Solution Brief

Netskope for GitHub

GitHub is a cloud-based software development platform used by more than 73 million developers across 4 million organizations to host and review code and manage projects. Netskope for GitHub reduces cloud risk by enabling organizations to monitor and control user activities while ensuring only authorized personnel can access GitHub repositories.

Key Use Cases

- **Detailed visibility.** Monitor GitHub user activities and access privileges in real-time along with exposure of code repositories.
- **Granular control.** Apply security policies that prevent risky user activities and promote safe usage.
- **Block malware and data exfiltration.** Prevent upload of malicious files and block download of sensitive data including PII, PCI, and PHI.
- **Maintain compliance.** Benchmark security settings against industry best practices and standards.

> “Attackers constantly try common passwords and leaked credentials from other services to gain access to sensitive information stored in cloud apps.”
>
> - Netskope Cloud Threat Report, January 2022

The Challenge

Supply chain attacks are known for the damage they can cause to enterprises and critical infrastructure providers through ransomware campaigns and disruptive attacks. Some attacks are enabled by misconfigured online repositories that allow attackers to exfiltrate, manipulate, and replace proprietary source code or weaponize open source components. As software development is now done globally, programmers and DevOps teams routinely use cloud and web-based platforms to coordinate and orchestrate projects from major releases to patch rollouts. GitHub currently hosts more than 200 million code repositories that developers depend on to be secure yet accessible to authorized personnel. Although GitHub provides extensive security controls, enterprises are still responsible for managing security settings and content for their repositories. This can be a challenge for security teams tasked with managing hundreds or even thousands of repositories.

The Solution

Netskope for GitHub

Netskope for GitHub provides real-time visibility and control of user activity, data loss prevention (DLP), and protection against cloud threats and malware. Netskope also provides insight into GitHub audit logs and code repository security settings, with the ability to enforce compliance policies by preventing proprietary code and other sensitive information from being shared with unauthorized third parties. For example, leverage Netskope’s award-winning DLP to detect and prevent a user from uploading PCI or PII data to a GitHub repository.

How Netskope Enables Secure Usage of GitHub

Granular visibility of GitHub usage

Drill down into the details and activities of users accessing GitHub. Understand in real-time the user identities and the types of devices accessing your GitHub environment. Audit the activities performed by your GitHub users including the creation, deletion, editing, uploading, or downloading of content. Perform ad-hoc queries or create reports of relevant access and usage information for compliance.

Granular control of GitHub users

Create granular, contextual policies based on user, activity, device, and more. Limit certain activities to only authorized users, and encourage correct user behaviors through coaching with custom user notifications—all in real-time. Coupled with UEBA, extend policies to leverage DLP and threat detection capabilities to protect your data and your organization.

> Netskope improves security posture and compliance by providing detailed visibility and granular control of GitHub users, repositories, and sensitive data such as source code.

Advanced, enterprise cloud DLP

Netskope lets you detect data violations in transfers to and from GitHub environments—including Shadow IT instances. Govern content uploads and downloads containing sensitive data using pre-built profiles for personally identifiable information (PII), payment card industry data (PCI), protected health information (PHI), source code, profanity, and more. Alternatively, you can custom-build DLP profiles using Netskope's robust set of advanced cloud DLP features such as AI/ML enhanced detection, 3,000+ data identifiers, 1,500+ file types, support for language agnostic double-byte characters, custom regular expressions, pattern matching, OCR, image recognition, proximity analysis, fingerprinting, and exact data match.

Continuous monitoring of code repositories

Part of the Netskope Intelligent Security Service Edge (SSE) platform, Netskope Cloud Access Security Broker (CASB) API and SaaS Security Posture Management (SSPM) capabilities can provide alerts when repository settings or logs indicate any deviation from standards or policies. Netskope SSPM continuously benchmarks GitHub settings against industry best practices to ensure compliance with security standards and regulations. For example, a specific control for GitHub can ensure that there are no inactive users or repositories.

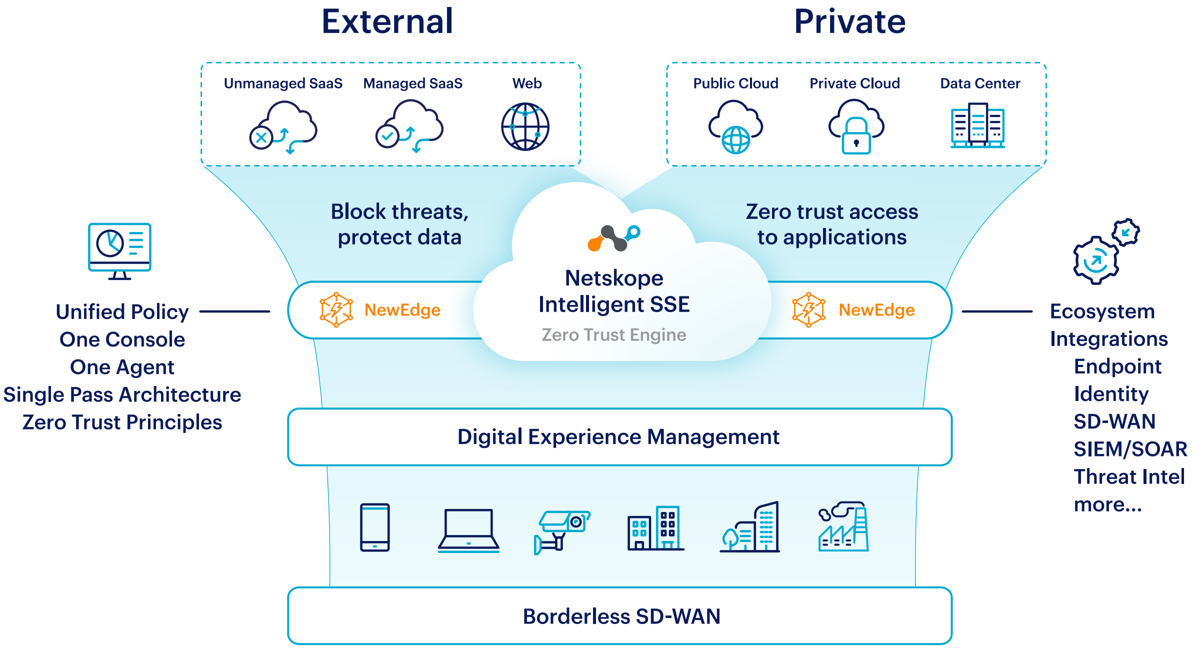
Netskope CASB API allows you to understand and govern who has access to your GitHub data at all times. Additionally, CASB API retrieves detailed audit logs from GitHub in order to provide a clear and detailed picture of activities within your GitHub environment.

Cloud threat and malware protection

Detect and respond to usage anomalies using Netskope's User and Entity Behavior Analytics (UEBA), machine learning and rules-based anomaly detection. See logins from suspicious locations, be alerted to data exfiltration, know when users' credentials have been compromised, and understand privileged user threats. Using Netskope's Threat Protection capabilities, detect and block cloud malware in real-time. Prevent the upload of malicious files into your GitHub environment, and prevent the download of infected files from other GitHub environments.

SUMMARY OF API AND INLINE PROTECTIONS FOR GITHUB	
API Protections	• Near real-time visibility of repository details and status including user membership and public exposure • Retrieval of detailed audit logs from GitHub • Security and compliance alerts when repository settings or logs indicate deviation from standards or policies
Inline Protections	• Real-time visibility and granular policy controls* for users accessing GitHub • Real-time inspection of data transfers between users and GitHub repositories • Detection and remediation of threats and DLP policy violations

* Real-time GitHub activities recognized by Netskope: Create, Delete, Download, Edit, Invite, Login Attempt, Login Failed, Login Successful, Logout, Post, Share, Upload, View.



Netskope for GitHub is part of Netskope Intelligent SSE, providing unrivaled performance, visibility, and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere.

About Netskope for GitHub

Netskope for GitHub includes features from three Netskope products: Netskope CASB API, Netskope CASB Inline (including Netskope Intelligent SSE and Netskope NG SWG), and Netskope SSPM. All products are delivered from the Netskope New Edge Network, fully integrated into a single pass architecture, and managed from a single console.