aruba
a Hewlett Packard Enterprise company

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN

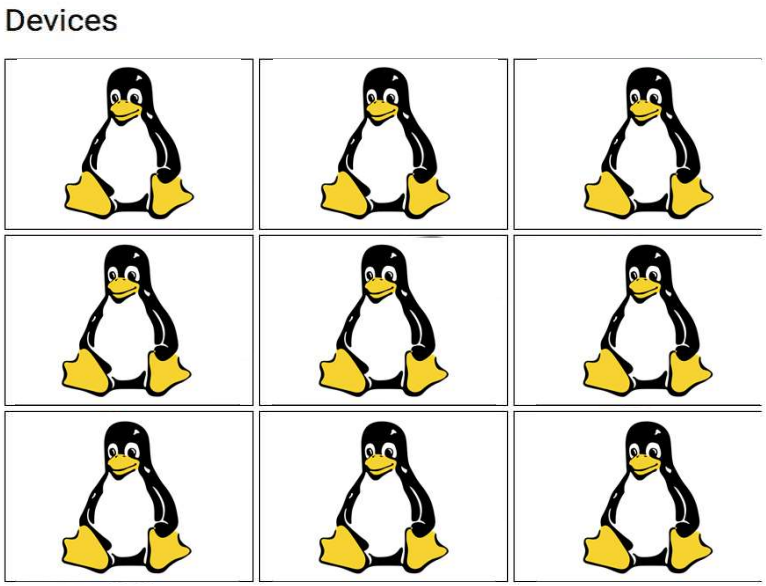
Endpoint Classification

Im Zeitalter von Cloud & IoT

Oliver Wehrli, Technology Consultant

#HSLU

Device Landscape is Increasing the Attack Surface



An increasing number of heterogenous, unknown devices are connected to the network

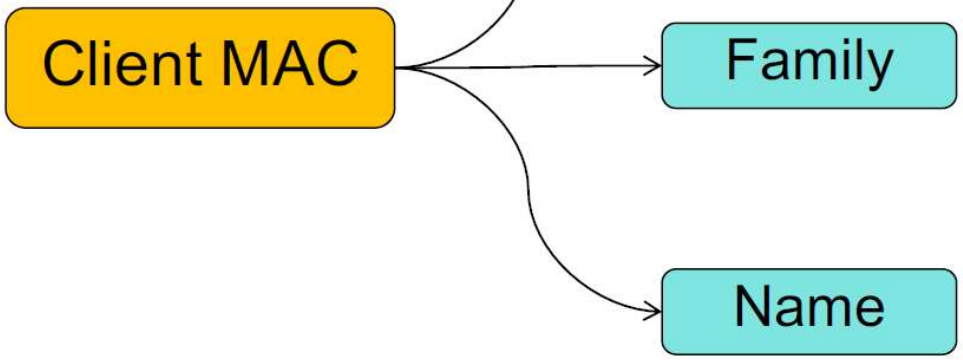
Security teams need better visibility into these devices and the growing attack surface

aruba
a Hewlett Packard Enterprise company

From Generic To Granular

aruba
a Hewlett Packard Enterprise company

What is a device profile?



- AP
- Computer
- Game Console
- Camera
- Smart Device

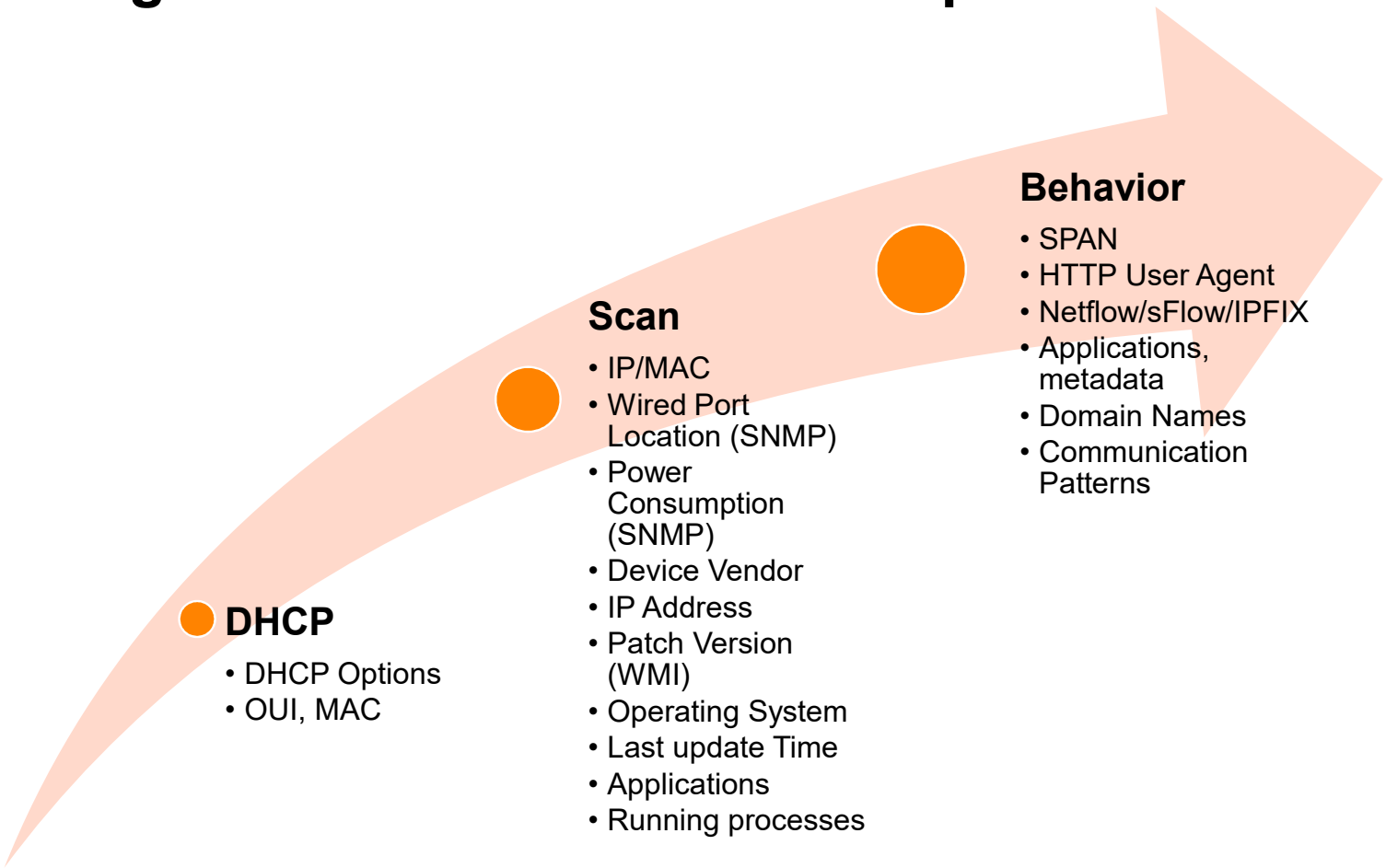
- Aruba AP
- Windows
- Android
- Apple

- Aruba AP 135
- Android Tablet
- Apple iPad
- Xerox Printer

Attributes

- MAC Vendor
- IP Address
- Hostname
- Switch port/AP location
- Conflict / Alternate profile

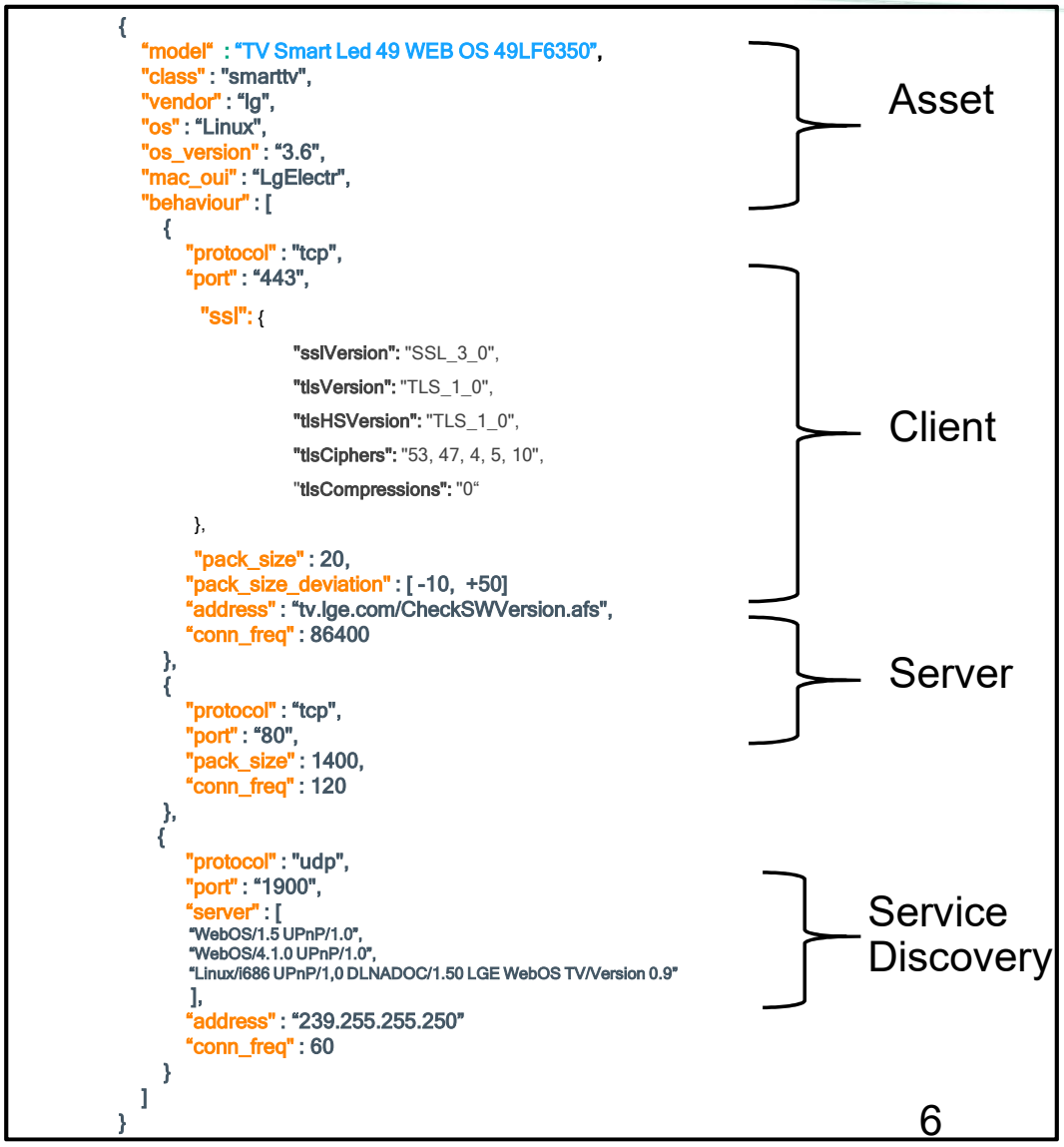
More profiling feeds create richer device profiles



Modelling an Endpoint

- Model **dynamic behavior**
  - Asset
  - Client
  - Server
  - Service discovery

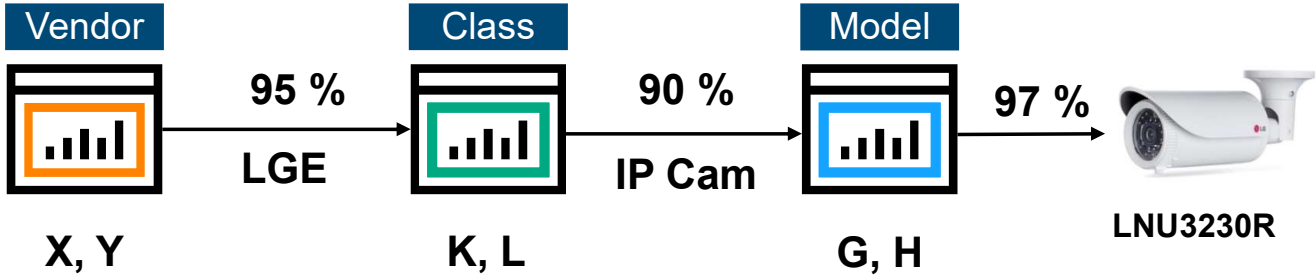
- Example Parameters
  - MAC_OUI, DHCP options
  - Operating System
  - Connections to a server using SSL on port 443
  - Used as HTTP Server on port 80
  - Uses SSDP on UDP port 1900 to annouce services every min



aruba
a Hewlett Packard Enterprise company

From context to classification

Weighted Bayesian Network



Training

Devices Database

MAC OUI	DHCP Vendor	Vendor
Hewlett-Packard	Hewlett-Packard JetDirect	HP
LgElectr	NA	LGE
LgElectr	LG Eletr	LGE
Sony	udhcp 1.15.3	Sony
Samsung	NA	Samsung
NOVELL	NA	Centrium

DHCP OPTS	Roles	TCP SYN	Class
1,3,10,35,20,50	Client	5FDAD1	IP Cam
1,3,10,35,20,50	Client Server	3235FD	IP Cam
2,5,6,9,15,60	Client	78DD69	smarttv
2,5,6,13,15,60	Client	DA4689	smarttv

Connection	SSL Ciphers	DHCP 55	Model
cam.lg.com:443	1,3,8,9,3	3,7,8,15,60	LNU3230R
:554		3,7,8,15,61	LNB5320
local:8080		3,7,8,15,62	LNU7210R

Machine Learning-based Device Classification

Discovered Devices

Static Rules

Classify known devices with established patterns

Rule Matches

Device Identified and Labeled

No Rule Match

ML-based Classification

Classification based on static, flow and behavior based attributes

aruba
a Hewlett Packard Enterprise company

Collectors and Profiles

There are two components to Profiling:

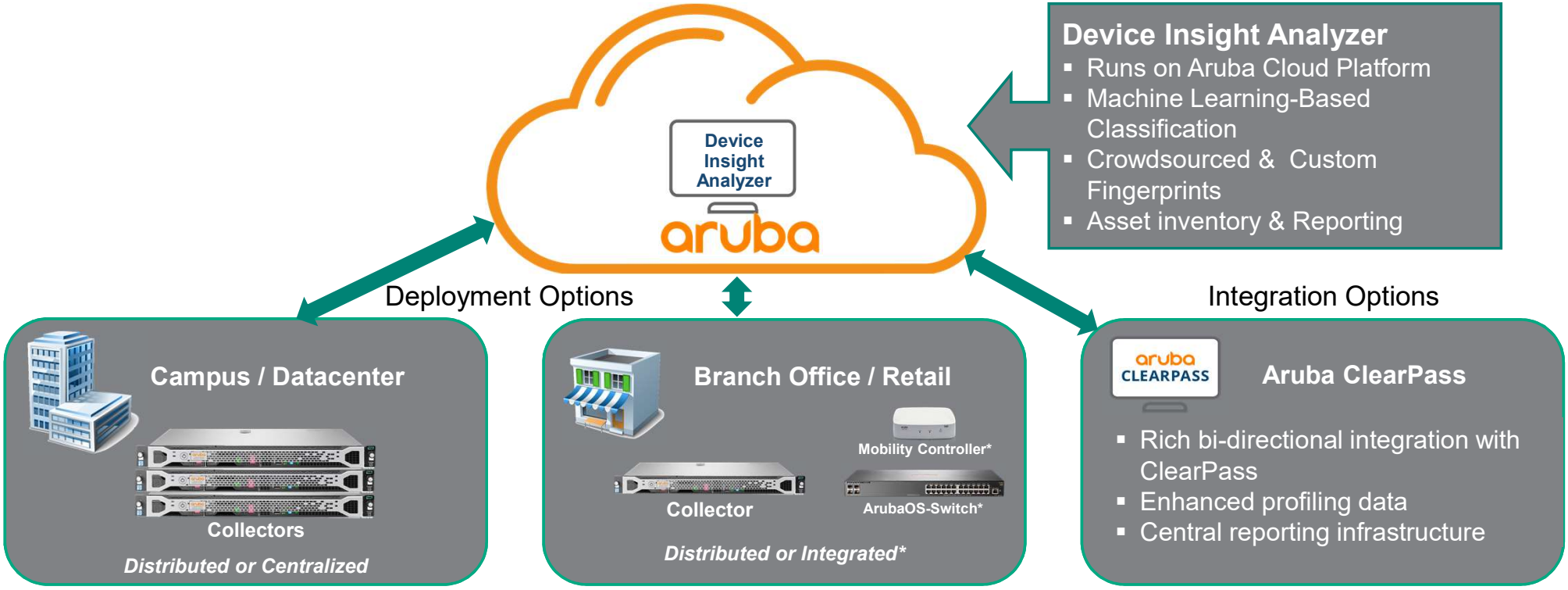
Collectors

– A collector is responsible for receiving the raw data (e.g. DHCP), extracting the important data and then sending it off to the profiler.

Profiler / Analyzer

– The analyzer takes the data from the collectors and applies profiling rules to determine that a device is an iPhone, camera, sensor, etc. The precision of the classification can be improved by leveraging **ML-techniques**, **crowd-sourcing** our **manual user input**.

Deployment Overview



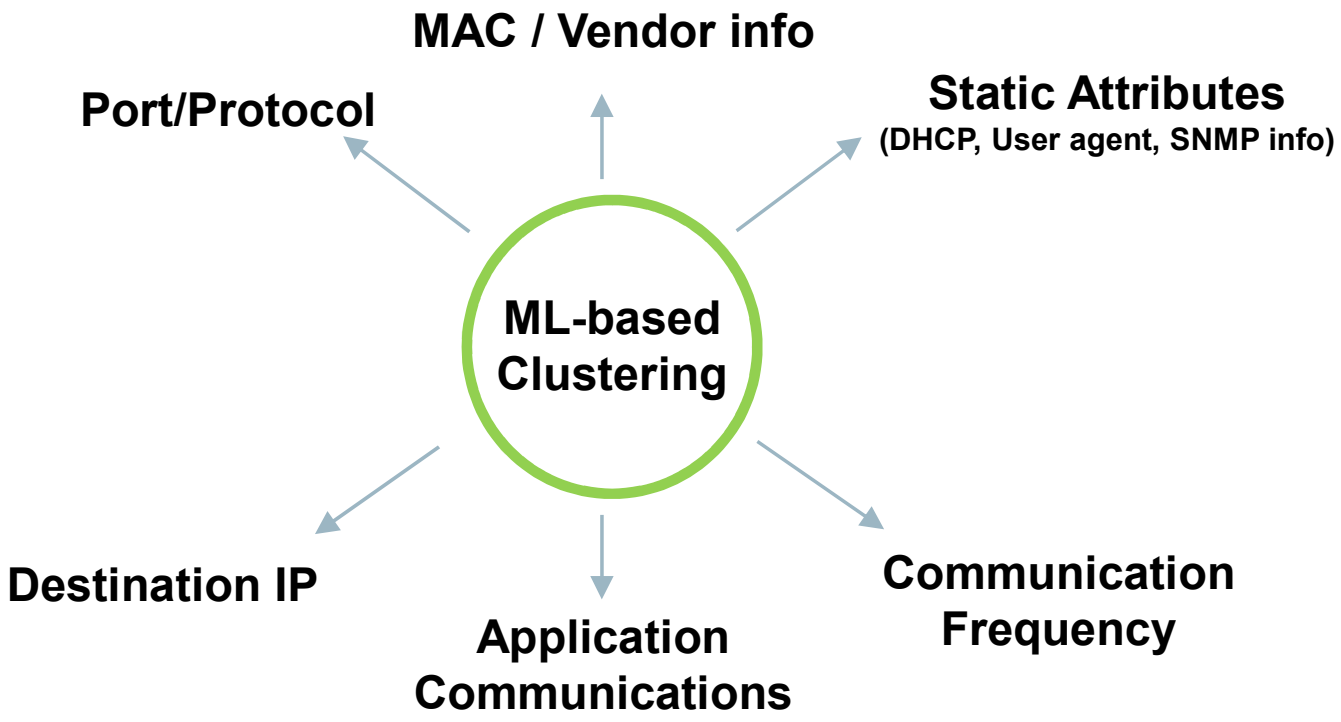
Collectors

- Hardware or Virtual Appliance
- Complete DPI support
- Passive Collection & Active Scanning
- Sends metadata to Device Insight Analyzer
- Integrated in Aruba WLAN/LAN*

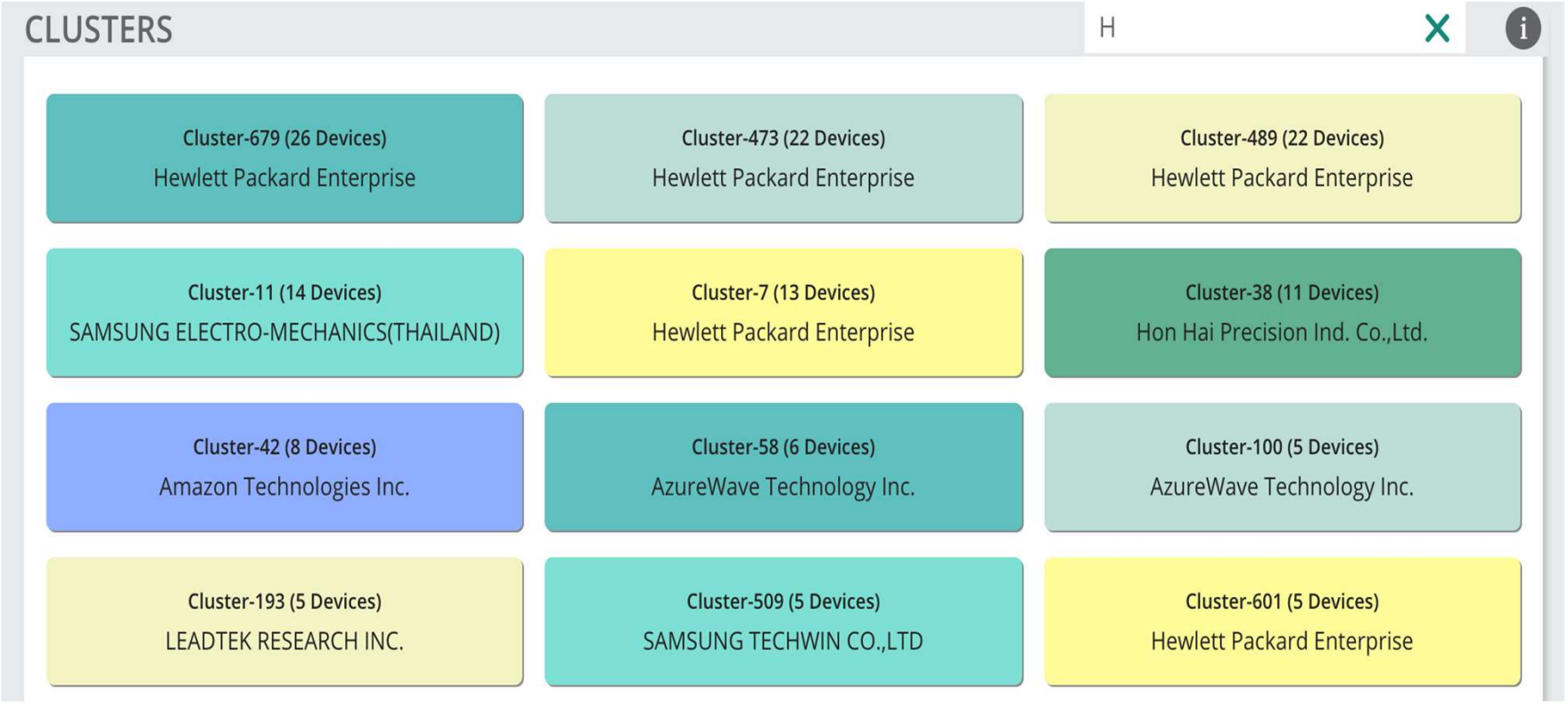
* Roadmap consideration

aruba
a Hewlett Packard Enterprise company

Machine Learning-based Clustering



Machine Learning-based Categorization



Evolving Device Fingerprint Support Using Crowdsourcing

Customer labels a device using clusters or rules

aruba
a Hewlett Packard Enterprise company

Aruba receives the signature

Signature is tested and validated

aruba
a Hewlett Packard Enterprise company

Signature is made available for use by all customers

aruba
a Hewlett Packard Enterprise company

OLIVER WEHRLI

TECHNOLOGY CONSULTANT | SWITZERLAND
T: +41 58 199 00 55

UEBERLANDSTRASSE 1 | CH-8600
DUEBENDORF | SWITZERLAND

AIRHEADS COMMUNITY | **FOLLOW US** | **Twitter** | **LinkedIn**

Thank You