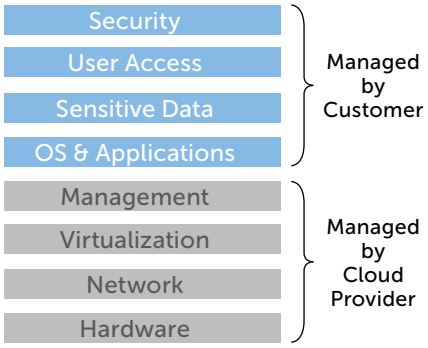
Kaspersky®
Cloud Security

Secure your Amazon cloud with Kaspersky Cloud Security solution

Why choose Kaspersky Lab for hybrid cloud protection:

- **The most awarded security solution**, optimized for your hybrid cloud.
- **Preserves systems efficiency**, giving you a full visibility and manageability over security in your clouds.
- **Enhanced functionality**, including application, web & device controls, and protection from advanced cyberthreats as well as ransomware attacks.
- **Works in harness** with your corporate infrastructure.
- **Saves resources** and significantly reduces operating costs in your hybrid cloud environment.

Shared Security Responsibility in public cloud environments



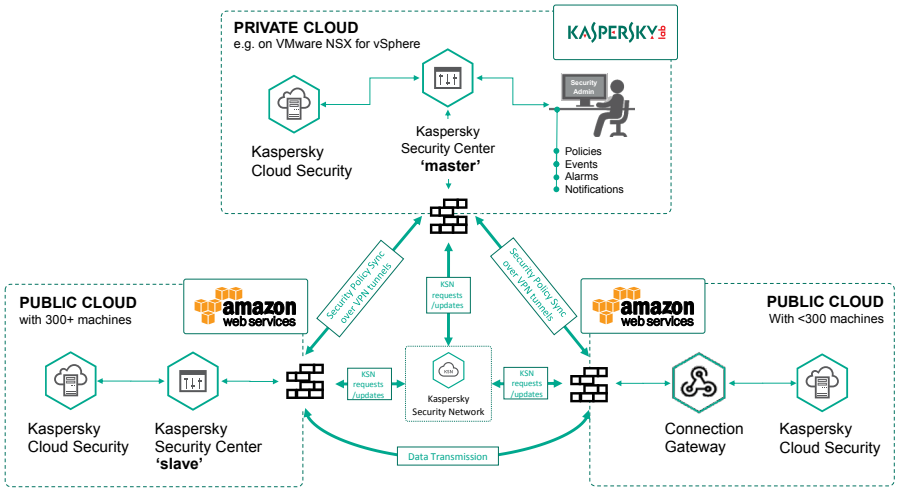
Orchestrate your hybrid cloud security with Amazon and Kaspersky Lab

The adoption of a hybrid cloud approach to data management and storage, with workloads moving freely between your own virtualized environment and one or more public clouds, introduces new security considerations. But, whether your data is running on- or off-premise, your overall objective remains the same – to effectively secure your organization, its digital assets, its business continuity and its employees.

Moving from a private to a hybrid cloud approach introduces a new responsibility model. While your service provider manages the security of the public cloud – infrastructure, hardware, network and virtualization layers – you remain responsible for what you put into the cloud – secure workloads, operating systems, data, and applications. And, of course, you also remain responsible for the cybersafety of employees, and for ensuring that your security solution meets your cybersecurity goals.

Amazon Web Services (AWS) provides a reliable, scalable and cost-efficient public cloud environment for your business workloads. VMs and their workloads protected by Kaspersky Cloud Security, regardless of whether then are operating in the public AWS-powered or private infrastructure of your hybrid cloud, should be subject to the same security levels and policies, and be full visible and manageable together through a single orchestration console.

This document explains just how straightforward it is to extend Kaspersky Cloud Security into your AWS cloud resources, delivering advanced security capabilities, full VM visibility and unified orchestration across your entire hybrid cloud.



Picture 1. Hybrid cloud with Amazon Web Services and Kaspersky Cloud Security

A general best practice recommendation - communication between clouds is conducted as standard via the public Internet. We strongly advise deploying **secure crypto-channels** (VPN tunnels) between your private and public cloud infrastructures to ensure the highest levels of protection and privacy; Amazon Virtual Private Cloud Network and Amazon Virtual Private Gateway can be used here.

If you are not already running version 10 of Kaspersky Security Center, we highly recommend upgrading to this version, as earlier versions may not be sufficiently full-featured to support this implementation.

You should also ensure that your **network infrastructure** is correctly configured to handle the traffic traveling between the infrastructure components as shown in the diagram above. For more details on how to set up network ports and firewall rules, please refer to the Implementation Guide for Kaspersky Security Center.

We offer two methods of Kaspersky Cloud Security solution deployment, depending on the size of your AWS cloud based operations. Both are very straightforward.

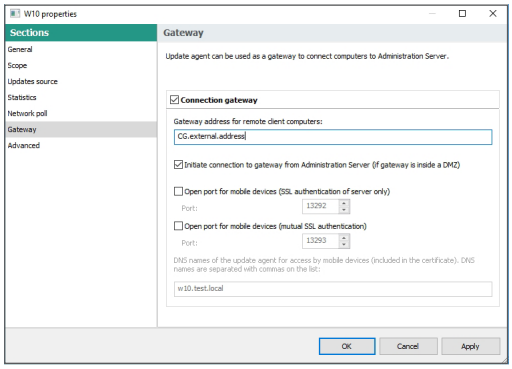
Hybrid Cloud Security: AWS Cloud + Private Cloud

Less than 300 VMs in the AWS cloud

Applying Kaspersky Cloud Security to your hybrid cloud at this level of public cloud activity simply involves the deployment of a Connection Gateway. This connects protected VMs in your public cloud directly to your normal private cloud based 'master' Kaspersky Security Center, so all VMs receive security policies, updates and license information.

When a **Connection Gateway** is used, protected VMs in your AWS public cloud directly connect to 'master' Kaspersky Security Center server to receive security policies, updates and license information. Anti-malware updates, scanning statistics and verdicts can also be downloaded from the cloud-based global service Kaspersky Security Network (KSN) if required.

Just install Kaspersky Network Agent onto a VM based in your AWS cloud, specifying the IP address of the 'master' Kaspersky Security Center in your private cloud. This VM is now the 'Connection Gateway', enabling all other VMs in your AWS cloud, located during the topology collection process, to connect to the 'master' Kaspersky Security Center.



Picture 2. Connection Gateway configuration settings

300 VMs or more in the AWS cloud

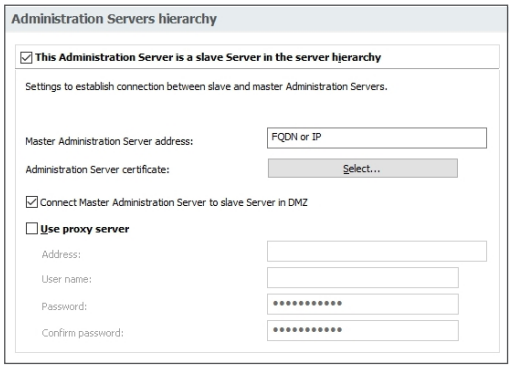
If a 'slave' Kaspersky Security Center is used, that server will centrally distribute all security policies, updates and license information to protected VMs in your AWS public cloud, after receiving everything from the 'master' server. This significantly reduces network utilization between clouds in larger-scale operations.

If you have at least 300 VMs in your public cloud, you should deploy an additional 'slave' Kaspersky Security Center rather than a Connection Gateway, ensuring sufficient redundancy to keep every VM operating securely at all times. Deploy your new 'slave' Kaspersky Security Center to an AWS cloud-based VM, using the straightforward deployment wizard.

The security of VMs in both clouds is now manageable either through your 'slave' Kaspersky Security Center or via the Connection Gateway, with all orchestration conducted through the 'master' Kaspersky Security Center inside your private cloud.

If you are using more than one public cloud in addition to your private cloud, a separate Connection Gateway or, if necessary, a 'slave' Kaspersky Security Center, should be installed onto a VM in each public cloud.

That's it – in either case, you're now ready to manage VMs in both your private and public clouds. Now you need only deploy Kaspersky Cloud Security agents onto the VMs to be protected, so our advanced security capabilities and controls can be applied and managed through your unified Kaspersky Security Center orchestration console, right across your hybrid cloud.



Picture 3. KSC with 'slave' role configuration settings

As a result:

- Setting up or propagating security policies from your private into your public cloud, configuring anti-malware database updates, monitoring security and receiving reports on all VMs together can all now be undertaken together centrally.
- Your virtual assets in the AWS public cloud are as secure as those in your private cloud environment, while your hybrid cloud infrastructure continues to operate at the highest levels of efficiency, without impacting on systems performance.
- The orchestration of your entire hybrid cloud, just like your private cloud, is conducted through a single pane-of–glass.

Hybrid Cloud Security: Multiple Public Clouds Only

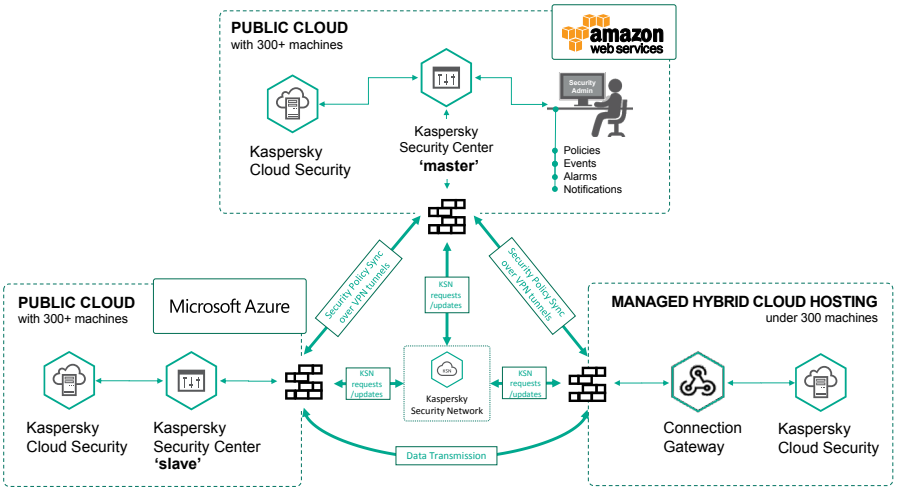
A hybrid cloud approach can comprise multiple public clouds but no private cloud, isolating the public infrastructure from the rest of IT. VMs sit in AWS and also in another public cloud or clouds, perhaps including Microsoft Azure or Managed Hybrid Cloud Hosting.

Again, **Kaspersky Cloud Security** can be used here to provide both harmonized protection capabilities and enterprise-level manageability and visibility, ensuring that regardless of public cloud location, every single VM is fully secure.

As there is no private cloud based 'master' Kaspersky Security Center already in use, there is one more step in this deployment process. You will need to install your 'master' Kaspersky Security Center onto a VM in one public cloud.

Then, just as in 'public plus private' hybrid clouds above, a Connection Gateway or, if the cloud contains more than 300 VMs, a 'slave' Kaspersky Security Center, is installed onto each other public cloud used. Finally Kaspersky Cloud Security is again installed onto every VM to be protected, in every location.

You can now manage all your VMs together in all public clouds via either a 'slave' Kaspersky Security Center or Connection Gateway, while all main security orchestration tasks are conducted through the single-pane-of-glass provided by your 'master' Kaspersky Security Center.

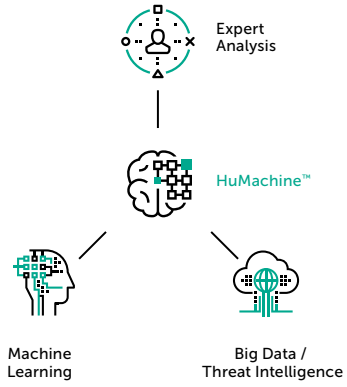


Picture 4. Hybrid cloud on multiple public clouds only

Hybrid Cloud Security Summary

Kaspersky Cloud Security solution has been engineered specifically to exploit the technological advantages that hybrid clouds offer, dynamically following infrastructure changes and delivering powerful security with optimum speed and resource efficiency. Our outstanding protection capabilities, together with unified security management for all physical and virtual endpoints, wherever they are based, enables you to roll out hybrid cloud projects at your own pace, smoothly, safely and with less pressure on IT resources.

Learn more about Kaspersky Cloud Security at
www.kaspersky.com/cloud-security



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

#truecybersecurity
#HuMachine

www.kaspersky.com