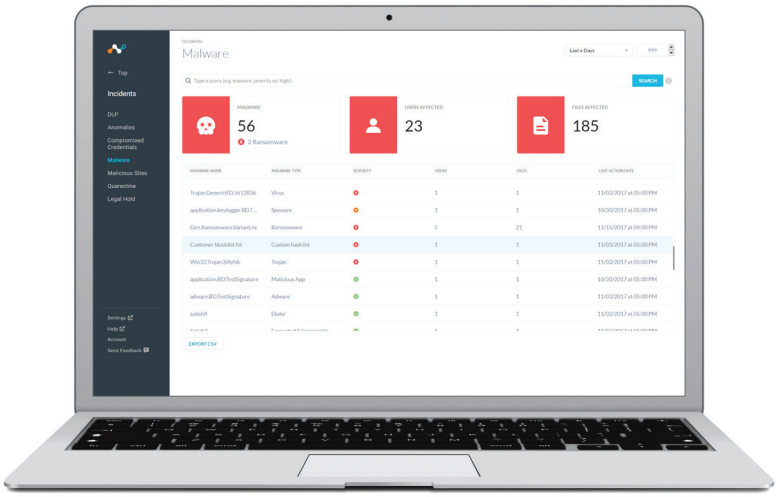
Netskope Advanced Threat Protection with Cylance

AT A GLANCE

- AI-based malware detection powered by Cylance available in Netskope Security Cloud
- Complements Netskope's already-robust Threat Protection solution that includes:
  - Pre-execution, heuristic analysis as well as dynamic, sandbox analysis
  - Unique technology for detecting ransomware outbreaks and automated recovery workflow
  - Threat intelligence sharing across Netskope cloud in minutes
  - STIX/TAXII integration to enrich other security tools with threat intelligence



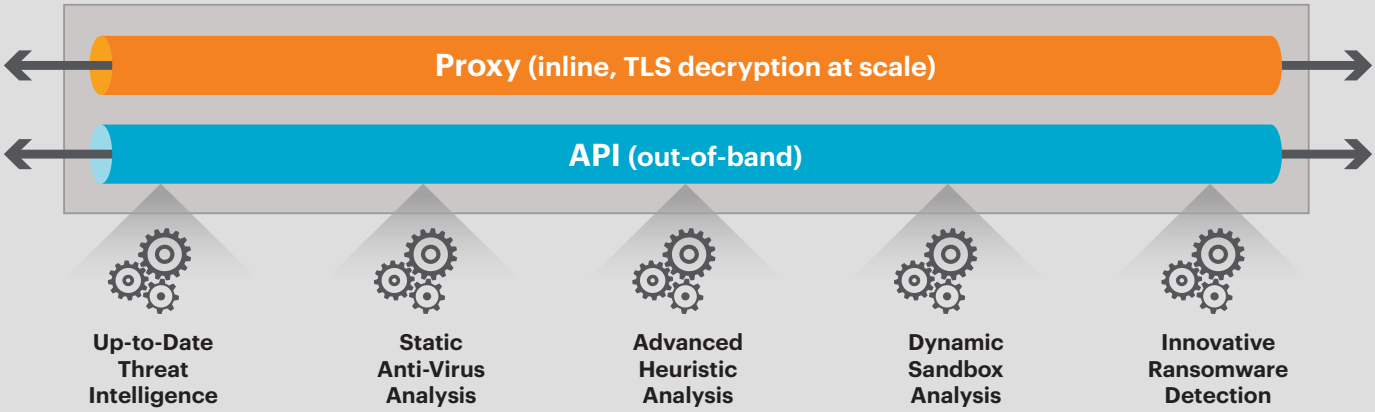
With novel cyber attacks emerging at a rapid pace and evading conventional defenses, organizations must look to new strategies and capabilities. Netskope Advanced Threat Protection with Cylance performs deep analysis to detect and prevent evasive, zero-day threats from the cloud and web.

PRODUCT OVERVIEW

The growing use of cloud services makes them an attractive target for attackers, and the web has long been a prime vector to spread malware and carry out other malicious activity. Backed by Netskope Threat Research Labs, a dedicated team focused on the discovery, analysis, and prevention of advanced threats, Netskope Threat Protection delivers state-of-the-art technologies — pre-execution, heuristic analysis and dynamic, sandbox analysis — to detect and prevent evasive, zero-day threats. The addition of Cylance as a detection engine in the Netskope Security Cloud allows for an added layer of protection with AI-based malware detection technology.

Netskope Threat Protection also provides innovative ransomware detection and remediation capabilities, which protect cloud storage services from propagating ransomware. Unauthorized encryption due to ransomware is detected in sanctioned cloud services — such as Microsoft Office 365 — by analyzing file operations and file content across more than 70 dimensions. Upon detecting ransomware, Netskope provides an integrated workflow that uses cloud storage service versioning capabilities to restore affected files from earlier versions.

Multi-Engine Threat Protection for Cloud and Web



360 DEGREE CLOUD AND WEB VISIBILITY

The Netskope all-mode architecture provides unparalleled visibility into the cloud and web, whether your users are on premises or remote, and whether they are using a browser, sync client or mobile app. Netskope also decrypts TLS-encrypted traffic, which is used by more than 90% of cloud services and more than half of all websites. Once Netskope inspects your cloud and web activity, multiple threat detection engines run in parallel. In addition to static anti-virus analysis and machine-learning-driven anomaly detection, Netskope runs the following additional advanced detection engines.

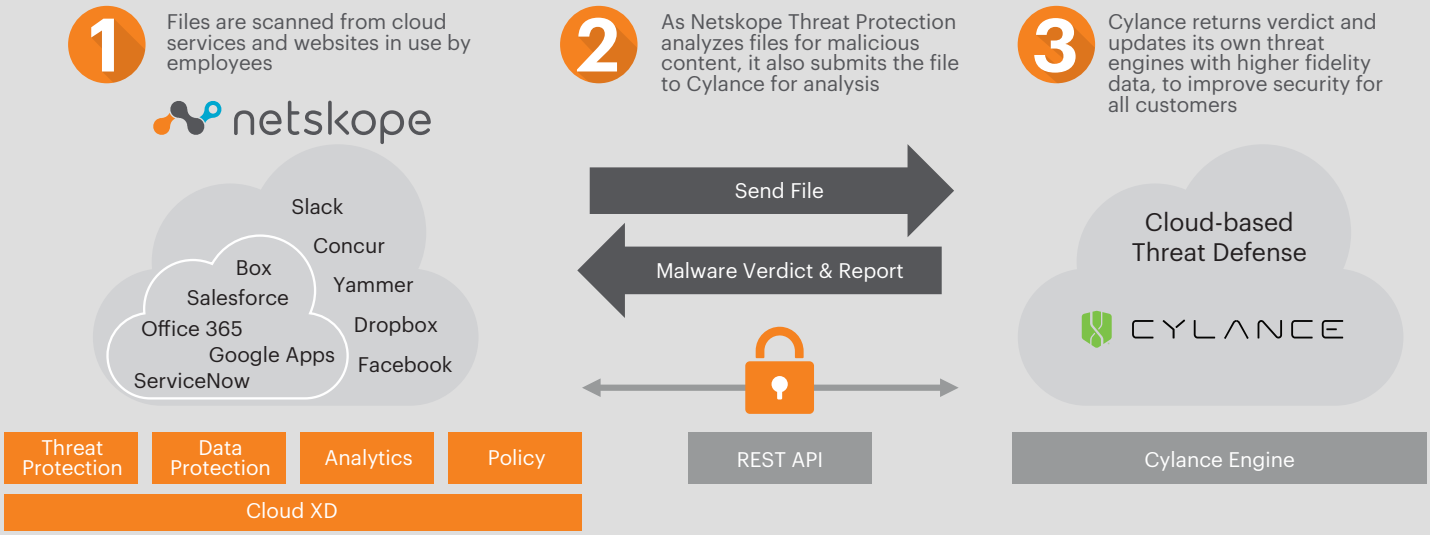
ADVANCED HEURISTIC ANALYSIS

The latest cyber attacks use layers of obfuscation and packing to evade conventional detection and analysis tools. Netskope recursively unpacks files and extracts internal objects to make them fully available for analysis. Advanced static analysis of binary files performs a deep analysis of binary file components without executing them. This pre-execution analysis identifies threat indicators across a wide range of binary file types, including Windows, Mac OS, Linux, iOS, Android, and more.

DYNAMIC SANDBOX ANALYSIS

Behavior-based analysis is a key technology for security teams to detect advanced threats. By detonating suspect files in a controlled, sandbox environment, files can be monitored for a wide range of malicious behavior. Effective sandbox technology must anticipate and defeat sandbox evasion techniques built into advanced malware, and also be architected for high performance to enable advanced threat detection at scale. Netskope Threat Protection includes a dynamic sandbox analysis engine that is immune to malware evasion techniques and is built on the Netskope high-performance, cloud-scale security platform.

Cylance in the Netskope Security Cloud



RANSOMWARE DETECTION AND REMEDIATION

Netskope Threat Protection includes Netskope's innovative ransomware detection and remediation technology. Files stored in sanctioned cloud storage services — such as Microsoft Office 365 — are examined by the Netskope ransomware detection engine. Proprietary machine learning monitors file operations and uses advanced data transformation algorithms to detect unauthorized file encryption using more than 70 dimensions. Upon the detection of ransomware encryption in a cloud storage service, Netskope third-party EDR integrations isolate and remediate affected endpoints. Finally, the Netskope platform restores encrypted files via an integrated workflow using previous versions in cloud storage services.

SHARING CLOUD THREAT INTELLIGENCE

Netskope Threat Research Labs, the dedicated Netskope threat intelligence team, actively researches advanced threats and curates threat intelligence from more than 40 external sources to keep Netskope Threat Protection ahead of new and emerging threats. In addition, new threat intelligence detected by the Netskope advanced threat detection engines is quickly shared across the Netskope cloud service to provide collective protection against newly discovered threats. Netskope also offers a REST API and supports STIX/TAXII and OpenIOC to enable the threat intelligence from the Netskope platform to be shared with other security tools.

CYLANCE ENGINE INTEGRATION

Netskope embeds Cylance's next-generation anti-malware engine that leverages AI, as an additional layer of malware scanning and dynamic analysis. As Netskope analyzes files for malicious content, in addition to existing threat detection engines in Netskope Threat Protection, they can now be analyzed by Cylance's predictive models (running inside the Netskope Security Cloud) to classify files as good or bad by correlating them with the features found in millions of good and bad samples. This enables further analysis of suspected malware — with a Cylance confidence scored returned upon analysis of each sample. This helps organizations ensure employees are protected from zero-day and unknown malware with multiple layers of analysis.

Netskope Advanced Threat Protection with Cylance

FEATURE	DESCRIPTION
Advanced Heuristic Analysis	• More than 3,500 file format families identified • Recursive unpacking of more than 300 families of installers, packers, and compressors • Static binary analysis extracts more than 3,000 threat indicators for Windows, Mac OS, Linux, iOS, Android, firmware, Flash, PDF, and other document types
Dynamic Sandbox Analysis	• Behavior-based analysis of files detonated in controlled, virtual environment • More than 30 file types supported including executables, scripts, and office documents • Includes Windows 7, Windows 8, and Windows 10 emulation environments
AI-based malware detection powered by Cylance	• Files scanned by Cylance engine in the Netskope cloud for further analysis • Add another layer of protection by scanning portable executables, PDFs, and Microsoft Office files for zero-day and unknown malware with Cylance machine learning algorithm • Gain a threat indicator and confidence score from Cylance's predictive model that classifies files as good or bad by correlating them with features found in millions of good and bad samples
Ransomware Detection and Remediation	• Scans files stored in sanctioned cloud services such as Microsoft Office 365 • Proprietary machine learning and advanced data transformation algorithms analyze files across more than 70 dimensions to detect unauthorized encryption • Integrated remediation workflow restores affected files to last known good versions in cloud storage services
Cloud Threat Intelligence	• Backed by Netskope Threat Research Labs, a dedicated team researching cloud threats and curating more than 40 external threat intelligence feeds • New threats detected by advanced engines quickly shared to provide collective protection • Export detected threat indicators/IOCs in STIX format to share with third party security products

THE NETSKOPE DIFFERENCE

Eliminate blind spots

Netskope Cloud XD™ understands SaaS, IaaS, and web in extreme definition to eliminate blind spots

Stop elusive attacks

Advanced threat protection stops elusive attacks that traverse SaaS, IaaS, and web to inflict damage

Guard data everywhere

360º data protection guards data everywhere through award-winning DLP and encryption

Full control, one cloud

Full control of SaaS, IaaS, and web, from one cloud-native platform that scales automatically

netskope

Netskope is the leader in cloud security. We help the world's largest organizations take advantage of cloud and web without sacrificing security. Our patented Cloud XD technology targets and controls activities across any cloud service or website and customers get 360-degree data and threat protection that works everywhere. We call this smart cloud security.