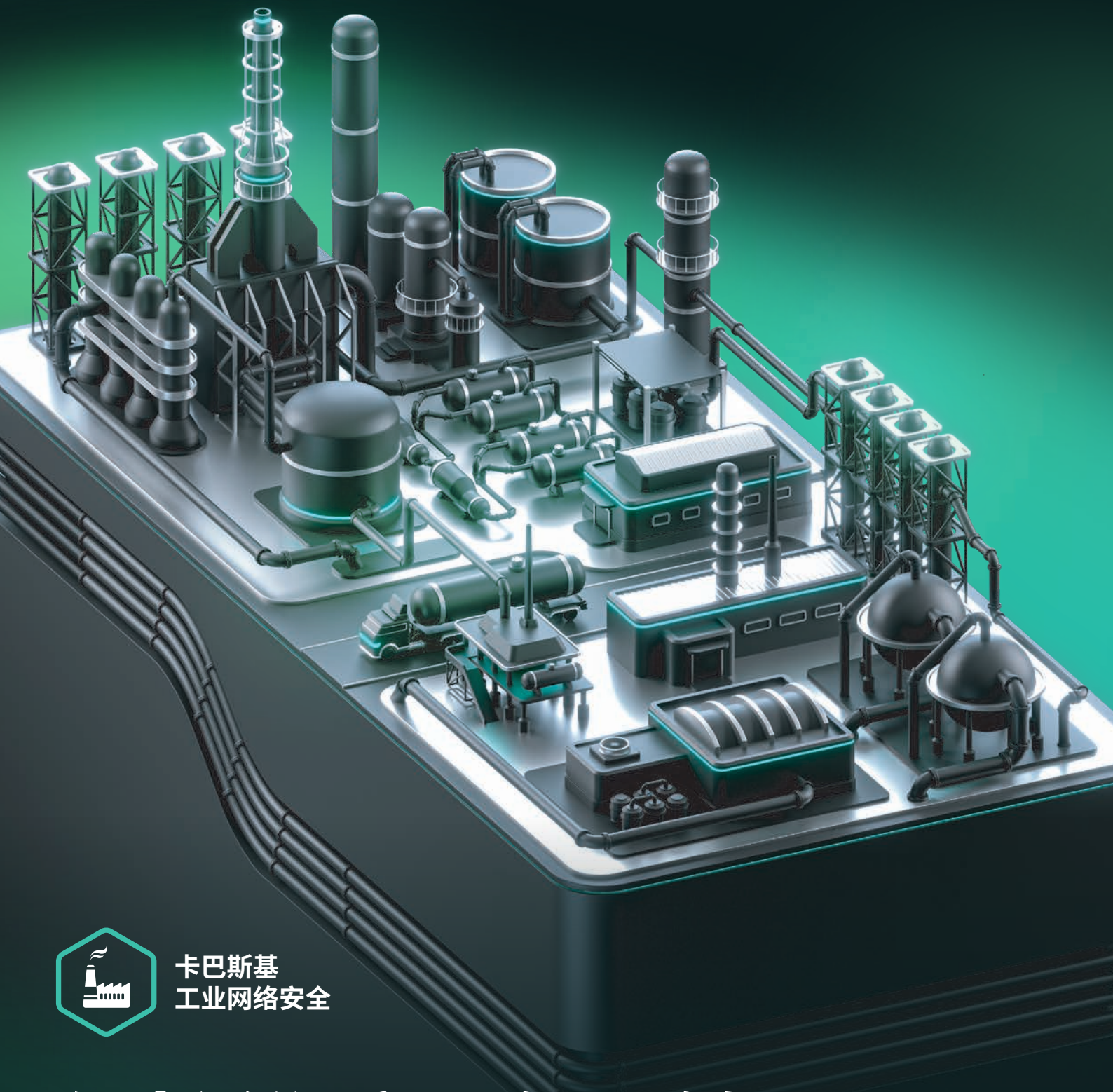
kaspersky



卡巴斯基
工业网络安全

# 保护维系业务运转的核心设施

kaspersky

# 关键基础设施态势感知和风险暴露控制

卡巴斯基工业网络安全 (KICS) 平台专用于为运营技术 (OT) 环境提供多层防护。它可确保技术流程的连续性和控制系统的可用性。


## 核心业务成果

统一 OT、SecOps、IT 和业务部门之间的工作流程，强化内部协同

抢占数字化转型先机，以安全架构推进工业 4.0 创新，保障关键流程稳定

保障数据主权，实现成本透明管理

精简内部、监管及行业合规流程，保障业务顺畅

依托可扩展的解决方案，灵活应对网络威胁变化

无缝集成卡巴斯基专业 IT 网络安全产品，提升整体防护效能。

kaspersky

# KICS XDR 平台能力

- 资产发现
- 漏洞和风险
- 网络可见性
- 流量分析工具集

- 入侵检测
- 异常检测
- 工业协议 **DPI**
- 事件关联
- 智能事故评分

- 卡巴斯基 **OT** 网络安全生态系统内，一系列第三方集成方案协同运作，发挥出潜在的联动效能。

- 实时威胁防御
- 本地活动控制
- 网络活动控制
- 系统监控


- 恶意软件扫描程序
- 漏洞
- 合规性
- 流量捕获
- 主机清查

- 端点遥测数据（进程、文件及网络活动）
- 响应措施
- 威胁发展链

- 单主机 - 网络事故
- 调查图表
- 警报充实
- 手动响应操作
- 网络访问限制

- 漏洞扫描
- 合规性审计
- 配置变更监控

- 扩展主机监控
- 硬件和应用程序清查
- 盲区覆盖（无界模式）

## 运营效益

### 占用空间小

凭借模块化部署以及灵活的可调节资源消耗设计，KICS 既不会影响系统性能与流程连续性，还能防止软件出现膨胀现象。

### 兼容性

支持超过 125 个 Windows 和 Linux 系统版本，且已完成对 200 多个工业自动化和控制系统 (IACS) 及设备的测试验证，支持您与现有基础设置相兼容。

### 原生集成

卡巴斯基工业网络安全解决方案节点安全 (KICS for Nodes) 与卡巴斯基工业网络安全解决方案网络安全 (KICS for Networks) 两款解决方案紧密协作、相得益彰，实现无阻碍集成、集中化管理以及扩展的跨产品功能，为企业网络安全提供支撑。

kaspersky

# 解决方案架构和应用场景

### 具备 AI 剖析功能的高级资产管理

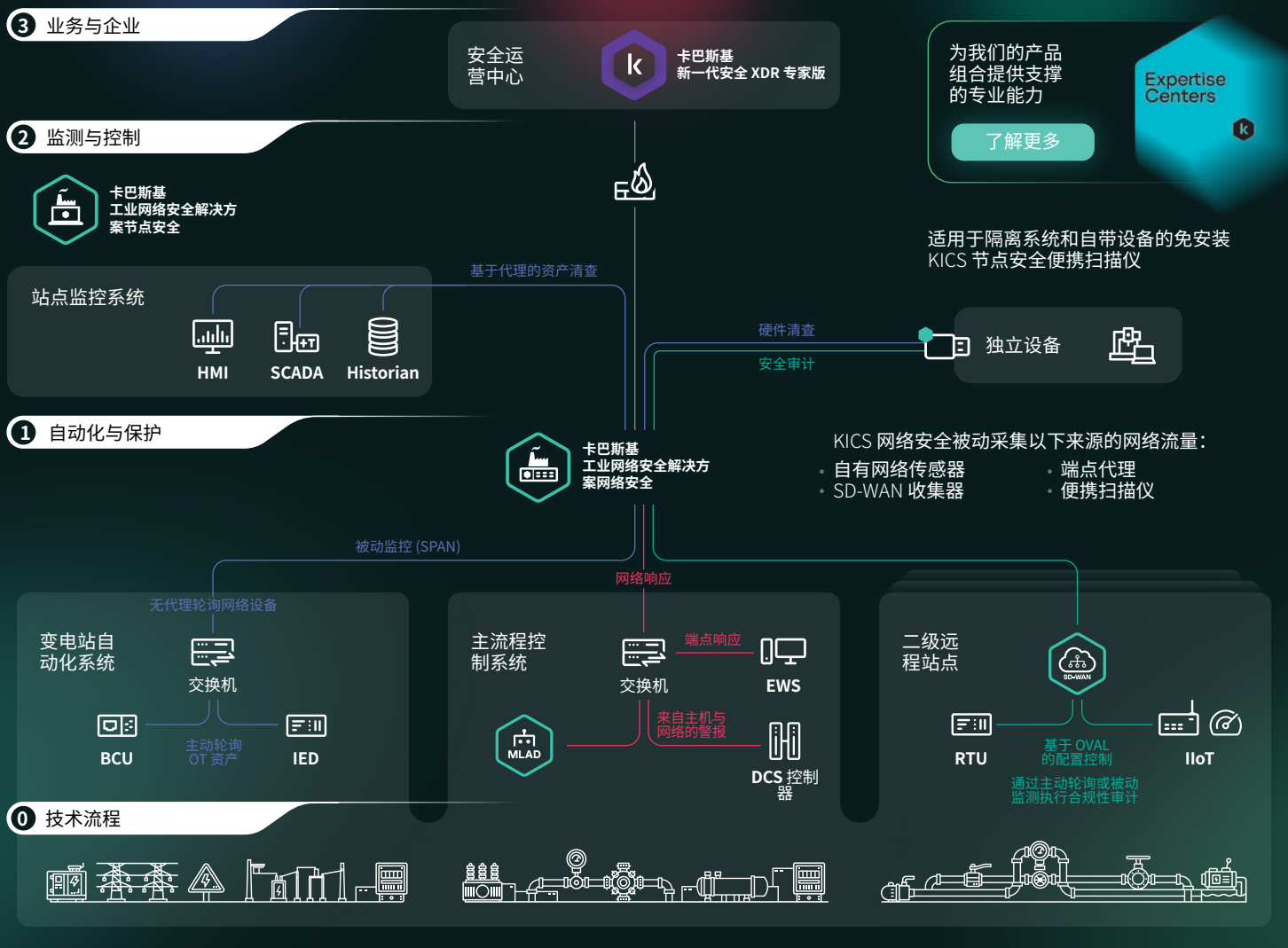
借助资产发现工具集与多方面的网络可见性，识别连接的设备及其交互情况，从而掌控影子基础设施，确保无未知设备隐患。

### 扩展检测和响应

可检测恶意或不安全活动，在威胁影响业务之前进行有效遏制。系统支持检测超 5,000 种网络攻击，对 50 多种工业协议进行深度数据包检测 (DPI)，并提供针对性的安全响应方案。

### 持续安全审计

借助 3,100 多条预定义审计规则和 1,300 多项 OVAL 漏洞测试，对分布式、“气隙”式及高敏感隔离环境展开安全评估，洞悉其安全态势。




## 集成案例

**卡巴斯基新一代安全 XDR 专家版**

KICS 平台与卡巴斯基新一代安全 XDR 专家版结合使用，可提供统一的 IT-OT XDR 能力，并为融合基础设施提供综合防护。

**卡巴斯基异常检测机器学习**

与异常检测机器学习 (MLAD) 解决方案集成后，KICS 网络安全可发送遥测数据以进行分析，并接收针对检测到的异常情况的警报。

**卡巴斯基 SD-WAN**

KICS 可利用 SD-WAN 基础设施收集工业流量、提供集中监控，并保护分布式工业对象和系统。

kaspersky.com



了解更多关于卡巴斯基保护 OT 系统和网络各层级免遭网络-物理威胁的技术、知识与专业能力

卡巴斯基工业网络安全

了解更多