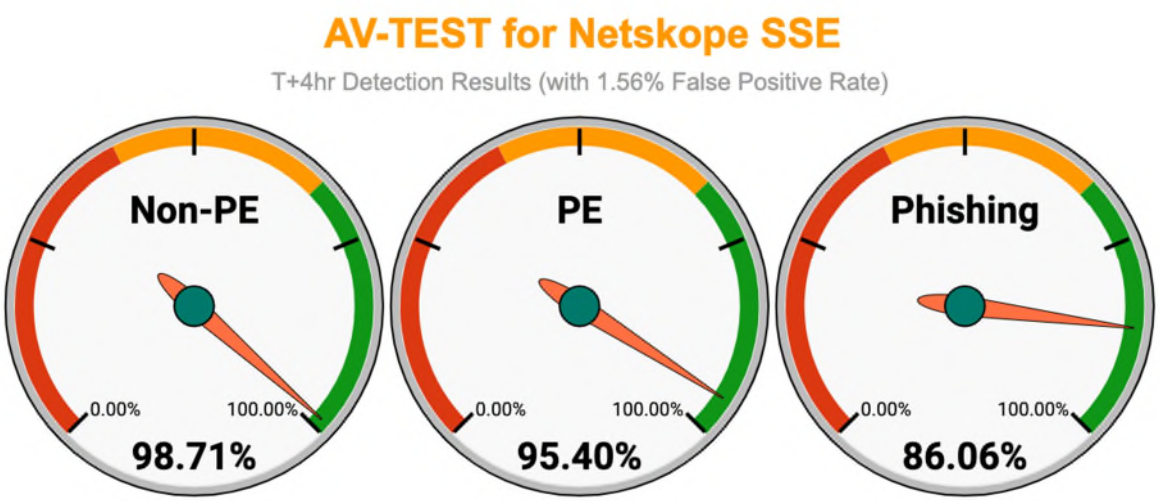
Evaluation of Netskope Intelligent Security Service Edge

A test commissioned by Netskope and performed by AV-TEST

Date of the test report: July 26, 2022 (version 1.00)

Executive Summary

In May 2022, AV-TEST performed a test of the Netskope Intelligent Security Service Edge (SSE) threat protection offering, focusing on blocking malicious URLs and phishing websites as well as false positive avoidance. The test is evaluating the protection at 'time zero' as well as on differences in the detection found four hours later.



In order to ensure a fair review, Netskope 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 3,261 malicious samples were tested in the first run. The samples were weighted towards phishing URLs (38%), and PE malware (35%) while non-PE malware consisted of the remaining (27%) of samples. In the retest, 3064 malicious samples were tested and were similarly weighted towards phishing URLs, PE and non-PE malware.

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 2,372 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 four to five new malware variants. This sums up to around 10 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.

Netskope has commissioned AV-TEST to review their SSE threat protection mechanisms which uses the Netskope Security Cloud to block malicious and unwanted domains, IP addresses, and cloud applications before a connection is ever established inspecting user traffic to websites, SaaS, Shadow IT, IaaS, and public facing custom apps. Multi-layer cloud-based threat protection is an effective way to stop malware earlier and prevent callbacks to attackers for users in any location.

Overview of the Netskope Security Cloud

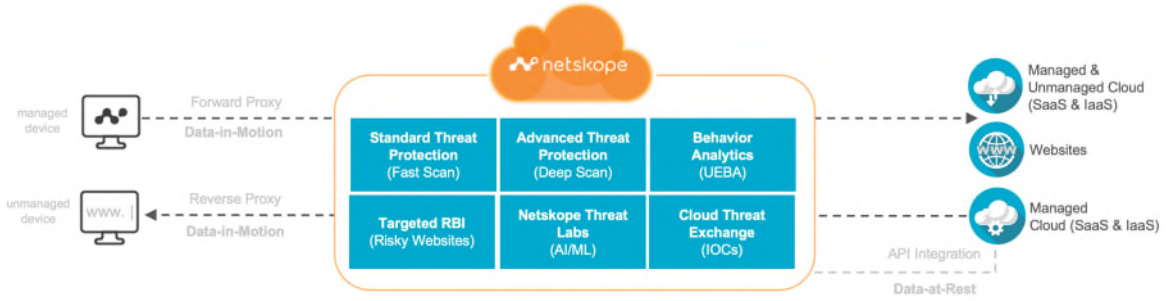
According to Netskope, who commissioned the test, their solution helps reduce risk, accelerate performance, and provide unrivaled visibility into any cloud, web, and private application activity.

To empower safe collaboration, Netskope balances trust against risk with granular controls that adapt to changes in the environment. Netskope SSE protects against advanced and cloud-enabled threats and safeguards data across all vectors (any cloud, any app, any user). A single-pass architecture delivers a fast user experience and simplified operations.

Netskope SSE and Cloud XD provide user context and visibility into User, app, instance, risk, and activity to provide protection from cloud phishing, ransomware and advanced threats.

Netskope Threat Protection inspects all traffic including encrypted traffic and uses a defense-in-depth approach with multiple threat scanning engines including Anti-Virus, inline machine learning classifiers for malware and phishing, URL security, Advanced heuristics analysis and sandbox detonation and analysis.

Cloud phishing evades legacy web and email defenses by delivering phishing attack elements from trusted managed cloud services using rogue account instances. Netskope understands the difference between company and rogue instances for managed cloud services, such as AWS, Azure, GitHub, Box, or Google Drive to block cloud phishing.



Threats detected in the out-of-band Netskope Advanced Threat Detection engines such as behavior analysis-based detection in the Cloud sandbox, advanced heuristics analysis and advanced machine learning (e.g., Office Classifier) are analyzed and extracted Indicators of Compromise (IOCs) are updated for inline blocking at hourly intervals.

The updates are implemented across the Netskope Security Cloud so any threat detected on a single tenant protects the entire Netskope Security Cloud community. In addition, threat intel from 40+ threat feeds and intel sources (e.g., Phishtank) are updated hourly.

The Netskope community-wide intel updates provide incremental improvements in detection rates which is reflected in the 4-hour retest detection results.

Test Cases

All of 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.

Netskope did not have access to sample URLs before the testing, nor did it 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.

Both performed tests were split 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 3,261 samples were used for the initial test-run ('time zero'). This included 1,146 malicious links to PE files, 872 links to other files with other malicious content (non-PE), and 1,243 samples of phishing websites. For the retest after 4 hours, some URLs didn't work anymore, as they were taken offline (e.g., by the attacker or internet provider). Therefore, only 3,064 test cases were used, including 1,086 links to PE files, 852 links to non-PE files and 1126 phishing URLs.

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 2,372 clean websites and downloads were used for the initial test (1,335 downloads and 1,037 websites). For the test-run 4 hours later, a total of 2368 samples could be used (1,334 downloads and 1,034 websites).

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 May 20 to 31, 2022.

Netskope SSE threat protection was configured with standard and advanced threat defense licenses, security risk categories were blocked, however, uncategorized websites and potentially risky sites including newly registered domains (NRDs) and Newly Observed domains (NODs) were allowed. Netskope Cloud Firewall was licensed and active in the testing to allow web traffic on ports 80/443 for TLS inspection and to block non-web traffic. Remote browser isolation (RBI), patient zero sandboxing to hold files until analyzed as clean, Cloud Threat Exchange for IOC sharing, and user/entity behavior analytics (UEBA) detections and policies were all inactive for the testing.

In production deployments, customers can enable added protection by blocking NRDs and NODs or using RBI, including for uncategorized and security risk categorized URLs. Cloud Threat Exchange can be used to share additional custom IOCs and threat intel. A Patient-zero prevention policy can further improve security posture for specific high-risk users (low User Confidence Index or UCI) and/or destinations (low Cloud Confidence Index or CCI).

Netskope User Behavior Analytics (UEBA) can further enhance Netskope threat protection defenses by detecting hidden threats (such as ransomware encrypted file movement) exhibited by anomalous user behaviors and insider threats that may be a result of compromised users.

Test Results

For non-PE file URLs, Netskope SSE initially scored 95.99% and increased to 98.71% in the retest as its top efficacy test category. Nearly as effective, PE file URLs initially scored 90.23% and increased to 95.40% in the retest. Detection of phishing URLs showed a significant improvement from the initial score of 67.74% by increasing to 86.06% in the retest. False positives were low in the initial test at 0.72% and stayed under 2% in the retest to remain a low risk.

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

	Initial 'time zero' test			Retest after 4 hours		
Detection Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of non-PE malware	872	837	95.99%	852	841	98.71%
… of PE malware	1,146	1,034	90.23%	1,086	1,036	95.40%
… of phishing URLs	1,243	842	67.74%	1,126	969	86.06%

The retest after 4 hours showed improvements in detection rates for all three areas with notable improvement in the phishing URL detection rate.

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

	Initial 'time zero' test			Retest after 4 hours		
False Positive Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of good applications	1,335	17	1.27%	1,334	36	2.70%
… of popular Alexa URLs	1,037	0	0.00%	1,034	1	0.10%

As one can see, the false positive rate increased slightly in the second run. However, the risk of a false positive still remains on a low level.

The improvements in the retest can be attributed to the Netskope Security Cloud threat intel updates described in the overview section.

Conclusion

Netskope SSE was tested independently by AV-TEST with no knowledge of samples tested, testing methodology, or providing samples for the testing. Threat efficacy detection results peaked to 98.71% for non-PE file URLs in the retest and false positives remained a low risk for initial and retesting.

Netskope customers may further benefit from using Targeted RBI for risky websites including NRDs and NODs to mitigate hidden threats and Cloud Threat Exchange to share IOCs with endpoints, email security solutions, and third-party threat feeds as these options were not active in the testing. Customers may also benefit from more restrictive access policies not used in this test (such as Patient zero prevention) for users exhibiting risky behaviors and accessing risky applications.