Dell SafeData

Netskope Cloud Inline

Cloud Access Security Broker, (CASB) with Inline - enabled protection

Confidently adopt cloud applications and services – without sacrificing security.

Netskope, a cloud access security broker (CASB), enables you to quickly identify and manage the use of cloud applications, regardless of whether they are managed or unmanaged and prevents sensitive data from being exfiltrated from your environment by risky insiders or malicious cybercriminals.

A Secure Access Services Edge (SASE) architecture makes it possible to identify users and devices, apply policy-based security controls, and deliver secure access to the appropriate applications or data. These capabilities directly align with the foundation of Netskope's cloud-native Security Platform, built to understand and protect SaaS, web, and IaaS environments while accessed from any device. All done from a single console, with a single architecture and integrated policies for all of the SASE services, including CASB, SWG, and Private Access.

Offering real-time, inline enforcement of security policies to prevent data loss and stop threats.

Unlike other CASB vendors, who provide API-only deployment modes, Netskope can provide Inline and API-based protection for cloud applications. With Inline protection, a user's corporate traffic is analyzed, and protections are triggered in real-time. Inline policy controls allow policy enforcement across thousands of SaaS applications and provide more granular controls specific to the application beyond the limits of what the API offers.

The Netskope Security Cloud Platform meets the Federal Risk and Authorization Management Program (FedRAMP) requirements and has achieved FedRAMP Authorization for its SASE-based TIC 3.0 Solutions.

Use Cases

Govern Usage – Netskope CASB can govern your organization's cloud usage and help discover "Shadow IT" with granular visibility and control.

Secure Data – Protects and prevents the loss of sensitive data across all the cloud services in your environment, not just the ones you sanction, whether users are on-premises or remote, on a mobile device, accessing from a web browser, entering from a mobile app or sync client. Secure sensitive content with 3,000+ data identifiers, support for 1,400+ file types, custom regex, fingerprinting, exact data match, and more. Use pre-defined profiles such as personally identifiable information (PII), protected health information (PHI), payment card industry (PCI) data, and source code, or create a custom profile. Remediate by putting files in legal hold, quarantine, or even encrypting the file.

Protect Against Threats - Netskope delivers comprehensive threat defense for all cloud and web services in real-time, with multi-layered threat detection and response capabilities. Multiple layers of threat detection include advanced malware inspection, machine learning driven anomaly detection, heuristic analysis, and sandbox analysis, which are all dynamically updated using multiple threat intelligence sources. Automate actions to quickly eliminate known threats as well as workflows to analyze further and reverse the effects of new attacks, which too often evade existing security solutions. Automatically reset compromised credentials as well when employees log into sanctioned cloud services like Microsoft Office 365 or Google G Suite.

Cloud Inline CASB Offering

CASB with Inline protection comes in a Standard, Professional, or Enterprise package based on the level of Data Loss Prevention (DLP) and Threat Protection needed. See below for further details.

Netskope CASB Inline	Inline Protection	Data Loss Prevention	Threat Protection
Standard	Yes	Standard	No
Professional	Yes	Standard	Standard
Enterprise	Yes	Advanced	Advanced

Key Features

Standard Data Loss Protection (DLP), as part of the CASB Standard and Professional offerings, provides; data-in-motion analysis for cloud apps and services, plus web traffic, files, and forms. It includes 40+ regulatory compliance templates, including GDPR, PCI, PHI, PII, source code, and more, leverages 3,000+ data identifiers for 1,400+ file types, plus custom regex, patterns, and dictionaries. It also now includes AI/ML standard document classifiers (e.g., resumes).

Advanced Data Loss Protection (DLP), as part of the CASB Enterprise offering, includes standard DLP plus; file fingerprinting with the degree of similarity and exact data matching inline. It includes AI/ML classifiers for documents (e.g., patents, source code, tax forms) and images (e.g., desktop screen captures, driver licenses, IDs, passports) inline as well.

Standard Threat Protection, which is part of the CASB Standard and Professional offering, provides; anti-malware engines, client traffic, exploit protection, true file type analysis, 40+ threat intel feeds, bare-metal sandboxing of portable executable (PE) files, and user/entity behavior analytics (UEBA) sequential anomaly rules.

Advanced Threat Protection as part of the CASB Enterprise offering includes standard threat protection plus; de-obfuscation and recursive unpacking of 350+ families of installers, packers, and compressors; pre-execution analysis and heuristics of 3,500+ file format families and 3,000+ static binary threat indicators; bare-metal sandboxing for 30+ file types, including executables, scripts, and documents, multiple ML-models and engines managed by Netskope, plus third-party sandbox and risk-based inspection (RBI) integration.

- Uncover and protect sensitive content stored in your cloud services
- Inventory content and users
- Perform a variety of actions such as revoke access, quarantine, and encrypt
- Simple and frictionless out-of-band deployment

Contact your dedicated Dell Endpoint Security Specialist today at endpointsecurity@dell.com about the Dell SafeData and SafeGuard and Response products that can help improve your security posture

netskope