SONICWALL

SonicWall Analytics

将数据转化为可操作洞察

SonicWall Analytics 将防火墙流量数据转换为跨用户、应用程序和网络的可操作洞察，从而帮助以更高的精度和速度降低安全风险——所有这些都通过一个界面。该分析引擎使用高性能云原生架构构建，可跨数千个防火墙节点大规模丰富大量原始数据，通过执行仪表板为利益相关者提供完整的可见性和安全透明度。

Analytics 通过使用各种形式的语义图、时间使用图表和表格来创建数据模型的知识表示，以帮助减少停留时间并减轻分析师的疲劳。通过增加的向下钻取功能，安全响应者可以调查关键数据点并将其归零，以暴露隐藏的风险从而进行早期干预，并针对在发现过程中展开的风险用户活动采取有证据支持的策略行动。

凭借全面的可见性和控制，安全分析师可以随时随地洞察一切，从而成为更好的风险管理者，而响应者可以将宝贵的时间和精力集中在跨最重要的应用程序和用户协调快速响应行动上，而不是对每个事件都做出反应。Analytics 以云敏捷性和云弹性扩展和执行，从而满足最苛刻的企业需求。

亮点

企业业务

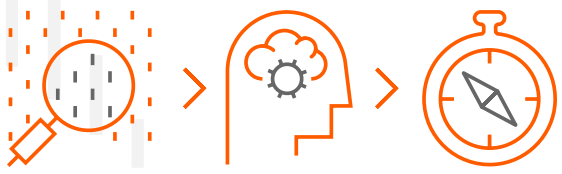
- 获得完全安全透明度
- 获取安全态势的实时快照
- 履行内部合规义务
- 进行准确的网络防御规划和预算
- 降低资本支出和运营支出

业务运营

- 一目了然轻松了解安全指标
- 从每个网络事件、用户事件和警报中激发洞察
- 制定准确的防御策略行动
- 以云敏捷性和云弹性扩展和执行

安全

- 发现隐藏风险
- 启用早期干预
- 及时响应不安全的用户活动
- 帮助分析师成为更好的风险管理者
- 将响应者变成更好的问题解决者



深入了解 SonicWall Analytics

www.sonicwall.com/analytics

DATASHEET

随时随地洞察一切

Analytics 使您可以全面了解租户、组或设备级别的整个 SonicWall 安全环境。执行仪表板对通过防火墙生态系统的所有网络流量和数据通信提供静态和接近实时的分析。所有日志数据都会被记录、汇总、情景化，并以有意义且易于使用的方式呈现，让您能够根据数据驱动的洞察发现、解读、分类并采取适当的防御响应。

Analytics 附带广泛的预定义报告，并且可以使用流量数据的任意组合灵活创建特定于您期望用途或意图的自定义报告，并定期交付它们。它提供长达一年的流量分析、安全漏洞和异常发现历史记录，以帮助您跟踪、衡量和运行安全第一的网络和安全运营中心。

图 1.0 执行仪表板

了解您的风险

向下钻取和透视功能使您能够自信地进一步检查与入口/出口流量、应用程序使用、用户和设备访问、威胁行为等相关的特定模式和趋势。通过混合使用端点、网络、用户和应用程序报告和分析，您可以主动分析或响应警报、异常和风险用户活动。凭借完全安全透明度，您将获得情境感知能力，以发现安全风险、协调策略活动、推动一致的安全强制实施并持续监控整个环境的结果。

使用 SaaS、虚拟或 IaaS 选项灵活部署

Analytics 为您提供灵活的部署选择，完美适合您的运营需求。

为了获得免维护体验，Analytics 可作为 SonicWall 托管的 SaaS 产品提供，并可通过互联网访问。SaaS 选项为您提供无限弹性以按需扩展，同时可降低运营成本。已去除硬件和软件采购、定制安装、定期维护和升级、资产折旧和报废成本的典型成本，取而代之的是低且可预测的年度订阅成本。

为实现全面的系统控制和合规性，您可以将 Analytics 内部部署为安装在您选择的虚拟平台（例如 VMWare 和 Microsoft Hyper-V）上的软件。您可以受益于虚拟化的所有运营和经济效益，包括系统可扩展性、系统配置速度和成本降低。

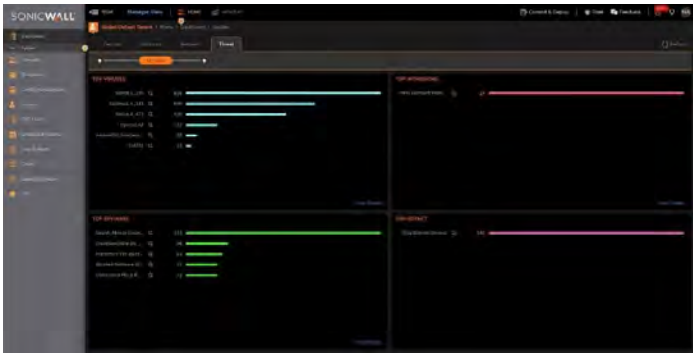


图 2.0 威胁汇总

功能摘要

功能	描述
数据聚合	自动聚合与规范流经所有防火墙的安全数据。
数据情景化	处理和丰富防火墙数据，并以结构化、有意义且易于使用的方式呈现，使安全团队、分析师和利益相关者能够发现、解读、确定优先顺序、制定决策并采取适当的防御措施。
流分析	网络安全数据流被连续处理并实时加载，结果显示在动态的交互式可视仪表板中。
用户分析	通过执行仪表板显示员工 Web 应用程序和网络使用的综合视图。它让您可以细粒度向下钻取历史记录，以针对有风险的用户 Web 活动建立有证据支持的策略控制措施。
应用程序流量分析	为组织提供对应用程序流量、带宽利用率和安全威胁的强大洞察力，同时提供强大的故障排除和取证功能。
安全分析	通过快速威胁检测获得实时可见性。使安全分析师和事件响应者能够寻找、识别和调查问题。
实时动态可视化	通过单一管理平台，安全分析师可以更精确、更快速地对安全数据进行深入的调查和取证分析。
快速检测和补救	追查不安全活动并通过采取准确行动迅速管理和补救风险的调查能力。
生产力报告 （需要在第 6/6.5 代防火墙上启用 AGSS/CGSS 许可证，在第 7 代防火墙上启用基本保护许可证）	提供对组织网络资源利用率的洞察。它可以生成强大的快照以及针对用户上网行为的深入报告。这些报告收集有关网站地址和访问用户访问日期的数据，并计算用户在每个站点上花费的时间以及在这些站点上花费的时间是在办公时间还是非办公时间。生产力报告将用户的 Web 活动分为生产力组，例如高效组、低效组、可接受组、不可接受组或自定义组，以帮助组织更好地了解网络使用模式并优化员工生产力。 例如，通过了解用户在非业务相关网站上花费的时间，人力资源部门的领导可以管理和应对潜在员工违反行为准则政策的行为。类似用例可以应用于所有其他功能组。
VPN 报告	总结 VPN 隧道中使用了哪些公司资源、它们消耗了多少带宽以及该流量的使用者是谁（即用户名和 IP 地址）。网络管理员可以利用这些信息来监控关键业务应用程序、控制或整形流量以及规划容量增长。

功能	描述
流量分析和报告	通过 IPFIX 或 NetFlow 协议为应用程序流量分析和使用数据提供流量报告代理，以进行实时和历史监控。为管理员提供有效且高效的界面以实时直观监控其网络，从而能够识别具有高带宽需求的应用程序和网站、查看每个用户的应用程序使用情况以及预测网络遭受的攻击和威胁。 • 具有一键过滤功能的实时报告界面 • 具有一键查看按钮的热门流量仪表板 • 具有附加流量属性选项卡的流量报告界面 • 具有强大关联和透视功能的流量分析界面 • 用于深入钻取单个会话和数据包的会话查看器
综合图形报告	提供对防火墙威胁、带宽使用情况、员工生产力、可疑网络活动和应用程序流量分析的可见性。
Syslog 报告	简化数据汇总，允许近乎实时地报告传入的 Syslog 消息。直接访问底层原始数据进一步促进了广泛的细粒度功能和高度可定制的报告。
计划报告	为所有计划报告提供单一入口点。一份报告可以组合多个单位的图表和表格。可以计划报告并以各种格式发送给一位或多位分析师。
清晰报告	提供可自定义的视图，以在单个页面上演示多个汇总报告。用户可以轻松浏览重要网络指标，以便快速分析各种报告中的数据。
多威胁报告	收集有关攻击的信息，使用 SonicWall Capture ATP、网关防病毒、反间谍软件、入侵防御和应用程序智能与控制安全服务提供对 SonicWall 防火墙所检测到的威胁活动的即时访问。
新攻击情报	报告特定类型的攻击、入侵企图和攻击源地址，使管理员能够快速响应持续威胁。
恶意无线接入点报告	显示所有正在使用的无线设备，以及来自主机之间点对点或对等网络的恶意行为以及用户连接到相邻恶意网络的意外关联。
Capture ATP 报告	提供一目了然的威胁分析仪表板和报告，其中详细说明了发送到服务的文件的分析结果，包括源、目标和摘要以及引爆后恶意软件操作的详细信息。
僵尸网络报告	包括四种报告类型：企图、目标、发起者和包含攻击向量上下文的时间线，例如僵尸网络 ID、IP 地址、国家/地区、主机、端口、接口、发起者/目标、源/目标和用户。
Geo IP 报告	包含基于流量来源或目标国家/地区的被阻流量的信息。包括四种报告类型：企图、目标、发起者和包含攻击向量上下文的时间线，例如僵尸网络 ID、IP 地址、国家/地区、主机、端口、接口、发起者/目标、源/目标和用户。
MAC 地址报告	在报告页面上显示媒体访问控制 (MAC) 地址。在五种报告类型中包含设备特定信息（发起者 MAC 和响应者 MAC）： • 数据使用 > 发起者 • 数据使用 > 响应者 • 数据使用 > 详情 • 用户活动 > 详情 • Web 活动 > 发起者
集中式日志记录	提供一个用于整合所有受管设备的安全事件和日志的集中位置，提供单一点来进行网络取证。
云原生架构	以云速度和云弹性从数万个防火墙节点收集、组合、处理、再处理、提取、关联和加载海量查询数据。

许可和包装

	功能特性	SaaS 分析	内部分析
管理	备份/还原 – 防火墙系统	是	是*
	报告（基于 Netflow/IPFIX）	是	是*
	分析（基于 Netflow/IPFIX）	仅来自本地文件	仅来自本地文件
报告	计划报告、实时监控器、摘要仪表板	是	是
	下载报告、应用程序、威胁、CFS、用户、流量、源目标（1 年流量报告）	是	是
分析（基于 Netflow/IPFIX）	使用向下钻取和透视进行网络取证和威胁搜寻	是	是
	Cloud App Security – Shadow IT 发现	是	否
	数据保留	30 天	1 年
技术支持		全天候支持	全天候支持**

*需要 AGSS/CGSS 服务或任何付费的 Capture Security Center 服务
**需要全天候支持许可证

最低系统要求

对于通过 Network Security Manager 在 SaaS 模式下的 SonicWall Analytics：

支持的 SonicWall 设备包括：

- SonicWall 网络安全设备：NSA 系列、NSa 系列、TZ 系列设备、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 设备：NSv 10 至 NSv 400

支持的 SonicWall 固件

- SonicWall SonicOS 6.0 或更高版本

互联网浏览器

- Microsoft® Internet Explorer 11.0 或更高版本（不使用兼容模式）
- Mozilla Firefox 37.0 或更高版本
- Google Chrome 42.0 或更高版本 Safari（最新版本）

对于 SonicWall Analytics 内部部署：

虚拟设备

- 虚拟机监控程序：VMware ESXi v5.5 / v6.0 / v6.5 / v6.7、Microsoft Hyper-V Win 2016
- 推荐 RAM：无限（最低 8 GB）
- 硬盘：基础 OVA 65 GB 需要外部安装
- vCPU：4/无限
- 网络接口：1
- VMware 兼容性指南

支持的 SonicWall 设备包括：

- SonicWall 网络安全设备：SuperMassive E10000 和 9000 系列、NSA 系列、NSa 系列、TZ 系列设备、SOHO-W、SOHO 250、SOHO 250W
- SonicWall Network Security Virtual 设备：NSv 系列

深入了解 SonicWall Analytics

www.sonicwall.com/analytics

关于 SonicWall

SonicWall 为超分布式时代和每个人都远程办公、每个人都移动办公、每个人都不太安全的工作现实提供了 Boundless Cybersecurity。通过了解未知、提供实时可见性并实现经济学突破，SonicWall 为世界各地的大型企业、政府和中小企业弥补了网络安全业务缺口。有关更多信息，请访问 www.sonicwall.com 或在 Twitter、领英、Facebook 和 Instagram 上关注我们。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
有关详情，请访问我们的网站。
www.sonicwall.com

SONICWALL