亚信安全™

深度威胁分析设备 DDAN

防范高级威胁和定向攻击的深度定制化沙箱分析组件

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。

通过提供可扩展的定制化沙箱及高级威胁分析能力，亚信安全深度威胁分析设备DDAN提升了来自亚信安全及第三方既有安全投资的价值。通过多种渠道侦测到的可疑威胁对象将会送给DDAN做高级威胁沙箱分析，一旦威胁被确认，新型威胁特征会自动更新给整体安全解决方案以实现威胁的进一步治理和预防。

关键能力

定制化沙箱

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沙箱逃逸。定制化沙箱环境采用了安全外部实时模式用于确认和分析多阶段下载攻击、恶意URL、命令与控制（C&C）等高级威胁，同时也支持自动和手动上传文件及URL样本。

灵活的部署

DDAN既可以作为独立沙箱部署，又可以作为外置增强沙箱组件与深度威胁发现产品平台（Deep Discovery）的相关产品协同部署。单台DDAN设备可支持多达60个沙箱，考虑到产品的高可用性和可扩展性， DDAN既支持多台设备的热备和冷备，又支持集群部署。

高级侦测技术

DDAN使用了诸如文件、IP及Web信誉，静态分析，启发式分析，行为分析，大数据分析、关联分析等多重侦测技术，可快速分析可疑文件中携带的多阶段恶意软件，恶意外联通讯、以及C&C服务器等威胁对象。

- 广泛的文档分析　DDAN使用多重分析引擎及定制化沙箱，可以分析广泛的文档类型：Windows可执行程序，MS　Office文件、PDF、Web内容、压缩文件等，用户可根据文件类型自定义沙箱分析策略。
- 文档漏洞检测　使用静态分析及定制化沙箱，DDAN可以侦测藏匿在普通文档对象中的高级恶意软件及漏洞攻击。
- URL分析　DDAN可以对邮件中嵌入的URL以及其他产品提交的URL执行沙箱分析。
- Web API及手动提交样本 任何产品和威胁分析人员可以通过DDAN的Web API接口提交可疑威胁样本。
- 本地威胁情报IOC共享　DDAN会自动共享本地威胁情报IOC给亚信安全或第三方安全产品。
- 同时支持Windows和Mac操作系统。

侦测勒索软件

DDAN不但可以使用特征码和信誉库等已知威胁信息发现勒索软件，还可以侦测与常见勒索软件相关的脚本模拟、零日漏洞、定向及密码保护的恶意软件。同时，定制化沙箱可以侦测到大规模文件篡改、文件加密、存储备份篡改等勒索软件触发的异常行为。

核心价值

提升侦测能力

- 超越普通沙箱的卓越侦测能力
- 让高级威胁沙箱逃逸无处遁形

看得见的投入产出比

- 通过产品协同、威胁情报共享以及额外的处理性能提升，增加既有安全投资的价值
- 减少可疑威胁对象的人工分析成本
- 避免勒索软件造成的昂贵的补救成本
- 支持分布或集中的灵活部署模式

NSS LABS 推荐

亚信安全™深度威胁解决方案

连续三年

最优

攻击检测

99.8% 侦测率

ICSA labs 认证

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

技术规格

深度威胁分析设备 DDAN			
产品型号	DDAN 310	DDAN 610	DDAN 1100
支持文件类型	ell, chm, class, dll, doc, docx, exe, gul, hwp, hwpx, jar, js, jse, jtd, lnk, mov, pdf, ppt, pptx, ps1, rtf, swf, vbs, vbe, xls, xlsx, xml 等		
支持操作系统	Windows XP, Win7, Win8/8.1, Win10, Windows Server 2003, 2008, 2012, Mac OS 等		
处理能力	15,000 样本/天	30,000 样本/天	60,000 样本/天
硬件规格	1U机架设计	1U机架设计	2U机架设计
电　　源	550W冗余电源	550W冗余电源	750W冗余电源

深度威胁发现产品平台（Deep Discovery）

深度威胁分析设备DDAN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DDAN之外，它还包括：

- **深度威胁发现设备TDA** 是一款网络全流量安全监控产品。它使用了包括沙箱分析在内的多重侦测技术，能监控所有端口及100多种通讯协议的应用，可快速定位并响应APT攻击与未知威胁，为用户提供最全面的网络威胁侦测。
- **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。
- **深度威胁终端取证与行为分析系统DDES** 是一套内容敏感的终端安全监控系统，它详细记录并报告了基于系统内核层面的各类重要活动及通讯事件，使威胁调查人员可以快速评估攻击的本质、影响和范围。利用深度威胁发现产品平台（Deep Discovery）及其他来源所提供的威胁情报IOC信息，DDES可以执行跨所有用户终端和服务器的多层次深度内容查询。

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