Netskope One Behavior Analytics

Data Sheet

Detect and control insider risk and compromise

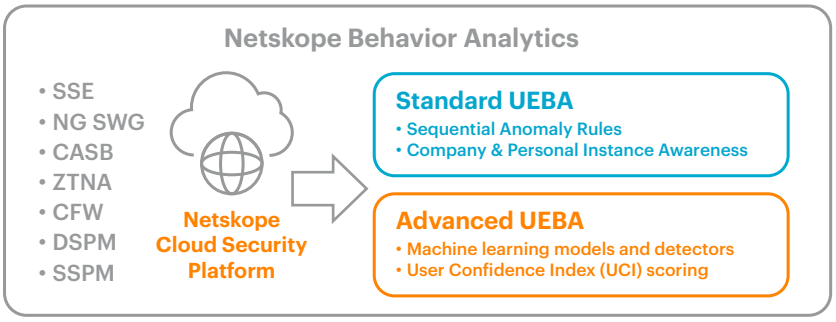
Rich metadata across five types of user traffic for web, apps, cloud services, shadow IT, and public facing custom apps drive Netskope Behavior Analytics to detect the unknown including activity between company and personal app instances.

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.

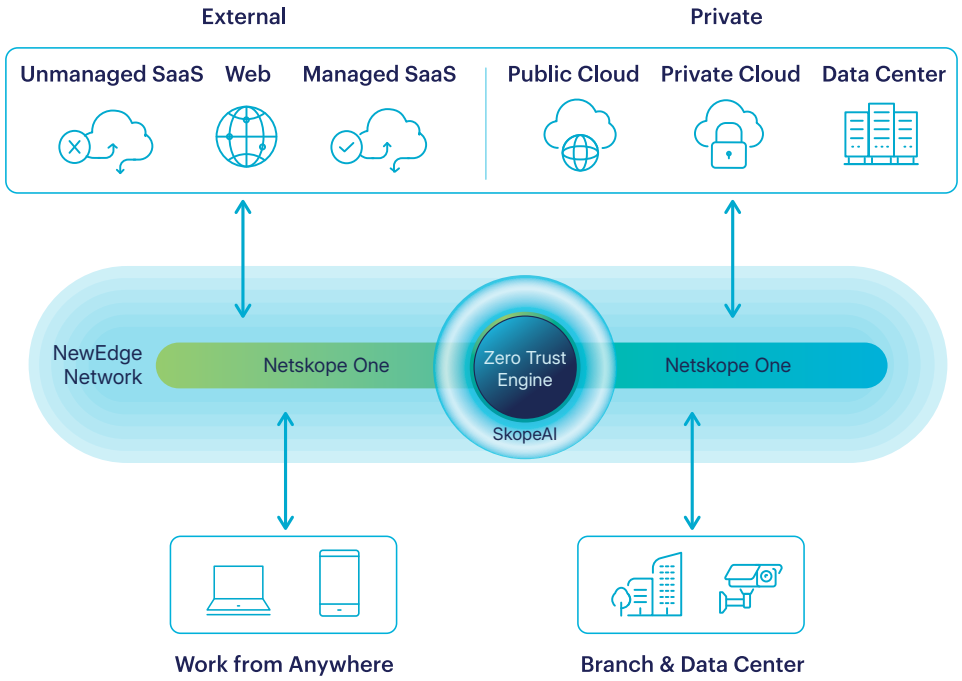
Cloud Risk Exchange
Enables customers to exchange risk scores such as UCI with third-party solutions, plus ingest user and device risk scores to compute weighted and daily averages. Cloud Risk Exchange is no charge to customers as an integration module.

"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

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.



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 65+ machine learning (ML) based anomaly detection models for insiders, compromised accounts and devices, and data exfiltration use cases. Advanced UEBA also includes 180+ 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.
C2 Beacon Detection	SOC Detection Pack (add-on with Advanced UEBA) enables AI/ML-based models to detect adversarial beacon anomalies with user and organization baselines. Command and control (C2) beacons from malleable frameworks like Cobalt Strike or Mythic are hard to detect with traditional defenses, however, ML models flip the scenario analyzing beacon behavior.

netskope

Interested in learning more? Request a demo

Netskope, a leader in modern security and networking, addresses the needs of both security and networking teams by providing optimized access and real-time, context-based security for people, devices, and data anywhere they go. Thousands of customers, including more than 30 of the Fortune 100, trust the Netskope One platform, its Zero Trust Engine, and its powerful NewEdge network to reduce risk and gain full visibility and control over cloud, AI, SaaS, web, and private applications—providing security and accelerating performance without trade-offs. Learn more at netskope.com.