



历经验证的多层防护，
筑牢企业邮箱全方位安全屏障。

卡巴斯基 邮件服务器安全

kaspersky



81%

的全球企业曾面临电子邮件攻击*

44%

的全球企业邮件流量均为垃圾邮件*

抢占先机，从容应对演进中的邮件安全威胁

电子邮件仍是全球应用最广泛的商务沟通工具，也是最主要的网络攻击路径之一。随着攻击者快速迭代手段并扩大威胁范围，攻击事件持续增加，包括勒索软件、二维码诈骗，以及利用 AI 深度伪造并精准冒充可信发件人的高仿攻击。这些攻击手段足以瓦解邮件系统自带的防御，使收件箱暴露于安全漏洞之中，导致企业遭受动辄数百万美元的损失。

无论企业规模大小，仅靠系统自带的基础邮件安全防护已远远不够。唯有先进的安全解决方案，方能确保当下的通信安全。

加固企业通信核心：邮件安全再升级

卡巴斯基邮件服务器安全 (KSMS) 是一款全方位的邮件安全平台，为商务邮件通信提供坚实的多层防护。该平台由机器学习及全球领先的威胁情报数据赋能，并与卡巴斯基产品组合无缝集成。

卡巴斯基邮件服务器安全涵盖所有邮件安全相关任务：



确保企业邮件交换安全可信、高效顺畅



显著降低邮件传播攻击带来的安全风险



实现对邮件基础设施的全方位可视化监控



支持随企业邮件基础设施扩展而轻松扩容

卡巴斯基邮件服务器安全的核心组件

卡巴斯基邮件服务器安全包含**三个组件，全部由单一授权许可提供**。支持组合使用以实现全面覆盖，亦可按需灵活选择。该产品支持多种部署与集成选项，包括一体化 SEG 软件设备、适用于 Microsoft Exchange 的 API 集成方案，以及保护 Microsoft 365 服务的云托管 SaaS 方案。



卡巴斯基
网络安全解决方案
邮件网关

本地部署

云端

虚拟或独立硬件设备



卡巴斯基
网络安全解决方案
Microsoft Office 365

SaaS



卡巴斯基
网络安全解决方案
Microsoft Exchange
Server

本地部署

* 数据来自卡巴斯基全球研究与分析团队和卡巴斯基威胁研究

关键电子邮件防护技术

卡斯基邮件服务器安全在邮箱和网关级别提供强大的电子邮件威胁防护,由先进的检测和响应引擎提供强大动力。

主要技术包括:

- 1

全方位反垃圾邮件保护
- 2

增强型内容过滤
- 3

加密压缩包安全扫描
- 4

精准防范网络钓鱼
- 5

强大的发件人身份验证功能
- 6

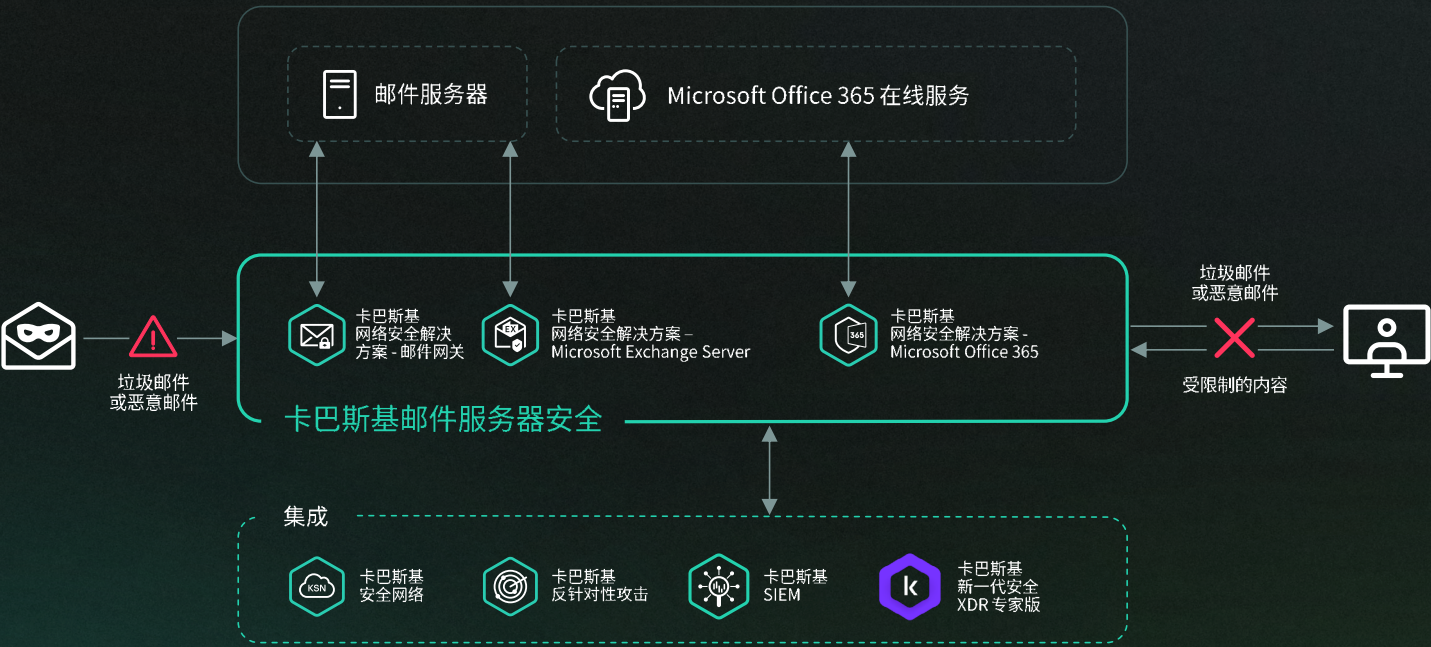
关键内容净化与重构
- 7

反恶意软件防御
- 8

高级沙盒检测技术
- 9

链接安全扫描

工作原理



为何选择卡巴斯基？



单一许可覆盖多种邮件安全用例与部署场景



依托历经验证的威胁情报与全球信誉数据，为 KSMS 提供实时防护支持



采用生态系统方法，实现与卡巴斯基其他安全解决方案的无缝协同



基于专有机器学习技术的多层防护矩阵，精准识别复杂威胁



清晰的授权模式：提供基础版 KSMS 以及具备扩展安全功能的高级版 KSMS Plus

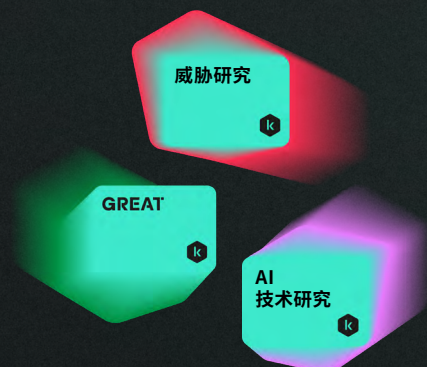


KSMS 及其引擎已通过全球多家权威分析机构与测试实验室的独立验证

深厚专业知识筑就的技术领先优势

卡巴斯基邮件服务器安全依托卡巴斯基专业中心多年的专业经验与实战技能，帮助应对严峻与复杂的网络威胁。

[了解详情](#)



卡巴斯基 网络安全解决方案 邮件服务器安全

[了解详情](#)

www.kaspersky.com.cn

© 2026 年 AO 卡巴斯基实验室。
注册商标和服务标志归其各自所有者所有。

#卡巴斯基
#引领未来