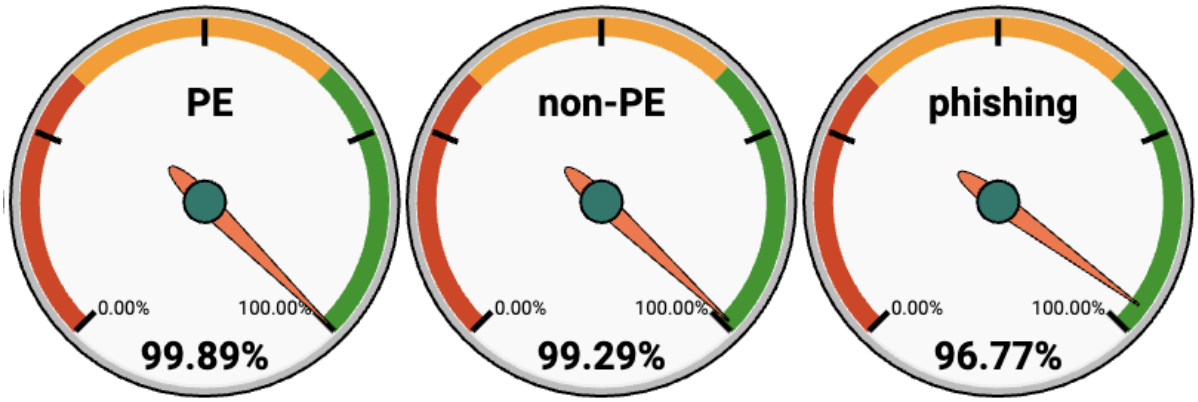
Evaluation of Netskope Intelligent Security Service Edge

A test commissioned by Netskope and performed by AV-TEST

Date of the test report: January 11, 2024 (version 1.00)

Executive Summary

In November 2023, AV-TEST performed a test of Netskope Intelligent Security Service Edge (SSE), 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 the differences in the detection found in a retest four hours later. The test was commissioned by Netskope.



T+4hr Detection results for malicious URLs

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. All tested links and malicious samples were verified by AV-TEST as recent and active.

The test focused on the detection rate of http and https links pointing directly to portable executables (PEs) malware (e.g., EXE, DLL, and other executable files), links pointing to non-PE malicious files (e.g., html, JavaScript, MS Office files) as well as phishing URLs. A total of 3,420 malicious samples were tested in the first run. The one-hour retest used 3278 malicious remaining active samples while the four-hour retest used 3087 malicious remaining active samples.

In addition, AV-TEST assessed the false positive rates by downloading well-known applications from both http and https websites. An additional false positive test was performed against known clean popular websites from Alexa's top list. A total of 2,659 test cases were used to check if the product incorrectly detects benign content as malicious, which could be potentially disruptive.

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

Phone +49 391 6075460 * E-Mail info@av-test.com * Web https://www.av-test.org

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.

Netskope commissioned AV-TEST to review their SSE capabilities in November 2023. By using the Netskope Security Cloud, Netskope SSE blocks malicious and unwanted domains, IP addresses and applications, prior to a connection being established. SSE inspects user traffic to websites, SaaS, Shadow IT, IaaS, and public facing custom apps. Multi-layered cloud-based threat protection stops the transfer of malware at an early stage from any location.

Overview of Netskope Intelligent Security Service Edge

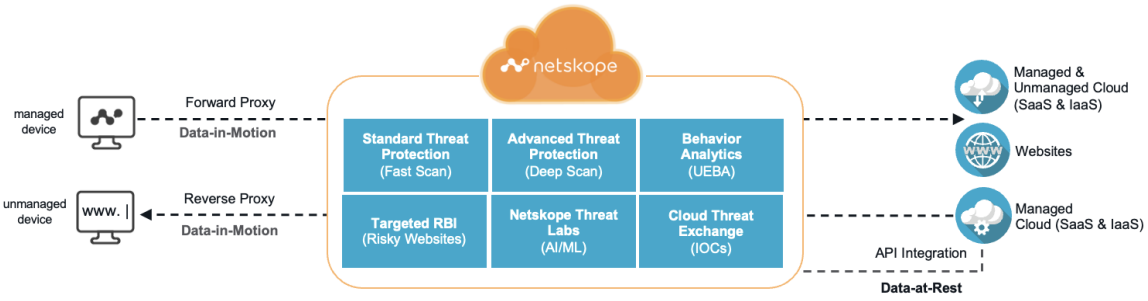
According to Netskope, which commissioned the test, their solution helps reduce risk, accelerate performance, and provide unrivaled visibility into any cloud, web, and managed or unmanaged application activity.

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

Netskope Intelligent SSE and the Netskope Zero Trust Engine provide user context and visibility into user confidence, app, instance, risk, and activity to provide protection from phishing, ransomware and advanced threats. The Zero Trust Engine also provides visibility and control over data movement and activity that may cause or otherwise be related to threats.

Netskope Threat Protection inspects all traffic in real-time including TLS encrypted traffic and uses a defense-in-depth approach with multiple threat scanning engines including Anti-Virus, IPS, inline machine learning classifiers for PE-based malware and phishing, URL security with dynamic ratings, plus advanced heuristics analysis and sandbox detonation and analysis with patient zero protection. All anti-malware and ML-based detections in real-time are also sandboxed for corroboration.

Cloud-hosted malware, exploits, scams, and phishing evades legacy web and email defenses by delivering attack elements from trusted and allowed application and cloud service domains using personal and rogue account instances. Netskope understands the difference between company, personal, and rogue instances for applications and cloud services, such as M365 apps including OneDrive and Sharepoint, Google Workspace apps including Gmail and Gdrive, GitHub, Box, or QQ Messenger to block cloud-delivered attacks in real-time.



New to Netskope since its last AV-TEST report in mid-2022 are advancements for inline AI/ML-based phishing detection where Netskope was awarded three new patents for its use of generative pre-trained transformers (GPT) trained on real-world phishing pages to detect new phishing pages. Cloud-hosted Microsoft fake login forms hosted in trusted SaaS apps are a prime example for this new real-time phishing detection engine.

Threats detected by the out-of-band Netskope Advanced Threat Detection engines such as behavior analysis-based detection in the Cloud sandbox for over 30 file types, advanced heuristics analysis, and advanced machine learning detection (e.g., Office Classifier, PDF Classifier) are analyzed and extracted. Indicators of Compromise (IOCs) are updated for inline blocking multiple times per hour.

Threat intel 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 multiple times per hour.

A significant improvement in threat protection and blocking is seen in the 1-hour retest demonstrating the importance of advanced threat protection background defenses and Netskope generated intel for unknown threats. Further improvement is seen in the 4-hour tests with frequent threat intel feed updates.

Test Description

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

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 to ensure that the domains are actively hosting malicious content at the time of the testing and that the samples are 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)
- URLs of phishing websites

A total of 3,420 samples were used for the initial test-run ('time zero'). This included 995 malicious links to PE files, 1275 links to other files with other malicious content (non-PE), and 1,150 links referring to phishing websites. For the retests conducted after a span of 1 hour and 4 hours, certain URLs were no longer functional, as they were taken offline (e.g., by the attacker or internet provider). For the one hour retest only 3,278 test cases were used, including 980 links to PE files, 1,223 links to non-PE files, and 1,075 phishing URLs. For the four hour retest, only 3,087 test cases were used, including 943 links to PE files, 1121 links to non-PE files and 1,023 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 curated 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 2,659 clean websites and downloads were used for the initial test (1,216 downloads and 1,443 websites). For the retest 1 hour later, a total of 2,659 samples could be used (1,216 downloads and 1,443 websites) unchanged from the initial test run. For the test-run 4 hours later, a total of 2,654 samples could be used (1,214 downloads and 1,440 websites) or five samples less.

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 conducted during the period of November 6 to 28, 2023.

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 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 Newly Registered Domains (NRDs) and Newly Observed Domains (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 between defenses within a security stack. 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 unknown and unapproved data movement and exfiltration, including ransomware encrypted file movement, that may be a result of insider threats or compromised accounts and devices.

Test Results

In terms of PE file URLs, Netskope showed an initial efficacy test score of 95.28%, which then improved to 99.49% in the 1-hour retest, then to 99.89% during the 4-hour retest. Similarly, for Non-PE file URLs an initial 96.63% detection rate was observed, and in the 1-hour retest increased to 99.26% and then the 4-hour retest increased to 99.29%. For the detection of phishing URLs, the initial score was 86.87%, increased in the 1-hour retest to 92%, and then after the 4-hour retest, it significantly improved to 96.77%. False positives were at a low rate of 0.38% at the initial test and stayed at a low rate of 0.75% in the retest.

	Initial 'time zero' test			Retest after 1 hour		
Detection Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of PE malware	995	948	95.28%	980	975	99.49%
… of Non-PE malware	1275	1232	96.63%	1223	1214	99.26%
… of phishing URLs	1150	999	86.87%	1075	989	92.00%

	Initial 'time zero' test			Retest after 4 hours		
Detection Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of PE malware	995	948	95.28%	943	942	99.89%
… of Non-PE malware	1275	1232	96.63%	1121	1113	99.29%
… of phishing URLs	1150	999	86.87%	1023	990	96.77%

The retest after 4 hours showed improvements in detection rates for all three test scenarios with the largest improvement in the phishing URL detection rate. The test scenario with the highest coverage was PE malware followed by Non-PE malware and then phishing URLs. Compared to its mid-2022 AV-TEST report ("Evaluation of Netskope Intelligent Security Service Edge"), Netskope has improved threat detection efficacy in all areas, also as seen in the 1-hour retest reducing the exposure time to new threats and has lowered its false positive rate.

Detailed results of false positive testing are as follows (a lower percentage of false positives is better):

	Initial 'time zero' test			Retest after 1 hour		
False Positive Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of good applications	1,216	7	0.58%	1,216	10	0.82%
… of popular Alexa URLs	1,443	3	0.21%	1,443	4	0.28%

	Initial 'time zero' test			Retest after 4 hours		
False Positive Rate	Reference	Detected	In percent	Reference	Detected	In percent
… of good applications	1,216	7	0.58%	1,214	14	1.15%
… of popular Alexa URLs	1,443	3	0.21%	1,440	6	0.42%

The false positive rate increased slightly in the 1 hour and 4 hour rounds of testing. However, the risk of a false positive remains on a low level upon all test runs.

Conclusion

Netskope Intelligent Security Service Edge (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 reached peaks of 99.89% for PE file URLs, 99.29% for Non-PE malware URLs, and 96.77% for phishing URLs in the retest with a consistently low risk of false positives during all three testing phases.