Netskope Cloud Risk Assessment

An analysis of your organization's cloud app usage and risk

What is the Netskope Cloud Risk Assessment?

Organizations are adopting cloud and SaaS at a rapid pace. Whether you allow or block these apps, chances are your users have found a way to access them. Performing a Netskope Cloud Risk Assessment will help you understand which are in use in your organization. The Assessment will provide you an overview of the apps, how enterprise-ready they are, how risky they are for your organization, and recommendations for mitigating that risk. It can provide answers to the hard questions your organization's leadership is asking, as well serve as a starting point for your cloud strategy.

What is included in the Assessment?

Netskope offers two Assessment types, Standard and Advanced. The table below outlines what you can expect from each.

WHAT'S INCLUDED	STANDARD	ADVANCED
Secure, dedicated Netskope tenant instance	Secure, dedicated tenant, no access	Secure, dedicated tenant, access for 1 month
Discovered apps by category	Top categories only	Summarized for all categories + drill down in tenant
Enterprise-readiness score and risk rating of discovered apps	Top apps only	Summarized for all apps + drill down in tenant
App risk analysis	---	App risk breakdown overall and in key categories
Data movement analysis	Summary of data movement	Detailed summary of data movement, including by users
Sanctioned app analysis	Summary of usage	Usage analysis + enterprise-readiness gaps
Usage and activity analysis[1]	Summary of risky activities	Risky activities (e.g., sharing, downloading, etc.) in key apps
Business concerns analysis	---	Usage identified against top business concerns
Risk analysis mapped to your organization's business concerns	---	Summary + analysis + drill down in tenant
Sensitive data exposure analysis (DLP violations in content at rest)[2]	Summary of DLP violations	Violations by type vs. total files scanned + exposure breakdowns
Sensitive data violation analysis (DLP violations in content en route)[3]	Summary of DLP violations	Violations discovered en route to and from discovered cloud apps
Recommendations	--	Recommendations mapped to business concerns + phased risk mitigation roadmap

[1] Available if Assessment performed in-line or in secure TAP deployment mode
[2] Must perform content discovery against DLP profile(s) as part of Introspection
[3] Available if Assessment performed in-line or in secure TAP deployment mode with DLP profiles enabled

How to Take Advantage of the Assessment

To take advantage of the Assessment, all you need to do is upload your web proxy or firewall logs to a secure, dedicated SOC-1 and SOC-2 Type II-certified Netskope tenant instance. You may also choose to have Netskope perform the Assessment using alternative deployments, including Introspection, secure TAP, or in-line, which will give you additional visibility into DLP violations and granular activity details. Once the analysis is complete, Netskope will present the Assessment to you and your team. If you choose to pursue the Advanced Assessment, you will have access to tenant instance for one month to perform additional analysis.

About Netskope

Netskope™ is the leader in safe cloud enablement. Only the Netskope Active Platform™ gives IT the ability to find, understand, and secure sanctioned and unsanctioned cloud apps. With Netskope, organizations can direct usage, protect sensitive data, and ensure compliance in real-time, on any device, including native apps on mobile devices and whether on-premises or remote, and with the broadest range of deployment options in the market. With Netskope, the business can move fast, with confidence.