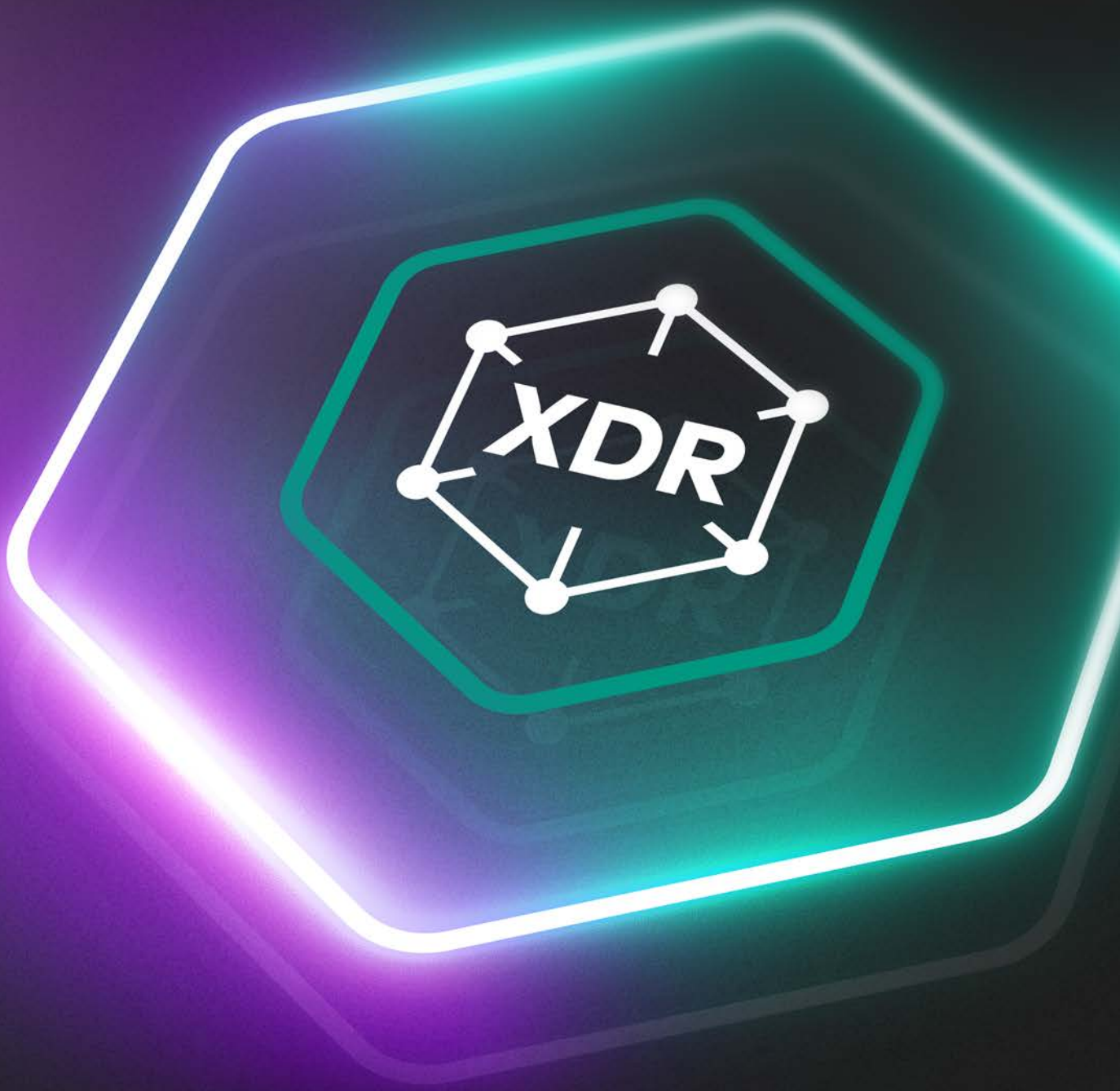


无与伦比的洞察力。
全面保护。

卡巴斯基扩展检测与响应

kaspersky 引领未来

企业网络安全的复杂性

网络威胁环境使组织要在关注核心业务运营的同时在网络安全方面保持领先具有极大的挑战性。再加上不断扩大的攻击面、监管要求和全球技能差距，很容易理解为什么现代企业面临如此大的压力，以及为什么如此多的网络攻击能够成功。

51%

的公司很难用当前的工具来检测和调查高级威胁

68%

的公司网络遭受了有针对性的攻击，并直接导致数据丢失

6 万亿美元

每年：全球网络犯罪的年度成本

400000

件每天都会检测到的新恶意软件

资料来源：卡巴斯基，
PurpleSec，CybersecurityVentures

卡巴斯基扩展检测与响应

完全的可见性。无与伦比的保护。

卡巴斯基 XDR 是一款强大的网络安全解决方案，可抵御复杂的网络威胁。它提供全面的可见性、相关性和自动化，利用包括端点、网络和云数据在内的各种数据源。

它从 2016 年作为原生 XDR 的卡巴斯基 Anti-Targeted Attack 平台发展到 2023 年的开放 XDR，提供了全方位的安全视图。卡巴斯基 XDR 可通过开放式单一管理平台轻松管理，提供全面的内部部署安全性，从而确保客户的敏感数据保留在自己的基础架构中，同时满足数据主权要求。

开放式 XDR

开放式 XDR 解决方案旨在与各种安全产品一起使用，从而允许组织集成来自不同供应商的各种安全产品，提供更大的灵活性和与供应商无关的功能。

原生 XDR

原生 XDR 解决方案通常与供应商自己的安全工具生态系统无缝配合协作，从而提供更统一和更加富有粘性的体验。这些解决方案专门为协同工作而设计，可在供应商的安全产品套件中提供深度集成、自动化和简化的工作流程。

关键技术

我们提供开放式 XDR 作为**单一开放平台**，这是创建网络安全产品统一生态系统的通用工具。卡巴斯基 XDR 的核心是我们领先的解决方案：卡巴斯基统一监控和分析平台、卡巴斯基企业端点安全和卡巴斯基端点检测和响应。对于高级网络管理，KATA 是一个附加选项。

监控和分析

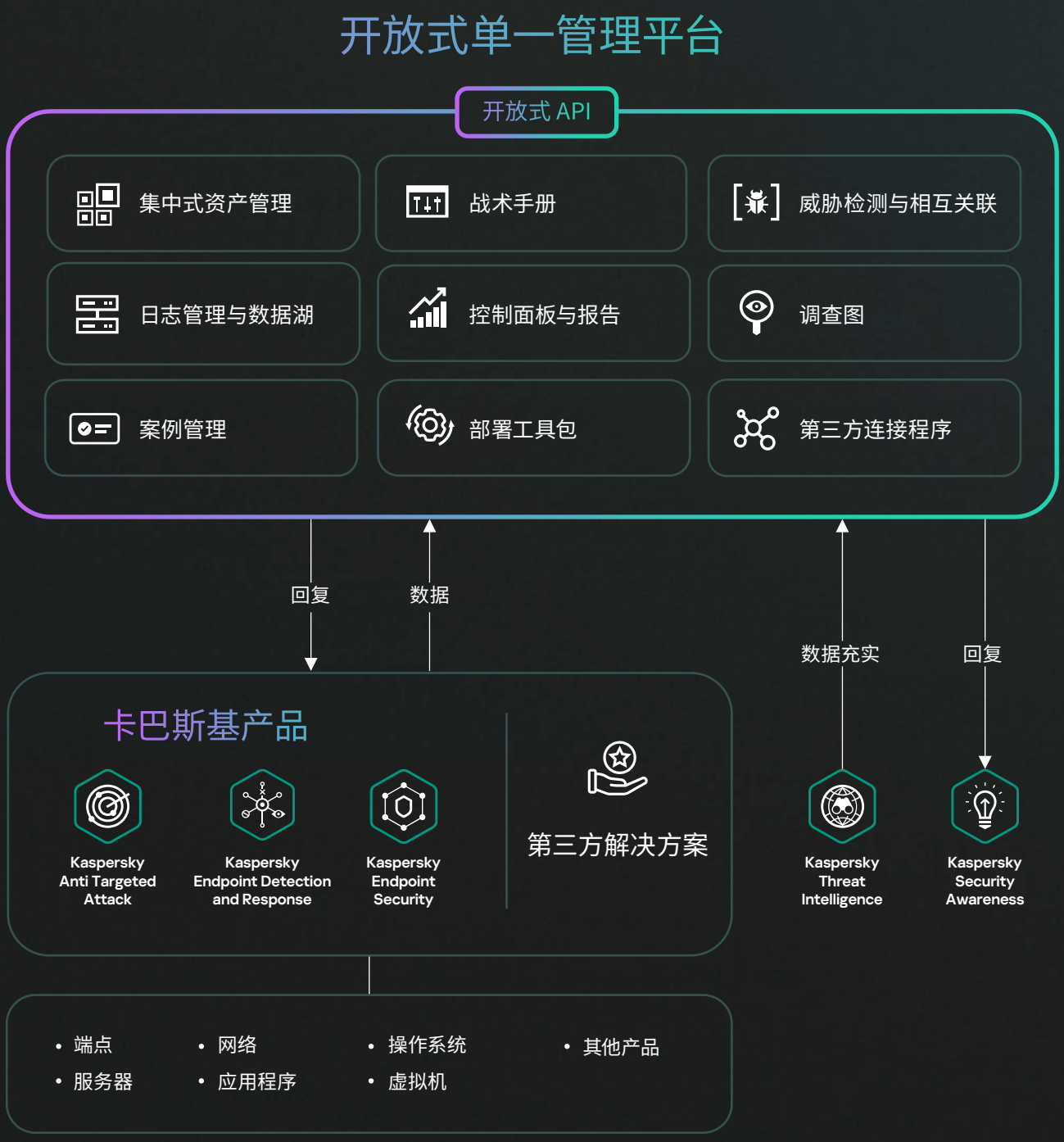
可提供集中收集和分析日志、实时关联安全事件和及时通知事件。包括一组现成的相关规则，可访问卡巴斯基威胁情报服务的丰富产品组合，以识别威胁、攻击和 IoC 并确定其优先级。

端点保护

提供强大的端点保护，从而防御勒索软件、恶意软件和无文件攻击。无论是在本地还是在云端，我们的端点保护使用机器学习和行为分析来保护运行任何主要操作系统的所有类型的端点。

端点检测和响应

为组织的所有端点提供全面可见性和卓越防御。得益于卡巴斯基独特、广泛的威胁情报，增强了威胁搜寻和发现功能，加之例行任务的自动化、引导式调查流程和可自定义的检测均有利于快速解决事件。



功能强大，效益显著

来自第三方的实时数据融合

集成来自第三方数据源的数据能力不局限于端点，通过实时相互关联得以增强。

自动响应和修复

隔离或孤立受损端点、阻止恶意活动并修复漏洞，从而减少手动操作和响应时间。

一流的 EPP/EDR

卡巴斯基被公认为全球领导者，为全球 EPP/EDR 解决方案设定了基准。卡巴斯基 EDR 在全球表现出色，屡获殊荣，积极参与国际刑警组织和 MAPP 等的活动。

无与伦比的可扩展性

卡巴斯基 XDR 能够支持在单个实例上包含数十万个端点的负载，在确保高可用性的同时实时跟踪威胁。

数据主权

卡巴斯基 XDR 是为数不多的提供全面的预置 XDR 解决方案的供应商之一，可确保客户的敏感数据保留在自己的基础架构中，同时满足数据主权要求。

跨越各种卡巴斯基产品的无缝紧密集成

产品之间的交互达到了第三方解决方案无法企及的水平，拥有统一的支持系统和无缝集成的设计。

支持 MSSP 方案的多租户模式

将 XDR 作为具有成熟租户的服务提供：一个租户的用户无法看到其他租户的数据，而主管理员 (MSSP) 可以为所有客户端构建检测和响应流程。

高级安全方案定制和整个基础架构的数据分析

赋能用户配置复杂的安全方案，增加了分析整个基础架构中的数据的能力。

集成功能

与卡巴斯基XDR合作的广泛集成提供了对潜在威胁的统一和情境化视图，从而为您的安全团队提供所需的所有工具和信息，以保护贵组织免受网络犯罪分子的任何攻击。

该产品的集成功能包括从其他系统和设备接收数据（日志）的能力，以及在其他产品中设置自动响应的能力。卡巴斯基 XDR 具有一系列与卡巴斯基和第三方产品的开箱即用集成。还可以添加额外的集成，这些集成可以由卡巴斯基专业服务部门、合作伙伴或客户自己开发（包括使用可连接产品的 API 功能）。可以与来自不同领域和不同供应商的系统集成，支持多种协议和数据格式。

按安全域划分

网络安全解决方案

- EPP & EDR 解决方案

网络、Web 和电子邮件安全

- 电子邮件保护
- 网络检测和响应 (NDR)
- 防火墙 (FW) 和下一代防火墙 (NGFW)
- 统一威胁管理 (UTM)
- 入侵检测系统(IDS)

云安全

- 云访问安全代理 (CASB)
- 云工作负载保护平台 (CWPP)

威胁情报

- 网络威胁情报 (CTI)

身份安全

- 身份和访问管理 (IAM)
- 特权访问管理 (PAM)

OT/物联网安全性安全意识

按运输类型划分

- TCP
- UDP
- Netflow
- sflow
- nats-jetstream
- kafka
- HTTP
- SQL
- SQLite
- MSSQL
- MySQL
- PostgreSQL
- Cockroach
- Oracle（甲骨文）
- Firebird
- 文件
- 1c-log and 1c-xml
- Diode
- FTP
- NFS
- WMI
- WEC
- SNMP
- SNMP-TRAP
- VmWare API

按数据类型划分

- XML
- Syslog
- Csv
- JSON
- SQL
- IPFIX
- CEF
- Netflow 5
- Netflow 9
- KV

按供应商分类

- 卡巴斯基
- 独立的
- AhnLab
- Aruba
- Avigilo
- Ayehu
- Barracuda
- BeyondTrust
- Bloombase
- BMC
- Bricata
- Brinqa
- Broadcom
- CheckPoint
- Cisco
- Citrix
- Claroty
- CloudPassage
- Corvil
- Cribl
- CrowdStrike
- CyberArk
- DeepInstinct
- Delinea
- EclecticIQ
- Edge Technologies
- Eltex
- Eset
- F5 BigIP
- FireEye
- Forcepoint
- Fortinet
- Gigamon
- 华为
- IBM
- Ideco
- Illumio
- Imperva
- Orion Soft
- Intralinks
- Juniper
- Kemptechnologies
- Kerio
- Lieberman
- MariaDB
- Microsoft
- MikroTik
- Minerva
- NetIQ
- NetScout
- Netskope
- Netwrix
- Nexthink
- NIKSUN
- Oracle（甲骨文）
- PagerDuty
- Palo Alto
- Penta Security
- Proofpoint
- Radware
- Recorded
- ReversingLabs
- SailPoint
- SentinelOne
- Sonicwall
- Sophos
- ThreatConnect
- ThreatQuotient
- Trend Micro
- Trustwave
- VMWare
- Vormetric
- WatchGuard - Firebox
- Winchill Fracas
- Zettaset
- Zscaler & etc.

我们的产品

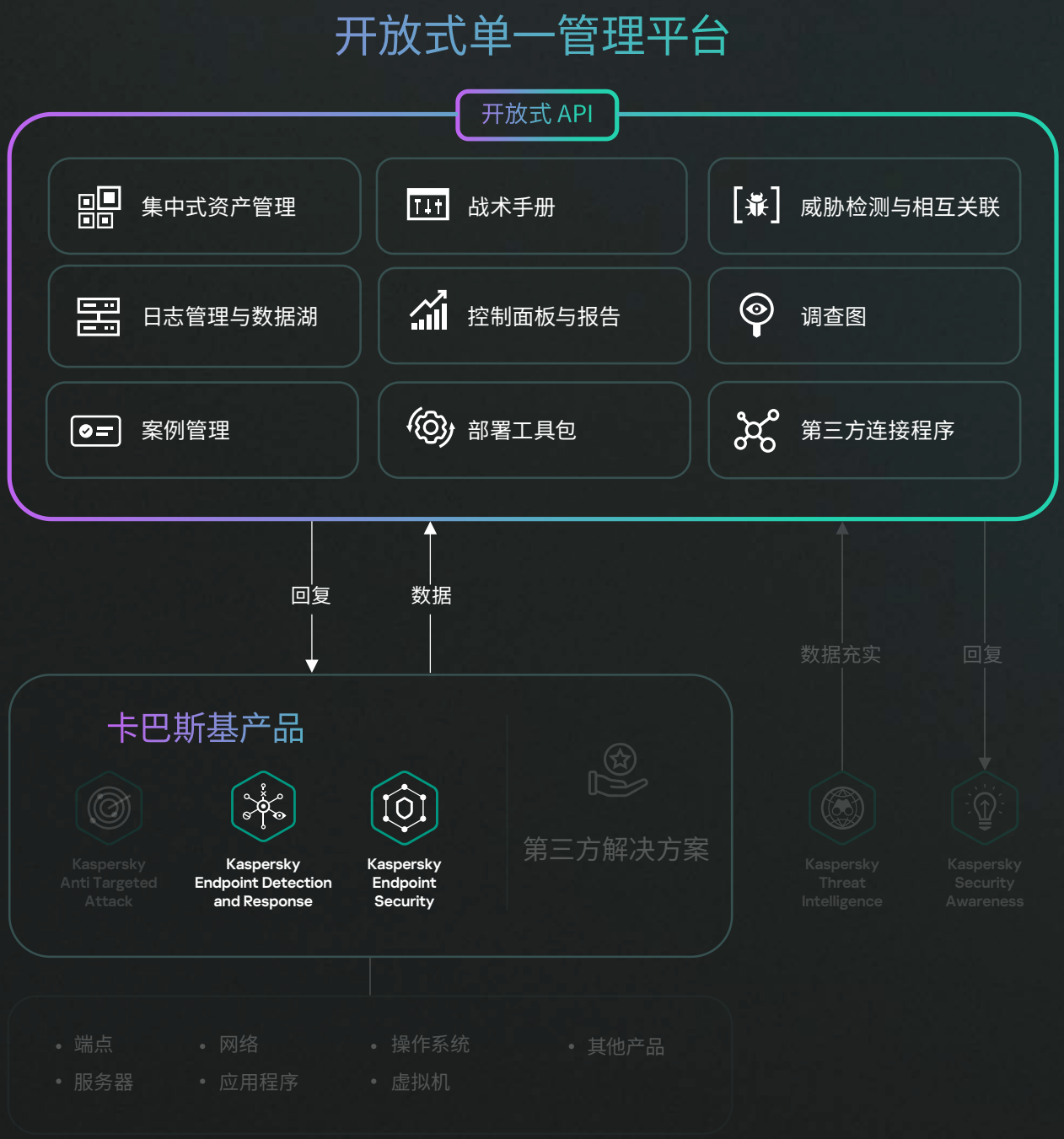
卡巴斯基 XDR 有两种选择。

卡巴斯基 XDR 优选版

卡巴斯基 XDR 优选版适用于已经有端点和 EDR 解决方案且不想替换它们的客户，他们更喜欢用关联引擎、自动化响应和第三方连接器来扩展功能。

卡巴斯基 XDR 专家版

卡巴斯基 XDR 专家版将一流的端点保护与卡巴斯基 EDR 专家版的高级检测功能、关联引擎和自动化响应相结合。可以添加第三方连接器将所有数据汇合到一起。



补充传感器附加值

卡巴斯基 XDR 支持无缝集成旨在保护特定资产的补充传感器，从而无缝集成到 XDR 中以提供额外的价值层，并将 XDR 转换为一个粘性平台，为分析师提供一个涵盖所有集成解决方案的集中式工作空间。

卡巴斯基 XDR 不仅可通过 EDR 增强您的防御能力，还提供灵活的集成功能，以便客户可以随时将产品添加到生态系统中。

		卡巴斯基 XDR 优选版	卡巴斯基 XDR 专家版
开放式单一管理平台及其组件	相互关联引擎（由KUMA 提供技术支持） · 第三方连接程序 · 日志管理与数据湖 · 威胁检测与相互关联 · 资产管理 · 控制面板与报告	●	●
	XDR 组件 · 案例管理 · 响应自动化和编排（战术手册） · 调查 · 部署工具包 · 开放式 API	●	●
卡巴斯基 EDR and KESB 功能	自动化、半自动化和手动检测		●
	跨受保护端点进行监控		●
	威胁控制		●
	恢复选项		●

卡巴斯基 XDR 优选版

Kaspersky Unified Monitoring and Analysis Platform

XDR 组件

卡巴斯基 XDR 专家版

Kaspersky Unified Monitoring and Analysis Platform

Kaspersky Endpoint Security for Business

Kaspersky Endpoint Detection and Response

XDR 组件

为什么选择卡巴斯基 XDR

久经考验。屡获殊荣。卡巴斯基保护。

卡巴斯基是一家成熟的全球网络安全公司，拥有丰富的安全专业知识。25年来，我们一直在保护世界各地的组织，我们的产品和服务获得了无数奖项和荣誉。2013 年至 2022 年间，卡巴斯基产品：

827
参加了 827 次独立测试和评审

587
获得 587 次第一名

685
获得前三名

2023 年，卡巴斯基被全球领先的技术研究和咨询公司 ISG 评为 XDR 解决方案市场的领导者。ISG 将"领导者"定义为拥有全面的产品和服务，并代表创新实力和竞争稳定性。

了解更多

Kaspersky Extended Detection and Response

申请演示

www.kaspersky.com.cn

#kaspersky
#bringonthefuture