Best Practices for Deploying ClearPass Device Insight

Viswesh Ananthakrishnan, Senior Director, Product Management
Agenda

ClearPass Device Insight Architecture
Discovery and Augmentation
Filtering and Tagging
CPPM Integration
POC Stats
Best Practices
ARUBA SECURITY USER/DEVICE LIFE CYCLE

Aruba 360 Security

Authorize

Respond

Monitor

Enforce

Discover

ClearPass Device Insight

IT access based on user/device attributes

Detect attacks with range of analytics

Act on attacks with a wide range of policy actions

Visibility through profiling and classification
CURRENT CHALLENGES IN DEVICE VISIBILITY

IT/Security teams lack visibility into devices on the network i.e. factory controllers, medical equipment

Current toolset fails to adequately address visibility and IoT use cases

Volume, variety and the innovation of “things” means manual approaches cannot keep pace

Without comprehensive visibility, effective security and compliance is not possible
CLEARPASS DEVICE INSIGHT

OVERVIEW

Reduces Risk by Eliminating Blind Spots through DPI-based discovery and profiling of devices

Automatically Clusters Unknown Devices and recommends classification using advanced machine learning and crowdsourcing intelligence

Ensures Secure Access via seamless integration with ClearPass Policy Manager
ClearPass Device Insight Architecture
ARCHITECTURE OVERVIEW

Combination of on-premises data collector (appliance or virtual) and cloud-based analyzer

Through Deep Packet Inspection (DPI), device attributes are extracted and metadata is sent to the cloud for analysis.
Recommended Collector Placement (SPAN)
Recommended Collector Placement (Packet Broker)
Discovery and Augmentation
Device Discovery and Augmentation Methods

• **Device Discovery**
  • *Subnet Scans* discover devices by probing the subnets within a specific segment.
  • *Discovery Scans* discover devices by probing the network starting with one or more seed devices (switches or routers) and scanning to a network depth that you specify.

• **Passive Profiling**
  • *Deep Packet Inspection*: When connected to a SPAN port on a switch, the network traffic will be used to identify endpoints, the protocols they are using on the network and the applications generating the network traffic.
    • SPAN
    • Packet Broker
    • IP Helper/DHCP

• **Augmentation Methods (Active Profiling)**
  • *NMAP port scans*: These scans collect IP Address, open ports and services running from any device.
  • *WMI scans*: These will gather OS version from Windows devices.
  • *SSH scans*: These will login to remote hosts with the provided credentials and gather the Mac Address, IP Address, Host Name from Mac/Linux devices.
  • *SNMP scans*: These will collect IP Address, device name, device type, sys description, switch ip and switch ports and SSID (for wireless endpoints).
Augmentation Methods by Use Case

**Active**
- This method contacts the endpoints

**Passive**
- This method does not contact the endpoints

<table>
<thead>
<tr>
<th>Use Case</th>
<th>SPAN (Device Behavior)</th>
<th>DHCP (IP Helper)</th>
<th>NMAP Scan</th>
<th>NAD SNMP Poll (ARP/Ports)</th>
<th>SNMP Poll (System Description)</th>
<th>WMI Scan</th>
<th>SSH Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery (Dynamic IP)</td>
<td>Required</td>
<td>Required</td>
<td>Recommended</td>
<td>Recommended (for location info)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Discovery (Static IP)</td>
<td>Required</td>
<td>N/A</td>
<td>Recommended</td>
<td>Required</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>User-Based</td>
<td>Recommended</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>IOT*</td>
<td>Required</td>
<td>Required</td>
<td>Recommended</td>
<td>Required</td>
<td>Recommended</td>
<td>Optional</td>
<td>Optional</td>
</tr>
</tbody>
</table>

* For environments with mission-critical, but sensitive IoT devices such as manufacturing or healthcare, it is recommended that those devices be excluded from active scanning techniques as a precaution against adversely impacting their performance.
The evolution of device profiling

- **Basic**
  - Apple iPad
  - MAC, DHCP Based
    - DHCP Options
    - DHCP Fingerprint
    - MAC OUI
  - Apple iPad Connected to 3rd Floor AP

- **Actionable**
  - Conference Room iPad on the 3rd Floor running the scheduling app
  - Behavior Based
    - SPAN
    - HTTP User Agent
    - Netflow/sFlow
    - Applications, metadata
    - Domain Names
    - Communication Patterns

- **Unhelpful**
  - Scan Based
    - IP/MAC
    - Wired or Wireless Location (SNMP)
  - Device Vendor
    - IP Address
    - Operating System
    - Applications
    - Open Ports

---

The evolution of device profiling.

Apple iPad
MAC, DHCP Based
- DHCP Options
- DHCP Fingerprint
- MAC OUI

Conference Room iPad on the 3rd Floor running the scheduling app

Behavior Based
- SPAN
- HTTP User Agent
- Netflow/sFlow
- Applications, metadata
- Domain Names
- Communication Patterns

Scan Based
- IP/MAC
- Wired or Wireless Location (SNMP)

Device Vendor
- IP Address
- Operating System
- Applications
- Open Ports
Filtering and Tagging
Filters

Filters are a method for finding devices based on any of their available attributes in ClearPass Device Insight.

A filter can match a group of devices which will be presented as a list which can be used as the basis of a report.

Filters are not persistent.

The only way to recall those devices which match the criteria you selected for your filter would be to save the filter as a tag.
Tags

Once a filter is saved as a tag, ClearPass Device Insight will maintain a list of all endpoints which match the criteria selected in the filter.

If a new device is discovered which matches the criteria, then it will automatically inherit the tag.

If a device no longer matches the criteria, the tag is removed automatically.

Tags can be selected in the UI to bring up a list of devices currently matching the criteria of the tag. The number following the tag name shows the current number of devices matching this tag.

The tag follows the endpoint.

An endpoint can have an unlimited number of tags.

The tag provides the ability to add more context to endpoints which could then be used as part of a policy.
Classification (Is a) vs. Tags (Has a)

Generic Car

Classification: Mercedes

Tag: 3-pronged star Logo

Classification $\iff$ ‘type’
Tag $\iff$ ‘property’
CPPM Integration
Integration Summary

ClearPass Device Insight

- Benefits from authentication and posture information for endpoints authenticated by CPPM.

ClearPass Policy Manager

- Integration requires ClearPass 6.8.1 or later
- Benefits from additional endpoint context information from CPDI.
- Device classification is moved to CPDI and is no longer handled locally.
- Requires a persistent connection to the Aruba Central cloud.
- New authorization options post integration.
ClearPass Device Insight Integration with ClearPass Policy Manager

From ClearPass Device Insight

Device Classification

Additional Context for endpoints

To ClearPass Policy Manager

Bi-directional event driven updates

To ClearPass Device Insight

Endpoint Authentication Context

Additional Context for endpoints

From ClearPass Policy Manager
Rule types in CPPM which get their information from CPDI after enabling integration

- **Authorization:[Endpoints Repository] Application Group**: A group of applications used by the endpoint (collaboration.file-sharing)
- **Authorization:[Endpoints Repository] Application ID**: A specific application used by the endpoint (dropbox)
- **Authorization:[Endpoints Repository] Destination Connections**: A destination host, port and protocol in the following format – 10.23.1.9:53:udp
- **Authorization:[Endpoints Repository] Open Ports**: A port number by itself which was found to be open on the endpoint.
- **Endpoint: Device Insight Tags**: Any tags which currently apply to this endpoint.
ClearPass Device Insight Tags used in enforcement policy
Endpoint profiling flow for devices discovered by ClearPass Policy Manager during authentication

1. Receive updates about the endpoint in near realtime*
2. Gather and store new endpoint data in the endpoints db
3. Sync the updated endpoints with CPDI
Endpoint profiling flow for devices discovered by ClearPass Device Insight

Discover new endpoints

Classify the endpoints

Update CPPM's endpoints repository
CPDI Proof of Concept Stats
<table>
<thead>
<tr>
<th>POC Stats*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>63 Total Inquiries</strong></td>
<td><strong>40 Already use CPPM</strong></td>
</tr>
<tr>
<td>Largest Environment: 600,000 endpoints</td>
<td>20+ currently active worldwide</td>
</tr>
</tbody>
</table>

* When this deck was published in mid-August
POC Stats: Which Industry Verticals Have Expressed Interest

<table>
<thead>
<tr>
<th>Industry Vertical</th>
<th>Interest</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare</td>
<td>20</td>
</tr>
<tr>
<td>Education</td>
<td>10</td>
</tr>
<tr>
<td>Retail</td>
<td>9</td>
</tr>
<tr>
<td>Service Provider</td>
<td>3</td>
</tr>
<tr>
<td>Government</td>
<td>3</td>
</tr>
<tr>
<td>Finance</td>
<td>3</td>
</tr>
<tr>
<td>Hospital</td>
<td>2</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2</td>
</tr>
<tr>
<td>Other</td>
<td>11</td>
</tr>
</tbody>
</table>
POC Stats: How many customers want visibility + enforcement

Visibility Only vs Enforcement

- Visibility Only: 10%
- Visibility Plus Enforcement: 90%
POC Stats: Available Data Sources

<table>
<thead>
<tr>
<th>Data Source</th>
<th>No</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPAN or Packet Broker</td>
<td>11.1</td>
<td>88.9</td>
</tr>
<tr>
<td>DHCP (From IP Helper Configuration)</td>
<td>1.6</td>
<td>98.4</td>
</tr>
<tr>
<td>Device Discovery through SNMP</td>
<td>1.6</td>
<td>98.4</td>
</tr>
<tr>
<td>Active Subnet Scans</td>
<td>9.5</td>
<td>90.5</td>
</tr>
</tbody>
</table>
Best Practices
Best Practices

Rules:
• Creating rules for classifying devices should be done with as many attributes as possible to be as specific as possible.
• Take a moment to study the existing rule that will overlap and then modify your rules accordingly.
• When overlapping rules are created, only the first rule created will be applied and the other overlapping rules will be unused.

Tags:
• Tags are independent of device classifications. Multiple tags can exist for a given device. As such, avoid overriding a device classification if the only difference is the context of the device.
• For example, there might be a group of Samsung Smart TVs on the network used for digital signage. Rather than changing the classification to indicate that they are used for digital signage, create a tag and apply the tag to those devices and let the tag indicate that the Smart TVs are for digital signage while the device classification stays as a Samsung Smart TV.
Best Practices

Segments and Subnets:

- In the analyzer UI, there is a concept of Segments and Subnets. Although it is possible to proceed without defining those, the best practice is to carefully plan for creating segments and subnets.
- Well defined segments and subnets allows for better reporting and filtering.
- Because active profiling scans such as NMAP, SSH, WMI and SNMP are enabled per segment, defining segments correctly is critical for making sure that only the right scans are done for any given subnet.
- For example, if there should be no Windows devices in a given subnet, then scanning with WMI is unnecessary at best.
Best Practices

CPPM Integration:

• The integration is still in its early stages where the first use cases are enhanced visibility and reporting. Start integration with CPPM via lab deployments, before going to production deployments.

• Avoid creating quarantine type policies based on Application ID or Application Group because those attributes are not refreshed very quickly today.
atmosphere

2019 APAC

Questions?
Thank You
Download the Event App
Gain access to the latest event information.

Rate this session
Access this survey via the mobile app and let us know what you think.

Locate this session:
- Agenda
- Select Date
- Find this session
- Click Survey
Join the Airheads Community
Scan the QR code to sign up now!

Ask Aruba
- Session 1: Tuesday, 24 Sep, 2:00pm – 2:45pm
- Session 2: Wednesday, 25 Sep, 1:45pm – 2:30pm
- Location: Town Hall at Tech Playground

Submit your Ask Aruba questions using the mobile app now!

Scan. Play. Win.
Play Now! Switch your thinking, say goodbye to the old ways and get ready for new innovations.

Visit the Tech Playground now!