亚信安全™

深度威胁发现设备TDA

强化全网威胁可视化，协助您快速定位高级威胁、勒索软件以及定向性攻击

经过精心设计的高级威胁和定向攻击可轻松绕开传统安全防御进入您的网络，在长期潜伏过程中不断窃取您的敏感数据和重要信息，以达到其商业、经济、政治等目的。为了侦测高级威胁及定向攻击，安全专家及分析人员推荐使用高级侦测技术作为现行安全策略的有效补充，专门应对当下的定制化威胁。

亚信安全深度威胁发现设备 TDA 是一款 360 度的高级威胁检测产品，可掌握全网络的流量来侦测并响应高级威胁与未知威胁。TDA 能侦测所有端口及 100 多种通讯协议的应用，为用户提供最全面的网络威胁侦测。TDA 采用三层式的侦测方法，第一层是静态分析，第二层是动态分析及行为侦测，第三层是事件关联，目的就是为了发掘隐匿的攻击活动。TDA 根据静态分析、动态分析、事件关联的汇总分析结果来实现威胁侦测的可视化。其独特的侦测引擎加上定制化沙箱动态模拟分析，能快速发掘并分析恶意文档，恶意软件、恶意网页，违规外连、勒索软件以及传统防护无法侦测到的内网攻击以及定向式攻击活动。其深入的威胁情报分析能力能协助安全管理员快速响应，并可自动与亚信安全产品或第三方情报中心透过公开标准分享情报，建立一个实时的定制化体系来防范黑客攻击。

关键优势

更好的安全防护

- 多重侦测技术
- 监测所有网络流量
- 定制化沙盒分析
- 侦测勒索病毒及其内网攻击行为
- 完整的威胁情报

看得见的投入产出比

- 强化既有的安全解决方案投资
- 弹性的部署方式
- 安全运营工作自动化
- 可联动亚信安全网关、服务器及终端产品实施全面防护

关键能力

全面威胁检测 TDA透过分析所有端口及 100 多种通讯协议的应用来解析出定向性攻击、高级威胁以及勒索软件的攻击行为。并基于对高级威胁的精准分析能力，TDA可以侦测并定位出处于外网攻击，内网扩散，违规外连等高级威胁的各个攻击阶段的攻击行为。

高级侦测技术 使用了诸如文件、IP及Web信誉，移动应用程序信誉、静态分析，启发式分析，恶意文档分析，定制化沙盒分析、关联分析等多重侦测技术，用以侦测勒索软件、零日漏洞攻击、高级威胁以及攻击者行为。

定制化沙盒分析 使用了与您操作系统的配置、驱动、应用程序、语言版本等精确匹配的虚拟沙箱镜像，用于提升高级威胁的侦测率，减少由于使用普通沙箱镜像所导致的高级威胁以及勒索软件沙箱逃逸。

完整威胁情报 确保分析出的本地威胁情报能够快速与亚信安全全球云安全智能防护网络（Smart Protection Network）进行关联分析与实时同步，并透过其它亚信安全产品进行有效的联动响应。

定位勒索软件攻击 TDA可检测脚本模拟，零日威胁和密码保护的定向性勒索软件攻击。除了充分利用行为分析和信誉分析，透过定制化沙盒模拟可检测出大量的文档篡改，加密和备份功能的异动。

亚信安全联动威胁防御的重要部分

为了充分应对当前的威胁形势，我们需要多层次防御平台，提供完整生命周期的威胁防护。亚信安全联动威胁防御（Connected Threat Defense）是一种全新的网络安全模式，它提供了一套更好的方案快速防护、侦测并响应针对您组织的新型威胁，同时提升网络威胁的可见性及可控性。

- 防护：评估潜在威胁，为终端、服务器及应用提供主动防护
- 侦测：检测传统防御无法识别的高级恶意软件、通讯及行为
- 响应：通过实时共享威胁情报和产品联动，快速响应新型威胁
- 可视及可控：通过全网络和全系统的可视化能力，定性定量分析并评估威胁的影响和范围

检测和抵御

- 高级威胁和定向性攻击
- 零日恶意软件和文档漏洞
- 攻击者的网络活动
- 网页威胁（漏洞注入、网页挂马、隐蔽强迫下载）
- 电子邮件威胁（网络钓鱼、鱼叉式网络钓鱼以及其他社交工程邮件击）
- 数据隐蔽泄漏
- 僵尸、木马、蠕虫病毒
- 键盘记录器和犯罪软件
- 破坏性应用程序

技术规格

	TDA 3200 EE	TDA 6200 EE	TDA 11200 EE	TDA 30000 EE
设备规格	1U 机架设计	1U 机架设计	2U 机架设计	2U 机架设计
部署方式				
SPAN/TAP （监控）模式	有	有	有	有
性能				
吞吐量	500 Mpbs	1.0 Gbps	2.5 Gbps	6.0 Gbps
最高并发连接	60,000	240,000	500,000	2,000,000
分析能力				
恶意文件检测	有	有	有	有
网络恶意行为分析检测	有	有	有	有
信誉分析	有	有	有	有
移动设备病毒检测	有	有	有	有
动态沙盒分析	选购 1 个 *注	选购 1 个 *注	选购 1 个 *注	默认 20 个 *注
沙盒处理能力	800 混合文件/天	800 混合文件/天	800 混合文件/天	16,000 混合文件/天
关联分析	有	有	有	有
管理				
WEB 管理界面	有	有	有	有
内建分析报表	有	有	有	有
冗余电源	有	有	有	有
设备故障检测	有	有	有	有
硬件状态监控	有	有	有	有

* 注：亦可选择外部沙盒服务器 DDAN 扩容动态沙盒分析能力

深度威胁发现产品平台(Deep Discovery)

深度威胁发现设备 TDA 隶属深度威胁发现产品平台（Deep Discovery），该平台可在您企业的重要部署位置 – 网络、Web、邮件、终端等提供全方位的高级威胁防护。除TDA之外，它还包括：

深度威胁安全网关Deep Edge 是基于内容检测的统一智能安全网关。它不仅提供完整 的应用防火墙功能,更重要地是针对100多种常用网络协议提供了入侵防护、虚拟补丁、APT防护、零日漏洞检测、防恶意软件、防勒索软件、恶意网站过滤、网站分类访问、VPN数据过滤、垃圾邮件及恶意邮件过滤等多项高级内容安全检测及防护功能。

深度威胁分析设备DDAN 提供定制化沙箱分析用以增强亚信安全及第三方安全产品的威胁防护能力。DDAN可以为网络安全产品（如:TDA）、Web 和邮件安全产品（如:Deep Edge、DDEI）及服务器与终端安全产品（如Deep Security、OSCE）提供集中的动态沙箱分析,可疑威胁对象通过产品联动的方式自动提交给DDAN进行分析。DDAN使用多重侦测和防逃逸技术,侦测Windows及Mac操作系统上的高级恶意软件、勒索软件、零日漏洞攻击、C&C违规外联、以及多阶段下载攻击等恶意威胁。

深度威胁邮件网关DDEI 用来侦测和阻止社交工程邮件所导致的高级威胁及勒索软件攻击。它采用先进的恶意软件检测引擎、文档漏洞检测、嵌入式URL 分析,以及定制化沙箱分析等技术,可快速识别并阻止或隔离这些定向攻击邮件。

AsiaInfo | 亚信安全

北京：86-10-5825 6889
上海：86-21-6384 8899
广州：86-20-8755 3895
南京：86-25-5851 2888
天津：86-22-6621 1165
成都：86-28-6687 6200
杭州：86-571-8190 3773

欲知更多网络安全及相关产品信息，
请拨打免费咨询电话：800-820-8876
或登录亚信安全官网：www.asiainfo-sec.com