kaspersky

# Essential Installation Service: Kaspersky Next XDR Expert

kaspersky

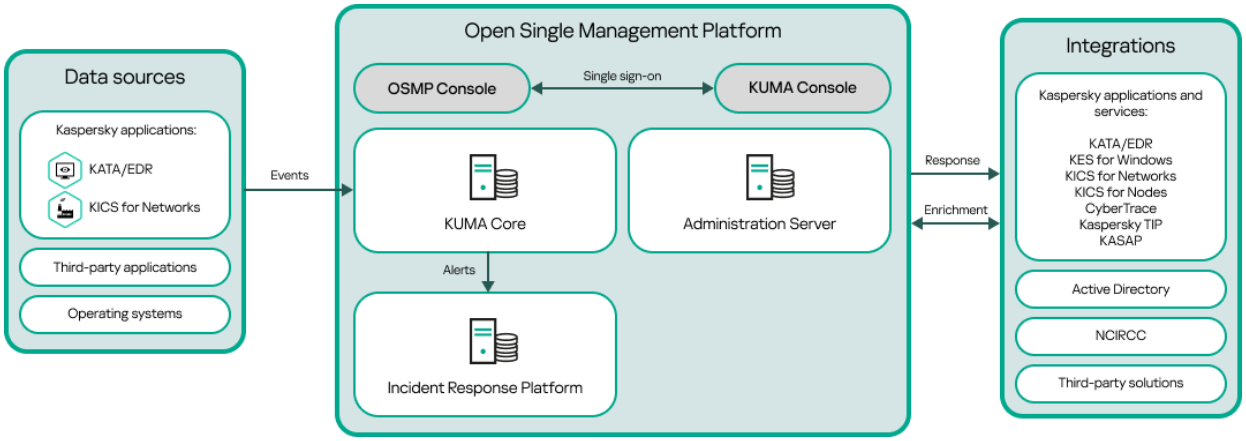
# Introduction

Kaspersky Professional Services is a set of services covering the complete product cycle, from assessment through implementation to maintenance and optimization.

Kaspersky Next XDR Expert is designed for highly advanced enterprises, usually with significant resources and a dedicated cybersecurity team or Security Operations Center (hereinafter SOC). Such organizations take a proactive approach to adopting the latest technologies, staying ahead of threats and implementing comprehensive security solutions.

Kaspersky Next XDR Expert is built on our Open Single Management Platform, which integrates all solution components (including Kaspersky and third-party tools) and enables interaction between them. It's an integral part of our unified IT-OT XDR technology stack, serving as a central component for incident management and supporting the administration and maintenance of security tasks.

The components of Kaspersky Next XDR Expert and their interaction:




Integrating Kaspersky Unified Monitoring and Analysis Platform (hereinafter KUMA) with other solutions and systems enhances the efficiency of threat monitoring and response, as well as extends the protection scope.

Kaspersky Next XDR Expert comprises the following main components:

1. Open Single Management Platform (hereinafter OSMP). The technology basis that Kaspersky Next XDR Expert is built on. OSMP unifies all the solution components and provides interaction between them. OSMP is scalable and supports integration with Kaspersky applications and third-party solutions.

2. OSMP Console. Provides a web interface for OSMP.

3. KUMA Console. Provides a web interface for Kaspersky Unified Monitoring and Analysis Platform.

4. KUMA Core. The central component of KUMA. KUMA receives, processes, and stores information security events and then analyzes the events using correlation rules. As a result of

the analysis, if the conditions of a correlation rule are met, KUMA creates an alert and sends it to Incident Response Platform.

5. Incident Response Platform. A component of Kaspersky Next XDR Expert that allows you to create incidents automatically or manually, manage the alert and incident lifecycle, assign alerts and incidents to SOC analysts, and respond to incidents automatically or manually, including through playbooks.

6. Administration Server (also referred to as the Server). The key component of endpoint protection of a client organization. The Administration Server provides centralized deployment and management of endpoint protection through EPP-applications and allows you to monitor the endpoint protection status.

7. Data sources. Information security hardware and software that generate events. After you integrate Kaspersky Next XDR Expert with the required data sources, KUMA receives the events to store and analyze them.

8. Integrations. Kaspersky applications and third-party solutions integrated with OSMP. Through integrated solutions, a SOC analyst can enrich data required for incident investigation and then respond to incidents.

## Coverage

All-in-one deployment scenario (1 server: OSMP Worker node - Kubernetes Worker node + DBMS; 1 server: KUMA services node(s) - Collector, Correlator, Storage), EDR basic configuration, connection to up to 7 standard event sources, integration with up to 3 Kaspersky solutions or infrastructure services.

## Service timeline

This service allows for a maximum of 15 working days to achieve the goal. Once everything is fully delivered to your satisfaction, the project will be defined as 'completed', even if less than 15 working days have been used.

The service can be divided into the following stages:

- Kick-off meeting, check list completion and scope confirmation
- Deployment and basic configuration (All-in-one deployment scenario, 2 servers)
- Event sources connection, integration of Kaspersky solutions
- Post-implementation activities

## 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.

The service is delivered remotely. To prepare and provide a deployment scenario, it is necessary to provide the data requested by Kaspersky engineers.

kaspersky

A representative of your IT department or security team must be available at all times during the service delivery to meet any reasonable request from our Kaspersky engineers, including permissions, access, etc.

The service is provided on current supported versions of Kaspersky Extended Detection and Response Expert, in accordance with the application lifecycle terms:

(https://support.kaspersky.com/corporate/lifecycle?type=limited,full&program=xdr-expert#b2b.block3.ksc12)

Any technical issues arising during deployment will addressed through our support service.

## Scope of work

1. OSMP Platform Deployment:
   1.1. Verify hardware requirements and pre-requisites
   1.2. Install OS and perform initial configuration
   1.3. Install and configure PostgreSQL database
   1.4. Create deployment YAML files
   1.5. Install OSMP Platform via KDT
2. Kaspersky Security Center for Linux (KSCL) Configuration:
   2.1. Activation of Kaspersky Security Center licenses
   2.2. Configuration of Kaspersky Security Center Administration Server settings and repository update task
   2.3. Creation and configuration of Kaspersky Security Center mandatory policies and tasks
   2.4. Configuration of device discovery
   2.5. Creation of the group structure
   2.6. Deployment of Network Agent on the endpoints (up to 50)
   2.7. Integrations – Domain Polling, Kerberos authentication, SMTP notifications, SIEM (optional)
   2.8. Connection Gateway deployment and configuration (optional)
   2.9. Creation and configuration of the Backup Task
3. Kaspersky Endpoint Security (KES) rollout:
   3.1. Creation and configuration of installation packages and remote deployment tasks
   3.2. KES protection rollout by batches (up to 50)
4. Kaspersky Sandbox Deployment:
   4.1. Verify hardware requirements and prerequisites
   4.2. OSMP Sandbox deployment using ISO
5. Kaspersky Endpoint Detection & Response (KEDR) Configuration:
   5.1. Configuration of the KEDR and Sandbox settings
   5.2. Installation of Virtual Machine images on the Sandbox
   5.3. Configuration of the malware interface on the Sandbox
   5.4. Deployment of EDR Agent (part of KES)
6. Kaspersky Extended Detection & Response (XDR) Configuration:
   6.1. XDR and KUMA initial configuration
   6.2. Configuration of collectors, correlator, storage

6.3. Integrations – Kaspersky Security Center and Sandbox
6.4. Integrations – LDAPS integration with KUMA (optional)
6.5. Onboarding of Log sources with OSMP (up to 10 OOTB log sources)
6.6. Configuration of event enrichment for Log sources – LDAP, DNS, GeoIP, MITRE (optional)
7. Post-implementation: knowledge transfer and summary report

## Outcome and deliverables

Next XDR Expert solution will be deployed and configured, your administrator will know how to deploy and complete basic configuration. You will receive a Report of Completion.

## Notes

We can perform additional configuration, deployment, and many other tasks that fall outside the scope of our off-the-shelf Service Packages, through our custom Professional Services portfolio. Please contact your Account Manager to discuss creating a custom proposal for you.

Examples of such services include:

- Integration of event sources, including standard ones
- Development of custom parsers for non-standard event sources
- Tuning and development of detection (correlation) rules
- Configuration of various response actions
- Custom reporting

Our schedule of work will be based on the availability of the most suitable Kaspersky resources, but work will start no later than 15 days after we receive your written approval to start the project.

www.kaspersky.com