

Hillstone[®]
山石网科

山石网科网络入侵防御系统

综合的网络威胁检测防御平台
全生命周期的高级威胁防护
基于 IPv6 的多维安全防护
多视角、丰富易用的报表
全面的环境感知能力

S 系列

SG-6000-S600 / SG-6000-S800 / SG-6000-S1060 / SG-6000-S1560 / SG-6000-S2060 /
SG-6000-S2160 / SG-6000-S2560 / SG-6000-S2660 / SG-6000-S3060 / SG-6000-S3260 /
SG-6000-S3560 / SG-6000-S3860 / SG-6000-S3960 / SG-6000-S5560 / SG-6000-S6680 /
SG-6000-S2680-GC

www.hillstonenet.com.cn

产品亮点

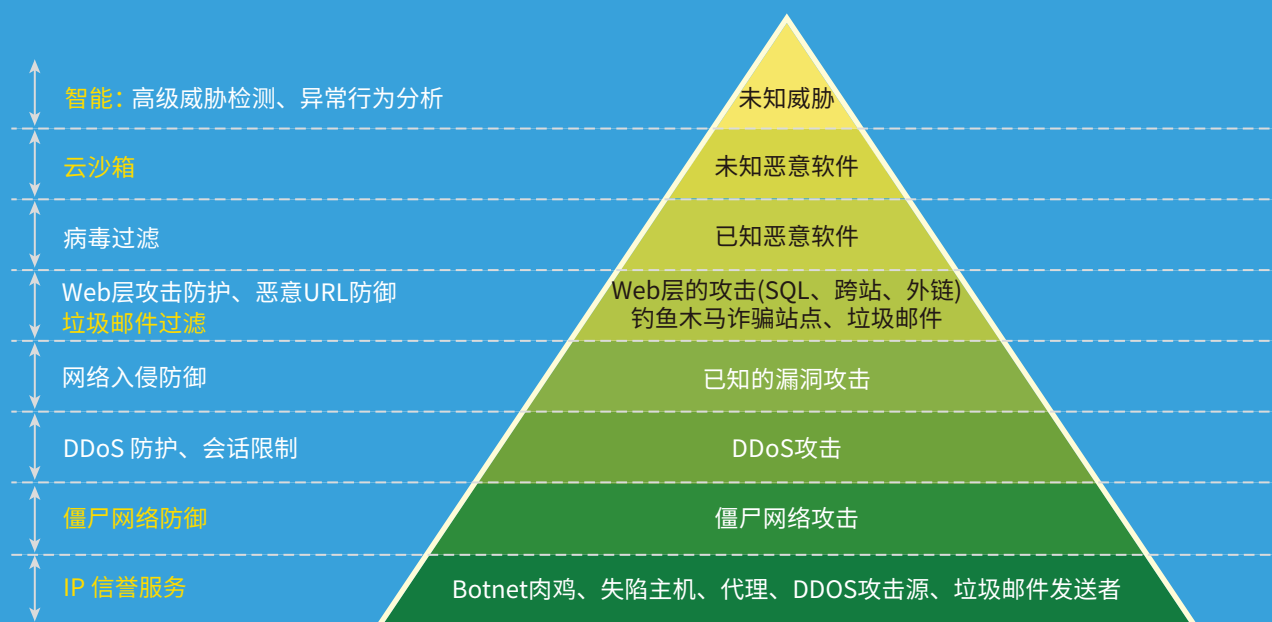
综合的网络威胁检测防御平台

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预知，用户需要综合的威胁检测防御平台。山石网科 S 系列拥有多重的威胁检测和防御能力，支持对僵尸网络攻击、DDoS 攻击、已知协议漏洞利用、Web 攻击、垃圾邮件、钓鱼、木马病毒和恶意软件等一系列网络入侵威胁进行检测及防御。

山石网科 S 系列具备智能的威胁检测防御功能，支持高级威胁检测和异常行为分析。支持核心资产服务器的重点监控和未知威胁检测。通过建立行为数据模型，可以有效发现各类未知威胁和服务器异常行为。山石网科 S 系列为用户提供 L2-L7 全面威胁防御能力，实现对底层的 ARP 攻击、网络层 DoS/DDoS 攻击、20 多种常见协议的异常、病毒蠕虫木马、恶意 URL 以及 Web 攻击等一系列入侵威胁进行检测及防御，还提供了增强的 Web 攻击防护能力，包括 SQL 注入、XSS 防御、CSRF 防护、高频交易限制、Web 访问控制、网站外链防护以及 CC 防护能力。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。

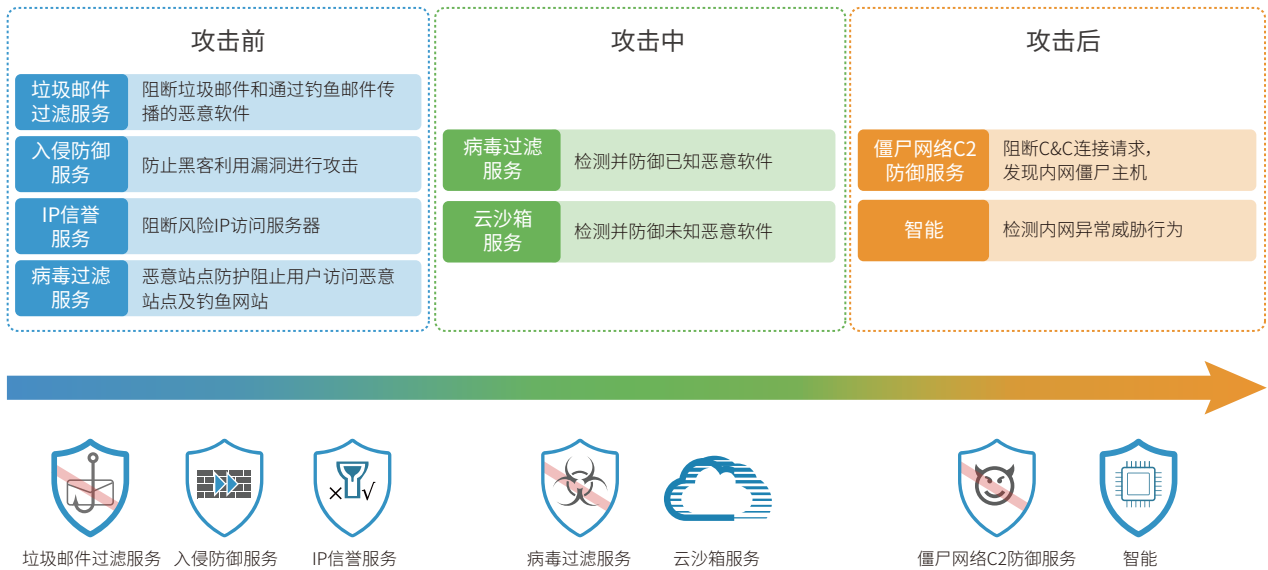
S 系列还提供多种安全增值服务：

- **IP 信誉服务：**精准识别 DDoS 攻击者、Tor 节点和暴力破解者等多种类型的风险流量，并在网络边界进行过滤，为用户提供安全的防护体验。
- **僵尸网络防御服务：**监控内网主机的 C&C 连接行为，有效发现内网受感染的僵尸肉鸡。通过阻断 C&C 连接，防止僵尸网络或高级威胁进一步破坏企业内网。
- **垃圾邮件过滤服务：**云端情报中心实时分析全球范围内最新的垃圾邮件。通过与云端情报库保持实时连接，并采用邮件哈希与云端交互，快速、高效对垃圾邮件进行分类检测和防御。
- **云沙箱服务：**拥有海量恶意样本库以及仿真分析环境，通过静态样本检测和动态行为分析，有效发现未知威胁。并通过威胁情报共享，实现单点发现，全局防护。



全生命周期的高级威胁防护

山石网科 S 系列具备攻击前、攻击中和攻击后丰富的威胁检测和防御手段。通过入侵防御服务、垃圾邮件过滤、IP 信誉服务和病毒过滤等,可以在网络攻击发生前进行阻断和防护。通过病毒过滤和云沙箱服务,对攻击过程中的入侵威胁进行防护。即使攻击已经发生,通过僵尸网络防御服务和山石智能也可以有效发现内网异常行为,阻断入侵威胁传播。



基于 IPv6 的多维安全防护

山石网科 S 系列具备全面的 IPv6 功能,支持业务可视化管理,精细化管控和多维安全防护。支持流量监控,用户识别,应用识别和丰富的日志报表功能,为用户提供从网络到业务应用的可视化管理。精细化管控包括安全策略、应用控制、用户管控和 URL 过滤等。强大的网络入侵检测和防御,高性能病毒过滤,攻击防护和上网行为审计功能,构建多维的安全防护体系。

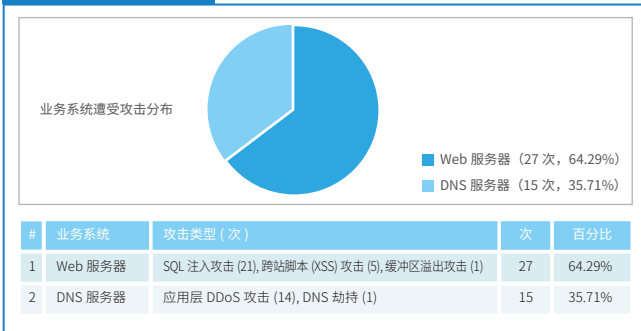


多视角、丰富易用的报表

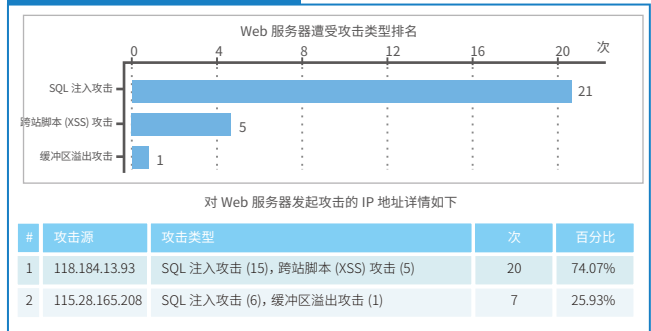
山石网科 S 系列提供了多视角和丰富易用的报表。便于客户单位不同职责的管理员从不同视角进行管理,在报表生成方面,有安全风险概览、业务系统风险详情、网络威胁详情、网络流量分析和系统运行情况五大项。



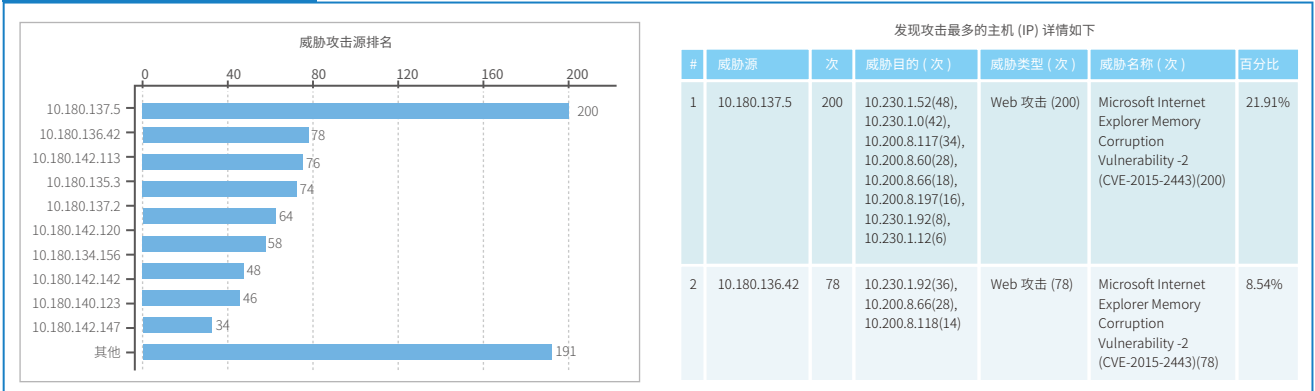
CIO 视角：安全风险概览



业务系统管理员视角：安全风险详情



安全管理员视角：威胁类型详情及汇总



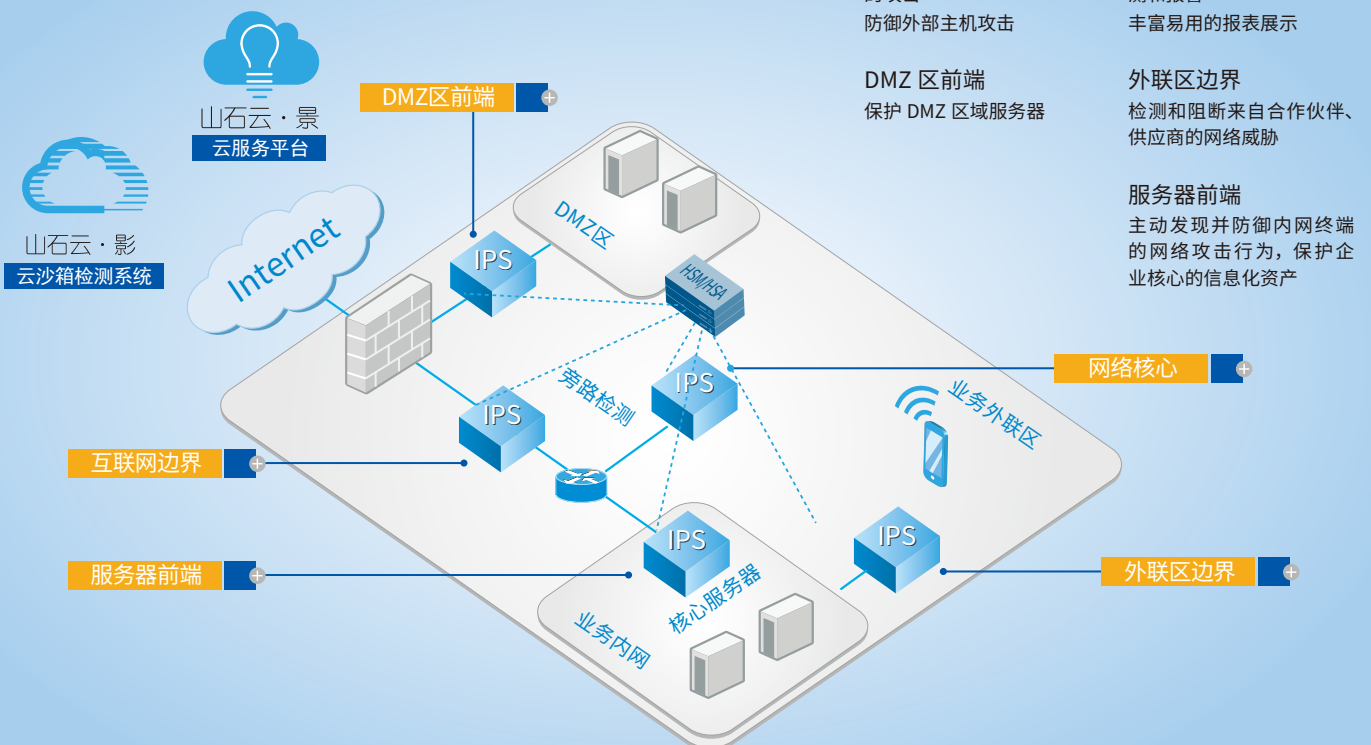
全面的环境感知能力

山石网科 S 系列能够全面感知网络流量中的用户、应用、内容，提高用户对网络环境的感知能力。

- 精确识别 3000 多个网络应用、几百余种移动应用和云应用，包含 SSL 加密流量的应用；
- 全面感知应用背景知识详情、提前规避风险，能够提供包含风险等级、是否存在已知漏洞、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，管理员可根据这些信息提前制定针对性的安全策略以避免特定应用风险；
- 提供基于应用、用户、内容的威胁、流量、并发连接等多维度可视化呈现。



典型部署场景





Copyright © 2019, 山石网科版权所有, 保留所有权利。

Hillstone、Hillstone Networks 标识、山石网科、StoneOS、StoneManager、Hillstone PnPVPN、UTM Plus 均为山石网科所属商标。
所有其他商标和注册商标均为其各自公司的财产。

本文所包含信息可能会有所修改, 恕不另行通知, 如需最新信息请浏览山石网科网站 (www.hillstonenet.com.cn)
科创板股票代码: 688030

文档编号: NIPS-S-3.2-Y19M10-CH-V17



官方微信



官方微博

中国 · 销售与服务热线: 400-828-6655