Hybrid Mesh Network Security

Security Efficacy Competitive Assessment

Detailed Lab Report for Check Point Software

April 2026
DR260112G
miercom.com/checkpoint

Table of Contents

1.0 Executive Summary 3

2.0 Hybrid Mesh Network Security Testing Summary Results 8

3.0 Security Effectiveness 9

3.1 Malware Prevention and Detection 9

3.2 Malicious Phishing URLs Prevention and Detection 11

3.3 Intrusion Prevention System (IPS) Efficacy 13

3.3.1 All CVE 13

3.3.2 CISA Known Exploited Vulnerabilities 14

4.0 Weighted Secure Browsing Speed 15

5.0 Risk Exposure 16

6.0 Products Tested 17

7.0 Test Setup 19

7.1 Miercom Advanced Offensive Threat Detection 21

7.2 VirusTotal 21

7.3 Testing Environment 22

About Miercom 23

Use of This Report 23

1.0 Executive Summary

In 2026, vendors are adopting hybrid mesh network security architectures that unify firewalls, SASE, and cloud security under a single policy framework to address the growing complexity of securing distributed enterprise networks.

While this architectural shift promises simplified management and consistent protection across environments, it also raises the bar for security effectiveness. To independently validate how leading vendors perform in this new model, Check Point engaged Miercom to evaluate hybrid mesh network security solutions in a controlled, comparative test.

Miercom conducted competitive security effectiveness testing of Check Point's Hybrid Mesh Network Security against products from Cisco, Fortinet, Palo Alto Networks and Zscaler. Comprehensive testing was conducted with all vendors' security services enabled, challenging each solution's ability to detect and block the latest malware. Modern threats like web-based malware attacks, targeted phishing attacks, application-layer attacks increase the threat level against organizations globally. The majority of new malware and intrusion attempts exploit weaknesses in applications, as opposed to networking components and services.

✓ Terms used in this report include **Prevention** vs. **Detection**. Prevent means malware was blocked. Detect-Only means malware was identified but not blocked.

Each product was configured according to the vendor's best practices.

Extensive Testing

Over three months, Miercom conducted continuous testing by downloading sets of 1,000 files from VirusTotal. These samples included DOCX, XLSX, PDFs, EXEs, DLLs, and archived files. Each solution was evaluated using anti-virus, IPS, anti-bot, URL filtering (URLF), sandboxing, and AI/ML-powered security engines, with testing conducted concurrently across all vendors.

Known Exploited Vulnerabilities (KEVs)

Miercom analyzed Common Vulnerabilities and Exposures (CVEs) listed in the Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) Catalog. This metric provides insight into product security and quality, as vulnerabilities included in CISA's KEV Catalog are actively exploited in real-world attacks. Organizations prioritize fixing these known vulnerabilities, as they are prime targets for hackers worldwide. These vulnerabilities can lead to significant operational costs due to necessary patches and remediation efforts. *(See Section 5.0)*

Intrusion Prevention System (IPS)

IPS block rate was evaluated using BreakingPoint, Keysight Technologies' network security testing platform that simulates real-world traffic, including cyberattacks. This assessment measured how effectively each solution detects and mitigates threats while maintaining

Secure Service Edge (SSE)

This report also evaluates the security efficacy of Secure Service Edge (SSE), commonly referred to as *Firewall-as-a-Service (FWaaS)*. Previous annual reports focused on on-premises and network firewalls. However, with the rise of the Hybrid Mesh Firewall architecture (as defined by Gartner), this 2025 report provides a holistic view of all three Hybrid Mesh Firewall use cases—On-premises, Cloud, and FWaaS.

Phishing

A comprehensive test of thousands of known threat actors operating phishing campaigns, as recorded by sites such as VirusTotal, OpenPhish, Fishtank, and others, was conducted, and every active phishing attack was tested on all vendors.

To validate the results, the last stage of the process was done manually.

Once a phishing site was confirmed active, an engineer followed up by simulating sensitive data being entered to see whether the security solution that was tested would recognize the threat at any point in the process.

Weighted Secure Browsing Speed

Miercom measured network performance with next-generation firewall protections enabled, focusing on connection and file download speeds to determine the potential impact of security enforcement on the end-user experience, which can cause issues such as latency, connection establishment delays, and poor application responsiveness. *(See Section 4.0)*

In this report, **Zero+1 Day** Malware (**up to 24 hours** past Zero-Day discovery) refers to newly discovered malware on the first day after discovery. These malware samples are less likely to be known by any vendor's signature detection mechanisms in the first 24 hours.

Key Findings

Critical Prevention Rate in the first 24 hours: Check Point led the group in immediate prevention of total malware samples. The first 24 hours of a malware campaign are the most dangerous, and this is the critical time to stop an attack before it quickly spreads and creates widespread damage. A security system with a higher block rate in the first 24 hours means an enterprise will be able to stop threats in real-time, minimizing the risk of data breaches, downtime, and damage from advanced persistent threats (APTs). This proactive capability enhances organizational resilience, and ensures future-proof security in an ever-evolving threat landscape.

- **Malware Prevention vs. Detection:** Check Point prevented 99.9% of new malware from a comprehensive set of file types including DOCX, XLSX, PDFs, EXEs, APKs, DLLs and archived files that were no more than **24 hours** old.

  Check Point led with the highest score preventing 99.9% of malware downloads.
  Palo Alto Networks had 66.1% prevention and 12.1% detect-only.
  Fortinet had 69.9% prevention.
  Cisco had 68.4% prevention and 10.4% detect-only.
  Zscaler had 64% prevention.

- **Remote User Malware Prevention (SSE):**

  Check Point led with a 99.8% total block rate.
  Cisco had a 97% total block rate.
  Fortinet had a 66.8% total block rate.
  Palo Alto Networks had a 65.4% total block rate.
  Zscaler had a 64% total block rate.

- **Phishing Prevention:** Recent phishing URLs confirmed active were used to evaluate detection performance across multiple vendors' security solutions. Because phishing campaigns are short-lived and URLs often go online and offline quickly, the results highlight the limitations of static URL filtering databases and the advantage of AI systems capable of analyzing page behavior and content in real time.

  Check Point proved to have the best overall prevention against phishing URLs, making use of (R82) advanced AI deep learning capabilities.

  Check Point led with a 100% prevention rate with no missed URLs.
  Palo Alto Networks had a 98.48% prevention rate with five missed URLs.
  Zscaler had a 94.5% prevention rate with 19 missed URLs.
  Fortinet had an 87.8% prevention rate with 41 missed URLs.
  Cisco had a 16% prevention rate with 279 missed URLs.

- **Remote User Phishing Prevention (SSE):**

  Check Point led with a 99.7% prevention rate with one missed URL.
  Zscaler had a 94.5% prevention rate with 18 missed URLs.
  Palo Alto Networks had a 92.8% prevention rate with 22 missed URLs.
  Fortinet had an 86.6% prevention rate with 41 missed URLs.
  Cisco had a 25.8% prevention rate with 227 missed URLs.

- **Intrusion Prevention System:** BreakingPoint IPS is a network security testing tool designed to simulate real-world traffic, including cyberattacks, to evaluate and optimize performance of IPS.

  Check Point led with a 99.49% block rate.
  Fortinet had a 94.18% block rate.
  Palo Alto Networks had an 92.56% block rate.
  Cisco had an 87% block rate.

- **Intrusion Prevention System: (CISA KEV)**

  Check Point led with a 99.87% block rate.
  Fortinet had a 97.5% block rate.
  Palo Alto Networks had an 89.36% block rate.
  Cisco had an 86.73% block rate.

- **Weighted Secure Browsing Speed:**

  Speed Test:

  Check Point led with an average of 1.12 Gbps.
  Palo Alto Networks had an average of 491 Mbps.
  Fortinet had an average of 72 Mbps.
  Cisco had an average of 503 Mbps.
  Zscaler had an average of 559 Mbps.

  File Download Test:

  Check Point led with an average of 74.9 ms for 10MB file / 7.07 ms for 1MB file.
  Fortinet had an average of 511 ms for 10MB file / 18.7 ms for 1MB file.
  Cisco had an average of 377.2 ms for 10MB file / 3.1 ms for 1MB file.
  Palo Alto Networks had an average of 283 ms for 10MB file / 20 ms for 1MB file.
  Zscaler had an average of 132.7 ms for 10MB file / 20.6 ms for 1MB file.

- **Cybersecurity and Infrastructure (CISA) Known Exploited Vulnerabilities (KEV):** CISA maintains the KEV Catalog, an authoritative repository of vulnerabilities that have been exploited in real-world cyberattacks. These figures reflect the number of known exploited vulnerabilities associated with each product as documented in the CISA KEV Catalog.

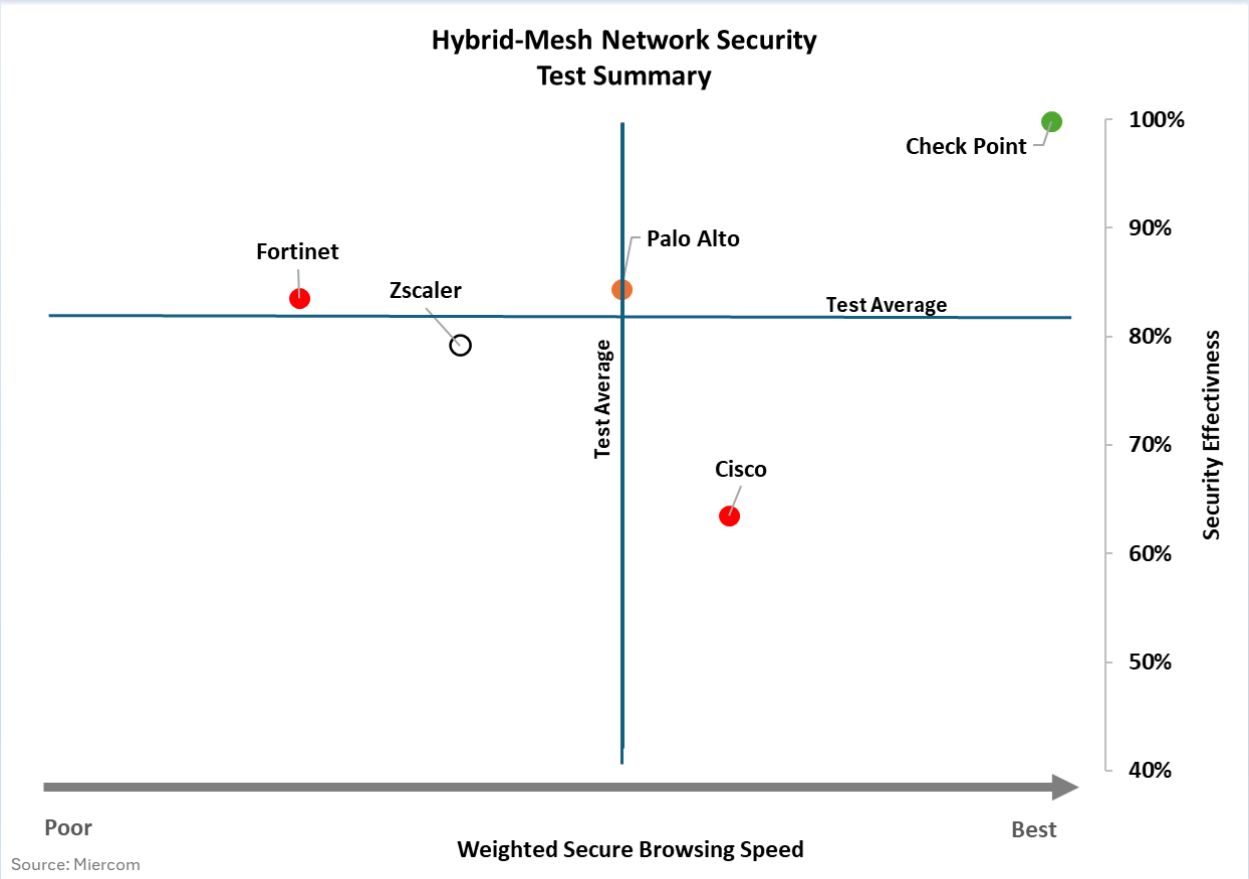
  Check Point ranked the best with only 1 KEV.
  Palo Alto Networks has 13 KEVs.
  Fortinet has 24 KEVs.
  Cisco has 30 KEVs.
  As a SASE vendor, Zscaler's score is not applicable since the solution is fully managed by the vendor, eliminating the need to report KEVs.

Check Point's Hybrid Mesh Network Security is recognized as the leading vendor in the Miercom Security Efficacy Competitive Assessment, achieving 99.79% overall security effectiveness and outperforming competitive solutions in multiple real-world network scenarios. Check Point's leadership in securing hybrid enterprise environments was clearly demonstrated in this evaluation. Check Point's Hybrid Mesh Network Security has earned the **Miercom Certified Secure** award.

Robert Smithers
CEO
Miercom

2.0 Hybrid Mesh Network Security Testing Summary Results

The grid below summarizes the results of all the tests run in the Hybrid Mesh Network Security evaluation. The vendors are placed on the grid based on their security effectiveness and weighted secure browsing speed. Their dot is color coded based on their risk exposure which is determined by the number of CVEs listed in CISA Known Exploited Vulnerability (KEV) for each vendor.



Low Risk: < 5 CVEs **Medium Risk: 6 – 10 CVEs** **High Risk: 11 - 19 CVEs** **Very High Risk: 20+ CVEs**

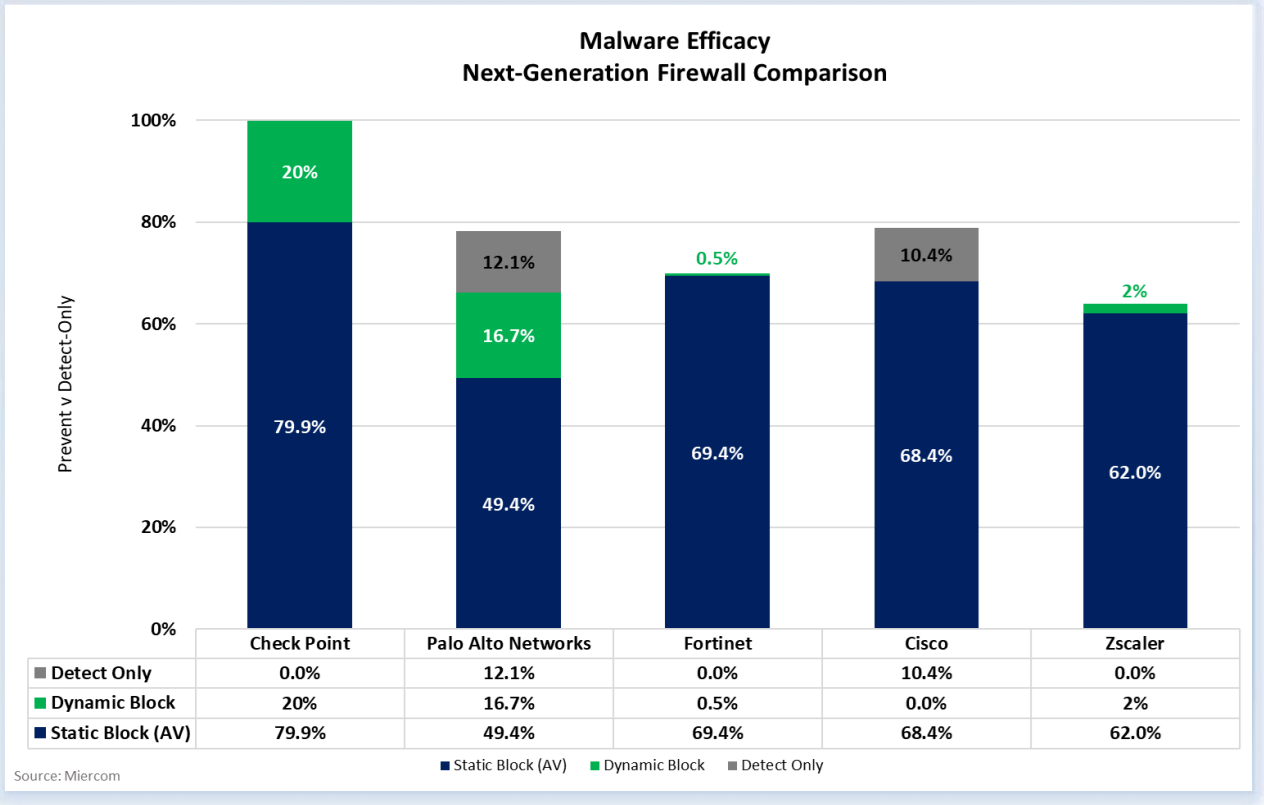
Hybrid Mesh Network Security Testing Summary					
Test Case	**Check Point**	**Palo Alto Networks**	**Fortinet**	**Zscaler**	**Cisco**
Security Effectiveness	99.79%	84.4%	83.53%	79.16%	63.52%
Weighted Secure Browsing Speed	9.5	5.5	2.5	4	6.5
Risk Exposure	**Low Risk** 1 CVE	**High Risk** 13 CVEs	**Very High Risk** 24 CVEs	N/A	**Very High Risk** 30 CVEs

3.0 Security Effectiveness

3.1 Malware Prevention and Detection

This year, Miercom strengthened the criteria for malicious file inclusion. The evaluation used newly observed malware samples from the previous 24 hours that were detected by nine security engines, compared to last year's threshold of 25 engines on VirusTotal, a platform that aggregates results from many security vendors. Lowering the detection threshold allows earlier-stage and less widely recognized malware to be included, making detection more challenging because these samples are identified by fewer security products. This approach better reflects the current threat landscape, where new malware variants appear rapidly as attackers adopt artificial intelligence.

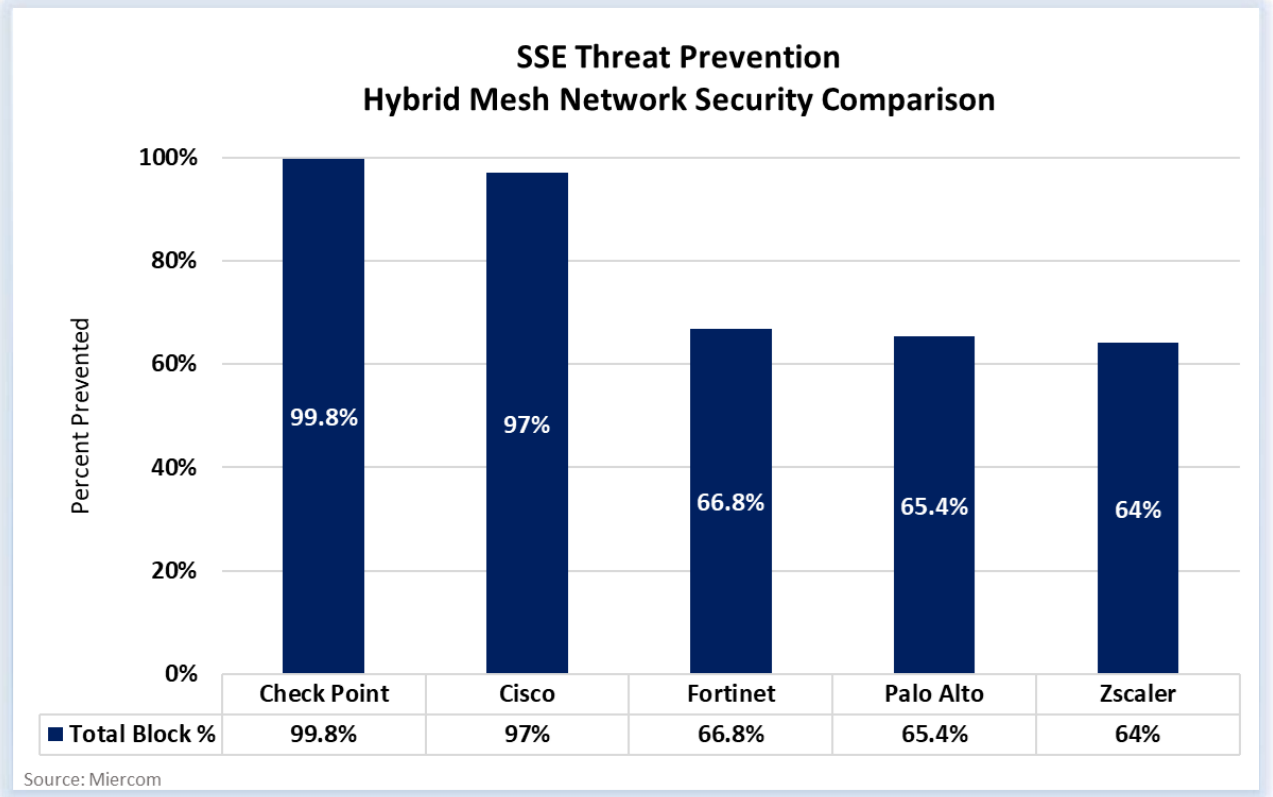
Summary of Hybrid Mesh Network Security Test Results: Blocking and Detection Efficacy comparing test results from recently discovered malware between products.



*The chart above shows how each vendor's firewall performed in Static and Dynamic **Prevention** vs. **Detection-Only**. Static Block means the solution identified malware using a signature (local or cloud) and immediately blocked it from entering the network. **Dynamic Block** means the solution identified and blocked malware by dynamically analyzing the file, using either sandboxing or AI/ML engines. **Detect-Only** means the solution identified malware but did not prevent malware from entering the network. Note that vendors did not get an opportunity to configure their own products, but each product was configured according to the vendors' best practices.*

New Variant Malware Prevention success rate: In this Malware test, Check Point prevented over 99.9% of malware from a large set of files and file types including executables, documents, and archives. Zscaler, Fortinet, Palo Alto Networks and Cisco had prevention rates of 64%, 69.4%, 66.2%, and 68.4% respectively.

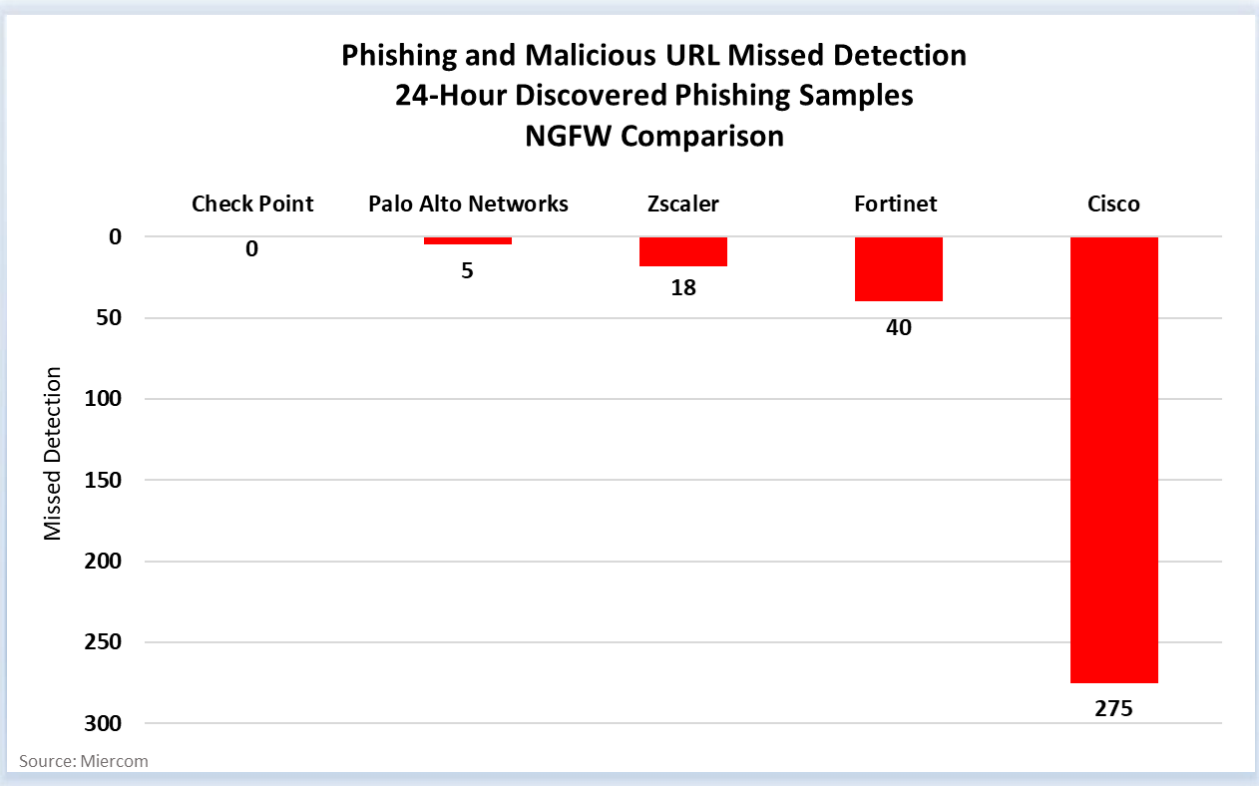
Summary of Hybrid Mesh Network Test Results: Secure Service Edge Threat Prevention comparing test results for security efficacy for the SSE use case – also known as Firewall-as-a-Service (FWaaS).



The chart above shows the performance of each vendor's solution in the SSE Threat Prevention test case. This evaluation measured the effectiveness of SSE FWaaS capabilities in blocking malware threats. While previous annual reports focused on On-premise and Cloud Network Firewalls, this assessment aligns with the evolving Hybrid Mesh Firewall architecture. It provides a comprehensive view across all three deployment models: On-premises, Cloud, and FWaaS.

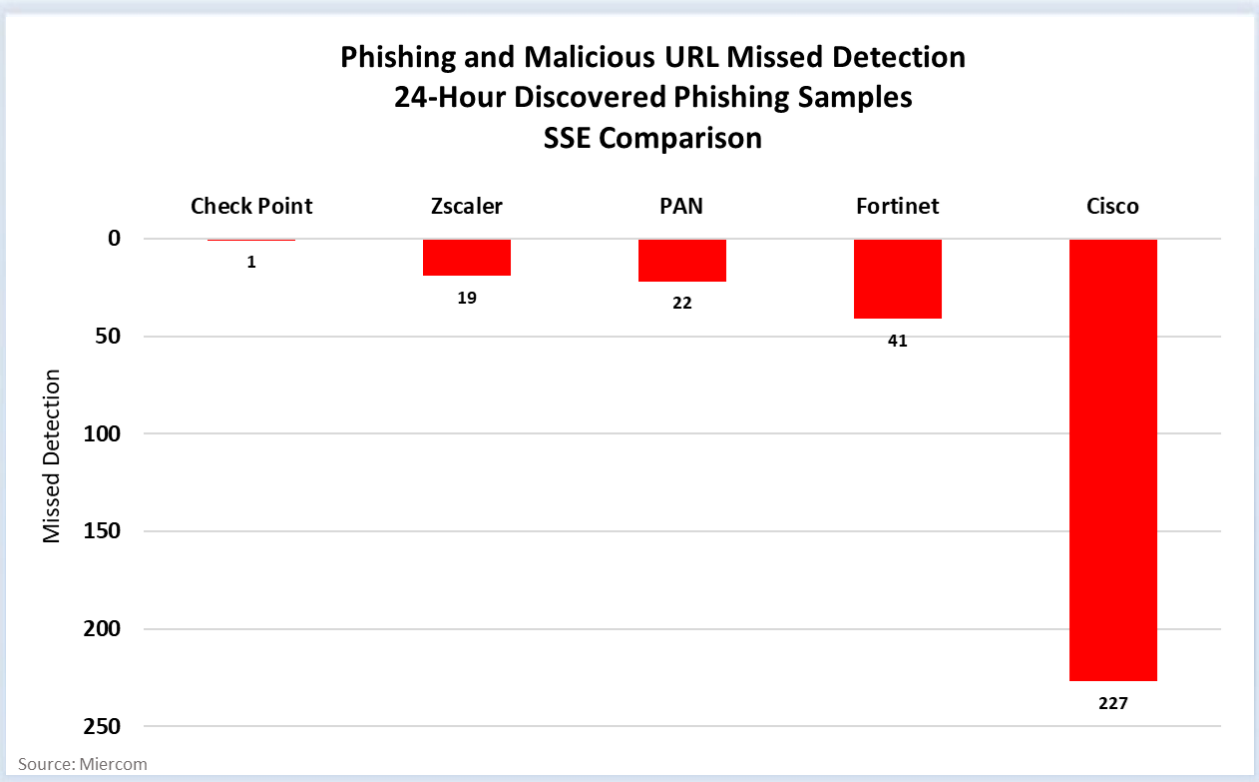
3.2 Malicious Phishing URLs Prevention and Detection

Summary of Hybrid Mesh Firewall Test Results: Blocking and Detection Efficacy based on results from recently discovered phishing attacks.



Missed phishing URLs, where lower is better. *The chart above shows how each vendor's product performs in blocking newly discovered phishing URLs* ***(excluding the first 24 hours; see phishing prevention section)****, with a focus on "live" AI-driven prevention of phishing and other malicious URLs. Check Point demonstrated not only static detection capabilities but also the ability to detect phishing websites dynamically using AI-based phishing protection, based on analysis of web page content such as corporate logos/icons, suspicious fields, irregular spellings, redirection, and many other malicious components of these websites. This dual-layer of protection (reputation-based and content analysis) for phishing detection is important, as many phishing websites change their IP address locations and domain names to defeat static reputation-based forms of protection.*

Summary of Hybrid Mesh Network Security Test Results: SSE Phishing and Malicious URL Detection comparing test results for security efficacy for the SSE use case – also known as Firewall-as-a-Service (FWaaS).



The chart above shows the performance of each vendor's solution in the SSE/SASE Threat Prevention test case. This evaluation measured the effectiveness of SSE FWaaS capabilities in blocking malware threats. While previous annual reports focused on On-premise and Cloud Network Firewalls, this assessment aligns with the evolving Hybrid Mesh Firewall architecture. It provides a comprehensive view across all three deployment models: On-premises, Cloud, and FWaaS

3.3 Intrusion Prevention System (IPS) Efficacy

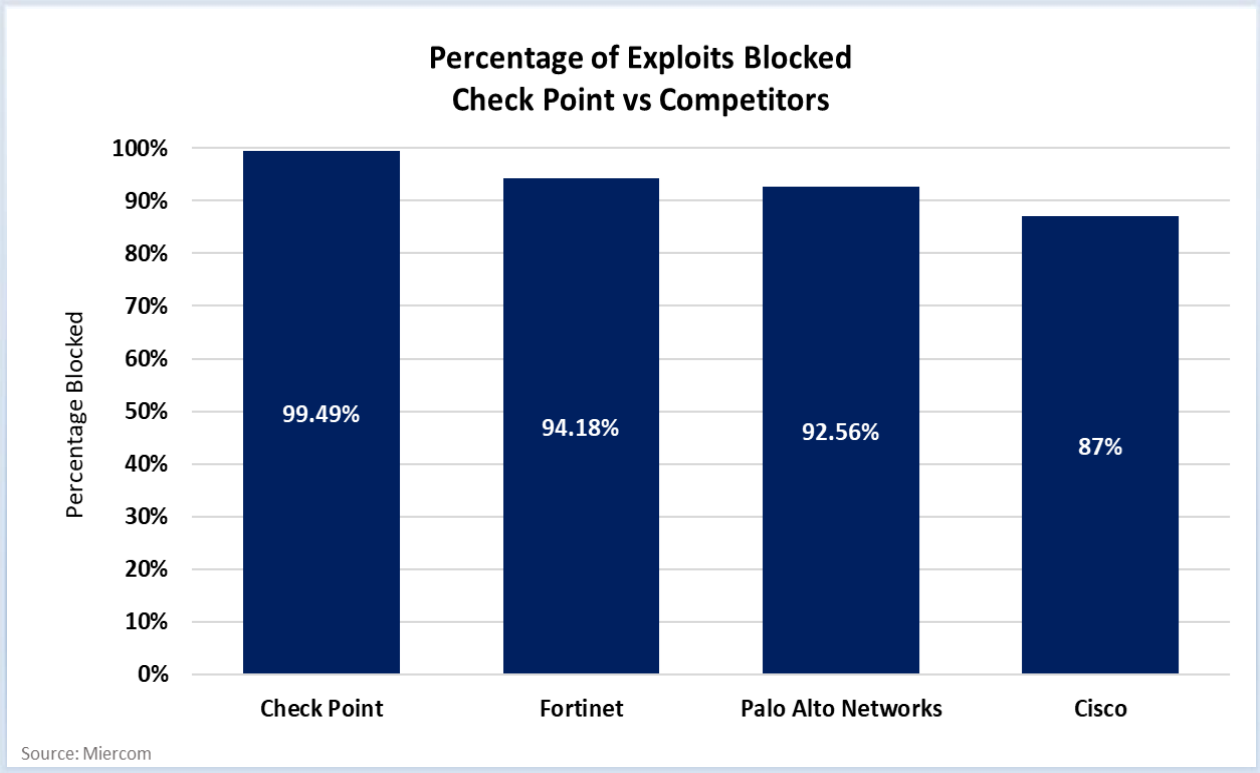
This section summarizes the effectiveness of the Intrusion Prevention System (IPS) capabilities of Hybrid Mesh Network Security solutions. Testing was conducted using BreakingPoint network security testing platform, which simulates enterprise traffic and exploit attempts. The evaluation measured the ability to detect and block exploit traffic associated with known vulnerabilities.

Two exploit datasets were used during testing. One dataset included CVEs with Critical, High and Medium severity levels. The second dataset includes CVEs listed in the CISA KEV catalog.

3.3.1 All CVE

This test used BreakingPoint strike list containing exploits mapped to CVEs with Critical, High and Medium severity levels published since 2017. The objective was to evaluate the ability of each solution to detect and block a broad set of known vulnerabilities.

Results represent the percentage of exploit attempts successfully blocked during testing.



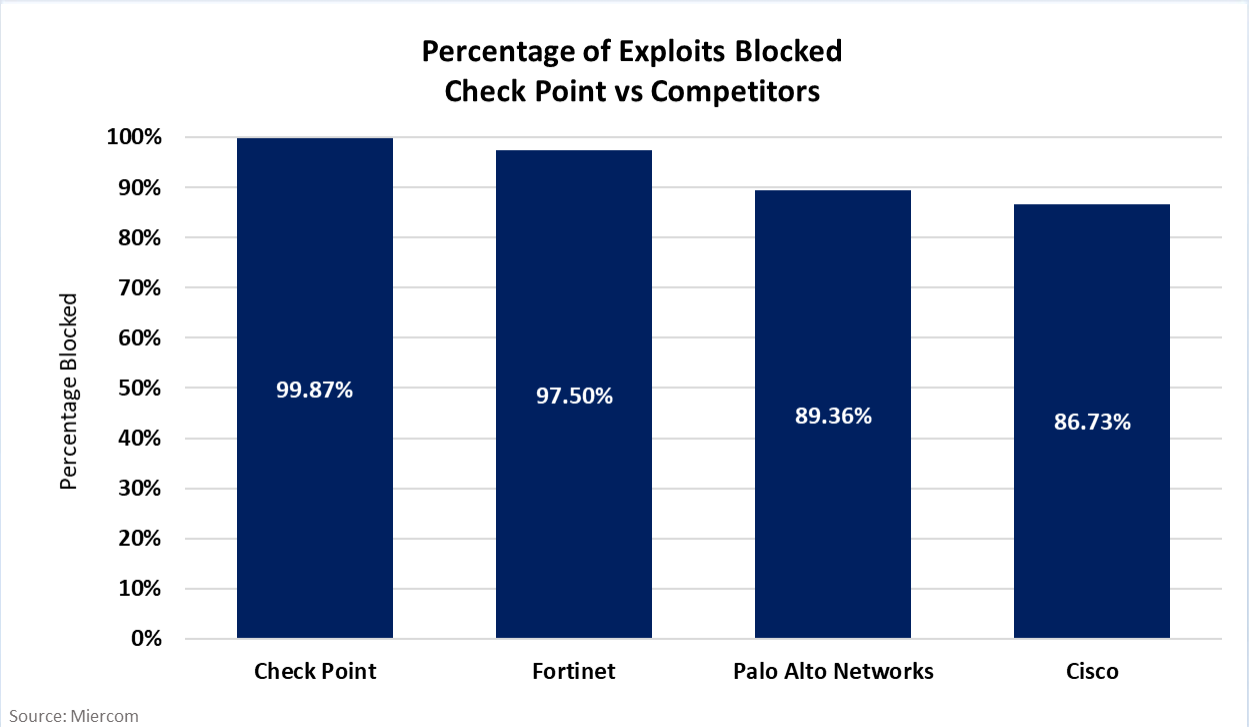
This chart shows how effectively each vendor blocks BreakingPoint exploits at High and Critical threat levels since 2017. Check Point leads with a score of 99.49% block rate, followed by Fortinet with 94.18%, Palo Alto Networks with 92.56%, and Cisco with 87%.

As a SASE vendor, Zscaler's score is not applicable since the solution is fully managed by the vendor, eliminating the need to report KEVs.

3.3.2 CISA Known Exploited Vulnerabilities

This test used a BreakingPoint strike list containing exploits mapped to vulnerabilities listed in the CISA KEV catalog. These vulnerabilities have been observed to be actively exploited.

Results represent the percentage of exploit attempts successfully blocked during testing.



This chart shows how effectively each vendor blocks BreakingPoint exploits mapped to vulnerabilities listed in the CISA KEV catalog. Check Point leads with a 99.87% block rate, followed by Fortinet with 97.5%, Palo Alto Networks with 89.36%, and Cisco with 86.73%.

As a SASE vendor, Zscaler's score is not applicable since the solution is fully managed by the vendor, eliminating the need to report KEVs.

4.0 Weighted Secure Browsing Speed

Summary of Enterprise and Hybrid Mesh Firewall Test Results: SSE/SASE Performance comparing test results for speed and file download for the SSE use case.

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

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

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

Speed and File Download Tests				
Check Point	**Americas**	**EMEA**	**APAC**	**Average**
fast.com / testmyspeed.com	1.2 Gbps	821 Mbps*	1.4 Gbps	**1.13 Gbps**
Cloudflare Speed Test	934 Mbps	1.4 Gbps	1.0 Gbps	
10MB xlsx / 1MB docx File Downloads	61.8 / 5.8 ms	77.8 / 9.2 ms	85 / 6.2 ms	**74.9 / 7.07sec**
Palo Alto Networks	**Americas**	**EMEA**	**APAC**	**Average**
fast.com / testmyspeed.com	770 Mbps	435 Mbps*	250 Mbps	**491 Mbps**
Cloudflare	869 Mbps	319 Mbps	302 Mbps	
10MB xlsx / 1MB docx File Downloads	344.4 / 19.4 ms	295.6 / 23.4 ms	209.4 / 17.2 ms	**283 / 20sec**
Fortinet	**Americas**	**EMEA**	**APAC**	**Average**
fast.com / testmyspeed.com	38 Mbps	56.4 Mbps*	78 Mbps	**72 Mbps**
Cloudflare	56 Mbps	79 Mbps	126 Mbps	
10MB xlsx / 1MB docx File Downloads	877.6 / 6 ms	353 / 28.6 ms	303 / 21.6 ms	**511 / 18.7sec**
Cisco	**Americas**	**EMEA**	**APAC**	**Average**
fast.com / testmyspeed.com	1.1 Gbps	931 Mbps*	680 Mbps	**503 Mbps**
Cloudflare	108 Mbps	76 Mbps	123 Mbps	
10MB xlsx / 1MB docx File Downloads	786.6 / 5.6 ms	60.6 / 5 ms	284.4 / 3.6 ms	**377.2 / 3.1ec**
Zscaler	**Americas**	**EMEA**	**APAC**	**Average**
fast.com / testmyspeed.com	920 Mbps	625 Mbps*	1.2 Gbps	**559 Mbps**
Cloudflare	210 Mbps	190 Mbps	210 Mbps	
10MB xlsx / 1MB docx File Downloads	982 / 24.6 ms	175.6 / 17.4 ms	212.6 / 19.8 ms	**132.7 / 20.6sec**

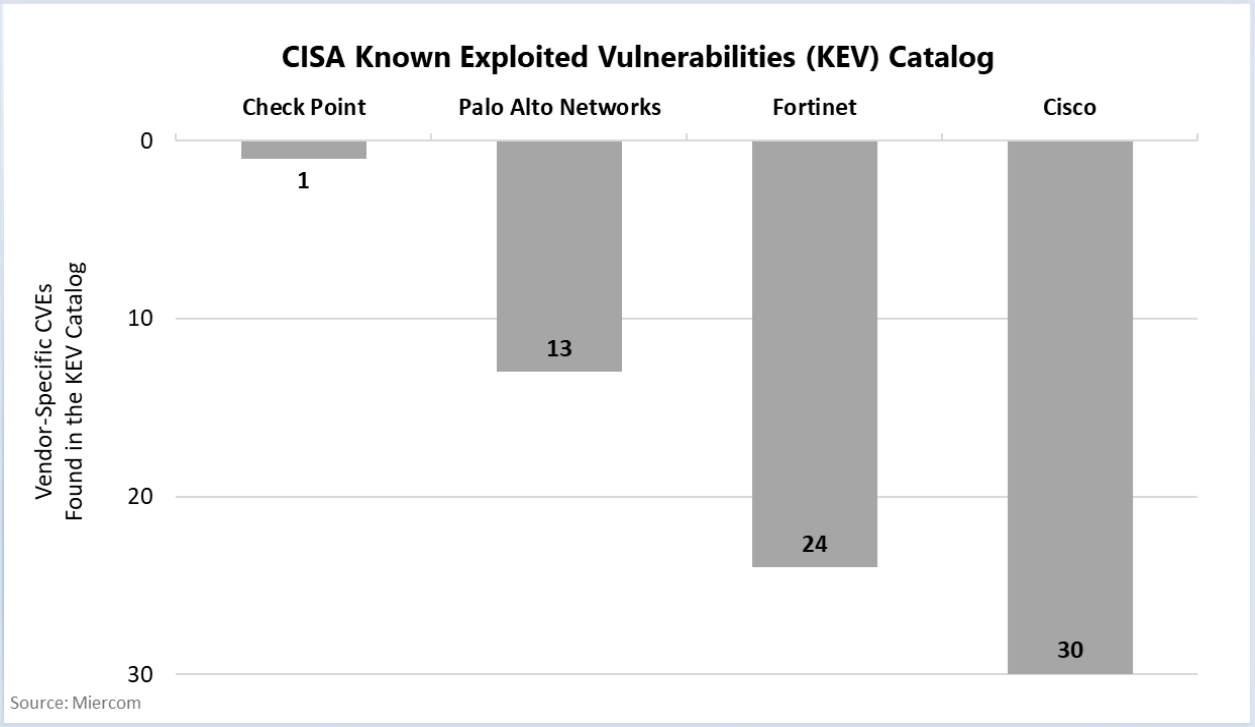
**fast.com results were inconsistent when testing Europe. testmyspeed.com was used instead.*

5.0 Risk Exposure

CISA maintains the KEV Catalog, an authoritative repository of vulnerabilities that have been exploited in real-world cyberattacks. This resource aids organizations in prioritizing vulnerabilities that pose significant risks due to active exploitation.

These figures reflect the number of known exploited vulnerabilities associated with each vendor's products as documented in the KEV Catalog. It is important to note that the presence of vulnerabilities can be influenced by factors like breadth of product portfolio, market share, and the complexities of the solutions offered by each vendor. Note that all gateways were configured in accordance with the vendor's best practices.

Organizations can stay informed about actively exploited vulnerabilities by regularly consulting the KEV Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog). Aiding in timely remediation efforts.



The chart above illustrates the total number vendor-specific CVEs identified in CISA's KEV Catalog. Check Point stands out for its exceptional security, with just one listed vendor-specific CVE.

As a SASE vendor, Zscaler's score is not applicable since the solution is fully managed by the vendor, eliminating the need to report KEVs.

6.0 Products Tested

Check Point

Check Point Next Generation Firewall, Version R82.10

Data sheet and specifications:
https://sc1.checkpoint.com/documents/R82.10/WebAdminGuides/EN/CP_R82.10_RN/Content/Topics-RN/Whats-New.htm
Best Practice Guide:
https://support.checkpoint.com/results/sk/sk111303

Check Point SASE

Data sheet and specifications:
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/SASE-Admin-Guide/Content/Topics-SASE-AG/Introduction/Introduction.htm
Best Practice Guide:
https://support.checkpoint.com/results/sk/sk111303

Palo Alto Networks

Palo Alto NGFW, Version 12.1.4

Data sheet and specifications:
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/ngfw/ngfw-release-notes-12-1.pdf
Best Practice Guide:
https://docs.paloaltonetworks.com/advanced-threat-prevention/getting-started/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasion

Prisma Access - Enterprise

Data sheet and specifications:
https://docs.paloaltonetworks.com/prisma-access/administration

Fortinet

FortiGate, Version 7.6.6

Data sheet and specifications:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-vm.pdf
Best Practice Guide:
https://www.plasmaticsun.com/blog/fortigate-best-practices-baseline

FortiSASE - Standard

Data sheet and specifications:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisase.pdf

Cisco Systems

Secure Firewall (FTD), Version 7.7.10

Data sheet and specifications:
https://www.cisco.com/c/en/us/products/collateral/security/firepower-ngfw-virtual/threat-defense-virtual-ngfwv-ds.html
Best Practice Guide:
https://sec.cloudapps.cisco.com/security/center/resources/firewall_best_practices

Cisco Secure Connect Advantage (Umbrella)

Data sheet and specifications:
https://www.cisco.com/c/en/us/products/collateral/plus-as-a-service/secure-connect-now-ds.html

Zscaler

Platform Version Saas, ZIA

Data sheet and specifications:
https://help.zscaler.com/zia/step-step-configuration-guide-zia
Best Practice Guide:
https://help.zscaler.com/zscaler-deployments-operations/zia-policy-leading-practices-guide

Vendor	Product	Version	Feature Bundles
Check Point	Next-Generation Firewall	R82.10	Sandblast
	Check Point SASE	SaaS	SASE - Internet Access Hybrid
Cisco	Secure Firewall	7.7.10	TMC
	Secure Connect	SaaS	Advantage
Fortinet	FortiGate	7.6.6	Enterprise
	FortiSASE	SaaS	Advanced
Palo Alto Networks	PAN-OS	12.1.4	Precision AI Network Security
	Prisma Access	SaaS	Enterprise
Zscaler	ZIA	SaaS	Transformation

7.0 Test Setup

Testing was designed to determine the strengths and weaknesses of each vendor's Hybrid Mesh Network Security offering. In addition to generating traffic patterns and attacks from industry test tools, we used unique, verified malicious samples for a customized, open-source approach. High prevention efficacy against this blend of malicious samples indicates well-rounded protection from multiple attack vectors.

Malware Prevention Test

Over the course of 90 days, we repeatedly downloaded sets of 1000 most recently submitted malicious files from VirusTotal, with over 9 engines with malicious verdict (high probability of being valid malware). These malicious samples consisted of DOCX, XLSX, PDFs, EXEs, DLLs and archived files. Each solution was assessed using Anti-virus, Anti-Malware, Anti-bot, URL Filtering (URLF), sandboxing, and AI/ML protection engines. Testing was run concurrently on each of the vendor's solutions.

For this year's test, the criteria for including malicious files was adjusted to better reflect the current threat landscape. Previously, only samples that were widely recognized as malicious by a large number of security engines were included. However, the rapid adoption of AI-assisted tools by attackers has made it significantly easier to generate large numbers of slightly modified malware variants. These variants often appear shortly after creation and may initially be detected by only a small portion of security products, despite being clearly malicious.

To better represent these early-stage threats, the minimum detection threshold was lowered — from files detected by at least 25 security engines to those detected by 9 or more on VirusTotal, a platform that aggregates results from many security vendors.

This change increases the difficulty of the test, as the included samples are less widely recognized and therefore more challenging for security solutions to detect and prevent.

Phishing Prevention Test

Recent phishing URLs confirmed to be active within approximately the past three months were used to evaluate detection performance across multiple vendors' security solutions.

The phishing URLs were sourced from VirusTotal and public lists, including PhishTank, OpenPhish, and the GitHub repository "Phishing-Database." Each URL was verified as both active and malicious using a script, reducing a pool of tens of thousands of suspected URLs to a few hundred confirmed live phishing URLs.

The resulting list of live phishing URLs was then tested against each solution to determine whether the URLs were blocked. URLs that were not blocked were subsequently inspected manually from a browser behind the relevant solution to trigger active or AI-based anti-phishing protections. This process determined whether the solution ultimately allowed access to the phishing URL.

Intrusion Prevention System Test

IPS block rate was evaluated using BreakingPoint, a cybersecurity and network testing platform designed to simulate real-world traffic, and security threats. This evaluation measured each solution's effectiveness in preventing medium to critical-severity (CVSS score 4-10) Common Vulnerabilities and Exposures (CVEs) published between 2017 to 2025 by using BreakingPoint's "Strikepack" tests.

Additionally, we evaluated the BreakingPoint CISA KEV catalog "Strikepack" bundle. This bundle includes all Strikepacks testing attacks from the CISA Known Vulnerability Catalog.

7.1 Miercom Advanced Offensive Threat Detection

Today's threat landscape is rapidly evolving with more complexity, requiring more offensive security and more dynamic methods of testing. Miercom's Advanced Offensive Security Testing incorporates scenario-driven methods to provide users with relevant data regarding their security readiness. These tests assess the ability of DUT to detect and prevent specific types of sensitive data from leaving the network without introducing performance degradation. Targeted traffic flows consist of emails that we generate to contain criteria such as user accounts, keywords, and randomized numeric strings formatted, like credit card numbers or tax identification numbers. Simulated targeted traffic is sent in simultaneously with real-world benign background traffic to evaluate detection efficacy and check for false positive detection.

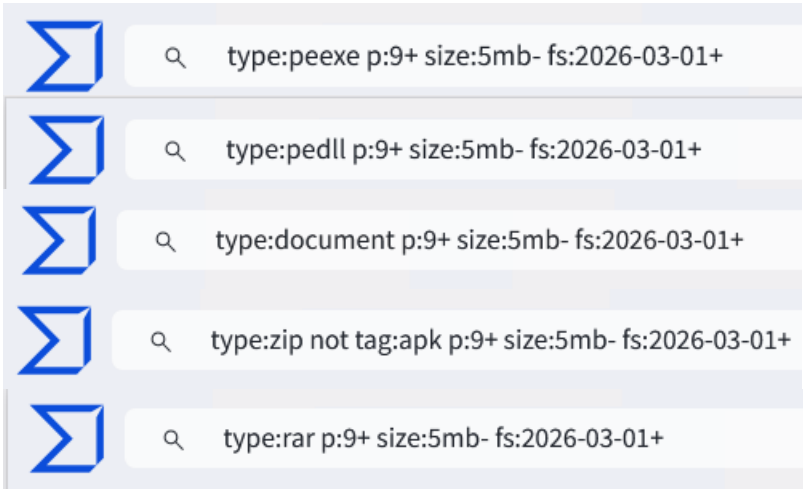
7.2 VirusTotal

Malware samples from VirusTotal were downloaded and later used for evaluating all the products.

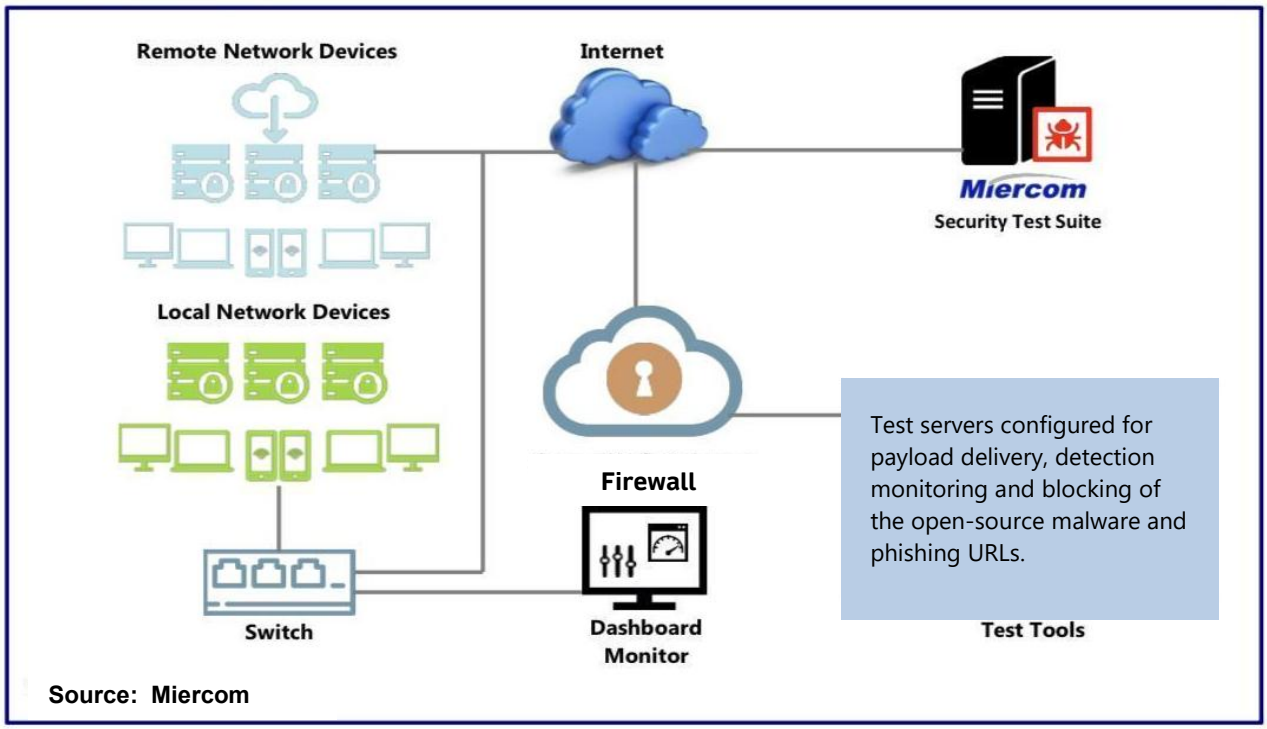
VirusTotal is a threat intelligence database that aggregates detections and reputation data on files, URLs, domains, and IP addresses from many security vendors and sources. Security teams use it to quickly look up suspicious indicators, validate alerts, enrich investigations with additional context, and identify related artifacts and campaigns by comparing results across multiple engines and data feeds.

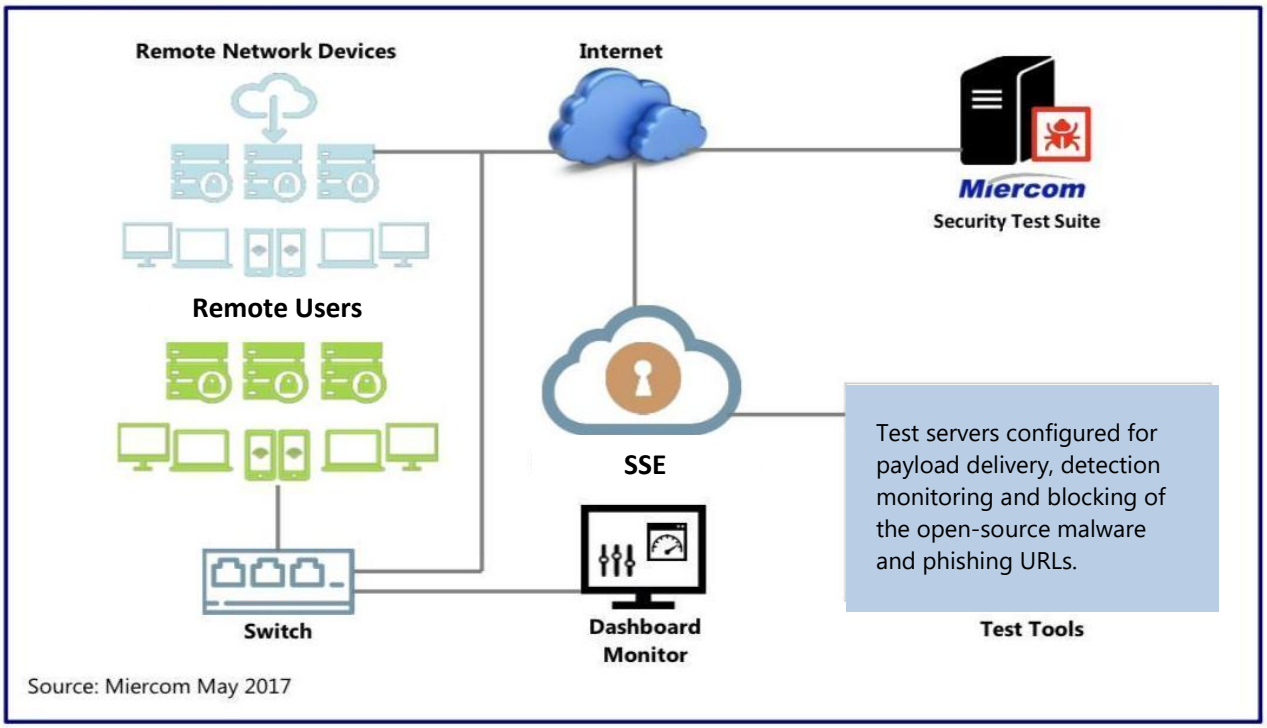
The rule set for selecting the VirusTotal samples features in testing is shown below. The sample set for Zero + 1 Malware consisted of hundreds of randomly selected, freshly submitted samples within 24 hours with at least 9 of VirusTotal's ~80 antimalware engines detecting it as malicious.

Examples of the rule set for selecting the VirusTotal samples are shown below:



7.3 Testing Environment





About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on 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.

© 2026 Miercom. All Rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the authors. Please email reviews@miercom.com for additional information.