

kaspersky

基本安装服务：
Kaspersky Next XDR Expert

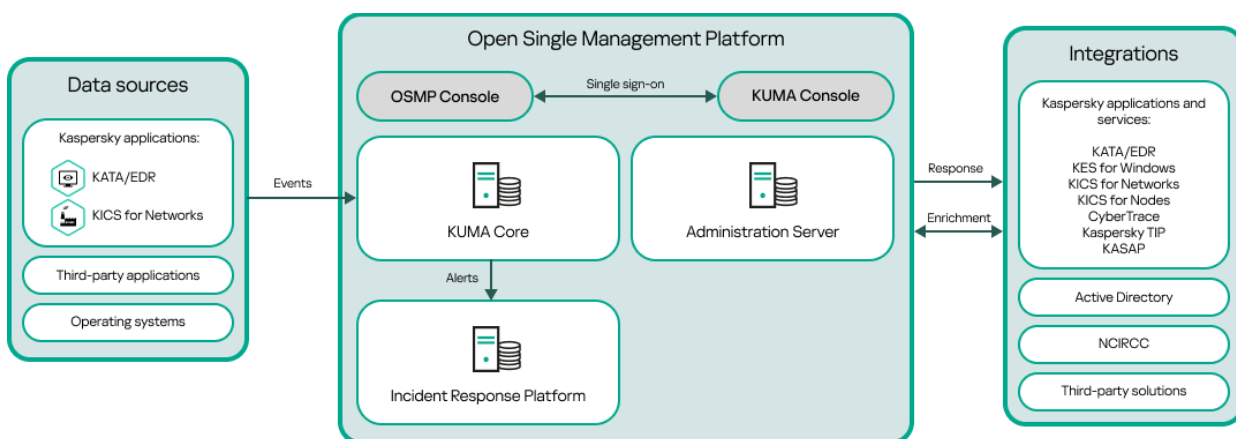
简介

卡巴斯基专家服务涵盖产品生命周期的各个阶段，提供从评估、实现到维护和优化等一系列服务。

Kaspersky Next XDR Expert 专为拥有雄厚资源和专属网络安全团队或安全运营中心（以下简称 SOC）的高成熟度企业而设计。此类组织积极采用最新技术，领先于威胁，并实施全面的安全解决方案。

Kaspersky Next XDR Expert 构建于我们的 Open Single Management Platform 之上，该平台集成了所有解决方案组件（包括卡巴斯基和第三方工具），并支持它们之间的交互。它是我们统一的 IT-OT XDR 技术栈的重要组成部分，作为事故管理的核心组件，支持安全任务的管理和维护。

Kaspersky Next XDR Expert 的组件及其交互：



通过将 Kaspersky Unified Monitoring and Analysis Platform（以下简称 KUMA）与其他解决方案和系统集成，可提高威胁监控和响应的效率，并扩展保护范围。

Kaspersky Next XDR Expert 包含以下主要组件：

1. Open Single Management Platform（以下简称 OSMP）。Kaspersky Next XDR Expert 的技术基础。OSMP 集成了所有解决方案组件，并支持它们之间的交互。OSMP 具有可扩展性，并支持与卡巴斯基应用程序和第三方解决方案集成。
2. OSMP 控制台。提供 OSMP 的 Web 界面。
3. KUMA 控制台。提供 Kaspersky Unified Monitoring and Analysis Platform 的 Web 界面。
4. KUMA Core。KUMA 的核心组件。KUMA 接收、处理和存储信息安全事件，然后使用关联规则分析这些事件。分析完成后，如果满足关联规则的条件，KUMA 将创建警报并将其发送到事故响应平台。

5. 事故响应平台。Kaspersky Next XDR Expert 的一个组件，允许您自动或手动创建事故、管理警报和事故的生命周期、将警报和事故分配给 SOC 分析师，以及自动或手动（包括通过行动手册）对事故做出响应。
6. 管理服务器（也称为服务器）。它是客户端组织关键的端点保护组件。管理服务器通过 EPP 应用程序提供端点保护的集中部署和管理，并允许您监控端点保护状态。
7. 数据源。用于生成事件的信息安全硬件和软件。通过将 Kaspersky Next XDR Expert 与所需数据源集成后，KUMA 将接收事件并进行存储和分析。
8. 集成。卡巴斯基应用程序和第三方解决方案与 OSMP 集成。通过集成后的解决方案，SOC 分析师可以增强事故调查所需的数据，并对事故做出响应。

服务范围

一体化部署方案（1 台服务器：OSMP 工作节点 - Kubernetes 工作节点 + DBMS；1 台服务器：KUMA 服务节点 - 收集器、关联器、存储），EDR 基本配置，连接最多 7 个标准事件源，与最多 3 个卡巴斯基解决方案或基础架构服务集成。

服务时间表

此服务最多需要 15 个工作日内来完成目标。若全部内容交付完毕且您验收满意，即使实际工作日不足 15 日，项目也将被视为“完成”。

服务可分为以下几个阶段：

- 启动会议、检查清单填写和范围确认
- 部署和基本配置（一体化部署方案，2 台服务器）；
- 连接事件源、集成卡巴斯基解决方案
- 实现后工作

要求及其他信息

请注意，如未完全满足以下列出的要求，卡巴斯基没有义务提供或尝试提供此服务。

此服务以远程方式交付。为了准备和提供部署方案，您需要提供卡巴斯基工程师要求的数据。

在服务交付期间，贵公司 IT 部门或安全团队的代表必须始终在岗，以满足卡巴斯基工程师提出的任何合理要求，包括权限、访问等。

该服务基于当前受支持的 Kaspersky Extended Detection and Response Expert 版本提供，并遵循应用程序生命周期期限：

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

部署过程中出现的任何技术问题将通过我们的支持服务进行解决。

工作范围

1. OSMP 平台部署：

- 1.1. 验证硬件要求和先决条件
 - 1.2. 安装操作系统并执行初始配置
 - 1.3. 安装和配置 PostgreSQL 数据库
 - 1.4. 建部署 YAML 文件
 - 1.5. 通过 KDT 安装 OSMP 平台
2. Kaspersky Security Center for Linux (KSCL) 配置：
 - 2.1. 激活 Kaspersky Security Center 授权许可
 - 2.2. 配置 Kaspersky Security Center 管理服务器设置和存储库更新任务
 - 2.3. 创建和配置 Kaspersky Security Center 强制性策略和任务
 - 2.4. 配置设备发现
 - 2.5. 创建组结构
 - 2.6. 在端点上部署网络代理（最多 50 个）
 - 2.7. 集成 — 域轮询、Kerberos 身份验证、SMTP 通知、SIEM（可选）
 - 2.8. 部署和配置连接网关（可选）
 - 2.9. 创建和配置备份任务
3. Kaspersky Endpoint Security (KES) 部署：
 - 3.1. 创建和配置安装包和远程部署任务
 - 3.2. 分批部署 KES 保护（最多 50 个）
4. Kaspersky Sandbox 部署：
 - 4.1. 验证硬件要求和先决条件
 - 4.2. 使用 ISO 部署 OSMP 沙盒
5. Kaspersky Endpoint Detection & Response (KEDR) 配置：
 - 5.1. 配置 KEDR 和沙盒设置
 - 5.2. 在沙盒上安装虚拟机镜像
 - 5.3. 在沙盒上配置恶意软件界面
 - 5.4. 部署 EDR 代理（KES 的一部分）
6. Kaspersky Extended Detection & Response (XDR) 配置：
 - 6.1. XDR 和 KUMA 初始配置
 - 6.2. 配置收集器、关联器和存储
 - 6.3. 集成 — Kaspersky Security Center 和沙盒
 - 6.4. 集成 — LDAPS 与 KUMA 集成（可选）
 - 6.5. 使用 OSMP 接入日志源（最多 10 个预置日志源）
 - 6.6. 配置日志源的事件增强 — LDAP、DNS、GeoIP、MITRE（可选）
7. 实现后工作：知识转移和总结报告

成果和交付物



完成 Next XDR Expert 解决方案的部署和配置，您的管理员将了解如何部署和完成基本配置。
您 将 收 到 一 份 完 成 报 告 。

备注

我们可以通过定制化的专业服务组合，执行超出我们现有服务包范围的额外配置、部署以及其他多项任务。请联系您的客户经理，讨论如何为您定制专属方案。

此类服务的示例包括：

- 事件源集成，包括标准事件源
- 非标准事件源的自定义解析器开发
- 检测（关联）规则的调优和开发
- 各种响应操作的配置
- 自定义报告

我们的工作安排将根据卡巴斯基适配资源的可用情况而定，但开始时间不晚于收到您书面项目启动批准后的 15 天内。



www.kaspersky.com.cn

© 2026 AO Kaspersky Lab。

保留所有权利。注册商标和服务标志均为其各自拥有者的财产。