

Shift your Web Security to the Cloud, for the Cloud

Why You Need a Next Generation
Secure Web Gateway (SWG)

EXECUTIVE OVERVIEW

As enterprises embrace digital transformation, the adoption of software-as-a-service (SaaS) is robust with nearly 1,295 apps and cloud services on average¹ being used in a given organization. While IT-managed apps like Office 365, Box, and Salesforce are important, they only make up about two to five percent of the cloud services and apps being adopted by the enterprise. Rather, cloud services and apps adopted by lines of business and independent users are fueling a majority of the growth in the cloud.

While unmanaged apps may be important for business productivity, they bring risks in the form of new avenues for malware and advanced threats and exposure of data by accident or intent. Since IT lacks access to these apps, and does not desire administration rights, they lose visibility and control and are forced to deal with the situation using legacy security tactics like blocking at the perimeter or the endpoint. This not only presents technical challenges, but also business challenges, given how the adoption of these unmanaged apps help the business.

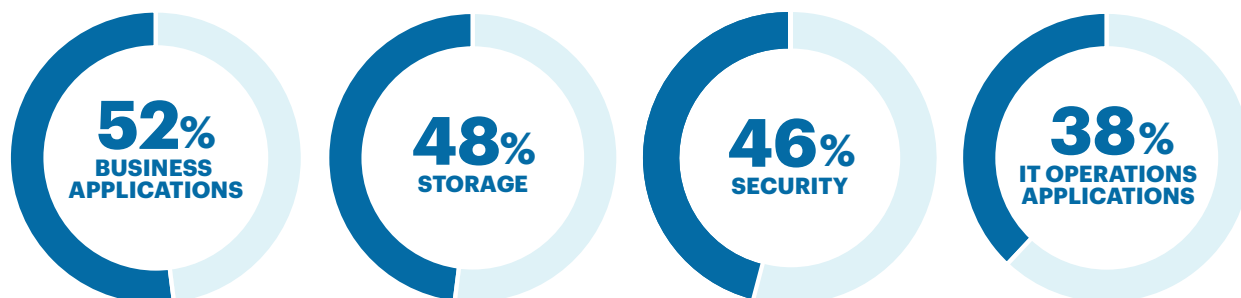
With managed apps controlled by IT making up the smallest portion of enterprise app use, the elephant in the room for security teams is the thousands of unmanaged apps that lack cloud vendor API access and, thus, require inline knowledge of app communications to understand the data-in-motion, activity, and app instance. Because legacy web security products don't understand activity and content within unmanaged apps to apply granular policy controls, the traditional world of a 'red zone' for bad applications and a 'green zone' for good applications has morphed into a 'grey zone'. Enterprises, left with the daunting challenge of protecting larger grey areas, need a single, unified platform for managing all apps, both managed and unmanaged, and web security that enables users to go directly to the web, on any device, wherever they are.

You are likely to approach these challenges with inline controls, most likely with forward or reverse proxy traffic visibility, monitoring and policy controls for apps and web traffic. This will require higher cloud performance to inspect encrypted traffic and an understanding of inline app API communications outside the scope of normal web traffic analysis in legacy web security solutions. This is the domain of an inline Cloud Access Security Broker, with data and threat protection defenses merging with secure web gateway (SWG) capabilities. The net result is an integrated SWG + CASB + Data Loss Prevention (DLP) solution in the cloud, for the cloud. At Netskope, we call this a Next Generation SWG.

¹ Netskope Threat Research Labs, 2019

A LOOK AT TODAY'S WEB

Organizations continue to adopt apps and cloud computing at a rapid pace to benefit from the promise of increased efficiency, improved agility, and better scalability. As organizations become more comfortable in embracing cloud services, more mission-critical and production-grade applications are either moving to the cloud or being replaced by SaaS apps with matching functionality. According to the Cybersecurity Insiders' 2019 Cloud Security Report, 52 percent of organizations are deploying business applications, 48 percent are using the cloud for storage, and 46 percent are moving security processes to the cloud. The message is clear, where the apps and data migrate, security will follow.



As the use of IT-managed cloud services and apps continue to rise, so does the use of unmanaged apps. This is especially disconcerting because they may potentially expose or leak data and can be leveraged for malware delivery or advanced threats. In fact, most organizations don't fully know what apps and cloud services are in use. The average enterprise, for example, has over 1,295 apps and cloud services in their environment. Managed apps, which are often managed by IT with cloud-based APIs for visibility, monitoring, and policy controls, represent between two to five percent of app and cloud service usage in an organization. The remaining 95 to 98 percent are unmanaged apps brought into use by departments and employees without IT consent or administration. Beyond the unmanaged business apps are the upwards of 30,000-plus personal collaboration, communication, productivity, and entertainment apps and cloud services that users can potentially access on a daily basis. Also, if you have recently looked at your web gateway traffic profile, 85% of web traffic on average is now app and cloud service related².

Because unmanaged apps and direct-to-cloud services lack APIs for visibility and monitoring, they raise the stakes for IT teams tasked with assessing risk, security, privacy, compliance, and other factors to determine their safe use. Clearly, inline web security controls that understand and provide visibility of user, app, instance, data, and activity are needed to reduce risk, protect data, and prevent and detect threats.

State of web threats

As more business applications and workloads move to the cloud, security teams are increasingly challenged in securing their cloud data, systems, and services. To begin with, encrypted web traffic is reaching a new threshold. In December 2019, Google notes in its HTTPS Encryption Transparency Report that 84 percent of traffic is HTTPS loaded into Chrome on Windows, up from 74 percent the prior year.

Web threats and attacks are also on the rise. As reported in the 2019 Symantec Internet Threat Report, one in ten URLs is malicious, up from one in sixteen. Endpoint attacks are up 56 percent, year over year. One in 412 emails is malicious, and malicious emails include scripts 48 percent and executables 26 percent of

² Netskope Threat Research Labs, 2019

the time. Forty-eight percent of malicious email attachments are Office files, up from five percent in 2017.

Attack trends also continue to paint a bleak picture. Sixty-five percent of targeted attacks used spear phishing with script-enabled attachments leading to web requests as the primary infection vector. Supply chain attacks are up 78 percent year over year and S3 bucket misconfigurations continue to expose millions of records.

84 PERCENT OF TRAFFIC IS HTTPS LOADED INTO CHROME ON WINDOWS, UP FROM 74 PERCENT THE PRIOR YEAR.

December 2019 Google
Transparency Report

WEB SECURITY IN THE DIGITAL AGE

People now expect to be able to work at any time, from any place, and on any device. These changes are dramatically altering the network and security infrastructure in many organizations. Rather than staying with a legacy, hub-and-spoke network architecture, with offices interconnected over costly, dedicated links and remote users accessing centralized resources over VPNs, more organizations are moving to a direct-to-web and direct-to-cloud model.

Furthermore, the underlying nature of the web is also changing, with static websites giving way to personalized web pages dynamically generated using the same underlying language that powers today's rapidly growing apps and cloud services. Accessing a single page could result in more than 100 HTTPS requests, including private API calls, ad networks, page analytics trackers, content delivery networks (CDNs), and third-party plug-ins.

Legacy security solutions fall short

Legacy web security solutions, typically delivered as physical appliances, are limited by fixed compute, storage, and I/O resources. This has meant that security teams needed to carefully size their web security solutions, monitor their performance, and periodically refresh their infrastructure to avoid performance problems. It is likely that when initially deployed, encrypted web traffic was below 30 to 40 percent but has now doubled during the five to seven-year life span of these web security appliances.

Legacy security solutions are also unable to understand the dynamic and contextual language of apps, cloud services, and personalized web sites. Additionally, they are often blind to encrypted, remote, and mobile traffic, putting organizations at risk for blended and multi-channel threats that straddle web sites, apps, and cloud storage. Apps also make it easy for users to share and access data, which can lead to data loss or introduce new threats. The legacy web security model of allow or deny makes the job to protect and secure critical information coarse grained—either too restrictive or too wide open.

Cloud drives focus on identity, access, data, and activity

Traditional web security HTTP and HTTPS proxies cannot decode the API communications used by cloud apps to understand the content and context. This capability belongs to the inline CASB, with its understanding of thousands of apps and cloud services. This is the main driving factor for the convergence of SWG and CASB capabilities.

The digital transformation to apps, cloud, and mobility is defining a new perimeter which must use identity, access, app, instance, data, and activity to define web security policy controls. These are key policy variables an inline CASB adds to web security. Users may also have company and personal instances of the same app, and this is where mistakes can happen that expose data or introduce threats. This is a new era for web security, where thousands of unmanaged web apps require more than allow or deny controls.

CLOUD VS. HYBRID VS. ON-PREMISES FOR WEB SECURITY

A multi-cloud, hybrid environment is the reality almost everyone faces; however, on-premises web security comes with cautions as it struggles to address today's app, cloud service, and web use. Security portfolios from years of acquisition have created too many administration panels and dashboards, separate policy controls, and excessive log volumes and alerts. Appliances often lack capacity to inspect encrypted traffic, or host multiple defenses, and are often last in line for new features and updates. Legacy web security defenses with simple allow and deny policy options fail to enable business units with the security required for managed and unmanaged apps. Lastly, some legacy SWG defenses often come with cryptic command line controls and complicated policy control scripts—often hundreds of lines long per customer—requiring rare administration skills that are hard for IT staff to implement and maintain.

Bringing the complexity of on-premises web security forward into a hybrid or cloud SWG strategy is questionable and likely unfeasible. While 74 percent of existing SWG deployments are appliances today, the compound annual growth rate (CAGR) for cloud-based SWG defenses is 32 percent compared to five percent for on-premise appliances³ and within five years they will surpass appliance SWG deployments.

Cloud-based web security from the cloud and for the cloud best addresses the requirements for web security going forward. A Next Gen SWG providing full integration of SWG, CASB and DLP capabilities improves the situation with cloud performance, scale, and unified policy controls for content and context. Cloud versus hybrid versus on-premises for web security favors cloud due to cloud performance for defenses, encryption, and machine learning analytics, and cloud scale for remote offices and for any user, location, and device. A cloud first approach for inline web security converging SWG + CASB + DLP into a Next Gen SWG is the reality today and the future.

CHANGING CRITICAL CAPABILITIES

For over a decade, SWG critical capabilities have remained mostly stable in analyst reports until December 2018, when sweeping changes surfaced impacting use cases. Even up through 2017 a secure web gateway solution was defined with the following critical capabilities:

- URL filtering
- Anti-malware
- App controls (allow or deny)
- User identity and authentication
- Role-based administration controls (RBAC)
- Reporting

In late 2018, the Gartner Critical Capabilities for Secure Web Gateways, December 27, 2018 report dramatically updated SWGs to the following critical capabilities:

- Advanced threat defense
- Cloud service
- Hybrid functionality
- CASB
- DLP

³ Gartner Magic Quadrant for Secure Web Gateways, November 26, 2018

- Advanced features
 - Remote browser isolation (RBI)
 - SD-WAN integration
 - Cloud-based firewall.

Most important are cloud services for:

- On-demand performance for encrypted traffic inspection and defenses
- Scale for remote offices and mobile users with direct to web access
- CASB inline visibility for thousands of apps
- DLP to prevent data exposure, theft or loss.

The advanced features highlight the transfer of the on-premise security stack infrastructure to the cloud, and position innovations like selectively using remote browser isolation to interpret and pixelate web requests to users, thus, isolating their devices from active web content, scripts, and hidden threats.

The headwinds of cloud adoption and cloud security defenses are occurring faster than expected, even for legacy web security vendors expecting regular renewals on SWG appliances. The 'inline' discussion for web security is converging SWG+CASB+DLP into cloud security platforms with one console and unified policies to reduce complexity and provide increased granularity for content and context in policy controls.

The shift has impacted use cases to understand user identity, device, app, instance, risk level, data, and activity for web security policy controls.

USE CASES FOR NEXT GEN SWGs

As networks become more and more decentralized and more users connect directly to the web and apps from any location and any device, the future for SWG is an integration partnership with CASB in a cloud first world for inline app visibility. Primary use cases for Next Gen SWGs with inline critical capabilities include:

- Monitoring and visibility of users, apps, and web access
- Malware detection and advanced threat defense
- Protecting remote offices and mobile workers.

Monitoring and Visibility of Users, Apps and Web Access

In almost all cases, even when enterprises feel they have a good understanding of the use of managed apps and cloud services via cloud API access for CASB solutions, use of unmanaged apps and cloud services is taking place. When users are not using the few numbers of managed apps, they are going directly to the internet to access unmanaged apps and cloud services. If they are within encrypted tunnels that are not being inspected, or the apps' inline API traffic is not being decoded, then they are completely bypassing inline web security defenses.

Using a CASB with only API-based access to managed apps is short sighted given that more than 95 to 98 percent of apps are not provisioned by IT, and IT does not desire administration rights. To understand the security, privacy, and compliance risks presented by the use of apps and cloud services, enterprises need visibility into:

- User or group
- Device type
- App and risk rating
- App instance or account
- Activity
- Type of data

Performing continuous monitoring of cloud usage is vital because new cloud services and apps are continually being introduced and business units will adopt them. Web security must be redefined by visibility and control, an ability to decode inline the API communications used by apps, often within encrypted tunnels. While HTTP and HTTPS proxies are popular in web gateways for traditional web traffic, the advancement of a proxy that understands app APIs and has the ability to quickly learn new app and cloud service communications and adjust to unannounced changes from app vendors is a requirement.

Malware Detection and Advanced Threat Defense

Separate solutions for web and cloud security can result in missed threats that use both the cloud and the web to cause damage. A blended attack may deliver a malicious script from a website and then use a cloud storage app for payload delivery within encrypted communications. Getting visibility into both the script execution and payload movement helps you get a complete picture of the threat. A combined defense needs to understand web traffic and cloud app communications within SSL/TLS encrypted traffic to prevent or detect this threat.

Threat protection is a core capability that must be evaluated when selecting a web security solution. Multiple defense layers including anti-malware, exploit prevention, pre-execution script analysis and heuristics, behavioral analysis, and cloud sandboxing alongside multiple threat intelligence feeds must be utilized. Enterprises should evaluate solutions on the ability to analyze app, cloud service, and web transactions in real time, decode rich contextual details about usage, and identify and control anomalous behavior and threats for user activity.

Protecting Remote Offices and Mobile Workers

In contrast to past hub-and-spoke network architectures where offices were interconnected over costly, dedicated links and remote users accessed centralized resources over VPN, organizations today want to enable remote offices and mobile users to go directly to the web, wherever they are.

Cloud scale and performance is required to protect remote offices and mobile workers, plus inspect SSL/TLS encrypted traffic, apply multiple defenses for prevention and detection, and protect data with DLP rules and policies.

A cloud-based security stack both protects remote and mobile workers and supports managed devices for mobile workers accessing web content and apps. The exception remains for unmanaged devices accessing unmanaged apps and the web at large, while all other deployments can be addressed via inline forward and reverse proxy, API-based CASB, or using an endpoint steering client. For example, using SSO/IAM integration with a reverse proxy provides security for managed apps, and DLP for the unmanaged devices accessing them, without needing an agent or steering client.

NETSKOPE NEXT GENERATION SWG

Built on the Netskope Security Cloud Platform, which consistently secures SaaS, infrastructure-as-a-service (IaaS), and web access, the Netskope NG SWG is a cloud-based web security solution that prevents malware, detects advanced threats, filters by category, protects data, and controls app use for any user, location, device. As a key part of the Netskope Platform, it unifies inline SWG, CASB, and DLP into common policy controls with custom reporting and rich metadata for ad-hoc queries.

Netskope was architected from the beginning to understand the context of today's cloud and web usage at the deepest level and provide real-time, granular visibility and control of thousands of apps and cloud services led by lines of business and users. This enables you to optionally block the use of high-risk apps and cloud services, but more importantly, safely enable the majority of apps that the business relies on with an understanding of content and context.







Netskope's cloud native architecture boosts performance and is built to scale, enabling you to understand risky activities, protect sensitive data, stop online threats, and respond to incidents in a way that fits how people actually work. By combining the perspective of an SWG solution set with the power of inline CASB functionality with DLP, the Netskope NG SWG delivers:

- **Web threat prevention and detection** provides multiple defenses for static and behavioral malware and web threat analysis including pre-execution analysis and heuristics, sandboxing, machine learning anomaly detection, and over 40 threat intelligence feeds including custom input of IOC hashes and URLs. Netskope provides three options of web threat protection and supports its own internal threat research team.
- **URL filtering and dynamic ratings** includes over 100 categories, supporting over 200 languages. Includes machine analysis for unrated web content in 70 categories, plus support for silent ad blocking, include/exclude URL lists, and custom categories. Also includes a site look-up tool and URL reclassification service.
- **Phishing protection** examines webmail content for web threats and URL links for malicious content or downloads. Includes behavioral machine analysis to detect file-less threats using PowerShell scripts or macros, often within documents and Microsoft Office files.
- **Data loss prevention** for data-in-motion for managed apps using managed or unmanaged devices, or unmanaged apps using managed devices. Over 3,000 data identifiers supporting over 1,000 file types with standard and advanced DLP features including exact data match, data fingerprinting, OCR (API-mode), and proximity analysis.
- **Encrypted traffic inspection** elastic cloud performance to securely inspect server-side native TLS v1.3 to v1.1 encrypted web traffic without deprecation for web threats, data protection, and application of web policy controls.
- **App risk ratings** for over 33,000 apps including over 50 attributes defined by the Cloud Security Alliance for security, privacy, risk, compliance including GDPR, financial, legal, and audit profiles.
- **App controls** for thousands of managed and unmanaged apps, browser native, and sync clients across managed and unmanaged devices on any network or in any location. Rich policy controls around content and context are driven by Cloud XD visibility including user, device, app, instance, risk rating, category, activity, content, and action.
- **Web isolation** ability to direct web traffic to remote browser isolation solutions based on policy controls for user, device, network location, action, URL category, or unknown, etc.
- **Solution integration** supports ICAP, plus a REST API for data access for integrations with DLP, EDR, SIEM, SOAR, or desired security solutions. Ninety days of rich metadata is available for detection, investigations, threat hunting, and ad-hoc queries.

Rich policy context of the Netskope NG SWG

USER, GROUP, OU	DEVICE	APP	INSTANCE	CCI RATING
 PAT SMITH  ACCOUNTING	 MANAGED  PERSONAL	 CLOUD STORAGE APP MANAGED AND UNMANAGED	 COMPANY  PERSONAL	+33K APPS  RISK SECURITY PRIVACY LEGAL/AUDIT GDPR 50+
URL CATEGORY	ACTIVITY	THREAT	CONTENT	POLICY ACTION
 FILE SHARING 100+ CATEGORIES	 UPLOAD FILE (UP, DOWN, SHARE, VIEW)	 AV/ML IOCS SCRIPTS MACROSEX SANDBOX	 DLP PROFILES AND RULES	 ALLOW, BLOCK, COACH, ENCRYPT, LEGAL HOLD, QUARANTINE, ETC.

1

	+		+		+		+		+	
PAT	FROM	ACCOUNTING	ON	DESKTOP	USING	BOX		PERSONAL		UPLOADING







= DLP CHECK, COACH IF PCI, PII, ETC.

2

	+		+		+		+		+	
PAT	FROM	ACCOUNTING	ON	DESKTOP	USING	BOX		COMPANY		UPLOADING






= CHECK FOR MALWARE/THREATS

3

	+		+		+		+		+	
PAT	FROM	ACCOUNTING	ON	MOBILE	USING	BOX		COMPANY		DOWNLOADING

= VIEW ONLY MODE

4

	+		+		+		+	
PAT	FROM	ACCOUNTING	ON	DESKTOP	BROWSING	WEB		GAMBLING SITE

= BLOCK SITE, COACH USER WITH AUP ALERT

THE NETSKOPE PLATFORM

The Netskope Platform was designed in the cloud, for the cloud, with high performance and scalable micro services on-demand. Today, multiple security solutions are provided from high-capacity and low-latency global connection points that remove unnecessary hops and traffic routing for an optimized user experience unmatched by competitors.

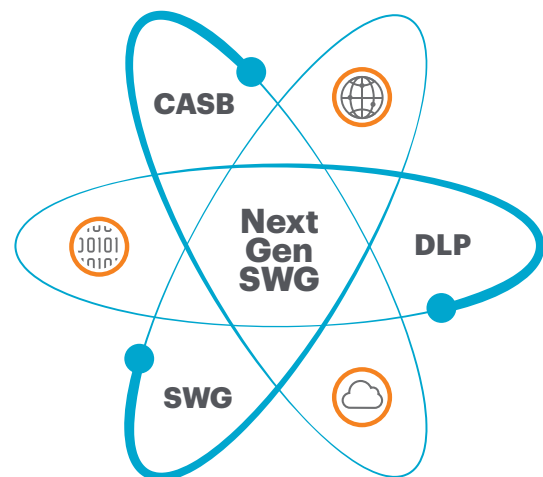
The Netskope Platform includes the following solutions:

- CASB API-based protection for managed apps and cloud services (e.g. Office 365, Salesforce, Box, Dropbox), providing cloud policy controls with threat protection and DLP for data-at-rest.
- CASB Inline Protection for managed apps (data-in-motion) and thousands of unmanaged apps. Providing granular policy controls with threat protection and DLP by being inline with cloud apps and decoding their API communications.
- SWG with granular policy controls for managing web traffic that include threat protection, URL filtering, and DLP policies.
- Cloud security posture management (CSPM) providing continuous assessment of IaaS cloud development platforms including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).
- Zero Trust Network Access (ZTNA) providing private access from users to specific apps, data resources, or cloud environments to replace legacy remote access VPN solutions.
- A unified console for policy definition across SaaS, IaaS and web with cloud performance and scale.

SUMMARY

Enterprises today are faced with the daunting challenge of seamlessly securing critical data traversing the network to access SaaS apps, IaaS, and the web from any endpoint. Although web security vendors have attempted to address this problem by packaging and moving their legacy solutions to the cloud, this approach does not address security challenges created by the use of SaaS and IaaS, or the way the dynamic web is built today. To realize this new network vision, a fundamentally different approach to security is needed—one that allows organizations to address these changes head-on with a unified cloud and web security platform that is designed for today's cloud-first enterprises. At Netskope we address this new approach with our Next Generation SWG.

Next Generation Secure Web Gateway



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.

To learn more visit, <https://www.netskope.com>.