Zscaler Internet Security Protection Test

A test commissioned by Zscaler Inc. and performed by AV-TEST GmbH

Date of the report: June 10, 2020

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Contents

01

Executive Summary

In February 2020, AV-TEST performed a review of the Zscaler Cloud Security Platform.

The review focuses on the protection against zero-day and known malware as well as the effectiveness of the Zscaler Internet Access (ZIA) Security Stack and Advanced Cloud Sandbox functionality.
The test was commissioned by Zscaler and performed by AV-TEST.

In order to ensure a fair review, Zscaler did not supply any samples (such as URLs or metadata) and did not influence or have any prior knowledge of the samples being tested. The test focused on the detection rate of links pointing directly to PE malware (e.g. EXE files), links pointing to other forms of malicious files (e.g. HTML, JavaScript), phishing URLs as well as false positives of websites and downloaded files (installers).
A total of 23,729 different samples were used.

Summary of Test Results

- In prevalent malware testing, a blocking rate of **99.7%** was delivered by using the **Zscaler Internet Access Security Stack and Advanced Cloud Sandbox**
- In real-world testing, based on blocking of known recent indicators, a testing protection rate of **97.7%** was delivered by using the **Zscaler Internet Access Security Stack and Advanced Cloud Sandbox**
- In real-word testing, the **Zscaler Cloud Effect**, which shares threat intelligence across the platform, helped to increase protection from **94.4% to 97.7%**
- Using **Advanced Cloud Sandbox**, coupled with the use of the **Zscaler Cloud Platform and Cloud Effect**, provided the best overall detection results

Test Results

In the first part of this study, the real-world protection against active and viable threats were measured. A malware sample was first accessed at time zero ("Patient 0") and the protection was measured using both the ZIA Security Stack with Cloud IPS and then again with the addition of Advanced Cloud Sandbox. After time zero ("Patient 0"), samples were analyzed again leveraging the Zscaler "Cloud Effect" which shares intelligence across the Zscaler Cloud Platform from other users (or organizations). Testing also leveraged manual submission via Sandbox API. A higher number of blocked samples indicates better results.

Real-World Testing	Samples Blocked %		
Number of test cases	PE URLs 1,747	Non-PE URLs 1,253	Phishing URLs 1,894
ZIA Security Stack (Patient 0)	88.6%	95.1%	88.5%
ZIA Security Stack (Cloud Effect)	91.9%	95.4%	88.5%
ZIA Security Stack w/ Adv. Cloud Sandbox (Patient 0)	94.4%	95.1%	88.5%
ZIA Security Stack w/ Adv. Cloud Sandbox (Cloud Effect)	97.7%	95.4%	88.5%
Sandbox API Results	99.5%	n/a	n/a

In a second test-run, the effectiveness against a set of prevalent malware files was measured. The samples used for the testing were hosted at a dedicated webserver owned by AV-TEST. The test covered hosted PE and non-PE files, as well as modified (slightly manipulated) PE files to defeat signature-based detections. A higher number of blocked samples indicates better results.

Prevalent Malware Testing	Samples Blocked %		
Number of test cases	PE files 10,189	Non-PE files 5,209	Modified PE files 1,131
ZIA Security Stack (Patient 0)	99.7%	99.3%	57.1%
ZIA Security Stack (Cloud Effect)	99.7%	99.3%	100.0%
ZIA Security Stack w/ Adv. Cloud Sandbox (Patient 0)	99.7%	99.4%	95.3%
ZIA Security Stack w/ Adv. Cloud Sandbox (Cloud Effect)	99.7%	99.4%	100.0%
Sandbox API Results	100.0%	n/a	99.7%

Finally, the false positive rates were measured using over 1,000 popular websites (as measured by Alexa's website ranking) and installer downloads of popular applications (PE files). A lower number of blocked test cases indicates better results.

False Positive Testing	Samples Blocked %	
Number of test cases	Alexa URLs 1,253	PE Installers 1,053
ZIA Security Stack (Patient 0)	0.2%	1.1%
ZIA Security Stack (Cloud Effect)	0.2%	1.1%
ZIA Security Stack w/ Adv. Cloud Sandbox (Patient 0)	0.2%	1.5%
ZIA Security Stack w/ Adv. Cloud Sandbox (Cloud Effect)	0.2%	1.5%
Sandbox API Results	n/a	1.0%

Even in the default configuration as "Patient 0", the protection offered by Zscaler was very good. Adding Advanced Cloud Sandbox increased detection significantly, especially in the case of modified (and thus, completely new and unknown) PE files. In both default and Advanced Cloud Sandbox testing, the use of the Zscaler Cloud Platform with Cloud Effect improved detection rates even more.

The full test details of the testing can be found in the following report.

02

Overview of the Zscaler Cloud Security Platform

The Zscaler Cloud Security Platform is comprised of multiple security services, hosted in a purpose built, globally distributed cloud platform

Called Zscaler Internet Access (ZIA), this unified security stack delivers full content inspection of all user traffic and inside of SSL, across 150 global data centers. The following are key components and features of Zscaler Internet Access:

- **Advanced ZIA Security Stack:** The full ZIA security stack contains Cloud Firewall/IPS, Cloud Sandbox, Cloud DLP, Cloud Access Security Broker (CASB) and Browser Isolation. For this test, AV-Test focused on Cloud Sandbox, Cloud IPS and other advanced threat detection engines.

- **Advanced Cloud Sandbox:** Native inline behavior analysis that allows for inspection of all malicious file types and provides ability to quarantine and hold file delivery until confirmed clean.

- **Zscaler Cloud Effect:** Increases protection by sharing threat intelligence across users and organizations using the Zscaler Cloud Platform and Advanced Cloud Sandbox.

- **SSL Inspection:** Available across a globally distributed collection of 150 data centers, delivers unlimited, full inspection of all user traffic to the complete ZIA Security Stack.

03

Zscaler Threat Protection Architecture

For quick and efficient detection of known and unknown threats, Zscaler Internet Access uses a layered approach to threat protection

The Zscaler Cloud Platform is a proxy-based cloud architecture that fully inspects all user content across a collection of threat detection techniques, and inside of SSL. These techniques help to quickly detect and prevent malware and advanced threats. Inspection is also fully distributed across the global Zscaler data center footprint, so every user receives the fastest connection and inspection regardless of location.

The following graphic depicts this top-down approach and how each layer complements the others:

1. **Content Type:** Policy control over file types and URL categories
2. **Reputation:** Blocking of known malicious IP, Domain, URL and File Hash via threat feeds and Zscaler Cloud Effect discovery
3. **IPS & Signatures:** Inspection and protection via Cloud IPS, Yara and AV engines
4. **Advanced Techniques:** Advanced analysis of web content and IOCs via Machine Learning and Zscaler PageRisk engines
5. **Behavior Analysis:** Inline Cloud Sandbox detonation and analysis (enhanced by Machine Learning) of unknown files with ability to hold delivery until confirmed clean

04

Methodology

All of the data used for testing, including all samples, URLs and metadata, was exclusively sourced by AV-TEST.

Zscaler had no access to this data before the testing, nor did Zscaler provide such data for the testing. All samples were previously verified to be either malicious websites, phishing links or known good samples. AV-TEST uses static and dynamic analysis of samples to ensure that the domains are actively hosting malicious content at the time of the testing and exhibit their malicious behavior.

The test was grouped into three main parts:

1. The Real-World Testing, focusing on links to malware and phishing websites which are hosted by the malware authors
2. The Prevalent Malware Testing, focusing on known and unknown malware samples, hosted on AV-TEST's webservers
3. False Positive Testing, covering false alarms and unintentional blocks caused by the protection layer

For the first test, the **Real-World Testing**, the data was split into three categories, covering the different types of attacks:

- URLs pointing to malicious PE files (portable executables for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually HTML or PHP websites, including links to scripts like JavaScript or VBS)
- Links to phishing websites

A total of 4,894 test cases were used. This includes 1,747 malicious links to PE files, 1,253 links to other files with other malicious content (nonPE), as well as 1,894 samples with phishing websites.

The second test, the **Prevalent Malware Testing**, was split in the following three categories:

- Malicious PE files (portable executables for Windows, EXE files)
- Other malicious files (non-PE files, including HTML and PHP websites as well as JavaScript or VBS content)
- Modified malicious PE files (the files were modified slightly from the original form, but are still fully functioning, and are completely new and unknown at the time of the testing)

In total, 16,529 test cases were used. This includes 10,189 malicious PE files, 5,209 other malicious objects as well as 1,131 modified PE samples.

Finally, a **False Positive Testing** was performed, covering the following two test criteria:

- Unintentional blocking rate of good and well-known websites, based on Alexa's top website ranking
- Unintentional blocking rate of installers (setup files) of trustworthy and popular Windows applications (all PE files)

This part of the test included a total of 2,306 test cases, namely 1,253 websites as well as 1,053 installers.

All of the URLs and files were accessed on virtualized Windows systems running the latest edition of Windows 10 Professional (version 1909), with all patches installed. All download attempts were triggered using Python scripts to access the URLs and files for the test. It was checked if the access to the URL or file was blocked or the download of malicious or good content was possible. The tests were performed in January and February 2020.

05

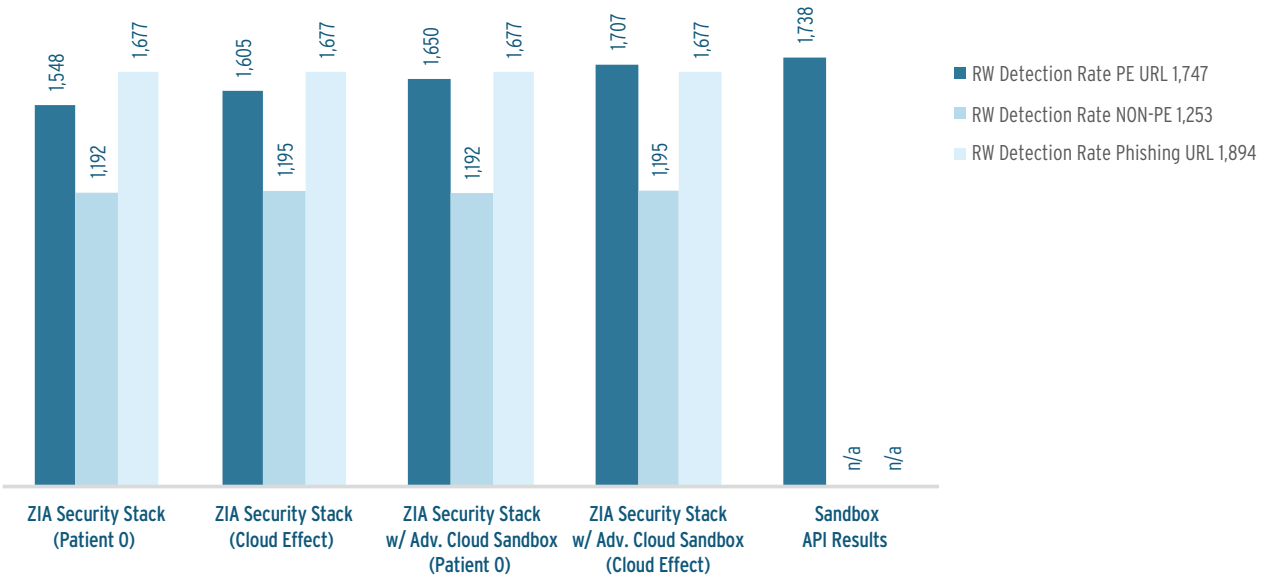
Test Results

In this section, the results of the three different tests - Real-World, Prevalent Malware and False Positives - will be shown and discussed.

Real-World Testing

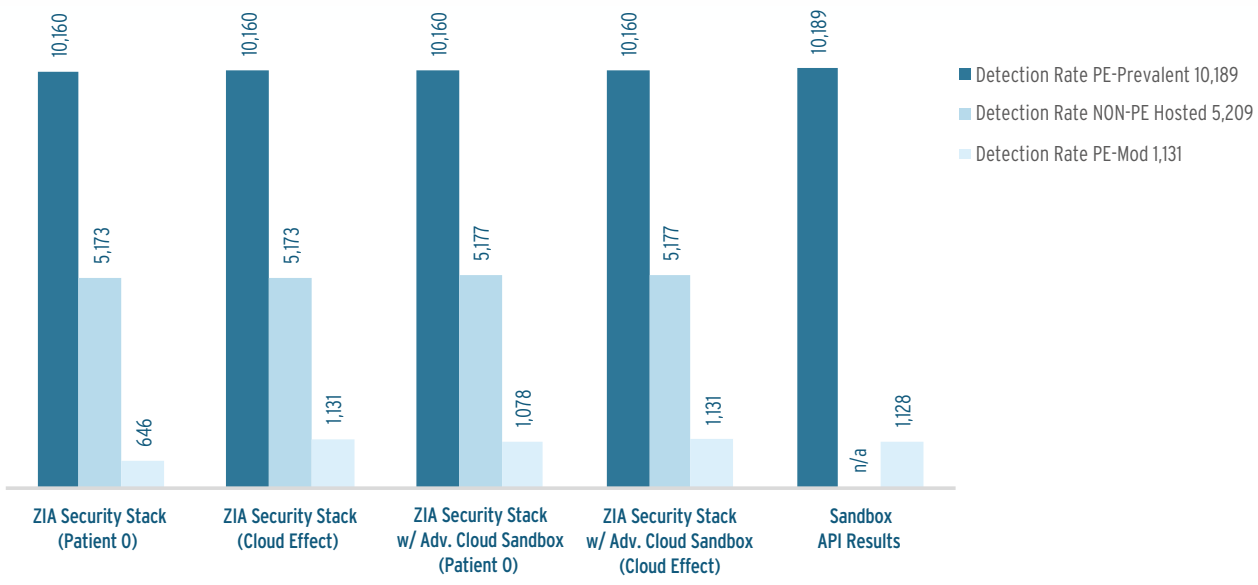
The table below shows the number of Real-World test cases (for every category and the total number) and the number of blocked samples for all configurations being tested. For this protection test, a higher number of blocked samples indicates better results.

The results are clearly showing that even in the default ZIA Security (Patient 0) configuration, the solution already offered a high protection rate. The Advanced Cloud Sandbox especially increased the protection rates for PE URLs while the detection of phishing URLs remains at the same level for all configurations and test cases.



Prevalent Malware Testing

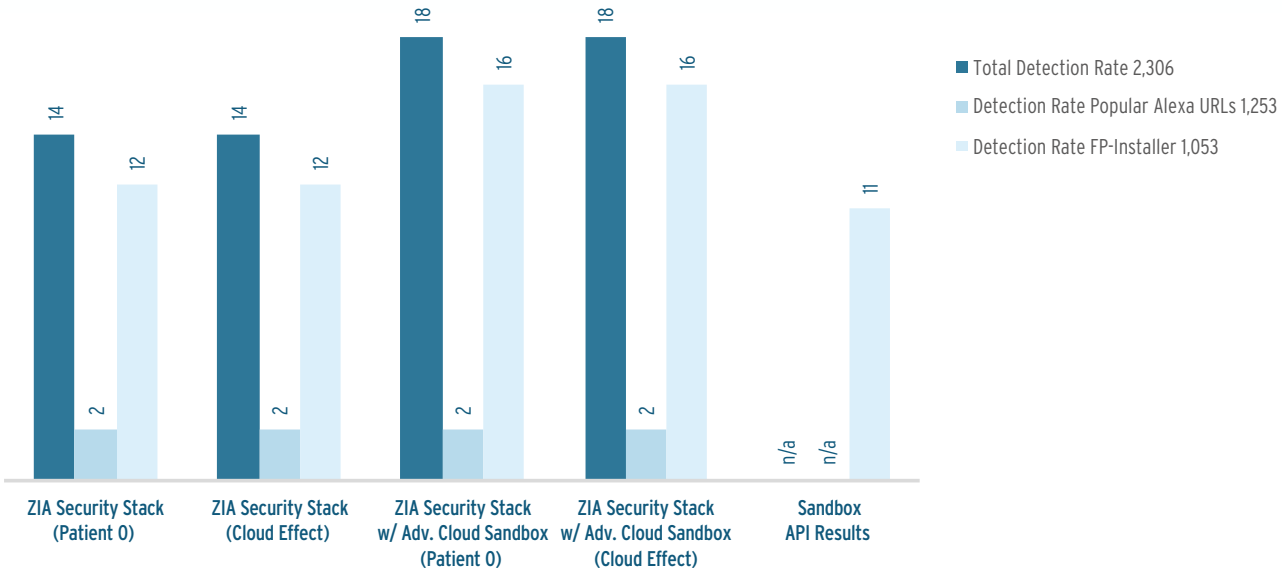
The table below shows the number of Prevalent Malware test cases as well as the number of blocked samples for all configurations being tested. For this protection test, a higher number of blocked samples indicates better results.



In this second part of the test, both the ZIA Security Stack and Advanced Cloud Sandbox demonstrated high detection rates when tested against known, prevalent malware samples. However, the advantage of the Advanced Cloud Sandbox is clearly visible when tested against modified and thus new and unknown malware samples.

False Positive Testing

The table below shows the number of False Positive test cases and the number of unintentionally blocked samples for all tested configurations. For this false alarm and blocking test, a lower number of blocked test cases indicates better results.



The number of falsely blocked websites remained at a similarly low level, regardless of the used Cloud Sandbox level. However, the Advanced Cloud Sandbox increased the number of falsely flagged installers slightly when compared with the ZIA Security Stack.

06

Conclusion

In all test scenarios, the reviewed Zscaler solutions performed very well in case of malware protection and false positive avoidance.

Adding Advanced Cloud Sandbox to the ZIA Security Stack offers the best protection, especially against new and unknown malware. Use of the Zscaler Cloud Effect also improves protection, where new and unknown malware detections are shared across the cloud platform.

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

About AV-TEST

AV-TEST GmbH is an independent supplier of services in the fields of IT Security and Antivirus Research, focusing on the detection and analysis of the latest malicious software and its use in comprehensive comparative testing of security products.

Due to the timeliness of the testing data, malware can instantly be analyzed and categorized, trends within virus development can be detected early, and IT-security solutions can be tested and certified. The AV-TEST Institute's results provide an exclusive basis of information helping vendors to optimize their products, special interest magazines to publish research data, and end users to make good product choices.

AV-TEST has operated out of Magdeburg (Germany) since 2004 and employs more than 30 team members, professionals with extensive practical experience.

The AV-TEST laboratories include 300 client and server systems, where more than 2,500 terabytes of independently-collected test data, containing both malicious and harmless sample information, are stored and processed.

For more information please visit our website at https://www.av-test.org .

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web https://www.av-test.org