kaspersky

Vulnerability and Patch Management implementation service

kaspersky

Introduction

This document describes the Vulnerability and Patch management modules implementation service performed by Kaspersky experts for your Company.

The goal of this service is to enable your administrator to use the full functionality of the Kaspersky Vulnerability Assessment and Patch Management module, identifying vulnerabilities and applying appropriate patches and updates to applications running in your environment, as well as controlling licenses, via your Kaspersky Security Center console.

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 3 stages:

Introduction	Configuration & Service Delivery	Finalisation
Meeting to explain the architecture.	Enabling and deploying the Kaspersky Vulnerability Assessment and Patch Management Kaspersky Endpoint Security module on Kaspersky Security Center	Preparation and delivery of our Completion Report.
All necessary environment checks (remote access, network communication, Internet access, server and license requirements).	Configuring the network agent that enables Kaspersky Security Center to replace WSUS (Windows Server Update Services) in your system.	
Explanation of: • How vulnerabilities and updates can be found. • How these vulnerabilities are fixed and updates are installed. • How Kaspersky Security Center replaces WSUS.	Creating the following tasks, and demonstrating how they can be performed via Kaspersky Security Center: • finding and fixing vulnerabilities • locating and installing appropriate updates.	

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.

- The service is delivered remotely and can be divided in 2 'windows' of 4 hours each – you will need to agree this timing with us in advance.
- You must provide access to their 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 environment must have Kaspersky Security Center and Kaspersky Network Agent installed
- The Network agents must be able to communicate fully with the Kaspersky Security Center, with no issues.
- Remote access must be executed on all computers with Kaspersky Security Center installed, and on every computer one which we'll be installing the vulnerability and patch management module.
- Your Kaspersky Endpoint Security for Business license must be for the Advanced level or above.

- We will need a minimum of 600 GB free disk space (in order to save the update module meta data)
- All computers included in the service must be running Windows
- The server must meet all the requirements of the current version of Kaspersky Security Center. For more information please visit the following websites (please select your application version in the upper right corner of the pages provided below):
    - Hardware and software requirements: https://support.kaspersky.com/KSC/14/en-US/96255.htm
    - Accounts for work with the DBMS: https://support.kaspersky.com/KSC/14/en-US/156275.htm
    - Ports used by Kaspersky Security Center: https://support.kaspersky.com/KSC/14/en-US/158830.htm
- If any failures are found during implementation that require analysis, these will be addressed through standard support incidents.

Scope of work

In Scope	Out of Scope
• Explaining the concept behind the Vulnerability Assessment and Patch Management module. • Explaining and demonstrating the various tasks involved in managing the module and its functionality. • Implementing the Vulnerability Assessment and Patch Management module as outlined in the 'Project timeline' section, based on a single instance of Kaspersky Security Center.	Kaspersky will not work on any task or product not explicitly described here under 'In Scope' & 'Deliverables'. This includes: • Creating any type of policy. The policy used by the network agent for implementation will be that already existing in the environment. • Creating any task that not strictly associated with the operation of the vulnerability and patch management module. • Integrating Kaspersky Security Center with Active Directory. • Installing any protection component. • Integration with Microsoft Windows Server Update Services. • Creating users, DNS, DHCP, Active Directory or any other network services. • Creating or editing any environment other than Kaspersky products. • Making backup copies of the machines or systems involved in the project. • Installing any operating system. • Creating a structure of main and slave servers • Installing any operating system.

Outcome and Deliverables

1. Your Kaspersky Endpoint Security installation will incorporate active Kaspersky Vulnerability Assessment and Patch Management functionality controlled from Kaspersky Security Center
2. Your administrators will understand how to identify and prioritize vulnerabilities, and how to manage the distribution of patches and updates.
3. Delivery of our Completion Report.

Notes

We can perform additional configurations and deployments, and many other tasks that fall outside the scope of our off-the-shelf Service Packages, 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.

www.kaspersky.com
https://support.kaspersky.com/corporate/professional_services