Solution Brief

Next Generation Secure Web Gateway

Provides next generation secure web gateway (Next Gen SWG) capabilities to prevent malware, detect advanced threats, filter websites by category, protect data, and control apps and cloud services for any user, location, or device. Single-pass inline proxy unmatched for its ability to decode cloud and web traffic including instance and activity.

Quick Glance

- Web and cloud granular policy controls including instance, activity, and data
- Single pass advanced threat and data protection with behavior anomaly detection
- Single cloud console with shared policy controls for SWG, Cloud/SaaS, and DLP
- Mature inline proxy protecting Fortune 100 customers for over eight years
- Cloud performance and global scale to protect any user, device, or location

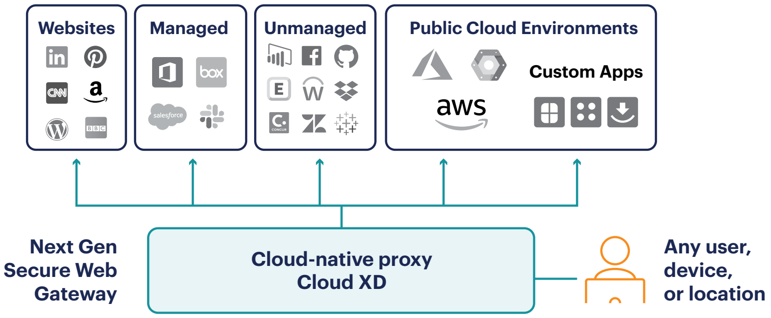
> Companies use an average of 2,415 cloud apps where **98%** are unmanaged and **89%** of users are in the cloud.

Changing landscape for web security

Companies online today use an average of 2,415 cloud apps with 89% of their users active in the cloud[1]. Over 98% of these apps are unmanaged, and whereas traditional API protection is limited to just managed apps, the Netskope Next Gen SWG decodes thousands of cloud apps inline. Cloud-enabled threats span all kill chain stages and represent 65% of malware downloads in 2022[2], mainly from cloud storage apps. SaaS has become the leading target of attacks using trusted domains and valid certificates to evade legacy defenses which are often aided by allow listing to make matters worse.

Cloud adoption also brings boundary crossings that legacy web defenses miss due to either a lack of visibility or coarse-grained allow/block controls with no understanding of context. Data can flow between company and personal instances of cloud apps, between managed and unmanaged cloud apps, and between low-risk and high-risk cloud apps not desired for use. Beyond instance awareness, is a need to understand activity and its anomalies, plus the content itself and the overall context. Next Gen SWG is at the core of security service edge (SSE) architecture, providing data context and granular policy controls for cloud and web.

[1] 2020 Netskope Cloud and Threat Report
[2] 2022 Netskope Cloud and Threat Report


Websites
Managed
Unmanaged
Public Cloud Environments
aws
Custom Apps
Next Gen Secure Web Gateway
Cloud-native proxy Cloud XD
Any user, device, or location

Next Gen SWGs secure web and cloud

- Website and URL access
- Managed and custom cloud apps
- 1000s of unmanaged cloud apps
- Public cloud environments
- Managed devices and BYOD
- Data context for policies
- Metadata to drive AI/ML

Granular policy controls with Cloud XD

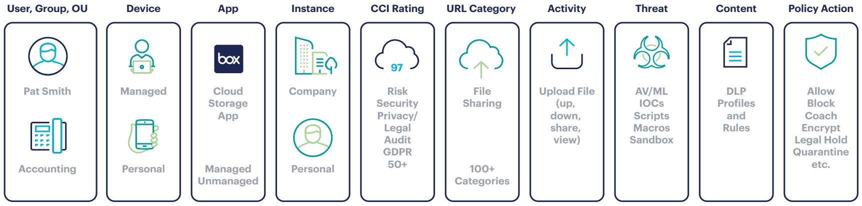
Dynamic websites today use the same underlying language as cloud apps and services. Being able to decode this language is a critical capability for next generation SWG solutions—for visibility of both cloud-enabled threats and sensitive data movement in the cloud. Data flowing in unmanaged apps drives the adoption of cloud-based SWG deployments which are able to secure users in any location on any device. This in turn drives the convergence of SWG, Cloud/SaaS inline, and DLP capabilities to deliver advanced threat and data protection for cloud and web traffic.

Coarse-grained "allow" or "block" policies of legacy web defenses are being replaced with an understanding of content and context for user, app, instance, risk rating, data, and activity in granular policy controls. An activity in a company instance of an app for confidential data may make sense, while the same activity within a personal instance could be data leakage or theft by a soon-to-depart employee.

Defining the next generation of SWG

Trying to solve security challenges with legacy defenses leaves many gaps. While a legacy SWG focused on web traffic paired with a CASB using API-protection of managed cloud apps sounds complete, this solution set misses the thousands of unmanaged cloud apps freely adopted by business units and users as part of their digital transformation. Adding allow/block controls for these cloud apps with a legacy SWG, or using a next generation firewall (NGFW), and cloud apps are simply allowed—missing the data flows, cloud threats, and context. Even using cloud app risk ratings to block high-risk apps, and coach users to safer alternatives still requires you to simply 'allow' some cloud apps, and activity, content and context remains lost. The truth is, legacy SWGs, NGFWs and even endpoint defenses are losing visibility because of cloud adoption and mobility, and they are no longer as effective.

There are many reasons why data and context are at the core of next gen SWGs, and why they are also a core principle of SSE architecture. Cloud DLP is the future as more users and data are outside data centers than within them today. Users access the web, managed apps, unmanaged apps, public clouds, and cloud-based public apps each working day. These five destinations all have data flows that inline cloud DLP rules and policies can protect. Threats have also become cloud-enabled across all kill chain stages and techniques like cloud phishing are compromising access and evading legacy defenses including endpoint protection. Next Gen SWG goes beyond legacy web logs, providing rich metadata to drive machine learning (ML)-based anomaly detection for threats and behaviors for cloud and web traffic.



Pat from accounting - on desktop - using personal Box instance - uploading files - DLP check - coach if PCI, PII, etc.
Pat from accounting - on desktop - using agency Box instance - uploading files - check for malware/threats
Pat from accounting - on mobile - using agency Box instance - downloading files - view-only mode
Pat from accounting - on desktop - browsing web gambling site - block site - coach user with AUP alert

Cloud XD enables rich policy context

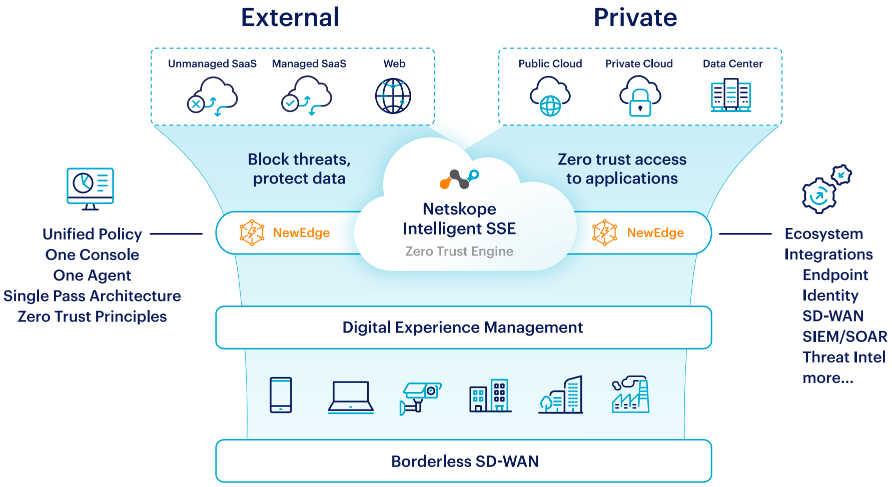
- User, group, and OU
- Managed or personal device
- URL, app, category, and risk rating
- Company or personal instance
- Activity and content for context
- Advanced threat protection
- Advanced DLP rules and policies
- Insider threat and behavior anomalies

Granular controls, metadata, and behavior anomaly detection

In a perfect world prevention would solve everything, however, the reality is security teams need to detect, investigate, and respond, plus apply new threat intelligence retrospectively. This requires the rich metadata for web and cloud traffic inclusive of app, instance, data, and activity provided by next gen SWGs. The metadata also drives ML models to detect advanced threats and user behavior anomalies including insider threats and account compromise. Allow/block no longer works, the answer is to 'allow' with granular controls and collect rich metadata to develop baselines for ML-based anomaly detection, plus enable investigation and response. Next Gen SWGs have the visibility across web and cloud traffic for data and context that is required and not possible with legacy SWGs.

Flexibility to build out your SASE architecture

Change takes time, and a solid architectural plan starts at the core. The Netskope Next Gen SWG provides a cloud-native core with expandable microservices to adopt more security capabilities as your security transformation progresses. Combining Netskope Private Access with Next Gen SWG provides a complete solution for the five destinations noted earlier, plus zero trust network access (ZTNA) for secure access to private apps in data centers and public cloud. Threat protection options include standard, advanced, and behavior analytics; while data loss prevention (DLP) options include standard and advanced options. These common platform defenses and policies can also be applied to CASB API-based inspection of managed cloud apps and cloud security posture management (CSPM) for public cloud environments—all from one console.



Netskope provides a cloud-native platform of microservices covering multiple capabilities within your SSE architecture and providing rich data context and granular policy controls.

NETSKOPE NEXT GEN SWG PACKAGES	STANDARD	PROFESSIONAL	ENTERPRISE
Cloud Security Platform			
NewEdge Netskope NewEdge is our global security network that enables our security cloud to deliver real- time, cloud-native security without the traditional performance vs security trade-off (at no extra cost)	Y	Y	Y
Traffic Steering We use a lightweight client to support a variety of out-of-band and inline traffic steering options, including forward and reverse proxy, API, steering client, log-based discovery, GRE, and/or IPsec tunnel support from on-premises locations	Y	Y	Y
Authentication Single Sign-On (SSO)/ Multi-Factor Authentication (MFA) / Identity and Access Management (IAM), SAML, AD, and LDAP	Y	Y	Y
Regular Cloud Security Updates Benefit from real-time updates of the Netskope Threat Protection engine from Netskope Threat Intelligence and third-party sources from over 40 high-quality partnerships (Cloud sharing)	Y	Y	Y
Standard Reporting Real-time reporting with up to 90 days of data across 40 attributes, with the ability to schedule ad- hoc reports	Y	Y	Y
Advanced Analytics Business intelligence and big data analytics provides organizations with 360° views of their cloud risk posture, covering web, applications, users & data and rich explore tools for over 500 attributes of metadata of web and cloud activity	Add-on	Y (Base)	Y (Base)
Cloud Exchange (CE) Cloud Exchange provides four modules to share threat intel and risk scores, automate workflows, and export logs. Cloud Exchange is also available as a managed service.	Y	Y	Y
SSL/TLS Inspection Real-time end-to-end SSL decryption with native support for TLS 1.3, with little impact on performance or security available at all locations within NewEdge	Y	Y	Y
JSON/API Analysis Real-time inspection of the language that SaaS applications speak		Y	Y
Cloud Security Services			
URL and Content Filtering Granular policy enforcement across 130+ categories, languages for 190+ countries, custom categories, translation services, safe search, silent ad blocking, dynamic ratings for unrated web pages, site look-up tool, reclassification service, and traffic inspection by category.	Y	Y	Y
File Type Control Ability to apply control to specific file type and size for a given user, location, and/or destination within policy		Y	Y
Bandwidth Optimization Traffic steering through NewEdge gains speed due to peering relationships with Microsoft, Amazon, and Google at all locations (+350 peering relationships)	Y	Y	Y
SaaS Insight Visibility into the SaaS applications being used, including the various activities and risk ratings of those applications through Netskope's Cloud Confidence Index (excluding policy control)		Y	Y

Cloud Security Services (con't)			
Cloud Confidence Index (CCI) Risk ratings for cloud apps and services, database includes over 57,000+ entries, coach users to safer alternatives with policy controls	**Y**	**Y**	**Y**
Cloud XD Real-time inline cloud security for managed and unmanaged SaaS applications (+50% of traffic), covering browsers, desktop apps, mobile apps, and sync clients		**Y**	**Y**
Instance Awareness Detection of data movement, insiders, and acceptable use policy based on corporate vs 3rd Party vs Personal instances of a SaaS/IaaS		**Y**	**Y**
Transaction Events Near real-time streaming of web proxy transaction events to cloud storage, SIEM, or XDR for detailed investigations	**Add-on**	**Add-on**	**Add-on**
Cloud Firewall Network security on all IP addresses, ports, and protocol rules (5-tuple)	**Add-on**	**Add-on**	**Add-on**
Threat Protection			
Inline Antimalware Signature-based detection, ML-based PE file analysis, and full file inspection in transit	**Y**	**Y**	**Y**
Web Intrusion Prevention System (IPS) Stop known exploits from websites towards endpoints and users	**Y**	**Y**	**Y**
Cloud-Based Threat Protection Use of instance awareness to identify non-sanctioned threats of corporate cloud applications to identify	**Y**	**Y**	**Y**
Advanced Heuristic Analysis Static analysis without execution of 3,000+ file types for threat indicators for signature-less malware detection	**Add-on**	**Add-on**	**Y**
Dynamic Sandbox Analysis Standard and Professional packages sandbox all AV/ML detections, Enterprise package sandboxes 30+ file types	**Y**	**Y**	**Y**
Remote Browser Isolation Remove the risk of active web-based threats and prevent data loss	**Add-on**	**Add-on**	**Add-on**
User and Entity Behaviour Analytics (UEBA) 9 sequential anomaly rules to detect cloud app bulk uploads, downloads, deletes, plus proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between the company and personal instances		**Y**	**Y**
UEBA User Confidence Index Custom sequential anomaly rules, user confidence scoring, event correlation timelines, and policy actions based on user score (User Confidence Index (UCI))		**Add-on**	**Y**
UEBA Machine Learning (ML) Models Use of advanced machine learning anomaly detection using 67 detectors and 44 ML-models for insider threats, compromised accounts, and data exfiltration		**Add-on**	**Y**

Data Protection			
Cloud Application Visibility Gain insight into all the cloud services and web applications that users are using	Y	Y	Y
Cloud Application Control Gain policy controls for web-based applications and cloud services		Y	Y
Data Loss Prevention (DLP) Analysis of in-motion data against DLP policies for alert and action, enhanced by 40+ regulatory compliance templates, 3,000+ data identifiers for 1,500+ file types, plus custom regex, patterns, dictionaries, and Artificial Intelligence (AI)/ Machine Learning (ML) for two standard document classifiers (e.g., resumes, source code)		Y	Y
Exact Data Matching File fingerprinting with the degree of similarity, exact data matching, and API mode Optical Character Recognition (OCR)		Add-on	Y
Artificial Intelligence (AI) and Machine Learning (ML) AI/ML classification for patent and M&A documents, tax forms, source code, plus images including desktop screenshots, passports, IDs, etc. (27 ML classifiers and growing)		Add-on	Y
Out-of-Band Cloud Access Security Broker (CASB) API-enabled security for managed SaaS applications to monitor and control usage and protect data	Add-on	Add-on	Add-on
Out-of-Band IaaS Storage Scan API-based security for Public Cloud (IaaS) Storage to scan and detect data loss and malware	Add-on	Add-on	Add-on
Cloud Security Posture Management (CSPM) Continuous security assessment (CSA) of AWS, Azure, and GCP via API to identify misconfigurations and assure compliance against industry best practices and regulatory standards	Add-on	Add-on	Add-on
SaaS Security Posture Management (SSPM) Continuous security assessment (CSA) of SaaS applications via API (M365, Salesforce, GitHub, and more) to identify misconfigurations and assure compliance against industry best practices and regulatory standards	Add-on	Add-on	Add-on

Netskope, a global SASE leader, is redefining cloud, data, and network security to help organizations apply zero trust principles to protect data. Fast and easy to use, the Netskope platform provides optimized access and real-time 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.