Netskope Threat Protection

Data Sheet

Prevent Web and Cloud-enabled Threats

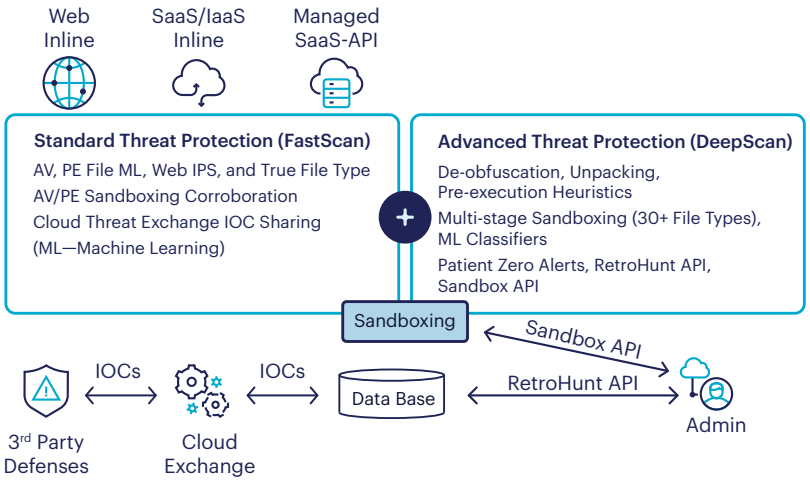
Multi-layer threat protection from malware and advanced threats for inline web and cloud traffic, and for data at rest in managed apps and cloud services. Plus, integration for automated and bidirectional threat intel sharing between defenses and threat intel sources.

Why is Netskope the best choice?

Netskope Intelligent Security Service Edge (SSE) threat protection provides high-efficacy threat detection and blocking for advanced malware (such as ransomware) and phishing. See the recent 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 event 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 Alerting:** DeepScan new malware detections provide patient zero 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 SSE detected 98.71% for non-portable executable (PE) URLs and 95.4% for PE URLs in a recent 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 detections get standard sandboxing for over 30 file types. 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.

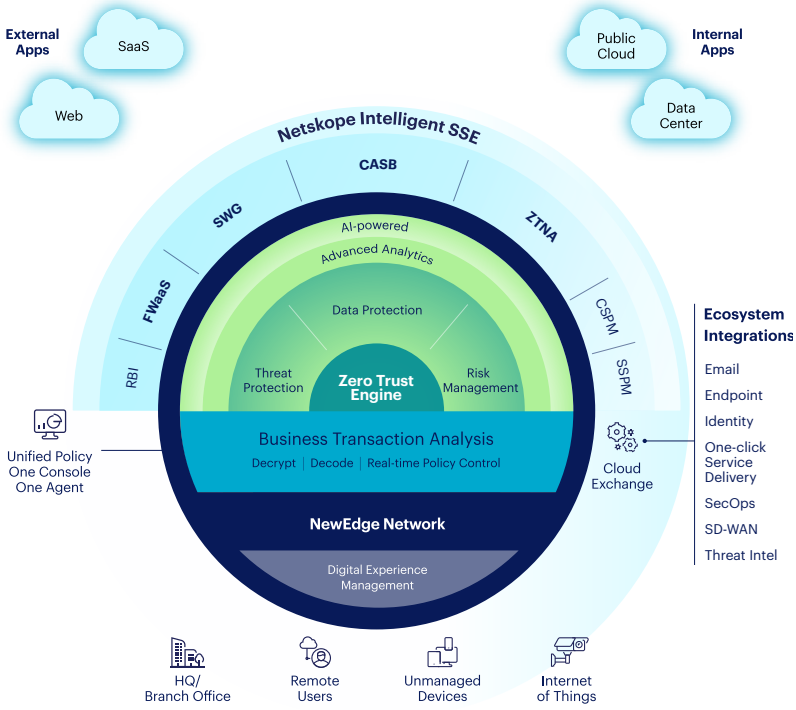
"For non-PE file URLs, Netskope SSE scored 98.71% in the retest as its top efficacy test category."

– AV-TEST Report, 26 July 2022

The Netskope Difference

Fast everywhere, data-centric, and cloud-smart.

Using patented technology called Netskope Cloud XD™, the Netskope Security Cloud eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites. With full control from one cloud, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection, including targeted RBI for risky websites that stops elusive attacks.



FEATURE	CAPABILITY
Standard Threat Protection	Provides anti-malware, ML-based PE analysis, 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 alerts for new detections, sandbox API for file submissions, RetroHunt API by file hash, and MITRE ATT&CK sandbox analysis reports.
Cloud Exchange	Four modules to share threat intel, automate workflows, exchange risk scores, and export logs. No charge to customers with more than 60 partner integrations. The Cloud Threat Exchange (CTE) module can be used with standard or advanced threat protection to automate IOC updates.
Add-on Defenses (RBI, CFW, UEBA)	Enhance threat protection with Targeted Remote Browser Isolation (RBI) for risky websites, Cloud Firewall (CFW) for all egress ports and protocols, and Behavior Analytics (UEBA) to detect device or account compromise, risky insiders, data exfiltration, plus user anomalies with User Confidence Index (UCI) risk scoring.

netskope

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. The Netskope platform provides optimized access and zero trust security for people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.