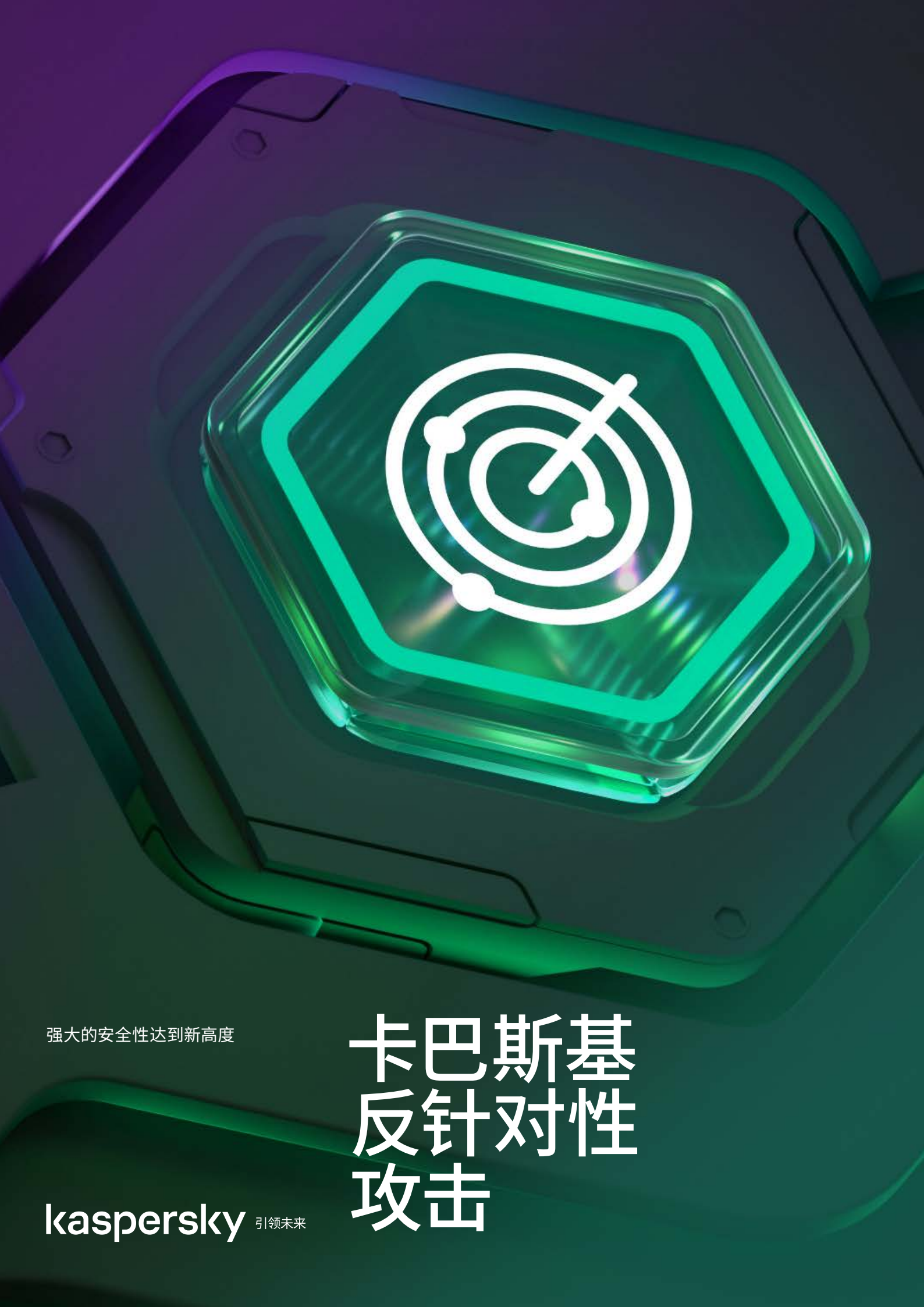


强大的安全性达到新高度

# 卡巴斯基反针对性攻击

kaspersky 引领未来

当今的网络犯罪分子专门设计独特和创新的系统渗透和破坏方法。随着威胁不断演变并变得更加复杂和具有破坏性，快速检测和最快、最适当的响应都变得至关重要。

**卡巴斯基反针对性攻击**

减少识别和响应威胁所需的时间

简化威胁分析和事件响应

帮助消除安全漏洞并减少攻击“停留时间”

在威胁检测和响应过程中自动执行手动任务

解放 IT 安全人员来执行其他关键任务

支持合规性

# 无与伦比的网络安全：领先于 APT 和复杂威胁

卡巴斯基反针对性攻击 (KATA) 可以帮助您构建可靠的防御机制，保护您的企业基础设施免受 APT 式威胁和定向攻击的侵扰，并为实现法规合规性提供支持，而且不需要额外的 IT 安全资源。借助能够最大程度利用自动化技术、最大限度提升成果质量的统一解决方案，您就可以快速识别、调查和响应复杂事件，从而帮助 IT 安全团队或 SOC 团队摆脱手动任务，提升其工作效率。

卡巴斯基反针对性攻击提供全面的反 APT 解决方案，可抵御最复杂的网络威胁。选择基本或高级 NDR 功能，并与 EDR 解决方案相结合以实现原生 XDR 方案。现在，您的 IT 安全专家拥有所有必要工具来处理卓越的多维威胁发现、应用尖端技术、进行有效调查、主动搜寻威胁以及提供快速、集中的响应。

## 灵活选择

3 个级别的 APT 保护：

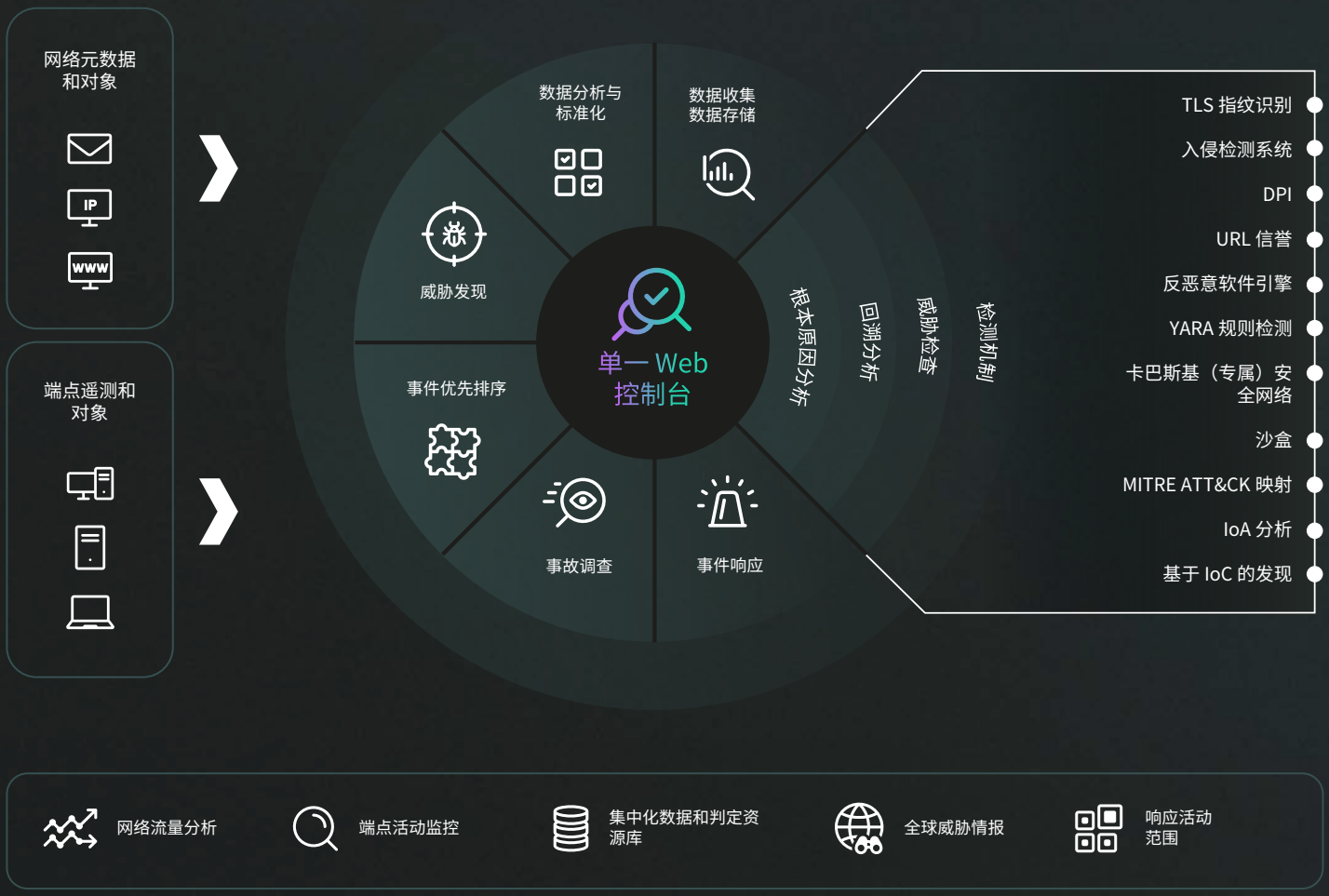
KATA → KATA NDR 加强版 → KATA NDR 专业版

## 对比

| | KATA | KATA NDR 加强版 | KATA NDR 专业版" |
|---|---|---|---|
| **基本 NDR 功能** | | | |
| • 网络流量监控和高级检测引擎<br>• TLS 指纹识别<br>• 与 IDS 警报相关的 PCAP<br>• URL 信誉分析<br>• 基于 IDS 规则的入侵检测（北南向）<br>• 网络引导式响应<br>• 自动化网关级响应和具有阻止模式的 ICAP 集成 | • | • | • |
| **先进的沙盒技术** | • | • | • |
| **卡巴斯基威胁情报和 MITRE ATT&CK 数据充实** | • | • | • |
| **增强的 NDR 功能** | | | |
| • 用于协议定义的 DPI<br>• 基于 IDS 规则的入侵检测（东西向）<br>• 网络会话表、网络映射、清单模块，可获得完整的网络可见性<br>• 网络遥测分析和端点监控（EPP Linux、Windows）<br>• 防范网络安全风险（未经授权的设备、ARP 欺骗等）<br>• 原始流量 (PCAP) 存储和回顾性分析<br>• 通过 API 连接器自动响应网络设备 | | • | • |
| **专家 EDR 功能** | | | • |
| **原生 XDR 功能** | | | • |

# 安全性的新高度

卡巴斯基反针对性攻击提供了一体化的 APT 防护解决方案，由我们的威胁情报提供支持，并与 MITRE ATT&CK 框架相匹配。所有潜在威胁入口点 – 网络、Web、邮件、PC、笔记本电脑、服务器和虚拟机 – 都在您的控制之下。




## 自动执行威胁发现和响应任务

优化您的安全、事件响应和 SOC 团队的成本效益

## 紧密、直接的集成

与现有安全产品相结合，提高整体安全级别并保护您的传统安全投资

## 完整的可见性

覆盖您的企业 IT 基础设施

## 最大的灵活性

允许在任何需要可视性和控制的物理和虚拟环境中部署

## 为何选择卡巴斯基

全球影响力和国际认可

经过验证的技术效率

透明且合规

世界一流的经验和专业知识

在 IT 安全行业备受推崇

27 年无与伦比的客户保护记录

# 卡巴斯基反针对性攻击

了解更多

www.kaspersky.com.cn



#kaspersky
#bringonthefuture