Hillstone
山石网科

山石网科入侵检测系统

L2-L7全面威胁检测能力

全面的环境感知能力

业界超高性价比

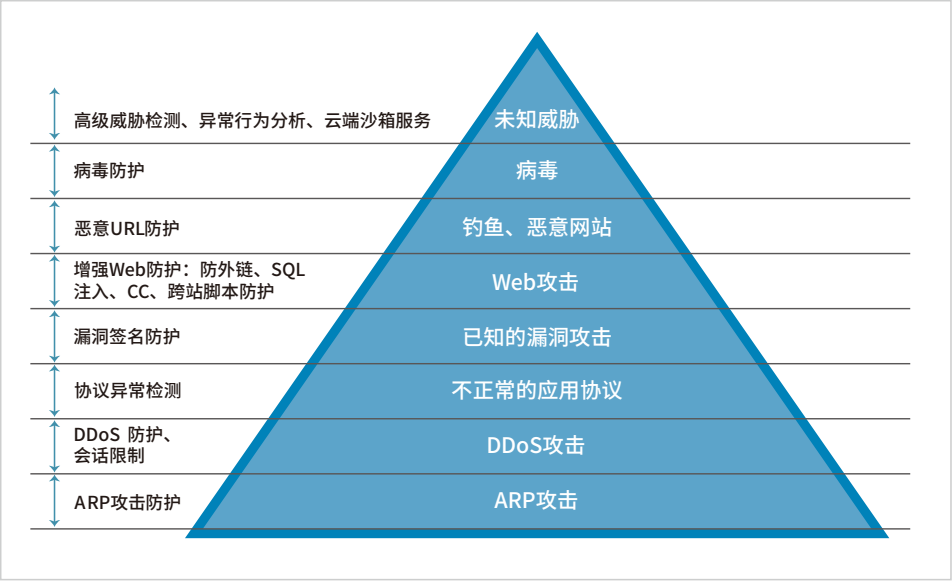
D 系列	SG-6000-D660 / SG-6000-D860 / SG-6000-D1600 / SG-6000-D1800 SG-6000-D2600 / SG-6000-D2800 / SG-6000-D5600 / SG-6000-D5800 SG-6000-D12600 / SG-6000-D12800 / SG-6000-D15600

山石网科D系列是专用于网络入侵攻击检测的安全产品，可广泛部署于政府、企业、高校、运营商等行业的互联网边界、服务器区域、内网威胁检测等应用场景中。

产品亮点

L2-L7 全面威胁检测能力

当前的体系化攻击往往尝试从业务系统中最薄弱的环节进行攻击渗透，系统中任何一个薄弱点都有可能成为攻击者的攻击突破目标。但由于攻击者从哪个节点突破无法提前被预知，客户需要全面的 L2-L7 威胁检测能力。



山石网科 D 系列拥有多重的威胁检测能力，支持对底层的 ARP 攻击、网络层 DoS/DDoS 攻击、常见协议的异常、病毒蠕虫木马、海量的恶意 URL 以及常见的 Web 攻击等一系列已知和未知威胁进行全面检测。全平台内嵌 8000+ 入侵攻击特征，超过 1300 万特征的病毒库，能够检测常见的病毒、蠕虫、后门、木马、僵尸网络攻击以及缓冲区溢出攻击和漏洞攻击，最大范围覆盖已知的流行入侵攻击行为的检测；同时，D 系列还支持自定义攻击特征，能够及时针对 0Day 漏洞定制防御规则，并最大化满足用户的特殊防护需求。此外，随着 Web 应用的丰富，针对 Web 的攻击越来越多，山石网络 D 系列还提供了针对 Web 攻击的检测能力，包括 SQL 注入、XSS 注入、Web 访问控制、网站外链防护以及 CC 攻击的检测能力。在 L2-L7 全方位的攻击防护基础上，山石网科还和微软 MAPP 等威胁防护领域的专业机构展开合作，致力于为客户提供更高的入侵检测率。

针对未知威胁的检测能力

恶意软件经常采用变形、隐藏技术的处理，使得自身的特征出现变化，成为“未知威胁”以躲避入侵检测系统的检测。山石网科入侵检测系统还可以和山石云 · 影联动，通过云沙箱技术来发现文件中的未知威胁。

山石网科网络入侵检测系统在网络上侦听数据流，识别各类的网络协议，捕获可疑文件并提交到山石云 · 影分析引擎。当接收到可疑文件后，山石云 · 影的沙箱分析引擎会根据文件的特性选择最佳的仿真环境来打开文件，捕获相关的执行行为，并利用已建的机器学习模型来判别该可疑文件是否是恶意文件。如果可疑文件被判定为恶意，沙箱会及时报警，并将该文件的执行行为、判定结果和相关静态特征反馈给入侵检测系统。

多视角、丰富易用的报表

山石网科 D 系列入侵检测系统提供了多视角和丰富易用的报表。便于客户单位不同职责的管理员从不同视角进行管理，在报表生成方面，有安全风险概览、业务系统风险详情、网络威胁详情、网络流量分析和系统运行情况五大项。

全面的环境感知能力

你无法保护你看不见的内容！山石网科 D 系列网络入侵检测系统提供了全面的环境感知能力，可提供基于应用、用户、访问内容三个维度的环境感知。

山石网科 D 系列提供了深度应用感知能力：

- 通过应用内容特征、应用行为特征及关联分析等多种手段，D 系列可准确识别 3,000 多个网络应用，其中包括几百多种移动应用和云应用，同时可识别基于 SSL 加密流量的应用。
- D 系列针对每一个应用提供详细的应用背景知识，管理员可根据这些信息制定针对性的安全策略以避免特定应用风险，这些背景知 识包括应用的风险等级、应用是否存在已知漏洞、应用是否存在大量带宽消耗可能、应用是否有文件传输行为等多维度信息。
- D 系列还提供基于应用的流量、并发连接分布、应用的威胁分布等多维度可视化能力。

山石网科 D 系列还提供了深入的用户及内容感知能力，可非常清晰的了解用户、业务系统的流量、并发连接、威胁等多个情况，同时，可了解用户正在访问哪些内容，哪些内容访问排名最高。

文档编号：EX-08-DSeries-5.5R2-0419-Ch-02

官方微信　　官方微博

中国 · 销售与服务热线：400-828-6655