Check Point 12200 Threat Prevention Appliance
With SandBlast Threat Emulation Cloud Service
2015 SWG Industry Assessment

DR151209G
March 2016

Miercom
www.miercom.com

Contents

Executive Summary

Check Point submitted the 12200 Threat Prevention Appliance with SandBlast Threat Emulation for evaluation in ongoing standardized testing for the Miercom Secure Web Gateway Industry Assessment 2015.

Testing assessed the capability of the Check Point 12200 Threat Prevention Appliance with SandBlast Threat Emulation for:

- Malware Detection
- Malicious URL Detection
- False Positive File Detection
- Exploit Handling
- Application Awareness and Control
- Archive File Detection
- Stability and Resiliency
- Advanced Offensive Security

Using proprietary sample sets and industry-leading tools, Miercom was able to deliver traffic over multiple mediums, such as HTTP and file transfer protocol, to evaluate the Check Point 12200 for its functionality as a Threat Prevention Appliance.

Key Findings

- Detected 100% of each malware – stopping the most polymorphic threats that modify attack method to evade security devices
- 90.7% detection of malicious phishing URLs, predominantly found in social messages and engineering tactics
- Detected 99.5% of threats while under protocol fuzzing and mutation attacks
- Maintaining excellent resource efficiency – 17.2% CPU and 13.4% memory usage

We were pleased with the overall performance of the Check Point 12200 Threat Prevention Appliance for its threat detection effectiveness. Its ability to block the most pervasive and evasive threats today has earned the Check Point 12200 Threat Prevention Appliance with SandBlast Threat Emulation the Certified Secure Certification.

Robert Smithers Jr.

CEO

Miercom

Miercom CERTIFIED SECURE™

Overview

Network threat protection on an enterprise requires exceptional detection efficacy, stability and reliability under stress attacks and with centralized management control for administrative support.

In December 2015, Miercom evaluated the Check Point 12200 Threat Prevention Appliance for its functionality in protection and control using scenario-driven tests in a simulated, real-world environment.

This report shows the results of engineering analysis of threat detection, techniques and management to verify its capability as a competitive secure web gateway.

The product was tested using the following criteria:

- Malware, archived malware and malicious URL detection
- Handling of false positive files and exploits
- Awareness and control of application downloads
- Threat security during malformed packet attacks
- Data leakage

The Check Point 12200 Threat Prevention Appliance scored 100% efficacy in malware and archived malware detection, and its detection granularity was exceptional, deriving its precision from its false positive awareness and categorization techniques. Threats detected were of the most complex nature known to date.

The Check Point 12200 Threat Prevention Appliance's application control software gave informative control over known applications and option for custom rules for those that were not.

The device was very stable under fuzzing and mutation attacks, using 17.2% CPU and 13.4% memory while simultaneously combatting over 500 threats.

Data leakage was prevented at a rate of 100% for randomized traffic of sensitive information such as phone numbers, credit cards, tax identification numbers and other data strings.

Results featured in this report and collected during testing will be used in the 2015 Miercom Secure Web Gateway Industry Assessment. This study is an ongoing endeavor in which all vendors have an equal opportunity to participate and contribute to the most comprehensive and challenging test program in the industry.

Check Point and competing vendors are afforded the opportunity before, during and after testing to comment on results and demonstrate their product's performance. The Industry Assessment is intended to reflect the most accurate product performance to assist customers in finding the appropriate purchase for their enterprise.

Methodology

The following tests were performed on the device to determine its security efficacy, detection and control granularity and its relative value.

Test Summary

Test	Description
Malware Detection Efficacy (Details on page 6)	Seven categories of malware, ranging from legacy to zero-day files, are delivered via HTTP requests to the DUT to determine the detection rate of threats amid normal traffic.
Malicious URL Detection Efficacy (Details on page 7)	Multiple sources of malicious URLs, gathered by Miercom and numerous experts, are collected and infused into white-listed traffic through the DUT to determine the detection rate of threats.
False Positive File	Predetermined amounts of black listed files are sent with white listed files to assess the DUT's reputation awareness capability to differentiate malicious files from legitimate traffic.
False Positive URL	Predetermined amounts of black listed URLs are sent with white listed URLs to measure the DUT's reputation awareness capability to differentiate malicious files from legitimate traffic.
Exploit Testing	Exploit scenarios are simulated to evaluate the level of network responses that the DUT prevents. Any network response yields of fail since responses allow attackers to command and control.
Application Awareness and Control	The DUT is verified for its capability to properly categorize sites and content for management and control purposes. This evaluates the granularity of application, Internet and social media control.
Archived File Malware Detection	Compressed files are embedded five and ten times to determine how deep the DUT will inspect zipped files for malware. Samples are delivered via HTTP from an external malware server.
Stability and Resiliency	The DUT must remain operational and stable during extended attacks and maintaining security under protocol fuzzing, mutations, power failure and failover.
Advanced Offensive Security	Sensitive data exfiltration and content filtering scenarios are performed to determine detection and prevention of the DUT without performance loss.

Malware Detection Samples

Malicious software, or malware, is any software used to disrupt computer or network operations, gather sensitive information, or gain access to computer systems. These samples were obtained from Miercom's honeypot, consisting of real and intricate malware developed for the purpose of this test. Although legacy samples were included in the set, the focus was on the detection of the most recent and advanced samples.

Active Threats	A constantly changing, unknown malware from external resources and private honeypots. These custom crafted, undetected samples and APTs have undergone AV evasion techniques such as encryption, black packaging, and payloads using normal traffic.
Advanced Evasive Techniques (AETs)	A network attack combining several known evasion methods to create a new attack delivered simultaneously over several layers. Its code is not necessarily malicious, but the danger the elusive attack whose access is undetectable. Currently, there are about 200 known evasion techniques recognized by vendor products. An AET can create millions of new evasion techniques from just a few combinations.
Advanced Persistent Threats (APTs)	A set of stealthy and continuous computer hacking processes, often orchestrated by humans targeting a specific entity. This malware usually attacks organizations or nations for business or political motives. An APT may consist of a staged payload that, when activated, allows an attacker to obtain shell access remotely via command line. These payloads are masked with randomization and evasion techniques to bypass AVs. The known APT samples used in our testing were sourced from Mandiant's Advanced Persistent Threat sample set.
BotNet	A collection of interconnected, communicating programs which use a technique known as Command and Control. An intermediary receives orders or command attacker and are then forwarded to all infected hosts. Botnets are commonly used in spamming and DDoS operations. Variants of the Zeus and Citadel botnets were collected from high-interaction honeypots and used in this test.
Legacy	Samples included several hundred variants of known malware that have been in circulation for 30 days or more. The malware classifications primarily consist of viruses and worms.
Malicious Documents	These samples were a mix of Microsoft Office documents (Word, PowerPoint and Excel files) that held known macro viruses, and PDF files containing a variety of viruses, APTs and worms.
RATs	Remote Access Threats (RATs) are malicious code disguised as something normal or usable, often masquerading inside other legitimate software. When activated in a victim host, they provide full remote control over that victim.

Malicious URL samples

Malicious URLs samples are real-world threats from an unbiased set of live Internet targets, either unknown or black-listed. There were four sets of samples used: two open source sets, a Miercom legacy set and a proprietary honeypot for a total of 10,000 threats. The malware and/or other malicious activity associated with the URL samples are explained below.

Malicious Lures	Users are often lured to malicious sites from links in social networks, blogs, search engines or email with phishing links, offering free software or prizes. The domain appears to be legitimate but directs the user to a malicious site, often containing exploit code or asking for personal credentials for a data theft scam.
Phishing	The act of baiting and deceiving the user to obtain credentials. Everyone who uses e-mail has at one time received some type of a phishing attempt. The same type of forgery exists with attacker-operated website domains used to deceive a user.
Malicious Embedded iFrames	iFrames (inline frames) were once used to reduce time to render web content when bandwidth was limited. Attackers leverage iFrames to embed content from an external, attacker controlled page to execute malicious code within the browser. iFrames often go undetected because of style specific attributes, such as a one pixel sized iFrame.
Evasive Malware	Malware can propagate onto a victim host in a number of ways to avoid detection. Droppers are commonly employed by malware authors to bypass security controls by having the victim install a seemingly harmless application. Once open or deployed the malicious payload from the attacker infects the victim.
Botnets	Botnets are vast networks of malware-infected computers on the Internet under the command and control of an attacker. URLs are employed by an attacker to increase longevity and sustainability of their botnet CNC (command and control) servers.
Exploits	Systems are controlled or denied service primarily through a compromised web site, or traffic redirected to a malicious web site. An exploit kit analyzes a target system for vulnerabilities or an open door, and when found, the attack delivers a malware dropper file.
Spyware	To covertly collect information about a person or organization without consent. Convincing sites often masquerade as legitimate products. These sites deceive a user into downloading and installing an application.
Malicious Redirection	This URL contains an HTTP parameter causing a web application to redirect to a malicious URL. After redirecting, an attacker may then attempt to steal user credentials or gain access to sensitive data.
Non-Binary Obfuscated Threats	These threats contain obfuscated, or embedded, malicious code which are written within normal code to mask the file’s true intent. Obfuscation, itself, is not necessarily malicious but if used for attack requires detection. Attackers use these threats to evade antivirus detection engines. Miercom uses obfuscated JavaScript and malicious code written into the most common file types.

Product Tested

Check Point 12000 Threat Prevention Appliance	
Version	r77.30
Model	12200
Software blades	NGTX Package + DLP Anti-Bot Antivirus Application Control Data Loss Prevention Intrusion Prevention System SandBlast Threat Emulation URL Filtering

Test tools

Miercom used a proprietary blend of industry leading test tools, scripts, and databases to provide a robust, comprehensive, and realistic testing environment. Samples from our Secure Web Gateway Industry Assessment are uniformly used in testing competitive products.

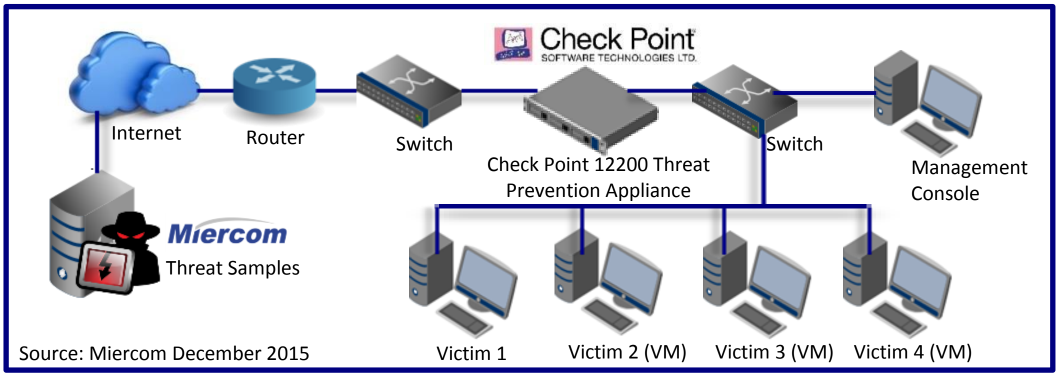
Test Partners

KALI LINUX™
"the quieter you become, the more you are able to hear"
WildPackets
SPIRENT
ixia
Nessus
BreakingPoint™
Find it before they do.™
metasploit®
idappcom

Ixia BreakingPoint gave the capability of sending protocol fuzzing, mutations and a multitude of attacks for testing stability and resiliency of the DUT. It was also able to simulate a real-world network environment, sending simulations of sensitive data through the DUT and determining data leakage detection during advanced security testing.

Test Bed Configuration

Test Bed Diagram



Source: Miercom December 2015

Malware and malicious URLs were delivered from the raw internet via multiple external sources in order to simulate a real world environment. These methods included HTTP, HTTPS and FTP file initialization from within the protected network behind the Check Point 12200 Threat Prevention Appliance.

Malicious samples were delivered directly to the DUT through a typical layer 3 network router and thoroughly inspected before it could be delivered to the local LAN.

The test bed consisted of a Check Point 12200 Threat Prevention Appliance, deployed in-line from a layer 2 network switch, to one physical computer endpoint and three virtual machines hosted on an ESXI 5.5 server. A physical computer was also used to monitor activity with the Check Point management console.

The appliance was configured with default settings to detect every security related category available within its administrative console and to use all available defenses.

Victim Environment

Virtual machines, hosted on VMware ESXi release 5.5, acted as protected victim computers during tests. These VMs were subjected to attacks from a malicious server. Following the attempted transfer of samples from server to victim, security-product log files are then reviewed. Log files were intended to show if a sample was detected, how long it took to detect it from time of initial request to download, and what post-detection remediation steps, if any, were taken by the security product.

Results Summary

The Check Point 12200 Threat Prevention Appliance had exceptional security proficiency in malware detection, application control, archived file detection and under-attack scenarios.

It's scored 100% in malware detection, against polymorphic threats that are altered constantly to evade security measures. On the false positive file samples, the DUT had a high level of visibility and classification that ensured its malware detection was reliable.

During protocol fuzzing and mutation attacks, there was 99.5% security efficacy with little increase in CPU usage while handling attacks and defending its security.

The Check Point 12200 Threat Prevention Appliance has not only high security, but it remains resilient during a scenario of possible denial-of-service attacks.

The following table summarizes the results of each test performed:

Malware Detection Efficacy	100% average detection, with significant detection for active, polymorphic threats
Malicious URL Detection Efficacy	Highest number blocked, which is over 170% more than the average number detected
False Positive File Samples	Perfect score, configurable sensitivity for detection
Exploits	Blocks exploits using either, or in combination, its URL filtering, antivirus or SandBlast Threat Emulation tools
Application Awareness and Control	Had specific and effective awareness and control, with preconfigured rules for common applications
Archived File Malware Detection	Detected malware in 5x- and 10x- level archives and distinguished them from clean archived files
Stability and Resiliency	99.5% of threats mixed in malformed traffic using only 17.2% CPU and 13.4% memory usage
Advanced Offensive Security	100% prevention of data leakage between more than 500 simulated external and internal hosts

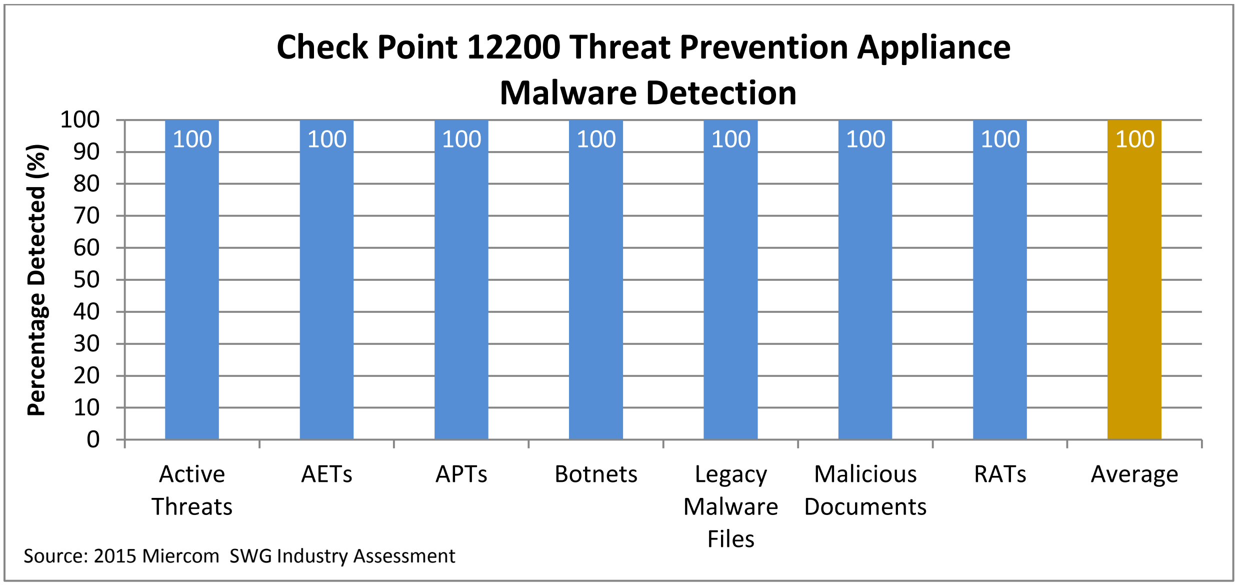
Malware Detection Efficacy

Description

The Check Point 12200 Threat Prevention Appliance was evaluated for how well it could detect malware before it entered the network. The most complex threats are Active Threats, AETs, and APTs.

Detection was expected to be extremely high in all seven categories. Detection for complex threats confirms the DUT has an advanced capability for network protection.

Results



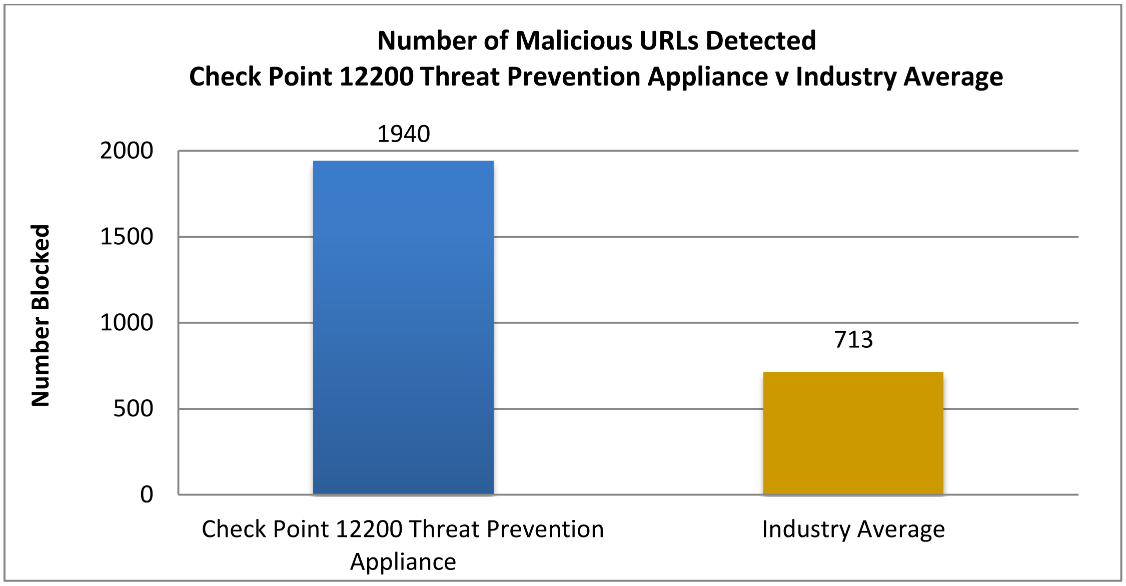
The Check Point 12200 Threat Prevention Appliance detected 100% for each malware set. Active threats, AETs and APTs were the most complex categories. Each sample was found by the Threat Prevention Appliance and did not infect the victim networks. The product had a 100% average detection efficacy.

Malicious URL Detection Efficacy

Description

The Check Point 12200 Threat Prevention Appliance was tested for its efficacy in malicious URLs before reaching the network. Moderate threats such as botnets, malicious lures and redirects, phishing and spyware are expected to yield higher detection than other, more complex, categories.

Results



The Check Point 12200 Threat Prevention Appliance detected a total of 1,940 malicious URLs which is over 170% more than the industry average Malicious URL detection.

False Positive File Samples

Description

A predetermined amount of false positive files were mixed with clean traffic and ran through the DUT to see how many would be flagged as malicious. The product is expected to have false positives, but a low number of false positives indicates high granularity.

False positives are typically non-malicious applications bundled with adware or other programs that slow performance and degrade the user experience. Most vendors categorize these files immediately as malicious, blocking a possible download from taking place.

Results

The Check Point 12200 Threat Prevention Appliance is able to demonstrate a perfect score in this test, no false positives depending on the configuration of the DUT more or less aggressive or handling of samples, such as hacking, recovery and cracking tools.

Note the grey area samples used in False Positive testing is really a tool to demonstrate vendor fidelity for the customers.

In this case the Check Point 12200 Threat Prevention Appliance did a fabulous job when asked to show it would pass or block depending on the type of media or files. Regardless of Check Point 12200 Threat Prevention Appliance handling of grey flies, it unquestionably passed 100% of clean malicious files, achieving a perfect score in the false positive test metric.

The Check Point 12200 Threat Prevention Appliance flagged 6 of the 34 samples as "Open Candy", otherwise known as Potential Unwanted Application/Program (PUA/PUP). Unlike most vendors, they did not automatically mark these samples as malicious. Instead, they were categorized as a PUA/PUP with an option to download. The DUT can be configured, if needed, to allow downloads based on the network requirements. This granularity and control makes the Check Point 12200 Threat Prevention Appliance a flexible and reliable gateway for enterprise networks. This is a fair assessment of the grey samples used for this test. Note the grey area samples used in False Positive testing is really a tool to demonstrate vendor fidelity for the customers.

Exploits

Description

Exploits are malware files or malicious URL trying to gain access to the network and allow remote control access by the attacker. The DUT was evaluated for its handling of these particular threats since they are more pervasive. The Threat Prevention Appliance was expected to block all exploits detected.

Results

The Check Point 12200 Threat Prevention Appliance handled each exploit depending on the nature of the attack. The response is managed either by its antivirus or SandBlast Threat Emulation software blade.

If the exploit was malware, like a RAT, the antivirus software blade would begin enforcement once the threat was detected, by dropping incoming packets to block it from entering the network.

If the exploit was a URL and known, the URL filtering tool would block the threat. If the URL was not known, such as a redirect, the antivirus or SandBlast Threat Emulation tool would quarantine the threat and block it from the network.

The DUT is configurable to block any detected threats from gaining access to the network.

Application Awareness and Control

Description

Applications and their content are categorized and controlled by security management to ensure privacy and protection for network endpoints. Social media is a major outlet of sites and applications that can cause information to be compromised or relayed to third parties, causing data loss violation policies. The DUT is evaluated for its control of applications and associated data.

Results

Upon opening applications such as remote desktop agent applications, file sharing programs and client chat installations, the DUT was observed for its ability to detect and control these executables.

The Check Point 12200 Threat Prevention Appliance had both informative and effective control over applications. Its built-in software blade allowed a customizable administrative control over traffic with options to add multiple categories and protocols for applications and URLs. The most widely used applications, including social media sources, were preconfigured for control by the blade, and custom rules can be created for other sources.

Archived File Malware Detection

Description

Files can be archived with loss-less data compression. Files are embedded in multiple folders with a compression algorithm and this can be performed once or several times.

Malware files are archived so as to appear hidden to the user downloading the compressed file. The DUT was tested for its ability to detect malware files that were archived 5x and 10x.

Results

The Check Point 12200 Threat Prevention Appliance detected malware which was archived both 5x and 10x. For the file nested 5x, the DUT immediately detected the malware. For the file nested 10x, it took the DUT about five minutes longer but still effectively detected the malicious file. Possible reasons for a longer time period until detection were that the malware was more nested and evasive in nature than the malware used in the file archived five times.

Both 5x- and 10x- level archives were tested again with a non-malicious file to validate the integrity of the DUT detection, ensuring it was not being overprotective. Some vendors block any file archived more than five times, malicious or not. The Check Point 12200 Threat Prevention Appliance has this option, but it was not enabled during testing. The DUT did not detect malware for the clean archived files, showing its malware detection was accurate.

Stability and Resiliency

Description

Although a multitude of attacks can be delivered to a network, such as protocol fuzzing and mutations leading to denial-of-service (DoS), the network must remain stable and maintain protecting the network.

For this test, the BreakingPoint Stack Scrambler component sends malformed IP, TCP, UDP, ICMP and Ethernet packets to the DUT. The fuzzing technique of the test component modifies part of the packet (checksum, protocol options) to generate corrupt data. During this fuzzing and mutation traffic, attacks are made on the DUT. The device is expected to block attacks while handling malformed packets. The results of this evaluation provide detection efficacy and its resource usage.

Results

A total of 576 attacks were made on the DUT while the Stack Scrambler sent malformed packets. The Check Point 12200 Threat Prevention Appliance detected 573 which is an efficacy rating of 99.5%. The three attacks missed were: ISC DSCP DoS, Cisco IP Phone SIP DoS, Cisco IOS IPv4 DoS.

No significant resources were used to both handle the incoming corrupt data and perform security measures against attacks; resource usage was very low. CPU usage was up to 17.2% and with memory peaking at 13.4%.

Advanced Offensive Security

Description

This test assessed the DUT for its data loss prevention (DLP) efficacy. Sensitive data was simulated and sent through the DUT to determine how many lawful interceptions had occurred.

The BreakingPoint test tool simulates a real-world network environment of internal and external hosts, sending randomized trigger data to a pool of endpoints and hosts via multiple delivery methods. For example, data can be delivered over voice, email, chat, URL, file transfers and network file sharing. BreakingPoint simulates phone numbers, tax IDs and credit cards. It also creates random strings to represent user patterns, file entries and list of file entries. The DUT is expected to filter content and prevent exfiltration of the data.

Results

The Check Point 12200 Threat Prevention Appliance had a data loss prevention efficacy of 100%, while the DUT monitored all traffic.

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 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.