netskope

SOLUTION BRIEF

Managing Insider Risk

Insider risk is a major challenge for security teams because it involves trusted users who may accidentally or intentionally engage in activity that opens the doors to a security incident. Regardless of the motivation, organizations must take steps to manage insider risk before it manifests into a data breach.

KEY USE CASES

- **Prevent Accidental Data Loss:** Check application configurations, identify publicly shared cloud storage, monitor sensitive data movement, and coach users.
- **Disrupt Attack Kill Chains:** Stop cloud phishing, command and control, and unauthorized access to stop attackers from impersonating valid users.
- **Uncover Behavior Anomalies:** Monitor risky/malicious behaviors with Netskope UEBA to detect insiders, compromised accounts, and data exfiltration.
- **Make Policy Decisions Based on Risk:** Use User Confidence Index (UCI) risk scoring with adaptive policy controls.

"One out of every seven users take data with them when they leave using personal app instances."

NETSKOPE THREAT LABS, CLOUD AND THREAT REPORT, JANUARY 2022

THE CHALLENGE

With insider risk, the actor isn't trying to gain access. The user already has access, but may take actions that place the organization's data at risk.

As such, insider risk stresses the organization's ability to control authorizations and dynamically adapt to changing circumstances, such as when the user starts acting in unconventional ways. It requires the security team to develop a nuanced understanding of user activities and behaviors, and evaluate when deviations occur. Authorization policies are particularly challenging to manage, because policies must evolve as conditions change and as people join and depart various roles. Security teams must find ways to stay on top of change, as it happens, and adapt as necessary.

MANAGING INSIDER RISK

Instead of chasing every possible threat permutation, organizations should address insider risk from the inside out. Start by using data protection to manage access to critical assets and control movement. Use contextual, behavior-driven controls to enable dynamic authorization policies based on risk factors and signals from the environment. Apply behavioral analytics, machine learning, and visualizations to focus on what's going on, and what's changing. These capabilities are a part of the Netskope Security Cloud.

NETSKOPE SECURITY CLOUD

The Netskope Security Cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps from anywhere, on any device. Only Netskope understands the cloud and delivers data-centric security from one of the world's largest and fastest security networks.

The rapid adoption of cloud apps, services, and mobile devices has resulted in data going to places where traditional security technology is blind. Netskope takes a data-centric approach to cloud security, following data everywhere it goes. From data created and exposed in the cloud to data going to unmanaged cloud apps and personal devices, Netskope protects data and users everywhere.

To address insider risk, Netskope Security Cloud delivers a number of key capabilities:

- **Data Protection:** Data protection in the Netskope Security Cloud provides both inline-based controls for data movement and API-based controls to monitor data at rest. In addition, Netskope Cloud XD and Next Gen SWG deliver zero trust data protection policy controls based on criteria such as users, applications, instances, and data.

- **Contextual Behavior:** Driven Risk Controls: User and Entity Behavior Analytics (UEBA) with AI/ML models dynamically identifies user and application risk factors to generate real-time user risk scores that influence adaptive policy decision.

- **Analytics:** Netskope Advanced Analytics provides a deep understanding of activity in the organization's cloud, with pre-build and customizable dashboards designed to stay ahead of threats.

DATA PROTECTION

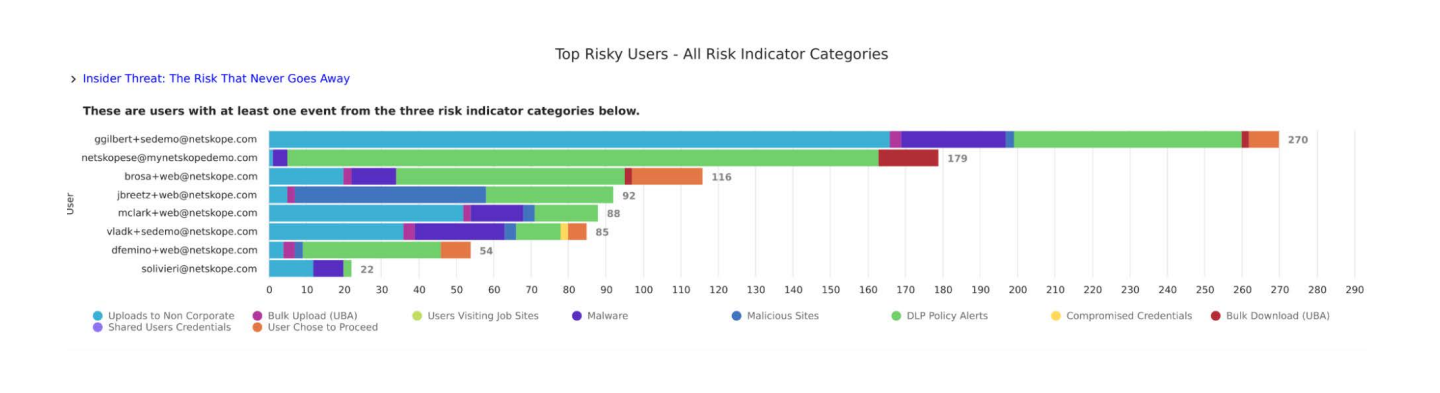
Data is the end game for many insider threats. As a baseline security measure, taking steps to prevent data loss helps disrupt both known and unforeseen threat vectors. However, many organizations with traditional enterprise DLP lack controls designed for cloud data protection, thus providing a poor fit against the current threat landscape.

Netskope delivers DLP for the cloud, from the cloud. It provides inline controls for policies over data access and movement, as well as API-based controls to monitor when data is improperly stored at rest, shared, or moved between cloud instances.

With Netskope, establish contextual zero trust access controls that reduce the attack surface area and decrease the amount of content required for inspection by DLP policies. For example, policies based on application, instance, and device can be combined to stop employees from downloading data to unmanaged and unprotected devices and to non-company managed accounts. Contextual policies help organizations establish layers of data protection, making it increasingly difficult for a malicious insider to advance on their goals and stop users from making careless mistakes, without impeding normal business processes.

"85% of Breaches Profiled Involved a Human Element"

Verizon, "2021 Data Breach Investigations Report Executive Summary"



CONTEXTUAL BEHAVIOR CONTROLS

Protections are only as effective as the policies that establish who and what they apply toward. With insider risk, threats exist within a gray area of potentially valid use, which makes policies much harder to define. The user is already trusted, but the user's intent is unknown, and any given action may or may not be dangerous. For example, a user downloading data is not necessarily a sign of a problem, but bulk downloads followed by uploads to a personal instance might be a sign of exfiltration.

Therefore, risk is not just access but also actions and activities. Netskope applies UEBA, which uses AI/ML models, to define when a particular set of conditions crosses the line for concern. The AI/ML models also build a user risk profile (User Confidence Index) that also can be applied to policy that governs authorizations to perform a given set of cloud activity.

In addition, use contextual enforcement of real-time coaching for handling policies in the gray zone. Your users may have a valid business justification for conducting risky actions, and coaching encourages the user to make safer decisions with the knowledge that proceeding with risky activity will be recorded and monitored.

DATA AND ANALYTICS

To find an insider, security teams have traditionally had to sift through an overwhelming amount of incongruous information that often lacks context. This work is not easy, especially when such efforts lead to dead ends.

Organizations must find better ways to make investigations more efficient and avoid wasted time. The proper toolset to assist with this work should establish visibility to see all activity along with the visualizations to interpret what's happening.

With Netskope Advanced Analytics, your teams can quickly get an understanding of their cloud environment and immediately drill into the details to see if there is an emergent issue. SecOps can monitor the Insider Threat dashboard to review risk factors such as application use, data download/uploads, and UEBA/DLP policy violations. If a particular user merits further investigation, the User Activity dashboard can be used for a broader examination of the user's actions with their associated logins. Dashboards can be enhanced and customized to meet your organization's requirements, making it possible to zero in on insider risks before damage is done.

"One-third of users leaving an organization create a spike in uploads to personal instances three times higher than baseline."

Cloud and Threat Report July 2021 Edition

BENEFITS	DESCRIPTION
Simplifies operations for better efficiency	Integrated analytics speeds up investigations, helping your team eliminate the noise and prioritize effort.
Delivers protection against multiple inside threat vectors	Stop accidental and malicious insider threats using layers of defenses across the entire kill chain.
Reduces effort with visibility and risk assessment automation	Use AI/ML to identify behavioral risks that are otherwise missed by traditional security policies.
Get precise control over your cloud	Contextual policies powered by Netskope Cloud XD provide visibility and control over high-risk activity.