Miercom

Licensed for Distribution by:

Check Point Software Technologies

March 2025
DR241205K

AI-Powered Cyber Security Platform Assessment

miercom.com/checkpoint

Table of Contents

1.0 Executive Summary

Cybersecurity is rapidly shifting and becoming more sophisticated, demanding continuous evolution and proactive measures to stay ahead of emerging risks. Most enterprises operate in a hybrid IT environment that requires consistent unified security across on-premises, cloud, remote, and mobile use cases. This includes implementing Zero Trust controls to bolster the organization's security posture. Success factors that are often overlooked include security management ease of use, breadth of security platform capabilities, and end-user experience (UX). These play critical roles in mitigating risks, particularly those arising from human error, often preventable through proper configuration, policy enforcement, and access to effective AI-based tools.

A well-designed management interface enables swift adjustments to critical settings, empowering users to engage productively while upholding cyber security. It supports informed decision-making, appropriate remediation requests, and a stronger security posture with less frustration. Specialized AI-based assistants are playing an increasingly important role in making cyber security administration much easier and more effective.

This detailed report evaluates the essential capabilities for an AI-powered cyber security platform to effectively protect digital assets - emphasizing *Three Foundational Pillars* necessary for the successful implementation of comprehensive and unified security.

- **The Power of AI to Boost Advanced Threat Prevention**

  AI/ML is essential for modern threat defense, addressing complex security policies, continuous CVE alerts, and evolving AI-driven attacks. A core element of a cyber security platform is continuous verification of users, assets, applications, and devices, including cloud services and IoT. The platform must enforce least-privilege access, granting entities only the resources needed for their roles. AI is a key technology with the broad spectrum of capabilities needed to address this challenge.

- **Hybrid Mesh Firewalls and Diverse Deployment Enforcement Points**

  The flexibility to support traditional enterprise firewalls and hybrid mesh firewalls with diverse deployment models is essential. A cyber security platform should accommodate on-premises firewalls, virtual firewalls, cloud firewalls, and Firewall-as-a-Service (FWaaS) to ensure consistent policy enforcement across all assets and users, regardless of their location.

- **Unified Management, User-friendly interfaces, and AI assistants**

  A cyber security platform should provide centralized management for seamless integration and control across security components. This unified approach streamlines policy orchestration across environments, minimizing misconfigurations and security gaps. With the emergence of specialized AI-based assistants, administrators can now more easily create, manage, and troubleshoot policies. AI copilots can also help quickly identify new vulnerabilities and recommend remediation steps for network, cloud, SSE/SASE, SaaS, endpoint, browser, mobile device, and email security - from a single system.

Check Point Software Technologies engaged Miercom to assess their AI-powered, cloud delivered Infinity Platform compared to similar offerings from leading cyber security platform vendors. This study is based on hands-on evaluation of these solutions, in which we challenged the provider with real world customer use cases. Miercom did not acquire these products, nor were the competitors invited to complete this assessment. Vendors are invited to have their products re-evaluated if there is any disagreement with the results featured in this report.

Key Findings

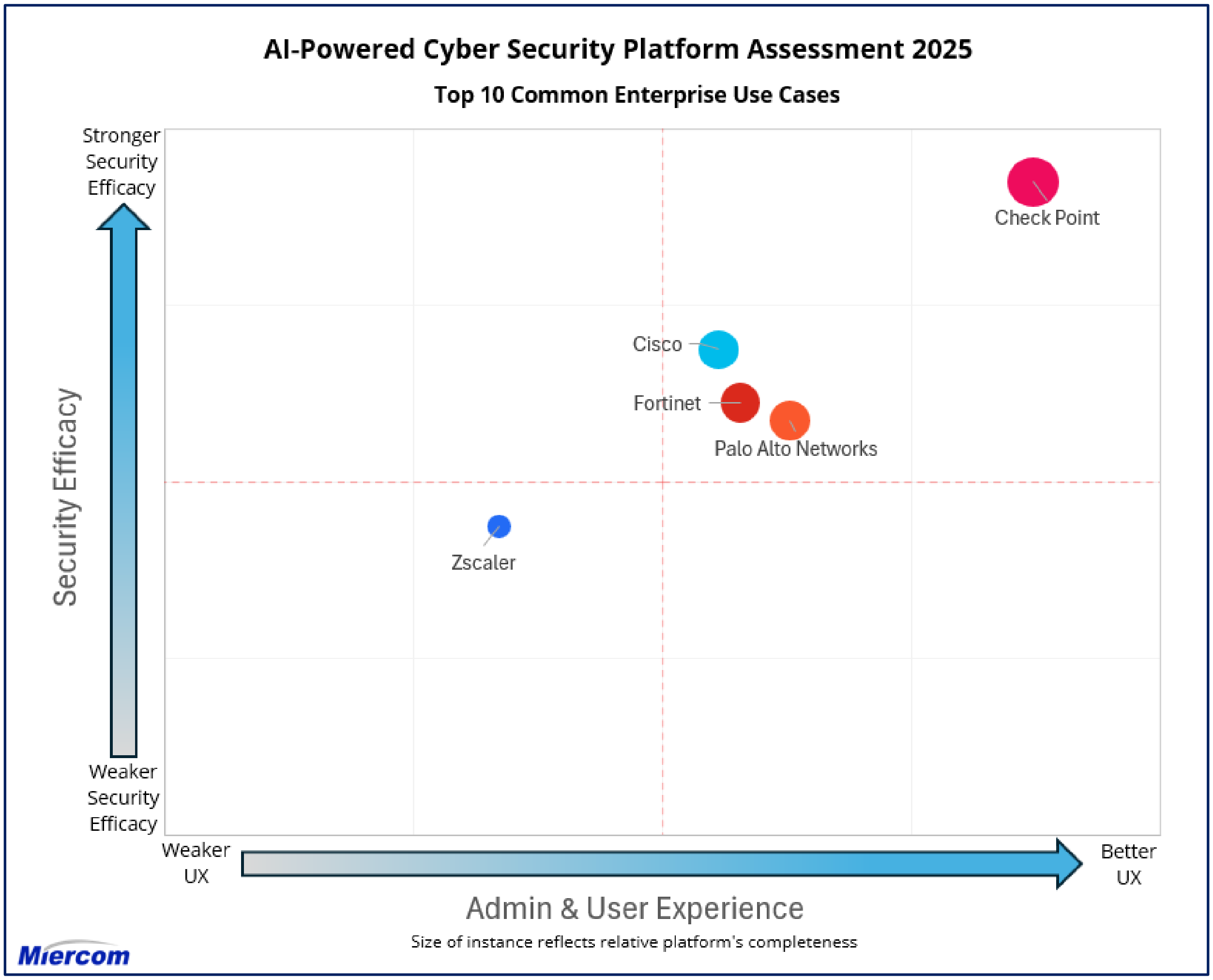
- **Security Efficacy:** Check Point's Infinity Platform demonstrated superior security efficacy, outperforming competitors in comprehensive threat prevention and response, excelling in the AI-driven testing scenarios.
- **Admin and User Experience:** The platform's straightforward user interface provides effortless management and precise decision-making for administrators. Check Point's Infinity AI Copilot performed the best, providing clear actionable insights with remediation guidance. It saved admin time and enhanced the overall ease of use.
- **Zero Trust Implementation:** Check Point surpassed competitors in executing common security policy implementation tasks in speed, accuracy, and completeness. Making it well suited for securing modern hybrid IT environments against persistent and evolving threats.

Check Point is recognized as a leading vendor in the Miercom AI-Powered Cyber Security Platform Assessment, outperforming competitive products in a comprehensive evaluation focusing on the most common cyber security implementations that enterprises perform daily. Check Point scored highest in both Admin & User Experience and Security Efficacy categories. Check Point's commitment to providing a superior AI-Powered Cyber Security Platform and its leadership in securing hybrid enterprise environments was clear in this analysis. Check Point's Infinity Platform has earned the **Miercom Certified Secure** award.

Robert Smithers
CEO, Miercom

2.0 Test Summary

The AI-Powered Cyber Security Platform Assessment marks the performance of cybersecurity vendors based on Security Efficacy and Admin & User Experience. Check Point leads, demonstrating the highest Security Efficacy and best Admin & User Experience.



Miercom AI-Powered Cyber Security Platform Assessment examined enterprise use cases for overall security efficacy, and administrative & user experience in deploying and configuring protection. The size of the individual markers represents the completeness of the vendor's platform. This assessment is pivotal for organizations prioritizing robust security for cyber security platform offerings.

The graphic also shows the relative *Platform Completeness* of the solution as far as meeting the requirements for an AI-Powered Cyber Security Platform. We evaluated three core requirements for AI-Powered Cyber Security platforms:

- Ability to Perform/Execute Zero Trust Capabilities integrated with AI
- Hybrid Mesh Firewall Architecture and Diverse Deployment Enforcement Points
- Centralized Management and Usability for Multiple Security Components

The AI-Powered Cyber Security Platform Implementation Scoring report assesses cybersecurity providers across a range of use cases relevant to security and policy management and user experience – including for hybrid mesh firewall and Zero Trust implementation.

Check Point leads with the highest overall score, reflecting it meets the key criteria effectively. The competitors follow with varying degrees of compliance across the criteria.

The overall scores at the bottom highlight Check Point’s leadership in this assessment, with other vendors showing lower compliance scores.

AI-Powered Cyber Security Platform Assessment Test Summary

Criteria	Use Case	Check Point	Cisco	Fortinet	Palo Alto Networks	Zscaler
1	On-Premise and Cloud Firewall Threat Protection Assessment	●	◑	◕	◕	◑
2	AI Copilot for Security Policy Analysis Automation and Active Implementation	●	◕	◕	◕	◑
3	AI Copilot for Vulnerability Assessment and Remediation	●	◑	◕	◕	◑
4	AI-Driven Threat Analysis and Mitigation Recommendations	◕	◑	◕	◕	◔
5	Collaborative and Delegated Security Administration	●	◑	◑	◑	◔
6	Cloud Service Providers Integration	●	◕	◕	◕	◑
7	Fast & Secure Internet Access for Remote Users	●	◕	◑	◑	◕
8	Clientless ZTNA	●	◕	◑	◑	◑
9	Email Phishing Robustness	●	◕	◑	◑	◑
10	Mobile Threat Defense (MTD)	●	◕	○	◕	○
OVERALL SCORE		**3.7**	**2.5**	**2.4**	**2.5**	**1.6**

Key									
4.0 – 3.5	●	**3.49 - 2.5**	◕	**2.49 – 1.50**	◑	**1.49 – .50**	◔	**0.49 - 0**	○
Fully Compliant		**Mostly Compliant**		**Marginally Compliant**		**Poorly Compliant**		**No Support**	

3.0 Introduction

As cyber threats become increasingly sophisticated and pervasive, the need for robust, comprehensive cybersecurity solutions cannot be overstated. Corporations are seeking platforms that not only protect their digital assets but also offer adaptability, scalability, and ease of integration within their existing hybrid IT infrastructures. In today's rapidly evolving cybersecurity landscape, where traditional defenses falter against sophisticated cyber threats, the combination of hybrid mesh firewalls and Zero Trust emerge as vital architectures. The Zero Trust core principle, "never trust, always verify," ensures continuous authentication and access authorization, significantly reducing security risks and promoting a proactive defense stance. The adoption of these architectures is crucial amidst rising data breaches and an expanding attack surface from new devices and cloud services. This adaptable framework offers significant benefits like:

- **Minimized Attack Surface:** Enforces least privilege and continuous verification to limit breach impacts.
- **Enhanced Threat Detection:** Allows for quicker detection and containment of threats through granular access controls.
- **Strengthened Compliance:** Aligns with evolving data privacy laws and standards.

Implementing these architectures can be challenging because of complexity, the requirement for integration with current systems, resource constraints, and the potential risks of vendor lock-in. This report explores key capabilities offered by AI-Powered Cyber Security platform providers.

- **Platform Capabilities**: Assessing features, continuous policy recommendations, deployment flexibility and easy integrations.
- **Security Efficacy:** Measuring real-world effectiveness against simulated attacks, including malware, phishing and network intrusion across all domains.
- **Administrator and User Experience:** Evaluating management interface intuitiveness and the power of AI to impact user productivity and satisfaction.

The Check Point Infinity Platform stands out as a leading solution, offering an integrated approach to threat prevention across network, cloud, and mobile environments. Check Point is distinguished by its unified and open security framework, which delivers continuous protection against threats and malicious activities while maintaining smooth business operations. Its key advantage is the ability to provide a comprehensive security strategy, combining network, cloud, endpoint, and mobile protection within a single executive dashboard for simplified management and enhanced visibility.

4.0 Products Tested

Products Tested	
Vendor/Software	Version
Check Point	
Infinity Portal/Smart-1 Cloud	SaaS/R82
Quantum Security Gateway	R82
Infinity AI Copilot	SaaS
Harmony SASE	SaaS
Infinity Portal/Harmony Email & Collaboration	SaaS
Infinity Portal/Harmony Mobile	SaaS
Cisco	
Security Cloud Control / Secure FMC	SaaS/7.6.0
Secure FTD	7.6.0
AI Assistant for Security	SaaS
Secure Connect	SaaS
Secure Endpoint (for Mobile)	SaaS
Email Threat Defense	SaaS
Fortinet	
FortiManager	7.6.1
FortiGate	7.6.1
FortiAI	SaaS
FortiSASE	SaaS
FortiMail	7.6.1
Palo Alto Networks	
Panorama, Strata Cloud Manager	11.2.4/SaaS
PAN-OS Gateway	11.2.4
Strata Copilot	SaaS
Prisma Access	SaaS
Cortex XDR	SaaS
Zscaler	
ZIA/ZPA/Client Connectors Admin Portals	SaaS
Zscaler Internet Access	SaaS
Zscaler Private Access	SaaS

5.0 AI-Powered Cyber Security Platform Use Cases

5.1 On-Premise and Cloud Firewall Threat Protection Assessment

Significance - Traditional NGFWs based on legacy threat protection engines struggle to defend against sophisticated cyber threats like unknown malware, zero-day phishing attacks, and advanced exploits. Organizations need NGFWs and hybrid mesh firewalls with advanced threat protection capabilities, such as behavioral analysis, sandboxing, AI engines, and comprehensive threat intelligence. These capabilities help detect and block emerging threats, prevent zero-day attacks, strengthen security posture, maintain business continuity, and stay ahead of evolving cyber risks.

To be effective, NGFW and hybrid mesh firewall security configurations need to be intuitive and easy to manage. Complex or cumbersome setup processes increase the risk of misconfigurations creating security gaps. A well-designed firewall enables security teams to quickly implement policies, make necessary adjustments, and respond to threats with minimal complexity***.***

Evaluation – This assessment evaluates the firewall's ability to detect and prevent unknown malware by downloading malware samples from VirusTotal across multiple file types. It also assesses the firewall's effectiveness in mitigating high and critical-severity Common Vulnerabilities and Exposures (CVEs) with a CVSS score of 7-10 published between 2022 and 2024. Additionally, the use case verifies the NGFW's capability to detect and block zero-day phishing attacks. The simplicity of configuring the NGFW was also analyzed.

Evaluation Procedure - Over 90 days, multiple sets of 500 malicious files were repeatedly downloaded from VirusTotal, selection based on detection by at least 25 threat engines ensuring a high probability of validity. These samples included DOCX, XLSX, PDFs, EXEs, PowerShell, Bash scripts, APKs, DLLs, and archived files. Each NGFW was evaluated using antivirus, anti-malware, anti-bot, URL filtering (URLF), sandboxing, and AI/ML protection engines, with testing conducted concurrently across vendor solutions.

To further challenge signature-based detection, malware samples were slightly modified to generate new hashes while retaining their malicious payload execution, simulating real-world evasion techniques.

IPS block rates were tested using BreakingPoint, a cybersecurity and network testing platform that simulates real-world traffic and threats. This evaluation measured the NGFW's effectiveness in blocking high and critical-severity CVEs.

The assessment also measured the NGFW's ability to detect and block newly discovered phishing and malicious URLs (less than 24 hours old) using multiple threat databases.

Observation and Rating – On-Prem and Cloud Firewall Threat Protection Assessment

Use Case 1	
On-Prem and Cloud Firewall Threat Protection Assessment - Evaluates the advanced threat protection effectiveness of the vendor's next-generation firewall solution.	
3.8 ●	**Check Point** - Excels across all evaluated aspects. Its administrative interface requires very few actions for configuration, ensuring that IT staff can quickly deploy and manage policies. Users benefit from a highly resilient security posture that delivers top-tier protection against malware – 99.9%, phishing – 99.74%, and intrusion attempts – 98.0 % block rate, making it the most robust option among those tested.
1.7 ◑	**Cisco** – Faces significant challenges in administration and security. Its configuration process is complex and requires frequent troubleshooting, placing a heavy burden on IT teams. With lower effectiveness in blocking threats across all categories: malware – 67.1%, phishing – 55.87%, and intrusion attempts – 42.6%. . Consequently, both the increased likelihood of security incidents and the additional workload for incident response results in greater maintenance demands for users.
3 ◕	**Fortinet** - Delivers reliable security with a moderately efficient administrative interface that occasionally requires extra troubleshooting. While its security defenses are acceptable: malware – 87.8%, phishing – 97.39%, intrusion attempts – 94.6%, there is room for improvement, particularly in malware and intrusion protections. The lower security performance in these areas elevates the risk of breaches, which in turn necessitates additional incident response efforts and greater maintenance for users.
2.8 ◕	**Palo Alto Networks** - Offers a balanced experience with an effective administrative interface that, however, requires some additional configuration to unlock its full effectiveness. The system provides decent protection in phishing – 98.69% and IPS – 91.6%, but its lower malware blocking capability -62.7% increases the risk of breaches. This heightened risk means that, when breaches occur, more incident response actions will be necessary, and users may face increased maintenance demands as a result.
2 ◑	**Zscaler** – Provides an average experience with an administrative and user interface that demands additional effort for configuration and ongoing maintenance. Despite a decent malware blocking performance – 90.9%, and phishing protection – 91.12%, its limitation in blocking intrusion attempts – 72.5% elevate the risk of breaches. This increased risk means that more incident response measures will be necessary, requiring both administrators and users to invest additional time in security management.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

5.2 AI-Powered Security Policy Analysis, Automation and Active Implementation

Significance – Access control policy modifications are routine yet critical in security operations, directly affecting an organization's ability to enforce security measures effectively. Manual analysis and implementation can be time-consuming and prone to errors, making automation a valuable enhancement. An AI-powered assistant should streamline this process by intelligently analyzing existing policies, identifying conflicts or misconfigurations, and providing actionable recommendations. Automating policy management not only improves efficiency but also ensures consistency, reducing security gaps. For firewall vendors, AI-driven policy modifications serve as a key competitive differentiator, enabling faster responses to evolving threats while maintaining compliance and strengthening overall security posture.

Evaluation - The test was designed to evaluate the effectiveness of AI Assistants in cyber security platforms for policy management tasks. The goal was to determine how well each vendor's AI assistant could:

- Analyze an existing Access Control Policy to check if a certain rule exists.
- Modify the policy by adding the necessary rules in the correct place.

Evaluation Procedure – The AI Assistants were evaluated based on two key criteria: Policy Analysis and Policy Modification. In Policy Analysis, the assessment focused on whether the AI could accurately determine if a rule existed and whether it provided a detailed explanation rather than a simple Yes or No response. In Policy Modification, the evaluation considered whether the AI suggested an appropriate placement for a new rule and whether it could apply the rule change itself. These criteria ensured a comprehensive review of the AI's ability to analyze and modify policies effectively.

Observation and Rating – AI-Powered Security Policy Analysis, Automation and Active Implementation

Use Case 2	
AI-Powered Security Policy Analysis, Automation and Active Implementation - Leveraging vendor's AI assistant feature to evaluate its ability to provide guidance on relevant configurations and directly modifying policy settings.	
3.8 ●	**Check Point** – Check Point’s AI Copilot successfully analyzed the access control policy and automatically modified it to allow HR access to the Social Networking category. It was the only solution that fully automated both the analysis and implementation without requiring manual intervention, demonstrating a seamless integration of AI-driven policy management.
3.2 ◕	**Cisco** – Cisco’s AI Assistant was able to determine that the HR department did not have access to the Social Networking category. However, it struggled with identifying the correct placement for the new rule and could not modify the policy directly, requiring administrators to manually determine where to insert the change.
2.7 ◕	**Fortinet** – FortiAI was unable to verify whether access was already granted and could not determine the correct placement for a new rule. Instead, it provided general guidance on how administrators could manually check for existing access and decide where to insert the rule. It also lacked the ability to modify the policy itself, requiring manual intervention.
2.7 ◕	**Palo Alto Network** – Strata Copilot could not determine if access was already granted and was unable to suggest the correct placement for a new rule. Instead, it provided instructions on how an administrator could manually check the policy and decide where to insert the change. While it offered step-by-step guidance for adding a rule, it lacked the capability to modify the policy directly.
2 ◑	**Zscaler** - Zscaler does not currently offer an AI-powered assistant for firewall policy management. As a result, it lacks automated analysis and modification capabilities, requiring administrators to manually check and update policies without AI-driven assistance.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

5.3 AI-Powered Vulnerability Assessment and Remediation

Significance - Ensuring that security infrastructure can proactively identify and mitigate emerging threats is essential for any organization. This test examines whether security products enhanced with AI Assistant functionality can accurately assess vulnerability to a sample known exploit and provide clear, actionable guidance for remediation. The ability to continuously monitor and swiftly secure systems against vulnerabilities is a key factor in maintaining overall security resilience.

Evaluation – The test simulates a realistic security inquiry by asking the AI Assistant, integrated within various security products, to determine if the current environment is vulnerable to a sample CVE (Common Vulnerabilities and Exposures). The inquiry expects the AI to verify whether appropriate protection is enabled on the security gateway. If protection is not in place, the AI must provide specific instructions on how to secure the system against this threat. This scenario challenges the AI's capability to both detect vulnerabilities and offer environment-specific remediation steps.

Evaluation Procedure – The evaluation focuses on the following criteria:

- Relevance and Completeness: The AI response should directly address the vulnerability inquiry and verify the status of protection mechanisms against a sample CVE.
- Actionability: If the environment is found to be vulnerable, the AI must offer clear, step-by-step instructions to implement the necessary security measures.
- Clarity and Specificity: The response should be understandable by security professionals, providing precise guidance that is directly applicable to the specific security gateway in use.
- Consistency: The solution should reliably deliver both an accurate vulnerability assessment and comprehensive remediation advice without ambiguity.

This approach ensures that the AI Assistant not only identifies potential security gaps but also supports prompt and informed decision-making to enhance overall security.

Observation and Rating – AI-Powered Vulnerability Assessment and Remediation

Use Case 3	
AI-Powered Vulnerability Assessment and Remediation - Assess each vendor's AI assistant in their ability to identify a specific vulnerability within their environment.	
4 ●	**Check Point** – Check Point received the highest score because its AI Copilot provided a complete and relevant response. It accurately verified whether the protection against a sample CVE was enabled and offered clear, actionable guidance for remediation. This comprehensive approach aligns perfectly with the evaluation criteria of relevance, actionability, clarity, and consistency.
1.5 ◑	**Cisco** – Cisco's AI Assistant was unable to provide any output in response to the query. The lack of any meaningful response significantly limits its ability to detect vulnerabilities and offer remediation guidance.
3.3 ◕	**Fortinet** – FortiAI's response included instructions on how to improve security; however, it lacked detailed verification of the current protection status. This limited the overall effectiveness of its remediation guidance.
3 ◕	**Palo Alto Networks** – Strata Copilot provided specific instructions on how to perform the vulnerability check, however, it considered only the PAN gateway itself for the answer, not the whole environment.
1.5 ◑	**Zscaler** – Zscaler does not offer an AI Assistant for their ZIA product. Without any mechanism to perform the vulnerability check or provide remediation instructions, its score reflects minimal functionality in this area.

Key									
4.0 – 3.5	●	**3.49 - 2.5**	◕	**2.49 – 1.50**	◑	**1.49 – .50**	◔	**0.49 - 0**	○
Fully Compliant		**Mostly Compliant**		**Marginally Compliant**		**Poorly Compliant**		**No Support**	

5.4 AI-Powered Threat Analysis & Mitigation Recommendations

Significance – Ensuring that security systems can identify and address threats that bypass initial defenses is critical. This test evaluates whether an AI Assistant can effectively analyze extensive log data to detect unblocked threats and provide actionable recommendations for improving security measures. The ability to promptly identify potential security gaps and offer remediation guidance is vital for maintaining robust defenses.

Evaluation - The scenario simulates a situation where an administrator asks the AI Assistant two specific questions:

- "Were there any threats that were not blocked today?"
- "What actions can I take to block these threats?"

The AI Assistant is expected to analyze millions of log entries to identify any threats that were not blocked and then offer precise, actionable recommendations to enhance security. This test challenges the AI's ability to process large datasets, identify anomalies, and generate clear guidance based on the observed log data.

Evaluation Procedure – The evaluation of the AI Assistant's performance is based on the following criteria:

- Relevance and Completeness: The response should accurately identify any threats that were not blocked, providing detailed information on the nature of these threats.
- Actionability: The AI assistant must offer clear, step-by-step recommendations for mitigating the identified threats and enhancing overall security.
- Clarity and Specificity: The guidance should be specific, unambiguous, and readily understandable by security administrators, ensuring that the recommendations are directly applicable.
- Data Processing Capability: The solution should efficiently analyze large volumes of log data and extract critical insights without overlooking important security events.

This evaluation approach ensures that the AI Assistant effectively supports threat detection and proactive security improvements through comprehensive log analysis and clear, actionable advice.

Observation and Rating – AI-Powered Threat Analysis & Mitigation Recommendations

Use Case 4	
AI-Powered Threat Analysis & Mitigation Recommendations – Test each vendor's AI Assistant for its ability to identify threats overlooked by the solution and provide actionable mitigation recommendations.	
3.3 ◕	**Check Point** - Administrators effectively interacted with Infinity AI Copilot, receiving the expected response. The AI identified threats missed by the solution in the past 24 hours and offered recommendations for mitigating these risks. It was also able to analyze threat logs upon request. However, the suggested remediation steps were not tailored to the specific environment in which the threats were detected.
1.8 ◑	**Cisco** – Administrators successfully engaged with AI Assistant, which provided insights into threats overlooked by the solution within the past 24 hours. However, the data was outdated by 16 hours, rendering it irrelevant. Additionally, AI Assistant was unable to read threat logs.
3.3 ◕	**Fortinet** – Administrators successfully engaged with FortiAI, which provided valuable insights into threats overlooked by the solution within the past 24 hours. However, the information lacked sufficient detail, and log searches were limited to specific sections of the portal.
2.5 ◕	**Palo Alto Networks** – Administrators successfully engaged with Strata Copilot, which provided valuable insights into threats that had been overlooked by the solution within the past 24 hours. It was also able to analyze threat logs upon request. However, it was unable to offer guidance on how to address or mitigate these identified threats.
1.3 ◔	**Zscaler** – Zscaler does not offer an AI Assistant for their ZIA product. Without any mechanism to perform this check or provide remediation instructions automatically, administrators will have to perform this task manually.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

5.5 Collaborative and Delegated Security Administration

Significance - For enterprises, it is crucial to have a security solution that enables collaborative efforts without introducing conflicts or creating security vulnerabilities. When multiple administrators work concurrently, the system must ensure that one admin's changes do not unknowingly contradict or override another's. For example, if an administrator adds a policy that was just modified by someone else without awareness of that change, it could lead to security gaps. Additionally, effective delegation is essential. The local administrators should be empowered to manage specific configurations within clearly defined boundaries, while central security maintains overall oversight. This dual approach prevents misconfigurations, avoids conflicts stemming from a lack of communication, and ensures that the integrity of the security framework is preserved across the organization.

Evaluation - The scenario involves a centralized management system where a central security team and multiple branch administrators work simultaneously. The central team oversees system-wide security configurations, while branch admins are delegated authority over specific URL filtering and access control policy segments (e.g., rules 7-10). This dual-layer model simulates real-world conditions where concurrent administrative actions could lead to overlapping or conflicting policies if not effectively managed, potentially resulting in unauthorized access or blind spots in security. Additionally, the delegated management aspect allows branch administrators to tailor their local policies for responsiveness without compromising core system-wide protections.

Evaluation Procedure – Four key areas were assessed: User Interface & Workflow, Conflict Resolution, Delegated Administration Capabilities, and Oversight & Security Integrity.

It examines the platform’s ease of use for both central and branch administrators, ensuring the interface enables seamless collaboration while reducing the risk of conflicting changes. Conflict resolution is tested by simulating concurrent policy modifications to assess the system’s ability to detect, prevent, and resolve overlapping or conflicting rules in real time.

Delegated administration is evaluated by verifying that branch administrators have read-only access to system-wide settings while being able to modify only their designated rules. The assessment ensures branch admins can view the full configuration, apply changes within their scope, and troubleshoot issues independently.

Finally, the evaluation confirms that central security administrators maintain full oversight, allowing them to monitor and manage branch-level changes effectively.

Observation and Rating – Collaborative and Delegated Security Administration

Use Case 5	
Collaborative and Delegated Security Administration - The system should enable multiple administrators to efficiently manage and address multiple tickets concurrently and reduce load on the central security administrator.	
3.8 ●	**Check Point** – Check Point ensures smooth collaboration with strong conflict management. Its SmartConsole UI locks objects and rules during edits, preventing conflicts. Delegated administration is streamlined with sub-policies, allowing branch admins to modify only designated areas while maintaining full visibility.
1.8 ◑	**Cisco** – Cisco struggles with collaboration and delegation. Unsaved changes by one admin can be lost when another saves, leading to conflicts. While sub-domains and sub-policies exist, complex setup and reliance on a local gateway limit branch admins' control, reducing efficiency.
2 ◑	**Fortinet** – Fortinet minimizes conflicts by restricting admin logins during changes but limits collaboration. It lacks clear guard rails for branch admins, granting them broader access than necessary, leading to challenges in conflict resolution and oversight.
2.3 ◑	**Palo Alto Networks** – Palo Alto Networks uses commit and config locks to prevent conflicts, but admins must monitor audit logs to avoid issues. While it allows limiting write permissions by feature or gateway, it does not support restricting both simultaneously, reducing flexibility in delegated administration.
1 ◔	**Zscaler** – Zscaler lacks robust concurrent administration and delegation controls. Admins have limited visibility into each other's changes, increasing misconfiguration risks. Branch admins have broad access without proper restrictions, weakening oversight and conflict management.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

5.6 Cloud Service Providers Integration

Significance - Integration with a cloud service provider (CSP) is critical for Zero-Trust platforms because it enables organizations to maintain stringent security controls over dynamic, cloud-based resources without sacrificing agility. In today's environment, where infrastructure is constantly evolving, having direct, secure integration with a CSP allows Zero-Trust solutions to automatically adapt policies based on real-time changes—ensuring that access to critical assets, such as database servers, remains tightly controlled. This integration minimizes administrative overhead, reduces the risk of misconfigurations, and limits the potential impact of a security breach by granting only the necessary permissions. It strengthens an organization's overall security posture while supporting the fast-paced, scalable operations that modern businesses require.

Evaluation - In this scenario, administrators are tasked with configuring the platform to grant access to database servers that are regularly updated by the MIS team. The goal is to simulate real-world conditions where the list of active database servers evolves, and the security policies must reflect these changes automatically. Administrators will work with tagged assets, ensuring that the system identifies and incorporates them correctly. The scenario tests the platform's ability to integrate dynamic cloud resources into its access control policies. By validating that the policy adjustments occur seamlessly as new servers are added or existing ones are updated, the test confirms the system's readiness for the fluid nature of modern cloud environments.

Evaluation Procedure - The evaluation procedure begins with logging into the Zero Trust Platform interface to determine whether cloud tags can be imported directly from AWS. If direct import is unavailable, the required tag (e.g., "use=proddataserver") must be manually created to ensure the system can recognize and utilize cloud-based asset identifiers. Next, configure a rule to allow SQL traffic from Production Web Servers to AWS-tagged database servers.

This process tests whether the platform supports seamless integration of dynamic cloud resources while maintaining robust access controls. Evaluators should observe how the system handles policy integration, the ease of use of the configuration interface, and the overall reliability in reflecting real-time changes in the environment.

Observation and Rating – Cloud Service Providers Integration

Use Case 6	
Cloud Service Providers Integration - The MIS team is tasked with managing a constantly evolving list of company database servers in the cloud, requiring dynamic access permissions.	
3.7 ●	**Check Point** – Requires only minimal permissions for cloud API access, allowing it to operate with a limited administrator account instead of needing full cloud environmen permissions. Additionally, it streamlines cloud object integration by letting administrators select dynamic objects directly from the cloud and insert them into the rule base withou creating separate internal objects, reducing complexity and misconfiguration risks.
3 ◕	**Cisco** – Cisco requires wide permissions for its cloud service provider API user, increasing exposure to the cloud environment. Additionally, it does not allow direct selection of cloud objects for policy rules, requiring administrators to first create a dynamic object with matching conditions before applying it to the rule base. This added complexity increases administrative effort and raises the risk of misconfiguration.
2.7 ◕	**Fortinet** – Fortinet does not offer minimal permissions integration, requiring administrators to undertake extra steps to add cloud objects to the rule base. This process includes the creation of internal objects with matching conditions, complicating rule creation and heightening misconfiguration risks. Its effectiveness is notable, but the process could be streamlined.
3.3 ◕	**Palo Alto Networks** – Supports minimal permissions integration. However, like other vendors, it does not allow administrators to directly select cloud objects from the cloud. Instead, they must create internal objects with matching conditions before adding them to policies, increasing administrative overhead and potential for misconfiguration.
1.7 ◑	**Zscaler** – Lacks the ability to integrate with cloud service provider API, leading to higher misconfiguration risks and a more restrictive implementation.

Key									
4.0 – 3.5	●	**3.49 - 2.5**	◕	**2.49 – 1.50**	◑	**1.49 – .50**	◔	**0.49 - 0**	○
Fully Compliant		**Mostly Compliant**		**Marginally Compliant**		**Poorly Compliant**		**No Support**	

5.7 Fast and Secure Internet Access for Remote Users

Significance - Remote work has become crucial for organizations, offering flexibility, cost savings, and business continuity, especially during disruptions. Due to the organization's concerns about routing remote users' traffic through the SASE providers Points of Presence (POPs) for inspection, which can lead to poor performance, fast internet access and strong security are vital to ensure employees can work efficiently and access resources without delays or risk of data breaches.

***Evaluation* –** Given the increasing importance of remote work for modern organizations, ensuring reliability and speed is critical for maintaining operational continuity. The main objective of this use case is to enable remote employees to complete their tasks efficiently and securely, regardless of their location.

This use case evaluates the solution's effectiveness through two key tests. First, an internet speed test that simulates remote user's internet access experience. Second, a malware prevention test introduces four common malicious file types to assess the solution's ability to detect and block cyber threats. Both tests were performed with all the vendors' security engines enabled.

Evaluation Procedure – To evaluate user experience and network performance, two tests were conducted:

- **Speed Test:** Repeated multiple times using a reliable speed test platform to measure connection performance.
- **File Download Simulation:** A 1MB DOCX file and a 10MB Excel spreadsheet were downloaded from SharePoint to assess file transfer efficiency.

Both tests were performed across three global regions—Americas, APAC, and EMEA—selecting locations strategically aligned with vendors' primary Points of Presence (PoPs) to ensure representative results.

To assess threat prevention capabilities, the system was tested against real-world malware samples:

- Malicious files were sourced from VirusTotal, selecting recent submissions flagged by 25+ security engines as high-probability threats.
- Samples included common web-browsing file formats such as PDFs, EXEs, SH scripts, and DLLs.
- The Test measured the platform's ability to detect and block malicious downloads in a remote user scenario.

All tests were conducted with SSL inspection and security engines enabled adhering to each vendor's best practice configurations.

Observation and Rating – Fast and Secure Internet Access for Remote Users

Use Case 7		
Fast and Secure Internet Access for Remote Users - Enable remote users to work from anywhere fast and securely.		
3.5	●	**Check Point** – Had the highest block rate of malicious files encountered by remote users at 99%. Check Point delivered the best user experience globally, achieving an average browsing speed of 1.2 Gbps and the fastest download times for 1MB and 10MB files from SharePoint at just 0.012 and 0.159 seconds, respectively.
3.2	◑	**Cisco** – Cisco had a block rate of 96% against malicious files encountered by remote users, Cisco delivered a decent user experience globally, achieving an average browsing speed of 980 Mbps and the download times for 1MB and 10MB files from SharePoint at just 0.251 and 1.077 seconds, respectively, while also providing fast internet and download speeds.
2.3	◑	**Fortinet** – Fortinet had a block rate of 84% against malicious files encountered by remote users, Fortinet delivered a below average user experience globally, achieving an average browsing speed of 173 Mbps and the download times for 1MB and 10MB files from SharePoint at just 0.235 and 1.083 seconds.
1.6	◑	**Palo Alto Networks** – PAN had a block rate of 74% against malicious files encountered by remote users. PAN delivered below average user experience globally, achieving an average browsing speed of 189 Mbps and the download times for 1MB and 10MB files from SharePoint at just 0.491 and 1.554 seconds.
2.7	◕	**Zscaler** – Zscaler had a block rate of 83% against malicious files encountered by remote users, Zscaler delivered a decent user experience globally, achieving an average browsing speed of 306 Mbps and the download times for 1MB and 10MB files from SharePoint at just 0.078 and 0.690 seconds, respectively.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

Speed and File Download Tests				
Check Point	**Americas**	**EMEA**	**APAC**	**Average**
fast.com	1.36Gbps	1.5Gbps	740Mbps	1.2Gbps
1MB/10MB File Downloads	0.020/0.192sec	0.007/0.124sec	0.11/0.163sec	0.012/0.159sec
Cisco	**Americas**	**EMEA**	**APAC**	**Average**
fast.com	720Mbps	1.4Gbps	820Mbps	980Mbps
1MB/10MB File Downloads	0.071/0.455sec	0.082/0.558sec	0.600/2.22sec	0.251/1.077sec
Zscaler	**Americas**	**EMEA**	**APAC**	**Average**
fast.com	216Mbps	306Mbps	396Mbps	306Mbps
1MB/10MB File Downloads	0.180/1.53sec	0.028/0.291sec	0.026/0.249sec	0.078/0.69sec
Palo Alto Networks	**Americas**	**EMEA**	**APAC**	**Average**
fast.com	104Mbps	203Mbps	260Mbps	189Mbps
1MB/10MB File Downloads	0.378/1.52sec	0.239/0.823sec	0.858/2.32sec	0.491/1.554sec
Fortinet	**Americas**	**EMEA**	**APAC**	**Average**
fast.com	94Mbps	190Mbps	236Mbps	173Mbps
1MB/10MB File Downloads	0.053/0.471sec	0.082/0558sec	0.600/2.22sec	0.235/1.08sec

5.8 Clientless ZTNA (Zero Trust Network Access)

Significance - Clientless users refer to individuals who access corporate resources without installing a dedicated security client on their devices. These users typically rely on web-based access via a browser to connect to corporate applications. Clientless access is commonly used by contractors, third-party vendors, partners, or remote employees who operate from unmanaged or personal devices. Organizations must ensure that clientless users with unmanaged devices can securely access corporate resources while maintaining strict security controls. Without proper security measures, these users can introduce significant risks. Providing secure remote access for clientless users is essential for business continuity and collaboration, but it must be done in a way that does not compromise security.

Evaluation – This use case assessed each vendor's capability to enable clientless users a secure remote access to corporate internal server. To enhance security, access was granted only when specific conditions were met, including user's location, days and time, device OS, and browser type.

Evaluation Procedure - The administrator configures a policy on the SASE platform to enable connections to the internal server while enforcing strict access controls through posture checks. These checks verify the user's identity and ensure compliance with the following conditions: the user is in the USA, access is requested between Monday and Thursday from 5:00 PM to 9:00 PM, the device is running Windows 10 or greater, and the browser used to connect is Google Chrome. The user is tasked with opening a browser, verifying identity, and connecting to the internal server.

Observation and Rating – Clientless ZTNA

Use Case 8	
Clientless ZTNA - Enable secure remote access to corporate resources from unmanaged devices.	
3.7 ●	**Check Point** – Administrators can effectively create posture profiles for clientless users and configure the necessary criteria. The user portal presents a clear overview of accessible applications, minimizing the risk of misconfiguration which highlights its overall effectiveness rating. A clear error message displayed when the user's access attempt violates posture checks.
2.7 ◕	**Cisco** – Creating posture profiles for clientless users is possible, albeit with some difficulty. All required criteria, except date and time, can be configured. The absence of a user portal means users must keep track of application access links manually. Despite this, misconfiguration is unlikely.
2.3 ◑	**Fortinet** – Administrators must configure the SWG with SSO. Local users are not supported. Only apps that are behind a FortiGate product are accessible. However, the user portal allows a clear view of the permitted applications. Not all the required criteria are available.
2 ◑	**Palo Alto Networks** – Administrators face challenges in configuring necessary criteria for clientless users. However, its user portal does provide a clear view of allowed applications. The likelihood of misconfiguration is high.
2 ◑	**Zscaler** – The platform experiences limitations in configuring access policy rules for clientless users, specifically with platform OS and country criteria. Adding these criteria can result in applications becoming invisible in the user portal. Although the portal permits a clear view of the permitted applications, challenges in task fulfillment and criteria configuration indicate a likelihood of misconfiguration.

Key									
4.0 – 3.5	●	3.49 - 2.5	◕	2.49 – 1.50	◑	1.49 – .50	◔	0.49 - 0	○
Fully Compliant		Mostly Compliant		Marginally Compliant		Poorly Compliant		No Support	

5.9 Email Phishing Robustness

Significance - Corporate email remains a primary target for cyber attackers. Employees rely on email daily but may not always recognize emerging threats, making it essential to implement a security solution that detects and mitigates attacks before they reach users' inboxes, ensuring both protection and business continuity.

Cyber threats are becoming more sophisticated, using deceptive tactics to evade detection. A growing technique is Quishing, where attackers embed QR codes in emails to bypass security filters. Additionally, phishing links concealed within images make detection more difficult, increasing the risk of user engagement.

Some vendors lack dedicated email security solutions, yet email remains a critical component of a zero-trust strategy, particularly as users access corporate email from unmanaged devices. Even without malicious links, attackers can exploit email to manipulate users into taking harmful actions.

Evaluation – The goal of this use cases is to evaluate the effectiveness of an email security solution in detecting and blocking phishing attacks that use various techniques. This assessment helps identify potential weaknesses in the email security infrastructure and improve defenses against real-world phishing threats.

Evaluation Procedure - The evaluation assesses the effectiveness of security solutions in detecting and mitigating various phishing attacks delivered through multiple techniques, including known phishing links, zero-day phishing links, QR code-based phishing, shortened malicious links, phishing links embedded in images, plain text phishing links, and phishing attacks hidden within email attachments. Each security product was deployed in a dedicated domain, with security policies configured according to best practices, ensuring that all models were set to alert and quarantine malicious threats. The Phishing Test Methodology involved using a sample of phishing links initially detected by the vendor as a baseline to evaluate the product's ability to block other evasive phishing techniques. This approach provides a comprehensive assessment of each solution's resilience against advanced phishing threats.

Observation and Rating – Email Phishing Robustness

Use Case 9	
Email Phishing Robustness - Evaluate the solutions ability to protect user's mailboxes from various phishing attack techniques.	
3.8 ●	**Check Point** – Check Point's email security solution provided comprehensive protection against all tested phishing attacks techniques while delivering an excellent administrative experience. Its user-friendly interface, streamlined policy management, and intuitive configuration options enable administrators to efficiently set up and manage security policies with minimal effort.
2.7 ◕	**Cisco** – While the system did not prevent all phishing attacks techniques , the administrator interface was intuitive offering a user-friendly experience with straightforward configuration and policy management. However, even when phishing emails were successfully quarantined for inspection, users continued to receive Outlook notifications indicating a new email had arrived. This could create confusion, as users might mistakenly believe the email was still accessible in their inbox.
2.2 ◑	**Fortinet** – While the product effectively prevented most phishing attack techniques, its reporting capabilities and administrator console navigation fell short of market expectations. The report lacked in-depth insights, making it difficult for administrators to analyze attack pattern and the console's navigation was not as intuitive as competing solutions, requiring extra effort to locate key settings, manage policies, and review security incidents.
1.7 ◑	**Palo Alto Networks** – The vendor is lacking an email security solution. Therefore, to simulate a real-world scenario where the email provider includes basic built-in security features, Microsoft native security was tested as a default solution.
1.7 ◑	**Zscaler** – The vendor is lacking an email security solution. Therefore, to simulate a real-world scenario where the email provider includes basic built-in security features, Microsoft native security was tested as a default solution.

Key									
4.0 – 3.5	●	**3.49 - 2.5**	◕	**2.49 – 1.50**	◑	**1.49 – .50**	◔	**0.49 - 0**	○
Fully Compliant		**Mostly Compliant**		**Marginally Compliant**		**Poorly Compliant**		**No Support**	

5.10 Mobile Threat Defense (MTD)

Significance – As mobile devices continue to play a central role in both personal and professional settings, securing them against evolving threats is critical. The absence of robust mobile protection capabilities exposes organizations to significant risks, including unauthorized access, data breaches, and exploitation of OS vulnerabilities. Devices that are rooted or jailbroken present a particularly high risk, as they bypass built-in security controls, making them more susceptible to malware and unauthorized modifications. Without advanced application analysis, organizations may unknowingly permit insecure or malicious apps that compromise sensitive information. Implementing comprehensive Mobile Threat Defense is essential to mitigate these risks, ensuring a secure mobile ecosystem and reducing the likelihood of security incidents that could have severe financial and reputational consequences.

Evaluation - This assessment evaluated several key mobile security vulnerabilities commonly exploited by attackers. The evaluation focused on three main areas:

Outdated Operating Systems: The assessment checked for vulnerabilities stemming from outdated mobile operating systems. Outdated OS versions often contain unpatched CVEs that attackers can exploit to compromise devices.

Rooted/Jailbroken Devices: The assessment examined the solution's ability to detect whether a device has been rooted (Android) or jailbroken (iOS). These modifications remove built-in security restrictions, making devices more susceptible to malware and other attacks.

Malicious Application Installation: The assessment tested the solution's ability to detect and prevent the installation of malicious applications. Malicious apps can grant attackers backdoor access to a device, enabling them to steal data, monitor user activity, and perform other harmful actions. This includes potentially monitoring a user's daily activities on the device.

Evaluation Procedure – To simulate real-world attack scenarios, each security solution was deployed on a different mobile device, using a variety of brands. Devices were intentionally outdated and rooted/jailbroken. Malicious applications were then introduced to evaluate the solution's ability to detect and prevent threats. Logs were monitored and collected from the administrator console. Security policies were configured following best practices to achieve test objectives.

Observation and Rating – Mobile Threat Prevention

Use Case 10	
Mobile Threat Prevention – Assess each vendors ability to block multiple mobile security threats.	
3.5 ●	**Check Point** – Administrators can configure rules and policies appropriately. . Administrators can navigate the interface but there are many menus and functions that can make it hard to understand. Overall, the product provides a full suite of MTD capabilities, effectively preventing all tested security threats.
3 ◕	**Cisco** – Administrators can navigate and configure appropriately, though the interface is not designed for a mobile solution. Administrators can easily understand and traverse the interface. Cisco's solution is missing certain security features, allowing out-of-date mobile devices to cause potential security risks.
0 ○	**Fortinet** – The absence of a security solution tailored for the mobile environment is evident in this test, as Fortinet struggles to effectively identify and block the mobile-focused cyber threats evaluated.
3 ◕	**Palo Alto Networks** – Administrators can navigate and configure appropriately, though the interface is not designed for a mobile solution. Users can easily understand and traverse the interface. Overall, the product maintained a positive user experience while successfully detecting malicious applications. However, its ability to identify rooted devices is limited to iOS, and it falls short in detecting vulnerabilities caused by outdated mobile operating systems.
0 ○	**Zscaler** – The absence of a security solution tailored for the mobile environment is evident in this test, as Zscaler struggles to effectively identify and block the mobile-focused cyber threats evaluated.

Key									
4.0 – 3.5	●	**3.49 - 2.5**	◕	**2.49 – 1.50**	◑	**1.49 – .50**	◔	**0.49 - 0**	○
Fully Compliant		**Mostly Compliant**		**Marginally Compliant**		**Poorly Compliant**		**No Support**	

6.0 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.

7.0 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 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 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.