Enterprise and Hybrid Mesh Firewall 2025 Q1

Security Efficacy
Competitive Assessment
Summary Lab Report

for

Check Point Software

3 February 2025
SR241113M

miercom.com/checkpoint

Table of Contents

1.0 Executive Summary

Miercom was engaged by Check Point to conduct competitive security effectiveness testing of the Check Point Enterprise and Hybrid Mesh Firewall compared to products from Cisco, Fortinet, Palo Alto Networks and Zscaler. Testing included verifying the effectiveness of anti-virus, anti-malware, anti-bot, URL Filtering (URLF), sandboxing, AI/ML and phishing protection engines.

Comprehensive testing was conducted with all vendors' security services enabled and challenged each solution's ability to detect and block the latest modern-day malware. Modern threats like web-based malware attacks, targeted phishing attacks, application-layer attacks, and others 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 **Prevent** vs. **Detect-Only**. Prevent means malware was blocked. Detect-Only means malware was identified but not blocked.

Extensive Testing

Over three months, Miercom conducted continuous testing by downloading sets of 500 files from Virus Total. These samples included: DOCX, XLSX, PDFs, EXEs, PowerShell and Bash scripts, APKs, DLLs and archived files. Each solution was evaluated using Anti-virus, IPS, Anti-bot, URLF, sandboxing and AI/ML-powered security engines. Testing was conducted concurrently across all vendors to assess their effectiveness in blocking modern cyber threats.

Known Exploited Vulnerabilities (KEVs)

Miercom analyzed the number of Common Vulnerabilities and Exposures (CVEs) listed on the Known Exploited Vulnerabilities (KEV) catalog maintained by CISA (Cybersecurity & Infrastructure Security Agency. This metric provides insight into product security and quality, as vulnerabilities included in CISA's KEV catalog are actively exploited in real-attacks. Organizations prioritize fixing these known vulnerabilities as they are prime targets for hackers worldwide. These vulnerabilities can lead to significant operational costs for organizations due to necessary patches and remediation efforts. *(See Section 2.4 for details.)*

Intrusion Prevention System (IPS)

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

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 cloud 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 Firewall-as-a-Service.

In this report, **Zero+1 Day** Malware (one day past Zero-Day discovery) means newly discovered malware on the first day of 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 for immediate prevention of the 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.

- **Zero+1 Day Malware Prevent vs. Detect:** Check Point prevented 99.9% of new malware from a comprehensive set of file types including DOCX, XLSX, PDFs, EXEs, PowerShell and Bash scripts, APKs, DLLs and archived files that were no more than one day old.
  - Check Point led with the highest score preventing 99.9% of malware downloads.
  - Palo Alto Networks had 62.7% prevention and 25.2% detect-only.
  - Fortinet had 87.8% prevention and 5.7% detect-only.
  - Cisco had 67.1% prevention and 7% detect-only.
  - Zscaler had 90.9% prevention and no detect only.
- **Zero+1 Day Malware Prevent (First to Block):**
  - Check Point led with a 99.9% prevention rate.
  - Palo Alto Networks had a 62.7% prevention rate.
  - Fortinet had an 87.7% prevention rate.
  - Cisco had a 67.1% prevention rate.
  - Zscaler had a 90.9% prevention rate.
- **Phishing Prevention:** Again, the first 24 hours are the most critical time to block attacks. 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 99.74% prevention rate with only one missed URL.
  - Palo Alto Networks had a 98.69% prevention rate with five missed URLs.
  - Fortinet had a 97.39% prevention rate with ten missed URLs.
  - Cisco had 55.87%. prevention rate with 169 missed URLs.
  - Zscaler had a 91.12% prevention rate with 34 missed URLs.

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

  Check Point led with a 99% total block rate.

  Palo Alto Networks had a 74% total block rate.

  Fortinet had an 84% total block rate.

  Cisco had a 96% total block rate.

  Zscaler had an 83% total block rate.

- **Cybersecurity and Infrastructure (CISA) Known Exploited Vulnerabilities:** These figures reflect the number of known exploited vulnerabilities associated with each vendor's product as well as how many KEVs they cover, as documented in the CISA KEV Catalog.

  Check Point ranked the best with only 1 known exploited vulnerability while providing coverage for 860.

  Palo Alto Networks has 11 known exploited vulnerabilities while providing coverage for 745.

  Fortinet has 16 known exploited vulnerabilities while providing coverage for 830.

  Cisco has 21 known exploited vulnerabilities while providing coverage for 756

  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.

- **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 98.0% average block rate.

  Palo Alto Networks had a 91.6% average block rate.

  Fortinet had a 94.6% average block rate.

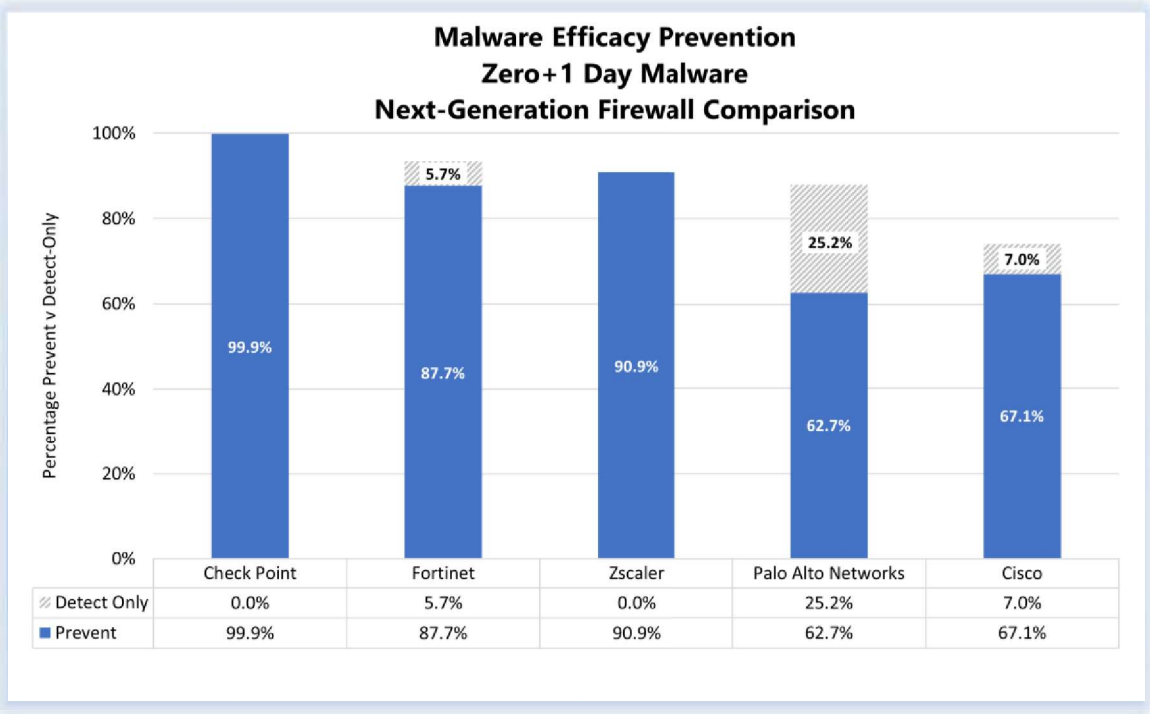
  Cisco had a 42.6% average block rate.

  Zscaler had a 72.5% average block rate.

2.0 Testing Summary Results

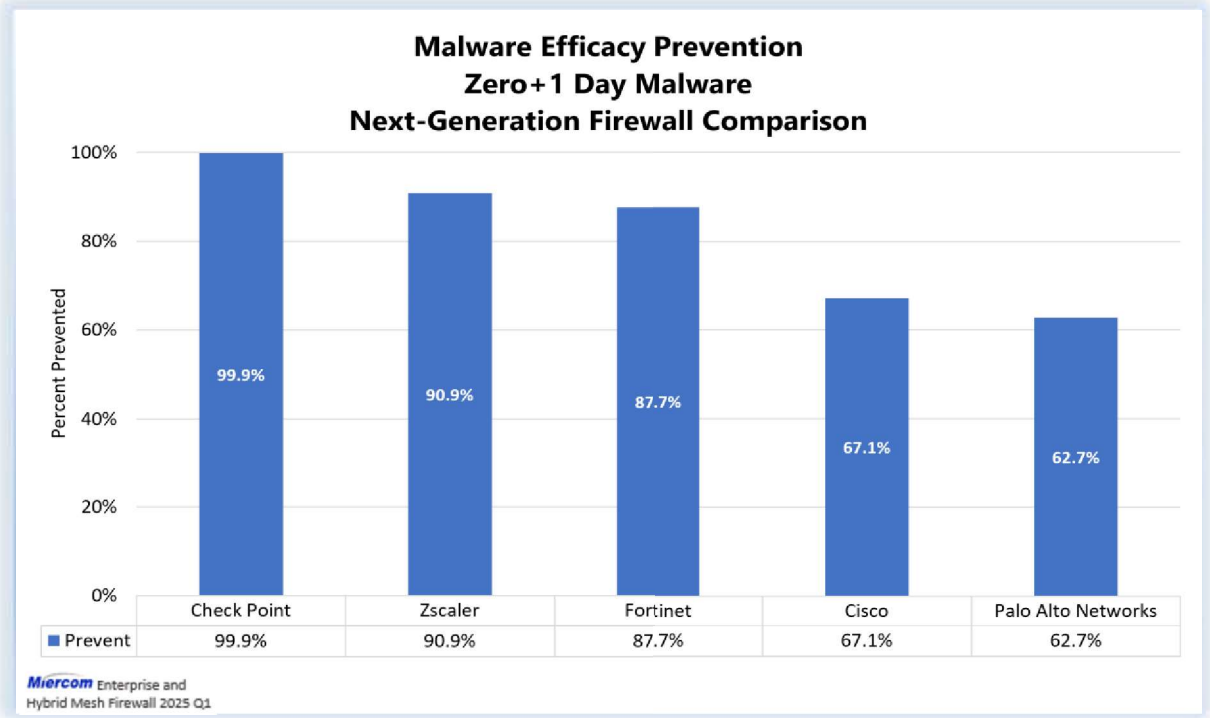
2.1 Malware Prevention and Detection Summary

Summary of Enterprise and Hybrid Mesh Firewall Test Results: Blocking and Detection Efficacy comparing test results from Zero+1 Day recently discovered malware between products.



*The chart above reflects how each vendor's firewall performed in **Prevention** vs. **Detection-Only** in the first 24 hours of an attack. **Prevent** means the solution identified malware and immediately blocked it from entering the network. **Detect-Only** means the solution identified malware but did not prevent that malware from entering the network. Note that vendors did not get an opportunity to configure their own products, but each product was configured to vendors' best practices.*

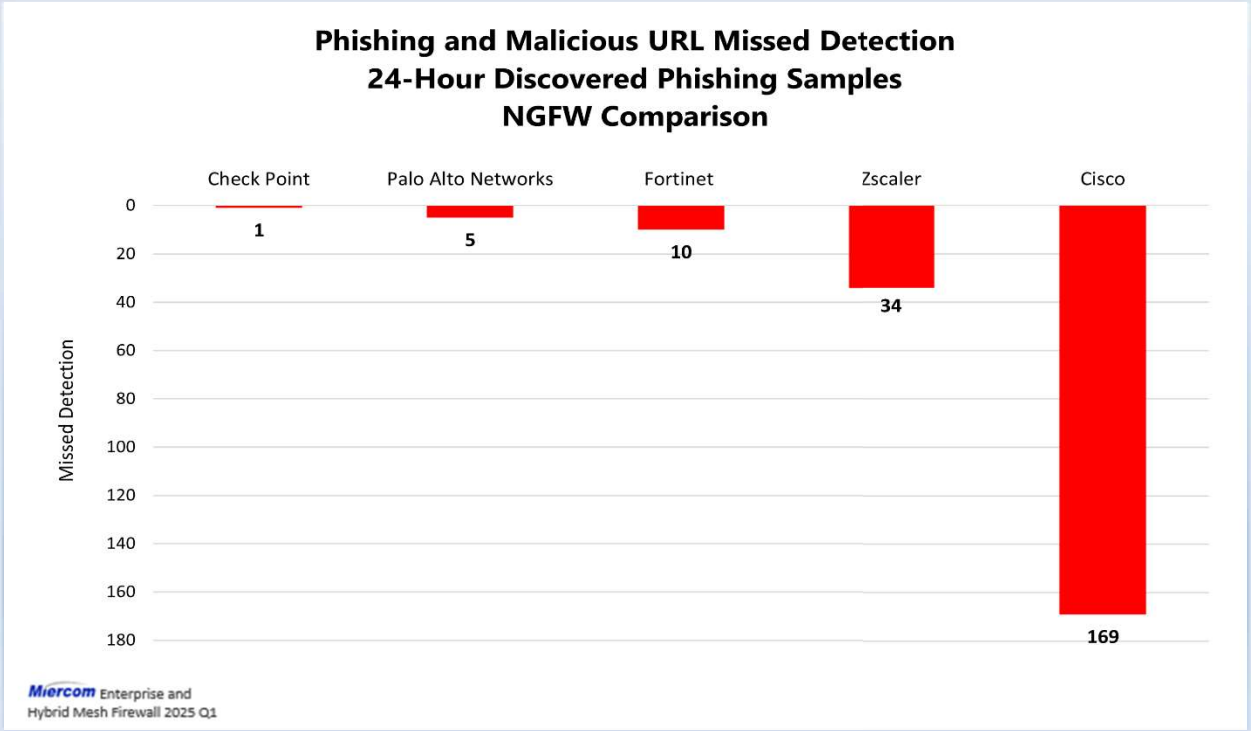
New Variant Malware Prevention success rate: In our Zero+1 Day Malware test, Check Point prevented over 99.9% of malware from a large set of files and file types including executables, documents, and archives. Fortinet, Zscaler, Palo Alto Networks and Cisco had prevention rates of 87.7%, 90.0%, 62.7%, and 67.1% respectively.



*This chart reflects how each vendor's firewall performed prevention in the first 24 hours of an attack. **Prevent** means the solution identified the malware and immediately blocked it from entering the network. Palo Alto Networks and Cisco had a false positive rate of 4.75%.*

2.2 Malicious Phishing URLs Prevention and Detection Summary

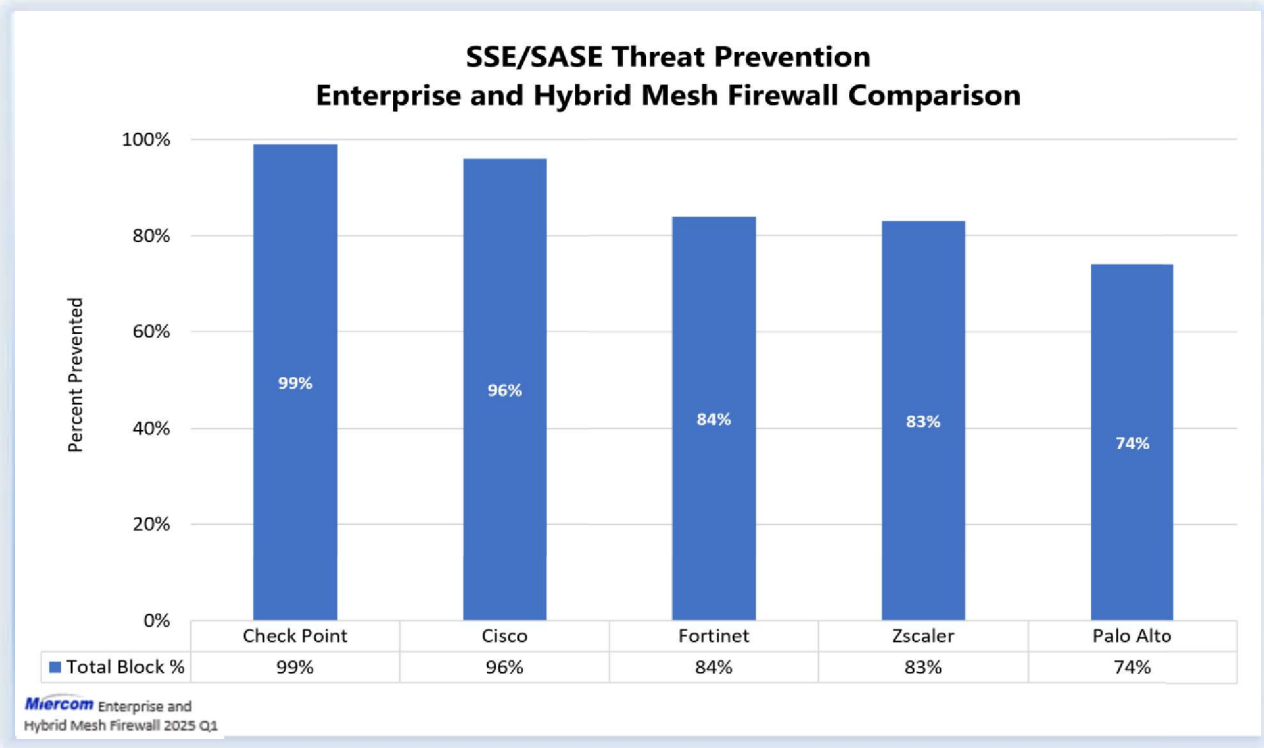
Summary of Enterprise and Hybrid Mesh Firewall Test Results: Blocking and Detection Efficacy comparing test results from recently discovered phishing and other malicious URLs.



Missed malicious URLs, less is better. *The chart above shows how each vendor's product performs in Detecting and Preventing newly discovered (less than 24-Hour known) phishing and other malicious URLs. Check Point demonstrated not only static detection ability but could also detect phishing websites dynamically with AI-based phishing protection, based on analysis of web page content such as corporate logos/icons, suspicious fields, irregular spellings, redirection, and many other obscured maleficent components of these websites. This double 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. In previous Miercom testing of a related product, Cisco Secure Access solution, Cisco achieved a 98% block rate for malicious URLs upon 24-hour retest when configured with Maximum Detection settings. Note this was a different environment for an SSE evaluation and was not an enterprise and hybrid mesh firewall only review as reflected in this report. This note is included for clarity and transparency.*

2.3 SSE/SASE Threat Prevention

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



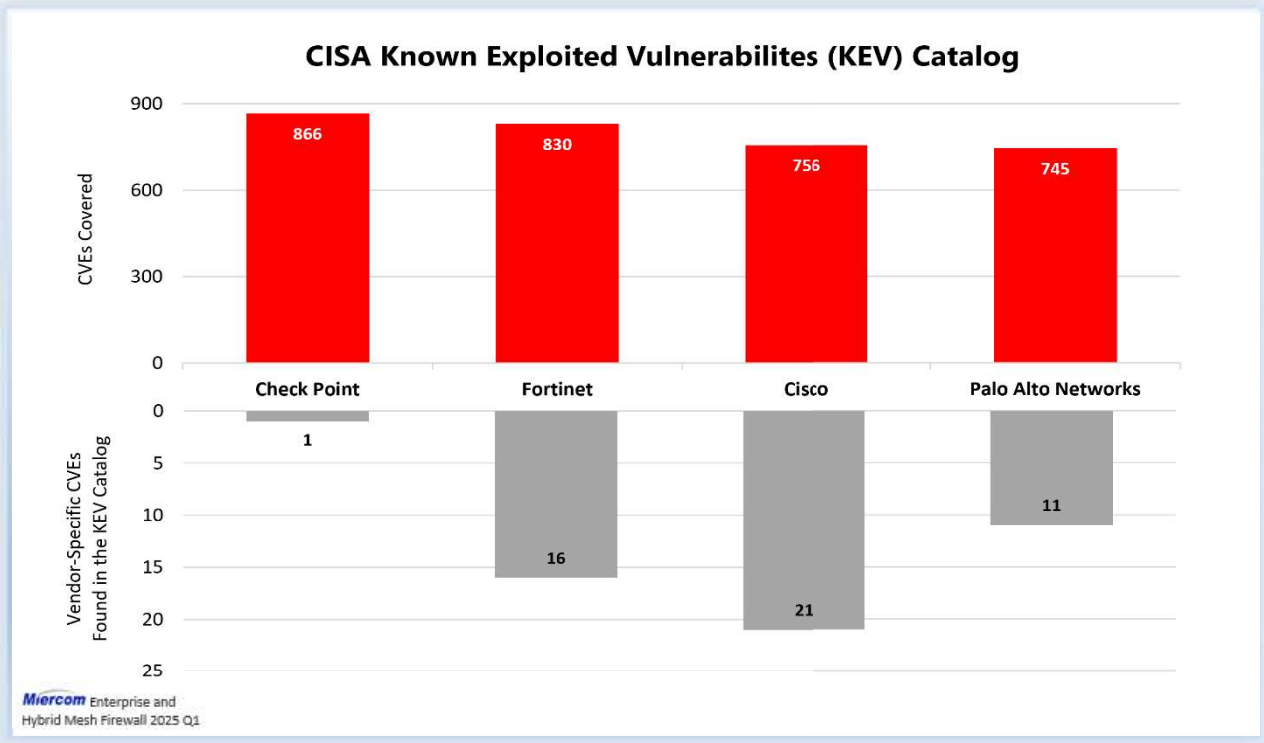
The chart above shows the performance of each vendor's solution in the SSE/SASE Threat Prevention test case. This evaluation measured the effectiveness of Secure Service Edge (SSE) Firewall-as-a-Service (FWaaS) capabilities in blocking malware threats. While previous annual reports focused on on-premise 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 Firewall-as-a-Service.

2.4 CISA KEV Evaluation

The Cybersecurity and Infrastructure Security Agency (CISA) maintains the Known Exploited Vulnerabilities (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.

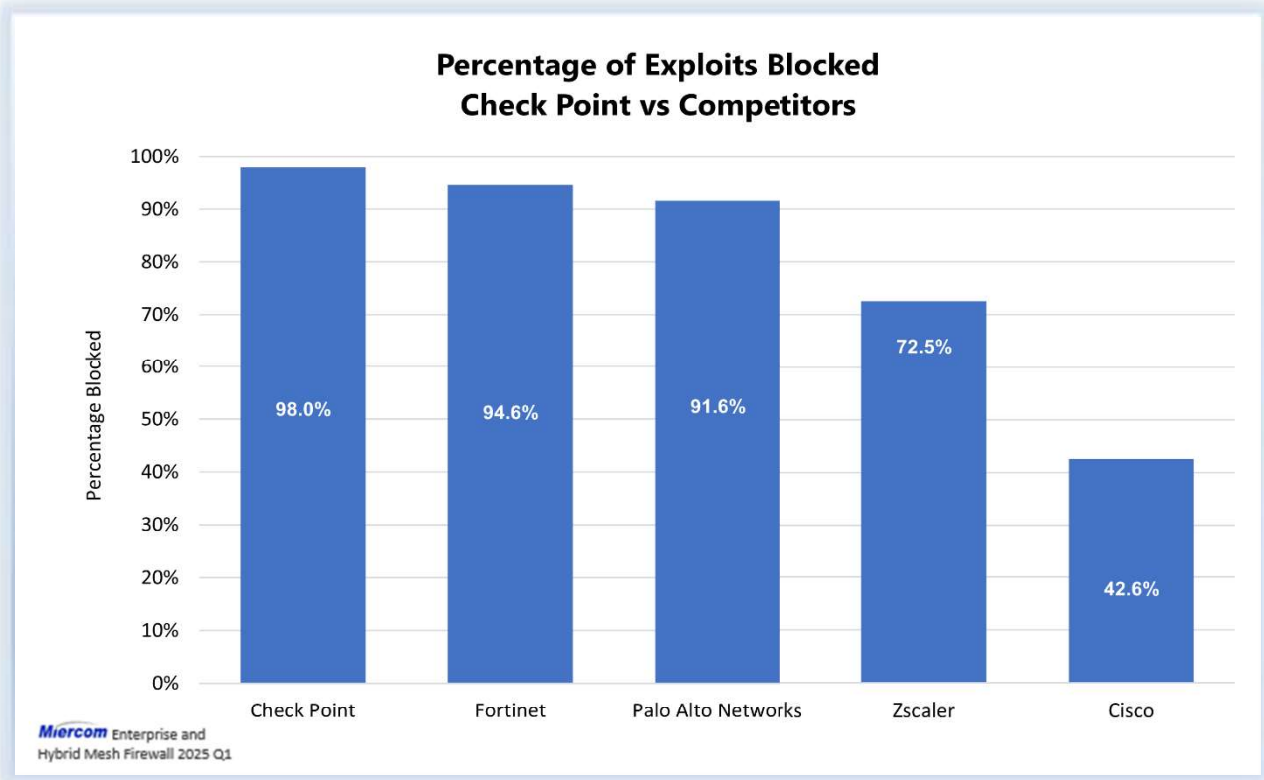
Organizations can stay informed about actively exploited vulnerabilities by regularly consulting the KEV Catalog (https://www.cisa.gov/known-exploited-vulnerabilities-catalog). Aiding in timely remediation efforts.



The chart above illustrates the total number of CVEs in CISA's KEV Catalog that each vendor has mitigated (red) alongside the vendor-specific CVEs identified in the catalog (gray). Check Point stands out for its exceptional security, with just one listed vendor-specific CVE and an impressive coverage of 866 CVEs listed in the catalog.

2.5 Intrusion Prevention System Testing Summary

Summary of Enterprise and Hybrid Mesh Firewall Test Results: Intrusion Prevention System comparing test results from Breaking Point, a network security testing tool designed to simulate real-world traffic, including cyberattacks, to evaluate and optimize performance of IPS.



This chart shows how effectively each vendor—Check Point, Fortinet, Palo Alto Networks, Cisco, and Zscaler—blocks Breaking Point exploits at High and Critical threat levels from the last three years. Check Point leads with a 98% average block rate, followed by Fortinet with 94.6%, Palo Alto Networks with 91.6%, Zscaler with 72.5%, and Cisco with 42.6%.

3.0 Products Tested

Check Point

Quantum NGFW, Version R82
Data sheet and specifications:
https://sc1.checkpoint.com/documents/R82/WebAdminGuides/EN/CP_R82_RN/CP_R82_ReleaseNotes.pdf

Harmony SASE – Essentials+
Data sheet and specifications:
https://sc1.checkpoint.com/documents/Infinity_Portal/WebAdminGuides/EN/SASE-Admin-Guide/Content/Topics-SASE-AG/Introduction/Introduction.htm

Palo Alto Networks

Palo Alto NGFW, Version 11.2.3
Data sheet and specifications:
https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/11-2/pan-os-release-notes/pan-os-release-notes.pdf

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

Fortinet

FortiGate, Version 7.6.0
Data sheet and specifications:
https://docs.fortinet.com/document/fortigate/7.6.0/administration-guide/954635/getting-started

FortiSASE - Standard
Data sheet and specifications:
https://docs.fortinet.com/document/fortisase/24.4.87/administration-guide/756835/introduction

Cisco Systems

Secure Firewall (FTD), Version 7.6.0
Data sheet and specifications:
https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/admin/760/management-center-admin-76/get-started-overview.html

Cisco Secure Connect Advantage (Umbrella)
Data sheet and specifications:
https://documentation.meraki.com/CiscoPlusSecureConnect
https://docs.umbrella.com/umbrella-user-guide/docs/umbrella-policies-overview

Zscaler

Platform Version Saas, ZIA
Data sheet and specifications:
https://help.zscaler.com/zia/step-step-configuration-guide-zia

4.0 Test Setup

Testing was designed to determine the strengths and weaknesses of each vendor's Enterprise and Hybrid Mesh Firewall 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.

Next-Generation Firewall (NGFW) Malware Prevention

Over the course of 90 days, we repeatedly downloaded sets of 500 malicious files from VirusTotal (most recently submitted) - with over 25 engines with malicious verdict (high probability of being valid malware). These malicious samples consisted of DOCX, XLSX, PDFs, EXEs, PowerShell and Bash scripts, APKs, 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.

To further challenge the signature detection mechanisms of the device under test (DUT) the malicious samples were slightly modified to ensure a new hash would be determined for these samples. The modification was done without affecting the malicious payload execution. This allowed the known malware samples to be discovered as new variants, which were a better challenge for the "signature" engines for the solutions.

SSE/SASE Malware Prevention

Over the course of 90 days, we repeatedly downloaded sets of malicious files from VirusTotal (most recently submitted) - with over 25 engines with malicious verdict (high probability of being valid malware). These malicious samples consisted of PDFs, EXEs, PowerShell, and DLL files, which are known to be common web browsing file formats. 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.

To further challenge the signature detection mechanisms of the device under test (DUT) the malicious samples were also slightly modified to ensure a new hash would be determined for these samples. The modification was done without affecting the malicious payload execution. This allowed the known malware samples to be discovered as new variants, which were a better challenge for the "signature" engines for the solutions.

Intrusion Prevention System

IPS block rate was evaluated using Breaking Point, a cybersecurity and network testing platform designed to simulate real-world traffic, and security threats. This evaluation measured each solution's effectiveness in preventing high and critical-severity (CVSS score 7-10) Common Vulnerabilities and Exposures (CVEs) published between 2022 to 2024 by using Breaking Point's updated database.

4.1 Miercom Advanced Offensive Threat Detection

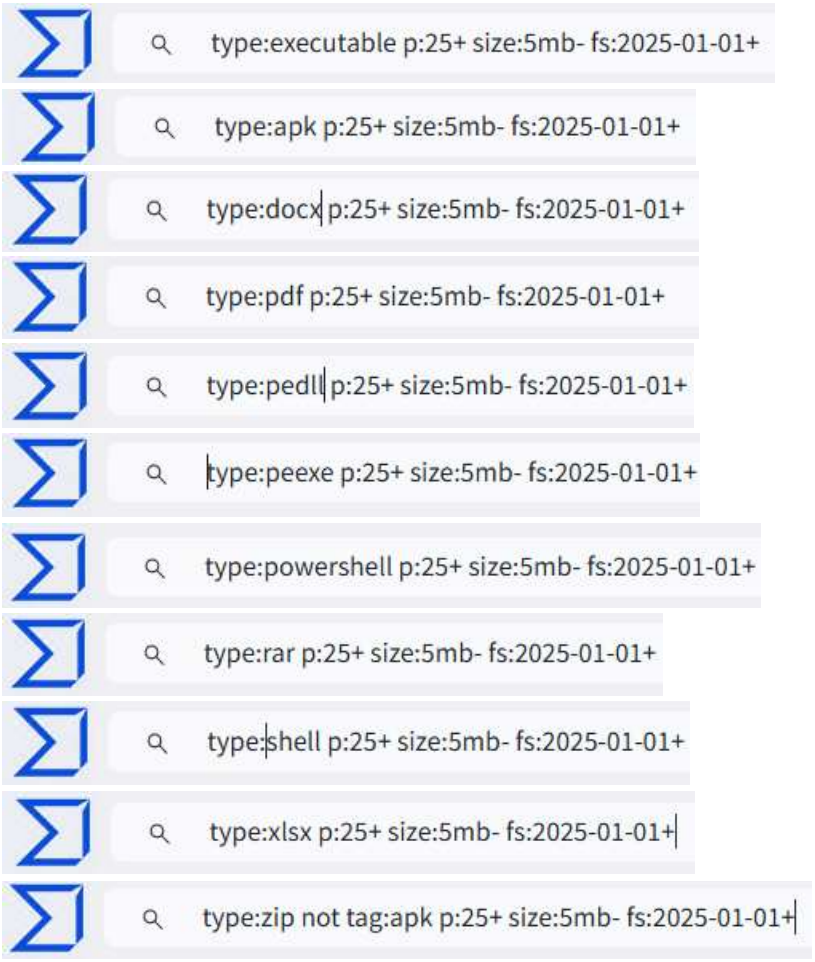
Today's threat landscape is rapidly evolving with more complexity, requiring more offensive security and more dynamic methods of testing. Miercom's Advanced Offensive Security Testing incorporates scenario-driven methods to provide users with relevant data regarding their security readiness. These tests 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.

4.2 VirusTotal

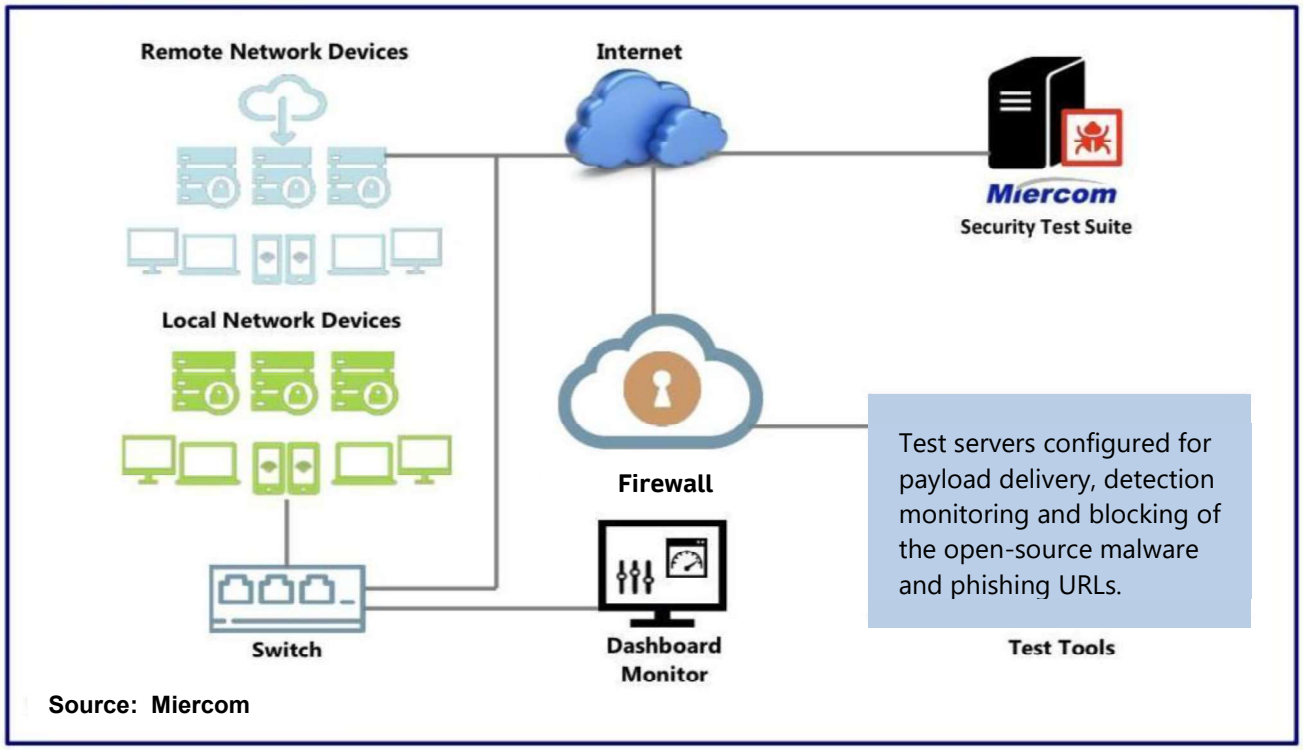
Malware samples from VirusTotal were downloaded and later used for evaluating all the products. A user can select a file from their computer with a web browser and send it to VirusTotal. VirusTotal offers many file submission methods, including the primary public web interface, desktop uploaders, browser extensions, and a programmatic API. The web interface has the highest scanning priority among the publicly available submission methods. Submissions may be scripted in any programming language using the HTTP-based public API.

The rule set for selecting the VirusTotal samples features in testing is shown below. The sample set for Zero + 1 Malware consisted of 1000 randomly selected, freshly submitted samples within 24 hours with at least 25 of VirusTotal's ~80.

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



4.3 Testing Environment



Vendor	Product	Version	Feature Bundles
Check Point	Quantum	R82	Sandblast
Cisco Systems	FirePower TD	7.6.0	TMC
Fortinet	FortiGate	7.6.0	Enterprise
Palo Alto Networks	PAN-OS	11.2.3	AV, WildFire, AWF
Zscaler	ZIA	SaaS	Transformation

5.0 About Miercom

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

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

6.0 Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify 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.