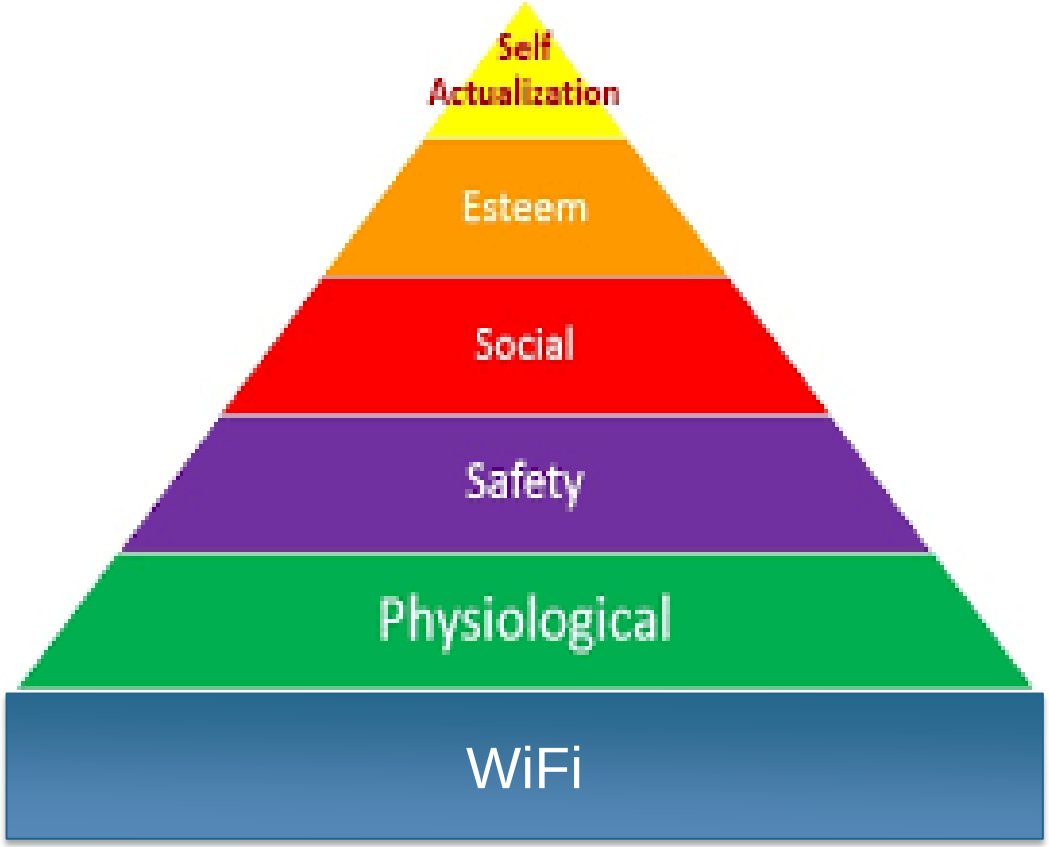
WiFi Security

WiFi India Summit-6th Feb-2019

Rajesh.Gandhi@arista.com

ARISTA

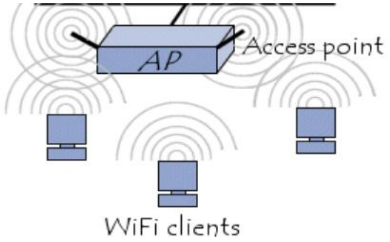


You Deserve Clean Wi-Fi

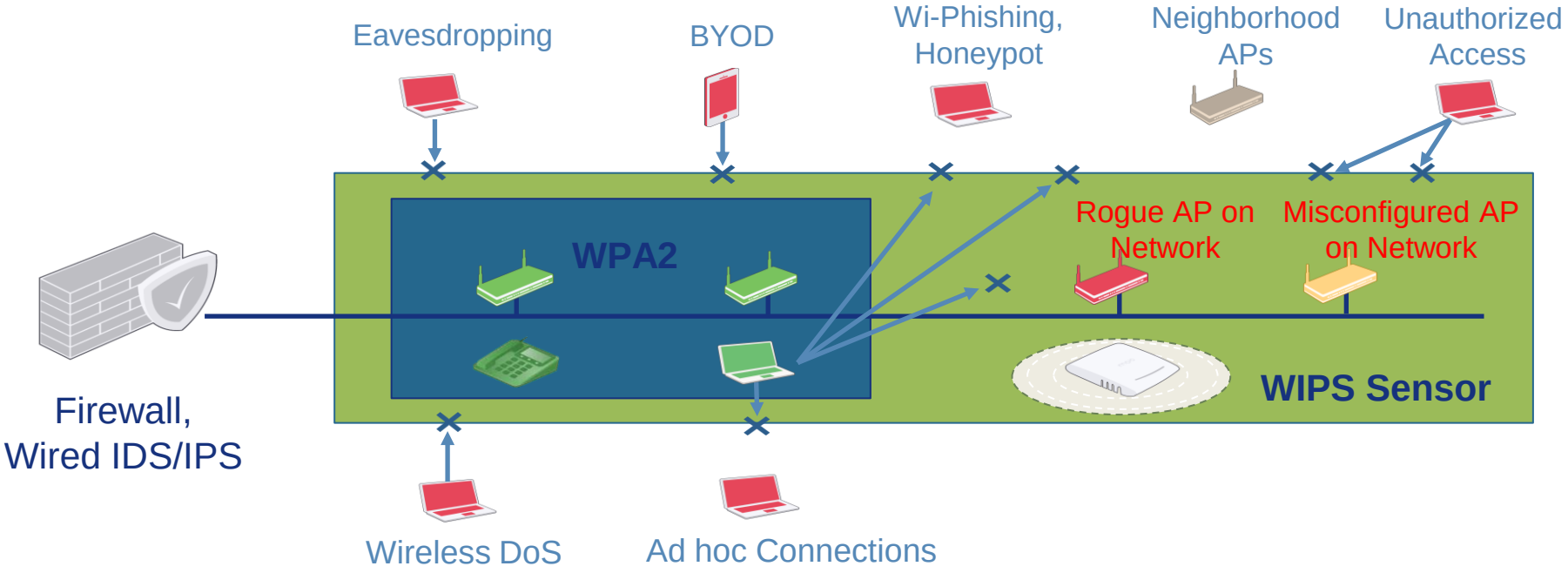
Most WiFi Networks are NOT secure

WiFi Security Problem

- Ever increasing wireless traffic in your airspace due to WiFi commoditization.
  - Threats hidden in large volume of traffic.
- WiFi signal is not contained within or without physical barriers.
- Off the shelf hacking tools have lowered the bar on attacker sophistication.
- WiFi networks continue to be exposed to new vulnerabilities. The last major was **Oct 16, 2017** called the KRACK (Key Reinstallation AttaCK).



WiFi Security with WPA2 and WIPS



WPA2 (802.11i)

Inline authentication and encryption applies to wireless devices that are managed by enterprise IT and properly configured.

WIPS (Wireless Intrusion Prevention System)

Overlay monitoring required to address threats from wireless devices that are not managed by enterprise IT and/or are misconfigured.

ARISTA

WIPS Security Protection

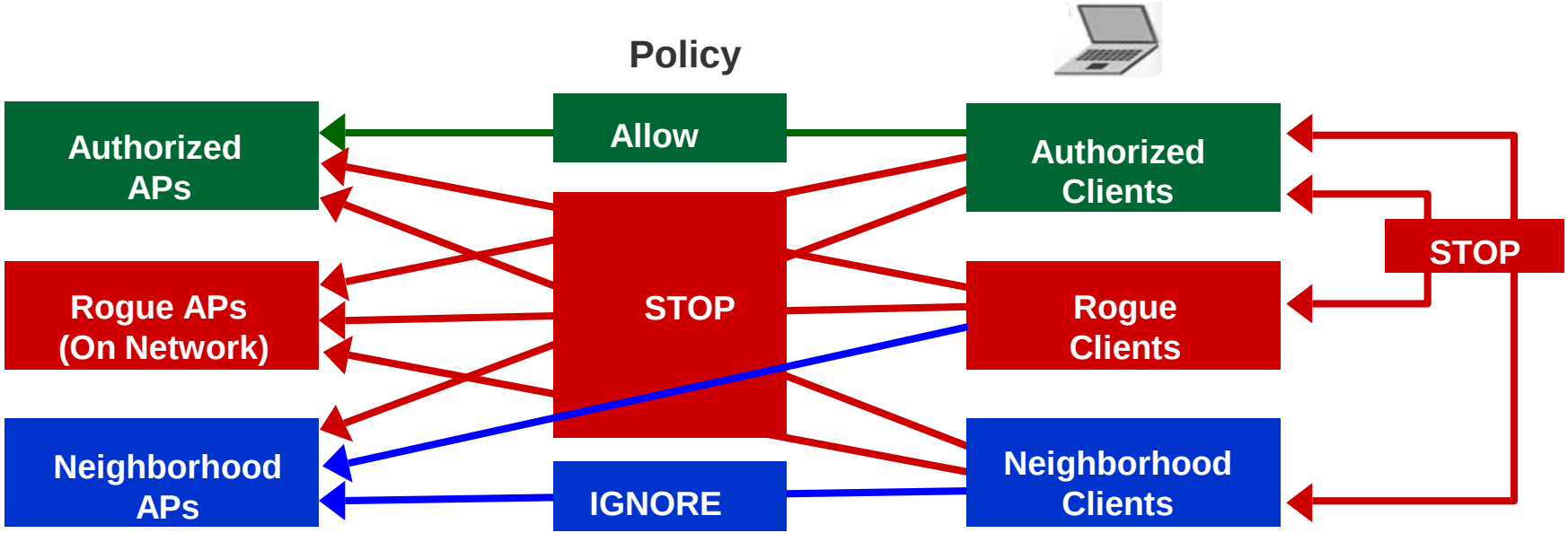
- WIPS addresses threat vectors orthogonal to WPA2
- Offers protection for both
  - Wired network (e.g. rogue APs, mis-configured APs), and
  - Wireless clients and connections (e.g. mis-associations, Evil Twin, honeypots, ad hoc connections, DoS attacks)
- Requires scanning all channels, not just the channels where your WiFi network operates
  - Including non-standard and non-regulatory domain channels

Old IDS Ways to Solve WIDS/WIPS Problem

Techniques	Downside
1. Admin-defined rules for classifying wireless devices	• Can't keep up with dynamic wireless environment. • Manual reviews required when rules generate alerts. Rules don't generate solid inferences. • Unsuitable for automatic prevention because rules generate false alarms.
2. Wireless signature matching to detect attacks	• All tools don't have signatures. • Can't handle zero day attacks. • Signatures generate false alarms.
3. Packet statistics anomaly detection	• What anomaly thresholds are right for your network to detect threat, but not cause false alarms?

Doesn't Work

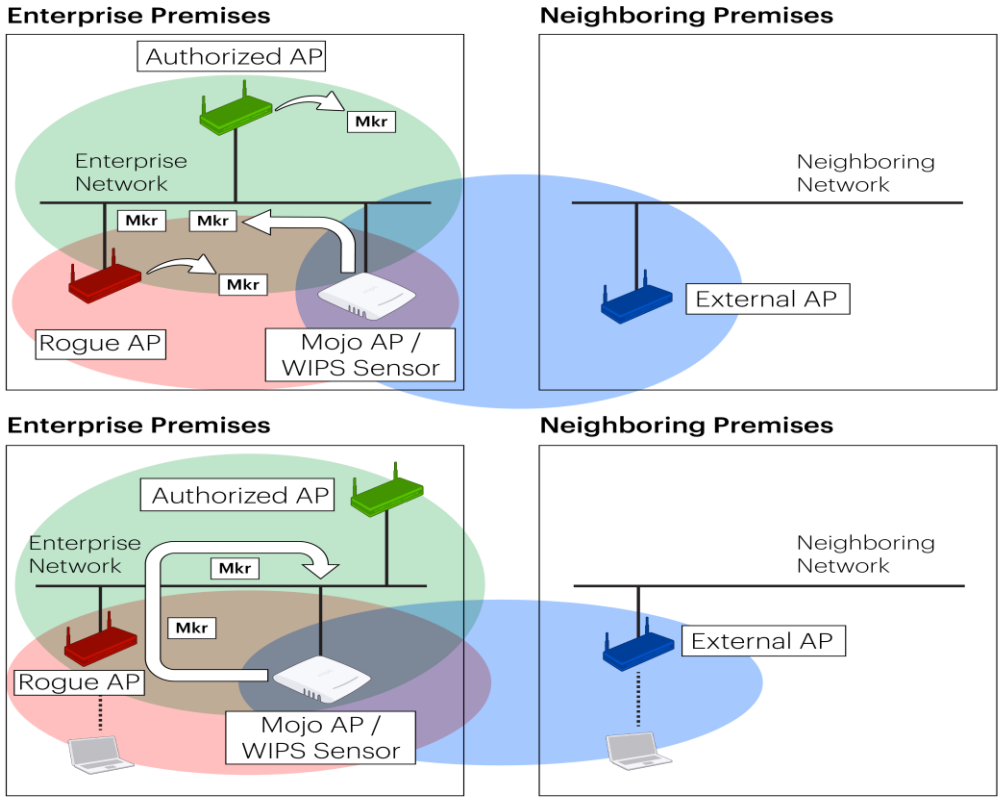
Mojo's Differentiated Approach – Expert System (Knowledge-based AI)



Policy based model, Autoclassification, Automatic Prevention

ARISTA

Automatic Rogue AP/Neighbor AP Classification



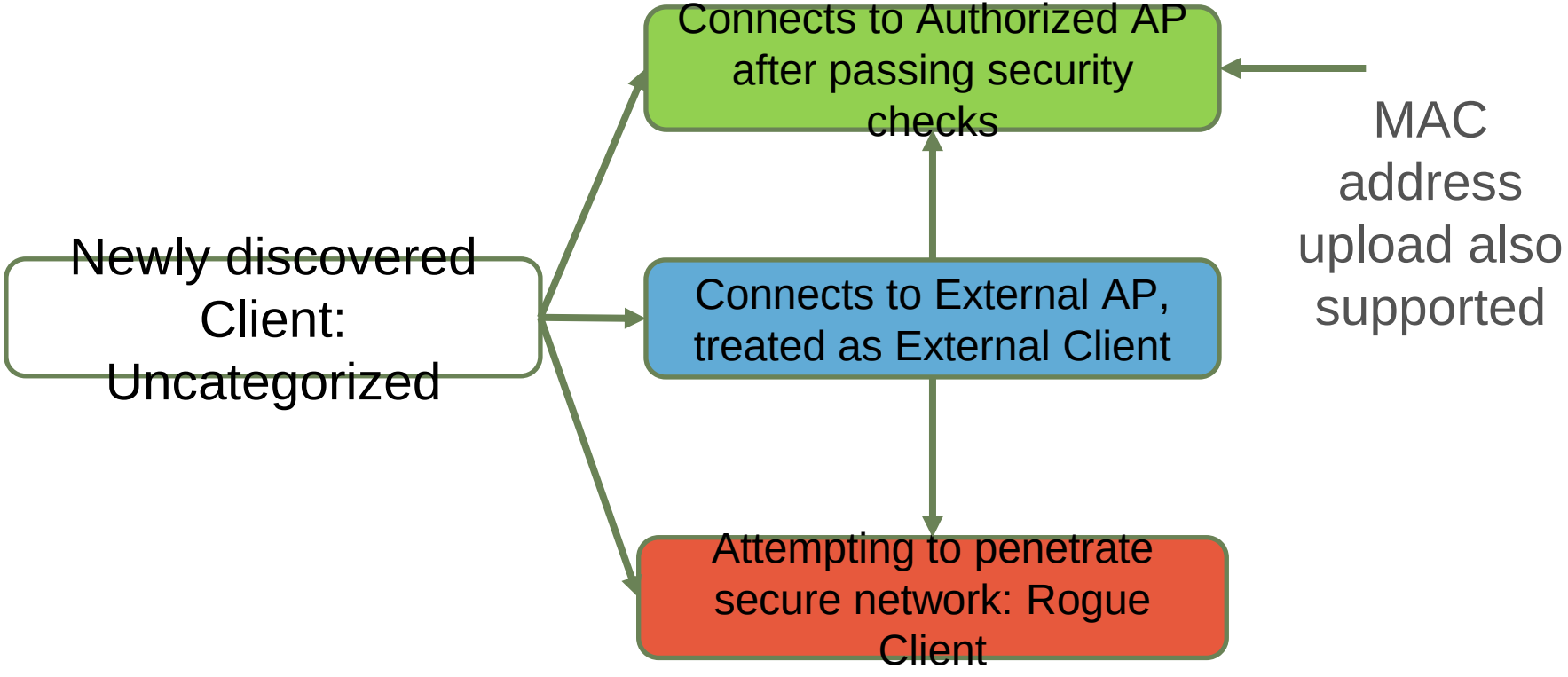
Patented Marker Packet™ techniques for on-wire/off-wire detection.

ARISTA

Mojo Auto-Classification Benefits

- No false negatives: No “suspects” in neighbor category
  - Market Packet™ techniques address cases that are beyond scope of passive correlation
- No false positives: No “liability” in automatically containing real rogues
  - Marker Packet™ techniques provide proof statement on wired connectivity
- Scalability through localized and standalone operation at network edge
  - No need of interaction with switch infrastructure, such as CAM table pulling
  - No user configured rules needed to classify rogue versus neighbor APs

Automatic Client Classification



Multiple Techniques to Block Red Paths

- One size doesn’t fit all
  - There are many permutations & combinations on connection type and Wi-Fi interface hw/sw
- Bag of tricks for comprehensive threat coverage
  - Deauth, timed deauth, client chasing, ARP manipulation, cell splitting, wireless side, wired side

Renowned Best WiFi Security!

- 37 granted US and international patents.
- Only WIPS to receive Gartner's highest rating: "Strong Positive"!

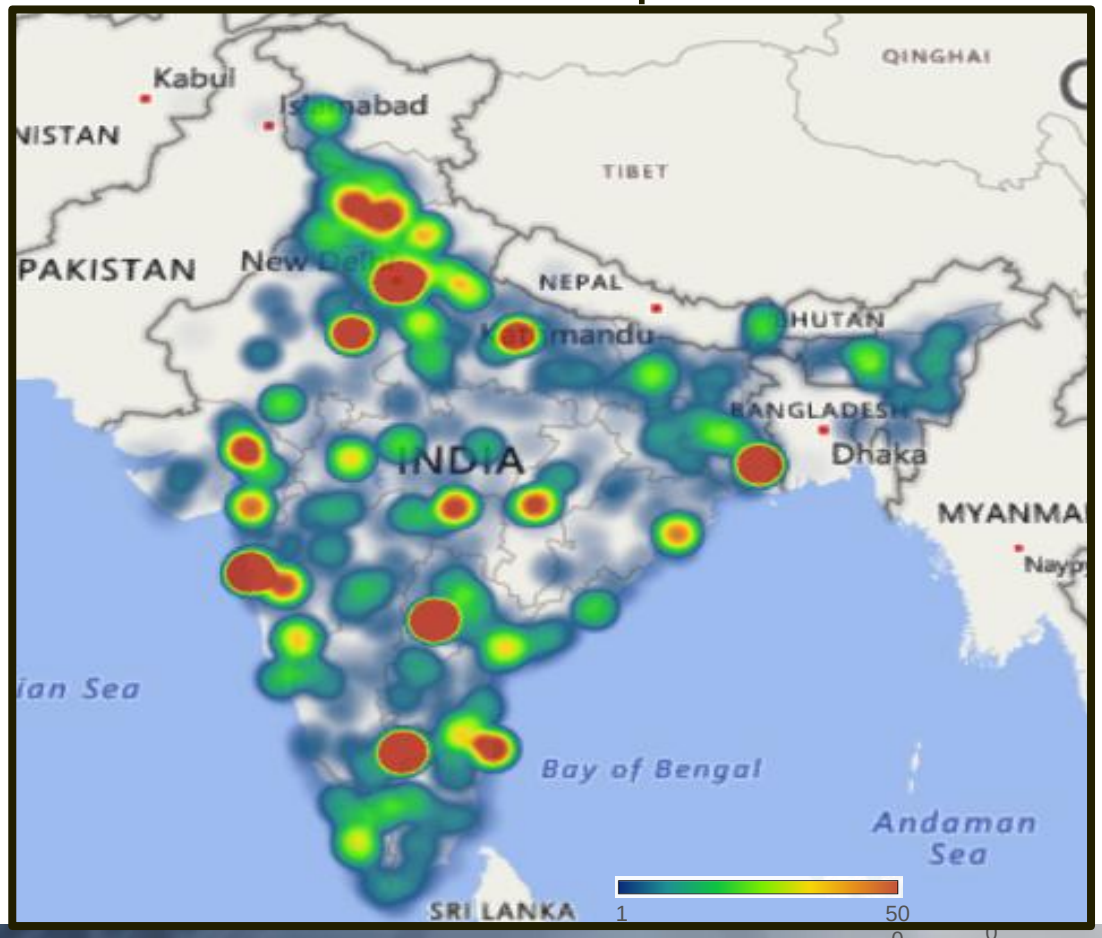
	RATING				
	Strong Negative	Caution	Promising	Positive	Strong Positive
AirTight Networks					x
Aruba Networks				x	
Cisco				x	
Fluke Networks				x	
Meraki			x		
Motorola				x	

- Fed and DoD approved: FIPS 140-2, Common Criteria, DISA UC AF

Large Enterprise	Retail & Hospitality	Education	Service Providers & OEM	Federal
ZURICH	BlueBay Hotels	UAX Universidad Alfonso X El Sabio	COMCAST BUSINESS	
Robert Half	kate spade NEW YORK	esc6 Dedicated to Serve	Jio	
TEXTRON	amc	WALSH UNIVERSITY A Catholic University of Distinction	epb Fiber Optics	
CITRIX	TGI FRIDAYS	KNOB NOSTER Public Schools	NEC	
Time Warner Cable	COSTCO WHOLESALE	OHIO HI-POINT Career Center	WatchGuard	
Outcome HEALTH	GNC LIVE WELL	SANTA ROSA COUNTY DISTRICT SCHOOLS		
	NOODLES & COMPANY World Kitchen			

ARISTA

Tier 1 Operator in India



APs

>175K

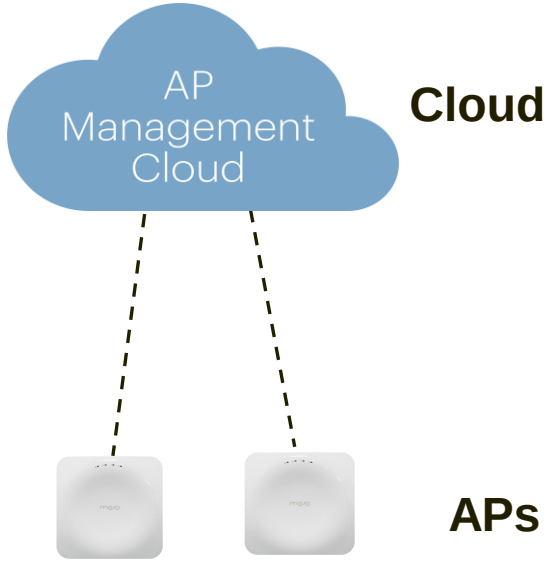
ARISTA

Lowest TCO and Most Security

Tri-Radio

11ac Wave-2

- Dedicated third radio on AP for WIPS
- Cloud based management
- WIPS included in base AP license
- Comprehensive threat protection
- Low operational overhead: Minimal config, high automation, false-alarm free



ARISTA

Arista Tri-Radio AP Advantage: All in one

Access

WIPS

Client

ARISTA

Mojo WIPS versus Competition

WIPS Comparison	Mojo	Aerohive	Meraki	Controller Based
Rogue AP Protection	Multiple Marker Packet™ + passive correlation techniques	Only 1 passive correlation technique	Only 1 passive correlation technique	Partial
Client Protection	Covers all cases of client misbehavior	Partial	No	No (Cisco) or partial (Others)
Auto Containment	Recommended and effective	Not Recommended and ineffective	Not Recommended and ineffective	Not Recommended and ineffective
False Positives and Negatives	Virtually zero, and in case of doubt, notifies about it	High, blind	High, blind	High, blind
Operational Effort	Low	High	HIgh	High
Dedicated Scanning Radio	3rd Radio on AP	Not supported	3rd radio on AP	Requires additional
Cost	No additional cost	No additional cost	No additional cost	Extra cost

Then WiFi Edge – Based on Cloud Architecture

MWM Service

Cloud or Local

Arista 7300X3 Spline

Cloud Integration Point

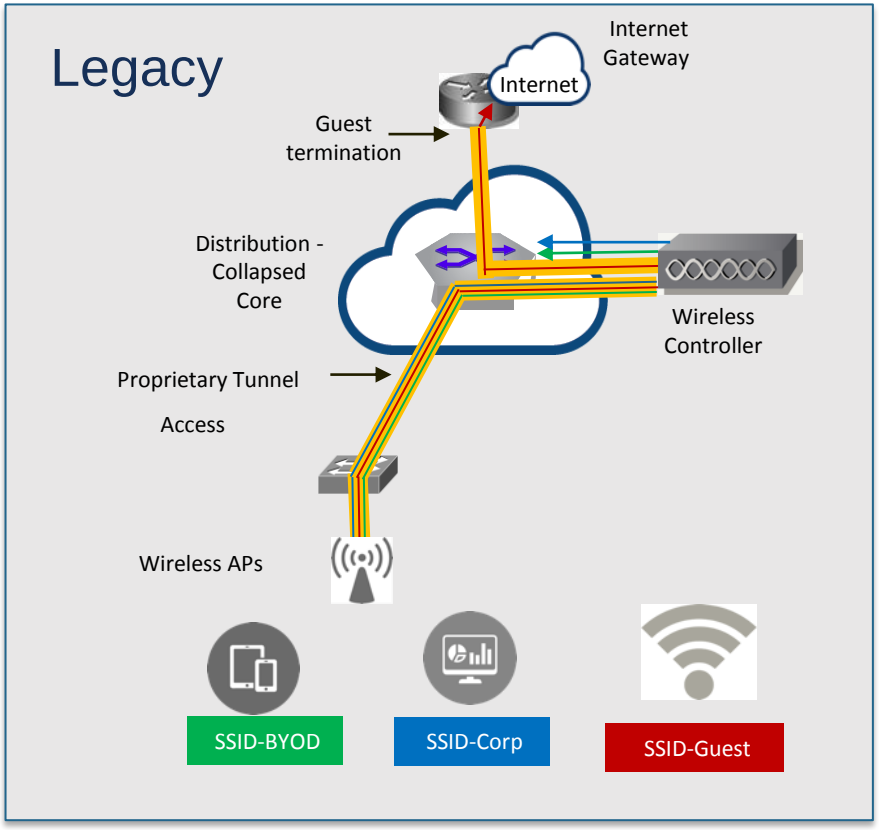
Local Network
- NMS
- SIEM
- Syslog

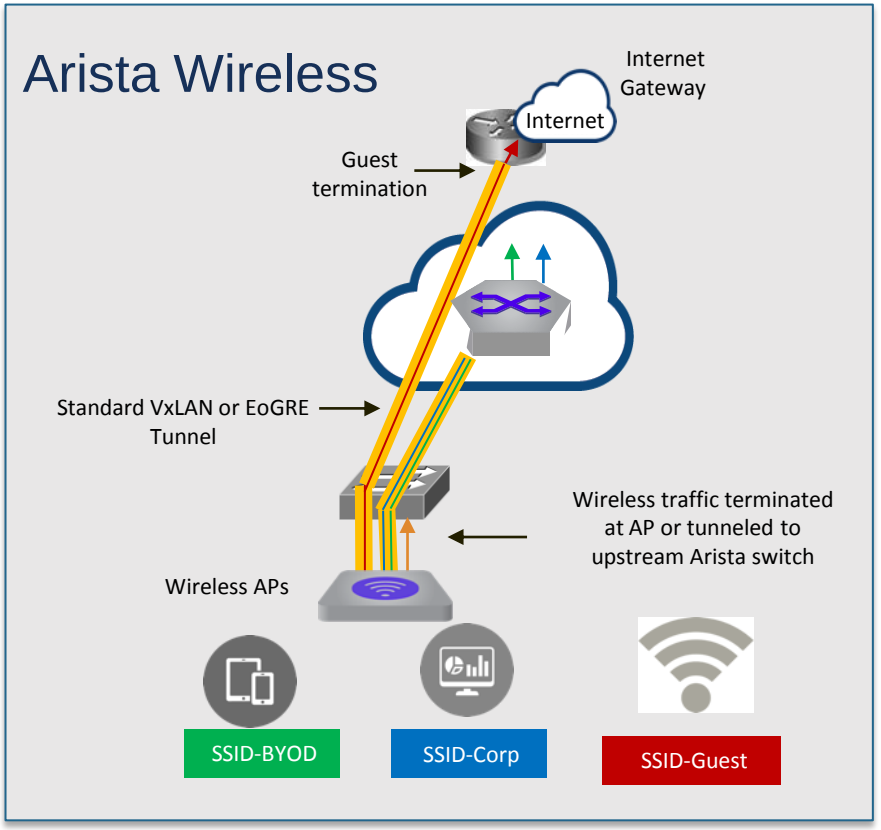
Data Plane – Local, flexible

Control Plane – Local & distributed

ARISTA

SIngle Control Plane – No Separate WLC/Controller





ARISTA

ARISTA