Protecting New and Existing Access Point Installations from Wi-Fi Hacking

December 2019
DR191115D

Miercom.com

www.miercom.com

Contents

1.0 Executive Summary 3

2.0 Test Summary 4

3.0 How We Did It 5

3.1 Product Setup 5

3.2 Test Bed Environment 8

4.0 Test Results 10

4.1 Rogue Access Point 11

4.2 Rogue Client 13

4.3 Neighbor Access Point 15

4.4 Ad-Hoc Network 17

4.5 Evil Twin Access Point 18

4.6 Misconfigured Access Point 19

4.7 Multiple Threat Execution 20

4.8 MAC Spoofing 21

4.8.1 MAC Spoofing Client 21

4.8.2 MAC Spoofing AP 22

4.9 Overlay Access Point 23

4.10 WatchGuard AP125 Overlay vs Aruba AP303 WIPS Overlay 25

About Miercom 26

Customer Use and Evaluation 26

Use of This Report 26

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.

In this second iteration of testing, WatchGuard Technologies engaged Miercom to competitively assess its APs against similar devices from Aruba, Cisco Meraki, Ruckus and Ubiquiti 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.

We found WatchGuard's Wi-Fi security solution (either AP325 or AP125 Overlay managed by the Wi-Fi Cloud) is the only vendor 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 testing observations.

Key Findings:

- Only vendor to automatically detect and prevent the six known Wi-Fi threat types simultaneously, while providing full client throughput performance
- WatchGuard APs provide cost-effective and far superior security and speed to detect in WIPS overlay mode on Wi-Fi networks with incumbent other third-party APs
- Only vendor to fully protect from complex spoofed AP and client exploits

Miercom has independently observed the performance of the WatchGuard Technologies AP325 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 Wireless Intrusion Prevention System products.

Robert Smithers, CEO

Miercom

2.0 Test Summary

Summary of Competitive Wireless Intrusion Prevention System (WIPS) Products

	WatchGuard AP325		Aruba AP303		Meraki MR33		Ruckus R510		Ubiquiti UAP-AC-SHD	
	D	**P**	**D**	**P**	**D**	**P**	**D**	**P**	**D**	**P**
Rogue AP	PASS	PASS	FAIL	FAIL	FAIL	MP	FAIL	FAIL	N/A	N/A
Rogue Client	PASS	PASS	N/A	MP	N/A	MP	N/A	MP	N/A	MP
Neighbor AP	PASS	PASS	FAIL	MP	N/A	MP	N/A	N/A	N/A	N/A
Ad-Hoc Network	PASS	PASS	PASS	FAIL	N/A	FAIL	PASS	N/A	N/A	N/A
Evil Twin AP	PASS	PASS	PASS	FAIL	PASS	MP	PASS	FAIL	PASS	N/A
Misconfigured AP	PASS	PASS	FAIL	MP	N/A	N/A	N/A	N/A	N/A	N/A
Concurrent Threats	100%	100%	0%	29%	17%	83%	33%	33%	21%	25%
MAC Spoof Client	PASS	PASS	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
MAC Spoof AP	PASS	PASS	N/A	N/A	N/A	N/A	PASS	FAIL	N/A	N/A

Source: Miercom 2019

D = Auto Detection P = Auto Prevention MP = Manual Prevention (user intervention) N/A = Not supported

Summary of WatchGuard AP125 as WIPS Overlay on AP Products

	WatchGuard AP125 + Aruba AP303		WatchGuard AP125 + Meraki MR33		WatchGuard AP125 + Ruckus R510		WatchGuard AP125 + Ubiquiti UAP-AC-SHD	
	D	**P**	**D**	**P**	**D**	**P**	**D**	**P**
Rogue AP	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Rogue Client	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Neighbor AP	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Ad-Hoc Network	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Evil Twin AP	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Misconfigured AP	PASS	PASS	PASS	PASS	PASS	PASS	PASS	PASS
Concurrent Threats	100%	100%	100%	100%	100%	100%	100%	100%

Source: Miercom 2019

D = Auto Detection P = Auto Prevention MP = Manual Prevention (user intervention) N/A = Not supported

All products were tested using the WatchGuard AP125 as a WIPS Overlay mode. Underlying AP auto-prevention was disabled.

3.0 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.

Testing was conducted over a six-week period, with four full test iterations completed per vendor for a total of 20 test cycles summarized in this report. The average of the four test run experiences is provided in this report.

3.1 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.

Management Platforms and Access Points

Management Platforms		
Vendor	**Management Platform**	
WatchGuard	WatchGuard Wi-Fi Cloud (Cloud), *8.8.0-179*	
Aruba	Aruba Central (Cloud) / Aruba Instant (Local), *8.5.0.2_71711*	
Cisco Meraki	Meraki Cloud Controller (Cloud)	
Ruckus	ZD 1200 (Local), *9.13.3.0 build 41*	
Ubiquiti	UniFi Controller, *5.11.39*	
Access Points		
Vendor	**Product**	**Firmware**
WatchGuard (Main)	AP325	8.8.0-646
WatchGuard (Secondary)	AP125	8.8.0-644.3
Aruba (Main)	AP303	8.5.0.2_71711
Aruba (Secondary)	AP335	8.5.0.2_71711
Cisco Meraki (Main)	MR33	26.5
Cisco Meraki (Secondary)	MR20	26.5
Ruckus (Main)	R510	9.13.3.0.41
Ruckus (Secondary)	R710	9.13.3.0.41
Ubiquiti (Main)	UAP-AC-SHD	4.0.42.10433
Ubiquiti (Secondary)	UAP-AC-PRO	4.0.54.10625

Each system is configured to utilize two SSIDs; one for the DUT and another for the secondary AP. When possible, the SSIDs are separated between the two test APs.

Primary (Main) AP: AP325, AP303, MR33, R510, UAP-AC-SHD

The primary AP broadcasts the WIPS-Test SSID as a 20-MHz band on Channel 6, and a 40-MHz band on Channels 149-153. The background traffic and WIPS test used the same SSID. All testing is performed with background traffic on both the 2.4 and 5-GHz radios.

Secondary AP: AP125, AP335, MR20, R710, UAP-AC-PRO

The secondary AP was only used for Misconfigured AP test, using Channel 161 for 5-GHz only. The Evil Twin AP test is the Wi-Fi Pineapple tool on Channel 11. For Aruba, the AP303 and AP335 APs were used to run testing, and there was no parent-child relationship between these two models. But since the AP335 has a dedicated third radio, and the detection is enabled by default, the AP335 was disabled when running single threat tests.

Unless previously stated otherwise, all tests are performed with two APs. The Evil Twin SSID was broadcast by the Wi-Fi Pineapple tool on Channel 11. The secondary AP only broadcast the Misconfigured AP SSID and used Channel 161. The Neighbor AP SSID was broadcast by an iPhone hotspot; we could not configure the channel. The Ad-Hoc Network SSID was broadcast by a Windows 7 laptop; we didn’t specify the use of the fixed channel.

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. For Aruba, the AP303 was only connected to 15 clients without any background traffic running during the test because it was ineffective at any WIPS functionality with a background traffic load applied.

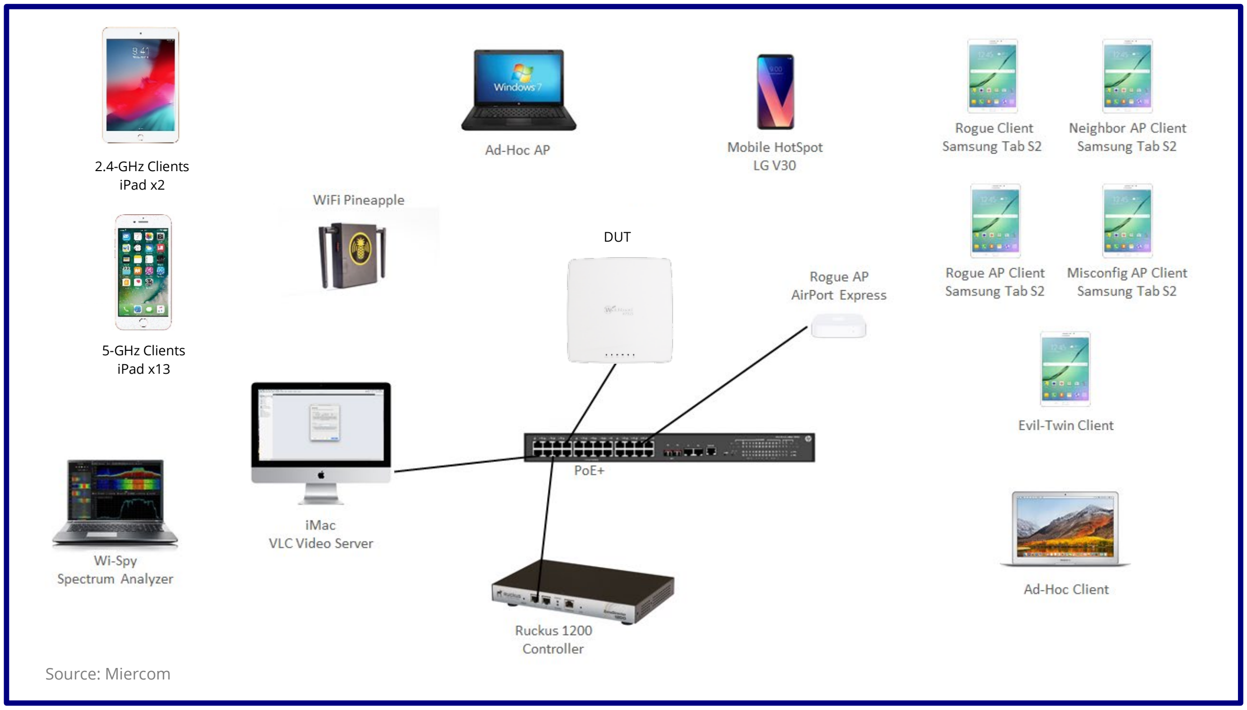
The Aruba AP303 has the potential to perform WIPS functionalities more effectively when a separate AP is in monitor mode. The Ruckus AP did not have a sensor mode, and it can support 15 clients with 150 Mbps background traffic. Therefore, the configuration of doubled APs (1 AP for Wi-Fi clients, 1 AP for WIPS) was not used as it would increase the cost of network deployment.

Vendor Product Settings

Product	Settings
WatchGuard AP325	• 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 • Intrusion Prevention Level set to "Interrupt" • Multicast to unicast conversion enabled
Aruba AP303	• In the following tests, the secondary AP is not used: – Neighbor AP – Ad-Hoc Network – Rogue AP • To ensure the WIPS functionalities are performed by the AP under test, the secondary AP is disabled for the WIPS prevention feature. Since the secondary AP(AP335) has a dedicated radio for scanning, we can't disable the detection feature of this AP • The WIPS settings are all configured to “High”. At the beginning of the configuration, we set the Intrusion detection to "High", but after we customized the detection and prevention configuration to enable all the tested threats; the severity setting automatically become to "Medium" • 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” 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 environment for video streaming *“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 MR33	• 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. We also use the client block policy to block the Rogue client and the client connected to the Misconfigured AP • Default multicast to unicast conversion was enabled

Ruckus R510	• 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 under Services tab • 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
Ubiquiti UAP-AC-SHD	• Ubiquiti enabled the WIPS detection by default and did not have the checkbox or configuration option to enable/disable it • Check the Event and Alert checkbox for Rogue AP detected under Notifications
AP125 Overlay	• Configure AP125 works in WIPS sensor mode • Disable the WIPS(detection and prevention) features in other vendors • Configure Authorized WLAN Policies for the SSID of other vendor on WatchGuard Wi-Fi Cloud. AP Auto-classification, Client Auto-classification, Intrusion Prevention and Intrusion Prevention Activation options have been configured to enforce a strict WIPS policy • The Intrusion Prevention Level set to "Interrupt" • Another vendor's AP should be placed in the same folder as AP125.

3.2 Test Bed Environment



Source: Miercom

Test Tools

Hak5 Pineapple
Creates and directs live attacks in a Wi-Fi environment while passively monitoring devices. It targets and audits devices (clients, access points) for damage control, as well as intercept communications using a comprehensive suite of Man-in-the-Middle attack tools. Report data can be set at intervals for vulnerability analysis to gain knowledge on Wi-Fi interaction and threat mitigation using an intuitive user interface and Linux-embedded software.

WireShark
Creates and analyzes packet captures of a live deployment while calculating application and network response times, data, and network volume for over 1,200 applications.

inSSIDer
Scans wireless environments for neighboring and interfering networks and identifies configuration issues for optimal Wi-Fi coverage (e.g. locating best channel, disabling legacy rates, finding security issues) for maximal speed and efficiency

Wi-Spy
Spectrum analyzer software that allows visibility of activity on both 2.4 and 5-GHz bands. It provides a real-time visual overview of interference from both Wi-Fi and non-Wi-Fi sources, channel saturation and dead spots.

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

Media Player
Used for multicast traffic generation using outstream of RTP/MPEG transport with video H.264+MP3 (MP4) codec with MPEG-TS encapsulation to test network and routing

4.0 Test Results

Throughput Traffic Load Test

The load from the Throughput Traffic Load Test also serves as the background traffic utilized during the security efficacy testing. The traffic was generated as IP multicast and used the built-in multicast-to-unicast conversion feature of each AP. Continuous traffic ensures radios of the AP are kept busy to realistically assess the WIPS functionalities. This was not a stress test. There were 15 clients, with 2 on the 2.4-GHz radio and 13 on the 5-GHz radio.

All vendors, excluding Aruba, had no difficulty providing reliable multicast video streaming to 15 clients. With only two clients under load, the background scanning for the Aruba AP303 WIPS did not appear to function. However, with security disabled, the Aruba AP303 could pass our traffic load test to provide streaming video to 15 clients.

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.

Product	2.4-GHz	5-GHz
WatchGuard AP325	Pass	Pass
Aruba AP303	Fail	Fail
Cisco Meraki MR33	Pass	Pass
Ruckus R510	Pass	Pass
Ubiquiti SHD	Pass	Pass

All APs but the Aruba AP303 were able to support dual-band video streaming while protecting the Wi-Fi network. The AP303 works on AP mode only; the WIPS (even background scanning) did not work well while streaming video traffic to the clients. The Aruba AP303 was not able to support the WIPS feature with background traffic. Even with only two clients loaded, videos can play well but background scanning of the AP303 did not appear to work. It cannot scan anything around the AP303. For security efficacy tests, we did not apply any background load for Aruba AP303 testing. We did, however, have the 15 background clients connected. Notably, the Cisco Meraki MR33 improved video streaming ability from previous testing last year.

4.1 Rogue Access Point

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

"Rogue" Terminology per WIPS Product

Product	External/Other AP/Different Network	Rogue/Malicious AP/Same Network
WatchGuard AP325	"External"	"Rogue"
Aruba AP303	"Interfering"	"Rogue"
Cisco Meraki MR33	"Other SSIDs"	"Rogue SSIDs"
Ruckus R510	"Rogue"	"Malicious Rogue"
Ubiquiti SHD	"Neighbor"	N/A

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 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)

Rogue AP Detection & Prevention Results (in seconds) per WIPS Product

Product	2.4-GHz Detection	5-GHz Detection	2.4-GHz Prevention	5-GHz Prevention
WatchGuard AP325	PASS 8.5s	PASS 50s	PASS 30s	PASS 53s
Aruba AP303	FAIL	FAIL	FAIL	FAIL
Cisco Meraki MR33	FAIL	FAIL	MP 25s (manual)	MP 29s (manual)
Ruckus R510	FAIL	FAIL	FAIL	FAIL
Ubiquiti SHD	N/A	N/A	N/A	N/A

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

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. For 2.4-GHz, the Rogue AP was detected in 8.5 seconds and prevented in 30 seconds. For 5-GHz, WatchGuard detected the Rogue AP in 50 seconds and prevented it in 53 seconds. After 10 minutes, the Aruba AP303 only scanned the Rogue AP 5-GHz SSID and classified it as "interfering" without report an event. Within 20 minutes, Aruba scanned both the 2.4 and 5-GHz Rogue AP SSIDs, marking the 5-GHz SSID as suspected Rogue (confidence level 20%) and reported the 5-GHz client to the external AP. After 40 minutes, the 5-GHz Rogue AP was detected, along with the associated client, but auto-prevention failed. Even with manual containment of the Rogue AP SSID, containment failed. Aruba technical support recommends a more powerful AP than the AP303 model or using an overlay. As a result, Aruba does not offer prevention – manual or automatic – of Rogue APs. Cisco classified the Rogue AP to "Other SSIDs"; auto-prevention did not take effect. Only after manually adding the SSID to a blacklist was it contained after 25 seconds for the 2.4-GHz radio and 29 seconds for the 5-GHz radio. Ruckus detected the Rogue AP but only as "rogue AP" and not "malicious rogue". Auto-prevention only works if the Rogue AP is classified as a "malicious rogue". Ruckus reported detected the Rogue AP as "Malicious AP" after 76 seconds for 2.4-GHz and 34 seconds for the 5-GHz radio. Auto-prevention and manual prevention therefore fail to contain the Rogue AP. Ubiquiti detects the Rogue AP and lists it in the Neighbor AP table after 240 seconds; however, manual block failed. Ubiquiti does not support Rogue AP detection, resulting in N/A for detection and prevention on both bands.

4.2 Rogue Client

Any client previously connected to a Rogue AP is considered a Rogue Client. This client poses a risk to the corporate monitored network because it may likely have been compromised with malware or remote access toolkits which attackers commonly use to spread laterally to other endpoint clients inside the network. 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)

Rogue Client Detection & Prevention Results (in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 3s	PASS 3.6s
Aruba AP303	N/A	MP 3.3s (manual)
Cisco Meraki MR33	N/A	MP 49s (manual)
Ruckus R510	N/A	MP 2s (manual)
Ubiquiti SHD	N/A	MP 2s (manual)

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes prevention could not be performed automatically, or the DUT was able to block clients known to be connected to the Rogue AP by other means
- N/A denotes feature is not supported

The WatchGuard product used automatic client classification, a technique based on client behavior, to detect the Rogue Client. The Rogue Client was detected in 3 seconds and prevented in 3.6 seconds. All other vendors were unable to detect the Rogue Client. Third-party detection is required when manual prevention is used in cases where auto-detection and/or auto-prevention fails. For Aruba, the Rogue Client was classified as an "interfering" client. Even after moving this client *from a Rogue AP to an Authorized AP, no event was reported. While auto-prevention was unsuccessful, manual prevention does contain the Rogue Client. Cisco does not support client classification and only manual prevention allowed the application of a blocked policy to a specific client for containment to take effect. Ruckus cannot detect a rogue AP as malicious, as seen in the previous Rogue AP test. Thus, this product cannot identify a client connected to a Rogue AP as a Rogue Client. The only way to block a Rogue Client is to add the wireless client to a blacklist and manually prevent specific client connection. Ubiquiti did not support detection of a Rogue AP; therefore, it could not identify connected clients as rogue either. Manual prevention is necessary to prevent Rogue Client success. According to Ubiquiti technical support, the only test where an AP is identified correctly as rogue is the "Evil Twin AP" test, in Section 5.5. Otherwise, for five of the six tests performed, Ubiquiti lists the SSID in a Neighbor AP listing. Our testing confirmed this. Without being able to identify the Rogue AP, the connecting client cannot be identified or blocked. For all vendors where detection of a Rogue Client failed, the prevention functionality is not considered automatic or fully enabled. The prevention test is therefore assumed to be manual blacklisting or third-party solution (e.g. overlay) to identify the client as rogue.*

4.3 Neighbor Access Point

A Neighbor AP is an independent AP that is not under the control of network administrators. It provides access to the Internet, or another network, that bypasses internal security or content filtering of the corporate network. Clients within local security are considered "authorized" upon connection to the corporate network.

For example, a corporate user typically cannot stream or access raw, unprotected Internet while at work. He or she likely connects to the neighbor network that allows this type of access, but then hops back to the corporate network – leaving the business open to malware. Additionally, a corporate user with personal information on their client device, such as a healthcare professional, risks having this data intercepted by Wi-Fi attackers if they connect to what they believe is a Neighbor AP. Realistically, it's possible this Neighbor AP providing Internet access could be an attacker's AP waiting for a corporate user to connect and steal data or plant remote access toolkits. Unlike the Evil Twin AP test in Section 4.5, the SSID is not copied or spoofed. In fact, a Neighbor AP may not even be malicious at all – its intent is to provide access outside internal security bounds.

However, if a trusted AP is within range, a protected network will prevent corporate-managed clients from connecting to a Neighbor AP. This ensure clients adhere to corporate security policies and do not bypass protection via an accessible Neighbor AP. All ingress streams remain intact by refusing access to external, wireless neighbor devices.

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)

Neighbor AP Detection & Prevention Results (in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 8s	PASS 8s
Aruba AP303	FAIL	MP 16s (manual)
Cisco Meraki MR33	N/A	MP 30s (manual)
Ruckus R510	N/A	N/A
Ubiquiti SHD	N/A	N/A

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

The WatchGuard AP was able to detect and automatically prevent the neighbor AP and attempted connection an authorized client within 8 seconds. The Aruba AP303 could only detect one out of the four attempts within 10 minutes; the other three attempts to detected failed – even after 40 minutes. Prevention was possible by manual intervention only, which is not consistent or reliable. Aruba could only detect the Neighbor AP (mobile hotspot) as "interfering" and reported the event as "valid client misassociation to external AP". Sometimes Aruba was unable to detect the SSID of the Neighbor AP. However, Aruba was the only vendor that could list the clients connected to the possibly malicious Neighbor AP, albeit not classifying them. Manual prevention was successful only 50 percent of the time, within an average of 16 seconds. Cisco detected the Neighbor AP SSID as "Other SSIDs". Auto-prevention was not available, but manual containment of the Neighbor AP was possible via SSID blacklisting. Ruckus did not detect an authorized client connecting to the Neighbor AP but identified the Neighbor AP SSID as rouge (not malicious) in 44 seconds. We assume then that Neighbor AP detection is not supported. Neither automatic nor manual prevention is supported – resulting in an N/A test result. Ubiquiti does not support Neighbor AP detection, so the customer will not know which client (listed in the history client table) is connecting to the Neighbor AP. Since the client is not detected, prevention – even manual – is not supported either.

4.4 Ad-Hoc Network

An Ad-Hoc Wi-Fi network poses a security risk to industries that must maintain strict file transfer auditing records. In an Ad-Hoc Wi-Fi connection, two endpoints can send and receive information that is invisible to network monitoring controls and may open the organization to additional file audit risk.

This test consisted of two connected Windows 7 laptops with direct client communication without additional infrastructure and determined detection and prevention of Ad-Hoc Network.

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)

Ad-Hoc Network Detection & Prevention Results (in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 63s	PASS 82s
Aruba AP303	PASS 149s	FAIL
Cisco Meraki MR33	N/A	FAIL
Ruckus R510	PASS 48s	N/A
Ubiquiti SHD	N/A	N/A

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

The WatchGuard AP detected and auto-prevented Ad-Hoc Network communication by successfully identifying the ad-hoc SSID. The Ad-Hoc Network was detected within an average of 63 seconds and blocked within 82 seconds. After more than 12 minutes, the Aruba AP303 classified the Ad-Hoc Network as an "interfering" AP and reported the event as "valid client misassociation to external AP"; it did not detect or report the even as "valid client misassociation to an ad-hoc network". Auto-prevention failed, and any manual attempt to contain or block the Ad-Hoc Network did not take effect. Cisco detected the Ad-Hoc Network SSID as "Other SSIDs" and auto-prevention was not available; manual blacklisting was supported but failed to contain the Ad-Hoc Network AP. Ruckus was able to detect the Ad-Hoc Network within an average of 48 seconds. It did not support auto-prevention of an authorized client connecting to the Ad-Hoc Network – resulting in an "N/A". Ubiquiti successfully scanned the Ad-Hoc Network SSID and listed it as a Neighbor AP within an average of 110 seconds. However, it was unable to classify as an Ad-Hoc Network distinction like WatchGuard. Ubiquiti makes no claim to be able to detect or prevent Ad-Hoc Network use – resulting in an "N/A".

4.5 Evil Twin Access Point

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)

Evil Twin AP Detection & Prevention Results (in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 5s	PASS 20s
Aruba AP303	PASS 59s	FAIL
Cisco Meraki MR33	PASS 225s	MP 19s (manual)
Ruckus R510	PASS 74s	FAIL
Ubiquiti SHD	PASS 53s	N/A

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

The WatchGuard AP detected the Evil Twin AP in about 5 seconds and auto-prevented it in 20 seconds. The Aruba detected the Evil Twin AP as an "Interfering" and reported this AP in the user interface within 59 seconds. The Evil Twin was reported as a "detected valid SSID misuse" event. Without being able to detect client association to the Evil Twin AP (Aruba reported the client number associated with the Evil Twin AP as 0), auto-prevention failed. Any manual attempts to contain the Evil Twin AP also failed. The Cisco Meraki AP detected the Evil Twin AP SSID as "spoofs", but auto-prevention did not take effect. Manual prevention was successful, within an average of 19 seconds, by blacklisting the Evil Twin SSID. The Ruckus AP detected the Evil Twin SSID as "SSID spoofing AP" within 74 seconds but could not auto-prevent and manual prevention also failed. Ubiquiti successfully detected the Evil Twin SSID as "Rogue AP" within an average of 53 seconds. Ubiquiti does not support prevention of Evil Twin APs. Manual prevention tests also failed.

4.6 Misconfigured Access Point

A Misconfigured AP broadcasts an SSID with settings violating a specific rule or 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)

Misconfigured AP Detection & Prevention Results (in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 1.5s	PASS 1.5s
Aruba AP303	FAIL	MP 9s (manual)
Cisco Meraki MR33	N/A	N/A
Ruckus R510	N/A	N/A
Ubiquiti SHD	N/A	N/A

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

The WatchGuard AP quickly identified and prevented the client from connecting to the Misconfigured AP within 1.5 seconds. The Aruba AP classified both the Misconfigured AP and connecting client as "authorized". After the authorized client moved from the authorized AP to the Misconfigured AP, no event was reported. Auto-prevention failed, but manual prevention allowed for successful containment of the specified client connected to the Misconfigured AP. Aruba is one of the few vendors that provides visibility of clients on networks other than those with protected SSIDs; therefore, it is possible to manually block with administrative intervention. Cisco Meraki did not support detection or prevention of an authorized client connecting to the Misconfigured AP, resulting in N/A. There is no telemetry to indicate which client to block, so there is no way of knowing which client to block. Ruckus cannot support detection of the Misconfigured AP, thus it cannot support detection of an authorized client connecting to a Misconfigured AP. Therefore, prevention is not supported. Like Cisco and Ruckus, Ubiquiti did not support detection or prevention since it is unable to see which client is connected to the Misconfigured AP.

4.7 Multiple Threat Execution

All threats from Sections 4.1-4.6 were concurrently executed to determine if the WIPS could detect and prevent all threats simultaneously.

Test Method:

1. Disable auto prevention
2. Enable all six threats concurrently with background load traffic
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)

Multiple Threat Detection & Prevention Results (%, in seconds) per WIPS Product

Product	Detection	Prevention
WatchGuard AP325	PASS 100%	PASS 100% in 32s
Aruba AP303	FAIL 0%	MP 29% in 34s (manual)
Cisco Meraki MR33	MP 17%	MP 83% in 96s (manual)
Ruckus R510	MP 33%	MP 33% in 8s (manual)
Ubiquiti SHD	MP 21%	MP 25% in 19s (manual)

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

WatchGuard identified and blocked 100 percent of the threats within 32 seconds of concurrent exposure. All threats were detected prior to enabling prevention. Aruba failed to detect any threat scenarios over four test iterations; reporting only a client associated to the Ad-Hoc network as a "valid client misassociation to external AP". At best, manual containment was successful for all scenarios except Rogue Client and Misconfigured AP. Sometimes only one of the threat scenarios was prevented - resulting in an average score of 29 percent within 33.8 seconds. Cisco could only detect the Evil Twin AP, resulting in a 17 percent score. Cisco required manual prevention to SSID blacklist Rogue AP/Ad-Hoc Network/Evil-Twin AP and addition of a blocked client policy for Rogue Client and Misconfigured AP. The Ad-Hoc Network was the only scenario where manual prevention did not take effect, resulting in an average prevention rate of 83 percent, within 96 seconds. The Ruckus AP could only detect two threat scenarios – Evil Twin AP and Ad-Hoc Network – yielding a detection efficacy of 33 percent. Ruckus could block any client connected to the managed AP (e.g. authorized AP and Misconfigured AP). However, clients connected to other SSIDs were essentially invisible to Ruckus, making blocking them impossible. Ruckus had manual prevention only for up to 33 percent of threats within 8 seconds. Ubiquiti could mostly only detect the Evil Twin AP scenario, exception for one iteration where two scenarios were identified – resulting in an average detection rate of 21 percent. Ubiquiti allowed manual prevention of all scenarios, but only stopped the Rogue Client and Misconfigured AP successfully for a 25 percent block rate in 18.7 seconds.

4.8 MAC Spoofing

This test has two components: MAC Spoofing Client and MAC Spoofing AP. A WIPS solution is expected to detect and prevent this type of exploit, which uses MAC access control and related policies of wired and wireless network-connected devices. An example of this attack is when traffic is captured and intercepted for free Wi-Fi access in hotels.

Two vendors were tested: WatchGuard and Ruckus. These were the only vendors that support MAC Spoofing protection. These tests are first performed without MAC Spoof detection enabled.

4.8.1 MAC Spoofing Client

MAC Spoof Client testing evaluates the WIPS product for its ability to detect a client that uses a spoofed MAC address from an authorized client on the network to obtain access. A trusted network is established with independent SSID MAC_Spoofing-Test Channel.

A Nokia Android phone was configured to use the MAC address of a trusted client on the authorized network. The test was to detect and prevent the client with spoofed (known) MAC address from accessing the network.

Test Method:

1. Setup independent SSID and Channel from existing test bed with one AP
2. Disable detection and prevention of MAC Spoof Client features
3. Establish a trusted client on the test network and verify access
4. Spoof a client MAC and determine if this rogue spoof client can access the network without authentication
5. Determine if the rogue MAC Spoof Client is listed in any way by the DUT, with no expectation of detection
6. Enabled MAC Spoof detection and prevention, repeating steps 3 through 5.
7. Record pass/fail for detection and prevention of MAC Spoof AP

MAC Spoofing Client Detection & Prevention Results

WatchGuard was able to detect and prevent the MAC Spoofing Client – iPad or Android phone. Ruckus could not detect or prevent MAC Spoofing Clients.

4.8.2 MAC Spoofing AP

This test determined detection and prevention of a client attempting to connect to a MAC spoofed AP. A rogue AP was introduced with a spoofed MAC, copied from another legitimate AP on the authorized network. The test determined how the DUT could mitigate the threat of the MAC spoofing AP by preventing clients from connecting to the rogue AP.

This test is a similar, but more complex version of, the Evil Twin AP test in Section 4.5. The Wi-Fi Pineapple tool acts as the Evil Twin AP – but unlike before, the MAC address is spoofed in addition to the SSID.

The goal of MAC spoofing is to increase the effectiveness of an Evil Twin AP attack and deceive victims of a Wi-Fi network into connecting to a rogue AP.

Test Method:

1. Locate the victim AP (legitimate) SSID
2. Setup independent AP (attacker) using the Wi-Fi Pineapple tool and spoof the victim AP MAC address
3. Disable detection and prevention of MAC Spoof AP features
4. Associate a client to the victim AP and ping wired host continuously
5. Associate a client to the MAC Spoof AP and ping wired host continuously
6. Determine if the rogue MAC Spoof AP is listed in any way by the DUT, with no expectation of detection
7. Enabled MAC Spoof AP detection and prevention, repeating steps 4 through 6.
8. Record pass/fail for detection and prevention of MAC Spoof AP

MAC Spoofing AP Detection & Prevention Results

WatchGuard could detect and prevent the rogue AP with spoofed MAC address. Ruckus could detect but was unable to prevent clients from connecting to the MAC spoofed AP.

4.9 Overlay Access Point

There is a distinction between Overlay WIPS and Integrated WIPS of the WLAN infrastructure. The Overlay WIPS provides a separate security layer than the inherent WIPS already in place. The Overlay WIPS can be the same vendor as the inherent WIPS, or a different vendor entirely.

In the Integrated WIPS environment, the APs dedicate about 99 percent of their time and resources to staying on traffic channels; this leaves about 1 percent or less for scanning off-traffic channels in what's referred to as "background scanning". According to the Certified Wireless Network Professionals, this leads to latency of detecting threats and missed detection of ad-hoc networks and neighbor AP connections. Advanced features are also not as efficient since wireless data cannot be collected from the less-traveled off-channels. Monitoring non-standard channels also is difficult since it requires more frequent off-channel scanning.

These insufficiencies can benefit from an Overlay which has a dedicated radio WIPS mode. And while Integrated WIPS can also be operated in this mode, it would require multiple APs to cover the facility, an allocated AP in WIPS monitoring mode, or some other controller hardware for management. The deployment cost of this setup should be considered. The Overlay has sensors covering the environment and a WIPS server for sensor management and WIPS.

Businesses may find deployment of an Overlay presents technical, architectural and financial implications. An example of this is a "preferred vendor"; it can be easier from a technical standpoint to use a vendor consistent with existing network equipment to reduce downtime and training costs.

If the Overlay is hardware-based the business must consider substantial deployment costs. Having a cloud-based Overlay can significantly reduce costs while widening the breadth of wireless protection.

To test the Overlay, we applied the WatchGuard AP125 with WIPS security onto an existing Wi-Fi network with competitive products. If possible, we disabled detection and prevention on the Integrated WIPS APs (Aruba AP303, Cisco Meraki MR33, Ruckus R510 and Ubiquiti UAP-AC-SHD). Aruba and Ruckus were able to disable detection and prevention features. For the other vendors, we disabled prevention.

By comparing the Overlay detection and prevention rating and times for each vendor/product, and results from Sections 4.1 through 4.7, we were able to distinguish the benefit of the WatchGuard AP125 Overlay for a vendor-diverse environment.

Test Method:

1. List the previous vendor test results (organic detection and prevention)
2. Disable detection and/or auto-prevention on the tested product
3. Apply the WatchGuard AP125 WIPS Overlay on the DUT
4. Add the DUT by vendor name/AP/SSID into the "authorized" AP in WatchGuard WLAN policy
5. Record detection and prevention PASS/MP/FAIL and times as previously conducted for tests
6. Compare the Overlay test result to the vendor's previous results

WatchGuard AP125 as WIPS Overlay on APs Detection & Prevention Results

	Aruba AP303		WatchGuard Overlay on Aruba AP303		Cisco Meraki MR33		WatchGuard Overlay on Cisco Meraki MR33		Ruckus R510		WatchGuard Overlay on Ruckus R510		Ubiquiti UAP-AC-SHD		WatchGuard Overlay on Ubiquiti UAP-AC-SHD	
	D	P	D	P	D	P	D	P	D	P	D	P	D	P	D	P
Rogue AP	FAIL	FAIL	PASS	PASS	FAIL	MP	PASS	PASS	FAIL	FAIL	PASS	PASS	N/A	N/A	PASS	PASS
Rogue Client	N/A	MP	PASS	PASS	N/A	MP	PASS	PASS	N/A	MP	PASS	PASS	N/A	MP	PASS	PASS
Neighbor AP	FAIL	MP	PASS	PASS	N/A	MP	PASS	PASS	N/A	N/A	PASS	PASS	N/A	N/A	PASS	PASS
Ad-Hoc Network	PASS	FAIL	PASS	PASS	N/A	FAIL	PASS	PASS	PASS	N/A	PASS	PASS	N/A	N/A	PASS	PASS
Evil Twin AP	PASS	FAIL	PASS	PASS	PASS	MP	PASS	PASS	PASS	FAIL	PASS	PASS	PASS	N/A	PASS	PASS
Misconfigured AP	FAIL	MP	PASS	PASS	N/A	N/A	PASS	PASS	N/A	N/A	PASS	PASS	N/A	N/A	PASS	PASS
Concurrent Threats	0%	29%	100%	100%	17%	83%	100%	100%	33%	33%	100%	100%	21%	25%	100%	100%

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

This chart compares the WatchGuard AP125 used in a WIPS Overlay mode compared to vendors' own inherently provided security protection. In all cases, WatchGuard provided greater protection for all scenarios tested.

4.10 WatchGuard AP125 Overlay vs Aruba AP303 WIPS Overlay

After comparing the Overlay results to the Integrated WIPS environment, we compared the WatchGuard Overlay to another vendor Overlay. In this case, we used the Aruba AP303 Overlay. Aruba could only be used as an Overlay on the same AP type; we were unable to overlay the Aruba AP303 on a different vendor AP. For example. the Aruba Controller would always mark the Ruckus AP as "contained" and begin taking blocking actions on connecting clients.

The only way to test the Aruba Overlay was to repeat the test on the Aruba AP225 as the DUT. We feel this gives Aruba an unfair advantage as both the AP225 and AP303 contribute to the scanning time and possible PASS/FAIL efficacy for threat detection. But we felt it reasonable to try a ubiquitous Aruba environment for this test, as it would display best-case results. Therefore, the prevention was turned off for the Aruba AP225 (Primary AP) and put the Aruba Overlay AP303 in control of security.

WatchGuard AP125 Overlay vs Aruba AP303 WIPS Overlay Mode Results

	Aruba AP303 Standalone		Aruba AP303 as Overlay		WatchGuard AP125 as Overlay on Aruba AP303	
	D	P	D	P	D	P
Rogue AP	FAIL	FAIL	PASS	PASS	PASS	PASS
Rogue Client	N/A	MP	FAIL	MP	PASS	PASS
Neighbor AP	FAIL	MP	FAIL	FAIL	PASS	PASS
Ad-Hoc Network	PASS	FAIL	PASS	PASS	PASS	PASS
Evil Twin AP	PASS	FAIL	FAIL	FAIL	PASS	PASS
Misconfigured AP	FAIL	MP	FAIL	FAIL	PASS	PASS
Concurrent Threats	0%	29%	33%	50%	100%	100%

Source: Miercom 2019

- PASS denotes all tests passed, with time shown for detection and/or prevention
- FAIL denotes feature indicated support by vendor's product but could not pass test
- MP (Manual Prevention) denotes that prevention could not be performed automatically and required user intervention
- N/A denotes feature is not supported

The Aruba AP303 alone only supported manual prevention of a Neighbor AP within 16 seconds; detection of Ad-Hoc Network and Evil-Twin AP; manual prevention of a Misconfigured AP in 9 seconds; and manually prevented 29 percent of concurrent threats in 34 seconds. With the Aruba AP303 Overlay applied to same-vendor AP225 WIPS with security disabled, more capabilities were supported. The Aruba Overlay allowed for the detection and prevention of a Rogue AP within 25 and 92 seconds, respectively on the 5-GHz radio. Despite the inability to detect the Rogue Client, manual prevention was achievable within 92 seconds. The Neighbor AP and Misconfigured AP tests failed when the Aruba Overlay was enabled, when it had marginally passed without it; we believe the Aruba AP303 is underpowered. However, the Ad-Hoc Network was detected in 42 seconds and prevented in 52 seconds. Concurrent threat protection increased from 0 to 33 percent detection and 29 to 50 percent prevention in 92 seconds. When the WatchGuard Overlay was enabled, every single test was passed – meaning automatic detection, reporting and prevention were successful for each scenario. The concurrent threat scenario was detected 100 percent of the time and prevented 100 percent.

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.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.