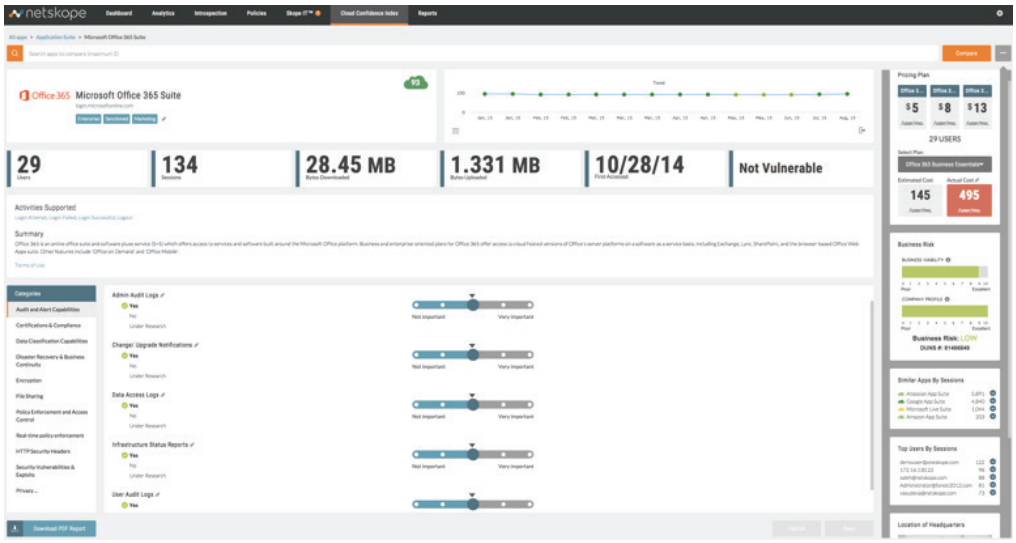
Netskope Cloud Confidence Index™

The Netskope Cloud Confidence Index™ (CCI) assesses a cloud app's enterprise readiness based on objective criteria, and assigns an overall score.



Cloud apps help your users get their jobs done more efficiently. But they're not always safe to use in your organization. How can you ensure an app meets your organization's security and compliance requirements? Does the cloud app offer the right level of data encryption? Does it have a disaster recovery plan in place? Is it subject to any security vulnerabilities or exploits? In short, is it enterprise ready?

Covering thousands of enterprise cloud apps, the Netskope Cloud Confidence Index™ (CCI) assesses an app's enterprise readiness based on objective criteria, and then assigns it an overall score. You can use the CCI to make decisions regarding app usage in your company. For instance, you can use CCI scores to recommend one app over another, or to gain the external validation that you need to discontinue use of an app that isn't up to your standards. Moreover, you can incorporate the CCI into your cloud app policies within the Netskope Active Platform – such as to restrict certain activities within the app or limit device types that are allowed to access the app – in order to declare an app suitable for your organization. Finally, you can take control and adjust the CCI input weightings to match your organization's requirements and criteria.

Enterprise-readiness Score Based on Objective Criteria

The CCI assesses the enterprise readiness of an app based on objective criteria in seven functional areas: inherent app security, auditing and third-party certifications, legal, service-level agreements, security vulnerabilities and exploits, financial viability, and privacy.

Data scientists at Netskope use a combination of publicly available information and observed app capabilities, assign numeric values to the presence or lack of each capability, and apply an algorithm to determine an overall enterprise-readiness index score that is normalized to a number between 0-100.

The score gives you an at-a-glance assessment of whether an app is ready for your enterprise, or if you'll need to limit access and permissions in the ones that can get your organization into trouble.

Using the CCI

The CCI groups apps into more than 50 categories, including cloud storage, collaboration, data and analysis, finance and accounting, customer relationship management, human resources, marketing, and software development. You can search for specific apps or review apps by category to select ones you'd like to recommend to your company. You can also use the app tagging feature to custom tag your apps based on your organizational app classification.

Only Netskope lets you make the CCI actionable by allowing you to incorporate CCI app scores into your real-time policies in the Netskope Active Platform. For example, you can enforce a policy blocking the upload of personally identifiable information (PII) to cloud storage apps with a CCI score of "medium" or below.

Finally, you can fine-tune the CCI for your organization by adjusting the index's input weightings to match your requirements and criteria.

Using the CCI to Maximize your App Investment

The CCI tracks the licensing costs for cloud apps and provides an estimated cost based on the number of users using the app. This helps you understand how much money is being spent on the sanctioned apps you know about and the unsanctioned apps that your users have signed up for without your knowledge. Quickly identify overlapping license usage and gain an upper hand on reducing costs.

Additionally, the CCI reports on the financial viability of apps based on their Dun & Bradstreet (DUNS) number. Quickly discover the business risk associated with a cloud app by viewing the cloud app's Business Viability and Company Profile. Each score has a value from 1 – 10 and has a color band to indicate low, medium, or high viability.

Finally, use the cloud app comparison capability to perform a side-by-side comparison of your final contenders to ensure that you're making the right data-driven decision.

Cloud Confidence Index Score Criteria

In order to determine the cloud confidence index for each app, data scientists at Netskope use a combination of publicly available information and observed app capabilities. The details are summarized in the table below:

FEATURES, BENEFITS AND CRITERIA
AUDIT AND ALERT CAPABILITIES **Ensure an app meets your auditing requirements as well as proactively informs you of app changes or maintenance windows.**
Netskope reviews criteria such as whether the app has Admin Audit Logs, User Audit Logs, and Data Access Logs, and whether they are made available to a subscriber for traceability, investigative purposes or to comply with regulatory requirements etc. Information whether the app provides Change/Upgrade Notifications and Infrastructure Status Reports is also recorded to ensure that a subscriber knows about app functionality changes, maintenance windows for software and hardware changes, as well as remediation status if the app has failed or is experiencing downtime.
CERTIFICATIONS & COMPLIANCE **Comply with regulations and industry guidance that matter to your business.**
Netskope investigates what Compliance Certifications the SaaS app has, including certifications such as HIPAA, PCIDSS20, SP800-53, GAPP, COBIT, Safe Harbor, and TRUSTe. Similarly, the Data Center Certifications that the SaaS app has are also reviewed. Netskope verifies certifications such as SOC-1, SOC-2, SOC-3, SAS70/SSAE-16, ISO27001, and ISO/IEC 27018.
DATA CLASSIFICATION CAPABILITIES **Classify your organizations' data, e.g., "public" or "confidential," so you can enforce policies on your content as necessary.**
Netskope looks into whether app Allows Classification of Data stored in their application into different security types and whether the app Treats Data Differently Based On Classification in terms of encryption, access control, etc. Additional information is reviewed to ascertain whether the app Allows Customer To Download Their Data When Leaving the service, When All Customer Data Is Erased, and Who Owns The Data/Content Uploaded to the app.
DISASTER RECOVERY & BUSINESS CONTINUITY **Minimize downtime or data loss in the event of an app failure or problem.**
Netskope reviews whether the app vendor Backs Up Customer Data In a Separate Location From Their Data Center, Utilizes Geographically Dispersed Data Centers to serve customers, Provides Disaster Recovery Service To All Customers, and investigates which IaaS/PaaS/Hosting Provider the app is hosted on. These details help give you the confidence that you will ensure business continuity data access in the event of a system failure or disaster. Additionally, it helps you determine your own recovery and remediation steps in case you have business-critical or sensitive data housed in an app that it is impacted by a disaster in a single location or even across an entire region.
ENCRYPTION **Ensure that any data that are stored and transmitted meet your data protection standards and policies.**
Netskope reviews whether the app Encrypts Data At Rest and Encrypts Data In Transit. For data at rest, Netskope also identifies what standard of encryption is used; for example, AES-256, RSA, DES, BitLocker, Blowfish etc. Additionally, we look into whether the app Segregates Data By Tenant and whether the app Supports Encryption With Tenant Managed Keys. This helps ensure that customer data aren't co-mingled with one another, that each tenant uses separate keys and that one tenant's breach or corruption won't impact others'.
FILE SHARING **Make sure the app will meet user requirements for sharing and collaboration.**
Netskope reviews whether the app Supports File Sharing and if it does, what File Sharing Capacity is supported, as well as if the app Allows Anonymous Sharing Of Data. The capacity is classified into Less than 5 GB, 5 GB - 10 GB and 10 GB And Over. This helps you determine whether it will be a good fit for your storage needs.

FEATURES, BENEFITS AND CRITERIA
POLICY ENFORCEMENT AND ACCESS CONTROL **Confirm similar levels of access controls and policy enforcement in cloud apps as in the rest of your environment.**
Netskope investigates what the Devices Supported are, and whether the app has a native client for each OS, on the following platforms: iOS, Android, Windows Mobile, BlackBerry, Browser or Desktop devices. Next, we look to see if the app Enforces Password Best Practices, supports Granular Action Based Authorization Policies, supports IP Filtering, and Has Role and Auth Based Support. This helps you determine whether the app enforces complex passwords, password durations, etc. to ensure data security and regulatory compliance, whether an app administrator has the ability to control authorizations for certain activities within the app, whether the app can use the user's source IP in order to control access to the app, and whether the app admin can segregate administrative privileges to ensure user privacy as well as limit impactful administrative changes to only a certain few, closely monitored individuals, respectively. Finally, we determine whether the app has SSO/AD Hooks, and if it Supports Multi-factor Authentication. The SSO/AD hooks criteria helps determine what are the available authentication mechanisms for the app, such as SAML, OAuth, OpenID, and Microsoft AD/LDAP. This also surfaces whether the app provides the ability to login with social media credentials such as Facebook, Twitter or Google. Support for multi-factor authentication reviews whether the app supports 2-factor or more factors of authentication such as one-time password (OTP) tokens, soft tokens, etc. to provide that additional layer of security.
REAL-TIME POLICY ENFORCEMENT **Inspect traffic to perform analytics and enforce your policies in real-time.**
This looks into whether it is possible to Proxy App Traffic, essentially looking at whether the app has enforced certificate/ public key pinning.
HTTP SECURITY HEADERS **Identify and safeguard against websites that are susceptible to attack by reviewing the security headers they employ.**
HTTP security headers were introduced to enhance the security of websites. Netskope reviews websites to determine whether they use security headers such as Content Security Policy, XSS-Protection, HTTP Strict Transport Security, X-Content-Type-Options, and X-Frame-Options.
SECURITY VULNERABILITIES & EXPLOITS **Ensure that your organization is not a candidate for data breach, damage to brand reputation, or loss of customer trust.**
This investigates whether the app is subject to Vulnerabilities & Exploits such as Heartbleed, OpenSSL CCS Injection, POODLE SSL v3 Fallback, FREAK, Logjam etc.
PRIVACY **Identify weak spots in your security program that could lead to potential data breaches by clearly understanding how your employees' privacy is handled by apps on mobile and browsers.**
This looks into the app privacy details around Mobile devices and Browsers. For mobile, Netskope helps determine whether the App Requires Access to Contacts, Calendar Data and Messages, whether the App Requires Access to Other Apps On The Device, and whether the App Performs System Operations. For browsers, Netskope helps determine whether the App Shares Personal Information (Name, Email, Address etc.), and whether the App Uses Third-Party Cookies.

About Netskope

Netskope™ is the leading cloud access security broker (CASB). Netskope gives IT the ability to find, understand, and secure cloud apps. Only Netskope empowers organizations to direct usage, protect sensitive data, and ensure compliance in real-time, on any device, for any cloud app so the business can move fast, with confidence.