ABT·安博通

看透安全 体验价值

安博通SPOS全系列

安全可视化产品与应用

策略可视化平台

随着网络安全威胁的不断升级，不仅要与时俱进的了解各种各样的网络进攻方式及手段，更要从根本上提高内在的网络安全防御力，掌握自身网络架构，清晰安全域的划分，部署和调整安全策略，以及明确流量异常和危险行为等。安博通安全策略自适应分析与大数据可视化平台旨在通过提高网络自身的免疫力来增强对各种内外部威胁的防御能力，从而能够全面清晰的帮助各行业用户打造网络安全防御体系的作战全景图，将对各种威胁的被动防御上升为主动部署，做到路径可视、策略可视、流量可视、风险可视、威胁可视以及变更可视。安博通安全策略自适应分析与大数据可视化平台可广泛应用于纵向行业网、云计算平台与大型局域网等场景，并为用户带来以下价值：

- 安全域、业务、用户的网络安全策略与路径全面可视
- 业务质量、用户行为、异常流量、安全风险关联可视
- 可视化感知网络安全风险，提升安全预测与防御能力

安博通安全策略自适应分析与大数据可视化平台分为基础策略层、流量分析层和能力叠加层。在基础策略层，要构建安全策略与访问路径的动态可视化地图大屏呈现平台；在流量分析层要实现业务性能可视化、安全状态可视化、异常流量可视化；而对于能力叠加层而言，要实现第三方监测事件叠加，威胁情报与安全态势集成，并达到关联分析的效果。平台工作的原理是对多方位安全策略与用户业务流量探针数据及第三方情报数据进行抽取，依靠分布式大数据分析技术进行监控、呈现与响应。

- **安全域基础架构可视化**

  实现网络防火墙、路由器、交换机等设备安全策略信息的自动提取与解析管理，其中包括对数据安全产生影响的路由信息、访问控制、NAT 策略，并运用可视化技术，实现网络安全域基础架构的可视化展示。

- **安全合规路径可视化**

  可以结合各行业业务流程、应用架构、数据架构等现状，分析各核心业务系统关键数据的合规基线策略，实现在安全域基础架构图层查询与展示基于业务的合规路径，预警网络风险，实现核心业务威胁面的可视化分析。

- **安全基线矩阵可视化**

  通过针对性对行业用户网络安全策略体系与业务系统分析，能够建立安全域间的安全策略矩阵、系统间的安全策略矩阵、用户与系统间的安全策略矩阵，实现安全策略合规矩阵的可视化展示，并通对基线持续监测，实现违反策略基线行为的自动可视化告警。

- **安全策略管理可视化**

  能够对全网安全策略进行管理和变更可视化，能够分析相关设备的冗余、冲突、无效策略，帮助用户排除用户配置风险。结合工作流与用户权限，实现策略变更申请、分析、审批全流程可视化。

- **业务流量安全可视化**

  基于 DPI 深度识别与大数据技术，通过用户、网络、应用、协议、服务器等多个维度识别业务类型识别，监控具体业务流量、会话、延迟、成功率、包长、访问地域等网络指标，统计业务指标基线，对超过指标基线告警，历史信息追溯分析。

- **安全能力叠加与威胁可视化**

  能够提供任意时段内的海量数据快速检索和挖掘能力，有效叠加不同的安全检测和防御能力，基于大数据技术进行数据关联，筛选过滤、挖掘分析，实现安全路径、业务流量、安全事件与威胁情报的综合网络安全态势可视化。

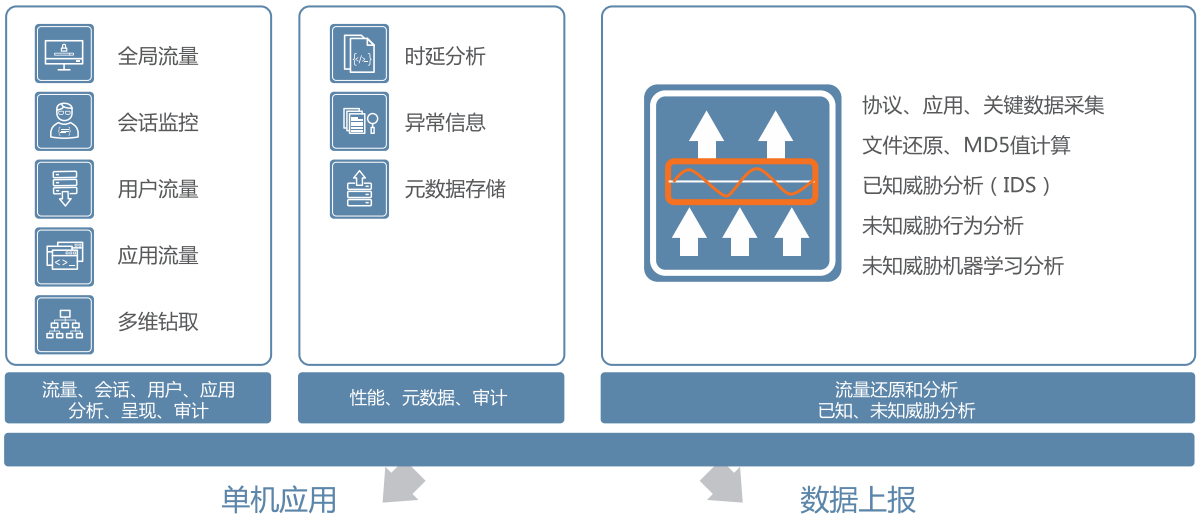
安博通安全策略自适应分析与大数据可视化平台采用可视化手段持续监控与分析，形成防御、检测、响应与预测的闭环，能够学习用户行为，动态演进策略以匹配用户行为，细粒度的响应保证业务连续性，用自适应安全架构应对高级定向攻击，逐步击破日新月异的网络安全威胁与风险。目前已入选 2016 年工信部电信和互联网行业网络安全试点示范项目。

流量可视化平台

产品简介

安博通流量安全可视平台是一款基于大数据和可视化技术的高性能网络流量数据采集和智能分析硬件平台，通过对镜像流量多维度及深层次的数据包内容解析和关联分析，以丰富的图形化方式对已知威胁、未知威胁、网络流量、应用性能等方面进行呈现，从而实现企业网络的全面威胁可视化和防护。

产品架构



产品功能特点

- **网络流量采集**

  平台采用旁路部署方式，不改变企业原有网络架构，支持交换机镜像、分光器、分流器等多种网络流量数据采集方式；

  支持基于 VLAN、VxLAN ID、MPLS TAG、网段等方式配置虚链路接口，实现对云数据中心、SDN 网络、分流交换汇聚流量进行灵活采集；

  可提供链路流量实时数据包抓取及历史数据，在捕获前可自定义捕获条件与参数。

- **应用协议解析**

  平台采用 DPI（Deep Packet Inspection）深度包检测技术进行应用层协议解析，可准确高效识别，充分分析网络流量构成、性能、流量等；

  支持对 HTTP、FTP、MYSQL、MAIL、OA 等具体的内部业务应用进行识别和解析，辅助大数据分析平台建立用户与业务的正常访问基准模型，为用户异常访问与异常用户访问检测提供有力数据支撑。

- **已知 + 未知威胁防御**

  平台支持以下三个层次的威胁防御解决方案

  1. 特征匹配：平台集成 NIDS 和 WEBIDS 的功能，针对网络流量进行基于特征匹配的检测，包括针对网络的攻击以及针对 Web 服务器渗透的行为；

  2. 行为分析：基于 IP 地址分类、协议类型和传输时间、传输数据量、域名、端口范围等元素，通过预定义行为和自定义行为的组合方式，将行为与流量提取出的信息进行比对和告警；

  3. 机器学习：通过百万级别的正例样本和反例样本进行训练，通过机器学习的方式提供基于 DGA 域名、C2C 流量的僵尸网络、钓鱼网站等恶意 URL 的分析结果。

- **流量全景呈现**

  平台对网络流量实现 OSI 7 层流量监控分析，可显示全双工接口的收、发和全部的流量、数据包信息；

  提供对主机、协议、会话等维度的分析内容呈现，并支持关联分析、智能排序、模糊查询、多级钻取等功能，例如从协议分布中查看某个应用协议的主机、会话对等；

  针对用户、用户组、业务应用及服务器对象，即可呈现历史数据统计分析结果，也可提供实时流量、会话信息的呈现与条件检索，让用户对网络流量、业务状态一目了然。

- **智能报表分析和数据上报**

  数据分析平台收集并储存流量安全可视平台采集的流量数据信息，基于大数据分析技术，提供丰富、强大的分析报表功能；

  数据分析平台可提供日报、周报、月报、季报、年报等短、中、长期的网络流量域用户行为报告；

  支持对网络的整体性能、网络的运行状况、网络的流量趋势乃至应用的服务质量进行分析，辅助网络管理人员预先确定应用资源需求以避免出现性能问题；

  平台支持完善的 Restful 数据接口，可以接受第三方平台的抓取指令，通过 syslog 等协议方式将数据上送到数据分析、安全沙箱等平台。

产品功能特点

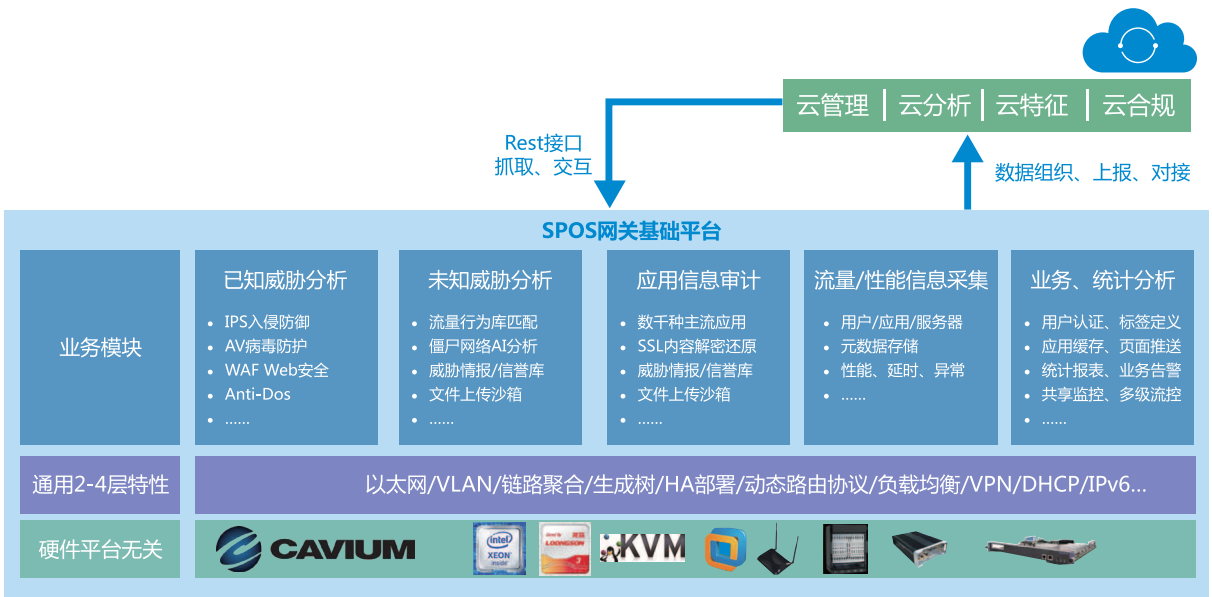
序号	应用场景名称	产品价值	
1	广域网场景	网络流量与质量的监控和呈现	关键业务性能监控与连续性保障
		自动诊断、定位网络或业务问题	用户行为日志审计与合规性分析
		异常流量监测与安全威胁发现	配合大数据分析平台，体现IT部门价值
2	云数据中心	虚拟链路网络流量与质量的监控和呈现	关键业务性能监控与连续性保障
		关键业务访问审计与合规性分析	IT资产漏洞扫描与安全检查
		异常流量监测与安全威胁发现	提升运维管理效率和响应速度
3	互联网出口	出口进出流量细粒度全景呈现	通过用户访问行为分析规范上网行为
		防防私接Wi-Fi监控	快速发现各种安全威胁与异常行为
		有效防止APT攻击与敏感数据泄露	

SPOS-Base

产品简介

安博通 SPOS-Base 安全操作系统套件，提升基础安全能力的最佳选择，SPOS-Base 产品具备高效率、高性能、平台无关等优势，在行为安全、Web 安全、文件安全等方面具备丰富的特性，能够以柔性方式融合于安全产品或安全解决方案之中，帮助第三方快速提升基础安全能力，打造共赢的生态局面。

产品架构



产品功能特点

- **广泛适配各种平台**

  SPOS-BASE 产品已经广泛应用在 MIPS 多核、X86、龙芯等多种架构上，也可以灵活适配在插卡、盒式设备等多种介质中，在 VMware、KVM、阿里云等虚拟化和云环境中也已经成功部署，对于主流平台架构，SPOS-Base 产品均可轻松运行或快速移植，实现安全能力的平台无关性。

- **高效一体化架构**

  SPOS-Base 产品采用一体化引擎架构，整个解析过程一次拆包，针对 SSL 解密等流程进行流程优化，提供高效率高性能的引擎性能，在网络流量转发、系统延时、多重安全业务开启时的高性能方面领先业界，能够提供优秀的网络安全产品底层平台架构，同时与云端运维管理、业务分析、安全沙箱等系统进行云端联动，实现云 + 端的高效协同化架构。

- **全面威胁防御能力**

  SPOS-Base 提供已知威胁(特征匹配、防病毒)+ 未知威胁(行为模式匹配 + 机器学习)的全面威胁防御解决方案，同时支持 IPsec/SSL VPN 等安全加密隧道能力 ,提供自动化高可靠的远程互连能力 ,集成海量的威胁和病毒特征，构建高效的安全防御体系。

- **Web 安全防护能力**

  SPOS-BASE 产品提供事前、事中、事后的全流程 Web 防护能力 ,包括弱密码检测、资产发现、网页防篡改、防盗链、高阶告警和报表等技术方案，可以帮助安全产品提升 Web 安全防护能力，有效地保护重要的 Web 服务器资源免受黑客攻击。

- **精细化管控和审计能力**

  SPOS-BASE 产品支持数千种主流互联网应用的管控和审计，支持基于应用动作的精细化处理，支持内网应用自定义和分析，实现访问的内容过滤和外发文件的留存，降低信息泄密风险和舆论风险，可以在互联网和内网场景下提供完善的应用行为、流量、性能管理解决方案。

- **多模式对接方案**

  在公共互联网 WLAN 上网等场景下，需要审计留存信息并拼接后以特定的格式上报给外部平台，SPOS-BASE 产品提供单点串行、单点旁路、多点集中、多点分布等多种对接模式，支持 20 余家数十个版本的后端平台对接能力，支持多种身份认证系统以及 WLAN 产品进行数据对接，提供业界领先的安全合规解决方案。

- **大数据 & 可视化分析能力**

  针对流量、威胁、行为、性能等信息，SPOS-BASE 产品凭借强大的流量分析技术，提供深入到应用层的信息提取 ,并支持完善的数据接口将数据上报到数据分析平台 ,同时在本地也提供多维度的统计报表和可视化呈现能力，提升安全解决方案的数据分析能力，帮助管理者更好地进行决策。

- **IPv6 全面支持**

  随着 IPv6 在国内实际化落地，IPv6 安全的需求随之更加旺盛，SPOS-BASE 产品已经完成 IPv6 技术储备，所有安全特性均支持在 IPv6 网络中部署，提供 IPv6 网络的安全防护、行为管控、流量控制、数据分析等解决方案。

数据分析与运维平台

产品概述

在企业信息化水平日新月异的今天，如何利用技术手段迅速持续提升自身核心竞争力成为企业日常运营中的最重要课题之一。安博通早已洞察到大数据时代到来所带来的行业机会，提早在云平台领域做出布局，推出安博通数据分析与运维平台，以领先的数据挖掘分析能力和集中管理能力在业界获得了良好的口碑。

安博通数据分析与运维平台在常见的总分型网络中，方便用户集中部署和集中监控，同时可以将端作为触手，进行统一集中管理和数据收集分析、服务质量探测、 特征库统一升级、内容与应用缓存以及集中身份认证等，为核心业务保驾护航，充分发挥云管端的优势。

产品特点

- **海量数据存储能力**

  数据分析与运维平台通过分布式处理的软件架构，使用独特的列存储技术，实现对同一列的数据归并，可以对海量数据进行可靠、高效的存储，其存储能力是一般数据库的 10 倍，为用户大量节省数据存储成本。

- **高速运算及数据查询**

  数据分析与运维平台通过分布式集群，并行处理能力加快处理速度，依赖高速的数据分析引擎，使用数据检索速度是一般数据库查询能力的 8 倍以上，能够实现海量数据秒级查询速度，5000 万秒级查询速度，并支持支持模糊匹配和数据追踪。

- **多样化数据呈现，多维度数据关联**

  数据分析与运维平台通过表格、趋势、报表、饼图、动态数据等多样化数据呈现方式，直观展现数据内部关联，可以是客户直观的感受数据价值，为业务开展等实际运营工作提供有效的管理手段。平台不仅能够分析 IT 数据，也能关联多样的格式化数据，并进行有效组织和协同分析，挖掘出数据价值点，增强企业的洞察能力、盈利能力，为企业获得可持续的竞争优势提供强大的保障。

- **策略集中管理**

  数据分析与运维平台具有集中策略管理能力，帮助管理员脱离苦海，集中新建七元组策略批量下发到每一台设备，对于政府、运营商、金融、电力和大型企业等分支结构众多的客户，可以极大的降低运维人员的工作量，帮助客户实现高效率管理运维。

- **精准审计监控**

  数据分析与运维平台通过收集用户浏览的网站、发表的内容，结合用户认证系统可以精准定位到每个用户的上网行为。针对非实名认证的移动终端的上网行为审计，监控功能可以从 " 全三维 "—用户、应用、设备三大维度进行全面审计，每个维度又可基于时间、应用、流量方向、用户、设备等元素进行细粒度查询，并可自动生成趋势图与用户 TOP N 排名，对网络流量立体的呈现，帮助用户迅速把握网络问题。

- **丰富业务报表**

  数据分析与运维平台具有丰富的业务报表功能，不仅能够轻松掌握设备运行状态，还能够满足合规性要求、运维汇报、工作总结等管理需求，支持流量报表、上网行为报表、关键字报表、用户综合报表等海量报表，支持根据用户和应用和多设备不同角度定义报表，同时也支持日、周、月、年和自定义时间范围的各个不同维度的报表，并且根据业务内置业务报表，将无形的工作转化为直观的图表进行工作汇报，从而减轻维护量、提升管理效率。

Web 应用漏洞扫描云平台

YUNSCANNER

产品简介

云扫描者 Web 应用安全漏洞扫描系统 (简称” 云扫描者 WVS”) 是安博通与禹成在线共同成立的安全实验室大禹 LAB 的研发团队，专门针对 Web 应用程序自身安全而开发的专业级的漏洞检测系统。在吸取国外领先的安全检测技术和经验基础上，针对 Web 应用程序漏洞扫描关键技术和技术难点，进行了深入的分析和研究，并取得了一系列突破性成果。在支持的漏洞种类、爬虫的爬行能力、登录表单的自动识别能力、漏报率和误报率等各项关键指标等方面，“云扫描者 WVS” 与业界同类产品相比，在国内甚至国际上都具有绝对的竞争优势。

“云扫描者 WVS” 能够广泛应用于各种类型的基于浏览器的 Web 应用系统，如各类网站、论坛、电子邮件、电子政务、在线交易平台、网上银行等等。不仅适用于这些系统的运营企业，而且适用于这些系统的开发企业和验收方。

核心技术

- **创新的爬虫技术**
  自主研发的基于最新浏览器引擎技术的爬虫，全面超越现有此类工具爬虫的爬行能力，这是确保低漏报率的根本保障。

- **跨站脚本检测率业界最高**
  针对 OWASP 排名第二的 XSS 漏洞的精确检测算法，不仅支持常规的 XSS 漏洞检测，同时对存储型 XSS 和 DOM XSS 提供强大的支持，并且误报率为零，全面超越现有此类工具针对 XSS 漏洞的检测能力。

- **Linux 适用性**
  基于 Linux 平台的系统，不受 Windows 版权和性能限制，性能上具有 Linux 平台先天优势。

- **强大的云部署能力**
  在产品架构设计之初，“云扫描者 WVS” 即考虑了对云计算的支持，不仅具有强大的云部署能力，而且提供了非常方便的接口，并具有强扩展性。

产品功能

- 全面支持 OWASP TOP10, 而且具有极低的误报率和漏报率；
- 按照 WASC 标准分类，支持的 Web 应用漏洞种类最全面、划分粒度最细；
- 基于最新浏览器引擎技术的爬虫，能够对各种动态内容进行处理，提供最全面、最强大的解析能力；
- 针对每一个检出的漏洞，通过扫描快照向用户提供漏洞证据；
- 针对每一个检出的漏洞，提供漏洞验证接口，方便用户对漏洞进行验证；
- 扫描日志，方便用户查看扫描认证结果和扫描进度；
- 认证结果快照，用户可根据快照内容，了解认证的真实结果；
- 对扫描到的所有页面，支持生成站点目录树；
- 支持认证扫描，并支持多种认证方式；
- 针对基于会话 Session 的认证扫描，提供自动捕获会话 Session 功能；
- 支持 HTTP 和 HTTPS 扫描；
- 支持代理扫描；
- 支持单用户并发扫描、多用户并发扫描；
- 针对单个扫描任务，支持多线程扫描；
- 提供扫描配置模版管理功能，方便用户批量进行扫描配置；
- 支持扫描路径设置，避免扫描不必要或危险的内容；
- 支持扫描黑名单设置，避免扫描不必要或危险的内容；
- 提供了一系列扫描加速选项，供专业安全从业人员使用，用户可以根据实际情况在扫描时间和扫描精度上的作出选择；
- 扫描配置提供了头注入选项，以满足特殊站点的安全需求；
- 扫描摘要，方便用户对扫描基本情况、漏洞情况和漏洞分布情况有一个整体了解；
- 提供 pdf 格式的报告，供用户下载。

典型应用场景

“云扫描者 WVS”部署灵活简单，只需要对目标站点“网络可达”即可进行 Web 应用程序漏洞扫描分析。但是，由于扫描时间受到网络访问速度的影响，建议将“云扫描者 WVS”部署到被评估 Web 服务器所在网络内部，以便能够获得最佳的扫描性能，而扫描操作人员只需要能通过浏览器远程访问到“云扫描者 WVS”即可。

主机安全监测平台

产品概述

青藤 - 安博通 Monitor 是由青藤云安全与安博通联合推出的一款终端安全监测产品，使用特征锚点、行为模式、关系模 型等独创方法，从进程、主机、网络三个维度全方位监测黑客行为，第一时间发现黑客有效入侵并做出响应，将企业损失最小化。

核心技术

- **特征锚点**
  黑客入侵的手段多种多样，但其目的是归一的：窃取有价值的核心数据资产。要接触到核心资产，有些路径是黑客的必经之路。在这些路径上打上特征锚点，对系统后门（rootkit、bootkit 等）、Webshell、文件完整性（文件内容或权限变更）和系统权限变更等进行监测，黑客一旦触碰锚点就会引发报警。

- **行为分析**

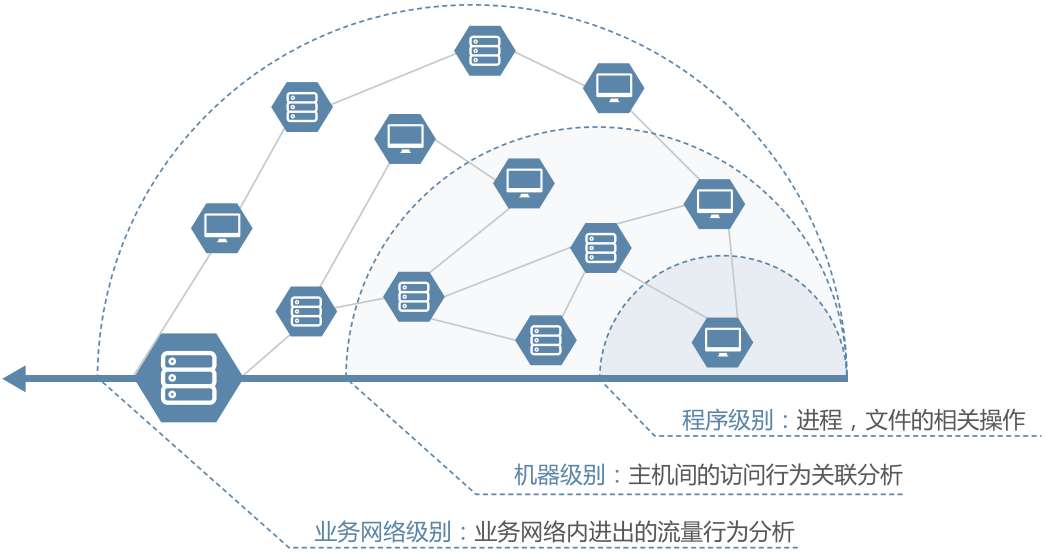
  专业安全经验，建立了黑客入侵的行为模型，包括进程的子进程产生、反弹 shell、异常登录、本地提权、shell 审计、系统敏感文件的读写、端口监听等，然后通过模式匹配的方法来做持续监控。

- **关系模型**

  在一个相对稳定的业务系统中，主机之间的进程访问关系是相对固定的。黑客在一步步窃取数据过程中，往往会对一些主机进行异常的访问。通过机器学习来建立不同业务角色间的访问关系模型，并持续进行监控，一旦发现有异常的访问行为就会报警出来。

- **基于行为识别的机器学习技术**

  青藤入侵检测系统会对行为数据进行多维度学习，一段时间后就可以建立起“正常”的行为模型，随着时间推移，系统会持续学习，自动评估模型的准确度并改进，识别发现真正的异常行为情况，从而在最大限度做到自动化的同时，做到最低的误报率。

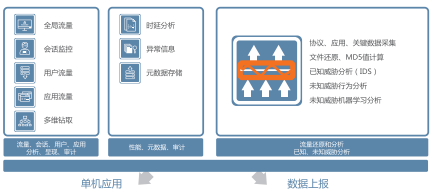


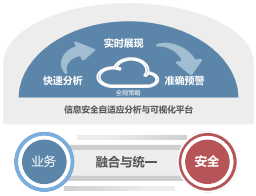
SPOS 全系列产品

SPOS-APP

YUNSCANNER

SPOS-TRACE





SPOS-BASE

业务模块	已知威胁分析	未知威胁分析	应用信息审计	流量/性能信息采集	业务、统计分析
通用2-4层特性	以太网/VLAN/链路聚合/生成树/HA部署/动态路由协议/负载均衡/VPN/DHCP/IPv6...				
硬件平台无关	CAVIUM KVM				

SPOS ENGINED

ABT·安博通

看透安全 体验价值

北京安博通科技股份有限公司

营销中心：北京市西城区裕民路18号北环中心2602室

电话：010-80699886

研发中心：北京市海淀区上地中关村软件园二期15号楼3层

电话：010-57649050

www.abtnetworks.com