kaspersky

Kaspersky Endpoint Security Deployment Service

kaspersky

Introduction

This document describes the Kaspersky Endpoint Security deployment service provided by our experts at Kaspersky.

The goal of this service is to have Kaspersky Endpoint Security up and running in your environment, including the deployment of your Kaspersky Security Center management console, with endpoint agents installed onto up to 50 machines, to your complete satisfaction, within the scope of work agreed.

Coverage

1(one) Kaspersky Security Center management console and up to 50 machines with Kaspersky Endpoint Security installed

Service timeline

This service allows for a maximum of 8 labor hours to achieve this goal. Once everything is fully delivered to your satisfaction, the project will be defined as 'completed', even if less than 8 labor hours have been used.

The service can be divided into the following stages:

Introduction	Deployment	Finalisation
Kick-off and talking through the Kaspersky Endpoint Security architecture.	Installing and configuring SQL 2019 Express for customers with less than 300 endpoints (optional) Installing and configuring Kaspersky Security Center.	Reviewing the dashboard to validate the installation and demonstrating that the installation has been fully and correctly completed.
Checking through your systems architecture and environment (establishing remote access, validating binaries, looking at server patching, network communications, internet access and server requirements). Checking your database, where it's situated and its resources.	Polling your discovery settings to locate the machines onto which we'll be installing Kaspersky Endpoint Security protection.	Preparing and delivering our report on completion.
	Creating a Network Agent and endpoint policies for your workstations.	
	Performing a series of tasks: Update, Full Scan, Quick Scan.	
	Downloading updates to the repository.	
	Reviewing Administration Server backup procedures.	
	Acitivating licenses.	
	Creating Kaspersky Endpoint Security and Network agent packages.	
	Creating groups.	
	Running installation tasks for the Network Agent and for Kaspersky Endpoint Security – for up to 50 endpoints.	

kaspersky

Requirements & Statements

Please note that Kaspersky is under no obligation to deliver or attempt to deliver this service if the requirements listed below have not been fully met. Please let us know immediately should meeting any of these requirements present a potential problem.

- The service is delivered remotely and can be divided in 2 'windows' of 4 hours each – you'll need to agree this timing with us in advance.
- You must provide access to your environment remotely using the Zoho Assist tool (TCP ports 80 and 443 only, see detailed requirements https://www.zoho.com/assist/kb/firewall-configuration.html)
- A representative of your IT department or security team must be available at all times during service delivery to meet any reasonable request from our Kaspersky Engineers, including permissions, access, etc.
- The server must meet the requirements of the current version of Kaspersky Security Center. For more information visit the following websites (please select your application version in the upper right corner of the pages provided below):
  - o Hardware and software requirements: https://support.kaspersky.com/KSC/14/en-US/96255.htm
  - o Accounts for work with the DBMS: https://support.kaspersky.com/KSC/14/en-US/156275.htm
  - o Ports used by Kaspersky Security Center: https://support.kaspersky.com/KSC/14/en-US/158830.htm
  - o Device discovery: https://support.kaspersky.com/KSC/14/en-US/3884_1.htm
- The Windows server onto which we'll will install Kaspersky Security Center must have the 2019 version of Windows or later, and must have ALL the latest patches installed.
- The following binaries/files must be available on the server (the distributives can be found at this link https://www.kaspersky.com/small-to-medium-business-security/downloads/endpoint)
- If you have less than 300 nodes, the SQL 2019 Express distributive - if you have more than 300 nodes, SQL Standard edition must already be installed and running in advance.
  - o Kaspersky Security Center distributive.
  - o Latest version of Kaspersky Endpoint Security.
  - o Kaspersky License Key file.
- The Kaspersky Security Center server must have access to the internet without any restriction, in order to perform downloads from the Kaspersky database.
- Any security product installed on the target machines will need to be removed. If this doesn't happen automatically, and if passwords or scripts for removing this and any other third-party software are not available, it will be your responsibility to remove any such software in advance. If necessary, we can create a separate support incident to handle this task, which will then need to be completed prior to the delivery of this service.
- We'll be creating a structure based on a single site with default configuration.
- Kaspersky Endpoint Security will be deployed onto up to 50 machines, and we'll show you how to perform this task for further endpoints in your environment.
- Any technical issues arising during deployment will addressed through our support service.

In Scope	Out of Scope
• Install SQL 2019 Express on a single server (optional). • Install Kaspersky Security Center on servers already running SQL. • Create a discovery method (Domain or Active Directory). • Create a package for Kaspersky Endpoint Security. • Create a package for Kaspersky Network Agent.	Kaspersky will not work on any task or product not explicitly described here under 'In Scope' & 'Deliverables'. This includes: • Creating any kind of cluster or high availability. • Integrating Kaspersky Security Center with Active Directory. • Creating exclusions for applications not working with Kaspersky protection. • Installing protection on Linux or Mac machines,

kaspersky

- Create a Policy for Kaspersky Endpoint Security and Kaspersky Network Agent.
- Configure the Kaspersky Security Center Backup task (backup to be stored on the same server).
- Create a task to download updates to the repository.
- Create a task to update Kaspersky Endpoint Security across the environment.
- Create an administration structure based on 'Servers' and 'Workstations'
- Create a task to perform a Quick Scan of the environment.
- Create a task to perform a Full Scan of the environment.
- Install the Kaspersky Network Agent onto up to 50 machines.
- Install Kaspersky Endpoint Security on up to 50 machines
- Remove incompatible 3rd party security application if we have the files to do it. If these files are not available, a support incident will be created to handle this task, which will then need to be delivered after the project completion.
- Perform a malware detection using EICAR.
- Create a Completion Report.

- mobile phones or tablets.
- Deploying MDM features.
- Deploying our Encryption or Patch Management modules.
- Configuring SIEM systems synchronization.
- Handling or integrating any product with Kaspersky Security Center (Except SQL as described as 'In Scope').
- Handling user creations, DNS, DHCP, Active Directory or any other network services.
- Creating or editing rules for External Firewalls or Routers.
- Creating or editing any hypervisor environment.
- Performing backups from any machines or systems involved on the project.
- Installing any operating system.

Outcome and deliverables

1. Kaspersky Security Center will be deployed and configured to manage your environment.
2. Kaspersky Endpoint Security will be deployed on up to 50 workstations.
3. Your administrator will understand how to manage your endpoint security through the Kaspersky Security Center console, and how to deploy Kaspersky Endpoint Security onto further workstations, now and in future.
4. You'll receive a Completion Report.

Notes

We can perform additional configurations and deployments, and many other tasks that fall outside the scope of our off-the-shelf services, through our custom Professional Services portfolio.   Please speak to your Account Manager about creating a custom proposal for you.

Our schedule of work will be based on the availability of the most appropriate Kaspersky resources, but work will start no longer than 15 days after we receive the go-ahead to start the project from you in writing.

kaspersky