netskope

Netskope for Web

Используя функционал защищенного веб-шлюза следующего поколения (NG SWG), платформа Netskope блокирует вредоносные программы, обнаруживает новейшие угрозы, фильтрует веб-трафик по категориям, защищает данные, а также контролирует приложения и облачные сервисы по любому пользователю, площадке или устройству. Платформа Netskope объединяет в себе защищенный веб-шлюз (SWG), брокер безопасного доступа в облако (CASB) и систему предотвращения утечек данных (DLP) – и все это в единой консоли.

Основные моменты

- Средства гранулярного контроля на основе политик для веб-трафика и приложений (включая данные, действия и контекст)
- Обучающие оповещения о рисках, помогающие пользователям самим освоить работу с приложениями и облачными сервисами
- Производительность и масштаб облака – для проверки любого пользователя, устройства или площадки
- Предотвращение утечек данных для управляемых и неуправляемых приложений и веб-трафика
- Защита от вредоносного ПО и расширенных угроз, "песочница" и свыше 40 источников информации об угрозах
- Единая облачная консоль с согласованными средствами контроля на основе политик для функций SWG, CASB и DLP

Новый ландшафт веб-безопасности

Цифровая трансформация, стимулируемая облаками и мобильностью, продолжает набирать обороты, и уже 85% трафика, идущего через веб-шлюзы, приходится на приложения и облачные сервисы, согласно Netskope Cloud Confidence Index[1]. Вдобавок 83% веб-трафика шифруется[2], что создает новые слепые зоны и открывает лазейки для угроз и утечки данных через управляемые и неуправляемые приложения, облачные сервисы и веб-трафик.

Сегодня среднестатистическая компания использует более 1295 приложений и облачных сервисов, причем свыше 95% из них относятся к неуправляемым и не предоставляют никаких прав администратора[3]. Чтобы понимать и защищать контент и контекст, защищенные веб-шлюзы должны выйти за рамки традиционной фильтрации веб-запросов по URL-адресам и начать декодировать идущий через API трафик тысяч приложений и облачных сервисов. Кроме того, для установки системы веб-безопасности в разрыв нужна как производительность облака по запросу для проверки зашифрованного веб-трафика, так и масштаб облака с глобально распределенным доступом к облаку для удаленных офисов и мобильных пользователей.

Поскольку все больше бизнес-операций и данных переносятся в облако, решения для веб-безопасности также должны развиваться, сокращая задержки, уменьшая количество ретрансляций в веб-маршрутах и повышая эффективность. Одного только облачного SWG с безопасным доступом к стандартному интернету уже недостаточно для сегодняшних и завтрашних бизнес-операций. Нужны безопасность и скорость, чтобы обеспечить доступ к облачным приложениям и сервисам с малой задержкой и высокой пропускной способностью.

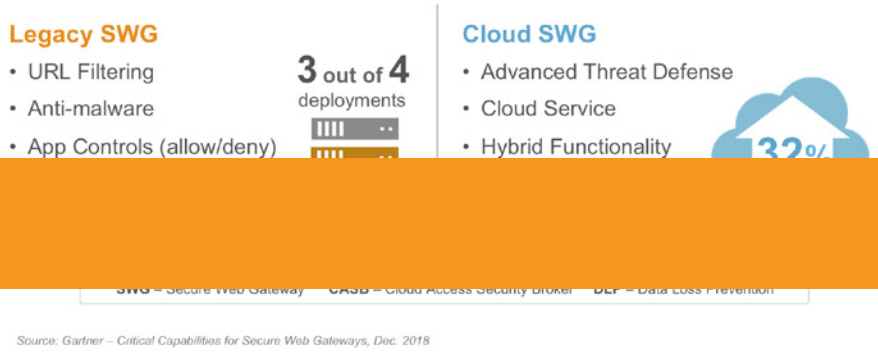
Cloud SWG with on-demand performance and scale

For over a decade, appliance based SWG deployments have dominated the landscape where approximately three out of four still exist today. However, this landscape is quickly changing to cloud SWG deployments qualified by the following Gartner "Critical Capabilities of Secure Web Gateways" report quote.

In the same Gartner report from December 2018, a significant shift surfaced for SWG capabilities, and to no surprise, driven by digital transformation. The chart below illustrates the shift from known legacy SWG features compared to new cloud SWG critical capabilities, highlighted in the report alongside the forecasted 32% compound annual growth rate.

"THE MOST DISRUPTIVE FACTOR IN THIS MARKET IS THE RAPID GROWTH OF THE CLOUD-BASED SWG SERVICES."

Critical Capabilities for Secure Web Gateways, Gartner, December 27, 2018



Source: Gartner – Critical Capabilities for Secure Web Gateways, Dec. 2018

The same Gartner report further notes, *"CASB functionality is rapidly becoming an important feature of SWG solutions"*. Given DLP is a

cloud, and without limits, it makes perfect sense.

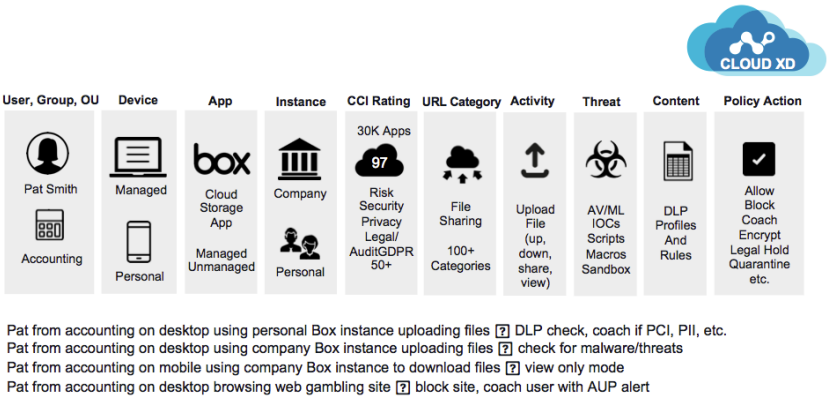
Granular policy controls with Cloud XD

Dynamic web sites today use the same underlying language as apps and cloud services. Being able to decode this language is a critical capability for next generation SWG solutions as data-flows-like-water in the cloud. Given less than 5% of apps are managed with IT administration rights, data flowing in unmanaged apps becomes the elephant-in-the-room for cloud SWG deployments to address with users in any location on any device. This drives the convergence of SWG, CASB, and DLP inline capabilities for complete visibility and granular policy controls into thousands of apps.

Coarse-grained "allow" or "deny" policies are also 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 app and data does not for a personal instance, as it could be data leakage or theft of a soon-to-depart employee.

Sources:
1. Netskope Threat Research Labs, 2019
2. Google HTTPS Encryption Transparency Report, September 2019
3. 2019 Cloud Security Report, Cybersecurity Insiders

Rich policy context of CASB+SWG+DLP



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

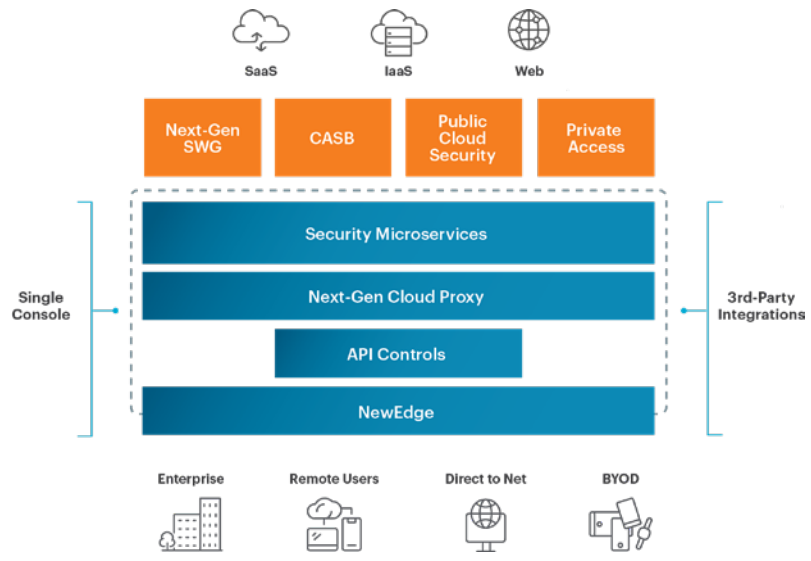
Netskope Cloud XD provides granular visibility and policy controls to web traffic, apps, and cloud services. Cloud XD decodes the language of the cloud and web for an intelligent, consolidated view of cloud and web usage. Unlike legacy web security solutions that overwhelm administrators with logs for every HTTP/S transaction, Cloud XD synthesizes and distills web activity to user site and page visits with the ability to drill down into fine grain details.

One platform and console with unified policy controls

The cloud delivers business acceleration and improved security, while Netskope extends those benefits even more so with one console and unified policy controls for combined inline SWG+CASB+DLP capabilities for the next generation of web security. The Netskope Platform offers several benefits supporting cloud-first organizations, including: a data-centric design to protect data and users everywhere; cloud-smart intelligence to safely enable the cloud and web; plus, an advanced, high-capacity global architecture that delivers fast and scalable security.

Netskope protects some of the largest global companies with industry-leading proxy inline inspection of web traffic, apps, and cloud services without limiting performance or scale, nor increasing latency. If you have concerns about data exposure or loss in unmanaged apps or web sites, plus advanced threats operating in these apps and sites, then Netskope can provide you some peace of mind.

Netskope platform



USE CASE & OVERVIEW	NEXT GENERATION SWG FEATURES INCLUDE:
Web Traffic, App, and Cloud Service Visibility and Control Netskope provides a custom app API proxy to understand thousands of apps for content and context unmatched by legacy SWG solutions. Easy to deploy cloud-based forward or reverse proxy deployments provide inline visibility and granular policy controls to web traffic, apps, and cloud services.	• Discovery via inline analysis or logs with the option to encrypt PII fields for privacy • URL filtering with 100+ categories for over 200 languages covering 99.9% of the active web • Dynamic web page ratings for 70 categories, plus custom categories, app categories, and YouTube categories • CASB managed and unmanaged app inline visibility and granular policy controls for over a thousand apps • Cloud Confidence Index™ (CCI) risk ratings for more than 36,000 apps and cloud services using 50+ CSA attributes • Cloud performance to inspect encrypted traffic
Malware and Advanced Threat Detection Multiple cloud defense layers include anti-malware, pre-execution script analysis and heuristics, sandboxing, and machine learning anomaly detection managed by Netskope Threat Research Labs.	• 40+ threat intelligence feeds, plus custom IOC hash and URL feeds • UEBA to detect access compromise and anomalies • Cloud-based sandboxing, plus 3rd party support for Checkpoint, Juniper, and Palo Alto Networks sandboxing • 90 days of rich metadata (default), longer by contract • Export data via REST API, plus share threat intelligence in open source formats
Data Loss Prevention (DLP) Allow or deny policies do not support business units freely adopting apps where one click can post, share, upload or download data. Understanding content and context is required for policy controls making DLP a critical capability. Netskope delivers with award-winning DLP for web traffic, apps, and cloud services.	• Cloud-based DLP with over 3,000 data identifiers supporting 1,000+ file types, plus 40+ pre-built policy templates • Detect data via multiple methods including custom regex, fingerprinting, exact data match, proximity analysis, pattern and keyword matching, metadata extraction, and OCR (API mode) • DLP actions include the ability to alert, allow, block, provide coaching messages, tombstone files, tokenize or encrypt data (structured and unstructured), legal hold, and quarantine data • Machine learning detection of data moving between company and personal app instances to detect insiders and data leakage
Advanced Web Analytics and Reporting Policy controls are defined and driven by Netskope Cloud XD with an intelligent user-focused view of web, app, and cloud service use for analytics and reporting. Cloud XD synthesizes and distills web activity into user site and page visits on which security teams want to focus.	• Enable SOC teams to quickly investigate alerts understanding content and context of web, app, and cloud service activity • Real-time analytics provide summary dashboards and reports • Drill down into more detailed views by user, site, and page • Flexible, ad-hoc query engine to mine 90 days of rich web and app activity metadata, longer by contract • Export data and open API integrate with 3rd-party solutions
Direct-to-Internet Coverage Netskope enables remote offices and mobile users to go directly to the web wherever they are located. Optionally, Netskope for Private Access for zero-trust network access replaces traditional VPNs connecting users directly to private apps, databases, or resources within public clouds and datacenters.	• IPsec and GRE tunnels for remote offices, plus a lightweight steering client for mobile users • High performance software-defined globally distributed data centers with optimized web routes and hops for low latency, typically less than 20ms latency for any user • Microservices cloud-native architecture designed for on-demand performance and scale of security services • Eliminate cost and performance issues associated with backhauling web traffic, plus web security appliances

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.