360政企安全
数字安全的领导者

数字时代EDR技术发展趋势

Gartner

数字时代EDR技术发展趋势

1. 背景概述

安全形势高危：随着5G、云计算、大数据和人工智能的持续发展，信息化、智能化已经渗透到社会发展的方方面面，网络空间的概念和范围得到前所未有的拓展。政府和企业信息化建设朝着高层次、多维度、立体化的方向发展，网络安全边界持续扩大，安全形势也越来越复杂。与此同时，网络空间的攻击面随之延伸和拓展，网络空间攻防双方信息的不对称性现象愈发明显。伴随着攻防对抗态势的升级，自动化、智能化技术与攻防技术的融合已成为网络安全技术发展的必然趋势之一，在数以亿计的终端上的安全防护变得越来越急迫，我们面临的是传统安全与高级威胁并存的防护环境。

业务环境复杂：在当前及未来的智能化社会，数据资产的安全变得尤为重要，而政企用户大量有价值的生产及业务数据早已成为有组织网络犯罪的重点目标。同时，在新冠疫情的冲击下，远程办公变得越来越普遍，用户会使用各类终端远程访问企业网络，企业既要保护终端安全，防止终端被攻击和突破，又要允许用户使用多种类型终端访问企业内部网络，并且要保证最小化的影响用户体验，这意味着企业的数据和人已经走出了企业的传统边界，使得企业的数据安全和网络安全的防护变得越来越复杂。

国际形势严峻：近年来，网络空间领域的斗争已经是大国博弈的焦点，网络战愈演愈烈，APT攻击活动大幅增加，仅2021年上半年，全球公开APT相关报告约500篇，涉及APT组织达90个，攻击目标涉及政府、国防军工、核工业、科研、医疗、金融等诸多行业。中国仍是APT攻击的主要受害者，针对我国的攻击持续上升，其中政府，教育和国防军工等相关单位是重点被攻击目标。

APT攻击具有针对性强、组织严密、持续时间长、隐蔽性高、采用技术手段先进等多种特征，检测相关的攻击给安全行业带来很大的挑战。对于攻击者而言，内网终端和主机既可以作为被攻击目标，也可以作为攻击的跳板。同时勒索病毒和APT结合的攻击方式也开始逐渐显现，外加新冠疫情冲击下直接带来的以聚焦远程办公为突破口，围绕新冠疫情话题攻击，针对医疗行业窃取抗疫情报的APT威胁也开始愈演愈烈。

技术挑战升级：传统的终端安全解决方案EPP是基于已知风险产出的文件特征库和规则库，仍然属于反病毒的技术范畴，无法用于检测未知风险。不同于传统的签名检测或启发式技术，EDR通过观察攻击行为将检测技术提升到新的层次，能真正解决终端安全所面临的APT、0day和勒索病毒等各类高级威胁，做到事前预防、事中检测和事后修复，是面向未来的终端安全解决方案。

EDR主要通过提供安全事件的完整可视来检测和防范未知风险。通常攻击者潜入到企业网络内部后会持续很长一段时间，其攻击手法比较隐蔽，企业一般很难直接检测到其攻击行为，更难形成有效的攻击告警机制。为了更好地解决这种问题，EDR采用了记录攻击者行为和系统事件的方式，所有行为信息都会被完整地记录下来，整个安全事件从发生了什么、如何发生、到如何修复等所有环节信息都会被完整地记录并以图形化方式展示出来。

随着我国网络安全形势的发展变化，尤其是2018年"永恒之蓝"勒索病毒的肆虐，让业界更加重视新攻击方式带来的安全技术挑战，EDR产品也迎来了发展的热潮。360作为终端安全产品的引领者，拥有17年终端安全攻防对抗经验，积累了海量的全网安全大数据，历经十余年与各种木马、各类APT家族的攻防实战，持续打磨终端的恶意行为检测和响应能力，积累了全面细致的终端行为检测技术，在产品效果上打造了行业标杆。

2. 国际标准

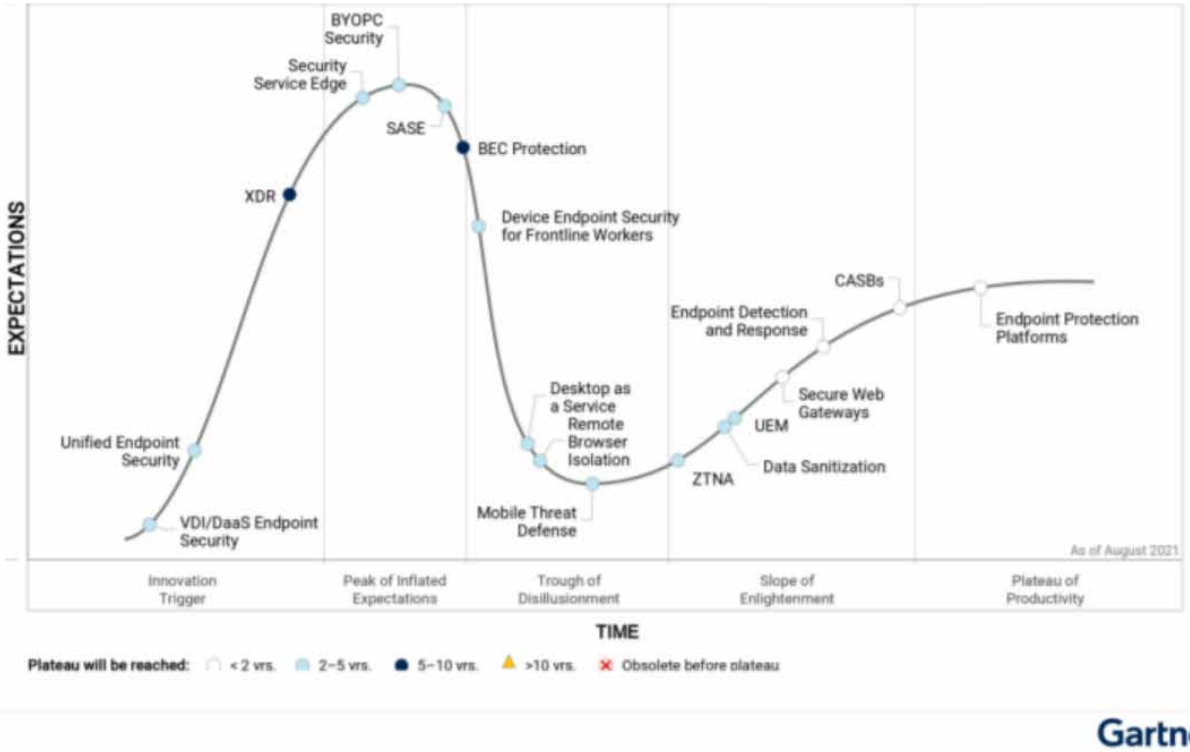
EDR是现阶段在终端安全和风险管理领域最成熟、应用范围最广泛的安全解决方案，能有效防止终端被攻击和突破，保证远程访问安全。但同时面临的挑战也在持续不断加大，一方面是随着勒索病毒、无文件攻击和鱼叉攻击等攻击方法和复杂性的持续提升；另一方面是突然增多的远程办公访问场景，因此安全防护需要以更创新的方式来应对这些高级威胁。

EDR解决方案要能够提供安全事件检测，安全事件调查，抑制终端利用，以及提供安全修复能力。作为总体安全防御里必不可少的关键部分，EDR要能够识别异常和恶意的行为，展示出高级威胁的技战术细节，同时能够采取及时措施有效应对。

EDR必须能够分析用户、进程、网络、驱动和配置等系统行为的变化。EDR非常关键的能力之一就是做好安全事件关联，理想的EDR能够自动响应，自动回滚安全事件造成的影响，能够自动化集成其他安全工具协同分析安全事件。部署模式上，优先云端部署，同时也支持客户侧私有化部署，为了有效应对越来越复杂的高级威胁，EDR需要部署在所有托管的终端和服务器上。

图1

2021年端点安全的技术成熟度曲线[1]



[1]Gartner Inc.，2021年端点安全的技术成熟度曲线，2021年8月11日，G00747412

3. EDR演进方向

3.1 必要能力

EDR通过实时监测端点上发生的各类行为，采集端点运行状态，在后端通过大数据安全分析、机器学习、沙箱分析和行为分析等技术，提供深度持续监控、威胁检测、高级威胁分析、调查取证、事件响应处置和追踪溯源等功能，及时检测并发现恶意活动，其中包括已知和未知威胁，并快速智能地做出响应，全面赋予端点主动、积极的安全防御能力。其从预测、防护、检测和响应四个维度，实现持续性安全防护，贯穿安全威胁事件的整个生命周期。

从中可以清晰的看出，EDR产品不可缺少的必要能力是：大数据存储及处理能力、安全分析能力和安全专家能力。

1）具备大数据存储及处理能力：安全大数据是支撑构建覆盖面足够广、精确度足够高的检测防御模型，以及发现攻击者痕迹的必要基础。大数据的存储及处理能力，核心目标是不丢失终端安全相关的重要数据，并通过分析原始终端安全数据而形成全局的、缜密的、连贯的攻击视图。在EDR中，端点采集的各类安全行为数据是终端安全防御、检测和响应的核心依据，是应对APT攻击的重要手段。通过对多维度高质量的大数据进行自动化和智能化的关联分析和运营，可以追溯攻击过程，寻找漏洞源和攻击源，是有效防御和确保终端安全的有效途径和方法。

2）具备安全分析能力：需要有各种安全检测分析技术，能对海量多异构数据进行分析，同时结合全网APT情报，确保各类威胁全面可视。由于高级威胁攻击的蛛丝马迹往往隐蔽在常规软件运行的类似行为当中，因此检测需要对终端海量数据进行安全分析，需要具备对历史数据的反复检测能力，这些都要求产品具备极强的大数据运算能力。针对APT攻击的极强持续性和阶段性，关联分析过程中应尽量收集各层面、各阶段的全方位数据，同时适量将时间窗口拉大，通过宽时间域数据分析提取具有内在关联的若干属性，识别出攻击发生的时间、地点、攻击类型和强度等信息，也就是攻击场景的重构技术，这也就是安全分析能力的核心之一。

3）具备能够部署及使用产品的专业人士：由于产品使用对专业性要求较高，多数企业选择采用驻场或远程托管给专业人士（MSS、MDR）。在传统EDR中，专业人士的角色是不可忽视的，缺少专业人士过硬的技术能力，EDR的安全分析能力将大打折扣。基于最新漏洞、APT等各种攻击方式，机器学习和大数据自动化关联分析固然必不可少，但对收集到的数据进行人工分析和解释也十分重要，分析师能够调查并提供合法的威胁解决方案。

3.2 关键能力

在EDR的必要能力基础上，360从实战层面提出了EDR的关键功能，包括端上的安全能力、云端的大数据存储和处理能力、安全分析能力和360核心安全大脑。在这几个核心能力的协同作用下，360 EDR能够帮助企业用户提升整个安全事件的可见性，通过定位到攻击行为让安全专家主动进行威胁狩猎。同时对安全事件进行检测和调查，并快速做出反应，及时阻止攻击者的恶意行为，保护企业的网络安全。

360 EDR终端上部署了非常轻量级的Agent，具备全面的安全事件采集能力。面对入侵活动特别是系统级事件，能够完整地记录攻击事件的上下文信息。基于内核之下虚拟化层的超强安全监控能力，能够监控账号修改事件、进程事件、网络事件、文件操作、驱动加载、磁盘和内存访问事件等，任何恶意或者异常的行为、事件和信息等都会被完整地监控并记录下来，为安全专家提供实时和后续的持续追踪分析。360 EDR自研的核心数据采集技术能够有效避免收集数据的探针被绕过，不同于传统基于环3的用户态探针，自研探针工作在内核下面的虚拟化层，能够在更底层截获到用户层和内核层的漏洞利用事件，从而保证了在端上能够完整地记录攻击者的任何恶意和可疑行为。

云端基于360在终端安全领域17年积累的安全大数据，具备全网安全攻防和态势感知能力，能够以业界最快的速度掌握最新安全情报，保证大容量数据的准确性、实时性以及快速的分析和处理能力，为终端安全的快速检测和响应提供安全大数据赋能。云端同时提供了对历史数据的回溯能力，通过引入新的行为特征库IOA和外部特征库IOC，可检查一段时间内的终端行为数据，配合威胁情报和安全人员的手动分析，给出最终的威胁评估结果。

安全分析能力是360最核心的安全能力之一，搭载由360核心安全大脑赋能的全球顶级云端查杀平台，基于360云引擎、鲲鹏大数据引擎、QVM II人工智能引擎和QEX引擎构造的立体协同检测机制，能够有效识别各类木马病毒、未知病毒或变种，提供服务安全防御的真能力。

云查杀引擎：360云查杀引擎建立在云端庞大的黑白名单数据库基础上，病毒检出率高、系统资源占用低。

鲲鹏引擎：360鲲鹏引擎是以数据驱动安全的思路构建的大数据特征引擎，具备自动化病毒特征提取分析能力。相较于传统引擎的病毒特征提取方式，鲲鹏引擎依托360核心安全大脑大存储、多样本、高算力和机器学习等资源，实现了后端病毒特征的自动分析提取。

QVM II引擎：新一代QVM智能识别引擎采用人工智能与机器学习的方法，对360目前已经积累的海量样本进行多次切片学习，抽取出病毒与恶意代码共性特征，建立恶意代码不同族系模型，对加壳和变种病毒具有出色的免疫能力。

QEX脚本引擎：针对非PE类宏病毒、VBS、REG等恶意文件，360（云）主机安全防护系统利用专用QEX脚本查杀引擎进行检测。该引擎既能结合精确特征和启发特征，检测出已知和高级恶意威胁，又能对VBS和BAT脚本模拟执行，根据输出结果做二次检查，确保结果的准确性。

安全专家和安全专业技术一直是360的安身立命之本，作为国内头号安全公司，360拥有大量顶级安全专家，他们从事安全攻防多年，积累了丰富的安全攻防经验，特别是应对高级威胁方面，为国家和企业共发现了50个境外APT组织，发现多个0day漏洞。

3.3 传统方案痛点

传统的EDR产品在实现上面临着很多痛点，无法解决多场景安全性问题，如不具备真正的大数据存储和处理能力，不具备真正从实战中总结出来的知识库和安全分析能力、安全专家和安全专业技能，终端上的信息采集能力比较欠缺、不具备完整采集攻击行为的能力，从而导致攻击者行为信息记录不全面。

为了营造市场概念，部分安全厂商用入侵检测、漏洞防御产品来充当EDR产品。这些产品在检测能力上还是传统的本地特征匹配，并不具备终端行为采集和大数据分析能力，甚至只是在反病毒防护产品基础上增加了设备间的联动。这对客户理解EDR产品特性造成了一定程度的误导。

3.3.1 大数据存储和处理能力不足

传统EDR产品缺少足够规模且高质量的大网安全数据积累，直接影响了攻击行为的整体识别效果。离开大数据谈EDR产品能力和价值是空谈，即使是大型企业部署数十万终端设备，所能掌握的安全数据量仍不够"大"。传统EDR产品后端缺乏安全大数据支撑，没有构建出覆盖面足够广、精确度足够高的检测防御模型，检测规则较为局限，同时情报能力的不足也大大影响了EDR产品总体的防御效果。

3.3.2 安全分析能力欠缺

APT攻击并非无迹可循，需要从大量的历史数据分析中得到启发，从而发现攻击者的痕迹。若缺乏真实攻防场景下的实战经验，就不具备发现并分析攻击者的能力。很多安全厂商的EDR产品，只是简单将终端上记录的一些行为数据传给云端，但是数据到了云端之后，怎样处理这些大数据，查询哪些关键信息仍是待解决的问题。由于缺少安全专家和安全专业知识，这些EDR产品无法快速基于历史数据和多终端横向数据来做关联分析，导致这些有价值的数据在客户侧很难被有效利用。

安全分析能力的另外一个重点是威胁情报的积累，威胁情报是EDR产品识别高级威胁攻击的钥匙，大多数厂商的威胁情报来自公开渠道，并没有自己的实战分析积累，因此很难及时发现新的攻击线索。

3.3.3 终端采集被攻击行为绕过

终端的关键行为记录要非常全面。由于高级威胁和正常程序的行为非常相似，只有行为记录更全面，才有可能发现异常，特别是系统级行为的监测和记录能力。众所周知，网络攻防是一个持续对抗的过程，APT组织也一直在尝试各类绕过行为，让传统EDR防御方式失效。基于文件数字签名、系统文件属性衍生的伪装混淆变本加厉，API Hooking绕过、白利用以及无文件攻击技术层出不穷，0day漏洞防不胜防，这些不断演进的攻击手段给当前EDR产品的检测防御能力带来了极大的压力。

传统的EDR产品信息采集和攻击者处于同一个层次，往往通过挂钩程序用户态（即Ring3层监控）内存中的DLL，实现对运行进程的监控。但是用户内存空间存在被修改的可能性，导致传统EDR产品的挂钩被抹除绕过，无法有效监测恶意攻击行为。

3.3.4 端点性能影响

EDR为了能获取最全面的威胁数据，往往会采集大量的端点信息，而行为数据采集活动容易消耗终端和服务器的宝贵资源。传统EDR产品缺少灵活的性能调优和自适应机制，无法实现安全能力与资源占用的良好平衡。如果消息截获层面在用户层，将对终端的性能和用户体验产生较大的影响。

3.3.5 专业能力有限

由于组织专业人士队伍普遍成本较高，中小企业难以承担，而专业人士本身也可能存在弱点。真正经过长期实战训练的专业人员极为稀缺，经历过全网真实攻击的专家更是凤毛麟角，因此难以判断为企业组织部署EDR的技术队伍是否满足EDR分析的需要。

3.4 EDR能力成熟度模型

360将EDR能力成熟度模型定义为4个等级，初级是EPP、中级是具备有限的EDR、高级是标准化的EDR、特级是SaaS化和智能化的EDR。

初级：企业在只有EPP的情况下，直接面对高级威胁是非常脆弱的。不仅无法进行有效防护，还无法检测到高级威胁的攻击，包括攻击的时间点和行为方式等都没有任何记录，企业的数据和网络安全面临着极大风险。

中级：在有限的EDR场景下，终端能够将收集到的攻击行为数据以及系统级事件上传到云端。但是云端的大数据处理能力和安全分析能力都比较欠缺，面对海量大数据，缺少安全知识和具备专业技能的安全专家，无法有效存储、处理以及利用这些安全大数据。

图2

360 EDR能力成熟度模型

资料来源：Qihu

高级：标准化的EDR，能够检测和调查安全事件，限制终端漏洞利用，提供安全修复指导建议。理想状态下，能够实时检测到安全攻击事件，同时基于云端的数据和安全能力分析，为终端提供快速响应，还具备一定的攻击后修复和清理能力，能够最大程度减少企业用户的损失。

特级：SaaS化和智能化的EDR，在云端采用SaaS多租户的部署模式，提供安全大数据的存储、数据实时处理、关联分析、并行查询以及秒级响应能力，支撑安全专家随时进行主动的威胁狩猎。同时基于查杀引擎、知识图谱和AI技术实现技术提升，使得EDR越来越智能化，包括对海量安全事件的自动分类、自动分优先级和对攻击行为采取自动响应等，极大地体现了下一代EDR的智能化特点。

3.5 EDR未来演进

基于以上EDR能力成熟度模型的定义，360认为未来EDR发展的两大关键词是：SaaS化和智能化。

未来EDR应该整合云端能力和终端资源以SaaS化服务形式面向大中小客户输出，增强内网端点威胁防御以及威胁对抗能力，保障各类生产和办公业务平稳持续运行。通过SaaS化提供云EDR的能力，同时可以将云端强大的数据存储、分析以及实时情报能力及时赋能到终端，实现终端和云端的实时交互。

用户通过订阅方式，能够及时获取到安全事件的完整分析报告，当终端记录的安全事件信息实时传到云端之后，无论终端是否在线，安全专家团队都能够非常方便地对安全事件进行查询和调查，并且能够实时回溯到指定的时间段进行过查询和分析。这就意味着在云端可以查询任何时间段的历史数据，且对终端的性能没有任何影响，这为安全专家针对任何恶意或可疑行为主动进行威胁狩猎提供了方便易用的平台。同时，借助安全专家团队的多年攻防经验，赋予产品安全有效的检测处置能力，能够相对智能地提供处理结果，并将防御和清除威胁及溯源结果及时反馈给用户。

通过主动进行威胁狩猎实现EDR早期发现威胁的目的，能够将24*7的威胁狩猎服务提供给云端用户，帮助企业用户解决长期安全运营问题。同时，云端通过图形化展示能够清晰展示安全攻击事件的全过程，包括事件发展的拓扑关系和详细信息，为用户提供完整的攻击报表。此外，基于云的架构部署一个轻量级的EDR终端，无论在时间上还是成本上，相对于私有化部署都将有很大的效率提升。

优势：

1) 数据打通：传统EDR产品后端缺乏安全大数据支撑，没有构建出覆盖面足够广、精确度足够高的检测防御模型，检测规则较为局限，同时情报能力的不足也大大影响了EDR总体的防御效果。SaaS化EDR打破了内网数据孤岛，弥补了传统EDR产品后端缺乏安全大数据支持的弊端，能够将自身威胁情报能力、检测分析能力以SaaS化形式赋能企业，助其构建覆盖广、精度高、可持续的防御体系，实现安全能力的成功落地。

2) 提升服务器资源利用率：传统EDR为了能获取最全面的威胁数据，往往会采集大量的端点信息，行为数据采集活动容易消耗终端和服务器的宝贵资源。通过SaaS化服务形式能更好地平衡安全能力与资源占用的问题，实现安全的同时减少端点性能资源的消耗，提升服务器资源利用率。

3) 降低成本：面对急剧增长的业务量，可以在短时间内完成部署，避免了大量控制台的服务器安装成本。同时在版本迭代期间，服务更新速度明显提升，后期功能和内容的增加也能够保证系统安全平滑拓展，对企业而言易于管理，降低了后期管理维护成本。此外，SaaS化EDR经过大规模场景实践验证和优化，很多坑不需要企业自己去踩，也不需要企业花费过多精力去做应用的优化适配。在提升系统稳定性的同时，节省了大量运维人力成本。

4) 提升服务稳定性、持续性：SaaS化EDR通过整合云端能力，可以帮助企业建立一套动态可持续演进的高级威胁能力体系，检测能力、情报能力能够持续更新，通过源源不断的安全赋能，实现对APT攻击的有效对抗。

4. 建设方案

4.1 产品优势

360终端检测响应系统EDR（以下简称"360 EDR"）是面向未来的EDR产品，同时具备SaaS化和智能化的特点，依托威胁情报，在360核心安全大脑的安全大数据、人工智能分析、攻击溯源等强大能力的支持下，通过持续监测端点活动行为，对于威胁风险进行深度检测、智能化分析和专业化处理。通过SaaS化技术方案，大幅降低用户成本，提升部署效率，联动全网大数据，全方位解决用户的终端安全问题。

作为面向未来的终端安全产品，360 EDR在产品化落地过程中具备了如下几方面突出优势：

1) 高质量数据采集能力-基于独一无二的核晶引擎

2) SaaS化-提供全网视角

3) 智能化-基于完备的安全分析能力和检测能力

4) 专业性-具备强大的安全专业团队

4.1.1 高质量数据采集能力

数据采集质量决定了EDR真正的检测效果，这一点经常被忽视，并误以为数据采集是简单工作。实际上采集高质量的安全数据是终端安全最有难度的工作之一。

高质量数据第一强调采集维度，多维度的大数据才是真正的大数据，时间维度包括攻击前、攻击中、攻击后，行为维度包括标准行为、差异行为、破坏行为，阶段维度包括有感染前、感染中，感染后等，只有这样的大数据才是高质量数据，基于高质量的数据才能真正发挥EDR的检测效果。

高质量数据第二强调采集精度，360核晶引擎直接抓获内核漏洞利用的行为，比通过大量进程、文件注册表等不直接相关的海量数据中，通过人力筛查蛛丝马迹去猜测是否有提权行为，要高效准确得多。更重要的是，目前EDR产品所使用的方法往往是少量系统标准接口（如文件注册表和进程的回调机制）、依赖于微软的ETW提供者，大量不满足要求的信息就靠注入加应用层HOOK。这些采集方法的问题首先是会轻易被攻击者绕过（例如Patching the patch、Direct system calls、P/Invoke to D/Invoke、Patching the Entrypoint等等公开的攻击手段），其次是数据细节不能满足高精度数据要求（例如：ETW的RPC事件数据细节不够，而360 EDR通过内核层面的RPC状态追踪，可记录更完整更精准的参数信息）。360 EDR使用360十几年积累的内核分析技术、独一无二的核晶硬件虚拟化引擎等多种引擎来收集安全数据，亦即基于顶尖终端技术能力实现了高精度数据的采集。

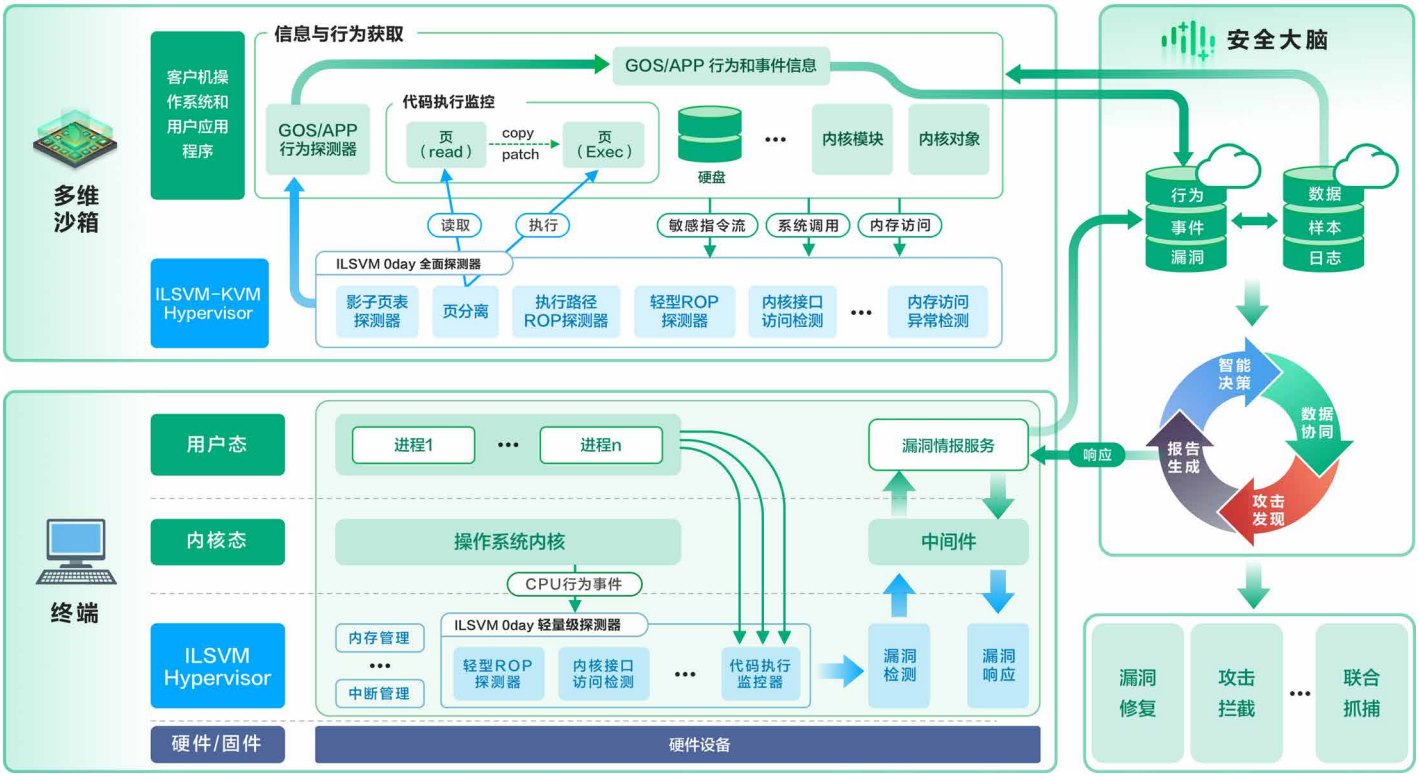
360 EDR提供超越内核级监控能力，利用CPU的硬件虚拟化机制增强64位系统的安全防护，对进程创建、进程注入、模块加载、注册表值写入、文件写入等等行为进行全面监控，规避了传统EDR大量依赖Ring3用户层监控技术的弊端，同时还能直接检测内核与应用层0day漏洞利用行为，有效对抗APT绕过攻击。

4.1.2 海量安全大数据

大数据作为360 EDR的持续驱动力，能够实时同步全球威胁，持续增强对APT攻击的检测和感知能力。基于17年实战经验，360已汇集了超300亿程序文件样本，22万亿安全日志、90亿域名信息、2EB 以上的安全大数据，可瞬间调用超过百万颗CPU参与计算、检索和关联多维度威胁数据。这是360 EDR的核心优势，即360拥有多维度、高质量的安全大数据，能够在全网范围内对安全事件做快速关联分析。

图3

360核心数据采集能力



资料来源：Qihu

4.1.3 安全分析能力

我们认为，“看见威胁”是终端防御的前提，而威胁检测能力的高低，直接影响“看见”的能力。360 EDR通过各种检测分析技术，对海量多异构数据进行分析，同时结合全网APT情报，确保了各类威胁全面可视。没有“可视”这一前提，任何威胁的处理都是一句空话，而威胁的可视化就是360 EDR的“雷达”能力，这种针对各类攻击的“雷达”能力，需要强大的安全分析能力支撑。360作为一家具有17年历史的数字安全领导公司，实现了从ToC到ToB/G的安全能力积累，因此具备了国内最强大的安全分析能力和技术。

4.1.4 专业团队支撑能力

人的因素在终端安全对抗过程中占据重要作用。360 EDR以世界级安全专家团队多年的攻防经验为基础，对产品核心功能进行持续打磨，赋予产品安全有效的检测处置能力。360拥有具备顶级漏洞挖掘能力的东半球最强白帽军团。至今为止，360专家已成功挖掘谷歌、微软、苹果等主流厂商CVE漏洞超3000个，获得微软、谷歌史上最高漏洞奖励，斩获中国首个“Pwnie Awards”黑客奥斯卡奖，并已成功追踪溯源海莲花、摩诃草、美人鱼、蔓灵花、蓝宝菇等针对中国的境外APT组织累计多达50个。这些数据足以证明360在攻防对抗方面的专业性和团队能力。在360 EDR的发展中，正因为这些专家团队的存在，才有效提升了其各项能力指标。

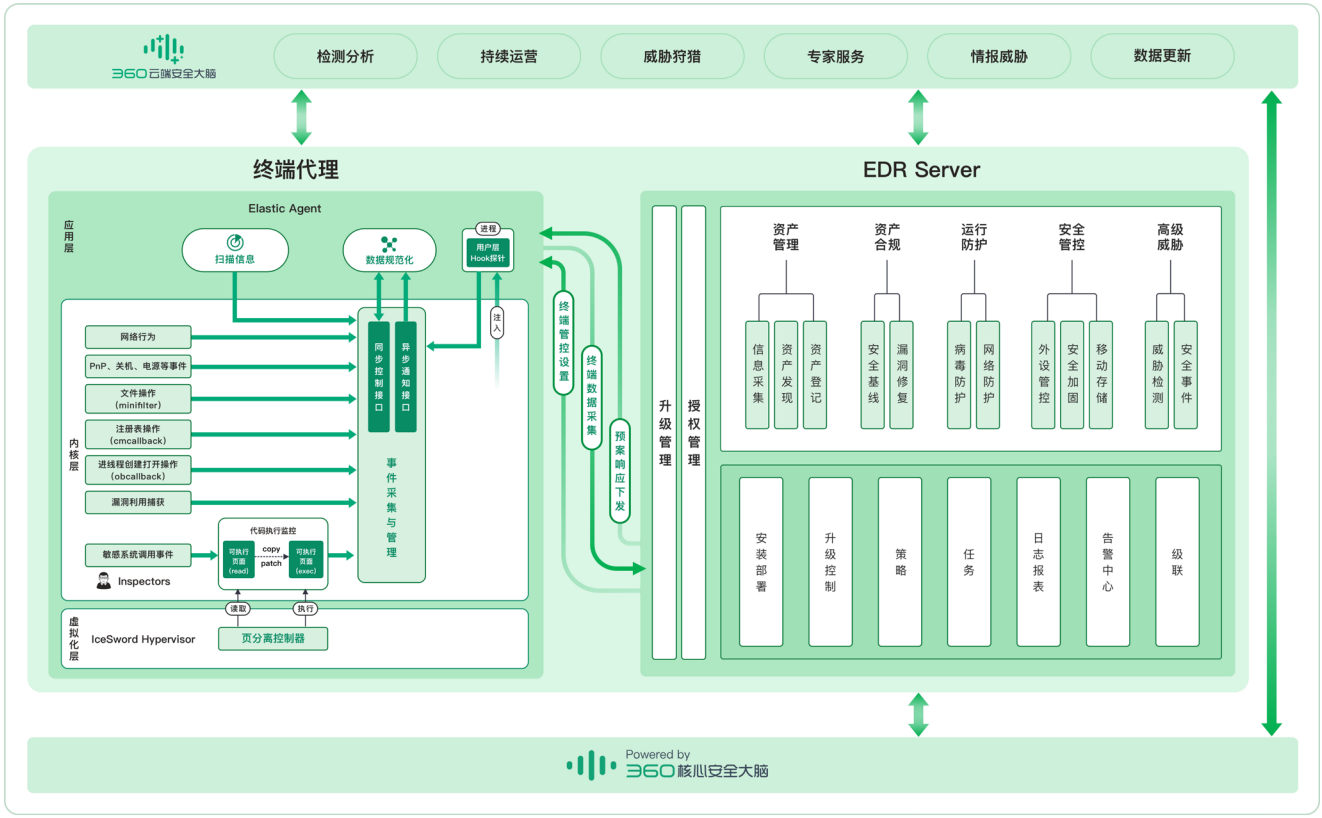
4.2 系统架构

4.2.1 EDR技术架构

360 EDR核心技术架构由三部分组成：包括终端代理探针Agent，EDR Server，以及核心安全大脑通用模块，其中终端代理探针Agent是360 EDR的最核心组成部分，通过冰刃的虚拟化技术、核晶引擎以及内核层全方位的监控技术，实现在攻击过程中全过程、全方位、高质量的数据采集，抽象且规范化后无损的传递给EDR Server用于威胁检索，同时接受并处理EDR Server对终端的处置命令，能够及时控制威胁。EDR Server具备对终端的管理能力，在升级、任务、策略等基础能力上增加了安全管理业务，包括资产管理、运行防护和安全管控等。在高级威胁业务中，通过其内置的威胁分析引擎，结合威胁情报实现威胁检测，同时提供

图4

360 EDR技术架构图



资料来源：Qihu

丰富的威胁抑制能力，可手动或自动对终端威胁进行处置，将威胁影响控制至最小。360核心安全大脑作为支撑赋能模块，汇聚了通用的功能和组件，为EDR Server提供威胁检测运算所需要的基础支撑，包括大数据存储和图数据库等。在联网场景下，EDR产品会和360云端安全大脑进行实时联动，能够充分利用全网大数据进行安全事件关联分析，实现对威胁情报持续运营，以及有效结合安全专家服务。

总体来说，360 EDR是一款专注于入侵检测与响应，有效应对各类高级威胁的新型终端安全产品，终端探针Agent基于360自研的核晶引擎技术，以非常轻量级的方式收集终端的进程、网络、文件，驱动等系统行为日志，在服务端利用威胁情报，各类检测引擎与全攻击链路行为分析等多种技术手段，实现对高级威胁的精准发现、自动化告警关联、攻击链路可视化展示与高效溯源、入侵事件响应及阻断等功能，同时支持对终端海量行为日志进行灵活检索，威胁狩猎，充分发挥核心安全大脑的数据存储和处理能力，以及云端威胁情报能力。

4.2.2 核心安全大脑架构

为了应对现而今数字化时代的复杂安全挑战，360运用系统思维，打破安全体系与数字体系的界限，融合攻防能力与管控能力，建立了一套可运营、可持续、可成长、可输出的面向未来的数字安全能力体系。360核心安全大脑3.0由一个安全大数据平台、一个云端赋能平台和多个安全分析引擎以及内嵌360十七年经验所积累的实战方法论组成。

核心安全大脑作为面向未来的数字安全能力体系中的“中枢系统”，负责全面体系化的核心运算及分析工作，通过联动“云端安全大脑”全面赋能360以及合作伙伴生态内的所有安全产品，从架构上打破云端知识、客户业务及生态数据之间的固有屏障，拓展全局安全视野，融通各类安全数据，协同整体实战决策；帮助相关安全产品在信息共享的全面覆盖、大数据集中分析研判、高级威胁情报赋能、网络安全产品体系化联动等全方面提升业务能力，帮助用户大幅度提升安全风险的识别、保护、检测、响应、恢复等各项能力。

通过结合威胁情报和360核心安全大脑的赋能，360 EDR实现了SaaS化和智能化，为用户提供最强大、最全面的安全分析能力、攻击溯源能力、可视化展现能力、快速响应能力、联防联动能力、定制化安全运营能力以及丰富的订阅服务。360EDR作为一个全SaaS服务平台，覆盖所有终端类型，包括Windows、Linux等常见平台，以及信创和Mac等特殊平台。针对明确的攻击风险，360 EDR可提供完整的修复和清理建议，为了避免再次被攻击，还会执行对应的安全加固、系统补丁、网络控制等防范措施，并实时同步到所有终端。

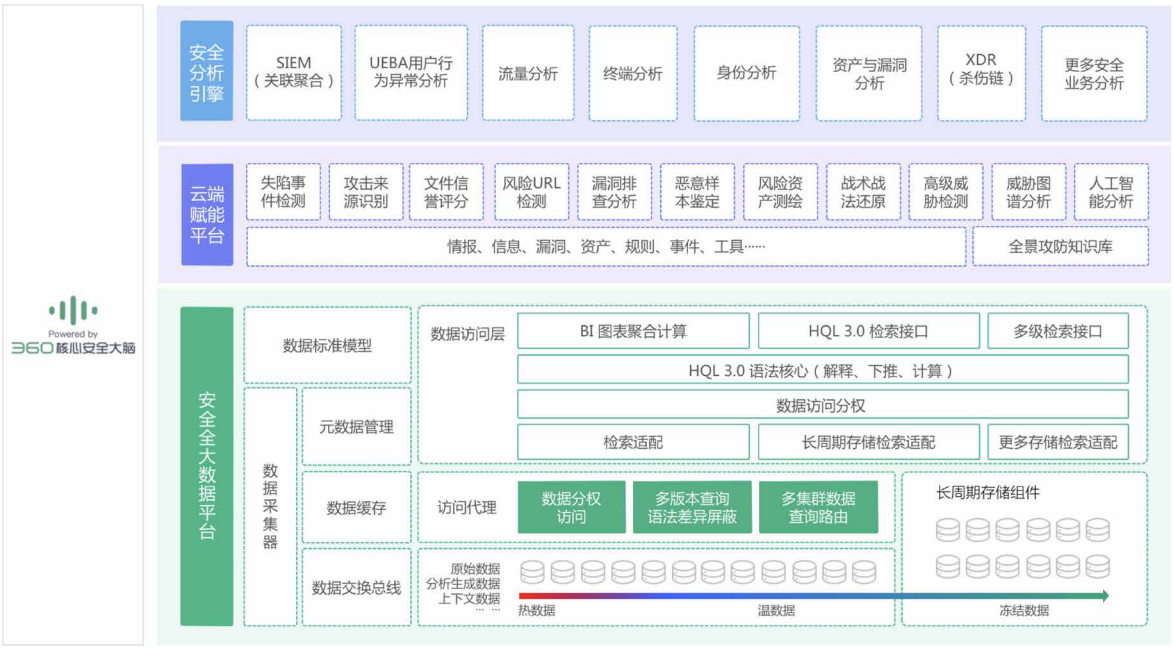
4.3 解决方案

4.3.1 环境背景

随着各行业组织数字化转型加速，重要基础设施、各种交通枢纽、各种能源设施、重要行业企业的生产资料都被搬上云端。大量终端设备联网意味着有更多的开放端点成为被攻击的目标。由于数字化的基础都建立在软件之上，如若软件因为存在漏洞而遭到攻击，核心服务和数据受到攻击，数字化的世界将会遭到重大破坏，继而直接影响物理世界的运转。

图5

360核心安全大脑



资料来源：Qihu

终端作为网络攻防的主战场，也是最新的攻防技术试验场，一直面对高级APT攻击的巨大压力。EDR作为一种应对高级威胁的解决方案，已经成为端点防御中的重要力量。然而攻防态势一直在演进变化，"矛"与"盾"之间的较量从未停止，传统的EDR建设方案在数字化时代也面临着新的挑战。由于传统EDR产品往往依托本地有限的检测能力，缺少云端海量安全大数据、高级威胁情报以及内存级安全事件检测能力，在面对高级威胁时往往束手无策，存在"威胁看不全"、"疲劳告警"以及"攻击绕过"等三大突出问题，直接影响了EDR的检测能力和溯源能力，导致EDR的落地效果大打折扣，具体表现在：

1. 威胁看不全："看见威胁"是EDR能力的基础，由于缺少全网安全大数据，尤其是缺少实战化的安全大数据，无法构建覆盖面足够广、精确度足够高的检测防御模型，检测规则较为局限，同时威胁情报能力的不足也大大影响了EDR"看见威胁"的能力。

2. 疲劳告警：如果对操作系统的运作机制缺乏深入研究，就无法细致区分系统正常事件和系统异常事件，如若把正常的进程行为、系统行为识别成威胁事件，EDR就会产生大量误报；另一方面，由于APT对抗经验的缺失，无法判断哪些异常是一般事件，哪些异常是需要重点关注的事件，导致EDR告警泛滥，而真正需要被关注的重要信息被淹没。大量冗余告警和不准确告警给安全分析人员带来了额外的工作量，直接影响安全专家依靠EDR进行分析研判的效率。

3. 攻击绕过：近几年来，漏洞攻击的检测技术一直在不断发展和演化，在大量APT攻击实例当中，0 day漏洞的未知性给相关的检测技术带来了很多的挑战。比如：

1) 0 day漏洞攻击特征不明确，由于特征不明确，0 day漏洞很容易绕过基于特征码的检测系统；

2) 攻击者通过各种混淆手段绕过检测；

3) 传统0 day漏洞攻击检测方法有很高的误报率；

4) 传统0 day攻击检测太依赖手动分析。

4.3.2 新一代EDR解决方案

随着攻防对抗的不断演化，以云端能力为核心，以安全大数据、威胁情报、高精度异常数据采集等核心技术为支撑，有效规避传统EDR检测技术的弊端，打造高维度的APT检测对抗能力，已经成为数字化时代应对APT高级攻击可预见的趋势。通常在一起APT事件中，0 day漏洞攻击的利用流程大致可分为如下几个阶段：

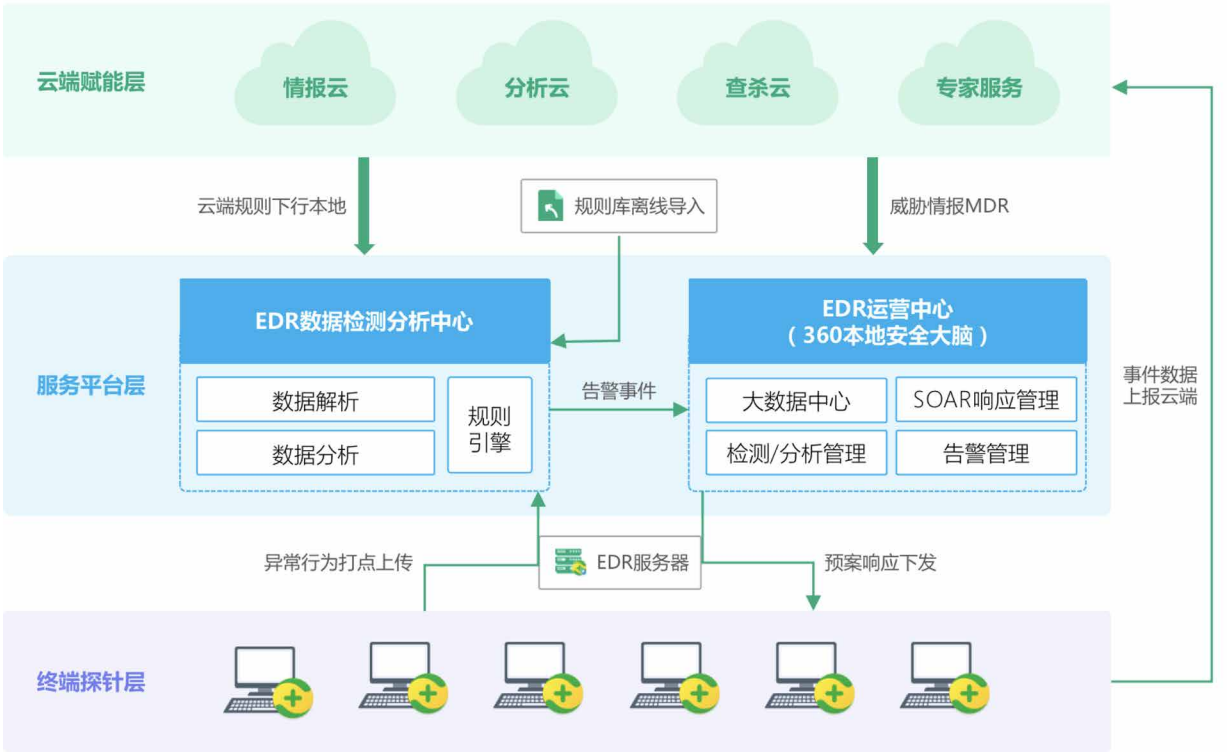
1) 触发阶段：如控制流转移到攻击者可控范围；

2) 利用阶段：如执行不同目标任务的Shellcode；

3) 扫尾阶段：如植入持久性目标恶意代码。

图6

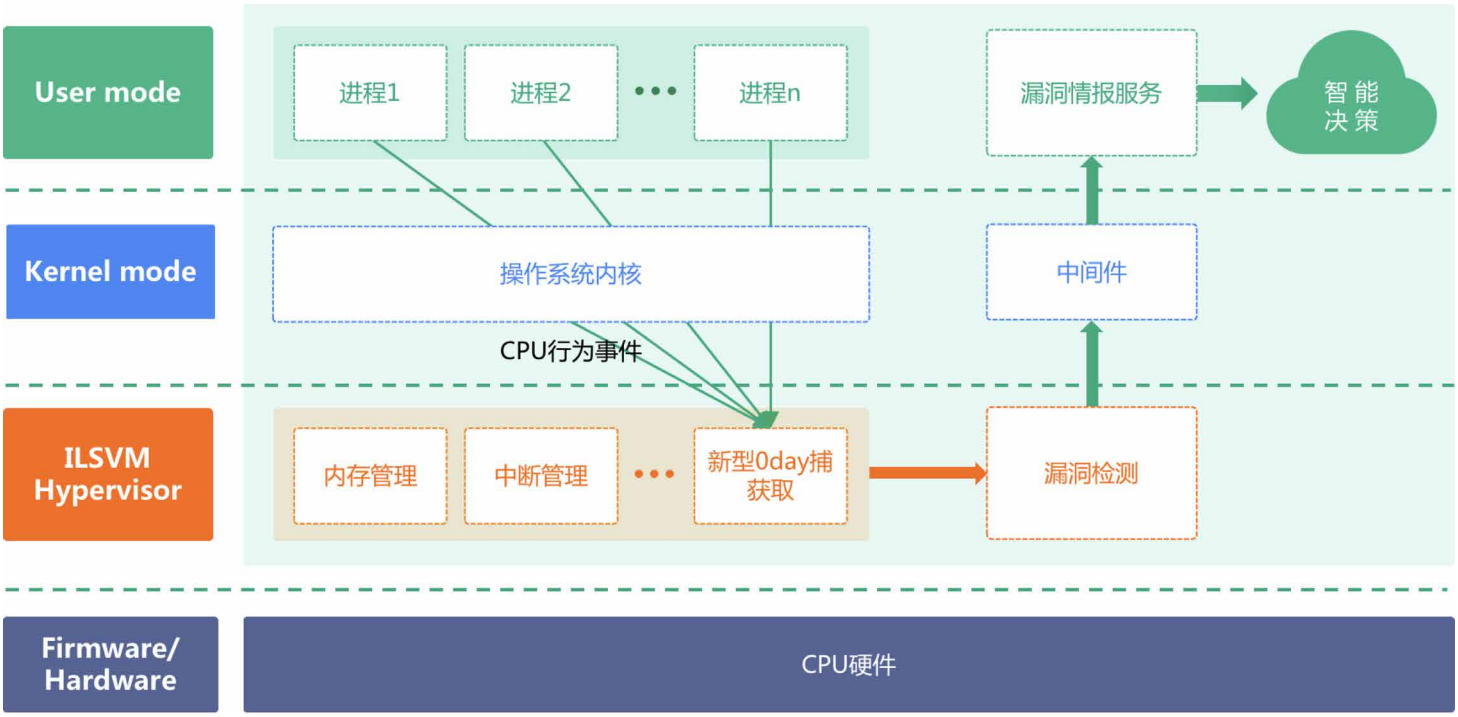
360新一代EDR解决方案



资料来源：Qihu

图7

冰刃安全虚拟机



资料来源: Qihu

绝大多数传统的手段只能在第三阶段即扫尾阶段发挥作用，而能够在第一阶段和第二阶段起到的检测作用十分有限，有的甚至在这两个阶段无法发挥作用，从而导致检测方案失去作用。而360有着天然的云和终端双重基因，经过17年亿级终端攻防实战经验积累，成功建立一套基于360核心安全大脑实时赋能，结合360"全视之眼"独有的终端探测技术，以全网安全大数据、全球威胁情报驱动的新一代EDR解决方案，为广大政企用户提供卓有成效的APT检测对抗能力。

其中360冰刃研究院自主研发和设计的终端漏洞捕获子系统，使用CPU的硬件特性和比操作系统内核态更高特权的轻量Hypervisor层，根据0 day攻击时在内存、CPU寄存器和进程中的最根本特征和表现（比如任何0 day漏洞攻击必定需要控制流的转移等特征），解决了市场上所有0 day漏洞检测方案的不足，对0 day攻击进行极为精确和实时的检测、拦截、响应和溯源。

终端漏洞捕获子系统采用了基于硬件虚拟化的漏洞利用无感检测技术，该技术由360冰刃研究院自主创新研发设计的冰刃安全虚拟机系统ILSVM（Icesword Lightweight Secure Virtual Machine）提供，ILSVM是一套针对安全需求实现的虚拟机系统，该虚拟机系统不依赖于各型市面上已有的虚拟机系统，而是从零开始重新设计开发的以实现安全检测与防御特性为主的全新轻量级虚拟机系统（ILSVM Hypervisor），它的设计和实现弥补了国内此类基础软件的空白，是目前国内乃至世界上唯一能在客户终端默认实时开启的安全虚拟机系统。目前，360安全卫士已在数亿客户端中运用了此技术。

冰刃安全虚拟机系统ILSVM能够保证对操作系统内核和应用态进程，完备全面的行为监控和特征收集，与传统0day检测、HIPS和AV等所不同的是，ILSVM能够对所有内存操作、内核操作、进程操作进行毫无遗漏的监控。这缘于ILSVM的特权级别是比内核特权更高的Hypervisor层，这是其他0day检测方案所不具备的。借助强大的ILSVM，能够在漏洞攻击的三个阶段均布置上多种全球独创的新型探测模块，对CPU的控制流和指令执行序列进行纤毫无遗的监控和分析，使发现漏洞利用攻击的能力提升到一个新的高度。这种终端上独有的专利性探测技术，为360 EDR解决方案提供赋能，对高级威胁检测起到了非常关键的作用！

360提供的新一代EDR解决方案具有三大特点：

1. 云-地双场景：

360 EDR提供云端SaaS化和本地私有化两种部署模式，满足互联网和隔离网双场景的安全防护需求。依托于360核心安全大脑理念和安全运营能力框架打造的SaaS化EDR，基于云视角打造的安全防护体系，使得终端的各类安全事件和云端的大数据做广泛的数据

联动，实现了安全能力从孤岛式、被动式的单点防护到主动式、全局式的纵深防御的有序演进。这种基于全网的SaaS化云安全体系防护也是EDR未来最有效的防护方式，天然具备低成本、高效率的优势，针对高级威胁的事件检测和溯源能力被大幅提升，且这种能力是持续的，还能够自我快速修正和迭代。

对于隔离网终端安全防御场景，360 EDR提供了本地私有化部署方式，可以把云端能力下沉到本地网络中，实现自运营的EDR管理模式。

2. 能力实战化：

数据是最完美的诠释，360 EDR在多家客户的实际建设运行过程中，对高级威胁起到了非常有效的防御作用。仅在2021年，就发现并处理了勒索病毒、暴力破解、挖矿木马、WebShell后门、恶意程序等重大攻击事件数百起；在客户内部风险管控方面，发现并处理了异常邮件发送，数据泄露，账号异常、违规外联等严重违规事件近百起。实践证明，360 EDR提供的安全响应能力将客户的风险处置能力从小时级提升到了分钟级，实现了安全事件零损失，保障了多家客户关键业务运行安全，关键数据不受影响，从根本上解决了客户对网络安全的隐忧。

3. 响应自动化：

360 EDR提供安全风险综合评估、SOAR自动化响应处置能力，可以实现自动化安全事件闭环处置流程，提高安全事件处置效率和效果。利用360核心安全大脑提供的威胁情报自动关联分析能力，360 EDR让高级威胁不再隐匿，攻击过程中所有关键环节全部可视，防护效果不再模糊，实现防护指标全部量化，让客户业务运行的更安全、更稳定、更高效！

4.3.3 客户案例

4.3.3.1 客户背景

A公司是一家中国领先的连锁商业集团，致力于成为全球最具创新的商超先锋。作为一个全业态多功能综合体，A公司集社交、娱乐、美食、零售功能于一体，形成了独立大型商超，是消费者进行休闲、娱乐和消费的重要场所，为消费者提供了极致的消费体验。

早在2015年，A公司就启动了数字化转型，并一直致力于打造以提升服务及消费能力为目标的数字化生态系统。基于公有云和三个数据中心，该企业建设了一系列内部业务系统和互联网零售外卖系统，为全国1300多个城市，上万家零售网点的20多万员工、千万级用户提供互联网零售、门店运营、供应链管理、智能外送等服务。庞大的数字会员基础与强劲的数字化能力也使其整体提高了运营效率，并为其快速扩张打下了坚实的基础。

360和A公司的合作，正值其数字化转型关键时期。作为旗舰型企业，A公司在数字化转型过程中，需要从安全、风险、合规、隐私、道德和社会责任等多个方面充分考虑。合作初期，360政企安全集团就帮助A公司梳理出了安全痛点，让客户对潜在的网络安全风险有了更全面的认识：

1. 网络攻击风险加剧：商业消费业务价值高，线上线下交流频繁，容易成为重点攻击和勒索对象。商业数据敏感性强，涉及到用户隐私，一旦泄露，对公司声誉影响很大。

2. 检测防御能力滞后：现有技术架构由于缺乏对海量数据集中化存储支撑，造成安全数据碎片化，不利于进行数据管理的统一规划；现有技术架构对大量数据处理能力低下，只能采取事后离线分析，不利于对威胁的实时感知，往往使防护工作处于被动响应状态；现有的技术架构扩展能力成本高，性能提升需要付出大量的设备消耗，不利于整个分析能力持续、有序地升级。

3. 长效安全运营机制缺失：缺少体系化的安全运营平台，缺少足够经验，尤其缺少拥有大型实网攻防经验的安全运营团队，因此无法确认当前内网是否存在风险，不知道风险何时植入、内部终端失陷和感染情况。同时，A公司终端分散，各地区安全防御协同性差，风险难以及时有效处置。该企业业务范围遍布全国31个省1300多个城市，覆盖供应链管理、商品加工生产、门店销售、经营管理等多个部门，风险及威胁处置往往需要跨地域、跨部门进行，协同性低，处置周期长，导致安全威胁得不到及时解决，安全隐患无法立即排除，企业长时间暴露在风险环境中。由于缺少长效的安全运营机制，A公司的终端安全运营处于被动低效的状态，终端整体防线脆弱，难以应对高级APT攻击。

近几年来，针对大型连锁集团商业客户的高级威胁层出不穷，有组织有目的网络攻击活动经常发生。针对已经存在和可能面临的网络安全风险，A公司对360提出了高标准的网络安全防护要求，包括实时检测并防御高级威胁、防范内部风险、保障业务连续、提升处置效率等。360基于A客户的安全要求，成功落地360 EDR解决方案，充分利用了终端的数据采集能力和360核心安全大脑的大数据分析能力以及360安全专家专业的安全分析能力，实现外部威胁可发现、内部风险可感知，及时、准确地处理网络攻击事件，帮助A公司多次规避网络安全威胁，实现安全能力从被动式单点防护到主动式纵深防御的有序演进，保障了A公司全国业务的平稳运行，为A公司的业务蓬勃发展保驾护航。

4.3.3.2 案例分析

A公司已经部署了360 EDR系统，在守护A公司的网络安全过程中，360还原了之前一次非常经典的漏洞利用APT攻击案例。某攻击组织预备入侵A公司并窃取相关技术资料和商业机密，对其造成经济打击。在接到任务后，攻击组织对A公司进行了大量的信息收集工作，整理出A公司常见的外网资产、网上销售渠道、电子邮箱以及其他相关信息。春节前期，A公司在外部平台发布关于征集春节礼品方案的相关征集文章，并附有相关的电子邮箱，这被黑客视为发起钓鱼邮件攻击的突破口。

在整个攻防过程中，360 EDR通过强大的终端异常行为数据采集能力，充分发挥积累了17年的云端安全大数据能力、SaaS化全网联动分析、基于360"全视之眼"的终端检测技术等核心能力，对本次APT攻击事件进行精确溯源，全面检视并验证了360 EDR在实网环境下的核心安全价值。

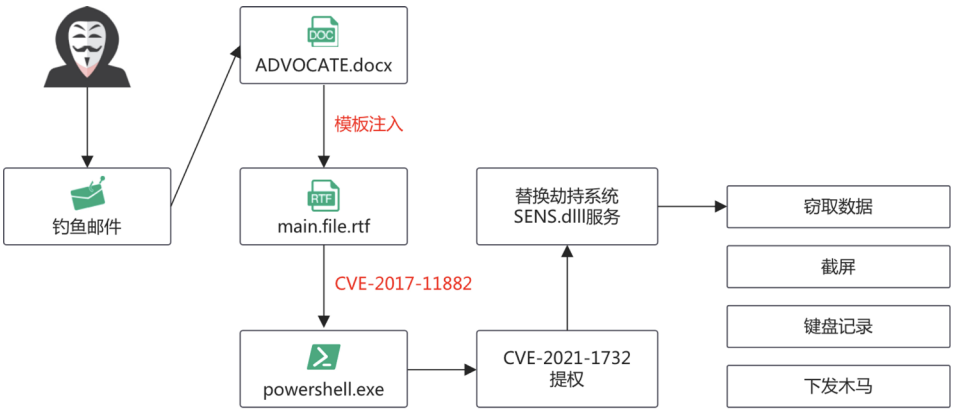
1 APT攻击-侦察和武器制作阶段：黑客通过社交媒体，搜索引擎搜集该企业员工的邮箱账号，并制作主题与"春节礼品卡"相关的钓鱼邮件及携带恶意代码的文档附件。

2 APT攻击-武器投递阶段：黑客将钓鱼邮件投递给该企业的诸多员工，其中由于不少员工因缺乏安全意识浏览了该邮件并打开了其中的文档附件，黑客在附件中利用模板注入技术(T1221)，在附件被打开后从远程服务器加载恶意的文档模板。攻击过程中产生的模板注入事件被360 EDR重点关注且成功检测。

3 APT攻击-漏洞利用阶段：模板是黑客预先放置的带office漏洞 (CVE-2017-11882) 的rtf恶意文档。漏洞触发后会调用PowerShell进程执行一段恶意脚本，异常进程链被360 EDR实时捕获并做清晰的图形化展示：

图8

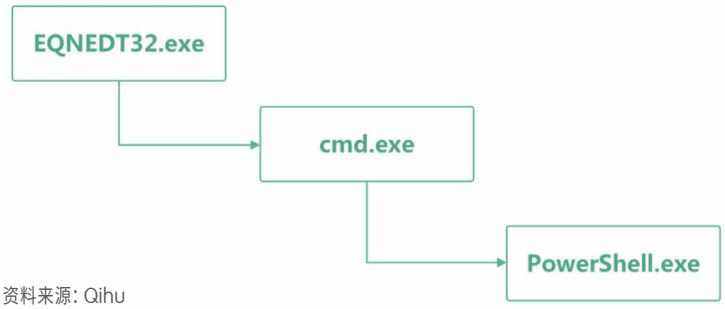
鱼叉攻击流程图



资料来源：Qihu

图9

APT攻击-利用阶段



资料来源：Qihu

4 APT攻击-提权阶段：脚本的功能是通过无文件攻击技术执行CVE-2021-1732漏洞利用代码，将权限提升为SYSTEM权限，并执行进一步的恶意功能。360 EDR及时检测到通过系统漏洞进行的各类提权行为。

5 APT攻击-安装驻留阶段：攻击者将权限提升到SYSTEM之后，替换系统SENS服务对应的动态链接库实现驻留。360 EDR及时检测到了白名单里的关键文件发生了变更。

6 APT攻击-命令与控制阶段：用户重启电脑后，SENS.dll随系统服务启动，SENS.dll是一个后门程序，会与黑客控制的C2服务器建立连接，并接受黑客下发的控制命令并执行，下发的命令包括收集用户电脑中的敏感文件、账号密码、截屏以及键盘记录，下发其它恶意程序等待。此时黑客已经完全控制了该企业内网中的这些机器，这些机器也被称为失陷主机。

7 APT攻击-横向渗透阶段：黑客并未在这些用户电脑中得到太多有价值的商业数据，于是决定向内网进行进一步的渗透，扩大控制范围，通过之前控制的失陷机器向内网发起了内网扫描，探测到企业内网的大致网络架构，并确定了域控，数据库服务器等多台重要的网络资源。360 EDR通过监控多种远程操作和远程执行计划等行为，及时且全面地捕获到了各类横向渗透事件。

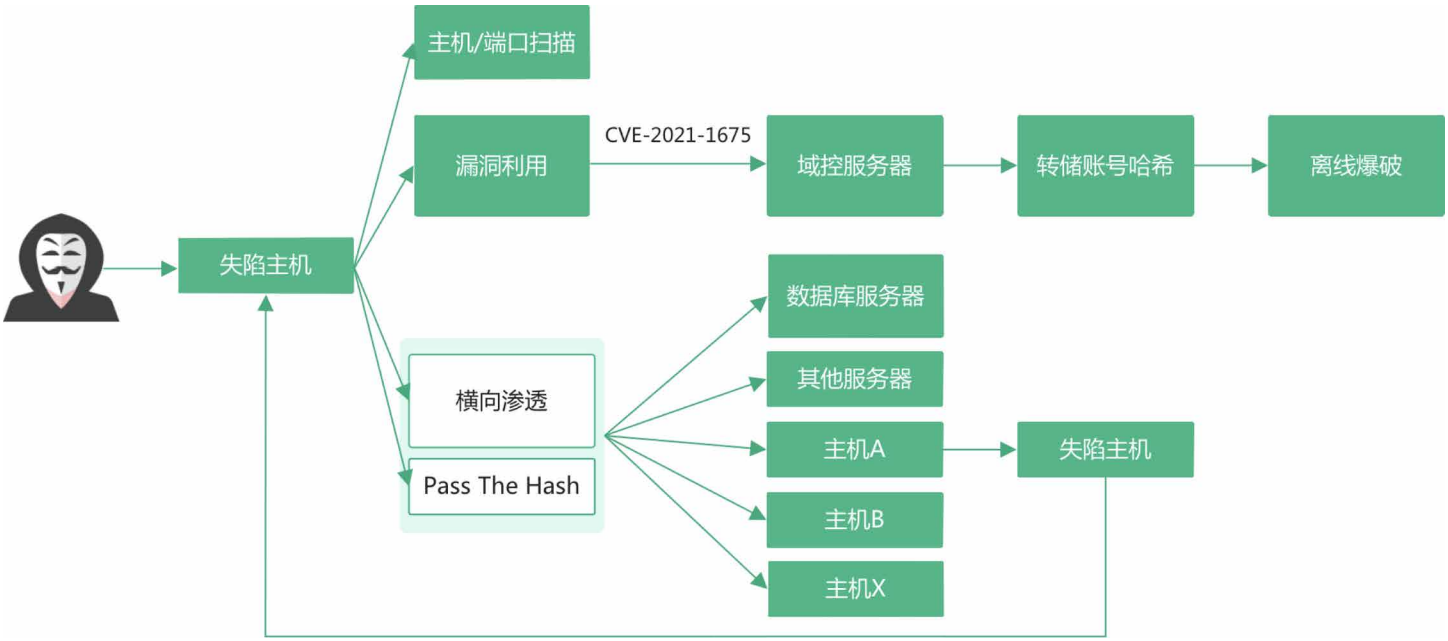
8 APT攻击-横向渗透阶段：黑客通过扫描域控服务器，发现域控存在打印机漏洞 (CVE-2021-1675)，黑客通过该漏洞拿下域控权限。

9 APT攻击-横向渗透阶段：黑客拿到域控权限后，通过Mimikatz工具转储了所有用户的账号和哈希，并将哈希通过离线爆破出明文密码。

10 APT攻击-横向渗透阶段：黑客通过横向渗透技术 (创建远程计划任务等) 在内网其它机器创建恶意的计划任务，计划任务内容为一段PowerShell命令，之后重复之前的攻击步骤。360 EDR及时检测到了这类基于远程计划的横向渗透行为。

图10

横向渗透



资料来源: Qihu

11 APT攻击-横向渗透阶段：部分哈希未被离线破解，黑客利用Pass The Hash技术，在目标机器上继续运行恶意PowerShell命令。

12 APT攻击-数据窃取阶段：黑客窃取到该企业大量的敏感数据，并将其发送到黑客控制的FTP服务器。

13 APT攻击-结束攻击阶段：黑客删除上述过程中使用的恶意程序，删除系统日志，渗透攻击结束。360 EDR通过实时的RPC监控，攻击者调用特定的和关键的API被实时记录下来。

4.3.4 新一代EDR解决方案价值

检测安全事件、调查安全事件是EDR的两大核心能力。在本次网络攻击溯源案例中，360 EDR通过全面准确采集终端异常数据、终端行为告警降噪、威胁情报关联分析碰撞，完整记录并还原了APT攻击的整个过程，充分体现了360 EDR在异常事件采集、大数据分析溯源方面的突出优势，体现了360 EDR在实战化环境下应对APT攻击的巨大价值。

1. 关键行为精准捕获

基于360 EDR内存级监控技术，360 EDR能全面监控进程、注册表、文件、网络行为，包括进程创建、进程注入、模块加载、注册表值写入、关键注册表写入、新文件创建、文件写入、网络访问、域名解析等，对Office漏洞利用、无文件攻击行为精确捕捉，可以清楚地看到每个关键的攻击过程，在触发到漏洞提权和域控漏洞利用时，会直接进行阻断，避免客户的关键数据被窃取。360 EDR采用的"全视之眼"端点探测技术，规避了ETW、API Hook等传统EDR方案的技术缺陷，对关键进程行为和异常调用不漏检，不错过APT在终端上的任何蛛丝马迹，有效规避了传统EDR产品检测不全面、检测片段缺失的问题。

2. APT攻击链完整溯源

360 EDR提供了针对高级APT攻击完整溯源的能力，通过把采集到的异常事件与360大数据分析能力结合，经过威胁情报碰撞形成完整的攻击链图谱。基于可视化的攻击链，安全运营人员可以针对暴力破解、漏洞提权、动态链接库劫持等多种攻击方案进行全面检测与可视化溯源。

3. 专业化安全运营机制

专业化的安全运营团队在应对紧急安全事件的过程中具有重要作用。A客户通过部署360 EDR产品，把360多年积累的安全专家运营能力成功下沉，从安全状态总览、安全事件分析、响应处置、评估改进等安全一站式工作台制定相应的威胁检测和响应流程。360拥有业界领先的网络安全专业化攻防团队和运营团队，在360 EDR落地A公司过程中，360安全运营专家深入业务场景，面向实战，从信息安全、网络安全拓展到业务安全，实现了安全能力的可持续提升，为客户打造不断迭代，能力持续增长的数字化安全防护体系。

本项目以端点安全防护为核心，以智能化检测技术和大数据存储分析技术为支撑，基于360核心安全大脑赋能，以17年端点安全攻防经验积累，倾力打造的云-地一体端点威胁纵深防御体系，解决了传统解决方案存在的终端检测能力不全、终端威胁难溯源、终端运营机制缺失等难题，建立了一套面向实战的APT攻击对抗体系，完全符合基于云的终端安全发展趋势，能够有效解决A公司当前以及未来面临的终端高级威胁防护难题，是真正适用于数字化时代的端点安全智能化解决方案。

5. 总结

360 EDR具备高质量数据采集能力。通过360核晶引擎增加采集数据的维度以及精度，实现在攻击时间维度上全过程数据采集，同时利用对操作系统全方位监控能力，有效对抗APT绕过攻击。通过长期高质量的数据积累，360已汇集了海量数据，同时能够通过强大的数据分析平台实现对多维度威胁数据的计算、检索、关联，可更快、更全面的发现未知威胁和威胁影响分析。在具备海量数据和数据分析能力基础上，360 EDR依托强大的分析能力和技术、顶尖安全分析人员，结合APT情报确保各类威胁全面可视，并提供全面的事件调查、威胁响应、防护措施以实现遏制和防范高级威胁。

360 EDR依靠360云端核心安全大脑的情报赋能，以及云地一体的架构，充分发挥360在数据、情报、专家的优势，是新时期端点安全防御的重大实践成果。未来的EDR将会朝着SaaS化和智能化的方向持续演进！

参考文献：Qihu

Gartner的调研报告

2021年端点安全的技术成熟度曲线

安全和风险管理领导人想方设法保护企业端点，防范攻击和破坏，并力求提供高效和安全的远程访问。随着EDR的成熟和广泛采用，XDR、UES、SSE和SASE应运而生，提供整合独立安全解决方案的方法。

分析

企业需要了解什么

本文件修订于2022年4月6日。您正在阅读的文件为修订版文件。如需详细信息，请参阅gartner.com的Corrections（更正）页面。

端点安全创新者一直专注于改进和打造自动化程度更高的威胁预防、检测和修复流程，并将端点检测和响应(EDR)以及扩展检测和响应(XDR)作为研究重点。远程工作的突然激增使安全远程访问成为企业优先事项，短期而言会使自带PC (BYOPC)和VPN重新成为关注焦点，长期来看则会非常依赖安全服务边缘(SSE)和安全访问服务边缘(SASE)。安全领导者有责任保护端点、防范攻击，并确保用户可从任何设备通过任何网络访问任何应用程序，尽量不影响用户体验。我们将介绍端点安全领域最相关的创新，供安全领导者采用和实施，以应对这些挑战。

技术成熟度曲线

端点安全的技术成熟度曲线跟踪了助力安全领导者保护其企业、防范攻击和破坏的创新。这一领域的技术和实践正受两种趋势的影响：端点攻击的日益复杂化和远程工作模式的突然兴起。

勒索软件、无文件和网络钓鱼攻击的增长促使技术供应商进行创新。为了应对高级攻击，搜寻威胁时将来自端点和其他地方的数据进行关联变得至关重要；因此，XDR首次进入技术成熟度曲线。同时，更成熟的EDR采用率也在提升，而EPP产品也将进入完全成熟阶段。最新的统一端点安全(UES)概念将进入技术成熟度曲线；它综合了EDR、端点保护平台(EPP)和移动威胁防御(MTD)的要素。商业电子邮件诈骗(BEC)仍然是重大威胁之一，BEC防护能力在今年仍需继续进行创新，以检测遭泄露的账户，对抗网络钓鱼攻击。此外，虽然安全Web网关(SWG)是基于网络的技术，但它对于预防端点攻击也至关重要，并越来越广泛地被组织采用，尤其是在云端部署中。

最近的新冠病毒肺炎疫情及诸多外部因素导致远程工作模式突然兴起。实现远程工作所需的技术和实践已经达到完全成熟的程度，已成为行业主要趋势，并且在组织中充当战术解决方案的频率急剧提升。这些技术和实践包括安全的企业数据通信(VPN)、云访问安全代理(CASB)、BYOPC、统一端点管理(UEM)和桌面即服务(DaaS)。这些远程工作将有很大一部分将长期持续下去，并需要采用战略性的解决方案。[1]凭借零信任网络访问(ZTNA)及其在支持SSE方面发挥的作用，用户能从任何设备通过任何网络访问任何应用。随着ZTNA和SASE的成熟，它们的采用率都在提升，尽管两者的提升速度不同。

优先级矩阵

技术成熟度曲线中出现了一个新的波形。走向期望膨胀期顶峰的大多数创新都涉及多渠道或多系统的安全。例如，UES涉及使用单一产品保护工作站以及智能手机和平板电脑。同样，XDR的范围超越了端点，将多种来源（如网络）的信息结合起来，以检测威胁。这种技术融合趋势受到越来越多的关注；2020年初，参与Gartner调查的最终用户组织中，25%的组织表示他们正在寻求供应商整合战略。[2]

在今年的高峰期，SASE已实现让端点用户以受保护的方式通过任何网络访问任何应用。这是端点安全成熟度曲线中的一个转型创新，安全领导者应该开始制定战略，调整对ZTNA、CASB和软件定义的广域网(SD-WAN)的投资，为SASE奠定基础。

面对不断变化的威胁和资源丰富的对手，EPP和EDR等技术努力跟上新威胁的步伐，提供新的检测技术。此类成熟的技术在成熟度曲线中的变化较为平缓。

不在技术成熟度曲线上的条目

浏览器隔离：独立的浏览器会话有很多用途：嵌入到安全工作空间技术中、用于在安全电子邮件和安全Web网关技术中呈现外部URL，以及作为一种手段，为远程工作者提供对关键应用的有限访问。端点安全工具种类很多，但人们对浏览器隔离的兴趣仍然很浓厚，尽管只有少数人将之视为一种独立功能。

虚拟移动架构(VMI)：VMI功能独特，可以将数据与本地设备隔离。然而，由于移动操作系统虚拟化的复杂性，包括缺乏离线访问以及Android底层操作系统的虚拟化版本与本地安装版本的差异，VMI作为保护托管或非托管设备上数据的安全的主要工具会受到限制。尽管该技术具有将数据与本地设备隔离的独特功能，但虚拟移动操作系统的复杂性，包括缺乏离线访问和底层操作系统的差异，使得VMI不适合作为保护（托管或非托管）设备上的数据的主要工具。

安全的企业数据通信：仅仅用VPN基础设施来解决远程访问的挑战，是一种成熟的远程访问方法，为众人所接受。以VPN为中心的安全企业数据通信正在走出成熟度曲线，这表明ZTNA概念和SASE工具的作用正在得到重视。这些工具现在与现有的VPN基础设施一并部署（在许多情况下会取代后者），为日益多元化的远程工作者提供合乎情境需要的动态访问控制。

向上攀升

VDI/DaaS端点安全

分析师：Chris Silva、Stuart Downes

效益评级：高

市场渗透率：1%至5%的目标受众

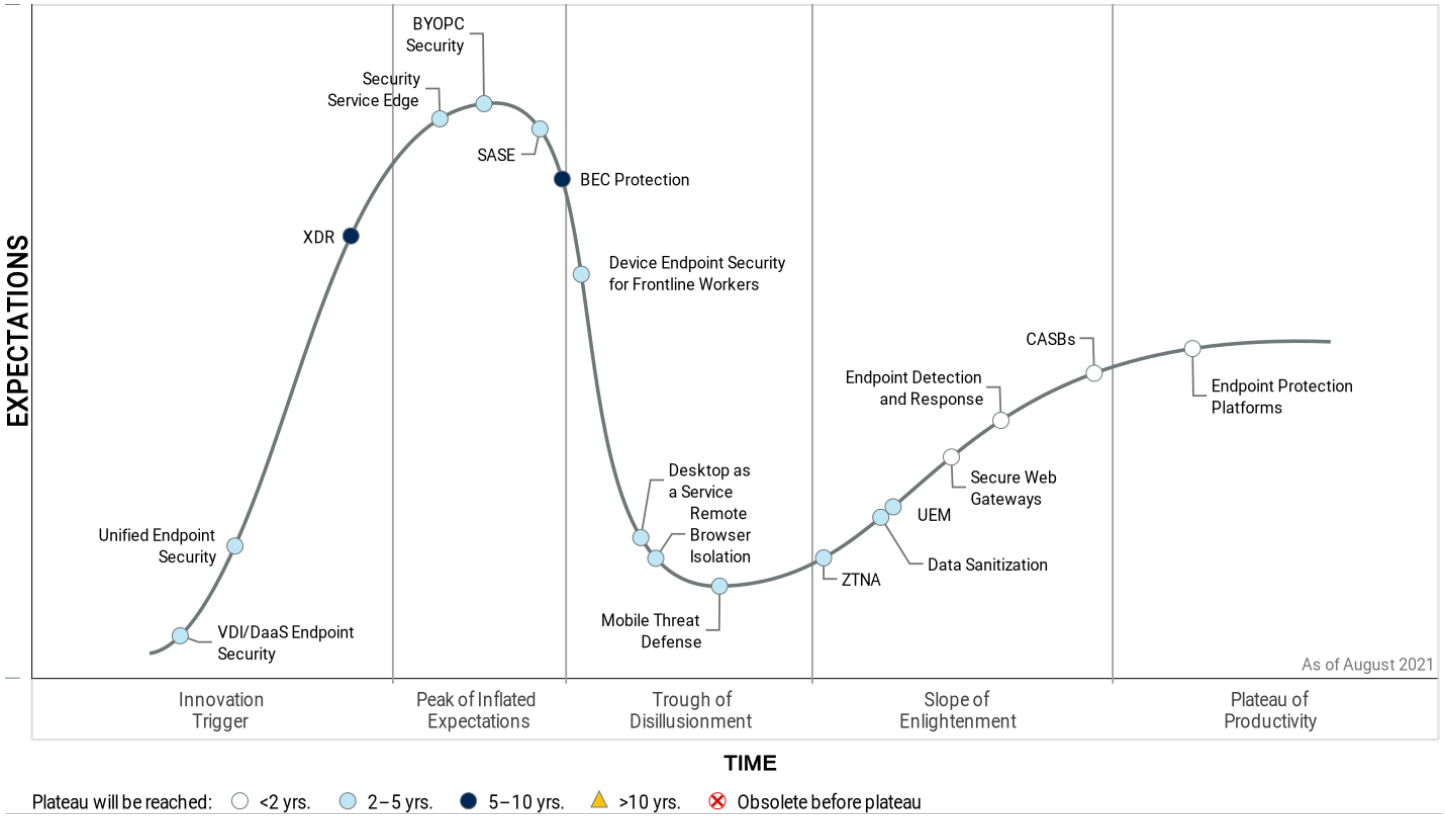
成熟度：新兴

定义：

VDI/DaaS端点安全涵盖与VDI和DaaS解决方案配合使用或嵌入到其中的安全软件，并提供额外的安全机制，例如会话劫持保护、画面监视预防和生物识别用户验证。

图1

2021年端点安全的技术成熟度曲线



资料来源：Gartner（2021年8月）

Gartner

表1: 2021年端点安全优先级矩阵

效益	获得主流采用的预期年数			
	不到2年	2-5年	5-10年	超过10年
具有变革性	CASBs	自带PC安全 SASE		
高	端点检测和响应 安全Web网关	桌面即服务 远程浏览器隔离 安全服务边缘 UEM 统一端点安全 VDI/DaaS端点安全	BEC保护 XDR	
中	端点保护平台	数据净化 针对一线员工的设备端点安全 移动威胁防御 ZTNA		
低				

资料来源：Gartner（2021年8月）

重要性

全球新冠病毒肺炎疫情使虚拟桌面基础设施(VDI)和桌面即服务(DaaS)得到进一步推广。越来越多的用户对围绕实际查看连接的用户的身份、虚拟会话的录制以及会话劫持风险表示了安全忧虑。因此，市场中逐渐出现新的安全软件领域，助力用户预防和抵御这些活动。

业务影响

为满足为所有用户授予对数据和应用的完整权限的需求，并同时支持各类设备，确保数据安全和主权，针对VDI和DaaS的额外安全插件的需求随之出现。这些插件可以与任何设备搭配使用，或作为专用安全浏览器或远程桌面应用的一部分发挥作用。这种机制能在保证身份和防止数据泄漏的同时实现访问。

驱动因素

- 为防止因虚拟连接造成数据泄漏，相关机构制定了围绕现有数据主权法规的相关合规条例。
- 迎合仅授权用户能查看虚拟化连接的内容的要求。
- 非托管/托管不善的设备上虚拟连接导致会话劫持或屏幕镜射的可能性增加。
- 越来越多企业使用VDI和DaaS来实现业务连续性，或确保远程员工、供应商和承包商能够通过非托管设备（在开展自带PC[BYOPC]计划的组织中很常见）或托管功能有限的设备（如Chromebook）访问企业应用和数据。

阻碍

- VDI和DaaS安全解决方案通常由第三方供应商提供，而不是由虚拟化供应商提供。如果虚拟化供应商进行更新，上述情况可能导致故障。
- 这个领域的供应商有可能成为提供特定功能的虚拟化供应商，而非独立的产品类别供应商。
- 并非所有供应商都支持所有的虚拟化解决方案。
- 用户可能会对使用摄像头监控家庭工作空间的安全软件感到担忧，大多数供应商不提供这一功能。
- 在整合安全工具的趋势下，企业将不得不承担购买、安装和管理另一个点解决方案的费用。

用户建议

- 将投资重点放在有文档支持的解决方案上，以满足相关的数据合规法律的要求。
- 追求控制基线，以利用剪切/复制/粘贴控制和对数据采集的限制，阻止数据传输到其他端点或从其他端点传输过来，并复制物理端点的现有安全态势。
- 除了这些基线控制外，还要确定在哪些地方应用适用于特定用例的控制（如生物识别身份验证）或何时需要验证特定用户的身份。
- 评估供应商在不降低性能或体验的情况下，整合预期或现有虚拟化解决方案的可能性。

供应商举例

Citrix; Minerva Labs; SecureReview; SentryBay; ThinScale

统一端点安全

分析师: Rob Smith

效益评级: 高

市场渗透率: 5%至20%的目标受众

成熟度: 新兴

定义:

统一端点安全(UES)将端点和保护以及MTD集中到统一的平台中，紧密连接面向最终用户设备的端点管理基础设施，如Windows10、macOS、iOS、Android（在某些情况下，还涵盖Linux和ChromeOS）。

重要性

随着近期全球疫情的爆发，人们开始需要使用自己拥有的任何设备实现快速访问。这导致使用多系统的情况（系统间往往不共享数据）面临安全挑战，进而造成更大的风险。UES通过为所有设备类型提供单一的数据湖来解决这个问题，使IT部门能够制定更明智的风险和访问决策。该技术还有一个优势，就是提供以前不适用于非托管设备的态势和配置信息。

业务影响

组织应以三个主要目标来评估UES的采用：

- 将检测和响应的范围从传统的笔记本电脑和台式机端点扩展至移动设备。UES的概念是XDR概念的一个子集，仅适用于端点。
- 从单个控制台统一端点安全和管理工作流程。
- 实现基于态势的复杂政策应用，同时支持安全远程访问等技术。

驱动因素

组织采用UES的驱动因素包括：

- 通过提供具有EPP、EDR和MTD相关功能的单一控制台，整合众多安全系统，减少其数量，以提供更直观的视图，简化管理。
- 需要确保使用各种设备类型的最终用户都能访问。这在全球疫情蔓延的背景下变得尤为关键。
- 需要向云端应用过渡并满足条件性访问的要求。UES是VPN、ZTNA和SASE等远程访问的条件性验证流程中的关键组成部分。在这种情况下，当设备允许访问时，系统将查询相应端点，确认其是否已安装UES。如果未安装，系统可以强制设备安装UES，以完成访问。如果已安装，UES将返回设备态势信息或安全评分。根据此类信息，系统将要求进行额外的认证，或者授予部分、完整访问权限或拒绝访问，并确定应当应用的相应安全措施。

阻碍

- UES有一个潜在缺点：整合后的系统总体而言并不是同类最佳解决方案；相反，它们在某一特定功能上属于同类最佳。只要这款统一产品的跨设备数据分析能力足够强大，UES就有可能成为保障所有端点安全的同类最佳解决方案。这将需要供应商同时了解传统客户端和移动安全，以建立独立的威胁检测框架，支持各种设备类型。
- 不是所有的企业都适合采用UES，短期而言更是如此。UES不适合拥有大量旧设备的企业，也不适合不打算对其远程访问进行现代化改造，而更喜欢借助传统的客户端管理而非UEM类方式来解决设备管理需求的企业。
- UES并不能解决不接受企业软件的非托管设备的条件性访问。

用户建议

- 采用UES策略，将所有的端点安全整合到单一控制台，降低支持成本，同时改善威胁预防、检测和事件响应机制。
- 评估现有的端点安全工具，以确定是否可将这些工具整合为单一UES解决方案，并与统一端点管理工具整合。
- 将UES与ZTNA/SASE结合起来，提供条件性访问控制。

供应商举例

BlackBerry; Broadcom (Symantec); Cybereason; Deep Instinct; McAfee; Microsoft; Sophos; Tanium; Tehtris

XDR

分析师： Peter Firstbrook

效益评级： 高

市场渗透率： 少于1%的目标受众

成熟度： 新兴

定义：

扩展检测和响应(XDR)是一种特定于供应商的威胁检测和事件响应工具，它将多个安全产品统一到一个安全运营系统中。其主要功能包括警报关联、事件响应和事件响应剧本自动化。

重要性

扩展检测和响应(XDR)在功能上类似于安全信息和事件管理(SIEM)以及安全编排、自动化和响应(SOAR)。但是，XDR与两者的最大区别在于其产品的集成和自动化程度、易用性以及对威胁检测和事件响应用例的关注。XDR解决方案供应商还必须直接提供多种安全控制，如EDR、CASB、防火墙、IAM、IDS等。

业务影响

XDR产品可以降低管理安全事件的总成本，提高事件响应团队的生产力，并降低组织的整体网络安全风险态势。

驱动因素

中型企业正在努力解决不同安全组件产生的警报。这些警报往往关联性较低，无法给出事件的全貌，相关企业也不能将其放入其他安全控制点的情境加以考虑。虽然现有的SIEM和SOAR工具可以提供类似的功能，但这些工具的成本、复杂性和持续维护是中端市场企业难以承受的。集成和维护同类最佳的安全工具组合所需人员和技能的相应代价非常高。XDR工具主要由拥有各类基础设施保护产品（EDR、CASB、SWG、SEG和NDR）的安全解决方案提供商销售。更高级的XDR工具通过集成身份、数据保护和应用程序访问，将重点放在堆栈上。

阻碍

只有一小部分供应商能够真正提供XDR产品。采用单个XDR方法可能导致过度依赖于单一供应商。在解决新威胁方面，能够提供XDR产品的大型供应商的执行速度通常比同类最佳的初创公司慢得多。所有的XDR工具都需要与其他供应商的安全产品进行一定程度的整合，然而大多数XDR产品的整合度仍然很低。安全产品的效果仍然是一个重要的因素，组合中的一些解决方案可能不如同类最佳的竞争产品有效。企业可能

会将XDR供应商提供的威胁情报和检测内容视作唯一来源。XDR工具降低了对知识渊博的操作员和全天候监控的需求，但并没有消除这种需求。请注意，XDR和SIEM产品之间的一个主要区别是，XDR不能满足事件响应之外的用例（如合规或运营）对长期日志存储的需求。

用户建议

- 与利益相关者一起确定XDR策略是否适合您的组织。
- 根据人员配置和生产力水平、IT联盟水平、风险容忍度和安全预算以及依赖单个供应商的容忍度和现有XDR组件工具的情况，来确定决策标准。
- 制定符合您的XDR战略的内部架构和采购策略，包括可能允许例外的时机和原因。
- 确保未来的安全采购和技术退役的规划与长期XDR架构策略保持一致。
- 寻求提供API的安全产品，以便与XDR进行信息共享并实现自动化。

在山之巅

安全服务边缘

分析师： Neil MacDonald、John Watts

效益评级： 高

市场渗透率： 1%至5%的目标受众

成熟度： 新兴

定义：

安全服务边缘(SSE)可保证对Web、云服务和私人应用的访问。其功能包括访问控制、威胁保护、数据安全、安全监控以及基于网络和API的集成所执行的可接受的使用控制。SSE主要以云端服务形式提供，可能包括本地或基于代理的组件。

重要性

云服务采用率日益增长推动了整个SASE市场的融合，而向远程工作的转变也起到了一定助推作用。SSE产品通过将多种不同的安全功能（如安全Web网关[SWG]；云访问安全代理[CASB]；零信任网络访问[ZTNA]；远程浏览器隔离[RBI]；以及防火墙即服务[FWaaS]）整合为单一供应商可提供的以云为中心的融合能力，降低复杂性并改善用户体验。

业务影响

更多企业正向远程工作转变并开始采用公共云服务，新冠肺炎疫情加速了这一趋势的发展。SSE允许组织使用以云为中心的方法来执行安全策略，为远程工作者提供支持。SSE可直接降低复杂性、成本和供应商数量。

驱动因素

- 用户、应用程序和企业数据可能位于各种位置。过去以数据中心为中心的安全架构/产品需要调整。SASE产品能满足这些必要的调整。
- 如果企业希望为用户和设备强化灵活的云端网络安全，而不借助他们选择的网络基础设施（例如，如果企业已部署SD-WAN），就会选择SSE。
- SSE往往具有更成熟的安全功能，与最近才在其产品中加入少量安全功能的一些SD-WAN供应商相比，对寻求更深入安全功能的买家更有吸引力。
- 基于身份和上下文的零信任、最少特权的访问是领先的SSE产品的核心能力。
- 通过整合供应商，企业可以减少管理复杂性、成本和用于定义安全策略的控制台的数量。这也有助于消除因覆盖范围差异或使用多种不同产品的不一致而产生的风险。
- 确保敏感数据检查和恶意软件检查在所有的访问渠道（SaaS、互联网和私人应用）中保持一致和同步，实现比分别单独进行更优越的性能。
- 企业通过在远程、分支机构或主办公室提供完全相同的安全体验来改善用户体验。

阻碍

- 一些组织希望从战略上整合并统一他们的安全访问战略，使用单一供应商提供的SD-WAN和SSE，而不是依赖两个独立的供应商。
- 大多数领先的SD-WAN供应商现在都有一套原生或通过合作伙伴提供的SSE服务，迫使SSE供应商增加基本的SD-WAN功能，以应对竞争压力。
- 由于各种能力的融合正在塑造市场，大多数供应商在单一类别中表现较好，而在其他类别中存在差距。此外，一些供应商还没有一套完整的SSE服务（例如，他们缺少FWaaS或其他安全服务）。
- 一些供应商在敏感数据识别和保护方面比较薄弱，而这种能力对于基于风险和上下文的访问决策至关重要。
- 以云为中心的SSE通常不能解决本地（如文件服务器）和端点DLP的需求。
- 并非所有供应商都会对所有服务的承诺实现性能SLA。

用户建议

- 整合供应商，并随着SWG、CASB和VPN合同的更新，削减复杂性和成本（用ZTNA方法取代）。充分利用通过整合这些服务而产生的融合市场。
- 列出设备和合同，以实施多年逐步淘汰本地边缘和分支机构的安全硬件的计划，助力云端SSE的交付。目标设定为理想情况下，将本地设备整合到一个单一的设备上。
- 积极推进分支机构转型、SD-WAN和多协议标签交换(MPLS)负载分流计划，以便将云端SSE纳入项目规划的范围。

供应商举例

Bitglass; Broadcom (Symantec); Forcepoint; iboss; McAfee; Menlo Security; Netskope; Palo Alto Networks; Versa; VMware; Zscaler

BYOPC安全

分析师: Rob Smith

效益评级: 具有变革性

市场渗透率: 20%至50%的目标受众

成熟度: 早期主流

定义:

自带PC(BYOPC)是一种端点部署策略，允许员工使用个人选择和购买的客户端设备来运行企业应用，访问公司服务和数据。它通常涵盖PC、Mac和Chromebook。由于用户设备存在非托管、未打补丁和受感染等情况，BYOPC可能伴随严重的潜在安全威胁。

重要性

- 鉴于实现居家工作的迫切需要和可用硬件的短缺，BYOPC在2020年开始被广泛采用，并继续带来新的重大安全风险。要支持BYOPC的需求，需要制定居家工作战略。此外，还需要提供支持BYOPC环境所需的安全工具。
- Gartner始终建议为用户提供可管理和安全的设备，而非BYOPC设备。但是由于全球环境的影响，BYOPC已经成为必要的策略。

业务影响

BYOPC伴随严重的安全风险，因为这些设备往往已感染恶意软件或勒索软件，并成为网络钓鱼攻击的潜在对象。因此，IT部门必须准备好限制和控制对任何BYOPC设备的访问。这意味着利用MFA、CASB、ZTNA、VDI和DaaS等关键安全技术来抵消PC硬件投资。如果不对这些技术进行投资，IT部门将面临勒索软件导致的更高潜在成本。

驱动因素

- 全球新冠肺炎病毒疫情使企业需要让员工用所拥有的各类设备迅速实现远程工作。
- 随着IT部门过渡到更加以云为先的环境，保护或管理PC的需求急剧下降，这也促进了向BYOPC的转变。
- 随着桌面即服务(DaaS)采用率的提升，IT部门正推行BYOPC，而不必提供设备。

阻碍

- BYOPC伴随巨大的安全风险，使企业易受到恶意软件或勒索软件的攻击。
- 由于设备种类繁多，BYOPC通常比托管设备需要更多的支持时间。
- BYOPC设备运行软件一般未安装最新补丁。
- BYOPC设备因用作家庭或共享设备，以前经常受到恶意软件或勒索软件入侵。

用户建议

- 假定任何BYOPC设备都安装有恶意软件或勒索软件，永远不应该被信任。
- 启用多因素身份验证(MFA)，用于对任何企业资源的所有访问。
- 包含所有应用数据。不允许在任何BYOPC设备上执行本地存储操作或上传本地数据，因为这可能感染系统。
- 对云应用执行各类访问时，使用云访问安全代理(CASB)或零信任网络访问(ZTNA)解决方案。
- 启用DaaS来复制员工的桌面，无需管理BYOPC。
- 虚拟化对任何传统的本地应用的访问。
- 在任何情况下都不允许从BYOPC访问VPN，因为这将造成严重的勒索软件感染风险。
- 为BYOPC制定相关政策，规定用户须遵守的最低标准，包括使用受支持且已更新补丁的操作系统、受支持且已更新的反恶意软件解决方案，以及完成网络安全知识培训。
- 自己熟悉其他家庭成员使用同一设备可能造成的风险。

供应商举例

Cisco; Citrix; Google; Microsoft; Okta; VMware

SASE

分析师: Joe Skorupa、Neil MacDonald

效益评级: 具有变革性

市场渗透率: 5%至20%的目标受众

成熟度: 未成熟

定义:

安全访问服务边缘(SASE)提供多种融合网络和安全即服务功能，例如SD-WAN、SWG、CASB、NGFW和零信任网络访问(ZTNA)。SASE为分支机构、远程员工和企业内部的一般互联网安全用例提供支持。SASE以服务的形式交付，基于设备或实体的身份实现零信任访问，并结合实时环境和安全及合规性策略。

重要性

SASE是现代数字业务转型的一个关键推动因素，转型内容包括远程工作的兴起，以及边缘计算和云交付应用的采用。该技术可提升可见性、敏捷性、弹性和安全性。SASE还极大地简化了关键网络和网络安全服务的交付和操作，主要是通过云交付的模式。在未来几年内，SASE可以将供应商所需的安全访问的数量从现在的四到六个减少到一到两个。

业务影响

SASE可实现以下优势:

- 新的数字业务用例（例如数字生态系统和移动员工支持环境）更加易于使用，同时通过供应商整合和专用电路负载分流来降低成本和复杂性
- 基础设施和运营以及安全团队能够以一致且集成的方式提供丰富的网络和网络安全服务，以支持数字业务转型、边缘计算和远程工作的需求

驱动因素

- SASE由企业数字化业务转型推动：分布式和移动式员工采用基于云的服务；边缘计算和业务连续性计划必须包括灵活、随时随地、安全的远程访问以及互联网和云服务的使用。
- 企业需要借助零信任安全架构，灵活地支持数字业务转型工作，同时保持复杂性可控，这是采用SASE的一个重要因素，主要作为一种基于云的服务交付。
- 对于IT部门来说，SASE可以减少新用户、地点、应用和设备的部署时间，并减少攻击面，将修复时间缩短最多95%。
- 基于数据中心边界安全的网络安全模式不适合解决现代数字企业及其分布式数字员工的动态需求。这将迫使传统的边界转变为一套基于云的融合功能（在企业需要的时候创建，以解决相应领域的需求），即动态创建的、基于策略的安全接入服务边缘，简称SASE。

阻碍

- **组织孤岛、现有投资和技能差距:** 完整SASE部署需要整个网络安全和网络团队采取协调一致的方法。
- **推动持续本地部署的组织偏见和监管要求:** 一些客户对云比较反感，希望自己有控制权。
- **全球覆盖。**SASE需要依赖云交付方式，而供应商的云足迹可能会阻碍该技术在某些地区的部署，如中国、俄罗斯和中东地区。这些地区的供应商的云端业务可能会受限。
- **SASE安全服务成熟度:** 在未来几年，SASE的功能将有很大不同。敏感数据的可见性和控制通常被视为高优先级的功能，但对大多数SASE供应商来说，这很难解决。您的首选供应商可能缺乏您所需要的功能，因此与两个供应商建立合作伙伴关系有时是可行的方法。

用户建议

- 在评估现有和新兴供应商的产品和路线图时，让CISO和网络架构师参与进来，以确保采取综合化方法。
- 利用WAN、防火墙、VPN刷新或SD-WAN来更新网络和网络安全架构。
- 努力确保所有核心服务的供应商不超过两家，以尽量减少复杂性，提高性能。
- 确定网络和安全所需的功能，包括延迟、吞吐量、地理覆盖范围和端点类型，以制定评估标准。
- 如果DLP是优先事项，请关注提供CASB的供应商。他们在这个领域有丰富经验。
- 单次部署中兼顾分支机构和远程访问，以确保策略一致，并尽量减少所需的供应商数量。部署ZTNA来增强或取代旧的VPN，以限制对旧技术的投资。
- 续签合同时，考虑合并供应商，以减少复杂性和成本。
- 利用分支机构转型和MPLS负载分流，为安全服务采用SASE。

供应商举例

Cato Networks; Fortinet; Palo Alto Networks; Versa Networks; VMware; Zscaler

BEC保护

分析师: Mark Harris

效益评级: 高

市场渗透率: 5%至20%的目标受众

成熟度: 早期主流

定义:

商业电子邮件诈骗(BEC)保护可检测和过滤恶意的电子邮件，这些邮件冒充业务伙伴实施欺诈，以达到骗取资金或数据的目的。

重要性

BEC消息通常不包含恶意链接或附件，而且经常从合法的邮件服务器发送，这使得它们很难辨认。攻击者往往通过公开的信息（如LinkedIn上的信息）获得充足信息，以提高攻击成功率。BEC攻击可能导致重大经济损失和声誉损害。

业务影响

BEC攻击会给所有行业造成巨大风险。2020年，这类攻击造成的损失在网络犯罪中的占比达到43%。这些攻击的技术水平通常相对较低，并主要针对重要人物，如应付账款团队成员或首席财务官。BEC攻击往往与电子邮件帐户接管攻击相结合。

虚假发票是最常见的BEC攻击方式。此类攻击会破坏信任关系，并造成经济损失。

驱动因素

BEC保护技术采用率之所以上升，是因为:

- 检测恶意附件或链接的传统技术对BEC攻击是无效的。
- 基于信誉的检测技术效果也相对较差，因为这些攻击往往来自具有良好信誉的合法电子邮件帐户。
- 向客户发送的伪造电子邮件很难被检测到，因为它们不涉及公司的电子邮件系统结构。
- BEC攻击可能会造成巨额损失，有时达到数百万美元。
- 所有的财务交易（包括更改工资单条目的请求）都可能面临攻击风险。
- BEC攻击最初往往很难察觉，往往只有目标收件人注意到付款未到账时，才发现欺诈。
- 遭破坏的电子邮件帐户使攻击者能够使用真实的电子邮件对话来转移资金。这些帐户接管攻击与合法电子邮件往来没有区别。

阻碍

- BEC保护不仅包括使用BEC解决方案，还包括(1)对组织内部员工和外部供应商（及其他相关人员）开展用户教育，以识别BEC攻击；(2)不再将电子邮件作为处理高风险金融交易的手段。向其他流程和程序转变或引入采购到支付的解决方案也会有所帮助。
- 即使是最有效的解决方案也不能确保100%有效，而且，随着攻击者使用的技术不断发展，专注于BEC的解决方案可能会无法防御当下使用的最新技术。
- 依靠云电子邮件供应商提供API的解决方案仅能实现这些API所提供的保护，并且仅受到Microsoft和Google对这些API的持续支持。
- BEC保护功能可能会在达到平稳期之前被纳入到广泛的电子邮件安全解决方案中。

用户建议

- 通过教育用户并使其了解BEC网络钓鱼技术，以及电子邮件在高风险交易中作为身份验证因素的局限性，从而增强用户意识，以推广电子邮件安全解决方案的使用。
- 执行标准操作流程，认证电子邮件的财务或数据交易，将高风险临时交易从电子邮件转移至认证级别更高的系统。
- 用先进的网络钓鱼保护来升级或辅助电子邮件安全解决方案，这些保护技术包括自然语言处理、自然语言理解、计算机视觉和基于机器学习的社交图形分析。
- 执行基于域的消息认证、报告和一致性(DMARC)，认证电子邮件域名，减少域名滥用。
- 针对电子邮件执行多因素身份验证，免受帐户接管侵害。

供应商举例

Abnormal; Armorblox; Mimecast; Proofpoint

陷入底谷

针对一线员工的设备端点安全

分析师: Patrick Hevesi

效益评级: 中

市场渗透率: 5%至20%的目标受众

成熟度: 早期主流

定义:

针对一线工人的设备端点安全包括一套技术，可为特制的设备及其用户提供保护。根据不同的行业和用例，设备可能需要被真实固定在特定位置上，在一个班次中接受追踪和使用前检查，或者可能在一个特定区域被多个用户使用。

重要性

一线工人主要使用完全托管的专用移动设备工作，这类设备专为岗位定制，已进行加固和锁定。这些设备的价格很高，而且很难进行更新和安装补丁以维持其安全性。这导致一些组织和供应商探索能保护移动应用的个人设备。然而，与完全托管的设备相比，这类设备可提供较少的控制，并可能使组织面临生产力损失、数据泄漏或其他恶意攻击风险。

业务影响

在许多情况下，一线设备不在内部，而是由客户、承包商、临时员工和雇员处理。一线场景涉及对敏感和关键系统的访问，这提高了风险，更需要预防措施，可能需要结合各种解决方案来缓解所有可能的安全风险。一些解决方案专为传统的移动管理场景而非一线工人而构建，可能需要定制开发才能满足安全要求。

驱动因素

- 更多公司开始让一线工人能够使用云SaaS应用，这会让组织和工人面临额外的云安全风险。
- 数据泄露或其他恶意攻击的风险已导致安全团队重新评估其一线端点安全战略和架构。
- 与BYOD趋势相一致，企业放开使用个人设备的限制，进而推动对围绕移动应用管理(MAM)和移动威胁防御的新解决方案的需求，刺激应用级容器解决方案的部署。

阻碍

- 如要在安全方面覆盖所有层面，往往需要根据包含专门硬件和额外云功能的多种用例增加多个层次。这可能为组织带来没有考虑到的额外费用。
- 针对一线工人的端点安全需要包含物理安全解决方案，例如摄像头、签入/签出流程、用户和设备身份管理、每次使用后需要清除数据的基于班次的设备，以及地理/位置类型的保护。这些要求进一步提升了为一线工人部署设备端点安全解决方案的成本和难度。

用户建议

对于需要专业解决方案的托管设备:

- 利用专用的专业解决方案。
- 借助EPP、UEM或MAM全面管理和锁定设备。
- 确保操作系统已应用安全设置、更新和补丁。
- 确保物理安全有保障（例如，信息亭的电缆、移动设备的地理围栏/地理定位、多用户设备的签入/签出流程）。

对于允许运行LOB和其他协作应用的非托管设备:

- 使用UEM工具来应用MAM策略，在工人应用上增加层或加密措施、MFA和基于时间的锁定机制。
- 评估MTD供应商的基于设备的风险认证，应用由MAM管理。

对于定制工人应用:

- 确保LOB应用的设计符合安全设计原则和定制的多用户身份验证。
- 使用应用屏蔽、应用包装和应用内MTD（或笼统意义上的"应用内保护"）来保护在设备上运行的二进制文件和应用中的知识产权。

对于云端的应用:

- 使用CASB实现威胁和数据保护。
- 当一线用户和设备使用外部SaaS服务时，允许他们使用自适应的访问控制。

供应商举例

CommuniTake Technologies; Imprivata (GroundControl); Lookout; Microsoft; Samsung Electronics; SOTI; Symantec; Veracode; Zebra Technologies; Zimperium

桌面即服务

分析师: Stuart Downes、Mark Margevicius、Tony Harvey

效益评级: 高

市场渗透率: 20%至50%的目标受众

成熟度: 早期主流

定义:

桌面即服务(DaaS)解决方案可完全通过远程托管的位置(如公共云),为工人提供虚拟化的桌面体验。DaaS消除了企业购买与桌面虚拟化相关的物理基础设施的需要,采用基于订阅和用量的支付结构。DaaS包括管理平面和资源的配置、修补和维护,以承载工作负载。

重要性

DaaS利用网络连接提供对应用和桌面的安全远程访问。任何数据都不会驻留在端点上,这种方式可为远程工作者提高解决方案的安全性、冗余度、爆发量和性能。DaaS提供可扩展的服务,允许客户按小时、按天、按月适当地选择合适的环境大小和使用量;然而,并非所有的服务都有如此精细的计费选项。

业务影响

全球疫情凸显了向任何地点的用户提供安全的桌面和应用体验的需求:

- 客户采用DaaS来保证居家工作的体验后,2020年的收入比2019年增长了98%。

DaaS为居家工作和混合工作模式实现了业务的连续性和地点灵活性。

DaaS增强了BYOPC用例的安全性,降低了企业的风险。

驱动因素

- 提高安全性和合规性,集中管理数据,尽量减少数据在笔记本电脑上的暴露情况。
- 支持远程工作,数据不会在端点上驻留。
- 允许任何设备型号的端点计算模式和自带PC(BYOPC)端点。
- 简化了在云端进行的最终用户计算操作,这一点在高度分散的员工队伍中尤其明显。
- 业务连续性,这是2020年DaaS增长的主要驱动因素。
- 按需台式机。
- 允许扩展云资源的财务模型和运营支出模型。
- 扩大规模以满足季节性工人等短期雇员的需求。
- 安全地将服务扩展到涵盖外部承包商,包括IT开发人员和业务流程外包(BPO)。
- 遇到兼并、收购和资产剥离情况时,能够实现对系统的快速访问。
- 丰富的图形用例(如工程、游戏开发、时尚和地理信息系统[GIS])均受益于支持GPU的工作站类虚拟桌面和应用。
- 在设备供应或高损耗率用例中,物理设备的提供面临困难。
- 消除了部署复杂的虚拟桌面基础设施(VDI)的需要。
- 使得业务扩展到新的地区,无需部署数据中心。

阻碍

- 成本:在许多情况下,直接的基础设施成本比较显示,与VDI或桌面PC相比,DaaS的IT成本较高,通常只有在包括业务和用户成本时,相应商业用例的成本才不会过高。
- DaaS中的多媒体流、网络会议和视频通话性能与物理端点的性能不等同。
- 存储在本地数据中心的应用和数据存在或被认为存在与网络相关的性能问题(当桌面或应用托管在云端时)。
- 一些DaaS解决方案需要复杂的配置,虽然比VDI简单,但在某些情况下可能需要仔细配置并选择适当的存储服务,以确保更好的DaaS体验。

用户建议

DaaS将继续发展成熟,2025年之前其采用率会继续上升。DaaS还没有走过泡沫化的底谷期,进入稳步爬升的光明期。客户应当:

- 了解DaaS的三个细分市场,并从适当的细分市场中选择一个供应商:(1)客户定义的DaaS:客户配置他们的DaaS体验并管理他们的工作负载。这比VDI需要的技能更少;*2)供应商定义的DaaS:供应商配置DaaS体验,客户管理相应工作负载;(3)托管式DaaS:供应商配置DaaS体验,供应商管理相应工作负载。
- 选择服务最符合您的要求的DaaS供应商;即使在每个细分市场中,供应商提供的服务也有差异。
- 优化多媒体流、网络会议和视频通话。
- 选择能提供您所需要的计费细粒度的DaaS供应商;有些供应商是按小时计费,有些是按天或按月计费。

供应商举例

Amazon Web Services; Citrix; Evolve IP; Microsoft; SACA; SimpleCloud; VMware; Workspot

远程浏览器隔离

分析师: Neil MacDonald、John Watts

效益评级: 高

市场渗透率: 5%至20%的目标受众

成熟度: 未成熟

定义:

远程浏览器隔离(RBI)将处理不受信任内容（通常来自互联网）的过程与用户及其设备分开，或将敏感的应用和数据与不受信任的设备分开。当用于保护不受信任的内容时，RBI可大大减少组织的攻击面，因为大量的攻击已经转移给用户和端点。当用于保护敏感数据和应用，防范不受信任设备的影响时，RBI有助于在使用BYOD时降低风险。

重要性

SWG确实有效，但有时仍难抵御攻击。浏览器隔离策略不会让互联网上的潜在恶意内容通过网络浏览器在端点上执行，而会将会话隔离（类似于VDI，但主要针对浏览器会话）。RBI还可以反向发挥作用，在通过CASB进行SaaS访问或通过ZTNA进行内部应用访问等用例中，保护敏感数据和应用，防范非托管和潜在受感染设备的攻击。

业务影响

大多数攻击是借由公共互联网实施的，攻击者会诱使用户通过网页浏览或电子邮件链接访问恶意网站。简单地从最终用户的桌面上删除浏览器（或更慎重一些，将其隔离起来）便可大大改善企业的安全态势，还可以防御勒索软件攻击。RBI保护还可以扩展到涵盖内部私人应用和来自非托管设备的SaaS应用，从而降低数据泄露的风险。

驱动因素

- 以URL黑名单形式出现的不良网站的静态签名可能无法阻止攻击，而且无法及时响应定向攻击。
- 屏蔽未分类的网站会损害最终用户的体验。
- 新冠肺炎病毒疫情促进了向远程工作的转变，提升了非托管设备的使用率。RBI提供了为非托管设备引入敏感数据保护等功能的控制点的方法，而CASB和ZTNA产品目前便在利用RBI来实现这一目的。
- 在外部解析的电子邮件中的URL经常被用于对员工进行网络钓鱼攻击。隔离这些URL可以减少网络钓鱼攻击。
- SASE集成了一套来自云端的访问功能，涵盖SWG、CASB和ZTNA。RBI在所有这些SASE用例中增加了价值，并正在成为这些产品的共有功能。
- 如果唯一要隔离的应用是浏览器，那么RBI比使用VDI进行隔离更便宜。

阻碍

- 用户体验是提升采用率的唯一严重障碍。将Chromium作为渲染引擎的标准化有助于解决大多数问题；然而，人们仍然对延迟和带宽对用户体验的影响表示担心。
- 浏览体验的本地化要求IP地址的分配与VPN出口点或本地POP进行区域性的结合。
- RBI的成本可能会很高昂。如果RBI是以云端服务的形式提供，就必须有人承担远程渲染所需的CPU和带宽成本。
- 大多数RBI产品是基于软件的，通过云端交付。有些公司会倾向于自己运行RBI解决方案。此外，基于硬件的RBI方法比基于软件的方法具有更强隔离效果，一些国防和情报场景可能会因此受益。

用户建议

- 为特定的高风险用户（如财务团队）或用例（如呈现基于电子邮件的URL）评估和试行浏览器隔离解决方案，特别是如果您所在组织希望规避风险时。
- 向您的SWG、CASB、ZTNA和/或SEG供应商施压，要求他们提供RBI作为可选的深度防御保护选项。
- 对于威胁保护，先让有限数量的高价值目标用户试用，选择性地隔离有限数量的URL，然后扩大用例。
- 根据性能和带宽评估不同供应商的呈现方法。
- 根据性能、延迟和带宽要求，评估不同供应商的呈现方法（例如，像素流、基于矢量）。
- 设计和部署将内容从公共互联网移入企业系统的功能，但必须先使用多层威胁检测技术进行密集扫描。
- 仅签署1年到2年的合同；市场在不断变化，价格可能会迫于压力下降。

供应商举例

Authentic8; Cloudflare; Ericom; Forcepoint (Cyberinc); Garrison; McAfee; Menlo Security; Proofpoint; Symantec (Broadcom); Zscaler

移动威胁防御

分析师: Dionisio Zumerle

效益评级: 中

市场渗透率: 5%至20%的目标受众

成熟度: 未成熟

定义:

移动威胁防御(MTD)可保护企业，防范针对iOS和Android移动设备的威胁。它提供针对设备、其网络连接和所安装应用的预防、检测和修复功能。为了防止和检测企业威胁（如恶意软件），MTD产品使用了各种技术，包括机器学习和行为分析。产品来自各种供应商，包括端点保护平台(EPP)供应商和独立MTD供应商。

重要性

MTD可保护移动设备，防范恶意威胁。通过识别易受攻击的设备、恶意应用和网络，MTD可改善移动安全状况，而且还提供可与其他端点或企业数据相关联的数据的可见性，以提高检测和响应能力。MTD可以对抗移动网络钓鱼攻击等诸多威胁。金融服务和其他高安全性且受监管的行业是这项技术的主要采用者。

业务影响

负责移动安全的IT领导者可以利用MTD来应对移动威胁。MTD可以与现有的UEM部署进行以威胁为重点的整合，也可以作为独立工具。

MTD可以为以下类型的组织提供安全保障：受监管行业；需要使用各种不同和分散的移动操作系统版本的企业；以及为移动设备提供企业访问，但选择不管理的组织。

驱动因素

- 从MTD中获得价值的企业是通过使用主动措施（如应用审查和设备漏洞管理）保障安全状况的，并没有借助检测和对抗高级攻击的能力。
- 新出现的用例假设MTD为零信任网络访问(ZTNA)架构的组成部分，以及用于检测和响应的扩展检测和响应(XDR)系统的组成部分（用户可以将XDR统一端点安全的试用环境）。在将MTD用于移动网络钓鱼保护时，上述方法可充当附加保护机制。
- EPP供应商正在进军这一领域，将其EPP产品的支持扩展到涵盖iOS和Android。

阻碍

- 经过一段时间的积极创新，MTD产品已经趋于成熟。然而，移动恶意软件仍是行业积极研究的领域。MTD产品已足够成熟，可供企业采用，还没有达到完全成熟的程度。
- MTD的采用速度比移动安全炒作所宣称的要慢。没有证据表明移动安全问题导致了重大的企业违规事件，这并没有使MTD成为企业的优先事项。
- 受监管行业和有高安全性要求的企业采用了MTD解决方案。在主流企业中，MTD产品的采用在很大程度上局限于那些希望改善其整体安全状况或为自携电子设备(BYOD)提供设备态势信息的企业，而不是那些旨在应对恶意移动威胁的企业。

用户建议

- 在高安全性和受监管的部门，以及拥有大型或分散的Android设备机群的组织中，优先采用MTD。
- 在投资MTD产品之前，为移动设备建立安全基线，并利用这些产品的应用审核和设备漏洞管理功能来展现即时的好处，而不是期望它们能对抗高级恶意威胁或发现重大漏洞。
- 将MTD与现有统一端点管理(UEM)工具进行整合。优先采用基于应用的选项，而将基于代理的部署用于"仅限企业自身业务"(COBO)场景。
- 使用MTD产品来保护实施BYOD政策的企业基础设施，并将之用于设备必须保持不受管理的其他用例。强调供应商的战略配合优先于产品的差异化，除非是在高安全性的背景下和有特殊移动安全需求的情况下。

供应商举例

BETTER; BlackBerry; Lookout; Microsoft; Samoby; Sophos; Symantec; Wandera; Zimperium

稳步爬升

ZTNA

分析师: John Watts、Lawrence Orans、Neil MacDonald

效益评级: 中

市场渗透率: 5%至20%的目标受众

成熟度: 未成熟

定义:

零信任网络访问(ZTNA)会在应用周围创建一个基于身份和上下文的逻辑访问边界。应用程序不会被发现，并且通过信任代理将访问权限限制为一组命名实体。代理验证指定参与者和设备的身份、上下文和策略遵守情况，然后才会允许访问，并禁止网络中的横向移动。这样，将应用从公众的视线中移除，大大减少了攻击面范围。

重要性

ZTNA是一项关键技术，用于通过信任代理实现用户到应用的分割，以执行安全政策，允许组织隐藏私人应用和服务，并为应用执行最小权限的访问模式。它综合了云安全联盟的软件定义边界(SDP)指南、Google的BeyondCorp愿景和O'Reilly的书籍《零信任网络》(Zero Trust Networks)中的概念。

业务影响

ZTNA可通过保护服务、抵御攻击而产生直接效益。与基本的VPN产品相比，ZTNA移除了完整网络访问，提高了用户体验、灵活性和可适应性。它通过简化的策略管理实现了更细化的用户到应用的分割。基于云的ZTNA产品会提高可扩展性和易用性。市场上的早期产品专注于Web应用，但现在已经扩展到与更广泛的应用和协议合作。

驱动因素

- 企业需要支持不适合传统访问方式的数字业务转型场景，如访问位于企业外部的应用、服务和数据。
- 2020年，随着新冠肺炎病毒疫情的爆发，人们突然转变为远程工作，传统的本地VPN基础设施变得紧张，因此需要灵活地快速扩展能力。
- 企业内部零信任倡议的兴起，导致本地和云端应用需要更精确的访问和会话控制。
- 希望对供应商进行整合，移除单点解决方案，采用更多具有SASE框架的供应商的产品，从而使ZTNA添加到现有的SWG或CASB服务中。
- 企业需要在不通过VPN暴露网络的前提下，将第三方（如供应商、供货商和承包商）安全地连接到应用，或将应用连接到互联网以进行访问。
- 企业具备将应用访问扩展到被收购公司的能力，可实现兼并和收购，而不需要在两家公司之间直接部署端点或连接网络。

阻碍

- 成本：通常需要每年向每个命名用户授予许可，其费用可能高于传统VPN。
- 有限支持：不是所有产品都支持所有应用。例如，有些只支持Web、RDP和SSH协议。
- 代理或无代理的ZTNA：一些供应商只提供一种方式来使用ZTNA。这限制了适用的用例。
- 身份管理不力：在云端没有联合身份支持的组织发现用例具有局限性，因为许多供应商依靠第三方身份供应商进行用户认证。
- 缺少本地信任代理：基于云的信任代理在远程访问方面运作良好，但要在本地扩展同样的政策，可能不是首选。虽然存在同时拥有云端和本地信任代理人的供应商，但这些供应商很少。
- 对用户可接受的应用访问权限了解有限：组织必须预先绘制正确的应用访问图，以获得ZTNA的全部好处。

用户建议

- 开放应用和服务，不需要使用VPN或DMZ。
- 使企业网络内外的应用访问的用户体验标准化。
- 为员工和IT承包商部署特定于应用的访问，以替代基于VPN的访问。
- 在兼并前扩展对系统的访问，而无需配置站点到站点VPN和防火墙规则。
- 通过减少全面自携电子设备(BYOD)管理要求并启用更安全的直接应用访问，允许在个人设备上访问。
- 恶意网络上的隐蔽系统，如暴露在互联网上的协作系统。
- 允许世界上潜在危险地区的用户与应用和数据进行交互，以减少或消除风险。
- 如果设备能支持轻量级SDP代理或物联网(IoT)网段上用于连接的虚拟设备连接器，则应确保能创建IoT设备的安全飞地。

供应商举例

Akamai; Appgate; Cato Networks; Ivanti; Netskope; Perimeter 81; Proofpoint; SAIFE; Zscaler

数据净化

分析师: Rob Schafer、Christopher Dixon

效益评级: 中

市场渗透率: 超过50%的目标受众

成熟度: 成熟主流

定义:

数据净化是一个有规律的过程，即专门、永久且不可逆地删除或破坏存储在内存设备上的数据，使其无法恢复。经净化的设备没有留存的可用数据，即使有先进的取证工具的帮助，数据也永远无法恢复。

重要性

用户越来越关注数据隐私和安全、泄漏、法规遵从，存储介质容量以及边缘计算和物联网设备的量级不断增长，使得强大、一致和广泛适用的数据净化成为所有IT组织的C级要求。切记：只要有一个携带数据的设备从本来很健全的程序中泄露，您就可能发现自己的数据在互联网上遭到售卖。

业务影响

虽然数据净化不一定能够增加收入或节约成本，但它将最大限度地降低严重的ITAD相关数据泄露可能导致的重大资金和品牌损失的风险。相应效益评级为中等，因为数据净化正得到越来越多的企业的认可，可作为最大限度降低数据安全所面临的重大商业风险的流程。

驱动因素

- 无论卸载的IT硬件的目标最终状态如何，数据净化或实际的硬盘销毁/粉碎都是确保符合内部和外部隐私和安全要求的关键活动。通常情况下，由经验丰富的ITAD供应商使用这一过程所需的软件和设备，可以确保效率最大化。鉴于不健全的数据净化过程可能使您的品牌面临的关键风险，您应该要求证明数据是按照通用的行业标准进行净化的。

- 利用国际标准，如（美国国家标准技术局第800-88号条款）或英国的资产处置和信息安全联盟(ADISA)标准。您的ITAD服务提供商还应提供国际信息销毁协会(NAID)的AAA认证（不仅仅是会员资格）。为了最大限度减少监管链的安全风险（如在转移到ITAD供应商设施的过程中的损失），许多ITAD经理（特别是在金融和医疗部门）要求在现场进行某种形式的数据净化。不要求现场数据净化的组织应至少对所有携带数据的设备实施数据加密，以尽量减少监管链的安全风险。

- 对所有带有存储组件的设备（例如，企业存储空间和服务器、PC、移动设备，以及日益增多的边缘计算设备和一些物联网设备）应用全面的数据净化。缺乏强大的数据净化能力往往是由于将资产生命周期阶段作为孤立的事件来处理，业务部门（如财务、安全、采购和IT）之间缺乏协调。

- 对于移动设备，通常通过移动设备管理器(MDM)实现远程数据擦除功能。虽然这不应该视为万无一失的机制，但其可靠性应足以应对大多数移动设备丢失或被盗的情形。

阻碍

- **自满:** "一切照旧"综合症："我们一直是这样做的，从来没有出现过问题。"数据安全要求迅速增加（例如，GDPR、HIPAA和美国《加利福尼亚州消费者隐私法案》[CCPA]），随之而来的是对数据安全和净化流程进行（年度）审查的要求。

- **成本:** 与许多成本较低的"相信我"备选方案（例如，承诺他的流程很可靠的"朋友"）相比，强有力的数据净化成本很高。切记：这关乎您的品牌在市场上的完整性。

- **缺乏执行意识:** 很多时候，C级高管层自信满满地表示他们拥有卓越的数据净化流程，但几年来却没有对这些流程进行彻底的审查/审计。大型组织很可能制定了严格的数据净化流程，但在某些偏远地区，这些流程的落实很难确保一致性。

用户建议

- 遵循IT风险管理生命周期的方法，涵盖关于数据归档、净化、设备再利用和报废的明确决定。

- 与数据净化的利益相关方（例如，IT、安全、隐私、合规、法律、IT资产经理）合作，制定恰当的数据净化标准和流程，根据数据敏感性，为端到端销毁流程提供具体指导。

- 由于不同的媒介需要不同的净化方法，应确保内部IT组织或外部IT资产处置(ITAD)供应商提供根据您的安全标准（如NIST 800-88r1）进行净化的数据销毁证书。

- 了解并尽量减少便携式存储设备（如USB驱动器、IoT设备）的安全风险。

- 对于外部提供的服务（如SaaS、IaaS、PaaS），了解合同终止的影响和数据出境流程，并向供应商询问他们的数据销毁、存储空间再利用和回收做法。

供应商举例

Blancco; ITRenew; WhiteCanyon Software

UEM

分析师: Dan Wilson、Chris Silva

效益评级: 高

市场渗透率: 20%至50%的目标受众

成熟度: 早期主流

定义:

统一端点管理(UEM)工具以员工为中心，通过运行Windows 10、Google Android和Chrome OS、Apple macOS、iPadOS和iOS的端点设备，提供基于代理和无代理的计算机和移动设备管理。UEM工具使用来自身份、应用、连接和设备的遥测数据，应用数据保护、设备配置和使用策略。这些工具还可与身份、安全和远程访问工具集成，以支持零信任。

重要性

UEM通过整合不同的工具以及简化跨设备和操作系统的流程来简化端点管理。UEM不仅提供管理功能，还提供与身份、安全和远程访问工具的深度集成，以支持零信任安全模式，使任何地方的员工都能得到支持。领先的UEM工具还使用分析和机器学习来实现情报驱动型体验自动化(IDEA)，以减少IT开销并改善员工体验。

业务影响

通过采用UEM，I&O领导者可以简化操作，改善端点管理。具体影响包括:

- 端点管理和修补不受地点限制，可为远程员工提供支持。
- 通过简化设备管理和支持流程，降低管理端点设备的总拥有成本(TCO)。
- 通过支持更多的设备类型和操作系统，实施更好的策略管理，并集成身份、安全和远程访问工具，降低了安全风险。

驱动因素

- 远程员工需要功能超越单个平台的工具，或者设备连接特定网络才能发挥作用的工具。
- IT部门希望简化和精简端点部署、管理和修补，以便为远程员工配置新设备，提高设备性能和可靠性，让员工了解整个端点生态，以降低安全风险。
- 对员工体验的日益重视要求员工能更加了解端点的性能、可靠性和一致性，这一点得到了新的UEM工具分析和自动化功能的支持。

阻碍

随着工具的成熟，对UEM的采用造成障碍的因素在不断减少，包括:

- 传统的组织模式中，移动和PC管理、远程访问和安全的责任由多个IT团队分担。
- IT部门在现代端点管理方面的技能组合存在差距，或花费过多精力维护高度定制和控制的设备配置。
- 对于目前没有使用移动设备或客户端管理工具的组织来说，成本可能是一个问题。
- 拥有数以千计的组策略对象(GPO)，但对每个对象的作用知之甚少的组织将竭力弄清相互关系，以便迁移到配置服务提供商(CSP)文件。
- 具有多个活动目录林或域、网络分段和/或自治子公司或业务部门的高度复杂环境也会与云原生UEM工具的集中化性质相冲突。

用户建议

随着UEM工具的成熟和采用率的提高，成熟度曲线已经超越了底谷期，走向了稳步爬升的光明期。一些企业仍在努力进行人力变革管理，以便调整流程并将IT人员的注意力重新集中到简化和现代化的端点管理上。

Gartner建议您:

- 利用疫情带来的势头，尽力让远程员工取代不同的MDM和CMT工具，并统一使用UEM，接受Windows 10和MacOS的现代操作系统管理。
- 审查IT政策和程序，以确定并消除对MDM、CMT或地点专用技术的不必要的参考或依赖。这将有助于避免常见的惰性、限制和以某事为借口违反政策的情况。
- 提高IT工程师和支持人员的技能或进行更换此类人员，以增加UEM、现代管理和自动化功能的使用。

安全Web网关

分析师: Lawrence Orans、John Watts

效益评级: 高

市场渗透率: 超过50%的目标受众

成熟度: 成熟主流

定义:

安全网络网关(SWG)利用URL过滤、高级威胁防御(ATD)和恶意软件检测来保护组织，确保相关互联网政策得到遵守。SWG可以作为基于云的服务、混合（云端和本地）解决方案或仅作为本地解决方案提供。

重要性

SWG介于用户和互联网之间，可为用户提供有效的保护，避免互联网产生的恶意软件的侵扰。同时，SWG的仪表板和报告工具也可用于了解用户在互联网上的行为。这一功能对于检测和调查员工是否违反了组织的互联网使用政策非常重要。

业务影响

安全Web网关提供了一个额外的保护层，可防止破坏性的攻击，使用户能更安全和更有效地使用基于云的服务。云交付的SWG还可以通过使用商品互联网访问（而不是通过MPLS链接将网络流量回传到集中式数据中心）和取消分支机构的防火墙，减少分支机构的网络成本。云端SWG服务还可以为不在企业网络中的移动用户提供保护。

驱动因素

- SaaS和远程工作的快速采用正在推动企业从本地基于设备的SWG迁移到云交付的SWG服务。
- 在SaaS时代，将所有流量从远程办公室回传到集中式数据中心的传统广域网架构已经过时了，因为防火墙和其他物理安全设备的位置是固定的。
- 现在，企业希望将流量直接从远程办公室发送到SaaS应用和互联网上的其他目的地。
- 新的广域网架构（直达互联网）需要基于云的安全堆栈（SWG是基础），该堆栈介于用户和互联网之间。
- 随着企业购买越来越多的基于云的安全服务，他们也越来越希望整合安全供应商。
- 从运营层面来说，管理多个云安全服务任务艰巨。例如，如果您有三个云安全服务，每个都可能需要自己的端点代理和自己的网络通道，以将流量从笔记本电脑引导到云服务。
- 订阅提供多种安全服务的单一云安全服务则更加便利（最常见的服务是SWG、云访问安全代理[CASB]和零信任网络访问[ZTNA]）。
- 其他安全服务包括防火墙即服务（对所有端口和协议应用政策）、数据丢失防护、沙盒和远程浏览器隔离。
- SWG供应商和CASB供应商正在蚕食对方的地盘，并增加额外的安全服务以应对供应商整合的威胁。

阻碍

- 提供低成本的基本URL过滤（而非完整SWG功能）的防火墙供应商通常与SWG供应商属于竞争关系。
- 基于云的递归DNS解决方案也已成为中端市场客户的常用解决方案，因为此类方案可提供经济有效的安全保护。
- 一些DNS服务使用选择性代理，他们代理以可疑网站为目的地的流量（一般而言，约10-15%的流量是代理的）。
- 由于DNS服务不会始终代理所有的流量，因此与使用完全代理模式的服务相比，它们提供的安全保护较差。
- 一些厌恶云服务的垂直行业一直抵制将本地SWG迁移到云端。金融服务和医疗保健垂直领域尤其如此。
- 中东地区在将本地代理迁移到云端方面一直进展缓慢。

用户建议

- 重新审视SWG市场，而不是自动更新传统方法。
- 寻求关键功能（如专门构建云解决方案、沙盒等高级威胁保护和CASB服务），以控制和监测对SaaS和数据中心应用的访问。
- 用基于云的出站防火墙服务取代分支机构防火墙。
- 考察ZTNA功能（主要部署为传统虚拟专用网络[VPN]的替代方案），因为它可以作为领先的SWG供应商的一项功能。

供应商举例

Cisco; ContentKeeper; Forcepoint; iboss; McAfee; Menlo Security; Netskope; Sangfor Technologies; Symantec (Broadcom); Zscaler

端点检测和响应

分析师： Paul Webber、Jon Amato

效益评级： 高

市场渗透率： 20%至50%的目标受众

成熟度： 成熟主流

定义：

EDR解决方案可以检测和调查安全事件，遏制攻击并生成修补指导。这些方案必须分析用户、流程和系统活动以及设备配置。用户和设备数据的报告与对检测到的事件的直接干预相结合。对威胁的自动响应和回滚是理想功能，与其他工具的集成和自动化非常关键。云托管占主导地位；一些供应商可以为本地托管非互联网连接的系统。

重要性

所有暴露在互联网上的系统或连接到内部网络的系统都可能遭受攻击，这些攻击往往针对易受攻击或未受保护的系统。EDR是整体防御的一个重要组成部分。应将EDR部署到所有托管系统中，以便识别异常或恶意活动，揭示高级攻击的战术和技术，并提供应对这些攻击的手段。

业务影响

- EDR是所有行业领域必备的保护层，应适用于所有连接到网络或处理企业数据的设备和服务器。
- 早期检测和快速响应现在至关重要，因为仅靠预防处理现代威胁和漏洞不太可行。
- EDR通常被规定为内部和外部政策中的强制性安全控制。
- 当其他层未能阻止漏洞被攻击时，EDR可提供最后的防御手段。

驱动因素

- 威胁的性质已发生变化。实现100%的预防和保护已不现实，旧的EPP工具应进行更新，以实现EDR功能。从近期供应链所遭受的攻击可以看出，隐蔽的和国家操纵的攻击会使用先进的技术防止被发现并绕过安全控制。
- 远程工作加速了对云托管产品的采用，现在此类产品占安装总数的60%，在所有新部署中占比95%。
- 无文件攻击现在是所有恶意软件类型的常见情况，使EDR工具的行为保护成为打击高级威胁和日益强大的人工操作勒索软件活动的关键能力。
- 针对某组织的高级攻击者已经证明他们可以禁用保护解决方案，这使得使防篡改保护成为关键设施。用户还需要全面的警报和遥测，以促进早期检测和快速响应。
- 由于威胁可能针对任何系统，EDR现在应该是整个分层端点安全控制中的一项必备关键能力，需要部署到所有托管端点和服务器上。
- 在事件发生时迅速做出实时响应的能力对于遏制威胁并阻止其蔓延至关重要。
- 加强现有的漏洞管理计划并提供减少攻击面的手段的重要性日益凸显，其目的是确保系统不会错误配置，没有未修补的漏洞。
- 从EDR代理收集的日志和事件也可用于回顾性威胁检测和威胁搜寻。
- EDR工具通常会附加管理相邻风险的能力，如存储介质的加密，以及应用和互联网活动的控制。
- 高级威胁、人工操作的勒索软件和国家操纵的攻击越来越隐蔽，组织需要一种新的安全工具，在应对复杂攻击时让所有控制领域全面合作。

阻碍

- 添加检测和响应功能现在是公认的主流趋势，尽管许多组织仍然缺乏利用这些功能的技巧。
- EDR的采用必须伴随着对培训响应者的投资，包括模拟真实攻击的"范围"培训。
- 技术熟练人员较少的组织应选择提供监测、警报且经常对警报进行分类的托管检测和响应服务。
- 基于定义的早期代理需要频繁的更新，并使用大量的系统资源，导致用户对端点代理的不信任。
- 云托管的工作负载往往有截然不同的"敏捷"部署管道，无法使用传统的端点安全工具。这通常会导致为敏捷部署的工作负载使用不同工具的不一致环境。
- 对于非Windows系统来说，功能对等性无法得到保证。因此，这些系统的端点安全解决方案缺乏完整的EDR检测和响应设施。

用户建议

- 识别可以远程部署和仅需少量维护的单个轻量级代理。
- 优先选择可更快提供价值的云托管EDR解决方案，以及能提供自动化流程的供应商。
- 以本身提供托管服务（如警报、监控、事件响应以及托管检测和响应）的供应商为主要选择对象。
- 优先选择那些能够消除漏洞并使端点免受攻击的供应商。这类供应商应该提供对端点的直接访问，以快速响应问题。
- 寻找能够重新使用现有投资（如ITSM、认证和威胁情报）的第三方集成。
- 指定具有防篡改功能的工具，确保代理不会被攻击者禁用。
- 确保数据得到充分保留，使用归档以获得更经济的存储，并将事件和警报发送到其他安全工具以获得更长时间的留存。
- 设法用其他安全遥测来源和工具之间的集成（如XDR系统所提供的功能）来增强解决方案。

供应商举例

Bitdefender; Cisco; CrowdStrike; Cybereason; FireEye; Microsoft; Palo Alto Networks; SentinelOne; Trend Micro; VMware Carbon Black

CASBs

分析师: Craig Lawson、Neil MacDonald

效益评级: 具有变革性

市场渗透率: 20%至50%的目标受众

成熟度: 成熟主流

定义:

云访问安全代理(CASB)通过将适用于SaaS、IaaS和PaaS的多种类型的安全策略执行整合到一个位置，为可见性、合规性、数据安全和威胁保护提供关键的云治理控制。这些控制包括授权、UEBA、动态访问控制、DLP、设备分析、对象加密、标记化、日志、警报和恶意软件清除。大多数CASB部署在云端；在本地部署的情况很少。

重要性

CASB对于企业为业务关键型云服务的使用提供保障至关重要。四个关键领域（可见性、合规性、数据安全和威胁保护）是使用CASB的主要价值主张。

业务影响

CASB可确保整个云服务的安全政策和治理的一致性。与传统的安全产品不同，CASB旨在保护存储在他人系统中的数据，适用于各行业中各种规模的组织，并能证明云服务可实现良好的管理。随着CASB功能的不断扩展以及与SWG/ZTNA的不断融合，同时鉴于更换供应商的相对便利性，在选择CASB时，建议选择一年的合同期限而非更长的期限。

驱动因素

- 最终用户组织需要确保对业务关键型云交付应用和基础设施的安全使用；确保一般互联网安全，以防止位于任何位置的用户受到威胁；并改善对现有服务的访问，同时利用零信任概念。今天，CASB正与SWG和ZTNA融合，提供这种"三角凳"的概念，以支持所有此类用例。
- 随着SWG供应商实现对业务关键型云应用和基础设施的安全使用，CASB供应商扩大功能以涵盖一般互联网安全和对现有服务的访问，安全领导者现在能够成功地交付上述三种能力，能同时提供这三种能力的供应商的数量也在日益增多。
- 新冠疫情的爆发使人们更加关注能直接受益于CASB技术的两个具体用例：向远程工作的大规模转变和业务关键型云服务使用率的不断提升。

阻碍

- 缺乏对DLP的关注会导致对CASB失去信心，因为企业无法建立全面的政策和管理假阳性率。
- 一部分控制是由CSP自己提供的，例如，Office 365的原生安全功能和Salesforce Shield。
- SaaS租约的组织所有权不明确导致CASB的部署不能充分保证SaaS的安全。
- 在通过扩大许可协议部署多个CASB的组织中，产品整合宣告失败。
- 一些供应商的CASB功能重叠，导致了重复和混乱。

用户建议

- 考察供应商在四个功能领域的能力：可见性、数据保护、威胁检测和合规性。
- 寻求对多种操作模式的支持，即转发代理、反向代理（或RBI）和API，以便通过CASB对托管和非托管设备和云服务提供先进支持。
- 争取将CASB、SWG和ZTNA转移到单一供应商，因为这些服务的融合风头正劲。

供应商举例

Bitglass; Broadcom (Symantec); Lookout (CipherCloud); McAfee; Microsoft; Netskope; Proofpoint

进入高峰期

端点保护平台

分析师: Paul Webber、Jon Amato

效益评级: 中

市场渗透率: 超过50%的目标受众

成熟度: 成熟主流

定义:

端点保护平台(EPP)通常通过在端点上安装代理来提供对现有和新兴威胁和漏洞的保护。此技术必须主要针对恶意软件以及基于文件和无文件的漏洞进行保护。EPP还必须利用设备活动的行为分析来识别和预防威胁。它必须执行已知应用的允许列表，并提供设施，以调查和补救利用逃避保护控制的事件。

重要性

攻击者对企业端点采用的攻击技术越来越复杂。具体而言，勒索软件攻击者已经从过去的较简单的自动化技术，发展到高度组织化的人工操作活动，经过精心调整，可从受害者那里获得尽可能多的赎金。许多工具和技术可用于防御这些攻击，但EPP是需要发展的主要端点工具，可用于对抗复杂攻击者。

业务影响

EPP仍然是普遍部署的恶意软件预防层，被认为是所有组织的基本安全保障。人工操作的勒索软件活动和国家操纵的攻击是无法预防的，这对有效的检测和响应能力提出了额外要求。攻击者利用配置不良的未修补系统，窃取凭证以成功入侵。然后，他们使用离地攻击和无文件恶意软件来绕过安全控制。

驱动因素

- EPP市场已作出调整，以应对更先进的威胁和更隐蔽的攻击者。目前，各组织都很重视预防未知和非基于文件的攻击。行业正探索机器学习和基于云的查询能力，以替代基于本地签名的识别。易用性、低资源利用率和更少的维护需求仍然是人们期待的亮点。防篡改机制必不可少。

- EPP市场的主要演变是更容易部署和管理的云原生解决方案，以及基于行为的检测和分析方面的进展，后者可识别零日威胁。经改进的原生操作系统安全（可保护凭证、预防内核攻击，并隔离关键的安全服务，使其不被破坏）以及虚拟化浏览器和应用已经对EPP供应商的市场份额造成了进一步的侵蚀。

- EPP供应商还将多种功能集成到一个平台上，以增强产品吸引力，并将安全保护扩展到涵盖IT运营做法（如防火墙管理、设备控制、威胁和漏洞管理以及修补），有些甚至还涵盖应用控制和存储加密。

阻碍

核心操作系统安全性的提高可能会使攻击者将注意力转到操作系统以外的范畴，例如应用安全弱点、BIOS漏洞和固件漏洞。更加隐蔽的攻击意味着需要端点检测和响应(EDR)功能来检测和响应高级威胁，以免威胁绕过依赖预防和保护技术的EPP工具。如要识别离地攻击和利用设备上的现存受信任实用程序的其他隐蔽技术，这些技术不是最佳选择。

用户建议

由于攻击不断转变为更先进和隐蔽的技术，安全和风险管理领导人应该：

- 寻找能提供单一代理的解决方案，该方案要能同时提供针对已知威胁和漏洞的保护和行为分析。理想的情况是这种解决方案应具有未知项目的云端查询和良好的防篡改保护。

- 识别解决方案是否有能力报告互联网、网络和应用活动，以获得疑似恶意活动的额外迹象，并识别未知威胁或异常活动。

- 部署设施来扫描系统的漏洞，并报告/管理安全补丁的安装，以强化安全和减少攻击面。

- 倾向于具有发现威胁后能迅速遏制威胁并能远程补救系统的解决方案，最好是具有每种功能的可选自动化。

- 评估供应商能否在组织缺乏管理先进EPP解决方案的内部资源或技能时提供托管服务产品。

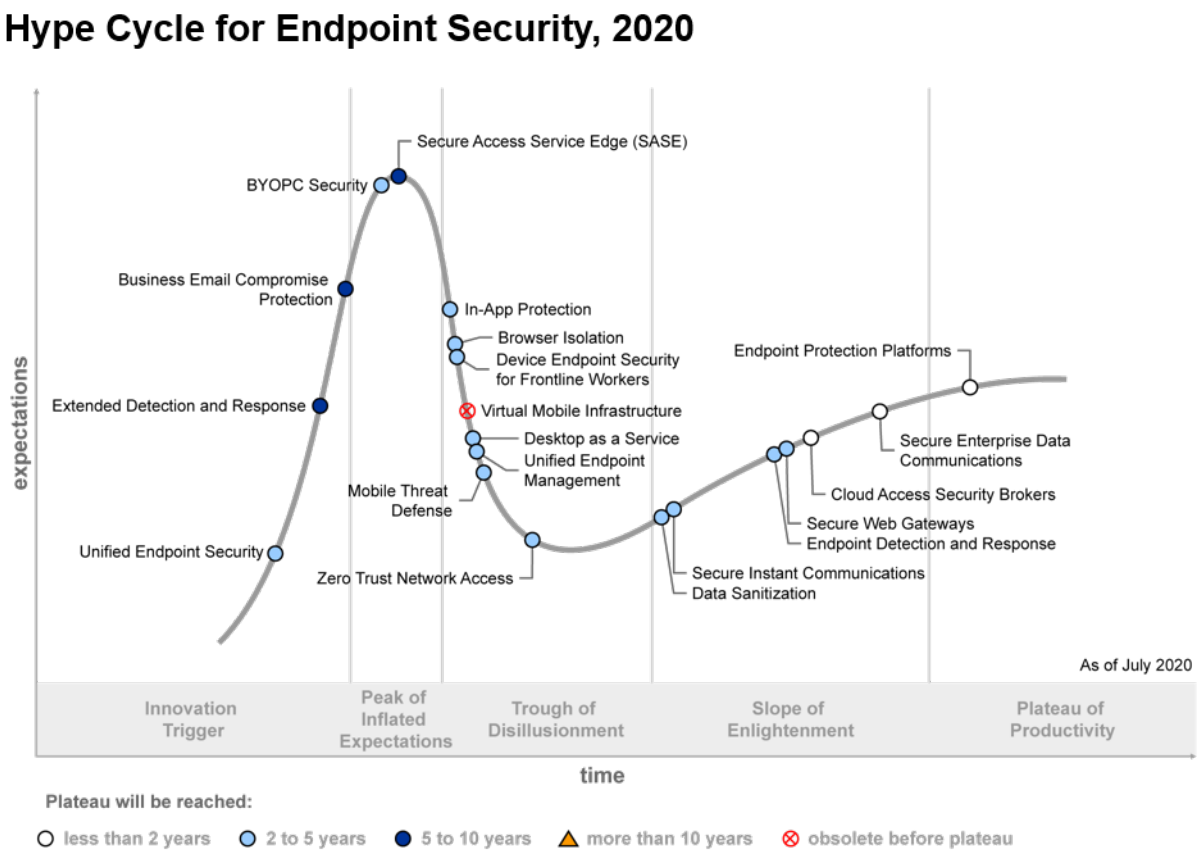
供应商举例

Broadcom (Symantec); Cisco; CrowdStrike; Cybereason; McAfee; Microsoft; SentinelOne; Sophos; Trend Micro; VMware Carbon Black

附录

图2

2020年端点安全的技术成熟度曲线



Source: Gartner
ID: 450232

资料来源: Gartner（2020年7月）

技术成熟度曲线阶段、效益评级和成熟度

表2：技术成熟度曲线阶段

阶段	定义
创新萌芽期	突破、公众展示、产品发布或其他活动引起了媒体和行业的巨大兴趣。
期望膨胀的顶峰期	在这一过度热情和不切实际预测的阶段，技术领导者大力推进的一些列宣传活动将带来某些成功，但随着创新被推到极限，更多的会是失败。唯一盈利的企业将会是会议主办机构和内容发行商。
泡沫化的底谷期	由于不能满足过于膨胀的期望，创新内容将快速过时。媒体的兴趣消失殆尽，只留下一些警示故事。
稳步爬升的光明期	日趋多样化的组织集中试验并付出辛勤的努力，促使人们对创新的适用性、风险和好处有了真正的了解。现成的商业方法和工具简化了发展过程。
实质生产的高峰期	创新的实际好处得到证实和认可。随着第二代和第三代工具和技术的出现，它们的稳定性日益提高。越来越多的组织对风险降低感到满意；采用率快速增长的阶段由此开始。约20%的技术的目标受众已采用进入该阶段的技术，或者正在采用相应技术。
获得主流采用的预期年数	创新达到实质生产的高峰期所需的时间。

资料来源：Gartner（2021年8月）

表3：效益评级

效益评级	定义
具有变革性	催生在各行各业运营业务的全新方式，使行业动向产生巨大的转变
高	催生执行横向或纵向流程的全新方式，使企业的收入大幅增加或成本显著降低
中	使既定流程实现渐进式改进，增加企业的收入或降低成本
低	略微改进了流程（例如，用户体验改进），难以增加收入或降低成本

资料来源：Gartner（2021年8月）

表4：成熟度

成熟度	状态	产品/供应商
初具雏形	在实验室中	无
新兴	由供应商实现商业化 由行业领导者试验和部署	第一代 价格较高 涉及较多的定制
未成熟	完善技术能力并提升对流程的了解 吸引超出早期采用者范畴的对象	第二代 涉及较少的定制
早期主流	技术可靠 供应商、技术和采用率快速提升	第三代 更多开箱即用方法
成熟主流	技术强大稳定 供应商或技术进步有限	几家主要的供应商
旧有	不适合新的发展 迁移成本约束更换	专注于维修收入
过时	很少使用	仅限二手/转售市场

资料来源：Gartner（2021年8月）

主要术语缩写词汇

BEC
商业电子邮件诈骗
BYOPC
自带PC
CASB
云访问安全代理
DaaS
桌面即服务
EDR
端点检测和响应
EPP
端点保护平台
SASE
安全访问服务边界
SSE
安全服务边缘
SWG
安全Web网关
UEM
统一端点管理
UES
统一端点安全
VDI
虚拟桌面架构
VMI
虚拟移动架构
VPN
虚拟专用网络
XDR
扩展检测和响应
ZTNA
零信任网络访问

Gartner研究纪要G00747412，Chris Silva，2021年8月11日

关于360政企安全集团

360政企安全集团是数字安全的领导者。17年来一直专注于为国家、政府、军队、企业、教育和金融治理等机构和企业提供网络安全技术、产品和服务，是国内较早涉足To G To B领域的安全企业之一。目前已与90%的部委、72%的央企、95%的大型金融机构和数百万中小企业开展了网络安全合作。

360政企安全
数 字 安 全 的 领 导 者

2019年9月1日，360政企安全集团启动政企安全3.0战略，以"共建、赋能、投入、培育"为新战略，着力构建大安全生态，带动国内网络安全产业共同成长，提升中国网络空间防御的综合能力。

随着中国加速实现数字化转型，建设数字中国已经成为国家战略。但网络安全威胁也普遍存在于所有数字场景中，如工业生产、能源、交通、医疗保健、金融以及城市和社会管理。因此，有必要达成数字时代安全共识，将安全作为数字战略的基础，构建数字时代的安全能力体系。

360企业安全集团作为这一共识的倡导者和追随者，于2020年8月31日更名为360政企安全集团，专注于"政+企"市场。

在这种情况下，360凭借17载实践经验总结采用一套新的战术，其标志是安全与数字系统集成，攻防与管控能力集成。这种新战术提供了数字安全能力框架，包含基础能力框架和八大数字安全框架。基础能力框架以安全大脑为核心，构建了攻击面防御、资源面管控、数据运营、专家运营等4大类基础设施。这套基础设施可以不断扩展，帮助党政军企用户构建一套可运营、可持续、可成长、可输出的安全能力。

该框架是数字安全能力体系的总体架构，能够形成大数据安全、云安全、物联网安全、新型终端安全、网络通信安全、供应链安全、应用安全、区块链安全等八大数字安全框架，以系统化安全解决方案应对新时代的安全挑战。

目前，这套框架先后服务于重庆、天津、青岛、鹤壁、苏州、郑州、上海、周口等城市的安全基础设施建设和运营，树立了标志性的城市级安全服务典范，构建起以网络安全大脑为核心的协同防御体系，整体提升我国应对数字时代高级威胁的安全能力。

除此之外，360政企安全集团也是国家网络安全保障的核心力量，在全国两会、十九大、九三阅兵、一带一路峰会、G20、金砖国家会议、APEC、建国七十周年庆典的重保工作，以及国家安全和国防安全相关工作中发挥了重要保障作用。