Kaspersky Managed Service Providers Program

Technical Reference Guide

www.kaspersky.com
#truecybersecurity

Table of contents

Program benefits

- **Flexible licensing** allow you to choose between a monthly subscription and an annual license. Because you own the product license, there's no need to spend time administrating contract renewals with customers — extending licenses is easy; no special action is required.

- **Increase sales revenues** with volume-based discounts — the more customers you have, the less you pay. Pricing depends on the total number of devices of all customers. Sell more and gain bigger discounts.

- **Be even more efficient and grow your client base without having to hire additional engineers.** With built-in best practices that drive operational efficiency, you'll improve your tech-to-device ratio and boost your bottom line. Increase your scalability and protect more endpoints with fewer headaches.

- **Improved usability.** Kaspersky Lab understands the importance of ease of use when it comes to security, and our design and usability specialists are closely involved in product development. By optimizing ease of use, we simplify the daily routine of IT administrators.

- **Fast start** with sales and technical security training. Position your business as a strategic security partner — we'll help you every step of the way. Access trial licenses to test and prove the quality of our solutions.

- **Become an SLA legend** and build trusting relationships with customers by providing first-line support. Kaspersky Lab standard and premium support options mean you'll always have access to fast resolution on critical issues, 24/7. Five premium support incidents are included with the MSP program (you can purchase more incidents if required).

- **Comprehensive partner sales and marketing materials**, including Kaspersky partner logo, email templates, sales guide and training, presentations and product collateral help you sell your services to existing customers and grow your new customer base.

MSP program requirements

Kaspersky Lab's MSP Program was created exclusively for our service provider partners. New partners need to complete the registration process; for existing partners who want to register as service providers, you can get MSP specialization. Both can be done on our partner portal: https://www.kasperskypartners.com/.

To become a Kaspersky Lab MSP partner, companies must meet the following requirements:

1. **You provide IT services to your customers**
   During the registration process you will be asked how many customers and nodes you manage and what IT services you provide to customers. Kaspersky Lab does not request detailed information about your customers. We respect your — and your customers' — privacy. You also need to accept our agreement on the partner portal.

2. **There must be a Kaspersky Lab integrated distributor available in your market**
   We have identified distributors working with service providers in your region and integrated with them to automate licensing and billing. You can find the list of distributors in your region on the partner portal.

3. **You provide first-line support to your customers**
   We'll help with technical training and a limited number of free premium supports for critical cases. Your technicians should complete the technical training before you start selling security services.

Products

Extend your managed service offerings with new security services built on Kaspersky Lab products:

Kaspersky® Endpoint Security for Business

Advanced

Combining Next Generation security and flexible role-based management to enforce IT policies across endpoints and servers.

- Vulnerability scanning and patching help to substantially eliminate attack entry points.
- Extended management features and resource-optimized server protection drive efficiency, regardless of platform or Internet connection.
- Cloud-enabled controls for businesses of all sizes lower exposure to attack on servers and workstations.
- Integrated encryption safeguards sensitive data and helps satisfy regulatory requirements.
- Automated cloning of secured system images saves time spent rolling-out systems and updating software.

Kaspersky® Endpoint Security for Business

Select

Low footprint, high-performance protection. Powered by HuMachine™ intelligence for strong, Next Generation security for any environment.

- Centralized web, application and device controls reduce attack surfaces while mobile device management extends True Cybersecurity into the mobile platform.
- Multiple layers of protection, powered by machine learning, stop ransomware, exploits and future threats in their tracks.
- All security functions are controlled via a single management console that also acts as a central point for managing many other Kaspersky Lab applications.

Kaspersky® Endpoint Security Cloud

Protection that's quick to roll out, easy to run and requires no additional hardware or software investment.

- Manage security for multiple endpoints, mobile devices and file servers remotely, from anywhere, with our web-based cloud console.
- Default security profile developed by Kaspersky Lab experts provide immediate protection while the centralized console enables flexible, simple administration capabilities. All you have to do to get started with Kaspersky Endpoint Security Cloud is register at cloud.kaspersky.com.
- No additional or new security tasks to manage — once the endpoint protection application is installed on a device, it automatically connects to the management console and receives the default security profile. Windows computers and file servers, Mac, iOS and Android devices are all supported.
- Multi-tenancy allows easy management of multiple companies within the same account. If your customer wants to view the security settings of their company, just add an additional administrator for a particular company's workspace.

Kaspersky® Hybrid Cloud Security for Azure

A flexible solution with multi-tenancy support that delivers superior protection for physical, virtual and public cloud workloads.

- The successor to Kaspersky Security for Virtualization, Kaspersky Hybrid Cloud Security supports tight integration with major virtualization platforms and public cloud APIs.
- Delivers the right balance of protection and efficiency for every scenario, enabling service providers to manage client risks without diluting the benefits.
- In addition to ongoing support for VMware vShield and VMware vCNS, Kaspersky Hybrid Cloud Security fully supports NSX technology, adding more capabilities such as advanced network security, flexible reconfiguration and micro-segmentation support to multi-layered threat protection and system hardening.
- Leverages powerful workload discovery and management capabilities offered by integration with public cloud APIs.
- Protects Docker and Windows Server 2016 containers.

Feature comparison across applications:

	Kaspersky Endpoint Security Cloud	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Hybrid Cloud Security	Kaspersky Hybrid Cloud Security Enterprise
Anti-malware	✓	✓	✓	✓	✓
Firewall	✓	✓	✓	✓	✓
Application Control for workstations		✓	✓		✓
Application control for servers			✓		✓
Web Control	✓	✓	✓	✓	✓
Device Control	✓	✓	✓	✓	✓
Network Threat Protection	✓	✓	✓	✓	✓
File Integrity Monitoring (FIM)					✓
Log inspection					✓
Windows support	✓	✓	✓	✓	✓
Mac support	✓	✓	✓		
Linux support		✓	✓	✓	✓
iOS support	✓	✓	✓		
Android support	✓	✓	✓		
Ransomware protection	✓	✓	✓	✓	✓
Cloud-based management console	✓				
On-premises management console		✓	✓	✓	✓
Vulnerability and patch management			✓		
SIEM integration			✓	✓	✓
Encryption			✓		
Client management tools			✓		
ConnectWise Automate integration	✓	✓	✓		
ConnectWise Manage integration	✓	✓	✓		
Autotask integration	✓	✓	✓		
Tigerpaw integration	✓	✓	✓		

Kaspersky® Security for Microsoft Office 365

Effective protection for Office 365 email.

- Moving processes into the cloud brings flexibility and resource efficiency, but it requires more security in addition to what's already offered by the platform – especially when it comes to dealing with spam and malware. Using advanced heuristics, sandboxing, machine learning and other next-generation technologies, Kaspersky Security for Microsoft Office 365 protects mail from spam, phishing, malicious attachments and unknown threats.
- The cloud-based console allows service providers to manage clients' mail security easily while benefitting from the convenience of a single entry point shared with Kaspersky Endpoint Security Cloud at cloud.kaspersky.com.

Kaspersky® Security for Exchange Mail Server

Protects internal and remote users (laptops, tablets and smartphones) from email attacks including spam, phishing and generic and advanced malware threats.

- Real-time anti-malware protection of customers' e-mail systems, supported by the cloud-assisted Kaspersky Security Network.
- User-friendly management tools, information on mail protection status, flexible settings for scans and reporting.
- Optimized reliability and performance help to minimize impact on essential business processes.
- Independently manage multiple customers or offices from the same console and account.

Kaspersky® Security for Internet Gateway

Robust web traffic protection

- Blocks web-based endpoint threats, including those based on social engineering and vulnerability exploitation.

Reduces risks and optimizes performance

- Embedded web control helps govern access to inappropriate Internet resources – reducing your risk of infection, your traffic loads and your employees' exposure to online distractions.

Durable and scalable

- A crash-proof failover architecture is supported by clustering, allowing for easy adjustment as traffic loads increase.

Convenient multi-tenancy

- Independent workspace management and role-based access control enables convenient management of multiple tenants' web gateway security from a single- view console.

Training and certification

Kaspersky Lab expects partners participating in the MSP Program to provide initial technical support to their customers. To better prepare you for this responsibility, technical training and certification is available. Training and certification can be found on the Kaspersky Lab Partner Portal: www.kasperskypartners.com

MSP partners must complete the following two compulsory trainings:

1. MSP sales training
2. Technical training, to include one of the following:
   - KL 002.104 Kaspersky Endpoint Security and Management - Fundamentals
   - KL 040.30 Kaspersky Endpoint Security Cloud

Professional services

There are certain situations where professional services are necessary. Time constraints and gaps in knowledge are two areas where engaging professional services may be required. Kaspersky Lab's Professional Services Team will assist with every aspect of deploying, configuring and upgrading Kaspersky Lab products. Kaspersky Lab Professionals Services include the following fee-based options for Managed Service Providers:

Kaspersky® Consultancy Service

On-site or remote assessment with customized service, which may include best practices, advice, specific education or troubleshooting to ensure that you're deriving maximum benefit from your Kaspersky Lab products. This service is typically dedicated to assist customers in large projects and with on-going operational support and maintenance of the implemented solution.

Kaspersky® Configuration Service

On-site or remote assessment with configuration of Kaspersky Lab products based on customer requirements, security policies and environment analysis to ensure the most effective Kaspersky Lab products configuration and policy settings. This service is also applicable for individual components of our products.

Kaspersky® Health Check Service

On-site or remote assessment of your current implementation and configuration of Kaspersky Lab security and systems management products. The service includes a detailed report and recommendations on how to improve your security and/or systems management efficiency, using the latest Kaspersky Lab security and systems management products.

Kaspersky® New StartUp Service

On-site or remote design, deployment and configuration of your chosen Kaspersky Lab security and/or systems management products.

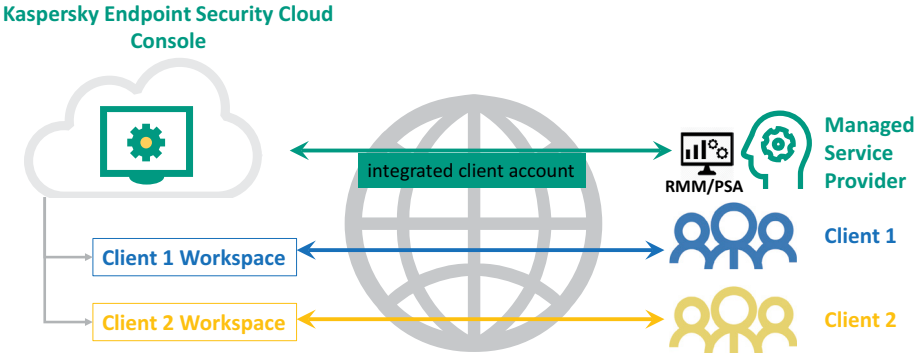
Kaspersky® Upgrade Service

On-site or remote upgrade of your existing Kaspersky Lab security and/or systems management products.

Technical designs

Kaspersky Endpoint Security Cloud

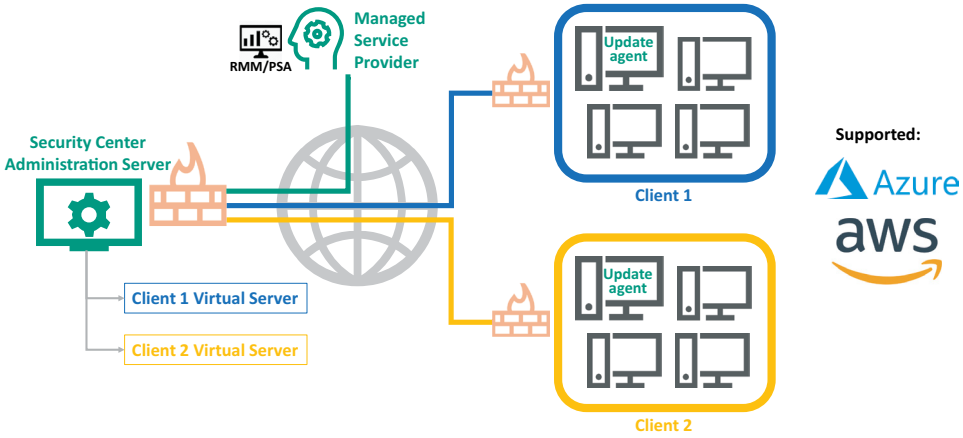
Kaspersky Endpoint Security Cloud offers endpoint protection and security management capabilities for different platforms, managed from a web-based cloud console and hosted by Kaspersky Lab. MSPs can create separate workspaces for each customer where deployment, protection and monitoring can be centrally managed.



Kaspersky Endpoint Security for Business Select and Kaspersky Endpoint Security for Business Advanced

Single-server environment with multi-tenancy – recommended for 1000 or fewer endpoints

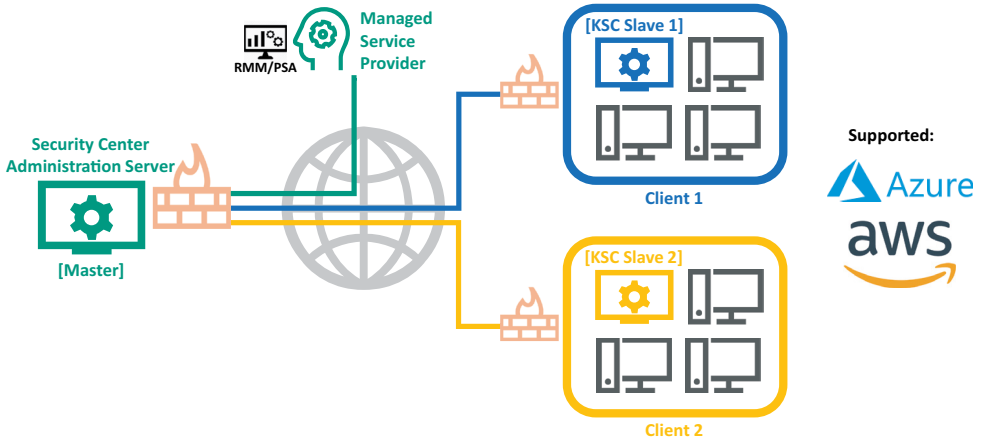
This design uses Virtual Administration Servers as part of the multi-tenant environment. We recommend that customers use Update Agents to localize signature updates and installation packages for deployment.



Multi-server environment – recommended for 1000+ managed endpoints, or for individual customers with more than 100 endpoints

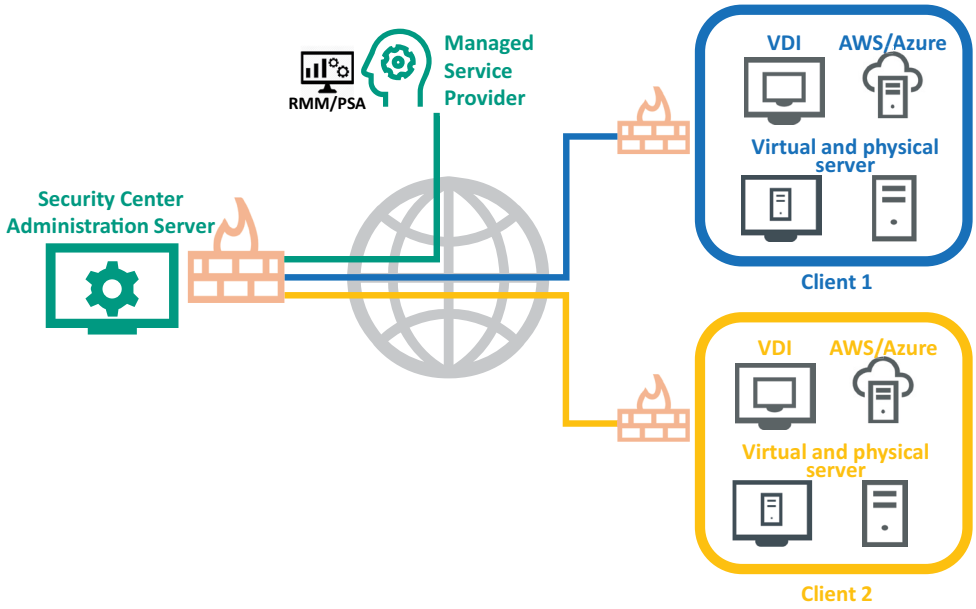
This design uses a Security Center Administration Server installation in each customer's network. These Slave servers connect back to the Master located in the partner's datacenter. Update Agents can still be used for larger networks but in most cases with this configuration the Slave Security Center Server acts as the repository for signature updates and installation packages.

As well as securing all your endpoints and servers, the **Advanced** license delivers extra security layers to protect sensitive data and eliminate vulnerabilities – and it helps simplify systems management tasks too.



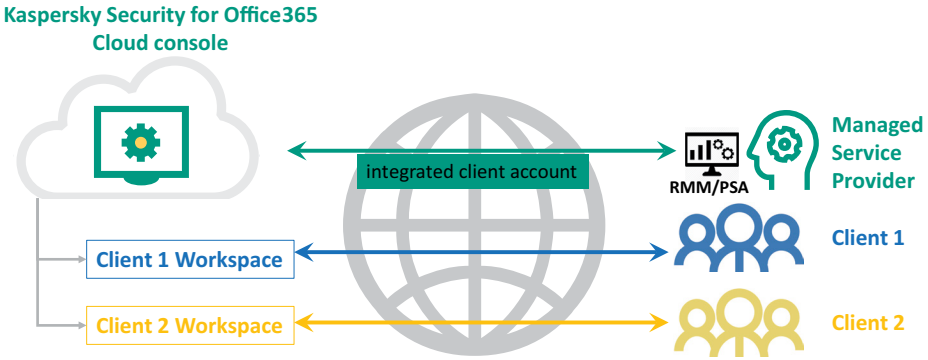
Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security protects applications and data on physical, virtual and cloud workloads, ensuring business continuity and accelerating compliance across your entire multi-cloud environment. Kaspersky Hybrid Cloud Security helps you create perfectly orchestrated and adaptive cybersecurity ecosystem that delivers the capabilities your multi-cloud workloads require without compromising on resource efficiency.



Kaspersky Security for Microsoft Office 365

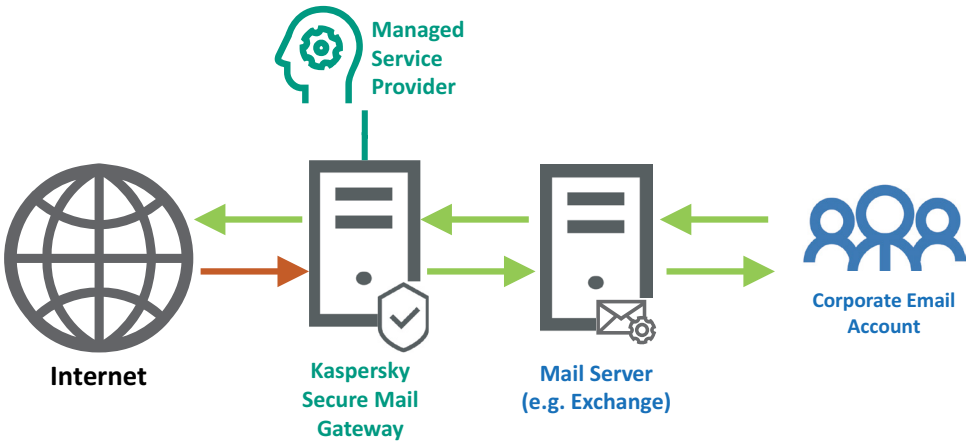
Protects Exchange Online mailboxes that are managed through Microsoft Office 365. Email messages are scanned for viruses, Trojans and other types of malware that are transmitted by email, as well as spam and phishing.



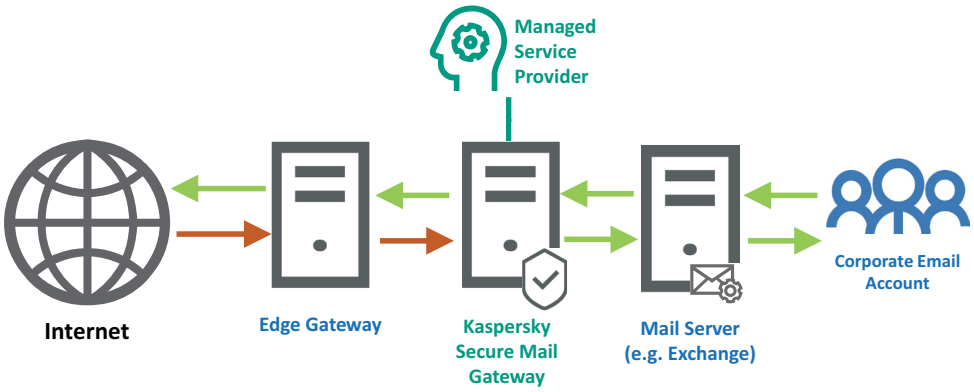
Kaspersky Security for Mail Server

Kaspersky Security for Mail Server protects mail on the latest versions of major mail and collaboration platforms – including Microsoft Exchange and Linux-based mail servers.

Direct Integration



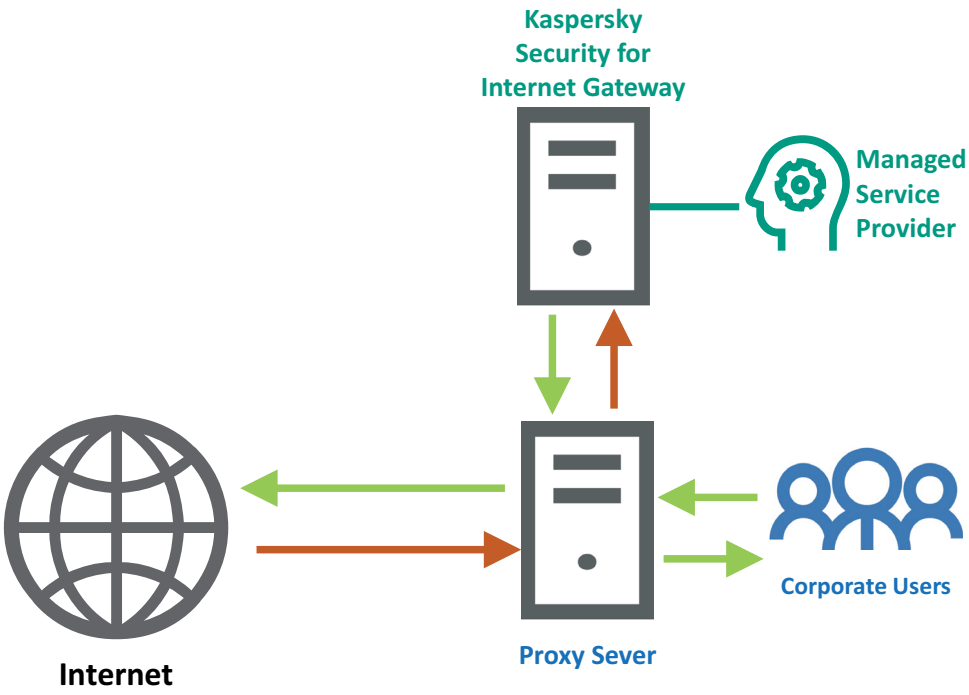
Integration through Edge Gateway



Kaspersky Security for Internet Gateways

Kaspersky Security for Internet Gateways exploits the role of the proxy server for web traffic passing between the corporate infrastructure and the outside world, protecting the corporate IT network.

When added to your existing protective infrastructure, Kaspersky Security for Internet Gateways reduces the risk of compromise, stopping incoming threats at gateway level and preventing them from reaching your endpoints



Customer onboarding checklist

Completed
FOR ALL DEPLOYMENTS
Confirm license availability
Create customer workspace
FOR KES CLOUD DEPLOYMENTS
Remove incompatible applications
Install Kaspersky Endpoint Security
FOR KESB SELECT and ADVANCED DEPLOYMENTS
Install Security Center Network Agent
Remove incompatible applications
Install Kaspersky Endpoint Security
Configure Update Agents (where applicable)
FOR KHCS DEPLOYMENTS (Private Cloud)
In the case of virtual infrastructure (hypervisors), deploy Kaspersky Virtual Appliance and configure virtual machines to communicate with the virtual appliance (VMWareTools or Light Agent Deployment)
In the case of physical servers, install Security Center Network Agent, remove incompatible applications and install Kaspersky Security for Windows Server or/and Kaspersky Endpoint Security for Linux
FOR KHCS DEPLOYMENTS (Public Cloud)
Prepare the AWS or Azure environment for KHCS deployment - create the necessary security groups and accounts
Install Security Center Network Agent, remove incompatible applications and install Kaspersky Security for Windows Server or/and Kaspersky Endpoint Security for Linux
REMAINING TASKS FOR ALL DEPLOYMENTS
Tune protection policies
Tune scan tasks
Monitor reports and events

Appendix A

Network ports used by Kaspersky Security Center

Port Number	Protocol	Description
8060	HTTP	Required for connecting to the web server, which allows you to manage the Kaspersky Security Center Web Console and organize the internal company portal.
8061	HTTPS	Required for connecting to the web server, which allows you to manage the Kaspersky Security Center Web Console and organize the internal company portal. The connections are encrypted.
13000	TCP	• Receiving data from client computers • Connecting Update Agents • Connecting slave Administration Servers using the secure SSL connection • Used by client computers when connecting to Update Agents
13000	UDP	Required for reporting on computers' shutdown
13111	TCP	Required for connecting to the KSN proxy server
13291	TCP	Required for the SSL connection between the Administration Console and the Administration Server.
13292	TCP	Required for connecting mobile devices.
14000	TCP	• Receiving data from client computers • Connecting Update Agents • Connecting slave Administration Servers without using the SSL connection • Used by client computers when connecting to Update Agents
14001	TCP	Used by client computers to connect to the Update Agent (if a computer with Administration Server installed serves as the Update Agent).
15000	UDP	Used by client computers for receiving a request to connect to the Administration Server, which receives the information about the computer in the real-time mode.
17000	TCP	Required for secure SSL connection to the activation proxy server.
17100	TCP	Required to connect to the activation proxy server when activating mobile hosts.

Network ports used by Kaspersky Endpoint Security Cloud

Port Number	Protocol	Description
443	TCP	• To connect to the Kaspersky Endpoint Security Cloud portal • To sign in to the Kaspersky Endpoint Security Cloud portal
13000	TCP	To manage: • Kaspersky Endpoint Security for Windows • Kaspersky Endpoint Security 10 for Mac
13292	TCP	To manage: • Kaspersky Endpoint Security for Android • Kaspersky Safe Browser for iOS
9443	TCP	To manage iOS MDM
8081	TCP	To download installation packages
443/8080	TCP	To connect to the KES Cloud Management Console

Appendix B

Using Kaspersky Security Center for Licensing

Licensing is a critical part of ensuring uninterrupted protection and avoiding problems due to expiry or blacklisted licenses. The main purpose of this capability is to provide the administrator with an automated tool to manage security application licenses.

1. You can deploy and configure Kaspersky Security Center to accurately maintain your licenses. Follow the steps below to install Kaspersky Security Center and monitor your protected endpoints for licensing purposes only.

2. Install Kaspersky Security Center Administration Server

3. Add the activation code to Security Center

4. Configure your perimeter security to allow communication between Security Center and Kaspersky Security Center Network Agent via the necessary networks ports.

5. REMOVE the Kaspersky Endpoint Security for Windows Protection Policy from the Managed Computer Group to prevent any issues with protection policy settings already configured for the endpoints.

6. Create a Virtual Admin Server for each customer

7. Create a stand-alone package for the Kaspersky Security Center Network Agent for each customer workspace.

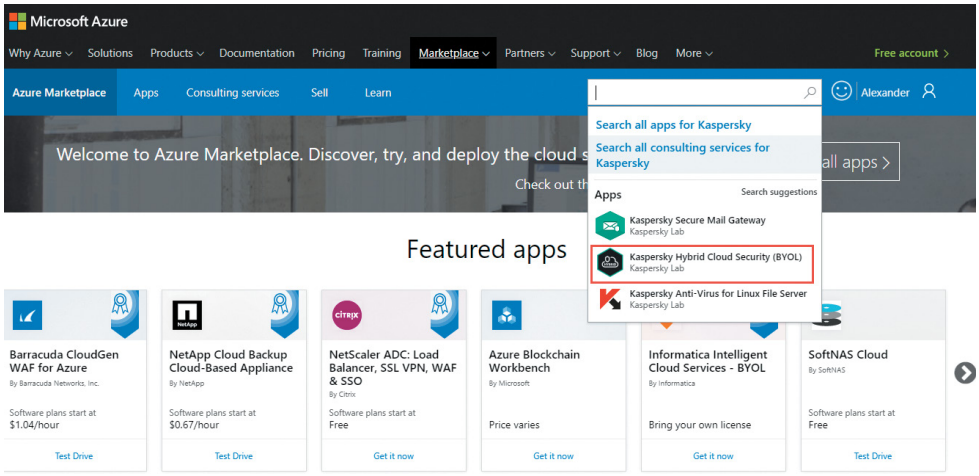
8. Deploy it to all protected endpoints using standard Kaspersky Security Center methods or third-party tools.

9. Confirm that Kaspersky Security Center Network Agents are actively communicating with the Kaspersky Security Center.

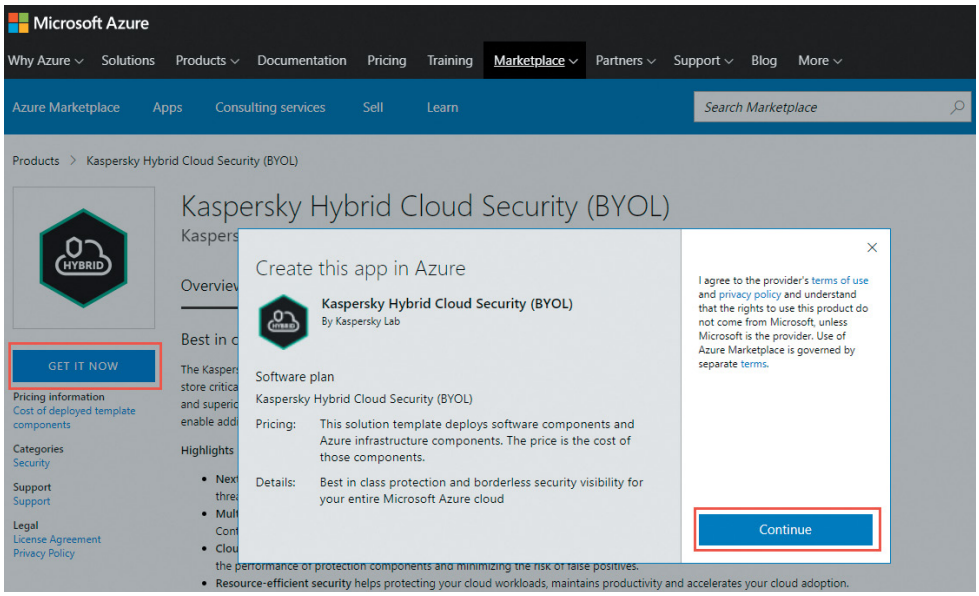
Appendix C

Deploying Kaspersky Security Center in AZURE

1. Log in to the **Microsoft Azure Marketplace** https://azuremarketplace.microsoft.com. In the **Search toolbar**, search for **Kaspersky Hybrid Cloud Security**, then choose **Kaspersky Hybrid Cloud Security (BYOL)** application.

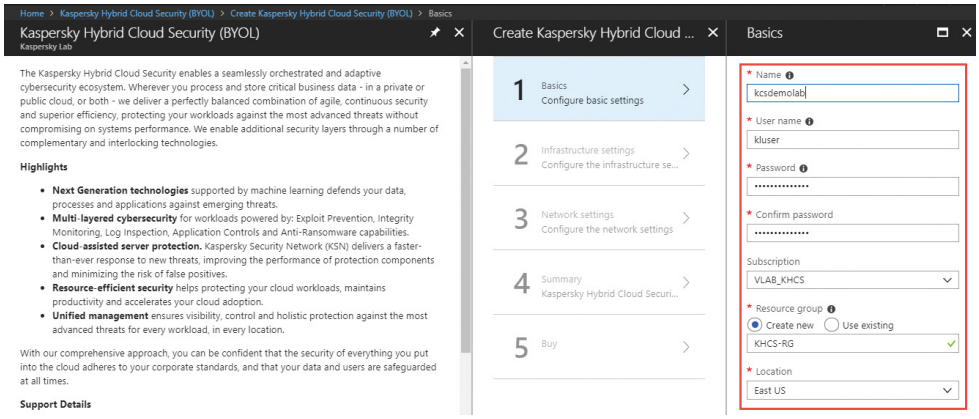


2. Click **GET IT NOW**, and then **Continue**. You will be forwarded to the **Microsoft Azure Portal** for subsequent KSC configuration.



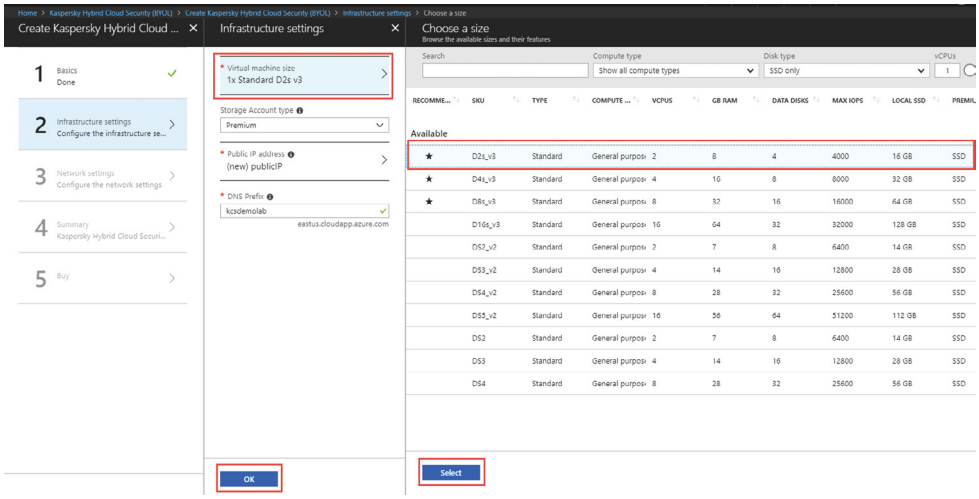
3. In the Microsoft Azure Portal, click Create and specify the basic settings of Kaspersky Security Center and then click **Ok**.

Here you'll need to enter a **name** for the VM (this host name will appear in the Azure Console), **Username** and **password** for the VM administrator, valid **subscription** and **Resource Group** and **Location**.

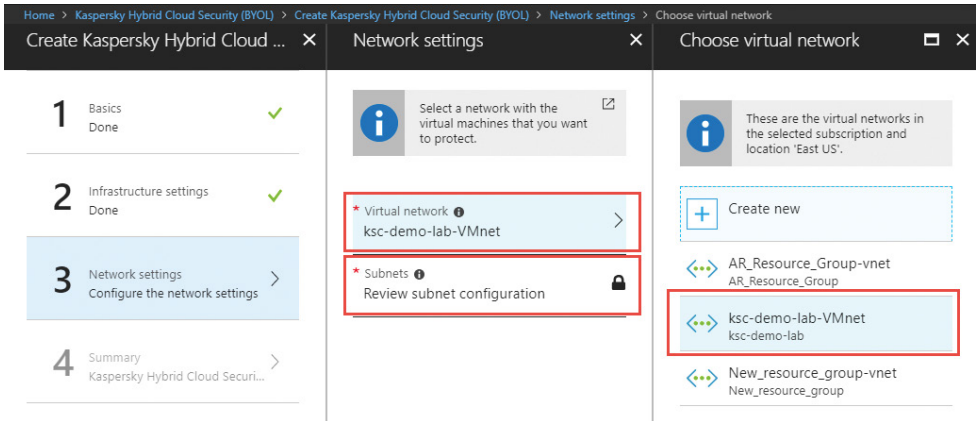


– Then choose the size of VM. For Proof of Concepts (PoC), the first available size will be enough.

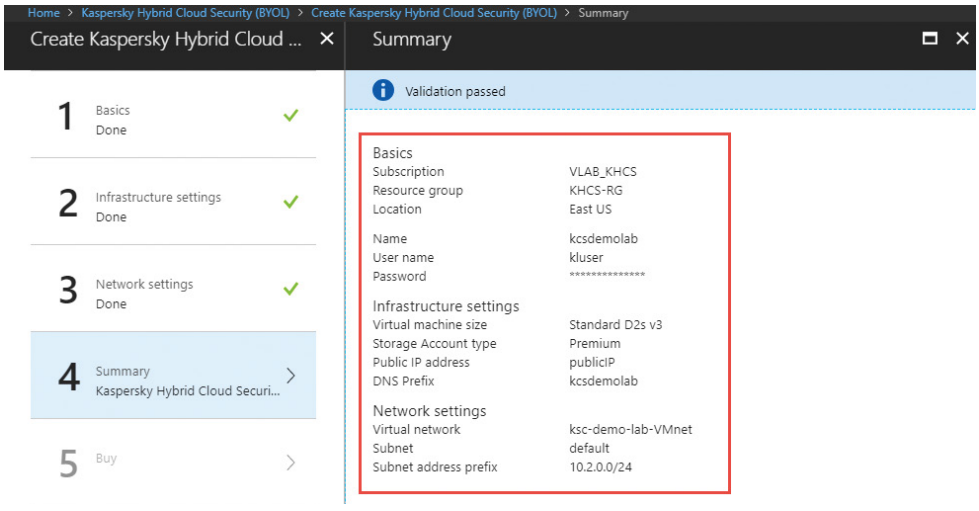
Keep the other settings as default, click **Select** and then **Ok**.



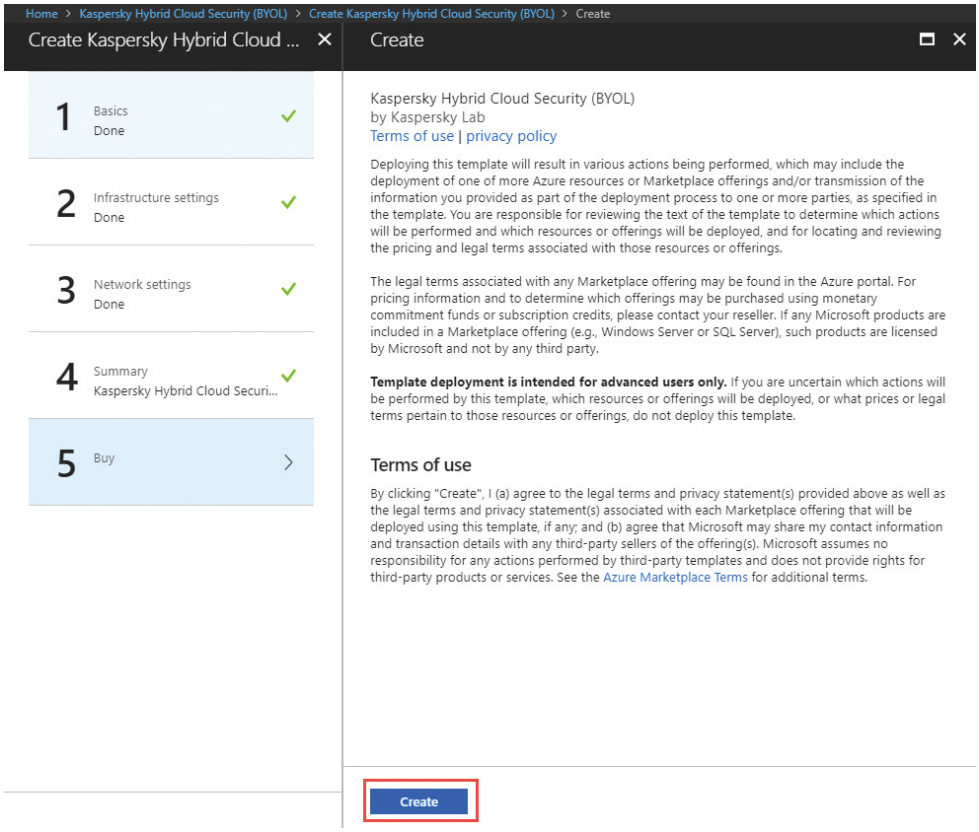
4. Choose a **Virtual Network** and click **Ok**.



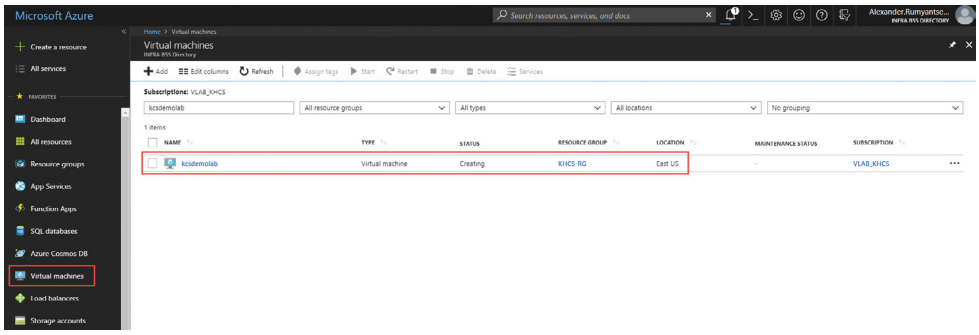
5. Review the summary.



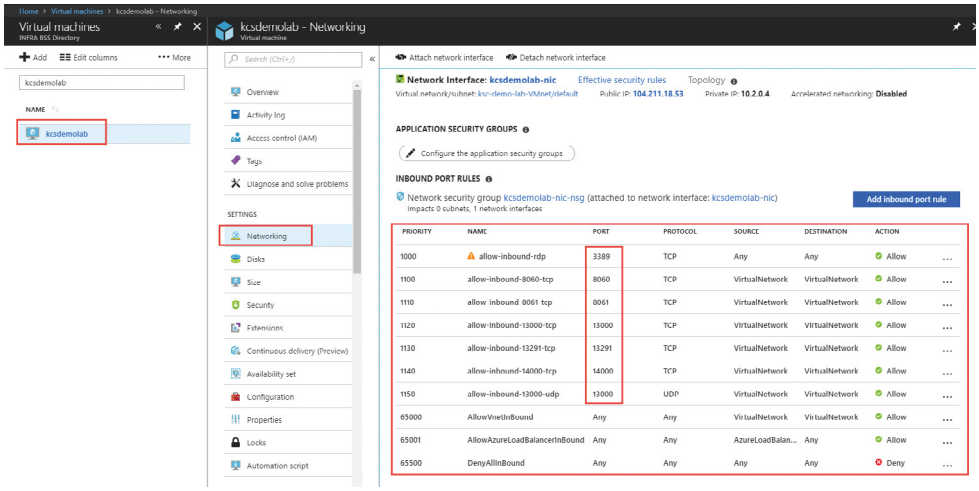
6. Read the Terms of Use. The process of creating the KSC Virtual Machine starts once you click **Create**.



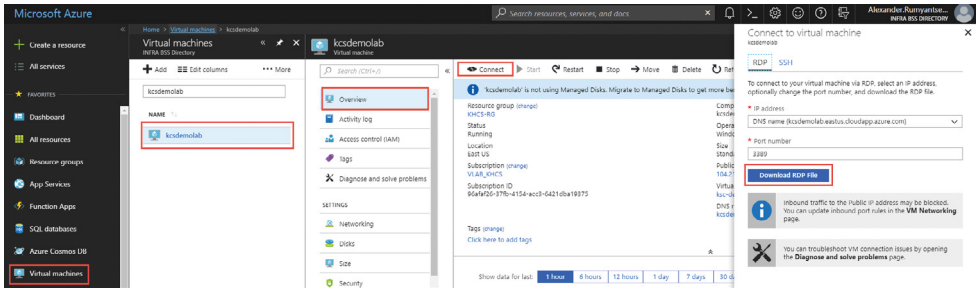
7. Open the **Virtual Machines** tab and verify that the **new KSC Virtual Machine** appears with the status **Creating**.



8. Verify that all the necessary **TCP/UDP ports** for this KSC VM **are open**. Click the KSC Virtual Machine and go to **Networking** settings.



9. Once the Kaspersky Security Center VM has been created and powered on, you can connect to it via RDP - click **Overview and then click Connect. Now download the RDP file.** Open the downloaded RDP file, input the **username** and **password** you set previously and connect to the KSC VM.

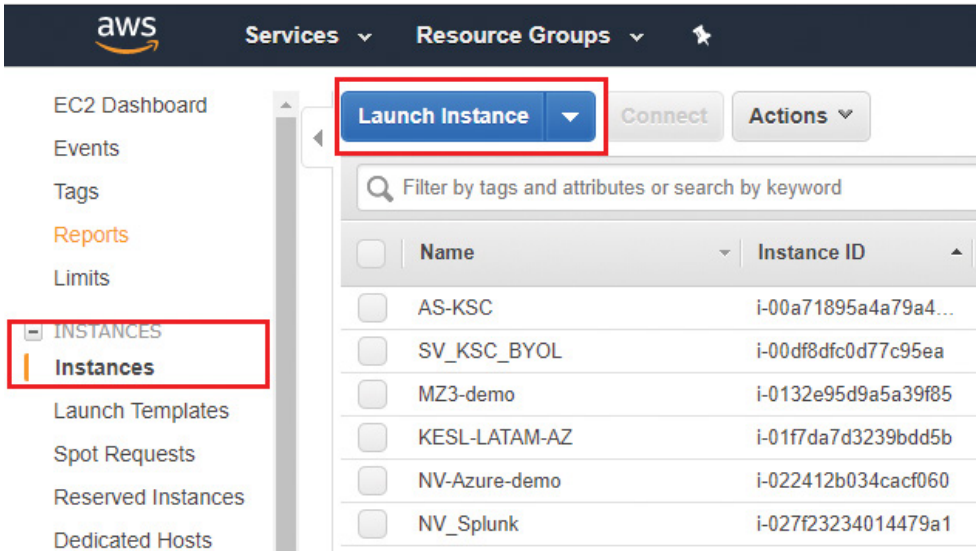


10. When you connect to the Administration Server, the KSC Console and the Quick Start Wizard will launch automatically. Follow the wizard and set up the Kaspersky Security Center according to your needs. When that's done, you can start deploying and managing your system.

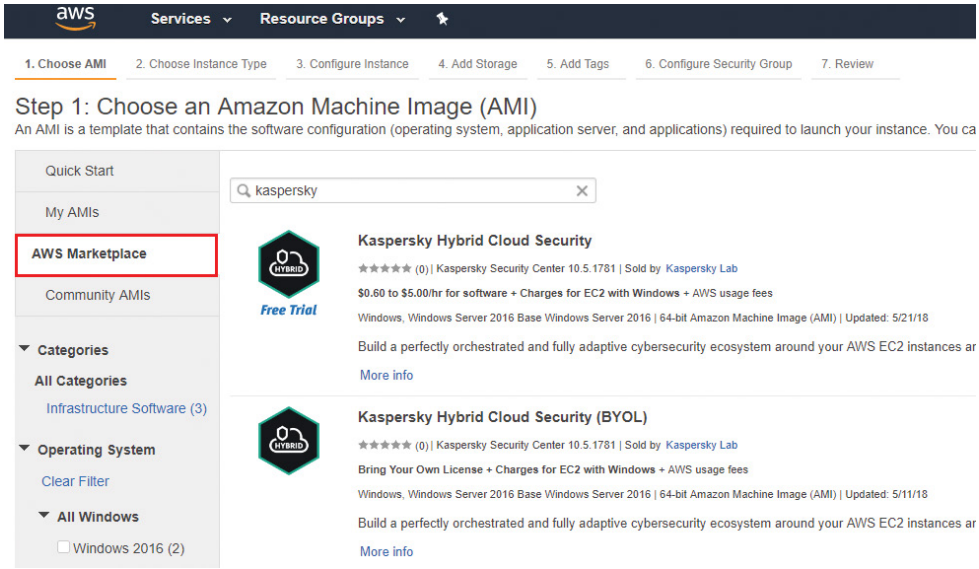
Appendix D

Deploying Kaspersky Security Center in AWS

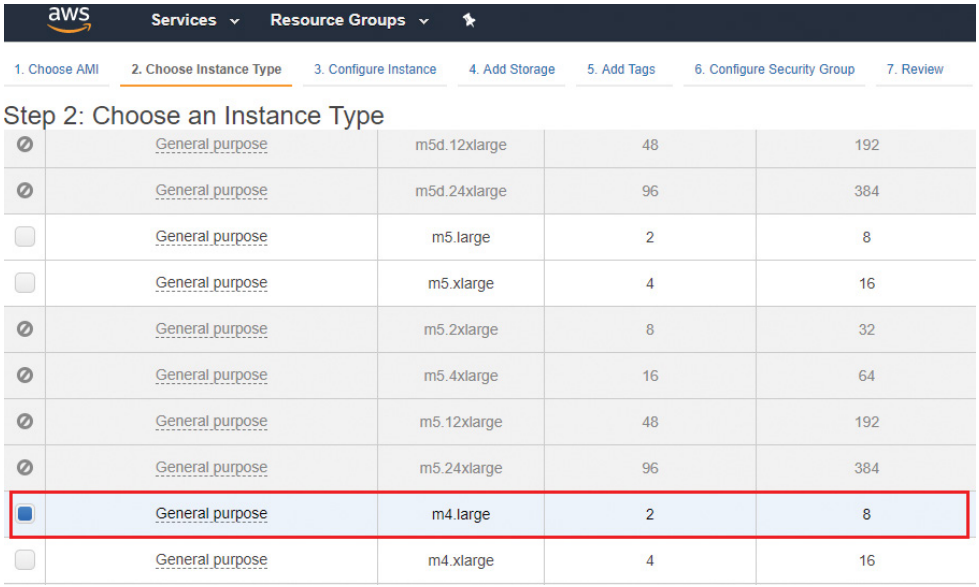
1. Log in to the **Amazon AWS Console**. Go to **EC2 – INSTANCES – Instances**. In the right pane, click L**aunch Instance**.



2. On this step, **choose an Amazon Machine Image (AMI)** page, switch to the **AWS Marketplace** tab and search for **Kaspersky**. Then select **Kaspersky Hybrid Cloud Security (BYOL)**. Read the description of the AMI and click Continue.

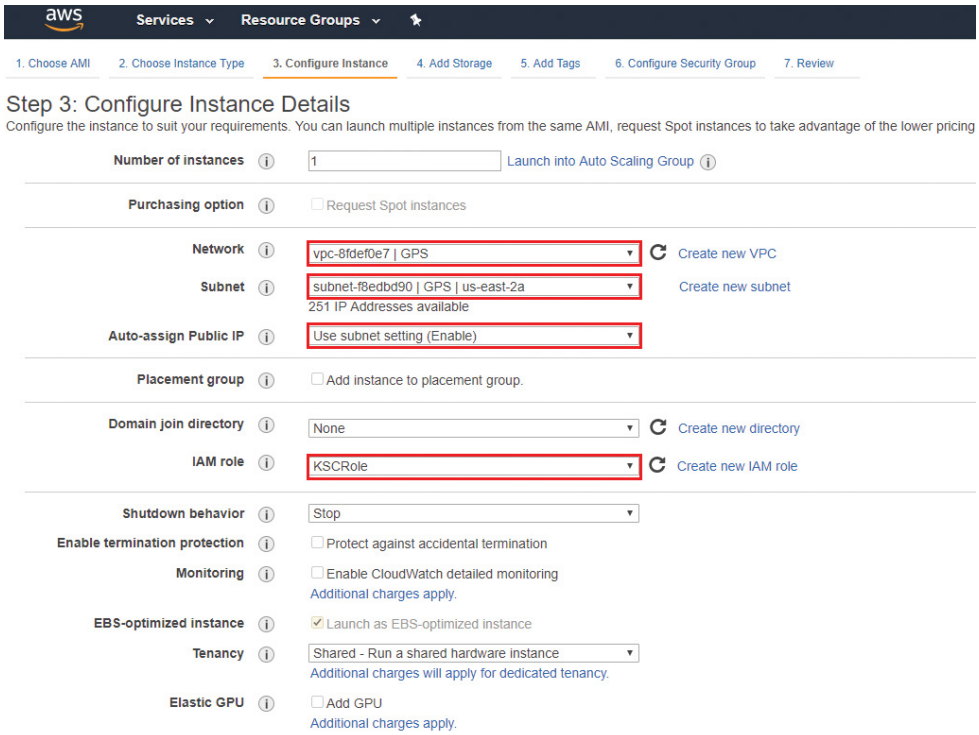


3. Choose an instance type and click **Next: Configure Instance Details**.

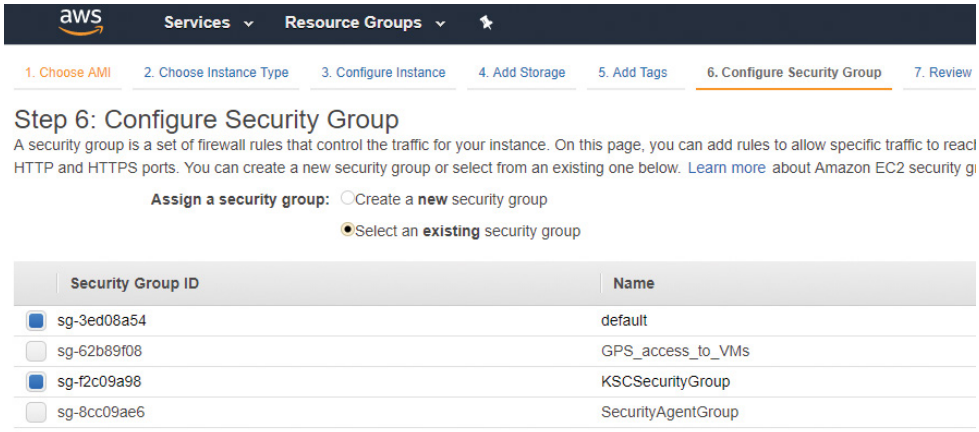


⊘	General purpose	m5d.12xlarge	48	192
⊘	General purpose	m5d.24xlarge	96	384
☐	General purpose	m5.large	2	8
☐	General purpose	m5.xlarge	4	16
⊘	General purpose	m5.2xlarge	8	32
⊘	General purpose	m5.4xlarge	16	64
⊘	General purpose	m5.12xlarge	48	192
⊘	General purpose	m5.24xlarge	96	384
☑	General purpose	m4.large	2	8
☐	General purpose	m4.xlarge	4	16

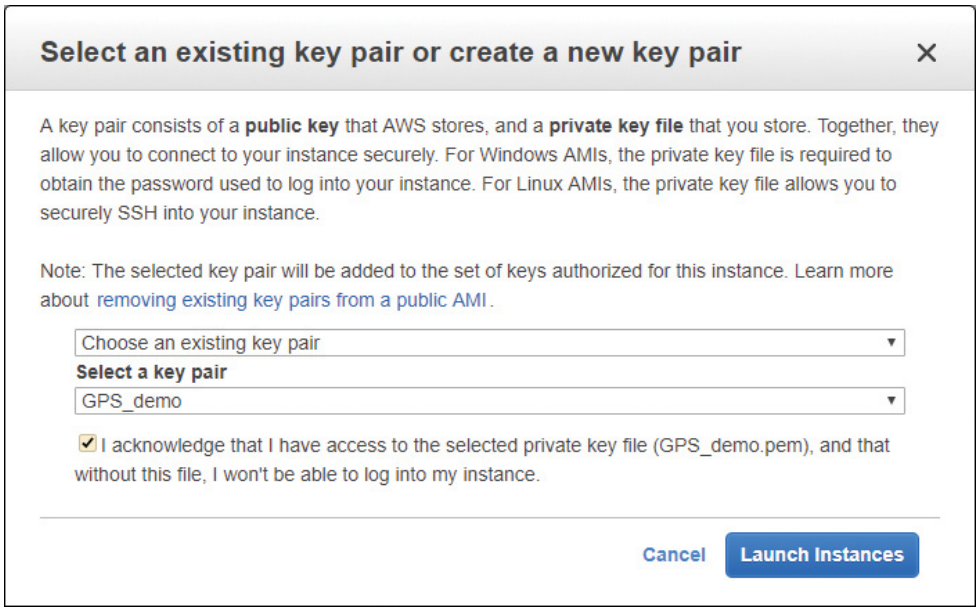
4. Select your VPC in the **Network, Subnet, IAM Role** for KSC and specify **Auto-assign Public IP** to connect to the VM. After that, click **Next: Add Storage**.



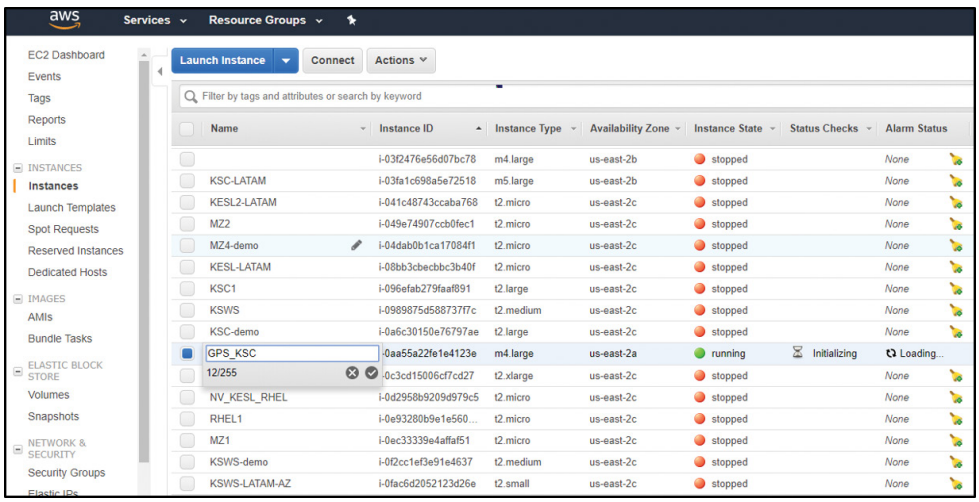
5. On this step **Add Storage** and on the next page **Add Tags**. **Don't** change any settings - then proceed to the next step: **Configure Security Group**. You can create a new security group with pre-configured open ports in this AMI or select an existing security group. In this guide, we will use a previously created security groups – **KSCSecurityGroup**. This provides access to KSC via RDP, so in addition to this group you just need to add a group, which provides stable Internet and internal communication. After you define security groups, click **Review and Launch**.



6. Select an existing key pair or create a new key pair to connect to the VM. Click **Launch Instances** and on the next page click **View Instances**.

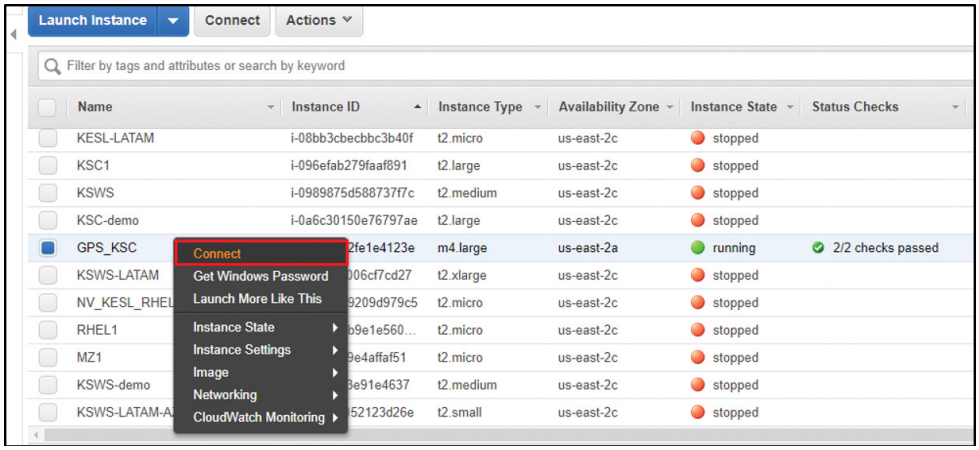


7. Find the new instance and assign a name. Wait for the instance to launch. The following values should be displayed: **Instance state: running. Status Checks: 2/2 checks passed**.

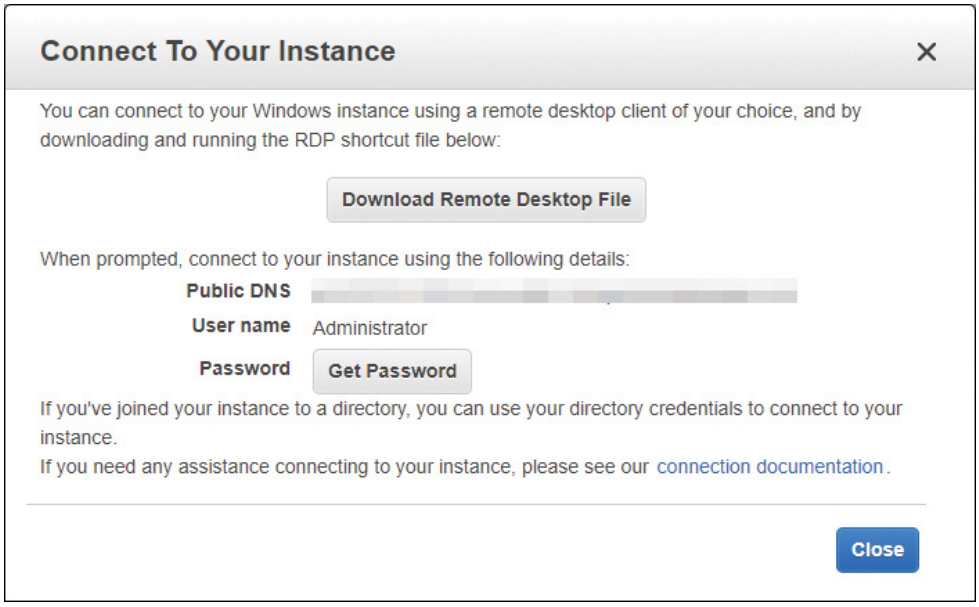


Kaspersky Security Center configuration

1. When the KSC AMI is ready, right-click on it and click **Connect**.



2. Click **Get Password** and decrypt the password with the EC2 key pair, created previously. Then download Remote Desktop File and connect to the VM.



3. Wait for the KSC installation to finish. The KSC Console will be launched automatically. When you connect to the Administration Server, Cloud Environment Configuration Wizard will start. Follow the wizard and set up the Kaspersky Security Center according to your needs. When that's done, you can start deploying and managing your system.

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