Netskope Cloud Risk Exchange

Data Sheet

Cloud Risk Exchange enables zero trust principles

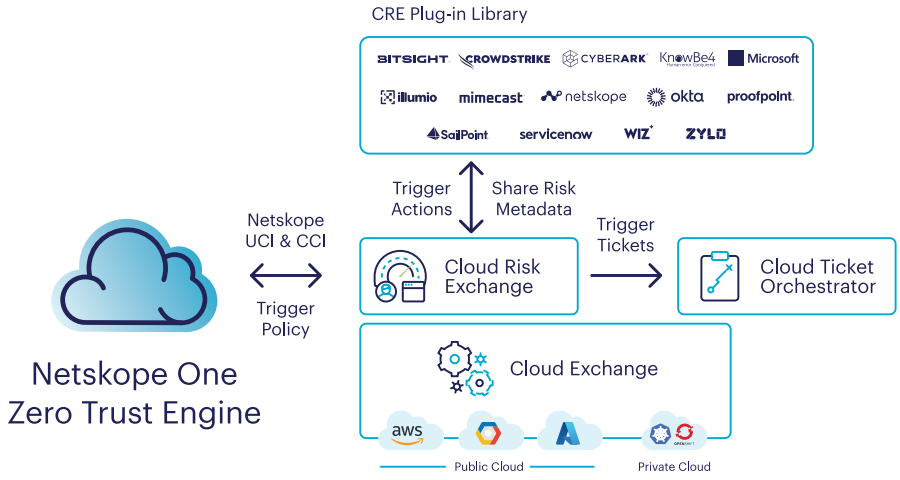
Cloud Risk Exchange (CRE) creates a single view into multiple connected systems' risk values for individual users, devices, or workloads/applications. Security analysts can match various scores, as nested, to trigger targeted actions in connected systems to drive overall IT risk reduction.

Why is Netskope the best choice?

The CRE module, a part of Netskope Cloud Exchange (CE), is a risk reduction service offered at no cost to customers. CRE enables customers to create a consolidated business rule framework based on third-party telemetry that maps to the Netskope Zero Trust Engine. It includes a library of supported plugins that can be configured to retrieve additional context across key risk pillars.

Get a snapshot of integrated risks and trends:

- **See your top concerns at a glance.** CRE brings together scores from your selected plug-ins, in clear dashboard format.
- **Normalize risk scores.** Decide for yourself what constitutes a high, medium, or low score for each plug-in, adjusting as needed.
- **Comprehensive view of risk trends.** Identify your riskiest users, devices, and workloads/applications and compare results over time.
- **Take action automatically.** Easily set business rules to trigger risk-reducing actions based on derived weighted scores.



Key Benefits and Capabilities

Reduce risk and enable zero trust principles

CRE collects disparate risk signals from a partner-enabled risk exchange ecosystem to drive IT risk reduction and provide greater visibility, responsiveness, and organization-wide agility.

Automated responses

Business rules let you automatically activate focused actions that reduce risk caused by individuals, devices, or workloads/applications.

Top risk scores presented in a dashboard

Use CRE to view one or more user, device, or workload/application risk scores from plugins like BitSight, CrowdStrike, KnowBe4, Microsoft, Okta, ServiceNow, and Wiz.

Custom score normalization

Business rules let you automatically activate focused actions that reduce risk caused by individuals, devices, or workload/applications.

> "It's really about zero implicit trust, as that's what we want to get rid of [1]."
>
> - Neil MacDonald, Distinguished VP Analyst, Gartner

[1] https://www.gartner.com/smarterwithgartner/new-to-zero-trust-security-start-here

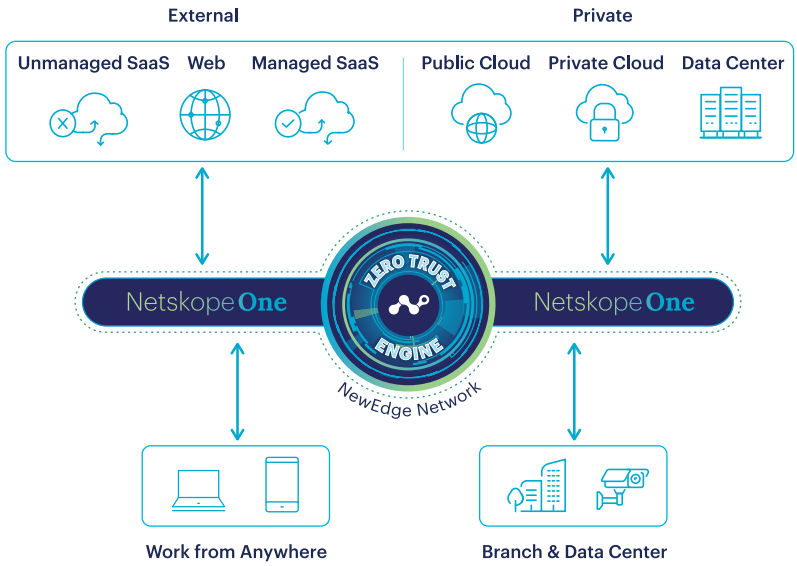
Reduce risk and enable zero trust principles

Netskope CRE-enabled customers can now automatically aggregate and normalize risk scores and labels based on a customer's unique take on what constitutes risk. Netskope aims to deliver integrations by consolidating additional context across the corporate digital estate involving identity (users, device, apps, workload, instance, data), location, activity, and behavior. Let's expand on what we mean across the following risk signal pillars:

NETSKOPE ZERO TRUST ENGINE RISK PILLARS	CAPABILITY
Activity Trust	Is a key pillar and Netskope differentiator with its unique insights into user actions, not yet informed by third parties.
App Trust	Is when Netskope learns about workloads from Wiz, CrowdStrike, or Illumio and Netskope updates the Netskope ZTNA configuration to reflect these updates. This information is further used to coach, limit, or block access and activities when an app is reported as a risk. Third-party app risk assessment solutions like BitSight, CrowdStrike CNAPP, Wiz, or ServiceNow may have insights into breaches or overall activity that increase risk to users. Identity providers (IdPs) like Okta and Microsoft can tell Netskope which apps have been federated for single sign-on. SaaS spend partners like Zylo and Productiv can tell Netskope when app subscriptions have been contractually approved. IT service management (ITSM) partners like ServiceNow can tell Netskope which apps have been fully onboarded.
Behavior Trust	Can be surfaced by advanced IdPs and companies with ML engines to discern normal from abnormal persona behavior. Integrations, such as with KnowBe4, identify poorly educated employees. CyberArk shares high-risk administrators. Mimecast shares high-risk spear-phishing victims. SailPoint shares ungoverned users, and Okta with its Okta Identity Threat Protection product.
Data Trust	Partners surface key findings, starting with persistent labels, around risky data, such as the Netskope integration with Microsoft Purview and Fortra.
Device Trust	Looks at whether hosts are safe or are compliant, vulnerability-free, non-compromised, and/or cooperate with solutions from Microsoft Defender for Endpoints.
Identity Trust	Incorporates findings from multiple partners for multiple use cases. These include compromised user or compromised private workloads from IdP partners like Okta, Microsoft Entra ID, CrowdStrike Falcon Identity Protect, Mimecast, and microsegmentation partners like Illumio that inform Netskope of sanctioned workloads or if those app workloads should be quarantined, or CNAPP partners like CrowdStrike and Wiz that also surface and differentiate safe and known from the high-risk public cloud workloads.
Instance Trust	Is when we learn that there is an inline and publicly reachable service that is explicitly known and identified by a third party, and particularly for cloud hyperscalers, are key findings of CNAPP partners like CrowdStrike and Wiz. Netskope can enforce appropriate access (or not) to these unsanctioned or high-risk services until they are compliant.

The Netskope Difference

Netskope One is a converged security and network as a service platform. Through its patented Zero Trust Engine, AI innovation, and the largest private security cloud we make it easy for our customers to defend their businesses and data while delivering a phenomenal end user experience and simplified operations. The platform delivers AI-powered data and threat protection that automatically adapts to the ever growing data landscape, including the widespread adoption of generative AI and new AI-driven attacks.



Top risk scores presented in a dashboard

Use CRE to view one or more user, device, or workload/application risk scores from plug-ins like BitSight, CrowdStrike, KnowBe4, Microsoft, Okta, ServiceNow, and Wiz.

FEATURE	CAPABILITY
Interval Configuration	Configure the frequency of polling.
Query Filtering	Filter queries to the exact types of scores desired to be retrieved.
Alerts	Receive alerts in your IT service management platform or receive notifications when an action is performed on users, devices, or applications. (Requires Netskope Cloud Ticket Orchestrator module.)
Dashboard	• Shows the average score of all tracked users, devices, or workloads/applications, the score of the current day and the day before, the delta between those scores, and the score trend over a configurable time frame. • Displays top 10 riskiest users (with the lowest weighted score). • View all and filter capabilities help you find the individual user, device, or workload/application scores and modify, as needed. • Set and modify weights of individual plugin scores.
Supported plug-ins	• BitSight • CrowdStrike • CyberArk • KnowBe4 • Microsoft • Mimecast • Illumio • Mimecast • Netskope • Okta • Proofpoint • Sailpoint • ServiceNow • Wiz • Zylo

netskope

Interested in learning more? Request a demo

Netskope, a global SASE leader, uses zero trust principles and AI/ML innovations to protect data and defend against cyber threats, optimizing both security and performance without compromise. Thousands of customers trust the Netskope One platform and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity. Learn more at netskope.com.