华为FireHunter6000沙箱

华为技术有限公司

HUAWEI

华为FireHunter6000沙箱

FireHunter可以检测出利用0-Day漏洞、高级逃逸技术等多种技术组合的APT攻击，保护您的网络免遭破坏，避免内部信息遭到窃取。

近年来，众多跨国公司甚至国家政府机构都饱受黑客的攻击，不仅在经济上遭受巨大损失，甚者还会泄露国家机密，对国家安全构成威胁。而攻击者利用的就是0-Day漏洞、高级逃逸技术等多种技术的组合，它们可以绕过现有的大部分安全设备，躲避多层次的网络防护和过滤，最终达到窃取关键信息资产、破坏企业IT基础设施等目的。由于此类威胁的目标多是针对经济或政治价值大的目标，造成的破坏程度极大，所以人们命名此类威胁为APT（Advanced Persistent Threat，高级持续性威胁）攻击。

APT攻击通常是定向型攻击，主要攻击涉及国计民生的基础设施，例如能源、金融、交通等。攻击者每次攻击前都会通过社会工程学收集目标IT系统的信息，从而通过这些信息有针对性地制定攻击入侵方案。例如攻击者收集到目标IT系统的已知漏洞或者0-Day漏洞，通过这些脆弱点渗透进入企业内部，并在企业内部扩散，最终获取到关键信息资产或者对目标IT基础设施造成破坏。

FireHunter6000沙箱是华为公司推出的新一代高性能APT威胁检测系统，通过还原交换机或者传统安全设备镜像的网络流量，在虚拟的环境内对网络中传输的文件进行检测，实现对未知恶意文件的检测。FireHunter6000沙箱面对高级恶意软件，通过信誉扫描、实时行为分析、大数据关联等本地和云端技术，分析和收集软件的静态及动态行为，凭借独有的行为模式库技术，FireHunter6000沙箱根据分析情况给出精确的检测结果，对“灰度”流量实时检测、阻断和报告呈现，有效避免未知威胁攻击的迅速扩散和企业核心信息资产损失。特别适用于金融、政府机要部门、能源、高科技等关键用户。

产品图

FireHunter6000系列

产品概述

FireHunter内置多个沙箱系统，可以在其中运行待分析程序，收集程序的静态及动态行为，并将行为展示给用户，最后给出该程序是否为恶意程序的定性结论，而FireHunter凭借的正是其独有的行为模式库技术。通过分析大量的病毒、漏洞、威胁特征，FireHunter提炼出各种恶意行为的规律和模式，并形成一套判断规则，其中每条规则都定义一种或多种软件行为，FireHunter会根据程序命中规则的情况给出对应的检测结果。

FireHunter支持的如下沙箱类型如下所示：

PE启发式沙箱：PE启发式沙箱用于检测Windows可执行文件，通过模拟硬件指令的方式来构建一个虚拟的执行环境，可以将PE文件加载到该环境中执行，收集文件的行为。与操作系统级的虚拟执行环境相比，PE启发式沙箱是一个进程级的启发式沙箱，分析文件时拥有较高的处理性能。

PDF沙箱：PDF沙箱用于检测PDF文件，通过模拟PDF文件阅读器的程序，可以对PDF文件进行行为分析。与操作系统级的虚拟执行环境相比，PDF沙箱是一个进程级的启发式沙箱，分析文件时拥有很高的处理性能。

Web沙箱：Web沙箱用于检测Web网页文件，通过模拟浏览器程序，可以对Web文件进行行为分析。与操作系统级的虚拟执行环境相比，Web沙箱是一个进程级的启发式沙箱，分析文件时拥有很高的处理性能。

虚拟执行环境沙箱：虚拟执行环境相对于前面PE、PDF、Web沙箱整体检测效率较低，但是检测质量要优于启发式沙箱。启发式沙箱可以根据文件的恶意特征来判断其是否为恶意文件，但是相当一部分恶意文件会隐藏其恶意特征，只有在真实运行起来该文件时才会触发恶意行为。为解决启发式沙箱的不足，FireHunter提供虚拟执行环境对这类威胁进行检测。虚拟执行环境是基于虚拟机技术构造的一个真实操作系统，当待检测文件在虚拟执行环境中被运行时，文件可以任意调用系统的API接口，就像在真实的主机上一样。FireHunter会监视文件对应进程的行为，并根据其行为特征判断其是否为恶意文件。当恶意文件对虚拟执行环境造成破坏性影响时，沙箱会自动恢复虚拟系统环境到初始化状态，不会对FireHunter的检测性能产生影响。

产品特点

多系统模拟，全面检测，有效防护未知威胁

全面的流量检测：具备流量还原能力，可以识别主流的文件传输协议如HTTP、SMTP、POP3、IMAP、FTP等，从而确保识别通过这些协议传输的恶意文件；

支持主流文件类型检测：FireHunter6000沙箱可以对主流的应用软件及文档进行恶意代码检测，包括支持Word、Excel、PPT、PDF、HTML、JS、EXE、JPG、GIF、PNG、FLASH、ZIP、SWF等软件及文档；

支持WEB流量检测：FireHunter6000沙箱可以对基于WEB的恶意代码的检测，支持Web页面零日漏洞检测技术，该能力在国内同类产品中是唯一支持的。支持该技术的厂家全球范围内也仅有两家，使FireHunter发现未知威胁的效率大大增加；

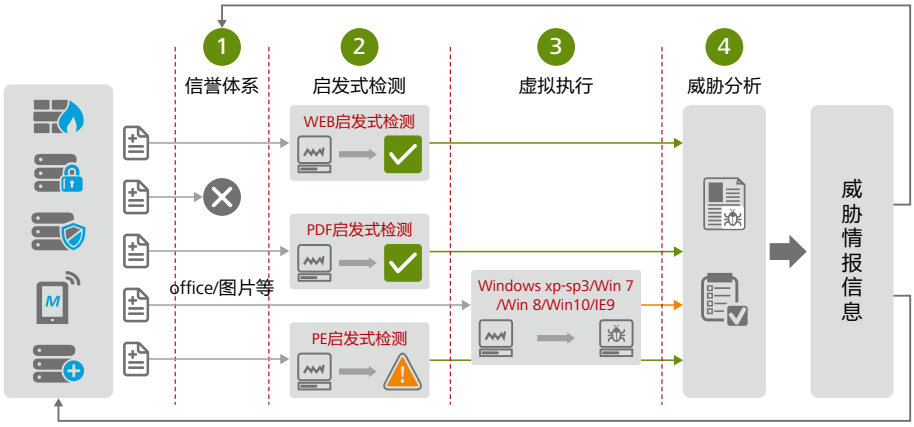
模拟主流的操作系统和应用软件：FireHunter6000可以模拟Windows 系列操作系统，可以模拟Internet Explorer等浏览器，可以模拟Office 、WPS等办公软件，Firehunter沙箱产品也可以根据用户的需要进行定制化的虚拟环境设置；

多重纵深检测，秒级响应，快速拦截未知威胁

分层的防御体系：FireHunter6000沙箱支持信誉匹配、启发式检测、及虚拟执行，从而具备快速针对以APT为代表的下一代威胁的应对能力；

业内一流的性能：华为提供业内一流的FireHunter6000沙箱分析能力，每天可以分析7万个样本，同时支持通过水平扩容方式组成分析集群。

提供准实时的处理能力：FireHunter6000沙箱提供接近实时的处理能力，有效的将对下一代威胁的检测的响应时间从几周降到秒级，并与下一代防火墙配合实现在线防御能力。



多维分析，降低误报，精确检测未知威胁

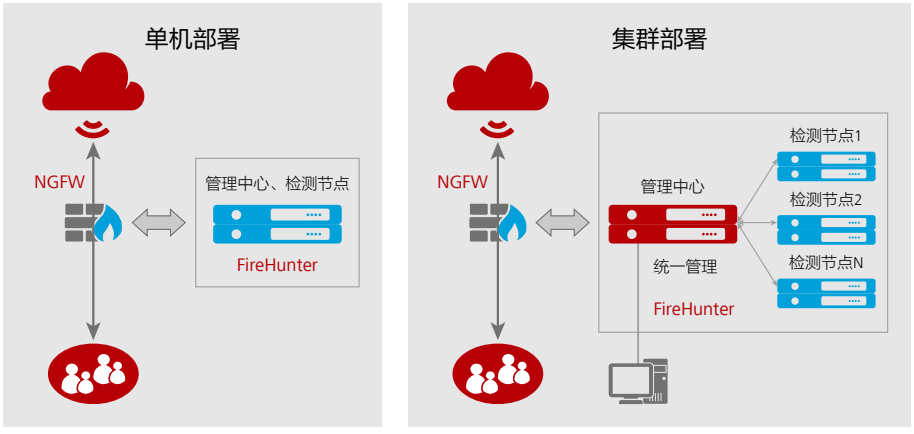
多维分析能力：多维分析能力：华为FireHunter6000沙箱通过静态分析，包括代码片段分析、文件格式异常、脚本恶意行为分析等，来缩小可疑流量范围；通过指令流监控，识别文件、服务操作，来进行动态分析，最后通过行为关联分析，判断定性。

产品部署模式

与NGFW联动、单机部署：NGFW负责还原文件，并将需要检测的文件送到沙箱进行检测。

与NGFW联动、集群部署：NGFW负责还原文件，并将需要检测的文件送到沙箱集群进行检测。沙箱FireHunter V100R001C20、C30版本支持4台集群。在集群中，有一台设备做管理中心，其他设备做检测节点。管理中心设备负责负载均衡、分发文件到检测节点进行检测，并统一对外提供检测结果查询接口。

单机独立部署：通过镜像的方式，先将流量镜像到沙箱，沙箱进行流量还原，还原出文件，并对文件进行检测。镜像部署支持设备镜像口镜像，也支持分光模式。该部署场景下，沙箱只对附件进行检测，拦截的功能由相关的安全设备实施。



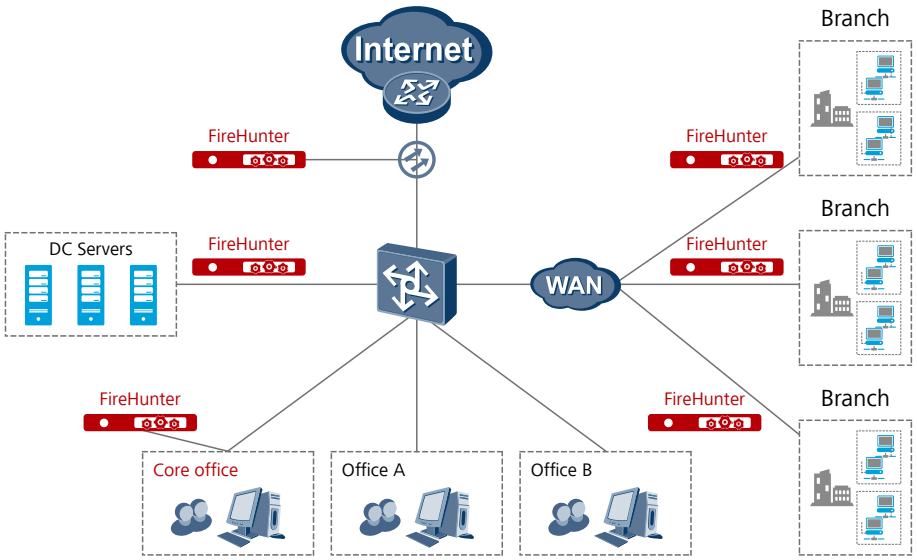
典型应用

1、互联网边界出口：重点防范来自互联网的恶意邮件、恶意web流量等。

2、分支接入边界：避免外联接入区域恶意文件、未知威胁扩散，分支总部之间任意扩散。

3、数据中心边界：重点保护服务器核心资产，发现内网潜伏的攻击、恶意扫描，渗透等。

4、核心部门边界：防范内网可疑文件传播，横向感染核心部门。



产品规格

硬件形态		
沙箱型号	支持型号：FireHunter6000 (直流或者交流)	
沙箱形态	• 机架式服务器，高度2U， X86服务器； • 不少于128G内存； • 双冗余电源； • 硬盘不少于2T； • SSD不少于128G； • 8*GE电口； • 2*10GE光口	
主要功能		
PE文件检测		
	支持对32位PE格式文件的检测	支持
	支持对压缩格式的PE文件的检测	支持
PDF文件检测		
	支持PDF格式文件的检测	支持
	支持对压缩格式的PDF文件的检测	支持
Web文件检测		
	支持对Html/Htm格式文件的检测	支持

	支持Html/Htm包含的Javascript文件的检测	支持
	支持对Flash格式的文件进行检测	支持
	支持对JavaApplet文件进行检测	支持
	支持对压缩格式的Web文件的检测	支持
Office文件检测		
	支持对word 2003，word 2007格式文件的检测	支持
	支持对excel 2003，excel 2007格式文件的检测	支持
	支持对powerpoint 2003，powerpoint 2007格式文件的检测	支持
	支持rtf格式文件的检测	支持
	支持对邮件附件中包含的Office文件的检测	支持
	支持对WPS格式文件的检测	支持
	支持对压缩格式的Office文件的检测	支持
图像文件检测		
	支持对gif格式文件的检测	支持
	支持对jpg格式文件的检测	支持
	支持对png格式文件的检测	支持
	支持对tiff格式文件的检测	支持
	支持对压缩格式的图像文件的检测	支持
流量还原		
	支持http、smtp、pop3、imap、ftp协议的流量还原	支持
部署方式		
	本地部署，与NGFW联动	支持
	本地旁路部署	支持
	集群部署	支持

订购信息

主机	02311GVW	功能模块-FireHunter6300-AC交流典配(2*750W交流,滑轨)
License	88033DNR	软件费用-FH6000-LIC-1AV-1Y-安全沙箱单引擎AV库升级服务1年License-Multiple Model
License	88033DNT	软件费用-FH6000-LIC-1AV-3Y-安全沙箱单引擎AV库升级服务3年License-Multiple Model
License	88033DNX	软件费用-FH6000-LIC-TML-1Y-安全沙箱威胁模型知识库升级服务1年License-Multiple Model
License	88033DPA	软件费用-FH6000-LIC- TML-3Y-安全沙箱威胁模型知识库升级服务3年License-Multiple Model

商标声明


、HUAWEI、**华为**、 
是华为技术有限公司的商标或者注册商标。
在本手册中以及本手册描述的产品中，出现的其他商标、产品名称、服务名称以及公司名称，由其各自的所有人拥有。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司

深圳市龙岗区坂田华为基地
电话: (0755) 28780808
邮编: 518129
版本号: M3-032102-20161220-C-1.0

www.huawei.com