360 终端安全响应系统

白皮书

■文档编号	■密级
■版本编号	■日期

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

版权声明

版本变更记录

时间	版本	说明	修改人

适用性说明

本模板用于撰写 **360 企业安全集团**中各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

威胁状况愈演愈烈

现今针对于终端的恶意威胁复杂性和多样性都有显著的变化和提升，短短的几年时间，恶意威胁就由原来的直接、随机、粗暴的恶意攻击手段转变为有目标、精确、持久隐藏的恶意攻击所取代。

同时现在高级威胁也并非像原来的单一的威胁事件，它们会依照安排好的多个阶段进行有条不紊的开展，预估好每一步骤，通过**侦测、武器化、传输、漏洞利用、植入渗透、C2、窃取**步骤达到最终的目的，并可在短时间造成用户的惨重损失，但是要发现、解决则需要几周或数月的时间，及越来越多传统的安全解决方案的没有办法有效的解决高级威胁的问题。

同时我们定义的终端不再仅仅是 Windows 操作系统的计算机，当再提及终端的时候，指的可能是任何类型的机器，包括：笔记本电脑、台式机、服务器、移动设备、嵌入式设备，SCADA 系统，甚至 IoT 设备，面对缤纷杂乱的终端，我们很难以统一的方式保护他们免受从复杂的攻击。

传统安全手段应对高级威胁的难点：

静态防御技术

静态防御技术基本依靠已知样本来识别恶意文件、URL 等相关信息，主要针对样本静态代码特征进行对比分析，同时依靠特征库的更新来发现较新的恶意威胁。但是随着攻击的进化，攻击者们使用不同的技术来逃避传统的检测和防御，同时每天新增捕获大的恶意样本，已经突破百万级别，这种检测手段显得力不从

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

心。

动态防御技术

动态防御技术用机器的力量对抗恶意样本和大量变种，通过动态沙箱等技术进行对抗。目前的沙箱在虚拟仿真环境下执行未知文件，通过其行为来判别威胁的一种方式。

但是攻击者很快就意识到恶意样本虽然不能回避沙箱，但可以去主动检测当前的运行环境是否为虚拟环境，而不是他们真正的目标终端，利用仿真时间有限，缺乏用户交互，只有特定的操作系统的图像等途径进行判断。攻击者利用这些技术来帮助确保他们的恶意代码不会在模拟环境中运行，并直到达到最终目的。

主动检测和响应分析

真正高效的威胁检测和响应产品应该收集终端上发生的一切行为，然后找出关键目标和威胁，其次对事件进行深度调查，最后对安全威胁进行有效的处置和抵御，缩短安全调查时间，提升威胁处置效率。

针对于高级威胁，必须用更好的方法来进行主动检测，依靠自动化的智能响应，而不是依赖人为干预。

目前的终端技术在针对检测和响应方面对比分析：

检测、响应能力	静态	动态	行为
数据可视性	无	查询、扫描	实时可见性 端点持续记录 行为记录

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

检测能力	签名方式检测	沙箱	威胁情报 行为分析
响应能力	人工处理	人工分析 事后取证	自动化分析
修复能力	签名检测 已知恶意软件	基于黑白名单 自定义禁止策略	可定制形式防御 自动修正

360 终端安全响应系统：

360 终端安全响应系统是国内首款针对于高级威胁进行快速检测和响应的新一代终端安全产品。它可以持续洞察内网终端的安全活动信息，结合 360 大数据威胁情报等线索对内网沦陷终端进行快速的检索和定位，并提供针对威胁事件的自动化响应和修复能力，在对抗高级威胁中获得更好的效果与更快的效率，最大限度压缩攻击者的攻击时间，减少高级威胁最终达到目的可能性。

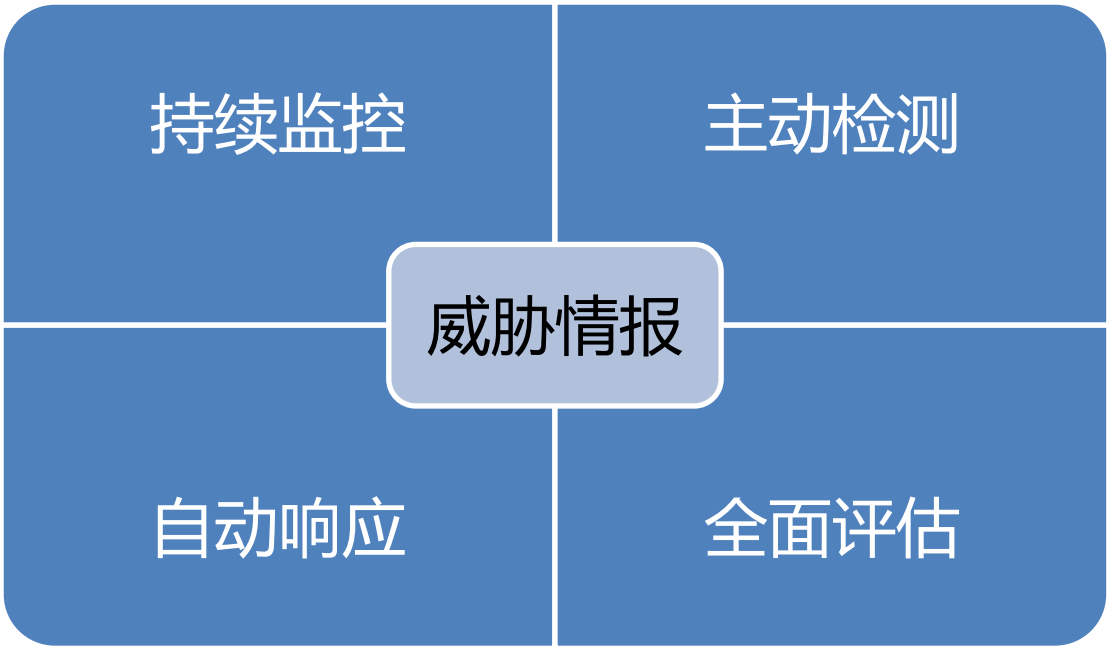
产品理念：

360 终端安全响应系统采取了一种全新的“攻防倒置”的思路，改变原有的防守方如果有一次的防御的失误，攻击者就会成功的渗透现象。而是依靠大数据威胁情报的指引，快速锁定威胁终端，通过实时数据和历史终端信息对于受害终端进行深度评估，揭示内网终端的安全缺陷，通过自动化响应机制进行处置。

终端安全响应系统可以将一个复杂的高级威胁安全响应，分解成了定位、评估、响应、修复等一系列行动过程，从而解决了 APT 攻击难以处置的问题。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

产品特性：



持续监控：

针对于高级威胁最关键的一点是能够发现复杂的和隐藏的恶意威胁。360 终端安全响应系统通过终端轻引擎连续的记录端点上行为数据、静态样本、软硬件资产等信息，实时上传到单独的大数据分析平台进行集中化存储，更便于安全事件的检测和评估，丰富安全工具的信息视图。

主动检测：

360 终端安全响应系统可实时接收 360 云端的大数据威胁情报，针对于情报中的样本 HASH、特征、IOC、以及相关的指标等信息做为沦陷终端的检索来源进行主动、实时快速的定位，对于威胁进行定级和预警。

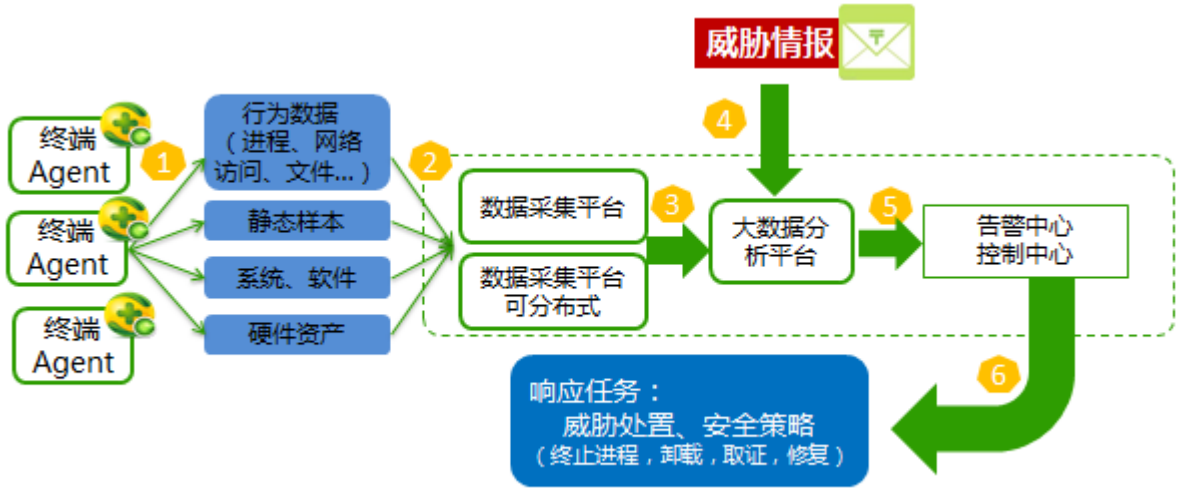
全面评估：

结合背景信息，对于沦陷终端进行全面的安全评估，检测沦陷终端涉及的范围、影响、相关的操作，识别易收攻击的资产和潜在的漏洞，提供相应的需补救的终端信息。

自动响应：

根据威胁告警信息触发自动响应策略和防御行动，根据威胁类型生成对应响应动作（例如：紧急遏制、远程取证、策略善后等），自动将威胁的影响降至最低。并可对威胁攻击后进行调查、取证，从而发现安全弱点，同时进行修复，提升安全基线。

产品部署图：



360 终端安全响应系统功能和优势

产品功能	产品优势
全局可视化	实时采集终端活动信息，消除安全盲点，实现终端全局可视化。
威胁情报	实时接收云端大数据威胁情报。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

高级检测	使用基于行为和机器学习的高级检测方法发现终端威胁。
主动分析	用户可以根据需求自定义规则去扑捉更具有针对性的威胁。
自动响应	对应不同高危威胁提供对应的快速安全响应处置方案。
高适配性	支持目前主流操作系统平台，以及无人值守终端、联网智能设备等。
高兼容性	全方面面兼容第三方应用和各类系统，保障业务持续不中断。
易部署	分析功能在大数据分析平台，对终端无任何压力。
安全生态	终端威胁情报和攻击行为模式共享，可与其它安全服务和产品对接。

用户收益:

看的见：通过全终端数据持续记录的方式，时刻准备着高级威胁入侵时的做出威胁还原所需的数据信息，给予坚实的终端数据支撑。

防的住：针对威胁事件，帮助用户拥有多种处置的手段，无需用户协调更多资源进行协助，减少风险留存时间。

查的准：帮助用户在复杂 IT 环境中，可以实时跟踪、定位每一个终端遭受的攻击状况，快速结合背景信息，全面、精准的评估全网终端面临的威胁。

搞的定：帮助用户梳理高级威胁的攻击全貌，针对完全漏洞进行补救，并完善安全架构。