360 终端安全响应系统

产品白皮书

目　录

1 引言

1.1 终端威胁的进化

经过近十年的大范围网络安全基础设施的建设，国内企业安全防护系统经历了一个从无到有、从有到全的发展过程，终端的定义也不再仅仅是 Windows 操作系统的计算机，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，大量的投资建设建起了庞大的安全防御工事：IDS、防火墙、扫描器、审计系统、WAF、防毒墙等安全设备应有尽有，但是针对于网络与终端的安全事件却层出不穷，敏感数据泄露的安全事故更是比比皆是，恶意威胁由原来的盲目、直接、粗暴的攻击手段转变为现在的精确化、持久化、隐匿式的恶意攻击，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、解决威胁、评估损失则需要数周甚至数月的时间，究其原因在于依靠已知特征、已知行为模式进行检测的网络安全防护技术手段无法预知新型恶意威胁的攻击特征与攻击行为模式，传统的防御技术在面对当今终端上的各种高级威胁问题已经不再适用。

1.2 终端静态防御技术

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。但是在互联网飞速发展的今天，新增捕获恶意样本每天已经突破百万级别，随着攻击的进化，攻击者们采用的攻击手法和技术都是未知漏洞（0day）、未知恶意代码等未知行为，这些技术手段可以轻松逃避传统的检测方法和防御技术，在这种情况下，依靠已知特征、已知行为模式的静态检测防御技术显得力不从心。

1.3 终端动态防御技术

动态防御技术是通过机器的力量对恶意样本及其大量变种进行对抗防御。最常见的技术就是动态沙箱，其是一种在虚拟仿真环境下执行未知文件并通过其行为来判别威胁的一种防御技术，通常利用多种沙箱环境来适配不同的恶意样本在不同的环境下执行的情况。但是攻击者在发起攻击前通常都会精心策划每一个攻击环节，包括：攻击工具的开发、控制网络的构建、木马程序的投递、本地的突防利用、通信通道的构建等等。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还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沙箱局限性进行环境判断判断，攻击者利用这些技术来确保他们的恶意代码在沙箱的模拟环境中不被运行，从而脱离沙箱环境后成功渗透到内网中。

1.4 新一代终端安全技术

攻击者通常都会在内网的各个角落留下蛛丝马迹，真相往往隐藏在网络的流量和系统的日志中。传统的安全事件分析思路是遍历各个安全设备的告警日志，尝试找出其中的关联关系。但依靠这种分析方式，传统安全设备通常都无法对高级攻击的各个阶段进行有效的检测，也就无法产生相应的告警，安全人员花费大量精力进行告警日志分析往往都是徒劳无功。对高级攻击进行检测需要从内网全量数据中进行快速分析，这要求本地具备收集并存储终端的海量的行为数据能力、检索能力，然后找出关键目标和威胁，对事件进行深度关联分析，最后对恶意威胁进行有效的处置和抵御。

以美国为代表的网络安全先进国家已经越来越清晰意识到：安全不是在一个点上的攻防与决战，而是一个长期的反复较量，为了打赢网络战争，需要全面的情报体系、需要对情报的分析解读能力，而不是像以往依靠某个报文、依靠某个会话、依靠某个文件的判断，因此以美国为首的发达国家率先提出了安全情报的概念，实际上就是全方位搜集所有可能与安全相关的数据信息，利用大数据分析技术对数据进行分析、解读，在此基础上挖掘出可能存在的潜在威胁、已经存在的高隐秘性攻击、或已经完成了的渗透行为。

由此可见，针对于内网终端高级威胁必须依靠威胁情报结合本地化自动化的智能响应才能大幅缩短安全调查时间，有效提升威胁处置效率。

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	静态防御技术	动态防御技术	检测与响应
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
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

2 产品介绍

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。

2.1 产品理念

360 终端安全响应系统是以威胁情报驱动的新一代终端安全产品，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，通过最新的安全线索快速锁定威胁终端，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。

在大数据威胁情报的指引下，终端安全响应系统可以将一个复杂的高级威胁安全响

应，分解成为定位、评估、响应、修复等一系列行动过程，从而解决了高级威胁难以处置的问题。

2.2 设计模型

图 1 终端安全响应设计模型图

持续监测：持续记录终端上的所有行为，将静态和动态的终端数据实时推送到大数据分析平台进行统一的存储和管理。

主动检测：实时接收大数据威胁情报、鉴定中心等告警线索信息，在大数据分析平台中主动检索、定位符合条件的威胁终端。

全面评估：针对于威胁终端进行全面的安全评估，结合终端背景数据，对于终端的安全漏洞、威胁的攻击步骤进行分析评估，发现整个攻击链与终端沦陷的根本原因。

自动响应：针对不同类型的终端威胁提供相应的自动响应手段，结合终端、业务、系统等因素提供补救手段，提升安全基线，防止同类型攻击再次发生。

2.3 产品组成与架构

360 终端安全响应系统主要包括终端采集器、数据采集平台、大数据分析平台、控制中心、威胁情报五个部分组成。

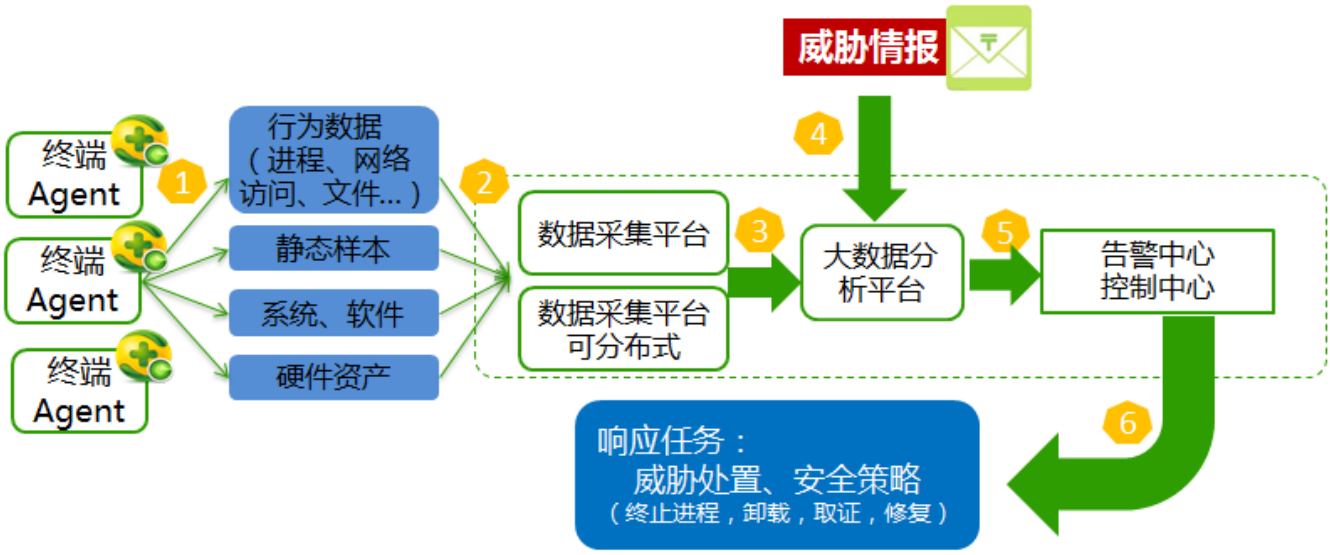

图 2 终端安全响应架构图

2.3.1 终端 Agent

终端 Agent 主要负责对全网终端的安全数据进行采集并对威胁事件进行自动化的响应处置，终端 Agent 会将采集到的终端安全数据会汇总到数据采集平台上进行统一的归类、加密，并传输给大数据分析平台。

终端 Agent 可以支持 IM 文件传输信息、驱动信息、操作系统信息、进程信息、DNS 访问审计、IP 访问记录、U 盘使用记录、软件安装信息、邮件日志信息、证书相关信息等。

2.3.2 大数据分析平台（硬件）

终端大数据分析平台用于存储终端采集器提交的终端安全数据信息，并对所有终端安全数据进行快速的处理并为检索提供支持，同时可与威胁情报或其他告警进行关联帮助进一步分析，对攻击进行有效地回溯定位。

分析平台承担对所有数据进行存储、预处理和检索的工作。由于传统关系型数据库在面对大量数据存储时经常出现性能不足导致查询相关数据缓慢，分析平台底层的数据检索模块采用了分布式计算和搜索引擎技术对所有数据进行处理，可通过多台设备建立集群以保证存储空间和计算能力的供应。

2.3.3 威胁情报

终端威胁情报来自 360 云端的分析成果，针对 APT 攻击、新型木马、特种免杀木马进行规则化描述。威胁情报通过人工智能结合大数据知识以及攻击者的多个维度特征还原出攻击者的全貌，包括程序形态，不同编码风格和不同攻击原理的同源木马程序，恶意服务器（C&C）等，通过全貌特征‘跟踪’攻击者，持续的发现未知威胁，最终确保发现的未知威胁的准确性，并生成了可供大数据本地分析平台使用的可机读的威胁情报。

2.3.4 控制中心

控制中心提供威胁追踪和告警响应的安全能力，威胁追踪提供安全运维人员对于威胁进行追踪的能力，威胁追踪功能可以提供给运维人员手工搜索全网终端安全数据的能力，可以通过模糊搜索、精确搜索来快速查找到有价值的特定内容，并可对特定内容进行类型的筛选、统计、过滤等功能。方便有安全经验的运维人员去主动发现内网的安全事件。告警中心会将与威胁情报关联到的内网安全事件进行告警，针对于涉及的终端、风险级别、事件的类型、告警的概要和详情进行详细的描述，提供安全响应的功能（目前响应能力包括结束进程、结束进程并隔离、删除），并针对已响应任务的进行查看，了解响应的终端范围与进度。

3 产品功能

功能	描述
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。

大数据平台	独立的大数据分布式检索平台，高效的对安全数据进行集中化管理、分析。
威胁情报	360 大数据威胁情报的实时接收。
威胁追踪	提供安全运维人员主动在内网终端数据中搜索、定位威胁线索的工具。
行为模式	针对于终端的相关行为操作进行实时动态监测、分析、检测，以确它是否为恶意行为。
自动化响应	对应不同的终端威胁提供对应的自动化响应策略和手段。
高适配性	支持目前主流操作系统平台，以及无人值守终端等。
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、检测、评估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。

4 产品部署方案

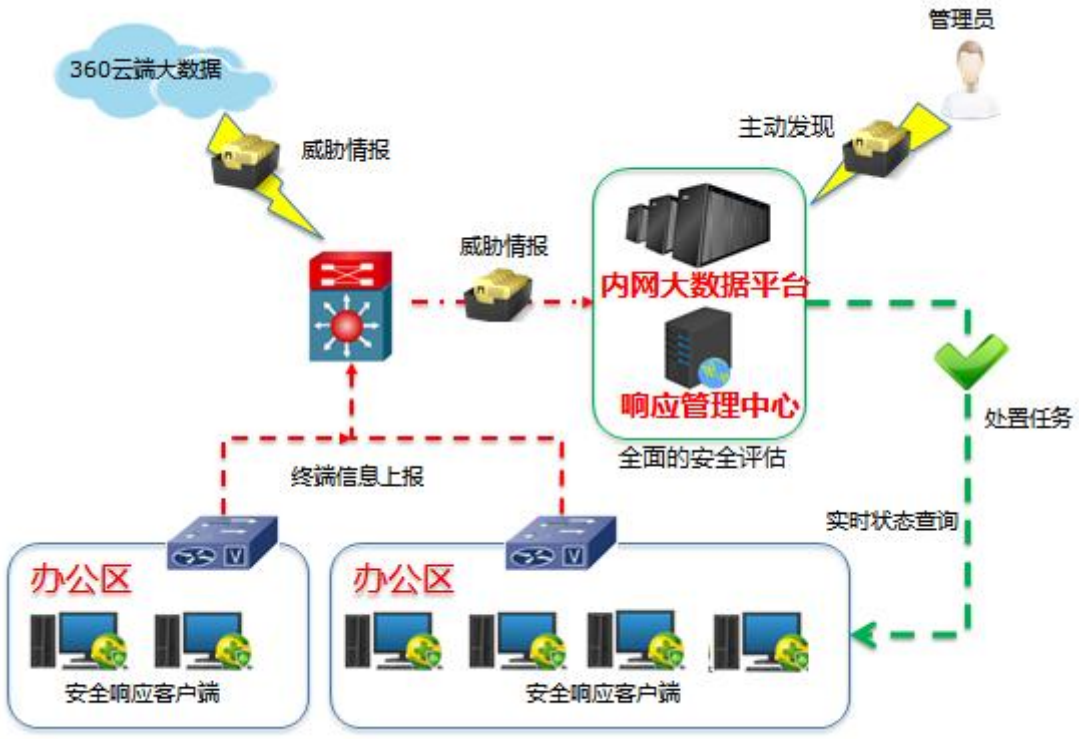

图 3 产品部署拓扑图

部署 360 终端安全响应系统可以帮助用户及时有效的内网终端感染的高级威胁，提升安全管理人员的发现速度和响应效率，最大限度的降低用户受攻击后的损失。

在此方案中，对用户终端中的安全数据进行采集和检测，所有终端安全数据经过压缩、加密后保存于大数据平台，结合云端威胁情报与本地分析平台中的终端行为数据进行对接，从而发现已经感染高级威胁的终端，对于终端快速定位，进行全面的安全评估，发现终端的威胁的根本原因，触发告警从而自动进行响应，斩断威胁的链条。

1、终端部署 360 终端安全响应系统的 Agent 客户端，对于数据进行采集和响应。

2、在服务器端部署 360 终端安全响应系统控制中心（默认控制中心和采集平台为一体），对于采集数据进行加密，同时对于终端 agent 进行采集策略的制定、告警通知、威胁追踪等功能。

3、在内网部署大数据分析平台，实时存储终端的安全数据，对于数据与外网威胁情报进行主动检测，从而发现沦陷终端。

5 产品优势

5.1 威胁情报驱动

依托于 360 公司云端的海量数据，以国内高水平安全研究实验室人员的技术支撑，通过机器学习与自动化数据处理技术，持续的发现未知威胁，通过统一的规范化格式将攻击中出现的多种攻击特征进行标准化并生成可机读威胁情报，用以驱动终端在第一时间内对威胁进行及时检测和响应。

5.2 持续采集监测

360 终端安全响应系统采用了最为完整的终端安全监测方案，通过终端安全数据的不间断采集、监测、与分析功能，可以显著提升发现潜在威胁的能力，提升调查工作的便捷性,为深入透彻的了解终端的威胁状况提供重要的背景基础。

5.3 快速检索定位

依托于 360 公司成熟的大数据运营经验，采用基于 Elastic Search 技术的搜索引擎，使用分布式多协同处理方式建立索引，达到实时、稳定、可靠的查询性能，快速返回终端威胁查询结果，有效地避免了传统系统中在处理海量数据遇到的稳定性、及时性、可靠性等技术瓶颈。

5.4 自动化响应

针对于发现的高级威胁事件，可提供对应的安全响应的处置策略和任务，对于威胁事件提供隔终止、隔离、取证等安全手段，快速终止威胁的持续发生。提升安全运维团队的响应的效率和处置威胁事件的能力。