Netskope One Threat Protection

Data Sheet

Prevent Web and Cloud-enabled Threats

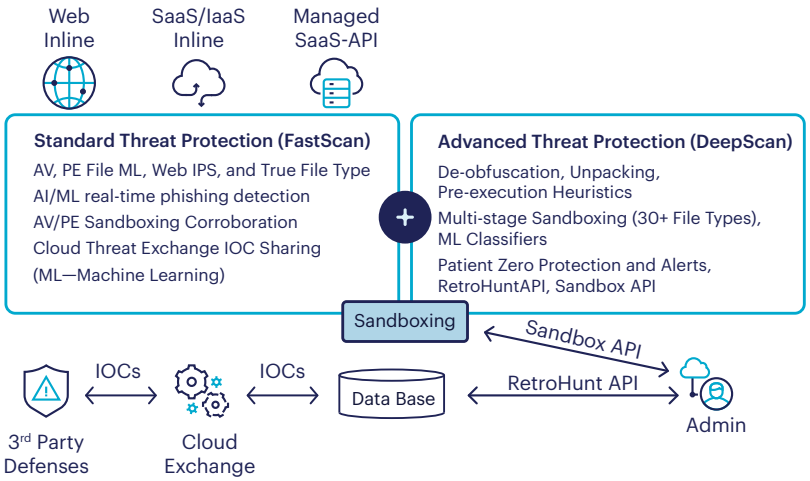
Multi-layer threat protection from malware and advanced threats for inline web and cloud traffic, and for data at rest in managed apps and cloud services. Plus, integration for automated and bidirectional threat intel sharing between defenses and threat intel sources.

Why is Netskope the best choice?

Netskope One Security Service Edge (SSE) threat protection provides high-efficacy threat detection and blocking for advanced malware (such as ransomware) and phishing. See the 2024 AV-Test report for details. Unlike endpoints, for gateways with a few milliseconds to detect threats, the results are "best in class" for threat efficacy with a fast user experience.

Complete SSE threat protection for secure access service edge (SASE) architecture

- **Inline Machine Learning PE Analysis:** Provides patient zero threat protection against new malware alongside anti-malware, web IPS, sandboxing, threat intel feeds, and automated iOC sharing in standard threat protection.
- **DeepScan Background Analysis:** Provides deobfuscation and recursive file unpacking, pre-execution heuristics, and multi-stage sandboxing for 30+ file types with behavior analysis in advanced threat protection.
- **Patient Zero Protection and Alerting:** DeepScan new malware detections provide patient zero protection and alerts for first exposed user(s), plus Cloud Exchange automates investigations into SOAR, XDR, and MDR services.
- **Sandbox and RetroHunt APIs:** New advanced Sandbox API for file submissions with MITRE ATT&CK analysis, plus a RetroHunt API by file hash, determines if a file is malicious or benign.



Key Benefits and Capabilities

Proven Effective Threat Protection

Netskope One SSE detected 99.29% for non-portable executable (PE) URLs and 99.89% for PE URLs in the 2024 AV-TEST. View the report for details.

Patient Zero Protection Against PE Malware

Standard ML defense against new PE malware to complement anti-malware, plus patient zero alerts from advanced defenses for first exposed users.

Standard and Advanced Sandboxing

All AV and ML standard threat detections are sandboxed. Advanced sandboxing adds detailed analysis with MITRE ATT&CK, sandbox API file submission, RetroHunt API by hash, and unique patient zero detections.

Automated Threat Intel Sharing

Cloud Threat Exchange is no charge to customers to automate bidirectional IOC sharing between their defenses, including endpoints, email security, and threat intel sources.

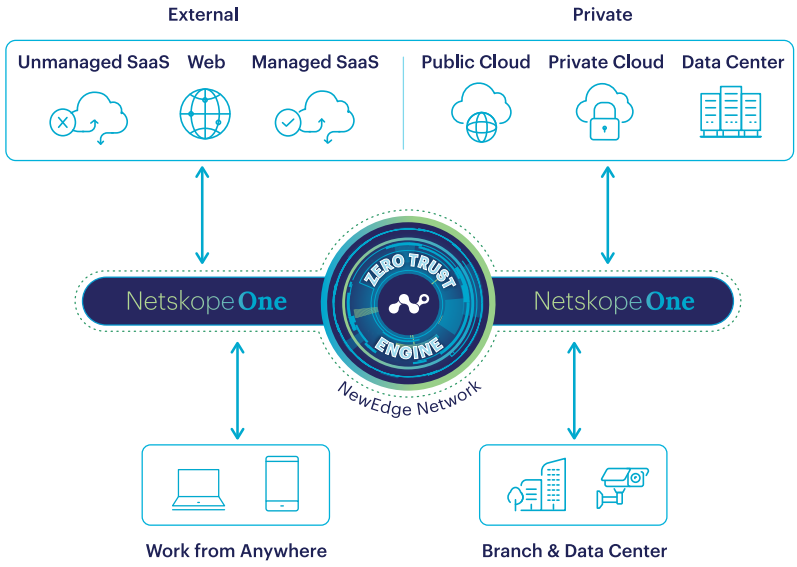
Hybrid Work First Line of Defense

Transform to SSE for any user, device, and location instead of hairpinning traffic to legacy security appliances unable to decode application and cloud services.

> "Netskope scored 99.89% for PE file URLs and 99.29% for non-PE URLs, plus 96.77% for phishing attacks."
>
> – AV-TEST Report, January 2024

The Netskope Difference

Netskope One is a converged security and network as a service platform. Through its patented Zero Trust Engine, AI innovation, and the largest private security cloud we make it easy for our customers to defend their businesses and data while delivering a phenomenal end user experience and simplified operations. The platform delivers AI-powered data and threat protection that automatically adapts to the ever-growing data landscape, including the widespread adoption of generative AI and new AI-driven attacks.



FEATURE	CAPABILITY
Standard Threat Protection	Provides anti-malware, ML-based PE file analysis, AI/ML real-time phishing detection, AV/ML corroborative sandboxing, web IPS, true file type checks, and 40+ threat intel feeds. Web filtering also provides security risk categories to block.
Advanced Threat Protection	Adds background defenses for deobfuscation, recursive file unpacking, pre-execution heuristics, multi-stage sandboxing for 30+ file types, ML classifiers and analysis, patient zero protection and alerts for new detections, sandbox API for file submissions, RetroHunt API by file hash, and MITRE ATT&CK sandbox analysis reports. Plus, inline malware retention into customer cloud storage and API inspection quarantine.
Cloud Exchange	Four modules to share threat intel, automate workflows, exchange risk scores, and export logs. No charge to customers with more than 70 partner integrations. The Cloud Threat Exchange (CTE) module can be used with standard or advanced threat protection to automate IOC updates between customer defenses.
Add-on Defenses (RBI, CFW, IPS, DNS Security, UEBA)	Enhance threat protection with Targeted or Extended Remote Browser Isolation (RBI) for risky websites and personal communications, Firewall-as-a-Service (FWaaS) and Intrusion Protection (IPS) for non-web egress traffic, DNS Security for threats and new domains, and Behavior Analytics (UEBA) to detect insiders, data theft and exfiltration, device or account compromise, and leverage User Confidence Index (UCI) scoring in real-time adaptive access poilcies.
Sandbox File Type Support	Sandbox file formats include: .apk, .csv, .dex, .jar, .html, .htm, .json, .swf, .mht, .eml, .mbx, .pem, .crt, .cer, .key, .pdf, .txt, .sgm, .tsv, unicode text files, .xhtml, .xml, .xpi, Archives (.7z, .lzfse, .msix, .war, .whl, .rar, .rev, .tar, .zip), and Microsoft files (.accdb, .mdb, .chm, .xlsx, .xlsm, .msg, .pptx, .pptm, .xap, .docx, .docm, .msi, .bat, .cmd, .one, .lnk) and may include other file formats.

netskope

Interested in learning more? Request a demo

Netskope, a global SASE leader, uses zero trust principles and AI/ML innovations to protect data and defend against cyber threats, optimizing both security and performance without compromise. Thousands of customers trust the Netskope One platform and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity. Learn more at netskope.com.