保障工业企业可持续发展
和数字化转型的安全平台

卡巴斯基工业网络安全平台

kaspersky 引領未來

被恶意软件攻击

自 2022 年初以来，近 30% 的与 ICS 相关的计算机受到恶意软件攻击，比上一年减少了近 10%

卡巴斯基 ICS CERT，
2022 年 6 月

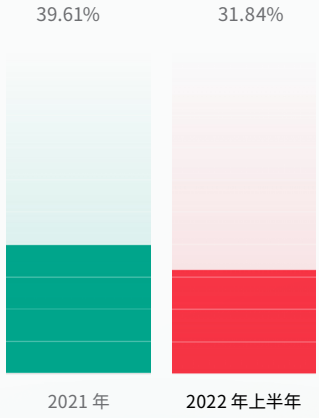
了解更多

工业企业针对其 IT 和 OT（运营技术）基础设施采用不同的网络安全防御措施。大多数企业已经在其企业网络中部署了成熟的检测和响应方案，但在 OT 方面，他们通常还是依赖过时的气隙方法。工业企业正变得越来越“数字化”，不断加大对智能技术、新型自动化系统和数字化转型举措的投资。这实际上弥合了 IT 和 OT 环境之间的传统鸿沟，而这条鸿沟在过去可以防止网络威胁入侵工业自动化和控制系统。

您也可能成为目标，但不要成为受害者

无论是意外的气隙破坏，还是恶意软件感染，您都可以避免成为受害者。哪怕是一个闪存驱动器、手机、网络钓鱼电子邮件或勒索软件，如果进入 ICS 环境，也会对公司的核心业务造成严重影响。同时，动机明确的黑客组织可能会入侵 OT 网络，对设备、流程、生产、安全和质量造成巨大破坏，他们也可能窃取有价值的信息。

自 2022 年初以来已拦截恶意对象的 ICS 计算机占比



为 OT 提供必要的网络安全防护

端点保护

保障独立和连接系统的安全。一款安全且经过测试的解决方案应帮助执行安全策略、提供合规支持、执行安全审核、管理清单、进行漏洞修复，并发挥端点传感器的作用来收集精确的遥测数据

网络保护

为通信可见性、威胁检测和资产管理提供支持。网络流量分析和入侵检测系统可控制防火墙设置、网络分段和网络合规使用的有效性，并有助于提供安全的人工响应

培训计划

帮助员工减少事故和尽量避免人为因素（人为错误）导致的风险

专家服务

用以调查基础设施、执行专业分析或减轻安全事件带来的影响

享誉全球

Frost and Sullivan 基于对全球工业 (OT/ICS) 网络安全市场的分析，授予卡巴斯基 “2020 年全球年度公司” 奖项

VDC 在其年度全球调查中，依据工业自动化领域 250 多名合格专业人员的综合评分，将卡巴斯基评为工业网络安全类顶级供应商

卡巴斯基的产品和服务

卡巴斯基工业网络安全 (KICS) 平台提供原生集成的多项技术，结合我们的专家培训和服务组合，可满足工业企业和关键基础设施运营商在网络安全方面的所有需求。

该平台是独特的工业企业生态系统中的关键要素，包括：

- 卡巴斯基一流的企业解决方案，提供真正的 IT-OT 融合以及 “一家供应商、多重价值” 的优势
- 用于信息物理安全、工业物联网安全、机器学习、安全远程工作区的各类专业化解决方案，提供无限、灵活的扩展能力

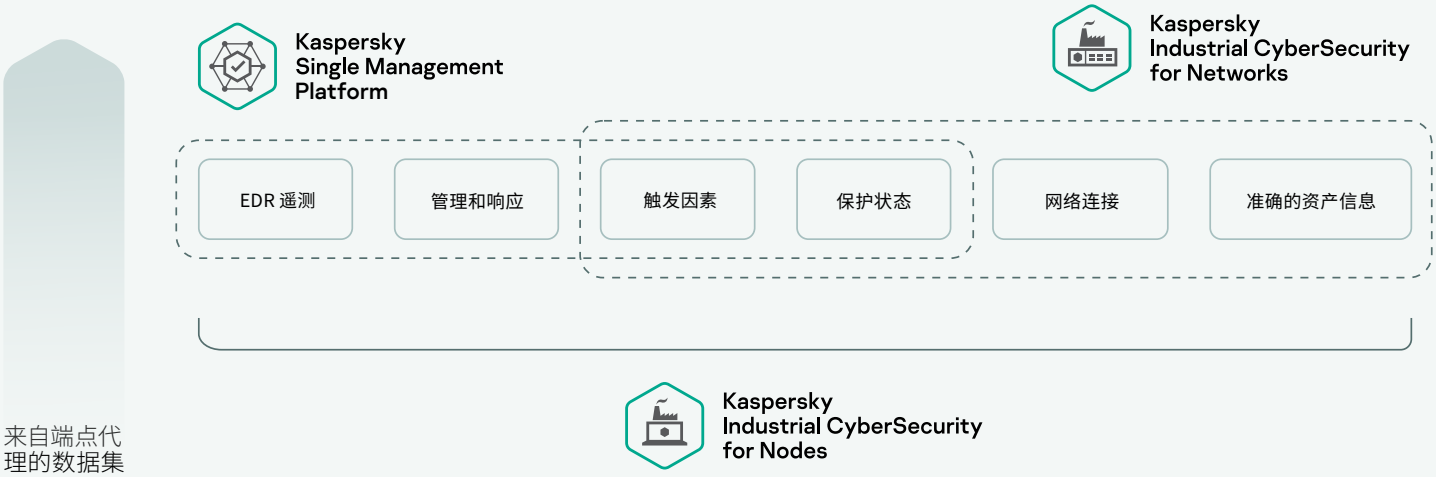
卡巴斯基工业网络安全平台在以下类别中处于领先地位：

- OT 端点安全
- OT 网络监控和可见性
- 异常检测、事件响应和报告
- OT 安全服务

搭配使用后，用户可以看到更大图景，并获取更广泛的背景信息：网络和端点级别的事件链、精确的资产参数、网络通信以及拓扑图（甚至是来自尚无法提供流量镜像的分段）。

产品

KICS 是一个 OT 网络安全平台，旨在全面保护各个级别的核心工业自动化和控制系统组件。平台组件无缝集成，帮助用户全面了解多个异地分布的 OT 网络和自动化系统，从而提升客户体验、情景感知能力和部署的灵活性。



卡巴斯基工业网络安全解决方案 - 节点安全 (KICS for Nodes) 是一款提供合规审核和端点传感器功能的端点保护、检测和响应软件。

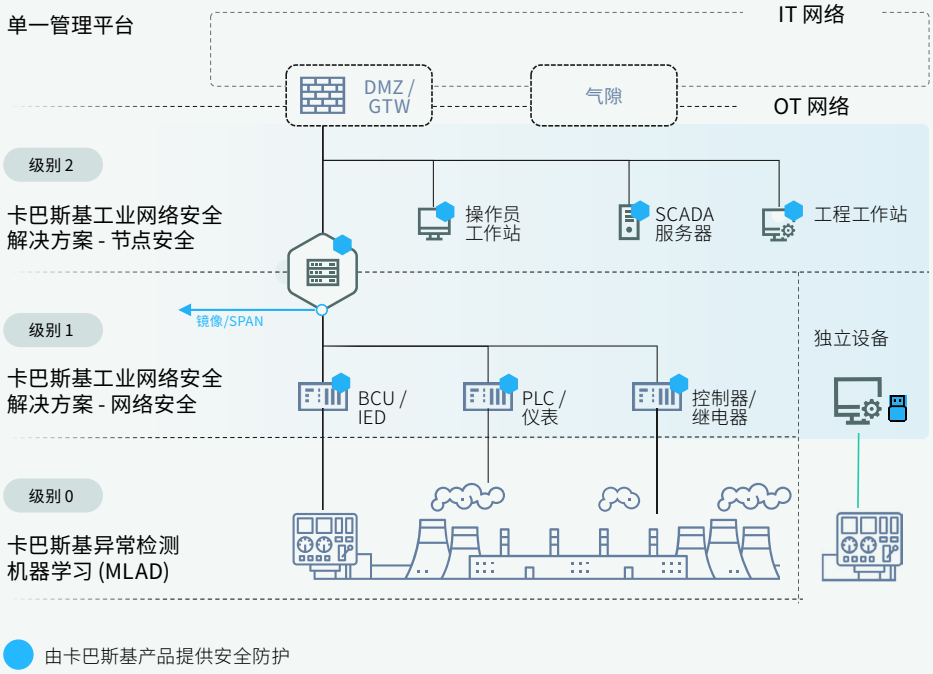
卡巴斯基工业网络安全解决方案 - 网络安全 (KICS for Networks) 用于 OT 网络流量分析、检测和响应。

单一管理平台为众多办公地点提供先进的 EDR 界面和快速扩展能力。

附加功能

该解决方案还提供多种附加功能。网络 **“主动轮询”** 技术可以快速准确地收集网络拓扑和资产设置。**“端点审核”** 功能有助于确保安全策略的合规性（包括当前设置的安全性）并控制漏洞。卡巴斯基工业网络安全解决方案 - 节点安全的 **“便携扫描仪”** 交付方式有助于确定独立气隙设备安全审核的最佳实践。**“异常检测机器学习”** 是一种深入技术过程的早期异常检测系统。

解决方案架构



特点

资产发现
被动 OT 资产识别和清点

深度包检测
技术流程遥测的近实时分析

网络完整性控制
检测未经授权的网络主机和流量

入侵检测系统
发送有关恶意网络活动的警报

指令控制
通过工业协议检测指令

外部集成
灵活的 API 集成带来了额外的检测和防御功能

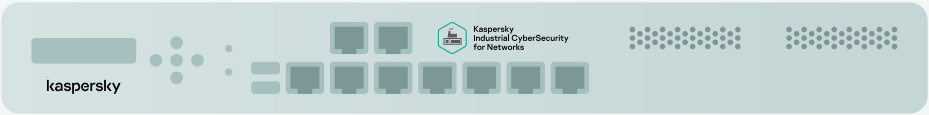
用于异常检测的机器学习
通过实时遥测和历史数据挖掘（递归神经网络）发现网络或设备异常

漏洞管理
由卡巴斯基 ICS CERT 提供支持的可更新工业设备漏洞数据库

Kaspersky Industrial CyberSecurity for Networks

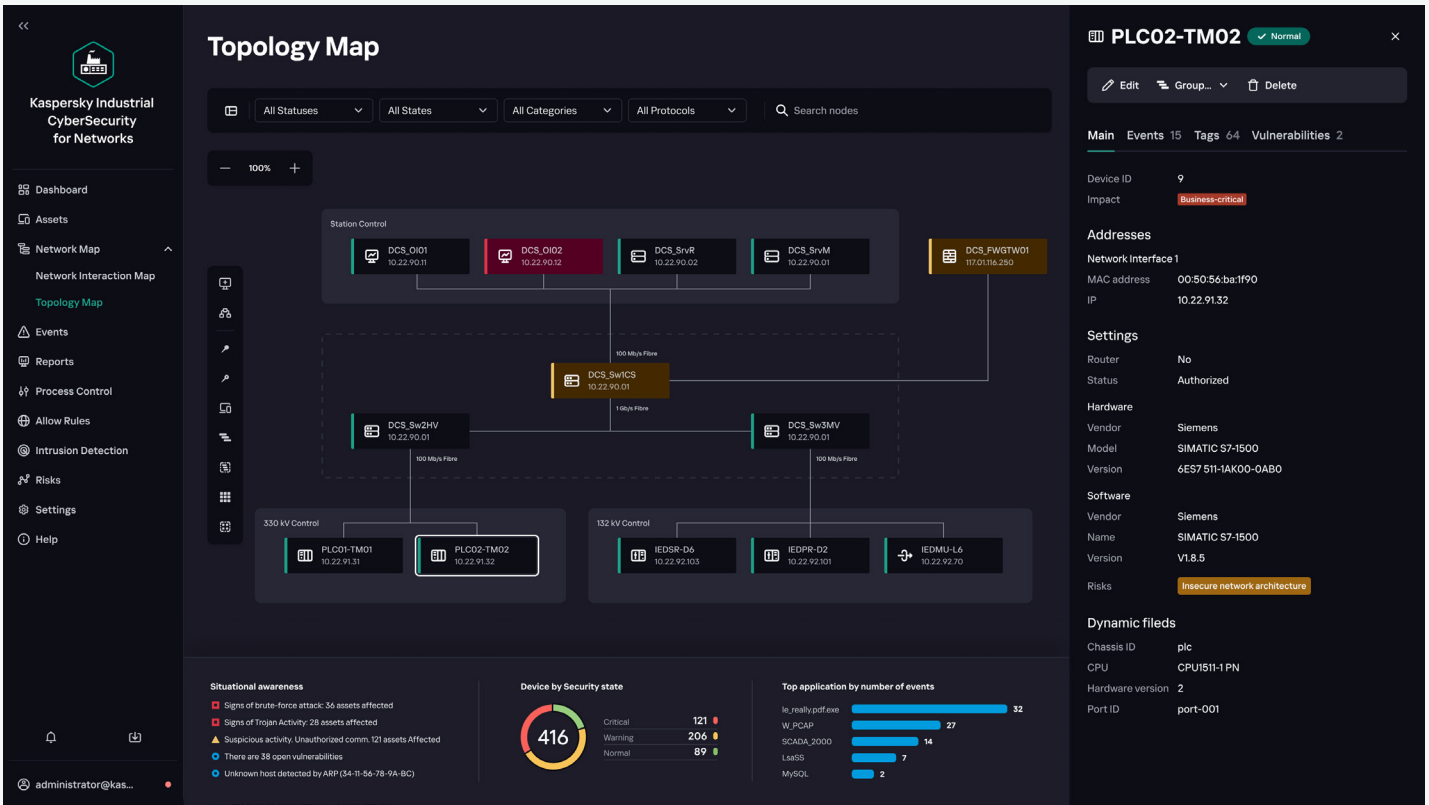
OT 网络流量分析、检测与响应。通过被动流量监控、主动轮询和端点传感器，提供清晰的风险可见性。

在异常和入侵出现初期对 ICS 网络进行检测，确保采取必要行动以防止对工业流程产生任何负面影响。



与设备无关的解决方案，可以快速并以最理想的方式集成到客户的既定采购、集成和质保实践中。

界面



卡巴斯基工业网络安全解决方案 - 节点安全可满足分布式自动化系统的严格要求：混合且复杂的环境、长运行时间、独立和关联的用例、有人值守和免维护的实例以及确保可控性的绝对优先。

Kaspersky Industrial CyberSecurity for Nodes

工业级、经过测试和认证的端点保护、检测和响应。适用于 Linux、Windows 和独立系统的影响小、兼容且稳定的解决方案。

工业端点保护、检测和响应

为现代化、数字、托管式和分布式自动化系统的每个端点提供保护。将根本原因分析流程中的事件可见性提升到更高水平。该代理收集端点遥测数据，从而以清晰、详细且直观的方式显示安全事件在工作站、服务器、网关和其他端点上的进展情况，确保事件得到妥善处理且不会再次发生，令自动化系统管理员安心无忧。

优点

对受保护设备的影响小，
确保实现最佳系统性能

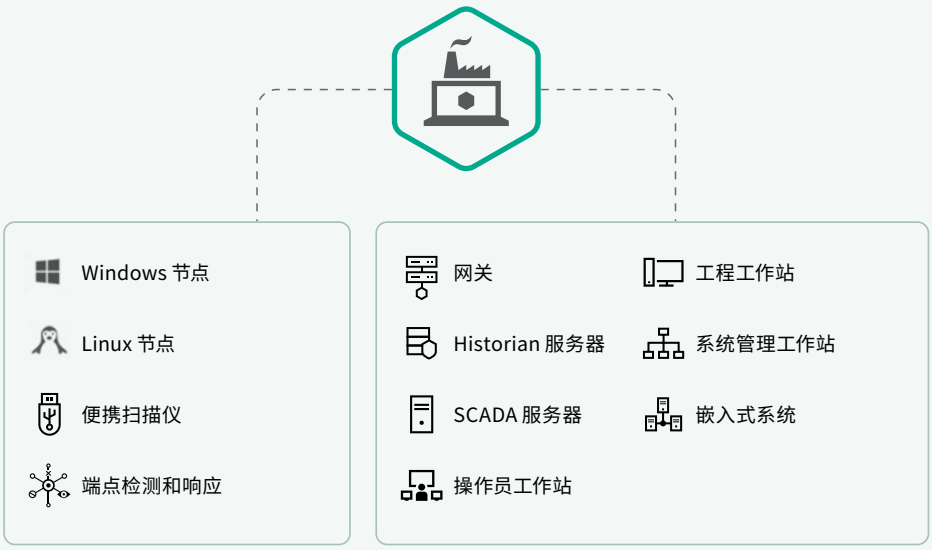
兼容
前几代的低性能计算机，
以及 Windows XP SP2
和 Windows Server 2003 SP1
及更高版本的系统

延长生命周期
许可有效期长达 5 年和延长支持服务

针对所有 MS 桌面、服务器和嵌入式 Windows 操作系统
提供完整功能

模块化部署
灵活的选项和安全的非侵入式设置

涵盖混合基础架构
Windows、Linux 及其可移植版本



卡巴斯基工业网络安全解决方案 - 节点安全 “便携式扫描仪”
在无法安装安全软件的独立机器、自动化系统或设备上实施网络安全策略。即便是独立的基础设施，也可提供终极情景感知和 OT 可见性。

免安装解决方案
卡巴斯基工业网络安全解决方案 - 节点安全可以在很多额外的 “便携式扫描仪” 闪存驱动器上激活。这有助于在维护窗口期间对多台计算机同时进行按需扫描，以收集端点数据并将其编制成一目了然的总结报告。

监管和内部政策合规
卡巴斯基工业网络安全解决方案 - 节点安全 “便携式扫描仪” 对访问 OT 站点的设备（包括第三方承包商的计算机）执行反恶意软件合规性检查。它占用的空间非常小，不会干扰现有的安全解决方案。

优点

情景感知

系统/策略管理

杀伤链和响应

报告和通知

SIEM 集成

HMI / MES 集成

Kaspersky
Single Management
Platform

单一管理平台是一个集中式安全管理解决方案，用于整个 OT 基础设施的安全编排，并提供所有异地分布式资产的地图，其中包含事件和事件分析等。该解决方案提高了混合 OT 和 IT 安全团队的效率。在这个平台上，所有安全控制措施可以协同运作，快速准确地做出响应。

专家服务

我们的服务套件是 KICS 产品组合的重要组成部分。
我们提供一整套安全服务，包括工业网络安全评估和事件响应。

工业网络安全评估

工业网络安全评估：卡巴斯基提供低侵入式工业网络安全评估，包括外部和内部渗透测试、OT 安全评估和自动化解决方案安全评估。卡巴斯基专家就公司的基础设施提供重要见解，并给出如何加强 ICS 网络安全防御能力的建议。

“ 与其他供应商相比，他们的 ICS 网络安全经验、专业技术和能够满足复杂需求的解决方案为我们创造了巨大价值，能够为我们公司未来安全战略的成功实施保驾护航。

Plzeňský Prazdroj
C&A 经理 Ond ej Sýkora

威胁情报

卡巴斯基专家收集的最新分析数据帮助客户更有效地抵御针对性工业网络攻击。分析数据以 TI 数据源或定制报告的形式呈现，可根据区域、行业和 ICS 软件参数来满足特定的客户需求。

“ 通过实践演习和学习卡巴斯基团队的专业知识，我们提升了对网络安全威胁的防御能力。

PacificLight 首席执行官
Yu Tat Ming

事件响应

一旦发生安全事件，卡巴斯基专家会收集并分析数据和恶意软件，重建事件时间表，确定可能的来源和动机，并制定详细的修复计划。计划包括从客户系统中删除恶意软件并回滚其恶意操作的建议。

培训和意识

> 卡巴斯基是为 ICS 集团提供专业工业网络安全技能培训的最佳公司。
>
> 首席技术官
> Søren Egede Knudsen

工业网络安全意识培训

为使用工业计算机化系统的员工及管理人员提供现场和在线互动培训与网络安全游戏。参与者会对当前威胁形势和专门针对工业环境的攻击媒介形成全新的认识，探索实用场景并掌握网络安全技能。

专家培训计划

ICS 渗透测试和 ICS 数字取证培训课程主要面向网络安全专业人员。参与者能够掌握在工业环境中进行全面渗透测试或数字取证所需的所有高级技能。

专业化解决方案生态系统

Kaspersky IoT Infrastructure Security

基于卡巴斯基的网络免疫方法为物联网提供网关级别的保护

了解更多

Kaspersky Antidrone

在任何规模的设施中保护空域免受无人机的攻击

了解更多

Kaspersky Secure Remote Workspace

具有网络免疫系统的功能性瘦客户端基础设施

了解更多

Kaspersky Security CAD

对用于设计和运营阶段的信息安全系统进行数字化建模

了解更多

Kaspersky Machine Learning for Anomaly Detection

工业技术流程中的早期异常检测系统

了解更多

Kaspersky Industrial CyberSecurity

了解更多

www.kaspersky.com.cn