天珣下一代恶意代码防护系统

技术白皮书

EDR

全方位保护主机安全

启明星辰 Venus
领航信息安全

目录

1 现状分析

1.1 安全面临现状

当前的企业以及组织单位中，大部分都部署了终端防护软件以保证终端的安全，避免入侵以及数据泄露事件的发生，然而效果有限。从研究机构的报告来看， 2015 年到 2016 年数据泄露事件的数量从 77503 起增长到了 10 万起，当前终端面临的安全威胁正在发生改变，同时关于终端的定义以及范畴也正在不断扩大，导致防护难度的增加。

- 终端类型多样性：终端操作系统或者主机操作系统在不断的升级和国产化，终端安全产品面临需要适配的终端环境越来越多，在不同的终端环境的前提下，安全的防护能力又得到了全新的挑战。
- 攻击方式多样性：攻击方式从原有的暴力进攻转成更加精准和隐蔽，在不通过单一的病毒或恶意软件感染来达到目的，而是通过一系列的侦查、定制、植入等手段相结合达到最终目的。
- 勒索恶意代码成为能嵌入到任何操作系统、任何业务系统中的中级杀手，被感染后将对业务造成较大影响或者经济损失。

1.2 下一代终端安全方案

主机安全通常被称为安全的最后一公里，由于主机类型的多样性、业务的多样性，主机安全在组织内都知道很重要，但是往往又得不到良好的配合导致终端产品推行受阻。启明星辰公司推出了下一代恶意代码防护系统，改变原有的产品简单粗暴的防护模式，通过全新轻量级客户端及高性能分析管理平台来对组织内的主机安全进行防护。

对于已知的威胁风险进行有效的安全防护，修复已知的安全漏洞，利用完善的样本库为基础，强化主机自身安全能力，以及防御已知威胁风险。

对于未知的威胁风险进行库比对、关联计算、对比计算同时结合产品的主动防御能力，实现对未知威胁的发现以及研判，对终端上的各种行为进行持续监控，能够更快速、更有效的解决恶意未知程序的攻击。

一起攻击事件在不同的阶段具备不同的行为特征，这些行为特征分开来看并不一定构成威胁，而原有的解决方案中并不具备将这些行为进行关联分析的能力，导致威胁无法被检测和阻止。要实现对未知威胁以及未知恶意代码攻击的检测必须依靠机器学习、分析能力，通过大量的行为日志分析和快速检索，找出关键目标和威胁，对相关事件进行关联分析，进而还原安全事件全貌，并进行有效的防御和处置

2 产品综述

2.1 产品简介

天珣下一代恶意代码防护系统作为主机安全中新的防御逻辑，一改传统的被动防御模式，将防护做在前面、保护做在前面，实现提前发现、提前分析、提前响应、提前扼制的防护思路，将主机安全的防御能力化被动为主动，采用极致轻量化客户端为信息采集基础节点，同时配合产品高性能分析、研判能力，全面强化主机安全，最终实现主机自安全的目标。

2.2 核心价值

EDR 轻量级客户端：采用全新一套设计理念，产品在设计中采用全新的无驱动、无 hook 的方式，彻底告别原有的臃肿终端，对主机性能占用降到最低。可更加便捷进行安全、部署。

EDR 自学习能力：采用自学习的策略创建方式，改变原有策略的配置逻辑，通过一套安全的白名单机制，对主机信息进行采样、辅助分析，并且支持一键生成策略能力。可更加便捷进行实施、上线。

EDR 完善的分析能力：利用白名单机制对主机数据进行获取同时集成威胁情报分析，让事件分析更准确。可更加便捷进行维护、调整。

2.3 核心功能

EDR采用轻量级无UI、无感知终端代理，集成威胁情报分析，创新性的将应用程序白名单、网络链接白名单、外设管理白名单等技术引入主机安全防护。 通过终端数据采集分析和威胁情报判断，自学习并生成的主机正常安全可信行为的白名单。如果发现其用户节点的行为不符合白名单中的行为特征，天珣主机安全防护系统将会对此行为进行记录或阻断，以此避免工业控制网络受到未知威胁，同时还可以有效的阻止操作人员异常操作带来的危

害。并且具备强大的病毒查杀及恶意代码查杀能力。确保：

（一）只有安全可信的进程可以运行；

（二）只有许可的进程才能进行许可的网络链接；

（三）只有允许的外接输入设备才允许接入使用；

（四）恶意代码及病毒查杀能力。

天珣下一代恶意代码防护系统定位为主机提供全生命周期的安全管理，通过在主机安装基于白名单技术的防护系统，能够防范恶意程序的运行、确保终端的网络链接安全可信、阻断病毒木马的扩散、规范外接输入设备的使用，保障终端的行为始终在受控信任范围内，实现对主机全面的安全防护。保障工作站、服务器的可用性、可靠性和可信性。主要功能：

2.3.1 白名单学习

通过周期自学习功能可快速方便生成可信白名单，解决业务繁杂难实施以及对终端进程运行不太了解的情况，降低客户的部署难度。同时支持自定义追加、手动导入等方式方便主机及的白名单维护。

2.3.2 进程白名单

监控系统运行情况，只允许运行白名单中的安全可信的进程(正常系统程序、授权的组态软件等)。对于运行白名单之外的进程，都将记录或阻断。即使被恶意导入危险程序也将第一时间被阻断，从源头上遏制了恶意代码的运行。

2.3.3 网络白名单

监控网络链接情况，只允许白名单中的安全可信的进程从指定端口与指定 IP 的指定端口连入或连出。白名单之外的网络链接，都将记录或阻断。即使终端被接入互联网，也只有安全可信的进程能在白名单内进行限定的网络连入或连出，实现在不更新补丁，不安装杀毒软件的情况下也能限制恶意代码的传播，防止攻击和被攻击。

2.3.4 外设白名单

监控外接输入设备使用情况，只允许白名单中的外接输入设备可以接入使用，白名单之外的外接设备，接入主机时将被记录或禁用。避免被非法人员恶意导入木马病毒及修改相关操作指令带来的安全风险。

2.3.5 恶意代码查杀

内置强大的恶意代码特征库，可用来应对已知的恶意代码，阻止恶意代码运行的同时，对恶意代码进行有效查杀，同时帮助用户发现当前主机存在的异常行为，并实现对安全事件的多维度关联分析，做出快速的响应和处置。

2.3.6 勒索病毒查杀

内置病毒查杀引擎，实现对勒索病毒的诱捕、判断、识别、定位和查杀勒索病毒，并能有效阻止勒索病毒的扩散与传播，精准定位到勒索病毒的感染源，进行快速查杀。

2.3.7 全面分析能力

控制中心可以针对管理所有主机上客户端进行集中管理，并将每个客户端发现的白名单违规等安全风险进行统计和分析展现，可以对全网进行全面安全风险分析和处理。同时支持一键处置的能力，快速的将分析结果转换成安全策略。

2.3.8 详细日志记录

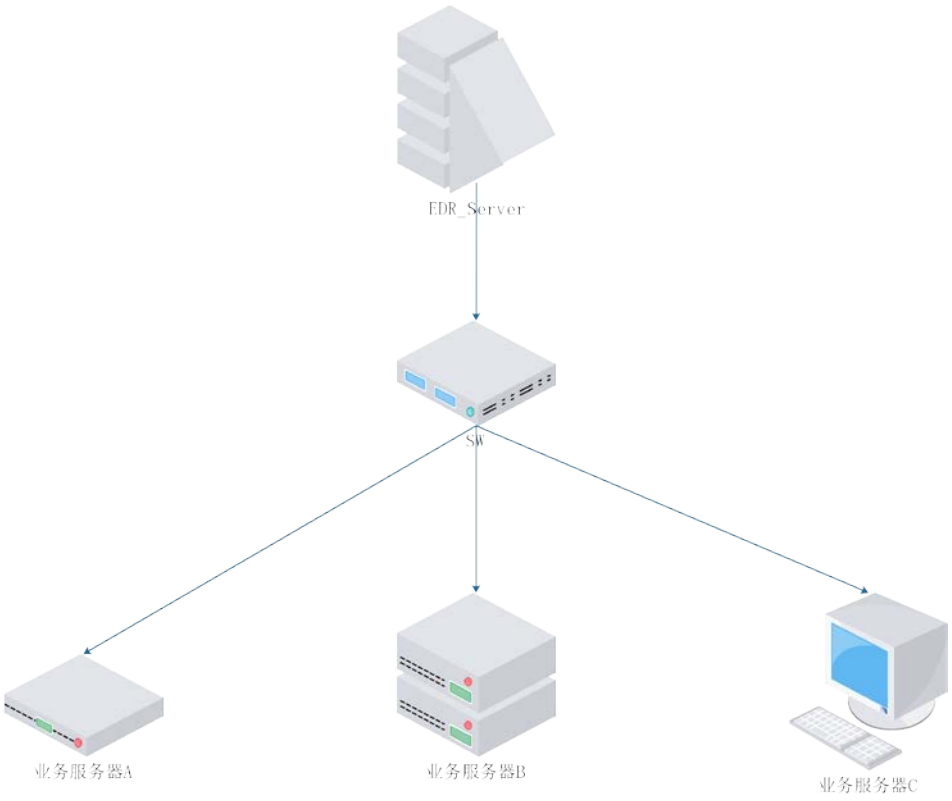
可记录事件类别、时间、设备信息、违反的白名单详情。可对违规事件进行深入详细分析，分析内容包括：进程的名称、路径、协议、端口、链接方向、目的地址、端口、进程 PID、PPID、父进程信息、文件大小、命令行信息、加载的模块、证书、md5 等等。

2.3.9 集中管理运维

EDR 可以根据组织架构进行分组管理，并通过主机、主机安全防护系统控制中心综合运用多种方法配置白名单，并对同一分组中一键下发策略，减少配置工作量。同时针对单个需要特别配置的工作站，可以进行定制化单点策略配置和审计。

2.4 产品部署

系统采用标准 C/S 架构，由服务器对所有下沉终端进行统一管理，策略同步、异步下发，日志统一搜集、分析。服务器端只需要部署到网络中与终端网络可达，对部署要求极低。



3 产品优势

1. 自学习智能匹配白名单生成技术

针对主机进行周期性学习，可一键生成白名单规则库，根据规则进行智能匹配。区别于实时采样技术生成的白名单规则，自学习技术能更准确、更高效的帮助用户建立可信白环境，能在最大程度降低误报和误判。

2. 离线威胁情报集成

集成启明星辰VenusEye，百亿级别特征库实现对主机实时威胁分析及预警。辅助自学习功能，确保只有安全可信的进程和行为列入白名单规则库，避免实时采样或手工添加误将病毒木马等加入白名单的风险。区别于传统杀毒软件高CPU、高内存占用的鉴别方式，所有威胁分析由服务端完成，对终端性能及资源几乎零影响。

3. 轻量化终端带来真正的兼容稳定

基于真实需求调研，真实用户案例实践，采用最简高效理念设计，客户端无UI、无感知，同时终端未采用任何驱动及HOOK技术实现，确保终端高效、低资源占用、稳定兼容运行。

4. 安全威胁主动追查

为用户提供了安全调查功能，依据终端异常行为告警或者关联分析产生的，安全事件告警进行威胁定位和溯源，变被动接收为主动响应，支持 IOC 批量搜查，极大的提高了调查效率，将安全威胁消灭在萌芽之初，对已发生的安全问题有据可查。

5. 弥补原有安全方案不足

针对 0day 攻击、未知恶意软件等原有安全解决方案无法发现和处理的问题，EDR 系统可以有效检测和处置，通过将多个维度的安全事件进行关联分析，准确定位攻击根源，避免大量告警造成的误判。