netskope

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

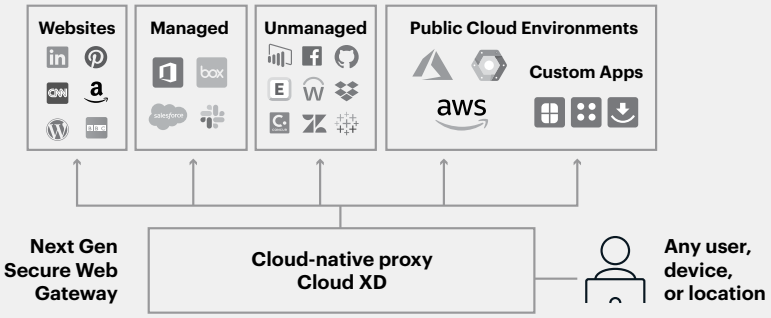
Companies use an average of 2,415 cloud apps where 98% are unmanaged and 89% of users are in the cloud.

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 in over 1,609 apps to represent 44% of threats detected in 2019[2]. SaaS has become the leading target of attacks using trusted domains and valid certificates to evade legacy defenses which are often aided by whitelisting 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 secure access service edge (SASE) architecture, providing data context and granular policy controls for cloud and web.

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



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 SASE
- Metadata to drive AI/ML

GRANULAR POLICY CONTROLS WITH CLOUD XD

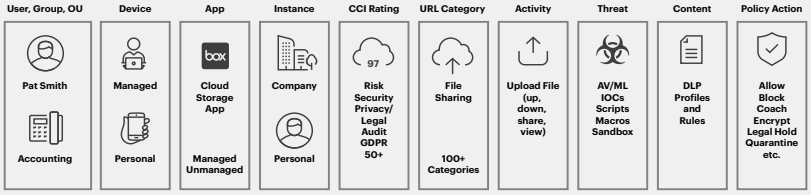
Dynamic websites today use the same underlying language as cloud apps and services. Being able to decode this language is a critical capability for next generation SWG solutions – for visibility of both cloud-enabled threats and sensitive data movement in the cloud. Data flowing in unmanaged apps drives 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 SASE 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 private 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

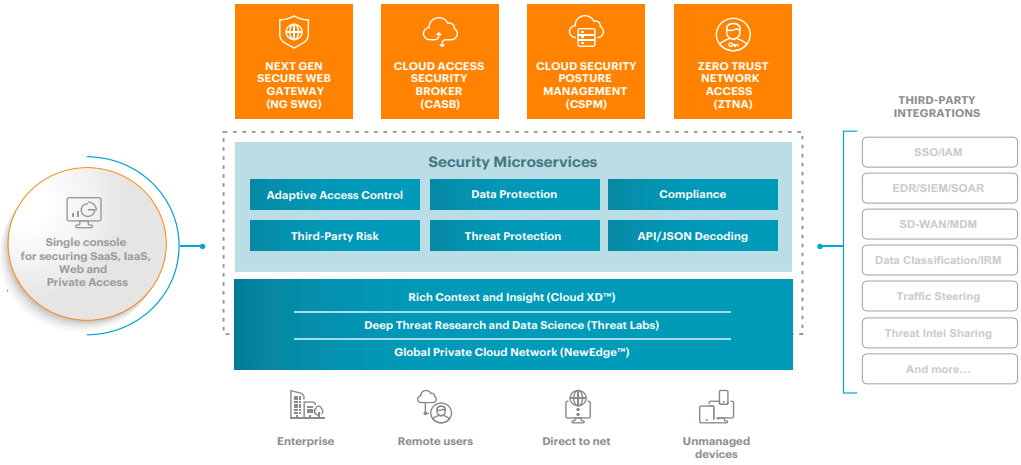
- User, group, and OU
- Managed or personal device
- URL, app, category, and risk rating
- Company or personal instance
- Activity and content for context
- Advanced threat protection
- Advanced DLP rules and policies
- Insider threat and behavior anomalies

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 SASE architecture and providing rich data context and granular policy controls.

NETSKOPE NEXT GEN SWG PACKAGES	PROFESSIONAL	ENTERPRISE
CLOUD SECURITY PLATFORM		
NewEdge Global Network – hyperscale, carrier grade private network, global data centers, fast performance with minimal round-trip times, extensively peered with major cloud providers	Y	Y
Traffic Forwarding – client for steering web, cloud, desktop apps, mobile apps, and sync-clients; or GRE and IPsec tunnels for offices	Y	Y
Forward/Reverse Proxy – supports managed devices with client to cloud and web, plus unmanaged devices without client (i.e. BYOD) to managed cloud apps	Y	Y
Cloud XD – decodes thousands of cloud apps providing content and context including activity and instance awareness for granular policy controls	Y	Y
Authentication – multiple SSO/MFA/IAMs, SAML, AD, and LDAP	Y	Y
TLS Inspection – native support for TLS v1.3, exclusions with policy controls	Y	Y
Analytics & Reporting – based on 90 days of data retention, longer by contract, standard reports and ad hoc queries across web and cloud use. Also, export data and open API integrate with third-party solutions	Y	Y
Cloud Threat Exchange – bi-directional sharing of IOCs to security stack & EPs with ready to use integrations for EPPs, SIEMs, and IR solutions, or add your own	Y	Y
CLOUD SECURITY SERVICES		
Cloud Confidence Index (CCI) – risk ratings for cloud apps and services, database includes over 33,000 entries, coach users to safer alternatives with policy controls	Y	Y
URL Filtering – provides 120+ categories, languages for 200+ countries, custom categories, YouTube 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 or domain	Y	Y
Standard Threat Protection – anti-malware engines, client traffic exploit protection, true file type analysis, 40+ threat intel feeds, bare-metal sandboxing of portable executable (PE) files, and UEBA sequential anomaly rules	Y	Y
Advanced Threat Protection – 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 RBI integration		Y
Behavior Analytics – UEBA machine-learning (ML) models for insider threats, compromised accounts, and data exfiltration, plus custom UEBA sequential anomaly rules, user confidence scoring, event correlation timelines, and policy actions based on user scores		Y
Standard Data Protection (DLP) – data-in-motion analysis for cloud apps and services, plus web traffic, files and forms. Includes 40+ regulatory compliance templates including GDPR, PCI, PHI, PII, source code, etc. Leverages 3,000+ data identifiers for 1,400+ file types, plus custom regex, patterns, and dictionaries. Also now includes AI/ML standard document classifiers (e.g. resumes)	Y	Y
Advanced Data Protection (DLP) – includes file fingerprinting with degree of similarity and exact data matching inline. Also, now 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		Y

Netskope also provides a 'SWG Standard' package for steering web traffic only that includes URL filtering and standard threat protection, plus a 'Web Inline' solution with just URL filtering.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and takes a data-centric approach that empowers security teams with the right balance of protection and speed they need to secure their digital transformation journey. Reimagine your perimeter with Netskope.