技术规格表

产品名称	**天阗高级持续性威胁检测与管理系统**
产品型号	**APT3000 V2.0**
产品规格	标准机架式设备，提供 220V±10%，双冗余电源； 配置 6 个千兆电口，2 个万兆光口，内置 16T 硬盘， 256G 内存。
产品性能	网络层吞吐量为 4Gbps；文件检测每天 2 万。
产品功能	能够将文件和数据报文等在沙箱中进行运行分析，通过分析能够检测出文件的行为信息以及异常调用的情况。 具备行为检测能力，能够对进程行为、注册表行为、文件行为、可疑网络行为等进行检测。 具备生成恶意代码行为报告的能力，当检测到恶意代码行为时，会生成恶意代码行为报告。 能够检测的文件格式种类 100 种。 能够针对不同的工作流自定义的选取与之相匹配的样本格式。 具备 20 种反沙箱行为检测。 支持静态检测、漏洞检测、行为检测三种检测机制，并且针对每种检测机制的检测流程都可以通过自定义的方式进行配置。 具备多种检测能力，包括正常邮件检测、HTTP 检测、FTP 检测、SMB 检测等，并且对于可疑样本能够通过手动上传的方式进行检测。 支持检测多种文件类型，包括：释放 PE 文件、删除文件夹、修改文件、拷贝自身、感染文件等敏感行为下载文件等；并且能够对文件系统的监控操作进行详细记录，记录的方式包括：写入文件（夹）、删除文件（夹）、读取文件（夹）等。 具备手动导入 pcap 包检测的能力，检测的内容多种多样，具体包括：特征检测、样本检

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦 邮政编码：100193
集团总机：010-82779088 集团传真：010-82779000 售后热线：400-624-3900
售后邮箱：support@venustech.com.cn 启明星辰微信公众号：venustech_weixin
官方微信 官方微博

	测、隐蔽信道检测等，通过检测能够展示出 pcap 包与事件对应关系以及能够展示检测时间和发生时间。 具备 10 种样本检测工作流配置，每天能够检测的文件数量为 2 万。
环境适应性	工作温度 0℃～40℃，存储温度-20℃～60℃，工作相对湿度 20%～80%

通讯地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号启明星辰大厦　邮政编码：100193
集团总机：010-82779088　集团传真：010-82779000　售后热线：400-624-3900
售后邮箱：support@venustech.com.cn　启明星辰微信公众号：venustech_weixin