ABT·安博通

看透安全 体验价值

网络攻击面可视化平台

技术白皮书

技术背景

当前 ,众多组织机构都必须针对——由其网络中成千上万个潜在的可利用攻击向量组成的——网络攻击面进行防御。随着新应用和技术的不断推出、新漏洞的不断发现，攻击面的规模和复杂性也在不断扩大。

2017 年 1 月 31 日，美国国防部美军国防信息系统局（DISA）宣布采用基于安全策略的网络建模与风险评估技术，对联合区域安全栈（JRSS）基础设施进行建模与连续监测，实现 JRSS 网络攻击面收敛与安全风险态势感知。

攻击面是一个给定的计算机或网络系统，可以被黑客访问和利用的脆弱性总和。如今，攻击者具有压倒性的优势，他们可以在任一时间、任一地点、利用任一漏洞发动攻击，而防御者必须做到全时、全网、全面。如何实现网络攻击面的监测、评估与收敛是防御者亟需解决的问题。

平台简介

2.1 平台概述

安博通网络攻击面可视化平台，采用 Gartner 提出的自适应安全架构，将安全基础架构建模与脆弱性评估技术相结合，计算给定网络系统的安全拓扑，实现资产、网络拓扑、安全访问控制、漏洞与威胁等要素的关联分析。

- **Gartner 新一代自适应安全防御架构**

平台能够对给定网络系统脆弱性的暴露程度进行评估，进而对其安全状态做出客观评价，并运用数据可视化技术对攻击面状态进行实时监控与分类指标呈现，实现：

- 安全路径与资产安全状态关联，安全拓扑端到端可视化。
- 重要资产与脆弱性定位，攻击面收敛与防御体系优化。
- 脆弱性关联网络暴露面，漏洞优先级精确评估。
- 网络异常与攻击事件定位，事件路径分析与溯源。

安博通网络攻击面可视化平台旨在通过提高网络自身的免疫力，增强对各种内、外部威胁的防御能力。将对各种威胁的被动防御上升为主动部署，实现安全策略可视、安全路径可视、安全策略变更可视、安全风险可视，为用户打造全面清晰的网络安全防御体系作战地图。平台可为安全防御体系添加强大的实时监控和响应能力，帮助企业有效预测风险，精准感知威胁。

2.2 技术原理

- **安全策略采集**

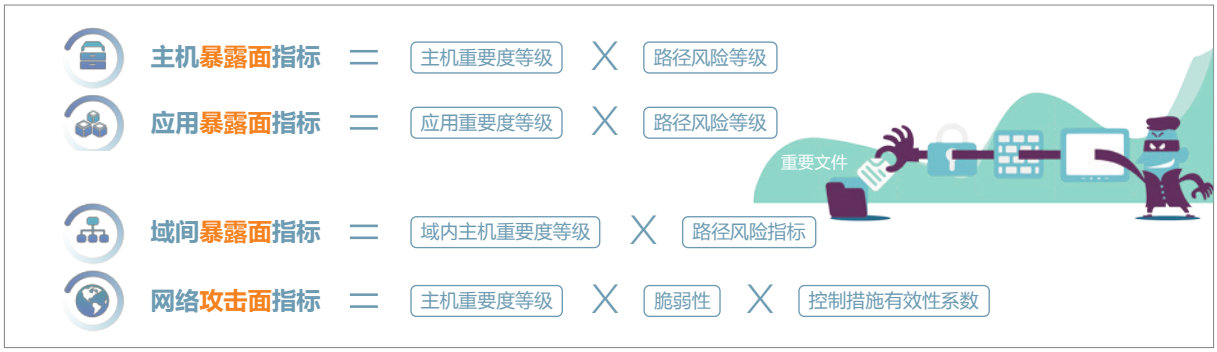
  实现网络中防火墙、路由器、交换机等设备安全控制策略信息的自动提取与解析，提取信息包括对网络安全产生影响的安全访问控制策略、NAT 策略与路由信息等。计算给定网络中任意点到任意点的所有安全访问关系与路径，并运用可视化技术，描绘安全拓扑，实现网络访问关系与安全路径的可视化查询、分析与呈现。

- **攻击面评估指标计算**

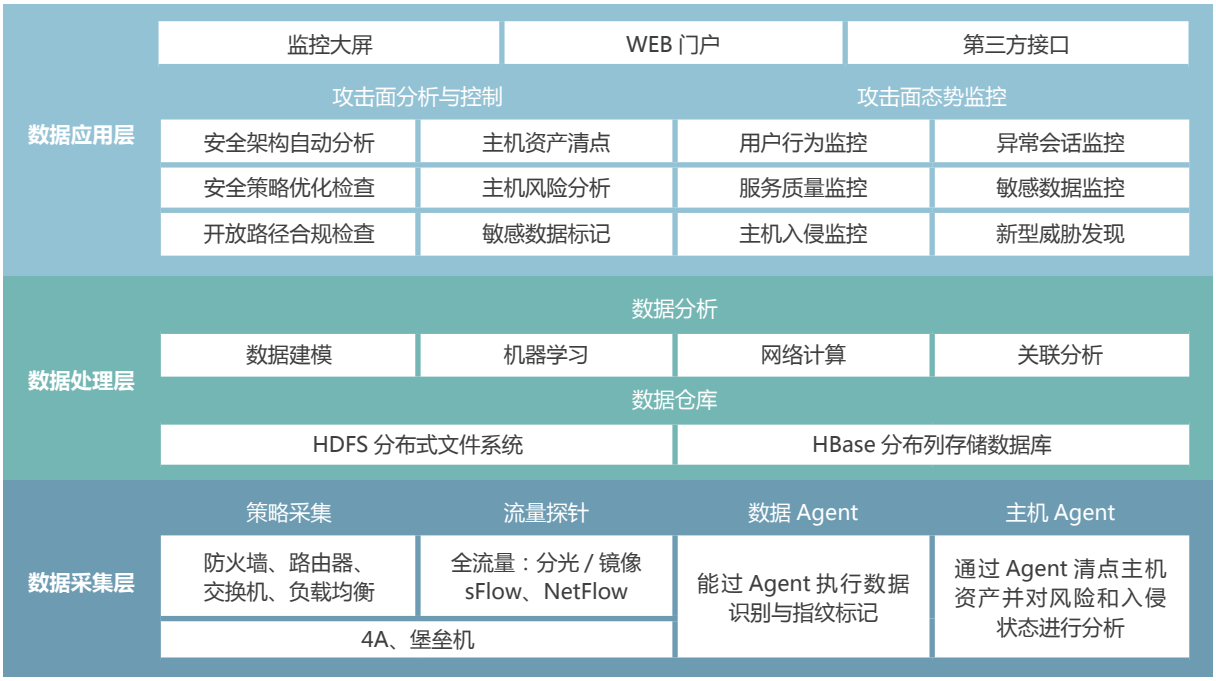
  网络安全基础架构模型之上叠加漏洞发现与评估系统，如网络漏洞扫描、流量分析与主机安全检测等系统，发现网络中的资产与资产所具有的漏洞，分析漏洞对不可信网络的暴露面，包括暴露路径与路径的安全性。综合赋值资产重要程度、资产脆弱性、对外暴露路径与暴露路径的安全性，得出资产、安全域、业务域或网络系统整体的攻击面指标。可结合第三方安全检测能力与威胁情报，关联分析网络异常与安全事件指标，进一步提高攻击面指标的广度、深度与精度。攻击面相关指标计算公示如下：

  R= L × I

  R=（暴露系数 × 资产重要度等级）×（发生的容易度 × 控制措施有效性系数）



2.3 平台架构



平台分为数据采集层、数据处理层和数据应用层三个层面 ,数据采集层分别通过 SSH、Telnet、TCP 等协议以模拟登陆、分光镜像及 Agent 的方式采集设备配置、网络流量、敏感数据及服务器日志等数据，存储到数据处理层的分布式文件系统和分布式列存储数据库中；以数据建模、机器学习、网格计算、关联分析等方法进行数据的融合分析计算，为数据应用层提供数据支撑；数据应用层以监控大屏、Web 门户两种方式提供攻击面分析与控制、攻击面态势监控服务，同时支持提供第三方接口与其他安全管理产品进行功能结合。

功能价值

3.1 网络安全策略可视化

3.1.1 功能介绍

可针对防火墙、路由器、交换机网络节点设备的安全访问控制策略进行优化检查分析，梳理出各类冗余策略、隐藏策略、过期策略、可合并策略、空策略等，管理员可根据分析结果再对策略进行精简和优化调整。

- **隐藏策略**

  同一策略组内 ,该策略的协议、IP、端口均为比其优先级更高策略的子集 ,不管动作是否一致或相反。例如 ,策略 1：A——B/C 允许；策略 2： A——B 允许 (或禁止)，则策略 2 被策略 1 所隐藏，永不会生效。

- **冗余策略**

  同一策略组内 ,该策略的协议、IP、端口与其优先级更高策略存在交叉包含关系或部分包含关系 ,动作一致。例如，策略 1： A——B 允许；策略 2： A——B/C 允许，则策略 2 包含策略 1，策略 1 可删除。

- **合并策略：**

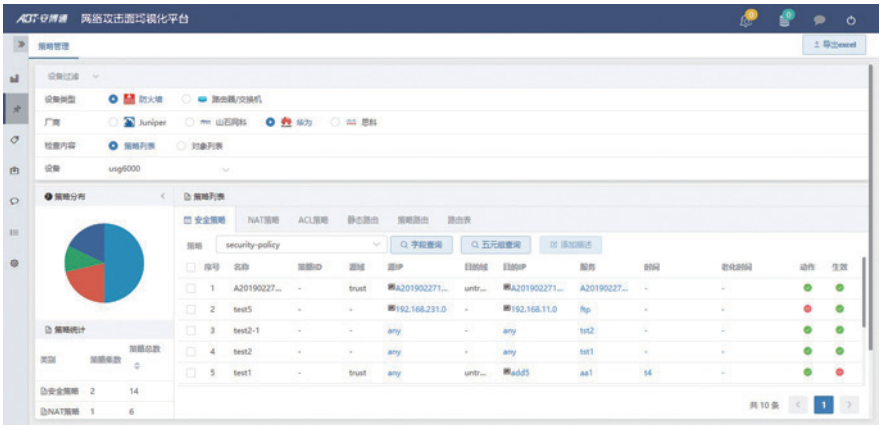
  指两条动作相同的策略，除动作项外，只在有一项不相同，其余均相同。例如，策略 1：192.1.1.1——B 允许；策略 2：192.1.1.2——B 允许，则建议策略 1 和策略 2 合并为一条策略：192.1.1.1/192.1.1.2 —— B 允许。

- **空策略：**

  策略中源地址或目标地址为对象，但对象为空。

- **过于宽松策略：**

  对允许策略中的“源地址、目的地址、服务端口”出现两个 any 选项、没有目标 IP、没有目标端口的访问策略均为识别为过于宽松策略。



3.1.2 功能价值

收缩网络访问权限，降低网络安全风险。当一条范围较宽的允许策略将后续配置的一条禁止策略隐藏，就意味着需要关闭的一条网络通道未关闭，而这条通道是可能被攻击者所利用。另外，过于宽松策略配置，如某条允许策略配置中存在过多的 any 选项，也就意味着开放的网络端口或允许的网络对象范围大，极有可能开放了一些不必要的网络权限，被攻击者利用可能性增大。策略可视化系统可对隐藏策略与宽松策略情况做到有效检查，从而规避由其引发的网络风险。

3.2 安全基础架构可视化

3.2.1 功能介绍

实现防火墙、路由器、交换机设备配置信息的自动提取与解析，解析内容包括对安全访问路径产生影响的路由信息、访问控制、NAT 策略，运用可视化技术，生成网络安全拓扑，安全拓扑体现安全域划分、安全域内业务系统、网络和安全设备节点、网络逻辑连接关系、网络安全访问关系，从而实现全网安全基础架构的可视化展示。

3.2.2 功能价值

通过网络安全基础架构分析与展示，网络管理者可以清晰的看到核心业务资产在网络中的分布，业务系统与网络对象之间的逻辑连接与访问控制关系，在此基础上网络管理者可以看清当前安全域的划分与安全控制设置是否合理，在发生安全事件时，还可基于此对事件处置提供决策依据。如当某一区域某一主机中毒，可以从网络拓扑上分析如何对此主机进行隔离控制，以防止病毒近一步蔓延，为病毒查杀工作争取时间。

3.3 网络暴露面可视化

3.3.1 功能介绍

支持以某一业务或服务器为目的进行 ANY 安全访问关系的查询和分析，并在策略态势总览图中通过连线展示访问关系，可以分析并直观显示网络中哪些源对象可以通过什么端口、协议访问此业务。

支持以某一对象为源，如安全域、网段、主机等进行 ANY 安全访问关系的查询与分析，在策略态势总览图中通过连线展示访问关系，可以分析并直观显示此源对象能够通过某端口、协议访问网络中 ANY 对象。

通过安全路径可视化分析与查询功能，可以轻松查找哪些核心业务开通了特定高危端口号（如 445，3389），哪些区域或网段能访问到核心资产，从而全面掌握重要信息系统与核心关键数据的安全性和风险点。

结合业务流程、应用架构、数据架构等现状，实现在安全基础架构图层上查询与展示安全路径，能够基于源地址、目的地址、常用协议、端口等条件过滤的路径查询与展示，能够显示此路径上的网络与安全节点，能够实现对源到目的多条网络路径可视化，并能够列出影响此路径的相关策略，对网络路径风险处置提供依据。

通过业务访问关系的梳理，设定包括安全域间的网络安全访问控制策略矩阵、业务间的网络安全访问控制策略矩阵、用户与业务间的网络安全访问控制策略矩阵，并能对安全基线矩阵进行持续监控，当发生安全访问关系的非法、非授权修改时，将在安全拓扑图上可视化展示此非法访问关系，相关区域同时闪红。

3.3.2 功能价值

可以基于以上功能发现网络安全控制存在的风险，如，以某一重要业务主机为目的进行查询，查询网络中哪些对象能够通过高危端口（如 3389、139、4489 等）访问此主机，由此可以发现网络中的危险访问通道。再如，基于某一终端域为源进行查询，查询网此终端可以通过 445 端口可以访问到的网络对象，由此可以分析出病毒在网络中的传播路径。

当通过暴露面分析功能发现网络对象间存在含风险的访问关系，可通过此功能进一步查询此访问关系背后的具体路径细节，经过了哪些安全控制节点，可以在此节点上进行安全控制策略调整，以阻断此访问通道，规避此路径风险。另外，策略可视化系统还可以发现两个网络对象间存在多条网络访问路径情况，而其中的某些路径并不是安全设定的主用路径或备用路径，也就是风险冗余路径，这类路径往往不被网络管理人员所知，且防御薄弱，被攻击者利用的可能大。

3.4 重要主机资产可视化

3.4.1 功能介绍

资产清点（Asset Inventory），致力于帮助用户从安全角度自动化构建细粒度资产信息，支持对业务层资产精准识别和动态感知，让保护对象清晰可见。使用 Agent-Server 架构，提供 10 余类主机关键资产清点，200 余类业务应用自动识别，并拥有良好的扩展能力。

1) 主机发现

通过设置检查规则，系统自动检查已安装探针主机，所在网络空间未纳入安全管理的主机，自动排除普通网络设备；针对不同网络状况，提供多种探查方法，包括“ARP 缓存分析”、“Ping 扫描”、“Nmap 扫描”、“连接记录分析”等，客户可灵活选择；功能基于实际业务环境发现主机，减少无意义网络资源消耗，保证探测与被探测主机正常运转。

2) 应用清点

自动化清点进程、端口、账号、中间件、数据库、大数据组件、Web 应用、Web 框架、Web 站点等十余类安全资产，覆盖通用资产；根据每个服务器业务特点，系统针对性识别应用，目前可识别业务应用已覆盖 200 余类，例如 Nginx、Apache、JBoss、Mysql、Memcached、Redis、Hbase 等等，每个应用在风险发现与入侵检测中，均提供对应安全策略保护；未来版本中，将允许自定义清点对象，可根据业务需要，自助清点数据；不同清点对象均采用单独模块管理，模块间保持一定联动性，确保同时运行的清点单元最小化，瞬时性能消耗最低。

3) 资产快速检索

对于每类业务资产，系统提供“主机视角”和“资产视角”两种通用维度，聚合展示数据，每个数据表格列均允许搜索与排序；每个表格额外提供大量可选列（不常用的数据列被默认隐藏），客户可灵活选择需显示的数据，定义自己的表格显示；复杂搜索场景，例如横跨多种资产联合搜索，系统已提供关键资产（主机，账号，进程等）全系统关联，在未来，还将提供全局搜索工具。

4) 资产面板

在获得资产信息后，将结合业务情况，形成“概览视图”与“分级视图”，展示企业整体资产状况。“概览视图”使用图形化的方式展示企业的关键资产状况，帮助用户直观的了解资产；“分级视图”通过树状结构逐层展示资产信息，并显示关键资产的数值，引导用户找到需要的信息；针对每种特定业务资产，产品提供“分析板”功能，多维度剖析单一资产，详细分析内部情况；此外功能还提供一些从安全角度出发的特殊资产视角，引导客户从安全维度发现一些问题。

5) 报表导出与 API 支持

所有数据均提供报表导出功能，可任意选择导出的数据列与数据行，形成自定义报表；所有资产均提供基础API，可结合自身业务情况，获得清点的数据，进行二次开发。

3.4.2 功能价值

1) 自动化构建资产信息，资产清晰可见

通过安装 Agent，可在 15 秒内，从正在运行的环境中，反向自动化构建主机业务资产结构，上报中央管控平台，集中统一管理；独特的主机发现系统，随时发现网络环境内没有纳入安全保护的主机，确保安全覆盖无死角；此外，对 Web 资产与数据库资产等高价值高敏感业务资产，进行了针对性资产建模，与风险发现和入侵检测功能配套提供安全保护。

2) 资产变化实时通知，安全不再落后于业务

生产环境下，业务服务器需要随着业务变化随时扩容或减配，业务资产也随之相应变化；传统安全方案无法完全匹配业务变化，其对资产实施保护的时间往往滞后甚至遗漏，这就给黑客组织可乘之机。平台在清点资产后，将保持对资产持续监控，保证监控数据与实际业务数据一致；对一些需要特殊关注的敏感资产（如：账号、进程、端口，数据库，Web 站点等）发生的变化，将提供实时或定时通知，客户安全团队可进行针对性处理，实现资产动态保护。

3) 灵活的检索方式，快速定位关键

在企业安全检查时，通常需要提供针对性的信息，但面对庞大分散的主机数据，信息梳理效率极低；在发生安全事件时，通常需要获得多角度，跨时间段的数据综合分析，获取这类数据需要横跨多个机构，多个系统，且数据结构杂乱无章，分析难度极大。资产清点参考大量国外先进产品经验，结合通用安全检查规范与安全事件的数据需求，形成细粒度资产清点体系；利用多维度的视图，引导用户轻松获得需要的资产信息；借助多角度的搜索工具，帮助用户快速定位关键资产信息。

3.5 脆弱性风险可视化

3.5.1 功能介绍

风险发现（Vulnerability Discover）致力于帮助用户精准发现内部风险，帮助安全团队快速定位问题并有效解决安全风险，并提供详细的资产信息、风险信息以供分析和响应。

1) 发现未安装的重要补丁

持续更新的补丁库以及 agent 探针式的主动扫描，能及时、精准发现系统需要升级更新的重要补丁，第一时间帮助用户发现潜在可被黑客攻击的危险。深入检测系统中各类应用、内核模块、安装包等各类软件的重要更新补丁，结合系统的业务影响、资产及补丁的重要程度、修复影响情况，智能提供最贴合业务的补丁修复建议。

2) 发现应用配置缺陷导致的安全问题

自动识别应用配置缺陷，通过比对攻击链路上的关键攻击路径，发现并处理配置中存在的问题，大大降低可被入侵的风险。如下图中黑客利用 redis 应用漏洞的攻击链路，针对黑客的每一步探测，系统均会进行持续性的检测，及时发现并处理了某个配置缺陷后，将有效解决潜在安全隐患、阻断黑客的进一步活动。

3) 快速发现系统和应用的新型漏洞

安全分析师团队持续关注国内外最新安全动态及漏洞利用方法，不断推出最新漏洞的检测能力，至今已积累 30000+ 的高价值漏洞库，包括系统 / 应用漏洞、EXP/POC 等大量漏洞，覆盖全网 90% 安全防护。同时，基于 Agent 的持续监测与分析机制，能迅速与庞大的漏洞库进行比对，精准高效地检测出系统漏洞。

4) 智能化的弱口令检测，支持多种应用

精准检测几十种应用弱密码，覆盖企业常用应用如 SSH、Tomcat、MySQL、Redis、OpenVPN 等。识别方法以离线破译优先，且识别弱口令后会对没有发生变化的离线弱口令文件哈希入库，如口令未发生新的变更，不再重复对弱口令进行检测，通过分布式的 Agent 对全量主机的弱口令检测，可极大的提高工作效率，快速的检测弱口令的同时对流量及业务的影响也降到了最低。同时，结合企业特征，系统能智能识别更多组合弱口令，支持用户自定义口令字典以及组合弱口令字典，能有效预防被黑客定向破译的风险。

5) 发现服务器上的违规操作

监控由于运维人员的违规操作引起的安全风险。Agent 会实时监控用户的操作命令，如修改重要配置文件、下载黑客工具、外传数据、bash 危险命令执行等，并结合黑客的攻击手段，持续检测并暴露这些可能存在威胁的安全隐患，及时通知给相关人员进行处理。

6) 发现资产暴露性风险

监测暴露在外的资产风险，如 Web 风险文件、危险进程端口对外、不必要的进程服务、不必要的系统账号等。建立多维分析模型，结合资产重要程度及资产上所有风险进行关联分析，综合分析出最易受攻击的资产。

3.5.2 功能价值

1) 提高攻击门槛，有效缩减 90% 攻击面

在资产细粒度清点的基础上，持续、全面透彻地发现潜在风险及安全薄弱点，根据多维度的风险分析和精确到命令行的处理建议，用户可及时处理重要风险，以限制黑客接触系统、发现漏洞和执行恶意代码，从而大大提高系统的攻击门槛。

2) 企业风险可视化，安全价值清晰可衡量

持续性监测所有主机的安全状况，图形化展现企业风险场景。为安全决策者动态展示企业安全指标变化、安全走势分析，使安全状况的改进清晰可衡量；为安全运维人员实时展示风险分析结果、风险处理进度，提供专业可视化的风险分析报告，使安全管理人员的工作价值得到可视化呈现。

3) 持续性监控分析，及时发现最重要的风险

主动、持续性地监控所有主机上的软件漏洞、弱密码、应用风险、资产暴露性风险等，并结合资产的重要程度进行风险分析，准确定位最急需处理的风险，帮助企业快速有效解决潜在威胁。另外，安全团队持续关注国内外最新安全动态及漏洞利用方法，不断推出最新漏洞的检测能力，实现紧急安全事件快速响应。

3.6 网络入侵可视化

3.6.1 功能介绍

入侵检测提供多锚点的检测能力，能够实时、准确地感知入侵事件，发现失陷主机，并提供对入侵事件的响应手段。

1) 暴力破解监控

通过实时监控登录行为，可以及时且自动化地发现黑客使用不同服务尝试暴力破解用户登录密码的攻击行为，并进行自动化封停处理，使得黑客不能进行更多的尝试。

2) Web 后门监控

通过自动化地监控关键路径，结合正则库，相似度匹配，沙箱等多种检测方法，实时感知文件变化，从而能够及时发现 Web 后门，并对后门影响部分进行清晰标注。

3) 反弹 Shell

通过对用户进程行为进行实时监控，结合行为的识别方法，及时发现进程的非法 Shell 连接操作产生的反弹 Shell 行为，有效感知“0day”漏洞利用的行为痕迹，并提供反弹 Shell 的详细进程树。

4) 本地提权监控

通过对用户进程行为进行实时监控，结合行为识别技术，我们能及时发现进程的提权操作并通知用户，并提供提权操作的详细信息。

5) 系统后门监控

区别于传统的特征分析，我们通过对进程关联信息的分析，结合模式识别和行为检测，提供了不依赖 Hash 的自动化系统后门检测方式，能够实现在多系统中进行多维度、高准度、快速度的后门发现，能够发现包括 Linux 下的 Rootkit、Bootkit，还有 Windows 下的可疑进程、可疑线程等多种后门。

6) 微蜜罐

微蜜罐可以简易灵活的配置，让主机对各端口进行监听，从而扩大监控范围。通过这样消耗小而覆盖面广的蜜罐配置，发现黑客端攻击行为的概率就会大大提升。所谓＂微＂蜜罐，也有“大”作用。

3.6.2 功能价值

1) 多锚点的检测能力，实时发现失陷主机

攻击者通常会同时采用多种手段来攻击用户主机。入侵检测通过多维度的感知网络叠加能力，对攻击路径的每个节点都进行监控，并提供跨平台多系统的支持能力，保证了能实时发现失陷主机，对入侵行为进行告警。

2) 不依赖对漏洞和黑客工具的了解，有效发现未知黑客攻击

传统的入侵检测能力往往依赖于对已知的漏洞和黑客工具的了解，通过基于特征的检测来发现攻击。该方法对于突发的新型漏洞和未知的攻击手段缺乏有效的发现能力，导致许多入侵行为不能被实时发现，从而造成无法挽回的损失。入侵检测结合专家经验，威胁情报、大数据、机器学习等多种分析方法，通过对用户主机环境的实时监控和深度了解，有效发现包括“0day”在内的各种未知黑客攻击。

3) 对业务系统“零”影响

需要进行安全监控的主机，往往也都承载着用户的核心业务系统，比如数据库、Web 后台等等。因此，安全监控对主机性能和业务系统的影响是一个非常重要的指标。Agent 以其轻量高效的特性，在保证对用户主机安全监控的前提下，不对其业务系统产生影响，为用户的主机安全提供了高效可靠的保护。

4) 结合资产信息，为响应提供最准确的一线信息

发现入侵事件只是入侵检测的第一步，提供入侵的详情信息和响应手段才能真正帮助用户解决问题。在独有的资产管理能力支持下，我们不只能发现入侵，更能够提供深入详细的入侵分析和响应手段，从而让用户精准有效地解决问题。

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号楼中兴通3A

电话：010-57649050

网址：www.abtnetworks.com