关键技术

APT 深度分析

为应对用户网络中APT类型攻击，如0day慢攻击等，锐捷网络安全态势感知方案结合历史数据分析、云端智能分析、沙箱模拟分析、安全专家咨询等机制，实现对攻击异常行为的识别和预警。同时利用流量探针分析数据及机器学习技术，建立业务访问模型，对攻击者异常业务访问及数据窃取行为进行及时判断发现，帮助用户实现对APT攻击的防御及处理。

云端管理协同

为实现用户网络对于外部威胁的主动防御，锐捷网络安全态势感知解决方案利用云端管理技术，将互联网云中心与本地系统进行联动，实现云端智能分析协助、威胁预警预测推送、云端威胁特征库管理等功能，为用户主动防御体系建设提供技术支撑。

外部情报联动

为实现用户网络对未知风险的及时预防，锐捷网络安全态势感知解决方案通过与第三方威胁情报中心合作，对最新风险类型及趋势进行及时获取，并结合用户网络安全漏洞风险，向用户提供前置化的风险预测，为用户网络安全加固提供针对性解决方案。

内部风险管理

漏洞风险与基线违规是影响用户网络安全的两大关键内部因素，锐捷网络安全态势感知解决方案针对性设计的内置漏洞扫描、外部漏洞扫描联动、基线合规管理、失陷主机定位功能，帮助用户实现漏洞与基线统一管理，降低用户网络脆弱性，减少网络风险。

安全联动协防

为实现用户网络对已发现威胁的主动防御，锐捷网络安全态势感知解决方案支持安全分析平台与安全设备联动机制。当发现明确攻击类型及解决方案时，安全分析平台自动向安全设备下发阻断指令，实现对网络威胁的及时控制。同时对需要进一步判断的攻击，在管理员进行信息确认后，安全分析平台自动进行阻断指令下发，避免误判发生几率，实现网络安全与业务运行的合理平衡。

工单管理与事件闭环

为保证安全事件的跟踪管理与有效闭环，锐捷网络安全态势感知解决方案支持工单管理功能，实现安全事件到人的业务关联。通过告警事件的派单动作，将事件转入到具体的工单管理模块中，并结合系统知识库提供给排查人员安全事件的原理以及相应的解决方案，有利于工作的开展和追踪。同时结合工单分发到整个事件闭环处理后，对已经修复的漏洞、应急安全事件处理进行成果呈现。

Ruijie 锐捷 Networks

锐捷网络股份有限公司

欲了解更多信息，欢迎登陆www.ruijie.com.cn，咨询电话：400-620-8818。

看得见的安全 信得过的网络

安全态势感知解决方案

如有疑问
扫一扫在线咨询

Ruijie 锐捷 Networks

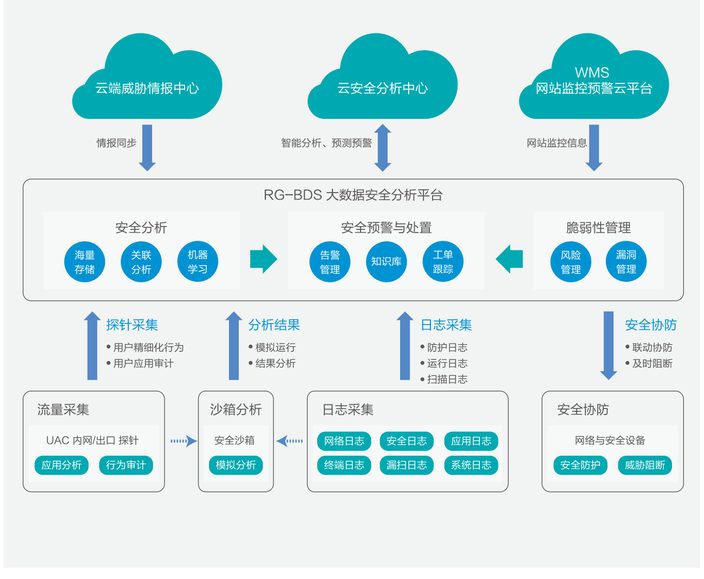
看得见的安全 信得过的网络

安全态势感知解决方案

当前，越来越多的用户借助云计算、大数据、物联网、移动互联网等为代表的新兴技术实现自身的业务再造与转型。与此同时，网络安全边界弱化、数据价值提升等一系列信息安全风险，也越来越受到用户关注，2017年网络安全更是被提升到了国家战略的高度。

然而全球网络安全形势并不容乐观，2017年5月份爆发的WannaCry勒索病毒及变种危害涉及150个国家，50万台电脑，造成损失近100亿美元，期间全球多家企业级用户业务被迫关停，这也直接暴露出传统信息安全防御体系在防护能力上的不足。如何为用户构建下一代安全防护体系成为安全领域的新课题。

安全态势感知解决方案是锐捷网络结合多年安全研究成果和网络安全建设经验，以大数据技术架构为核心开发的集安全要素获取、分析、处理、跟踪、预测为一体的全流程安全解决方案。结合机器学习、外部情报联动等技术，实现对整体网络的安全态势感知。目前，方案已成熟应用于政府、交通、企业、医疗、教育等多行业用户，帮助用户真正实现“看得见的安全，信得过的网络”。



核心能力

为实现对网络安全态势的精准感知，锐捷网络安全态势感知解决方案从攻击发现、APT深度分析、威胁预测、安全知识库协助、工单跟踪闭环等模块构建全流程安全体系，打造以下四大核心能力：

攻击行为可发现

随着安全技术的不断发展，安全攻击威胁越来越向常态化、隐蔽化发展，包括 0day 模式的高级攻击等， 这让用户网络安全形势日益严峻。如何实现非法攻击行为的及时发现是用户网络攻防战中至关重要的一环。

锐捷网络安全态势感知解决方案通过对基础网络、中间件、业务系统、终端、安全设备等多维度安全攻击感知信息采集，结合深度分析、机器学习等关键技术，实现对用户网络中攻击行为的及时发现和精准定位，并通过攻击溯源、归并告警等多种方式进行可视化呈现，让用户网络中的攻击行为无处可藏。

安全防护可协同

仅通过部署设备进行安全加固，并不等于真正安全。为实现对用户整体网络的安全防护，发挥各安全组件最佳协同效应，在用户网络安全攻防战中，如何实现“人+平台+设备”的有机结合及高效协同，跨越安全设备到真正安全之间的鸿沟，是安全防护体系建设的一大难题。

锐捷网络安全态势感知解决方案，通过分析平台与安全设备联动、云端智能分析协同、安全知识库体系协助、安全专家咨询、工单跟踪闭环等机制，构建“人+平台+设备”的立体化主动防御安全体系，帮助用户建设可协同的安全网络，实现安全设备到真正安全的鸿沟跨越。

威胁态势可预测

安全攻防战本质上是时间战，获得时间优势就掌握了安全战场上的主动权。如何实现对安全威胁态势的提前预测，成为安全防护技术领域发展的新趋势，也是下一代安全运营中心典型特征之一。

锐捷网络安全态势感知解决方案通过外部威胁情报同步、攻击趋势分析、业务曲线学习等机制，对未来威胁态势进行提前预判，同时结合预警发布、专家咨询服务等功能及机制设计，实现用户网络未来威胁态势预测，并提供针对性安全防护解决方案。

安全状态可度量

在网络安全领域，不存在百分百的安全。当攻击成本远大于利益获取时，网络安全就可以得到保障。帮助用户找到最适合自身场景的安全建设方案尤其重要，但如何进行安全状态的量化评估一直是困扰用户的难题，投入了大量精力对网络进行安全建设，实际的安全状态却无法有效衡量。

锐捷网络安全态势感知解决方案根据安全日志、漏洞、风险、脆弱性等权重综合评判现网安全状态，量化全网及业务的安全评分，并通过安全评分趋势、告警和工单处理等趋势图直观的呈现安全建设业绩，帮助用户建设可度量的安全网络。

关键技术

多维度信息采集

为实现对安全攻击的全方位分析，锐捷网络安全态势感知解决方案支持多维度的安全信息采集，包括从网络、业务、主机等组件采集运行日志数据，从安全设备采集防护数据，从探针设备采集应用分析数据、从沙箱设备采集威胁分析数据等。同时结合外部威胁情报信息及漏洞扫描信息，进行海量安全数据的关联分析，实现对安全威胁的精准定位。