WatchGuard Wi-Fi Security and Performance Validation

7 September 2018
DR180720H

Miercom.com

www.miercom.com

Contents

1.0 Executive Summary

Businesses of all types and across all industries are facing increased pressure from customers, vendors, and even employees to offer secure and fast wireless access. Although offering Wi-Fi is vital, it remains vulnerable to wireless threats. Networks may unknowingly allow client connections to a malicious access point (AP), putting all endpoints at risk. Wireless Intrusion Prevention System (WIPS) technology helps APs intelligently challenge Wi-Fi attackers while maintaining performance.

WatchGuard Technologies engaged Miercom to competitively assess its APs against similar devices from Aruba, Cisco Meraki, and Ruckus to understand how its WIPS automation compares. WIPS is designed to address Wi-Fi security threats such as rogue APs, rogue clients, neighbor APs, ad-hoc networks, APs with spoofed SSIDs and misconfigured APs.

In our testing, we found WatchGuard's Wi-Fi security solution (AP420 managed by the Wi-Fi Cloud) is the only one on the market to offer exceptional security against all Wi-Fi threat categories, supporting automatic detection and prevention where other vendors did not. The following key findings highlight our observations.

Key Findings:

- **Only vendor to automatically detect and prevent six known Wi-Fi threat types simultaneously; unlike competing vendors, WatchGuard also maintained performance**
- **Only vendor supporting automatic detection and prevention of rogue APs and clients**
- **Only vendor to automatically detect and prevent endpoints from communications over Ad-Hoc Wi-Fi connection**
- **The only vendor to automatically prevent connections to "Evil Twin" APs and dangerous connections to misconfigured APs such as private SSIDs without encryption**

Miercom has independently observed the performance of the WatchGuard Technologies AP420 Cloud-Managed Wi-Fi solution and awards the ***Miercom Certified Secure*** accreditation in recognition of its superior performance in the competitive security assessment against similar competitive products.

Robert Smithers

CEO

Miercom

2.0 Test Summary

Table 1: Test Results per Vendor

	WatchGuard AP420		Aruba IAP335		Cisco Meraki MR53		Ruckus R710	
Test	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**	**Detect**	**Prevent**
Rogue AP	P	P	F	*N/A*	F	MP	F	*N/A*
Rogue Client	P	P	F	*N/A*	F	MP	*N/A*	MP
Neighbor AP	P	P	P	P	F	*N/A*	F	*N/A*
Ad-Hoc Network	P	P	F	*N/A*	F	*N/A*	P	*N/A*
"Evil Twin" AP	P	P	P	F	P	MP	P	F
Misconfigured AP	P	P	P	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*
Concurrent Threats	P	P	F	F	F	F	F	F

P – Pass

MP – Marginal Pass; require manual prevention

F – Failure to detect or protect from the referenced test

N/A – Feature not supported

3.0 Product Tested

WatchGuard Technologies AP420 Indoor Access Point

- Tri-radio 4x4:4 MU-MIMO, 802.11ac Wave 2 support to serve high-density environments
- 10 integrated antennas, 2-GbE ports with PoE+
- 2x2 MIMO dual band radio for dedicated Wireless Intrusion Prevention System (WIPS) and RF optimization with WatchGuard Wi-Fi Cloud enabled for continuous performance scanning
- Scans for wireless threats and enforces security policy even if WatchGuard Wi-Fi Cloud connection is interrupted
- 2.5 Gbps maximum aggregate data rate
- Dynamic RF optimization through smart steering, band steering and optimal channel selection

Aruba Networks IAP335 Access Point

- Dual radio 802.11ac with MU-MIMO
- 1.73 Mbps performance in 5-GHz band
- Antenna polarization diversity for optimized RF performance and spectrum analyzer to remotely scan 2.4 and 5-GHz radio bands for sources of RF interference
- Integrated wireless intrusion protection to protect against threats and eliminate need for separate RF sensors and security appliances

Source: Hewlett Packard Enterprise

Cisco Meraki MX53 Access Point

- Cloud-managed 4x4:4 802.11ac Wave 2 support with 160 MHz channels and MU-MIMO support
- 2.5 Gbps maximum aggregate frame rate
- Dedicated third radio for real-time WIPS and RF optimization
- Integrated security for protected client connectivity with AES encryption and WPA2-Enterprise authentication
- One-click guest isolation and PCI compliance reports
- Enterprise Mobility Manager and Mobile Device Management for automatic, context-aware security and policy integration

Source: Cisco Meraki

Ruckus Wireless R710 Access Point

- 802.11ac MU-MIMO with dual-band support
- 1.73 Gbps rates on 5-GHz band
- BeamFlex+ signal improvement and integrated smart antenna
- WPA-PSK (AES) and 802.1X support
- Cloudpath security and management, SPoT real-time Wi-Fi location engine and SCI network analytics

Source: Ruckus Wireless

4.0 How We Did It

Testing discussed in this report was intended to assess the security capabilities of the APs in a realistic environment. Testing was conducted in a Miercom approved test bed.

4.1 Product Setup

The table below lists all management platforms, access points and respective firmware at the time of testing. Each AP, or Device Under Test (DUT), was tested using the same test bed, client types, channelization, bandwidth and tools for provide comparable results.

Table 2: Management Platforms and Access Points

Management Platforms		
Vendor	**Management Platform**	
WatchGuard	WatchGuard Wi-Fi Cloud (Cloud)	
Aruba	Aruba Central (Cloud) / Aruba Instant (Local)	
Cisco Meraki	Meraki Cloud Controller (Cloud)	
Ruckus	ZD 1200 (Local)	
Access Points		
Vendor	**Product**	**Firmware**
WatchGuard (Main)	AP420	8.5.0-658
WatchGuard (Secondary)	AP120	8.5.0-658
Aruba (Main)	IAP335	8.3.0.0_64659
Aruba (Secondary)	IAP225	8.3.0.0_64659
Cisco Meraki (Main)	MR53	MR 25.11
Cisco Meraki (Secondary)	MR33	MR 25.11
Ruckus (Main)	R710	10.1.1.0
Ruckus (Secondary)	R610	10.1.1.0

Each system is configured to utilize three SSIDs. When possible, the SSIDs are separated between the two test APs.

Primary (Main) AP: AP420, IAP335, MR53, R710

The primary AP broadcasts the WIPS-Test SSID as a 20-MHz band on Channel 1, and a 40-MHz band on Channels 149-153. This SSID is used for background traffic. All testing is performed with background traffic on both the 2.4 and 5-GHz radios.

Background Traffic

The background traffic was generated as IP multicast and used the Multicast to Unicast conversion built-in feature of each AP. This continuous traffic was intended to keep radios of each AP busy to ensure the WIPS functionalities could be accurately assessed. It was not intended to be stress test. There were 18 clients, with 6 on the 2.4-GHz radio and 12 on the 5-GHz radio.

All vendors, excluding Meraki, had no difficulty providing reliable multicast video streaming to 18 clients. Meraki was only able to support three clients per radio before video would become unwatchable.

It is important to note that monitor mode was not used. Each tested AP was expected to provide both Wi-Fi performance and reliable WIPS simultaneously.

Table 3: Multicast Video Streaming

Product	2.4-GHz	5-GHz
WatchGuard AP420	Pass	Pass
Aruba IAP335	Pass	Pass
Cisco Meraki MR53	Fail	Fail
Ruckus R710	Pass	Pass

Cisco supported only three clients per radio. Beyond that, we observed regular pixilation and/or freezing.

Secondary AP: AP120, IAP225, MR53, R610

The secondary AP contains the Evil-Twin on Channel 36, along with the WIPS-Test (No Encryption) or WIPS-Test-Open (No Encryption) SSIDs on Channel 36. These two SSIDs are used for the "Evil Twin" test and Misconfigured AP test. (Note: This configuration is used for all APs except for Aruba, which required an altered configuration due to the broadcast of all SSIDs from both its APs. This behavior is caused by the parent-child relationship between the IAP335 and IAP225. This relationship requires the IAP225 be disabled for the Neighbor AP and Ad-Hoc Network tests to ensure the primary AP performs the WIPS functionality when identifying and blocking the authorized client from associating with the "Neighbor" SSID).

Unless otherwise stated above, all tests are performed with two APs. The WIPS-Test-Open and "Evil Twin" SSIDs were only configured and broadcast on the secondary AP (excluding Aruba). The Neighbor AP broadcasts on Channel 149, the Ad-Hoc Network broadcasts on Channel 6, and the "Evil Twin" broadcasts on Channel 11.

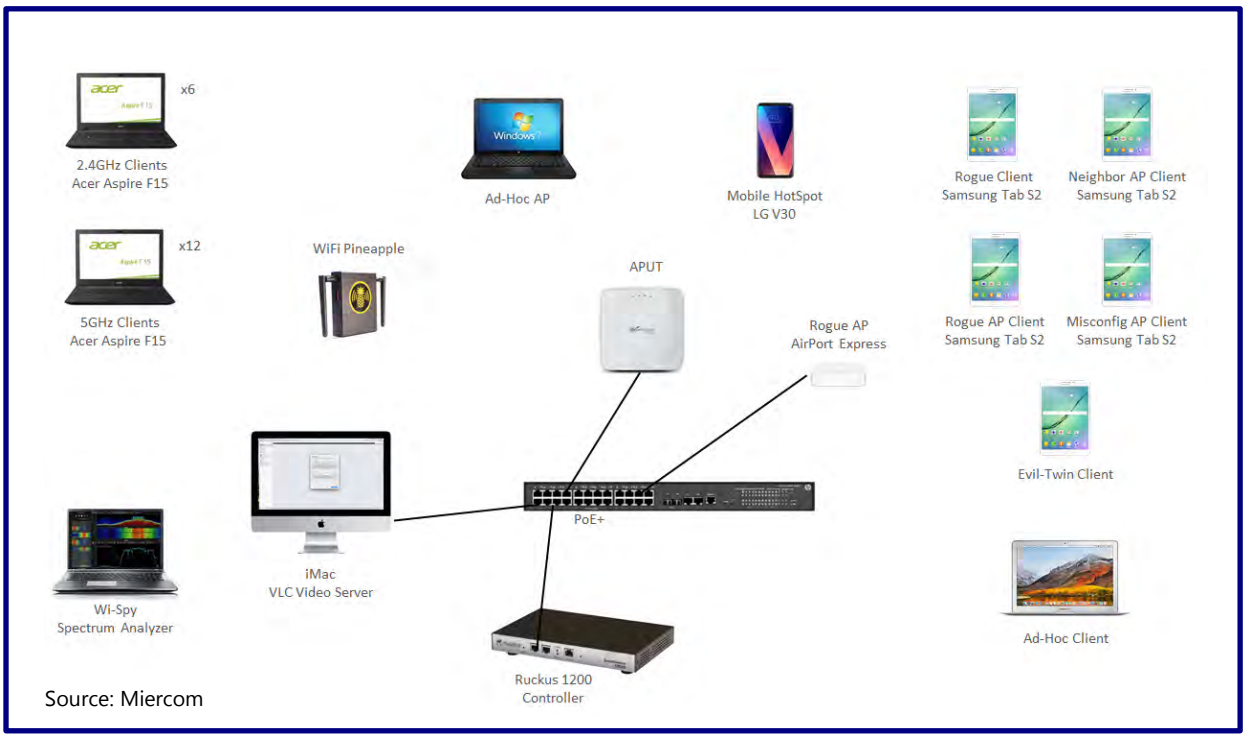
Results are based on a single AP protection scenario, in this case the primary (main) AP is under analysis for security functionality while providing video streaming service to clients on both the 2.4 and 5-GHz radios. The Aruba and Ruckus systems have the potential to perform WIPS functionalities more effectively when a separate AP is in monitor mode. This configuration was not used as it would have doubled the number of APs (1 AP for Wi-Fi clients, 1 AP for WIPS), driving up the overall cost of network deployment.

Table 4: Vendor Product Settings

Product	Settings
WatchGuard AP420	• Configured settings using tab inside the WIPS section of the user interface • Authorized WLAN policy, AP Auto-classification, Client Auto-classification, Intrusion Prevention and Intrusion Prevention Activation options have been configured to enforce a strict WIPS policy • Multicast to unicast conversion enabled
Aruba IAP335	• In the following tests, the secondary AP is not used: – Neighbor AP – Ad-Hoc Network • In the configuration utilized, both APs utilize the same settings due to a parent-child relationship between the main and secondary APs • To ensure the WIPS functionalities are performed by the AP under test, the secondary AP is disabled for the selected tests • The WIPS settings are all configured to "High" • Set to utilize background scanning option at the default interval, using 2.4 and 5-GHz radios to scan for other networks and possible security threats • Wired and wireless containments are activated • Wireless containment uses the "Deauth Only" and "Tarpit all stations" options • For the wireless containment option, the user interface alerts the user to the potential of violating FCC rules and asserts that Aruba shall not be liable for any repercussions due to the wireless containment functionality *"Note: The Federal Communications Commission ("FCC") and some third parties have alleged that, under certain circumstances, use of containment functionality violates 47 U.S.C. §333 and/or other FCC rules, regulations or policies.* *Before using any containment functionality, you should determine whether your intended use is allowed under the applicable rules, regulations and policies.* *Aruba shall not be liable for any claims, sanctions, or other direct, indirect, special, consequential or incidental damages related to your use of containment functionality." [Source]* • DMO (multicast to unicast conversion) was enabled

Cisco Meraki MR53	• Contains built-in third radio for background scanning and WIPS functionality • Configuration settings can be found under the configure tab in the Air Marshal Settings – The "Block clients from connecting to rogue SSIDs by default" option has been selected for all instances in which protection is enabled • In addition to automatic prevention, the manual SSID blacklist is utilized to demonstrate the possibility of administrative intervention in some of the test scenarios • Default multicast to unicast conversion was enabled
Ruckus R710	• Set to utilize background scanning option at 10 second intervals (default is 20 seconds) to use 2.4 and 5-GHz radios to scan other networks and possible security threats • Settings used can be found under the "Wireless Intrusion Detection and Prevention System" • Intrusion Detection and Prevention section of the settings are set to enable report for all rogue devices and protect network from malicious rogue APs

4.2 Test Bed Environment



Source: Miercom

4.3 Test Tools

Hak5 Pineapple

- Create and direct live attacks in a Wi-Fi environment, while passively monitoring devices
- Target and audit devices (clients, access points) for damage control.
- Intercept communications using their comprehensive suite of Man-in-the-Middle tools
- Report data at set intervals for vulnerability analysis
- Gain knowledge on Wi-Fi interaction and threat mitigation using intuitive user interface and Linux-embedded software

WireShark

- Create and analyze packet captures
- Calculates application and network response times, data and network volume for over 1,200 applications

inSSIDer

- Scan wireless environments for neighboring and interfering networks
- Identify configuration issues for optimal Wi-Fi coverage – locate best channel, disable legacy rates, identify security issues for maximal speed and efficiency

Wi-Spy

- Spectrum analyzer (included in inSSIDer)
- Allows visibility of interference from both Wi-Fi and non-Wi-Fi sources

NetSpot

- Perform wireless site survey for visual management, troubleshooting, auditing and planning of wireless network deployment
- Locate rogue access points
- Detect unauthorized workstations, cross-channel interference and false-positive connections
- Check security settings (Open, WEP, WPA/WPA2 Personal/Enterprise), non-broadcasting SSIDs and Wi-Fi signal strength

VLC Media Player (Multicast Traffic Generation)

- Out stream of RTP/MPEG Transport with Video H.264+MP3 (MP4) codec with MPEG-TS encapsulation to test network and routing

5.0 Test Results

5.1 Rogue Access Point

Rogue APs are not controlled by the administrator and are on the same network as authorized APs. These APs can allow unmanaged clients to access the network.

Table 5: "Rogue" Terminology per Product

Product	External/Other AP/ Different Network	Rogue/Malicious AP/ Same Network
WatchGuard AP420	"External"	"Rogue"
Aruba IAP335	"Interferer"	"Rogue"
Cisco Meraki MR53	"Other SSIDs"	"Rogue SSIDs"
Ruckus R710	"Rogue"	"Malicious Rogue"

The term "Rogue" varies from vendor to vendor and is clarified in the table above. For instance, Ruckus defines "rogue" as any external AP. Our test methodology assumes any rogue is malicious, but Ruckus requires identification criteria be met before implementing security, making successful detection only if it marks the Apple-Rogue SSID as malicious.

Many Wi-Fi security solutions utilize MAC address correlation to identify devices on the same network. The Apple AirPort AP used as the rogue AP in this test has a differential of more than 5 bits between the wired and wireless interfaces. This variance could potentially cause correlation algorithm to fail, making the AP undetectable on the wire and therefore undetectable as a rogue AP. Products unable to detect that the AP is connected to the same network as the DUT will result in a "Fail" outcome and imply susceptibility to attackers utilizing products similar to the Apple AirPort or who have altered their MAC address with a customized tool. WatchGuard has overcome this issue with its patented "Marker Packets" technology which identifies same network devices with a more reliable detection method.

Test Method:

1. Configure Apple AirPort Open/NAT mode
2. Connect Apple AirPort to same network as DUT
3. Enable auto prevention
4. Start timer when Apple AirPort SSIDs are detected by NetSpot or inSSIDer
5. Connect clients to Apple AirPort (1 Client to 2.4-GHz and 1 Client to 5-GHz)
6. From clients connected to Rogue AP, ping wired host continuously
7. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 6: Rogue AP Detection and Prevention Results

Product	2.4-GHz Detection	5-GHz Detection	2.4-GHz Prevention	5-GHz Prevention
WatchGuard AP420	1s	1s	1s	3s
Aruba IAP335	Fail*	Fail*	N/A	N/A
Cisco Meraki MR53	Fail*	Fail*	20s (manual)	20s (manual)
Ruckus R710	Fail	Fail	N/A	N/A

**The asterisk assigned to the Aruba and Meraki Failures denote the potential to successfully detect a rogue with other access points when MAC association is successful. Third-party detection is required for manual prevention in cases where auto-detection fails.*

Each Wi-Fi security solution was tested for its ability to identify the Apple AirPort as a "Rogue" or "Malicious Rogue" AP. This type of rogue AP helps highlight the flaw in utilizing MAC association as a detection method. The WatchGuard AP was the only solution able to detect and prevent on both radios. Detection was about one second, and prevention was one second for the 2.4-GHz radio and three seconds for the 5-GHz radio. The Cisco Meraki AP did not detect the Apple AirPort as a rogue AP – only as another SSID. But manual prevention works for both radios in around 20 seconds. The Aruba AP misidentified the connected rogue AP as an "Interferer" AP. In Aruba's case, this type of AP is considered an external, disconnected AP. Its MAC address correlation algorithm was bypassed, unable to determine that the rogue AP was, in fact, connected to the network. As a result, the Aruba AP does not offer prevention – manual or automatic. The Ruckus AP had the ability to detect the rogue AP, but it identified it simply as "rogue" but not "malicious". For Ruckus, a Rogue AP must be identified in its interface as "Malicious Rogue" to prevent clients from connecting to the possibly harmful AP. In the event detection of the rogue AP fails, the prevention functionality will not be enabled, and therefore is not assessed. This case is indicated by "N/A".

5.2 Rogue Client

Any client previously connected to a rogue access point is considered a rogue client. This client poses a possible risk because of its connection to an uncontrollable device that may have compromised the client.

The rogue client attempted to connect to the DUT and ping the wired host continuously. The time to detect and prevent the rogue client was recorded, with a 10-minute maximum period allowed.

Test Method:

1. Start with an Uncategorized Client
2. Bring up a Rogue AP (e.g. Apple-Rogue and/or AP discoverable by MAC adjacency for DUT that is unable to detect the Apple AirPort as "Rogue")
3. Connect Uncategorized Client to Rogue AP
4. Confirm Rogue AP is seen by DUT as "rogue"
5. Verify Uncategorized Client is now recognized as Rogue Client
6. Disconnect Rogue Client from Rogue AP
7. Enable auto prevention in DUT
8. Connect client to Authorized AP and ping wired host continuously
9. Start timer as soon as Rogue Client connects to Authorized AP
10. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 7: Rogue Client Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	1s	1s
Aruba IAP335	Fail	N/A
Cisco Meraki MR53	Fail	90s (manual)
Ruckus R710	N/A	3s (manual)

The WatchGuard product used auto client classification, a technique based on client behavior, to detect the rogue client. Both the Aruba and Cisco Meraki did not detect the rogue client, even when it correctly identified the rogue access point it was connected to; the manual MAC blacklist failed, as it was not part of their WIPS. Third-party detection is required when manual prevention is used in cases where auto-detection fails. The Ruckus product was not able to find a rogue access point (malicious rogue) and, therefore, cannot identify any client associated with it as a rogue client. The detection for Ruckus is therefore assigned a score of "N/A". Ruckus was able to prevent a rogue client only through manual means via a client blacklist. In the event detection of the rogue client fails, the prevention functionality will not be enabled, and therefore is not assessed. This case is indicated by "N/A". While this manual client blacklisting is available, another system or third-party solution would be required to identify the client as "Rogue".

5.3 Neighbor Access Point

A Neighbor AP is an independent AP that is not under the control of network administrators. It provides access through a separate network but could be used to bypass internal security or content filtering policies. A client is identified as "authorized" upon connection to the corporate network. For WatchGuard, an authorized client is automatically controlled by network and WIPS policies. These policies allow or deny association to broadcasted SSIDs.

This test determined if WIPS could detect and prevent an authorized client from connecting to an external Neighbor AP without interfering with other clients on the neighboring AP.

Test Method:

1. Add authorized SSID
2. Verify AP as listed as Authorized AP in user interface
3. Connect client to Authorized AP
4. Verify client is listed as Authorized Client in user interface
5. Bring up Neighbor AP (e.g. Mobile HotSpot)
6. Enable auto prevention in DUT
7. Connect a neighbor client to Neighbor AP and ping local wired host continuously
8. Connect Authorized Client to Neighbor AP and ping local wired host continuously
9. Start timer as soon as Authorized Client connects to Neighbor AP
10. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 8: Neighbor Access Point Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	1s	3s
Aruba IAP335	1s	1s
Cisco Meraki MR53	Fail	N/A
Ruckus R710	Fail	N/A

The WatchGuard AP was able to detect the neighbor AP in about one second and prevent an authorized client from connecting to it within three seconds. Aruba was able to detect the AP and prevent "Valid Client Misassociation" within one second. Both the Cisco Meraki and Ruckus APs do not detect that an authorized client has connected to a neighbor AP. In this case, the WatchGuard and Aruba products distinguish themselves with background client tracking. These products remember which clients have connected to their network and monitor other networks. When a previously connected client attempts to connect to an unauthorized access point, the prevention is activated, and the client can be protected. In the event detection of an authorized client connected to a neighboring AP fails, the prevention functionality will not be enabled, and therefore is not assessed. This case is indicated by "N/A".

5.4 Ad-Hoc Network

The Ad-Hoc Network identified in this testing consists of a Windows endpoint communicating with an ad-hoc Macbook client. This allows clients to directly communicate without any additional infrastructure.

Test Method:

1. Create ad-hoc AP
2. Enabled auto-prevention
3. Associate authorized client to ad-hoc AP and ping wired host continuously
4. Start timer when the ad-hoc SSID is detected by NetSpot or inSSIDer
5. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 9: Ad-Hoc Network Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	83s	83s
Aruba IAP335	Fail	N/A
Cisco Meraki MR53	Fail	N/A
Ruckus R710	40s	N/A

The WatchGuard AP auto-prevented ad-hoc network communication by successfully identifying the ad-hoc SSID. The Aruba AP reported "Valid Client Misassociation" in 90 seconds but did not report the AP as ad-hoc. The Cisco Meraki AP did not detect the Ad-Hoc AP but reports it as "Other SSID"; manual prevention failed. The Ruckus AP detected the Ad-Hoc AP in 40 seconds but does not support auto prevention for ad-hoc networks, and manual prevention failed.

5.5 "Evil Twin"

The "Evil Twin" is any AP with a spoofed SSID. For this testing, the spoofed SSID is the imitation of an Authorized AP's SSID. The MAC address and channel assignment are different from the target. A spoofed SSID allows for clients to accidentally connect to the wrong network and potentially fall victim to a Man-in-the-Middle (MiTM) attack.

Test Method:

1. Add an SSID to Evil Twin AP
2. Ensure SSID is enabled only in 5-GHz band
3. Verify non-malicious instance of Evil Twin AP is seen as Authorized in the user interface
4. Enable auto prevention in DUT
5. Enable Wi-Fi Pineapple AP spoofer on 2.4-GHz band (SSID only)
6. Start timer as soon as Evil Twin AP is detected by NetSpot or inSSIDer
7. Associate a client to non-malicious instance of Evil Twin AP to be spoofed and ping wired host continuously
8. Associate a client to the spoofed Evil Twin AP and ping wired host continuously
9. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 10: "Evil Twin" Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	3s	3s
Aruba IAP335	60s	Fail
Cisco Meraki MR53	84s	30s (manual)
Ruckus R710	60s	Fail

The WatchGuard AP detected and prevent the Evil Twin AP in about three seconds. Two pings were successful before it was found and stopped, and reporting was observed after about 90 seconds. The client was still able to connect to the non-malicious instance of the Evil Twin SSID. Third-party detection is required when manual prevention is used in cases where auto-detection fails. The Aruba detected the Evil Twin AP as an "Interferer" and reported this AP in the user interface within 90 seconds. The Evil Twin was reported as "Violating Valid SSID Conf", but detection of the spoofed SSID was intermittent, making prevention fail. The Cisco Meraki AP was able to detect the Evil Twin SSID, but since it only supports manual prevention of spoofs via blacklisting, it was able to manually prevent Evil Twin connection within 30 seconds. The client was able to connect to the non-malicious instance of the Evil Twin SSID even with the malicious Evil Twin SSID blacklisted. The Ruckus AP could identify the Evil Twin AP in 60 seconds as a "malicious AP". Auto prevention failed, regardless if the Evil Twin AP was placed on the same channel as the Ruckus AP.

5.6 Misconfigured Access Point

A Misconfigured AP is defined as an AP broadcasting an SSID with settings which violate a specific rule set or desired policy set by the administrator. In this test, the Misconfigured AP did not use encryption on the protected SSID.

Test Method:

1. Add an SSID with Open security using the same SSID name as an Authorized SSID with WPA2/PSK security
2. Enabled auto prevention
3. Associate a client to the properly configured AP (WIPS-Test/WPA2PSK) and ping wired host continuously
4. Associate a client to the Misconfigured AP (WIPS-Test/Open) and ping wired host continuously
5. Start time as soon as client connects to Misconfigured AP
6. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 11: Misconfigured AP Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	1s	1s
Aruba IAP335	1s	N/A
Cisco Meraki MR53	N/A	N/A
Ruckus R710	N/A	N/A

The WatchGuard AP instantly identified and prevented the client from connecting to the Misconfigured AP, as the client tried to connect. The Aruba AP was able to report that a "Valid Client" was transmitting and/or receiving unencrypted frames. Both the Cisco Meraki and Ruckus Aps did not support either detection or prevention of the Misconfigured AP (e.g. "Open APs"). When the Misconfigured AP functionality is not supported, the result is indicated by "N/A".

5.7 Multiple Threat Execution

All threats from Sections 5.1-5.6 were concurrently executed. The objective of this test was to determine if WIPS could detect and prevent all threats simultaneously. The DUT is required to detect or auto prevent all six threats to be considered a pass in the respective section.

Test Method:

1. Disable auto prevention
2. Enable all six threats concurrently
3. Associate all clients and initiate pings to host continuously
4. Enable auto prevention
5. Record approximate time to detect and prevent by WIPS (10-minute maximum allowed)

Table 12: Multiple Threat Execution Detection and Prevention Results

Product	Detection	Prevention
WatchGuard AP420	6/6, 100%	6/6, 100% in 20s
Aruba IAP335	3/6, 50%	1/6, 17% in 20s
Cisco Meraki MR53	1/6, 17%	3/6, 50% in 43s (manual)
Ruckus R710	2/6, 33%	1/6, 17% in 3s (manual)

The WatchGuard AP identified and blocked 100 percent of the threats within 20 seconds of concurrent exposure. All threats were detected prior to enabling prevention. The Aruba AP detected the Neighbor AP ("Client Misassociation"), Evil Twin AP and Misconfigured AP. It reported only the Ad-Hoc AP but as a "Valid Misassociation" and not an Ad-hoc network. The Cisco Meraki AP detected only the Evil Twin AP; it required manual prevention against the Rogue AP, Rogue Client and Evil Twin AP. Third-party detection is required when manual prevention is used in cases where auto detection fails. The Ruckus AP could only detect the Ad-hoc network and Evil Twin AP, but like the Ruckus AP required manual prevention. It was only able to successfully block the Rogue Client via client blacklisting.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed. Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the Performance Verified program, the industry's most thorough and trusted assessment for product usability and performance.

Customer Use and Evaluation

We encourage customers to do their own product trials, as tests are based on the average environment and do not reflect every possible deployment scenario. We offer consulting services and engineering assistance for any customer who wishes to perform on-site evaluation.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.