Harden Your Netskope Controls

Reach

Find and Fix Misconfigurations and Activated Unused Security Capabilities

Netskope Secure Service Edge

Netskope is a cloud-delivered security platform that provides Secure Service Edge (SSE) capabilities to protect how users access the internet, SaaS applications, and private applications. Netskope enforces security policies on web traffic, governs access to cloud applications, and prevents sensitive data from leaving the organization.

The Configuration Challenge

Over time, Netskope configurations change and drift from security baselines. Why? Security teams are overwhelmed and understaffed, yet still tasked with managing extremely large security stacks, with new features released annually. Concurrently, other teams change controls without security visibility. As a result, misconfigurations hide from view and valuable protections are left unused, creating exposures.

Key Capabilities

Block access to websites and web apps that are deemed malicious and enforce acceptable use policies.

Control access to critical business applications based on device risk posture and limit activity if necessary

SSL Inspection policies detect malware, C&C traffic, and malicious downloads within HTTP sessions.

Zero Trust Network Access (ZTNA) to securely connect users to private applications without exposing internal networks to the internet.

Common Misconfigurations

Overly permissive web access policies allow risky web categories and fail to block malicious domains.

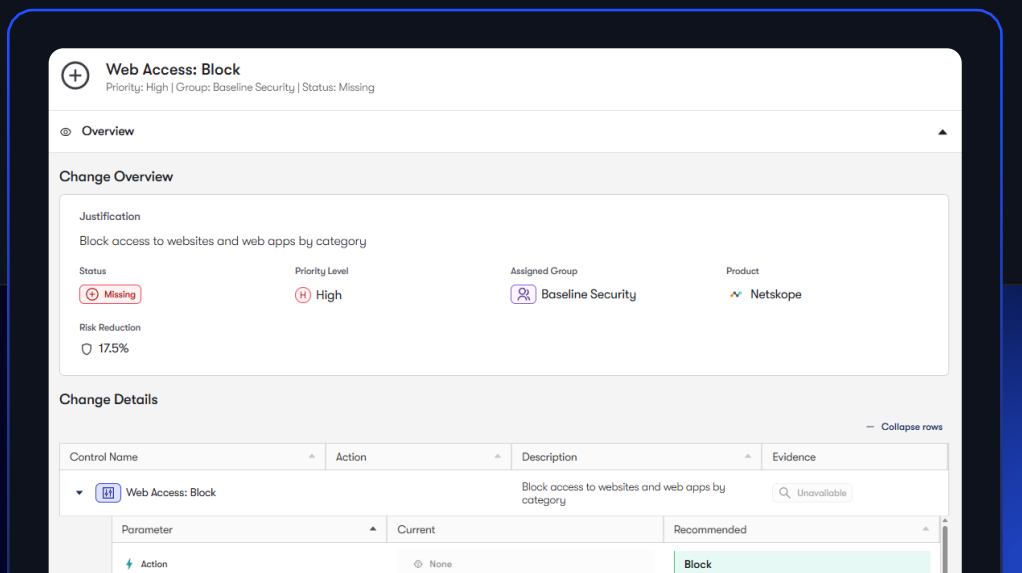
Inconsistently enabled SSL inspection or malware scanning allows threats through encrypted traffic.

Inactive Zero Trust controls for critical business applications leave access ungated.

Unclassified devices block other security controls that depend on device classification.

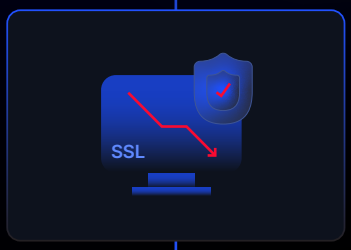
Reach Supercharges Your Netskope Deployment

Reach connects to Netskope and analyzes policy configurations across web access, SaaS governance, and data protection controls. Reach develops a genius-level understanding of how your Netskope tool is being used (and misused), and then automatically identifies and remediates misconfigurations, activates unused capabilities, and validates over time that security posture remains strong.



Secure Web Gateway policy rules and category controls

Reach identifies and remediates overly permissive web access policies, risky category allowances, and policy exceptions that bypass inspection so that organizations can reduce web-based attack surface and prevent access to malicious or high-risk destinations.

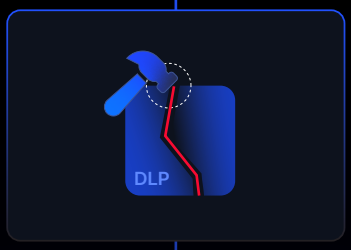


SSL inspection and malware inspection settings

Reach analyzes whether encrypted traffic inspection and malware scanning protections are properly configured and corrects disabled inspection capabilities or policy bypasses so that organizations can detect threats hidden in encrypted web traffic and strengthen overall web security coverage.

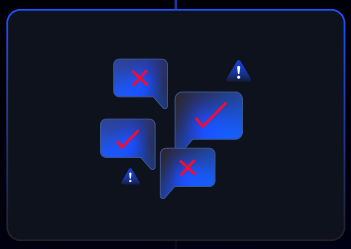
SaaS application governance

Reach identifies and remediates unsanctioned application usage, excessive access permissions, or weak governance policies so that organizations can reduce shadow IT risk and prevent unauthorized SaaS access to corporate data.



Data protection and policy enforcement

Reach identifies policies that are defined but not enforced, incomplete inspection rules, or gaps in data protection enforcement, and then automatically remediates these issues so that organizations can better prevent sensitive data exfiltration across web and cloud applications.



Access control policies and rule conflicts

Reach analyzes policy logic, rule precedence, and configuration structure and identifies conflicting rules, redundant policies, or overly broad access exceptions so that organizations can restore intended policy enforcement and maintain consistent security controls across their Netskope deployment.

Reach + netskope

Together, Reach and Netskope help organizations strengthen protection across web and cloud access by keeping security policies properly configured and continuously aligned to best practices. Customers reduce web and SaaS attack surface, improve data protection, and close gaps caused by risky policies or misconfigurations. The result is greater confidence that Netskope is not just deployed, but actively delivering the protection, coverage, and control it was meant to provide.

Learn More reach.security/connect | Webpage | Demo Video