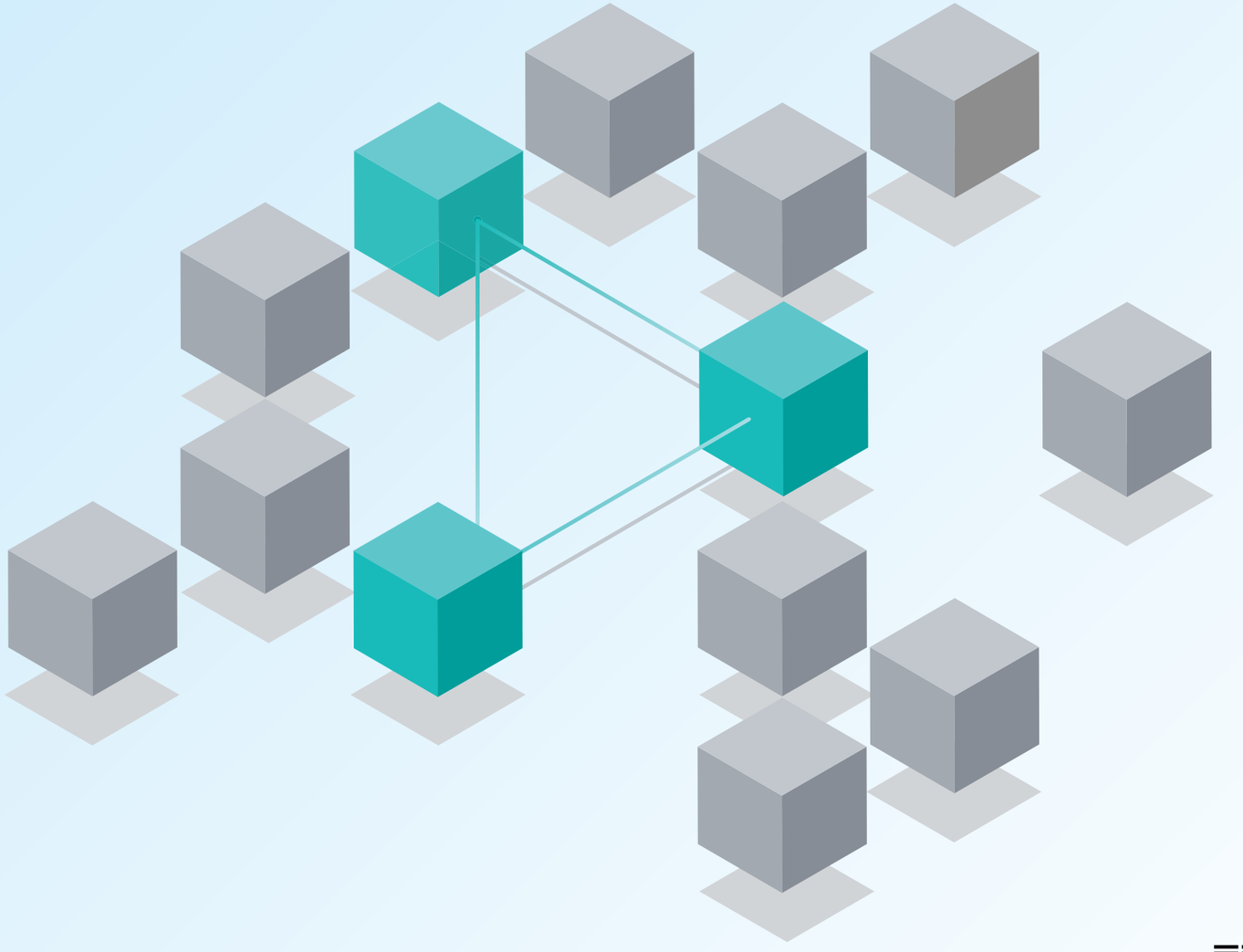
EDR 购买指南

如何为您的企业挑选最佳端点检测和响应解决方案



REAQTA
an IBM Company

IBM

目录

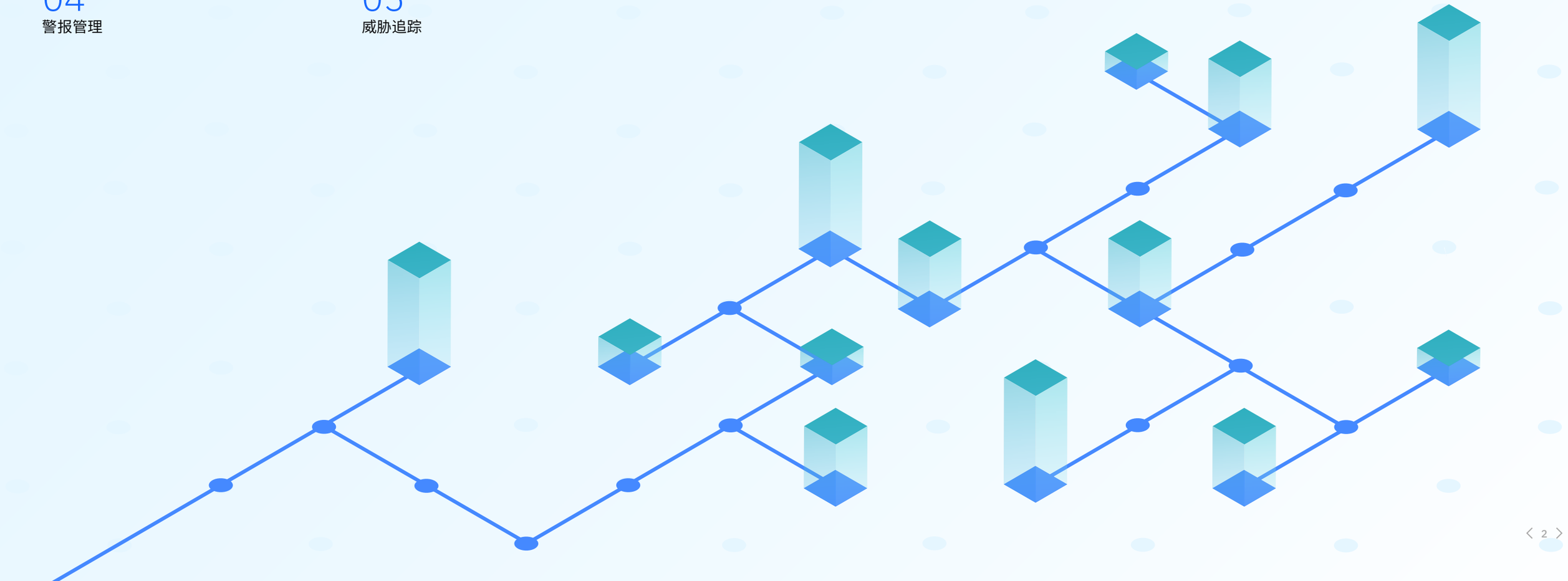
01
简介

02
端点资产状态
全面可见

03
自动化和易用性

04
警报管理

05
威胁追踪



01
简介

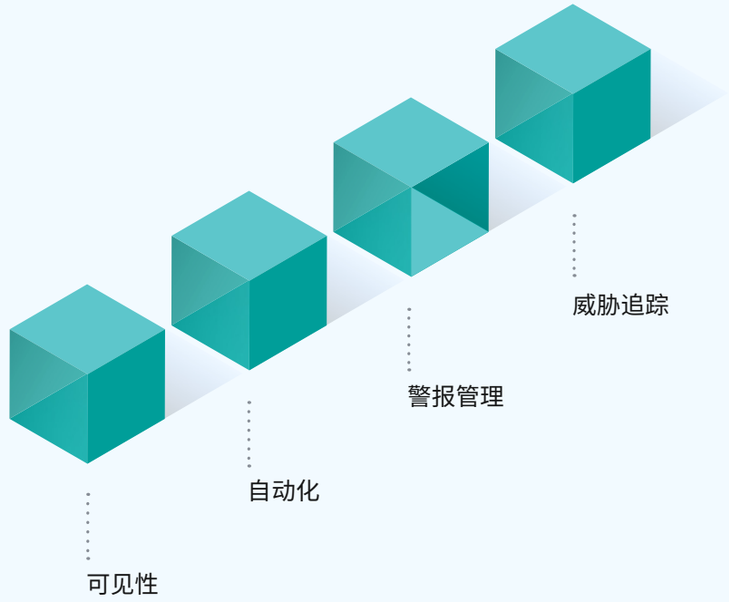
什么是 EDR?我为什么需要它?
近年来，端点和数据量与日俱增，其互联互通性不断增强，而来自威胁制造者的恶意活动亦日益增加。这些因素对各种规模企业的业务连续性都造成了重大威胁。越来越多的企业成为网络犯罪分子和国家级威胁制造者攻击行为的受害者。

传统的保护方法可对抗已知威胁，但容易受到未知复杂攻击技术的攻击，而且没有提供对资产的可见性，这是保护这些系统的主要障碍之一。专家级端点保护技术通常仅面向规模庞大或资金充沛的的顶级企业或机构。此外，现在很多攻击发生的速度极快，其中还包含许多移动部分，因此导致依赖传统端点保护方案的团队无法跟上攻击的速度。

端点检测和响应 (EDR) 解决方案可主动自动阻止和隔离恶意软件，同时为安全团队配备恰当的工具，让团队能够自信地应对这些挑战。现代 EDR 可通过有效缓解发展迅速的自动化高级威胁（如勒索软件和无文件攻击）来确保业务连续性，不会增加分析师工作量，也不需要聘请高水平的安全专家。

您是否面临下列挑战?
- 现有解决方案失效
- 可见性有限
- 缺少熟练员工
- 警报疲劳
- 潜在威胁

有效的现代 EDR 包含四个要素，我们将在下面的章节中予以阐述：



02

端点资产状态全面可见

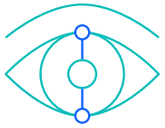
保护端点安全的主要障碍之一是缺乏可见性，因此，现代 EDR 解决方案应提供对正在运行的应用程序和进程全面深入的可视化管理。

出现威胁时，需在对方展开攻击时针对威胁行为自动创建带有图形故事线的实时警报，其中包括便于分析师全面看清和掌握正在发生的事件的 MITRE ATT&CK 映射。

端点安全软件解决方案，即便不是全部，也大多数处于操作系统内部运行，这为端点代理划定了边界，限制了代理的功能和可见性，同时还消耗了更多的计算机资源。如果使用在管理程序层运行且不易被发现的端点代理，不仅可以最大限度地减少资源利用，还能提供出色的可见性，便于监控所有进程行为，同时对攻击者始终保持隐身。

需满足的功能：

- 端点全面可见性
- 实时警报
- 创建故事线
- 无障碍代理
- 统一的工作流程



需解答的问题：

→ 你们的解决方案是否能够让用户 全面深入地观察和了解正在运行的应用程序和进程？

→ 随着攻击的展开，你们的解决方案如何实时提供有意义的信息，便于用户更好地了解所面临的威胁？

→ 除检测攻击行为和发出警报之外，你们的托管安全服务提供商 (MSSP) 是否提供端对端的响应和补救措施？

03
自动化和易用性

2022 年及其后若干年，技术上更加先进复杂的威胁和攻击预计将会持续增加，很多企业和机构均会疲于应对网络犯罪分子的袭扰。现代 EDR 应该能够通过智能自动化减轻不断增长的工作量，同时还需易于使用，以减少对高水平安全专家的需求。

购买者从 EDR 迅速获益的关键，是落实自动化和精简措施。借助人工智能自动化，大部分工作都留给算法来完成，最大限度地减少了人机交互的活动。通过这样的人工智能算法，软件更加易于使用，团队可以迅速投入正常运转，无需长时间启用准备。

发生攻击时，响应时间至关重要：调查时间应小于一分钟，以便在高级威胁损害基础设施之前将其铲除。

购买者应寻找可自主运行并具备自动检测和响应能力的 EDR，这样便于分析师实时清晰地了解攻击发展的总体状况，并可提供指导性补救措施，以便迅速恢复正常运行。

需满足的功能：
- 自主检测
- 引导修复
- 代理分析
- 快速响应
- 易于使用

需解答的问题：

→ 操作 EDR 是否需要高级技能？

→ 为减少分析师工作量，EDR 是否能够自主运行？

→ 在响应时间方面，威胁分析是在云中还是代理中进行？

→ 假如在云中进行威胁分析，如果没有连接互联网会发生什么？

04

警报管理

EDR 与传统的防病毒 (AV) 解决方案相比，关键区别在于AV 依靠可用签名进行检测，需要了解威胁才能阻挡威胁攻击。另一方面，EDR 采取了行为方法分析，根据恶意软件和其他潜在威胁在端点上的行为方式来识别这些软件和威胁。此外，与 AV 不同，EDR 在本质上是轻量级解决方案，不需要频繁更新。

因此，现代 EDR 中使用的人工智能必须能够以极高的准确度和保真度进行快速检测，最大限度减少警报数量和分析师工作量。购买者要自行了解其使用的人工智能和机器学习技术。与依靠预训练模型和分析进行检测的人工智能引擎相比，EDR 利用初始学习模型识别各个端点的正常行为，从而能够在出现不正常情况时提高检测和警报的准确性。

为缩短响应时间并帮助分析师缓解警报疲劳，现代 EDR 应配备强大的人工智能驱动警报管理系统。该系统应能够向分析师学习，然后在日常警报处理中自动应用分析师决策。部署全自动人工智能驱动警报管理系统是对抗警报疲劳、减少员工流失以及重新掌控局面的关键。

需满足的功能：

- 高保真警报
- 使用人工智能模型
- 警报疲劳预防
- 警报管理

需解答的问题：

→ 你们的解决方案是否提供了自动处理和关闭警报的方法？

→ 你们的解决方案如何帮助分析师节省时间？

→ 你们的解决方案如何减少误报？

→ 如果员工离职，如何保留他/她所了解的关于我们系统基础设施方面的知识？

05
威胁追踪

威胁追踪是现代 EDR 解决方案的重要组成部分，是保持干净、无威胁的环境所必不可少的工作。威胁追踪可迅速确定新威胁是否已进入环境并及时识别薄弱环节。数据挖掘可用于搜索和消除不易被察觉的潜在威胁，这些威胁可能会在环境中存在数月甚至数年，等待被攻击者利用。

由其本质所决定，内存威胁和无文件威胁很难追踪，当攻击者使用不同的变体在大型基础设施中移动时更加难以跟踪。现代 EDR 应该具备自动追踪搜寻功能，利用数据挖掘，确保安全团队能够自动寻找在行为和功能上与其他事件有相似之处的威胁，并在数秒钟之内提供结果。

追踪威胁时保持灵活性非常重要，购买者寻求购买的 EDR 应该不仅能够提供一个大型预建检测战术手册库（可直接部署其中的检测战术），还能在无需脚本知识的情况下根据企业机构安全需求所赋予的、独有的特定场景，轻松创建具备量身定制优势的战术手册。

威胁追踪通常被比作大海捞针，EDR 搜索必须能够深入研究特定搜索参数，确保以包容或排他的方式将这些参数结合在一起，实时提供全面细致的结果。为进一步帮助分析师节省时间，应在易于理解的图形用户界面 (GUI) 上显示结果，便于分析师轻松直观地搜索任何指定时间、任何端点的任何事件。

需满足的功能：
- 搜索潜在威胁
- 自动追踪
- 创建自定义战术手册
- 无需脚本
- 数据挖掘
- 实时性
- 图形概览

需解答的问题：

→ 用户可以创建自定义检测策略和战术手册吗？

→ 威胁追踪场景能自动运行吗？

→ 你们是否提供威胁追踪图形概览以便于快速鉴别分类？

→ 创建战术手册是否需要了解脚本知识？

后续步骤

详细了解 IBM Security ReaQta 并申请演示相关内容。

国际商业机器（中国）有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编：100020

美国出品
2022 年 4 月