kaspersky 引领未来

如何保护企业免受复杂网络攻击

您是否曾夜不能寐，担心某种高级网络威胁可能潜伏在您的基础设施中，伺机窃取您的知识产权或勒索您的企业或业务？

如果是的话，您就有了充分的理由。顾名思义，高级持续性威胁 (APT) 使用复杂的黑客技术来获取系统的访问权限。一旦他们攻破了防线，就可能在数月甚至数年内不被发现，获得更高级别的访问权限，并收集和泄露您的数据，造成潜在的毁灭性后果。

谁处于风险之中？

毫不意外，发起 APT 或定向攻击需要大量技术、精力和资源，因此这类攻击的主要目标通常是拥有敏感或专有数据的政府部门或大型企业，这些目标才能让他们的投入物有所值。

但尽管如此，APT 仍然是一种应该引起各类企业关注的攻击方式，甚至中型企业也可能面临风险。

例如，APT 攻击者越来越多地将矛头指向构成其最终目标供应链的小型公司。由于此类公司通常防御较弱，它们可能被用作访问与之合作的大型组织的跳板。

因此，无论您是大型企业还是可能被利用来攻击大型组织的小型企业，**了解您可能面临的威胁的性质**都非常重要。这包括 APT 和其他定向攻击，以及防御这些攻击所需的能力。

所有行业均成为目标

过去两年，在所有行业都发现了人为驱动的定向攻击。2024 年，IT 和政府行业分别以 14.7% 和 13.8% 的比例领先。

来源： 卡巴斯基托管检测和响应 2024 年分析师报告

488 万美元

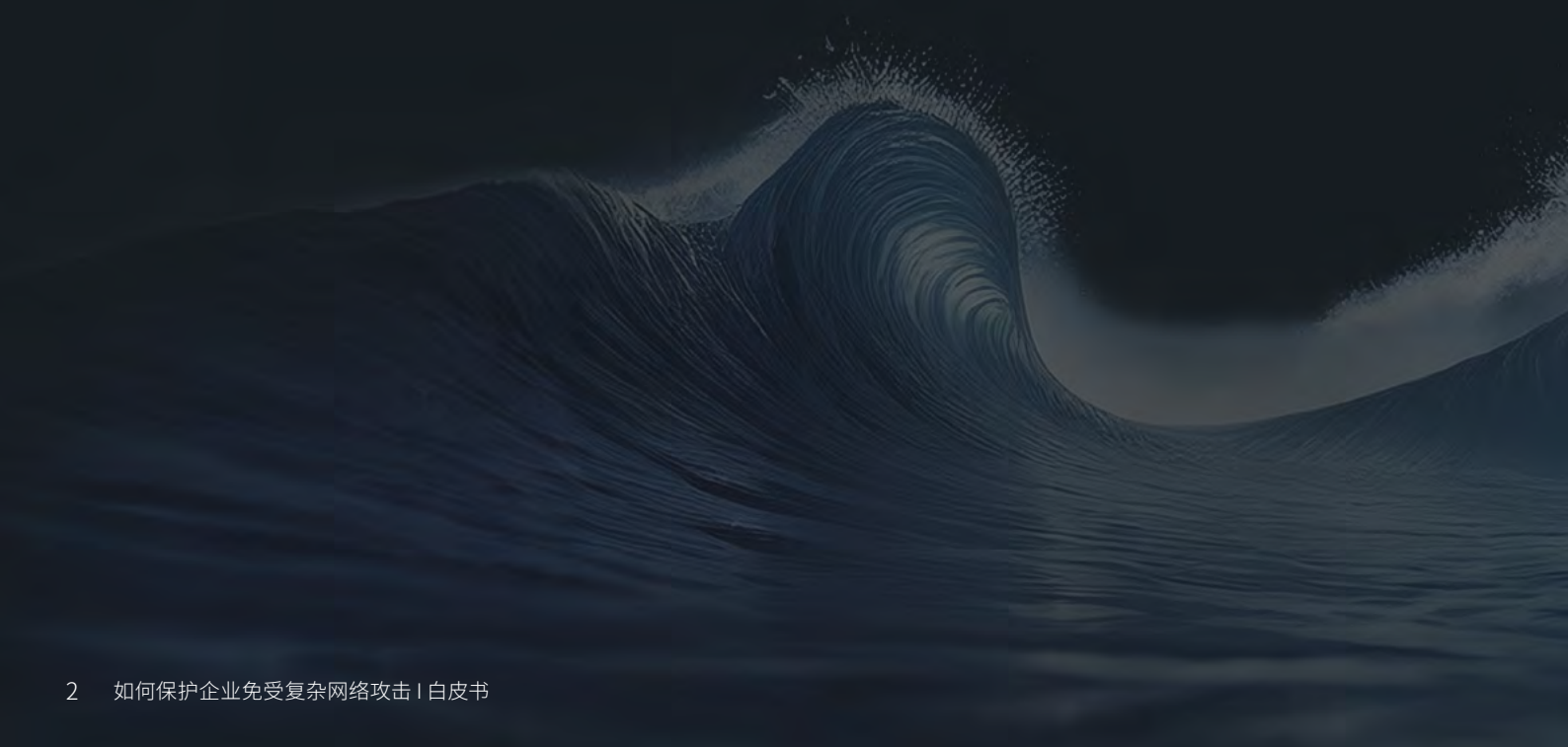
2024 年全球数据泄露的平均成本比 2023 年增长 10%，达到历史最高水平。在中东地区，这一指标明显更高，达到 875 万美元。

来源： IBM 的 2024 年数据泄露损失报告

258 天

识别和遏制泄露的时间。恢复期的延长不仅加剧了财务损失，还使组织容易受到进一步的攻击。

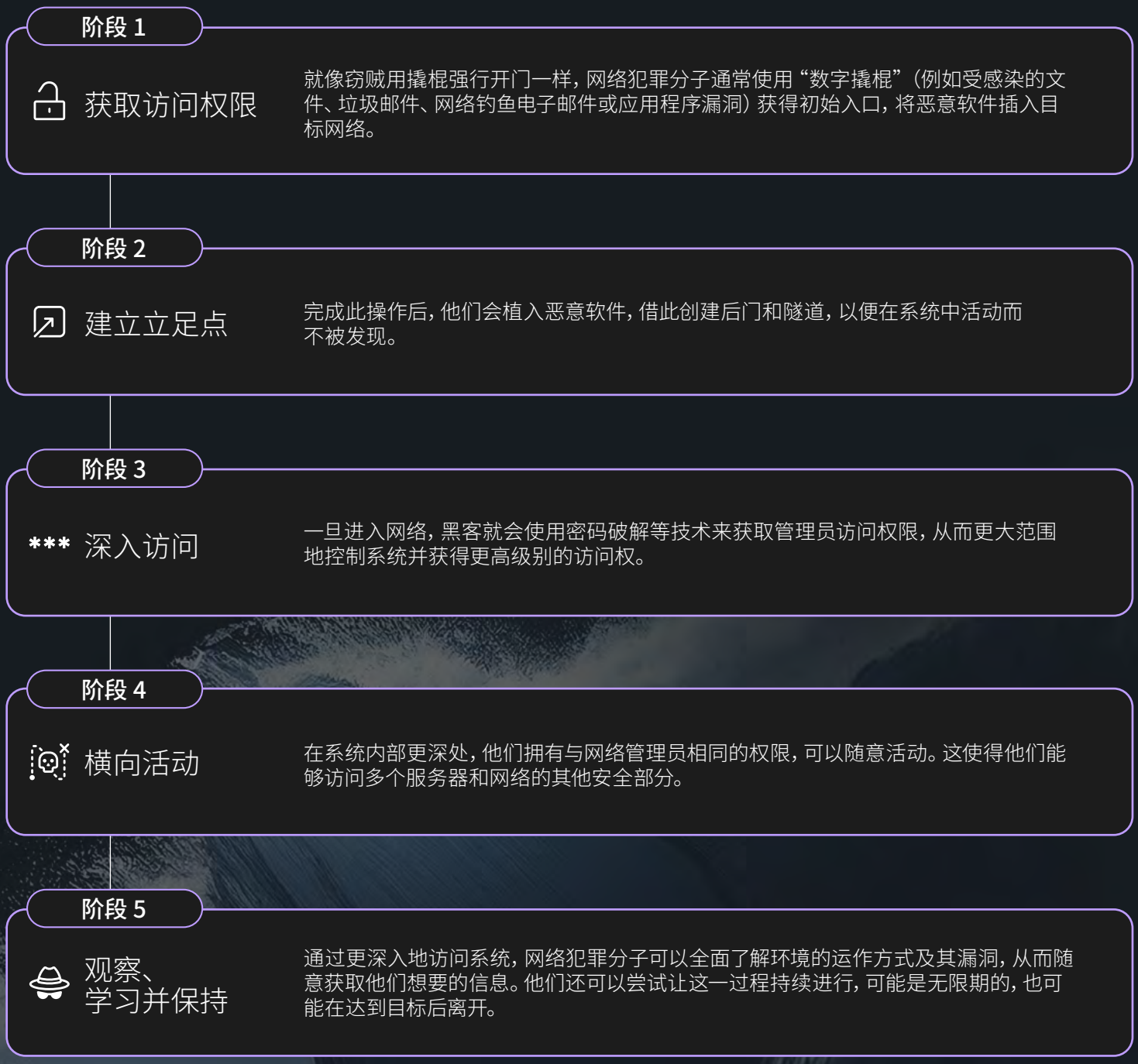
来源： IBM 的 2024 年数据泄露损失报告



APT 如何运作?

APT 的主要目的是获取目标的 IT 和/或 OT（运营技术）系统的持续访问权限，黑客通常通过一个五阶段过程来实现。

图 1：APT 的发展阶段



APT 攻击受害者的潜在后果是什么?

从媒体对任何经历过定向攻击的组织的相关报道不难看出，影响可能是严重且长远的。虽然直接影响通常包括数据丢失和业务中断造成的财务损失，但长期影响可能包括组织声誉和客户信任受损，以及潜在的法律诉讼。

当然，还有一个问题是修复组织 IT 基础设施的损坏，这通常需要数月甚至数年的时间才能完成。而且，根据您所处的行业，还可能产生行业特定的后果。

图 2：了解 APT 对企业安全的影响

金融

- 关键服务中断
- 未经授权的交易
- 套现攻击
- 身份盗窃的法律后果

政府

- 网络间谍活动的潜在影响
- 关键基础设施受损
- 电子政务服务中断
- 公民个人数据泄露

电子商务

- 通过身份盗窃接管账户的法律影响
- 欺诈交易
- 拒绝 IT 服务，收入损失
- 可能因违反 GDPR、PCI DSS 等法规而被罚款

运输

- 运行中断和停机
- 供应链延迟，成本增加
- 生命威胁
- 关键基础设施受损

食品

- 库存短缺和停产
- 食品质量受损
- 可能受到化学物质、毒素等的污染
- 需要依靠手动操作

医疗

- 关键服务中断
- 患者个人数据泄露
- 公众信任受损
- 潜在生命威胁

IT 和电信

- 客户流失
- 销售损失
- 计划外网络停机
- 固定和移动服务中断

工业

- 环境灾害
- 运营中断
- 计划外停机时间增加
- 级联故障或全系统停电

>2

每天发生的高严重性事件数量。

43%

在卡巴斯基 2024 年检测到的所有高严重性事件中，43% 是人为驱动的定向攻击 (APT)。

来源：卡巴斯基托管检测和响应 2024 年分析师报告

这对您的网络防御意味着什么?

APT 和其他定向攻击的一大危险是，即使它们被发现，并且直接威胁似乎已经过去，黑客仍可能留下多个后门，以便可以随时卷土重来。

另一个问题是，许多传统的网络防御措施（例如反病毒和防火墙）通常无法抵御这些类型的攻击。

从上面对发起 APT 或定向攻击所涉及的步骤的简短总结中可以明显看出，防御这些威胁需要多层次的方法——整合能够保护端点、网络、云、电子邮件、互联网接入等的解决方案。

这不仅有助于预防和降低复杂攻击的风险，还有助于最大限度地减少发生此类事件所造成的中断和成本。

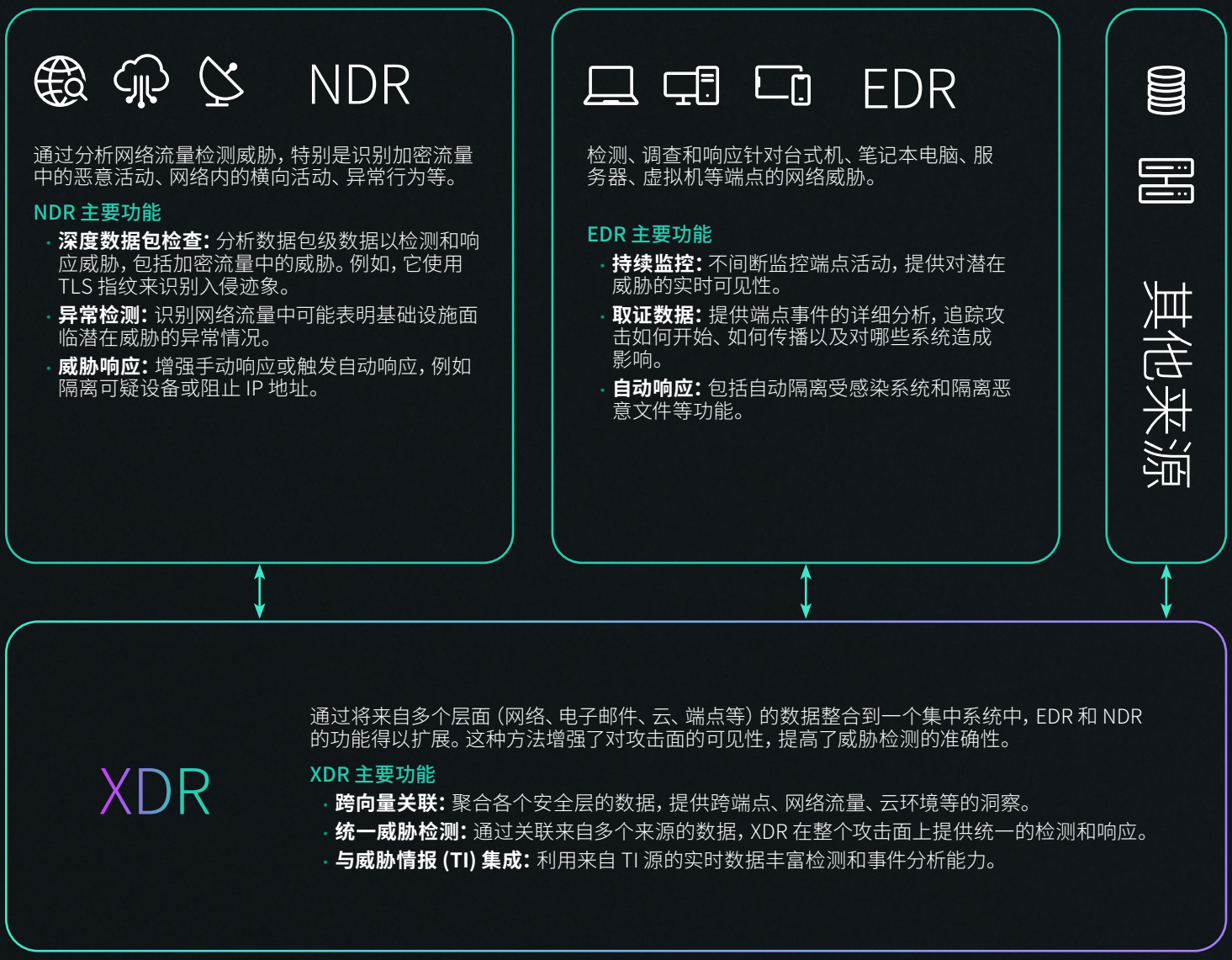
这涉及哪些类型的解决方案，应该如何部署?

如何保护企业免受复杂网络攻击

虽然端点保护平台 (EPP) 本身无法防范定向攻击，但它将提供重要的数据源，用于分析新的、正在进行的或历史的攻击。因此，它应作为一套解决方案的一部分来使用，这套解决方案还包括：

- 端点检测与响应 (EDR) – 提供设备级别的端点保护和可见性，识别并响应对工作站、服务器等的威胁。
- 网络检测与响应 (NDR) – 监控并分析网络流量，检测异常情况，并响应网络级别的潜在威胁。
- 扩展检测与响应 (XDR) – 集成 EDR、NDR 和其他安全层，以增强可见性并自动响应威胁。

图 3：EDR、NDR、XDR：如何运作？



2024 年，调查和报告高严重性事件的平均时间增加了 48%，这表明与 2023 年相比，攻击的平均复杂性有所上升。事实也印证了这一点，绝大多数触发的检测规则和 IoA 来自于专业的 XDR 工具，而不是像前几年那样来自操作系统日志。

来源：卡巴斯基托管检测和响应 2024 年分析师报告

那么应该选择哪种或哪些解决方案？

选择合适的解决方案取决于您组织的特定需求、基础设施和威胁形势：

- 选择 EDR，如果传统的端点保护工具不再能满足需求，并且您需要更高级的保护来抵御以端点为目标的网络威胁（如恶意软件、勒索软件、网络钓鱼等）。
- 选择 NDR，如果基于网络的威胁是您的主要关注点，并且您需要高级功能来分析和响应网络流量异常。
- 选择 XDR，如果您需要跨多个向量的全面保护，以及关联整个 IT 基础设施中的威胁的能力。
- 更好的是，将 EDR、NDR 和 XDR 结合到一个安全生态系统中，提供对广泛的规避性威胁和高级网络威胁的全面防御。

图 4：EDR、NDR、XDR – 最适合谁？

网络安全解决方案	最适合哪种组织？
EDR	• 优先考虑端点保护并需要实时了解端点活动的组织。 • 拥有许多分布式端点的组织，例如金融机构或医疗保健提供商，将极大地受益于 EDR 实时检测和响应基于端点的威胁的能力。
NDR	• 严重依赖网络流量并需要高级功能来检测基于网络的威胁的组织。 • 拥有专门 IT 安全团队的公司或受到严格监管的企业，例如数据中心、服务提供商或政府机构，可以受益于 NDR 检测和响应基于网络的威胁的能力。
XDR	• 需要在整个 IT 基础设施中使用具有全面的威胁检测和响应功能的统一安全平台的组织。 • 具有复杂的 IT 环境、需要全面安全方法的大型组织。例如，拥有本地数据中心和云环境的跨国企业将受益于 XDR 跨多个平台提供统一威胁检测的能力，同时通过集中事件响应降低运营复杂性。

卡巴斯基
反针对性攻击

卡巴斯基如何赋能?

卡巴斯基反针对性攻击 (KATA) 提供全面的反 APT 保护，可抵御复杂的网络威胁。它帮助组织：

- 迅速检测、分析和响应定向攻击。
- 在所有关键攻击入口点（包括网络、电子邮件、Web 和端点）实现强大的安全性。
- 保护关键资产。
- 确保遵守行业法规。

上述功能的实现得益于卡巴斯基反针对性攻击三个层级中强大的 NDR 和 EDR 技术。

三个 KATA 层级提供对高级持续性威胁 (APT) 的防护，从基本和高级 NDR 到原生 XDR。

- **KATA**：作为基本的 NDR 解决方案，提供检测和响应网络威胁的基本功能。
- **KATA NDR 增强版**：以 KATA 层级的基本功能为基础，提供高级 NDR 功能。
- **KATA 卓越版**：结合 NDR 和 EDR 功能，提供原生 XDR 功能。它可保护多个威胁入口点，包括网络、Web、电子邮件、端点、服务器和虚拟机。

图 5：卡巴斯基反针对性攻击选择灵活。

对比标准	KATA	KATA NDR 增强版	KATA 卓越版
描述	基本 NDR	高级 NDR	NDR+EDR（原生 XDR）
基本 NDR 功能	·	·	·
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		·	·
专家 EDR 功能			·
原生 XDR 功能			·

选择基本或高级 NDR 功能，或选择结合了 NDR 和 EDR 的解决方案来实现原生 XDR 方案，保护您免受最复杂的网络威胁——所有功能集成在一个平台内。在 KATA 卓越版中，您将获得对整个 IT 基础设施的全面、一体化的 APT 防护和可见性。

为什么选择卡巴斯基反针对性攻击平台

全面了解您的 IT 基础设施

提供一整套独特的技术，以消除盲点并控制所有潜在的威胁入口点，包括网络、网页、端点和电子邮件——所有功能都集成在一个统一的平台内。

通过全球威胁情报增强的保护

通过直接访问卡巴斯基私人安全网络的全球信誉数据库、卡巴斯基威胁情报以及 MITRE ATT&CK 框架映射，丰富威胁分析和响应。

久经验证的可靠技术

利用创新技术进行先进的机器学习驱动的威胁检测、深入调查和快速事件响应，获得领先分析机构的认可和全球主要客户的信赖。

卡巴斯基反针对性攻击

了解更多

卡巴斯基反针对性攻击视频演示

立即观看

高级威胁预测

立即阅读

www.kaspersky.com.cn