白皮书

从端点检测和响应 (EDR) 升级到扩展检测和响应 (XDR)：明确升级时机

kaspersky 引领未来

从端点检测和响应 (EDR) 升级到扩展检测和响应 (XDR)：明确升级时机

如今，面临高风险威胁的已不再局限于知名企业。这一态势标志着网络安全领域正迎来重大转折。长久以来，传统认知将大型企业视作高级网络攻击的主要目标，受此影响，市面上多数强大的安全解决方案均围绕大型企业需求设计。中型企业逐渐成为复杂网络攻击的“高价值”与“战略”目标。

这一转变促使众多首席信息官 (CIO) 和 IT 安全专家重新评估既有的网络安全战略。此外，当前许多安全解决方案（尤其是小型安全团队或大型 IT 部门所采用的方案），已难以应对日益增多的威胁数量以及现代威胁的复杂特性。

为何中型企业会成为网络犯罪分子的主要目标？

配备小型网络安全团队的企业已成为高级网络攻击的主要目标。数据显示，中小型企业每年平均遭受攻击达 16 次，而大型企业（因行业而异）每年平均遭遇的攻击次数也不超过 18 次。[1]那么，攻击者为何会盯上那些看似无需企业级防护的小型企业呢？

攻击大型企业的“跳板”

许多小型企业是入侵大型企业的关键“跳板”。网络犯罪分子往往盯上的是更大的网络，故而会搜寻最易突破的入口。通过攻击小型企业，他们得以破坏更广泛的供应链，引发连锁性损害。仅 2025 年，就有 54% 的大型企业认为，供应链的相互依赖是网络安全复杂性不断攀升的主要因素。[2]尽管大型企业在 2024 年的网络韧性有所提升，但小型企业仍处于劣势，35% 的小型企业表示自身网络安全韧性不足。[2]

缺少合格的专业人员

大多数小型网络安全团队都希望提升威胁检测与事件响应能力，但却受限于资源匮乏与预算不足。近期研究显示，41% 的信息安全专业人员指出，所在企业的网络安全团队存在“有些”或“严重”的人手短缺问题。[3]在很多情况下，这意味着中小型企业主要依赖普通 IT 人员处理网络安全任务。这不仅会让小型团队不堪重负，还会因缺乏专业培训而使企业暴露于更高的网络威胁风险之下。不幸的是，网络犯罪分子对此漏洞了如指掌，并会伺机加以利用。

复杂工具容易攻破的目标

事实证明，中型企业往往成为易受攻击的对象，许多企业缺乏足够的网络安全措施来抵御复杂威胁。不过，将中型企业视为“易攻目标”的责任，不应完全归咎于 IT 团队。关键在于，当下部署复杂攻击手段的门槛已大幅降低。小型企业普遍采用较为基础的 IT 安全解决方案，如网络安全设备、端点保护平台 (EPP) 及云工作负载保护平台 (CWPP)。然而，随着网络犯罪分子利用先进工具轻松绕过这些基础防护，这类解决方案的有效性正持续减弱。

中小型企业每年平均遭遇 16 次网络攻击。[1]

现代工具与因素如何降低了攻击者的攻击难度？

要深入理解复杂攻击为何快速增长，我们需要将网络犯罪视为一个蓬勃发展的全球性产业，而非仅仅局限于技术层面的威胁。当下，网络犯罪分子已构建起可扩展的商业模式，实现了攻击流程的流水化作业、收入来源的多元化拓展，以及攻击手段的快速迭代与创新。“能力倍增器”的出现，更是加速了复杂攻击的蔓延，即便技术能力有限的网络犯罪分子，借助高级工具也能轻松发起复杂攻击。

当下，网络犯罪分子的攻击手段持续迭代升级，他们善于利用新技术和系统漏洞，以更为高效、隐蔽的方式发起攻击，这无疑给组织的安全防护带来了更为严峻的挑战。

下面我们将介绍助力攻击者更轻易入侵目标的关键工具与因素。

社交工程

网络钓鱼等社会工程攻击通常通过心理操纵手段诱使企业员工泄露私密信息，而 AI 技术的应用让此类攻击的部署门槛大幅降低。例如，以网络犯罪为导向的 AI 聊天机器人可以帮助攻击者生成措辞严谨、极具迷惑性的钓鱼邮件，甚至伪造出看似正规的 DocuSign 电子签名请求。借助这一工具，攻击者无需耗费太多精力，就能避开传统钓鱼攻击的预警机制、制作出高度个性化的伪造邮件，并通过心理操纵手段营造出紧迫且真实的氛围，从而提升攻击成功率。其他社会工程攻击常采用多阶段策略：前期，攻击者会发送大量垃圾邮件，利用员工对工作事务的重视心理，诱使其提交看似合法的服务台工单；随后，攻击者冒充 IT 支持人员，通过 Microsoft Teams 联系员工，以工作协助等为由，诱骗员工扫描恶意二维码，这些二维码会植入远程监控工具，一旦员工“中招”，攻击者便可借此非法获取网络访问权限，进而实施更深入的攻击。

间谍软件即服务

间谍软件开发者通常借助暗网论坛、非法交易平台等渠道，以出租或售卖的形式，向购买者提供其工具的使用权限。购买者群体广泛，涵盖黑客、具备国家背景的行为主体以及有跟踪意图的人员等。他们支付费用后，即可获取键盘记录器、麦克风/摄像头访问工具、移动监控套件、远程访问工具 (RAT)、浏览器和电子邮件拦截工具，还有 GPS 追踪器等间谍软件的使用权。

这些工具具备高度隐蔽性，可在用户毫无察觉、未经授权的情况下，从目标设备中收集各类信息，并将其传输至攻击者手中，严重威胁用户的隐私与安全。

勒索软件即服务 (RaaS)

勒索软件即服务 (RaaS) 套件本质上属于“即插即用”型工具，网络犯罪分子无需繁琐的手动操作，就能轻松发起复杂的网络攻击。这类套件具备代码灵活调整功能的恶意软件，这些恶意软件能够巧妙避开安全系统（像反病毒软件、防火墙等）的检测。因此，现有的网络安全框架在抵御 RaaS 攻击时显得力不从心，难以提供充足有效的防护，让企业、政府以及个人都暴露在高风险之下[4]

与软件即服务 (SaaS) 模式类似，网络犯罪分子只需每月支付低至 40 美元的费用，就能从 RaaS 套件中获取勒索软件工具、全天候技术支持，还能使用支付处理门户等资源，大大降低了发动勒索软件攻击的门槛和成本。然而，一次勒索软件攻击给受害者带来的损失极为惨重。平均损失高达 491 万美元，这其中涵盖了因系统停机导致的业务中断损失、客户流失带来的长期收益减少，以及可能面临的监管罚款等多方面费用。[5]

过时软件

众多企业在软件补丁的安装与更新工作上存在滞后性，进而导致软件漏洞长期存在。勒索软件团伙尤其擅长利用零日漏洞实施攻击，他们精准把握自身攻击速度远超企业补丁更新速度这一优势，肆意发起网络攻击。数据显示，85% 的漏洞在发现后 30 天内未能得到修复，47% 的漏洞在 60 天后依旧处于未修复状态，甚至有 20% 的漏洞在半年在半年之后仍然存在，持续威胁着企业的网络安全。[6]

2024 年，41.6% 的安全事件与勒索软件相关，而 2023 年这一比例仅为 33.3%。可以预见，未来勒索软件仍将是全球各类组织面临的主要安全威胁。[7]

对高级防护的需求

受干扰流程：

- 通信 — 41%
- 客户支持 — 36%
- 营销自动化 — 34%
- 物流 — 32%
- 产品开发/生产 — 31%
- CRM、销售 — 27%
- 采购与付款 — 26%
- 工资 — 17%

网络安全漏洞给中小型企业造成的损失，是其已配备网络安全预算的 1.5 倍。[1]

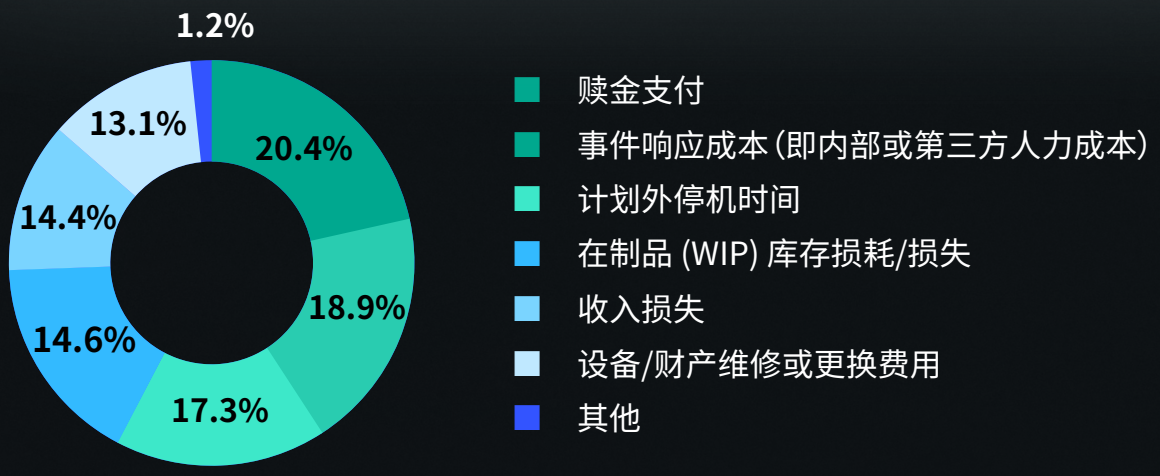
除复杂的网络攻击有所增加之外，近期研究显示，企业因业务中断及漏洞修复所产生的成本，相较于前一年度增长了近 11%。[6] 这一增长主要源于复杂攻击导致漏洞的“生命周期”显著延长。

在当前形势下，网络攻击已难以完全规避，但企业检测与响应攻击的效率，直接决定了安全事件是沦为“小插曲”，还是演变为“灾难性漏洞”。例如，2024 年，按初始攻击媒介划分，持续时间最长的三类漏洞分别是网络钓鱼、内部人员恶意行为以及凭证被盗/遭受入侵。这三类攻击也在按初始媒介划分的四大高危害漏洞之列，凸显了攻击停留时间与造成损害之间的紧密关联。[5]

攻击者在未被发现的情况下停留时间越长，造成的损害就愈发严重。因此，平均检测时间 (MTTD) 作为事件管理中的关键绩效指标，能够直观反映团队检测安全事件的能力水平。而平均响应时间 (MTTR) 则体现了团队清除威胁所需的平均时长。在此背景下，安全运营自动化对于提升这些指标具有至关重要的意义。事实上，已采用安全流程自动化的企业，其 MTTR 显著缩短了 46%。[8]

安全事件究竟是能被有效控制，还是将演变成影响范围广泛的重大灾难，其关键往往取决于响应的及时性。仅关注平均检测时间 (MTTD) 这一指标远远不够，如果平均响应时间 (MTTR) 不够理想，即便能够迅速检测出潜在威胁，却无法在第一时间予以遏制，那么前期快速检测的意义也将大打折扣。在应对安全事件时，时间就是成本，每一秒的流逝都可能带来不可估量的损失。组织若具备快速响应安全漏洞的能力，不仅能够节省数百万乃至更高的成本支出，还能轻松满足各项监管要求，切实维护自身的良好声誉。

食品饮料行业的网络安全漏洞平均成本[9]



当 EDR 无法满足时

多年来，端点检测和响应 (EDR) 工具一直是网络安全战略的基础，这一定位当之无愧。EDR 能够为网络安全团队提供极具价值的数据与可视化工具，帮助团队精准定位威胁根源，并判断是否需要采取进一步的响应举措。相较于传统反病毒工具，EDR 在能力与有效性方面均展现出显著优势。

然而，当下的威胁态势已发生巨大变化，事件响应和威胁调查的重要性愈发凸显。在此背景下，高风险企业衍生出了更为复杂的需求，而这类需求只有借助扩展检测和响应 (XDR) 功能才能满足。

但对于小型企业而言，由于缺乏必要的硬件设施、预算支持以及具备专业资质的人员对遥测数据进行高效处理与深入分析，部署一套完整的 XDR 解决方案往往难以实现。

这使得中小型企业陷入两难境地：现有的解决方案已无法契合实际需求，而企业级 XDR 方案则过于高端、成本高昂，对于当前亟待解决的问题而言，实用性欠佳。与此同时，企业的攻击面仍在持续扩大，安全团队需要应对的警报数量庞大，已然不堪重负。

那么，企业究竟该如何判断是否应当升级自身的网络安全防护方案呢？

警报疲劳压垮团队

当企业部署并使用多种网络安全工具时，往往会触发海量的警报信息。面对如此庞大的数据洪流，IT 安全团队很快便会陷入应接不暇的困境。特别是当团队所掌握的上下文信息不足，难以对警报的优先级进行合理判定，进而无法高效开展调查工作时，问题便会愈发严峻。这个过程不仅繁琐复杂，而且随着时间推移，团队遗漏新出现威胁的概率会不断攀升。团队成员极有可能因长期处于高压状态而产生职业倦怠，甚至引发员工离职潮。

> “若网络安全专业人员能够严格恪守本职、尽职尽责，许多安全事件本可得以避免。然而，他们日常所承担的工作，涵盖日志与规则的细致检查、账户权限的严格审核以及政策合规性的全面保障等，这些任务虽性质琐碎，却对整体安全防护体系起着不可或缺的关键作用。尽管这些工作在技术层面并不复杂，但长期完全依赖人工执行，极易导致从业人员产生职业倦怠，进而影响工作效率与质量。”
>
> 卡巴斯基统一平台负责人 Ilya Markelov

尽管 EDR 平台在标记端点级异常方面表现出色，但通常缺乏更为广泛的上下文信息，难以让分析师全面理解攻击的整体态势与全貌。因此，分析师不得不展开“侦探式”排查工作。由此可见，找到一套行之有效的方法，用于筛选警报、获取清晰且全面的安全态势可见性，对于企业提升网络安全防护水平而言，已然至关重要。

攻击面扩大，但资源未增加

系统加固是帮助中小型企业缩小攻击面的关键措施。本质上看，系统加固涵盖了对网络安全漏洞的精准识别与及时修复，旨在通过削减潜在攻击媒介的数量，并剔除攻击者能够轻易加以利用的不必要服务或功能。

然而，保持系统加固需要持续监控并及时进行补丁更新，以此应对新暴露出的安全漏洞。不仅如此，企业还需时刻紧跟网络安全法规的动态变化，严格遵守频繁更新的各项要求，这无疑使得企业所承担的合规负担进一步加重。毋庸置疑，对于资源相对匮乏、人力有限的小型团队来说，要切实有效地推进系统加固工作，往往会面临诸多困难与挑战。

员工难以抵御网络钓鱼和社会工程攻击

即使企业部署了 EDR，仍可能面临员工成为网络钓鱼或社会工程攻击受害者的风险。这并非代表 EDR 效能不足，而是反映出当前威胁态势已发生重大变化。EDR 擅长识别已知恶意软件、监控系统行为及标记异常活动，但无法防范人为失误引发的安全风险，而据统计，22% 的安全漏洞都与人为操作失误密切相关。[5]

钓鱼攻击无需利用软件漏洞，而是精准利用人类行为模式中的薄弱环节。攻击者仅需通过一封精心伪造的电子邮件或仿冒登录页面，即可诱导员工泄露敏感凭证或下载恶意载荷，这种攻击方式即便对于最先进的 EDR 平台而言也无能为力。

当员工群体普遍缺乏对此类攻击的辨识能力时，便凸显出企业网络安全战略亟待升级的紧迫性。单纯依赖 EDR 解决方案已不足以构建完整的安全防护体系，企业需将防护维度扩展至人员安全意识培养与行为管控层面。从 EDR 升级，正是为了应对当前日益严峻且复杂多变的社会工程学威胁，提供更为精准、有效的防范与应对策略。

攻击被发现时为时已晚

当攻击者通过合法渠道获取系统访问权限后，EDR 检测到入侵时可能为时已晚，权限早已被成功获取。IBM 研究显示，2024 年企业平均需要 194 天才能识别出一个安全漏洞，而遏制漏洞进一步扩散还需额外消耗 64 天。[5]这一时间延迟不可小觑。它意味着企业将面临长达数月的潜在数据泄露风险、横向移动风险以及持续不断地恶意攻击威胁。

每多拖延一天未能发现漏洞，敏感数据被盗取、核心系统遭入侵或者勒索软件被成功部署的可能性就会显著增加。

人工响应拖慢速度

具备完善且定期接受事件响应计划测试的企业，在应对安全事件时所承担的成本，平均较缺乏此类计划的企业低 58%。[10] 但什么样的事件响应计划才算“完善”呢？简而言之，其核心在于速度。现代攻击周期正迅速缩短。以勒索软件为例，它能够在几分钟内就锁定企业的核心系统，使运营陷入瘫痪。在如今威胁态势快速演变的格局下，单纯依靠人工方式响应安全事件已显得力不从心，难以跟上攻击的节奏。

与自动化系统不同，人工响应网络安全事件的速度明显滞后，即便最轻微的延迟也可能引发更大范围的漏洞风险，给企业带来更为严重的安全危害。

因此，事件响应自动化的重要性绝不容小觑。通过自动化，安全团队能够实时识别并迅速对抗各类威胁，极大地缩短了系统暴露在风险中的时间窗口。此外，自动化还能解放安全团队的人力，使他们能够将更多的时间和精力投入到其他需要专业技能的关键任务上，进而为企业节省时间、成本和资源，提升整体的安全防护效率和经济效益。

是否需要升级？

完整的 XDR 解决方案虽对抵御高级威胁至关重要，但目前市场上的 XDR 解决方案尚未充分契合小型 IT 和网络安全团队的特定需求。

中型企业因预算有限、资源不足，往往容易成为复杂网络攻击的目标，也因此难以高效部署先进的防护措施。

这类专业的 XDR 解决方案，在部署和操作层面通常具有较高的复杂性。小型 IT 团队受限于人力、技术资源以及时间等因素，往往难以在短期内熟练掌握其使用方法。但随着网络安全威胁的不断演变，小型企业对于一些 XDR 功能的需求正日益凸显，且这种需求并非大型企业所独有。我们的 MDR 分析师报告中指出：“2024 年，调查和报告网络事件的平均耗时相较于 2023 年增加了 48%，这一数据直观地反映出当前攻击的复杂性有了显著提升。”这些结论是基于对触发的检测规则和攻击指标 (IoA) 的分析得出，而这些关键的检测规则和攻击指标，大多源自专业的 XDR 工具。这意味着与往年相比，网络安全形势已经发生了重大变化。在过去，操作系统日志在威胁检测中占据着重要地位，但如今，其作用已逐渐被专业的 XDR 工具所超越。在此背景下，像 XDR 这类专业工具对于成功检测和调查现代威胁而言，已经变得至关重要。[7]

卡巴斯基如何赋能?

为小型团队升级防护的企业级防护

卡巴斯基新一代安全 XDR 优选版专为小型 IT 和网络安全团队设计。此解决方案能够有效强化企业的事件响应效能、系统培育专业技术能力,且可避免为日常运营增添耗时冗余的任务负荷。

自动执行多个流程,助力您的团队将精力聚焦于更为关键的核心事务。

发挥卓越的端点防护功能

通过自动化防护机制,避免业务中断。借助经过行业认证,依托机器学习技术的反勒索软件与反恶意软件工具,助您轻松抵御已知及未知威胁的侵扰。

开展全面且系统的培训工作

为您的 IT 员工和非技术人员提供保持安全的知识和技能。加强您的 IT 安全团队,同时在您的员工中建立一个强大的、有安全意识的文化。

通过系统强化和培训修复漏洞

基于用户行为进行系统加固,缩小攻击面。通过集中式漏洞、补丁和加密管理节省时间,提供团队所需的全部培训,助力充分发挥新网络安全功能的价值。

借助可信赖的云安全技术,管控影子 IT 风险

通过控制影子 IT,减少漏洞并保护数据和员工。了解各类云服务使用情况,有效阻止未经授权的访问行为,同时识别 Microsoft 365 应用中存储的敏感数据。

扩展您的检测和响应能力

深度洞察威胁态势及其在端点内外的活动路径。通过自动化与引导式响应策略反击攻击,利用基础调查工具追踪其活动动态。

减少警报疲劳

新一代安全 XDR 优选版中的警报聚合功能,结合有效、成熟的端点防护,可减少团队需分析的警报数量。这不仅能提高效率、缓解警报疲劳,助力团队将宝贵时间和精力聚焦于更多核心安全任务上。

XDR 不再只为服务于大型企业

探索专为小型团队升级安全效能的新一代解决方案。

卡巴斯基
新一代XDRO

了解更多

参考资料:

[1] 卡巴斯基,B2B IT 安全风险追踪报告,(卡巴斯基,2024 年)
[2] Tuteja Akhilesh, 复杂网络安全环境下供应链相互依赖引发的 5 大风险因素(世界经济论坛,2025 年)
[3] 卡巴斯基,现代信息安全专业人员画像(卡巴斯基,2024 年)
[4] Willie Alan, 勒索软件即服务 (RaaS) 的演变:AI 在网络犯罪及应对措施中的作用(斯坦福大学,2025 年)
[5] IBM,2024 年数据泄露成本报告(IBM,2024 年)
[6] Verizon,2024 年数据泄露调查报告(Verizon,2024 年)
[7] 卡巴斯基,战火中的堡垒:2024 年网络威胁纪事(卡巴斯基 MDR 分析师报告,2024 年)
[8] Verizon,2024 年数据泄露调查报告(Verizon,2024 年)
[9] 卡巴斯基与 VDC 联合调查结果(保障 OT 环境安全,2024 年)
[10] IBM,2022 年数据泄露成本报告(IBM,2022 年)

www.kaspersky.com.cn

#卡巴斯基
#引领未来