NGFW Firewall Security Benchmark 2023

Firewall Security Efficacy Competitive Assessment Summary Lab Report

for

Check Point Software

February 2023
SR220915Q

miercom.com

Table of Contents

1.0 Executive Summary

Miercom was engaged by Check Point to conduct competitive security effectiveness testing of the Check Point Next Generation Firewalls (NGFW) as compared to products from Cisco, Fortinet, and Palo Alto Networks. Testing included verifying the effectiveness of anti-virus, anti-malware, Intrusion Prevention System (IPS), anti-bot, URL Filtering (URLF), sandboxing, machine learning, and phishing protection. We conducted tests with all security services enabled and challenged each solution's ability to detect and block 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 to exploit weaknesses in applications, as opposed to networking components and services. NGFWs with advanced threat prevention offer the best protection against the latest generation of cyberattacks.

Our testing specifically focused on the ability to detect and prevent new malware variants within the first 24 hours and the first 3 days of their discovery as well as detecting and preventing new phishing sites.

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 vendors' signature detection mechanisms in the first 24 hours. Zero+3 Day Malware is used for malware samples uploaded at least 'three days ago' to common virus registries like VirusTotal and therefore should have been detected by most leading security vendors.

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

Key Findings

Critical Prevention Rate in the first 24 hours: Check Point led in the group test 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 spend less time, money, and energy responding to and remediating infected servers and endpoints.

- **Zero+1 Day Malware Prevent vs. Detect Tests:** Check Point prevented over 99.7% of new malware from a comprehensive set of files and file types, including executables, documents, and archived files that were no more than one day old.

  Check Point led with the highest score preventing 99.7% of malware downloads

Fortinet had 72.7% prevention and 26.7% detect-only
Palo Alto Networks had 43.6% prevention and 39.0% detect-only
Cisco had 46.1% prevention and no cases of detect-only
2.1.1 Prevention vs Detection-Only for Zero+1 Day Malware

- **Zero+1 Day Malware Prevent (First to Block) Results**
  Check Point led with a 99.7% prevention rate
  Fortinet had a 72.7% prevention rate
  Palo Alto Networks had a 43.6% prevention rate
  Cisco had a 46.1% prevention rate
  2.1.2 Prevention Efficacy for Zero+1 Day Malware

- **False Positive Malware Detection:** Content falsely reported as malicious creates unnecessary workload and stress on security teams. This, in turn, creates complacency and reduces an organization's overall security posture and security efficacy.
  Check Point led the group with the lowest false positive detection rate of 0.13%
  Fortinet had a 0.23% false positive rate
  Cisco had a 0.27% false positive rate
  Palo Alto Networks had a 0.30% false positive rate
  3.1.1 False Positive Detection Rate for Malware

- **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 its newly released 'Titan' release (R81.20) advanced AI deep learning capabilities.
  Check Point led with a 99.9% phishing and malicious URL prevention rate
  Palo Alto Networks had a 99.0% prevention rate
  Fortinet had a 92.1% prevention rate
  Cisco had a 27.4%. prevention rate
  2.2.1 Phishing and Malicious URL Prevention

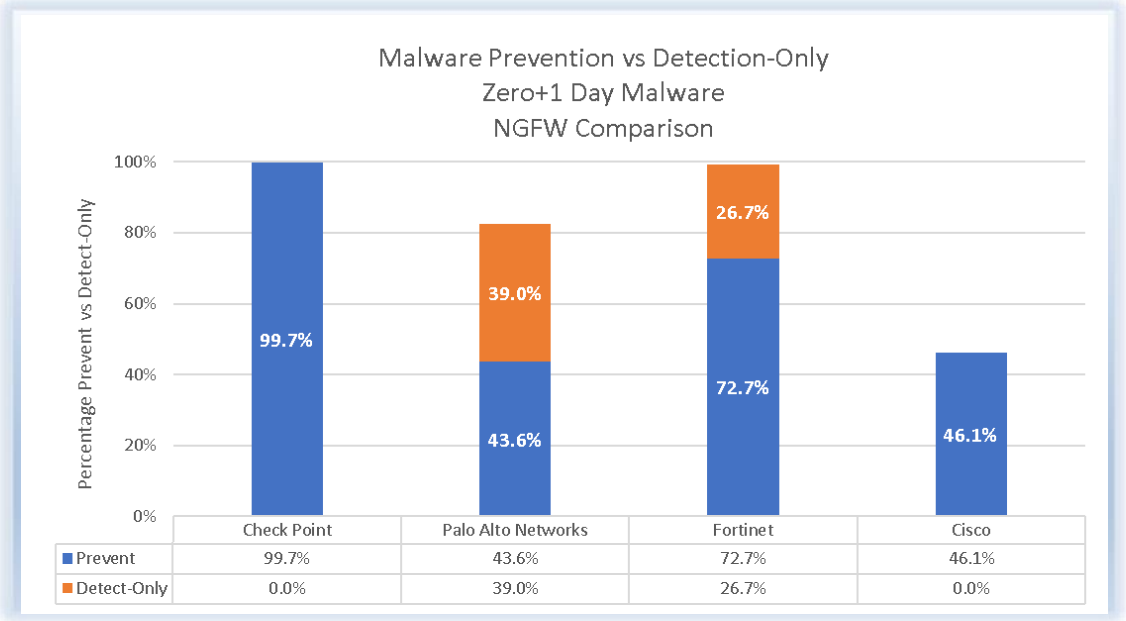
- **Integrated Machine Learning Technology:** We evaluated each vendor's product with the most aggressive detection settings and detection features available, including Machine Learning (ML). Check Point and Fortinet uniquely incorporate ML capabilities into the immediate detection and block response. We also had an opportunity to test Palo Alto Network's version 10.2.3 and their latest 11.0 and observed improvement in their Inline ML detection, but no improvement in the overall prevention for these tests.

2.0 Testing Summary Results

2.1 Malware Prevention and Detection Summary

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

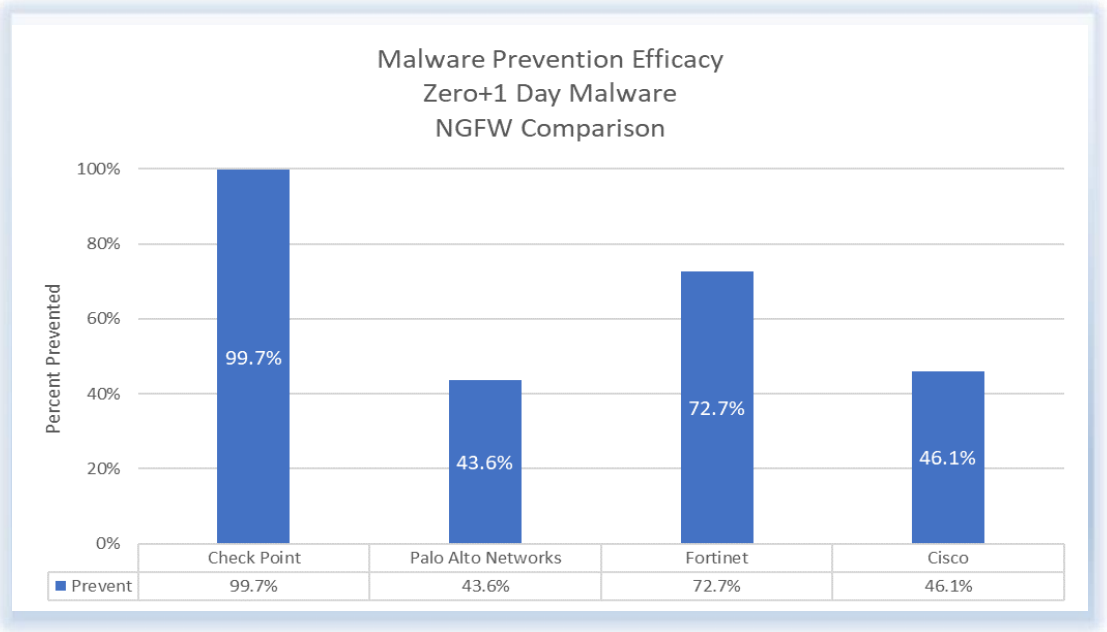
2.1.1 Malware Prevention vs Detection-Only Zero+1 Day Malware



*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.*

New Variant Malware Prevention success rate: In our Zero+1 Day Malware test, Check Point prevented over 99.7% of malware from a large set of files and file types including executables, documents, and archives. Palo Alto Networks, Fortinet, and Cisco had prevention rates of 43.6%, 72.7%, and 46.1% respectively.

2.1.2 Malware Prevention Efficacy Zero+1 Day Malware

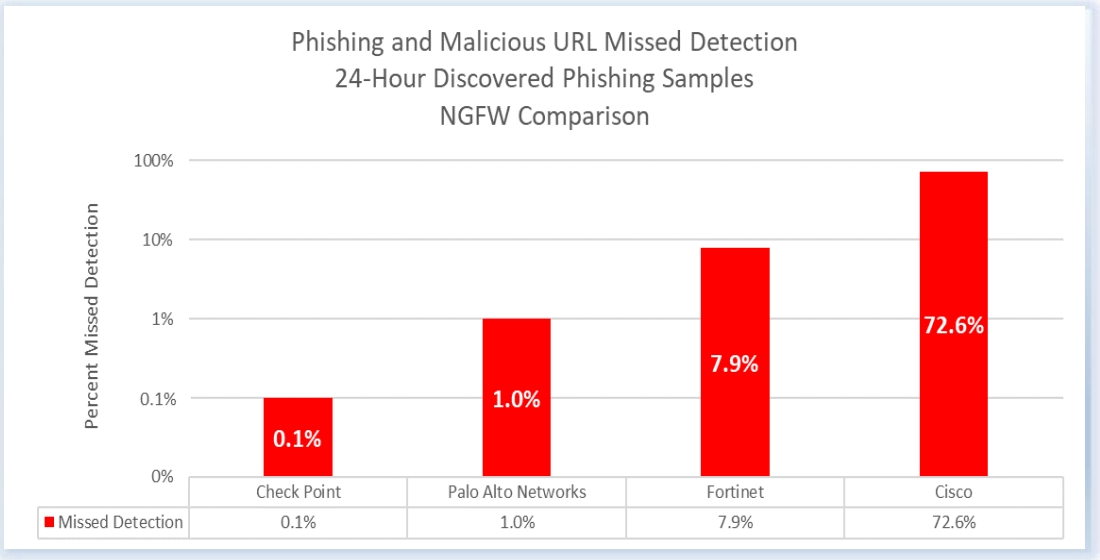


The chart above reflects how each vendor's firewall performed prevention in the first 24 hours of an attack. ***Prevent*** *means the solution identified the malware and immediately blocked it from entering the network.*

2.2 Malicious Phishing URLs Prevention and Detection Summary

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

2.2.1 Phishing and Malicious URL Prevention



Missed malicious URLs, less is better. *The chart above shows how each vendor's NGFW product performs in Detecting and Preventing of 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.*

3.0 False Positive Detection

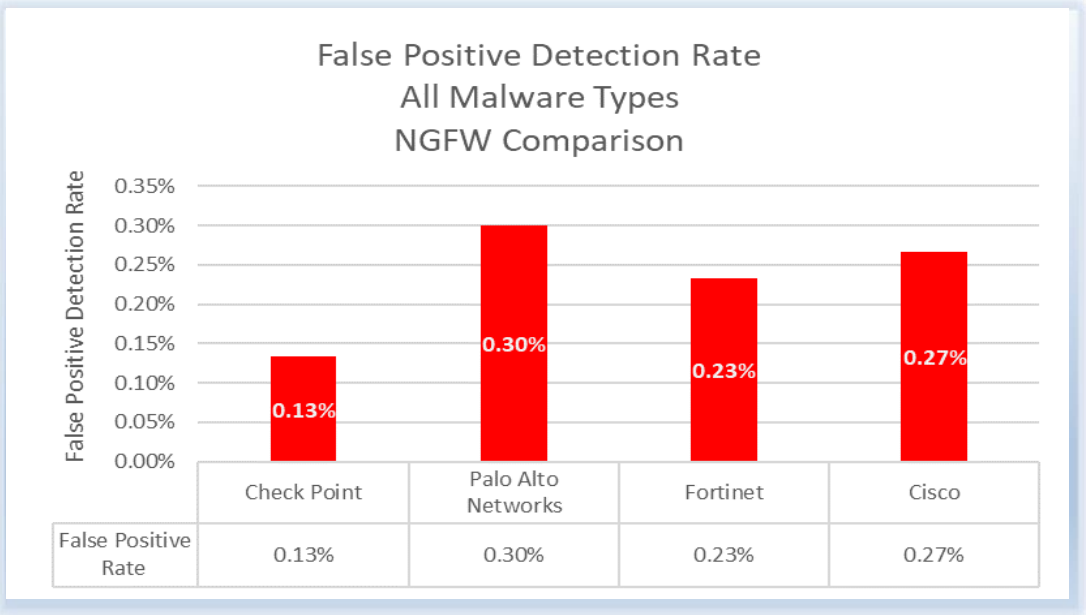
3.1 False Positive Testing Summary

False positive occurrences are non-malicious (or benign) files that are misidentified as malicious. Some files fall into a gray category due to their possible misuse on a network. An example of this is a password recovery tool, which, while not technically malicious, is often detected for its malicious potential.

Samples tested the granularity of the NGFW's AV engine. An intelligent AV engine flags only malicious files (true positive), so that users can continue clean file transactions. If the false positive detection is too high, the AV engine is considered overly aggressive, hindering network activity and productivity. An intelligent AV engine knows when to pass and not pass samples.

We sent a mixture of false positive samples (clean, suspicious files) and true positives (malware files) via HTTP. Of the clean files sent, we calculated the percentage of samples the NGFW mistakenly flagged as malicious.

3.1.1 False Positive Rate for Malware Detection



For false positive detection, less is better. *We examined each of the NGFW products for incidents of false positive detection in the malware tests. These are sample files that may be challenging for the NGFW products to determine whether they are malicious or not when they are not actually malicious. Check Point scored the best, with lowest false positive detection compared to Palo Alto Networks, Fortinet, and Cisco. Testing included review of thousands of samples over 90 days.*

4.0 Products Tested

Check Point

R81 Quantum

Version: R81.20 Titan

Data sheet and specifications:

https://downloads.checkpoint.com/fileserver/SOURCE/direct/ID/103832/FILE/CP_R81_ReleaseNotes.pdf

Palo Alto Networks

Palo Alto Networks PA-440 Series

Version: PAN-OS 10.2, 11.0

Data sheet and specifications:

https://docs.paloaltonetworks.com/content/dam/techdocs/en_US/pdf/pan-os/10-2/pan-os-release-notes/pan-os-release-notes.pdf

https://www.paloaltonetworks.com/resources/datasheets/pa-400-series

Fortinet

FortiGate-VM

Version: FortiGate/FortiOS 7.2.2

https://docs.fortinet.com/document/fortigate/7.2.2/administration-guide/954635/getting-started

Cisco Systems

Cisco Firepower 2120

Version 7.2.1

Data sheet and specifications:

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/roadmap/management-center-new-features-by-release.html#d54e123a1635

https://www.cisco.com/c/en/us/products/collateral/security/firepower-2100-series/datasheet-c78-742473.html

5.0 Test Setup

The testing conducted was designed to determine the strengths and weaknesses of each NGFW product. In addition to generating traffic patterns and attacks from industry test tools, we use unique, verified malicious samples for a customized, open-source approach. High detection efficacy against this blend of malicious samples indicates well-rounded protection from multiple attack vectors.

Over the course of 90 days, we repeatedly downloaded sets of 360 malicious files from VirusTotal (most recently submitted) - with over 30 engines with verdict malicious (high probability of being valid malware). These malicious samples consisted of Office docx, Office xlsx, pdf, exe, and dll and archived files. We assessed each NGFW solution using AV + Anti-Malware, IPS, anti-bot, URLF, sandboxing, and machine learning inline detection mechanisms. Testing was run concurrently on each of the vendor's NGFW solutions.

To further challenge the signature detection mechanisms of the devices under test (DUTs) 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 better challenged the "signature" engines for the NGFWs.

5.1 Miercom Advanced Offensive Threat Detection

The threat landscape evolves each day and with more complexity, requiring not only more offensive security but also more dynamic methods of testing. Miercom's Advanced Offensive Security Testing incorporates scenario-driven methods to provide consumers with relevant data regarding their security. These tests assess the ability of the 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.

5.2 VirusTotal

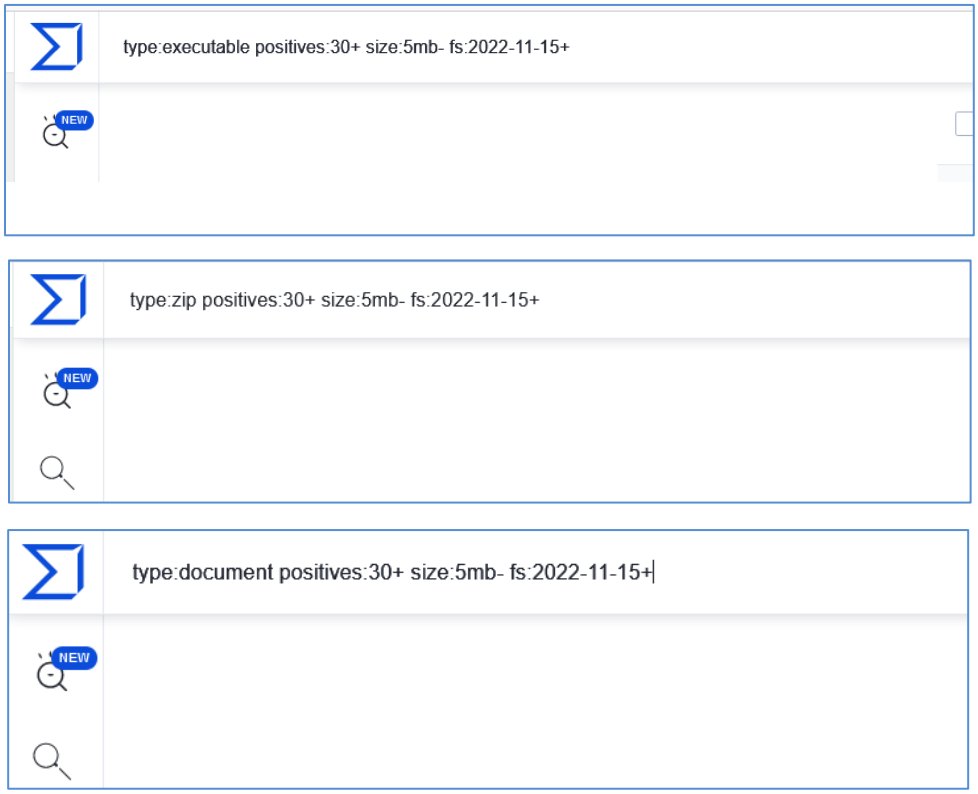
Malware samples from VirusTotal were downloaded and were later used for evaluating all the NGFW products. A user can select a file from their computer using a web browser and send it to VirusTotal. VirusTotal offers many file submission methods, including the primary public web interface, desktop uploaders, 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.

As with files, URLs can be submitted via multiple different means, including the VirusTotal webpage, browser extensions, and the API.

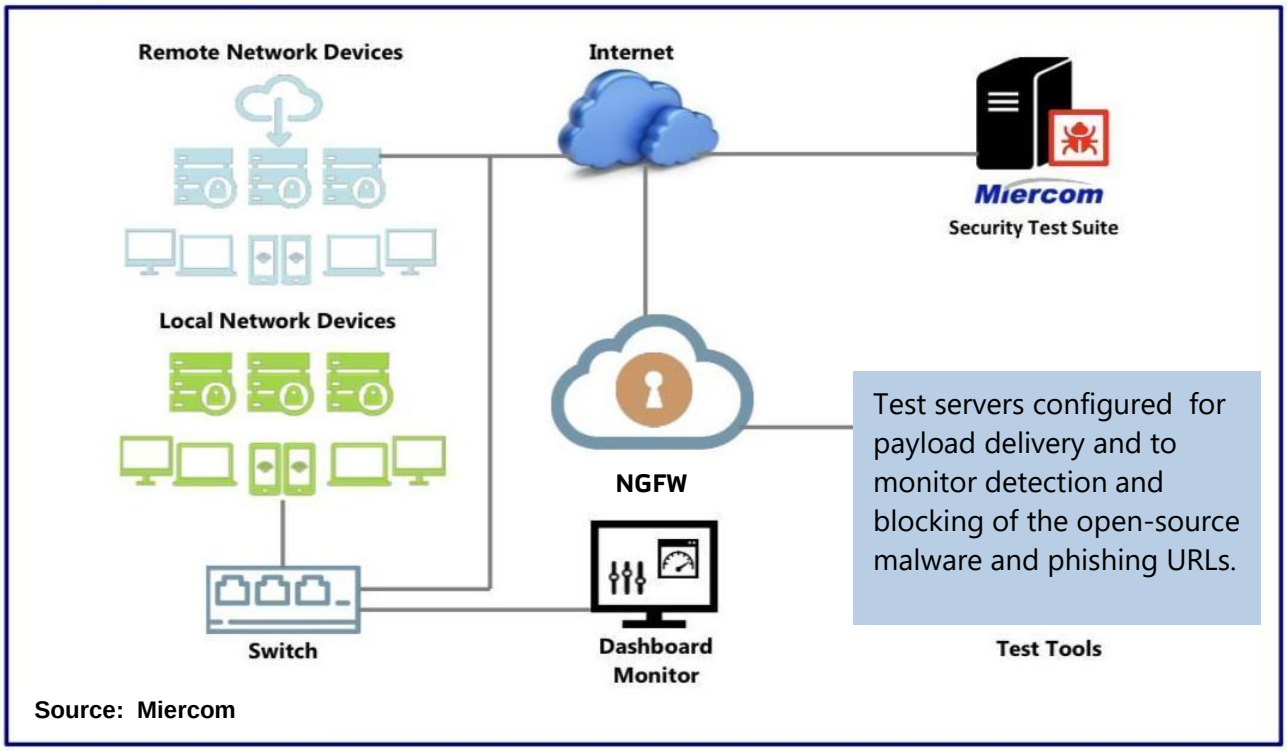
Upon submitting a file or URL, basic results are shared with the submitter, and between the examining partners, who use results to improve their systems. As a result, you are contributing to raising the global IT security level by submitting files, URLs, domains, etcetera to VirusTotal.

Each test was comprised of newly acquired, confirmed malicious files from VirusTotal. Thousands of new samples were evaluated repeatedly for 90 days.

The rule set for selecting the VirusTotal samples is shown below:



5.3 Testing Environment



Vendor	Product	Version	Feature Bundles
Check Point	Quantum Cyber Security Platform	R81.20 Titan	SandBlast
Cisco Systems	Virtual Firewall and Cisco Firepower 2120	7.2.1	TMC
Fortinet	FortiGate-VM	FortiOS 7.2.1	UTP
Palo Alto Networks	PAN VM Series and PA-440	PAN-OS 10.2.3, 11.0	Professional Bundle

6.0 About Miercom

Miercom has published hundreds of network product analyzes 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 analyzes, 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 of 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 may contain certain vendors' representations that Miercom reasonably verified but is beyond our control to verify with 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 trademarks in connection with any activities, products, or services that are not ours or in a manner that may be confusing, misleading, or deceptive or in a manner that disparages us or our information, projects, or developments.

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 miercom.com/tou