



SR250513B
August 2025

Licensed for Distribution by:

Kandji

macOS EDR Competitive Assessment Summary Report

miercom.com/kandji

Table of Contents

1.0 Executive Summary	3
2.0 EDR Test Summary.....	7
3.0 About Kandji EDR	9
4.0 Test Evaluation	11
4.1 Malware Detection	11
4.2 Response and Remediation	18
4.3 Alerting & Reporting	19
4.4 Real Time and Historical Analysis	20
4.5 Resource Consumption.....	21
4.6 Multi-Platform Support	23
4.7 Vendor Technical Support (Post Onboarding)	24
4.8 Onboarding Experience	25
4.9 Total Cost of Ownership	26
4.10 Evasion / Disabling EDR Technique	27
4.11 Blacklist and Whitelist Enforcement Functionality	28
4.12 Sample Submission	29
4.13 MITRE ATT&CK Simulations	30
4.14 Security Management Systems Integration.....	32
4.15 MDM (Mobile Device Management) Features and Capabilities	33
5.0 About Miercom	34
6.0 Use of This Report	34

1.0 Executive Summary

In today's enterprise environments, the absence of a modern Endpoint Detection and Response (EDR) solution often leaves organizations vulnerable to hidden and persistent threats. Traditional antivirus tools and basic device management systems typically rely on known malware signatures, offering little insight into unusual or emerging attack patterns. Without EDR, businesses are unable to detect breaches until damage has been done, leading to extended incident response cycles and increased risk exposure.

EDR solutions address this gap by continuously monitoring endpoint behavior, collecting detailed activity logs, and enabling automated containment of suspicious processes. Rather than waiting for alerts triggered by known threats, EDR observes how software behaves, allowing security teams to detect anomalies and block emerging threats during execution. This proactive visibility significantly improves response times, reduces breach impact, and streamlines investigation efforts, shifting enterprise security from a reactive stance to a more resilient posture.

Kandji EDR brings this capability into macOS environments in a way that emphasizes simplicity and native integration. It taps into Apple's built-in Endpoint Security framework to monitor low-level system events without adding heavy overhead. As a result, Kandji can detect malicious behavior early—before threats can spread or conceal themselves—and automatically quarantine and abort problematic activity. Its detection rules are rooted in ongoing forensic research and global telemetry, enabling rapid updates in response to newly discovered threats or attack techniques. By embedding these capabilities within the existing Kandji device management platform, companies deploy one agent that serves both management and protection purposes, streamlining both onboarding and ongoing operations.

As enterprises move to manage larger and more diverse fleets of devices, the need for comprehensive endpoint protection becomes increasingly urgent. EDR fills a critical blind spot left by legacy tools. Kandji EDR, with its tight macOS integration, native platform leverage, and unified deployment model, offers a streamlined and effective solution. It provides organizations with the visibility, speed, and operational simplicity necessary to detect and respond to threats before they escalate.

Kandji engaged Miercom to conduct an evaluation of Kandji EDR as compared to competitive offerings. This report provides a detailed evaluation of Kandji EDR alongside other leading EDR solutions. It focuses on how each tool approaches threat detection, response capabilities, deployment models, and operational fit in enterprise settings. The goal is to offer a clear basis for comparison to help organizations select a solution that aligns with their specific technical and operational requirements.

Key Strengths

- **Highest malware detection efficacy for all products in this class for macOS**
A 98.4% malware detection efficacy including Zero Day threats. Initial block, file interaction and behavioral detection all contribute to this accomplishment.
- **Strong behavioral detection** Kandji EDR proved in hands on testing to stop “detonated” malware that other leading vendors could not detect. Behavioral detection contributed to an 89.5% detection capability. This is a critical capability as threats are always evolving, many are likely not added to signature based detection lists initially.
- **Successfully detected multiple Behavioral Attack techniques**, including:
 - Reverse shell execution
 - File download
 - Hidden file creation
 - LaunchAgent persistence
 - Privilege escalation
 - Permission change to executable
- **Supports automatic quarantine** of files and processes seamlessly without a complicated configuration settings. Protected users and administrators are advised of the activity.
- **Alerts clearly presented in a “Threats Dashboard”** with all pertinent details including threat name, file path, process, user, and timestamp; Also supports Slack and email notifications and more.
- **Offers a REST API and Amazon S3 Activity Log Integration** for automatic export of activity logs, enabling SIEM integration for monitoring, analysis, and compliance.
- **90-day threat history retention**, with filtering by detection type and threat status.
- **Lightweight agent**, consuming 0.6% CPU and 25.4 MB RAM during scans, 0% CPU idle, ensuring minimal performance impact. Kandji performed overall best in the testing comparison for resource consumption, especially heavy utilization tests compared to other vendors in the study. Kandji’s unique approach to selective initial block based on signature hash, followed with behavior blocking or malicious samples are interacted / activated provides a competitive edge on resource consumption.
- **Built on a tight integration** between MDM and EDR.

- **Onboarding is streamlined**, with low friction agent deployment, MDM-based tamper protection, and comprehensive documentation.
- **Offers 24/5 support** via live chat and email: no phone support.
- **Accessible support portal** and knowledge base cover macOS security, integrations, and troubleshooting in depth.

Kandji is recognized as a leading vendor in the Miercom Endpoint Detection and Response Platform Assessment, outperforming competitive products in a comprehensive evaluation focusing on Endpoint Detection and Response. *Kandji EDR for macOS achieved a malware detection efficacy of 98.4% including thwarting zero-day exploits. Kandji EDR achieved the highest efficacy score for all macOS EDR solutions known in the market and tested to date.*



Kandji's overall malware efficacy and Endpoint Detection and Response capabilities shows their commitment to providing a superior Endpoint Detection and Response platform and has earned the **Miercom Certified Secure** award.

Robert Smithers
CEO, Miercom

2.0 EDR Test Summary

Complete details can be found in section 4.0 Test Evaluation.

Kandji EDR vs Industry Average Endpoint Detection and Response Platform Assessment Summary			
Evaluation Criteria		Kandji	Industry Average
4.1	Malware Detection Efficacy: Best overall malware detection for macOS was observed with Kandji. Of the detected malware, 80.8% was caught during the interaction-stage, 8.9% caught via initial analysis, and 8.6% post-execution. The low miss rate of 1.6% is the best in the group. While the solution lacks strong static detection, its behavioral engine is effective at identifying threats during system-level changes. This approach introduces slight latency in threat identification but offers broader protection against unknown or polymorphic malware.		
4.2	Response and Remediation: Automatically quarantines malicious files and processes but does not have full device isolation. Admins can initiate device lock or wipe on compromise.		
4.3	Alerting and Reporting: Alerts are shown in a Threats dashboard with threat name, user, file, process, and timestamp. Supports email and Slack notifications. Lacks a process tree or timeline but provides sufficient investigation context.		
4.4	Real Time and Historical Analysis: Threats are organized as File or Behavioral, with filtering by type and status. History is retained for 90 days to support retrospective analysis.		
4.5	Resource Consumption: Low system impact: 0% CPU idle / 0.6% CPU active; memory usage ranged from 24.5 MB to 25.4 MB during scans.		
4.6	Multi-Platform Support: No, platform support is limited to macOS.		
4.7	Vendor Technical Support Post Onboarding: Provides 24/5 live chat and email support via web portal. Phone support is not available. Provides a well-documented knowledge base includes setup, integration, and troubleshooting.		
4.8	Onboarding: Streamlined deployment with clear documentation and minimal user permissions required. Agent install is fast and low-friction.		
4.9	Total Cost of Ownership: Kandji offers a streamlined, integrated MDM and EDR solution priced at \$168 per device annually (\$96 MDM + \$72 EDR, consistent whether bundled or separate). While its EDR cost is slightly below the macOS industry average of \$75, Kandji delivers added value through simplified deployment, included training and support, and reduced need for additional IT resources—resulting in overall operational cost efficiency.		

4.10	<u>Evasion / Disabling EDR Technique:</u> Uses MDM-based controls to prevent uninstall on supervised devices. The agent cannot be terminated locally through standard means and includes basic protections against removal or tampering via LaunchDaemons and file system controls. Also includes automatic installs and turns itself back on if disabled or removed.			
4.11	<u>Blacklist and Whitelist:</u> Lacks support for IP, domain, or URL blocking; only hashes of known malicious files and the path to the known malicious files are available.			
4.12	<u>Sample Submission:</u> Threat samples can be submitted to support. Blocking rules are tracked internally.			
4.13	<u>MITRE ATT&CK Simulations:</u> - Reverse shell (perl) - Persistence via LaunchAgent - File download (curl) - Privilege escalation (sudo) - Hidden file (SetFile) - Permission change (chmod +x) - Keylogging (log stream) - Name Masquerading (osascript)			
4.14	<u>Security Management Systems Integration:</u> Offers a REST API and Amazon S3 Activity Log Integration for automatic export of activity logs, enabling SIEM integration for monitoring, analysis, and compliance.			
4.15	<u>MDM Capabilities:</u> Tightly integrates EDR and MDM for macOS. Includes automated deployment, compliance templates, third-party patching, and remediation. Supports DDM and tools like Passport, making it ideal for Apple-focused organizations needing low-touch, scalable device management with built-in security controls.			
OVERALL RATING				
SCORE		3.3	2.9	
Key				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail
4.0 – 3.5	3.49 – 2.5	2.49 – 1.50	1.49 – .50	0.49 - 0

3.0 About Kandji EDR

Kandji EDR is a threat detection and response tool built specifically for macOS, delivered as an addition to the Kandji device management platform. It operates through a lightweight local agent that works alongside Kandji's existing web-based management interface.

The agent leverages Apple's Endpoint Security framework to monitor system events, including file operations, process execution, and interactions with external storage. By capturing these events in real time, the solution identifies suspicious activity and flags it for administrator review.

Detection is handled in two modes:

- Detect Mode: Logs and alerts on potential threats.
- Protect Mode: Escalates response by isolating threats—quarantining files and terminating processes—when configured.

Threats are classified as malware, potentially unwanted programs (PUPs), malicious behavior, or suspicious behavior—with each detection generating a structured event record. These records include details such as file paths, process metadata, hashes, and device impact status.

Administrators interact with threat data through Kandji's web console. They can view aggregated threat events, inspect per-device activity, apply allow/block rules based on file hash or path, and export event data via CSV or API.

Central to Kandji's approach is integration with its macOS management toolkit. EDR is deployed alongside existing management workflows—Blueprints and Assignment Maps—allowing a single agent to handle both device configuration and security detection.

Kandji's security team continuously refines detection capabilities based on internal telemetry and research. Recent updates have extended behavioral monitoring to include real-time identification of actions such as suspicious SSH usage, abnormal process spawning, and attempts to download from known threat sources. In Protect mode, confirmed malicious behavior triggers immediate quarantine and process termination. Kandji publishes research findings and novel threat intelligence to share insights into emerging macOS threats.

Kandji EDR offers macOS-focused threat detection through a unified, event-based monitoring system, configurable response modes, and integration within an existing Apple device management framework—enabling administrators to observe, evaluate, and act on endpoint threats within familiar workflows.

Products Tested

Vendor	Product Name	Version
Kandji	Kandji Endpoint Detection & Response (EDR) for Mac	4.6.21 (5300)

4.0 Test Evaluation

4.1 Malware Detection

Description: This test measures how well EDR solutions detect macOS-based malware across realistic scenarios covering both static and dynamic attack stages. Scenarios include:

- Known Malware at Rest: Detection of inactive, known threats via signature scanning.
- Evasive and Unknown Malware: Identification of modified or zero-day samples.
- File Write Detection: Response to malware written to disk or memory.
- Execution Permission Changes: Detection of files made executable.

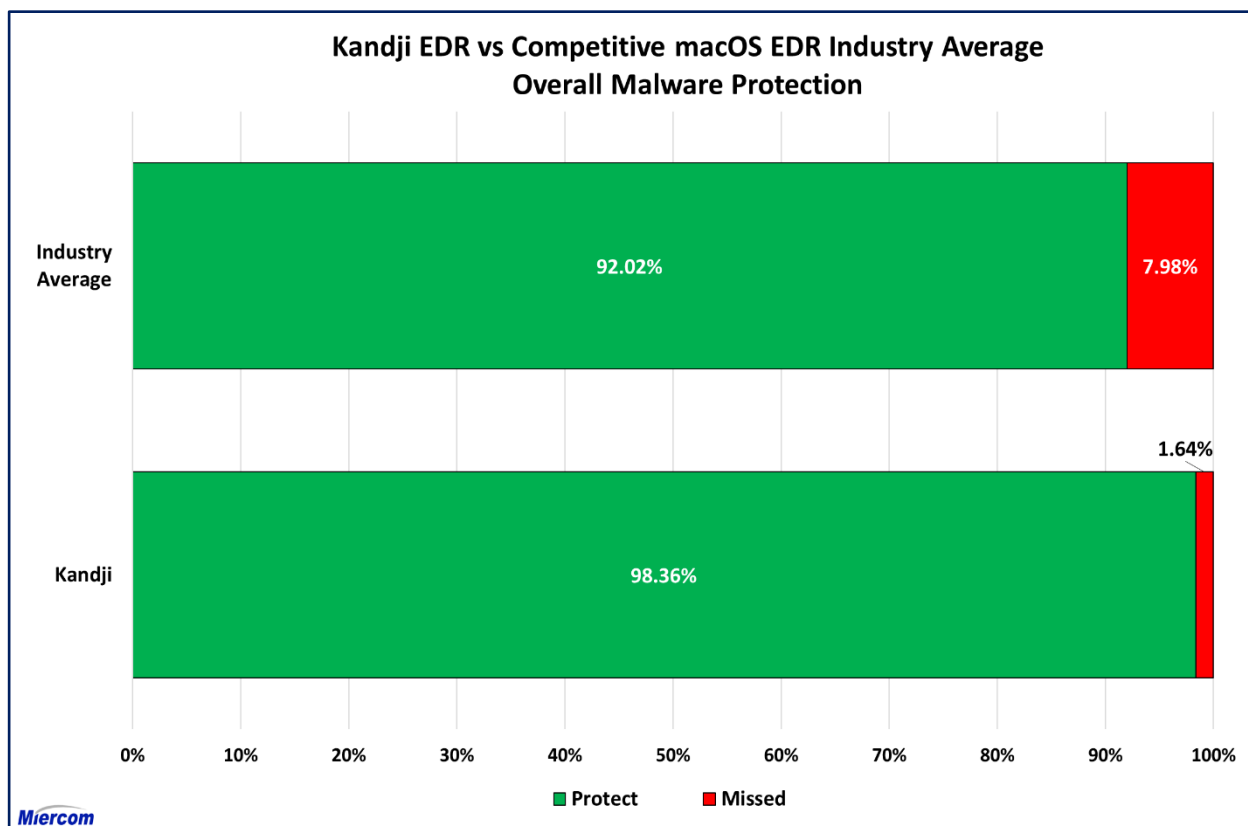
These cases reflect key points in the attack chain and reveal each product's baseline detection capabilities.

Detonation Behavior and macOS Malware Testing

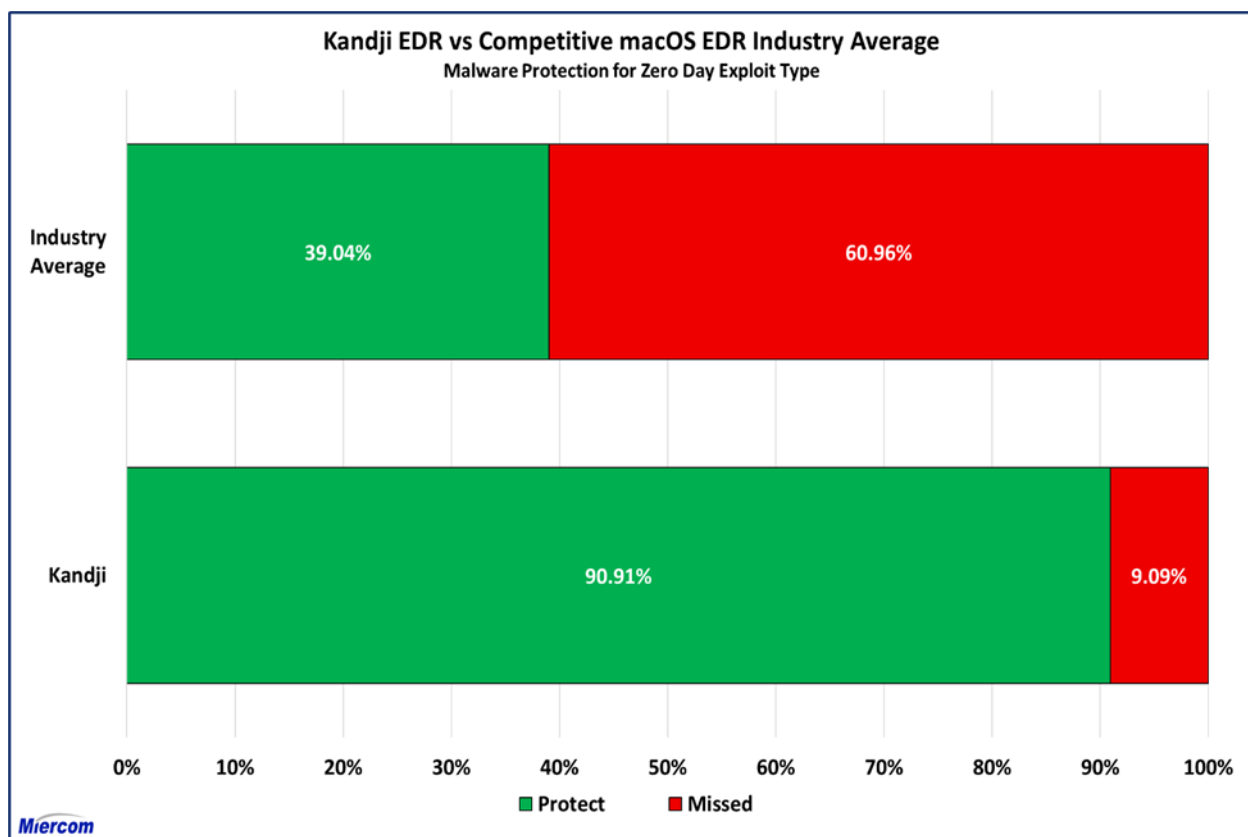
Standard detonation procedures used in testing included:

- Executed macOS binary files e.g., .exec, Mach-O via Terminal using `chmod +x` and `./filename.`
- Executed binaries via Terminal using the command `file ./filename.`
- Ran Python scripts with `python3 ./filename.py` after identifying them with the file command.
- Detonated PHP-based malware after installing PHP and using `php ./filename.php.`
- Executed scripts that attempted outbound connections simulating C2 callback behavior.
- Inspected files with `head ./filename` to verify embedded shell commands prior to execution.
- Fixed Windows-formatted line endings CRLF and executed script-based payloads.
- Deployed and launched QCOW image files containing auto-executing malware.
- Decoded and manually executed base64-encoded or obfuscated payloads embedded in script files.
- Used file command to determine appropriate interpreter e.g., Python, PHP, shell.
- Extracted and ran payloads from compressed packages e.g., .zip, .pkg that triggered post-extraction or post-install activity.
- Observed persistence and post-execution behavior to verify whether samples deleted themselves or remained on disk.

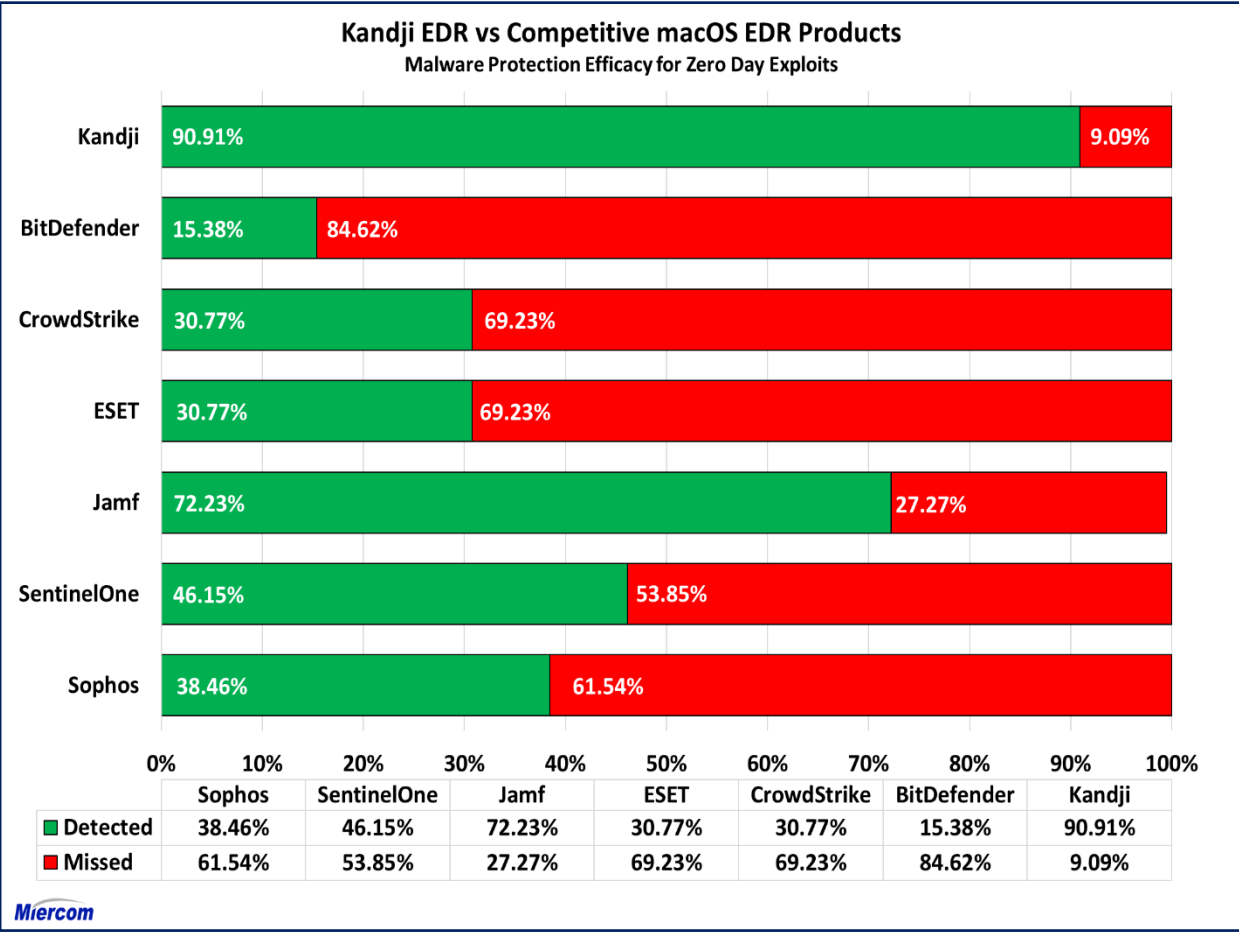
These detonation methods were designed to simulate realistic user interactions and attacker techniques, ensuring the EDR's behavioral and post-execution detection capabilities were adequately tested.



This chart above compares Kandji's malware detection efficacy against the industry average of competitive macOS EDR products evaluated and scored. The overall "Protect" score includes initial signature blocking, file interaction blocking and malicious payload detonation detection. Kandji successfully detected 98.36% of threats, outperforming the industry average of 92.02%. Only 1.64% of threats were missed by Kandji, compared to an average miss detection rate of 7.98% of competing macOS EDR solutions. These results reflect Kandji's strong performance in behavioral threat detection across various macOS exploit stages.



This chart above compares Kandji's Zero Day malware detection efficacy against the industry average of competitive macOS EDR products evaluated and scored. The overall "Protect" score includes initial signature blocking, file interaction blocking and malicious payload detonation detection. Kandji successfully detected 90.91% of Zero Day threats, significantly outperforming the industry average of 39.04%. Only 9.09% of Zero Day threats were missed by Kandji, compared to an average miss detection rate of 60.96% of competing macOS EDR solutions.



This chart compares the zero-day malware detection efficacy of industry leading EDR solutions. Kandji stands out with a 90.91% detection rate, outperforming other solutions like BitDefender 15.38%, CrowdStrike 30.77%, ESET 30.77%, and Sophos 38.46%. While Jamf comes closest at 72.23% detection, no other product approaches Kandji's high level of zero-day malware protection.

Observation:

Malware Efficacy				
	Kandji – Detection primarily occurred during the interaction-stage 80.84%, with 8.88% caught via initial analysis and 8.64% post-execution. The low miss rate 1.64% is the best in the group. While the solution lacks strong static detection, its behavioral engine effectively identifies threats during system-level changes. This introduces slight latency in threat identification but offers broader protection against unknown or polymorphic malware. For zero-day threats, Kandji achieved a detection rate of 90.91%. Notably absent, was a full device scan option.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

Miercom macOS Malware Sample Definitions

Standard
macOS.AdLoad Adware that maintains persistence using launch agents and configuration profiles. It injects ads, hijacks web traffic, and alters system settings. Often considered low-risk, it can download and execute additional payloads, like spyware and credential-stealing tools.
macOS.BirdMiner macOS-based cryptocurrency miner that operates in the background without user awareness. Distributed via trojanized software, BirdMiner leverages system resources to mine Monero, resulting in degraded performance and potential hardware strain.
macOS.Calisto This Trojan is classified as an infostealer. It targets macOS keychains, browser data, and system files, with a primary focus on extracting sensitive information. Although now considered a legacy threat, Calisto is notable for its role as a prototype for more advanced macOS malware families.
macOS.CoinTicker A threat that installs legitimate cryptocurrency trading applications bundled with hidden backdoors. Once deployed, CoinTicker enables remote access to infected systems and facilitates the theft of user credentials and cryptocurrency-related data.
macOS.Coldroot A remote access trojan (RAT) that provides persistent access to macOS systems. Features include keystroke logging, screen capture and arbitrary command execution. Coldroot is delivered through deceptive installers and targets multiple macOS versions.
macOS.Cookieminer Credential-stealing malware that focuses on extracting browser cookies, SSH credentials, cryptocurrency wallet keys, and active session data. It achieves persistence through launch agents and is often associated with broader data exfiltration campaigns.
macOS.XLoader Information-stealing malware from the Formbook family, it collects browser data, captures keystrokes, and takes screenshots. It is used to harvest credentials and exfiltrate sensitive data. Persistence is achieved using simple mechanisms, allowing it to remain active on infected systems with minimal user awareness.
Advanced Threats
macOS.AppleJeus Malware associated with state-sponsored activity, distributed through cryptocurrency trading applications that appear legitimate. Once installed, the malware delivers remote access trojans (RATs) that enable persistent system access, data collection, and network movement. It is commonly linked to financially motivated and espionage-driven operations.

macOS.Convuster
Used in targeted campaigns, it achieves long-term persistence on macOS systems through launch agents and script-based payloads. Primarily employed for surveillance, data collection and as a staging mechanism for additional malware in espionage contexts.
macOS.KeRanger
Distributed through compromised software, KeRanger encrypts files and issues ransom demands in cryptocurrency. It maintains persistence using LaunchDaemons and periodically connects to command-and-control (C2) servers to receive further instructions, such as updated encryption keys or tasking.
macOS.Macma
A surveillance tool identified in targeted attacks. Macma collects a range of user data including screenshots, keystrokes, and files, while disguising itself as a legitimate application. Its features are consistent with tools used in custom espionage operations.
macOS.Tarmac
Downloader that serves as an initial stage in multi-step attack chains. It is responsible for retrieving and executing additional payloads based on attacker objectives. It gains access via phishing campaigns or malicious ads, remaining minimally active until instructed otherwise.
macOS.WireLurker
A cross-platform threat capable of affecting both macOS and iOS systems. It spreads via trojanized applications and USB connections, harvesting device data and enabling remote command execution. Wire Lurker is notable for bridging the macOS-iOS infection vector, allowing attacks to move between platforms.
macOS.XCSSET
Targets macOS developers by embedding malicious code within Xcode projects. When a compromised project is built, the malware executes, enabling the attacker to modify browser behavior—particularly in Safari—by injecting JavaScript and capturing user credentials. It leverages the development environment as an entry point and as a distribution mechanism.
macOS.Zuru
Stealth-oriented malware used in targeted attacks, distributed through pirated or trojanized software. It facilitates unauthorized remote access and data exfiltration. While less prevalent, it has been linked to low-profile surveillance ops and long-term persistence strategies.

4.2 Response and Remediation

Description: This test assesses how the system under test (SUT) responds to detected threats. The evaluation focuses on the breadth and reliability of available response mechanisms, including alert generation, endpoint isolation, process termination, and file or user quarantine. The objective is to determine the solution's ability to contain or mitigate threats once identified, and to understand how consistently and accurately these actions are executed across different threat scenarios.

Observation:

Response and Remediation				
	Kandji – Supports automatic quarantine of malicious files and processes when identified as threats. It does not provide an device quarantine feature. Device lock or wipe is available if a device is compromised, but this action must be initiated manually.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.3 Alerting & Reporting

Description: An effective Endpoint Detection and Response (EDR) solution should provide the capability to directly observe and remediate threats on individual endpoints, including tools for investigation, containment, and threat elimination.

Observation:

Alerting & Reporting				
	Kandji – Displays alerts in a Threats dashboard with details such as threat name, file, user, process, and timestamp. Supports email and Slack notifications. No process tree or visual timeline, but provides sufficient context e.g., file path, hash for investigation.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.4 Real Time and Historical Analysis

Description: An effective EDR solution should support both real-time and historical analysis. Real-time visibility allows the system to observe endpoint activity as it occurs, facilitating the prompt detection of potentially malicious behavior. Historical analysis, on the other hand, utilizes previously collected data to investigate past incidents, identify recurring patterns, and inform future prevention strategies. Together, these capabilities contribute to a more comprehensive approach to threat detection and response.

Observation:

Real Time and Historical Analysis				
	Kandji – Once a threat is detected, the Threats dashboard allows users to search and filter threats based on classification and threat status. Threats are organized into two categories: File and Behavioral detections. Additionally, the platform retains threat history for up to 90 days, enabling historical analysis.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.5 Resource Consumption

Description: This test evaluates the efficiency of the EDR solution by measuring its memory and CPU usage under typical operating conditions. The objective is to determine whether the agent maintains a minimal resource footprint during both idle and active states. Testing is conducted in three phases: first, with the agent enabled but the system idle, and second, during an active event—such as an on-demand scan or the execution of a test script. Third, a large number of files were unzipped at once to simulate a heavy file inspection workload and observe how the agent handled sustained resource demands. These measurements assess the potential impact of an EDR agent on system performance.

Observation:

Resource Consumption				
	Kandji – While idle, the agent consumed 0% CPU and 24.5 MB of memory. During scanning and real-time threat protection, resource usage rose slightly to 0.6% CPU and 25.4 MB. Under heavy usage, consumption rose to 32.6% CPU and 33.5 MB of memory.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

CPU Consumption:

Vendor	Idle	Scanning/RTP	Heavy Usage
Kandji	0%	0.6%	32.6%
Industry Average	0.13%	2.4%	68.4%

Memory Consumption:

Vendor	Idle	Scanning/RTP	Heavy Usage
Kandji	24.5 MB	25.4 MB	33.5 MB
Industry Average	37.1 MB	46.2 MB	69.91 MB

The tables above show three stages of testing resources consumption while actively providing EDR protection: 1) The agent idle on the protected device, 2) scanning and real time protecting, and 3) heavy usage where a large amount of files were processed. CPU and Memory utilization were measured during all three steps. Kandji had one of the best observed ratings with the least CPU and Memory utilization while blocking threats.

4.6 Multi-Platform Support

Description: This test evaluates the extent to which the EDR solution supports multiple operating systems, including Windows, macOS, Linux, and mobile platforms such as iOS and Android. The aim is to assess whether the solution can maintain consistent security visibility and threat detection capabilities across a heterogeneous device environment.

Observation:

Multi-Platform Support				
	Kandji – Platform support is limited to macOS.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.7 Vendor Technical Support (Post Onboarding)

Description: During the deployment and use of an EDR solution, users may encounter configuration questions, operational issues, or require clarification on specific features. This evaluation considers the availability, accessibility, and quality of vendor-provided support resources, including technical documentation, knowledge bases and customer support channels—to determine how effectively users can obtain assistance throughout the implementation and operational lifecycle.

Observation:

Vendor Technical Support (Post Onboarding)				
	Kandji – Provides 24/5 live chat and email support through the web app. Ticket management is available via a support portal. A comprehensive knowledge base covers setup, integration and troubleshooting for macOS environments. No phone support is offered, but the available channels are accessible and well-documented.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.8 Onboarding Experience

Description: Some vendors offer training as part of the EDR solution, either bundled with the purchase or available as a separate service. This evaluation considers the quality and availability of onboarding resources, including formal training sessions, setup guidance, and user-facing instructional materials. An effective onboarding process should provide users with the knowledge needed to navigate and operate the platform confidently. Clear communication during implementation, along with continued support availability, is also a key factor in assessing the overall onboarding experience.

Observation:

Onboarding Experience				
	Kandji –Onboarding process is highly streamlined, supported by detailed documentation and guidance from the support team. Agent installation is straightforward, requiring minimal user permissions.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.9 Total Cost of Ownership

Description: This use case evaluates the total cost associated with acquiring and implementing the EDR solution, including licensing, deployment, operational cost, and any supplementary services. It focuses on overall value by assessing how the solution’s capabilities, features and security performance align with its cost. The objective is to determine whether the investment is proportionate to the level of functionality and protection provided.

Observation:

Total Cost of Ownership				
	Kandji – Capital Expense: Priced at \$168 per device annually for its combined MDM and EDR solution. The cost remains the same whether purchased as a bundle or separately, with MDM priced at \$96 and EDR at \$72. While Kandji’s EDR product falls on the higher end of the pricing spectrum, they offer a streamlined, integrated approach. Operational Cost: Kandji's operational and deployment costs were notably lower, driven by its streamlined setup process that enables faster implementation and reduced overhead. Training and support are included, minimizing additional expenses. With no need for extra resources, adoption is simplified and overall cost efficiency is improved.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.10 Evasion / Disabling EDR Technique

Description: This test evaluates the EDR solution's ability to detect and prevent unauthorized attempts to disable, uninstall, or interfere with its endpoint protection agent on macOS. Tamper protection—also referred to as self-defense—plays a critical role in ensuring that the agent remains active and cannot be easily modified or terminated by users or attackers with local access. The assessment includes attempts to terminate agent processes, stop associated services, and uninstall the software without proper authorization. In addition to resisting these actions, the solution is expected to generate appropriate alerts or logs to notify security teams of attempted tampering, supporting visibility and timely response.

Observation:

Evasion / Disabling EDR Technique				
	Kandji – Uses MDM-based controls to prevent uninstall on supervised devices. The agent cannot be terminated locally through standard means and includes basic protections against removal or tampering via LaunchDaemons and file system controls. Also includes automatic installs and turns itself back on if disabled or removed.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.11 Blacklist and Whitelist Enforcement Functionality

Description: This use case evaluates the EDR solution's ability to block or allow specific files, file hashes, IP addresses, domains, and URLs through blacklist (blocklist) and whitelist (allowlist) functionality. Blacklisting involves explicitly preventing known malicious files, network destinations, or indicators from executing or being accessed on an endpoint. Whitelisting involves allowing trusted files or connections to bypass detection and prevention mechanisms, ensuring legitimate business operations are not interrupted. The focus is on verifying whether the EDR can enforce these controls based on file attributes and network indicators.

Observation:

Blacklist and Whitelist Enforcement Functionality				
	Kandji – Supports block/allow lists for hashes of known malicious files and the path to the known malicious files, but not for IPs, URLs, or domains.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.12 Sample Submission

Description: This use case evaluates the EDR solution’s ability to accept and analyze manually submitted files for security inspection. The test verifies whether users can upload suspicious files through the platform’s interface for observation and whether the system can process those submissions to generate detection verdicts. The assessment considers the platform’s capacity to classify submitted samples as malicious or benign and to provide relevant context or threat intelligence. This functionality is important for investigating files that may not be flagged through automated detection mechanisms but still warrant further analysis by security teams.

Observation:

Sample Submission				
	Kandji – Submissions can be sent to support. Applied block rules are tracked internally.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.13 MITRE ATT&CK Simulations

Description: This test assesses the EDR solution's ability to detect behaviors consistent with a macOS-based supply chain attack. It simulates the execution flow of a compromised NPM package installed through the Cursor IDE, incorporating techniques observed in real-world incidents. The simulated behavior chain includes system configuration changes, persistence via LaunchAgents, the creation of a reverse shell, payload delivery to hidden directories, and modification of file permissions to prepare for execution.

Other elements include use of obfuscated, base64-encoded commands, execution of bash scripts written to disk, enumeration of Sudo privileges to mimic privilege escalation attempts and permission changes to reflect malware staging activities. This represents a combination of tactics across execution, persistence, privilege escalation and defense evasion.

The goal of this test is to evaluate whether the EDR solution can detect and appropriately correlate these events as part of a multi-step attack on macOS, providing timely and actionable visibility into potentially malicious activity.

Simulated Attack	Behavior Description	MITRE Technique	ID
Remote Desktop Access Enabled	Simulates a backdoor via Apple Remote Desktop configuration	Remote Services: Apple Remote Desktop	T1021.001
Process Name Masquerading	Renames the active process to evade detection	Indicator Removal on Host: Masquerading	T1036.003
Payload Dropped in Hidden Directory	Places a benign script in a hidden file system path	Indicator Removal on Host: Hidden Files and Directories	T1564.001
File Permission Changed to Executable	Uses chmod +x to simulate malware staging	File and Directory Permissions Modification	T1222.002
Simulated Reverse Shell Executed	Executes a harmless command resembling a remote shell call	Command and Control: Application Layer Protocol	T1071.001
Script Run with Admin Privileges	Script is executed with Sudo, representing attacker privilege escalation	Abuse Elevation Control Mechanism: Sudo	T1548.003
Bash Payload Executed from /tmp	Creates and executes a script in /tmp to simulate payload execution	Command and Scripting Interpreter: Bash	T1059.004
Keylogging via Unified Logging	Uses log stream to capture key press events for keylogging simulation	Input Capture: Keylogging	T1056.001
LaunchAgent Created for Persistence	Writes .plist to ~/Library/LaunchAgents to maintain persistence	Boot or Logon AutoStart Execution: Launch Agents	T1547.001
Bash History Cleared (Anti-Forensics)	Clears shell command history to simulate anti-forensics behavior	Modify System Configuration: Clear Command History	T1112

Observation:

MITRE ATT&ACK Simulations				
	Kandji – 8/10 Detected - Detected reverse shell execution using <code>perl</code> - Detected file download using <code>curl</code> - Detected hidden file creation using <code>SetFile</code> - Detected process name masquerading using <code>osascript</code> - Detected privilege escalation attempt via <code>sudo</code> - Detected permission change to executable using <code>chmod +x</code> - Detected keylogging simulation using <code>log stream</code> - Detected persistence mechanism via <code>LaunchAgent</code> creation using <code>plist</code>			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.14 Security Management Systems Integration

Description: This test case evaluates the EDR solution’s ability to integrate with external security platforms, including Security Information and Event Management systems, Security Orchestration, Automation and Response tools, and other components of the broader security stack. The assessment focuses on the availability and usability of APIs, support for standard log formats e.g., syslog, JSON, webhook capabilities, and pre-built integrations or connectors.

Effective integration enables security teams to centralize event visibility, automate incident response workflows and enrich alerts with contextual data from multiple sources. This evaluation considers how easily EDR-generated alerts, logs and telemetry can be forwarded, parsed, and acted upon by other security tools, with an emphasis on interoperability and operational efficiency.

Observation:

Integration Into Security Management Systems				
	Kandji – Supports a REST API and Amazon S3 Activity Log Integration, enabling automatic export of tenant activity logs for analysis, monitoring, and compliance. This allows seamless integration with SIEM platforms and streamlines centralized log collection.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

4.15 MDM (Mobile Device Management) Features and Capabilities

Description: This test evaluates the MDM capabilities provided by or integrated with the EDR solution. The assessment focuses on the completeness and effectiveness of MDM features as they relate to security posture, endpoint control, and administrative usability within Apple device environments. Key areas of evaluation include the onboarding process, integration between MDM and EDR components, ease of deployment, and policy enforcement capabilities. The test also considers support for automation, compliance workflows, third-party patching, platform coverage for macOS, iOS, and advanced features such as scripting, scoping, and Declarative Device Management. Solutions are examined for their suitability across various organizational needs, from low-touch deployments to complex, regulated environments requiring granular control.

Observation:

MDM Features and Capabilities				
	Kandji – Offers MDM integration with its EDR platform. Onboarding is direct, with automated workflows enabling rapid deployment across Apple endpoints. The platform includes predefined compliance templates, automatic third-party app patching, and built-in remediation, reducing manual configuration and administrative effort. Support for Declarative Device Management and native tools like Passport enhances functionality for administrators and users. The solution is well-suited for organizations seeking scalable, low-touch Apple device management with strong security alignment.			
	Industry Average – Miercom evaluated eight EDR for macOS solutions and averaged the criteria finding for this element provided here. Each vendor is given the opportunity to configure their solutions for optimal security efficacy and performance. Some vendors opted not to participate, in which Miercom used published best practices for configuration as well as the vendor provide technical support with the solution evaluated.			
Key				
				
Fully Compliant	Mostly Compliant	Marginally Compliant	Poorly Compliant	No Support
Excellent	Good	Fair	Needs Improvement	Fail

5.0 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.

6.0 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.

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>.