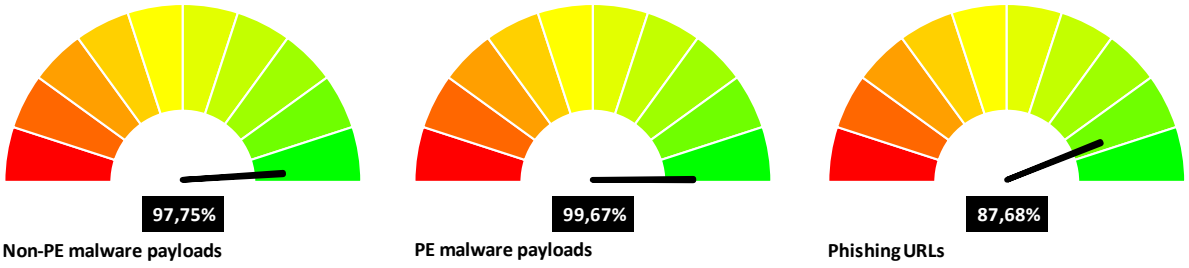
Evaluation of Skyhigh Security Service Edge

A test commissioned by Skyhigh and performed by AV-TEST

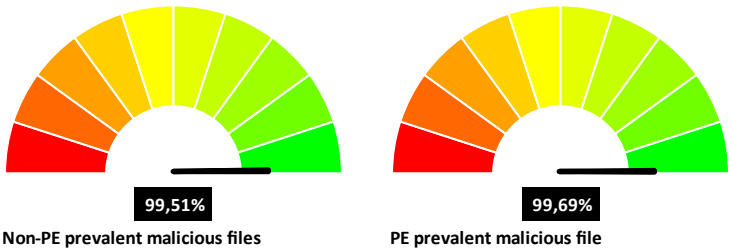
Date of the test report: November 1st, 2023 (version 1.00)

Executive Summary

In August/September 2023, AV-TEST performed a test of the “Skyhigh Security Service Edge” focusing on blocking malicious URLs and phishing websites as well as false positive avoidance. In addition to the standard test scope a test of prevalent malware was carried out. The test was commissioned by Skyhigh Security.



Detection results for malicious URLs



Detection results for malicious prevalent files

To ensure a fair review, Skyhigh did not supply any samples (such as malicious or clean samples, URLs or associated metadata) and did not influence or have any prior knowledge of the samples tested or the testing methodology. All links and malicious samples tested were verified by AV-TEST as recent and active.

The test focused on the detection rate of links pointing directly to portable executables (PEs) malware (e.g., EXE files), links pointing to other forms of malicious files (e.g., html, JavaScript) as well

as phishing URLs. A total of 3,111 malicious samples were tested in the first run. The samples were weighted towards phishing URLs (36.52%), and PE malware (29.12%) while non-PE malware consisted of the remaining (34.36%) of samples.

Additional to the standard test scope a test with prevalent malware samples was executed. Therefore 10.672 PE and 12.477 Non-PE samples were processed.

Besides this, we evaluated the false positive rates using downloads for well-known applications from http and https websites. An additional false positive test was performed against known clean popular websites from Alexa's top list. A total of 3,183 test cases were used.

The full details of the test setup and the testing scenarios can be found in the following sections of this test report.

Test Overview

Every second, AV-TEST discovers three to four new malware variants. This sums up to around 9 million new malware every month, or more than 1.35 billion malware objects in total which are included in AV-TEST's database.

While most malware targets the Windows platform, protection for all operating systems is a required practice. Attaining protection against the growing number of threats is essential for all enterprises. Phishing is a great example of an attack that impacts all operating systems and relies on fooling the end user into thinking the site is legitimate so the attacker can steal sensitive information.

Skyhigh has commissioned AV-TEST to review their Skyhigh Security Service Edge.

Overview of Skyhigh Security Service Edge

According to Skyhigh Security - formerly McAfee Enterprise -, who commissioned the test, their industry-leading cloud-native Security Service Edge (SSE) solution enables your workforce and protects your data across web, cloud, email, and private apps.

It converges Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), Private Access (ZTNA), Data Loss Prevention (DLP) and Remote Browser Isolation (RBI) into a single platform, Skyhigh Cloud Platform.

Skyhigh takes a data-first approach to SSE; data and threat protection are performed at every control point to reduce the cost of security and simplify your management - all from a single converged platform.

Skyhigh's advanced threat protection prevents zero-day threats with Remote Browser Isolation (RBI) by containing web browsing activity inside an isolated cloud, and with the unique Gateway Anti-Malware (GAM) engine with inline emulation-based sandboxing.

https://www.skyhighsecurity.com/products/security-service-edge.html

Test Description

All the tests were performed in AV-TEST's laboratory in Magdeburg, Germany. All data used for testing, including all samples URLs and metadata, was exclusively sourced by us.

Skyhigh did not have access to sample URLs before the testing, nor did they provide such data for the testing. All samples were previously verified by AV-TEST as known to be malicious. We use static and dynamic analysis of samples to ensure that the domains are actively hosting malicious content at the time of the testing and exhibiting their malicious behavior.

The test set is divided into three categories, covering the different types of attacks:

- URLs pointing to malicious PE files (for Windows, EXE files)
- URLs with other malicious destinations (non-PE files, usually html or php websites, including links to scripts such as JavaScript or VBS)
- Links to phishing websites

A total of 3,111 samples were used for the Real World test. This included 906 malicious links to malicious PE files, 1,069 links to other files with other malicious content (non-PE), and 1,136 samples of phishing websites.

For false positive testing, AV-TEST used the following types of known clean files and websites from http and https sources:

- URLs pointing to clean file downloads (mainly PE for Windows, EXE files)
- URLs with other non-malicious destinations (non-PE files, usually clean html or php websites)

All samples used for the false positive testing were carefully selected and validated. In an exhaustive review by AV-TEST, the samples did not show any signs of malicious behavior and were considered clean. A total of 3,183 clean websites and downloads were used for that test (1,156 downloads and 2,027 websites).

Beside these tests an additional prevalent malware detection test was executed. “Prevalent malware” refers to malware that is widespread and commonly encountered in a specific time. 10.672 PE and 12.477 Non-PE prevalent malware samples were hosted at an AV-TEST server and downloaded from that location.

All URLs were accessed on virtualized Windows systems running Windows 10 Professional (English, 64 bit), with all patches installed.

All download attempts were triggered using Python scripts to access the URLs for the test. Testing included checking if access to the URL was successful or if it was blocked by the product. The tests were performed during the period of August 8 to September 22, 2023.

Skyhigh SSE was configured with a standard license.

Focusing on baseline threat protection, Gateway Anti-Malware (GAM) and URL Filtering were used (default), Uncategorized and Unverified (new) websites were allowed. Malware-, Phishing- and Potentially Unwanted categories were blocked explicitly.

Skyhigh Private Access (ZTNA), Remote Browser Isolation (RBI), and User/Entity Behavior Analytics (UEBA) were not used in this test scenario. Customers can further customize their threat protection by adding these security features based on individual needs.

Test Results

For malware PE file download URLs, Skyhigh SSE scored 99.67% as its top efficacy test category. Nearly as effective, the detection of malicious non-PE file download URLs scored 97.75%. Detection of phishing URLs showed a score of 87.68%. False positives were very low at 0.66%.

The detailed results of the detection tests are as follows (higher is better):

Detection Rate	Reference	Detected	In percent
… of PE malware	906	903	99.67%
… of non-PE malware	1,069	1,045	97.75%
… of phishing URLs	1,136	996	87.68%

Detecting the prevalent malware samples Skyhigh SSE shows an efficiency of 99.69% for malicious PE files and 99.51% for Non-PE malware files.

Detection Rate (prevalent)	Reference	Detected	In percent
… of PE malware	10,6726	10.639	99.69%
… of non-PE malware	12,477	12.416	99.51%

For the false positive testing, the detailed results are the following ones (lower is better):

False Positive Rate	Reference	Detected	In percent
… of good applications	1,156	7	0.61%
… of popular Alexa URLs	2,0279	14	0.69%

The Non-PE false positive tests are performed against sites listed in Alexa's list of most popular websites. These samples were verified to be clean, i.e. not containing malicious code. A corporate security product may however want to go beyond detecting malware and block sites with other potential policy violations, such as hosting user-supplied content that can contain stolen goods like software licenses, books or music. Access could imply liability risks to a company. Some of these (BitTorrent) sites are however among the top 500 most popular sites worldwide.

Conclusion

Skyhigh SSE was tested independently by AV-TEST with no knowledge of samples tested or providing samples for the testing. Threat efficacy detection results peaked at 99.67% for PE file URLs and shows a very low false positives rate with 0.66%.

The industry median of the results of all tested SWG products (2022-06 / 2023-10) separated by test categories is for PE 86.83%, Non-PE 90.48% and for phishing URLs 77.69%.

Considering all the results of the products tested by AV-TEST Skyhigh is among the top performers in that product category and offers strong protection against the used test cases.