Kaspersky for Business

KASPERSKY[®]



Kaspersky Managed Service Providers Program

Technical Reference Guide

www.kaspersky.com #truecybersecurity

Table of contents

Program benefits
MSP program requirements
Products
Training and certification
Professional services
Technical designs
Kaspersky Endpoint Security Cloud
Kaspersky Endpoint Security for Business Select6
Kaspersky Endpoint Security for Business Advanced6
Kaspersky Hybrid Cloud Security
Kaspersky Security for Microsoft Office 3658
Kaspersky Security for Mail Server
Kaspersky Security for Internet Gateways
Customer onboarding checklist
Appendix A
Appendix B
Appendix C
Appendix D

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



Kaspersky® Endpoint Security for Business Select



Kaspersky® Endpoint Security Cloud



Kaspersky® Hybrid Cloud Security for Azure 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.

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.

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.

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	✓	✓	 Image: A set of the set of the	×	✓
Firewall	 Image: A set of the set of the	✓	×	✓	 Image: A second s
Application Control for workstations		~	~		~
Application control for servers			×		 Image: A second s
Web Control	 Image: A second s	✓	×	×	 Image: A second s
Device Control	 Image: A set of the set of the	✓	 Image: A second s	×	 Image: A set of the set of the
Network Threat Protection	✓	✓	×	 ✓ 	 Image: A second s
File Integrity Monitoring (FIM)					✓
Log inspection					 Image: A set of the set of the
Windows support	 Image: A second s	✓	×	×	 Image: A second s
Mac support	 Image: A second s	✓	 Image: A second s		
Linux support		✓	×	~	 Image: A set of the set of the
iOS support	✓	~	×		
Android support	 Image: A second s	✓	×		
Ransomware protection	 Image: A set of the set of the	✓	×	 ✓ 	 Image: A second s
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	×	×	×		

\wedge	Kaspersky	Effective protection for Office 365 email.
	Security for Microsoft Office 365	 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 <u>cloud.kaspersky.com</u>.
	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

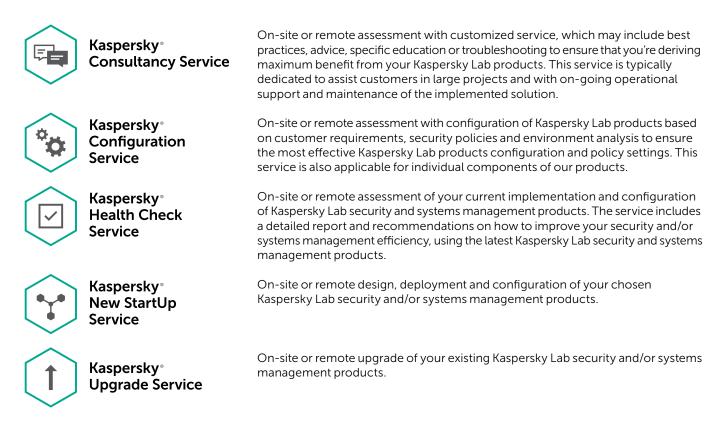
Kaspersky Lab expects partners participating in the MSP Program to provide initial technical support to their customers. To better prepare you for this responsibility, technical training and certification is available. Training and certification can be found on the Kaspersky Lab Partner Portal: www.kasperskypartners.com

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

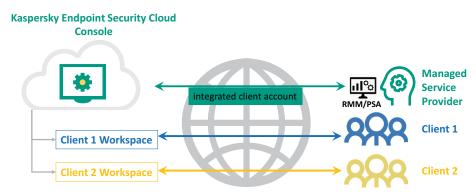
There are certain situations where professional services are necessary. Time constraints and gaps in knowledge are two areas where engaging professional services may be required. Kaspersky Lab's Professional Services Team will assist with every aspect of deploying, configuring and upgrading Kaspersky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



Technical designs

Kaspersky Endpoint Security Cloud

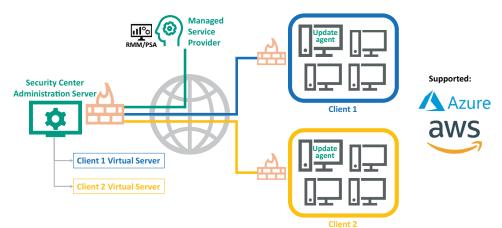
Kaspersky Endpoint Security Cloud offers endpoint protection and security management capabilities for different platforms, managed from a web-based cloud console and hosted by Kaspersky Lab. MSPs can create separate workspaces for each customer where deployment, protection and monitoring can be centrally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

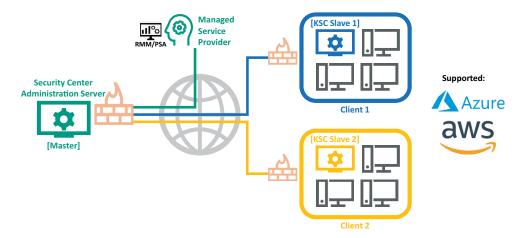
This design uses Virtual Administration Servers as part of the multi-tenant environment. We recommend that customers use Update Agents to localize signature updates and installation packages for deployment.



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

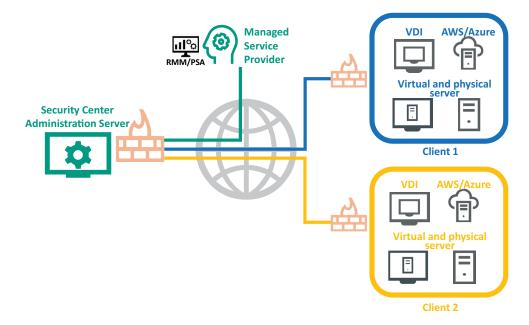
This design uses a Security Center Administration Server installation in each customer's network. These Slave servers connect back to the Master located in the partner's datacenter. Update Agents can still be used for larger networks but in most cases with this configuration the Slave Security Center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



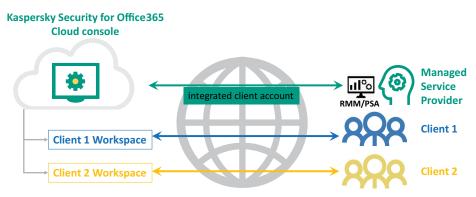
Kaspersky Hybrid Cloud Security

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

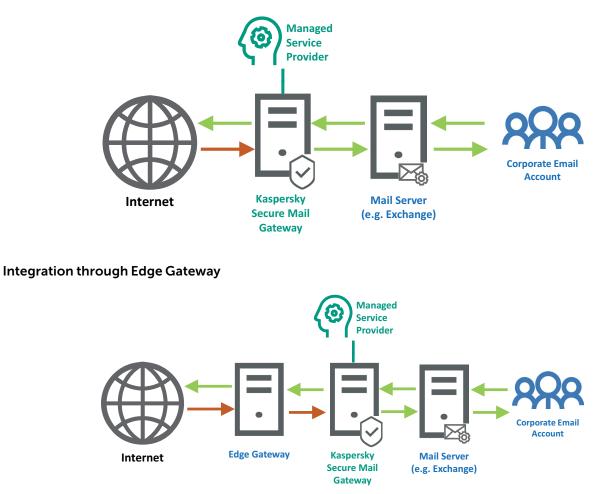
Protects Exchange Online mailboxes that are managed through Microsoft Office 365. Email messages are scanned for viruses, Trojans and other types of malware that are transmitted by email, as well as spam and phishing.



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.

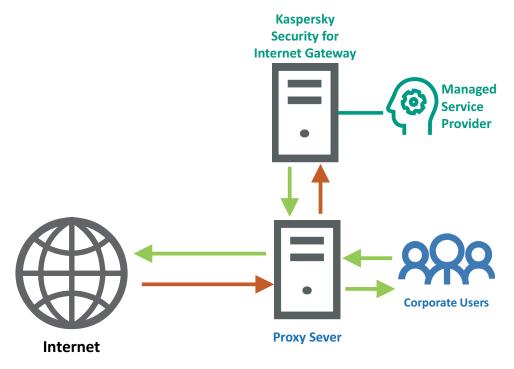
Direct Integration



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	НТТР	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	ТСР	 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' sh	nutdown				
13111	ТСР	Required for connecting to the KSN proxy server					
13291	ТСР	Required for the SSL connection betwee Administration Server.	en the Administration Console and the				
13292	ТСР	Required for connecting mobile devices					
14000	ТСР	 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	ТСР	Used by client computers to connect to Administration Server installed serves as					
15000	UDP		request to connect to the Administration bout the computer in the real-time mode.				
17000	ТСР	Required for secure SSL connection to the secure SSL connection to the secure SSL connection to the secure se	he activation proxy server.				
17100	ТСР	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	ТСР	 To connect to the Kaspersky Endpoint Security Cloud portal To sign in to the Kaspersky Endpoint Security Cloud portal
13000	ТСР	To manage: • Kaspersky Endpoint Security for Windows • Kaspersky Endpoint Security 10 for Mac
13292	ТСР	To manage: • Kaspersky Endpoint Security for Android • Kaspersky Safe Browser for iOS
9443	ТСР	To manage iOS MDM
8081	ТСР	To download installation packages
443/8080	ТСР	To connect to the KES Cloud Management Console

Appendix B

Using Kaspersky Security Center for Licensing

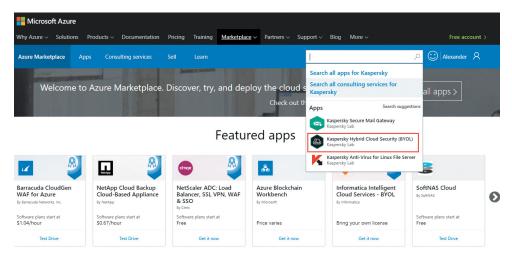
Licensing is a critical part of ensuring uninterrupted protection and avoiding problems due to expiry or blacklisted licenses. The main purpose of this capability is to provide the administrator with an automated tool to manage security application licenses.

- 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.

Why Azure ~ Solutions	Products \lor	Documen	tation Pricing	Training	Marketplace ~	Partners ∨ S	upport ~ Blog More ~	
Azure Marketplace	Apps Const	ulting servic	es Sell	Learn			Search Marketplace	\$
Products > Kaspersky Hy	brid Cloud Secur	ity (BYOL)						
		ersky I	Hybrid (Cloud	Security	(BYOL)		
GET IT NOW GET IT NOW Pricing information Cost of deployed template components Categories Security Support	Kaspers Overviev Best in c The Kaspen store critica and superic enable addi Highlights • Next	Software p	By Kaspersky Lab Ilan Hybrid Cloud Sec This solution ten Azure infrastruct those componer	urity (BYOL) urity components.	Security (BYOL) is software compor ints. The price is th orderless security v	e cost of	X lagree to the provider's terms of use and privacy policy and understand that the rights to use this product do not come from Microsoft, unless Microsoft is the provider. Use of Azure Marketplace is governed by separate terms.	
support support .egal .icense Agreement Privacy Policy	threa • Mult Cont • Clou	rrormance of	your entire Micro	osoft Azure c	loud		Continue	

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**.

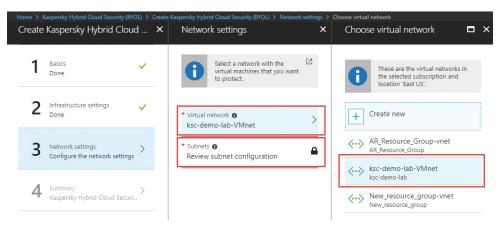
Kaspersky Hybrid Cloud Security (BYOL)	* ×	Create	Kaspersky Hybrid Cloud	×	Basics	
The Kaspersky Hybrid Cloud Security enables a seamlessly orchestrated and adaptive cybersecurity ecosystem. Wherevery you process and store critical business data - in a private or public cloud, or both - we deliver a perfectly balanced combination of agile, continuous security and superior efficiency, protecting your workloads against the most advanced threats without	^	1	Basics > Configure basic settings		* Name kcsdemolab	
compromising on systems performance. We enable additional security layers through a number o complementary and interlocking technologies. Highlights	f	2	Infrastructure settings > Configure the infrastructure se		kluser * Password ①	
 Next Generation technologies supported by machine learning defends your data, processes and applications against emerging threats. Multi-layered opbersecurity for workloads powered by: Exploit Prevention, Integrity Monitoring, Log Impaction, Application Controls and Anti-Ransomware capabilities. Cloud-assisted server oractection, Kaspecky Security Network (NSV) delivers a faster- 		3	Network settings		Confirm password	
 brow assume the processor the procesor the processor the processor the processor the pr	1	4	Summary Kaspersky Hybrid Cloud Securi >		Subscription VLAB_KHCS * Resource group	~
advanced threats for every workload, in every location. With our comprehensive approach, you can be confident that the security of everything you put into the cloud adheres to your corporate standards, and that your data and users are safeguarded at all times.		5	Buy >		Create new Use existing KHCS-RG Location East US	×
Support Details					Last 03	

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

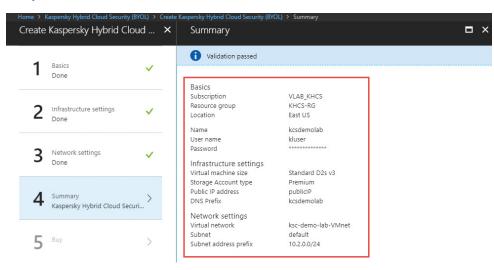
Keep the other settings as default, click **Select** and then **Ok**.

		× b	Infrastructure settings	×	Choose and Browse the av	a SiZe allable sizes and th							
			* Virtual machine size		Search			Compute type		Disk type			VCPUs
	isics one	~	1x Standard D2s v3	>				Show all compute types	*	SSD only		*	1
			Storage Account type		RECOMME	SKU	TYPE	COMPUTE 1 VCPUS	GB RAM	DATA DISKS	MAX IOPS	LOCAL SSD	PRE
2 Inf Co	frastructure settings onfigure the infrastructure se.	. >	Premium	\sim	Available								
			 Public IP address (new) publicIP 	>	*	D2s_v3	Standard	General purpose 2	8	4	4000	16 GB	SSD
	etwork settings onfigure the network settings	>			*	D4s_v3	Standard	General purpose 4	16	8	8000	32 GB	SSD
			* DNS Prefix 😧 kcsdemolab	~	*	D8s_v3	Standard	General purposi 8	32	16	16000	64 GB	SSD
	immary ispersky Hybrid Cloud Securi.	>	eastus.cloudap			D16s_v3	Standard	General purposi 16	64	32	32000	128 GB	SSD
• Ka	ispersky Hybrid Cloud Securi.					DS2_v2	Standard	General purposi 2	7	8	6400	14 GB	SSD
5 80		5				D\$3_v2	Standard	General purpose 4	14	16	12800	28 GB	SSD
2		<i></i>				DS4_v2	Standard	General purposi 8	28	32	25600	56 GB	SSD
						D\$5_v2	Standard	General purposi 16	56	64	51200	112 GB	SSD
						D\$2	Standard	General purpose 2	7	8	6400	14 GB	SSD
						DS3	Standard	General purpose 4	14	16	12800	28 GB	SSD
						DS4	Standard	General purpose 8	28	32	25600	56 GB	SSD

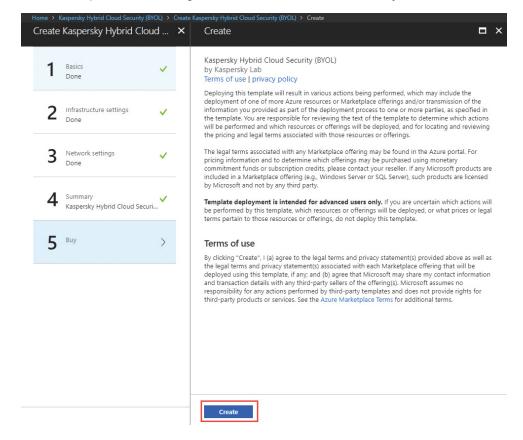
4. Choose a Virtual Network and click Ok.



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.

Microsoft Azure			D Sec	rch resources, services, and docs	× 🗘 >_ 🏽 😳 🔿	Alexander.Rumyantse
+ Create a resource	Virtual machines					* ×
i≘ All services	+ Add III Edit columns 🖏 Refresh	🏟 Assign tags 🕨 Start Restart	🔳 Stop 📋 Delete 🚝 S	envices		
	Subscriptions: VLA8_KHCS					
	kcsdemolab	All resource groups	✓ All types	✓ All locations	V No grouping	~
Dashboard	1 items					
All resources	NAME 12	TYPE 🐤	STATUS	RESOURCE GROUP To LOCATION	MAINTENANCE STATUS	SUBSCRIPTION 10
😂 Resource groups	🗌 👰 kcsdemolab	Virtual machine	Creating	KHCS-RG East US		VLAB_KHCS ····
🔕 App Services						
Function Apps						
🧃 SQL databases						
🦉 Azure Cosmos DB						
Virtual machines						
Load balancers						
🥁 Storage accounts						

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.

FRA BSS Directory	Networking	kcsdernolab - Networkir Virtual machine	ıg								
Add III Edit columns	•• More		"	Attach netwo	ork interface 🐠 Detach network inte	erface					
ocsdemolab		Verview			sterface: kcsdemolab-nic Eff aubnet: ksc-demo-lab-VMnet/default		urity rules Topology 2 104.211.18.53 Privat		ccelerated networkir	ng: Disabled	
kcsdemolab		Activity Ing			ECURITY GROUPS						
		Tays Ulagnose and solve problems			curity group kcsdemolab-nic-nsg	(attached	to network interface: kcs	:demolab-nic)		Add inbound po	ert rule
		SETTINGS		Impacts 0 sub	onets, 1 network interfaces						
		🙇 Networking		PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	
		😕 Disks		1000	A allow-inbound-rdp	3389	TCP	Any	Any	S Allow	
		Size		1100	allow-inbound-8060-tcp	8060	TCP	VirtualNetwork	VirtualNetwork	Allow	
		C Secunty		1110	allow inbound 0061 tcp	8061	TCP	VirtualNetwork	VirtualNetwork	Allow	
		Extensions		1120	allow-Inbound-13000-tcp	13000	TCP	VirtualNetwork	VirtualNetwork	Allow	
		🐔 Continuous delivery (Preview)		1130	allow-inbound-13291-tcp	13291	TCP	VirtualNetwork	VirtualNetwork	S Allow	
				1140	allow-inbound-14000-tcp	14000	TCP	VirtualNetwork	VirtualNetwork	Allow	
		👰 Availability set		1140							
		 Availability set Configuration 		1150	allow-inbound-13000-udp	13000	UDP	VirtualNetwork	VirtualNetwork	Allow	
						13000 Any	UDP Any	VirtualNetwork VirtualNetwork	VirtualNetwork VirtualNetwork	AllowAllow	
		Configuration		1150	allow-inbound-13000-udp	Апу			VirtualNetwork		

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.

Microsoft Azure			$\mathcal P$ Search resources, services, and docs $ imes$ $\mathbb Q$	>_ 🎲 😳 🕐 🕞 Alexander.Rumyantse 🌏
+ Create a resource	Home > Virtual machines > kosternolate Virtual machines « * X INTRA BSS Directory Add == Exit columns ···· More	kcsdemolab Virtual machine	≪	Connect to virtual machine X kessenses RDP SSH
- * FAVORITES	kesdemolab	Overview Activity log	tesselemolubr is not using Managed Disks. Migrate to Managed Disks to get more be Resource group (nange) test-set tesselemolubr is not using Managed Disks. Migrate to Managed Disks to get more be	To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file. * IP address
All resources Resource groups	kcsdemolab	Access control (IAM) Tags	Status Opera Running Windk Location Sce Bast US Stand	DNS name (kisidemolab.eastus.doudapp.azure.com) Port number 3289
App Services Function Apps		X Diagnose and solve problems	Subscription (owge) Public VIAILORCS 1042 Subscription ID Virtual 964#326-3785-4154-sec2-6421 (bs18875 bsc-s) DDN 5	Download RDP File
🥫 SQL databases		Networking Disks	koder Tags (minge) Click here to add tags	You can update inbound port rules in the VM Networking page. You can troubleshoot VM connection issues by opening
 Azure Cosmos DB Virtual machines 		Size	Show data for last: 1 hour 6 hours 12 hours 1 day 7 days 30 d.	the Diagnose and solve problems page.

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 Launch Instance.

aws	Services	✓ Resource Groups	; v 1
EC2 Dashboard Events			Connect Actions *
Tags Reports Limits		Name	versearch by keyword ✓ Instance ID ▲
INSTANCES Instances		AS-KSC SV_KSC_BYOL	i-00a71895a4a79a4 i-00df8dfc0d77c95ea
Launch Templates Spot Requests		MZ3-demo KESL-LATAM-AZ	i-0132e95d9a5a39f85 i-01f7da7d3239bdd5b
Reserved Instance Dedicated Hosts	s	NV-Azure-demo NV_Splunk	i-022412b034cacf060 i-027f23234014479a1

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.

aws Services	• Resource Gr	roups 🗸 🏌
1. Choose AMI 2. Choose Insta Step 1: Choose an An AMI is a template that contain	Amazon Ma	ure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review chine Image (AMI) uration (operating system, application server, and applications) required to launch your instance. You ca
Quick Start	Q kaspersky	
My AMIs AWS Marketplace Community AMIs Categories	Free Trial	Kaspersky Hybrid Cloud Security ****** (0) Kaspersky Security Center 10.5.1781 Sold by Kaspersky Lab \$0.60 to \$5.001hr for software + Charges for EC2 with Windows + AWS usage fees Windows, Windows Server 2016 Base Windows Server 2016 64-bit Amazon Machine Image (AMI) Updated: 5/21/18 Build a perfectly orchestrated and fully adaptive cybersecurity ecosystem around your AWS EC2 instances ar
All Categories Infrastructure Software (3) Clear Filter All Windows Windows 2016 (2)	Cirgaid	More info Kaspersky Hybrid Cloud Security (BYOL) ****** (0) Kaspersky Security Center 10.5.1781 Sold by Kaspersky Lab Bring Your Own License + Charges for EC2 with Windows + AWS usage fees Windows, Windows Server 2016 Base Windows Server 2016 64-bit Amazon Machine Image (AMI) Updated: 5/11/18 Build a perfectly orchestrated and fully adaptive cybersecurity ecosystem around your AWS EC2 instances ar More info

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

. Choose AMI	2. Choose Instance Type	3. Configure Instance 4. Add Stora	ge 5. Add Tags	6. Configure Security Group 7. Review
tep 2: Cl	hoose an Instance	еТуре		
0	General purpose	m5d.12xlarge	48	192
0	General purpose	m5d.24xlarge	96	384
	General purpose	m5.large	2	8
	General purpose	m5.xlarge	4	16
0	General purpose	m5.2xlarge	8	32
0	General purpose	m5.4xlarge	16	64
0	General purpose	m5.12xlarge	48	192
0	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**.

aWS Services → R	esourc	e Groups 🗸 🗙
1. Choose AMI 2. Choose Instance Type	3. Co	nfigure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review
Step 3: Configure Instan Configure the instance to suit your require		etails You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricin
Number of instances	(j)	1 Launch into Auto Scaling Group (j)
Purchasing option	(i)	Request Spot instances
Network	(i)	vpc-8fdef0e7 GPS Create new VPC
Subnet	(i)	subnet-f8edbd90 GPS us-east-2a Create new subnet 251 IP Addresses available
Auto-assign Public IP	(j)	Use subnet setting (Enable)
Placement group	()	Add instance to placement group.
Domain join directory	()	None Create new directory
IAM role	(i)	KSCRole Create new IAM role
Shutdown behavior		Stop •
Enable termination protection	()	Protect against accidental termination
Monitoring	(i)	Enable CloudWatch detailed monitoring Additional charges apply.
EBS-optimized instance	(i)	✓ Launch as EBS-optimized instance
Tenancy	(j)	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
Elastic GPU		Add GPU Additional charges apply.

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.

aws	Services 🗸 Re	source Groups 🗸	*				
1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review	
A security group i	S ports. You can create a	at control the traffic for y new security group or s	elect from an exis		an add rules to allow specific tra Learn more about Amazon EC:		
	Assign a security gro	 OCreate a new s Select an existi 					
Security	Group ID			Name			
sg-3ed08a	54			default			
sg-62b89f0	08			GPS_access_to_VMs			
sg-f2c09a9	98			KSCSecurityGroup			
sq-8cc09ae	e6			SecurityAgentGroup			

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.

-	Select an existing key pair or create a new key pair ×
	A key pair consists of a public key that AWS stores, and a private key file that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.
	Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.
	Choose an existing key pair
	Select a key pair
	GPS_demo •
	✓ I acknowledge that I have access to the selected private key file (GPS_demo.pem), and that without this file, I won't be able to log into my instance. Cancel Launch 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.

aws se	rvices	~ Re	esource Groups	× *							
EC2 Dashboard	• 1	Launch	Instance 👻	Connect	Actions 🛩						
Events						-					
Tags		Q, Filte	r by tags and attrib	utes or search b	y keyword						
Reports	1	N	ame		Instance ID	Instance Type -	Availability Zone ~	Instance State ~	Status Checks -	Alarm Statu	IS
Limits		01				mounee type	Artimubility Lone	motanee blate	Status Checks		
INSTANCES					i-03f2476e56d07bc78	m4.large	us-east-2b	stopped		None	1
Instances		K	SC-LATAM		i-03fa1c698a5e72518	m5.large	us-east-2b	stopped		None	1
Launch Templates		KE	SL2-LATAM		i-041c48743ccaba768	t2.micro	us-east-2c	stopped		None	2
Spot Requests		M	Z2		i-049e74907ccb0fec1	t2.micro	us-east-2c	stopped		None	2
Reserved Instances		M	Z4-demo	ø	i-04dab0b1ca17084f1	t2.micro	us-east-2c	stopped		None	1
Dedicated Hosts		KE	SL-LATAM		i-08bb3cbecbbc3b40f	t2.micro	us-east-2c	stopped		None	1
IMAGES		K	SC1		i-096efab279faaf891	t2.large	us-east-2c	stopped		None	1
AMIS		K	sws		i-0989875d588737f7c	t2.medium	us-east-2c	stopped		None	1
Bundle Tasks		K	SC-demo		i-0a6c30150e76797ae	t2.large	us-east-2c	stopped		None	1
		GF	S_KSC		·0aa55a22fe1e4123e	m4.large	us-east-2a	running	🛛 Initializing	C Loading	
ELASTIC BLOCK STORE		12/	255	80	-0c3cd15006cf7cd27	t2.xlarge	us-east-2c	stopped		None	١
Volumes		N	/_KESL_RHEL		i-0d2958b9209d979c5	t2.micro	us-east-2c	stopped		None	1
Snapshots		R	HEL1		i-0e93280b9e1e560	t2.micro	us-east-2c	stopped		None	1
NETWORK &		M	Z1		i-0ec33339e4affaf51	t2.micro	us-east-2c	stopped		None	1
SECURITY		K	SWS-demo		i-0f2cc1ef3e91e4637	t2.medium	us-east-2c	stopped		None	,
Security Groups		K	SWS-LATAM-AZ		i-0fac6d2052123d26e	t2.small	us-east-2c	stopped		None	1

Kaspersky Security Center configuration

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

Laur	nch Instance 🔻	Connect A	Actions V				
Q,	Filter by tags and at	tributes or search by	keyword				
	Name	•	Instance ID 🔺	Instance Type 🔹	Availability Zone 👻	Instance State 👻	Status Checks
	KESL-LATAM	i	-08bb3cbecbbc3b40f	t2.micro	us-east-2c	stopped	
	KSC1	i	i-096efab279faaf891	t2.large	us-east-2c	stopped	
	KSWS	i	-0989875d588737f7c	t2.medium	us-east-2c	stopped	
	KSC-demo	i	-0a6c30150e76797ae	t2.large	us-east-2c	stopped	
	GPS_KSC	Connect	2fe1e4123e	m4.large	us-east-2a	running	2/2 checks passed
	KSWS-LATAM	Get Windows Pas	sword 006cf7cd27	t2.xlarge	us-east-2c	stopped	
	NV_KESL_RHEL	Launch More Like	This 9209d979c5	t2.micro	us-east-2c	stopped	
	RHEL1	Instance State	▶ b9e1e560	t2.micro	us-east-2c	stopped	
	MZ1	Instance Settings	9e4affaf51	t2.micro	us-east-2c	stopped	
	KSWS-demo	lmage Networking	Be91e4637	t2.medium	us-east-2c	stopped	
	KSWS-LATAM-A	CloudWatch Moni	52123d26e	t2.small	us-east-2c	stopped	

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.

ou can connect to your Wind ownloading and running the P	ows instance using a remote desktop client of your choice, and by RDP shortcut file below:	
	Download Remote Desktop File	
When prompted, connect to yo	our instance using the following details:	
Public DNS	and the second	
User name	Administrator	
Password	Get Password	
you've joined your instance t istance.	o a directory, you can use your directory credentials to connect to your	
you need any assistance cor	nnecting to your instance, please see our connection documentation.	

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

@ 2018 AO Kaspersky Lab. All rights reserved. Registered trademarks and service marks are the property of their respective owners.

