kaspersky

Feature List

Kaspersky EDR Optimum v 1.0

Q2 2020

Introduction

This document describes the existing features and capabilities of Kaspersky Endpoint Detection and Response Optimum solution (Kaspersky EDR Optimum).

As cybercriminals specifically craft their attacks by using fileless techniques, obfuscation methods and legitimate system-native tools (e.g., Powershell, WMI, PsExec) to bypass endpoint protection, corresponding defensive approaches must evolve as well.

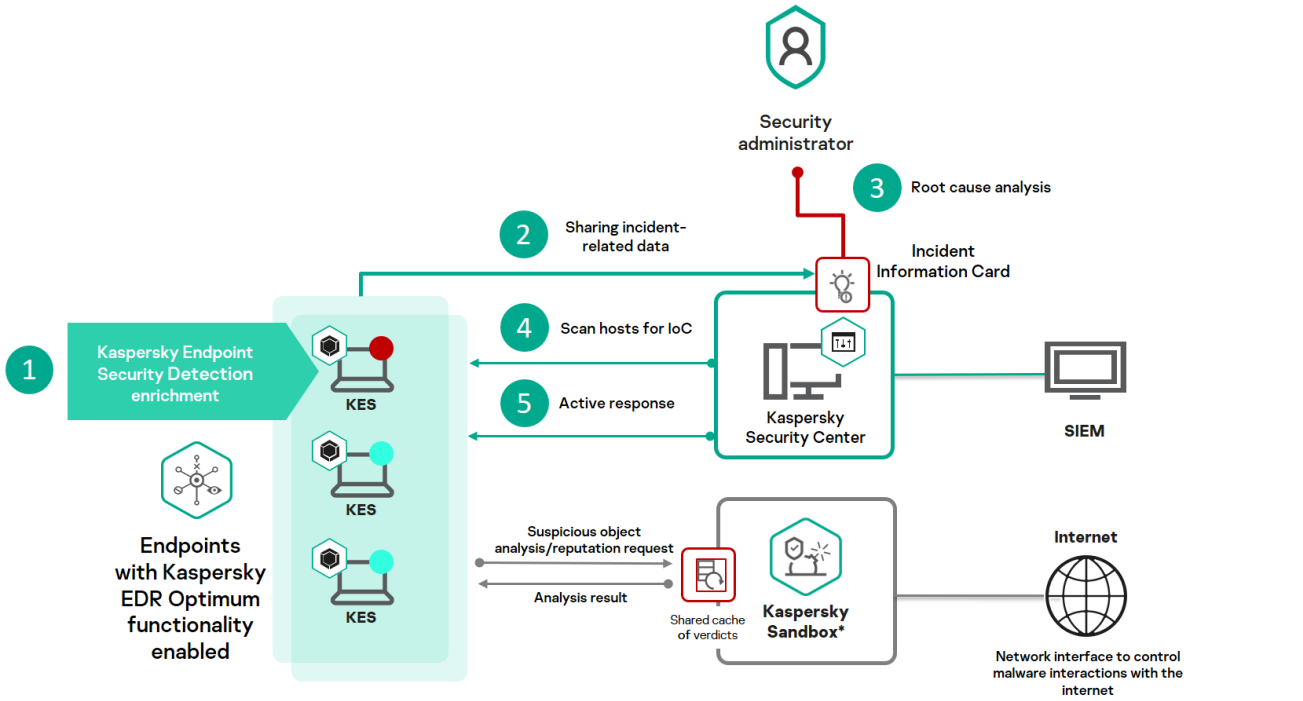
Keeping in mind skills shortage and budget limitations inherent to the majority of businesses today, Kaspersky EDR Optimum is designed to reduce the minimum required level of security expertise by offering your IT and security personnel a simple and highly-automated tool to detect and respond to complex threats.

Kaspersky EDR Optimum leverages the power of the flagship Kaspersky Endpoint Security platform by consolidating its multilayered defense techniques (including and not limited to behavior-based protection, exploit prevention, cloud-based reputation, etc.) and root cause analysis, threat indicators discovery and response capabilities into a single solution.

EDR Optimum with a centralized management console helps to bring immediate attention of IT or security personnel to emerging threats - bring more light to the real cause of incident, track malicious activities at the host level, search for similar activity in the infrastructure, and provide sufficient tools to conduct easy and adequate response.

Out-of-the-box integration with automatic Kaspersky Sandbox complements with additional behavior analysis of advanced threats, including unknown ones.

EDR Optimum does not require any resource-demanding components, thus minimizing costs related with solution deployment.



Integrated Solution Operational Scheme

* Optional component – part of integrated solution

kaspersky

Architecture

Component	Description
EDR agent (further in text – Agent)	Agents are installed on endpoints (as a part of Kaspersky Endpoint Security) running under the Windows operating system, and responsible for: • collecting data on threat verdicts and threat context from Kaspersky Endpoint Security • enrichment of verdicts with gathered incident-related and system data • providing incident-related data with Kaspersky Security Center for data visualization including attack execution map and root cause • IoC (Indicator of Compromise) scanning process on the endpoint • response actions In case of integration with Kaspersky Sandbox product, the agent is responsible for routing the objects to the sandboxing module. • Agent is a part of Kaspersky Endpoint Security • Managed by Kaspersky Security Center (On premise and Hosted deployment option) Examples of incident data relating to the detection of suspicious events being shared with Kaspersky Security Center for further analysis and response may include: • Kaspersky Endpoint Security/Kaspersky Sandbox detects and automatic response results • Start/End Process • Registry changes • DLL Loading • Remote host connection • File creation, etc.
Kaspersky Security Center Web	Incident-related data is stored in Incident Information Card for 30 days.
Kaspersky Sandbox (optional component – purchased separately)	The object dynamic analysis (isolated environment) module with ability to automatically scan endpoints and apply response in case if suspicious activity has been detected by the sandbox.

kaspersky

Detection and investigation

Kaspersky EDR Optimum as a part if integrated Endpoint Protection solution, utilizes multiple detection engines and capabilities of Kaspersky Endpoint Security for Business product.

Feature	Description
Automated detection	
Automated detection of malicious activity using Kaspersky Endpoint Security/Kaspersky Sandbox	Detection capability implemented in Kaspersky Endpoint Security comprises and not limited to the following engines and mechanisms: • Behavior Detection, • Adaptive Anomaly Control, • Exploit Detection, • Fileless threats detection • Reputation analysis (Kaspersky Security Network) • Custom threat indicators detection (Kaspersky Sandbox), etc. All the findings of Kaspersky Endpoint Security detection are enriched by the system artifacts collected by the KES/agent, and only relevant incident-related data is shared with Kaspersky Security Center. Behavior analysis capability designed to address advanced and evasive threats can be complemented by fully automatic Kaspersky Sandbox* component (exploring behavior of analyzed objects in detail in isolated environment) - providing additional data for root cause analysis. *Requires purchase of additional product license - Kaspersky Sandbox
Semi-automated detection (IoC-based detection)	
Automatic event creation with ability to generate IoC	The list of indicators is generated based on the data shared by the Endpoint agent and proposed to the analyst for further actions (search for a similar incident on other hosts, response) The list of IoCs is represented in Incident Information Card in KSC.
Scan endpoint infrastructure using system-generated IoCs (real-time)	Search for similar incidents by scanning the infrastructure using IoCs automatically generated by the system. The indicators can be pre-selected by the user before scanning process occurs.
Scan endpoint infrastructure using external (third-party) set of IoCs	To simplify the work of information security specialists in identifying Indicators of Compromise, Kaspersky EDR Optimum can upload third-party IoCs (e.g. from any threat intelligence provider or regulation body) in OpenIOC format. Search is carried out using file-based threat indicators (file hashes). The list of supported OpenIOC terms can be shared by Kaspersky.

	The IoC terms validity checks are performed to ensure IoC syntax correctness and full support when importing the file/list of files.
IoC scan queries over endpoint (by schedule)	IoC scanning of endpoint infrastructure can be carried out according to a schedule. The scanning process takes place directly on the endpoints, and their current status is checked.
IoC export	Automatically generated artifacts related to Kaspersky Endpoint Security can be exported and saved in OpenIOC format.

Visibility

EDR Optimum provides full visibility into the incident, ensures immediate understanding of what's happening, and the ability for a quick response before damage can occur.

Feature	Description
Incident Information Card	Each new threat case in EDR Optimum is opened and populated with automatically generated information after malicious/suspicious activity has been detected on the endpoint. The card is generated by Kaspersky Security Center and includes (not limited to) the following categories of information: • Attack execution map/threat visualization • Incident events (registered artifacts – file/process details/URL information/registry modification, etc.) • Host information (name, ip address, MAC address, list of users, OS, domain controller role, etc.) • General information on detection, including detection mode (ods/oas/amsi/on execute, etc.) • Registry changes, autorun detects • Response status (i.e. quarantined, disinfected) • File appearance history, etc. Response activities are available for selection from the incident card.
Root cause analysis: Attack execution map/threat visualization	The graph contains key processes, network connections, DLLs, registry hives being involved/affected by an incident. All detections are highlighted on the graph providing the analyst full context of incident and facilitating the process of revealing affected components.
Various representation modes for collected artifacts	All incident-related artifacts gathered can be sorted by group (processes, registry, connections etc.) or by list.

kaspersky

Response

Automatic detection coupled with response capabilities help the organization to automatically counter the most evasive attacks, including new exploits, new ransomware, and fileless threats, as well as techniques exploiting legitimate system tools.

Feature	Description
Response framework	Reduces the number of routine manual tasks undertaken, and cuts response times from hours to minutes, through supporting a wide range of automated response activities, including: • Putting objects in prevention mode • Performing host isolation • Adding file to KES Whitelist/send an object to Kaspersky for further analysis • Critical areas scan • Quarantine/recovery of objects • File deletion • Terminate processes • Running commands on the endpoint The response actions can be configured when editing IoC scan settings. The response actions are performed by the Endpoint agent. Note: In addition to Kaspersky EDR Optimum functionality, Kaspersky Endpoint Security already has particular response functionality (i.e., Automatic Rollback).
Automatic cross-endpoint response	Auto generation of threat indicators (IoC) with ability to apply response actions on network infrastructure
Response actions and task execution	
Prevent file execution	Prevent file execution (automated action in case when IoC is found). Object is being added to the black list.The task can be performed over the entire network.
Host isolation	The current host/remote host can be isolated from the rest of the network in case when IoC is found. The mechanisms of exclusions is used to secure the Endpoint agent communications (with Kaspersky Security Center, Kaspersky Sandbox) in case of network isolation. Custom host isolation exclusion rules can be configured (i.e. by adding particular network resources to exclusion e.g. DNS or selecting predefined profiles).
Delete object from endpoints	Objects can be remotely deleted from a single endpoint or a group of machines

Process termination	Stopping execution of suspicious process – any process can be remotely killed on an endpoint, to contain the threat on the endpoint and to block data exfiltration and lateral movement attempts in real time
Quarantine the file	Moving an object to the special repository for storing suspicious objects
Scan a system	Scanning the critical areas using Kaspersky Endpoint Security functionality
Remote program execution	Any additional software can be run remotely on a dedicated endpoint machine
Commands execution on the host	Any commands can be run remotely on a dedicated endpoint machine
Adding to Kaspersky Endpoint Security whitelist	Whitelisting the object (based on Kaspersky Endpoint Security detection) using Kaspersky Security Center.
Sharing suspicious objects with Kaspersky experts	The suspicious file can be send for analysis to Kaspersky
Recovery	
File recovery from quarantine	Any object stored in Quarantine can be recovered back to the endpoint at any time
Enabling isolated hosts on the network	Isolated hosts can be enabled on the network by the specialist. The time out value for isolation rules can be configured.
Rollback	Kaspersky EDR Optimum, while sharing a single agent with Kaspersky Endpoint Security, provides a rollback procedure that protects different objects, including files, registry keys, etc.

Administration

Feature	Description
Single web console	Kaspersky EDR Optimum is fully managed via the Kaspersky Security Center 12 - web interface designed for: • Monitoring security posture • Presenting information on detections and incident-related information (with visualization) generated and shared by Endpoint agent • Applying response actions and tracking the response status

	• Installing Kaspersky applications on devices in the network and manage installed applications • Managing policies and tasks • IOC scans initiation • Reporting on the security system status and managing delivery of reports to administrators and security experts. • Vulnerability and patch management • Setting parameters of interaction with SIEM, etc. Connection to the Kaspersky Security Center can be established via any popular web browser. Access rights are issued in accordance with predefined roles (RBAC support). IT administration and security tasks are combined in a single console. Both on-premise and hosted (cloud) deployment modes are supported.
Centralized agent management	Endpoint Agents are managed via KSC Web console (maintenance/deploy/statuses, etc.)
Notification of system component failure and errors	By Kaspersky Security Center
Reporting	By Kaspersky Security Center
Endpoint Agent self-defense mechanism	Prevent modifying agent-related files/system components entries, etc.

Integration capabilities

Feature	Description
Integration with SIEMs	Events can be exported in CEF format and imported into a SIEM system for correlation with information from other log sources
Native integration with Kaspersky Endpoint Security	Kaspersky EDR Optimum shares a single agent with Kaspersky Endpoint Security. Data from Kaspersky Endpoint Security (detects, blocking, suspicious events) are provided to the EDR Optimum console (Kaspersky Security Center) to facilitate the process of detection and investigation.
Integration with Kaspersky Sandbox	Kaspersky EDR Optimum capabilities can be further enhanced with an automated Kaspersky Sandbox for discovering threats designed to bypass endpoint protection.
External IoC upload	IoCs can be imported in OpenIoC format for use in infrastructure searches