亚信安全™

深度威胁邮件网关 DDEI

侦测并阻止社交工程邮件导致的高级威胁及勒索软件攻击

高级威胁和定向攻击已经证明了它们绕开传统安全防御实施网络攻击和窃取敏感数据的能力。亚信安全的一项最新研究显示，超过90%的定向攻击始于社交工程邮件，这类邮件通常含有传统邮件或终端安全产品无法侦测的恶意附件或URL。

攻击者经常将这些恶意附件或URL伪装成常规邮件内容，精心制作成社交工程邮件发送给毫无防备的企业员工，用于实施APT或勒索软件等定向攻击。亚信安全深度威胁邮件网关 DDEI 使用高级侦测技术，专门用于侦测并阻止此类社交工程邮件的攻击。DDEI通常可以采用MTA（拦截），BCC（监控），或SPAN/TAP（监控）模式进行部署。

关键能力

无缝协同

可以和企业现有的传统邮件网关无缝协同工作，专门用于侦测社交工程邮件携带的包括勒索软件在内的高级恶意软件。

强大的分析技术

可侦测零日漏洞攻击，高级威胁，勒索软件以及其他攻击行为。它使用了诸如文件、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，以及定制化沙箱分析等技术侦测已知和未知威胁，并且能够和亚信安全全球云安全智能防护网络（Smart Protection Network）共享本地及云端威胁情报。

灵活的策略

可根据威胁的不同级别设置不同的邮件处理策略：拦截、隔离、带威胁标记转发、移除并替换恶意附件、日志记录、告警收件人等。

定制化沙箱分析

提供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。DDEI提供了集成的定制化沙箱功能。

阻止加密勒索软件攻击

事实证明，邮件是勒索软件惯用的攻击载体，从社交工程邮件发起的那一刻开始，第一个受害者会在40秒到一分钟之内打开恶意邮件，您企业的所有用户将置身于极度风险之中。

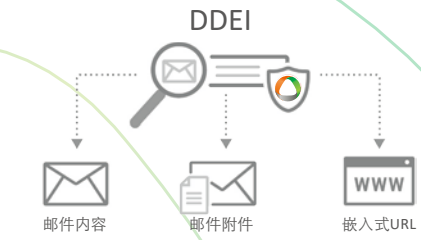
核心价值

更好的安全防护

- 阻止大多数发起APT攻击所使用的社交工程邮件
- 在破坏产生之前侦测并拦截勒索软件
- 通过定制化沙箱分析，发现传统邮件安全产品无法侦测的高级威胁

看得见的投入产出比

- 阻止社交工程邮件，避免昂贵的事后补救措施
- 拦截勒索软件，再也不用担心支付高额的赎金或数据恢复费用
- 可以和现有的邮件安全解决方案无缝协同工作
- 通过阻止、隔离、记录、移除威胁、通知收件人等方式减少恶意邮件威胁



NSS LABS 推荐

深度威胁解决方案
连续3年
有效攻击检测
推荐

99.8% 侦测率

ICSA labs 认证

DDEI能够通过以下方法侦测并阻止面向毫无防备的邮件用户发起的勒索软件攻击：

- 针对已知勒索软件：特征码及信誉分析技术
- 针对未知勒索软件：通讯指纹、脚本模拟、零日漏洞、定向及密码保护的恶意软件分析技术
- 通过定制化沙箱分析大规模文件篡改、文件加密、存储备份篡改等异常行为

一旦侦测到勒索软件，DDEI会将其拦截，避免发送给最终收件人，阻止险些发生在用户端的数据加密。

技术规格

深度威胁邮件网关 DDEI			
型号及规格	DDEI 5100	DDEI 7100	DDEI 9100
部署选项	MTA（阻止）、BCC（监控）和SPAN/TAP（监控）模式		
处理能力	100,000 封电子邮件/天	400,000 封电子邮件/天	800,000 封电子邮件/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

侦测及保护

- 定向攻击及高级威胁
- 零日恶意软件及文档漏洞攻击
- 勒索软件攻击
- 攻击行为及恶意网络活动
- 漏洞注入及网站挂马攻击等Web威胁
- 社交工程钓鱼等邮件威胁
- 数据泄漏及渗透
- 僵尸，木马，蠕虫，键盘记录器
- 破坏性应用程序

深度威胁发现产品平台（Deep Discovery）

深度威胁邮件网关DDEI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DDEI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 和IMSA）及服务器与终端安全产品（如Deep Security、OSCE和DDES）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

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/