DefensePro：实时行为攻击缓解设备

非官方中文译本•安天技术公益翻译组 译注

文档信息			
原文名称	DefensePro: Real-Time, Behavioral Based Attack Mitigation		
原文作者	Unknown	原文发布单位	Radware
作者简介			
原文出处	http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
免责声明	本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

DefensePro 有哪些功能？

网络犯罪分子不遵循常规的作息时间。相反，他们昼夜不寐的去寻找和开发网络中存在的漏洞。你需要综合性的企业网络安全设备以满足当今日新月异的安全挑战。

Enter Radware's DefensePro —— 一款实时行为攻击缓解设备，能够保护你的基础设施免于网络应用设备宕机、应用设备漏洞利用、恶意代码传播、网络异常、信息窃取及其他新兴的网络攻击。

DefensePro 提供顶级的安全保护措施，包括 DDoS 攻击缓解措施和基于 SSL 的保护措施，以充分保护你的应用和网络不受已知的、新兴的网络安全攻击形式的攻击，如 DoS 攻击、DDoS 攻击、互联网饱和度及基于 SSL 的攻击等，具体措施如下：

（AMS）不影响合法流量的专用保护硬件

DefensePro 使用基于 Radware's OnDemand Switch 的专用硬件平台，其吞吐量高达 40Gbps。该设备内嵌两个独特的专用硬件组件：一个 DoS 缓解引擎（DME），在不影响合法流量的情况下，组织大量的 DDos 攻击、DoS 攻击和洪水式攻击；一个字符串匹配引擎（SME），用于加速签名检测。

集中式的攻击管理、监控和上报

APSolute Vision 为大量的 DefensePro 设备提供了集中式的管理、监控和上报解决方案。它提供了用户实时识别、优先级及对策略违反、网络攻击和内部威胁的响应。

全套的安全模块

入侵防御系统（IPS）、网络行为分析（NBA）、拒绝服务防御（DoS）、引擎声誉管理及 SSL 攻击防御等。除了签名检测外，它还采用多个检测&缓解模块，包括自适应行为分析和挑战响应技术。

内嵌的精准度，外路径的可扩展性

DefensePro 设备可内嵌安装部署在“净化中心”或者是“净化中心”的外路径处，旨在最短的时间内提供最大力度的缓解精准性。

DefensePro 具有哪些更突出的功能？

基于标准的特征码检测技术阻止已知的漏洞被利用，DefensePro 包括被实时特征码技术保护的专利，该技术可在完全不需要人工参与和不阻断用户合法流量的条件下，检测和缓解新兴的实时网络攻击，如 0day 攻击、DoS/DDoS 攻击和应用程序滥用攻击等。

DefensePro 是 Radware 下一代 AMS（攻击缓解系统：一套专为最先进的互联网传播攻击设计的专利技术）的核心组成，AMS 在以下方面具备数据中心无法进行的网络攻击检测和缓解能力：

云托管的服务和应用

工具、服务器和应用需要在虚拟环境下的保护

移动工作人员越来越依赖于远程访问企业内部的应用程序和软件即服务（SaaS）

先进的检测和缓解技术需要转移到开放式的网络结构