Miercom

DR240228F

March 2024

Licensed for Distribution by:

Check Point Software

Zero Trust Platform Assessment

Miercom Zero Trust Security Benchmark™ 2024

Table of Contents

1.0 Executive Summary

In the rapidly evolving cybersecurity landscape, the adoption of a Zero Trust architecture is imperative for organizations seeking to enhance their security posture. The ease of use and the quality of the user and admin experience (UX) are paramount in mitigating the risk of major security breaches, many of which stem from human error—errors avoidable through proper configuration, policy settings, or other components of the security architecture.

The effectiveness of the management interface in enabling swift and efficient updates to these settings is critical, as it not only streamlines admin tasks but also empowers users to engage with the solution in their daily operations. A user interface that enables participants to be well-informed and to make intelligent decisions regarding their networking activities is indispensable. Such an interface encourages users to request remediation for unwarranted restrictions, enhancing the overall security posture by reducing frustration and ensuring that users have the necessary access to carry out their roles.

This detailed report evaluates the critical capabilities required for a Zero Trust platform to effectively safeguard digital assets, emphasizing *Three Foundational Pillars* necessary for the successful implementation of a *Zero Trust Strategy*.

- **Centralized Management and Usability for Multiple Security Components:**
  A Zero Trust platform must offer centralized management, enabling seamless integration and control over security components. This unified management framework simplifies the orchestration of complex security policies across diverse environments, reducing the risk of misconfigurations. Such a platform ensures that security administrators can effectively manage network security, cloud security, SaaS security, endpoint, and email protection from a single pane of glass.
- **Hybrid Architecture and Diverse Deployment Enforcement Points:**
  The flexibility to support a hybrid architecture with diverse deployment models is essential. A Zero Trust platform should accommodate on-premise firewalls, virtual firewalls, cloud firewalls, and Firewall-as-a-Service (FWaaS) to ensure consistent policy enforcement across all assets, regardless of their location.
- **Ability to Perform/Execute Zero Trust Capabilities:**
  Fundamental to Zero Trust is the continuous verification of users, assets, applications, and devices, including emerging technologies such as cloud services and IoT devices. The platform must enforce access controls that adhere to the principle of least privilege, ensuring that entities are granted access only to the resources necessary for their roles and functions.

Check Point Software Technologies engaged Miercom to conduct a private assessment of their AI-powered, cloud delivered Infinity Platform compared to similar offerings from leading Zero Trust Platform vendors. This study was based on Check Point demonstration of customer use cases and Miercom open-source research of these products. 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 in the results featured in this report.

Key Findings

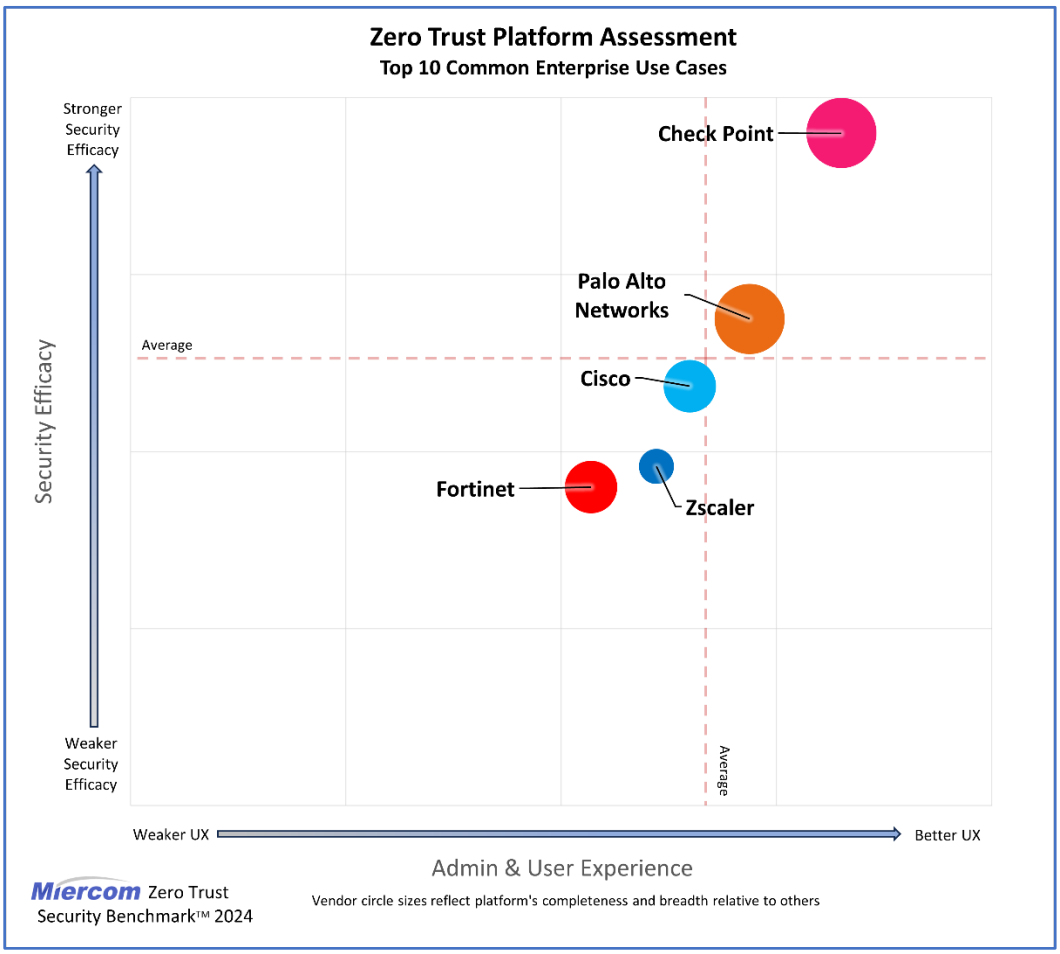
- **Security Efficacy:** Check Point Infinity is recognized for its superior security efficacy, outperforming competitors in comprehensive threat prevention and response capabilities based on 10 common use case implementations for Zero Trust.
- **Admin and User Experience:** The Check Point platform is extremely effective in terms of administrative and user experience, attributed to its intuitive interface and simplified management processes, enhancing overall ease of use.
- **Zero Trust Implementation:** Check Point Infinity has excelled in the evaluation of 10 zero trust implementation common tasks for enterprise businesses. Check Point Infinity Platform is well suited to securing modern IT environments against persistent and evolving threats.

Check Point is recognized as a leading vendor in the Miercom Zero Trust Platform Assessment, outperforming competitive products in a comprehensive evaluation focusing on the Top 10 most common Zero Trust 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 Zero Trust Platform and its leadership in the Zero Trust security landscape was clear in this analysis. Check Point Security Technologies has earned the **Miercom Certified Secure** award.

Robert Smithers
CEO, Miercom

2.0 Test Summary

The Zero Trust Platform Assessment marks the performance of various cybersecurity vendors in terms of "Security Efficacy" and "Admin & User Experience." Check Point leads the chart, demonstrating the highest security efficacy and the best admin and user experience.



Miercom Zero Trust Platform Assessment examined the top 10 enterprise ZTP use cases for overall security efficacy, 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 Zero Trust Platform offerings.

The graphic also shows the relative *Zero Trust Platform Completeness* of the solution as far as meeting the requirements of a Zero Trust Platform. We evaluated three core requirements for a Zero Trust platform:

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

The Zero Trust Security Platform Implementation Scoring report assesses cybersecurity providers across a range of use cases relevant to zero trust security.

Check Point leads with the highest overall score of 3.5, 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.

Zero Trust Platform Assessment Test Summary						
Criteria	**Use Case**	**Check Point**	**Cisco**	**Fortinet**	**Palo Alto Networks**	**Zscaler**
1	URL Categories Access Restriction	●	◕	◕	◕	◕
2	Concurrent Administrators	◕	◑	◕	◕	◔
3	Cloud Service Providers Integration	●	◕	◕	◕	◑
4	Delegated Management	●	◑	◕	◕	◔
5	Malicious Website Protection	●	◑	◔	◑	◕
6	Phishing Protection	●	◑	◕	◕	◕
7	IPS Exception	●	◑	●	◕	◕
8	Email Protection	●	◕	◕	◕	◑
9	Clientless ZTNA	●	◕	○	◑	◑
10	Remote User Browser Interface	●	●	◑	◕	◑
OVERALL SCORE		**3.5**	**2.4**	**2.3**	**2.8**	**2.2**

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

In an era where cyber threats are 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 IT infrastructures. In today's rapidly evolving cybersecurity landscape, where traditional defenses falter against sophisticated cyber threats, Zero Trust emerges as a vital architecture. Its 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 Zero Trust is crucial amidst rising data breaches and an expanding attack surface from new devices and cloud services. Zero Trust's dynamic, adaptable framework offers significant benefits:

- **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 industry standards.

Deploying Zero Trust can be daunting due to its complexity and the need for integration with existing systems, limited resources, and the risks of vendor lock-in. This report examines the Zero Trust capabilities across leading Zero Trust Platform vendors:

- **Platform Capabilities**: Assessing features, deployment flexibility, integrations, and user-friendliness.
- **Security Efficacy:** Measuring real-world effectiveness against simulated attacks.
- **Administrator and User Experience:** Evaluating management interface intuitiveness and the impact on user productivity and satisfaction.

Check Point Infinity Platform emerges as a frontrunner, promising a consolidated approach to threat prevention across networks, cloud, and mobile environments. Check Point stands out for its unified security architecture, designed to provide seamless protection against threats and malicious activities while ensuring uninterrupted business operations. Its strength lies in its ability to offer a multi-layered security strategy, combining network security, cloud security, endpoint protection, and mobile security under a single executive dashboard for simplified management and ease of overall visibility.

4.0 Products Tested

Products Tested	
Vendor/Software	Version
Check Point	
Infinity Portal/Quantum Gateway	R81.20/R82
Infinity Portal/Harmony SASE	SaaS
Infinity Portal/Smart-1 Cloud	SaaS (R81.20/R82)
Infinity Portal/Harmony Email & Collaboration	SaaS
Cisco	
FirePower FTD	7.4.0
Secure Connect	SaaS
FirePower Management Center	7.4.0
Microsoft E3	SaaS
Fortinet	
FortiGate	7.4.2
FortiSASE	SaaS (23.4.49
FortiManager	7.4.2
FortiMail	7.4.0
Palo Alto Networks	
PAN-OS Gateway	11.1.1
Prisma Access	SaaS (4.0.0 preferred)
Panorama	11.1.1
Microsoft E3	SaaS
Zscaler	
Zscaler Internet Access	SaaS
Zscaler Private Access	SaaS
Microsoft E3	SaaS

5.0 Zero Trust Platform Assessment Use Cases

5.1 URL Categories Access Restriction

Description - We evaluated the procedures for granting and restricting access to social media platforms within an organization. This section specifically addresses the procedures an administrator must follow to enable social media access; for example, the Human Resources (HR) department while imposing restrictions on other departments. Additionally, it covers the process for allowing and overseeing exceptions under special circumstances.

Users restricted from social media can submit a justification for needing access, which, if deemed valid, results in automatic access granting. This "bypass" mechanism, requiring justification, is designed primarily for overcoming business operation-related blocks, such as mitigating time wasted on social media, rather than circumventing security measures against malicious content. This process is tailored for non-security related content access, ensuring a balanced approach to productivity and security.

Impact - Balancing productivity and security within a company's network requires a nuanced approach to social media access and exposure. Businesses must navigate the dual challenges of allowing reasonable social media use while protecting against potential risks, such as malicious attack and compliance breaches. However, overly restrictive or poorly communicated policies can lead to employees feeling demotivated or resisting compliance. Additionally, there is a risk that users might misinterpret access denials as technical issues rather than legitimate security measures. Achieving an optimal balance that safeguards company interests without impeding employee morale is essential for effective social media management in the workplace.

Evaluation Procedure - Explore and evaluate the user interfaces for login and access management across leading Zero Trust Platform vendors.

Conduct a thorough assessment of the efficiency and user-friendliness in establishing rules to clock social media usage within the simulated business scenario, while also accommodating special exceptions. This evaluation spans both user-level and administrative-level logins, aiming to understand the ease and flexibility of policy implementation across different access tiers.

Observation and Rating – URL Categories Access Restriction Use Case

Use Case 1	
URL Categories Access Restriction - The Human Resources (HR) department relies heavily on social media platforms for various critical functions such as recruitment, employer branding, and employee engagement initiatives. However, unrestricted access to social media across all departments is a productivity drain and a potential security and reputational risk.	
3.5 ●	**Check Point** – The interface of Check Point is notably user-friendly, offering effortless navigation that facilitates quick and intuitive drag-and-drop actions, significantly reducing configuration times. The simplicity in administration and the incorporation of automation minimize the likelihood of errors. The system ensures users are directed appropriately, enhancing access control to social media, and making misconfigurations rare. Its overall performance is marked by both security and ease of use.
3.0 ◕	**Cisco** – Cisco's interface is straightforward though it requires navigating through multiple menus to establish individual rules, with additional steps for configuring logs. Users are alerted to restrictions but can bypass them. The complex menu system raises concerns about potential misconfigurations. Despite this, the interface remains user-friendly, albeit with a suggestion for simplifications.
2.8 ◕	**Fortinet** – Fortinet's interface necessitates the use of profiles for implementing block/alert pages, complicating direct URL-based rules. The GUI can be perplexing, requiring additional profile configurations that may confuse users. Despite these challenges, user integration remains effective. The possibility of misconfigurations due to the interface complexity suggests a need for improvement to enhance overall usability.
3.1 ◕	**Palo Alto Networks** – The process involves navigating through several menus for rule creation and profile management for block/alert pages, which cannot be directly applied within rules. This, along with the requisite for extra logging configurations and profiles for new rules, complicates the admin experience. However, user configuration is straightforward, making the system simple and effective for users, though administrative aspects require refinement for better efficiency.
3.0 ◕	**Zscaler** – Zscaler's interface exhibited slow responsiveness, and users must disable certain features to properly display alert pages, adding to the time taken for configuration. Users are clearly notified by the alert, and options are provided to either bypass the block page or return to the previous page. While the likelihood of misconfiguration is low, the additional steps required in the interface could pose a risk. Although user-friendly, the overall effectiveness of Zscaler's GUI could benefit from enhancements to improve speed and streamline the user experience.

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 Concurrent Administrators

Description - This use case explores a collaborative environment where a security team, composed of multiple administrators, is tasked with managing simultaneous requests. The team operates within a centralized management system, implementing and modifying security rules for multiple branch offices. Access issues can occur when conflicting or overlapping policies from administrators inadvertently allow users to access resources.

Impact - The ability for multiple administrators to access and modify security settings concurrently can lead to the creation of conflicting policies. This not only breeds confusion but also increases the risk of misconfigurations within the security framework, potentially compromising the organization's overall security posture.

Evaluation Procedure - This assessment involves accessing and navigating the user interfaces. The focus is on evaluating the platforms' user-friendliness and efficiency in URL filtering policy creation by an administrator in various scenarios. A critical part of the evaluation is to observe how the system handles policy conflicts when a user attempts to access a resource. The testing environment must ensure that the multiple administrators can simultaneously manage and apply policies without creating security gaps. A key criterion is to avoid the creation of "blind spots;" administrators should not need to painstakingly review every setting to ensure no unauthorized changes have been made.

Observation and Rating – Concurrent Administrators Use Case

Use Case 2	
Concurrent Administrators - The system should enable multiple administrators to efficiently manage and address multiple tickets concurrently.	
3.4 	**Check Point** – Check Point's SmartConsole GUI uniquely locks individual objects and rules during modifications, streamlining admin usage and preventing conflicts with other users. This design facilitates seamless concurrent operations without compromising security, significantly reducing the likelihood of misconfiguration. Overall, Check Point delivers exceptional effectiveness and supports collaborate work efficiently.
2.0 	**Cisco** – Cisco's system, upon an administrator saving their configuration, inadvertently causes any unsaved changes by other logged-in administrators to be lost. While this ensures secure admin use, it leads to potential work loss and misconfiguration due to admin conflicts. The overall security is robust, but the lack of support for concurrent management detracts from the administrator experience.
2.5 	**Fortinet** – Fortinet's recommended "best practice" involved restricting admin login during ongoing changes to prevent concurrent access issues. This approach, while intended for security, raises concerns for potential misconfiguration and admin lockouts, suggesting a need for improvement in collaborative settings.
3.0 	**Palo Alto Networks** – In scenarios demonstrated, changes saved by one admin may override those by another, unless "commit lock" or "config lock" features are employed to restrict changes to the current admin. Although these features prevent concurrent editing, they require careful monitoring of change logs to avoid misconfigurations. Palo Alto Networks offers a good level of effectiveness with provisions for collaborative work, provided there is due diligence in change management.
1.0 	**Zscaler** – The lack of visibility among administrators regarding their colleagues' changes can lead to potential misconfigurations, posing security risks and operational confusion. Enhancements are necessary to support efficient teamwork in concurrent settings.,

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 Cloud Service Providers Integration

Description - This use case focuses on enabling administrative control to grant access to database servers identified by specific IP addresses, as listed by the system team. These servers, tagged assets within EC2 environments, demand dynamic policy updates to ensure seamless access amidst frequent changes. The MIS team continually updates the list of database servers hosted in the cloud, facilitating uninterrupted access to these resources.

Impact - This use case underscores the necessity for agile policy management within cloud environments, such as AWS, where database servers undergo regular updates and additions. It eliminates the need for manual policy adjustments every time a new database server instance is introduced, advocating for automation in policy updates, consistency in application, and efficiency in administration.

Evaluation Procedure - The process involves logging into and navigating through the interfaces of Zero Trust Platform vendors. The configuration challenge lies in the ability to integrate cloud-based tagged resources to be used natively in the security policy.

If it is not possible to import directly from cloud, create the tag object manually first ("use=prod-dataserver") A new rule is created. Name: "Allow database servers" Source: Production Web Servers (local object). Destination: object based on AWS tag "use=prod-dataserver". Service/application: SQL. Action: allow.

Observation and Rating –Cloud Service Providers Integration Use Case

Use Case 3	
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.	
3.6 ●	**Check Point** – The integration offers minimal permissions. This approach not only enhances efficiency but also significantly reduces the risk of misconfiguration. By requiring minimal permissions, the integration avoids the necessity of granting the System Under Test (SUT) access to the entire cloud environment, limiting access strictly to necessary areas. This targeted access strategy effectively minimizes the potential impact, or blast radius, in the event of a security breach.
3.0 ◕	**Cisco** – Lacks minimal permissions integration, necessitating additional steps for administrators to incorporate cloud objects into the rule base. This process involves creating an internal object with specific matching conditions before rule establishment, increasing complexity and potential for misconfiguration. Despite these challenges, its overall effectiveness remains commendable.
2.5 ◕	**Fortinet** – Like Cisco, 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** – Provides minimal permissions integration but also requires additional steps for adding cloud objects to the rule base, including the creation of internal objects with match conditions. This complexity may lead to misconfiguration.
1.5 ◑	**Zscaler** – The feature for importing AWS tags is limited to the creation of access rules from AWS resources to the internet. This potential for misconfiguration contributes to the subpar overall effectiveness.

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 Delegated Management

Description - This use case involves enabling branch administrators to manage localized access control and URL filtering policies within a defined scope, such as editing specific rules (e.g., rules 7-10) while having read-only access to the remainder. It aims to empower local admins to manage their gateway's policy, access logs, and perform troubleshooting, all within the guardrails set by central management. The objective is to decentralize certain administrative responsibilities, allowing branch admins to tailor URL filtering policies to their specific needs without affecting security protocols established by the central security administrator.

Impact - The primary goal of this use case is to alleviate the workload on central security administrators by granting branch admins autonomy over their local URL filtering policies. This approach ensures that branch-specific needs can be addressed more efficiently, without compromising the integrity of the overall security framework. It allows for a more responsive and flexible security posture at the branch level, enhancing the organization's ability to adapt to local challenges while maintaining a consistent, secure environment.

Evaluation Procedure - The process involves access interfaces to assess how each platform supports delegated administration capabilities. The evaluation will focus on the ability of branch admins to independently manage and modify their URL Filtering polices, including view the full configuration and applying changes within their purview. It is crucial that branch admins are restricted from altering any system-wide settings or overriding the central security polices, particularly those pertaining to the blocking of hazardous sites. The effectiveness of each platform in facilitating these segregated responsibilities without compromising on security or oversight will be examined.

Observation and Rating – Delegated Management Use Case

Use Case 4	
Delegated Management - To streamline operations and offload responsibilities from the central security administrator, it is desirable to empower branch administrators with the ability to manage their URL filtering policies. This empowerment should come without the risk of them overriding overarching security policies set by the main security administrator.	
3.5 ●	**Check Point** – Offers a straightforward configuration process, allowing for the creation of sub-domains and sub-policies to establish clear boundaries, or "guard rails," which local administrators cannot override. These administrators have visibility over the entire configuration but are restricted to modifying only their specific areas of responsibility. The system's overall effectiveness is praised for its simplicity and ease of use.
1.5 ◑	**Cisco** - Supports the creation of guard rails through sub-domains and sub-policies, though the configuration process is notably more complex and poses a risk of connectivity issues. This approach is feasible only when a local gateway exists at the branch, limiting the local administrator's ability to modify guard rails while granting them visibility and the ability to adjust other rules beyond URL filtering within their domain. It requires improvements in configuration simplicity.
2.5 ◕	**Fortinet** - Presents a complex configuration challenge, lacking the capability to establish guard rails for local administrators. This setup allows local admins to modify the entire URL policy, introducing a potential for misconfiguration due to the necessity of separate logins and users to access different parts of the gateway. It demands enhancements in configuration manageability.
2.8 ◕	**Palo Alto Networks** - Features a configuration process criticized for its tediousness, primarily due to the absence of a default read-only permissions setting. The platform does not support the creation of effective guard rails for local administrators, who can alter any URL filtering configuration. While the risk of misconfiguration is low, the repetitive nature of the process detracts from its overall effectiveness.
1.0 ◔	**Zscaler** - Similarly does not provide the capability to limit branch administrators exclusively to managing URL filtering policies. Branch admins are given extensive configurational control, including policies on cloud app, file type, and mobile access control, among others. Although they can prevent the branch admin from overriding the main admin policy, it requires setting up a new policy.

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 Malicious Website Protection

Description - In this use case, a user is visiting a malicious site with the ability to hijack his workstation and subsequently breach the organization. The objective is to protect against this type of attack.

Impact - The focus of this evaluation is to both evaluate the ease-of-use of configuring best-practices to prevent web-based attacks and, to check the effectiveness of the SUT in preventing them.

Evaluation Procedure - The procedure involves logging in and accessing the interfaces of the product under evaluation. The evaluation will assess each vendor's interface for ease of use and effectiveness by creating a threat protection policy as an administrator using the vendor's recommended best practices and simulating a user attempting to visit a malicious website. This is achieved by directing the user to web pages containing HTML with malicious JavaScript (JS) and PDF files embedded with malicious content, to test the policy's redundancy and effectiveness.

This comprehensive evaluation aims to identify which vendor offers the most user-friendly and efficient solution for preventing the execution of zero-day ransomware files, thereby enhancing organizational security. A blend of traffic 66% malicious HTML and 33% malicious PDF files was used for this testing.

Observation and Rating – Malicious Website Protection Use Case

Use Case 5	
Malicious Website Protection - After a user inadvertently triggered a zero-day ransomware attack which cost the organization millions, the imperative is clear: such an incident must be prevented from occurring. A blend of traffic 66% malicious HTML and 33% malicious PDF files was used for this testing.	
3.6 ●	**Check Point** – The interface is user-friendly, requiring minimal adjustments to establish a robust policy. The likelihood of misconfiguration is low, contributing to its commendable overall effectiveness. Check Point proved a 100% total block rate for malicious HTML and PDFs.
1.5 ◑	**Cisco** – Navigating the interface proves challenging due to its complex structure, featuring numerous menus and configuration pages. This complexity increases the risk of accidental missteps, negatively impacting its overall effectiveness. Cisco proved a 36% total block rate for malicious HTML and PDFs. We were unable to configure the Cisco firewall to block malicious HTML files for this testing, but Cisco did achieve a 97% block rate for the PDF component of this test. We are investigating this issue with Cisco.
1.3 ◔	**Fortinet** – The administration interface is straightforward, though the policy creation process involves navigating through several menus, which could potentially lead to errors. Fortinet proved a 30% total block rate for malicious HTML and PDFs.
2.0 ◑	**Palo Alto Networks** - Users may find the interface bewildering, with a plethora of menus and pages complicating the policy setup process. This complexity detracts from the system's overall effectiveness. Palo Alto Networks proved a 32.5% total block rate for malicious HTML and PDFs.
2.5 ◕	**Zscaler** – While the interface is user-friendly it requires additional steps for policy management, which introduces the possibility of errors. Nonetheless, the platform maintains an acceptable level of overall effectiveness. Zscaler proved an 80% total block rate for malicious HTML and PDFs.

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 Phishing Protection

Description - Phishing websites pose a significant threat to organizational security. This use case explores a proactive approach to safeguarding an organization from such threats by utilizing admin-generated rules to block access to phishing sites, alongside implementing educational measures for users on recognizing and avoiding phishing attempts.

Impact - The primary goal of this use case is to assess the user-friendliness and navigational efficiency of the interfaces provided by various vendors. Additionally, it aims to evaluate the effectiveness of each vendor in blocking phishing websites based on admin-enacted rules.

Evaluation Procedure - Administrators will log in and navigate the interfaces of Zero Trust Platform vendors. They will proceed to create a rule specifically designed to block phishing websites. Following the rule implementation, any attempts by users to access such sites will be blocked, and users will be educated on the dangers of phishing. Vendors will be assessed on the ease with which these protective measures can be implemented, as well as their success rate in effectively blocking access to phishing websites.

Observation and Rating – Phishing Protection Use Case

Use Case 6	
Phishing Protection - In response to a zero-day attack facilitated via a phishing site, we have evaluated the ability to protect our network using actual phishing URLs from openfish.com and phishunt.io. The scores shown below are an average rating of the User & Admin Experience (UX) and the overall Security Efficacy.	
3.6 ●	**Check Point** – The interface is exceptionally user-friendly, requiring minimal settings to configure policies effectively. Although it did not achieve a perfect score, the likelihood of misconfiguration is low, ensuring a high overall effectiveness in blocking phishing attempts. Check Point proved a 100% total block rate for phishing URLs.
N/A ◑	**Cisco** – The GUI is straightforward, though setting up a policy necessitates some configuration. This risk of misconfiguration appears relatively low. However, we did experience inconsistent efficacy results. We observed 53% in this round of testing which used both openphish.com and phishunt.io. However, in September 2023 we independently observed a 99% efficacy using openphish.com. This is pending re-evaluation. We have removed this scoring item from Cisco for this evaluation as it would be unfair to penalize them.
3.2 ◕	**Fortinet** – Navigating the GUI is a breeze, with a few settings needed to establish policies. The simplicity of the interface significantly reduces the risk of misconfiguration, translating to strong overall effectiveness. Fortinet proved a 95.86% total block rate for phishing URLs.
3 ◕	**Palo Alto Networks** – The GUI is user-friendly, but policy creation requires more steps. A notable drawback is the absence of a block message, replaced by a generic browser error, which may diminish user experience. Despite this, the risk of misconfiguration is low, and overall effectiveness is considered acceptable. Palo Alto Networks proved a 96.55% total block rate for phishing URLs.
3.3 ◕	**Zscaler** – The GUI stands out for its ease of navigation and streamlined policy configuration. With a minimal but possible risk of misconfiguration, the platform still achieved a high overall effectiveness in protecting against phishing attacks. Zscaler proved a 97.24% total block rate for phishing URLs.

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 IPS Exception

Description - In this use case, a legitimate user's activity is erroneously blocked by an intrusion prevention system (IPS), identified as a false positive. The challenge for the administrator is to swiftly locate the blocking log and configure an exception to permit the previously blocked traffic.

Impact - Administrators frequently engage in troubleshooting and responding to user inquiries as part of their routine responsibilities. This scenario highlights the importance of user-friendly security logging and the straightforward creation of exceptions, highlighting the efficiency of administrative tools in managing security protocols.

Evaluation Procedure - This evaluation involves logging into and navigating the interfaces of various security vendors. The process begins when a user encounters a block message and reaches out to the help desk. Subsequently, the administrator is tasked with creating an exception for the specific protection rule that triggered the false positive, ensuring that the user's legitimate activities are no longer impeded.

Observation and Rating – IPS Exception Use Case

Use Case 7	
IPS Exception - In this situation where a user's legitimate activity is incorrectly blocked by an IPS as a false positive, the ease of managing and correcting this issue is essential for maintaining operational efficiency.	
3.5 ●	**Check Point** – The GUI is exceptionally user-friendly, requiring minimal configuration to establish a protection policy. The straightforward design minimizes the risk of misconfiguration, leading to high overall effectiveness.
2.3 ◑	**Cisco** – The GUI is accessible, yet setting up a protection policy demands some effort. There is a notable risk of misconfiguration.
3.5 ●	**Fortinet** – In this area, the GUI was intuitive, configuring a protection policy was hassle-free, thanks to the minimalistic approach to settings. This simplicity significantly reduces the likelihood of errors, contributing to its high effectiveness.
2.8 ◕	**Palo Alto Networks** - While the GUI is straightforward, the process to formulate a protection policy involves multiple steps. Its moderate overall effectiveness score is attributed to the chance of misconfiguration due to this complexity.
2.5 ◕	**Zscaler** – The interface is user-friendly, though crafting a protection policy necessitates a bit more effort. There is a moderate risk of misconfiguration, but despite this, its overall effectiveness remains commendable.

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**	

5.8 Email Protection

Description - This use case focuses on protecting users against phishing attempts via email, a prevalent vector for such attacks. The aim is to assess the effectiveness and user-friendliness of email security solutions in preventing phishing attacks.

This test also looks at Quishing, a new type of attack where a phishing link is encoded in a QR code. The user is tempted to scan this code with their phone, where they are statistically less protected – This could lead to credential theft and to a possible breach.

Impact - Email-based phishing is a widespread and insidious method of attack. Evaluating the ease of setup, the robustness of the security measures, and the simplicity with which users can recover emails mistakenly marked as phishing (false positives) is crucial.

Evaluation Procedure - Access the management interfaces of various securing solutions from leading vendors. Administrators are tasked with configuring these solutions to intercept and block phishing emails effectively.

An email containing a phishing link is dispatched. The security solution, following the administrator's configured rules, should automatically block this email, preventing it form reaching its intended target.

The phishing link is then converted into a QR code, which is embedded in a new email and sent again. The security system should consistently block this email as well, demonstrating its ability to thwart phishing attempts in varied forms.

This test assess the user-friendliness of the security solution, particularly its ability to empower users to recover emails wrongly identified as phishing threats (false positives) without necessitating intervention from an administrator. This examines the balance between strict security measures and the flexibility required for effective email management strategies.

Observation and Rating – Email Protection Use Case

Use Case 8	
Email Protection - To safeguard users from phishing attacks via email, a comprehensive evaluation of various vendors reveals distinct levels of protection and capabilities.	
3.5 ●	**Check Point** – Stands out with multiple layers of defense, including NGFW, Email, Mobile, Endpoint, and SSE, uniquely capable of thwarting Quishing (QR Code Phishing) attacks. Its advanced AI-driven phishing prevention feature, "Zero-Phishing," minimizes the likelihood of misconfiguration. The high overall effectiveness highlights Check Point's robust protection across multiple fronts.
3.0 ◕	**Cisco** - Offers diverse layers of security encompassing NGFW, Email, Mobile, Endpoint, and SSE. Despite its comprehensive protection, Cisco lacks AI phishing prevention and fails to block Quishing attacks. This poses a risk for users scanning QR codes with unprotected devices, potentially leading to credential leaks.
3.0 ◕	**Fortinet** – Mirrors Cisco's security layers but also lacks AI phishing prevention, sharing the same vulnerability to Quishing attacks. This vulnerability underscore the importance of protecting mobile devices against potential credential theft. The low likelihood of misconfiguration point to Fortinet's reliable but not foolproof defense.
2.5 ◕	**Palo Alto Networks** – Provides a broad spectrum of protection, including NGFW, Mobile, Endpoint, and SSE, enhanced by AI phishing prevention, However, it falls short in blocking Quishing Attacks, leaving users at risk of credential leaks via mobile scans. The low risk of misconfiguration but incomplete phishing defense is reflected in its overall effectiveness.
2.0 ◑	**Zscaler** – Relies on a singular layer of defense without AI phishing prevention, showing vulnerability users scanning QR codes on unprotected devices might face credential leaks. The likelihood of misconfigurations is noted, with a decent overall effectiveness, indicating Zscaler's potential for bolstering its phishing defense mechanisms.

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 Clientless ZTNA

Description - This use case is designed to facilitate secure access for remote users to corporate resources using their own devices (BYOD). Initially, when a user accesses an internal server through a web browser from the office, the administrator sets up a policy on the on-premises gateway to permit web access to this server, allowing the user to navigate to the Production FTP server. For remote work scenarios, such as a user working from home, the administrator needs to enable access from the user's personal computer without compromising security. Access is granted only when specific criteria are met, including user's identity, user's location, browser type and more. Subsequently, the user logs into the SASE portal from their browser and access the same server as they would from the office.

Impact - The shift towards remote work has underscored the necessity for flexible yet secure access to corporate assets from any location or device. This use case addresses the critical balance between enabling productivity for remote employees and third-party contractors while maintaining strict security measures to protect sensitive corporate information.

Evaluation Procedure - Administrators log in and navigate the interfaces of the products evaluated. The process begins with the administrator creating a policy on the on-premises gateway that allows access to an internal server. Then, a user can access this internal server via a browser. To accommodate remote access from the personal and unmanaged devices, the administrator establishes a policy on the SASE platform that enables connection to the internal server, incorporating strict access control based on posture checks. These checks validate the user's location, the time and date of access, the operation system type and version, and the browser type used. Finally, the user can connect to the internal server using their personal device, ensuring secure and seamless access to corporate resources regardless of their physical location.

Observation and Rating – Clientless ZTNA Use Case

Use Case 9	
Clientless ZTNA - Enable secure remote access to corporate resources from unmanaged devices.	
3.5 ●	**Check Point** – Administrators can effectively create posture profiles for clientless users and configure all necessary criteria. The user portal presents a clear overview of accessible applications, minimizing the risk of misconfiguration highlight its high overall effectiveness rating.
2.8 ◕	**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.
0.0 ○	**Fortinet** – Currently, Fortinet does not offer support for secure, private access to internal applications for clientless users.
2.4 ◑	**Palo Alto Networks** – Administrators face challenges in fulfilling the task requirements and configuring necessary criteria for clientless users. However, its user portal does provide a clear view of allowed applications. The likelihood of misconfiguration is high.
1.8 ◑	**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. 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**	

5.10 Remote Users Browsing Experience

Description - This use case outlines the process where an administrator implements SSL Inspection along with Threat Prevention to oversee and secure web traffic. Subsequently, a user engages in downloading various file types and sizes from SharePoint, followed by utilizing internet speed testing tools to evaluate the integrity and speed of their connection. This exercise is crucial for assessing the performance and dependability of the secure connection.

Impact - In the context of the escalating significance of remote work for contemporary organizations, reliability and speed are non-negotiable for operational continuity. The central objective of this use case is to empower remote employees to execute their tasks efficiently and securely from any geographical location.

Evaluation Procedure - The evaluation involves interfacing with security solutions from leading vendors. The procedure commences with the administrator setting up SSL Inspection and configuring a threat prevention directive for web traffic. The user then initiates a practical test of the configured rules by downloading a variety of file types and sizes from SharePoint. Additionally, the user employs internet speed testing tools to verify the stability and speed of the connection, thereby confirming the efficacy of the security measure in a remote working scenario.

Observation and Rating – Remote Users Browsing Experience Use Case

Use Case 10	
Remote Users Browsing Experience - Enhancing remote work speed and security	
3.7 ●	**Check Point** – Streamlines the remote working experience by enabling on-device internet protection via split tunneling configuration, with SSL Inspection and Threat Prevention activated by default. This approach ensures a superior user experience characterized by direct internet connectivity, yielding a swifter and more fluid online interaction with minimal risk of misconfiguration. The simplicity and efficiency of Check Point's solution are noteworthy, making it an effortless and straightforward choice for ensuring secure and rapid remote access.
3.5 ●	**Cisco** – Facilitates a smooth remote work setup by allowing administrators to establish a secure private access policy that incorporates predefined rules and configurations. This user-friendly interface significantly reduces the likelihood of misconfiguration and promotes an uncomplicated, intuitive experience. Cisco stands out for its straightforward design, ensuring that remote work is both secure and effortlessly managed. We noted it took more effort than should have been required to configure the SUT for remote browsing experience.
1.5 ◑	**Fortinet** – Fortinet's approach requires administrators to implement a policy for internet access and configure an endpoint profile with advanced threat protection settings. Moreover, due to the cloud Points of Present (PoP) routing, users may experience suboptimal performance. The additional configuration steps introduce a higher probability of misconfiguration, rendering a mediocre overall effectiveness rating.
2.8 ◕	**Palo Alto Networks** – Administrators using Palo Alto Networks need to create a decryption policy to inspect all web traffic, create a new Profile Group and excluding the default File Blocking profile to allow legitimate files to be downloaded by the user. Additionally, policies for threat prevention must be applied. Like others that route through cloud PoP, the user experience can suffer. The intricacy of the necessary configurations increased the risk of misconfiguration, which may compromise the platforms' overall efficacy.
2.0 ◑	**Zscaler** – Administrators are tasked with creating rules to inspect all web traffic and additional sandbox rules for scanning specific file types. Disabling default configurations is necessary to enable comprehensive scanning of Office 365 traffic. The routing of traffic through cloud PoP can diminish the user experience. Consequently, the overall effectiveness of Zscaler's platform might fall short of the ideal, particularly in scenarios demanding high-performance standards.

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 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.