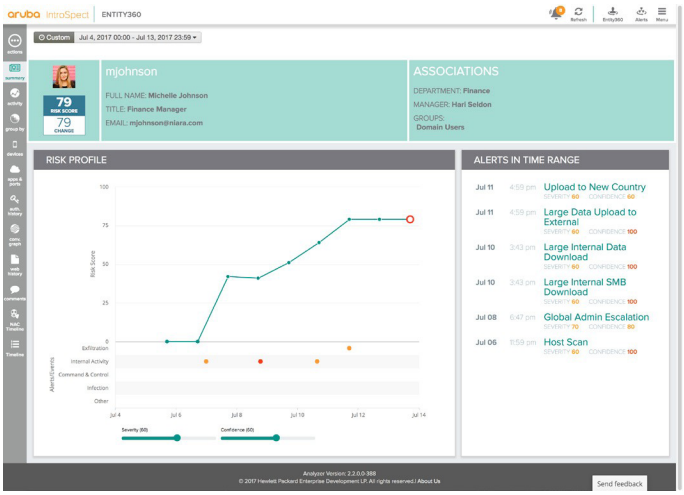
产品资料

Aruba IntroSpect

行为分析安全平台



用户和实体行为分析

Aruba 的用户和实体行为分析（UEBA）解决方案——Aruba IntroSpect 通过发现用户行为中的细微变化来检测攻击，这些变化通常指示已经避开了传统安全防御的内部攻击。Aruba IntroSpect 将先进的基于人工智能的机器学习（ML）、精确可视化和定律洞察力集于一身，具备对恶意、受侵害或粗心用户、系统和设备的洞察力，可在威胁造成损害之前消除威胁。

凭借 Spark/Hadoop 平台，IntroSpect 在企业范围内集成基于行为的攻击检测和适用于法律事件调查及响应。

检测对象：安全分析用例

IntroSpect 提供 100 多个有督导和无督导的创新机器学习模型，专注于在杀伤链的每个阶段检测有针对性的攻击：

- 帐户滥用
- 帐户接管
- 命令与控制
- 数据泄露
- 横向位移
- 密码共享
- 权限提升
- 崩溃风险
- 网络钓鱼
- 勒索软件

主要优势

高级分析

- 100 多个有督导和无督导的创新机器学习模型
- 适应性学习
- 可扩展模型（新的用例、数据源）

最广泛数据源

- 数据包、流量、日志、警报
- 取决于用例的任何组合

不断更新风险评分

- 按严重性、顺序、分布和时间进行加权评分
- 业务环境通知风险评分

快速调查

- 节省 10 倍的时间和精力
- 数据包级别的完整历史记录

快速部署

- 预置软件或云端
- 独立或集成平台
- 从本地或从 SIEM、日志管理、数据包代理中收集数据
- 通过 IntroSpect 标准版简化启动

企业规模

- Spark/Hadoop 平台
- 每天数十亿次事件
- 成千上万的用户和设备

快速调查和响应

从系统管理员到系统到传感器——提供即时可见性

IntroSpect Entity360 是节省了解、诊断和响应攻击所需时间和精力的关键工具。Entity360 提供全面的安全配置文件，包含持续的风险评分和丰富的安全信息——否则分析师可能要花费数小时或数天的时间来搜索数月或数年内积累的安全数据，并将其编译成数据包级别。Entity360：

· 为用户、系统和设备提供所需的配置文件
· 通过开放的应用程序接口（API）访问 SIEM、NAC 系统等
· 提供预装事件响应剧本
· 为客户节省 30 小时 / 调查时间
· 自动检测受到攻击影响的其他实体

威胁捕捉

通过强大的查询接口轻松实现主动威胁捕捉，查找、搜索和汇总数据存储无需支付额外费用。

· 丰富的分析功能可在任何时间范围内检测威胁
· 使用来自 STIX 的 IOC 和自定义威胁源自动搜索历史数据
· 可视化功能指示异常和重大交互
· 监测和标记重大活动，以协助捕捉和调查威胁

数据源

IntroSpect 平台处理最广泛的数据源，包括：

·VPN、FW、IPS/IDS、网络代理、电子邮件日志
·NetFlow、Bro 日志
·EndPoint 保护日志
·DLP 日志
· 数据包
·DNS 日志
· 活动目录日志
·DHCP 日志
· 外部威胁源
· 来自第三方安全体系架构的警报

部署方案

· 本地软件或设备
· 本地 Hadoop 应用程序
·AWS 或 Azure 虚拟私有云（VPC）

主要集成产品制造商

·Aruba ClearPass
·HPE ArcSight
·IBM QRadar
·Splunk
·Intel McAfee Nitro
·Gigamon
·Carbon Black
·Microsoft
·Palo Alto Networks
·FireEye
·Cisco
·Symantec

订购信息

部件号	说明
硬件	
JZ261A	Aruba IntroSpect 5Gbps混合数据包日志和流数据处理器（包括1年支持服务）FPC 2000设备
JZ262A	Aruba IntroSpect 5Gbps混合数据包日志和流数据处理器（包括1年支持服务）PP 1000设备
JZ263A	Aruba IntroSpect Analyzer 2000（包括1年支持服务）设备
JZ264A	Aruba IntroSpect Analyzer 2500（包括1年支持服务和SSD）硬件
JZ265A	Aruba IntroSpect Analyzer 1000分析仪节点（包括1年支持服务和铜管理端口）设备
JZ266A	Aruba Intro Spectra Analyzer 1000计算节点（包括1年支持服务和铜管理端口）设备
JZ267A	Aruba IntroSpect Analyzer 1050分析仪节点（包括1年支持服务和光纤管理端口）设备
JZ268A	Aruba IntroSpect Analyzer 1050计算节点（包括1年支持服务和光纤管理端口）设备
JZ269A	Aruba IntroSpect Analyzer 1500分析仪节点（包括1年支持服务、SSD和铜管理端口）设备
JZ270A	Aruba IntroSpect Analyzer 1500计算节点（包括1年支持服务、SSD和铜管理端口）设备
JZ271A	Aruba IntroSpect Analyzer 1550分析仪节点（包括1年支持、SSD和光纤管理端口）设备
JZ272A	Aruba IntroSpect Analyzer 1550计算节点（包括1年支持服务、SSD和光纤管理端口）设备
JZ273A	Aruba IntroSpect Switch 24端口10G（包括1年支持服务）设备
软件：数据包处理软件定价——订阅	
JZ231AAE	Aruba IntroSpect数据包处理器100Mbps 1年E-STU
JZ232AAE	Aruba IntroSpect数据包处理器100Mbps 3年E-STU
JZ233AAE	Aruba IntroSpect数据包处理器100Mbps永久E-LTU
软件：全数据包捕获软件定价——订阅	
JZ234AAE	Aruba IntroSpect全数据包捕获100Mbps 1年E-STU
JZ235AAE	Aruba IntroSpect全数据包捕获100Mbps 3年E-STU
JZ236AAE	Aruba IntroSpect全数据包捕获100Mbps永久E-LTU
软件：分析仪软件定价——订阅	
JZ237AAE	Aruba IntroSpect安全分析标准版1K实体（用户、服务器和物联网）1年E-STU
JZ238AAE	Aruba IntroSpect安全分析标准版1K实体（用户、服务器和物联网）3年E-STU
JZ239AAE	Aruba IntroSpect安全分析标准版1K实体（用户、服务器和物联网）永久E-LTU
JZ240AAE	Aruba IntroSpect安全分析高级版1K实体（用户、服务器和物联网）1年E-STU
JZ241AAE	Aruba IntroSpect安全分析高级版1K实体（用户、服务器和物联网）3年E-STU
JZ242AAE	Aruba IntroSpect安全分析高级版1K实体（用户、服务器和物联网）永久E-LTU
JZ243AAE	Aruba IntroSpect标准版安全分析升级到高级版1K实体1年E-STU
JZ244AAE	Aruba IntroSpect标准版安全分析升级到高级版1K实体3年E-STU
JZ245AAE	Aruba IntroSpect标准版安全分析升级到高级版1K实体永久E-LTU

订购信息	
部件号	说明
软件：其他许可方案	
JZ246AAE	Aruba IntroSpect Analyzer HA标准版1K实体（用户、服务器和物联网）1年E-STU
JZ247AAE	Aruba IntroSpect Analyzer HA标准版1K实体（用户、服务器和物联网）3年E-STU
JZ248AAE	Aruba IntroSpect Analyzer HA标准版1K实体（用户、服务器和物联网）永久E-LTU
JZ249AAE	Aruba IntroSpect Analyzer高级版1K实体（用户、服务器和物联网）1年E-STU
JZ250AAE	Aruba Intro Spectra Analyzer高级版1K实体（用户、服务器和物联网）3年E-STU
JZ251AAE	Aruba IntroSpect Analyzer高级版1K实体（用户、服务器和物联网）永久E-LTU
JZ252AAE	Aruba IntroSpect Analyzer HA标准版升级到高级版1K实体1年E-STU
JZ253AAE	Aruba IntroSpect Analyzer HA标准版升级到高级版1K实体3年E-STU
JZ254AAE	Aruba IntroSpect Analyzer HA标准版升级到高级版1K实体永久E-LTU
实验室许可证	
JZ255AAE	Aruba IntroSpect Analyzer实验室许可证1年E-STU
JZ256AAE	Aruba IntroSpect Analyzer实验室许可证3年E-STU
JZ257AAE	Aruba IntroSpect Analyzer实验室许可证永久E-LTU
JZ258AAE	Aruba IntroSpect数据包处理器实验室许可证1年E-STU
JZ259AAE	Aruba IntroSpect数据包处理器实验室许可证3年E-STU
JZ260AAE	Aruba IntroSpect数据包处理器实验室许可证永久E-LTU
维护——软件	
	Aruba IntroSpect Analyzer标准版1K实体1年支持服务E-STU
	Aruba IntroSpect Analyzer高级版1K实体1年支持服务E-STU
	Aruba IntroSpect Analyzer HA标准版1K实体1年支持服务E-STU
	Aruba Intro Spectra Analyzer高级版1K实体1年支持服务E-STU
	Aruba IntroSpect 100Mbps数据包处理1年支持服务E-STU
	Aruba IntroSpect 100Mbps全数据包捕获1年支持服务E-STU

Aruba IntroSpect标准版和高级版型号通常在北美地区出售，在其他地区的可用性有限。预计到2018年将实现全球销售。联系我们了解更多有关国家/地区可用性的信息。

Aruba——慧与（中国）有限公司旗下公司

Aruba 是慧与公司旗下公司，是面向全球各类规模企业的新一代网络解决方案的领先供应商。公司提供 IT 解决方案，帮助组织为工作和个人生活的各个方面依赖基于云的商业应用的新一代精于移动之道的用户提供服务。请访问 www.arubanetworks.com 了解更多信息。关于 Twitter 和 Facebook 上 Aruba 的实时新闻更新，以及有关移动领域和 Aruba 产品的最新技术讨论，请访问 Airheads Social：http://community.arubanetworks.com。

a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
1.844.473.2782 | 电话 : 1.408.227.4500 | 传真 : 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com