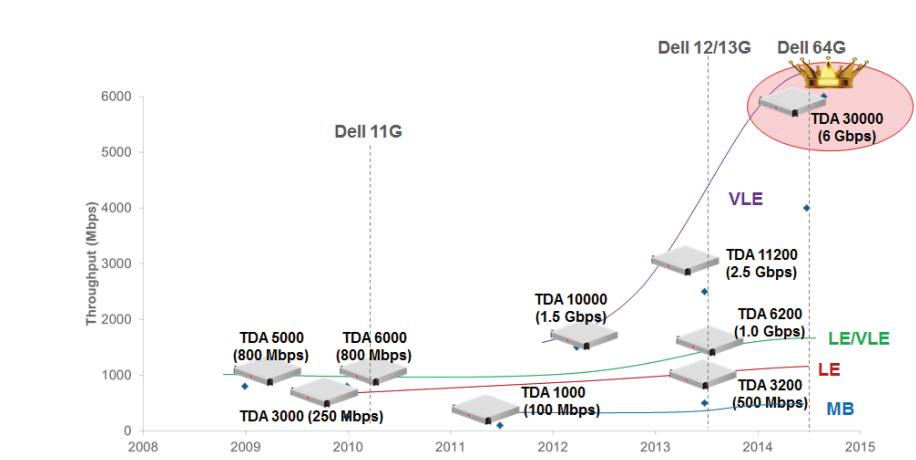


亚信安全™ 深度威胁发现设备TDA产品参数

	TDA 3200EE	TDA 6200EE	TDA 11200EE	TDA 30000EE
硬件规格				
设备规格	1U机架	1U机架	2U机架	2U机架
处理器	四核处理器	四核处理器 x 2	六核处理器 x 2	十二核处理器 x 2
内存	8GB	16GB	16GB	64GB
硬盘	2 x 500GB以上(RAID1)	2 x 500GB以上(RAID1)	2 x 500GB以上(RAID1)	8 x 600GB以上(15KRPM SAS), RAID 10
性能				
吞吐量	500Mbps	1.0Gbps	2.5Gbps	6.0Gbps
最高并发连接	30,000	120,000	250,000	2,000,000
可连接性				
监听端口	3个千兆铜口，最多可扩展至9个铜口或4个光口	5个千兆铜口，最多可扩展至9个铜口或4个光口	7个千兆铜口，最多可扩展至19个铜口或8个光口	2个千兆铜口，2个光口，最多可扩展到8个千兆铜口或8个光口
管理端口	1个千兆以太网铜口	1个千兆以太网铜口	1个千兆以太网铜口	1个千兆以太网铜口
命令行管理端口	1 x RS-232	1 x RS-232	1 x RS-232	1 x RS-232
运行模式				
SPAN端口监控	有	有	有	有
分析能力				
恶意文件检测	有	有	有	有
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	选购	选购	默认
沙盒处理能	800文件/天	1,000文件/天	1,000文件/天	有
关联分析	有	有	有	有
管理				
Web管理界面	有	有	有	有
内建报表	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
物理参数				
高度	1.69英寸	1.69英寸	8.73厘米	8.73厘米
宽度	17.09英寸	17.09英寸	48.2厘米	48.2厘米
厚度	25.29英寸	25.29英寸	75.58厘米	75.58厘米
重量	19.9kg	19.9kg	29.2kg	32.5kg
电源	350W x 2	550W x 2	750W x 2	750W x 2

深度威胁发现设备 TDA 产品型号概览





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

亚信科技（成都）有限公司保留对本文档以及此处所述产品进行更
改而不通知的权利。在安装及使用本软件之前，请阅读自述文件、
发布说明和最新版本的适用用户文档，这些文档可以通过亚信科技
的以下Web 站点获得：
<http://www.asiainfo-sec.com.cn/download/zh-cn/>

亚信安全™
深度威胁发现设备 TDA
实时应用安全的可见性、洞察力和控制

高级持续性威胁和针对性攻击已清楚地证明其抵御传统安全防护、保持长期不被检测到以及隐藏泄露公司数据和知识产权的能力。IT消费化和云计算等技术发展趋势进一步加剧了这些攻击的严重性，削弱了外围安保的作用，从而使网络更容易遭到攻击。分析人员和专家已认识到这些问题，并建议企业加强其安全监测及防御，采用专业的针对高级持续性威胁的检测技术和前瞻性的实时威胁管理流程。

亚信安全™ 深度威胁发现设备 TDA 为企业和政府组织提供了降低高级持续性威胁攻击(APT)和针对性攻击风险所需的全网范围的可见性、洞察力和控制。深度威胁发现设备以独特方式实时检测和虚拟模拟分析技术，提供防止、发现和抑制针对公司数据的攻击所需的深入分析和行动情报。

亚信安全™ 深度威胁发现设备 TDA 集成网络封包,应用内容,文件过滤与云计算安全侦测引擎可以在威胁生命周期的各个阶段识别恶意内容、通信和行为，从而以最低的误判率和最大的覆盖范围提供最佳的检测。通过对高级持续性威胁恶意软件和隐蔽式攻击者行为的检测和深入分析，深度威胁发现设备可为企业和政府组织提供在不断发展的网络环境中检测APT和针对性攻击所需的可见性和情报。



检测和抵御

- APT 和针对性攻击
- 零日恶意软件和文档漏洞
- 攻击者的网络活动
- Web威胁(漏洞、隐蔽强迫下载)
- 电子邮件威胁（网络钓鱼、鱼叉网络钓鱼）
- 数据隐藏泄露
- Bot、特洛伊木马、蠕虫病毒
- 按键记录软件和犯罪软件
- 破坏性应用程序

APT威胁生命周期

如今，高级持续性攻击使用多阶段方式来窃取重要数据——获取入口点，下载其他恶意软件，打开后门程序访问，找到并危害目标系统，然后上传数据。

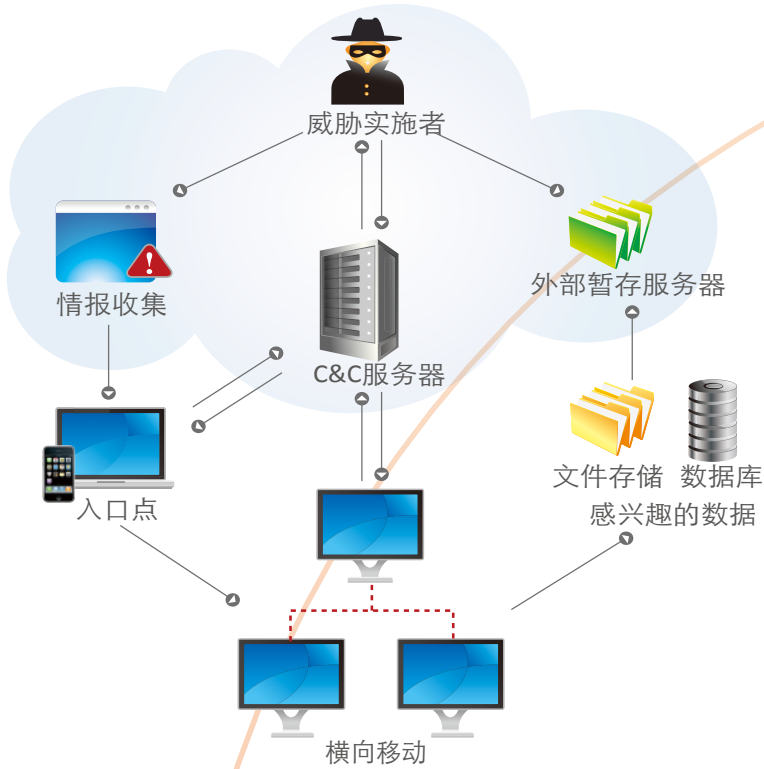
尽管笔记本电脑数据危害可快速发生，但从初始入侵到目标数据受到危害通常需要几天或几周的时间。实际发现并完全抑制危害所用的时间可能为几个月。在此期间，企业网络中潜伏着入侵者，其目的是持续危害重要数据。

深度威胁发现设备的工作方式

APT 和针对性攻击已证明可避开标准外围、网络和端点安全防御的能力。威胁发现设备专门用于检测 APT 和针对性攻击——在攻击生命周期的各个阶段识别反映高级恶意软件或攻击者活动的恶意内容、通信和行为。

威胁发现设备使用3个层面的检测方案来执行初始检测，然后进行模拟和关联，最后通过最终的交叉关联发现隐蔽的高级持续性威胁活动以及其他只有通过长期观察才能发现的隐蔽活动。专业的检测和关联引擎可提供最准确、最新的防护，并辅之以由亚信安全云计算安全智能防护网络和专业威胁研究人员提供的全球威胁情报。结果是检测率高，误判率低，并提供深入的事件报告信息，以加快攻击的抑制。

	攻击检测	检测方法
恶意内容	- 包含嵌入文档漏洞的电子邮件 - 隐蔽强迫下载 - 零日攻击与已知恶意软件	- 解码与解压缩嵌入文件 - 可疑文件的沙盒模拟 - 浏览器漏洞套件检测 - 恶意代码扫描（签名和启发式技术）
可疑通信	- 针对以下所有恶意软件的 对外连网通信：僵尸病毒、下载软件、数据窃取、蠕虫病毒和混合性威胁 - 攻击者实施的后门程序活动	- 通过动态列入黑名单、白名单进行的目标分析（URL、IP、域、电子邮件、IRC 通道等） - 云计算安全智能防护网络 URL 信誉 - 通信行为识别规则
攻击行为	- 恶意软件活动：传播、下载、发送垃圾邮件等 - 攻击者活动：扫描、暴力攻击、服务漏洞利用等 - 数据隐蔽泄露	- 基于规则的启发式分析 - 对 80 多种协议和应用程序(含基于HTTP的应用程序)的使用情况进行识别和分析



主要功能

高级持续性威胁检测
威胁发现设备通过对所有类型的网络流量进行非入侵性、单纯侦听的检测，专注于在攻击生命周期的各个阶段识别反映高级持续威胁的恶意软件或攻击者活动的恶意内容、通信和行为。

- **专用的威胁引擎**和多级关联规则提供最佳的检测和最低的误判率
- **虚拟分析程序**使用沙盒模拟，提供对可疑内容的其他检测和完全的取证分析
- **云计算安全智能防护网络**情报和专业威胁研究人员提供不断更新的检测情报和关联规则，以识别攻击

威胁跟踪、分析和处理措施

威胁发现设备具有独特的高性能体系结构，旨在满足所有规模的客户严格且多样的容量要求。上至数千兆位的公司主干网，下至远程办公地点，该产品在所有硬件、软件和虚拟设备上均可用。

专家百科

为您提供了解及应对攻击所需的威胁情报

- 直接访问亚信安全情报门户以获取特定攻击或恶意软件的信息
- 抑制和补救建议
- 针对特定威胁更新的说明



灵活的大容量部署

威胁发现设备控制台提供直观的实时威胁可见性和深入分析，以便安全管理人员可以专注于实际风险、进行取证分析并快速解决问题。

实时威胁控制台

威胁可见性和深入分析触手可及

- 快速访问小组件提供的关键信息
- 深入分析攻击特征、行为和通信
- 地图系统识别恶意通信的来源

重点资产观察名单

提供以风险为中心的监控，监控严重性高的威胁和高价值资产

- 重点跟踪指定主机上的可疑活动和事件
- 通过威胁检测或客户选择来确定要跟踪的主机
- 详细的事件时间线可跟踪涉及目标主机的所有攻击活动

企业威胁管理战略整体价值

