



核心功能

面向所有人	面向中小型企业			面向各种规模的企业	
卡巴斯基 新一代安全 EDR 基础版	卡巴斯基 新一代安全 EDR 优选版	卡巴斯基 新一代安全 XDR 优选版	卡巴斯基 新一代安全 MXDR 优选版	卡巴斯基 新一代安全 EDR 专家版	卡巴斯基 新一代安全 XDR 专家版

- 自动化防御大规模威胁 - 系统加强 - 云发现	●	●	●	●	●
- 针对复杂威胁的端点检测和响应 - 补丁管理 - 远程抹除 - 加密管理 - 移动安全管理（内置 MTM+EMM） - 面向 IT 管理员的网络安全培训		●	●	●	●
- 云组织 - 数据发现 - 网络安全解决方案 - Microsoft Office 365		●	●	●	●
- 警报聚合¹ - 来自警报卡的 Active Directory 响应¹ - 卡巴斯基云沙盒²			●	●	
卡巴斯基自动化安全意识平台³		●	●		●
卡巴斯基 SOC 提供全天候不间断监控、威胁搜索与调查服务，同时配套其他 MDR 功能⁴			●		
- 针对复杂和持续性威胁的高级端点检测和响应 - 内置高级沙盒 - 服务管理（仅限 Windows） - 取证				●	●
- 针对复杂和持续性威胁的扩展检测和响应 - 用于数据收集、规范化、监控和关联的互相关引擎 - 电子邮件安全 - 混合云安全 100 次卡巴斯基威胁搜索请求支持					●

¹ 相较于卡巴斯基新一代安全 XDR 优选版，卡巴斯基新一代安全 XDR 专家版提供更丰富的聚合与响应功能选项
² 授权许可中包含卡巴斯基威胁情报门户的查询配额（折合 0.5 用户数）
³ 授权许可中包含卡巴斯基自动化安全意识平台的访问权限（折合 0.2 用户数）
⁴ 有关完整功能明细，详见卡巴斯基新一代安全专家版和卡巴斯基新一代安全优选版功能清单。某些功能的可用性可能因部署方式和所选授权许可而异。

了解更多

基础版功能	优选版功能	专家版功能 ³
自动保护免受大规模威胁 • 多层反恶意软件 • 行为检测 • 漏洞入侵防护 • 通用 Linux 内核模块 (ULKM) • 修复引擎 • 端点级别的文件、电子邮件、网页和网络威胁防护 • 防火墙 • 主机入侵防护 • AMSI 防护 • BadUSB 攻击防御 • 使用警报卡进行根本原因分析 • 通过卡巴斯基安全网络获取全球威胁情报 • 移动威胁防御	针对复杂威胁的端点检测和响应 • 具有自动跨端点响应的入侵指标 (IoC) 搜索 • 自适应异常控制 • 一键引导式响应 • 系统关键对象检查 • 将文件移至隔离区/从隔离区恢复文件 • 网络隔离/移除网络隔离 • 获取/删除文件 • 启动/终止进程 • 关键区域扫描 • 执行预防 • 执行命令 系统加强 • 补丁管理 • 远程抹除 • 加密管理 • 移动安全管理（内置 MTM+EMM） 云安全 • 云组织 • 数据发现 • Microsoft Office 365 安全：Exchange、OneDrive、SharePoint、Teams IT 培训 • 面向 IT 管理员的网络安全培训	针对复杂威胁的扩展检测和响应 • 警报聚合 • 来自警报卡的 Active Directory 响应 自动化安全意识平台 • 灵活的员工安全意识培训 • 提供 25 种语言的定制课程 • 安全意识仪表板及报告 • 视频和音频培训格式 • 来自警报卡的自动化安全意识平台响应 卡巴斯基云沙盒 • 在云沙盒中上传和执行文件 • 从网页地址上传文件，然后在云沙盒中执行 • 反规避功能，以对抗旨在避免沙盒的恶意软件 • 执行从云沙盒报告中提取的文件 • 导出分析结果 • 自动检测文件类型 • 管理执行的过时任务 托管保护 • 全天候持续监控和威胁搜寻 • 提交事件供卡巴斯基 SOC 进行进一步调查 • 与 SOC 团队就事件进行直接沟通 • 通过电子邮件/Telegram 通知事件 • 引导式和自动响应方案 • 用于与 IRP/SOAR 集成的 REST API • 人工智能机制加速事件调查 • 资产当前状态的可见性 • 与第三方 EPP 应用程序兼容 • 易操作的 MDR 门户控制面板 • 定期报告 • 原始遥测数据可存储 3 个月 • 泄露凭证洞察 针对复杂和持续性威胁的高级端点检测和响应 • 端点遥测收集 • 主动威胁捕获和回顾性分析 • 攻击指标 (IoA) 高级检测 • YARA 规则 • MITRE ATT&CK 映射 内置高级沙盒 • 模拟对象的多级评估和行为分析 • 管理虚拟机模板 • 内置专用网络界面，用于监测恶意对象与互联网资源的交互 • 模拟普通用户的操作 • 抵御恶意软件所用的现代沙盒绕过技术 服务管理（仅限 Windows） • 启动/停止/删除/暂停/恢复服务 • 修改自动服务类型 取证 • 处理，文件，自动运行列表 • 进程内存转储 • 内存转储 • 磁盘映像 • NTFS 服务文件 • 注册表项 针对复杂和持续性威胁的扩展检测和响应 • 具有时间表模式的调查图 • 事件响应，使用 SLA 进行灵活的案例管理 • 行动手册：响应自动化和编排 • 部署工具包和开放 API • 视觉行动手册编辑器 用于数据收集、规范化、监控和关联的互相关引擎 300 多个第三方连接器 • 控制面板和报告 • 具有数据湖的日志管理 • 高级威胁检测和相互关联 • 警报聚合和资产管理 • 域控制器数据获取和响应 • 基于人工智能的资产风险评估 • DLL 劫持人工智能检测 • AI 检测账户盗窃 • AI 赋能的事件汇总 • 基于生成式 AI 的 SOC 分析师助手 • 资源依赖关系图 电子邮件安全 • 基于机器学习的恶意软件、垃圾邮件和网络钓鱼检测 • 多种部署选项（SEG、云、独立） • 内容过滤 • 使用 SPF、DKIM 和 DMARC 进行电子邮件发件人身份验证 • 集成功能 • 扩展数据导出至 SIEM • 通过与 KATA 中的网络沙盒原生集成展开附件分析 混合云安全 • 系统完整性监控 • 日志检查 • 私有云支持：VMware、Red Hat Enterprise Linux、KVM • 公共云支持：Google Cloud、Microsoft Azure、AWS

³基础版与优选版的多数功能在专家版中同样适用，但部分功能存在差异，例如 MXDR、KASAP 等功能的可可用性。请参阅卡巴斯基新一代安全专家版和卡巴斯基新一代安全优选版功能列表。某些功能的可用性可能因部署方式和所选授权许可而异。