# 卡巴斯基新一代安全-EDR 专家版

为您的端点基础设施提供强大、先进的保护

kaspersky 引领未来

**卡巴斯基**
**新一代安全- EDR 专家版**

卡巴斯基新一代安全- EDR 专家版是全面的扩展检测和响应 (EDR) 平台， 它是卡巴斯基新一代安全系列的高级产品，也是该系列重要的组成部分。卡巴斯基新一代安全- EDR 专家版在您的整个基础设施中部署主动防御，针对复杂的威胁提供终极网络安全防护。

# 卡巴斯基新一代安全- EDR 专家版

数据、用户和企业系统相互关联，而端点仍然是网络攻击者的主要目标，因此不仅需要实施预防性的威胁技术，还要采取先进的安全措施。

**卡巴斯基新一代安全- EDR 专家版**是一款强大的端点检测和响应解决方案，可与端点保护平台 (EPP) 结合使用来阻止大规模攻击。它还能自动扫描更加复杂的网络威胁，主动进行事件调查，并为 IT 专家提供所需的全面响应工具来有效开展工作。

卡巴斯基新一代安全- EDR 专家版能够迅速遏制威胁，并消除分布式基础设施中的事件。它能够支持并提升 IT 安全部门的工作：通过单一代理商提供全方位的端点保护，减少已安装产品所需的维护和支持，因此不会影响性能。

## 奖项

我们的技术定期接受独立测试实验室的测试，而我们产品的质量也得到了领先分析机构的认可。我们已赢得诸多国际奖项。

## 卡巴斯基新一代安全- EDR 专家版能够为您的企业提供的优势：

- 通过屡获殊荣的 EPP 和强大的 EDR 功能，提高您的安全防护效率
- 加强您对端点基础设施的控制
- 改进对高级威胁的检测和补救措施
- 通过资源分配的优化，帮助建立威胁检测、事件管理和响应流程
- 在符合监管要求和标准的基础上为您提供支持

## EDR

### 2 检测

基于 IoC、IoA 和自定义规则的威胁发现

利用全球威胁情报丰富信息的检测

主动威胁捕获和回顾性分析

### 3 调查

深入调查和根本原因分析

基本数字取证工具包

### 4 响应

支持各种响应操作

## EPP

### 1 防御

强大的反病毒引擎

多层安全控制措施和数据保护

漏洞和补丁管理

行为分析和自适应异常控制

# 关键功能

卡巴斯基新一代安全- EDR 专家版提供了企业基础设施中的所有端点的全面概览，而且实现了威胁调查中的每个阶段的可视化。强大的检测引擎和根本原因分析工具确保了威胁检测和调查的高效性和有效性。

回顾性分析以及 MITRE ATT&CK 知识库检测关联，让您能够识别攻击者所使用的战术和技术。该产品还提供主动威胁捕获功能和卡巴斯基威胁情报门户的访问权限，让专家能够重现攻击者的行动顺序，甚至可以抵御最复杂的攻击。

## EPP

### 领先的预防技术，包括基于机器学习 (ML) 的技术

- 自动阻止威胁
- 自动恢复
- 防止加密尝试
- 防止漏洞被利用
- 防止凭证被盗

### 安全和数据控制措施

- 应用程序控制
- Web 控制
- 设备控制
- 自适应异常控制
- 加密和策略管理
- 便携式设备加密

### 漏洞评估和补丁管理

- 高级补丁管理
- 漏洞评估
- 授权许可管理
- 集中式应用程序和操作系统部署
- 远程管理工具
- 资产清查

## EDR

### 自动检测高级威胁

- 数据收集和存储
- 基于攻击指标 (IoA) 规则的高级检测机制
- 自动访问威胁情报 (KSN)
- 回顾性分析
- MITRE ATT&CK 映射

### 入侵指标 (IoC) 搜索和威胁捕获

- 完全可见性和控制
- 事件优先排序
- IoC 扫描
- YARA 规则
- 可访问威胁捕获
- 灵活的查询构建器，实现主动威胁捕获

### 响应

- 事件响应工具
- 自动化响应任务设置
- 响应建议
- 威胁控制
- 集中式事件本地化

# 卡巴斯基
# 新一代安全- EDR 专家版

了解更多

www.kaspersky.com.cn

© 2024 AO Kaspersky Lab。
注册商标和服务商标归其各自所有者所有。

#kaspersky
#bringonthefuture