Miercom

October 2024

DR231210D

CISCO

Cisco Wireless Competitive Assessment

miercom.com/cisco

Table of Contents

1.0 Executive Summary 3
2.0 Report Evaluation Criteria 4
2.1 Products Tested 4
3.0 Throughput Performance 5
3.1 Multi-Gigabit Throughput Performance 5
3.2 Multi-Client Performance 7
3.3 Access Point PoE Efficiency 8
3.4 Access Point Power Requirements 9
3.5 Power Optimization Features for Access Points 10
4.0 Wireless Security Testing 11
4.1 Rogue AP Detection and Containment 11
4.1.1 Rogue AP Detection 11
4.1.2 Rogue Containment 13
4.2 Rogue AP with PMF Enabled: Detection and Containment 14
4.3 WIPS Security 15
5.0 Network Operations 16
5.1 Wireless Planning 16
5.2 Firmware Upgrade 17
5.3 Compliance Audit 18
5.4 Technology Upgrade 19
6.0 Artificial Intelligence Operations 20
6.1 AI-Driven RF Optimization 20
6.2 Network Trends and Insights 22
6.3 Comparative Benchmarking 23
6.4 Access Points Comparison 25
6.5 Application Performance Monitoring 26
6.5.1 Wireless Application Visibility 26
6.5.2 Wireless Application Assurance 27
Appendix A: Report Evaluation Criteria 28
Appendix B: Performance Test Setup 29
B.1: Multi-Gigabit Throughput Performance 29
B.2: Multi-Client Throughput Performance 29
Appendix C: Sustainability 30
Appendix D: Wireless Security 30
D.1: Rogue AP Detection and Containment 30
D.2: Rogue AP with PMF Enabled: Detection and Containment 31
D.3: WIPS Testing 31
Appendix E: Network Operations 32
E.1: Firmware Upgrade 32
Appendix F: Artificial Intelligence Operations 34
F.1: Wireless Application Visibility 34
About Miercom 35
Use of This Report 35

Copyright ©2024 Miercom

1.0 Executive Summary

Enterprise wireless networks continue to evolve to meet the business needs of users, devices, and things. Cisco Systems, Inc. engaged Miercom to independently assess Cisco Catalyst Center (on-premise) and Cisco Meraki (SaaS Cloud), alongside the latest competitive offerings of Hewlett Packard Enterprise (HPE-Aruba) and Juniper-Mist Technologies in four key areas: **Performance**—examines the characteristics of optimal end-user experience in terms of AP throughput. **Sustainability**—considers the enterprise's ability to save on electricity and reduce its energy footprint. **Security**—assesses the wireless network's resistance to attacks through the network. **Operational Simplicity**—evaluates the ease of deploying, managing, monitoring, and optimizing the wireless network.

Key Findings:

- **High Performance:** Cisco Access Points offer the best overall throughput performance, followed by HPE Aruba and Juniper Mist.
- **Sustainability:** Cisco offers energy-efficient access points along with innovative power saving functions that help customers meet their sustainability goals.
- **Wireless Security:** Cisco stands out with its best-in-class wireless security, excelling in detecting and containing rogue devices and wireless attacks.
- **Network Operations:** Cisco provides automation for all stages of the network lifecycle at scale, saving time, resources, and money for IT operations. In contrast, HPE-Aruba and Juniper Mist lack the depth of automation features.
- **AI Operations and Insights:** Cisco distinguishes itself as a complete AIOps solution, covering all the network assurance use cases, including troubleshooting and optimizing the wireless network for users and applications. This feature sets it apart from its competitors.

The Cisco Catalyst Center, Cisco Meraki, Catalyst 9100 Series Wi-Fi 6E APs, and Catalyst 9800 Series Wireless Controller were thoroughly observed and subjected to an extensive analysis. This process clearly shows that the Cisco solution improves performance, secures applications, while simplifying and maintaining network operations.

We proudly award the Cisco Catalyst 9100 Series Access Points, Cisco Catalyst 9800 Series Wireless Controller, Cisco Catalyst Center, and Cisco Meraki the **Miercom Performance Verified** certification.

Robert Smithers

CEO, Miercom

Copyright ©2024 Miercom

2.0 Report Evaluation Criteria

Products were assessed under two main categories. The first category tested the performance, PoE efficiency, and security of the wireless solution (AP and the management platform). The second category evaluated the network operations and assurance capabilities by examining each vendor's dashboard on the respective management platform.

2.1 Products Tested

Access Points			
6-GHz: 4x4 **5-GHz: 4x4** **2.4-GHz: 4x4**	CW9166	AP655	AP45
6-GHz: 4x4 **5-GHz: 4x4** **2.4-GHz: 2x2**	CW9164	N/A	N/A

N/A – No product with this capability

For test bed setup, testing tools and firmware versions, refer to Appendix A.

Management/Assurance/Orchestration Platforms

Cisco Catalyst Center is a management and orchestration solution offering a long-term commitment to deploying, managing, monitoring, and troubleshooting any network environment. Its Assurance module provides insightful tools – AI-Enhanced RRM, AI Network Analytics, Network 360, Intelligent Capture – giving IT teams the context needed to identify and remediate issues. The solution automatically collects and organizes device, app, and user data over time, helping admins correlate and analyze data to make informed decisions and address potential problems before they impact user services in the end-to-end wired and wireless network.

Cisco Meraki is a cloud software-as-a-service platform offering full-stack management, automation, and assurance of wired, wireless, SD-WAN, cameras, and sensors. The dashboard offers insights into network configurations, poor client experience, detailed root cause analysis, and optimization strategies to reduce the number of support tickets.

Aruba Central Cloud is a cloud-based network management and analytics platform that offers deployment and management of wired, wireless and SD-WAN networks. The AI Insights module leverages AI/ML to provide up to one month of insights into network issues. Network admins can access the AI Insights dashboard to take corrective actions on network problems.

Mist Cloud is a microservices-based cloud management and assurance platform for Mist APs, Juniper SRX and 128T Routers, and EX Switches. It features MARVIS, used for Network Assurance and AI Anomaly Detection. MARVIS includes a Virtual Network Assistant powered by a Natural Language Processing engine that helps network admins quickly identify and resolve network issues by pinpoint root causes.

Copyright ©2024 Miercom

3.0 Throughput Performance

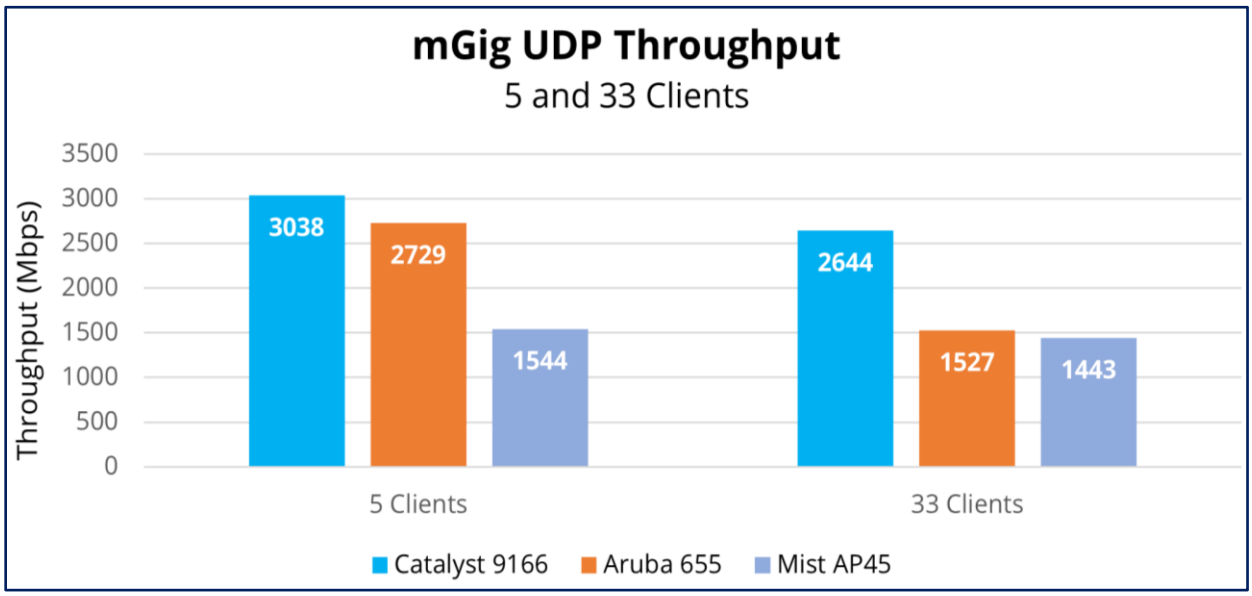
Wi-Fi 6E Introduction

Wi-Fi 6E the IEEE 802.11ax standard introduced the 6 GHz band, in addition to the existing 2.4 and 5 GHz bands. This addition triples the amount of spectrum available, providing more channels, reducing interferences, and higher bandwidth. Wi-Fi 6E APs can support more devices simultaneously while maintaining high throughput, making it ideal for dense environments and high-demand applications. This advancement is set to enhance wireless communication by offering faster speeds, lower latency, and more reliable connections, particularly in crowded spaces. With any new technology, transitioning to Wi-Fi 6E requires careful consideration of infrastructure upgrades and compatibility with existing devices, but its benefits for future-proofing networks are significant.

3.1 Multi-Gigabit Throughput Performance

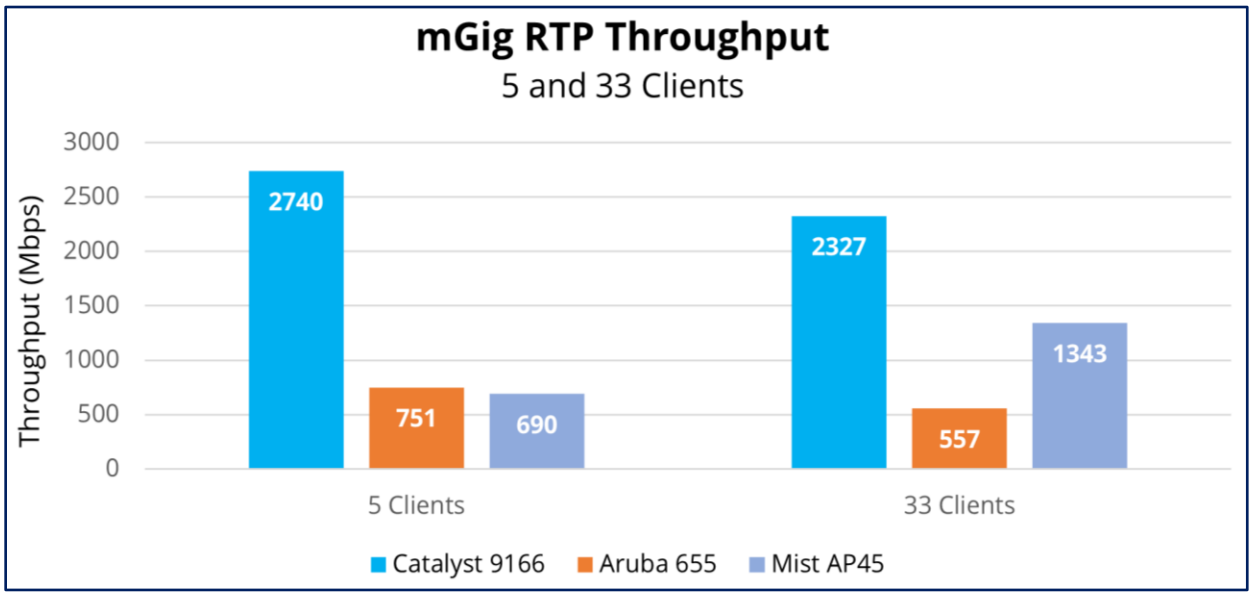
Wired throughput bottlenecks can cause packet dropping and latency, affecting end-user clients and overall network efficiency. This test aimed to observe the APs' maximum capacity and if today's Wi-Fi 6E APs require a modern mGig switch infrastructure.

Refer to Appendix B.1 for testing methodology.



When serving 5 clients, the Cisco 9166 posted an impressive UDP throughput of 3 Gbps+, surpassing Aruba 655 by 11% and outperforming Mist AP45 by an impressive 96%. With 33 clients connected, the Cisco 9166's performance was 73% higher than the Aruba AP655 and 83% better than the Mist AP45. For Aruba AP, in the 33 clients' UDP test, we noticed the test was failing at the 40-second mark during the tests run.

Copyright ©2024 Miercom

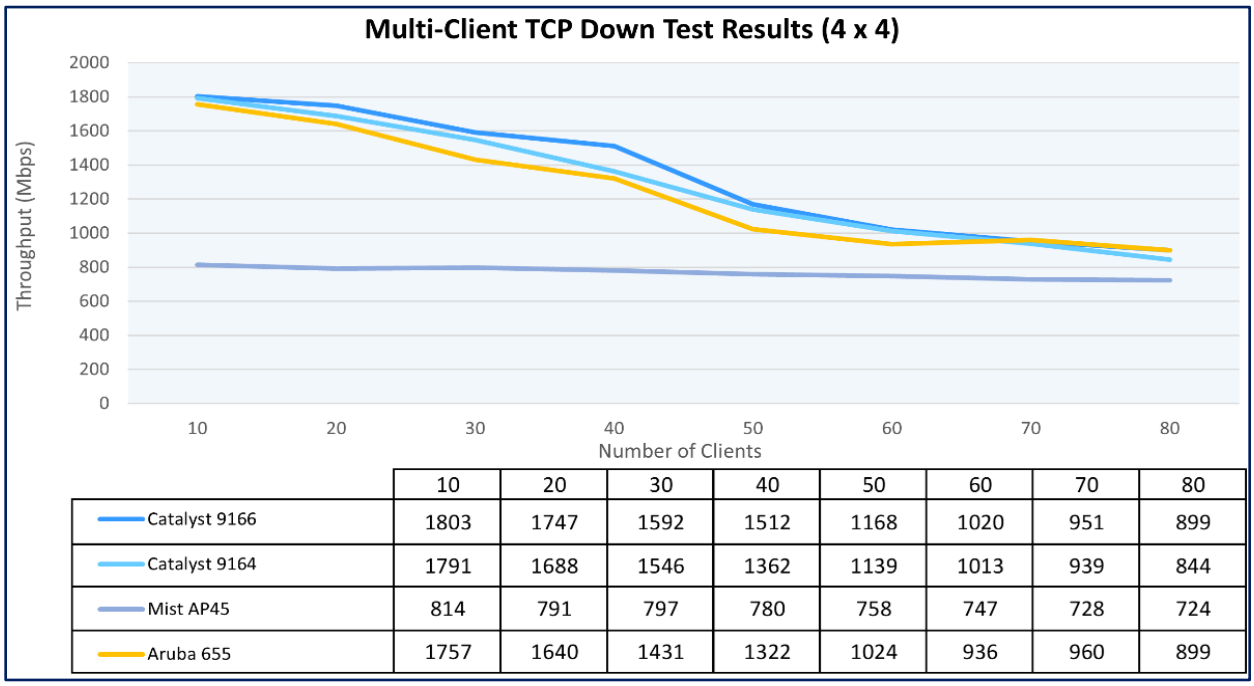


During testing, the Aruba AP failed to generate any throughput using the default RTP script. To address this, we tried different data rates in the IxChariot RTP script, which produced optimal results. In Mist, the AP generated traffic with the default RTP script, but the throughput was lower with 5 clients compared to 33 clients. When serving 5 clients, the Cisco 9166 RTP throughput was 3.64 times greater than the Aruba AP655 and 3.97 times greater than the Mist AP45. With 33 clients, Cisco 9166 RTP throughput was 4.17 times greater than Aruba AP655 and 1.73 times greater than the Mist AP45. Both Aruba and Mist AP failed at the 30-second mark during the test run.

3.2 Multi-Client Performance

As businesses scale, the ability of a network infrastructure to support multiple simultaneous clients without performance degradation ensures seamless operations and enhances user experience. Consistent throughput ensures that each client receives a stable and reliable connection. This scalability and reliability are essential for meeting the demands of a growing user base and applications without compromising performance.

Refer to Appendix B.2 for testing methodology.



	10	20	30	40	50	60	70	80
Catalyst 9166	1803	1747	1592	1512	1168	1020	951	899
Catalyst 9164	1791	1688	1546	1362	1139	1013	939	844
Mist AP45	814	791	797	780	758	747	728	724
Aruba 655	1757	1640	1431	1322	1024	936	960	899

For the performance comparison of all 4x4 radio-antenna APs, the Cisco 9166 had the highest performance, even as client count increased. The Cisco 9166, on average, outperformed Mist AP45 by 74% and Aruba 655 by 7%. The Cisco 9164 also maintained superior performance, with 68% better overall throughput than Mist AP45 and 3.6% better than Aruba 655. The graph shows a consistent decline in throughput as the client count increases, which is common in multi-client test environments. Yet, the Cisco APs manage to sustain a comparatively higher throughput rate.

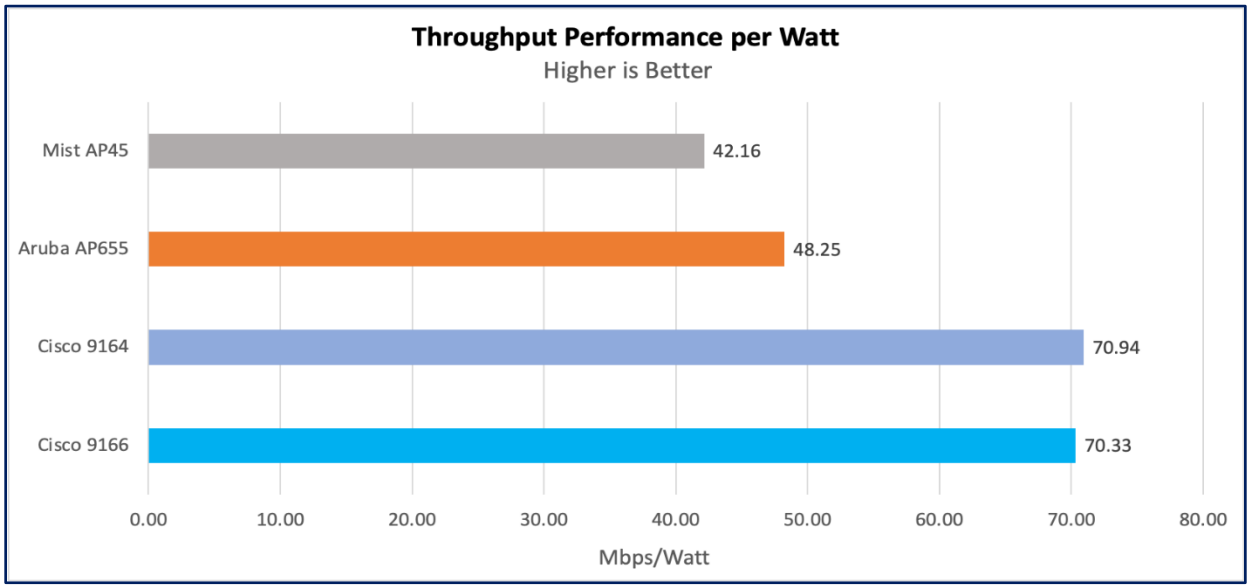
Copyright ©2024 Miercom

3.3 Access Point PoE Efficiency

Power over Ethernet (PoE) consumption management contributes to a more cost-effective, environmentally friendly, and sustainable network infrastructure. The addition of the 6 GHz radio and the latest AP hardware components greatly enhances the throughput and overall capacity of the wireless networks. However, this also means that access points consume more power. It is vital to take the initiative to maintain access points' energy efficiency while providing superior throughput.

Refer to Appendix C for testing methodology.

Access Point PoE Efficiency – Competitive Summary



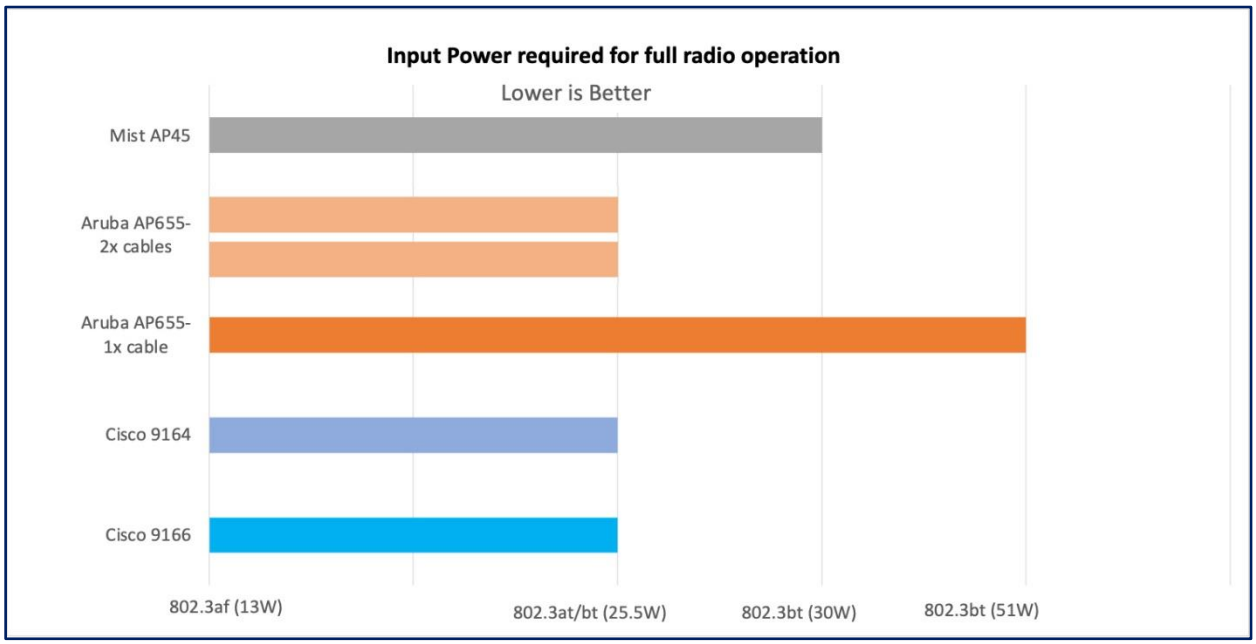
PoE consumption throughput per watt--Higher is better. The Cisco 9166 PoE throughput efficiency was 67% superior to the Mist AP45 and 46% more efficient than the Aruba 655.

Copyright ©2024 Miercom

3.4 Access Point Power Requirements

Network upgrades to the latest fleet of switches and access points are typically performed in phases. In many instances, the wireless network is upgraded before the switching infrastructure. The Wi-Fi 6E access points typically require 802.3bt to operate without any restrictions on the number of antenna chains and transmit power. Connecting the APs to the legacy switches with 802.3af or 802.3at PoE output reduces the APs' capabilities, impacting the wireless client experience.

AP PoE Requirements – Competitive Summary



Cisco CW9166 supports full radio operation at 802.3at power. In comparison, Aruba AP655 and Juniper AP45 are reduced to lower radio chains when powered with 802.3at. Aruba AP655 supports Dual PoE ethernet ports, which can combine PoE power, providing unrestricted access at 802.3at.

Copyright ©2024 Miercom

3.5 Power Optimization Features for Access Points

Software automation features for power optimization can also help maintain energy efficiency in the network. A well-defined power policy ensures that the AP is operating efficiently within the power budget, wherein the required interfaces in the AP are given priority over others, such as Wi-Fi radios, and USB. AP Power Saving Mode allows APs to reduce power usage during low activity periods. Insights on power savings can provide administrators with actionable data about the energy usage patterns within the network, enabling informed decisions about where and how energy savings can be achieved. Additionally, Switch Port Scheduling contributes by allowing the power to be turned off on switch ports during non-operational hours, further reducing unnecessary power consumption. By leveraging these power optimization features, organizations can enhance energy management.

Access Point Power Optimization Summary

Test Case	Cisco	HPE Aruba	Juniper Mist
PoE Power Policy	✓	✓	⊘
AP Power Save Mode	✓	⊘	⊘
AP Power Saving Insights	✓ On-Prem Only	⊘	⊘
Switch Port Scheduling	✓ Cloud Only	⊘	⊘

**Power Save mode in Aruba Central is currently offered as a beta feature for selected customers only.*

4.0 Wireless Security Testing

The functional testing included three categories: Rogue AP detection using dedicated radio scanning, Rogue AP containment after a rogue AP was identified , and the Wireless Intrusion Prevention System (WIPS) capabilities of different network devices. The results are discussed in the following sections.

4.1 Rogue AP Detection and Containment

Unauthorized access points, whether unintentionally set by an employee or by some malicious actor, can pose a threat to the security and integrity of the wireless network. Clients connected to the rogue APs can easily compromise the network by accessing restricted subnets, spreading malware, and much more. A robust rogue management solution should be able to accurately identify and promptly alert about Rogue APs in the network. Furthermore, it should be able to prevent rogue APs and clients from gaining unauthorized access to the network.

4.1.1 Rogue AP Detection

Refer to Appendix D.1 for test setup and evaluation criteria.

Rogue Broadcasting with Identical SSID Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
Rogue broadcasting an identical SSID as the network AP	**Channel 36, 100, and 149**			
	Detection	✓	✓	✓ Detected as Honeypot
	Accuracy • Detection • Channel	✓	✓ • Inconsistent detection of Rogue AP on CH 100 & 149 • Sometimes incorrect channel detected on CH 36	✓ Inconsistent detection of Rogue AP on all channels
	Channel 36			
	Time to detect	✓ 2 seconds	⊘ 3 – 5 Minutes	⊘ 2 – 5 Minutes
	Channel 100			
	Time to detect	✓ 2 seconds	⊘ 5 – 7 minutes	⊘ 3 – 5 minutes
	Channel 149			
	Time to detect	✓ 2 seconds	⊘ 5 – 10 minutes	⊘ 5 – 7 minutes

Copyright ©2024 Miercom

Rogue Broadcasting with Different SSID Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
Rogue broadcasting a different SSID than the network AP	**Channel 36, 100, and 149**			
	Detection	✓	✓	⊘ Incorrectly detected as neighbor AP
	Channel 36			
	Accuracy • Detection • Channel	✓	✓	✓ Inconsistent detection
	Time to detect	✓ 2 seconds	⊘ Within 3 minutes	⊘ 5 – 7 minutes
	Channel 100			
	Accuracy • Detection • Channel	✓	✓ Inconsistent detection	✓ Inconsistent detection
	Time to detect	✓ 2 seconds	⊘ 5 – 7 minutes	⊘ 5 – 7 minutes
	Channel 149			
	Accuracy • Detection • Channel	✓	✓ Inconsistent detection	✓ Inconsistent detection
	Time to detect	✓ 2 seconds	⊘ 5 – 10 minutes	⊘ 5 – 7 minutes

The Cisco 9166, equipped with a dedicated tri-band scanning radio, consistently identified Rogue APs across all channels within seconds. Aruba's rogue detection varied across channels, likely due to the lack of a dedicated scanning radio, resulting in inaccuracies and delays in reporting, ranging from 3-10 minutes. Mist's performance was like Aruba's but occasionally showed shorter detection times by 1-2 minutes. Mist misclassified Rogue APs as neighboring APs when the rogue device broadcasted a different SSID than the network AP. Both Aruba and Mist showed inconsistent rogue detection, with instances where no rogue APs were displayed on the dashboard during multiple test iterations.

Copyright ©2024 Miercom

4.1.2 Rogue Containment

Refer to Appendix D.1 for test setup and evaluation criteria.

Rogue Broadcasting with Identical SSID Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
	Channel 36			
Rogue broadcasting an identical SSID as the network AP	**Containment**	✓	✓	⊘ No option to contain
	Time to contain	✓ <1 Minute	✓ 2 Minutes	⊘
	Reporting	✓ 3 – 5 Minutes	✓ 2 Minutes	⊘
	Channel 149			
	Containment	✓	⊘	⊘ No option to contain
	Time to contain	✓ <1 Minute	⊘	⊘
	Reporting	✓ 3 – 5 Minutes	⊘	⊘

Rogue Broadcasting with Different SSID Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
	Channel 36			
Rogue broadcasting a different SSID than the network AP	**Containment**	✓	✓	⊘ No option to contain
	Time to contain	✓ <1 Minute	✓ 2 Minutes	⊘
	Reporting	✓ 3 – 5 Minutes	✓ 2 Minutes	⊘
	Channel 149			
	Containment	✓	⊘	⊘ No option to contain
	Time to contain	✓ <1 Minute	⊘	⊘
	Reporting	✓ 3 – 5 Minutes	⊘	⊘

Cisco's rogue auto-containment feature successfully contained the rogue AP on all the channels within a minute but reported the containment in 3 to 5 minutes on the dashboard. In contrast, Aruba's performance varied significantly, showing containment and reporting effectiveness on channel 36 but proving ineffective on channel 149. Mist's manual containment feature offers an approach to contain rogue APs displayed in a list view. We noticed, it did not give the option to contain the rogue AP, since it detected the rogue AP as a honeypot. However, if it were detected as a rogue AP, we would see a contain option.

Copyright ©2024 Miercom

4.2 Rogue AP with PMF Enabled: Detection and Containment

Protected Management Frames (PMF) or 802.11w is a required feature in WPA3 networks. It plays a crucial role in bolstering Wi-Fi network security by safeguarding the exchange of management frames between client devices and access points. However, it makes it harder to detect rogue APs with PMF enabled due to encrypted management frames. Additional measures are required for effective rogue detection and containment.

Refer to Appendix D.2 for test setup and evaluation criteria.

Rogue Broadcasting with Identical SSID with PMF Enabled Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
		Channel 36		
Rogue broadcasting with PMF enabled on an identical SSID as the network AP	Detection	✓	✓	✓
	Time to detect	✓	✓	✓ 2 Minutes
	Containment	✓ On-Prem Only	✓	No PMF Containment Feature
	Reporting	✓ 3 – 5 Minutes	✓ 5 – 7 Minutes	

Rogue Broadcasting with Different SSID with PMF Enabled Test Case Summary

Test Case	Results	Cisco	HPE Aruba	Juniper Mist
		Channel 36		
Rogue broadcasting with PMF enabled on a different SSID as the network AP	Detection	✓	✓	⊘ Incorrectly detected as neighbor AP
	Time to detect	✓	✓ 1 – 3 Minutes	✓ 2 – 3 Minutes
	Containment	✓ On-Prem Only	✓	No PMF Containment Feature
	Reporting	✓ 3 – 5 Minutes	✓ 5 – 7 Minutes	

When Rogue AP was broadcasting both identical and distinct WPA3 SSIDs, Cisco exhibited consistent performance in detecting, containing, and reporting the AP, mirroring its previous performance. Aruba showed improvement in detecting the rogue AP with PMF enabled but still experienced a 2–4 minutes delay in reporting time compared to Cisco. With different SSIDs, Aruba experienced a slight delay of 1-3 minutes in detecting the rogue AP. Mist was successfully able to detect PMF enabled rogue AP but lacked PMF containment features.

Copyright ©2024 Miercom

4.3 WIPS Security

Wireless Intrusion Prevention System (WIPS) monitors wireless networks by actively scanning the air for suspicious activity, such as man-in-the-middle attack, denial-of-service in the network. Successful identification of the attacks is crucial for maintaining the security and integrity of wireless networks, especially in environments where wireless communication is critical or where the risk of unauthorized access is high.

Refer to Appendix D.3 for test setup and evaluation criteria.

WIPS Signature Detection Test Case Summary

Wireless Attacks **Evaluation:** 1) Signature Detection 2) Reporting Time	**Cisco**	**HPE Aruba**	**Juniper Mist**
Broadcast Probe	✓	✓ Detects as "Rate anomaly at station"	⊘
	✓ (<15 secs)	✓ (> 1 min)	
Disassociation Probe	✓	⊘	⊘
	✓ (<15 secs) **On-Prem Only**		
Broadcast De-authentication	✓	⊘	⊘
	✓ (<15 secs) **On-Prem Only**		
RTS Flood or RTS Virtual Carrier Sense Attack	✓	✓ Detects as "RTS Rate anomaly")	⊘
	✓ (>1 min) **On-Prem Only**	✓ (> 1 min)	
Reassociation request Flood	✓	⊘	⊘
	✓ (<15 secs)		
Authentication Flood	✓	✓	⊘
	✓ (<15 secs) **Cloud Only**	✓ (>1 min)	
Association Request Flood, Malformed Association Request	✓	✓	⊘
	✓ (<15 secs)	✓ (>1 min)	
Fuzzed Beacon	✓	⊘	⊘
	✓ (<15 secs)		
Fuzzed Probe Request	✓	⊘	⊘
	✓ (<15 secs)		
Beacon Flood	✓	✓ Detects as "AP impersonation"	⊘
	✓ (<15 secs)	✓ (>1 min)	
Invalid MAC OUI	✓	✓ Detects as "Invalid Address Combination"	⊘
	✓ (<15 secs)	✓ (>1 min)	

Cisco successfully identified most of the signatures within 15 seconds, except for RTS Flood, which took more than one minute to detect. Overall, Cisco demonstrated precise detection and timely reporting of ongoing attacks. Aruba's documentation mentions support for most of the signatures under test, but they do not align with the testing results. Aruba often misidentified the attack types and reported incidents well after initiating the attack. Additionally, Mist did not detect any signatures during the testing.

Copyright ©2024 Miercom

5.0 Network Operations

Network Operations encompasses the entire lifecycle from initial design and planning at Day 0, where networks are architected and onboarded, through Days 1 and 2 for active management. This includes regular firmware upgrades, adherence to compliance standards and responding to security advisories, Day N for transformation – where long-term evolution of the network takes place through integration of new technology upgrades and device refresh cycles. This structured approach ensures that the wireless network performance remains efficient, secure, and up to date with technological advancements, offering optimal performance throughout its operational life.

This section focuses on areas that comprise operational simplicity. Including features like Wireless Planning, Firmware Updates, Compliance Audits and Technology Upgrades.

5.1 Wireless Planning

Wireless planning is a necessary step to ensure a robust wireless network with ubiquitous coverage. The planning for 6E APs dramatically benefits from integrating survey tools like Ekahau, iBwave, and Hamina Wireless. These tools facilitate the auto-creation of floor plans that can be imported to the management dashboard to simplify AP deployment and enhance design accuracy of wireless networks. The use of wireless heatmaps helps to resolve potential coverage and interference issues, 3D wireless heatmaps can enhance RF troubleshooting and optimization in complex physical areas such as warehouses where signals can vary at different elevations. The planned AP feature can help visualize the RF coverage before the APs are installed on the floor or simulate coverage improvement by adding planned APs on floor maps.

Wireless Planning Summary

Test Case	Cisco	HPE Aruba	Juniper Mist
Survey Tool Integration	✓	✓	✓
	• Ekahau • Hamina Wireless	• Ekahau • Hamina Wireless	• Ekahau • iBwave • Hamina Wireless
Planned AP view	✓	✓	⊘
Wireless 3D Maps	✓ On-Prem only	⊘	⊘
Wireless Coverage Optimizer	✓ On-Prem only	⊘	⊘

Copyright ©2024 Miercom

5.2 Firmware Upgrade

Firmware upgrades for network devices are essential for maintaining network security, reliability, and efficiency. These upgrades require careful planning and execution during the downtime window. Management dashboards can aid in monitoring the upgrade process of the network devices. The additional features, such as firmware vulnerability check and image update status view, not only ease the network upgrade process but also offer more control and confidence.

Refer Appendix E.1 for details on the firmware upgrade capabilities of the management platform.

Firmware Upgrade Summary

Test Case	Cisco	HPE Aruba	Juniper Mist
Unified software view for all Network Devices Images (Wired, Wireless)	✓	✓	✓ • Separate Upgrade View • Upgrade per site
Trustworthiness Integration Display security advisories for images	✓ On-Prem Only	⊘ Check separately online	⊘ Check separately online
Image Compliance Status Display devices that are running outdated firmware	✓	✓	✓ Version compliance for APs not for Mist Edge.
Mark Golden Image Tag an image as golden and run compliance check on all devices	✓ On-Prem Only	⊘	⊘
Image Upgrade Pre and Post Check Validation	✓ On-Prem Only	⊘	⊘
Image Update Status	✓ On-Prem Only All stages status	✓ Logs available but no reason for update failure	✓ AP Live status percent but no reason for failure
AP Rolling Upgrade Minimize client downtime	✓	✓	⊘
Version Limit View For devices that does not support new firmware version or later	✓ On-Prem Only	⊘	⊘
Device Upgrade History with one-click Rollback option	✓ Cloud Only	✓ Manual Rollback	✓ Manual Rollback
Firmware Release Notes in Dashboard	✓ Cloud Only	✓ Outside of Dashboard	✓ Outside Dashboard

Cisco Catalyst Center and Meraki dashboard offer a unified view of all devices' image upgrades. Cisco Catalyst Center provides insights into the device upgrade process, which helps diagnose any device upgrade failure. Aruba also offers a unified view and an audit trail for image upgrade success or failure. However, it lacks granular insights offered by the Cisco Catalyst Center. Mist provides a separate view of firmware upgrades for different devices. Moreover, it lacks visibility into a device's upgrade process, limiting the image failure diagnosis function.

Copyright ©2024 Miercom

5.3 Compliance Audit

Network compliance is essential for maintaining the security and efficiency of network operations. Multiple automatic network audit types ensure the network runs with the desired settings, reducing vulnerabilities and potential network failures. Configuration drift feature tracks any in-band or out-of-band deviation from the intended configuration of the network device. Software image compliance helps track the devices running outdated or non-standard firmware images. Implementing PSIRT advisories addresses vulnerabilities swiftly. The network profile and network setting compliance track any violation from the intended network configuration and settings such as AAA server, DHCP server, WLAN configuration, etc. Addressing end-of-life devices prevents risks associated with outdated technology. Automated configurations promote consistency and reduce errors, although manual configuration is necessary for specific adjustments.

Compliance Audit for Wireless Controllers/Gateways and APs Summary

Compliance Audit	Cisco	HPE Aruba	Juniper Mist
Configuration Drift	✓ On-Prem Only	⊘	⊘
Software Image	✓	✓	✓
Security Advisories	✓ On-Prem Only	⊘	⊘
Network Settings	✓	✓	⊘
End of Life Check	✓ On-Prem Only	⊘	⊘

Copyright ©2024 Miercom

5.4 Technology Upgrade

Knowing if your wireless network is due for an upgrade is crucial in maintaining network quality. A dashboard that can provide insights into Wi-Fi 6/6E clients helps future-proof infrastructure for optimum network performance. Such a dashboard enables organizations to access comprehensive Wi-Fi 6/6E insights, including increased airtime efficiency, reduced latency, and better handling of high-density network environments. By monitoring Wi-Fi 6/6E stats, IT teams can evaluate current network utilization and performance, identify bottlenecks, and determine the impact of new devices and applications. Assessing network readiness through these dashboards allows organizations to make informed decisions about upgrades and to leverage the benefits of Wi-Fi 6 or Wi-Fi 6E technology.

Technology Upgrade Summary

	Cisco	HPE Aruba	Juniper Mist
Wi-Fi 6 / 6E Readiness Dashboard	✓ Cloud supports only Wi-Fi 6 view	⊘	⊘
Wi-Fi 6/6E Client Summary	✓	✓	✓
Wi-Fi 6/6E AP Summary	✓ On-Prem Only	✓ Basic	✓ Basic
Wi-Fi 6/6E Benefits View	✓ Cloud supports only Wi-Fi 6 view	⊘	⊘
Wi-Fi 6/6E Insights & recommendation	✓ Cloud supports only Wi-Fi 6 view	⊘	⊘

Copyright ©2024 Miercom

6.0 Artificial Intelligence Operations

Network assurance and AIOps ensure the reliability and performance of a network infrastructure. Traditional Network Monitoring Systems focus on device-related alerts, but complex modern networks require more. AIOps leverages AI and ML to enhance monitoring, troubleshooting, and optimization. These platforms gather and analyze vast amounts of data and offer tools to identify poor users experience, root cause issues and optimize network performance. Using an AIOps platform, organizations can streamline processes and optimize the use of IT resources.

6.1 AI-Driven RF Optimization

Radio Resource Management (RRM) automatically optimizes wireless network performance by dynamically assigning each AP to the best channel and power level, mitigating interference and congestion across 2.4, 5, or 6 GHz bands. Traditional RRM configurations are often complex, requiring precise adjustments, but AI-Driven RRM simplifies the process. It use machine learning to proactively optimize the network, provides RF performance scores, AI-recommended actions for improved RF health, and a comprehensive RF dashboard for intuitive analysis of network performance issues.

AI-Enhanced RRM is vital for optimizing wireless network performance and efficiency. An AI-driven workflow simplifies radio configurations. The Busy Hours feature automatically identifies peak hours and limits RRM changes during those times. The RRM performance view delivers a comprehensive summary and score, providing deep insights into network performance and highlighting areas for improvement. Actionable recommendations guide network administrators in making informed decisions to enhance connectivity and reduce interference. The ability to simulate RRM changes before implementation is a critical feature, allowing for impact assessment without risking network stability. Additionally, detailed channel and radar information assists in optimizing the allocations of frequencies and managing interference, especially in environments with high-density device usage.

Copyright ©2024 Miercom

AI-Driven RRM Summary

Test Case	Cisco	HPE Aruba	Juniper Mist
Configuration • AI-Profile creation workflow • Busy Hours	✓	✓ • AirMatch profile workflow • No busy hours	✓ • Profile workflow • No busy hours
RRM Performance View • Summary and score • Insights on score	✓ On-Prem Only • Summary with score • Drill down on low performance score	⊘ • No summary/score • Basic insights no drill down	✓ • Summary • Basic insights
Actionable Recommendations	✓ On-Prem Only	⊘	⊘
Simulate RRM changes before applying	✓ On-Prem Only	⊘	⊘
Channel and Radar Information	✓	✓ • No radar view	✓ • No radar view

Cisco Catalyst Center and Meraki's AI-Enhanced RRM provide a busy hour feature that intelligently identifies the most active hours of a network based on the traffic pattern and avoids any unnecessary RF changes during that period, helping sudden client disconnections. Cisco Catalyst Center provides a dedicated dashboard to visualize the RRM performance and a drill-down view to troubleshoot poor RRM performance. It further gives actionable insights for admins to quickly optimize the RF plan with an option to simulate the RF changes before applying them. Aruba offers a basic RRM view called AirMatch, with a view into radio distribution, TX channel, and power changes. Mist provides a dedicated radio management dashboard with a summary view that displays a few metrics on RRM performance. However, it lacks a path to optimize or troubleshoot poor RRM performance. Both Aruba and Mist lack features like the Busy Hours of Cisco.

Copyright ©2024 Miercom

6.2 Network Trends and Insights

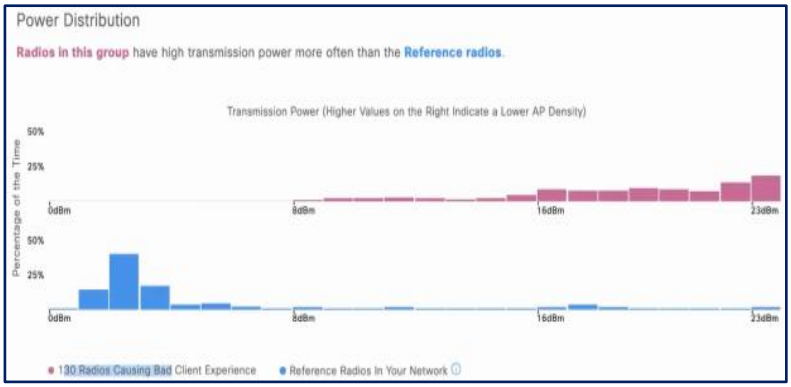
Analyzing data over time, ML algorithms identify patterns indicative of a deteriorating network allowing for intervention before they become disruptions. Long-term trend analysis predicts future network needs and plan upgrades, ensuring the network is capable of handling increased demands.

Cisco Catalyst Center

The Cisco Catalyst Center analyzes data spanning four weeks using AI, enabling it to group APs, assess impacts and root causes, spotlight underperforming APs, and enhance risk mitigation strategies.

In Trends and Insights, we explored AP Performance Advisories diving deeper into metrics of the APs that are causing poor client experience due to multiple RF related issues. One insight card was of Low AP Density showcasing AP radios impacting client experience.

The Power Distribution Chart visualizes the transmit power of problematic radios compared to that of reference radios that don't have any client experience problem. The dashboard catalogs APs with poor client experiences, detailing AP model, the impact, the number of clients affected, and the KPIs impacting client experience. A single click on the APs takes further root cause analysis of the problem.



The Radio Tx Power Distribution chart is color-coded to show radios causing a bad client experience.

HPE-Aruba

Aruba Central's AI Insights dashboard serves as the starting point for diagnosing RF related issues. Selecting an issue provides insights into underlying causes and offers recommendations for resolution. While it allows for the review of up to one month of historical data, mirroring the Catalyst Center's capacity, it falls short in delivering the same level of granularity and detail to the user.

Juniper Mist

In Mist, insights into AP issues are accessed through the Marvis Actions dashboard. It offers two RF related insights – Coverage Hole and Insufficient Capacity. Selecting an issue brings up a list of issues with affected sites, APs, issue date and so on. Clicking on the issue provides a floor map highlighting the primary APs involved. This level of troubleshooting in Juniper Mist stops short of providing the depth of information and context-based root cause analysis seen in the Catalyst Center.

Copyright ©2024 Miercom

6.3 Comparative Benchmarking

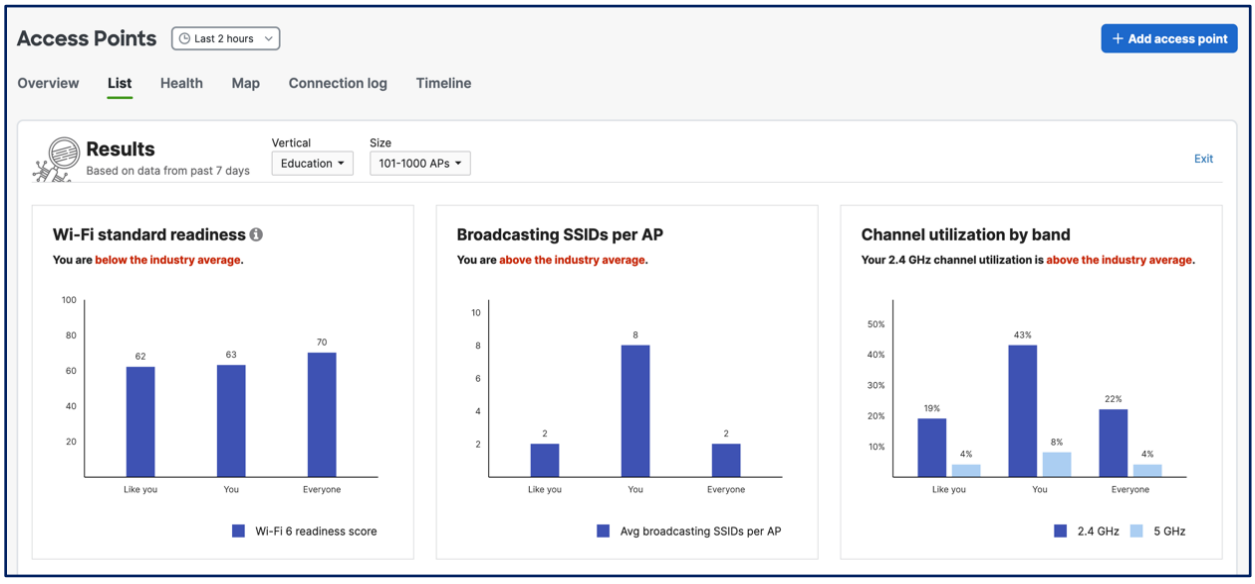
Comparative analytics enables organizations to benchmark performance against industry standards or historical data, revealing strengths and weaknesses. Comparing metrics across similar processes and time periods helps gain insights that drive strategic improvements and innovation. It provides a context for understanding data, making informed decisions, and optimizing operations.

Cisco Catalyst Center

Cisco Catalyst Center's benchmarking capabilities provides an on-demand network performance comparison with industry peers and within the organization. The Peer Comparison feature is based on thousands of similar sized and types of networks. Network Comparison drills down for performance metrics based on buildings, AP models, and endpoint types within the network. In our evaluation, we selected the Onboarding Error Source KPI in the Peer Comparison tab, highlighting the network's most common onboarding error and compared it with similar industry network error reports. The peer comparison offers a clear direction for targeted improvements in the network.

Cisco Meraki

Meraki's Network Like Yours introduces a wireless benchmarking tool that automatically identifies the selected network and compares it against similar vertical industry networks based on key design parameters. It allows in-depth exploration of each metric, offering custom recommendations to elevate the network's performance score. In our assessment, the tool provided insights across three KPIs- Wi-Fi 6 readiness, Broadcasting SSID per AP, and Channel Utilization. It also made suggestions for enhancing the network by giving pinpoint recommendations.



Observe that the Broadcasting SSID per AP highlights that the network had 8 SSIDs broadcasting per AP, which was much higher than similar networks, which had only 2. Clicking on the graph showed further impact details and recommendations to reduce the number of SSIDs.

Copyright ©2024 Miercom

HPE-Aruba

Aruba Central offers peer comparison within the troubleshooting workflow of the issues displayed in the AI Insights dashboard. Some problems, such as connectivity, provide a class baseline graph representing industry comparison, offering a benchmark against similar networks. Additionally, Aruba Central features a Company baseline, which compares all sites within the network, providing an internal performance benchmark. This functionality mirrors Cisco's benchmarking capabilities. Still, it is not on-demand and needs to be more comprehensive, limiting its utility in certain contexts.

Juniper Mist

Juniper Mist platform does not currently offer the capability for industry peer comparisons. However, it offers network site comparisons for SLE metrics through the Premium Analytics feature.

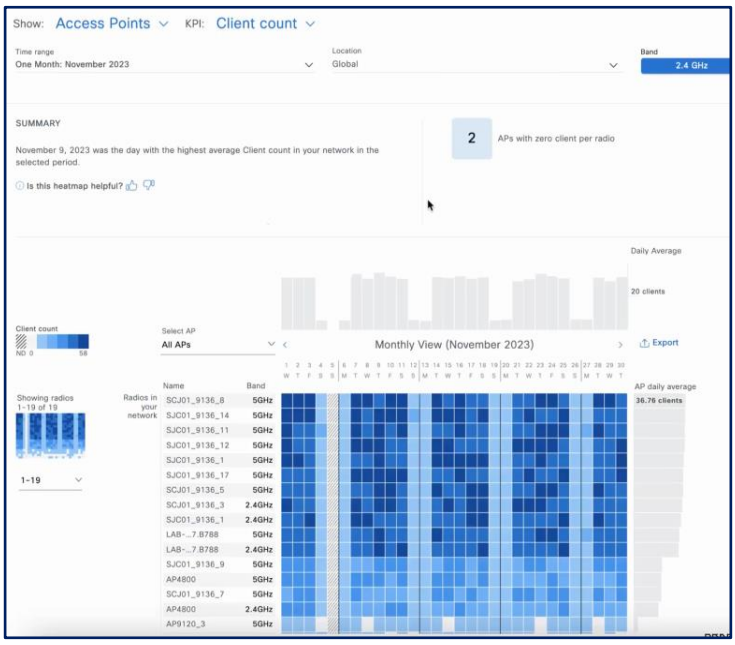
Copyright ©2024 Miercom

6.4 Access Points Comparison

The wireless network environment is constantly changing, and it is hard to keep track of the network performance over days and months. Network admins can benefit from long-term insights into the APs' behavior based on key performance indicators such as channel utilization, interference, radio resets, and many others. For example, Higher-Ed admins can observe the behavior of their APs in the current semester compared to the previous semester, enabling them to make informed decisions.

Cisco Catalyst Center

The Catalyst Center's Network Heatmap feature graphically depicts key network metrics, including signal strength, interference, and client distribution. Using color-coded mapping, network performance issues are quickly recognized. This feature is vital for network optimization as it allows network admins to swiftly pinpoint areas that require improvements. In our evaluation, we monitored the daily client count change on the APs for one month, providing insights into when some APs had many clients connected to them during certain days. This adaptability makes the network heatmap versatile in addressing a broad spectrum of customer needs through visualized data analysis.



The Network Heatmap provides a comparison of the network, insights and displays a month range of data up to a year.

HPE-Aruba

Aruba Central does not offer a similar feature to the Catalyst Center's Network Heatmap. Instead, we examined an RF Health report. However, it did not offer the same level of intuitive, at-a-glance insight as Cisco's heatmap solution.

Juniper Mist

Juniper Mist's Network Analytics dashboard allows customers to create reports, but it does not offer any comparison between APs. Juniper Mist's Premium Analytics offers long-term reports, including site comparison, but it lacks a dedicated view for AP KPIs found in the Catalyst Center's Network Heatmap. This difference underscores a gap in the ease with which network administrators can visually assess and address network performance issues.

Copyright ©2024 Miercom

6.5 Application Performance Monitoring

6.5.1 Wireless Application Visibility

Effective application traffic management begins with accurately identifying and categorizing all operational applications within a network as per their relevance to the business. Visibility into applications and their usage plays a crucial role in improving security and network capacity planning. Without a deep packet inspection-based application identification, the control and prioritization of mission critical traffic streams would be limited.

Refer to Appendix F.1 for test methodology.

Wireless Application Visibility Test Results

Applications Category **Evaluation:** Number of applications identified on the dashboard (shown in percentage)	**Cisco**	**HPE Aruba**	**Juniper Mist**
Collaboration Facetime, Webex, MS-Teams, Slack	100%	100%	50%
File Sharing Box, One Drive, Office 365, Google Drive	100%	75%	50%
Infrastructure Amazon Services, GCP, Salesforce, Azure	100%	100%	25%
Video Streaming Netflix, Amazon Prime	100%	100%	100%
Social Networking Facebook, Instagram, LinkedIn, TikTok, Reddit	80%	80%	60%
Gaming and Music Xbox Live Web, Discord, PS App, Apple Music, Spotify	100%	60%	20%
Websites ESPN, BBC, Wikipedia, GitHub, Adobe, CNN	100%	100%	0%

Cisco demonstrated exceptional proficiency in identifying and classifying applications across various categories. Cisco's deep packet inspection-based signature detection accurately detected nearly all applications and provided granular reporting. For instance, Cisco's analysis of MS Teams was comprehensive, distinguishing between MS Teams-Audio, MS Teams-Video, and MS Teams-Sharing. Aruba application identification was second best, as it nearly identified all applications but struggled in the gaming and music application category. Mist underperformed significantly, failing to recognize most applications and displaying them in the "Unknown" category.

Copyright ©2024 Miercom

6.5.2 Wireless Application Assurance

Following identification, assessing user experience becomes crucial, examining whether users are satisfied with application performance, including critical metrics like jitter, packet loss, and throughput. Application experience troubleshooting can be further enhanced by integrating the management solution with the application provider. For example, integration with Webex provides details of a poor Webex call session from the server side. It helps network administrators isolate the segment in the application path that may be causing application issues.

Wireless Application Assurance Summary

Wireless Application Assurance	Cisco	HPE Aruba	Juniper Mist
Flow based Telemetry	✓ On-Prem Only NetFlow	⊘	⊘
Application Experience Latency, Packet Loss, Jitter	✓ On-Prem Only	✓ Offers basic app experience for collaboration apps	✓ App Experience only for Zoom and MS Teams
Application Integration	✓ On-Prem Only MS Teams and Webex	⊘	✓ MS Teams and Zoom

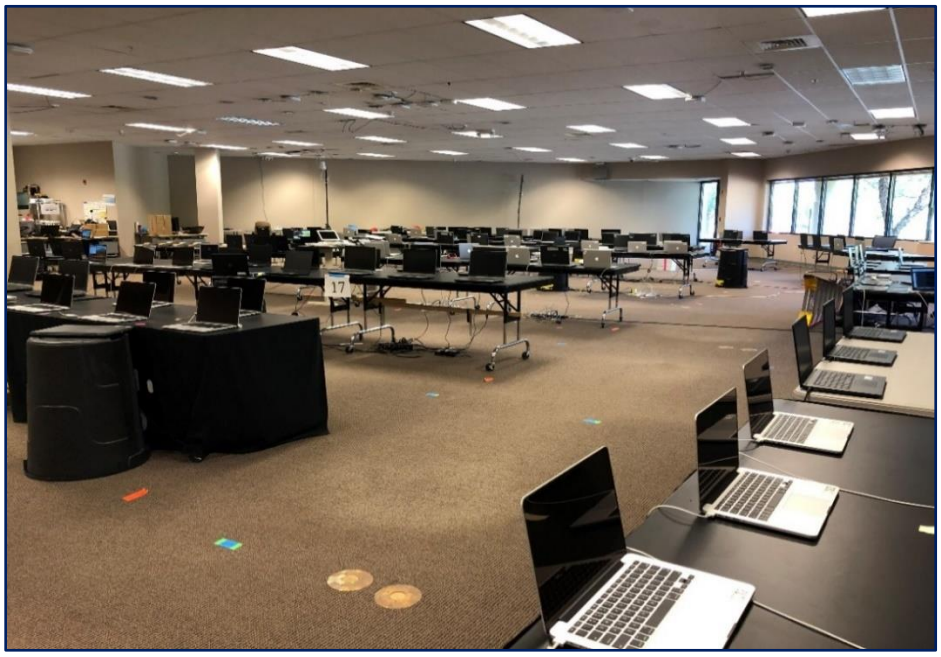
Cisco Catalyst Center provides qualitative metrics for applications through NetFlow support in the Cisco Catalyst 9800 controller. It also integrates with Webex and MS Teams to accelerate troubleshooting into poor application experience. Aruba Central lacks an application experience view. Instead, it offers a UCC dashboard, which provides visibility into the call quality of collaboration applications. However, it does not offer detailed qualitative metrics like latency, jitter, and packet loss. Mist only provides application experience, through application integration, for MS Teams and Zoom. It gets call metrics from the application server side but lacks information from the network end.

Copyright ©2024 Miercom

Appendix A: Report Evaluation Criteria

Test Bed Overview

Using hands-on testing in a live business environment, we challenged each device with real-world scenarios to determine performance, automation, assurance, and remote worker capabilities.



Source: Cisco

A view of the test setup is shown above. The AP under test was ceiling mounted and clients were spread around the AP from 10ft. (3m) to 45ft. (13.7m).

Test Tools

The following tools are a representative list of tools used to carry out analysis:

Ixia IxChariot

IxChariot network tool quantifies and compares wireless AP performance. This tool can support multiple platforms and test automation to simulate real-world applications for device and system performance under specific load conditions. IxChariot can produce and transfer traffic between wireless endpoints in set packet sizes for statistical reporting. The IxChariot endpoint application is installed on each mobile client, and tests are configured via the management console's WebUI to enable the client devices to receive and transmit traffic.

Firmware Version		
Cisco	**HPE Aruba**	**Juniper Mist**
17.13.1	10.5.0.1_88128	0.14.29132

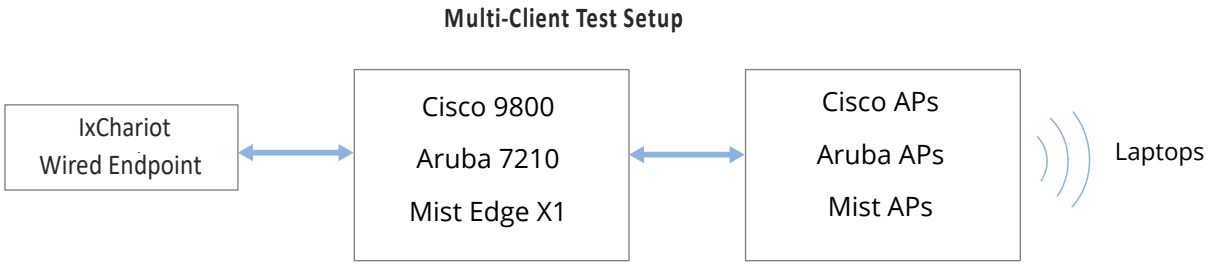
Copyright ©2024 Miercom

Appendix B: Performance Test Setup

This test compared Wireless AP performance from different with similar radio capabilities – with 802.11ax, OFDMA, MU-MIMO and Application Visibility enabled. The clients used in different test cases were 40 Wi-Fi 6 laptops with Intel AX200 2x2 chipsets, 20 Wi-Fi 6E laptops, with Intel AX210 2x2 chipsets and 20 Wi-Fi 5 MacBook Pro 3x3 laptops. Depending on the use cases, a real-world representative mixture of wireless client devices was connected to the AP under test, set to operate on 6 GHz- Channel 1 in 160 MHz, 5GHz- Channel 36 in 80-MHz and 2.4 GHz- Channel 1 in 20-MHz.

The Ixia IxChariot test system was configured to deliver UDP, RTP and TCP downstream traffic from wired endpoints with an ethernet link through the AP to the wireless client devices.

In the testing setup, the APs were connected to Cisco 9300 switch with 5-gigabit uplink ports. The APs were configured to tunnel the traffic to the centralized controller of the vendor. Up to five wired endpoints were used to generate traffic to run the performance tests.



B.1: Multi-Gigabit Throughput Performance

How we did it?

We performed two tests- In the first test, we ran the UDP script on 5 Intel 11ax clients (1 client on 6 GHz, 2 clients on 5 GHz and 2 clients on 2.4 GHz) and then on 33 Intel 11ax clients (15 clients on 6 GHz, 15 on 5 GHz, and 3 on 2.4 GHz). The test was conducted with 33 clients to check the performance at scale. Afterward, we repeated the same process using the RTP script for the second test. For the test we used bridge mode or FlexConnect mode to achieve maximum throughput.

B.2: Multi-Client Throughput Performance

How we did it?

We used the TCP High-Performance script for the multi-client test with downstream traffic originating from the wired Windows laptops toward 80 wireless clients. The test was performed on 10, 20, 30, 40, 50, 60, 70, and 80 clients.

Copyright ©2024 Miercom

Appendix C: Sustainability

How we did it?

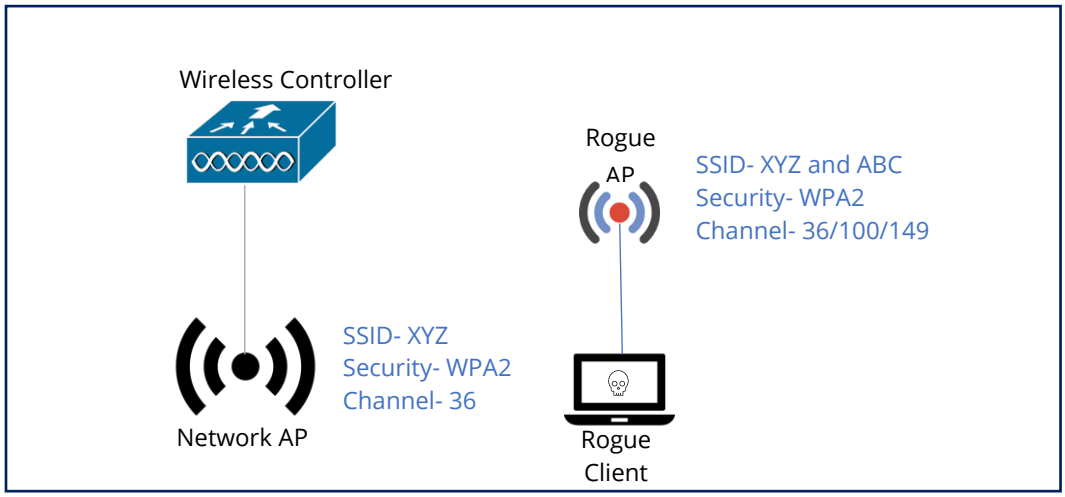
To evaluate the access points' power efficiency, we observed each AP's operating power consumption during the 80-client performance test see section B.2 above. We calculated the power efficiency in Mbps/watt by dividing the AP throughput by the power consumed on the switch port using the “show power inline policy” command.

Appendix D: Wireless Security

D.1: Rogue AP Detection and Containment

How we did it?

As part of our testing process, we configured a Netgear Wireless Router to function as a Rogue AP. This rogue AP was set to broadcast alongside several network APs, including the Cisco 9166, Aruba AP655, and Mist AP45. We conducted tests across channels 36, 100, and 149 to assess the APs’ efficacy in detecting rogues across the 5 GHz spectrum. Our testing scenarios included rogue AP broadcasting identical SSID as the network APs and a different SSID.



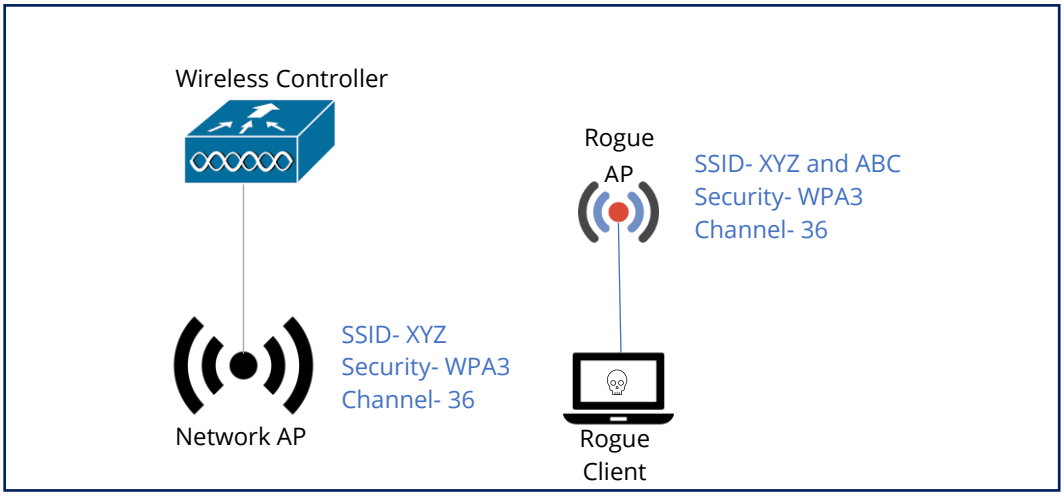
The evaluation criteria for the wireless security platform Cisco Catalyst Center, Cisco Meraki, Juniper Mist, and Aruba Central included the following:

1) The accuracy to detect the rogue access point.
2) The time taken to detect the rogue access point.
3) The time taken to contain the rogue access point on channels 36 and 149.

D.2: Rogue AP with PMF Enabled: Detection and Containment

How we did it?

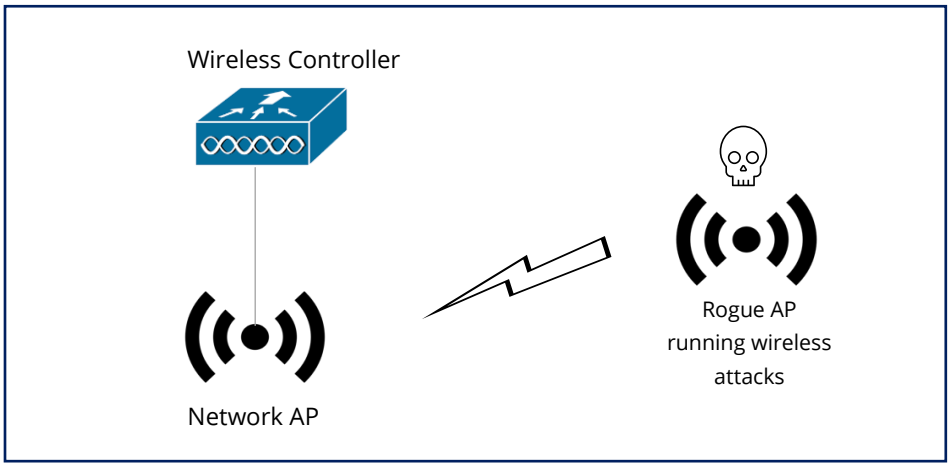
This test assesses the network's ability to detect, contain and report PMF-enabled rogue AP. Our testing scenarios included rogue AP broadcasting identical WPA3 SSID as the network APs and a different WPA3 SSID.



D.3: WIPS Testing

How we did it?

We used an AP with automated scripts running, sending 13 types of over-the-air attacks. Each test script was run individually for a certain period. The criteria for a successful test were to observe the accuracy and time taken by the respective management platform to report the wireless attack signatures.



Appendix E: Network Operations

E.1: Firmware Upgrade

Cisco Catalyst Center

The Cisco Catalyst Center's Image Repository provides a unified view of all software images across network devices. The process of upgrading a wireless controller is seamlessly linked to the concurrent update of associated APs.

Upon selecting the Cisco Catalyst 9800-40 Wireless Controller for analysis, we were shown a list of software images available for download. A golden tag can be assigned to the image to set it as a reference point based on its release date or stability. The Inventory page of the Catalyst Center aids in identifying non-compliant images within the wireless controller inventory, particularly if a device has not been updated to the latest golden image. This feature proves invaluable in multi-controller environments by simplifying the identification and prioritization of devices requiring updates.

Our analysis focused on the software image update process for a wireless controller, using a workflow within the Catalyst Center. A Readiness report automatically assesses and confirms the device's preparedness for the upgrade. The distribute phase allocates the image to the controller, with options to incorporate additional custom checks to ensure the device's readiness. The activate phase initiates the deployment of the image and additional pre- and post-checks for software activation. The process allows for scheduling the distribution and activation phases, enhancing operational flexibility. A summary overview details the devices and images involved in the upgrade.

One attribute of this workflow is its diagnostic capability, particularly its ability to pinpoint failure points during the upgrade process. This feature can be indispensable for maintaining network integrity, both wired and wireless, by enabling precise troubleshooting and corrective measures in complex network environments.

Cisco Meraki

The Cisco Meraki platform offers a unified approach to software image upgrades with Firmware Upgrade dashboard for all Meraki products. It highlights recent firmware changes, as well as rollback capabilities if a new firmware version introduce operational challenges. Additionally, the dashboard presents version limits, detailing support of latest firmware versions for specific devices. It also shows the devices' firmware statuses based on the latest images available. This insight is invaluable for determining which network devices require updates.

Our evaluation within a test environment focused on the firmware upgrade of the APs through the Cisco Meraki dashboard. Initially, the firmware version for the upgrade is selected. Then, users define their upgrade strategy: executing a simultaneous upgrade across all APs – suitable for off-peak hours to mitigate network downtime – or opting for a staggered approach to minimize operational disruptions during peak times. Following this, the upgrade is scheduled for a specific date and time.

Copyright ©2024 Miercom

This culminates with a summary and final confirmation step, with the actual upgrade commencing five minutes post-confirmation. This is provided if required. Through this approach, firmware upgrades are conducted with minimal impact on network performance and user experience.

HPE Aruba

HPE-Aruba, like Cisco Meraki, has integrated a user-centric approach towards firmware management with its dedicated firmware page. The platform lists all network devices, their current firmware versions alongside recommended versions. This design allows users to assess the compliance of their devices' firmware but also to schedule upgrades to minimize interruptions.

When an AP is selected from this interface, the Upgrade Access Point Firmware workflow is activated. The firmware version is selected along with the time for upgrade. Options include immediate or delayed implementation. An additional feature is an audit trail, tracking the progress of the firmware upgrade. It does not have the ability to diagnose the cause of an unsuccessful upgrade.

Juniper Mist

In contrast to Cisco's centralized approach for firmware management, Juniper Mist adopts a more decentralized strategy, users must navigate to each site in their network to initiate firmware upgrades for APs. Despite this, upon the creation or addition of a new site, Juniper Mist activates automatic firmware updates, mirroring Cisco Meraki's method of ensuring devices remain updated with minimal user intervention. Juniper Mist incorporates a version customization feature, akin to Cisco's family of images concept, allowing for tailored firmware version upgrades for each AP.

For manual upgrades, the process involves selecting the relevant site, choosing the APs for the upgrade, and finally click the Upgrade APs button. Prior to the initiation of the upgrade, users are prompted to select the firmware version to deploy. A notable limitation of the Juniper Mist system is its absence of a rolling upgrade feature. This means that all selected APs undergo the upgrade process simultaneously, requiring the scheduling of such activities during off-peak hours to avoid substantial disruptions to network operations.

Copyright ©2024 Miercom

Appendix F: Artificial Intelligence Operations

F.1: Wireless Application Visibility

How we did it?

We tested a total of number of 32 applications within different categories of application types. We evaluated each platform’s application detection capabilities by running different types of application traffic using phone apps and web browser for a certain period. Then, we observed each vendor's application dashboard individually to ensure correct application identification.

Copyright ©2024 Miercom

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.

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 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.

Miercom's Fair Test Policy allows for any vendor evaluated to challenge or retest these results in accordance with Miercom Terms of Use Agreement if there are any disagreements in our findings presented here.

Miercom did not acquire products for this review, nor has Miercom agreed to any vendor's End User License Agreement (EULA) or any other overly restrictive agreements that limit free press, product evaluations, editorial works, or publishing product reviews. We believe in providing accurate objective information to assist customers make informed purchasing decisions.

By downloading, circulating, or using 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.

© 2024 Miercom. All Rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. Please email reviews@miercom.com for additional information.