山石云瞻威胁情报服务概述

随着信息化和网络的高速发展，针对我国关键基础设施及政府网站等的攻击事件高发，特别是实时性更强、传播规模更广的挖矿病毒、勒索软件等网络攻击行为。传统的安全防御方式难以应对高级持续性威胁（APT）、0day 等新型网络威胁。威胁情报的出现改变了以往被动检测为主的防护模式，利用大数据等技术手段以更加智能的方式掌握网络安全事件、重大漏洞、攻击手段等信息，并在第一时间采取预警和应急响应等工作,威胁情报的应用和不断落地，使得安全防御更加智能。

山石网科推出山石云瞻威胁情报服务，旨在帮助用户提升网络威胁主动防御水平，更好的应对威胁。

服务亮点

热点威胁情报主动推送，提前一步防御威胁

山石云瞻威胁情报中心结合全球情报和热点威胁，第一时间将业界最高危的威胁事件情报主动推送到设备端，帮助用户聚焦高危重点威胁，发现未知威胁、0day 攻击等；并提供安全事件详情，帮助用户了解设备的防护状态，提供针对性防护措施或者防护建议，实现快速响应；同时帮助用户了解企业资产是否已存在热点高危威胁，提供持续地威胁检测分析。

威胁事件溯源分析，高位视角洞察威胁

山石云瞻威胁情报服务帮助管理员从海量告警信息中自动聚焦重点威胁，提高运维效率。同时通过与云端威胁情报中心联动丰富威胁信息，实现威胁事件溯源分析，及时应对关键威胁。

本地安全设备协同联动，提升威胁检测能力

山石云瞻威胁情报中心针对威胁情报进行深度整合，将威胁情报数据，比如 IP、域名、AV 等一些机读情报自动化集成到山石网科的安全网关设备中。通过云端与本地的智能协同联动，可实现及时、有效、精准的阻断，有效提高本地的威胁检测能力，本地威胁检测特征库的时效性、准确性和流行覆盖度都将优于传统的威胁特征库检测。同时山石云瞻云端威胁情报中心内置的海量情报可提供更加丰富的画像内容和人读情报，用作安全高级人员手工查询和高级威胁分析。

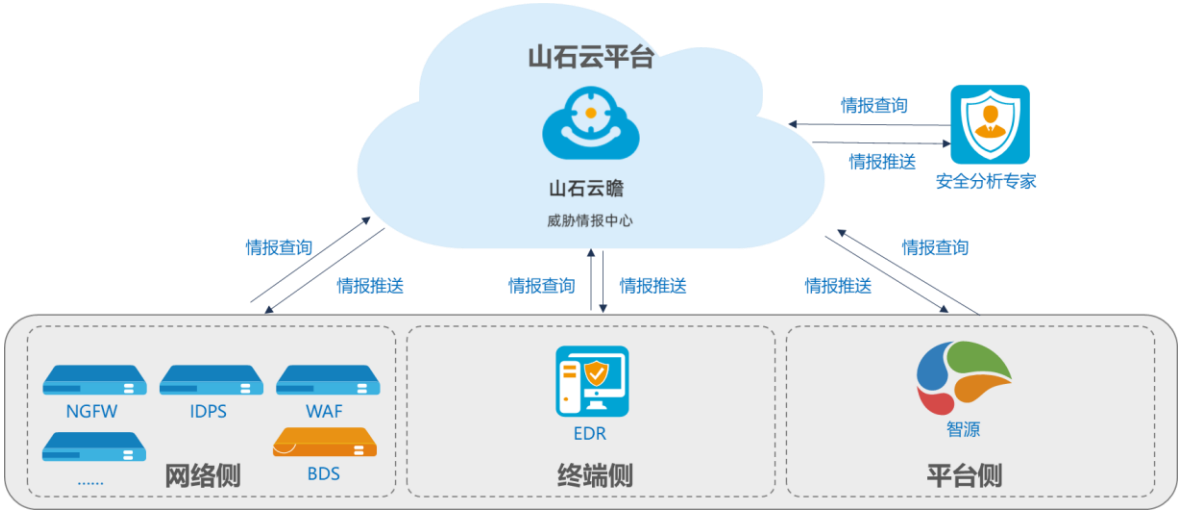
客户价值

云端智能与本地协同防御，变静态防御为积极主动防御

山石云瞻威胁情报中心作为能力中心，通过云端威胁情报的收集、处理和分析，可为客户提供及时准确的威胁情报数据。通过云端与本地安全产品协同联动，客户能够及时了解当前最需关注的热点威胁，协助客户深入全面的掌握威胁信息，实现威胁追踪和攻击溯源，帮助客户实施积极主动的威胁防御和快速响应策略，提升客户网络威胁防御水平。

典型应用

本地安全产品集成威胁情报能力实现云端赋能和威胁溯源分析，提前感知威胁。



股票代码：688030

文档编号：HS- CloudVista –CH-v1.1-20200804

官方微信　　官方微博

中国·销售与服务热线：　400-828-6655