2015 Miercom
Next Generation Firewall Solution Testing:
Performance, Compliance and Advantages

DR150406D
December 2015

Miercom
www.miercom.com

Contents

Executive Summary

Miercom was engaged by Zscaler to conduct independent performance testing and an assessment of key features and capabilities of the Zscaler Internet Security platform, comparing its cloud-based Zscaler Next Generation Firewall product to competing vendors that use traditional hardware and software devices.

In late April 2015, Miercom tested the Zscaler Next Generation Firewall against three competitive next generation firewall (NGFW) products, all products were provided by Zscaler. The products were all evaluated using a set of security and compliance criteria combining Zscaler's proprietary test suite and Miercom's independent test harness. The tests focused on the following performance areas:

- **Security**: ability to provide protection against basic and advanced threats
- **Compliance**: ability to enforce typical data loss prevention and access policies

As part of the security test section of this study, Miercom assessed malware efficacy using its own sample set. The effectiveness of each security solution was tested, and the results were combined with a Total Cost of Ownership assessment provided by Zscaler to create a map demonstrating relative value.

Key Findings

- The Zscaler Next Generation Firewall exhibits a high-value, low-cost option for enterprises looking for an extra layer of security with very low deployment impact in comparison to traditional hardware-based solutions
- Cloud-based solutions have the advantage of scanning traffic in real-time to give global, up-to-date protection to any user at all times
- Zscaler performed very well against advanced malware samples, scoring 100% in blocking AETs and APTs, and 97% against active threats. Its SSL decryption provides a novel approach to detect malware sent over the internet.

Based on the impressive results of our testing, we award the Miercom Performance Verified Certification to the Zscaler Next Generation Firewall, having turned in an outstanding performance in Miercom's ongoing network security study

Robert Smithers
CEO
Miercom

Next Generation Firewall

Cyber-attacks have historically been noisy and opportunistic, focusing on server-side vulnerabilities, and traditional firewalls focused on blocking IP addresses, ports and protocols. But the world has changed. Today, attackers that once targeted enterprise servers have now realized that it is far easier to exploit client machines, thanks to weak defenses and naive users. Increasingly sophisticated cyber-threats are using more complex attack methodologies like protocol tunneling and port hopping to fool traditional firewalls.

Defending against these complex attack methodologies requires a new generation of firewall that understands users and can defend against application-based attacks. More specifically, a Next Generation Firewall must be able to:

- Identify applications with full application context awareness
- Identify and block threats that try to use "known good" ports and protocols
- Identify and block threats that try to use evasive tactics such as non-standard ports or "port hopping"
- Identify and block threats that try to use SSL
- Identify users, groups and locations and apply policy regardless of IP address
- Identify and block outbound data leaks
- Identify and block outbound botnet command and control communications
- Provide global visibility and granular policy management

And do all of this while delivering extremely high throughput and reliability at a reasonable cost.

About the Test

Our tests focused on three criteria: security, compliance, and product advantages. The tests were designed to facilitate comparison of the performance of the Zscaler Next Generation Firewall and competing NGFW hardware, and quantify differences in terms of value.

Miercom Malware Testing

The test for efficacy in malware detection was performed with Miercom's malware database and evaluated on a percentage scale. In combination with a cost factor based on the price of comparable deployments, each vendor's results were graphically expressed in a performance value chart.

Malware Tested

Advanced Evasive Technique (AET)	AETs are network attacks that combine several different known evasion techniques to create a new technique that won't be recognized by network security. These attacks can be delivered in pieces, at different times, or over several layers of the network at the same time.
Advanced Persistent Threat (APT)	APTs are considered "backdoors" into a victim network. APT malware consists of a staged payload that allows an attacker to obtain shell access. Payloads are often masked with randomization and evasion techniques to bypass anti-virus scanners.
Botnet	Botnet malware is a collection of interconnected programs which communicate about performing malicious tasks. When placed on an endpoint device, the programs work together to extract information and infect other machines. Some tasks include stealing sensitive data and intellectual property, participating in DDoS attacks, and emailing spam.
Legacy Malicious Files	Legacy samples include known malware that have been in circulation for thirty days or more and consist mostly of viruses and worms. Legacy samples should not require sandbox analysis. Should any pass through an antivirus filter, the sandbox should then have identified it immediately due to the known heuristics of each malware sample.
Malicious Documents	An additional sample set of malicious documents used in tested contained a mix of Microsoft Office documents (Microsoft Word, PowerPoint, and Excel files) that held known macro viruses, and PDF files containing a variety of viruses, APTs and worms.
Active Threats	Active Threat malware samples are constantly changing, unknown threats that have been custom-crafted. These undetected samples were acquired from external resources, private honeypots, and APTs that have undergone antivirus evasion techniques such as encryption and payloads that deliver malicious content.
Remote Access Trojans (RATs)	RATs are malicious code disguised inside other legitimate software. When activated in a victim host, they provide full remote control over that victim. The RAT sample set used in our testing consisted of a mixture of Microsoft Office documents and PDF files.

Zscaler Security and Compliance Testing

Zscaler provided a series of tests to evaluate the security and compliance performance of NGFW products. Each test received either a "Pass" or "Fail" result, which equate to 100% secure or less than 100%, respectively.

Security Tests Provided by Zscaler

Malicious URLs	Hackers can launch zero day and 'watering hole' attacks by compromising legitimate sites with malicious code. This test checks to see if the security solution blocks a malicious page hosted on a compromised site.
Malware Download over HTTPS	A Zohomail account was set up, and a malicious file was attached to an email connected via HTTPS. The Zohomail account was configured with secure socket layer (SSL) encryption. This test checks to see if the security solution blocks malware encrypted via SSL.
EICAR Hosted on Different Site	The European Institute for Computer Antivirus Research (EICAR) file is a standard test file to evaluate the response of antivirus (AV) programs using virtual malware. This test using this standardized set can provide security testing efficacy via a recognized benchmark data set.
Zipped Malicious Files	Virus payloads using compressed/zipped files are used to deliver. Unzipping takes computational power that can slow traffic down, so many appliance-based security systems skip analyzing files zipped multiple times. This test evaluates the ability of a security appliance to detect a malicious file that has been embedded in five layers and ten layers of compressed ZIP files.
Phishing Sites	Phishing attacks are targeted at employees to steal corporate credentials or sensitive personal data. This test checks to see if the security solution blocks one of the latest validated phishing sites uncovered by Phishtank.com.
Botnets	Once a device is compromised, it's no longer entirely under your control. An attacker directs it to exfiltrate your intellectual property, infect other machines on your internal network, and participate in Distributed Denial of Service attacks, email spam, spreading spyware, and other malicious attacks. This test tries to contact a known Botnet command and control server ('calling home') to determine if the security solution blocks it.
Browser Exploit and Metasploit	Malicious code of browser exploits and metasploits breach browser security to alter the user's settings. They may exploit HTML or JavaScript to run other unwanted code. This test checks to see if the security solution in
Cross Site Scripting	Cross Site Scripting attacks inject malicious code into an otherwise legitimate site. This type of attack can steal credentials and session keys (e.g. passwords) from visitors of this site, and tarnish the reputation of the compromised site. This test visits a website that has been compromised by malicious code and checks to see if it is able to compromise your web browser, or if the security solution blocks it.
Cookie Stealing	Cookie theft is the primary method used to steal personal information such as logins. Different methods of script injection are utilized to accomplish this; specifically Adobe Flash employed on common, trusted sites (e.g. YouTube, Ebay). This test takes a cookie from one website and tries to post it to a second one, a clear sign of an attempt to hijack the web session.
Adware Sites	Adware is software supported by advertisements. These ads will automatically infiltrate sites to generate revenue for the author. This test checks to see if the security solution blocks a known adware site.

Obfuscated JavaScript	Obfuscated code is when either the entire code, or a piece of it, is masked to hide the true intent of the code. Obfuscation itself is not necessarily malicious, but when it hides the intent to hide malicious content, it requires detection. This test checks to see if the security solution blocks a web page containing obfuscated JavaScript.
Browser Version and Plug-in Control	Browsers that are not updated with the latest versions, or may have missing patches, can entice hackers to exploit these vulnerabilities and infect a user's computer. Third party plug-ins are risky and open more vulnerabilities. This test checks to see if the security solution blocks a browser version with known vulnerabilities from accessing a web site.

Compliance Tests

Compliance tests were created and provided by Zscaler to cover the following five general areas of violated confidentiality within a network:

Credit Card Exposure	Organizations requiring payment card industry (PCI) compliance must adhere to data security standards where credit card data is completely protected. Credit card numbers are an obvious target for theft and fraud. Many negative consequences and penalties result from unsecure networks that can cost an enterprise remediation service fees and its reputation.	This test checks if a set of numbers that match the format of valid credit card numbers can be sent out over the network.
Intellectual Property Exposure	Intellectual Property is monumental to enterprises of all forms, but especially in technology companies whose property entails incredible amounts of nuances. Hackers are motivated by competitors to steal intellectual property to gain an advantage that could have profound consequences for the vulnerable organization.	This test checks if the security appliance under test can detect and block an attempt to leak sensitive intellectual property data by various online methods, such as posting the data to a website or emailing it.
Sensitive Information Exposure	Personal information is targeted by criminals who use it to commit theft and fraud. Breach of confidential data can expose an organization to negative legal consequences and federal actions, in addition to remediation fees to monitor affected consumers.	This test checks if a set of numbers that match the format of valid United States Social Security numbers (SSNs) can be sent out from the network.
Restricted Access	Companies complying with US and European Union (EU) trade laws are obligated to restrict users from visiting websites in countries under embargo. Countries with hostile attitudes towards the US and EU generally host compromised websites and provide low levels of internet security. Blocking specific IP ranges by geography limits can reduce user exposure to threats.	This test checks the ability of the user to visit a website located in North Korea, which is under US and EU Trade embargo, while using the security appliance under test.
Anonymizer Sites	Employees try to bypass company policies to view blacklisted sites or other harmful content by use of anonymizing proxies. These anonymizers open a backdoor for malware, and expose data of an enterprise to untrusted third parties. This may result in a serious depth of negative consequences and legal issues.	This test checks the ability of a user to use an anonymizing site, by attempting to visit a blacklisted site through a well-known anonymizer, while using the security appliance under test.

Miercom verified performance in security and compliance using Zscaler's tests, and incorporated proprietary tests in the following areas: EICAR file, zipped malicious files, phishing sites, and botnets.

Products Tested

Zscaler

The Zscaler Next Generation Firewall (April 2015 version) is a cloud-delivered solution that protects all non-data center locations including branch offices and remote locations of an organization. It is part of the Zscaler Internet Security platform, which incorporates multiple security and compliance applications—URL filtering, anti-virus, advanced threat protection, sandboxing, next generation firewall, data loss prevention, cloud application security, traffic bandwidth management, and much more in a single, seamless system. Zscaler delivers this broad security and compliance via the security cloud, with over 100 data centers worldwide.

Zscaler does this by bi-directionally inspecting every byte of Internet traffic, blocking malware and cyber-attacks, preventing intellectual property leakage and enforcing business policies. Zscaler is designed to protect all of an organization's users and systems – including road warriors, mobile users, and guest Wifi users. And all of this is done with global real-time visibility and reporting, and granular policy-based management.

Fortinet

The FortiGate 60D (version 5.2.1 Build 618) with FortiCloud is a comprehensive security appliance which utilizes threat management tools to deliver protection for on premise and remote networks.

Vendor A Next Generation Firewall and Cloud Sandbox Subscription Service

This vendor has restrictions in their product license agreement on publishing results associated with their name, so their name and product details are withheld.

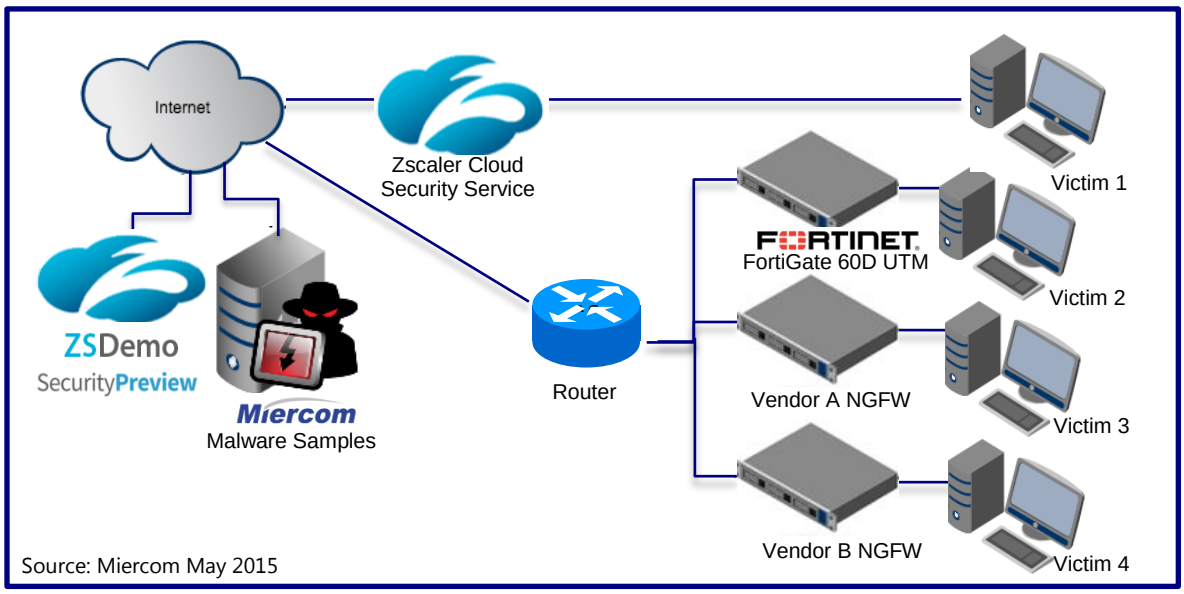
Vendor B Next Generation Firewall

This vendor has restrictions in their product license agreement on publishing results associated with their name, so their name and product details are withheld.

How We Did It

Miercom used industry leading test tools, scripts, and databases to provide the most robust, comprehensive, and realistic testing environment possible. The appliances were configured to block every security related category available within its administrative console and to use all available defenses.

Test Bed Setup



Deployment

The Zscaler Cloud Service solution was deployed using a VPN tunnel created by configuring the router to access the target web server. IPSec VPN tunneling used the pre-shared key for authentication. Miercom forwarded all traffic destined for any port to the Zscaler Cloud Service. The VPN tunneling provides visibility into the internal IP addresses, which was used for Zscaler security policy and logging.

The competing vendors were deployed in-line, with the device under test in between the router and the client system.

Victim Environment

Virtual machines, hosted on VMware ESXi release 5.5, acted as the victim computer during testing. The virtual machine was subjected to attacks from a malicious server. Downloading of malicious files from the server was observed for each malicious file and reported as allowed or blocked by the observer. The same procedure was followed for malicious URL and Phishing sites as well as the other tests from Zscaler's test suite.

Malware Samples

The malware sample sets used in this analysis were obtained from various public and private sources. Known malware (Legacy, APT, BotNet, Malicious Documents, RATs / Trojans) were obtained from VirusTotal and other public sources. Zero-Day samples were custom crafted by both internal and external resources, obtained from private honeypots that have been deployed around the globe, and APTs that have undergone AV evasion techniques, such as encryption, black packaging, payloads that use normal and allowed egress traffic, etc.

Devices Tested

Name	Function	Version
Zscaler Internet Security	Next Generation Firewall	Latest version as of April 2015
Fortinet FortiGate 60D w/ FortiCloud	Unified Threat Management	V5.2.1 Build 618
Vendor A	Next Generation Firewall	Version A
Vendor B	Next Generation Threat Protection	Version B

Configurations

Zscaler

This product was employed with a cloud-based setup via VPN tunneling. Its protection includes control of: firewall, DNS, mobile applications, file types, URL and cloud applications, browsers, bandwidth and FTP. It was configured to provide protection against malware, mobile malware, advanced threats, zero-day malware and APTs, and data loss. Decryption and inspection of SSL traffic was also activated.

Fortinet

This product was deployed in-line with full Unified Threat Management (UTM) which consists of: antivirus, endpoint control, application control, data loss protection, email filter, web filter, intrusion protection, and explicit proxy.

Vendor A

This vendor has restrictions in their product license agreement on publishing results associated with their name, so their name and product details are withheld.

Vendor B

This vendor has restrictions in their product license agreement on publishing results associated with their name, so their name and product details are withheld.

Security and Compliance Test Results

Security tests were a combination of the Miercom Malware Test and the security test suite provided by Zscaler. From these results, Zscaler scored 97.4% efficacy for malware detection and 100% for Zscaler security tests. Fortinet, Vendor A and Vendor B scored less than 55% efficacy for the security tests.

Compliance results further showed Zscaler's ability to adhere to security standards regarding sensitive data transfer and user restrictions. Zscaler scored 100% efficacy, 60% above the vendor average.

The Miercom Malware Test results were also incorporated into a performance valuation chart to place a value on efficacy when factoring in the cost of hardware, software and deployment. Zscaler, as a cloud service, does not utilize on-premise hardware and was found to be simpler and more cost-effective to acquire, deploy and manage.

Miercom Malware Test

Malicious software, or malware, is any software used to disrupt computer or network operations, gather sensitive information, or gain access to computer systems.

This test was conducted using Miercom's sample set. The samples were taken from our cloud server and tested on each product. The number of undetected samples was calculated and recorded by a Python script.

Products are expected to block all malware, scoring 100% in each category, to ensure their efficacy is a reliable representation of their malware blocking capabilities.

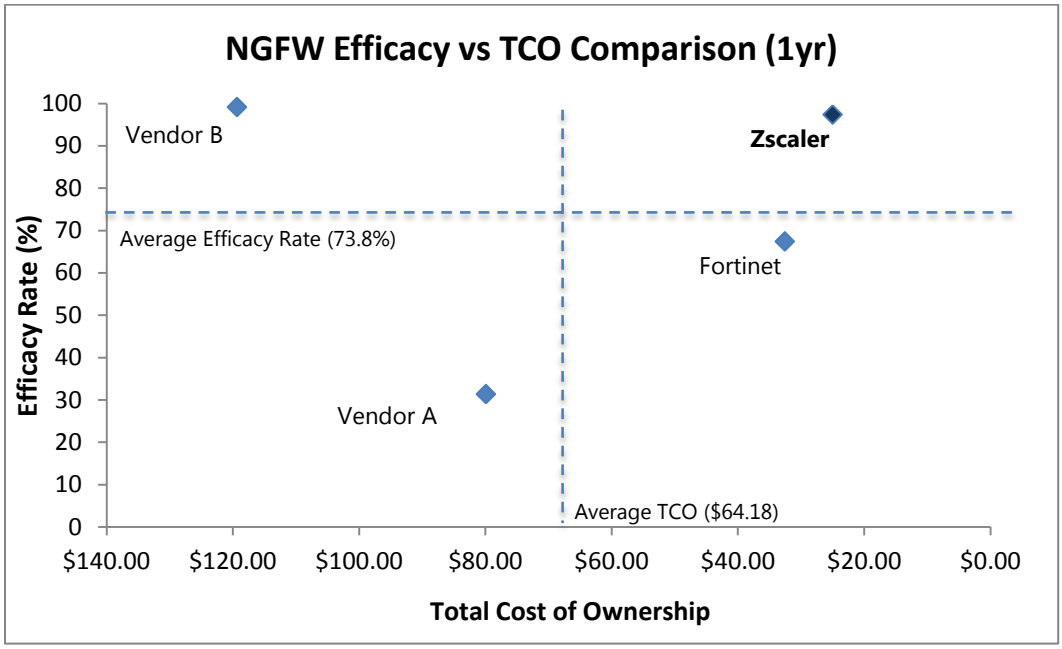
Zscaler	• excellent efficacy in six 6 of 7 malware categories • scored 100% in 5 of 7 categories • 100% efficacies against AET and APTs, implying Zscaler's relevant strength in the most complex malware.
Fortinet	• excellent efficacy in less than half of the malware categories • 100% efficacy against bots and legacy files, the most common malware • low performance in blocking malicious documents • offered absolutely no protection at all against AETs, the more lethal threats to date
Vendor A	• did not perform well for Miercom's 7 category malware set • adequate efficacy only in one category: APTs • extremely low efficacy for more than half of the categories, particularly bots and RATs • failed to protect against AETs, implying protection is extremely weak against active threats.
Vendor B	• excellent efficacy in all categories • 100% efficacies against AETs, APTs, and active threat malware where threats are more sophisticated.

Performance and TCO Valuation

The malware efficacy scores of Zscaler, Fortinet, Vendor A and Vendor B were compared to the vendor average for a point of reference.

Costs of each device with its tested hardware, software packages, support, and licenses were supplied by Zscaler. This total cost is calculated per individual user over the course of one year.

By combining these two factors, the product's value was plotted on the chart below.



Zscaler's high efficacy rate and low cost placed it in the top right quadrant of the value map, ranking it highest in cost-effectiveness among the solutions tested. Its position distinguishes it as a viable choice for end-users seeking a cost effective NGFW option with strong security.

Zscaler's TCO advantage would be magnified when applied across multi-site deployments. For example, a deployment of 100 offices with an appliance-based solution would require additional capital expenditures to account for each site and its failover redundancy, implying the number of devices purchased would be doubled. This far exceeds the cost of Zscaler's single cloud-based solution to cover all offices. For more information on the cost differences among the solutions tested, see page 21.

Zscaler Security Tests

These security tests reflect typical attacks on a network and were provided by Zscaler. Miercom used these tests to verify if Zscaler and its competitors could successfully block these attempts. Miercom verified results using tests provided by Zscaler and its proprietary tests for the following: EICAR file, zipped malicious files, phishing sites, and botnets.

Products are expected to block threats completely; vendors received a "Pass" for 100% blocked, or "Fail" for <100% blocked.

Results Table

Security Tests	Zscaler	Fortinet	Vendor A	Vendor B
Malicious URLs	Pass	Pass	Pass	Pass
Malware over HTTPS	Pass	Fail	Fail	Fail
EICAR Test	Pass	Pass	Fail	Pass
Zipped File (5x)	Pass	Pass	Fail	Pass
Zipped File (10x)	Pass	Pass	Fail	Pass
Phishing	Pass	Pass	Fail	Pass
Botnet	Pass	Pass	Fail	Pass
Exploit & Metasploit	Pass	Fail	Fail	Fail
Cross Site Script & Cookies	Pass	Pass	Fail	Fail
Adware	Pass	Fail	Fail	Fail
Obfuscated JavaScript	Pass	Fail	Fail	Pass
Data Loss Prevention	Pass	Fail	Fail	Fail
Browser Version & Plug-in	Pass	Fail	Fail	Fail

Zscaler succeeded in passing each Security Test when verified by Miercom. The results are summarized in the table on the following page.

Results Summary

Test	Vendors Passed
Malicious URLs	All vendors
Malware Download over HTTPS	Zscaler only. Its cloud platform method remains novel in terms of SSL inspection
EICAR Hosted on Different Site	All, except Vendor A
Zipped Malicious Files	All, except Vendor A
Phishing Sites	All, except Vendor A
Botnets	All, except Vendor A
Blocking Browser Exploit and Metasploit	Zscaler only
Cross Site Script	Zscaler and Fortinet
Adware Sites	Zscaler only
Obfuscated JavaScript	Zscaler and Vendor B
Data Loss Prevention	Zscaler only
Browser Version and Plug-in Control	Zscaler only

Zscaler Data Loss Compliance Tests

Compliance tests provided by Zscaler, evaluated the security appliance's ability to prevent data loss and comply with corporate policies. The following types of data loss and policy restrictions were analyzed:

Credit Card Exposure	This test checks if a set of numbers that match the format of valid credit card numbers can be sent out over the network.
Intellectual Property Exposure	This test checks if the security appliance under test can detect and block an attempt to leak sensitive intellectual property data by various online methods, such as posting the data to a website or emailing it.
Sensitive Information Exposure	This test checks if a set of numbers that match the format of valid United States Social Security numbers (SSNs) can be sent out from the network.
Restricted Access	This test checks the ability of the user to visit a website located in North Korea, which is under US and EU Trade embargo, while using the security appliance under test.
Anonymizer Sites	This test checks the ability of a user to use an anonymizing site, by attempting to visit a blacklisted site through a well-known anonymizer, while using the security appliance under test.

Results Table

Each test received a "Pass" for preventing 100% data loss or a "Fail" for preventing anything less than 100%.

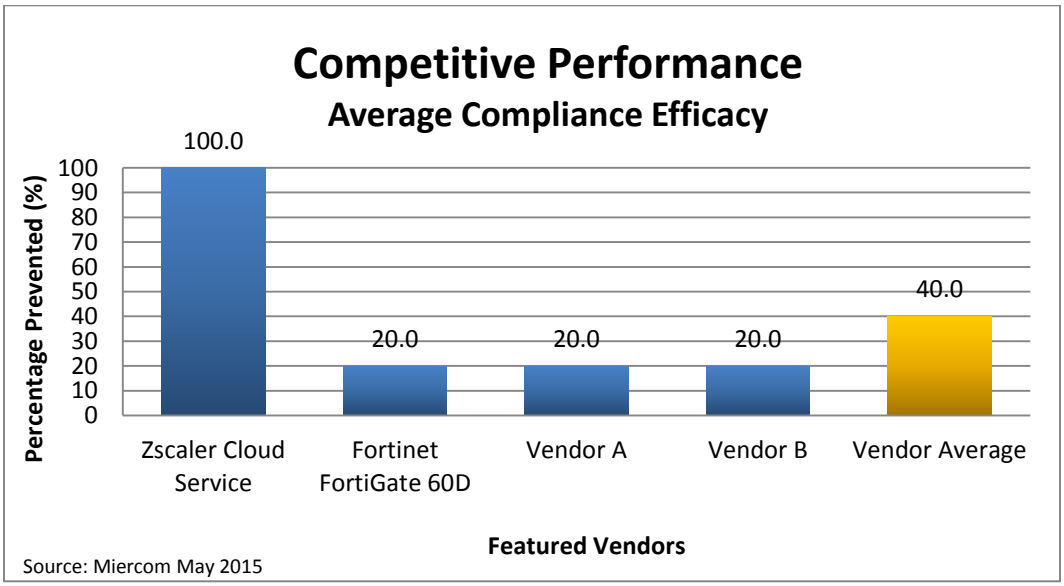
Compliance Tests	Zscaler	Fortinet	Vendor A	Vendor B
Credit Card Exposure	Pass	Fail	Fail	Fail
Intellectual Property Exposure	Pass	Fail	Pass	Fail
Sensitive Info Exposure	Pass	Fail	Fail	Fail
Restricted Access	Pass	Fail	Fail	Fail
Anonymizer Sites	Pass	Pass	Fail	Pass

Zscaler passed every test, scoring 100% in compliance performance, proving advantageous in terms of efficacy for this test series when compared to competing vendors.

Results Summary

Test	Vendors Passed
Credit Card Exposure	Zscaler only
Intellectual Property Exposure	Zscaler and Vendor A
Sensitive Information Exposure	Zscaler only
Restricted Access	Zscaler only
Anonymizer Sites	All, except Vendor A

Below is a comparison of how each vendor performed in the series of compliance tests.



Zscaler scored 100% in compliance efficacy, 60% higher than the average performance. Its results infer its exceptional ability to prevent data loss and adhere to corporate policies.

Discussion of Test Results

Basic Security

Basic security consists of detection of threats that have been in circulation for quite some time. These are the simpler security tests, and although basic, having detection against these tests is vital for a security appliance.

Zscaler performed very well against Miercom's malware set, specifically legacy files, scoring 100%. For Zscaler's security tests, it passed for malicious URL testing, EICAR test files, botnets, exploits, cookie stealing, script injection, adware and sandboxing.

Fortinet maintained fair performance with an average malware blocking efficacy of 67.4%, but it performed 100% detection against the basic threats such as legacy files, botnets and RATs. Other basic security tests that it passed were malicious URLs, EICAR files, phishing, botnets, script injection and cookie stealing; but did not protect against zipped malicious files, exploits, and adware.

Vendor A displayed low performance. Basic malware testing yielded a mere 49% blocking against legacy files, and 0% against botnets and RATs. Although it passed Zscaler's malicious URL test, it could not pass tests for EICAR files, zipped malicious files, phishing, botnets, exploits, cookies, and adware.

Vendor B maintained substantial performance, scoring 100% against basic malware types from the Miercom sample set; and passing Zscaler's security tests for: EICAR files, zipped malicious files, phishing, and botnets. However, it was not recorded as protecting against exploits, script injection, cookie stealing and adware.

Advanced Security

Advanced security tests require more sophisticated methods to protect against threats that either have a more convoluted form of attack or are extracting highly sensitive data.

Zscaler exhibited very strong efficacy against advanced malware samples. The Cloud solution scored 100% in AETs and APTs, and 97% against active threats which are a huge risk to networks on an ever-changing basis. Being that it operates in the Cloud, it has the advantage to scan through traffic in real-time in a way that gives the network the most up to date protection at all times.

Zscaler also passed the test for malware downloaded on SSL, which is a novel approach to detecting malware. It also passed the test against obfuscated JavaScript, a very convoluted approach that attackers use to infuse malicious content. Zscaler also had 100% protection against various types of data loss and compliance.

Fortinet showed fair performance when blocking advanced malware samples, yielding protection 0% against AETs and 65% against APTs. In addition, it could not fully detect malware downloaded over SSL, obfuscated JavaScript detection, data loss prevention, and browser/plugin related vulnerabilities.

Vendor A had low performance efficacy against advanced malware, scoring 0% against AETs and 30% against active threats. APTs were blocked by 80%, so Vendor A was capable of recognizing and blocking persistent threats. However, this appliance was unable to fully inspect malicious content over SSL, detect obfuscated JavaScript, prevent data loss, and protect against browser version and plug-in attacks.

Vendor B performed well against the advanced malware: AETs, APTs, active threats, and obfuscated JavaScript. However, it was incapable of blocking malware in SSL, thoroughly preventing data loss, and protecting against browser version and plug-in vulnerabilities.

Sandboxing Advantage

Sandboxing Limits

Sandboxing is a virtual machine built into a security appliance which tests threats before letting them enter the network. Based on suspicious signatures, threats are flagged for sandboxing to simulate behavior of the file and analysis is run to determine whether or not it is truly malicious. If it is, then it is blocked.

Limits to how many files can be sent through the sandbox depend entirely on the amount of memory that the device can allocate to this function.

Zscaler essentially was found to have no limits since it's a purely cloud-based solution. There is no practical capacity limitation for processing power or memory when processing files for the sandboxing function.

Point-based solutions by definition consist of local hardware devices which are limited by their memory size and CPU when processing files, for their sandboxing solution.

Sandboxing Reports and Forensics

Sandboxing determines whether a threat is truly malicious, but it is helpful to know where a file came from, the type of threat it is, and its analysis details.

Zscaler exhibited excellent report and forensic quality, delivering information about file origin, destination, type, category, analysis and direct URL. It provided a feature to download summaries of the original file, dropped files, and packet captures. From the interface, a user or administrator can see how the file bypassed security, how it networks, how stealth the file is, and which methods were used to evade security. Also, it displays how the threat attempts to leak information, exploit vulnerabilities, and persist against security measures. This sandboxing interface and functionality is above and beyond the basic sandboxing tool of other security appliances.

Fortinet showed decent, albeit rudimentary, quality. It provided only source and destination IPs, analysis, and URL information about each file.

Vendor A displayed very limited capabilities, and was not a valuable source for information regarding files.

Vendor B displayed very good quality, providing file name, category, source and destination IPs, analysis, and URL for each file. Detailed reporting was available and better than other security appliances tested, however not to the extent of the Zscaler's.

Deployment

Deployment complexity is always a consideration for an enterprise due to labor costs and the "opportunity costs" of dedicating technical and management resources to setting up and maintaining security systems.

Zscaler's cloud-based system required little effort in terms of deployment, with no hardware or software involved. An administrator simply has to set up either a Generic Routing Encapsulation (GRE) tunnel or IPSec VPN tunnel to connect the traffic from the network to the cloud portal. The setup was relatively easy and required very little time.

All competing vendors used in-line deployment.

Fortinet was relatively easy to set up since it also came with a configuration wizard. The installation was very quick.

Vendor A had a very difficult set up. This appliance did not come with a configuration wizard, and all settings had to be done manually. The process was time consuming because of the lack of guidance.

Vendor B had a very easy set up, and a configuration wizard made steps taken very simple. However, installation is very time consuming since it requires software, such as configuration blades, updates, downloads and licenses. The updates and downloads took the most time. Deployment was simple, but requires a lot of software installation.

Costs

Implementation of network security technologies can be an expensive process, in terms of product cost, time to deploy, maintenance and personnel expenditures. These factors should be considered when evaluating any security appliance.

Total Cost of Ownership (TCO) valuation is meant to measure cost against performance of the product to give insight to the end user about where their funds are best allocated. Favorable TCO is low, implying that the value is worth more than its cost.

Zscaler does not have any hardware or software, and its set up requires one of two options for deployment, which is up to the user. Given the absence of a physical box, there is no need for labor and installation costs. Its high performance also protects against remediation costs and risk associated with security breaches. Its TCO is very low.

Fortinet produces an appliance that delivers more protection with additional software tools available. The product has reasonable basic security, and an easy, quick deployment. This product is an inexpensive option, however what it saves the user in cost, it leaves open to risk in terms of efficacy. Its TCO is average.

Vendor A has a security appliance that did not perform well in security, and has high price relative to its tested competitors. Considering the difficult and time consuming set up, labor costs would only further increase expenditures. This product is not favorable in terms of either security or price. Its TCO is very high.

Vendor B offers a security appliance that yields more protection with each software blade available. The more software packages added, the higher the cost. Relatively speaking, the appliance costs more than its competitors. However, it offers substantial protection, easy deployment, and a favorable endpoint interface. Its TCO is average.

Fair Test Notification

All vendors with products featured in this report were afforded the opportunity before, during, and after testing was complete to demonstrate the performance of their product(s). Any vendor with a product tested by Miercom in one of our published studies that disagrees with our findings is extended an opportunity for a retest and to demonstrate the performance of the product(s) at no charge to the vendor. All vendors are welcome to demonstrate their performance on their own to Miercom. Miercom will update these results if new data presents itself.

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.