

Overview

Aruba IntroSpect User and Entity Behavior Analytics

Product overview

Aruba's User and Entity Behavior Analytics (UEBA) solution, Aruba IntroSpect, detects attacks by spotting small changes in behavior that are often indicative of attacks that have evaded traditional security defenses. Aruba IntroSpect integrates advanced AI-based machine learning (ML), pinpoint visualizations and instant forensic insight into a single solution, so attacks involving malicious, compromised or negligent users, systems and devices are found and remediated before they damage the operations and reputation of the organization.

With a Spark/Hadoop platform, IntroSpect uniquely integrates both behavior-based attack detection and forensically-rich incident investigation and response at enterprise scale.

What We Detect: Security Analytics Use Cases

IntroSpect provides 100+ supervised and unsupervised machine learning models focused on detecting targeted attacks at each stage of the kill chain:

- Account Abuse
 - Account Takeover
 - Command and Control
 - Data Exfiltration
 - Lateral Movement
 - Password Sharing
 - Privilege Escalation
 - Flight Risk
 - Phishing
 - Ransomware
-

Key Benefits

Advanced Analytics

- 100+ supervised and unsupervised machine learning models
- Adaptive learning
- Extensible models (new use cases, data sources)

Widest Range of Data Sources

- Packets, flows, logs, alerts
- Any combination depending on use cases

Continuously Updated Risk Scoring

- Weighted by severity, sequence, distribution and time
- Business context informs risk score

Overview

Accelerated Investigations

- 10x reduction time and effort
- Complete historical record down to packet level

Fast Deployment

- On-prem or cloud
- Standalone or integrated platform
- Ingest data natively or from SIEM, log management, packet broker
- Streamlined start via IntroSpect Standard Edition

Enterprise Scale

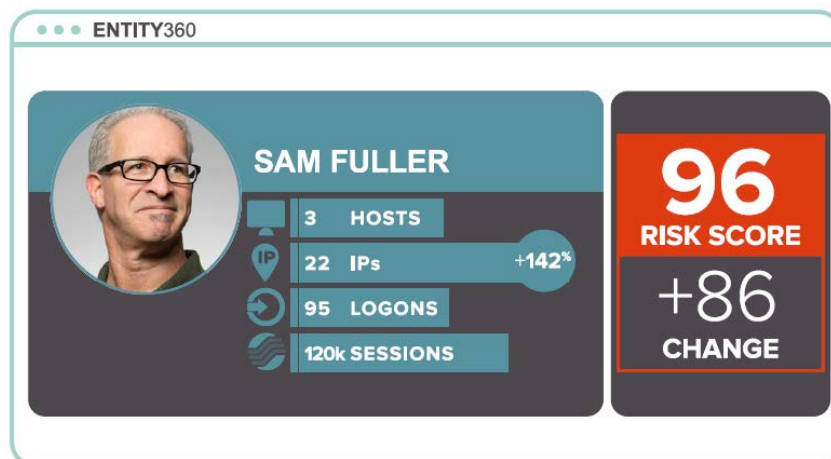
- Spark/Hadoop platform
- Billions of events per day
- Hundreds of thousands of users and devices

Accelerated Investigation and Response

From SysAdmins to Systems to Sensors — Providing Instant Visibility

IntroSpect Entity360 is key to reducing the time and effort required to understand, diagnose and respond to an attack. Entity360 provides a comprehensive security profile with continuous risk scoring and enriched security information – analysts would otherwise spend hours or days searching for and compiling months and years of security data down to the packet level. Entity360 provides:

- Profiles for users, systems and devices
- Access by SIEM, NAC systems, etc. via an open API
- Pre-packaged incident response playbooks
- Customer-measured 30 hours/investigation savings
- Automatic detection of other entities impacted by the attack



Threat Hunting

Overview

Proactive threat hunting is easily accomplished with a powerful query interface, without the overhead of finding, searching, and summarizing isolated data stores.

- Rich analytics to test threat hypotheses across any timeframe
 - Automated search of historical data using IOC's from STIX and custom threat feeds
 - Visualizations to highlight anomalies and significant interactions
 - Significant activity monitored and tagged to assist with both hunting and investigations
-

Data Sources

The IntroSpect platform processes the broadest range of data sources, including:

- VPN, FW, IPS/IDS, Web proxy, Email logs
 - NetFlow, Bro logs
 - EndPoint protection logs
 - DLP logs
 - Packets
 - DNS logs
 - Active Directory logs
 - DHCP logs
 - External threat feeds
 - Alerts from 3rd party security infrastructure
-

Deployment Options

- On-premise software or appliance
 - On-premise Hadoop application
 - AWS or Azure Virtual Private Cloud (VPC)
-

Key Integrations

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

Configuration

Ordering Information

Description	Part Number
Hardware	
Aruba IntroSpect 5Gbps Hybrid Packet Log and Flow Data Processor (with 1yr Support) FPC 2000 Appliance	JZ261A
Aruba IntroSpect 5Gbps Hybrid Packet Log and Flow Data Processor (with 1yr Support) PP 1000 Appliance	JZ262A
Aruba IntroSpect Analyzer 2000 (includes 1yr Support) Appliance	JZ263A
Aruba IntroSpect Analyzer 2500 (includes 1yr Support and SSD) Hardware	JZ264A
Aruba IntroSpect Analyzer 1000 Analyzer Node (includes 1yr Support and Copper Mgmt Port) Appliance	JZ265A
Aruba IntroSpect Analyzer 1000 Compute Node (includes 1yr Support and Copper Mgmt Port) Appliance	JZ266A
Aruba IntroSpect Analyzer 1050 Analyzer Node (includes 1yr Support and Fiber Mgmt Port) Appliance	JZ267A
Aruba IntroSpect Analyzer 1050 Compute Node (includes 1yr Support and Fiber Mgmt Port) Appliance	JZ268A
Aruba IntroSpect Analyzer 1500 Analyzer Node (with 1yr Support and SSD and Copper Mgmt Port) Appliance	JZ269A
Aruba IntroSpect Analyzer 1500 Compute Node (with 1yr Support and SSD and Copper Mgmt Port) Appliance	JZ270A
Aruba IntroSpect Analyzer 1550 Analyzer Node (with 1yr Support and SSD and Fiber Mgmt Port) Appliance	JZ271A
Aruba IntroSpect Analyzer 1550 Compute Node (with 1yr Support and SSD and Fiber Mgmt Port) Appliance	JZ272A
Aruba IntroSpect Switch 24-Port 10G (includes 1yr Support) Appliance	JZ273A
Software: Packet Processing Software Pricing – Subscription	
Aruba IntroSpect Packet Processor 100Mbps 1yr E-STU	JZ231AAE
Aruba IntroSpect Packet Processor 100Mbps 3yr E-STU	JZ232AAE
Aruba IntroSpect Packet Processor 100Mbps Perpetual E-LTU	JZ233AAE
Software: Full Packet Capture Software Pricing – Subscription	
Aruba IntroSpect Full Packet Capture 100Mbps 1yr E-STU	JZ234AAE
Aruba IntroSpect Full Packet Capture 100Mbps 3yr E-STU	JZ235AAE
Aruba IntroSpect Full Packet Capture 100Mbps Perpetual E-LTU	JZ236AAE
Software: Analyzer Software Pricing – Subscription	
Aruba IntroSpect Security Analytics Standard Ed 1K Entities (Users and Servers and IoT) 1yr E-STU	JZ237AAE
Aruba IntroSpect Security Analytics Standard Ed 1K Entities (Users and Servers and IoT) 3yr E-STU	JZ238AAE
Aruba IntroSpect Security Analytics Std Ed 1K Entities (Users and Servers and IoT) Perpetual E-LTU	JZ239AAE
Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) 1yr E-STU	JZ240AAE
Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) 3yr E-STU	JZ241AAE
Aruba IntroSpect Security Analytics Advanced Ed 1K Entities (Users and Servers and IoT) Perp E-LTU	JZ242AAE
Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities 1yr E-STU	JZ243AAE
Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities 3yr E-STU	JZ244AAE
Aruba IntroSpect Security Analytics Standard to Advanced Upgrade 1K Entities Perp E-LTU	JZ245AAE
Software: Additional Licensing Options	
Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) 1yr E-STU	JZ246AAE
Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) 3yr E-STU	JZ247AAE
Aruba IntroSpect Analyzer HA Standard Ed 1K Entities (Users and Servers and IoT) Perpetual E-LTU	JZ248AAE
Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) 1yr E-STU	JZ249AAE
Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) 3yr E-STU	JZ250AAE

Configuration

Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities (Users and Servers and IoT) Perp E-LTU	JZ251AAE
Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities 1yr E-STU	JZ252AAE
Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities 3yr E-STU	JZ253AAE
Aruba IntroSpect Analyzer HA Standard to Advanced Upgrade 1K Entities Perp E-LTU	JZ254AAE

Lab Licenses

Aruba IntroSpect Analyzer Lab License 1yr E-STU	JZ255AAE
Aruba IntroSpect Analyzer Lab License 3yr E-STU	JZ256AAE
Aruba IntroSpect Analyzer Lab License Perpetual E-LTU	JZ257AAE
Aruba IntroSpect Packet Processor Lab License 1yr E-STU	JZ258AAE
Aruba IntroSpect Packet Processor Lab License 3yr E-STU	JZ259AAE
Aruba IntroSpect Packet Processor Lab License Perpetual E-LTU	JZ260AAE

Maintenance – Software

Aruba IntroSpect Analyzer Standard Ed 1K Entities 1 yr Support E-STU
Aruba IntroSpect Analyzer Advanced Edition 1K Entities 1yr Support E-STU
Aruba IntroSpect Analyzer HA Standard Edition 1K Entities 1yr Support E-STU
Aruba IntroSpect Analyzer HA Advanced Edition 1K Entities 1yr Support E-STU
Aruba IntroSpect 100Mbps Packet Processing 1yr Support E-STU
Aruba IntroSpect 100Mbps Full Packet Capture 1yr Support E-STU

Summary of Changes

Date	Version History	Action	Description of Change
07-Aug-2017	Version 1	Created	Document Creation



Sign up for updates



**Hewlett Packard
Enterprise**

© Copyright 2017 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

To learn more, visit: <http://www.hpe.com/networking>

a00018425 - 15985 - Worldwide - V1 - 07-August-2017