

Detect and control insider risk and compromise

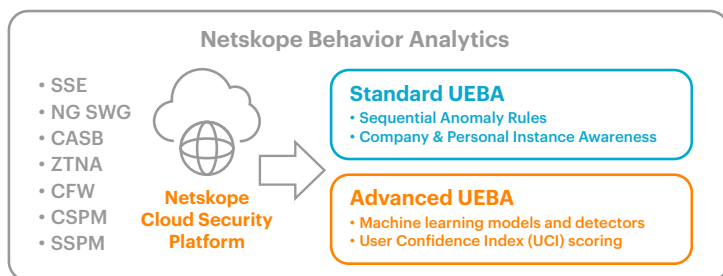
Rich metadata across five types of user traffic for web, apps, cloud services, shadow IT, and public facing custom apps drive Netskope Behavior Analytics to detect the unknown including activity between company and personal app instances.

WHY IS NETSKOPE THE BEST CHOICE?

Netskope single-pass inspection for web and cloud traffic, plus API inspection of managed apps and security posture management provides a wealth of context for user and entity behavior analytics (UEBA). Anomaly and alert correlation drive user risk scoring for adaptive policy controls, real-time coaching, step-up authentication, and investigations.

BEHAVIOR ANALYTICS DRIVEN BY RICH CONTEXTUAL METADATA TO DETECT THE UNKNOWN

- **Machine learning anomaly detection and correlation:** Understands user behavior baselines for uploads, downloads, and app activity to determine multiple anomalies to then correlate into alerts.
- **Sequential anomaly rules across apps and cloud services:** Quickly detect bulk data activity (upload, download, delete), plus failed logins, proximity, rare events, and suspicious data movement.
- **App instance awareness of company and personal:** Understands data movement between company and personal app instances, often related to employment changes or insider activity.
- **User Confidence Index (UCI) scoring drives adaptive policies:** UCI ranges from 1000 (good) to 1 (low) based on UEBA and other policy alerts to drive adaptive policy controls.



KEY BENEFITS AND CAPABILITIES

Detect insiders' anomalous behaviors

From baselines and peer groups detect anomalies for data activity, movement, including between managed and personal apps.

Detect unknown data movement

UEBA alerts highlight suspicious data movement visualized in Netskope Advanced Analytics Sankey charts by user, app, instance, and activity.

Trust-driven adaptive policy controls

Leverage user (UCI) and app risk (CCI) scores in adaptive policy controls to provide safer app alternatives, real-time coaching, justification, request step-up authentication, or limit the type of app activity.

Profile user risk

Dashboards quickly show high-risk users, significant changes in user risk, event correlation timelines, and investigation drill down details.

Cloud Risk Exchange

Enables customers to exchange risk scores such as UCI with third-party solutions, plus ingest user and device risk scores to compute weighted and daily averages. Cloud Risk Exchange is no charge to customers as an integration module.

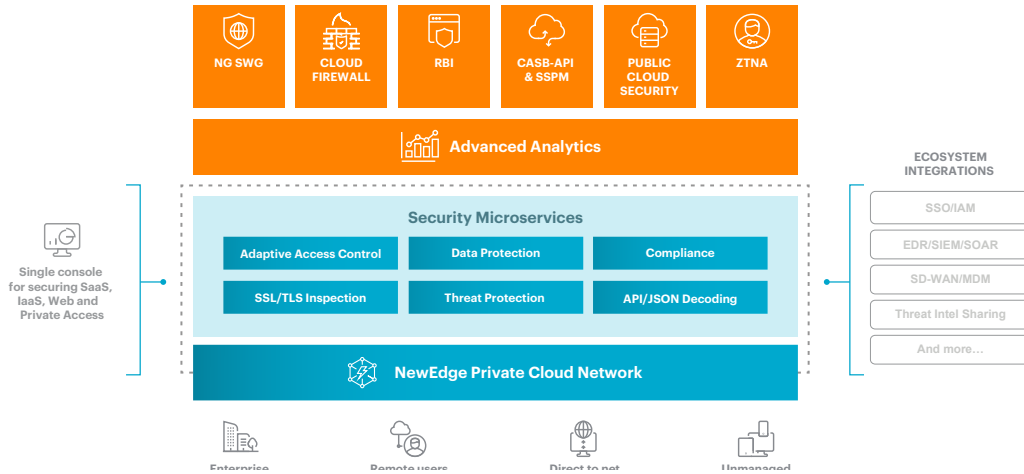
“In their last 30 days of employment, one-third of the users leaving an organization create a spike in uploads to personal instances that is three times higher than their baseline behavior.”

– NETSKOPE CLOUD AND THREAT REPORT, JULY 2021

THE NETSKOPE DIFFERENCE

Fast everywhere, data-centric, and cloud-smart.

Using patented technology called Netskope Cloud XD™, the Netskope Security Cloud eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud (SaaS and IaaS) services and millions of websites. With full control from one cloud, our customers benefit from 360-degree data protection that guards data everywhere and advanced threat protection, including targeted RBI for risky websites that stops elusive attacks.



YOUR NEEDS	THE NETSKOPE SOLUTION
Standard UEBA	Includes sequential anomaly rules to detect cloud app bulk data uploads, downloads, deletes, plus proximity, failed logins, shared credentials, rare events, risky countries, and data exfiltration between company and personal app instances.
Advanced UEBA	Includes Standard UEBA, with the added ability to customize sequential rules, plus 25+ machine learning (ML) based anomaly detection models for insiders, compromised accounts and devices, and data exfiltration use cases. Advanced UEBA also includes 30+ detectors including inline, API, and private access.
User Confidence Index (UCI)	Included with Advanced UEBA, UCI provides user risk scoring and event correlation timelines with the ability to invoke policy actions based on score, and a REST API for UCI export. UCI is key to detecting insiders with alert and event correlation on data activity and movement.
Adaptive Policy Controls	Leverage UCI scores for adaptive policy controls, including step-up authentication, real-time coaching, justifications, limiting activity, or blocking based on other policy variables including data sensitivity and app risk.
Cloud Risk Exchange	Cloud Risk Exchange is a no-cost integration module for customers to exchange user and device risk scores, including UCI for risk curation and remediation actions with technology partners.



Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, Netskope is fast everywhere, data-centric, and cloud-smart, all while enabling good digital citizenship and providing a lower total-cost-of-ownership.