kaspersky

Health Check Service Package

kaspersky

Introduction

This document describes our Health Check Service Package for Kaspersky Software products installed into your network, performed by our experts.

Objective

With any software product, issues relating to its configuration and operation can cause serious disruption if overlooked for an extended period. It's crucial to check the health status of your Kaspersky products regularly, so that any potential issues can be detected at an early stage. This is what our Health Check Service is designed to do.

During this service, your Kaspersky engineer will review the configuration of your Kaspersky products and check existing Kaspersky product reports and events for errors.

As a result of this service, you will receive a comprehensive report with the findings discovered in process and suggestions for improvement.

Total estimated business hours & project timeline

We offer this service at three levels, depending on the number of policies requiring validation and whether you would also wish us to present our results. Each level includes a specified number of hours. In each case, once everything is fully delivered to your satisfaction, the project will be defined as 'completed' even if less than the total number of hours specified have been used.

2 hours	4 hours	8 hours
1. Kick-off to explain the activities. 2. Environment analysis. 3. Create and send a final report.	1. Kick-off to explain the activities. 2. Environment analysis. 3. Create and send a final report.	1. Kick off to explain the activities. 2. Environment analysis. 3. Create final report. 4. Present the Result.

Requirements & further information

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.

1. The service will be delivered remotely. 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)
2. Our 8 hours level service can be divided in 2 'windows' - one to collect the data and other to present the results. You will need to agree the duration of each of these 2 windows with us in advance.
3. We will require direct access to your Kaspersky Security Center management console, including groups, subgroups, tasks, policies, properties of objects, etc, and to your protected devices, in order to understand your local configuration.
4. 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.

kaspersky

Scope of work

In scope:

2 hours	4 hours	8 hours
1. Validate your single Kaspersky Security Center server configuration. This is essential, as the whole analysis is based on a centralized administration. 2. Validate 1 Kaspersky Endpoint Security for Windows policy. 3. Validate 1 Kaspersky Security for Windows Server policy. 4. Validate your Network Agent Policies. 5. Review your Kaspersky Security Center infrastructure configuration. 6. Provide a report suggesting improvements based on best practice.	1. Validate your single Kaspersky Security Center server configuration. This is essential, as the whole analysis is based on a centralized administration. 2. Validate up to 2 Kaspersky Endpoint Security for Windows policies. 3. Validate up to 2 Kaspersky Security for Windows Server policies. 4. Validate your Network Agent Policies. 5. Review your Kaspersky Security Center infrastructure configuration. 6. Provide a report suggesting improvements based on a best practice.	1. Validate your single Kaspersky Security Center server configuration. This is essential as the whole analysis is based on a centralized administration. 2. Validate up to 4 Kaspersky Endpoint Security for Windows policies. 3. Validate up to 4 Kaspersky Security for Windows Server policies. 4. Validate your Network Agent Policies. 5. Review your Kaspersky Security Center infrastructure configuration. 6. Provide a report suggesting improvements based on a best practice. 7. Present the Results.

Out of Scope:

- Kaspersky will not work in any task or product not explicitly listed in the relevant 'Inside Scope' section above.
- Kaspersky will not fix any problem found during the analysis.

Outcome and Deliverables

You will receive a comprehensive report with recommendations on how to improve your security levels using your Kaspersky Security for Business solution:

- Revealing any issues with the health and configuration of the Kaspersky products installed on your network.
- Providing our recommendations on how to fix any such issues and potential problems.

Notes

Kaspersky Health Check is an activity that checks whether your Kaspersky products are configured as recommended. It is not a security assessment service, and its implementation does not in any way guarantee the complete security of your installation.

Additional configurations, deployment and corrections can also be added to this scope to meet your specific needs if required. Please ask your account manager to create a custom proposal for you.

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

kaspersky

www.kaspersky.com
Kaspersky Professional Services